www.mientayvn.com

Khi đọc qua tài liệu này, nếu phát hiện sai sót hoặc nội dung kém chất lượng xin hãy thông báo để chúng tôi sửa chữa hoặc thay thế bằng một tài liệu cùng chủ đề của tác giả khác. Tài liệu này bao gồm nhiều tài liệu nhỏ có cùng chủ đề bên trong nó. Phần nội dung bạn cần có thể nằm ở giữa hoặc ở cuối tài liệu này, hãy sử dụng chức năng Search để tìm chúng.

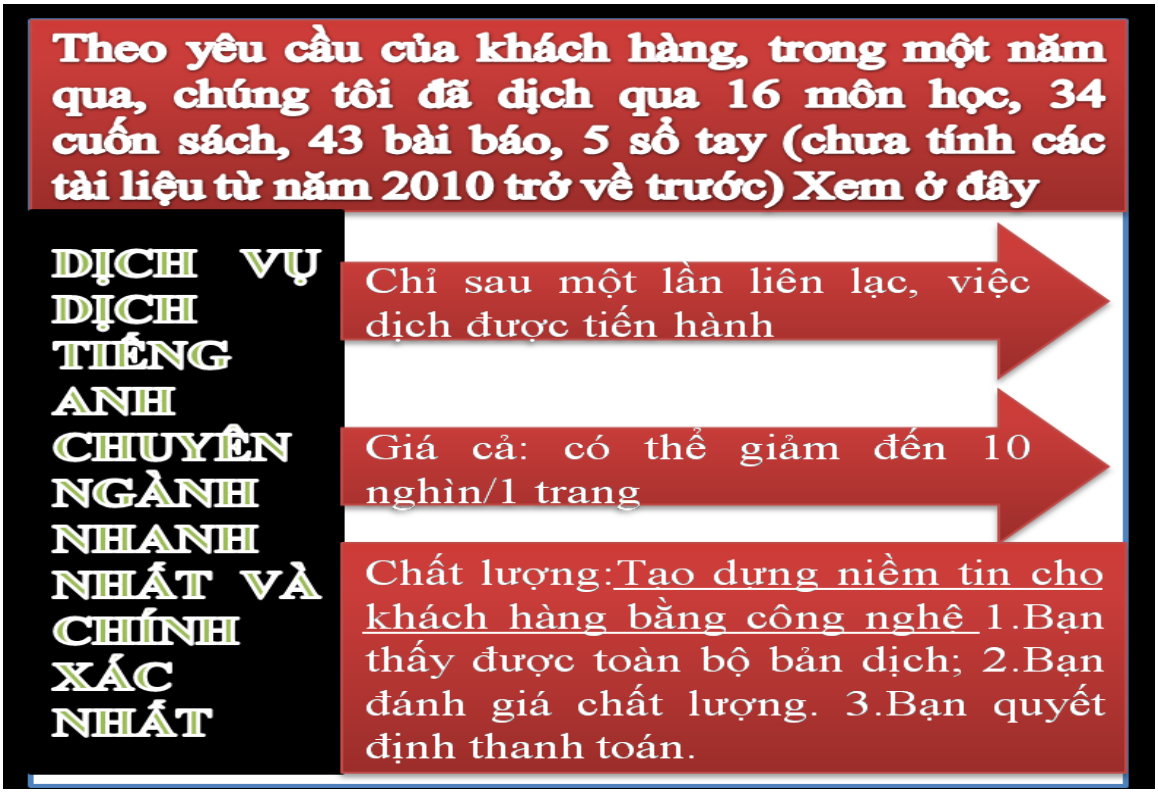
Bạn có thể tham khảo nguồn tài liệu được dịch từ tiếng Anh tại đây:

http://mientayvn.com/Tai_lieu_da_dich.html

Thông tin liên hệ:

Yahoo mail: thanhlam1910_2006@yahoo.com

Gmail: frbwrthes@gmail.com



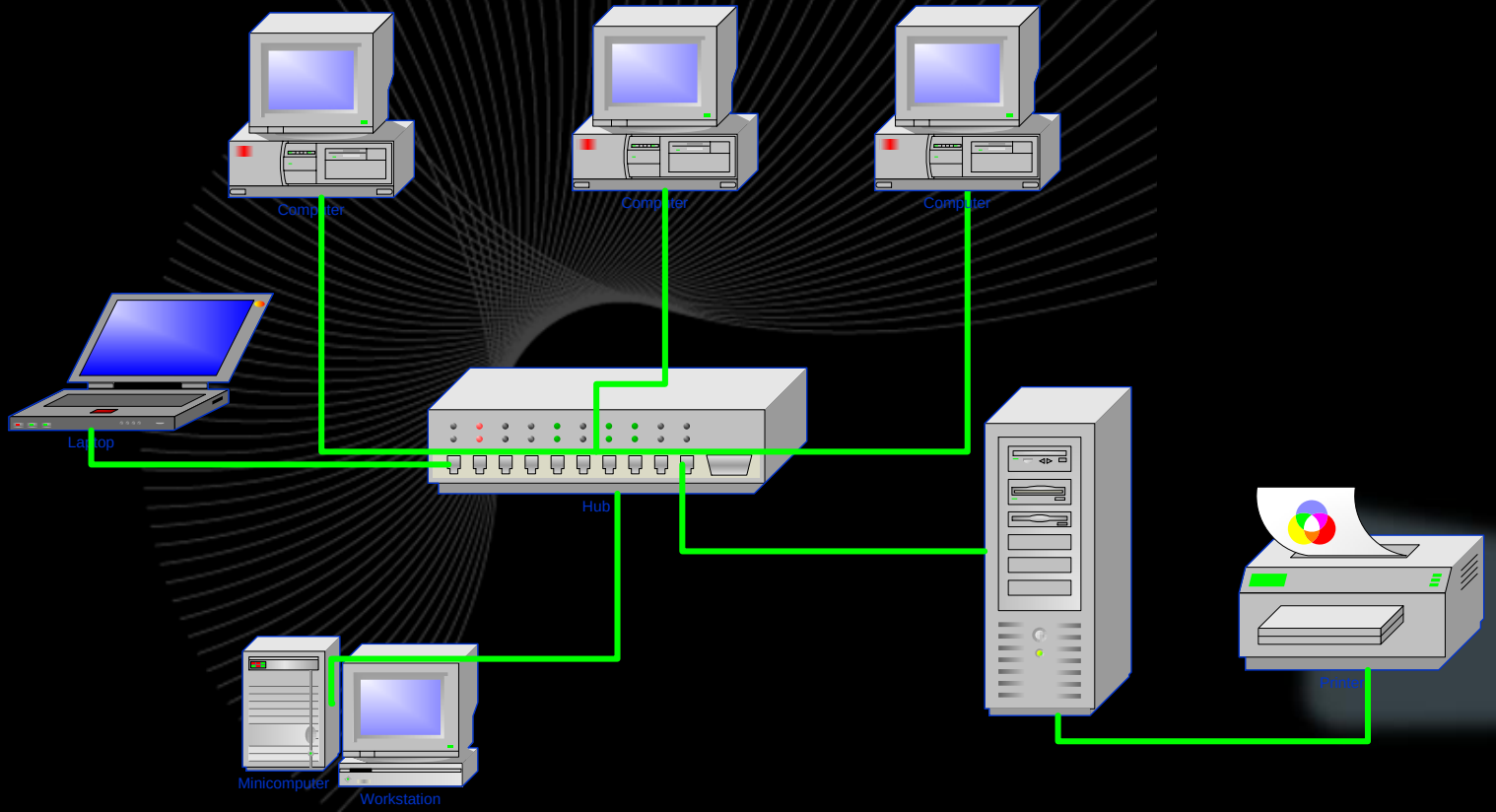
# Mạng máy tính

- Vì sao phải kết nối mạng ?
- Khái niệm mạng máy tính
- Lợi ích của mạng máy tính

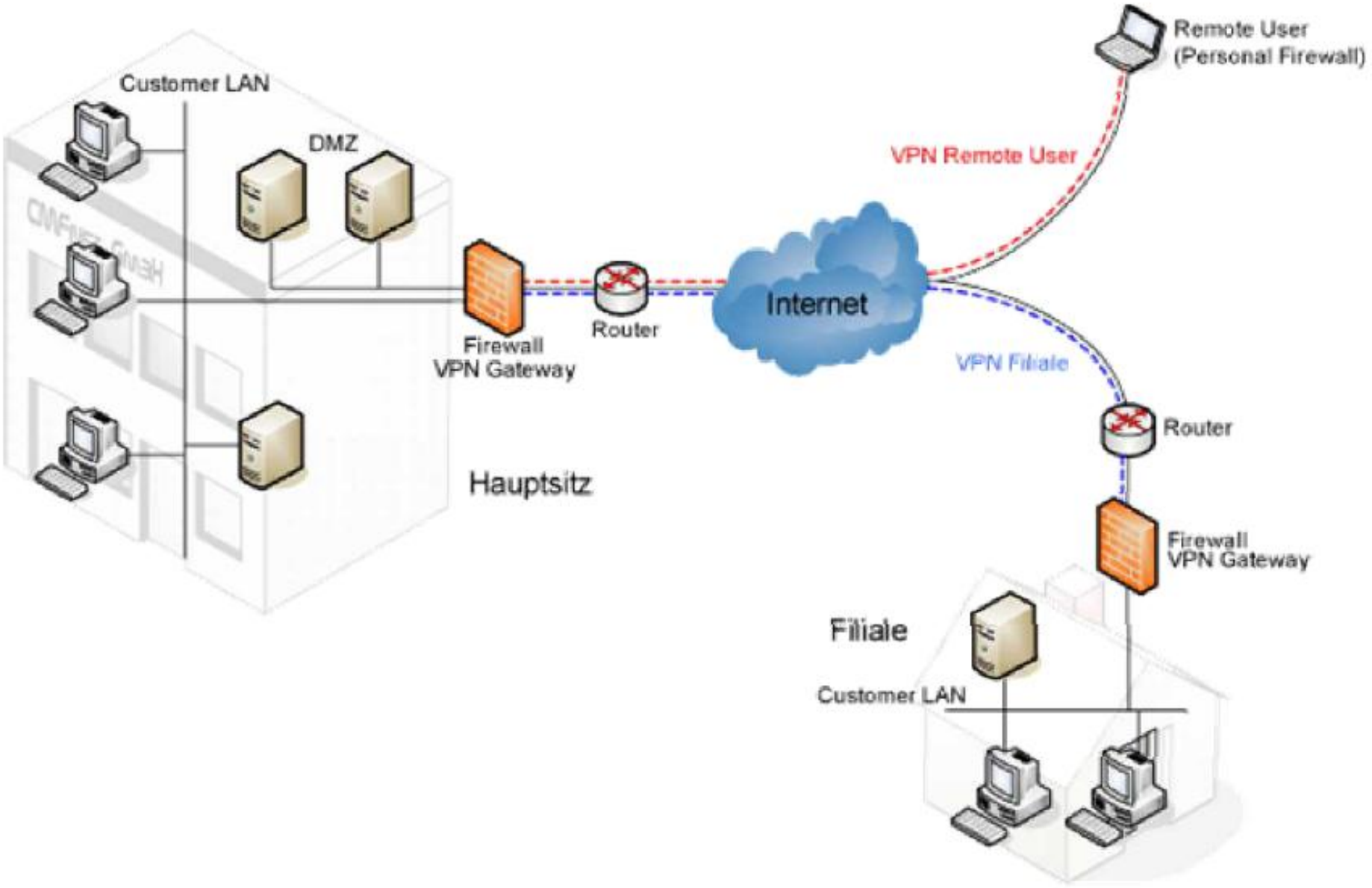
# Vì sao phải kết nối mạng ?

# Khái niệm mạng máy tính

- Mạng máy tính là tập hợp **nhiều máy tính điện tử và các thiết bị đầu cuối** được kết nối với nhau bằng các thiết bị liên lạc nhằm **trao đổi** thông tin, cùng **chia sẻ** phần cứng, phần mềm và dữ liệu.

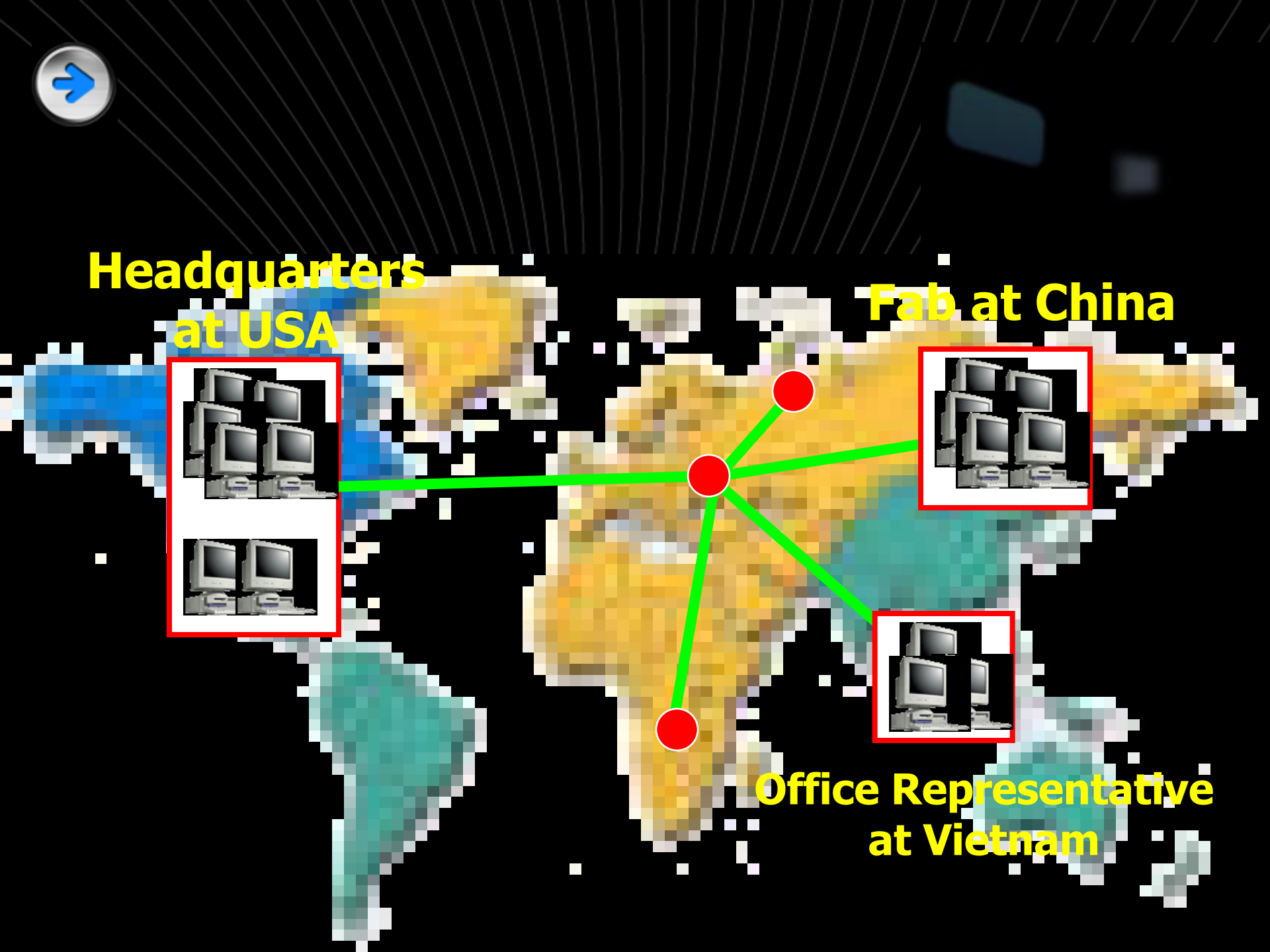


# Mạng máy tính – Ví dụ



# Lợi ích của mạng máy tính

- **Trao đổi và chia sẻ thông tin nhanh chóng**
  - Trao đổi thư điện tử (email)
  - Trò chuyện trực tuyến (chat)
  - Chia sẻ thông tin trên internet
  - Học tập trực tuyến (e-learning)

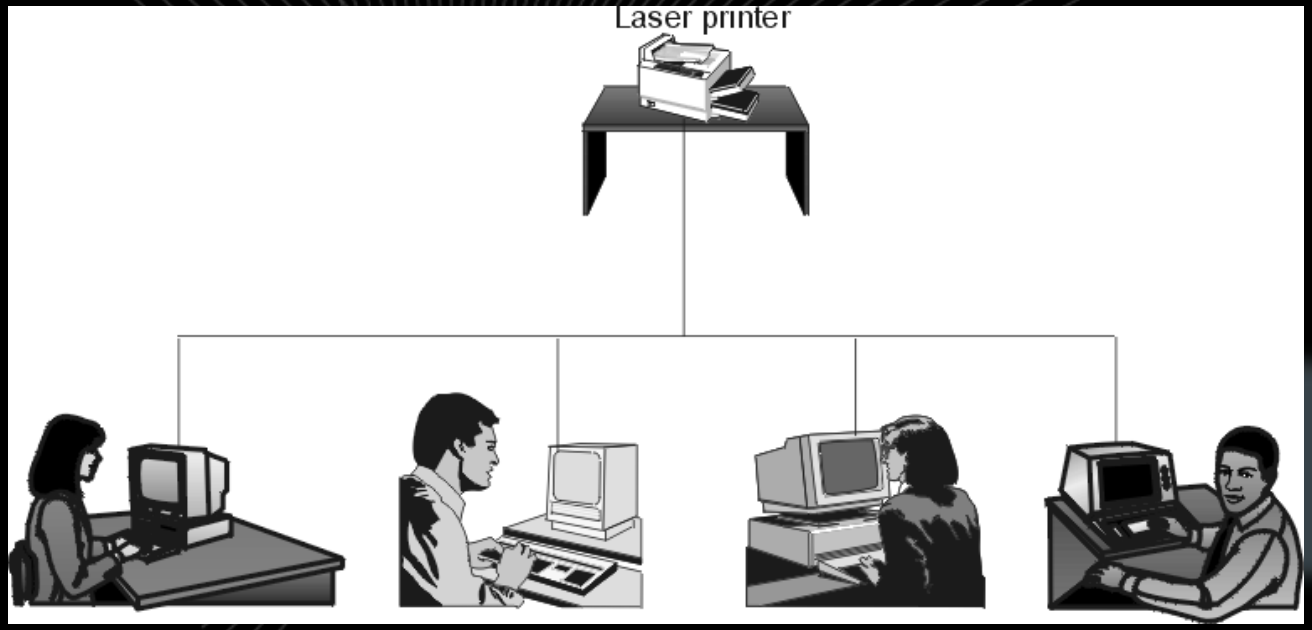

Headquarters
at USA
Fab at China
Office Representative
at Vietnam

# Lợi ích của mạng máy tính

- **Chia sẻ và sử dụng chung tài nguyên**

**Tài nguyên:**

- Dữ liệu
- Phần cứng (CD-ROM, máy in, ổ cứng, … )
- Phần mềm (Các chương trình)



# Lợi ích của mạng máy tính

- Nâng cao độ tin cậy
- Công việc đạt hiệu suất cao
- Tiết kiệm chi phí
- Tăng cường tính bảo mật thông tin
- Thống nhất dữ liệu
- Tăng cường khả năng tính toán
- ……

# Supercomputers

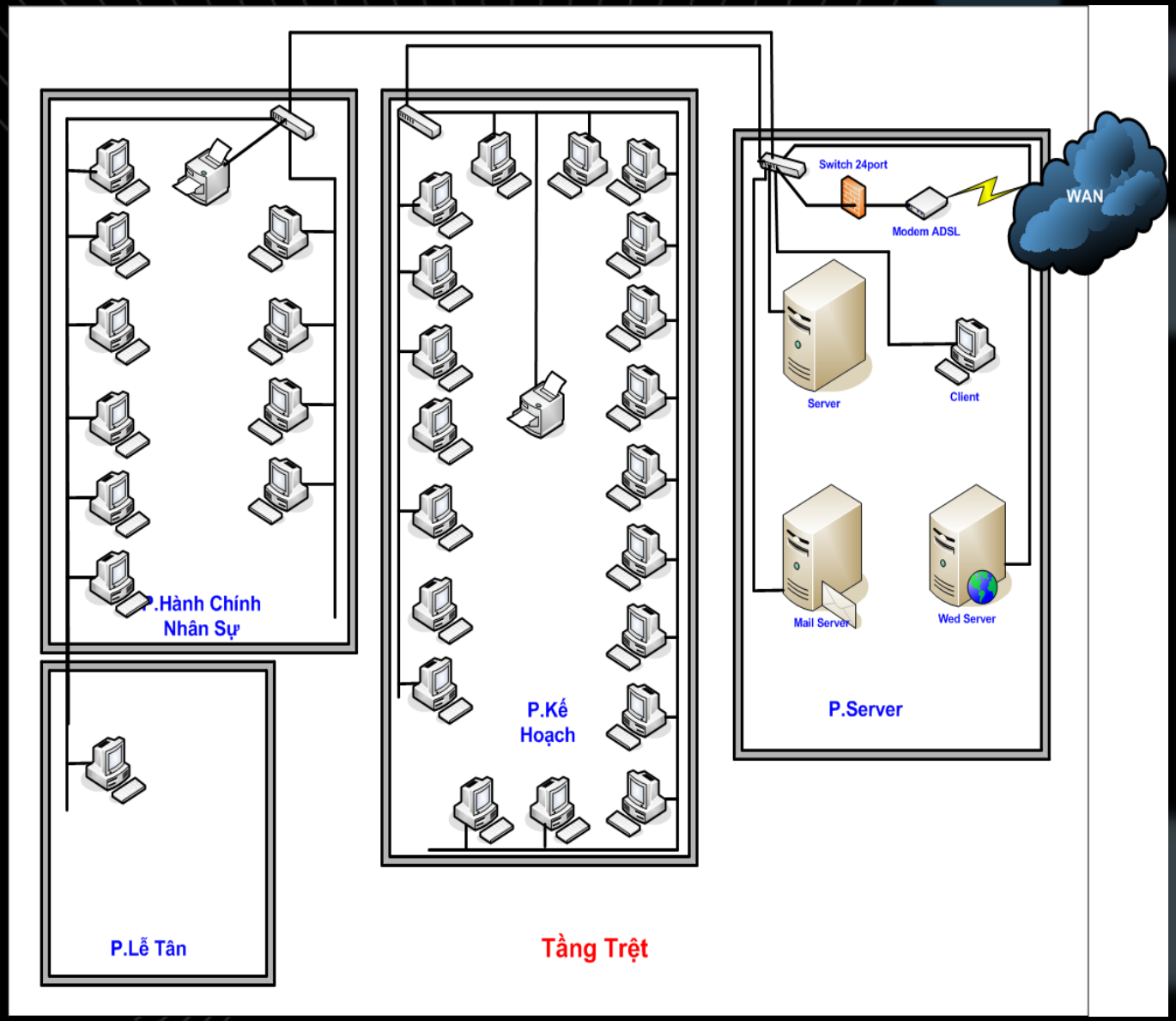
- Dùng trong các tổ chức có yêu cầu tính toán đặc biệt, tốc độ cực kỳ cao và chính xác.

# PHÂN LOẠI MẠNG

- **Có 3 cách phân loại mạng cơ bản sau:**
  - Phân loại mạng theo phạm vi
  - Phân loại theo cách thức kết nối mạng.
  - Phân loại theo kiến trúc

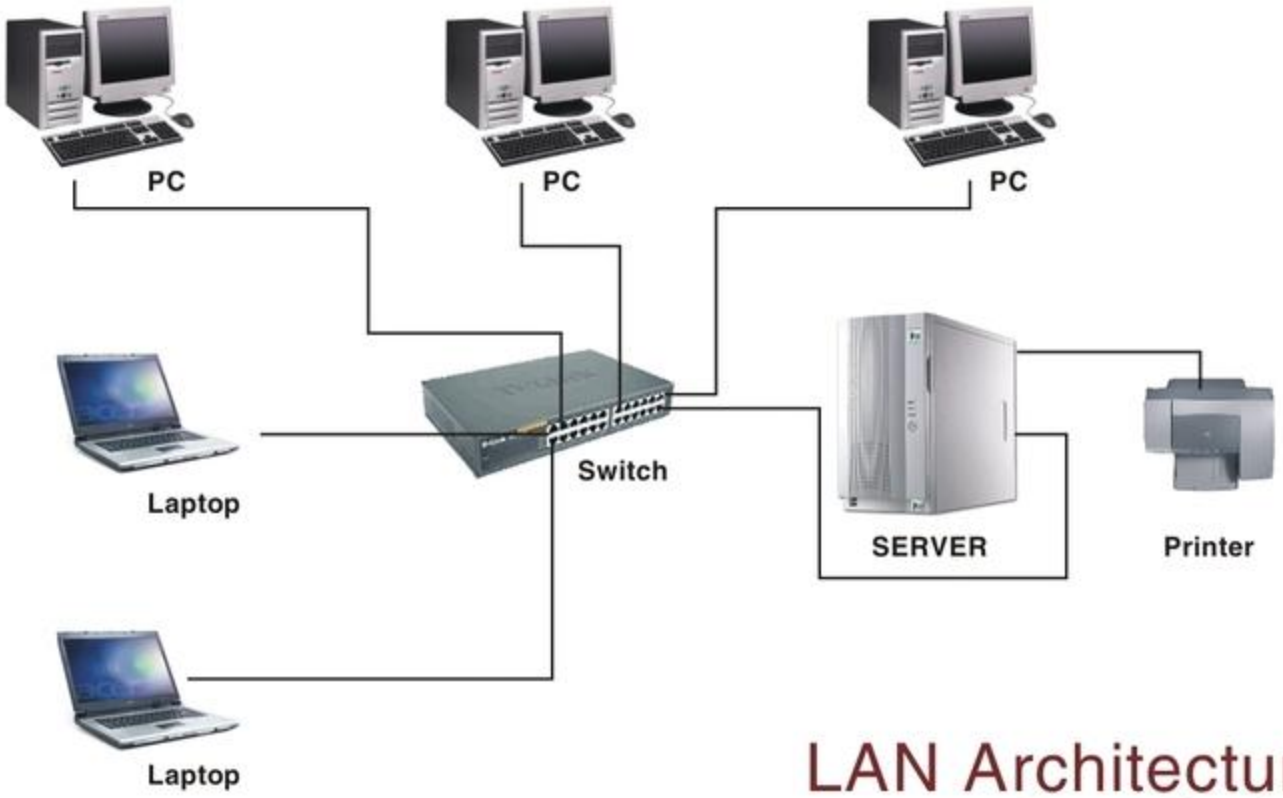
# PHÂN LOẠI MẠNG

- **Phân loại mạng theo phạm vi**
  - LAN
  - MAN
  - WAN
  - GAN


P.Hành Chính
Nhân Sự
P.Lễ Tân
P.Kế
Hoạch
Switch 24port
Modem ADSL
WAN
Server
Client
Mail Server
Wed Server
P.Server
Tầng Trệt

# Phân loại mạng theo phạm vi

- **LAN (Local Area Network): Mạng cục bộ**
  - Sử dụng trong phạm vi cơ quan, tổ chức…
  - Kết nối các máy tính trong khu vực có bán kính khoảng 100m → 10km
  - Có giới hạn về địa lý
  - Tốc độ truyền dữ liệu khá cao
  - Do một tổ chức quản lý




# LAN Architecture

***Route Co., Ltd.***

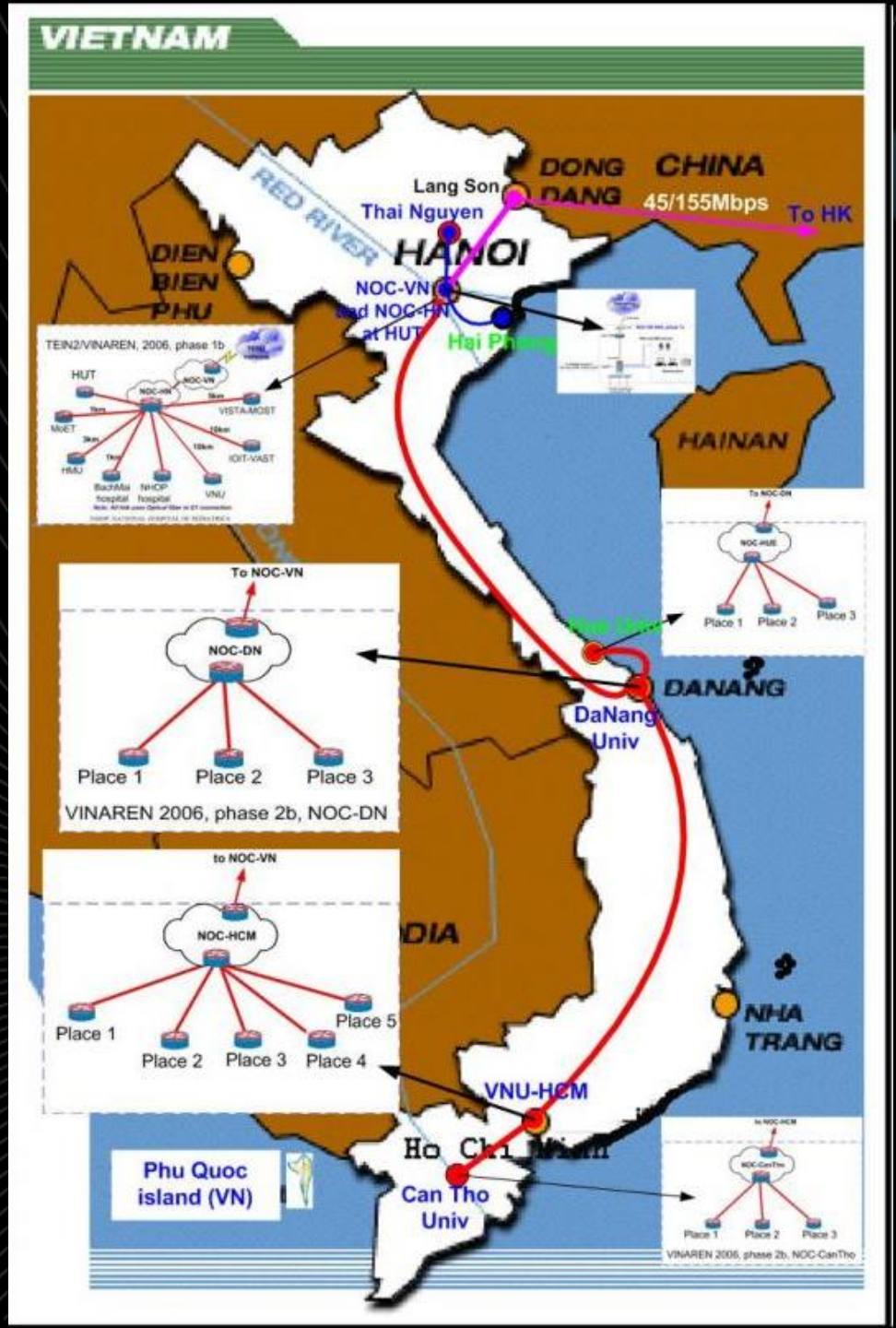
# Phân loại mạng theo phạm vi

- **MAN (Metropolitan Area Network): Mạng đô thị**
  - Có kích thước vùng địa lý lớn hơn LAN nhưng nhỏ hơn WAN
  - Thường kết nối các máy tính trong phạm vi thành phố
  - Do một tổ chức quản lý
  - Có thể hỗ trợ chung vận chuyển dữ liệu và đàm thoại hay ngay cả truyền hình
  - Thường dùng cáp đồng trục, cáp quang.

# Phân loại mạng theo phạm vi

- **WAN (Wide Area Network): Mạng diện rộng**
  - Bao trùm một khu vực, lãnh thổ, quốc gia..
  - Thường là sự kết nối nhiều LAN
  - Tốc độ truyền dữ liệu khá thấp
  - Do nhiều tổ chức quản lý
  - Các kỹ thuật thường dùng:
    - Các đường điện thoại
    - Truyền thông bằng vệ tinh.

# WAN


VIETNAM
RED RIVER
Lang Son
DONG DANG
CHINA
45/155Mbps
To HK
Thai Nguyen
HANOI
DIEN BIEN PHU
NOC-VN and NOC-HN at HUT
Hai Phong
HAINAN
TEIN2/VINAREN, 2006, phase 1b
HUT
NOC-HN
NOC-VN
VISTA-MOST
MoET
IOIT-VAST
HMU
BachMai hospital
NHOP hospital
VNU
To NOC-VN
NOC-DN
Place 1
Place 2
Place 3
VINAREN 2006, phase 2b, NOC-DN
DANANG
DaNang Univ
to NOC-VN
NOC-HCM
Place 1
Place 2
Place 3
Place 4
Place 5
NHA TRANG
VNU-HCM
Ho Chi Minh
Phu Quoc island (VN)
Can Tho Univ
VINAREN 2006, phase 2b, NOC-CanTho

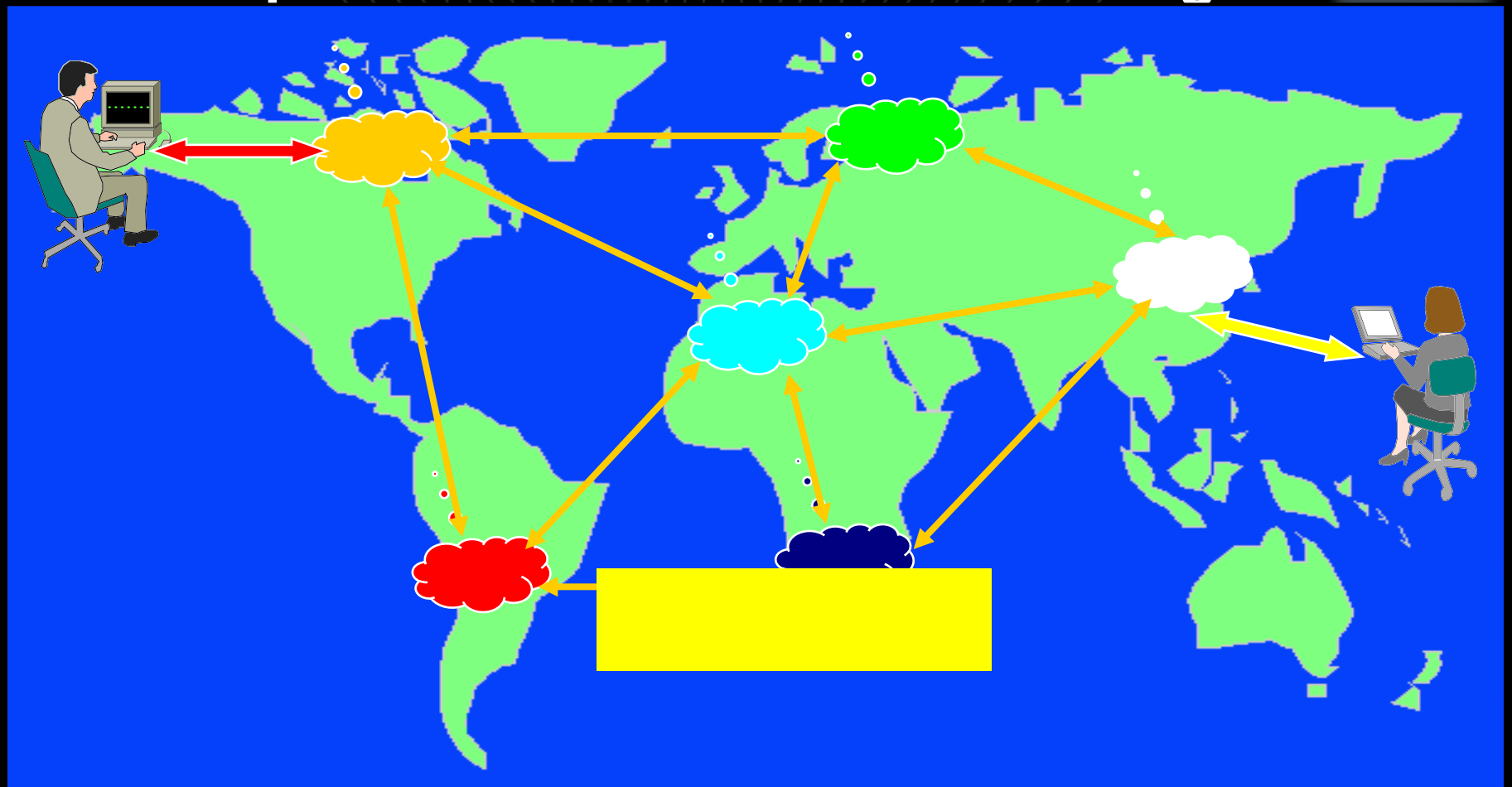
# Phân loại mạng theo phạm vi

- **GAN (Global Area Network): Mạng toàn cầu**
  - Kết nối các máy tính từ các châu lục khác nhau
  - Kết nối hai hay nhiều mạng riêng biệt
  - Mạng toàn cầu kết nối mạng của các tổ chức, cá nhân trên thế giới.
  - Thường được thực hiện thông qua mạng viễn thông, vệ tinh

| Đường kính mạng | Vị trí của các máy tính | Loại mạng |
|---|---|---|
| 1 m | Trong một mét vuông | Mạng khu vực cá nhân |
| 10 m | Trong 1 phòng | Mạng cục bộ, gọi tắt là mạng LAN (Local Area Network) |
| 100 m | Trong 1 tòa nhà | |
| 1 km | Trong một khu vực | |
| 10 km | Trong một thành phố | Mạng thành phố, gọi tắt là mạng MAN (Metropolitan Area Network) |
| 100 km | Trong một quốc gia | Mạng diện rộng, gọi tắt là mạng WAN (Wide Area Network) |
| 1000 km | Trong m ột châu lục | |
| 10000 km | Cả hành tinh | |

# **Khái niệm** Internet

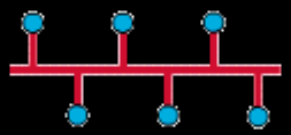
- **Internet là một hệ thống thông tin toàn cầu bao gồm các mạng máy tính được liên kết với nhau với mục đích trao đổi và chia sẻ thông tin.**



# PHÂN LOẠI MẠNG

- **Topology của mạng (Tô pô mạng): Cách kết nối các máy tính với nhau về mặt hình học.**
- **Phân loại theo cách thức kết nối mạng LAN**
  - Star
  - Bus
  - Ring

# Tô pô mạng



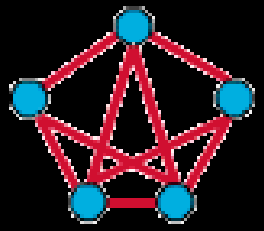
Tuyến tính

Sao mở rộng

Vòng

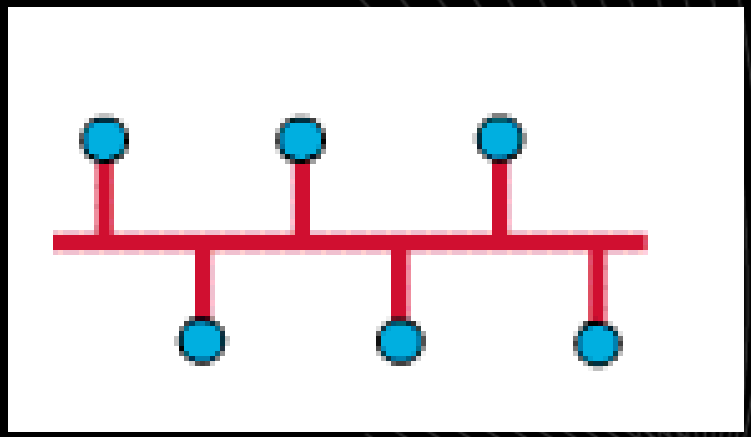
Phân cấp

Sao



Mạng lưới

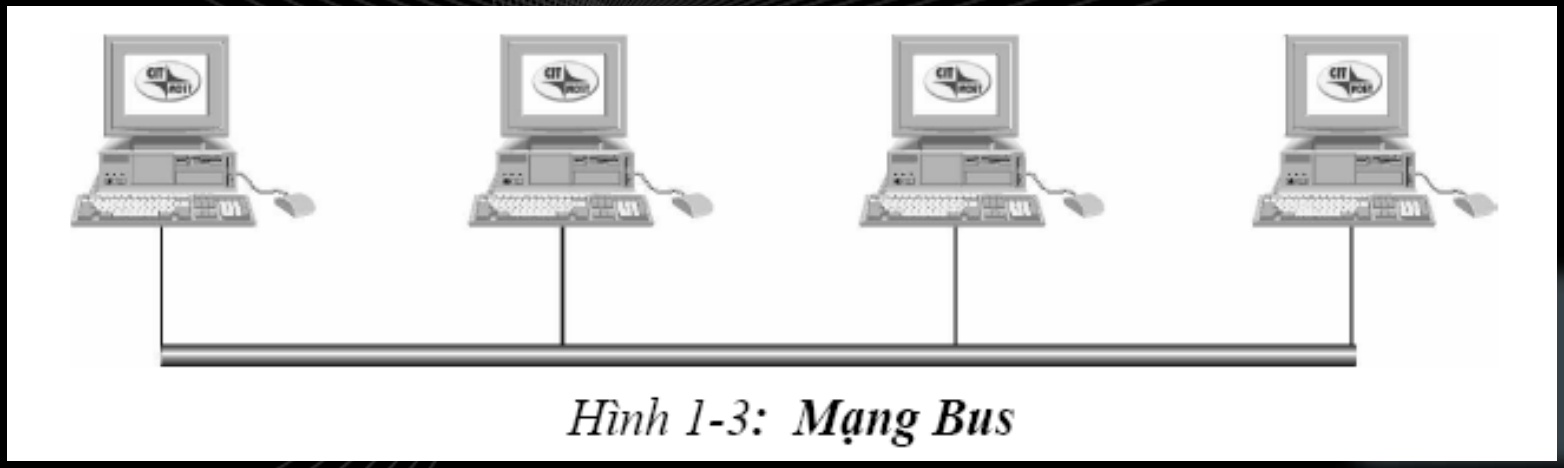
# Tô pô mạng dạng tuyến tính (BUS)



- Một hành lang chính (backbone)
- Tất cả các nút cùng nối vào hành lang chính
- Phía cuối hai đầu dây cáp được chặn bởi đầu kết cuối

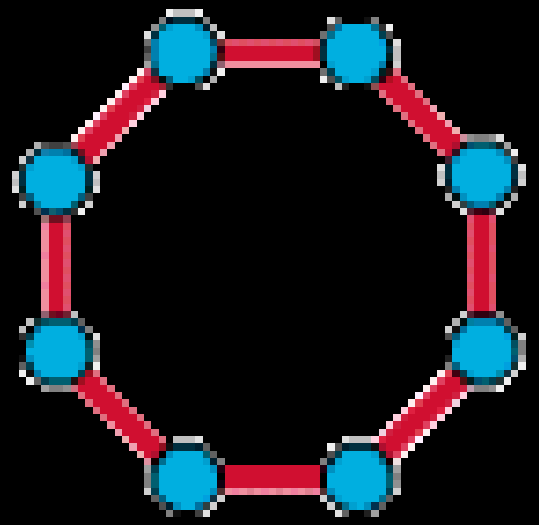
# Tô pô mạng dạng tuyến tính (BUS)

- Sai hỏng của một nút không ảnh hưởng mạng
- Mở rộng hay thu hẹp dễ dàng
- Dùng dây cáp ít, lắp đặt dễ dàng
- Dễ ùn tắc, đụng độ thông tin, số nút hạn chế
- Khó phát hiện điểm hỏng



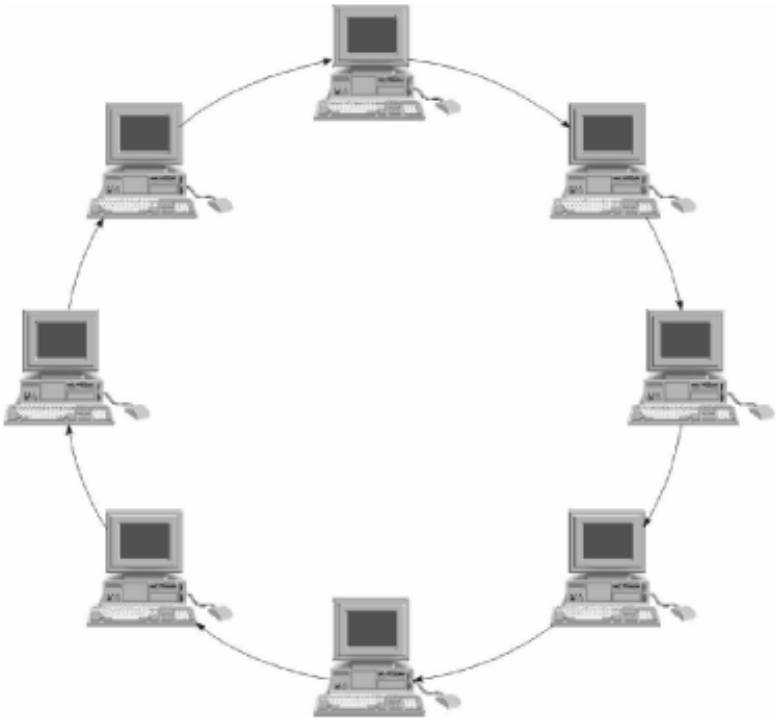
*Hình 1-3: Mạng Bus*

# Tô pô mạng: dạng vòng (RING)



- Không có hành lang chính
- Mỗi nút được kết nối trực tiếp với nút bên cạnh tạo thành vòng kín

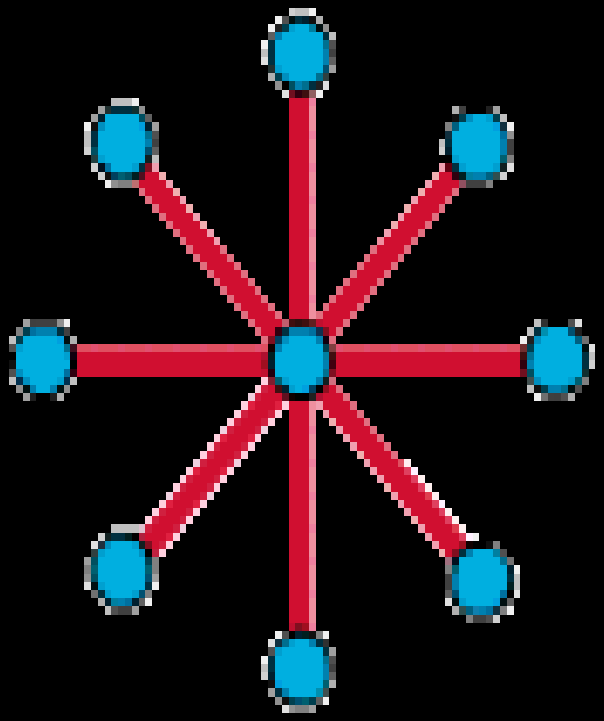
# Tô pô mạng: dạng vòng (RING)



*Hình 1-6: **Mạng vòng RING***

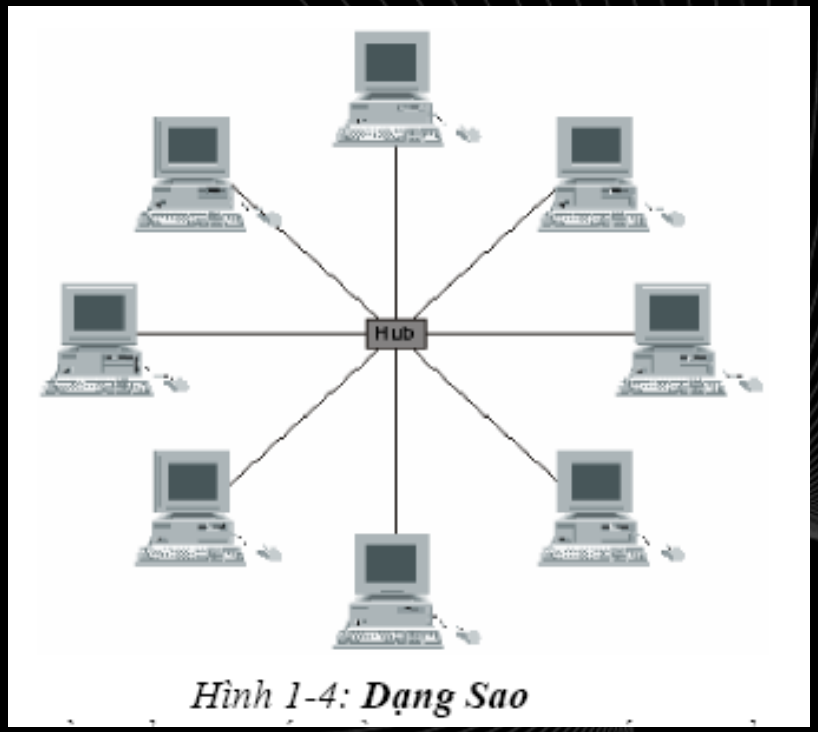
- Giảm tối đa khả năng đụng độ thông tin
- Khoảng cách mỗi nút có thể tăng lên
- Tiết kiệm dây
- Một nút hỏng sẽ ảnh hưởng đến toàn mạng

# Tô pô mạng: dạng sao (STAR)



- Tất cả các nút được kết nối vào một điểm trung tâm
- Thiết bị trung tâm có thể là bộ chuyển mạch (switch), thiết bị phân kênh (hub)

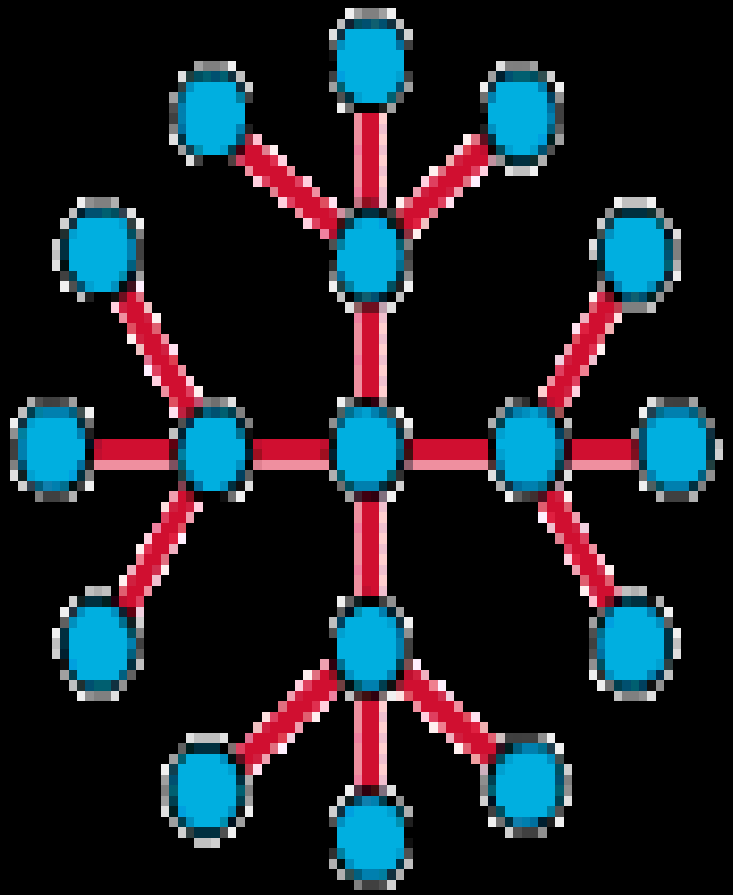
# Tô pô mạng: dạng sao (STAR)



Hình 1-4: Dạng Sao

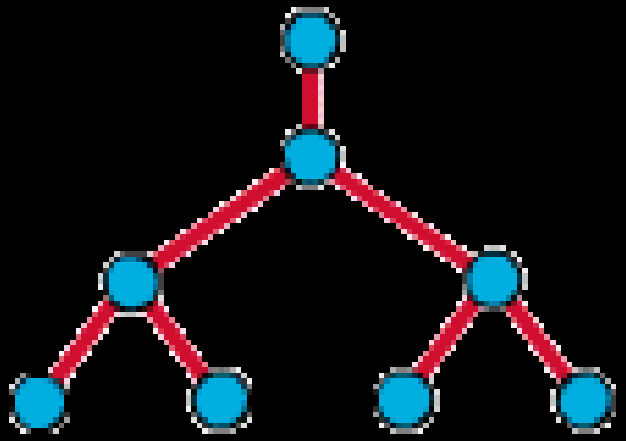
- Một nút hỏng không ảnh hưởng đến mạng
- Tận dụng tối đa tốc độ
- Kiểm soát lỗi, cấu hình lại dễ dàng
- Khả năng hoạt động và mở rộng phụ thuộc thiết bị trung tâm
- Chi phí lắp đặt cao

# Tô pô mạng: dạng sao mở rộng



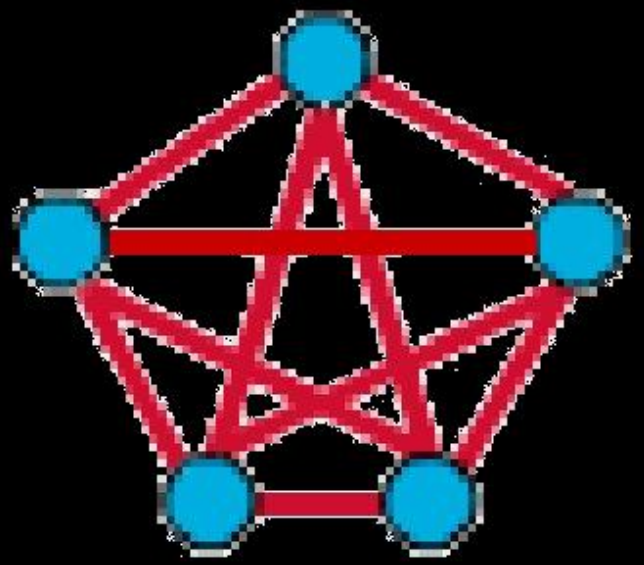
- Kết nối các hình sao
- Thiết bị trung tâm là một bộ chuyển mạch hay thiết bị phân kênh
- Tăng kích thước và chiều dài mạng

# Tô pô mạng: dạng phân cấp



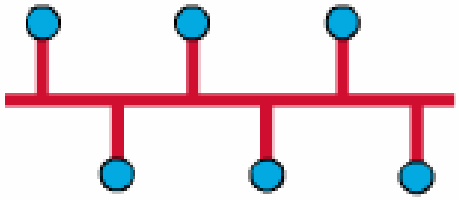
- Tương tự dạng sao mở rộng nhưng dùng một máy tính để điều khiển lưu lượng mạng.

# Tô pô mạng: dạng mắt lưới

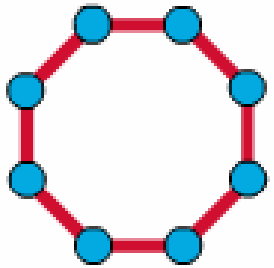


- Mỗi nút có một đường kết nối với tất cả các nút khác trong mạng
- Đảm bảo hoạt động liên tục

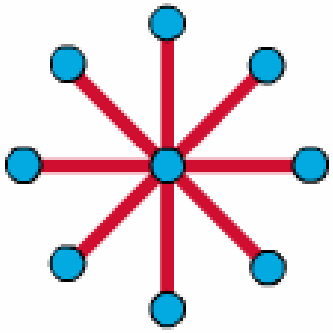
# Tô pô mạng



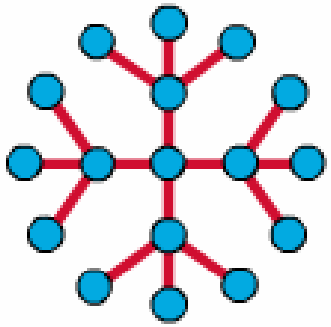
Bus Topology



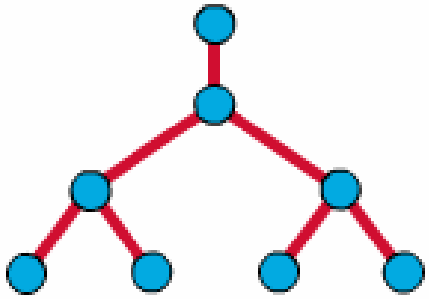
Ring Topology



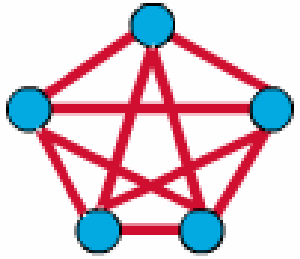
Star Topology



Extended Star Topology



Hierarchical Topology



Mesh Topology

# Các mô hình ứng dụng mạng

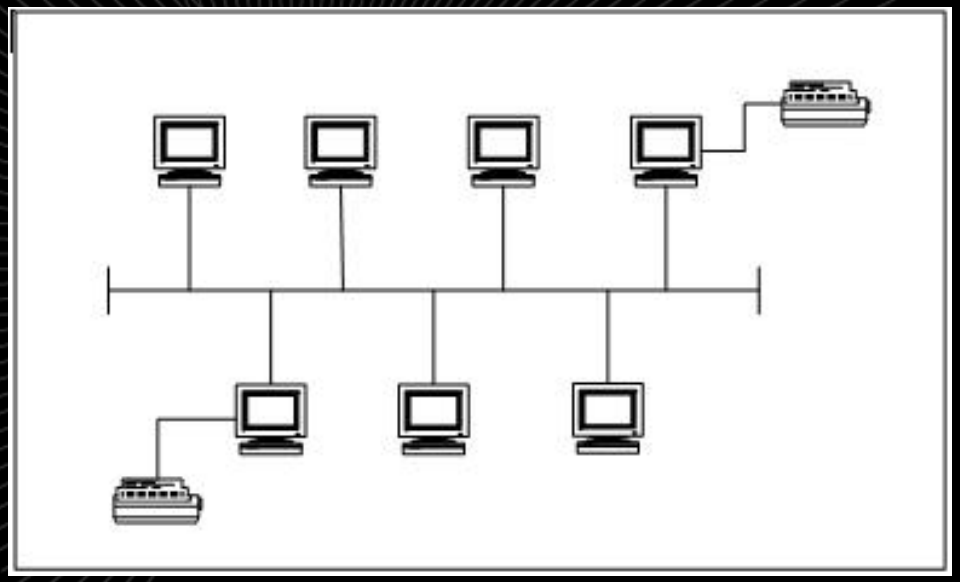
- Mạng ngang hàng (Peer-to-Peer)
- Mạng khách chủ (Client – Server)

- Khái niệm client
- Khái niệm server

# LAN – Mô hình ngang hàng

- **Mô hình mạng ngang hàng**

  **(Peer-to-peer network): Các máy tính trong mô hình mạng này có vai trò ngang hàng với nhau (vừa là server, vừa là client) và liên lạc trực tiếp với nhau không cần thông qua server.**



# LAN – Mô hình ngang hàng

- **Ưu điểm:**
  - đơn giản, dễ cài đặt, tổ chức và quản trị;
  - chi phí thiết bị thấp
- **Khuyết điểm:**
  - dữ liệu phân tán
  - khả năng bảo mật thấp rất dễ bị xâm nhập
  - các tài nguyên không được sắp xếp nên rất khó định vị và tìm kiếm.

# LAN – Mô hình Khách/Chủ

- **Mô hình mạng khách chủ (Client/Server network):**
  - có một hệ thống máy tính cung cấp các tài nguyên và dịch vụ cho cả hệ thống mạng sử dụng gọi là các máy chủ (Server).
  - Một hệ thống máy tính sử dụng các tài nguyên và dịch vụ này được gọi là máy khách (Client).
  - Các Server thường có cấu hình mạnh (tốc độ xử lý nhanh, kích thước lưu trữ lớn) hoặc là các máy chuyên dụng.

# Mạng khách – chủ

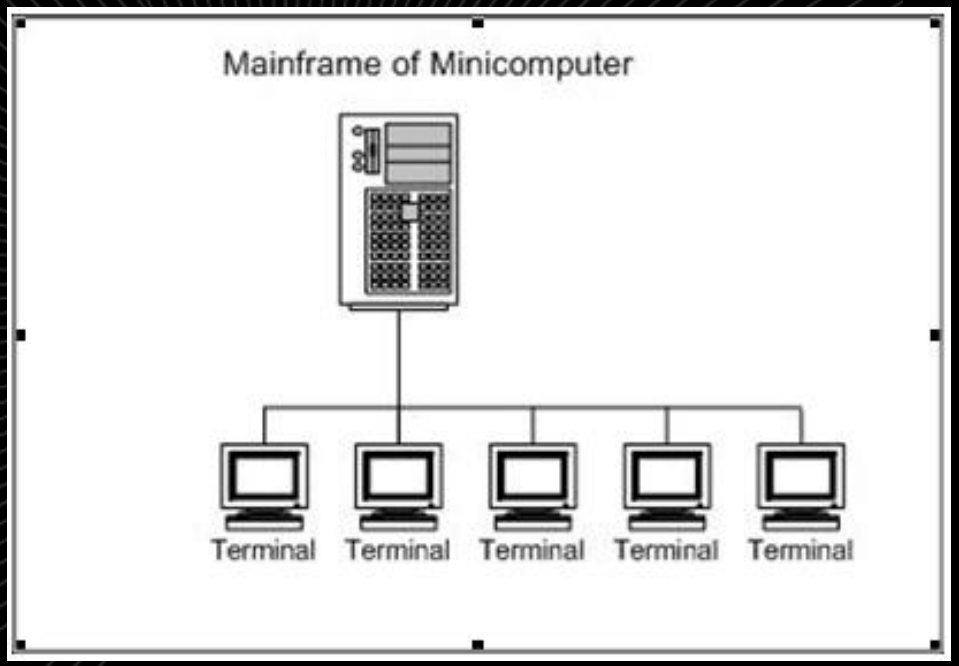
- **Ưu điểm:**
  - Do các dữ liệu được lưu trữ tập trung nên dễ bảo mật, sao lưu (backup) và đồng bộ với nhau.
  - Tài nguyên và dịch vụ được tập trung nên dễ chia sẻ và quản lý và có thể phục vụ cho nhiều người dùng.
- **Khuyết điểm:**
  - Các Server chuyên dụng rất đắt tiền
  - Phải có nhà quản trị cho hệ thống.

# CÁC MÔ HÌNH XỬ LÝ MẠNG

- Mô hình xử lý mạng tập trung.
- Mô hình xử lý mạng phân phối.
- Mô hình xử lý mạng cộng tác.

# CÁC MÔ HÌNH XỬ LÝ MẠNG

- **Mô hình xử lý mạng tập trung.**
  - Toàn bộ các tiến trình xử lý diễn ra tại máy tính trung tâm.
  - Các máy trạm đầu cuối không lưu trữ và xử lý dữ liệu.

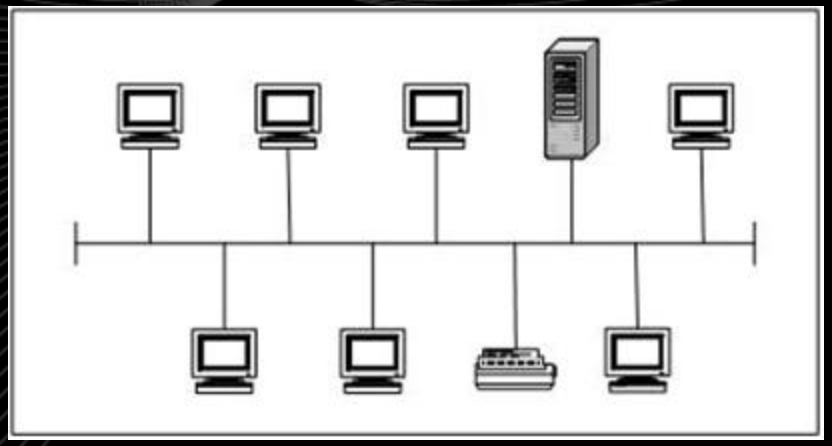


# CÁC MÔ HÌNH XỬ LÝ MẠNG

- **Mô hình xử lý mạng tập trung.**
- **Ưu điểm:**
  - Dữ  liệu được bảo mật an toàn, dễ backup và diệt virus.
  - Chi phí các thiết bị thấp.
- **Khuyết điểm:**
  - Khó đáp ứng được các yêu cầu của nhiều ứng dụng khác nhau
  - Tốc độ truy xuất chậm.

# CÁC MÔ HÌNH XỬ LÝ MẠNG

- **Mô hình xử lý mạng phân phối**
  - Các máy tính có khả năng hoạt động độc lập, các công việc được tách nhỏ và giao cho nhiều máy tính khác nhau thay vì tập trung xử lý trên máy trung tâm.
  - Các máy tính được nối mạng với nhau nên chúng có thể trao đổi dữ liệu và dịch vụ.



# CÁC MÔ HÌNH XỬ LÝ MẠNG

- **Mô hình xử lý mạng phân phối**
  - **Ưu điểm:** truy xuất nhanh, phần lớn không giới hạn các ứng dụng.
  - **Khuyết điểm:** dữ liệu lưu trữ rời rạc khó đồng bộ, backup và rất dễ nhiễm virus.

# CÁC MÔ HÌNH XỬ LÝ MẠNG

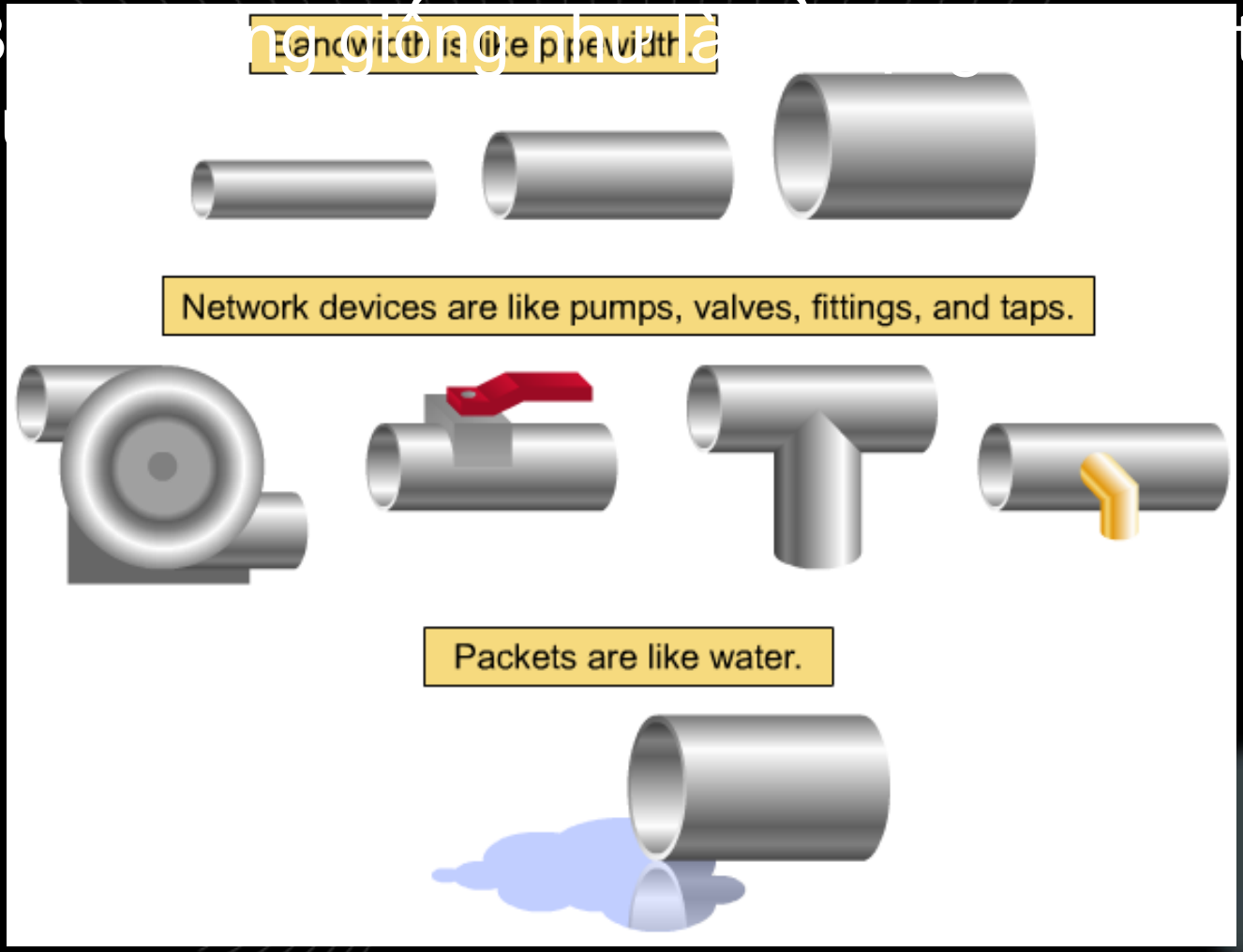
- **Mô hình xử lý mạng cộng tác**
  - Bao gồm nhiều máy tính có thể hợp tác để thực hiện một công việc. Một máy tính có thể mượn năng lực xử lý bằng cách chạy các chương trình trên các máy nằm trong mạng.
  - Ưu điểm: rất nhanh và mạnh, có thể dùng để chạy các ứng dụng có các phép toán lớn
  - Khuyết điểm: các dữ liệu được lưu trữ trên các vị trí khác nhau nên rất khó đồng bộ và backup, khả năng nhiễm virus rất cao.

# Băng thông

- Là lượng thông tin có thể chảy qua một kết nối mạng trong một khoảng thời gian cho trước.

# Dạng tương tự băng thông

- Ống nước
  - B ng giống như là t ống n



# Đo lường băng thông

- **Đơn vị cơ bản của băng thông là bit/giây (bps)**
  - Ngàn bit/giây: Kbps
  - Triệu bit/giây: Mbps
  - Tỉ bit/giây: Gbps
  - Ngàn tỉ bit/giây: Tbps

| Unit of Bandwidth | Abbrev. | Equivalence |
|---|---|---|
| Bits per second | bps | 1 bps = fundamental unit of bandwidth |
| Kilobits per second | kbps | 1 kbps = 1,000 bps = $10^3$ bps |
| Megabits per second | Mbps | 1 Mbps = 1,000,000 bps = $10^6$ bps |
| Gigabits per second | Gbps | 1 Gbps = 1,000,000,000 bps = $10^9$ bps |

# Thông lượng ≤ Băng thông

- **Thông lượng là băng thông thực tế đo được vào một thời điểm cụ thể.**
- **Các yếu tố ảnh hưởng đến thông lượng:**
  - Thiết bị mạng
  - Kiểu dữ liệu truyền
  - Cấu trúc liên kết mạng (topo mạng)
  - Số lượng người dùng
  - Máy tính của người dùng
  - Máy tính phục vụ
  - Các điều kiện khác như năng lượng…

# Sự quan trọng của băng thông

- Hữu hạn
- Tiết kiệm tiền bạc
- Tiêu chuẩn để tính chất lượng mạng
- Tăng liên tục

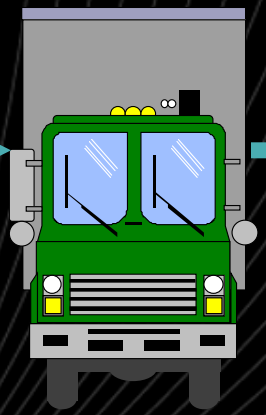
# CÁC MÔ HÌNH NETWORKING

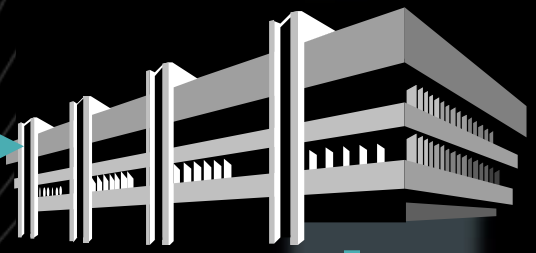
- Mô hình OSI
- Mô hình TCP/IP
- Giao thức: là một tập các tiêu chuẩn để trao đổi thông tin giữa hai hệ thống máy tính

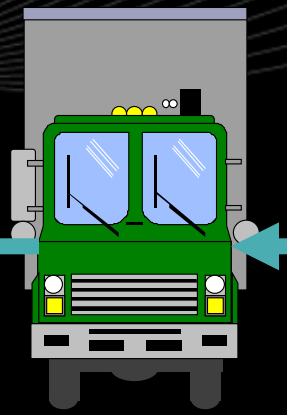
# Mailing system

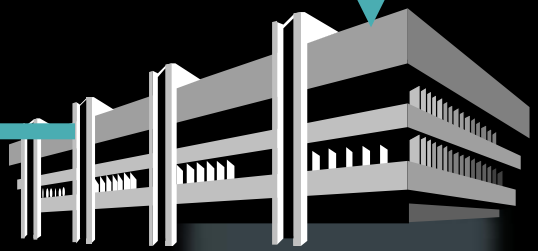
Letter

Addressed Envelope









Letter

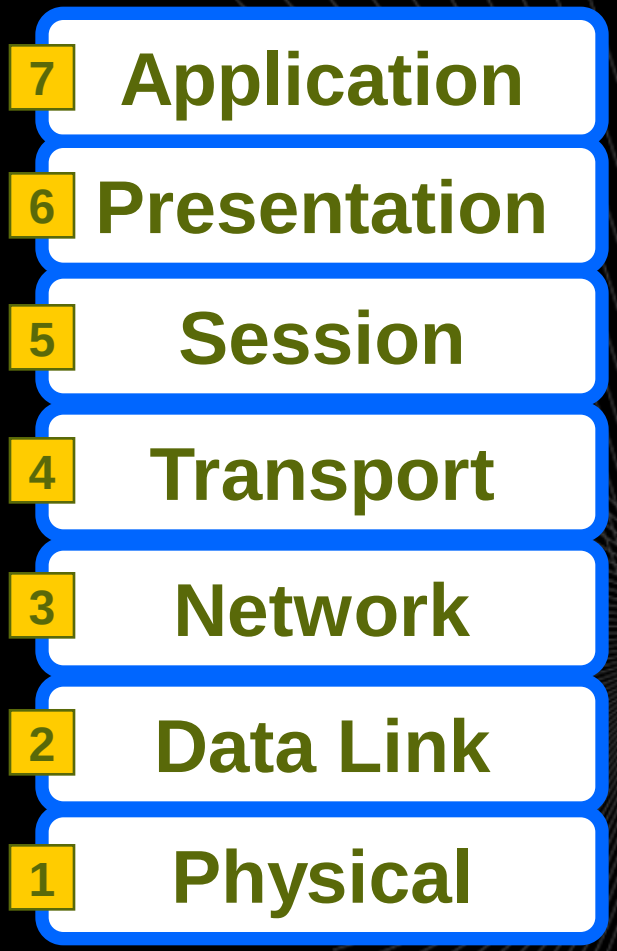
Addressed Envelope

# OSI là gì? (Open Systems Interconnection model)

- Là mô hình mạng chuẩn hóa do ISO (International Standard Organization) đề nghị
- Gồm có 7 lớp với các chức năng khác nhau
- Định ra các tiêu chuẩn thống nhất cho các nhà sản xuất, cung cấp sản phẩm, dịch vụ mạng.

# Giao tiếp qua mạng

# Mô hình OSI 7 lớp




Tầng ứng dụng: Cung cấp các ứng dụng mạng: email, web, chat, truyền file...

Tầng trình bày: Trình bày dữ liệu

Tầng giao dịch: Thiết lập các giao dịch giữa 2 máy tính

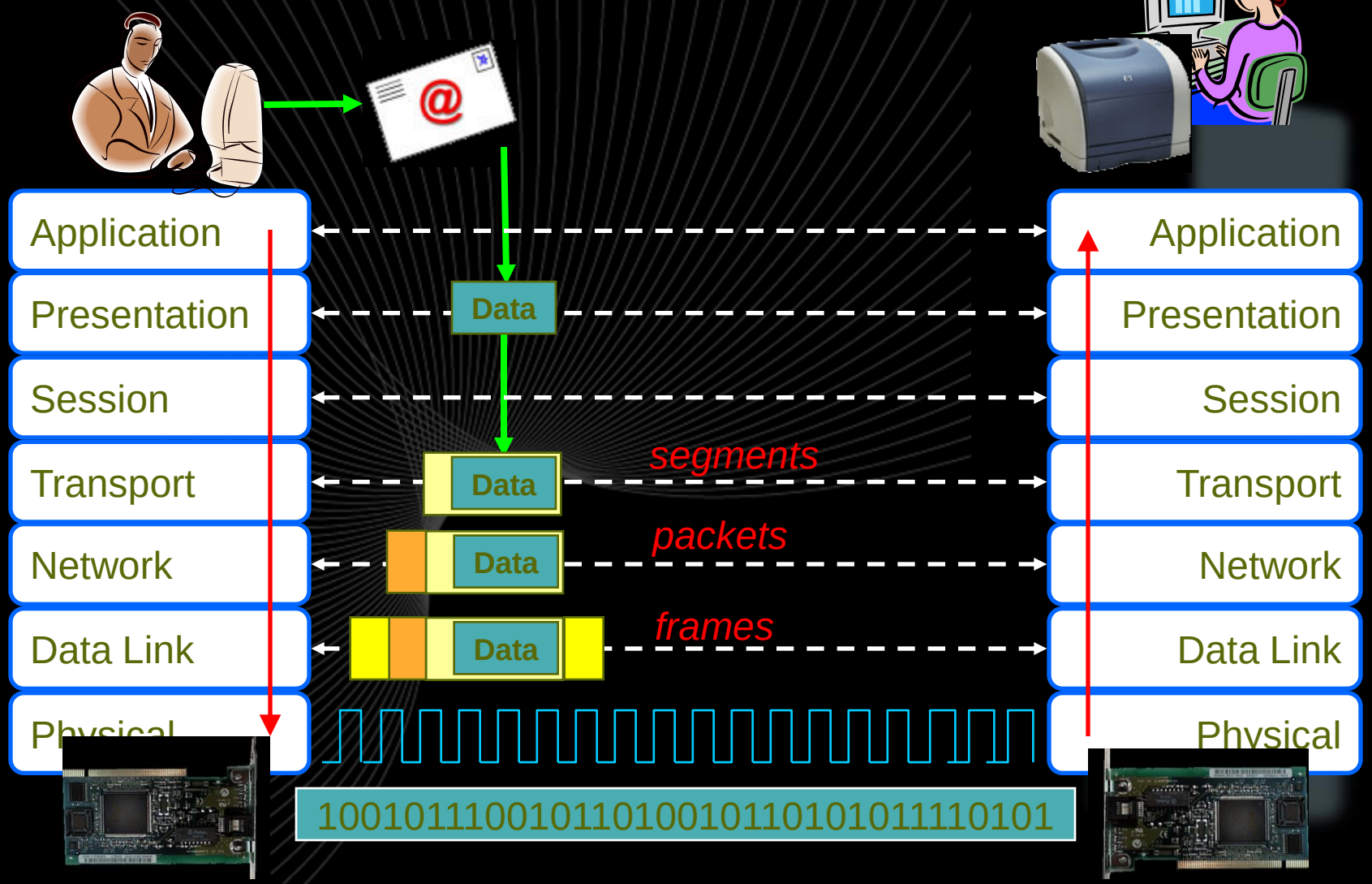
Tầng giao vận: Bảo đảm truyền nhận đúng dữ liệu

Tầng mạng: Quản lý địa chỉ, tìm đường, truyền nhận các packet (gói dữ liệu). (router, nic)

Tầng liên kết dữ liệu: Điều khiển liên kết, truy xuất đường truyền (bridge, switch)

Tầng vật lý: Kết nối vật lý, truyền các bit dữ liệu (repeater, hub)

# Giao tiếp qua mô hình OSI 7 lớp



# TCP/IP là gì?

- Mô hình kết nối mạng do U.S. DoD (Department of Defense) đề nghị
- Xuất hiện 1971 trong mạng ARPANET
- Gồm có **4 lớp**
- Là chuẩn giao tiếp của **Internet**

# Mô hình TCP/IP

| | |
|---|---|
| Application | Tầng ứng dụng |
| Transport | Tầng giao vận |
| Internet | Tầng Internet |
| Network Access | Tầng truy cập mạng |

# Mô hình TCP/IP (tt)

- **Tầng ứng dụng:**
  - Hỗ trợ cho các ứng dụng của người dùng
  - Http, smtp,…
- **Tầng giao vận:**
  - Đảm bảo truyền dữ liệu đáng tin cậy
  - Nhận dữ liệu theo đúng thứ tự
- **Tầng Internet:**
  - Các hệ thống kết nối với các mạng khác nhau
  - Được cài đặt ở end system và router
- **Tầng truy cập mạng:**
  - Trao đổi dữ liệu giữa end system và mạng
  - Kiểm soát địa chỉ đích
  - Yêu cầu dịch vụ…

# Các khái niệm cơ bản khác

- *Giao thức* **(protocol): cách thức giao tiếp với nhau**
- **Giao thức:**

  **i nhau.**

  - Tương tự với ngôn ngữ, ám hiệu,...
  - Ví dụ các giao thức thuộc TCP/IP:
    - SMTP (Simple Mail Transfer Protocol)
    - POP3 (Post Office Protocol v.3)
    - HTTP (HyperText Transfer Protocol)
    - FTP (File Transfer Protocol)
    - IP (Internetwork Protocol)

# Ví dụ về giao thức

Hi

TCP connection req

Hi

TCP connection response

Mấy giờ rồi?

GET http://www.yahoo.com

time

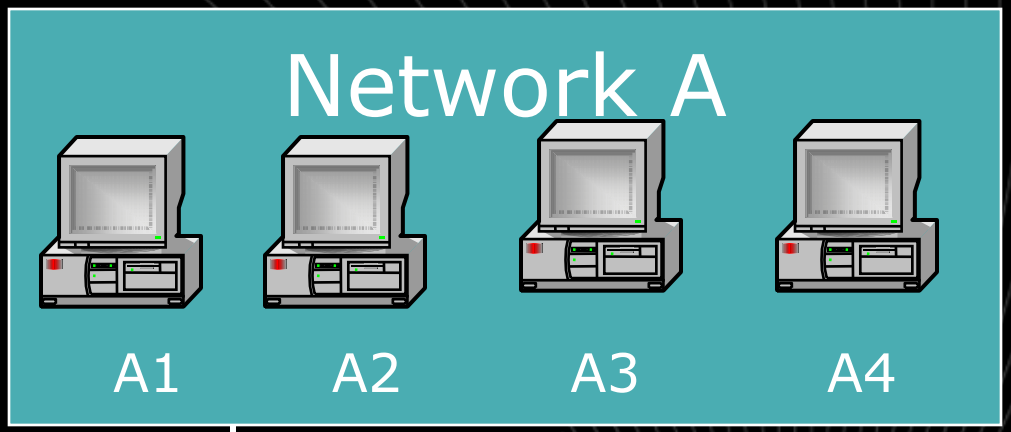
2:00

<file>

# ĐỊA CHỈ

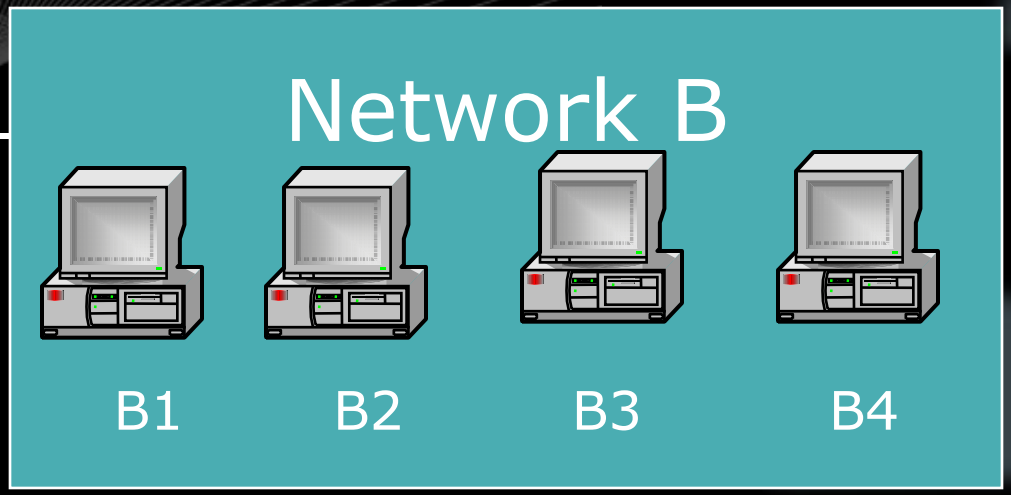
- **Bất kỳ thiết bị nào trên Internet truyền thông với các thiết bị Internet khác đều phải có một định danh duy nhất**
- **Mỗi máy tính có 1 địa chỉ duy nhất → giúp nhận diện và định vị lẫn nhau.**
- **Có 2 loại địa chỉ:**
  - Địa chỉ IP (IP address)
  - Địa chỉ vật lý (Physical address/MAC)

# ĐỊA CHỈ IP




A1, A2, …, B1, B2,… biểu diễn các địa chỉ

A, B: phần mạng
1, 2,… : địa chỉ của máy tính trong mạng (host)



# ĐỊA CHỈ IP

- **Gồm 2 thành phần:**
  - Địa chỉ mạng (network)
  - Địa chỉ của máy tính trên mạng (host)
- **Mỗi máy tính trên mạng gọi là host**

- **Mỗi máy tính kết nối vào mạng có 1 địa chỉ IP duy nhất**

# ĐỊA CHỈ IP

- Địa chỉ IP là một dãy số 32 bit (4 byte)
- Biểu diễn theo từng byte (gọi là các octet) cách nhau bởi dấu chấm (.)

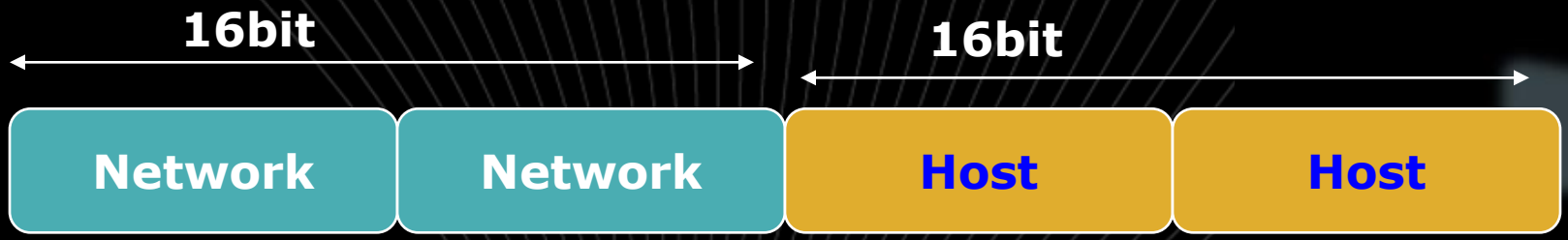
| Byte 1 | . | Byte 2 | . | Byte 3 | . | Byte 4 |
|---|---|---|---|---|---|---|

- Mỗi octet nằm trong dải từ 0 đến 255
- Ví dụ:
  - 192.168.1.1
  - 203.162.7.43
  - ? 555.4.3.2 có là một địa chỉ IP

# ĐỊA CHỈ IP

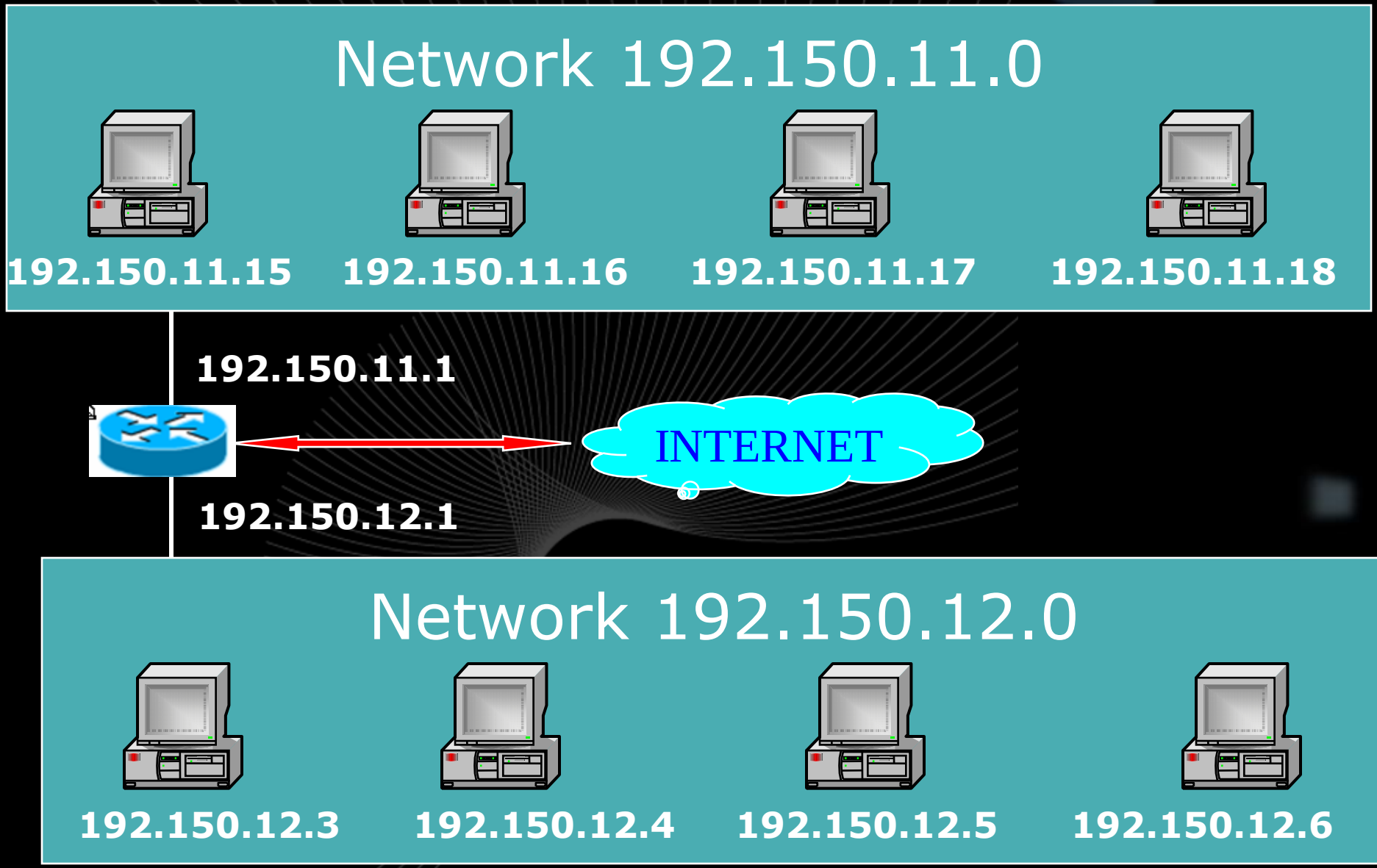
- **Các địa chỉ IP được chia thành các lớp (class) để phân ra các mạng lớn, trung bình và nhỏ.**
  - Địa chỉ lớp A: các mạng lớn
  - Địa chỉ lớp B: các mạng trung bình
  - Địa chỉ lớp C: các mạng nhỏ
  - Lớp D, E: dành cho các mục đích khác
- **Địa chỉ lớp A**

## Địa chỉ lớp B




## Địa chỉ lớp C

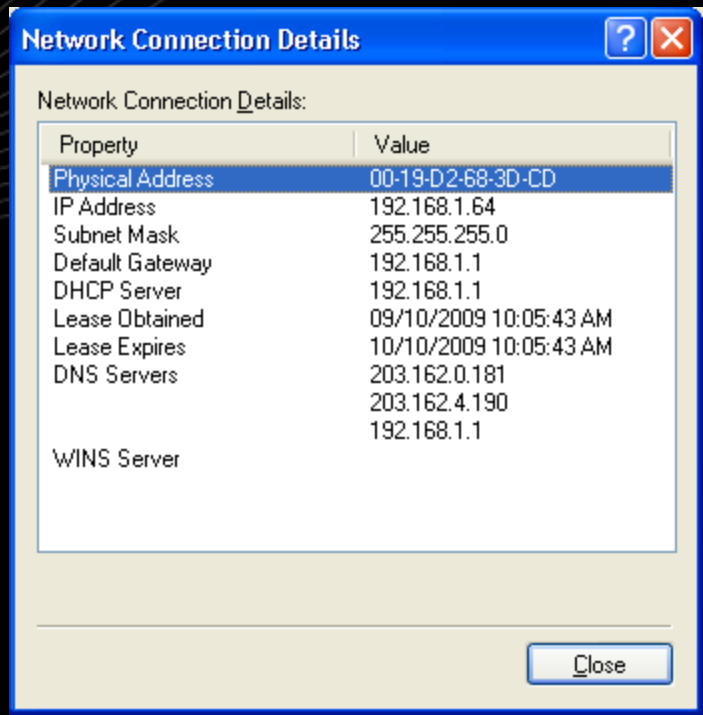
# ĐỊA CHỈ IP


Network 192.150.11.0
192.150.11.15
192.150.11.16
192.150.11.17
192.150.11.18
192.150.11.1
INTERNET
192.150.12.1
Network 192.150.12.0
192.150.12.3
192.150.12.4
192.150.12.5
192.150.12.6

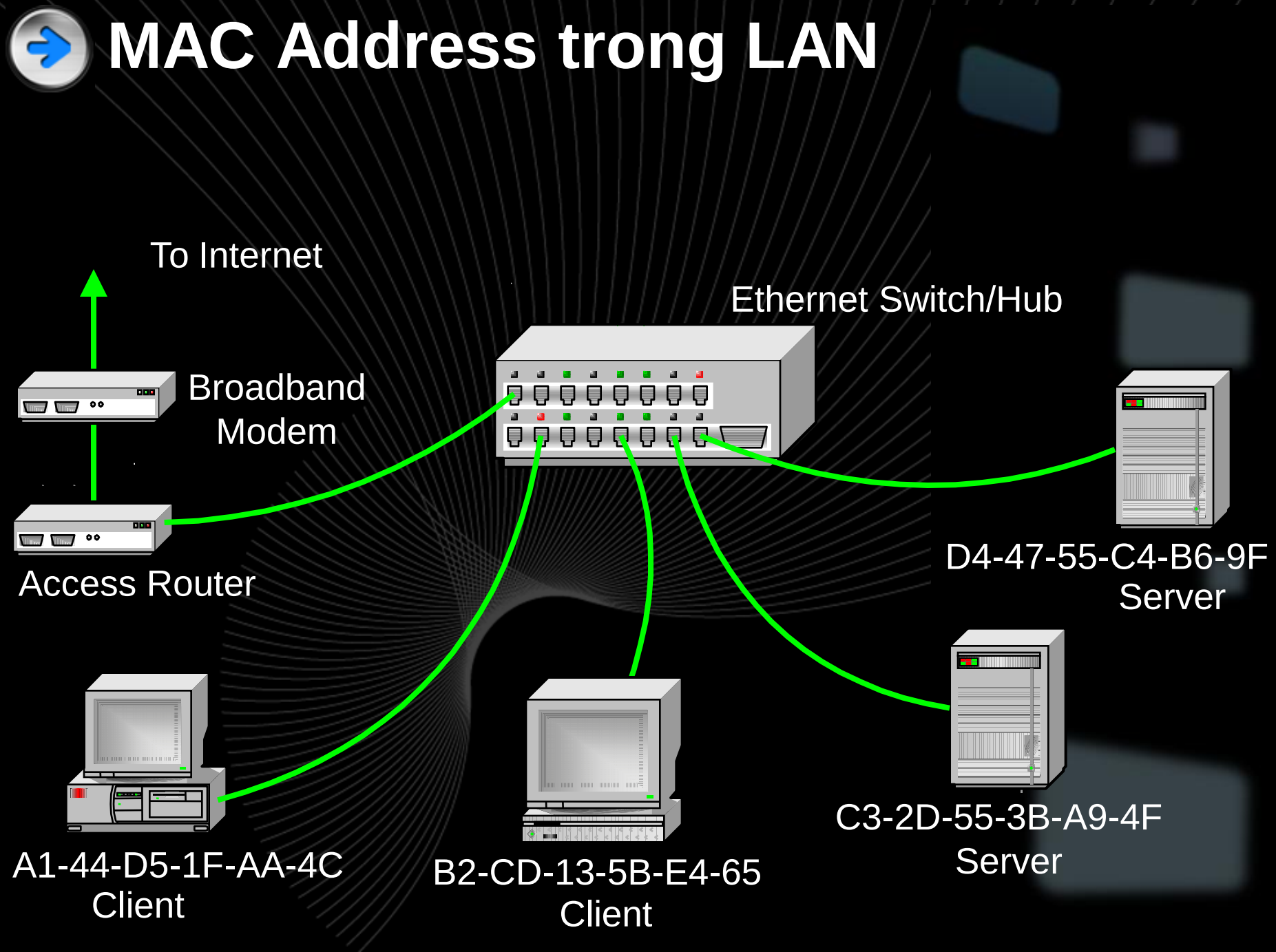
# ĐỊA CHỈ VẬT LÝ (MAC)

- Là địa chỉ duy nhất
- Các địa chỉ vật lý được gán bởi nhà sản xuất card giao tiếp mạng NIC
- Gồm 6 byte, viết trong hệ thập lục phân (16)
- Ví dụ: 00-0B-CD-33-26-9D

- Cách xem địa chỉ IP, MAC?



# MAC Address trong LAN



# Các lớp địa chỉ IP

- ***Class A*** : **0.0.0.0 ÷ 127.255.255.255**
- ***Class B*** : **128.0.0.0 ÷ 191.255.255.255**
- ***Class C*** : **192.0.0.0 ÷ 223.255.255.255**
- ***Class D*** : **224.0.0.0 ÷ 239.255.255.255**
- ***Class E*** : **240.0.0.0 ÷ 255.255.255.255**
- **Các vùng *địa chỉ dành riêng* cho LAN**
  - 10.0.0.0 ÷ 10.255.255.255
  - 172.16.0.0 ÷ 172.31.255.255
  - 192.168.0.0 ÷ 192.168.255.255

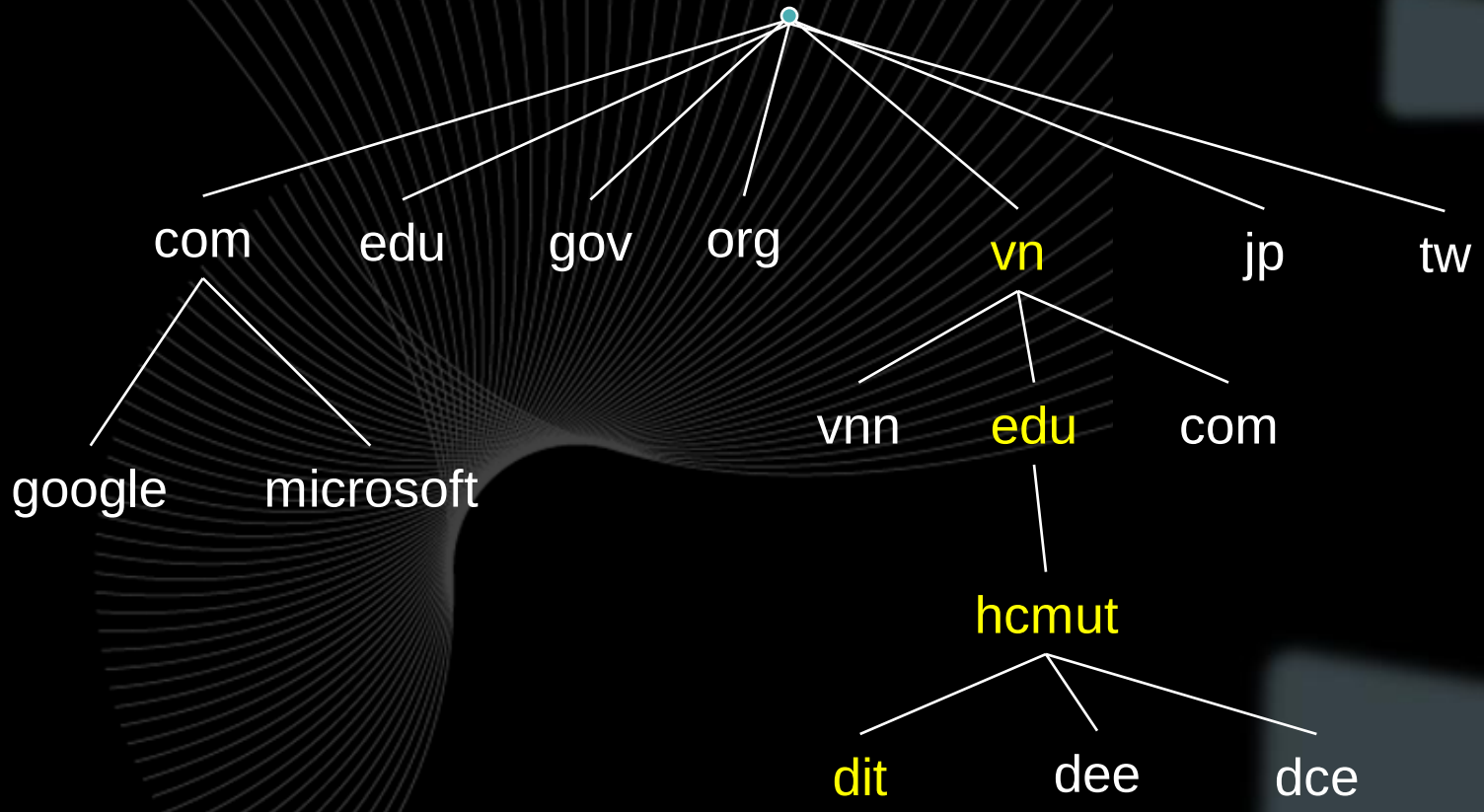
# Các khái niệm cơ bản khác (t.t)

- **Từ địa chỉ IP đến *Domain Name***
  - Là dạng tên gợi nhớ do tổ chức InterNIC và các phân nhánh cấp. Ví dụ

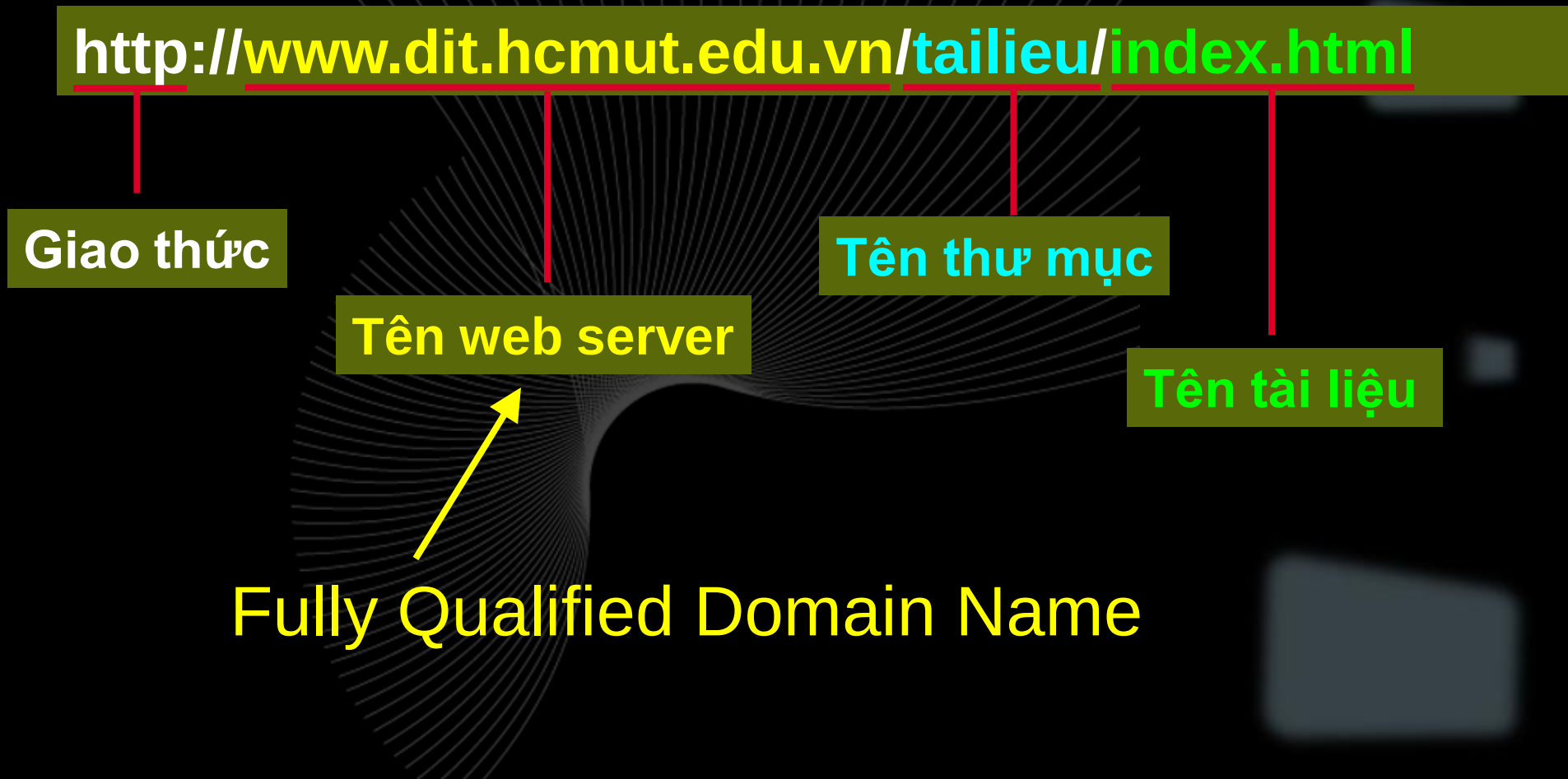
    nhacso.net

    cit.udn.vn
- **Cây phân cấp tên miền DNS (Domain Name System)**
  - Quốc gia: au, vn, de, it, fr, ch
  - Tổ chức: com, edu, mil, org, gov

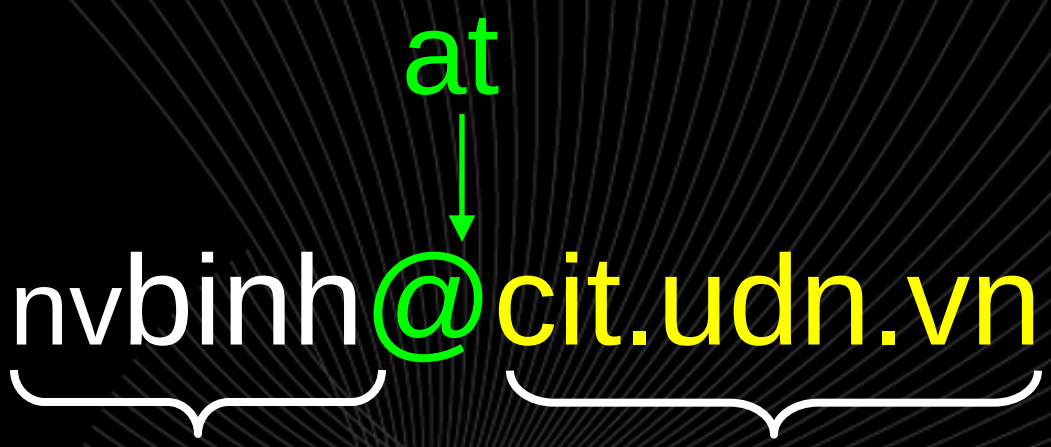
# Domain Name System



# Uniform Resource Locator (URL)

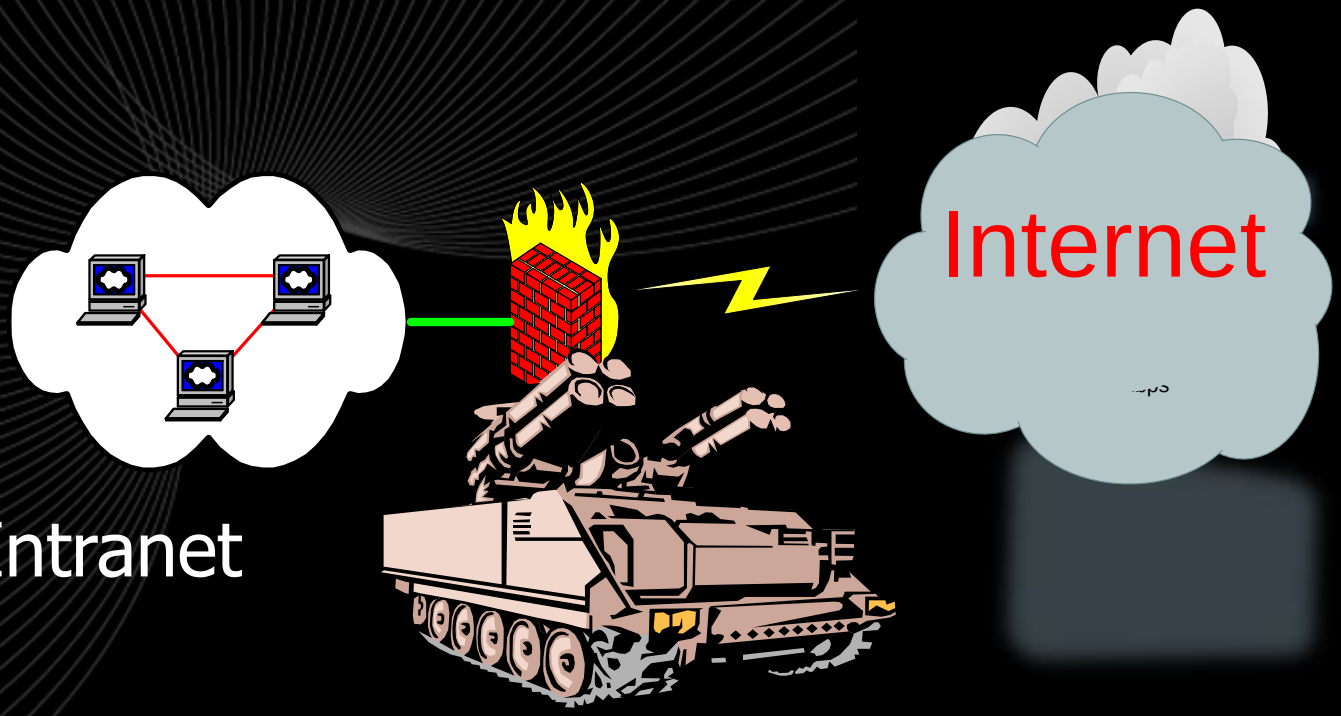


# Internet Mail Address



# Các khái niệm cơ bản khác (t.t)

- *Firewall*
  - bức tường lửa, ngăn cách giữa Intranet và Internet, có nhiệm vụ bảo vệ mạng Intranet.



LOGO

# Các phương tiện truyền dẫn

# Nội Dung

- **Khái niệm phương tiện truyền dẫn**
- **Các đặc tính của phương tiện truyền dẫn**
- **Các loại cable:**
  - Cáp đồng trục (Coaxial)
  - Cáp xoắn đôi (Twisted-Pair)
  - Cáp quang (Fiber-optic)
- **Các kỹ thuật bấm cáp mạng**

# Phương Tiện Truyền Dẫn

- **Khái niệm:**
  - Trên 1 máy tính, các dữ liệu được truyền trên 1 môi trường truyền dẫn (Transmission Media), nó là phương tiện vật lý cho phép truyền tải tín hiệu giữa các thiết bị
- **Có 2 loại phương tiện truyền dẫn:**
  - Hữu tuyến (Bounded Media)
  - Vô tuyến  (Boundless Media)

# Phương Tiện Truyền Dẫn

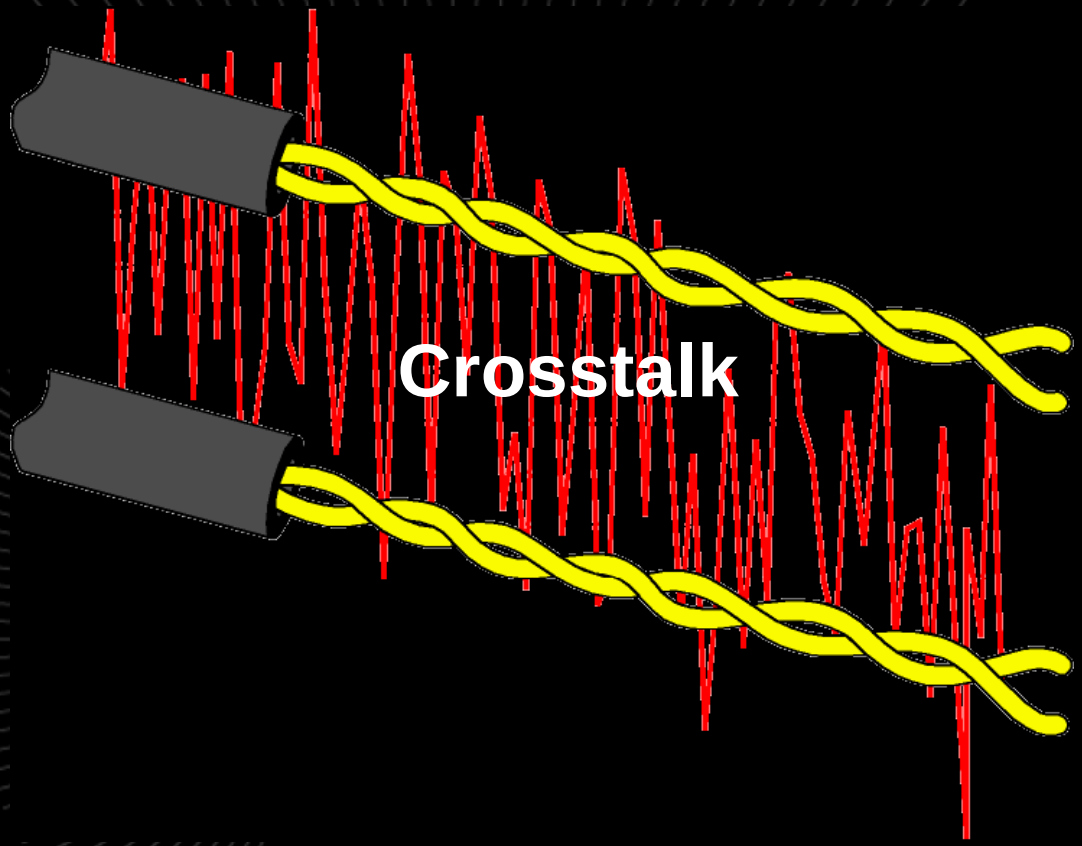
- **Các đặc tính của phương tiện truyền dẫn:**
  - Chi phí
  - Yêu cầu cài đặt (đối với từng loại cable)
  - Băng thông (bandwidth)
  - Nhiễu điện từ
  - Độ suy dần (Attenuation)
  - Nhiễu xuyên kênh (Crosstalk)

# Phương Tiện Truyền Dẫn

- Vd Độ suy dần (Attenuation):

# Phương Tiện Truyền Dẫn

- Vd nhiễu xuyên kênh:



# Các đặc tả cáp

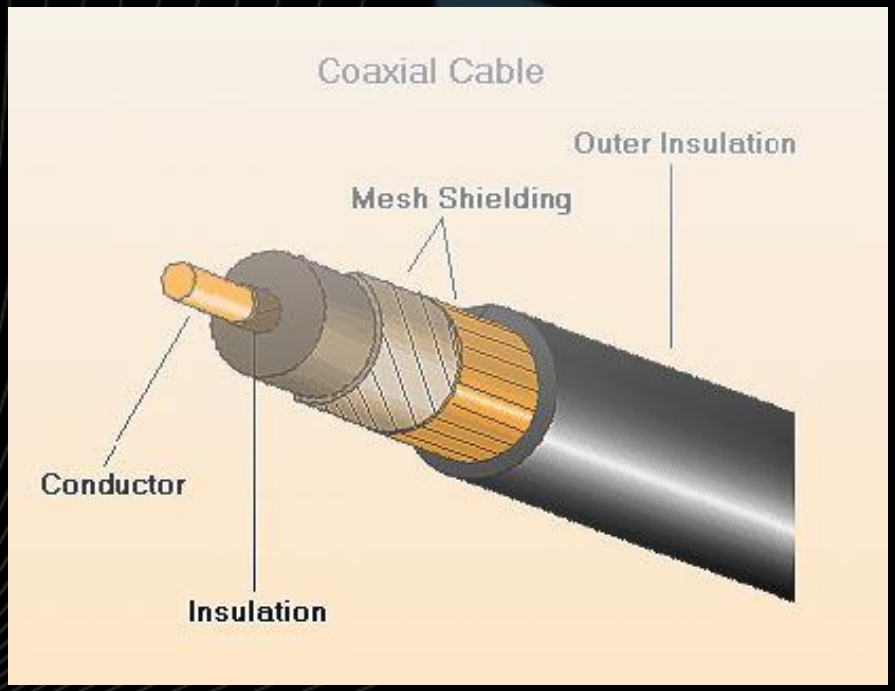
- **10BASE-T:**
  - tốc độ truyền 10Mbps
  - T: twisted pair – cáp xoắn đôi
- **10BASE5: truyền qua khoảng cách 500m**
- **10BASE2: truyền qua khoảng cách 200m**

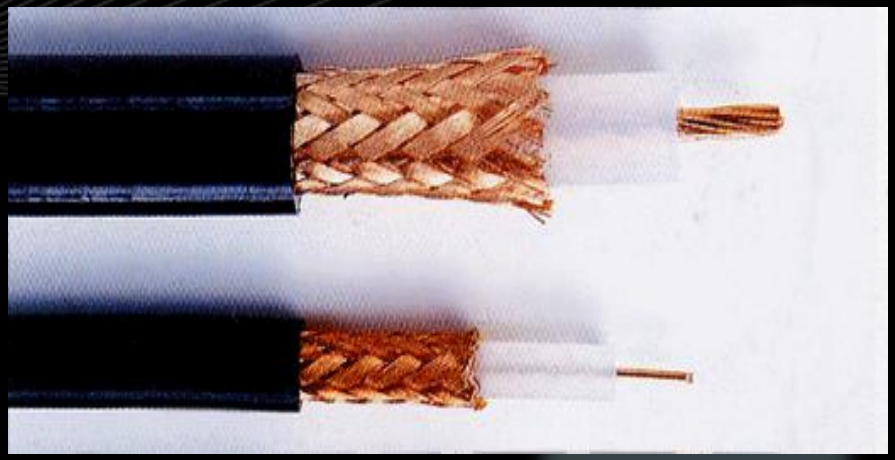
# Môi Trường Hữu Tuyến

- **Các loại cáp:**
  - Cáp đồng trục (Coaxial)
    - Thinnet
    - Thicknet
  - Cáp xoắn đôi (Twisted-Pair)
    - STP (Shielded Twisted-Pair)
    - UTP (Unshielded Twisted-Pair)
  - Cáp quang (Fiber-optic)

# Các loại cáp

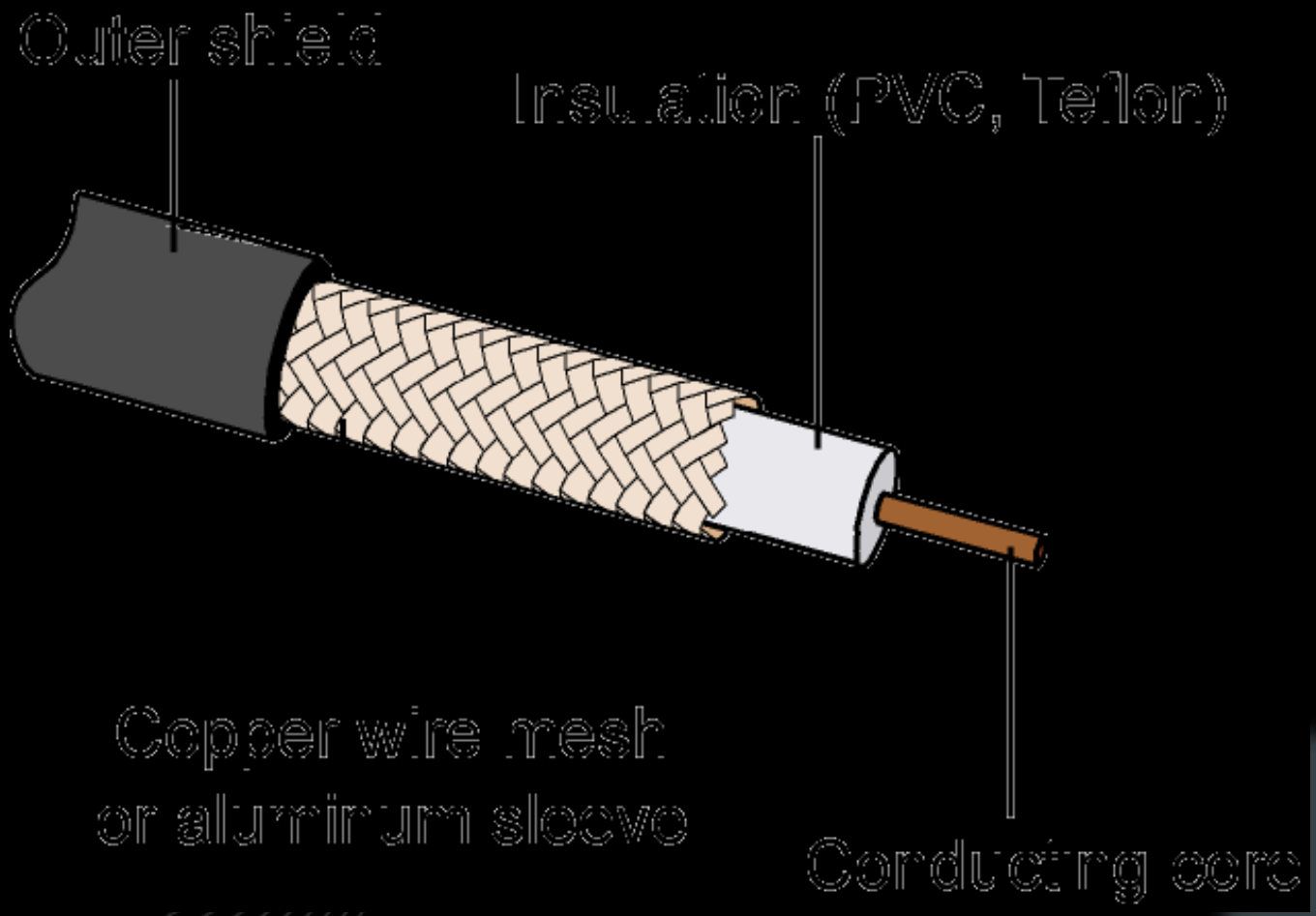
- **Cáp đồng trục (Coaxial)**
  - Là kiểu cáp đầu tiên được dùng trong mạng LAN
  - Cấu tạo:
    - Dây dẫn trung tâm: đồng, đồng bện
    - Lớp cách điện
    - Dây dẫn ngoài: dây đồng bện, lá
    - Lớp vỏ plastic bảo vệ
    - Ưu điểm: rẻ, nhẹ, dễ kéo dây



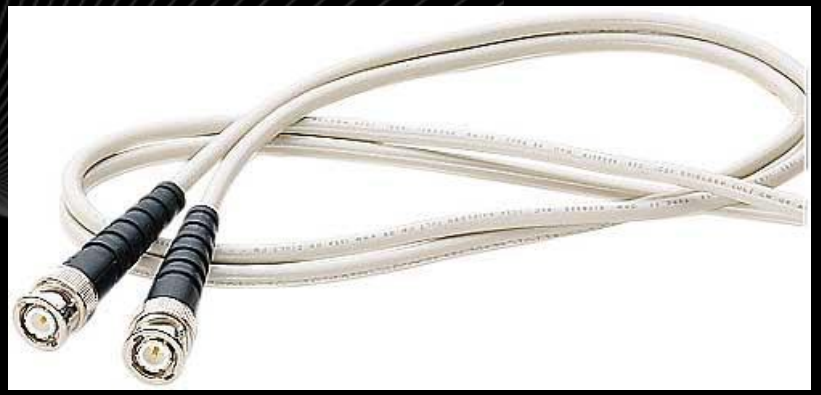
# Các loại cáp

- Cáp đồng trục (Coaxial)



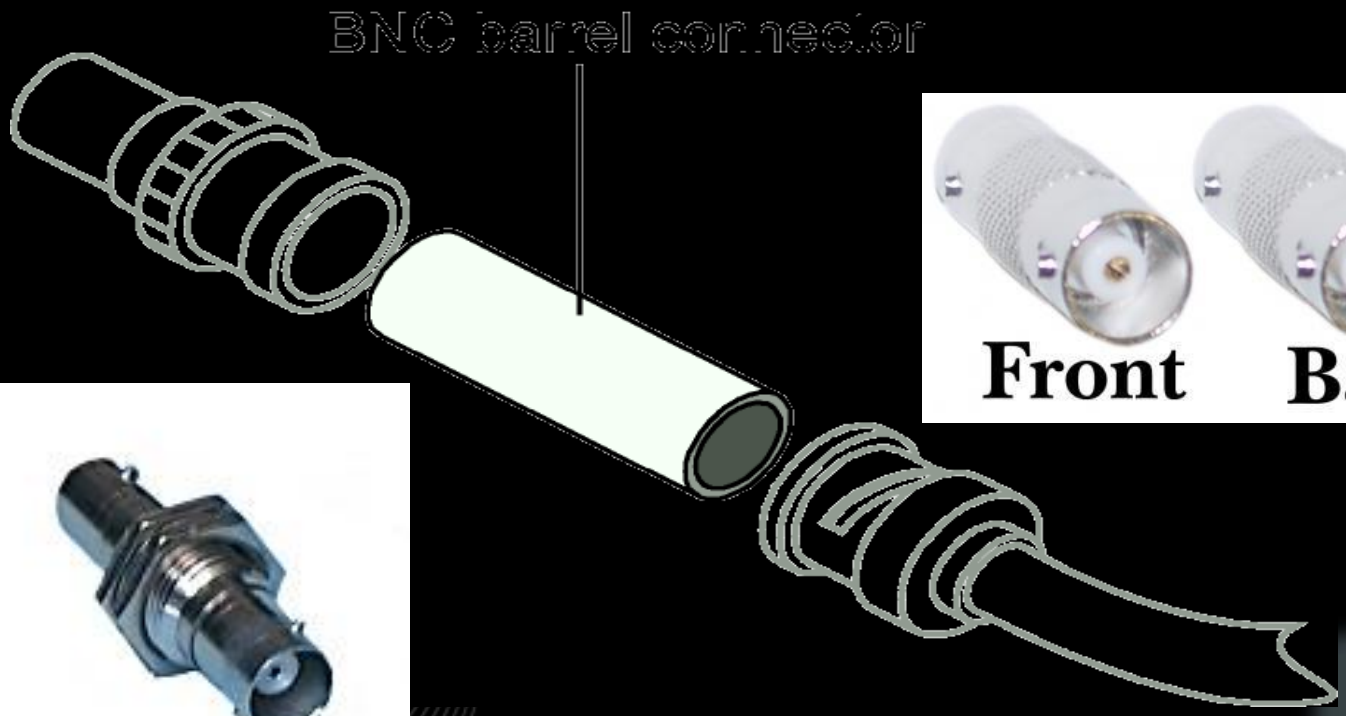
# Các loại cáp

- **Cáp đồng trục chia thành 2 loại:**
  - Thinnet (mỏng): có đường kính khoảng 6mm, thuộc họ RG58, chiều dài tối đa là 185m



# Các loại cáp

- Kết nối cáp 2 đoạn cáp Thinnet (mỏng)

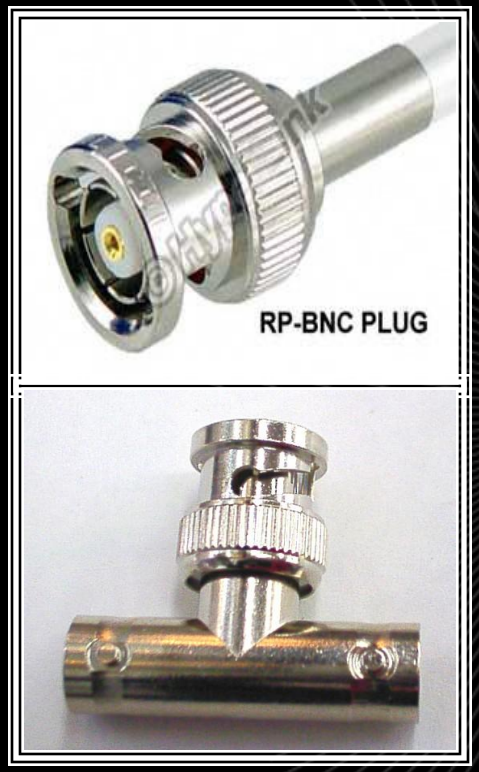


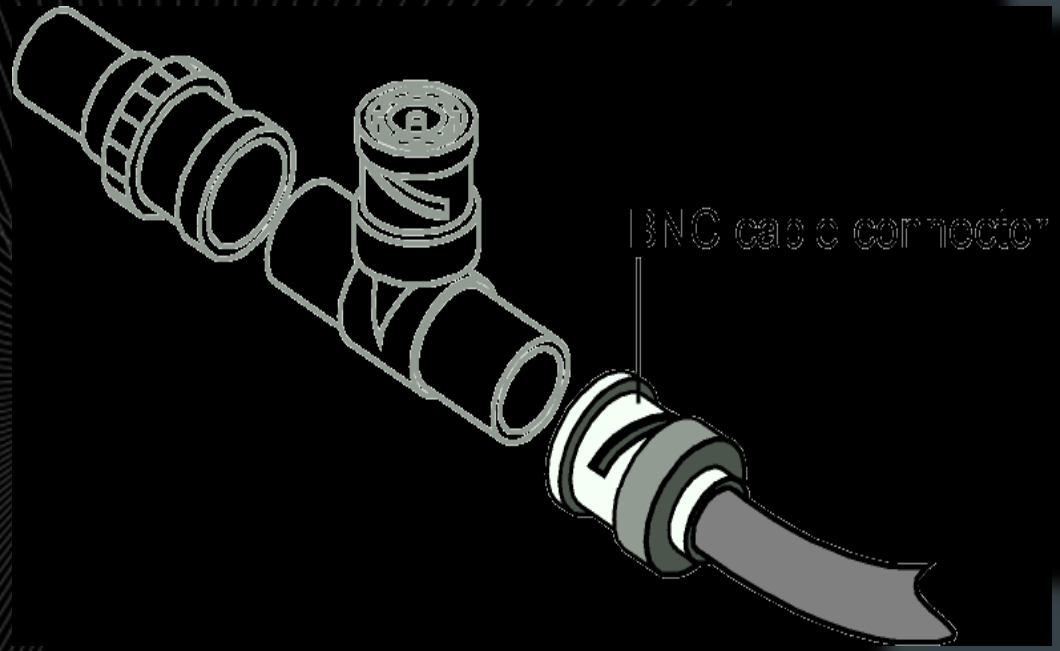
# Bộ nối cáp đồng trục và máy tính

BNC Connector

# Các loại cáp

- Kết nối cáp Thinnet (mỏng) với PC



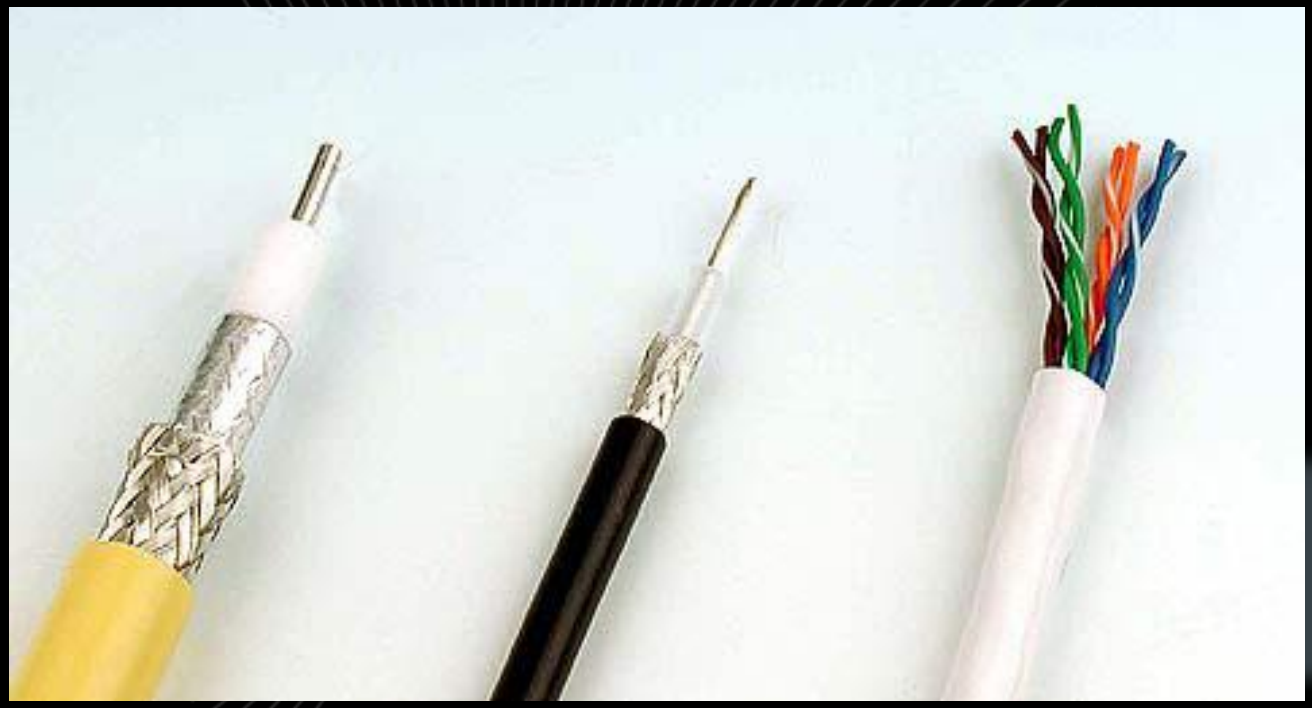



# Các loại cáp

- Kết nối cáp Thinnet (mỏng) với PC

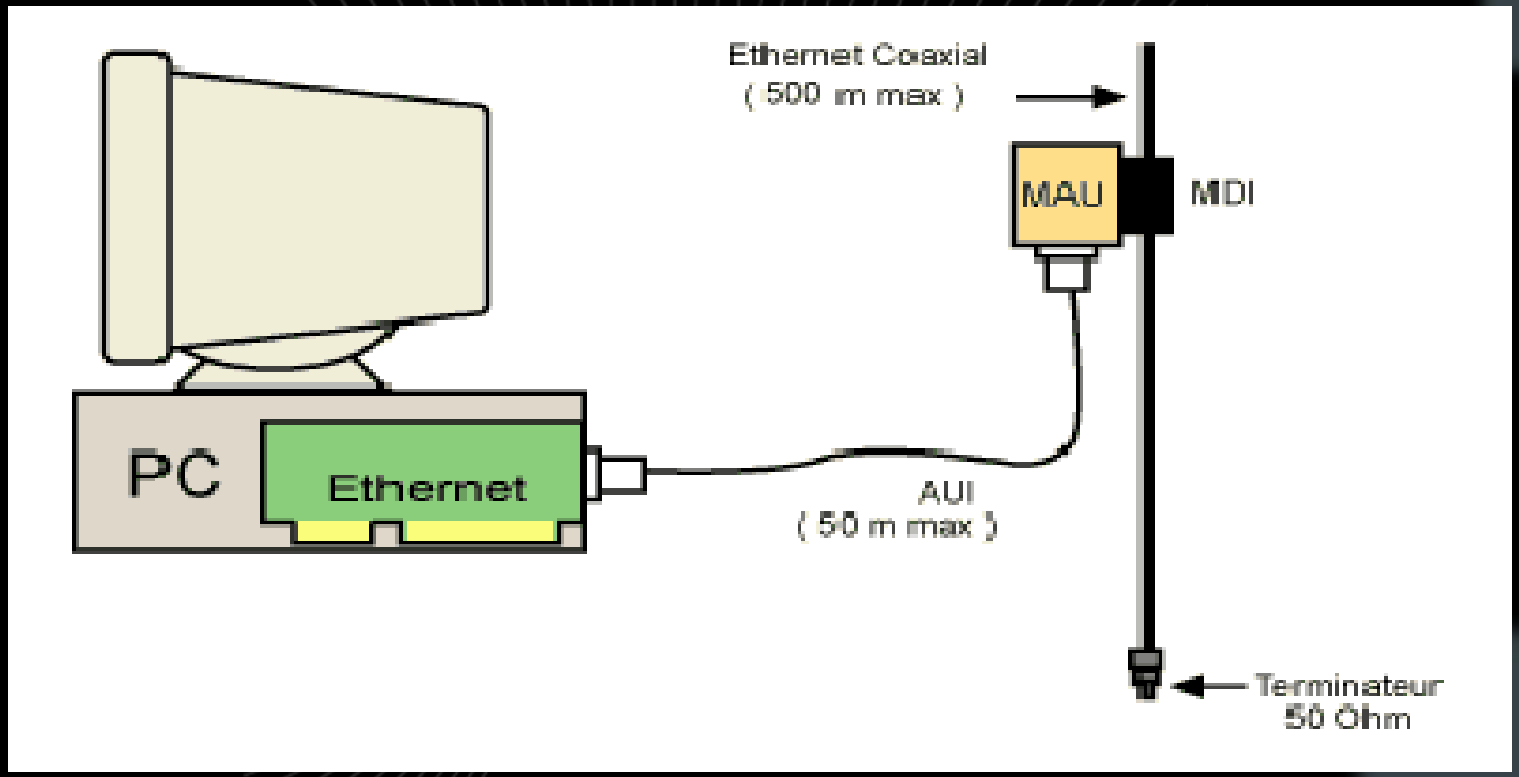
# Các loại cáp

- **Cáp đồng trục chia thành 2 loại:**
  - Thicknet (dày): có đường kính khoảng 13mm, thuộc họ RG58, chiều dài tối đa là 500m



# Các loại cáp

- Kết nối cáp Thicknet (dày)

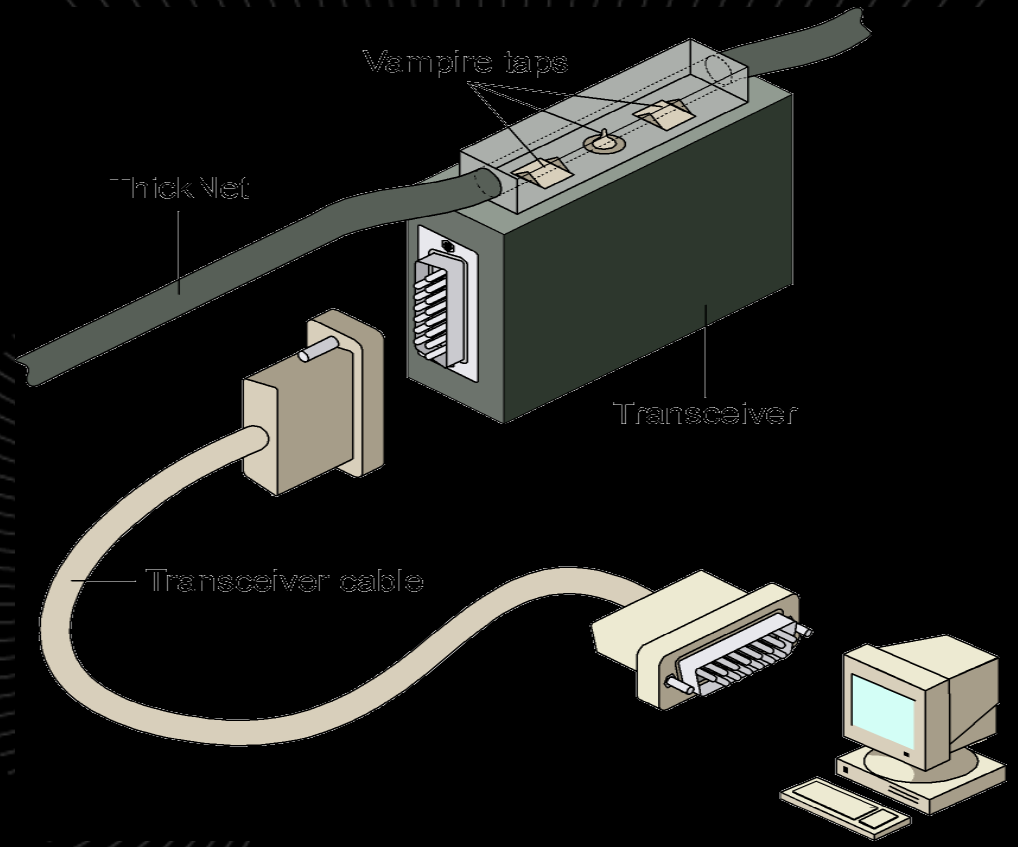


# Các loại cáp

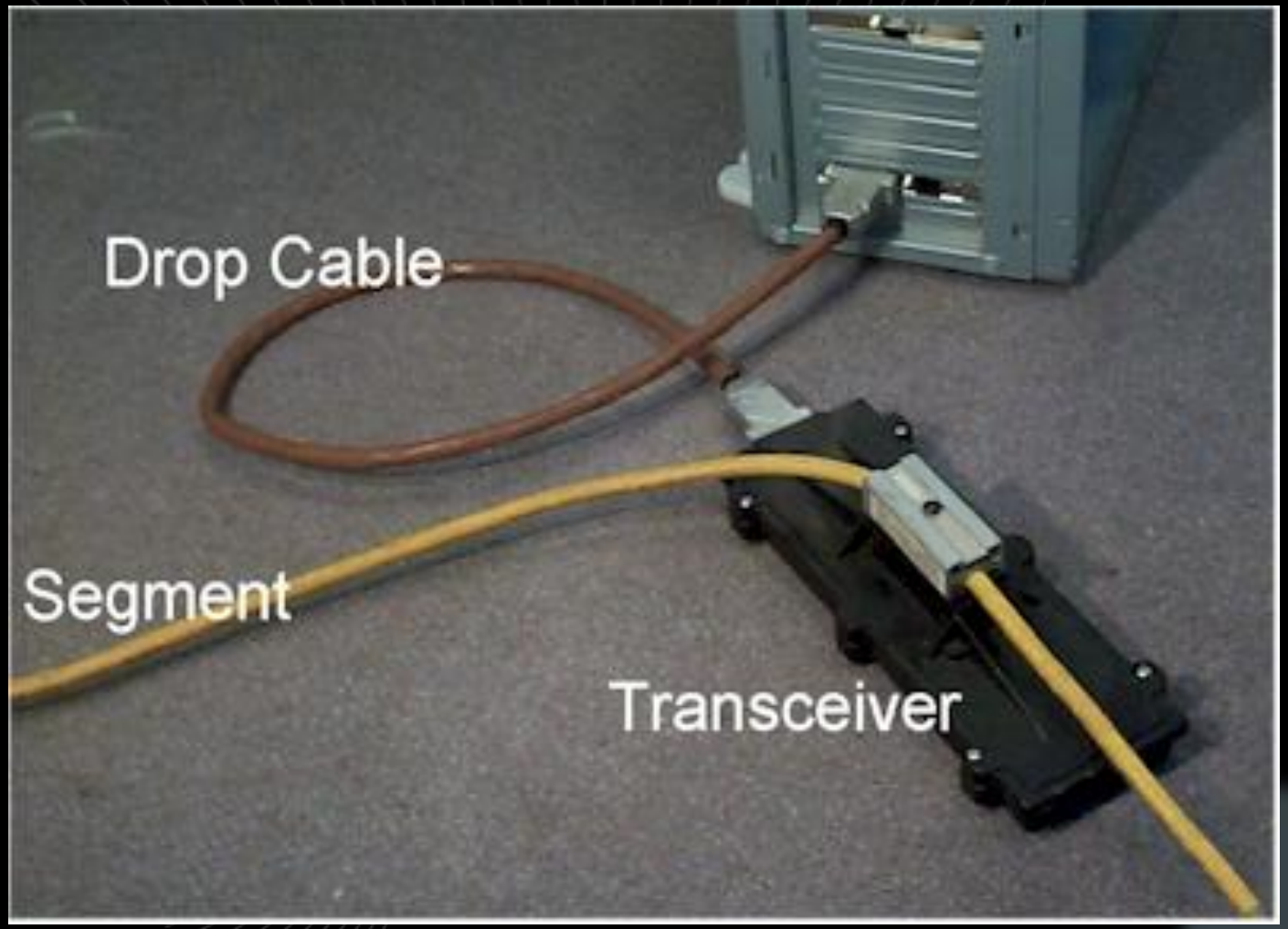
- Kết nối cáp Thicknet (dày)
- Card NIC phải hỗ trợ chuẩn AUI (Attachment Unit Interface) DB-15

# Các loại cáp

- **Kết nối cáp Thicknet (dày)**
  - Dùng bộ chuyển đổi Transceiver



# Các loại cáp

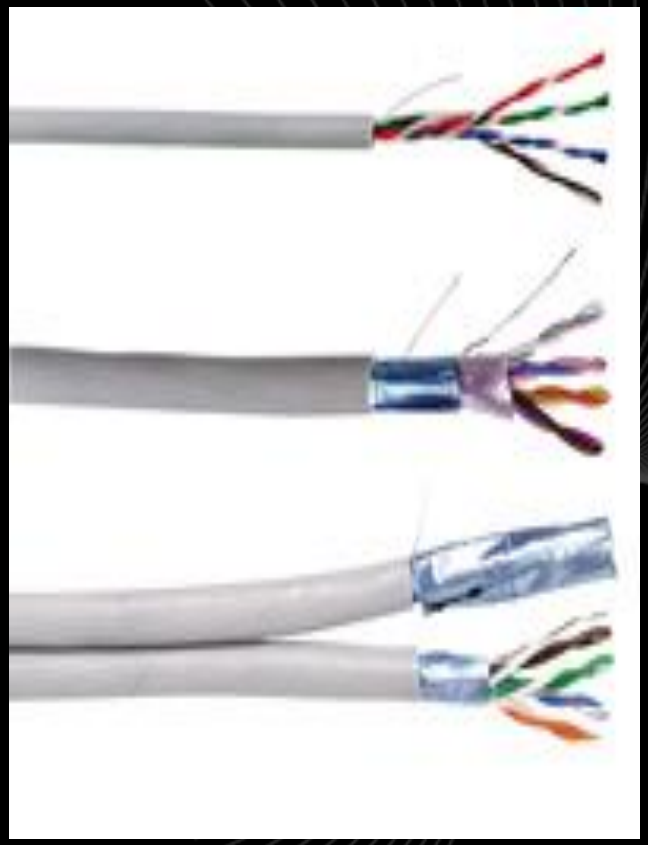


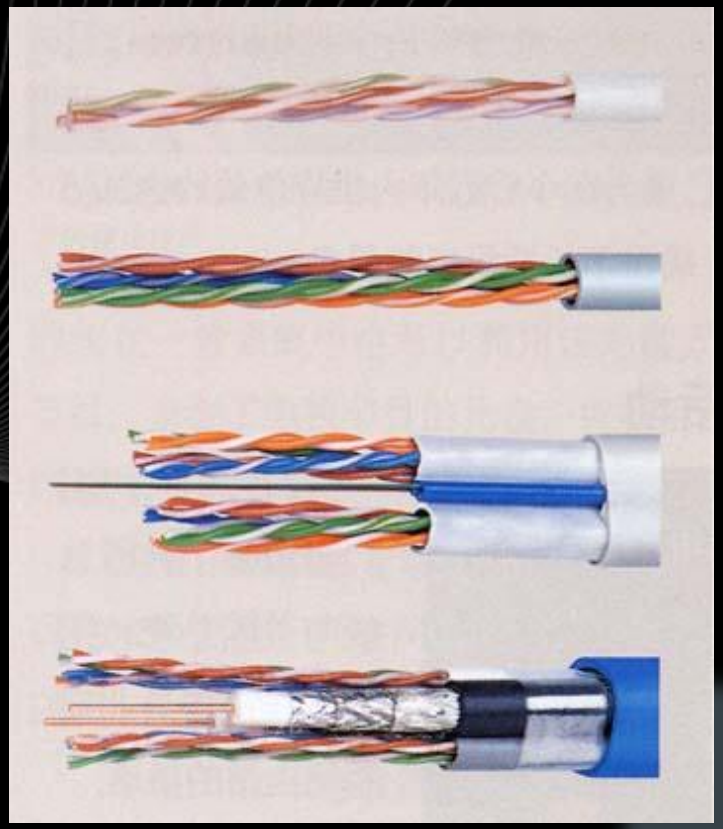
# Các loại cáp

- **Cáp xoắn đôi (Twisted-Pair)**
  - Gồm nhiều cặp dây đồng xoắn lại với nhau nhằm chống phát xạ nhiễu điện từ
  - Do giá thành thấp nên cáp xoắn được dùng rất rộng rãi
- **Có 2 loại cáp xoắn đôi:**
  - Cáp xoắn đôi có vỏ bọc chống nhiễu STP
  - Cáp xoắn đôi không có vỏ bọc chống nhiễu UTP

# Các loại cáp

- Cáp xoắn đôi (Twisted-Pair)



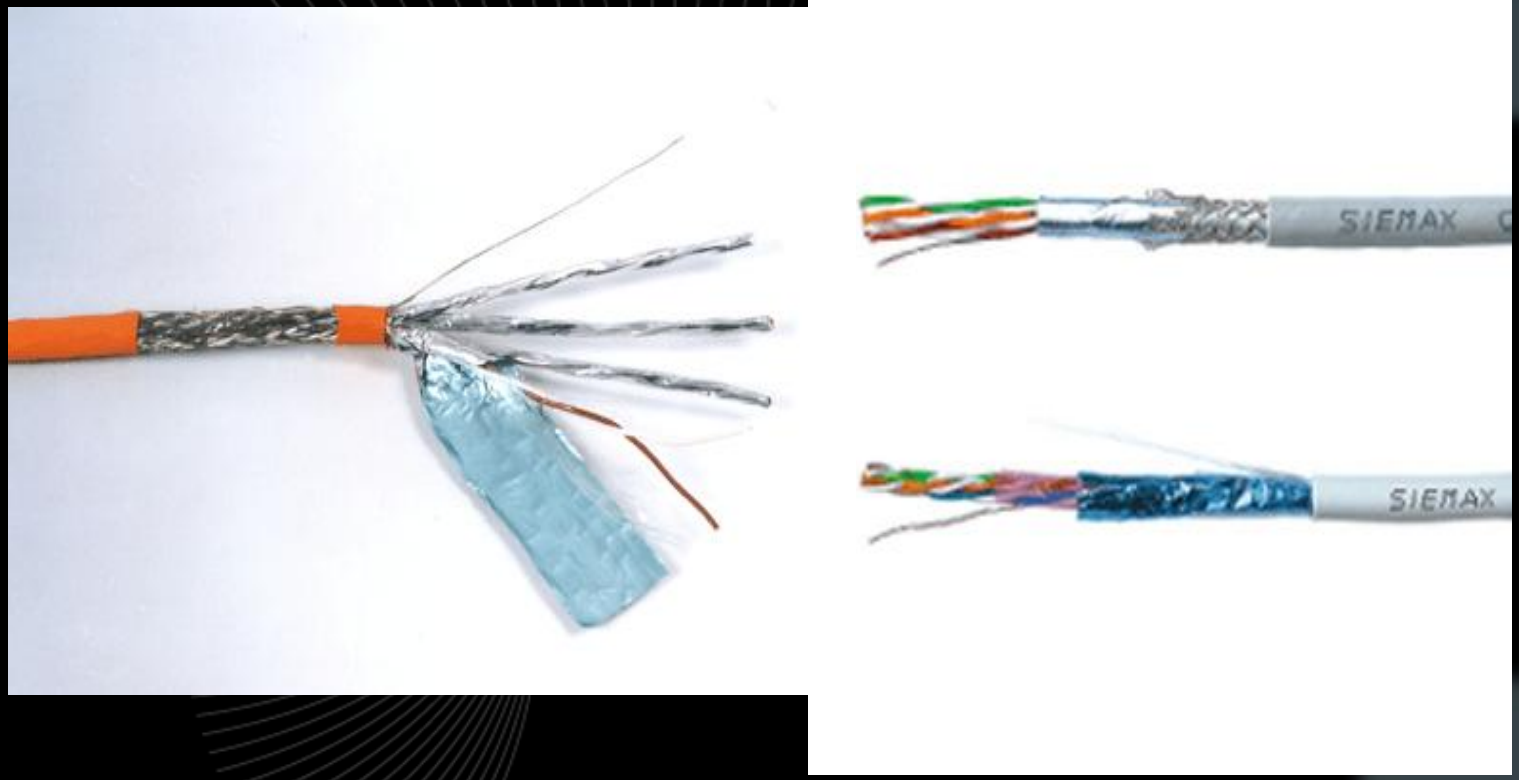


# Các loại cáp

- **Cáp STP (Shielded Twisted-Pair)**
  - Gồm nhiều cặp xoắn được phủ bên ngoài 1 lớp vỏ làm bằng dây đồng bện
  - Lớp vỏ này có chức năng chống nhiễu từ bên ngoài và chống phát xạ nhiễu bên trong
  - Lớp chống nhiễu này được nối đất để thoát nhiễu
  - Tốc độ: lý thuyết 500Mbps, thực tế 155Mbps với chiều dài 100m
  - Đầu nối: DIN (DB-9), RJ45

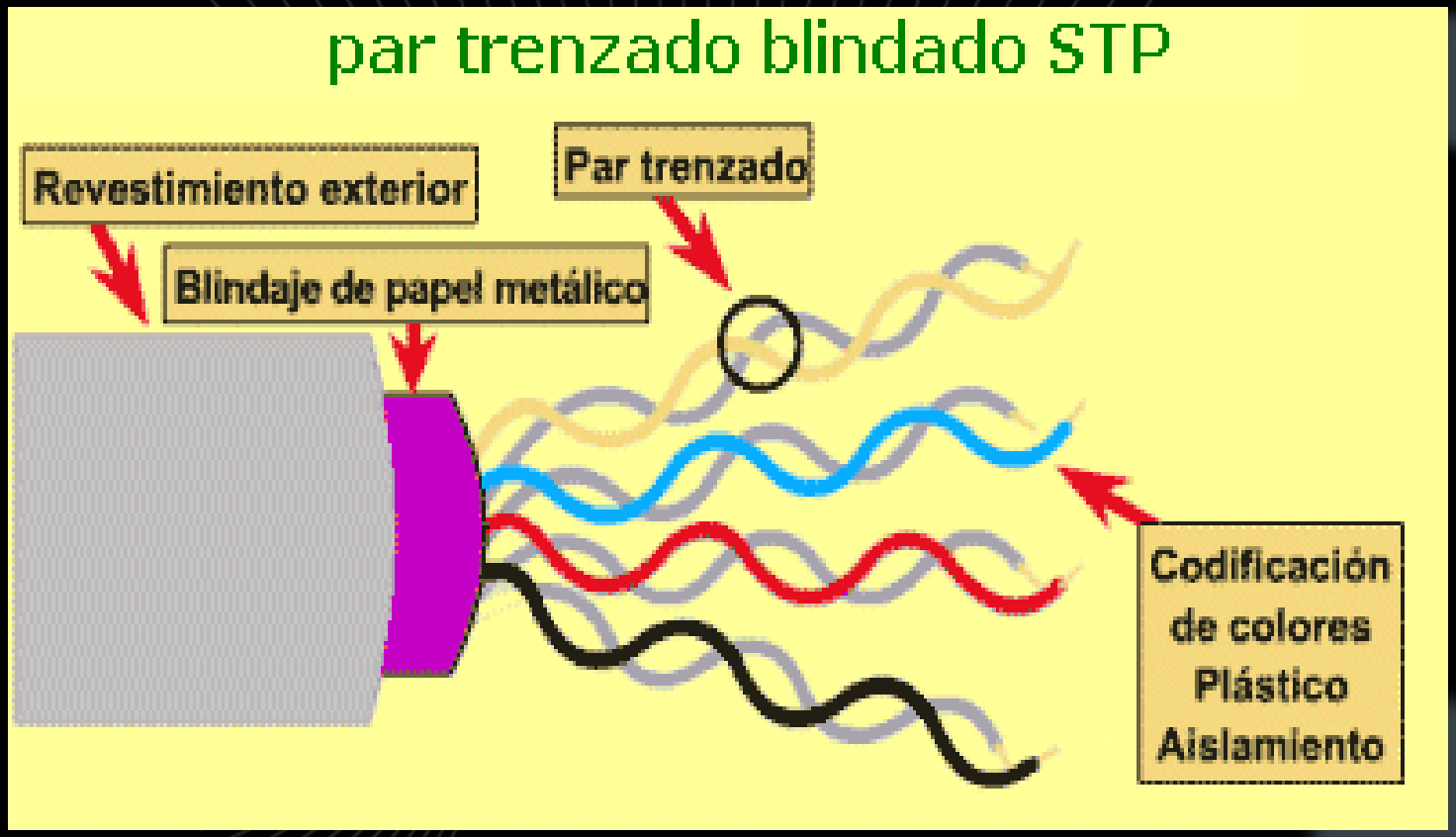
# Các loại cáp

- Cáp STP (Shielded Twisted-Pair)



# Các loại cáp

- Cáp STP (Shielded Twisted-Pair)

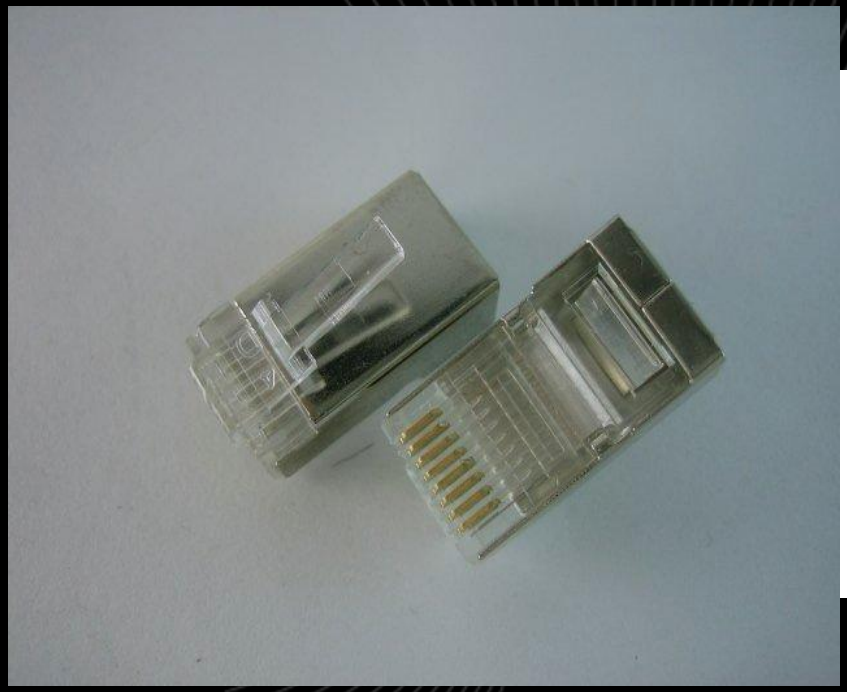


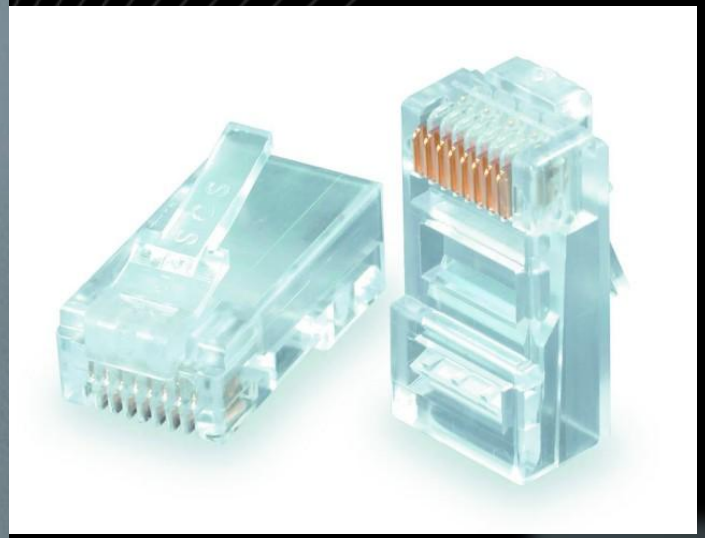
# Các loại cáp

- **Cáp STP (Shielded Twisted-Pair)**
  - Đầu nối DB-9

# Các loại cáp

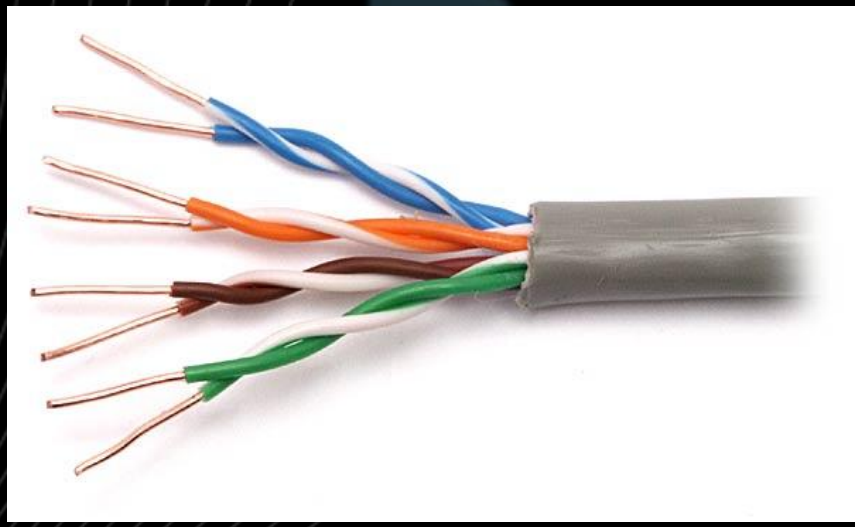
- **Cáp STP (Shielded Twisted-Pair)**
  - Đầu nối RJ45 for STP

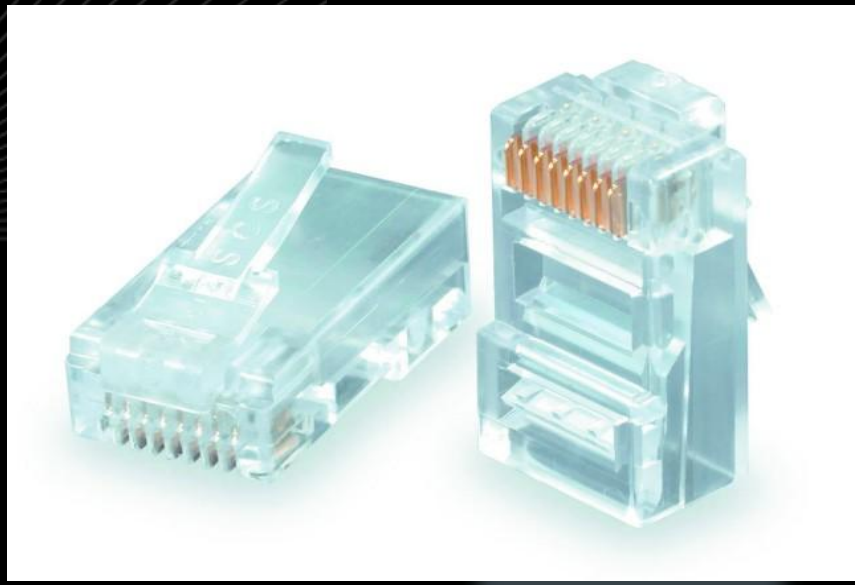




# Các loại cáp

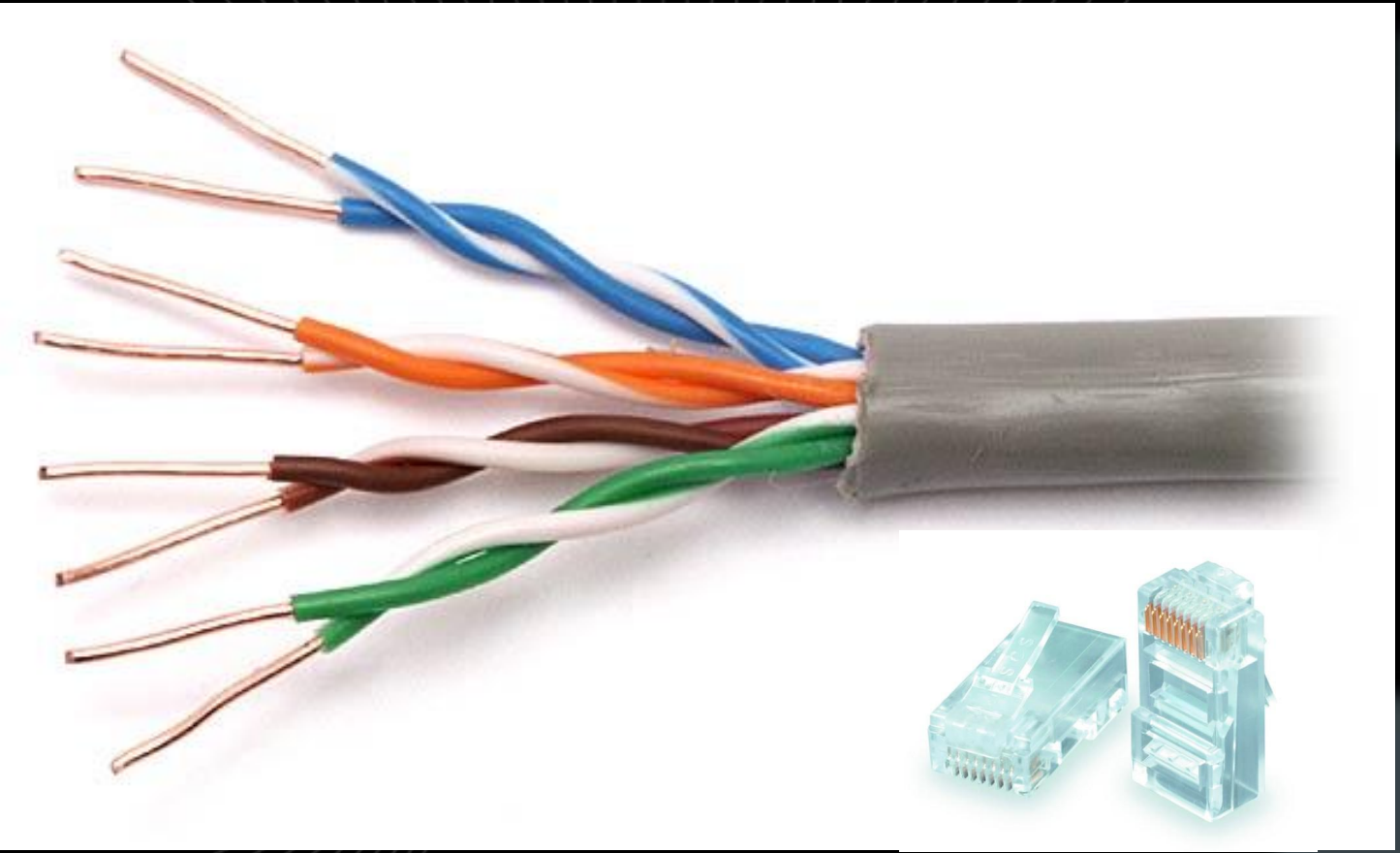
- **Cáp UTP (Unshielded Twisted-Pair)**
  - Gồm nhiều cặp xoắn như cáp STP nhưng nó không có lớp vỏ bọc chống nhiễu
  - Khoảng cách truyền tối đa của đoạn cáp là 100m
  - Dễ bị nhiễu khi đặt gần các thiết bị như: đường dây điện cao thế, nhiễu xuyên kênh…





# Các loại cáp

- Cáp UTP (Unshielded Twisted-Pair)



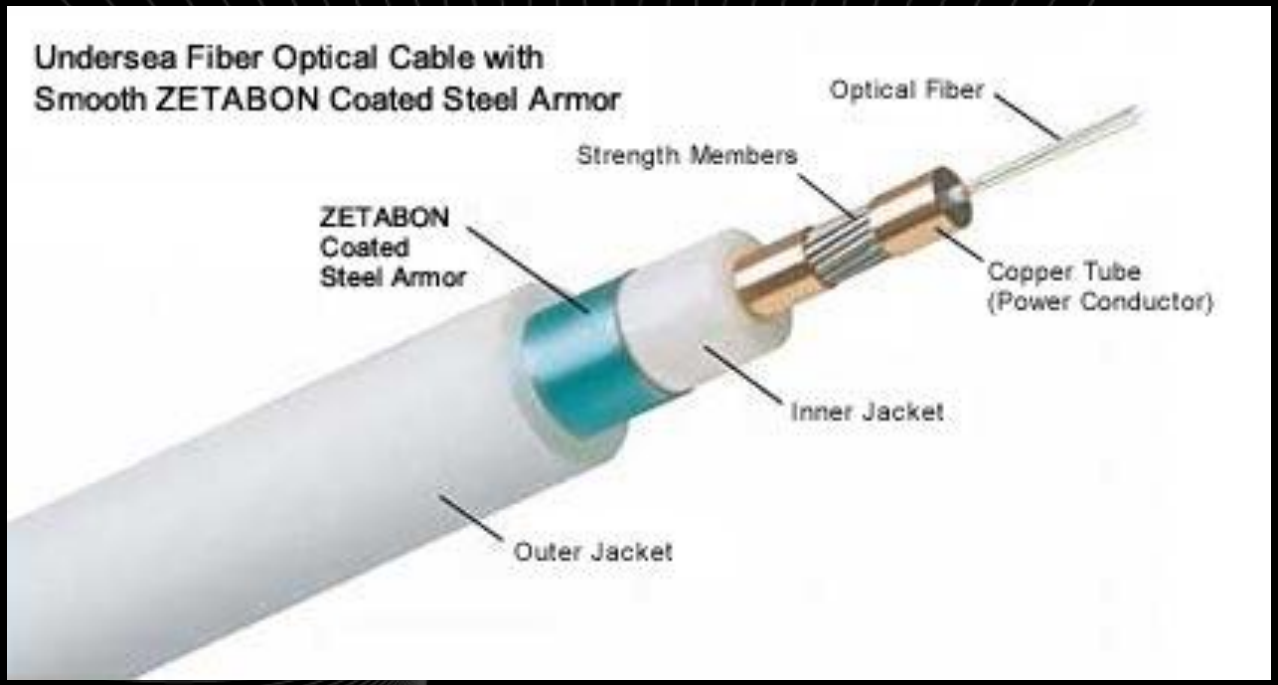
# Các loại cáp

- **Cáp UTP có 6 loại:**
  - Loại 1(Cat1): truyền âm thanh, tốc độ <4Mbps
  - Loại 2(Cat2): gồm 4 cặp xoắn, tốc độ 4Mbps
  - Loại 3(Cat3): gồm 4 cặp xoắn, tốc độ 10Mbps
  - Loại 4(Cat4): gồm 4 cặp xoắn, tốc độ 16Mbps
  - Loại 5(Cat5): gồm 4 cặp xoắn, tốc độ 100Mbps
  - Loại 6(Cat6): gồm 4 cặp xoắn, tốc độ 1000Mbps

# Các loại cáp

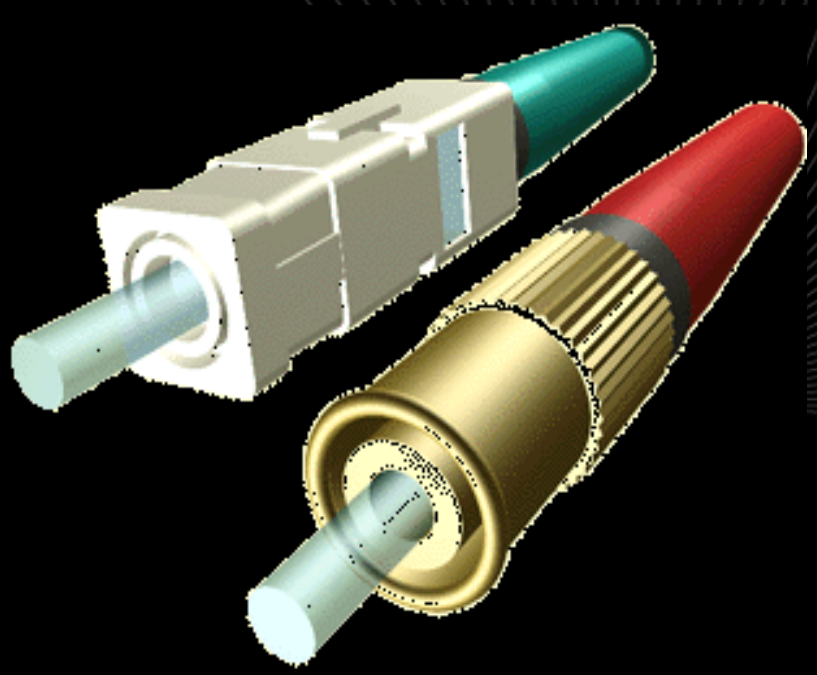
- **Cáp quang (Fiber-Optic)**
  - Có cấu tạo gồm dây dẫn trung tâm là sợi thủy tinh hoặc plastic đã được tinh chế nhằm cho phép truyền đi tối đa các tín hiệu ánh sáng
  - Cáp quang chỉ truyền sóng ánh sáng (không truyền tín hiệu điện) với băng thông cực cao
  - Băng thông cho phép đến 2Gbps, có thể dài đến vài km
  - Giá thành quá cao, khó lắp đặt

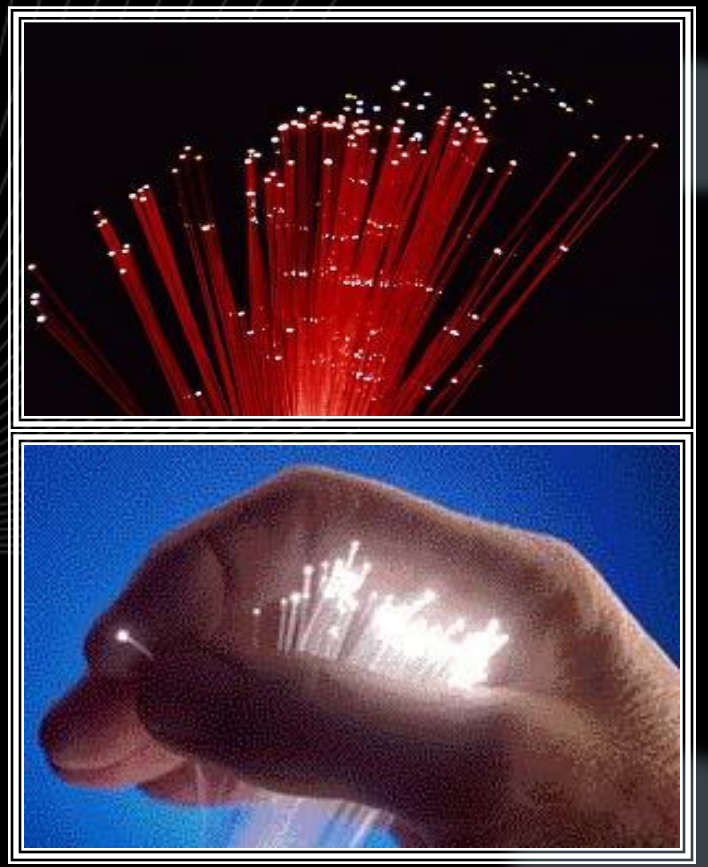
# Cáp quang


Undersea Fiber Optical Cable with
Smooth ZETABON Coated Steel Armor
Optical Fiber
Strength Members
ZETABON
Coated
Steel Armor
Copper Tube
(Power Conductor)
Inner Jacket
Outer Jacket

# Các loại cáp

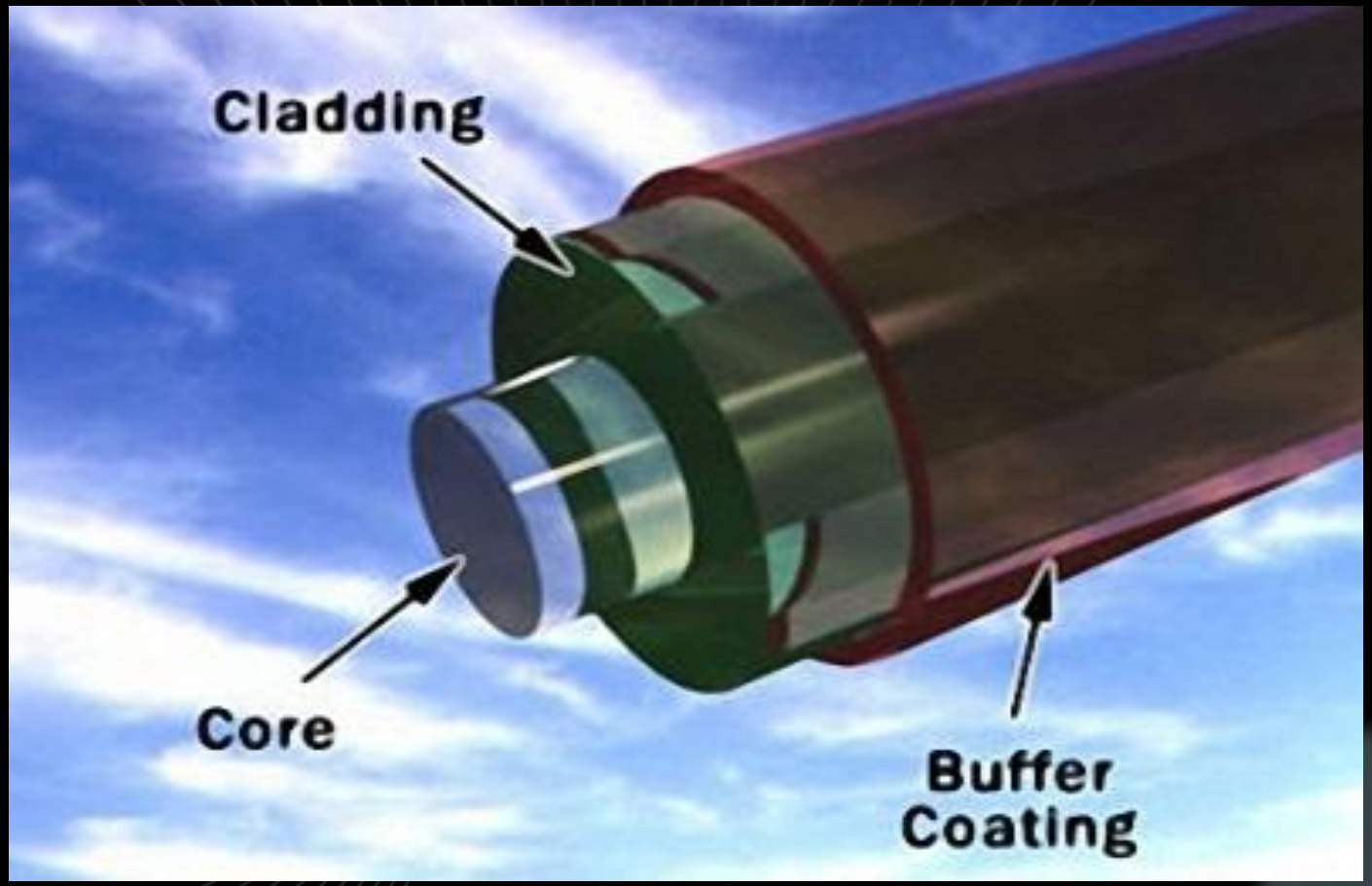
- Cáp quang (Fiber-Optic)





# Các loại cáp

- Cáp quang (Fiber-Optic)



# Các loại cáp

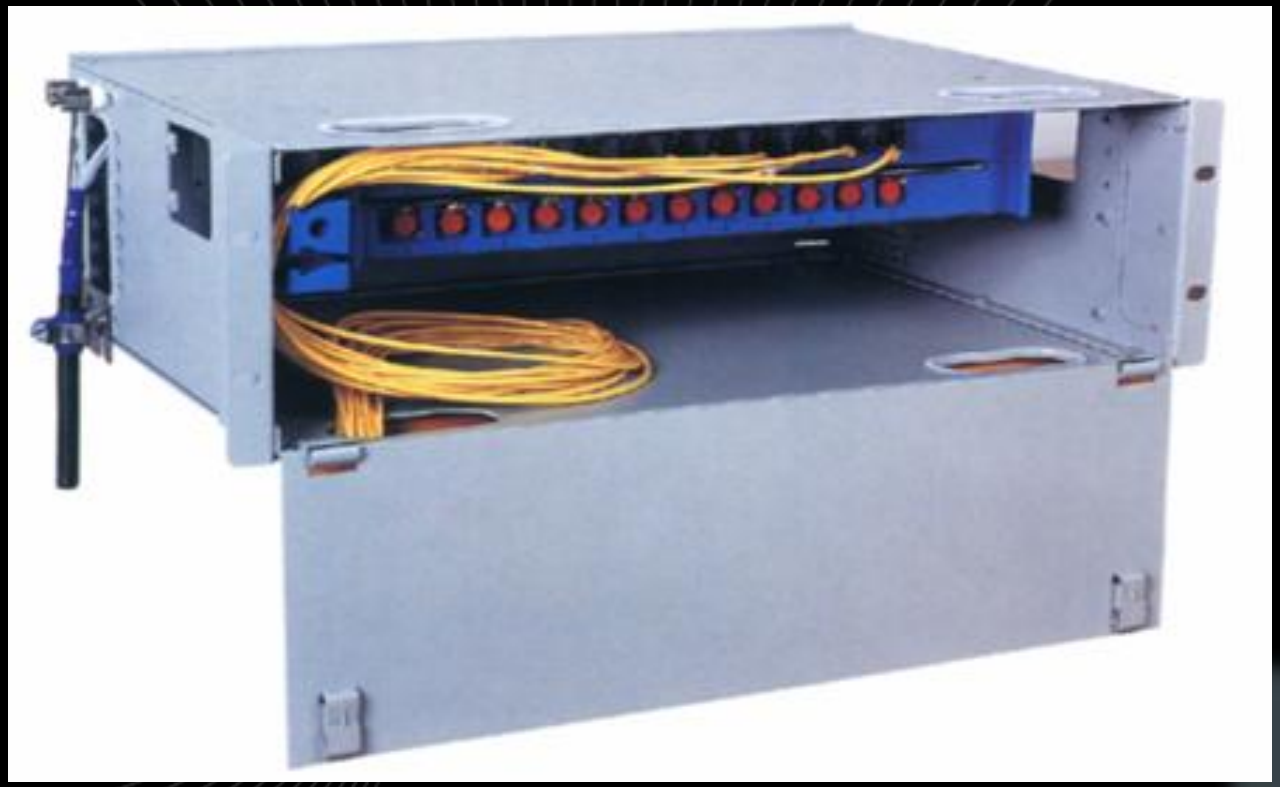
- **Cáp quang hỗ trợ 2 chế độ:**
  - **Multi-mode (đa chế độ)**
    - Sợi cáp thủy tinh có thể truyền được nhiều tia sáng trong cùng một khoảng thời gian
    - Khoảng cách đường truyền không xa bằng loại Single-mode
  - **Single-mode (chế độ đơn)**
    - Sợi cáp thủy tinh chỉ truyền 1 tia sáng duy nhất trên đường dây

# Các loại cáp

- **Các loại cáp quang:**
  - Loại lõi 8.3 micron, lớp lót 125 micron (đơn)
  - Loại lõi 62.5 micron, lớp lót 125 micron (đa)
  - Loại lõi 50 micron, lớp lót 125 micron (đa)
  - Loại lõi 100 micron, lớp lót 140 micron (đa)
- **Hộp đấu nối cáp quang:**
  - Do cáp quang thể bẻ cong nên khi nối cáp quang vào các thiết bị khác chúng ta phải thông qua hộp đấu nối (ODF - Optical Distribution Frame)

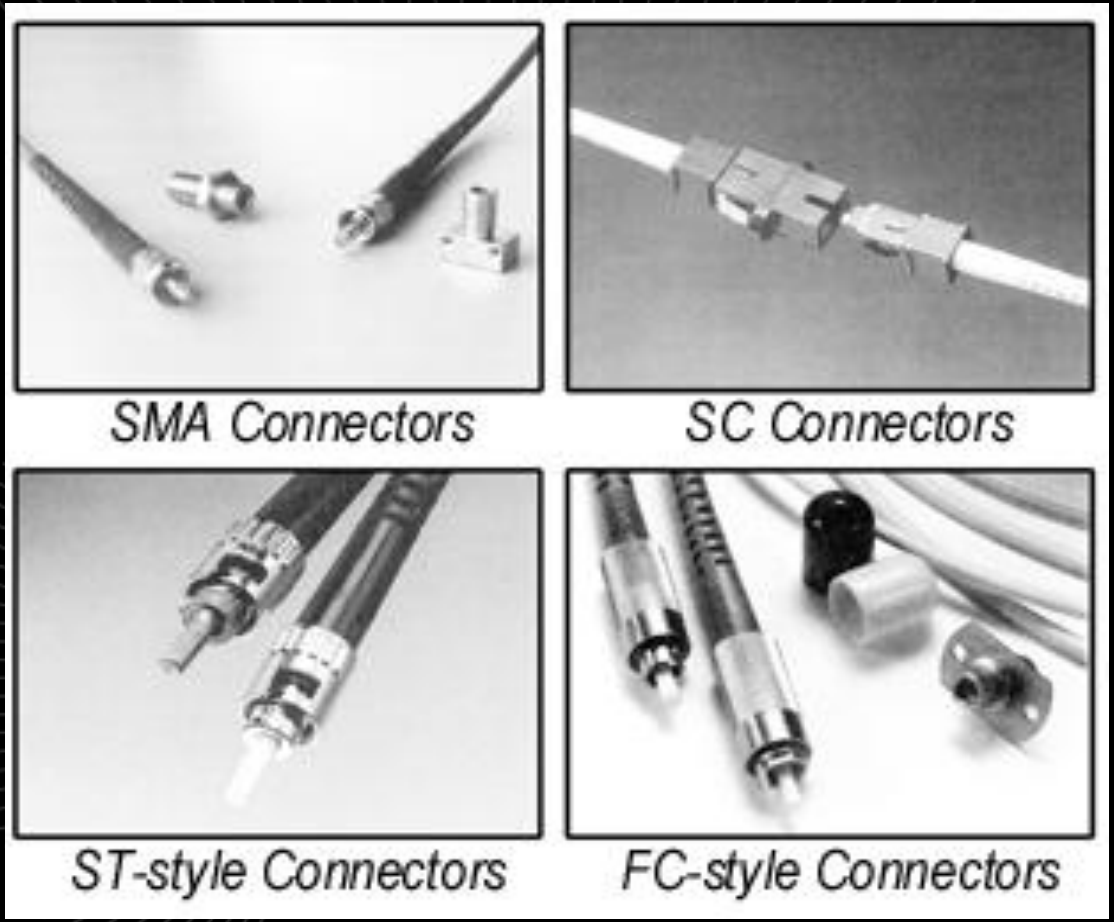
# Các loại cáp

- Hộp đấu nối cáp quang (ODF)



# Các loại cáp

- Đầu nối cáp quang:



# Môi Trường Vô Tuyến

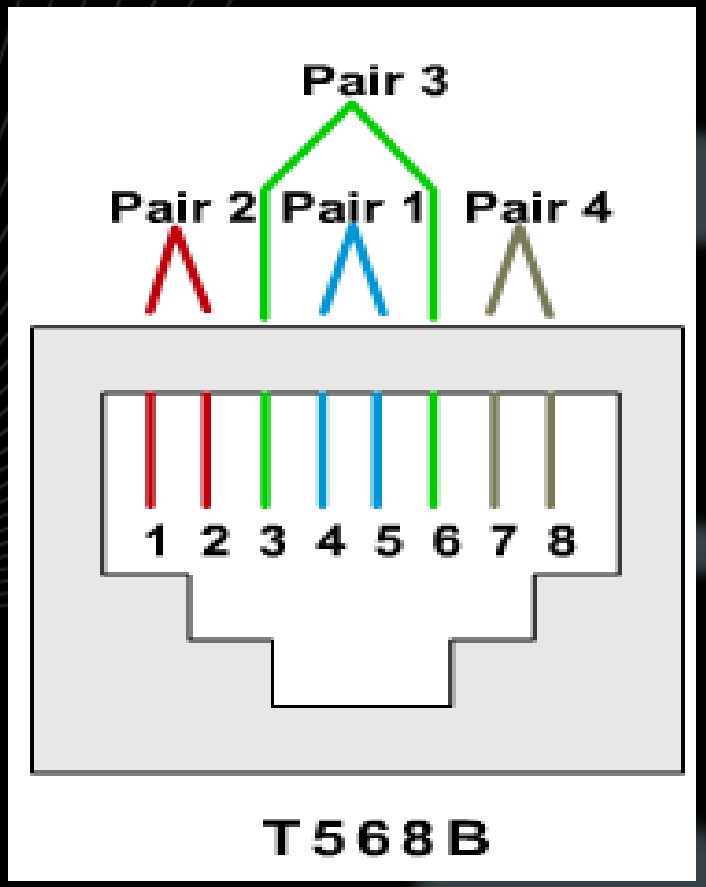
- **Sóng Radio hoạt động trên dãi tần:**
  - 10KHz -> 1GHz
- **Sóng Viba hoạt động trên dãi tần:**
  - 21GHz -> 23GHz
  - Sóng Viba mặt đất và sóng Viba vệ tinh
  - Tốc độ từ 1 -> 10Mbps
- **Sóng Hồng Ngoại hoạt động trên dãi tần:**
  - 100GHz -> 1000GHz
  - Tốc độ từ 1 -> 10Mbps

# Kỹ Thuật Bấm Cáp

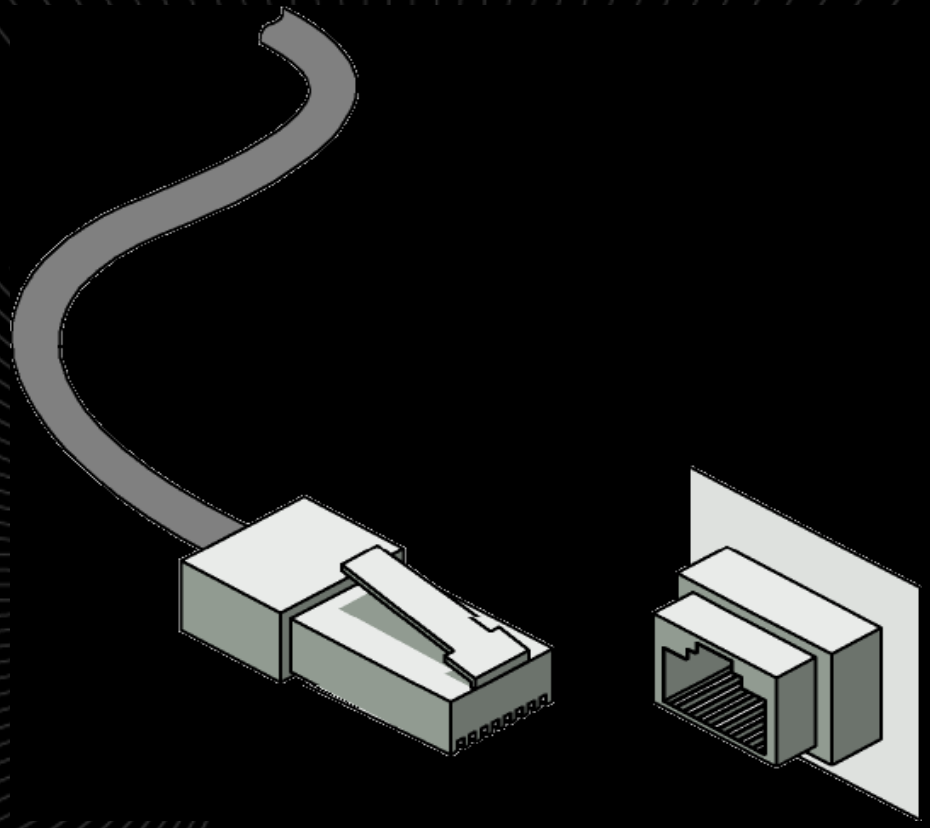
- **Có 2 chuẩn bấm cáp chính:**
  - Chuẩn T568A
  - Chuẩn T568B
- **Có 3 kỹ thuật bấm cáp:**
  - Cáp thẳng (Straight-through)
  - Cáp chéo (Crossover)
  - Cáp Console

# Qui ước mã màu cáp TIA/EIA 568B

| Pin | Color |
|---|---|
| 1 | White Orange |
| 2 | Orange |
| 3 | White Green |
| 4 | Blue |
| 5 | White Blue |
| 6 | Green |
| 7 | White Brown |
| 8 | Brown |

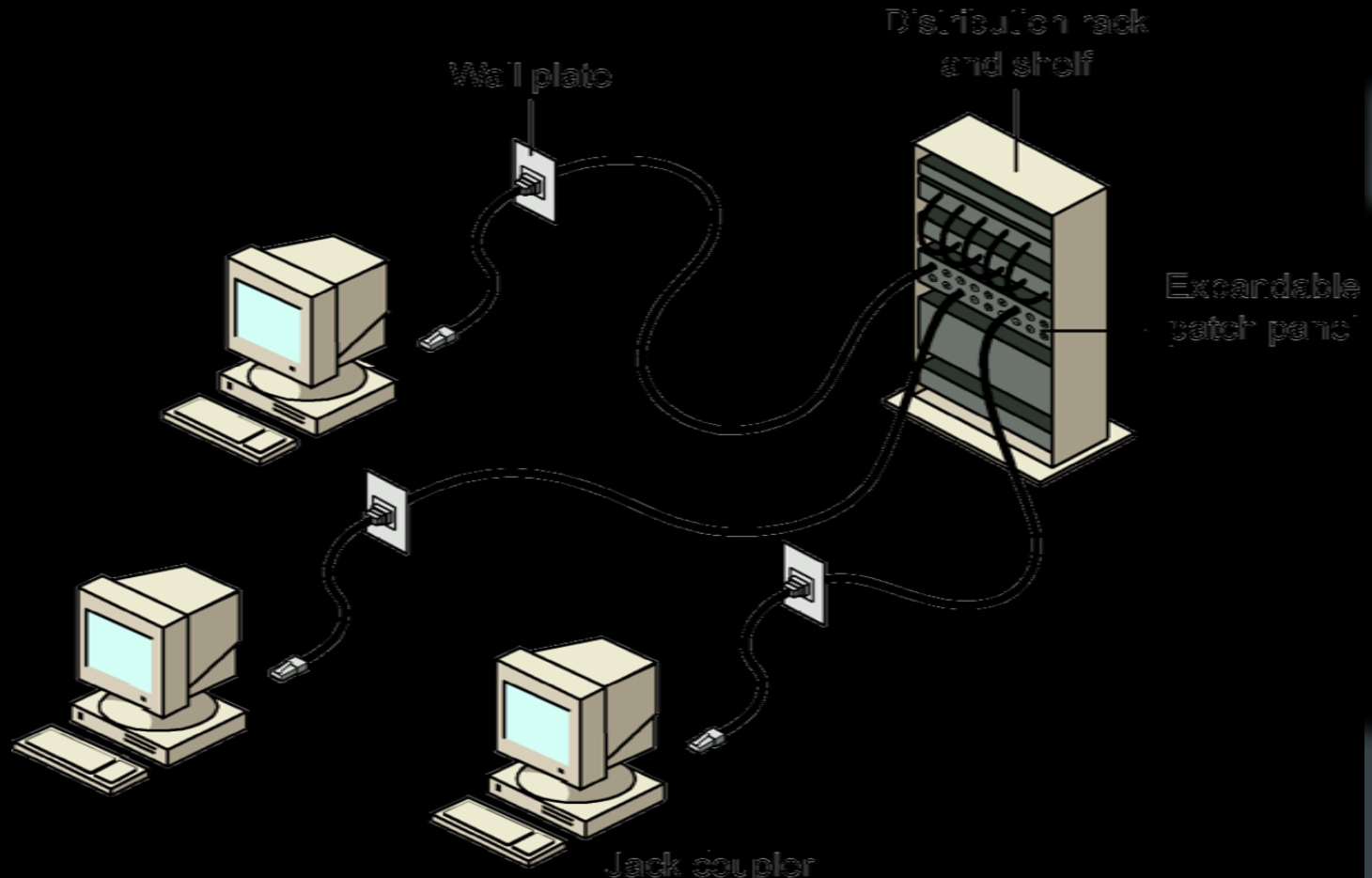


- Đầu nối outlet sử dụng RJ45



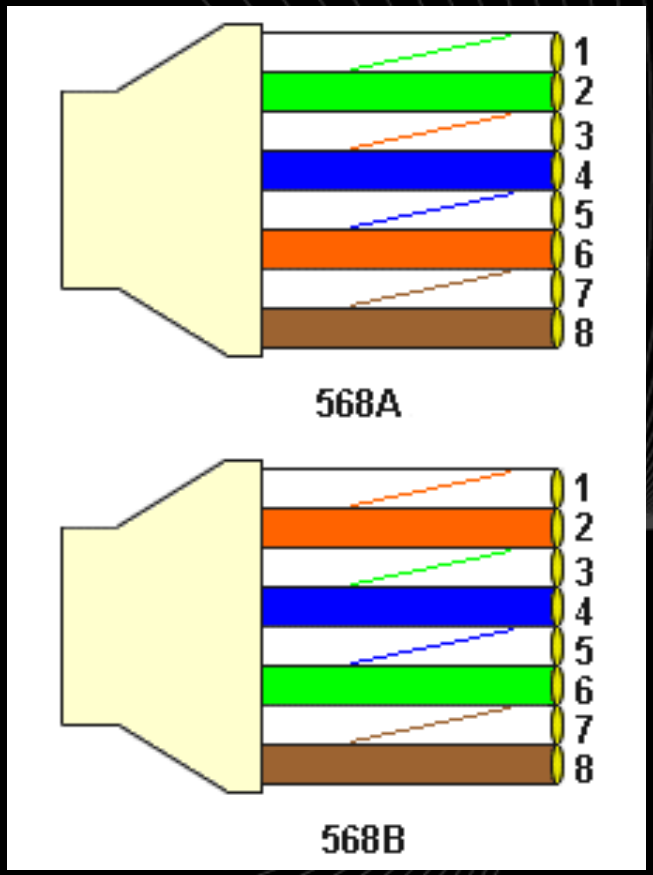
## Đầu nối outlet, Patch Panel sử dụng

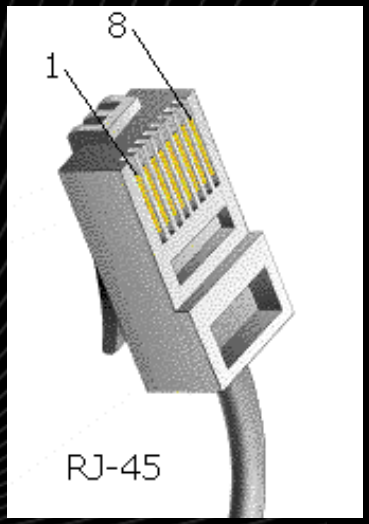
## Đầu nối outlet sử dụng RJ45



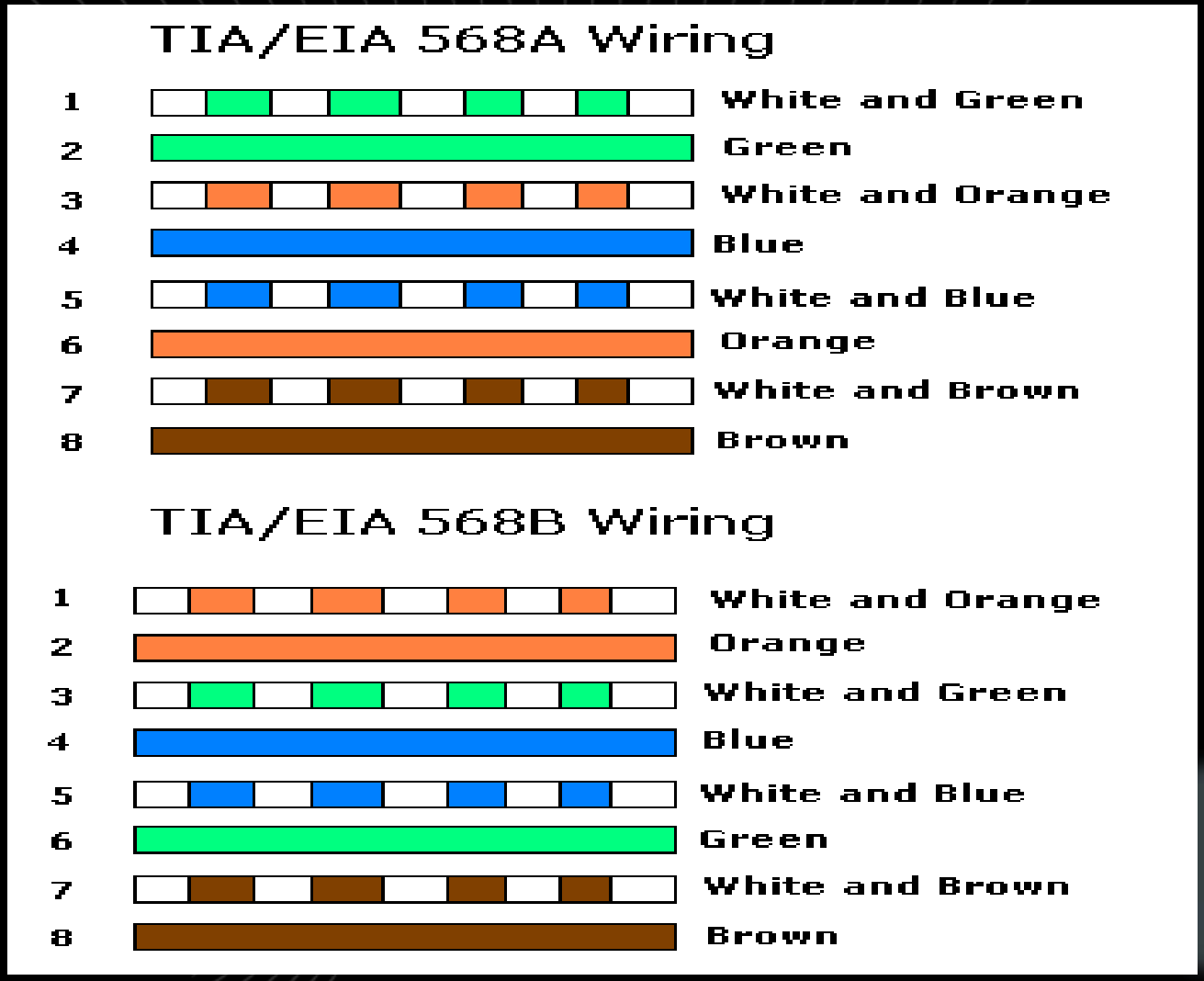
# Kỹ Thuật Bấm Cáp

- Có 2 chuẩn chính:



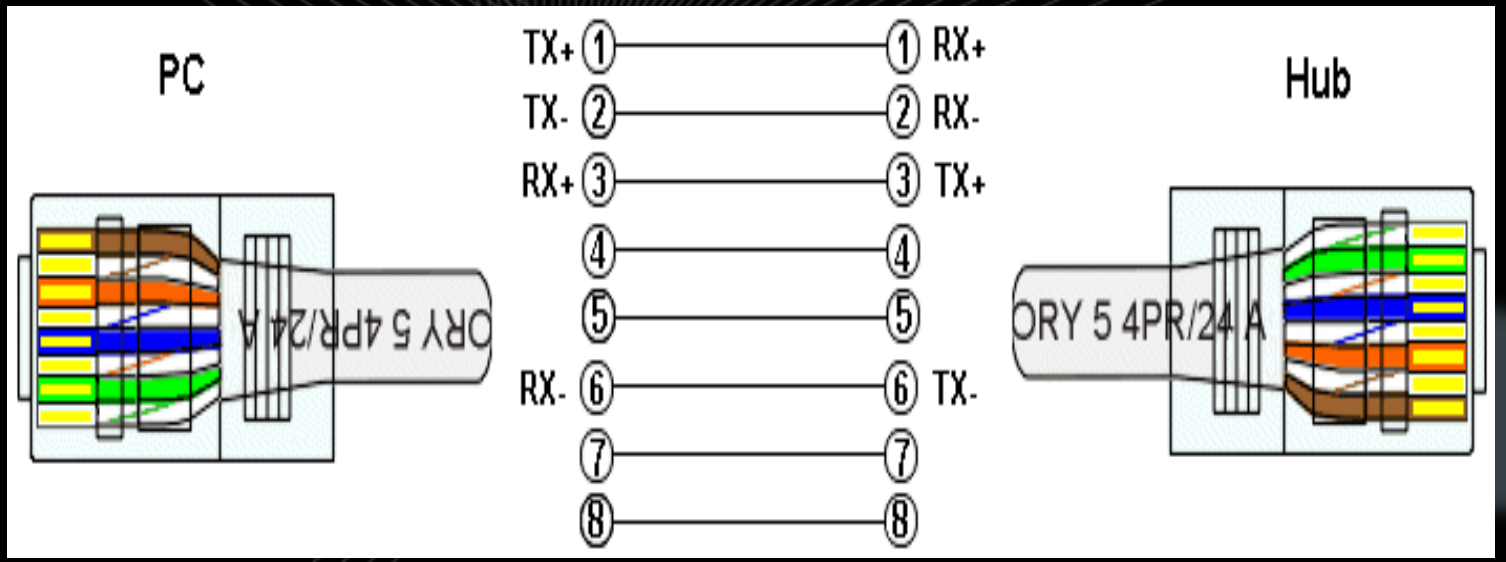



# Kỹ Thuật Bấm Cáp



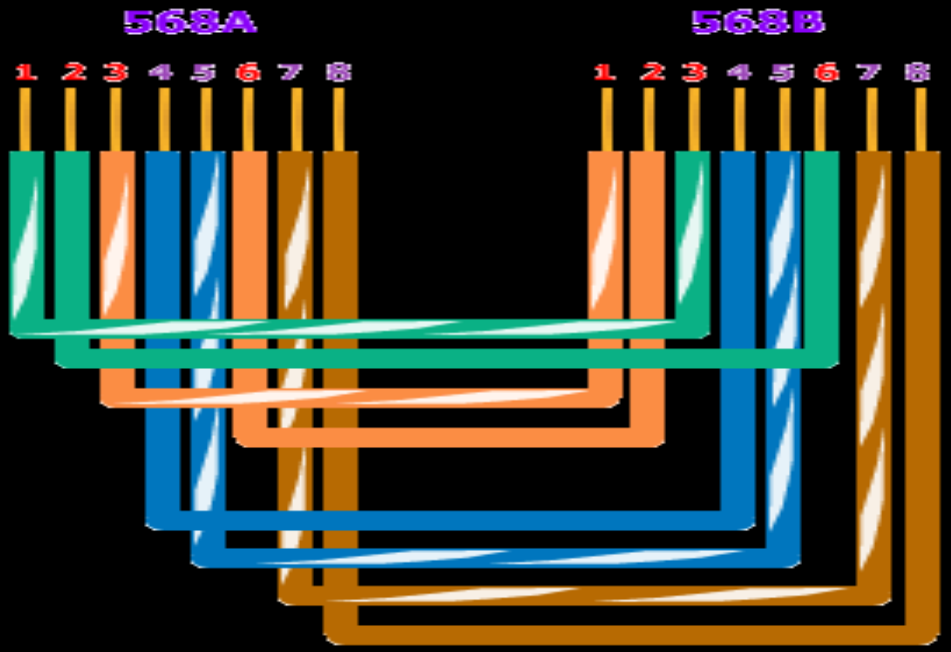
# Kỹ Thuật Bấm Cáp

- **Cáp thẳng (Straight-through)**
  - Là cáp để nối PC với các thiết bị mạng như: Hub, Switch, Router…
  - Theo chuẩn 10/100Based-T, dùng chân 1,2,3,6 trên đầu RJ45

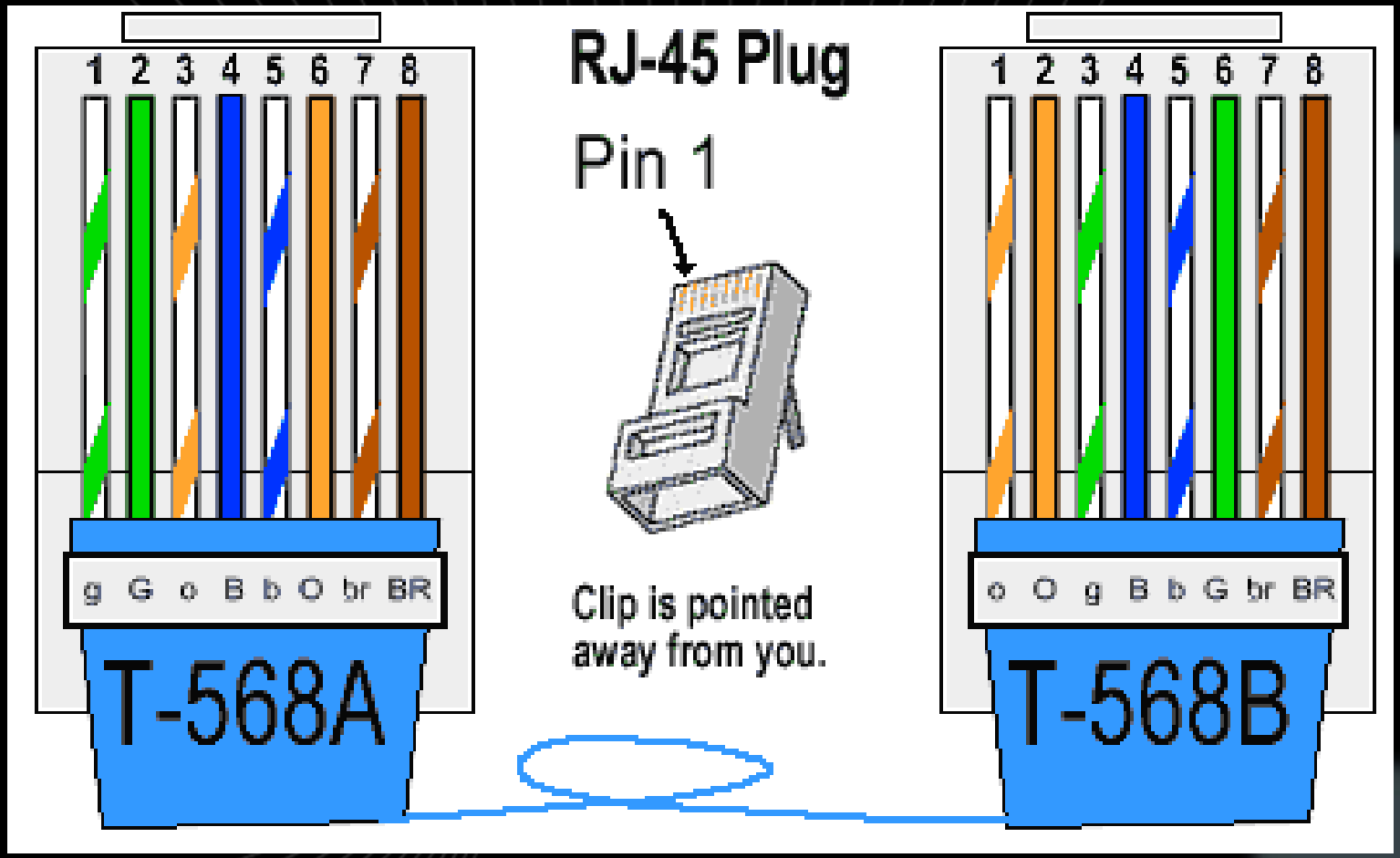


# Kỹ Thuật Bấm Cáp

- **Cáp chéo (Crossover)**
  - Là cáp để nối giữa 2 thiết bị giống nhau: PC-PC, Hub-Hub, Switch-Switch…
  - Theo chuẩn 10/100Based-T

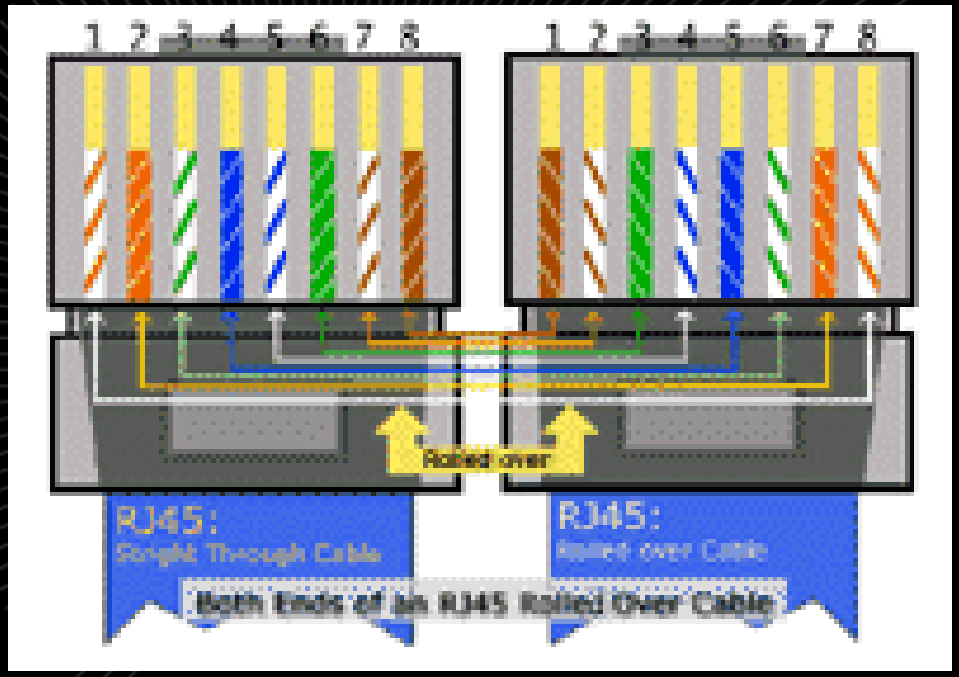


# Kỹ Thuật Bấm Cáp



# Kỹ Thuật Bấm Cáp

- **Cáp Console**
  - Là cáp dùng để nối từ PC vào các thiết bị mạng, chủ yếu dùng để cấu hình các thiết bị: Switch, Router…



# Kỹ Thuật Bấm Cáp

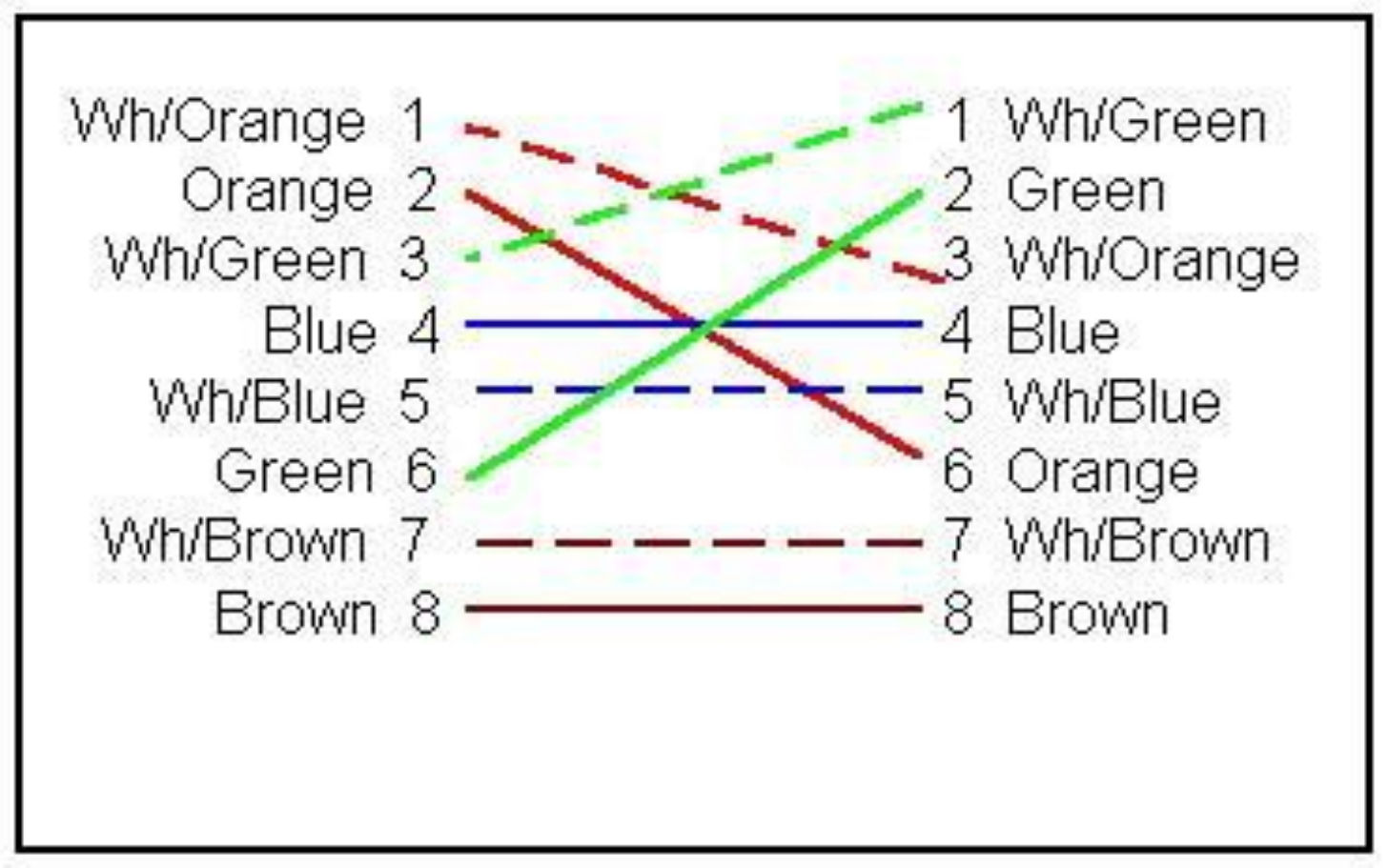
- Sử dụng thiết bị Test cáp:

# Kỹ Thuật Bấm Cáp

- Test cáp thẳng (Straight-through)

# Kỹ Thuật Bấm Cáp

- Test cáp chéo (Crossorve)



LOGO

# CÁC THIẾT BỊ LIÊN KẾT MẠNG

# CÁC THIẾT BỊ LIÊN KẾT MẠNG

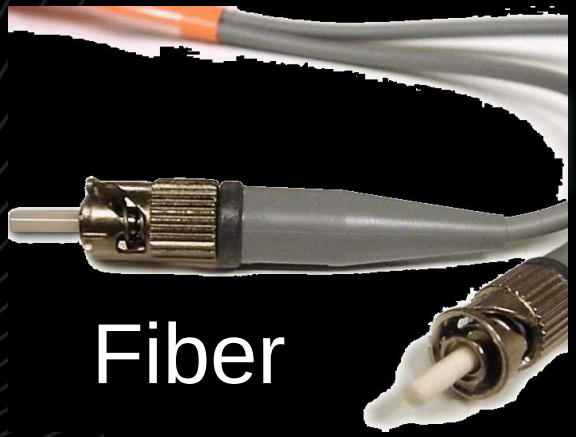
1. Dây cáp mạng - Cable
2. Vi mạch mạng - NIC
3. Bộ lặp – Repeater
4. Bộ tập trung – Hub
5. Cầu nối – Bridge
6. Bộ chuyển mạch – Switch
7. Bộ tìm đường – Router
8. Cổng kết nối – Gateway

# CÁC THIẾT BỊ LIÊN KẾT MẠNG

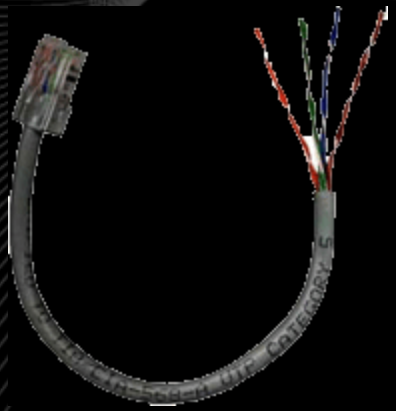
1. *Dây cáp mạng - Cable*
2. Vi mạch mạng - NIC
3. Bộ lặp – Repeater
4. Bộ tập trung – Hub
5. Cầu nối – Bridge
6. Bộ chuyển mạch – Switch
7. Bộ tìm đường – Router
8. Cổng kết nối – Gateway

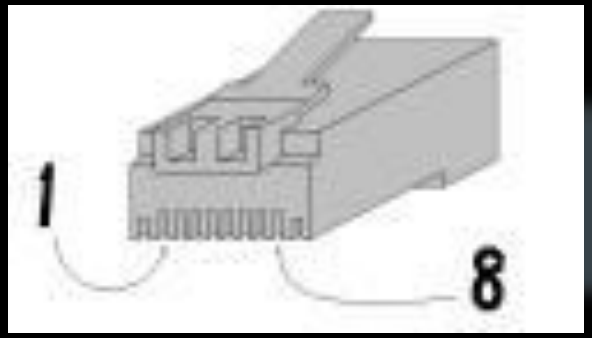
# *Dây cáp mạng - Cable*

Coaxial cable



Fiber



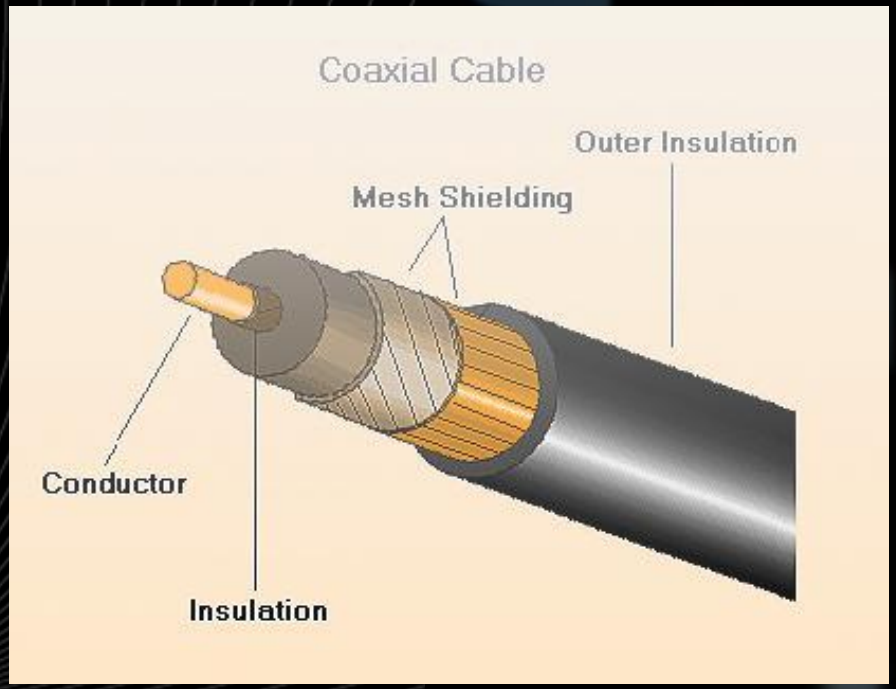


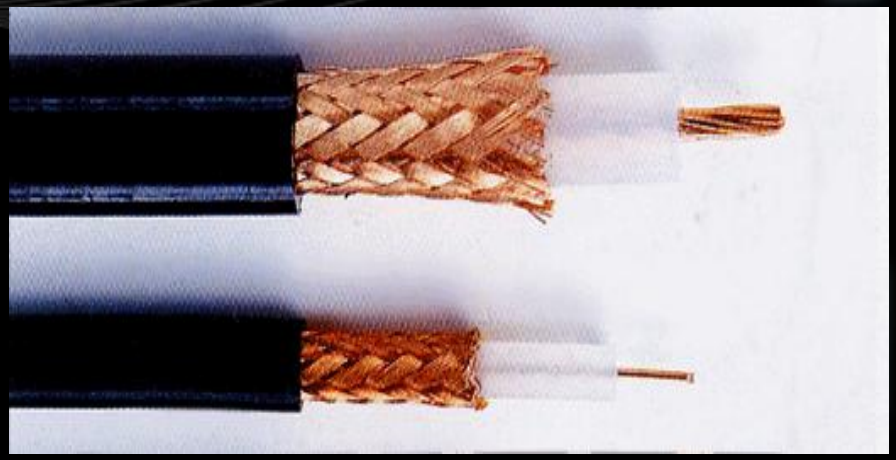
# Chuẩn cáp Ethernet

- **Ethernet**
  - 10Base-T (100m, Unshielded Twisted Pair = UTP)
  - 10Base-2 (~200m, Coax)
  - 10Base-5 (500m, Coax)
  - 10Base-FL (2000m=2km, Multimode Fiber)
- **Fast Ethernet**
  - 100Base-TX (100m over CAT5 UTP)
  - 100Base-FX (2000m=2km over MM Fiber)
- **Gigabit Ethernet**
  - 1000Base-SX (300m over MM Fiber)
  - 1000Base-LX (550m over MM Fiber, 3000m over SM Fiber)

# *Cáp đồng trục (coaxial cable)*

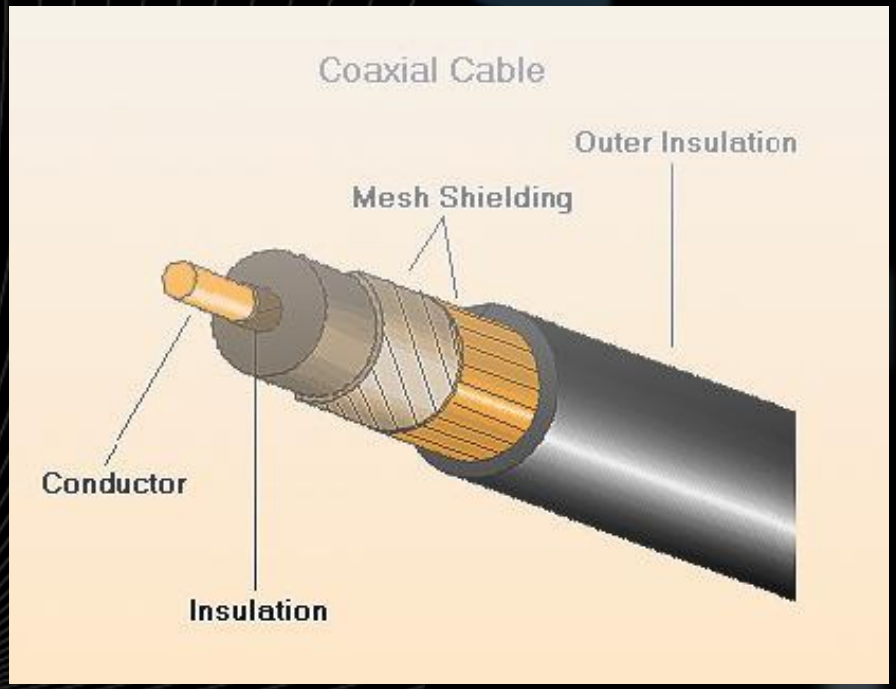
- Cáp đồng trục bao gồm một ống dẫn điện hình trụ tròn rỗng vây quanh một dây dẫn đơn bên trong, tạo thành 2 phần tử dẫn điện

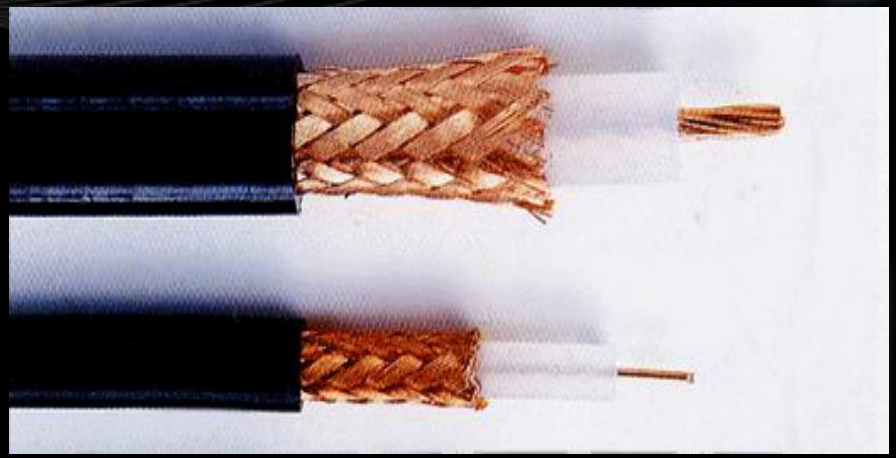


# *Cáp đồng trục (coxial cable)*

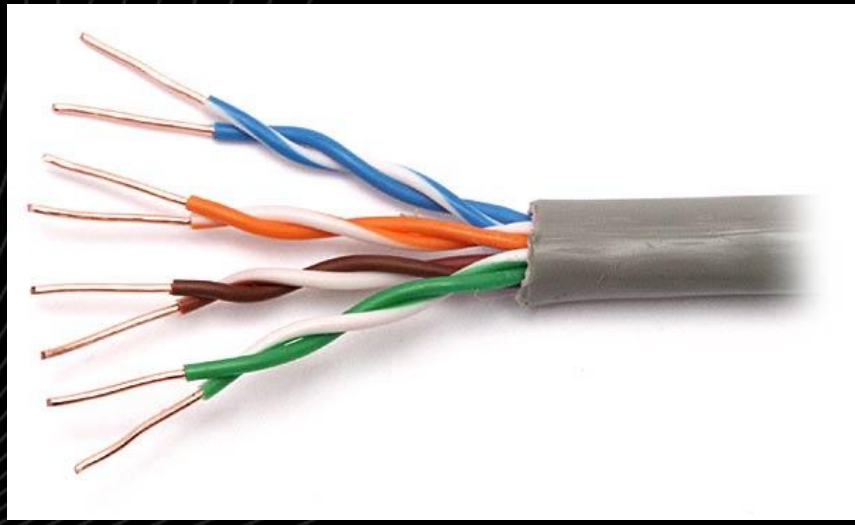
- Có độ ảnh hưởng nhiễu thấp.
- Có thể truyền tín hiệu với tốc độ cao
- Cho phép truyền với khoảng cách lớn hơn so với cáp xoắn đôi
- Có 2 loại: cáp gầy (thinnet) và cáp béo (thicknet).



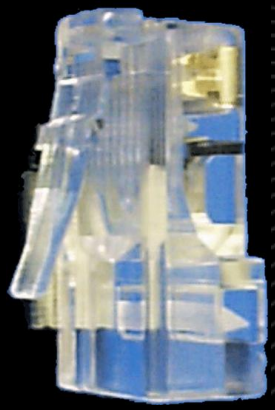
# Cáp không có vỏ bọc chống nhiễu – UTP (Cáp xoắn đôi trần)

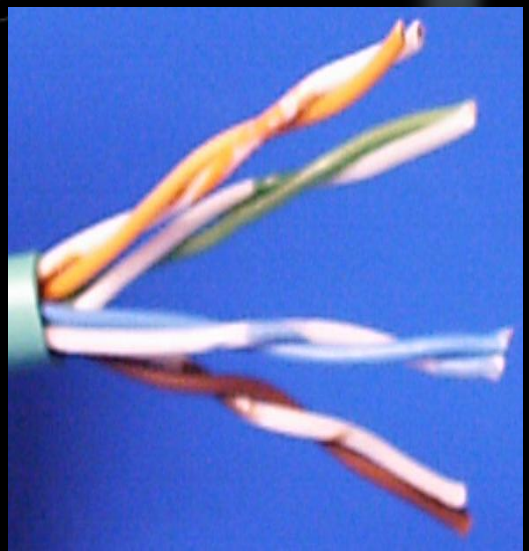
- Gồm 8 dây đồng tách biệt được bọc cách điện với các màu khác nhau
- Mỗi cặp 2 dây xoắn nhau từng đôi một để hạn chế sự thoái hóa tín hiệu
- Cáp xoắn đôi dùng giắc cắm RJ45.



# Cáp không có vỏ bọc chống nhiễu - UTP

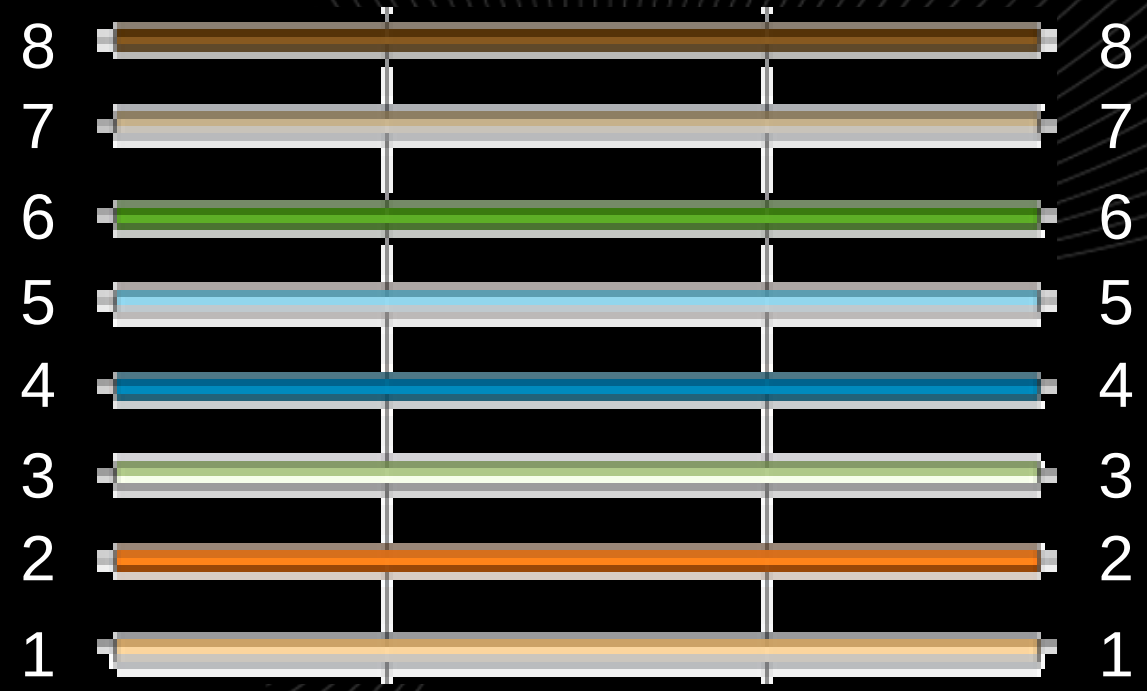
- Dễ dàng lắp đặt và rẻ tiền hơn so với các loại đường truyền khác
- Kích thước nhỏ, chiếm ít diện tích
- Cáp UTP dễ bị ảnh hưởng bởi tạp âm và xuyên nhiễu hơn các loại khác
- Khoảng cách truyền tín hiệu ngắn hơn so với cáp đồng trục hay cáp quang





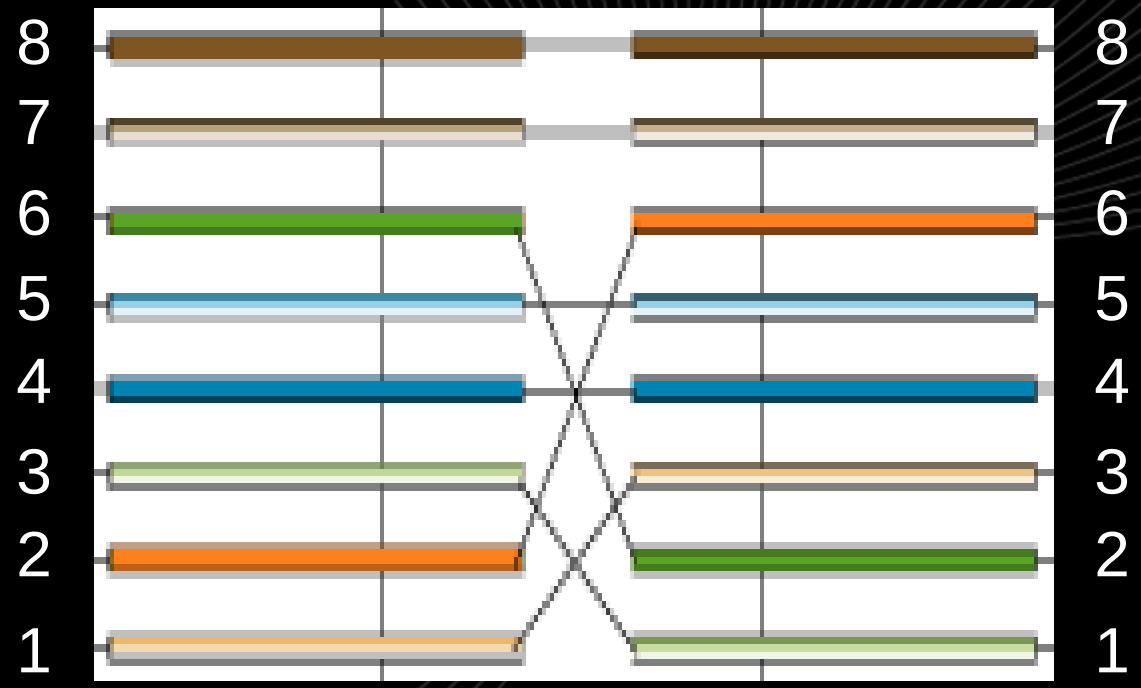
# Qui ước đấu cáp MDI

- **Cáp thẳng (straight): PC-switch, switch-router, PC-hub.**



# Qui ước đấu cáp MDI-X

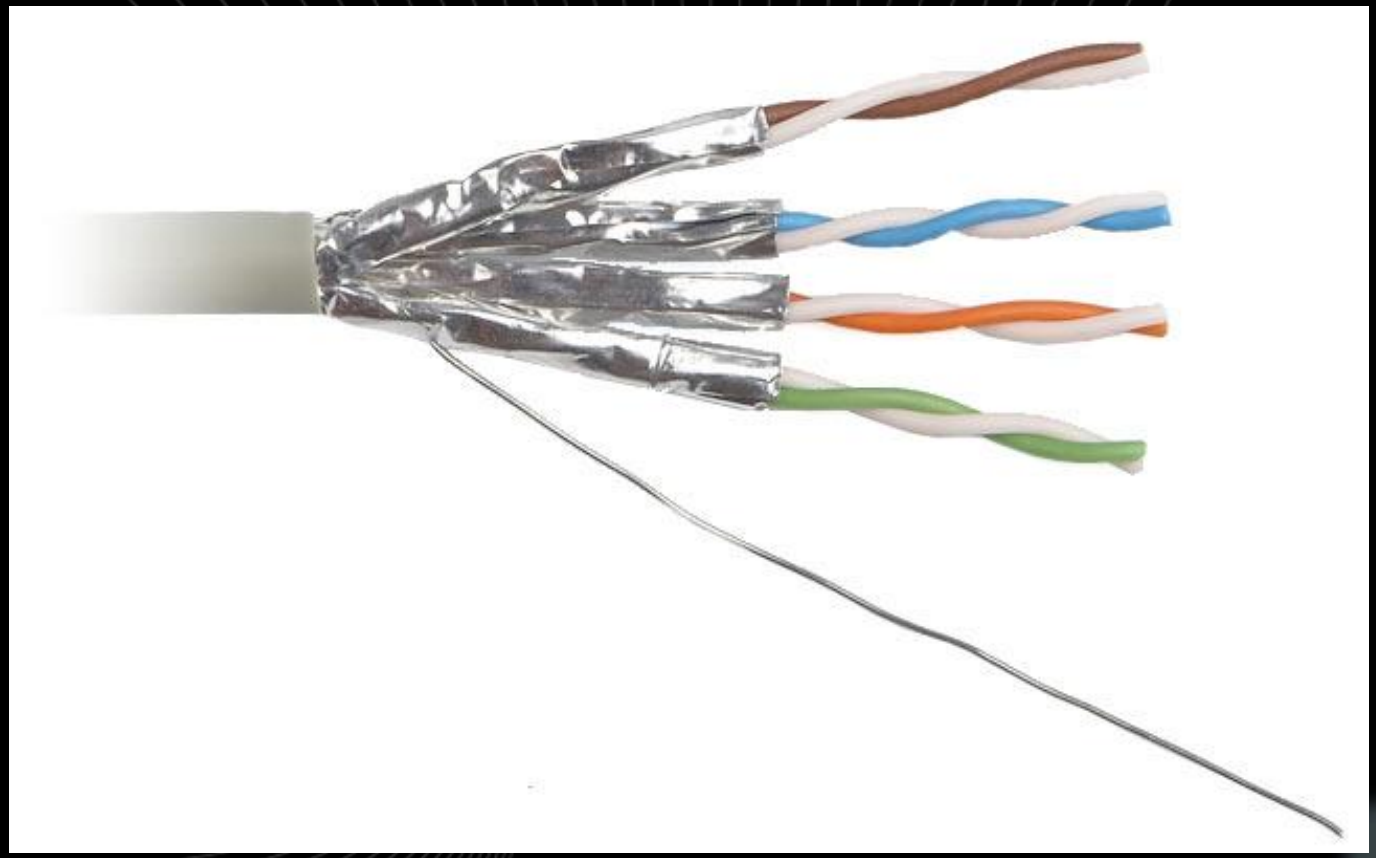
- **Cáp chéo (crossover): nối các thiết bị hub-switch, hub-hub, switch-switch, router-router, router-PC, PC-PC.**



***QuickGuide***

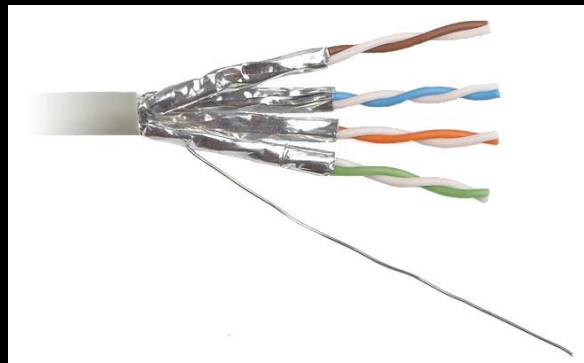
1-3, 2-6

# Cáp có vỏ bọc chống nhiễu-STP



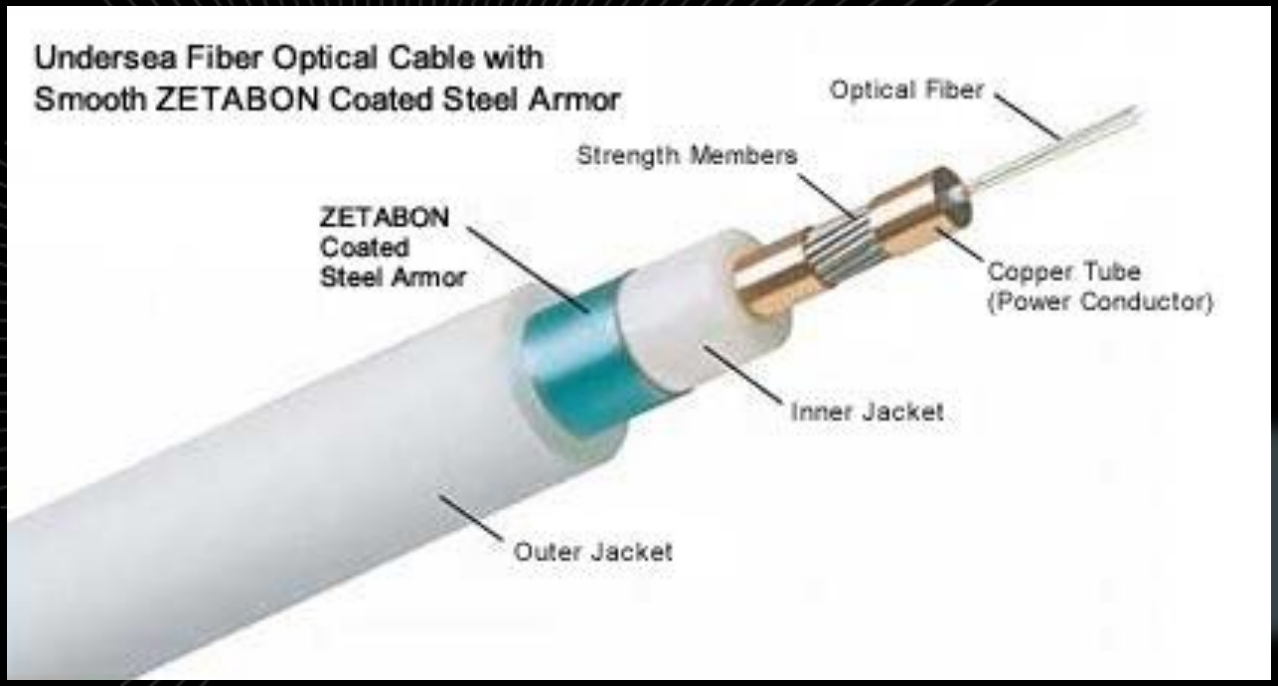
# Cáp có vỏ bọc chống nhiễu-STP

- Gồm 8 cặp xoắn với nhau từng đôi một (như cáp UTP)
- Mỗi cặp dây được bọc trong một lá kim loại
- Giảm nhiễu điện giữa các cặp dây và nhiễu xuyên âm
- Truyền dữ liệu ở tốc độ cao hơn trên khoảng cách lớn hơn loại UTP
- Chi phí cao hơn và khó khăn trong việc lắp đặt so với cáp UTP



# Cáp quang

- Truyền tín hiệu dữ liệu dưới dạng số ở hình thái xung ánh sáng.
- Cáp này không bị ảnh hưởng nhiễu điện.
- Có khả năng truyền tốc độ rất lớn (hàng trăm đến hàng nghìn Mbps).

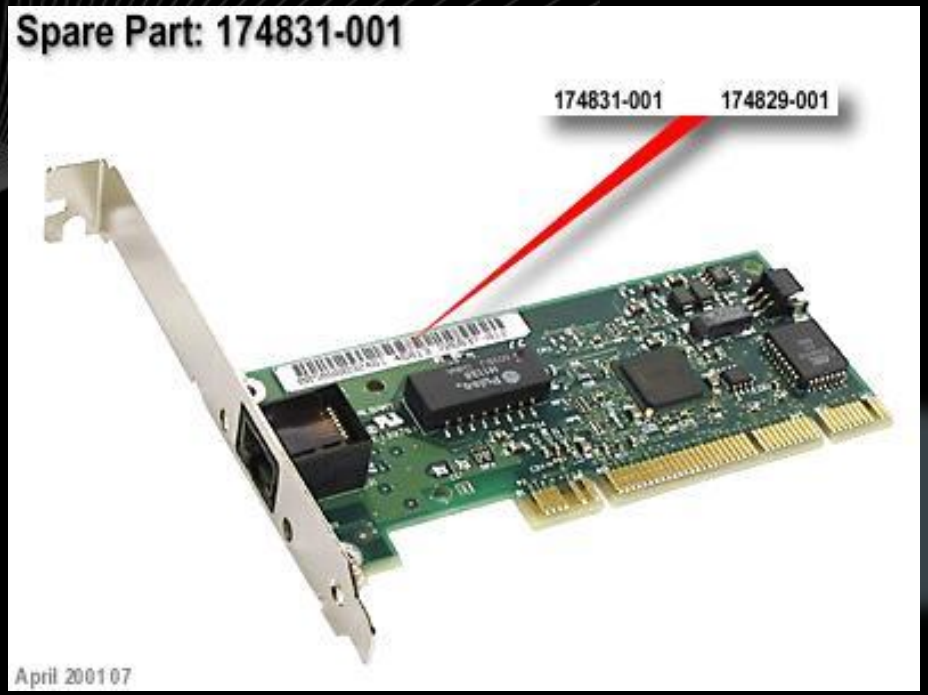


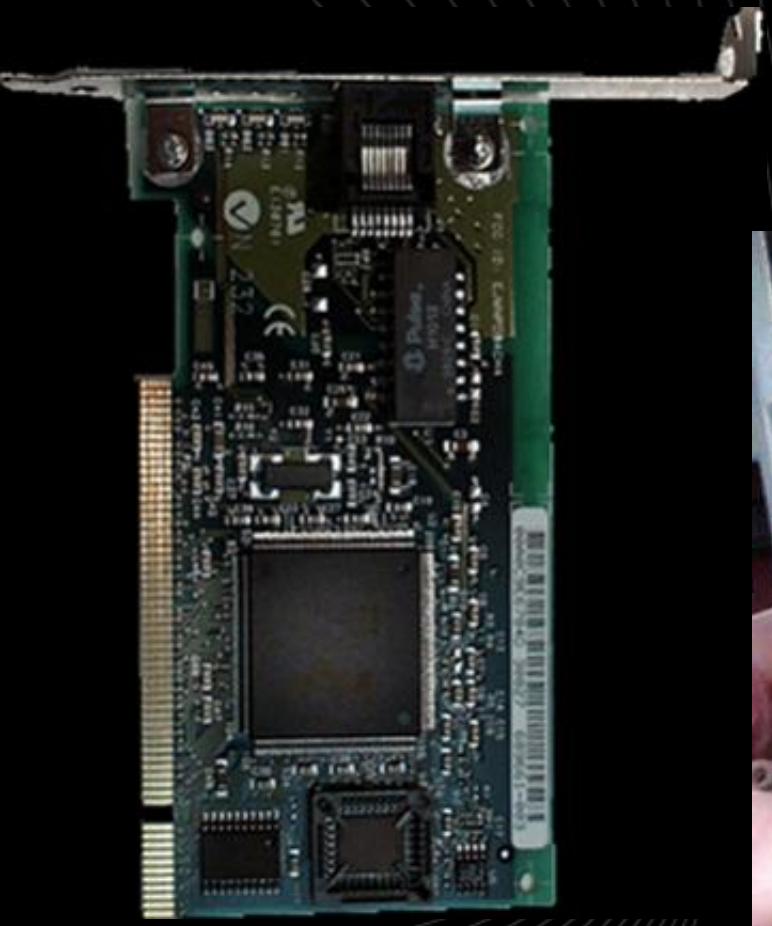
# CÁC THIẾT BỊ LIÊN KẾT MẠNG

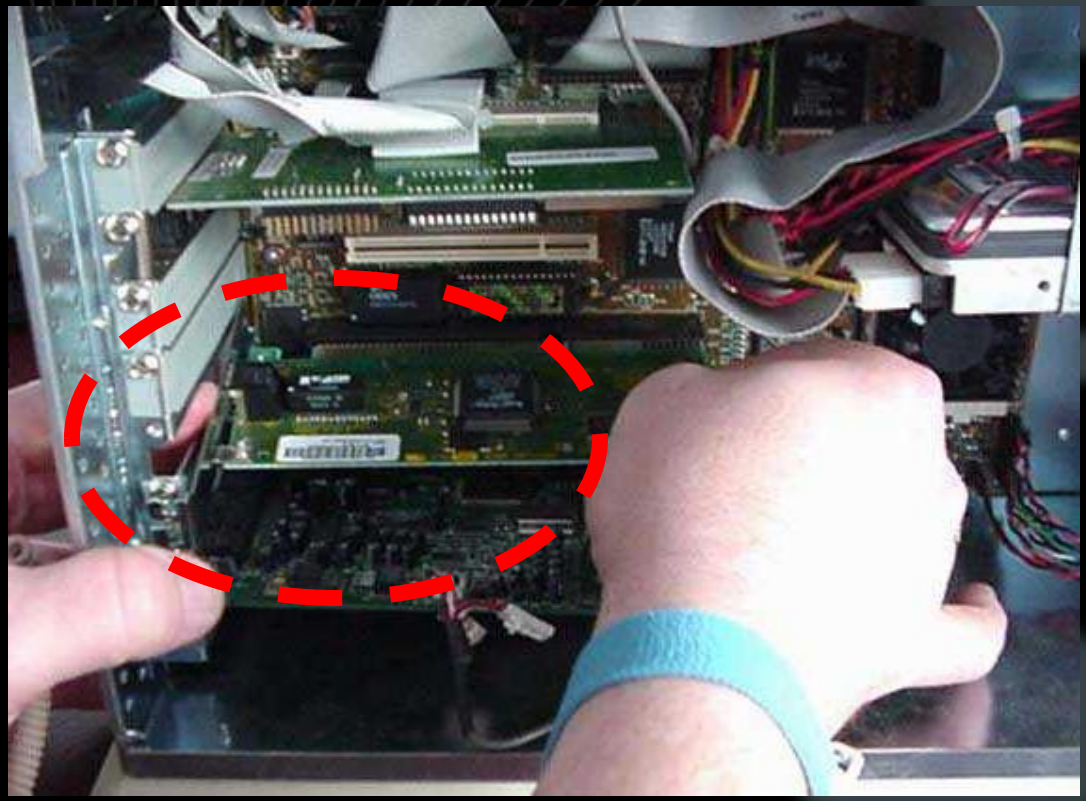
1. Dây cáp mạng - Cable
2. *Vi mạch mạng - NIC*
3. Bộ lặp – Repeater
4. Bộ tập trung – Hub
5. Cầu nối – Bridge
6. Bộ chuyển mạch – Switch
7. Bộ tìm đường – Router
8. Cổng kết nối – Gateway

# Card mạng - NIC

- Kết nối máy tính vào mạng.
- Cung cấp địa chỉ MAC trong các lần kết nối.
- Truyền dữ liệu từ bus dữ liệu của một nút tới một nút khác trong mạng.
- Gởi dữ liệu đến nút mạng khác.
- Kiểm soát luồng dữ liệu giữa máy tính và hệ thống cáp.

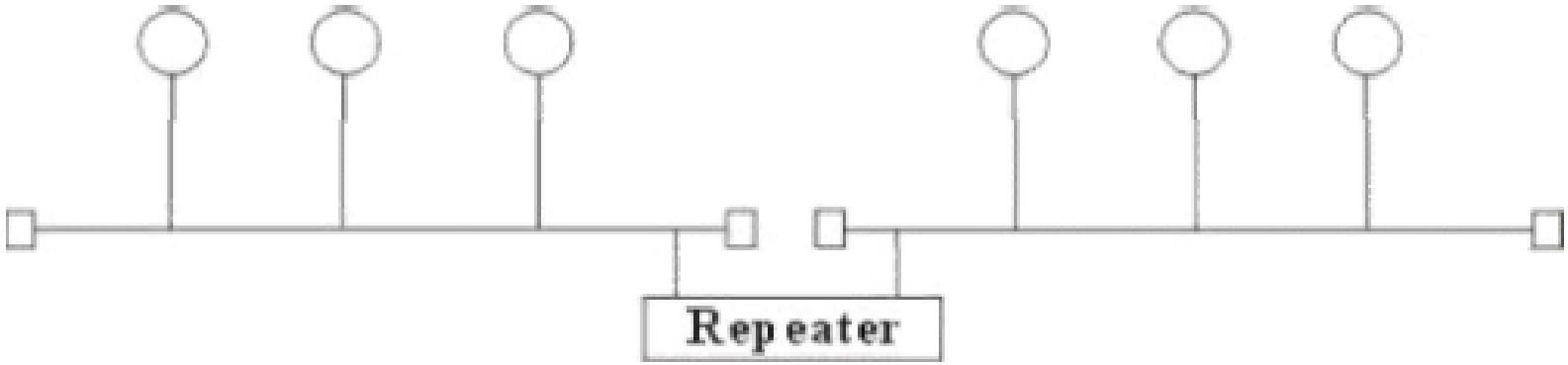






# CÁC THIẾT BỊ LIÊN KẾT MẠNG

1. Dây cáp mạng - Cable
2. Vi mạch mạng - NIC
3. *Bộ lặp – Repeater*
4. Bộ tập trung – Hub
5. Cầu nối – Bridge
6. Bộ chuyển mạch – Switch
7. Bộ tìm đường – Router
8. Cổng kết nối – Gateway




*Hình 2-8:* ***Mô hình liên kết mạng của Repeater.***

# Bộ lặp – Repeater

- **Repeater (Layer 1 - Physical)**
  - UTPCat5 ~100m ⇒ cần thiết bị khuếch đại tín hiệu khi nối xa hơn 100m
  - Chỉ có 2 port: 1 in 1 out
- **Không có xử lý tín hiệu.**
- **Loại bỏ các tín hiệu méo, nhiễu, khuếch đại tín hiệu đã bị suy hao.**
- **Có 2 loại: Repeater điện và Repeater điện quang.**
- **Nối hai mạng có cùng giao thức truyền thông**

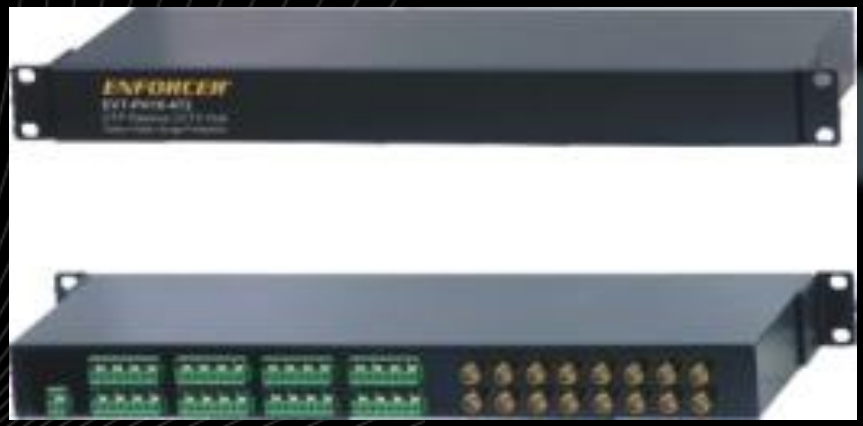
FiberExtender Repeater
CELTEC S.A.
INTERFAZ 1
LOS
BUCLE
PLL
INTERFAZ 2
LOS
BUCLE
PLL
uP READY
LINK
POWER ON
RTC
RS232

# CÁC THIẾT BỊ LIÊN KẾT MẠNG

1. Dây cáp mạng - Cable
2. Vi mạch mạng - NIC
3. Bộ lặp – Repeater
4. *Bộ tập trung – Hub*
5. Cầu nối – Bridge
6. Bộ chuyển mạch – Switch
7. Bộ tìm đường – Router
8. Cổng kết nối – Gateway

# Bộ tập trung - HUB

- Còn gọi là multi-port repeater.



- Hub được coi là một Repeater có nhiều cổng. Một Hub có từ 4 đến 24 cổng và có thể còn nhiều hơn.
- Khi cấu hình mạng là hình sao (*Star topology*), Hub đóng vai trò là trung tâm của mạng.
- Với một Hub, khi thông tin vào từ một cổng và sẽ được đưa đến tất cả các cổng khác.

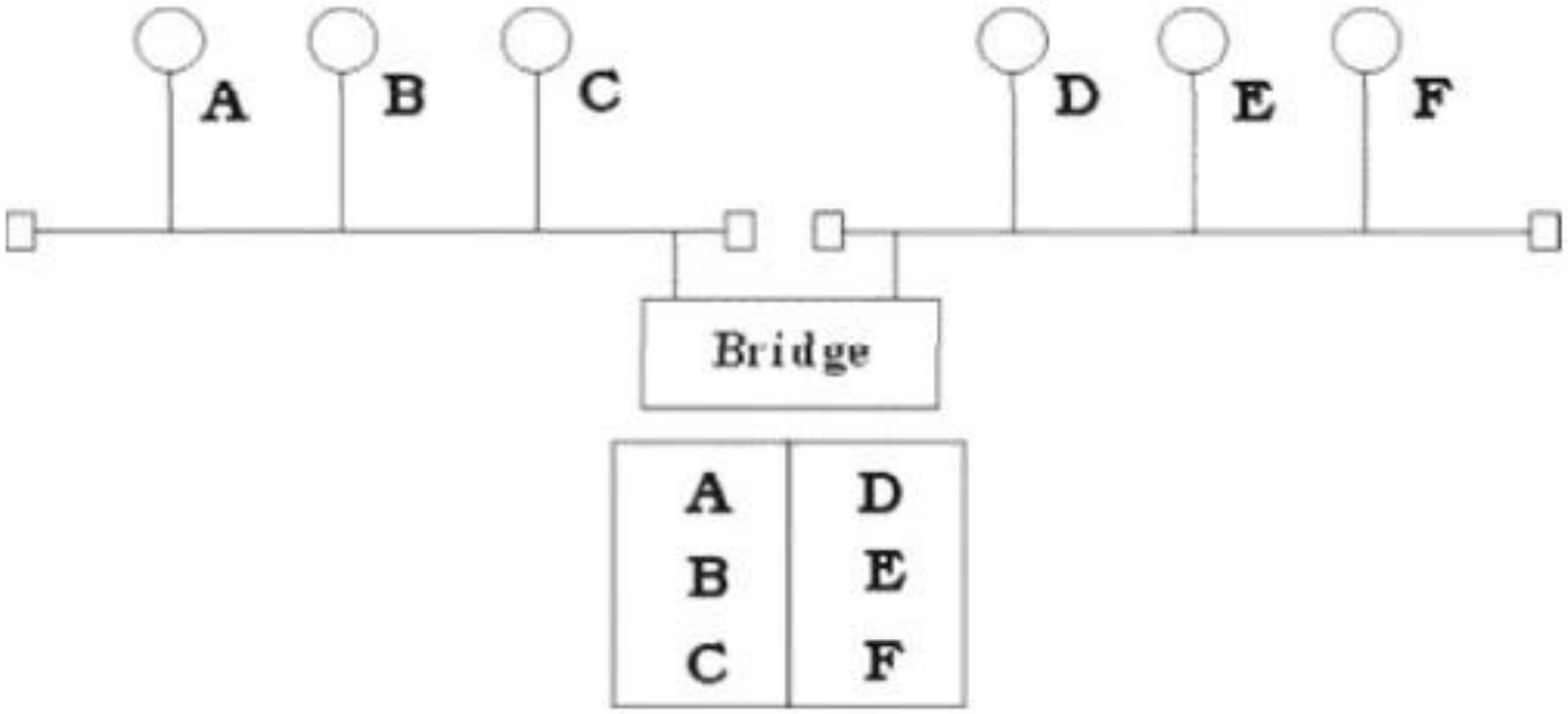
## Bộ tập trung - HUB

- **Còn gọi là multi-port repeater.**
- **Có 3 loại:**
  - Hub bị động (Passive Hub) : không chứa các linh kiện điện tử và cũng không xử lý các tín hiệu dữ liệu, nó có chức năng duy nhất là tổ hợp các tín hiệu từ một số đoạn cáp mạng
  - Hub chủ động (Active Hub) : có thể khuyếch đại và xử lý các tín hiệu điện tử truyền giữa các thiết bị của mạng (tái sinh tín hiệu) → khoảng cách giữa các thiết bị có thể tăng lên
  - Hub thông minh (Intelligent Hub): có thêm bộ nhớ và bộ vi xử lý để có thể hoạt động như bộ tìm đường

# CÁC THIẾT BỊ LIÊN KẾT MẠNG

1. Dây cáp mạng - Cable
2. Vi mạch mạng - NIC
3. Bộ lặp – Repeater
4. Bộ tập trung – Hub
5. *Cầu nối – Bridge*
6. Bộ chuyển mạch – Switch
7. Bộ tìm đường – Router
8. Cổng kết nối – Gateway

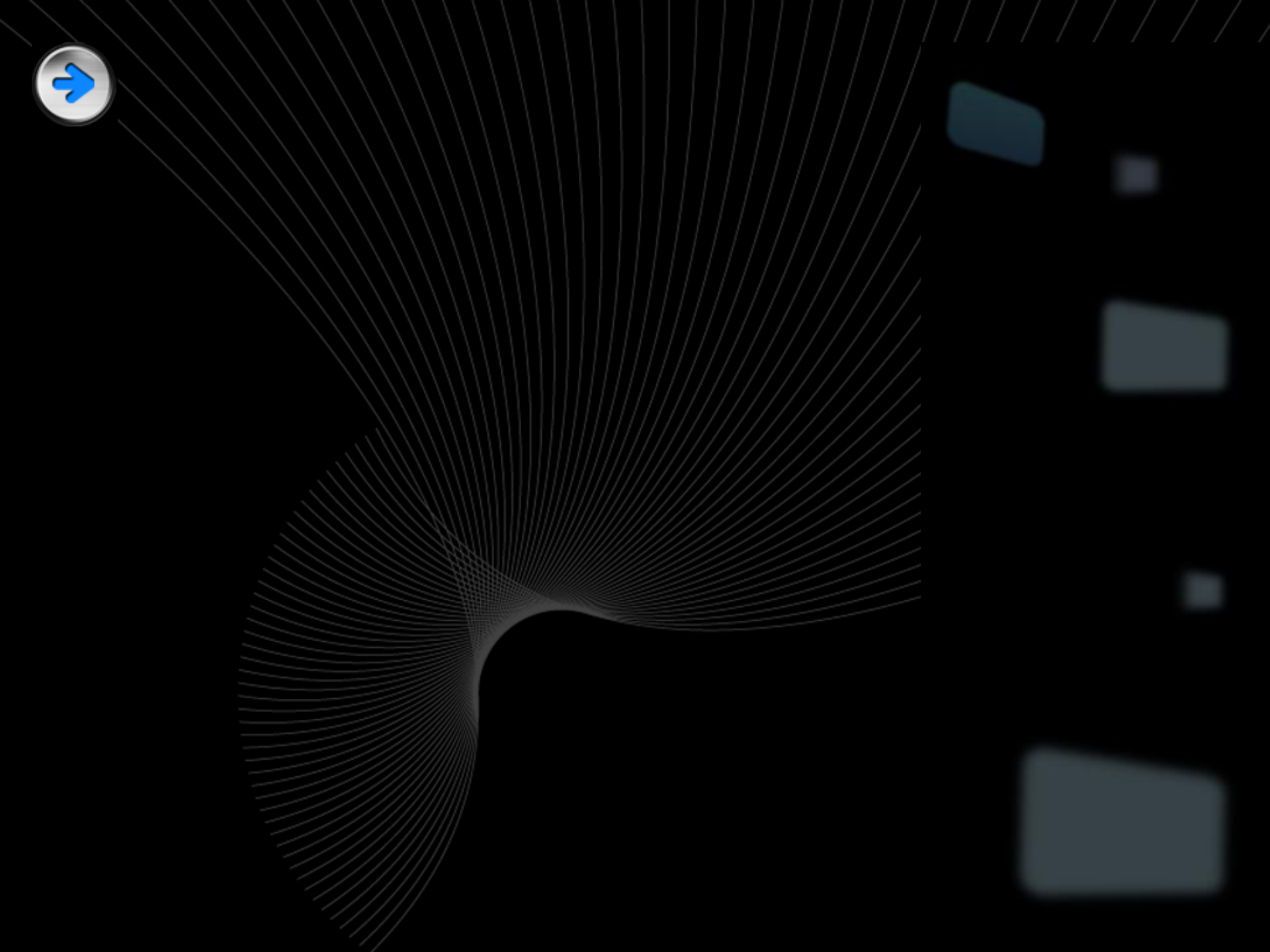
# Cầu nối - Bridge

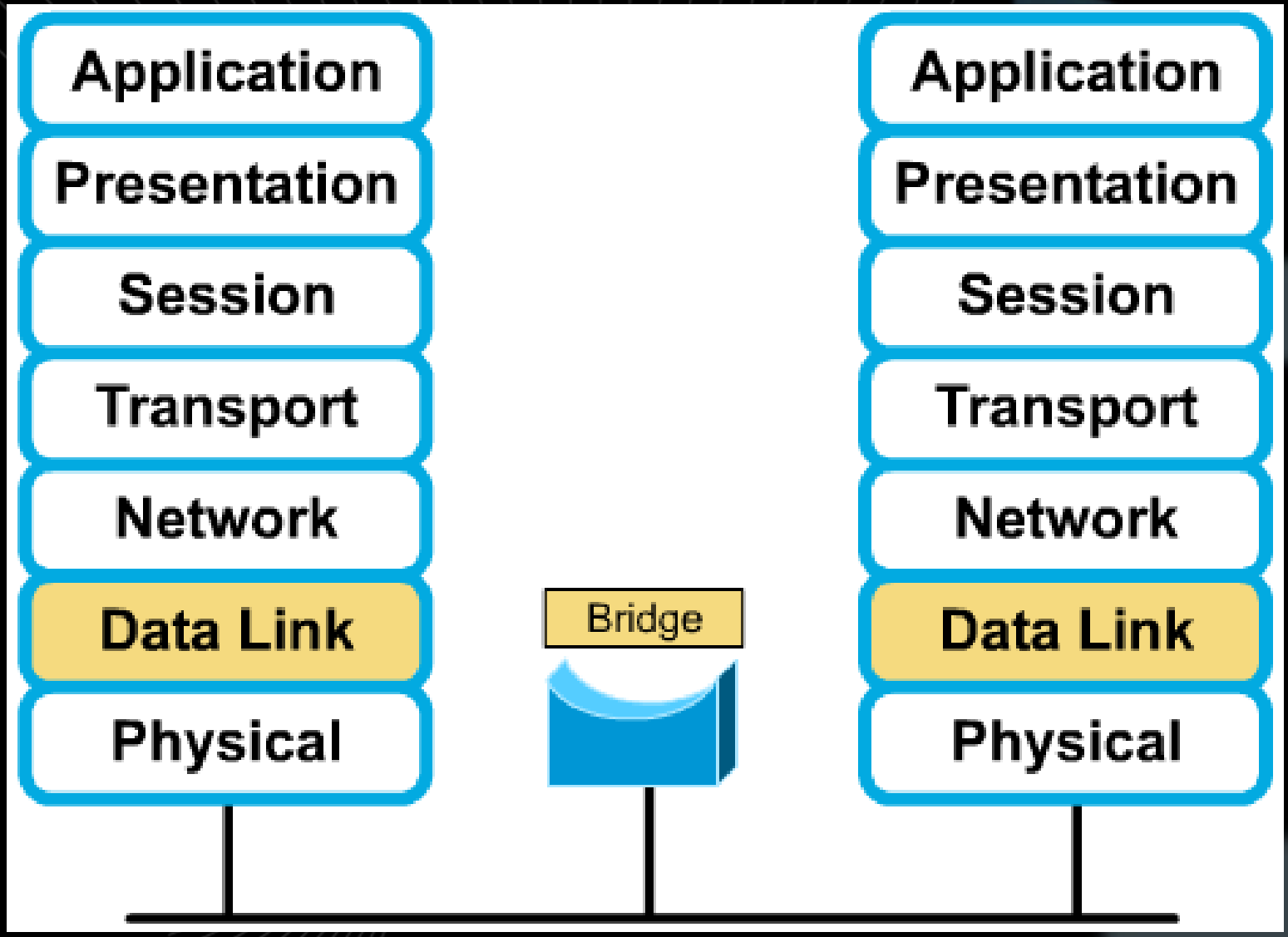



*Hình 2-11:* ***Hoạt động của Bridge***

# Cầu nối - Bridge

- Bridge là một thiết bị có xử lý dùng để nối hai mạng giống nhau hoặc khác nhau.
- Chuyển tiếp hoặc chặn các frame dựa trên địa chỉ MAC
- Cầu nối đọc các gói tin và xử lý chúng trước khi quyết định có chuyển đi hay không.



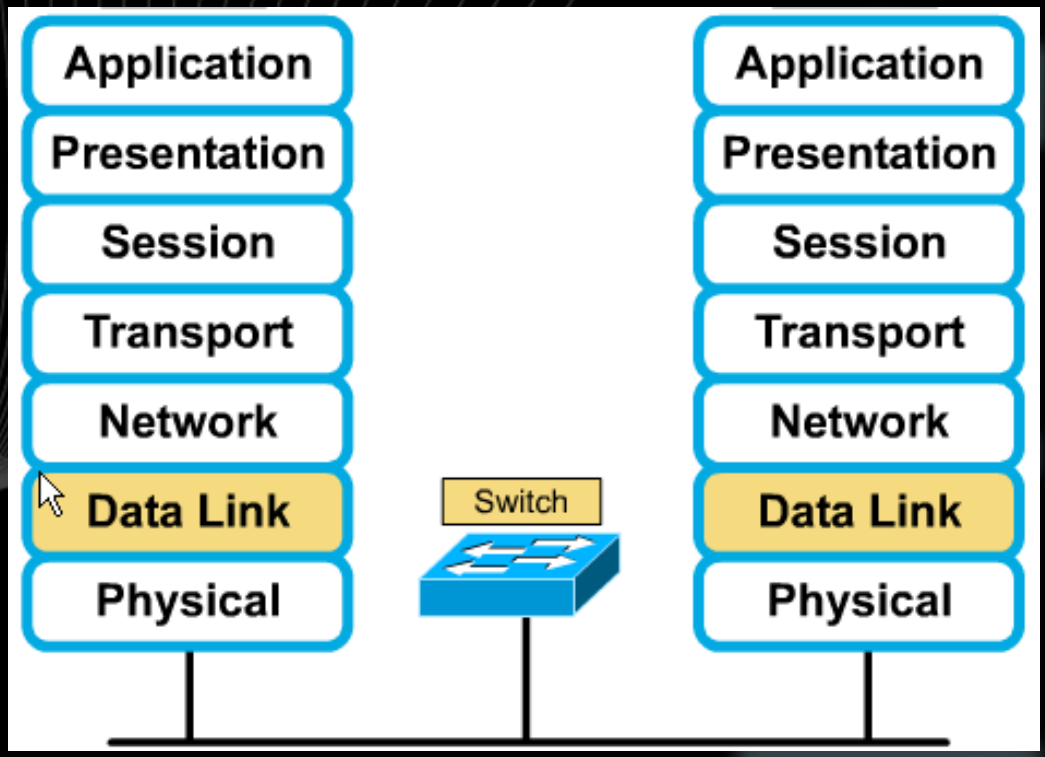

Application
Presentation
Session
Transport
Network
Data Link
Physical
Bridge
Application
Presentation
Session
Transport
Network
Data Link
Physical

# CÁC THIẾT BỊ LIÊN KẾT MẠNG

1. Dây cáp mạng - Cable
2. Vi mạch mạng - NIC
3. Bộ lặp – Repeater
4. Bộ tập trung – Hub
5. Cầu nối – Bridge
6. *Bộ chuyển mạch – Switch*
7. Bộ tìm đường – Router
8. Cổng kết nối – Gateway

# Bộ chuyển mạch – Switch

- Switch (Layer 2 - Data Link) là multi-port bridge



# SWITCH

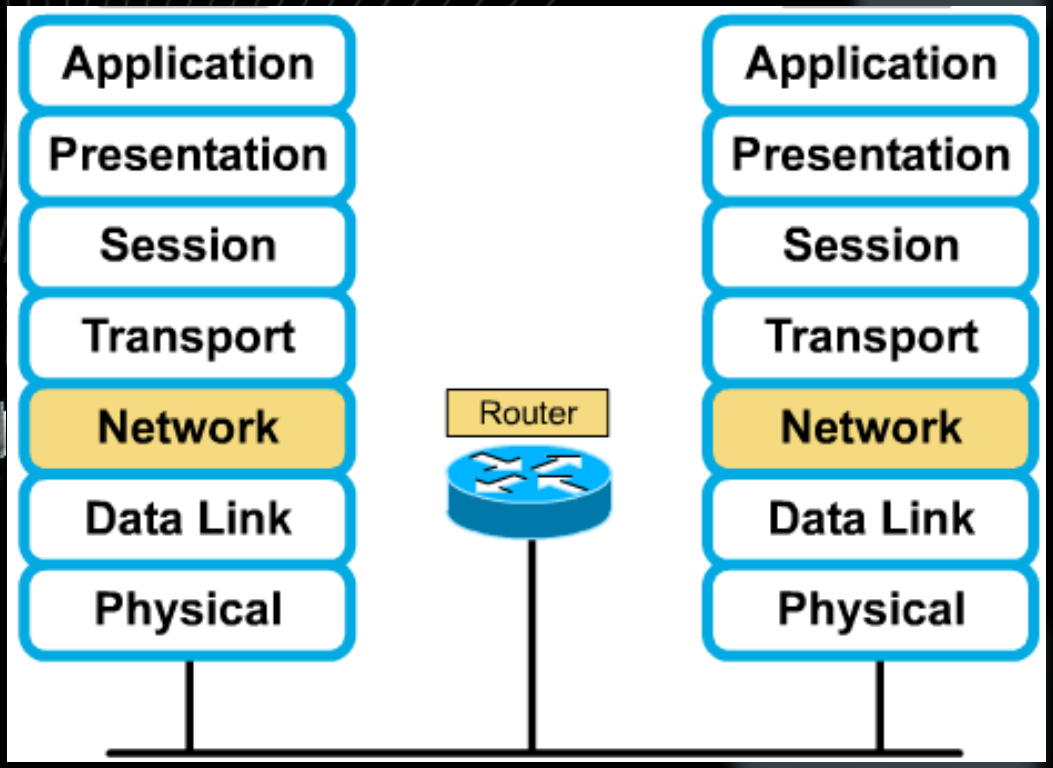
- Khác với HUB thông thường, thay vì chuyển một tín hiệu đến từ một cổng cho tất cả các cổng, nó chỉ chuyển tín hiệu đến cổng có trạm đích.
- Switch làm giảm đụng độ trên mạng
- Switch lưu lại bản ghi nhớ địa chỉ MAC của tất cả các thiết bị mà nó kết nối tới.
- Khi nhận được khung dữ liệu, switch sẽ biết đích xác cổng nào cần gửi tới, giúp tăng tối đa thời gian phản ứng của mạng.

# CÁC THIẾT BỊ LIÊN KẾT MẠNG

1. Dây cáp mạng - Cable
2. Vi mạch mạng - NIC
3. Bộ lặp – Repeater
4. Bộ tập trung – Hub
5. Cầu nối – Bridge
6. Bộ chuyển mạch – Switch
7. *Bộ tìm đường – Router*
8. Cổng kết nối – Gateway

# Bộ tìm đường – Router

- Router (Layer 3 – Network)



# Router

- Router thường được kết nối với ít nhất 2 mạng
- Router có thể tìm được đường đi tốt nhất cho các gói tin qua nhiều kết nối để đi từ trạm gửi thuộc mạng đầu đến trạm nhận thuộc mạng cuối.
- Router có thể được sử dụng trong việc nối nhiều mạng với nhau và cho phép các gói tin có thể đi theo nhiều đường khác nhau để tới đích

# CÁC THIẾT BỊ LIÊN KẾT MẠNG

1. Dây cáp mạng - Cable
2. Vi mạch mạng - NIC
3. Bộ lặp – Repeater
4. Bộ tập trung – Hub
5. Cầu nối – Bridge
6. Bộ chuyển mạch – Switch
7. Bộ tìm đường – Router
8. *Cổng kết nối – Gateway*

# Cổng nối – Gateway

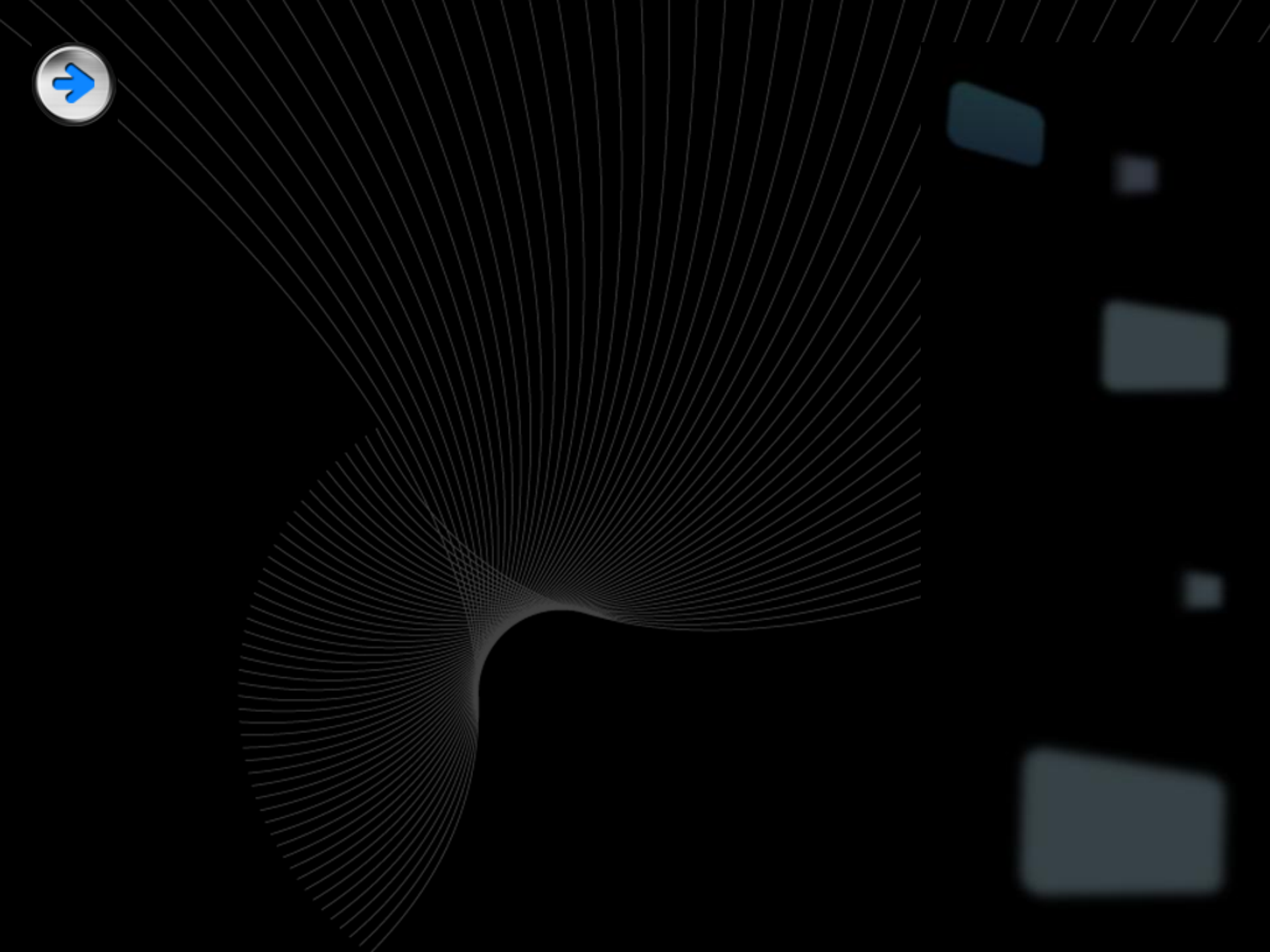
- Kết nối các mạng không thuần nhất.
- Một số cổng kết nối sử dụng toàn bộ 7 tầng của mô hình OSI

# CÁC GIAO THỨC TRUYỀN TRÊN MẠNG

## CHƯƠNG 3

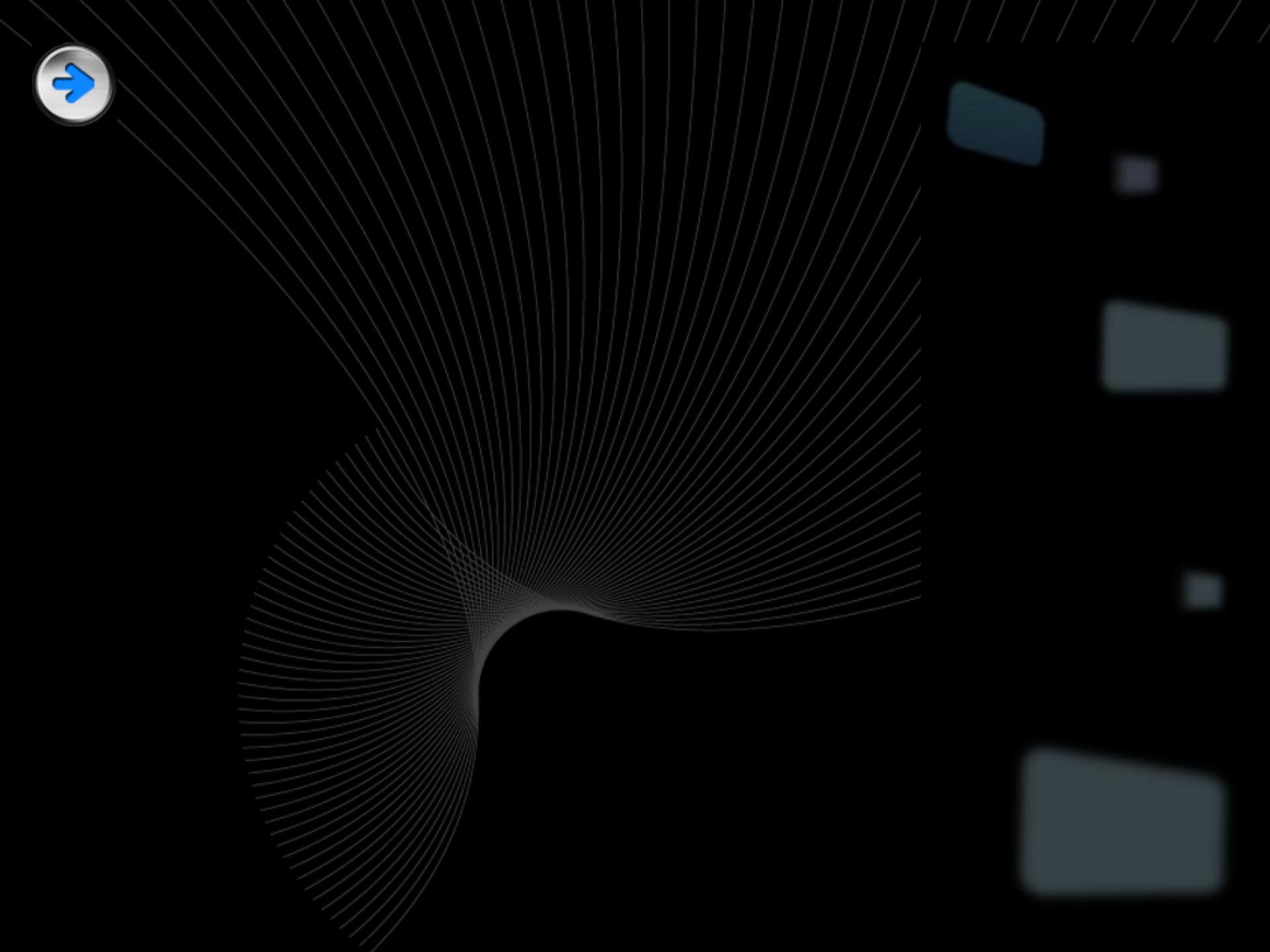
LOGO

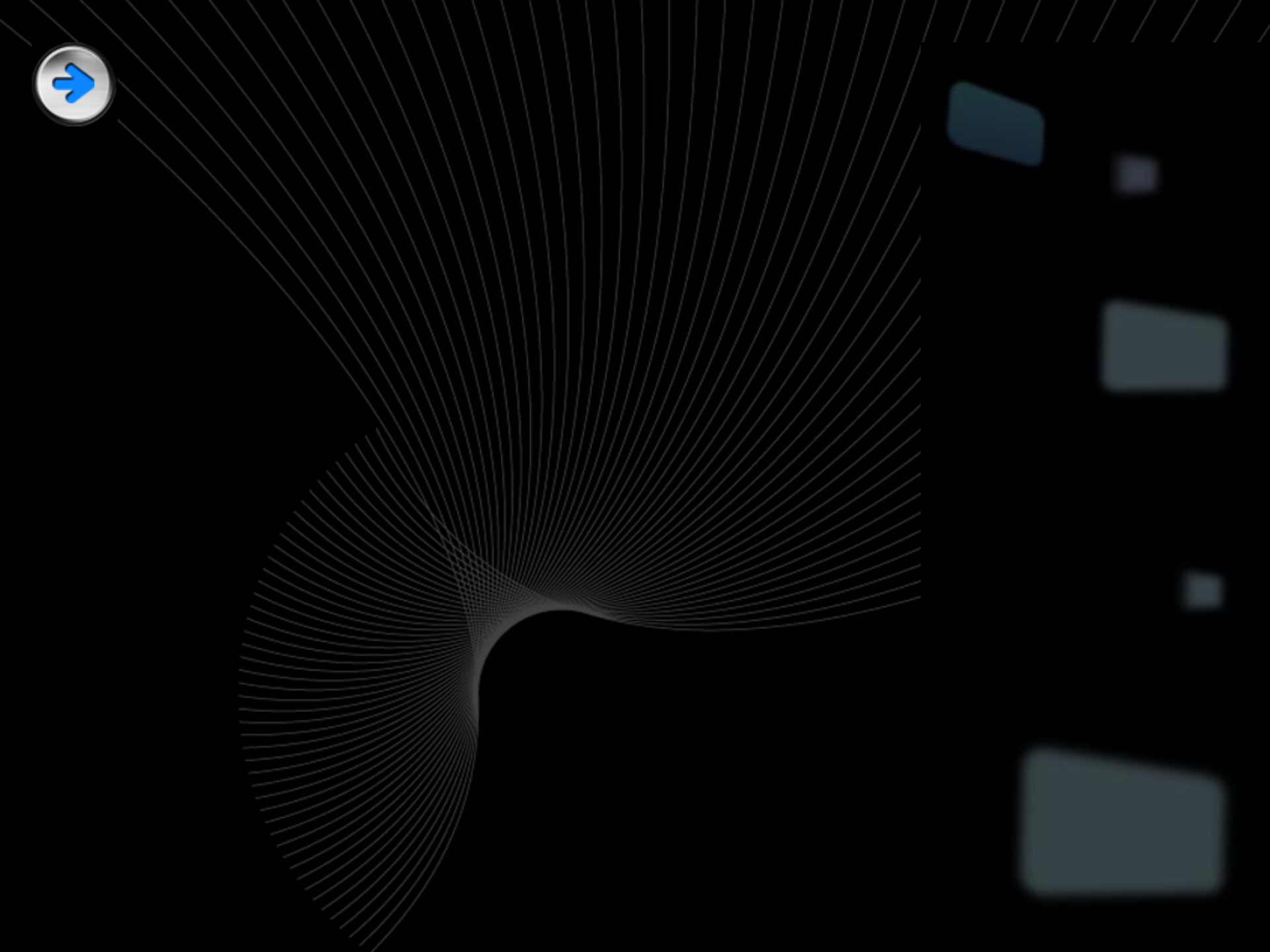
# ĐỊA CHỈ IP



LOGO

# ĐỊA CHỈ IP

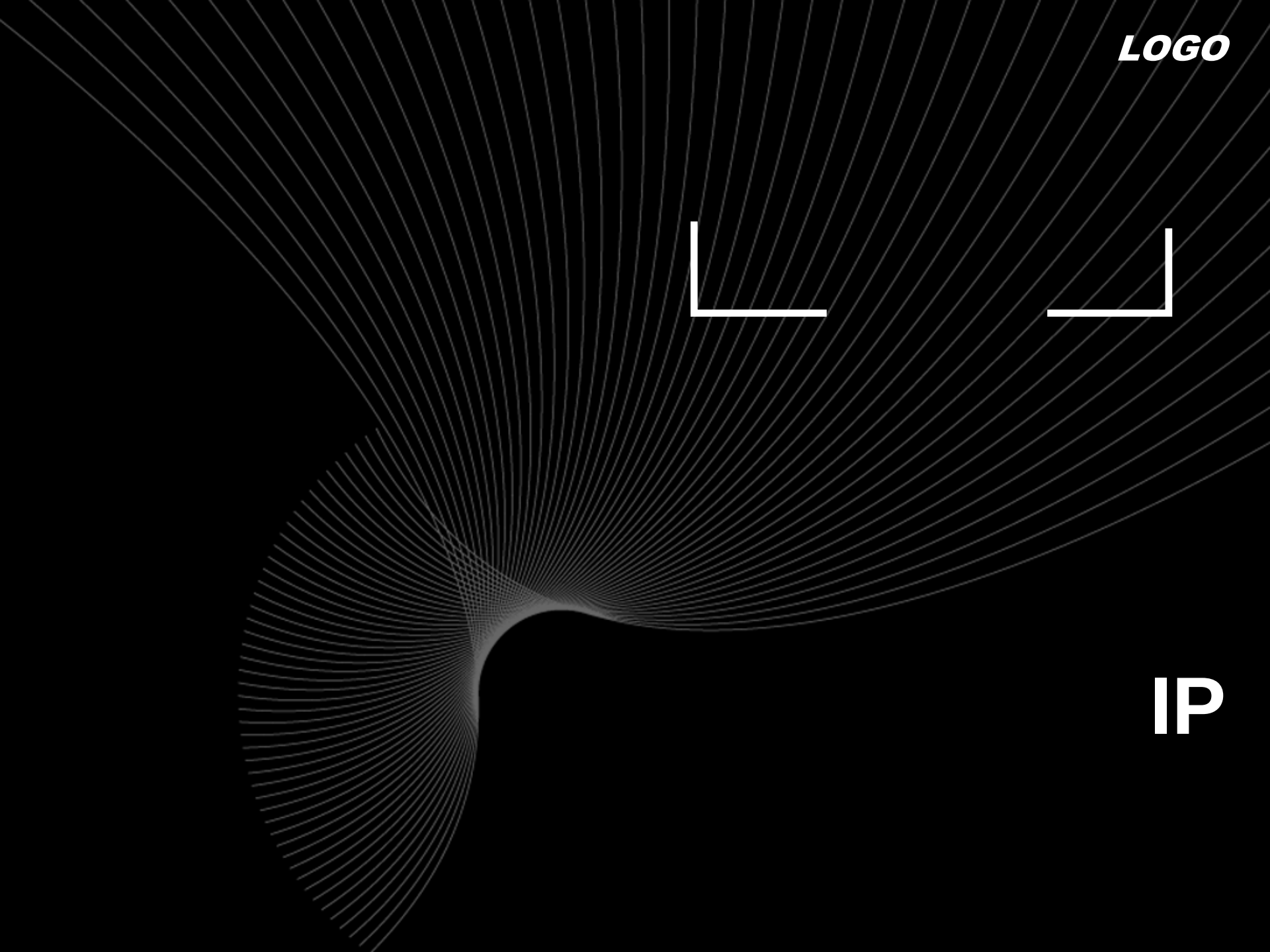




LOGO

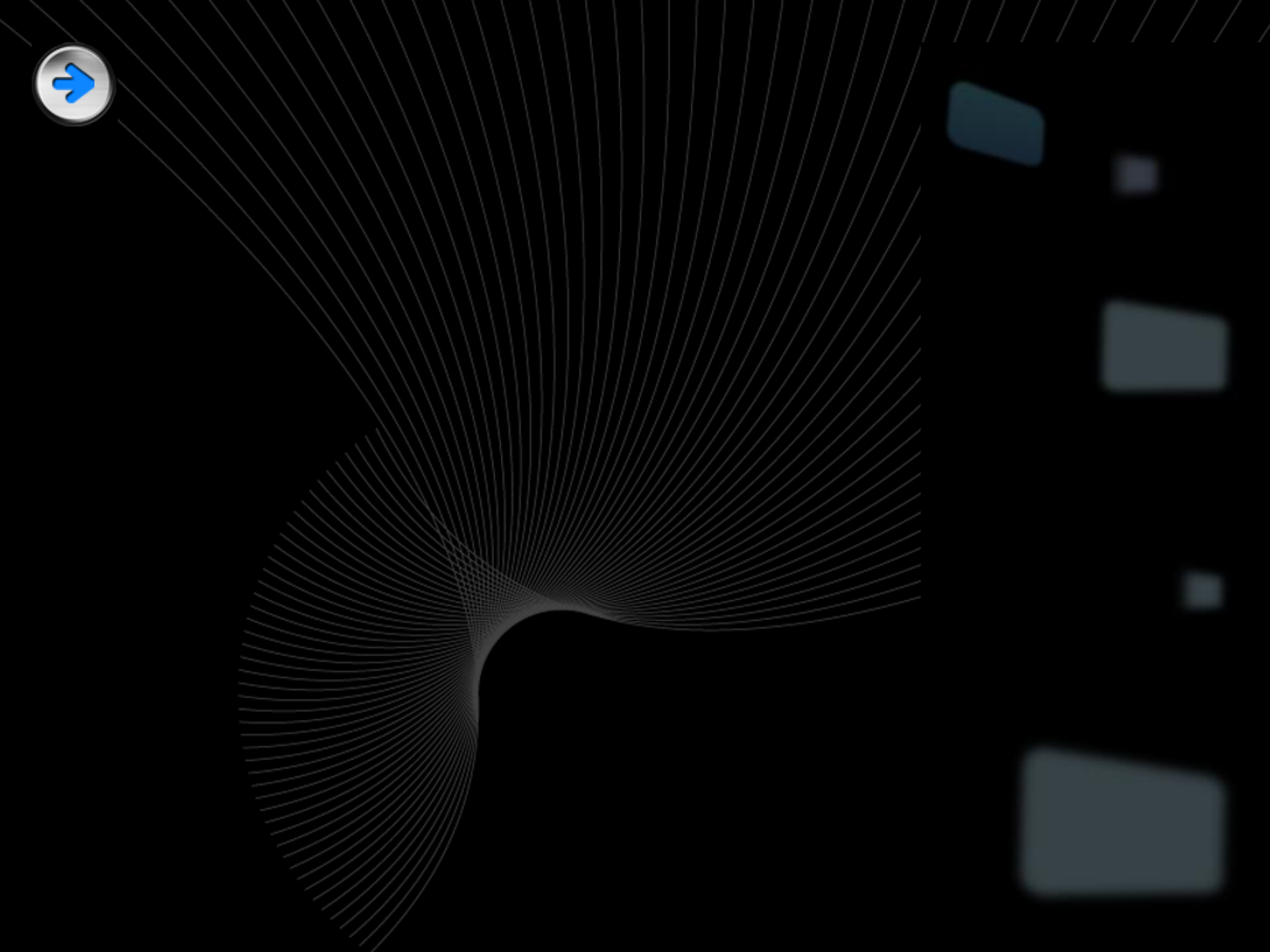
# CÁC THIẾT BỊ MẠNG

# CÁC THIẾT BỊ MẠNG

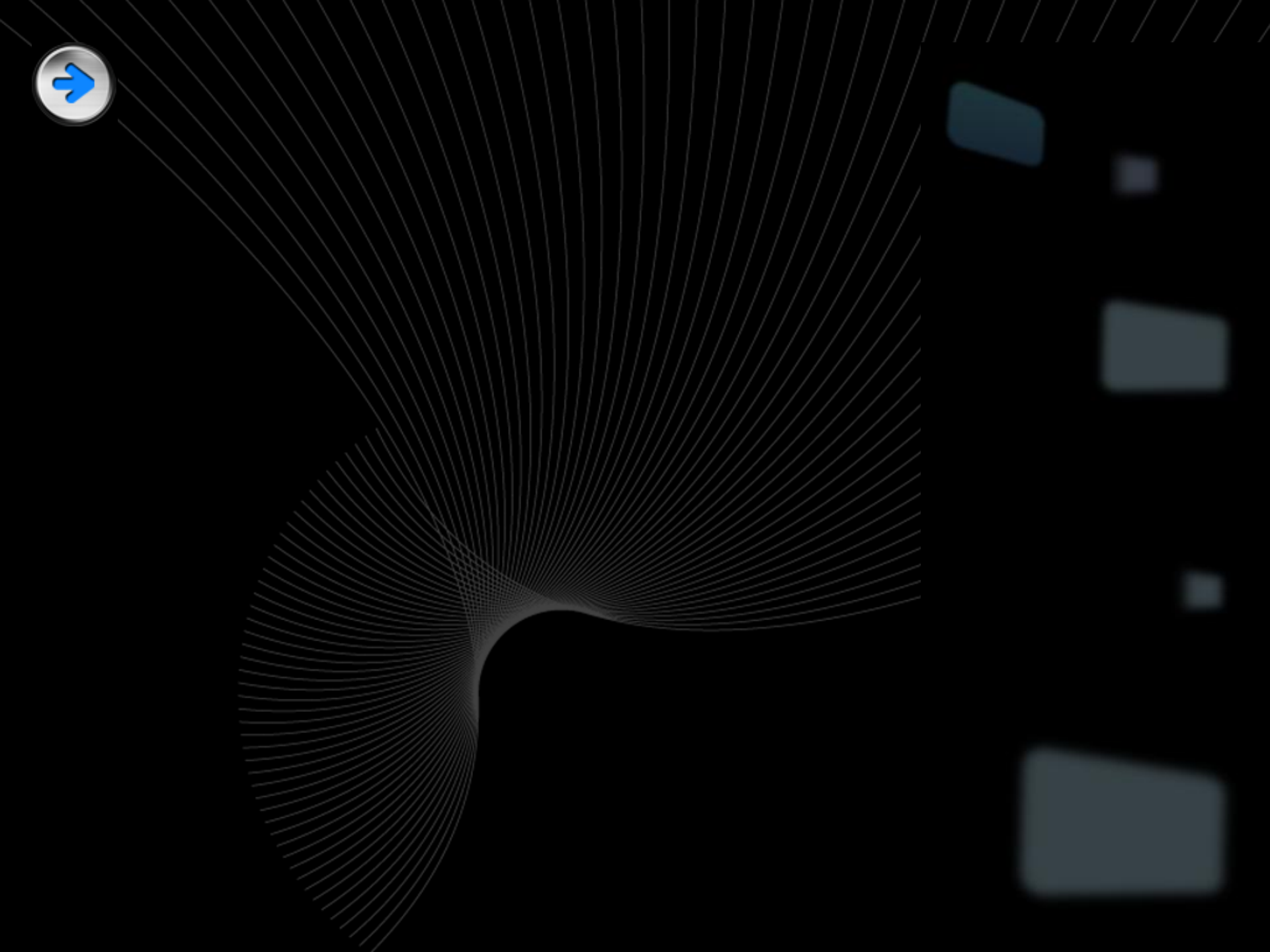

LOGO
IP

# CÁC THUẬT NGỮ

# MỘT SỐ PHÍM TẮT

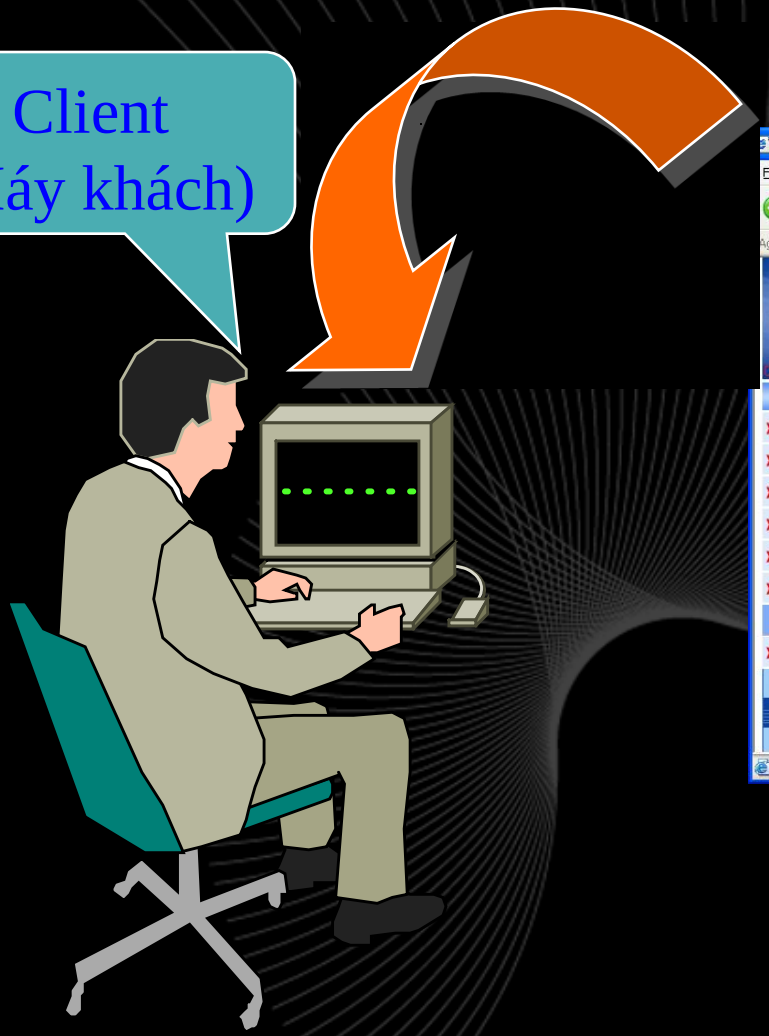


# Mô hình CLIENT/SERVER

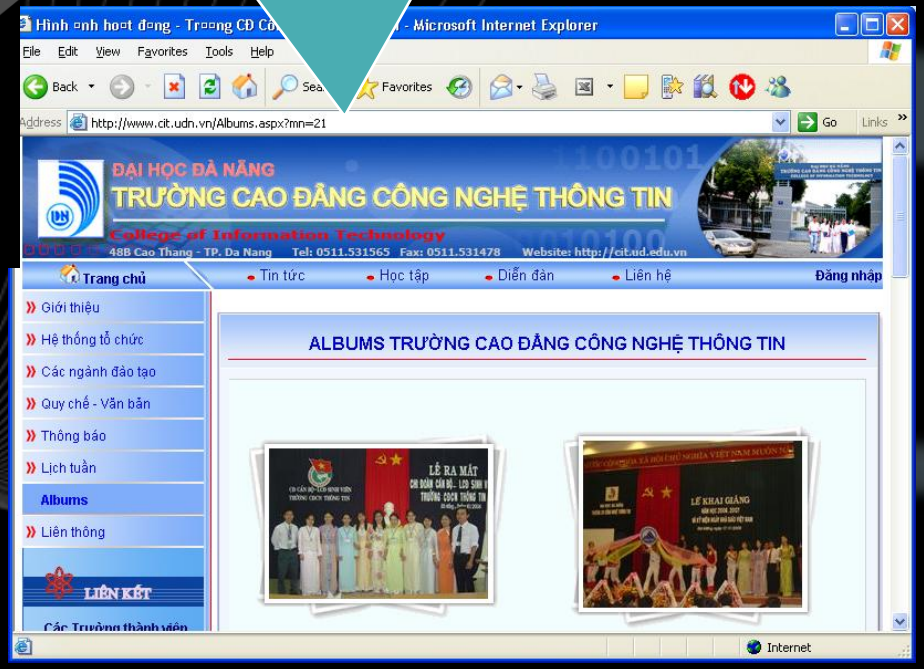


# Client

Client
(Máy khách)

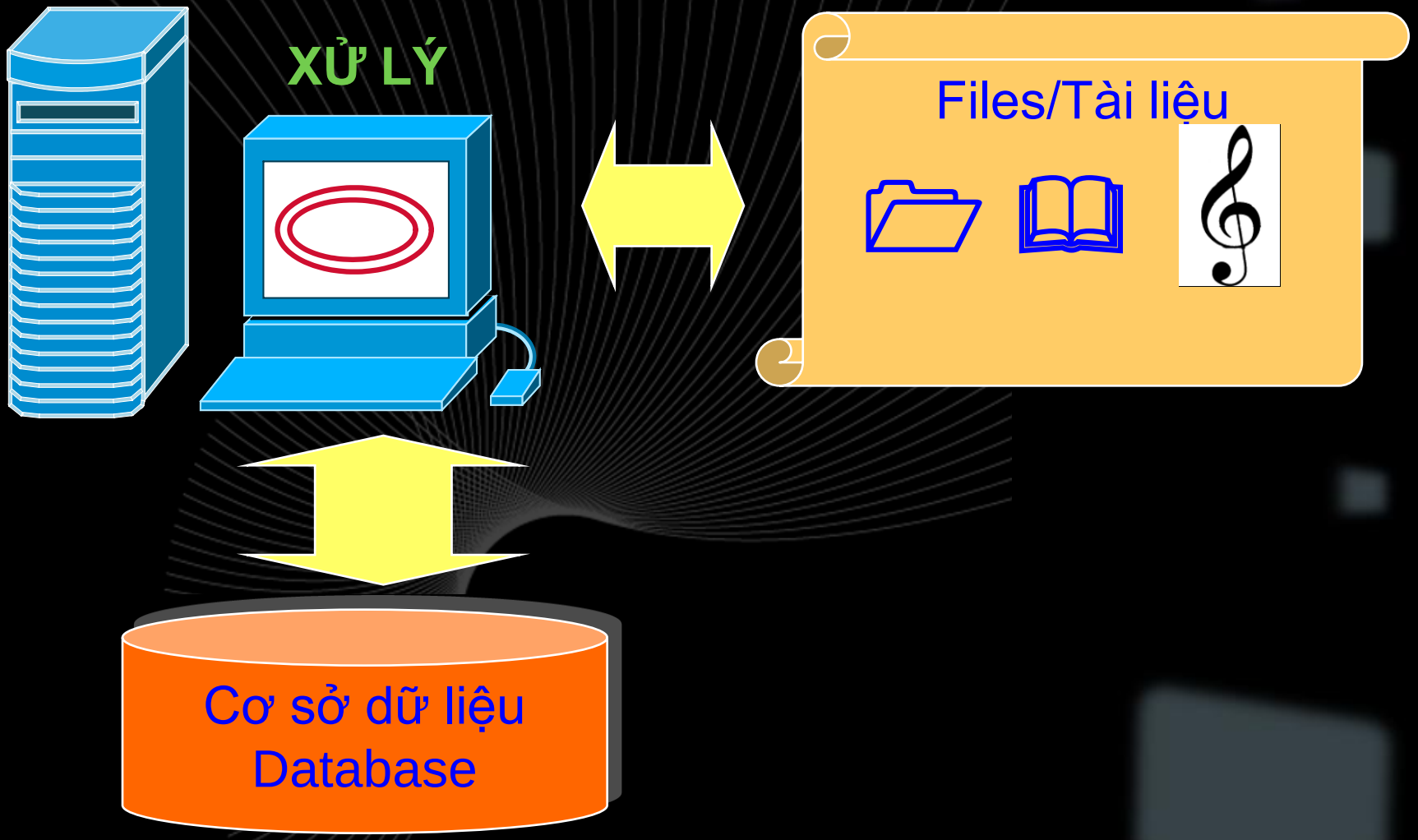


http://www.cit.udn.vn/Albums




Browser
(Internet Explorer)

# Server



# Nguyên tắc hoạt động

http://www.cit.udn.vn

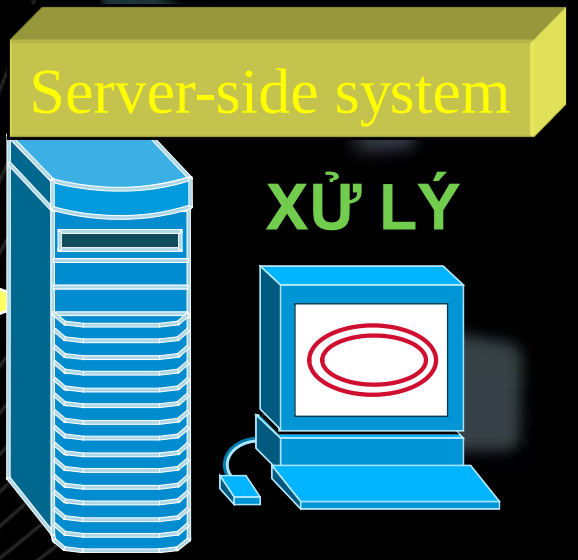
Request (Yêu cầu)

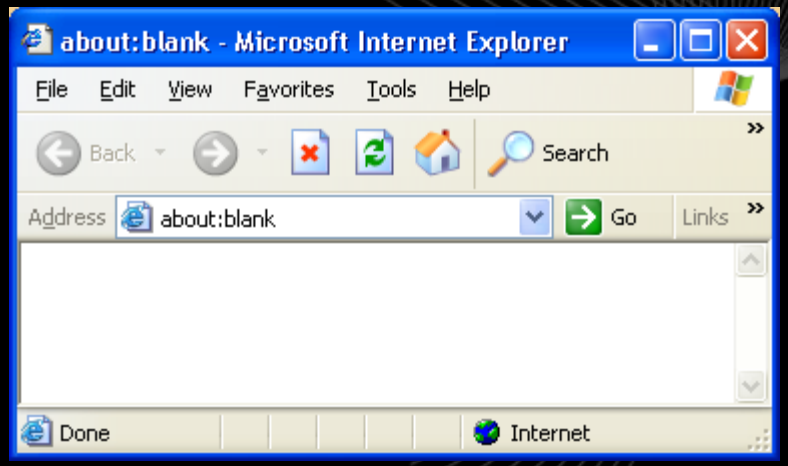
HTTP transport

HTML + CSS

Server-side system

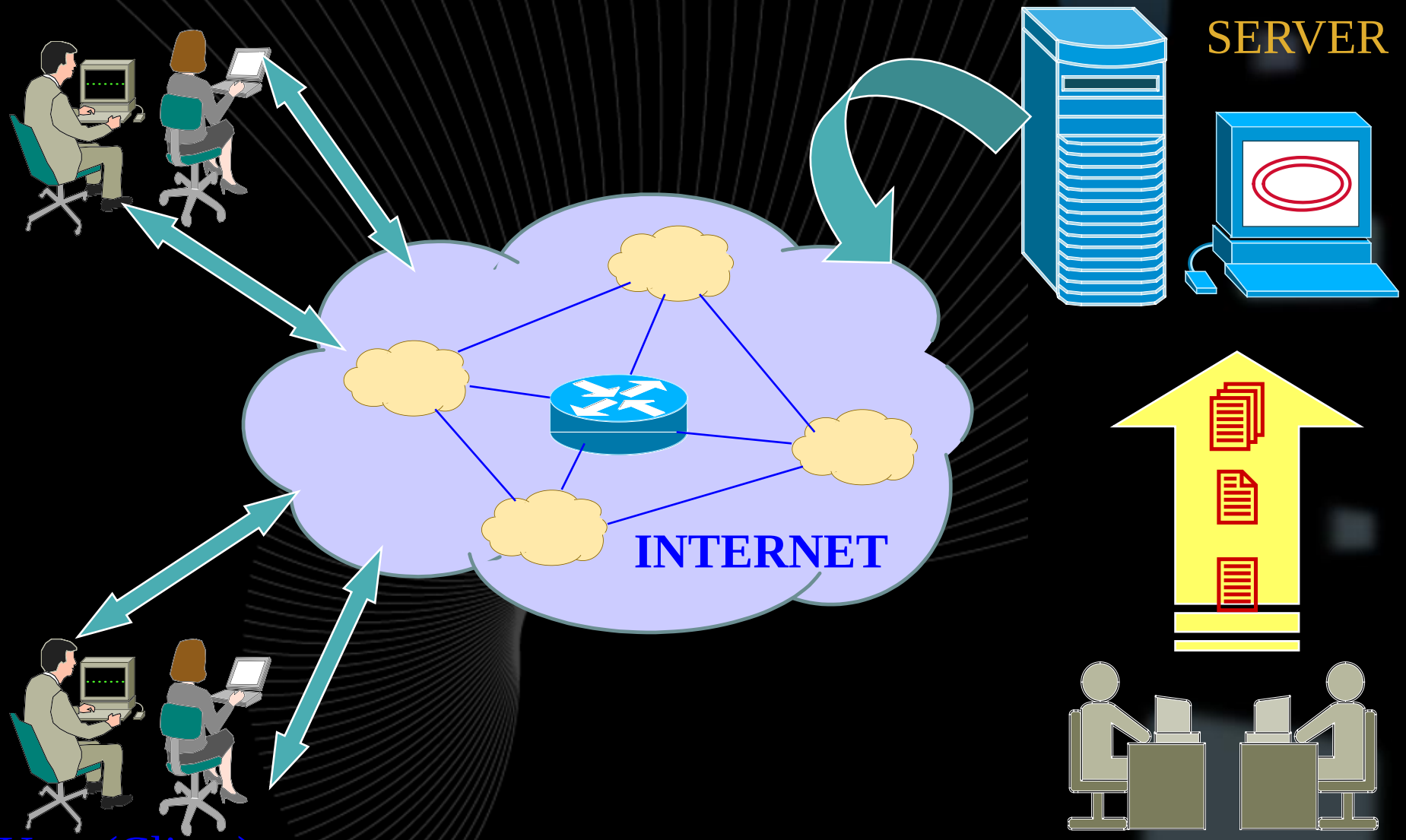
XỬ LÝ






Cơ sở dữ liệu
Database

# Internet



# SÁCH

# Nhập môn Mạng máy tính

# PHẦN I. NHẬP MÔN LÝ THUYẾT MẠNG

## Chương 1. Tổng quan về công nghệ mạng máy tính và mạng cục bộ

I. Lịch sử mạng máy tính

II. Giới thiệu mạng máy tính

2.1. Định nghĩa mạng máy tính và mục đích của việc kết nối mạng

2.1.1. Nhu cầu của việc kết nối mạng máy tính.

2.1.2. Định nghĩa mạng máy tính

2.2. Đặc trưng kỹ thuật của mạng máy tính

2.2.1. Đường truyền

2.2.2. Kỹ thuật chuyển mạch

2.2.3. Kiến trúc mạng

2.2.4. Hệ điều hành mạng

2.3. Phân loại mạng máy tính

2.3.1. Phân loại mạng theo khoảng cách địa lý :

2.3.2. Phân loại mạng theo kỹ thuật chuyển mạch

2.3.3. Phân loại theo kiến trúc mạng sử dụng

2.3.4. Phân loại theo hệ điều hàng mạng

2.4. Giới thiệu các mạng máy tính thông dụng nhất

2.4.1. Mạng cục bộ

2.4.2. Mạng diện rộng với kết nối LAN TO LAN.

2.4.3. Liên mạng INTERNET.

2.4.4. Mạng INTRANET

III. Mạng cục bộ, kiến trúc mạng cục bộ

3.1. Mạng cục bộ

3.2. Kiến trúc mạng cục bộ.

3.3. Các phương pháp truy cập đường truyền vật lý

3.3.1 Phương pháp đa truy nhập sử dụng sóng mang có phát hiện xung đột CSMA/CD

3.3.2. Phương pháp Token Bus.

3.3.2. Phương pháp Token Ring.

IV. Chuẩn hoá mạng máy tính

4.1. Vấn đề chuẩn hoá mạng và các tổ chức chuẩn hoá mạng

4.2. Mô hình tham chiếu OSI 7 lớp

4.3. Các chuẩn kết nối thông dụng nhất IEEE 802.X và ISO 8802.X

**Chương 2. Các thiết bị mạng thông dụng và các chuẩn kết nối vật lý**

I. Các thiết bị mạng thông dụng

1.1. Các loại cáp truyền

1.1.1. Cáp đôi dây xoắn (Twisted pair cable)

1.1.2. Cáp đồng trục (Coaxial cable) băng tần cơ sở

1.1.3. Cáp đồng trục băng rộng (Broadband Coaxial Cable)

1.1.4. Cáp quang

1.2. Các thiết bị ghép nối.

1.2.1. Card giao tiếp mạng (Network Interface Card viết tắt là NIC).

1.2.2. Bộ chuyển tiếp (REPEATER )

1.2.3. Các bộ tập trung (HUB).

1.2.4. Switching Hub

1.2.5. Modem

1.2.6. Router

II. Một số kiểu nối mạng thông dụng và các chuẩn

2.1.Các thành phần thông thường trên một mạng cục bộ gồm có

2.2. Kiểu 10BASE5

2.3. Kiểu 10BASE2

2.4. Kiểu 10BASE-T

2.5. Kiểu 10BASE-F

**Chương 3. Giới thiệu giao thức TCP/IP**

I. Giao thức IP.

1.1. Họ giao thức TCP/IP

1.2. Chức năng chính của - Giao thức liên mạng IP(v4)

1.2.1. Địa chỉ IP

1.2.2. Cấu trúc gói dữ liệu IP

1.2.3. Phân mảnh và hợp nhất các gói IP

1.2.4. Định tuyến IP

II. Giao thức lớp chuyển tải (Transport Layer)

2.1. Giao thức TCP

2.2 Cấu trúc gói dữ liệu TCP

2.3. Thiết lập và kết thúc kết nối TCP

**Chương 4. Giao thức** (4)

I. Chức năng của giao thức

II. Giao thức trong kiến trúc phân tầng. Chồng giao thức

III. Các giao thức chuẩn

IV. Cài đặt và gỡ bỏ giao thức

**Chương 5. Quản trị mạng** (6)

I. Khái quát.

II. Quản lý tài khoản mạng

2.1. Khái niệm, các loại Account. Kích hoạt, huỷ bỏ, vô hiệu hoá tạm thời tài khoản.

2.2. Chiến lược quản trị tài khoản. Khái niệm Group, Profile.

2.3. Theo dõi hiệu suất mạng. Hiện tượng tắc nghẽn. Các công cụ quản trị. Giao thức SNMP.

2.4. Duy trì nhật ký mạng.

III. Phòng ngừa mất dữ liệu

3.1. Các loại nguy cơ đe doạ dữ liệu.

3.2. Hệ thống sao lưu trên băng từ. Lịch biểu sao lưu.

3.3. Các hệ thống dung lỗi.

PHẦN II. QUẢN TRỊ MẠNG

# Chương 1. Tổng quan về công nghệ mạng máy tính và mạng cục bộ

Chương này cung cấp các khái niệm, các kiến thức cơ bản nhất về mạng máy tính và phân loại mạng máy tính. Các nội dung giới thiệu mang tính tổng quan về mạng cục bộ, kiến trúc mạng cục bộ, phương pháp truy cập trong mạng cục bộ và các chuẩn vật lý về các thiết bị mạng. Đây là những kiến thức cơ bản rất hữu ích do phạm vi sử dụng của mạng cục bộ là đang phổ biến hiện nay. Hầu hết các cơ quan, tổ chức, công ty có sử dụng công nghệ thông tin đều thiết lập mạng cục bộ riêng.

Các khái niệm, nội dung cơ bản trong chương 1 cần phải nắm vững đối với tất cả các học viên vì chúng sẽ được sử dụng nhiều trong các chương tiếp theo.

## I. Lịch sử mạng máy tính

Internet bắt nguồn từ đề án ARPANET (Advanced Research Project Agency Network) khởi sự trong năm 1969 bởi Bộ Quốc phòng Mỹ (American Department of Defense). Đề án ARPANET với sự tham gia của một số trung tâm nghiên cứu, đại học tại Mỹ (UCLA, Stanford, . . . ) nhằm mục đích thiết kế một mạng WAN (Wide Area Network) có khả năng tự bảo tồn chống lại sự phá hoại một phân mạng bằng chiến tranh nguyên tử. Đề án này dẫn tới sự ra đời của nghi thức truyền IP (Internet Protocol). Theo nghi thức này, thông tin truyền sẽ được đóng thành các gói dữ liệu và truyền trên mạng theo nhiều đường khác nhau từ người gửi tới nơi người nhận. Một hệ thống máy tính nối trên mạng gọi là **Router** làm nhiệm vụ tìm đường đi tối ưu cho các gói dữ liệu, tất cả các máy tính trên mạng đều tham dự vào việc truyền dữ liệu, nhờ vậy nếu một phân mạng bị phá huỷ các **Router** có thể tìm đường khác để truyền thông tin tới người nhận. Mạng ARPANET được phát triển và sử dụng trước hết trong các trường đại học, các cơ quan nhà nước Mỹ, tiếp theo đó, các trung tâm tính toán lớn, các trung tâm truyền vô tuyến điện và vệ tinh được nối vào mạng, . . . trên cơ sở này, ARPANET được nối với khắp các vùng trên thế giới.

Tới năm 1983, trước sự thành công của việc triển khai mạng ARPANET, Bộ quốc phòng Mỹ tách một phân mạng giành riêng cho quân đội Mỹ (MILNET). Phần còn lại, gọi là NSFnet, được quản lý bởi NSF (National Science Foundation) NSF dùng 5 siêu máy tính để làm **Router** cho mạng, và lập một tổ chức không chính phủ để quản lý mạng, chủ yếu dùng cho đại học và nghiên cứu cơ bản trên toàn thế giới. Tới năm 1987, NSFnet mở cửa cho cá nhân và cho các công ty tư nhân (BITnet), tới năm 1988 siêu mạng được mang tên INTERNET.

Tuy nhiên cho tới năm 1988, việc sử dụng INTERNET còn hạn chế trong các dịch vụ truyền mạng (FTP), thư điện tử(E-mail), truy nhập từ xa (TELNET) không thích ứng với nhu cầu kinh tế và đời sống hàng ngày. INTERNET chủ yếu được dùng trong môi trường nghiên cứu khoa học và giảng dạy đại học. Trong năm 1988, tại trung tâm nghiên cứu nguyên tử của Pháp CERN (Centre Européen de Recherche Nuclaire) ra đời đề án Mạng nhện thế giới WWW

(World Wide Web). Đề án này, nhằm xây dựng một phương thức mới sử dụng INTERNET, gọi là phương thức Siêu văn bản (HyperText). Các tài liệu và hình ảnh được trình bày bằng ngôn ngữ HTML (HyperText Markup Language) và được phát hành trên INTERNET qua các hệ chủ làm việc với nghi thức HTTP (HyperText Transport Protocol). Từ năm 1992, phương thức làm việc này được đưa ra thử nghiệm trên INTERNET, rất nhanh chóng, các công ty tư nhân tìm thấy qua phương thức này cách sử dụng INTERNET trong kinh tế và đời sống. Vốn đầu tư vào INTERNET được nhân lên hàng chục lần. Từ năm 1994 INTERNET trở thành siêu mạng kinh doanh. Số các công ty sử dụng INTERNET vào việc kinh doanh và quảng cáo lên gấp hàng nghìn lần kể từ năm 1995. Doanh số giao dịch thương mại qua mạng INTERNET lên hàng chục tỉ USD trong năm 1996 . . .

Với phương thức siêu văn bản, người sử dụng, qua một phần mềm truy đọc (Navigator, Browser), có thể tìm đọc tất cả các tài liệu siêu văn bản công bố tại mọi nơi trên thế giới (kể cả hình ảnh và tiếng nói). Với công nghệ WWW, chúng ta bước vào giai đoạn mà mọi thông tin có thể có ngay trên bàn làm việc của mình. Mỗi công ty hoặc người sử dụng, được phân phối một trang cội nguồn (Home Page) trên hệ chủ HTTP. Trang cội nguồn, là siêu văn bản gốc, để tự do có thể tìm tới tất cả các siêu văn bản khác mà người sử dụng muốn phát hành. Địa chỉ của trang cội nguồn được tìm thấy từ khắp mọi nơi trên thế giới. Vì vậy, đối với một xí nghiệp, trang cội nguồn trở thành một văn phòng đại diện điện tử trên INTERNET. Từ khắp mọi nơi, khách hàng có thể xem các quảng cáo và liên hệ trực tiếp với xí nghiệp qua các dòng siêu liên (HyperLink) trong siêu văn bản.

Tới năm 1994, một điểm yếu của INTERNET là không có khả năng lập trình cục bộ, vì các máy nối vào mạng không đồng bộ và không tương thích. Thiếu khả năng này, INTERNET chỉ được dùng trong việc phát hành và truyền thông tin chứ không dùng để xử lý thông tin được. Trong năm 1994, hãng máy tính SUN Corporation công bố một ngôn ngữ mới, gọi là JAVA (cafe), cho phép lập trình cục bộ trên INTERNET, các chương trình JAVA được gọi thẳng từ các siêu văn bản qua các siêu liên (Applet). Vào mùa thu năm 1995, ngôn ngữ JAVA chính thức ra đời, đánh dấu một bước tiến quan trọng trong việc sử dụng INTERNET. Trước hết, một chương trình JAVA, sẽ được chạy trên máy khách (Workstation) chứ không phải trên máy chủ (Server). Điều này cho phép sử dụng công suất của tất cả các máy khách vào việc xử lý số liệu. Hàng triệu máy tính (hoặc vi tính) có thể thực hiện cùng một lúc một chương trình ghi trên một siêu văn bản trong máy chủ. Việc lập trình trên INTERNET cho phép truy nhập từ một trang siêu văn bản vào các chương trình xử lý thông tin, đặc biệt là các chương trình điều hành và quản lý thông tin của một xí nghiệp. phương thức làm việc này, được gọi là INTRANET. Chỉ trong năm 1995-1996, hàng trăm nghìn dịch vụ phần mềm INTRANET được phát triển. Nhiều hãng máy tính và phần mềm như Microsoft, SUN, IBM, Oracle, Netscape,... đã phát triển và kinh doanh

hàng loạt phần mềm hệ thống và phần mềm cơ bản để phát triển các ứng dụng INTERNET / INTRANET.

## II. Giới thiệu mạng máy tính

### 2.1. Định nghĩa mạng máy tính và mục đích của việc kết nối mạng

#### 2.1.1. Nhu cầu của việc kết nối mạng máy tính

Việc nối máy tính thành mạng từ lâu đã trở thành một nhu cầu khách quan vì :

- Có rất nhiều công việc về bản chất là phân tán hoặc về thông tin, hoặc về xử lý hoặc cả hai đòi hỏi có sự kết hợp truyền thông với xử lý hoặc sử dụng phương tiện từ xa.

- Chia sẻ các tài nguyên trên mạng cho nhiều người sử dụng tại một thời điểm (ổ cứng, máy in, ổ CD ROM . . .)

- Nhu cầu liên lạc, trao đổi thông tin nhờ phương tiện máy tính.

- Các ứng dụng phần mềm đòi hòi tại một thời điểm cần có nhiều người sử dụng, truy cập vào cùng một cơ sở dữ liệu.

#### 2.1.2. Định nghĩa mạng máy tính

Nói một cách ngắn gọn thì mạng máy tính là tập hợp các máy tính độc lập (autonomous) được kết nối với nhau thông qua các đường truyền vật lý và tuân theo các quy ước truyền thông nào đó.

Khái niệm máy tính độc lập được hiểu là các máy tính không có máy nào có khả năng khởi động hoặc đình chỉ một máy khác.

Các đường truyền vật lý được hiểu là các môi trường truyền tín hiệu vật lý (có thể là hữu tuyến hoặc vô tuyến).

Các quy ước truyền thông chính là cơ sở để các máy tính có thể "nói chuyện" được với nhau và là một yếu tố quan trọng hàng đầu khi nói về công nghệ mạng máy tính.

### 2.2. Đặc trưng kỹ thuật của mạng máy tính

Một mạng máy tính có các đặc trưng kỹ thuật cơ bản như sau:

#### 2.2.1. Đường truyền

Là thành tố quan trọng của một mạng máy tính, là phương tiện dùng để truyền các tín hiệu điện tử giữa các máy tính. Các tín hiệu điệu tử đó chính là các thông tin, dữ liệu được biểu thị dưới dạng các xung nhị phân (ON_OFF), mọi tín hiệu truyền giữa các máy tính với nhau đều thuộc sóng điện từ, tuỳ theo tần số mà ta có thể dùng các đường truyền vật lý khác nhau

Đặc trưng cơ bản của đường truyền là giải thông nó biểu thị khả năng truyền tải tín hiệu của đường truyền.

Thông thuờng người ta hay phân loại đường truyền theo hai loại:

- Đường truyền hữu tuyến (các máy tính được nối với nhau bằng các dây cáp mạng).

- Đường truyền vô tuyến: các máy tính truyền tín hiệu với nhau thông qua các sóng vô tuyền với các thiết bị điều chế/giải điều chế ở các đầu mút.

### 2.2.2. Kỹ thuật chuyển mạch:

Là đặc trưng kỹ thuật chuyển tín hiệu giữa các nút trong mạng, các nút mạng có chức năng hướng thông tin tới đích nào đó trong mạng, hiện tại có các kỹ thuật chuyển mạch như sau:

- Kỹ thuật chuyển mạch kênh: Khi có hai thực thể cần truyền thông với nhau thì giữa chúng sẽ thiết lập một kênh cố định và duy trì kết nối đó cho tới khi hai bên ngắt liên lạc. Các dữ liệu chỉ truyền đi theo con đường cố định đó.

- Kỹ thuật chuyển mạch thông báo: thông báo là một đơn vị dữ liệu của người sử dụng có khuôn dạng được quy định trước. Mỗi thông báo có chứa các thông tin điều khiển trong đó chỉ rõ đích cần truyền tới của thông báo. Căn cứ vào thông tin điều khiển này mà mỗi nút trung gian có thể chuyển thông báo tới nút kế tiếp trên con đường dẫn tới đích của thông báo

- Kỹ thuật chuyển mạch gói: ở đây mỗi thông báo được chia ra thành nhiều gói nhỏ hơn được gọi là các gói tin (packet) có khuôn dạng qui định trước. Mỗi gói tin cũng chứa các thông tin điều khiển, trong đó có địa chỉ nguồn (người gửi) và địa chỉ đích (người nhận) của gói tin. Các gói tin của cùng một thông báo có thể được gởi đi qua mạng tới đích theo nhiều con đường khác nhau.

### 2.2.3. Kiến trúc mạng

Kiến trúc mạng máy tính (network architecture) thể hiện cách nối các máy tính với nhau và tập hợp các quy tắc, quy ước mà tất cả các thực thể tham gia truyền thông trên mạng phải tuân theo để đảm bảo cho mạng hoạt động tốt.

Khi nói đến kiến trúc của mạng người ta muốn nói tới hai vấn đề là hình trạng mạng (Network topology) và giao thức mạng (Network protocol)

- Network Topology: Cách kết nối các máy tính với nhau về mặt hình học mà ta gọi là tô pô của mạng. Các hình trạng mạng cơ bản đó là: hình sao, hình bus, hình vòng

- Network Protocol: Tập hợp các quy ước truyền thông giữa các thực thể truyền thông mà ta gọi là giao thức (hay nghi thức) của mạng. Các giao thức thường gặp nhất là : TCP/IP, NETBIOS, IPX/SPX, . . .

### 2.2.4. Hệ điều hành mạng

Hệ điều hành mạng là một phần mềm hệ thống có các chức năng sau:

- Quản lý tài nguyên của hệ thống, các tài nguyên này gồm:

+ Tài nguyên thông tin (về phương diện lưu trữ) hay nói một cách đơn giản là quản lý tệp. Các công việc về lưu trữ tệp, tìm kiếm, xoá, copy, nhóm, đặt các thuộc tính đều thuộc nhóm công việc này

+ Tài nguyên thiết bị. Điều phối việc sử dụng CPU, các ngoại vi... để tối ưu hoá việc sử dụng

- Quản lý người dùng và các công việc trên hệ thống.

Hệ điều hành đảm bảo giao tiếp giữa người sử dụng, chương trình ứng dụng với thiết bị của hệ thống.

- Cung cấp các tiện ích cho việc khai thác hệ thống thuận lợi (ví dụ FORMAT đĩa, sao chép tệp và thư mục, in ấn chung ...)

Các hệ điều hành mạng thông dụng nhất hiện nay là: WindowsNT, Windows9X, Windows 2000, Unix, Novell.

## 2.3. Phân loại mạng máy tính

Có nhiều cách phân loại mạng khác nhau tuỳ thuộc vào yếu tố chính được chọn dùng để làm chỉ tiêu phân loại, thông thường người ta phân loại mạng theo các tiêu chí như sau

- Khoảng cách địa lý của mạng

- Kỹ thuật chuyển mạch mà mạng áp dụng

- Kiến trúc mạng

- Hệ điều hành mạng sử dụng ...

Tuy nhiên trong thực tế người ta thường chỉ phân loại theo hai tiêu chí đầu tiên

### 2.3.1. Phân loại mạng theo khoảng cách địa lý :

Nếu lấy khoảng cách địa lý làm yếu tố phân loại mạng thì ta có mạng cục bộ, mạng đô thị, mạng diện rộng, mạng toàn cầu.

Mạng cục bộ ( LAN - Local Area Network ) : là mạng được cài đặt trong phạm vi tương đối nhỏ hẹp như trong một toà nhà, một xí nghiệp...với khoảng cách lớn nhất giữa các máy tính trên mạng trong vòng vài km trở lại.

Mạng đô thị ( MAN - Metropolitan Area Network ) : là mạng được cài đặt trong phạm vi một đô thị, một trung tâm văn hoá xã hội, có bán kính tối đa khoảng 100 km trở lại.

Mạng diện rộng ( WAN - Wide Area Network ) : là mạng có diện tích bao phủ rộng lớn, phạm vi của mạng có thể vượt biên giới quốc gia thậm chí cả lục địa.

Mạng toàn cầu ( GAN - Global Area Network ) : là mạng có phạm vi trải rộng toàn cầu.

### 2.3.2. Phân loại theo kỹ thuật chuyển mạch:

Nếu lấy kỹ thuật chuyển mạch làm yếu tố chính để phân loại sẽ có: mạng chuyển mạch kênh, mạng chuyển mạch thông báo và mạng chuyển mạch gói.

Mạch chuyển mạch kênh (circuit switched network) : Khi có hai thực thể cần truyền thông với nhau thì giữa chúng sẽ thiết lập một kênh cố định và duy trì kết nối đó cho tới khi hai bên ngắt liên lạc. Các dữ liệu chỉ truyền đi theo con đường cố định đó. Nhược điểm của chuyển mạch kênh là tiêu tốn thời gian để thiết lập kênh truyền cố định và hiệu suất sử dụng mạng không cao.

Mạng chuyển mạch thông báo (message switched network) : Thông báo là một đơn vị dữ liệu của người sử dụng có khuôn dạng được quy định trước. Mỗi thông báo có chứa các thông tin điều khiển trong đó chỉ rõ đích cần truyền tới của thông báo. Căn cứ vào thông tin điều khiển này mà mỗi nút trung gian có thể chuyển thông báo tới nút kế tiếp trên con đường dẫn tới đích của thông báo. Như vậy mỗi nút cần phải lưu giữ tạm thời để đọc thông tin điều khiển trên thông báo, nếu thấy thông báo không gửi cho mình thì tiếp tục chuyển tiếp thông báo đi. Tuỳ vào điều kiện của mạng mà thông báo có thể được chuyển đi theo nhiều con đường khác nhau.

Ưu điểm của phương pháp này là :

- Hiệu suất sử dụng đường truyền cao vì không bị chiếm dụng độc quyền mà được phân chia giữa nhiều thực thể truyền thông.

- Mỗi nút mạng có thể lưu trữ thông tin tạm thời sau đó mới chuyển thông báo đi, do đó có thể điều chỉnh để làm giảm tình trạng tắc nghẽn trên mạng.

- Có thể điều khiển việc truyền tin bằng cách sắp xếp độ ưu tiên cho các thông báo.

- Có thể tăng hiệu suất sử dụng giải thông của mạng bằng cách gắn địa chỉ quảng bá (broadcast addressing) để gửi thông báo đồng thời tới nhiều đích.

Nhược điểm của phương pháp này là:

- Không hạn chế được kích thước của thông báo dẫn đến phí tổn lưu giữ tạm thời cao và ảnh hưởng đến thời gian trả lời yêu cầu của các trạm .

Mạng chuyển mạch gói (packet switched network) : ở đây mỗi thông báo được chia ra thành nhiều gói nhỏ hơn được gọi là các gói tin (packet) có khuôn dạng qui định trước. Mỗi gói tin cũng chứa các thông tin điều khiển, trong đó có địa chỉ nguồn (người gửi) và địa chỉ đích (người nhận) của gói tin. Các gói tin của cùng một thông báo có thể được gởi đi qua mạng tới đích theo nhiều con đường khác nhau.

Phương pháp chuyển mạch thông báo và chuyển mạch gói là gần giống nhau. Điểm khác biệt là các gói tin được giới hạn kích thước tối đa sao cho các nút mạng (các nút chuyển mạch) có thể xử lý toàn bộ gói tin trong bộ nhớ mà không phải lưu giữ tạm thời trên đĩa. Bởi vậy nên mạng chuyển mạch gói truyền dữ liệu hiệu quả hơn so với mạng chuyển mạch thông báo.

Tích hợp hai kỹ thuật chuyển mạch kênh và chuyển mạch gói vào trong một mạng thống nhất được mạng tích hợp số ISDN (Integated Services Digital Network).

### 2.3.3. Phân loại theo kiến trúc mạng sử dụng

Kiến trúc của mạng bao gồm hai vấn đề: hình trạng mạng (Network topology) và giao thức mạng (Network protocol)

Hình trạng mạng: Cách kết nối các máy tính với nhau về mặt hình học mà ta gọi là tô pô của mạng

Giao thức mạng: Tập hợp các quy ước truyền thông giữa các thực thể truyền thông mà ta gọi là giao thức (hay nghi thức) của mạng

Khi phân loại theo topo mạng người ta thường có phân loại thành: mạng hình sao, tròn, tuyến tính

Phân loại theo giao thức mà mạng sử dụng người ta phân loại thành mạng : TCP/IP, mạng NETBIOS . ..

Tuy nhiên cách phân loại trên không phổ biến và chỉ áp dụng cho các mạng cục bộ.

### 2.3.4. Phân loại theo hệ điều hàng mạng

Nếu phân loại theo hệ điều hành mạng người ta chia ra theo mô hình mạng ngang hàng, mạng khách/chủ hoặc phân loại theo tên hệ điều hành mà mạng sử dụng: Windows NT, Unix, Novell . . .

## 2.4. Giới thiệu các mạng máy tính thông dụng nhất

### 2.4.1. Mạng cục bộ

Một mạng cục bộ là sự kết nối một nhóm máy tính và các thiết bị kết nối mạng được lắp đặt trên một phạm vị địa lý giới hạn, thường trong một toà nhà hoặc một khu công sở nào đó.

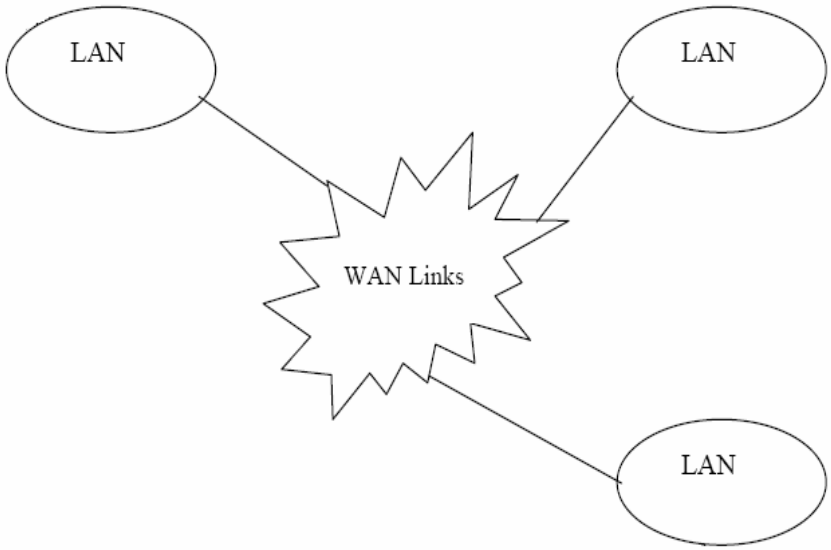
Mạng cục bộ có các đặc tính sau:

- Tốc độ truyền dữ liệu cao

- Phạm vi địa lý giới hạn

-Sở hữu của một cơ quan/tổ chức

### 2.4.2. Mạng diện rộng với kết nối LAN TO LAN




Mạng diện rộng bao giờ cũng là sự kết nối của các mạng LAN, mạng diện rộng có thể trải trên phạm vi một vùng, quốc gia hoặc cả một lục địa thậm chí trên phạm vi toàn cầu.

- Tốc độ truyền dữ liệu không cao

- Phạm vi địa lý không giới hạn

- Thường triển khai dựa vào các công ty truyền thông, bưu điện và dùng các hệ thống truyền thông này để tạo dựng đường truyền

- Một mạng WAN có thể là sở hữu của một tập đoàn/tổ chức hoặc là mạng kết nối của nhiều tập đoàn/tỗ chức 16

### 2.4.3. Liên mạng INTERNET

Với sự phát triển nhanh chóng của công nghệ là sự ra đời của liên mạng INTERNET,

- Là một mạng toàn cầu

- Là sự kết hợp của vô số các hệ thống truyền thông, máy chủ cung cấp thông tin và dịch vụ, các máy trạm khai thác thông tin

- Dựa trên nhiều nền tảng truyền thông khác nhau, nhưng đều trên nền giao thức TCP/IP

- Là sở hữu chung của toàn nhân loại

- Càng ngày càng phát triển mãnh liệt

### 2.4.4. Mạng INTRANET

Thực sự là một mạng INTERNET thu nhỏ vào trong một cơ quan/công ty/tổ chức hay một bộ/nghành . . ., giới hạn phạm vi người sử dụng, có sử dụng các công nghệ kiểm soát truy cập và bảo mật thông tin .

Được phát triển từ các mạng LAN, WAN dùng công nghệ INTERNET

## III. Mạng cục bộ, kiến trúc mạng cục bộ

### 3.1. Mạng cục bộ

Tên gọi "mạng cục bộ" được xem xét từ quy mô của mạng. Tuy nhiên, đó không phải là đặc tính duy nhất của mạng cục bộ nhưng trên thực tế, quy mô của mạng quyết định nhiều đặc tính và công nghệ của mạng. Sau đây là một số đặc điểm của mạng cục bộ:

Đặc điểm của mạng cục bộ

- Mạng cục bộ có quy mô nhỏ, thường là bán kính dưới vài km. Đặc điểm này cho phép không cần dùng các thiết bị dẫn đường với các mối liên hệ phức tạp

- Mạng cục bộ thường là sở hữu của một tổ chức. Điều này dường như có vẻ ít quan trọng nhưng trên thực tế đó là điều khá quan trọng để việc quản lý mạng có hiệu quả.

- Mạng cục bộ có tốc độ cao và ít lỗi. Trên mạng rộng tốc độ nói chung chỉ đạt vài Kbit/s. Còn tốc độ thông thường trên mạng cục bộ là 10, 100 Kb/s và tới nay với Gigabit Ethernet, tốc độ trên mạng cục bộ có thể đạt 1Gb/s. Xác suất lỗi rất thấp.

### 3.2. Kiến trúc mạng cục bộ

*** Định nghĩa Topo mạng:**

Cách kết nối các máy tính với nhau về mặt hình học mà ta gọi là tô pô của mạng

Có hai kiểu nối mạng chủ yếu đó là :

- Nối kiểu điểm - điểm (point - to - point).

- Nối kiểu điểm - nhiều điểm (point - to - multipoint hay broadcast).

Theo kiểu điểm - điểm, các đường truyền nối từng cặp nút với nhau và mỗi nút đều có trách nhiệm lưu giữ tạm thời sau đó chuyển tiếp dữ liệu đi cho tới đích. Do cách làm việc như vậy nên mạng kiểu này còn được gọi là mạng "lưu và chuyển tiếp" (store and forward).

Theo kiểu điểm - nhiều điểm, tất cả các nút phân chia nhau một đường truyền vật lý chung. Dữ liệu gửi đi từ một nút nào đó sẽ được tiếp nhận bởi tất cả các nút còn lại trên mạng, bởi vậy cần chỉ ra địa chỉ đích của dữ liệu để căn cứ vào đó các nút kiểm tra xem dữ liệu đó có phải gửi cho mình không.

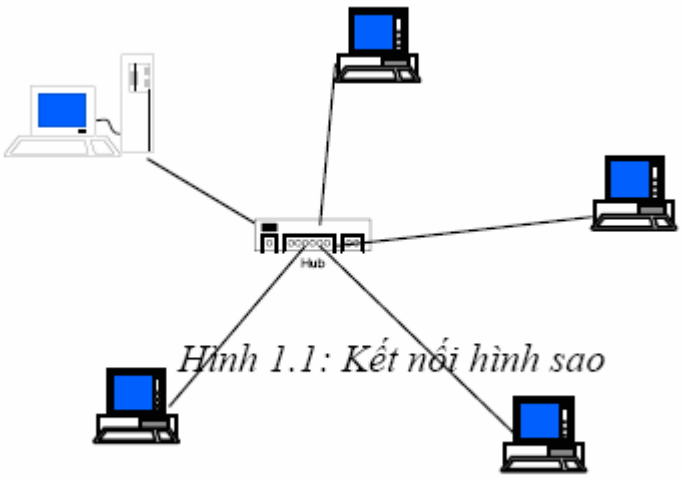
*** Phân biệt kiểu tô pô của mạng cục bộ và kiểu tô pô của mạng rộng.**

Tô pô của mạng rộng thông thường là nói đến sự liên kết giữa các mạng cục bộ thông qua các bộ dẫn đường (router). Đối với mạng rộng topo của mạng là hình trạng hình học của các bộ dẫn đường và các kênh viễn thông còn khi nói tới tô pô của mạng cục bộ người ta nói đến sự liên kết của chính các máy tính.

### a) Mạng hình sao

Mạng hình sao có tất cả các trạm được kết nối với một thiết bị trung tâm có nhiệm vụ nhận tín hiệu từ các trạm và chuyển đến trạm đích. Tuỳ theo yêu cầu truyền thông trên mạng mà thiết bị trung tâm có thể là bộ chuyển mạch (switch), bộ chọn đường (router) hoặc là bộ phân kênh (hub). Vai trò của thiết bị trung tâm này là thực hiện việc thiết lập các liên kết điểm-điểm (point-to-point) giữa các trạm.

Ưu điểm: Thiết lập mạng đơn giản, dễ dàng cấu hình lại mạng (thêm, bớt các trạm), dễ dàng kiểm soát và khắc phục sự cố, tận dụng được tối đa tốc độ




*Hình 1.1: Kết nối hình sao*

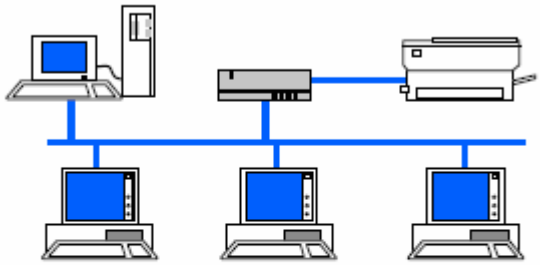
truyền của đường truyền vật lý.

Nhược điểm: Độ dài đường truyền nối một trạm với thiết bị trung tâm bị hạn chế (trong vòng 100m, với công nghệ hiện nay). Hub

### b) Mạng trục tuyến tính (Bus):

Trong mạng trục tất cả các trạm phân chia một đường truyền chung (bus). Đường truyền chính được giới hạn hai đầu bằng hai đầu nối đặc biệt gọi là terminator. Mỗi trạm được nối với trục chính qua một đầu nối chữ T (T-connector) hoặc một thiết bị thu phát (transceiver).

Khi một trạm truyền dữ liệu tín hiệu được quảng bá trên cả hai chiều của bus, tức là mọi trạm còn lại đều có thể thu được tín hiệu đó trực tiếp. Đối với các bus một chiều thì tín hiệu chỉ đi về một phía, lúc đó các terminator phải được thiết kế sao cho các tín hiệu đó phải được dội lại trên bus để cho các trạm trên mạng đều có thể thu nhận được tín hiệu đó. Như vậy với topo mạng trục dữ liệu được truyền theo các liên kết điểm-đa điểm (point-to-multipoint) hay quảng bá (broadcast).



*Hình 1.2. Kết nối kiểu bus*

Ưu điểm : Dễ thiết kế, chi phí thấp

Nhược điểm: Tính ổn định kém, chỉ một nút mạng hỏng là toàn bộ mạng bị ngừng hoạt động

**c) Mạng hình vòng**

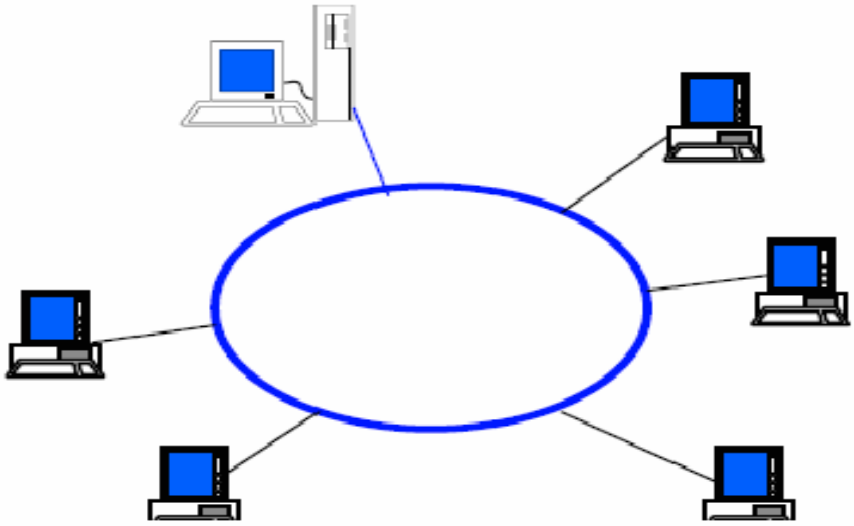
Trên mạng hình vòng tín hiệu được truyền đi trên vòng theo một chiều duy nhất. Mỗi trạm của mạng được nối với vòng qua một bộ chuyển tiếp (repeater) có nhiệm vụ nhận tín hiệu rồi chuyển tiếp đến trạm kế tiếp trên vòng. Như vậy tín hiệu được lưu chuyển trên vòng theo một chuỗi liên tiếp các liên kết điểm-điểm giữa các repeater do đó cần có giao thức điều khiển việc cấp phát quyền được truyền dữ liệu trên vòng mạng cho trạm có nhu cầu.

Để tăng độ tin cậy của mạng ta có thể lắp đặt thêm các vòng dự phòng, nếu vòng chính có sự cố thì vòng phụ sẽ được sử dụng.

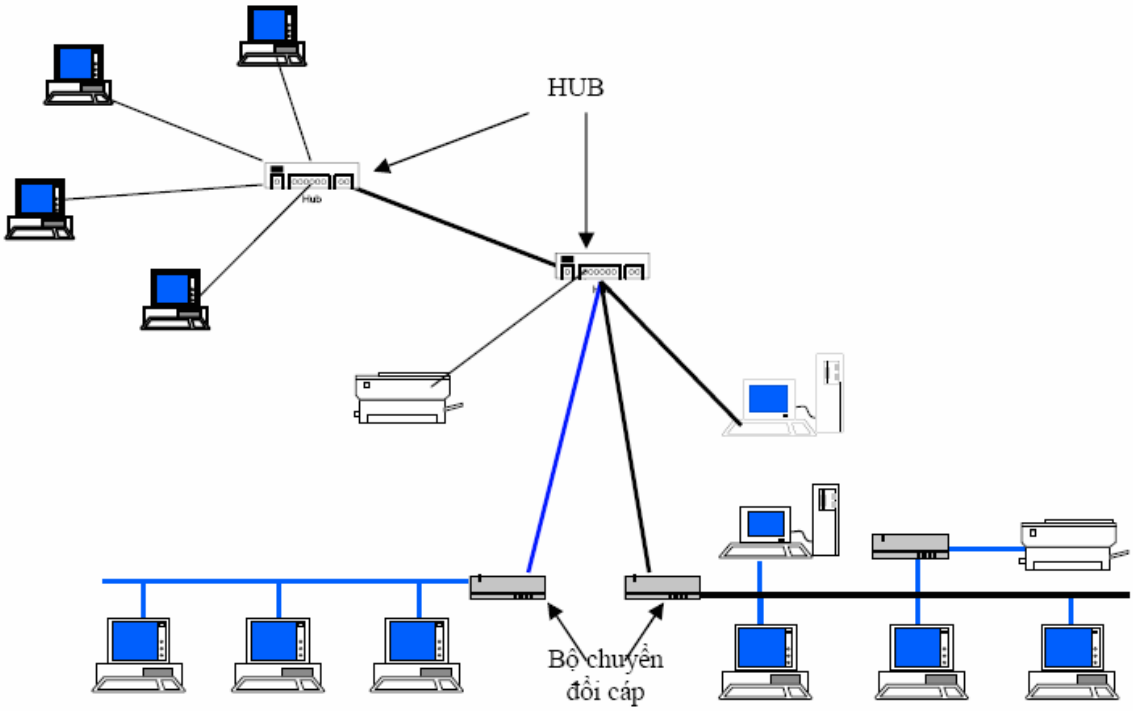
Mạng hình vòng có ưu nhược điểm tương tự mạng hình sao, tuy nhiên mạng hình vòng đòi hỏi giao thức truy nhập mạng phức tạp hơn mạng hình sao.

**d) Kết nối hỗn hợp**

Là sự phối hợp các kiểu kết nối khác nhau, ví du hình cây là cấu trúc phân tầng của kiểu hình sao hay các HUB có thể được nối với nhau theo kiểu bus còn từ các HUB nối với các máy theo hình sao.



Hình 1.3 Kết nối kiểu vòng




Hình 1.4. Một kết nối hỗn hợp

## 3.3. Các phương pháp truy cập đường truyền vật lý

Trong mạng cục bộ, tất cả các trạm kết nối trực tiếp vào đường truyền chung. Vì vậy tín hiệu từ một trạm đưa lên đường truyền sẽ được các trạm khác "nghe thấy". Một vấn đề khác là, nếu nhiều trạm cùng gửi tín hiệu lên đường truyền đồng thời thì tín hiệu sẽ chồng lên nhau và bị hỏng. Vì vậy cần phải có

một phương pháp tổ chức chia sẻ đường truyền để việc truyền thông được đúng đắn.

Có hai phương pháp chia sẻ đường truyền chung thường được dùng trong các mạng cục bộ:

- Truy nhập đường truyền một cách ngẫu nhiên, theo yêu cầu. Đương nhiên phải có tính đến việc sử dụng luân phiên và nếu trong trường hợp do có nhiều trạm cùng truyền tin dẫn đến tín hiệu bị trùm lên nhau thì phải truyền lại.

- Có cơ chế trọng tài để cấp quyền truy nhập đường truyền sao cho không xảy ra xung đột

### 3.3.1 Phương pháp đa truy nhập sử dụng sóng mang có phát hiện xung đột CSMA/CD (Carrier Sense Multiple Access with Collision Detection)

Giao thức CSMA (Carrier Sense Multiple Access) - đa truy nhập có cảm nhận sóng mang được sử dụng rất phổ biến trong các mạng cục bộ. Giao thức này sử dụng phương pháp thời gian chia ngăn theo đó thời gian được chia thành các khoảng thời gian đều đặn và các trạm chỉ phát lên đường truyền tại thời điểm đầu ngăn.

Mỗi trạm có thiết bị nghe tín hiệu trên đường truyền (tức là cảm nhận sóng mang). Trước khi truyền cần phải biết đường truyền có rỗi không. Nếu rỗi thì mới được truyền. Phương pháp này gọi là LBT (Listening before talking). Khi phát hiện xung đột, các trạm sẽ phải phát lại. Có một số chiến lược phát lại như sau:

- Giao thức CSMA không kiên trì.Trạm nghe đường, nếu kênh rỗi thì truyền, nếu không thì ngừng nghe một khoảng thời gian ngẫu nhiên rồi mới thực hiện lại thủ tục. Cách này có hiệu suất dùng kênh cao hơn. (1)

- Giao thức CSMA 1-kiên trì. Khi trạm phát hiện kênh rỗi trạm truyền ngay. Nhưng nếu có xung đột, trạm đợi khoảng thời gian ngẫu nhiên rồi truyền lại. Do vậy xác suất truyền khi kênh rỗi là 1. Chính vì thế mà giao thức có tên là CSMA 1-kiên trì. (2)

- Giao thức CSMA p-kiên trì. Khi đã sẵn sàng truyền, trạm cảm nhận đường, nếu đường rỗi thì thực hiện việc truyền với xác suất là $p < 1$ (tức là ngay cả khi đường rỗi cũng không hẳn đã truyền mà đợi khoảng thời gian tiếp theo lại tiếp tục thực hiện việc truyền với xác suất còn lại $q=1-p$. (3)

• Ta thấy giải thuật (1) có hiệu quả trong việc tránh xung đột vì hai trạm cần truyền thấy đường truyền bận sẽ cùng rút lui chờ trong những khoảng thời gian ngẫu nhiên khác nhau sẽ quay lại tiếp tục nghe đường truyền. Nhược điểm của nó là có thể có thời gian không sử dụng đường truyền sau mỗi cuộc gọi.

• Giải thuật (2) cố gắng làm giảm thời gian "chết" bằng cách cho phép một trạm có thể được truyền dữ liệu ngay sau khi một cuộc truyền kết thúc. Tuy

nhiên nếu lúc đó lại có nhiều trạm đang đợi để truyền dữ liệu thì khả năng xẩy ra xung đột sẽ rất lớn.

• Giải thuật (3) với giá trị p được họn hợp lý có thể tối thiểu hoá được cả khả năng xung đột lẫn thời gian "chết" của đường truyền.

• Xẩy ra xung đột thường là do độ trễ truyền dẫn, mấu chốt của vấn đề là: các trạm chỉ "nghe" trước khi truyền dữ liệu mà không "nghe" trong khi truyền, cho nên thực tế có xung đột thế nhưng các trạm không biết do đó vẫn truyền dữ liệu.

• Để có thể phát hiện xung đột, CSMA/CD đã bổ xung thêm các quy tắc sau đây:

- Khi một trạm truyền dữ liệu, nó vẫn tiếp tục "nghe" đường truyền . Nếu phát hiện xung đột thì nó ngừng ngay việc truyền, nhờ đó mà tiết kiệm được thời gian và giải thông, nhưng nó vẫn tiếp tục gửi tín hiệu thêm một thời gian nữa để đảm bảo rằng tất cả các trạm trên mạng đều "nghe" được sự kiện này.(như vậy phải tiếp tục nghe đường truyền trong khi truyền để phát hiện đụng độ (Listening While Talking))

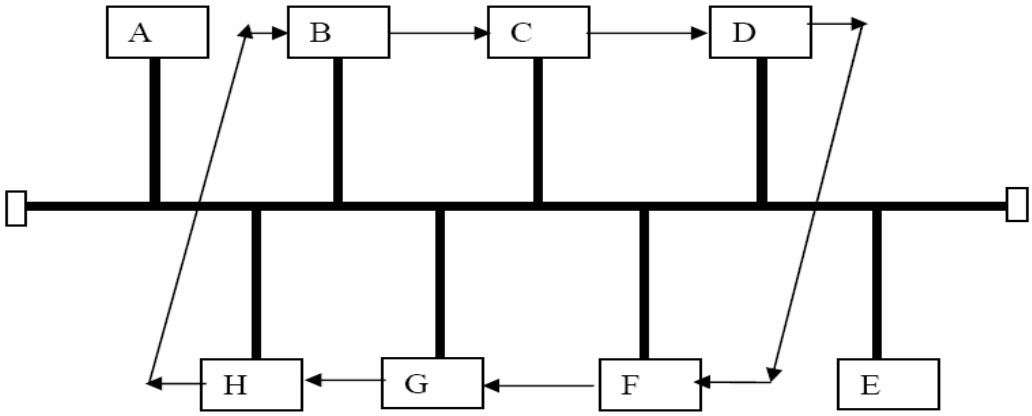
- Sau đó trạm sẽ chờ trong một khoảng thời gian ngẫu nhiên nào đó rồi thử truyền lại theo quy tắc CSMA.

Giao thức này gọi là **CSMA có phát hiện xung đột** (Carrier Sense Multiple Access with Collision Detection viết tắt là CSMA/CD), dùng rộng rãi trong LAN và MAN.

### 3.3.2. Phương pháp Token Bus

Nguyên lý chung của phương pháp này là để cấp phát quyền truy nhập đường truyền cho các trạm đang có nhu cầu truyền dữ liệu, một thẻ bài được lưu chuyển trên một vòng logic được thiết lập bởi các trạm đó. Khi một trạm nhận được thẻ bài thì sẽ được phép sử dụng đường truyền trong một thời gian nhất định. Trong khoảng thời gian đó nó có thể truyền một hay nhiều đơn vị dữ liệu. Khi đã truyền xong dữ liệu hoặc thời gian đã hết thì trạm đó phải chuyển thẻ bài cho trạm tiếp theo. Như vậy, công việc đầu tiên là thiết lập vòng logic (hay còn gọi là vòng ảo) bao gồm các trạm đang có nhu cầu truyền dữ liệu được xác định vị trí theo một chuỗi thứ tự mà trạm cuối cùng của chuỗi sẽ tiếp liền sau bởi trạm đầu tiên. Mỗi trạm sẽ biết địa chỉ của trạm liền trước và kề sau nó. Thứ tự của các trạm trên vòng logic có thể độc lập với thứ tự vật lý. Các trạm không hoặc chưa có nhu cầu truyền dữ liệu không được vào trong vòng logic.

Trong ví dụ trên, các trạm A, E nằm ngoài vòng logic do đó chỉ có thể tiếp nhận được dữ liệu dành cho chúng.




*Hình 1.5. Ví dụ về vòng logic*

Việc thiết lập vòng logic không khó nhưng việc duy trì nó theo trạng thái thực tế của mạng mới là khó. Cụ thể phải thực hiện các chức năng sau:

a) Bổ xung một trạm vào vòng logic : các trạm nằm ngoài vòng logic cần được xem xét một cách định kỳ để nếu có nhu cầu truyền dữ liệu thì được bổ xung vào vòng logic.

b) Loại bỏ một vòng khỏi vòng logic : khi một trạm không có nhu cầu truyền dữ liệu thì cần loại bỏ nó ra khỏi vòng logic để tối ưu hoá việc truyền dữ liệu bằng thẻ bài

c) Quản lý lỗi : một số lỗi có thể xẩy ra như trùng hợp địa chỉ, hoặc đứt vòng logic.

d) Khởi taọ vòng logic : khi khởi tạo mạng hoặc khi đứt vòng logic cần phải khởi tạo lại vòng logic.

### 3.3.3. Phương pháp Token Ring

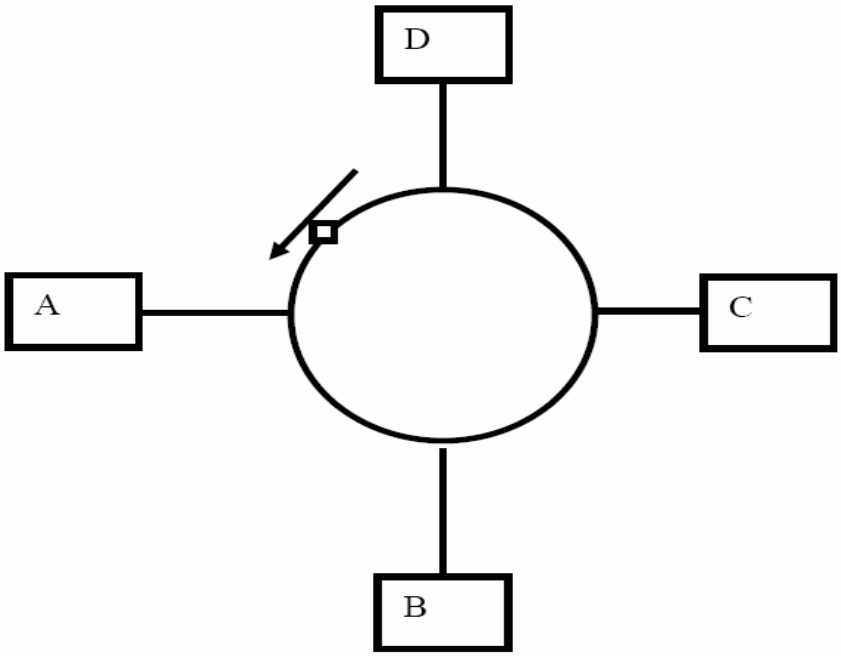
Phương pháp này cũng dựa trên nguyên tắc dùng thẻ bài để cấp phát quyền truy nhập đường truyền. Nhưng ở đây thẻ bài lưu chuyển theo theo vòng vật lý chứ không theo vòng logic như dối với phương pháp token bus.

Thẻ bài là một đơn vị truyền dữ liệu đặc biệt trong đó có một bit biểu diễn trạng thái của thẻ (bận hay rỗi). Một trạm muốn truyền dữ liệu phải chờ cho tới khi nhận được thẻ bài "rỗi". Khi đó trạm sẽ đổi bit trạng thái thành "bận" và truyền một đơn vị dữ liệu đi cùng với thẻ bài đi theo chiều của vòng. Lúc này không còn thẻ bài "rỗi " nữa do đó các trạm muốn truyền dữ liệu phải đợi. Dữ liệu tới trạm đích được sao chép lại, sau đó cùng với thẻ bài trở về trạm nguồn. Trạm nguồn sẽ xoá bỏ dữ liệu đổi bit trạng thái thành "rỗi" và cho lưu chuyển thẻ trên vòng để các trạm khác có nhu cầu truyền dữ liệu được phép truyền

Sự quay trở lại trạm nguồn của dữ liệu và thẻ bài nhằm tạo khả năng báo nhận tự nhiên: trạm đích có thể gửi vào đơn vị dữ liệu (phần header) các thông tin về kết quả tiếp nhận dữ liệu của mình. Chẳng hạn các thông tin đó có thể là: trạm đích không tồn tại hoặc không hoạt động, trạm đích tồn tại nhưng dữ liệu không được sao chép, dữ liệu đã được tiếp nhận, có lỗi...

Trong phương pháp này cần giải quyết hai vấn đề có thể dẫn đến phá vỡ hệ thống đó là mất thẻ bài và thẻ bài "bận" lưu chuyển không dừng trên vòng .Có nhiều phương pháp giải quyết các vấn đề trên, dưới đây là một phương pháp được khuyến nghị:

Đối với vấn đề mất thẻ bài có thể quy định trước một trạm điều khiển chủ động. Trạm này sẽ theo dõi, phát hiện tình trạng mất thẻ bài bằng cách dùng cơ




*Hình 1.6. Thẻ bài trong mạng* Ring

chế ngưỡng thời gian (time - out) và phục hồi bằng cách phát đi một thẻ bài "rỗi" mới.

Đối với vấn đề thẻ bài bận lưu chuyển không dừng, trạm điều khiển sử dụng một bit trên thẻ bài để đánh dấu khi gặp một thẻ bài "bận" đi qua nó. Nếu nó gặp lại thẻ bài bận với bit đã đánh dấu đó có nghĩa là trạm nguồn đã không nhận lại được đơn vị dữ liệu của mình do đó thẻ bài "bận" cứ quay vòng mãi. Lúc đó trạm điều khiển sẽ chủ động đổi bit trạng thái "bận" thành "rỗi" và cho thẻ bài chuyển tiếp trên vòng. Trong phương pháp này các trạm còn lại trên mạng sẽ đóng vai trò bị động, chúng theo dõi phát hiện tình trạng sự cố trên trạm chủ động và thay thế trạm chủ động nếu cần.

## IV. Chuẩn hoá mạng máy tính

### 4.1. Vấn đề chuẩn hoá mạng và các tổ chức chuẩn hoá mạng

Khi thiết kế, các nhà thiết kế tự do lựa chọn kiến trúc mạng cho riêng mình. Từ đó dẫn tới tình trạng không tương thích giữa các mạng máy tính với nhau. Nhu cầu trao đổi thông tin càng lớn thúc đẩy việc xây dựng khung chuẩn về kiến trúc mạng để làm căn cứ cho các nhà thiết kế và chế tạo thiết bị mạng.

Chính vì lý do đó, tổ chức tiêu chuẩn hoá quốc tế ISO (Internatinal Organnization for Standarzation) đã xây dựng mô hình tham chiếu cho việc kết nối các hệ thống mở OSI (reference model for Open Systems Interconnection). Mô hình này là cơ sở cho việc kết nối các hệ thống mở phục vụ cho các ứng dụng phân tán.

Có hai loại chuẩn cho mạng đó là :

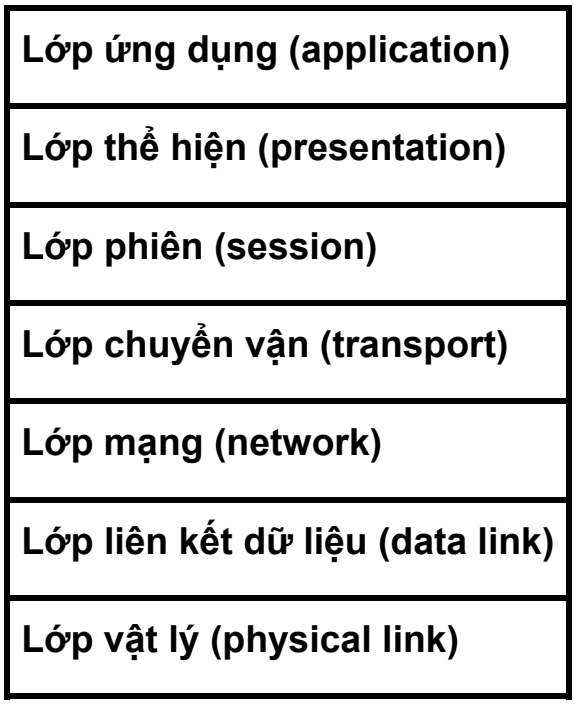
- Các chuẩn chính thức ( de jure ) do các tổ chức chuẩn quốc gia và quốc tế ban hành.

- Các chuẩn tực tiễn ( de facto ) do các hãng sản xuất, các tổ chức người sử dụng xây dựng và được dùng rộng rãi trong thực tế

### 4.2. Mô hình tham chiếu OSI 7 lớp

Khi thiết kế, các nhà thiết kế tự do lựa chọn kiến trúc mạng cho riêng mình. Từ đó dẫn tới tình trạng không tương thích giữa các mạng máy tính với nhau. Vấn đề không tương thích đó làm trở ngại cho sự tương tác giữa những người sử dụng mạng khác nhau. Nhu cầu trao đổi thông tin càng lớn thúc đẩy việc xây dựng khung chuẩn về kiến trúc mạng để làm căn cứ cho các nhà thiết kế và chế tạo thiết bị mạng .

Chính vì lý do đó, tổ chức tiêu chuẩn hoá quốc tế ISO (Internatinal Organnization for Standarzation) đã xây dựng mô hình tham chiếu cho việc kết nối các hệ thống mở OSI (reference model for Open Systems Interconnection). Mô hình này là cơ sở cho việc kết nối các hệ thống mở phục vụ cho các ứng dụng phân tán. Mô hình OSI được biểu diễn theo hình dưới đây:




Hình 1.7. Mô hình OSI 7 lớp

**a) Lớp vật lý**

Lớp này bảo đảm các công việc sau:

- Lập, cắt cuộc nối.
- Truyền tin dạng bit qua kênh vật lý.
- Có thể có nhiều kênh.

**b) Lớp liên kết dữ liệu**

Lớp này đảm bảo việc biến đổi các tin dạng bit nhận được từ lớp dưới (vật lý) sang khung số liệu, thông báo cho hệ phát, kết quả thu được sao cho các thông tin truyền lên cho mức 3 không có lỗi. Các thông tin truyền ở mức 1 có thể làm hỏng các thông tin khung số liệu (frame error). Phần mềm mức hai sẽ thông báo cho mức một truyền lại các thông tin bị mất / lỗi. Đồng bộ các hệ có tốc độ xử lý tính khác nhau, một trong những phương pháp hay sử dụng là dùng bộ đệm trung gian để lưu giữ số liệu nhận được. Độ lớn của bộ đệm này phụ thuộc vào tương quan xử lý của các hệ thu và phát. Trong trường hợp đường truyền song công toàn phần, lớp datalink phải đảm bảo việc quản lý các thông tin số liệu và các thông tin trạng thái.

**c) Lớp mạng**

Nhiệm vụ của lớp mạng là đảm bảo chuyển chính xác số liệu giữa các thiết bị cuối trong mạng. Để làm được việc đó, phải có chiến lược đánh địa chỉ thống nhất trong toàn mạng. Mỗi thiết bị cuối và thiết bị mạng có một địa chỉ

mạng xác định. Số liệu cần trao đổi giữa các thiết bị cuối được tổ chức thành các gói (packet) có độ dài thay đổi và được gán đầy đủ địa chỉ nguồn (source address) và địa chỉ đích (destination address).

Lớp mạng đảm bảo việc tìm đường tối ưu cho các gói dữ liệu bằng các giao thức chọn đường dựa trên các thiết bị chọn đường (router). Ngoài ra, lớp mạng có chức năng điều khiển lưu lượng số liệu trong mạng để tránh xảy ra tắc ngẽn bằng cách chọn các chiến lược tìm đường khác nhau để quyết định việc chuyển tiếp các gói số liệu.

**d) Lớp chuyển vận**

Lớp này thực hiện các chức năng nhận thông tin từ lớp phiên (**session**) chia thành các gói nhỏ hơn và truyền xuống lớp dưới, hoặc nhận thông tin từ lớp dưới chuyển lên phục hồi theo cách chia của hệ phát (Fragmentation and Reassembly). Nhiệm vụ quan trọng nhất của lớp vận chuyển là đảm bảo chuyển số liệu chính xác giữa hai thực thể thuộc lớp phiên (end-to-end control). Để làm được việc đó, ngoài chức năng kiểm tra số tuần tự phát, thu, kiểm tra và phát hiện, xử lý lỗi.Lớp vận chuyển còn có chức năng điều khiển lưu lượng số liệu để đồng bộ giữa thể thu và phát, tránh tắc nghẽn số liệu khi chuyển qua lớp mạng. Ngoài ra, nhiều thực thể lớp phiên có thể trao đổi số liệu trên cùng một kết nối lớp mạng (multiplexing).

**e) Lớp phiên**

Liên kết giữa hai thực thể có nhu cầu trao đổi số liệu, ví dụ người dùng và một máy tính ở xa, được gọi là một phiên làm việc. Nhiệm vụ của lớp phiên là quản lý việc trao đổi số liệu, ví dụ: thiết lập giao diện giữa người dùng và máy, xác định thông số điều khiển trao đổi số liệu (tốc độ truyền, số bit trong một byte, có kiểm tra lỗi parity hay không, v.v.), xác định loại giao thức mô phỏng thiết bị cuối (terminal emulation), v.v. Chức năng quan trọng nhất của lớp phiên là đảm bảo đồng bộ số liệu bằng cách thực hiện các điểm kiểm tra. Tại các điểm kiểm tra này, toàn bộ trạng thái và số liệu của phiên làm việc được lưu trữ trong bộ nhớ đệm. Khi có sự cố, có thể khởi tạo lại phiên làm việc từ điểm kiểm tra cuối cùng (không phải khởi tạo lại từ đầu).

**f) Lớp thể hiện**

Nhiệm vụ của lớp thể hiện là thích ứng các cấu trúc dữ liệu khác nhau của người dùng với cấu trúc dữ liệu thống nhất sử dụng trong mạng. Số liệu của người dùng có thể được nén và mã hoá ở lớp thể hiện, trước khi chuyển xuống lớp phiên. Ngoài ra, lớp thể hiện còn chứa các thư viện các yêu cầu của người dùng, thư viện tiện ích, ví dụ thay đổi dạng thể hiện của các tệp, nén tệp...

**g) Lớp ứng dụng**

Lớp ứng dụng cung cấp các phương tiện để người sử dụng có thể truy nhập được vào môi trường OSI, đồng thời cung cấp các dịch vụ thông tin phân

tán. Lớp mạng cho phép người dùng khai thác các tài nguyên trong mạng tương tự như tài nguyên tại chỗ.

### 4.3. Các chuẩn kết nối thông dụng nhất IEEE 802.X và ISO 8802.X

Bên cạnh việc chuẩn hoá cho mạng nối chung dẫn đến kết quả cơ bản nhất là mô hình tham chiếu OSI như đã giới thiệu. Việc chuẩn hoá mạng cục bộ nói riêng đã được thực hiện từ nhiều năm nay để đáp ứng sự phát triển của mạng cục bộ.

Cũng như đối với mạng nói chung, có hai loại chuẩn cho mạng cục bộ, đó là :

- Các chuẩn chính thức ( de jure ) do các tổ chức chuẩn quốc gia và quốc tế ban hành.
- Các chuẩn tực tiễn ( de facto ) do các hãng soản xuất, các tổ chức người sử dụng xây dựng và được dùng rộng rãi trong thực tế
- Các chuẩn IEEE 802.x và ISO 8802.x

IEEE là tổ chức đi tiên phong trong lĩnh vực chuẩn hoá mạng cục bộ với đề án IEEE 802 với kết quả là một loạt các chuẩn thuộc họ IEEE 802.x ra đời. Cuối những năm 80, tổ chức ISO đã tiếp nhận họ chuẩn này và ban hành thành chuẩn quốc tế dưới mã hiệu tương ứng là ISO 8802.x.

**IEEE 802.**: là chuẩn đặc tả kiến trúc mạng, kết nối giữa các mạng và việc quản trị mạng đối với mạng cục bộ.

**IEEE 802.2**: là chuẩn đặc tả tầng dịch vụ giao thức của mạng cục bộ.

**IEEE 802.3**: là chuẩn đặc tả một mạng cục bộ dựa trên mạng Ethernet nổi tiếng của Digital, Intel và Xerox hợp tác xây dựng từ năm 1980.

Tầng vật lý của IEEE 802.3 có thể dùng các phương án sau để xây dựng:

- 10BASE5 : tốc độ 10Mb/s, dùng cáp xoắn đôi không bọc kim UTP (Unshield Twisted Pair), với phạm vi tín hiệu lên tới 500m, topo mạng hình sao.

- 10BASE2 : tốc độ 10Mb/s, dùng cáp đồng trục thin-cable với trở kháng 50 Ohm, phạm vi tín hiệu 200m,topo mạng dạng bus.

- 10BASE5 : tốc độ 10Mb/s, dùng cáp đồng trục thick-cable (đường kính 10mm) với trở kháng 50 Ohm, phạm vi tín hiệu 500m, topo mạng dạng bus.

- 10BASE-F: dùng cáp quang, tốc độ 10Mb/s phạm vi cáp 2000m.

**IEEE 802.4**: là chuẩn đặc tả mạng cục bộ với topo mạng dạng bus dùng thẻ bài để điều việc truy nhập đường truyền.

**IEEE 802.5**: là chuẩn đặc tả mạng cục bộ với topo mạng dạng vòng (ring) dùng thẻ bài để điều việc truy nhập đường truyền.

**IEEE 802.6**: là chuẩn đặc tả mạng tốc độ cao kết nối với nhiều mạng cục bộ thuộc các khu vực khác nhau của một đô thị (còn được gọi là mạng MAN - Metropolitan Area Network)

**IEEE 802.9**: là chuẩn đặc tả mạng tích hợp dữ liệu và tiếng nói bao gồm 1 kênh dị bộ 10 Mb/s cùng với 96 kênh 64Kb/s. Chuẩn này được thiết kế cho môi trường có lượng lưu thông lớn và cấp bách.

**IEEE 802.10**: là chuẩn đặc tả về an toàn thông tin trong các mạng cục bộ có khả năng liên tác .

**IEEE 802.11**: là chuẩn đặc tả mạng cục bộ không dây (Wireless LAN) hiện đang được tiếp tục phát triển.

**IEEE 802.12**: là chuẩn đặc tả mạng cục bộ dựa trên công nghệ được đề xuất bởi AT&T, IBM và HP gọi là 100 VG - AnyLAN. Mạng này có topo mạng hình sao và một phương pháp truy nhập đường truyền có điều khiển tranh chấp. Khi có nhu cầu truyền dữ liệu, một trạm sẽ gửi yêu cầu đến hub và trạm chỉ có truyền dữ liệu khi hub cho phép.

# Chương 2. Các thiết bị mạng thông dụng và các chuẩn kết nối vật lý

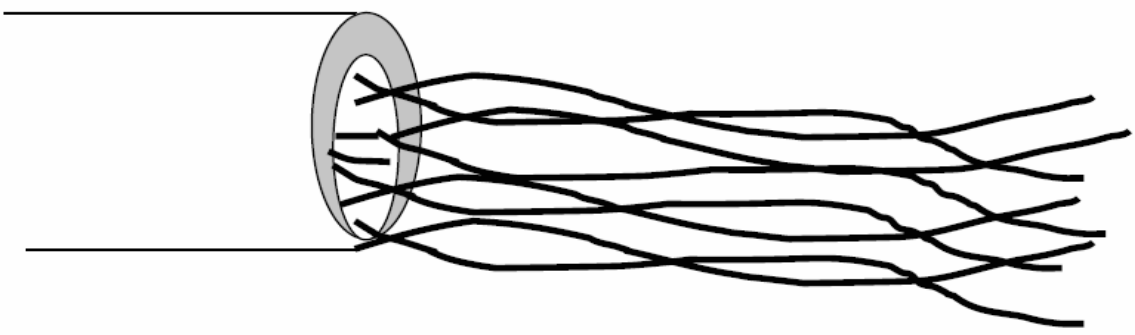
## I. Các thiết bị mạng thông dụng

### 1.1. Các loại cáp truyền

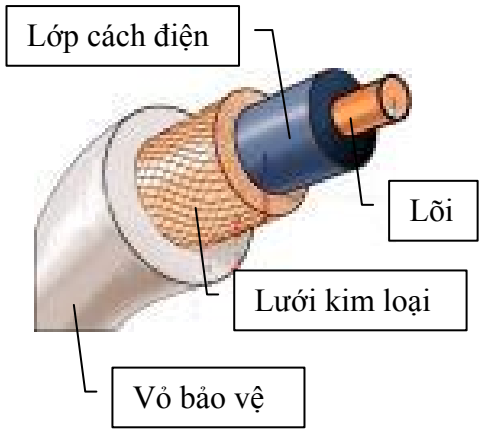
#### 1.1.1. Cáp đôi dây xoắn (Twisted pair cable)

Cáp đôi dây xoắn là cáp gồm hai dây đồng xoắn để tránh gây nhiễu cho các đôi dây khác, có thể kéo dài tới vài km mà không cần khuyếch đại. Giải tần trên cáp dây xoắn đạt khoảng 300–4000Hz, tốc độ truyền đạt vài kbps đến vài trăm Mbps. Cáp xoắn có hai loại:

- Loại có bọc kim loại để tăng cường chống nhiễu gọi là cap STP (Shield Twisted Pair). Loại này trong vỏ bọc kim có thể có nhiều đôi dây. Về lý thuyết thì tốc độ truyền có thể đạt 500 Mb/s nhưng thực tế thấp hơn rất nhiều (chỉ đạt 155 Mbps với cáp dài 100 m)



Hình 2.1 Cáp UTP CAT 5



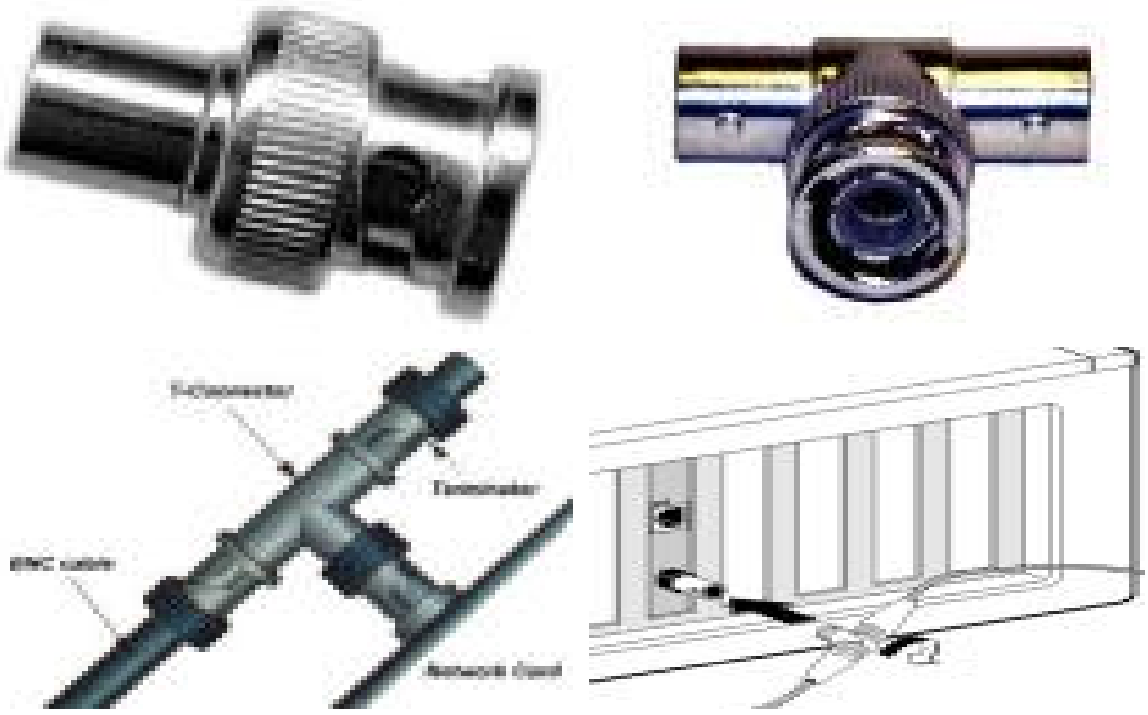

Hình 2.2 Cáp đồng trục

- Loại không bọc kim gọi là UTP (UnShield Twisted Pair), chất lượng kém hơn STP nhưng rất rẻ. Cap UTP được chia làm 5 hạng tuỳ theo tốc độ truyền. Cáp loại 3 dùng cho điện thoại. Cáp loại 5 có thể truyền với tốc độ 100Mb/s rất hay dùng trong các mạng cục bộ vì vừa rẻ vừa tiện sử dụng. Cáp này có 4 đôi dây xoắn nằm trong cùng một vỏ bọc

### 1.1.2. Cáp đồng trục (Coaxial cable) băng tần cơ sở

Là cáp mà hai dây của nó có lõi lồng nhau, lõi ngoài là lưới kim loại. , Khả năng chống nhiễu rất tốt nên có thể sử dụng với chiều dài từ vài trăm met đến vài km. Có hai loại được dùng nhiều là loại có trở kháng 50 ohm và loại có trở kháng 75 ohm

Dải thông của cáp này còn phụ thuộc vào chiều dài của cáp. Với khoảng cách1 km có thể đạt tốc độ truyền từ 1– 2 Gbps. Cáp đồng trục băng tần cơ sở thường dùng cho các mạng cục bộ. Có thể nối cáp bằng các đầu nối theo chuẩn BNC có hình chữ T. ở VN người ta hay gọi cáp này là cáp gầy do dịch từ tên trong tiếng Anh là ‘Thin Ethernet”.

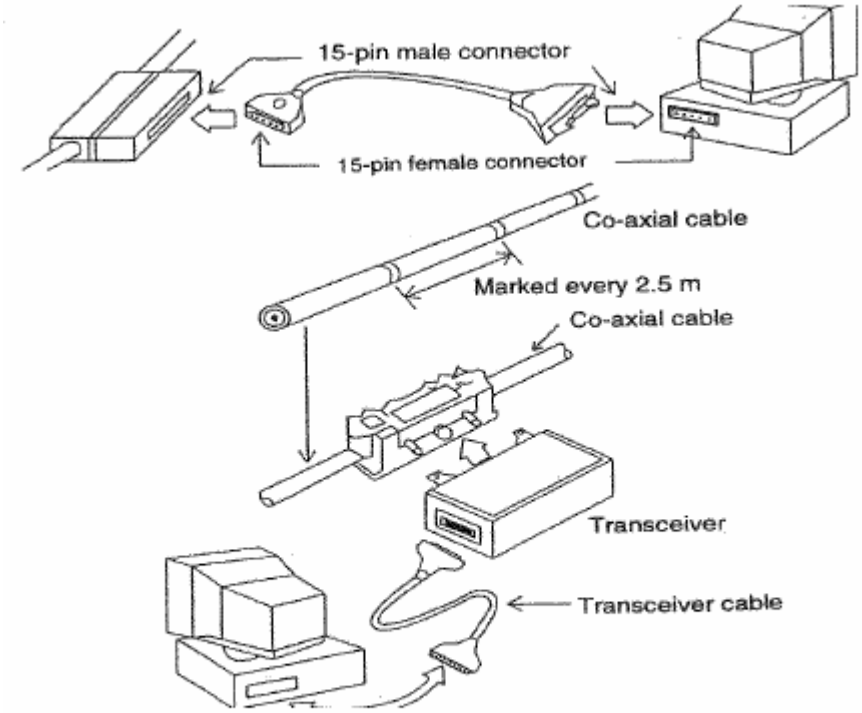


Một loại cáp khác có tên là “Thick Ethernet” mà ta gọi là cáp béo. Loại này thường có màu vàng. Người ta không nối cáp bằng các đầu nối chữ T như cáp gầy mà nối qua các kẹp bấm vào dây. Cứ 2m5 lại có đánh dấu để nối dây

(nếu cần). Từ kẹp đó người ta gắn các tranceiver rồi nối vào máy tính. (Xem hình 2.3)

### 1.1.3. Cáp đồng trục băng rộng (Broadband Coaxial Cable)

Đây là loại cáp theo tiêu chuẩn truyền hình (thường dùng trong truyền hình cap) có giải thông từ 4 – 300 Khz trên chiều dài 100 km. Thuật ngữ "băng rộng" vốn là thuật ngữ của ngành truyền hình còn trong ngành truyền số liệu điều này chỉ có nghĩa là cáp loại này cho phép truyền thông tin tương tự (analog) mà thôi. Các hệ thống dựa trên cáp đồng trục băng rộng có thể truyền song song nhiều kênh. Việc khuyếch đại tín hiệu chống suy hao có thể làm theo kiểu khuyếch đại tín hiệu tương tự (analog). Để truyền thông cho máy tính cần chuyển tín hiệu số thành tín hiệu tương tự.




Hình 2.3 Kết nối bằng Traceiver

### 1.1.4. Cáp quang

Dùng để truyền các xung ánh sáng trong lòng một sợi thuỷ tinh phản xạ toàn phần. Môi trường cáp quang rất lý tưởng vì

- Xung ánh sáng có thể đi hàng trăm km mà không giảm cường độ sáng.

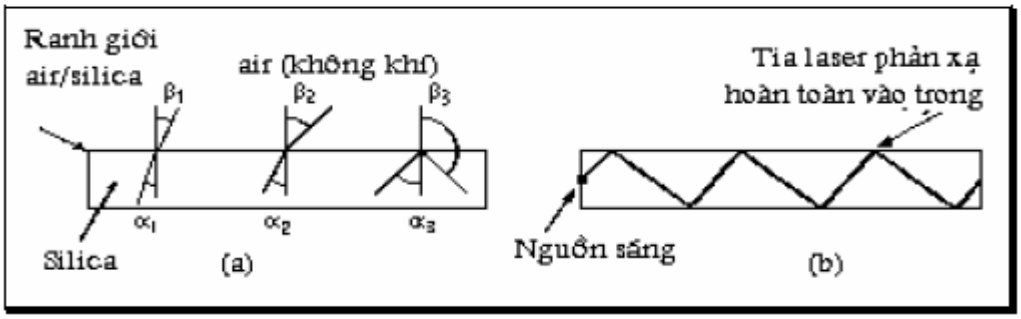
- Giải thông rất cao vì tần số ánh sáng dùng đối với cáp quang cỡ khoảng 1014 –1016

- An toàn và bí mật

- Không bị nhiễu điện từ

Chỉ có hai nhược điểm là khó nối dây và giá thành cao.

Để phát xung ánh sáng người ta dùng các đèn LED hoặc các diod laser. Để nhận người ta dùng các photo diode , chúng sẽ tạo ra xung điện khi bắt được xung ánh sáng




Hình 2.4. Truyền tín hiệu bằng cáp quang

Cáp quang cũng có hai loại

- Loại đa mode (multi mode fiber): khi góc tới thành dây dẫn lớn đến một mức nào đó thì có hiện tượng phản xạ toàn phần. Nhiều tia sáng có thể cùng truyền miễn là góc tới của chúng đủ lớn. Các cap đa mode có đường kính khoảng 50 µ

- Loại đơn mode (single mode fiber): khi đường kính dây dẫn bằng bước sóng thì cáp quang giống như một ống dẫn sóng, không có hiện tượng phản xạ nhưng chỉ cho một tia đi. Loại này có đường kính khoản 8 µ và phải dùng diode laser. Cáp quang đơn mode có thể cho phép truyền xa tới hàng trăm km mà không cần phải khuyếch đại.

## 1.2. Các thiết bị ghép nối

### 1.2.1. Card giao tiếp mạng (Network Interface Card viết tắt là NIC)

Đó là một card được cắm trực tiếp vào máy tính. Trên đó có các mạch điện giúp cho việc tiếp nhận (receiver) hoặc/và phát (transmitter) tín hiệu lên mạng. Người ta thường dùng từ tranceiver để chỉ thiết bị (mạch) có cả hai chức năng thu và phát. Transceiver có nhiều loại vì phải thích hợp đối với cả môi trường truyền và do đó cả đầu nối. Ví dụ với cáp gầy card mạng cần có đường giao tiếp theo kiểu BNC, với cáp UTP cần có đầu nối theo kiểu giắc điện thoại RJ45, cáp béo dùng đường nối kiểu AUI , với cáp quang phải có những transceiver cho phép chuyển tín hiệu điện thành các xung ánh sáng và ngược lại.

Để dễ ghép nối, nhiều card có thể có nhiều đầu nối ví dụ BNC cho cáp gầy, RJ45 cho UTP hay AUI cho cáp béo

Trong máy tính thường để sẵn các khe cắm để bổ sung các thiết bị ngoại vi hay cắm các thiết bị ghép nối.

### 1.2.2. Bộ chuyển tiếp (REPEATER )

Tín hiệu truyền trên các khoảng cách lớn có thể bị suy giảm. Nhiệm vụ của các repeater là hồi phục tín hiệu để có thể truyền tiếp cho các trạm khác. Một số repeater đơn giản chỉ là khuyếch đại tín hiệu. Trong trường hợp đó cả tín hiệu bị méo cũng sẽ bị khuyếch đại. Một số repeater có thể chỉnh cả tín hiệu.

### 1.2.3. Các bộ tập trung (Concentrator hay HUB)

HUB là một loại thiết bị có nhiều đầu để cắm các đầu cáp mạng. HUB có thể có nhiều loại ổ cắm khác nhau phù hợp với kiểu giắc mạng RJ45, AUI hay BCN. Như vậy người ta sử dụng HUB để nối dây theo kiểu hình sao. Ưu điểm của kiểu nối này là tăng độ độc lập của các máy . Nếu dây nối tới một máy nào đó tiếp xúc không tốt cũng không ảnh hưởng đến máy khác.

Đặc tính chủ yếu của HUB là hệ thống chuyển mạch trung tâm trong mạng có kiến trúc hình sao với việc chuyển mạch được thực hiện theo hai cách: store-and-forward hoặc on-the-fly. Tuy nhiên hệ thống chuyển mạch trung tâm làm nảy sinh vấn đề khi lỗi xảy ra ở chính trung tâm, vì vậy hướng phát triển trong suốt nhiều năm qua là khử lỗi để làm tăng độ tin cậy của HUB.

Có loại HUB thụ động (passive HUB) là HUB chỉ đảm bảo chức năng kết nối hoàn toàn không xử lý lại tín hiệu. Khi đó không thể dùng HUB để tăng khoảng cách giữa hai máy trên mạng.

HUB chủ động (active HUB) là HUB có chức năng khuyếch đại tín hiệu để chống suy hao. Với HUB này có thể tăng khoảng cách truyền giữa các máy.

HUB thông minh (intelligent HUB) là HUB chủ động nhưng có khả năng tạo ra các gói tin mang tin tức về hoạt động của mình và gửi lên mạng để người quản trị mạng có thể thực hiện quản trị tự động

### 1.2.4. Switching Hub (hay còn gọi tắt là switch)

Là các bộ chuyển mạch thực sự. Khác với HUB thông thường, thay vì chuyển một tín hiệu đến từ một cổng cho tất cả các cổng, nó chỉ chuyển tín hiệu đến cổng có trạm đích. Do vậy Switch là một thiết bị quan trọng trong các mạng cục bộ lớn dùng để phân đoạn mạng. Nhờ có switch mà đụng độ trên mạng giảm hẳn. Ngày nay switch là các thiết bị mạng quan trọng cho phép tuỳ biến trên mạng chẳng hạn lập mạng ảo.

Switch thực chất là một loại bridge, về tính năng kỹ thuật, nó là loại bridge có độ trễ nhỏ nhất. Khác với bridge là phải đợi đến hết frame rồi mới truyền, switch sẽ chờ cho đến khi nhận được địa chỉ đích của frame gửi tới và lập tức được truyền đi ngay. Điều này có nghĩa là frame sẽ được gửi tới LAN cần gửi trước khi nó được switch nhận xong hoàn toàn.

### 1.2.5. Modem

Là tên viết tắt từ hai từ điều chế (MOdulation) và giải điều chế (DEModulation) là thiết bị cho phép điều chế để biến đổi tín hiệu số sang tín hiệu tương tự để có thể gửi theo đường thoại và khi nhận tín hiệu từ đường thoại có thể biến đổi ngược lại thành tín hiệu số. Tuy nhiên có thể sử dụng nó theo kiểu kết nối từ xa theo đường điện thoại

### 1.2.6. Router

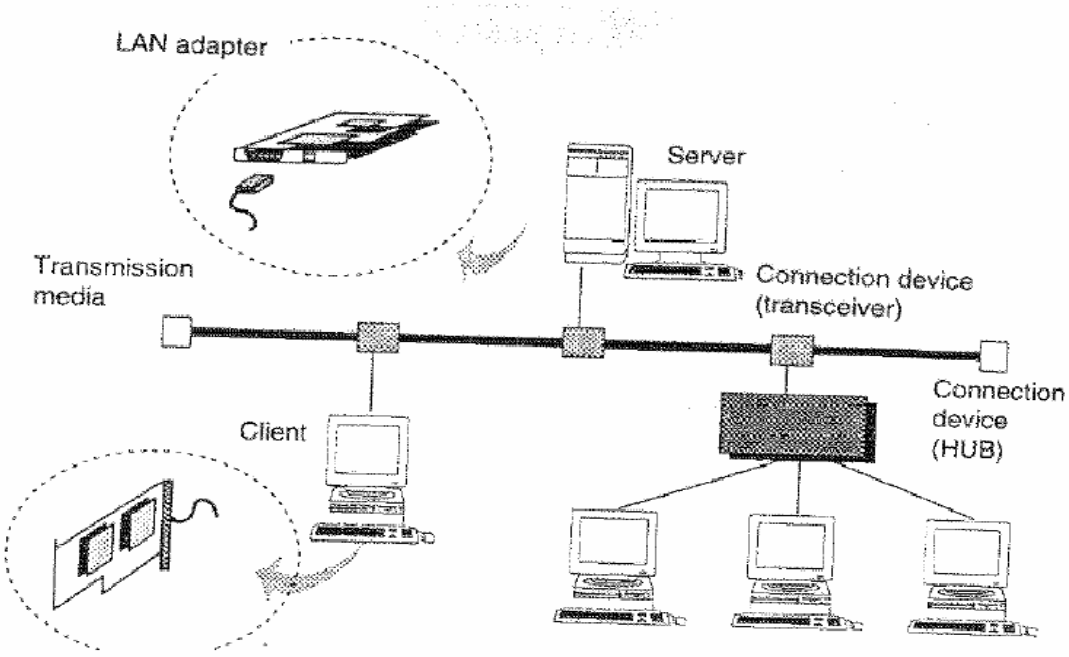
Router là một thiết bị không phải để ghép nối giữa các thiết bị trong một mạng cục bộ mà dùng để ghép nối các mạng cục bộ với nhau thành mạng rộng. Router thực sự là một máy tính làm nhiệm vụ chọn đường cho các gói tin hướng ra ngoài.

Khác với repeaters và bridges, router là thiết bị kết nối mạng độc lập phần cứng, nó được dùng để kết nối các mạng có cùng chung giao thức. Chức năng cơ bản nhất của router là cung cấp một môi trường chuyển mạch gói (packet switching) đáng tin cậy để lưu trữ và truyền số liệu. Để thực hiện điều đó, nó thiết lập các thông tin về các đường truyền hiện có trong mạng, và khi cần nó sẽ cung cấp hai hay nhiều đường truyền giữa hai mạng con bất kỳ tạo ra khả năng mềm dẻo trong việc tìm đường đi hợp lý nhất về một phương diện nào đó.

## 1.3. Một số kiểu nối mạng thông dụng và các chuẩn

### 1.3.1.Các thành phần thông thường trên một mạng cục bộ gồm có

- Các máy chủ cung cấp dịch vụ (server)
- Các máy trạm cho người làm việc (workstation)
- Đường truyền (cáp nối)
- Card giao tiếp giữa máy tính và đường truyền (network interface card)
- Các thiết bị nối (connection device)




Hình 2.6. Cấu hình của một mạng cục bộ

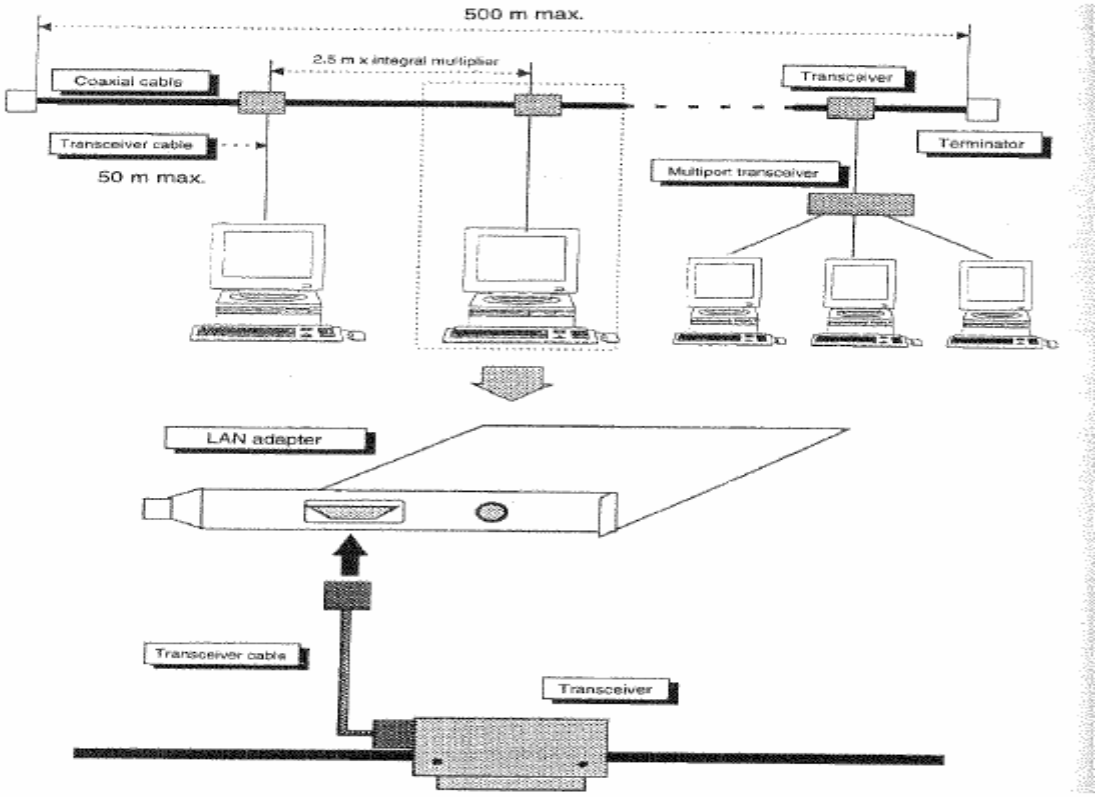
Hai yếu tố được quan tâm hàng đầu khi kết nối mạng cục bộ là tốc độ trong mạng và bán kính mạng. Tên các kiểu mạng dùng theo giao thức CSMA/CD cũng thể hiện điều này. Sau đây là một số kiểu kết nối đó với tốc độ 10 Mb/s khá thông dụng trong thời gian qua và một số thông số kỹ thuật:

| Chuẩn | IEEE 802.3 | | |
|---|---|---|---|
| Kiểu | 10BASE5 | 10BASE2 | 10BASE-T |
| Kiểu cáp | Cáp đồng trục | Cáp đồng trục | Cáp UTP |
| Tốc độ | 10 Mb/s | | |
| Độ dài cáp tối đa | 500 m/segment | 185 m/segment | 100 m kể từ HUB |
| Số các thực thể truyền thông | 100 host /segment | 30 host / segment | Số cổng của HUB |

### 1.3.2. Kiểu 10BASE5:

Là chuẩn CSMA/CD có tốc độ 10Mb và bán kính 500 m. Kiểu này dùng cáp đồng trục loại thick ethernet (cáp đồng trục béo) với tranceiver. Có thể kết nối vào mạng khoảng 100 máy

Tranceiver:Thiết bị nối giữa card mạng và đường truyền, đóng vai trò là bộ thu-phát




Hình 2.7 Kết nối theo chuẩn 10BASE5

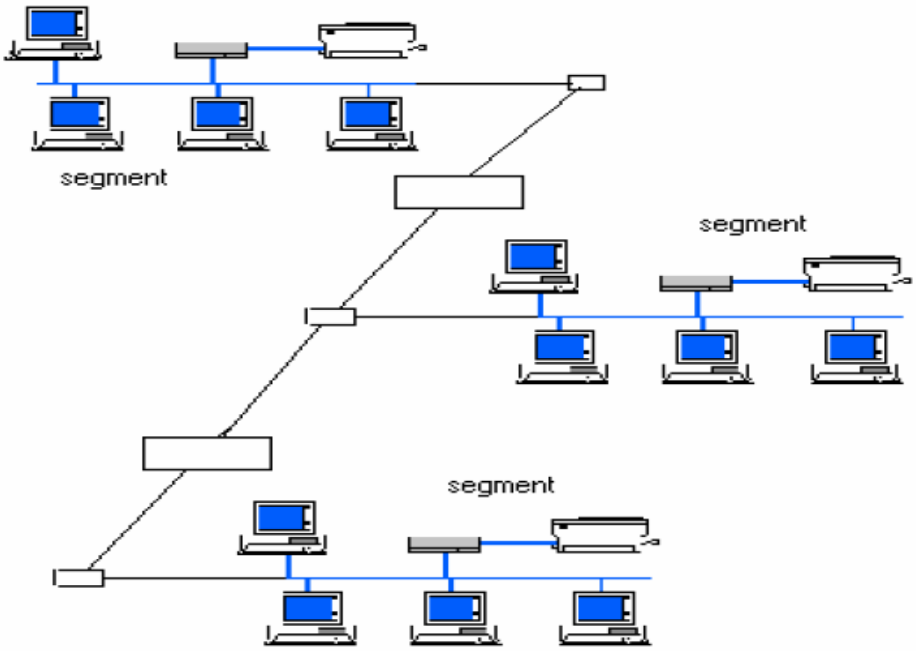
Đặc điểm của chuẩn 10BASE 5

| | |
|---|---|
| Tốc độ tối đa | 10 Mbps |
| Chiều dài tối đa của đoạn cáp của một phân đoạn (segment) | 500 m |
| Số trạm tối đa trên mỗi đoạn | 100 |
| Khoảng cách giữa các trạm | >=2,5 m (bội số của 2,5 m (giảm thiểu hiện tượng giao thoa do sóng đứng trên các đoạn ?)) |
| Khoảng cách tối đa giữa máy trạm và đường trục chung | 50 m |
| Số đoạn kết nối tối đa | 2 (=>tối đa có 3 phân đoạn) |

| | |
|---|---|
| Tổng chiều dài tối đa đoạn kết nối (có thể là một đoạn kết nối khi có hai phân đoạn, hoặc hai đoạn kết nối khi có ba phân đoạn) | 1000 m |
| Tổng số trạm + các bộ lặp Repeater | Không quá 1024 |
| Chiều dài tối đa | 3*500+1000=2500 m |

### 1.3.3. Kiểu 10BASE2:

Là chuẩn CSMA/CD có tốc độ 10Mb và bán kính 200 m. Kiểu này dùng cáp đồng trục loại thin ethernet với đầu nối BNC. Có thể kết nối vào mạng khoảng 30 máy

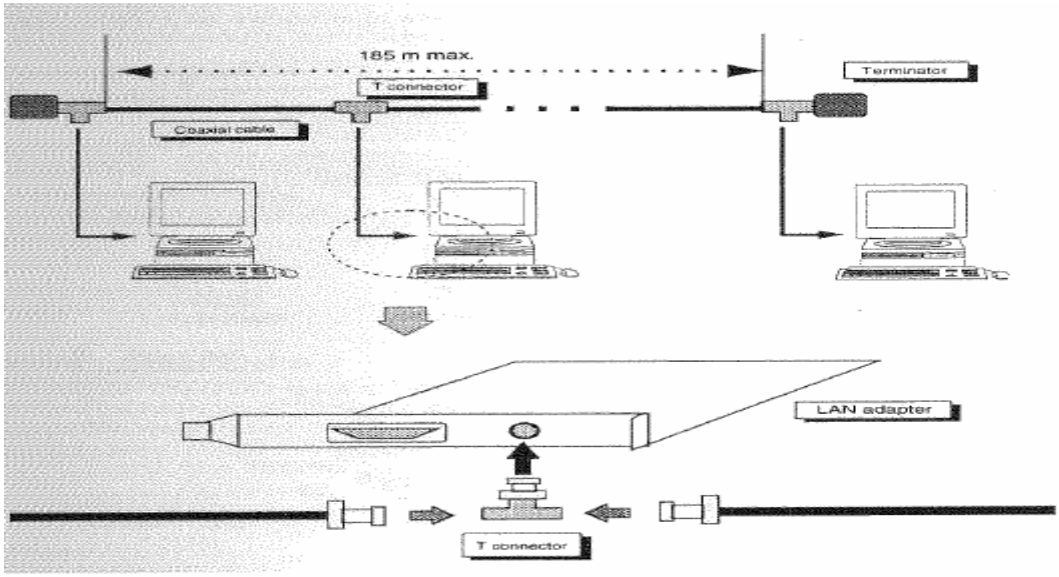



Hình 2.8 Kết nối tối đa 3 phân đoạn mạng

Đặc điểm của chuẩn 10BASE 2

| | |
|---|---|
| Tốc độ tối đa | 10 Mbps |
| Chiều dài tối đa của đoạn cáp của một phân đoạn (segment) | 185 m |
| Số trạm tối đa trên mỗi đoạn | 30 |
| Khoảng cách giữa các trạm | >=0,5 m |

| | |
|---|---|
| Khoảng cách tối đa giữa máy trạm và đường trục chung | 0 m |
| Số đoạn kết nối tối đa | 2 (=>tối đa có 3 phân đoạn) |
| Tổng chiều dài tối đa đoạn kết nối (có thể là một đoạn kết nối khi có hai phân đoạn, hoặc hai đoạn kết nối khi có ba phân đoạn) | 1000 m |
| Tổng số trạm + các bộ lặp Repeater | Không quá 1024 |



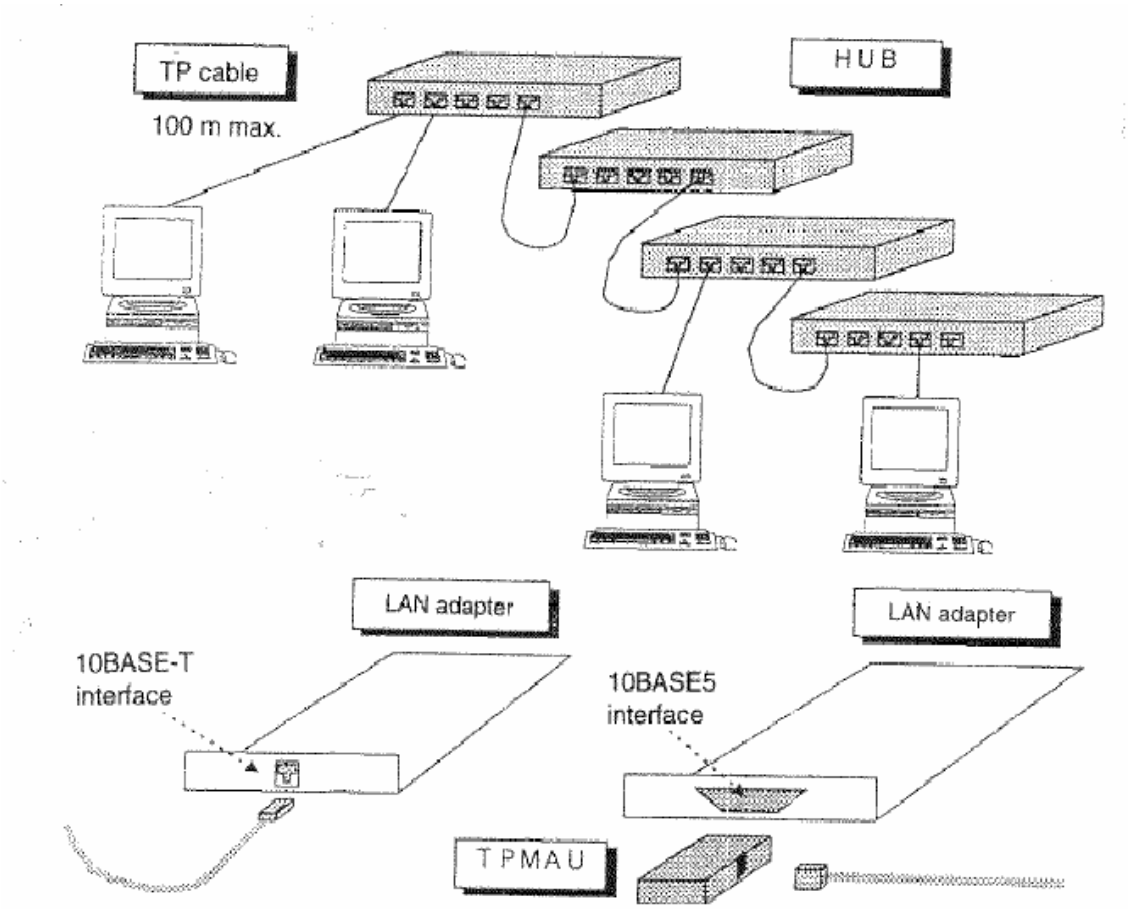

Hình 2.9 Nối theo chuẩn 10BASE2 với cáp đồng trục và đầu nối BNC

### 1.3.4. Kiểu 10BASE-T

Là kiểu nối dùng HUB có các ổ nối kiểu RJ45 cho các cáp UTP. Ta có thể mở rộng mạng bằng cách tăng số HUB, nhưng cũng không được tăng quá nhiều tầng vì hoạt động của mạng sẽ kém hiệu quả nếu độ trễ quá lớn .

| | |
|---|---|
| Tốc độ tối đa | 10 Mbps |
| Chiều dài tối đa của đoạn cáp nối giữa máy tính và bộ tập trung HUB | 100 m |

Hiện nay mô hình phiên bản 100BASE-T bắt đầu được sử dụng nhiều, tốc độ đạt tới 100 Mbps, với card mạng, cab mạng, hub đều phải tuân theo chuẩn 100BASE-T.




Hình 2.10 Nối mạng theo kiểu 10BASE-T với cáp UTP và HUB

### 1.3.5. Kiểu 10BASE-F

Dùng cab quang (Fiber cab), chủ yếu dùng nối các thiết bị xa nhau, tạo dựng đường trục xương sống (backborn) để nối các mạng LAN xa nhau (2-10 km)

## Chương 3. Giới thiệu giao thức TCP/IP

Chương ba cung cấp các kiến thức liên quan đến TCP/IP và địa chỉ IP. Giao thức TCP/IP trở thành giao thức mạng phổ biến nhất nhờ sự phát triển không ngừng của mạng Internet. Các mạng máy tính của các cơ quan, tổ chức, công ty hầu hết đều sử dụng TCP/IP làm giao thức mạng nhờ tính dễ mở rộng và qui hoạch của nó. Đồng thời, do sự phát triển của mạng Internet nên nhu cầu kết nối ra Internet và sử dụng TCP/IP đã trở nên thiết yếu cho mọi đối tượng

Chương này đòi hỏi các học viên phải quen thuộc với các kiến thức cơ bản về hệ nhị phân, các khái niệm bit, byte, chuyển đổi nhị phân, thập phân. Các cách biểu diễn cấu trúc gói tin theo dạng trường bit, byte cũng yêu cầu học viên phải có được hiểu biết cơ sở về kỹ thuật thông tin truyền thông.

# I. Giao thức IP

## 1.1. Họ giao thức TCP/IP

Sự ra đời của họ giao thức TCP/IP gắn liền với sự ra đời của Internet mà tiền thân là mạng **ARPA**net (**A**dvanced **R**esearch **P**rojects **A**gency) do Bộ Quốc phòng Mỹ tạo ra. Đây là bộ giao thức được dùng rộng rãi nhất vì tính mở của nó. Điều đó có nghĩa là bất cứ máy nào dùng bộ giao thức TCP/IP đều có thể nối được vào Internet. Hai giao thức được dùng chủ yếu ở đây là **TCP** (**T**ransmission **C**ontrol **P**rotocol) và **IP** (**I**nternet **P**rotocol). Chúng đã nhanh chóng được đón nhận và phát triển bởi nhiều nhà nghiên cứu và các hãng công nghiệp máy tính với mục đích xây dựng và phát triển một mạng truyền thông mở rộng khắp thế giới mà ngày nay chúng ta gọi là Internet. Phạm vi phục vụ của Internet không còn dành cho quân sự như **ARPA**net nữa mà nó đã mở rộng lĩnh vực cho mọi loại đối tượng sử dụng, trong đó tỷ lệ quan trọng nhất vẫn thuộc về giới nghiên cứu khoa học và giáo dục.

Khái niệm *giao thức (*protocol) là một khái niệm cơ bản của mạng thông tin máy tính. Có thể hiểu một cách khái quát rằng đó chính là tập hợp tất cả các qui tắc cần thiết (các thủ tục, các khuôn dạng dữ liệu, các cơ chế phụ trợ...) cho phép các thao tác trao đổi thông tin trên mạng được thực hiện một cách chính xác và an toàn. Có rất nhiều họ giao thức đang được thực hiện trên mạng thông tin máy tính hiện nay như IEEE 802.X dùng trong mạng cục bộ, CCITT X25 dùng cho mạng diện rộng và đặc biệt là họ giao thức chuẩn của ISO (tổ chức tiêu chuẩn hóa quốc tế) dựa trên mô hình tham chiếu bảy tầng cho việc nối kết các hệ thống mở. Gần đây, do sự xâm nhập của Internet vào Việt nam, chúng ta được làm quen với họ giao thức mới là TCP/IP mặc dù chúng đã xuất hiện từ hơn 20 năm trước đây.

TCP/IP (Transmission Control Protocol/ Internet Protocol) TCP/IP là một họ giao thức cùng làm việc với nhau để cung cấp phương tiện truyền thông liên mạng được hình thành từ những năm 70.

Đến năm 1981, TCP/IP phiên bản 4 mới hoàn tất và được phổ biến rộng rãi cho toàn bộ những máy tính sử dụng hệ điều hành UNIX. Sau này Microsoft cũng đã đưa TCP/IP trở thành một trong những giao thức căn bản của hệ điều hành Windows 9x mà hiện nay đang sử dụng.

Đến năm 1994, một bản thảo của phiên bản IPv6 được hình thành với sự cộng tác của nhiều nhà khoa học thuộc các tổ chức Internet trên thế giới để cải tiến những hạn chế của IPv4.

Khác với mô hình ISO/OSI tầng liên mạng sử dụng giao thức kết nối mạng "không liên kết" (connectionless) IP, tạo thành hạt nhân hoạt động của Internet. Cùng với các thuật toán định tuyến RIP, OSPF, BGP, tầng liên mạng IP cho phép kết nối một cách mềm dẻo và linh hoạt các loại mạng "vật lý" khác nhau như: Ethernet, Token Ring , X.25...

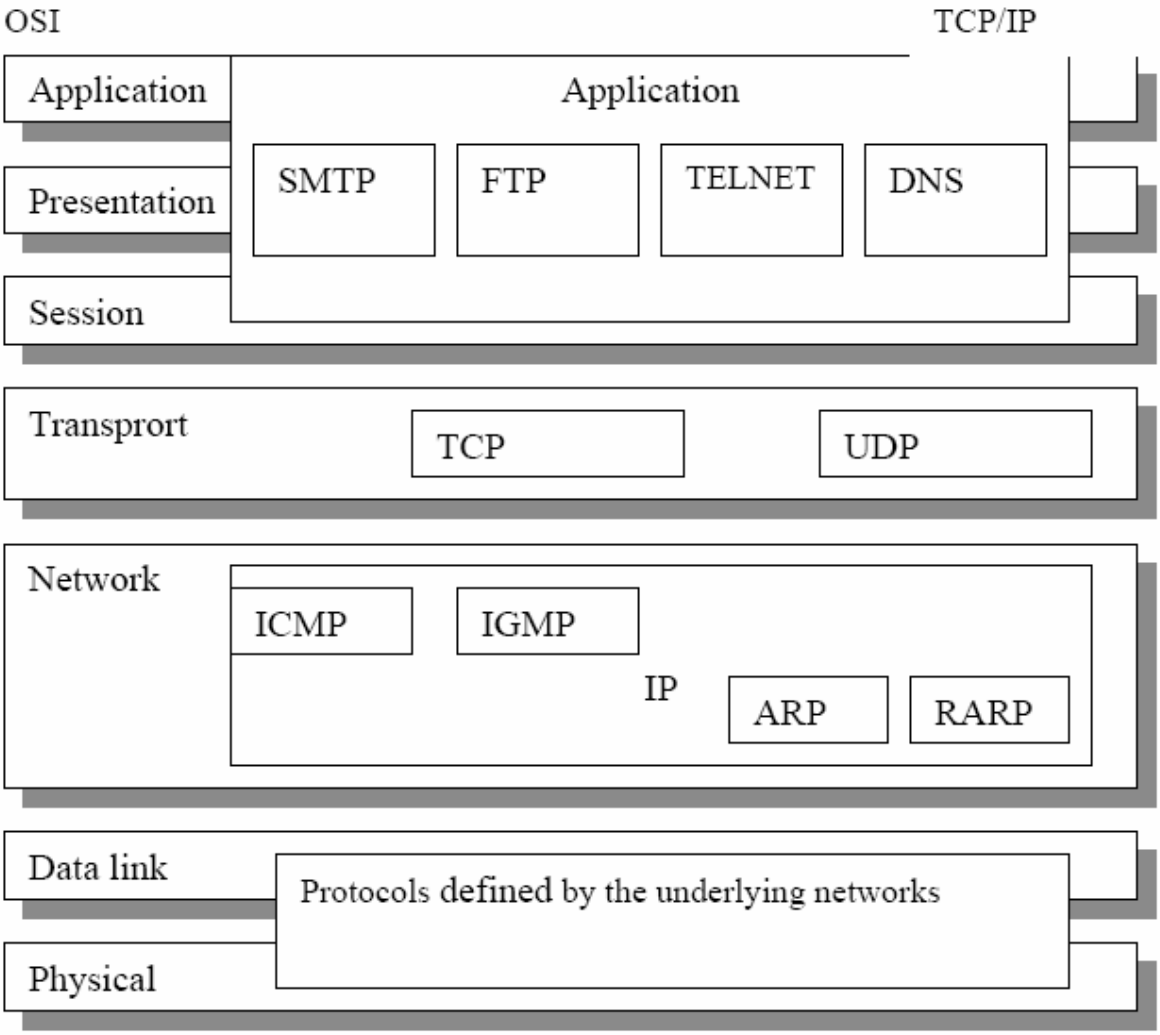
Giao thức trao đổi dữ liệu "có liên kết" (connection - oriented) TCP được sử dụng ở tầng vận chuyển để đảm bảo tính chính xác và tin cậy việc trao đổi dữ liệu dựa trên kiến trúc kết nối "không liên kết" ở tầng liên mạng IP.

Các giao thức hỗ trợ ứng dụng phổ biến như truy nhập từ xa (telnet), chuyển tệp (FTP), dịch vụ World Wide Web (HTTP), thư điện tử (SMTP), dịch vụ tên miền (DNS) ngày càng được cài đặt phổ biến như những bộ phận cấu thành của các hệ điều hành thông dụng như UNIX (và các hệ điều hành chuyên dụng cùng họ của các nhà cung cấp thiết bị tính toán như AIX của IBM, SINIX của Siemens, Digital UNIX của DEC), Windows9x/NT, Novell Netware,...

Như vậy, TCP tương ứng với lớp 4 cộng thêm một số chức năng của lớp 5 trong họ giao thức chuẩn ISO/OSI. Còn IP tương ứng với lớp 3 của mô hình OSI.

Trong cấu trúc bốn lớp của TCP/IP, khi dữ liệu truyền từ lớp ứng dụng cho đến lớp vật lý, mỗi lớp đều cộng thêm vào phần điều khiển của mình để đảm bảo cho việc truyền dữ liệu được chính xác. Mỗi thông tin điều khiển này được gọi là một header và được đặt ở trước phần dữ liệu được truyền. Mỗi lớp xem tất cả các thông tin mà nó nhận được từ lớp trên là dữ liệu, và đặt phần thông tin điều khiển header của nó vào trước phần thông tin này. Việc cộng thêm vào các header ở mỗi lớp trong quá trình truyền tin được gọi là encapsulation. Quá trình nhận dữ liệu diễn ra theo chiều ngược lại: mỗi lớp sẽ tách ra phần header trước khi truyền dữ liệu lên lớp trên.

Mỗi lớp có một cấu trúc dữ liệu riêng, độc lập với cấu trúc dữ liệu được dùng ở lớp trên hay lớp dưới của nó. Sau đây là giải thích một số khái niệm thường gặp.




Hình 3.1 Mô hình OSI và mô hình kiến trúc của TCP/IP

Stream là dòng số liệu được truyền trên cơ sở đơn vị số liệu là Byte.

Số liệu được trao đổi giữa các ứng dụng dùng TCP được gọi là stream, trong khi dùng UDP, chúng được gọi là message.

Mỗi gói số liệu TCP được gọi là segment còn UDP định nghĩa cấu trúc dữ liệu của nó là packet.

Lớp Internet xem tất cả các dữ liệu như là các khối và gọi là datagram. Bộ giao thức TCP/IP có thể dùng nhiều kiểu khác nhau của lớp mạng dưới cùng, mỗi loại có thể có một thuật ngữ khác nhau để truyền dữ liệu.

Phần lớn các mạng kết cấu phần dữ liệu truyền đi dưới dạng các packets hay là các frames.

| | |
|---|---|
| Application | Stream |
| Transport | Segment/datagram |
| Internet | Datagram |
| Network Access | Frame |

Hình 3.2 Cấu trúc dữ liệu tại các lớp của TCP/IP

**Lớp truy nhập mạng**

Network Access Layer là lớp thấp nhất trong cấu trúc phân bậc của TCP/IP. Những giao thức ở lớp này cung cấp cho hệ thống phương thức để truyền dữ liệu trên các tầng vật lý khác nhau của mạng. Nó định nghĩa cách thức truyền các khối dữ liệu (datagram) IP. Các giao thức ở lớp này phải biết chi tiết các phần cấu trúc vật lý mạng ở dưới nó (bao gồm cấu trúc gói số liệu, cấu trúc địa chỉ...) để định dạng được chính xác các gói dữ liệu sẽ được truyền trong từng loại mạng cụ thể.

So sánh với cấu trúc OSI/OSI, lớp này của TCP/IP tương đương với hai lớp Datalink, và Physical.

Chức năng định dạng dữ liệu sẽ được truyền ở lớp này bao gồm việc nhúng các gói dữ liệu IP vào các frame sẽ được truyền trên mạng và việc ánh xạ các địa chỉ IP vào địa chỉ vật lý được dùng cho mạng.

**Lớp liên mạng**

Internet Layer là lớp ở ngay trên lớp Network Access trong cấu trúc phân lớp của TCP/IP. Internet Protocol là giao thức trung tâm của TCP/IP và là phần quan trọng nhất của lớp Internet. IP cung cấp các gói lưu chuyển cơ bản mà thông qua đó các mạng dùng TCP/IP được xây dựng.

## 1.2. Chức năng chính của - Giao thức liên mạng IP(v4)

Trong phần này trình bày về giao thức IPv4 (để cho thuận tiện ta viết IP có nghĩa là đề cập đến IPv4).

Mục đích chính của IP là cung cấp khả năng kết nối các mạng con thành liên mạng để truyền dữ liệu. IP cung cấp các chức năng chính sau:

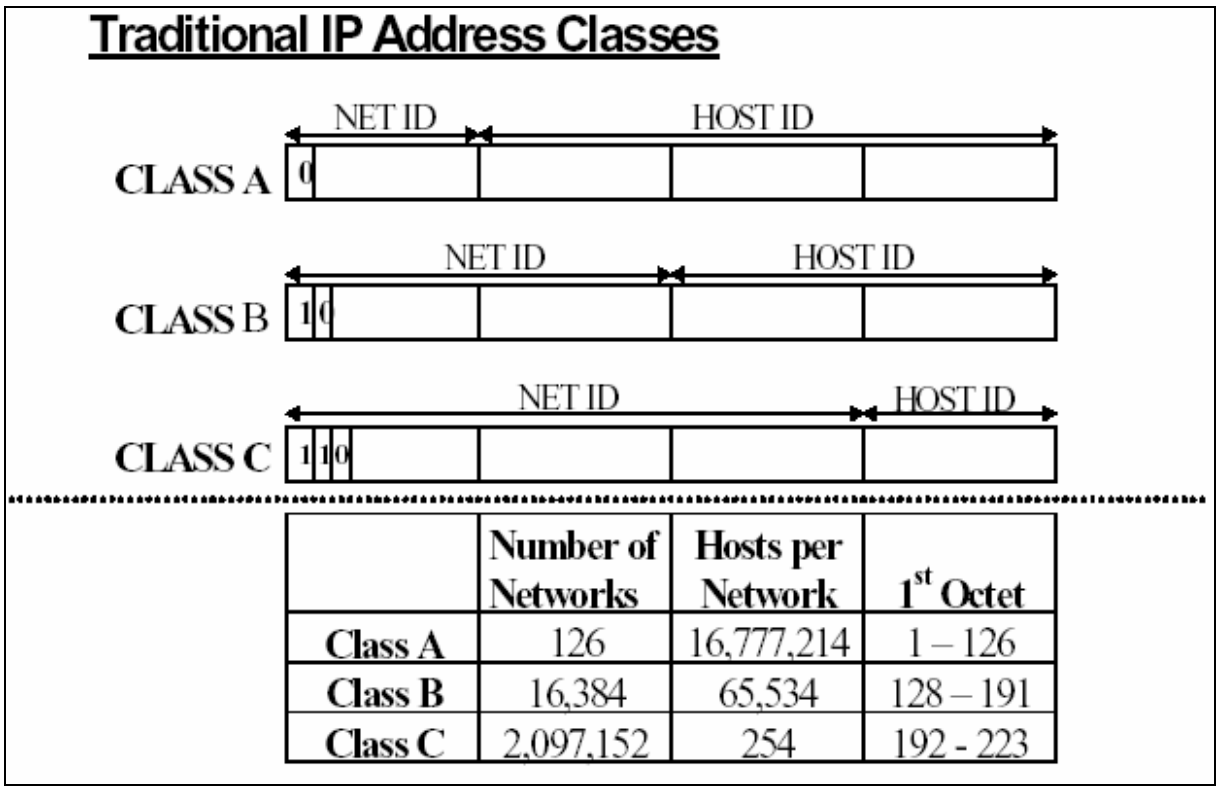
- Định nghĩa cấu trúc các gói dữ liệu là đơn vị cơ sở cho việc truyền dữ liệu trên Internet.

- Phần định danh địa chỉ mạng Network Number

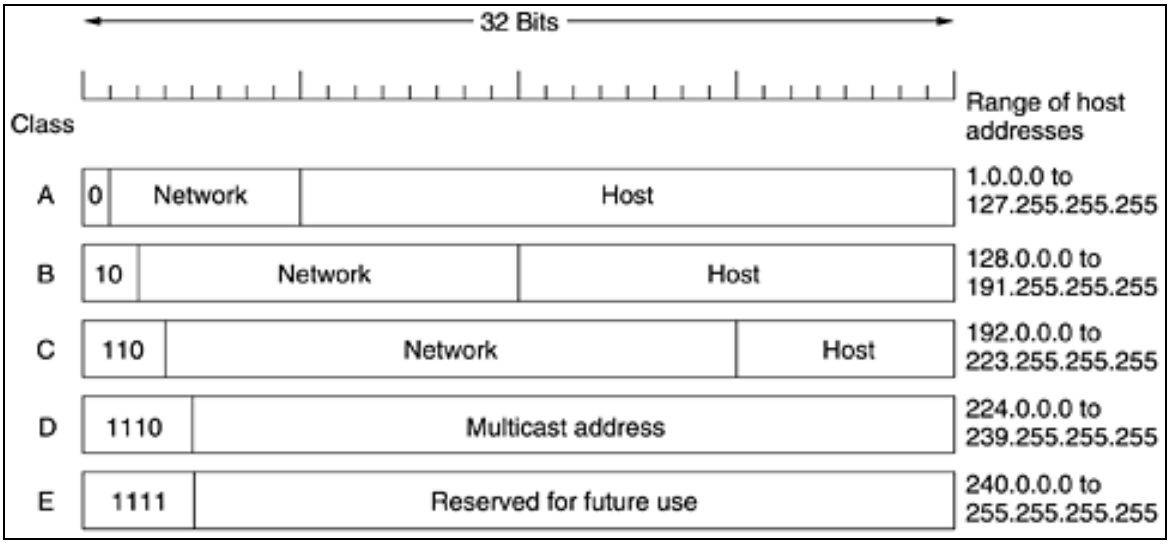
- Phần định danh địa chỉ các trạm làm việc trên mạng đó Host Number

Ví dụ 128.4.70.9 là một địa chỉ IP

Do tổ chức và độ lớn của các mạng con của liên mạng có thể khác nhau, người ta chia các địa chỉ IP thành 5 lớp ký hiệu A,B,C, D, E với cấu trúc được xác định trên hình 3.4.




| | Number of Networks | Hosts per Network | 1st Octet |
|---|---|---|---|
| Class A | 126 | 16,777,214 | 1 – 126 |
| Class B | 16,384 | 65,534 | 128 – 191 |
| Class C | 2,097,152 | 254 | 192 - 223 |




Hình 3.4. Cấu trúc địa chỉ IP

Các bit đầu tiên của byte đầu tiên được dùng để định danh lớp địa chỉ (0- lớp A; 10 lớp B; 110 lớp C; 1110 lớp D; 11110 lớp E).

- Lớp A cho phép định danh tới 126 mạng (sử dụng byte đầu tiên), với tối đa 16 triệu host (3 byte còn lại, 24 bits) cho mỗi mạng. Lớp này được dùng cho các mạng có số trạm cực lớn. Tại sao lại có 126 mạng trong khi dùng 8 bits? Lí do đầu tiên, 127.x (01111111) dùng cho địa chỉ loopback, thứ 2 là bit đầu tiên của byte đầu tiên bao giờ cũng là 0, 1111111(127). Dạng địa chỉ lớp A (network number. host.host.host). Nếu dùng ký pháp thập phân cho phép 1 đến 126 cho vùng đầu, 1 đến 255 cho các vùng còn lại.

- Lớp B cho phép định danh tới 16384 mạng (10111111.11111111.host.host), với tối đa 65535 host trên mỗi mạng. Dạng của lớp B (network number. Network number.host.host). Nếu dùng ký pháp thập phân cho phép 128 đến 191 cho vùng đầu, 1 đến 255 cho các vùng còn lại

- Lớp C cho phép định danh tới 2.097.150 mạng và tối đa 254 host cho mỗi mạng. Lớp này được dùng cho các mạng có ít trạm. Lớp C sử dụng 3 bytes đầu định danh địa chỉ mạng (110xxxxx). Dạng của lớp C (network number. Network number.Network number.host). Nếu dùng dạng ký pháp thập phân cho phép 129 đến 233 cho vùng đầu và từ 1 đến 255 cho các vùng còn lại.

- Lớp D dùng để gửi IP datagram tới một nhóm các host trên một mạng. Tất cả các số lớn hơn 233 trong trường đầu là thuộc lớp D

- Lớp E dự phòng để dùng trong tương lai

Như vậy địa chỉ mạng cho lớp: A: từ 1 đến 126 cho vùng đầu tiên, 127 dùng cho địa chỉ loopback, B từ 128.1.0.0 đến 191.255.0.0, C từ 192.1.0.0 đến 233.255.255.0

**Ví dụ:**

192.1.1.1 địa chỉ lớp C có địa chỉ mạng 192.1.1.0, địa chỉ host là 1

200.6.5.4 địa chỉ lớp C có địa chỉ mạng 200.6.5, địa chỉ mạng là 4

150.150.5.6 địa chỉ lớp B có địa chỉ mạng 150.150.0.0, địa chỉ host là 5.6

9.6.7.8 địa chỉ lớp A có địa chỉ mạng 9.0.0.0, địa chỉ host là 6.7.8

128.1.0.1 địa chỉ lớp B có địa chỉ mạng 128.1.0.0, địa chỉ host là 0.1

Network ID không thể là 127 - dành cho chức năng loop-back là kiểm tra vòng lặp tại thiết bị, không thực hiện chuyển dữ liệu.

Network ID và host ID không thể là 255 (các bit đặt là 1) - 255 là địa chỉ quảng bá

Network ID và host ID không thể là 0 (các bit đặt là 0) - 0 có nghĩa là chính mạng đó.

| | | |
|---|---|---|
| IP Address | **160.30.20**.10 | **10100000 00011110 00010100** 00001010 |
| Subnet Mask | **255.255.255**.0 | **11111111 11111111 11111111** 00000000 |
| Result | **160.30.20**.0 | **10100000 00011110 00010100** 00000000 |

| | | |
|---|---|---|
| IP Address | **160.30.20**.100 | **10100000 00011110 11001000** 01100100 |
| Subnet Mask | **255.255.255**.0 | **11111111 11111111 11111111** 00000000 |
| Result | **160.30.20**.0 | **10100000 00011110 00010100** 00000000 |

Cách viết mask theo độ dài tiếp đầu ngữ (prefix length).

Để ngắn gọn có thể viết mask theo số bit 1 liên tiếp tính từ đầu.

Ví dụ 255.255.255.0 có 24 bit 1 do đó viết địa chỉ 160.30.20.10/24.

Theo quy tắc đó: lớp A có mask là 255.0.0.0 (/8),

lớp B - 255.255.0.0 (/16),

lớp C - 255.255.255.0 (/24).

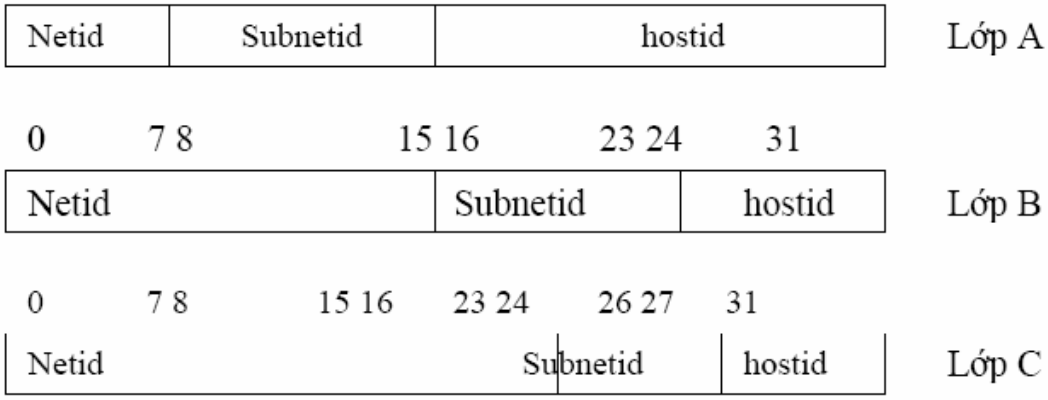
**Subneting**

Trong nhiều trường hợp, một mạng có thể được chia thành nhiều mạng con (subnet), lúc đó có thể đưa thêm các vùng subnetid để định danh các mạng con. Vùng subnetid được lấy từ vùng hostid, cụ thể đối với 3 lớp A, B, C như sau:

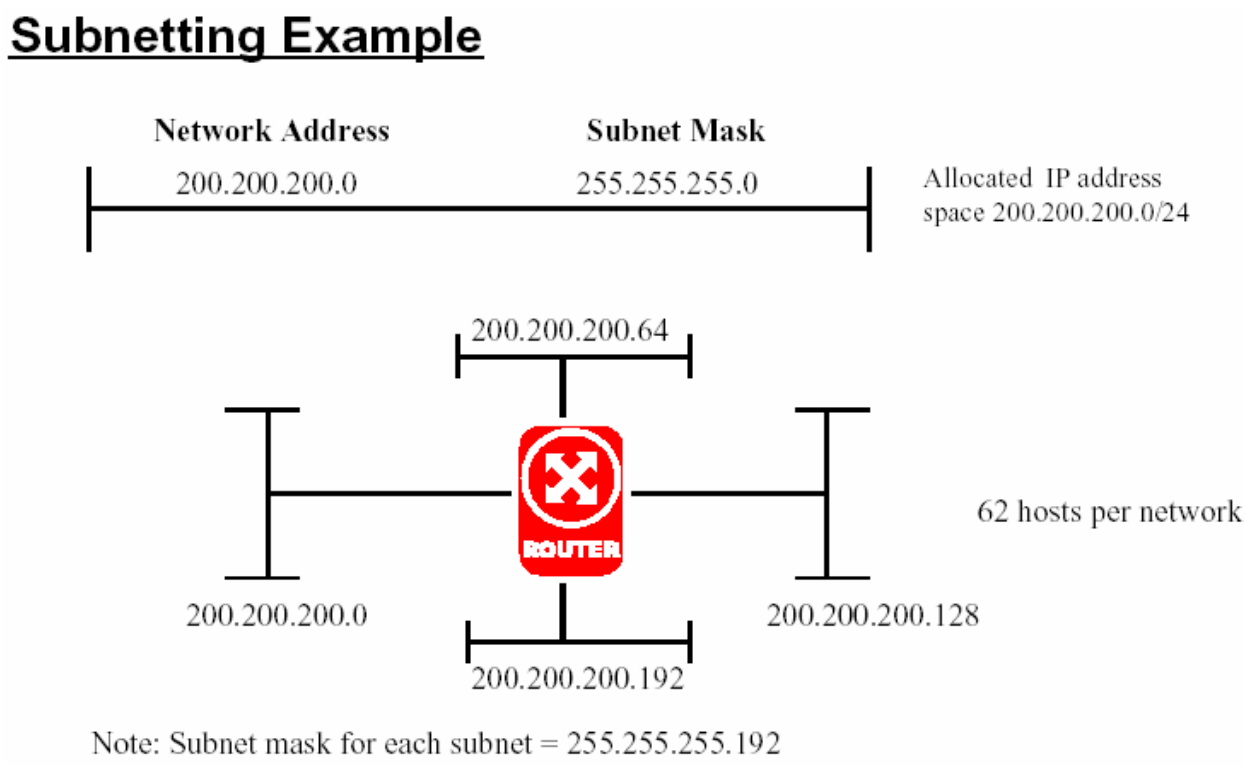
Ví dụ:

17.1.1.1 địa chỉ lớp A có địa chỉ mạng 17, địa chỉ subnet 1, địa chỉ host 1.1

129.1.1.1 địa chỉ lớp B có địa chỉ mạng 129.1, địa chỉ subnet 1, địa chỉ host 1.




Hình 3.6 Bổ sung vùng subnetid




Hình 3.7. Ví dụ SubNet

Subnet Mask là 255.255.255.192 hay là /26

04 mạng nhỏ hơn với địa chỉ mạng là

Mạng 1: 200.200.200.0/26 -> từ 200.200.200.1 đến 200.200.200.62

Mạng 2: 200.200.200.64/26 -> từ 200.200.200.65 đến 200.200.200.126

Mạng 3: 200.200.200.0/128 -> từ 200.200.200.129 đến 200.200.200.190

Mạng 4: 200.200.200.0/192 -> từ 200.200.200.193 đến 200.200.200.254.

Xác định tên máy tính

Mỗi máy tính được gán một địa chỉ IP. Để dễ nhớ thì gán thêm một tên dùng bảng chữ cái, gọi là domain name, ví dụ dhsp.edu.vn.

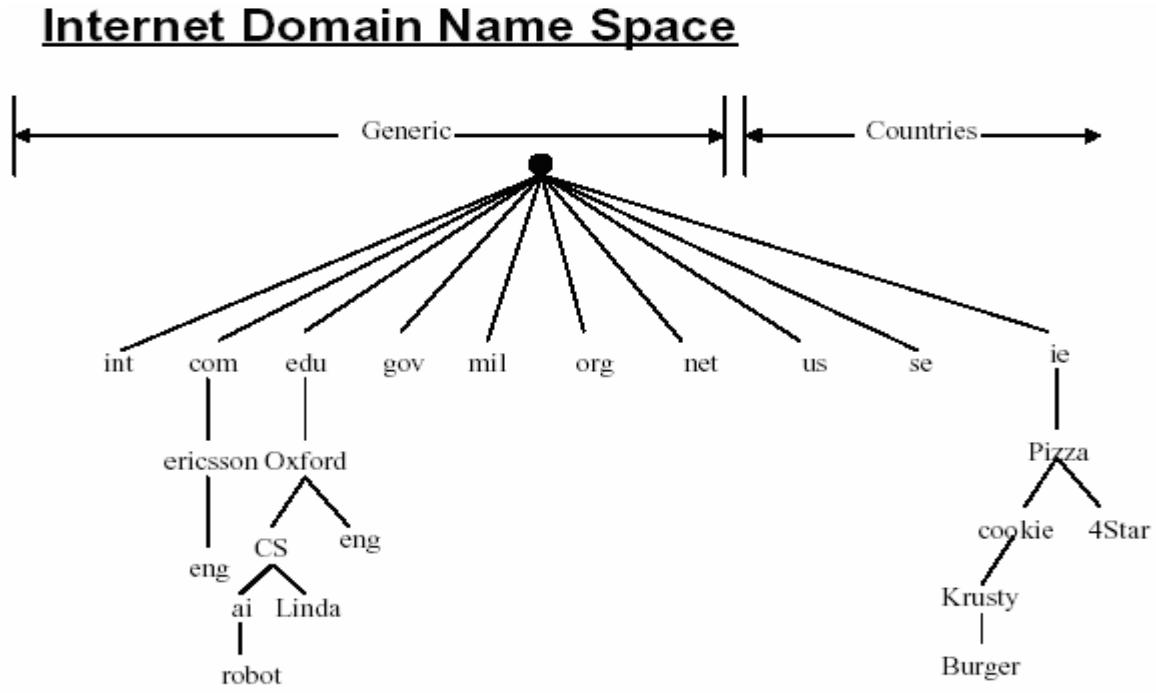
Để xác định tên của một máy tính, cần một phương pháp ánh xạ giữa địa chỉ số và tên gọi. Hệ thống xác định tên từ IP là CSDL DNS (Domain Name System).

DNS được tổ chức theo cấu trúc phân hệ, phần gần gốc hơn là tên ở phía bên phải, các hệ thống lớn chia ra các hệ thống nhỏ, và lại được chia tiếp theo. Các DNS có các loại chính như sau: loại top-level - bậc cao; loại thông thường; loại theo quốc gia.

Các loại thông thường:

- **com** (Commercial organisation)
- **edu** (Educational institution)
- **gov** (Government organisation)
- **mil** (Military group)
- **net** (Major network support centre)
- **org** (Organisation other than those above)
- **int** (International organisation)

Loại tên nước: hai chữ cái viết tắt (ISO 3166 quy định): vd Việt nam là vn; Anh - uk; Úc - au, vv.




Hình 3.9

Cách thức xác định tên và IP từ tên:

1. Client gửi yêu cầu xác định IP cho tên mr-a.khoacntt.dhsphn.edu.vn tới Local Name Server.

2. LNS không có quyền đối với tên này nên yêu cầu Root name server.

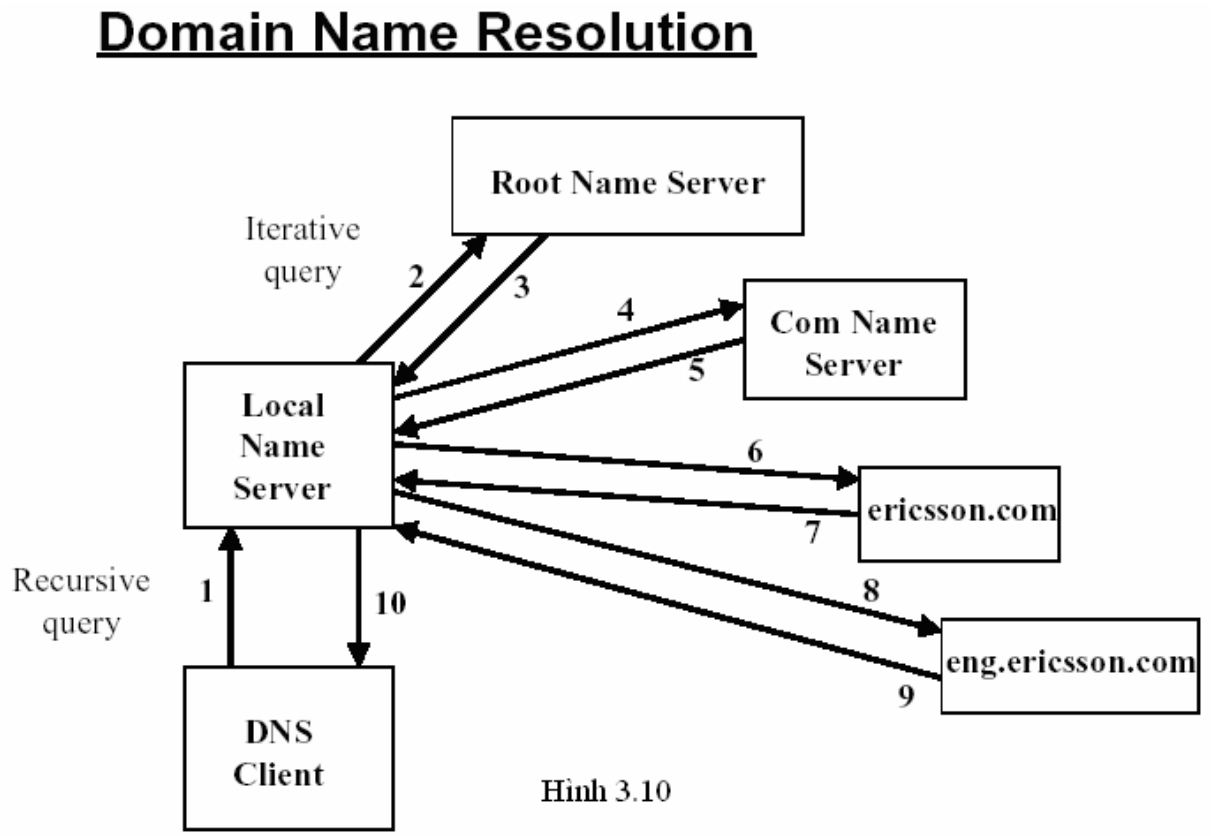
3. RNS gửi lại LNS địa chỉ IP của vn name server.

4. LNS yêu cầu tới vn server

5. vn server trả lời địa chỉ IP của DNS quản lý tên miền edu.vn.

6. LNS yêu cầu tới server trên và nhận trả lời cho server name tiếp theo,...

Quá trình tiếp diễn tới khi đạt được name server quản lý chính xác tên như trên.




Hình 3.10

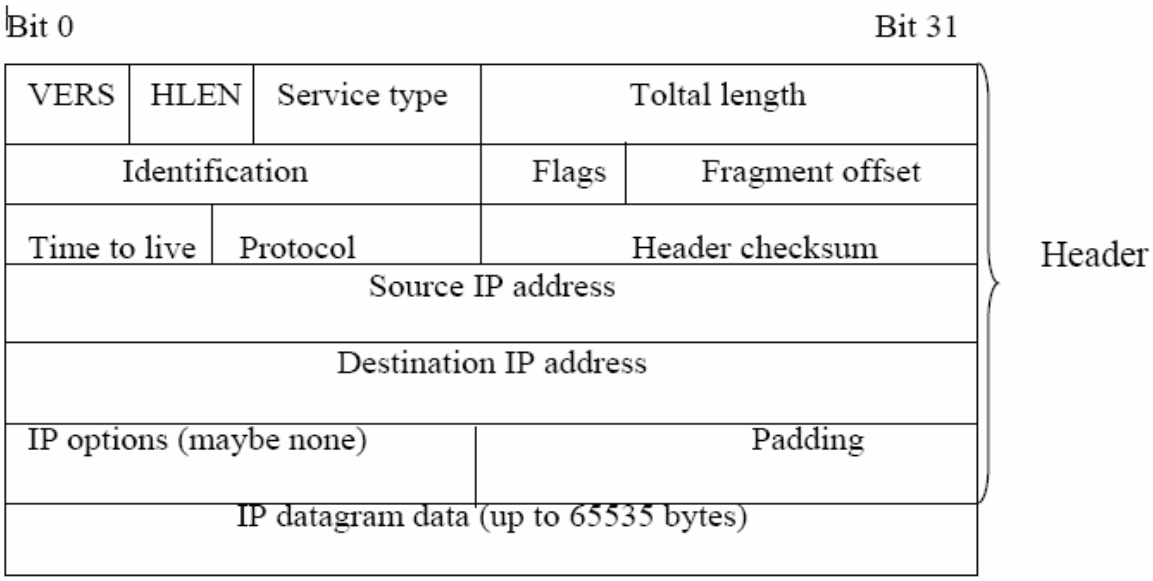
Các Name Server giữ các thông tin về xử lý tên miền trong bộ đệm, khi có thông tin sẽ gửi một thông báo gồm tên miền và địa chỉ IP tới Client và cách liên lạc với name server đó. Do đó việc xử lý tên sẽ nhanh hơn.

Các bộ đệm có cơ chế đặt thời gian sống (Time-To-Live) cho các thông tin lưu trữ.

### 1.2.2. Cấu trúc gói dữ liệu IP

IP là giao thức cung cấp dịch vụ truyền thông theo kiểu "không liên kết" (connectionless). Phương thức không liên kết cho phép cặp trạm truyền nhận không cần phải thiết lập liên kết trước khi truyền dữ liệu và do đó không cần phải giải phóng liên kết khi không còn nhu cầu truyền dữ liệu nữa. Phương thức kết nối "không liên kết" cho phép thiết kế và thực hiện giao thức trao đổi dữ liệu đơn giản (không có cơ chế phát hiện và khắc phục lỗi truyền). Cũng chính vì vậy độ tin cậy trao đổi dữ liệu của loại giao thức này không cao.

Các gói dữ liệu IP được định nghĩa là các datagram. Mỗi datagram có phần tiêu đề (header) chứa các thông tin cần thiết để chuyển dữ liệu (ví dụ địa chỉ IP của trạm đích). Nếu địa chỉ IP đích là địa chỉ của một trạm nằm trên cùng một mạng IP với trạm nguồn thì các gói dữ liệu sẽ được chuyển thẳng tới đích; nếu địa chỉ IP đích không nằm trên cùng một mạng IP với máy nguồn thì các gói dữ liệu sẽ được gửi đến một máy trung chuyển, IP gateway để chuyển tiếp. IP gateway là một thiết bị mạng IP đảm nhận việc lưu chuyển các gói dữ liệu IP giữa hai mạng IP khác nhau. Hình 3.11 mô tả cấu trúc gói số liệu IP.




Hình 3.11. Cấu trúc gói dữ liệu IP

- VER (4 bits) : chỉ Version hiện hành của IP được cài đặt.

- IHL (4 bits) : chỉ độ dài phần tiêu đề (Internet Header Length) của datagram, tính theo đơn vị word (32 bits). Nếu không có trường này thì độ dài mặc định của phần tiêu đề là 5 từ.

- Type of service (8 bits): cho biết các thông tin về loại dịch vụ và mức ưu tiên của gói IP, có dạng cụ thể như sau:

| | | | | |
|---|---|---|---|---|
| Precedence | D | T | R | Unused |

Trong đó:

Precedence (3 bits): chỉ thị về quyền ưu tiên gửi datagram, cụ thể là:

111 Network Control (cao nhất) 011- flash

110 Internetwork Control 010 Immediate

101 CRITIC/ECP 001 Priority

100 Flas Override 000 Routine (thấp nhất)

D (delay) (1 bit) : chỉ độ trễ yêu cầu

D=0 độ trễ bình thường,

D=1 độ trễ thấp

T (Throughput) (1 bit) : chỉ số thông lượng yêu cầu

T=1 thông lượng bình thường

T=1 thông lượng cao

R (Reliability) (1 bit): chỉ độ tin cậy yêu cầu

R=0 độ tin cậy bình thường

R=1 độ tin cậy cao

- Total Length (16 bits): chỉ độ dài toàn bộ datagram, kể cả phần header (tính theo đơn vị bytes), vùng dữ liệu của datagram có thể dài tới 65535 bytes.

- Identification (16 bits) : cùng với các tham số khác như (Source Address và Destination Address) tham số này dùng để định danh duy nhất cho một datagram trong khoảng thời gian nó vẫn còn trên liên mạng

- Flags (3 bits) : liên quan đến sự phân đoạn (fragment) các datagram. Cụ thể

| O | DF | MF |
|---|---|---|

Bit 0 : reserved chưa sử dụng luôn lấy giá trị 0

Bit 1 : (DF)= 0 (may fragment)

1 (Don't Fragment)

Bit 2 : (MF)= 0 (Last Fragment)

1 (More Fragment)

- Fragment Offset (13 bits) : chỉ vị trí của đoạn (fragment) ở trong datagram, tính theo đơn vị 64 bits, có nghĩa là mỗi đoạn (trừ đoạn cuối cùng) phải chứa một vùng dữ liệu có độ dài là bội của 64 bits.

- Time To Live (TTL-8 bits) : quy định thời gian tồn tại của một gói dữ liệu trên liên mạng để tránh tình trạng một datagram bị quẩn trên mạng. Giá trị này được đặt lúc bắt đầu gửi đi và sẽ giảm dần mỗi khi gói dữ liệu được xử lý tại những điểm trên đường đi của gói dữ liệu (thực chất là tại các router). Nếu giá trị này bằng 0 trước khi đến được đích, gói dữ liệu sẽ bị huỷ bỏ.

- Protocol (8 bits): chỉ giao thức tầng kế tiếp sẽ nhận vùng dữ liệu ở trạm đích (hiện tại thường là TCP hoặc UDP được cài đặt trên IP).

- Header checksum (16 bits): mã kiểm soát lỗi sử dụng phương pháp CRC (Cyclic Redundancy Check) dùng để đảm bảo thông tin về gói dữ liệu được truyền đi một cách chính xác (mặc dù dữ liệu có thể bị lỗi). Nếu như việc kiểm tra này thất bại, gói dữ liệu sẽ bị huỷ bỏ tại nơi xác định được lỗi. Cần chú ý là IP không cung cấp một phương tiện truyền tin cậy bởi nó không cung cấp cho ta một cơ chế để xác nhận dữ liệu truyền tại điểm nhận hoặc tại những điểm trung gian. Giao thức IP không có cơ chế Error Control cho dữ liệu truyền đi, không có cơ chế kiểm soát luồng dữ liệu (flow control).

- Source Address (32 bits): địa chỉ của trạm nguồn.

- Destination Address (32 bits): địa chỉ của trạm đích.

- Option (có độ dài thay đổi) sử dụng trong một số trường hợp, nhưng thực tế chúng rất ít dùng. Option bao gồm bảo mật, chức năng định tuyến đặc biệt

- Padding (độ dài thay đổi): vùng đệm, được dùng để đảm bảo cho phần header luôn kết thúc ở một mốc 32 bits

- Data (độ dài thay đổi): vùng dữ liệu có độ dài là bội của 8 bits, tối đa là 65535 bytes.

### 1.2.3. Phân mảnh và hợp nhất các gói IP

Các gói dữ liệu IP phải được nhúng trong khung dữ liệu ở tầng liên kết dữ liệu tương ứng, trước khi chuyển tiếp trong mạng. Quá trình nhận một gói dữ liệu IP diễn ra ngược lại. Ví dụ, với mạng Ethernet ở tầng liên kết dữ liệu quá trình chuyển một gói dữ liệu diễn ra như sau. Khi gửi một gói dữ liệu IP cho mức Ethernet, IP chuyển cho mức liên kết dữ liệu các thông số địa chỉ Ethernet đích, kiểu khung Ethernet (chỉ dữ liệu mà Ethernet đang mang là của IP) và cuối cùng là gói IP. Tầng liên kết số liệu đặt địa chỉ Ethernet nguồn là địa chỉ kết nối mạng của mình và tính toán giá trị checksum. Trường type chỉ ra kiểu khung là 0x0800 đối với dữ liệu IP. Mức liên kết dữ liệu sẽ chuyển khung dữ liệu theo thuật toán truy nhập Ethernet.

Một gói dữ liệu IP có độ dài tối đa 65536 byte, trong khi hầu hết các tầng liên kết dữ liệu chỉ hỗ trợ các khung dữ liệu nhỏ hơn độ lớn tối đa của gói dữ liệu IP nhiều lần (ví dụ độ dài lớn nhất của một khung dữ liệu Ethernet là 1500 byte). Vì vậy cần thiết phải có cơ chế phân mảnh khi phát và hợp nhất khi thu đối với các gói dữ liệu IP.

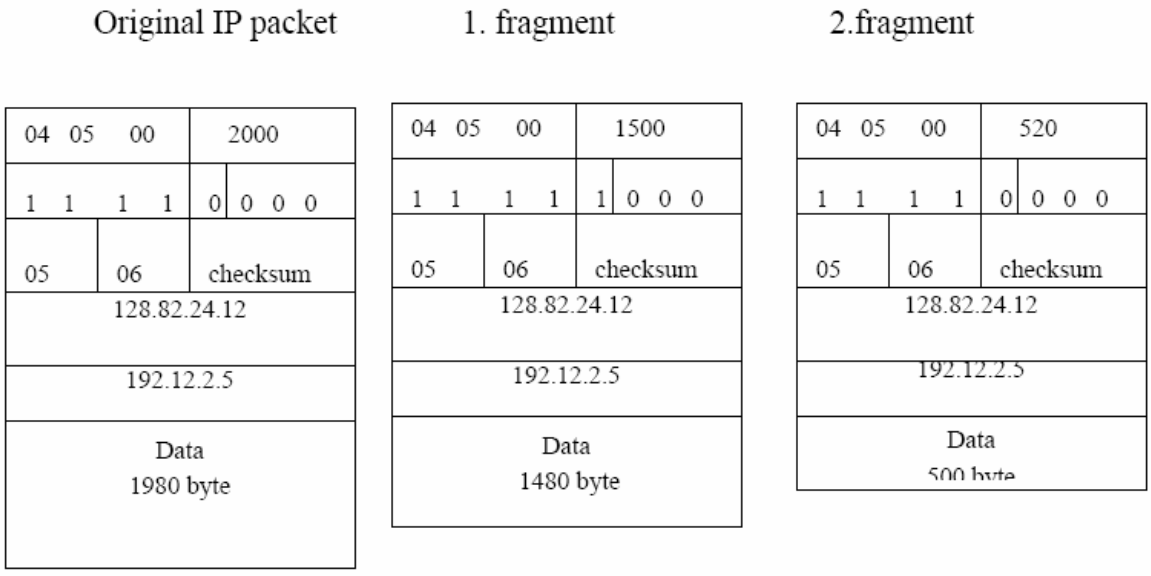
Độ dài tối đa của một gói dữ liệu liên kết là MTU (Maximum Transmit Unit). Khi cần chuyển một gói dữ liệu IP có độ dài lớn hơn MTU của một mạng cụ thể, cần phải chia gói số liệu IP đó thành những gói IP nhỏ hơn để độ dài của nó nhỏ hơn hoặc bằng MTU gọi chung là mảnh (fragment). Trong phần tiêu đề của gói dữ liệu IP có thông tin về phân mảnh và xác định các mảnh có quan hệ phụ thuộc để hợp thành sau này.

Ví dụ Ethernet chỉ hỗ trợ các khung có độ dài tối đa là 1500 byte. Nếu muốn gửi một gói dữ liệu IP gồm 2000 byte qua Ethernet, phải chia thành hai gói nhỏ hơn, mỗi gói không quá giới hạn MTU của Ethernet.

P dùng cờ MF (3 bit thấp của trường Flags trong phần đầu của gói IP) và trường Flagment offset của gói IP (đã bị phân đoạn) để định danh gói IP đó là một phân đoạn và vị trí của phân đoạn này trong gói IP gốc. Các gói cùng trong chuỗi phân mảnh đều có trường này giống nhau. Cờ MF bằng 1 nếu là gói đầu của chuỗi phân mảnh và 0 nếu là gói cuối của gói đã được phân mảnh.

Quá trình hợp nhất diễn ra ngược lại với quá trình phân mảnh. Khi IP nhận được một gói phân mảnh, nó giữ phân mảnh đó trong vùng đệm, cho đến khi nhận được hết các gói IP trong chuỗi phân mảnh có cùng trường định danh. Khi phân mảnh đầu tiên được nhận, IP khởi động một bộ đếm thời gian (giá trị ngầm định là 15s). IP phải nhận hết các phân mảnh kế tiếp trước khi đồng hồ tắt. Nếu không IP phải huỷ tất cả các phân mảnh trong hàng đợi hiện thời có cùng trường định danh.

Khi IP nhận được hết các phân mảnh, nó thực hiện hợp nhất các gói phân mảnh thành các gói IP gốc và sau đó xử lý nó như một gói IP bình thường. IP thường chỉ thực hiện hợp nhất các gói tại hệ thống đích của gói.




Hình 3.12. Nguyên tắc phân mảnh gói dữ liệu

### 1.2.4. Định tuyến IP

Có hai loại định tuyến:

- Định tuyến trực tiếp: Định tuyến trực tiếp là việc xác định đường nối giữa hai trạm làm việc trong cùng một mạng vật lý.

- Định tuyến không trực tiếp. Định tuyến không trực tiếp là việc xác định đường nối giữa hai trạm làm việc không nằm trong cùng một mạng vật lý và vì vậy, việc truyền tin giữa chúng phải được thực hiện thông qua các trạm trung gian là các gateway.

Để kiểm tra xem trạm đích có nằm trên cùng mạng vật lý với trạm nguồn hay không, người gửi phải tách lấy phần địa chỉ mạng trong phần địa chỉ IP. Nếu hai địa chỉ này có địa chỉ mạng giống nhau thì datagram sẽ được truyền đi trực tiếp; ngược lại phải xác định một gateway, thông qua gateway này chuyển tiếp các datagram.

Khi một trạm muốn gửi các gói dữ liệu đến một trạm khác thì nó phải đóng gói datagram vào một khung (frame) và gửi các frame này đến gateway gần nhất. Khi một frame đến một gateway, phần datagram đã được đóng gói sẽ được tách ra và IP routing sẽ chọn gateway tiếp dọc theo đường dẫn đến đích. Datagram sau đó lại được đóng gói vào một frame khác và gửi đến mạng vật lý để gửi đến gateway tiếp theo trên đường truyền và tiếp tục như thế cho đến khi datagram được truyền đến trạm đích.

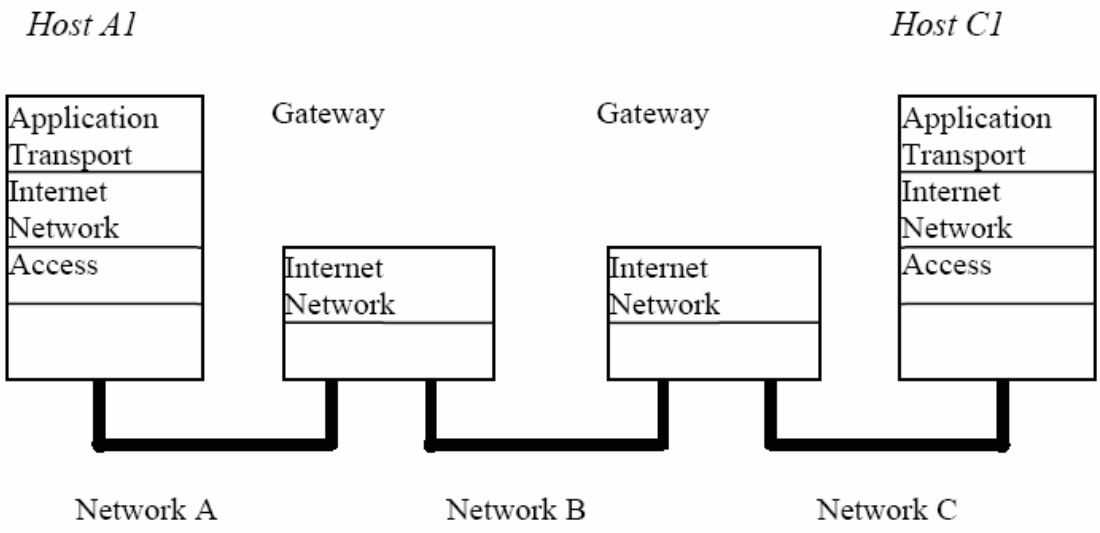
**Chiến lược định tuyến**:

Trong thuật ngữ truyền thống của TCP/IP chỉ có hai kiểu thiết bị, đó là các cổng truyền (gateway) và các trạm (host). Các cổng truyền có vai trò gửi các gói dữ liệu, còn các trạm thì không. Tuy nhiên khi một trạm được nối với nhiều mạng thì nó cũng có thể định hướng cho việc lưu chuyển các gói dữ liệu giữa các mạng và lúc này nó đóng vai trò hoàn toàn như một gateway.

Các trạm làm việc lưu chuyển các gói dữ liệu xuyên suốt qua cả bốn lớp, trong khi các cổng truyền chỉ chuyển các gói đến lớp Internet là nơi quyết định tuyến đường tiếp theo để chuyển tiếp các gói dữ liệu.

Các máy chỉ có thể truyền dữ liệu đến các máy khác nằm trên cùng một mạng vật lý. Các gói từ A1 cần chuyển cho C1 sẽ được hướng đến gateway G1 và G2. Trạm A1 đầu tiên sẽ truyền các gói đến gateway G1 thông qua mạng A. Sau đó G1 truyền tiếp đến G2 thông qua mạng B và cuối cùng G2 sẽ truyền các gói trực tiếp đến trạm C1, bởi vì chúng được nối trực tiếp với nhau thông qua mạng C. Trạm A1 không hề biết đến các gateway nằm ở sau G1. A1 gửi các gói số liệu cho các mạng B và C đến gateway cục bộ G1 và dựa vào gateway này để định hướng tiếp cho các gói dữ liệu đi đến đích. Theo cách này thì trạm C1 trước tiên sẽ gửi các gói của mình đến cho G2 và G2 sẽ gửi đi tiếp cho các trạm ở trên mạng A cũng như ở trên mạng B.

Hình vẽ sau mô tả việc dùng các gateway để gửi các gói dữ liệu:




Hình 3.13. Định tuyến giữa hai hệ thống

**Việc phân mảnh các gói dữ liệu**: Trong quá trình truyền dữ liệu, một gói dữ liệu (datagram) có thể được truyền đi thông qua nhiều mạng khác nhau. Một gói dữ liệu (datagram) nhận được từ một mạng nào đó có thể quá lớn để truyền đi trong gói đơn ở trên một mạng khác, bởi mỗi loại cấu trúc mạng cho phép một đơn vị truyền cực đại (Maximum Transmit Unit - MTU), khác nhau. Đây chính là kích thước lớn nhất của một gói mà chúng có thể truyền. Nếu như một gói dữ liệu nhận được từ một mạng nào đó mà lớn hơn MTU của một mạng khác thì nó cần được phân mảnh ra thành các gói nhỏ hơn, gọi là fragment. Quá trình này gọi là quá trình phân mảnh. Dạng của một fragment cũng giống như dạng của một gói dữ liệu thông thường. Từ thứ hai trong phần header chứa các thông tin để xác định mỗi fragment và cung cấp các thông tin để hợp nhất các fragment này lại thành các gói như ban đầu. Trường identification dùng để xác định fragment này là thuộc về gói dữ liệu nào.

## I.6. Một số giao thức điều khiển

### I.6.1. Giao thức ICMP

ICMP ((Internet Control Message Protocol) là một giao thức điều khiển của mức IP, được dùng để trao đổi các thông tin điều khiển dòng số liệu, thông báo lỗi và các thông tin trạng thái khác của bộ giao thức TCP/IP. Ví dụ:

- Điều khiển lưu lượng dữ liệu (Flow control): khi các gói dữ liệu đến quá nhanh, thiết bị đích hoặc thiết bị định tuyến ở giữa sẽ gửi một thông điệp ICMP trở lại thiết bị gửi, yêu cầu thiết bị gửi tạm thời ngừng việc gửi dữ liệu.

- Thông báo lỗi: trong trường hợp địa chỉ đích không tới được thì hệ thống sẽ gửi một thông báo lỗi "Destination Unreachable".

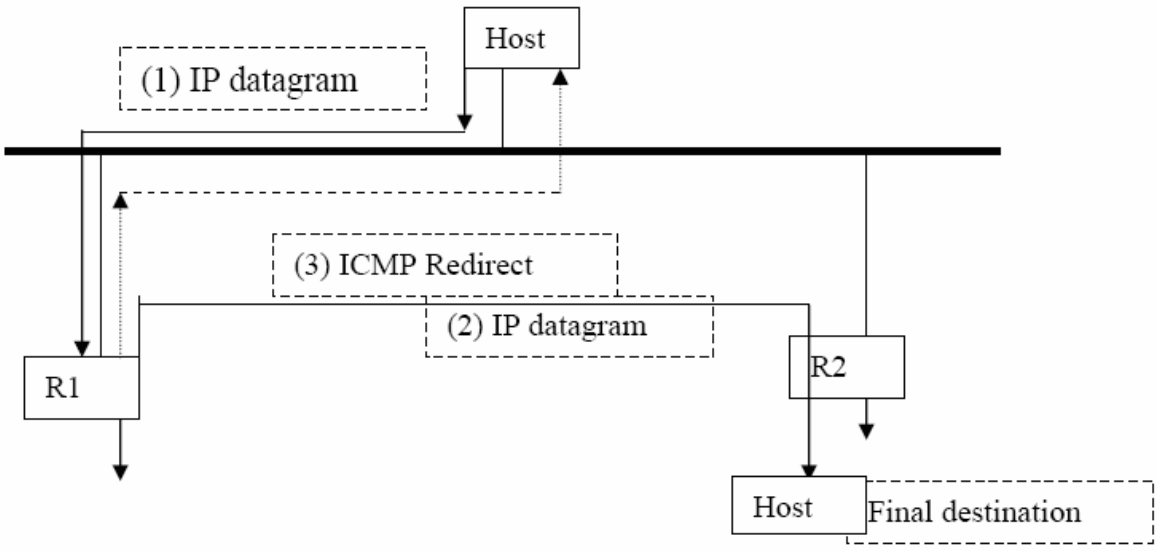
- Định hướng lại các tuyến đường: một thiết bị định tuyến sẽ gửi một thông điệp ICMP "định tuyến lại" (Redirect Router) để thông báo với một trạm là nên dùng thiết bị định tuyến khác để tới thiết bị đích. Thông điệp này có thể chỉ được dùng khi trạm nguồn ở trên cùng một mạng với cả hai thiết bị định tuyến.

- Kiểm tra các trạm ở xa: một trạm có thể gửi một thông điệp ICMP "Echo" để kiểm tra xem một trạm có hoạt động hay không.

Sau đây là mô tả một ứng dụng của giao thức ICMP thực hiện việc định tuyến lại (Redirect):

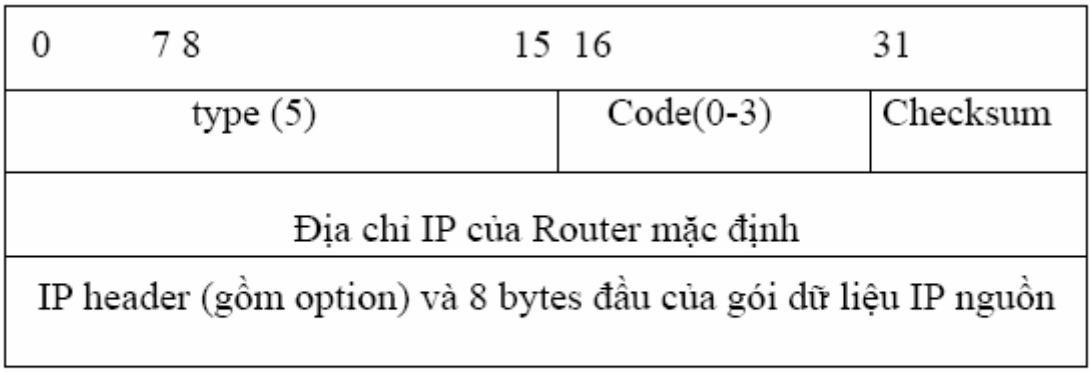
Ví dụ: giả sử host gửi một gói dữ liệu IP tới Router R1. Router R1 thực hiện việc quyết định tuyến vì R1 là router mặc định của host đó. R1 nhận gói dữ liệu và tìm trong bảng định tuyến và nó tìm thấy một tuyến tới R2. Khi R1 gửi gói dữ liệu tới R2 thì R1 phát hiện ra rằng nó đang gửi gói dữ liệu đó ra ngoài trên cùng một giao diện mà gói dữ liệu đó đã đến (là giao diện mạng LAN mà cả host và hai Router nối đến). Lúc này R1 sẽ gửi một thông báo ICMP Redirect Error tới host, thông báo cho host nên gửi các gói dữ liệu tiếp theo đến R2 thì tốt hơn.

Tác dụng của ICMP Redirect là để cho mọt host với nhận biết tối thiểu về định tuyến xây dựng lên một bảng định tuyến tốt hơn theo thời gian. Host đó có thể bắt đầu với một tuyến mặc định (có thể R1 hoặc R2 như ví dụ trên) và bất kỳ lần nào tuyến mặc định này được dùng với host đó đến R2 thì nó sẽ được Router mặc định gửi thông báo Redirect để cho phép host đó cập nhật bảng định tuyến của nó một cách phù hợp hơn. Khuôn dạng của thông điệp ICMP redirect như sau:




Hình 3.8 Thực hiện việc định tuyến lại

Có bốn loại thông báo ICMP redirect khác nhau với các giá trị mã (code) như bảng sau:




Hình 3.9 Dạng thông điệp ICMP redirect

| Code | Description |
|---|---|
| 0 | Redirect cho mạng |
| 1 | Redirect cho host |
| 2 | Redirect cho loại dịch vụ (TOS) và mạng |
| 3 | Redirect cho loại dịch vụ và host |

Các loại định hướng lại của gói dữ liệu ICMP

Redirect chỉ xảy ra khi cả hai Router R1 và R2 cùng nằm trên một mạng với host nhận direct đó.

## I.6.2. Giao thức ARP và giao thức RARP

Địa chỉ IP được dùng để định danh các host và mạng ở tầng mạng của mô hình OSI, chúng không phải là các địa chỉ vật lý (hay địa chỉ MAC) của các trạm đó trên một mạng cục bộ (Ethernet, Token Ring,...). Trên một mạng cục bộ hai trạm chỉ có thể liên lạc với nhau nếu chúng biết địa chỉ vật lý của nhau. Như vậy vấn đề đặt ra là phải thực hiện ánh xạ giữa địa chỉ IP (32 bits) và địa chỉ vật lý (48 bits) của một trạm. Giao thức ARP (Address Resolution Protocol) đã được xây dựng để chuyển đổi từ địa chỉ IP sang địa chỉ vật lý khi cần thiết. Ngược lại, giao thức RARP (Reverse Address Resolution Protocol) được dùng để chuyển đổi địa chỉ vật lý sang địa chỉ IP. Các giao thức ARP và RARP không phải là bộ phận của IP mà IP sẽ dùng đến chúng khi cần.

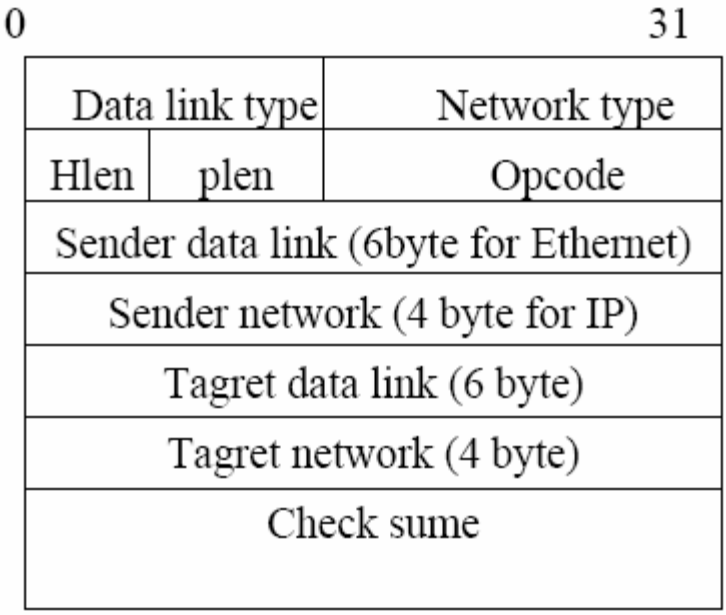
**Giao thức ARP**

Giao thức TCP/IP sử dụng ARP để tìm địa chỉ vật lý của trạm đích. Ví dụ khi cần gửi một gói dữ liệu IP cho một hệ thống khác trên cùng một mạng vật lý Ethernet, hệ thông gửi cần biết địa chỉ Ethernet của hệ thống đích để tầng liên kết dữ liệu xây dựng khung gói dữ liệu.

Thông thường, mỗi hệ thống lưu giữ và cập nhật bảng thích ứng địa chỉ IP-MAC tại chỗ (còn được gọi là bảng ARP cache). Bảng thích ứng địa chỉ được cập nhật bởi người quản trị hệ thống hoặc tự động bởi giao thức ARP sau mỗi lần ánh xạ được một địa chỉ thích ứng mới. Khuôn dạng của gói dữ liệu ARP được mô tả trong hình

- Data link type: cho biết loại công nghệ mạng mức liên kết (ví dụ đối với mạng Ethernet trường này có giá trị 01).

- Network type: cho biết loại mạng (ví dụ đối với mạng IPv4, trường này có giá




Hình 3.10 Mô tả khuôn dạng của gói ARP

trị $0800_{16}$).

- Hlen (hardware length): độ dài địa chỉ mức liên kết (6 byte).

- Plen (Protocol length): cho biết độ dài địa chỉ mạng (4 byte)

- Opcode (operation code): mã lệnh yêu cầu: ; mã lệnh trả lời .

- Sender data link: địa chỉ mức liên kết của thiết bị phát gói dữ liệu này.

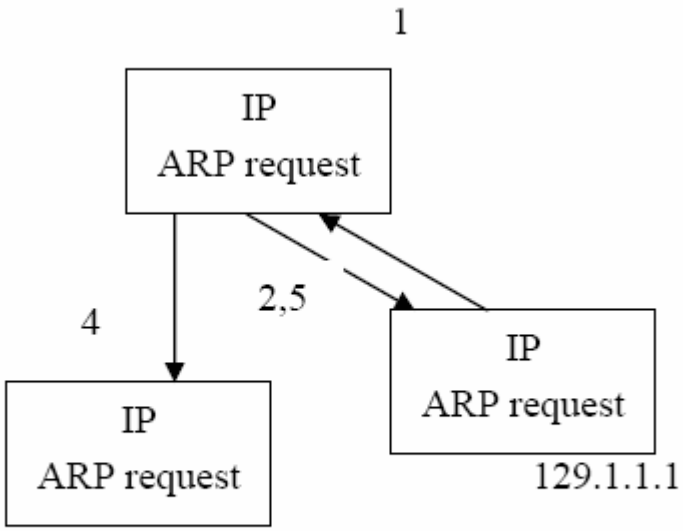
- Sender network : địa chỉ IP của thiết bị phát.

- Tagret data link: trong yêu cầu đây là địa chỉ mức liên kết cần tìm (thông thường được điền 0 bởi thiết bị gửi yêu cầu); trong trả lời đây là địa chỉ mức liên kết của thiết bị gửi yêu cầu.

- Tagret network : trong yêu cầu đây là địa chỉ IP mà địa chỉ mức liên kết tương ứng cần tìm; trong trả lời đây là địa chỉ IP của thiết bị gửi yêu cầu.

Mỗi khi cần tìm thích ứng địa chỉ IP - MAC, có thể tìm địa chỉ MAC tương ứng với địa IP đó trước tiên trong bảng địa chỉ IP - MAC ở mỗi hệ thống. Nếu không tìm thấy, có thể sử dụng giao thức ARP để làm việc này. Trạm làm việc gửi yêu cầu ARP (ARP_Request) tìm thích ứng địa chỉ IP -MAC đến máy phục vụ ARP - server. Máy phục vụ ARP tìm trong bảng thích ứng địa chỉ IP - MAC của mình và trả lời bằng ARP_Response cho trạm làm việc. Nếu không, máy phục vụ chuyển tiếp yêu cầu nhận được dưới dạng quảng bá cho tất cả các trạm làm việc trong mạng. Trạm nào có trùng địa chỉ IP được yêu cầu sẽ trả lời với địa chỉ MAC của mình. Tóm lại tiến trình của ARP được mô tả như sau

1. IP yêu cầu địa chỉ MAC.




Hình 3.11 Tiến trình ARP

2. Tìm kiếm trong bảng ARP.

3. Nếu tìm thấy sẽ trả lại địa chỉ MAC.

4. Nếu không tìm thấy, tạo gói ARP yêu cầu và gửi tới tất cả các trạm.

5. Tuỳ theo gói dữ liệu trả lời, ARP cập nhật vào bảng ARP và gửi địa chỉ MAC đó cho IP.

**Giao thức RARP**

Reverse ARP (Reverse Address Resolution Protocol) là giao thức giải thích ứng địa chỉ AMC - IP. Quá trình này ngược lại với quá trình giải thích ứng địa chỉ IP - MAC mô tả ở trên, nghĩa là cho trước địa chỉ mức liên kết, tìm địa chỉ IP tương ứng.

## II. Giao thức lớp chuyển tải (Transport Layer)

### 2.1. Giao thức TCP

TCP (Transmission Control Protocol) là một giao thức "có liên kết" (connection - oriented), nghĩa là cần thiết lập liên kết (logic), giữa một cặp thực thể TCP trước khi chúng trao đổi dữ liệu với nhau.

TCP cung cấp khả năng truyền dữ liệu một cách an toàn giữa các máy trạm trong hệ thống các mạng. Nó cung cấp thêm các chức năng nhằm kiểm tra tính chính xác của dữ liệu khi đến và bao gồm cả việc gửi lại dữ liệu khi có lỗi xảy ra. TCP cung cấp các chức năng chính sau:

1. Thiết lập, duy trì, kết thúc liên kết giữa hai quá trình.

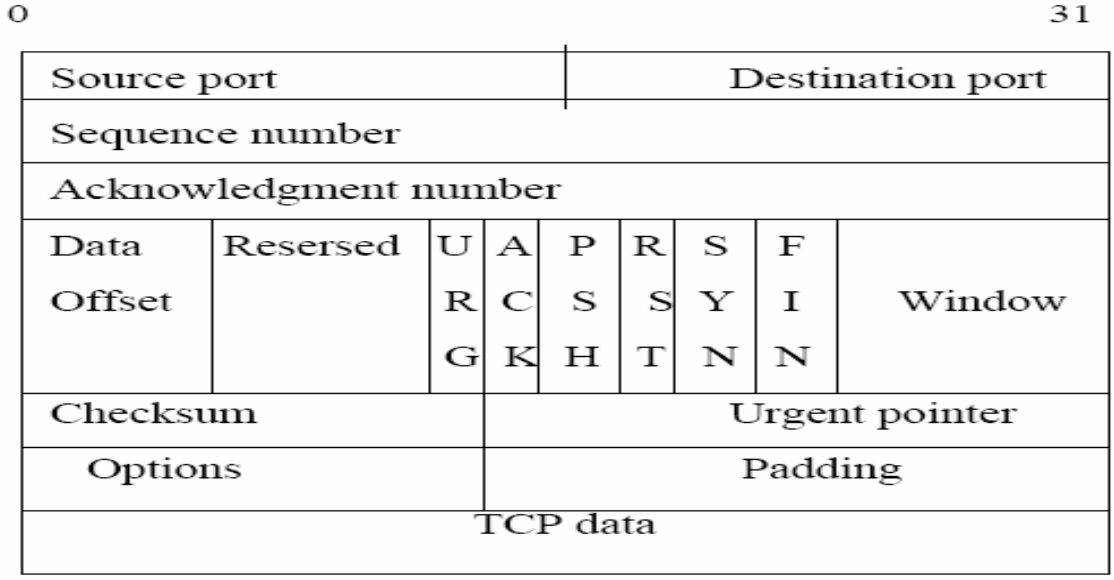
2. Phân phát gói tin một cách tin cậy.

3. Đánh số thứ tự (sequencing) các gói dữ liệu nhằm truyền dữ liệu một cách tin cậy.

4. Cho phép điều khiển lỗi.

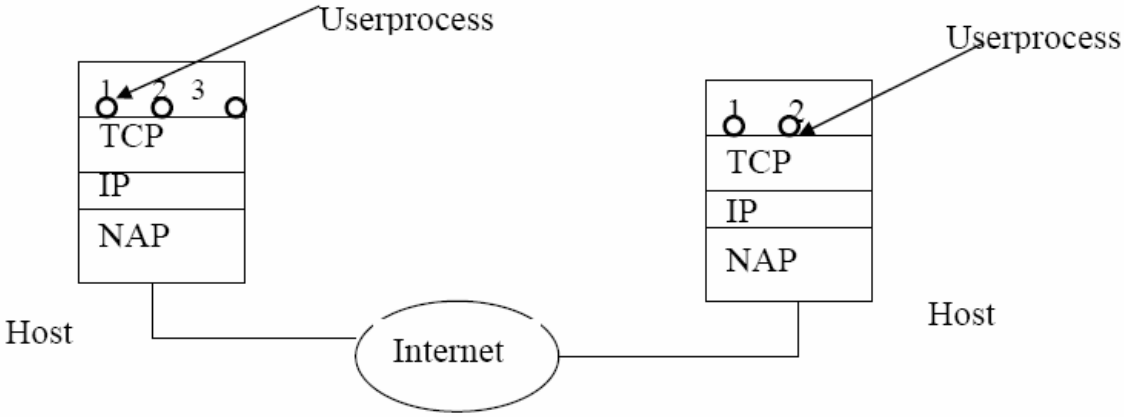
5. Cung cấp khả năng đa kết nối với các quá trình khác nhau giữa trạm nguồn và trạm đích nhất định thông qua việc sử dụng các cổng.

6. Truyền dữ liệu sử dụng cơ chế song công (full-duplex).




Hình 3.14. Khuôn dạng của TCP segment

### 2.2 Cấu trúc gói dữ liệu TCP




**NAP:** Network Access Protocol

Hình 3.15. Cổng truy cập dịch vụ TCP

- Source port (16 bits) : số hiệu cổng của trạm nguồn

- Destination port (16 bits) : số hiệu cổng của trạm đích

- Sequence Number (32 bits): số hiệu của byte đầu tiên của segment trừ khi bit SYN được thiết lập. Nếu bit SYN được thiết lập thì Sequence Number là số hiệu tuần tự khởi đầu (ISN) và byte dữ liệu đầu tiên là ISN +1.

- Acknowlegment: vị trí tương đối của byte cuối cùng đã nhận đúng bởi thực thể gửi gói ACK cộng thêm 1. Giá trị của trường này còn được gọi là số tuần tự thu. Trường này được kiểm tra chỉ khi bit ACK=1.

- Data offset (4 bits) : số tượng từ 32 bit trong TCP header. Tham số này chỉ ra vị trí bắt đầu của vùng dữ liệu

- Reserved (6 bits) : dành để dùng trong tương lai. Phải được thiết lập là 0.

- Control bits : các bit điều khiển

  - URG : vùng con trỏ khẩn (Urgent Pointer) có hiệu lực.

  - ACK : vùng báo nhận (ACK number) có hiệu lực.

- PSH : chức năng Push. PSH=1 thực thể nhận phải chuyển dữ liệu này cho ứng dụng tức thời.

  - RST : thiết lập lại (reset) kết nối.

  - SYN : đồng bộ hoá các số hiệu tuần tự, dùng để thiết lập kết nối TCP.

  - FIN : thông báo thực thể gửi đã kết thúc gửi dữ liệu.

- Window (16 bits): cấp phát credit để kiểm soát luồng dữ liệu (cơ chế của sổ). Đây chính là số lượng các byte dữ liệu, bắt đầu từ byte được chỉ ra trong vùng ACK number, mà trạm nguồn đã sẵn sàng để nhận

- Checksum (16 bits) : mã kiểm soát lỗi (theo phương pháp CRC) cho toàn bộ segment (header + data)

- Urgent pointer (16 bits) : con trỏ này trỏ tới số hiệu tuần tự của byte đi theo sau dữ liệu khẩn, cho phép bên nhận biết được độ dài của dữ liệu khẩn. Vùng này chỉ có hiệu lực khi bit URG được thiết lập

- Options (độ dài thay đổi): khai báo các option của TCP, trong đó có độ dài tối đa của vùng TCP data trong một segment

- Padding (độ dài thay đổi) : phần chèn thêm vào header để bảo đảm phần header luôn kết thúc ở một mốc 32 bits. Phần thêm này gồm toàn số 0.

- TCP data (độ dài thay đổi) : chứa dữ liệu của tầng trên, có độ dài tối đa ngầm định là 536 bytes. Giá trị này có thể điều chỉnh bằng cách khai báo trong vùng options.

Một tiến trình ứng dụng trong một host truy nhập vào các dịch vụ của TCP cung cấp thông qua một cổng (port) như sau:

Một cổng kết hợp với một địa chỉ IP tạo thành một socket duy nhất trong liên mạng. TCP được cung cấp nhờ một liên kết logic giữa một cặp socket. Một socket có thể tham gia nhiều liên kết với các socket ở xa khác nhau. Trước khi truyền dữ liệu giữa hai trạm cần phải thiết lập một liên kết TCP giữa chúng và khi kết thúc phiên truyền dữ liệu thì liên kết đó sẽ được giải phóng. Cũng giống như ở các giao thức khác, các thực thể ở tầng trên sử dụng TCP thông qua các hàm dịch vụ nguyên thuỷ (service primitives), hay còn gọi là các lời gọi hàm (function call).

## 2.3. Thiết lập và kết thúc kết nối TCP

### Thiết lập kết nối

Thiết lập kết nối TCP được thực hiện trên cơ sở phương thức bắt tay ba bước (Tree - way Handsake) hình 3.14. Yêu cầu kết nối luôn được tiến trình trạm khởi tạo, bằng cách gửi một gói TCP với cờ SYN=1 và chứa giá trị khởi tạo số tuần tự ISN của client. Giá trị ISN này là một số 4 byte không dấu và được tăng mỗi khi kết nối được yêu cầu (giá trị này quay về 0 khi nó tới giá trị $2^{32}$). Trong thông điệp SYN này còn chứa số hiệu cổng TCP của phần mềm dịch vụ mà tiến trình trạm muốn kết nối (bước 1).

Mỗi thực thể kết nối TCP đều có một giá trị ISN mới số này được tăng theo thời gian. Vì một kết nối TCP có cùng số hiệu cổng và cùng địa chỉ IP được dùng lại nhiều lần, do đó việc thay đổi giá trị INS ngăn không cho các kết nối dùng lại các dữ liệu đã cũ (stale) vẫn còn được truyền từ một kết nối cũ và có cùng một địa chỉ kết nối.

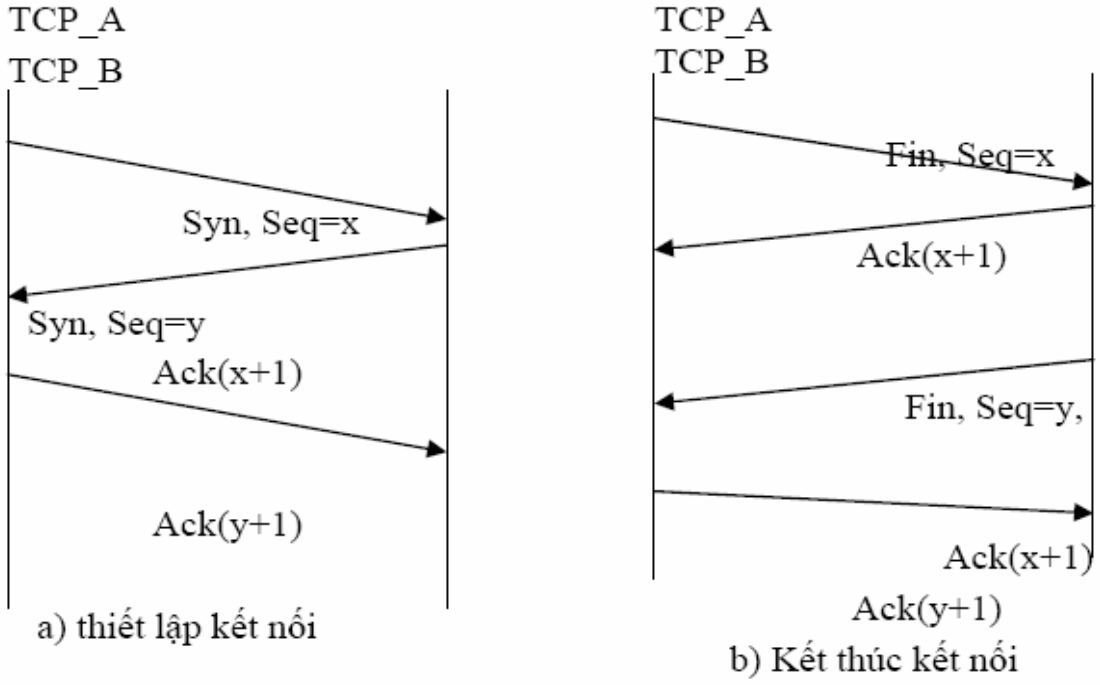
Khi thực thể TCP của phần mềm dịch vụ nhận được thông điệp SYN, nó gửi lại gói SYN cùng giá trị ISN của nó và đặt cờ ACK=1 trong trường hợp sẵn sàng nhận kết nối. Thông điệp này còn chứa giá trị ISN của tiến trình trạm trong

trường hợp số tuần tự thu để báo rằng thực thể dịch vụ đã nhận được giá trị ISN của tiến trình trạm (bước 2).

Tiến trình trạm trả lời lại gói SYN của thực thể dịch vụ bằng một thông báo trả lời ACK cuối cùng. Bằng cách này, các thực thể TCP trao đổi một cách tin cậy các giá trị ISN của nhau và có thể bắt đầu trao đổi dữ liệu. Không có thông điệp nào trong ba bước trên chứa bất kỳ dữ liệu gì; tất cả thông tin trao đổi đều nằm trong phần tiêu đề của thông điệp TCP (bước 3).

**Kết thúc kết nối**

Khi có nhu cầu kết thúc kết nối, thực thể TCP, ví dụ cụ thể A gửi yêu cầu kết thúc kết nối với FIN=1. Vì kết nối TCP là song công (full-duplex) nên mặc dù nhận được yêu cầu kết thúc kết nối của A (A thông báo hết số liệu gửi) thực thể B vẫn có thể tiếp tục truyền số liệu cho đến khi B không còn số liệu để gửi và thông báo cho A bằng yêu cầu kết thúc kết nối với FIN=1 của mình. Khi thực thể TCP đã nhận được thông điệp FIN và sau khi đã gửi thông điệp FIN của chính mình, kết nối TCP thực sụ kết thúc.




Hình 3.16. Quá trình kết nối theo ba bước

## Chương 1: Tổng quan về công nghệ mạng máy tính và mạng cục bộ

Chương này cung cấp các khái niệm, các kiến thức cơ bản nhất về mạng máy tính và phân loại mạng máy tính. Các nội dung giới thiệu mang tính tổng quan về mạng cục

bộ, kiến trúc mạng cục bộ, phương pháp truy cập trong mạng cục bộ và các chuẩn vật lý về các thiết bị mạng. Đây là những kiến thức cơ bản rất hữu ích do phạm vi sử dụng của mạng cục bộ là đang phổ biến hiện nay. Hầu hết các cơ quan, tổ chức, công ty có sử dụng công nghệ thông tin đều thiết lập mạng cục bộ riêng.

Các khái niệm, nội dung cơ bản trong chương 1 cần phải nắm vững đối với tất cả các học viên vì chúng sẽ được sử dụng nhiều trong các chương tiếp theo.

## Mục 1: Mạng máy tính

## I. Lịch sử mạng máy tính

Internet bắt nguồn từ đề án ARPANET (Advanced Research Project Agency Network) khởi sự trong năm 1969 bởi Bộ Quốc phòng Mỹ (American Department of Defense). Đề án ARPANET với sự tham gia của một số trung tâm nghiên cứu, đại học tại Mỹ (UCLA, Stanford, . . . ) nhằm mục đích thiết kế một mạng WAN (Wide Area Network) có khả năng tự bảo tồn chống lại sự phá hoại một phân mạng bằng chiến tranh nguyên tử. Đề án này dẫn tới sự ra đời của nghi thức truyền IP (Internet Protocol). Theo nghi thức này, thông tin truyền sẽ được đóng thành các gói dữ liệu và truyền trên mạng theo nhiều đường khác nhau từ người gửi tới nơi người nhận. Một hệ thống máy tính nối trên mạng gọi là **Router** làm nhiệm vụ tìm đường đi tối ưu cho các gói dữ liệu, tất cả các máy tính trên mạng đều tham dự vào việc truyền dữ liệu, nhờ vậy nếu một phân mạng bị phá huỷ các **Router** có thể tìm đường khác để truyền thông tin tới người nhận. Mạng ARPANET được phát triển và sử dụng trước hết trong các trường đại học, các cơ quan nhà nước Mỹ, tiếp theo đó, các trung tâm tính toán lớn, các trung tâm truyền vô tuyến điện và vệ tinh được nối vào mạng, . . . trên cơ sở này, ARPANET được nối với khắp các vùng trên thế giới.

Tới năm 1983, trước sự thành công của việc triển khai mạng ARPANET, Bộ quốc phòng Mỹ tách một phân mạng giành riêng cho quân đội Mỹ (MILNET). Phần còn lại, gọi là NSFnet, được quản lý bởi NSF (National Science Foundation) NSF dùng 5 siêu máy tính để làm **Router** cho mạng, và lập một tổ chức không chính phủ để quản lý mạng, chủ yếu dùng cho đại học và nghiên cứu cơ bản trên toàn thế giới. Tới năm 1987, NSFnet mở cửa cho cá nhân và cho các công ty tư nhân (BITnet), tới năm 1988 siêu mạng được mang tên INTERNET.

Tuy nhiên cho tới năm 1988, việc sử dụng INTERNET còn hạn chế trong các dịch vụ truyền mạng (FTP), thư điện tử(E-mail), truy nhập từ xa (TELNET) không thích ứng với nhu cầu kinh tế và đời sống hàng ngày. INTERNET chủ yếu được dùng trong môi trường nghiên cứu khoa học và giảng dạy đại học. Trong năm 1988, tại trung tâm nghiên cứu nguyên tử của Pháp CERN (Centre Européen de Recherche Nuclaire) ra đời đề án Mạng nhện thế giới WWW (World Wide Web). Đề án này,

nhằm xây dựng một phương thức mới sử dụng INTERNET, gọi là phương thức Siêu văn bản (HyperText). Các tài liệu và hình ảnh được trình bày bằng ngôn ngữ HTML (HyperText Markup Language) và được phát hành trên INTERNET qua các hệ chủ làm việc với nghi thức HTTP (HyperText Transport Protocol). Từ năm 1992, phương thức làm việc này được đưa ra thử nghiệm trên INTERNET, rất nhanh chóng, các công ty tư nhân tìm thấy qua phương thức này cách sử dụng INTERNET trong kinh tế và đời sống. Vốn đầu tư vào INTERNET được nhân lên hàng chục lần. Từ năm 1994 INTERNET trở thành siêu mạng kinh doanh. Số các công ty sử dụng INTERNET vào việc kinh doanh và quảng cáo lên gấp hàng nghìn lần kể từ năm 1995. Doanh số giao dịch thương mại qua mạng INTERNET lên hàng chục tỉ USD trong năm 1996 . . .

Với phương thức siêu văn bản, người sử dụng, qua một phần mềm truy đọc (Navigator, Browser), có thể tìm đọc tất cả các tài liệu siêu văn bản công bố tại mọi nơi trên thế giới (kể cả hình ảnh và tiếng nói). Với công nghệ WWW, chúng ta bước vào giai đoạn mà mọi thông tin có thể có ngay trên bàn làm việc của mình. Mỗi công ty hoặc người sử dụng, được phân phối một trang cội nguồn (Home Page) trên hệ chủ HTTP. Trang cội nguồn, là siêu văn bản gốc, để tự do có thể tìm tới tất cả các siêu văn bản khác mà người sử dụng muốn phát hành. Địa chỉ của trang cội nguồn được tìm thấy từ khắp mọi nơi trên thế giới. Vì vậy, đối với một xí nghiệp, trang cội nguồn trở thành một văn phòng đại diện điện tử trên INTERNET. Từ khắp mọi nơi, khách hàng có thể xem các quảng cáo và liên hệ trực tiếp với xí nghiệp qua các dòng siêu liên (HyperLink) trong siêu văn bản.

Tới năm 1994, một điểm yếu của INTERNET là không có khả năng lập trình cục bộ, vì các máy nối vào mạng không đồng bộ và không tương thích. Thiếu khả năng này, INTERNET chỉ được dùng trong việc phát hành và truyền thông tin chứ không dùng để xử lý thông tin được. Trong năm 1994, hãng máy tính SUN Corporation công bố một ngôn ngữ mới, gọi là JAVA (cafe), cho phép lập trình cục bộ trên INTERNET, các chương trình JAVA được gọi thẳng từ các siêu văn bản qua các siêu liên (Applet). Vào mùa thu năm 1995, ngôn ngữ JAVA chính thức ra đời, đánh dấu một bước tiến quan trọng trong việc sử dụng INTERNET. Trước hết, một chương trình JAVA, sẽ được chạy trên máy khách (Workstation) chứ không phải trên máy chủ (Server). Điều này cho phép sử dụng công suất của tất cả các máy khách vào việc xử lý số liệu. Hàng triệu máy tính (hoặc vi tính) có thể thực hiện cùng một lúc một chương trình ghi trên một siêu văn bản trong máy chủ. Việc lập trình trên INTERNET cho phép truy nhập từ một trang siêu văn bản vào các chương trình xử lý thông tin, đặc biệt là các chương trình điều hành và quản lý thông tin của một xí nghiệp. phương thức làm việc này, được gọi là INTRANET. Chỉ trong năm 1995-1996, hàng trăm nghìn dịch vụ phần mềm INTRANET được phát triển. Nhiều hãng máy tính và phần mềm như Microsoft, SUN, IBM, Oracle, Netscape,... đã phát triển và kinh doanh hàng

loạt phần mềm hệ thống và phần mềm cơ bản để phát triển các ứng dụng INTERNET / INTRANET.

# II. Giới thiệu mạng máy tính

## I.1. I.Định nghĩa mạng máy tính và mục đích của việc kết nối mạng

### I.1.1. Nhu cầu của việc kết nối mạng máy tính

Việc nối máy tính thành mạng từ lâu đã trở thành một nhu cầu khách quan vì :

- Có rất nhiều công việc về bản chất là phân tán hoặc về thông tin, hoặc về xử lý hoặc cả hai đòi hỏi có sự kết hợp truyền thông với xử lý hoặc sử dụng phương tiện từ xa.

- Chia sẻ các tài nguyên trên mạng cho nhiều người sử dụng tại một thời điểm (ổ cứng, máy in, ổ CD ROM . . .)

- Nhu cầu liên lạc, trao đổi thông tin nhờ phương tiện máy tính.

- Các ứng dụng phần mềm đòi hòi tại một thời điểm cần có nhiều người sử dụng, truy cập vào cùng một cơ sở dữ liệu.

### I.1.2. Định nghĩa mạng máy tính

Nói một cách ngắn gọn thì mạng máy tính là tập hợp các máy tính độc lập (autonomous) được kết nối với nhau thông qua các đường truyền vật lý và tuân theo các quy ước truyền thông nào đó.

Khái niệm máy tính độc lập được hiểu là các máy tính không có máy nào có khả năng khởi động hoặc đình chỉ một máy khác.

Các đường truyền vật lý được hiểu là các môi trường truyền tín hiệu vật lý (có thể là hữu tuyến hoặc vô tuyến).

Các quy ước truyền thông chính là cơ sở để các máy tính có thể "nói chuyện" được với nhau và là một yếu tố quan trọng hàng đầu khi nói về công nghệ mạng máy tính.

## I.2. Đặc trưng kỹ thuật của mạng máy tính

Một mạng máy tính có các đặc trưng kỹ thuật cơ bản như sau:

### I.2.1. Đường truyền

Là thành tố quan trọng của một mạng máy tính, là phương tiện dùng để truyền các tín hiệu điện tử giữa các máy tính. Các tín hiệu điệu tử đó chính là các thông tin, dữ liệu được biểu thị dưới dạng các xung nhị phân (ON_OFF), mọi tín hiệu truyền giữa các máy tính với nhau đều thuộc sóng điện từ, tuỳ theo tần số mà ta có thể dùng các đường truyền vật lý khác nhau

Đặc trưng cơ bản của đường truyền là giải thông nó biểu thị khả năng truyền tải tín hiệu của đường truyền.

Thông thuờng người ta hay phân loại đường truyền theo hai loại:

- Đường truyền hữu tuyến (các máy tính được nối với nhau bằng các dây cáp mạng).

- Đường truyền vô tuyến: các máy tính truyền tín hiệu với nhau thông qua các sóng vô tuyền với các thiết bị điều chế/giải điều chế ở các đầu mút.

### I.2.2. Kỹ thuật chuyển mạch:

Là đặc trưng kỹ thuật chuyển tín hiệu giữa các nút trong mạng, các nút mạng có chức năng hướng thông tin tới đích nào đó trong mạng, hiện tại có các kỹ thuật chuyển mạch như sau:

- Kỹ thuật chuyển mạch kênh: Khi có hai thực thể cần truyền thông với nhau thì giữa chúng sẽ thiết lập một kênh cố định và duy trì kết nối đó cho tới khi hai bên ngắt liên lạc. Các dữ liệu chỉ truyền đi theo con đường cố định đó.

- Kỹ thuật chuyển mạch thông báo: thông báo là một đơn vị dữ liệu của người sử dụng có khuôn dạng được quy định trước. Mỗi thông báo có chứa các thông tin điều khiển trong đó chỉ rõ đích cần truyền tới của thông báo. Căn cứ vào thông tin điều khiển này mà mỗi nút trung gian có thể chuyển thông báo tới nút kế tiếp trên con đường dẫn tới đích của thông báo

- Kỹ thuật chuyển mạch gói: ở đây mỗi thông báo được chia ra thành nhiều gói nhỏ hơn được gọi là các gói tin (packet) có khuôn dạng qui định trước. Mỗi gói tin cũng chứa các thông tin điều khiển, trong đó có địa chỉ nguồn (người gửi) và địa chỉ đích (người nhận) của gói tin. Các gói tin của cùng một thông báo có thể được gởi đi qua mạng tới đích theo nhiều con đường khác nhau.

### I.2.3. Kiến trúc mạng

Kiến trúc mạng máy tính (network architecture) thể hiện cách nối các máy tính với nhau và tập hợp các quy tắc, quy ước mà tất cả các thực thể tham gia truyền thông trên mạng phải tuân theo để đảm bảo cho mạng hoạt động tốt.

Khi nói đến kiến trúc của mạng người ta muốn nói tới hai vấn đề là hình trạng mạng (Network topology) và giao thức mạng (Network protocol)

- Network Topology: Cách kết nối các máy tính với nhau về mặt hình học mà ta gọi là tô pô của mạng. Các hình trạng mạng cơ bản đó là: hình sao, hình bus, hình vòng

- Network Protocol: Tập hợp các quy ước truyền thông giữa các thực thể truyền thông mà ta gọi là giao thức (hay nghi thức) của mạng. Các giao thức thường gặp nhất là : TCP/IP, NETBIOS, IPX/SPX, . . .

### I.2.4. Hệ điều hành mạng

Hệ điều hành mạng là một phần mềm hệ thống có các chức năng sau:

- Quản lý tài nguyên của hệ thống, các tài nguyên này gồm:

+ Tài nguyên thông tin (về phương diện lưu trữ) hay nói một cách đơn giản là quản lý tệp. Các công việc về lưu trữ tệp, tìm kiếm, xoá, copy, nhóm, đặt các thuộc tính đều thuộc nhóm công việc này

+ Tài nguyên thiết bị. Điều phối việc sử dụng CPU, các ngoại vi... để tối ưu hoá việc sử dụng

- Quản lý người dùng và các công việc trên hệ thống.

Hệ điều hành đảm bảo giao tiếp giữa người sử dụng, chương trình ứng dụng với thiết bị của hệ thống.

- Cung cấp các tiện ích cho việc khai thác hệ thống thuận lợi (ví dụ FORMAT đĩa, sao chép tệp và thư mục, in ấn chung ...)

Các hệ điều hành mạng thông dụng nhất hiện nay là: WindowsNT, Windows9X, Windows 2000, Unix, Novell.

## I.3. Phân loại mạng máy tính

Có nhiều cách phân loại mạng khác nhau tuỳ thuộc vào yếu tố chính được chọn dùng để làm chỉ tiêu phân loại, thông thường người ta phân loại mạng theo các tiêu chí như sau

- Khoảng cách địa lý của mạng

- Kỹ thuật chuyển mạch mà mạng áp dụng

- Kiến trúc mạng

- Hệ điều hành mạng sử dụng ...

Tuy nhiên trong thực tế người ta thường chỉ phân loại theo hai tiêu chí đầu tiên

### I.3.1. Phân loại mạng theo khoảng cách địa lý :

Nếu lấy khoảng cách địa lý làm yếu tố phân loại mạng thì ta có mạng cục bộ, mạng đô thị, mạng diện rộng, mạng toàn cầu.

Mạng cục bộ ( LAN - Local Area Network ) : là mạng được cài đặt trong phạm vi tương đối nhỏ hẹp như trong một toà nhà, một xí nghiệp...với khoảng cách lớn nhất giữa các máy tính trên mạng trong vòng vài km trở lại.

Mạng đô thị ( MAN - Metropolitan Area Network ) : là mạng được cài đặt trong phạm vi một đô thị, một trung tâm văn hoá xã hội, có bán kính tối đa khoảng 100 km trở lại.

Mạng diện rộng ( WAN - Wide Area Network ) : là mạng có diện tích bao phủ rộng lớn, phạm vi của mạng có thể vượt biên giới quốc gia thậm chí cả lục địa.

Mạng toàn cầu ( GAN - Global Area Network ) : là mạng có phạm vi trải rộng toàn cầu.

### I.3.2. Phân loại theo kỹ thuật chuyển mạch:

Nếu lấy kỹ thuật chuyển mạch làm yếu tố chính để phân loại sẽ có: mạng chuyển mạch kênh, mạng chuyển mạch thông báo và mạng chuyển mạch gói.

Mạch chuyển mạch kênh (circuit switched network) : Khi có hai thực thể cần truyền thông với nhau thì giữa chúng sẽ thiết lập một kênh cố định và duy trì kết nối đó cho tới khi hai bên ngắt liên lạc. Các dữ liệu chỉ truyền đi theo con đường cố định đó. Nhược điểm của chuyển mạch kênh là tiêu tốn thời gian để thiết lập kênh truyền cố định và hiệu suất sử dụng mạng không cao.

Mạng chuyển mạch thông báo (message switched network) : Thông báo là một đơn vị dữ liệu của người sử dụng có khuôn dạng được quy định trước. Mỗi thông báo có chứa các thông tin điều khiển trong đó chỉ rõ đích cần truyền tới của thông báo. Căn cứ vào thông tin điều khiển này mà mỗi nút trung gian có thể chuyển thông báo tới nút kế tiếp trên con đường dẫn tới đích của thông báo. Như vậy mỗi nút cần phải lưu giữ tạm thời để đọc thông tin điều khiển trên thông báo, nếu thấy thông báo không gửi cho mình thì tiếp tục chuyển tiếp thông báo đi. Tuỳ vào điều kiện của mạng mà thông báo có thể được chuyển đi theo nhiều con đường khác nhau.

Ưu điểm của phương pháp này là :

- Hiệu suất sử dụng đường truyền cao vì không bị chiếm dụng độc quyền mà được phân chia giữa nhiều thực thể truyền thông.

- Mỗi nút mạng có thể lưu trữ thông tin tạm thời sau đó mới chuyển thông báo đi, do đó có thể điều chỉnh để làm giảm tình trạng tắc nghẽn trên mạng.

- Có thể điều khiển việc truyền tin bằng cách sắp xếp độ ưu tiên cho các thông báo.

- Có thể tăng hiệu suất sử dụng giải thông của mạng bằng cách gắn địa chỉ quảng bá (broadcast addressing) để gửi thông báo đồng thời tới nhiều đích.

Nhược điểm của phương pháp này là:

- Không hạn chế được kích thước của thông báo dẫn đến phí tổn lưu giữ tạm thời cao và ảnh hưởng đến thời gian trả lời yêu cầu của các trạm .

Mạng chuyển mạch gói (packet switched network) : ở đây mỗi thông báo được chia ra thành nhiều gói nhỏ hơn được gọi là các gói tin (packet) có khuôn dạng qui định trước. Mỗi gói tin cũng chứa các thông tin điều khiển, trong đó có địa chỉ nguồn (người gửi) và địa chỉ đích (người nhận) của gói tin. Các gói tin của cùng một thông báo có thể được gởi đi qua mạng tới đích theo nhiều con đường khác nhau.

Phương pháp chuyển mạch thông báo và chuyển mạch gói là gần giống nhau. Điểm khác biệt là các gói tin được giới hạn kích thước tối đa sao cho các nút mạng (các nút chuyển mạch) có thể xử lý toàn bộ gói tin trong bộ nhớ mà không phải lưu giữ tạm thời trên đĩa. Bởi vậy nên mạng chuyển mạch gói truyền dữ liệu hiệu quả hơn so với mạng chuyển mạch thông báo.

Tích hợp hai kỹ thuật chuyển mạch kênh và chuyển mạch gói vào trong một mạng thống nhất được mạng tích hợp số ISDN (Integated Services Digital Network).

### I.3.3. Phân loại theo kiến trúc mạng sử dụng

Kiến trúc của mạng bao gồm hai vấn đề: hình trạng mạng (Network topology) và giao thức mạng (Network protocol)

Hình trạng mạng: Cách kết nối các máy tính với nhau về mặt hình học mà ta gọi là tô pô của mạng

Giao thức mạng: Tập hợp các quy ước truyền thông giữa các thực thể truyền thông mà ta gọi là giao thức (hay nghi thức) của mạng

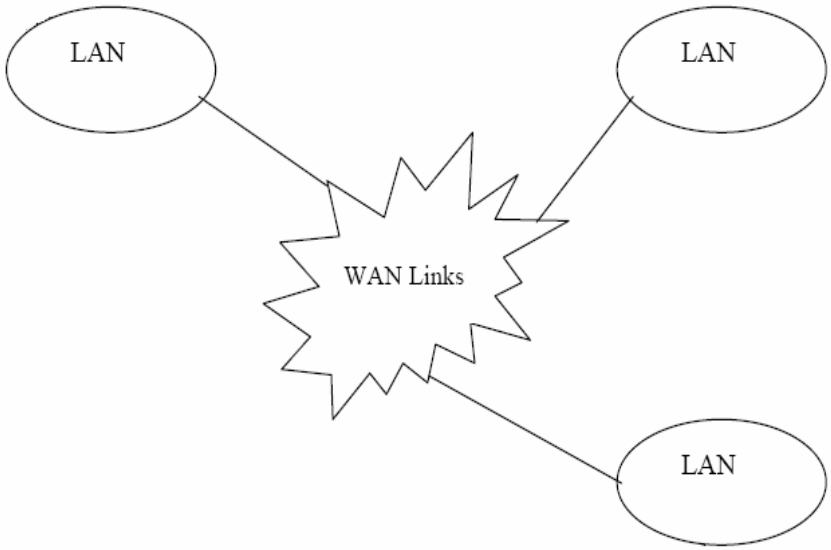
Khi phân loại theo topo mạng người ta thường có phân loại thành: mạng hình sao, tròn, tuyến tính

Phân loại theo giao thức mà mạng sử dụng người ta phân loại thành mạng : TCP/IP, mạng NETBIOS . ..

Tuy nhiên cách phân loại trên không phổ biến và chỉ áp dụng cho các mạng cục bộ.

### I.3.4. Phân loại theo hệ điều hàng mạng

Nếu phân loại theo hệ điều hành mạng người ta chia ra theo mô hình mạng ngang hàng, mạng khách/chủ hoặc phân loại theo tên hệ điều hành mà mạng sử dụng: Windows NT, Unix, Novell . . .




## I.4. Giới thiệu các mạng máy tính thông dụng nhất

### I.4.1. Mạng cục bộ

Một mạng cục bộ là sự kết nối một nhóm máy tính và các thiết bị kết nối mạng được lắp đặt trên một phạm vị địa lý giới hạn, thường trong một toà nhà hoặc một khu công sở nào đó.

Mạng cục bộ có các đặc tính sau:

- Tốc độ truyền dữ liệu cao

- Phạm vi địa lý giới hạn

-Sở hữu của một cơ quan/tổ chức

### I.4.2. Mạng diện rộng với kết nối LAN TO LAN

Mạng diện rộng bao giờ cũng là sự kết nối của các mạng LAN, mạng diện rộng có thể trải trên phạm vi một vùng, quốc gia hoặc cả một lục địa thậm chí trên phạm vi toàn cầu.

- Tốc độ truyền dữ liệu không cao

- Phạm vi địa lý không giới hạn

- Thường triển khai dựa vào các công ty truyền thông, bưu điện và dùng các hệ thống truyền thông này để tạo dựng đường truyền

- Một mạng WAN có thể là sở hữu của một tập đoàn/tổ chức hoặc là mạng kết nối của nhiều tập đoàn/tỗ chức 16

### I.4.3. Liên mạng INTERNET

Với sự phát triển nhanh chóng của công nghệ là sự ra đời của liên mạng INTERNET,

- Là một mạng toàn cầu

- Là sự kết hợp của vô số các hệ thống truyền thông, máy chủ cung cấp thông tin và dịch vụ, các máy trạm khai thác thông tin

- Dựa trên nhiều nền tảng truyền thông khác nhau, nhưng đều trên nền giao thức TCP/IP

- Là sở hữu chung của toàn nhân loại

- Càng ngày càng phát triển mãnh liệt

### I.4.4. Mạng INTRANET

Thực sự là một mạng INTERNET thu nhỏ vào trong một cơ quan/công ty/tổ chức hay một bộ/nghành . . ., giới hạn phạm vi người sử dụng, có sử dụng các công nghệ kiểm soát truy cập và bảo mật thông tin .

Được phát triển từ các mạng LAN, WAN dùng công nghệ INTERNET

## II. Mạng cục bộ, kiến trúc mạng cục bộ

### II.1. Mạng cục bộ

Tên gọi "mạng cục bộ" được xem xét từ quy mô của mạng. Tuy nhiên, đó không phải là đặc tính duy nhất của mạng cục bộ nhưng trên thực tế, quy mô của mạng quyết định nhiều đặc tính và công nghệ của mạng. Sau đây là một số đặc điểm của mạng cục bộ:

Đặc điểm của mạng cục bộ

- Mạng cục bộ có quy mô nhỏ, thường là bán kính dưới vài km. Đặc điểm này cho phép không cần dùng các thiết bị dẫn đường với các mối liên hệ phức tạp

- Mạng cục bộ thường là sở hữu của một tổ chức. Điều này dường như có vẻ ít quan trọng nhưng trên thực tế đó là điều khá quan trọng để việc quản lý mạng có hiệu quả.

- Mạng cục bộ có tốc độ cao và ít lỗi. Trên mạng rộng tốc độ nói chung chỉ đạt vài Kbit/s. Còn tốc độ thông thường trên mạng cục bộ là 10, 100 Kb/s và tới nay với Gigabit Ethernet, tốc độ trên mạng cục bộ có thể đạt 1Gb/s. Xác suất lỗi rất thấp.

### II.2. Kiến trúc mạng cục bộ

### II.2.1. Đồ hình mạng (Network Topology)

*** Định nghĩa Topo mạng:**

Cách kết nối các máy tính với nhau về mặt hình học mà ta gọi là tô pô của mạng

Có hai kiểu nối mạng chủ yếu đó là :

- Nối kiểu điểm - điểm (point - to - point).

- Nối kiểu điểm - nhiều điểm (point - to - multipoint hay broadcast).

Theo kiểu điểm - điểm, các đường truyền nối từng cặp nút với nhau và mỗi nút đều có trách nhiệm lưu giữ tạm thời sau đó chuyển tiếp dữ liệu đi cho tới đích. Do cách làm việc như vậy nên mạng kiểu này còn được gọi là mạng "lưu và chuyển tiếp" (store and forward).

Theo kiểu điểm - nhiều điểm, tất cả các nút phân chia nhau một đường truyền vật lý chung. Dữ liệu gửi đi từ một nút nào đó sẽ được tiếp nhận bởi tất cả các nút còn lại trên mạng, bởi vậy cần chỉ ra địa chỉ đích của dữ liệu để căn cứ vào đó các nút kiểm tra xem dữ liệu đó có phải gửi cho mình không.

*** Phân biệt kiểu tô pô của mạng cục bộ và kiểu tô pô của mạng rộng.**

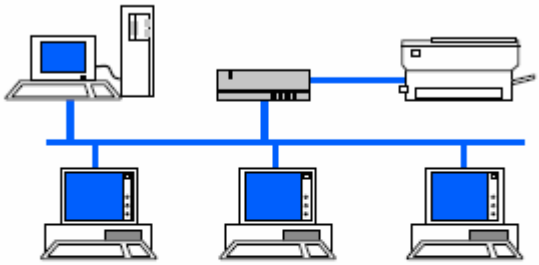
Tô pô của mạng rộng thông thường là nói đến sự liên kết giữa các mạng cục bộ thông qua các bộ dẫn đường (router). Đối với mạng rộng topo của mạng là hình trạng hình học của các bộ dẫn đường và các kênh viễn thông còn khi nói tới tô pô của mạng cục bộ người ta nói đến sự liên kết của chính các máy tính.

**a) Mạng hình sao**

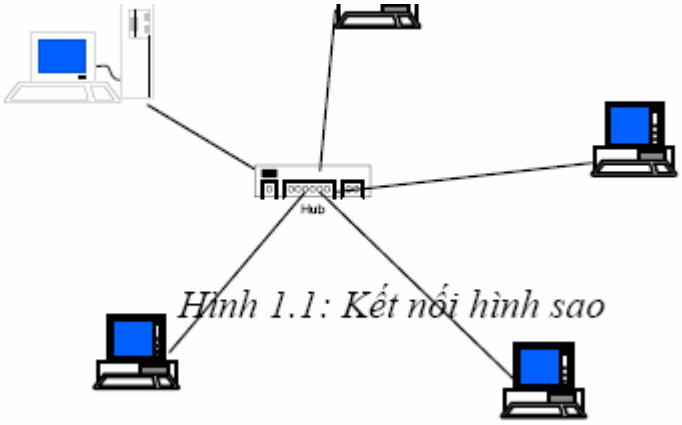
Mạng hình sao có tất cả các trạm được kết nối với một thiết bị trung tâm có nhiệm vụ nhận tín hiệu từ các trạm và chuyển đến trạm đích. Tuỳ theo yêu cầu truyền thông trên mạng mà thiết bị trung tâm có thể là bộ chuyển mạch (switch), bộ chọn đường (router) hoặc là bộ phân kênh (hub). Vai trò của thiết bị trung tâm này là thực hiện việc thiết lập các liên kết điểm-điểm (point-to-point) giữa các trạm.

Ưu điểm: Thiết lập mạng đơn giản, dễ dàng cấu hình lại mạng (thêm, bớt các trạm), dễ dàng kiểm soát và khắc phục sự cố, tận dụng được tối đa tốc độ truyền của đường truyền vật lý.

Nhược điểm: Độ dài đường truyền nối một trạm với thiết bị trung tâm bị hạn chế (trong vòng 100m, với công nghệ hiện nay). Hub



Hình 1.2. Kết nối kiểu bus




Hình 1.1: Kết nối hình sao

**b) Mạng trục tuyến tính (Bus):**

Trong mạng trục tất cả các trạm phân chia một đường truyền chung (bus). Đường truyền chính được giới hạn hai đầu bằng hai đầu nối đặc biệt gọi là terminator. Mỗi trạm được nối với trục chính qua một đầu nối chữ T (T-connector) hoặc một thiết bị thu phát (transceiver).

Khi một trạm truyền dữ liệu tín hiệu được quảng bá trên cả hai chiều của bus, tức là mọi trạm còn lại đều có thể thu được tín hiệu đó trực tiếp. Đối với các bus một chiều thì tín hiệu chỉ đi về một phía, lúc đó các terminator phải được thiết kế sao cho các tín hiệu đó phải được dội lại trên bus để cho các trạm trên mạng đều có thể thu nhận được tín hiệu đó. Như vậy với topo mạng trục dữ liệu được truyền theo các liên kết điểm-đa điểm (point-to-multipoint) hay quảng bá (broadcast).

Ưu điểm : Dễ thiết kế, chi phí thấp

Nhược điểm: Tính ổn định kém, chỉ một nút mạng hỏng là toàn bộ mạng bị ngừng hoạt động

**c) Mạng hình vòng**

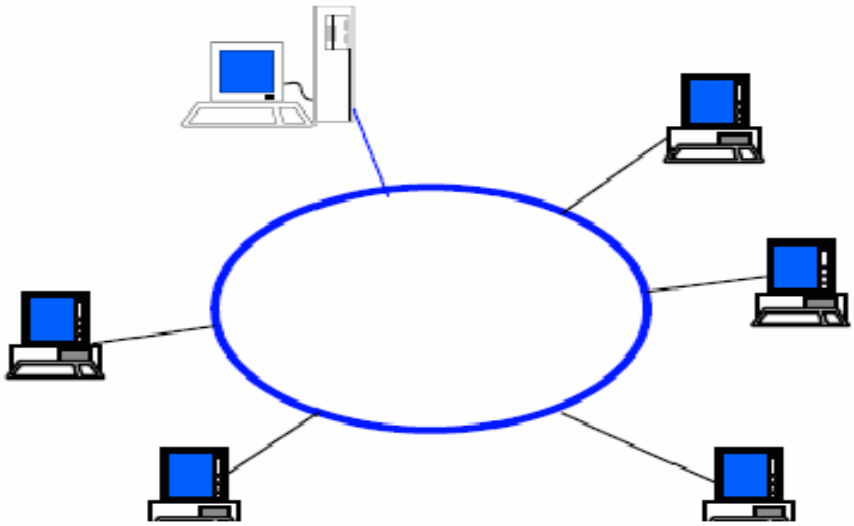
Trên mạng hình vòng tín hiệu được truyền đi trên vòng theo một chiều duy nhất. Mỗi trạm của mạng được nối với vòng qua một bộ chuyển tiếp (repeater) có nhiệm vụ nhận tín hiệu rồi chuyển tiếp đến trạm kế tiếp trên vòng. Như vậy tín hiệu được lưu chuyển trên vòng theo một chuỗi liên tiếp các liên kết điểm-điểm giữa các repeater do đó cần có giao thức điều khiển việc cấp phát quyền được truyền dữ liệu trên vòng mạng cho trạm có nhu cầu.

Để tăng độ tin cậy của mạng ta có thể lắp đặt thêm các vòng dự phòng, nếu vòng chính có sự cố thì vòng phụ sẽ được sử dụng.

Mạng hình vòng có ưu nhược điểm tương tự mạng hình sao, tuy nhiên mạng hình vòng đòi hỏi giao thức truy nhập mạng phức tạp hơn mạng hình sao.

**d) Kết nối hỗn hợp**

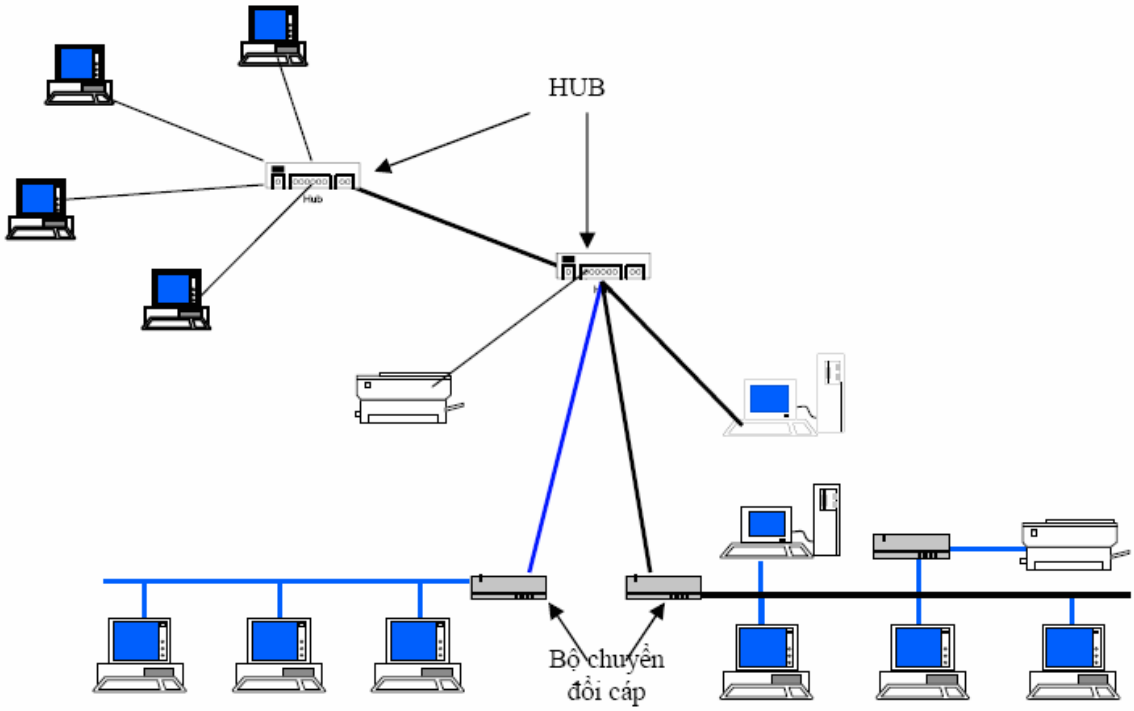
Là sự phối hợp các kiểu kết nối khác nhau, ví du hình cây là cấu trúc phân tầng của kiểu hình sao hay các HUB có thể được nối với nhau theo kiểu bus còn từ các HUB nối với các máy theo hình sao.



Hình 1.3 Kết nối kiểu vòng

## II.3. Các phương pháp truy cập đường truyền vật lý

Trong mạng cục bộ, tất cả các trạm kết nối trực tiếp vào đường truyền chung. Vì vậy tín hiệu từ một trạm đưa lên đường truyền sẽ được các trạm khác "nghe thấy". Một vấn đề khác là, nếu nhiều trạm cùng gửi tín hiệu lên đường truyền đồng thời thì tín hiệu sẽ chồng lên nhau và bị hỏng. Vì vậy cần phải có một phương pháp tổ chức chia sẻ đường truyền để việc truyền thông được đúng đắn.




Hình 1.4. Một kết nối hỗn hợp

Có hai phương pháp chia sẻ đường truyền chung thường được dùng trong các mạng cục bộ:

- Truy nhập đường truyền một cách ngẫu nhiên, theo yêu cầu. Đương nhiên phải có tính đến việc sử dụng luân phiên và nếu trong trường hợp do có nhiều trạm cùng truyền tin dẫn đến tín hiệu bị trùm lên nhau thì phải truyền lại.

- Có cơ chế trọng tài để cấp quyền truy nhập đường truyền sao cho không xảy ra xung đột

### II.3.1 Phương pháp đa truy nhập sử dụng sóng mang có phát hiện xung đột CSMA/CD (Carrier Sense Multiple Access with Collision Detection)

Giao thức CSMA (Carrier Sense Multiple Access) - đa truy nhập có cảm nhận sóng mang được sử dụng rất phổ biến trong các mạng cục bộ. Giao thức này sử dụng

phương pháp thời gian chia ngăn theo đó thời gian được chia thành các khoảng thời gian đều đặn và các trạm chỉ phát lên đường truyền tại thời điểm đầu ngăn.

Mỗi trạm có thiết bị nghe tín hiệu trên đường truyền (tức là cảm nhận sóng mang). Trước khi truyền cần phải biết đường truyền có rỗi không. Nếu rỗi thì mới được truyền. Phương pháp này gọi là LBT (Listening before talking). Khi phát hiện xung đột, các trạm sẽ phải phát lại. Có một số chiến lược phát lại như sau:

- Giao thức CSMA không kiên trì.Trạm nghe đường, nếu kênh rỗi thì truyền, nếu không thì ngừng nghe một khoảng thời gian ngẫu nhiên rồi mới thực hiện lại thủ tục. Cách này có hiệu suất dùng kênh cao hơn. (1)

- Giao thức CSMA 1-kiên trì. Khi trạm phát hiện kênh rỗi trạm truyền ngay. Nhưng nếu có xung đột, trạm đợi khoảng thời gian ngẫu nhiên rồi truyền lại. Do vậy xác suất truyền khi kênh rỗi là 1. Chính vì thế mà giao thức có tên là CSMA 1-kiên trì. (2)

- Giao thức CSMA p-kiên trì. Khi đã sẵn sàng truyền, trạm cảm nhận đường, nếu đường rỗi thì thực hiện việc truyền với xác suất là $p < 1$ (tức là ngay cả khi đường rỗi cũng không hẳn đã truyền mà đợi khoảng thời gian tiếp theo lại tiếp tục thực hiện việc truyền với xác suất còn lại $q=1-p$. (3)

• Ta thấy giải thuật (1) có hiệu quả trong việc tránh xung đột vì hai trạm cần truyền thấy đường truyền bận sẽ cùng rút lui chờ trong những khoảng thời gian ngẫu nhiên khác nhau sẽ quay lại tiếp tục nghe đường truyền. Nhược điểm của nó là có thể có thời gian không sử dụng đường truyền sau mỗi cuộc gọi.

• Giải thuật (2) cố gắng làm giảm thời gian "chết" bằng cách cho phép một trạm có thể được truyền dữ liệu ngay sau khi một cuộc truyền kết thúc. Tuy nhiên nếu lúc đó lại có nhiều trạm đang đợi để truyền dữ liệu thì khả năng xảy ra xung đột sẽ rất lớn.

• Giải thuật (3) với giá trị p được họn hợp lý có thể tối thiểu hoá được cả khả năng xung đột lẫn thời gian "chết" của đường truyền.

• Xảy ra xung đột thường là do độ trễ truyền dẫn, mấu chốt của vấn đề là: các trạm chỉ "nghe" trước khi truyền dữ liệu mà không "nghe" trong khi truyền, cho nên thực tế có xung đột thế nhưng các trạm không biết do đó vẫn truyền dữ liệu.

• Để có thể phát hiện xung đột, CSMA/CD đã bổ xung thêm các quy tắc sau đây:

- Khi một trạm truyền dữ liệu, nó vẫn tiếp tục "nghe" đường truyền . Nếu phát hiện xung đột thì nó ngừng ngay việc truyền, nhờ đó mà tiết kiệm được thời gian và giải thông, nhưng nó vẫn tiếp tục gửi tín hiệu thêm một thời gian nữa để đảm bảo rằng tất cả các trạm trên mạng đều "nghe" được sự kiện

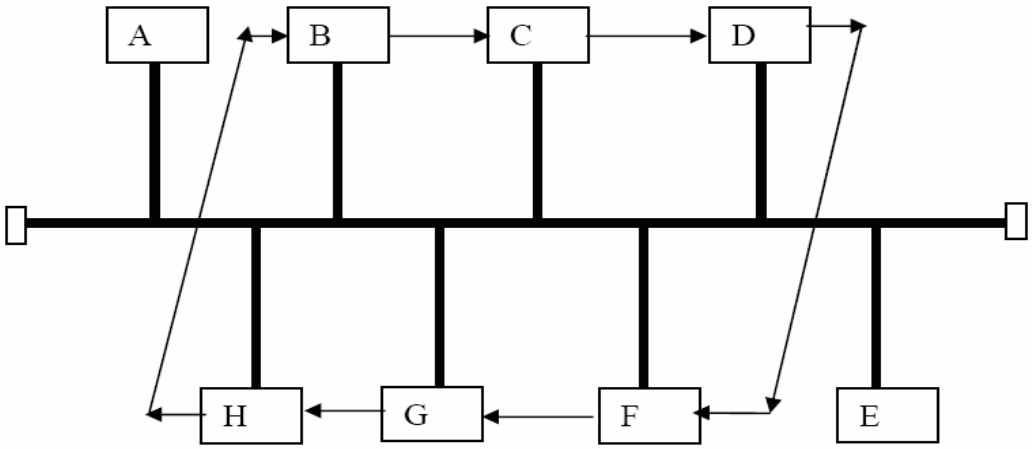
này.(như vậy phải tiếp tục nghe đường truyền trong khi truyền để phát hiện đụng độ (Listening While Talking))

- Sau đó trạm sẽ chờ trong một khoảng thời gian ngẫu nhiên nào đó rồi thử truyền lại theo quy tắc CSMA.

Giao thức này gọi là **CSMA có phát hiện xung đột** (Carrier Sense Multiple Access with Collision Detection viết tắt là CSMA/CD), dùng rộng rãi trong LAN và MAN.

## II.3.2. Phương pháp Token Bus

Nguyên lý chung của phương pháp này là để cấp phát quyền truy nhập đường truyền cho các trạm đang có nhu cầu truyền dữ liệu, một thẻ bài được lưu chuyển trên một vòng logic được thiết lập bởi các trạm đó. Khi một trạm nhận được thẻ bài thì sẽ được phép sử dụng đường truyền trong một thời gian nhất định. Trong khoảng thời gian đó nó có thể truyền một hay nhiều đơn vị dữ liệu. Khi đã truyền xong dữ liệu hoặc thời gian đã hết thì trạm đó phải chuyển thẻ bài cho trạm tiếp theo. Như vậy,




*Hình 1.5. Ví dụ về vòng logic*

công việc đầu tiên là thiết lập vòng logic (hay còn gọi là vòng ảo) bao gồm các trạm đang có nhu cầu truyền dữ liệu được xác định vị trí theo một chuỗi thứ tự mà trạm cuối cùng của chuỗi sẽ tiếp liền sau bởi trạm đầu tiên. Mỗi trạm sẽ biết địa chỉ của trạm liền trước và kề sau nó. Thứ tự của các trạm trên vòng logic có thể độc lập với thứ tự vật lý. Các trạm không hoặc chưa có nhu cầu truyền dữ liệu không được vào trong vòng logic.

Trong ví dụ trên, các trạm A, E nằm ngoài vòng logic do đó chỉ có thể tiếp nhận được dữ liệu dành cho chúng.

Việc thiết lập vòng logic không khó nhưng việc duy trì nó theo trạng thái thực tế của mạng mới là khó. Cụ thể phải thực hiện các chức năng sau:

a) Bổ xung một trạm vào vòng logic : các trạm nằm ngoài vòng logic cần được xem xét một cách định kỳ để nếu có nhu cầu truyền dữ liệu thì được bổ xung vào vòng logic.

b) Loại bỏ một vòng khỏi vòng logic : khi một trạm không có nhu cầu truyền dữ liệu thì cần loại bỏ nó ra khỏi vòng logic để tối ưu hoá việc truyền dữ liệu bằng thẻ bài

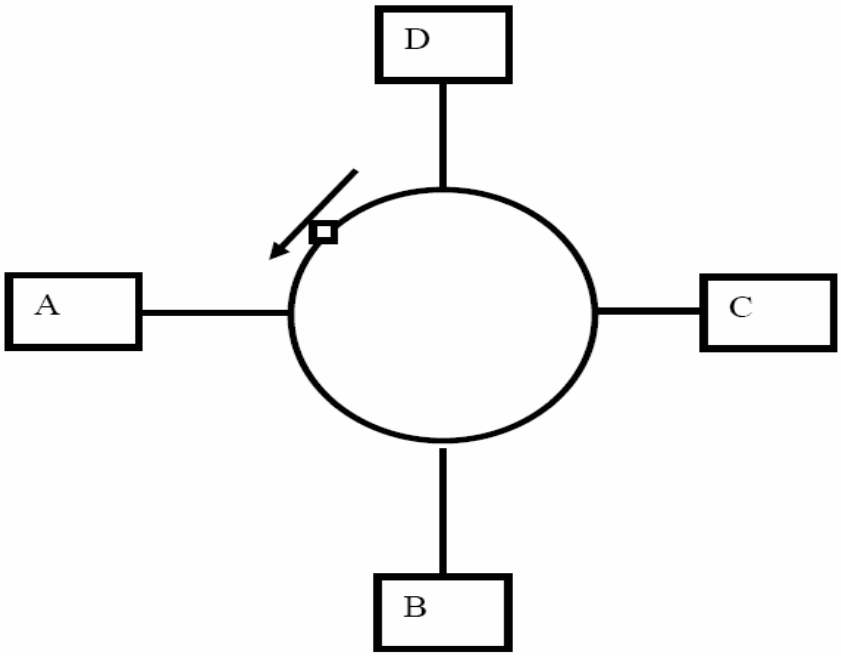
c) Quản lý lỗi : một số lỗi có thể xẩy ra như trùng hợp địa chỉ, hoặc đứt vòng logic.

d) Khởi taọ vòng logic : khi khởi tạo mạng hoặc khi đứt vòng logic cần phải khởi tạo lại vòng logic.

## II.3.2. Phương pháp Token Ring

Phương pháp này cũng dựa trên nguyên tắc dùng thẻ bài để cấp phát quyền truy nhập đường truyền. Nhưng ở đây thẻ bài lưu chuyển theo theo vòng vật lý chứ không theo vòng logic như dối với phương pháp token bus.

Thẻ bài là một đơn vị truyền dữ liệu đặc biệt trong đó có một bit biểu diễn trạng thái của thẻ (bận hay rỗi). Một trạm muốn truyền dữ liệu phải chờ cho tới khi nhận được thẻ bài "rỗi". Khi đó trạm sẽ đổi bit trạng thái thành "bận" và truyền một đơn vị dữ liệu đi cùng với thẻ bài đi theo chiều của vòng. Lúc này không còn thẻ bài "rỗi " nữa do đó các trạm muốn truyền dữ liệu phải đợi. Dữ liệu tới trạm đích được sao chép




*Hình 1.6. Thẻ bài trong mạng* Ring

lại, sau đó cùng với thẻ bài trở về trạm nguồn. Trạm nguồn sẽ xoá bỏ dữ liệu đổi bit trạng thái thành "rỗi" và cho lưu chuyển thẻ trên vòng để các trạm khác có nhu cầu truyền dữ liệu được phép truyền

Sự quay trở lại trạm nguồn của dữ liệu và thẻ bài nhằm tạo khả năng báo nhận tự nhiên: trạm đích có thể gửi vào đơn vị dữ liệu (phần header) các thông tin về kết quả tiếp nhận dữ liệu của mình. Chẳng hạn các thông tin đó có thể là: trạm đích không tồn tại hoặc không hoạt động, trạm đích tồn tại nhưng dữ liệu không được sao chép, dữ liệu đã được tiếp nhận, có lỗi...

Trong phương pháp này cần giải quyết hai vấn đề có thể dẫn đến phá vỡ hệ thống đó là mất thẻ bài và thẻ bài "bận" lưu chuyển không dừng trên vòng .Có nhiều phương pháp giải quyết các vấn đề trên, dưới đây là một phương pháp được khuyến nghị:

Đối với vấn đề mất thẻ bài có thể quy định trước một trạm điều khiển chủ động. Trạm này sẽ theo dõi, phát hiện tình trạng mất thẻ bài bằng cách dùng cơ chế ngưỡng thời gian (time - out) và phục hồi bằng cách phát đi một thẻ bài "rỗi" mới.

Đối với vấn đề thẻ bài bận lưu chuyển không dừng, trạm điều khiển sử dụng một bit trên thẻ bài để đánh dấu khi gặp một thẻ bài "bận" đi qua nó. Nếu nó gặp lại thẻ bài bận với bit đã đánh dấu đó có nghĩa là trạm nguồn đã không nhận lại được đơn vị dữ liệu của mình do đó thẻ bài "bận" cứ quay vòng mãi. Lúc đó trạm điều khiển sẽ chủ động đổi bit trạng thái "bận" thành "rỗi" và cho thẻ bài chuyển tiếp trên vòng. Trong phương pháp này các trạm còn lại trên mạng sẽ đóng vai trò bị động, chúng theo dõi phát hiện tình trạng sự cố trên trạm chủ động và thay thế trạm chủ động nếu cần.

## III. Chuẩn hoá mạng máy tính

### III.1. Vấn đề chuẩn hoá mạng và các tổ chức chuẩn hoá mạng

Khi thiết kế, các nhà thiết kế tự do lựa chọn kiến trúc mạng cho riêng mình. Từ đó dẫn tới tình trạng không tương thích giữa các mạng máy tính với nhau. Nhu cầu trao đổi thông tin càng lớn thúc đẩy việc xây dựng khung chuẩn về kiến trúc mạng để làm căn cứ cho các nhà thiết kế và chế tạo thiết bị mạng.

Chính vì lý do đó, tổ chức tiêu chuẩn hoá quốc tế ISO (Internatinal Organnization for Standarzation) đã xây dựng mô hình tham chiếu cho việc kết nối các hệ thống mở OSI (reference model for Open Systems Interconnection). Mô hình này là cơ sở cho việc kết nối các hệ thống mở phục vụ cho các ứng dụng phân tán.

Có hai loại chuẩn cho mạng đó là :

- Truyền tin dạng bit qua kênh vật lý.
- Có thể có nhiều kênh.

**b) Lớp liên kết dữ liệu**

Lớp này đảm bảo việc biến đổi các tin dạng bit nhận được từ lớp dưới (vật lý) sang khung số liệu, thông báo cho hệ phát, kết quả thu được sao cho các thông tin truyền lên cho mức 3 không có lỗi. Các thông tin truyền ở mức 1 có thể làm hỏng các thông tin khung số liệu (frame error). Phần mềm mức hai sẽ thông báo cho mức một truyền lại các thông tin bị mất / lỗi. Đồng bộ các hệ có tốc độ xử lý tính khác nhau, một trong những phương pháp hay sử dụng là dùng bộ đệm trung gian để lưu giữ số liệu nhận được. Độ lớn của bộ đệm này phụ thuộc vào tương quan xử lý của các hệ thu và phát. Trong trường hợp đường truyền song công toàn phần, lớp datalink phải đảm bảo việc quản lý các thông tin số liệu và các thông tin trạng thái.

**c) Lớp mạng**

Nhiệm vụ của lớp mạng là đảm bảo chuyển chính xác số liệu giữa các thiết bị cuối trong mạng. Để làm được việc đó, phải có chiến lược đánh địa chỉ thống nhất trong toàn mạng. Mỗi thiết bị cuối và thiết bị mạng có một địa chỉ mạng xác định. Số liệu cần trao đổi giữa các thiết bị cuối được tổ chức thành các gói (packet) có độ dài thay đổi và được gán đầy đủ địa chỉ nguồn (source address) và địa chỉ đích (destination address).

Lớp mạng đảm bảo việc tìm đường tối ưu cho các gói dữ liệu bằng các giao thức chọn đường dựa trên các thiết bị chọn đường (router). Ngoài ra, lớp mạng có chức năng điều khiển lưu lượng số liệu trong mạng để tránh xảy ra tắc ngẽn bằng cách chọn các chiến lược tìm đường khác nhau để quyết định việc chuyển tiếp các gói số liệu.

**d) Lớp chuyển vận**

Lớp này thực hiện các chức năng nhận thông tin từ lớp phiên (**session**) chia thành các gói nhỏ hơn và truyền xuống lớp dưới, hoặc nhận thông tin từ lớp dưới chuyển lên phục hồi theo cách chia của hệ phát (Fragmentation and Reassembly). Nhiệm vụ quan trọng nhất của lớp vận chuyển là đảm bảo chuyển số liệu chính xác giữa hai thực thể thuộc lớp phiên (end-to-end control). Để làm được việc đó, ngoài chức năng kiểm tra số tuần tự phát, thu, kiểm tra và phát hiện, xử lý lỗi.Lớp vận chuyển còn có chức năng điều khiển lưu lượng số liệu để đồng bộ giữa thể thu và phát, tránh tắc nghẽn số liệu khi chuyển qua lớp mạng. Ngoài ra, nhiều thực thể lớp phiên có thể trao đổi số liệu trên cùng một kết nối lớp mạng (multiplexing).

**e) Lớp phiên**

Liên kết giữa hai thực thể có nhu cầu trao đổi số liệu, ví dụ người dùng và một máy tính ở xa, được gọi là một phiên làm việc. Nhiệm vụ của lớp phiên là quản lý việc trao đổi số liệu, ví dụ: thiết lập giao diện giữa người dùng và máy, xác định thông số điều khiển trao đổi số liệu (tốc độ truyền, số bit trong một byte, có kiểm tra lỗi parity hay không, v.v.), xác định loại giao thức mô phỏng thiết bị cuối (terminal emulation), v.v. Chức năng quan trọng nhất của lớp phiên là đảm bảo đồng bộ số liệu bằng cách thực hiện các điểm kiểm tra. Tại các điểm kiểm tra này, toàn bộ trạng thái và số liệu của phiên làm việc được lưu trữ trong bộ nhớ đệm. Khi có sự cố, có thể khởi tạo lại phiên làm việc từ điểm kiểm tra cuối cùng (không phải khởi tạo lại từ đầu).

### f) Lớp thể hiện

Nhiệm vụ của lớp thể hiện là thích ứng các cấu trúc dữ liệu khác nhau của người dùng với cấu trúc dữ liệu thống nhất sử dụng trong mạng. Số liệu của người dùng có thể được nén và mã hoá ở lớp thể hiện, trước khi chuyển xuống lớp phiên. Ngoài ra, lớp thể hiện còn chứa các thư viện các yêu cầu của người dùng, thư viện tiện ích, ví dụ thay đổi dạng thể hiện của các tệp, nén tệp...

### g) Lớp ứng dụng

Lớp ứng dụng cung cấp các phương tiện để người sử dụng có thể truy nhập được vào môi trường OSI, đồng thời cung cấp các dịch vụ thông tin phân tán. Lớp mạng cho phép người dùng khai thác các tài nguyên trong mạng tương tự như tài nguyên tại chỗ.

## III.3. Các chuẩn kết nối thông dụng nhất IEEE 802.X và ISO 8802.X

Bên cạnh việc chuẩn hoá cho mạng nối chung dẫn đến kết quả cơ bản nhất là mô hình tham chiếu OSI như đã giới thiệu. Việc chuẩn hoá mạng cục bộ nói riêng đã được thực hiện từ nhiều năm nay để đáp ứng sự phát triển của mạng cục bộ.

Cũng như đối với mạng nói chung, có hai loại chuẩn cho mạng cục bộ, đó là :

- Các chuẩn chính thức ( de jure ) do các tổ chức chuẩn quốc gia và quốc tế ban hành.

- Các chuẩn tực tiễn ( de facto ) do các hãng soản xuất, các tổ chức người sử dụng xây dựng và được dùng rộng rãi trong thực tế

- Các chuẩn IEEE 802.x và ISO 8802.x

IEEE là tổ chức đi tiên phong trong lĩnh vực chuẩn hoá mạng cục bộ với đề án IEEE 802 với kết quả là một loạt các chuẩn thuộc họ IEEE 802.x ra đời. Cuối những năm 80, tổ chức ISO đã tiếp nhận họ chuẩn này và ban hành thành chuẩn quốc tế dưới mã hiệu tương ứng là ISO 8802.x.

**IEEE 802.**: là chuẩn đặc tả kiến trúc mạng, kết nối giữa các mạng và việc quản trị mạng đối với mạng cục bộ.

**IEEE 802.2**: là chuẩn đặc tả tầng dịch vụ giao thức của mạng cục bộ.

**IEEE 802.3**: là chuẩn đặc tả một mạng cục bộ dựa trên mạng Ethernet nổi tiếng của Digital, Intel và Xerox hợp tác xây dựng từ năm 1980.

Tầng vật lý của IEEE 802.3 có thể dùng các phương án sau để xây dựng:

- 10BASE5 : tốc độ 10Mb/s, dùng cáp xoắn đôi không bọc kim UTP (Unshield Twisted Pair), với phạm vi tín hiệu lên tới 500m, topo mạng hình sao.

- 10BASE2 : tốc độ 10Mb/s, dùng cáp đồng trục thin-cable với trở kháng 50 Ohm, phạm vi tín hiệu 200m,topo mạng dạng bus.

- 10BASE5 : tốc độ 10Mb/s, dùng cáp đồng trục thick-cable (đường kính 10mm) với trở kháng 50 Ohm, phạm vi tín hiệu 500m, topo mạng dạng bus.

- 10BASE-F: dùng cáp quang, tốc độ 10Mb/s phạm vi cáp 2000m.

**IEEE 802.4**: là chuẩn đặc tả mạng cục bộ với topo mạng dạng bus dùng thẻ bài để điều việc truy nhập đường truyền.

**IEEE 802.5**: là chuẩn đặc tả mạng cục bộ với topo mạng dạng vòng (ring) dùng thẻ bài để điều việc truy nhập đường truyền.

**IEEE 802.6**: là chuẩn đặc tả mạng tốc độ cao kết nối với nhiều mạng cục bộ thuộc các khu vực khác nhau của một đô thị (còn được gọi là mạng MAN - Metropolitan Area Network)

**IEEE 802.9**: là chuẩn đặc tả mạng tích hợp dữ liệu và tiếng nói bao gồm 1 kênh dị bộ 10 Mb/s cùng với 96 kênh 64Kb/s. Chuẩn này được thiết kế cho môi trường có lượng lưu thông lớn và cấp bách.

**IEEE 802.10**: là chuẩn đặc tả về an toàn thông tin trong các mạng cục bộ có khả năng liên tác .

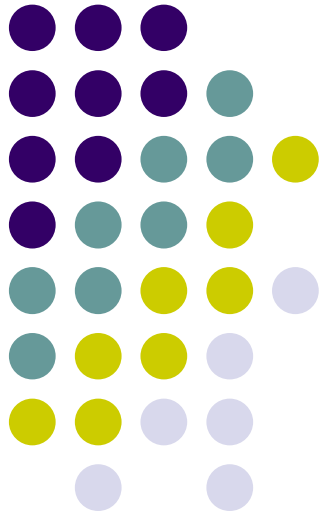
**IEEE 802.11**: là chuẩn đặc tả mạng cục bộ không dây (Wireless LAN) hiện đang được tiếp tục phát triển.

**IEEE 802.12**: là chuẩn đặc tả mạng cục bộ dựa trên công nghệ được đề xuất bởi AT&T, IBM và HP gọi là 100 VG - AnyLAN. Mạng này có topo mạng hình sao và một phương pháp truy nhập đường truyền có điều khiển tranh chấp. Khi có nhu cầu truyền dữ liệu, một trạm sẽ gửi yêu cầu đến hub và trạm chỉ có truyền dữ liệu khi hub cho phép.

# Mạng máy tính

Giảng viên: Ngô Hồng Sơn

Bộ môn Truyền thông và Mạng máy tính
Khoa CNTT- ĐHBK Hà Nội

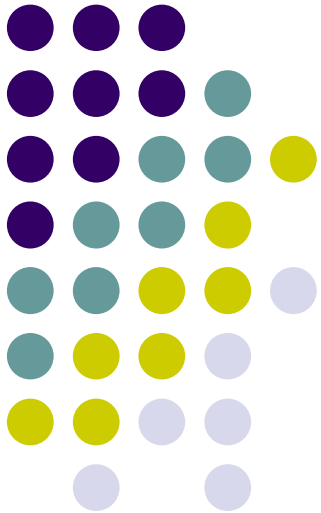


# Nội dung

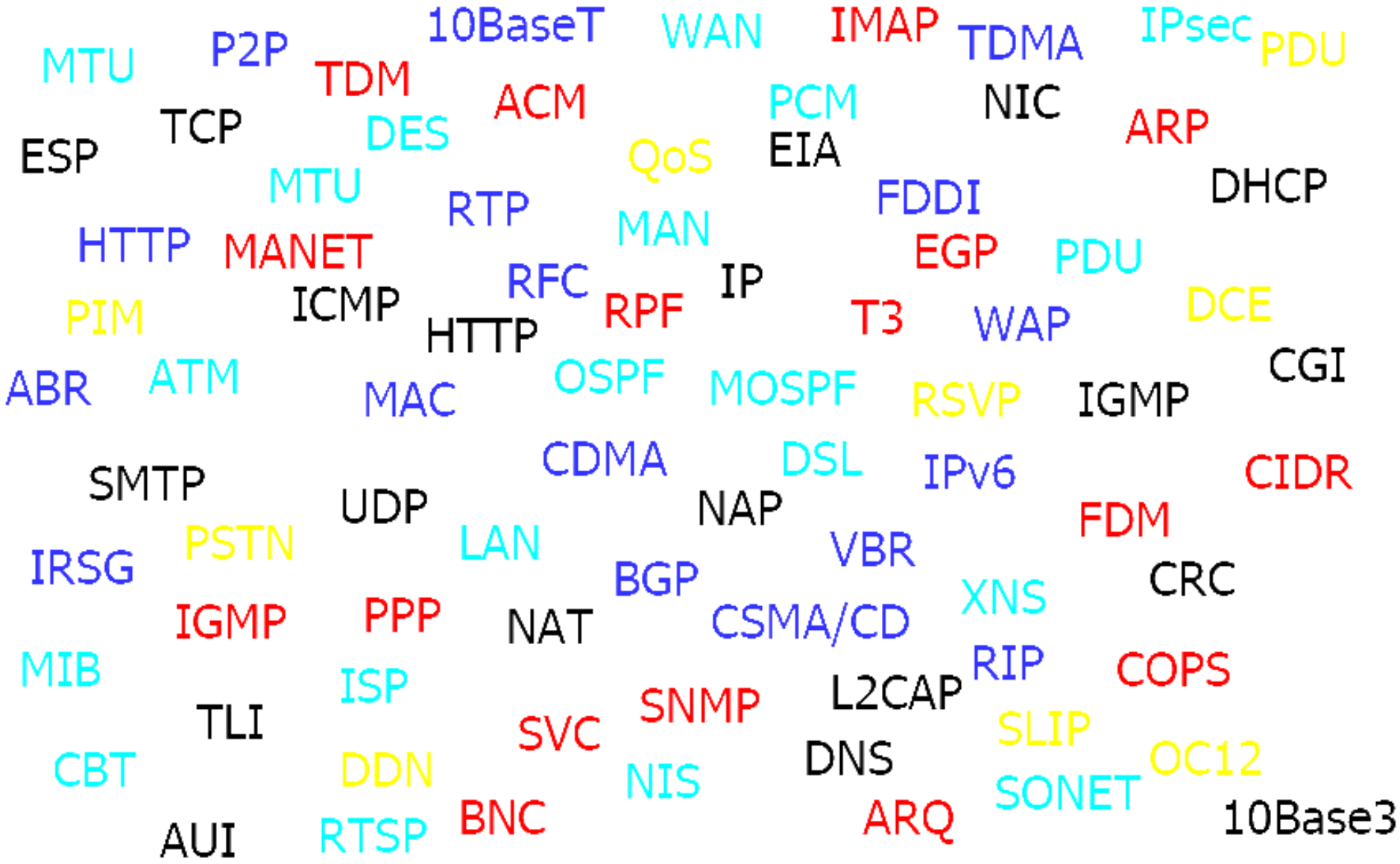
- Giới thiệu môn học
- Cơ bản về mạng máy tính
- Lược sử mạng máy tính và Internet
- Internet ở Việt Nam

# Giới thiệu môn học

Mục đích
Chủ đề và lịch học
Đánh giá
Liên hệ giáo viên



# Mục đích môn học





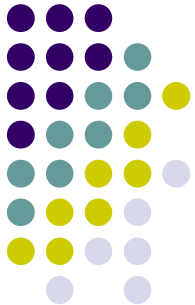

*Source: Hung Q Ngo' course*

# Mục đích môn học

*Kết thúc môn học này, các sinh viên ngành CNTT sẽ có khả năng:*

- Nêu và giải thích các công nghệ liên quan đến mạng máy tính và Internet
  - Nguyên lý cơ bản của mạng máy tính
  - Họ giao thức TCP/IP
- Giải thích được Internet hoạt động như thế nào
- Sử dụng hiệu quả Internet, vận dụng để có thể cài đặt các công nghệ và dịch vụ mới

# Lịch học dự kiến



| | | |
|---|---|---|
| 1 | 22-Aug-08 | Giới thiệu môn học, lịch sử mạng máy tính |
| 2 | 29-Aug-08 | Cơ bản về mạng máy tính |
| 3 | 5-Sep-08 | Tầng mạng, IP |
| 4 | 12-Sep-08 | Bài toán và các giao thức chọn đường đi |
| 5 | 19-Sep-08 | Tầng giao vận, TCP, UDP |
| 6 | 26-Sep-08 | Tầng ứng dụng, Web, Mail, FTP, DNS |
| 7 | 3-Oct-08 | Tầng liên kết dữ liệu |

# Lịch học dự kiến

| | | |
|---|---|---|
| 8 | 10-Oct-08 | LAN (VLAN, WLAN), WAN (...) |
| 9 | 17-Oct-08 | Tầng vật lí, các vấn đề về truyền số liệu |
| 10 | 24-Oct-08 | Advanced topic: Mạng thế hệ mới |
| 11 | 31-Oct-08 | Advanced topic: An toàn an ninh mạng |
| 12 | 7-Nov-08 | *Topic presentation* |
| 13 | 14-Nov-08 | *Topic presentation* |
| 14 | 21-Nov-08 | *Topic presentation* |
| 15 | 28-Nov-08 | Tổng kết và ôn tập |

# Đánh giá kết quả

- Bài tập lớn 40%
  - Hai bài
- Thi cuối kỳ 60%

# Cách làm việc

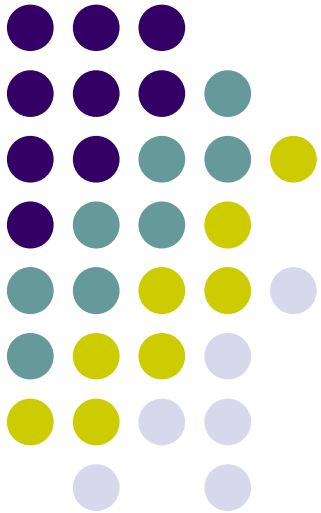
- Để học tốt
  - Đọc tài liệu trước khi đến lớp
  - Tham gia tích cực vào bài giảng
    - Thảo luận, trả lời và ĐẶT câu hỏi.
  - Tìm kiếm câu trả lời trên Web hoặc thảo luận với bạn bè
- Liên hệ với giáo viên
  - 8:30 – 10:00 sáng thứ 2 hàng tuần.
  - Bộ môn TTM – Khoa CNTT, 329 C1
  - ĐT: 8680896
  - Mail: sonnh@it-hut.edu.vn

# Tài liệu tham khảo

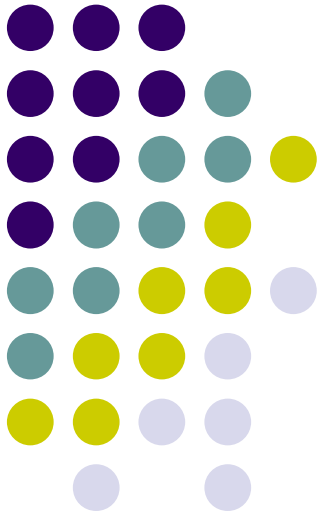

- [1] Nguyễn Thúc Hải, “Mạng máy tính và các hệ thống mở”
- [2] W. Stallings, “Data and Computer Communications”, Mac Millan,
- [3] James F. Kurose, Keith W. Ross, “Computer networks: a top-down approach featuring the Internet”, Addison Wesley.

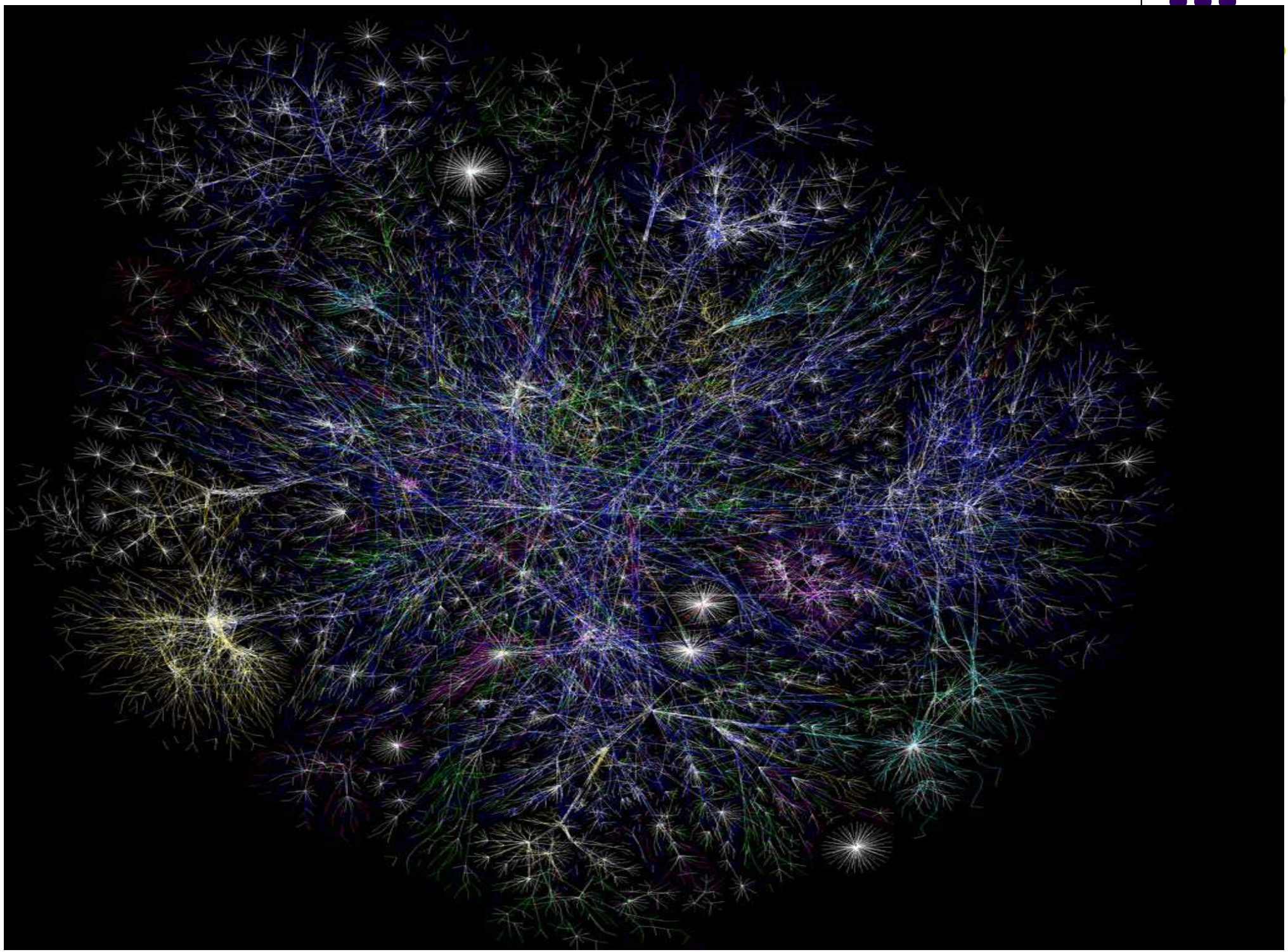
# Cơ bản về mạng máy tinh

Khái niệm mạng máy tính
Kiến trúc mạng
Chuyển mạch gói vs. chuyển mạch kênh



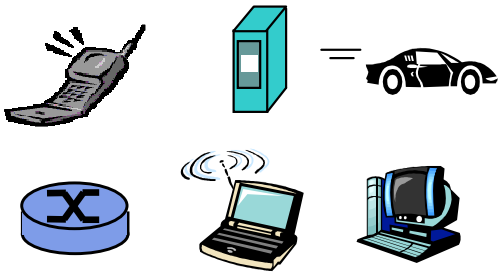
# Mạng máy tính là gì

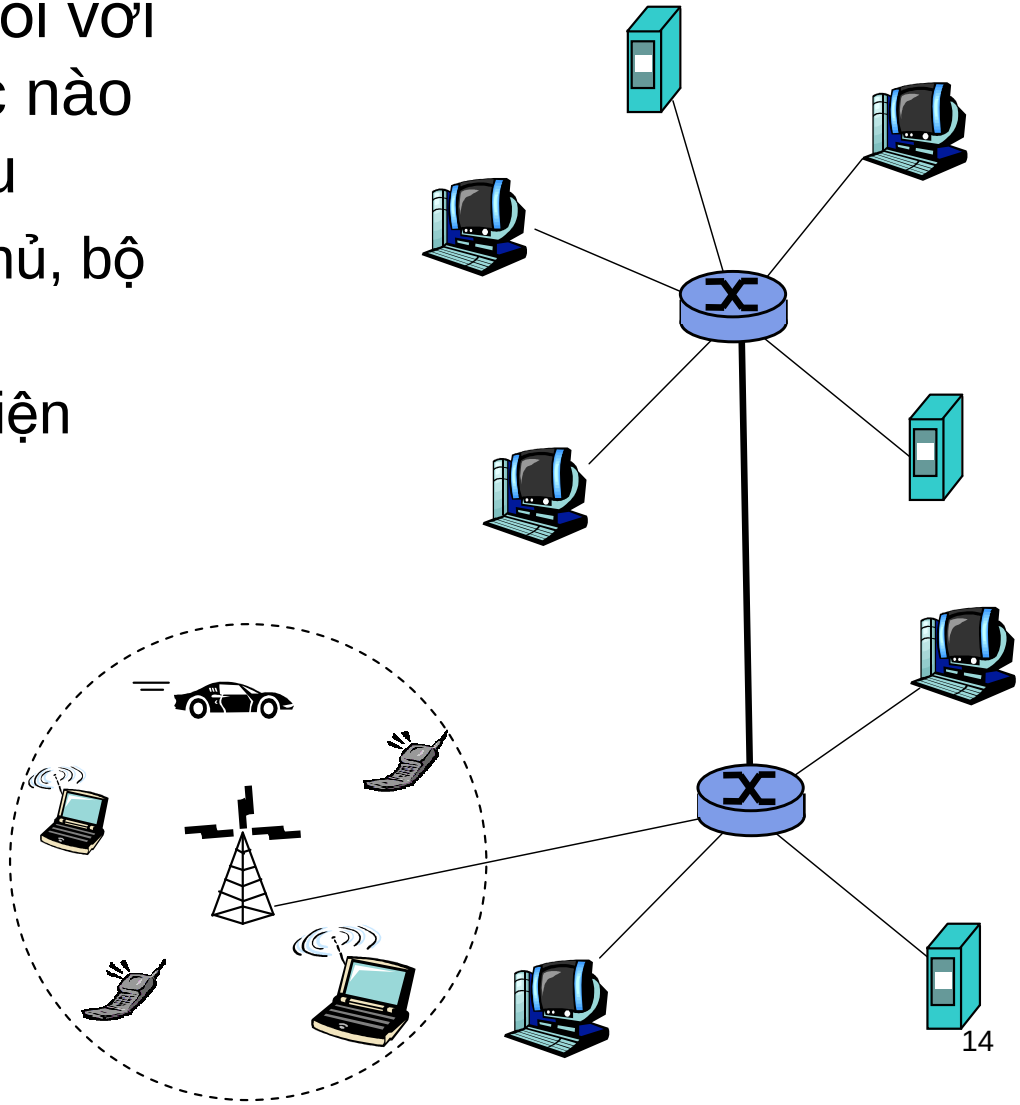




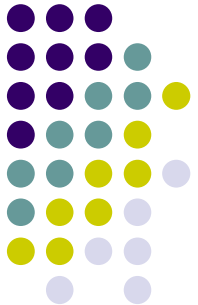
# Khái niệm

- Tập hợp các máy tính kết nối với nhau dựa trên một kiến trúc nào đó để có thể trao đổi dữ liệu
  - Máy tính: máy trạm, máy chủ, bộ định tuyến
  - Kết nối bằng một phương tiện truyền
  - Theo một kiến trúc mạng
- Các dạng máy tính?



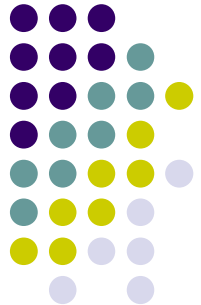


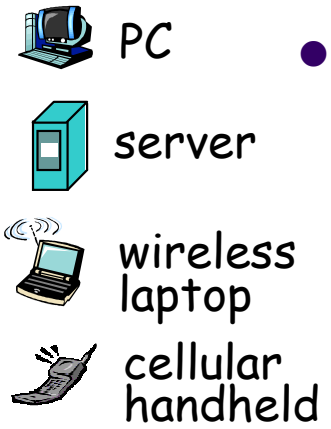
# Ví dụ về mạng máy tính



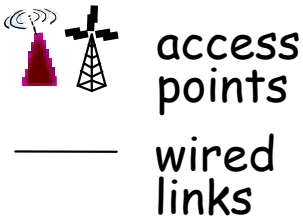
- Mạng Internet
- Mạng Ethernet
- Mạng LAN không dây: 802:11
- Hệ thống mạng ngân hàng: mạng lưới máy rút tiền
- Hệ thống bán vé tàu qua mạng
- …

# Internet ngày nay



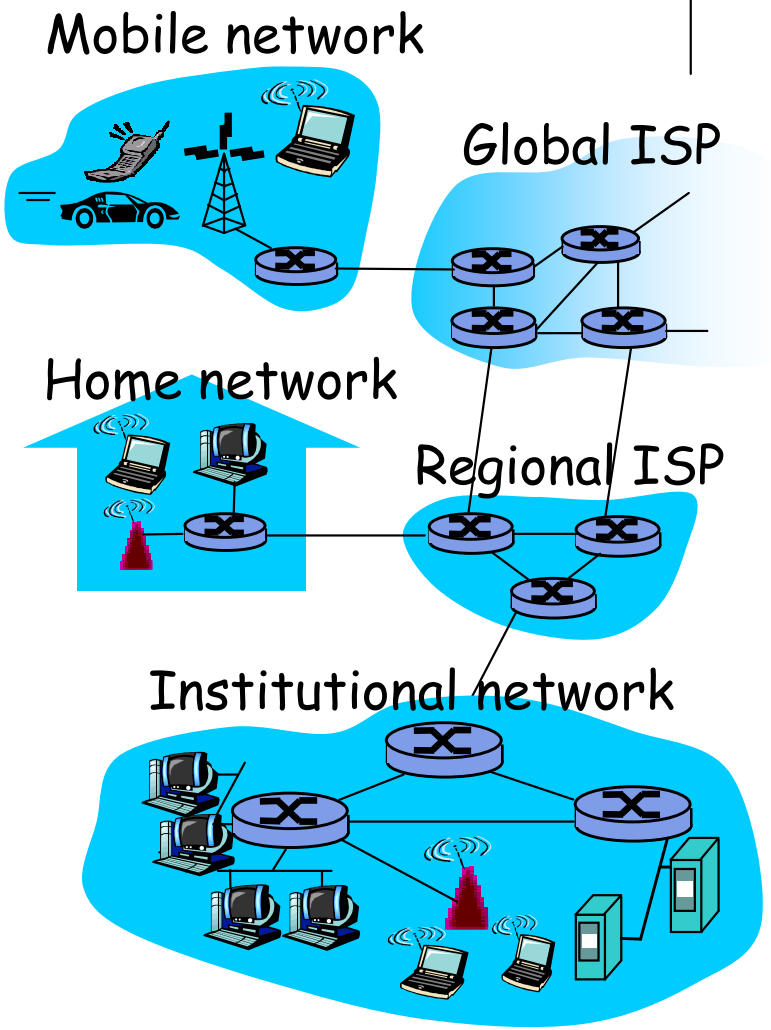



- Hàng triệu thiết bị kết nối: *hosts = end systems*
  - chạy *các ứng dụng mạng*

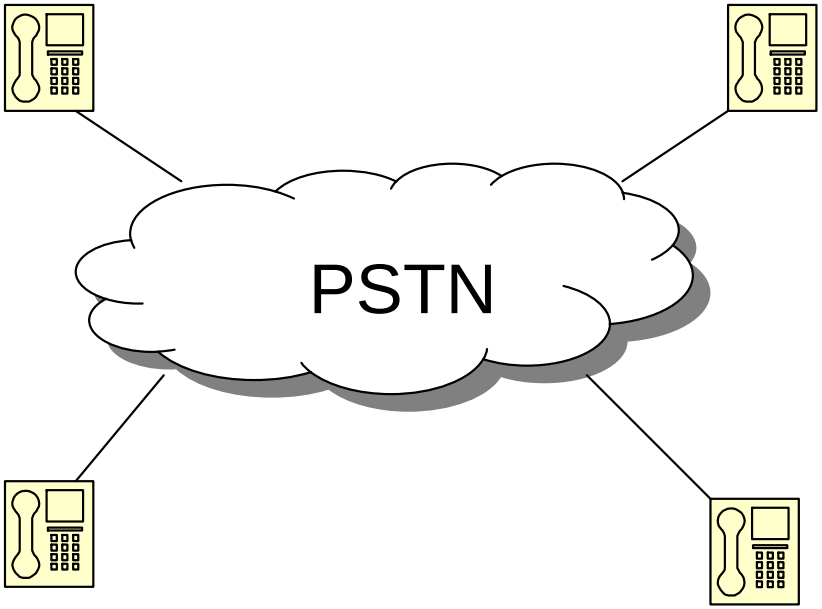



- *Đường truyền*
  - Cáp quang, đồng, vệ tinh, …
  - Tốc độ truyền = *băng thông*

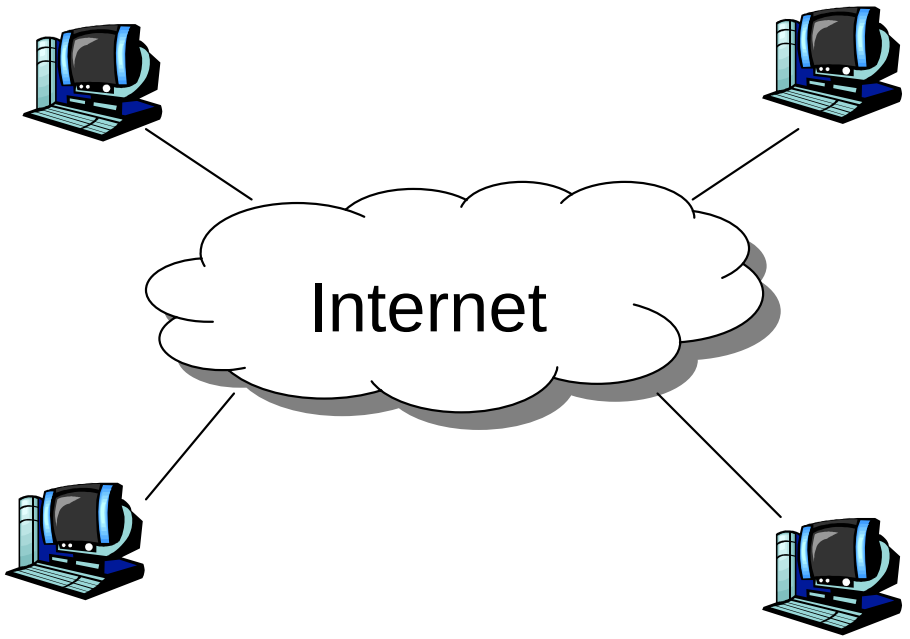
- *Bộ định tuyến:* chuyển tiếp các gói tin (dữ liệu)



# Xử lý tập trung hay phân tán




- Mạng điện thoại công cộng, tập trung: mạng xử lý mọi thứ



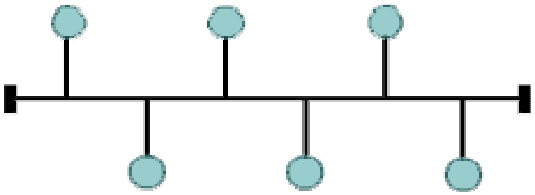

- Máy tính có khả năng lớn hơn
- Hầu hết các chức năng tập trung ở mạng máy tính
- Mạng: Truyền dữ liệu

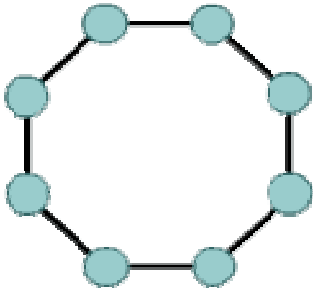


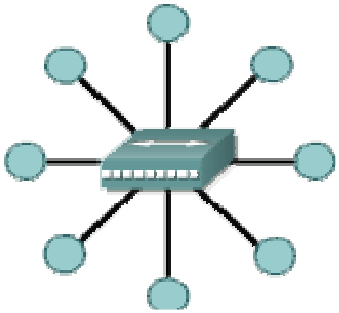
PSTN: Public Switch Telephone Network

# Kiến trúc mạng

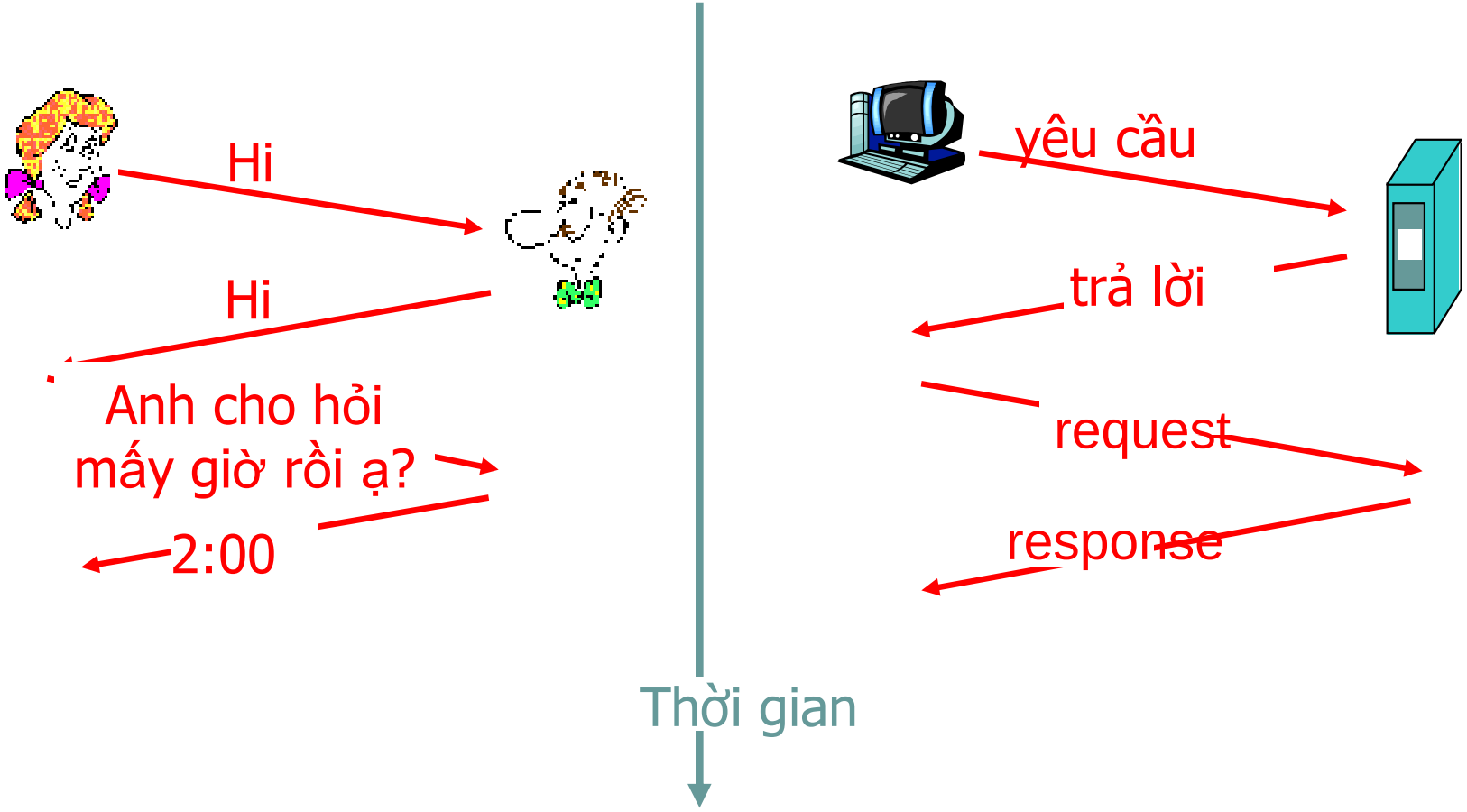
- Kiến trúc mạng: Hình trạng (topology) và giao thức (protocol)
- Hình trạng mạng
  - Trục (Bus), Vòng (Ring), Sao (Star)…
  - Thực tế là sự kết hợp của nhiều hình trạng khác nhau







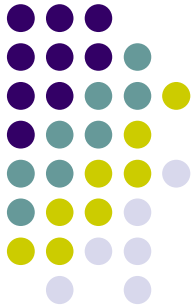
# Giao thức là gì?




Giao thức người-người

Giao thức máy-máy

# Giao thức mạng

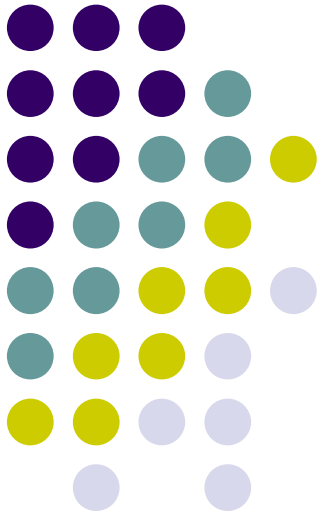


- Protocol: Quy tắc để truyền thông
  - Gửi một thông điệp với yêu cầu hoặc thông tin
  - Nhận một thông điệp với thông tin, sự kiện hoặc hành động
- Định nghĩa khuôn dạng và thứ tự truyền, nhận thông điệp giữa các thực thể trên mạng hoặc các hành động tương ứng khi nhận được thông điệp
- Ví dụ về giao thức mạng: TCP, UDP, IP, HTTP, Telnet, SSH, Ethernet, …

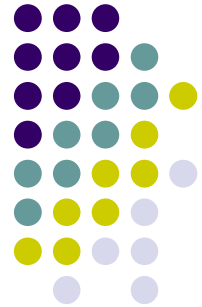
# Mô hình truyền thông

Chuyển mạch gói vs. Chuyển mạch kênh

Hướng liên kết vs. Không liên kết



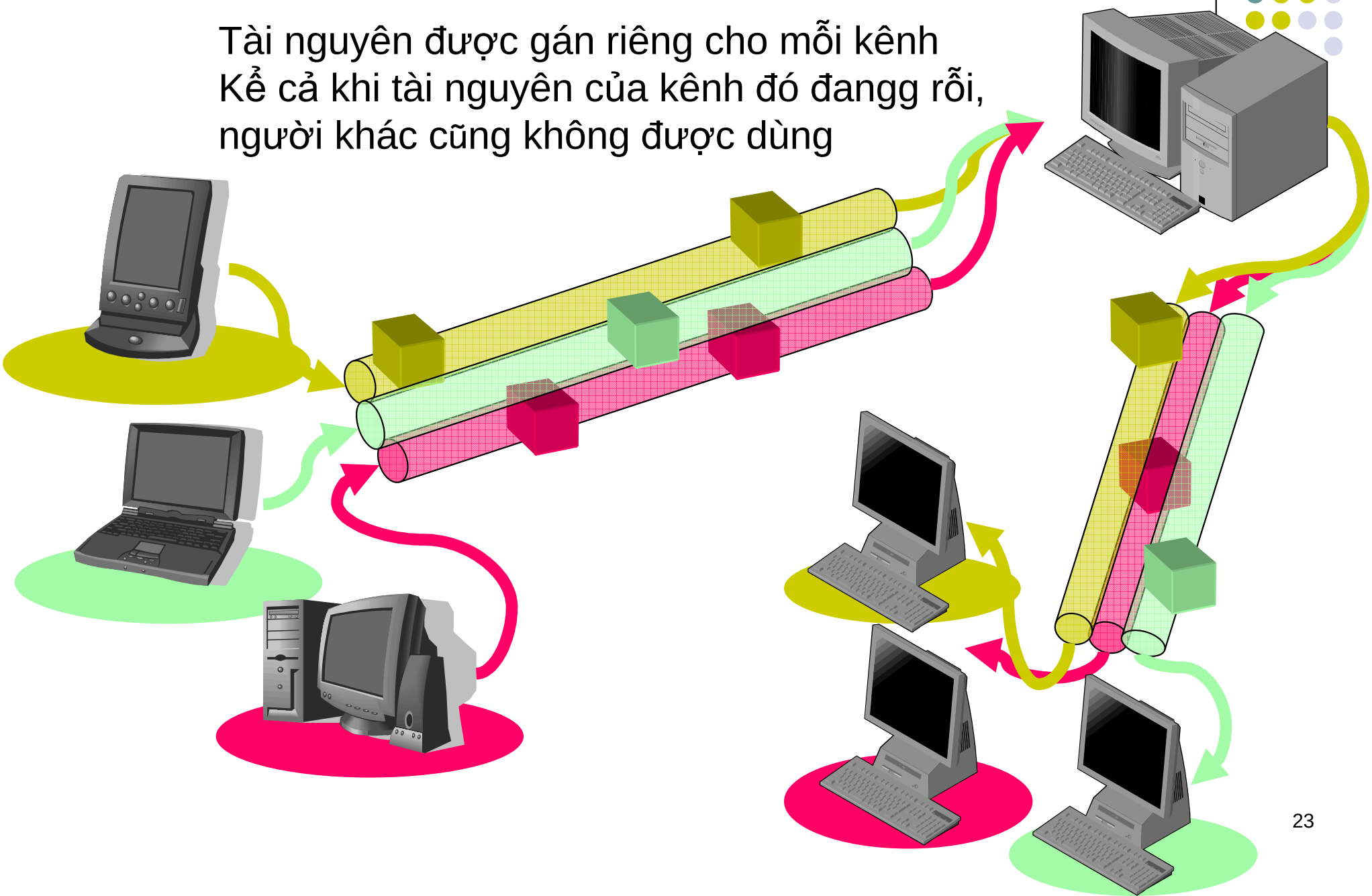
# Chuyển mạch gói vs. Chuyển mạch kênh



- Chuyển mạch kênh
  - Trao đổi dữ liệu sử dụng một kênh riêng .
  - Mỗi liên kết sử dụng một kênh. Tài nguyên cho kênh đó không được sử dụng bởi người khác trừ khi đóng liên kết
- Chuyển mạch gói
  - Dữ liệu được chia thành các gói nhỏ (packets), và được chuyển qua mạng
  - Nhiều liên kết có thể chia sẻ một kênh
  - Internet (với giao thức IP – Internet Protocol) sử dụng chuyển mạch gói

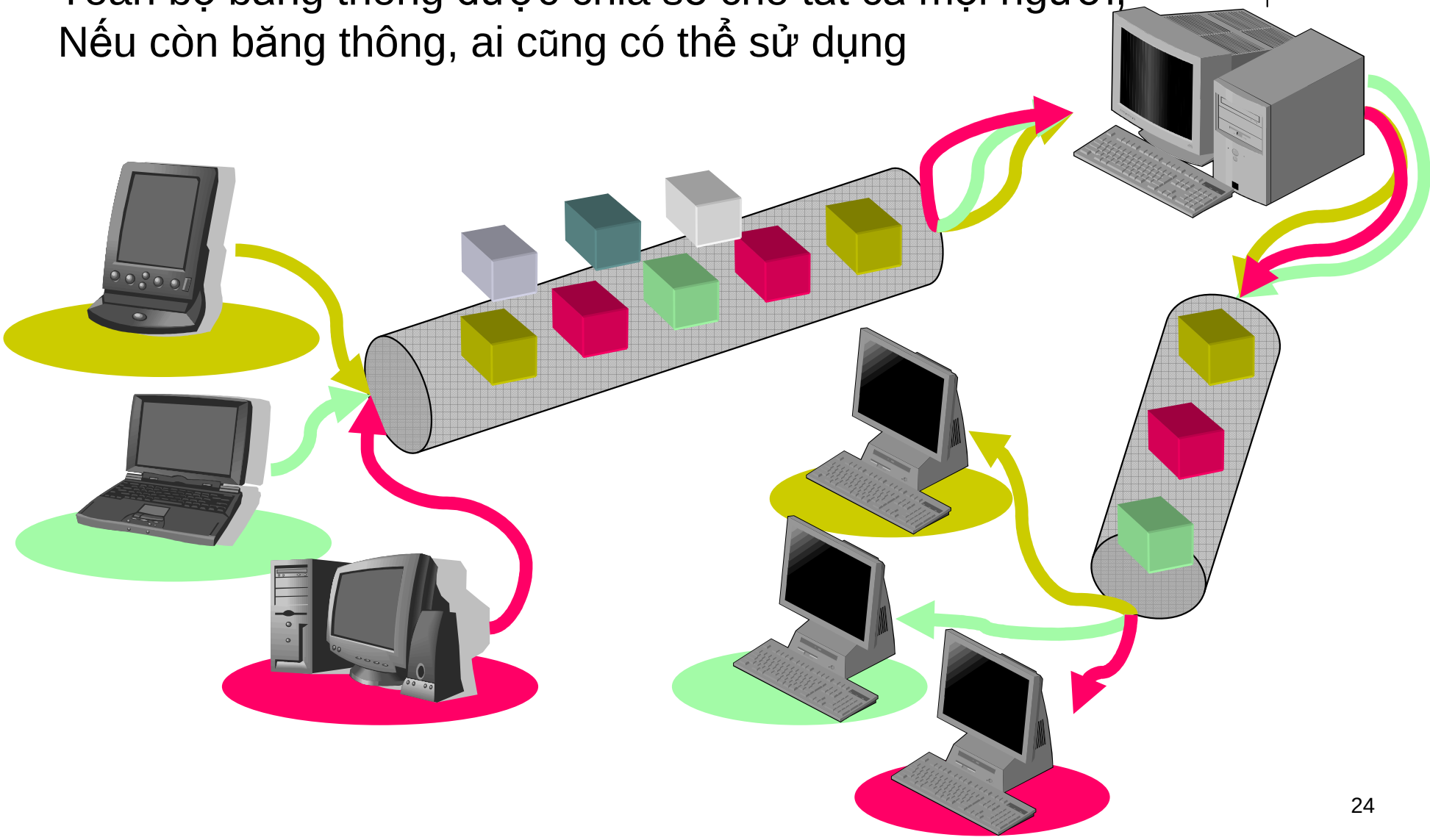
# Chuyển mạch kênh

Tài nguyên được gán riêng cho mỗi kênh
Kể cả khi tài nguyên của kênh đó đangg rỗi, người khác cũng không được dùng

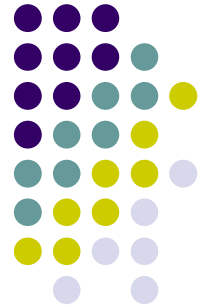


# Chuyển mạch gói

Toàn bộ băng thông được chia sẻ cho tất cả mọi người,
Nếu còn băng thông, ai cũng có thể sử dụng

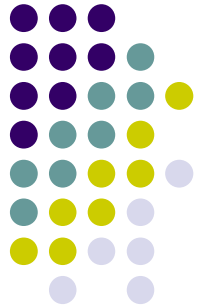


# Chuyển mạch gói vs. Chuyển mạch kênh



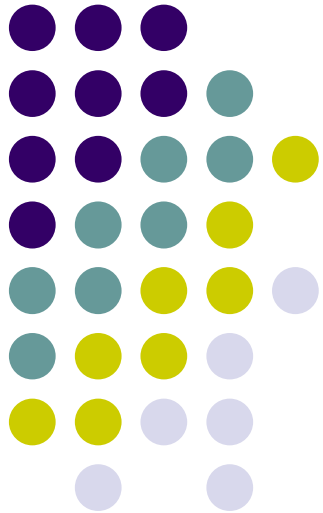
- Chuyển mạch kênh
  - Mỗi kênh chỉ dùng cho duy nhất 1 liên kết
  - Bảo đảm băng thông (cần cho các ứng dụng audio/video)
  - Lãng phí nếu liên kết đó không sử dụng hết khả năng của kênh
- Chuyển mạch gói
  - Tăng hiệu quả sử dụng băng thông
  - Tốt cho các dạng dữ liệu đến ngâu nhiên, không định trước
  - Hạn chế: Tắc nghẽn làm trễ và mất gói tin, không bảo đảm băng thông

# Truyền thông hướng liên kết vs. không liên kết



- Truyền thông hướng liên kết :
  - Dữ liệu được truyền qua một liên kết đã được thiết lập
  - Ba giai đoạn: Thiết lập liên kết, truyền dữ liệu, Hủy bỏ liên kết
  - Tin cậy
- Truyền thông không liên kết
  - Không thiết lập liên kết, chỉ có giai đoạn truyền dữ liệu
  - Không tin cậy - “Best effort”

# Một số tham số trong mạng



# Các tham số cơ bản

- Băng thông - Bandwidth
- Thông lượng - Throughput
- Độ trễ- Delay
- Độ mất gói tin - Loss

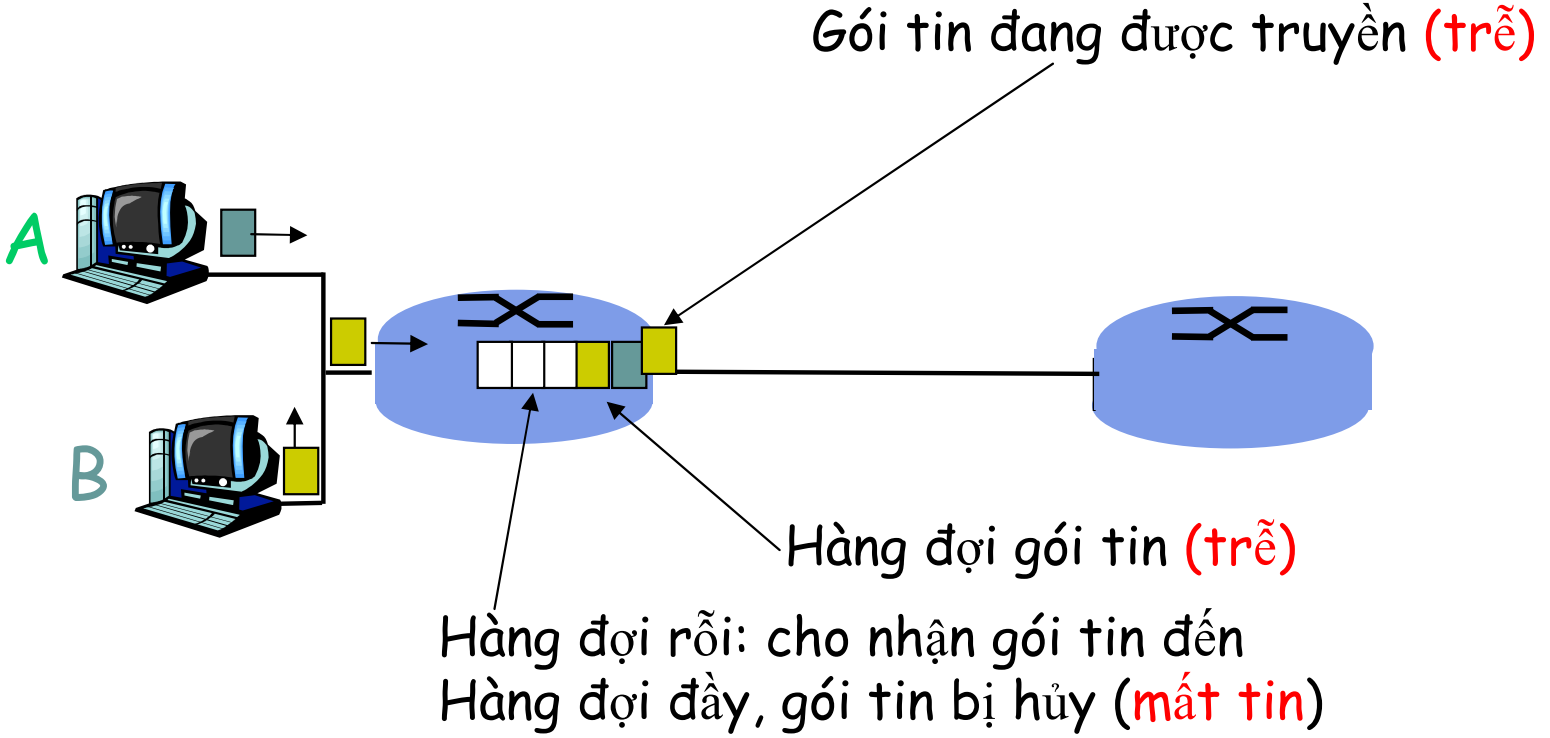
# Băng thông

- Khái niệm
- Đơn vị
  - bps, kbps, Mbps, Gbps, Tbps
- Uplink/downlink

# Vì sao có mất và trễ tin?

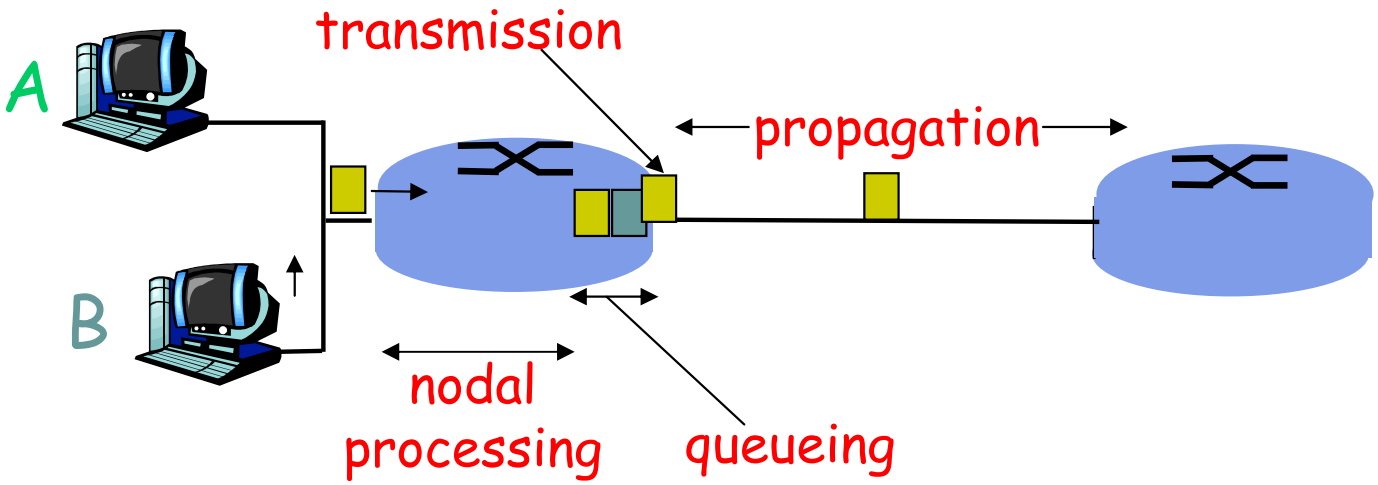
Các gói tin phải xếp hàng trong bộ định tuyến!

- Tốc độ đến của các gói tin vượt quá khả năng đường ra
- Các gói tin phải xếp hàng chờ đến lượt



# 4 nguyên nhân gây trễ tin

- 1. Xử lý tại nút mạng:
  - Kiểm soát lỗi
  - Tìm đường ra
- 2. Xếp hàng
  - Thời gian chờ đi ra
  - Phụ thuộc độ tắc nghẽn của router



# 4 nguyên nhân gây trễ tin

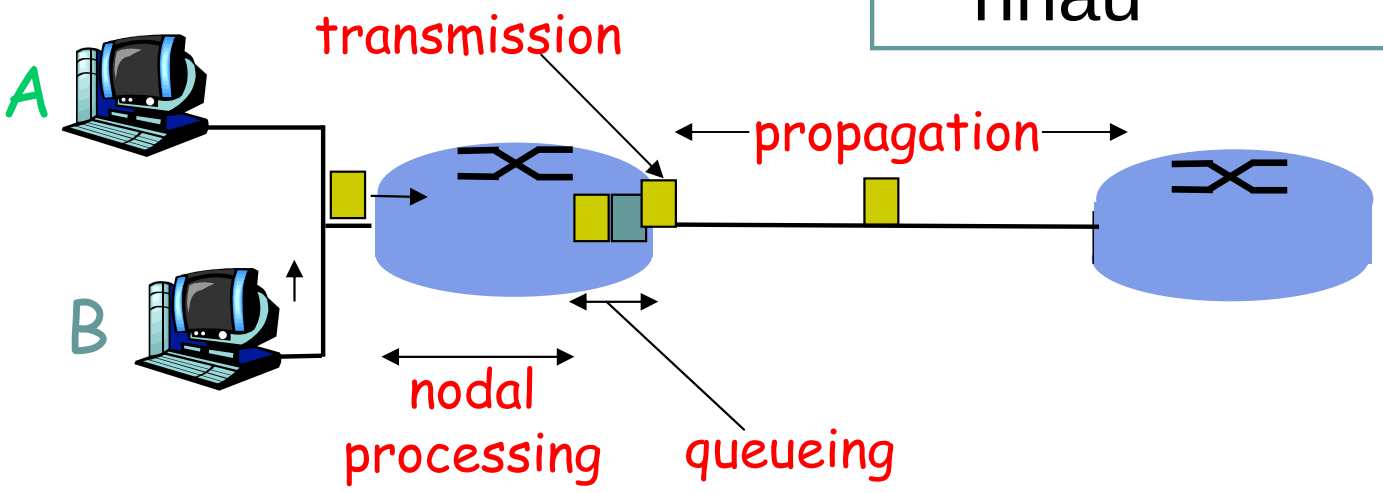
## 3. Trễ truyền tin:

- R= băng thông (bps)
- L= độ dài packet (bits)
- Trễ truyền tin = L/R

## 4. Trễ lan truyền:

- d = độ dài đường truyền
- s = tốc độ tín hiệu (~$2x10^8$ m/sec)
- Trễ lan truyền = d/s

Chú ý: s và R rất khác nhau



# Tổng thời gian trễ

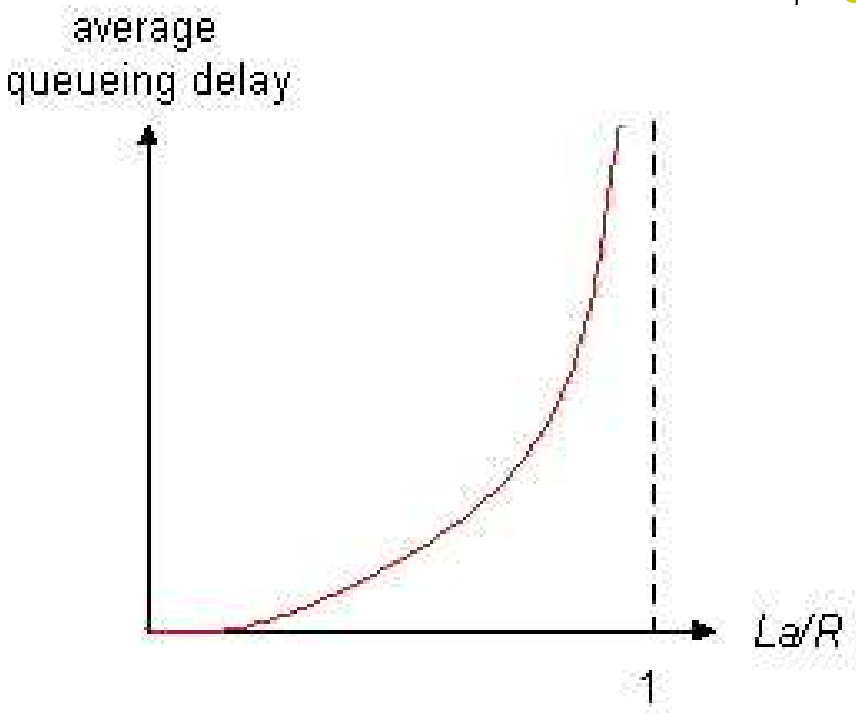
$$d_{\text{nodal}} = d_{\text{proc}} + d_{\text{queue}} + d_{\text{trans}} + d_{\text{prop}}$$

- $d_{proc}$ = processing delay
  - Vài microsecs hay ít hơn
- $d_{queue}$ = queuing delay
  - Phụ thuộc vào độ tắc nghẽn
- $d_{trans}$ = transmission delay
  - = L/R, lớn với những đường truyền tốc độ thấp
- $d_{prop}$ = propagation delay
  - vài microsecs tới hàng trăm msecs

# Trễ hàng đợi

- R= băng thông (bps)
- L= độ dài gói tin (bits)
- a= tốc độ đến của gói tin

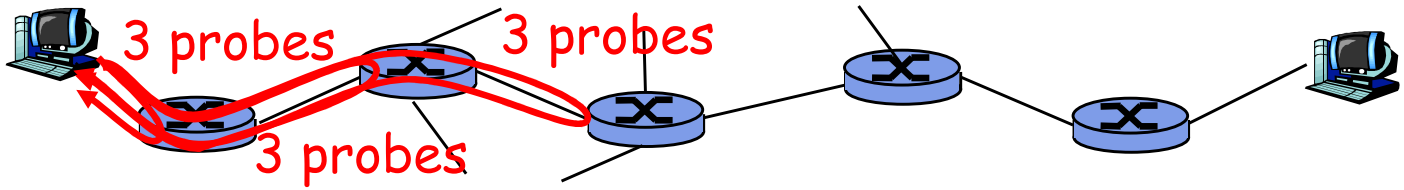
Lưu lượng đến = La/R




- La/R ~ 0: trễ hàng đợi nhỏ
- La/R -> 1: trễ lớn dần lên
- La/R > 1: quá khả năng, trễ vô cùng

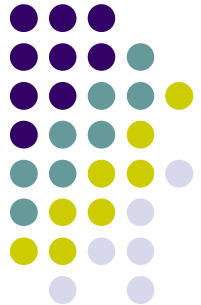
# Độ trễ và đường đi thực tế trên Internet

- Làm thế nào để biết đường đi và độ trễ?
- **`Traceroute` program:** cung cấp độ trễ và đường đi end-to-end.
- For all *i:*
  - Gửi 3 gói tin tới router *i* trên đường tới đích
  - router *i* trả lại một gói tin cho người gửi
  - Bên gửi đo khoảng thời gian giữa gửi và nhận



# Ví dụ

traceroute: gaia.cs.umass.edu to www.eurecom.fr



Three delay measurements from gaia.cs.umass.edu to cs-gw.cs.umass.edu

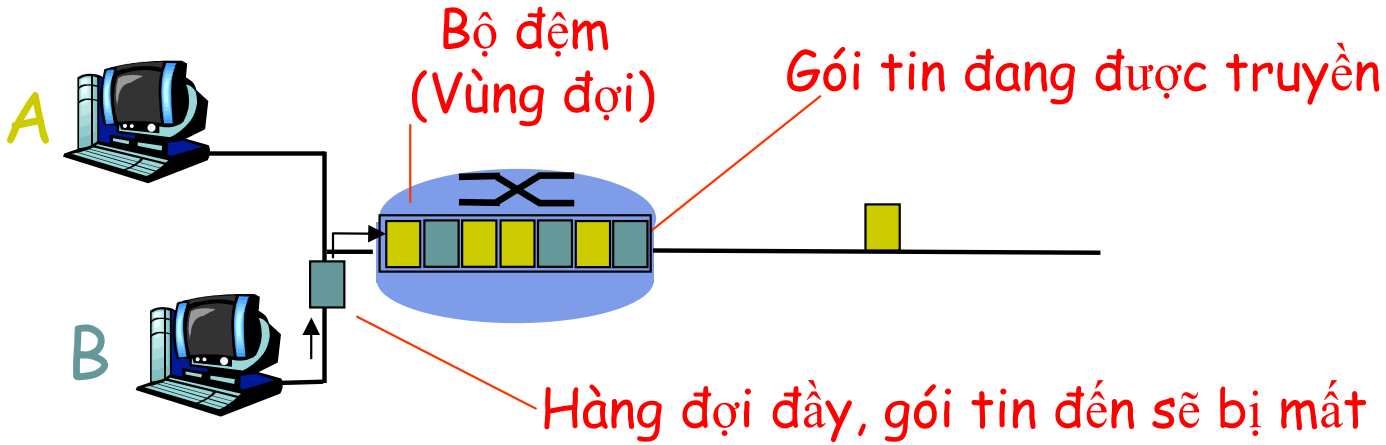
```
1  cs-gw (128.119.240.254)  1 ms  1 ms  2 ms
2  border1-rt-fa5-1-0.gw.umass.edu (128.119.3.145)  1 ms  1 ms  2 ms
3  cht-vbns.gw.umass.edu (128.119.3.130)  6 ms 5 ms 5 ms
4  jn1-at1-0-0-19.wor.vbns.net (204.147.132.129)  16 ms 11 ms 13 ms
5  jn1-so7-0-0-0.wae.vbns.net (204.147.136.136)  21 ms 18 ms 18 ms
6  abilene-vbns.abilene.ucaid.edu (198.32.11.9)  22 ms  18 ms  22 ms
7  nycm-wash.abilene.ucaid.edu (198.32.8.46)  22 ms  22 ms  22 ms
8  62.40.103.253 (62.40.103.253)  104 ms 109 ms 106 ms
9  de2-1.de1.de.geant.net (62.40.96.129)  109 ms 102 ms 104 ms
10  de.fr1.fr.geant.net (62.40.96.50)  113 ms 121 ms 114 ms
11  renater-gw.fr1.fr.geant.net (62.40.103.54)  112 ms  114 ms  112 ms
12  nio-n2.cssi.renater.fr (193.51.206.13)  111 ms  114 ms  116 ms
13  nice.cssi.renater.fr (195.220.98.102)  123 ms  125 ms  124 ms
14  r3t2-nice.cssi.renater.fr (195.220.98.110)  126 ms  126 ms  124 ms
15  eurecom-valbonne.r3t2.ft.net (193.48.50.54)  135 ms  128 ms  133 ms
16  194.214.211.25 (194.214.211.25)  126 ms  128 ms  126 ms
17  * * *
18  * * *
19  fantasia.eurecom.fr (193.55.113.142)  132 ms  128 ms  136 ms
```

trans-oceanic link

* means no response (probe lost, router not replying)

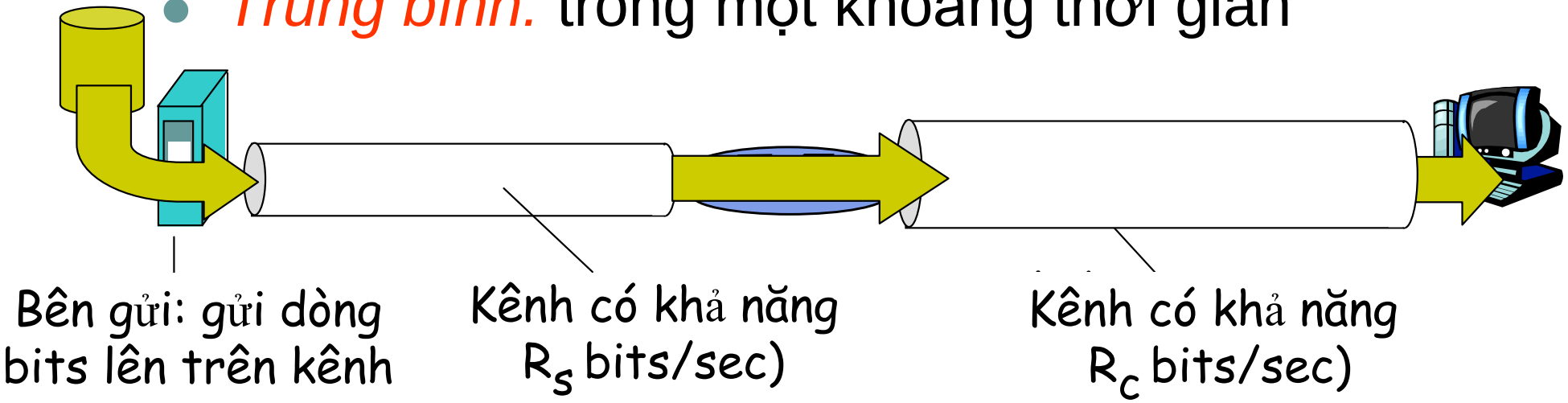
# Mất tin (loss)

- Hàng đợi (vùng đệm) của mỗi đường truyền có kích thước giới hạn
- Gói tin nào tới hàng đợi đầy sẽ bị mất
- Gói tin bị mất có thể được truyền lại hoặc không.



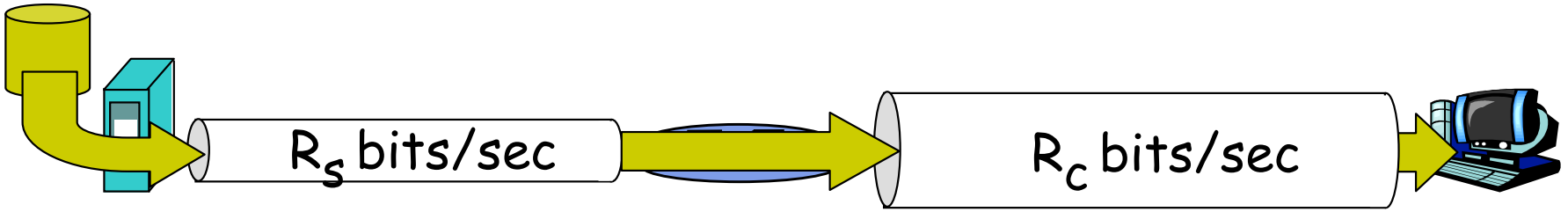
# Thông lượng

- *Thông lượng:* tốc độ (đơn vị bits/sec) mà tại đó các bits được truyền giữa bên gửi/bên nhận
  - *Tức thời:* tốc độ tại một thời điểm
  - *Trung bình:* trong một khoảng thời gian

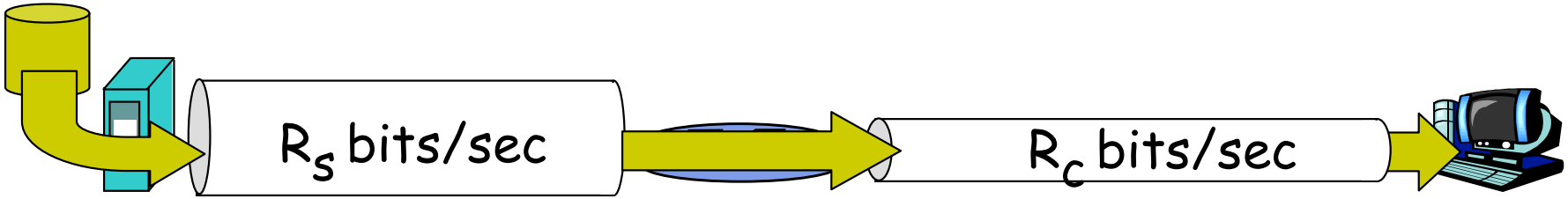


# Thông lượng

- $R_s < R_c$ Thông lượng trung bình?




- $R_s > R_c$ Thông lượng trung bình?

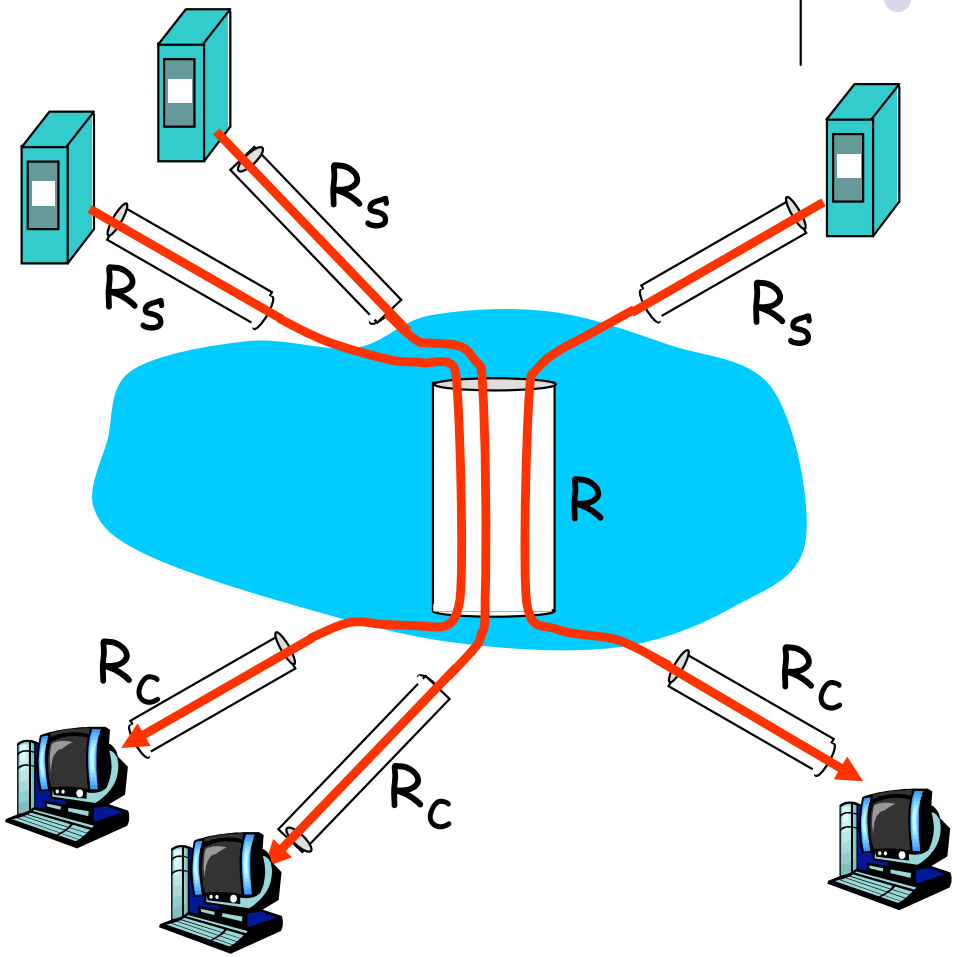



*Nút thắt cổ chai*

Đường truyền mà tại đó giới hạn toàn bộ băng thông của tuyến

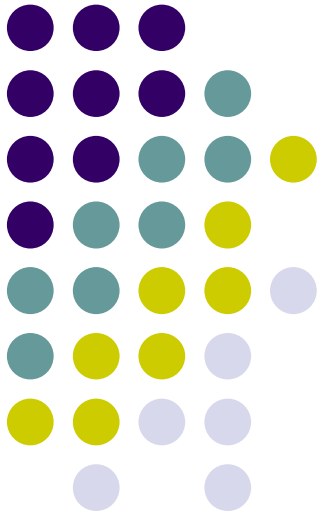
# Thông lượng: Ví dụ trên Internet

- Thông lượng của mỗi kết nối min($R_c$,$R_s$,R/10)
- Thực tế: $R_c$ hoặc $R_s$ thường xuyên bị thắt cổ "chai"




10 liên kết chia sẻ 1 đường R bits/sec

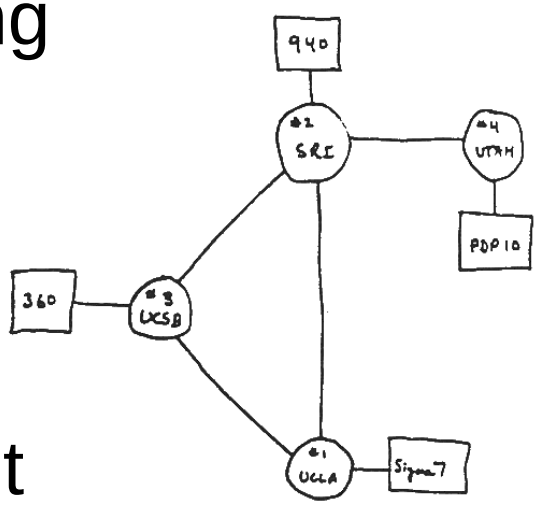
# Lược sử mạng & Internet



# Thời kỳ đầu

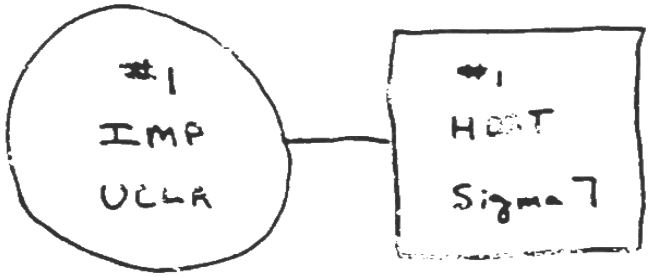
***1961-1972: Các nguyên lý mạng chuyển mạch gói***

- 1960s: Mạng điện thoại & sự phát triển của máy tính
- 1961: Kleinrock – Lý thuyết hàng đợi, hiệu quả của chuyển mạch gói
- 1964: Baran – mạng chuyển mạch gói
- 1967: ARPAnet được phê duyệt (Advanced Research Projects Agency)



THE ARPA NETWORK

# Nguồn gốc Internet




- Bắt đầu từ một thí nghiệm của dự án của ARPA
- Một liên kết giữa hai nút mạng (IMP tại UCLA và IMP tại SRI).

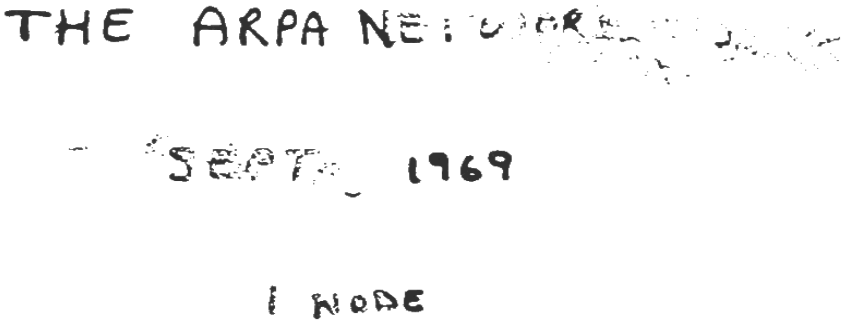


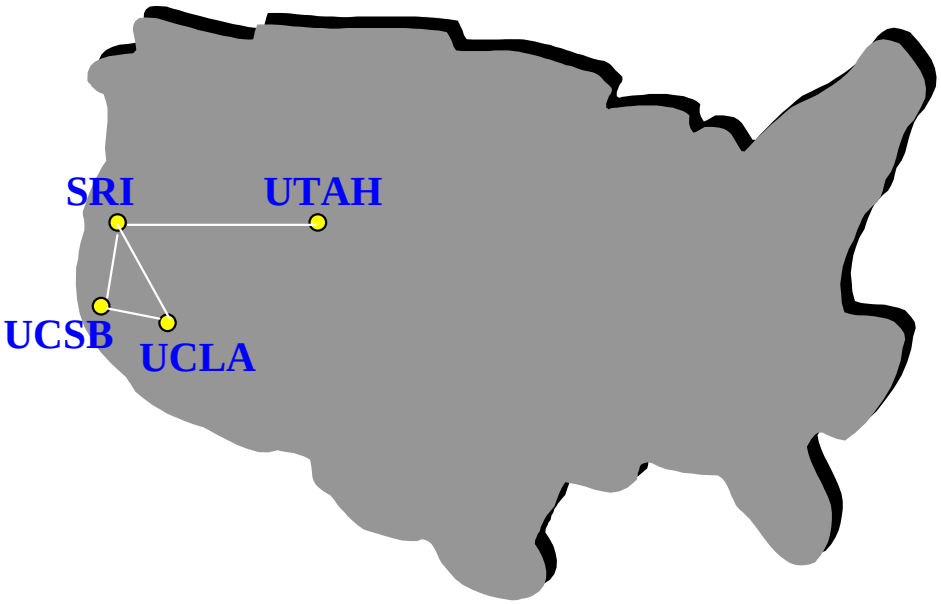

FIGURE 6.1 Drawing of September 1969 (Courtesy of Alex McKenzie)

ARPA: Advanced Research Project Agency
UCLA: University California Los Angeles
SRI: Stanford Research Institute
IMP: Interface Message Processor



Source: http://www.cybergeography.org/atlas/historical.html

# 3 tháng sau, 12/1969




Một mạng hoàn chỉnh với 4 nút, 56kbps

UCSB:University of California, Santa Barbara
UTAH:University of Utah

source: http://www.cybergeography.org/atlas/historical.html

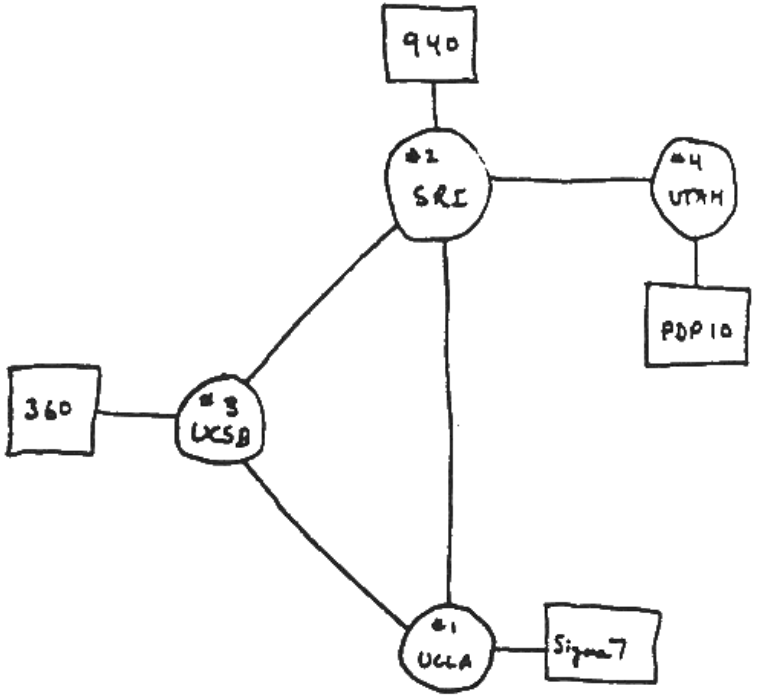
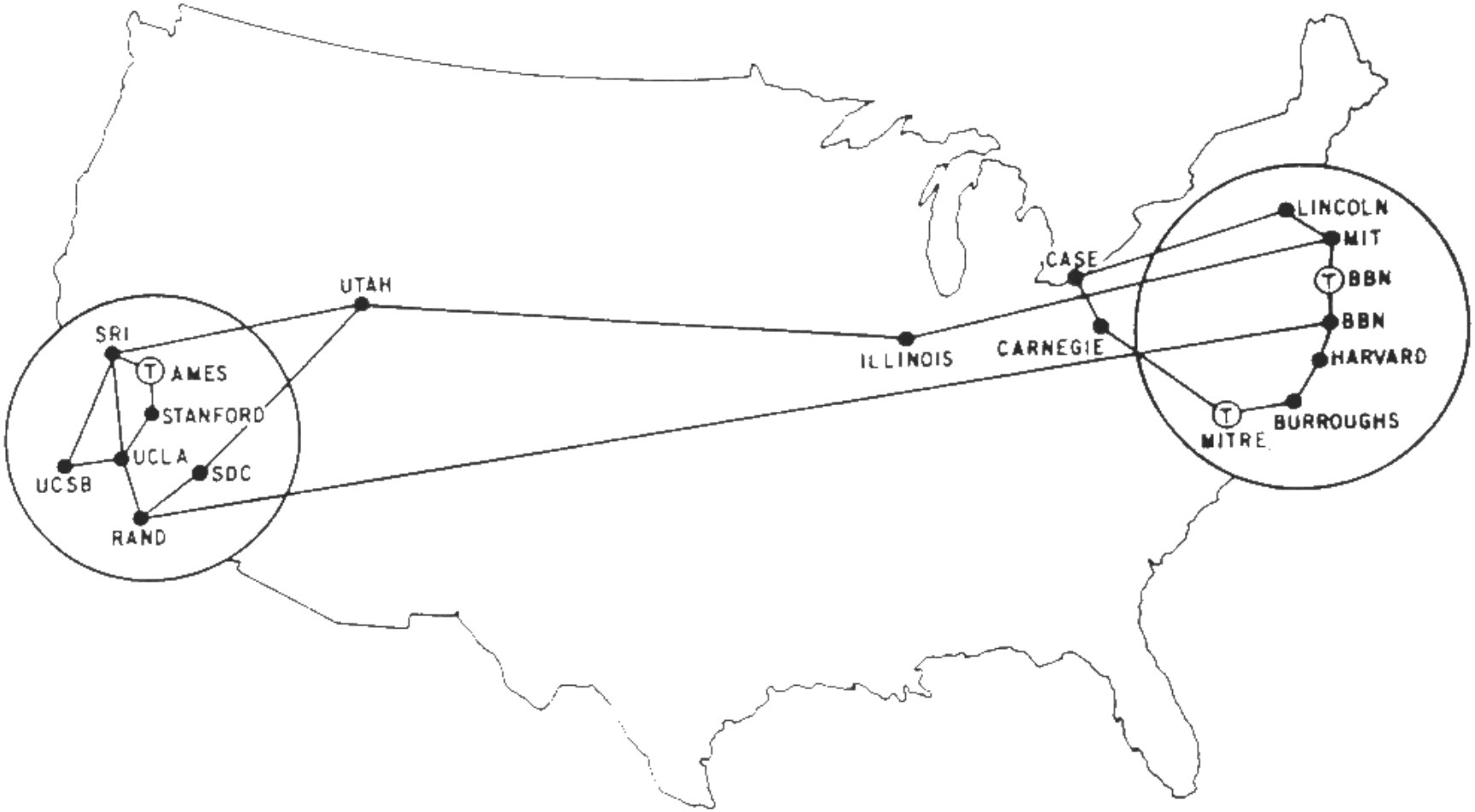



**FIGURE 6.2** Drawing of 4 Node Network (Courtesy of Alex McKenzie)

# ARPANET thời kỳ đầu, 1971

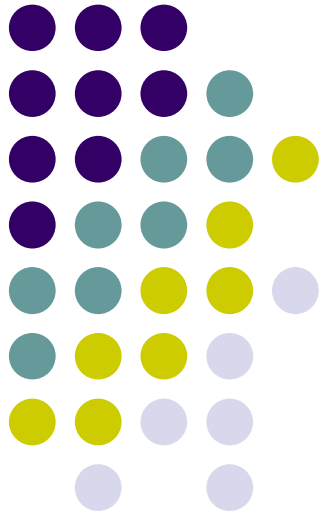



MAP 4 September 1971

Source: http://www.cybergeography.org/atlas/historical.html

Mạng phát triển với tốc độ thêm mỗi nút một tháng

# Thập niên 70: Kết nối liên mạng, kiến trúc mạng mới và các mạng riêng



# Sự mở rộng của ARPANET, 1974

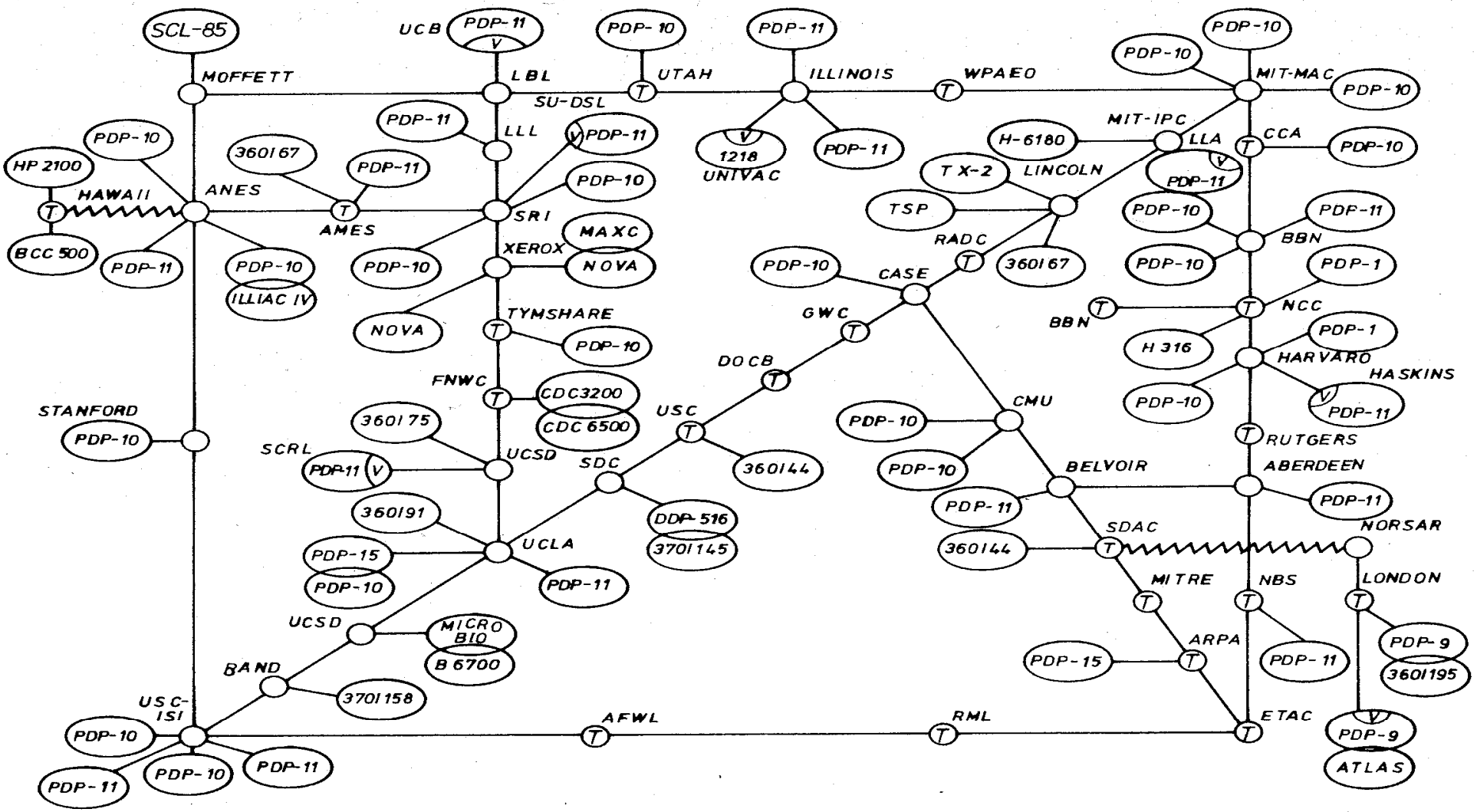
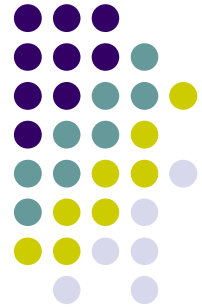



Abb. 4 ARPA NETwork, topologische Karte. Stand Juni 1974.

source:
http://www.cybergeography.org/atlas/historical.html

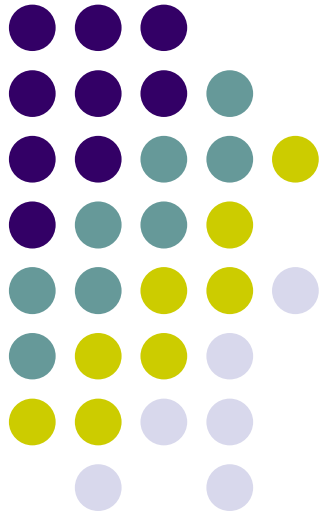
Lưu lượng mỗi ngày vượt quá 3.000.000 gói tin

# Thập niên 70



- Từ đầu 1970 xuất hiện các mạng riêng:
  - ALOHAnet tại Hawaii
  - DECnet, IBM SNA, XNA
- 1974: Cerf & Kahn – nguyên lý kết nối các hệ thống mở (Turing Awards)
- 1976: Ethernet, Xerox PARC
- Cuối 1970: ATM

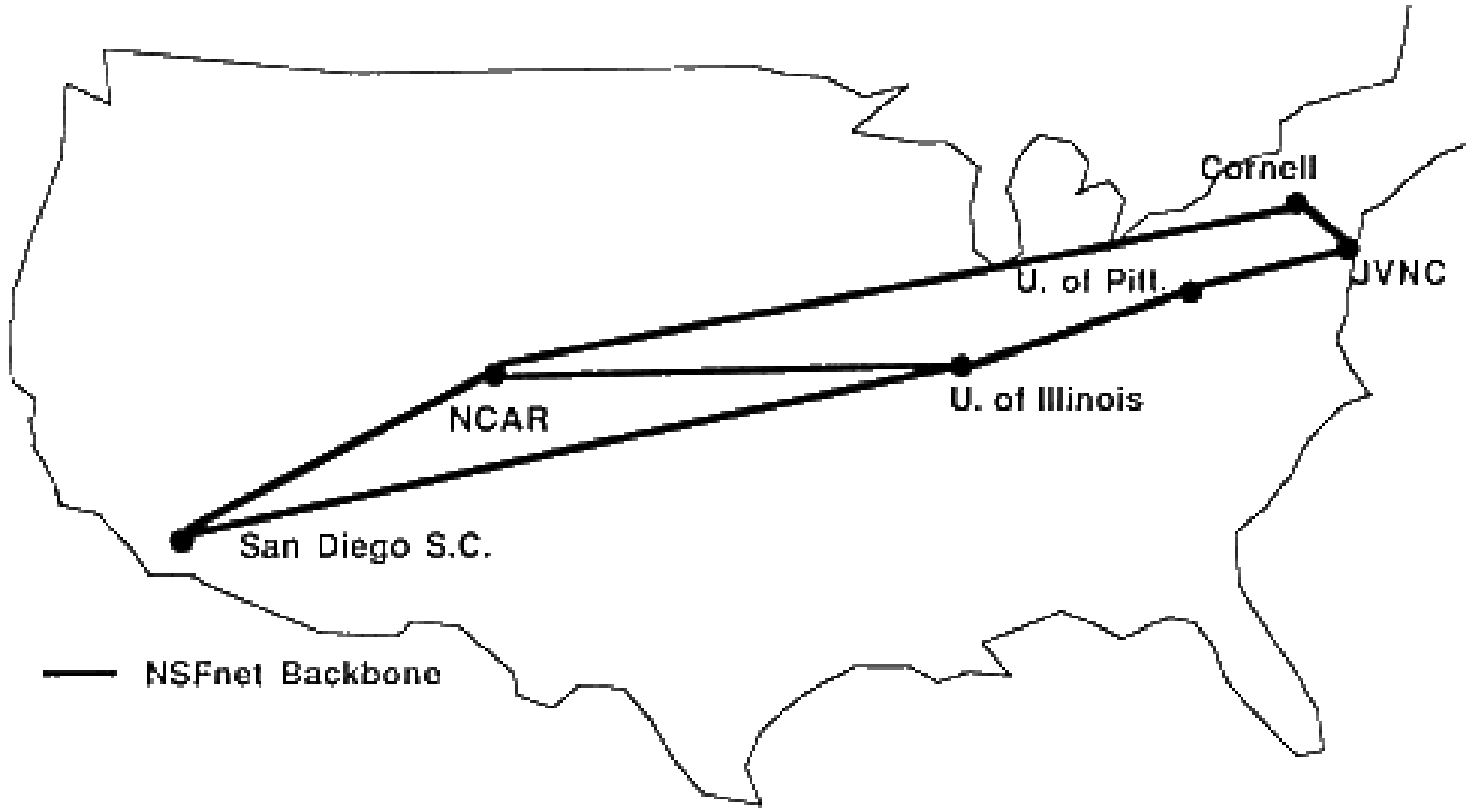
# Thập niên 80: Các giao thức mới, kết nối thêm mạng mới



# 1981: Xây dựng mạng NSFNET

NSF: National Science Foundation

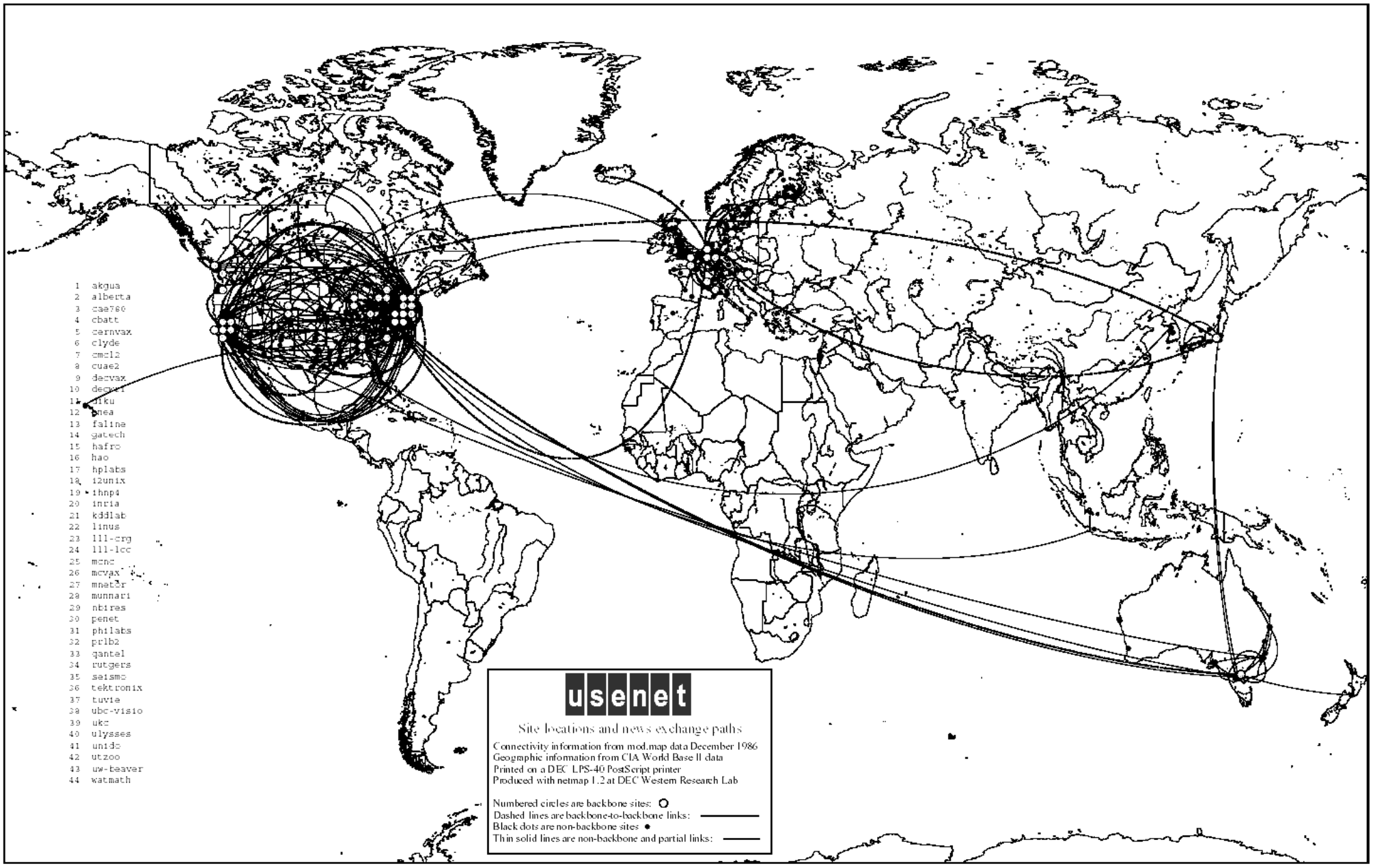
Phục vụ cho nghiên cứu khoa học, do sự quá tải của ARPANET




NSFnet Backbone Network

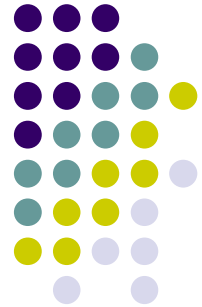
National Center for Atmospheric Research
March 19, 1994

# 1986: Nối kết USENET& NSFNET



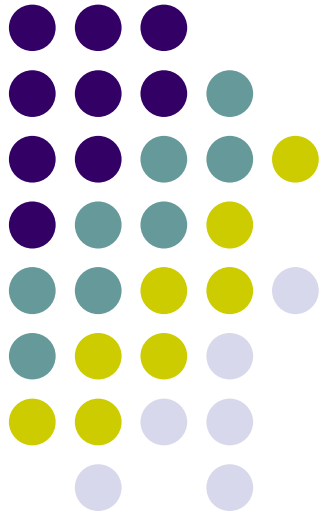

Source: http://www.cybergeography.org/atlas/historical.html

# Thêm nhiều mạng và giao thức mới

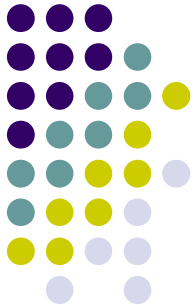


- Thêm nhiều mạng mới nối vào: MFENET, HEPNET (Dept. Energy), SPAN (NASA), BITnet, CSnet, NSFnet, Minitel …
- TCP/IP được chuẩn hóa và phổ biến vào 1980
- Berkeley tích hợp TCP/IP vào BSD Unix
- Dịch vụ: FTP, Mail, DNS …

# Thập niên 90: Web và thương mại hóa Internet



# Thập niên 90

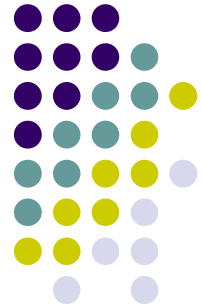


- Đầu 90: ARPAnet chỉ là một phần của Internet
- Đầu 90: Web
  - HTML, HTTP: Berners-Lee
  - 1994: Mosaic, Netscape
- Cuối 90: Thương mại hóa Internet

Cuối 1990's – 2000's:

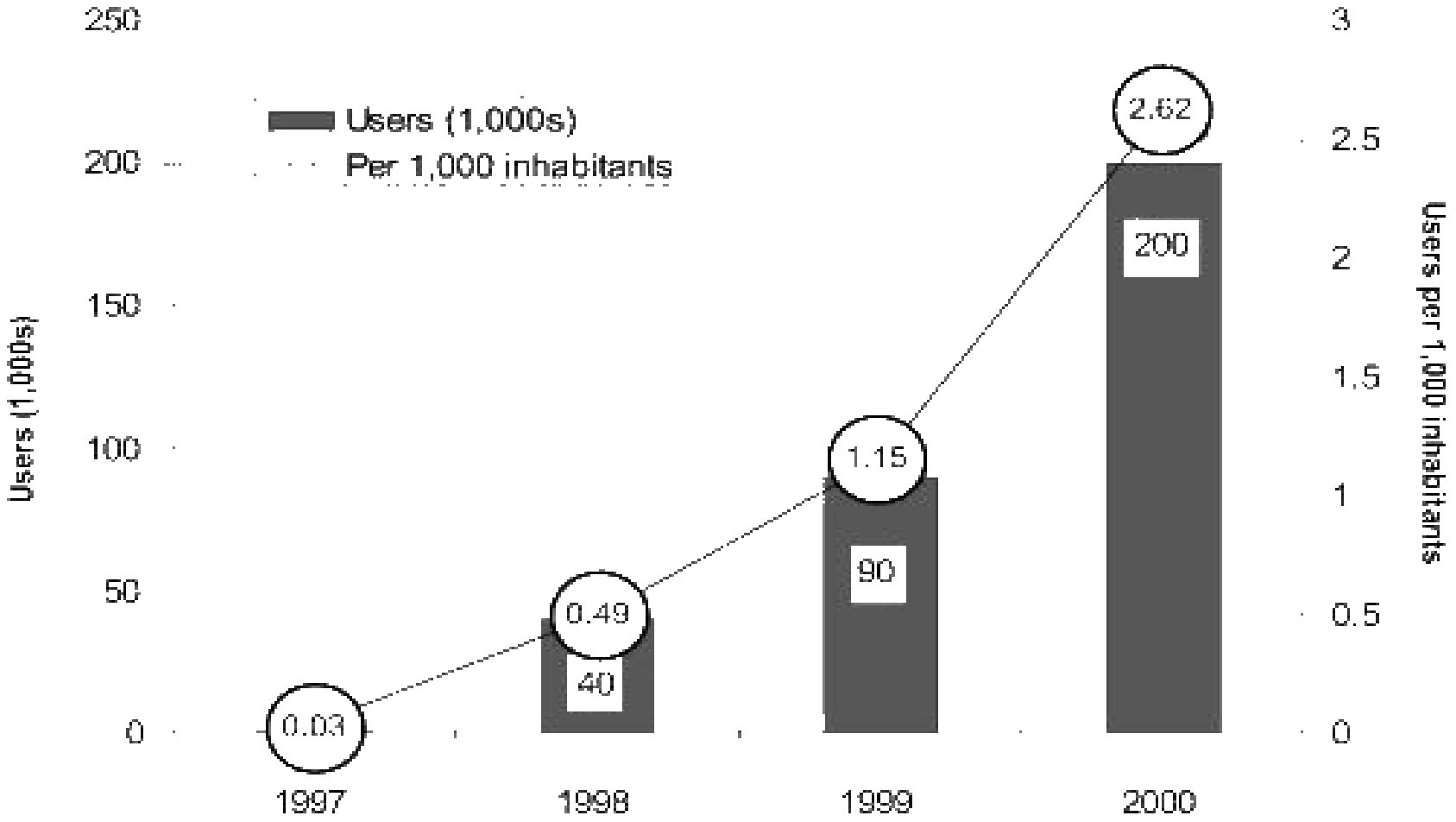
- Nhiều ứng dụng mới: chat, chia sẻ file P2P…
- E-commerce, Yahoo, Amazon, Google…
- > 50 triệu máy trạm, > 100 triệu NSD
- Vấn đề an toàn an ninh thông tin!
  - Internet dành cho tất cả mọi người
  - Tất cả các dịch vụ phải quan tâm tới vấn đề này

# Lược sử Internet Việt Nam



- 1991: Nỗ lực kết nối Internet không thành. ☹ (Vì một lý do nào đó)
- 1996:  Giải quyết các cản trở, chuẩn bị hạ tầng Internet
  - ISP: VNPT
  - 64kbps, 1 đường kết nối quốc tế, một số NSD
- 1997: Việt Nam chính thức kết nối Internet
  - 1 IXP: VNPT
  - 4 ISP: VNPT, Netnam (IOT), FPT, SPT
- 2007: "Mười năm Internet Việt Nam"
  - 20 ISPs, 4 IXPs
  - 19 triệu NSD, 22.04% dân số

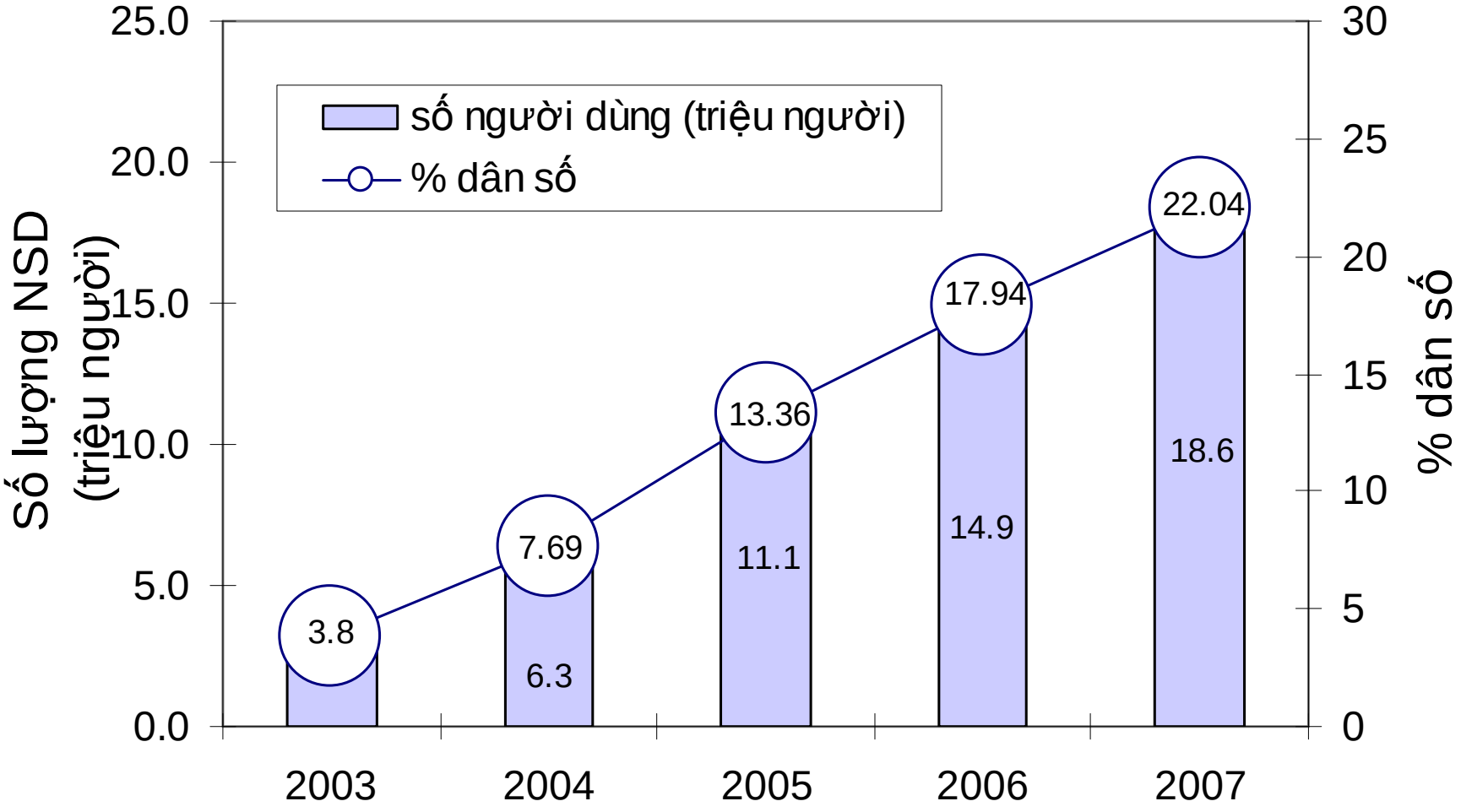
# Phát triển Internet ở VN




**Ước tính số người dùng bằng hai lần số thuê bao**

*Source: Vietnam Internet Case Study*, http://www.itu.int/asean2001/reports/material/VNM%20CS.pdf

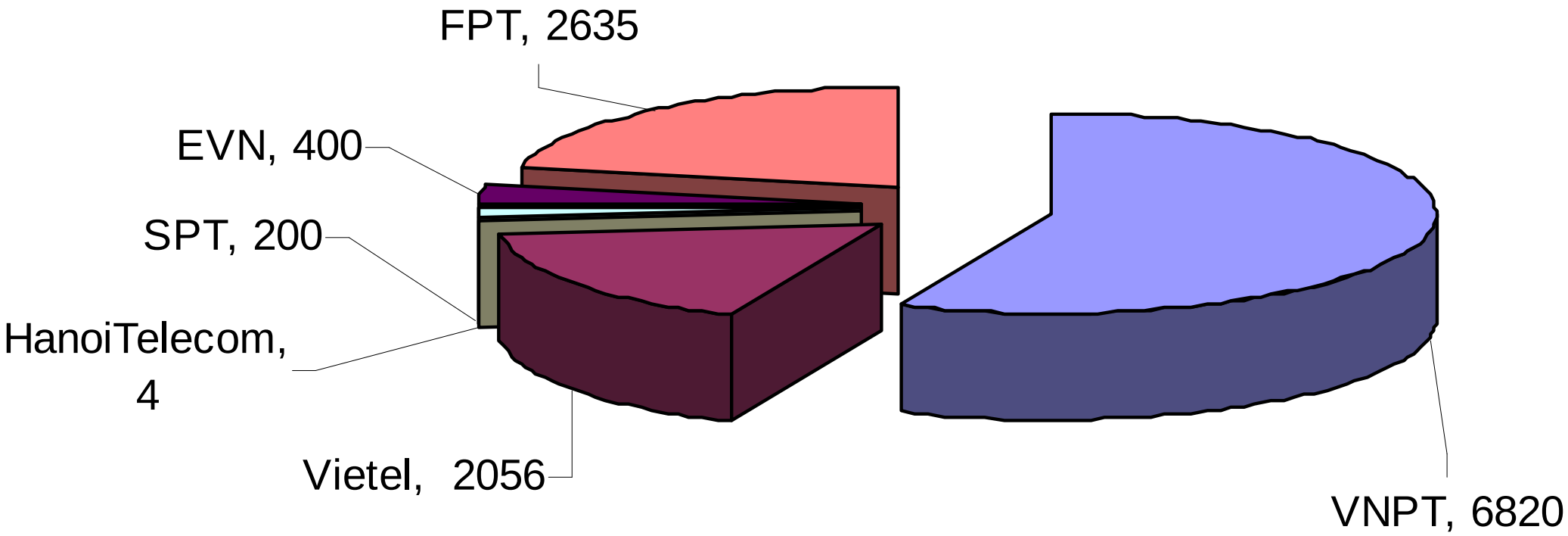
# Thống kê gần đây





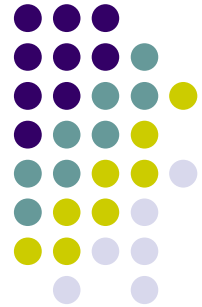

Source: *Vnnic*, http://www.thongkeinternet.vn

# Băng thông kết nối đi quốc tế (Mbps), Q.3 2007



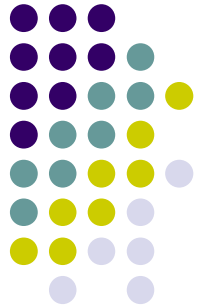

**Tổng cộng: 12115.0 Mbps**

# Internet những năm 2000s: Tương lai là của các bạn



- Ứng dụng và công nghệ mới
  - Youtube, Skype, Bittorrent, Video & VoIP...
  - Mạng không dây, mạng quang học, thông tin di động
  - ….
- Internet sẽ tiếp tục cải tiến dịch vụ và biến đổi không ngừng
  - Mang lại sự thuận tiện cho mọi người
  - Các bạn (sinh viên CNTT) sẽ làm được điều đó!

# Tóm tắt



- Giới thiệu môn học
- Lược sử Internet
- Khái niệm mạng máy tính
- Kiến trúc mạng
  - Topology
  - Protocol
- Mô hình truyền thông
  - Chuyển mạch kênh vs. chuyển mạch gói
  - Không liên kết vs. Hướng liên kết
- Các tham số cơ bản

# Tuần tới…

- Kiến trúc phân tầng
- Mô hình tham chiếu OSI
- Địa chỉ IP, MAC, số hiệu cổng
- DNS và dịch vụ tên miền

**TRƯỜNG ĐẠI HỌC BÁCH KHOA ĐÀ NẴNG**
**KHOA CÔNG NGHỆ THÔNG TIN**

——— Â ———

GIÁO TRÌNH MÔN HỌC

# MẠNG MÁY TÍNH

**Ths. NGUYỄN TẤN KHÔI**

*(Lưu hành nội bộ)*
**Đà Nẵng – 2004**

# MỤC LỤC

*Chương 1 MỞ ĐẦU 1*

**1.1 Giới thiệu ..... 1**

**1.2 Phân loại mạng ..... 2**

1.2.1 Dựa theo khoảng cách địa lý ..... 2

1.2.2 Dựa theo cấu trúc mạng ..... 2

1.2.3 Theo phương pháp chuyển mạch ..... 3

**1.3 Kiến trúc phân tầng và chuẩn hoá mạng ..... 5**

1.3.1 Các tổ chức chuẩn hoá mạng ..... 5

1.3.2 Kiến trúc phân tầng ..... 6

**1.4 Mô hình OSI ..... 7**

1.4.1 Kiến trúc của mô hình OSI ..... 7

1.4.2 Sự ghép nối giữa các mức ..... 8

1.4.3 Chức năng của mỗi tầng ..... 9

1.4.4 Các giao thức chuẩn của OSI ..... 11

**1.5 Hệ điều hành mạng ..... 12**

**1.6 Mạng Internet ..... 13**

1.6.1 Lịch sử ra đời và phát triển ..... 13

1.6.2 Cấu trúc của mạng Internet ..... 14

1.6.3 Các kiến trúc khác ..... 15

*Chương 2 TẦNG VẬT LÝ 16*

**2.1 Môi trường truyền tin ..... 16**

2.1.1 Phương tiện truyền ..... 16

2.1.2 Các thông số cơ bản của môi trường truyền tin ..... 19

**2.2 Chuẩn giao diện ..... 19**

2.2.1 Modem ..... 19

2.2.2 DTE và DCE ..... 21

2.2.3 Chuẩn RS-232C ..... 21

*Chương 3 TẦNG LIÊN KẾT DỮ LIỆU 22*

**3.1 Chức năng ..... 22**

**3.2 Các vấn đề của tầng liên kết dữ liệu ..... 22**

3.2.1 Cung cấp dịch vụ cho tầng mạng ..... 22

3.2.2 Khung tin - Nhận biết gói tin ..... 23

3.2.3 Kiểm tra lỗi ..... 23

3.2.4 Điều khiển luồng dữ liệu ..... 23
3.2.5 Quản lý liên kết ..... 24
3.2.6 Nén dữ liệu khi truyền ..... 24
**3.3 Phát hiện và hiệu chỉnh lỗi ..... 24**
3.3.1 Phương pháp bit chẵn lẻ (Parity) ..... 25
3.3.2 Tính theo đa thức chuẩn ..... 25
3.3.3 Mã sửa sai ..... 26
**3.4 Thủ tục liên kết dữ liệu cơ bản ..... 27**
3.4.1 Giao thức đơn công với kênh có lỗi ..... 28
**3.5 Điều khiển dòng truyền ..... 28**
3.5.1 Cơ chế cửa sổ ..... 29
3.5.2 Trao đổi bản tin với cửa sổ 1 bit ..... 30
3.5.3 Vận chuyển liên tục ..... 31
**3.6 Các giao thức của tầng Liên kết dữ liệu ..... 33**
3.6.1 Giao thức BSC ..... 33
3.6.2 Giao thức HDLC ..... 34
***Chương 4 MẠNG CỤC BỘ 37***
**4.1 Các cấu hình của mạng LAN ..... 37**
4.1.1 Mạng dạng hình sao (Star Topology) ..... 37
4.1.2 Mạng hình tuyến (Bus Topology) ..... 38
4.1.3 Mạng dạng vòng (Ring Topology) ..... 38
4.1.4 Mạng dạng kết hợp ..... 39
**4.2 Các giao thức điều khiển truy nhập đường truyền ..... 39**
4.2.1 Phương pháp CSMA ..... 40
4.2.2 Phương pháp CSMA/CD ..... 41
4.2.3 Điều khiển truy nhập bus với thẻ bài ..... 41
4.2.4 Điều khiển truy nhập vòng với thẻ bài ..... 43
**4.3 Chuẩn hóa mạng cục bộ ..... 44**
4.3.1 Chuẩn Ethernet ..... 46
***Chương 5 TẦNG MẠNG 47***
**5.1 Các vấn đề của tầng mạng ..... 47**
5.1.1 Định địa chỉ cho tầng mạng ..... 47
5.1.2 Dịch vụ cung cấp cho tầng giao vận ..... 48
5.1.3 Tổ chức các kênh truyền tin trong tầng mạng ..... 49
5.1.4 Tìm đường đi trong mạng ..... 50
5.1.5 Tắc nghẽn trong mạng ..... 51

**5.2 Kết nối liên mạng ..... 51**
5.2.1 Các thiết bị dùng để kết nối liên mạng ..... 52
**5.3 Giao thức liên mạng IP ..... 58**
5.3.1 Cấu trúc khung tin IP ..... 59
5.3.2 Địa chỉ IP ..... 64
**5.4 Phân chia mạng con ..... 66**
**5.5 Hoạt động của giao thức IP ..... 67**
**5.6 Các giao thức liên quan đến IP ..... 68**
5.6.1 Giao thức phân giải địa chỉ ARP ..... 68
5.6.2 Giao thức RARP (Reverse Address Resolution Protocol) ..... 71
5.6.3 Giao thức ICMP ..... 71
**5.7 Phiên bản IPv6 ..... 76**
5.7.1 Khung tin IPng v6 ..... 77
**5.8 Định tuyến trên Internet ..... 77**
5.8.1 Bảng chọn đường ..... 77
5.8.2 Xây dựng bảng chọn đường cho các Router/Gateway ..... 78
**5.9 Mạng X.25 ..... 80**
5.9.1 Cơ sở kỹ thuật ..... 80
**5.10 Kỹ thuật FRAME RELAY ..... 82**
5.10.1 Khuôn dạng gói dữ liệu Frame-Relay ..... 82
***Chương 6 TẦNG GIAO VẬN 84***
**6.1 Các vấn đề của tầng giao vận ..... 84**
6.1.1 Cung cấp dịch vụ cho tầng phiên ..... 84
6.1.2 Chất lượng dịch vụ QoS ..... 86
6.1.3 Các lớp giao thức của tầng giao vận ..... 87
6.1.4 Thủ tục giao vận trên X. 25 ..... 90
***Chương 7 HỌ GIAO THỨC TCP/IP 91***
**7.1 Mô hình TCP/IP ..... 91**
**7.2 Giao thức TCP ..... 93**
7.2.1 Khuôn dạng gói tin TCP ..... 94
7.2.2 Quá trình nối-tách ..... 96
7.2.3 Quá trình trao đổi dữ liệu ..... 97
7.2.4 Thứ tự thực hiện ứng dụng TCP/IP ..... 97
**7.3 Giao thức UDP ..... 100**
**7.4 Cổng và Socket ..... 101**

7.4.1 Số hiệu cổng ..... 101
7.4.2 Socket ..... 101
**7.5 Mô hình giao tiếp Client/Server ..... 103**
7.5.1 Quá trình trao đổi dữ liệu dùng Stream Socket ..... 103
7.5.2 Quá trình trao đổi dữ liệu dùng Datagram Socket ..... 104
7.5.3 Ví dụ chương trình client/server ..... 105
***Chương 8 TẦNG PHIÊN 108***
**8.1 Dịch vụ OSI cho tầng Phiên ..... 108**
8.1.1 Cung cấp cho người sử dụng dịch vụ tầng phiên (SS-user) ..... 108
8.1.2 Điều khiển trao đổi dữ liệu ..... 109
8.1.3 Điều hành phiên làm việc ..... 110
8.1.4 Liên kết phiên ..... 111
**8.2 Giao thức chuẩn tầng phiên ..... 111**
8.2.1 Các loại SPDU, các tham số và chức năng ..... 112
***Chương 9 TẦNG TRÌNH DIỄN 114***
**9.1 Vai trò và chức năng ..... 114**
9.1.1 Phiên dịch dữ liệu ..... 116
**9.2 Dịch vụ OSI cho tầng trình diễn ..... 116**
**9.3 Giao thức chuẩn tầng trình diễn ..... 117**
9.3.1 Các chuẩn khác cho tầng trình diễn ..... 118
***Chương 10 TẦNG ỨNG DING 119***
**10.1 An toàn thông tin trên mạng ..... 119**
10.1.1 Các chiến lược an toàn hệ thống ..... 119
10.1.2 An toàn thông tin bằng mã hóa ..... 120
**10.2 CáC phương pháp mã hóa dữ liệu ..... 122**
10.2.1 Phương pháp hoán vị ..... 122
10.2.2 Phương pháp thay thế ..... 123
10.2.3 Phương pháp mã hóa chuẩn DES ..... 124
10.2.4 Phương pháp mã hoá khoá công khai ..... 128
**10.3 Cơ chế bảo vệ bằng firewall ..... 132**
10.3.1 Các loại firewall và cơ chế hoạt động ..... 134
**10.4 Hệ thống tên miền DNS (Domain Name System ) ..... 137**
10.4.1 Không gian tên miền DNS ..... 138
10.4.2 Máy chủ quản lý tên ..... 140
10.4.3 Chương trình phân giải tên ..... 140

**10.5 Hệ quản trị mạng ..... 140**
10.5.1 Hệ bị quản trị ..... 141
10.5.2 Cơ sở dữ liệu chứa thông tin quản trị mạng ..... 141
**10.6 Dịch vụ thư điện tử ..... 142**
10.6.1 Giao thức SMTP ..... 143
10.6.2 MIME ..... 147
10.6.3 Giao thức POP ..... 151
**10.7 Dịch vụ truy cập từ xa - TELNET ..... 154**
10.7.2 Dịch vụ truyền tập tin FTP ..... 156
10.7.3 UserNEWS ..... 162
10.7.4 WORLD-WIDE-WEB ..... 163

*Chương 1*

# MỞ ĐẦU

## 1.1 Giới thiệu

Mạng máy tính là tập hợp nhiều máy tính điện tử và các thiết bị đầu cuối được kết nối với nhau bằng các thiết bị liên lạc nhằm trao đổi thông tin, cùng chia sẻ pcứng, phần mềm và dữ liệu với nhau

Mạng máy tính bao gồm phần cứng, các giao thức và các phần mềm mạng.

Khi nghiên cứu về mạng máy tính, các vấn đề quan trọng được xem xét là giao thức mạng, cấu hình kết nối của mạng, và các dịch vụ trên mạng.

Mạng máy tính có những công dụng như sau :

1. *Tập trung tài nguyên tại một số máy và chia sẻ cho nhiều máy khác*

- Nhiều người có thể dùng chung một phần mềm tiện ích.
- Dữ liệu được quản lý tập trung nên an toàn hơn, trao đổi giữa những người sử dụng thuận lợi hơn, nhanh chóng hơn.
- Mạng máy tính cho phép người lập trình ở một trung tâm máy tính này có thể sử dụng các chương trình tiện ích của một trung tâm máy tính khác đang rỗi, sẽ làm tăng hiệu quả kinh tế của hệ thống.

2. *Khắc phục sự trở ngại về khoảng cách địa lý.*
3. *Tăng chất lượng và hiệu quả khai thác thông tin.*
4. *Cho phép thực hiện những ứng dụng tin học phân tán*
5. *Độ an toàn tin cậy của hệ thống tăng lên nhờ khả năng thay thế khi có sự cố với máy có sự cố :* An toàn cho dữ liệu và phần mềm vì phần mềm mạng sẽ khoá các tập tin khi có những người không đủ quyền hạn truy xuất các tập tin và thư mục đó.
6. *Phát triển các công nghệ trên mạng:* Người sử dụng có thể trao đổi thông tin với nhau dễ dàng và sử dụng hệ mạng như là một công cụ để phổ biến tin tức, thông báo về một chính sách mới, về nội dung buổi họp, về các thông tin kinh tế khác như giá cả thị trường, tin rao vặt (muốn bán hoặc muốn mua một cái gì đó), hoặc sắp xếp thời khoá biểu của mình chen lẫn với thời khoá biểu của những người khác , . . .

## 1.2 Phân loại mạng

### 1.2.1 Dựa theo khoảng cách địa lý

Mạng máy tính có thể phân bổ trên một khu vực nhất định hoặc có thể trong một quốc gia hay toàn cầu. Dựa vào phạm vi phân bố, người ta có thể phân ra các loại mạng như sau:

a. LAN (Local Area Network - Mạng cục bộ) : LAN thường được sử dụng trong nội bộ một cơ quan/tổ chức..., kết nối các máy tính trong một khu vực bán kính khoảng 100m-10km. Kết nối được thực hiện thông qua các môi trường truyền thông tốc độ cao, ví dụ cáp đồng trục hay cáp quang.

b. MAN (Metropolitan Area Network - Mạng đô thị) : Kết nối các máy tính trong phạm vi một thành phố. Kết nối này được thực hiện thông qua các môi trường truyền thông tốc độ cao (50-100 Mbit/s).

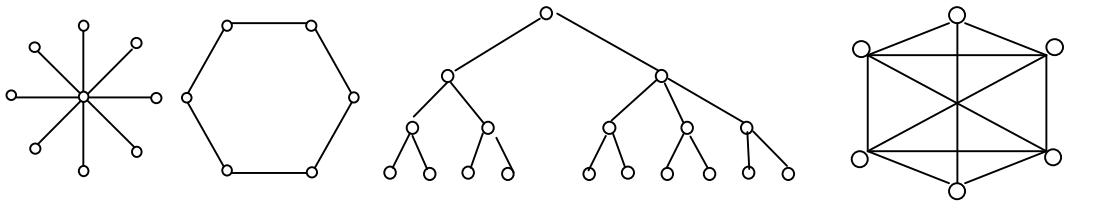
c. WAN (Wide Area Network) - Mạng diện rộng, kết nối máy tính trong nội bộ các quốc gia hay giữa các quốc gia trong cùng một châu lục. Thông thường kết nối này được thực hiện thông qua mạng viễn thông. Các WAN có thể được kết nối với nhau thành GAN hay tự nó đã là GAN.

d. GAN (Global Area Network) : Mạng toàn cầu, kết nối máy tính từ các châu lục khác nhau. Thông thường kết nối này được thực hiện thông qua mạng viễn thông và vệ tinh.

Trong các khái niệm nói trên, WAN và LAN là hai khái niệm hay được sử dụng nhất.

### 1.2.2 Dựa theo cấu trúc mạng

#### *1.2.2.1 Kiểu điểm - điểm (point - to - point)*

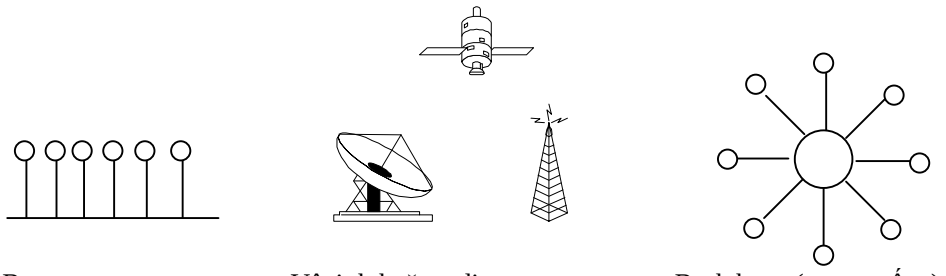



Hình 1-1. Cấu trúc mạng kiểu điểm-điểm.

Đường truyền nối từng cặp nút mạng với nhau. Thông tin đi từ nút nguồn qua nút trung gian rồi gởi tiếp nếu đường truyền không bị bận. Do đó còn có tên là mạng lưu trữ và chuyển tiếp (*store and forward*).

#### *1.2.2.2 Kiểu khuyếch tán*

Bản tin được gởi đi từ một nút nào đó sẽ được tiếp nhận bởi các nút còn lại (còn gọi là broadcasting hay point to multipoint). Trong bản tin phải có vùng địa chỉ cho phép mỗi nút kiểm tra xem có phải tin của mình không và xử lý nếu đúng bản tin được gởi đến.




Hình 1-2. Sơ đồ kết nối theo kiểu khuyếch tán.

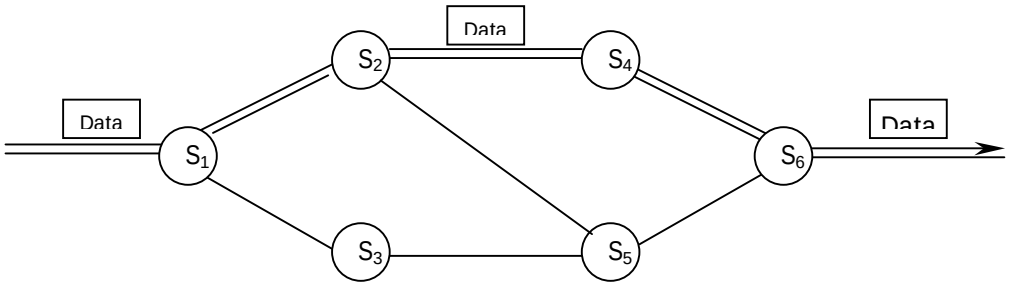
Trong cấu trúc dạng Bus và Vòng cần cơ chế "*trọng tài*" để giải quyết các xung đột (collision) xảy ra khi nhiều nút muốn truyền tin đồng thời. Trong cấu trúc vệ tinh hoặc radio, mỗi nút cần có ăng-ten thu và phát.

### 1.2.3 Theo phương pháp chuyển mạch

- Mạng chuyển mạch kênh (Line switching network), ví dụ như mạng điện thoại.
- Mạng chuyển mạch thông báo (Message switching network)
- Mạng chuyển mạch gói (Packet switching network)

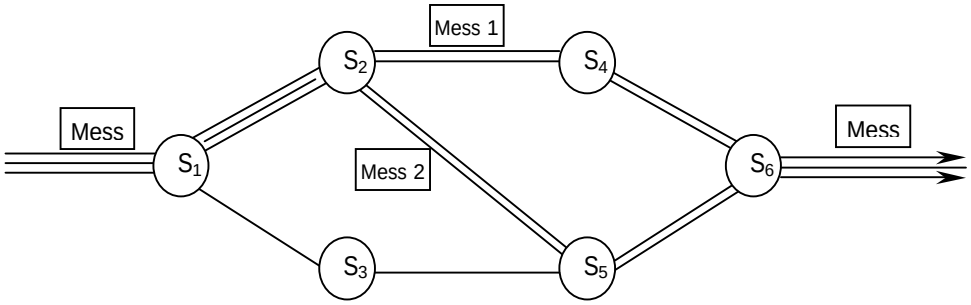
#### *1.2.3.1 Chuyển mạch kênh*

Chuyển mạch kênh (line switching) được dùng trong mạng điện thoại. Một kênh cố định được thiết lập giữa cặp thực thể cần liên lạc với nhau. Mạng này có hiệu suất không cao vì có lúc kênh bỏ không.




Hình 1-3. Mạng chuyển mạch kênh.

### *1.2.3.2 Mạng chuyển mạch bản tin*




Hình 1-4. Phương pháp chuyển mạch thông báo.

Các nút của mạng căn cứ vào địa chỉ đích của "bản tin" để chọn nút kế tiếp. Như vậy các nút cần lưu trữ và đọc tin nhận được, quản lý việc truyền tin. Trong trường hợp bản tin quá dài và nếu sai phải truyền lại thì hiệu suất không cao. Phương pháp này giống như cách gởi thư thông thường.

- Ưu điểm so với phương pháp chuyển mạch kênh:

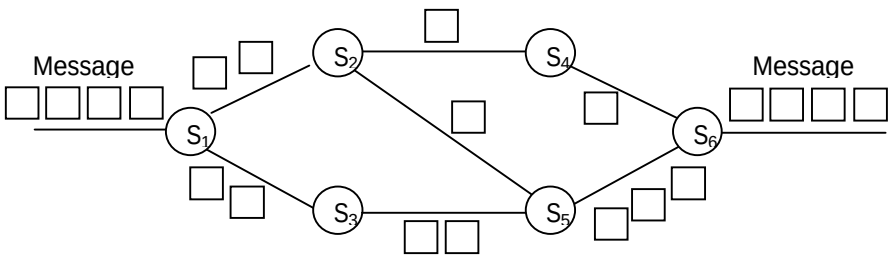
- Hiệu suất sử dụng đường truyền cao vì không bị chiếm dụng độc quyền mà được phân chia giữa nhiều thực thể.
- Mỗi nút mạng (hay nút chuyển mạch thông bao) có thể lưu trữ message cho tới khi kênh truyền rỗi mới gửi bản tin đi. Do đó giảm được tình trạng tắc nghẽn (congestion) trên mạng.
- Điều khiển việc truyền tin bằng cách sắp xếp độ ưu tiên cho các bản tin.
- Có thể tăng hiệu suất sử dụng giải thông của mạch bằng cách gán địa chỉ quảng bá (broadcast) để gởi bản tin đồng thời đến nhiều đích.

- Nhược điểm:

- Do không hạn chế kích thước của bản tin nên có thể dẫn đến phí tổn lưu trữ tạm thời cao và ảnh hưởng đến thời gian hồi đáp và chất lượng truyền đi.

Mạng chuyển mạch thông báo thích hợp với các dịch vụ thông tin kiểu thư điện tử (Email) hơn là đối với các ứng dụng có tính thời gian thực vì tồn tại độ trễ nhất định do lưu trữ và xử lý thông tin điều khiển tại mỗi nút.

### *1.2.3.3 Mạng chuyển mạch gói*




Hình 1-5. Mạng chuyển mạch gói.

Bản tin được chia thành nhiều gói tin (packet) độ dài 512 bytes, phần đầu là địa chỉ đích, mã để tập hợp các gói. Các gói của các bản tin khác nhau có thể được truyền độc lập trên cùng một đường truyền. Vấn đề phức tạp ở đây là tạo lại bản tin ban đầu, đặc biệt khi được truyền trên các con đường khác nhau.

Chuyển mạch gói mềm dẻo, hiệu suất cao. Xu hướng phát triển hiện nay là sử dụng hai kỹ thuật chuyển mạch kênh và chuyển mạch gói trong cùng một mạng thống nhất gọi là mạng ISDN (*Integrated Services Digital Network* - Mạng thông tin số đa dịch vụ).

## 1.3 Kiến trúc phân tầng và chuẩn hoá mạng

Tình trạng không tương thích giữa các mạng đặc biệt là các mạng trên thị trường gây trở ngại cho những người sử dụng khác nhau. Do đó cần phải xây dựng mô hình chuẩn làm cơ sở cho các nhà nghiên cứu thiết kế mạng để tạo ra các sản phẩm mới về mạng, dễ phổ cập, sản xuất, sử dụng. Các chuẩn có vai trò quan trọng trong công tác thiết kế và xây dựng các hệ thống kỹ thuật và công nghệ.

*Chuẩn hóa mạng máy tính là nêu ra các tiêu chuẩn cơ bản thống nhất về cấu trúc mạng giúp cho các mạng khác nhau có thể trao đổi thông tin được với nhau.*

Để mạng hoạt động đạt khả năng tối đa, các tiêu chuẩn được chọn phải cho phép mở rộng mạng để có thể phục vụ những ứng dụng không dự kiến trước trong tương lai tại lúc lắp đặt hệ thống và điều đó cũng cho phép mạng làm việc với những thiết bị được sản xuất từ nhiều hãng khác nhau.

### 1.3.1 Các tổ chức chuẩn hoá mạng

Hai tổ chức chính thực hiện chuẩn hóa mạng là ISO và CCTTT.

1. ISO (*International Standards Organization*) - Tổ chức chuẩn hóa quốc tế. ISO hoạt động dưới sự bảo trợ của LHQ. Thành viên của ISO là các cơ quan tiêu chuẩn hóa của các quốc gia và các Ban chuyên môn. Ban TC97 được chia ra thành các tiểu ban và các nhóm công tác.
2. IEEE (*Institute of Electrical and Electronic Engineers*) - Viện nghiên cứu các vấn đề về kỹ thuật điện và điện tử của Mỹ. IEEE chịu trách nhiệm về tầng Data Link và Physical. Phân ban các chuẩn này là phân ban 802 (thành lập tháng Hai năm 1980).
3. CCITT (*Commité Consultatif Internatinal pour Télégraphe et Téléphone*) - Tổ chức tư vấn quốc tế về điện báo và điện thoại hoạt động dưới sự bảo trợ của LHQ, chuyên nghiên cứu nhằm công bố các khuyến nghị thống nhất về mạng

máy tính. Bao gồm các khuyến nghị liên quan đến việc truyền dữ liệu trên mạng, mạng ISDN.

4. ANSI (*American National Standards Institute*) :Viện nghiên cứu các chuẩn quốc gia của Mỹ.
5. ECMA (*European Computer Manufactures Association*) : Hiệp hội máy tính châu âu
6. ATM Forum (*Asynchronous Transfers Mode*) - Thực hiện các giải pháp cho mạng ISDN.
7. IETF (*Internet Enggineering Task Force*) : Sản xuất các chuẩn liên quan đến Internet (SNMP, TCP/IP ...)

### 1.3.2 Kiến trúc phân tầng

Để giảm độ phức tạp thiết kế, kiến trúc mạng được tổ chức thành một cấu trúc đa tầng, mỗi tầng được xây trên tầng trước nó, tầng dưới sẽ cung cấp dịch vụ cho tầng cao hơn. Tầng N trên một máy thực hiện việc giao tiếp với tầng N trên một máy khác. Các qui tắc, luật lệ được sử dụng cho việc giao tiếp này được gọi là các giao thức của tầng N.

Các thực thể (entity) nằm trên các tầng tương ứng trên những máy khác nhau gọi là các tiến trình đồng mức. Các tiến trình đồng mức giao tiếp với nhau bằng cách sử dụng các giao thức trong tầng của nó.

Giữa 2 tầng kề nhau tồn tại một giao diện (*interface*) xác định các hàm nguyên thủy và các dịch vụ tầng dưới cung cấp cho tầng trên.

Tập hợp các tầng và các giao thức được gọi là kiến trúc mạng (*Network Architecture*).

Cấu trúc phân tầng của mạng máy tính có ý nghĩa đặc biệt như sau :

- Thuận tiện trong công tác thiết kế, xây dựng và cài đặt các mạng máy tính, trong đó mỗi hệ thống thành phần được xem như là một cấu trúc đa tầng.
- Mỗi tầng được xây dựng dựa trên cơ sở tầng kề liền trước đó. Như vậy tầng dưới sẽ cung cấp dịch vụ cho tầng trên.
- Số lượng, tên gọi và chức năng của mỗi tầng sẽ được người thiết kế mạng máy tính cụ thể quy định.
- Tập hợp các giao thức, các vấn đề kỹ thuật và công nghệ cho mỗi tầng có thể được khảo sát, nghiên cứu triển khai độc lập với nhau.

- Giao thức : Mỗi khi trao đổi thông tin như điện thoại, telex, viết . . . người ta phải tuân theo một số quy luật. Các quy luật này được nhóm lại và gọi là giao thức (*protocol*).

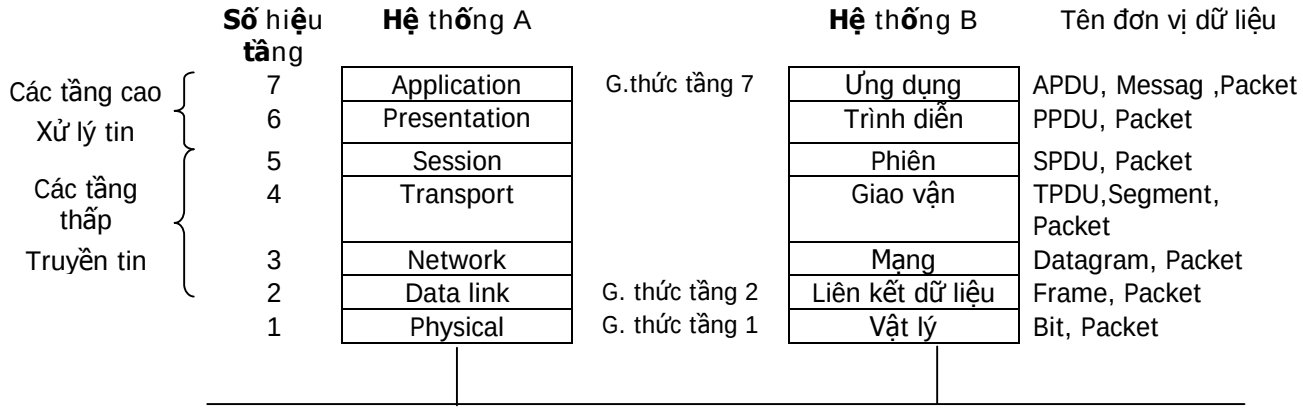
Giao thức có các chức năng chính như sau :

1. Định nghĩa cấu trúc khung một cách chính xác cho từng byte, các ký tự và bản tin.
2. Phát hiện và xử lý các lỗi, thông thường là gửi lại bản tin gốc sau khi phát hiện lần trước bị lỗi
3. Quản lý thứ tự các lệnh để đếm các bản tin, nhận dạng, tránh mất hoặc thu thừa bản tin.
4. Đảm bảo không nhầm lẫn giữa bản tin và lệnh
5. Chỉ ra các thuộc tính đường dây khi lập các đường nối đa điểm hoặc bán song công (cho biết ai đối thoại với ai).
6. Giải quyết vần đề xung đột thâm nhập (yêu cầu đồng thời), gửi khi chưa có số liệu, mất liên lạc, khởi động.

## 1.4 Mô hình OSI

### 1.4.1 Kiến trúc của mô hình OSI

Dựa trên kiến trúc phân tầng, ISO đã đưa ra mô hình 7 tầng (layer) cho mạng, gọi là mô hình kết nối hệ thống mở hoặc mô hình OSI (Open Systems Interconnection model), vào năm 1984.




Hình 1-6. Mô hình OSI 7 tầng.

Nhóm các tầng thấp (*physical, data link, network, transport*) liên quan đến các phương tiện cho phép truyền dữ liệu qua mạng. Các tầng thấp đảm nhiệm việc truyền dữ liệu, thực hiện quá trình đóng gói, dẫn đường, kiểm duyệt và truyền từng nhóm dữ liệu. Các tầng này không cần quan tâm đến loại dữ liệu mà nó nhận được từ hay gửi cho tầng ứng dụng, mà chỉ đơn thuần là gửi chúng đi.

Nhóm các tầng cao (*session, presentation, application*) liên quan chủ yếu đến việc đáp ứng các yêu cầu của người sử dụng để triển khai các ứng dụng của họ trên mạng thông qua các phương tiện truyền thông cung cấp bởi các nhóm tầng thấp.

Hệ thống kết nối mở OSI là hệ thống cho phép truyền thông tin với các hệ thống khác, trong đó các mạng khác nhau, sử dụng những giao thức khác nhau, có thể thông báo cho nhau thông qua chương trình để chuyển từ một giao thức này sang một giao thức khác.

Mô hình OSI đưa ra giải pháp cho vấn đề truyền thông giữa các máy tính không giống nhau. Hai hệ thống, dù khác nhau đều có thể truyền thông với nhau một cách hiệu quả nếu chúng đảm bảo những điều khiển chung sau đây :

1. Các hệ thống đều cài đặt cùng một tập hợp các chức năng truyền thông.
2. Các chức năng đó được tổ chức thành cũng một tập các tầng. Các tầng đồng mức phải cung cấp các chức năng như nhau, nhưng phương thức cung cấp không nhất thiết phải giống nhau.
3. Các tầng đồng mức phải sử dụng một giao thức chung.

Để đảm bảo những điều trên cần phải có các chuẩn xác định các chức năng và dịch vụ được cung cấp bởi một tầng (nhưng không cần chỉ ra chúng phải cài đặt như thế nào). Các chuẩn cũng phải xác định các giao thức giữa các tầng đồng mức. Mô hình OSI chính là cơ sở để xây dựng các chuẩn đó.

### 1.4.2 Sự ghép nối giữa các mức

Trong thực tế dữ liệu không truyền trực tiếp từ tầng i máy này sang tầng i máy kia (trừ tầng thấp nhất). tầng thấp nhất có đường truyền thông vật lý tới tầng thấp nhất của máy tương ứng từ đó dữ liệu và thông tin điều khiển lại được chuyển ngược lên tầng trên. Tầng trên chỉ xác định đường truyền thông lôgic (truyền thông ảo).

- Các Header của giao thức : Thông thường, thông tin điều khiển giao thức được gói thành một khối và được đặt trước dữ liệu nó đi kèm và được gọi là *Header* hay *Protocol Header*, được dùng để truyền thông tin giữa các tầng và giữa các máy tính với nhau. Các header của giao thức được phát triển theo các luật được cho trong tập tài liệu ASN.1 của ISẶ.
- Khi máy A gửi tin đi, các đơn vị dữ liệu đi từ tầng trên xuống dưới. Qua mỗi tầng nó được bổ sung thông tin điều khiển của tầng đó.
- Khi nhận tin, thông tin đi từ dưới lên. Qua mỗi tầng thông tin điều khiển được khử bỏ dần và cuối cùng máy B nhận được bản tin của A.

### 1.4.3 Chức năng của mỗi tầng

***1. Tầng Vật lý***

Cung cấp phương tiện truyền tin, thủ tục khởi động, duy trì huỷ bỏ các liên kết vật lý. Giữ nhiệm vụ chuyển tải các bit thông tin trên kênh truyền thông. Tầng Vật lý làm việc với các giao diện cơ, điện và giao diện thủ tục (chức năng) trên môi trường vật lý, không quan tâm đến nội dung biểu diễn của các bit.

Thực chất tầng này thực hiện nối liền các phần tử của mạng thành một hệ thống bằng các phương pháp vật lý, ở mức này sẽ có các thủ tục đảm bảo cho các yêu cầu về chuyển mạch hoạt động nhằm tạo ra các đường truyền thực cho các chuỗi bit thông tin.

***2. Tầng liên kết dữ liệu***

Thiết lập, duy trì, huỷ bỏ các liên kết dữ liệu kiểm soát luồng dữ liệu, phát hiện và khắc phục sai sót truyền tin

Tiến hành chuyển đổi thông tin dưới dạng chuỗi các bit ở mức mạng thành từng đoạn gọi là khung tin (frame). Sau đó đảm bảo truyền liên tiếp các khung tin tới tầng vật lý, đồng thời xử lý các thông báo từ trạm thu gửi trả lại. Bit thông tin trong khung tin đều mang những ý nghĩa riêng, bao gồm các *trường địa chỉ, trường kiểm tra, dữ liệu và kiểm tra lỗi* dùng cho các mục đích riêng.

Nhiệm vụ chính của mức 2 này là khởi tạo, tổ chức các khung tin và xử lý các thông tin liên quan tới khung tin.

***3. Tầng mạng***

Tầng mạng được xây dựng dựa trên kiểu nối kết *điểm - điểm* do tầng LKDL cung cấp, bảo đảm trao đổi thông tin giữa các mạng con trong một mạng lớn, mức này còn được gọi là mức thông tin giữa các mạng con với nhau.

Có nhiệm vụ gán địa chỉ cho các bản tin và chuyển đổi địa chỉ logic hay các tên thành các địa chỉ vật lý.

Thực hiện chọn đường truyền tin, cung cấp dịch vụ định tuyến (chọn đường) cho các gói dữ liệu trên mạng. Tầng này chỉ ra dữ liệu từ nguồn tới đích sẽ đi theo tuyến nào trên cơ sở các điều kiện của mạng, độ ưu tiên dịch vụ và các nhân tố khác.

Kiểm soát luồng dữ liệu, khắc phục sai sót, cắt/hợp dữ liệu, giúp loại trừ sự tắc nghẽn cũng như điều khiển luồng thông tin.

***4. Tầng Giao vận***

Tầng giao vận giúp đảm bảo độ tin cậy khi chuyển giao dữ liệu và tính toàn vẹn dữ liệu từ nơi gửi đến nơi nhận. Điều này được thực hiện dựa trên cơ chế kiểm tra lỗi do các tầng bên dưới cung cấp. Tầng giao vận còn chịu trách nhiệm tạo ra nhiều kết nối cục bộ trên cùng một kết nối mạng gọi là ghép kênh (multiplexing), phân chia thời gian xử lý (time sharing), cắt hợp dữ liệu.

Nhiệm vụ của mức này là xử lý các thông tin để chuyển tiếp các chức năng từ tầng phiên đến tầng mạng và ngược lại. Thực chất mức truyền này là để đảm bảo thông tin giữa các máy chủ với nhau. Mức này nhận các thông tin từ tầng phiên, phân chia thành các đơn vị dữ liệu nhỏ hơn và chuyển chúng tới mức mạng.

***5. Tầng phiên***

Thiết lập, duy trì, đồng bộ hoá và huỷ bỏ các phiên truyền thông. Liên kết phiên phải được thiết lập thông qua đối thoại và trao đổi các thông số điều khiển.

Dùng tầng giao vận để cung cấp các dịch vụ nâng cao cho phiên làm việc như: kiểm soát các cuộc hội thoại, quản lý thẻ bài (*token*), quản lý hoạt động (*activity management*).

Nhận dạng tên và thủ tục cần thiết cũng như là các công việc bảo mật, để hai ứng dụng có thể giao tiếp với nhau trên mạng. Nhờ tầng phiên, những người sử dụng lập được các đường nối với nhau, khi cuộc hội thoại được thành lập thì mức này có thể quản lý cuộc hội thoại đó theo yêu cầu của người sử dụng. Một kết nối giữa hai máy cho phép người sử dụng được đăng ký vào một hệ thống phân chia thời gian từ xa hoặc chuyển tập tin giữa 2 máy.

***6. Tầng trình diễn***

Quản lý cách thức biểu diễn thông tin theo cú pháp dữ liệu của người sử dụng, loại mã sử dụng (ASCII, QBCDIC, ...) và thực hiện các vấn đề nén dữ liệu.

Nhiệm vụ của mức này là lựa chọn cách tiếp nhận dữ liệu, biến đổi các ký tự, chữ số của mã ASCII hay các mã khác và các ký tự điều khiển thành một kiểu mã nhị phân thống nhất để các loại máy khác nhau đều có thể thâm nhập vào hệ thống mạng.

***7. Tầng ứng dụng***

Tầng này là giao diện giữa người sử dụng và môi trường hệ thống mở.

Tầng này có nhiệm vụ phục vụ trực tiếp cho người sử dụng, cung cấp tất cả các yêu cầu phối ghép cần thiết cho người sử dụng, yêu cầu phục vụ chung như chuyển các File, sử dụng các Terminal của hệ thống,.... Mức sử dụng bảo đảm tự động hoá quá trình thông tin, giúp cho người sử dụng khai thác mạng tốt nhất.

### 1.4.4 Các giao thức chuẩn của OSI

#### *1.4.4.1 Các hàm nguyên thủy*

Mỗi thực thể truyền thông với các thực thể ở tầng trên và dưới nó qua một *giao diện* (interface). Giao diện này gồm một hoặc nhiều điểm truy cập dịch vụ (SAP - Service Access Point). Thực thể tầng N-1 cung cấp dịch vụ cho thực thể tầng N thông qua việc gọi các hàm dịch vụ nguyên thủy (primitive).

Hàm nguyên thuỷ chỉ rõ chức năng cần thực hiện và được dùng để chuyển dữ liệu và thông tin điều khiển. Bốn hàm nguyên thuỷ được sử dụng để định nghĩa tương tác giữa các tầng kề nhau như sau :

| | |
|---|---|
| request | *Ịêu cầu* |
| indication | *Chỉ báo* |
| response | *Trả lời* |
| confirm | *Xác nhận* |

*request* được gởi bởi người sử dụng dịch vụ ở tầng N+1 trong hệ thống A để gọi thủ tục của giao thức ở tầng N. Ịêu cầu này được cấu tạo dưới dạng một hoặc nhiều đơn vị dữ liệu giao thức (PDU - *Protocol Data Unit*) để gởi tới B.

Khi nhận được PDU, một thủ tục của giao thức ở tầng N của B sẽ thông báo yêu cầu đó lên tầng N+1 bằng hàm nguyên thủy *indication*. Sau đó *response* được gởi từ N + 1 của B xuống N gọi thủ tục giao thức tầng N để trả lời tới A.

Khi nhận được trả lời này một thủ tục giao thức tầng N sẽ gởi hàm *confirm* lên N+1 để hoàn tất chu trình yêu cầu thiết lập liên kết của người sử dụng ở tầng N+1 của A.

Các chu trình của người sử dụng khác nhau được phân biệt nhờ khái niệm điểm thâm nhập dịch vụ (SAP - *Service Access Point*) ở ranh giới của 2 tầng N + 1 và N.

#### *1.4.4.2 Các phương thức truyền thông*

Tại mỗi tầng trong mô hình OSI có 2 phương thức hoạt động chính được sử dụng : phương thức có liên kết (*connection oriented*) và phương thức không liên kết (*connectionless*).

Với các phương thức truyền không liên kết thì chỉ có một giai đoạn truyền dữ liệu. Các gói tin dữ liệu (còn được gọi là datagram) được truyền độc lập với nhau theo một con đường xác định dần bằng địa chỉ đích được đặt trong mỗi datagram. Có 3 giai đoạn phân biệt :

- *Thiết lập liên kết* : hai thực thể cùng tầng ở hai đầu của liên kết sẽ thương lượng với nhau về tập các tham số sử dụng trong giai đoạn truyền dữ liệu.
- *Truyền dữ liệu* : các cơ chế kiểm soát sai sót, luồng dữ liệu, ghép kênh, cắt hợp dữ liệu được thực hiện để tăng cường độ tin cậy và hiệu suất của việc truyền dữ liệu.
- *Kết thúc truyền* : giải phóng các tài nguyên hệ thống đã được cấp phát cho liên kết để dùng vào mục đích khác.

Tương ứng với 3 giai đoạn trao đổi trên, có 3 loại thủ tục cơ bản được sử dụng : CONNECT, DATA, DISCONNECT.

Ví dụ đối với giao thức tầng N ta có các thủ tục :

| | |
|---|---|
| N_CONNECT | Thiết lập liên kết |
| N_DATA | Truyền dữ liệu |
| N_DISCONNECT | Huỷ bỏ liên kết |

Ngoài ra có một số các thủ tục phụ được sử dụng tuỳ theo chức năng của mỗi tầng.

| | | |
|---|---|---|
| *Ví dụ:* | Thủ tục N_RESTART | Dùng để khởi động lại hệ thống ở tầng 3 |
| | Thủ tục T_EXPEDITED_DATA | Dùng cho việc truyền dữ liệu nhanh tầng 4 |
| | Thủ tục S_TOKEN_GIVE | Dùng để chuyển điều khiển ở tầng 5 |

Mỗi thủ tục trên sẽ dùng các hàm nguyên thuỷ (*request, indication, response, confirm*) để tạo thành các hàm cơ bản của mô hình OSI.

## 1.5 Hệ điều hành mạng

Việc lựa chọn hệ điều hành mạng (NOS - Network Operating System) làm nền tảng cho mạng tuỳ thuộc vào kích cỡ của mạng hiện tại và sự phát triển trong tương lai, ngoài ra còn tuỳ thuộc vào những ưu điểm và nhược điểm của từng hệ điều hành.

Một số hệ điều hành mạng phổ biến hiện nay:

- Hệ điều hành mạng UNIX: Đây là hệ điều hành do các nhà khoa học xây dựng và được dùng rất phổ biến trong giới khoa học, giáo dục. Hệ điều hành mạng UNIX là hệ điều hành đa nhiệm, đa người sử dụng, phục vụ cho truyền thông tốt. Nhược điểm của nó là hiện nay có nhiều Version khác nhau, không thống nhất gây khó khăn cho người sử dụng và là hệ điều hành này phức tạp.
- Hệ điều hành mạng Windows 2000: Đây là hệ điều hành của hãng Microsoft, cũng là hệ điều hành đa nhiệm, đa người sử dụng. Được xây dựng dựa trên công nghệ của hệ điều hành Windows NT. Đặc điểm của nó là tương đối dễ sử dụng, hỗ trợ mạnh cho các phần mềm WINDOWS. Windows 2000 có thể

liên kết tốt với máy chủ Novell Netware, Unix. Tuy nhiên, để chạy có hiệu quả, Windows 2000 Server đòi hỏi cấu hình máy tương đối mạnh.

- Hệ điều hành mạng NetWare của Novell: Đây là hệ điều hành phổ biến trên thế giới trong thời gian cuối, nó có thể dùng cho các mạng nhỏ (khoảng từ 5-25 máy tính) và cũng có thể dùng cho các mạng lớn gồm hàng trăm máy tính. Netware là một hệ điều hành LAN dùng cho các máy tính theo chuẩn của IBM hay các máy tính Apple Macintosh, chạy trên hệ điều hành MS-DOS hoặc OS/2.

## 1.6 Mạng Internet

### 1.6.1 Lịch sử ra đời và phát triển

Vào những năm 60, Bộ Quốc phòng Mỹ cho triển khai khẩn trương một mạng lưới thông tin với yêu cầu: Nếu như một trạm trung chuyển nào đó trong mạng bị phá huỷ, toàn bộ hệ thống thông tin vẫn phải làm việc bình thường... Cơ quan Nghiên cứu Dự án Cao cấp (ARPA - Advanced Research Projects Agency) thuộc Bộ Quốc phòng Mỹ được giao trách nhiệm thực hiện việc nghiên cứu kỹ thuật liên mạng (internet) nhằm đáp ứng yêu cầu trên. Đây là mạng chuyển mạch gói (packet switching) đầu tiên trên thế giới, lấy tên là ARPAnet. Ban đầu, ARPAnet chỉ gồm một vài mạng nhỏ được chọn lựa của các trung tâm nghiên cứu và phát triển khoa học. Giao thức truyền thông lúc bấy giờ là kiểu điểm - điểm, rất chậm và thường xuyên gây tắc nghẽn trên mạng. Để giải quyết vấn đề này, vào năm 1974 Vinton G. Cerf và Robert O. Kahn đưa ra ý tưởng thiết kế một bộ giao thức mạng mới thuận tiện hơn, đó chính là tiền thân của giao thức TCP/IP.

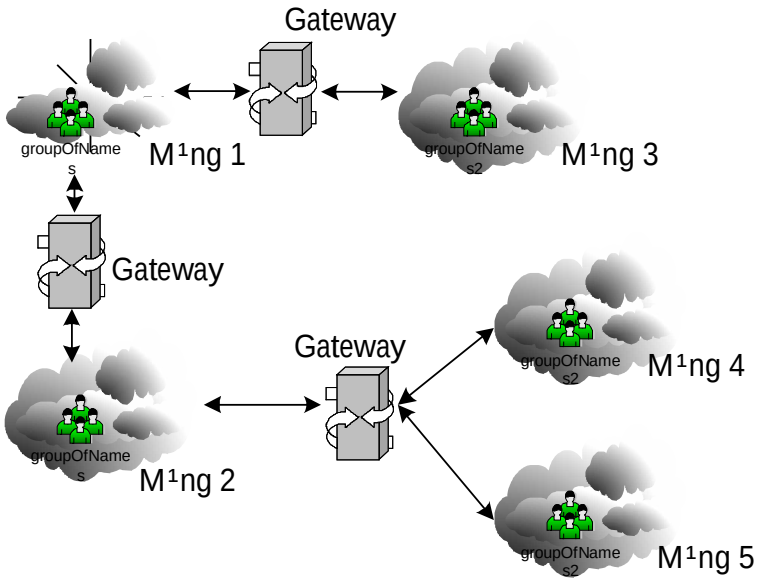
Tháng 09/1983, dưới sự tài trợ của Bộ Quốc phòng Mỹ, Berkeley Software Distribution đưa ra bản Berkeley UNIX 4.2BSD có kết hợp giao thức TCP/IP, biến TCP/IP thành phương tiện kết nối các hệ thống UNIX. Trên cơ sở đó, mạng ARPANỌT nhanh chóng lan rộng và chuyển từ mạng thực nghiệm sang hoạt động chính thức: nhiều trường đại học, viện nghiên cứu ghi tên gia nhập để trao đổi thông tin. Đến năm 1984, mạng ARPANỌT được chia thành hai nhóm mạng nhỏ hơn là MILNET, dành cho quốc phòng, và nhóm mạng thứ hai vẫn gọi là ARPANET, dành cho nghiên cứu và phát triển. Hai nhóm này vẫn có mối liên hệ trao đổi dữ liệu với nhau qua giao thức TCP/IP và được gọi chung là Enternet.

Mạng Internet đã và đang trở thành phương tiện trao đổi thông tin toàn cầu, là phương thức thông tin nhanh với lưu lượng truyền tải dữ liệu rất lớn. Thông qua Internet mà các nhà nghiên cứu khoa học kỹ thuật, các cơ quan giáo dục đào tạo, các nhà doanh nghiệp... có thể trao đổi thông tin với nhau, hoặc truy cập thông tin

của nhau về các công trình, các lĩnh vực nghiên cứu mới nhất; về các phương pháp, hình thức giáo dục và đào tạo, về các thông tin kinh tế, thị trường giá cả... một cách nhanh chóng, thuận tiện và dễ dàng.

### 1.6.2 Cấu trúc của mạng Internet

Mạng Internet không phải một mạng đơn mà là bao gồm nhiều mạng con (sub-network) được kết nối với nhau thông qua các cổng (gateway) như trên hình. Thuật ngữ mạng con ở đây mang nghĩa một *đơn vị mạng hoàn chỉnh* trong hệ thống mạng lớn. Mạng con hoàn toàn có thể là một mạng WAN với quy mô quốc gia, và có khả năng hoạt động độc lập với Internet. Do giao thức TCP/IP không phụ thuộc lớp vật lý, các mạng con có thể sử dụng những công nghệ ghép nối khác nhau (như Ọthernet, X.25,...) mà vẫn giao tiếp được với nhau.

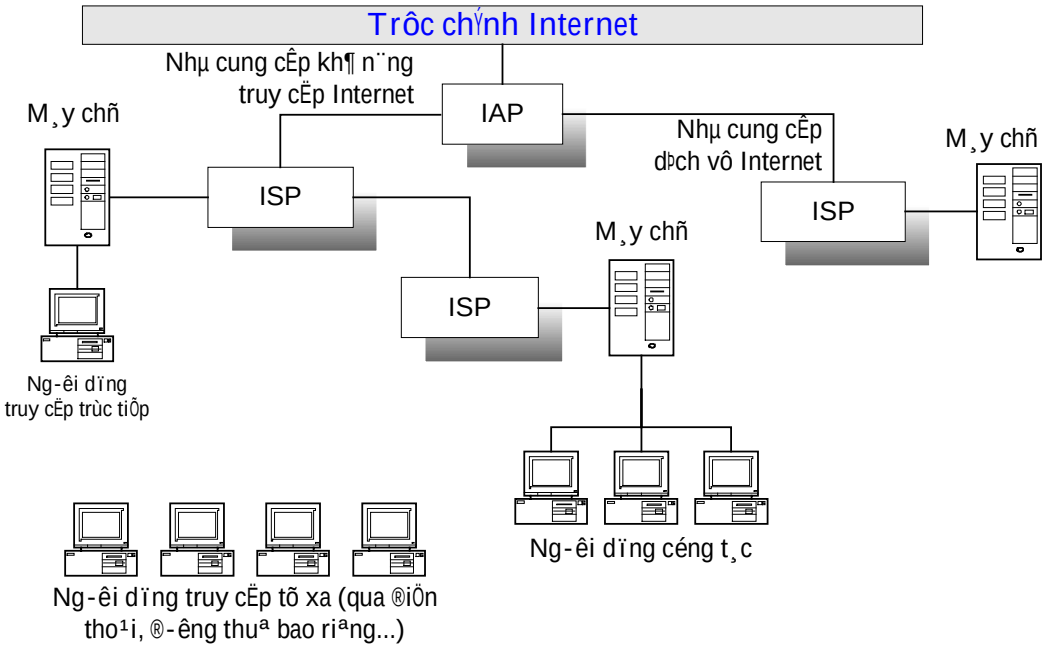



Hình 1-7. Cấu trúc của mạng Internet.

Các cổng được dùng để nối các mạng con tạo thành một mạng lớn.

Có 2 cách kết nối với Internet như sau :

- Máy con nối trong mạng LAN (hay WAN) và mạng này nối với Internet
- Máy con nối đến một trạm cung cấp dịch vụ Internet (Internet Service Provider), thông qua đó kết nối với Internet. Trong hình trên, ta có thể thấy các trạm ISP lại kết nối với Internet thông qua IAP (Internet Access Provider). Một IAP có thể làm luôn chức năng của ISP nhưng ngược lại thì không.




Hình 1-8. Sơ đồ kết nối của các trung tâm cung cấp dịch vụ (ISP)

### 1.6.3 Các kiến trúc khác

| Level | ISO | ARPANET | SNA | DECNET |
|---|---|---|---|---|
| 7 | Application | User | End User | Application |
| 6 | Presentation | Telnet, FTP | NAU Services | |
| 5 | Session | (none) | Data Flow Control | (none) |
| | | | Transmision Control | |
| 4 | Transport | Host - Host | | Network Services |
| | | SRC to DESI - IMP | Path Control | |
| 3 | Network | | | Transport |
| | | IMP - IMP | | |
| 2 | Datalink | | Data Link Control | Data Link Control |
| 1 | Physical | Physical | Physical | Physical |

ARPANET: Advanced Research Projects Agency
FTP: File Transfer Protocol
SNA: System Network Architecture cña IBM
IMP: Interface Message Procesor
NAU: Network Addressable Unit

*Chương 2*

# TẦNG VẬT LÝ

Nhiệm vụ của tầng vật lý là chuyển các bit tin từ máy này đến máy kia. Tốc độ truyền tin phụ thuộc vào môi trường truyền tin. Tín hiệu truyền có thể ở dạng tương tự (*analog*) hoặc ở dạng số (*digital*). Hướng phát triển hiện nay :

- Truyền tin bằng cáp quang, bằng vệ tinh.
- Hệ thống nối nhanh (Fast - Connect), hệ thống chuyển mạch gói
- Mạng thông tin số đa dịch vụ (Integrated Services Digital Network)

## 2.1 Môi trường truyền tin

### 2.1.1 Phương tiện truyền

Mục đích lắp đặt cáp là đảm bảo dung lượng (tốc độ) cần thiết cho các nhu cầu truyền thông trong mạng. Hệ thống cáp cần phải ổn định. Để đạt được mục tiêu này, người quản trị mạng phải cân đối bốn yếu tố sau:

- Tốc độ truyền lớn nhất của hệ thống cáp hiện hành, khả năng nâng cấp.
- Nhu cầu về tốc độ truyền thông trong vòng 5-10 năm tới là bao nhiêu.
- Chọn trong số những loại cáp đang có trên thị trường.
- Chi phí để lắp đặt thêm cáp dự phòng.

Việc kết nối vật lý một máy tính vào mạng được thực hiện bằng cách cắm một card giao tiếp mạng NIC (Network Interface Card) vào khe cắm của máy tính và nối với cáp mạng. Sau khi kết nối vật lý đã hoàn tất, quản lý việc truyền tin giữa các trạm trên mạng tuỳ thuộc vào phần mềm mạng.

NIC sẽ chuyển gói tín hiệu vào mạng LAN, gói tín hiệu được truyền đi như một dòng các bit dữ liệu thể hiện bằng các biến thiên tín hiệu điện. Khi nó chạy trong cáp dùng chung, mọi trạm gắn với cáp đều nhận được tín hiệu này, NIC ở mỗi trạm sẽ kiểm tra địa chỉ đích trong tín hiệu đầu của gói để xác định đúng địa chỉ đến, khi gói tín hiệu đi tới trạm có địa chỉ cần đến, đích ở trạm đó sẽ sao gói tín hiệu rồi lấy dữ liệu ra khỏi khung tin và đưa vào máy tính.

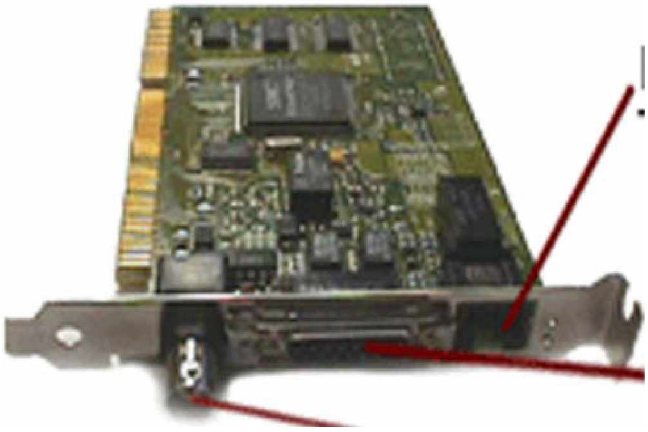
Có hai kỹ thuật truyền tín hiệu đã mã hóa lên mạng : Truyền ở dải tần gốc (baseband) và truyền ở dải tần rộng (broadband).

Đặc tính của cáp bao gồm sự nhạy cảm với nhiễu của điện, độ mềm dẻo, khả năng uốn nắn để lắp đặt, cự ly truyền dữ liệu, tốc độ truyền (Mbit/s). Hiện nay, tốc độ truyền dữ liệu trên các loại cáp biến động từ 10Mbit/s đến 100Mbit/s và hơn nữa.

Có 3 nhóm cáp chính được dùng để nối hầu hết các mạng :

- Cáp đồng trục (Coaxial)
- Cáp xoắn đôi (Twisted-Pair) : gồm có cáp xoắn đôi trần (Unshielded Twisted-Pair) và cáp xoắn đôi có bọc (Shielded Twisted-Pair).
- Cáp sợi quang (Fiber-Optic)

### *2.1.1.1 Card mạng*



Hình 2-1. Card mạng (NIC)

Card mạng còn được gọi là card giao tiếp mạng NIC (Network Interface Card) được lắp đặt trong mỗi máy tính trong mạng cục bộ, Card này có nhiệm vụ chuyển dữ liệu từ máy tính vào cáp mạng và ngược lại. Quá trình này chính là sự chuyển đổi từ tín hiệu số của máy tính thành các tín hiệu điện hay quang được truyền dẫn trên cáp mạng. Đồng thời nó cũng thực hiện chức năng tổ hợp dữ liệu thành các gói và xác định nguồn và đích của gói.

- Các loại đầu nối cho card mạng :

Một vài loại card mạng có nhiều đầu nối để nối với cáp mạng, để xác định đầu nào dùng ta có thể thay đổi các jump hay công tắc chuyển DIP ngay trên card mạng hoặc sử dụng phần mềm.

- Mạng thin Ethernet sử dụng các đầu nối cáp đồng trục BNC (British Naval Connector)
- Mạng thicknet dùng giắc nối AUI 15 chân để cắm vào đầu DB15 của card mạng.
- Mạng Ethernet twisted-pair (10 Base T) sử dụng đầu nối RJ45.

### *2.1.1.2 Cáp đồng trục*

Cáp đồng trục được chế tạo gồm một dây đồng ở giữa chất cách điện, chung quanh chất cách điện được quán bằng dây bện kim loại dùng làm dây đất. Giữa dây đồng dẫn điện và dây đất có một lớp cách ly, ngoài cùng là một vỏ bọc bảo vệ.

Cáp đồng trục có hai loại : loại nhỏ (Thin) và loại to (Thick). Dây cáp đồng trục loại nhỏ được thiết kế để truyền tin cho băng tần cơ bản (Base Band) hoặc băng tần rộng (broadband). Dây cáp loại to dùng cho đường xa, dây cáp nhỏ dùng cho đường gần, tốc độ truyền tin qua cáp đồng trục có thể đạt tới 35 Mbit/s.

#### *2.1.1.3 Cáp dây xoắn (Twisted Pair)*

Cáp xoắn gồm hai sợi dây đồng được xoắn cách điện với nhau. Nhiều đôi dây cáp xoắn gộp với nhau và được bọc chung bởi vỏ cáp hình thành cáp nhiều sợi. Cáp này có đặc tính dễ bị ảnh hưởng của nhiễu điện nên chỉ truyền dữ liệu ở cự ly khoảng 100m (khoảng 328 feet). Cáp xoắn đôi có hai loại: cáp xoắn đôi không bọc (UTP) và cáp xoắn đôi có bọc (STP).

Cáp xoắn thường được dùng trong hệ thống điện thoại để truyền tín hiệu tương tự (analog) cũng như tín hiệu số (digital). Trong khoảng cách vài km thì không cần bộ khuyếch đại và có tốc độ ở mức megabit/giây.

#### *2.1.1.4 Cáp quang (Fiber Optics)*

Khi các tín hiệu số được điều chế thành các tín hiệu xung ánh sánh thì được truyền tải qua cáp quang. Cáp sợi quang bao gồm một sợi thuỷ tinh cực mảnh gọi là lõi (core), được bao bọc bởi một lớp thuỷ tinh đồng tâm gọi là lớp vỏ bọc hay còn gọi là lớp phủ (cladding). Đôi khi các sợi được làm bằng chất dẻo. Chất dẻo dễ lắp đặt hơn nhưng không thể mang xung ánh sáng đi xa như thuỷ tinh.

Mỗi sợi thuỷ tinh chỉ truyền tín hiệu theo một hướng nhất định, do đó cáp có 2 sợi nằm trong vỏ bọc riêng biệt : một sợi truyền và một sợi nhận. Cáp sợi quang có thể truyền tín hiệu đi xa hơn với tốc độ cực nhanh (theo lý thuyết cáp quang có thể truyền tín hiệu với tốc độ tối đa 200.000Mbit/s).

Cáp quang có dải thông lớn hơn cáp đồng, ưu điểm mạnh của cáp quang là khoảng cách truyền dẫn lớn, giá rẻ, dung lượng truyền cao.

#### *2.1.1.5 Vệ tinh thông tin*

Vệ tinh truyền thông (communication satellites) nhận thông tin mặt đất, khuyếch đại tín hiệu thu được và phát lại xuống mặt đất ở tần số khác để tránh giao thoa (interference) với tín hiệu thu được. Các vệ tinh có vai trò như những trạm lặp tin giữa các trạm mặt đất với nhau. Một vệ tinh đều phủ sóng rất rộng và có thể có nhiều trạm mặt đất, thường hoạt động ở tần số 12 - 14Ghz. Truyền tin qua vệ tinh có dãi truyền rất rộng, do đó những khoảng cách xa (hàng trăm km) được bảo đảm chất lượng tin. Ngoài ra giá của truyền vệ tinh đang giảm nhanh.

Uỷ ban kỹ thuật điện tử (IEEE) đề nghị dùng các tên sau đây để chỉ 3 loại dây cáp dùng với mạng Ethernet chuẩn 802.3 :

1. Dây cáp đồng trục sợi to (thick coax) gọi là 10BASE5, có tốc độ 10 Mbps, tần số cơ sở, ≤ 500m.

2. Dây cáp đồng trục sợi nhỏ (thin coax) gọi là 10BASE2, có tốc độ 10 Mbps, tần số cơ sở, ≤ 200m.
3. Dây cáp đôi xoắn không vỏ bọc (twisted pair) gọi là 10BASET, có tốc độ 10 Mbps, tần số cơ sở, sử dụng cáp sợi xoắn.
4. Dây cáp quang (Fiber Optic Inter-Repeater Link) gọi là FOIRL .

### 2.1.2 Các thông số cơ bản của môi trường truyền tin

#### *2.1.2.1 Độ suy giảm*

Tín hiệu trên đường dây bị suy giảm trong quá trình truyền tin. Để khắc phục ta dùng các bộ khuyếch đại (amplifiers). Độ suy giảm được tính bằng đơn vị decibel. Nếu điện thế ban đầu là $V_1$ và sau đó giảm xuống $V_2$ thì số decibel của độ suy giảm được định nghĩa như sau:

$$\mathrm{S\,(decibel)} = 20\log_{10}\frac{V_1}{V_2}$$

#### *2.1.2.2 Độ nhiễu*

Điện từ trường trong môi trường truyền tin gây nhiễu cho các tín hiệu mang thông tin. Để khắc phục ta dùng các bộ lọc nhiễu (*filters*). Để đặc trưng độ nhiễu trên đường dây, ta dùng tỉ số tần số tín hiệu/tạp âm (Signal/Noise - S/N) :

$$SN(decibel) = 10\log_{10}\frac{S}{N} \quad (S: Signal;\ \ N: Noise)$$

#### *2.1.2.3 Tốc độ truyền*

$$C = B\log_2\left(1+\frac{S}{N}\right) bit/s$$

Trong đó B là độ rộng dải tần tính bằng Hz. C là tốc độ tính bằng bit/giây (b/s). Nếu mạng điện thoại có dải tần 3000Hz, tỉ số S/N = 20dB thì tốc độ truyền cực đại là :

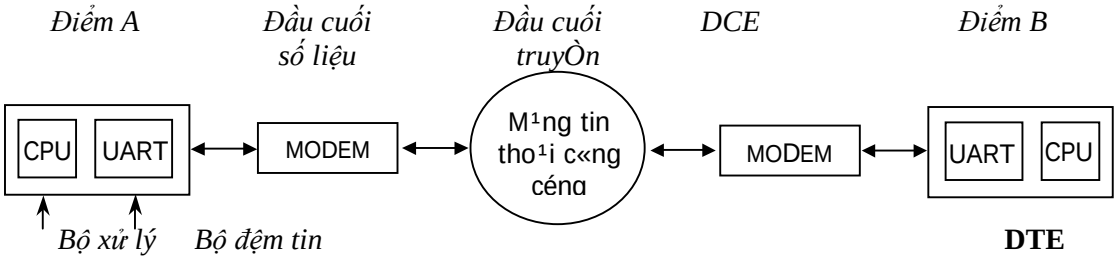
$$\frac{S}{N} = 10\log_{10}\frac{S}{N} = 20 \rightarrow \frac{S}{N} = 100 \qquad C = B\log_2\left(1+\frac{S}{N}\right) = 3000\times\log_2(1+100) = 19963b/s$$

Các tín hiệu trên kênh truyền có thể là tín hiệu tương tự hoặc tín hiệu số và tương ứng sẽ tạo thành kênh tương tự hoặc kênh số.

## 2.2 Chuẩn giao diện

### 2.2.1 Modem

Modem là bộ điều chế và giải điều chế biến đổi các tín hiệu số thành các tín hiệu tương tự và ngược lại trên mạng điện thoại.




Hình 2-2. Sơ đồ truyền tin giữa hai điểm A và B.

Tín hiệu số từ máy tính đến modem, được modem biến đổi thành tín hiệu tương tự để có thể đi qua mạng điện thoại. Tín hiệu này đến modem ở điểm B được biến đổi ngược lại thành tín hiệu số đưa vào máy tính ở B.

Các kỹ thuật điều chế cơ bản là điều chế biên độ AM, điều chế tần số FM, điều chế pha PM .

- Điều chế biên độ : Các tín hiệu 1 và 0 được phân biệt bởi biên độ, còn tần số của tín hiệu là giống nhau. Điều chế biên độ để thực hiện nhưng dễ bị nhiễu.
- Điều chế tần số : Các tín hiệu 1 và 0 được phân biệt bởi tần số, còn biên độ các tín hiệu giống nhau.

  Kỹ thuật điều tần phức tạp hơn nhưng tính chống nhiễu cao.
- Điều chế theo pha : Các tín hiệu 1 và 0 được phân biệt bởi các pha của dao động, còn biên độ và tần số của các tín hiệu giống nhau. Điều pha cũng phức tạp nhưng ít bị nhiễu.

Để tăng tốc độ truyền tin người ta kết hợp điều pha với điều biên gọi là điều pha biên.

Hiện nay có rất nhiều loại modem hiện đại từ loại thấp: 300, 600, 1200, 2400 bit/s, đến loại 9600 bit/s. Với tốc độ truyền tương đối cao trên đường truyền băng hẹp (băng thoại) nên đòi hỏi những phương pháp điều biên phức tạp.

Các *phương thức truyền dữ liệu* giữa hai điểm có thể là:

- Một chiều đơn (simplex)
- Hai chiều luân phiên (half - duplex)
- Hai chiều đầy đủ (duplex)

Truyền một chiều đơn chỉ cho phép truyền một hướng. Truyền hai chiều luân phiên cho phép truyền hai hướng, nhưng mỗi thời điểm chỉ có một hướng được truyền, sau đó phải thực hiện chuyển mạch để truyền ngược lại. Truyền hai chiều đầy đủ có thể nhận hoặc phát cùng một lúc. Các modem hiện nay đều có thể hoạt động ở hai chế độ bán song công và song công.

### 2.2.2 DTE và DCE

Trước khi nghiên cứu các chuẩn cho giao diện tầng Vật lý, chúng ta có hai khái niệm mới : đó là DTE và DCE.

- DTE (Data Terminal Equipment - Đầu cuối số liệu) : là khái niệm được sử dụng để chỉ các máy mà người sử dụng bình thường thao tác trực tiếp lên đó. Các máy này có thể là máy tính hay trạm cuối.
- DCE (Data Communication Equipment - Đầu cuối truyền) : là khái niệm chỉ các thiết bị cuối kênh dữ liệu có chức năng nối các DTE với các đường truyền vật lý và chuyển đổi dữ liệu. DCE có thể là các Modem, Tranducer, Multiplexer...

ISO qui định các chuẩn quy ước phương thức ghép nối giữa đầu cuối số liệu DTE và đầu cuối truyền DCE.

### 2.2.3 Chuẩn RS-232C

Đầu những năm 50, chuẩn RS-232(Recommended Standard 232C, của EIA) được phát triển để truyền tin giữa các thiết bị đầu cuối dữ liệu. Chuẩn này hiện nay đang được sử dụng, nó chính là các cổng COM1, COM2 trên các máy PC.

- *Phần cơ học :* là một bộ có 25 chân độ rộng tính ở giữa là 47,05mm ± 13 hàng trên đánh số 1 ÷ 13 (trái qua phải) hàng dưới 14 ÷ 25 (trái qua phải).
- *Phần điện :* gồm qui ước logic 1 <-3V và logic 0 >+ 3V.

  Tốc độ truyền cho phép 20 *kbps* qua dây cáp 15m (thường là 9,6 *kbps*)

Từ năm 1987, RS-232-C đã được sửa đổi và đặt tên lại là EIA-232-D. Ngoài ra còn có một số chuẩn mở rộng khác như RS-422-A, RS-423-A RS-449, các khuyến nghị loại X của CCITT như X21. . .. Mặc dầu RS-232-C vẫn là chuẩn thông dụng nhất cho giao diện DTE/DCE nhưng các chuẩn mới nói trên được áp dụng phổ biến hiện nay.

Đối với các máy tính, thông thường người ta sử dụng hai cổng COM1, COM2 để *kết nối trực tiếp*. Cổng COM1 có địa chỉ vào/ra là 3F8_3FF hex và ngắt là IRQ4, cổng COM2 có địa chỉ vào/ra là 2F8_2FF hex và ngắt là IRQ3. Các chân cắm của hai cổng cũng được chuẩn hóa để tiện lợi hơn cho việc sử dụng.

*Chương 3*

# TẦNG LIÊN KẾT DỮ LIỆU

## 3.1 Chức năng

Tầng liên kết dữ liệu thực hiện các công việc chính như sau :

- Định danh các thiết bị trên mạng, cấu hình logic của mạng.
- Điều khiển luồng dữ liệu và việc truy nhập ở tầng vật lý.
- Phát hiện và chỉnh sửa các lỗi xuất hiện trong quá trình truyền dữ liệu.

Chức năng chính của tầng LKDL là tách rời các khung thành các bít để truyền đi và kiến tạo các khung (frames) từ các dòng bít nhận được.

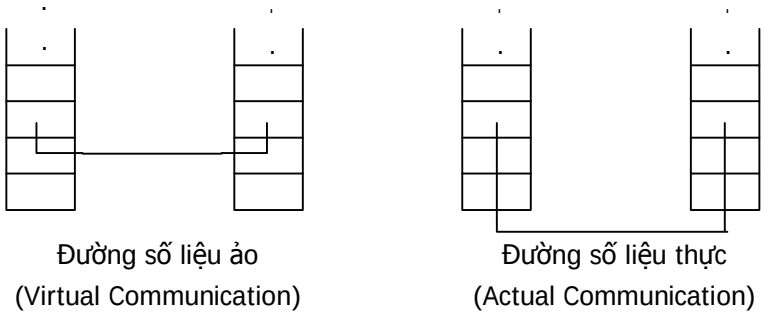
Tầng LKDL nghiên cứu các thuật toán thực hiện thông tin hiệu suất, tin cậy giữa hai máy cạnh nhau ở tầng 2. Đưa ra các thủ tục truyền tin có lưu ý đến lỗi có thể xẩy ra do nhiễu trên đường dây, sự trễ do lan truyền.

Thông thường, tầng LKDL có liên quan đến nhiễu của tín hiệu của phương tiện truyền vật lý, cho dù là truyền qua dây đồng, cáp quang hay truyền thông qua sóng ngắn. Nhiễu là một vấn đề rất thông thường và có thể do rất nhiều nguồn khác nhau, trong đó có cả nhiễu của các tia vũ trụ, nhiễu do tạp âm của khí quyển và từ các nguồn khác nhau.

## 3.2 Các vấn đề của tầng liên kết dữ liệu

### 3.2.1 Cung cấp dịch vụ cho tầng mạng

Tầng 2 chuyển dữ liệu từ mức 3 ở máy nguồn tới mức 3 ở máy nhận.




Hình 3-1. đường truyền dữ liệu trong tầng LKDL.

Các dịch vụ tầng 2 có thể là:

1. Dịch vụ không kết nối, không biên nhận (*Unacknowledged Connectionless Service*)
2. Dịch vụ không kết nối, có biên nhận (*Acknowledged Connectionless Service*)
3. Dịch vụ có kết nối (*Connection Oriented Service*)

Dịch vụ kết nối có hướng có 3 giai đoạn: *kết nối, truyền số liệu, tách bỏ liên kết* (kết thúc) : CONNECT, DATA, DISCONNECT. Truyền tin giữa 2 tầng kề nhau dùng các hàm dịch vụ nguyên thủy (request, indication, response và confirm).

Dịch vụ không kết nối được thể hiện bằng một bước duy nhất là truyền tin, không cần thiết lập liên kết logic. Các đơn vị dữ liệu truyền độc lập với nhau.

### 3.2.2 Khung tin - Nhận biết gói tin

Để cung cấp dịch vụ cho tầng mạng, tầng LKDL phải dùng dịch vụ được cung cấp từ tầng Vật lý. Tầng Vật lý tiếp nhận dòng bít và giao cho nơi nhận. Dòng bit này có thể có lỗi. Tầng LKDL sẽ kiểm tra và nếu cần sẽ sửa lỗi.

Tầng LKDL tách dòng bit thành các khung tin (frame) và tính thông số kiểm tra tổng (checksum) cho mỗi khung tin này, nếu kết quả tính được khác với checksum chứa trong khung tin, nghĩa là có lỗi và khi đó lỗi sẽ được thông báo cho nơi gửi.

Muốn tách các khung tin, có thể chèn các đoạn phân cách (timegaps) vào giữa các khung tin, giống như khoảng trống (*space*) giữa các từ trong văn bản. Nhưng điều này khó thực hiện nên người ta thường dùng các phương pháp sau :

- Đếm số ký tự : Hiện nay ít được dùng, vì từ đếm cũng bị lỗi khi truyền.
- Dùng ký tự bắt đầu (STX) và kết thúc (ETX) với ký tự đệm (DLE).
- Dùng các cờ (*flags*) đánh dấu bắt đầu và kết thúc với các bit đệm.

### 3.2.3 Kiểm tra lỗi

Các cách để kiểm tra lỗi trong quá trình truyền :

- Dùng thông số trả lời có biên nhận (ACK) hoặc không biên nhận (NAK) để biết đã nhận đúng bản tin hay phải phát lại.
- Dùng bộ định thời gian, nếu quá thời gian quy định không có trả lời nghĩa là bản tin chưa nhận được.
- Dùng phương pháp đánh số thứ tự các khung tin (frame) được gửi đi.

Quá trình kiểm tra lỗi đồng thời với quản lý thời gian và số thứ tự của các khung tin nhằm bảo đảm mỗi khung tin chỉ nhận được một lần duy nhất. Đây là chức năng quan trọng của tầng LKDL.

### 3.2.4 Điều khiển luồng dữ liệu

Trong quá trình truyền dữ liệu, nếu tốc độ bên phát nhanh hơn bên thu thì xảy ra hiện tượng mất tin do không nhận kịp. Vì vậy cần phải điều khiển luồng truyền

(*flow control* ) để quá trình thu phát được phối hợp nhịp nhàng và đồng bộ với nhau. Chức năng có tại một vài cấp giao thức, kể cả tầng con LLC.

Các giao thức phải chứa các quy tắc xác định rõ khi nào nơi gởi có thể phát các khung tin kế tiếp.

### 3.2.5 Quản lý liên kết

Một chức năng khác của tầng LKDL là quản lý các kết nối như tách, nối, đánh số khung tin, bắt đầu lại khi lỗi, quản lý các thiết bị đầu cuối thứ cấp hoặc sơ cấp bằng khung tin thăm dò (poll).

### 3.2.6 Nén dữ liệu khi truyền

Nén dữ liệu là một vấn đề quan trọng đơn vị việc truyền dữ liệu trên mạng. Về cơ bản, nén dữ liệu là ép chúng lại để đỡ tốn chỗ khi lưu trữ trên đĩa và đỡ tốn thời gian khi truyền trên đường dây. Thực tế, các dữ liệu số chứa nhiều đoạn lặp đi lặp lại, nén dữ liệu sẽ thay thế các thông tin lặp lại bằng một ký hiệu hoặc một đoạn mã để rút ngắn độ dài của tập tin. Các kỹ thuật nén dữ liệu cơ sở bao gồm :

- *Null compression* : Thay thế một dãy các dấu cách bằng một mã nén và một giá trị số lượng các dấu cách.
- *Run-length compression* : Mở rộng kỹ thuật trên bằng cách nén bất kỳ một dãy nào có từ 4 ký tự lặp. Các ký tự này được thay thế bằng một mã nén, là một trong các ký tự này, và một giá trị bằng đúng số lần lặp.
- *Keyword encoding* : Tạo ra một bảng mã cho các từ hoặc các cặp ký tự thường xuyên xuất hiện và thay thế.
- *Phương pháp thống kê Huffman* : Kỹ thuật nén này giả thiết rằng sự phân bố của các ký tự trong dữ liệu là không đồng nhất. Tức là một số ký tự xuất hiện nhiều hơn các ký tự khác. Ký tự nào càng xuất hiện nhiều thì càng ít tốn bit để mã hóa nó. Một bảng được tạo ra để ghi lại lược đồ mã hóa và bảng này có thể chuyển cho modem nhận để nó biến đổi trở lại các ký tự đã mã hóa.
- Ngoài ra còn một thuật toán nén nữa được gọi là nén ngẫu nhiên. Thuật toán này được sử dụng trong một chuẩn nén dữ liệu V.24bits

## 3.3 Phát hiện và hiệu chỉnh lỗi

Trong khi truyền đi một byte trong hệ thống máy tính thì khả năng xảy ra một lỗi do hỏng hóc ở phần nào đó hoặc do nhiễu gây nên là khá lớn. Các kênh vào-ra thường xẩy ra nhiều lỗi, đặc biệt là khi truyền số liệu. Phần lớn các hệ thống đều có các phương pháp phát hiện và sau đó sửa lỗi. Quá trình sửa lỗi thường khó hơn rất nhiều so với phát hiện lỗi. Có thể chia phương pháp xử lý lỗi ra làm hai nhóm:

- Phát hiện lỗi và thông báo cho bên phát biết để phát lại tin.
- Phát hiện lỗi và tự sửa.

### 3.3.1 Phương pháp bit chẵn lẻ (Parity)

Đây là phương pháp thường dùng nhất để phát hiện lỗi. Bằng cách thêm 1 bit (được gọi là bit chẵn lẻ) vào từ nhị phân phụ thuộc vào tổng số các bit 1 trong một từ là một số chẵn hay lẻ, và nhờ vào phép toán logic XOR, ta sẽ biết được bit thêm vào đó là bit chẵn hay bit lẻ.

Mạch kiểm tra sẽ xác định các số bit 1 có đúng tính chẵn lẻ hay không. Phương pháp tương đối đơn giản và có hai cách như sau :

- Kiểm tra ngang (VRC - Vertical Redundancy Checking) : Thêm một bit chẵn lẻ vào mỗi byte để phát hiện lỗi. Cách này làm mất đi khoảng 12,5% dung lượng bản tin. Để khắc phục ta có thể dùng phép kiểm tra tổng các byte.
- Kiểm tra dọc (LRC - Longitudinal Redundancy Checking) : lỗi được phát hiện trong các khối byte thay cho việc tìm lỗi trong từng byte. Trong phương pháp này người ta thêm mỗi khối *1 byte ở cuối*, byte này mang các thông tin về tính chất đặc thù của khối (Characteristic Redundancy Checking - CRC). Byte này đơn giản có thể tính bằng phép logic XOR của tất cả các byte trong khối hoặc tính theo đa thức chuẩn để được FCS.

  *Ví dụ :*

| Vị trí bit trong ký tự | Khối ký tự truyền đi | | | | | LRC |
|---|---|---|---|---|---|---|
| | A | S | C | I | I | |
| 0 | 1 | 1 | 1 | 1 | 1 | 1 |
| 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| 2 | 0 | 1 | 0 | 0 | 0 | 1 |
| 3 | 0 | 0 | 0 | 1 | 1 | 0 |
| 4 | 0 | 0 | 0 | 0 | 0 | 0 |
| 5 | 0 | 1 | 1 | 0 | 0 | 0 |
| 6 | 1 | 1 | 1 | 1 | 1 | 1 |
| VRC | 0 | 0 | 1 | 1 | 1 | 1 |

Kiểm soát lỗi 2 chiều : VRC-LRC.

Bên nhận sẽ kiểm tra parity theo cả hai chiều để phát hiện và định vị lỗi cho từng ký tự. ( $1 \oplus 1 = 0$ $0 \oplus 0 = 0$ $1 \oplus 0 = 0$ $0 \oplus 1 = 1$ )

### 3.3.2 Tính theo đa thức chuẩn

Cách tính check sum như sau :

- Giả sử ta nhận được bản tin M(x).

- Nếu đa thức chuẩn G(x) có bậc là r, ta bổ sung thêm r bit 0 vào cuối bản tin và được m+r bit tương ứng đa thức xrM(x).
- Chia xrM(x) theo module 2 cho G(x). Kết quả ta được số dư T(x) là checksum được phát đi.

Các đa thức chuẩn thường được dùng để tính biến kiểm tra tổng là :

CRC-12 = $x^{12} + x^{11} + x^3 + x^2 + x + 1$ (dùng cho ký tự 6 bit)

CRC-16 = $x^{16} + x^{15} + x^2 + 1$ (dùng cho ký tự 8 bit)

CRC-CCTTT= $x^{16} + x^{12} x^5 + 1$ (dùng cho ký tự 8 bit)

*Ví dụ* Khung tin ban đầu 1101011011, G(x) = $x^4 + x + 1$, vậy r = 4, chuỗi bit thêm : 10011. Ta có xrM(x) = 1101011011 0000. Chia xrM(x) theo module 2 cho G(x), ta được thông số kiểm tra tổng T(x) = 1110

```
  11010'1'1011 0'00'0'
⊕ 10011
  01001 1
   10011
    0000010110
          10011
          0010100
             10011
              001110 → Số dư là 1110
```

Khung tin được truyền đi: 1101011011 1110

### 3.3.3 Mã sửa sai

Để sửa sai một bit, ta dùng tập mã Hamming dựa trên các "bit chẵn lẻ" được rải vào các bit số liệu trong từng byte theo nguyên lý cân bằng chẵn lẻ để chỉ ra các bit lỗi.

Nếu trong bản tin có k bit và số "bit chẵn lẻ" là r, thì số bit tin và "bit chẵn lẻ" phát đi sẽ là n=k+r. r bit kiểm tra luôn các vị trí 1, 2, 4, 8,..., 2r-1 và được tạo bởi cộng module 2 giá trị nhị phân của các vị trí có bit '1' của từ mã. Vì các bit kiểm tra chiếm vị trí $2^i$ với i = 0, 1, 2,..., r-1 nên độ dài cực đại của các từ mã Hamming là n $\leq 2^r - 1$ và từ dãy số cực đại của các bit tin được bảo vệ là : k $\leq (2^r - 1 - r)$. Từ đây ta xác định được r.

*Ví dụ:* Bản tin 11 bit (10101011001) được bảo vệ bởi mã Hamming.

Từ điều kiện 11 ≤ 2' - 1-r, ta cần 4 bit kiểm tra (r =4) để tạo mã Hamming (n=11+4=15)

| 1 | 0 | 1 | 0 | 1 | 0 | 1 | C | 1 | 0 | 0 | C | 1 | C | C |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |

Các bít kiểm tra C được tính như sau:

VÞ trÝ bit 1 Gi¸ trÞ nhÞ ph©n

| | |
|---|---|
| 15 | 1111 |
| 13 | 1101 |
| 11 | 1011 |
| 9 | 1001 |
| 7 | 0111 |
| | 1101 |

-> TËp m· c¸c bit kiÓm tra Hamming: 0100

Tõ m· Hamming: 10101010010011100

NÕu b¶n tin nhËn ®-îc lµ:

| 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 |

↑ bit error

| **Vị** trí bit 1 | Giá trị nhị phân |
|---|---|
| 15 | 1111 |
| 13 | 1101 |
| 9 | 1001 |
| 7 | 0111 |
| 4 | 0100 |
| 3 | 0011 |
| | 1011 (11) |

→ Vb trÝ sai ë bit 11

## 3.4 Thủ tục liên kết dữ liệu cơ bản

Để truyền tin có độ tin cậy cao ta dùng dịch vụ liên kết (Connection Oriented Service).

Ví dụ máy A gửi số liệu cho máy B, khi tầng 2 đã được nối, số liệu từ tầng 3 máy A chuyển xuống tầng 2 nhờ chương trình con “FromNetworkLayer”. Tầng 2 bổ sung phần đầu thông tin điều khiển và tính cờ kiểm tra tổng (FCS).

| Khung tin (Frame) = | Đầu tin (Header) | Thông tin (Information) | FCS |
|---|---|---|---|

Khung tin được phát sang tầng 2 máy B nhờ chương trình con ToPhysicalLayer.

Máy B đợi tin bằng chương trình con Procedure CallWait(Event). Khi khung tin tới bên nhận, máy B tính cờ kiểm tra tổng, nếu không đúng cờ sẽ báo event = CKsumErr, nếu khung tin đúng nó báo event=FrameArrival và thu nhận khung tin từ tầng Vật lý nhờ chương trình con FromPhysicalLayer.

Sau đó đầu tin chứa các thông tin điều khiển (*header*) sẽ được kiểm tra và nếu tất cả đều đúng cả, phần số liệu được chuyển lên tầng 3 nhờ chương trình con ToNetworkLayer.

- Giao thức đơn công với kênh không lỗi và không chờ : Trong giao thức này do tin chỉ truyền theo một hướng, đường kênh không có lỗi nên số liệu luôn sẵn sàng không phải chờ.
- Giao thức đơn công với kênh không lỗi và phải đợi : Bên thu bộ nhớ hạn chế và tốc độ vật lý hữu hạn, do đó bên phát phải chờ.

### 3.4.1 Giao thức đơn công với kênh có lỗi

- *Bên nhận*

Khi nào đường kênh có lỗi, bên nhận sẽ chỉ gửi tín hiệu biên nhận nếu gói tin nhận được là đúng, nếu gói tin nhận được là sai thì sẽ bị bỏ đi. Quá thời hạn qui định, bên phát sẽ gửi lại gói tin. Quá trình này lặp lại cho đến khi nhận được gói tin đúng. Trong trường hợp này, tầng 3 ở máy B không biết được gói tin bị mất hay nhận hai lần, tầng 2 phải nhận biết được điều này.

Có thể xảy ra các trường hợp :

- Tầng 3 ở máy A gửi gói tin X xuống tầng 2 của nó và phát đi.
- Máy B nhận được và trả lời bằng tín hiệu biên nhận ACK.
- Tín hiệu biên nhận bị mất trên đường đi.
- Quá thời gian qui định mà máy A không nhận được tín hiệu biên nhận, nó sẽ phát lại gói tin X. Dẫn đến máy B nhận được hai gói tin X

Để giải quyết vấn đề này người ta đánh dấu gói tin gửi đi và bên nhận gửi tín hiệu cho biết đã nhận gói tin số mấy.

- *Bên phát*

Bên phát sau khi phát gói tin, có 3 khả năng xảy ra: nhận được tín hiệu biên nhận đúng, tín hiệu biên nhận bị mất hoặc quá thời gian mà chưa nhận được trả lời. Nếu tín hiệu biên nhận đúng, máy A nhận tiếp gói tin từ tầng mạng đặt vào vùng đệm (*buffer*), xoá gói tin trước, tăng số thứ tự gói tin phát. Nếu tín hiệu biên nhận bị mất hoặc đã quá thời gian mà chưa nhận được thì phát lại gói tin với số thứ tự gói tin không thay đổi.

Bên nhận nếu nhận đúng gói tin thì tiếp nhận và chuyển đến tầng mạng và phát tín hiệu biên nhận. Nếu gói tin sai hoặc nhận 2 lần thì không được chuyển lên tầng mạng.

## 3.5 Điều khiển dòng truyền

Để tận dụng đường dây, các tín hiệu biên nhận (ACK ) được ghép cùng với gói tin. Khi gói tin đến, thay cho việc trả lời ngay tín hiệu biên nhận, bên thu nhận tiếp gói tin từ tầng mạng để ghép cùng cùng tín hiệu biên nhận và gửi trả lời. Kỹ thuật này được gọi là Piggybacking (ghép thêm).

Ưu điểm của phương pháp này là tận dụng đường kênh. Nếu quá thời gian (vài μs) mà không có gói tin mới thì bên thu cũng phải trả lời tín hiệu biên nhận để bên phát không phải phát lại gói tin cũ.

Để tận dụng đường kênh, bên phát và bên thu phải đồng bộ để bên thu kịp nhận các gói tin và bên phát cũng không lãng phí đường truyền, người ta dùng cơ chế cửa sổ trượt (sliding windows). Cửa sổ mở to thì số gói tin đưa lên đường kênh nhiều hơn(tốc độ nhanh), cửa sổ mở bé thì số gói tin đưa lên đường kênh ít lại (tốc độ chậm lại). Tương tự như cửa chắn đập nước.

### 3.5.1 Cơ chế cửa sổ

Người ta dùng số bit để đặc trưng cho độ rộng cực đại của cửa sổ. Trong thủ tục này, mỗi gói tin đi sẽ được đánh số từ 0 đến Max (Max là $2^n$ - 1) thông qua một dãy gồm các số 0, 1. Chẳng hạn cửa sổ 3 bit sẽ quản lý các gói tin có số từ 0 $\rightarrow$7. Ta có thể dùng *n* tuỳ ý.

Danh sách các gói tin gửi đi giữ trong cửa sổ phát. Danh sách các gói tin nhận được giữ trong cửa sổ nhận. Cửa sổ phát và nhận không bắt buộc phải có kích thước, giới hạn trên và dưới giống nhau.

Mặc dầu thủ tục này cho phép tầng liên kết dữ liệu linh hoạt hơn về thứ tự gởi, nhận gói tin nhưng nó yêu cầu phải đảm bảo tầng mạng đích ở bên nhận có cùng thứ tự với tầng mạng nguồn ở bên gửi.

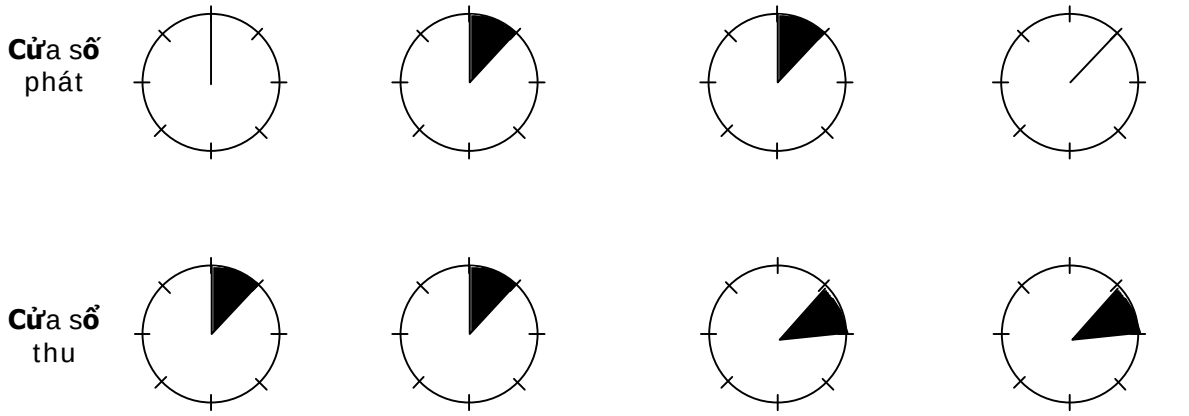
- *Cửa sổ bên phát*

Trong cửa sổ bên phát đặt các gói tin gửi đi nhưng chưa nhận được tín hiệu biên nhận. Khi nhận được gói tin mới đến từ tầng mạng để phát đi, biên trên cửa sổ tăng 1, và khi có tín hiệu biên nhận, biên dưới của cửa sổ tăng 1. Bên phát luôn giữ trong bộ nhớ các gói tin đã phát đi nhưng chưa nhận được tín hiệu biên nhận vì có thể phát lại. Như vậy nếu Max bằng n thì bên phát cần n vùng đệm để giữ các gói tin đã phát đi nhưng chưa nhận được trả lời. Nếu cửa sổ đã tới Max thì tầng liên kết dữ liệu bên phát ngừng nhận tin từ tầng 3 cho đến khi có bộ đệm tự do.

- *Cửa sổ bên nhận*

Cửa sổ bên nhận chứa các gói tin được chuyển đến. Khi gói tin có số thứ tự trùng với biên dưới của cửa sổ được nhận, cửa sổ chuyển tin lên tầng ba, phát tín hiệu biên nhận và quay một đơn vị. Không như cửa bên phát, cửa sổ bên nhận luôn duy trì cùng một kích thước. Khi kích thước cửa sổ = 1, tầng 2 nhận gói tin theo thứ tự. Nhưng nếu kích thước cửa sổ lớn hơn thì không phải như vậy.

Hoạt động của cửa sổ có kich thước là 3 bit với độ trượt 1 bit như sau :

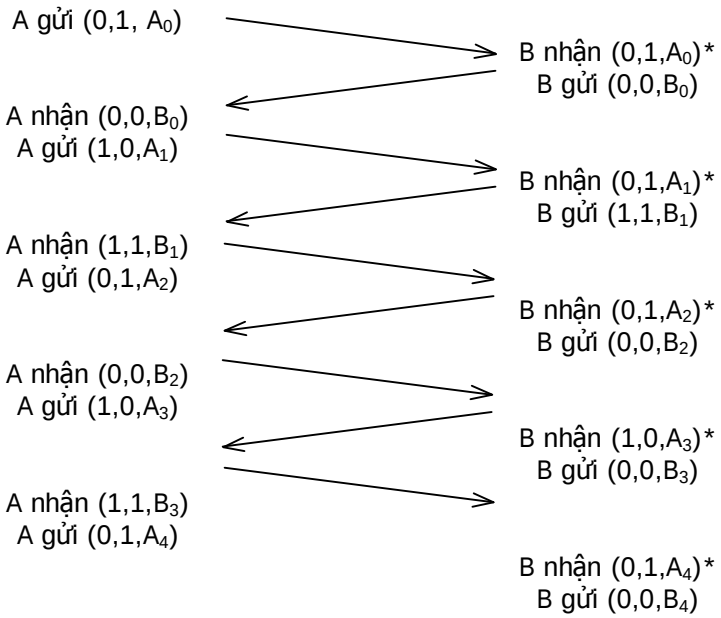



Hình 3-2. điều khiển dòng truyền theo cơ chế cửa sổ.

### 3.5.2 Trao đổi bản tin với cửa sổ 1 bit

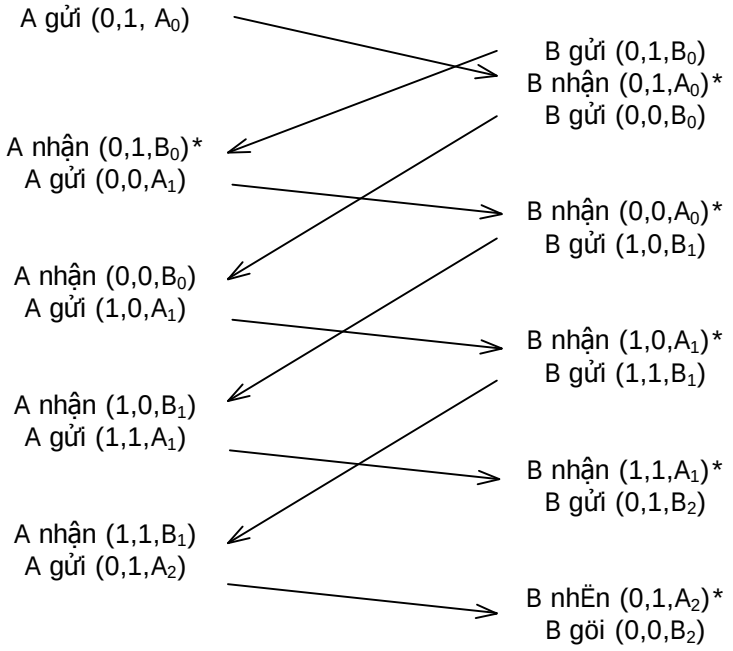
Bản tin gồn có gói tin với phần điều khiển (Header). Phần điều khiển gồm có số gói tin, số thứ tự phát *seq*, số gói tin, số thứ tự nhận là *ack*.

Trong trường hợp bình thường máy A gửi trước như sau :




Hình 3-3. Trao đổi bản tin với cửa sổ 1 bit bình thường.

Trong trường hợp bất thường máy A và B cùng gửi như sau :




Hình 3-4. Trao đổi bản tin với cửa sổ 1 bit bất thường.

Máy A ở tầng 2 nhận gói tin ở tầng 3, tạo bản tin và gửi đi. Khi bản tin này đến tầng 2 máy B, nó sẽ được kiểm tra xem có bị lặp lại không. Nếu đúng là bản tin đang mong đợi thì nó được chuyển lên tầng 3 và cửa sổ nhận dịch đi 1 nấc.

Vùng tín hiệu biên nhận chứa số bản tin cuối cùng đã được nhận mà không có lỗi. Nếu số này trùng với số bản tin vừa gửi. Bên phát sẽ lấy bản tin tiếp theo từ tầng mạng. Nếu số không đúng nó phải gửi lại bản tin cũ.

### 3.5.3 Vận chuyển liên tục

Thực tế cho ta thấy thời gian từ lúc phát gói tin đến lúc nhận trả lời biên nhận ACK là không đáng kể. Khi đó, nếu đường kênh vệ tinh có tốc độ 50Kbp/s với trễ lan truyền 500 ms, ta dùng thủ tục điều khiển dòng truyền gửi gói tin là 1000 bit qua vệ tinh. Thời gian phát gói tin là 20ms, vậy sau 520ms mới nhận được tín hiệu biên nhận trả lời. Như vậy bên phát phải chờ đến 96% thời gian (500/520), chỉ có 4% độ rộng băng được dùng đến.

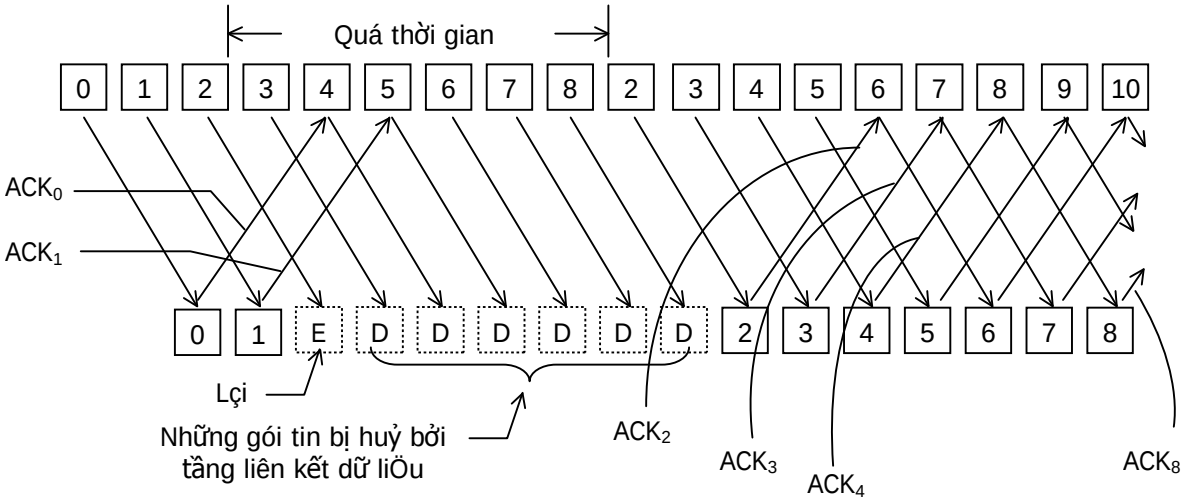
Để nâng cao hiệu suất đường truyền ta không chờ tín hiệu biên nhận mà cứ phát tiếp. Ví dụ, với thời gian phát 20ms cho một gói tin, ta sẽ gửi liên tục 26 gói tin. Như thế khi gửi hết 26 gói tin thì mất khoảng thời gian là 520 ms, đúng lúc tín hiệu biên nhận cho gói tin 0 cũng vừa đến. Kỹ thuật này gọi là Pipe-Lining (vận chuyển liên tục).

Khi có gói tin ở đoạn giữa bị hỏng thì làm thế nào ?, có bỏ những gói tin đúng đi tiếp sau nó không?. Có hai phương pháp như sau :

- Phát lại tất cả các gói tin kể từ gói tin hỏng (*go back n*)
- Phát lại chỉ riêng gói tin bị hỏng, còn gọi là phát có chọn lọc .
- Phát lại từ gói tin hỏng

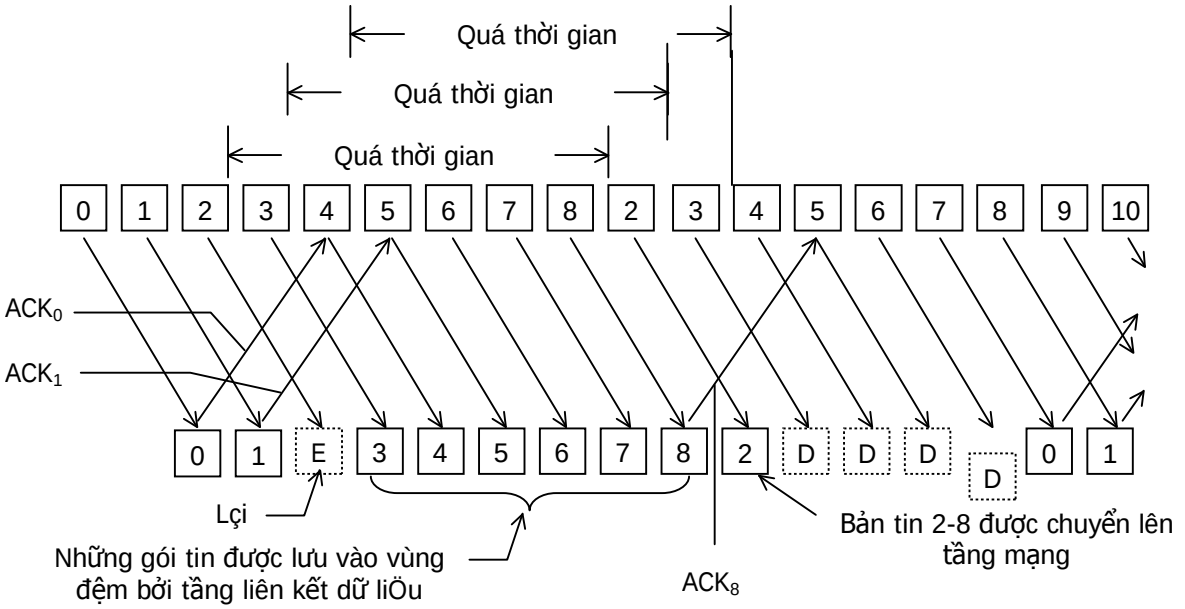
Trong trường hợp này, bên thu huỷ bỏ các gói tin tiếp theo gói tin bị hỏng. Bên phát phát lại tất cả các gói tin chưa được biên nhận bắt đầu từ gói tin bị hỏng.

Phương pháp này lãng phí đường truyền vì phải phát lại nhiều gói tin.




Hình 3-5. Cơ chế vận chuyển liên tục.

### *3.5.3.1 Phát lại có chọn läc*




Hình 3-6. Cơ chế phát bản tin có chọn lọc.

Trong phương pháp này, các gói tin nhận được có thể không theo thứ tự nhưng sẽ được sắp xếp lại để chuyển lên tầng mạng theo đúng thứ tự. Khi có gói tin bị lỗi, bên thu tiếp tục thu các gói tin đúng sau gói tin hỏng ở tầng 2. Bên phát chỉ phát lại

gói tin hỏng. Phương pháp này ứng với cửa sổ bên thu lớn hơn 1 và đòi hỏi bộ nhớ lớn để giữ các gói tin sau gói tin hỏng.

## 3.6 Các giao thức của tầng Liên kết dữ liệu

Tầng LKDL cung cấp các phương tiện để truyền thông tin qua liên kết vật lý đảm bảo tin cậy thông qua các cơ chế đồng bộ hóa, kiểm soát lỗi và kiểm soát luồng dữ liệu. Các giao thức được xây dựng cho tầng LKDL (DLP - Data Link Protocol) được phân thành hai loại :

1. Giao thức dị bộ (asynchronous DLP) : Cho phép một ký tự dữ liệu được truyền đi bất kỳ lúc nào mà không cần quan tâm đến các tính hiệu đồng bộ trước đó.
2. Giao thức đồng bộ (synchronous DLP) : Chèn các ký tự điều khiển hoặc các cờ giữa các dữ liệu của người sử dụng để báo cho bên nhận. Có hai nhóm giao thức đồng bộ :
    a. Đồng bộ hướng ký tự (character -oriented)
    b. Đồng bộ hướng bit (bit - oriented)

Các hệ thống truyền thông đòi hỏi hai mức đồng bộ hóa :

- Mức vật lý : để giữ đồng bộ giữa các đồng hồ người gửi và người nhận
- Mức LKDL : để phân biệt dữ liệu của người sử dụng với các 'cờ'và các vùng thông tin điều khiển khác

Sau đây ta xét hai loại giao thức đồng bộ là giao thức truyền tin đồng bộ nhị phân BSC (Binary Synchronous Control) và giao thức điều khiển liên kết dữ liệu mức cao HDLC (Highlevel Data Link Control).

### 3.6.1 Giao thức BSC

Đây là giao thức *hướng ký tự* (COP - Character Oriented Protocol) được xây dựng dựa trên các ký tự đặc biệt của một bộ mã chuẩn nào đó (như ASCII hoặc EBCDIC) hoạt động theo phương thức hai chiều luân phiên.

#### *3.6.1.1 Tập ký tự điều khiển*

ENQ (05): Enquire - Yêu cầu trả lời từ một trạm xa
ACK (06): Acknowledgement - Thông báo tiếp nhận tốt thông tin
NAK (15): Negative ACK - Thông báo tiếp nhận không tốt thông tin
STX (02): Start of text - Kết thúc phần Header và bắt đầu phần dữ liệu
ETX (03): End of text - Kết thúc phần dữ liệu
ETB (17): End of transmission block - Kết thúc đoạn tin (khối dữ liệu)

SOH (01): Start of heading - Bắt đầu phần header của bản tin
EOT (04): End of transmission - Kết thúc quá trình truyền tin và giải phóng liên kết
DLE (10): Data Link Escape - Để thay đổi ý nghĩa của các ký tự điều khiển truyền tin khác
SYN (16): Synchronous - Ký tự đồng bộ bản tin dùng để duy trì đồng bộ giữa 2 bên

### *3.6.1.2 Khuôn dạng tổng quát bản tin của giao thức BSC*

| SYN | SYN | SOH | Header | STX | TIN<br>Số ký tự (độ rộng 5-8 bit) | ETX/ETB | CRC |
|---|---|---|---|---|---|---|---|

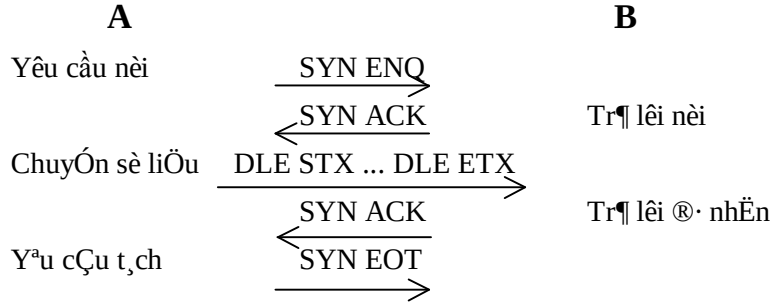
| Nơi nhận | Number Seq | Control | Biên nhận |
|---|---|---|---|

Để thông suốt bản tin, có thể dùng thêm các byte đệm :

| SYN | SYN | | DLE | DLE | | DLE | ETX/ETB | CRC |
|---|---|---|---|---|---|---|---|---|

Khi phát nếu ký tự phát trùng với DLE thì ta chèn thêm DLE. Khi thu, DLE chèn thêm sẽ được khử bỏ.

Ví dụ về thủ tục BCS




## 3.6.2 Giao thức HDLC

HDLC là giao thức hướng bit (Bit Oriented Protocol - BOP) có các phần tử của giao thức (đơn vị dữ liệu, thủ tục) được xây dựng từ các cấu trúc nhị phân (xâu bit) và khi nhận dữ liệu sẽ được tiếp nhận lần lượt từng bit một.

Đây là giao thức có vị trí quan trọng nhất, được ISO phát triển để sử dụng trong cả hai trường hợp : điểm - điểm và nhiều điểm, cho phép truyền thông hai chiều đồng thời.

### *3.6.2.1 Khuôn dạng tổng quát bản tin của giao thức HDLC*

<--- *Hướng truyền*

| | 8 bits | 8 bits | 128-1024 bytes | | |
|---|---|---|---|---|---|
| Flag | HEADER | | INFORMATION | FCS | Flag |
| 01111110 | Address | Control | Số các bit | (16 bit) | 01111110 |

*Trong đó :*

- *Flag* (01111110): là cờ dùng để nhận biết điểm bắt đầu và kết thúc bản tin.

Để tránh sự xuất hiện của mã cờ trong nội dung của bản tin, người ta cài đặt cơ chế '*cứng*' có các chức năng sau :

- Khi truyền tin cứ sau năm bit 1 liên tiếp thì thêm một bit 0 để không nhầm với Flag : 01101111111110010

  01101111011110010

  ↑ *bit chèn thêm (khi thu thì bit này sẽ được khử bỏ)*
- Khi nhận tin, nếu phát hiện có bit 0 sau 5 bit 1 liên tiếp thì tự động loại bỏ bít 0 đó đi.

- *Address* : vùng chứa địa chỉ trạm đích của khung tin.
- *Information* : vùng ghi thông tin truyền đi, có kích thước không xác định.
- *FCS (Frame Check Sequence)* : vùng để ghi mã kiểm soát lỗi (checksum) cho nội dung khung tin, dùng phương pháp CRC với đa thức sinh là CRC-CCITT = $x^{16} + x^{12} + x^5 + 1$
- *Control* : vùng định danh cho các loại khung tin khác nhau của HDLC, có ba dạng như sau :

  Dạng I : hiệu lực truyền tin tức - Information
  Dạng S : hiệu lực điều hành sự nối - Supervisor
  Dạng N : chức năng phụ của điều hành nối – Unnumbered

#### *3.6.2.2 Phương thức trao đổi thông tin*

Giao thức HDLC có 3 phương thức trao đổi thông tin chính, ứng với mỗi phướng thức có các giao thức khung tin tương ứng là SNRM, SARM hoặc SABM :

- *Phương thức trả lời chuẩn SNRM (Set Normal Response Mode):* Được sử dụng trong trường hợp cấu hình không cân bằng, có một trạm điều khiển chung (master), các trạm còn lại (slave) chỉ có thể truyền tin khi trạm chủ cho phép.
- *Phương thức trả lời dị bộ SARM (Set Asynchronous Response Mode):* Cũng được sử dụng trong trường hợp cấu hình không cân bằng như trường hợp trên, nhưng các trạm slave được phép truyền tin mà không cần sự cho phép của trạm master. Phương thức này được sử dụng trong trường hợp điểm-điểm với liên kết 2 chiều, cho phép trạm slave gửi các gói tin (frame) không đồng bộ với trạm master.

- *Phương thức trả lời dị bộ cân bằng SABM* (Set Asynchronous Balanced Mode) : Sử dụng trong trường hợp điểm-điểm, liên kết 2 chiều. Trong đó các trạm đều có vai trò tương đương.

#### *3.6.2.3 Các giao thức dẫn xuất của HDLC*

- LAP (Link Access Procedure) : tương ứng với phương thức trả lời dị bộ (ARM).
- LAPB (Link Access Protocol-Balanced) : tương ứng với phương thức trả lời dị bộ cân bằng (ABM), được dùng hầu hết trong các mạng truyền dữ liệu công cộng X25.
- LAP-D (Link Access Procedure, D Channel ) : Được xây dựng từ LAP-B và được dùng như giao thức liên kết dữ liệu cho các mạng ISDN
- SDLC, ADCCP

#### *3.6.2.4 So sánh BOP và COP*

- BOP nhận lần lượt từng bit một, do đó mềm dẻo, dễ dàng tương thích với các hệ khác nhau.
- BOP có overhead (phụ trội) ngắn, số bít bổ sung và số tín hiệu điều khiển ít do đó có tốc độ cao.
- Thủ tục điều khiển trên bit nhị phân đảm bảo không phụ thuộc mã dùng. Cách giải quyết này mềm dẻo và cho phép giải quyết vô số yêu cầu khác.
- Thủ tục HDLC được coi là chuẩn quốc tế và sẽ thông trị trong thời gian tới, nó thích ứng với các hệ thống phức tạp. Đối với các thiết bị ít phức tạp có thể dùng HDLC đơn giản hoá để đảm bảo sự tương thích với HDLC và sự phát triển mở rộng hệ thống sau này.

# BÀI TẬP

1. Tìm hiểu thêm về chuẩn giao tiếp RC232 và các chuẩn khác được phát tiển từ chuẩn này.
2. Tìm hiểu các chuẩn mở rộng của giao thức HDLC.

-

*Chương 4*

# MẠNG CỤC BỘ

Mạng cục bộ (LAN) là hệ truyền thông tốc độ cao được thiết kế để kết nối các máy tính và các thiết bị xử lý dữ liệu khác cùng hoạt động với nhau trong một khu vực địa lý nhỏ như ở một tầng của toà nhà, hoặc trong một toà nhà.... (100m đến vài km), có tốc độ truyền dữ liệu cao (có thể tới 100Mbps), tỷ lệ sai số dữ liệu nhỏ ($10^{-8}$ ->$10^{-11}$). Một số mạng LAN có thể kết nối lại với nhau trong một khu làm việc.

Mạng LAN thường bao gồm một hoặc một số máy chủ (file server, host), còn gọi là máy phục vụ) và một số máy tính khác gọi là trạm làm việc (Workstations, Client) hoặc còn gọi là nút mạng (Network Node) - một hoặc một số máy tính cùng nối vào một thiết bị nút.

## 4.1 Các cấu hình của mạng LAN

Cấu hình (topology) của mạng là cấu trúc hình học không gian mà thực chất là cách bố trí phần tử của mạng cũng như cách nối giữa chúng với nhau. Thông thường mạng có 3 dạng cấu trúc là: Mạng dạng hình sao (Star Topology), mạng dạng vòng (Ring Topology) và mạng dạng tuyến (Linear Bus Topology). Ngoài 3 dạng cấu hình kể trên còn có một số dạng khác biến tướng từ 3 dạng này như mạng dạng cây, mạng dạng hình sao - vòng, mạng hỗn hợp,v.v....

### 4.1.1 Mạng dạng hình sao (Star Topology)

Mạng dạng hình sao bao gồm một trung tâm và các nút thông tin. Các nút thông tin là các trạm đầu cuối, các máy tính và các thiết bị khác của mạng. Trung tâm của mạng điều phối mọi hoạt động trong mạng với các chức năng cơ bản là:

- Xác định cặp địa chỉ gửi và nhận được phép chiếm tuyến thông tin và liên lạc với nhau.
- Cho phép theo dõi và xử lý sai trong quá trình trao đổi thông tin.
- Thông báo các trạng thái của mạng...

Ưu điểm :

- Hoạt động theo nguyên lý nối song song nên nếu có một thiết bị nào đó ở một nút thông tin bị hỏng thì mạng vẫn hoạt động bình thường.
- Cấu trúc mạng đơn giản và các thuật toán điều khiển ổn định.
- Mạng có thể mở rộng hoặc thu hẹp tuỳ theo yêu cầu của người sử dụng.

Nhược điểm:

- Khả năng mở rộng mạng hoàn toàn phụ thuộc vào khả năng của trung tâm. Khi trung tâm có sự cố thì toàn mạng ngừng hoạt động.

- Mạng yêu cầu nối độc lập riêng rẽ từng thiết bị ở các nút thông tin đến trung tâm. Khoảng cách từ máy đến trung tâm rất hạn chế (100 m).

Nhìn chung, mạng dạng hình sao cho phép nối các máy tính vào một bộ tập trung (HUB) bằng cáp xoắn, giải pháp này cho phép nối trực tiếp máy tính với HUB không cần thông qua trục BUS, tránh được các yếu tố gây tắc nghẽn mạng. Gần đây, cùng với sự phát triển switching hub, mô hình này ngày càng trở nên phổ biến và chiếm đa số các mạng mới lắp.

### 4.1.2 Mạng hình tuyến (Bus Topology)

Theo cách bố trí hành lang các đường như hình vẽ thì máy chủ (host) cũng như tất cả các máy tính khác (workstation) hoặc các nút (node) đều được nối về với nhau trên một trục đường dây cáp chính để chuyển tải tín hiệu.

Tất cả các nút đều sử dụng chung đường dây cáp chính này. Phía hai đầu dây cáp được bịt bởi một thiết bị gọi là terminator. Các tín hiệu và gói dữ liệu (packet) khi di chuyển lên hoặc xuống trong dây cáp đều mang theo địa chỉ của nơi đến.

Loại hình mạng này dùng dây cáp ít nhất, dễ lắp đặt. Tuy vậy cũng có những bất lợi đó là sẽ có sự ùn tắc giao thông khi di chuyển dữ liệu với lưu lượng lớn và khi có sự hỏng hóc ở đoạn nào đó thì rất khó phát hiện, một sự ngừng trên đường dây để sửa chữa sẽ ngừng toàn bộ hệ thống.

### 4.1.3 Mạng dạng vòng (Ring Topology)

Mạng được bố trí theo dạng vòng tròn, đường dây cáp được thiết kế làm thành một vòng khép kín, tín hiệu chạy quanh theo một chiều nào đó. Các nút truyền tín hiệu cho nhau mỗi thời điểm chỉ được một nút mà thôi. Dữ liệu truyền đi phải có kèm theo địa chỉ cụ thể của mỗi trạm tiếp nhận.

Mạng Token Ring có thể chạy ở tốc độ 4Mbps hoặc 16Mbps. Phương pháp truy cập dùng trong mạng Token Ring gọi là Token passing. Token passing là phương pháp truy nhập xác định, trong đó các xung đột được ngăn ngừa bằng cách ở mỗi thời điểm chỉ một trạm có thể được truyền tín hiệu. Điều này được thực hiện bằng việc truyền một bó tín hiệu đặc biệt gọi là Token (mã thông báo) xoay vòng từ trạm này qua trạm khác. Một trạm chỉ có thể gửi đi bó dữ liệu khi nó nhận được Token, khi đó nó sẽ chiếm được quyền ưu tiên hoạt động trên mạng.

Mạng dạng vòng có thuận lợi là có thể nới rộng ra xa, tổng đường dây cần thiết ít hơn so với hai kiểu trên. Nhược điểm là đường dây phải khép kín, nếu bị ngắt ở một nơi nào đó thì toàn bộ hệ thống cũng bị ngừng.

### 4.1.4 Mạng dạng kết hợp

#### *4.1.4.1 Kết hợp hình sao và tuyến (star/Bus Topology)*

Cấu hình mạng dạng này có bộ phận tách tín hiệu (spitter) giữ vai trò thiết bị trung tâm, hệ thống dây cáp mạng có thể chọn hoặc Ring Topology hoặc Linear Bus Topology.

Ưu điểm của cấu hình này là mạng có thể gồm nhiều nhóm làm việc ở cách xa nhau, ARCNET là mạng dạng kết hợp Star/Bus Topology. Cấu hình dạng này đưa lại sự uyển chuyển trong việc bố trí đường dây tương thích dễ dàng đối với bất cứ toà nhà nào.

#### 4.1.4.2 Kết hợp hình Sao và Vòng (Star/Ring Topology)

Cấu hình dạng kết hợp Star/Ring Topology, có một "thẻ bài" (token) được chuyển vòng quanh một cái HUB trung tâm. Mỗi trạm làm việc được nối với HUB - là cầu nối giữa các trạm làm việc và để tăng khoảng cách cần thiết.

Một hub thông thường có nhiều cổng nối với người sử dụng để gắn máy tính và các thiết bị ngoại vi. Mỗi cổng hỗ trợ một bộ kết nối dùng cặp dây xoắn 10BASET từ mỗi trạm của mạng. Khi bó tín hiệu Ethernet được truyền từ một trạm tới hub, nó được lặp lại trên khắp các cổng khác của hub. Các hub thông minh có thể định dạng, kiểm tra, cho phép hoặc không cho phép bởi người điều hành mạng từ trung tâm quản lý hub. Có ba loại hub:

- Hub đơn (stand alone hub)
- Hub modun (modular hub) : Modular hub rất phổ biến cho các hệ thống mạng vì nó có thể dễ dàng mở rộng và luôn có chức năng quản lý, modular có từ 4 đến 14 khe cắm, có thể lắp thêm các modun Ethernet 10BASET.
- Hub phân tầng (stackable hub) : thuận tiện cho những cơ quan muốn đầu tư tối thiểu ban đầu nhưng lại có kế hoạch phát triển LAN sau này.

## 4.2 Các giao thức điều khiển truy nhập đường truyền

Giao thức dùng để đánh giá khả năng của một mạng được phân chia bởi các trạm như thế nào. Hệ số này được quyết định chủ yếu bởi hiệu quả sử dụng môi trường truy xuất (medium access) của giao thức.

Mọi kênh phương tiện chỉ có thể hỗ trợ một lần tín hiệu. Nếu hai máy tính truyền trên kênh cùng một lúc, các tín hiệu của chúng sẽ gây nhiễu cho nhau (ví dụ như hai người cùng nói một lúc). Có hai phương pháp điều khiển việc truy nhập phương tiện để không xảy ra sự cố gây nhiễu : truy nhập ngẫu nhiên và truy nhập có điều khiển.

- *Loại truy nhập ngẫu nhiên*

Trạm có thể truy nhập phương tiện truyền tuỳ theo ý muốn, bất kỳ ở thời điểm ngẫu nhiên nào.

a. Kỹ thuật truy cập ngẫu nhiên đối với dạng bus

- Phương pháp đa truy nhập sử dụng sóng mang (CSMA - Carrier Sense Multiple Access).
- Phương pháp đa truy nhập sử dụng sóng mang với phát hiện xung đột (CSMA/CD - with Collision Detection)

b. Kỹ thuật truy cập ngẫu nhiên đối với dạng vòng

- Phương pháp chèn thanh ghi (Register insertion)
- Phương pháp vòng có ngăn (Slotted-ring)

- *Loại truy nhập có điều khiển*

Phương pháp điều khiển tranh chấp thường thích hợp với các mạng có sự trao đổi dữ liệu không liên tục và tương đối ít máy tính. Đây là dạng thông dụng trong cấu trúc mạng cục bộ.

- Kỹ thuật bus với thẻ bài (Token Bus) : dùng cho các mạng LAN
- Kỹ thuật vòng với thẻ bài (Token Ring) : dùng cho các mạng LAN
- Kỹ thuật tránh xung đột : dùng cho các mạng cục bộ tốc độ cao.

### 4.2.1 Phương pháp CSMA

Còn được gọi là phương pháp LBT (Listen Before Talk - Nghe trước khi nói). Một trạm có dữ liệu cần truyền trước hết phải 'nghe' xem phương tiện truyền rỗi hay bận. Nếu rỗi thì bắt đầu truyền tin, còn nếu bận thì thực hiện một trong ba giải thuật sau :

- Giải thuật '*non-persistent*' : Tram rút lui (không kiên trì) chờ đợi một thời gian ngẫu nhiên nào đó rồi lại bắt đầu 'nghe' đường truyền. Giải thuật này có hiểu quả tránh xung đột nhưng có thời gian chết.
- Giải thuật '*1-persistent*' : Trạm tiếp tục nghe đến khi phương tiện truyền rỗi thì tiến hành truyền dữ liệu đi (với xác xuất 1). Giải thuật này giảm thời gian chết, xong nếu có nhiều trạm cùng chờ và tiến hành phát dữ liệu cùng một lần thì sẽ xảy ra xung đột.
- Giải thuật '*p-persistent*' : trạm tiếp tục nghe, đến khi phương tiện truyền rỗi thì tiến hành phát tin với một xác xuất nhất định nào đó (mỗi trạm có gắn một hệ số ưu tiên). Ngược lại trạm 'rút lui' trong một thời gian cố định rồi

truyền với xác suất p hoặc tiếp tục chờ đợi với xác xuất 1-p. Giải thuật này phức tạp nhưng giảm được tối đa xung đột và thời gian chết.

Phương pháp CSMA chỉ 'nghe trước khi nói', không có khả năng phát hiện xung đột trong quá trình truyền, dẫn đến lãng phí đường truyền.

### 4.2.2 Phương pháp CSMA/CD

Phương pháp CSMA/CD có nguồn gốc từ hệ thống radio đã phát triển ở trường đại học Hawai vào khoảng năm 1970, gọi là ALOHANET, còn được gọi là phương pháp LWT (Listen While Talk - Nghe cả trong khi nói). Các va chạm luôn xảy ra tại một cấp nào đó trên các mạng, với số lượng gia tăng theo tỉ lệ thuận khi các phiên truyền gia tăng.

Phương pháp CSMA/CD ngoài các chức năng của CSMA còn bổ sung các quy tắc sau :

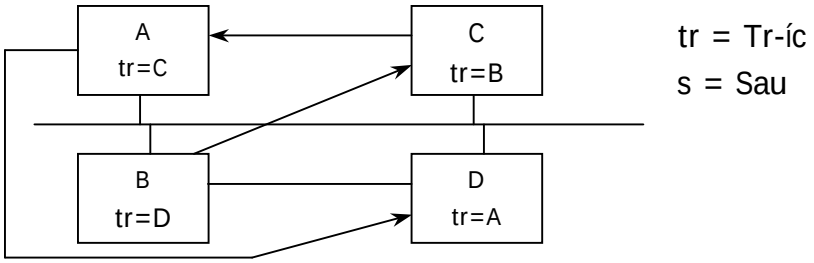
1. Khi đang truyền vẫn tiếp tục nghe đường dây.
2. Nếu phát hiện có xung đột thì *ngừng truyền* và *tiếp tục gởi sóng mang* thêm một thời gian nữa để bảo đảm các trạm đều có thể nghe được sự kiện xung đột.
3. Sau khi chờ đợi một thời gian ngẫu nhiên thì trạm thử truyền lại bằng cách sử dụng các phương pháp của CSMA.

Với phương pháp CSMA/CD thời gian chiếm dụng vô ích đường truyền giảm xuống bằng thời gian dùng để phát hiện một đụng độ. CSMA/CD sử dụng ba giải thuật 'persistent' ở trên. Trong đó giải thuật '*1-persistent*' được sử dụng trong mạng Ethernet, Mitrenet và được chọn cả trong chuẩn IEEE.802. Ngoài ra mỗi chuẩn LAN còn có thêm các cơ chế bổ sung.

### 4.2.3 Điều khiển truy nhập bus với thẻ bài

Các trạm trên bus tạo nên một vòng logic, được xác định vị trí theo một dãy thứ tự, trong đó trạm cuối sẽ tiếp liền ngay sau trạm đầu tiên. Mỗi trạm được biết địa chỉ của các trạm kề sau và kề trước nó.

Thẻ bài dùng cấp phát quyền truy nhập, được lưu chuyển trong vòng logic. Khi trạm nhận được thẻ bài thì được trao quyền sử dụng phương tiện trong một thời gian xác định để truyền dữ liệu. Khi truyền xong hoặc hết thời hạn, trạm sẽ chuyển thẻ bài đến trạm kế tiếp trong vòng logic. Các trạm không sử dụng thẻ bài vẫn có mặt trên bus nhưng chúng chỉ có thể trả lời cho yêu cầu xác nhận (nếu chúng là đích của gói tin nào đó). Thứ tự vật lý của trạm trên bus là không quan trọng, độc lập với thứ tự logic.




Hình 4-1. Điều khiển truy nhập bus với thẻ bài.

*Các chức năng :*

- Khởi tạo vòng logic : khi thiết lập mạng hoặc khi vòng logic bị gãy.
- Bổ sung trạm vào vòng logic (xem xét định kỳ) bằng cách mời nút đứng sau nhập vòng. Loại bỏ một trạm ra khỏi vòng logic bằng cách nối trạm trước và sau nó với nhau
- Quản lý sai sót : trùng địa chỉ, gãy vòng (các trạm bị treo, rơi vào trạng thái chờ lẫn nhau), bởi nút giữ Token.
- Khi đang giữ thẻ mà có trạm khác nhận được gói tin thì chứng tỏ nút khác đã có thẻ, lúc đó nó sẽ bỏ thẻ bằng cách chuyển sang trạng thái 'nghe'.
- Khi nút đã hoàn thành công việc, nó gửi thẻ đến nút đứng sau, nếu nút tiếp sau hoạt động thì nó gởi thẻ chuyển sang trạng thái bị động. Nếu ngược lại, nó gửi thẻ cho nút kế tiếp lần nữa. Nếu hai lần gửi không được thì xem như nút kế tiếp hỏng và gửi đi gói tin "tìm nút kế tiếp" để tìm nút tiếp theo.
- Nếu không thành công thì nút bị xem là có sự cố. Nút ngừng hoạt động và 'nghe' trên bus.

- Dạng bản tin của mạng Token bus

| Bắt đầu tin | Điều khiển gói tin | Địa chỉ nguồn | Địa chỉ đích | TIN | FSC | Kết thúc tin |
|---|---|---|---|---|---|---|
| 1 byte | 1 byte | 2-6 bytes | 2 - 6 bytes | | 4 bytes | 1 byte |
| | Khung tin cực đại 8191 bytes | | | Tốc độ có thể là 1; 5; 10Mbps | | |

- So sánh CSMA/CD và Token Bus

- Token bus quản lý phức tạp hơn so với CSMA/CD. Trong trường hợp tải nhẹ thì không hiệu quả bằng CSMA/CD (do phải qua nhiều trạm)
- Tuy nhiên Token Bus có hiệu quả trong trường hợp tải nặng, dễ điều hoà lưu thông trên mạng Token Bus. Không quy định độ dài tối thiểu của gói tin, không cần nghe trước khi nói.

### 4.2.4 Điều khiển truy nhập vòng với thẻ bài

Đây là giao thức thông dụng được dùng trong các LAN có cấu trúc vòng (Ring). Phương pháp này sử dụng một khối tín hiệu đặc biệt gọi là Token di chuyển vòng quanh mạng theo một chiều xác định. Một trạm muốn truyền phải đợi cho đến khi nhận được thẻ bài. Khi một trạm đang chiếm Token thì nó có thể phát đi một gói dữ liệu. Khi đã phát hết gói dữ liệu cho phép hoặc không còn gì để phát nữa thì trạm đó chuyển khung thẻ bài đến cho trạm kế tiếp trên mạng. Trong token có chứa một địa chỉ đích và được luân chuyển tới các trạm theo một trật tự đã định trước. Đối với cấu hình mạng dạng xoay vòng thì trật tự của sự truyền token tương đương với trật tự vật lý của các trạm xung quanh vòng.

Các chuẩn mạng sử dụng phương pháp điều khiển truy nhập thẻ bài :

- Chuẩn IEEE 802.5, còn gọi là chuẩn Token Ring.
- FDDI là chuẩn sợi quang 100 Mps sử dụng phương pháp chuyển thẻ bài và vòng tròn.

Phương pháp chuyển thẻ bài thích hợp trong các điều kiện như sau :

- Khi mạng đang tải dữ liệu quan trọng về thời gian do phương pháp này cung cấp khả năng bàn giao.
- Khi mạng được sử dụng nhiều, do tránh được xung đột.
- Khi một vài trạm có mức ưu tiên cao hơn so với các trạm khác. Phương pháp chuyển thẻ bài có thể áp dụng các mức ưu tiên cho trạm để ngăn cấm một trạm bất kỳ không được độc quyền về mạng.
- Do thẻ bài luân chuyển quanh mạng nên mỗi trạm có thể truyền theo quãng thời gian tối thiểu.

Phương pháp chuyển thẻ bài đòi hỏi cơ chế điều khiển phức tạp và chi phí đầu tư phần cứng cao, nhưng được thiết kế với độ tin cậy cao. Tuy vậy hiện nay Ethernet vẫn là chuẩn LAN thông dụng, chứng tỏ được ưu điểm của phương pháp tranh chấp khi sử dụng trên các mạng LAN.

Giao thức truyền token có trật tự hơn nhưng cũng phức tạp hơn CSMA/CD, có ưu điểm là vẫn hoạt động tốt khi lưu lượng truyền thông lớn. Giao thức truyền token tuân thủ đúng sự phân chia của môi trường mạng, hoạt động dựa vào sự xoay vòng tới các trạm. Việc truyền token sẽ không thực hiện được nếu việc xoay vòng bị đứt đoạn. Giao thức phải chứa các thủ tục kiểm tra token để cho phép khôi phục lại token bị mất hoặc thay thế trạng thái của token và cung cấp các phương tiện để sửa đổi logic (thêm vào, bớt đi hoặc định lại trật tự của các trạm).

Khung tin cực đại là 16KB ở chế độ truyền 16Mbps và 4KB ở chế độ truyền 4Mps.

Dạng bản tin với mạng Token Ring :

| Bắt đầu tin | Điều khiển thâm nhập | Điều khiển gói tin | Địa chỉ nguồn | Địa chỉ đích | TIN | FSC | Kết thúc gói tin | Trạng thái gói tin |
|---|---|---|---|---|---|---|---|---|
| 1 byte | 1 byte | 2-6 bytes | 2 - 6 bytes | 2 - 6 bytes | | 4 bytes | 1 byte | 1 byte |

#### *4.2.4.1 Phương pháp điều khiển truy nhập dò báo*

Dò báo (*polling*) là một phương pháp điều khiển truy cập sử dụng một thiết bị trung tâm để điều khiển toàn bộ việc truy cập mạng. Đây là phương pháp được sử dụng phổ dụng nhất trên các mạng máy tính lớn.

Thiết bị trung tâm có tên là thiết bị chính sẽ yêu cầu dữ liệu từ các thiết bị khác trên mạng có tên là thiết bị thứ cập (*secondaries*). Sau khi được dò báo, thiết bị thứ cấp có thể truyền một lượng dữ liệu được xác định bởi các giao thức dùng trên mạng. Một thiết bị thứ cấp không thể truyền trừ phi nó được thiết bị chính dò báo.

Phương pháp dò báo có nhiều ưu điểm của phương pháp chuyển thẻ bài như :

- Dự đoán được các lần truy cập định sẵn.
- Gán được các mức ưu tiên, tránh được va chạm.

So sánh phương pháp dò báo và phương pháp chuyển thẻ bài : kỹ thuật dò báo tập trung hóa quyền điều khiển. Nhìn dưới góc độ quản lý thì đây là một ưu điểm, nhưng nếu cơ chế điều khiển trung tâm bị hỏng, mạng sẽ ngừng hoạt động. Phương pháp chuyển thẻ bài sử dụng các chức năng điều khiển phân phối hơn do đó ít bị hỏng tập trung tại một điểm. Bên cạnh đó, phương pháp dò báo đôi khi lãng phí các lượng băng thông lớn do phải dò báo từng thiết bị thứ cấp, cho dù các thiết bị không có gì để truyền.

## 4.3 Chuẩn hóa mạng cục bộ

Các chuẩn LAN là các tiêu chuẩn công nghệ cho Lan được phê chuẩn bởi các tổ chức chẩun hóa quốc tế, nhằm hướng dẫn các nhà sản xuất thiết bị mạng đi đến sự thống chung khả năng sử dụng chung các sản phẩm của họ, vì lợi ích của người sử dụng và tạo điều kiện thuận lợi cho các nghiên cứu phát triển.

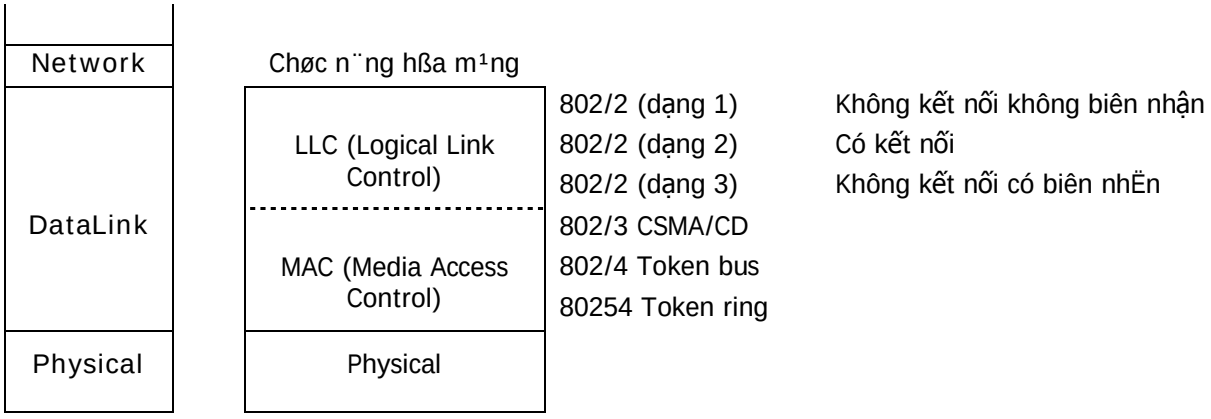
Các chuẩn này quy định môi trường truyền dẫn cũng như cách thức sử dụng chúng trong kết nối LAN; Các giao thức truyền thông ở các tầng vật lý và tầng liên kết dữ liệu của mạng theo mô hình OSI.

Các giao thức truyền thông ở các tầng trên của mô hình OSIhiện tại được xác định qua một số giao thức phổ biến như TCP/IP, IPX/SPX, NetBIOS,. . .

Uỷ ban IEEE phát triển tiêu chuẩn IEEE LAN và đề xuất phân chia hai tầng thấp nhất của mô hình OSI như dưới đây.

Theo chuẩn 802 thì tầng LKDL được chia thành 2 tầng con:

- Tầng con điều khiển logic LLC (Logical Link Control Sublayer) : giữ vai trò tổ chức dữ liệu, tổ chức thông tin để truyền và nhận. Thủ tục tầng LLC không bị ảnh hưởng khi sử dụng các đường truyền dẫn khác nhau, nhờ vậy mà linh hoạt hơn trong khai thác.
- Tầng con điều khiển xâm nhập mạng MAC (Media Access Control Sublayer). làm nhiệm vụ điều khiển việc xâm nhập mạng.




Hình 4-2. Các tầng con LLC và MAC.

Chuẩn 802.2 ở mức con LLC tương đương với chuẩn HDLC của ISO hoặc X.25 của CCITT.

Chuẩn 802.3 xác định phương pháp thâm nhập mạng tức thời có khả năng phát hiện lỗi chồng chéo thông tin CSMA/CD. Phương pháp CSMA/CD được đưa ra từ năm 1993 nhằm mục đích nâng cao hiệu quả mạng. Theo chuẩn này các mức được ghép nối với nhau thông qua các bộ ghép nối.

Chuẩn IEEE 802.3 dùng cho mạng Ethernet (sử dụng giao thức truy nhập CSMA/CD) bao gồm cả 2 phiên bản băng tần cơ bản và băng tần mở rộng.

Chuẩn IEEE 802.4 liên quan tới sự sắp xếp tuyến token, thực chất là phương pháp thâm nhập mạng theo kiểu phát tín hiệu thăm dò token qua các trạm và đường truyền bus.

Chuẩn IEEE 802.5 dùng cho mạng dạng vòng và trên cơ sở dùng tín hiệu thăm dò token. Mỗi trạm khi nhận được tín hiệu thăm dò token thì tiếp nhận token và bắt đầu quá trình truyền thông tin dưới dạng các frame. Các frame có cấu trúc tương tự như của chuẩn 802.4. Phương pháp xâm nhập mạng này quy định nhiều mức ưu tiên khác nhau cho toàn mạng và cho mỗi trạm, việc quy định này vừa cho người thiết kế vừa do người sử dụng tự quy định.

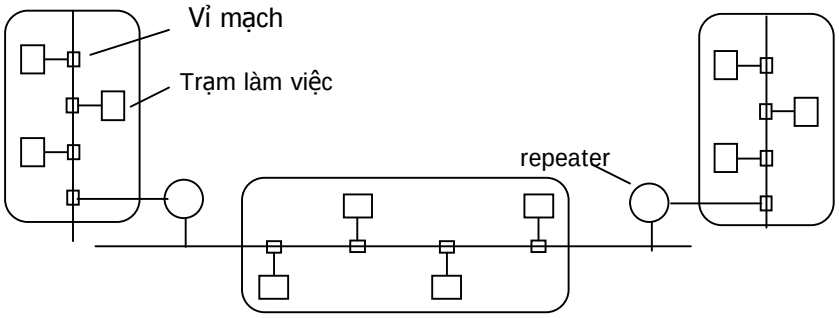
Chuẩn IEEE 802.11 dùng cho mạng không dây (Wireless).

### 4.3.1 Chuẩn Ethernet

Chuẩn Ethernet được sử dụng phổ biến nhất, đến mức đôi khi được hiểu đồng nghĩa với LAN. Tuy nhiên nó đã được xây dựng và phát triển qua các giai đoạn với các tên gọi là DIX standard Ethernet và IEE 802.3 standard. Chuẩn Ethernet do các công ty Xerox, Intel và Digital equipment xây dựng và phát triển. Ethernet LAN được xây dựng theo chuẩn 7 lớp trong cấu trúc mạng của ISO, mạng truyền số liệu Ethernet cho phép đưa vào mạng các loại máy tính khác nhau kể cả máy tính mini. Ethernet có các đặc tính kỹ thuật chủ yếu sau đây:

- Có cấu trúc dạng tuyến phân đoạn, đường truyền dùng cáp đồng trục, tín hiệu truyền trên mạng được mã hoá theo kiểu đồng bộ (Manchester), tốc độ truyền dữ liệu là 10 Mb/s.
- Chiều dài tối đa của một đoạn cáp tuyến là 500m, các đoạn tuyến này có thể được kết nối lại bằng cách dùng các bộ chuyển tiếp và khoảng cách lớn nhất cho phép giữa 2 nút là 2,8 km.
- Sử dụng tín hiệu băng tần cơ bản, truy xuất tuyến (bus access) hoặc tuyến token (token bus), giao thức là CSMA/CD, dữ liệu chuyển đi trong các gói. Gói tin dùng trong mạng có độ dài từ 64 đến 1518 byte.

- Cấu trúc của mạng Ethernet : Mạng Ethernet có cấu trúc dạng bus như sau :




Hình 4-3. Cấu trúc của mạng Ethernet.

Số trạm cực đại trong mạng là 1024, số lượng segment của mạng giới hạn nhỏ hơn 5 segment, khoảng cách tối đa giữa hai trạm là 2,5km. Mạng sử dụng cáp đồng trục tốc độ 10Mps. Cấu trúc khung tin Ethernet có khuôn dạng như sau :

| Cờ | Địa chỉ đích | Địa chỉ nguồn | Loại tin | TIN | CRC | Cờ |
|---|---|---|---|---|---|---|
| | 6 bytes | 6 bytes | 2 bytes | 46 – 1500 bytes | 4 bytes | |

*Chương 5*

# TẦNG MẠNG

Tầng mạng đảm bảo truyền tin thông suốt giữa hai nút đầu cuối trong mạng. Trên cơ sở cấu hình của mạng, tầng mạng sẽ kiểm tra sơ đồ kết nối (*topology*) của toàn mạng để quyết định đường đi tối ưu truyền gói dữ liệu, tránh quá tải trên một đường truyền trong khi một số đường truyền rỗi. Thực hiện cắt/ hợp dữ liệu khi qua mạng và liên kết mạng khi có nhiều mạng nối với nhau.

## 5.1 Các vấn đề của tầng mạng

### 5.1.1 Định địa chỉ cho tầng mạng

Tầng mạng sử dụng các kiểu địa chỉ bổ sung sau :

1. Địa chỉ mạng logic (Logical network addresses), định tuyến các gói tin theo các mạng cụ thể trên liên mạng. Dùng để định danh một mạng cụ thể trên liên mạng dưới dạng một nguồn hay đích của một gói tin.
2. Địa chỉ dịch vụ (Service addresses), định tuyến các gói tin theo các tiến trình cụ thể đang chạy trên thiết bị đích, dùng định danh một giao thức hay tiến trình trên máy tính là nguồn hay đích của một gói tin.
3. Địa chỉ mạng vật lý (MAC) định danh một thiết bị cụ thể dưới dạng một nguồn hay đích của một khung.

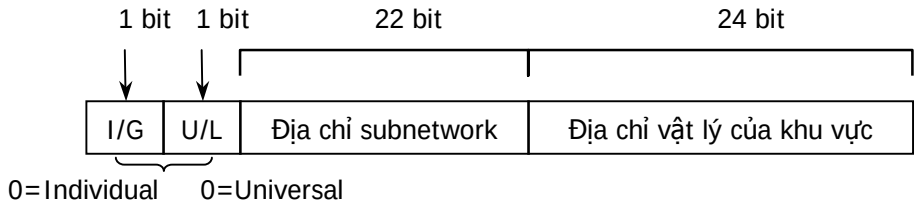
*Địa chỉ vật lý của máy trạm :*

Mỗi thiết bị trên một mạng có một địa chỉ vật lý duy nhất để giao tiếp với các thiết bị khác, còn gọi là địa chỉ phần cứng. Trên tất cả các mạng hiện nay, mỗi địa chỉ xuất hiện một lần duy nhất (nghĩa là mỗi thiết bị chỉ có một địa chỉ duy nhất). Đối với phần cứng, địa chỉ thường được mã hoá trong thiết bị card mạng (Network Interface Card), có thể được đặt bằng chuyển mạch hoặc bằng phần mềm. Trong mô hình OSI thì địa chỉ này được đặt ở lớp vật lý.

Độ dài của địa chỉ vật lý phụ thuộc vào từng mạng, chẳng hạn với mạng Ethernet và một số mạng khác thì dùng địa chỉ vật lý dài 48 bit. Để trao đổi thông tin thì cần có địa chỉ của nơi gởi, và địa chỉ của nơi nhận.

Hiện nay IEEE đang đảm nhiệm việc ấn định địa chỉ vật lý tổng thể (*universal physical address*) cho các subnetwork. Đối với mỗi subnetwork, IEEE ấn định một phần địa chỉ đồng nhất đối với tất cả các subnetwork gọi là OUI (Organization Unique Identifier) phần này có độ dài là 24 bit, cho phép IEEE ấn định phần địa chỉ 24 bit còn lại theo yêu cầu. (Trên thực tế, hai trong 24 bit địa chỉ OUI là các bit điều khiển, do đó 22 bit là để xác định subnetwork đó. Dó đó chỉ có khoảng $2^{22}$ địa chỉ

được dùng, nếu với tốc độ phát triển như hiện nay có thể sẽ thiếu địa chỉ trong tương lai). Sau đây là cấu tạo của địa chỉ OUI :




Hình 5-1. Cấu tạo của địa chỉ vật lý ĂUI.

### 5.1.2 Dịch vụ cung cấp cho tầng giao vận

- Các dịch vụ phải độc lập với công nghệ được dùng trong mạng.
- Tầng giao vận phải độc lập với công nghệ được dùng trong mạng.
- Các địa chỉ mạng phải thống nhất để tầng giao vận có thể dùng cả mạng LAN và WAN.

*Có 2 loại dịch vụ :*

- Dịch vụ truyền tin có liên kết (*Connection Ăriennted Service*)
- Dịch vụ truyền tin không liên kết (*Connectionless Service*)

Sự khác nhau giữa hai dịch vụ

| **Vấn đề** | **Dịch vụ có liên kết** | **Dịch vụ không liên kết** |
|---|---|---|
| Khởi động kênh | Cần thiết | Không |
| Địa chỉ đích | Chỉ cần lúc khởi động | Cần ở mọi gói tin |
| Thự tự gói tin | Được đảm bảo | Không đảm bảo |
| Kiểm soát lỗi | ở tầng mạng | ở tầng giao vận |
| Điều khiển thông lượng | ở tầng mạng | ở tầng giao vận |
| Thảo thuận tham số | Có | Không |
| Nhận dạng liên kết | Có | Không |

Các hàm cơ bản của dịch vụ liên kết tầng mạng :

N-CONNECT. Request (callce, caller, acks wanted, exp wanted, qos, user data)
N-CONNECT. Indication (callce, caller, acks wanted, exp wanted, qos, user data)
N-CONNECT. Response (response acks wanted, exp wanted, qos, user data)
N-CONNECT. Confirmation (response acks wanted, exp wanted, qos, user data)
N-DISCONNNECT. Request (originator, reason, user data, responding address)
N-DISCONNNECT. Indication (originator, reason, user data, responding address)
N-DATA. Request (user data)
N-DATA. Indication (user data)
N-DATA-ACKNOWLEDGED. Request ()
N-DATA-ACKNOWLEDGED. Indication ()
N-EXPEDITED-DATA. Request (user data)
N-EXPEDITED-DATA. Indication (user data)
N-RESET. Request (originator, reason)

N-RESET. Indication (originator, reason)
N-RESET. Response()
N-RESET. Confim()

Các hàm cơ bản của dịch vụ không liên kết tầng mạng

N-UNITDATA. Request (source address, destination address, qos, user_data)
N-UNITDATA. Indication (source address, destination address, qos, user_data)
N-FACILITY. Request (qos)
N-FACILITY. Indication (destination address, qos, reason)
N-FACILITY. Indication (destination address, qos, reason)

Hàm N_FACILITY.request cho phép NSD dịch vụ mạng biết tỷ lệ phần trăm gói tin đang được giao vận.

Hàm N_REPORT.indication cho phép tầng mạng thông báo lại cho NSD dịch vụ mạng.

### 5.1.3 Tổ chức các kênh truyền tin trong tầng mạng

Có hai loại kênh truyền tin hoạt động trong mạng :

#### *5.1.3.1 Kênh ảo (virtual circuit)*

Tương đương kênh điện thoại trong tầng vật lý sử dụng trong mạng có liên kết. Kênh ảo được thiết lập cho mỗi liên kết. Một khi đã được thiết lập thì các gói tin được chuyển đi tương tự trong mạng điện thoại cho đến khi liên kết bị hủy bỏ.

- Mỗi nút mạng chứa một kênh ảo, với cửa vào cho một kênh ảo
- Khi một liên kết được khởi động, một kênh ảo chưa dùng sẽ được chọn
- Nút chọn kênh ảo chứa đường dẫn đến trạm tiếp theo và có số thấp nhất

Khi gói tin khởi động đến nút đích, nút chọn kênh ảo có số thấp nhất thay thế số trong gói tin và chuyển vào trạm đích. Số kênh ảo nối với trạm đích có thể khác số kênh ảo mà trạm nguồn sử dụng.

#### *5.1.3.2 Mạng Datagram*

Tương đương với điện báo sử dụng trong mạng không liên kết. Trong mạng này, không có tuyến đường nào được thiết lập. Các gói tin có thể đi theo nhiều đường khác nhau mà không nhất thiết theo một trình tự xác định. Thông tin vào là địa chỉ đích, thông tin ra là nút mạng phải tới.

Mạng Datagram phức tạp về điều khiển nhưng nếu kênh hỏng thì dễ dàng đi theo kênh khác. Do đó có thể giải quyết được vấn đề tắc nghẽn dữ liệu.

- Các đặc trưng của mạng Datagram và mạng kênh ảo

| Vấn đề | Mạng datagram | Mạng kênh ảo |
|---|---|---|
| *Khởi động kênh* | Không | Cần thiết |
| *Địa chỉ (đ/c) hoá* | Gói tin phải có đ/c nguồn và đ/c đích | Gói tin chỉ cần số của kênh ảo |
| *Thông tin tìm đường* | Không cần bất cứ thông tin nào. | Mỗi kênh ảo cần một vùng trong bảng |
| *Tìm đường* | Mỗi gói tin tìm đường độc lập. Phải tìm đường mỗi khi có gói tin tới nút mạng. | Được thiết lập khi khởi động kênh ảo mới. Liên kết sẽ được duy trì cho cả phiên. |
| *Điều khiển* | Chỉ mất gói tin ở trong nút hỏng | Kênh ảo đi qua nút hỏng sẽ bị huỷ |
| *Hỏng nút* | Khó khắc phục | Dễ khắc phục hơn |
| *Độ phức tạp* | Trong tầng giao vận | Trong tầng mạng |
| *Thích hợp* | Các dịch vụ liên kết và không liên kết | Các dịch vụ liên kết |

### 5.1.4 Tìm đường đi trong mạng

Chức năng quan trọng nhất của tầng mạng là dẫn đường cho các gói tin từ trạm nguồn tới trạm đích. Thuật toán tìm đường là qui trình để quyết định chọn đường ra khỏi nút mạng nhằm gởi gói tin đi tiếp tới nút khác.

- Yêu cầu của thuật toán tìm đường

- Chính xác, ổn định, đơn giản và tối ưu.
- Thuật toán tìm đường phải có khả năng cập nhật lại cấu hình và đường vận chuyển để không phải khởi động lại mạng khi có một nút hỏng hoặc phải ngừng hoạt động của các máy ở trạm.

- Các thuật toán chia làm hai nhóm chính:

- Nhóm không thích nghi (*non adaptive*) : việc chọn đường không dựa vào việc đánh giá tình trạng giao thông và cấu hình trong thời gian thực.
- Nhóm thích nghi (*adaptive*) : việc tìm đường phải thích nghi với tình trạng giao thông hiện tại.

Sơ đồ mạng được biểu diễn dưới dạng đồ thị, mỗi nút của đồ thị là một nút mạng, cung của đồ thị biểu diễn đường truyền nối giữa hai nút. Việc chọn đường giữa hai nút mạng là tìm đường ngắn nhất giữa chúng.

Mỗi cung được gán một nhãn cho biết thời gian trung bình phải đợi và thời gian truyền một gói tin chuẩn. Thời gian này được thử mỗi giờ hay mỗi ngày một lần. Đường ngắn nhất là đường có ít bước chuyển tiếp qua nút nhất và có số đo độ dài nhỏ nhất, mất ít thời gian.

Có nhiều thuật toán để tìm đường ngắn nhất giữa 2 điểm, ví dụ như thuật toán Dijkstra (1959). Ta xây dựng đồ thị cho các nút mạng và tìm khoảng cách giữa các nút mạng.

### 5.1.5 Tắc nghẽn trong mạng

Khi có quá nhiều gói tin trong mạng hay một phần của mạng làm cho hiệu suất của mạng giảm đi vì các nút mạng không còn đủ khả năng lưu trữ, xử lý, gửi đi và chúng bắt đầu bị mất các gói tin. Hiện tượng này được gọi là sự tắc nghẽn (*congestion*) trong mạng.

Hàng đợi sẽ bị đầy (phải lưu tập tin, tạo các bảng chọn đường ...) nếu khả năng xử lý của nút yếu hoặc khi thông tin vào nhiều hơn khả năng của đường ra

*Điều khiển dòng dữ liệu* là xử lý giao thông giữa điểm với điểm, giữa trạm thu và phát. Trong khi đó điều khiển tránh tắc nghẽn là một vấn đề tổng quát hơn bao gồm việc tạo ra hoạt động hợp lý của các máy tính của các nút mạng, quá trình lưu trữ bên trong nút, điều khiển tất cả các yếu tố làm giảm khả năng vận chuyển của toàn mạng.

- Các biện pháp ngăn ngừa

- Bố trí khả năng vận chuyển, lưu trữ, xử lý của mạng dư so với yêu cầu.
- Huỷ bỏ các gói tin bị tắc nghẽn quá thời hạn.
- Hạn chế số gói tin vào mạng nhờ cơ chế cửa sổ (*flow control*).
- Chặn đường vào khi của các gói tin khi mạng quá tải.

## 5.2 Kết nối liên mạng

Nhu cầu trao đổi thông tin và phân chia các tài nguyên dùng chung đòi hỏi hoạt động truyền thông không chỉ ở phạm vi cục bộ mà ở cả khuôn khổ quốc gia và quốc tế. Từ đó dẫn đến sự nối kết các mạng viễn thông tin học được đặt ở các vị trí địa lý khác nhau và chịu sự quản lý của các tổ chức hoặc quốc gia khác nhau.

Sự nối kết mạng (*Networks Interconnection*) giống như ghép nối mạng đơn lẻ nhưng phức tạp hơn nhiều do tính chất không thuần nhất của các mạng con được kết nối. Chúng có thể có kiến trúc khác nhau bao gồm các máy tính nút mạng. Đường truyền khác nhau, chiến lược quản lý khác nhau.

Người ta thường xem xét các vấn đề sau để kết nối các mạng con lại với nhau :

- Xem mỗi nút của mạng con như là một hệ thống mở : mỗi nút mạng con có thể truyền thông trực tiếp với một nút của mạng con khác bất kỳ. Như thế yêu cầu phải xây dựng một chuẩn chung cho các mạng.
- Xem mỗi mạng như là một hệ thống mở : Hai nút thuộc hai mạng con không bắt tay trực tiếp với nhau mà phải thông qua một phần tử trung gian gọi là *giao diện kết nối (interconnection interface)* dat giữa hai mạng con đó.

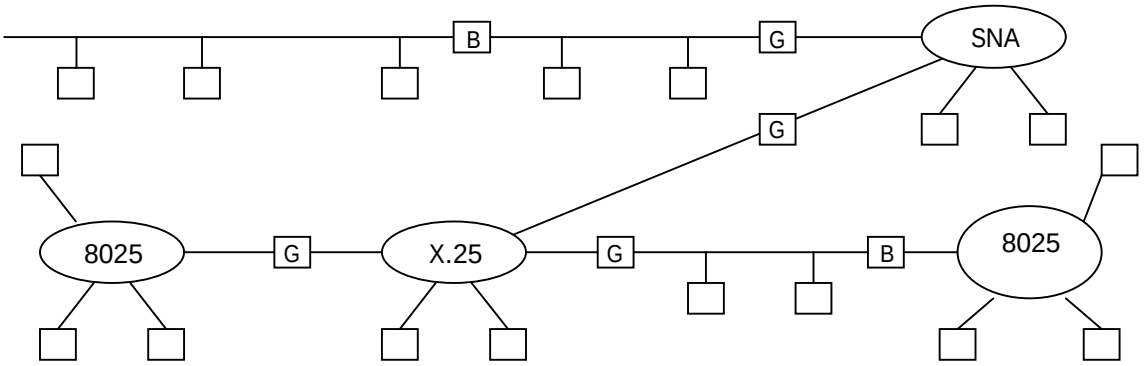
Chức năng của giao diện kết nối phụ thuộc vào sự khác biệt kiến trúc của mạng con : sự khác biệt càng lớn thì chức năng của giao diện càng phức tạp.

Có thể có các kết nối mạng như sau :

| | |
|---|---|
| LAN-LAN | : Nối các mạng cục bộ. |
| LAN-WAN | : Nối các mạng cục bộ với mạng đường dài. |
| WAN-WAN | : Nối các mạng đường dài |
| LAN-WAN- LAN | : Nối mạng đường dài với mạng cục bộ. |

Nếu máy nguồn và máy đích không ở cùng một mạng phải tìm đường từ mạng này sang mạng khác. Nếu trạm nguồn và đích không ở hai mạng liền kề thì giải quyết tìm đường qua nhiều trạm.

Các mạng khác nhau có các giao thức khác nhau, dẫn đến khác nhau về dạng khuôn của gói tin, đầu gói tin, điều khiển dòng dữ liệu và qui tắc xác nhận.



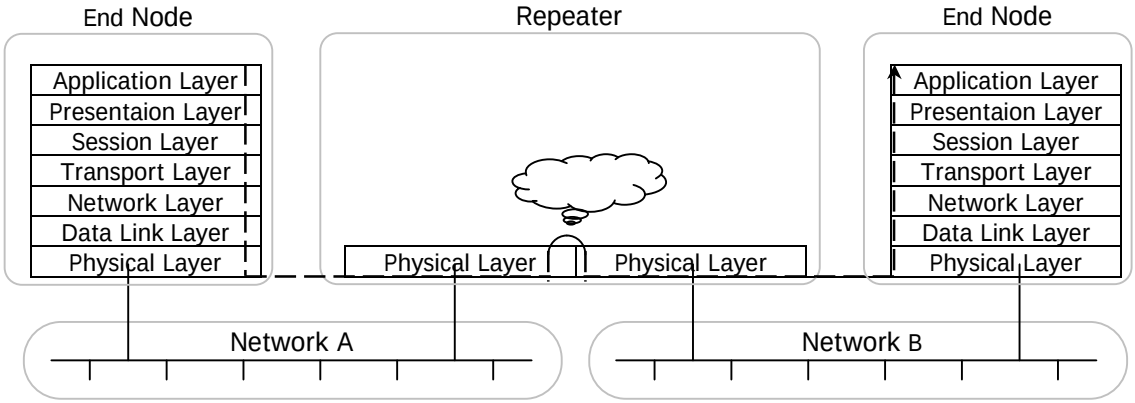

Hình 5-2. Kết nối liên mạng.

### 5.2.1 Các thiết bị dùng để kết nối liên mạng

Việc kết nối các LAN riêng lẻ thành một liên mạng chung gọi là Internetworking, sử dụng các thiết bị kết nối thông dụng như sau :

#### *5.2.1.1 Bộ lặp*

Bộ lặp (repeater) thực hiện chức năng ở tầng vật lý để khuyếch đại tín hiệu khi tín hiệu truyền đi xa. Bộ lặp được sử dụng để kết nối các đoạn mạng lại với nhau. Bộ lặp nhận tín hiệu từ một đoạn mạng, tái tạo và truyền tín hiệu này đến đoạn mạng khác. Nhờ có bộ lặp mà tín hiệu bị suy yếu do phải truyền qua một đoạn cáp dài có thể trở lại dạng ban đầu và truyền đi được xa hơn.




Hình 5-3. Sơ đồ kiến trúc của Repeater trong mô hình OSI.

Bộ lọc không có khả năng xử lý lưu lượng. Tất các tín hiệu điện, bao gồm cả nhiễu điện từ và các lỗi khác cũng được lặp và khuếch đại. Để bộ lặp hoạt động, cả hai đoạn mạng nối tới bộ lặp phải sử dụng cùng một phương thức truy nhập đường truyền. Ví dụ: bộ lặp không thể nối một đoạn mạng sử dụng phương thức CSMA/CD và một đoạn mạng sử dụng phương thức chuyển thẻ bài.

Bộ lặp có thể di chuyển gói dữ liệu từ phương tiện truyền dẫn này sang phương tiện truyền dẫn khác. Ví dụ có thể nhận gói dữ liệu từ một đoạn mạng dùng cáp đồng trục và chuyển gói đó sang đoạn mạng sử dụng cáp quang.

#### *5.2.1.2 Hub*

HUB là một thiết bị liên kết mạng được sử dụng rộng rãi. HUB còn là thành phần trung tâm trong cấu trúc mạng hình sao (Star). Mạng Star sử dụng sự phân chia tín hiệu trong HUB để đưa các tín hiệu ra các đường cáp khác nhau. Do vậy, có 3 loại HUB có thể sử dụng trong mạng là: HUB chủ động, HUB thụ động và HUB lai.

- ***HUB chủ động:*** Hầu hết các HUB đều là HUB chủ động, chúng tái tạo và truyền lại tín hiệu giống như bộ lặp. HUB thường có nhiều cổng nên thỉnh thoảng chúng còn được gọi là bộ lặp đa cổng. HUB chủ động đưa ra các tín hiệu mạnh hơn do đó cho phép đoạn cáp dài hơn.

Hình 5-4. Thiết bị kết nối mạng HUB.

- *HUB thụ động:* Các HUB thụ động hoạt động như các điểm kết nối, chúng không tái tạo hoặc khuếch đại tín hiệu.
- *HUB lai:* Các HUB thích ứng với nhiều loại cáp khác nhau được gọi là HUB lai.

#### *5.2.1.3 Cầu nối (Bridge)*

Cầu nối là một thiết bị hoạt động ở tầng liên kết dữ liệu. Dùng để nối hai hoặc nhiều đoạn (*segment*) của mạng LAN khác nhau.

Hình 5-5. Cầu nối.

- Chức năng của cầu nối :

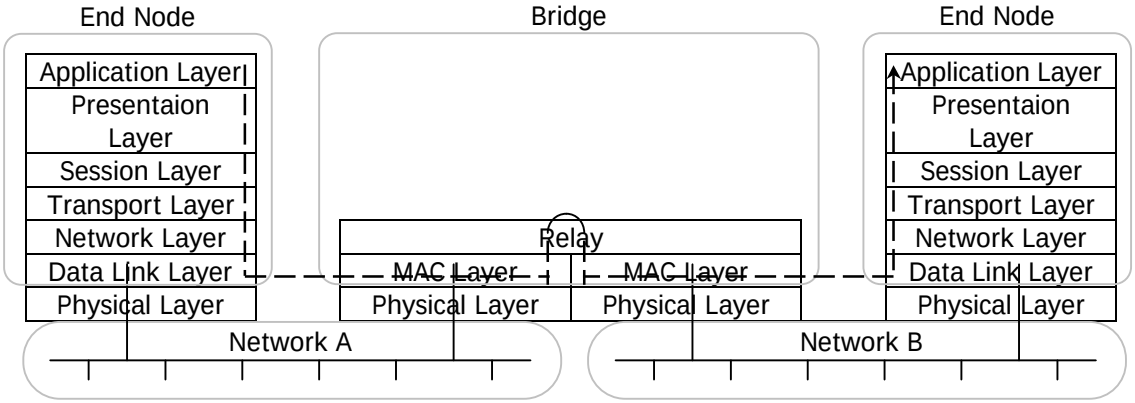
- Mở rộng khoảng cách của phân đoạn mạng, tăng số lượng máy tính trên mạng.
- Lọc những gói dữ liệu để gửi đi (hay không gửi) cho đoạn nối, hoặc gửi trả lại nơi xuất phát.
- Phân chia một mạng lớn thành hai mạng nhỏ nhằm cô lập lưu lượng, tăng tốc độ mạng. Nếu lưu lương từ một nhóm máy tính trở nên quá tải và làm giảm hiệu suất toàn mạng thì cầu nối có thể cô lập máy tính hoặc bộ phận này.
- Làm giảm hiện tượng tắc nghẽn do số lượng máy tính nối vào mạng qua lớn : Cầu nối có thể tiếp nhận một mạng quá tải và chia nó thành hai mạng riêng biệt, nhằm giảm bớt lưu lượng truyền trên mỗi đoạn mạng và do đó mỗi mạng sẽ hoạt động hiệu quả hơn.
- Kết nối các phương tiện truyền dẫn khác nhau, như cáp xoắn đôi và cáp quang.
- Kết nối các đoạn mạng sử dụng phương thức truy nhập đường truyền khác nhau, chẳng hạn CSMA/CD và chuyển thẻ bài.

- Nguyên lý hoạt dộng

- Cầu nối không phân biệt giữa giao thức này với giao thức khác, chỉ có nhiệm vụ chuyển lưu lượng của tất cả các giao thức dọc theo mạng. Vì giao thức nào cũng di chuyển ngang qua cầu nối, nên tuỳ thuộc vào từng máy tính quyết định chúng có thể nhận diện được giao thức nào.

- Cầu nối hoạt động trên nguyên tắc mỗi nút mạng có một địa chỉ riêng. Cầu nối chuyển gói dữ liệu dự trên địa chỉ của nút đích (địa chỉ MAC). Khi dữ liệu truyền qua cầu nối, thông tin địa chỉ của máy tính được lưu trong RAM của cầu nối dùng để xây dựng bảng địa chỉ dựa trên địa chỉ nguồn của gói tin.

Giao diện Bridge chỉ chứa tầng 1 và tầng con MAC, có chức năng chuyển đổi khuôn dạng của các đơn vị dữ liệu (frame) của các giao thức khác nhau và gửi chúng tới các mạng cục bộ đích có kèm theo phối hợp tốc độ.




Hình 5-6. Sơ đồ kiến trúc của Bridge trong mô hình OSI.

Ví dụ một Bridge nối giữa IEEE 820.3 và IEEE 820.5. Cầu nối này có hai card mạng: card Token Ring và card Ethermet để giao tiếp với hai mạng.

### *5.2.1.4 Bộ dẫn đường (router)*

Trong môi trường gồm nhiều đoạn mạng với giao thức và kiến trúc mạng khác nhau, cầu nối không thể đảm bảo truyền thông nhanh trong tất cả các đoạn mạng. Mạng có độ phức tạp như vậy cần một thiết bị không những biết địa chỉ của mỗi đoạn mạng, mà còn quyết định tuyến đường tốt nhất để truyền dữ liệu và lọc lưu lượng quảng bá trên các đoạn mạng cục bộ. Thiết bị như vậy được gọi là bộ định tuyến.

Hình 5-7. Bộ định tuyến.

- Chức năng của bộ định tuyến :

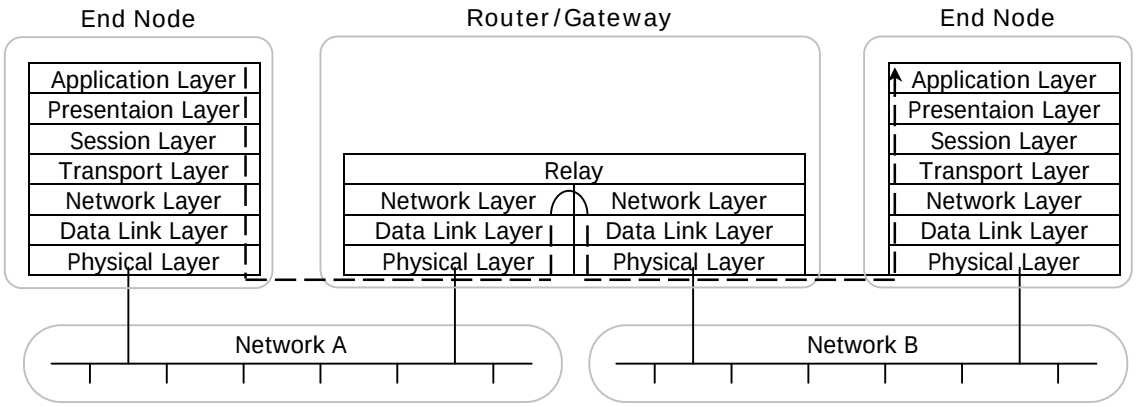
- Chuyển đổi và định tuyến gói dữ liệu qua nhiều mạng dựa trên địa chỉ phân lớp của mạng, cung cấp các dịch vụ như bảo mật, quản lý lưu thông...
- Phân chia một mạng lớn thành nhiều mạng nhỏ, và có thể kết nối nhiều đoạn mạng với nhau.
- Lọc gói tin và cô lập lưu lượng mạng : hoạt động như một rào cản an toàn giữa các đoạn mạng ( do có thể lọc dữ liệu).
- Ngăn chặn tình trạng quảng bá vì chúng không chuyển tiếp các gói tin quảng bá, cải thiện việc phân phát gói dữ liệu.
- Các bộ định tuyến có thể chia sẽ thông tin trạng thái và thông tin định tuyến với nhau và sử dụng thông tin này để bỏ qua các kết nối hỏng hoặc chậm.

- Nguyên lý hoạt động :

Trong bộ định tuyến có một bảng định tuyến chứa các địa chỉ mạng. Tuy nhiên, địa chỉ mạng có thể được lưu trữ tuỳ thuộc vào giao thức mạng đang chạy. Bộ định tuyến sử dụng bảng định tuyến để xác định địa chỉ đích cho dữ liệu nhận được. Bảng này liệt kê các thông tin sau:

- Địa chỉ mạng đã kết nối.
- Cách kết nối tới các mạng khác.
- Phí tổn truyền dữ liệu qua các lộ trình đó.

Khi bộ định tuyến nhận được một gói dữ liệu cần gởi đến mạng ở xa, nó kiểm tra bảng đinh tuyến và chọn đường đi tối ưu (theo một tiêu chuẩn nào đó) để gởi gói dữ liệu đến đích.




Hình 5-8. Sơ đồ kiến trúc của Router trong mô hình OSI.

- Truyền dữ liệu qua bộ định tuyến

Trong mọi trường hợp, khi một trạm xác định rằng nó phải gởi một gói dữ liệu tới một trạm trên một mạng khác. Công việc đầu tiên trạm này cần làm là lấy địa chỉ vật lý MAC của Router (địa chỉ cổng nối ngầm định). Sau đó nó điền thông tin trong trường địa chỉ vật lý đích của gói dữ liệu bằng địa chỉ vật lý MAC của Router, và trường thông tin địa chỉ đích ở tầng mạng (chẳng hạn địa chỉ IP nếu dùng giao thức TCP/IP) bằng địa chỉ của trạm đích.

Khi Router kiểm tra địa chỉ đích, nó xác định xem nó biết hay không biết cách chuyển tiếp gói dữ liệu đến bước nhảy tiếp theo (Router kế tiếp trên đường đi) bằng cách kiểm tra địa chỉ. Nếu địa chỉ mạng đích nằm trong gói dữ liệu không có bảng định tuyến, Router thường bỏ gói dữ liệu đi. Trong trường hợp địa chỉ mạng đích có bảng định tuyến, Router thay địa chỉ vật lý đích bằng địa chỉ vật lý của bước nhảy tiếp theo và truyền gói dữ liệu đến bước nhảy tiếp theo.

Như vậy, khi một gói tin được chuyển qua liên mạng, địa chỉ vật lý đích của nó thay đổi, nhưng địa chỉ của giao thức không đổi.

Bộ định tuyến được chia thành 2 loại, tuỳ theo cách sử dụng chúng. Bộ định tuyến cục bộ (Local Router) nối các đoạn mạng ở gần nhau. Hai bộ định tuyến ở xa nhau (Remote Router) nối hai đoạn mạng ở xa qua các kênh truyền thông.

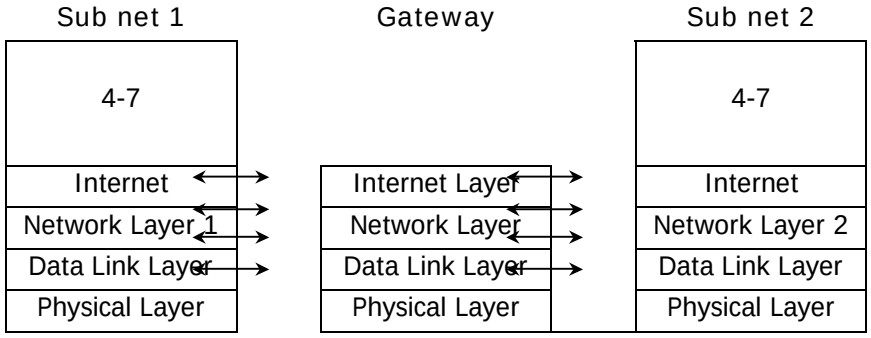
#### *5.2.1.5 Bộ chuyển mạch*

Chức năng chính của bô chuyển mạch (switch) là cùng một lúc duy trì nhiều cầu nối giữa các thiết bị mạng bằng cách dựa vào một loại đường truyền xương sống (backbone) nội tại tốc độ cao. Switch có nhiều cổng, mỗi cổng có thể hỗ trợ toàn bộ Ọthernet LAN hoặc Token Ring. Bộ chuyển mạch kết nối một số LAN riêng biệt và cung cấp khả năng lọc gói dữ liệu giữa chúng.

Các bộ chuyển mạch là loại thiết bị mạng mới, hiện đang được sử dụng rộng rãi vì Switch cho phép chuyển sang chế độ truyền không đồng bộ ATM.

#### *5.2.1.6 Gateway*

Hoạt động ở mức mạng, thực hiện ghép nối với WAN. Nguyên lý chung của nối kết này là tạo ra 1 tầng "*liên mạng*" (internet) chung trong tất cả các kiến trúc của mạng con tham gia nối kết. Tầng liên mạng thường là tầng con nằm ngay trên tầng 3 mô hình OSI.




Hình 5-9. Sơ đồ kiến trúc của gateway trong mô hình OSI.

Tầng con Internet được cài đặt trong tất cả các trạm cũng như trong các giao diện kết nối (gateway), Tầng này cung cấp dịch vụ truyền thông liên mạng với hai chức năng chính :

- Chuyển đổi các đơn vị dữ liệu của giao thức (Protocol Data Unit - PDU)
- Chọn đường đi cho các PDU này.

Các gói tin ở tầng con Internet lưu thông trong mạng theo phương pháp '*gói/bóc*' (encapsulation/decasulation). Khi một datagram được truyền từ mạng con này sang mạng con khác thông qua gateway thì nó được bổ sung thêm vào (hoặc tách ra) các phần thông tin điều khiển cần thiết tương ứng với các mạng con.

## 5.3 Giao thức liên mạng IP

Giao thức IP (Internet Protocol) hoạt động ở tầng mạng, cung cấp dịch vụ dữ liệu không liên kết (connectionless) cho nhiều giao thức liên kết dữ liệu khác. Đơn vị dữ liệu dùng trong giao thức IP được gọi là *datagram*, hay còn gọi là khung tin IP.

- Chức năng của giao thức IP :

- Định nghĩa gói tin Datagram là đơn vị dữ liệu cơ bản của việc truyền tin trên mạng Internet.
- Xác định mô hình đánh địa chỉ cho các khung tin và quản lý các quá trình trao đổi, xử lý các khung tin này.
- Chọn đường cho các datagram trên mạng
- Cung cấp cơ chế trên gói tin trên mạng hiệu quả nhất.
- Phân đoạn và tổng hợp các gói tin.

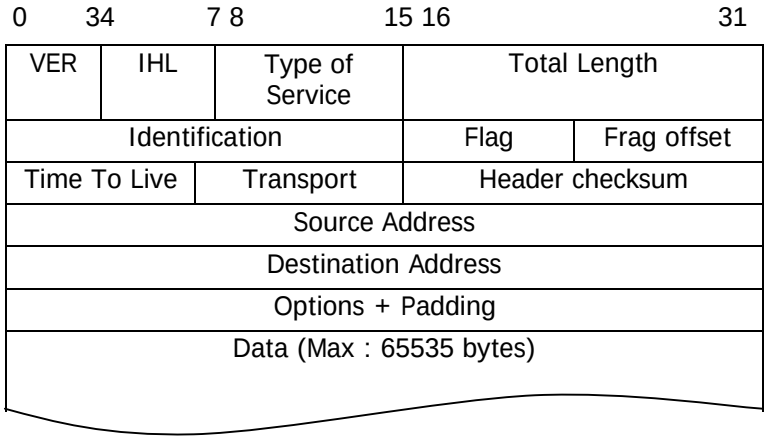
- Tính chất của giao thức IP :

- Hoạt động theo phương thức không kết nối : IP không chuyển các thông tin điều khiển trước khi truyền dữ liệu.

- Không tin cậy : giao thức IP không có khả năng phát hiện và khắc phục lỗi., không quan tâm đến vấn đề dữ liệu có được nhận một cách chính xác hay không. Do đó, các gói dữ liệu có thể bị thất lạc, bị trùng lặp, bị chuyển chậm hoặc đi không đúng thứ tự, mỗi gói dữ liệu được xử lý độc lập với nhau và có thể gửi theo những đường định tuyến khác nhau.

### 5.3.1 Cấu trúc khung tin IP

IP Header được gắn cho mỗi datagram, chứa các thông tin cần thiết cho sự hoạt động của gói tin trên mạng. Cấu trúc khung tin IP như hình sau :




Hình 5-10. Cấu trúc khung tin IP.

*VER (4 bit)*

Chứa phiên bản giao thức IP đang dùng. Phiên bản hiện nay là IPV4.

Một phần của giao thức IP quy định rằng phần mềm nhận dữ liệu trước tiên phải kiểm tra phiên bản của IP trong các khung tin đến, trước khi phân tích tiếp phần còn lại của Header và dữ liệu. Nếu như không đúng phiên bản thì lớp IP của máy nhận sẽ từ chối và bỏ qua toàn bộ nội dung của khung tin đến.

*IHL (Internet Header length) (4 bit)*

Chứa chiều dài của Header IP do máy gửi dữ liệu tạo nên, chiều dài này được tính theo các word có chiều dài 32 bit. Header ngắn nhất có chiều dài là 5 word (20 byte), nhưng do việc dùng các trường lựa chọn có thể làm tăng chiều dài của Header lên đến 6 word (24 byte). IHL dùng để giao thức IP được vị trí kết thúc của Header và bắt đầu phần dữ liệu của khung tin.

*Type of Service - Loại dịch vụ (8 bits)*

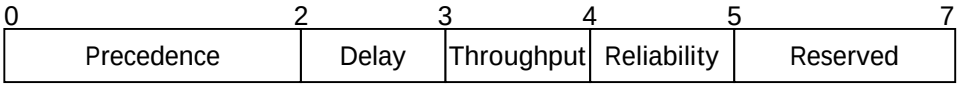
Trường này chứa các thông tin về quyền ưu tiên của việc truyền datagram và các ảnh hưởng có thể xảy ra trong quá trình truyền các datagram

đó. IP chuẩn không yêu chỉ ra các hành động cụ thể dựa trên giá trị của trường *Type of Service*. IP chỉ định sử dụng nó trong việc thiết lập các tuỳ chọn cho các mạng con và nó sẽ truyền qua trong bước nhảy tới.

Ví dụ, việc truy nhập vào mạng Token Ring cần thiết có các mức độ ưu tiên được xác định. IP có thể chuyển các mức độ ưu tiên của nó sang các mức độ ưu tiên tương ứng của mạng Token Ring.

Một số máy tính và bộ chọn đường (*router*) không quan tâm đến giá trị của trường này trong khi một số khác lại dựa vào đây để quyết định đường truyền.

Cấu trúc của trường như sau :




Cấu trúc của trường Type of Service

Precedence (3 bít) : chỉ thị về quyền ưu tiên gửi datagram, cụ thể là :

111 - Network Control (cao nhất) 011 - Flash
110 - Internetwork Control 10 - Immediate
101 - CRITIC/ECP 001 - Priority
100 - Flag Overrride 000 - Routime (thấp nhất)

D (Delay) - 1 bit : chỉ độ trễ yêu cầu
D = 0 độ trễ bình thường
D = 1 độ trễ thấp

T (Throughput) - 1 bit : chỉ thông lượng yêu cầu
T = 0 thông lượng bình thường
T = 1 thông lượng cao

R (Reliability) - 1 bít chỉ độ tin cậy yêu cầu
R = 0 độ tin cậy bình thường
R = 1 độ tin cậy cao

Ba bit đầu tiên của trường này là để chỉ ra quyền của khung tin đó, với các giá trị từ 0 (bình thường) đến 7 (Mạng điều khiển). Nếu giá trị của phần này càng cao thì khung tin đó càng quan trọng và trên lý thuyết thì khung tin này phải được chuyển đến đích nhanh hơn. Nhưng trên thực tế thì TCP/IP và các phần cứng dùng giao thức TCP/IP đều bỏ qua trường này và coi tất cả các khung tin có độ ưu tiên như nhau.

Ba bit tiếp theo là ba cờ 1-bit để điều khiển thời gian trễ, độ tin cậy, và thông lượng (throughput) của khung tin. Nếu tất cả các bit đều là 0 thì có nghĩa là đặt ở chế độ bình thường. Nếu bit thứ nhất là 1 thì có nghĩa là thời gian trễ thấp, truyền nhanh và độ tin cậy cao cho từng cờ. Còn hai bit còn lại của trường này không dùng. Phần lớn các bit của trường này đều bị bỏ qua khi thực hiện IP, và tất cả các khung tin đều được đặt thời gian trễ, thời gian truyền, và độ tin cậy như nhau.

Trong thực tế, hầu hết tất cả các bit của trường loại dịch vụ đều được đặt về giá trị 0 bởi vì sự khác nhau về quyền, thời gian trễ, thời gian truyền, độ tin cậy giữa các máy hầu như không tồn tại trừ khi một mạng mới được thành lập.

*Total Length (16 bits) - Chiều dài gói tin*

Trường này cho biết toàn bộ chiều dài của khung tin (datagram) bao gồm phần Header và phần dữ liệu, đơn vị tính bằng byte. Độ lớn của trường này là 16 bit do đó mà chiều dài của khung tin tối đa là 65535 byte.

*Indentification (16 bits) -Trường định danh*

Trường này chứa một giá trị đặc trưng do máy gửi khung tin tạo ra, cùng với các tham số khác (như Source Address và Destination Address), tham số này dùng để định danh duy nhất một khung tin trong khoảng thời gian nó tồn tại trên liên mạng.

Số trong trường này được cần đến khi sắp xếp các khung tin để đảm bảo rằng các khung tin không bị lẫn lộn với nhau. Khi lớp IP nhận được một đoạn dữ liệu từ các lớp cao hơn thì nó sẽ gán các số định danh này vào. Nếu như khung tin đã được tách (bằng kỹ thật tách thông tin) thì tất cả các khung tin sẽ mang cùng một số định danh như nhau.

*Flags (3 bits) - Các cờ*

Trường này có chiều dài 3 bit, liên quan đến sự phân đoạn các datagram.

Bit 0 : Dùng để dự trữ - chưa sử dụng, luôn có giá trị 0

Bit 1 : (DF) = 0 (May Fragment)

=1 (Don’t Fragment)

Bit 2 : (MF) = 0 (Last Fragment)

=1 (More Fragment)

Nếu như cờ DF có giá trị là 1 thì có nghĩa là khung tin không thể tách ra được trong bất cứ trường hợp nào. Nếu như mà phần mềm của lớp IP hiện tại không thể gửi khung tin đến nới nhận nếu như không tách ra, mà hiện tại bit cờ đang là 1 thì khi đó khung tin sẽ bị huỷ bỏ và một thông báo lỗi được gửi đến thiết bị phát.

Nếu router không thể truyền nguyên cả một datagram mà bit này được thiết lập bằng 1 thì datagram đó sẽ bị loại bỏ và nó sẽ có một thông báo lỗi gửi đến máy phát. Bất kì một người quản lý mạng nào cũng có thể sử dụng cách này để kiểm tra độ lớn của các datagram có thể được truyền trên các phần khác nhau trên mạng kết hợp.

Nếu như cờ MF là 1 có nghĩa là khung tin hiện tại vẫn đang còn các gói tin khác nữa đang đến, do đó mà phải cần đến việc sắp xếp lại để khôi phục lại message ban đầu. Khung tin cuối cùng đến sẽ lớn hơn các khung tin bình thường vì nó còn chứa thêm phần MF=0 để báo cho máy nhận biết là đã hết các khung tin cần thiết không cần phải đợi thêm nữa. Có thể là các khung tin đến không đúng với thứ tự chúng đã được phát đi, do đó cờ MF còn được dùng cùng với trường Fragment Off để chỉ cho máy nhận được thứ tự của toàn bộ message ban đầu.

*Fragment Offset (13 bits)*

Nếu mà cờ MF bằng 1 (tức là có sự tách thông tin từ một khung tin lớn), khi đó fragment offset chứa .vị trí của các message con trong message ban đầu trong khung tin hiện thời. Điều này cho phép IP sắp xếp lại các khung tin thành message ban đầu t theo đúng trật tự.

Offset thường được để ở đầu message. Trường này có chiều dài là 13 bit, do vậy offset được tính theo đơn vị 8 byte, tương ứng với gói lớn nhất là 65535 byte. Việc dùng số định danh để chỉ rằng khung tin đến là thuộc bản tin nào, lớp IP ở máy nhận có thể dùng fragment offset để sắp xếp lại message ban đầu.

*TTL (Time to Live - Thời gian sống)*

Trường này cho biết khoảng thời gian tính bằng giây mà một khung tin có thể tồn tại trên mạng trước khi nó bị huỷ bỏ. Giá trị này được nút gửi khung tin đi ấn định.

Các chuẩn của TCP/IP quy định rằng trường TTL phải được giảm đi ít nhất là 1 giây cho mỗi nút xử lý khung tin đó, thậm chí là thời gian xử lý có thể nhỏ hơn 1 giây. Khi một gateway nhận được một khung tin thì thời gian đến được đính vào khung tin do đó nếu như khung tin đó phải chờ để được xử lý. Bởi vậy nếu một gateway nào đó mà bị quá tải và không thể lấy khung tin về, khi đó bộ đếm thời gian của trường TTL sẽ tự động giảm đi trong quá trình chờ để được xử lý. Nếu trường TTL giảm về 0 thì khi đó khung tin đó phải được nút hiện thời hủy bỏ, sẽ có một thông báo gửi về máy gửi.

Hầu hết các TCP/IP cài đặt giá trị trường TTL khoảng 60 hoặc cao hơn, nghĩa là datagram có thể đi qau 60 router hay hop để đến đích. Trường TTL được thiết kế để tránh việc các gói dữ liệu cứ chuyển vòng quanh trên mạng mà không có đường ra.

*Giao thức giao vận (Transport Protocol)*

Trường này chứa số định danh của giao thức giao vận mà đã xử lý khung tin. Số định danh này do trung tâm thông tin mạng Internet NIC ấn định. Hiện nay đã có khoảng 50 giao thức giao vận được ấn định. Hai giao thức quan trọng nhất là : ICMP (Internet Control message Protocol) và TCP.

*Header checksum*

Dùng để tính checksum của trường Header để làm cho quá trình xử lý thông tin được nhanh hơn. Do trường TTL bị giảm đi 1 giây mỗi khi được xử lý, trường checksum cũng thay đổi tại các máy mà khung tin đi qua. Thuật toán checksum là một thuật toán nhanh và có hiệu quả, nhưng có một số trường hợp bị sai chẳng hạn mất hoàn toàn một từ 16 bit mà 16 bit này đều bằng 0. Tuy nhiên trường checksum do cả TCP và UDP để đóng gói, các lỗi này sẽ được phát hiện khi khung tin được tập hợp để truyền trên mạng.

*Source Address (32 bits) :* chứa địa chỉ IP 32 bit của máy gửi.

*Destination Address (32 bits) :* chứa địa chỉ IP 32 bit của máy nhận.

Hai trường trên được tạo ra cùng với khung tin và không bị thay đổi trong quá trình truyền.

*Options (32 bits) - Phần lựa chọn*

Phần lựa chọn được tạo ra từ một vài mã mà các mã này có độ dài có thể thay đổi được. Nếu như có nhiều lựa chọn trong khung tin, thì các lựa chọn đó được đặt liên tục nhau trong phần Header của IP. Tất cả các lựa chọn này được điều khiển bằng một byte có ba trường: ***Cờ copy*** có độ dài 1 bit, ***loại lựa chọn*** có độ dài 2 bit, và ***trường số lựa chọn*** có độ dài 5 bit. Trường cờ copy được dùng để quy định là lựa chọn sẽ được thực hiện như thế nào nếu ở một gateway nào đó cần đến kỹ thuật tách thông tin. Nếu như cờ này có giá trị là 0 thì có nghĩa là lựa chọn đó sẽ được copy vào khung tin thứ nhất mà không copy vào các khung tin tiếp theo sau. Nếu như cờ này có giá trị là 1 thì có nghĩa là lựa chọn đó sẽ được sao chép vào tất cả các khung tin.

Các lựa chọn quan trọng là Record route và Timestamp.

*Record route*

Trường Record Route (*Bản ghi chọn đường)* chứa danh sách dự trữ của các route mà datagram đã đi qua trên đường tìm tới đích. Mỗi lần đi qua một router thì trường này sẽ bổ sung một địa chỉ của router đó vào danh sách của nó. Độ dài của trường này do máy nguồn xác lập, do đó rất có thể là nó sẽ bị

đầy trước khi datagram tìm được đến đích. Trong trường hợp này thì các địa chỉ của các router sau sẽ không được thêm vào danh sách của nó.

*Timestamp :* Có 3 định danh cho trường Timestamp. Trường này có thể chứa:

- Danh sách của 32 bit Timestamp.
- Danh sách của địa chỉ IP và các cặp Timestamp tương ứng.

Danh sách của các địa chỉ cho trước bởi máy nguồn. Một nút bất kỳ được ghi vào trường này chỉ khi địa chỉ của nó là mục kế tiếp trong danh sách này. Trường này có thể bị đầy nếu rơi vào hai trường hợp đầu, trong trường hợp này sẽ có trường ghi tràn (overllow field) dùng để đếm số nút mà không thể ghi vào timestamp được.

*Padding (Độ dài thay đổi)*

Nội dung của phần **Padding** phụ thuộc vào phần **Options** như thế nào. Phần Padding thường được dùng để bảo đảm rằng chiều dài Header của khung tin luôn là một số nguyên bội số của 32.

*Data* : Vùng dữ liệu có độ dài thay đổi, nhưng luôn là bội số của 8 bits, và tối đa là 65535 bytes.

### 5.3.2 Địa chỉ IP

Mỗi thiết bị nối vào mạng TCP/IP được gán một địa chỉ IP duy nhất (mỗi card mạng sẽ có địa chỉ IP riêng). Khi sử dụng mạng cục bộ không kết nối với các mạng khác, người sử dụng có thể gán địa chỉ IP tuỳ ý cho các máy trạm. Tuy nhiên, đối với các site Internet thì địa chỉ IP phải được cung cấp từ trung tâm quản lý thông tin mạng trên thế giới (NIC - Network Information Center).

Địa chỉ của IP có độ dài 32 bit, được chia làm 4 phần, mỗi phần 1 byte, phân cách nhau bằng dấu chấm. Dạng tổng quát : ***x.y.z.t*** với $0 \leq x,y,z,t \leq 255$

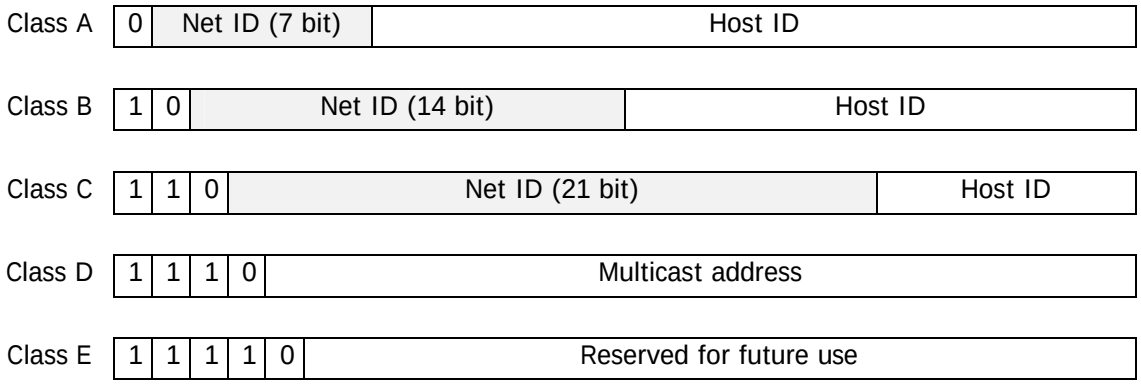
*Ví dụ:* 128.83.12.14 hoặc 0x80530C0E Hex.

Địa chỉ IP bao gồm hai phần thông tin: địa chỉ mạng (network address) và địa chỉ máy (host address): NetworkID.HostID

Khi đề nghị NIC cung cấp địa chỉ IP ta sẽ không nhận được địa chỉ tương ứng của máy trạm, thay vào đó là địa chỉ mạng và ta có quyền gán địa chỉ cho các máy trạm của mạng trong phạm vi địa chỉ được cung cấp.

#### *5.3.2.1 Các lớp địa chỉ IP*

Địa chỉ IP thuộc một trong E lớp địa chỉ, từ lớp A đến E. Các lớp địa chỉ nhằm để phân loại các mạng có quy mô khác nhau.




Hnh 5-11. Các lớp địa chỉ IP.

1. Lớp A (1≤ x ≤ 126) : NetworkID= x, HostID=y.z.t

- Cho phép định danh 126 mạng, với tối đa $2^{24}$ (= 167.772) máy trạm trên mỗi mạng, lớp A giới hạn số subnetwork trong Internet.
- Các mạng lớp A thuộc loại mạng diện rộng (very large), như mạng quốc gia

2. Lớp B (128≤ x ≤ 191) : NetworkID= x.y, HostID=z.t

- Cho phép định danh đến 16384 mạng, với tối đa $2^{16}$ (=65.536) host trên mỗi mạng.
- Mạng lớp B thuộc loại mạng trung bình như mạng University Campuses.

3. Lớp C (192 ≤ x ≤ 223) : NetworkID= x.y.z, HostID=t

- Giới hạn số trạm trong mạng lớn nhất là 256, có 21 bit cho địa chỉ mạng. Cho phép định danh đến 2 triệu mạng, với tối đa 254 host trên mỗi mạng.
- Mạng lớp C được sử dụng cho các loại LAN, như các mạng Enterprise-wide.

4. Lớp D (224≤ x ≤ 239)

- Địa chỉ lớp D dùng cho các giao thức đặc biệt (Internet Group management Protocol - IGMP) và các giao thức khác.

5. Lớp E (240≤ x ≤ 255) : Để dành cho sự phát triển về sau.

- Các máy trong cùng một mạng phải có địa chỉ mạng giống nhau.
- Các mạng khác nhau có địa chỉ mạng khác nhau.

#### *5.3.2.2 Các địa chỉ IP đặc biệt*

1. Địa chỉ quay vòng : 127.y.z.t

Tất cả các gói tin được gửi đến địa chỉ 127.0.0.0 sẽ được gửi ngược trở lại máy tính. Gói tin này được sao chép từ nơi truyền đến bộ đệm nơi nhận trên cùng một máy tính. Địa chỉ loopback có thể được sử dụng như một địa chỉ kiểm tra

nhanh xem phần mềm TCP/IP có được cấu hình thích hợp. Trên hệ điều hành Windows địa chỉ loopback là 127.0.0.1 còn Unix là 127.1.*.

2. Mặt nạ mạng (Netmask)

***Mặt nạ mạng*** của một địa chỉ IP là một giá trị 32 bits trong đó các bit tương ứng với phần địa chỉ mạng bằng 1, các bit của phần máy bằng 0.

Ví dụ : Địa chỉ IP lớp B có mặt nạ mạng là 255.255.255.0 sẽ cho địa chỉ mạng con là 180.10.15.0

3. Địa chỉ quảng bá (broadcast address)

Địa chỉ này có các bit của phần HostID bằng 1, được sử dụng khi muốn chuyển một gói tin đến mọi máy tính trong mạng con.

Ví dụ một mạng con có địa chỉ là 180.10.0.0 sẽ có địa chỉ quảng bá là 180.10.255.255. Tương tự, một mạng con có địa chỉ là 180.10.15.0 sẽ có địa chỉ quảng bá là 180.10.15.255.

Đặc biệt địa chỉ 255.255.255.255 quảng bá cục bộ (local broadcast) hay còn gọi là limited broadcast có thể sử dụng trong các LAN.

Địa chỉ 0.0.0.0 cũng được sử dụng trong bảng định tuyến để chỉ đến điểm vào mạng cho địa chỉ bộ định tuyến mặc định.

## 5.4 Phân chia mạng con

Để thuận tiện cho việc quản lý và định hướng dữ liệu trên mạng lớn, người ta thường tổ chức mạng IP theo cơ chế địa chỉ phân cấp : mỗi mạng được chia nhỏ thành nhiều mạng con, mỗi mạng con thực hiện các dvc về địa chỉ trong nội bộ mạng đó. Sự phân cấp này cho phép giảm khối lượng công việc chọn đường cho các gói tin trong toàn liên mạng.

Mỗi mạng con chịu trách nhiệm cho việc chọn đường cho các gói tin IP trong mạng của mình, các gói tin này được nhận ra nhờ phần địa chỉ mạng của nó. Trong các mạng loại A, B, C thì phần địa chỉ này có độ dài cố định. Tuy nhiên, để tạo sự linh hoạt trong việc phân chia mạng con thì địa chỉ mạng có thể mở rộng sang các bit của địa chỉ máy. Đó là kỹ thuật phân chia mạng con.

Ví dụ một mạng loại B có địa chỉ mạng là 203.160.9.0 và mặt nạ mạng là 255.255.255.0 (địa chỉ mạng dài 24 bit). Người ta cần chia mạng này thành 4 mạng cục bộ riêng, do đó sẽ lấy thêm 2 bit cho địa chỉ mạng (26 bit). Vậy ta có địa chỉ các mạng con này là :

Địa chỉ mạng 1 :

| 203 | 160 | 9 | 0 |
|---|---|---|---|
| 11001011 | 10100000 | 00001001 | 00000000 |

Địa chỉ mạng 2 :

| 203 | 160 | 9 | 64 |
|---|---|---|---|
| 11001011 | 10100000 | 00001001 | 01000000 |

Địa chỉ mạng 3 :

| 203 | 160 | 9 | 128 |
|---|---|---|---|
| 11001011 | 10100000 | 00001001 | 10000000 |

Địa chỉ mạng 4 :

| 203 | 160 | 9 | 192 |
|---|---|---|---|
| 11001011 | 10100000 | 00001001 | 11000000 |

Mặt nạ của các mạng con này là : 255.255.255.192

| 255 | 255 | 255 | 192 |
|---|---|---|---|
| 11111111 | 11111111 | 11111111 | 11000000 |

Việc phân chia mạng được tiến hành bởi người quản trị hệ thống và thường dựa trên ranh giới vật lý giữa các nhánh mạng. Khi có gói dữ liệu cần chuyển đi, bộ định tuyến sẽ dùng mặt nạ mạng để kiểm tra gói dữ liệu này thuộc mạng con nội bộ hay thuộc mạng ngoài. Sự phân chia mạng riêng thành các mạng con chỉ có ý nghĩa bên trong mạng đó.

Nếu kết nối Internet thông qua một mạng LAN, điều quan trọng là phải sử dụng đúng mặt nạ mạng. Cũng giống như địa chỉ IP, một mặt nạ mạng con có thể được gán một cách riêng lẻ hay có thể tự động thông qua DHCP (Dynamic Host Configuration Protocol).

## 5.5 Hoạt động của giao thức IP

Nếu địa chỉ đích của gói tin IP không nằm trên cùng mạng với máy chủ nguồn thì giao thức IP trong máy chủ hướng gói tin đến bộ định tuyến nội bộ. Nếu bộ định tuyến này không được nối đến mạng đích, gói tin sẽ được gởi đến một bộ định tuyến khác. Cứ thế cho đến khi tới trạm đích. Việc quy định truyền theo đường truyền nào của router dựa trên bảng đường truyền (*routing table*). Các bộ định tuyến có thể phát hiện :

- Một mạng mới đã được thêm vào liên mạng
- Đường dẫn đến trạm đích đã bị hỏng

Các bước thực hiện bởi một thực thể IP như sau :

- *Đối với thực thể IP ở trạm nguồn*

- Khi nhận được lệnh SEND từ tầng trên, nó thực hiện các bước như sau:
- Tạo một IP datagram dựa trên các tham số của lệnh SEND
- Tính checksum và ghép vàp phần đầu của datagram
- Ra quyết định chọn đường
- Chuyển datagram xuống tầng dưới

• *Đối với gateway*

- Khi nhận được datagram quá cảnh, nó thực hiện các tác động như sau :
- Tính checksum, nếu không đúng thì loại bỏ datagram
- Giảm giá trị tham số thời gian tồn tại. Nếu hết thời gian thì loại bỏ datagram
- Ra quyết định chọn đường
- Phân loại datagram nếu cần
- Kiến tạo lại phần đầu IP bao gồm giá trị mới của vùng TTL, checksum, Fragmentation.
- Chuyển datagram xuống tầng dưới để truyền qua mạng.

• *Tại trạm đích*

- Tính checksum, nếu không đúng thì loại bỏ datagram.
- Tập hợp các đoạn của datagram.
- Chuyển dữ liệu và các tham số điều khiển lên tầng trên.

Như vậy, do gói tin IP không sửa đổi, đơn giản nên hiệu suất đường truyền cao. Vì gói tin IP cung cấp dịch vụ giao nhận gói tin không tin cậy nên cần có giao thức ICMP để hỗ trợ, các bản tin ICMP được đóng gói và chuyển tải trong các gói tin IP. Tầng TCP đảm nhận việc bảo đảm các datagram được truyền đến đích một cách an toàn và đầy đủ.

## 5.6 Các giao thức liên quan đến IP

### 5.6.1 Giao thức phân giải địa chỉ ARP

Địa chỉ IP được dùng để *định danh các host và mạng ở tầng mạng* của mô hình OSI, và chúng không phải là các địa chỉ vật lý (hay địa chỉ MAC) của các trạm đó trên cùng một mạng cục bộ (Ethernet, Token Ring, ...). Trên một LAN như vậy, hai trạm chỉ có thể liên lạc với nhau nếu chúng biết địa chỉ vật lý của nhau.

Vấn đề đặt ra là phải thực hiện ánh xạ địa chỉ IP (32 bits) và địa chỉ vật lý (48 bits) của một trạm. Giao thức ARP (Address Resolution Protocol) đã được xây dựng để chuyển đổi từ địa chỉ IP sang địa chỉ vật lý khi cần thiết. Ngược lại, giao

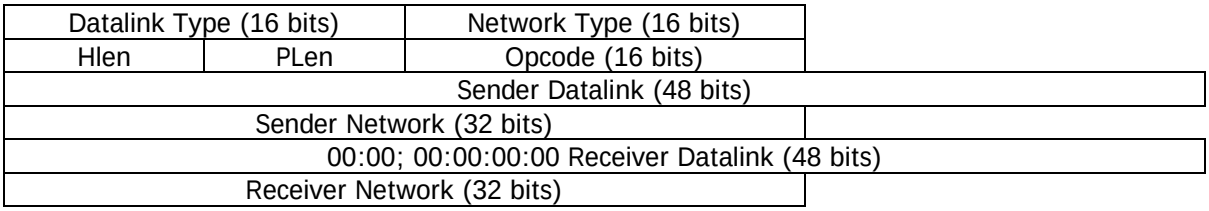
thức RARP (Reserse Address Resolution Protocol) được dùng để chuyển đổi từ địa chỉ vật lý sang địa chỉ IP.

Cả hai giao thức ARP và RARP đều không phải là bộ phận của IP, IP sẽ dùng đến chúng khi cần.

Mỗi ghép nối mạng có *địa chỉ giao thức mạng* (IP address) và *địa chỉ giao thức liên kết dữ liệu* (Datalink Protocol Address) riêng. Do đó cần có bảng ánh xạ giữa hai địa chỉ này ( địa chỉ ảo và địa chỉ vật lý ). Bảng địa chỉ này có thể làm bằng tay, nhưng do khối lượng địa chỉ lớn, tăng khá nhanh, nên người ta giải quyết thông qua thủ tục "*Tìm giải pháp cho địa chỉ*" (Address Resolution Protocol -ARP).

Các gói tin ARP được đóng gói trong khung dữ liệu liên kết (data link frame). Đối với mạng Ethernet, kiểu trường (type field) sẽ là 0x0806.

ARP ánh xạ địa chỉ IP sang địa chỉ liên kết dữ liệu (datalink address). Trạm tin sẽ gửi gói tin yêu cầu ARP (request packet) với khuôn dạng gói tin như hình sau.



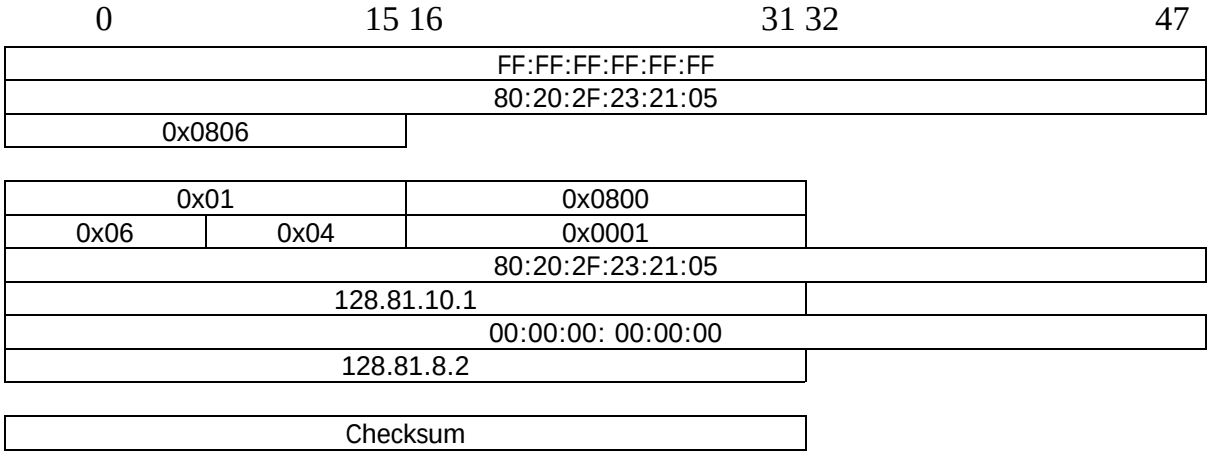

Hình 5-12. Khuôn dạng gói tin ARP.

- Data link type: Loại dữ liệu liên kết, với mạng Ethernet thì trường này có giá trị là 0x0001
- Network type : Loại địa chỉ mạng, Ethernet type used for IP (0x0800)
- Hlen : Độ rộng của phần địa chỉ dữ liệu liên kết, với mạng Ethernet độ rộng là 6 bytes
- Plen : Độ rộng của địa chỉ mạng, trong giao thức IP, phần này là 4 byte
- Opcode : Có giá trị là 0x0001 cho thủ tục yêu cầu ARP, 0x0002 cho ARP trả lời.
- Sender datalink and sender network : Địa chỉ vật lý và địa chỉ ảo (địa chỉ mạng) của người gửi
- Receive datalink and receive network : Địa chỉ vật lý và địa chỉ ảo (địa chỉ mạng) của người nhận

*Ví dụ:* Trạm A muốn gửi trạm B một gói tin IP. Cả hai máy A, B đều có cùng có địa chỉ mạng IP và cùng kết nối vào mạng Ethernet như hình sau :

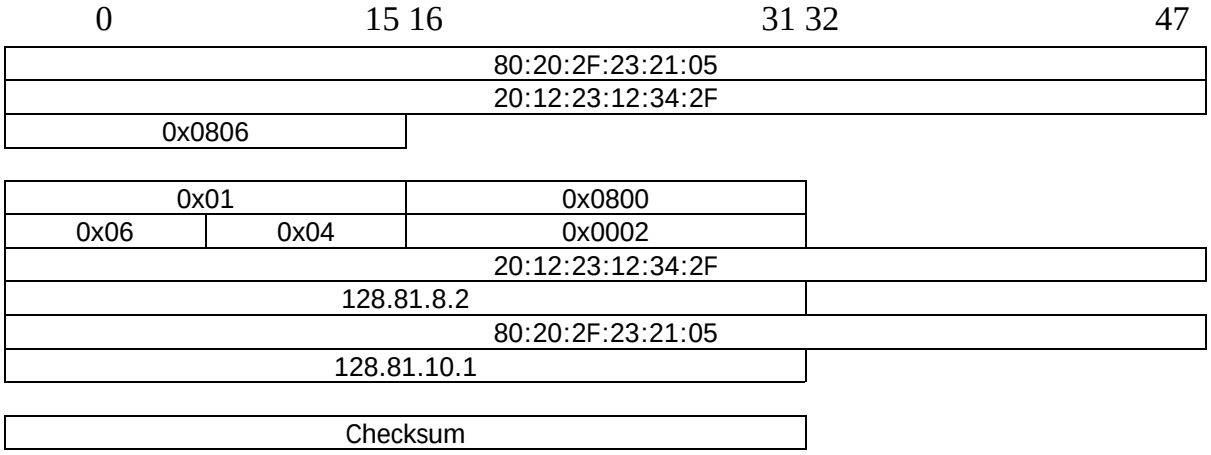
Trạm A biết được địa chỉ mạng của trạm B nhưng không biết địa chỉ vật lý của trạm B. Trạm A cần hỏi địa chỉ vật lý của trạm B để gửi tin. Khi đó trạm A phát đi một gói tin ARP yêu cầu (ARP request packet) đóng gói trong khung tin Ethernet.

- Quá trình gởi yêu cầu ARP




Hình 5-13. Khuôn dạng gói tin ARP yêu cầu.

Gói tin yêu cầu ARP (ARP request packet) được gửi tới các trạm, chỉ trạm B là đúng địa chỉ IP. Trạm B sẽ tạo ARP trả lời :




Hình 5-14. Khuôn dạng gói tin ARP trả lời.

Trạm B bổ sung IP_ to_Ethernet Address entry của host A và ARP cache của B

Trạm A bổ sung IP_to_Ethernet Address entry của host B và ARP cache của A

Như vậy bảng ánh xạ tự động bổ sung những đường dẫn (entry) mới mà nó biết, đồng thời cũng huỷ bỏ những đường dẫn (entry) mà nó không dùng đến.

### 5.6.2 Giao thức RARP (Reverse Address Resolution Protocol)

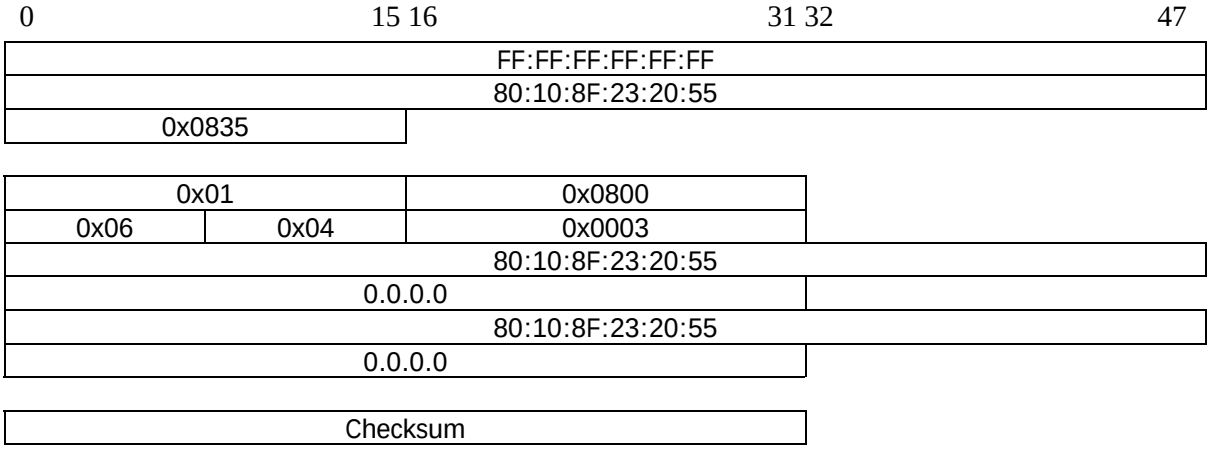
Đôi khi ta cần ánh xạ ngược lại.

Ví dụ một trạm không ổ đĩa, biết địa chỉ vật lý (datalink address) tức là địa chỉ card mạng giữ ở bộ nhớ ROM, nhưng không biết địa chỉ IP vì không có ổ đĩa. Khi này cần ánh xạ từ địa chỉ vật lý sang địa chỉ mạng.

Ta cũng làm như trên, nhưng thay kiểu trường từ 0x0806 bằng 0835.

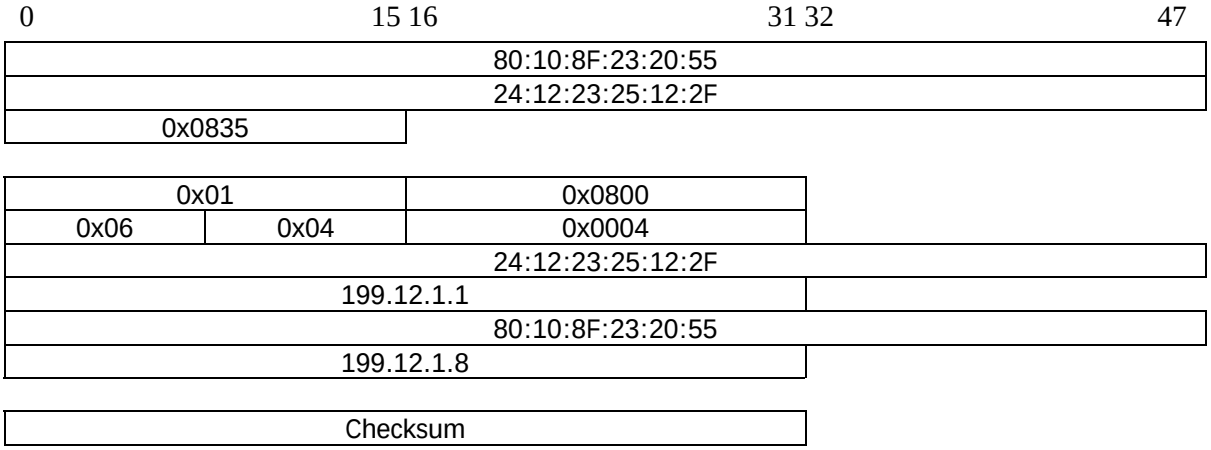
Yêu cầu chuyển đổi (reverse request) là 0x0003 và trả lời chuyển đổi (reverse reply) là 0x0004.

- Quá trình gởi yêu cầu RARP




Hình 5-15. Khuôn dạng gói tin RARP yêu cầu.

- Quá trình gởi trả lời RARP




Hình 5-16. Khuôn dạng gói tin trả lời RARP .

### 5.6.3 Giao thức ICMP

Giao thức ICMP (Internet Control Message Protocol) thực hiện truyền các thông tin điều khiển (các báo cáo về các tình trạng lỗi trên mạng, ...) giữa các

gateway hoặc các máy chủ trên liên mạng theo giao thức IP. Tình trạng lỗi có thể là: một datagram không thể đến được đích của nó, hoặc một router không đủ bộ nhớ đệm để lưu và chuyển một datagram, ... . Một thông báo ICMP được khởi tạo và chuyển cho IP. IP sẽ bọc (*encapsulate*) thông báo đó với một IP header và truyền đến cho router hoặc trạm đích.

#### *5.6.3.1 Ccác thành phần của thông báo ICMP hỗ trợ xác định lỗi và truy vấn*

Thông báo ICMP được chia làm 2 loại: thông báo lỗi ICMP và thông báo truy vấn ICMP.

Các thông báo ICMP khác nhau về định dạng tuỳ vào chức năng của từng loại, nhưng kiến trúc tổng quát bao gồm 2 phần: phần đầu (ICMP header) và phần dữ liệu (ICMP data).

Phần đầu của thông báo ICMP luôn bắt đầu bằng 3 trường:

a. TYPE: 8 bits, xác định loại thông báo ICMP.

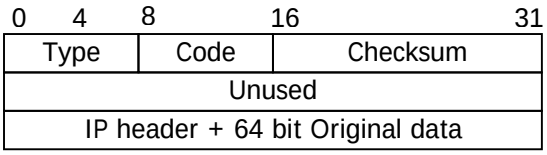
b. CODE: 8 bits, cung cấp thông tin chi tiết của từng loại thông báo ICMP.

c. CHECKSUM: 16 bits, xác định sự toàn vẹn dữ liệu trong quá trình truyền.

***1. Các thông báo lỗi ICMP***

Về mặt kỹ thuật, ICMP được thiết kế để cung cấp các thông tin về trạng thái không ổn định và thực hiện thông báo các trường hợp lỗi phát sinh của hệ thống phần cứng cũng như phần mềm làm ngăn chặn, huỷ bỏ quá trình gửi, nhận hoặc xử lý các datagram trên mạng Internet trước khi được chuyển đến đích cuối cùng.

Có 5 loại thông báo lỗi ICMP trong bảng I.1 và các thông báo có dạng chung như hình sau :




Hình 5-17. Dạng chung thông báo lỗi của ICMP

| Type | Thông báo lỗi ICMP |
|---|---|
| 3 | Destination Unreachable |
| 4 | Source Quench |
| 5 | Redirect |
| 11 | Time Exceeded |
| 12 | Parameter Problem |

***Bảng I.1***: Các loại thông báo lỗi của ICMP

Original IP header: 20-60 bytes chứa IP header của gói bị lỗi.

Original data: 8 bytes, chứa nội dung 64 bits đầu tiên của gói dữ liệu bị lỗi.

- *Destination Unreachable*

Các thông báo ICMP Destination Unreachable được tạo ra khi không thể chuyển đến 1 đích được xác định trong IP datagram. Bao gồm các loại lỗi sau:

| Code | Nội dung thông báo ICMP |
|---|---|
| 0 | Network Unreachable |
| 1 | Host Unreachable |
| 2 | Protocol Unreachable |
| 3 | Port Unreachable |
| 4 | Fragmentation needed and DF flag set |
| 5 | Source Route Fail |
| 6 | Destination Network unknown |
| 7 | Destination Host unknown |
| 8 | Source Host Isolated |
| 9 | Communication with Destination Network is Administratively Prohibited |
| 10 | Communication with Destination Host is Administratively Prohibited |

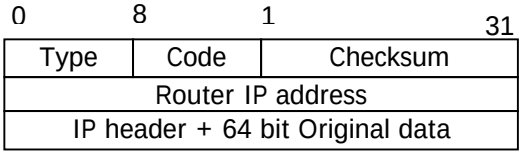
Bảng 5-1. Các lỗi của ICMP Destination Unreachable

- *Source Quench :* Khi vùng đệm của hệ thống nhận không đủ chỗ trống lưu trữ, hệ thống sẽ phát ra thông báo Source Quench. Trường CẶDỌ của thông báo này luôn luôn nhận giá trị 0.
- *Redirect :* Một thông báo ICMP Redirect được tạo ra bởi 1 router trong trường hợp nó nhận thấy rằng một máy tính đang sử dụng con đường định tuyến không tối ưu.

Trường CẶDỌ nhận 4 giá trị trong bảng và có định dạng như hình sau:

| Code | Nội dung |
|---|---|
| 0 | Redirect for the network (or subnet) |
| 1 | Redirect for the host |
| 2 | Redirect for the type of service and network |
| 3 | Redirect for the type of service and host |

Bảng 5-2. Các lỗi của ICMP Redirect




Hình 5-18. Dạng ICMP Redirect

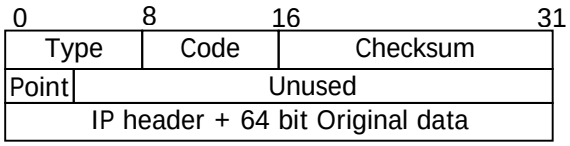
Router ip address là địa chỉ của bộ định tuyến mà máy nguồn sẽ dùng để trỏ máy đích.

- *Time Exceeded :* Router sẽ huỷ bỏ, không xử lý 1 datagram khi giá trị TTL của nó bằng 0 và phát ra một thông báo ICMP Time Exceeded. Có 2 loại ICMP Time Exceeded như sau:

| Code | Nội dung |
|---|---|
| 0 | Bộ đếm thời gian sống TTL của 1 datagram bằng 0 |
| 1 | Quá thời gian đợi để kết hợp các gói bị phân mảnh |

Bảng 5-3. Các lỗi của ICMP Time Qxceeded.

- *Parameter Problem :* Thông báo này được gửi đi khi có lỗi xuất hiện ở phần các tham số chọn lựa của datagram gửi đến. Trường CẶDỌ của thông báo này nhận 3 giá trị trong bảng và có định dạng như hình sau :




Hình 5-19. Dạng ICMP Parameter Problem

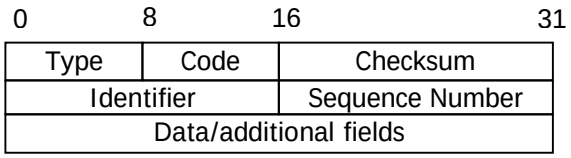
| Code | Giải thích |
|---|---|
| 0 | Có một lỗi đặc biệt trong lược đồ dữ liệu. |
| 1 | Phần option của IP header chưa định nghĩa. |
| 2 | Lỗi Header Length và (hoặc) Total Packet Length trong IP header. |

Bảng 5-4. Các lỗi của ICMP Parameter Problem

Pointer: xác định vị trí gây ra lỗi trong datagram.

***2. Các thông báo truy vấn ICMP***

ICMP được sử dụng trong việc khảo sát các đặc trưng chung của mạng với 2 loại thông báo request và reply. Có 8 loại thông báo truy vấn ICMP được liệt kê trong bảng và có định dạng như hình sau :



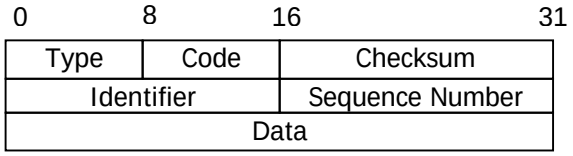

Hình 5-20. Dạng ICMP truy vấn.

| Type | Loại thông báo |
|---|---|
| 0 | Echo Reply |
| 8 | Echo Request |
| 13 | Timestamp Request |
| 14 | Timestamp Reply |
| 15 | Information Request |
| 16 | Information Reply |
| 17 | Address Mask Request |
| 18 | Address Mask Reply |

Bảng 5-5. Các loại thông báo truy vấn ICMP.

- Identifier được sử dụng để phân biệt các thông báo được gởi đến các host khác nhau.
- Sequence number được sử dụng để phân biệt các thông báo được gửi đến cùng một host.
- Data/additional fields được dùng theo từng loại thông báo truy vấn ICMP.

- *Echo Request vµ Echo Reply*



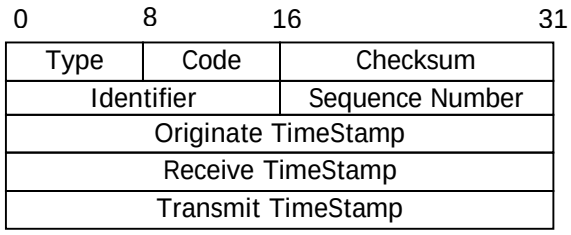

Hình 5-21. Dạng ICMP Echo Request & Reply.

Người ta sử dụng ICMP Echo để xác định xem một địa chỉ IP đích còn hoạt động hay không bằng cách gửi thông báo ICMP Echo Request đến hệ thống đích và chờ xem nếu nhận được thông báo ICMP Echo Reply thì sẽ xác định đích đấy vẫn còn hoạt động ngược lại thì đã bị down. Định dạng thông báo như trong hình sau :

Kích thước của DATA thay đổi tuỳ thuộc vào từng loại hệ điều hành. Trong hệ điều hành UNIX, kích thước của nó là 56 bytes, trong Microsoft Windows là 32 bytes,...

- *Timestamp Request và Timestamp Reply*

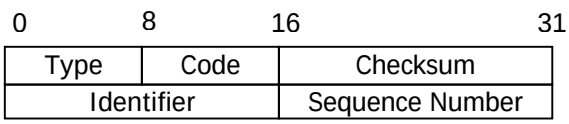
Mỗi máy đều có 1 đồng hồ riêng xác định thời gian vận hành của nó, quá trình hoạt động trong những hệ thống phần mềm phân tán thì sự khác biệt nhau lớn về thời gian giữa các máy tính sẽ gây ra nhiều vấn đề khó khăn. ICMP cung cấp một cơ chế cho phép lấy thời gian từ một máy khác và có định dạng như hình sau.




Hình 5-22. ICMP Timestamp Request & Reply

- Originate timestamp là thời gian máy nguồn thực hiện gửi báo.
- Receive timestamp là thời gian đầu tiên máy đích nhận được thông báo.
- Transmit timestamp là thời gian cuối bên đích xử lý thông báo và gửi đi.

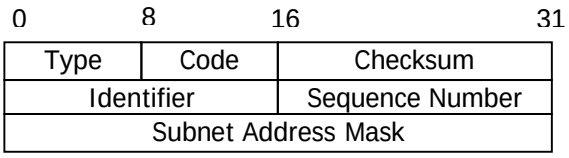
- *Information request và reply*




Hình 5-23. ICMP information request & reply

Được sử dụng nhằm hỗ trợ các hệ thống máy trạm không đĩa khi khởi động; cho phép các máy tính tìm ra địa chỉ Internet của chúng lúc khởi động hệ thống.

- *Address Mask Request và Reply*




H×nh 5-24. ICMP Ađress Mask Request & Reply

Để biết subnet mask, máy sẽ gửi một thông báo ICMP Address Mask Request đến 1 router và chờ nhận thông báo ICMP Address Mask Reply. Subnet Address Mask chứa địa chỉ của mặt nạ con của mạng.

Các bộ định tuyến phát bản tin ICMP để báo cho các trạm biết : gói tin không tới, hoặc tồn tại đường đi tốt hơn. Một số trường hợp có thể xảy ra là :

- *Destination unreachable* (không tới được đích): Bản tin không tới được đích do có lỗi hoặc không tìm được đường đi.
- *Routing redirect* (đổi đường đi): Thay đổi đường đi của bản tin do tồn tại đường đi tối ưu hơn (yêu cầu đổi đường đi).
- *Time expirect* (hết thời gian): Hết thời hạn khi TTL về 0 (timeout).
- *Echo request và cho echo reply* : Xuất hiện yêu cầu và trả lời.

  ICMP được dùng vào việc gỡ rối mạng cho biết tình trạng của mạng.

Lệnh Ping ***(Packet Internet Oroper)*** được dùng để hỏi (query) hệ thống (máy tính) khác để đảm bảo rằng một kết nối vẫn đang hoạt động (active). Lệnh Ping hoạt động bằng cách gửi ra một yêu cầu phản hồi (echo request) ICMP (Internet Control Message Protocol). Nếu như phần mềm IP của máy tính nhận được yêu cầu ICMP đó, nó đưa ra một trả lời phản hồi (echo reply) ngay lập tức. Máy gửi lại tiếp tục gửi một yêu cầu phản xạ cho đến khi lệnh ping được kết thúc bằng một tổ hợp phím thoát (Ctrl+C hoặc phím Delete trên UNIX).

## 5.7 Phiên bản IPv6

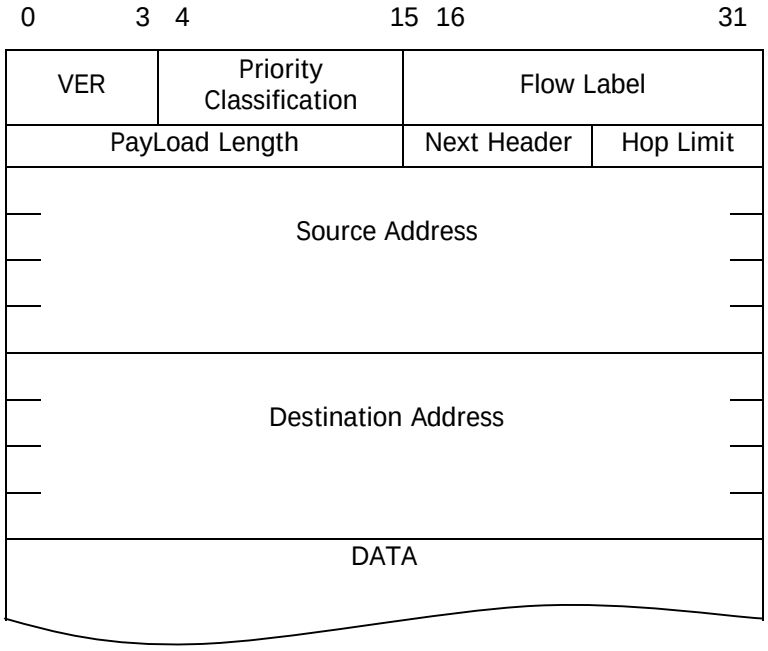
Với sự phát triển nhanh chóng của Internet thì địa chỉ IP 32 bit không thể đáp ứng được nhu cầu sử dụng Internet. Để khắc phục điều này phiên bản IP6 (IP Next Generation) đang được phát triển. Phiên bản IPv6 có các thay đổi như sau :

- Sử dụng 128 bit địa chỉ mạng thay cho 32 bit địa chỉ như phiên bản IPv4.
- Mở rộng phần Header cho ứng dụng và lựa chọn của khung tin.
- Hỗ trợ các loại dữ liệu audio và video.

- Có các giao thức mở rộng : cho phép bổ sung nhiều thông tin vào một datagram.

### 5.7.1 Khung tin IPng v6

Phần Header của các khung tin Ipng đã được thay đổi so với phiên bản 4. Phần lớn sự thay đổi của IPng là địa chỉ IP 128 bit và bỏ các trường không cần thiết. Cấu tạo của khung tin IPng như sau :




H×nh 5-25. CÊu t¹o cña gãi tin IPv6.

## 5.8 Định tuyến trên Internet

### 5.8.1 Bảng chọn đường

Một số phương thức thông thường xây dựng một bảng chọn đường (routing *table*) như sau :

- Bảng cố định được tạo ra dựa vào sơ đồ của mạng, bảng này liên tục được thay đổi và được cập nhật lại mỗi khi có sự thay đổi vật lý ở bất cứ nơi nào của mạng.
- Bảng động được dùng để ước lượng về đường truyền và các thông điệp từ các nút khác để điều chỉnh lại thông tin của bảng bên trong.
- Bảng dẫn đường cố định chính được tải về từ một trung tâm của các nút mạng trong một khoảng thời gian nhất định hoặc được tải về khi cần thiết.

Mỗi một phương thức đều có các ưu, nhược điểm của nó. Bảng động được đặt ở từng nút mạng hoặc được tải về trong những khoảng thời gian nhất định từ một

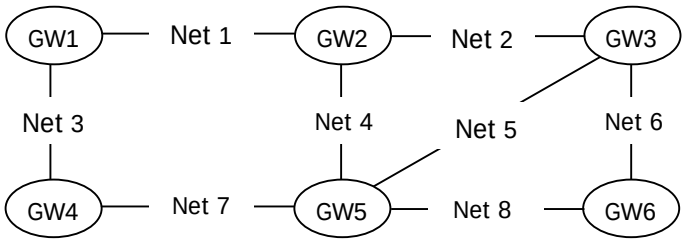
nơi chứa bảng cố định, nó không phức tạp và thích ứng với những thay đổi nhanh chóng trên mạng. Bảng chính thường là tốt hơn bảng cố định bởi vì quản lý một bảng ở trung tâm sẽ dễ dàng hơn quản lý từng bảng được đặt tại mỗi nút mạng.

### 5.8.2 Xây dựng bảng chọn đường cho các Router/Gateway

Trong liên mạng, tại mỗi cổng phải có một bảng chọn đường để chỉ ra muốn đến mạng đích nào thì phải đến cổng tiếp theo là cổng nào. Bảng chọn đường gồm hai phần : phần bên trái là mạng đích, nơi muốn đến, phần bên phải là khoảng cách tới đó và cổng tiếp theo.

Để xây dựng bảng chọn đường, từ cổng đang đứng ta xét các mạng cạnh đó, sau đó là các mạng ở cạnh các cổng tiếp theo và cứ thế cho đến hết các mạng trong liên mạng.

Ví dụ 1: Lập bảng chọn đường cho các router.gateway của liên mạng sau :




| GW1 | |
|---|---|
| Neti | D,G |
| 1 | 0,1 |
| 2 | 1,2 |
| 3 | 0,1 |
| 4 | 1,2 |
| 5 | 2,2(4) |
| 6 | 2,2 |
| 7 | 1,4 |
| 8 | 2,2(4) |

| GW2 | |
|---|---|
| Neti | D,G |
| 1 | 0,2 |
| 2 | 0,2 |
| 3 | 1,1 |
| 4 | 0,2 |
| 5 | 1,3(5) |
| 6 | 1,3 |
| 7 | 1,5 |
| 8 | 1,5 |

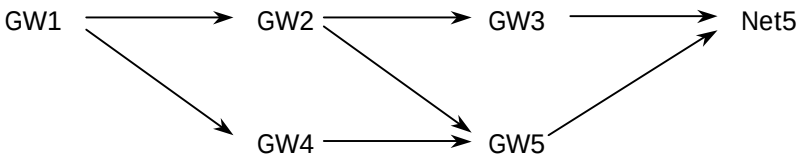
| GW3 | |
|---|---|
| Neti | D,G |
| 1 | 1,2 |
| 2 | 0,3 |
| 3 | 2,2 |
| 4 | 1,2(5) |
| 5 | 0,3 |
| 6 | 0,3 |
| 7 | 1,5 |
| 8 | 1,5(6) |

| GW4 | |
|---|---|
| Neti | D,G |
| 1 | 1,2 |
| 2 | 2,1(5) |
| 3 | 0,4 |
| 4 | 1,5 |
| 5 | 1,5 |
| 6 | 2,5 |
| 7 | 0,4 |
| 8 | 1,5 |

| GW5 | |
|---|---|
| Neti | D,G |
| 1 | 1,2 |
| 2 | 1,2 |
| 3 | 1,4 |
| 4 | 0,5 |
| 5 | 0,5 |
| 6 | 1,3(6) |
| 7 | 0,5 |
| 8 | 0,5 |

| GW6 | |
|---|---|
| Neti | D,G |
| 1 | 2,3(5) |
| 2 | 1,3 |
| 3 | 2,5 |
| 4 | 1,5 |
| 5 | 1,3(5) |
| 6 | 0,6 |
| 7 | 1,5 |
| 8 | 0,6 |

Dựa vào bảng chọn đường, tìm đường đi từ GW1 tới Net 5 như sau :




Đối với nhiều host, bảng dẫn đường tĩnh hoạt động như sau :

- Nếu đích nằm trong mạng cục bộ, dữ liệu được gởi đến máy đích
- Nếu đích nằm trên mạng ở xa, dữ liệu được chuyển tiếp đến gateway cục bộ.

Tuỳ thuộc vào kích cỡ của mạng mà các giao thức chọn đường khác nhau sẽ được sử dụng. Giao thức chọn đường trong một hệ thống nội bộ là RIP (Routing Information Protocol). Giao thức chọn đường giữa các hệ thống là EGP (External Gateway Protocol) và BGP (Border Gateway Protocol).

## 5.9 Mạng X.25

Vào những năm cuối thập niên 70, người ta phải cần đến một loạt các giao thức để cung cấp cho những người sử dụng mạng diện rộng WAN kết nối thông qua mạng dữ liệu công cộng (Public Data Networks - PDNs). Các loại hình PDNs như TELENET và TYMNET đã đạt được những thành công đáng ghi nhận, nhưng việc tiêu chuẩn hóa giao thức dường như còn ngoài tầm những người sử dụng mạng PDNs do việc đòi hỏi tính tương thích của thiết bị ngày một cao và đồng thời chi phí phải thấp. Kết quả của sự nỗ lực không ngừng này là sự ra đời của một loạt giao thức, trong đó X.25 được xem là giao thức phổ biến nhất.

Mạng X.25 và các giao thức liên quan do một tổ chức Quốc gia gọi là Hiệp hội Viễn thông Quốc tế (ITU) quản lý. Ban chịu trách nhiệm về các nghiệp vụ truyền tín hiệu âm thanh và dữ liệu của ITU gọi là ủy ban Tư vấn Quốc tế về Điện thoại và Điện báo (CCITT). Các thành viên của CCITT bao gồm FCC, PTTs Âu châu, các doanh nghiệp truyền thông và nhiều hãng máy tính, truyền dữ liệu khác. Do nhiều thành quả đóng góp trực tiếp có tính kế thừa, mạng X.25 thực sự được xem là mạng tiêu chuẩn có tính toàn cầu.

### 5.9.1 Cơ sở kỹ thuật

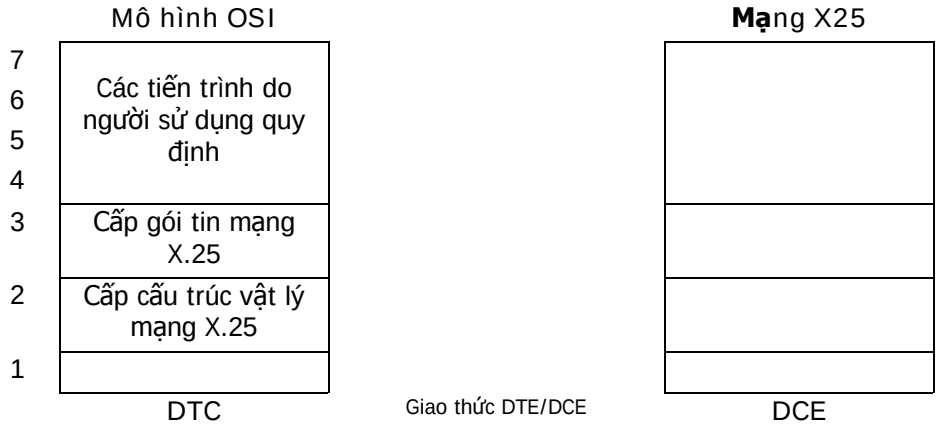
Mạng X.25 là một mạng điện thoại dùng để truyền dữ liệu. Để bắt đầu thực hiện quá trình giao tiếp, một máy tính cần phải liên kết với một máy khác để yêu cầu thực hiện giao tiếp. Máy được yêu cầu liên kết có thể chấp nhận hoặc từ chối việc giao tiếp. Nếu liên kết được chấp nhận, hai hệ thống có thể bắt đầu truyền tải thông tin qua lại hai chiều đồng thời với nhau. Cả hai bên đều có thể chấm dứt việc giao tiếp vào bất cứ thời điểm nào tùy ý.

Các đặc tính của mạng X.25 cho phép xác định quá trình tương tác từ nút-đến-nút (point-to-point) giữa các thiết bị truyền dữ liệu đầu cuối (Data Terminal Equipment - DTE) với các thiết bị kết cuối mạch truyền dữ liệu (Data Circuit-terminating Equipment - DCE). DTEs (bao gồm các trạm đầu cuối và máy chủ của người sử dụng mạng) kết nối với DCEs (bao gồm modem, các gói tin và các cổng truy cập PDN, thường đặt tại các trạm truyền thông), DCEs lại nối kết vào kênh chuyển mạch gói (Packet Switching Exchanges - PSEs) và các DCEs khác trong mạng PSNs và cuối cùng đến một DTE khác.

Một DTE có thể xem là một trạm đầu cuối nhưng không thực hiện đầy đủ các chức năng của mạng X.25. Các DTE được nối kết với DCE thông qua một thiết bị chuyển đổi gọi là thiết bị ghép/tách gói tin (Packet Assembler/Disassembler - PAD).

Quá trình hoạt động của mạch ghép nối từ trạm đầu cuối đến PAD, các dịch vụ do PAD cung cấp và các tương tác giữa PAD và các máy chủ do CCITT quy định.

Sơ đồ đặc tính của mạng X.25 kiểu phân tầng từ 1 tới 3 theo mô hình tham chiếu cho việc nối kết các hệ thống mở OSI. Tầng 3 của mạng X.25 mô tả các quy trình định dạng và chuyển mạch gói giữa các thành tố tầng 3 ngang cấp. Tầng 2 của mạng X.25 do các thủ tục truy cập liên kết cân bằng (Link Access Procedure Balance - LAPB) kiểm soát. LAPB xác lập các đơn vị gói tin (packet framing) cho các liên kết DTE/DCE. Tầng 1 của mạng X.25 xác lập các thủ tục về điện và cơ để kích hoạt và chấm dứt quá trình kết nối vật lý của DTE và DCE. Mối quan hệ này được minh họa theo hình vẽ dưới đây. Chú ý rằng tầng 2 và 3 cũng tham chiếu theo tiêu chuẩn ISO 7776 (LAPB) và ISO 8208 (các tầng gói tin mạng X.25).




Hình 5-26. Mối quan hệ giữa các tầng trong mạng X.25.

Quá trình giao tiếp từ nút-tới-nút (end-to-end) giữa các DTEs được thực hiện hoàn thiện thông qua một sự kết nối song phương gọi là liên kết truyền ảo (virtual circuit). Các liên kết ảo cho phép các hệ mạng khác nhau có thể giao tiếp được với nhau thông qua mọi nút liên kết trung gian mà không cần đến các bộ phận chuyên dụng để định rõ các liên kết vật lý. Các liên kết ảo hoặc có thể duy trì vĩnh viễn hoặc có thể tạm thời. Liên kết ảo vĩnh viễn được gọi là PVCs (Permanent Virtual Circuits), liên kết ảo tạm thời được gọi là SVCs (Switched Virtual Circuits). PVCs chủ yếu áp dụng cho phương thức truyền dữ liệu thường xuyên còn SVCs được áp dụng cho phương thức truyền dữ liệu không thường xuyên. Tầng 3 của mạng X.25 liên quan tới phương thức giao tiếp từ nút tới nút bao gồm cả hai liên kết ảo PVCs và SVCs.

Một khi đã thiết lập liên kết ảo, PTE có thể thực hiện truyền một gói tin đến một PTE khác bằng cách chuyển gói tin đến DCE thông qua một liên kết ảo thích hợp. Sau đó DCE sẽ tiến hành ền ưu tiên của liên kết ảo để định ra thức truyền gói tin lên mạng X.25. Các giao thức của tầng 3 mạng X.25 sẽ tiến hành chèn thông tin

vào giữa các DTE được kiểm soát bởi DCE của mạng phía nhận gói tin rồi sau đó được chuyển đến DTE đích.

## 5.10 Kỹ thuật FRAME RELAY

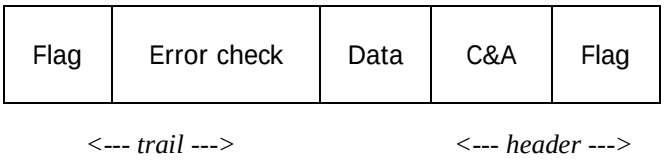
Bước sang thập kỷ 80 và đầu thập kỷ 90, công nghệ thông tin có những bước tiến đặc biệt là chế tạo và sử dụng cáp quang vào mạng truyền dẫn tạo nên chất lượng thông tin rất cao. Sử dụng giao thức X25 để truyền đa số liệu trên mạng cáp quang, dữ liệu nhận được có thể đánh giá là đạt yêu cầu. Tuy nhiên người ta nhận thấy rằng sử dụng giao thức này làm mất rất nhiều thời gian để truyền số liệu trên mạng cáp quang. Do đó công nghệ Frame Relay ra đời có thể chuyển nhận các khung lớn tới 4096 byte trong khi đó gói tiêu chuẩn của X25 khuyến cáo dùng là 128 byte, không cần thời gian cho việc hỏi đáp, phát hiện lỗi và sửa lỗi ở lớp 3 (*No protocol at Network Layer*) nên Frame Relay có khả năng chuyển tải nhanh hơn hàng chục lần so với X25 ở cùng tốc độ. Frame Relay rất thích hợp cho truyền số liệu tốc độ cao và cho kết nối LAN to LAN và cả cho âm thanh, nhưng điều kiện tiên quyết để sử dụng công nghệ Frame relay là chất lượng mạng truyền dẫn phải cao.

Frame-Relay bắt đầu được đưa ra như tiêu chuẩn của một trong những giao thức truyền số liệu từ năm 1984 trong hội nghị của ủy ban Tư vấn Quốc tế về Điệnthoại và Điện báo CCITT và cũng được Viện tiêu chuẩn quốc gia Mỹ ANSI đưa thành tiêu chuẩn của ANSI vào năm đó.

Mục tiêu chính của Frame-Relay cũng giống như của nhiều tiêu chuẩn khác, đó là tạo ra một giao diện chuẩn để kết nối thiết bị - của các nhà sản xuất thiết bị khác nhau - giữa người dùng và mạng UNI (*User to Network Interface*). Frame-Relay được thiết kế nhằm cung cấp dịch vụ chuyển khung nhanh cho các ứng dụng số liệu tương tự như X.25 hay ATM.

Mạng truyền số liệu theo công nghệ chuyển mạch gói X.25 chỉ có thể phục vụ cho các nhu cầu truyền số liệu tốc độ thấp (tối đa tới 128 Kbps) nhưng nó có tính an toàn cao, khắc phục được các yếu điểm của một mạng truyền dẫn chất lượng kém. Với các công nghệ truyền dẫn hiện nay, vấn đề nâng cấp chất lượng các đường truyền dẫn không còn quá phức tạp như trước kia. Vì vậy, chúng ta còn có thể chọn hướng phát triển là xây dựng mạng truyền số liệu theo công nghệ Frame-relay và tiến tới công nghệ ATM.

### 5.10.1 Khuôn dạng gói dữ liệu Frame-Relay




Hình 5-27. Khuôn dạng gói dữ liệu Frame-Relay.

- Flag: Cờ
- Error check: Trường kiểm tra lỗi
- Data: Trường dữ liệu
- C&A: Trường địa chỉ và điều khiển

Để thực hiện nhiệm vụ truyền số liệu, mạng Frame-Relay sẽ phải giải quyết vấn đề tắc nghẽn thông tin trên mạng, thực chất đây là vấn đề của tầng Mạng trong mô hình 7 tầng. Frame-Relay làm việc ở tầng Liên kết nhưng cũng phải giải quyết vấn đề này để đảm bảo khả năng lưu chuyển thông tin. Hầu hết các mạng truyền số liệu đều sử dụng kỹ thuật điều khiển luồng để giải quyết vấn đề tắc nghẽn. Có hai phương pháp được sử dụng khi xảy ra tắc nghẽn trong mạng: thông báo cho người dùng, router, chuyển mạch về sự cố tắc nghẽn xảy ra và thực hiện các công việc nhằm hiệu chỉnh luồng thông tin. Cả hai phương pháp này mạng Frame-Relay đều dùng đến các bit BECN (Backward Explicit Congestion Notification) và bit FECN (Forward Explicit Congestion Notification) trong trường điều khiển.

Bit FECN được thiết lập khi có tắc nghẽn để thông báo rằng thủ tục xử lý tắt nghẽn đã được khởi tạo, và tương ứng với lưu lượng bị nghẽn từ hướng của Frame có bit FECN tới. Ngược lại, bit BECN cũng được thiết lập khi có tắc nghẽn để thông báo rằng thủ tục xử lý nghẽn đã được khởi tạo, nhưng tương ứng với lưu l-ượng bị nghẽn từ hướng ngược với Frame có bit BECN tới. Khi các bit này được thiết lập thì mạng phải dùng đến một liên kết logic dự phòng để chuyển các thông tin để xử lý nghẽn, đó là liên kết với mã nhận dạng DLCI (Data Link Connection Identifier) số 1023. Các liên kết với mã nhận dạng nhỏ hơn được dùng để truyền số liệu của người dùng.

# BÀI TẬP

1. Viết sơ đồ mô tả thuật giải hoạt động chọn đường trên mạng.
2. Khảo sát cấu trúc và hoạt động của giao thức điều khiển ICMP
3. Tìm hiểu các lệnh của hệ điều hành Windows và Linux để xem và thay đổi các thông số bảng chọn đường.

*Chương 6*

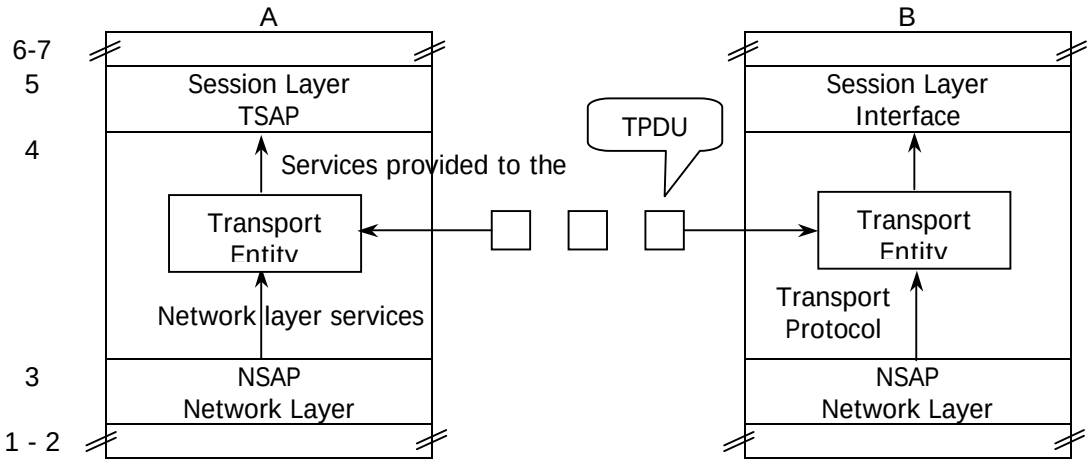
# TẦNG GIAO VẬN

Tầng giao vận làm nhiệm vụ thiết lập, duy trì và huỷ bỏ các cuộc giao tiếp giữa hai máy, đảm bảo việc dữ liệu truyền giống hoàn toàn dữ liệu nhận. Dữ liệu qua các mạng con có thể bị lỗi, tập tin tầng giao vận thực hiện cải thiện chất lượng dịch vụ, đảm bảo dữ liệu được truyền một cách chính xác và truyền lại nếu như phát hiện thấy lỗi. Tầng giao vận *quản lý dữ liệu gửi*, *xác định trật tự* của dữ liệu và *độ ưu tiên* của dữ liệu đó.

## 6.1 Các vấn đề của tầng giao vận

### 6.1.1 Cung cấp dịch vụ cho tầng phiên

Để thực hiện mục tiêu chuyển giao dữ liệu tin cậy, an toàn cho tầng 5, tầng 4 phải dùng các dịch vụ được cung cấp từ tầng 3 (network layer). Phần cứng và phần mền trong phần 4 để thực hiện công việc coi là thực thể giao vận (*transport entity*). Mối quan hệ giữa các lớp 3, 4, 5, được mô tả bởi hình sau:




Hình 6-1. Mối quan hệ giữa các thực thể trong tầng Phiên.

Có hai dịch vụ mạng nên cũng có hai dịch vụ giao vận: *dịch vụ có kết nối* và *không kết nối*.

Do dữ liệu qua các subnet có thể sai sót, người sử dụng không có được điều khiển trên subnet hoặc tăng cường quản lý lỗi ở tầng hai. Chỉ có khả năng đặt thêm một tầng trên lớp 3 để cải thiện chất lượng dịch vụ (QoS). Nếu giữa chúng một tầng giao vận được kết  nối mạng được kết thúc đột ngột và không biết được sự cố gì đã xảy ra, nó có thể thiết lập một kết nối mới ở lớp mạng tới tầng giao vận ở xa và gởi yêu cầu hỏi số liệu nào đến, số liệu nào không tự nó biết được sai sót xảy ra ở đâu. Tầng 4 có thể phát hiện mất gói tin, số liệu bị biến đổi, N-RESET ở lớp mạng. Tầng 1 -> 4 cung cấp dịch vụ giao vận. Tầng 5 ->7 sử dụng dịch vụ giao vận

- Các hàm dịch vụ của tầng giao vận có kết nối

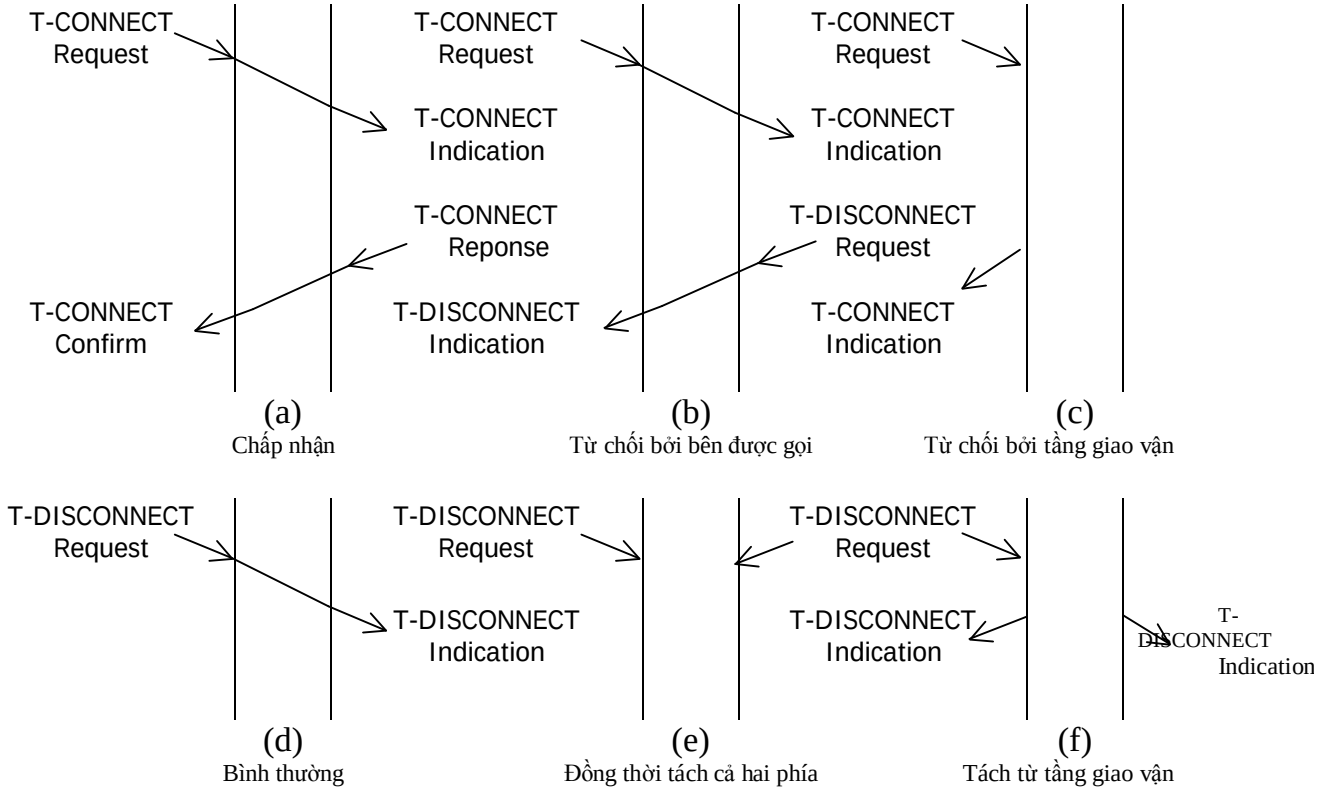
Ngoài phần giao thức chuẩn, ISO còn định nghĩa các dịch vụ mà tầng Giao vận cung cấp cho các thực thể ở tầng Phiên trong trường hợp có liên kết, dưới dạng một tập hợp các hàm dịch vụ nguyên thủy(services primitives) như sau :

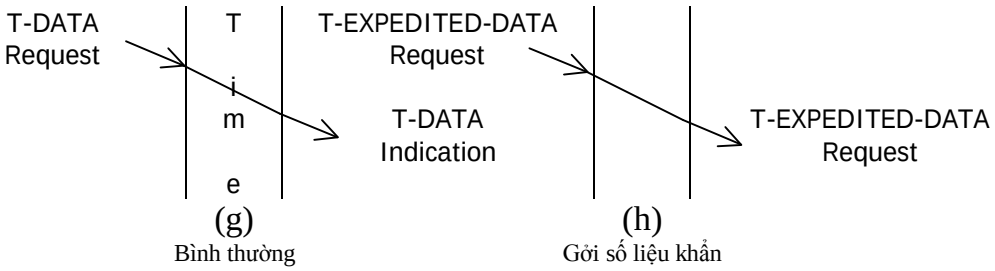
T-CONNECT request (callce, caller, exp wanted, qos, user data)
T-CONNECT indication (callce, caller, exp wanted, qos, user data)
T-CONNECT response (qos, responder, exp wanted, user data)
T-CONNECT confirm (qos, responder, exp wanted, user data)
T-DISCONNECT request (user data)
T-DISCONNECT indication (reason, user data)
T-DATA request (user data)
T-DATA indication (reason, user data)
T-EXPEDITED-DATA request (user data)
T-EXPEDITED-DATA indication (reason, user data)

- Các hàm dịch vụ của tầng giao vận không có kết nối : Chỉ có hai hàm dịch vụ được định nghĩa :

T-UNITDATA request (callce, caller, QoS, user data)
T-UNITDATA indication (callce, caller, QoS, user data)

- Quan hệ giữa các hàm OSI nguyên thủy : Quá trình nối, tách và trao đổi dữ liệu diễn ra như sau :






Hình 6-2. Quan hệ giữa các hàm OSI nguyên thủy.

Giải thích

(a) Quá trình nối được chấp nhận
(b) Quá trình nối bị từ chối bởi bên được gọi
(c) Quá trình nối bị từ chối bởi tầng Giao vận do lỗi của người sử dụng hoặc người chung cấp dịch vụ giao vận gây nên.
(d) Quá trình tách bình thường
(e) Quá trình tách đồng thời cả hai phía
(f) Quá trình tách từ tầng Giao vận
(g) Quá trình trao đổi dữ liệu bình thường
(h) Quá trình trao đổi dữ liệu khẩn

Trong hình (c) trên, việc từ chối có thể do lỗi của người sử dụng hoặc người cung cấp dịch vụ giao vận gây nên. Khi đó, không có gì được phát qua mạng vì vậy đầu kia không nghe được gì cả. Có những qui tắc cho người sử dụng các hàm dịch vụ giao vận. Ví dụ, không được dùng T-DISCONNECT.request khi tiếp nối chưa được thiết lập.

### 6.1.2 Chất lượng dịch vụ QoS

Chức năng cơ bản của tầng 4 là tăng cường chất lượng dịch vụ được cung cấp bởi tầng 3. Nếu lớp chất lượng chưa tốt, tầng Giao vận sẽ khắc phục khoảng ngăn cách giữa những gì mà người sử dụng tầng Giao vận muốn và những gì mà lớp mạng cung cấp. Các tham số của chất lượng dịch vụ QoS (Quality of Service) bao gồm :

- *Thời gian thiết lập liên kết* là thời gian từ khi gởi yêu cầu tới thời điểm nhận được xác nhận liên kết.
- *Xác nhận không thành công của thiết lập liên kết* - là tỷ lệ yêu cầu liên kết không được chấp nhận trong một thời hạn tối đa.
- *Lưu lượng của liên kết* do số byte hữu ích có thể truyền trong một giây, lưu lượng được tính *trong một cuộc trao đổi* hoặc dựa vào *khả năng của mạng theo 2 chiều.*

- *Thời gian trễ (*Độ trễ truyền dẫn - transmit delay) là khoảng thời gian giữa thời điểm mà người sử dụng dịch vụ của tầng Giao vận bên phát gởi thông báo tời thời điểm thực thể của tầng Giao vận bên thu nhận được. Đánh giá theo 2 chiều.
- *Tỷ lệ lỗi* là tỷ số giữa tin báo bị lỗi (hoặc mất) trên tổng số tin báo được truyền trong một chu kỳ định trước.
- *Xác nhận sự cố truyền:* tỷ số giữa thời gian có sự cố với thời gian cả chu kỳ quan sát.
- *Thời gian hủy liên kết* là thời gian từ khi một người sử dụng phát huy cầu huỷ liên kết đến khi liên kết được huỷ thật sự tại thiết bị đầu cuối từ xa.
- *Xác suất lỗi khi hủy liên kết* là tỷ lệ số yêu cầu hủy liên kết không được thực hiện trong thời gian lớn nhất.
- *Khả năng bảo vệ* là khả năng của người sử dụng cấm thiết bị đầu cuối bên ngoài truy nhập bất hợp pháp hay thay đổi dữ liệu truyền.
- *Thông số ưu tiên:* cho phép người sử dụng có quyền ưu tiên được phục vụ cao hơn đối với một liên kết.
- *Thông số hủy bỏ* cho phép tầng giao vận tự quyết định huỷ liên kết khi có tắc nghẽn hay các vấn đề bên trong mạng.

Người sử dụng khi yêu cầu liên kết sẽ gởi tất cả các thông số với các giá trị yêu cầu tới tầng giao vận và bắt đầu quá trình đàm thoại với các thông số đó.

So sánh các hàm cơ bản của dịch vụ giao vận và dịch vụ mạng, ta thấy các dịch vụ mạng và giao vận gần giống nhau. Sự khác nhau là dịch vụ mạng cho phép người sử dụng xử lý Acknowledgements và N-RQSQTS. Ngược lại, dịch vụ giao vận không quan tâm đến vì dịch vụ lớp giao vận là tin cậy, không có lỗi. Dịch vụ mạng được dùng bởi tầng giao vận.

### 6.1.3 Các lớp giao thức của tầng giao vận

Các dịch vụ tầng giao vận bảo đảm bằng các giao thức giữa 2 thực thể của tầng cũng tương tự như giao thức của tầng liên kết dữ liệu nó giải quyết vấn đề lỗi, điều khiển lưu lượng và bảo đảm trình tự mảng tin.

tầng liên kết dữ liệu, hai IMP truyền tin trực tiếp qua đường kênh vật lý. ở tầng giao vận, đường kênh vật lý này được thay bằng subnet. Sự khác nhau này kéo theo sự khác nhau về xây dựng các thủ tục. ở tầng giao vận phải xác định địa chỉ nơi nhận, ở tầng liên kết dữ liệu thì không cần vì chỉ có một đường truyền tin giữa hai điểm. Quá trình kết nối ở tầng giao vận cũng phức tạp hơn ở tầng liên kết giữ liệu.

Tầng giao vận đòi hỏi khả năng lưu trữ trong mạng (subnet) để giữ những gói tin bị sự cố và đòi hỏi thủ tục đặc biệt. tầng giao vận số các kết nối lớn hơn nên các vấn đề bộ đệm và điều khiển dòng phức tạp hơn.

Từ quan điểm thiết kế thủ tục giao vận, các dịch vụ được cho bởi mạng quan trọng hơn các tính chất thực tế của mạng, mặc dù cái sau bị ảnh hưởng mạnh bởi cái trước. Tuy vậy, trong một phạm vi nào đó, dịch vụ mức mạng có thể che những mặt ít được chú ý của mạng và cung cấp ghép nối tốt hơn. Để tiện lợi xem xét các thủ tục giao vận, ta chia các dịch vụ trên mạng thành 3 nhóm :

| Nhóm | Ý nghĩa |
|---|---|
| ***Nhóm A*** | - Hoàn thiện, tỷ lệ các gói tin bị mất, trùng lặp hoặc bị hỏng không đáng kể.<br>- Lệnh N-RESET có thể bỏ qua.<br>- Tầng giao vận đơn giản, không cần các dịch vụ phục hồi và sắp xếp lại thứ tự gói tin.<br>- Thường là mạng cục bộ. |
| ***Nhóm B*** | - Gói tin bị mất, nhưng kiểm soát được.<br>- Thỉnh thoảng tầng mạng gởi lệnh N-RESET do tắc nghẽn, hỏng phần cứng, vấn đề phần mềm.<br>- Thông thường là mạng đường dài<br>• Giao thức tầng Giao vận có nhiệm vụ:<br>- Thiết lập tại liên kết. Đồng bộ lại<br>- Theo dõi toàn bộ yêu cầu khởi động lại cho NSD. |
| ***Nhóm C*** | - Truyền tin không tin cậy, không liên kết<br>- Mạng đường dài, kết nối nhiều mạng con<br>- Giao thức của tầng giao vận phức tạp, phải có khả năng phục hồi lỗi khi xảy ra sự cố và sắp xếp lại thứ tự các gói tin. |

Bảng 6-1. Các nhóm dịch vụ của tầng Giao vận.

Dịch vụ mạng xấu thì giao thức của tầng giao vận sẽ phức tạp hơn. OSI đã nhận thức vấn đề này và chia giao thức của tầng giao vận thành 5 lớp ứng với các loại mạng như sau :

| Lớp | Ý nghĩa |
|---|---|
| *Lớp O*<br>*Mạng loại A* | - Lớp thủ tục đơn giản<br>- Kết nối mạng khi có yêu cầu giao vận không phải giải quyết lỗi<br>- Chủ yếu tạo ra trình tự, điều khiển dòng dữ liệu để tầng mạng hoạt động tốt.<br>- Bao gồm cơ cấu thiết lập và huỷ liên kết ở tầng giao diện. |
| *Lớp 1*<br>*Mạng loại B* | Có tính chất tương tự lớp 0, ngoài ra còn thêm:<br>- Khởi động lại mạng sau khi N-RESET. Giao thức có khả năng báo nhận (ACK) và truyền dữ liệu khẩn.<br>- Đồng bộ lại và sau đó nối lại liên lạc giữa các thực thể giao vận đã bị gián đoạn<br>- Lớp 1 không kiểm tra lỗi và kiểm soát dòng dữ liệu. |
| *Lớp 2*<br>*Mạng loại A* | Lớp 2 là phiên bản của lớp 0 và được xây dựng cho mạng tin cậy và có thêm một số chức năng như sau :<br>- Sự ghép kênh : Hai hay nhiều liên kết của tầng giao vận có thể dùng chung một kết nối ở tầng mạng.<br>- Sử dụng khi nhiều liên kết ở tầng giao vận được mở đồng thời, nối liên kết có lưu lượng nhỏ.<br>Ví dụ như hệ thống đặt vé máy bay cho phép tiết kiệm đường truyền. |
| *Lớp 3*<br>*Mạng loại B* | Là tổ hợp lớp 1 và lớp 2<br>- Cho phép dồn kênh<br>- Khởi động lại<br>- Điều khiển dòng dữ liệu. |
| *Lớp 4*<br>*Mạng loại C* | Lớp 4 có hầu hết các chức năng của lớp trước và bổ sung thêm một số khả năng kiểm soát luồng dữ liệu.<br>- Phải có biện pháp giải quyết vấn đề mất gói tin, gói tin bị hỏng<br>- Phải giải quyết yêu cầu khởi động lại<br>- Thủ tục Giao vận phức tạp nhất. |

Bảng 6-2. Các lớp dịch vụ của tầng Giao vận.

Dịch vụ không có kết nối đặt tất cả sự phức tạp và thủ tục Giao vận.

### 6.1.4 Thủ tục giao vận trên X. 25

Thủ tục X. 25 là thủ tục có nối và tin cậy, coi như lớp mạng loại A. Do đó thủ tục giao vận trên X.25 là thủ tục giao vận lớp 0 mô hình OSI. Thủ tục này được thể hiện qua các hàm dịch vụ cơ bản và quá trình nối, tách, trao đổi số liệu của thủ tục.

#### *6.1.4.1 Các hàm dịch vụ cơ bản*

Các hàm dịch vụ cơ bản được thực hiện bằng các chương trình con minh họa bằng ngôn ngữ Pascal

1. Hàm Connect thực hiện T-CONNECT .request

   connum = CONNECT(local, remote)

Hàm dịch vụ này để thiết lập kết nối tầng giao vận giữa 2 máy. Nếu kết nối thành công, hàm trả về một số dương, ngược lại hàm trả về số âm.

2. Hàm Listen thực hiện T-CONNECT.indication

   connum = LISTEN (local)

Hàm này dùng để thông báo tiếp nhận yêu cầu kết nối

3. Hàm Disconnect thực hiiện T-DISCONNECT.request

   status = DISCONNECT (commun)

Hàm này dùng để kết thúc kết nối, tham số commun cho biết kết nối nào sẽ bị ngắt, kết quả thực hiện sẽ được gán cho biến status với giá trị OK hoặc error

4. Hàm Send thực hiện T-DATA.request

   status = SEND (commun, buffer, bytes)

Hàm này để phát nội dung ở buffer với kích thước là bytes cho số kết nối đặt ở commun. Kết quả đặt ở status.

5. Hàm Receive thực hiện T-DATA.indication

   status = RECEIVE (commun buffer, bytes)

Hàm này để nhận tin vào buffer với kích thước là giá trị ở biến bytes. Kết quả thực hiện đặt vào status giá trị OK hoặc error.

*Chương 7*

# HỌ GIAO THỨC TCP/IP

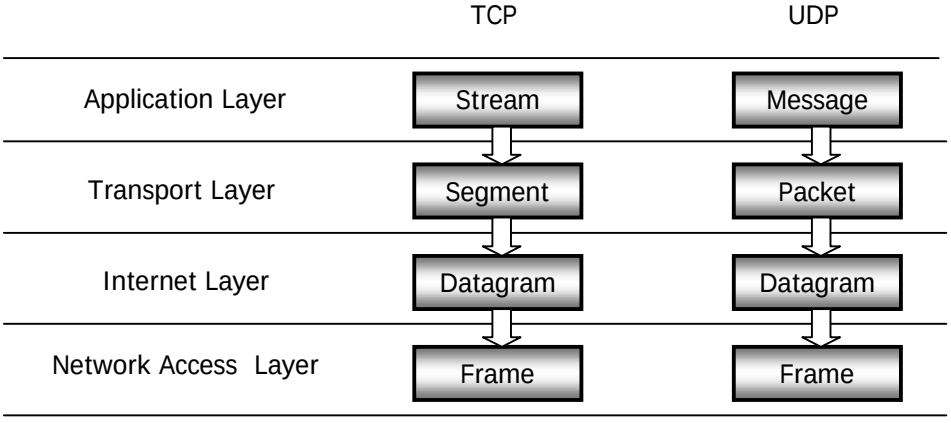
Do đặc tính của mô hình OSI là một mô hình tham chiếu, việc áp dụng mô hình OSI vào thực tế thường có hiệu suất kém do dữ liệu phải truyền qua tất cả các lớp của mô hình OSI ở cá hai máy, mô hình OSI là tiêu chuẩn để các nhà phát triển dựa vào mà phát triển các mô hình khác tối ưu hơn. Có rất nhiều mô hình khác nhau như NetBIOS, IPX/SPX, TCP/IP, tuy nhiên mô hình TCP/IP hiện nay đang được sử dụng phổ biến nhất.

TCP/IP thực chất là một họ giao thức cùng làm việc với nhau để cung cấp ptn truyền thông liên mạng. Mô hình TCP/IP có những tính chất chung như sau :

- TCP /IP độc lập với phần cứng mạng vật lý, điều này cho phép TCP/IP hoạt động trên nhiều mạng khác nhau như Ethernet, Token Ring, X25, dial up,...
- TCP/IP sử dụng sơ đồ đánh địa chỉ toàn cục duy nhất : mỗi máy tính trên mạng TCP/IP có một địa chỉ xác định duy nhất. Mỗi gói tin gởi trên mạng có một tiêu đề chứa địa chỉ nguồn và đích.
- Chuẩn giao thức mở : TCP/IP có thể thực hiện trên bất kỳ phần chứng hay hệ điều hành nào.
- Hoạt động theo mô hình Client/Server.
- Cung cấp các giao thức ứng dụng : cung cấp cho người lập trình phương thức truyền dữ liệu trên mạng giữa các ứng dụng mà còn cung cấp nhiều giao thức ở mức ứng dụng như giao thức truyền nhận mail, truyền file, . . .
- TCP/IP hỗ trợ cho liên mạng (internetworking) và định tuyến, các giao thức mức cao được chuẩn hoá thích hợp và cung cấp sẵn các dịch vụ người dùng.

## 7.1 Mô hình TCP/IP

Cấu trúc của bộ giao thức TCP/IP có bốn tầng, được mô tả như hình vẽ sau




Hình 7-1. Kiến trúc TCP/IP và các đơn vị dữ liệu.

Chức năng của các tầng như sau :

***1. Tầng truy cập mạng NAL (Network Access Layer)***

- Cung cấp cho hệ thống phương thức để truyền dữ liệu trên các thiết bị phần cứng vật lý khác nhau của mạng.
- Đóng gói các lược đồ dữ liệu IP (IP datagram) vào các *frame* truyền trên mạng và việc ánh xạ các địa chỉ IP thành các địa chỉ vật lý tương ứng dùng cho mạng trước khi truyền xuống kênh vật lý.
- Định nghĩa cách thức truyền các khối dữ liệu IP : Các giao thức ở lớp này phải biết chi tiết các phần cấu trúc vật lý mạng ở dưới nó để định dạng chính xác các dữ liệu sẽ được truyền phụ thuộc vào từng loại mạng vật lý cụ thể.

Lớp truy cập mạng NAL của mô hình kiến trúc TCP/IP tương đương với ba lớp thấp nhất của mô hình OSI là Network layer, Datalink layer, và Physical layer.

***2. Tầng mạng***

Tầng mạng chịu trách nhiệm định tuyến các thông báo (message) qua các mạng vật lý khác nhau, liên mạng, giao thức ở lớp này là IP là giao thức quan trọng nhất vì IP cung cấp dịch vụ giao nhận gói tin cơ bản trên các mạng TCP/IP, mọi giao thức ở các lớp trên và bên dưới tầng mạng đều sử dụng giao thức IP để thực hiện việc giao nhận dữ liệu. Hơn nữa IP bổ sung một hệ thống địa chỉ logic được gọi là địa chỉ IP, được sử dụng bởi lớp Internet và các lớp cao hơn để nhận diện các thiết bị và thực hiện định tuyến liên mạng.

***3. Tầng Giao vận (Host to Host Transport Layer)***

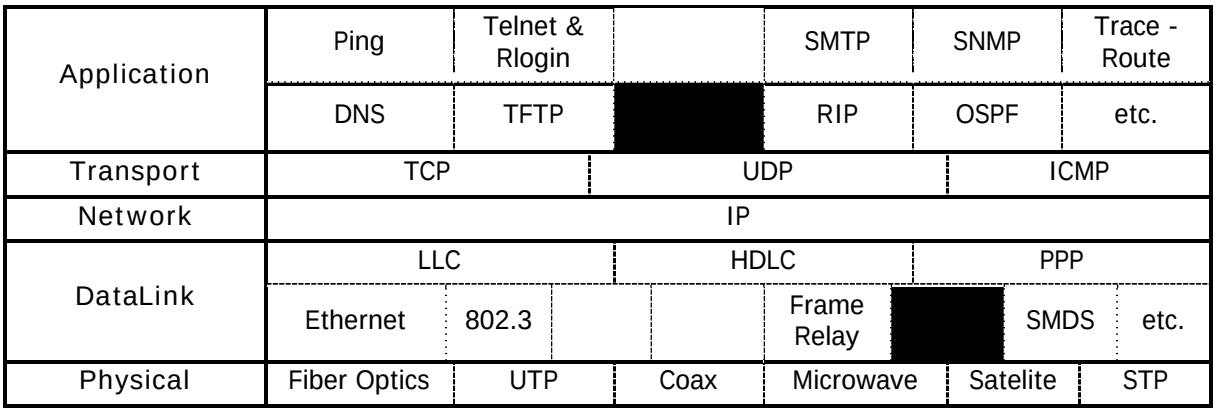
- Cung cấp phương tiện liên lạc từ một chương trình ứng dụng này đến chương trình ứng dụng khác, chịu trách nhiệm đảm bảo toàn vẹn dữ liệu đầu cuối.
- Trong lớp này có 2 giao thức quan trọng nhất:

- Transmission Control Protocol (TCP) : Về chức năng TCP tương đương với lớp giao thức đầy đủ nhất của giao thức chuẩn Transport của OSI. Tuy nhiên, khác với mô hình ISO, TCP sử dụng phương thức trao đổi các dòng dữ liệu (data stream ) giữa người sử dụng.
- User Datagram Protocol (UDP) : cung cấp dịch vụ giao nhận dữ liệu theo kiểu “không liên kết” (connectionless), không cần phải thực hiện thiết lập liên kết logic giữa một cặp thực thể UDP trước khi chúng trao đổi dữ liệu với nhau.

***4. Tầng ứng dụng (Application Layer)***

Bao gồm tất cả các tiến trình sử dụng các giao thức của lớp Transport để truyền dữ liệu. Có nhiều giao thức ứng dụng ở lớp này, phần lớn là nhằm cung cấp cho người dùng các dịch vụ ứng dụng, sử dụng 2 giao thức chính TCP và UDP.

Tầng ứng dụng cung cấp các dịch vụ trên Internet như thư điện tử (SMTP), truyền file (FTP), v.v.. Tầng dưới là phần mạng để định tuyến địa chỉ đến.




Hình 7-2. Họ giao thức TCP/IP.

| | | |
|---|---|---|
| Telnet | Tele Comunication | Dịch vụ truy cập từ xa. |
| FTP | File Transfer Protocol | Dịch vụ truyền File. |
| SMTP | Simple Mail Transfer Protocol | Dịch vụ truyền thư đơn giản. |
| DNS | Domain Name System | Hệ thống tên miền |
| SNMP | Simple Network Management Protocol | Giao thức quản lý mạng đơn giản |
| RPC | Remote Procedure Call | Thủ tục gọi từ xa |
| RIP | Routing Information Protocol | Giao thức định tuyến thông tin |
| TCP | Transmission Control Protocol | Giao thức TCP |
| UDP | User Datagram Protocol | Giao thức dữ liệu của người dùng. |
| IP | Internet Protocol | Giao thức IP |
| ICMP | Internet Control Message Protocol | G.thức kiểm soát message giữa các mạng. |
| FDDI | Fiber Distributed Data Multiplexing | |

## 7.2 Giao thức TCP

Tầng Giao vận sử dụng hai giao thức chính là TCP và UDP. Giao thức TCP (Transmission Control Protocol) đảm bảo độ tin cậy giữa nơi gởi và nơi nhận (end-to-end) trong điều kiện lớp mạng loại C không tin cậy. Dòng số liệu có chiều dài tuỳ ý được phân thành những đoạn không vượt quá 64KB, gửi đi đến đầu bên kia lại được gộp lại thành bản tin ban đầu.

- Chức năng của giao thức TCP :

| Chức năng | Giải thích |
|---|---|
| Phát hiện lỗi | Bằng cách sử dụng một trường checksum để kiểm tra lỗi bất cứ khi nào datagram được cắt ra trong quá trình truyền. |
| Truyền lại | TCP sẽ truyền lại các gói tin bị mất hoặc bị sai hỏng trong quá trình truyền. |
| Đánh số thứ tự | Cho phép bên gởi đã phát đi các gói tin theo một trật tự, bên nhận đã nhận và kết hợp các gói tin theo một trật tự đã định |
| Báo nhận và kiểm soát luồng | Bên TCP nhận sẽ gửi một đoạn báo nhận xác định một số chức năng trong quá trình truyền tin. |
| Phát gói tin đến đúng ứng dụng yêu cầu | Mỗi đoạn gói tin TCP có một số hiệu cổng nguồn và đích, là giá trị duy nhất để xác định một phiên làm việc. |

- Tính chất của giao thức TCP :

| Tính chất | Giải thích |
|---|---|
| Tin cậy | TCP cung cấp khả năng tin cậy bằng cách gởi lại dữ liệu đến khi bên nhận có một báo nhận hỏng. Đơn vị dữ liệu mà TCP truyền đi là segment và được giao thức IP phân ra thành các datagram. |
| Hướng kết nối | TCP thiết lập kết nối logic giữa các máy khi truyền dữ liệu, hoạt động theo cơ chế "bắt tay" (handshake), và có nhiệm vụ đồng bộ việc kết nối giữa hai máy. |
| Dòng dữ liệu | TCP xử lý dữ liệu dưới dạng một dòng nối tiếp các byte, theo cơ chế đánh số thứ tự gói tin. |

### 7.2.1 Khuôn dạng gói tin TCP

TCP là một giao thức có liên kết (*connection - oriented*) nghĩa là cần phải thiết lập liên kết logic giữa một cặp thực thể TCP trước khi chúng trao đổi dữ liệu với nhau, có 3 giai đoạn : ***thiết lập liên kết, truyền tải dữ liệu*** và ***hủy liên kết***. Đơn vị dữ liệu của TCP được gọi là **segment** (đoạn dữ liệu). Cấu trúc đơn vị dữ liệu của TCP được mô tả như hình sau :

*Source Port - Số hiệu cổng nguồn (16 bits)*

Xác định số hiệu cổng của trạm nguồn - User TCP cục bộ (thường là một chương trình ứng dụng trên lớp cao hơn).

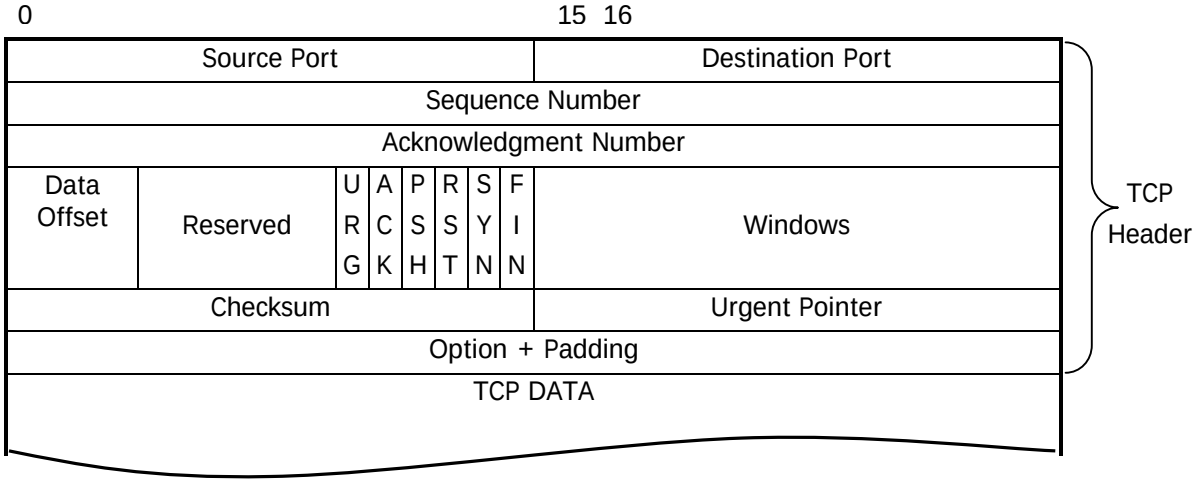
*Destination Port - Số hiệu cổng đích (16 bits)*

Xác định số hiệu cổng của trạm đích của máy ở xa. Dùng để nhận diện các tiến trình điểm đầu mút ở kênh ảo TCP.

*Sequence Number - Số thứ thự (32 bits)*

Trường này chứa một số chỉ vị trí hiện tại của khối tin trong Message. Số này cũng được các phiên bản khác nhau của TCP để cung cấp số thứ tự của khối tin ban đầu (ISN).

Đây là số hiệu byte đầu tiên của segment trừ khi bit SYN được thiết lập. Nếu bit SYN được thiết lập thì Sequence Number là số hiệu tuần tự khởi đầu (ISN) và byte dữ liệu đầu tiên là ISN+1.




Hình 7-3. Cấu trúc của gói tin TCP.

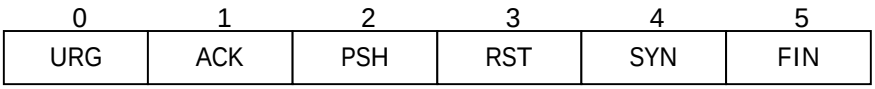
*Acknowledgment Number - Số phúc đáp (32 bits)*

Dùng để chỉ ra số hiệu của segment (khối tin) sắp được truyền tiếp theo mà trạm đích đang chờ để nhận. Dùng báo nhận tốt các Segment mà trạm nguồn đã gửi cho trạm đích. Ngoài ra nó cũng chỉ ra số thứ tự của khối tin nhận được sau cùng; nó chỉ ra số thứ tự của khối tin nhận được cộng thêm 1.

*Data offset (32 bits) :* Trường này dùng để chỉ ra vị trí bắt đầu của trường dữ liệu.

*Reserved (6 bits) :* Chưa dùng đến, dành sử dụng về sau. Các bit được đặt bằng 0.

*Control Bits* - Các bit điều khiển




Cờ URG : Nếu có giá trị là 1 thì thì trường urgent pointer rất quan trọng.
Cờ ACK : Nếu có giá trị là 1 thì trường Acknowledgment rất quan trọng.
Cờ PSH : Nếu thiết lập thì tức là chức năng PUSH sắp được thực hiện.
Cờ RST : Nếu được thiết lập thì kết nối hiện tại sắp được khởi tạo lại.
Cờ SYN : Chỉ ra số thứ tự của đoạn tin sẽ được đồng bộ hoá. Cờ này được dùng khi mà kết nối được thiết lập.
Cờ FIN : Nếu cờ này thiết lập, nó chỉ ra rằng phía gửi không còn dữ liệu để gửi nữa. Điều này tương đương với việc đánh dấu kết thúc quá trình truyền.

*Window - Cửa sổ (16 bits)*

Trường này cấp phát thẻ dùng để kiểm soát luồng dữ liệu theo cơ chế cửa sổ. Đây là số lượng các byte dữ liệu khối tin mà phía thu có thể chấp nhận được.

*Checksum (16 bits)*

Chứa mã kiểm soát lỗi (theo phương pháp CRC) cho toàn bộ segment.

*Urgent Pointer - Con trỏ khẩn (16 bits)*

Trường này được dùng khi mà cờ URG được thiết lập; con trỏ này trỏ tới số hiệu tuần tự của các byte đi theo sau dữ liệu khẩn, cho phép bên nhận biết được độ dài của dữ liệu khẩn.

*Options (có độ dài thay đổi)*

Trường này dùng để xác định các Option của TCP. Mỗi lựa chọn bao gồm một số (1 byte) để chỉ ra lựa chọn đó, một số chỉ giá trị của các byte trong trường Option, và các giá trị lựa chọn. Hiện nay với TCP mới có 3 Option được định nghĩa, như sau:

Số 0 : Cuối danh sách các lựa chọn
Số 1 : Không hoạt động (*No Operation*)
Số 2 : Kích cỡ lớn nhất của một Segment

Trường Options chỉ để xác định kích thước lớn nhất của bộ đệm mà TCP nhận có thể chấp nhận được. Bởi vì TCP dùng trường dữ liệu có chiều dài thay đổi được nên có thể có trường hợp là máy gửi sẽ tạo ra một đoạn tin mà phía nhận không thể chấp nhận được.

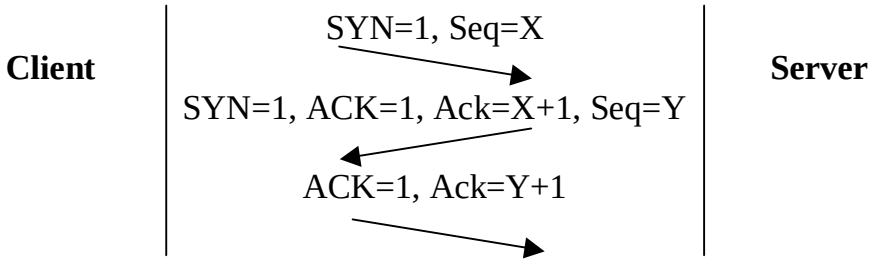
*Padding :*

Dùng để bổ sung vào Header để bảo đảm rằng phần Header luôn là bội số của 32 bit. Phần thêm vào bao gồm toàn số 0.

*TCP Data (Có độ dài thay đổi)*

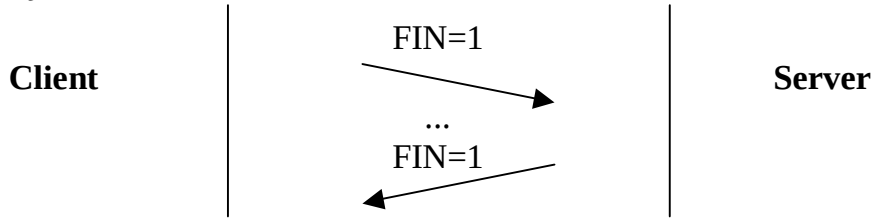
Chứa dữ liệu của tầng trên, độ dài tối đa ngầm định là 536 bytes. Giá trị có thể điều chỉnh bằng cách khai báo trong vùng Options.

### 7.2.2 Quá trình nối-tách



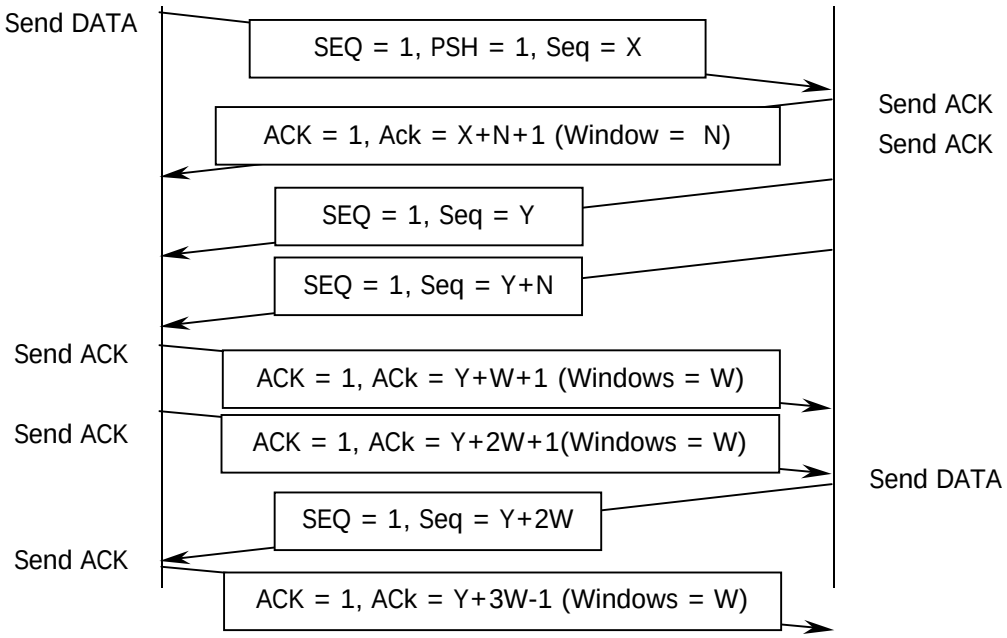
Quá trình thiết lập kết nối bằng thủ tục bắt tay 3 lần (three-way hand). Client gửi bản tin với SYN=1 (yêu cầu kết nối). Server nhận được, gửi bản tin với SYN=1 và ACK=1. Client lại đáp lại với bản tin ACK=1.

Kết thúc kết nối bằng thủ tục bắt tay hai lần (two-way hand). Bên kết thúc gởi số liệu, gởi bản tin với FIN=1, TCP cho phép nhận tiếp tục số liệu cho đến khi bên kia gửi bản tin FIN=1




Ngoài ra, thủ tục TCP/IP còn dùng để kết nối giữa LAN và WAN như một thủ tục cho mạng LAN.

### 7.2.3 Quá trình trao đổi dữ liệu




H×nh 7-4. S¬ ®å qu¸ tr×nh trao ®æi d÷ liÖu cña TCP.

W= maximun Segment size (W>N)

2W = Windows limit

### 7.2.4 Thứ tự thực hiện ứng dụng TCP/IP

Sự kết hợp của thủ tục TCP và IP thực sự là sự kết hợp giữa các mạng máy tính nối với nhau cho phép người dùng các mạng máy tính nối với nhau cho phép người dùng các mạng khác nhau liên lạc và làm việc được với nhau.

Thủ tục TCP là thủ tục tại đầu cuối, còn IP dùng để chạy trên mạng. Khi người sử dụng thủ tục TCP tạo được phân đoạn TCP và kết hợp vào IP để tạo thành IP datagram. Router căn cứ vào địa chỉ IP trong gói tin và thông tin chứa trong bảng định tuyến để chuyển gói này đi tới các router sau. Khi gói tin IP đến router cuối cùng, router này tìm và chuyển gói tin đến địa chỉ hệ thống đầu cuối.

Nếu IP datagram không chuyển tới đầu cuối được vì một lý do nào đó, nó sẽ bị hủy bỏ và giao thức IP không còn thông báo được điều này cho người sử dụng biết. Giao thức TCP cung cấp mối liên hệ tin cậy giữa các đầu cuối, đảm bảo dữ liệu phát đi đúng địa chỉ, không bị thiếu hay phát lặp nghĩa là tại điểm cuối cùng thủ tục TCP sẽ đọc số thứ tự trong phân đoạn TCP để biết gói tin bị thiếu hay gói đã nhận rồi và báo lại cho bên phát biết.

Gói tin IP không phụ thuộc vào các giao thức cụ thể của các mạng khác nhau mà nó đi qua (X.25 hay Frame relay v.v..). Với IP các mạng chỉ đơn thuần là đường dẫn các Router. Ta có thể hình dung IP datagram như một phong bì bình thường, người gửi thư không quan tâm đến bức thư đến được người nhận bằng ô tô, tàu hỏa hay máy bay.

Sự kết hợp giữa thủ tục TCP và IP giúp người dùng sử dụng được các dịch vụ trao đổi trên Internet thực hiện qua các bước chính sau đây:

**Bước 1:** Các dữ liệu ứng dụng kết hợp với số thứ tự để hình thành phân đoạn TCP.

Người sử dụng dùng dịch vụ trên mạng như thư điện tử, Telnet hay FTP v.v.. có nghĩa là đưa các dữ liệu của người dùng vào phần dữ liệu của gói tin TCP. Giao thức TCP sẽ đưa vào phần header của gói tin các thông tin sau:

- Số hiệu cổng quy định của Internet.
- Số thứ tự Segment gửi đi.
- Thông báo cho bên gửi biết đã nhận được Segment thứ mấy (ACK)
- Số byte cần phát.

**Bước 2:** Kiến tạo ra gói tin IP datagram

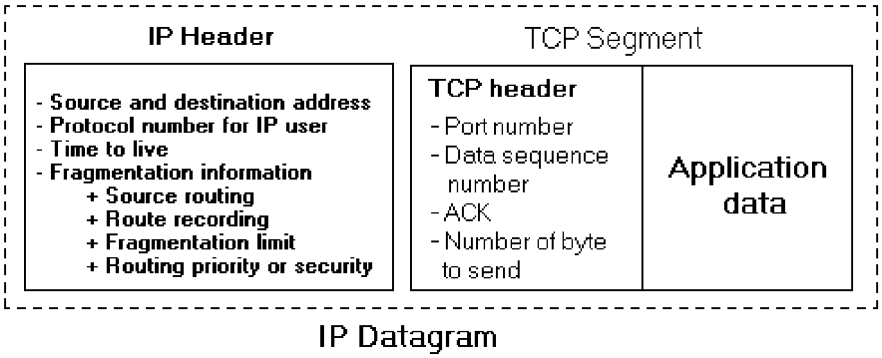
Trên cơ sở của gói tin TCP, IP thêm các thông tin sau đây vào để tạo thành IP Datagram.

- Địa chỉ phát và nhận : Router sử dụng địa chỉ này để định tuyến.
- Số thủ tục (Protocol number): định nghĩa thủ tục mà IP thực hiện.
- Thời gian tồn tại (Time to live): định nghĩa số Router bắt buộc Datagram phải đi qua trước khi nó bị hủy bỏ.
- Thông tin về các phân đoạn bị chia nhỏ trong quá trình chuyển đi trên mạng.

Kích thước gói tin thay đổi tùy thuộc vào mạng khác nhau, chẳng hạn như kích thước gói tin trong mạng Ethernet là 1500 bytes còn mạng X.25 chỉ có 128 bytes.

- Các thông tin tùy chọn

- Source Routing (Định tuyến bên phát): cung cấp danh sách các Router sử dụng.
- Route recording (Ghi lại tuyến đường đã đi qua): Thông tin sẽ yêu cầu mỗi Router ghi lại địa chỉ IP khi nó chuyển datagram qua, dùng để thống kê được số liệu của đường dẫn trong Internet.
- Fragmentation limit (Giới hạn phân mảnh): Định nghĩa cỡ lớn nhất (tính theo byte) của một datagram có thể chuyển đi mà không cần phải chia nhỏ.
- Routing priority or security (Ưu tiên hoặc bảo đảm an toàn cho Datagram): chỉ rõ tuyến nào dành ưu tiên hay tuyến nào bảo đảm được an toàn cho datagram.




Hình 7-5. Cấu trúc của IP Datagram.

Như vậy Datagram thực chất là hình thức một gói tin chứa dữ liệu thông tin được dùng trong internet.

**Bước 4:** Chuyển gói đến địa chỉ đích

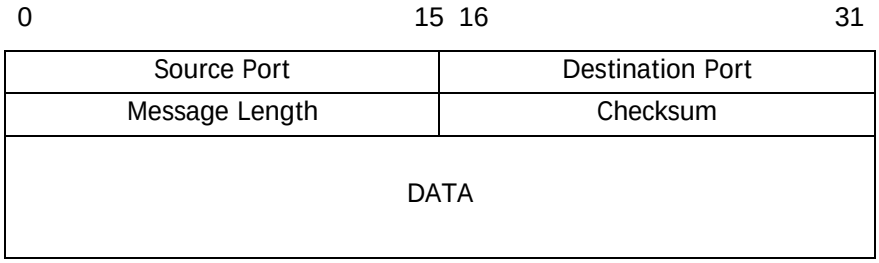
Các IP Datagram chuyển qua các lớp dưới đưa vào và định tuyến để tìm tới địa chỉ đến qua mạng căn cứ vào địa chỉ vật lý của mạng lưới ví dụ như địa chỉ mạng X.25, mạng Frame relay hoặc ngay bản thân của Internet. Tất cả các thông tin này đều nằm trong bảng định tuyến trong các Router. Các mạng X.25 hay Frame relay chỉ làm nhiệm vụ chuyển tải các Datagram.

Tại phía đầu cuối thu, TCP tách IP datagram để lấy phân đoạn TCP xử lý dữ liệu thông tin, đối chiếu số thứ tự, phát hiện những gói thiếu thiếu hay đã nhận được, đồng thời cũng nhận được thông báo (ACK) từ phía phát báo cho biết bên đấy đã nhận được gói thứ mấy do bên này phát đi.

Phía thu thông báo (ACK) cho bên phát biết số dữ liệu đã nhận được đồng thời cũng yêu cầu phát lại những gói tin thiếu nếu có.

## 7.3 Giao thức UDP

Giao thức UDP (User Datagram Protocol) cho phép người sử dụng gởi bản tin mà không cần thiết lập liên kết, do đó không bảo đảm việc giao nhận chính xác hoặc thứ tự bản tin. Giao thức UDP dùng cho dịch vụ không tin cậy 100%. Thực tế trong các mạng 99% bản tin UDP được giao nhận đúng đích. Do ít chức năng phức tạp nên UDP hoạt động nhanh hơn so với TCP.




Hình 7-6. Khuôn dạng của UDP Datagram.

Các trường có ý nghĩa như sau:

- *Source Port* - Số hiệu cổng nguồn (của máy gửi): Một trường có thể lựa chọn được với số hiệu cổng. Nếu một số hiệu cổng không xác định thì trường này có giá trị là 0.
- *Destination Port* - Số hiệu cổng trên máy nhận.
- *Message Length* - Chiều dài của dữ liệu trong đó cả phần Header và dũ liệu.
- *Trường Checksum*: là 16 bit bù một của phép tổng bù một của trường dữ liệu, có cả phần pseudoHeader giống như của TCP.

Trường checksum của UDP cũng có thể lựa chọn được, nhưng không được dùng. Không một checksum nào được dùng cho phần dữ liệu vì phần checksum của IP chỉ dùng cho phần Header IP mà thôi. Nếu phần checksum không được dùng thì các bit của trường này được thiết lập là 0.

Giao thức UDP được sử dụng trong một số tình huống đặc biệt :

- Khi truyền một dữ liệu nhỏ thì dùng UDP có hiệu quả hơn so với việc kết nối và hủy kết nối khi sử dụng TCP.
- Các ứng dụng hỏi đáp, mong muốn trả lời trong một thời gian ngắn sau khi người sử dụng gởi đi yêu cầu. Trả lời cũng là một cơ chế báo nhận. Người ta sử dụng giao thức UDP như trong các dịch vụ ứng dụng không yêu cầu độ chính xác cao như thông báo giờ hay các dịch vụ gởi nhắn tin, tỷ giá .. .

- Một số mô hình nén để truyền các thông tin audio, video, có thể chấp nhận được một vài gói dữ liệu bị hỏng hay thất lạc.
- Một vài ứng dụng có đô tin cậy riêng trong khi truyền dữ liệu thì nên dùng UDP hơn là TCP.

## 7.4 Cổng và Socket

### 7.4.1 Số hiệu cổng

Khi một máy khách kết nối vào máy chủ thì có thể yêu cầu nhiều dịch vụ khác nhau trên máy chủ. Mỗi dịch vụ đều có cách gởi và nhận dữ liệu theo quy ước riêng. TCP và UDP chỉ chịu trách nhiệm đưa dữ liệu từ một máy tính náy đến một máy tính khác, còn dữ liệu đó được gởi đến dịch vụ theo cách nào thì phải thông qua cổng của dịch vụ.

Cổng được đặc trưng bởi một số có giá trị từ 0 đến 65535. Các cổng chuẩn từ 0 - 1023 là cổng được dùng cho các dịch vụ phổ biến như FTP, eMAIL, POP3, HTTP, ... Không thể có hai tiến trình cùng sử dụng chung một số hiệu cổng.

Các số hiệu cổng (Port Numbers) được dùng thông dụng trong thực tế :

| UDP Port | | TCP Port | |
|---|---|---|---|
| 0 | Reversed | 0 | Reversed |
| 7 | Echo | 1 | TCP Multiplexor |
| 37 | Time | 20 | FTP_ Data Connection |
| 42 | Name Server | 21 | FTP_ Command Connection |
| 53 | Domain Name Server | 23 | TELNET |
| 69 | Trivial File Transfer Program ( TFTP ) | 25 | SMTP |
| 514 | System Log | 42 | Name Server |
| . . . . . | | 53 | Domain Name Server |
| | | 79 | Finger_ find a active user |
| | | 80 | HTTP |

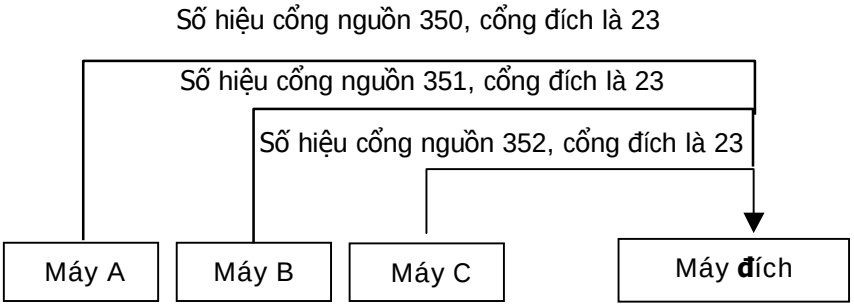
### 7.4.2 Socket

Mỗi socket xác định một điểm cuối trong liên kết truyền thông hai chiều giữa các tiến trình giao tiếp trên mạng, là đối tượng mà qua đó các dịch vụ ứng dụng truyền hoặc nhận các gói dữ liệu trên mạng. Khi cần gởi dữ liệu đi, các tiến trình ghi dữ liệu vào socket, khi có dữ liệu đến, các tiến trình sẽ đọc socket để lấy dữ liệu.

Trong những năm 80, do nhu cầu cần có một giao diện lập trình ứng dụng API (Application Programming Interface) để phát triển các trình ứng dụng trên mạng TCP/IP, giao diện socket đã được xây dựng lần đầu tiên trên hệ điều hành UNIX. Loại Berkelay Socket (Berkeley Software Distribution - BSD, tại Trường Đại học

- Loại socket : Stream socket hoặc Datagram socket.

Một liên kết giữa hai máy trên với nhau được xác định bởi một cặp socket : Socket (Host1, Port1) và Socket (Host2, Port2). Số **Socket** là duy nhất cho phép một tiến trình có thể giao tiếp với một tiến trình khác trên mạng.




Hình 7-7. Nhiều máy nguồn nối với một máy đích.

Một liên kết có thể được thiết lập theo một trong hai cách : chủ động (active) hoặc bị động. Các thực thể tầng trên sử dụng TCP thông qua bằng cách gọi các hàm dịch vụ nguyên thủy. Dịch vụ TCP được thiết lập nhờ một liên kết logic giữa một cặp Socket. Một Socket có thể tham gia nhiều liên kết với các Socket ở xa khác nhau. Vì các khung tin được đưa qua cổng đều có đầy đủ các thông tin về socket (với địa chỉ IP), cho nên không có xung đột dữ liệu xảy ra.

## 7.5 Mô hình giao tiếp Client/Server

TCP/IP phụ thuộc vào khái niệm máy khách (Client) và máy chủ (Server). Thuật ngữ Server dùng để chỉ những chương trình cung cấp các dịch vụ thông qua mạng. Các Server nhận đảm nhiệm chức năng đáp ứng các yêu cầu của máy khách, thực hiện việc phục vụ và trả lại kết quả. Thuật ngữ Client dùng để chỉ các chương trình ứng dụng gởi các yêu cầu đến Server và chờ kết quả trả về.

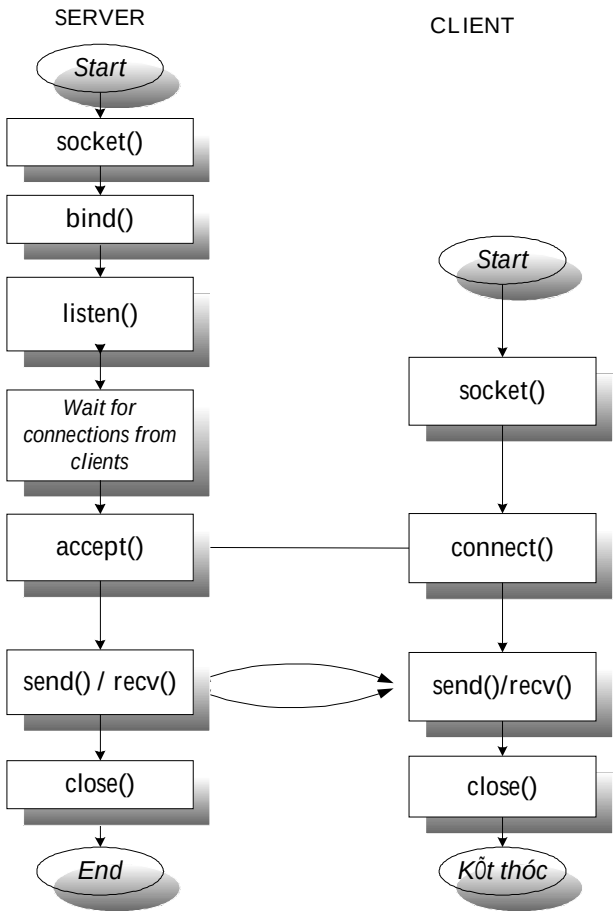
Các chương trình Client và Server thường thực thi trên các máy khác nhau. Mỗi chương trình Server có thể cùng đáp ứng cho nhiều chương trình Client trên nhiều máy tính khác nhau cùng một lúc.

### 7.5.1 Quá trình trao đổi dữ liệu dùng Stream Socket

Stream socket dựa trên nền giao thức TCP đòi hỏi phải tạo một kết nối trước khi hai bên có thể truyền hoặc nhận dữ liệu cho nhau. Stream Socket cung cấp một dòng các byte dữ liệu không có phân cách có thể truyền hai chiều. Các dòng dữ liệu có thể tin cậy được phân phát tuần tự, dữ liệu không trùng lắp, nghĩa là các gói dữ liệu được phân phát theo thứ tự được phát, và mỗi lần chỉ có một gói riêng biệt được truyền.

Dạng socket này rất thích hợp với mô hình Client/Server. Server sẽ tạo một socket, gán cho nó một tên (cung cấp một địa IP của máy và một port để giao tiếp), và đợi client nối kết đến socket. Bên client cũng tạo một socket và nối kết đến tên socket trên server. Khi server phát hiện có yêu cầu kết nối từ client, nó sẽ tạo một socket mới và sử dụng socket mới đó để giao tiếp với client. Socket cũ tiếp tục đợi kết nối từ các client khác.

Sơ đồ trao đổi dữ liệu giữa Client/Server bằng cách dùng Socket được biểu diễn như sau :



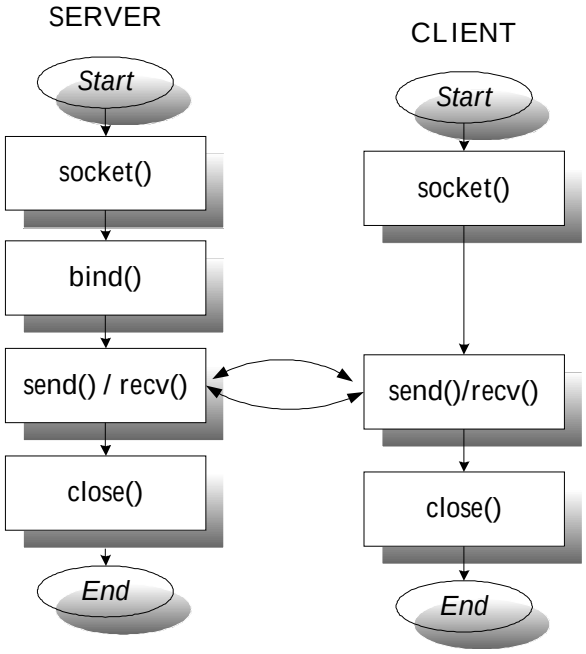

Hình 7-8. Sơ đồ trao đổi dữ liệu giữa Client/Server bằng StreamSocket.

### 7.5.2 Quá trình trao đổi dữ liệu dùng Datagram Socket

Datagram Socket dựa trên giao thức UDP không đòi hỏi phải thiết lập một kết nối trước khi truyền và nhận dữ liệu. Dữ liệu chỉ là một gói đơn, vì vậy dạng socket này thường dùng để truyền các mẫu tin, không cần nhiều các header lớp ứng dụng. Dạng socket này cung cấp luồng dữ liệu không bảo đảm theo thứ tự hoặc không bị trùng lắp, không bảo đảm dữ liệu sẽ đến được nơi nhận. Dữ liệu có thể đến không theo thứ tự được phát và có khả năng bị trùng lặp. Nhưng sự phân cách giữa các

mẫu tin thì được duy trì. Trong mạng LAN datagram có khả năng tin cậy tương đối tốt, nhưng trong mạng WAN, như mạng Internet thì không được đảm bảo.

§ Lưu đồ client/server sử dụng giao thức UDP




Hình 7-9. Sơ đồ trao đổi dữ liệu giữa Client/Server bằng DatagramSocket.

### 7.5.3 Ví dụ chương trình client/server

Trong ví dụ dưới đây chương trình server thực hiện các bước thiết lập cho việc chờ đợi một kết nối từ chương trình client. Sau khi thiết lập kết nối với client, cả hai thực hiện một số thao tác truyền và nhận thông tin rồi kết thúc chương trình.

#### *7.5.3.1 Mã lệnh chương trình Server*

- Tạo ra một socket với hàm *socket()*.
- Ràng buộc socket với một địa chỉ bằng hàm *bind ()*.
- Dùng hàm *listen()* để chờ đợi một kết nối.
- Nhận bất kỳ thông tin nào yêu cầu kết nối bằng hàm *accept()*.
- Nhận các thông báo gửi đến bằng hàm *read()* và gửi thông báo đến client bằng hàm *write()*.
-

```
/* mksock.c make and bind to a socket - userver*/
#include<stdio.h>
#include<sys/socket.h>
#include<sys/un.h>
#include<unistd.h>

void die(char * message);
void copyData(int from, int to);
```

```
int main(void) {
  struct sockaddr_un address;
  int sock,conn;
  size_t addrLength;
  if ((sock=socket(PF_UNIX,SOCK_STREAM,0))<0)
   die("socket");
/*unlik("./sample_socket");*/
  address.sun_family=AF_UNIX;
  strcpy(address.sun_path,"./sample_socket");

addrLength=sizeof(address.sun_family)+strlen(address.sun_path);
if(bind(sock,(struct sockaddr *)&address,addrLength))
  die("bind");
if(listen(sock,5))
  die("listen");
while((conn=accept(sock,(struct sockaddr*)&address,&addrLength))>=0) {
  printf("---getting data\n");
  copyData(conn,1);
  printf("---done\n");
  close(conn);
}
if (conn<0) die("accept");
close(sock);
return 0;
}
void die(char * message){
  perror(message);
  exit(1);
}
void copyData(int from,int to){
  char buf[1024];
  int amount;
  while ((amount=read(from,buf,sizeof(buf)))>0){
          if(write(to,buf,amount)!=amount){
                  die ("write");
                  return;
  }
}
if (amount<0) die("read");
}
```

### *7.5.3.2 Mã lệnh chương trình client*

Từ chương trình client , để thực hiện được một kết nối đến server và truyền nhận thông tin chỉ cần thực hiện 2 bước cơ bản như sau:

- Tạo một *socket()* tương ứng với chương trình *server* cụ thể .
- Yêu cầu đến server thực hiện kết nối bằng cách gọi hàm *connect()*.

Nếu một kết nối được tạo ra, client có thể gửi yêu cầu bằng hàm *write()* và nhận các đáp ứng phản hồi bằng hàm *read()*.

```
/* sockconn.c - connect to a socket - uclient*/
#include<sys/socket.h>
#include<sys/un.h>
#include<unistd.h>

void die (char * message);
```

```
void copyData(int from, int to);

int main(void){
  struct sockaddr_un address;
  int sock;
  size_t addrLength;

  if ((sock=socket(PF_UNIX,SOCK_STREAM,0))<0)        die("socket");
  address.sun_family=AF_UNIX;
  strcpy(address.sun_path,"./sample_socket");

  addrLength=sizeof (address.sun_family) + strlen(address.sun_path);
  if(connect(sock,(struct sockaddr *)& address,addrLength))   die("connect");
  copyData(0,sock);
  close(sock);
  return 0;
}
void die(char * message){
  perror(message);
  exit(1);
}
void copyData(int from, int to){
  char buf[1024];
  int amount;
  while ((amount=read(from,buf,sizeof(buf)))>0){
    if(write(to,buf,amount)!=amount) {
                    die("write");
                    return;
    }
  }
if (amount<0)      die("read");
}
```

---

# BÀI TẬP

1. Tìm hiểu các mô tả Socket và cấu trúc dữ liệu của socket mà hệ điều hành cấp phát để lưu trữ các thông tin cần thiết cho kết nối mạng.
2. Tìm hiểu các thư viện lập trình WinSock trên hệ điều hành Windows.
3. Viết các chương trình giao tiếp Client/Server theo mô hình giao tiếp TCP/IP hoặc UDP/IP.

*Chương 8*

# TẦNG PHIÊN

Tầng phiên (Session Layer) làm nhiệm vụ tổ chức và đồng bộ sự chuyển đổi dữ liệu giữa các tiến trình ứng dụng khác nhau. Tầng Phiên làm việc với tầng ứng dụng để cung cấp các tập dữ liệu, được gọi là các điểm đồng bộ, các điểm này cho phép một ứng dụng biết quá trình truyền và nhận dữ liệu được thực hiện như thế nào.

Tầng phiên chịu trách nhiệm thiết lập và duy trì một phiên truyền thông giữa hai trạm hoặc nút mạng. Một phiên truyền thông qua một mạng hoạt động có phần giống với một cuộc gọi qua các đường dây điện thoại. Tầng Phiên cố gắng thiết lập một phiên truyền thông giữa hai nút trên một mạng. Cả hai nút đều thừa nhận phiên truyền thông này thường sẽ được gán một số hiệu nhận diện. Mỗi nút có thể ngắt phiên truyền thông giữa hai nút trên một mạng được gọi là *một cổng luận lý* (Socket). Khi một phiên truyền thông được thiết lập, một cổng luận lý sẽ được mở ra. Một phiên truyền thông được kết thúc được gọi là *một cổng luận lý bị đóng* (Close Socket).

Mục tiêu của tầng phiên là có khả năng cung cấp cho người sử dụng các chức năng cần thiết để quản lý các phiên ứng dụng cụ thể như:

- Điều phối việc trao đổi dữ liệu giữa các ứng dụng bằng cách thiết lập và giải phóng (một cách ***logic***) các phiên (hay gọi là các hội thoại ***dialogues***).
- Cung cấp các điểm đồng bộ hóa để kiểm soát việc trao đổi dữ liệu.
- áp đặt các qui tắc cho các tương tác giữa các ứng dụng của người sử dụng.
- Cung cấp cơ chế lấy lượt (nắm quyền) trong các quá trình trao đổi dữ liệu.

Trong tầng phiên thì vấn đề đồng bộ hóa được thực hiện tương tự như một cơ chế kiểm tra / phục hồi (*check point/reset*).Trong một hệ quản trị tập tin, dịch vụ này cho phép người sử dụng xác định các điểm đồng bộ hóa trong dòng dữ liệu và có thể khôi phục lại việc hội thoại bắt đầu từ một trong các điểm đó.

## 8.1 Dịch vụ OSI cho tầng Phiên

Tầng phiên làm việc quản lý các cuộc thoại giữa hai máy tính bằng cách thiết lặp, quản lý, và kết thúc các phiên truyền thông.

### 8.1.1 Cung cấp cho người sử dụng dịch vụ tầng phiên (SS-user)

- Thiết lập một liên kết với một người sử dụng dịch vụ tầng phiên khác, trao đổi dữ liệu với người sử dụng đó một cách đồng bộ và hủy bỏ liên kết một cách có trật tự khi không dùng đến nữa.

- Thương lượng về việc dùng các thẻ bài (TOKEN) để trao đổi dữ liệu,đồng bộ hóa và hủy bỏ liên kết ,sắp xếp phương thức trao đổi dữ liệu (half-duplex hoặc full-duplex).
- Thiết lập các điểm đồng bộ hóa trong các hội thoại và khi xảy ra sự cố thì có thể khôi phục lại việc hội thoại bắt đầu từ một điểm đồng bộ hóa đã thỏa thuận.
- Ngắt hội thoại và khôi phục lại hội thoại sau đó từ một điểm xác định trước.

Các dịch vụ xác định điểm đồng bộ hóa là nhằm vào hai mục đích :

1) Các điểm đồng bộ hóa có thể phân tách các phần của một hội thoại.
2) Các điểm đồng bộ hóa có thể dùng để phục hồi lỗi.

*Các điểm đồng bộ hóa chính* dùng để cấu trúc quá trình trao đổi dữ liệu thành một chuỗi các đơn vị hội thoại (dialogue), mỗi điểm này phải được xác nhận và người sử dụng sẽ bị hạn chế trong một số dịch vụ nhất định cho tới khi nhận được một sự xác nhận mới. Một điểm đồng bộ hóa chính được dùng để tách biệt các hai đơn vị hội thoại liên tiếp.

*Các điểm đồng bộ hóa phụ* được dùng để cấu trúc quá trình trao đổi dữ liệu ở trong một đơn vị hội thoại, và các điểm này không cần phải được xác định trước.Việc dùng các điểm đồng hóa phụ trong quá trình truyền tập nó sẽ ngăn chặn việc truyền lại dữ liệu với một khối lượng lớn

*Một đơn vị hội thoại* là một Activity (hành động) nguyên tử trong đó mọi hành động truyền thông không có liên quan gì đến bất kỳ một hoạt động truyền thông nào trước và sau đó. Một hành động bao gồm nhiều đơn vị hội thoại, và đây cũng chính là một tập hợp logic các nhiệm vụ liên quan với nhau; ở một thời điểm thì chỉ có một activity trên một liên kết phiên nhưng một activity thì có thể diễn ra trên nhiều liên kết phiên, nó có thể bị ngắt và sau đó có thể khôi phục lại trong một liên kết phiên khác, một vòng đời của một liên kết phiên thì có thể có nhiều Activity liên tiếp.

### 8.1.2 Điều khiển trao đổi dữ liệu

Việc trao đổi dữ liệu xảy như sau để thực hiện một trong ba phương thức như sau : hai chiều đồng thời (*full-duplex*), hai chiều luân phiên (*haft -duplex*), một chiều (*simplex*).

#### *8.1.2.1 Trao đổi dữ liệu một chiều*

Liên quan đến các đợt chuyển giao dữ liệu một chiều. Báo cháy là một ví dụ, nó gửi một thông điệp báo động đến trạm chống cháy, nhưng không thể (và không cần) nhận các thông điệp từ trạm chống cháy.

Với phương thức một chiều thì ít xảy ra: chẳng hạn như dữ liệu được gửi đến một đối tượng tạm thời không làm việc, thì chỉ có một chương trình nhận với một nhiệm vụ duy nhất là tiếp nhận dữ liệu đến và giữ lại.

#### *8.1.2.2 Trao đổi dữ liệu hai chiều luân phiên*

Liên quan đến các đợt chuyển giao dữ liệu hai chiều, ở đó các luồng dữ liệu mỗi lần đi theo mỗi hướng. Khi một thiết bị hoàn tất một phiên truyền, nó phải " trả lại " vật tải cho thiết bị kia để đến phiên thiết bị đó được truyền.

Với phương thức luân phiên hai chiều thì nảy sinh các vấn đề như sau :

- Các đối tượng sử dụng phiên phải “lấy lượt” để truyền dữ liệu (điển hình của phương thức này là dùng cho các ứng dụng hỏi đáp).
- Thực thể tầng phiên *(session entity)* duy trì tương tác luân phiên bằng cách báo cho các đối tượng khi đến lược họ sẽ truyền dữ liệu.

#### *8.1.2.3 Trao đổi dữ liệu hai chiều đồng thời.*

Cho phép tiến hành các đợt chuyển giao dữ liệu hai chiều đồng thời bằng cách cung cấp cho mỗi thiết bị một kênh truyền thông riêng biệt. Điện thoại tiếng là những thiết bị song công đầy đủ, và một trong hai bên của một cuộc đàm thoại có thể nói bất kỳ lúc nào. Hầu hết các môđem máy tính đều có thể hoạt động theo chế độ song công đầy đủ.

Chế độ truyền thông bán song công có thể dẫn đến tình trạng băng thông bị lãng phí trong quãng thời gian mà đợt truyền thông đang quay trả. Trong khi đó, chế độ truyền thông song công đầy đủ thường yêu cầu một ban thông lớn hơn so với chế độ truyền thông bán song công

Với phương thức hai chiều đồng thời thì cả hai bên cùng đồng thời gửi dữ liệu cùng một lúc, một khi phương thức này đã được thỏa thuận thì không đòi hỏi phải có nhiệm vụ quản trị tương tác đặt biệt đây cũng là một phương thức phổ biến nhất.

### 8.1.3 Điều hành phiên làm việc

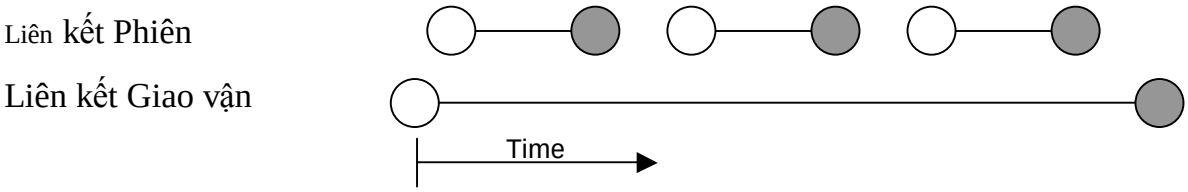
Phiên làm việc (session) là một cuộc thoại chính thức giữa một bên yêu cầu dich vụ và một bên cung cấp dịch vụ. Các phiên bản làm việc thường có ít nhất ba giai đoạn :

- *Thiết lập tuyến liên kết :* Bên yêu cầu dịch vụ sẽ yêu cầu khởi phát một dịch vụ. Trong quá trình xác lập, phiên truyền thông được thiết lập và các quy tắc được thoả thuận.
- *Chuyển giao dữ liệu* : Do các quy tắc được thoả thuận trong khi xác lập, nên mỗi bên của cuộc thoại sẽ biết nội dung mong đợi. Phiên truyền thông sẽ hữu hiệu và các lỗi cũng dễ phát hiện.
- *Giải phóng các kết nối* : Khi hoàn tất phiên làm việc, cuộc thoại kết thúc trong trật tự.

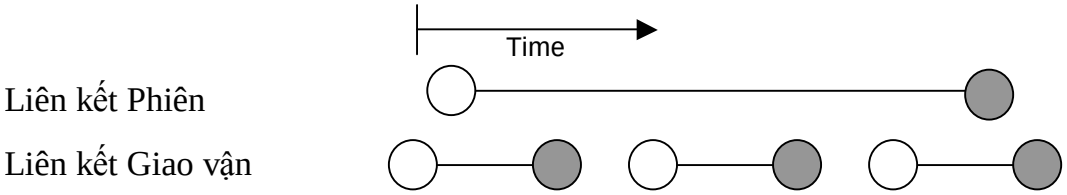
### 8.1.4 Liên kết phiên

Tầng Phiên thực hiện đặt tương ứng liên kết phiên với các liên kết giao vận. Trong một quá trình liên kết có thể xảy ra 2 trường hợp :

1. Một liên kết giao vận thiết lập với nhiều liên kết phiên liên tiếp :




2. Nhiều liên kết giao vận sử dụng cùng một liên kết phi[a]n:




Ký hiệu : : Thiết lập liên kết

: Giải phóng liên kết

## 8.2 Giao thức chuẩn tầng phiên

Giao thức chuẩn tầng phiên sử dụng tới 34 loại đơn vị dữ liệu (SPDU) khác nhau,và có khuôn dạng tổng quát như sau :

Trong đó :

- SI: Định danh của loại SPDU (một trong 34 loại)

- LI(length indicator): Chỉ độ dài của vùng tham số(parameters)
- PARAMETERS: vùng khai báo các tham số SPDU, mỗi loại SPDU có danh sách tham số riêng. Mỗi tham số được khai báo dưới dạng tổng quát gồm 3 vùng con : parameter identifier, length indecation, parameter value và chúng được gọi theo đơn vị pi hoặc PGI (mỗi đơn vị PGI gồm có 3 vùng con: PGI, LENGTH INDICATION, PARAMETER VALUE).
- User data: chứa dữ liệu của người sử dụng.

### 8.2.1 Các loại SPDU, các tham số và chức năng

| SPDU | PARAMENTERS | FUNCTION |
|---|---|---|
| CONNECT | Connection ID, Protocol Options, Version Number, Serial Number, Token setting, Maximum TSDU size, Requirements, Calling SSAP, Called SSAP, User Data. | Initiate session Connection |
| ACCEPT | Same as CONNECT SPDU. | Etablist SESSION CONNECTION |
| REFUSE | Connection ID, Transport disconnect, Requirements, Version number, Season. | Reject connection request |
| FINISH | Transport Disconnect, User Data. | Initiate Orderly Release |
| DISC0NNECT | User Data. | Acknowledge orderly Release |
| NOT FINISHED | User Data. | Reject Orderly Release |
| ABORT | Transport disconnect, Protocol Error Code, User Data. | Abnormal connection Release |
| ABORT ACCEPT | Transport disconnect, Protocol Error Code, User Data. | Acknowledge Abort |
| DATA TRANSFER | Enclosure item,User Data. | Transfer normal Data |
| EXPEDITED | User data. | Transfer typed data |
| CAPABILITY DATA ACK | User Data. | Acknowledge Capability data |
| GIVE TOKENS | Tokens. | Transfer tokens |
| PLEASE TOKENS | Tokens , User Data. | Request token Assignment |
| GIVE TOKENS CONFIRM | - | Transfer all tokens |
| GIVE TOKENS ACK | - | Acknowledge all tokens |
| MONOR SYNC POINT | Confirm required flag, Serial number, User data. | Define minor sync point |
| MINOR SYNC ACK | Serial number, User Data. | Acknowledge minor sync point |
| MAJOR SYNC POINT | End of activity flag, Serial number, User Data. | Define major sync point |
| MAJOR SYNC ACK | Serial number,User data. | Acknowledge major sync point |
| RESYNCHRONIZED | Tokens sittings, resync type, serial number, user data. | Resynchorize |
| RESYNCHRONIZED ACK | Tokens settings, Serial number, User Data. | Acknowledge resynchronize |

| | | |
|---|---|---|
| PREPERE | Type. | Notify type SPDU is coming |
| EXCEPTION REDORT | SPDU bit pattem. | Protocol Error detected |
| EXCEPTION DATA | Reason, User Data. | Put protocol in Error state |
| ACTIVITY START | Activity ID, User data. | Signal beginning of activity |
| ACTIVITY RESUME | Connect ID, Old activity ID, New Activity ID, User data. | Signal resumption of activity |
| ACTIVITY INTERRUPT | Reason. | Interrupt activity |
| ACTIVITY INTERRUPT ACK | - | Acknowledge interrupt |
| ACTIVITY DISCARD | Reason. | Cancel activity |
| ACTIVITY DISCARD ACK | - | Acknowledge cancellation |
| ACTIVITY END | Serial number/User data. | Signal activity end |
| ACTIVITY END ACK | Serial number/User data. | Acknowledge activity end |

Tầng Phiên đóng một vai trò quan trọng trong việc trao đổi thông tin giữa các máy Client với máy Server. Nhưng thông tin mà chúng ta cần truyền tải thì được chia nhỏ ra thành các khung (hay gói) trước khi chúng được truyền tải qua một mạng. Mỗi tầng của mô hình 7 tầng OSI đều có thể bổ sung thêm các thông tin vào đoạn đầu và đoạn cuối của một khung dữ liệu vvà sau đó các thông tin này sẽ được đọc bởi tầng tương đương ở máy trạm tiếp nhận. Và một số tầng khác có thể bổ sung thêm phần đầu(header) và cả một phần đuôi(trailer) vào khung dữ liệu có sẵn. Sau đó, khung dữ liệu này truyền chuyển tới tầng tương đương trên trạm tiếp nhận.

*Chương 9*

# TẦNG TRÌNH DIỄN

Tầng Trình diễn có nhiệm vụ phân cách giữa các tầng cao hơn và các tầng thấp hơn từ định dạng dữ liệu của tầng ứng dụng, chuyển đổi định dạng dữ liệu từ định dạng của tầng ứng dụng thành định dạng thông thường, gọi là "trình diễn hợp với quy tắc". Tầng Trình diễn xử lý dữ liệu không phụ thuộc vào máy tính từ tầng ứng dụng thành dữ liệu có định dạng phụ thuộc vào máy tính để chuyển cho các tầng thấp hơn.

Tầng trình diễn xử lý cú pháp, hoặc các quy tắc văn phạm, cần thiết cho phiên truyền thông giữa hai máy tính, bảo đảm cho các hệ thống cuối truyền th6ng có kết quả khi chúng sử dụng các dạng biểu diễn dữ liệu khác nhau. Tầng này trình bày một dạng thức dữ liệu đồng dạng cho tầng ứng dụng.

## 9.1 Vai trò và chức năng

Mục đích của tầng trình diễn là đảm bảo cho các hệ thống cuối có thể truyền thông có kết quả ngay cả khi chúng sử dụng các biểu diễn dữ liệu khác nhau .Để đạt được điều đó nó cung cấp một biểu diễn chung để dùng trong truyền thông và cho phép chuyển đổi từ biểu diễn cục bộ sang biểu diễn chung đó.

Tồn tại 3 dạng cú pháp thông tin được trao đổi giữa các thực thể ứng dụng :

- Cú pháp dùng bởi thực thể ứng dụng nguồn.
- Cú pháp dùng bởi thực thể ứng dụng đích.
- Cú pháp dùng bởi giữa các thực thể trình diễn ,loại cú pháp này gọi là cú pháp truyền (transfer syntax).

Tầng trình diễn đảm nhận việc chuyển đổi biểu diễn thông tin giữa cú pháp truyền và mỗi một cú pháp kia khi có yêu cầu

Chú ý rằng không tồn tại một cú pháp truyền xác định trước duy nhất cho mọi hoạt động trao đổi dữ liệu. Cú pháp truyền được duy nhất cho mọi hoạt động trao đổi dữ liệu. Cú pháp truyền được sử dụng trên một liên kết cụ thể của tầng trình diễn phải được thương lượng giữa các thực thể trình diễn tương ứng. Mỗi bên lựa chọn một cú pháp truyền sao cho có thể sẵn sàng được chuyển đổi sang cú pháp người sử dụng và ngược lại. Ngoài ra cú pháp truyền được chọn phải phản ánh các yêu cầu dịch vụ khác chẳng hạn nhu cầu nén dữ liệu .việc thương lượng cú pháp truyền sử dụng có thể được thay đổi trong vòng đời liên kết đó .Tầng trình diễn chỉ liên quan đến cú pháp truyền vì thế trong giao thức sẽ không quan tâm đến các cú pháp sử dụng bởi thực thể ứng dụng. Tuy nhiên mỗi thực thể trình diễn phải chịu trách nhiệm chuyển đổi giữa cú pháp người sử dụng và cú pháp truyền.

Các khái niệm liên quan đến bối cảnh của tầng trình diễn : Khi qua ranh giới giữa hai tầng trình diễn và tầng phiên có một sự thay đổi quan trọng trong cách nhìn dữ liệu. Đối với tầng phiên trở xuống tham số User Data trong các service primitives được đặc tả dưới dạng nhị phân (một chuỗi các byte). Giá trị này có thể được đưa vào trực tiếp trong các SDU (Service Data Unit) để chuyển giữa các tầng trong một hệ thống và trong các PDU (Protocol Data Unit) để chuyển giữa các tầng đồng mức ở hệ thống kết nối với nhau. Tuy nhiên tầng ứng dụng lại liên quan chặt chẽ với cách nhìn dữ liệu của người sử dụng nói chung cách nhìn đó là một tập thông tin có cấu trúc nào đó như là văn bản (text) trong một tài liệu một tệp về nhân sự hoặc một cơ sở dữ liệu .... Người sử dụng chỉ quan tâm đến ngữ nghĩa (semantics) của dữ liệu. Do đó tầng trình diễn ở giữa chỉ có nhiệm vụ cung cấp phương thức biểu diễn dữ liệu và chuyển đổi thành các giá trị nhị phân dùng cho các tầng dưới nghĩa là tất cả những gì liên quan đến cú pháp của dữ liệu

Tuy nhiên trong thực tế không thể tách bạch hoàn toàn giữa cú pháp và ngữ nghĩa và ngữ nghĩa dữ liệu. Nếu tầng ứng dụng không biết gì về cú pháp thì tầng trình diễn không biết gì về nhữ nghĩa thì không thể nào hoàn tất được việc kết hợp ngữ nghĩa với cú pháp dùng để tạo ra một biểu diễn cụ thể các giá trị dữ liệu cho dịch vụ phiên.

ở tầng ứng dụng thông tin được biểu diễn dưới dạng cú pháp trừu tượng (abstract syntax) liên quan đến các kiểu dữ liệu (data values) cú pháp trừu tượng này đặc tả một cách nhìn hình thức dữ liệu độc lập với mọi biểu diễn cụ thể.

Do vậy một cú pháp trừu tượng có nhiều đặc điểm giống kiểu dữ liệu như các ngôn ngữ lập trình Pascal, C .... Các ngữ nghĩa như là BNF. Các giao thức tầng ứng dụng mô tả các PDU của chúng bằng một cú pháp trừu tượng. Tầng trình diễn tương tác với tầng ứng dụng cũng dựa trên cú pháp trừu tượng này, tầng trình diễn có nhiệm vụ dịch thuật cú pháp trừu tượng của tầng ứng dụng và cú pháp truyền (transfer syntax) mô tả các giá trị dữ liệu dưới dạng nhị phân thích hợp cho việc tương tác với dịch vụ phiên việc dịch thuật này được thực hiện nhờ qui tắc mã hoá chỉ rõ biểu diễn của mỗi giá trị dữ liệu thuộc một kiểu nào đó .

Trước khi sử dụng liên kết của một tầng trình diễn để trao đổi dữ liệu thì hai thực thể trình diễn ở hai đầu phải thoả thuận về cú pháp truyền được xem như là bối cảnh trình diễn (presentation context) được dùng để trao đổi dữ liệu

Cú pháp truyền phải yểm trợ cú pháp trừu tượng tương ứng. Ngoài ra cú pháp truyền có thể có các thuộc tính khác không liên quan gì đến cú pháp trừu tượng mà nó yểm trợ ví dụ một cú pháp trừu tượng có thể yểm trợ bởi bất kì một cú pháp truyền về cơ bản thì giống nhau chỉ khác nhau ở chỗ một cung cấp khả năng mật mã, một chỗ cung cấp cả hai và một không cung cấp khả năng nào.

### 9.1.1 Phiên dịch dữ liệu

Một mục tiêu quan trọng cần giải quyết khi thiết kế các mạng đó là cho phép kiểu máy tính khác nhau trao đổi dữ liệu. Tuy mục tiêu này ít khi được giải quyết toàn vẹn, nhưng việc vận dụng hiệu quả các kỹ thuật phiên dịch dữ liệu có thể giúp nhiều kiểu máy tính truyền thông với nhau. Có bốn dạng phiên dịch dữ liệu, thứ tự bít, thứ tự byte, mã ký tự, và cú pháp tập tin như sau :

- Thứ tự bit : Khi số nhị phân được truyền qua một mạng, chúng gởi đi theo từng bit, thứ tự byte, mã ký tự, và cú pháp tập tin.
- Phiên dịch thứ tự Byte : Các giá trị phức tạp thường phải được biểu thị bằng nhiều byte, nhưng các máy tính khác nhau thường dùng quy ước khác nhau về việc sẽ truyền byte nào trước. Các bộ vi xử lý Intel bắt đầu bằng byte ít quan trọng nhất. Do chúng bắt đầu tại đầu nhỏ, nên được gọi là kết đầu nhỏ. Các bộ vi xử lý Motorola bắt đầu bằng byte quan trọng nhất. Để hoà hợp những khác biệt này, ta cần phải có tính năng phiên dịch thứ tự byte.
- Phiên dịch mã ký tự : Hầu hết các máy tính đều dùng một trong các bảng mã đánh số nhị phân dưới đây để biểu thị các bộ ký tự : Bảng mã ASCII được dùng để biểu thị các ký tự tiếng Anh trên tất cả máy tính và hầu hết các máy tính mini. EBCDIC (Extended Binary Coded Decimal Interchange Code = Mã hoán đổi thập phân mã hoá nhị phân mở rộng) được dùng để biểu thị cho các ký tự tiếng Anh trên máy tính lớn nhất.
- Phiên dịch cú pháp tập tin : Khi các dạng thức tập tin khác nhau giữa các máy tính, các dạng đó đòi hỏi phải phiên dịch.

## 9.2 Dịch vụ OSI cho tầng trình diễn

Dịch vụ OSI cho tầng trình diễn có 2 loại : một loại bao gồm các dịch vụ liên quan đến biểu diễn của dữ liệu người sử dụng để đảm bảo cho hai thực thể ứng dụng có thể trao đổi dữ liệu thành công ngay khi chúng dùng các biểu diễn cục bộ khác nhau cho dữ liệu đó, loại thứ hai bao gồm các dịch vụ cho phép các thực thể ứng dụng có thể sử dụng các dịch vụ tầng phiên để quản lý hội thoại.

Để cung cấp loại dịch vụ thứ nhất tầng trình diễn thực hiện hai nhiệm vụ sau :

- Thương lượng về cú pháp truyền : với mỗi kiểu dữ liệu người sử dụng cho trước một cú pháp truyền được thương lượng.
- Chuyển đổi : dữ liệu cung cấp bởi người sử dụng được chuyển đổi thành biểu diễn theo cú pháp truyền để truyền đi , ngược lại dữ liệu nhận được để giao cho người sử dụng sẽ chuyển đổi từ biểu diễn theo cú pháp truyền sang biểu diễn của người sử dụng.

ở thời điểm bất kì trong vòng đời của một liên kết trình diễn dịch vụ trình diễn dịch vụ trình diễn có liên quan đến một hoặc nhiều bối cảnh trình diễn (presentation context). Mối bối cảnh chỉ rõ cú pháp trừu tượng của dữ liệu đó. Có hai loại bối cảnh được sử dụng :

- Defined context set : bao gồm các bối cảnh đã được xác định thông qua sự thoả thuận giữa người sử dụng dịch vụ trình diễn (presentation service user) vaf người cung cấp dịch vụ trình diễn (presentation service provider).
- Default context : là một bối cảnh trình diễn mà người cung cấp dịch vụ trình diễn luôn luôn biết rõ và người sử dụng khi vắng mặt

Ở tầng phiên do kiến trúc phân tầng của ISO các thực thể ứng dụng không thể truy cập trực tiếp tới các dịch vụ tầng phiên, do vậy các yêu cầu dịch vụ liên quan đến tầng phiên phải được chuyển qua tầng trình diễn đến các dịch vụ tầng phiên.

## 9.3 Giao thức chuẩn tầng trình diễn

Giao thức chuẩn của ISO/CCITT cho tầng Trình diễn đặc tả những nội dung chính sau đây:

- Cấu trúc và mã hoá các đơn vị dữ liệu của giao thức trình diễn (PPDU) dùng để truyền dữ liệu và thông tin điều khiển .
- Các thủ tục để truyền dữ liệu và thông tin điều khiển giữa các thực thể trình diễn của hai hệ thống mở.
- Liên kết giữa giao thức trình diễn với dịch vụ trình diễn và với dịch vụ phiên .

Cũng như các PDU ở các tầng khác ,các PPDU cũng có khuôn dạng tổng quát bao gồm một phần đầu (header ) chứa các thông tin điều khiển và có thể thêm mmột phần chứa dữ liệu được truyền từ trên xuống hoặc được truyền lên cho tầng trên. Giao thức trình diễn sử dụng 14 PPDU được liệt kê trong bảng 2-17 cùng với các tham số của chúng .

Qua bảng trên ta thấy số lượng PPDU không nhiều như số lượng SPDU (ở tầng Phiên) và nhiều tham số (có đánh dấu *) là giống với các tham số của các SPDU. Như vậy cả về phương diện dịch vụ và giao thức, tầng trình diễn và tầng Phiên có một mối liên kết rất chặt chẽ .

Qua xem xét các tầng dưới từ tầng phiên trở xuống, chúng ta thấy có 2 nguyên lý sau đây luôn được tuân thủ :

- Mỗi dịch vụ tầng n được cài đặt nhờ trao đổi các nPDU;
- Mỗi nPDU trở thành User data và được “nhét” vào trong một (n-1) PDU;

Tuy nhiên ở tầng trình diễn (và cả ở tầng ứng dụng mà ta sẽ thấy), các nguyên lý đó không còn luôn luôn được áp dụng .Thực tế là không phải mọi dịch vụ trình diến đều yêu cầu các PPDU và một số tham số của một số PPDU không được chuyển thành User data trong một SPDU. Để giải thích động cơ củ a sự khác biệt đó, ta xem xét hai dịch vụ trình diễn : thiết lập liên kết (connection etablishment) và chuyển thẻ bài (token passing).

Khi phát triển các giao thức cho 3 tầng cao của Mô hình óI,người ta thấy rõ ràng nên thương lượng và thiết lập đồng thời các liên kết Phiên ,trình diễn và ứng dụng,mặc dù điều đó đòi hỏi một quan hệ 1-1 chặt chẽ (không có dồn kênh) với cùng vòng đời cho cả ba loại liên kết .Quá trình thiết lập đồng thời các liên kết đó được gọi là quá trình nhúng (embeding), vì các PDU CONNECT.request và CONNECT.response cho cả ba tầng cao đó ,cái này được nhúng vào trong cái kia.

Khuôn dạng của các PDDU header được đặc tả theo cú pháp trừu tượng chuẩn.

### 9.3.1 Các chuẩn khác cho tầng trình diễn

Ngoài các chuẩn về dịch vụ và giao thức cho tầng Trình diễn như đã trình bày ở trên, ISO và CCITT đã phát triển các chuẩn liên quan đến cú pháp trừu tượng (Abstract Syntas) và quy tắc mã hoá (Encoding Rules) mà chúng ta đã nói đến khi trình bày vai trò và chức năng của tầng Trình diễn

Các chuẩn của ISO gồm có :

- ISO 8824:Abstract Syntax Notation One(viết tắt là ASNI.1)
- ISO 8825:Báic Encoding Rules(Viết tắt là BER)
- Tương ứng CCITT có các khuyến nghị X208 (ANSI.1) và X.209 (BER).

Khái niệm cú pháp trừu tượng mà ISO và CCITT định nghĩa được dựa trên khái niệm kiểu dữ liệu (data type) mà chúng ta đã quen thuộc trong các ngôn ngữ lập trình phổ biến. Thông thường các ngôn ngữ này định nghĩa trước các kiểu dữ liệu đơn giản như integer và boolean, cùng với các phương thức tổ hợp các kiểu đơn giản đó để có các cấu trúc dữ liệu phức tạp hơn. Hơn nữa, các phương pháp tổ hợp có thể thực hiện một cách đệ quy cho phép tạo ra các kiểu phức tạp tuỳ ý.

*Chương 10*

# TẦNG ỨNG DING

Tầng ứng dụng giao tiếp trực tiếp với người sử dụng. Nhiệm vụ của tầng ứng dụng là hiển thị các thông tin nhận được và gửi các thông tin mới của người sử dụng cho các tầng thấp hơn.

Tầng ứng dụng liên quan đến tiến trình cung cấp các dịch vụ trên mạng, các dịch vụ này bao gồm : dịch vụ tập tin, dịch vụ in, dịch vụ cơ sở dữ liệu, và các dịch vụ khác.

Chúng ta sẽ xem xét các vấn đề trước khi bắt đầu với các ứng dụng. Đó là sự an toàn mạng, dịch vụ tên miền DNS dùng để điều khiển đặt tên trong Internet, giao thức hỗ trợ quản trị mạng, phần còn lại là các ứng dụng thực như thư điện tử, UserNet, FTP, Telnet, WWW ...

## 10.1 An toàn thông tin trên mạng

Việc kết nối mạng máy tính nhằm sử dụng và chia sẻ tài nguyên của các đối tượng trong hệ thống mạng cho dù họ có thể cách xa nhau về mặt địa lý. Tài nguyên hệ thống ở đây chủ yếu là là thông tin. Tuy nhiên đây là loại tài nguyên dễ bị xâm phạm, bị đánh cắp, bị tráo đổi nhất, đặc biệt là nó đang được trong lưu giữ trong môi trường mạng đầy phức tạp và phải chia xẻ cho nhiều người dùng khác nhau ở những vị trí khác nhau.

Vấn đề an toàn thông tin trên mạng đòi hỏi phải sử dụng nhiều biện pháp khác nhau từ cơ bản đến phức tạp, tuỳ theo lượng thông tin cần bảo vệ và khả năng cho phép của từng hệ thống cụ thể.

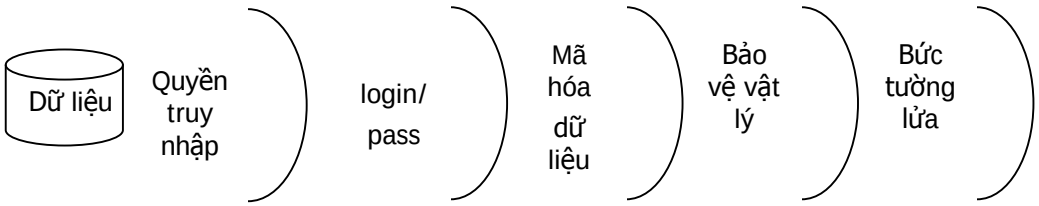
### 10.1.1 Các chiến lược an toàn hệ thống

1. Quyền hạn tối thiểu : Đây là chiến lược nền tảng nhất. Theo nguyên tắc này bất kì đối tượng nào cũng chỉ có những quyền hạn nhất định đối với những tài nguyên mạng nhất định khi thâm nhập vào mạng.
2. Bảo vệ theo chiều sâu : Tạo nhiều cơ chế an toàn cho hệ thống để chúng hỗ trợ cho nhau.
3. Cơ chế nút thắt : Tạo ra một “cửa khẩu” hẹp và chỉ cho phép thông tin đi vào hệ thông của mình bằng duy nhất con đường này. Đồng thời phải tổ chức một cơ chế kiểm soát và điều khiển các luồng thông tin đi qua cửa khẩu này.
4. Tính toàn cục : Các hệ thống an toàn đòi hỏi phải có tính toàn cục của các hệ thống cục bộ. Nếu có kẻ nào đó có thể bẻ gãy một cơ chế an toàn thì chúng có thể thành công bằng cách tấn công hệ thống nội bộ từ bên trong.

5. Tính đa dạng của việc bảo vệ : Cần phải sử dụng nhiều biện pháp khác nhau cho những hệ thống khác nhau. Nếu không, kẻ nào đó tấn công được hệ thống này thì cũng có thể tấn công vào hệ thống khác.

- Các mức bảo vệ thông tin trên mạng:

Vì không có một giải pháp bảo vệ nào an toàn tuyệt đối nên người ta thường sử dụng nhiều mức bảo vệ khác nhau tạo thành nhiều lớp rào chắn cho hệ thống. Mô hình như sau :




Hình 10-1. Các mức bảo vệ thông tin trên mạng.

### 10.1.2 An toàn thông tin bằng mã hóa

Để bảo vệ thông tin trên đường truyền, người ta chuyển đổi nó từ dạng nhận thức được sang dạng không nhận thức được trước khi truyền đi trên mạng nhằm bảo đảm tính bí mật cần thiết. Quá trình này diễn ra ở trạm phát được gọi là mã hoá thông tin (encrypting), ở trạm nhận phải thực hiện quá trình ngược lại, tức là biến đổi thông tin từ dạng không nhận thức được (đã mã hoá) sang dạng nhận thức được (dạng gốc), quá trình này gọi là giải mã (decrypting). Đây là một lớp bảo vệ thông tin rất quan trọng và được ứng dụng trong hầu hết các hệ thống mạng.

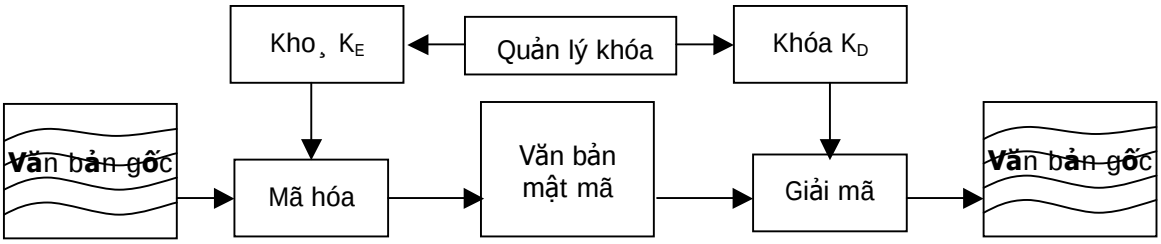
Để bảo vệ thông tin bằng mật mã, người ta thường tiếp cận theo hai hướng:

- Từ nút đến nút (end_to_end )
- Theo đường truyền (link_oriented security)

Theo cách thứ nhất, thông tin được mã hoá để bảo vệ trên đường truyền giữa hai nút mà không quan tâm đến nguồn và đích của thông tin đó. Ớ đây ta chú ý rằng thông tin chỉ được bảo vệ trên đường truyền, tức là ở mỗi nút đều có quá trình giải mã để sau đó thông tin được chuyển đi tiếp, do đó các nút cần được bảo vệ tốt.

Ngược lại theo cách thứ hai, thông tin trên mạng được bảo vệ trên toàn đường truyền từ nguồn đến đích. Thông tin sẽ được mã hoá ngay sau khi mới tạo ra và chỉ được giải mã khi đã về đến đích. Cách này có nhược điểm là chỉ có dữ kiệu người dùng mới được mã hoá còn các thông tin điều khiển thì phải giữ nguyên để có thể xử lí tại các nút.

Quá trình mã hoá và giải mã được mô tả như sau :




Hình 10-2. Sơ đồ quá trình mã hóa.

+ Văn bản gốc (plaintext) là văn bản chưa được mã hoá.

+ Khoá (key) : gồm một số hữu hạn các bit thường được biểu thị dưới dạng các xâu kí tự chữ số, số thập phân hoặc thập lục phân. Trong thực tế thường dùng các khoá có 8 kí tự.

Nếu gọi : M là văn bản gốc

C là văn bản mật mã (Ciphertext)

E là hàm mã hoá (Encryption Function )

D là hàm giải mã (Descryption Function)

Ta có hàm biểu diễn sự phụ thuộc giữa văn bản gốc và văn bản mã như sau:

$C = E(M)$

$M = D(C) = D(E(M))$

Khoá KE được dùng để mã hoá, khoá KD được dùng để giải mã .

Có rất nhiều phương pháp mã hoá nhưng tất cả đều qui về 2 phương pháp chung tuỳ theo việc sử dụng cặp khoá KD và KE:

- Khoá KD trùng với khoá KE : phương pháp này gọi là mã hoá khoá đối xứng, với phương pháp này yêu cầu khoá phải được giữ bí mật tuyệt đối, vì khoá dùng để mã hoá cũng được dùng giải mã.
- Khoá KD khác với khoá KE : phương pháp này gọi là mã hoá khoá công khai. Trong đó, có thể chuyển đổi vai trò giữa 2 khoá và rất khó để suy ra khoá này từ khoá kia. Khoá mã hoá (KE) có thể đưa ra công khai nhưng khoá dùng giải mã (KD) phải được giữ bí mật tuyệt đối.

Người ta còn phân biệt 2 loại khóa:

- Các khoá dùng trong thời gian dài gọi là khoá chính (primary) hay khoá mã hoá (key encryption).
- Các khoá được dùng trong khuôn khổ một cuộc truyền thông gọi là khoá làm việc (working) hay khoá mã hoá dữ liệu (data encryption).

## 10.2 CáC phương pháp mã hóa dữ liệu

### 10.2.1 Phương pháp hoán vị

Phương pháp này sắp xếp lại các kí tự trong văn bản gốc để tạo ra văn bản mật mã. Phương pháp này có một số kỹ thuật sau :

*1. Đảo ngược toàn bộ văn bản gốc*

Từ văn bản gốc, ta mã hoá bằng cách viết theo thứ tự ngược lại. Ví dụ DHKTDN được mã hoá thành NDTKHD. Đây là một trong những phương pháp mã hoá đơn giản nhất và chỉ mang tính tham khảo vì không an toàn.

2. *Mã hoá theo mẫu hình học*

Sắp xếp lại văn bản gốc theo mẫu hình học nào đó (thường là ma trận 2 chiều) để tạo văn bản mật mã.

Ví dụ : ĐAIHOCĐANANG được viết thành ma trận 3 x 4:

| | | | |
|---|---|---|---|
| Đ | A | I | H |
| O | C | Đ | A |
| N | A | N | G |

Nếu ta lấy các kí tự ra theo thứ tự các hàng là 3,1,2 ta sẽ có văn bản mật mã là N A N G O C Đ A Đ A I H. Phương pháp cũng kém an toàn, có thể dựa vào tần số xuất hiện của các kí tự trong bản mã để suy ra văn bản gốc.

3. *Đổi chổ cột*

Sắp xếp lại văn bản gốc thành dạng hình chữ nhật theo các cột, sau đó các cột được sắp xếp lại và lấy các kí tự theo chiều ngang.

Ví dụ : văn bản TRUONGDAIHOCKYTHUATDANANG được viết thành ma trận 5 x 5 :

| Cột | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| Văn bản | T | R | U | O | N |
| | G | D | A | I | H |
| | O | C | K | I | T |
| | H | U | A | T | D |
| | A | N | A | N | G |

Vì có 5 cột nên có thể sắp xếp lại theo 5!= 120 cách khác nhau. Nếu ta chuyển vị các cột theo thứ tự 2,3,4,1,5 rồi lấy các kí tự theo hàng ta sẽ có văn bản mã như sau: RUOTN DAIGH CKYOT UATHD NANAG.

Ta thấy rằng, với một văn bản càng lớn (nhiều kí tự) số cách sắp xếp có thể sẽ rất lớn làm tăng khả năng an toàn. Hạn chế của phương pháp này là toàn bộ ma trận kí tự phải được sinh để mã hoá và giải mã và cũng dễ nhầm lẫn trong việc giải mã.

*4. Hoán vị các kí tự của văn bản gốc theo chu kì cố định T*

Cho hàm f là hoán vị của một khối gồm T kí tự thì khoá mã hoá được biểu diễn bởi hàm K(T,f). Do vậy, văn bản gốc :

$M = m_1\ m_2\ md\ md_{+1} \ldots m_{2d}$

Trong đó $m_i$ là các kí tự riêng lẻ sẽ được mã hoá thành :

$Ek(M) = mf_{(1)}\ mf_{(2)} \ldots mf_{(d)}\ md_{+f(1)} \ldots md_{+f(d)}$

Với $mf_{(1)}\ mf_{(2)} \ldots mf_{(d)}$ là một hoán vị của $m_1\ m_2 \ldots md$

Ví dụ : giả sử T=7 và f hoán vị dãy i = 12345 thành f(i)=23415, chẳng hạn từ gốc STUDY được biểu diễn như sau :

| *Vị trí đầu* | *Vị trí hoán vị* | *từ* | *Mã hoá* |
|---|---|---|---|
| 1 | 2 | S | T |
| 2 | 3 | T | U |
| 3 | 4 | U | D |
| 4 | 1 | D | S |
| 5 | 5 | Y | Y |

Bằng cách đó văn bản gốc TRUONGDAIHOCKYTHUATDANANG được mã hoá thành RUOTN DAIGH CKYOT UATHD NANAG

### 10.2.2 Phương pháp thay thế

Phương pháp này mã hoá văn bản bằng cách thay thế mỗi kí tự trongvăn bản bằng một kí tự khác nào đó (có thể là chữ cái, chữ số hoặc kí hiệu), có thể dùng một trong các phương pháp thay thế sau :

*1. Thay thế đơn giản*

Mỗi kí tự trong văn bản gốc được thay thế bằng một kí tự tương ứng trong văn bản mật mã. Một ánh xạ 1 – 1 được dùng để mã hoá và giải mã thông điệp.

*2. Thay thế đồng âm*

Mỗi kí tự trong văn bản gốc được mã hoá với một số kí tự của văn bản mật mã (ánh xạ 1 - n). Ngoài ra còn một số phương pháp thay thế khác như thay thế đa mẫu tự, thay thế theo sơ đồ...

Một trong những mật mã thay thế đơn giản được biết đến nhiều nhất là mã Morse, trong đó các chữ cái được thay thế bằng các kí tự gạch và chấm. Bảng mã ASCII ta thường dùng cũng là một dạng mật mã thay thế đơn giản. Trong đó, chữ A

được biểu diễn bằng chuỗi số nhị phân 1000001 hoặc số thập phân 65, chữ B được biểu diễn bởi 1000010 hoặc 66,v.v...

Một dạng mật mã khác cũng được biết đến nhiều đó là bảng chữ cái dịch chuyển. ở đây, các chữ cái trong bảng được dịch chuyển sang phải k vị trí, k gọi là khoá. Ta có hàm dịch chuyển : f(a) = ( a + k ) mod n với a là một chữ cái trong bảng mã, n là số chữ cái (n=26 nếu là bảng chữ tiếng Anh chuẩn).

Ví dụ : với k = 5 ta có :

Bảng chữ gốc : A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Bảng chữ mật mã : F G H I J K LMN O P Q R S T U V W X Y Z A B C D E

Để giải mã, người nhận phải biết khoá k và phục hồi lại văn bản gốc bằng cách biến đổi ngược.

Như vậy nếu văn bản gốc là TRUONG DAI HOC KY THUAT DA NANG thì văn bản mã sẽ là YWZTSL IFN MTH PN YMZFY IF SFSL. Phương pháp này kém an toàn vì chỉ cần thử lần lượt 26 khả năng là ta đã giải mã được.

Một phương pháp thay thế khác tốt hơn là dùng từ khoá theo sơ đồ Vignère. Theo sơ đồ này, từ khoá được cộng vào liên tiếp theo từng kí tự một cho văn bản gốc, mỗi kí tự được biểu diễn bởi một vị trí của nó trong bảng kí tự và phép cộng được thực hiện theo môđun 26. Ví dụ, giả sử ta có bằng :

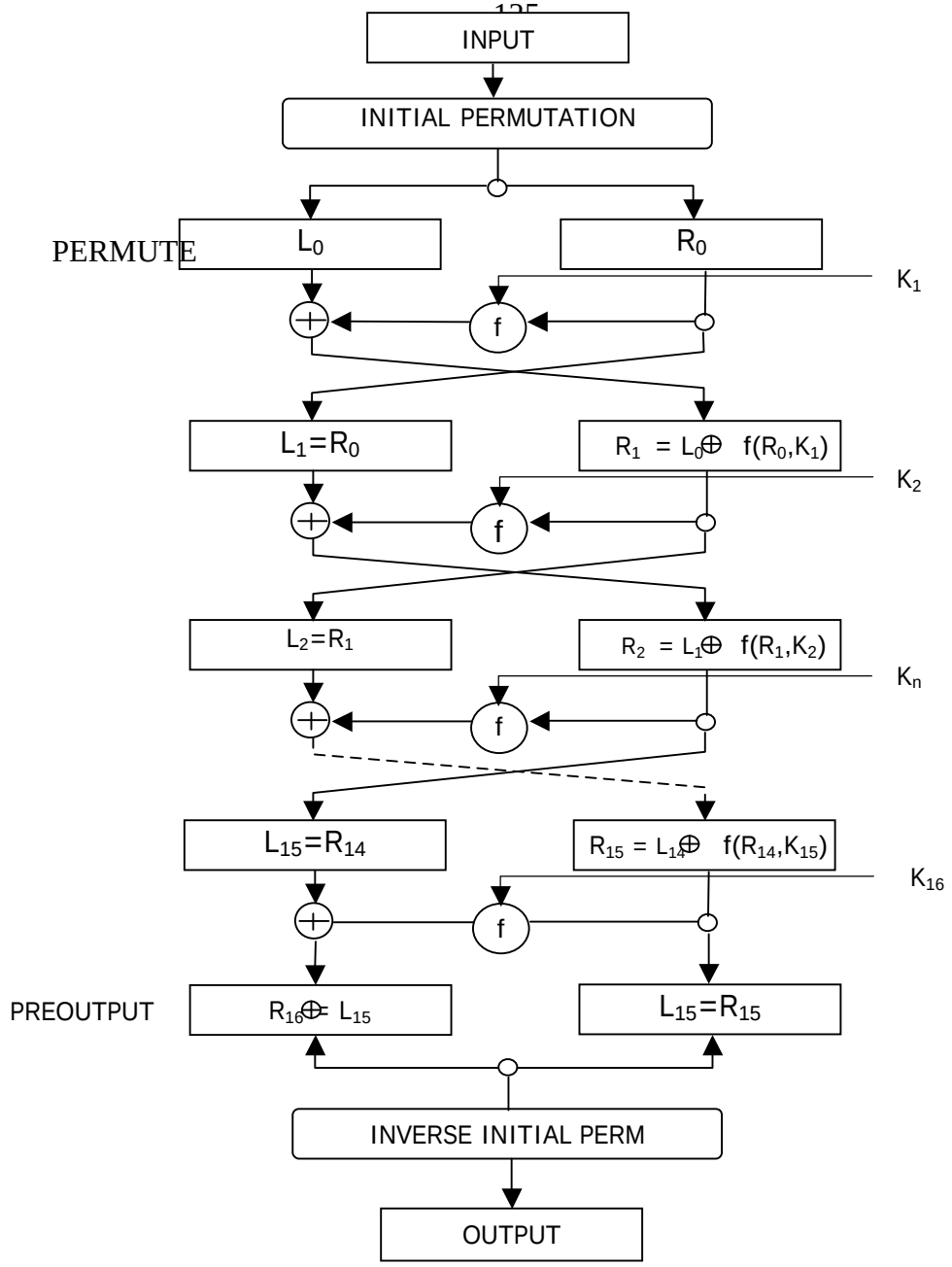
| ***Vị trí*** | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ***Ký tự*** | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S |

| 19 | 20 | 21 | 22 | 23 | 24 | 25 |
|---|---|---|---|---|---|---|
| T | U | V | W | X | Y | Z |

Cho từ khoá là ABCDEF, văn bản DAIHOC được mã hoá thành DBKKSH. Lưu ý rằng ở trên các từ được viết tách ra cho dễ đọc, trên thực tế dữ liệu được truyền thành từng dòng liên tục để sau đó bí mật tính chu kì.

### 10.2.3 Phương pháp mã hóa chuẩn DES

Những thuật toán hiện đại hơn dùng kết hợp cả hai kỹ thuật thay thế và đổi chỗ. Trong đó phương pháp được biết đến nhiều nhất là chuẩn mã hoá dữ liệu DES (Data Encryption Standard) được Mỹ và hãng IBM phát triển trong những năm 70. Lưu đồ mã hoá DES được mô tả như hình sau.

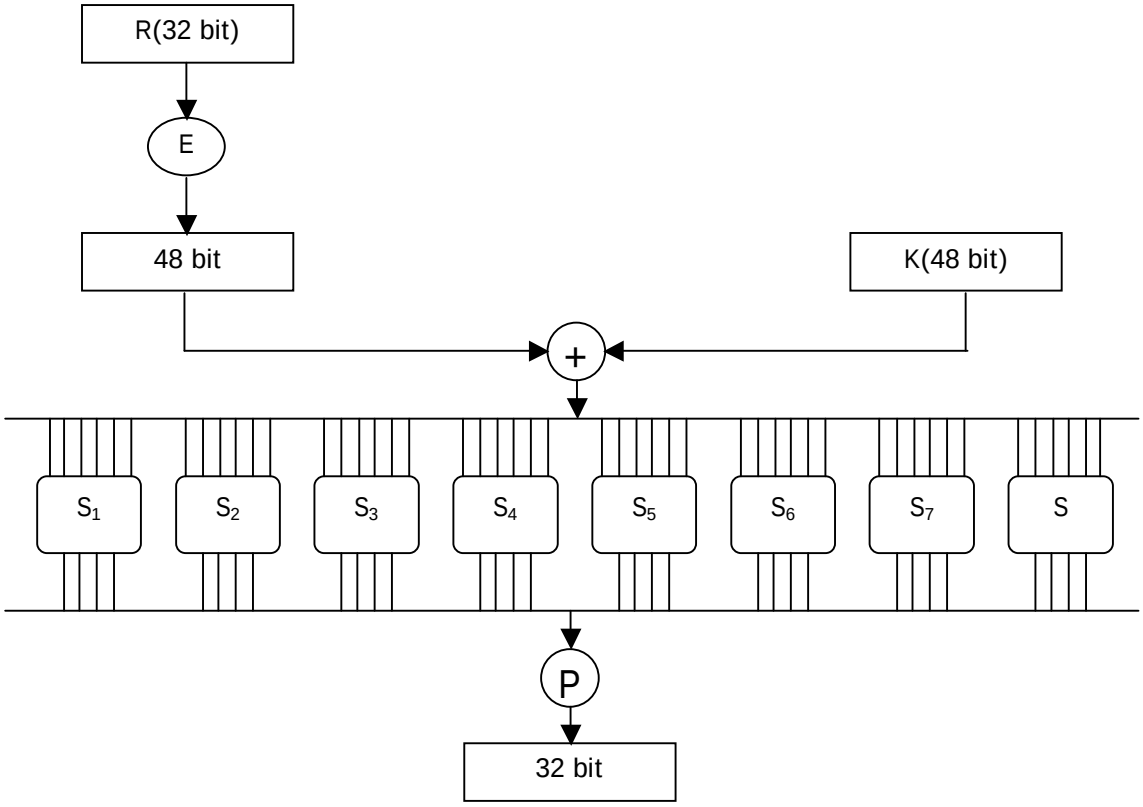



Hình 10-3. Sơ đồ mã hoá DES.

Đầu vào là một dãy 64 bit biểu diễn một khối các kí tự trong văn bản gốc và đầu ra là một dãy 64 bit biểu diễn văn bản mã. Quá trình mã hoá được chia làm 3 giai đoạn :

Đầu tiên văn bản gốc được chuyển qua bộ hoán vị khởi đầu (initial permutation-IP) để tạo ra 64 bit đã hoán vị . Sau đó thực hiện 16 phép lặp của một hàm chữ số (cipher function), kí hiệu là f(R,K) là tổ hợp cả kĩ thuật hoán vị lẫn kĩ thuật thay thế. Trong đó R là dãy con phải (32 bit) của văn bản gốc, khoá K có độ dài 56 bit. 64 bit đầu ra được làm đầu vào cho hoán vị ngược với hoán vị khởi đầu $IP^{-1}$ để tạo ra 64 bit văn bản gốc.

Chi tiết của hàm f(R,K) được mô tả như sau :




Hình 10-4. Hàm f(R,K).

Phép toán của f(R,K) :

Giả sử, bit đầu tiên trong kết quả hoán vị là bit 58 trong dãy ban đầu, bit thứ 2 trong kết quả là bit thứ 50 trong dãy ban đầu,v.v... Dãy hoán vị được chia làm 2 dãy con 32 bit : dãy con trái, kí hiệu là $L_0$ trong sơ đồ, và dãy con phải kí hiệu là $R_0$. Hàm f(R,K) dùng các phép toán thay thế và một khoá $K_1$ để chuyển $R_0$ thành một dãy 32 bit mới, kí hiệu $f(R_0,K_1)$. Dãy bit này được cộng vào $L_0$ từng bit một theo mođun 2(phép toán cộng loại trừ) để tạo ra dãy con phải ở giai đoạn tiếp theo. Dãy $R_0$ ban đầu trở thành dãy con trái $L_1$.

Phép hoán vị ban đầu IP được cho như bảng dưới đây :

| IP | | | | | | | |
|---|---|---|---|---|---|---|---|
| 58 | 50 | 42 | 34 | 26 | 18 | 10 | 2 |
| 60 | 52 | 44 | 36 | 28 | 20 | 12 | 4 |
| 62 | 54 | 46 | 38 | 30 | 22 | 14 | 6 |
| 64 | 56 | 48 | 40 | 32 | 24 | 16 | 8 |
| 57 | 49 | 41 | 33 | 25 | 17 | 9 | 1 |
| 59 | 51 | 43 | 35 | 27 | 19 | 11 | 3 |
| 61 | 53 | 45 | 37 | 29 | 21 | 13 | 5 |
| 63 | 55 | 47 | 39 | 31 | 23 | 15 | 7 |

Chuỗi các phép toán được thực hiện 16 lần với 16 khoá khác nhau $K_1$, $K_2$,..., $K_{16}$, ngoại trừ một điều là không có "phép chuyển qua" ở giai đoạn cuối cùng. Những phép toán này tạo ra dãy 64 bit $R_{16}L_{16}$, được đánh dấu PREOUTPUT trong sơ đồ. Phép toán ngược $IP^{-1}$ của phép hoán vị IP được dùng để biến đổi dãy PREOUTPUT để tạo ra bản mã cuối cùng.

| $IP^{-1}$ | | | | | | | |
|---|---|---|---|---|---|---|---|
| 40 | 8 | 48 | 16 | 56 | 24 | 64 | 32 |
| 39 | 7 | 47 | 15 | 55 | 23 | 63 | 31 |
| 38 | 6 | 46 | 14 | 54 | 22 | 62 | 30 |
| 37 | 5 | 45 | 13 | 53 | 21 | 61 | 29 |
| 36 | 4 | 44 | 12 | 52 | 20 | 60 | 28 |
| 35 | 3 | 43 | 11 | 51 | 19 | 59 | 27 |
| 34 | 2 | 42 | 10 | 50 | 18 | 58 | 26 |
| 33 | 1 | 41 | 9 | 49 | 17 | 57 | 25 |

Dãy con phải được kí hiệu bởi R trước hết được mở rộng thành một dãy số 48 bit dùng bảng chọn bit E sau đây :

| E | | | | | |
|---|---|---|---|---|---|
| 32 | 1 | 2 | 3 | 4 | 5 |
| 4 | 5 | 6 | 7 | 8 | 9 |
| 8 | 9 | 10 | 11 | 12 | 13 |
| 12 | 13 | 14 | 15 | 16 | 17 |
| 16 | 17 | 18 | 19 | 20 | 21 |
| 20 | 21 | 22 | 23 | 24 | 25 |
| 24 | 25 | 26 | 27 | 28 | 29 |
| 28 | 29 | 30 | 31 | 32 | 1 |

Như vậy, khối 6 bit đầu tiên gồm các bit 32,1,2,3,4,5 của R; khối thứ hai gồm các bit 4,5,6,7,8,9, ... Sau đó một phép toán thay thế được áp dụng cho dãy 48 bit này bằng cách cộng nó (theo phép cộng loại trừ) với khoá 48 bit. Một phép thay thế khác được sử dụng cho các khối 6 bit để tạo ra các khối 4 bit để kết quả cuối cùng là dãy 32 bit. Ví dụ bảng thay thế cho $S_1$ là :

| $S_1$ | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Số** hàng | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| 0 | 14 | 5 | 13 | 1 | 2 | 15 | 11 | 8 | 3 | 10 | 6 | 12 | 5 | 9 | 0 | 7 |
| 1 | 0 | 15 | 7 | 4 | 14 | 2 | 13 | 1 | 10 | 6 | 12 | 11 | 9 | 5 | 3 | 8 |
| 2 | 4 | 1 | 14 | 8 | 13 | 6 | 12 | 11 | 15 | 12 | 9 | 7 | 3 | 10 | 5 | 0 |
| 3 | 15 | 12 | 8 | 2 | 14 | 9 | 1 | 7 | 5 | 11 | 3 | 14 | 10 | 0 | 6 | 13 |

Để minh hoạ cách sử dụng, giả sử rằng khối 6 bit đầu tiên là 101000. Số nhị phân 10 tạo bởi bit đầu tiên và bit cuối cùng xác định một hàng trong bảng, cụ thể là hàng 2, 4 bit giữa 0100 xác định cột trong bảng, cụ thể là cột 4. Biểu diễn nhị phân 4 bit 1101 của phần tử 13 ở hàng 2 cột 4 trong bảng là giá trị thay thế cho 6 bit này. các phép toán tương tự $S_2$, $S_3$,..., $S_8$ được dùng để chuyển đổi cho các khối 6 bit khác.

Phép hoán vị cuối cùng P được áp dụng cho dãy 32 bit để tạo ra f(R,K):

| P | | | |
|---|---|---|---|
| 16 | 7 | 20 | 21 |
| 29 | 12 | 28 | 17 |
| 1 | 15 | 23 | 26 |
| 5 | 18 | 31 | 10 |
| 2 | 8 | 24 | 14 |
| 32 | 27 | 3 | 9 |
| 19 | 13 | 30 | 6 |
| 22 | 11 | 4 | 25 |

Mười sáu khoá khác nhau dùng trong DES được lấy ra theo một qui định chặt chẽ từ một khoá 64 bit duy nhất. Như vậy người dùng chỉ cần giữ một khoá để mã hoá và giải mã hơn là giữ 16 khoá khác nhau. Thuật toán giải mã cũng tương tự như khi mã hoá, chỉ khác một diều là 16 khoá được dùng theo thứ tự ngược lại.

Việc giải mã được thực hiện  ngược lại với 64 bit văn bản mã làm đầu vào cho hoán vị ngược với hoán vị khởi đầu $IP^{-1}$ để tạo ra 64 bit văn bản gốc.

Phương pháp DES được Uỷ ban tiêu chuẩn quốc gia (National Bureau of Standards) Hoa Kỳ đề nghị như là một sơ đồ mã hoá “chuẩn “. Tuy nhiên, người ta còn đang tranh luận liệu khoá 48 bit có đủ dài hay chưa và các phép toán thay thế có đủ độ bảo mật cần thiết hay chưa.

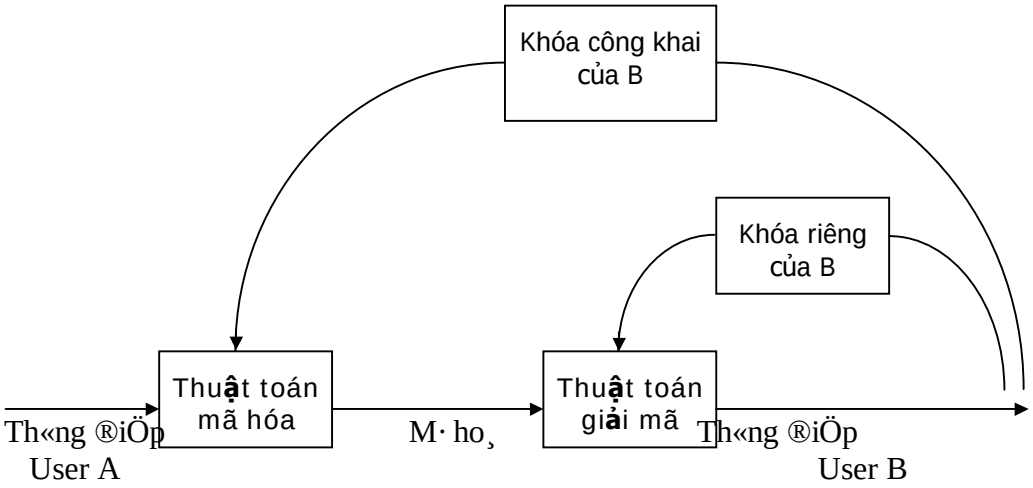
### 10.2.4 Phương pháp mã hoá khoá công khai

#### *10.2.4.1 Nguyên lí mã hóa công khai*

Trong khi thuật toán mã hoá cổ điển dùng một khoá chung cho mã hoá và giải mã thì phương pháp mã hoá bằng khoá công khai sử dụng hai khoá có quan hệ với nhau trong thuật toán để ứng dụng trong mã hoá/giải mã. Các thuật toán này có đặc trưng quan trọng là khó có thể tính toán bằng máy để tìm ra được khoá giải mã nếu chỉ biết được khoá mã hoá và phương pháp mã hoá.

Một số các thuật toán mã hóa công khai (như RSA chẳng hạn) còn có một đặc trưng nữa là khả năng hoán đổi vai trò giữa cặp khoá. Có nghĩa là khi khoá này dùng để mã hoá thì khoá kia dùng để giải mã và ngược lại.

Hình sau mô tả nguyên lí quá trình mã hoá/giải mã bằng khoá công khai :




Hình 10-5. Quá trình mã hoá/giải mã bằng khoá công khai.

Quá trình mã hoá/giải mã như sau:

b. Mỗi hệ thống cuối trong một mạng tạo ra một cặp khoá dùng để mã hoá và giải mã thông tin khi nhận được chúng.

c. Mỗi hệ thống phải có 2 khóa, khóa công khai và khóa bí mật, khoá công khai được công bố lên mạng tại nơi cho phép đăng kí công cộng hoặc đưa vào file. Khoá còn lại phải được giữ bí mật tuyệt đối.

d. Nếu A muốn gửi thông điệp cho B, A sẽ dùng khoá công khai của B trên mạng để mã hoá nó rồi gởi.

e. Khi B nhận được thông điệp của A, B sẽ dùng khoá riêng của mình để giải mã thông điệp nhận được. Không ai có thể giải mã thông điệp được vì chỉ có một mình B biết khoá giải mã.

Thông tin về khoá phải được giữ an toàn tuyệt đối và có thể cập nhật hoặc thay đổi lại khoá cũ. Việc tạo ra các hệ thống bảo vệ và quản lí khoá cũng cần hết sức chặt chẽ.

#### *10.2.4.2 Phương pháp mã hóa RSA*

Bản thuyết trình đầu tiên của Diffe và Hellman đưa ra năm 1976 tại hội nghị MIT và gần như ngay lập tức, sự thách thức về vấn đề mã hoá đã tìm được câu trả lời bởi hệ thống mã hoá công khai. Một trong những câu trả lời đầu tiên đưa ra vào năm 1977 bởi Ron Rivest, Adi Shamir và Len Adltôian được công bố vào năm 1978

(gọi tắt là rsa). ý tưởng RSA trở thành gần như độc tôn và được sử dụng rộng rãi trong phương pháp mã hoá bằng khoá công khai.

Giả sử ta có :

Văn bản gốc : $M = M_1 M_2 ... Mk$

Văn bản mã hóa : $C = C_1 C_2 ... Ck$ , trong đó $Ci = M_i^E \bmod n$, n là tích 2 số nguyên tố bất kì p và q.

Thuật toán RSA dùng thuyết số để phát triển phương pháp phát sinh một cặp các số nguyên tố - các khoá, thuật toán dựa trên nhận xét: *Có thể dễ dàng sinh ra 2 số nguyên tố lớn và khi nhân chúng với nhau thì rất khó khi muốn phân tích tích của chúng thành thừa số và khó có thể tìm được số còn lại từ số kia*.

Theo một hệ quả của định lí Euler đưa ra: *Cho 2 số nguyên tố p và q và hai số nguyên n và m để n=p.q và 0<m<n, tồn tại một số nguyên duy nhất k sao cho:*

$$(mk^{\phi(n)+1} = mk^{(p-1)(q-1)+1}) \bmod m = n$$

trong đó $\phi(n)$ là hàm Euler với giá trị số nhỏ hơn n và có quan hệ nguyên tố với n, $\phi(n)=(p-1)(q-1)$.

Do đó ta có thể đạt được kết quả mong muốn nếu: $ED = k\phi(n) + 1$

Điều này tương đương với: $ED \bmod \phi(n) = 1$.

Thuật toán RSA được mô tả như sau:

1. Chọn 2 số nguyên tố p, q.
2. Tính tích n = p*q
3. Tính $\phi(n) = (p-1)(q-1)$
4. Chọn E thỏa $USCLN(\phi(n), E) = 1$ ; *với* $1 < E < \phi(n)$
5. Tìm D thỏa $DE \bmod \phi(n) = 1$.

Khoá công khai là KE = {E,n}, khoá riêng là KD = {D,n} hoặc ngược lại.

Giả sử rằng user A công bố khoá công khai KE lên mạng và user B muốn gửi thông điệp cho user A :

- B sẽ dùng khóa công khai của user A để mã hoá thông điệp của mình bằng công thức $C = ME \bmod n$, rồi gởi nó đi.
- User A sẽ nhận được thông điệp đã mã hoá và giải mã nó bằng khoá riêng của mình bằng công thức $M = CD \bmod n$

Ví dụ: Chọn p =7, q =17

Tính n = p*q = 7*17 = 119

$\phi(n) = (p-1)*(q-1) = 96$

Chọn E thỏa : USCLN(E, 96) = 1. Ta chọn E = 5.

Tìm D thỏa : D*E mod 96 = 1 và D < 96 , suy ra D =77.

Ta được KE = {5,119} , KD = {77,119}.

Giả sử M = 19. Quá trình mã hoá: $C = 19^5 \bmod 119 = 66$.

Quá trình giải mã: $M = 66^{77} \bmod 119 = 19$.

#### *10.2.4.3 Các vấn đề nảy sinh trong thuật toán*

1. Vấn đề phức tạp trong tính toán.

Trong quá trình mã hoá và giải mã, thuật toán RSA phát sinh ra các số nguyên rất lớn, cho dù có phép chia modulo n. Rivest, Shamir và Adltôian đề nghị rằng các số p và q phải có độ dài trên 100 chữ số để đảm bảo an toàn gần như tuyệt đối. Như vậy sự luỹ thừa quá lớn và sau đó cho dù có chia modulo n thì kết quả trung gian cũng sẽ khổng lồ và rất dễ dẫn đến tràn số. Ta có thể ứng dụng tính chất của phép chia modulo sau:

((a mod n) * (b mod n)) mod n = (a * b) mod n

Do đó, chúng ta có thể làm giảm kết quả trung gian trong phép chia này đi. Điều này làm cho các phép toán trở nên khả thi hơn.

2. Vấn đề bẻ khoá

Với thuật toán thay thế và hoán vị, về mặt lí thuyết khi độ dài của khoá càng lớn thì mức độ an toàn càng cao, nhưng những người giải mã giàu kinh nghiệm vẫn có thể phân tích tần số xuất hiện của một số kí tự xác định hay tổ hợp của chúng để từ đó suy ra khoá và thực hiện giải mã. Trong thuật toán RSA khoá KE(E,n) là khoá công khai nên ta không cần giữ bí mật, ta chỉ giữ bí mật cho khoá riêng KD(D,n). Vì vậy, để bẻ khóa phải xác định được D từ các giá trị E và n. Theo như cách chọn các số E và D, điều này có thể làm được nếu có thể phân tích n thành tích của hai số nguyên tố. Như vậy tính an toàn của thuật toán RSA phụ thuộc vào sự khó khăn của việc xác định các thừa số nguyên tố của một số nguyên tố lớn. Hiện nay nếu sử dụng thuật toán phân tích thừa số nhanh nhất của Schroeppel thì cũng cần đến : $S = \exp[(\ln n)\ln(\ln n)]^{1/2}$ bước tính toán để phân tích n thành p và q.

Bảng dưới đây hiển thị các thời gian dự đoán của các nhà phân tích, giả sử rằng mỗi phép toán được thực hiện trong 1 micro giây :

| Độ dài của khóa | Thời gian |
|---|---|
| 50 | 4 giờ |

| | |
|---|---|
| 75 | 104 ngày |
| 100 | 74 năm |
| 200 | 4.000.000 năm |
| 300 | $5 \times 10^{15}$ năm |
| 500 | $4 \times 10^{25}$ năm |

Phương pháp mã hoá với khoá công khai xem như được bảo đảm vì hiện nay vẫn chưa tìm ra một thuật toán phân tích thừa số nguyên tố có hiệu quả.

#### *10.2.4.4 ứng dụng của mã hoá dữ liệu*

Mã hoá dữ liệu có các ưu điểm là an toàn vì ít phụ thuộc vào cấu trúc hệ thống mạng. Ngoài ra mã hoá dữ liệu có tính bảo mật do dữ liệu được mã hoá rồi thì chỉ có những người có quyền mới có thể giải mã để nhận lại được dữ liệu ban đầu. Các phương pháp mã hoá trên có thể áp dụng trong những tình huống sau :

- Phương pháp mã hoá thay thế kết hợp với phương pháp mã hoá hoán vị dùng tạo ra phương pháp mã hoá DES.
- Các dịch vụ e-mail trên mạng Internet hay các mạng cục bộ có thể sử dụng thuật toán RSA để tạo ra một mặt nạ nhận dạng (authentication mask) các thông điệp giữa các cá nhân với nhau. Có nghĩa là chỉ những người nhận được thư gởi cho mình bằng khoá mã hoá của mình thì mới giải mã được thông điệp đó và hoàn toàn không thể (nói theo nguyên tắc) đọc được các thư không phải gởi cho mình.
- Kỹ thuật mã hoá chữ kí số (digital signature) có thể dùng để tạo ra một chữ kí mã hoá dùng để xác định, nhận dạng một đối tượng trong các dịch vụ thương mại, ví dụ như các thẻ tín dụng hoặc các loại visa, cardphone chẳng hạn....
- Thư điện tử e-mail cũng có thể kết hợp thuật toán này với các thuật toán mã hoá khác như DES theo mô hình có thể là:

- Nội dung thư được mã hoá bằng phương pháp DES
- Tạo một chữ ký số và mã hoá bằng khoá RSA
- Khoá DES dùng để giải mã có thể được mã hoá bằng RSA và gửi kèm trong thư luôn mà không cần phải bí mật. Người nhận sẽ dùng khóa riêng của mình để giải mã khoá DES, sau đó giải mã thư nhận được.

## 10.3 Cơ chế bảo vệ bằng firewall

Vấn đề quan trọng trong việc quản lý các tài nguyên thông tin là cơ chế bảo vệ chống việc truy cập bất hợp pháp trong khi vẫn cho phép người được ủy nhiệm sử dụng những nguồn thông tin mà họ được cấp quyền, và phương pháp chống thất

thoát thông tin được truyền tải trên các mạng truyền dữ liệu công cộng (Public Data Communication Network). Đó chính là yêu cầu của một giải pháp hoặc hệ thống an ninh cho hệ thống mạng hay còn gọi là hệ thống an ninh dữ liệu (Data Security System).

Nhu cầu an ninh hệ thống ngày càng trở nên quan trọng vì nhiều nguyên nhân như các đối thủ luôn tìm cách để nắm được mọi thông tin liên quan, ngày càng nhiều hacker truy cập thông tin từ các mạng nội bộ theo nhiều mục đích khác nhau.

Một giải pháp an ninh cho hệ thống mạng được ứng dụng nhiều đó là bức tường lửa (firewall). Thuật ngữ firewall có nguồn gốc từ một kỹ thuật thiết kế trong xây dựng để ngăn chặn, hạn chế hỏa hoạn. Trong công nghệ mạng thông tin, firewall là một kỹ thuật được tích hợp vào hệ thống mạng để chống lại việc truy cập trái phép nhằm bảo vệ các nguồn thông tin nội bộ cũng như hạn chế sự xâm nhập vào hệ thống của một số thông tin khác không mong muốn.

***Về mặt chức năng hệ thống***, firewall là một thành phần được đặt giữa hai mạng để kiểm soát tất cả các việc lưu thông và truy cập giữa chúng với nhau, bao gồm:

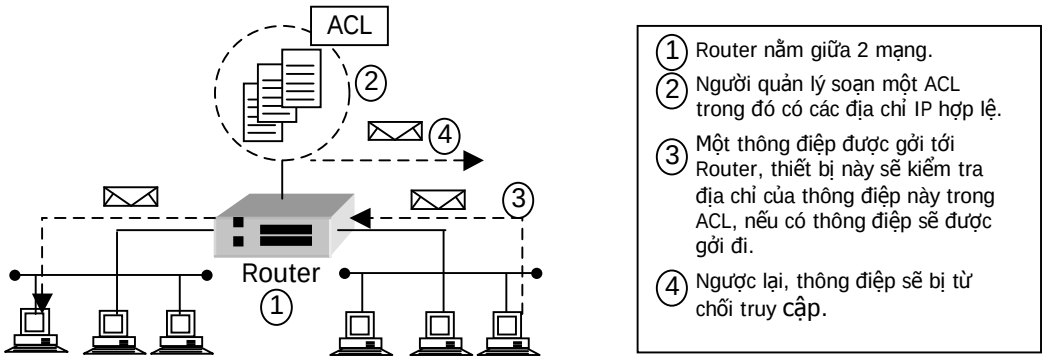
1. Tất cả các trao đổi dữ liệu từ trong ra ngoài và ngược lại phải thực hiện thông qua firewall.
2. Chỉ có những trao đổi nào được phép bởi chế độ an ninh của hệ thống mạng nội bộ (trusted network) mới được quyền lưu thông qua firewall.

***Về mặt vật lý***, firewall bao gồm:

1. Một hoặc nhiều hệ thống máy chủ kết nối với các bộ định tuyến (router) hoặc có chức năng router.
2. Các phần mềm quản lý an ninh chạy trên các hệ thống máy chủ. Thông thường là các hệ quản trị xác thực (Authentication), cấp quyền (Authorization) và kế toán (Accounting).

Firewall bao gồm phần cứng và/hoặc phần mềm nằm giữa 2 mạng (như mạng nội bộ và mạng Internet), bảo vệ mạng nội bộ bằng cách cấm các người sử dụng truy cập trái phép đến và đồng thời ngăn chặn những thông điệp không được phép gửi đi cho người nhận bên ngoài mạng. Firewall có thể nằm trên bộ dẫn đường hay trên Server. Cơ chế làm việc của Firewall dựa trên việc kiểm tra các gói dữ liệu IP lưu chuyển giữa hai mạng tùy thuộc vào các qui tắc mà người quản trị hệ thống đã xác lập.

Khái quát phương thức làm việc của Firewall như trong hình vẽ sau:




Hình 10-6. Cơ chế hoạt động của Firewall.

### 10.3.1 Các loại firewall và cơ chế hoạt động

Khi nói đến việc lưu thông dữ liệu giữa các mạng với nhau thông qua firewall thì điều đó có nghĩa rằng firewall hoạt động kết hợp chặt chẽ với giao thức TCP/IP. Vì giao thức này làm việc theo thuật toán chia nhỏ các dữ liệu nhận được từ các ứng dụng trên mạng, hay chính xác hơn là các dịch vụ chạy trên các giao thức (Telnet, SMTP, DSN, SMNP, NFS,...) thành các gói dữ liệu rồi gán cho các gói này những địa chỉ để có thể nhận dạng tái lập lại ở đích cần gửi đến. Do đó các loại firewall cũng liên quan rất nhiều đến các packet và các địa chỉ của chúng.

#### *10.3.1.1 Bộ lọc packet (Packet filtering)*

Loại firewall này thực hiện việc kiểm tra số nhận dạng địa chỉ của các packet để cho phép chúng có thể lưu thông qua lại hay không. Các thông số có thể lọc được của một packet như sau:

1. Địa chỉ IP nơi xuất phát (source IP address).
2. Địa chỉ IP nơi nhận (destination IP address).
3. Cổng TCP nơi xuất phát (TCP source port).
4. Cổng TCP nơi nhận (TCP destination port).

Nhờ đó firewall có thể ngăn cản được các kết nối vào những máy chủ hoặc mạng nào đó được xác định, hoặc khóa việc truy cập vào hệ thống nội bộ từ những địa chỉ không cho phép.

Hơn nữa việc kiểm soát các cổng làm cho firewall có khả năng chỉ cho phép một số loại kết nối nhất định vào máy chủ nào đó, hoặc chỉ có những dịch vụ nào đó (Telnet, SMTP, FTP,...) được phép mới chạy được trên hệ thống mạng nội bộ.

#### *10.3.1.2 Cổng ứng dụng (Application gateway)*

Đây là một loại firewall được thiết kế để tăng cường chức năng kiểm soát các loại dịch vụ, giao thức được cho phép truy cập vào hệ thống mạng. Cơ chế hoạt

động của nó dựa trên cách thức gọi là Proxy Service (dịch vụ đại diện): một ứng dụng nào đó được quy chiếu đến (hay đại diện bởi) một Proxy Service trong khi các Proxy Service chạy trên các hệ thống máy chủ thì được quy chiếu đến application gateway của firewall. Cơ chế lọc của packet filtering phối hợp kiểm soát với cơ chế "đại diện" của application gateway cung cấp một khả năng an toàn và uyển chuyển hơn.

Ví dụ một hệ thống mạng có chức năng lọc các gói tin ngăn các kết nối bằng Telnet vào hệ thống chỉ trừ một chủ duy nhất -Telnet application gateway là được phép. Một người sử dụng dịch vụ Telnet muốn kết nối vào hệ thống phải thực hiện các bước sau :

1. Thực hiện dịch vụ TELNET đến Telnet application gateway rồi cho biết tên của máy chủ bên trong cần truy cập.
2. Gateway kiểm tra địa chỉ IP nơi xuất phát của người truy cập rồi cho phép hoặc từ chối tùy theo chế độ an ninh của hệ thống.
3. Người truy cập phải vượt qua được hệ thống kiểm tra xác thực.
4. Proxy Service tạo một kết nối Telnet giữa gateway và máy chủ cần truy cập.
5. Proxy Service liên kết lưu thông giữa người truy cập và máy chủ.

Cơ chế hoạt động này có ý nghĩa quan trọng trong việc thiết kế an ninh hệ thống ví dụ như:

1. Che giấu các thông tin: người dùng chỉ có thể nhìn thấy trực tiếp các gateway được phép.
2. Tăng cường kiểm tra truy cập bằng các dịch vụ xác thực (Authentication).
3. Giảm đáng kể giá thành cho việc phát triển các hệ quản trị xác thực vì các hệ thống này được thiết kế chỉ quy chiếu đến application gateway.
4. Giảm thiểu các quy tắc kiểm soát của bộ lọc (Packet filtering). Điều này làm tăng tốc độ hoạt động của firewall.

#### *10.3.1.3 Bộ lọc session thông minh (Smart session filtering)*

Cơ chế hoạt động phối hợp giữa bộ lọc packet và cổng ứng dụng như trên cung cấp một chế độ an ninh cao tuy nhiên nó cũng bị vài hạn chế. Vấn đề chính hiện nay là làm sao để cung cấp đủ Proxy Service cho rất nhiều ứng dụng khác nhau đang phát triển ồ ạt. Điều này có nghĩa là nguy cơ, áp lực đối với việc đánh lừa firewall gia tăng lên rất lớn nếu các proxy không kịp đáp ứng.

Trong khi giám sát các packet ở những mức phía trên, nếu như lớp network đòi hỏi nhiều công sức hơn đối với việc lọc các packet đơn giản, thì việc giám sát

các giao dịch lưu thông ở mức mạng (Session) đòi hỏi ít công việc hơn. Cách này cũng loại bỏ được các dịch vụ đặc thù cho từng loại ứng dụng khác nhau.

Nếu kết hợp khả năng ghi nhận thông tin về các session và sử dụng nó để tạo các quy tắc cho bộ lọc thì sẽ có được một bộ lọc thông minh hơn. Đó chính là cơ chế hoạt động của bộ lọc session thông minh.

Vì một session ở mức network được tạo bởi 2 packet lưu thông theo 2 chiều, cho nên nếu thiết kế 2 quy tắc lọc cho 2 chiều này: một để kiểm soát các packet lưu thông từ host phát sinh ra nó đến máy chủ cần tới, một để kiểm soát packet trở về từ máy chủ phát sinh. Một bộ lọc thông minh sẽ nhận biết được rằng packet trở về theo chiều ngược lại nên quy tắc thứ 2 là không cần thiết. Do vậy, cách để tiếp nhận các packet không mong muốn sinh ra từ bên ngoài firewall sẽ khác biệt rất rõ với cách tiếp cận cho các packet do những kết nối được phép (ra bên ngoài). Và như vậy dễ dàng nhận dạng các packet "bất hợp pháp".

#### *10.3.1.4 Firewall hỗn hợp (Hybrid firewall)*

Trong thực tế các firewall được sử dụng là sự kết hợp của nhiều kỹ thuật để tạo ra hiệu quả an ninh tối đa. Ví dụ việc để lọt lưới tại các kiểm soát của bộ lọc packet có thể được thực hiện tại bộ lọc session thông minh ở mức ứng dụng. Các giám sát của bộ lọc lại được bọc lót chặt chẽ bởi các dịch vụ proxy của application gateway.

#### *10.3.1.5 Một vài ứng dụng của Firewall*

Từ các chế độ hoạt động trên, firewall được ứng dụng nhiều vào hệ thống an ninh dữ liệu. Có 3 yêu cầu chính cho vấn đề an ninh hệ thống theo tiêu chuẩn ISO cho mô hình mạng OSI :

- Quản lý xác thực (Authentication)
- Quản lý cấp quyền (Authorization)
- Quản lý kế toán (Accounting management)
-

***f. Ưu điểm của Firewall***

Firewall là điểm kiểm tra các kết nối giữa mạng nội bộ và mạng Internet bên ngoài, mọi kết nối đều phải đi qua cửa khẩu này. Đây chính là một bộ lọc an toàn bởi vì có rất nhiều dịch vụ đang hoạt động trên Internet, nếu chúng ta không có một cơ chế kiểm soát chặt chẽ thì các dịch vụ này sẽ tự do mang thông tin tràn vào mạng của chúng ta và ngược lại.

Firewall có thể được sử dụng để ghi nhận lại các hoạt động kết nối với Internet. Bởi vì, mọi hoạt động như vậy đều phải thông qua Firewall nên nó có thể cung cấp thêm chức năng thu thập mọi thông tin về các kết nối xảy ra giữa mạng nội bộ và mạng Internet bên ngoài.

Ta cũng có thể sử dụng Firewall để bảo vệ một máy đơn của người sử dụng.

***g. Hạn chế của Firewall***

Bên cạnh những mặt tích cực của Firewall kể trên, nó còn có những hạn chế và những việc mà nó không thể thực hiện được như sau:

1. Bên cạnh việc ngăn chặn các người dùng trong mạng nội bộ kết nối ra ngoài khi không được phép thì nó cũng ngăn cản các việc làm tốt của họ.
2. Firewall không thể chống lại các mối nguy hiểm mới, bởi vì chúng nằm ngoài sự kiểm soát của Firewall.
3. Do không kiểm tra trên nội dung của các gói tin, nên Firewall không sử dụng để ngăn ngừa các thông tin xấu trên một dịch vụ đã được cho phép và cũng không thể nhận biết các đoạm mã virus trong các tập tin truyền đi.

## 10.4 Hệ thống tên miền DNS (Domain Name System )

Địa chỉ Internet 32 bit thỏa mãn yêu cầu kỹ thuật, nhưng phức tạp và khó nhớ đối với người dùng. Giải pháp đưa ra ở đây là dùng những tên gợi nhớ thay cho địa chỉ số là tự nhiên và dễ nhớ đối với người sử dụng. Hơn nữa, dùng tên tin cậy hơn địa chỉ số vì địa chỉ số có thể thay đổi những tên luôn luôn dùng lại được. Do đó nảy sinh vấn đề cách đặt tên và ánh xạ địa chỉ IP với tên.

Trước đây trung tâm thông tin Internet NIC chịu trách nhiệm cấp phát và quản lý tên. Người ta dùng một file có tên host.txt trên Windows hoặc /etc/hosts trên Unix, tập tin này chứa tên của tất cả các mạng, router, host và địa chỉ IP tương ứng với chúng. Các tên được cấp phát không có mối liên hệ gì với nhau. Khi Internet phát triển, giải pháp này trở nên phức tạp không chấp nhận được về mặt quản lý.

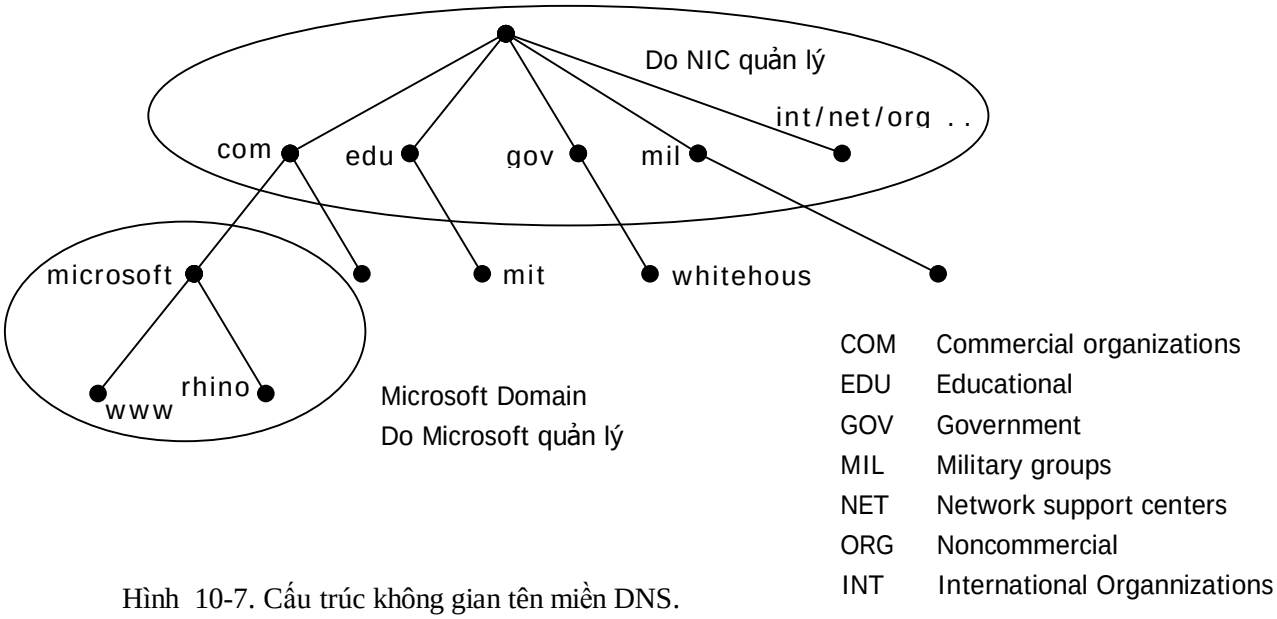
Theo Paul Mockepetris, người thiết kế chính DNS, mục tiêu thiết kế bắt đầu của DNS là để thay thế các tập tin host phức tạp bằng một cơ sở dữ liệu phân tán nhẹ hơn có khả năng cung cấp một *không gian tên thứ bậc, sự quản lý phân tán, có bộ đệm cục bộ (caching), các kiểu dữ liệu mở rộng, kích thước cơ sở dữ liệu không giới hạn và có hiệu năng.*

DNS tương ứng với tầng 7 của mô hình OSI và dùng giao thức UDP hay TCP ở tầng dưới. Việc truy cập DNS thực hiện theo mô hình Client/Server. Hầu hết các hệ thống kết nối Internet đều hỗ trợ DNS. Các đặc tả chính của DNS được định

nghĩa trong các tài liệu RFC 974, 1034, 1035. Dịch vụ cài đặt giao thức DNS phổ biến nhất là BIND (Berkeley Internet Name Domain), được phát triển đầu tiên tại Berkeyley cho hệ điều hành Unix.

DNS gồm 3 thành phần : ***Namespace, các NameServer và Resolver.***

### 10.4.1 Không gian tên miền DNS




Hình 10-7. Cấu trúc không gian tên miền DNS.

DNS tổ chức không gian tên miền theo cấu trúc cây, trên cùng là gốc, rồi đến các nút cha, nút con... và cuối cùng là các nút lá.

Một máy tính trong mạng sẽ ứng với một nút của cây. Như ở cây trên, máy ở lá www sẽ có địa chỉ hoàn chỉnh là www.microsoft.com. Mỗi nút trên cây biểu diễn một miền (domain) trong hệ thống DNS; mỗi miền lại có một hay nhiều miền con. Tại mỗi miền này đều phải có máy chủ DNS tương ứng quản lý hệ thống tên trong miền đó.

*Nút trên cây :* Mỗi nút có một tên tương ứng dài từ - đến 63 ký tự dưới 128 trong bảng mã ASCII. Các nút kề nhau không được có cùng tên. Mỗi nút có một tập (có thể rỗng) các *bản ghi tài nguyên* (Resource Record - RR) chứa thông tin đi kèm nút đó. Nhãn rỗng dành riêng cho nút gốc, ký hiệu bằng dấu chấm (.).

*Miền con :* Được tạo thành từ mỗi nút của không gian tên và các nút bên dưới có thể đi đến được các nút đó.

*Vùng :* là một phần cây con của cây DNS được quản lý như một thực thể riêng. Vùng có thể bao gồm một miền hay một miền với một số miền con. Các miền con mức thấp hơn của một vùng lại có thể chia thành các vùng rời nhau.

*Tên miền của một nút* : là dãy các nhãn từ một nút trên cây đến gốc của cây. Các nhãn trong tên miền cách nhau bằng dấu chấm (.). *Tên miền tuyệt đối* kết thúc bằng dấu chấm. Ví dụ "poneria.ISI.EDU.". *Tên miền tương đối* không kết thúc bằng dấu chấm và sẽ được phần mềm cục bộ ghép đầy đủ khi xử lý. Để đơn giản việc cài đặt, độ dài tên miền được giới hạn dưới 255. Một miền là miền con của miền khác nếu tên miền đó chứa tên miền kia. Ví dụ A.B.C.D là miền con của các miền con của các miền B.C.D, C.D, D và miền gốc.

*Tên miền đầy đủ* là tên các nút từ gốc đến lá của cây nối với nhau và phân cách bằng dấu chấm. Ví dụ : mrp2.widgets.mfg.universal.co.uk

*Các miền mức đỉnh* : Miền gốc và các miền mức đỉnh của cây DNS do NIC quản lý. Các tên miền mức đỉnh có thể chia ba loại :

- Các miền tổ chức (tên 3 ký tự) : com, edu, gov, . . .
- Các miền địa lý (các mã quốc gia, 2 ký tự) : uk, vn, ca, fr, . . .
- Miền in-addr-arpa : miền đặc biệt dùng để ánh xạ địa chỉ thành tên.

Trách nhiệm quản lý không gian tên DNS dưới mức đỉnh được NIC ủy nhiệm cho các tổ chức khác. Các tổ chức này lại chia không gian tên phía dưới và uỷ nhiệm xuống. Mô hình quản lý phân tán này cho phép DNS được quản lý tự trị bởi các tổ chức tham gia. Cách đặt tên như vậy có tác dụng phân cấp quản lý vùng tên. Các tổ chức có thể tự tạo và quản lý không gian tên riêng của mình trong mạng, không phụ thuộc vào sự cho phép của NIC.

Vấn đề tên và vùng còn được nhiều hãng lớn bổ sung và làm phong phú thêm bằng những giải pháp của riêng họ. Ví dụ Microsoft có WINS - Windows Internet Naming Service, IBM có DDNS - Dynamic Domain Name System.

#### *10.4.1.1 Cú pháp tên miền*

Cú pháp cho tên miền sau đây cho phép phù hợp với nhiều ứng dụng như mail, telnet, . . .

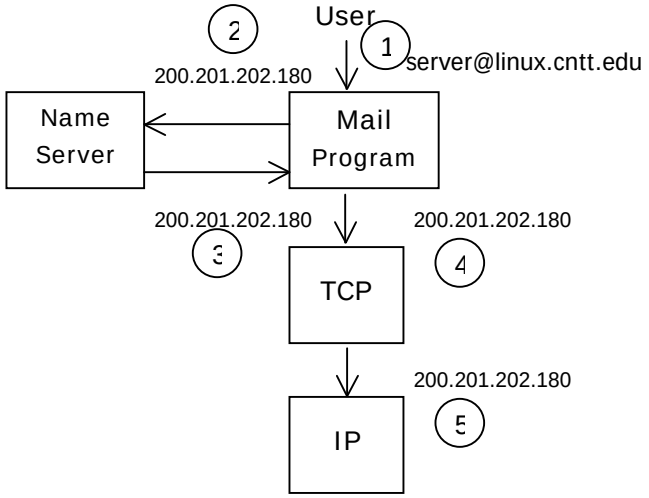
<domain>::=<subdomain>| " "
<subdomain>::=<label>|<subdomain> "." <label>
<label>::=<letter>[[<ldh-str>]<let-dig>]
<ldh-str>::=<let-dig-hyp>|<let-hyp><ldh-str>
<let-dig-hyp>::=<let-dig>| "-"
<let-dig>::=<letter>|<digit>
<letter>::= ký tự từ A-Z, a-z
<digit>::= chữ số 0-9

### 10.4.2 Máy chủ quản lý tên

Máy chủ quản lý tên (Name Server) là hệ thống chương trình quản lý cấu trúc cây của miền và các tập thông tin đi kèm. Máy chủ tên có thông tin đầy đủ về một số tập con gọi là vùng của không gian tên và các con trỏ đến các nameserver khác để lấy tin về một miền bất kỳ của cây miền. Các máy chủ tên có thông tin đầy đủ về một số phần của cây miền được gọi là có thẩm quyền (authoritative) về các phần đó. Một *vùng* (zone) là một đơn vị thông tin có thẩm quyền của cơ sở dữ liệu DNS. Trong thực tế, các máy chủ tên thường lưu tạm thời trong bộ đệm cấu trúc và thông tin các vùng và thông tin về các vùng khác để tăng hiệu năng. Các máy chủ quản lý tên trong vùng trao đổi thông tin với nhau bằng Zone Transfer Protocol.

### 10.4.3 Chương trình phân giải tên

Chương trình phân giải tên (Resolver) là các thường trình hệ thống lấy thông tin từ namserver để trả lời yêu cầu của những ứng dụng khách (client). Resolver phải có khả năng truy cập đến ít nhất một nameserver và dùng thông tin từ nameserver đó để trực tiếp trả lời câu hỏi hay để hỏi tiếp đến các nameserver khác. Chương trình người sử dụng có thể truy cập trực tiếp đến resolver, do đó không cần có một giao thức giữa resolver và chương trình người dïng.




Hình 10-8. Quá trình phân giải tên trong thực tế .

## 10.5 Hệ quản trị mạng

Hệ thống quản trị mạng (Network Management) còn gọi là mô hình Manager/Agent bao gồm các thành phần như sau :

- Hệ quản trị - Manager
- Hệ bị quản trị - Managed system
- Một cơ sở dữ liệu chứa thông tin quản trị và giao thức quản trị mạng.
- Hệ quản trị - Manager

Thực hiện cung cấp giao diện giữa người quản trị mạng và các thiết bị mạng được quản trị, bao gồm các thông tin thể hiện dưới dạng đồ họa, đồ thị, số liệu thống kê, báo cáo. Ví dụ như hiển thị dạng đồ họa bản đồ về topology liên mạng thể hiện các vị trí của các LAN segments, từ đó có thể chọn xem trạng thái hoạt động hiện hành của nó.

### 10.5.1 Hệ bị quản trị

- Bao gồm tiến trình Agent và các đối thượng quản trị (manager objects).
- Tiến trình Agent thực hiện các thao tác quản trị mạng như đặt các tham số cấu hình và các thống kê hoạt động hiện hành của các router trên một segments cho trước.
- Các đối tượng quản trị bao gồm các trạm làm việc, máy server, hub, kênh truyền.

### 10.5.2 Cơ sở dữ liệu chứa thông tin quản trị mạng

Được gọi là *cơ sở thông tin quản trị* (Management Information Base - MIB) được lưu trữ tại Server và Client. MIB được tổ chức thành một cấu trúc cây, gọi là SMI (Structure of Management Information). SMI bắt đầu từ gốc root, tiếp theo là các nhánh chứa các đối tượng quản trị được phân loại lôgic.

Kiến trúc quản trị mạng ISO như sau :

1. Quản trị sự cố (Fault Management) : phát hiện, cô lập và khắc phục sự cố.
2. Quản trị kế toán (Accounting Management) : kiểm soát va 2đánh giá việc sử dụng tài nguyên trong mạng
3. Quản trị cấu hình (Configuration Management)
4. Quản trị hiệu năng (Performance Management)
5. Quản trị an toàn (Security Management)

Simple Network Management Protocol (SNMP) được tạo ra ban đầu với mục đích cung cấp phương tiện để điều khiển các router trên mạng. SNMP, mặc dù là một phần trong gia đình giao thức TCP/IP, không phụ thuộc vào IP. SMNP được thiết kế độc lập với giao thức truyền, tuy nhiên phần lớn các hãng đều sản xuất SNMP chạy trên IP.

SNMP thực chất là gồm 3 giao thức cấu tạo thành, tất cả đều được thiết kế để làm việc với mục đích điều hành:

- Management Information Base (MIB): Một cơ sở dữ liệu chứa các thông tin trạng thái.

- Structure and Identification of Management Information (SMI): Một tiêu chuẩn định nghĩa các đầu mục của một MIB.
- Simple Network Management Protocol (SNMP): Phương thức trao đổi thông tin giữa các thiết bị và Server.

## 10.6 Dịch vụ thư điện tử

Electronic Mail (viết gọn là e-Mail, thư điện tử) là một trong những dịch vụ thông tin phổ biến nhất trên Internet. Dịch vụ e-Mail giúp mọi người có thể trao đổi thông tin với nhau trên mạng Internet. Liên lạc bằng thư điện tử nhanh hơn, thuận tiện hơn và chi phí thấp hơn rất nhiều so với trao đổi thư từ qua đường bưu điện bình thường. Ngoài ra còn cho phép họ gửi cho nhau cả các loại tài liệu như: các văn bản, các báo cáo, các chương trình máy tính, . .. và nhiều thông tin khác nữa.

Mỗi người sử dụng đều có một thư mục lưu trữ thư trên máy Server gọi là Mailbox. Tất cả các địa chỉ mail bao gồm hai phần được ngăn cách nhau bằng 1 ký tự @ (ampersand). Ví dụ : . Tên miền có thể được chia nhiều phần cách nhau bởi dấu chấm (.). Một địa chỉ mail tiêu biểu có các thành phần như sau :

*Username @ ServerName. Type of Organization . Country*

Cấu trúc của một E-Mail bao gồm các phần như sau :

- ***Phần tiêu đề thư***

Phần này do các MTA (Message Transfer Agent) tạo ra và sử dụng, nó chứa các thông tin để chuyển nhận e-Mail như địa chỉ của nơi nhận, địa chỉ của nơi gửi. Các hệ thống e-Mail cần những thông tin này để chuyển dữ liệu từ máy tính này sang máy tính khác. Cấu tạo phần này gồm nhiều trường (field), mỗi trường là một dòng văn bản ASCII chuẩn 7 bit như sau: <tên trường >: <nội dung của trường>.

Sau đây là một số trường thông tin thông dông:

| Trường | Chức năng |
|---|---|
| DATE | Chỉ ngày giờ nhận mail. |
| FROM | Chỉ địa chỉ người gởi. |
| TO | Chỉ địa chỉ người nhận. |
| CC | Chỉ địa chỉ những người nhận bản copy của mail. Các người nhận thấy được địa chỉ của những người cùng nhận trong nhóm. |
| BCC | Chỉ địa chỉ những người nhận bản sao chép của bức mail, nhưng từng người không biết những người nào sẽ nhận bức thư này. |
| REPLY-TO | Chứa các thông tin để người nhận có thể trả lời lại, thường nó chính là địa chỉ người gởi. |
| MESSAGE-ID | Định danh duy nhất, được sử dụng bởi hệ điều hành. |
| SUBJECT | Chủ đề của nội dung thư. |

Các trường trên là các trường chuẩn do giao thức SMTP quy định, ngoài ra trong phần header cũng có thể có thêm một số trường khác do chương trình e-Mail tạo ra nhằm quản lý các e-Mail riêng. Các trường này được bắt đầu bằng ký tự X- và thông tin theo sau là cũng giống như ta thấy trên một trường chuẩn.

- ***Phần nội dung***

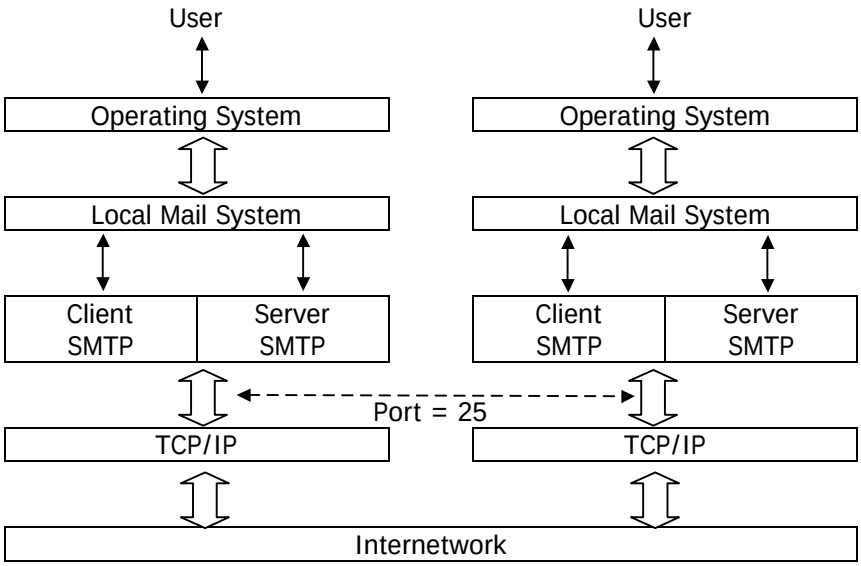
Để phân biệt phần tiêu đề và phần nội dung của e-Mail, người ta qui ước đặt ranh giới là một dòng trắng (chuỗi ký tự "\r\n"). Kết thúc của phần nội dung là chuỗi ký tự "\r\n.\r\n".

Như vậy nội dung bức thư nằm trong khoảng giữa dòng trắng đầu tiên và ký tự kết thúc thư, và trong phần nội dung của bức thư không được phép tồn tại chuỗi ký tự kết thúc thư. Mặt khác do môi trường truyền thông là mạng Internet nên các ký tự cấu thành phần thân của bức thư phải là các ký tự ASCII chuẩn.

### 10.6.1 Giao thức SMTP

SMTP (Simple Mail Transfer Protocol) là giao thức qui định việc truyền mail chủ yếu dùng trong mạng Internet.

Mối quan hệ giữa SMTP và hệ thống Mail cục bộ như sau:




Hình 10-9. Quan hệ giữa SMTP và hệ thống Mail cục bộ.

Client liên quan đến thư đi, Server liên quan đến nhận thư. Hệ thống thư cục bộ hộp thư (mailbox) cho mỗi user. Mail box có 2 phần: phần cục bộ và phần toàn cục.

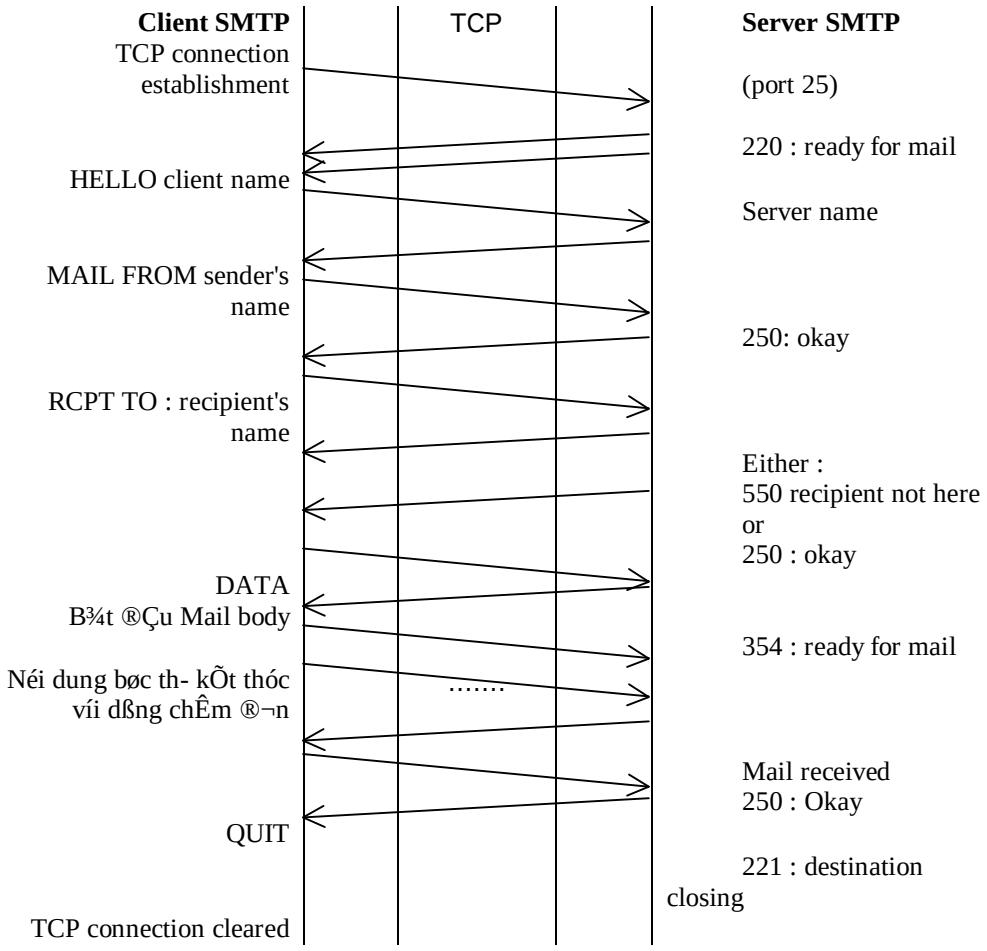
Sau khi tháo bức thư trong khuôn dạng chuẩn, hệ thống mail cục bộ xác định tên người nhận ở hộp thư cục bộ hay phải gửi ra ngoài. để gửi bức thư Client SMTP

phải biết địa chỉ IP của nơi nhận qua DNS và gửi qua cổng địa chỉ SMTP (25) để bắt đầu thiết lập kết nối server SMTP nơi nhận. Khi mối nối đã được thiết lập, Client bắt đầu chuyển bức thư đến Server bởi các lệnh của SMTP. SMTP dùng từ khóa như các lệnh để thực hiện thao tác chuyển giao mail. Một số lệnh chính của SMTP trong phiên làm việc giữa Client MTA và Server MTA như sau :

| Lệnh | Tác dụng |
|---|---|
| HELLO | Xưng danh với SMTP bên nhận, báo cho bên nhận biết bên gởi là ai. SMTP bên gởi gửi lệnh này đầu tiên cho SMTP bên nhận. |
| MAIL | Khởi động một cuộc giao dịch mail mà mục đích cuối cùng là chuyển giao các mail tới một hay nhiều Mailbox (nơi chứa Mail nhận được) khác nhau. |
| RCPT | Nói rõ người nhận mail là ai. |
| DATA | Các dòng sau lệnh DATA là dữ liệu của Mail. Đối với SMTP, chuỗi ký tự "CRLF.CRLF" báo nhận biết kết thúc nội dung bức Mail. |
| RSET | Bỏ (Reset) cuộc giao dịch hiện tại. |
| NOOP | Yêu cầu SMTP bên nhận không làm gì ngoài việc trả về câu trả lời OK (dùng để kiểm tra). |
| QUIT | Yêu cầu SMTP nhận trả lời OK và kết thúc phiên giao dịch hiện tại. |
| VRFY | Yêu cầu SMTP bên nhận kiểm tra người nhận là đúng, xác nhận các tham số gởi theo dòng lệnh. |
| SEND | Khởi động một cuộc giao dịch mà mail sẽ được gởi tới một hay nhiều thiết bị đầu cuối chứ không phải mailbox. |
| SOML | Khởi động một cuộc giao dịch mà mail sẽ được gởi tới một hay nhiều thiết bị đầu cuối hay mailbox. |
| SAML | Khởi động một cuộc giao dịch mà mail sẽ được gởi tới một hay nhiều thiết bị đầu cuối và mailbox. |
| HELP | Yêu cầu SMTP bên nhận gửi thông tin giúp đỡ cho SMTP bên phát. |
| EXPN | Yêu cầu SMTP bên nhận gởi về danh sách những người nhận Mail để có thể mở rộng việc chuyển mail cho các user khác. |
| TURN | Yêu cầu SMTP bên nhận gưi OK và đổi vai trò trở thành SMTP gởi. |

Bảng 10-1. Các lệnh của giao thức SMTP.

SMTP (trong RFC 821) ban đầu được thiết kế để cho phép các mail server chuyển đổi các mail message. Cơ chế chính được dùng để chuyển đổi các mail là phân đường các message quanh Internet. SMTP hoạt động trên mô hình lưu và truyền trong đó client nắm các message cần để truyền đến server và gửi các lệnh đến server để báo cho server cách xử lí các message. Mail client có thể là một mail server khác, nó có một hay nhiều message phải truyền đến một server khác. Hầu hết các Internet mail client sử dụng SMTP để gửi các message.




Hình 10-10. Cơ chế trao đổi SMTP.

#### *10.6.1.1 Quy tắc làm việc với SMTP*

1. Mỗi câu lệnh phân cách tham số theo sau bằng khoảng trắng và kết thúc bằng ký tự CRLF. Mail đi từ SMTP gởi đến một SMTP nhận và đến lượt SMTP nhận trở thành SMTP gởi để gửi mail đi tiếp cho đến khi chúng được giao vào Mailbox của người nhận.
2. Các lệnh SMTP phải diễn ra một cách tuần tự.
3. Việc đánh địa chỉ phải theo cách đánh địa chỉ Internet.

Giao thức SMTP qui định các Server MTA (ở đây là SMTP bên nhận) phải gởi tín hiệu phản hồi ACK sau mỗi lệnh mà nó nhận được từ Client MTA. Mỗi câu trả lời của bên nhận đều mở đầu với một mã số theo sau mới là thông tin dạng text. Mỗi số mở đầu trong mã số có một ý nghĩa khác nhau, nó chỉ ra rằng kết quả thực hiện thao tác là tốt (số 2), thất bại (số 5) hay chưa hoàn thành (số 3).

#### *10.6.1.2 Một số mã phản hồi thông dụng của SMTP*

220 Dịch vụ đã sẵn sàng.

221 Đóng kết nối đã được thiết lập.

250 Thao tác do Client MTA yêu cầu đã được hoàn thành.

354 Sẵn sàng nhận nội dung của mail.

550 Thao tác yêu cầu không thực hiện được do không có mailbox trên máy.

.v.v...

#### *10.6.1.3 Phiên giao dịch SMTP*

Để hiểu cách dùng một số lệnh chúng ta xem xét qua ví dụ sau: Bên gởi tên Thuận ở máy Sample1 muốn gởi cho Tín , Thức ở máy Sample2, giả sử Thức không có Mailbox tại Sample2.

Bên gởi thực hiện một kết nối đến SMTP Server.

RECEIVER : 220 sample2 Simple Mail Transfer Service Ready
Khi được kết nối qua giao thức TCP/IP, máy nhận trả lời với mã 220
để báo cho máy gởi biết dịch vụ SMTP đã sẵn sàng.
SENDER : HELO sample1
Bên nhận đã sẵn sàng, bên gởi gởi HELLO và xưng tên người gởi.
RECEIVER : 250 sample2
Trả với mã 250 báo cho biết bên nhận đã sẵn sàng.
SENDER : MAIL FROM: <>
Bên gởi dùng lệnh MAIL để khởi động phiên giao dịch. Cú pháp trên cho bên nhận biết
địa chỉ bên gởi (mailbox của bên gởi) để bên nhận gởi thông báo lỗi nếu có về bên gởi.
RECEIVER : 250 OK
Trả lời với mã 250 cho biết đã chấp nhận.
SENDER: RCPT TO: <>
Bên gởi cho biết e-Mail đích
RECEIVER: 250 OK
Trả lời với mã 250 cho biết đã chấp nhận
SENDER : RCPT TO: <>
Muốn gởi cho bao nhiêu người dùng bấy nhiêu lệnh RCPT kèm theo địa chỉ nhận,
bên nhận nếu đúng sẽ trả về mã 250 kèm theo OK.
RECEIVER : 550 No such user here
Báo kèm theo mã 550 cho biết không có mailbox trên địa chỉ trên đối với nơi nhận.
SENDER : DATA
Báo cho bên nhận biết dữ liệu bắt đầu từ sau từ DATA.
RECEIVER : 354 Start mail input; end with <CRLF>.<CRLF>
Mã 354 báo cho biết đã sẵn sàng nhận mail, kết thúc mail với ký tự "CRLF.CRLF".
SENDER : Bắt đầu thân của mail
SENDER : . . .
SENDER : (đến khi kết thúc gởi CRLF.CRLF)
RECEIVER : 250 OK
E-Mail đã được chấp nhận.

SENDER : QUIT

Phát lệnh báo kết thúc phiên giao dịch.

RECEIVER : 221 sample2 Service closing transmission channel

Mã 221 đóng kết nối đã thiết lập

#### *10.6.1.4 Giao thức mở rộng ESMTP*

SMTP có một hạn chế gây khó khăn lớn trong việc truyền nhận mail là giới hạn tối đa kích thước nội dung một bức mail chỉ là 128KB. Do vậy người ta đã cải tiến chuẩn SMTP thành một chuẩn mở rộng mới gọi là ESMTP, cho phép tăng giới hạn kích thước của mail lên trên 1MB.

Để biết xem Server MTA có theo chuẩn ESMTP hay không, thay vì dùng lệnh HELO ở đầu một cuộc giao dịch, Client MTA dùng lệnh mới EHLO, nếu Server MTA có trang bị, nó sẽ trả về mã thành công là 250. Ngày nay chuẩn ESMTP đã thay thế chuẩn SMTP ở đa số các hệ thống.

Chẳng hạn để khởi động cuộc giao dịch với kích thước mail lên tới 1MB, sử dụng dòng lệnh sau:

MAIL FROM :<thuan@sample1> SIZE=1000000

### 10.6.2 MIME

Từ khi MIME (Multipurpose Internet Mail Extention) được đưa ra, kiểu dữ liệu mà user có thể gửi thông qua e-Mail được mở rộng. Ban đầu dữ liệu chỉ ở dạng text. Ngày nay, ta có thể gửi các tài liệu (file *.doc), các file ảnh hay các file âm thanh.

Để có thể phân phát các kiểu dữ liệu này, khuôn dạng các message trên Internet nên được mở rộng. MIME được phát triển cho mục đích này.

#### *10.6.2.1 Cấu trúc message của MIME*

MIME không phải cho các ứng dụng e-Mail mới, nhưng cho phép mở rộng khả năng e-Mail trên Internet trong khi vẫn giữ các ứng dụng giao vận và nền tảng hiện tại. Khuôn dạng MIME duy trì các cấu trúc message cơ bản với các phần Header và phần body (tham khảo RFC 822). Ví dụ về khuôn dạng của một tài liệu MIME như sau :

{Dòng này xác định MIME message}

MIME-Version: 1.0

To:

Subject: Book CD

{Dòng này xác định đây là một kiểu messsage hỗn hợp và các phần được phân tách nhau bởi dấu biên}

Content-Type: multipart/mixed; boundary="--------6B9767D111AE"

X-Mozilla-Status: 0001

{Kết thúc phần header}
{Biên đầu tiên, thể hiện phần đầu của message}

--------6B9767D111AE
{Đây là đoạn text, thể hiện các kí tự dạng US-ASCII}
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
{Kết thúc phần header}

Davis,
I am .....
Thanhs,
Davis
{Phần sau là phần đánh dấu biên}

--------6B9767D111AE
{Phần tiếp  sau là một file nhị phân}
Content-Type: application/octet-stream
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="Sublic2.doc"
{Phần dưới đây là nội dung file}

0M8.....
{Phần sau đây là biên kết thúc file}

--------6B9767D111AE

#### *10.6.2.2 MIME version header*

MIME version header định danh một message như một message MIME, và xác định version của MIME chuẩn để dịch message. Nếu không tìm thấy header, client sẽ đối xử với message theo khuôn dạng chuẩn trong RFC. Phiên bản hiện tại của MIME là 1.0. Cú pháp của MIME header version như sau:

MIME-Version: 1.0

*1. Content Type header*

Content Type header xác định khuôn dạng file được gán vào trong một đối tượng. Header báo cho MIME cách hiển thị hay thao tác trên thân của message. Content Type Header bao gồm tên của header, theo sau bởi kiểu MIME. Kiểu MIME theo sau hai tên và được cách biệt nhau bởi kí tự slash (/). Tên đầu tiên là tên kiểu và tên thứ hai là một tên phụ. Sau đây là các ví dụ của Content type header:

Content-Type: image/jpeg
Content-Type: image/gif
Content-Type: image/bmp
Content-Type: image/mpeg

Content-Type: application/octet-stream

Ba ví dụ đầu tiên trong phần này, đối tượng là kiểu ảnh (cũng là kiểu nhị phân), kiểu con của nó là jpeg, gif, và bmp. Các file ảnh này được nhúng vào trong các message. Dòng thứ tư trong các ví dụ này đó là một file chương trình.

Các kiểu và kiểu con có thể được thiết lập bởi các tham số. Mỗi tham số bao gồm một tên tham số, theo sau bởi dấu bằng (=) và tiếp theo là giá trị tham số. Các tham số này được tách biệt giữa kiểu và kiểu con, cũng như các tham số khác và được tách biệt nhau bởi dấu chấm phẩy. Ví dụ sau đây thể hiện một tập các tham số:

Content-Type: text/plain; charset=us-ascii

Kiểu đối tượng này báo cho người đọc message rằng các phần theo sau là dạng text và sử dụng các kí tự theo kiểu text.

Header này có thể hoàn toàn tuỳ chọn. Nếu nó không được cung cấp thì message được đối xử như một chuỗi các kí tự ASCII.

2. *Content Transfer Encoding Header*

Content Transfer Encoding Header xác định mô hình mã hoá được sử dụng để nhúng đối tượng vào trong thân của message. Để nhúng một đối tượng nhị phân vào trong một thư điện tử, cần phải chuyển nó sang kiểu dạng ASCII, do vậy nó được biên dịch theo khuôn dạng RFC 822. Ví dụ một cú pháp header dùng để mã hoá nội dung khi truyền là Content-Transfer-Encoding Base64.

Tài liệu MIME định nghĩa 5 kiểu mã hoá, nhưng 3 kiểu mã hoá thể hiện đối tượng không được mã hoá. Mã hoá 7 bit thường được dùng cho các vùng text theo khuôn dạng MIME. Hai kiểu kia mã hoá theo kiểu 8 bit và nhị phân, chỉ được sử dụng khi chuyển thư không phải SMTP, do SMTP chỉ cho phép các kí tự ASCII theo kiểu mã hoá 7 bit. Hai mô hình mã hoá còn lại đó là quoted-printable và base64 để chuyển các các đối tượng từ dạng nhị phân sang kiểu ASCII.

#### *10.6.2.3 Cấu trúc message MIME đa phần*

Một trong số các khả năng phổ biến của MIME đó là có một message đa phần. Bằng cách sử dụng message đa phần, ta có thể nhúng cả hình ảnh và âm thanh vào các message text hay xây dựng một ứng dụng về một đối tượng hoạt hình, nó bao gồm một số file cần thiết để chạy ứng dụng.

Cấu trúc message đa phần bao gồm nhiều message kết hợp vào trong thân của một message, mỗi message với thông tin header của nó thể hiện kiểu nội dung mà mô hình mã hoá. Các phần này được tách biệt bởi các dấu biên mà message chính định ra. Để hiểu chi tiết về cấu trúc của một message đa phần, xem RFC 1521.

#### *10.6.2.4 Mã hóa BASE64*

Thuật toán mã hoá Base64 được thiết kế để mô tả một chuỗi tuỳ ý các giá trị 8bit mà con người không có khả năng đọc được thành các kí tự ASCII. Thuật toán mã hoá và giải mã đơn giản nhưng dữ liệu mã hoá sẽ lớn hơn dữ liệu nguồn 33%.

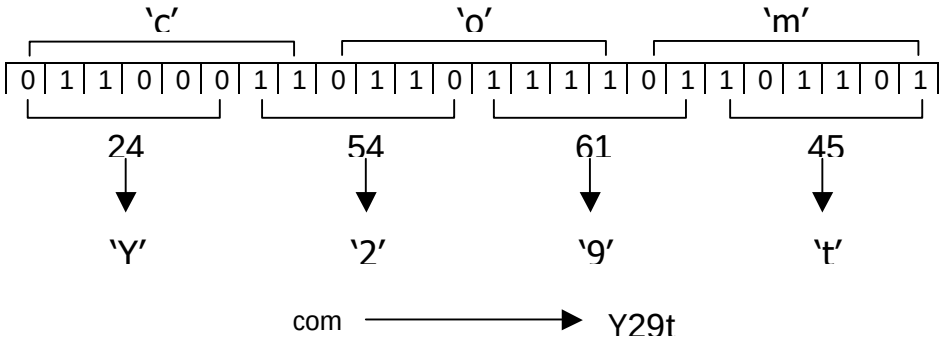
Một tập 65 kí tự US-ASCII được dùng, cho phép 6bits biểu diễn cho các kí tự có thể in được. (Kí tự thứ 65, "=", là một kí tự xử lý đặc biệt)

Tiến trình mã hoá biểu diễn nhóm 24 bits dữ liệu nhập thành 4 kí tự mã hoá ở đầu ra. Tiến trình thực hiện từ trái sang phải, một nhóm 24 bit nhập được kết hợp từ nhóm 3 kí tự 8bits. 24 bits đó được chia làm 4 nhóm kí tự 6bits, mỗi nhóm được dịch thành một kí tự đơn dựa vào bảng mã Base64.

**Bảng mã Base64**

| Value | Encoding | Value | Encoding | Value | Encoding | Value | Encoding |
|---|---|---|---|---|---|---|---|
| 0 | A | 17 | R | 34 | i | 51 | z |
| 1 | B | 18 | S | 35 | j | 52 | 0 |
| 2 | C | 19 | T | 36 | k | 53 | 1 |
| 3 | D | 20 | U | 37 | l | 54 | 2 |
| 4 | E | 21 | V | 38 | m | 55 | 3 |
| 5 | F | 22 | W | 39 | n | 56 | 4 |
| 6 | G | 23 | X | 40 | o | 57 | 5 |
| 7 | H | 24 | Y | 41 | p | 58 | 6 |
| 8 | I | 25 | Z | 42 | q | 59 | 7 |
| 9 | J | 26 | a | 43 | r | 60 | 8 |
| 10 | K | 27 | b | 44 | s | 61 | 9 |
| 11 | L | 28 | c | 45 | t | 62 | + |
| 12 | M | 29 | d | 46 | u | 63 | / |
| 13 | N | 30 | e | 47 | v | | |
| 14 | O | 31 | f | 48 | w | (pad) | = |
| 15 | P | 32 | g | 49 | x | | |
| 16 | Q | 33 | h | 50 | y | | |

Ví dụ sau mô tả tiến trình mã hoá 3 kí tự nhập là "com":




Luồng dữ liệu được mã hoá đầu ra phải được biểu diễn bằng các dòng có độ dài không lớn hơn 76 kí tự. Tất cả các kí tự xuống dòng hay các kí tự khác không có trong bảng mã Base64 đều được phần mềm giải mã bỏ qua.

Khi nhóm bit dòng nhập ít hơn 24 bits (nghĩa là đến cuối của dữ liệu cần mã hoá) thì cần có xử lý đặc biệt. Khi có ít hơn 24 bits dòng nhập thì các bits 0 được thêm vào phía bên phải nhóm bit để được đủ số 24 bits. Khi dòng nhập đã đủ 24bits thì có các khả năng có thể xảy ra:

1. Phần cuối cùng của dữ liệu cần mã hoá là 24 bits thì dữ liệu đầu ra cuối cùng sẽ là 4 kí tự đã mã hoá mà không có kí tự đệm "=".
2. Phần cuối cùng của dữ liệu cần mã hoá chính xác là 8 bits thì dữ liệu đầu ra cuối cùng sẽ là 2 kí tự đã mã hoá kèm theo với 2 kí tự đệm “=” ở cuối.

- Nếu phần cuối cùng của dữ liệu cần mã hoá chính xác là 16 bits thì dữ liệu đầu ra cuối cùng sẽ gồm 3 kí tự đã mã hoá kèm theo với 1 kí tự đệm “=” ở cuối.

Bởi vì các kí tự đệm chỉ được thêm vào cuối của dữ liệu nên khi gặp bất kì một kí tự “=” nào thì hiển nhiên là đã đến vị trí kết thúc của dữ liệu.

### 10.6.3 Giao thức POP

Người sử dụng có thể gửi thư bằng cách sử dụng SMTP, và có thể nhúng bất kỳ đối tượng nào vào trong message thông qua việc sử dụng khuôn dạng MIME. Tuy nhiên, với SMTP, server để nhận được các message thư phải nối đến client và gửi tất cả các message được phân phát cho client. Do đó, người sử dụng  phải đăng ký tên máy dưới dạng tên địa chỉ Internet của người nhận.

SMTP được thiết kế trong trường hợp nhiều user sử dụng tất cả thời gian của họ kết nối đến một vài host và chạy một phiên đầu cuối. Giao thức không được thiết kế cho các tình huống thông dụng hiện nay, trong đó, hầu hết tất cả các user sử dụng e-mail kết nối hạn chế đến mail server đang giữ hộp thư. Người sử dụng phải duy trì các message thư trên server và chuyển nó đến cho client khi client yêu cầu. Đây là một mục đích trong thiết kế của POP.

POP (Post office Protocol) được thiết kế để bù đắp cho SMTP trong phần nhận các message. Những người thiết kế POP không gộp các chức năng gửi message và cho rằng SMTP tiếp tục được sử dụng để thực hiện các chức năng đó. Với giao thức POP, máy tính  nhận khởi tạo kết nối. Máy nhận kết nối đến mail server, login và nhận bất kỳ một message nào đang chờ. Do vậy mà máy gửi không cần biết gì về máy nhận trừ khi nó sử dụng login và password để đăng nhập. Ngày nay, hầu hết tất cả các mail client trên Internet mà bạn có thể sử dụng để kết hợp cả SMTP và POP.

#### *10.6.3.1 Mô hình thông tin POP*

Trong mô hình lưu và phát, server mail cục bộ lưu các message đến khi các client nhận nó. POP client kết nối với server trên cổng 110 của TCP. Để đăng nhập vào server, user sử dụng định danh (ID) và password. Sau khi đăng nhập thành công vào server, client có thể yêu cầu server về các message mới đang sẵn sàng, lấy bất kỳ message nào mà server đang gửi hay xoá đi một message nào đó trên server.

Mô hình thông tin POP sử dụng 3 trạng thái giao tác để cung cấp chức năng này đến POP client:

- Trạng thái đặc quyền : Server kiểm tra quyền truy nhập của client (ID và password).
- Trạng thái giao tác : Client có thể nhận hay xoá các message.
- Trạng thái cập nhật : Trạng thái này được chuyển đến ngay sau khi client tạo ra lệnh QUIT.

Trạng thái cập nhật là trạng thái cho phép thao tác trên các message. Khi client đang ở trên trạng thái giao tác, bạn có thể tạo ra lệnh reset để huỷ bỏ tất cả các thao tác xóa trước đó (undo).

#### *10.6.3.2 Chuẩn POP3*

Giao thức POP3 được cải tiến từ giao thức POP. Nhiệm vụ của giao thức POP3 là lấy mail từ mailbox về khi nào người nhận muốn.

Đặc điểm của hệ thống dùng POP là cho phép người sử dụng login vào POP Server và nhận các mail từ mailbox của mình mà không cần phải login vào mạng mặc dù các mailbox thường nằm ở các Mail Server nằm trong mạng ( thông thường muốn thâm nhập mạng ta phải có một account trên mạng và phải cung cấp Password khi đăng nhập vào mạng ). Người sử dụng có thể truy xuất POP Server từ bất cứ một hệ thống nào trên mạng Internet, từ bất cứ UA nào dùng giao thức POP.

POP3 định nghĩa 3 giai đoạn tạo thành POP Session : Giai đoạn 1 là giai đoạn xác định tính hợp pháp của người nhận mail (Authorization); giai đoạn 2 là giai đoạn giao dịch giữa PC và POP Server (Transaction) và giai đoạn 3 là giai đoạn cập nhật thông tin (Update).

Sau khi thiết lập kết nối với Server, giai đoạn đầu Client sẽ cho Server biết nó là ai. Nếu Client hợp pháp POP Server sẽ mở Mailbox và bắt đầu chuyển sang giai đoạn giao dịch. Giai đoạn giao dịch, chương trình Client sẽ yêu cầu POP3 Server cung cấp các thông tin như danh sách mail..v..v..hay yêu cầu gởi về cho nó một bức mail xác định nào đó. Giai đoạn cuối cùng sẽ cập nhật và đóng kết hiện hành.

Các lệnh thông dụng của giao thức POP3 :

| Lệnh | ý nghĩa |
|---|---|
| **User** | Cho biết tên của user cho POP Server |
| **Pass** | Yêu cầu một Password cho người sử dụng trên Server |
| **Quit** | Đóng kết nối TCT đã được thiết lập trước đó |
| **Stat** | POP Server trả về số lượng Mail có trong mailbox của người sử dụng cùng kích thước chúng |
| **List** | Trả về các ID và size của các Message |
| **Retr** | Nhận một Message từ Mailbox (yêu cầu tham số là ID của mail cần nhận) |
| **Dele** | Đánh dấu một Message để xóa (yêu cầu tham số là ID của mail cần xóa) |
| **Noop** | POP Server trả về +OK nhưng không làm gì cả |
| **Last** | Yêu cầu POP Server trả về số Message đã truy nhập |
| **Top** | Liệt kê Header của Mail |
| **Rset** | Hủy đánh dấu trên Message bị đánh dấu để xóa |

POP3 chỉ định nghĩa 2 loại trả lời cho mỗi câu lệnh là : +OK để chỉ thao tác hoàn thành tốt và - ERR để báo có lỗi. Ví dụ cách dùng một số lệnh của POP3 như sau (các hàng sau dấu chấm phẩy để chú thích lệnh).

Giai đoạn 1 : Nhận dạng user

```
CLIENT : USER user01     ; cho biết tên user là user01
SERVER : +OK             ; báo thành công
CLIENT : PASS abc        ; cho biết password là abc
SERVER : +OK user01's    ; maildrop has 2 messages ( 520 octets)
```

Giai đoạn 2 : Trao đổi

```
CLIENT : STAT            ; số mail có trong mailbox
SERVER : +OK 2 520       ; Có 2 mail với tổng kích thước là 520
CLIENT : LIST            ; Liệt kê các ID và kích thước các mail
SERVER : +OK 2 message ( 520 octets )
SERVER : 1 110           ; mail thứ 1 kích thước 110
SERVER : 2 410           ; mail thứ 2 kích thước 410
CLIENT : LIST 1  ; Cho thông tin về mail có ID là 1
SERVER : +OK 1 110
CLIENT : LIST 4
SERVER : -ERR            no such message, only 2 message in maildrop
. . .v. . .v . . .
```

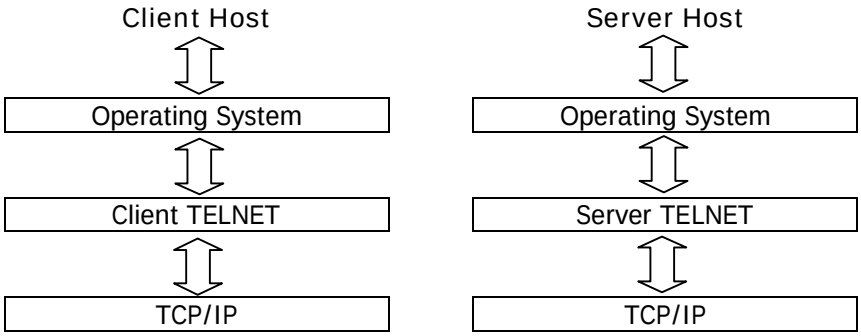
Giai đoạn 3 : Kết thúc

```
CLIENT : QUIT ; đóng kết nối TCP hiện hành
SERVER : +OK dhbk POP3 server signing off
```

Chú ý rằng các message bị đánh dấu để xóa bằng lệnh DELE thực sự chưa bị xóa ngay để nếu sau đó ta có thể dùng lệnh phục hồi không xóa bằng lệnh RSET,

chúng chỉ thực sự bị xóa bỏ khỏi maildrop khi bước vào giai đoạn Update (khi gởi lệnh QUIT).

## 10.7 Dịch vụ truy cập từ xa - TELNET




Hình 10-11. Phương thức truy nhập từ xa Telnet.

Chương trình Telnet (TELecommunication NETwork) cho phép truy cập từ xa hoặc có các thiết bị ảo thông qua mạng (điều này có nghĩa là bình thường thì bạn không thể có được thiết bị này nhưng nay nhờ có dịch vụ Telnet, bạn có thể truy cập và dùng được các thiết bị đầu cuối do đó gọi là các thiết bị đầu cuối ảo). Nói cách khác, một user A có thể truy cập vào một máy B ở bất cứ nơi nào trong mạng và làm việc với máy đó giống như đang ngồi trước máy đó. Dịch vụ Telnet được cung cấp qua cổng số 23 của TCP/IP. Khái niệm Telnet để chỉ cả *dịch vụ và giao thức* cung cấp các dịch vụ truy cập từ xa này.

Giao thức Telnet dùng một khái niệm Network ***Virtual Terminal*** (NVT), để định nghĩa kết nối Telnet cho cả hai phía. Mỗi đầu của kết nối (mỗi NVT) có một bàn phím và một máy in logic. Máy in logic có thể hiển thị các kí tự và bàn phím logic có thể tạo các kí tự. Máy in logic thường là một màn hình của thiết bị đầu cuối, trong khi đó bàn phím logic thường là bàn phím của người dùng

Khi một kết nối Telnet được thiết lập, Telnetd (hay bất kỳ một chương trình nào khác mà làm việc như là Telnet server) bắt đầu quá trình chạy một số các ứng dụng. Mỗi phím được ấn sẽ phải qua Telnet, Telnetd, và các ứng dụng được dùng trong quá trình thực hiện một phiên làm việc của kết nối Telnet.

Người sử dụng đưa vào lệnh và số liệu, chương trình Telnet ở máy khách (client Telnet) sẽ chuyển lệnh và số liệu đến chương trình Telnet trên máy chủ (server telnet) tương ứng. Server telnet xử lý và gửi kết quả trở lại cho Client Telnet.

### *10.7.1.1 Các lệnh của Telnet*

Hai hệ thống Telnet Client/Server liên lạc với nhau bằng những lệnh gồm những *kí tự đơn* hay một *chuỗi kí tự*, nó được mã hoá trong dạng chuẩn NVT (Network Virtual Terminal - Mạng đầu cuối ảo).

Khi một kết nối Telnet được thiết lập, một số dịch vụ có thể sẵn sàng để lựa chọn. Giá trị của chúng có thể thay đổi trong một phiên làm việc Telnet (*Telnet Session*) nếu cả hai phía của kết nối đồng ý sự thay đổi đó. (Có thể xảy ra trường hợp một đầu của kết nối Telnet không thể cho phép hay không cho phép một dịch vụ trong quá trình kết nối Telnet diễn ra do sự cho quyền của nhà quản lý hoặc các thiết lập nguồn (Source settings)). Có bốn giao thức Telnet được dùng để Để nghị (offer), Từ chối (refuse), Yêu cầu (request) và Ngăn chặn (prevent) các dịch vụ, đó là các động từ: WILL, WON'T, DO và DON'T. Các động từ trên được thiết kế đi với nhau theo từng cặp ( WILL/WON'T và DO/DON'T).

| **Lệnh** | **Mã thập phân** | **ý nghĩa** |
|---|---|---|
| IAC | 255 | Nhận biết byte tiếp theo là lệnh |
| NOP | 241 | Không điều khiển |
| EC | 247 | Xóa ký tự (Erase character) |
| EL | 248 | Xóa dòng (Erase line) |
| GA | 249 | Về đầu (Go ahead) |
| AYT | 246 | Are you there |
| IP | 244 | Quá trình ngắt (Interrupt process) |
| AO | 245 | Xóa bỏ đầu ra (Abort output) |
| BRK | 243 | Dừng (break output) |
| DMARK | 242 | Phục hồi đầu ra (Resume output) |
| SB | 250 | Bắt đầu trao đổi (Start potion request) |
| SE | 240 | Kết thúc (End) |
| WILL | 251 | Thỏa thuận/Yêu cầu (Agreement/request option) |
| WONT | 252 | Từ chối (Refuse option request) |
| DO | 253 | Tiếp nhận yêu cầu (Accept request option) |
| DON'T | 254 | Từ chối tiếp nhận yêu cầu |

- Các hàm chức năng khác :

| **Tên** | **Mã** | **ý nghĩa** |
|---|---|---|
| Transmit binary | 0 | Yêu cầu/T.nhận trao đổi số nhị phân 8 bit |
| Echo | 1 | Ký tự phản hồi (Echo character receiving back to sender) |
| Status | 5 | Trạng thái (Request/reply status of receiving TELNET) |
| Timing mark | 6 | Đánh dấu thời gian. |
| Terminal type | 24 | Loại yêu cầu/trả lời của thiết bị đầu cuối. |
| Line mode | 34 | Gửi dòng ký tự |

Ví dụ các dòng lệnh tiêu biểu như sau :

IAC, SB, WILL, 'O', SE : Yêu cầu bên nhận nhận số nhị phân 8 bit
IAC, SB, DO, 'O', SE : Hệ truy nhập từ xa nhận trả lời tiếp nhận
IAC, SB, DON'T, 'O', SE : Hoặc từ chối
IAC, SB, DO, 'O', SE : Bên nhận yêu cầu
IAC, SB, WILL, 'O', SE : Bên gửi thỏa thuận
IAC, SB, WON'T, 'O', SE : Hoặc từ chối

- Làm việc với Telnet

- Truy nhập vào mạng TCP/IP từ máy trạm
- Gõ lệnh : telnet <ĐịachỉIP hoặc tênmáyServer>
- Thao tác trên màn hình Telnet.

### 10.7.2 Dịch vụ truyền tập tin FTP

Giao thức truyền tập tin FTP (File Transfer Protocol) cho phép truyền các tập tin giữa hai máy tính, quản lý các thư mục và truy cập vào thư tín điện tử. FTP không được thiết kế để truy cập vào một máy khác và chạy các chương trình ở máy đó. FTP giúp người sử dụng truy cập file và thư mục trên một máy chủ ở xa và thực hiện những thao tác trên thư mục như sau :

- Liệt kê các file trên một thư mục cục bộ hay ở xa.
- Đổi tên và xóa tập tin (nếu có quyền).
- Truyền file đi hay về từ trạm và máy ở xa (download/upload).

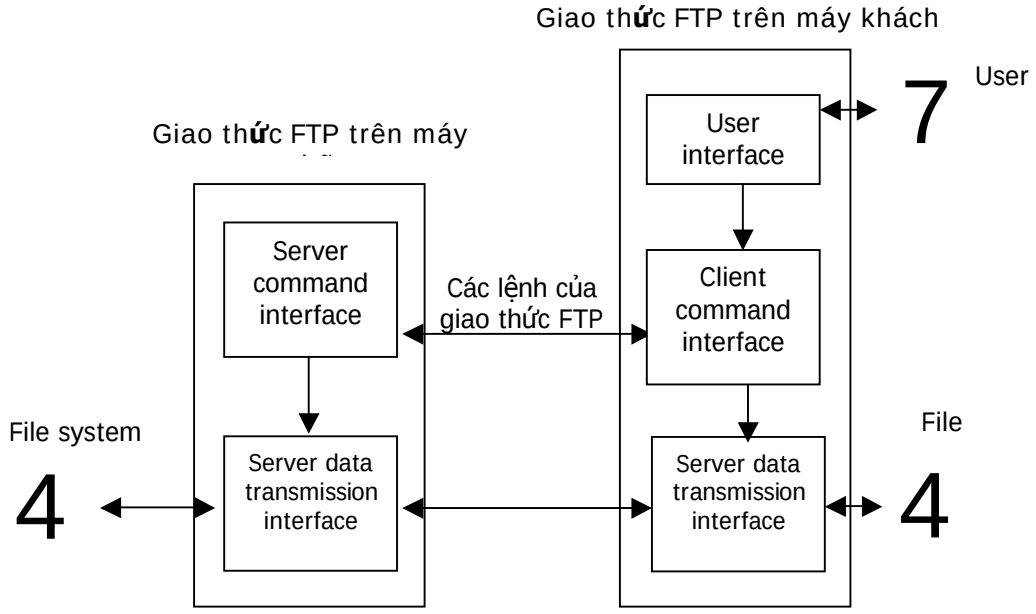
FTP dùng hai kênh TCP, với số hiệu cổng 20 là ***kênh dữ liệu***, và số hiệu cổng 21 là ***kênh lệnh*** (*command channel*). FTP khác các ứng dụng khác của TCP/IP ở là FTP quản lý tất cả việc truyền các tập tin bằng foreground thay vì background. Nói cách khác, FTP không dùng các hàng đợi hay các tiến trình kiểu ống (spooler) do đó bạn có thể quan sát quá trình truyền tập tin trong thời gian thực. Bằng cách dùng TCP, FTP loại trừ được việc quản lý kết nối và độ tin cậy, bởi vì FTP có thể dựa trên TCP để thực hiện các chức năng này một cách chính xác.

Kết nối đầu tiên, kênh lệnh, được khởi tạo thông qua FTP client. Client kết nối với server dựa trên cổng 21 của TCP, cung cấp cho server tên (login) và password và sau đó tiến đến các phiên FTP. Nếu client tạo ra một lệnh yêu cầu một dòng trả lời từ server, kênh lệnh sẽ truyền trả lời này.

Khi client gởi một yêu cầu có nhiều hơn một trả lời để gửi hay nhận dữ liệu, kênh thứ hai được đặt vào hoạt động. Để thiết lập kết nối thứ hai, bạn có 3 tuỳ chọn. Mặc định, server khởi tạo kết nối thứ 2 thông qua cổng 20 của TCP và kết nối đến một socket thứ hai trên client, sử dụng cùng một địa chỉ và cổng như trong kết nối thứ nhất trên client. Tuy nhiên, client có thể chỉ định một địa chỉ khác hay một cổng khác để truyền dữ liệu, trong trường hợp này, server cố gắng kết nối đến client

thông qua việc sử dụng một địa chỉ mới. Tuỳ chọn thứ 3 là client khởi tạo một kết nối truyền dữ liệu là báo cho server chuyển sang chế độ thụ động, server trả lời một địa chỉ và số hiệu cổng để truyền dữ liệu.

Ngay sau khi truyền dữ liệu kết thúc, kết nối để truyền dữ liệu được đóng lại. Kết nối này được mở lại khi client tạo ra một lệnh yêu cầu truyền dữ liÖu.




Hình 10-12. Mô hình giao tiếp FTP.

- FTP hoạt động theo mô hình Client/Server bao gồm thành phần chính :

  + Đơn vị trao đổi dữ liệu (Data Transmission interface)/

  + Đơn vị nhận biết lệnh (Command interface)

### *10.7.2.1 Chế độ truyền dẫn*

Có 3 chế độ được dùng để truyền dữ liệu giữa hai hệ thống. Chế độ đầu tiên là ngầm định nhưng 2 chế độ kia truyền hiệu quả hơn và có thể phục hồi.

- ***Truyền theo dòng:*** đây là chế độ truyền ngầm định, gửi một file dưới dạng một chuỗi các byte; FTP server và client không định dạng file đó. File nguồn không có cách gì để báo hết nội dung truyền, do vậy vấn đề kết thúc file được qui định bằng đóng kết nối dữ liệu.
- ***Truyền theo khối:*** chia file thành các khối, và mỗi khối có thêm các byte điều khiển (header). Trong header có một trường xác định số lượng byte trong khối, trường mô tả mã, nó có thể định đó là khối đặc biệt, kết thúc trong quá trình truyền. Chế độ truyền này cho phép phục hồi khi bị ngắt trong quá trình truyền file thông qua việc báo truyền lại một khối chỉ định trong trường count của header.

- ***Chế độ truyền nén:*** nén file để truyền thông qua việc sử dụng thuật toán mã hoá mã run-length. Thuật toán nhằm làm giảm các byte lặp lại vào trong hai byte kế tiếp. Byte đầu tiên cho biết byte theo sau là nén và số lần nó được lặp lại. Để thể hiện nén, bit đầu tiên của byte điều khiển được thiết lập 1. Nếu bit này là 0, nó cho biết byte theo sau không phải là byte nén. Phần còn lại của byte điều khiển xác định số lượng các byte không nén theo sau. Do vậy, hiệu quả khi nén các kí tự lặp lại đó là không làm mất đi các kí tự không nén.

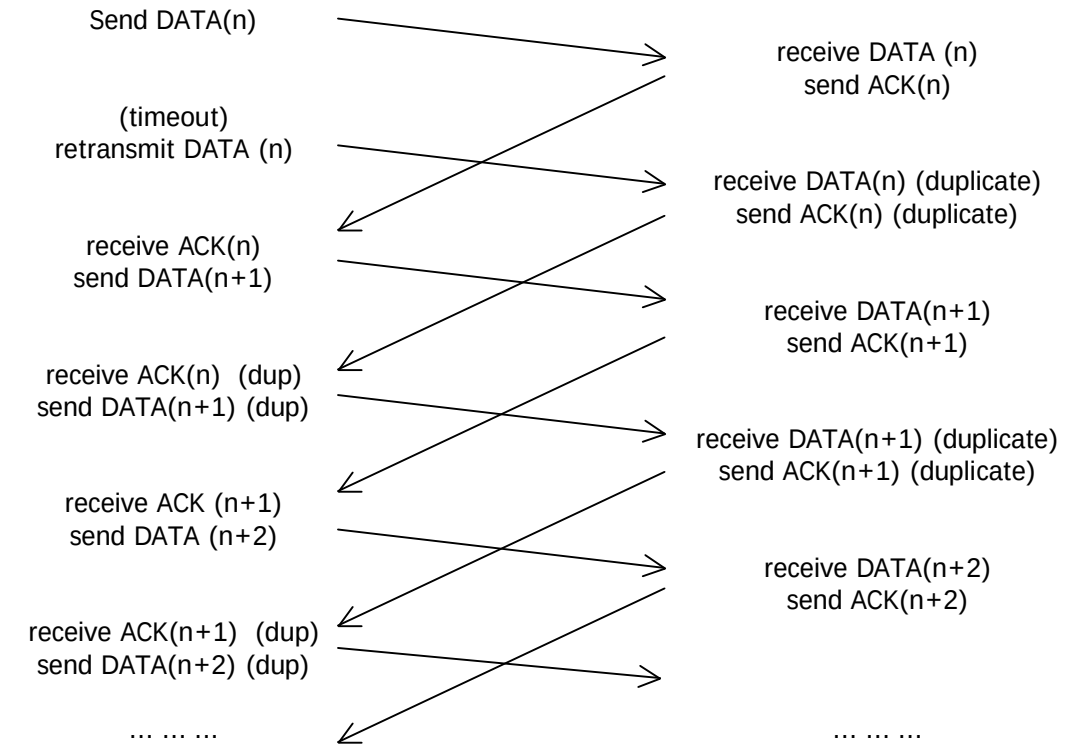
Để bắt đầu, client gửi yêu cầu **read** hay **write**. Gói tin trao đổi có độ dài đến 512 bytes. Mỗi block số liệu có đánh số và phải được biên nhận để gửi tiếp hay phát lại. Để tránh phát trùng lặp khi hết thời hạn, phát lại bản tin vừa phát và khi nhận ACK (n) trùng lặp thì không phát gì .

### *10.7.2.2 Dạng bản tin FTP*

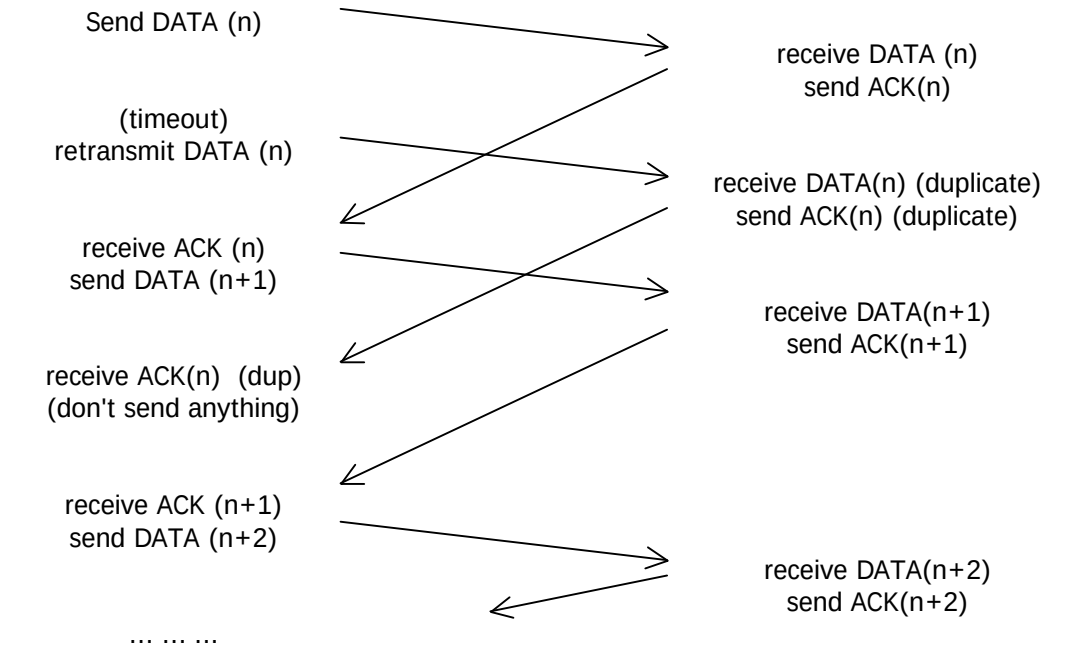
| | | | | | |
|---|---|---|---|---|---|
| Read request (RRQ) | opcode | String | EOs | String | EOs |
| | 01 | File name | 0 | mode | 0 |
| | 2 bytes | n bytes | 1 byte | n bytes | 1 byte |
| Write request (WRQ) | opcode | String | EOs | String | EOs |
| | 02 | File name | 0 | mode | 0 |
| | 2 bytes | n bytes | 1 byte | n bytes | 1 byte |
| DATA | opcode | Block# | Data | | |
| | 03 | | | | |
| | 2 bytes | 2 bytes | n bytes, 0≤n≤512 | | |
| Acknowled-gement (ACK) | opcode | Block# | | | |
| | 04 | | | | |
| | 2 bytes | 2 bytes | | | |
| Read request (RRQ) | opcode | | String | EOs | |
| | 05 | Errorcode | Err String | 0 | (EOs : End of String) |
| | 2 bytes | 2 bytes | n bytes | 1 byte | |

Hình 10-13. Khuôn dạng bản tin FTP.

*Ví dụ:* Quá trình phát lặp :




+ Tr¸nh ph¸t lÆp




Hình 10-14. Quá trình phát lặp bản tin FTP.

### *10.7.2.3 Quá trình làm việc FTP*

1. Truy nhập vào mạng TCP/IP từ máy trạm.
2. Gõ lệnh : ftp <Địa_chỉ_máy_Server>.
3. Làm việc với FTP.

Khi một kết nối FTP được thiết lập, thực hiện các bước như sau:

- Duyệt tên và mật khẩu (ID) của người dùng.
- Xác định thư mục bắt đầu làm việc.
- Định nghĩa chế độ truyền tập tin.
- Cho phép các lệnh của người dùng.
- Huỷ kết nối.

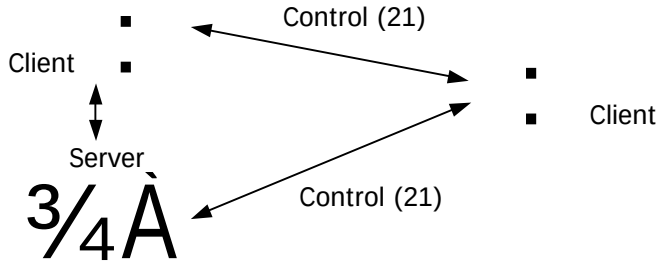
| **Lệnh FTP** | **Mô tả** |
|---|---|
| ascii | Chuyển sang chế độ truyền ascii |
| bell | âm thanh của chương trình sau khi truyền mỗi tập tin |
| binary | Chuyển sang chế độ truyền nhị phân |
| cd *directory* | Chuyển đổi thư mục hiện hành trên server |
| cdup | Lùi thư mục hiện hành về một cấp trước đó |
| close | Huỷ kết nối |
| delete *filename* | Xoá một tập tin trên server |
| dir *directory* | Hiển thị thư mục *directory* của server |
| get *filename* | Truyền tập tin trên server về máy cục bộ |
| hash | Hiển thị/làm mất dấu # cho mỗi khối các ký tự đã truyền được |
| help | Hiển thị các trợ giúp |
| lcd *directory* | Chuyển đổi thư mục hiện hành trên máy cục bộ |
| ls *directory* | Xem danh sách các tập tin trong thư mục directory trên Server |
| mdelete *files* | Xóa nhiều tập tin trên máy Server |
| mdir *directories* | Liệt kê các tập tin trong nhiều thư mục trên máy Server |
| mget *files* | Lấy một số file trên Server về thư mục hiện hành của máy cục bộ |
| mkdir *directory* | Tạo thư mục directory trên máy Server |
| mput *files* | Gửi một số tập tin từ máy cục bộ lên máy Server |
| open *host* | Kết nối với Server host từ xa |
| put *filename* | Truyền tập tin từ máy cục bộ lên máy Server |
| pwd | Hiển thị thư mục hiện thời của server |
| status | Hiển thị trạng thái của ftp |
| rename *file1 file2* | Đổi tên *file1* trên máy Server thành *file2* |
| quote | Cung cấp một lệnh FTP một cách trực tiếp |
| quit | Chấm dứt kết nối và thoát khỏi ftp |
| ? | Hiển thị danh sách lệnh |

Đề truyền một tập tin từ *thư mục hiện hành* trên máy Client đến máy Server bạn dùng lệnh *put*, ngược lại, muốn tải tập tin từ máy Server về máy Client, bạn dùng lệnh *get*. Cú pháp như sau :

```
ftp>put   local_file   remote_file
ftp>get   remote_file   local_file
```

Khi truy cập vào hệ thống, nếu chưa có account, người sử dụng có thể sử dụng một login name đặc biệt là *anonymous* để truy cập vào hệ thống. Acount này không có mật khẩu.

FTP cho phép truyền các tập tin thông qua máy thứ 3, máy này nằm giữa client và server. Thủ tục này được gọi là truyền tay ba điều này cần thiết để có được có được sự cho phép chính xác để truy cập vào máy ở xa. Hình sau mô tả sơ đồ của thủ tục này :




Hình 10-15. Truyền các tập tin thông qua máy thứ 3.

#### *10.7.2.4 Khuôn dạng dữ liệu*

Khi truyền dữ liệu giữa hai hệ thống, có thể sử dụng 4 kiểu dữ liệu để truyền. Trong số các kiểu dữ liệu này thì có 2 kiểu dữ liệu hay được sử dụng nhất hiện nay, hai kiểu khác vẫn được hỗ trợ nhưng ít được sử dụng. Các hệ thống ở cả hai đầu trong quá trình đàm thoại FTP phải hỗ trợ tất cả các kiểu dữ liệu sau đây:

- Kiểu ASCII, đây là kiểu mặc định được dùng trong các phiên FTP. Nó được dùng để truyền các file text. Nếu bạn cố truyền các file nhị phân mà bạn không thay đổi mode thì bạn cũng nhận được kết quả ở dạng text, do vậy nội dung của file đã bị thay đổi.
- EBCDIC được sử dụng để truyền các file giữa giữa các host, sử dụng EBCDIC như một tập các kí tự bên trong của nó. Về mặt kỹ thuật thì kiểu dữ liệu ASCII và EBCDIC là giống nhau, chỉ khác một điều là tập các kí tự mà nó sử dụng
- Kiểu nhị phân là kiểu được sử dụng để truyền các file nhị phân như các file ảnh và các file chương trình (các file ZIP và các file DOC). Việc truyền các file này dưới dạng một chuỗi các byte, kiểu dữ liệu này không quan tâm đến môi trường của máy đích và cấu trúc từ. Tất cả các cài đặt FTP nên hỗ trợ kiểu truyền dữ liệu này cũng như kiểu ASCII.
- Kiểu dữ liệu cục bộ. Kiểu dữ liệu này dựa trên byte, xác định cho các host cục bộ. Khuôn dạng phải khả dụng với các hệ thống khác để cấu trúc lại dữ liệu dựa vào dựa trên khuôn dạng ban đầu.

Kiểu dữ liệu ASCII và EBCDIC có thể có tham số tuỳ chọn thứ hai để xác định các ràng buộc dữ liệu. Khi được sử dụng, tham số này là một tuỳ chọn được thêm vào để xác định kiểu dữ liệu. Các ràng buộc định dạng phụ thuộc vào việc sử dụng của file được truyền. Liệu một file có thể được in, xem, hay được xử lí như một đầu vào. Việc định dạng một file có thể khác nhau ở mỗi đích. Các khuôn dạng dữ liệu sau được ít sử dụng hơn kiển dữ liệu ngầm định:

- Khuôn dạng không in: là kiểu dữ liệu ngầm định ASCII và EBCDIC. Khuôn dạng file này không có thông tin định dạng. Chú ý rằng, định dạng sử các dạng chuẩn cho kí tự cách và phân lề.
- Định dạng Telnet được sử dụng cho các file một thiết bị đầu cuối dùng để hiển thị. Định dạng này gồm các kí tự điều khiển, kí tự xuống dòng, tab.
- Kiểm soát di chuyển bao gồm các kí tự điều khiển định dạng in. Theo khuôn dạng này, kí tự đầu tiên của mỗi dòng không được in ra. Thay vào đó, kí tự này xác định sự di chuyển theo trục đứng so với mép giấy trước khi một bản ghi hay một dòng nào đó được in ra.

#### *10.7.2.5 Các cấu trúc dữ liệu*

Giao thức FTP cho phép truyền các file có cấu trúc với 3 cấu trúc file khác nhau. Các cấu trúc tập tin này chủ yếu dùng để truyền các tập tin giữa các hệ thống có cấu trúc lưu trữ khác nhau. Có các dạng như sau :

- Cấu trúc theo kiểu file, xem file một chuỗi các byte dữ liệu nối tiếp nhau mà không được cấu trúc bên trong.
- Cấu trúc bản ghi được sử dụng để truyền các file là một chuỗi các bản ghi. Cấu trúc này được sử dụng cho các Host IBM nhưng hiện nay ít sử dụng.
- Cấu trúc trang được sử dụng cho các file được chia thành các đối tượng với kích thước khác nhau, có thể có các thông tin khác được thêm vào trong đó. Cấu trúc trang có một cấu trúc header để định nghĩa kích thước của trang, theo sau là nội dung của trang. Header của mỗi trang còn chứa số hiệu trang logic của các trang dữ liệu nhưng số hiệu trang đó không cần thiết khi truyền.

### 10.7.3 UserNEWS

| Biểu tượng | Ý nghĩa | Biểu tượng | Ý nghĩa |
|---|---|---|---|
| :-) | Tôi hạnh phúc | =):=) | ABC Lincol |
| :-( | Tôi buồn/ tức giận | =):=) | Bác Sorn |
| :-\| | Tôi thờ ơ | *<:-) | ông già Noel |
| ;-) | Tôi nháy mắt | <:-( | Người tối dạ |
| ;-(0) | Tôi kêu la | (-: | Người Uực |
| :-(*) | Người nôn (mửa) | :-)x | Man with bowtic |
| :+) | Cằm chẻ | # -) | Tóc mướt |
| :-)) | Cằm chẻ | 8 -) | Mang kính |
| :-{) | Ria | C:-) | Mão lớn |

Khi mà có nhiều người thuê bao USENET, nhu cầu về những newsgroup mới, chuyên biệt hơn luôn được đòi hỏi. Kết quả là một thủ tục để tạo ra newsgroup mới, chuyên biệt hơn luôn được đòi hỏi. Kết quả là một thủ tục để tạo ra những

Newsgroup mới được. Trên Newsgroup, người ta có thể thảo luận, bầu cử, trao đổi với nhau.

### 10.7.4 WORLD-WIDE-WEB

World Wide Web (WWW) là một hệ thống quản lý thông tin phi cấu trúc. Bao gồm các Server cung cấp thông tin theo định dạng siêu văn bản (Hypertext) và các client (Browser, trình duyệt) nhận thông tin từ người sử dụng và đồng thời hiển thị thông tin mà các Server cung cấp theo định dạng được chỉ định bởi người sử dụng.

Thông tin trên WWW được biểu diễn trong các trang Web. Mỗi trang Web có thể là một chỉ mục hoặc một tài liệu chứa văn bản, hình ảnh, âm thanh, các liên kết... Người sử dụng có thể truy cập thông tin cần thiết trên WWW thông qua các đối tượng đã được đánh dấu trong tài liệu.

Các lệnh được dùng với WWW đã được định nghĩa trong giao thức HTTP (HyperText Transfer Protocol). Đây là giao thức chuẩn để liên lạc giữa Client và Server. Yêu cầu được gửi tới Server thông qua Client. Server xử lý các yêu cầu và gửi kết quả về cho Client  yêu cầu. Kết quả sẽ được trình bày dưới dạng thích hợp cho người sử dụng.

- Phía máy chủ

Mỗi web Site có một máy chủ đảm nhận việc “lắng nghe” TCP tại cổng 80 cho những kết nối đến từ các máy khách (thường là các trình duyệt). Sau khi một kết nối được thiết lập, máy khách gửi yêu cầu và máy chủ trả lời đáp lại, kết nối chấm dứt. Giao thức HTTP định nghĩa cho các yêu cầu và trả lời hợp lệ.

Ví dụ người dùng kích lên một mẫu văn bản hoặc có thể là biểu tượng trỏ đến trang có tên (tức là URL hay địa chỉ tới máy trạm Internet). Một URL có 3 phần sau: tên của giao thức (http), tên của máy nơi có chứa trang web, và tên của tập tin chứa trang đó (hypetext/WWW/TheProject.html). Từ khi người dùng nhấp chuột cho đến khi trang web được hiện ra trên màn hình đã xảy ra các sự kiện sau :

1. Trình duyệt kiểm tra URL (xem xét đối tượng được chọn là gì).
2. Trình duyệt hỏi DNS về địa chỉ IP của URL.
3. DNS trả lời là 18.23.0.23
4. Trình duyệt tạo một kết nối TCP đến cổng 80 trên địa chỉ 18.23.0.23
5. Trình duyệt gửi lệnh GET /hypetext/WWW/TheProject.html.
6. Máy chủ  gửi đến tập tin TheProject.html
7. Giải phóng kết nối TCP.

8. Trình duyệt hiển thị tất cả các văn bản trong tập tin TheProject.html.
9. Trình duyệt tiếp tục lấy về và hiển thị tất cả các hình ảnh có trong TheProject.html.

#### *10.7.4.1 Ngôn ngữ HTML*

HTML (HyperText Markup Laguage) là một ngôn ngữ HTML là một ngôn ngữ có cấu trúc, nó bao gồm các thẻ (TAGS) và các thực thể (ENTITY), dùng để cung cấp các chỉ thị định dạng để phục vụ cho việc trình bày văn bản trên Web.

Một tập tin HTML là một tập tin văn bản trong đó một số xâu ký tự được coi là các thẻ đánh dấu các vùng tài liệu và ấn định các ý nghĩa đặc biệt cho chúng. Các thẻ là các xâu ký tự được bắt đầu là dấu nhỏ hơn (<) và kết thúc bằng dấu lớn hơn (>). Các thẻ có thể được phân làm nhiều loại tùy theo nội dung, chức năng, kiểu tác động của chúng như: Thẻ mô tả định dạng, thẻ mô tả cấu trúc, thẻ rỗng, thẻ chứa...

Cấu trúc tổng quát của một tài liệu HTML như sau :

<HTML> *Thông báo cho trình duyệt đây là một văn bản tài liệu HTML*
<HEAD> *Thông báo bắt đầu phần đầu của tài liệu*
<TITLE> *Tiêu đề của tài liệu* </TITLE>
Phần đầu của tài liệu đặt tại đây
</HEAD> *Kết thúc phần đầu*
<BODY> *Thông báo bắt đầu phần thân tài liệu*
.....
Nội dung tài liệu HTML được đặt tại đây
</BODY> *Kết thúc phần thân tài liệu*
</HTML> *Kết thúc tài liệu HTML*

Phần đầu đề của tài liệu HTML thường chứa tiêu đề của tài liệu, tên tác giả, lời chú thích, tóm tắt... Đây là phần giúp ích cho việc tìm kiếm thông tin trên WEB hoặc cho các dịch vụ tìm kiếm có thể đánh chỉ mục, tiến hành tìm kiếm một cách dễ dàng. Một số các thẻ phục vụ trong phần đầu như: Title, Meta, Isindex...

Phần thân là phần chính của tài liệu HTML, nằm giữa cặp thẻ <BODY> và </BODY>, nó định nghĩa, hiển thị toàn bộ nội dung bên trong của tài liệu. Trong phần thân ta có thể sử dụng các thẻ để định dạng văn bản, chèn các hình ảnh, bảng biểu, liên kết...

Người sử dụng có thể tạo một tài liệu HTML bằng cách sử dụng các trình soạn thảo Web chuyên dụng như Microsoft Front Page 2000, hoặc Microsoft Word, Notepad ...

Một số thẻ HTML quan trọng :

### 1. *Thẻ <!-- (chú thích) -->:*

Dùng để thêm những dòng chú thích trong file HTML, người ta dùng thẻ nầy. Nội dung văn bản nằm giữa <!-- và --> sẽ được chương trình Browse bỏ qua. Cho phép có khoảnh trắng giữa -- và >, nhưng không được có khoảng trắng giữa <! và -- .

Thí dụ:

<HEAD> <TITLE>The HTML Reference</TITLE>

<!-- Created by Nguyen Tan Khoi, April 1996 --> </HEAD>

### 2. *Thẻ <A>*

Dùng để tạo các siêu liên kết (HyperLink). WWW cho phép kết nối và giao tiếp giữa các tài nguyên một cách dễ dàng nhờ định nghĩa các loại liên kết sau:

1. Liên kết giữa các thành phần khác nhau trong một tài liệu HTML.
2. Liên kết giữa các tài liệu HTML khác nhau.
3. Liên kết với các dạng tài liệu Multimedia.
4. Truy cập tới các dịch vụ thông tin khác trên mạng Intranet/Internet

Các thuộc tính của thẻ <A> như sau:

*a. Liên kết đến điểm neo trong trang HTML*

- NAME: Thuộc tính NAME xác định một vị trí để những thành phần khác trong tài liệu hoặc trong tài liệu khác có thể tham trỏ đến (gọi là điểm neo trong tài liệu HTML). Thí dụ :

  <A NAME="coffee"> Coffee</A>

  Các tài liệu khác có thể liên kết với tài liệu này ngay tại vị trí xác định.

*b. Liên kết đến một trang HTML*

<A HREF = "URL_HTML[#Name_Anchor]"> *Nội dung thông báo* </A>

Trong đó URL_HTML là địa chỉ để tham chiếu tới tài liệu HTML.

Nếu chỉ ra Name_Anchor thì có nghĩa ta định nghĩa một điểm neo dùng để chuyển đến một vị trí được quy định sẵn trong tài liệu HTML này. Thí dụ:

The <A HREF="document.html#glossary"> GLOSSARY </A>

Trong thí dụ trên, nếu kích vào "GLOSSARY" sẽ được chuyển đến tài liệu document.html, ngay tại vị trí điểm neo có tên glossary trong tài liệu này.

c. *Liên kết với các kiểu dữ liệu khác nhau*

Để liên kết giữa tài liệu hiện thời với các kiểu dữ liệu khác nhau như: hình ảnh, âm thanh, video...

<A HREF ="URL_DATA"> ...</A>

Trong đó URL_DATA là địa chỉ tới kiểu dữ liệu cần liên kết. Ví dụ:

<A HREF ="car.jpg">

<IMG SRC ="carla.gif" WIDTH=87 HEIGHT=60> </A>

d. *Liên kết với các dịch vụ thông tin khác trên mạng*

<A HREF = "URL_Service" > ... </A>

Trong đó URL_Service là một địa chỉ đến các dịch vụ trên internet.

<A HREF="http://..."> Liên kết với 1 Web Site.

<A HREF="ftp://..."> Với 1 Ftp Site.

<A HREF="gopher://..."> Với 1 Gopher server.

<A HREF="news:..."> Liên kết với 1 nhóm Tin.

<A HREF="mailto:..."> liên kết tới 1 địa chỉ gởi Mail. Liên kết nầy sẽ kích hoạt chương trình Mail và tự động điền địa chỉ vào mục To dùm bạn. Bạn có thể khai báo luôn cả chủ đề thư (?subject).

Thí dụ: <A HREF="mailto:cmlehunt@swan.ac.uk?

subject=The HTMLib is fantastic">link text</A>

- TARGET: Chương trình Browser có thể nạp đối tượng liên kết vào 1 cửa sổ chỉ định bằng thẻ nầy. Nếu cửa sổ nầy cha có, trình Browse sẽ mở 1 cửa sổ mới. Chủ yếu thẻ nầy dùng cho frames.

  Dạng chung:

  <A HREF="url.html" TARGET="window_name">Link text</A>

  Trong đó window_name là tên đặt cho Frame.

  Khi kích chuột vào dòng "Link text", trang "url.html" sẽ được nạp vào frame có tên chỉ định.

Ngoài ra ta còn có thể chèn thêm các Script sau vào thẻ <A> dựa vào các phương thức như sau :

| Phương thức | Giải thích |
|---|---|
| OnMouseOver | Khi bạn di chuyển Mouse đến liên kết, sẽ có 1 dòng văn bản mô tả xuất hiện trong thanh trạng thái của trình Browse. Thí dụ:<br><A HREF="index.html"<br>OnMouseOver="self.status=('Back to the main page')">Link text</A><br>Dòng chữ "Back to the main page" sẽ hiện trong thanh trạng thái khi dời Mouse đến chữ "Link text". |
| OnMouseOut | Tương tự như trên nhưng dòng chữ nầy lại xuất hiện khi kéo Mouse ra khỏi liên kết. Thí dụ:<br><A HREF="index.html"<br>OnMouseOut="alert('Oh please go to this document')">Link text</A> |
| OnClick | Khi bấm Mouse lên liên kết, sẽ xuất hiện hộp thoại yêu cầu xác nhận. Thí dụ:<br><A HREF="http://www.netscape.com/"<br>OnClick="confirm('Are you want to go to the Netscape site?')">Link text</A> |

### 3. *Thẻ <INPUT>*

Dùng để tạo một field để nhận tác động của người sử dụng.

<INPUT TYPE = "*Kiểu*" NAMQ = "*TênĐT*"
SIZQ = "*KíchThước*"
VALUQ = "*Giatri*" MAXLQNGTH = "n" . . . >

Các thuộc tính:

| Thuộc tính | Giải thích |
|---|---|
| ALIGN | So hàng cho field. |
| CHECKED | Kiểm tra người dùng đã đánh dấu cho checkbox hay radio button chưa. |
| MAXLENGTH | Chỉ định độ dài ký tự có thể nhập vào text field, độ dài nầy có thể lớn hơn kích thước Text field. Mặc định là không giới hạn. |

| | |
|---|---|
| NAME | Tên của Field. |
| SIZE | Khai báo kích thước hay số lượng ký tự cho field. |

- TYPE: Chỉ định kiểu của Field:

| Giá trị | Giải thích |
|---|---|
| BUTTON | Chèn một nút bấm vào tài liệu. Giá trị VALUE dùng chỉ định Text sẽ hiện trong nút nầy. Thí dụ:<br><input type="button" value="hello" name="btnhello"> |
| HIDDEN | Với thuộc tính nầy, field sẽ không hiển thị ra nhưng nội dung của field vẫn có giá trị. Dùng trao đổi thông tin ngầm giữa Client/Server. |
| PASSWORD | Giống như Text, nhưng ký tự nhập vào sẽ không hiển thị ra. |
| CHECKBOX | Chèn 1 chechbox vào tài liệu. Thí dụ :<br> So thich<br><input type="checkbox" name="C1" value="ĂN">The thao<br><input type="checkbox" name="C2" value="ĂN">Xem phim |
| RADIO | Chèn 1 field có dạng nút Radio. Ví dụ :<br> Gioi tinh<br><input type="radio" checked value="V1" name="R1">Nam<br><input type="radio" name="R2" value="V2">Nu |
| RESET | Chèn 1 nút bấm dùng phục hồi lại tình trạng cũ cho các field. Đặt tên của nút nầy qua thuộc tính Values. |
| SUBMIT | Một dạng nút bấm giống RỌSỌT. Có tác dụng giống nh xác nhận đồng ý. Thí dụ:<br> <input type="submit" value="Submit" name="B1"><br><input type="reset" value="Reset" name="B2"> <br>Chèn 1 nút có tên "SUBMIT" và sẽ hiển thị thông báo "Xin chao các bạn" khi người sử dụng Mouse vào nút nầy :<br><INPUT TYPE="SUBMIT" OnClick="Xin chao các bạn'"> |
| TEXT | Nhập 1 dòng text vào fields. Dùng thuộc tính SIZỌ và MAXLENGTH để quy định kích thước. Trong trường hợp cần nhập |

| | |
|---|---|
| | nhiều dòng, phải dùng thẻ <TEXTAREA>. |
| VALUE | Chỉ định Text sẽ hiển thị trên các nút bấm. |
| IMAGE | Chèn field chứa hình ảnh để người dùng bấm Mouse khi chọn.<br><INPUT TYPE="IMAGE" SRC="../ iexplore.gif" ALIGN="middle"> |

### 4. *Thẻ TEXTAREA*

Cho phép nhập nhiều dòng văn bản vào một hộp Text.

Thí dụ:

```
<TEXTAREA
NAME="descr"
COLS="30"          ROWS="3"
OnBlur="count_char(document.egForm.descr.value)">Enter a short description here
 </TEXTAREA>
```

Ví dụ : <textarea name="Ghichu" rows="2" cols="20"></textarea>

### 5. *Thẻ FORM*

Forms là một thiết lập nhỏ trong HTML, nó cho phép người sử dụng đưa vào các thông tin. Giao diện Forms tạo nên sự thuận lợi trong việc tương tác giữa người sử dụng và các dịch vụ. Trên Form ta có thể tạo các thành phần như các nút lệnh, các trường văn bản (Text) hay các danh sách lựa chọn ... Khi forms được hoàn thành bởi người sử dụng, Client sẽ gửi thông tin đến Server, Server sẽ thực thi các chương trình kết hợp với form và các tham số là các thông tin nhận từ Form.

Thông thường các Form sử dụng cho hai mục đích chính:

- Dùng để thu thập thông tin từ người sử dụng.
- Là trung gian để tương tác qua lại giữa người sử dụng và hệ thống.

Cú pháp : <Form ACTION = “Action” METHOD="PhuongThuc">

**Action**: là một URL hoặc một Script mà khi nút ***Submit*** được nhấn nó sẽ thực thi.

**Method=**GET/POST : Xác định kiểu yêu cầu mà trình duyệt gởi đến cho Server.

- METHOD = GET: trình duyệt sẽ bổ sung dữ liệu đầu vào dưới dạng một biến môi trường là CGI_QueryString.
- METHOD=POST: Forrn dữ liệu đầu vào sẽ đợi từ các thiết bị nhập của Server cùng với một số dữ liệu được lưu trữ trong biến môi trường CGI_ContentLength.

**EncType:** cung cấp kiểu Mime của tập được dùng như đầu vào trong các biểu mẫu.

Ví dụ : <Form ACTION = METHOD="GET">

### 6. *Thẻ TABLE*

- Dùng để tạo ra một bảng. Bảng được tạo thành từ các hàng, trên mỗi hàng có các ô (cell).

```
<TABLE>
        <TABLE   BORDER = “n” . . . >
        <TR>
                <TD>  . . . </TD> <TD>  . . . </TD> <TD>  . . . </TD>
        </TR>
        . . . .
        <TR>
                <TD>  . . . </TD> <TD>  . . . </TD> <TD>  . . . </TD>
        </TR>
</TABLE>
```

### 7. *Thẻ SELECT*

- Hiển thị hộp ComboBox cho phép chọn lựa một trong nhiều giá trị :

```
<SELECT  NAME =”TenĐT”>
        <OPTION SELECTED VALUE =”Gia trị 1”> Nội dung 1
        <OPTION SELECT VALUE =”Gia trị 2”> Nội dung 2
                . . .
</SELECT>
```

*Ví dụ :*

```
<p>Que quan <select size="1" name="cboQuequan">
        <option selected>Da Nang</option>
        <option>Hue</option>
        <option>Ha Noi</option>
        </select></p>
```

### 8. *Thẻ <APPLET>*

Dùng để chèn Applet Java vào trang Web. Có dạng tổng quát sau:

```
<APPLET
    [CODEBASE = URL] [CODE = appletFile]
    [NAME = appletInstanceName]:
    [ARCHIVE = compressed file] [ALT = alternateText]
    [WIDTH = pixels]  [HEIGHT = pixels]  [ALIGN = alignment]
    [VSPACE = pixels] [HSPACE = pixels]
    [ARCHIVE = URL to archive]
 </APPLET>
```

Trong đó :

| Tham số | Giải thích |
|---|---|
| CODEBASE=URL | Chỉ định địa chỉ tuyệt đối của Applet. |
| CODE=appletFile | Chỉ định địa chỉ tương đối của Applet. |
| ALT=alternateText | Chỉ định dòng text sẽ hiển thị trong trường hợp trình Browse không hiểu Applet. |
| NAME = appletInstanceName | Đặt tên cho Applet để phục vụ cho việc tìm kiếm. |
| WIDTH=pixels HEIGHT=pixels | Chỉ định kích thước cho Applet. |
| ALIGN=alignment | Dùng canh lề, có các giá trị sau: LEFT, RIGHT, TOP, TEXTTOP, MIDDLE, ABSMIDDLE, BASELINE, BOTTOM, ABSBOTTOM. |
| VSPACE=pixels HSPACE=pixels | Chỉ định khoảng trống bao chung quanh Applet. |
| ARCHIVE=compressed file | Khai báo các file nén cần thiết của Applet để trình Browse tải về máy cá nhân, phục vụ cho việc đọc lại sau nầy. |

Ví dụ:

```
<APPLET CODEBASE=http://200.201.202.180/applets/ NervousText
CODE="NervousText.class"
WIDTH=400      HEIGHT=75
ALIGN=CENTER>
<PARAM NAME="text" VALUE="This is the Applet Viewer.">
</APPLET>
```

Chỉ thị cho trình Browse nạp Applet ở địa chỉ htttp://java.sun.com/JDK-prebeta1/applets/NervousText/NervousText.class". Chỉ định kích thước là 400x75 pixels và canh giữa dòng. Nếu trình Browse hiểu Applet, dòng "This is the Applet Viewer." sẽ hiển thị và Applet tạo hiệu ứng cho dòng chữ nầy. Nếu trình Browse không hiểu Applet, nó sẽ bỏ qua nội dung của <APPLET> cũng như <PARAM> và chỉ hiển thị nội dung của <BLOCKQUOTE>

9. ***Thẻ <IMG>***

Dùng để chèn 1 file hình vào tài liệu HTML

Các thuộc tính :

- ALIGN="left/right/top/texttop/middle/absmiddle/baseline/bottom/absbotto": So hàng hình ảnh với Text.
- ALT="Alternative Text": Cho hiển thị 1 dòng text thay thế cho file hình trong trường hợp trình Browse đang ở trong chế độ không hiển thị hình ảnh. Dòng Text nầy cũng hiển thị theo dạng ToolTip khi dời chuột đến hình.

Ví dụ: <IMG SRC="triangle.gif" ALT="Warning:"> Read these instructions.

- SRC="URL of image": Chỉ định đia chỉ file hình chèn vào trang Web.

Ví dụ : <IMG SRC="warning.gif">Be sure to read these instructions.

- WIDTH=value/ HEIGHT=value: Chỉ định khoảng cách dành sẳn cho hình trong khi trình Browse nạp toàn bộ hình.
- BORDER=value: Chỉ định cho hiển thị đường viền bao quanh hình ảnh. Ta có thể chọn "0" để hiển thị đường viền màu xanh khi có liên kết.
- VSPACE=value HSPACE=value: Quy định khoảng trống giữa hình và Text. VSPACE cho trên và dới hình, HSPACE cho trái và phải hình. Value tính theo pixel.
- LOWSRC: Thuộc tính nầy cho phép hiển thị 2 hình lần lượt trong cùng 1 vị trí. Thường dùng để nạp một hình nhỏ trong khi chờ đợi nạp hình chính có dung luợng file lớn hơn:

Ví dụ: <IMG SRC="hiquality.gif" LOWSRC="lowquality.gif">

Đầu tiên trình Browse sẽ hiển thị file hình "lowquality.gif". Sau khi nạp hoàn tất cả trang, trình duyệt sẽ nạp file hình chính thức vào thay thế.

### *10.7.4.2 Chỉ định tài nguyên trong URL*

Để chỉ định vị trí của tài nguyên HTTP dùng URL (Uniform Resouce Locators) đó là tên quy ước để nhận diện một cách duy nhất vị trí của một thư mục

hoặc một tập tin trên Intranet/Internet. Trong URL cũng chỉ định giao thức kết nối như HTTP, GOPHER... cần thiết cho việc tìm kiếm và lấy tài nguyên. Nếu ta biết URL của một tài nguyên ta có thể truy xuất nó một cách trực tiếp hoặc thông qua các siêu liên kết trong các tài liệu.

URL sử dụng một dòng đơn các ký tự ASCII. Sơ đồ này bao gồm các giao thức trên Intranet/Internet như FTP, Gopher, http... URL là một trong những công cụ cơ sở của WWW và được dùng trong các tài liệu HTML để tham chiếu đến các tài nguyên trên mạng.

Một URL gồm các thông tin sau :

a. Tên các giao thức khi truy cập Server (như HTTP, Gopher, Wais...).

b. Tên miền của Server thực thi, theo bất cứ thông tin về user và password của site trên Intranet/Internet.

c. Số cổng mà server sử dụng. Nếu điều này không được chỉ rõ trình duyệt sẽ dùng số cổng mặc định trong giao thức (cổng 80).

d. Định vị của tài nguyên trong kiến trúc phân cấp của Server.

#### *10.7.4.3 Giao thức HTTP*

Giao thức HTTP (Hyper Text Transfer Protocol - Giao thức truyền siêu văn bản) sử dụng cho các dịch vụ truyền thông đa phương tiện WWW, dựa trên mô hình Client/Server. Dịch vụ WWW cho phép NSD kết hợp văn bản, âm thanh, hình ảnh, hoạt hình tạo nên nguồn thông tin tư liệu. Đặc biệt ở đây là thông tin tư liệu trong WWW có dạng HyperText - là dạng tư liệu chuẩn trong WWW. Giao thức cho phép lấy và đọc nhanh các tư liệu đó. HTTP là giao thức truyền thông nhưng có thêm ưu điểm là thông tin tư liệu cần truy cập lại có chứa các liên kết tới cá tư liệu khác nằm khắp nơi trên mạng Internet.

Phần mềm cho WWW Server là một chương trình điều khiển sự thu nhập các tư liệu WWW trên một máy chủ. Để truy cập WWW, cần thiết phải chạy hệ thống ứng dụng WWW là một trình duyệt (browser) trên máy của WWW Client.

HTTP là một giao thức Internet Client/Server, được thiết kế để truyền các dạng dữ liệu  siêu văn bản. HTTP là một giao thức không trạng thái, nghĩa là khi Server đáp ứng dữ liệu được yêu cầu bởi Client xong thì server huỷ bỏ kết nối đó không tốn bộ nhớ cho sự kiện. Không trạng thái là yếu tố làm cho tốc độ truyền dẫn giữa HTTP Server và HTTP Client rất nhanh.

Các giao tiếp HTTP truyền dữ liệu dưới dạng các ký tự 8 bit hay một octet. Điều này đảm bảo truyền dẫn an toàn mọi dạng dữ liệu bao gồm hình ảnh, âm thanh, các tài liệu HTML hay các chương trình khả thi.

### 1. *Các giai đoạn kết nối của HTTP*

Một HTTP Server kết nối thông qua 4 giai đoạn:

- ***Mở kết nối:*** Client tiếp xúc với Server tại địa chỉ internet và số cổng chỉ định trong URL (cổng mặc định là 80)
- ***Tạo yêu cầu :*** Client gửi một thông điệp tới Server yêu cầu dịch vụ. Yêu cầu bao gồm các tiêu đề HTTP, nó định nghĩa phương thức được yêu cầu cho tác vụ và cung cấp thông tin về khả năng của Client (được theo sau dữ liệu gửi tới Server). Các phương thức HTTP điển hình là GET để nhận các đối tượng từ Server hoặc POST để chuyển dữ liệu cho đối tượng (ví dụ như các chương trình GateWay) trên Server.
- ***Gửi đáp ứng :*** Server trả lời cho Client bao gồm các tiêu đề để trả lời trạng mô tả trạng thái của tác vụ (ví dụ thành công, không thành công...) theo sau dữ liệu thật sự.
- ***Đóng kết nối:*** Kết nối được đóng, Server không giữ lại dấu vết của tác vụ đã hoàn thành. Thủ tục này có nghĩa là mỗi kết nối chỉ xử lý một tác vụ và do đó chỉ có thể tải xuống Client chỉ một tệp dữ liệu. Tính chất không trạng thái của tác vụ cũng có nghĩa là mỗi kết nối không hề biết về các kết nối trước đó.

### 2. *Các phương thức của giao thức HTTP*

| Phương thức | Giải thích |
|---|---|
| GET | Lấy dữ liệu hiển thị trong URL. Dữ liệu cũng có thể gửi trong URL thông qua một chuỗi truy vấn. Đây cũng là nơi dữ liệu gửi từ ISINDEX hoặc Form với thuộc tính METHOD="GET" |
| HEAD | Lấy thông tin của HTTP, Header chỉ định trong URL. |
| POST | Gửi dữ liệu đến cho URL nếu URL là tồn tại. Phương thức này được dùng bởi những thành phần của Form trong HTML với giá trị thuộc tính METHOD="POST". |
| PUT | Là nơi mà dữ liệu gửi bởi Client biểu thị trong URL, nó sẽ thay thế nội dung của URL đã có. |
| DELETE | Xóa tài nguyên cục bộ tại nơi được chỉ định bởi URL. |
| LINK | Liên kết một đối tượng đã tồn tại với một đối tượng khác. |
| UNLINK | Huỷ bỏ một liên kết đã được tạo bởi phương thức LINK. |

# BÀI TẬP

1. Những nguyên tắc cơ bản giám sát và quản trị hệ thống mạng máy tính
2. Khảo sát cấu trúc và hoạt động dịch vụ DNS
3. Khảo sát cấu trúc và hoạt động của giao thức SNMP
4. Khảo sát cấu trúc và hoạt động của giao thức HTTP
5. Tìm hiểu giao thức DHCP.

- - - - - - - - - - - - - - - - - - - - - - - - -

# TÀI LIỆU THAM KHẢO

**Tiếng Việt**

[1] Nguyễn Thúc Hải, ***Mạng máy tính và các hệ thống mở*** , NXB Giáo dục, 1997

[2] Lê Văn Sơn, ***Giáo trình mạng máy tính***, Trường ĐH Bách Khoa Đà Nẵng, 1998

[3] Nguyễn Hồng Sơn, ***Giáo trình hệ thống mạng máy tính CCNA,*** Nhà XB Lao động, 2002

**Tiếng Anh**

[4] Douglas E.Comer, ***Computer Networks and Internets***, Prentice Hall, 1997

[5] Ed Taylor, ***TCP/IP complete***, McGraw-Hill, 1998

[6] Microsoft Press, ***Networking Essentials***

[7] Stallings W., ***Data and Computer Communications***, Macmillan Publishing, 1995

[8] Tanenbaum Andrew S., ***Computer*** **Networks,** Prentice Hall, 1997

[9] Pujolle, ***Les rĐseaux***, EYROLLES, 2003

***@2004, Nguyễn Tấn Khôi***

**Khoa Công Nghệ Thông Tin - Trường Đại học Bách Khoa Đà Nẵng**

----------o & o----------

# Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin
# Giáo Trình Mạng Máy Tính – V1.0

Chương 1: Tổng quan về mạng máy tính
Mục đích
Chương này nhằm giới thiệu cho người học những nội dung sau: • Các loại mạng truyền dữ liệu đã tồn tại trước khi của mạng máy tính ra đời. • Cấu trúc tổng quát của một mạng máy tính. • Hai chế độ truyền tải dữ liệu cơ bản là Chuyển mạch và Chuyển gói. • Những lợi ích mà mạng máy tính mang lại.

Yêu cầu
Sau khi học xong chương này, người học phải có được những khả năng sau: Phân biệt được hai loại mạng Chuyển mạch và Chuyển gói; Định nghĩa được mạng máy tính là gì và trình bày được cấu trúc tổng quát của một mạng máy tính. Nêu lên được những lợi ích mà mạng máy tính mang lại.

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

1

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

1.1 Mạng điện báo
Mạng điện báo sử dụng hệ thống mã Morse để mã hóa thông tin cần truyền đi. Mã Morse sử dụng hai tín hiệu là tít và te (ký hiệu bằng dấu chấm (•) và dấu gạch ngang (-)). Mỗi một ký tự latin sẽ được mã hóa bằng một chuỗi tíc/te riêng biệt, có độ dài ngắn khác nhau. Để truyền thông tin đi, bên gởi sẽ lần lượt mã hóa từng ký tự của thông điệp thành mã Morse, bên nhận sau đó sẽ thực hiện quá trình giải mã. Văn bản được truyền đi được gọi là một thông điệp (message) hay một thư tín (Telegram). Vào năm 1851 mạng thư tín đầu tiên được sử dụng để nối hai thành phố London và Paris. Sau đó không lâu, hệ thống mạng này được mở rộng toàn châu Âu. Cấu trúc của mạng gồm có hai thành phần là Trạm điện báo (Telegraph Station) và Trạm chuyển điện báo ( Telegraph Switching Station) được nối lại với nhau bằng hệ thống dây truyền dẫn. Trạm điện báo là nơi cho phép truyền và nhận các thông điệp dưới dạng các mã Morse, thông thường được thể hiện bằng âm thanh tít và te. Để truyền và nhận thông tin cần có một điện báo viên thực hiện quá trình mã hóa và giải mã thông tin truyền/nhận. Vì không thể nối trức tiếp tất cả các trạm điện báo lại với nhau, người ta sử dụng các Trạm chuyển điện báo để cho phép nhiều trạm điện báo sử dụng chung một đường truyền để truyền tin. Tại mỗi trạm chuyển điện báo có một thao tác viên chịu trách nhiệm nhận các điện báo gởi đến, xác định đường đi để chuyển tiếp điện báo về nơi nhận. Nếu đường truyền hướng về nơi nhận đang được sử dụng để truyền một điện báo khác, thao tác viên sẽ lưu lại điện báo này để sau đó truyền đi khi đường truyền rãnh. Để tăng tốc độ truyền tin, hệ thống Baudot thay thế mã Morse bằng mã nhị phân 5 bits (có thể mã hóa cho 32 ký tự). Các trạm điện báo cũng được thay thế bằng các máy têlêtíp (teletype terminal) cho phép xuất / nhập thông tin dạng ký tự. Hệ thống sử dụng kỹ thuật biến điệu (Modulation) và đa hợp (Multiplexing) để truyền tải thông tin.

1.2 Mạng điện thoại
Mạng điện thoại cho phép truyền thông tin dưới dạng A âm thanh bằng cách sử dụng hệ thống truyền tín hiệu tuần tự. Mạng điện thoại hoạt động H1.1 Mạng chuyển mạch theo chế độ chuyển mạch định hướng nối kết (circuit switching), tức thiết lập đường nối kết tận hiến giữa hai bên giao tiếp trước M¸ y chĩ khi thông tin được truyền đi (connection oriented). (Host)

B

1.3 Mạng hướng đầu cuối
Đây là mô hình của các hệ thống máy tính lớn (Main Frame) vào những năm của thập niên 1970. Hệ thống gồm một máy chủ mạnh (Host) có năng lực tính toán cao được nối kết với nhiều thiết bị đầu cuối đần độn (Dumb terminal) chỉ làm nhiệm vụ xuất nhập thông tin, giao tiếp với người sử dụng.

Thiết bị đầu cuối (Dumb Terminal)

ThiÕ bÞ® u cuèi t bÞ® Ç (Dumb Terminal) H1.2 Mạng hướng đầu cuối

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

2

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

1.4 Mạng máy tính
Mạng máy tính là mạng của hai hay nhiều máy tính được nối lại với nhau bằng một đường truyền vật lý theo một kiến trúc nào đó. Mạng có thể có kiến trúc đơn giản như hình dưới đây:

H1.3 Mạng cục bộ đơn giản

Hoặc phức tạp hơn đó là hệ thống gồm nhiều mạng đơn giản nối lại với nhau như hình sau: Một hệ thống mạng tổng quát được cấu thành từ 3 thành phần: Đường biên mạng ( Network Edge): Gồm các máy tính (Host) và các chương trình ứng dụng mạng (Network Application) Đường trục mạng ( Network Core): Gồm các bộ chọn đường (router) đóng vài trò là một mạng trung tâm nối kết các mạng lại với nhau. Mạng truy cập, đường truyền vật lý (Access Network , physical media): Gồm các đường truyền tải thông tin.

H1.4 Mạng diện rộng phức tạp

1.4.1 Đường biên mạng
Bao gồm các máy tính (Host) trên mạng nơi thực thi các chương trình ứng dụng mạng (Network Application). Đôi khi người ta còn gọi chúng là các Hệ thống cuối (End Systems) với ý nghĩa đây chính là nơi xuất phát của thông tin di chuyển trên mạng, cũng như là điểm dừng của thông tin. Quá trình trao đổi thông tin giữa hai máy tính trên mạng có thể diễn ra theo hai mô hình: Mô hình Khách hàng / Người phục vụ (Client / server model) hay Mô hình ngang hàng (peer-to-peer model).
H1.5 Đường biên mạng

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

3

1.4.1.1 Mô hình khách hàng/người phục vụ (client/server):
Trong mô hình này một máy tính sẽ đóng vai trò là client và máy tính kia đóng vai trò là server. Máy tính client sẽ gởi các yêu cầu (request) đến máy tính server để yêu cầu server thực hiện công việc gì đó. Chẳng hạn khi người dùng duyệt web trên mạng Internet, trình duyệt web sẽ gởi yêu cầu đến web server đề nghị web server gởi về trang web tương ứng. Máy tính server khi nhận được một yêu cầu từ client gởi đến sẽ phân tích yêu cầu để hiểu được client muốn đều gì, để thực hiện đúng yêu cầu của client. Server sẽ gởi kết quả về cho client trong các thông điệp trả lời (reply). Ví dụ, khi web server nhận được một yêu cầu gởi đến từ trình duyệt web, nó sẽ phân tích yêu cầu để xác định xem client cần nhận trang web nào, sau đó mở tập tin html tương ứng trên đĩa cứng cục bộ của nó để gởi về trình duyệt web trong thông điệp trả lời. Một số ứng dụng được xây dựng theo mô hình client / server như: www, mail, ftp,...

1.4.1.2 Mô hình ngang cấp (peer-to-peer):
Trong mô hình này, một máy tính vừa đóng vai trò là client, vừa đóng vai trò là server. Một số ứng dụng thuộc mô hình này như: Gnutella, KaZaA

1.4.2 Đường trục mạng
Là hệ thống mạng của các bộ chọn đường (routers), làm nhiệm vụ chọn đường và chuyển tiếp thông tin, đảm bảo sự trao đổi thông tin thông suốt giữa hai máy tính nằm trên hai nhánh mạng cách xa nhau. Câu hỏi đặt ra là làm sao thông tin có thể được truyền đi trên mạng? Người ta có thể sử dụng một trong hai chế độ truyền tải thông tin là: Chuyển mạch (circuit switching) và chuyển gói (packet switching).

H1.6 Mạng đường trục

1.4.2.1 Chuyển mạch (circuit switching)
Chế độ này hoạt động theo mô hình của hệ thống điện thoại. Để có thể giao tiếp với máy B, máy A phải thực hiện một cuộc gọi (call). Nếu máy B chấp nhận cuộc gọi, một kênh ảo được thiết lập dành riêng cho thông tin trao đổi giữa A và B. Tất cả các tài nguyên được cấp cho cuộc gọi này như băng thông đường truyền, khả năng của các bộ hoán chuyển thông tin đều được dành riêng cho cuộc gọi, không chia sẻ cho các cuộc gọi khác, mặc dù có những khoảng lớn thời gian hai bên giao tiếp “im lặng”. Tài nguyên (băng thông) sẽ được chia thành nhiều những “phần” bằng nhau và sẽ gán cho các cuộc gọi. Khi cuộc gọi sở hữu một “phần” tài nguyên nào đó, mặc dù không sử

H1.7 Mạng chuyển mạch

dụng đến nó cũng không chia sẻ tài nguyên này cho các cuộc gọi khác. Việc phân chia băng thông của kênh truyền thành những “phần” có thể được thực hiện bằng một trong hai kỹ thuật: Phân chia theo tần số (FDMA-Frequency Division Multi Access) hay phân chia theo thời gian (TDMA- Time Division Multi Access).

4

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

1.4.2.2 Mạng chuyển gói
A

statistical multiplexing Trong phương pháp này, thông tin trao đổi giữa hai máy tính (end systems) được phân thành những 1.5 Mbs B gói tin (packet) có kích thước tối queue of packets đa xác định. 45 Mbs waiting for output Gói tin của những người dùng link khác nhau ( ví dụ của A và B) sẽ chia sẻ nhau băng thông của kênh D truyền. Mỗi gói tin sẽ sử dụng E toàn bộ băng thông của kênh H1.8 Mạng chuyển gói truyền khi nó được phép. Điều này sẽ dẫn đến tình trạng lượng thông tin cần truyền đi vượt quá khả năng đáp ứng của kênh truyền. Trong trường hợp này, các router sẽ ứng sử theo giải thuật lưu và chuyển tiếp (store and forward), tức lưu lại các gói tin chưa gởi đi được vào hàng đợi chờ cho đến khi kênh truyền rãnh sẽ lần lượt gởi chúng đi.

10 Mbs Ethernet

C

1.4.2.3 So sánh mạng chuyển mạch và mạng chuyển gói
Chuyển gói cho phép có nhiều người sử dụng mạng hơn: Giả sử: Một đường truyền 1 Mbit Mỗi người dùng được cấp 100Kbps khi truy N users cập “active” Thời gian active chiếm 10% tổng thời gian. 1 Mbps link Khi đó: circuit-switching: cho phép tối đa 10 users H1.9 Chia sẻ đường truyền trong packet switching: cho phép 35 users, (xác suất mạng chuyển gói có hơn 10 “active” đồng thời là nhỏ hơn 0.004) Chuyển gói: Thích hợp cho lượng lưu thông dữ liệu lớn nhờ cơ chế chia sẻ tài nguyên và không cần thiết lập cuộc. Cần có cơ chế điều khiển tắt nghẽn và mất dữ liệu. Không hỗ trợ được cơ chế chuyển mạch để đảm bảo tăng băng thông cố định cho một số ứng dụng về âm thanh và hình ảnh.

1.4.2.4 Mạng truy cập
Cho phép nối các máy tính vào các router ngoài biên. Nó có thể là những loại mạng sau: Mạng truy cập từ nhà, ví dụ như sử dụng hình thức modem dial qua đường điện thoại hay đường ADSL. Mạng cục bộ cho các công ty, xí nghiệp. Mạng không dây.

H1.10 Mạng truy cập

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

5

1.4.3 Các lợi ích của mạng máy tính

1.4.3.1 Mạng tạo khả năng dùng chung tài nguyên cho các người dùng.

Vấn đề là làm cho các tài nguyên trên mạng như chương trình, dữ liệu và thiết bị, đặc biệt là các thiết bị đắt tiền, có thể sẵn dùng cho mọi người trên mạng mà không cần quan tâm đến vị trí thực của tài nguyên và người dùng. Về mặt thiết bị, các thiết bị chất lượng cao thường đắt tiền, chúng thường được dùng chung cho nhiều người nhằm giảm chi phí và dễ bảo quản. Về mặt chương trình và dữ liệu, khi được dùng chung, mỗi thay đổi sẽ sẵn dùng cho mọi thành viên trên mạng ngay lập tức. Điều này thể hiện rất rõ tại các nơi như ngân hàng, các đại lý bán vé máy bay...

1.4.3.2 Mạng cho phép nâng cao độ tin cậy.

Khi sử dụng mạng, có thể thực hiện một chương trình tại nhiều máy tính khác nhau, nhiều thiết bị có thể dùng chung. Điều này tăng độ tin cậy trong công việc vì khi có máy tính hoặc thiết bị bị hỏng, công việc vẫn có thể tiếp tục với các máy tính hoặc thiết bị khác trên mạng trong khi chờ sửa chữa.

1.4.3.3 Mạng giúp cho công việc đạt hiệu suất cao hơn.

Khi chương trình và dữ liệu đã dùng chung trên mạng, có thể bỏ qua một số khâu đối chiếu không cần thiết. Việc điều chỉnh chương trình (nếu có) cũng tiết kiệm thời gian hơn do chỉ cần cài đặt lại trên một máy. Về mặt tổ chức, việc sao chép dữ liệu phòng hờ tiện lợi hơn do có thể giao cho chỉ một người thay vì mọi người phải tự sao chép phần của mình.

1.4.3.4 Tiết kiệm chi phí.

Việc dùng chung các thiết bị ngoại vi cho phép giảm chi phí trang bị tính trên số người dùng. Về phần mềm, nhiều nhà sản xuất phần mềm cung cấp cả những ấn bản cho nhiều người dùng, với chi phí thấp hơn tính trên mỗi người dùng.

1.4.3.5 Tăng cường tính bảo mật thông tin.

Dữ liệu được lưu trên các máy phục vụ tập tin (file server) sẽ được bảo vệ tốt hơn so với đặt tại các máy cá nhân nhờ cơ chế bảo mật của các hệ điều hành mạng.

1.4.3.6 Việc phát triển mạng máy tính đã tạo ra nhiều ứng dụng mới

Một số ứng dụng có ảnh hưởng quan trọng đến toàn xã hội: khả năng truy xuất các chương trình và dữ liệu từ xa, khả năng thông tin liên lạc dễ dàng và hiệu quả, tạo môi trường giao tiếp thuận lợi giữa những người dùng khác nhau, khả năng tìm kiếm thông tin nhanh chóng trên phạm vi toàn thế giới,...

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

Chương 2: Các thành phần của mạng máy tính
Mục đích
Chương này nhằm giới thiệu cho người học những vấn đề sau: • Các thành phần liên quan đến phần cứng của một mạng máy tính • Sự phân loại mạng máy tính theo các tiêu chí khác nhau • Kiến trúc phần mềm của một mạng máy tính, đặc biệt là kiến trúc có thứ bậc của các giao thức mạng • Mô hình tham khảo OSI

Yêu cầu
Sau khi học xong chương này, người học phải có được những khả năng sau: • Phân biệt được các loại mạng: mạng quảng bá, mạng chuyển mạch, mạng cục bộ, mạng diện rộng, mạng không dây, liên mạng, … • Biện luận được sự cần thiết của tiếp cận phân lớp kiến trúc mạng trong việc thiết kế và xây dựng các hệ thống mạng máy • Phân biệt được các khái niệm quan trọng trong kiến trúc phần mềm mạng như dịch vụ mạng, giao diện mạng và giao thức mạng • Trình bày được ý nghĩa của mô hình OSI, chức năng cơ bản mỗi tầng trong mô hình

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

7

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

2.1 Phần cứng mạng máy tính
2.1.1 Phân loại mạng máy tính theo kỹ thuật truyền tin
Dựa theo kỹ thuật truyền tải thông tin, người ta có thể chia mạng thành hai loại là Mạng quảng bá (Broadcast Network) và mạng điểm nối điểm (Point – to – point Network)

2.1.1.1 Mạng quảng bá
Trong hệ thống mạng quảng bá chỉ tồn tại một kênh truyền được chia sẻ cho tất cả các máy tính. Khi một máy tính gởi tin, tất cả các máy tính còn lại sẽ nhận được tin đó. Tại một thời điểm chỉ cho phép một máy tính được phép sử dụng đường truyền.

2.1.1.2 Mạng điểm nối điểm
Trong hệ thống mạng này, các máy tính được nối lại với nhau thành từng cặp. Thông tin được gởi đi sẽ được truyền trực tiếp từ máy gởi đến máy nhận hoặc được chuyển tiếp qua nhiều máy trung gian trước khi đến máy tính nhận.

2.1.2 Phân loại mạng máy tính theo phạm vị địa lý
Trong cách phân loại này người ta chú ý đến đại lượng Đường kính mạng chỉ khoảng cách của hai máy tính xa nhất trong mạng. Dựa vào đại lượng này người ta có thể phân mạng thành các loại sau: Đường kính mạng 1m 10 m 100 m 1 km 10 km 100 km 1000 km 10000 km Vị trí của các máy tính Trong một mét vuông Trong 1 phòng Trong 1 tòa nhà Trong một khu vực Trong một thành phố Trong một quốc gia Trong m ột châu lục Cả hành tinh Loại mạng Mạng khu vực cá nhân Mạng cục bộ, gọi tắt là mạng LAN (Local Area Network) Mạng thành phố, gọi tắt là mạng MAN (Metropolitan Area Network) Mạng diện rộng, gọi tắt là mạng WAN (Wide Area Network)

2.1.2.1 Mạng cục bộ
Đây là mạng thuộc loại mạng quảng bá, sử dụng một đường truyền có tốc độ cao, băng thông rộng, có hình trạng (topology) đơn giản như mạng hình bus, mạng hình sao (Star topology), mạng hình vòng (Ring topology).

2.1.2.1.1 Mạng hình bus
Tất cả các máy tính được nối lại bằng một dây dẫn (Cáp đồng trục gầy hoặc đồng trục béo). Khi một trong số chúng thực hiện truyền tin, tín hiệu sẽ lan truyền đến tất cả các máy tính còn lại. Nếu có hai máy tính truyền tin cùng một lúc thì sẽ dẫn đến tình trạng đụng độ và trạng thái lỗi xảy ra.

H2.1 Mạng hình Bus

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

8

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

2.1.2.1.2 Mạng hình sao
Các máy tính được nối trực tiếp vào một Bộ tập trung nối kết, gọi là Hub. Dữ liệu được chuyển qua Hub trước khi đến các máy nhận. Hub có nhiều cổng (port), mỗi cổng cho phép một máy tính nối vào. Hub đóng vai trò như một bộ khuyếch đại (repeater). Nó khuyếch đại tín hiệu nhận được trước khi truyền lại tín hiệu đó trên các cổng còn lại. H2.2 Mạng Ưu điểm của mạng hình sao là dễ dàng cài đặt, không dừng mạng khi nối thêm hình sao vào hoặc lấy một máy tính ra khỏi mạng, cũng như dễ dàng phát hiện lỗi. So với mạng hình Bus, mạng hình sao có tín ổn định cao hơn. Tuy nhiên nó đòi hỏi nhiều dây dẫn hơn so với mạng hình bus. Toàn mạng sẽ bị ngưng hoạt động nếu Hub bị hư. Chi phí đầu tư mạng hình sao cao hơn mạng hình Bus.

2.1.2.1.3 Mạng hình vòng
Tồn tại một thẻ bài (token: một gói tin nhỏ) lần lượt truyền qua các máy tính. Một máy tính khi truyền tin phải tuân thủ nguyên tắc sau: Chờ cho đến khi token đến nó và nó sẽ lấy token ra khỏi vòng tròn. Gởi gói tin của nó đi một vòng qua các máy tính trên đường tròn. Chờ cho đến khi gói tin quay về H2.3 Mạng hình vòng Đưa token trở lại vòng tròn để nút bên cạnh nhận token

2.1.2.2 Mạng đô thị
Mạng MAN được sử dụng để nối tất cả các máy tính trong phạm vi toàn thành phố. Ví dụ như mạng truyền hình cáp trong thành phố.

ô

ị

2.1.2.3 Mạng diện rộng
Mạng LAN và mạng MAN thông thường không sử dụng các thiết bị chuyển mạch, điều đó hạn chế trong việc mở rộng phạm vi mạng về số lượng máy tính và khoảng cách. Chính vì thế mạng diện rộng được phát minh. Trong một mạng WAN, các máy tính (hosts) được nối vào một mạng con (subnet) hay đôi khi còn gọi là đường trục mạng (Backbone), trong đó có chứa các bộ chọn đường (routers) và các đường truyền tải (transmission lines). Các Routers thông thường có nhiệm vụ lưu và chuyển tiếp các gói tin mà nó nhận được theo nguyên lý cơ bản sau: Các gói tin đến một router sẽ được lưu vào trong một hàng chờ, kế đến router sẽ 9

H2.5 Mạng diện rộng

H2.6 Lưu và chuyển tiếp trong mạng WAN

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

quyết định nơi gói tin cần phải đến và sau đó sẽ chuyển gói tin lên đường đã được chọn.

2.1.3 Mạng không dây
Nếu phân biệt mang theo tiêu chí hữu tuyến hay vô tuyến thì ta có thêm các loại mạng không dây sau:

2.1.3.1 Nối kết hệ thống (System interconnection)
Mạng này nhằm mục đích thay thế hệ thống cáp nối kết các thiết bị cục bộ vào máy tính như màn hình, bàn phím, chuột, phone, loa ,....

Hình 2.7 (a) Thiết bị không dây, (b) Mạng cục bộ không dây

2.1.3.2 Mạng cục bộ không dây (Wireless LANs):
Tất cả các máy tính giao tiếp với nhau thông qua một trạm cơ sở (Base Station) được nối bằng cáp vào hệ thống mạng.

2.1.3.3 Mạng diện rộng không dây (Wireless WANs):
Thông thường mạng điện thoại di động số thuộc dạng này. Với các công nghệ mới cho phép băng thông mạng có thể đạt đến 50 Mbps với khoảng cách vài kilomet

H2.9 Mạng diện rộng không dây

Trong hình (a ) các máy tính sử dụng công nghệ mạng vô tuyến để nối kết với router. Ngược lại trong hình (b), các máy tính được nối bằng đường dây hữu tuyến với một router, để từ đó router sử dụng kỹ thuật vô tuyến để liên lạc với các router khác.

2.1.4 Liên mạng (Internetwork)
Thông thường một mạng máy tính có thể không đồng nhất ( homogeneous), tức có sự khác nhau về phần cứng và phần mềm giữa các máy tính. Trong thực tế ta chỉ có thể xây dựng được các mạng lớn bằng cách liên nối kết (interconnecting) nhiều loại mạng lại với nhau. Công việc này được gọi là liên mạng (Internetworking). Ví dụ: Nối kết một tập các mạng LAN có kiểu khác nhau như dạng Bus với dạng vòng của một công ty.

Nối các mạng LAN lại với nhau nhờ vào một mạng diện rộng, lúc đó mạng WAN đóng vai trò là một Subnet. Nối các mạng WAN lại với nhau hình thành mạng WAN lớn hơn. Liên mạng lớn nhất hiện nay là mạng toàn cầu Internet.

2.2 Phần mềm mạng

Đây là thành phần quan trọng thật sự làm cho mạng máy tính vận hành chứ không phải là phần cứng. Phần mềm mạng được xây dựng dựa trên nền tảng của 3 khái niệm là giao thức (protocol), dịch vụ (service) và giao diện (interface). Giao thức (Protocol): Mô tả cách thức hai thành phần giao tiếp trao đổi thông tin với nhau. Dịch vụ (Services): Mô tả những gì mà một mạng máy tính cung cấp cho các thành phần muốn giao tiếp với nó. Giao diện (Interfaces): Mô tả cách thức mà một khách hàng có thể sử dụng được các dịch vụ mạng và cách thức các dịch vụ có thể được truy cập đến.

2.2.1 Cấu trúc thứ bậc của giao thức

Nền tảng cho tất cả các phần mềm làm cho mạng máy tính hoạt động chính là khái niệm kiến trúc thứ bậc của giao thức (protocol hierachies). Nó tổ chức các dịch vụ mà một mạng máy tính cung cấp thành các tầng/lớp (layers) Hai thành phần bộ phận ở hai máy tính khác nhau, nhưng ở cùng cấp, chúng luôn luôn thống nhất với nhau về cách thức mà chúng sẽ trao đổi thông tin. Qui tắc trao đổi thông tin này được mô tả trong một giao thức (protocol). Một hệ mạng truyền tải dữ liệu thường được thiết kế dưới dạng phân tầng. Để minh họa ý nghĩa của nó ta xem xét mô hình hoạt động của hệ thống gởi nhận thư tín thế giới. Hai đối tác A ở Paris và B ở Thành phố Cần Thơ thường xuyên trao đổi thư từ với nhau. Vì A không thể nói tiếng Việt và B không thể nói tiếng Pháp, trong khi đó cả hai có thể hiểu tiếng Anh, cho nên nó được chọn là ngôn ngữ để trao đổi thư từ, văn bản giữa A và B. Cả hai gởi thư từ cơ quan của họ. Trong công ty có bộ phận văn thư lãnh trách nhiệm tập hợp và gởi tất cả các thư của công ty ra bưu điện. Tiến trình A gởi cho B một lá thư diễn ra như sau: 1. A viết một lá thư bằng tiếng Pháp bằng bút máy của anh ta. 2. A đưa lá thư cho thư ký, biết tiếng Anh để thông dịch lá thư ra tiếng Anh, sau đó bỏ lá thư vào bao thư với địa chỉ người nhận là địa chỉ của B. 3. Nhân viên của bộ phận văn thư chịu trách nhiệm thu thập thư của công ty ghé qua văn phòng của A để nhận thư cần gởi đi. 4. Bộ phận văn thư thực hiện việc phân loại thư và dán tem lên các lá thư bằng một máy dán tem. 5. Lá thư được gởi đến bưu điện ở Paris. 6. Lá thư được ô tô chuyển đến trung tâm phân loại ở Paris. 7. Những lá thư gởi sang Việt Nam được chuyển đến sân bay ở Paris bằng tàu điện ngầm. 8. Lá thư gởi sang Việt nam được chuyển đến sân bay Tân Sơn Nhất (Thành Phố Hồ Chí Minh) bằng máy bay. 9. Thư được ô tô chở đến trung tâm phân loại thư của Thành Phố Hồ Chí Minh. 10. Thư cho cơ quan của B được chuyển về Bưu điện Cần Thơ bằng ô tô. 11. Thư cho cơ quan của B được chuyển đến công ty của B bằng ô tô. 12. Bộ phận văn thư của công ty của B tiến hành phân loại thư.

13. Thư được phát vào một giờ đã định đến các người nhận, trong trường hợp này có văn phòng của B. 14. Thư ký của B mở thư ra và dịch nội dung lá thư gởi cho B sang tiếng Việt. 15. B đọc lá thư của A đã gởi cho anh ta. Ta có thể tóm tắt lại tiến trình trên bằng một mô hình phân tầng với các nút của mạng thư tín này như sau:

(1) (2)

(15) (14) (13) (12)

(3) (4)

(5)

(6)

(8) (9) (10) (7) H2.10 Mô hình gởi nhận thư tín thế giới

(11)

Trong mô hình trên,mỗi tầng thì dựa trên tầng phía dưới. Ví dụ, các phương tiện của giao thông của tầng như ô tô, tàu hỏa, máy bay (của tầng liên kết dữ liệu) tầng vận chuyển thì cần hạ tầng cơ sở như đường ô tô, đường sắt, sân bay (của tầng vật lý). Đối với mỗi tầng, các chức năng được định nghĩa là các dịch vụ cung cấp cho tầng phía trên nó. Các đường thẳng màu đỏ trong sơ đồ xác định các dịch vụ được cung cấp bởi các tầng khác nhau. Thêm vào đó, các chức năng của từng tầng tương ứng với các luật được gọi là các giao thức (Protocols).

2.2.2 Ví dụ về cấu trúc thứ bậc của giao thức
Xem xét một ví dụ khác liên quan đến hệ thống truyền tập tin từ máy tính X sang máy Y. Hai máy này được nối với nhau bởi một dây cáp tuần tự. Chúng ta xem xét một mô hình gồm 3 tầng: • Người sử dụng muốn truyền một tập tin sẽ thực hiện một lời gọi đến tầng A nhờ vào một hàm đã được định nghĩa sẵn, send_file(fileName, destination). Trong đó fileName là tập tin cần truyền đi, destination là địa chỉ của máy tính nhận tập tin. • Tầng A phân chia tập tin thành nhiều thông điệp và truyền từng thông điệp nhờ lệnh send_message(MessageNo, destination) do tầng B cung cấp. • Tầng B quản lý việc gởi các thông điệp, đảm nhiệm việc phân chia các thông điệp thành nhiều đơn vị truyền tin, gọi là các khung (frame); gởi các khung giữa X và Y tuân theo luật đã định trước (protocol) như tần suất gởi, điều khiển luồng, chờ báo nhận của bên nhận, điều khiển lỗi.

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

A : Tầng ứng dụng

B : Tầng quản lý thông điệp

C : Tầng vật lý

H2.11 Ứng dụng 3 tầng

Tầng B giao cho tầng C một chuỗi các bit mà chúng sẽ được truyền lên đường truyền vật lý, không quan tâm gì về ý nghĩa của các bit, để đến nơi nhận. Thông tin được truyền trên một kênh truyền đơn giản hoặc phức tạp và được định hướng đến nơi nhận. Bên nhận thực hiện ngược lại tiến trình của bên gởi. Cả bên nhận và bên gởi cùng có số lần gởi/nhận giống nhau.
• Tập tin Khung

Tín hiệu H2.12 Đơn vị truyền dữ liệu qua các tầng

Ta cũng chú ý rằng, kích thước của các đơn vị truyền tin trong từng tầng là khác nhau. Ở tầng A đơn vị là một tập tin. Tầng B, đơn vị truyền tin là các khung theo một cấu trúc đã được định nghĩa. Tầng C, đơn vị truyền tin là các tín hiện được truyền trên đường truyền vật lý.

2.2.3 Dịch vụ mạng
Hầu hết các tầng mạng đều cung cấp một hoặc cả hai kiểu dịch vụ: Định hướng nối kết và Không nối kết. Dịch vụ định hướng nối kết (Connection-oriented): Đây là dịch vụ vận hành theo mô hình của hệ thống điện thoại. Đầu tiên bên gọi phải thiết lập một nối kết, kế đến thực hiện nhiều cuộc trao đổi thông tin và cuối cùng thì giải phóng nối kết. Dịch vụ không nối kết (Connectionless): Đây là dịch vụ vận hành theo mô hình kiểu thư tín. Dữ liệu của bạn trước tiên được đặt vào trong một bao thư trên đó có ghi rõ địa chỉ của người nhận và địa chỉ của người gởi. Sau đó sẽ gởi cả bao thư và nội dung đến người nhận. Một số những dịch vụ thường được cung cấp ở mỗi tầng mạng cho cả hai loại có nối kết và không nối kết được liệt kê ở bảng dưới đây: Loại Có nối kết Dịch vụ Luồng thông điệp tin cậy ( Reliable message stream) Luồng byte tin cậy ( Reliable byte stream) Ví dụ Ví dụ gởi tuần tự các trang Đăng nhập từ xa

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

13

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

Không nối kết

Nối kết không tin cậy (Unreliable connection) Thư tín không tin cậy (Unreliable datagram) Thư tín có báo nhận (Acknowledged datagram) Yêu cầu - trả lơi (Request – Reply)

Âm thanh số Mail theo kiểu bó Mail được đăng ký Truy vấn cơ sở dữ liệu

Mỗi loại dịch vụ được cung cấp với chất lượng khác nhau. Các loại dịch vụ có nối kết thường đảm bảo thứ tự đến nơi của thông tin như thứ tự chúng đã được gởi đi, cũng như đảm bảo dữ liệu luôn đến nơi. Hai điều này thường không được đảm bảo trong các dịch vụ loại không nối kết.

2.2.3.1 Các phép toán của dịch vụ
Một dịch vụ thường được mô tả bằng một tập hợp các hàm cơ bản (primitives) hay đôi khi còn gọi là các tác vụ (operations) sẵn có cho các khách hàng sử dụng. Một số các hàm cơ bản thường có cho một dịch vụ định hướng nối kết như sau: Hàm cơ bản LISTEN CONNECT RECIEVE SEND DISCONNECT Chức năng Nghẽn để chờ một yêu cầu nối kết gởi đến Yêu cầu thiết lập nối kết với bên muốn giao tiếp Nghẽn để chờ nhận các thông điệp gởi đến Gởi thông điệp sang bên kia Kết thúc một nối kết

Quá trình trao đổi thông tin giữa Client, người có nhu cầu sử dụng dịch vụ và server, người cung cấp dịch vụ được thực hiện bằng cách sử dụng các hàm cơ sở trên được mô tả như kịch bản sau: Server LISTEN RECIEVE SEND DISCONNECT Client CONNECT SEND RECIEVE DISCONNECT

H2.13 Mô hình dịch vụ có nối kết

2.2.3.2 Sự khác biệt giữa dịch vụ và giao thức
Giao thức và dịch vụ là hai nền tảng rất quan trọng trong việc thiết kết và xây dựng một hệ thống mạng. Cần hiểu rõ ý nghĩa và phân biệt sự khác biệt giữa chúng. Dịch vụ: là một tập các phép toán mà một tầng cung cấp cho tầng phía trên của nó gọi sử dụng.

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

14

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

Giao thức: là một tập các luật mô tả khuôn dạng dữ liệu, ý nghĩa của các gói tin và thứ tự các gói tin được sử dụng trong quá trình giao tiếp. Chú ý: Cùng một service có thể được thực hiện bởi các protocol khác nhau; mỗi protocol có thể được cài đặt theo một cách thức khác nhau ( sử dụng cấu trúc dữ liệu khác nhau, ngôn ngữ lập trình là khác nhau, vv...)

H2.14 Quan hệ giữa dịch vụ và giao thức

2.3 Mô hình tham khảo OSI
Để dễ dàng cho việc nối kết và trao đổi thông tin giữa các máy tính với nhau, vào năm 1983, tổ chức tiêu chuẩn thế giới ISO đã phát triển một mô hình cho phép hai máy tính có thể gởi và nhận dữ liệu cho nhau. Mô hình này dựa trên tiếp cận phân tầng (lớp), với mỗi tầng đảm nhiệm một số các chức năng cơ bản nào đó. Để hai máy tính có thể trao đổi thông tin được với nhau cần có rất nhiều vấn đề liên quan. Ví dụ như cần có Card mạng, dây cáp mạng, điện thế tín hiệu trên cáp mạng, cách thức đóng gói dữ liệu, điều khiển lỗi đường truyền vv... Bằng cách phân chia các chức năng này vào những tầng riêng biệt nhau, việc viết các phần mềm để thực hiện chúng trở nên dễ dàng hơn. Mô hình OSI giúp đồng nhất các hệ thống máy tính khác biệt nhau khi chúng trao đổi thông tin. Mô hình này gồm có 7 tầng: Tầng 7: Tầng ứng dụng (Application Layer) Đây là tầng trên cùng, cung cấp các ứng dụng truy xuất đến các dịch vụ mạng. Nó bao gồm các ứng dụng của người dùng, ví dụ như các Web Browser (Netscape Navigator, Internet Explorer ), các Mail User Agent (Outlook Express, Netscape Messenger, ...) hay các chương trình làm server cung cấp các dịch vụ mạng như các Web Server (Netscape Enterprise, Internet Information Service, Apache, ...), Các FTP Server, các Mail server (Send mail, MDeamon). Người dùng mạng giao tiếp trực tiếp với tầng này. Tầng 6: Tầng trình bày (Presentation Layer) Tầng này đảm bảo các máy tính có kiểu định dạng dữ liệu khác nhau vẫn có thể trao đổi thông tin cho nhau. Thông thường các mày tính sẽ thống nhất với nhau về một kiểu định dạng dữ liệu trung gian để trao đổi thông tin giữa các máy tính. Một dữ liệu cần gởi đi sẽ được tầng trình bày chuyển sang định dạng trung gian trước khi nó được truyền lên mạng. Ngược lại, khi nhận dữ liệu từ mạng, tầng trình bày sẽ chuyển dữ liệu sang định dạng riêng của nó. Tầng 5: Tầng giao dịch (Session Layer)

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

15

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

Tầng này cho phép các ứng dụng thiết lập, sử dụng và xóa các kênh giao tiếp giữa chúng (được gọi là giao dịch). Nó cung cấp cơ chế cho việc nhận biết tên và các chức năng về bảo mật thông tin khi truyền qua mạng. Tầng 4: Tầng vận chuyển (Transport Layer) Tầng này đảm bảo truyền tải dữ liệu giữa các quá trình. Dữ liệu gởi đi được đảm bảo không có lỗi, theo đúng trình tự, không bị mất mát, trùng lắp. Đối với các gói tin có kích thước lớn, tầng này sẽ phân chia chúng thành các phần nhỏ trước khi gởi đi, cũng như tập hợp lại chúng khi nhận được. Tầng 3: Tầng mạng (Network Layer) Tầng này đảm bảo các gói tin dữ liệu (Packet) có thể truyền từ máy tính này đến máy tính kia cho dù không có đường truyền vật lý trực tiếp giữa chúng. Nó nhận nhiệm vụ tìm đường đi cho dữ liệu đến các đích khác nhau trong mạng. Tầng 2: Tầng liên kết dữ liệu (Data-Link Layer) Tầng này đảm bảo truyền tải các khung dữ liệu (Frame) giữa hai máy tính có đường truyền vật lý nối trực tiếp với nhau. Nó cài đặt cơ chế phát hiện và xử lý lỗi dữ liệu nhận. Tầng 1: Tầng vật ký (Physical Layer) Điều khiển việc truyền tải thật sự các bit trên đường truyền vật lý. Nó định nghĩa các tín hiệu điện, trạng thái đường truyền, phương pháp mã hóa dữ liệu, các loại đầu nối được sử dụng. Về nguyên tắc, tầng n của một hệ thống chỉ giao tiếp, trao đổi thông tin với tầng n của hệ thống khác. Mỗi tầng sẽ có các đơn vị truyền dữ liệu riêng:
• • • •

Tầng vật lý: bit Tầng liên kết dữ liệu: Khung (Frame) Tầng Mạng: Gói tin (Packet) Tầng vận chuyển: Đoạn (Segment)
H2.15-Xử lý dữ liệu qua các tầng

Trong thực tế, dữ liệu được gởi đi từ tầng trên xuống tầng dưới cho đến tầng thấp nhất của máy tính gởi. Ở đó, dữ liệu sẽ được truyền đi trên đường truyền vật lý. Mỗi khi dữ liệu được truyền xuống tầng phía dưới thì nó bị "gói" lại trong đơn vị dữ liệu của tầng dưới. Tại bên nhận, dữ liệu sẽ được truyền ngược lên các tầng cao dần. Mỗi lần qua một tầng, đơn vị dữ liệu tương ứng sẽ được tháo ra. Đơn vị dữ liệu của mỗi tầng sẽ có một tiêu đề (header) riêng. OSI chỉ là mô hình tham khảo, mỗi nhà sản xuất khi phát minh ra hệ thống mạng của mình sẽ thực hiện các chức năng ở từng tầng theo những cách thức riêng. Các cách thức này thường được mô tả dưới dạng các chuẩn mạng hay các giao

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

16

thức mạng. Như vậy dẫn đến trường hợp cùng một chức năng nhưng hai hệ thống mạng khác nhau sẽ không tương tác được với nhau. Hình dưới sẽ so sánh kiến trúc của các hệ điều hành mạng thông dụng với mô hình OSI. Để thực hiện các chức năng ở tầng 3 và tầng 4 trong mô hình OSI, mỗi hệ thống mạng sẽ có các protocol riêng: UNIX: Tầng 3 dùng giao thức IP, tầng 4 giao thức TCP/UDP Netware: Tầng 3 dùng giao thức IPX, tầng 4 giao thức SPX Microsoft định nghĩa giao thức NETBEUI để thực hiện chức năng của cả tầng 3 và tầng 4 Nếu chỉ dừng lại ở đây thì các máy tính UNIX, Netware và NT sẽ không trao đổi thông tin được với nhau. Với sự lớn mạnh của mạng Internet, các máy tính cài đặt các hệ điều hành khác nhau đòi hỏi phải giao tiếp được với nhau, tức phải sử dụng chung một giao thức. Đó chính là bộ giao thức TCP/IP, giao thức của mạng Internet.

H2.16 - Kiến trúc của một số hệ điều hành mạng thông dụng

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

17

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

Chương 3: Tầng vật lý
Mục đích
Chương này nhằm giới thiệu những nội dung cơ bản sau: • Giới thiệu mô hình của một hệ thống truyền dữ liệu đơn giản và các vấn đề có liên quan đến trong một hệ thống truyền dữ liệu sử dụng máy tính • Giới thiệu các phương pháp số hóa thông tin • Giới thiệu về đặc điểm kênh truyền, tính năng kỹ thuật của các loại cáp truyền dữ liệu • Giới thiệu các hình thức mã hóa dữ liệu số để truyền tải trên đường truyền

Yêu cầu
Sau khi học xong chương này, người học phải có được những khả năng sau: • Liệt kê được những vấn đề cơ bản có liên quan đến một hệ thống truyền dữ liệu • Mô tả được các hình thức số hóa thông tin • Phân biệt và tính toán được các đại lượng liên quan đến đặc tính của một kênh truyền như: Băng thông, tần số biến điệu, tốc độ dữ liệu, nhiễu, dung lượng và giao thông của một kênh truyền • Mã hóa được dữ liệu số nhờ vào các tín hiệu số và tuần tự theo các kỹ thuật khác nhau.

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

18

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

3.1 Giới thiệu
Về cơ bản, một hệ thống mạng truyền dữ liệu đơn giản nhất được mô tả như sau:

H3.1 Hệ thống truyền dữ liệu đơn giản

Trong mô hình trên, dữ liệu gồm có văn bản, hình ảnh, âm thanh, phim ảnh cần được số hóa dưới dạng nhị phân (bit 0, 1) để dễ dàng cho xử lý và truyền tải. Thiết bị truyền được nối với thiết bị nhận bằng một đường truyền hữu tuyến hoặc vô tuyến. Truyền tin là quá trình thiết bị truyền gởi đi lần lượt các bit của dữ liệu lên kênh truyền để nó lan truyền sang thiết bị nhận và như thế là dữ liệu đã được truyền đi. Các thiết bị truyền và nhận là các máy tính. Để cho hệ thống này có thể hoạt động được thì các vấn đề sau cần phải được xem xét: Cách thức mã hóa thông tin thành dữ liệu số. Các loại kênh truyền dẫn có thể sử dụng để truyền tin. Sơ đồ nối kết các thiết bị truyền và nhận lại với nhau. Cách thức truyền tải các bit từ thiết bị truyền sang thiết bị nhận. Hệ thống trên là hệ thống cơ bản nhất cho các hệ thống truyền dữ liệu. Nó thực hiện đầy đủ các chức năng mà tầng vật lý trong mô hình OSI qui định.

3.2 Vấn đề số hóa thông tin
Thông tin tồn tại dưới nhiều hình thức khác nhau. Để xử lý, mà đặc biệt để truyền tải thông tin ta cần phải mã hóa chúng. Lời nói : Hệ thống : điện thoại Bộ mã hóa : micro Bộ giải mã : Loa Truyền tải : tín hiệu tuần tự hay tín hiệu số Dữ liệu tin học : Hệ thống : mạng truyền tin. Bộ mã hóa : Bộ điều khiển truyền thông. Bộ giải mã:Bộ điều khiển truyền thông Truyền tải : Tín hiệu tuần tự hoặc tín hiệu số. Ánh tĩnh : Hệ thống: fax Bộ mã hóa : scanner Bộ giải mã : Bộ thông dịch tập tin Truyền tải : Tín hiệu tuần tự hoặc tín hiệu số.

Truyền hình : Hệ thống : truyền quảng bá Bộ mã hóa : caméra Bộ giải mã : bộ thu TV + antenne Truyền tải : Tín hiệu tuần tự hoặc tín hiệu số.

Trong thời đại chúng ta, thông tin thường được thể hiện dưới dạng các trang tài liệu hỗn hợp, như các trang web, mà ở đó đồng thời có thể thể hiện văn bản, hình ảnh tĩnh, hình ảnh động, phim ảnh,.... Thông tin thực tế được thể hiện dưới dạng đa phương tiện. Mỗi một loại thông tin sở hữu

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

19

hệ thống mã hóa riêng, nhưng kết quả thì giống nhau: một chuỗi các số 0 và 1. Việc truyền tải thông tin bao gồm việc truyền tải các bit này. Mô hình mã hóa như sau:

H3.2 Sơ đồ số hóa dữ liệu

3.2.1 Số hóa văn bản
Hệ thống mã hóa đầu tiên liên quan đến văn bản là hệ thống mã Morse, được sử dụng rộng rãi trước khi có máy tính. Đây là một bộ mã nhị phân sử dụng 2 ký tự chấm (.) và gạch (-) để số hóa văn bản (có thể xem tương đương với các bit 0 và 1). Tuy nhiên nó có nhiều điểm bất lợi sau: Nghèo nàn: ít các ký tự được mã hóa; Nó sử dụng sự phối hợp của các dấu gạch và dấu chấm với độ dài khác nhau, điều này không được tiện lợi đặc biệt cho các ký tự có tần suất xuất hiện giống nhau. Chính vì thế nó không được dùng để số hóa thông tin. Nếu chúng ta qui định rằng số bit dùng để mã hóa cho một ký tự phải bằng nhau thì với p bit ta có thể mã hóa cho 2p ký tự. Hệ thống mã hóa như thế đã được dùng trong quá khứ.
H3.3 Mã Morse

Ví dụ : 5 bit: dùng trong hệ thống ATI (Alphabet Télégraphique International) 7 bit : gọi là mã ASCII (American Standard Code for Informatics Interchange) được dùng rộng rãi trong máy tính.

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

H3.4 Mã ASCII chuẩn

Bảng mã này có cả các ký tự không in được gọi là các ký tự điều khiển được dùng để tạo ra các tác vụ trên các thiết bị tin học hay dùng để điều khiển thông tin truyền tải. Bảng mã 8 bits: có mã ASCII mở rộng và mã EBCDIC Vì máy tính lưu thông tin dưới dạng các byte 8 bit nên khi sử dụng mã ASCII 7 bít thì bit có trọng số lớn nhất (vị trí thứ 7) luôn có giá trị là 0. Chúng ta có thể sử dụng bit này để định nghĩa các ký tự đặc biệt bằng cách đặt nó giá trị 1. Và như thế chúng ta có một bảng mã ASCII mở rộng. Tuy nhiên, điều này sẽ dẫn đến việc tồn tại nhiều bảng mã ASCII mở rộng khác nhau làm khó khăn trong việc trao đổi thông tin trên phạm vi toàn thế giới. Mã EBCDIC dùng 8 bits để mã hóa nhờ đó có thể thể hiện được 256 ký tự. Nó được sử dụng trong các máy tính IBM. Tuy nhiên nó không thông dụng như mã ASCII. Mã 16 bits : Mã Unicode Mã này được phát triển gần đây để thỏa mãn nhu cầu trao đổi thông tin giữa những người dùng Web. Nó mã hóa hầu hết tất cả các ký tự của các ngôn ngữ trên thế giới. Nó tương thích với mã ASCII 7 bits ở 127 ký tự đầu tiên. Hiện nay mã Unicode bắt đầu được sử dụng rộng rãi.

3.2.2 Số hóa hình ảnh tĩnh
Ảnh số thật sự là một ảnh được vẽ nên từ các đường thẳng và mỗi đường thẳng được xây dựng bằng các điểm. Một ảnh theo chuẩn VGA với độ phân giải 640x480 có nghĩa là một ma trận gồm 480 đường ngang và mỗi đường gồm 640 điểm ảnh (pixel).

Ảnh gốc

Ảnh 1 độ phân giải
H3.5 Mã hóa hình ảnh tĩnh

Ảnh đã số hóa

Một điểm ảnh được mã hóa tùy thuộc vào chất lượng của ảnh: Ảnh đen trắng : sử dụng một bit để mã hóa một điểm : giá trị 0 cho điểm ảnh màu đen và 1 cho điểm ảnh màu trắng. Ảnh gồm 256 mức xám: mỗi điểm được thể hiện bằng một byte (8 bits) ;

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

21

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

Ảnh màu: người ta chứng minh rằng một màu là sự phối hợp của ba màu cơ bản là đỏ (Red), xanh lá (Green) và xanh dương (Blue). Vì thế một màu bất kỳ có thể được biểu biễn bởi biểu thức: x = aR + bG +cB Trong đó a, b, c là các lượng của các màu cơ bản. Thông thường một ảnh đẹp sẽ có lượng màu với giá trị từ 0 đến 255. Và như thế, một ảnh màu thuộc loại này được thể hiện bằng 3 ma trận tương ứng cho 3 loại màu cơ bản. Mỗi phần tử của mảng có giá trị của 8 bits. Chính vì thế cần có 24 bit để mã hóa cho một điểm ảnh màu. Kích thước của các ảnh màu là đáng kể, vì thế người ta cần có phương pháp mã hóa để giảm kích thước của các ảnh.

3.2.3 Số hóa âm thanh và phim ảnh
Dữ liệu kiểu âm thanh và phim ảnh thuộc kiểu tín hiệu tuần tự. Các tín hiệu tuần tự được số hóa theo cách thức sau đây:
Biên độ Tín hiệu tuần tự

1 - Lấy mẫu Tín hiệu được lấy mẫu: với tần số f, ta đo biên độ của tín hiệu, như thế ta được một loạt các số đo.
thời gian
H3.6 Lấy mẫu

Biên độ

thời gian
H3.7 Lượng hóa

2 - Lượng hóa Ta xác định một thang đo với các giá trị là lũy thừa của 2 ( 2p ) và thực hiện việc lấy tương ứng các số đo vào giá trị thanh đo.

3- Mã hóa Mỗi một giá trị sau đó được mã hóa thành các giá trị nhị phân và đặt vào trong các tập tin. 01100110011011111010111011001O.....
H3.8 Mã hóa

Dung lượng tập tin nhận được phụ thuộc hoàn toàn vào tần số lấy mẫu f và số lượng bit dùng để mã hóa giá trị thang đo p ( chiều dài mã cho mỗi giá trị).

3.3 Các loại kênh truyền
3.3.1 Kênh truyền hữu tuyến
Cáp thuộc loại kênh truyền hữu tuyến được sử dụng để nối máy tính và các thành phần mạng lại với nhau. Hiện nay có 3 loại cáp được sử dụng phổ biến là: Cáp xoắn đôi (twisted pair), cáp đồng trục (coax) và cáp quang (fiber optic). Việc chọn lựa loại cáp sử dụng cho mạng tùy thuộc vào nhiều yếu tố như: giá thành, khoảng cách, số lượng máy tính, tốc độ yêu cầu, băng thông

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

22

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

3.3.1.1

Cáp xoắn đôi (Twisted Pair)

Cáp xoắn đôi có hai loại: Có vỏ bọc (Shielded Twisted Pair) và không có vỏ bọc (Unshielded Twisted Pair). Cáp xoán đôi có vỏ bọc sử dụng một vỏ bọc đặc biệt quấn xung quanh dây dẫn có tác dụng chống nhiễu. Cáp xoán đôi trở thành loại cáp mạng được sử dụng nhiều nhất hiện nay. Nó hỗ trợ hầu hết các khoảng tốc độ và các cấu hình mạng khác nhau và được hỗ trợ bởi hầu hết các nhà sản xuất thiết bị mạng.
H3.9 (a) Cáp xoắn đôi không có võ bọc – (b) Cáp xoắn đôi có võ bọc

Các đặc tính của cáp xoán đôi là:
• • • • • • •

Được sử dụng trong mạng token ring (cáp loại 4 tốc độ 16MBps), chuẩn mạng Ethernet 10BaseT (Tốc độ 10MBps), hay chuẩn mạng 100BaseT ( tốc độ 100Mbps) Giá cả chấp nhận được. UTP thường được sử dụng bên trong các tòa nhà vì nó ít có khả năng chống nhiễu hơn so với STP. Cáp loại 2 có tốc độ đạt đến 1Mbps (cáp điện thoại) . Cáp loại 3 có tốc độ đạt đến 10Mbps (Dùng trong mạng Ethernet 10BaseT) (Hình a) Cáp loại 5 có tốc độ đạt đến 100MBps (dùng trong mạng 10BaseT và 100BaseT) (Hình b) Cáp loại 5E và loại 6 có tốc độ đạt đến 1000 MBps (dùng trong mạng 1000 BaseT)

3.3.1.2

Cáp đồng trục (Coaxial Cable)

Cáp đồng trục là loại cáp được chọn lựa cho các mạng nhỏ ít người dùng, giá thành thấp. Có cáp đồng trục gầy (thin coaxial cable) và cáp đồng trục béo (thick coaxial cable)

•

Cáp đồng trục gầy, ký hiệu RG-58AU, được dùng trong chuẩn mạng Ethernet 10Base2.

H3.10 Cáp đồng trục

H3.11 Cáp đồng trục gầy

•

Cáp đồng trục béo, ký hiệu RG-11, được dùng trong chuẩn mạng 10Base5 Các loại đầu nối được sử dụng với cáp đồng trục gầy là đầu nối chữ T (T connector), đầu nối BNC và thiết bị đầu cuối (Terminator)

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

23

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

H3.12 Đầu nối chữ T và BNC

3.3.1.3

Cáp quang (Fiber Optic)

Cáp quang truyền tải các sóng điện từ dưới dạng ánh sáng. Thực tế, sự xuất hiện của một sóng ánh sáng tương ứng với bit “1”và sự mất ánh sáng tương ứng với bit “0”. Các tín hiệu điện tử được chuyển sang tín hiệu ánh sáng bởi bộ phát, sau đó các tín hiệu ánh sáng sẽ được chuyển thành các sung điện tử bởi bộ nhận. Nguồn phát quang có thể là các đèn LED (Light Emitting Diode) cổ điển, hay các diod laser. Bộ dò ánh sáng có thể là các tế bào quang điện truyền thống hay các tế bào quang điện dạng khối.

H3.13 Cấu trúc cáp quang

Sự lan truyền tín hiệu được thực hiện bởi sự phản xạ trên bề mặt. Thực tế, tồn tại 3 loại cáp quang. Chế độ đơn: một tia sáng trên đường truyền tải Hai chế độ còn lại gọi là chế độ đa: nhiều tia sáng cùng được truyền song song nhau Trong chế độ đơn, chiết suất n2 > n1. Tia laser có bước sóng từ 5 đến 8 micromètres được tập trung về một hướng. Các sợi loại này cho phép tốc độ bit cao nhưng khó xử lý và phức tạp trong các thao tác nối kết.
Chiết suất n2

Tia sáng laser Chiết suất n1 H3.14 Cáp quang chế độ đơn - chế độ đa không thẩm thấu - chế độ đa thẩm thấu

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

24

Chế độ đa không thẩm thấu Các tia sáng di chuyển bằng cách phản xạ giữa bề mặt của 2 môi trường có chiết suất khác nhau (n2>n1) và mất nhiều thời gian hơn để các sóng di chuyển so với chế độ đơn. Độ suy giảm đường truyền từ 30 dB/km đối với các loại cáp thủy tinh và từ 100 dB/km đối với loại cáp bằng chất dẽo. Chế độ đa bị thẩm thấu Chiết suất tăng dần từ trung tâm về vỏ của ống. Vì thế sự phản xạ trong trường hợp này thì rất nhẹ nhàng. Từ cách đây nhiều năm người ta có thể thực hiện đa hợp trên cùng một sợi quang nhiều thông tin bằng cách dùng các sóng có độ dài khác nhau. Kỹ thuật này được gọi là WDM (Wavelength Division Multiplexing).

3.3.2 Kênh truyền vô tuyến
Kênh truyền vô tuyến thì thật sự tiện lợi cho tất cả chúng ta, đặc biệt ở những địa hình mà kênh truyền hữu tuyến không thể thực hiện được hoặc phải tốn nhiều chi phí (rừng rậm, hải đảo, miền núi). Kênh truyền vô tuyến truyền tải thông tin ở tốc độ ánh sáng. Gọi: c là tốc độ ánh sáng, f là tần số của tín hiệu sóng λ là độ dài sóng. Khi đó ta có $c = \lambda f$

H3.15 Phân bổ phổ sóng điện từ trên

Tín hiệu có độ dài sóng càng lớn thì khoảng cách truyền càng xa mà không bị suy giảm, ngược lại những tín hiệu có tần số càng cao thì có độ phát tán càng thấp. Hình H3.15 mô tả phổ của sóng điện tử được dùng cho truyền dữ liệu. Khoảng tần số càng cao càng truyền tải được nhiều thông tin.

3.4 Đặc điểm kênh truyền
Phương tiện thường được dùng để truyền tải dữ liệu ( các bits 0,1) từ thiết bị truyền đến thiết bị nhận trên một kênh truyền nhận vật lý là các tín hiệu tuần tự hay tín hiệu số.

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0
Cường độ Cường độ

Thời gian

Thời gian

H3.16 Tín hiệu tuần tự : được biểu diễn bằng một độ lớn vật H3.17 Tín hiệu số : được biểu diễn bởi một độ lớn vật lý với một lý thay đổi một cách liên tục vài giá trị xác định riêng rời

3.4.1 Truyền tải tín hiệu sóng dạng hình sin
Sóng dạng hình sin, không kết thúc hoặc suy giảm sau một khoảng thời gian là dạng tín hiệu tuần tự đơn giản nhất, dễ dàng tạo ra được. Hơn thế nó còn đặc biệt được chú ý đến bởi yếu tố sau: bất kỳ một dạng tín hiệu nào cũng có thể được biểu diễn lại bằng các sóng hình sin. Yếu tố này được rút ra từ một nghiên cứu cụ thể nó cho phép chúng ta có thể định nghĩa một vài đặc điểm của kênh truyền vật lý. Xem xét một kênh truyền, giả sử rằng các điểm nối kết là trực tiếp, không có ngắt quảng, được hình thành từ hai sợi kim loại. Một đoạn của kênh truyền được xem như một đèn 4 cực gồm một điện trở R và một tụ điện C.

vin(t)

vout(t)

H3.18 Mô hình kênh truyền dữ liệu vật lý

Tín hiệu hình sin được áp vào giữa các cực (giữa 2 sợi dây) được tín theo biểu thức: vin(t) = Vin sin wt Trong đó Vin : là hiệu điện thế cực đại; w : nhịp ; f = w/2pi : là tần số; T = 2pi/w = 1/f : là chu kỳ. Tín hiệu đầu ra sẽ là: vout(t) = Vout sin (wt + F) Với : F : là độ trễ pha. Mức điện thế ngỏ ra tùy thuộc vào điện thế ngỏ vào và đặc điểm vật lý của đèn bốn cực. Các luật trường điện tử chứng minh rằng trong trường hợp đơn giản nhất ta có: Vout/Vin = (1 + R2C2w2)-1/2 F = atan(-RC w)

Ta nhận thấy rằng điện thế ngỏ ra Vout thì yếu hơn điện thế ngỏ vào Vin. Ta nói có một sự giảm thế và một sự lệch pha F giữa hiệu điện thế ngỏ vào và hiệu điện thế ngỏ ra. Nếu ta chồng 2 sóng điện thế ngỏ vào và điện thế ngỏ ra trong một sơ đồ thời gian, ta có kết quả như sau:

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

26

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

Cường độ Độ giảm thế

Tín hiệu vào Tín hiệu ra

Thời gian

H3.19 Sự trể pha và giảm thế của tín hiệu ngỏ ra

Độ suy giảm trên kênh truyền A của tín hiệu là một tỷ lệ về công suất Pin/Pout của tín hiệu phát Pin và tín hiệu nhận được Pout. Mỗi công suất được tính với đơn vị là watts. Ta biểu diễn độ suy giảm bằng đơn vị decibel: A(w) = 10 log10(Pin/Pout)

Hình bên mô tả đồ thị biểu diễn mối tương quan giữa độ suy giảm và tần số sóng phát trên một kênh truyền nào đó. Ta thấy rằng tần số tối ưu nhất là f0 và như thế, nếu chúng ta muốn độ suy giảm là nhỏ nhất thì chúng ta sẽ chọn sóng phát hình sin có tần số càng gần f0 càng tốt.

Tần số
H3.20 Tương quan giữa tần số và độ suy giảm của tín hiệu

3.4.2 Truyền tín hiện bất kỳ
Lý thuyết toán Fourrier đã chứng minh rằng bất kỳ một tín hiện nào cũng có thể xem như được tạo thành từ một tổng của một số hữu hạn hoặc vô hạn các sóng hình sin. Không đi sâu vào chứng minh ta có kết quả sau: • Một tín hiệu bất kỳ x(t) thì có thể phân tích thành một tập hợp các tín hiệu dạng sóng hình sin. • Nếu là tín hiệu tuần hoàn, thì ta có thể phân tích nó thành dạng một chuỗi Fourier. Thuật ngữ chuỗi ở đây ý muốn nói đến một loạt các sóng hình sin có tần số khác nhau như là các bội số của tần số tối ưu f0. • Nếu tín hiệu không là dạng tuần hoàn, thì ta có thể phân tích nó dưới dạng một bộ Fourier ; với các sóng hình sin có tần số rời rạc.

3.4.3 Băng thông của một kênh truyền (Bandwidth)
Bởi vì một tín hiệu bất kỳ có thể được xem như là một sự kết hợp của một chuỗi các sóng hình sin, nên ta có thể xem rằng, sự truyền tải một tín hiệu bất kỳ tương đương với việc truyền tải các sóng hình sin thành phần. Vì tần số của chúng là khác nhau, chúng có thể đến nơi với độ suy giảm là khác nhau, một trong số chúng có thể không còn nhận ra được. Nếu ta định nghĩa một ngưỡng còn “nghe” được A0, thì tất cả các tín hiệu hình sin có tần số nhỏ hơn f1 được xem như bị mất. Tương tự các tín hiệu có tần số lớn hơn f2 cũng được xem là bị mất. Những tín hiện có thể nhận ra được ở bên nghe là các tín hiệu có tần số nằm giữa f1 và f2. Khoản tần số này được gọi là băng thông của một kênh truyền.

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

27

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

A(db) Băng thông W

f
H3.21 Băng thông của kênh truyền

Nói một các khác, với một tín hiệu phức tạp bất kỳ, tín hiệu này sẽ truyền tải được nếu như tần số của các sóng hình sin thành phần của nó có tần số nằm trong khoảng băng thông của kênh truyền. Chúng ta cũng nhận thấy rằng, băng thông càng lớn thì càng có nhiều tín hiệu được truyền đến nơi. Chính vì thế chúng ta thường quan tâm đến các kênh truyền có băng thông rộng.. Ví dụ :độ rộng băng thông của kênh truyền điện thoại là 3100 Hz vì các tín hiệu âm thanh có thể nghe được nằm ở khoảng tần số từ 300 Hz đến 3400 Hz.

3.4.4 Tần số biến điệu và tốc độ dữ liệu (Baund rate and bit rate)
Một thông điệp thì được hình thành từ một chuỗi liên tiếp các tín hiệu số hay tuần tự. Mỗi tín hiệu có độ dài thời gian là t. Các tín hiệu này được lan truyền trên kênh truyền với vận tốc 108 m/s trong kênh truyền cáp quang hay 2.106 m/s trong kênh kim loại. Chúng ta thấy rằng tốc độ lan truyền không phải là yếu tố quyết định. Yếu tố quyết định chính là nhịp mà ta đặt tín hiệu lên kênh truyền. Nhịp này được gọi là tần số biến điệu:
R = 1/t ( đơn vị là bauds).

Nếu thông điệp dạng nhị phân, và mỗi tín hiện chuyển tải n bit, khi đó ta có tốc độ bit được tính như sau:
D = nR (đơn vị là bits/s)

Giá trị này thể hiện nhịp mà ta đưa các bit lên đường truyền. Ví dụ : Cho hệ thống có R = 1200 bauds và D = 1200 bits/s. Ta suy ra một tín hiện cơ bản chỉ chuyển tải một bit. Một số ví dụ về tần số biến điệu và tốc độ dữ liệu: Ví dụ 1 : Truyền tải các dữ liệu số bằng các tín hiệu tuần tự. Ta sử dụng hai kiểu tín hiệu tuần tự, mỗi loại có độ dài sóng D, sóng thứ nhất có tần số f1, sóng thứ hai có tần số f2 (gấp đôi tần số f1). Cả hai tín hiệu đều có thể nhận được ở ngõ ra. Ta qui định rằng tín hiệu thứ nhất truyền bit “0” và tín hiệu thứ hai truyền bit "1". Nhịp được sử dụng để đưa các tín hiệu lên đường truyền bằng với nhịp truyền các bit bởi vì mỗi tín hiệu thì truyền một bit. Sự phân biệt giữa tín hiệu 0 và 1 dựa trên sự khác biệt về tần số của 2 tín hiệu sin. Sự mã hóa này được gọi là biến điệu tần số. Ví dụ 2 : Truyền dữ liệu số bởi các tín hiệu tuần tự. Trong trường hợp này ta sử dụng 4 loại tín hiệu hình sin lệch pha nhau Pi/4. Mỗi loại tín hiệu có thể

Cường độ

Thời gian D

R = 1/Δ
Cường độ

D=R

H3.22 Biến điệu tần số Thơi gian

R = 1/∆

D = 2R 28

Biên Sọan: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

vận chuyển 2 bits hoặc 00, 01, 10 hay 11. Với cách thức như thế, tốc độ dữ liệu sẽ gấp đôi tần số biến điệu. Sự phân biệt giữa các tín hiệu trong trường hợp này dự vào pha của tín hiệu. Ta gọi là biến điệu pha. Ví dụ 3 : Truyền tải các dữ liệu số bằng các tín Cường độ hiệu số. Ta sử dụng 8 tín hiệu số cùng độ dài nhưng có biên độ khác nhau. Mỗi tín hiệu truyền tải 3 bits bởi chúng có thể đại diện cho 8 sự kết hợp khác nhau của 3 bit. Sự phân biệt giữa các tín hiệu Thời gian trong trường hợp này dựa vào biên độ của các tín hiệu. Ta gọi là biến điệu biên độ. Để có được một tốc độ truyền dữ liệu cao R = 1/ ∆ D =3 R nhất, ta tìm cách cải thiện tốc độ bit. Bởi vì D = H3.24 Biến điệu biên độ n R, ta có thể tăng tốc độ bit bằng cách tăng một trong các yếu tố sau: o Hoặc tăng n (số bit truyền tải bởi một tín hiệu), tuy nhiên nhiễu là một rào cản quan trọng. o Hoặc R( tần số biến điệu), tuy nhiên chúng ta cũng không thể vượt qua tần số biến điệu cực đại Rmax . Kết quả sau đây đã được chứng minh bởi Nyquist (1928) xác định mối ràng buộc giữa tần số biến điệu cực đại và băng thông của kênh truyền W: • Rmax = 2 W, • Kết quả này được tính toán trên lý thuyết, trong thực tế thì Rmax = 1,25 W

3.4.5 Nhiễu và khả năng kênh truyền
Nhiễu bao gồm các tín hiệu ký sinh chúng chồng lên các tín hiệu được truyền tải và chúng làm cho các tín hiệu này bị biến dạng
Cường độ Tín hiệu bị Nhiễu Thời gian Tín hiệu truyền
H3.25 Nhiễu trên kênh truyền

Chúng ta có thể phân biệt thành 3 loại nhiễu : • Nhiễu xác định: phụ thuộc vào đặc tính kênh truyền • Nhiễu không xác định • Nhiễu trắng từ sự chuyển động của các điện tử Nhiễu phiền tối nhất dĩ nhiên là loại nhiễu không xác định. Chúng có thể làm thay đổi tín hiệu vào những khoảng thời gian nào đó làm cho bên nhận khó phân biệt được đó là bit “0” hay bit “1”. Chính vì thế mà công suất của tín hiệu nên lớn hơn nhiều so với công suất của nhiễu. Tỷ lệ giữa công suất tín hiệu và công suất nhiễu tính theo đơn vị décibels được biểu diễn như sau : S/B = 10log10(PS(Watt)/PB(Watt)) Trong đó PS và PB là công suất của tín hiệu và công suất của nhiễu. Định lý Shannon (1948) giải thích tầm quan trọng của ty lệ S/B trong việc xác định số bit tối đa có thể chuyên chở bởi một tín hiệu như sau:

Kết hợp với định lý của Nyquist, ta có thể suy ra tốc độ bit tối đa của một kênh truyền được tính theo công thức sau:

C được gọi là khả năng của kênh truyền , xác định tốc độ bit tối đa có thể chấp nhận được bởi kênh truyền đó. Ví dụ : Kênh truyền điện thoại có độ rộng băng thông là W = 3100 Hz tỷ lệ S/B = 20 dB. Từ đó ta tính được khả năng của kênh truyền điện thoại là : C = 20,6 Kbits/s .

3.4.6 Giao thông (Traffic)
Giao thông là một khái niệm liên quan đến sự sử dụng một kênh truyền tin. Giao thông cho phép biết được mức độ sử dụng kênh truyền từ đó có thể chọn một kênh truyền phù hợp với mức độ sử dụng hiện tại. Để đánh giá giao thông, ta có thể xem một cuộc truyền tải hay một cuộc giao tiếp là một phiên giao dịch (session) với độ dài trung bình là T ( đơn vị là giây). Cho Nc là số lượng phiên giao dịch trung bình trên một giờ. Mật độ giao thông E được tính theo biểu thức sau : Nói cách khác, mật độ giao thông là đại lượng dùng để đo mức độ sử dụng kênh truyền trong một giây. Thực tế, khi phân tích kỹ hơn ta sẽ thấy rằng trong một phiên giao dịch sẽ chứa nhiều khoảng im lặng (không dùng kênh truyền), ta có thể phân biệt thành 2 loại phiên giao dịch sau: • Các phiên giao dịch mà ở đó thời gian sử dụng T được sử dụng hết. • Các phiên giao dịch mà ở đó thời gian T có chứa các khoảng im lặng. Trong trường hợp thứ hai, mật độ giao thông thì không phản ánh đúng mức độ bận rộn thật sự của kênh truyền. Ta tách một phiên giao dịch thành nhiều giao dịch (transaction) với độ dài trung bình là p bit, cách khoảng nhau bởi những khoảng im lặng. Giả sử Nt là số giao dịch trung bình trong một phiên giao dịch.
Khoảng im lặng Giao dịch (gói tin có độ dài trung bình p)

E = T Nc / 3600

1 phiên giao dịch độ dài T=Nt giao dịch

Gọi D là tốc độ bit của kênh truyền, tốc độ bit thật sự d trong trường hợp này là:

và tần suất sử dụng kênh truyền được định nghĩa bởi tỷ số:

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

Ví dụ : Trong một tính toán khoa học từ xa, người dùng giao tiếp với máy tính trung tâm. Cho : p = 900 bits, Nt = 200, T = 2700 s, Nc = 0.8, D = 1200 b/s. Khi đó • Mật độ giao thông trung bình là E = 0.6 • Tầng suất sử dụng kênh truyền θ = 0.05

3.5 Mã hóa đường truyền (Line Coding)
Sau khi số hóa thông tin, vấn đề chúng ta phải quan tâm kế tiếp là cách truyền tải các bit “0” và “1”. Ta có thể sử dụng tín hiệu số hoặc tín hiệu tuần tự để truyền tải các bit “0”, “1”. Công việc này còn được gọi là mã hóa đường truyền (line coding).

3.5.1 Mã hóa đường truyền bằng tín hiệu số
Trong phương pháp này ta sử dụng một tín hiệu số cho bit “0” và một tín hiệu số khác cho bit “1”. Có nhiều cách thức để thực hiện điều này. Một số phương pháp mã hóa phổ biến như: Mã NRZ (Non Return to Zero), RZ (Return to Zero), lưỡng cực (bipolar) NRZ và RZ: a) NRZ : Điện thế mức 0 để thể hiện bit 0 và điện thế khác không V0 cho bit "1" b) RZ : Mỗi bit "1" được thể hiện bằng một chuyển đổi điện thế từ V0 về 0. c) Lưỡng cực NRZ : Các bit "1" được mã hóa bằng một điện thế dương, sau đó đến một điện thế âm và tiếp tục như thế. bipolar d) Lưỡng cực RZ : Mỗi bit “1” được thể hiện bằng một chuyển đổi từ điện thế khác không về điện thế không. Giá trị của điện thế khác không đầu tiên là dương sau đó là âm và tiếp tục chuyển đổi qua lại như thế. Mã hóa hai pha (biphase):

bipolar

Các mã loại này được định nghĩa so với phương pháp mã NRZ như sau: a) Mã hai pha thống nhất đôi khi còn gọi là mã Manchester: bit "0" được thể hiện bởi một chuyển đổi từ tín hiệu dương về tín hiệu âm và ngược lại một bit “1” được thể hiện bằng một chuyển đổi từ tín hiệu âm về tín hiệu dương.

Dữ liệu truyền Xung đồng hồ Mã 2 pha thống nhất

b) Mã hai pha khác biệt : Nhảy một pha 0 để thể hiện bit “0” và nhảy một pha Pi để thể hiện bit "1".

Mã 2 pha khác biệt

H3.26 Mã hóa đường truyền bằng tín hiệu số

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

31

3.5.2 Mã hóa đường truyền bằng tín hiệu tuần tự
Thông thường người ta sử dụng một sóng mang hình sin v(t) = V sin( t + ) để mã hóa đường truyền. Trong đó ta thay đổi một số tham số để thể hiện các bit "0" và "1" : Thay đổi V, ta có biến điệu biên độ (Amplitude modulation) Thay đổi , ta có biến điệu tần số ( Frequency modulation) Thay đổi , ta có biến điệu pha (Phase modulation) Bên truyền thực hiện quá trình mã hóa một bit thành tín hiệu tuần tự gọi là biến điệu (modulation). Ngược lại bên nhận, nhận được tín hiệu tuần tự phải giải mã thành một bit, gọi là hoàn điệu (demodulation). a) Sử dụng tín hiệu số theo mã NRZ b) Sử dụng biến điệu biên độ c) Sử dụng biến điệu tần số d) Sử dụng biến điệu pha e) Sử dụng biến điệu pha

H3.26 Mã hóa đường truyền bằng tín hiệu hiệu tuần tự

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

32

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

Chương 4: Tầng liên kết dữ liệu ( Data link layer )
Mục đích
Chương này nhằm giới thiệu cho người học những nội dung chủ yếu sau: • Các chức năng cơ bản mà tầng liên kết dữ liệu đảm trách • Vai trò của khung trong vấn đề xử lý lỗi đường truyền và các phương pháp xác định khung • Giới thiệu các phương pháp phát hiện lỗi như Phương pháp kiểm tra chẵn lẽ, Phương pháp kiểm tra theo chiều dọc và Phương pháp kiểm tra phần dư tuần hoàn. • Giới thiệu các giao thức điều khiển lỗi cho phép theo dõi tình trạng lỗi của dữ liệu gởi đi • Giới thiệu các giao thức xử lý lỗi, chỉ ra các cách giải quyết trường hợp dữ liệu truyền đi bị lỗi.

Yêu cầu
Sau khi học xong chương này, người học phải có được các khả năng sau: • Biện luận được vai trò của tầng liên kết dữ liệu trong vấn đề xử lý lỗi dữ liệu truyền nhận • Trình bày được các phương pháp định khung đếm ký tự, phương pháp sử dụng byte là cờ và phương pháp sử dụng cờ đặc biệt • Phân biệt được sự khác nhau giữa các chức năng phát hiện lỗi, điều khiển lỗi và xử lý lỗi của tầng hai. • Cài đặt được cơ chế phát hiện lỗi theo các phương pháp kiểm tra chẵn lẽ, Phương pháp kiểm tra theo chiều dọc và Phương pháp kiểm tra phần dư tuần hoàn • Cài đặt được các giao thức điều khiển lỗi Dừng và chờ, giao thức cửa sổ trượt • Cài đặt được giao thức xử lý lỗi Go-Back-N và giao thức Selective Repeat • Trình bày được ý tưởng cơ bản của giao thức HDLC

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

33

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

4.1 Chức năng của tầng liên kết dữ liệu
Tầng liên kết dữ liệu đảm nhận các chức năng sau: Cung cấp một giao diện được định nghĩa chuẩn cho các dịch vụ cung cấp cho tầng mạng. Xử lý lỗi đường truyền. Điều khiển luồng dữ liệu nhờ đó bên truyền nhanh không làm tràn dữ liệu bên nhận chậm

4.1.1 Các dịch vụ cơ bản của tầng liên kết dữ liệu
Nhiệm vụ của tầng liên kết dữ liệu là cung cấp các dịch vụ cho tầng mạng. Dịch vụ chính của tầng liên kết dữ liệu là truyền tải dữ liệu nhận được từ tầng mạng trên máy gởi đến tầng mạng trên máy nhận. Để làm được điều này, tầng liên kết dữ liệu lấy các gói tin (Packet) mà nó nhận được từ tầng mạng và gói chúng vào trong các khung (frame) để truyền đi. Mỗi khung chứa phần tiêu đề (Header), thông tin cần truyền đi (Payload field) và thông tin theo dõi khác (Trailer).

H4.1 Vị trí và chức năng của tầng liên kết dữ liệu

Có 3 dịch vụ cơ bản mà tầng liên kết dữ liệu thường cung cấp là: Dịch vụ không nối kết không báo nhận (unacknowledged connectionless service), thường được sử dụng trong mạng LAN. Dịch vụ không nối kết có báo nhận (acknowledged connectionless service), thường dùng cho mạng không dây. Dịch vụ nối kết định hướng có báo nhận (acknowledged connection-oriented service), thường dùng trong mạng WANs.

4.1.2 Xử lý lỗi
Để có thể truyền tải được dữ liệu nhận từ tầng mạng đến máy nhận, tầng liên kết dữ liệu phải sử dụng các dịch vụ được cung cấp bởi tầng vật lý. Tất cả những gì tầng vật lý thực hiện là nhận một chuỗi các bits thô và cố gắng truyền chúng đến máy đích. Tầng vật lý không đảm bảo về độ tin cậy của các bits được truyền đi. Số lượng bits đến nơi nhận có thể nhiều, ít, hay bằng số bits đã gởi đi, thậm chí giá trị của chúng cũng có thể khác với giá trị mà chúng đã được gởi đi. Chính vì thế mà tầng liên kết dữ liệu phải dò tìm và xử lý các lỗi trên dữ liệu nhận được.

4.1.3 Định khung
Như đã nói ở phần trên, đơn vị truyền tin của tầng liên kết dữ liệu là các khung. Vấn đề đặt ra là làm sao bên nhận biết được điểm bắt đầu và điểm kết thúc của khung. Chính vì vậy mà tầng liên kết dữ liệu cần thiết phải qui định khuôn dạng của khung mà mình sử dụng. Có 3 phương pháp để định khung phổ biến sau: Đếm ký tự (Character count) Sử dụng các bytes làm cờ hiệu và các bytes độn (Flag byte with byte stuffing)
Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

34

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

Sử dụng cờ bắt đầu và kết thúc khung cùng với các bit độn (Starting and ending flags with bit stuffing)

4.1.3.1

Phương pháp đếm ký tự (Character Count)

Phương pháp này sử dụng một trường trong phần tiêu đề để mô tả số lượng các ký tự có trong khung. Bất lợi của phương pháp này là nếu một ký tự đếm của một khung nào đó bị lỗi sẽ làm cho các khung phía sau không thể xác định được. Phương pháp này vì thế mà ít được sử dụng.

H4.2 Định khung bằng phương pháp đếm ký tự

4.1.3.2

Phương pháp sử dụng byte làm cờ và các byte độn (Flag byte with byte stuffing)

Phương pháp này sử dụng một byte có giá trị đặc biệt để làm cờ hiệu (flag byte) đánh dấu điểm bắt đầu và kết thúc của khung. Một vấn đề phát sinh trong phương pháp này là, trong dữ liệu có thể chứa byte có giá trị của cờ hiệu. Điều này sẽ làm gẫy khung. Để giải quyết vấn đề này, người ta đưa vào phía trước byte dữ liệu có giá trị của cờ hiệu một byte đặc biệc gọi là byte ESC. Bên nhận khi nhận được byte ESC theo sau là giá trị của cờ hiệu thì sẽ bỏ đi ký tự ESC đồng H4.3 (a)Khung được đánh dấu bởi cờ hiệu, thời biết đây chưa phải là điểm (b) Dữ liệu có chứa cờ hiệu và byte ESC. kết thúc của khung. Tương tự, nếu trong dữ liệu có chứa ký tự ESC thì ta cũng đưa thêm vào phía trước nó một ký tự ESC. Kỹ thuật này được gọi là ký tự độn (character stuffing). Yếu điểm của phương pháp này là nó dựa trên ký tự dạng 8 bits vì thế sẽ không sử dụng được trong các hệ thống sử dụng chuẩn mã 16 bits như Unicode chẳng hạn.

4.1.3.3

Sử dụng cờ bắt đầu và kết thúc khung cùng với các bit độn (Starting and ending flags with bit stuffing).

Phương pháp này sử dụng mẫu bit đặc biệt, 01111110, để làm cờ đánh dấu điểm bắt đầu và kết thúc khung. Khi bên gởi phát hiện có 5 bits 1 liên tiếp trong dữ liệu gởi đi, nó sẽ thêm vào bit 0.

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

35

Ngược lại, nếu bên nhận phát hiện 5 bits liên tiếp và theo sau bằng một bit 0, nó sẽ loại bỏ bit 0 ra khỏi dữ liệu. Nhờ thế cờ sẽ không xuất hiện trong dữ liệu gởi.

H4.4 (a) Dữ liệu gốc, (b)Dữ liệu chuyển lên đường truyền, (c) Dữ liệu nhận sau khi loại bỏ các bit độn.

4.1.4 Điều khiển lỗi (Error Control)
Một vấn đề khác cần phải xem xét là cách nào để đảm bảo rằng toàn bộ các khung đã được phân phát đến tầng mạng và được phân phát theo đúng trình tự chúng đã được gởi. Điều này không cần quan tâm trong dịch vụ không nối kết không báo nhận. Tuy nhiên nó cần phải được đảm bảo trong dịch vụ nối kết định hướng. Cách thường được dùng để đảm bảo việc phân phát tin cậy là cung cấp cho người gởi một vài phản hồi từ người nhận về tình trạng nhận khung. Hệ thống sẽ định nghĩa một khung đặc biệt, gọi là khung báo nhận (acknowledgement), để cho người nhận thông báo cho người gởi tình trạng của dữ liệu nhận là tốt hay xấu. Nếu người gởi nhận được một báo hiệu tốt về gói tin, người gởi an tâm rằng gói tin đã được phân phát một cách an toàn. Ngược lại, một khung báo không nhận (unacknowledgement) báo hiệu rằng có một số vấn đề gì đó đối với khung nhận và nó cần phải được truyền lại. Một khả năng khác có thể xảy ra là khung gởi đi hoàn toàn bị mất không đến được người nhận. Trong trường hợp này sẽ không có một khung báo nhận nào được gởi về cho người gởi, làm cho người gởi rơi vào trạng thái chờ đợi vĩnh viễn. Để giải quyết vấn đề này, người ta thêm vào tầng liên kết dữ liệu một bộ đếm thời gian (timer). Khi bên gởi truyền một khung đi, nó sẽ thiết lập bộ đếm thời gian. Bộ đếm thời gian sẽ không còn hiệu lực (time-out) sau một khoảng thời đủ lớn để khung được truyền đến người nhận, xử lý ở đó, và khung báo nhận đến được người gởi. Thông thường nếu khung được nhận tốt, khung báo nhận sẽ trở về người gởi trước thời gian qui định. Khi đó bộ đếm thời gian sẽ bị hủy. Tuy nhiên, nếu khung báo nhận bị mất, bộ đếm thời gian sẽ trôi qua, báo hiệu cho người gởi về vấn đề phát sinh. Giải pháp trong trường hợp này là bên gởi gởi lại khung. Như thế khung được truyền đi nhiều lần có thể làm cho khung được gởi lên tầng mạng nhiều hơn một lần. Để phòng ngừa trường hợp này, người ta gán vào mỗi khung gởi đi một Số thứ tự (sequence number), nhờ đó bên nhận phân biệt được các khung được truyền lại.

4.1.5 Điều khiển luồng (Flow Control)
Một vấn đề thiết kế quan trọng khác cần phải xem xét trong tầng liên kết dữ liệu là sự khác biệt về tốc độ truyền / nhận dữ liệu của bên truyền và bên nhận. Có hai tiếp cận để giải quyết vấn đề này. Tiếp cận điều khiển luồng dựa trên phản hồi (feedback based flow control): Người nhận gởi thông tin về cho người gởi cho phép người gởi gởi thêm dữ liệu, cũng như báo với người gởi những gì mà người nhận đang làm. Tiếp cận điều khiển luồng dựa trên tần số (rate based flow control): Trong giao thức truyền tin cài sẵn cơ chế giới hạn tần suất mà người gởi có thể truyền tin.

4.2 Vấn đề xử lý lỗi
4.2.1 Bộ mã phát hiện lỗi
Khi truyền tải một chuỗi các bit, các lỗi có thể phát sinh ra, bit 1 có thể biến thành bit 0 hay ngược lại. Ta định nghĩa tỷ lệ lỗi bởi tỷ số sau: τ = Số bít bị lỗi / Tổng số bít được truyền Tỷ lệ lỗi này có giá trị từ 10-5 đến 10-8. Tùy thuộc vào từng loại ứng dụng, một lỗi có mức độ nghiêm trọng khác nhau, chính vì thế cần có các cơ chế cho phép phát hiện lỗi cũng như sửa lỗi. Các thống kê cho thấy rằng 88% các lỗi xẩy ra do sai lệch một bit và 10% các lỗi xảy ra do sự sai lệch 2 bit kề nhau. Chính vì thế ta ưu tiên cho vấn đề phát hiện các lỗi trên một bit và sửa đổi chúng một cách tự động. Với ý tưởng như thế, ta sử dụng các mã phát hiện lỗi: bên cạnh các thông tin hữu ích cần truyền đi, ta thêm vào các thông tin điều khiển. Bên nhận thực hiện việc giải mã các thông tin điều khiển này để phân tích xem thông tin nhận được là chính xác hay có lỗi.
Thông tin hữu ích Bộ mã hóa Thông tin hữu ích + Thông tin điều khiển
H4.5 Mô hình xử lý lỗi trong truyền dữ liệu

Thiết bị gởi

Bộ giải mã

Thông tin hữu ích

Thiết bị nhận

Thông tin điều khiển được đưa vào có thể theo 2 chiến lược. Chiến lược thứ nhất gọi là bộ mã sửa lỗi (Error-correcting codes) và chiến lược thứ hai gọi là bộ mã phát hiện lỗi (Error-detecting codes). Bộ mã sửa lỗi cho phép bên nhận có thể tính toán và suy ra được các thông tin bị lỗi (sửa dữ liệu bị lỗi). Trong khi bộ mã phát hiện lỗi chỉ cho phép bên nhận phát hiện ra dữ liệu có lỗi hay không. Nếu có lỗi bên nhận sẽ yêu cầu bên gởi gởi lại thông tin. Với tốc độ của đường truyền ngày càng cao, người ta thấy rằng việc gởi lại một khung thông tin bị lỗi sẽ ít tốn kém hơn so với việc tính toán để suy ra giá trị ban đầu của các dữ liệu bị lỗi. Chính vì thế đa số các hệ thống mạng ngày nay đều chọn bộ mã phát hiện lỗi.

4.2.2 Những bộ mã phát hiện lỗi (Error-Detecting Codes)
Có nhiều sơ đồ phát hiện lỗi, trong đó có các sơ đồ thông dụng là: Kiểm tra chẵn lẻ (Parity checks) Kiểm tra thêm theo chiều dọc (Longitudinal reduncy check) Kiểm tra phần dư tuần hoàn (Cyclic redundancy check)

4.2.2.1

Kiểm tra chẵn lẻ (Parity Check)

Sơ đồ phát hiện bit lỗi đơn giản nhất là nối một bit chẵn-lẻ vào cuối của mỗi từ trong khung. Một ví dụ tiêu biểu là việc truyền các ký tự ASCII, mà trong đó một bit chẵn-lẻ

được nối vào mỗi ký tự ASCII 7 bit. Giá trị của bit này được lựa chọn sao cho có một số chẵn của bit 1, với kiểm tra chẵn (even parity) hoặc một số lẻ của bit 1, với kiểm tra lẻ (odd parity). Ví dụ, nếu bên gởi đang truyền một ký tự ASCII G ( mã ASCII là1110001) và đang dùng phương pháp kiểm tra lẽ, nó sẽ nối một bit 1 và truyền đi 11100011. Bên nhận sẽ kiểm tra ký tự nhận được và nếu tổng của các bit 1 là lẻ, nó xem như không có lỗi. Nếu một bit hoặc một số lẻ bất kỳ các bit bị lỗi đảo ngược thì rõ ràng bên nhận sẽ phát hiện được lỗi. Tuy nhiên, nếu hai hay một số chẵn bất kỳ các bit bị lỗi đảo ngược thì nó sẽ không phát hiện được lỗi. Trên thực tế những xung nhiễu lại thường đủ dài để có thể phá hủy hơn một bit, đặc biệt là với tốc độ dữ liệu cao. Do đó, cần phải có một phương pháp cải thiện trường hợp này.
Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

37

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

4.2.2.2

Kiểm tra thêm theo chiều dọc (Longitudinal Redundancy Check or Checksum)

Có thể cải thiện sơ đồ trên bằng cách Parity bits dùng phương pháp LRC. Trong phương pháp này, khung được xem như một khối nhiều ký tự được sắp 1011011 1 xếp theo dạng hai chiều, và việc kiểm tra được thực hiện cả chiều ngang lẫn 1101011 1 chiều dọc. Theo chiều ngang, mỗi ký tự được Data bits 0011101 0 thêm vào một bit kiểm tra chẵn lẽ như trường hợp trên, và được gọi là 1111000 0 bit Kiểm tra chiều ngang VRC (Vertical Redundancy Check). Theo chiều dọc, cung cấp thêm một 1000101 1 ký tự kiểm tra, được gọi là ký tự Kiểm tra chiều dọc LRC 0101111 1 (Longitudinal Redundancy Check) hay Checksum. Trong đó, bít thứ i LRC bits 0 1 1 1 1 1 1 0 của ký tự này chính là bit kiểm tra cho tất cả các bit thứ i của tất cả các H4.6 Kiểm tra chiều dọc tuần hoàn ký tự trong khối. Các phép đo chỉ ra rằng việc dùng cả hai VRC và LRC giảm đi tỷ lệ lỗi không phát hiện được hai đến bốn bậc so với dùng chỉ VRC. Hãy xem trường hợp bit 1 và 3 trong ký tự 1 đang bị lỗi. Khi bên nhận tính toán được bit VRC cho ký tự 1, nó sẽ kiểm tra với bit VRC đã nhận, và sẽ không phát hiện được lỗi. Tuy nhiên, khi nó tính toán được ký tự LRC, bit 1 và 3 của ký tự này sẽ khác với những bit đó trong ký tự LRC nhận được, và sẽ phát hiện được lỗi. Tuy nhiên, ngay sơ đồ này cũng không phải là thật sự tốt. Bây giờ, nếu giả sử bit 1 và 3 của ký tự 5 cũng bị lỗi, phương pháp này sẽ không phát hiện được điểm sai.

4.2.2.3

Kiểm tra phần dư tuần hoàn (Cyclic Redundancy Check)

Để cải tiến hơn nữa các nhà thiết kế đã dùng kỹ thuật mới dễ dàng và hiệu quả được gọi là kiểm tra phần dư tuần hoàn, trong đó có thể sử dụng một số phương pháp cài đặt khác nhau như: modulo 2, đa thức, thanh ghi dịch và các cổng Exclusive-or. Các thủ tục với modulo 2 diễn ra như sau. Với một thông điệp M có k bit cần gởi đi, bên gởi sẽ nối vào cuối thông điệp một chuỗi F có r bit, được gọi là Chuỗi kiểm tra khung (FCS: Frame Check Sequence). Chuỗi kiểm tra khung sẽ tính toán sao cho khung kết quả T được hình thành từ việc nối M với F (gồm k + r bit) có thể chia hết bởi số P nào đó được định trước. Bên gởi sẽ gởi T đi. Khi bên nhận nhận được T, nó sẽ thực hiện phép chia modulo T cho P. Nếu phép chia không hết, tức có số dư, bên nhận xác định rằng khung T đã bị lỗi, ngược lại là không có lỗi. Nếu khung không có lỗi, bên nhận sẽ tách thông điệp M từ T, là k bits trọng số cao của T. Phương pháp này dùng phép chia modulo 2 trong việc chia T cho P, phép toán modulo 2 dùng một phép cộng nhị phân không nhớ và đó cũng chính là phép toán Exclusive-or. Ví dụ sau mô tả phép toán cộng và nhân modulo 2:
1111 + 1010 0101 x 11001 11 11001 11001 101011

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

38

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

Giả sử ta có: o M: Thông điệp k bit cần được gởi sang bên nhận. o F : Chuỗi kiểm tra khung FCS gồm r bit là thông tin điều khiển được gởi theo M để giúp bên nhận có thể phát hiện được lỗi. o T =MF là khung (k + r) bit, được hình thành bằng cách nối M và F lại với nhau. T sẽ được truyền sang bên nhận, với r < k Với M (k bit) , P (r+1 bit), F (r bit), T (k+r bit), thủ tục tiến hành để xác định checksum F và tạo khung truyền như sau: o Nối r bit 0 vào cuối M, hay thực hiện phép nhân M với 2r o Dùng phép chia modulo 2 chia chuỗi bit M*2r cho P. o Phần dư của phép chia sẽ được cộng với M*2r tạo thành khung T truyền đi. o Trong đó P được chọn dài hơn F một bit, và cả hai bit cao nhất và thấp nhất phải là 1 Ví dụ: o Giả sử ta có: M = 1010001101 (10 bit) P = 110101 (6 bit) FCS cần phải tính toán ( 5 bit) o Ta lần lượt thực hiện các bước sau: Tính M*25 = 101000110100000. Thực hiện phép chia modulo M*25 cho P như hình dưới, ta được phần dư F = 01110 Tạo khung gởi đi là T = M*2r + F = 101000110101110
(P) 1 1 0 1 0 1 1 1 0 1 0 1 0 1 1 0 1 0 1 0 0 01 1 0 1 0 0 0 0 0 1 1 01 0 1 1 1 1 0 11 1 1 0 1 01 0 1 1 1 0 1 0 0 0 0 0 0 1 1 1 0 1 0 1 1 0 1 0 1 01 1 1 1 1 00 0 0 0 0 1 1 1 1 1 0 1 1 0 1 0 1 0 1 0 1 1 0 0 0 0 0 0 0 1 0 1 1 0 0 1 1 0 1 0 1 1 1 0 0 1 0 1 1 0 1 0 1 0 0 1 1 1 0 0 0 0 0 0 0 0 1 1 1 0=F ( Q : Kết quả phép chia) ( M*2r)

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

39

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

Ngoài ra người ta còn có thể sử dụng phương pháp đa thức để biểu diễn phương pháp kiểm tra phần dư tuần hòan. Trong phương pháp này người ta biểu diễn các chuỗi nhị phân dưới dạng những đa thức của biến x với các hệ số nhị phân. Các hệ số tương ứng với các bit trong chuỗi nhị phân cần biểu diễn. Giả sử ta có M=110011và P = 11001, khi đó M và P sẽ được biểu diễn lại bằng 2 đa thức sau: M(x) = x5 + x4 + x + 1
P(x) = x4 + x3 + 1

Những phép toán trên đa thức vẫn là modulo 2. Quá trình tính CRC được mô tả dưới dạng các biểu thức sau: X n M( X ) R( X ) 1. = Q( X ) + P( X ) P( X ) n 2. T ( X ) = X M ( X ) + R( X ) Các version thường được sử dụng của P là : CRC-12 = X12 + X11 + X3 + X2 + X + 1 CRC-16 = X16 + X15 + X2 + 1 CRC-CCITT = X16 + X12 + X5 + 1 CRC-32 = X32 + X26 + X23 + X22 + X16 + X12 + X11 + X10 + X8 + X7 + X5 + X4 + X2 + X +1 Ví dụ: Cho: M=1010001101, P=110101 Ta có: r=5 M(x)= x9+x7+x3+x2+1 x5M(x)= x14+x12+x8+x7+x5 P(x) = x5+x4+x2+1 Thực hiện phép toán:

Q(x)= x9+ x8+ x6+x4+x2 +x1 F(x)= x3+ x2+ x1 <> 01110 Khung cần truyền đi là T= 101000110101110 =>

4.3 Một số giao thức điều khiển lỗi (Error Control)
Phần kế tiếp chúng ta xem xét một số giao thức cơ bản được sử dụng nhiều trong việc điều khiển lỗi. Các giao thức này được xây dựng dựa trên các giả định sau: Chúng ta có máy tính A muốn gởi dữ liệu cho máy tính B. Luôn luôn có đủ dữ liệu cho máy A gởi đi . Các giao diện giao tiếp với tầng mạng và tầng vật lý đã được định nghĩa chuẩn. Bên nhận thông thường thực hiện việc chờ đợi một sự kiện nào đó phát sinh bằng cách gọi hàm wait_for_event(). Các giao thức được trình bày dưới dạng các chương trình viết bằng ngôn ngữ c. Chúng sử dụng các định nghĩa trong tập tin protocol.h có nội dung như sau:

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

40

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

/* Kích thước tối đa của một gói tin */ /* Kiểu luận lý */ /* Số thứ tự của khung gởi hoặc khung báo nhận*/ packet; /* Định nghĩa kiểu của gói tin */ /* Các loại khung */ /* Kiểu dữ liệu của khung: */ //Loại khung //Số thứ tự của khung gởi đi //Số thức tự của khung muốn báo nhận //Thông tin gởi nhận, // là gói tin nhận của tầng mạng /* Chờ một sự kiện xuất hiện; trả về kiểu của sự kiện */ /* Nạp gói tin nhận được từ tầng mạng vào khung để gởi đi */ /* Chuyển dữ liệu từ khung nhận được cho tầng mạng */ /* Nhận khung đến từ tầng vật lý và lưu nó vào khung r */ /* Chuyển một khung xuống tầng vật lý để truyền đi */ /* Khởi động đồng hồ và bật sự kiện quá thời hạn cho khung thứ k đang gởi đi */ /* Dừng đồng hồ và tắt sự kiện quá thời hạn cho khung thứ k đang gởi đi */ /* Khởi động đồng hồ phụ và bật sự kiện quá thời hạn cho khung phản hồi*/ /* Dừng đồng hồ phụ và tắt sự kiện quá thời hạn cho khung phản hồi*/ /* Cho phép tầng mạng tạo sự kiện tầng mạng đã sẵn sàng */ /* Cấm tầng mạng tạo sự kiện tầng mạng đã sẵn sàng */ /* Macro để tăng giá trị K theo kiểu quay vòng */

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

41

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

4.3.1 Giao thức truyền đơn công không ràng buộc (Unrestricted Simplex Protocol)
Protocol 1 (utopia) được dùng cho việc truyền tải thông tin theo một chiều từ người gởi sang người nhận. Kênh truyền được giả định là không có lỗi và bên nhận được giả định rằng có thể xử lý được hết tất cả các thông tin gởi đến một cách nhanh chóng. Chính vì thế mà bên gởi chỉ đơn thuần thực hiện một vòng lặp đưa dữ liệu lên đường truyền với tốc độ nhanh nhất có thể.

/* Vùng đệm để chứa khung gởi đi */ /* Vùng đệm để chứa gói tin gởi đi */ /* Nhận gói tin từ tầng mạng để gởi đi */ /* Đưa gói tin vào khung để gởi đi */ /* Gởi khung xuống tầng vật lý để gởi lên đường truyền */

/* Chờ sự kiện, chỉ xuất hiện khi khung đến */ /* Nhận khung từ tầng vật lý */ /* Lấy thông tin ra khỏi khung và gởi lên tầng mạng */

P4.1 Giao thức truyền đơn công không ràng buộc

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

42

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

4.3.2 Giao thức truyền đơn công dừng và chờ (Simplex Stop-and-wait Protocol)
Giao thức Stop-and-wait cũng được thiết kế cho các cuộc truyền tải thông tin một chiều từ người gởi sang người nhận. Kênh truyền tải thông tin một lần nữa cũng được giả định rằng không có lỗi như giao thức Unrestricted Simplex Protocol. Tuy nhiên, trong trường hợp này, bên nhận chỉ có một vùng lưu trữ có khả năng hạn chế và một tốc độ xử lý giới hạn, vì thế giao thức phải được thiết kế dự phòng cho trường hợp dữ liệu máy gởi đến nhanh làm tràn vùng lưu trữ thông tin của bên nhận.

/* Vùng đệm để chứa khung gởi đi */ /* Vùng đệm để chứa gói tin gởi đi */ /* Sự kiện báo hiệu khung đến */ /* Nhận gói tin từ tầng mạng để gởi đi */ /* Đưa gói tin vào khung để gởi đi */ /* Gởi khung xuống tầng vật lý để gởi lên đường truyền */ /* Chờ sự kiện đến của khung báo nhận gởi về từ bên gởi*/

/* Chờ sự kiện, chỉ xuất hiện khi khung đến */ /* Nhận khung từ tầng vật lý */ /* Lấy thông tin ra khỏi khung và gởi lên tầng mạng */ /* Gởi khung báo nhận sang bên gởi */

P4.2 Giao thức truyền đơn công truyền và chờ

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

43

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

4.3.3 Giao thức truyền đơn công cho kênh truyền có nhiễu (Simplex Protocol for Noisy Channel )
Giả sử ta bỏ đi giả thuyết kênh truyền không có lỗi. Trong trường hợp này, với các kỹ thuật xử lý lỗi (Parity check, CRC), bên nhận có thể phát hiện ra được các khung bị lỗi. Tuy nhiên, điều gì sẽ xảy ra nếu khung gởi đi bị mất, không đến được nơi nhận. Khi đó sẽ dẫn đến tình trạng như sau: Người gởi không biết được khung có đến nơi nhận tốt hay không. Giải pháp là yêu cầu người nhận gởi các khung báo nhận thông báo về tình hình các khung bị lỗi. Các khung báo nhận có thể bị mất. Giải pháp: Mỗi khi gởi một khung đi, Bên gởi sẽ thiết lập một bộ đếm thời gian. Nếu sau một khoảng thời gian qui định mà không nhận được khung báo nhận, bên gởi sẽ gởi lại các khung không được báo nhận Bên nhận không phân biệt được các khung trùng lắp do bên gởi gởi lại. Giải pháp: Mỗi khung sẽ có một số thứ tự để phân biệt lẫn nhau. Số thứ tự này sẽ được tăng dần cho đến một giá trị cực đại sau đó lại quay về giá trị 0. Trong ví dụ sau, số thứ tự có giá trị cực đại là 1. Như vậy ta chỉ sử dụng 2 giá trị là 0 và 1 để đánh số thứ tự cho khung.
/* Giá trị tối đa của số thứ tự khung là 1 */

/* Số thứ tự của gói tin của lần gởi kế tiếp */ /* Khung để gởi dữ liệu đi */ /* Vùng lưu trữ cho gói tin gởi */ /* Khởi động số thứ tự cho khung gởi */ /* Nhận gói tin đầu tiên từ tầng mạng để gởi đi */ /* Xây dựng khung để gởi đi */ /* Đánh số thứ tự cho khung */ /* Gởi khung xuống tầng vật lý để truyền đi */ /* Nếu khung báo nhận đến chậm, tạo sự kiện time-out */

/* Số thứ tự của gói tin chờ nhận kế tiếp */ /* Khung nhận và khung báo nhận */ /* Khởi động số thứ tự cho khung nhận */ /* Chờ một sự kiện xảy ra*/ /* Nếu là sự kiện khung đến */ /* - Nhận khung dữ liệu từ tầng vật lý */ /* - Nếu đúng là khung đang chờ */ /* - Gởi dữ liệu nhận được lên tầng mạng */ ố

P4.3 Giao thức truyền đơn công cho kênh truyền có nhiễu

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

44

4.4 Giao thức của sổ trượt (Sliding windows)
4.4.2 Vấn đề truyền tải thông tin theo hai chiều (Duplex)
Chúng ta muốn việc truyền tải thông tin giữa hai bên giao tiếp diễn ra một cách đồng thời theo hai chiều hơn là chỉ một chiều để khai thác tối đa khả năng của kênh truyền. Để thực hiện được điều này, chúng ta thực sử dụng chế độ truyền tải hai chiều, gọi là song công (Duplex). Nguyên tắc thực hiện như sau: Vẫn thực hiện việc truyền tải khung, tuy nhiên ta có phân biệt thành các loại khung: dữ liệu (data), báo nhận ACK (acknowledgement), và báo không nhận NACK(Not Acknowledgement) trong trường xác định loại (Type) của khung. Khi một bên nào đó truyền tin, nó có thể kết hợp đưa thông tin báo cho bên kia biết tình trạng của gói tin mà nó đã nhận trước đó. Ta gọi là kỹ thuật piggyback.

4.4.3 Giới thiệu về giao thức cửa sổ trượt
Thay vì chỉ truyền đi một khung tại một thời điểm (simplex), giao thức cửa sổ trượt cho phép bên gởi có thể gởi đi nhiều khung. Giao thức này sử dụng một cửa sổ để cho phép bên gởi theo dõi các khung mà nó được phép gởi đi và các khung mà nó đang chờ báo nhận, gọi là cửa sổ gởi (Sending Windows). Một cửa sổ khác để bên nhận theo dõi các khung mà nó được phép nhận, gọi là cửa sổ nhận (Receiving Windows). Cấu trúc của cửa sổ được mô tả như sau: Phần tô đen là phạm vi của cửa sổ gồm có cửa trước và cửa sau cùng di chuyển theo một chiều. Kích thước của cửa sổ là chiều của cung giới hạn từ cửa sau đến cửa trước. Kích thước của cửa sổ có thể thay đổi. Khi cửa trước di chuyển, cửa sổ được mở rộng ra. Ngược lại khi cửa sau di chuyển, kích thước của cửa sổ bị thu hẹp lại và nó làm cho cửa sổ thay đổi vị trí, trượt / quay H4.7 Cấu trúc cửa sổ trượt quanh một tâm của vòng tròn. Kích thước nhỏ nhất của cửa số là 0, khi đó cửa trước và cửa sau nằm cùng một vị trí. Giả sử, có n=2k vị trí cho các cửa, khi đó kích thước tối đa của cửa sổ là n-1 (không là n để phân biệt với kích thước là 0). Giả sử ta dùng k bit để đánh số thứ tự cho các khung. Ta sẽ có 2k khung, đánh số từ 0 đến 2k-1. Khi đó cửa sổ trượt sẽ được chia thành 2k vị trí tương ứng với 2k khung. Đối với cửa sổ gởi, các vị trí nằm trong cửa sổ trượt biểu hiện số thứ tự của các khung mà bên gởi đang chờ bên nhận báo nhận. Phần bên ngoài cửa sổ là các khung có thể gởi tiếp. Tuy nhiên phải đảm bảo rằng, cửa sổ gởi không được vượt quá kích thước tối đa của cửa sổ. Đối với bên nhận, các vị trí nằm trong cửa sổ biểu hiện số thứ tự các khung mà nó đang sẵn sàng chờ nhận. Kích thước tối đa của cửa sổ biểu thị dung lượng bộ nhớ đệm của bên nhận có thể lưu tạm thời các gói tin nhận được trước khi xử lý chúng. Giả sử bên nhận có một vùng bộ nhớ đệm có khả năng lưu trữ 4 khung nhận được. Khi đó, kích thước tối đa của cửa sổ sẽ là 4.

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

4.4.4 Hoạt động của cửa sổ trượt
Ví dụ sau mô tả hoạt động của cửa sổ trượt với kích thước cửa sổ là 1, sử dụng 3 bits để đánh số thứ tự khung (từ 0 đến 7).

H4.8 Hoạt động của cửa sổ trượt

Khởi đầu, Hình (a): Bên gởi: chưa gởi khung nào nên kích thước của cửa sổ là 0. Bên nhận đang chờ nhận khung 0, kích thước cửa sổ là 1 Bên gởi gởi khung số 0: Nó kiểm tra kích thước của cửa số trượt là 0, nhỏ hơn kích thước tối đa nên nó được phép gởi. Cửa trước của cửa sổ gởi di chuyển lên một bước chứa giá trị 0 là số thứ tự của khung báo nhận bên gởi đang chờ. Kích thước cửa sổ trượt lúc này là 1, đạt đến kích thước tối đa nên nó không được phép gởi thêm khung nữa (Hình b). Bên nhận nhận được khung 0: nó kiểm tra và nhận thấy khung không có lỗi. Nó gởi khung báo nhận số 0 về cho bên nhận. Đồng thời cửa sau của nó di chuyển để loại khung số 0 ra khỏi cửa sổ trượt. Cửa trước cũng di chuyển để mở rộng kích thước cửa sổ đến giá trị tối đa. Lúc này cửa sổ nhận chứa khung số 1 là khung mà nó đang chờ nhận tiếp (Hình c). Bên gởi nhận được khung báo nhận số 0: Vì đây là khung báo hiệu bên nhận đã nhận tốt nên cửa sau của cửa sổ gởi di chuyển để loại khung số 0 ra khỏi cửa sổ gởi. Lúc này cửa sổ gởi có kích thước là 0, bên gởi có quyền gởi tiếp khung (Hình d) Như vậy khi kích thước của cửa sổ trượt là 1, ta có giao thức stop-and-wait.

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

46

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

4.4.5 Cài đặt giao thức cửa sổ trượt kích thước 1 bit (A One-Bit Sliding Window Protocol)
/* Kích thước cửa sổ là 1 */

/* Số thứ tự của khung gởi đi kế tiếp */ /* Số thứ tự của khung báo nhận đang chờ nhận */ /* Khung nhận và khung gởi */ /* Gói tin chờ gởi */ /* Khởi động số thứ tự khung gởi */ /* Khởi động số thứ tự khung báo nhận chờ nhận */ /* Nhận gói tin từ tầng mạng để gởi đi */ /* Đưa gói tin dữ liệu vào khung để gởi */ /* Đặt số thứ tự cho khung */ /* Đặt số thứ tự báo nhận vào khung */ /* Đưa khung xuống tầng vật lý để gởi */ /* Khởi động bộ đếm thời gian */ /* Chờ sự kiện Khung đến, Khung bị lỗi, quá thời gian */ /* Một khung đến không bị lỗi */ /* Nhận khung từ tầng vật lý */ /* Kiểm tra có phải là khung đang chờ nhận không */ /* Lấy gói tin ra khỏi khung và chuyển lên tầng mạng */ /* Tăng số thứ tự của khung chờ nhận kế tiếp */ /* Nếu bên kia đã báo nhận khung vừa gởi */ /* Xóa bộ đếm thời gian */ /* Nhận gói tin kế tiếp từ tầng mạng để gởi đi */ /* Tăng số thứ tự của khung kế tiếp */ /* Đưa gói tin vào khung để gởi */ /* Đặt số thứ tự cho khung gởi */ /* Đặt số thứ tự khung báo nhận */ /* Đưa khung xuống tầng vật lý để gởi */ /* Khởi động bộ đếm thời gian */

P4.4 Cài đặt cửa sổ trượt với kích thước là 1

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

47

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

4.4.6

Ví dụ về 2 kịch bản của giao thức trên

(a): Việc gởi nhận diễn ra bình thường theo đúng tuần tự (b): Việc gởi nhận diễn ra theo một trình tự bất kỳ Ký hiệu A send (seq, ack, packet number) để chỉ rằng A gởi B một khung có số thứ tự là seq, đồng thời báo cho B biết A đã nhận được tốt khung có số thứ tự ack của B gởi sang. Khung chứa gói tin thứ packet number. Dấu * biểu thị rằng khung tốt, và gói tin được lấy ra khỏi khung để chuyển cho tầng mạng.

H4.9 Kịch bản giao thức cửa sổ trượt với kích thước là 1

1.1.1 Vấn đề điều khiển lỗi (Error Control)
Vấn đề kế tiếp cần phải quan tâm là bên nhận sẽ làm gì nếu khung bị lỗi. Giải pháp đơn giản là truyền lại tất cả các khung bắt đầu từ khung thứ N bị lỗi. Nếu có những khung khác được nhận trong khoảng thời gian này thì chúng đều bị bỏ qua. Đây gọi là giao thức Go-Back-N. Giải pháp thứ hai là chỉ truyền lại những khung bị lỗi, và chờ đến khi nó được gởi lại trước khi tiếp tục việc gởi tin, gọi là giao thức Selective Repeat.

4.4.6.1

Giao thức Go-Back-N

Giao thức Go-Back-N thì rất đơn giản. Khi một khung bị lỗi. Bên nhận bỏ qua khung. Vì không một báo nhận nào gởi về cho bên nhận nên sự kiện quá thời gian xảy ra, bên gởi phải gởi lại ung bị lỗi và toàn bộ các khung phía sau nó.

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

48

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

Ví dụ:

H4.10 Giao thức Go-Back-N

Trong ví dụ trên, bên nhận phát hiện ra khung số 2 bị lỗi nó bỏ qua các khung sau đó (3,4,5,6,7,8), chỉ chờ nhận lại khung số 2. Phía bên gởi chờ báo nhận từ bên nhận cho đến khi quá thời gian, nó sẽ thực hiện gởi lại các khung 2, 3, 4, 5, 6, .... Đoạn chương trình sau cài đặt giao thức Go-Back-N /* Giao thức này cho phép nhiều khung được gởi đi. Bên gởi có thể gởi trước đến MAX_SEQ khung mà không cần chờ một báo nhận. Điểm lưu ý khác là tầng mạng không phải luôn luôn có dữ liệu sẵn sàng để gởi. Khi nào có dữ liệu để gởi, tầng mạng sẽ sinh ra một sự kiện network-layer- ready.*/ k
/* Kích thước lớn nhất của cửa sổ trượt, phải là 2 -1*/

/*

True nếu a<=b<c

*/

/*

Tạo khung gởi gói tin đi

*/ /* Khung để gởi gói tin đi */ /* Đưa gói tin vào khung */ /* Đặt số thứ tự cho khung gởi*/ /* Đặt số thứ tự cho khung cần báo nhận /* Gởi khung xuống tầng vật lý để truyền đi */ /* Khởi động bộ đếm thời gian cho khung gởi đi*/

/* Số thứ tự cho khung gởi kế tiếp */ /* Khung lâu nhất chưa được báo nhận */ /* Khung chờ nhận kế tiếp / /* Khung */ /* Vùng bộ nhớ đệm cho các khung gởi đi */ /* Số lượng bộ nhớ đệm đang được dùng */ /* Chỉ số mảng của vùng nhớ đệm */

/* Cho phép tầng mạng tạo sự kiện network_layer_ready */ /* Đặt báo nhận đầu tiên chờ nhận là 0 */ /* Khung đầu tiên gởi đi là 0 */ Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

49

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0 /* Chờ 1 trong 4 sự kiện liệt kê ở trên xảy ra */ /* Tầng mạng có một gói tin cần gởi đi */ /* Chấp nhận, lưu và truyền đi một khung mới */

/* Nhận khung từ tầng vật lý*/ /* Tăng kích thước cửa sổ gởi */ /* Gởi khung đi */ /* Di chuyển cửa trước của cửa sổ gởi */

/* Một khung dữ liệu hay điều khiển vừa đến */ /* Nhận khung từ tầng vật lý */ /* Là khung đang được chờ đợi */ /* Chuyển gói tin lên tầng mạng */ Di chuyển cửa sau của cửa sổ nhận */ /* Nếu là Ack thứ n, sẽ không quan tâm đến các ACK n-1, n-2, ... */ /* Xử lý các báo nhận */

/* Giảm kích thước cửa sổ gởi */ /* Khung đã đến, xóa bộ đếm thời gian */ /* Tăng số thứ tự khung chờ nhận kế tiếp */

/* Khung nhận bị lỗi, bỏ qua */ /* Quá thời gian, truyền lại tất cả các khung đang chờ báo nhận */ /* Bắt đầu truyền lại */ /* Truyền lại */ /* Chuẩn bị để truyền khung kế tiếp */

/* Vùng đệm còn khả năng chứa gói tin ? */

P4.5 Cài đặt giao thức Go-Back-N

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

50

4.4.6.2 Giao thức Selective Repeat

Trong giao thức này, khung bị lỗi bị bỏ đi, nhưng các khung nhận tốt sau đó đều được lưu lại tạm thời trong vùng nhớ đệm. Khi quá thời gian, bên gởi chỉ gởi lại khung cũ nhất chưa được báo nhận. Nếu khung này đến nơi chính xác, bên nhận có thể chuyển lên tầng mạng tất cả các khung đã được lưu vào bộ nhớ đệm theo đúng thứ tự. Trong giao thức này, bên nhận sử dụng khung Báo không nhận NAK (Negative Acknowledge) khi phát hiện ra khung bị lỗi, ví dụ lỗi CRC, sai thứ tự gói tin. NAK sẽ được gởi về bên nhận trước khi sự kiện quá thời gian báo nhận của khung bị lỗi xảy ra. Nhờ đó tăng được hiệu xuất truyền tin.

H4.11 Giao thức Selective Repeat với cửa sổ trượt lớn hơn 1

Trong ví dụ trên các khung 0, 1 được nhận tốt và đã được báo nhận, còn khung số 2 thì bị lỗi trên đường truyền. Khi khung số 3 đến, tầng liên kết dữ liệu phát hiện lỗi về số thứ tự khung chờ nhận, vì thế nó gởi khung NAK cho khung số 2 và lưu tạm thời khung số 3 vào vùng nhớ đệm. Tương tự, các khung 4 và 5 cũng được lưu lại mà chưa chuyển lên tầng mạng (vì phải chờ nhận khung số 2). Khi khung NAK 2 đến bên gởi, nó truyền lại ngay khung số 2. Khi khung số 2 đến bên nhận, nó đã có đủ các khung 2,3,4,5 theo đúng thứ tự vì thế nó chuyển 4 khung này lên tầng mạng theo một thứ tự đúng đắn. Đồng thời bên nhận gởi về bên gởi khung ACK 5 để báo rằng đã nhận tốt đến khung số 5. Trong trường hợp khung NAK2 bị mất, không đến được bên gởi, thì sự kiện quá thời gian sẽ xảy ra. Khi đó bên gởi cũng chỉ gởi lại khung số 2 mà thôi.

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

/* Giao thức này chấp nhận các khung đến không đúng thứ tự, nhưng chúng lại được chuyển lên tầng mạng theo một thứ tự đúng đắn. Với mỗi khung gởi đi, sẽ có một bộ đếm thời gian đi kèm. Khi quá thời hạn chỉ khung tương ứng được gởi lại, thay vì gởi lại tất cả các khung như giao thức Go-Back-N */
/* Số thứ tự khung lớn nhất*/ /* Kích thước tối đa cửa sổ gởi và nhận /* Chưa gởi khung NAK*/ /* Khung cũ nhất đã gởi */ Kiểm tra b có là giá trị giữa a và c không

/* Tạo và gởi khung dữ liệu / báo nhận / báo lỗi */ /* Khung */ /* Kiểu khung: data, ack, nak */ /* Đặt số thứ tự cho khung dữ liệu gởi đi */ /* Chỉ gởi 1 NAK cho một khung */ /* Gởi khung đi */
/* Khởi động bộ đếm thời gian cho khung dữ liệu gởi */

* Ngừng bộ đếm thời gian chờ báo nhận*/

/* Khung chờ được báo nhận */ /* Khung kế tiếp gởi đi */ /* Khung đang chờ nhận */ /* Khung kế tiếp chưa được nhận */ /* Chỉ số vùng nhớ tạm */ /* Khung nhận và gởi */ /* Vùng đệm cho dữ liệu gởi */ /* Vùng đệm cho dữ liệu nhận */ /* Theo dõi sử dụng vùng đệm dữ liệu nhận */ /* Số lượng vùng đệm gởi đang được sử dụng */ /* Gán giá trị khởi động */

/* Khởi tạo các vùng đệm nhận rỗng */

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

52

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

/* Chờ 1 trong 5 sự kiện phát sinh */ /* Nhận, lưu và truyền một khung mới */ /* Mở rộng kích thước cửa sổ gởi */ /* Nhận gói tin từ tầng mạng */ * Gởi khung đi */ /* Tăng số thứ tự khung gởi kế tiếp */ /* Một khung dữ liệu hoặc điều khiển vừa đến */ /* Nhận khung từ tầng vật lý */ /* Là khung dữ liệu có lỗi thì gởi khung NAK, ngược lại tính giờ để gởi khung ACK */

/* Là khung có thứ tự chấp nhận và chưa được lưu dữ liệu lại*/ /* Đưa dữ liệu vào vùng đệm */ /* Đánh dấu vùng đệm đã sử dụng */ /* Chuyển tất cả các khung đang trong vùng đệm lên tầng mạng và mở rộng cửa sổ nhận */

/* Di chuyển cửa sau cửa sổ nhận */ /* Di chuyển cửa trước cửa sổ nhận */ /* Khởi động đồng hồ cho các báo nhận */

/* Giảm kích thước cửa sổ gởi */ /* Khung đã đến nơi thật sự */ /* Di chuyển cửa dưới của cửa sổ gởi */

/* Khung bị lỗi */ /* Bên gởi xử lý chậm */ /* Quá thời gian cho các báo nhận */

P4.6 Cài đặt giao thức Selective-Repeat

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

53

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

Một số điểm cần lưu ý khi sử dụng cửa số trượt với kích thước lớn hơn 1:
4.4.6.1.1 Kích thước tối đa của cửa sổ gởi và nhận là bao nhiêu ?

Giả sử ta dùng 3 bit để đánh số cho khung. Như vậy bên gởi được phép gởi trước tối đa 7 khung trước khi chờ bên nhận gởi báo nhận về.

H4.11 Giao thức cửa số trượt với kích thước là 7

o Lúc đầu bên gởi gởi đi 7 khung từ 0 đến 6, bên nhận đang sẵn sàng chờ nhận bất kỳ một khung nào có số thứ tự từ 0 đến 6 (Hình a). o Tất cả các khung đến nơi không có lỗi, bên nhận gởi các báo nhận và chuyển cửa số nhận về vị trí sẵn sàng để nhận các khung 7,0,1,2,3,4 và 5 (Hình b). o Tại thời điểm đó, đường truyền có sự cố làm cho tất cả các khung báo nhận đều mất. Quá thời gian, bên gởi gởi lại khung 0. Khi khung này đến bên nhận, nó kiểm tra xem khung có nằm trong cửa sổ nhận không. Điều không may mắn đã xảy ra: khung 0 nằm trong cửa sổ nhận mới (Hình b). Bên nhận nhận khung 0 xem như một khung mới hoàn toàn và chuyển khung 0 lên tầng mạng. Như vậy tầng mạng đã nhận 2 lần cùng một gói tin, tức giao thức vận hành sai. o Tình trạng này có thể tránh được nếu ta đảm bảo rằng cửa sổ nhận mới không đè chồng lên cửa sổ trước đó. Điều này có thể thực hiện được nếu ta giới hạn kích thước tối đa của của sổ nhận bằng một nửa khoảng đánh số thứ tự của khung. o Ví dụ: Nếu dùng 3 bit để đánh số thứ tự khung từ 0 đến 7 thì kích thước tối đa cửa sổ nhận là (7-0+1)/2 =4. o Nếu dùng 4 bit để đánh số thứ tự khung từ 0 đến 15 thì kích thước tối đa cửa sổ nhậnt là (15-0+1)/2 =8.

4.4.6.2.1 Số lượng buffer để lưu khung là bao nhiêu?
Số lượng buffer chỉ cần bằng kích thước tối đa của cửa sổ nhận, không cần thiết phải bằng số lượng khung. Ví dụ: Nếu dùng 3 bit để đánh số thứ tự khung từ 0 đến 7 thì kích thước tối đa cửa sổ nhận là (7-0+1)/2 =4 và số lượng buffer cần thiết cũng là 4.

4.4.6.2.2 Khi nào gởi báo nhận cho một gói tin?
Ta thấy rằng, khi một khung đến, báo nhận của khung này sẽ không được gởi ngược về một cách tức thì. Thay vào đó, nó sẽ được gởi kèm trong khung dữ liệu kế tiếp của bên nhận. Nếu bên nhận không có dữ liệu để gởi đi, báo nhận sẽ bị giữ lại khá lâu. Chính vì thế, mỗi khi có khung đến thì bộ đếm thời gian start_ack_timer được khởi động. Nếu trong suốt khoảng thời gian này không có một khung dữ nào cần gởi đi, thì sau đó một khung báo nhận riêng biệt sẽ được gởi đi. Bộ đếm thời gian start_ack_timer sinh ra sự kiện ack_timeout. Chúng ta cũng phải đảm bảo rằng, bộ đếm thời gian start_ack_timer thì ngắn hơn bộ đếm thời gian chờ báo nhận cho các khung dữ liệu.

4.4.7

Giao thức HDLC (High-Level Data Link Control)

Giao thức điều khiển liên kết dữ liệu quan trong nhất là HDLC. Không phải vì nó được sử dụng rộng rãi mà nó còn là cơ sở cho nhiều giao thức điều khiển liên kết dữ liệu khác.

4.4.7.2 Các đặc tính của giao thức HDLC
Giao thức HDLC định nghĩa 3 loại máy trạm, hai cấu hình đường nối kết và 3 chế độ điều khiển truyền tải

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

54

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

4.4.7.2.1 Ba loại trạm trong HDLC
o Trạm chính (Primary Station): Có trách nhiệm điều khiển các thao thác về đường truyền. Các khung được gởi từ trạm chính gọi là lệnh (Command). o Trạm phụ (Secondary Station): Hoạt động dưới sự kiểm soát của trạm chính. Khung gởi từ trạm phụ gọi là các trả lời. Trạm chính duy trì nhiều đường nối kết luận lý đến các trạm phụ trên đường truyền. o Trạm hỗn hợp (Combined Station): Bao gồm đặc điểm của trạm chính và trạm phụ. Một trạm hỗn hợp có thể gởi đi các lệnh và các trả lời.

4.4.7.2.2 Hai cấu hình đường nối kết:
o Cấu hình không cân bằng (Unbalanced Configuration): Gồm một máy trạm chính (Primary Station) và nhiều máy trạm phụ (Secondary station) và hỗ trợ cả 2 chế độ truyền song công và bán song công o Cấu hình cân bằng (Balanced Configuration): Bao gồm 2 máy trạm hỗn hợp, và hỗ trợ cả 2 chế độ truyền song công và bán song công.

4.4.7.2.3 Có 3 chế độ truyền tải là:
o Chế độ trả lời bình thường (NRM- Normal Response Mode), được sử dụng với cấu hình đường nối kết không cân bằng. Máy chính có thể khởi động một cuộc truyền tải dữ liệu về cho máy phụ. Nhưng máy phụ chỉ có thể thực hiện việc truyền dữ liệu cho máy chính như là những trả lời cho các yêu cầu của máy chính. o Chế độ cân bằng bất đồng bộ (ABM - Asynchronous Response Mode): Được sử dụng với cấu hình nối kết cân bằng. Cả hai máy đều có quyền khởi động các cuộc truyền tải dữ liệu mà không cần sự cho phép của máy kia. o Chế độ trả lời bất đồng bộ (ARM-Asynchronous Response Mode): Sử dụng cấu hình không cân bằng. Một máy phụ có thể khởi động một cuộc truyền tải và không cần sự cho phép tường minh của máy chính. Máy chính vẫn đảm trách vai trò bảo trì đường truyền bao gồm việc khởi động, phục hồi lỗi và xóa nối kết. Chế độ NRM đòi hỏi phải có nhiều đường dây để nối một máy chính với nhiều thiết bị đầu cuối. Chế độ ABM được sử dụng nhiều nhất trong 3 chế độ, nó cho phép sử dụng hiệu quả đường truyền. Chế độ ARM thì ít được dùng đến.

4.4.7.3 Cấu trúc khung
HDLC sử dụng chế độ truyền tải đồng bộ, các bits dữ liệu truyền đi được gói vào trong các khung và sử dụng một cấu trúc khung cho tất cả các loại dữ liệu cũng như thông tin điều khiển. Khung trong giao thức HDLC có cấu trúc như sau:

H4.12 Cấu trúc khung của HDLC

Flag (8 bit) Address (8 bit) Control (8bit) Information (128-1024 bytes)

Là cờ dùng để xác định điểm bắt đầu và kết thúc của khung, giá trị nó là 01111110. HDLC sử dụng kỹ thuật bit độn để loại trừ sự xuất hiện của cờ trong dữ liệu. Vùng ghi địa chỉ để xác định máy phụ được phép truyền hay nhận khung. Được dùng để xác định loại khung. Mỗi loại có thông tin điều khiển khác nhau. Có 3 loại khung: Thông tin (I), Điều khiển (S ) và không đánh số (U). Vùng chứa dữ liệu cần truyền.

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

55

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

Vùng chứa mã kiểm soát lỗi, dùng phương pháp đa thức CRCFCS (Frame Check Sequence- 8 CCITT = X16 + X12 + X5 +1 bit) Giá trị 8 bit của trường control hình thành 3 loại khung như sau:

Khung I

Khung S

Khung U

H4.13 Cấu trúc trường điều khiển trong khung HDLC

Giao thức HDLC sử dụng một cửa sổ trượt với số thứ tự khung 3 bít. Trường seq trong khung I để chỉ số thứ tự của khung thông tin hiện tại. Trường Next để chỉ số thứ tự của khung thông tin mà bên gởi đang chờ nhận ( thay vì là khung đã nhận tốt như giao thứ cửa sổ trượt đã giới thiệu ở phần trước). Bit P/F có ý nghĩa là Poll/Final, tức chọn hoặc kết thúc. Khi máy tính chính mời một máy phụ truyền tin, thì bit này được đặt lên 1 có ý nghĩa là P (Poll, chọn). Ngược lại khi thông tin được truyền từ máy phụ lên máy chính thì nó được đặt xuống 0, để báo với máy chính rằng máy phụ hiện tại vẫn còn dữ liệu để gởi đi. Khi máy phụ gởi khung cuối cùng, bit này được đặt lên 1, có ý nghĩa là F (Final, kết thúc), để báo cho máy chính biết rằng nó đã hoàn thành việc truyền tải thông tin. Khung S (Supervisory Frame) là khung điều khiển, dùng để kiểm soát lỗi và luồng dữ liệu trong quá trình truyền tin. Khung S có 4 kiểu được xác định bởi tổ hợp giá trị của 2 bit trong trường Type. SS=0 RR (Receive Ready), là khung báo nhận, thông báo sẵn sàng 0 nhận dữ liệu, đã nhận tốt đến khung Next-1, và đang đợi nhận khung Next. Được dùng đến khi không còn dữ liệu gởi từ chiều ngược lại để vừa làm báo nhận (figgyback) SS=0 REJ (Reject): đây là một khung báo không nhận (negative 1 acknowledge), yêu cầu gởi lại các khung, từ khung Next. SS=1 RNR (Receive Not Ready): thông báo không sẵn sàng nhận 0 tin, đã nhận đến đến khung thứ Next-1, chưa sẵn sàng nhận khung Next SS=1 SREJ (Selective Reject): yêu cầu gởi lại một khung có số 1 thức tự là Next Khung U (Unnumbered Frame) thường được sử dụng cho mục đích điều khiển đường truyền, nhưng đôi khi cũng được dùng để gởi dữ liệu trong dịch vụ không nối kết. Các lệnh của khung U được mô tả như sau:

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

56

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

1111P100 1100P001 1111P000 1100P010 1100F110 1100F001

Lệnh này dùng để thiết lập chế độ truyền tải SABM (Set Asynchronous Balanced Mode). Lệnh này dùng để thiết lập chế độ truyền tải SNRM (Set Normal Response Mode). Lệnh này dùng để thiết lập chế độ truyền tải SARM (Set Asynchronous Response Mode). Lệnh này để yêu cầu xóa nối kết DISC (Disconnect). UA (Unumbered Acknowledgment). Được dùng bởi các trạm phụ để báo với trạm chính rằng nó đã nhận và chấp nhận các lệnh loại U ở trên. CMDR/FRMR (Command Reject/Frame Reject). Được dùng bởi trạm phụ để báo rằng nó không chấp nhận một lệnh mà nó đã nhận chính xác.

4.4.7.4 Một vài kịch bản về giao thức HDLC
Kịch bản (a) mô tả các khung liên quan trong quá trình thiết lập và xóa nối kết. Đầu tiên một trong hai bên giao tiếp sẽ gởi khung SABM sang bên kia và thiết lập một bộ đếm thời gian. Bên phía còn lại khi nhận được khung SABM sẽ trả lời bằng khung UA. Bên yêu cầu nối kết khi nhận được khung UA sẽ xóa bỏ bộ đếm thời gian. Nối kết đã được hình thành và hai bên có thể truyền khung qua lại cho nhau. Nối kết sẽ xóa đi nếu một trong hai bên giao tiếp gởi khung DISC. Trong một trường hợp khác, nếu sau một khoảng thời gian trôi qua, bên yêu cầu nối kết không nhận được khung UA, nó sẽ cố gắng gởi lại khung SABM một số lần qui định. Nếu vẫn không nhận được khung UA, bên yêu cầu nối kết sẽ thông báo lỗi lên tầng cao hơn. Seq A SABM B A I,0,0 I,0,1 SABM UA I,1,3 I,3,2 DISC I,2,4 I,3,4 RR,4 (b) Two way data exchange (c) Busy Condition RR,0,P RR,4,F I,4,0 I,1,1 I,2,1 Next B A I,3,0 RNR,4 R,0,P RNR,4,F B

Time Out

UA

(a) Link Setup and disconnect

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

57

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

Seq A Time Out SABM SABM UA B A

Next B A I,3,0 RNR,4 R,0,P RNR,4,F B

I,0,0 I,0,1 I,1,1 I,2,1 I,1,3 I,3,2

RR,0,P RR,4,F I,4,0

DISC UA (a) Link Setup and disconnect A I,3,0 I,4,0 I,5,0 REJ,4

I,2,4 I,3,4 RR,4 (b) Two way data exchange B A I,2,0 I,3,0 RE,4

(c) Busy Condition B

Time out RR,0,P

I,4,0 RR,3,F I,5,0 I,6,0 I,3,0 RR,4

(d) Reject Recovery

(e) Timeout Recovery

H4.14 Một vài kịch bản của HDLC

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

58

Kịch bản (b) mô tả tiến trình trao đổi khung I giữa hai bên. Ta thấy rằng bên A gởi liên tiếp các khung (I,1,1 và I,2,1) mà không nhận được khung báo nhận thì số thứ tự của khung chờ nhận vẫn không thay đổi, trong trường hợp này là 1. Ngược lại khi bên B nhận liên tiếp các khung (I,1,1 và I,2,1) mà không gởi khung nào đi, thì khung chờ nhận kế tiếp của khung thông tin truyền đi phải là số kế tiếp của khung vừa nhận, là 3. Trong kịch bản (c) máy A không thể xử lý kịp các khung do B gởi đến vì thế nó gởi khung RNR để yêu cầu B tạm dừng việc việc truyền tải. Bên B định kỳ gởi thăm dò bên A bằng cách gởi khung RR với bit P được đặt lên 1. Nếu bên A vẫn chưa thể nhận thông tin từ bên B nó sẽ trả lời bằng khung RNR, ngược lại nếu A đã sẵn sàng thì nó sẽ trả lời bằng khung RR. Trong kịch bản (d), bên A gởi sang B ba khung thông tin 3,4 và 5. Khung 4 bị mất hoàn toàn trên đường truyền. Khi bên B nhận được khung 5, nó sẽ bỏ qua khung này vì sai thứ tự khung. B gởi REJ với trường Next là 4 để yêu cầu A gởi lại tất cả các khung từ khung số 4. Kịch bản (e) minh họa cách thức phục hồi lỗi dựa vào thời gian (timeout). Khung số 3 bị lỗi và do đó B bỏ nó. B không thể gởi khung REJ vì nó không thể xác định được đó có phải là khung I hay không. Bên A sau một khoảng thời gian trôi qua không thấy khung trả lời từ B, nó sẽ gởi khung RR với bit P=1 để kiểm tra trạng thái của bên kia. Bên B sẽ đáp lại bằng khung RR với trường Next là 3 để báo hiệu khung số 3 đã mất. Sau đó A sẽ truyền lại khung số 3.

4.4.7.5 Giao thức Điểm nối điểm (PPP- Point-to-Point Protocol)
PPP là một giao thức đặc biệt quan trọng trong mạng Internet. Nó cho phép truyền tải thông tin giữa các router trên mạng hay để cho phép nối các máy tính người dùng vào mạng của nhà cung cấp dịch vụ Internet (ISP).

H4.15 Sơ đồ nối kêt của giao thức PPP

Giao thức PPP được định nghĩa trong RFC (Request For Comments) 1661 và sau đó được mở rộng thêm bằng các RFC 1662, RFC 1663. PPP thực hiện chức năng phát hiện lỗi trên dữ liệu truyền, hỗ trợ nhiều giao thức vận hành trên nó, phân phối địa chỉ IP khi máy tính nối kết vào mạng, kiểm tra quyền đăng nhập và nhiều tính năng khác. PPP cung cấp 3 đặc tính sau: Định nghĩa một phương pháp định khung cùng với phương pháp phát hiện lỗi. 1. Giao thức điều khiển đường truyền cho phép thiết lập kênh giao tiếp, kiểm tra kênh, thỏa thuận về các thông số truyền tin và xóa kênh truyền khi không cần thiết nữa. Giao thức này được gọi là giao thức LCP ( Link Control Protocol). 2. Có phương pháp thương lượng về các tùy chọn tầng mạng một cách độc lập với giao thức mạng được sử dụng. Phương pháp được chọn lựa NCP (Network Control Protocol) khác nhau cho mỗi giao thức mạng. Để hiểu rõ về giao thức PPP, ta xét trường hợp quay số nối kết máy tính ở nhà vào mạng của một ISP.

Đầu tiên máy tính các nhân sẽ quay số thông qua modem đến router của ISP. Router sẽ tiếp nhận cuộc gọi và một nối kết vật lý được hình thành. Máy tính sẽ gởi một loạt các gói tin theo giao thức LCP trong một hoặc nhiều khung của giao thức PPP để thỏa thuận về các thông số mà PPP sẽ sử dụng. Sau đó một loạt các gói tin của giao thức NCP sẽ được gởi đi để thực hiện cấu hình tầng mạng. Thông thường máy tính muốn sử dụng giao thức TCP/IP nên nó cần một địa chỉ IP. Giao thức NCP sẽ gán địa chỉ IP cho máy tính. Từ lúc này, máy tính đóng vai trò như một máy trên mạng Internet. Nó có thể gởi và nhận các gói tin của giao thức IP. Khi người dùng kết thúc, NCP xóa đi nối kết của tầng mạng và giải phóng địa chỉ IP của máy tính để sử dụng cho các máy tính khác nối vào sau đó. Giao thức LCP sẽ xóa nối kết của tầng liên kết dữ liệu. Và cuối cùng máy tính sẽ yêu cầu modem kết thúc cuộc gọi (Hang up) và giải phóng nối kết ở tầng vật lý. Khung của giao thức PPP tương tự như khung của giao thức HDLC, tuy nhiên đây là khung theo kiểu hướng ký tự. Nó sử dụng kỹ thuật byte độn.

H4.16 Cấu trúc khung của giao thức PPP

PPP sử dụng byte đặc biệt 01111110 để làm cờ đánh dấu điểm bắt đầu và kết thúc của khung. Địa chỉ 11111111 để chỉ rằng tất cả các trạm đều nhận khung. Nhờ đó giao thức LCP không cần thiết phải đánh địa chỉ cho các trạm. Trường Control có giá trị 00000011 để biểu thị rằng giao thức không sử dụng cơ chế báo nhận dựa trên số thứ tự của khung. Trường Protocol để xác định phần gói tin được chứa đựng trong phần Payload được định nghĩa bởi giao thức mạng nào. Mỗi protocol đã được qui định một giá trị riêng. Bit đầu tiên là 0 được sử dụng cho các giao thức mạng IP, IPX, OSI CLNP, XNS. Kích thước mặc định là 2 bytes, tuy nhiên giao thức LCP có thể thỏa thuận để sử dụng 1 byte. Payload là nơi chứa gói tin với chiều dài khác nhau. Chiều dài tối đa mặc định là 1500 bytes, tuy nhiên LCP có thể thỏa thuận để thay đổi. Cuối cùng là trường checksum dùng để kiểm tra lỗi trong khung.

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

Chương 5: MẠNG NỘI BỘ & LỚP CON ĐIỀU KHIỂN TRUY CẬP
Mục đích
Chương này nhằm giới thiệu với người học những nội dung sau: • Các phương chia sẻ đường truyền chung giữa các máy tính trong một mạng cục bộ như: các phương pháp chia kênh, các phương pháp truy cập đường truyền ngẫu nhiên và các phương pháp phân lượt truy cập đường truyền. • Giới thiệu chi tiết về nguyên tắc hoạt động của các chuẩn mạng cục bộ như họ các chuẩn mạng Ethernet, FDDI và mạng không dây

Yêu cầu
Sau khi học xong chương này, người học phải có được các khả năng sau: • Trình bày được sự khác biệt cơ bản về cách thức chia sẻ đường truyền chung giữa các máy tính trong các phương pháp chia kênh, truy cập đường truyền ngẫu nhiên và phân lượt truy cập đường truyền. • Trình bày được nguyên tắc chia sẻ đường truyền chung giữa các máy tính theo các phương pháp FDMA, TDMA, CDMA, ALOHA, CSMA, CAMA/CD, Token Passing, … • Trình bày được những đặc điểm và nguyên tắc hoạt động của các chuẩn thuộc họ mạng Ethernet, mạng FDDI và chuẩn mạng không dây 802.11

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

61

5.1 Tổng quan về LAN

Như đã trình bày trong phần 2.1, theo tiêu chí đánh giá là khoảng cách địa lý thì người ta thường phân loại mạng máy tính thành ba kiểu: Mạng nội bộ - Local Area Network (LAN) Mạng đô thị - Metropolitan Area Network (MAN) Mạng diện rộng - Wide Area Network (WAN) Trong thực tế, LAN và WAN thường được cài đặt nhất. Mạng LAN được sử dụng để nối kết một dãi rộng các thiết bị trong một phạm vi hẹp, ví dụ: trên cùng một tầng, một tòa nhà hay một khuôn viên (thường không vượt quá 10Km). Ngày nay, LAN là loại mạng được sử dụng rất phổ biến trong mọi lĩnh vực của xã hội. Người ta thường nghĩ đến LAN như là mạng có thông lượng cao, độ trì hoãn thấp. Hiện tại có rất nhiều công nghệ xây dựng mạng LAN mà chúng ta sẽ xem xét đến ngay sau đây. Nhiều chuẩn mạng LAN đã được phát triển trong đó Ethernet và FDDI là phổ biến nhất. Người ta thường gọi chung họ các chuẩn mạng LAN là IEEE 802. Về góc độ kỹ thuật, LAN có các tính chất quan trọng sau: Tất cả các host trong mạng LAN cùng chia sẻ đường truyền chung. Do đó chúng hoạt động dựa trên kiểu quảng bá (broadcast). Không yêu cầu phải có hệ thống trung chuyển (routing/switching) trong một LAN đơn. Thông thường, một mạng LAN được định nghĩa dựa trên các thông số sau: Hình thái (topology): Chỉ ra kiểu cách mà các host trong mạng được đấu nối với nhau. Đường truyền chia sẻ (xoắn đôi, đồng trục, cáp quang): Chỉ ra các kiểu đường truyền mạng (network cables) được dùng để đấu nối các host trong LAN lại với nhau. (Xin xem lại mô tả chi tiết các kiểu đường truyền trong chương Tầng Vật Lý). Kỹ thuật truy cập đường truyền (Medium Access Control - MAC): Chỉ ra cách thức mà các host trong mạng LAN sử dụng để truy cập và chia sẻ đường truyền mạng. MAC sẽ quản trị việc truy cập đến đường truyền trong LAN và cung cấp cơ sở cho việc định danh các tính chất của mạng LAN theo chuẩn IEEE.

5.2 Hình thái mạng

Hình thái mạng sẽ xác định hình dáng tổng quát của một mạng. Hiện tại, người ta đã định nghĩa ra được nhiều hình thái mạng khác nhau tương ứng với những tính chất đặc thù của chúng. Hình thái mạng là tiêu chí bắt buộc dùng để xây dựng mạng LAN và nó chủ yếu quan tâm đến việc làm cho mạng được liên thông, che dấu chi tiết về các thiết bị thực đối với người dùng.

5.2.1 Mạng hình sao

H5.1 Sơ đồ mạng hình sao

Tất cả các máy tính trong mạng được đấu nối tới một thiết bị tập trung tín hiệu trung tâm. Thành phần trung tâm của mạng được gọi là Hub. Phương thức hoạt động của mạng hình sao như sau: Mọi máy tính đều phát tín hiệu ra Hub và Hub phát lại tín hiệu vào đến tất cả các đầu ra. Mỗi máy tính có một nối kết riêng lẻ đến Hub

5.2.2 Mạng hình vòng

H5.2 Sơ đồ mạng hình vòng

Không có thiết bị trung tâm trong sơ đồ nối mạng hình vòng. Đường nối kết mạng sẽ đi trực tiếp từ một máy tính đến máy tính khác. Thực tế, có một đoạn cable ngắn nối máy tính với vòng.

5.2.3 Mạng hình bus

H5.3 Sơ đồ mạng hình bus

Trong sơ đồ mạng hình bus, người ta dùng một dây cáp (cable) đơn nối kết toàn bộ LAN. Mỗi máy tính có một đầu nối đến cáp được chia sẻ. Với một đường truyền chia sẻ như thế thì sẽ có khả năng đụng độ xảy ra khi các máy tính cùng phát tín hiệu ra đường truyền cùng một lúc. Do đó, phải có giải pháp làm cho các máy tính hoạt động đồng bộ với nhau nhằm cho phép chỉ một máy tính truyền thông tin tại một thời điểm.

5.3 Lớp con MAC (Media Access Control Sublayer)
Như đã trình bày ở trên, chương này trình bày về mạng LAN – mạng dạng truyền quảng bá và các giao thức truyền quảng bá của nó. Trong bất kỳ mạng dạng quảng bá nào, vấn đề then chốt luôn là cách thức người ta quyết định ai có quyền truy cập kênh truyền tại một thời điểm. Để làm rõ vấn đề hơn, hãy xem xét ví dụ sau: Có sáu người đang họp thông qua hệ thống điện thoại, mọi người đều được nối kết để có thể nghe và nói với những người khác. Khi một người ngừng nói mà có hai người hoặc nhiều hơn cùng phát biểu tiếp sẽ tạo ra tình trạng lộn xộn. Trong các cuộc họp dạng gặp mặt trực tiếp, tình trạng lộn xộn này có thể được giải quyết bằng cách đưa tay xin phát biểu. Nhưng trong hệ thống hội thảo thông qua điện thoại này, khi mà đường truyền rảnh, việc quyết định ai sẽ nói tiếp có vẻ khó làm hơn. Đã có nhiều giao thức dùng giải quyết vấn đề trên. Và chúng chính là nội dung trình bày của phần này. Nói một cách khác, các kênh truyền dạng quảng bá thỉnh thoảng còn được gọi là các kênh đa truy cập (multiaccess channels) hay là các kênh truy cập ngẫu nhiên (random access channels). Các giao thức được sử dụng để quyết định ai có quyền truy cập đường truyền quảng bá trước được gom vào trong một lớp con của tầng liên kết dữ liệu gọi là lớp con MAC. Lớp con MAC là đặc biệt quan trọng trong mạng LAN, do nhiều mạng LAN sử dụng đường truyền dạng quảng bá như là phương tiện truyền thông nền tảng. Các mạng WAN, theo xu hướng ngược lại, lại dùng các nối kết dạng điểm-điểm (ngoại trừ các mạng dùng vệ tinh). Về cơ bản, có ba phương pháp điều khiển truy cập đường truyền: Chia kênh, truy cập ngẫu nhiên (Random Access) và phân lượt (“Taking-turns”). Giải thích cụ thể về ba phương pháp điều khiển truy cập đường truyền trên sẽ được trình bày ngay sau đây.

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

63

5.3.1 Phương pháp chia kênh
Ý tưởng chung của phương pháp này là: đường truyền sẽ được chia thành nhiều kênh truyền, mỗi kênh truyền sẽ được cấp phát riêng cho một trạm. Có ba phương pháp chia kênh chính: FDMA, TDMA, CDMA.

5.3.1.1

Chia tần số (FDMA – Frequency Division Multiple Access)

Một phương thức truyền thống để chia sẻ một kênh truyền đơn cho nhiều người dùng cạnh tranh là Chia tần số (FDMA). Phổ của kênh truyền được chia thành nhiều băng tần (frequency bands) khác nhau. Mỗi trạm được gán cho một băng tần cố định. Những trạm nào được cấp băng tần mà không có dữ liệu để truyền thì ở trong trạng thái nhàn rỗi (idle). Ví dụ: Một mạng LAN có sáu trạm, các trạm 1, 3, 4 có dữ liệu cần truyền, các trạm 2, 5, 6 nhàn rỗi.

H5.4 Mạng FDMA

Nhận xét: Do mỗi người dùng được cấp một băng tần riêng, nên không có sự đụng độ xảy ra. Khi chỉ có số lượng người dùng nhỏ và ổn định, mỗi người dùng cần giao tiếp nhiều thì FDMA chính là cơ chế điều khiển truy cập đường truyền hiệu quả. Tuy nhiên, khi mà lượng người gởi dữ liệu là lớn và liên tục thay đổi hoặc đường truyền vượt quá khả năng phục vụ thì FDMA bộc lộ một số vấn đề. Nếu phổ đường truyền được chia làm N vùng và có ít hơn N người dùng cần truy cập đường truyền, thì một phần lớn phổ đường truyền bị lãng phí. Ngược lại, có nhiều hơn N người dùng có nhu cầu truyền dữ liệu thì một số người dùng sẽ phải bị từ chối không có truy cập đường truyền vì thiếu băng thông. Tuy nhiên, nếu lại giả sử rằng số lượng người dùng bằng cách nào đó luôn được giữ ổn định ở con số N, thì việc chia kênh truyền thành những kênh truyền con như thế tự thân là không hiệu quả. Lý do cơ bản ở đây là: nếu có vài người dùng rỗi, không truyền dữ liệu thì những kênh truyền con cấp cho những người dùng này bị lãng phí. Có thể dễ dàng thấy được hiệu năng nghèo nàn của FDMA từ một phép tính theo lý thuyết xếp hàng đơn giản. Bắt đầu là thời gian trì hoãn trung bình T trong một kênh truyền có dung lượng C bps, với tỉ lệ đến trung bình là λ khung/giây, mỗi khung có chiều dài được chỉ ra từ hàm phân phối mũ với giá trị trung bình là 1/μ bit/khung. Với các tham số trên ta có được tỉ lệ phục vụ là μC khung/giây. Từ lý thuyết xếp hàng ta có:

$$T = \frac{1}{\mu C - \lambda}$$

Ví dụ: nếu C = 100 Mbps, 1/μ = 10000 bits và λ = 5000 khung/giây thì T = 200 μs. Bây giờ nếu ta chia kênh lớn này thành N kênh truyền nhỏ độc lập, mỗi kênh truyền nhỏ có dung

lượng C/N bps. Tỉ lệ trung bình các khung đến các kênh truyền nhỏ bây giờ là λ/N. Tính toán lại T chúng ta có:

TFDMA =

1 μ (C / N )−(λ / N )

=

N μC − λ

= NT

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

64

Thời gian chờ đợi trung bình trong các kênh truyền con sử dụng FDMA là xấu hơn gấp N lần so với trường hợp ta sắp xếp cho các khung được truyền tuần tự trong một kênh lớn.

5.3.1.2

Chia thời gian (TDMA – Time Division Multiple Access)

Trong phương pháp này, các trạm sẽ xoay vòng (round) để truy cập đường truyền. Vòng ở đây có thể hiểu là vòng thời gian. Một vòng thời gian là khoảng thời gian đủ để cho tất cả các trạm trong LAN đều được quyền truyền dữ liệu. Qui tắc xoay vòng như sau: một vòng thời gian sẽ được chia đều thành các khe (slot) thời gian bằng nhau, mỗi trạm sẽ được cấp một khe thời gian – đủ để nó có thể truyền hết một gói tin. Những trạm nào tới lượt được cấp cho khe thời gian của mình mà không có dữ liệu để truyền thì vẫn chiếm lấy khe thời gian đó, và khoảng thời gian bị chiếm này được gọi là thời gian nhàn rỗi (idle time). Tập hợp tất cả các khe thời gian trong một vòng được gọi lại là khung (frame). Ví dụ:

H5.5 Mạng TDMA

Mạng LAN dùng cơ chế truy cập đường truyền TDMA trên có sáu trạm. Các trạm 1, 3, 4 có dữ liệu cần truyền. Các trạm 2, 5, 6 nhàn rỗi. Chúng ta cũng áp dụng cùng một nhận xét về mạng TDMA như mạng FDMA. Mỗi người dùng được cấp phát một khe thời gian. Và nếu người dùng không sử dụng khe thời gian này để truyền dữ liệu thì thời gian sẽ bị lãng phí.

5.3.1.3

Kết hợp giữa FDMA và TDMA

Trong thực tế, hai kỹ thuật TDMA và FDMA thường được kết hợp sử dụng với nhau, ví dụ như trong các mạng điện thoại di động. Các điện thoại di động TDMA sử dụng các kênh 30 KHz, mỗi kênh lại được chia thành ba khe thời gian. Một thiết bị cầm tay sử dụng một khe thời gian cho việc gởi và một khe khác cho việc nhận dữ liệu. Chẳng hạn như các hệ thống: Cingular (Nokia 8265, TDMA 800/ 1900 MHz, AMPS 800 mHz ), AT&T Wireless. Hệ thống GSM sử dụng các kênh 200 KHz được chia thành 8 khe thời gian. Một thiết bị cầm tay sẽ sử dụng một khe thời gian trong hai kênh khác nhau để gởi và nhận thông tin. Các hệ thống Cingular, T-Mobile, AT&T đang chuyển sang dùng kỹ thuật này.

H5.6 Kết hợp giữa TDMA và FDMA

5.3.1.4

Phân chia mã (CDMA – Code Division Multiple Access)

CDMA hoàn toàn khác với FDMA và TDMA. Thay vì chia một dãy tần số thành nhiều kênh truyền băng thông hẹp, CDMA cho phép mỗi trạm có quyền phát dữ liệu lên toàn bộ phổ tần của đường truyền lớn tại mọi thời điểm. Các cuộc truy cập đường truyền xảy ra đồng thời sẽ được tách biệt với nhau bởi kỹ thuật mã hóa. CDMA cũng xóa tan lo lắng cho rằng những khung dữ liệu bị đụng độ trên đường truyền sẽ bị biến dạng. Thay vào đó CDMA chỉ ra rằng nhiều tín hiệu đồng

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

65

thời sẽ được cộng lại một cách tuyến tính! Kỹ thuật CDMA thường được sử dụng trong các kênh truyền quảng bá không dây (mạng điện thoại di động, vệ tinh …). Trước khi đi vào mô tả giải thuật CDMA, hãy xem xét một ví dụ gần giống như sau: tại một phòng đợi trong sân bay có nhiều cặp hành khách đang chuyện trò. TDM có thể được so sánh với cảnh tượng: tất cả mọi người đều đứng giữa phòng, chờ đến lượt mình được phát biểu. FDM thì giống như cảnh tượng: mỗi một cặp được sắp vào một ô nói chuyện riêng. Còn CDMA lại giống như cảnh: mọi người đều đứng ngay trong phòng đợi, nói chuyện đồng thời, nhưng mỗi cặp chuyện trò sẽ sử dụng một ngôn ngữ riêng. Cặp nói tiếng Pháp chỉ líu lo với nhau bằng tiếng Pháp, bỏ qua mọi tiếng động không phải là tiếng Pháp và coi đó như là tiếng ồn. Vì thế, vấn đề then chốt trong CDMA là khả năng rút trích ra được tín hiệu mong muốn trong khi từ chối mọi thứ khác và coi đó là tiếng ồn ngẫu nhiên. Trong CDMA, thời gian gởi một bit (bit time) lại được chia thành m khoảng nhỏ hơn, gọi là chip. Thông thường, có 64 hay 128 chip trên một bit, nhưng trong ví dụ phía dưới, chúng ta dùng 8 chip cho đơn giản. Nhiều người dùng đều chia sẻ chung một băng tần, nhưng mỗi người dùng được cấp cho một mã duy nhất dài m bit gọi là dãy chip (chip sequence). Dãy chip này sẽ được dùng để mã hóa và giải mã dữ liệu của riêng người dùng này trong một kênh truyền chung đa người dùng. Ví dụ, sau đây là một dãy chip: (11110011). Để gởi bit 1, người dùng sẽ gởi đi dãy chip của mình. Còn để gởi đi bit 0, người dùng sẽ gởi đi phần bù của dãy chip của mình. Ví dụ với dãy chip trên, khi gởi bit 1, người dùng sẽ gởi 11110011; khi gởi bit 0 thì người dùng sẽ gởi 00001100. Để tiện cho việc minh họa, chúng ta sẽ sử dụng các ký hiệu lưỡng cực sau: bit 0 được ký hiệu là 1, bit 1 được ký hiệu là +1. Cũng cần phải đưa ra một định nghĩa mới: tích trong (inner product): Tích trong của hai mã S và T, ký hiệu là S•T, được tính bằng trung bình tổng của tích các bit nội tại tương ứng của hai mã này.

1 S •T = m
Ví dụ:
S = +1 + 1 + 1 − 1 − 1 + 1 + 1 − 1 T = +1 + 1 + 1 + 1 − 1 − 1 + 1 − 1 S •T =

∑

m

i =1

S iTi

+ 1 + 1 + 1 + (−1) + 1 + (−1) + 1 + 1 1 = 8 2 Bây giờ ta xem xét cách thức cấp phát chuỗi chip cho các trạm, sao cho không gây ra lẫn lộn thông tin giữa các trạm với nhau. Định nghĩa: Hai mã S và T có cùng chiều dài m bits được gọi là trực giao khi: S•T = 0. Ví dụ: S = +1 + 1 − 1 − 1 − 1 − 1 − 1 + 1 T = −1 − 1 + 1 − 1 − 1 − 1 + 1 + 1 (−1) + (−1) + (−1) + 1 + 1 + 1 + (−1) + 1 =0 8 Nếu các người dùng trong hệ thống có các mã trực giao với nhau thì họ có thể cùng tồn tại và truyền dữ liệu một cách đồng thời với khả năng bị giao thoa dữ liệu là ít nhất. Qui ước: Gọi Di là bit dữ liệu mà người dùng i muốn mã hóa để truyền trên

mạng. Ci là chuỗi chip (mã số) của người dùng i. Sau đây là cách thức mã hóa tín hiệu để gởi lên đường truyền và giải mã để lấy dữ liệu đó ra: Tín hiệu được mã của người dùng i: Zi = Di x Ci S •T =

Biên Sọan: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

66

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

Tín hiệu tổng hợp được gởi trên đường truyền:
$Z = \sum_{i=1}^{n} Zi$

với n là tổng số người dùng gởi tín hiệu lên đường truyền tại cùng thời điểm Giải mã: Dữ liệu mà người dùng i lấy về từ tín hiệu tổng hợp chung: Di = Z • C i Nếu Di > “ngưỡng”, coi nó là 1, ngược lại coi nó là -1 Ví dụ: Hệ thống có 4 người dùng A, B, C, D. Các mã số tương ứng của họ như sau:

Nếu ký hiệu theo kiểu lưỡng cực thì:

Để ý các mã số A, B, C, D là trực giao! Có sáu ví dụ: 1) Chỉ có người dùng C gởi bit 1: 2) B gởi bit 1, C gởi bit 1 3) A gởi bit 1, B gởi bit 0 4) A, C đều gởi bit 1, B gởi bit 0 5) A, B, C, D đều gởi bit 1 6) A, B, D gởi bit 1, C gởi bit 0 Ta tính toán được các mã tổng hợp gởi lên đường truyền như sau:

Bây giờ, ta tính được dữ liệu nguyên thủy của người dùng ở trạm C, sau khi đã rút trích ra từ mã tổng hợp như sau:

Nhận xét: Đầu tiên, chúng ta phải giả sử rằng tất cả các dãy chip được đồng bộ hóa để được gởi nhận cùng thời điểm. Nhưng trong thực tế, kiểu đồng bộ hóa như vậy là không thể có được. Những gì người ta có thể làm được để đồng bộ hóa là: người gởi và người nhận đồng bộ hóa với nhau bằng cách cho người gởi gởi một dãy chip được định nghĩa trước, dãy này phải đủ dài để cho bên nhận có thể theo kịp bên gởi. Tất cả các cuộc truyền nhận khác được xem như là nhiễu ngẫu nhiên. Người ta chứng minh được rằng, chuỗi chip càng dài thì xác suất phát hiện ra chuỗi này một cách chính xác là càng cao với sự hiện diện của nhiễu. Cũng cần phải giả thiết rằng: bên nhận biết chính xác bên gởi là ai. Tuy trong thực tế, cần phải trung thực mà nói rằng: đặt giả thiết thì dễ hơn là làm. Nhưng hãy tin tưởng là CDMA có nhiều chi tiết phức tạp hơn và thông minh hơn để làm được chuyện đó.
Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

67

5.3.2 Phương pháp truy cập đường truyền ngẫu nhiên (Random Access)
Trong phương pháp này, người ta để cho các trạm tự do tranh chấp đường truyền chung để truyền từng khung dữ liệu một. Nếu một trạm cần gởi một khung, nó sẽ gởi khung đó trên toàn bộ dải thông của kênh truyền. Sẽ không có sự phối hợp trình tự giữa các trạm. Nếu có hơn hai trạm phát cùng một lúc, "đụng độ" (collision) sẽ xảy ra, các khung bị đụng độ sẽ bị hư hại. Giao thức truy cập đường truyền ngẫu nhiên được dùng để xác định: Làm thế nào để phát hiện đụng độ. Làm thế nào để phục hồi sau đụng độ. Ví dụ về các giao thức truy cập ngẫu nhiên: slotted ALOHA và pure ALOHA, CSMA và CSMA/CD, CSMA/CA.

5.3.2.1

ALOHA

Vào những năm 1970, Norman Abramson cùng các đồng sự tại Đại học Hawaii đã phát minh ra một phương pháp mới ưu hạng dùng để giải quyết bài toán về cấp phát kênh truyền. Sau đó công việc của họ tiếp tục được mở rộng bởi nhiều nhà nghiên cứu khác. Mặc dù công trình của Abramson, được gọi là hệ thống ALOHA, sử dụng hệ thống truyền quảng bá trên sóng radio mặt đất, nhưng ý tưởng cơ sở của nó có thể áp dụng cho bất kỳ hệ thống nào trong đó những người dùng không có phối hợp với nhau sẽ tranh chấp sử dụng đường truyền chung duy nhất. Ở đây, chúng ta sẽ thảo luận về hai phiên bản của ALOHA: pure (thuần túy) và slotted (được chia khe).

5.3.2.1.1

Slotted ALOHA

Thời gian được chia thành nhiều slot có kích cỡ bằng nhau (bằng thời gian truyền một khung). Một trạm muốn truyền một khung thì phải đợi đến đầu slot thời gian kế tiếp mới được truyền. Dĩ nhiên là sẽ xảy ra đụng độ và khung bị đụng độ sẽ bị hư. Tuy nhiên, dựa trên tính phản hồi của việc truyền quảng bá, trạm phát luôn có thể theo dõi xem khung của nó phát đi có bị hủy hoại hay không bằng cách lắng nghe kênh truyền. Những trạm khác cũng làm theo cách tương tự. Trong trường hợp vì lý do nào đó mà trạm không thể dùng cơ chế lắng nghe đường truyền, hệ thống cần yêu cầu bên nhận trả lời một khung báo nhận (acknowledgement) cho bên phát. Nếu phát sinh đụng độ, trạm phát sẽ gởi lại khung tại đầu slot kế tiếp với xác suất p cho đến khi thành công. Ví dụ minh họa: Có 3 trạm đều muốn truyền một khung thông tin.

H5.7 Minh họa giao thức Slotted ALOHA

Do sẽ có đụng độ mà mất khung thông tin, một câu hỏi đặt ra là: đâu là tỉ suất truyền khung thành công của các trạm trong mạng? Giả sử có N trạm muốn truyền dữ liệu, mỗi trạm truyền khung thông tin của mình trong một slot với xác suất p. Xác suất để một trạm

trong N trạm truyền thành công S(p) được tính như sau: S ( p) = Np(1 − p) N −1 Khi p = 1 N , S(p) đạt giá trị cực đại (1 − 1 N ) N −1

5.3.2.1.2

Pure ALOHA

Kỹ thuật Pure ALOHA đơn giản hơn Slotted ALOHA do không có sự đồng bộ hóa giữa các trạm. Mỗi khi muốn truyền một khung thông tin, trạm sẽ truyền nó ngay mà không cần đợi đến đầu của

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

68

slot thời gian kế tiếp. Vì thế xác xuất bị đụng độ tăng thêm! Nghĩa là khung thông tin được gởi tại thời điểm t0 sẽ đụng độ với những khung được gởi trong khoảng thời gian [t0-1, t0+1].

H5.8 Minh họa giao thức Pure ALOHA

Gọi P là xác xuất của một sự kiện nào đó, ta có những phân tích sau: P(nút i truyền thành công) = P(để nút i truyền) × P(không có nút nào khác truyền trong khoảng [t -1,t ]) . 0 0 ×

P(không có nút nào khác truyền trong khoảng [t0, t0+1])

= p (1 − p ) N −1 (1 − p ) N −1 S(p) = P(một nút bất kỳ trong N nút truyền thành công) = Np (1 − p ) N −1 (1 − p ) N −1 Những phân tích vừa nêu giả sử rằng luôn có thường trực N trạm trong mạng. Và trong trường hợp tối ưu, mỗi trạm thử truyền vơi xác suất 1/N. Trong thực tế, số lượng các trạm thường trực trong mạng luôn thay đổi. Giả sử chúng ta có tổng cộng m trạm làm việc. n trạm là thường trực trên mạng, mỗi trạm thường trực trên mạng sẽ cố gởi khung thông tin với xác suất cố định p. m-n trạm còn lại là không thường trực, và chúng có thể gởi khung thông tin với xác suất pa, với pa có thể nhỏ hơn p. Nhận xét chung về ALOHA: Hiệu năng thấp do không có thăm dò đường truyền trước khi gởi khung, dẫn đến việc mất nhiều thời gian cho việc phát hiện đụng độ và phục hồi sau đụng độ. Hoạt động theo kiểu ALOHA có khả năng dẫn đến việc hệ thống bị “chết đứng” do mọi nỗ lực gởi gói tin của tất cả các trạm đều bị đụng độ. Slotted ALOHA trở nên quan trọng với lý do không mấy rành mạch lắm. Nó ra đời vào những năm 1970, được sử dụng trong một số hệ thống thí nghiệm thời đó, và rồi hầu như bị lãng quên. Và khi công nghệ truy cập Internet không qua cable được phát minh, đột nhiên lại phát sinh vấn đề làm sao để cấp phát đường truyền được chia sẻ cho nhiều người dùng cạnh tranh, Slotted ALOHA lại được lôi ra từ thùng rác để cứu rỗi cuộc đời. Vẫn thường có chuyện là các giao thức hợp lý một cách hoàn hảo lại không được sử dụng vì những lý do về chính trị, nhưng nhiều năm sau đó, một số người thông thái lại nhận ra rằng những giao thức bỏ đi từ lâu rồi đó lại có thể giúp họ giải quyết được vấn đề. Với lý do như vậy, trong chương này, chúng ta sẽ nghiên cứu một số giao thức ưu hạng hiện tại không được sử dụng rộng rãi lắm nhưng biết đâu có thể được sử dụng dễ dàng trong các ứng dụng ở tương lai. Dĩ nhiên là chúng ta cũng sẽ nghiên cứu nhiều giao thức đang được sử dụng rộng rãi hiện nay.

5.3.2.2

CSMA – Carrier Sense Multiple Access

Giao thức ALOHA mặc dù đã chạy được, nhưng một điều đáng ngạc nhiên là người ta lại để cho các trạm làm việc tự do gởi thông tin lên đường truyền mà chẳng cần quan tâm đến việc tìm hiểu xem những trạm khác đang làm gì. Và điều đó dẫn đến rất nhiều vụ đụng độ tín hiệu. Tuy nhiên, trong mạng LAN, người ta có thể thiết kế các trạm làm việc sao cho chúng có thể điều tra xem các trạm khác đang làm gì và tự điều chỉnh hành vi

của mình một cách tương ứng. Làm như vậy sẽ giúp cho hiệu năng mạng đạt được cao hơn. CSMA là một giao thức như vậy! Các giao thức mà trong đó các trạm làm việc lắng nghe đường truyền trước khi đưa ra quyết định mình phải làm gì tương ứng với trạng thái đường truyền đó được gọi là các giao thức có “cảm nhận” đường truyền (carrier sense protocol). Cách thức hoạt động của CSMA như sau: lắng nghe

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

69

kênh truyền, nếu thấy kênh truyền rỗi thì bắt đầu truyền khung, nếu thấy đường truyền bận thì trì hoãn lại việc gởi khung. Thế nhưng trì hoãn việc gởi khung cho đến khi nào? Có ba giải pháp: Theo dõi không kiên trì (Non-persistent CSMA): Nếu đường truyền bận, đợi trong một khoảng thời gian ngẫu nhiên rồi tiếp tục nghe lại đường truyền. Theo dõi kiên trì (persistent CSMA): Nếu đường truyền bận, tiếp tục nghe đến khi đường truyền rỗi rồi thì truyền gói tin với xác suất bằng 1. Theo dõi kiên trì với xác suất p (P-persistent CSMA): Nếu đường truyền bận, tiếp tục nghe đến khi đường truyền rỗi rồi thì truyền gói tin với xác suất bằng p. Dễ thấy rằng giao thức CSMA cho dù là theo dõi đường truyền kiên trì hay không kiên trì thì khả năng tránh đụng độ vẫn tốt hơn là ALOHA. Tuy thế, đụng độ vẫn có thể xảy ra trong CSMA! Tình huống phát sinh như sau: khi một trạm vừa phát xong thì một trạm khác cũng phát sinh yêu cầu phát khung và bắt đầu nghe đường truyền. Nếu tín hiệu của trạm thứ nhất chưa đến trạm thứ hai, trạm thứ hai sẽ cho rằng đường truyền đang rảnh và bắt đầu phát khung. Như vậy đụng độ sẽ xảy ra.

H5.9 Mô tả không gian và thời gian diễn ra đụng độ

Hậu quả của đụng độ là: khung bị mất và toàn bộ thời gian từ lúc đụng độ xảy ra cho đến khi phát xong khung là lãng phí! Bây giờ phát sinh vấn đề mới: các trạm có quan tâm theo dõi xem có đụng độ xảy ra không và khi đụng độ xảy ra thì các trạm sẽ làm gi?

5.3.2.2.1

CSMA với cơ chế theo dõi đụng độ (CSMA/CD – CSMA with Collision Detection)

CSMA/CD về cơ bản là giống như CSMA: lắng nghe trước khi truyền. Tuy nhiên CSMA/CD có hai cải tiến quan trọng là: phát hiện đụng độ và làm lại sau đụng độ. Phát hiện đụng độ: Trạm vừa truyền vừa tiếp tục dò xét đường truyền. Ngay sau khi đụng độ được phát hiện thì trạm ngưng truyền, phát thêm một dãy nhồi (dãy nhồi này có tác dụng làm tăng cường thêm sự va chạm tín hiệu, giúp cho tất cả các trạm khác trong mạng thấy được sự đụng độ), và bắt đầu làm lại sau đụng độ. CSMA/CD, cũng giống như các giao thức trong LAN khác, sử dụng mô hình quan niệm như trong hình sau:
Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

70

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

H5.10 CSMA/CD có thể ở một trong ba trạng thái: tranh chấp, truyền, rảnh

Tại thời điểm t0, một trạm đã phát xong khung của nó. Bất kỳ trạm nào khác có khung cần truyền bây giờ có thể cố truyền thử. Nếu hai hoặc nhiều hơn các trạm làm như vậy cùng một lúc thì sẽ xảy ra đụng độ. Đụng độ có thể được phát hiện bằng cách theo dõi năng lượng hay độ rộng của xung của tín hiệu nhận được và đem so sánh với độ rộng của xung vừa truyền đi. Bây giờ ta đặt ra câu hỏi: Sau khi truyền xong khung (hết giai đoạn truyền), trạm sẽ bỏ ra thời gian tối đa là bao lâu để biết được là khung của nó đã bị đụng độ hoặc nó đã truyền thành công? Gọi thời gian này là “cửa sổ va chạm” và ký hiệu nó là Tw. Phân tích sau đây sẽ cho ra câu trả lời. Hình sau sẽ mô phỏng chi tiết về thời gian phát khung giữa hai trạm A và B ở hai đầu mút xa nhất trên đường truyền tải.

H5.11 Thời gian cần thiết để truyền một khung

Đặt Tprop là thời gian lan truyền tín hiệu giữa hai đầu mút xa nhau nhất trên đường truyền tải. Tại thời điểm t, A bắt đầu phát đi khung dữ liệu của nó. Tại t+Tprop-ε, B phát hiện kênh truyền rảnh và phát đi khung dữ liệu của nó. Tại t+ Tprop, B phát hiện sự đụng độ. Tại t+2Tprop-ε, A phát hiện sự đụng độ. Theo phân tích trên, thì Tw = 2Tprop

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

71

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

H5.12 Phát hiện đụng độ khi truyền tin

Việc hủy bỏ truyền khung ngay khi phát hiện có đụng độ giúp tiết kiệm thời gian và băng thông, vì nếu cứ tiếp tục truyền khung đi nữa, khung đó vẫn hư và vẫn phải bị hủy bỏ.

H5.13 Xử lý khu đụng độ

Làm lại sau khi đụng độ: Sau khi bị đụng độ, trạm sẽ chạy một thuật toán gọi là back-off dùng để tính toán lại lượng thời gian nó phải chờ trước khi gởi lại khung. Lượng thời gian này phải là ngẫu nhiên để các trạm sau khi quay lại không bị đụng độ với nhau nữa. Thuật toán back-off hoạt động như sau: Rút ngẫu nhiên ra một con số nguyên M thõa: $0 \leq M \leq 2^k$ . Trong đó k = min( n,10) , với n là tổng số lần đụng độ mà trạm đã gánh chịu. Kỳ hạn mà trạm phải chờ trước khi thử lại một lần truyền mới là M*Tw. Khi mà n đạt đến giá trị 16 thì hủy bỏ việc truyền khung. (Trạm đã chịu đựng quá nhiều vụ đụng độ rồi, và không thể chịu đựng hơn được nữa!)

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

72

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

ĐÁNH GIÁ HIỆU SUẤT CỦA GIAO THỨC CSMA/CD: Gọi: P là kích thước của khung, ví dụ như 1000 bits. C là dung lượng của đường truyền, ví dụ như 10 Mbps. Ta có thời gian phát hết một khung thông tin là P/C giây. Trung bình, chúng ta sẽ thử e lần trước khi truyền thành công một khung. Vì vậy, với mỗi lần phát thành công một khung (tốn P/C giây), ta đã mất tổng cộng 2eTprop (≈5Tprop) vì đụng độ. Thành thử hiệu năng của giao thức (tỉ lệ giữa thời gian hoạt động hữu ích trên tổng thời gian hoạt động) là:
P C P C

+ 5Tprop

=

1 1+
5Tprop
P C

Tprop C 1 a= = 1 + 5a , với P

Giá trị của a đóng vai trò rất quan trọng đến hiệu suất hoạt động của mạng kiểu CSMA/CD.

5.3.3 Phương pháp phân lượt truy cập đường truyền
Bây giờ thử nhìn lại hai phương pháp điều khiển truy cập đường truyền “chia kênh” và “truy cập ngẫu nhiên”, ta sẽ thấy chúng đều có những điểm hay và hạn chế: Trong các giao thức dạng chia kênh, kênh truyền được phân chia một cách hiệu quả và công bằng khi tải trọng đường truyền là lớn. Tuy nhiên chúng không hiệu quả khi tải trọng của đường truyền là nhỏ: có độ trì hoãn khi truy cập kênh truyền, chỉ 1/N băng thông được cấp cho người dùng ngay cả khi chỉ có duy nhất người dùng đó hiện diện trong hệ thống. Các giao thức dạng truy cập ngẫu nhiên thì lại hoạt động hiệu quả khi tải trọng của đường truyền thấp. Nhưng khi tải trọng đường truyền cao thì phải tốn nhiều chi phí cho việc xử lý đụng độ. Các giao thức dạng “phân lượt” sẽ để ý đến việc tận dụng những mặt mạnh của hai dạng nói trên. Ý tưởng chính của các giao thức dạng “phân lượt” là không để cho đụng độ xảy ra bằng cách cho các trạm truy cập đường truyền một cách tuần tự. Về cơ bản, có hai cách thức để “phân lượt” sử dụng đường truyền: Thăm dò (polling): Trạm chủ (master) sẽ mời các trạm tớ (slave) truyền khi đến lượt. Lượt truyền được cấp phát cho trạm tớ có thể bằng cách: trạm chủ dành phần cho trạm tớ hoặc trạm tớ yêu cầu và được trạm chủ đáp ứng. Tuy nhiên có thể thấy những vấn đề sẽ gặp phải của giải pháp này là: chi phí cho việc thăm dò, độ trễ do phải chờ được phân lượt truyền, hệ thống rối loạn khi trạm chủ gặp sự cố. Chuyền thẻ bài (token passing): Thẻ bài điều khiển sẽ được chuyển lần lượt từ trạm này qua trạm kia. Trạm nào có trong tay thẻ bài sẽ được quyền truyền, truyền xong phải chuyền thẻ bài qua trạm kế tiếp. Những vấn đề cần phải quan tâm: chi phí quản lý thẻ bài, độ trễ khi phải chờ thẻ bài, khó khăn khi thẻ bài bị mất.

5.3.3.1

Ví dụ về phương pháp thăm dò: Thăm dò phân tán (Distributed Polling)

Thời gian được chia thành những “khe” (slot). Giả sử hệ thống hiện có N trạm làm việc. Một chu kỳ hoạt động của hệ thống bắt đầu bằng N khe thời gian ngắn dùng để đặt chỗ (reservation slot). Khe thời gian dùng để đặt chỗ bằng với thời gian lan truyền tín hiệu giữa hai đầu mút xa nhất trên đường truyền. Tới khe đặt chỗ thứ i, trạm thứ i nếu muốn truyền dữ liệu sẽ phát tín hiệu đặt chỗ của mình lên kênh truyền, và tín hiệu này sẽ được nhìn thấy bởi tất cả các trạm khác trong mạng. Sau thời gian đặt chỗ, các trạm bắt đầu việc truyền dữ liệu của mình theo đúng trình tự đã đăng ký.

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

73

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

H5.14 Mô tả các chu kỳ hoạt động của hệ thống Thăm dò phân tán

5.3.3.2

Ví dụ về phương pháp chuyển thẻ bài: Token Ring

Giao thức này sử dụng mạng kiểu hình vòng, dùng thẻ bài để cấp quyền sử dụng đường truyền. Mạng token ring bao gồm một tập hợp các trạm được nối với nhau thành một vòng.

H5.15 Mô hình hoạt động của mạng Token Ring

Dữ liệu luôn chạy theo một hướng vòng quanh vòng. Mỗi trạm nhận khung từ trạm phía trên của nó và rồi chuyển khung đến trạm phía dưới. Thẻ bài là công cụ để quyết định ai có quyền truyền tại một thời điểm. Cách thức hoạt động của mạng token ring như sau: một thẻ bài, thực chất chỉ là một dãy bit, sẽ chạy vòng quanh vòng; mỗi nút sẽ nhận thẻ bài rồi lại chuyển tiếp thẻ bài này đi. Khi một trạm có khung cần truyền và đúng lúc nó thấy có thẻ bài tới, nó liền lấy thẻ bài này ra khỏi vòng (nghĩa là không có chuyển tiếp chuỗi bit đặc biệt này lên vòng nữa), và thay vào đó, nó sẽ truyền khung dữ liệu của mình đi. Khi khung dữ liệu đi một vòng và quay lại, trạm phát sẽ rút khung của mình ra và chèn lại thẻ bài vào vòng. Hoạt động cứ xoay vòng như thế. Card mạng dùng cho token ring sẽ có trên đó một bộ nhận, một bộ phát và một bộ đệm dùng chứa dữ liệu. Khi không có trạm nào trong vòng có dữ liệu để truyền, thẻ bài sẽ lưu chuyển vòng quanh. Nếu một trạm có dữ liệu cần truyền và có thẻ bài, nó có quyền truyền một hoặc nhiều khung dữ liệu tùy theo qui định của hệ thống. Mỗi khung dữ liệu được phát đi sẽ có một phần thông tin chứa địa chỉ đích của trạm bên nhận; ngoài ra nó còn có thể chứa địa chỉ muticast hoặc broadcast tùy theo việc bên gởi muốn gởi khung cho một nhóm người nhận hay tất cả mọi người trong vòng. Khi khung thông tin chạy qua mỗi trạm trong vòng, trạm này sẽ nhìn vào địa chỉ đích trong khung đó để biết xem có phải nó là đích đến của khung không. Nếu phải, trạm sẽ chép nội dung của khung vào trong bộ đệm của nó, chỉ chép thôi chứ không được xóa khung ra khỏi vòng. Một vấn đề cần phải quan tâm đến là một trạm đang giữ thẻ bài thì nó có quyền truyền bao nhiêu dữ liệu, hay nói cách khác là trạm được cho bao nhiêu thời gian để truyền dữ liệu? Chúng ta gọi thời gian này là thời gian giữ thẻ bài – THT (Token Holding Time). Trong trường hợp trong vòng chỉ có một trạm cần truyền dữ liệu và các trạm khác không có nhu cầu truyền, thì ta có thể cấp THT cho trạm có nhu cầu càng lâu càng tốt. Điều này sẽ làm tăng hiệu suất sử dụng hệ thống một cách đáng kể. Bởi vì sẽ thật là ngớ ngẩn nếu bắt trạm ngừng, chờ thẻ bài chạy hết một vòng, rồi lại
Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

74

truyền tiếp. Tuy nhiên, giải pháp trên sẽ không hoạt động tốt nếu có nhiều trạm trong vòng cần gởi dữ liệu. THT dài chỉ thích hợp cho những trạm cần truyền nhiều dữ liệu, nhưng lại không phù hợp với những trạm chỉ có ít thông điệp cần gởi đi ngay cả khi thông điệp này là tối quan trọng. Điều này cũng giống như tình huống mà bạn xếp hàng để sử dụng máy ATM ngay sau một anh chàng định rút ra 10 triệu đồng, trong khi bạn chỉ cần vào đấy để kiểm tra tài khoản của mình còn bao nhiêu tiền! Trong các mạng 802.5, THT mặc định là 10 ms. Từ thời gian giữ thẻ bài, chúng ta lại nghĩ ra một số đo quan trọng khác: Thời gian xoay vòng của thẻ bài – TRT (Token rotation time), nghĩa là lượng thời gian bỏ ra để thẻ bài đi hết đúng một vòng. Dễ nhận thấy rằng: TRT ≤ Số nút hoạt động × THT + Độ trễ của vòng Với “Độ trễ của vòng” là tổng thời gian để thẻ bài đi hết một vòng khi trong vòng không có trạm nào cần truyền dữ liệu, “Số nút hoạt động” ám chỉ số trạm có dữ liệu cần truyền. Giao thức 802.5 cung cấp một phương thức truyền dữ liệu tin cậy bằng cách sử dụng hai bit A và C ở đuôi của khung dữ liệu. Hai bit bày ban đầu nhận giá trị 0. Khi một trạm nhận ra nó là đích đến của một khung dữ liệu, nó sẽ đặt bit A trong khung này lên. Khi trạm chép khung vào trong bộ nhớ đệm của nó, nó sẽ đặt bit C lên. Khi trạm gởi thấy khung của nó quay lại với bit A vẫn là 0, nó biết là trạm đích bị hư hỏng hoặc không có mặt. Nếu bit A là 1, nhưng bit C là 0, điều này ám chỉ trạm đích có mặt nhưng vì lý do nào đó trạm đích không thể nhận khung (ví dụ như thiếu bộ đệm chẳng hạn). Vì thế khung này có thể sẽ được truyền lại sau đó với hy vọng là trạm đích có thể tiếp nhận nó. Chi tiết cuối cùng cần phải xem xét là: chính xác khi nào thì trạm sẽ nhả thẻ bài ra? Có hai đề nghị: a) nhả thẻ bài ra ngay sau khi trạm vừa truyền khung xong (RAT); b) nhả thẻ bài ra ngay sau khi trạm nhận lại khung vừa phát ra (RAR).

H5.16 Nhả token: a)RAT b)RAR

Quản lý hoạt động của mạng Token Ring Cần thiết phải đề cử ra một trạm làm nhiệm vụ quản lý mạng token ring gọi là monitor. Công việc của monitor là đảm bảo sức khỏe cho toàn bộ vòng. Bất kỳ trạm nào cũng có thể trở thành monitor. Thủ tục bầu chọn monitor diễn ra khi vòng vừa được tạo ra hoặc khi monitor của vòng bị sự cố. Một monitor mạnh khỏe sẽ định kỳ thông báo sự hiện diện của nó cho toàn vòng biết bằng một thông điệp đặc biệt. Nếu một trạm không nhận được thông báo hiện diện của monitor trong một khoảng thời gian nào đó, nó sẽ coi như monitor bị hỏng và sẽ cố trở thành monitor mới. Khi một trạm quyết định rằng cần phải có một monitor mới, nó sẽ gởi một thông điệp thỉnh cầu, thông báo ý định trở thành monitor của mình. Nếu thông điệp này chạy một vòng và về lại được trạm, trạm sẽ cho rằng mọi người đồng ý vị trí monitor của nó. Còn nếu đồng thời có nhiều trạm cùng gởi thông điệp thỉnh cầu, chúng sẽ phải áp dụng một luật lựa chọn nào đó, chẳng hạn như “ai có địa chỉ cao nhất sẽ thắng cử”.
Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

75

Nhiệm vụ đáng chú ý của monitor là phải đảm bảo rằng luôn luôn có sự hiện diện của thẻ bài ở đâu đó trên vòng, có thể là đang di chuyển hay đang bị giữ bởi một trạm nào đó. Rõ ràng là thẻ bài có thể bị biến mất vì lý do nào đó chẳng hạn như lỗi bit, trạm đang giữ nó bị hư hỏng. Để phát hiện ra việc thẻ bài bị mất, khi thẻ bài chạy ngang qua monitor, nó sẽ bật một bộ đếm thời gian để tính giờ. Bộ đếm này có giá trị tối đa là: Số lượng trạm × THT + Độ trễ của vòng Trong đó “Số lượng trạm” là số các trạm làm việc đang hiện diện trên vòng, “độ trễ của vòng” là tổng thời gian lan truyền tín hiệu trên vòng. Nếu bộ đếm đạt đến giá trị tối đa mà monitor vẫn không thấy thẻ bài chạy qua nó nữa thì nó sẽ tạo ra thẻ bài mới. Monitor cũng phải kiểm tra xem có khung nào bị hỏng hoặc vô thừa nhận hay không. Một khung nếu có lỗi checksum hoặc khuôn dạng không hợp lệ sẽ chạy một cách vô định trên vòng. Monitor sẽ thu khung này lại trước khi chèn lại thẻ bài vào vòng. Một khung vô thừa nhận là khung mà đã được chèn thành công vào vòng, nhưng cha của nó bị chết, nghĩa là trạm gởi nó chỉ gởi nó lên vòng, nhưng chưa kịp thu nó lại thì đã bị chết (down). Những khung như vậy sẽ bị phát hiện bằng cách thêm vào một bit điều khiển gọi là monitor bit. Khi được phát lần đầu tiên, monitor bit trên khung sẽ nhận giá trị 0. Khi khung đi ngang qua monitor, monitor sẽ đặt monitor bit lên 1. Nếu monitor thấy khung này lại chạy qua nó với monitor bit là 1, nó sẽ rút khung này ra khỏi vòng. Một chức năng quản lý vòng khác là phát hiện ra một trạm bị chết. Nếu một trạm trong vòng bị chết, nó sẽ làm đứt vòng. Để tránh tình trạng này người ta thêm vào trạm một rờ-le điện tử (relay). Khi trạm còn mạnh khỏe, rờ-le sẽ mở và trạm được nối với vành, khi trạm bị chết và ngưng không cung cấp năng lượng cho rờ-le, rờ-le sẽ tự động đóng mạch và bỏ qua trạm này.

H5.17 Sử dụng relay để tránh đứt vòng

Khi monitor nghi ngờ một trạm bị chết, nó sẽ gởi đến trạm đó một khung đặc biệt gọi là khung beacon. Nếu không nhận được trả lời thích đáng, monitor sẽ coi trạm đó đã chết. ĐÁNH GIÁ VỀ MẠNG TOKEN RING: Ta sẽ khảo sát hai kiểu chuyển thẻ bài: Release After Reception (RAR) và Release After Transmisions (RAT). RAR: Nhả thẻ bài sau khi nhận lại dữ liệu Sau khi một trạm phát đi khung dữ liệu của nó, trạm sẽ chờ đến khi khung này quay trở lại mới chuyền thẻ bài cho trạm kế tiếp. Mạng IEEE 802.5 Token Ring (16Mbps) sử dụng cơ chế này.

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

H5.18 Mô phỏng cơ chế chuyền thẻ bài trong RAR

Ta gọi hiệu suất truyền khung là ηRAR. Mạng kiểu RAR sẽ đạt được hiệu suất tối đa nếu một trạm phát liên tục. Đặt: Tprop là thời gian lan truyền tín hiệu giữa hai đầu mút xa nhau nhất trên đường truyền tải. Ttran là thời gian để phát hết một khung dữ liệu lên đường truyền. P là kích thước của khung dữ liệu, ví dụ 1000 bits. C là dung lượng của đường truyền, ví dụ 10 Mbps. Có T = C tran Sau đây là biểu đồ mô phỏng mối liên quan giữa thời gian phát khung và thời gian truyền tín hiệu:
P

H5.19 Thời gian lan truyền và phát khung với RAR

Có thể thấy: Với

η RAR =
a=

Tprop Ttran

1 1+ a

Trong trường hợp một trạm luôn phải nhường token ngay sau khi token đi hết một vòng và quay trở lại nó thì hiện trạng phân bổ thời gian được vẽ ra dưới đây:

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

77

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

H5.20 Các khoảng thời gian một trạm phải trải qua khi gởi dữ liệu và chuyền thẻ bài

Giả sử token có kích thước quá nhỏ để coi như thời gian phát nó bằng không, mạng có N trạm làm việc và khoảng cách giữa các trạm là bằng nhau. Vì vậy, thời gian lan truyền tín hiệu từ một trạm đến một trạm liền kề nó là Tprop/N. Có thể nhận thấy thời gian để token chuyển từ một trạm sang một trạm kề nó là Tprop/N. Vì vậy: T 1 1

η RAR =

tran

Tprop + Ttran +

Tprop N

=

□ N + 1 □ Tprop 1+ □ □ □ N □ Ttran

≈

1+ a

RAT: Nhả thẻ bài ngay sau khi truyền dữ liệu Với kỹ thuật RAT, trạm sẽ chuyền thẻ bài điều khiển cho trạm kế tiếp ngay sau khi nó vừa phát song khung dữ liệu. Ví dụ mạng FDDI (Fiber Distributed Data Interface - 100Mbps) sử dụng kỹ thuật này.

Gọi hiệu suất truyền khung là η RAT . Với kỹ thuật RAT, hiệu suất đạt tối đa khi một trạm liên tục truyền khung. Sau đây là biểu đồ thời gian mô phỏng:

H5.21 Mô phỏng kỹ thuật RAT

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

78

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

Có thể thấy khi một trạm phát khung liên tục thì η RAT = 1 Tuy nhiên khi một trạm buộc phải nhả token ngay sau khi nó vừa phát dữ liệu xong, thì biểu đồ thời gian có khác: 1 Thời điểm Thời điểm Thời điểm 0

H5.22 Thời gian phát và lan truyền khung

2

3

N

1

Ttran +

Tprop N
Tprop N

Tprop Ttran

2Ttran + 2

H5.23 Khi một trạm phải nhả token ngay sau khi nó vừa phát dữ liệu

Ta tính lại hiệu suất như sau:

η RAT =
Với

5.3.3.3

Ví dụ về phương pháp chuyền thẻ bài: Token Bus

Ttran 1 1 = = Ttran T a Ttran + prop 1 + 1 prop 1 + prop Tprop N N N Ttran a= Ttran B C

A

D

H

G

H5.24 Sơ đồ mạng Token Bus

F

E

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

79

Kỹ thuật Token Bus về bản chất là sử dụng mạng hình bus. Tuy nhiên người ta muốn thiết lập một vòng ảo trên đó để nó hoạt động giống như Token Ring. Nguyên tắc hoạt động như sau: trạm có nhu cầu truyền dữ liệu thì sẽ tham gia vào vòng ảo, ngược lại thì sẽ nằm ngoài và chỉ nghe thôi! Giải thuật bổ sung một trạm vào vòng: Mỗi trạm trong vòng có trách nhiệm định kỳ tạo điều kiện cho các trạm khác tham gia vào vòng. Trước khi chuyển thẻ bài đi, trạm sẽ gởi thông báo “tìm trạm đứng sau” (có địa chỉ giữa nó và trạm đứng liền kề hiện tại). Nếu sau một thời gian xác định mà vẫn không có yêu cầu gia nhập nào, trạm sẽ chuyển thẻ bài đến trạm kế tiếp như thường lệ. Nếu có yêu cầu gia nhập vòng, thì trạm sẽ ghi nhận trạm mới yêu cầu là trạm kế tiếp của nó và sẽ chuyển thẻ bài tới trạm kế mới này. Giải thuật rút lui ra khỏi vòng: Khi muốn rút ra khỏi vòng, trạm sẽ chờ đến khi nó có token, sau đó sẽ gởi yêu cầu “nối trạm đứng sau” tới trạm đứng trước nó, yêu cầu trạm đứng trước nối trực tiếp với trạm đứng liền sau nó. Ngoài ra còn phải quan tâm đến tình trạng mất thẻ bài, các trạm thành viên trong vòng bị hư hỏng.

5.4 Chuẩn hóa mạng cục bộ

Ngoài mô hình OSI dùng cho việc chuẩn hóa các mạng nói chung, việc chuẩn hóa mạng cục bộ cũng đã được thực hiện trong một khoảng thời gian dài. Do đặc trưng riêng, việc chuẩn hóa mạng cục bộ chỉ được thực hiện trên hai tầng thấp nhất, tương ứng với tầng vật lý và liên kết dữ liệu trong mô hình OSI.

H5.25 Mô hình phân tầng của mạng cục bộ

Trong LAN, tầng liên kết dữ liệu được chia làm hai tầng con: LLC (Logical Link Layer) và MAC. MAC quản lý việc truy cập đường truyền, trong khi LLC đảm bảo tính độc lập của việc quản lý các liên kết dữ liệu với đường truyền vật lý và phương pháp truy cập đường truyền MAC. IEEE (Institute of Electrical and Electronic Engineers) là tổ chức đi tiên phong trong lĩnh vực chuẩn hóa mạng cục bộ với dự án IEEE 802 nổi tiếng bắt đầu được triển khai từ năm 1980 và kết quả là hàng loạt chuẩn thuộc họ IEEE 802.x ra đời, tạo nền tảng quan trọng cho việc thiết kế và cài đặt mạng nội bộ trong thời gian qua. Vị trí của họ chuẩn này càng cao hơn khi ISO đã xem xét và tiếp nhận chúng thành chuẩn quốc tế mang tên 8802.x. Đến nay họ IEEE 802.x bao gồm các chuẩn sau: IEEE 802.1 : High Level Interface IEEE 802.2 : Logical Link Control (LLC) IEEE 802.3: CSMA/CD

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

IEEE 802.4: Token bus IEEE 802.5: Token ring IEEE 802.6: MAN IEEE 802.7: Broadband Technical Advisory Group IEEE 802.8: Fiber Technical Advisory Group IEEE 802.9: Intergrated Data and Voice Network IEEE 802.10: Standard for Interoperable LAN security IEEE 802.11: Wireless LAN IEEE 802.12: 100VG – AnyLAN H5.23 sẽ mô tả vị trí tương đối của các chuẩn trên khi so sánh với chuẩn OSI:

H5.26 Quan hệ giữa các chuẩn IEEE và mô hình OSI

IEEE 802.1 là chuẩn đặc tả kiến trúc mạng, nối kết giữa các mạng và việc quản trị mạng đối với mạng cục bộ. IEEE 802.2 là chuẩn đặc tả tầng LLC (dịch vụ, giao thức) của mạng cục bộ. Có 3 kiểu giao thức LLC chính được định nghĩa: LLC type 1: Là giao thức kiểu không liên kết, không báo nhận. LLC type 2: Là giao thức kiểu có liên kết. LLC type 3: Là giao thức dạng không liên kết, có báo nhận. Các giao thức này được xây dựng dựa theo phương thức cân bằng của giao thức HDLC và có các khuôn dạng dữ liệu và các chức năng tương tự, đặc biệt là trong trường hợp LLC-type 2. IEEE 802.3: Là chuẩn đặc tả một mạng cục bộ dựa trên mạng Ethernet nổi tiếng do Digital, Intel và Xerox hợp tác phát triển từ năm 1990. IEEE 802.3 bao gồm cả tầng vật lý và tầng con MAC với các đặc tả sau: o Đặc tả dịch vụ MAC. o Giao thức MAC. o Đặc tả vật lý độc lập với đường truyền. o Đặc tả vật lý phụ thuộc vào đường truyền. Phần cốt lõi của IEEE 802.3 là giao thức MAC dựa trên phương pháp CSMA/CD đã trình bày ở phần trước. IEEE 802.4 là chuẩn đặc tả mạng cục bộ với hình trạng bus sử dụng thẻ bài để điều khiển truy cập đường truyền. IEEE 802.4 cũng bao gồm cả tầng vật lý và tầng con MAC với các đặc tả sau: o Đặc tả dịch vụ MAC. o Giao thức MAC. o Đặc tả dịch vụ tầng vật lý. o Đặc tả thực thể tầng vật lý. o Đặt tả đường truyền. IEEE 802.5 là chuẩn đặc tả mạng cục bộ với hình trạng vòng sử dụng thẻ bài để điều khiển truy cập đường truyền. IEEE 802.5 cũng bao gồm cả tầng vật lý và tầng con MAC với các đặc tả sau: o Đặc tả dịch vụ MAC.

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

81

o Giao thức MAC. o Đặc tả thực thể tầng vật lý. o Đặc tả nối trạm. IEEE 802.6 là chuẩn đặc tả một mạng tốc độ cao nối kết nhiều LAN thuộc các khu vực khác nhau của một đô thị. Mạng này sử dụng cáp quang với hình trạng dạng bus kép (dual-bus), vì thế còn được gọi là DQDB (Distributed Queue Dual Bus). Lưu thông trên mỗi bus là một chiều và khi cả cặp bus cùng hoạt động sẽ tạo thành một cấu hình chịu lỗi. Phương pháp điều khiển truy cập dựa theo một giải thuật xếp hàng phân tán có tên là QPDS (Queued-Packet, Distributed-Switch). IEEE 802.9 là chuẩn đặc tả một mạng tích hợp dữ liệu và tiếng nói bao gồm 1 kênh dị bộ 10 Mbps cùng với 95 kênh 64 Kbps. Giải thông tổng cộng 16 Mpbs. Chuẩn này được thiết kế cho các môi trường có lưu lượng lưu thông lớn và cấp bách. IEEE 802.10 là chuẩn đặc tả về an toàn thông tin trong các mạng cục bộ có khả năng liên tác (interoperable). IEEE 802.11 là chuẩn đặc tả mạng LAN không dây (Wireless LAN). Xu hướng chọn phương pháp truy cập CSMA được khẳng định. IEEE 802.12 là chuẩn đặc tả mạng cục bộ dựa trên công nghệ được đề xuất bởi AT&T, IBM và HP, gọi là 100 VG – AnyLAN. Mạng này sử dụng hình trạng mạng hình sao và một phương pháp truy cập đường truyền có điều khiển tranh chấp. Khi có nhu cầu truyền dữ liệu, trạm sẽ gởi yêu cầu đến hub và trạm chỉ có thể truyền dữ liệu khi được hub cho phép. Chuẩn này nhằm cung cấp một mạng tốc độ cao (100 Mbps và có thể lớn hơn) có thể hoạt động trong các môi trường hỗn hợp Ethernet và Token Ring, bởi thế nó chấp nhận cả hai dạng khung. 100 VG – AnyLAN là đối thủ cạnh tranh đáng gờm của 100BASE-T (Fast Ethernet) nhờ một số tính năng trội hơn, chẳng hạn về khoảng cách đi cáp tối đa cho phép…

## 5.5 Giới thiệu một số công nghệ mạng LAN

### 5.5.1 Ethernet (802.3)

Ethernet đã dễ dàng trở thành công nghệ mạng LAN thành công nhất trong suốt 20 năm qua. Được phát triển vào giữa thập kỷ 1970s bởi các nhà nghiên cứu tại Xerox Palo Atlto Research Center (PARC), Ethernet là một ví dụ thực tiễn của loại mạng cục bộ sử dụng giao thức CSMA/CD.

### 5.5.2 Tổng quan

Khởi thủy, một phân đoạn mạng của Ethernet (Ethernet segment) được cài đặt trên một sợi cable đồng trục dài tối đa 500 m. Các trạm nối vào Ethernet segment bằng cách “mắc dây” (tab) nối vào nó. Các điểm đấu nối phải cách nhau ít nhất 2,5 m. Transceiver, một thiết bị nhỏ được gắn trực tiếp vào điểm đấu nối, làm nhiệm vụ nghe ngóng khi đường truyền rỗi để đưa tín hiệu ra đó khi trạm phát tín hiệu. Transceiver cũng làm nhiệm vụ nhận tín hiệu đến. Đến lượt transceiver lại được nối đến card mạng Ethernet, được gắn trong máy trạm. Tất cả những chi tiết luận lý làm nên giao thức Ethernet được cài đặt trong card mạng này.

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

H5.27 Bức phác họa Ethernet của Bob Metcalfe, người sáng lập ra Ethernet (Xerox PARC - 1972) Và mô tả chi tiết transceiver + adaptor

Các segment có thể được nối với nhau bởi các repeater. Một repeater là một thiết bị dùng để chuyển tiếp tín hiệu số. Tuy nhiên, không được có hơn 4 repeater được đặt giữa hai trạm, có nghĩa là một mạng Ethernet nguyên thủy chỉ kéo dài tối đa là 2500 m. Bất kỳ tín hiệu nào được phát ra Ethernet sẽ được truyền quảng bá ra toàn mạng, repeater có nhiệm vụ chuyển tín hiệu từ trong segment ra ngoài, và nhận tín hiệu từ ngoài phát quảng bá vào trong segment.

H5.28 Ethernet Repeater

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

83

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

5.5.2.1

Khuôn dạng khung thông tin của Ethernet

Bên gởi sẽ bao gói gói tin IP thành khung Ethernet như sau:

H5.29 Khuôn dạng khung thông tin Ethernet Preamble: dài 7 bytes với mẫu 10101010 theo sau bởi 1 byte với mẫu 10101011, được sử dụng để đồng bộ hóa tốc độ đồng hồ giữa bên gởi và bên nhận. Source and dest. addresses: Địa chỉ nguồn và đích, gồm 6 bytes. Khung được nhận bởi tất cả các trạm trong LAN. Khung bị xóa nếu dest. address không trùng với địa chỉ MAC của bất kỳ trạm nào hoặc không phải thuộc dạng multicast. Type: chỉ ra giao thức được sử dụng ở tầng cao hơn, thường là IP, nhưng các giao thức khác vẫn được hỗ trợ - ví dụ: Novell IPX và AppleTalk. CRC: Phần kiểm tra lỗi. Lỗi được kiểm tra tại trạm đích. Nếu khung có lỗi, nó sẽ bị xóa.

5.5.2.2

Địa chỉ Ethernet

Mỗi host trong một mạng Ethernet (thật ra là tất cả các host trên thế giới) có một địa chỉ Ethernet duy nhất. Mô tả một cách kỹ thuật, địa chỉ được gắn vào card mạng chứ không phải máy tính; nó được ghi vào ROM trên card mạng. Các địa chỉ Ethernet thường được in theo thể thức mà con người có thể đọc được: một dãy gồm 6 bytes được viết dưới dạng thập lục phân, cách nhau bởi dấu hai chấm. Ví dụ 8:0:2b:e4:b1:2 là cách biểu diễn dễ đọc của địa chỉ Ethernet sau 00001000 00000000 00101011 11100100 10110001 00000010 Để đảm bảo rằng mọi card mạng được gán một địa chỉ duy nhất, mỗi nhà sản xuất thiết bị Ethernet được cấp cho một phần đầu địa chỉ (prefix) khác nhau. Ví dụ Advanced Micro Devices đã được cấp phần đầu dài 24 bit x08002 (hay 8:0:2). Nhà sản xuất này sau đó phải đảm bảo phần đuôi (suffix) của các địa chỉ mà họ sản xuất ra là duy nhất. Mỗi khung được phát ra Ethernet sẽ được nhận bởi tất cả các card mạng có nối với đường truyền. Mỗi card mạng sẽ so sánh địa chỉ đích trong khung với địa chỉ của nó, và chỉ cho vào máy tính những khung nào trùng địa chỉ. Địa chỉ duy nhất như vậy gọi là địa chỉ unicast. Ngoài ra còn có loại địa chỉ broadcast là loại địa chỉ quảng bá, có tất cả các bit đều mang giá trị 1. Mọi card mạng đều cho phép các khung thông tin có địa chỉ đích là broadcast đi đến host của nó. Cũng có một loại địa chỉ khác gọi là multicast, trong đó chỉ một vài bit đầu được đặt là 1. Một host có thể lập trình điều khiển card mạng của nó chấp nhận một số lớp địa chỉ multicast. Địa chỉ multicast được dùng để gởi thông điệp đến một tập con (subset) các host trong mạng Ethernet.

5.5.2.3

Cách thức mã hóa tín hiệu

Để chuyển đổi dữ liệu bit sang tín hiệu truyền trên đường truyền, Ethernet dùng kiểu mã hóa Manchester. Trong sơ đồ mã hóa Manchester, một bit sẽ được mã hóa bằng một sự thay đổi điện thế. Với bit “1”, điện thế đổi từ 1 xuống 0. Còn với bit “0”, điện thế đổi từ 0 lên 1.

H5.30 Mã hóa Machester

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

84

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

5.5.2.4

Giải thuật truy cập đường truyền

Ethernet sử dụng giải thuật CSMA/CS+Exponential backoff, được trình bày cụ thể như sau:
Nhận một gói tin từ tầng cao hơn; K := 0; n :=0; // K: thời gian chờ đợi ngẫu nhiên; n: số vụ đụng độ đã gặp phải repeat: chờ trong khoảng thời gian K*512 bit-time; while (đường truyền bận) wait; chờ tiếp 96 bit-time sau khi nhận thấy không có tín hiệu trên đường truyền; truyền khung và chú ý phát hiện đụng độ; if (có đụng độ) { ngừng truyền và phát tiếp một dãy nhồi 48-bit; n ++; m:= min(n, 10); chọn K ngẫu nhiên từ tập hợp {0, 1, 2, …, 2m-1}. if (n < 16) goto repeat; else bỏ việc truyền; }

5.5.2.5

Các công nghệ Ethernet 10-BASE-2

5.5.2.5.1

Giải thích các ký hiệu: 10: 10 Mbps 2: chiều dài cable tối đa là 200 m Base: Baseband, Broad: Broadband. Mạng Ethernet 10BASE2 sử dụng cáp đồng trục gầy, hình thái bus. Trong trường hợp mạng có nhiều segments, các repeaters sẽ được sử dụng để nối kết các segments này lại.

Hình 2.31 Mô hình mạng 10BASE2

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

85

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

5.5.2.5.2

10-BASE-T và 100-BASE-T

Mạng đạt tốc độ 10/100 Mbps, về sau được gọi là “fast Ethernet”. Chữ T viết tắt cho Twisted Pair: cáp xoắn đôi. Cách thức nối mạng được mô phỏng như sau:

H5.32 Mô hình mạng 10BaseT

Các HUB được nối tới các SWITCH bằng cáp xoắn đôi. Với cách thức đấu nối như vậy, mạng được gọi là “hình sao”. Cơ chế CSMA/CD được cài đặt tại HUB

5.5.2.5.3

GIGABIT ETHERNET

Gbit Ethernet sử dụng khuôn dạng khung chuẩn của Ethernet. Nó cho phép mạng hoạt động trên cả hai kiểu nối kết điểm điểm và kênh quảng bá chia sẻ. Trong kiểu nối kết điểm-điểm, Gbit Ethernet sử dụng các switches thay cho các hub. Đường truyền được sử dụng theo kiểu hai chiều đồng thời với tốc độ 1 Gbps. Trong kiểu kênh quảng bá chia sẻ, Gbit Ethernet sử dụng các hubs làm kênh quảng bá và áp dụng giải thuật CSMA/CD để các trạm chia sẻ việc sử dụng các hubs này.

5.5.3 FDDI (Fiber Distributed Data Interface)
Theo nhiều phương diện, FDDI tương tự như 802.5 và IBM Token Ring. Tuy nhiên, cũng có những khác biệt đáng kể, một số phát sinh vì lý do FDDI chạy trên cáp quang, một số khác phát sinh do có nhiều đổi mới sau khi người ta phát minh ra IBM Token Ring. Chúng ta sẽ thảo luận về những khác biệt quan trọng trong phần dưới đây.

5.5.3.1

Các tính chất vật lý

Không giống như mạng 802.5, một mạng FDDI bao gồm một vòng đôi = hai vòng độc lập truyền dữ liệu theo hai chiều ngược nhau (xem H5.33.a).

H5.33 Vòng quang đôi: a) hoạt động bình thường; b) vòng chính bị hỏng

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

86

Vòng phụ không được sử dụng trong khi hệ thống hoạt động bình thường, nó chỉ vào cuộc khi vòng chính bị sự cố (xem H5.33.b). Nghĩa là vòng chính sẽ quành lại vòng phụ để tạo ra một vòng hoàn chỉnh, và chính điều này giúp cho FDDI có khả năng chịu lỗi khi một cộng cáp bị đứt hay một trạm trong vòng bị hỏng. Do phải chịu phí tổn khi cấu hình theo kiểu vòng đôi, nên FDDI còn cho phép một trạm chọn nối vào chỉ một vòng đơn thôi. Những trạm như vậy gọi là những "trạm nối đơn" (single attachment station – SAS). Những trạm nối cả vào hai vòng dĩ nhiên sẽ được gọi là những "trạm đấu đôi" (dual attachment station – DAS). Một bộ tập trung (concentrator) sẽ được sử dụng để nối các SAS vào vòng đôi (xem H5.34)

H5.34 Các SAS được nối vào bộ tập trung

Nếu một SAS bị hỏng hóc, bộ tập trung sẽ phát hiện ra tình trạng này và sử dụng cơ chế bỏ qua tín hiệu quang (obtical bypass) để cô lập SAS bị hỏng, vì thế giữ cho vòng được thông suốt. Trong FDDI, bộ đệm của giao diện mạng có thể có kích thước khác nhau tại những trạm khác nhau, mặc dù kích thước của nó không bao giờ nhỏ hơn 9 bit và lớn hơn 80 bit. Một trạm cũng có thể bắt đầu phát các bit trong bộ đệm đi trước khi bộ đệm của nó bị đầy. Dĩ nhiên là tổng thời gian để một thẻ bài di chuyển hết một vòng là một hàm của kích thước của các bộ đệm này. Ví dụ, FDDI là mạng tốc độ 100 Mbps, nó có thời gian xử lý 1 bit là 10 ns. Nếu mỗi trạm cài đặt buffer dài 10 bit và chờ cho đến khi buffer bị đầy một nửa mới bắt đầu truyền, thì mỗi trạm tạo ra thời gian trì hoãn là 5 × 10 ns = 50 ns đối với tổng thời gian xoay vòng mạng. FDDI còn có các tính chất vật lý khác. Chẳng hạn, một mạng đơn có giới hạn chuẩn là có tối đa 500 trạm làm việc, với khoảng cách xa nhất giữa một cặp trạm bất kỳ là 2 km. Nhưng trên hết, mạng lại bị giới hạn với kích thước tổng cộng là 200 km cáp quang. Do tính chất là vòng đôi, nên tổng kích thước cáp quang nối tất cả các trạm là 100 km. Ngoài ra, mặc dù ký tự "F" ám chỉ cáp quang, nhưng chuẩn FDDI đã được định nghĩa để có thể chạy trên một số thiết bị tải khác, bao gồm cả cáp đồng trục và cáp xoắn đôi. Tuy nhiên cũng nên cẩn thận khi xét đến tổng kích thước mà vòng bao phủ. Như chúng ta sẽ thấy dưới đây, lượng thời gian bỏ ra để cho thẻ bài đi hết một vòng mạng sẽ đóng vai trò quan trọng trong giải thuật điều khiển truy cập. FDDI sử dụng phương pháp mã hóa 4B/5B. Do FDDI chuẩn mạng phổ biến đầu tiên sử dụng cáp quang, nên các con chíp mã hóa dạng 4B/5B chạy trên tốc độ của FDDI có rất nhiều ngoài thị trường.

5.5.3.2

Giải thuật "Thẻ bài được định thời" – Timed Token

Các luật qui định thời gian giữ thẻ bài trong FDDI phức tạp hơn trong 802.5 một ít. THT cho mỗi trạm được tính như trong phần trình bày về Token Ring, và được tinh chỉnh để có được một giá trị hợp lý. Ngoài ra, để đảm bảo cho mỗi trạm có cơ hội truyền trong một khoảng thời gian cụ thể nào đó, nghĩa là để đặt một cận trên cho giá trị TRT mà mọi trạm đều thấy được, chúng ta định nghĩa thông số "đích thời gian xoay vòng của thẻ bài" (target token rotation time – TTRT). (Việc các trạm thống nhất với nhau về thời gian TTRT

như thế nào sẽ được trình bày trong phần phía dưới). Mỗi trạm đo thời gian giữa hai lần liên tiếp thẻ bài đến nó, chúng ta gọi thời gian này là TRT đo được của trạm (measured TRT). Nếu thời gian TRT đo được của trạm lớn hơn thời gian TTRT được dàn xếp trước đó thì thẻ bài bị trễ, vì thế trạm sẽ không được truyền dữ liệu nữa. Ngược lại, thẻ bài đến sớm và trạm sẽ có quyền giữ thẻ bài trong khoảng thời gian (TTRT-TRT).
Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

87

Tuy nhiên, có vấn đề phát sinh như sau: Nếu một nút có quá nhiều dữ liệu cần phải gởi có cơ hội giữ thẻ bài, nó sẽ tận dụng hết thời gian giữ thẻ bài được phép. Vì thế nút kế sau nó sẽ tính toán và thấy thời gian TTRT và TRT là bằng nhau, nghĩa là nút kế sau này sẽ không có quyền truyền dữ liệu nữa. Để tính đến khả năng này, FDDI định nghĩa hai lớp giao thông trên mạng: đồng bộ và dị bộ. Khi một trạm có được thẻ bài, nó luôn được phép gởi dữ liệu dạng đồng bộ mà không cần phải quan tâm là thẻ bài tới sớm hay trễ. Ngược lại, trạm có thể gởi dữ liệu dạng dị bộ chỉ khi thẻ bài tới sớm. Chú ý rằng các khái niệm đồng bộ và dị bộ ở đây có thể gây hiểu lầm. Bằng cách dùng khái niệm đồng bộ, FDDI ám chỉ rằng giao thông trên mạng là có nhạy cảm với độ trễ thông tin. Ví dụ, người ta sẽ muốn gởi âm thanh hay video trên mạng FDDI theo kiểu đồng bộ. Ngược lại, những ứng dụng nào quan tâm đến thông lượng của đường truyền thì sẽ thích kiểu truyền dị bộ hơn. Ví dụ, ứng dụng truyền file trên mạng sẽ muốn sử dụng kiểu lưu thông dị bộ trên FDDI. Lại thêm vấn đề phát sinh: Do kiểu lưu thông dạng đồng bộ không có quan tâm đến việc thẻ bài đến sớm hay muộn, nên có khả năng nếu trạm co-dãn thời gian gởi dữ liệu đồng bộ thì thông số TTRT không còn ý nghĩa gì nữa! Để giải quyết vấn đề này, ta qui định: tổng thời gian gởi dữ liệu đồng bộ trong một vòng xoay của thẻ bài không được vượt quá TTRT.

5.5.3.3

Quản lý thẻ bài

Các cơ chế mà FDDI dùng để đảm bảo luôn có một thẻ bài hợp lệ chạy trên vòng cũng khác so với 802.5, do chúng dính với quá trình thiết đặt TTRT. Trước tiên, tất cả các trạm trong vòng luôn quan sát để đảm bảo là thẻ bài không bị mất. Để ý rằng một trạm trên vòng luôn có thể thấy được thời gian truyền hợp lệ của khung hay là thẻ bài. Thời gian rỗi tối đa giữa những lần truyền hợp lệ mà mỗi trạm nên biết qua là bằng độ trễ của vòng cộng với thời gian bỏ ra để truyền một khung đầy. (Trên một vòng có kích thước tối đa, thời gian tối đa để truyền một khung đầy là nhỏ hơn 2.5 ms). Do đó, mỗi trạm sẽ đặt bộ đếm lên, bộ đếm này sẽ hết hạn trong thời gian 2.5 ms. Nếu bộ đếm hết hạn, trạm sẽ nghi ngờ là có vấn đề không ổn và sẽ phát khung “thỉnh cầu”. Ngược lại khi bộ đếm chưa hết hạn mà trạm thấy được một sự truyền hợp lệ, nó sẽ đặt lại giá trị tối đa của bộ đếm là 2.5 ms. Khung thỉnh cầu trong FDDI khác với trong 802.5 do nó có chứa giá trị TTRT mà trạm mời chào (bid for the TTRT), nghĩa là: đó là thời gian xoay vòng của thẻ bài mà trạm cảm thấy đủ để các ứng dụng chạy trên nó thỏa mãn các ràng buộc về thời gian. Một trạm có thể gởi khung thỉnh cầu trong khi không có thẻ bài trong tay, và nó thường làm vậy khi có nghi ngờ mất thẻ bài hoặc khi mới tham gia vào vòng lần đầu tiên. Nếu khung thỉnh cầu đi được hết một vòng và quay lại, trạm phát sẽ xóa nó đi và hiểu rằng giá trị TTRT được mời chào trong đó là giá trị nhỏ nhất. Bây giờ có thể coi là trạm đang nắm thẻ bài, nghĩa là nó có trách nhiệm chèn vào mạng một thẻ bài hợp lệ, và có thể tiếp tục với giải thuật dùng thẻ bài thông thường. Khi một nút nhận được một khung thỉnh cầu, nó kiểm tra xem giá trị TTRT được mời chào trong đó có nhỏ hơn giá trị TTRT của chính nó không. Nếu nhỏ hơn, nó sẽ đặt lại giá trị TTRT của nó thành giá trị TTRT được mời chào. Nếu lớn hơn, trạm sẽ xóa khung thỉnh cầu này đi, chèn vào vòng một khung thỉnh cầu mới chứa giá trị

TTRT được mời chào bằng giá trị TTRT của nó. Trường hợp cuối cùng, nếu giá trị TTRT được mời chào bằng với giá trị TTRT của trạm, trạm sẽ so sánh địa chỉ của trạm gởi khung thỉnh cầu và địa chỉ của nó, địa chỉ nào lớn hơn sẽ thắng – nghĩa là bên thắng sẽ sở hữu khung thỉnh cầu. Do đó, nếu một khung thỉnh cầu đi hết một vòng và trở về trạm gởi, trạm gởi sẽ biết rằng nó là người mời chào giá trị TTRT duy nhất và nó có thể tạo ra một thẻ bài mới một cách an toàn. Tại thời điểm đó, tất cả các trạm bấy giờ đều đồng ý rằng giá trị TTRT là giá trị đủ nhỏ để làm cho tất cả chúng cảm thấy hạnh phúc! 5.5.4
8 Start of frame

Khuôn dạng của khung thông tin
8 Control 48 Dest addr 48 Src addr Body 32 CRC 8 End of frame 24 Status

H5.35 Khung thông tin FDDI

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

88

Do FDDI sử dụng cơ chế mã hóa 4B/5B, nên nó dùng các ký tự điều khiển 4B/5B. Ngoài ra trong phần Control có tồn tại một bit để phân biệt kiểu lưu thông là dị bộ hay đồng bộ.

5.5.5 Mạng không dây (802.11)

Mạng không dây là kỹ thuật nối mạng đang phát triển nhanh hiện nay. Như chúng ta đã biết, khả năng để xây dựng mạng không dây là hầu như không có giới hạn, trải dài từ cách sử dụng tín hiệu hồng ngoại để dựng mạng nội bộ trong phạm vi một tòa nhà cho đến việc kiến thiết mạng toàn cầu từ một lưới các vệ tinh quĩ đạo thấp. Phần này sẽ có cái nhìn gần hơn vào một kỹ thuật cụ thể xoay quanh chuẩn 802.11 đang nổi hiện nay. Giống như những người anh em Ethernet và Token Ring, 802.11 được thiết kế để hoạt động trong một phạm vi địa lý hẹp (các ngôi nhà, các tòa nhà văn phòng, các khu đại học) và thách thức quan trọng nó đặt ra là phải trù tính đến việc truy xuất đến phương tiện truyền thông chia sẻ - trong trường hợp này là các tín hiệu lan truyền trong không gian. 802.11 hỗ trợ thêm một số tính năng như các dịch vụ có giới hạn về thời gian, quản lý năng lượng và các cơ chế an toàn, nhưng chúng ta chỉ tập trung vào thảo luận về chức năng cơ bản của nó thôi.

5.5.5.1

Các tính chất vật lý

802.11 được thiết kế để chạy trên ba phương tiện vật lý khác nhau - hai dựa trên sóng radio phổ rộng và một dựa trên tia hồng ngoại được khuếch tán. Phiên bản chạy trên sóng radio hiện đang chạy với tốc độ 11 Mbps, nhưng có thể sớm đạt được tốc độ 54 Mbps. Ý tưởng đằng sau khái niệm phổ tần rộng là nhằm trải rộng tín hiệu lên trên một băng tần rộng hơn so với bình thường, vì thế có thể giảm thiểu tác động của sự giao thoa tín hiệu với các thiết bị khác. Ví dụ, kỹ thuật “nhảy tần số” (frequency hopping) là một kỹ thuật sử dụng phổ tần rộng, nó xoay quanh việc gởi tín hiệu qua một dãy tần số ngẫu nhiên; nghĩa là lần đầu sẽ gởi trên một tần số, lần hai gởi trên tần số khác, lần thứ ba và vân vân. Dãy tần số này không thật sự là ngẫu nhiên mà được tính toán một cách có giải thuật bởi một bộ sinh số ngẫu nhiên. Bên nhận sẽ dùng cùng một giải thuật như bên gởi và do đó có thể nhảy qua các tần số khác nhau đồng bộ với bên gởi để nhận chính xác khung thông tin. Một kỹ thuật sử dụng phổ tần rộng khác, được gọi là “dãy trực tiếp” (direct sequence), cũng đạt được cùng một hiệu quả bằng cách thể hiện một bit trong khung thành nhiều bit trong tín hiệu truyền đi. Với mỗi bit bên gởi muốn truyền đi, nó thực ra sẽ gởi một chuỗi bit là kết quả của phép toán exclusive-OR của bit đó với một chuỗi n bit ngẫu nhiên. Cũng như trong frequency hopping, chuỗi n bit này được sinh ra bởi một bộ sinh số ngẫu nhiên và được hiểu bởi cả hai bên gởi và nhận. Các giá trị được truyền đi, được gọi là “mã cắt lát” n bit (n-bit chipping code), sẽ rải tín hiệu trên một dãi tần rộng hơn gấp n lần so với dãi tần mà thông thường khung cần để được truyền đi. H5.35 là một ví dụ về mã cắt lát 4 bit.

H5.36 Ví dụ về mã cắt lát 4 bit.

802.11 định nghĩa một lớp vật lý sử dụng cơ chế “nhảy tần số” (trên 79 dải tần có độ rộng 1-Mhz), lớp vật lý thứ hai sử dụng “dãy trực tiếp” (sử dụng dãy cắt lát 11 bit). Cả hai chuẩn đều chạy trên sóng điện từ băng tần 2.4 GHz. Trong cả hai trường hợp, việc trải rộng phổ truyền đều có điểm

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

89

thú vị là làm cho tín hiệu giống như nhiễu đối với bất kỳ bên nhận nào không biết chuỗi ngẫu nhiên giả. Chuẩn vật lý thứ ba của 802.11 dựa trên tín hiệu hồng ngoại. Tín hiệu lưu thông sẽ được khuếch tán, nghĩa là bên gởi và bên nhận không cần phải hướng vào nhau và không cần tầm nhìn rõ ràng. Kỹ thuật này có phạm vi hoạt động khoảng 10 m và bị giới hạn chỉ trong các tòa nhà mà thôi.

5.5.5.2

Tránh đụng độ (Collision Avoidance)

Thoạt nhìn, có vẻ như giao thức không dây cũng tuân thủ cùng giải thuật như ở Ethernet: đợi cho đến khi đường truyền rỗi thì mới truyền, lùi lại nếu có đụng độ. 802.11 cũng làm tương tự như vậy. Tuy nhiên, vấn đề phức tạp hơn trong hệ thống mạng không dây, bởi vì không phải tất cả các nút đều có thể thấy nhau!

A

B

C

D

H5.37 Ví dụ về mạng không dây

Xét tình huống được chỉ ra trong H5.37, mỗi trạm chỉ có thể gởi và nhận tín hiệu đến hai nút kề trái và phải của nó. Ví dụ nút B có thể trao đổi các khung dữ liệu với nút A và C nhưng không thể phát tín hiệu đến D được, trong khi C chỉ có thể trao đổi với B và D mà không thể với A. (Tầm phủ sóng của A và D không được vẽ trong hình). Giả sử cả A và C cùng muốn nói giao tiếp với B và do đó chúng cùng gởi khung đến B. A và C không biết gì về nhau do sóng không thể đi xa như vậy. Hai khung này sẽ bị đụng độ tại B, nhưng không như trong Ethernet, không ai trong A và C hay biết gì về sự đụng độ này. A và C được gọi là các nút ẩn (hiden nodes) đối với nhau. Một vấn đề liên quan nữa, gọi là vấn đề "nút bị phơi trần" (exposed node problem), phát sinh trong tính huống sau: Giả sử B đang gởi cho A, nút C nhận biết được tình huống này vì nó nghe được việc truyền của B. Và sẽ là sai lầm nếu C kết luận là nó không thể truyền đến bất kỳ nút nào khác do nó nghe thấy B đang truyền. Ví dụ, giả sử C muốn truyền cho D thì việc này không gây ảnh hưởng gì vì việc truyền từ C đến D không can dự vào khả năng nhận tín hiệu của A từ B. (Chỉ gây ảnh hưởng khi A truyền cho B, nhưng trong trường hợp này B đang truyền). 802.11 giải quyết hai vấn đề trên bằng một giải thuật gọi là "Đa truy cập với cơ chế tránh đụng độ" – Multiple Access with Collision Avoidance (MACA). Ý tưởng là cho hai bên gởi và nhận trao đổi những khung điều khiển với nhau trước khi thật sự truyền dữ liệu. Việc trao đổi này dụng ý là để thông báo cho các trạm lân cận rằng một phiên truyền dữ liệu sắp xảy ra. Cụ thể giải thuật như sau: Bên gởi gởi một khung "yêu cầu gởi" – Request To

Send (RTS) đến bên nhận; khung RTS có chứa một trường, trong đó chỉ ra bên gởi muốn giữ kênh truyền bao lâu ( nghĩa là nó chỉ ra chiều dài của khung cần gởi). Bên nhận sẽ trả lời bằng khung “sẵn sàng nhận” – Clear To Send (CTS); khung này sẽ lặp lại trường chiều dài khung như phía bên gởi. Bất kỳ trạm nào thấy khung CTS cũng hiểu được rằng trạm bên nhận ở gần nó, cho nên nó sẽ không thể gởi khung trong khoảng thời gian được chỉ ra trong CTS. Còn những trạm thấy khung RTS nhưng không thấy khung CTS đâu thì chắc chắn là không ở gần bên nhận, do đó chúng có quyền tự do gởi khung đi. Có thêm hai chi tiết nữa để hoàn thiện bức tranh về Wireless LAN. Thứ nhất, bên nhận gởi một khung báo nhận (ACK) cho bên gởi sau khi đã nhận thành công một khung dữ liệu. Tất cả các nút khác phải chờ khung ACK này đi qua trước khi thử truyền khung của mình. (Khung ACK này không có trong phiên bản MACA gốc, thay vào đó nó được đề nghị trong một phiên bản mở rộng được gọi là MACW: MACA for Wireless LANs). Thứ hai, trường hợp có hơn hai trạm phát hiện kênh truyền rỗi, chúng sẽ gởi khung RTS cùng lúc, dẫn đến các khung này bị va chạm với nhau. 802.11 không có hỗ trợ cơ chế phát hiện đụng độ, thay vào đó, các trạm nhận ra sự đụng độ khi
Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

90

chúng không nhận được các khung CTS sau một khoảng thời gian nào đó. Nếu thế, mỗi trạm sẽ chờ đợi sau một khoảng thời gian ngẫu nhiên nào đó trước khi thử gởi khung RTS lần nữa. Khoảng thời gian mà một trạm chờ để thử lại được định nghĩa giống như thuật toán back-off trong Ethernet.

5.5.5.3

Hệ thống phân tán

Như những gì đã trình bày, 802.11 có thể thích hợp với cấu hình mạng dạng ad-hoc, trong đó các nút có thể hoặc không thể giao tiếp với những nút còn lại, tùy thuộc vào khoảng cách giữa chúng là gần hay xa. Ngoài ra, do một trong những thuận lợi của mạng không dây là các nút có thể tự do di chuyển do chúng không bị trói buộc bởi hệ thống dây nối, tập các nút có thể thấy nhau trực tiếp là thay đổi theo thời gian. Để giúp giải quyết vấn đề di động và nối kết một phần này, 802.11 định nghĩa thêm một kiến trúc trên một tập các nút. Các nút có quyền tự do giao tiếp trực tiếp với nhau như đã trình bày, nhưng trong thực tế chúng hoạt động bên trong kiến trúc này.

H5.38 Các điểm truy cập được nối kết vào mạng phân tán

Thay vì tất cả các nút được tạo ra như nhau, một số nút được phép đi lang thang (đó là máy laptop của bạn) và một số được nối kết tới một hạ tầng mạng có nối dây. Các trạm nối kết có dây được gọi là các điểm truy cập - “access point” (AP) và chúng được nối với nhau bằng cái gọi là hệ thống phân tán. H5.38 mô phỏng một hệ thống phân tán nối kết ba điểm truy cập, mỗi điểm truy cập phục vụ các nút di động trong khu vực mình phụ trách. Mỗi khu vực này giống như một cell trong hệ thống điện thoại di động, với AP hoạt động giống như Base station. Mặc dù hai nút có thể giao tiếp trực tiếp với nhau nếu chúng ở trong tầm với của nhau, tuy nhiên ý tưởng ở trong kiến trúc này là: mỗi nút sẽ kết hợp với một điểm truy cập của nó. Ví dụ, để nút A giao tiếp được với nút E, đầu tiên A gởi khung của nó đến điểm truy cập AP-1, AP-1 sẽ gởi khung qua hệ thống phân tán đến AP-3, rồi AP-3 sẽ phân phát khung đến E. Chỉ ra AP-1 làm cách nào để chuyển khung đến AP-3 là nằm ngoài phạm vi của 802.11, một giao thức cầu nối (sẽ được nghiên cứu ở tầng mạng) có thể được sử dụng để làm nhiệm vụ này. Những gì 802.11 có thể làm là xác định cách thức các nút chọn ra AP của chúng, và thú vị hơn nữa là làm sao giao thức này hoạt động được trong tình cảnh các nút di chuyển từ cell này đến cell khác. Kỹ thuật để chọn ra một AP được gọi là kỹ thuật “quét” (scanning) và nó xoay quanh bốn bước sau: 1. Nút gởi một khung Probe (thăm dò). 2. Tất cả điểm truy cập (AP) trong tầm với của nút sẽ trả lời bằng một khung Probe Response (trả lời thăm dò). 3. Nút sẽ chọn một trong các điểm truy cập trên và gởi đến điểm truy cập đó một khung Association Request (yêu cầu gia nhập). 4. Điểm truy cập trả lời bằng một khung Association Reponse (trả lời cho yêu cầu gia nhập). Một nút tiến hành giao thức này khi nó lần đầu tham gia vào mạng hoặc nó không hài lòng với AP hiện tại. Điều này có thể xảy ra, ví dụ như vì tín hiệu từ AP hiện tại yếu dần do nút càng di chuyển xa AP. Mỗi khi nút kiếm được AP mới, AP mới sẽ nhắc nhở AP cũ về sự thay đổi này.

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

91

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

H5.39 Sự di động của nút mạng

Lấy ví dụ như trong H5.38, khi mà nút C di chuyển từ cell được phục vụ bởi AP-1 sang cell được phục vụ bởi AP-2. Khi C di chuyển, nó gởi khung Probe đến AP-2 và được AP-2 trả lời bằng khung Probe Response. Tại thời điểm đó, C thích AP-2 hơn AP-2, do đó nó gia nhập vào điểm truy cập này. Cơ chế vừa được mô tả được gọi là cơ chế “quét chủ động” – active scanning, do nút chủ động dò tìm điểm truy cập. Các AP cũng thường xuyên gởi khung Beacon (đèn hiệu) để quảng cáo cho khả năng của mình, bao gồm tốc độ truyền được điểm truy cập hỗ trợ. Cơ chế này được gọi là “quét thụ động” – passive scanning, và một nút có thể chuyển sang điểm truy cập này đơn giản bằng cách gởi môt khung Association Request ngược lại AP.

5.5.5.4

Khuôn dạng khung

H5.40 Khuôn dạng khung 802.11

Hầu hết các thông tin trong khung 802.11, như được vẽ trong H5.40, là đều như chúng ta mong muốn. Khung bao gồm địa chỉ nguồn và đích, mỗi cái dài 48 bits; dữ liệu tối đa 2312 bytes; và phần kiểm tra lỗi CRC 32 bits. Trường Control chứa ba trường con: Trường Type dài 6 bits – dùng để chỉ ra khung là khung dữ liêu, hay là khung RTS, hay là CTS, hoặc cũng được sử dụng bởi giải thuật quét; một cặp trường mỗi trường dài 1 bit gọi là ToDS và FromDS, sẽ được giải thích ngay sau đây. Điều kỳ dị trong khung 802.11 là nó chứa đến bốn địa chỉ. Cách thức thông dịch các địa chỉ này lại phụ thuộc vào việc thiết đặt các bít ToDS và FromDS trong trường Control. Điều này là để tính đến khả năng khung phải được chuyển tiếp qua hệ thống phân tán, có nghĩa là bên gởi nguyên thủy không nhất thiết phải là nút phát khung gần đây nhất. Cũng tương tự đối với địa chỉ bên nhận. Trong trường hợp đơn giản nhất, khi một nút gởi khung trực tiếp đến nút kia, cả hai bit DS đều có giá trị 0, Addr1 chứa địa chỉ nút đích, Addr2 chứa địa chỉ nút nguồn. Trong trường hợp phức tạp nhất, cả hai bit DS mang giá trị 1, chỉ ra rằng khung thông tin đi từ nút không dây qua hệ thống phân tán và rồi từ hệ thống phân tán đến nút không dây bên đích. Với cả hai bit DS được đặt, Addr1 định danh đích cuối cùng, Addr2 định danh nút gởi tạm thời (là nút đã chuyển khung từ hệ thống phân tán đến đích cuối cùng), Addr3 định danh nút đích tạm thời (là nút đã nhận khung từ nút không dây và trung chuyển khung xuyên qua hệ thống phân tán), Addr4 định danh nút gởi nguyên thủy. Trong ví dụ H5.37, Addr1=E, Addr2=AP-3, Addr3=AP-1, Addr4=A.

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

92

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

Chương 6: Tầng mạng (Network Layer)
Mục đích
Chương này nhằm giới thiệu cho người đọc những nội dung sau: • Vai trò của router trong việc xây dựng các liên mạng có phạm vi rộng và không đồng nhất về chuẩn của các mạng cục bộ thành phần • Các dịch vụ mà tầng mạng phải cung cấp cho tầng vận chuyển • Cơ chế hoạt động của router • Các vấn đề liên quan đến giải thuật chọn đường cho các router • Giới thiệu về bộ giao thức liên mạng IP

Yêu cầu
Sau khi học xong chương này, người đọc phải có được những khả năng sau: • Mô tả được sơ đồ tổng quát của một liên mạng ở tầng 3 và vai trò của router trong liên mạng này • Trình bày được các dịch vụ mà tầng mạng phải cung cấp cho tầng vận chuyển • Giải thích cơ chế truyền tải thông tin theo kỹ thuật truyền tải lưu và chuyển tiếp của các router • Giải thích được ý nghĩa của bảng chọn đường trong router • Phân biệt được các loại giải thuật chọn đường khác nhau • Cài đặt được các giải thuật chọn đường Dijkstra, Ford-Fulkerson, Distance Vector, Link state • Nêu lên được các phương pháp để chống tắc nghẽn trên mạng diện rộng • Biết cách thiết lập sơ đồ đánh địa chỉ IP cho mạng • Thực hiện được việc phân mạng con theo những yêu cầu khác nhau theo cả hai phương pháp : Phân lớp hoàn toàn và Vạch đường liên miền không phân lớp • Xây dựng được bảng chọn đường thủ công cho các router trong mạng IP • Nêu lên được ý nghĩa của các giao thức ARP, RARP và ICMP trong bộ giao thức IP

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

93

6.1 Giới thiệu

Chúng ta đã xem xét cách thức xây dựng và vận hành của các mạng đơn lẻ sử dụng các nối kết điểm điểm, các đường truyền chia sẻ và các bộ hoán chuyển (switch). Vấn đề phát sinh là có nhiều người muốn xây dựng hệ thống mạng riêng của họ theo nhiều kỹ thuật khác nhau nhưng lại muốn giao tiếp với nhau mà không quan tâm rằng họ đang hoạt động trên các hệ thống không đồng nhất. Chương này sẽ trình bày về cách thức để nối kết những mạng không đồng nhất lại với nhau. Có hai vấn đề quan trọng cần phải quan tâm khi nối kết các mạng: tính không đồng nhất (heterogeneity) và phạm vi (scale) khác nhau của chúng. Giải thích một cách đơn giản, tính không đồng nhất là khi người dùng trên hai mạng khác kiểu nhau muốn giao tiếp với nhau. Phức tạp hơn một chút, ta có thể thấy việc nối kết các host trên các mạng khác nhau có thể sẽ đòi hỏi việc duyệt qua nhiều mạng trung gian, mà các mạng trung gian này lại có thể có kiểu khác nhau. Chúng có thể là mạng Ethernet, Token Ring hay mạng dạng điểm nối điểm, hoặc nhiều kiểu mạng hoán chuyển (switch) khác nhau, và chúng lại sử dụng các phương thức đánh địa chỉ riêng, các phương pháp truy cập đường truyền riêng và cả mô hình dịch vụ riêng nữa. Thách thức đối với vấn đề không đồng nhất là làm sao cung cấp cho người dùng một dịch vụ nối kết host-host dễ hiểu xuyên qua mớ hỗn độn các mạng không đồng nhất. Để hiểu về vấn đề phạm vi mạng, ta lấy một ví dụ có giá trị là sự phát triển của mạng Internet, mạng có tốc độ phát triển gần gấp đôi sau mỗi năm trong vòng 20 năm qua. Kiểu phát triển chóng mặt này buộc chúng ta phải đối mặt với nhiều thách thức. Một trong số đó là việc vạch đường: Làm sao để tìm ra một đường đi hữu hiệu xuyên qua một mạng gồm cả triệu nút mạng? Thêm một vấn đề có liên quan đến vạch đường là phương pháp đánh địa chỉ, là cách gán cho mỗi nút trên mạng một định danh duy nhất. Tầng mạng có nhiệm vụ đưa các gói tin từ máy gởi qua các chặn đường để đến được máy nhận. Để đến được đích đến, gói tin có thể phải đi từng bước một qua nhiều router trung gian. Điều này thì trái ngược với tầng liên kết dữ liệu vốn chỉ chịu trách nhiệm truyền tải các khung đi từ đầu này đến đầu kia của một kênh truyền vật lý. Để thực hiện được nhiệm vụ này, tầng mạng phải biết được hình trạng của mạng đường trục (subnet) và chọn đường thích hợp để cho gói tin đi. Nó phải chú ý đến việc chọn đường sao cho tránh được tình trạng tắc nghẽn trên một số đường truyền và router trong khi số khác thì đang rãnh rỗi.

6.2 Các vấn đề liên quan đến việc thiết kế tầng mạng

6.2.1 Kỹ thuật hoán chuyển lưu và chuyển tiếp (Store-and-Forward Switching)

Xét một liên mạng như hình dưới đây

H6.1 Kỹ thuật lưu và chuyển tiếp trên tầng mạng

Trong đó các router nằm trong hình oval được nối lại với nhau bằng các đường truyền theo kiểu điểm nối điểm được gọi là các thiết bị của nhà cung cấp đường truyền (Carrier's equipment). Các thiết bị nằm bên ngoài hình oval được gọi là các thiết bị của khách hàng (Customer's Equipment).

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

94

Máy tính H1 được nối trực tiếp vào router A của nhà cung cấp đường truyền bằng một đường nối kết thường trực (lease line). Máy H2 nối kết vào một mạng LAN cục bộ. Trong mạng LAN có router F thuộc sở hữu của khách hàng. F được nối với router E của nhà cung cấp cũng bằng một đường nối kết thường trực. Cho dù cách thức nối kết vào mạng của các máy tính có thể khác nhau như trường hợp máy H1 và H2, nhưng cách thức các gói tin của chúng được truyền đi đều giống nhau. Một máy tính có một gói tin cần truyền đi sẽ gởi gói tin đến router gần nó nhất, có thể là router trên LAN của nó hoặc router của nhà cung cấp đường truyền. Gói tin được lưu lại ở đó và được kiểm tra lỗi. Kế đến gói tin sẽ được chuyển đến một router kế tiếp trên đường đi đến đích của gói tin. Và cứ tiếp tục như thế cho đến khi đến được máy nhận gói tin. Đây chính là kỹ thuật lưu và chuyển tiếp.

6.2.2 Các dịch vụ cung cấp cho tầng vận chuyển
Các dịch vụ tầng mạng cung cấp cho tầng vận chuyển cần được thiết kế hướng đến các mục tiêu sau: Các dịch vụ này cần nên độc lập với kỹ thuật của các router. 1. Tầng vận chuyển cần được độc lập với số lượng, kiểu và hình trạng của các router hiện hành. 2. Địa chỉ mạng cung cấp cho tầng vận chuyển phải có sơ đồ đánh số nhất quán cho dù chúng là LAN hay WAN. Tầng mạng cung cấp hai dịch vụ chính là Dịch vụ không nối kết (Connectionless Service) và Dịch vụ định hướng nối kết (Connection – Oriented Service). Trong dịch vụ không nối kết, các gói tin được đưa vào subnet một cách riêng lẽ và được vạch đường một cách độc lập nhau. Không cần thiết phải thiết lập nối kết trước khi truyền tin. Các gói tin trong trường hợp này được gọi là thư tín (Datagram) và subnet được gọi là Datagram Subnet. Ngược lại trong dịch vụ định hướng nối kết, một đường nối kết giữa bên gởi và bên nhận phải được thiết lập trước khi các gói tin có thể được gởi đi. Nối kết này được gọi là mạch ảo (Virtual Circuit) tương tự như mạch vật lý được nối kết trong hệ thống điện thoại và subnet trong trường hợp này được gọi là virtual circuit subnet.

6.2.2.1

Cài đặt dịch vụ không nối kết ( Implementation of Connectionless Service)

Xét hệ thống mạng như hình H6.2. Giả sử rằng quá trình P1 có nhiều thông điệp cần gởi cho quá trình P2. Khi đó P1 sẽ gởi các thông điệp này cho tầng vận chuyển và yêu cầu tầng vận chuyển truyền sang quá trình P2 trên máy tính H2. Tầng vận chuyển sẽ gắn thêm tiêu đề (header) của nó vào thông điệp và chuyển các thông điệp xuống tầng mạng.

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

Đích đến

Bước kế tiếp

H6.2 Hoạt động của Datagram subnet

Giả sử rằng thông điệp gởi đi thì lớn gấp 4 lần kích thước tối đa của một gói tin, vì thế tầng mạng phải chia thông điệp ra thành 4 gói tin 1,2,3 và 4, và lần lượt gởi từng gói một đến router A bằng một giao thức điểm nối điểm như PPP chẳng hạn. Mỗi router có một bảng thông tin cục bộ chỉ ra nơi nào có thể gởi các gói tin để có thể đến được những đích đến khác nhau trên mạng. Mỗi mục từ của bảng chứa 2 thông quan trọng nhất đó là Đích đến (Destination) và ngỏ ra kế tiếp (Next Hop) cần phải chuyển gói tin đến để có thể đến được đích đến này. Ta gọi là bảng chọn đường (Routing Table). Ví dụ Lúc khởi đầu, router A có bảng chọn đường như hình H6.2 (lúc đầu). Khi gói tin 1,2 và 3 đến router A, nó được lưu tạm thời để kiểm tra lỗi. Sau đó chúng được chuyển tiếp sang router C vì theo thông tin trong bảng chọn đường của A. Gói tin 1 sau đó tiếp tục được chuyển đến E và kế đến là F. Sau đó nó được gói lại trong một khung của tầng liên kết dữ liệu và được chuyển đến máy H2 bởi mạng LAN. Các gói tin 2 và 3 cũng có cùng đường đi tương tự. Sau đó, do một số sự cố về đường truyền, router A cập nhật lại bảng chọn đường của mình như hình H6.2(lúc sau). Khi đó gói tin số 4 đến router A, nó sẽ chuyển gói tin này sang B để có thể đi được đến H2. Giải thuật chịu trách nhiệm quản lý thông tin trong bảng chọn đường cũng như thực hiện các quyết định về chọn đường được gọi là Giải thuật chọn đường (Routing algorithm).

6.2.2.2

Cài đặt dịch vụ định hướng nối kết (Connection – Oriented Service)

Đối với dịch vụ nối kết định hướng chúng ta cần một mạch ảo trên subnet. Mục đích của việc sử dụng mạch ảo là để tránh phải thực hiện việc chọn lại đường đi mới cho mỗi gói tin gởi đến cùng một đích. Khi một nối kết được thực hiện, một đường đi từ máy tính gởi đến máy tính nhận được chọn như là một phần của giai đoạn thiết lập nối kết (Connection setup) và được lưu trong bảng chọn đường của các router nằm trên đường đi. Khi nối kết kết thúc, mạch ảo bị xóa. Với dịch vụ định hướng nối kết, mỗi gói tin có mang một số định dạng để xác định mạch ảo mà nó thuộc về.

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

96

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

H6.3 Hoạt động của Datagram subnet

Như hình H6.3, máy tính H1 thực hiện một nối kết với máy tính H2 qua nối kết số 1. Nối kết này được ghi nhận trong mục từ đầu tiên trong bảng chọn đường của các router. Dòng đầu tiên trong bảng chọn đường của router A nói rằng: những gói tin mang số nhận dạng nối kết số 1 đến từ máy H1 phải được gởi sang router C với số nhận dạng nối kết là 1. Tương tự, cho các mục từ đầu tiên của router C và E. Điều gì xảy ra nếu máy tính H3 muốn nối kết với máy tính H2. Nó chọn số nhận dạng nối kết là 1, vì đây là nối kết đầu tiên đối với H3, và yêu cầu subnet thiết lập mạch ảo. Điều này đã làm cho các router phải thêm vào mục từ số 2 trong bảng chọn đường. Đối với router A, số nhận dạng nối kết với H3 là 1, trùng với nối kết với H1, không làm router A lẫn lộn vì A có thêm thông tin máy gởi là H1 hay H3. Tuy nhiên, đối với các router C, E và F thì không thể phân biệt được đâu là nối kết của H1 và đâu là nối kết của H3 nếu sử dụng số nhận dạng nối kết là 1 cho cả 2 nối kết. Chính vì thế A đã gán một số nhận dạng khác, là số 2, cho các gói tin gởi đến C có nguồn gốc từ H3.

6.2.2.3

So sánh giữa Datagram subnet và Virtual-Circuit subnet

Bảng sau so sánh điểm mạnh và điểm yếu của 2 loại dịch vụ không nối kết và định hướng nối kết: Vấn đề Thiết lập nối kết Đánh địa chỉ Thông tin trạng thái Chọn đường Ảnh hưởng khi router bị hỏng Chất lượng dịch vụ Datagram Subnet Không cần Mỗi gói tin chứa đầy đủ địa chỉ gởi và nhận Router không cần phải lưu giữ thông tin trạng thái của các nối kết Mỗi gói tin có đường đi khác nhau Không bị ảnh hưởng, ngoại trừ gói tin đang trên đường truyền bị hỏng Khó đảm bảo Circuit Subnet Cần thiết Mỗi gói tin chỉ chứa số nhận dạng nối kết có kích thước nhỏ. Mỗi nối kết phải được lưu lại trong bảng chọn đường của router. Đường đi được chọn khi mạch ảo được thiết lập, sau đó tất cả các gói tin đều đi trên đường này. Tất cả các mạch ảo đi qua router bị hỏng đều bị kết thúc Có thể thực hiện dễ dàng nếu có đủ tài nguyên gán trước cho từng nối kết 97

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

Điều khiển tắc nghẽn

Khó điều khiển

Có thể thực hiện dễ dàng nếu có đủ tài nguyên gán trước cho từng nối kết

6.3 Giải thuật chọn đường
6.3.1 Giới thiệu
Vạch đường về bản chất là một bài toán trong lý thuyết đồ thị. Hình 6.4 thể hiện một đồ thị biểu diễn cho một mạng.

A 3 4 C B 9 1 1 D 1 E

6 2 F

H6.4 Mạng được biểu diễn như một đồ thị

Các nút trong đồ thị (được đánh dấu từ A đến F) có thể là các host, switch, router hoặc là các mạng con. Ở đây chúng ta tập trung vào một trường hợp các nút là các router. Các cạnh của đồ thị tương ứng với các đường nối kết mạng. Mỗi cạnh có một chi phí đính kèm, là thông số chỉ ra cái giá phải trả khi lưu thông trên nối kết mạng đó. Vấn đề cơ bản của việc vạch đường là tìm ra đường đi có chi phí thấp nhất giữa hai nút mạng bất kỳ, trong đó chi phí của đường đi được tính bằng tổng chi phí khi đi qua tất cả các cạnh làm thành đường đi đó. Nếu không có một đường đi giữa hai nút, thì độ dài đường đi giữa chúng được xem như bằng vô cùng.

6.3.2 Mục tiêu của giải thuật chọn đường
Xác định đướng đi nhanh chóng, chính xác. Khả năng thích nghi được với những thay đổi về hình trạng mạng. Khả năng thích nghi được với những thay đổi về tải đường truyền. Khả năng tránh được các nối kết bị tắt nghẽn tạm thời Chi phí tính toán để tìm ra được đường đi phải thấp

6.3.3 Phân loại giải thuật chọn đường
Giải thuật chọn đường có thể được phân thành những loại sau: Chọn đường tập trung (Centralized routing): Trong mạng có một Trung tâm điều khiển mạng (Network Control Center) chịu trách nhiệm tính toán và cập nhật thông tin về đường đi đến tất cả các điểm khác nhau trên toàn mạng cho tất cả các router. Chọn đường phân tán (Distributed routing): Trong hệ thống này, mỗi router phải tự tính toán tìm kiếm thông tin về các đường đi đến những điểm khác nhau trên mạng. Để làm được điều này, các router cần phải trao đổi thông tin quan lại với nhau. Chọn đường tĩnh (Static routing): Trong giải thuật này, các router không thể tự cập nhật thông tin về đường đi khi hình trạng mạng thay đổi. Thông thường nhà quản mạng sẽ là người cập nhật thông tin về đường đi cho router. Chọn đường động (Dynamic routing): Trong giải thuật này, các router sẽ tự động cập nhật lại thông tin về đường đi khi hình trạng mạng bị thay đổi.

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

98

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

6.3.4 Các giải thuật tìm đường đi tối ưu
Đường đi tối ưu từ A đến B là đường đi "ngắn" nhất trong số các đường đi có thể. Tuy nhiên khái niệm "ngắn" nhất có thể được hiểu theo nhiều ý nghĩa khác nhau tùy thuộc vào đơn vị dùng để đo chiều dài đường đi. Đối với các router, các đại lượng sau có thể được sử dụng để đo độ dài đường đi: o Số lượng các router trung gian phải đi qua (HOP) o Độ trì quản trung bình của các gói tín o Cước phí truyền tin Mỗi giải thuật chọn đường trước tiên phải chọn cho mình đơn vị đo chiều dài đường đi. Để xác định được đường đi tối ưu, các giải thuật chọn đường sử dụng phương pháp đồ thị để tính toán. Trước tiên, nó mô hình hóa hình trạng mạng thành một đồ thị có các đặc điểm như sau: Nút là các router. Cạnh nối liền 2 nút là đường truyền H6.5 Mô hình hóa mạng thành đồ thị nối hai router. Trên mỗi cạnh có giá đó là chiều dài đường đi giữa 2 router thông qua đường truyền nối hai router . Chiều dài đường đi từ nút A đến nút B là tổng tất cả các giá của các cạnh nằm trên đường đi. Nếu không có đường đi giữa 2 router thì xem như giá là vô cùng. Trên đồ thị này sẽ thực hiện việc tính toán tìm đường đi ngắn nhất.

6.3.4.1

Giải thuật tìm đường đi ngắn nhất Dijkstra

Mục đích là để tìm đường đi ngắn nhất từ một nút cho trước trên đồ thị đến các nút còn lại trên mạng. Giải thuật được mô tả như sau: Gọi: o S là nút nguồn cho trước o N: là tập hợp tất cả các nút đã xác định được đường đi ngắn nhất từ S. o Di: là độ dài đường đi ngắn nhất từ nút nguồn S đến nút i. o lij: là giá của cạnh nối trực tiếp nút i với nút j, sẽ là ∞ nếu không có cạnh nối trực tiếp giữa i và j. o Pj là nút cha của của nút j. Bước 1: Khởi tạo o N={S}; Ds=0; o Với ∀i≠S: Di=lsi , Pi=S Bước 2: Tìm nút gần nhất kế tiếp o Tìm nút i ∉ N thoả Di= min (Dj) với j ∉ N o Thêm nút i vào N. o Nếu N chứa tất cả các nút của đồ thị thì dừng. Ngược lại sang Bước 3 o Bước 3: Tính lại giá đường đi nhỏ nhất Với mỗi nút j ∉ N: Tính lại Dj= min{ Dj, Di+ lij} ; Pj=i; Trở lại Bước 2 Ví dụ: Cho mạng có hình trạng như đồ thị hình H6.6: Tìm đường đi ngắn nhất từ nút 1 đến các nút còn lại. Áp dụng giải thuật ta có: S=1 Các bước thực hiện được mô tả như sau:

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

H6.6 Hình trạng mạn

99

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

Lần lặp Khởi tạo 1 2 3 4 5

N {1} {1,3} {1,3,2} {1,3,2,6} {1,3,2,6,4} {1,3,2,6,4,5}

D2 3 3 3

D3 2 2

D4 5 4 4 4 4

D5 ∞ ∞ 7 5 5 5

D6 ∞ 3 3 3

P2 1 1 1

P3 1 1

P4 1 3 3 3 3

P5 1 1 2 6 6 6

P6 1 3 3 3

Từ kết quả trên ta vẽ được cây có đường đi ngắn nhất từ nút số 1 đến các nút còn lại như hình H6.7. Từ cây đường đi ngắn nhất này, ta xác định được rằng: để đi đến các router router 4, 5, 6 , bước kế tiếp router 1 cần gởi gói tin đến là router số 3 (next hop). Chú ý, đường ngắn nhất này chỉ đúng theo hướng từ nút số 1 về các nút còn lại và chỉ đúng cho nút số 1 mà thôi. Thông thường giải thuật Dijkstra được sử dụng theo mô hình chọn đường tập trung. Trong đó, Trung tâm điều khiển mạng sẽ tìm cây đường đi ngắn nhất cho từng router trên mạng và từ đó xây dựng bảng chọn đường tối ưu cho tất cả các router.

H6.7 Cây đường đi ngắn nhất từ nút 1

6.3.4.2

Giải thuật chọn đường tối ưu Ford-Fulkerson

Mục đích của giải thuật này là để tìm đường đi ngắn nhất từ tất cả các nút đến một nút đích cho trước trên mạng. Giải thuật được mô tả như sau: Gọi o d là nút đích cho trước o Di là chiều dài đường đi ngăn nhất từ nút i đến nút d. o Ci là nút con của nút i Bước 1: Khởi tạo: o Gán Dd = 0; o Với ∀i≠d: gán Di= ∞; Ci= -1; Bước 2: Cập nhật giá đường đi

ngắn nhất từ nút i đến nút d o Di= min{ lij+ Dj} với ∀j≠i => Ci = j; o Lặp lại cho đến khi không còn Di nào bị thay đổi giá trị Ví dụ, cho sơ đồ mạng có hình trạng như đồ thị hình H6.8. Hãy tìm đường đi ngắn nhất từ nút khác trên đồ thị đến nút 6. Áp dụng giải thuật ta có: d=6 Các bước thực hiện được mô tả như sau:

H6.8 Hình trạng mạng

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

100

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

Lần lặp Khởi tạo 1 2 3

D1 ∞ ∞ 3 3

D2 ∞ ∞ 4 4

D3 ∞ 1 1 1

D4 ∞ 3 3 3

D5 ∞ 2 2 2

C1 -1 -1 3 3

C2 -1 -1 4 4

C3 -1 6 6 6

C4 -1 3 3 3

C5 -1 6 6 6

Từ kết quả trên ta vẽ lại được cây đường đi ngắn nhất từ các nút khác nhau về nút đích số 6 như H6.9. Cây này cho phép xác định đường đi tối ưu từ những nút khác nhau về nút số 6. Chẳng hạn tại nút 1, để đi về nút số 6 thì bước kế tiếp phải đi là nút số 3. Tương tự, tại nút 2, để đi về nút số 6 thì bước kế tiếp phải đi là nút số 4. Giải thuật này được sử dụng theo mô hình phân tán. Ở đó mỗi router sẽ tự tính toán, tìm cây có đường đi ngắn nhất từ các nút khác về nó. Từ đó suy ra đường đi tối ưu cho các nút khác đến nó và gởi các đường đi này đến từng nút trên mạng.

H6.9 Cây đường đi ngắn nhất về nút 6

6.3.5 Giải pháp vạch đường Vector Khoảng cách (Distance Vector)
Ý tưởng của Distance-Vector như sau: Mỗi nút thiết lập một mảng một chiều (vector) chứa khoảng cách (chi phí) từ nó đến tất cả các nút còn lại và sau đó phát vector này đến tất cả các nút láng giềng của nó. Giả thiết đầu tiên trong Distance-Vector là: mỗi nút phải biết được chi phí của các đường nối từ nó đến tất cả các nút láng giềng có đường nối kết trực tiếp với nó. Một nối kết bị đứt (down) sẽ được gán cho chi phí có giá trị vô cùng. Để xem xét giải thuật vạch đường Distance-Vector hoạt động như thế nào, cách dễ nhất là xem xét đồ thị được cho như trong hình H6.10
B C A D E

F

G

Hình 6.10 Một mạng làm ví dụ trong giải thuật Distance-Vector

Trong ví dụ này, chi phí trên mỗi đường nối đều được đặt là 1. Chúng ta có thể biểu diễn sự hiểu biết của các nút về khoảng cách từ chúng đến các nút khác như trong bảng H6.11
Thông tin được lưu tại các nút A B C D E F G A
0 1 1 ∞ 1 1 ∞

B
1 0 1 ∞ ∞ ∞ ∞

Khoảng cách đến nút C D E
1 1 0 1 ∞ ∞ ∞ ∞ ∞ 1 0 ∞ ∞ 1 1 ∞ ∞ ∞ 0 ∞ ∞

F
1 ∞ ∞ ∞ ∞ 0 1

G
∞ ∞ ∞ 1 ∞ 1 0

H6.11 Các khoảng cách ban đầu được lưu tại mỗi nút

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

101

Chúng ta có thể xem mỗi một hàng trong bảng 6.11 như là một danh sách các khoảng cách từ một nút đến tất cả các nút khác. Khởi đầu, mỗi nút đặt giá trị 1 cho đường nối kết đến các nút láng giềng kề nó, ∞ cho các đường nối đến tất cả các nút còn lại. Do đó, lúc đầu A tin rằng nó có thể tìm đến B qua một bước nhảy (hop) và rằng nó không thể đi đến D được. Bảng vạch đường lưu tại A thể hiện những niềm tin mà A có được, ngoài ra còn lưu thêm nút kế tiếp mà A cần phải đi ra để đến một nút nào đó. Khởi đầu, bảng vạch đường của nút A trông giống như trong bảng 6.12
Đích (Destination) B C D E F G Chi phí (Cost) 1 1 ∞ 1 1 ∞ Nút kế tiếp (Next Hop) B C E F -

H6.12 Bảng vạch đường khởi đầu tại nút A

Bước kế tiếp trong giải thuật vạch đường Distance-Vector là: mỗi nút sẽ gởi một thông điệp đến các láng giềng liền kề nó, trong thông điệp đó chứa danh sách các khoảng cách mà cá nhân nút tính được. Ví dụ, nút F bảo nút A rằng F có thể đi đến nút G với chi phí là 1; A cũng biết được rằng nó có thể đến F với chi phí là 1, vì thế A cộng các chi phí lại thành chi phí đi đến G là 2 thông qua F. Tổng chi phí là 2 này nhỏ hơn chi phí vô cùng lúc đầu, do đó A ghi lại nó có thể đi đến G thông qua F với chi phí là 2. Tương tự, A học được từ C rằng, nó có thể đi đến D thông qua C với chi phí là 2, và chi phí này nhỏ hơn chi phí cũ là vô cùng. Cùng lúc A cũng học từ C rằng, nó có thể đi đến B thông qua C với chi phí là 2, nhưng chi phí này lại lớn hơn chi phí cũ là 1, vì thế thông tin mới này bị bỏ qua. Tại thời điểm này, A có thể cập nhật lại bảng chọn đường của nó với chi phí và nút ra kế tiếp để có thể đi đến tất cả các nút khác trong mạng. Kết quả được cho trong bảng H6.13
Đích (Destination) B C D E F G Chi phí (Cost) 1 1 2 1 1 2 Nút kế tiếp (Next Hop) B C C E F F

H.6.13 Bảng vạch đường cuối cùng tại nút A

Nếu không có sự thay đổi về hình trạng mạng nào, chỉ cần vài cuộc trao đổi thông tin vạch đường giữa các nút trong mạng thì mọi nút đều có được thông tin vạch đường hoàn hảo. Quá trình đem thông tin vạch đường nhất quán đến mọi nút trong mạng được gọi là sự hội tụ (convergence). Hình 6.14 chỉ ra thông tin về chi phí cuối cùng từ một nút đến các nút khác trong mạng khi quá trình vạch đường đã hội tụ.

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0
Thông tin được lưu tại các nút A B C D E F G

A 0 1 1 2 1 1 2

B 1 0 1 2 2 2 3

Khoảng cách đến nút C D E 1 2 1 1 2 2 0 1 2 1 0 3 2 3 0 2 2 2 2 1 3

F 1 2 2 2 2 0 1

G 2 3 2 1 3 1 0

H6.14 Các khoảng cách cuối cùng được lưu tại mỗi nút

Nét đẹp của loại giải thuật phân tán như trên nằm ở chỗ nó cho phép tất cả các nút đạt được thông tin vạch đường mà không cần phải có sự hiện diện của bộ điều khiển trung tâm nào. Còn có vài chi tiết làm cho giải thuật Distance-Vector hoàn hảo hơn. Thứ nhất, chú ý rằng có hai tình huống khác nhau mà tại đó một nút quyết định gởi thông tin vạch đường của mình cho các nút láng giềng kề bên. Tình huống đầu tiên là sự cập nhật theo chu kỳ (periodic update). Trong tình huống này, mỗi nút tự động gởi bản cập nhật thường xuyên, ngay cả khi không có thay đổi gì trong đó cả. Điều này giúp cho các nút khác biết được nút hiện tại đang còn sống. Vả lại việc cập nhật thường xuyên còn giúp cho các nút láng giềng có thể có được thông tin vạch đường nhanh chóng trong trường hợp thông tin của chúng bị mất. Tần số phát thông tin vạch đường đi có thể khác nhau tùy vào giải thuật, chúng thường có giá trị từ vài giây đến vài phút. Tình huống thứ hai gọi là sự cập nhật do bị kích hoạt (triggered update). Tình huống này xảy ra mỗi khi có sự thay đổi thông tin trong bảng vạch đường của nút. Nghĩa là mỗi khi bảng vạch đường có sự thay đổi, nút sẽ gởi bản cập nhật này cho các láng giềng của mình. Bây giờ ta xem xét điều gì xảy ra khi một đường nối kết hay một nút bị hỏng. Những nút đầu tiên phát hiện ra điều này sẽ gởi thông tin vạch đường mới cho láng giềng của chúng ngay, và thông thường hệ thống sẽ ổn định với tình trạng mới một cách nhanh chóng. Còn đối với câu hỏi làm sao nút phát hiện ra sự cố, có nhiều câu trả lời khác nhau. Cách tiếp cận thứ nhất là: một nút liên tục kiểm tra đường nối tới các nút láng giềng khác bằng cách gởi các gói tin điều khiển tới chúng và kiểm tra xem nó có nhận được các gói tin trả lời hay không. Cách tiếp cận khác là: một nút phát hiện ra một đường nối kết (hay nút ở đầu kia của đường nối) gặp sự cố khi nó không nhận được thông tin vạch đường một cách định kỳ từ láng giềng của nó. Ví dụ, xem xét điều gì sẽ xảy ra khi F phát hiện ra đường nối từ nó đến G bị hỏng. Đầu tiên, F đặt chi phí của đường nối từ nó đến A thành vô cùng và gởi thông tin này đến A. Do A đã biết là cần 2 bước để đi từ nó đến G thông qua F, A sẽ đặt lại chi phí từ nó đến G là vô cùng. Tuy nhiên, với bản cập nhật kế tiếp từ C, A phát hiện ra rằng có một đường đi dài 2 hops từ C đến G, do đó nó sẽ cập nhật lại đường đi từ nó đến G dài 3 hops thông qua C. Và khi A quảng cáo thông tin này cho F, F lại cập nhật lại đường đi dài 4 hops đến G thông qua A. Không may là: một số tình huống phát sinh lỗi khác lại làm cho mạng mất ổn định nghiêm trọng. Giả sử nối kết từ A đến E bị đứt. Trong những chu kỳ cập nhật sau, A thông báo đường đi từ nó đến E dài vô cùng, nhưng B và C lại quảng cáo

đường đi từ chúng đến E dài 2 hops. Nếu các bản cập nhật được định thời để phát cùng lúc, B sẽ sửa lại độ dài đường đi từ nó đến E là 3 thông qua C, C sửa lại độ dài đường đi từ nó đến E là 3 thông qua B. Sau đó A lại nghe B và C quảng cáo độ dài đường đi từ chúng đến E là 3 và giả sử A chọn B là nút kế tiếp để đi đến E, nó sẽ cập nhật lại độ dài đoạn đường là 4. Đến chu kỳ kế tiếp, B nghe C nói độ dài từ C đến E là 3 nên cập nhật lại độ dài đường đi từ B đến E là 4 thông qua C, C thì làm ngược lại: sửa lại con đường từ nó đến E là 4 thông qua B. Rồi lại đến lượt A nghe B sửa lại độ dài từ A đến E là 5 thông qua B. Sự thể sẽ tiếp diễn cho đến khi các độ dài tăng đến một số có thể coi là vô cùng. Nhưng tại thời điểm này, không nút nào biết là E không thể đến được, và các bảng vạch đường trong mạng luôn không ổn định. Tình huống này được gọi là vấn đề “đếm tới vô cùng” (count-to-infinity problem).

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

103

Có vài giải pháp giải quyết một phần vấn đề “đếm tới vô cùng”. Giải pháp thứ nhất là dùng một số khá nhỏ để coi như gần bằng vô cùng. Ví dụ như chúng ra có thể quyết định số lượng bước nhảy (hop) tối đa để đi qua một mạng là không quá 16, và do đó ta chọn 16 là số gần bằng vô cùng. Con số này ít ra cũng giới hạn được thời gian mà các nút có thể phải bỏ ra để đếm tới vô cùng. Tuy nhiên giải pháp này có thể gặp vấn đề nếu một số nút mạng được chia tách và mạng có thể cần nhiều hơn 16 bước nhảy để duyệt hết nó. Một kỹ thuật khác dùng để cải thiện thời gian dùng để ổn định hóa mạng được gọi là kỹ thật “chia tầm nhìn” (split horizon). Ý tưởng là: khi một nút gởi một bảng cập nhật vạch đường cho các láng giềng của nó, nó sẽ không gởi những thông tin vạch đường mà nó đã nhận từ một nút láng giềng ngược lại chính nút láng giềng đó. Ví dụ như nếu B có một đường đi (E, 2, A) trong bảng vạch đương của nó, B chắc hẳn phải biết rằng nó học con đường này từ A, vì thế mỗi khi B gởi thông tin cập nhật cho A nó sẽ không gởi con đường (E, 2) trong đó. Tuy nhiên giải pháp này chỉ tốt khi nó xoay quanh 2 nút mà thôi.

6.3.6 Giải pháp chọn đường “Trạng thái nối kết” (Link State)
Vạch đường kiểu Link-state là một ví dụ thứ hai trong họ giao thức vạch đường bên trong một miền. Giả thiết đầu tiên trong Link-state cũng khá giống trong Distance-vector: Mỗi nút được giả định có khả năng tìm ra trạng thái của đường nối nó đến các nút láng giềng và chi phí trên mỗi đường nối đó. Nhắc lại lần nữa: chúng ta muốn cung cấp cho mỗi nút đủ thông tin để cho phép nó tìm ra đường đi có chi phí thấp nhất đến bất kỳ đích nào. Ý tưởng nền tảng đằng sau các giao thức kiểu Link-state là rất đơn giản: Mọi nút đều biết đường đi đến các nút láng giềng kề bên chúng và nếu chúng ta đảm bảo rằng tổng các kiến thức này được phân phối cho mọi nút thì mỗi nút sẽ có đủ hiểu biết về mạng để dựng lên một bản đồ hoàn chỉnh của mạng. Giải thuật Link-state dựa trên hai kỹ thuật: sự phân phối một cách tin cậy thông tin về trạng thái các đường nối kết; và sự tính toán các đường đi từ kiến thức tổng hợp về trạng thái các đường nối kết.

6.3.6.1

Làm ngập một cách tin cậy (Reliable Flooding)

“Làm ngập” là quá trình thực hiện cam kết: “tất cả các nút tham gia vào giao thức vạch đường đều nhận được thông tin về trạng thái nối kết từ tất cả các nút khác”. Như khái niệm “làm ngập” ám chỉ, ý tưởng cơ sở của Link-state là cho một nút phát thông tin về trạng thái nối kết của nó với mọi nút láng giềng liền kề, đến lượt mỗi nút nhận được thông tin trên lại chuyển phát thông tin đó ra các nút láng giềng của nó. Tiến trình này cứ tiếp diễn cho đến khi thông tin đến được mọi nút trong mạng. Cụ thể hơn, mỗi nút tạo ra gói tin cập nhật, còn được gọi là gói tin trạng thái nối kết (link-state packet – LSP), chứa những thông tin sau: ID của nút đã tạo ra LSP Một danh sách các nút láng giềng có đường nối trực tiếp tới nút đó, cùng với chi phí của đường nối đến mỗi nút. Một số thứ tự Thời gian sống (time to live) của gói tin này Hai mục đầu là cần thiết cho việc tính toán chọn đường; hai mục sau cùng được sử dụng để giúp cho quá trình làm ngập thật chắc. Tính tin cậy ở đây đòi hỏi việc đảm bảo các nút trong mạng có được thông tin có phiên bản mới nhất, do có nhiều LSP trái ngược nhau từ một nút được phát lên mạng. Đảm bảo

việc làm ngập có thể tin cậy được là một việc khó (Ví dụ, một phiên bản cũ của giao thức vạch đường link-state trong ARPANET đã làm cho mạng này bị tê liệt vào năm 1981). Việc làm ngập được thực hiện như sau: Đầu tiên, việc truyền các LSP giữa các nút kề nhau được bảo đảm tính tin cậy bằng cách sử dụng cơ chế báo nhận (acknowledgement) và làm lại khi bị lỗi (retransmission) giống như ở tầng liên kết dữ liệu. Tuy nhiên, cần thực hiện thêm một số bước để đảm bảo việc phát một LSP từ một nút đến tất cả các nút khác trong mạng là đáng tin cậy. Giả sử nút X nhận được một phiên bản LSP có nguồn gốc từ nút Y nào đó. Chú ý rằng nút Y có thể là bất kỳ router nào ở trong cùng một miền với X. X kiểm tra xem nó đã có bất kỳ phiên bản LSP nào từ Y không. Nếu không, nó sẽ lưu LSP này. Nếu có, X sẽ so sánh hai số thứ tự trong hai
Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

104

LSP. Nếu LSP mới đến có số thứ tự lớn hơn số thứ tự của LSP có sẵn, X cho rằng LSP mới đến là mới hơn, và do đó X sẽ thay LSP cũ bằng phiên bản mới này. Ngược lại, với một số thứ tự nhỏ hơn (hoặc bằng), LSP mới đến sẽ bị coi là cũ hơn cái đang có sẵn (hoặc ít ra là không mới hơn), và vì thế nó sẽ bị bỏ qua, không cần phải làm gì thêm. Nếu LSP mới đến là cái mới hơn, nút X sẽ gởi một phiên bản của LSP này ra tất cả các nút láng giềng liền kề nó ngoại trừ nút láng giềng vừa gởi cho nó phiên bản LSP mới vừa đề cập. Đến phiên các nút láng giềng của X lại xoay qua phát tán LSP mới này sang các nút láng giềng khác. Việc “LSP không được gởi ngược lại nút vừa phát ra nó” sẽ giúp dẫn đến điểm dừng của quá trình phát tán LSP này. Sự phát tán dây chuyền có điểm dừng này sẽ đảm bảo cho việc đem phiên bản LSP mới nhất đến tất cả các nút trong mạng. Hình H6.15 thể hiện một LSP được dùng làm ngập một mạng nhỏ. Hình (a) thể hiện X nhận được một LSP mới; (b) X đẩy LSP mới ra A và C; (c) A và C đẩy LSP qua B; (d) B đẩy LSP qua D và quá trình làm ngập kết thúc.

(a)

(b)

(c)

(d)

H6.15 Việc làm ngập mạng với các gói tin LSP

Cũng giống như trong giải thuật Distance-Vector, sẽ có hai tình huống mà một nút quyết định gởi LSP đến các nút láng giềng: gởi một cách định kỳ hoặc gởi do bị kích hoạt. Một trong những ưu tiên hàng đầu của cơ chế làm ngập (flooding) là phải đảm bảo đem thông tin mới nhất đến mọi nút trong mạng càng nhanh càng tốt và các thông tin cũ phải được rút ra không cho lưu thông trên mạng nữa. Thêm nữa, rất là lý tưởng nếu ta có thể giảm thiểu lượng thông tin vạch đường lưu chuyển trên mạng – một kiểu phí tổn theo cách nhìn của nhiều người. Một phương pháp cần thiết để giảm thiểu phí tổn dành cho việc vạch đường là tránh gởi các LSP trừ trường hợp hết sức cần thiết. Điều này có thể thực hiện được bằng cách sử dụng các bộ định thời (timer) có giá trị rất lớn – thường là kéo dài hàng giờ - dùng để định kỳ phát các LSP. Còn để đảm bảo rằng thông tin cũ phải được thay thế bởi thông tin mới, các LSP sẽ mang số thứ tự. Mỗi khi một nút phát LSP mới, nó sẽ tăng số thứ tự lên 1. Không giống như hầu hết các giao thức khác, số thứ tự trong LSP sẽ không được đếm xoay vòng (modulo), vì thế trường chứa số này phải đủ lớn (ví dụ như 64 bit). Nếu một nút bị chết (down) và sau đó được khởi động lại, nó sẽ khởi động trường số thứ tự lại bằng 0. Nếu một nút bị chết quá lâu, tất cả các LSP của nút đó sẽ bị mãn kỳ (timed out); ngoài ra, nếu cuối cùng nút này lại nhận được LSP của chính nó với số thứ tự lớn hơn bản gốc, nút có thể lấy số lớn hơn làm số thứ tự mới. Các LSP cũng mang theo thời gian sống của nó (Time to live - TTL). Điều này dùng để đảm bảo các LSP cũ rút cuộc cũng bị xóa khỏi mạng. Một nút luôn luôn giảm trường TTL của một LSP mới đến nó đi 1 trước khi chuyển LSP này ra các nút láng giềng. Khi trường TTL còn 0, nút

phát lại LSP với TTL = 0, điều đó sẽ được thông dịch bởi tất cả các nút trong mạng như là tín hiệu cho phép xóa LSP đó.

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

105

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

6.3.6.2

Tính toán chọn đường trong Link State

Khi một nút có một phiên bản LSP từ tất cả các nút khác trong mạng, nó đã có thể tính toán ra bản đồ hoàn chỉnh cho hình thái của mạng, và từ bản đồ này nút có thể quyết định con đường tốt nhất đến tất cả các nút còn lại trong mạng. Giải pháp chọn đường chính là giải thuật tìm đường đi ngắn nhất Dijkstra.

6.3.7 Vạch đường phân cấp (Hierarchical Routing)
Khi mạng tăng kích thước, kích thước bảng vạch đường của các router tăng theo. Không chỉ bộ nhớ của router bị tiêu hao quá nhiều cho việc trữ các bảng vạch đường, mà CPU còn phải tốn nhiều thời gian để quét bộ nhớ và cũng cần nhiều băng thông hơn để truyền những thông tin chọn đường này. Rồi cũng sẽ đến lúc mạng máy tính phát triển đến mức không một router nào có đủ khả năng trữ một đầu mục thông tin về một router khác, vì thế việc vạch đường phải phát triển theo đường hướng khác: vạch đường phân cấp. Khi việc vạch đường phân cấp được áp dụng, các router được chia thành những vùng (domain). Trong mỗi vùng, mỗi router biết cách vạch đường cho các gói tin đi đến được mọi đích trong nội vùng của nó, nhưng không biết gì về cấu trúc bên trong của các vùng khác. Khi nhiều vùng được nối kết với nhau, đương nhiên mỗi vùng được công nhận tính độc lập để giải phóng các router trong các vùng đó khỏi việc phải tìm hiểu hình trạng của các vùng khác. Với những mạng thật lớn, kiến trúc phân cấp hai mức có thể sẽ không đủ; có thể cần phải nhóm các vùng lại thành liên vùng, nhóm các liên vùng thành khu vực... Hình H6.16 thể hiện một mạng được vạch đường phân cấp gồm hai mức có năm vùng. Bảng vạch đường đầy đủ của router A gồm có 17 mục từ như trong hình H6.16(b). Khi vạch đường được thực hiện theo kiểu phân cấp, bảng vạch đường của A giống như bảng H6.16(c), có mọi mục từ chỉ đến các router cục bộ giống như trước, tuy nhiên các mục từ chỉ đến các vùng khác lại được cô đặc lại thành một router. Do tỉ lệ các router trong các vùng tăng, vì thế cách làm này giúp rút ngắn bảng vạch đường.

H6.16 Vạch đường phân cấp

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

106

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

6.3.8 Vạch đường trong mạng di động

Ngày nay, hàng triệu người đang sở hữu máy tính xách tay, và thông thường họ muốn đọc email cũng như truy xuất các hệ thống tập tin cho dù họ đang ở bất kỳ nơi nào trên thế giới. Việc sử dụng các host di động này dẫn đến một vấn đề phức tạp mới: để vạch đường cho gói tin đến host di động, trước tiên phải tìm ra nó đã. Chủ đề về tích hợp các host di động lại thành một mạng là tương đối mới, tuy vậy trong phần này chúng ta sẽ phác thảo ra một số vấn đề phát sinh và chỉ ra các giải pháp khả thi.

H6.17 Mô hình mạng có hệ thống không dây

Mô hình mạng mà các nhà thiết kế thường sử dụng được chỉ ra trong hình H6.17. Ở đây chúng ta có một mạng WAN bao gồm vài router và host. Mạng WAN được dùng để nối kết các mạng LAN, MAN, các tế bào mạng không dây (Wireless cell). Các host không bao giờ di chuyển được gọi là cố định, chúng được nối vào mạng bởi các đường cáp đồng hoặc quang. Ngược lại, chúng ta sẽ phân biệt hai loại host khác: loại di cư (migratory host) và loại lang thang (roaming host). Loại host di cư về bản chất là host cố định, nhưng chúng thỉnh thoảng lại chuyển từ địa bàn (site) này đến địa bàn mạng kia, và chúng chỉ có thể sử dụng mạng mới khi được nối kết vật lý vào đấy. Loại host lang thang thực chất vừa chạy vừa tính toán, nó muốn duy trì các nối kết mạng ngay cả khi đang di chuyển. Chúng ta sẽ sử dụng thuật ngữ “host di động” để ám chỉ hai loại di động vừa nói đến, tức là chúng đã đi khỏi nhưng lại muốn duy trì liên lạc về nhà. Tất cả các host được giả sử đều có vị trí mạng nhà (home location) và vị trí này không bao giờ thay đổi. Các host cũng có địa chỉ lâu dài tại nhà (home address) và địa chỉ này có thể được dùng để xác định vị trí mạng nhà của nó, cũng giống như số điện thoại 84-071-831301 chỉ ra số đó ở Việt Nam (mã 084), thành phố Cần Thơ (mã 071). Mục tiêu của việc vạch đường trong hệ thống có các host di động là phải đảm bảo có thể gởi được gói tin đến host di động sử dụng địa chỉ tại nhà của nó và làm cho các gói tin đến được host di động một cách hiệu quả cho dù host này có ở đâu đi nữa. Trong mô hình ở hình H6.17, WAN được chia thành các đơn vị nhỏ, ở đây chúng ta gọi là khu vực (area), thường là LAN hoặc tế bào mạng không dây. Mỗi khu vực có một hoặc nhiều trợ lý đối ngoại (foreign agent - FA) – đó là những tiến trình làm nhiệm vụ theo dõi các host khách đang viếng thăm khu vực của mình. Thêm vào đó, mỗi khu vực còn có một trợ lý đối nội (home agent HA), làm nhiệm vụ theo dõi những host có nhà nằm trong khu vực nhưng hiện đang viếng thăm khu vực khác. Khi một host đi vào một khu vực mới (có thể là host này muốn thường trú trong mạng LAN mới hoặc chỉ đi ngang cell này thôi), nó phải đăng ký với trợ lý đối ngoại ở đó. Thủ tục đăng ký diễn ra như sau:

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

1. Theo chu kỳ, mỗi trợ lý đối ngoại sẽ phát ra những thông điệp thông báo sự hiện diện của nó cùng với địa chỉ. Một host mới tới sẽ chờ lắng nghe thông báo này. Nếu host cảm thấy nó đã chờ lâu nhưng không nhận được thông báo, host có thể tự phát câu hỏi: Có bất kỳ trợ lý đối ngoại nào ở đây không? 2. Host di động đăng ký với trợ lý đối ngoại, cung cấp thông tin về địa chỉ ở nhà, địa chỉ MAC và một số thông tin về an ninh khác. 3. Trợ lý đối ngoại liên hệ với trợ lý đối nội ở nhà của host đó và nói: Một host của ông đang ở đây. Thông điệp mà trợ lý đối ngoại gởi cho trợ lý đối nội bên kia chứa địa chỉ mạng của trợ lý đối ngoại đó. Thông điệp này còn chứa thông tin an ninh dùng để thuyết phục trợ lý đối nội bên kia rằng host di động của nó thực sự đang ở đó. 4. Trợ lý đối nội bên kia kiểm tra thông tin an ninh, trong đó có một tem thời gian, để chứng tỏ được rằng tem này vừa được tạo ra trong vòng vài giây. Và nếu kết quả kiểm tra là tốt đẹp, nó sẽ bảo trợ lý đối ngoại bên kia tiến hành làm việc. 5. Khi trợ lý đối ngoại nhận được sự chấp thuận của trợ lý đối nội bên kia, nó tạo ra một đầu mục trong các bảng quản lý và thông báo cho host di động rằng: Bạn đã đăng ký thành công. Lý tưởng nhất là khi một host di động rời khỏi một cell, nó phải thông báo với trợ lý đối ngoại ở đó để xóa đăng ký. Nhưng đa phần người sử dụng thường tắt máy ngay khi sử dụng xong. Khi một gói tin được gởi đến một host di động, đầu tiên gói tin đó được gởi đến mạng LAN nhà của host đó (bước 1 trong hình H6.18.

H6.18 Vạch đường trong mạng di động

Bên gởi, ví dụ đang ở Tiền Giang, gởi gói tin đến mạng nhà của host di động ở Cần Thơ. Giả sử host di động đang ở Đồng Tháp. Trợ lý đối nội ở Cần Thơ tìm ra được địa chỉ tạm thời của host di động, đóng gói gói tin đó và chuyển cho trợ lý đối ngoại của mạng ở Đồng Tháp (bước 2). Đến phiên trợ lý đối ngoại ở Đồng Tháp mở gói gói tin đó và phát cho host di động thông tin dưới dạng khung thông tin ở mức liên kết dữ liệu. Sau đó trợ lý đối ngoại ở Đồng Tháp sẽ bảo bên gởi ở Tiền Giang hãy đóng gói và gởi gói tin trực tiếp đến Đồng Tháp (bước 3). Từ đó trở về sau, nhưng gói tin mà bên gởi muốn gởi cho host di động được gởi trực tiếp đến trợ lý đối ngoại tại Đồng Tháp, rồi được trợ lý đối ngoại phát trực tiếp đến host (bước 4).

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

108

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

6.4 Các giải thuật chống tắc nghẽn
Khi có quá nhiều gói tin hiện diện trong một mạng con (hoặc một phần của nó), hiệu năng hoạt động của hệ thống bị giảm. Tình trạng này được gọi là “tắc nghẽn”.

H6.19 Mô tả tắc nghẽn

Hình H6.19 mô tả lại hiện tượng tắc nghẽn. Khi số lượng gói tin chạy trong mạng con nằm dưới ngưỡng cho phép, chúng đều được phân phối đến đích (ngoại trừ những gói tin bị lỗi), và số lượng gói tin được phân phối tỉ lệ thuận với số lượng gói tin được phát ra lúc đầu. Tuy nhiên, khi mật độ giao thông tăng quá cao, các router không còn đáp ứng kịp nữa và chúng dần dần đánh mất một số gói tin. Điều này có xu hướng làm cho vấn đề tắc nghẽn nghiêm trọng thêm. Khi mà giao thông cực cao, hiệu năng hệ thống sụp đổ hoàn toàn và hầu như không gói tin nào được phân phát đến đích. Có vài yếu tố góp phần gây ra tắc nghẽn. Nếu đột nhiên nhiều luồng mang các gói tin đến một nút tại nhiều ngõ vào, và tất cả các gói tin này đều cần một ngõ ra, thì một hàng đợi sẽ xuất hiện. Nếu không đủ bộ nhớ để lưu các gói tin trên hàng đợi này, một số gói tin sẽ bị mất. Tăng thêm bộ nhớ chỉ giúp không mất gói tin trong hàng đợi, nhưng Nagle (1987) đã chỉ ra rằng: nếu một router có bộ nhớ vô hạn, sự tắc nghẽn lại càng tồi tệ hơn! Lý do là khi mà gói tin đến được đầu của hàng đợi thì nó đã bị mãn kỳ (timed out), và do đó sẽ có nhiều phiên bản trùng với gói tin đó được bên gởi gởi đến router, làm tăng thêm tải của mọi hướng đi đến đích của gói tin. Các bộ xử lý chậm cũng có thể gây ra tắc nghẽn. Nếu CPU của router xử lý các gói tin trung chuyển qua nó chậm, hàng đợi cũng sẽ phát sinh, cho dù dung lượng các đường nối vào và ra đều vượt yêu cầu. Tóm lại, đường truyền băng thông thấp có thể gây ra tắc nghẽn. Nâng cấp đường truyền nhưng năng lực xử lý của bộ xử lý tại router yếu cũng gây ra tắc nghẽn. Thành thử, nâng cấp một phần mà không phải là toàn bộ hệ thống chỉ đẩy sự tắc nghẽn từ nơi này đến nơi khác mà thôi. Vấn đề phát sinh từ sự bất cân đối giữa các bộ phận của hệ thống, và nó chỉ qua đi khi mà các bộ phận này được giữ cân bằng với nhau.

6.4.1 Các nguyên tắc chung để điều khiển tắc nghẽn
Nhiều bài toán trong các hệ thống phức tạp, ví dụ như trong mạng máy tính, có thể được xem xét theo quan điểm của lý thuyết điều khiển (control theory). Cách tiếp cận này dẫn đến việc chia các giải pháp thành hai loại: vòng đóng và vòng mở (closed loop and open loop). Các giải pháp dạng vòng đóng cố gắng giải quyết vấn đề tắc nghẽn bằng cách đưa ra thiết kế tốt cho mạng, thực chất là để đảm bảo tắt nghẽn sẽ không xảy ra. Một khi mạng được khởi động và chạy, sẽ không có việc sửa chữa giữa kỳ.
Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

109

Các công cụ thực hiện việc điều khiển kiểu vòng mở bao gồm việc quyết định khi nào nên chấp nhận luồng giao thông mới, quyết định khi nào thì bỏ qua các gói tin và bỏ qua gói nào. Tất cả các công cụ trên đều có đặc điểm chung là chúng đưa ra các quyết định mà không quan tâm đến trạng thái hiện hành của mạng. Ngược lại, các giải pháp kiểu vòng đóng dựa trên quan niệm về chu trình phản hồi thông tin. Cách tiếp cận này bao gồm 3 phần: 1. Giám sát hệ thống để phát hiện nơi nào và khi nào xảy ra tắc nghẽn. 2. Chuyển thông tin đến những nơi cần có những hành động ứng phó. 3. Điều chỉnh lại hoạt động của hệ thống để khắc phục sự cố. Nhiều kiểu đo lường có thể được sử dụng để giám sát một mạng con để phát hiện ra tắc nghẽn ở đó. Các kiểu đo lường thường dùng nhất là tỉ lệ các gói tin bị bỏ qua do thiếu không gian trữ đệm, chiều dài trung bình của các hàng đợi, số lượng các gói tin bị mãn kỳ và được tái truyền, thời gian trì hoãn gói tin trung bình. Trong mọi tình huống, các số đo tăng đồng nghĩa với việc tăng tắc nghẽn. Bước thứ hai trong chu trình phản hồi là chuyển thông tin về tắc nghẽn từ điểm được phát hiện bị tắc nghẽn đến điểm có trách nhiệm xử lý tình huống đó. Cách dễ nhất là để cho router phát hiện ra tắc nghẽn phát thông báo đến nút nguồn vừa gởi thông tin đến làm tắc hệ thống. Dĩ nhiên, thông báo này làm cho tắc nghẽn tăng thêm tạm thời. Một cách thông báo tắc nghẽn khác là: Người ta dành riêng một bit hoặc một trường trong gói tin để trong trường hợp có tắc nghẽn, router có thể bật bit hoặc trường này lên và gởi nó đến mọi ngõ ra nhằm thông báo cho các láng giềng của nó biết. Hoặc cũng có thể dùng cách phản hồi sau: Cho các host hoặc router thường xuyên gởi các gói tin thăm dò ra ngoài để hỏi thẳng về tình hình tắc nghẽn. Thông tin này có thể được sử dụng để chuyển hướng vạch đường vòng qua khu vực bị tắc nghẽn. Ví dụ thực tế: Một số đài phát thanh thường phái một số máy bay trực thăng bay vòng quanh thành phố để báo cáo lại những trục đường bị tắc, từ đó thông báo đến thính giả giúp họ chuyển hướng lái xe tránh những điểm nóng. Sự hiện diện của tắc nghẽn đồng nghĩa với việc: tài nguyên của hệ thống không đủ để tải gánh nặng thông tin truyền qua. Vì thế ta nghĩ ra hai giải pháp: tăng tài nguyên hoặc giảm tải. Ví dụ, một mạng con có thể bắt đầu sử dụng các đường điện thoại quay số để tạm thời tăng băng thông giữa một số điểm nào đó. Trong các hệ thống vệ tinh, việc tăng công suất truyền đồng nghĩa với việc cung cấp băng thông lớn hơn. Chia tách lưu lượng thông tin cho chúng chạy trên nhiều đường đi khác nhau cũng có thể giúp tăng băng thông. Cuối cùng, các router dự phòng (thường để dự phòng tình huống các router chính bị sự cố) có thể được mang ra chạy trực tuyến để tăng dung lượng truyền tải của hệ thống khi tắc nghẽn nghiêm trọng xảy ra. Tuy nhiên, đôi khi ta không thể tăng tài nguyên của hệ thống lên nữa, hoặc tài nguyên đã tăng tối đa. Cách thức duy nhất để chống lại tắc nghẽn là giảm tải. Có nhiều cách giảm tải, ví dụ: từ chối phục vụ một số người dùng, giảm cấp dịch vụ đối với vài hoặc tất cả người dùng, và buộc người dùng cung cấp lịch trình phát ra yêu cầu của họ.

### 6.4.2 Các biện pháp phòng ngừa tắc nghẽn

Tại tầng mạng, việc chọn sử dụng mạch ảo hay datagram sẽ tác động đến tắc nghẽn do nhiều giải thuật điều khiển tắc nghẽn chỉ chạy trên mạch ảo. Giải pháp “lập hàng đợi cho các gói tin và phục vụ chúng” liên quan đến việc một router có một hàng đợi cho mỗi ngõ vào, một hàng đợi cho mỗi ngõ ra hay cả hai. Nó cũng liên quan đến trình tự xử lý các gói tin trong hàng đợi ( round-robin hay dựa trên sự ưu tiên). Chính sách hủy bỏ gói tin sẽ chỉ

ra gói tin nào cần bị hủy bỏ khi không còn không gian chứa. Một chính sách tốt có thể giúp làm giảm tắc nghẽn, ngược lại có thể làm tắc nghẽn trầm trọng thêm. Một giải thuật vạch đường tốt có thể giúp tránh được tắc nghẽn bằng cách trải đều giao thông trên tất cả đường nối, trong khi một giải thuật tồi chỉ đơn giản gởi quá nhiều thông tin lên một đường tải đã quá tải rồi. Cuối cùng, việc quản lý thời gian sống của gói tin sẽ phải đưa ra quyết định là một gói tin có thể sống bao lâu trong hàng đợi trước khi bị hủy bỏ. Thời gian sống quá dài sẽ làm

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

110

trì trệ công việc rất lâu. Nhưng nếu thời gian sống quá ngắn, các gói tin thỉnh thoảng sẽ bị mãn kỳ (timed-out) trước khi chúng đến được đích, vì thế dẫn đến việc tái truyền.

6.4.3 Điều khiển tắc nghẽn trong các mạng con dạng mạch ảo
Một giải pháp đơn giản là điều khiển cấp phép (admission control). Ý tưởng như sau: một khi có cảnh báo về tắc nghẽn, hệ thống sẽ không thiết lập thêm mạch ảo nào nữa đến khi sự cố qua đi. Vì thế, trong lúc tắc nghẽn xảy ra, những cố gắng thiết lập mạch ảo đều thất bại. Lý do: cho phép nhiều người vào đấy sẽ làm cho vấn đề trở nên trầm trọng hơn. Cách tiếp cận khác là cho phép tạo ra các mạch ảo mới nhưng cẩn trọng vạch đường cho các mạch ảo mới này đi vòng qua khu vực bị vấn đề tắc nghẽn. Ví dụ, xem xét mạng con như trong hình H6.20, trong đó hai router bị tắc nghẽn.

H6.20 (a) Một mạng con bị tắc nghẽn. (b) Mạng con được vẽ lại sau khi loại trừ các điểm gây tắc nghẽn.

Giả sử một host được nối với router A muốn thiết lập nối kết tới một host của router B. Thường thì nối kết này sẽ chạy qua một trong hai nút bị tắc nghẽn. Để tránh chuyện này, chúng ta vẽ lại mạng con như trong hình (b), bỏ qua các router bị tắc nghẽn cùng với các đường nối của chúng. Đường chấm chỉ ra một đường đi có thể tránh được tắc nghẽn. Một chiến lược khác liên quan đến mạch ảo là: host và mạng con thỏa thuận với nhau về việc thiết lập mạch ảo. Thỏa thuận này thường bao gồm dung lượng và đường đi của thông tin, chất lượng dịch vụ được yêu cầu và các thông số khác. Để đảm bảo thực hiện được thỏa thuận, mạng con sẽ dành riêng tài nguyên trên suốt con đường mạch ảo đi qua. Các tài nguyên này bao gồm không gian bảng vạch đường và buffer trên các router, cùng với băng thông trên các đường nối. Trong tình huống này, tắc nghẽn hầu như không xảy ra trên một mạch ảo mới bởi vì tất cả tài nguyên cần thiết đã được đảm bảo sẵn dùng. Kiểu dành riêng tài nguyên này có thể được thực hiện toàn thời gian như là một phương thức hoạt động chuẩn, hoặc chỉ được thực hiện khi tắc nghẽn xảy ra. Nếu được thực hiện toàn thời gian sẽ có hạn chế là lãng phí tài nguyên. Nếu đường truyền 6 Mbps được tận hiến cho 6 mạch ảo, mỗi mạch ảo tiêu tốn 1 Mbps, thì đường truyền này luôn được đánh dấu là đầy, cho dù hiếm có khi nào 6 mạch ảo con của nó truyền hết công suất tại cùng thời điểm.

6.4.4 Điều khiển tắc nghẽn trong mạng con dạng Datagram
Trong mạng dạng Datagram, mỗi router có thể dễ dàng kiểm soát hiệu năng của các đường ra và các tài nguyên khác. Ví dụ, nó có thể gán cho mỗi đường nối một biến thực u, với giá trị từ 0.0 đến 1.0, dùng phản ánh hiệu năng gần đây của đường nối đó. Để duy trì độ chính xác tốt cho u, một mẫu hiệu năng tức thời f của đường nối sẽ được lấy thường xuyên, và u sẽ được cập nhật như sau trong đó hằng số a quyết định router quên đi lịch sử gần đây nhanh như thế nào.

umới = a ncũ + (1 - a) f

111

Khi u vượt qua ngưỡng, đường ra rơi vào trạng thái “cảnh báo”. Mỗi gói tin mới tới sẽ được giữ lại và chờ kiểm tra xem đường ra có ở trạng thái cảnh báo không. Nếu có, một số hành động sẽ được thực hiện, và chúng ta sẽ thảo luận ngay sau đây.

6.4.4.1

Các gói tin chặn (Choke Packets)

Khi một gói tin đến router và ngõ ra của nó đang ở trong trạng thái báo động, router sẽ gởi một gói tin chặn ngược về nút nguồn đã gởi gói tin đó. Gói tin gặp tắc nghẽn như đã nói sẽ được đánh dấu để nó không làm phát sinh các gói tin chặn khác nữa. Khi gói tin chặn đến được nút nguồn, nút nguồn sẽ giảm lưu lượng thông tin đến điểm bị nghẽn đi X phần trăm. Do có thể còn vài gói tin đang trên đường đi đến đích bị nghẽn, sau này nút nguồn nên bỏ qua các gói tin chặn phát ra tiếp từ đích đó. Sau giai đoạn trên, nút nguồn bỏ thêm một khoảng thời gian để lắng nghe thêm các gói tin chặn khác. Nếu chúng còn tới, đường nối vẫn bị nghẽn, nút nguồn tiếp tục giảm dung lượng truyền. Nếu không còn gói tin chặn nào chạy ngược về nút nguồn trong thời gian lắng nghe, nó có thể từng bước tăng lưu lượng truyền lên.

6.4.4.2

Gởi các gói chặn từng bước một ( Hop-by-Hop Choke Packets)

Ở tốc độ cao hoặc qua khoảng cách xa, việc gởi gói tin chặn ngược về nút nguồn là không hiệu quả, bởi vì phản ứng của nút nguồn sẽ chậm. Một cách tiếp cận khác là làm cho gói tin chặn có tác dụng tại mọi nút trung gian mà nó đi qua. Hãy xem hình ví dụ 5.18(b).

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

Lưu lượng vẫn tối đa

Lưu lượng đã giảm

(a)
H6.21 (a) Một gói tin chặn chỉ tác động lên nút nguồn. (b) Một gói tin chặn tác động lên mọi nút mà nó đi qua

(b)

Ở trong hình 5.18(b), ngay khi gói tin chặn vừa đến F, F liền giảm lưu lượng truyền đến D. Tương tự, khi gói tin chặn đến E, E sẽ giảm lưu lượng truyền đến F. Cuối cùng gói tin chặn đến A và lưu lượng được giảm suốt tuyến đường từ A đến D. Hiệu quả của sơ đồ chặn từng bước một là có thể giải phóng điểm bị nghẽn nhanh chóng. Tuy nhiên cái giá phải trả là nó tiêu tốn băng thông hướng lên cho gói tin chặn. Nhưng cái lợi cuối cùng là ở chỗ, giải pháp này bóp chết tắc nghẽn ngay trong trứng nước.

6.5 Liên mạng
Đến thời điểm này, chúng ta đều ngầm định rằng chúng ta đang làm việc trên một mạng đơn đồng nhất với mọi máy tính chạy cùng một giao thức trong cùng một tầng. Không may là sự ngầm hiểu này hơi quá lạc quan. Đã và đang tồn tại nhiều loại mạng khác nhau bao gồm LAN, WAN, MAN. Nhiều giao thức khác nhau đang được sử dụng rộng rãi trên nhiều tầng mạng khác nhau. Trong phần này, chúng ta sẽ có cái nhìn cẩn trọng hơn về các vấn đề phát sinh khi hai hoặc nhiều mạng được nối kết với nhau thành một liên mạng (internet). Các mạng máy tính đã đa dạng và sẽ vẫn đa dạng, và có nhiều lý do lý giải cho nhận định này. Trước tiên, cơ sở để cài đặt các mạng là khác nhau. Gần như tất cả các máy PC đều cài đặt TCP/IP. Nhiều công ty lớn sử dụng máy mainframe của IBM sử dụng mạng SNA. Một số lượng lớn các công ty điện thoại đang điều hành các mạng ATM. Một số mạng LAN dùng cho các máy tính PC vẫn còn sử dụng Novell IPX hoặc AppleTalk. Cuối cùng, mạng không dây là một lĩnh vực đang phát triển rộng với nhiều giao thức hoạt động trong đó. Chiều hướng sử dụng mạng phức tạp này sẽ còn tiếp diễn nhiều năm nữa với nhiều lý do về tính kế thừa, kỹ thuật mới, và thực tế là không phải nhà sản xuất nào cũng thích thú với việc giúp cho khách hàng của họ dễ dàng chuyển đổi sang hệ thống của nhà sản xuất khác. Thứ hai, do máy tính và thiết bị mạng ngày càng rẻ, cho nên cấp có thẩm quyền quyết định mua sắm mạng máy tính ngày càng xuống thấp trong cơ cấu các công ty, tổ chức. Nhiều công ty đưa ra chính sách: dự trù mua sắm trên 1 triệu USD do cấp quản lý cao nhất quyết định, mua sắm trên 100.000 USD do cấp trung quyết định, dưới 100.000 USD thì cấp trưởng bộ phận có toàn quyền quyết định. Vì thế, ví dụ, bộ phận kỹ thuật thì có thể cài đặt các máy trạm Unix chạy TCP/IP, còn bộ phận tiếp thị có quyền cài các máy Mac với giao thức AppleTalk. Thứ ba, các mạng khác khau sử dụng các công nghệ hoàn toàn khác nhau. Vì thế sẽ không mấy ngạc nhiên nếu thấy một sản phẩm phần cứng mới thì cũng xuất hiện phần mềm mới đi kèm. Ví
Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

113

dụ, một gia đình trung bình hiện nay trang bị mạng giống như một văn phòng trung bình ngày xưa: đầy các máy tính không thể nói chuyện với nhau. Nhưng ở tương lai không xa, đấy sẽ là nơi có đầy đủ điện thoại, TV, máy tính và các dụng cụ khác, tất cả được nối kết với nhau và có thể được điều khiển từ xa. Kỹ thuật mới này chắc chắn sẽ sinh ra một kiểu mạng mới với các giao thức mới.

H6.22 Một liên mạng

Để lấy ví dụ về cách thức các mạng khác nhau được nối kết với nhau như thế nào, hãy xem xét hình H6.22. Ở đây, ta có một mạng tổ hợp với nhiều địa bàn khác nhau, được kết dính với nhau bởi một mạng WAN/ATM. Tại một địa bàn, một back-bone FDDI được dùng để nối kết một mạng Ethernet, một mạng không dây 802.11 và một trung tâm dữ liệu dùng mạng SNA. Mục tiêu của nối kết liên mạng là cho phép người dùng trên một mạng con có thể liên lạc được với người dùng trên các mạng con khác. Để làm được việc này, ta phải đảm bảo gởi cho được gói tin từ mạng con này đến bất kỳ mạng con khác. Do các mạng con khác nhau về nhiều lĩnh vực, cho nên không dễ để truyền một gói tin từ nơi này đến nơi kia.

6.5.1 Các mạng con được nối kết với nhau ra sao?
Các mạng có thể được nối liên thông bằng nhiều kiểu thiết bị khác nhau: Ở tầng vật lý: Các mạng có thể được nối kết bằng các repeater hoặc hub, những thiết bị chỉ đơn thuần làm nhiệm vụ di chuyển các bit từ mạng này sang mạng kia. Ở tầng LKDL: Người ta dùng các cầu nối (bridges) hoặc switches. Chúng có thể nhận các khung, phân tích địa chỉ MAC và cuối cùng chuyển khung sang mạng khác trong khi song song đó, chúng vừa làm nhiệm vụ giám sát quá trình chuyển đổi giao thức, ví dụ như từ Ethernet sang FDDI hoặc 802.11. Ở tầng mạng: Người ta dùng các router để nối kết các mạng với nhau. Nếu hai mạng có tầng mạng khác nhau, router có thể chuyển đổi khuôn dạng gói tin, quản lý nhiều giao thức khác nhau trên các mạng khác nhau. Ở tầng vận chuyển: Người ta dùng các gateway vận chuyển, thiết bị có thể làm giao diện giữa hai đầu nối kết mức vận chuyển. Ví dụ gateway có thể làm giao diện trao đổi giữa hai nối kết TCP và NSA. Ở tầng ứng dụng: Các gateway ứng dụng sẽ làm nhiệm vụ chuyển đổi ngữ cảnh của các thông điệp. Ví dụ như gateway giữa hệ thống email Internet và X.400 sẽ làm nhiệm vụ chuyển đổi nhiều trường trong header của email. Trong chương này, chúng ta chỉ quan tâm đến việc nối kết liên mạng ở tầng mạng dùng các router. Phương thức hoạt động của router được chỉ ra trong hình H5.23.

H6.23. Hai mạng Ethernet được nối kết bằng các routers

Ở đây, hai router được nối với nhau bằng đường nối điểm-điểm, có thể là đường leased-line dài hàng trăm km. Máy S muốn gởi cho máy D một gói tin, do đó nó đóng gói gói tin này thành một khung và gởi lên đường truyền. Khung đến được router của LAN1, router này liền bóc vỏ khung, lấy gói tin ra. Gói tin này sẽ được phân tích để tìm ra địa chỉ mạng (IP) của máy đích, địa chỉ này sẽ được tham khảo trong bảng vạch đường của router LAN1. Dựa trên địa chỉ này, router LAN1 quyết định chuyển gói sang router LAN2 bằng cách đóng thành khung gởi cho router LAN2.

6.5.2 Nối kết các mạng con dạng mạch ảo
Có hai kiểu liên mạng: dạng mạch ảo và datagram. Trong quá khứ, hầu hết các mạng công cộng là hướng nối kết (các mạng Frame Relay, SNA, ATM cũng vậy). Rồi với sự chấp nhận rộng rãi của công chúng đối với mạng Internet, mạng dạng datagram lên ngôi. Tuy nhiên sẽ là không chính xác khi nói mạng datagram là mãi mãi. Với sự phát triển quan trọng của các mạng đa phương tiện, có vẻ như liên lạc hướng nối kết đang trở lại ở dạng này hay dạng khác, do dễ đảm bảo chất lượng dịch vụ hơn. Vì thế cũng nên dành một chút thời gian để nói về mạng dạng mạch ảo. Trong liên mạng dạng mạch ảo như trong hình H6.24, một nối kết tới một host ở mạng xa được thực hiện giống như truyền thống. Mạng con thấy rằng đích đến ở xa và nó sẽ phác thảo một mạch ảo đến router gần mạng đích nhất. Rồi nó tạo một mạch ảo từ router đấy đến một gateway của nó (thực chất là router đa giao thức). Gateway này ghi lại thông tin về mạch ảo này trong bảng vạch đường và tiếp tục xây dựng một mạch ảo khác từ nó đến mạng con kế tiếp. Quá trình này cứ tiếp diễn cho đến khi mạch ảo đến được host đích.

H6.24 Liên mạng dạng mạch ảo

Mỗi khi có một gói tin trung chuyển qua, một gateway lưu gói tin này lại, chuyển đổi khuôn dạng gói tin này và số hiệu mạch ảo khi cần thiết, rồi chuyển nó qua gateway tiếp theo trên con đường mà mạch ảo chỉ ra. Đặc điểm quan trọng của cách làm này là: một dãy các mạch ảo được thiết lập từ host nguồn, qua một hoặc nhiều gateway rồi mới đến đích. Mỗi gateway duy trì các bảng lưu lại những mạch ảo nào đi qua nó, chúng sẽ được vạch đường ra đâu và số mạch ảo mới là gì.

6.5.3 Nối kết các mạng con dạng datagram
Mô hình liên mạng dạng datagram được chỉ ra trong hình H6.25.

Hình 6.25 Liên mạng dạng datagram

Trong mô hình này, dịch vụ duy nhất mà tầng mạng cung cấp cho tầng vận chuyển là khả năng đẩy gói tin vào mạng con và hy vọng nó đến đích. Mô hình này không đòi hỏi mọi gói tin phải đi đến đích trên cùng một con đường. Trong hình trên, các gói tin đi từ host 1 đến host 2 theo nhiều đường khác nhau. Quyết định vạch đường được đưa ra riêng lẻ cho từng gói tin, tùy thuộc vào lưu lượng thông tin tại thời điểm gói tin được gởi. Chiến lược này cho phép lựa chọn nhiều đường đi cho các gói tin và như vậy sẽ giúp đạt được nhiều băng thông hơn dạng mạch ảo. Mặt trái của nó là: không có sự đảm bảo gói tin có thể đến đích được. Mô hình như trong hình H6.25 thật ra không đơn giản như ta thấy. Thứ nhất, nếu mỗi mạng con có một tầng mạng riêng thì một gói tin từ một mạng không thể trung chuyển qua mạng khác được. Người ta có thể nghĩ là sẽ có các router đa giao thức làm nhiệm vụ chuyển đổi khuôn dạng gói tin từ dạng này sang dạng kia. Nhưng trừ khi dạng thức của hai gói tin có mối liên hệ gần với nhau và có cùng trường thông tin, không thì việc chuyển đổi khuôn dạng thường kết thúc thất bại. Với lý do này, giải pháp chuyển đổi khuôn dạng thường ít khi được chọn. Thứ hai, nghiêm trọng hơn, là vấn đề về cơ chế định địa chỉ. Thử tưởng tượng một trường hợp đơn giản: một host trên Internet đang cố gởi một gói tin IP đến một host trong một mạng SNA láng giềng. Địa chỉ IP và SNA là khác nhau. Người ta sẽ cần một cơ chế ánh xạ địa chỉ giữa IP và SNA theo hai chiều. Thêm nữa, quan niệm như thế nào là địa chỉ trong hai mạng trên là hoàn toàn khác nhau. Trong IP, một host (thực ra là một card mạng) có một địa chỉ. Trong SNA, các thực thể khác host (ví dụ thiết bị phần cứng) cũng có thể có địa chỉ. Trong trường hợp tốt nhất, người ta có thể duy trì một cơ sở dữ liệu để ánh xạ mọi thứ này sang mọi thứ kia và ngược lại, và cơ sở dữ liệu này có thể mở rộng được, nhưng nó lại thường là ngọn nguồn của lắm rắc rối. Một giải pháp khác là xây dựng gói tin internet có hiệu lực toàn cầu, và tất cả các router đều có thể hiểu được nó. Gói tin IP chính là sản phẩm của ý tưởng này. Tuy rằng việc kêu gọi mọi người chấp nhận một khuôn dạng duy nhất là khó do nhiều công ty có tham vọng xây dựng khuôn dạng độc quyền của mình, gói tin IP tự nó vẫn phát triển rộng rãi và được coi là chuẩn toàn cầu.

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

116

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

6.5.4 Vạch đường trong liên mạng
Vạch đường trong liên mạng cũng tương tự như trong mạng con đơn, nhưng thêm vào một chút phức tạp. Xét một liên mạng được cho trong hình 5.23

H6.26. (a) Một liên mạng. (b) Đồ thị biểu diễn liên mạng

Có sáu mạng con được nối kết với nhau bởi sáu router. Tạo ra mô hình đồ thị trong tình huống này là phức tạp do mỗi router đều có thể truy cập trực tiếp (gởi gói tin) đến router khác. Ví dụ, B trong hình 6.2H6(a) có thể nối kết trực tiếp tới A qua mạng 2, C qua mạng 2, và D qua mạng 3. Điều đó dẫn đến đồ thị như trong hình H6.26(b). Một khi đồ thị đã được dựng lên, các giải thuật vạch đường đã biết, như Distance-Vector hoặc Link-State, có thể được áp dụng bởi các router đa giao thức. Như vậy sẽ dẫn đến giải thuật vạch đường hai mức: trong nội bộ một mạng con – vạch đường nội hạt (interior gateway protocol) và giữa các mạng con với nhau – vạch đường liên mạng (exterior gateway protocol). Thực tế, do các mạng con là độc lập với nhau, chúng có thể sử dụng các giải thuật khác nhau. Mỗi mạng con được gọi là một hệ thống tự trị (Autonomous System – AS). Một gói tin liên mạng khởi đầu bằng địa chỉ LAN cục bộ của nó, được phát tới router đa giao thức nội bộ, tại đó, mã lệnh ở lớp mạng sẽ quyết định chuyển gói tin đó qua router nào kế tiếp. Nếu router đó có thể đối thoại được bằng giao thức của mạng nội bộ, thì gói tin sẽ được chuyển trực tiếp. Ngược lại, gói tin sẽ được đóng khung bằng giao thức của router đó trước khi chuyển tiếp. Tiến trình này cứ tiếp diễn cho đến khi gói tin đến được đích. Một trong những điểm khác nhau giữa vạch đường liên mạng và vạch đường nội hạt là vạch đường liên mạng đòi hỏi việc đi qua nhiều lãnh địa quốc tế. Nhiều luật khác nhau được đặt ra. Chẳng hạn luật của Canada nói rằng: dữ liệu từ Canada gởi đến một nơi của Canada thì không được quá cảnh ra bên ngoài. Nghĩa là lưu thông từ Windsor, Ontario đến Vancouver không được quá cảnh sang Detroit của Mỹ, trong khi con đường ngang qua Detroit là con đường ngắn nhất và rẻ nhất. Điểm khác nhau nữa giữa vạch đường nội hạt và liên mạng là chi phí. Trong cùng một mạng, một giải thuật tính cước phí duy nhất được áp dụng. Tuy nhiên, nhiều mạng khác nhau sẽ có cơ chế quản lý cước phí khác nhau.

6.5.5 Phân mảnh và tái hợp
Mỗi mạng sẽ qui định kích cỡ tối đa của các datagram chạy trong nó. Sự giới hạn này xuất phát từ nhiều lý do: Phần cứng: ví dụ như kích cỡ giới hạn của khung Ethernet. Hệ điều hành: ví dụ như tất cả các buffer đều có kích thước 512 bytes. Giao thức: số lượng các bits trong trường chỉ chiều dài của gói tin. Tương thích với một chuẩn quốc gia hay quốc tế nào đó. Mong muốn giảm thiểu tác động của việc truyền lại do lỗi gây ra. Mong muốn ngăn chặn một gói tin chiếm đường truyền quá lâu.

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

117

Và kết quả là các nhân viên thiết kế mạng không được tự do chọn kích thước gói tin tối đa như ý thích của họ. Kích thước dữ liệu tối đa của gói tin thay đổi từ 45 bytes (ATM cell) đến 65515 (gói tin IP). Vấn đề xuất hiện rõ ràng khi môt gói tin lớn muốn đi ngang một mạng con có kích thước gói tin tối đa quá nhỏ. Một giải pháp là làm cho vấn đề này không xảy ra. Nói cách khác, liên mạng nên sử dụng một giải thuật vạch đường có thể tránh được việc gởi gói tin qua các mạng không có khả năng tiếp nhận. Tuy nhiên giải pháp này thực ra không giải quyết được vấn đề. Nếu mạng đích không đủ khả năng tiếp nhận gói tin thì sao? Giải pháp duy nhất là cho phép các gateway chia nhỏ gói tin thành nhiều mảnh (fragment), gởi các mảnh này đi như là một gói tin độc lập. Tuy nhiên việc tái hợp các mảnh con này lại là việc khó.

H6.27. (a) Sự phân mảnh trong suốt. (b) Sự phân mảnh không trong suốt

Có hai chiến lược tái hợp các mảnh lại thành gói tin gốc: trong suốt và không trong suốt. Trong chiến lược phân mảnh trong suốt, khi một gói tin lớn đi qua một mạng con và mạng con này quyết định phải phân mảnh gói tin, một gateway của mạng con này sẽ làm nhiệm vụ phân mảnh gói tin lớn đó. Khi các mảnh đi hết qua mạng con, phải có một gateway khác đứng ra tập hợp lại chúng, tái tạo lại gói tin ban đầu và chuyển tiếp đến mạng con kế tiếp. Ví dụ trong hình H6.27, ở ngõ vào Mạng 1, gói tin lớn được phân mảnh bởi gateway G1, sau khi các mảnh đi qua hết Mạng 1, gateway G2 sẽ tập hợp chúng lại và tái tạo thành gói tin ban đầu. Chiến lược phân mảnh trong suốt rất trực quan, tuy nhiên có nhiều vấn đề phải bàn. Thứ nhất, gateway ở đầu ra phải biết khi nào nó đã thu lượm lại hết các phân mảnh. Thứ hai, làm sao để mọi phân mảnh phải đi ra cùng một gateway. Thứ ba, chi phí bỏ ra để phân mảnh và tái hợp gói tin lớn khi nó đi qua hàng loạt các mạng con. Với chiến lược phân mảnh không trong suốt, các mạng con trung gian có thể phân mảnh gói tin lớn, nhưng không có nhiệm vụ tái hợp lại nó. Việc tái hợp chỉ được thực hiện tại đích đến của gói tin này. Chiến lượt phân mảnh không trong suốt đòi hỏi mọi host trên mạng đều có khả năng tái hợp thông tin. Ngoài ra nó còn làm phát sinh chi phí cho các header của các mảnh con. Tuy nhiên cái lợi đạt được là: do chiến lược này có quyền chọn lựa nhiều gateway ở đầu ra của mạng con, cho nên hiệu suất vạch đường và truyền gói tin tăng lên nhiều lần. Từ đây, phát sinh nhu cầu về một cách thức đánh số các mảnh sao cho quá trình tái hợp được dễ dàng. Một cách đánh số thông dụng nhất là cách đánh số của internet. Ví dụ một gói tin có 10 bytes, số thứ tự của gói tin là 27 sẽ được biểu diễn như sau:

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

H6.28(a) Hình dạng gói tin ban dầu

Offset của mảnh là 0 vì đây chính là mảnh đầu tiên hay duy nhất trong gói tin. Bit kết thúc khung là 1 nghĩa là đã hết gói tin, là 0 nghĩa là còn mảnh nằm sau. Bây giờ gói tin này đi qua một mạng con có giới hạn kích thước gói tin tối đa là 8 bytes, nó sẽ bị phân làm hai mảnh:

H6.28(b) Gói bị chia thành hai mảnh 8 bytes và 2 bytes

Mảnh đầu tiên có offset trong gói tin là 0, bit kết thúc là 0 (còn mảnh thứ hai). Mảnh thứ hai có offset trong gói tin là 8 (nó bắt đầu ở vị trí thứ 8), và là mảnh cuối cùng. Nếu hai mảnh trên lại đi ngang qua gateway có giới hạn gói tin là 5 bytes, thì chúng sẽ bị phân mảnh như sau:

H6.28(c) Gói tin bị phân làm 3 mảnh.

6.6 Bộ giao thức liên mạng (IPs - Internet Protocols)
6.6.1 Giới thiệu
Các giao thức liên mạng là bộ giao thức cho các hệ thống mở nổi tiếng nhất trên thế giới bởi vì chúng có thể được sử dụng để giao tiếp qua bất kỳ các liên mạng nào cũng như thích hợp cho các giao tiếp trong mạng LAN và mạng WAN. Các giao thức liên mạng bao gồm một bộ các giao thức truyền thông, trong đó nổi tiếng nhất là Giao thức điều khiển truyền tải (TCP - Transmission Control Protocol) và Giao thức liên mạng (IP – Internet Protocol) hoạt động ở tầng 4 và tầng 3 trên mô hình OSI. Ngoài hai giao thức này, bộ giao thức IP còn đặc tả nhiều giao thức cho tầng ứng dụng, ví dụ như giao thức cho dịch vụ thư điện tử, giao thức mô phỏng thiết bị đầu cuối và giao thức truyền tải tập tin. Bộ giao thức liên mạng lần đầu tiên được phát triển vào giữa những năm của thập niên 70 khi Văn phòng các dự án nghiên cứu chuyên sâu của bộ quốc phòng Mỹ (DARPA-Defense Advanced Research Projects Agency ) quan tâm đến việc xây dựng một mạng chuyển mạch gói (packetswitched network) cho phép việc trao đổi thông tin giữa các hệ thống máy tính khác nhau của các viện nghiên cứu trở nên dễ dàng hơn. Với ý tưởng nối các hệ thống máy tính không đồng nhất lại với nhau, DARPA đã cấp kinh phí nghiên cứu cho đại học Stanford, Bolt, Beranek, and Newman (BBN) về vấn đề này. Kết quả của những nổ lực phát triển của dự án này là bộ giao thức Liên mạng đã được hoàn thành vào những năm cuối của thập niên bảy mươi. Sau đó TCP/IP được tích hợp vào hệ điều hành UNIX phiên bản BSD (Berkeley Software Distribution) trở thành nền tảng cho mạng Internet và dịch vụ WWW (World Wide Web).

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

119

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

H6.29 Kiến trúc của mạng TCP/IP so với mô hình OSI

6.6.2 Giao thức liên mạng IP (Internet Protocol)
Giao thức liên mạng, thường gọi là giao thức IP (Internet Protocol) là một giao thức mạng hoạt động ở tầng 3 của mô hình OSI, nó qui định cách thức định địa chỉ các máy tính và cách thức chuyển tải các gói tin qua một liên mạng. IP được đặc tả trong bảng báo cáo kỹ thuật có tên RFC (Request For Comments) mã số 791 và là giao thức chủ yếu trong Bộ giao thức liên mạng. Cùng với giao thức TCP, IP trở thành trái tim của bộ giao thức Internet. IP có hai chức năng chính : cung cấp dịch vụ truyền tải dạng không nối kết để chuyển tải các gói tin qua một liên mạng ; và phân mãnh cũng như tập hợp lại các gói tin để hỗ trợ cho tầng liên kết dữ liệu với kích thước đơn vị truyền dữ liệu là khác nhau.

6.6.2.1

Định dạng gói tin IP (IP Packet Format)

Hình sau mô tả cấu trúc của một gói tin IP

H6.30 Cấu trúc gói tin IP

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

120

Ý nghĩa của các trường được mô tả như sau: Version (Phiên bản): Xác định phiên bản của giao thức đang được sử dụng. IP Header Length (Chiều dài của phần tiêu đề : Xác định chiều dài của phần tiêu đề của gói tin, tính bằng đơn vị là từ - 32 bits (32-bit word). Type-of-Service (Kiểu của dịch vụ : Đặc tả mức độ quan trọng mà giao thức phía trên muốn xử lý gói tin. Total Length (Tổng chiều dài gói tin): Đặc tả chiều dài, tính bằng byte, của cả gói tin IP, bao gồm cả phần dữ liệu và tiêu đề. Identification ( Số nhận dạng ): Số nguyên nhận dạng gói tin dữ liệu hiện hành. Trường này được sử dụng để ráp lại các phân đoạn của gói tin. Flags (Cờ hiệu): Gồm 3 bít, bit có trọng số nhỏ để xác định gói tin có bị phân đoạn hay không. Bit thứ 2 xác định có phải đây là phân đoạn cuối cùng của gói tin hay không. Bit có trọng số lớn nhất chưa sử dụng. Fragment Offset (Vị trí của phân đoạn): Biểu thị vị trí của phân đoạn dữ liệu so với vị trí bắt đầu của gói dữ liệu gốc, nó cho phép máy nhận xây dựng lại gói tin ban đầu. Time-to-Live (Thời gian sống của gói tin): Lưu giữ bộ đếm thời gian, giá trị sẽ được giảm dần đến khi nó có giá trị là 0 thì gói tin sẽ bị xóa. Điều này giúp ngăn ngừa tình trạng gói tin được truyền đi lòng vòng không bao giờ đến được đích. Protocol(Giao thức): Biểu hiện giao thức ở tầng trên sẽ nhận gói tin khi nó đã được giao thức IP xử lý. Header Checksum (Tổng kiểm tra lỗi tiêu đề): kiểm tra tính toàn vẹn của phần tiêu đề. Source Addres : Địa của máy gởi gói tin. Destination Address: Địa chỉ của máy nhận gói tin. Options: Tùy chọn cho phép để hỗ trợ một số vấn đề, chẳng hạn vấn đề bảo mật. Data: Chứa dữ liệu của tầng trên gởi xuống cần truyền đi.

6.6.3 Cấu trúc địa chỉ IP
Mỗi máy tính trên mạng TCP/IP phải được gán một địa chỉ luận lý có chiều dài 32 bits, gọi là địa chỉ IP.

H6.31 Cấu trúc địa chỉ IP

32 bits của địa chỉ IP được chia thành 2 phần : Phần nhận dạng mạng (network id) và phần nhận dạng máy tính (Host id). Phần nhận dạng mạng được dùng để nhận dạng một mạng và phải được gán bởi Trung tâm thông tin mạng Internet (InterNIC - Internet Network Information Center) nếu muốn nối kết vào mạng Internet. Phần nhận dạng máy tính dùng để nhận dạng một máy tính trong một mạng.

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

H6.32 Phân lớp địa chỉ IP

Để dễ dàng cho việc đọc và hiểu bởi con người, 32 bits của địa chỉ IP được nhóm lại thành 4 bytes và được phân cách nhau bởi 3 dấu chấm (.). Giá trị của mỗi bytes được viết lại dưới dạng thập phân, với giá trị hợp lệ nằm trong khoản từ 0 đến 255. Câu hỏi được đặt ra là bao nhiêu bits dành cho phần nhận dạng mạng và bao nhiêu bits dành cho phần nhận dạng máy tính. Người ta phân các địa chỉ ra thành 5 lớp : A, B, C, D và E. Trong đó, chỉ có lớp A, B và C được dùng cho các mục đích thương mại. Các bits có trọng số cao nhất chỉ định lớp mạng của địa chỉ. Hình sau mô tả cách phân chia lớp cho các địa chỉ IP. Thông tin chi tiết về các lớp được mô tả như bảng sau : Lớp Dạng Mục đích Các bits cao nhất Khoản địa chỉ Số bít phần nhận dạng mạng / Số bít phần nhận dạng máy tính 7/24 14/16 Tổng số máy tính trong một mạng 16.777. 214 (224 - 2) 65. 543 (216 - 2) 254 (28 - 2)

A B

C

D E

N.H.H.H Cho một số ít các tổ chức lớn N.N.H.H Cho các tổ chức có kích thước trung bình N.N.N.H Cho các tổ chức có kích thước nhỏ Truyền nhóm Dành cho thí nghiệm

0 10

1.0.0.0 đến 126.0.0.0 128.1.0.0 đến 191.254.0.0 192.0.1.0 đến 223.255.254.0 224.0.0.0 đến 239.255.255.255 240.0.0.0 đến 254.255.255.255
Ghi chí H : Host, N=Network

110

21/8

1110 1111

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

122

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

6.6.4 ột số địa chỉ IP đặc biệt
Địa chỉ mạng (Network Address): là địa chỉ IP mà giá trị của tất cả các bits ở phần nhận dạng máy tính đều là 0, được sử dụng để xác định một mạng. o Ví dụ : 10.0.0.0; 172.18.0.0 ; 192.1.1.0 Địa chỉ quảng bá (Broadcast Address) : Là địa chỉ IP mà giá trị của tất cả các bits ở phần nhận dạng máy tính đều là 1, được sử dụng để chỉ tất cả các máy tính trong mạng. o Ví dụ : 10.255.255.255, 172.18.255.255, 192.1.1.255 Mặt nạ mạng chuẩn (Netmask) : Là địa chỉ IP mà giá trị của các bits ở phần nhận dạng mạng đều là 1, các bits ở phần nhận dạng máy tính đều là 0. Như vậy ta có 3 mặt nạ mạng tương ứng cho 3 lớp mạng A, B và C là : o Mặt nạ mạng lớp A : 255.0.0.0 o Mặt nạ mạng lớp B : 255.255.0.0 o Mặt nạ mạng lớp C : 255.255.255.0 Ta gọi chúng là các mặt nạ mạng mặc định (Default Netmask) Lưu ý : Địa chỉ mạng, địa chỉ quảng bá, mặt nạ mạng không được dùng để đặt địa chỉ cho các máy tính Địa chỉ mạng 127.0.0.0 là địa chỉ được dành riêng để đặt trong phạm vi một máy tính. Nó chỉ có giá trị cục bộ ( trong phạm vi một máy tính). Thông thường khi cài đặt giao thức IP thì máy tính sẽ được gián địa chỉ 127.0.0.1. Địa chỉ này thông thường để kiểm tra xem giao thức IP trên máy hiện tại có hoạt động không. Địa chỉ dành riêng cho mạng cục bộ không nối kết trực tiếp Internet : Các mạng cục bộ không nối kết trực tiếp vào mạng Internet có thể sử dụng các địa chỉ mạng sau để đánh địa chỉ cho các máy tính trong mạng của mình : o Lớp A : 10.0.0.0 o Lớp B : 172.16.0.0 đến 172.32.0.0 o Lớp C : 192.168.0.0

6.6.5 Ý nghĩa của Netmask
Với một địa chỉ IP và một Netmask cho trước, ta có thể dùng phép toán AND BIT để tính ra được địa chỉ mạng mà địa chỉ IP này thuộc về. Công thức như sau : Network Address = IP Address & Netmask Ví dụ : Cho địa chỉ IP = 198.53.147.45 và Netmask = 255.255.255.0. Ta thực hiện phép toán AND BIT (&) hai địa chỉ trên: Biểu diễn thập phân 198.53.147.45 255.255.255.0 198.53.147.0 Biểu diễn nhị phân 11000110 00110101 10010011 00101101 11111111 11111111 11111111 00000000 11000110 00110101 10010011 00000000

IP Address Netmask Network Address

6.6.6 Phân mạng con (Subnetting)
6.6.6.1 Giới thiệu
Phân mạng con là một kỹ thuật cho phép nhà quản trị mạng chia một mạng thành những mạng con nhỏ, nhờ đó có được các tiện lợi sau : Đơn giản hóa việc quản trị : Với sự trợ giúp của các router, các mạng có thể được chia ra thành nhiều mạng con (subnet) mà chúng có thể được quản lý như những mạng độc lập và hiệu quả hơn.

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

123

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

Có thể thay đổi cấu trúc bên trong của mạng mà không làm ảnh hướng đến các mạng bên ngoài. Một tổ chức có thể tiếp tục sử dụng các địa chỉ IP đã được cấp mà không cần phải lấy thêm khối địa chỉ mới. Tăng cường tính bảo mật của hệ thống : Phân mạng con sẽ cho phép một tổ chức phân tách mạng bên trong của họ thành một liên mạng nhưng các mạng bên ngoài vẫn thấy đó là một mạng duy nhất. Cô lập các luồng giao thông trên mạng : Với sự trợ giúp của các router, giao thông trên mạng có thể được giữ ở mức thấp nhất có thể.

H6.33 Địa chỉ mạng con đối với thế giới bên ngoài

Hình trên mô tả một địa chỉ IP đã được phân mạng con xuất hiện với thế giới Internet bên ngoài và với mạng Intranet bên trong. Internet chỉ đọc phần nhận dạng mạng và các router trên Internet chỉ quan tâm tới việc vạch đường cho các gói tin đến được router giao tiếp giữa mạng Intranet bên trong và mạng Internet bên ngoài. Thông thường ta gọi router này là cửa khẩu của mạng (Gateway). Khi một gói tin IP từ mạng bên ngoài đến router cửa khẩu, nó sẽ đọc phần nhận dạng máy tính để xác định xem gói tin này thuộc về mạng con nào và sẽ chuyển gói tin đến mạng con đó, nơi mà gói tin sẽ được phân phát đến máy tính nhận.

6.6.6.2

Phương pháp phân mạng con

Nguyên tắc chung để thực hiện phân mạng con là : Phần nhận dạng mạng (Network Id) của địa chỉ mạng ban đầu được giữ nguyên. Phần nhận dạng máy tính của địa chỉ mạng ban đầu được chia thành 2 phần : Phần nhận dạng mạng con (Subnet Id) và Phần nhận dạng máy tính trong mạng con (Host Id). Network Id Host Id

Subnet Id
H6.33 Cấu trúc địa chỉ IP khi phân mạng con

Để phân mạng con, người ta phải xác định mặt nạ mạng con (subnetmask). Mặt nạ mạng con là một địa chỉ IP mà giá trị các bit ở phần nhận dạng mạng (Network Id) và Phần nhận dạng mạng

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

124

con (Subnet Id) đều là 1 trong khi giá trị của các bits ở Phần nhận dạng máy tính (Host Id) đều là 0. Hình H6.34 mô tả mặt nạ phân mạng con cho một mạng ở lớp C. Network Id 11111111 11111111 11111111

Host Id
111 00000

Subnet Id
H6.34 Mặt nạ mạng con khi phân mạng con

Khi có được mặt nạ mạng con, ta có thể xác định địa chỉ mạng con (Subnetwork Address) mà một địa chỉ IP được tính bằng công thức sau : Subnetwork Address = IP & Subnetmask Có hai chuẩn để thực hiện phân mạng con là : Chuẩn phân lớp hoàn toàn (Classfull standard) và chuẩn Vạch đường liên miền không phân lớp CIDR (Classless Inter-Domain Routing ). Thực tế, CIDR chỉ mới được đa số các nhà sản xuất thiết bị và hệ điều hành mạng hỗ trợ nhưng vẫn chưa hoàn toàn chuẩn hóa.

6.6.6.2.1

Phương pháp phân lớp hoàn toàn (Classfull Standard)

Chuẩn này qui định địa chỉ IP khi phân mạng con sẽ gồm 3 phần : Phần nhận dạng mạng của địa chỉ ban đầu (Network Id): Phần nhận dạng mạng con (Subnet Id) : Được hình thành từ một số bits có trọng số cao trong phần nhận dạng máy tính (Host Id) của địa chỉ ban đầu Và cuối cùng là phần nhận dạng máy tính trong mạng con (Host Id) bao gồm các bit còn lại. Ví dụ : Hình sau mô tả cấu trúc địa chỉ IP lớp C khi thực hiện phân mạng con Original Network Id IP bình thường Original Network Id IP có phân mạng con Subnet Id H6.35 Địa chỉ IP phân mạng con theo chuẩn Phân lớp hoàn toàn

Original Host Id

Host Id

Số lượng bits thuộc phần nhận dạng mạng con xác định số lượng mạng con. Giả sử phần nhận dạng mạng con chiếm 4 bits. Như vậy, về mặt lý thuyết ta có thể phân ra thành 24=16 mạng con. Tuy nhiên phần nhận dạng mạng con gồm toàn bit 0 hoặc bit 1 không được dùng để đánh địa chỉ cho mạng con vì nó trùng với địa chỉ mạng và địa chỉ quảng bá của mạng ban đầu. Ví dụ : Cho địa chỉ mạng lớp C : 192.168.1.0 với mặt nạ mạng mặc định là 255.255.255.0. Xét trường hợp phân mạng con cho mạng trên sử dụng 2 bits để làm phần nhận dạng mạng con. Mặt nạ mạng trong trường hợp này là 255.255.255.192. Khi đó ta có các địa chỉ mạng con như sau :

125

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

Địa chỉ IP Mạng ban đầu Mạng con 1 Mạng con 2 Mạng con 3 Mạng con 4

Biểu diễn dạng thập phân 192.168.1.0 192.168.1.0 192.168.1.64 192.168.1.128 192.168.1.192

Biểu diễn dạng nhị phân 1100 0000 1100 0000 1100 0000 1100 0000 1100 0000 1010 1000 1010 1000 1010 1000 1010 1000 1010 1000 0000 0001 0000 0001 0010 0001 0000 0001 0000 0001 0000 0000 0000 0000 0100 0000 1000 0000 1100 0000

Ta nhận thấy rằng: Địa chỉ mạng con thứ nhất 192.168.1.0 trùng với địa chỉ mạng ban đầu. Địa chỉ mạng con thứ tư 192.168.1.192 có địa chỉ quảng bá trùng với địa chỉ quảng bá của mạng ban đầu . Chính vì thế mà hai địa chỉ này ( có phần nhận dạng mạng con toàn bit 0 hoặc toàn bit 1) không được dùng để đánh địa chỉ cho mạng con. Nói tóm lại, với n bits làm phần nhận dạng mạng con ta chỉ có thể phân ra được 2n-2 mạng con mà thôi. Mỗi mạng con cũng có địa chỉ quảng bá. Đó là địa chỉ mà các bits ở phần nhận dạng máy tính đều có giá trị là 1. Ví dụ : Địa chỉ IP Mạng con 1 Địa chỉ quảng bá Mạng con 2 Địa chỉ quảng bá Biểu diễn dạng thập phân 192.168.1.64 192.168.1.127 192.168.1.128 192.168.1.191 Biểu diễn dạng nhị phân 1100 0000 1100 0000 1100 0000 1100 0000 1010 1000 1010 1000 1010 1000 1010 1000 0010 0001 0010 0001 0000 0001 0000 0001 0100 0000 0111 1111 1000 0000 1011 1111

Như vậy qui trình phân mạng con có thể được tóm tắt như sau : Xác định số lượng mạng con cần phân, giả sử là N. Biểu diễn (N+1) thành số nhị phân. số lượng bit cần thiết để biểu diễn (N+1) chính là số lượng bits cần dành cho phần nhận dạng mạng con. Ví dụ N=6, khi đó biểu diễn của (6+1) dưới dạng nhị phân là 111. Như vậy cần dùng 3 bits để làm phần nhận dạng mạng con Tạo mặt nạ mạng con Liệt kê tất cả các địa chỉ mạng con có thể, trừ hai địa chỉ mà ở đó phần nhận dạng mạng con toàn các bits 0 và các bit 1. Chọn ra N địa chỉ mạng con từ danh sách các mạng con đã liệt kê.

6.6.6.2.2

Phương pháp Vạch đường liên miền không phân lớp CIDR (Classless Inter-Domain Routing )

CIDR là một sơ đồ đánh địa chỉ mới cho mạng Internet hiệu quả hơn nhiều so với sơ đồ đánh địa chỉ cũ theo kiểu phân lớp A, B và C. CIDR ra đời để giải quyết hai vấn đề bức xúc đối với mạng Internet là : Thiếu địa chỉ IP Vượt quá khả năng chứa đựng của các bảng chọn đường.

6.6.6.3

Vấn đề thiếu địa chỉ IP

Với sơ đồ đánh địa chỉ truyền thống, các địa chỉ được phân ra thành các lớp A, B và C. Mỗi địa chỉ có 2 phần, phần nhận dạng mạng và phần nhận dạng máy tính. Khi đó số lượng mạng và số máy tính tối đa cho từng mạng được thống kê như bảng sau :

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

126

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

Lớp mạng A B C

Số lượng mạng 126 65.000 Hơn 2 triệu

Số máy tính tối đa trong mạng 16.777.214 65.534 254

Bởi vì các địa chỉ của mạng Internet thường được gán theo kích thước này dẫn đến tình trạng lãng phí. Trường hợp bạn cần 100 địa chỉ, Bạn sẽ được cấp một địa chỉ lớp C. Như vậy còn 154 địa chỉ không được sử dụng. Chính điều này dẫn đến trình trạng thiếu địa chỉ IP cho mạng Internet. Theo thống kê, chỉ có khoảng 3% số địa chỉ đã được cấp phát được sử dụng đến. Chính vì thế sơ đồ đánh địa chỉ mới CIDR ra đời để khắc phục tình trạng trên.

6.6.6.4

Vấn đề vượt quá khả năng chứa đựng của các bảng chọn đường

Khi số lượng mạng trên mạng Internet tăng cũng đồng nghĩa với việc tăng số lượng router trên mạng. Trong những năm gần đây, người ta dự đoán rằng các router đường trục của mạng Internet đang nhanh chóng tiến đến mức ngưỡng tối đa số lượng router mà nó có thể chấp nhận được. Thậm chí với những công nghệ hiện đại dùng để sản xuất các router thì về mặt lý thuyết kích thước tối đa của một bảng chọn đường cũng chỉ đến 60.000 mục từ (đường đi). Nếu không có những cải tiến thì các router đường trục sẽ đạt đến con số này và như thế không thể mở rộng mạng Internet hơn nữa. Để giải quyết hai vấn đề trên, cộng đồng Internet đã đưa ra các giải pháp sau : Sửa đổi lại cấu trúc cấp phát địa chỉ IP để tăng hiệu quả Kết hợp việc chọn đường có cấu trúc để giảm tối đa số lượng các mục từ trong bảng chọn đường.

6.6.6.5

Sửa đổi lại cấu trúc cấp phát địa chỉ IP

CIDR được sử dụng để thay thế cho sơ đồ cấp phát cũ với việc qui định các lớp A, B, C. Thay vì phần nhận dạng mạng được giới hạn với 8, 16 hoặc 24 bits, CIDR sử dụng phần nhận dạng mạng có tính tổng quát từ 13 đến 27 bits. Chính vì thế các khối địa chỉ có thể được gán cho mạng nhỏ nhất với 32 máy tính đến mạng lớn nhất hơn 500.000 máy tính. Điều này đáp ứng gần đúng yêu cầu đánh địa chỉ của các tổ chức khác nhau.

6.6.6.6

Địa chỉ CIDR

Một địa chỉ theo cấu trúc CIDR, gọi tắt tắt địa chỉ CIDR, bao gồm 32 bits của địa chỉ IP chuẩn cùng với một thông tin bổ sung về số lượng các bit được sử dụng cho phần nhận

dạng mạng. Ví dụ : Với địa chỉ CIDR 206.13.01.48/25 thì chuỗi số "/25" chỉ ra rằng 25 bits đầu tiên trong địa chỉ IP được dùng để nhận dạng duy nhất một mạng, số bits còn lại dùng để nhận dạng một máy tính trong mạng. Bảng sau so sánh giữa sơ đồ đánh địa chỉ theo kiểu CIDR và sơ đồ đánh địa chỉ theo chuẩn phân lớp hoàn toàn. Số bits nhận dạng mạng trong địa chỉ CIDR /27 /26 /25 /24 /23 /22 Lớp tương ứng trong chuẩn phân lớp hoàn toàn 1/8 lớp C ¼ lớp C 1/2 lớp C 1 lớp C 2 lớp C 4 lớp C Số lượng máy tính trong mạng 32 64 128 256 512 1.024

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

127

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

/21 /20 /19 /18 /17 /16 /15 /14 /13

8 lớp C 16 lớp C 32 lớp C 64 lớp C 128 lớp C 256 lớp C (= 1 lớp B) 512 lớp C 1,024 lớp C 2,048 lớp C

2.048 4.096 8.192 16.384 32.768 65.536 131.072 262.144 524.288

Kết hợp việc chọn đường có cấu trúc để giảm tối đa số lượng các mục từ trong bảng chọn đường. Sơ đồ đánh địa chỉ theo theo CIDR cũng cho phép kết hợp các đường đi, ở đó mục từ trong bảng chọn đường ở mức cao có thể đại diện cho nhiều router ở mức thấp hơn trong các bảng chọn đường tổng thể. Sơ đồ này giống như hệ thống mạng điện thoại ở đó mạng được thiết lập theo kiến trúc phân cấp. Một router ở mức cao (quốc gia), chỉ quan tâm đến mã quốc gia trong số điện thoại, sau đó nó sẽ vạch đường cho cuộc gọi đến router đường trục phụ trách mạng quốc gia tương ứng với mã quốc gia đó. Router nhận được cuộc gọi nhìn vào phần đầu của số điện thoại, mã tỉnh, để vạch đường cho cuộc gọi đến một mạng con tương ứng với mã tỉnh đó, và cứ như thế. Trong sơ đồ này, các router đường trục chỉ lưu giữ thông tin về mã quốc gia cho mỗi mục từ trong bảng chọn đường của mình, mỗi mục từ như thế đại diện cho một số khổng lồ các số điện thoại riêng lẽ chứ không phải là một số điện thoại cụ thể. Thông thường, các khối địa chỉ lớn được cấp cho các nhà cung cấp dịch vụ Internet (IP- Internet Service Providers) lớn, sau đó họ lại cấp lại các phần trong khối địa chỉ của họ cho các khách hàng của mình. Hiện tại, mạng Internet sử dụng cả hai sơ đồ cấp phát địa chỉ Classfull standard và CIDR. Hầu hết các router mới đều hỗ trợ CIDR và những nhà quản lý Internet thì khuyến khích người dùng cài đặt sơ đồ đánh địa chỉ CIDR. Tham khảo thêm về CIDR ở địa chỉ http://www.rfc-editor.org/rfcsearch.html với các RFC liên quan sau:
• • • •

RFC 1517: Applicability Statement for the Implementation of CIDR RFC 1518: An Architecture for IP Address Allocation with CIDR RFC 1519: CIDR: An Address Assignment and Aggregation Strategy RFC 1520: Exchanging Routing Information Across Provider Boundaries in the CIDR Environment

6.6.7 Vạch đường trong giao thức IP
Cho ba mạng Net1, Net2 và Net3 nối lại với nhau nhờ 3 router R1, R2 và R3. Mạng Net4 nối các router lại với nhau. Công việc đầu tiên trong thiết kế mạng liên mạng IP là chọn địa chỉ mạng cho các nhánh mạng. Trong trường hợp này ta chọn mạng lớp C cho 4 mạng như bảng sau:

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

128

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

Mạng Net1 Net2 Net3 Net4

Địa chỉ mạng 192.168.1.0 192.168.2.0 192.168.3.0 192.168.4.0

Mặt nạ mạng 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0

Kế tiếp, gán địa chỉ cho từng máy tính trong mạng. Ví dụ trong mạng Net1, các máy tính được gán địa chỉ là 192.168.1.2 (Ký hiệu .2 là cách viết tắt của địa chỉ IP để mô tả Phần nhận dạng máy tính) và 192.168.1.3. Mỗi router có hai giao diện tham gia vào hai mạng khác nhau. Ví dụ, giao diện tham gia vào mạng NET1 của router R1 có địa chỉ là 192.168.1.1 và giao diện tham gia vào mạng NET4 có địa chỉ là 192.168.4.1.

H6.36 Ví dụ về liên mạng một liên mạng sử dụng giao thức IP

Để máy tính của các mạng có thể giao tiếp được với nhau, cần phải có thông tin về đường đi. Bảng chọn đường của router có thể tạo ra thủ công hoặc tự động. Đối với mạng nhỏ, nhà quản trị mạng sẽ nạp đường đi cho các router thông qua các lệnh được cung cấp bởi hệ điều hành của router. Bảng chọn đường trong giao thức IP có 4 thông tin quan trọng là : Địa chỉ mạng đích Mặt nạ mạng đích Router kế tiếp sẽ nhận gói tin (Next Hop) Giao diện chuyển gói tin đi Trong ví dụ trên, các router sẽ có bảng chọn đường như sau :

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

129

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

Các máy tính cũng có bảng chọn đường. Dưới đây là bảng chọn đường của máy tính có địa chỉ 192.168.3.3 :

Mạng đích default ý nói rằng ngoài những đường đi đến các mạng đã liệt kê phía trên, các đường đi còn lại thì gởi cho NextHop của mạng default này. Như vậy, để gởi gói tin cho bất kỳ một máy tính nào nằm bên ngoài mạng 192.168.3.0 thì máy tính 192.168.3.3 sẽ chuyển gói tin cho router 3 ở địa chỉ 192.168.3.1.

6.6.7.1

Đường đi của gói tin

Để hiểu rõ có chế hoạt động của giao thức IP, ta hãy xét hai trường hợp gởi gói tin : Trường hợp máy tính gởi và nhận nằm trong cùng một mạng và trường hợp máy tính gởi và máy tính nhận nằm trên hai mạng khác nhau. Giả sử máy tính có địa chỉ 192.168.3.3 gởi một gói tin cho máy tính 192.168.3.2. Tầng hai của máy gởi sẽ đặt gói tin vào một khung với địa chỉ nhận là địa chỉ vật lý của máy nhận và gởi khung lên đường truyền NET3, trên đó máy tính nhận sẽ nhận được gói tin. Bây giờ ta xét trường hợp máy tính có địa chỉ 192.168.3.3 trên mạng NET3 gởi gói tin cho máy tính có địa chỉ 192.168.1.2 trên mạng Net1. Theo như bảng chọn đường của máy gởi, các gói tin có địa chỉ nằm ngoài mạng 192.168.3.0 sẽ được chuyển đến router R3 (địa chỉ 192.168.3.1). Chính vì thế, máy tính gởi sẽ đặt gói tin vào một khung với địa chỉ nhận là địa chỉ vật lý của giao diện 192.168.3.1 và đưa lên đường truyền NET3. Nhận được gói tin, R3 phân tích địa chỉ IP của máy nhận để xác định đích đến của gói tin . Bảng chọn đường cho thấy, với đích đến là mạng 192.168.1.0 thì cần phải chuyển gói tin cho router R1 ở địa chỉ 192.168.4.1 thông qua giao diện 192.168.4.3. Vì thế R3 đặt gói tin vào một khung với địa chỉ nhận là địa chỉ vật lý của giao diện 192.168.4.1 của router R1 và đưa lên đường truyền NET4. Tương tự, R1 sẽ chuyển gói tin cho máy nhận 192.168.1.2 bằng một khung trên đường truyền NET1.

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

130

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

Ta nhận thấy rằng, để đi đến được máy nhận, gói tin được chuyển đi bởi nhiều khung khác nhau. Mỗi khung sẽ có địa chỉ nhận khác nhau, tuy nhiên địa chỉ của gói tin thì luôn luôn không đổi.

6.6.7.2

Giao thức phân giải địa chỉ (Address Resolution Protocol)

Nếu một máy tính muốn truyền một gói tin IP nó cần đặt gói tin này vào trong một khung trên đường truyền vật lý mà nó đang nối kết vào. Để có thể truyền thành công khung, máy tính gởi cần thiết phải biết được địa chỉ vật lý (MAC) của máy tính nhận. Điều này có thể thực hiện được bằng cách sử dụng một bảng để ánh xạ các địa chỉ IP về địa chỉ vật lý. Giao thức IP sử dụng giao thức ARP (Address Resolution Protocol) để thực hiện ánh xạ từ một địa chỉ IP về một địa chỉ MAC.

H6.37 Giao thức ARP

Một máy tính xác định địa chỉ vật lý của nó vào lúc khởi động bằng cách đọc thiết bị phần cứng và xác định địa chỉ IP của nó bằng cách đọc tập tin cấu hình, sau đó lưu thông tin về mối tương ứng giữa địa chị IP và MAC của nó vào trong vùng nhớ tạm (ARP cache). Khi nhận được một địa chỉ IP mà ARP không thể tìm ra được địa chỉ vật lý tương ứng dựa vào vùng nhớ tạm hiện tại, nó sẽ thực hiện một khung quảng bá có định dạng như sau :

Tổng quát

Các trường Ethernet Destination Address

Kích thức (byte) 6 6 2 2 2

Các giá trị Địa chỉ máy nhận, trong trường hợp này là một địa chỉ quảng bá Địa chỉ của máy gởi thông điệp Kiểu khung, có giá trị là 0x0806 khi ARP yêu cầu và 0x8035 khi ARP trả lời Giá trị là 1 cho mạng Ethernet Có giá trị là 0x0800 cho địa chỉ IP

Ethernet Header

Ethernet Source Address Frame Type

ARP request/reply

Hardware Type Protocol Type

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

131

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

Hardware Address Size in bytes

1

Chiều dài của địa chỉ vật lý, có giá trị là 6 cho mạng Ethernet Chiều dài địa chỉ của giao thức, có giá trị là 4 cho giao thức IP Là 1 nếu là khung yêu cầu, là 2 nếu là khung trả lời Không sử dụng đến trong yêu cầu của ARP -

Protocol Address Size 1 in bytes Operation Sender Ethernet Address Sender IP Address Destination Ethernet Address Destination IP Address 2 6 4 6 4

Nhờ vào việc gởi các yêu cầu này, một máy tính có thể bổ sung thông tin cho vùng cache của giao thức ARP, nhờ đó cập nhật kịp thời mọi sự thay đổi của sơ đồ mạng. Thông thường thời gian quá hạn (Time-out) cho một thông tin trong vùng cache là 20 phút. Một yêu cầu ARP cho một máy tính không tồn tại trên nhánh mạng được lặp lại một vài lần xác định nào đó. Nếu một máy tính được nối kết vào nhiều hơn một mạng bằng giao diện mạng, khi đó sẽ tồn tại những vùng cache ARP riêng cho từng giao diện mạng. Lưu ý, ARP trên một máy tính chỉ thực hiện việc xác địa chỉ vật lý cho các địa chỉ cùng địa chỉ mạng / mạng con với nó mà thôi. Đối với các gói tin gởi cho các máy tính có địa chỉ IP không cùng một mạng / mạng con với máy gởi sẽ được chuyển hướng cho một router nằm cùng mạng với máy gởi để chuyển đi tiếp. Vì các yêu cầu ARP được quảng bá rộng rãi, cho nên bất kỳ một máy tính nào đang duy trì một vùng cache đều có thể theo dõi tất cả các yều cầu được quảng bá này để lấy thông tin về địa chỉ vật lý và địa chỉ IP của máy gởi yêu cầu và bổ sung vào vùng cache của nó khi cần thiết. Khi một máy tính khởi động, nó gởi một yêu cầu ARP ( có thể cho chính nó) như để thông báo với các máy tính khác về sự xuất hiện của nó trong mạng cục bộ. Có thể gán nhiều hơn một địa chỉ IP cho một địa chỉ vật lý. Chú ý rằng, định dạng của yêu cầu ARP thì được thiết kế để có thể hỗ trợ được cho các giao thức khác ngoài IP và Ethernet.

6.6.7.3

Giao thức phân giải địa chỉ ngược RARP (Reverse Address Resolution Protocol)

Ngày nay, các trạm làm việc không đĩa cứng (Diskless workstation) được sử dụng rộng rãi. Mỗi máy tính chỉ cần bộ xử lý và bộ nhớ, tất cả không gian lưu trữ được cung cấp từ một máy chủ (Server) sử dụng một hệ thống tập tin mạng theo một chuẩn nào đó. Do không có các tập tin cấu hình, tiến trình khởi động của các máy tính này thường sử dụng một giao thức truyền tải tập tin rất đơn giản như TFTP. Tuy nhiên, trước khi có thể nối kết đến được server, các trạm làm việc cần phải biết được địa chỉ IP của nó. Giao thức RARP được dùng trong trường hợp này. RARP sử dụng cùng định dạng yêu cầu của ARP nhưng trường Operation có giá trị là 3 cho yêu cầu và 4 cho trả lời. Trên server duy trì một bảng mô tả mối tương quan giữa địa chỉ vật lý và địa chỉ IP của các máy trạm. Khi nhận được yêu cầu RARP, server tìm trong bảng địa chỉ và trả về địa chỉ IP tương ứng cho máy trạm đã gởi yêu cầu.

6.6.7.4

Giao thức thông điệp điều khiển Internet ICMP (Internet Control Message Protocol)

Giao thức ICMP được cài đặt trong hầu hết tất cả các máy tính TCP/IP. Các thông điệp của giao thức được gởi đi trong các gói tin IP và được dùng để gởi đi các báo lỗi hay các thông tin điều khiển.
Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

132

ICMP tạo ra nhiều loại thông điệp hữu ích như : Đích đến không tới được (Destination Unreachable), Thăm hỏi và trả lời (Echo Request and Reply), Chuyển hướng (Redirect), Vượt quá thời gian (Time Exceeded), Quảng bá bộ chọn đường (Router Advertisement) Cô lập bộ chọn đường (Router Solicitation) .... Nếu một thông điệp không thể phân phát được thì nó sẽ không được gởi lại. Điều này để tránh tình trạng di chuyển không bao giờ dừng của các thông điệp ICMP. Nếu một thông điệp « Đích đến không tới được » được gởi đi bởi một router, điều đó có nghĩa rằng router không thể gởi gói tin đến đích được. Khi đó router sẽ xóa gói tin ra khỏi hàng đợi của nó. Có hai nguyên nhân làm cho một gói tin không thể đi đến nơi được. Phần lớn là máy gởi mô tả một địa chỉ nhận mà nó không tồn tại trên thực tế. Trường hợp ít hơn là router không biết đường đi đến nơi nhận gói tin. Thông điệp Đích đến không tới được được chia thành bốn loại cơ bản là : Mạng không đến được (Network unreachable) : Có nghĩa là có sự cố trong vấn đề vạch đường hoặc địa chỉ nhận của gói tin. Máy tính không đến được (Host unreachable) : Thông thường dùng để chỉ trục trặc trong vấn đề phân phát, như là sai mặt nạ mạng con chẳng hạn. Giao thức không đến được (Protocol unreachable) : Máy nhận không hỗ trợ giao thức ở tầng cao hơn như gói tin đã mô tả. Cổng không đến được (Port unreachable) : Socket của giao thức TCP hay cổng không tồn tại. Một thông điệp « Thăm hỏi và trả lời » được tạo ra bởi lệnh ping từ một máy tính để kiểm tra tính liên thông trên liên mạng. Nếu có một thông điệp trả lời, điều đó biểu hiện rằng giữa máy gởi và máy nhận có thể giao tiếp được với nhau. Một thông điệp « Chuyển hướng » được gởi bởi một router đến máy đã gởi gói tin để khuyến cáo về một đường đi tốt hơn. Router hiện tại vẫn chuyển tiếp gói tin mà nó nhận được. Thông điệp chuyển hướng giữ cho bảng chọn đường của các máy tính được nhỏ bởi vì chúng chỉ cần chứa địa chỉ của một router mà thôi, thậm chí router đó cung cấp đường đi không phải là tốt nhất. Đôi khi sau khi nhận được thông điệp chuyển hướng, thiết bị gởi vẫn sử dụng đường đi cũ. Một thông điệp « Vượt quá thời hạn » được gởi bởi một router nếu thời gian sống (Time–to-live) của gói tin, tính bằng số router hay giây, có giá trị là 0. Thời gian sống của gói tin giúp phòng ngừa trường hợp gói tin được gởi đi lòng vòng trên mạng và không bao giờ đến nơi nhận. Router sẽ bỏ đi các gói tin đã hết thời gian sống.

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

Chương 7: TẦNG VẬN CHUYỂN
Mục đích
Chương này nhằm giới thiệu với người đọc những nội dung sau: • Vai trò của tầng vận chuyển và các chức năng mà tầng vận chuyển cung cấp cho tầng ứng dụng • Ý nghĩa và cơ chế thiết lập nối kết và giải phóng nối kết cho các nối kết điểm – điểm • Chi tiết về hay giao thức TCP và UDP thuộc tầng vận chuyển

Yêu cầu
Sau khi học xong chương này, người học phải có được những khả năng sau: • Biện luận được sự cần thiết của tầng vận chuyển trong một liên mạng • Giải thích được cơ chế thiết lập và xóa nối kết các cuộc giao tiếp điểm-điểm của tầng vận chuyển • Trình bày được nguyên tắc hoạt động của hai giao thức TCP và UDP của mạng Internet

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

134

7.1

Dịch vụ của tầng vận chuyển

Trong khi tầng mạng đảm bảo việc chuyển gói tin từ một host đến một host khác, tầng vận chuyển lại làm trung gian giữa tầng mạng và các ứng dụng mạng – nó chuyển thông tin giữa các tiến trình chạy trên các host khác nhau. Phần sau sẽ thảo luận về các dịch vụ và kiểu dịch vụ mà tầng vận chuyển cung cấp cho tầng ứng dụng.

7.1.1 Các dịch vụ cung cấp cho tầng ứng dụng
Mục tiêu quan trọng của tầng vận chuyển là cung cấp dịch vụ vận chuyển gói tin hiệu quả, tin cậy và tiết kiệm chi phi cho người dùng của nó, ở đây là các tiến trình chạy ở tầng ứng dụng. Phần cứng/mềm nằm trong lớp vận chuyển và hoạt động ở đó được gọi là thực thể vận chuyển. Thực thể vận chuyển có thể nằm ở nhân của hệ điều hành, trong một tiến trình người dùng riêng biệt, trong một gói thư viện liên quan đến các ứng dụng mạng, hoặc thậm chí được gói gọn trong card mạng. Mối quan hệ logic giữa tầng mạng, tầng vận chuyển và tầng ứng dụng được thể hiện trong hình sau H7.1.

H7.1 Các tầng mạng, vận chuyển và ứng dụng

Có hai kiểu dịch vụ vận chuyển: có nối kết và không nối kết. Và tầng vận chuyển cũng phải cung cấp các tham số để người dùng chỉ định loại dịch vụ họ mong muốn. Loại dịch vụ vận chuyển có nối kết hoạt động giống như dịch vụ có nối kết của tầng mạng. Nghĩa là nó có 3 kỳ: thiết lập nối kết, truyền dữ liệu và hủy nối kết. Loại dịch vụ không nối kết cũng giống như ở tầng mạng, chỉ đơn giản đẩy gói tin ra mạng và hy vọng nó đến đích. Từ đây phát sinh câu hỏi: Hai tầng vận chuyển và mạng hoạt động giống nhau, sao không nhập lại làm một? Câu trả lời rất dễ gây tranh cãi: Mã lệnh vận chuyển nằm hoàn toàn trong máy tính của người dùng, nhưng lớp mạng hầu hết chạy trên các router. Nếu nhập cả hai vào một lớp mạng, giả sử lớp mạng cung cấp dịch vụ không thỏa đáng thì sao? Nếu lớp mạng thường xuyên làm mất gói tin thì sao? Nếu các router bị chết thường xuyên thì sao? Vấn đề phát sinh ở chỗ, người dùng không có quyền điều khiển thực sự lên lớp mạng, do đó họ không thể giải quyết vấn đề dịch vụ không tốt bằng cách chọn các đường đi khác, hay áp đặt thêm nhiều giải pháp điều khiển lỗi lên lớp liên kết dữ liệu. Khả năng duy nhất có thể được là đặt trên lớp mạng một lớp khác làm nhiệm vụ cải thiện chất lượng dịch vụ. Nếu, trong một mạng con dạng hướng nối kết, một thực thể vận chuyển được thông báo giữa lúc truyền dữ liệu rằng kết nối mạng đã bị gãy, nó có thể thiết lập một kết nối mạng khác đến bên đối thoại bên kia, rồi gởi đi câu hỏi

rằng dữ liệu nào đã đến, cái nào chưa và cuối cùng khởi động lại từ điểm bị bỏ dở dang. Dữ liệu bị mất hoặc bị hư hỏng sẽ được phục hồi bởi lớp vận chuyển, do đó việc chuyển dữ liệu an toàn hơn. Như thường lệ, tại lớp vận chuyển, người ta thiết kế các hàm dịch vụ cơ sở để triệu gọi các dịch vụ vận chuyển và các hàm này là đơn giản, duy nhất và độc lập với các hàm cơ sở ở tầng mạng. Nhờ vào sự độc lập này, sự phức tạp ở mức mạng bị che đi, các nhà lập trình ứng dụng có thể viết mã lệnh dựa vào một tập hợp chuẩn các hàm cơ sở mức vận chuyển và cho chương trình của họ chạy trên nhiều loại mạng mà không bị đau đầu bởi các vấn đề về giao diện các mạng con khác nhau và việc truyền tải không tin cậy.

7.1.2 Các hàm dịch vụ cơ sở
Các hàm dịch vụ cơ sở ở lớp vận chuyển được chia thành hai nhóm theo phương thức hoạt động: có nối kết và không nối kết.

7.1.3 Các hàm dịch vụ hướng nối kết
Hàm
LISTEN CONNECT SEND RECEIVE DISCONNECT

Gói tin gởi đi
Không có Yêu cầu kết nối (Connection Request) Dữ liệu (Data) Không có Yêu cầu hủy kết nối (Disconnection Request)

Ý nghĩa
Nghẽn cho đến khi tiến trình nào đó nối kết tới Chủ động yêu cầu thiết lập nối kết đến tiến trình khác Gởi thông tin đi Nghẽn cho đến khi một gói tin đến và nhận nó Muốn hủy kết nối với bên đối tác

7.1.4 Các hàm dịch vụ dạng không nối kết
Hàm
SEND RECEIVE

Gói tin gởi đi
Dữ liệu (Data) Không có

Ý nghĩa
Gởi thông tin đi Nghẽn cho đến khi một gói tin đến và nhận nó

7.2 Các yếu tố cấu thành giao thức vận chuyển
Cũng giống như giao thức ở tầng liên kết dữ liệu, giao thức vận chuyển phải đối phó với các vấn đề về điều khiển lỗi, đánh số thứ tự gói tin và điều khiển luồng dữ liệu. Tuy nhiên, giao thức trên hai tầng có nhiều điểm khác biệt quan trọng. Những khác biệt này xuất phát từ sự khác biệt của môi trường hoạt động của chúng (như được chỉ ra trong hình H7.2).

H7.2. (a) Môi trường của lớp liên kết dữ liệu. (b) Môi trường của lớp vận chuyển

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

136

Tại lớp liên kết dữ liệu, hai router giao tiếp với nhau qua một kênh truyền vật lý, trong khi tại lớp vận chuyển, kênh truyền này được thay bằng cả một mạng con. Sự khác nhau này sẽ dẫn đến nhiều hệ lụy mà những người thiết kế giao thức vận chuyển phải đau đầu giải quyết: định địa chỉ các tiến trình trên các host khác nhau như thế nào, xử lý như thế nào đối với những trường hợp mất gói tin trong quá trình trao đổi hoặc gói tin đi chậm dẫn đến mãn kỳ và gởi thêm một gói tin bị trùng lắp, đồng bộ hóa hai tiến trình đang trao đổi dữ liệu như thế nào khi mà chúng đang ở rất xa nhau.

7.2.1 Định địa chỉ
Khi một tiến trình mong muốn thiết lập nối kết với một tiến trình khác từ xa, nó phải chỉ ra rằng nó muốn kết nối với tiến trình nào. (Vận chuyển hướng không nối kết cũng gặp vấn đề tương tự: thông điệp sẽ gởi đến ai?). Một phương pháp định địa chỉ ở tầng vận chuyển của Internet là dùng số hiệu cổng (port), còn ở trong mạng ATM là AAL-SAP. Chúng ta sẽ dùng từ chung nhất để định địa chỉ tiến trình là TSAP (Transport Service Access Point). Tương tự, địa chỉ trong tầng mạng được gọi là NSAP. Hình H7.3 mô phỏng mối quan hệ giữa NSAP, TSAP và kết nối vận chuyển. Các tiến trình ứng dụng, cả client và server đều phải gắn vào một TSAP và thiết lập nối kết đến TSAP khác. Và kết nối này chạy qua cả hai TSAP. Mục tiêu của việc sử dụng các TSAP là vì trong một số mạng, mỗi máy tính chỉ có một NSAP, do đó cần phải có cách phân biệt nhiều điểm cuối mức vận chuyển khi chúng đang chia sẻ một NSAP. Ví dụ, dàn cảnh một cuộc kết nối mức vận chuyển có thể diễn ra như sau: 1. Một server phục vụ thông tin về thời gian trên host 2 gắn nó vào TSAP 1522 để chờ một cuộc gọi đến. 2. Một tiến trình ứng dụng chạy trên host 1 muốn biết giờ hiện tại, vì thế nó đưa ra một yêu cầu nối kết chỉ ra TSAP 1208 là cổng nguồn và TSAP 1522 là cổng đích. Hành động này dẫn đến một kết nối vận chuyển được thiết lập giữa hai tiến trình client và server trên hai host 1 và 2.

H 6.3. TSAP, NSAP và kết nối vận chuyển

3. Tiến trình client gởi một yêu cầu đến server để hỏi về thời gian. 4. Server trả lời thời gian hiện tại cho client. 5. Kết nối vận chuyển cuối cùng được giải phóng.

7.2.2 Thiết lập nối kết

Việc thiết lập nối kết nghe có vẻ dễ dàng, nhưng khi thực hiện có thể sẽ gặp nhiều rắc rối. Thoạt nhìn, một phiên thiết lập nối kết sẽ diễn ra như sau: một bên sẽ gởi TPDU yêu cầu nối kết (Connection Request – CR) đến bên kia, bên kia sẽ gởi một TPDU trả lời chấp nhận nối kết (Connection Accepted – CA). Vấn đề phát sinh khi mạng làm mất, tồn trữ quá lâu hay làm trùng lắp các gói tin do hai thực thể vận chuyển trao đổi qua lại với nhau. Ví dụ một tình huống như sau: tiến trình 1 gởi yêu cầu kết nối đến tiến trình 2, yêu cầu này bị các mạng con trung gian trì hoãn do tắc nghẽn. Mãn kỳ, tiến trình 1 gởi lại yêu cầu nối kết, vừa lúc đó yêu cầu nối kết bị trì hoãn cũng đến tiến trình 2. Giải thuật thiết lập nối kết phổ biến nhất là giải thuật bắt tay 3 chiều (three-way hand-shake). Xin xem các tình huống được mô phỏng trong Hình H7.4. Giả sử yêu cầu nối kết phát sinh ở host 1. Host 1 chọn một số thứ tự là x và đính kèm số đó trong TPDU CR ( CR (seq=x) ) gởi đến host 2. Host 2 báo nhận ACK ( ACK (seq = y, ACK = x) ) và thông báo số thứ tự khởi đầu của nó là y. Cuối cùng host 1 báo nhận cho host 2 nó đã biết số thứ tự khởi đầu của host 2 là y bằng TPDU dữ liệu đầu tiên gởi đến host 2 ( DATA (seq=x, ACK=y) ). Bây giờ xét đến tình huống TPDU CR bị trùng lắp. Khi TPDU CR thứ hai đến host 2, host 2 liền trả lời ACK vì tưởng rằng host 1 muốn thiết lập nối kết khác. Khi host 1 từ chối cố gắng thiết lập nối kết của host 2, host 2 hiểu rằng nó đã bị lừa bởi CR bị trùng lắp và sẽ từ bỏ nối kết đó. Trường hợp xấu nhất là cả hai TPDU CR và ACK của host 1 đều bị trùng lắp. Như trong ví dụ (b), host 2 nhận được một CR trễ và trả lời cho yêu cầu đó với số thứ tự khởi đầu y. Giả sử, không may trong trả lời cho yêu cầu CR trước đó, host 2 thông báo số thứ tự khởi đầu của nó là z. Báo nhận ở chiều thứ ba của host 1 lại bị trễ. Khi host 1 nhận được báo nhận ACK (seq=y, ACK=x), nó nhận ra rằng thông báo DATA (seq=x, ACK=z) bị trễ, do đó nó từ bỏ nối kết này.

H7.4 Khung cảnh việc bắt tay 3 chiều. (a) Hoạt động bình thường. (b) Bản CR bị trùng lắp. (c) Cả CR và ACK đều bị trùng lắp

7.2.3 Giải phóng nối kết

Việc giải phóng nối kết đơn giản hơn thiết lập nối kết. Tuy nhiên, người ta sẽ còn gặp nhiều khó khăn không ngờ tới. Bây giờ chúng ta sẽ đề nghị hai kiểu giải phóng nối kết: dị bộ và đồng bộ. Kiểu dị bộ hoạt động như sau: khi một bên cắt nối kết, kết nối sẽ bị hủy bỏ (giống như trong hệ thống điện thoại). Kiểu đồng bộ làm việc theo phương thức ngược lại: khi cả hai đồng ý hủy bỏ nối kết, nối kết mới thực sự được hủy. Giải phóng nối kết kiểu dị bộ là thô lỗ và có thể dẫn đến mất dữ liệu. Ví dụ tình huống trong Hình H7.5. Sau khi nối kết thành công, host 1 gởi một gói dữ liệu đến đúng host 2. Sau đó host 1 gởi tiếp một gói dữ liệu khác. Không may, host 2 gởi đi một yêu cầu cắt nối kết (DISCONNECT) trước khi gói dữ liệu thứ hai đến. Kết quả là kết nối được giải phóng và dữ liệu bị mất.

H7.5 Sự cắt kết nối một cách thô lỗ sẽ dẫn đến mất dữ liệu

Rõ ràng, chúng ta cần một giải pháp hữu hiệu hơn để tránh mất dữ liệu. Một giải pháp là sử dụng việc giải phóng nối kết đồng bộ, trong đó, mỗi host đều có trách nhiệm trong việc giải phóng nối kết. Một nút phải tiếp tục nhận dữ liệu sau khi đã gởi đi yêu cầu giải phóng nối kết (DISCONNECT REQUEST – CR) đến bên đối tác, cho đến khi nhận được chấp thuận hủy bỏ nối kết của bên đối tác đó. Người ta có thể hình dung giao thức như sau: đầu tiên host 1 nói: “Tôi xong rồi, anh xong chưa?”. Nếu host 2 trả lời: “Tôi cũng xong, tạm biệt” thì kết nối coi như được giải phóng an toàn. Tuy nhiên, giải pháp trên không phải lúc nào cũng chạy đúng. Có một bài toán nổi tiếng dùng để mô tả vấn đề, được gọi là bài toán “hai sứ quân” (Two army problem).

H7.6 Bài toán hai sứ quân

Có hai sứ quân đang dàn trận đánh nhau. Quân trắng dàn quân dưới thung lũng, quân xanh chia thành hai cánh quân chiếm lĩnh hai đỉnh đồi áng ngữ hai bên thung lũng đó. Chỉ huy của hai cánh quân xanh muốn thông báo và nhất trí với nhau về thời điểm cùng tấn công quân trắng. Do quân

số hai cánh quân xanh cộng lại mới đủ sức thắng quân trắng, một cánh quân xanh tấn công riêng lẻ sẽ bị quân trắng tiêu diệt. Hai cánh quân xanh muốn đồng bộ hóa cuộc tấn công của họ bằng cánh gởi các thông điệp qua lại. Nhưng những thông điệp đó phải chạy ngang qua thung lũng và có khả năng bị quân trắng phá hỏng. Câu hỏi ở đây là có giao thức nào đảm bảo sự thắng lợi của quân xanh hay không? Giả sử chỉ huy cánh quân xanh số 1 gởi thông điệp đến chỉ huy cánh quân xanh số 2: “Tôi dự định tấn công vào lúc hoàng hôn ngày 14 tháng 12 năm 2004, có được không?”. May mắn thay, chỉ huy cánh quân xanh số 2 nhận được thông điệp và trả lời “Đồng ý”. Vậy cuộc tấn công có chắc xảy ra không? Không chắc, bởi vì chỉ huy cánh quân xanh số 2 không chắc câu trả lời của anh ta đến được chỉ huy của cánh quân số 1. Bây giờ ta cải tiến giao thức thêm một bước: cho nó trở thành giao thức ba chiều: Bên cánh quân số 1 gởi bản hiệp đồng tấn công cho bên cánh quân số 2, bên cánh quân số 2 trả lời đồng ý, bên cánh quân 1 thông báo cho bên 2 nó đã biết được sự đồng ý của bên 2. Thế nhưng nếu thông báo cuối cùng của bên 1 bị mất thì sao? Bên 2 cũng sẽ không tấn công! Nếu ta cố cải tiến thành giao thức n chiều đi nữa thì việc hiệp đồng vẫn thất bại nếu thông báo cuối cùng bị mất. Ta có thể thấy mối tương đồng giữa bài toán hai sứ quân và giải pháp giải phóng nối kết. Thay vì hợp đồng tấn công, hai bên hợp đồng hủy nối kết! Giải pháp cuối cùng là hai bên sử dụng phương pháp hủy nối kết ba chiều cùng với bộ định thời: Bên phát động việc hủy nối kết sẽ bật bộ định thời cho mỗi yêu cầu giải phóng nối kết của nó, nếu yêu cầu giải phóng nối kết bị mãn kỳ mà chưa nhận được trả lời của bên đối tác, nó sẽ gởi lại yêu cầu một lần nữa. Nếu yêu cầu hủy nối kết bị mãn kỳ liên tục N lần, bên phát động sẽ tự ý hủy bỏ nối kết đó. Bên đối tác khi nhận được yêu cầu hủy nối kết từ phía phát động, sẽ trả lời chấp thuận và cũng bật bộ định thời. Nếu mãn kỳ mà trả lời chấp thuận của nó không có báo trả từ phía phát động, bên đối tác sẽ tự hủy nối kết. Hình H7.7 sẽ mô phỏng một số tình huống phát sinh trong quá trình hủy nối kết 3 chiều có sử dụng bộ định thời.

(a) Trường hợp hủy kết nối 3 chiều bình thường

(b) Khung ACK cuối cùng bị mất

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

140

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

(c) Trả lời bị mất

(d) Trả lời mất và các gói tin DR theo sau cũng bị mất

H7.7 Một số tình huống hủy nối kết theo phương pháp 3 chiều

7.2.4 Điều khiển thông lượng
Điều khiển thông lượng trong tầng vận chuyển về cơ bản là giống giao thức cửa sổ trượt trong tầng liên kết dữ liệu, nhưng kích thước cửa sổ của bên gởi và bên nhận là khác nhau. Mỗi host có thể có quá nhiều kết nối tại một thời điểm, vì thế nó không chắc là có thể đảm bảo cung cấp đủ số lượng buffer cho mỗi kết nối nhằm thực hiện đúng giao thức cửa sổ trượt. Cần phải có sơ đồ cung cấp buffer động. Trước tiên, bên gởi phải gởi đến bên nhận một yêu cầu dành riêng số lượng buffer để chứa các gói bên gởi gởi đến. Bên nhận cũng phải trả lời cho bên gởi số lượng buffer tối đa mà nó có thể cung cấp. Mỗi khi báo nhận ACK cho một gói tin có số thứ tự SEQ_NUM, bên nhận cũng phải gởi kèm theo thông báo cho bên gởi biết là lượng buffer còn lại là bao nhiêu để bên gởi không làm ngập bên nhận. Ví dụ sau sẽ mô phỏng một tình huống trao đổi thông tin giữa hai máy A và B.

A 1 2 3 4 5 6 7 8 9 10

Thông điệp <yêu cầu 8 buffers> <ack = 0, buf = 4> <seq = 0, data = m0> <seq = 1, data = m1> <seq = 2, data = m2> <ack = 1, buf = 3> <seq = 3, data = m3> <seq = 4, data = m4> <seq = 2, data = m2> <ack = 4, buf = 0>

B

Giải thích A muốn B cung cấp 8 buffers B chỉ cấp cho A 4 buffers thôi A còn lại 3 buffers A còn lại 2 buffers

…

Thông điệp bị mất, nhưng A nghĩ nó còn 1 buffer B báo nhận cho thông điệp 0 và 1, còn 3 buffers A còn lại 1 buffer A không còn buffer nào và phải dừng Thông điệp thứ 2 của A mãn kỳ và được truyền lại Mọi thứ đã được báo nhận, nhưng A vẫn nghẽn

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

141

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

11 12 13 14 15 16

<ack = 4, buf = 1> <ack = 4, buf = 2> <seq = 5, data = m5> <seq = 6, data = m6> <ack = 6, buf = 0>

A có thể gởi 1 gói tin thứ 5 B có thêm 1 buffer nữa A còn lại 1 buffer A nghẽn một lần nữa A vẫn còn nghẽn Khả năng dẫn đến deadlock

…

<ack = 6, buf = 4>

H7.8 Ví dụ một phiên giao dịch giữa hai thực thể tầng vận chuyển

Một vấn đề tiềm tàng trong sơ đồ dùng buffer động là cơ chế hoạt động của nó có thể dẫn đến deadlock. Ví dụ trong hàng 16, nếu báo nhận <ack = 6, buf = 4> của bên B bị mất, cả hai bên A và B đều rơi vào trạng thái deadlock. Để tránh tình trạng này, nên cho các host định kỳ gởi các báo nhận và trạng thái buffer lên mọi kết nối vận chuyển của chúng.

7.3 Tầng vận chuyển trong mạng Internet
Trong Internet, tầng vận chuyển được thiết kế ra với ý đồ thực hiện các nhiệm vụ sau: Đảm bảo việc phân phối thông điệp qua mạng. Phân phối các thông điệp theo thứ tự mà chúng được gởi. Không làm trùng lắp thông điệp. Hỗ trợ những thông điệp có kích thước lớn. Hỗ trợ cơ chế đồng bộ hóa. Hỗ trợ việc liên lạc của nhiều tiến trình trên mỗi host. Tầng vận chuyển trong Internet cũng hỗ trợ hai phương thức hoạt động không nối kết và có nối kết với hai giao thức liên lạc tương ứng là UDP và TCP.

7.3.1 Giao thức UDP (User Datagram Protocol)
UDP là dịch vụ truyền dữ liệu dạng không nối kết. Không có thiết lập nối kết giữa hai bên truyền nhận, do đó gói tin UDP (segment) có thể xuất hiện tại nút đích bất kỳ lúc nào. Các segment UDP tự thân chứa mọi thông tin cần thiết để có thể tự đi đến đích. Khuôn dạng của chúng như sau:
0 16 31 SrcPort Length Data DstPort Checksum

H7.9 Khuôn dạng của một segment UDP

Giải thích: SrcPort: Địa chỉ cổng nguồn, là số hiệu của tiến trình gởi gói tin đi. DstPort: Địa chỉ cổng đích, là số hiệu của tiến trình sẽ nhận gói tin. Length: Tổng chiều dài của segment, tính luôn cả phần header. Checksum: Là phần kiểm tra lỗi. UDP sẽ tính toán phần kiểm tra lỗi tổng hợp trên phần header, phần dữ liệu và cả phần header ảo. Phần header ảo chứa 3 trường trong IP header: địa chỉ IP nguồn, địa chỉ IP đích, và trường chiều dài của UDP. Phương thức tính toán như sau:

142

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0
u_short cksum(u_short *buf, int count) { register u_long sum = 0; while (count--) { sum += *buf++; if (sum & 0xFFFF0000) { /* bit carry xuất hiện, vì thế gấp và cộng dồn nó lại */ sum &= 0xFFFF; sum++; } } return ~(sum & 0xFFFF); }

Xem thông điệp là một chuỗi các số nguyên 16 bits. Cộng dồn các số nguyên này từng bit một. Kết quả cộng dồn cuối cùng chính là phần kiểm tra lỗi. Data: Phần dữ liệu hai bên gởi cho nhau. UDP hoạt động không tin cậy cho lắm, vì: Không có báo nhận dữ liệu từ trạm đích; không có cơ chế để phát hiện mất gói tin hoặc các gói tin đến không theo thứ tự; không có cơ chế tự động gởi lại những gói tin bị mất; không có cơ chế điều khiển luồng dữ liệu, và do đó có thể bên gởi sẽ làm ngập bên nhận.

7.3.2 Giao thức TCP (Transmission Control Protocol)
Ngược với giao thức UDP, TCP là giao thức vận chuyển tinh vi hơn, dùng để cung cấp dịch vụ vận chuyển tin cậy, hướng nối kết theo kiểu truyền thông tin bằng cách phân luồng các bytes. TCP là giao thức truyền hai hướng đồng thời, nghĩa là mỗi một nối kết hỗ trợ hai luồng bytes chạy theo hai hướng. Nó cũng bào gồm một cơ chế điều khiển thông lượng cho mỗi luồng bytes này, để cho phép bên nhận giới hạn lượng dữ liệu mà bên gởi có thể truyền tại một thời điểm nào đó. TCP cũng hỗ trợ cơ chế đa hợp, cho phép nhiều tiến trình trên một máy tính có thể đồng thời thực hiện đối thoại với đối tác của chúng.

7.3.2.1

Hai đầu mút truyền dữ liệu với nhau như thế nào?

TCP là giao thức hướng byte, nghĩa là bên gởi ghi các bytes lên nối kết TCP, bên nhận đọc các bytes từ nối kết TCP đó. Mặc dù TCP mô tả dịch vụ mà nó cung cấp cho tầng ứng dụng là theo kiểu “luồng các bytes”, nhưng tự thân TCP không truyền từng byte một qua mạng Internet. Thay vào đó, thực thể TCP trên máy nguồn trữ tạm đủ số bytes phát ra từ tiến trình gởi để tạo nên một gói tin có kích thước hợp lý rồi mới gởi gói tin đó đến thực thể TCP ngang hàng bên máy đích. Thực thể TCP bên máy đích sẽ bóc các bytes dữ liệu trong gói tin ra và đặt chúng vào buffer của nó. Tiến trình bên nhận từ đó có thể đọc các bytes từ buffer này tùy thích. Quá trình truyền nhận trên được mô phỏng trong Hình H7.10.

H7.10. Cách thức TCP quản lý luồng các bytes

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

143

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

7.3.2.2

Khuôn dạng TCP Segment

Các gói tin được trao đổi bởi hai thực thể TCP trong Hình H7.10 được gọi là các segment (đoạn), do mỗi gói tin mang theo một đoạn của cả một luồng các bytes. Mỗi segment có một header như được chỉ ra trong Hình H7.11.

H.11 Khuôn dạng TCP header

Giải thích: Các trường SrcPort và DstPort chỉ ra địa chỉ cổng nguồn và đích, giống như trong UDP. Hai trường này cùng với hai địa chỉ IP nguồn và đích sẽ được kết hợp với nhau để định danh duy nhất một kết nối TCP. Nghĩa là một kết nối TCP sẽ được định danh bởi một bộ 4 trường
(Cổng nguồn, Địa chỉ IP nguồn, Cổng đích, Địa chỉ IP đích)

Các trường Acknowledgement, SequenceNum và AdvertisedWindow tất cả được sử dụng trong giải thuật cửa sổ trượt của TCP. Bởi vì TCP là giao thức hướng byte, nên mỗi byte của dữ liệu sẽ có một số thứ tự; trường SequenceNum chứa số thứ tự của byte đầu tiên của một dãy các bytes chứa trong một segment. Các trường Acknowledgement và AdvertisedWindow được dùng để thông báo tiến độ nhận các bytes trong luồng dữ liệu và khả năng tiếp nhận chúng. Để đơn giản hóa vấn đề, chúng ta bỏ qua sự thật là dữ liệu có thể chạy theo hai chiều, ở đây ta đưa ra sơ đồ như sau: bên gởi sẽ gởi một segment dữ liệu, byte dữ liệu đầu tiên trong segment đó sẽ có số thứ tự là SequenceNum; bên nhận sẽ báo nhận bằng các trường Acknowledgement và AdvertisedWindow.

H7.12 Gởi dữ liệu và báo nhận

Cách thức hai bên sử dụng các trường trên như thế nào sẽ được trình bày trong phần điều khiển luồng dữ liệu. Trường Flags dài 6 bits được sử dụng để chứa thông tin điều khiển giữa hai bên sử dụng giao thức TCP. Một bit trong trường này là một cờ, cụ thể như sau: SYN, FIN, RESET, PUSH, URG, ACK. Hai cờ SYN và FIN được dùng để thiết lập và giải phóng nối kết. Cờ ACK được đặt mỗi khi trường Acknowledgement là hợp lệ. Cờ URG được dùng để đánh dấu segment này chứa dữ liệu khẩn cấp. Khi cờ này được đặt, trường UrgPtr sẽ chỉ ra nơi bắt đầu của dữ liệu không khẩn cấp (dữ liệu khẩn cấp luôn nằm ở đầu của phần dữ liệu).

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

144

Cờ PUSH báo hiệu cho bên nhận rằng bên gởi đã dùng thao tác PUSH, tức là bên gởi đã không chờ nhận đủ các bytes để lấp đầy một segment, trong buffer gởi dù có bao nhiêu bytes dữ liệu cũng được bên gởi đóng vào segment và gởi đi. Cuối cùng, cờ RESET được dùng để thông báo rằng bên nhận đã bị rối (ví dụ như nó đã nhận một segment mà đáng lẽ ra không phải là segment đó), vì thế nó muốn hủy bỏ nối kết. Trường Checksum được sử dụng chính xác giống như trong giao thức UDP. Do header của TCP có độ dài thay đổi, nên trường HdrLen sẽ chỉ ra độ dài cụ thể của phần header này.

7.3.2.3

Bắt tay trong TCP

TCP sử dụng giao thức bắt tay 3 chiều. Bước 1: Cient (bên chủ động) gởi đến server một segment yêu cầu nối kết, trong đó chứa số thứ tự khởi đầu mà nó sẽ dùng (Flags = SYN, SequenceNum = x). Bước 2: Server trả lời cho client bằng một segment, trong đó báo nhận rằng nó sẵn sàng nhận các byte dữ liệu bắt đầu từ số thứ tự x+1 (Flags = ACK, Ack = x + 1) và cũng báo rằng số thứ tự khởi đầu của bên server là y (Flags = SYN, SequenceNum = y). Bước 3: Cuối cùng client báo cho server biết, nó đã biết số thứ tự khởi đầu của server là y (Flags = ACK, Ack = y+1).

H7.12 Bắt tay 3 chiều trong TCP

7.3.2.4

Hủy bắt tay trong TCP

Việc hủy bắt tay trong TCP được thực hiện qua 4 bước: Bước 1: Cient (bên chủ động) gởi đến server một segment yêu cầu hủy nối kết (Flags = FIN). Bước 2: Server nhận được một segment FIN, sẽ trả lời bằng một segment ACK. Sau khi đã hoàn tất hết mọi thứ để đóng nối kết, server sẽ gởi cho client tiếp một segment FIN. Bước 3: Client nhận được FIN sẽ trả lời ACK sau đó nó sẽ chuyển sang trạng thái chờ đợi có định hạn. Trong thời gian chờ đợi này, client sẽ trả lời ACK cho mọi khung FIN. Hết thời gian chờ đợi, client sẽ thật sự đóng nối kết. Bước 4: Server khi nhận được ACK sẽ thật sự đóng nối kết.

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

H7.13 Hủy nối kết trong TCP

7.3.2.5

Điều khiển thông lượng trong TCP

TCP dùng phương pháp điều khiển thông lượng “cửa sổ trượt với kích thước cửa sổ động”. Nhắc lại rằng TCP là giao thức hướng bytes. Ta có thể tưởng tượng hình ảnh sau: tiến trình bên gởi ghi ra một luồng các bytes, tiến trình bên nhận đọc vào một luồng các bytes.

H7.14 Truyền nhận theo luồng bytes

Như đã nói, TCP không truyền nhận dữ liệu cho ứng dụng từng byte một mà nó trữ tạm các bytes trong buffer đến khi đủ đóng gói thành một segment thì mới truyền đi.

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

146

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

H7.15 Các luồng bytes được phân đoạn như thế nào

Byte đầu tiên của mỗi luồng bytes sẽ được đánh số bằng “số thứ tự khởi đầu”, và số này được dàn xếp trong giai đoạn bắt tay 3 chiều. Trường SequenceNum trong TCP segment chứa số thứ tự của byte đầu tiên nằm trong segment đó. Cũng như trong giao thức cửa sổ trượt, khi bên nhận nhận được n bytes trong một segment, bắt đầu từ byte thứ SequenceNum, nó sẽ báo nhận tốt n bytes này và chờ nhận tiếp từ byte thứ Acknowledgement (Acknowledgement = SequenceNum + n).

H7.16 Ví dụ về điều khiển thông lượng trong TCP

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

147

Do kích thước cửa sổ là động, nên trong mỗi khung báo nhận của mình, bên nhận đính kèm theo thông báo về kích thước cửa sổ sẵn dùng của nó (lượng buffer còn trống), đó chính là trường AdvertisedWindow trong TCP segment. Lần sau, bên gởi sẽ không được gởi lượng bytes vượt quá AdvertisedWindow. Trong ví dụ trên, lúc đầu bên nhận có kích thước buffer là 4 KB. Bên gởi đặt số thứ tự khởi đầu là 0, sau đó truyền 2 KB. Buffer bên nhận còn lại 2 KB rỗng, do đó nó báo nhận “Acknowledgement = 2048, AdvertisedWindow = 2048”. Bên gởi gởi tiếp 2 KB, khi đó buffer bên nhận bị đầy, nó liền báo nhận “Acknowledgement = 4096, AdvertisedWindow = 0”. Không còn buffer nhận, nên bên gởi sẽ tạm thời bị nghẽn. Sau khi bên nhận xử lý xong 2 KB, nó liền báo “Acknowledgement = 4096, AdvertisedWindow = 2048”. Lúc này bên gởi có thể gởi tiếp tối đa là 2 KB, nhưng nó chỉ còn 1 KB dữ liệu để gởi mà thôi.

Chương 8: CÁC ỨNG DỤNG MẠNG

Chương này sẽ tìm hiểu một số ứng dụng mạng phổ biến hiện nay, chủ yếu tập trung vào giao thức hoạt động của chúng. Ví dụ đầu tiên được xem xét là dịch vụ tên phân tán, dịch vụ đầu tiên được cài đặt trong một mạng máy tính. Về thực chất dịch vụ tên là cái mà các ứng dụng khác phải phụ thuộc vào. Một server phục vụ tên thường được sử dụng bởi các ứng dụng khác hơn là bởi con người. Sau đó, các ứng dụng mạng truyền thống và phổ biến sẽ được giới thiệu, bao gồm các dịch vụ MAIL, WEB và FTP. Cũng cần nói trước rằng, những dịch vụ mạng vừa nói sẽ dựa trên hai giao thức vận chuyển đã được đề cập trong chương 6 là TCP và UDP.

8.1 Dịch vụ tên (DNS)

Cho đến bây giờ, chúng ta vẫn dùng địa chỉ để định danh các host. Trong khi rất thuận tiện cho việc xử lý của các router, các địa chỉ số không thân thiện với người dùng lắm. Vì lý do này, các host thường được gán cho một cái tên thân thiện và dịch vụ tên được sử dụng để ánh xạ từ cái tên thân thiện với người dùng này sang địa chỉ số vốn rất thân thiện với các router. Dịch vụ như vậy thường là ứng dụng đầu tiên được cài đặt trong một mạng máy tính do nó cho phép các ứng dụng khác tự do định danh các host bằng tên thay vì bằng địa chỉ. Dịch vụ tên thường được gọi là phần trung gian (middleware) vì nó lấp đầy khoảng cách giữa các ứng dụng khác và lớp mạng phía dưới. Tên host và địa chỉ host khác nhau ở hai điểm quan trọng. Thứ nhất, tên host thường có độ dài thay đổi và dễ gợi nhớ, vì thế nó giúp người dùng dễ nhớ hơn. Thứ hai, tên thường không chứa thông tin gì để giúp mạng định vị (chuyển các gói tin đến) host. Địa chỉ, ngược lại, lại hàm chứa thông tin vạch đường trong đó. Trước khi đi vào chi tiết cách thức đặt tên cho các host trong mạng như thế nào, chúng ta đi định nghĩa một số thuật ngữ trước: Không gian tên (name space) định nghĩa tập các tên có thể có. Một không gian tên có thể là phẳng (flat) – một tên không thể được chia thành các thành phần nhỏ hơn, hoặc phân cấp. Hệ thống tên duy trì một tập các ánh xạ (collection of bindings) từ tên sang giá trị. Giá trị có thể là bất cứ thứ gì chúng ta muốn hệ thống tên trả về khi ta cấp cho nó một tên để ánh xạ; trong nhiều trường hợp giá trị chính là địa chỉ host. Một cơ chế phân giải (resolution mechanism) là một thủ tục mà khi được gọi với tham số là một tên, sẽ trả về một giá trị tương ứng. Một server tên (name server) là một kết quả cài đặt cụ thể của một cơ chế phân giải luôn sẵn dùng trên mạng và có thể được truy vấn bằng cách gởi đến nó một thông điệp. Mạng Internet đã có sẵn một hệ thống đặt tên được phát triển tốt, gọi là hệ thống tên miền (domain name system – DNS). Vì thế chúng ta sẽ dùng DNS làm cơ sở để thảo luận về vấn đề đặt tên cho các host. Khi người dùng đưa một tên host đến một ứng dụng (có thể tên host đó là một phần của một tên hỗn hợp như địa chỉ email chẳng hạn), ứng dụng này sẽ liên hệ với hệ thống tên để dịch tên host sang địa chỉ host. Sau đó ứng dụng liền tạo một nối kết đến host đó thông qua giao thức TCP chẳng hạn. Hiện trạng được mô tả trong hình H8.1.

H8.1 Tên máy được dịch sang địa chỉ, các số từ 1-5 thể hiện trình tự các bước xử lý

8.1.1 Miền phân cấp
DNS cài đặt không gian tên phân cấp dùng cho các đối tượng trên Internet. Các tên DNS được xử lý từ phải sang trái, sử dụng các dấu chấm (.) làm ký tự ngăn cách. (Mặc dù các tên DNS được xử lý từ phải qua trái, người dùng thường đọc chúng từ trái sang phải). Ví dụ tên miền của một host là mail.cit.ctu.edu.vn. Chú ý rằng các tên miền được sử dụng để đặt tên các đối tượng trên Internet, không phải chỉ được dùng để đặt tên máy. Ta có thể mường tượng cấu trúc phân cấp của DNS giống như hình dáng cây. Hình H8.2 là một ví dụ.

H8.2 Cây phân cấp tên miền

Có thể thấy rằng, cây phân cấp không quá rộng ở mức đầu tiên. Mỗi quốc gia có một tên miền, ngoài ra còn có 6 miền lớn khác gồm: edu, com, gov, mil, org và net. Sáu miền lớn này nằm ở Mỹ. Những tên miền không chỉ ra tên nước một cách tường minh thì mặc nhiên là nằm ở Mỹ.

8.1.2 Các server phục vụ tên
Một cấu trúc tên miền phân cấp hoàn chỉnh chỉ tồn tại trong ý niệm. Vậy thì trong thực tế cấu trúc phân cấp này được cài đặt như thế nào? Bước đầu tiên là chia cấu trúc này thành các cây con gọi là các vùng (zone). Ví dụ, hình H8.3 chỉ ra cách thức cấu trúc phân cấp trong hình H8.2 được chia thành các vùng như thế nào.

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

H8.3 Cấu trúc miền phân cấp được chia thành các vùng

Mỗi một vùng có thể được xem là đơn vị quản lý một bộ phận của toàn hệ thống phân cấp. Ví dụ, vùng cao nhất của hệ thống phân cấp được quản lý bởi NIC (Network Information Center), vùng ctu được quản lý bởi Trường Đại Học Cần Thơ. Một vùng luôn có mối liên hệ đến các đơn vị cài đặt cơ bản trong DNS - các server tên. Thông tin chứa trong một vùng được thiết lập tại hai hoặc nhiều server tên. Mỗi server tên có thể truy xuất được qua mạng Internet. Client gởi yêu cầu đến server tên, server tên sẽ trả lời cho yêu cầu đó. Câu trả lời đôi khi chứa thông tin cuối cùng mà client cần, đôi khi lại chứa chỉ điểm đến một server tên khác mà client nên gởi câu hỏi đến đó. Vì thế, theo cách nhìn thiên về cài đặt, người ta có thể nghĩ về DNS được cài đặt bằng cấu trúc phân cấp các server tên hơn là bằng cấu trúc phân cấp các miền.

H8.4 Cấu trúc phân cấp của các server tên Để ý rằng mỗi vùng được cài đặt trong hai hoặc nhiều server tên với lý do dự phòng; nghĩa là nếu một server bị chết sẽ còn các server khác thay thế. Mặt khác, một server tên cũng có thể được dùng để cài đặt nhiều hơn một vùng. Mỗi server tên quản lý thông tin về một vùng dưới dạng một tập các mẫu tin tài nguyên (resource record). Mỗi mẫu tin tài nguyên là một ánh xạ từ tên sang giá trị (name to value binding), cụ thể hơn là một mẫu tin gồm 5 trường:
(Tên, Giá trị, Kiểu, Lớp, TTL)

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

151

Các trường Tên và Giá trị là những gì chúng ta muốn có, ngoài tra trường Kiểu chỉ ra cách thức mà Giá trị được thông dịch. Chẳng hạn, trường Kiểu = A chỉ ra rằng Giá trị là một địa chỉ IP. Vì thế các mẫu tin kiểu A sẽ cài đặt kiểu ánh xạ từ tên miền sang địa chỉ IP. Ví dụ như mẫu tin:
(ns.ctu.edu.vn, 203.162.41.166, A, IN)

chỉ ra rằng địa chỉ IP của host có tên ns.ctu.edu.vn là 203.162.41.166. Ngoài ra còn có những kiểu khác: NS: Trường Giá trị chỉ ra tên miền của máy tính đang chạy dịch vụ tên, và dịch vụ đó có khả năng thông dịch các tên trong một miền cụ thể. Ví dụ mẫu tin:
(ctu.edu.vn, ns.ctu.edu.vn, NS, IN)

chỉ ra rằng server tên của miền ctu.edu.vn có tên là ns.ctu.edu.vn. CNAME: Trường Giá trị chỉ ra một cái tên giả của một host nào đó. Kiểu này được dùng để đặt thêm bí danh cho các host trong miền. MX: Trường Giá trị chỉ ra tên miền của host đang chạy chương trình mail server mà server đó có khả năng tiếp nhận những thông điệp thuộc một miền cụ thể. Ví dụ mẫu tin
(ctu.edu.vn, mail.ctu.edu.vn, MX, IN)

chỉ ra rằng host có tên mail.ctu.edu.vn là mail server của miền ctu.edu.vn. Trường Lớp được sử dụng nhằm cho phép thêm vào những thực thể mạng không do NIC quản lý. Ngày nay, lớp được sử dụng rộng rãi nhất là loại được Internet sử dụng; nó được ký hiệu là IN. Cuối cùng trường TTL chỉ ra mẫu tin tài nguyên này sẽ hợp lệ trong bao lâu. Trường này được sử dụng bởi những server đang trữ tạm các mẫu tin của server khác; khi trường TTL hết hạn, các mẫu tin chứa trường TTL hết hạn đó sẽ bị các server xóa khỏi cache của mình. Để hiểu rõ hơn cách thức các mẫu tin tài nguyên được thể hiện trong cấu trúc phân cấp, hãy xem ví dụ được vẽ trong hình H8.3. Để đơn giản hóa vấn đề, chúng ta bỏ qua trường TTL và cung cấp thông tin tương ứng cho một server tên làm nhiệm vụ quản lý cho một vùng. Đầu tiên, server tên gốc (root name server) sẽ chứa một mẫu tin NS cho mỗi server cấp hai. Nó cũng chứa một mẫu tin A để thông dịch từ một tên server cấp hai sang địa chỉ IP của nó. Khi được ghép với nhau, hai mẫu tin này cài đặt một cách hiệu quả một con trỏ từ server gốc đến mỗi server cấp hai của nó.
(edu.vn, dns1.vnnic.net.vn, NS, IN);thông tin về miền con edu.vn lưu ở máy dns1.vnnic.net.vn (dns1.vnnic.net.vn, 203.162.57.105, A, IN);máy dns1.vnnic.net.vn có địa chỉ 203.162.57.105 (cisco.com, ns1.cisco.com, NS, IN)

Kế tiếp, miền edu.vn có một server tên hiện hữu tại máy dns1.vnnic.net.vn và server này lại chứa các mẫu tin sau: (ctu.edu.vn, ns.ctu.edu.vn, NS, IN) (ns.ctu.edu.vn, 203.162.41.166, A, IN)

Cuối cùng server ns.ctu.edu.vn lại chứa thông tin về các máy tính của trường Đại Học Cần Thơ cũng như các miền con của Trường Đại Học Cần Thơ (cit.ctu.edu.vn, ns.cit.ctu.edu.vn, NS, IN) (ns.cit.ctu.edu.vn, 203.162.36.144, A, IN) (ctu.edu.vn, mail.ctu.edu.vn, MX, IN) (mail.ctu.edu.vn, 203.162.139.21, A, IN) (www.ctu.edu.vn, mail.ctu.edu.vn, CNAME, IN)

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

152

Chú ý rằng trên lý thuyết các mẫu tin có thể được dùng để định nghĩa bất kỳ kiểu đối tượng nào, DNS lại thường được sử dụng để định danh các host và site. DNS không được dùng để định danh cá nhân con người hoặc các đối tượng khác như tập tin hay thư mục, việc định danh này được thực hiện trong các hệ thống phục vụ tên khác. Ví dụ X.500 là hệ thống định danh của ISO được dùng để định danh con người bằng cách cung cấp thông tin về tên, chức vụ, số điện thoại, địa chỉ, và vân vân. X.500 đã chứng tỏ là quá phức tạp nên không được hỗ trợ bởi các search engine nổi tiếng hiện nay. Tuy nhiên nó lại là nguồn gốc phát sinh ra chuẩn LDAP (Lightweight Directory Access Protocol). LDAP vốn là thành phần con của X.500 được thiết kế để làm phần front-end cho X.500. Ngày nay LDAP đang trở nên phổ biến nhất là ở cấp độ công ty, tổ chức lớn, đóng vai trò là hệ thống học và quản lý thông tin về người dùng của nó.

8.1.3 Phương pháp phân tích tên

Với một hệ thống phân cấp các server tên đã trình bày, bây giờ chúng ta đi tìm hiểu cách thức một khách hàng giao tiếp với các server này để phân tích cho được một tên miền thành địa chỉ. Giả sử một khách hàng muốn phân tích tên miền www.ctu.edu.vn, đầu tiên khách hàng này sẽ gởi yêu cầu chứa tên này đến server tên gốc. Server gốc không thể so khớp tên theo yêu cầu với các tên mà nó chứa, liền trả lời cho khách hàng một mẫu tin kiểu NS chứa edu.vn. Server gốc cũng trả về tất cả các mẫu tin có liên quan đến mẫu tin NS vừa nói, trong đó có mẫu tin kiểu A chứa địa chỉ của dns1.vnnic.vnn.vn. Khách hàng chưa có thông tin cuối cùng mà nó muốn, tiếp tục gởi yêu cầu đến server tên tại địa chỉ 203.162.57.105. Server tên thứ hai này lại không thể so khớp tên theo yêu cầu với các tên mà nó chứa, tiếp tục trả lời cho khách hàng một mẫu tin loại NS chứa tên ctu.edu.vn cùng với mẫu tin kiểu A tương ứng với tên server là ns.ctu.edu.vn. Khách hàng lại tiếp tục gởi yêu cầu đến server tên tại địa chỉ 203.162.41.166 và lần này nhận được câu trả lời cuối cùng có kiểu A cho tên www.ctu.edu.vn. Ví dụ trên chắc chắn sẽ để lại nhiều câu hỏi về quá trình phân giải tên. Câu hỏi thường được đặt ra là: Lúc khởi đầu, làm sao khách hàng có thể định vị được server gốc? Đây là bài toán cơ bản đặt ra cho mọi hệ thống phục vụ tên và câu trả lời là: hệ thống phải tự thân vận động để có được thông tin về các server gốc! Trong tình huống của hệ thống DNS, ánh xạ từ tên sang địa chỉ của một hay nhiều server gốc được phổ biến cho mọi người, nghĩa là ánh xạ đó được loan báo thông qua các phương tiện truyền thông khác nằm ngoài hệ thống tên. Tuy nhiên, trong thực tế không phải tất cả khách hàng đều biết về các server gốc. Thay vào đó, chương trình khách hàng chạy trên mỗi host trong Internet được khởi động với các địa chỉ lấy từ server tên cục bộ. Ví dụ, tất cả các host trong Khoa Công Nghệ Thông Tin của Trường Đại Học Cần Thơ đều biết server tên nội bộ đang chạy trên máy ns.cit.ctu.edu.vn. Đến lượt server tên cục bộ này lại chứa các mẫu tin tài nguyên cho một hoặc nhiều server gốc của nó, ví dụ:

( . , a.root-servers.net, NS, IN) (a.root-server.net, 198.41.0.4, A, IN)

Trong ví dụ trên, server tên cục bộ có thông tin về một server tên gốc của nó (chú ý miền gốc được ký hiệu bằng dấu chấm) là a.root-servers.net, địa chỉ IP tương ứng của server gốc này là 198.41.0.4. Từ đó, việc phân giải một tên miền bắt đầu từ câu truy vấn của khách hàng đến server cục bộ. Nếu server cục bộ không có sẵn câu trả lời, nó sẽ gởi câu

hỏi đến server từ xa dùm cho khách hàng. Chuỗi hành động trên có thể được mô tả trong hình H8.5

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

153

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

H8.5 Quá trình phân giải tên trong thực tế, các số 1 đến 8 chỉ ra trình tự thực hiện

8.2 Electronic Mail (SMTP, MIME, POP3, IMAP)
Email là một trong những ứng dụng mạng lâu đời nhất nhưng lại phổ dụng nhất. Thử nghĩ khi bạn muốn gởi thông điệp đến một người bạn ở đầu kia của thế giới, bạn muốn mang thư chạy bộ qua đó hay chỉ đơn giản lên máy tính gõ ít hàng và nhấn nút Send? Thật ra, những bậc tiền bối của mạng ARPANET đã không tiên đoán được email sẽ là ứng dụng then chốt chạy trên mạng này, mục tiêu chính của họ là thiết kế hệ thống cho phép truy cập tài nguyên từ xa. Hệ thống email ra đời không mấy nổi bật, để bây giờ lại được sử dụng hằng ngày bởi hàng triệu người trên thế giới. Mục tiêu của phần này là chỉ ra những nhân vật hoạt động trong hệ thống email, vai trò của họ, giao thức mà họ sử dụng và khuôn dạng thông điệp mà họ trao đổi với nhau.

8.2.1 Các thành phần của hệ thống email
Một hệ thống email thường có 3 thành phần chính: Bộ phận trợ giúp người dùng (User Agent), Mail Server và các giao thức mà các thành phần này dùng để giao tiếp với nhau. Người ta phân loại các giao thức như sau: Giao thức giữa các mail servers bao gồm: o SMTP (Simple Mail Transfer Protocol): được các server dùng để chuyển thư qua lại với nhau. Ví dụ nôm na, nó giống như cách thức mà các trạm bưu điện dùng để chuyển các thùng thư của khách hàng cho nhau. Thông tin chi tiết về giao thức này được mô tả trong tài liệu RFC 822. Giao thức giữa mail server và user agent bao gồm: o POP3 (Post Offic Protocol version 3 [RFC 1939]): được user agent sử dụng để lấy thư về từ hộp thư của nó trên server. o SMTP: được user agent sử dụng để gởi thư ra server. o IMAP: (Internet Mail Access Protocol [RFC 1730]): Có nhiều tính năng vượt trội hơn POP3. Ngoài ra IMAP còn cho phép gởi mail.

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

154

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

H8.6 Các thành phần của hệ thống email

8.2.2 Khuôn dạng của một email
RFC 822 định nghĩa một email gồm có hai phần: phần tiêu đề (header) và phần thân (body).

H8.7Khuôn dạng của email

Cả hai phần đều được thể hiện dưới dạng ký tự ASCII. Lúc đầu, phần thân được qui định có khuôn dạng văn bản đơn giản. Sau này người ta đề nghị một chuẩn mới gọi là MIME, có thể cho phép phần thân của email chứa bất kỳ loại dữ liệu nào. Phần tiêu đề bao gồm nhiều dòng thông tin, mỗi dòng kết thúc bằng hai ký tự <CRLF>. Phần tiêu đề được chia khỏi phần thân bởi một hàng rỗng. Mỗi một hàng tiêu đề chứa một cặp “tên” và “giá trị”, cách nhau bởi dấu hai chấm (:). Người dùng có thể rất quen với nhiều hàng tiêu đề vì họ thường phải điền thông tin vào đấy. Ví dụ Tên
From: To: Subject: Date:

Giá trị Địa chỉ người gởi Địa chỉ của người nhận Chủ đề thư Ngày gởi

RFC 822 được mở rộng năm 1993 (và được cập nhật lại năm 1996) để cho phép email mang được nhiều loại dữ liệu: audio, video, hình ảnh, tài liệu Word, … MIME (Multipurpose Internet Mail Extensions) về cơ bản có ba phần. Phần đầu tiên là tập các dòng header dùng để bổ túc cho phần header cũ của RFC 822. Theo nhiều cách, những dòng header này mô tả dữ liệu chứa trong phần thân. Cụ thể như sau:
Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

155

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

Tên
MIME-Version: Content-Description: Content-Type: Content-Transfer-Encoding:

Giá trị Phiên bản MIME đang sử dụng Mô tả trong thư đang có dữ liệu gì Mô tả kiểu dữ liệu đang nằm trong thư Mô tả cách thức mã hóa dữ liệu trong thư

Phần thứ hai là các định nghĩa cho một tập các kiểu nội dung (và kiểu con nếu có). Ví dụ một số kiểu mà MIME định nghĩa: Kiểu
image/gif image/jpeg text/plain text/richtext application

Ý nghĩa Ảnh dạng gif Ảnh dạng jpeg Văn bản đơn giản Văn bản mở rộng (có đặt font chữ, được định dạng đậm, nghiêng hoặc gạch dưới …) Dữ liệu trong thư được xuất ra từ một ứng dụng nào đó. Chẳng hạn: application/postscript: tài liệu Postscript ( .ps)
application/msword: tài liệu Microsoft Word (.doc)

MIME cũng định nghĩa kiểu multipart để chỉ ra cách mà phần thân của thư mang nhiều loại dữ liệu khác nhau như thế nào. Chỉ có một kiểu con của multipart là mixed với ý nói rằng trong phần thân của thư có nhiều mảnh dữ liệu khác nhau, độc lập với nhau và được sắp xếp theo một trình tự cụ thể. Mỗi mảnh dữ liệu sẽ có phần tiêu đề riêng để mô tả kiểu dữ liệu của mảnh đó. Phần thứ ba mô tả cách thức mã hóa các kiểu dữ liệu nói trên để có thể truyền chúng dưới dạng ASCII. Lý do để mọi bức thư phải chứa các ký tự ASCII là vì để đi được đến đích, bức thư đó có thể phải trung chuyển qua nhiều gateway, mà các gateway này đều coi mọi bức thư dưới dạng ASCII. Nếu trong thư chứa bất kỳ ký tự nào khác ASCII thì thư sẽ bị đứt gãy nội dung. MIME sử dụng phương pháp mã hóa trực tiếp dữ liệu nhị phân thành các ký tự nhị phân, gọi là base64. Ý tưởng của base64 là ánh xạ 3 bytes dữ liệu nhị phân nguyên thủy thành 4 ký tự ASCII. Giải thuật đơn giản như sau: tập hợp 3 bytes dữ liệu nhị phân lại thành 24 bits, sau đó chia 24 bits này thành 4 cụm, một cụm 6 bits. Một cụm 6 bits được ánh xạ vào một trong 64 ký tự ASCII hợp lệ; ví dụ 0 ánh xạ thành A, 1 ánh xạ thành B… Nếu nhìn vào bức thư đã được mã hóa dạng base64, người dùng sẽ thấy chỉ có 52 chữ cái cả hoa lẫn thường, 10 chữ số từ 0 đến 9 và các ký tự đặc biệt + và /. Đối với những người dùng chỉ sử dụng trình đọc thư hỗ trợ duy nhất kiểu ký tự thì việc đọc những bức thư có kiểu base64 sẽ rất là đau khổ. Vì lý do nhân đạo, MIME còn hỗ trợ kiểu mã hóa ký tự thường được gọi là 7-bit. 7-bit sẽ giữ nguyên dạng ký tự mà người ta nhập vào. Tổng hợp lại, ví dụ một bức thư có 2 loại dữ liệu: văn bản thường, một ảnh JPEG, sẽ có hình dáng như sau:

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

156

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

From: ptphi@cit.ctu.edu.vn To: TH27@cit.ctu.edu.vn Subject: Picture of students. MIME-Version: 1.0 Content-Type: multipart/mixed; boundary="—98766789" --98766789 Content-Transfer-Encoding: 7bit Content-Type: text/plain Hi, Please find a picture of you. --98766789 Content-Transfer-Encoding: base64 Content-Type: image/jpeg base64 encoded data ..... ..... .....base64 encoded data --98766789--

8.2.3 Chuyển thư

Kế đến, chúng ta sẽ xem xét giao thức SMTP – giao thức được dùng để chuyển thư từ máy này đến máy kia. Để đặt SMTP vào đúng ngữ cảnh, chúng ta nên nhắc lại các nhân vật then chốt trong hệ thống email. Đầu tiên, người dùng tương tác với trình đọc thư (hay còn gọi là user agent) để soạn, lưu, tìm kiếm và đọc thư của họ. Hiện trên thị trường có nhiều phần mềm đọc thư, cũng giống như hiện cũng đang có nhiều loại trình duyệt Web vậy. Thứ hai, có trình xử lý thư (hay còn gọi là mail server) chạy trên một máy nào đó trong mạng nội bộ của người dùng. Có thể xem mail server như một bưu điện: Người dùng trao cho mail server các bức thư mà họ muốn gởi cho người dùng khác, mail server sử dụng giao thức SMTP trên TCP để chuyển bức các thư này đến mail server bên đích. Mail server bên đích nhận các thư đến và đặt chúng vào hộp thư của người dùng bên đích. Do SMTP là giao thức mà rất nhiều người có thể tự cài đặt, vì thế sẽ có rất nhiều sản phẩm mail server hiện có trên thị trường. Sản phẩm mail server thường được sử dụng nhất là sendmail, ban đầu được cài đặt trong hệ điều hành Berkeley Unix. Tất nhiên mail server bên máy gởi có thể kết nối SMTP/TCP trực tiếp tới mail server bên máy nhận, nhưng trong thực tế, một bức thư có thể đi ngang qua vài mail gateways trước khi đến đích. Cũng giống như máy đích, mỗi mail gateway cũng chạy một mail server. Không phải ngẫu nhiên mà các nút chuyển thư trung gian được gọi là mail gateway. Công việc của chúng cũng giống như các IP gateway là lưu tạm và chuyển phát tiếp các bức thư của người dùng. Điểm khác nhau duy nhất giữa chúng là, mail gateway trữ tạm các bức thư trong đĩa, trong khi các IP gateway trữ tạm các gói tin IP trong bộ nhớ. Bạn có thể đặt câu hỏi: tại sao lại cần đến các mail gateways? Tại sao không dùng phương pháp nối kết SMTP/TCP trực tiếp từ bên gởi sang bên nhận? Lý do thứ nhất, người gởi không muốn kèm trong thư địa chỉ của máy đích. Ví dụ, riêng việc nhập vào trong thư địa chỉ đích ptphi@cit.ctu.edu.vn đã mất công rồi, không ai thấy thoải mái khi phải nhập thêm địa chỉ máy đích là machine-of-phi.cit.ctu.edu.vn. Thứ hai, không chắc lúc bên gởi thiết lập nối kết đến bên nhận, người dùng bên nhận đã bật sẵn máy! Thành thử chỉ cần địa chỉ thư bên nhận là đủ. Khi bức thư đến được mail gateway của Khoa Công Nghệ Thông Tin – Đại học Cần Thơ, nếu người dùng ptphi đang mở máy, mail gateway sẽ chuyển thư cho anh ta ngay, nếu không mail gateway sẽ trữ tạm thư trên đĩa của nó đến khi ptphi bật máy lên và kiểm tra thư.

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

157

Dù có bao nhiêu mail gateways trung gian trên đường đến đích vẫn không đáng lo lắng, bởi vì mỗi mail gateway trung gian sẽ nỗ lực sử dụng một kết nối SMTP độc lập đến gateway kế tiếp trên đường đi nhằm chuyển thư càng ngày càng đến gần người nhận. SMTP là một giao thức đơn giản dùng các ký tự ASCII. Sau khi thiết lập nối kết TCP đến cổng 25 của máy đích (được coi là server), máy nguồn (được coi là client) chờ nhận kết quả trả về từ server. Server khởi đầu cuộc đối thoại bằng cách gởi một dòng văn bản đến client thông báo danh tính của nó và khả năng tiếp nhận thư. Nếu server không có khả năng nhận thư tại thời điểm hiện tại, client sẽ hủy bỏ nối kết và thử thiết lập lại nối kết sau. Nếu server sẵn sàng nhận thư, client sẽ thông báo lá thư đó từ đâu đến và ai sẽ là người nhận. Nếu người nhận đó tồn tại, server sẽ thông báo cho client tiếp tục gởi thư. Sau đó client gởi thư và server báo nhận cho thư đó. Sau khi cả hai bên hoàn tất phiên truyền nhận, kết nối sẽ được đóng lại. Ví dụ một phiên truyền nhận được cho ngay dưới đây. Những dòng bắt đầu bằng C: là của phía client gởi đi; bằng S: là các câu trả lời của server. S: 220 ctu.edu.vn C: HELO cit.ctu.edu.vn S: 250 ctu.edu.vn says hello to cit.ctu.edu.vn C: MAIL FROM: <ptphi@cit.ctu.edu.vn> S: 250 Sender ok C: RCPT TO: <lhly@yale.edu> S: 250 Recipient ok C: DATA S: 354 Enter mail, end with "." on a line by itself C: Subject: It’s Xmast! C: So I hope you a merry Xmas and a happy new year! C: . S: 250 Message accepted for delivery Như đã thấy trong ví dụ, client gởi đi một lệnh (HELO, MAIL FROM, RCPT TO, DATA, C: QUIT QUIT) và server trả lời bằng một mã số (250, 354, 221) có kèm theo lời chú thích có thể đọc S: 221 Bye-Bye được. Client kết thúc thư bằng <CRLF>.<CRLF>. Sau đây là bảng giải thích một số lệnh của client và mã số trả lời của server.

Lệnh
HELO MAIL FROM RCPT TO DATA QUIT

Trả lời
250 550 354 221

LỆNH CỦA CLIENT Ý nghĩa Câu chào và xưng danh của client Địa chỉ email của người gởi Địa chỉ email của người nhận Bắt đầu truyền nội dung của thư Hủy nối kết TRẢ LỜI CỦA SERVER Ý nghĩa Yêu cầu hợp lệ Yêu cầu không hợp lệ, không tồn tại hộp thư như client đã chỉ ra. Cho phép bắt đầu nhập thư vào. Kết thúc thư bằng <CRLF>.<CRLF> Server đang đóng kết nối TCP

Vẫn còn nhiều lệnh và mã trả lời chưa được trình bày, xin tham khảo tài liệu RFC 822 để có được đầy đủ thông tin.

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

158

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

8.2.4 Phân phát thư
Như đã trình bày, khi đứng về góc độ người dùng thư, họ sẽ dùng user agent để gởi và nhận thư cho họ. User agent dùng giao thức SMTP để gởi thư đi, dùng giao thức POP3 hoặc IMAP để nhận thư về.

8.2.4.1

POP3

Một phiên làm việc theo giao thức POP3 bắt đầu tại user agent. User agent khởi động một nối kết TCP đến cổng 110 của mail server. Khi kết nối thực hiện xong, phiên làm việc POP3 sẽ trải qua theo thứ tự ba kỳ: 1. Chứng thực. 2. Giao dịch dữ liệu. 3. Cập nhật. Kỳ chứng thực buộc người dùng thực hiện thủ tục đăng nhập bằng cách nhập vào hai lệnh sau: Lệnh
USER <tên người dùng> PASS <mật khẩu>

Ý nghĩa Khai báo tên người dùng. Khai báo mật khẩu.

Báo trả của mail server sẽ là một trong hai câu sau: Trả lời Ý nghĩa +OK <chú thích> Khai báo của người dùng là đúng. +ERR <chú thích> Khai báo của người dùng là sai và lời giải thích. Trong kỳ giao dịch, người dùng có thể xem danh sách thư chưa nhận về, nhận thư về và xóa thư trong hộp thư của mình khi cần thiết. Các lệnh mà người dùng thường sử dụng để giao dịch với server là: Lệnh Ý nghĩa Nếu dùng LIST không tham số, server sẽ trả về toàn bộ danh sách LIST [<số thứ tự thư>] các thư chưa nhận. Nếu có tham số là số thứ tự thư cụ thể, server sẽ trả về thông tin của chỉ bức thư đó thôi. RETR <số thứ tự thư> Tải lá thư có số thứ tự <số thứ tự thư> về. DELE <số thứ tự thư> Xóa lá thứ số <số thứ tự thư> khỏi hộp thư. QUIT Hoàn tất giai đoạn giao dịch và hủy nối kết TCP Các trả lời của server có thể là các số liệu mà client yêu cầu hoặc các thông báo +OK, -ERR như trong phần đăng nhập. Sau đây là dàn cảnh một phiên làm việc ví dụ giữa người dùng ptphi khi anh ta đăng nhập và làm việc trên hộp thư của mình tại server có địa chỉ mail.cit.ctu.edu.vn. Client Server
+OK POP3 server ready USER ptphi +OK PASS godblessus +OK login successfully LIST

Giải thích Server sẵn sàng phục vụ client Server xác nhận người dùng hợp lệ Chứng thực thành công ptphi kiểm tra hộp thư

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

159

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0
+OK 1 1024 2 2550 RETR 1 +OK DELE 1 +OK QUIT +OK Bye-Bye

Hộp thư của ptphi còn hai thư chưa nhận về, thư thứ nhất có kích thước 1024 bytes, thư thứ hai có kích thước 2550 bytes ptphi tải thư thứ nhất về server gởi thư thứ 1 cho ptphi ptphi xóa thư thứ nhất trong hộp thư server xoá thư thứ 1 thành công ptphi hủy nối kết server hủy nối kết

8.2.4.2

IMAP

Với những người dùng có một tài khoản email trên một ISP và người dùng này thường truy cập email trên một PC thì giao thức POP3 hoạt động tốt. Tuy nhiên, một sự thật trong ngành công nghệ máy tính, khi một thứ gì đó đã hoạt động tốt, người ta lập tức đòi hỏi thêm nhiều tính năng mới (và tự chuốc lấy nhiều phiền nhiễu). Điều đó cũng xảy ra đối với hệ thống email. Ví dụ, người ta chỉ có một tài khoản email, nhưng họ lại muốn ngồi đâu cũng truy cập được nó. POP3 cũng làm được chuyện này bằng cách đơn giản tải hết các email xuống máy PC mà người dùng này đang ngồi làm việc. Và dĩ nhiên là thư từ của người dùng này nằm rải rác khắp nơi. Sự bất tiện này khơi mào cho sự ra đời của giao thức phân phối thư mới, IMAP (Internet Message Access Protocol), được định nghĩa trong RFC 2060. Không giống như POP2, IMAP coi các thông điệp mặc nhiên nằm trên server vô hạn và trên nhiều hộp thư. IMAP còn đưa ra cơ chế cho phép đọc các thông điệp hoặc một phần của thông điệp, một tính năng hữu ích khi người dùng kết nối đến server bằng đường truyền tốc độ chậm như điện thoại nhưng lại đọc các email có âm thanh, hình ảnh… Với quan niệm cho rằng người dùng không cần tải thư về lưu trên PC, IMAP cung cấp các cơ chế cho phép tạo, xóa và sửa đổi nhiều hộp thư trên server. Cung cách làm việc của IMAP cũng giống như POP3, ngoài trừ trong IMAP có rất nhiều lệnh. IMAP server sẽ lắng nghe trên cổng 143. Cũng nên chú ý rằng, không phải mọi ISP đều hỗ trợ cả hai giao thức POP3 và IMAP. Bảng sau so sánh các tính năng của POP3 và IMAP Tính năng Giao thức được định nghĩa ở đâu? Cổng TCP được dùng Email được lưu ở đâu Email được đọc ở đâu Thời gian nối kết Sử dụng tài nguyên của server Nhiều hộp thư Ai lưu phòng hờ các hộp thư Tốt cho người dùng di động Kiểm soát của người dùng đối với việc tải thư về Tải một phần thư Quota đĩa có là vấn đề không? Dễ cài đặt Được hỗ trợ rộng rãi POP3 RFC 1939 110 PC của người dùng Off-line Ít Tối thiểu Không Người dùng Không Ít Không Không Có Có IMAP RFC 2060 143 Server On-line Nhiều Nhiều hơn Đúng ISP Có Tốt Có Thỉnh thoảng Không Đang phát triển

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

160

8.3 World Wide Web (HTTP)
Ứng dụng Web đã rất thành công, giúp cho nhiều người có thể truy cập Internet đến nỗi Web được hiểu đồng nghĩa với Internet! Có thể hiểu Web như là một tập các client và server hợp tác với nhau và cùng nói chung một ngôn ngữ: HTTP (Hyper Text Transfer Protocol). Đa phần người dùng tiếp xúc với Web thông qua chương trình client có giao diện đồ họa, hay còn gọi là trình duyệt Web (Web browser). Các trình duyệt Web thường được sử dụng nhất là Netscape Navigator (của Netscape) và Internet Explorer (của Microsoft). Hình H8.8 thể hiện trình duyệt Explorer đang trình bày trang chủ của Khoa Công Nghệ Thông Tin – Đại Học Cần Thơ:

H8.8 Trình duyệt Web Internet Explorer

Bất kỳ trình duyệt Web nào cũng có chức năng cho phép người dùng “mở một URL”. Các URL (Uniform Resource Locators) cung cấp thông tin về vị trí của các đối tượng trên Internet; chúng thường trông giống như sau: http://www.cit.ctu.edu.vn/index.html Nếu người dùng mở URL trên, trình duyệt Web sẽ thiết lập một kết nối TCP đến Web Server tại địa chỉ www.cit.ctu.edu.vn và ngay lập tức tải tập tin index.html về và thể hiện nó. Hầu hết các tập tin trên Web chứa văn bản và hình ảnh, một số còn chứa audio và video clips. Chúng còn có thể chứa các liên kết đến các tập tin khác – được gọi là các liên kết siêu văn bản (hypertext links). Khi người dùng yêu cầu trình duyệt Web mở ra một liên kết siêu văn bản (bằng cách trỏ chuột và

click lên liên kết đó), trình duyệt sẽ mở một nối kết mới, tải về và hiển thị một tập tin mới. Vì thế, rất dễ để duyệt từ server này đến server khác trên khắp thế giới để có được hết những thông tin mà người dùng cần. Khi người dùng chọn xem một trang Web, trình duyệt Web sẽ nạp trang Web đó từ Web server về sử dụng giao thức HTTP chạy trên TCP. Giống như SMTP, HTTP là giao thức hướng ký tự. Về cốt lõi, một thông điệp HTTP có khuôn dạng tổng quát sau: START_LINE <CRLF> MESSAGE_HEADER <CRLF> <CRLF> MESSAGE_BODY <CRLF> Hàng đầu tiên chỉ ra đấy là thông điệp yêu cầu hay trả lời. Nó sẽ chỉ ra "thủ tục cần được thực hiện từ xa" (trong tình huống là thông điệp yêu cầu) hoặc là "trạng thái trả về" (trong tình huống là thông điệp trả lời). Tập hợp các hàng kế tiếp chỉ ra các tùy chọn hoặc tham số nhằm xác định cụ thể tính chất của yêu cầu hoặc trả lời. Phần MESSAGE_HEADER có thể không có hoặc có một vài hàng tham số và được kết thúc bằng một hàng trống. HTTP định nghĩa nhiều kiểu header, một số liên quan đến các thông điệp yêu cầu, một số liên quan đến các thông điệp trả lời và một số lại liên quan đến phần dữ liệu trong thông điệp. Ở đây chỉ giới thiệu một số kiểu thường dùng. Cuối cùng, sau hàng trống là phần nội dung của thông điệp trả lời (MESSAGE_BODY), phần này thường là rỗng trong thông điệp yêu cầu.

8.3.1 Các thông điệp yêu cầu
Hàng đầu tiên của một thông điệp yêu cầu HTTP sẽ chỉ ra 3 thứ: thao tác cần được thực thi, trang Web mà thao tác đó sẽ áp lên và phiên bản HTTP được sử dụng. Bảng sau sẽ giới thiệu một số thao tác phổ biến.

Hành động
OPTIONS GET HEAD POST PUT DELETE TRACE CONNECT

Mô tả
Yêu cầu thông tin về các tùy chọn hiện có. Lấy về tài liệu được xác định trong URL Lấy về thông tin thô về tài liệu được xác định trong URL Cung cấp thông tin cho server Tải tài liệu lên server và đặt ở vị trí được xác định trong URL Xóa tài liệu nằm ở vị trí URL trên server Phản hồi lại thông điệp yêu cầu Được sử dụng bởi các proxy

Hai thao tác thường được sử dụng nhiều nhất là GET (lấy một trang Web về) và HEAD (lấy về thông tin của một trang Web). GET thường được sử dụng khi trình duyệt muốn tải một trang Web về và hiển thị nó cho người dùng. HEAD thường được sử dụng để kiểm tra tính hợp lệ của một liên kết siêu văn bản hoặc để xem một trang nào đó có bị thay đổi gì không kể từ lần tải về trước đó. Ví dụ, dòng START_LINE
GET http://www.cit.ctu.edu.vn/index.html HTTP/1.1

nói rằng: người dùng muốn tải về trên server www.cit.ctu.edu.vn trang Web có tên index.html và hiển thị nó. Ví dụ trên dùng URL tuyệt đối. Ta cũng có thể sử dụng URL tương đối như sau:
GET /index.html HTTP/1.1 Host: www.cit.ctu.edu.vn

Ở đây, Host là một trong các trường trong MESSAGE_HEADER.

8.3.2 Các thông điệp trả lời
Giống như các thông điệp yêu cầu, các thông điệp trả lời bắt đầu bằng một hàng START_LINE. Trong trường hợp này, dòng START_LINE sẽ chỉ ra phiên bản HTTP đang được sử dụng, một mã 3 ký số xác định yêu cầu là thành công hay thất bại và một chuỗi ký tự chỉ ra lý do của câu trả lời này. Ví dụ, dòng START_LINE
HTTP/1.1 202 Accepted

chỉ ra server đã có thể thõa mãn yêu cầu của người dùng. Còn dòng
HTTP/1.1 404 Not Found

chỉ ra rằng server đã không thể tìm thấy tài liệu như được yêu cầu. Có năm loại mã trả lời tổng quát với ký số đầu tiên xác định loại mã.

Mã
1xx 2xx 3xx 4xx 5xx

Loại
Thông tin Thành công Chuyển hướng Lỗi client Lỗi server

Lý do
Đã nhận được yêu cầu, đang tiếp tục xử lý Thao tác đã được tiếp nhận, hiểu được và chấp nhận được Cần thực hiện thêm thao tác để hoàn tất yêu cầu được đặt ra Yêu cầu có cú pháp sai hoặc không thể được đáp ứng Server thất bại trong việc đáp ứng một yêu cầu hợp lệ

Cũng giống như các thông điệp yêu cầu, các thông điệp trả lời có thể chứa một hoặc nhiều dòng trong phần MESSAGE_HEADER. Những dòng này cung cấp thêm thông tin cho client. Ví dụ, dòng header Location chỉ ra rằng URL được yêu cầu đang có ở vị trí khác. Vì thế, nếu trang Web của Khoa Công Nghệ Thông Tin được di chuyển từ địa chỉ http://www.cit.ctu.edu.vn/index.html sang địa chỉ http://www.ctu.edu.vn/cit/index.html mà người dùng lại truy cập vào URL cũ, thì Web server sẽ trả lời như sau
HTTP/1.1 301 Moved Permanently Location: http://www.ctu.edu.vn/cit/index.html

Trong tình huống chung nhất, thông điệp trả lời cũng sẽ mang theo nội dung trang Web được yêu cầu. Trang này là một tài liệu HTML, nhưng vì nó có thể chứa dữ liệu không phải dạng văn bản (ví dụ như ảnh GIF), dữ liệu này có thể được mã hóa theo dạng MIME. Một số hàng trong phần MESSAGE_HEADER cung cấp thêm thông tin về nội dung của trang Web, bao gồm ContentLength (số bytes trong phần nội dung), Expires (thời điểm mà nội dung trang Web được xem như lỗi thời), và Last-Modified (thời điểm được sửa đổi lần cuối cùng).

8.3.3 Các kết nối TCP
Nguyên tắc chung của giao thức HTTP là client nối kết đến cổng TCP số 80 tại server, server luôn lắng nghe trên cổng này để sẵn sàng phục vụ client. Phiên bản đầu tiên

(HTTP/1.0) sẽ thiết lập một nối kết riêng cho mỗi hạng mục dữ liệu cần tải về từ server. Không khó để thấy rằng đây là cơ chế không mấy hiệu quả: Các thông điệp dùng để thiết lập và giải phóng nối kết sẽ phải được trao đổi qua lại giữa client và server và khi mà tất cả client muốn lấy thông tin mới nhất của một trang Web, server sẽ bị quá tải. Cải tiến quan trọng nhất trong phiên bản HTTP/1.1 là nó cho phép các kết nối lâu dài – client và server sẽ trao đổi nhiều thông điệp yêu cầu/trả lời trên cùng một kết nối TCP. Kết nối lâu dài có hai cái lợi. Thứ nhất, nó làm giảm thiểu chi phí cho việc thiết lập/giải phóng nối kết. Thứ hai, do client gởi nhiều thông điệp yêu cầu qua một kết nối TCP, cơ chế điều khiển tắc nghẽn của TCP sẽ hoạt động hiệu quả hơn. Tuy nhiên, kết nối lâu dài cũng có cái giá phải trả. Vấn đề phát sinh ở chỗ: không ai trong client và server biết được kết nối đó sẽ kéo dài bao lâu. Điều này thực sự gây khó khăn cho phía server bởi vì tại mỗi thời điểm, nó phải đảm bảo duy trì kết nối đến cả ngàn client. Giải pháp cho vấn đề này là: server sẽ mãn kỳ và cắt nối kết nếu nó không nhận được một yêu cầu cụ thể nào từ phía

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

163

client trong một khoảng thời gian định trước. Ngoài ra, cả client và server phải theo dõi xem phía bên kia có chủ động cắt nối kết hay không và lấy đó làm cơ sở để tự cắt nối kết của mình. (Nhắc lại rằng, cả hai bên phải cắt nối kết thì nối kết TCP mới thực sự kết thúc).

### 8.3.4 Trữ đệm

Một trong những lĩnh vực nghiên cứu tích cực nhất hiện nay về Internet là làm sao để trữ tạm các trang Web một cách hiệu quả. Việc trữ tạm mang lại nhiều lợi ích. Từ phía client, việc nạp và hiển thị một trang Web từ bộ đệm gần đấy là nhanh hơn rất nhiều so với từ một server nào đó ở nửa vòng trái đất. Đối với server, có thêm một bộ đệm để can thiệp vào và phục vụ giúp yêu cầu của người dùng sẽ giảm bớt tải trên server. Việc trữ đệm có thể được cài đặt tại nhiều nơi khác khau. Ví dụ, trình duyệt Web có thể trữ tạm những trang Web mới được nạp về gần đây, để khi người dùng duyệt lại những trang Web đó, trình duyệt sẽ không phải nối kết ra Internet để lấy chúng về mà dùng bản trữ sẵn. Ví dụ khác, một khu vực làm việc (site) có thể đề cử một máy làm nhiệm vụ trữ tạm các trang Web, để những người dùng sau có thể sử dụng các bản trữ sẵn của những người dùng trước. Yêu cầu của hệ thống này là mọi người dùng trong site phải biết địa chỉ của máy tính làm nhiệm vụ bộ trữ tạm, và họ chỉ đơn giản là liên hệ với máy tính này để tải các trang Web về theo yêu cầu. Người ta thường gọi máy tính làm nhiệm vụ trữ tạm các trang Web cho một site là proxy. Vị trí trữ đệm có thể di chuyển gần hơn đến phần lõi của Internet là các ISP. Trong tình huống này, các site nối kết tới ISP thường không hay biết gì về việc trữ tạm ở đây. Khi các yêu cầu HTTP từ các site được chuyển phát đến router của ISP, router liền kiểm tra xem URL được yêu cầu có giống với các URL được trữ sẵn hay không. Nếu có, router sẽ trả lời ngay. Nếu không, router sẽ chuyển yêu cầu đến server thật sự và cũng không quên lưu vào bộ đệm của mình thông điệp trả lời từ phía server đó. Việc trữ tạm là đơn giản. Tuy nhiên bộ đệm phải đảm bảo những thông tin trữ đệm trong đó không quá cũ. Để làm được việc này, các Web server phải gán “ngày hết hạn” (tức là trường Expires trong header) cho mọi trang Web mà nó phục vụ cho client. Nhân đó, các bộ đệm cũng lưu lại thông tin này. Và từ đó, các bộ đệm sẽ không cần phải kiểm tra tính cập nhật của trang Web đó cho đến khi ngày hết hạn đến. Tại thời điểm một trang Web hết hạn, bộ đệm sẽ dùng lệnh HEAD hoặc lệnh GET có điều kiện (GET với trường If-Modified-Since trong phần header được đặt) để kiểm tra rằng nó có một phiên bản mới nhất của trang Web kia. Tổng quát hơn, cần phải có “các chỉ thị hướng dẫn” cho việc trữ đệm và các chỉ thị này phải được tuân thủ tại mọi bộ đệm. Các chỉ thị sẽ chỉ ra có nên trữ đệm một tài liệu hay không, trữ nó bao lâu, một tài liệu phải tươi như thế nào và vân vân.

## 8.4 Truyền tập tin (FTP)

Thông qua dịch vụ FTP, người dùng tại một máy tính có thể đăng nhập và thao tác lên hệ thống tập tin được chia sẻ của một máy tính từ xa. Mục tiêu của dịch vụ FTP là: 1) Đảm bảo việc chia sẻ tập tin (chương trình máy tính hoặc dữ liệu) trên mạng. 2) Khuyến khích việc sử dụng không trực tiếp (thông qua chương trình) tài nguyên trên các máy tính khác. 3) Người dùng không cần phải quan tâm đến sự khác nhau của các hệ thống tập tin trên mạng. 4) Truyền dữ liệu một cách tin cậy và hiệu quả.

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

164

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

8.4.1 Mô hình dịch vụ FTP
Hình H8.9 mô tả mô hình của dịch vụ FTP

H8.9 Mô hình dịch vụ FTP

Trong hệ thống này, người dùng sẽ ra lệnh cho FTP user agent. User agent sẽ nối kết tới FTP server để dàn xếp thủ tục làm việc, thực thi các tác vụ theo yêu cầu và trả kết quả về cho người dùng.

8.4.2 Giao thức FTP
Đầu tiên, user agent thiết lập một kết nối điều khiển trên cổng 21 tới FTP server. Sau khi đã thỏa thuận các tham số truyền nhận, hai bên sẽ thiết lập một kênh dữ liệu chạy trên cổng 20. Dữ liệu của các tập tin được trao đổi qua lại giữa user agent và server sẽ chạy trên kênh dữ liệu này. Kênh dữ liệu là kênh hoạt động theo phương thức hai chiều và không nhất thiết phải luôn tồn tại.

Hình 8.10 Giao tiếp giữa Client và Server trong giao thức FTP

8.4.3 Các lệnh cơ bản
Sau đây là các lệnh cơ bản mà người dùng có thể sử dụng để thao tác lên hệ thống FTP Lệnh Tham số Ý nghĩa FTP host-name Nối kết đến FTP server có địa chỉ host-name Cung cấp tên người dùng cho FTP server để thực hiện USER user-name quá trình chứng thực ASCII Chỉ định kiểu dữ liệu truyền nhận là ký tự BINARY Chỉ định kiểu dữ liệu truyền nhận là nhị phân LS Xem nội dung thư mục từ xa CD remote-dir Chuyển đến thư mục khác trong hệ thống tập tin từ xa Tải tập tin remote-file trên FTP server về hệ thống tập GET remote-file local-file tin cục bộ và đặt tên là local-file Nạp tập tin cục bộ local-file lên server và đặt tên là PUT local-file remote-file remote-file Tạo một thư mục có tên dir-name trên hệ thống tập tin MKDIR dir-name từ xa. RMDIR dir-name Xóa thư mục có tên dir-name trên hệ thống tập tin từ xa QUIT Đóng nối kết FTP và thoát khỏi chương trình FTP Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

165

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

Mục lục

Chương 1 ..... Error! Bookmark not defined.
Tổng quan về mạng máy tính.....1 1.1 Mạng điện báo.....2 1.2 Mạng điện thoại .....2 1.3 Mạng hướng đầu cuối .....2 1.4 Mạng máy tính .....3 1.4.1 Đường biên mạng .....3 1.4.1.1 Mô hình khách hàng/người phục vụ (client/server):.....4 1.4.1.2 Mô hình ngang cấp (peer-to-peer): .....4 1.4.2 Đường trục mạng.....4 1.4.2.1 Chuyển mạch (circuit switching).....4 1.4.2.2 Mạng chuyển gói.....5 1.4.2.3 So sánh mạng chuyển mạch và mạng chuyển gói.....5 1.4.2.4 Mạng truy cập .....5 1.4.3 Các lợi ích của mạng máy tính.....6 1.4.3.1 Mạng tạo khả năng dùng chung tài nguyên cho các người dùng.....6 1.4.3.2 Mạng cho phép nâng cao độ tin cậy.....6 1.4.3.3 Mạng giúp cho công việc đạt hiệu suất cao hơn. .....6 1.4.3.4 Tiết kiệm chi phí. .....6 1.4.3.5 Tăng cường tính bảo mật thông tin. .....6 1.4.3.6 Việc phát triển mạng máy tính đã tạo ra nhiều ứng dụng mới.....6 Chương 2 .....7 Các thành phần của mạng máy tính .....7 2.1 Phần cứng mạng máy tính.....8 2.1.1 Phân loại mạng máy tính theo kỹ thuật truyền tin.....8 2.1.1.1 Mạng quảng bá.....8 2.1.1.2 Mạng điểm nối điểm .....8 2.1.2 Phân loại mạng máy tính theo phạm vị địa lý .....8 2.1.2.1 Mạng cục bộ.....8 2.1.2.1.1 Mạng hình bus.....8 2.1.2.1.2 Mạng hình sao.....9 2.1.2.1.3 Mạng hình vòng .....9 2.1.2.2 Mạng đô thị .....9 2.1.2.3 Mạng diện rộng .....9 2.1.3 Mạng không dây.....10 2.1.3.1 Nối kết hệ thống (System interconnection) .....10 2.1.3.2 Mạng cục bộ không dây (Wireless LANs): .....10 2.1.3.3 Mạng diện rộng không dây (Wireless WANs): .....10 2.1.4 Liên mạng (Internetwork) .....10 2.2 Phần mềm mạng.....11 2.2.1 Cấu trúc thứ bậc của giao thức.....11 2.2.2 Ví dụ về cấu

trúc thứ bậc của giao thức .....12 2.2.3 Dịch vụ mạng .....13 2.2.3.1 Các phép toán của dịch vụ .....14 2.2.3.2 Sự khác biệt giữa dịch vụ và giao thức .....14 2.3 Mô hình tham khảo OSI.....15 Chương 3 .....18 Tầng vật lý.....18

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

166

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

3.1 Giới thiệu .....19
3.2 Vấn đề số hóa thông tin .....19
3.2.1 Số hóa văn bản .....20
3.2.2 Số hóa hình ảnh tĩnh.....21
3.2.3 Số hóa âm thanh và phim ảnh .....22 3.3
Các loại kênh truyền .....22
3.3.1 Kênh truyền hữu tuyến.....22
3.3.1.1 Cáp xoắn đôi (Twisted Pair) .....23
3.3.1.2 Cáp đồng trục (Coaxial Cable).....23
3.3.1.3 Cáp quang (Fiber Optic) .....24 3.3.2
Kênh truyền vô tuyến .....25 3.4 Đặc
điểm kênh truyền .....25 3.4.1.1
Truyền tải tín hiệu sóng dạng hình sin.....26 3.4.1.2
Truyền tín hiện bất kỳ .....27 3.4.1.3 Băng
thông của một kênh truyền (Bandwidth) .....27 3.4.1.4 Tần số biến
điệu và tốc độ dữ liệu (Baund rate and bit rate) .....28 3.4.1.5 Nhiễu và khả năng
kênh truyền.....29 3.4.1.6 Giao thông (Traffic)
.....30 3.5 Mã hóa đường truyền (Line
Coding) .....31 3.5.1 Mã hóa đường truyền
bằng tín hiệu số.....31 3.5.2 Mã hóa đường truyền
bằng tín hiệu tuần tự .....32 Chương 4
.....33 Tầng
liên kết dữ liệu.....33
( Data link layer )
.....33 4.1 Chức
năng của tầng liên kết dữ liệu.....34 4.1.1 Các
dịch vụ cơ bản của tầng liên kết dữ liệu.....34 4.1.2 Xử lý lỗi
.....34 4.1.3 Định
khung.....34 4.1.3.1 Phương
pháp đếm ký tự (Character Count) .....35 4.1.3.2 Phương pháp
sử dụng byte làm cờ và các byte độn (Flag byte with byte stuffing) 35 4.1.3.3 Sử dụng cờ
bắt đầu và kết thúc khung cùng với các bit độn (Starting and ending flags with bit
stuffing).....35 4.1.4 Điều khiển
lỗi (Error Control).....36 4.1.5 Điều khiển luồng
(Flow Control) .....36 4.2 Vấn đề xử lý
lỗi.....37 4.2.1 Bộ mã phát
hiện lỗi .....37 4.2.2 Những bộ mã
phát hiện lỗi (Error-Detecting Codes) .....37 4.2.2.1 Kiểm tra chẵn lẻ
(Parity Check).....37 4.2.2.2 Kiểm tra thêm theo
chiều dọc (Longitudinal Redundancy Check or Checksum) 38 4.2.2.3 Kiểm tra phần dư
tuần hoàn (Cyclic Redundancy Check).....38 4.3 Một số giao thức điều khiển
lỗi (Error Control) .....40 4.3.1.1 Giao thức truyền đơn
công không ràng buộc (Unrestricted Simplex Protocol) 42 4.3.1.2 Giao thức truyền đơn
công dừng và chờ (Simplex Stop-and-wait Protocol) 43 4.3.1.3 Giao thức truyền đơn công

cho kênh truyền có nhiễu (Simplex Protocol for Noisy Channel ) 44 4.4 Giao thức của sổ trượt (Sliding windows) .....45 4.4.1 Vấn đề truyền tải thông tin theo hai chiều (Duplex) .....45 4.4.2 Giới thiệu về giao thức cửa sổ trượt.....45

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

167

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

4.4.3 Hoạt động của cửa sổ trượt .....46
4.4.4 Cài đặt giao thức cửa sổ trượt kích thước 1 bit (A One-Bit Sliding Window Protocol 47 4.4.5 Vấn đề điều khiển lỗi (Error Control) .....48
4.4.5.1 Giao thức Go-Back-N .....48
4.4.5.2 Giao thức Selective Repeat .....51
4.4.5.2.1 Kích thước tối đa của cửa sổ gởi và nhận là bao nhiêu ?.....54 4.4.5.2.2 Số lượng buffer để lưu khung là bao nhiêu? .....54 4.4.5.2.3 Khi nào gởi báo nhận cho một gói tin? .....54 4.4.6 Giao thức HDLC (High-Level Data Link Control).....54 4.4.6.1 Các đặc tính của giao thức HDLC .....54 4.4.6.1.1 Ba loại trạm trong HDLC.....55 4.4.6.2 Hai cấu hình đường nối kết: .....55 4.4.6.3 Có 3 chế độ truyền tải là:.....55 4.4.6.4 Cấu trúc khung .....55 4.4.6.5 Một vài kịch bản về giao thức HDLC .....57 4.4.6.6 Giao thức Điểm nối điểm (PPP- Point-to-Point Protocol).....59 Chương 5 .....61 MẠNG NỘI BỘ .....61 &.....61 LỚP CON ĐIỀU KHIỂN TRUY CẬP .....61 5.1 Tổng quan về LAN .....62 5.2 Hình thái mạng.....62 5.2.1 Mạng hình sao .....62 5.2.2 Mạng hình vòng .....63 5.2.3 Mạng hình bus.....63 5.3 Lớp con MAC (Media Access Control Sublayer) .....63 5.3.1 Phương pháp chia kênh .....64 5.3.1.1 Chia tần số (FDMA – Frequency Division Multiple Access).....64 5.3.1.2 Chia thời gian (TDMA – Time Division Multiple Access) .....65 5.3.1.3 Kết hợp giữa FDMA và TDMA.....65 5.3.1.4 Phân chia mã (CDMA – Code Division Multiple Access) .....65 5.3.2 Phương pháp truy cập đường truyền ngẫu nhiên (Random Access).....68 5.3.2.1 ALOHA.....68 5.3.2.2 CSMA – Carrier Sense Multiple Access.....69 5.3.3 Phương pháp phân lượt truy cập đường truyền.....73 5.3.3.1 Ví dụ về phương pháp thăm dò: Thăm dò phân tán (Distributed Polling) .73 5.3.3.2 Ví dụ về phương pháp chuyển thẻ bài: Token Ring .....74 5.3.3.3 Ví dụ về phương pháp chuyền thẻ bài: Token Bus.....79 5.4 Chuẩn hóa mạng cục bộ.....80 5.5 Giới thiệu một số công nghệ mạng LAN.....82 5.5.1 Ethernet (802.3).....82 5.5.1.1 Tổng quan .....82 5.5.1.2 Khuôn dạng khung thông tin của Ethernet.....84 5.5.1.3 Địa chỉ Ethernet

.....84 5.5.1.4 Cách thức mã hóa tín hiệu.....84 5.5.1.5 Giải thuật truy cập đường truyền .....85 5.5.1.6 Các công nghệ Ethernet .....85 5.5.2 FDDI (Fiber Distributed Data Interface).....86 5.5.2.1 Các tính chất vật lý.....86 5.5.2.2 Giải thuật “Thẻ bài được định thời” – Timed Token .....87 5.5.2.3 Quản lý thẻ bài .....88

Đại Học Cần Thơ - Khoa Công Nghệ Thông Tin - Giáo Trình Mạng Máy Tính – V1.0

5.5.3 Mạng không dây (802.11) .....89
5.5.3.1 Các tính chất vật lý.....89
5.5.3.2 Tránh đụng độ (Collision Avoidance) .....90 5.5.3.3
Hệ thống phân tán .....91 5.5.3.4
Khuôn dạng khung .....92 Chương 6
.....93 Tầng
mạng.....9
3 (Network
Layer).....93 6.1
Giới thiệu .....94 6.2
Các vấn đề liên quan đến việc thiết kế tầng mạng.....94
6.2.1.1 Kỹ thuật hoán chuyển lưu và chuyển tiếp (Store-and-Forward Switching)94 6.2.2
Các dịch vụ cung cấp cho tầng vận chuyển .....95 6.2.2.1
Cài đặt dịch vụ không nối kết ( Implementation of Connectionless Service) 95 6.2.2.2 Cài
đặt dịch vụ định hướng nối kết (Connection – Oriented Service).....96 6.2.2.3 So sánh
giữa Datagram subnet và Virtual-Circuit subnet.....97 6.3 Giải thuật chọn
đường.....98 6.3.1 Giới
thiệu.....98 6.3.2 Mục tiêu
của giải thuật chọn đường.....98 6.3.3 Phân loại giải
thuật chọn đường.....98 6.3.4 Các giải thuật tìm
đường đi tối ưu.....99 6.3.4.1 Giải thuật tìm đường
đi ngắn nhất Dijkstra .....99 6.3.4.2 Giải thuật chọn đường tối
ưu Ford-Fulkerson .....100 6.3.5 Giải pháp vạch đường Vector
Khoảng cách (Distance Vector) .....101 6.3.6 Giải pháp chọn đường “Trạng thái
nối kết” (Link State).....104 6.3.6.1 Làm ngập một cách tin cậy (Reliable
Flooding).....104 6.3.6.2 Tính toán chọn đường trong Link State
.....106 6.3.7 Vạch đường phân cấp (Hierarchical Routing)
.....106 6.3.8 Vạch đường trong mạng di
động.....107 6.4 Các giải thuật chống tắc nghẽn
.....109 6.4.1 Các nguyên tắc chung để
điều khiển tắc nghẽn .....109 6.4.2 Các biện pháp phòng ngừa
tắc nghẽn.....110 6.4.3 Điều khiển tắc nghẽn trong các
mạng con dạng mạch ảo .....111 6.4.4 Điều khiển tắc nghẽn trong mạng
con dạng Datagram .....111 6.5 Liên mạng
.....113 6.5.1 Các
mạng con được nối kết với nhau ra sao?.....114 6.5.2 Nối kết
các mạng con dạng mạch ảo.....115 6.5.3 Nối kết các
mạng con dạng datagram .....116 6.5.4 Vạch đường
trong liên mạng.....117 6.5.5 Phân mảnh và tái
hợp .....117 6.6 Bộ giao thức liên mạng
(IPs - Internet Protocols) .....119 6.6.1 Giới
thiệu.....119 6.6.2 Giao
thức liên mạng IP (Internet Protocol).....120 6.6.2.1 Định
dạng gói tin IP (IP Packet Format).....120 6.6.3 Cấu trúc địa

chỉ IP.....121 6.6.4 Một số địa chỉ IP đặc biệt.....123 6.6.5 Ý nghĩa của Netmask .....123 6.6.6 Phân mạng con (Subnetting) .....123 6.6.6.1 Giới thiệu .....123 6.6.6.2 Phương pháp phân mạng con.....124 6.6.6.2.1 Phương pháp phân lớp hoàn toàn (Classfull Standard).....125

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

169

6.6.6.2.2 Phương pháp Vạch đường liên miền không phân lớp CIDR (Classless Inter-Domain Routing )....126 6.6.7 Vạch đường trong giao thức IP ....128 6.6.7.1 Đường đi của gói tin ....130 6.6.7.2 Giao thức phân giải địa chỉ (Address Resolution Protocol)....131 6.6.7.3 Giao thức phân giải địa chỉ ngược RARP (Reverse Address Resolution Protocol) 132 6.6.7.4 Giao thức thông điệp điều khiển Internet ICMP (Internet Control Message Protocol) 132 Chương 7 ....134 TẦNG VẬN CHUYỂN ....134
7.1 Dịch vụ của tầng vận chuyển ....135
7.1.1 Các dịch vụ cung cấp cho tầng ứng dụng....135
7.1.2 Các hàm dịch vụ cơ sở ....136 7.2 Các yếu tố cấu thành giao thức vận chuyển....136
7.2.1 Định địa chỉ ....137
7.2.2 Thiết lập nối kết....138
7.2.3 Giải phóng nối kết ....139
7.2.4 Điều khiển thông lượng....141 7.3 Tầng vận chuyển trong mạng Internet ....142
7.3.1 Giao thức UDP (User Datagram Protocol) ....142
7.3.2 Giao thức TCP (Transmission Control Protocol)....143 Chương 8 ....149 CÁC ỨNG DỤNG MẠNG ....149
8.1 Dịch vụ tên (DNS) ....149
8.1.1 Miền phân cấp ....150
8.1.2 Các server phục vụ tên ....150
8.1.3 Phương pháp phân tích tên....153 8.2 Electronic Mail (SMTP, MIME, POP3, IMAP) ....154 8.2.1 Các thành phần của hệ thống email....154 8.2.2 Khuôn dạng của một email....155 8.2.3 Chuyển thư ....157 8.2.4 Phân phát thư....159 8.2.4.1 POP3 ....159 8.2.4.2 IMAP....160 8.3 World Wide Web (HTTP) ....161 8.3.1 Các thông điệp yêu cầu ....162 8.3.2 Các thông điệp trả lời ....163 8.3.3 Các kết nối TCP ....163 8.3.4 Trữ đệm ....164 8.4 Truyền tập tin (FTP) ....164 8.4.1 Mô hình dịch vụ FTP ....165 8.4.2 Giao thức FTP ....165 8.4.3 Các lệnh cơ bản ....165

Biên Soạn: Th.s Ngô Bá Hùng – Ks Phạm Thế Phi - 01/2005

170

**********

http://ngoclinhson.violet.vn, http://ngoclinhson.tk - website đang xây dựng, cập nhật:

+ Văn bản thiết yếu về Giáo dục và Đào tạo;
+ Tài liệu về Quản lý Giáo dục;
+ Tài liệu về các hoạt động giáo dục;
+ Tài liệu về Tin học, công nghệ thông tin, thiết kế web;
+ Giáo trình, giáo án, đề thi/kiểm tra (và đáp án);
+ Tài liệu cá nhân có được về mọi lĩnh vực;
+ Các phần mềm cá nhân có được về mọi lĩnh vực;

(Một số chuyên mục, nội dung trước tiên ưu tiên khối THPT).

Các tài liệu đã upload có thể được chỉnh sửa, bổ sung theo thời gian, có thể thay thế bằng một tài liệu khác giá trị hơn; sẽ bị xóa đi nếu phát hiện thiếu chính xác hoặc không có giá trị. Do đó, tại một địa chỉ, cùng một tiêu đề có thể download được tài liệu khác hoặc mới hơn.

Ban quản trị cố gắng cung cấp kèm theo nguồn gốc tài liệu một cách đầy đủ nhất, đặc biệt là về tác giả, thời gian tài liệu, thời gian upload hay cung cấp...

Ban quản trị ưu tiên tài liệu dạng văn bản (word). Các tài liệu sẽ được chuyển mã Unicode và chuẩn hóa văn bản trong điều kiện cho phép.

Yêu cầu cao quả thực quá sức của một website cá nhân do đó không tránh khỏi sai sót, rất mong sự đóng góp chia sẻ của quý thầy cô và các bạn. Quản trị website rất trân trọng và cảm ơn sự ủng hộ của mọi người.

**********

**TRƯỜNG ĐẠI HỌC ĐÀ LẠT**
**KHOA CÔNG NGHỆ THÔNG TIN**

**TRẦN NGÔ NHƯ KHÁNH**

**BÀI GIẢNG TÓM TẮT**

# MẠNG MÁY TÍNH

**Dành cho sinh viên ngành Công nghệ Thông tin**

**(Lưu hành nội bộ)**

**Đà Lạt 2008**

# Mục Lục

**Chương I. Những khái niệm căn bản về mạng ..... 4**
I.1. Khái niệm và phân loại mạng ..... 4
I.2. Dịch vụ mạng ..... 8
I.3. Giao thức mạng ..... 8
I.4. Các mô hình tham chiếu(reference models) ..... 10
I.5. Hệ điều hành trong môi trường mạng ..... 15
I.6. Mạng Internet ..... 16
**Chương II. Tầng vật lý ..... 18**
II.1. Chức năng ..... 18
II.2. Môi trường truyền tin ..... 18
II.3. Đặc tả các loại cáp mạng ..... 20
II.4. Chuẩn giao diện ..... 22
**Chương III. Giao thức tầng liên kết dữ liệu ..... 24**
III.1. Chức năng và dịch vụ ..... 24
III.2. Cơ chế phát hiện và sửa lỗi ..... 30
III.3. Các giao thức đa truy cập ..... 33
III.4. Khái niệm mạng LAN ..... 38
III.5. Địa chỉ vật lý (MAC address) ..... 47
III.6. Một số công nghệ tầng liên kết dữ liệu khác ..... 47
**Chương IV. Giao thức tầng mạng ..... 53**
IV.1. Chức năng của tầng mạng ..... 53
IV.2. Bộ định tuyến và các thiết bị kết nối mạng khác: ..... 56
IV.3. Giao thức IP (IP Protocol) ..... 61
IV.4. Các giao thức liên quan đến IP ..... 69
IV.5. Giao thức định tuyến ..... 70
IV.6. Định tuyến trên Internet ..... 77
**Chương V. Giao thức tầng giao vận ..... 79**
V.1. Dịch vụ tầng vận chuyển ..... 79

V.2. Giao thức không kết nối UDP ..... 80
V.3. Giao thức hướng kết nối TCP ..... 81
V.4. So sánh TCP và UDP ..... 87
**Chương VI. Giao thức tầng ứng dụng ..... 89**
VI.1. Chức năng: ..... 89
VI.2. World Wide Web - HTTP ..... 89
VI.3. Giao thức truyền File-FTP ..... 92
VI.4. Giao thức SMTP ..... 93
VI.5. Các giao thức nhận mail: ..... 102
VI.6. Dịch vụ phân giải tên miền (DNS Services-Domain Name System Services) ..... 105

# Mở đầu

Cùng với sự phát triển mạnh mẽ của công nghệ thông tin ngày nay, mạng máy tính đóng một vai trò quan trọng, cung cấp những dịch vụ tiện ích cho nhiều lĩnh vực đời sống xã hội khác nhau.

Giáo trình này nhằm cung cấp cho sinh viên ngành Công nghệ Thông tin những kiến thức căn bản về mạng máy tính, cách thức hoạt động và tổ chức của một hệ thống mạng. Các khái niệm về kiến trúc phân tầng, các giao thức mạng trong các tầng khác nhau. Tài liệu cũng trình bày về mô hình TCP/IP, các công nghệ mạng phổ biến, các thiết bị cần thiết để triển khai một hạ tầng mạng, khái niệm địa chỉ IP, định tuyến,…

Tuy đã có nhiều cố gắng trong quá trình biên soạn nhưng vẫn còn nhiều thiếu sót, chúng tôi mong nhận được các ý kiến đóng góp của các thầy cô, đồng nghiệp và các bạn sinh viên để chúng tôi có thể hoàn thiện giáo trình này hơn.

# Chương I. Những khái niệm căn bản về mạng

## I.1. Khái niệm và phân loại mạng

### I.1.1. Khái niệm

Mạng máy tính là tập hợp nhiều máy tính điện tử và các thiết bị đầu cuối được kết nối với nhau bằng các thiết bị liên lạc nhằm trao đổi thông tin, cùng chia sẽ phần cứng, phần mềm và dữ liệu với nhau.

Mạng máy tính bao gồm phần cứng, các giao thức và các phần mềm mạng.

Khi nghiên cứu về mạng máy tính, các vấn đề quan trọng được xem xét là giao thức mạng, cấu hình kết nối mạng và các đích vụ trên mạng.

Mạng máy tính có những công dụng như sau:

1. Tập trung tài nguyên tại môt số máy và chia sẽ cho nhiều máy khác
   - Nhiều người có thể dùng chung một tiện ích.
   - Dữ liệu đực quản lý tập trung nên an toàn hơn, trao đổi giữa người sử dụng thuận lợi hơn, nhanh chóng hơn.
   - Mạng máy tính cho phép người lập trình ở một trung tâm máy tính này có thể sử dụng các chương trình tiện ích của một trung tâm máy tính khác đang rỗi, sẽ làm tăng hiệu quả kinh tế của hệ thống.
2. Khắc phục trở ngại về khoảng cách địa lý.
3. Tăng chất lượng và hiệu quả khai thác thông tin.
4. Cho phép thực hiện những ứng dụng tin học phân tán.
5. Độ an toàn, tin cậy của hệ thống tăng lên nhờ khả năng thay thế máy có sự cố khi có sự cố*:* An toàn cho dữ liệu của phần mềm vì phần mềm mạng sẽ khóa các tập tin khi có người không đủ quyền hạn truy xuất các tập tin và các thư mục đó.
6. Phát triển các công nghệ trên mạng: Người sử dụng có thể trao đổi thông tin với nhau dễ dàng và sử dụng các hệ mạng như là một công cụ để phổ biến tin tức, thông báo về một chính sách mới, về nội dung buổi họp, về các thông tin kinh tế như giá cả thị trương, tin rao vặt (muốn bán hoặc mua một cái gì đó), hoặc sắp xếp thời khóa biểu của mình chen lẫn với thời khóa biểu của những người khác …

### I.1.2. Phân loại mạng

- **Dựa theo khoảng cách địa lý**

Mạng máy tính có thể phân bổ trên một khu vực nhất định trong phạm vi quốc gia hay toàn cầu. Dựa vào phạm vi phân bố, người ta có thể phân ra các loại mạng như sau:

a. LAN ( Local Area Netwowk – mạng cục bộ): LAN thường được sử dụng trong nội bộ một cơ quan tổ chức… kết nối các máy tính trong một khu vực bán kính khoảng 100m đến 100km. Kết nối được thực hiện thông qua các môi trường truyền thông tốc độ cao, ví dụ cáp đồng trục hay cáp quang.

b. MAN (Metropolitan Area Network – mạng đô thị) : Kết nối các máy tính trong phạm vi một thành phố. Kết nối này được thực hiện qua các môi trường truyền thông tốc độ cao ( 50 – 100 Mbit/s)

c. WAN (Wide Area Network – mạng diện rộng) : Kết nối các máy tính trong nội bộ các quốc gia hay các quốc gia trong cùng một châu lục. Thông thường kết nối này được thực hiện thông qua mạng viễn thông. Các WAN có thể được kết nối với nhau thành GAN hay tự nó đã là GAN.

d. GAN (Global Area Network - Mạng toàn cầu) : Kết nối máy tính từ các châu lục khác nhau. Thông thường kết nối này được thực hiện thông qua mạng viễn thông và vệ tinh.

Trong các khái niệm nói trên, WAN và LAN là hai khái niệm hay được sử dụng nhất.

- **Dựa theo cấu trúc mạng**

1. ***Kiểu điểm - điểm (point – to – point)***

Đường truyền nối từng cặp nút mạng với nhau. Thông tin đi từ nút nguồn qua nút trung gian rồi gởi tiếp nếu đường truyền không bị bận. Do đó còn có tên là mạng lưu trữ và chuyển tiếp (*store and forward).*

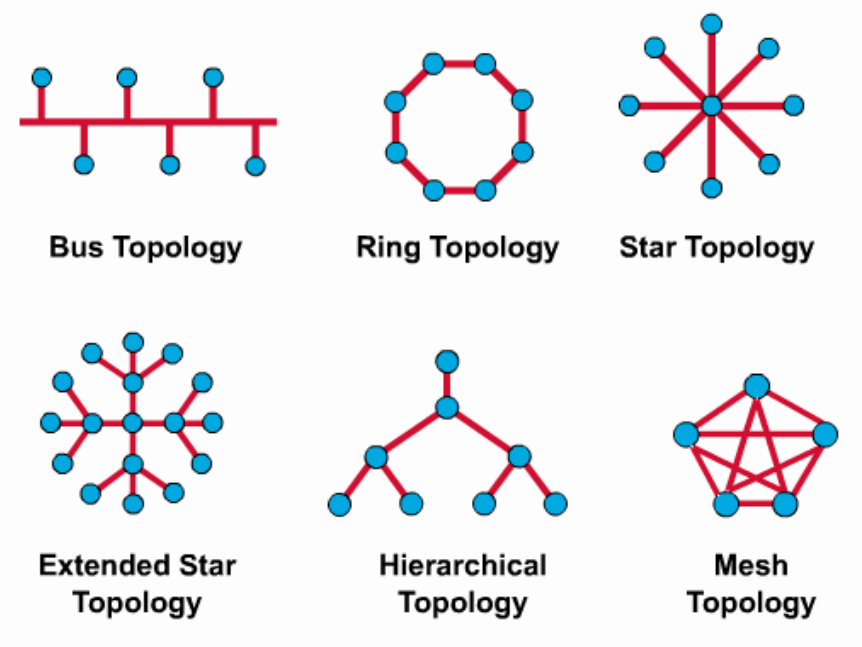
Ví dụ: mạng hình sao(star), dạng vòng (ring), dạng cấp bậc (hierarchical)

***2. Kiểu quảng bá (broadcast)***

Bản tin được gửi đi từ một nút nào đó sẽ được tiếp nhận bởi các nút còn lại (còn gọi là broadcasting hay point-to-multipoint). Trong bản tin phải có vùng địa chỉ cho phép mỗi nút kiểm tra xem có phải bản tin của mình không và xử lý nếu đúng bản tin được gởi đến.

Ví dụ: mạng bus.

Trong cấu trúc dạng Bus và Vòng cơ chế "*Trọng tài"* dùng để giải quyết các xung đột *(collision)* xảy ra khi nhiều nút muốn truyền tin đồng thời. Trong cấu trúc vệ tinh hoặc radio, mỗi nút cần có ăng ten thu và phát.

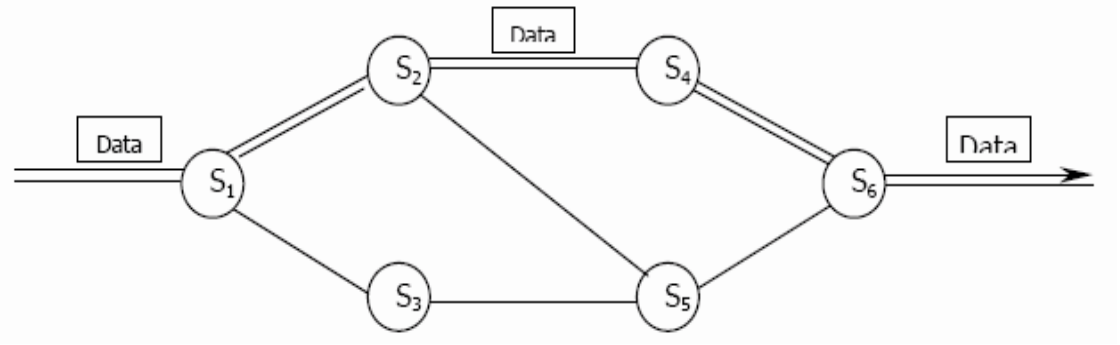



Hìng I-1. Một số dạng cấu trúc mạng

- **Dựa theo phương pháp chuyển mạch**
  - Mạng chuyển kênh (Line switching network), ví dụ như mạng điện thoại.
  - Mạng chuyển mạch thông báo (Message switching network)
  - Mạng chuyển mạch gói (Packet switching network)

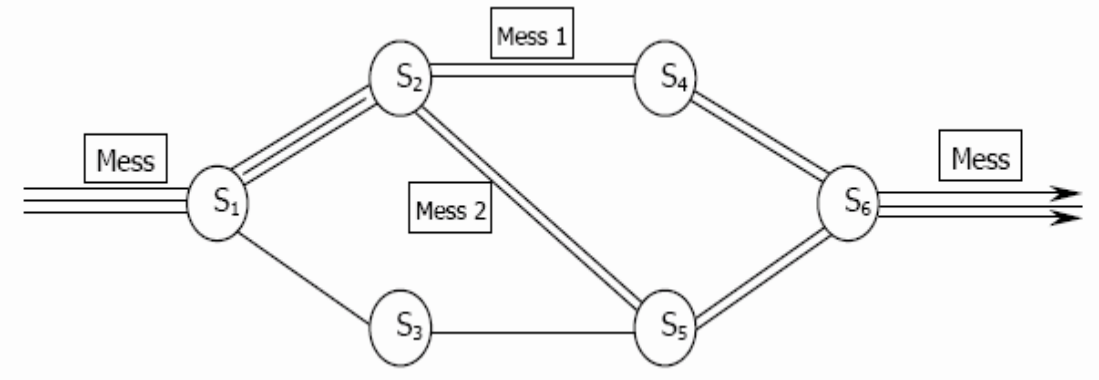
### *1. Mạng chuyển mạch kênh*

Chuyển mạch kênh (line switching) được dùng trong mạng điện thoại. Một kênh cố định được thiết lập các cặp thực thể cần liên lạc với nhau. Mạng này có hiệu suất không cao vì có lúc kênh bỏ không.




Hình I-2. Mạng chuyển mạch kênh.

### *2. Mạng chuyển mạch bản tin*




Hình I-3. Phương pháp chuyển mạch thông báo

Các nút của mạng căn cứ vào địa chỉ đích của "bản tin" để chọn nút kết tiếp. Như vậy các nút cần lưu trữ và đọc tin nhận được, quản lý việc truyền tin. Trong trường hợp bản tin quá dài và nếu sai phải truyền lại thì hiệu suất không cao. Phương pháp này giống như cách gởi thư thông thường.

Ưu điểm so với phương pháp chuyển mạch kênh:

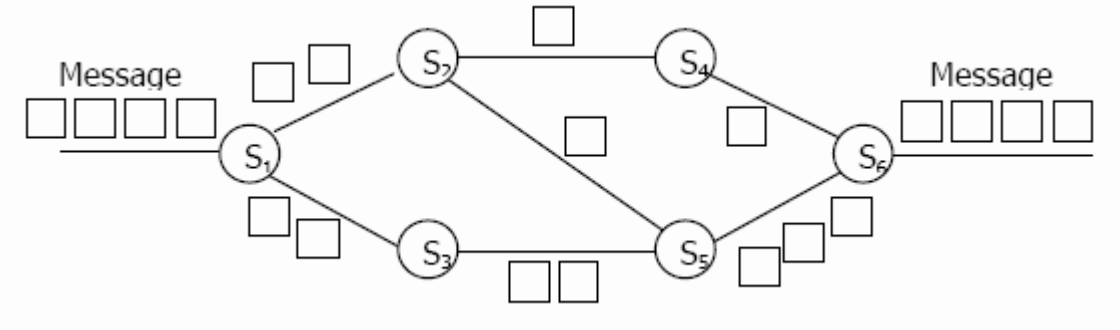
- Hiệu suất sử dụng đường truyền cao vì không bị chiếm dụng độc quyền mà được chia cho nhiều thực thể.
- Mỗi nút mạng (hay nút chuyển mạch thông báo) có thể lưu trữ bản tin cho tới khi kênh truyền mới gởi bản tin lại. Do đó giảm được tình trạng tắc nghẽn (congestion) trên mạng.
- Điều khiển việc truyền tin bằng cách sắp xếp độ ưu tiên của các bản tin.
- Có thể tăng hiệu suất sử dụng giải thông của mạch bằng cách gán địa chỉ quảng bá (broadcast) để gởi bản tin đồng thời đến nhiều đích.

Nhược điểm

- Do không hạn chế kích thước của bản tin nên có thể dẫn đến phí tổn lưu trữ tạm thời cao và ảnh hưởng đến thời gian hồi đáp và chất lượng truyền đi.
- Mạng chuyển mạch thông báo thích hợp với các dịch vụ thông tin kiểu thư điện tử (Email) hơn là đối với các ứng dụng có tính thời gian thực vì tồn tại độ trễ nhất định do lưu trữ và xử lý thông tin điều khiển tại mỗi nút.

### *3. Mạng chuyển mạch gói*

Bản tin được chia thành nhiều gói tin (packet) với độ dài 512 bytes, phần đầu là địa chỉ đích, mã để tập hợp các gói. Các gói của các bản tin khác nhau có thể được truyền độc lập trên cùng một đường truyền. Vấn đề phức tạp ở đây là tạo lại bản tin ban đầu, đặc biệt khi được truyền trên nhiều con đường khác nhau.




Hình I-4. Mạng chuyển mạch gói

Chuyển mạch gói mềm dẻo, hiệu suất cao. Xu hướng phát triển hiện nay là sử dụng hai kỹ thuật chuyển mạch kênh và chuyển mạch gói cùng một mạng thống nhất gọi là ISDN (*Interated Services Digital Network* – Mạng thông số đa dịch vụ).

## I.2. Dịch vụ mạng

Một số dịch vụ mạng phổ biến:

- Dịch vụ tập tin (File Services): Cho phép các máy tính trên mạng chia sẻ tập tin với nhau.
- Dịch vụ in ấn (Print Service): Nhiều máy trên mạng sử dụng chung một máy in. Giúp giảm chi phí và tăng độ linh hoạt
- Dịch vụ thư tính (Message Service): Là dịch vụ cho phép gửi/nhận thư điện tử. Thư có thể kèm phim ảnh, âm thanh,…
- Dịch vụ thư mục (Directory Service): Cho phép quản lý tất cả thông tin các đối tượng trên mạng, nhờ đó quá trình quản lý và chia sẻ tài nguyên hiệu quả hơn.
- Dịch vụ ứng dụng (Application Service): Dịch vụ cung cấp kết quả cho các chương trình ở client bằng cách thực hiện các chương trình phù hợp ở server.

## I.3. Giao thức mạng

Giao thức (protocol) là tập hợp các quy tắc giao tiếp giữa các hệ máy tính. Giao thức có các chức năng chính sau:

1. Định nghĩa cấu trúc khung một cách chính xác cho từng byte, các kí tự và bản tin.
2. Phát hiện và xử lý lỗi, thông thường là gửi lại bản tin gốc sau khi phát hiện lần trước bị lỗi.

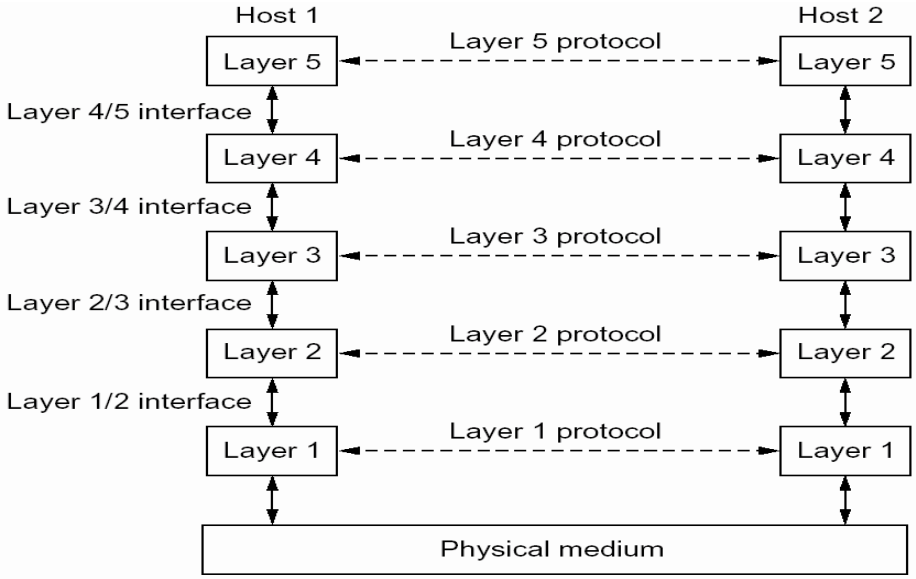
3. Quản lý thứ tự các lệnh để đếm bản tin, nhận dạng, tránh mất hoặc nhận thừa bản tin.
4. Đảm bảo không nhầm lẫn bản tin và lệnh.
5. Chỉ ra các thuộc tính đường dây khi lập các đường nối đa điểm hoặc bán song công (cho biết ai đang trao đổi thông tin với ai).
6. Giải quyến vấn đề xung đột truy cập (yêu cầu đồng thời), gửi khi chưa có số liệu, mất liên lạc, khởi động.

Để giảm độ phức tạp thiết kế, giao thức mạng hiện nay được thiết kế theo kiến trúc đa tầng, mỗi tầng được xây dựng trên tầng trước nó, tầng bên dưới sẽ cung cấp dịch vụ cho tầng bên trên. Tầng N trên một máy sẽ thực hiện việc giao tiếp với tầng N trên máy khác. Các nguyên tắc, luật lệ sử dụng cho việc giao tiếp này gọi là các giao thức của tầng N.

Các thực thể (entity) nằm trên tầng tương ứng ở những máy khác nhau gọi là các tiến trình đồng mức. Các tiến trình đồng mức giao tiếp với nhau bằng các giao thức của tầng đó. Giữa hai tầng kề nhau tồn tại một giao diện (interface) xác định các hàm nguyên thủy và các dịch vụ tầng dưới cung cấp cho tầng bên trên.

Tập hợp các tầng và các giao thức hình thành kiến trúc mạng (Network Architecture). Cấu trúc phân tầng của máy tính có ý nghĩa đặc biệt như sau:

- Thuận tiện trong việc thiết kế, xây dựng và cài đặt các mạng máy tính, trong đó mỗi hệ thống được xem là cấu trúc đa tầng.
- Mỗi tầng được xây dựng trên cơ sở tầng trước đó, tầng dưới cung cấp dịch vụ cho tầng bên trên.
- Tập hợp các giao thức, các vấn đề kĩ thuật và công nghệ có thể được khảo sát, nghiên cứu, triển khai độc lập với nhau.




Hình I-5. Mô hình trao đổi dữ liệu giữa các tầng

## I.4. Các mô hình tham chiếu(reference models)

### I.4.1. Mô hình OSI

Mô hình OSI (Open System Interconnection) là một cơ sở dành cho việc chuẩn hoá các hệ thống truyền thông, nó được nghiên cứu và xây dựng bởi ISO. Việc nghiên cứu về mô hình OSI được bắt đầu tại ISO vào năm 1971 với mục tiêu nhằm tới việc nối kết các sản phẩm của các hãng sản xuất khác nhau và phối hợp các hoạt động chuẩn hoá trong các lĩnh vực viễn thông và hệ thống thông tin. Theo mô hình OSI, chương trình truyền thông được chia ra thành 7 tầng với những chức năng phân biệt cho từng tầng. Hai tầng đồng mức khi liên kết với nhau phải sử dụng một giao thức chung. Trong mô hình OSI có hai loại giao thức chính được áp dụng: giao thức hướng liên kết (connection - oriented) và giao thức không liên kết (connectionless)

- **Giao thức hướng liên kết**: trước khi truyền dữ liệu hai tầng đồng mức cần thiết lập một liên kết logic và các gói tin được trao đổi thông qua liên kết này, việc có liên kết logic sẽ nâng cao độ an toàn trong truyền dữ liệu.
- **Giao thức không liên kết:** trước khi truyền dữ liệu không thiết lập liên kết logic và mỗi gói tin được truyền độc lập với các gói tin trước hoặc sau nó.

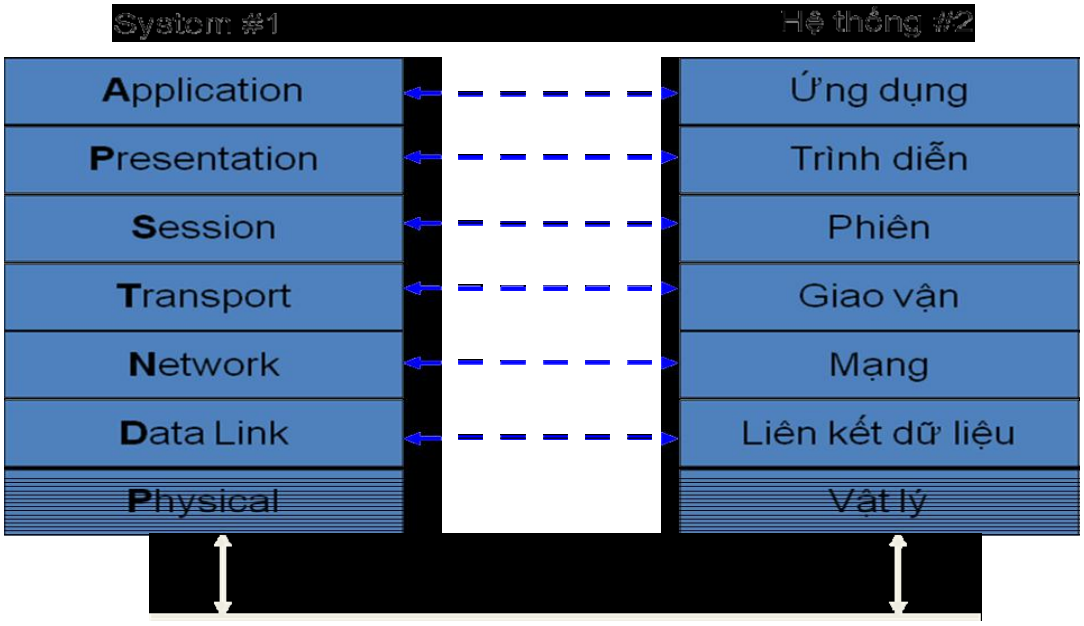
Như vậy với giao thức có liên kết, quá trình truyền thông phải gồm 3 giai đoạn phân biệt:

• Thiết lập liên kết (logic): hai thực thể đồng mức ở hai hệ thống thương lượng với nhau về tập các tham số sẽ sử dụng trong giai đoạn sau (truyền dữ liệu).

• Truyền dữ liệu: dữ liệu được truyền với các cơ chế kiểm soát và quản lý kèm theo (như kiểm soát lỗi, kiểm soát luồng dữ liệu, cắt/hợp dữ liệu...) để tăng cường độ tin cậy và hiệu quả của việc truyền dữ liệu.

• Hủy bỏ liên kết (logic): giải phóng tài nguyên hệ thống đã được cấp phát cho liên kết để dùng cho liên kết khác.

Đối với giao thức không liên kết thì chỉ có duy nhất một giai đoạn truyền dữ liệu.




Hình I-6. Mô hình OSI

Chức năng các tầng trong mô hình OSI:

- **Tầng ứng dụng (Application layer)**: tầng ứng dụng quy định giao diện giữa người sử dụng và môi trường OSI, nó cung cấp các phương tiện cho người sử dụng truy cập vả sử dụng các dịch vụ của mô hình OSI.
- **Tầng trình bày (Presentation layer)**: tầng trình bày chuyển đổi các thông tin từ cú pháp người sử dụng sang cú pháp để truyền dữ liệu, ngoài ra nó có thể nén dữ liệu truyền và mã hóa chúng trước khi truyền để bảo mật.
- **Tầng phiên (Session layer)**: tầng phiên quy định một giao diện ứng dụng cho tầng vận chuyển sử dụng. Nó xác lập ánh xạ giữa các tên, đặt địa chỉ, tạo ra các tiếp xúc ban đầu giữa các máy tính khác nhau trên cơ sở các giao dịch truyền thông. Nó đặt tên nhất quán cho mọi thành phần muốn đối thoại riêng với nhau.
- **Tầng vận chuyển (Transport layer)**: tầng vận chuyển xác định địa chỉ trên mạng, cách thức chuyển giao gói tin trên cơ sở trực tiếp giữa hai đầu mút (end-to-end). Để bảo đảm được việc truyền ổn định trên mạng tầng vận chuyển thường đánh số các gói tin và đảm bảo chúng chuyển theo thứ tự.
- **Tầng mạng (Network layer)**: tầng mạng có nhiệm vụ xác định việc chuyển hướng, vạch đường các gói tin trong mạng, các gói tin này có thể phải đi qua nhiều chặng trước khi đến được đích cuối cùng.

- **Tầng liên kết dữ liệu (Data link layer):** tầng liên kết dữ liệu có nhiệm vụ xác định cơ chế truy nhập thông tin trên mạng, các dạng thức chung trong các gói tin, đóng các gói tin...
- **Tầng vật lý (Physical layer)**: tầng vật lý cung cấp phương thức truy cập vào đường truyền vật lý để truyền các dòng bit không cấu trúc, ngoài ra nó cung cấp các chuẩn về điện, dây cáp, đầu nối, kỹ thuật nối mạch điện, điện áp, tốc độ cáp truyền dẫn, giao diện nối kết và các mức nối kết..

### I.4.2. Mô hình TCP/IP

Mô hình OSI chỉ mang tính chất lý thuyết, phục vụ nghiên cứu và học tập. Có nhiều mô hình khác nhau như NetBIOS, IPX/SPX,..nhưng mô hình được sử dụng rộng rãi cho Internet là TCP/IP. Về lịch sử phát triển, vào cuối những năm 1960 và đầu 1970, bộ quốc phòng Mỹ (Department of Defense - DoD) được giao trách nhiệm phát triển mạng ARPANET. Mạng ARPANET bao gồm mạng của những tổ chức quân đội, các trường đại học và các tổ chức nghiên cứu kết nối bằng đường điện thoại, được dùng để hỗ trợ cho những dự án nghiên cứu khoa học và quân đội. Khi vệ tinh và mạng vô tuyến được sử dụng để trao đổi thông tin, các giao thức cũ không còn đủ đáp ứng dẫn đến yêu cầu có một kiến trúc tham chiếu mới. Vì vậy khả năng kết nối linh động nhiều mạng khác nhau được đặt lên hàng đầu. Kiến trúc này sau đó được biết đến với tên gọi mô hình tham chiếu TCP/IP, dựa trên hai giao thức chính của kiến trúc.

Mô hình kiến trúc TCP/IP được chia làm 4 tầng:

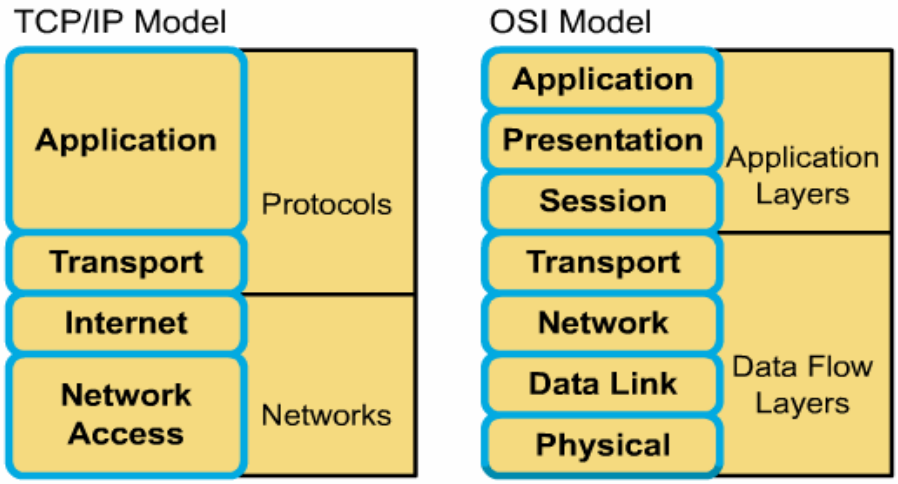
1. **Tầng truy cập mạng (Network Access)**

Cung cấp cho hệ thống phương thức để truyền dữ liệu trên các thiết bị phần cứng vật lý khác nhau của mạng. Đồng thời đóng gói các lược đồ dữ liệu IP (IP datagram) thành các khung (frame) truyền trên mạng và ánh xạ địa chỉ IP thành các địa chỉ vật lý tương ứng.

Tầng này còn định nghĩa cách thức truyền các khối dữ liệu IP, các giao thức của tầng này phải biết chi tiết cấu trúc vật lý mạng ở dưới để định dạng chính xác dữ liệu sẽ được truyền.

2. **Tầng mạng**

Tầng mạng chịu trách nhiệm định tuyến các bản tin (message) qua các mạng vật lý khác nhau, liên mạng. Giao thức chính của tầng này là IP, cung cấp dịch vụ giao nhận gói tin cơ bản trên các mạng TCP/IP. Giao thức IP bổ sung một địa chỉ logic là gọi là địa chỉ IP được sử dụng để nhận diện thiết bị và định tuyến liên mạng.




Hình I-7. Các lớp tương ứng giữa TCP/IP và OSI

### 3. Tầng giao vận

Tầng giao vận còn được gọi là tầng truyền Trạm-tới-Trạm (Host-to-Host) chịu trách nhiệm cung cấp cho tầng ứng dụng các dịch vụ tạo lập phiên và truyền dữ liệu. Các giao thức chính của tầng Giao vận là TCP (Transmision Control Protocol) và UDP (User Datagram Protocol).

- TCP cung cấp các dịch vụ truyền thông tin cậy một-một (one-to-one), hướng liên kết (connection-oriented). TCP chịu trách nhiệm thiết lập các kết nối TCP, gửi các gói tin có sắp xếp, thông báo, và các gói tin phục hồi dữ liệu bị mất trong quá trình truyền.
- UDP cung cấp các dịch vụ truyền tin một-một, một-nhiều, không liên kết và không tin cậy. UDP được sử dụng khi lượng dữ liệu cần truyền nhỏ (ví dụ dữ liệu không điền hết một gói tin), khi việc thiết lập liên kết TCP là không cần thiết, hoặc khi các ứng dụng hoặc các giao thức tầng trên cung cấp dịch vụ đảm bảo trong khi truyền.

Tầng Giao vận chịu trách nhiệm tầng Giao vận trong mô hình OSI và một số nhiệm vụ của tầng Phiên (Session) của OSI.

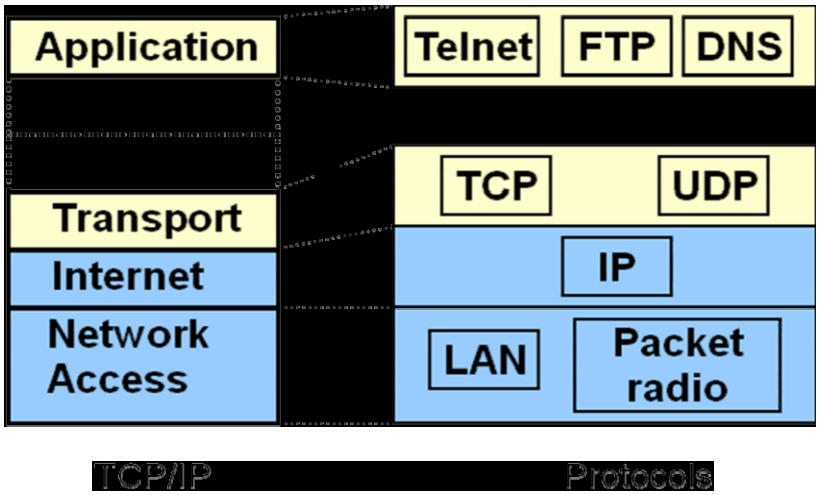
### 4. Tầng ứng dụng:

Tầng ứng dụng cung cấp các ứng dụng với khả năng truy cập các dịch vụ của các tầng khác và định nghĩa các giao thức mà các ứng dụng sử dụng để trao đổi dữ liệu. Có nhiều giao thức tầng ứng dụng và các giao thức mới luôn luôn được phát triển.

Các giao thức được ứng dụng rộng rãi nhất của tầng ứng dụng được sử dụng để trao đổi thông tin của người sử dụng là:

- Giao thức truyền tin siêu văn bản HTTP (HyperText Transfer Protocol) được sử dụng để truyền các tệp tạo nên trang web của World Wide Web.

- Giao thức FTP - File Transfer Protocol đươợc sử dụng để thực hiện truyền file.
- Giao thức SMTP - Simple Mail Transfer Protocol đươợc sử dụng để truyền các thông điệp thư và các tệp đính kèm.
- Telnet, một giao thức mô phỏng trạm đầu cuối, được sử dụng để đăng nhập từ xa vào các máy trạm trên mạng.




Hình I-8 Các giao thức của TCP/IP

**Chuẩn mạng máy tính(network standards)**

Tình trạng không tương thích gữa các mạng đặc biệt là các mạng trên thị trường gây trở ngại cho những người sử dụng khác nhau. Do đó cần phải xây dựng mô hình chuẩn làm cơ sở cho các nhà nghiên cứu, thiết kế mạng để tạo ra các sản phẩm mới về mạng, dễ phổ cập, sản xuất, sử dụng. Các chuẩn có vai trò quan trọng trong công tác thiết kế và xây dựng các hệ thống kỹ thuật và công nghệ.

*Chuẩn hóa mạng máy tính là nêu ra các tiêu chuẩn cơ bản thống nhất về cấu trúc mạng giúp cho các mạng khác nhau có thể trap đổi thông tin được với nhau.*

Để mạng hoạt động đạt khả năng tối đa, các tiêu chuẩn được chọn phải cho phép mở rộng mạng để có thể phục vụ những ứng dụng không dự kiến trước trong tương lai tại lúc lắp đặt hệ thống và điều đó cũng cho phép mạng làm việc với những thiết bị được sản xuất từ nhiều hãng khác nhau.

Một số tổ chức thực hiện chuẩn hóa mạng:

1. ISO (*International Standards Organization* – Tổ chức chuẩn hóa quốc tế) hoạt động dưới sự bảo trợ của LHQ. Thành viên của ISO là các cơ quan tiêu chuẩn hóa của các quốc gia và các ban chuyên môn. Ban TC97 được chia ra thành các tiểu ban và các nhóm công tác.

2. IEEE (*Institute of Electrical and Electronic Engineers* - Viện nghiên cứu các vấn đề về kỹ thuật điện và điện tử Mỹ) chịu trách nhiệm về tầng Data Link và physical. Phân ban các chuẩn này là phân ban 802 ( thành lập tháng 2 năm 1980)
3. CCITT (*Commite Consultatof Intẻnational pour Télégraphe et Téléphone*- Tổ chức tư vấn quốc tế về điện báo và điện thoại) hoạt động dưới sự bảo trợ của LHQ, chuyên nghiên cứu nhằm công bố các khuyến nghị thống nhất về mạng máy tính. Bao gồm các khuyến nghị liên quan đến việc truyền dữ liệu trên mạng, mạng ISDN.
4. ANSI (*American National Standards Institute)* – Viện nghiên cứu các chuẩn quốc gia Mỹ).
5. ECMA (*European Computer Manufactures Association)* – Hiệp hội máy tính Châu Âu.
6. ATM Forum (*Asynchronous Transfers Mode)* - Thực hiện các giải pháp cho mạng ISDN.
7. IETF (*Internet Enggineering Task Force)* - Sản xuất các chuẩn liên quan đến Internet (SNMP, TCP/IP…)

## I.5. Hệ điều hành trong môi trường mạng

Việc lựa chọn hệ điều hành mạng (NOS – Network Operating System) làm nền tảng cho mạng phụ thuộc vào kính cỡ của mạng hiện tại và sự phát triển trong tương lai, ngoài ra còn tùy thuộc vào những ưu điểm và nhược điểm của từng hệ điều hành.

Một số hệ điều hành mạng phổ biến hiện nay:

- Hệ điều hành UNIX: là hệ điều hành do các nhà khoa học xây dựng và được dùng phổ biến trong giới khoa học, giáo dục. Hệ điều hạnh mạng UNIX là hệ điều hành đa nhiệm, đa người sử dụng, phục vụ cho truyền thông tốt. Nhược điểm của nó là hiện nay có nhiều version khác nhau, không thống nhất gây khó khăn cho người sử dụng và hệ điều hành này phức tạp.
- Hệ điều hành mạng Windows 2000: là hệ điều hành của hãng Microsoft, cũng là hệ điều hành đa nhiệm, đa người sử dụng. Được xây dựng dựa trên công nghệ của hệ điều hành Windows NT. Đặc điểm của nó tương đối dễ sử dụng , hỗ trợ mạnh cho phần mềm WINDOWS. Windows 2000 có thể liên kết tốt với máy chủ Novell Netware, Unix. Tuy nhiên, để chạy có hiệu quả, Windows 2000 Server đòi hỏi cấu hình máy tương đối mạnh. Phiên bản tiếp theo là hệ điều hành Windows Server 2003.
- Hệ điều hành mạng NetWare: là hệ điều hành của hãng Novell, nó có thể dùng cho các mạng nhỏ (khoảng từ 5 – 25 máy tính) và cũng có thể dùng cho các mạng lớn gồm hàng trăm máy tính. Netware là hệ điều hành LAN

dùng cho các máy tính theo chuẩn IBM hay các máy Apple Macintosh, chạy trên hệ điều hành MS-DOS hoặc OS/2.

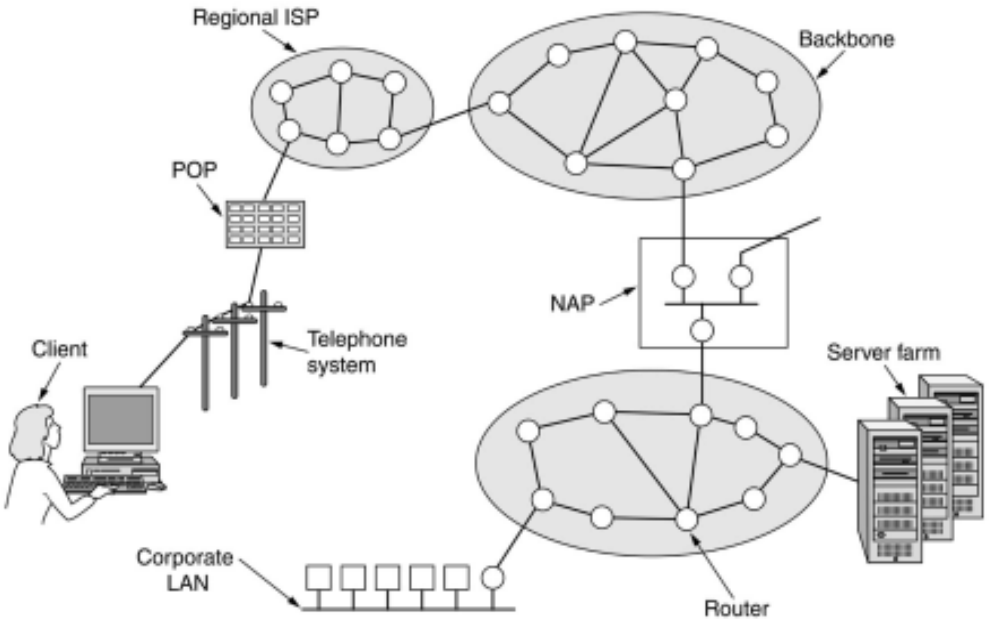
## I.6. Mạng Internet

Vào những năm 60 thế kỷ 20, Bộ Quốc phòng Mỹ cho triển khai một mạng lưới thông tin với yêu cầu: nếu như một trạm trung chuyển nào đó trong mạng bị phá hủy, toàn bộ hệ thống thông tin vẫn hoạt động bình thường… Cơ quan Nghiên cứu Dự án Cao cấp (ARPA – Advanced Research Projects Agency) thuộc Bộ Quốc phòng Mỹ được giao trách nhiệm thực hiện việc nghiên cứu kỹ thuật liên mạng(internet) nhằm đáp ứng yêu cầu trên. Đây là mạng chuyển mạch gói (paket switching) đầu tiên trên thế giới, lấy tên là ARPAnet. Ban đầu, ARPAnet chỉ gồm một vài mạng nhỏ được chọn lựa của các trung tâm nghiên cứu và phát triển khoa học. Giao thức truyền thông lúc bấy giờ là kiểu *điểm- điểm*, rất chậm và thường xuyên gây tắc nghẽn trên mạng. Để giải quyết vấn đề này, vào năm 1974 Vinton G. Cerf và Robert O. Kahn đưa ra ý tưởng thiết kế một bộ giao thức mạng mới thuận tiện hơn, đó chính là tiền thân của giao thức TCP/IP.

Tháng 09/1983, dưới sự tài trợ của Bộ Quốc phòng Mỹ, Berkeley Software Distribution đưa ra bản Berkeley UNIX 4.2BSD có kết hợp giao thức TCP/IP. biến TCP/IP thành phương tiện kết nối các hệ thống UNIX. Trên cơ sở đó , mạng ARPANET nhanh chóng lan rộng và chuyển từ mạng thực nghiệm sang hoạt động chính thức: nhiều trường đại học, viện nghiên cứu ghi tên gia nhập để trao đổi thông tin. Đến năm 1984, mạng ARPANET được chia thành hai nhóm là MILNET, dành cho Quốc phòng và nhóm mạng thứ hai vẫn gọi là ARPANET, dành cho nghiên cứu và phát triển. Hai nhóm này vẫn có mối liên hệ trao đổi dữ liệu với nhau qua giao thức TCP/IP và được gọi chung là Internet.

Mạng Internet đã và đang trở thành phương tiện trao đổi thông tin toàn cầu, là phương thức thông tin nhanh với lưu lượng truyền tải dữ liệu rất lớn. Thông qua Internet mà các nhà nghiên cứu khoa học kỹ thuật, các cơ quan giáo dục đào tạo, các nhà doanh nghiệp,… có thể trao đổi thông tin với nhau, hoặc truy cập thông tin của nhau về các công trình, các lĩnh vực nghiên cứu mới nhất; về các phương pháp, hình thức giáo dục và đào tạo, về các thông tin kinh tế, thị trường giá cả,… một cách nhanh chóng, thuận tiện và dễ dàng.

Mạng Internet không phải là một mạng đơn mà là bao gồm nhiều mạng con (sub-network) được kết nối với nhau thông qua các cổng (gateway). Thuật ngữ mạng con ở đây mang nghĩa một *đơn vị mạng hoàn chỉnh* trong hệ thống mạng lớn. Mạng con hoàn toàn có thể là một mạng WAN với quy mô quốc gia và có khả năng hoạt động độc lập với Internet. Do giao thức TCP/IP không phụ thuộc lớp vật lý, các mạng con có thể sử dụng những công nghệ ghép nối khác nhau (như Ethernet, X.25,...) mà vẫn giao tiếp được với nhau.




Hình I-9.Mô hình mạng Internet

Các cổng được dùng để nối các mạng con tạo thành mạng lớn.

Có hai cách kết nối mạng như sau:

- Máy con nối trong mạng LAN( hay WAN) và mạng này nối với Internet
- Máy con nối đến một trạm cung cấp dịch vụ Internet (Internet Service Provider), thông qua đó kết nối vơi Internet. Các trạm ISP lại kết nối với Internet thông qua IAP (Internet Access Provider). Một IAP có thể làm luôn chức năng của ISP nhưng ngược lại thì không.

# Chương II. Tầng vật lý

## II.1. Chức năng

Tầng vật lý cung cấp phương thức truy cập vào đường truyền vật lý để truyền các dòng bit không cấu trúc, ngoài ra nó cung cấp các chuẩn về điện, dây cáp, đầu nối, kỹ thuật nối mạch điện, điện áp, tốc độ cáp truyền dẫn, giao diện nối kết và các mức nối kết..

## II.2. Môi trường truyền tin

Mục đích lắp đặt cáp là đảm bảo dung lượng (tốc độ) cần thiết cho các nhu cầu truyền thông trên mạng. Để hệ thống cáp hoạt động ổn định, người quản trị mạng cần cân đối các yếu tố sau:

- Tốc độ truyền lớn nhất của hệ thống cáp hiện hành, khả năng nâng cấp.
- Nhu cầu về tốc độ truyền thông trong những năm tới (5-10 năm) là bao nhiêu.
- Chọn những loại cáp nào có trên thị trường.
- Chi phí để lắp đặt cáp dự phòng.

Việc kết nối vật lý một máy tính vào mạng được thực hiện bằng cách cắm một card giao tiếp mạng NIC (Network Interface Card) vào khe cắm của máy tính và nối với cáp mạng. Sau khi kết nối vật lý hoàn tất, việc quản lý truyền tin giữa các trạm trên mạng phục thuộc vào phần mềm mạng.

NIC sẽ chuyển gói dữ liệu vào mạng LAN, gói tin được truyền đi như một dòng các bit dữ liệu thể hiện bằng các biến thiên tín hiệu điện. Khi nó chạy trong cáp dùng chung, mọi trạm gắn với cáp đều nhận tín hiệu này. NIC ở mỗi trạm sẽ kiểm tra địa chỉ đích trong tín hiệu đầu của gói để xác định đúng địa chỉ cần đến, đích ở trạm đó sẽ sao chép gói tín hiệu rồi lấy dữ liệu ra khỏi khung tin và đưa vào máy tính.

Đặc tính của cáp bao gồm sự nhạy cảm với nhiễu của điện, độ mềm dẻo và khả năng uốn nắn để lắp đặt, cự ly truyền dữ liệu và tốc độ truyền (Mbps).

Có ba nhóm cáp chính được sử dụng để nối hầu hết các mạng

- Cáp đồng trục (Coaxial)
- Cáp xoắn đôi (Twisted-pair)
- Cáp quang (Fiber Optic)

### II.2.1. Card mạng

Card mạng, còn được gọi là card giao tiếp mạng-NIC, được lắp đặt tại mỗi máy trong mạng cục bộ. Card này có nhiệm vụ chuyển dữ liệu từ máy tính vào cáp mạng và ngược lại. Quá trình này chính là sự chuyển đổi từ tín hiệu số của máy tính thành tính hiệu điện hay quang được truyền trên cáp mạng. Đồng thời card mạng cũng thực hiện chức năng tổ hợp dữ liệu thành các gói và xác định nguồn đích của gói.

Hình II-1 Card giao tiếp mạng

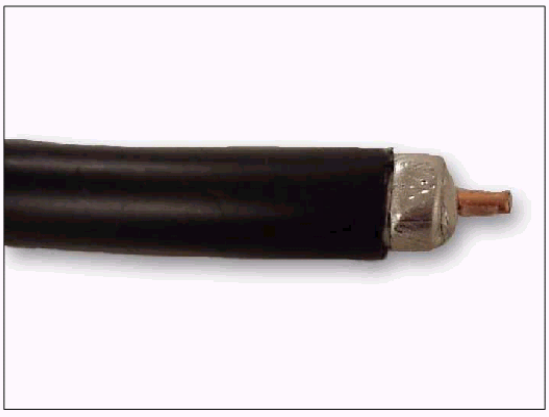
Các loại đầu nối cho cáp mạng:

- Mạng Thin Enthernet sử dụng các đầu cáp đồng trục BNC.
- Mạng Thick Net sử dụng jack nối AUI 15 chân để cắm vào đầu DB 15 của card mạng.
- Mạng Ethernet Twisted-pair sử dụng đầu nối RJ45.

### II.2.2. Cáp đồng trục:

Cáp đồng trục được chế tạo gồm một dây đồng ở giữa chất cách điện, xung quanh chất cách điện được quấn bằng dây bên kim loại làm dây đất. Giữa dây đồng dẫn điện và dây đất có một lớp cách ly, ngoài cùng là vỏ bọc bảo vệ.

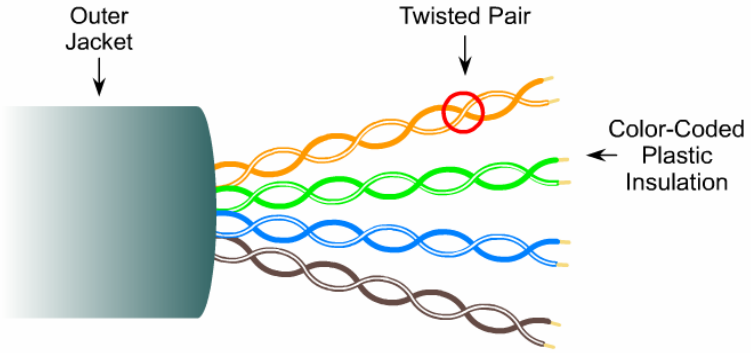
Cáp đồng trục có hai loại : loại nhỏ (Thin) và loại to (Thick).



Hình II-2 Cáp đồng trục

### II.2.3. Cáp xoắn cặp:

Cáp xoắn gồm hai sợi dây đồng được xoắn cách điện với nhau. Nhiều đôi dây cáp xoắn gộp với nhau và được bọc chung bởi vỏ cáp hình thành cáp nhiều sợi. Loại cáp này có đặc tính là dễ bị ảnh hưởng của nhiễu điện nên chỉ truyền được dữ liệu ở cự ly khoảng 100m. Cáp xoắn đôi có hai loại là cáp xoắn đôi không có vỏ bọc(UTP) và cáp xoắn đôi có vỏ bọc(STP).




Hình II-3 Cáp xoắn đôi UTP

### II.2.4. Cáp quang:

Khi tín hiệu số được điều chế thành các tín hiệu xung ánh sáng thì được truyền tải qua cáp quang. Cáp quang bao gồm một sợi thủy tinh cực mảnh gọi là lõi (core), được bao phủ bởi lớp thủy tinh đồng tâm gọi là lớp vỏ bọc hay lớp phủ (cladding). Đôi khi các sợi được làm bằng chất dẻo. Chất dẻo dễ lắp đặt hơn nhưng không thể mang xung ánh sáng đi xa như thủy tinh.

Mỗi sợi thủy tinh chỉ truyền được tín hiệu theo một hướng nhất định, do đó cáp thường có 2 sợi nằm trong vỏ bọc riêng biệt: một sợi truyền và một sợi nhận. Cáp quang có thể truyền tín hiệu đi xa với tốc độ cực nhanh (theo lý thuyết cáp quang có thể truyền tín hiệu với tốc độ tối đa 200.000 Mbps).

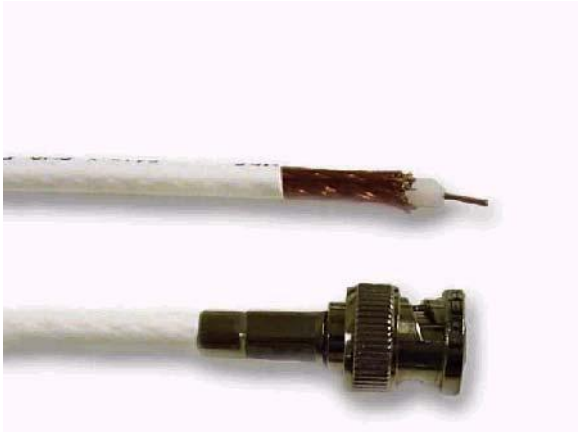
## II.3. Đặc tả các loại cáp mạng

Thông thường đặc điểm kĩ thuật của cáp mạng gồm có:

- Tốc độ truyền dữ liệu tối đa. Đây là đặc điểm quan trọng và ảnh hưởng bởi vật liệu chế tạo cáp.
- Loại dữ liệu truyền. Có hai kĩ thuật truyền tín hiệu mã hóa lên mạng là truyền ở dải tầng gốc (baseband) và truyền ở dải tầng rộng (boardband).
- Tín hiệu có thể truyền bao xa trên loại cáp cụ thể trước khi bị suy giảm

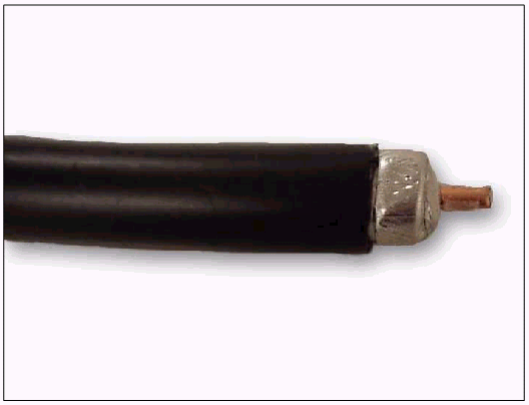
Một số ví dụ:

- 10BASE2
  - Tốc độ truyền dẫn 10 Mbps
  - Loại dữ liệu truyền là dải tầng gốc (kĩ thuật số)
  - Khoảng cách tối đa giữa hai nút là 200 m, còn gọi là cáp Thinnet



Hình II-4 Cáp ThinNet

- 10BASE5
  - Tốc độ truyền dẫn 10 Mbps
  - Loại dữ liệu truyền là dải tầng gốc (kĩ thuật số)
  - Khoảng cách tối đa giữa hai nút là 500 m, còn gọi là cáp Thicknet



Hình II-5 Cáp ThickNet

- 100BASET
  - Tốc độ truyền dẫn 100 Mbps
  - Loại dữ liệu truyền là dải tầng gốc (kĩ thuật số)
  - Là cáp xoắn đôi.

Hình II-6 Cáp xoắn đôi

## II.4. Chuẩn giao diện

### II.4.1. Modem:

Modem là bộ điều chế và giải điều chế, biến đổi các tín hiệu số thành tín hiệu tương tự và ngược lại trên mạng điện thoại.

Tín hiệu số từ máy tính đến modem, được modem biến đổi thành tín hiệu tương tự để có thể đi qua mạng điện thoại. Tín hiệu này đến modem ở máy tính đầu kia, được biến đổi thành tín hiệu số đưa vào máy tính này.

Các kỹ thuật điều chế cơ bản:

- Điều chế biên độ AM: Các tín hiệu 0 và 1 được phân biệt bằng biên độ, còn tầng số của tín hiệu giống nhau. Điều chế biên độ dễ thực hiện nhưng dễ bị nhiễu.
- Điều chế tần số FM: Các tín hiệu 0 và 1 được phân biệt bởi tần số, còn biên độ tín hiệu giống nhau. Kỹ thuật này phức tạp hơn nhưng tính chống nhiễu cao.
- Điều chế theo pha PM: Các tín hiệu 0 và 1 được phân biệt theo pha của dao động, còn biên độ và tần số của các tín hiệu giống nhau. Điều pha cũng phức tạp nhưng tính chống nhiễu cao.

Để tăng tốc độ truyền tin người ta kết hợp điều pha và điều biên gọi là điều pha biên.

Hiện nay có nhiều loại modem từ loại thấp 300, 600, 1200, 2400 bit/s đến loại 9600 bit/s.

Các phương thức truyền dữ liệu giữa hai điểm có thể là:

- Một chiều đơn (simplex).

- Hai chiều luân phiên (half-duplex).
- Hai chiều đầy đủ (duplex)

### II.4.2. DTE và DCE:

DTE (Data Terminal Equipment-Đầu cuối số liệu): là các khái niệm được sử dụng để chỉ các máy mà người sử dụng bình thường thao tác trực tiếp lên đó. Các máy này có thể là máy tính hay trạm cuối.

DCE (Data Communication Equipment-Đầu cuối truyền): là khái niệm chỉ các thiết bị cuối kênh dữ liệu có chức năng nối các DTE với các đường truyền vật lý và chuyển đổi dữ liệu. DCE có thể là các modem, multiplexer,..

# Chương III. Giao thức tầng liên kết dữ liệu

## III.1. Chức năng và dịch vụ

### III.1.1. Chức năng

Tầng liên kết dữ liệu (Data link) thực hiện các công việc chính như sau:

- Định danh các thiết bị trên mạng, cấu hình logic của mạng.
- Điều khiển luồng dữ liệu và việc truy nhập ở tầng vật lý
- Phát hiện và chỉnh sửa các lỗi xuất hiện trong quá trình truyền dữ liệu.

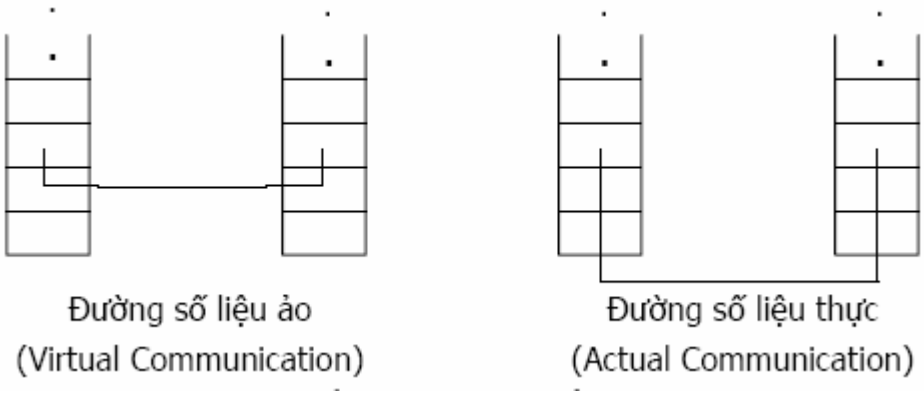
Chức năng chính của tầng LKDL là tách rời các khung thành các bit để truyền đi và kiến tạo các khung (frames) từ các dòng bit nhận được.

Tầng LKDL nghiên cứu các thuật toán thực hiện thông tin hiệu suất, tin cậy giữa hai máy cạnh nhau ở tầng 2. Đưa ra các thủ tục truyền tin có lưu ý đến lỗi có thể xảy ra do nhiễu trên đường dây, sự trễ do lan truyền.

Thông thường, tầng LKDL có liên quan đến nhiễu của tín hiệu của phương tiện truyền vật lý, cho dù là truyền qua dây đồng, cáp quang hay truyền thông qua sóng ngắn. Nhiễu là một vấn đề rất thông thường và có thể do rất nhiều nguồn khác nhau, trong đó có cả nhiễu của các tia vũ trụ, nhiễu do tạp âm của khí quyển và từ các nguồn khác nhau.

### III.1.2. Cung cấp dịch vụ cho tầng mạng

Tầng 2 chuyển dữ liệu từ mức 3 ở máy nguồn tới mức 3 của máy nhận.




Hình III-1. Đường truyền dữ liệu trong tầng LKDL.

Các dịch vụ tầng 2 có thể là:

1. Dịch vụ không kết nối, không hồi báo (*Unacknowledged Connectionless Service)*
2. Dịch vụ không kết nối, có hồi báo (*Acknowledged Connectionless Service)*
3. Dịch vụ có kết nối *(Connection Oriented Service)*

Dịch vụ kết nối có hường gồm 3 giai đoạn: *kết nối, truyền số liệu, tách bỏ liên kết* (kết thúc): CONECT, DATA, DISCONNECT. Dịch vụ không kết nối được thể hiện bằng một bước duy nhất là truyền tin, không cần thiết lập liên kết logic. Các đơn vị dữ liệu truyền độc lập với nhau.

### III.1.3. Khung tin - Nhận biết gói tin

Để cung cấp dịch vụ cho tầng mạng, tầng LKDL phải dùng dịch vụ được cung cấp từ tầng vật lý. Tầng vật lý tiếp nhận dòng bit và giao cho nơi nhận. Dòng bit này có thể có lỗi. Tầng LKDL sẽ kiểm tra và nếu cần sẽ sửa lỗi.

Tầng LKDL tách dòng bit thành các khung (flame) và tính thông số kiểm tra (checksum) cho mỗi khung tin này, nếu kết quả tính được khác với checksum chứa trong khung tin, nghĩa là có lỗi và khi đó lỗi sẽ được thông báo cho nơi gởi.

Muốn tách các khung tin, có thể chèn các đoạn phân tách (timegaps) vào giữa các khung tin, giống như khoảng trống (space) giữa các từ trong văn bản. Nhưng điều này khó thực hiện nên người ta thường dùng các phương pháp sau:

- Đếm số ký tự: hiện nay ít được dùng vì từ đếm cũng bị lỗi khi truyền.
- Dùng ký tự bắt đầu (STX) và kết thúc (ETX) với ký tự đệm (DLE).
- Dùng các cờ (*flags)* đánh dấu bắt đầu và kết thúc với các bít đệm.

### III.1.4. Điều khiển dòng truyền

Để tận dụng đường dây, các tín hiệu biên nhận (ACK) được ghép cùng với gói tin. Khi gói tin đến, thay cho việc trả lời ngay tín hiệu bên nhận, bên thu nhận tiếp gói tin từ mạng để ghép cùng tín hiệu biên nhận và gởi trả lời. Kỹ thuật này được gọi là Piggybacking (ghép thêm).

Ưu điểm của phương pháp này là tận dụng đường kênh. Nếu quá thời gian (vài μs) mà không có gói tín hiệu mới thì bên thu phải trả lời tín hiệu biên nhận để bên phát lại không phát lại gói tin cũ.

Để tận dụng đường kênh, bên phát và bên thu phải đồng bộ để bên thu kịp nhận các gói tin và bên phát cũng không lãng phí đường truyền, người ta dùng cơ chế cửa sổ trượt (sliding windows). Cửa sổ mở to thì số gói tin đưa lên đường kênh nhiều hơn (tốc độ nhanh), cửa sổ mở bé thì số gói kênh đưa lên đường kênh ít lại (tốc độ chậm lại). Tương tự như cửa chắn đập nước.

## *1. Cơ chế cửa sổ*

Người ta dùng số bit để đặc trưng cho độ rộng cực đại của cửa sổ. Trong thủ tục này, mỗi gói tin đi sẽ được đánh số từ 0 đến Max (Max là $2^n - 1$) thông qua một dãy gồm các số 0, 1. Chẳng hạn cửa sổ 3 bit sẽ quản lý các gói tin có số từ 0Ặ 7. Ta có thể dùng n tùy ý.

Danh sách các gói tin gởi đi trong cửa sổ phát. Danh sách các gói tin nhận được gởi trong cửa sổ nhận, cửa sổ phát và nhận không bắt buộc phải có kích thước, giới hạn trên và dưới giống nhau.

Mặc dù thủ tục này cho phép tầng liên kết dữ liệu linh hoạt hơn về thứ tự gởi, nhận gói tin nhưng nó yêu cầu phải đảm bảo tầng mạng đích ở bên nhận có cùng thứ tự với tầng mạng nguồn ở bên gửi.

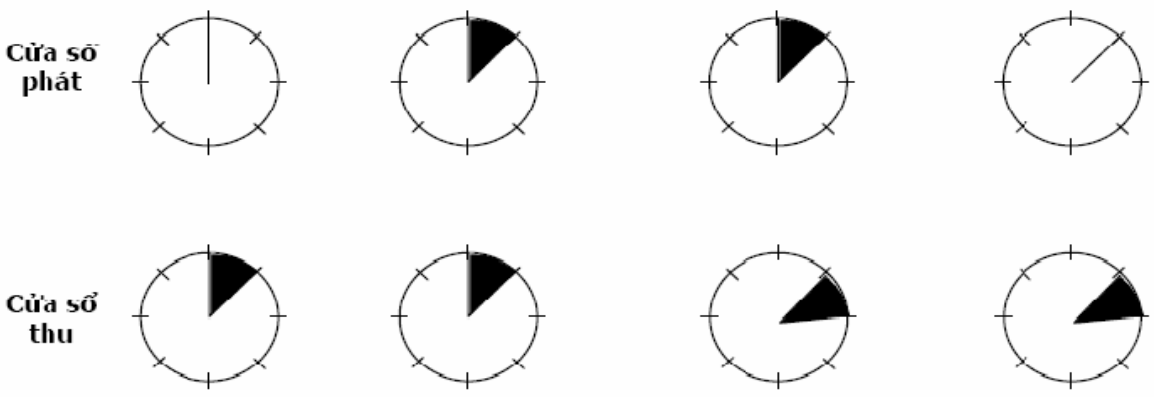
- ***Cửa sổ bên phát***

Trong cửa sổ bên phát đặt các gói tin gởi đi nhưng chưa nhận được tín hiệu biên nhận. Khi nhận được gói tin mới đến từ tầng mạng để phát đi, biên trên cửa sổ tăng 1 và khi có tín hiệu biên nhận biên dưới của cửa sổ tăng 1. Bên phát luôn giữ trong bộ nhớ các gói tin đã phát đi nhưng chưa nhận được tín hiệu biên nhận vì có thể phát lại. Như vậy nếu Max bằng n thì bên phát cần n vùng đệm để các gói tin đã phát đi nhưng chưa nhận được trả lời. Nếu cửa sổ đã tới Max thì tầng liên kết giữ liệu bên phát ngừng nhận tin từ tầng 3 cho đến khi có bộ đệm tự do.

- ***Cửa sổ bên nhận***

Cửa sổ bên nhận chứa các gói tin được chuyển đến. Khi gói tin có số thứ tự trùng biên dưới của cửa sổ được nhận, cửa sổ chuyển tin lên tầng ba, phát tín hiệu biên nhận và quay một đơn vị. Không như cửa bên phát, cửa sổ bên nhận luôn duy trì một kích thước. Khi kích thước cửa sổ bằng 1, tầng 2 nhận gói tin theo thứ tự. Nhưng nếu kích thước cửa sổ lớn hơn thì không phải như vậy.

Hoạt động của cửa số có kích thước là 3 bit với độ trượt một bit như sau:

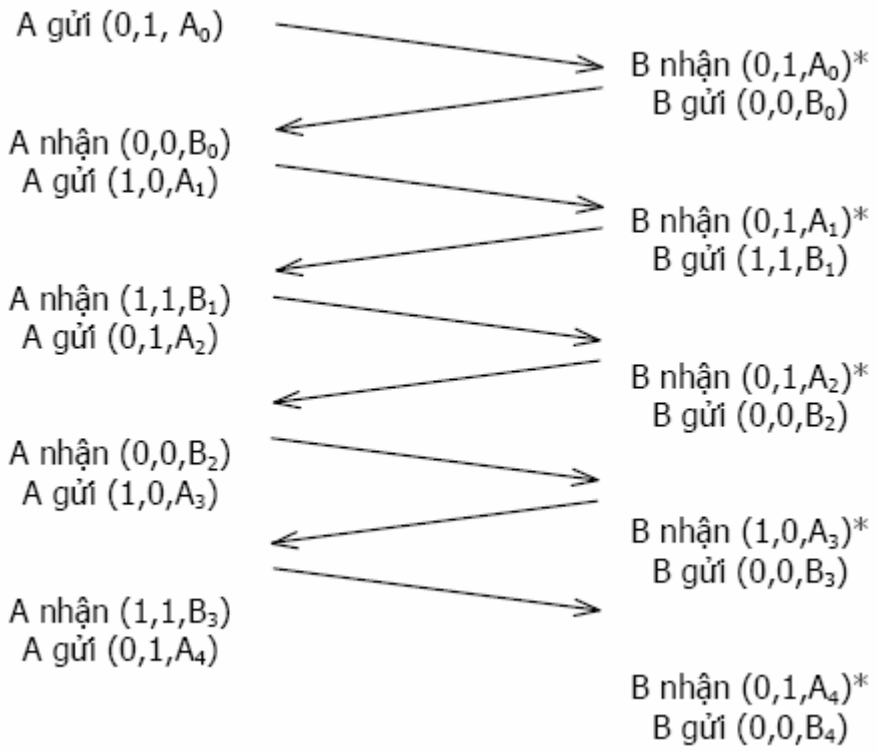



Hình III-2. Điều khiển dòng truyền theo cơ chế cửa sổ (Bắt đầu-Gửi gói tin đầu tiên-Nhận tin và trả lời ACK-Nhận ACK)

### *2. Trao đổi bản tin với cửa sổ 1 bit*

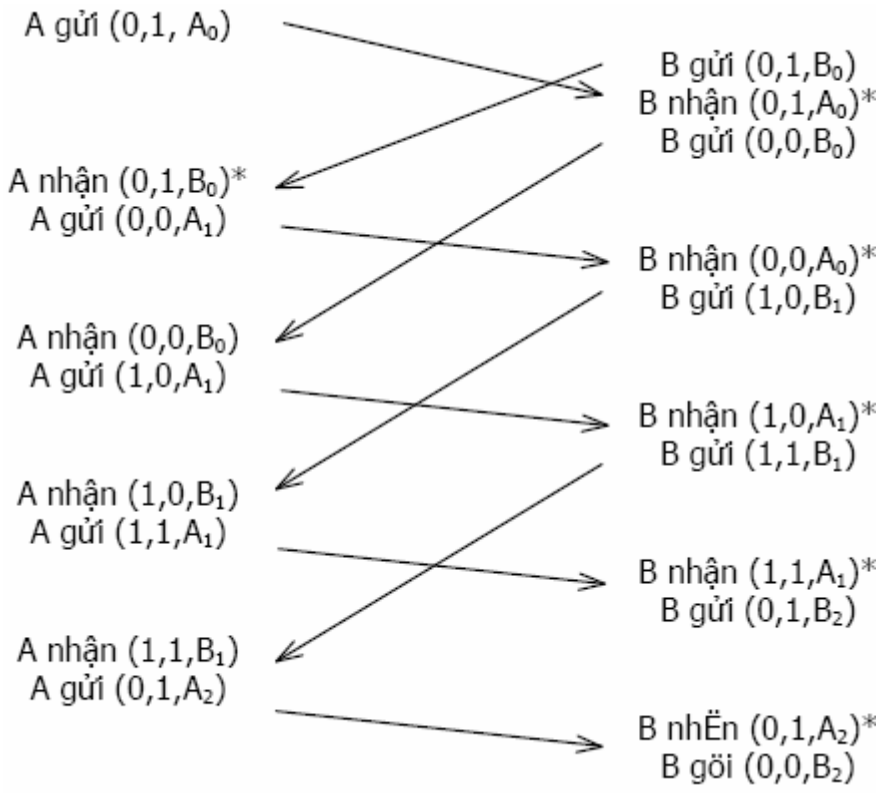
Bản tin gồm có gói tin với phần điều khiển (Header). Phần điều khiển gồm có số thứ tự phát *seg*, số thứ tự nhận của *ack*, số gói tin.

Trong trường hợp bình thường máy A gủi trước như sau:




Hình III-3. Trao đổi bản tin với cửa sổ 1 bit bình thường.

Trong truòng hợp bất thường máy A và B cùng gởi như sau:




Hình III-4. Trao đổi bản tin với cửa sổ 1 bit bất thường.

Máy A ở tầng 2 nhận gói tin ở tầng 3, tạo bản tin và gởi đi. Khi bản tin này đến tầng 2 máy B, nó sẽ được kiểm tra có bị lặp lại hay không. Nếu đúng là bản tin đang mong đợi thì nó được chuyển lên tầng 3 và cửa sổ nhận dịch đi một nấc.

Vùng tín hiệu biên nhận chứa số bản tin cuối cùng đã được nhận mà không có lỗi, nếu số này trùng với số bản tin vừa gởi, bên phát sẽ lấy bản tin tiếp theo từ tầng mạng. Nếu số không đúng nó phải gởi lại bản tin cũ.

### *3. Vận chuyển liên tục*

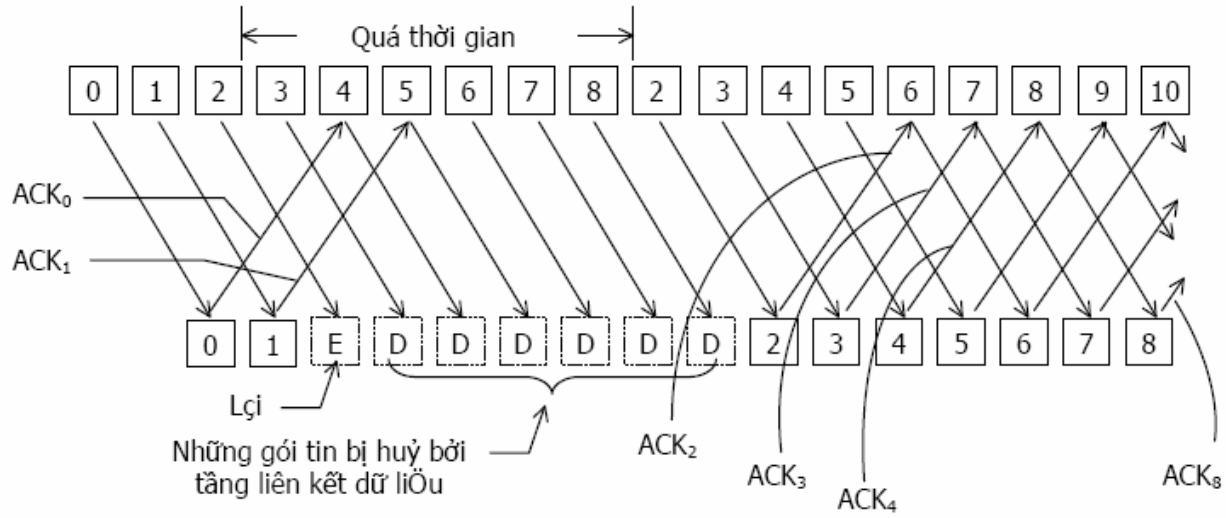
Thực tế cho thấy thời gian từ lúc phát gói tin đến khi nhận trả lời biên nhận ACK là không đáng kể. Khi đó, nếu đường kênh vệ tinh có tốc độ 50Kbp/s với trễ lan truyền 500 ms, ta dùng thủ tục điều chỉnh dòng truyền gởi gói tin là 1000 bit qua vệ tinh. Thời gian phát gói tin 20 ms, vậy sau 520 ms mới nhận được tín hiệu biên nhận cho gói tin 0 cũng vừa đến. Kỹ thuật này gọi là Pipe-Lining (vận chuyển liên tục).

Khi có gói tin ở đoạn giữa bị hỏng thì làm thế nào? Có bỏ những gói tin đúng đi tiếp sau nó không? Có hai phương pháp như sau:

- Phát lại các gói tin kể từ gói tin hỏng (*go back n)*
- Phát lại chỉ riêng gói tin bị hỏng, còn gọi phát tin có chọn lọc.
- Phát lại từ gói tin hỏng.

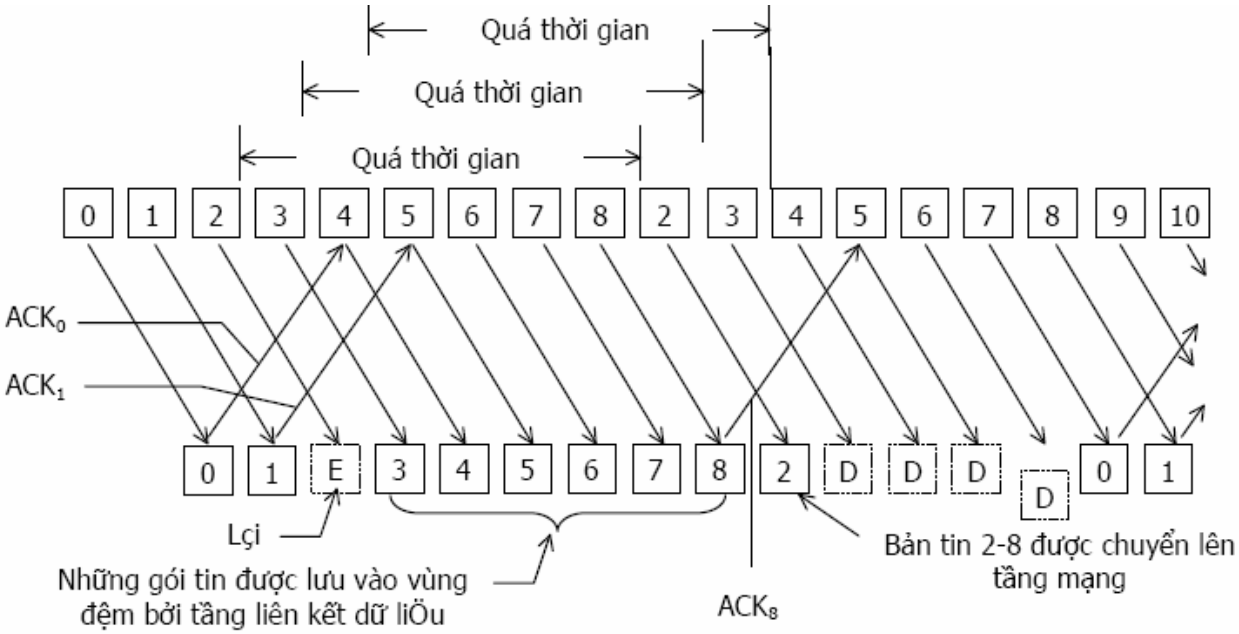
Trong trường hợp này, bên thu hủy bỏ các gói tin tiếp theo gói tin bị hỏng. Bên phát phát lại các gói tin chưa được biên nhận bắt đầu từ gói tin bị hỏng.

Phương pháp này lãng phí đường truyền vì phải phát lại nhiều gói tin.




Hình III-5. Cơ chế vận chuyển liên tục

* ***Phát lại có chọn lọc***




Hình III-6. Cơ chế phát bản tin có chọn lọc.

Trong phương pháp này, các gói tin nhận được có thể không theo thứ tự nhưng sẽ được sắp xếp lại để chuyển lên tầng mạng theo đúng thứ tự. Khi có gói tin bị lỗi, bên thu tiếp tục thu các gói tin đứng sau gói tin hỏng ở tầng 2. Bên phát chỉ phát lại gói tin hỏng. Phương pháp này ứng với cửa sổ bên thu lớn hơn 1 và đòi hỏi bộ nhớ lớn để các gói tin sau gói tin hỏng.

## III.2. Cơ chế phát hiện và sửa lỗi

Lỗi bit thường xảy ra trong frame. Mặc dù lỗi rất ít khi xảy ra, đặc biệt là trên cáp quang, tuy nhiên cần có những kỹ thuật để phát hiện lỗi khi lỗi xảy ra. Một kỹ thuật được biết trong việc phát hiện lỗi khi truyền là phương pháp kiểm tra CRC (cyclic redundancy check). Nó được sử dụng hầu hết trong các giao thức Byte-Oriented, Bit-Oriented, CSMA/CD và FDDI.

Hai phương pháp đơn giản được sử dụng rộng rãi là: two-demensional parity và checksum. Two-demensional parity được sử dụng trong giao thức BISYNC lúc nó truyền các ký tự ASCII. Checksum được sử dụng bởi một vài giao thức Internet.

Ý tưởng cơ bản của CRC là thêm các thông tin dư vào frame, thông tin này được sử dụng để phát hiện lỗi. Ví dụ chúng ta có thể truyền hai bản sao của dữ liệu, nếu hai bản sao giống nhau ở máy nhận, có thể là trong trường hợp này là cả hai đều đúng. Ngược lại, nếu hai bản sao này khác nhau thì một trong hai bản sao bị sai, do đó phải thực hiện truyền lại.

Nhược điểm của các tiếp cận trên:

- Thêm n bit dư cho một thông điệp n bit
- Không phát hiện sai nếu lỗi sai xảy ra ở cùng một vị trí.

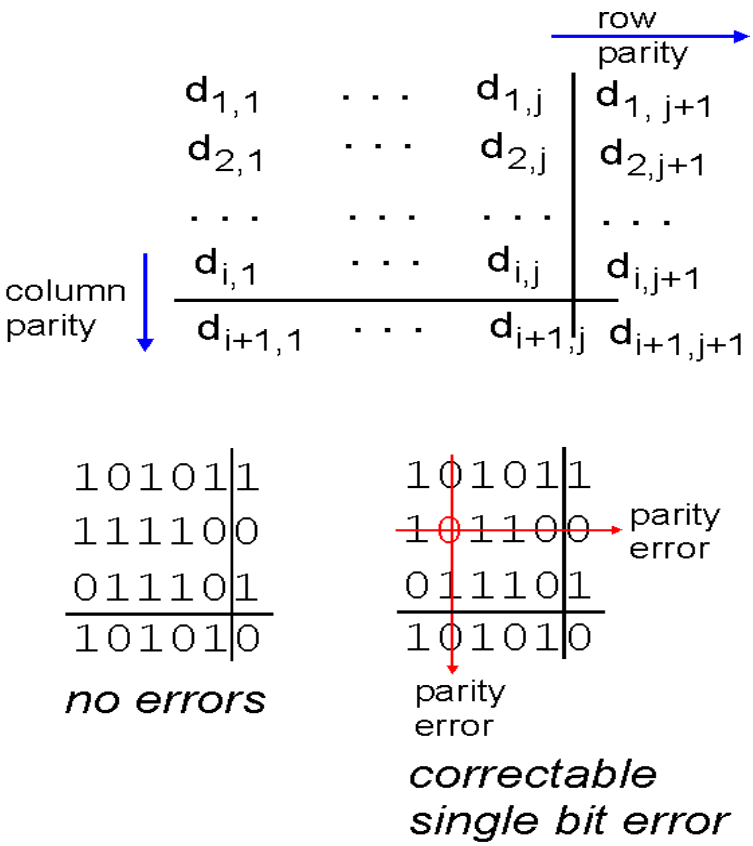
Chúng ta có thể hoàn toàn cung cấp một khả năng phát hiện lỗi tốt với việc gửi k bit dư cho một thông điệp n bit (k<<n). Ví dụ trên Ethernet, mỗi khung mang 12000 bit (1500byte) dữ liệu chỉ yêu cầu mã 32 bit CRC.

Việc thêm các bit không có nghĩa là thêm thông tin mới vào thông điệp. Thay vào đó, chúng có thể sử dụng một vài thuật toán tối ưu tác động trực tiếp vào thông điệp nguồn. Cả hai máy gửi và máy nhận biết chính xác thuật toán làm gì. Máy gửi tác động thuật toán đến thông điệp để tạo ra bit dư, sao đó nó truyền cả thông điệp và các bit dư. Máy nhận tác động cùng thuật toán vào thông điệp nhận, nếu phát hiện sai nó yêu cầu truyền lại hay sữa sai nếu có thể.

Phát hiện lỗi chỉ là một phần của vấn đề, vấn đề tiếp theo là xử lý lỗi khi lỗi được phát hiện. Có hai cách phương pháp được sử dụng lúc phát hiện một thông điệp bị lỗi.

- Thông báo cho máy gửi thông điệp bị lỗi và máy gửi sẽ truyền lại.
- Nếu lỗi chỉ xảy ra tại một số bit nào đó, một số thuật toán sẽ phát hiện lỗi và cho phép tạo lại một thông điệp đúng như ban đầu thậm chí sau khi thông điệp đã bị hỏng.

### a. Two-Dimension Parity




Hình III-7. Phương pháp Two-dimesion parity

**b. Internet Checksum**

Thuật toán này không sử dụng ở mức liên kết tuy nhiên nó cung cấp cùng chức năng với CRC và parity.

Ý tưởng: ta cộng tất cả các từ mà nó được truyền, sau đó truyền dữ liệu cùng với kết quả của phép cọng đó. Kết quả được gọi là checksum. Máy nhận thực hiện tính toán tương tự trên dữ liệu nhận và so sánh kết quả với kết quả cheksum. Nếu kết quả sai, máy nhận biết có lỗi xuất hiện. Thông thường người ta xem dữ liệu bị checksum là các số nguyên 16 bit, cộng tất cả các số nguyên này lại và ta được được kết quả là một số 16 bit. Đó chính là checksum.

Ưu điểm: chỉ thêm vào 16 bit nhưng có thể kiểm tra dữ liệu chiều dài bất kỳ.

Nhược điểm: nếu một cặp bit sai ở cùng một vị trí thì chúng không thể bị phát hiện.

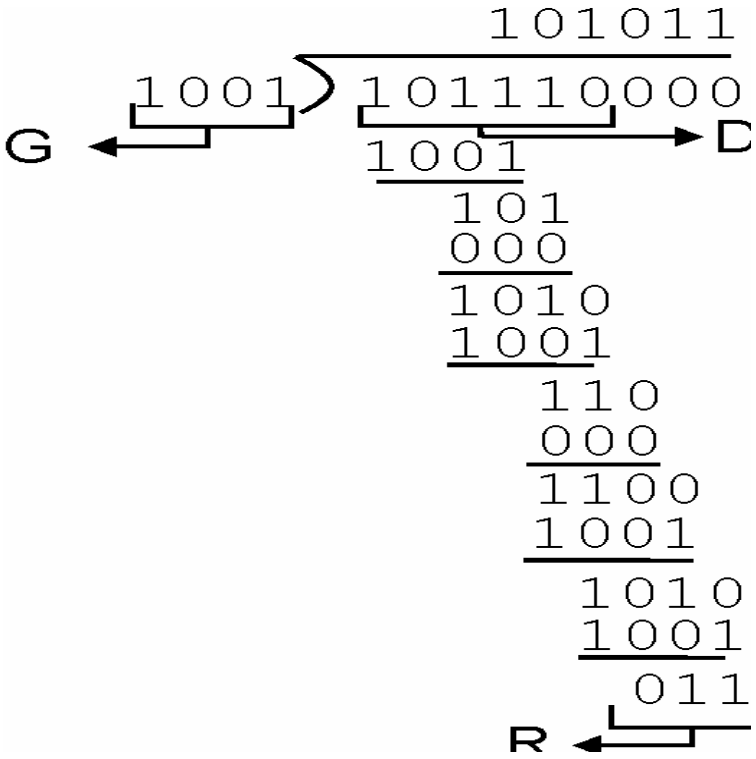
Lý do sử dụng một thuật toán này:

- Nó rất dễ cài đặt trong phần mềm. Kinh nghiệm trong APPANET thì sử dụng thuật toán checksum như thế là đầy đủ.

- Thuật toán này được bảo vệ bởi một giao thức end-to-end. Các lỗi chính hầu hết đã được phát hiện bởi các thuật toán phát hiện lỗi mạnh mẽ như là CRC tại mức liên kết.

**c. CRC**

CRC là phương pháp phát hiện lỗi thoả mãn việc sử dụng một số ít nhất các bit thêm vào nhưng có thể phát hiện tất cả các lỗi khi truyền. Ví dụ chỉ sử dụng 32 bit CRC có thể dùng để kiểm tra dữ liệu dài hàng ngàn byte.




Hình III-8. Ví dụ minh họa phương pháp CRC

**Ý tưởng:**

Một thông điệp n+1 bit có thể được biểu diễn bởi một đa thức bậc n. Đa thức sử dụng giá trị của mỗi bit trong thông điệp làm hệ số của đa thức.

Để hổ trợ cho việc tính CRC, máy gửi và máy nhận cùng sử dụng một đa thức chia. Có một nhóm các đa thức chia mà chúng là những chọn lựa rất tốt trên các các môi trường khác nhau và sự chọn lựa thường phụ thuộc vào việc thiết kế giao thức. Ví dụ Ethenet sử dụng CRC 32.

Lúc máy gửi muốn chuyển một thông điệp M(x) mà nó dài (n+1)bit, điều gì thật sự xảy ra với một thông điệp n+1 bit và k bit thêm vào.

- Gọi P(x) là đa thức gồm thông điệp truyền và bit dư.
- Nếu P(x) được truyền qua liên kết và không có lỗi xuất hiện trong quá trình truyền, thì thiết bị nhận có thể chia P(x) cho C(x) với phần

dư là 0. Ngược lại, nếu phần dư khác không thì máy nhận biết rằng có lỗi xuất hiện trong khi truyền.

Nhận xét đa thức:

- Các bậc của đa thức chỉ là 0 hoặc 1.
- B(x) có thể chia cho C(x) nếu bậc của nó cao hơn C(x).
- B(x) chỉ có thể chia một lần cho C(x) nếu mũ của chúng bằng nhau.
- Phần dư của B(x) chia cho C(x) có thể lấy từ kết quả của việc lấy B(x)-C(x).
- B(x) trừ C(x) thực chất là thực hiện phép XOR từng cặp hệ số.

**Thuật toán:**

Cộng k bit zero vào cuối thông điệp ta được thông điệp T(x).

Chia T(x) cho C(x) và tìm phần dư.

Trừ T(x) cho phần dư.

Mạng Ethernet và 802.5 sử dụng CRC 32, HDLC sử dụng CRC_CCITT. ATM sử dụng CRC-8, 10, 12.

Phương pháp kiểm tra lỗi này dễ dàng thi hành tại phần cứng, đơn giản chỉ là sử dụng thanh ghi và cổng XOR. Bảng 2.3 đưa ra một số đa thức sử dụng trong CRC.

| CRC | C(x) |
|---|---|
| CRC-8 | $x^8 + x^2 + x^1 + 1$ |
| CRC-10 | $x^{10} + x^9 + x^5 + x^4 + x^1 + 1$ |
| CRC-12 | $x^{12} + x^{11} + x^3 + x^2 + 1$ |
| CRC-16 | $x^{16} + x^{15} + x^2 + 1$ |
| CRC-CCITT | $x^{16} + x^{12} + x^5 + 1$ |
| CRC-32 | $x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$ |

## III.3. Các giao thức đa truy cập

Giao thức dùng để đánh giá khả năng của một mạng được phân chia bởi các trạm như thế nào. Hệ số này được quyết định chủ yếu bởi hiệu quả sử dụng môi trường truy xuất (medium access) của giao thức.

Mọi kênh phương tiện chỉ có thể hỗ trợ một lần tín hiệu. Nếu hai máy tính truyền trên kênh cùng một lúc, các tín hiệu của chúng sẽ gây nhiễu cho nhau (ví dụ như hai người cùng nói một lúc). Có hai phương pháp điều khiển việc truy nhập

phương tiện để không xảy ra sự cố gây nhiễu: truy cập ngẫu nhiên và truy cập có điều khiển.

*a. Loại truy cập ngẫu nhiên*

Trạm có thể truy nhập phương tiện truyền tùy theo ý muốn, bất kỳ ở thời điểm ngẫu nhiên nào.

- Kỹ thuật cập ngẫu nhiên đối với dạng bus
  - Phương pháp đa truy nhập sử dụng sóng mang (CSMA – Carrier Sense Multiple Access).
  - Phương pháp đa truy nhập sử dụng sóng mang với phát hiện xung đột ( CSMA/CD – With Collision Detection)
- Kỹ thuật cập ngẫu nhiên đối với dạng vòng
  - Phương pháp chèn thanh ghi (Registeer insertion)
  - Phương pháp vòng có ngăn (Slotted-ring)

b. *Loại truy nhập có điều khiển*

Phương pháp điều khiển tranh chấp thường thích hợp với các mạng có sự trao đổi dữ liệu không liên tục và tương đối ít máy tính. Đây là đạng thông dụng trong cấu trúc mạng cục bộ.

- Kỹ thuật bus với thẻ bài (Tocken Bus): dùng cho các mạng LAN.
- Kỹ thuật vòng với thẻ bài ( Tocken Ring): dùng cho các mạng LAN
- Kỹ thuật tránh xung đột: dùng cho các mạng cục bộ tốc độ cao

### III.3.1. Phương pháp CSMA

Còn được gọi là phương pháp LBT (Listen Before Talk – Nghe trước khi nói). Một trạm có dữ liệu cần truyền trước hết phải "nghe" xem phương tiện truyền rỗi hay bận. Nếu rỗi thì bắt đầu truyền tin, còn nếu bận thì thực hiện một trong ba giải thuật sau:

- Giải thuật '*non-persistent' :* Trạm rút lui (không kiên trì) chờ đợi một thời gian ngẫu nhiên nào đó rồi bắt đầu 'nghe' đường truyền. Giải thuật này có hiệu quả tránh xung đột nhưng có thời gian chết.
- Giải thuật '*l-persistent':* trạm tiếp tục nghe đến khi phương tiện truyền rỗi thì tiến hành truyền dữ liệu đi (với xác xuất 1). Giải thuật này giảm thời gian chết, xong nếu có nhiều trạm cùng chờ và tiến hành phát dữ liệu cùng một lần thì sẽ xảy ra xung đột.
- Giải thuật '*p-persistent':* Trạm tiếp tục nghe, đến khi phương tiện truyền rỗi thì tiến hành phát tin với một xác suất nhất định nào đo (mỗi trạm có gắn một hệ số ưu tiên). Ngược lại trạm 'rút lui' trong

một thời gian cố định rồi truyền với sác xuất p hoặc tiếp tục chờ đợi với sác xuất 1-n. Giải thuật này phức tạp nhưng giảm được tối đa xung đột và thời gian chết.

Phương pháp CSMA chỉ 'nghe trước khi nói', không có khả năng phát hiện xung đột trong quá trình truyền, dẫn đến lãng phí đường truyền.

### III.3.2. Phương pháp CSMA/CD

Phương pháp CSMA/CD có nguồn gốc từ hệ thống radio đã phát triển ở trường đại học Hawai vào khoảng năm 1970, gọi là ALOHANET, còn được gọi là phương pháp LWT ( Listen While Talk – Nghe trong khi nói). Các va chạm luôn xảy ra tại một cấp nào đó trên các mạng, với số lượng tham gia tăng theo tỉ lệ thuận khi các phiên truyền gia tăng.

Phương pháp CSMA/CD ngoài các chức năng của CSMA còn bổ xung các quy tắc sau:

- Khi đang truyền vẫn tiếp tục nghe đường dây.
- Nếu phát hiện có xung đột thì *ngừng truyền và tiếp tục gởi sóng mang* thêm một thời gian nữa để đảm bảo các trạm đều có thể nghe được sự kiện xung đột.
- Sau khi chờ đợi một thời gian ngẫu nhiên thì trạm thử truyền lại bằng cách sử dụng các phương pháp của CSMA.

Với phương pháp CSMA/CD, thời gian chiếm dụng vô ích đường truyền giảm xuống bằng thời gian dùng để phát hiện một đụng độ. CSMA/CD sử dụng ba giải thuật 'persistent' ở trên. Trong đó giải thuật '*l-persistent'* được sử dụng trong mạng Ethernet, Mitrenet và được chọn cả trong chuẩn IEEE.802. Ngoài ra mỗi chuẩn LAN còn có thêm các cơ chế bổ sung.

### III.3.3. Điều khiển truy nhập bus với thẻ bài

Các trạm trên bus tạo nên một vòng logic, được xác định vị trí theo một dãy thứ tự, trong đó trạm cuối sẽ tiếp liền ngay sau trạm đầu. Mỗi trạm được biết địa chỉ của các trạm kề sau và kề trước nó.

Thẻ bài dùng cấp phát quyền truy nhập, được lưu chuyển trong vòng logic. Khi trạm nhận được thẻ bài thì được trao quyền sử dụng phương tiện trong một thời gian xác định để truyền dữ liệu. Khi truyền xong hoặc hết thời hạn, trạm sẽ chuyển thẻ bài đến trạm kế tiếp trong vòng logic. Các trạm không sử dụng thẻ bài vẫn có mặt trên bus nhưng chúng chỉ có thể trả lời cho yêu cầu xác nhận (nếu chúng là đích của gói tin nào đó). Thứ tự vật lý của trạm trên bus là không quan trọng, độc lập với thứ tự logic.

***Các chức năng:***

- Khởi tạo vòng logic: khi thiết lập mạng hoặc khi vòng logíc bị gãy.

- Bổ sung trạm vào vòng logic (xem xét định kỳ) bằng cách mời nút đứng sau nhập vòng. Loại bỏ một trạm ra khỏi vòng logic bằng cách nối trạm trước và sau nó với nhau.
- Quản lý sai sót: trùng địa chỉ, gãy vòng (các trạm bị treo, rơi vào trạng thái chờ lẫn nhau) bởi nút giữ Token.
- Khi giữ thẻ mà không có trạm khác nhận được gói tin thì chứng tỏ nút khác đã có thẻ, lúc đó nó sẽ bỏ thẻ bằng cách chuyển sang trạng thái "nghe".
- Khi nút hoàn thành công việc, nó gởi thẻ đến nút đứng sau, nếu nút tiếp sau hoạt động thì nó gởi thể chuyển sang trạng thái bị động. Nếu ngược lại, nó gởi thẻ cho nút kế tiếp lần nữa. Nếu hai lần gởi không được thì xem như nút kế tiếp hỏng và gởi đi gói tin "tìm nút kế tiếp" để tìm nút tiếp theo.
- Nếu không thành công thì nút bị xem là có sự cố. Nút ngừng hoạt động và "nghe" trên bus.

 Định dạng khung bản tin mạng mạng Token bus

| Bắt đầu tin | Điều khiển gói tin | Địa chỉ nguồn | Địa chỉ đích | TIN | FSC | Kết thúc tin |
|---|---|---|---|---|---|---|
| 1 byte | 1 byte | 2-6 bytes | 2 - 6 bytes | | 4 bytes | 1 byte |
| | Khung tin cực đại 8191 bytes | | | Tốc độ có thể là 1; 5; 10Mbps | | |

 So sánh CSMA/CD và Token bus

- Token bus quản lý phức tạp hơn so với CSMA/CD. Trong trường hợp tải nhẹ thì không hiệu quả bằng CMSA/CD (do phải qua nhiều trạm).

- Tuy nhiên Token Bus có hiệu quả trong trường hợp tải nặng, dễ điều hòa lưu thông trên mạng Token bus. Không quy định độ dài tối thiểu của gói tin, không cần nghe trước khi nói.

### III.3.4. Điều khiển truy cập vòng với thẻ bài

Đây là giao thức thông dụng được dùng trong các LAN có cấu trúc vòng (Ring). Phương pháp này sử dụng một khối tín hiệu đặc biệt gọi là Token di chuyển vòng quanh mạng theo một chiều xác định. Một trạm muốn truyền phải đợi cho đến khi nhận được thẻ bài. Khi một trạm đang chiếm token thì nó có thể phát đi một gói dữ liệu. Khi đã phát hết gói dữ liệu cho phép hoặc không còn gì để phát nữa thì trạm đó chuyển sang khung thẻ bài đến cho trạm kế tiếp trên mạng. Trong Token có chứa một địa chỉ đích và được luân chuyển tới các trạm theo một trật tự đã định trước. Đối với cấu hình dạng xoay vòng thì trất tự của sư truyền Token tương đương với trật tự vật lý của các trạm xung quanh vòng.

Các chuẩn mạng sử dụng phương pháp điều khiển truy nhập thẻ bài:

- Chuẩn IEEE 802.5 còn gọi là chuẩn Token Ring.
- FDDI là chuẩn sợi quang 100Mpb sử dụng phương pháp chuyển thẻ bài và vòng tròn.

Phương pháp chuyển thẻ bài thích hợp trong các điều kiện như sau:

- Khi mạng đang tải dữ liệu quan trọng về thời gian do phương pháp này cung cấp khả năng bàn giao.
- Khi mạng được sử dụng nhiều, do tránh được xung đột.
- Khi một vài trạm có mức ưu tiên cao hơn so với các trạm khác. Phương pháp chuyển thẻ bài có thể áp dụng các mức ưu tiên cho trạm để ngăn cấm một trạm bất kỳ không được độc quyền về mạng.
- Do thẻ bài luân chuyển quanh mạng nên mỗi mạng có thể truyền theo quãng thời gian tối thiểu.

Phương pháp chuyển thẻ bài đòi hỏi cơ chế điều khiển phức tạp và chi phí đầu tư phần cứng cao, nhưng được thiết kế với độ tin cậy cao. Tuy vậy hiện nay Ethernet vẫn là chuẩn LAN thông dụng, chứng tỏ được ưu điểm của phương pháp tranh chấp khi sử dụng trên các mạng LAN.

Giao thức truyền Token có trật tự hơn nhưng cũng phức tạp hơn CSMA/CD, có ưu điểm là vẫn hoạt động tốt khi lưu lượng truyền thông lớn. Giao thức truyền Token tuân thủ đúng sự phân chia của môi trường mạng, hoạt động dựa vào việc xoay vòng bị đứt đoạn. Giao thức phải chứa thủ tục kiểm tra Token để cho phép khôi phục lại oken bị mất hoặc thay thế trạng thái của Token và cung cấp các phương tiện để sửa đổi logic (thêm vào, bớt đi hoặc định lại trật tựu của các trạm)

Khung tin cực đại 16KB ở chế độ truyền 16Mps và 4KB ở chế độ truyền 4Mps.

Dạng bản tin mạng Token Ring:

| Bắt đầu tin | Điều khiển thâm nhập | Điều khiển gói tin | Địa chỉ nguồn | Địa chỉ đích | TIN | FSC | Kết thúc gói tin | Trạng thái gói tin |
|---|---|---|---|---|---|---|---|---|
| 1 byte | 1 byte | 2-6 bytes | 2 - 6 bytes | 2 - 6 bytes | | 4 bytes | 1 byte | 1 byte |

**Phương pháp điều khiển truy nhập dò báo**

Dò báo (polling) là một phương pháp điều khiển truy cập sử dụng một thiết bị trung tâm điều khiển toàn bộ việc truy nhập mạng. Đây là phương pháp được sử dụng phổ dụng nhất trên các mạng máy tính lớn.

Thiết bị trung tâm có tên là thiết bị chính sẽ yêu cầu dữ liệu từ các thiết bị khác trên mạng có tên là thiết bị thứ cấp (secondary). Sau khi được dò báo thiết bị thứ cấp có thể truyền một dữ liệu được xác định bởi các giao thức dùng trên mạng. Một thiết bị thứ cấp không thể truyền trừ khi nó được thiết bị chính dò báo.

Phương pháp dò báo có nhiều ưu điểm của phương pháp chuyển thẻ bài như:

- Dự đoán được các lần truy cập định sẵn.
- Gán được các mức ưu tiên, tránh được va chạm.

So sánh phương pháp dò báo và phương pháp chuyển thẻ bài : kỹ thuật dò báo tập trung hóa quyền điều khiển. Nhìn dưới góc độ quản lý thì đây là một ưu điểm, nhưng nếu cơ chế điều khiển trung tâm bị hỏng, mạng sẽ ngừng hoạt động. Phương pháp chuyển thẻ bài sử dụng các chức năng điều khiển phân phối hơn do đó ít bị hỏng tập trung tại một điểm. Bên cạnh đó, phương pháp dò báo đôi khi lãng phí các lượng băng thông lớn do phải dò báo từng thiết bị thứ cấp, cho dù các thiết bị không có gì để truyền.

## III.4. Khái niệm mạng LAN

### III.4.1. Các cấu trúc của mạng LAN

Cấu trúc (topology) của mạng là cấu trúc hình học không gian, thực chất là cách bố trí phần tử của mạng cũng như cách thức nối giữa chúng với nhau. Thông thường có 3 dạng cấu trúc là: mạng dạng hình sao (Star topology), mạng dạng vòng (Ring topology) và mạng dạng tuyến (Bus topology). Ngoài ra còn có một số dạng biến thể khác như mạng dạng cây, mạng hỗn hợp, sao mở rộng,…

**1. Mạng dạng hình sao (Star topology)**

Mạng dạng hình sao bao gồm một trung tâm và các nút thông tin. Các nút thông tin là các trạm đầu cuối, các máy tính và các thiết bị khác của mạng. Trung tâm của mạng điều phối mọi hoạt động trong mạng với chức năng cơ bản là:

- Xác định cặp địa chỉ gửi và nhận được phép chiếm tuyến thông tin và liên lạc với nhau.
- Cho phép theo dõi và xử lý sai trong quá trình trao đổi thông tin.
- Thông báo các trạng thái của mạng.

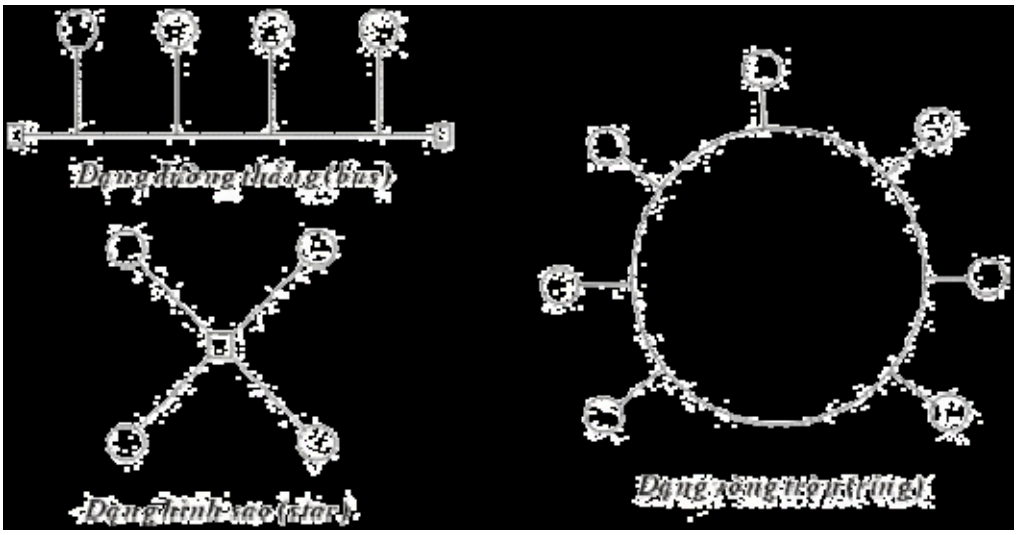
Ưu điểm:

- Hoạt động theo nguyên lý nối song song nên nếu có một thiết bị nào đó ở một nút thông tin bị hỏng thì mạng vẫn hoạt động bình thường.
- Cấu trúc mạng đơn giản và các thuật toán điều khiển ổn định.
- Mạng có thể mở rộng hoặc thu hẹp tùy theo yêu cầu người sử dụng.

Nhược điểm:

- Khả năng mở rộng mạng phụ thuộc hoàn toàn vào khả năng của trung tâm. Khi trung tâm có sự cố thì mạng ngừng hoạt động.
- Mạng yêu cầu kết nối độc lập riêng lẻ từng thiết bị ở các nút thông tin đến trung tâm. Khoảng cách từ máy đến trung tâm hạn chế (thường 100 m).

Thông thường, mạng hình sao cho phép nối các máy tính vào một bộ tập trung (HUB) bằng cặp xoắn, giải pháp này cho phép nối trực tiếp nhiều máy tính với HUB không cần qua trục BUS, tránh được các yếu tố gây nghẽn mạng. Cùng với sự phát triển của Switch, mà hình này ngày càng trở nên phổ biến.



Hình III-9. Một số cấu trúc chính của mạng LAN

## 2. Mạng dạng tuyến (Bus topology)

Trong mạng hình bus, các máy tính và nút mạng sẽ đều được nối về với nhau trên một trục đường dây cáp chính để chuyển tải tín hiệu.Tất cả các nút đều sử dụng chung đường dây cáp chính này. Phía hai đầu dây cáp được bịt bởi một thiết bị gọi là terminator. Các tín hiệu và dữ liệu khi di chuyển lên và xuống trong dây cáp đều mang theo địa chỉ nơi đến.

Loại mạng này dùng ít dây cáp nhất, dễ lắp đặt. Tuy vậy cũng có những bất lợi khi sẽ có sự ùn tắc khi dữ liệu di chuyển với lưu lượng lớn và khi có sự hỉng hóc ở đoạn nào đó thì rất khó phát hiện. Hư hỏng trên đường dây chính sẽ ngừng toàn bộ hệ thống.

## 3. Mạng dạng vòng (Ring topology)

Mạng được bố trí theo dạng vòng tròn, đường dây cáp được thiết kế làm thành một vòng khép kín, tín hiệu chạy quanh theo một chiều nào đó. Các nút

truyền tín hiệu cho nhau mỗi thời điểm chỉ được một nút mà thôi. Dữ liệu truyền đi phải kèm theo địa chỉ cụ thể của trạm tiếp nhận.

Mạng Token Ring có thể chạy ở tốc độ 4Mbps hoặc 16 Mbps. Phương pháp truy cập dùng trong mạng Token Ring gọi là Toking passing.Token passing là phương pháp truy cập xác định, trong đó các xung đột được ngăn ngừa bằng cách ở mỗi thời điểm chỉ có một trạm có thể truyền dữ liệu. Điều này được thực hiện bằng việc truyền một tín hiệu đặc biệt gọi là Token xoay vòng từ trạm này qua trạm khác. Mỗi trạm chỉ có thể gửi dữ liệu khi nó nhận được Token.

Mạng dạng vòng có thuận lợi là có thể nới rộng ra xa, tổng đường dây cần thiết ít hơn so với hai kiểu trên. Nhược điểm điểm là đường dây phải khép kín, nếu bị ngắt ở một nơi nào đó thì toàn bộ hệ thống cũng bị ngừng.

### III.4.2. Các chuẩn mạng LAN

Các chuẩn LAN là các tiêu chuẩn công nghệ cho LAN được phê chuẩn bởi các tổ chức chuẩn hóa quốc tế, nhằm hướng dẫn các nhà sản xuất thiết bị mạng đi đến sự thống nhất chung khả năng sử dụng chung các sản phẩm của họ, vì lợi ích của người sử dụng và tạo điều kiện thuận lợi cho các nghiên cứu phát triển.

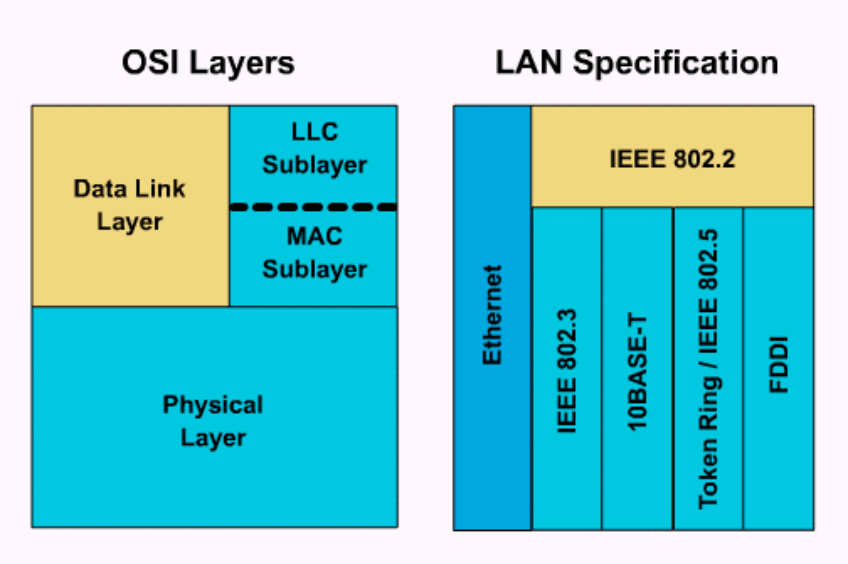
Các chuẩn quy định môi trường truyền dẫn cũng như cách thức sử dụng chúng trong kết nối LAN: các giao thức truyền thông ở các tầng vật lý và tầng liên kết dữ liệu của mạng theo mô hình OSI.

Các giao thức truyền thông ở các tầng trên mô hình OSI hiện tại được xác định qua một số giao thức phổ biến như TCP/IP, IPX/SPX, NetBIOS…

Ủy ban IEEE phát triển tiêu chuẩn IEEE LAN và đề xuất phân chia hai tầng thấp nhất của mô hình OSI như dưới đây:

Theo chuẩn 802 thì tầng LKDL được chia thành hai tần:

- Tầng con điều chỉnh logic LLC(Logical Link Control Sub-layer) : giữ vai trò tổ chức dữ liệu, tổ chức thông tin để truyền và nhận. Thủ tục tầng LLC không bị ảnh hưởng khi sử dụng các đường truyền dẫn khác nhau, nhờ vậy mà linh hoạt hơn trong khai thác.
- Tầng con điều khiển xâm nhập mạng MAC (Media Access Control Sub-layer), làm nhiệm vụ điều khiển truy cập mạng.




Hình III-10. Các tầng LLC và MAC.

Chuẩn 802.2 ở mức con LLC tương đương với chuẩn HDLC của ISO hoặc X.25 của CCITT.

Chuẩn 802.3 xác định phương pháp truy cập mạng tức thời có khả năng phát hiện lỗi chồng chéo thông tin CSMA/CD. Phương pháp CSMA/CD được đưa ra từ năm 1993 nhằm mục đích nâng cao hiệu quả mạng. Theo chuẩn này các mức được ghép nối với nhau thông qua các bộ ghép nối.

Chuẩn IEEE 802.3 dùng cho mạng Ethernet ( sử dụng giao thức truy nhập CSMA/CD) bao gồm cả hai phiên bản băng tần cơ bản và băng tần mở rộng.

Chuẩn IEEE 802.4 liên quan đến sự sắp xếp tuyến token, thực chất là phương pháp truy cập mạng theo kiểu phát tín hiệu thăm dò token qua các trạm và đường truyền bus.

Chuẩn IEEE 802.5 dùng cho mạng dạng vòng và trên cơ sở dùng tín hiệu thăm dò token. Mỗi trạm khi nhận được tín hiệu thăm dò token thì tiếp nhận token và bắt đầu quá trình truyền thông tin dưới dạng các frame. Các frame có cấu trúc tương tự như của chuẩn 802.4. Phương pháp truy cập mạng này quy định nhiều mức ưu tiên khác nhau cho toàn mạng và cho mỗi trạm, việc quy định này vừa do người thiết kế vừa do người sử dụng quy định.

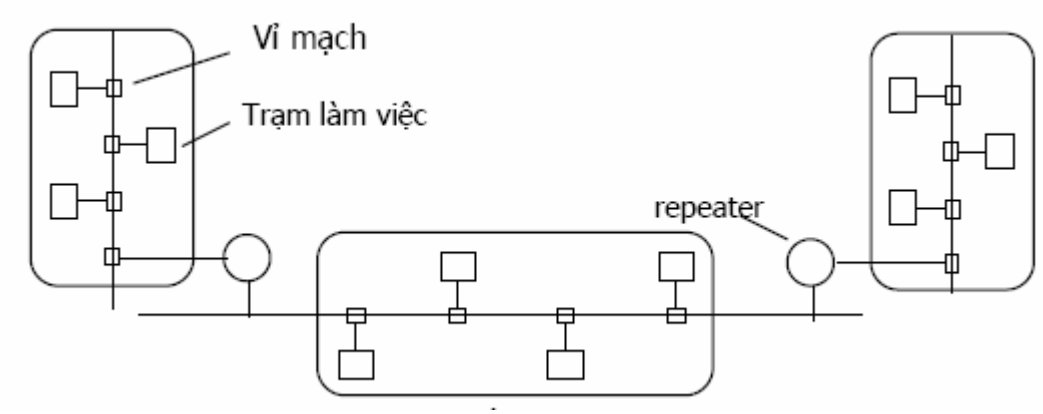
Chuẩn IEEE 802.11 dùng cho mạng không dây (Wireless)

## 1. Chuẩn Ethernet

Đây là kỹ thuật mạng cục bộ thành công nhất những năm gần đây và sử dụng công nghệ CSMA/CD(Carrier Sence, Multiple Access With Collision Detect)

Ethernet là một mạng đa truy xuất, các nút gửi và nhận khung qua một liên kết chia sẻ.Digital Equipment Corporation và Intel Corporation kết hợp với Xerox định nghĩa chuẩn Ethernet vào năm 1978. Chuẩn này sau đó được xây dựng thành

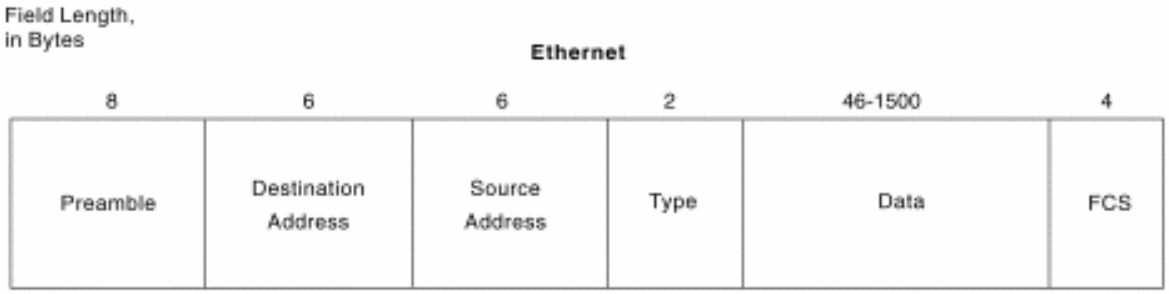
chuẩn 802.3 IEEE(chuẩn năm 1978 là con của chuẩn này). 802.3 xây dựng thêm nhiều chức năng mới. Gần đây, nó đã có phiên bản 100 Mbps được gọi là Fast Ethernet và 1000 Mbps gọi là Giagabit Ethernet.




Hình III-11. Cấu trúc Ethernet dạng bus.

Thuật toán kiểm soát truy xuất đường truyền chia sẻ trong Ethernet gọi là Ethernet's Media Accsess Control. Nó đặc thù được thi hành trên phần cứng của card mạng.

**Định dạng khung cơ bản:**




Hình III-12. Định dạng khung Ethernet

- 64 bit Preamble (một chuỗi thay đổi giữa 0 và 1) cho phép máy nhận đồng bộ tín hiệu với máy gửi.
- Cả máy nguồn và máy đích đều có 48 bit địa chỉ.
- Trường Type chứa khoá để thực hiện phân kênh(ở các giao thức mức cao).
- Mỗi khung chứa tối đa 1500 byte và tối thiểu 46 byte dữ liệu (nếu thiếu các host phải đệm dữ liệu thêm vào trước khi truyền, lý do là khung phải đủ lớn để giúp phát hiện xung đột).
- FCS-Frame Check Sequence**:** Sử dụng 32 bit CRC kiểm tra lỗi.
- Các khung trong Ethernet truyền theo kiểu Bit-Oriented.

- Ethernet có 14 byte header.
- Card mạng tại các máy gửi sẽ gắn Preamble, CRC trước khi truyền và ngược lại, nó sẽ được loại bỏ tại card mạng của máy nhận.

**Thuật toán truyền**

Ý tưởng:

Lúc một card giao tiếp mạng có một khung để gởi và liên kết rãnh, nó truyền khung ngay lập tức, không có sự điều đình với các card giao tiếp mạng khác. Giới hạn kích thước 1500 byte có nghĩa rằng card giao tiếp mạng chỉ có thể chiếm giữ đường dây trong một khoảng thời gian cố định.

Lúc một card giao tiếp mạng có một khung để gởi và liên kết bận, nó đợi cho tới khi đường dây rãnh và truyền ngay lập tức khi liên kết trở nên rảnh. Chúng được gọi là giao thức 1-persistent vì một card giao tiếp mạng với 1 khung để gửi sẽ truyền với xác suất 1 bất kỳ lúc nào đường dây trở nên rãnh.

Tổng quát, thuật toán truyền p-persistent với xác suất 0 <= p <=1 sau khi đường dây rãnh và khả năng trì hoãn với xác suất q = 1-p, lý do chọn p < 1 là do có thể nhiều adapter đợi đường dây rãnh và chúng ta không muốn tất cả chúng cùng truyền một lúc. Nếu một adaptor truyền ngay với một xác suất 33%(giả sử) tức là 3 adapter đợi để truyền. Mặc dù với lý do trên, trong thực tế một adapter luôn truyền ngay lập tức sau khi liên kết rãnh và thật sự rất hiệu quả khi thực hiện cách này.

Nếu cả hai cùng truyền một lúc thì gọi là hiện tượng xung đột. Vì Ethernet hổ trợ phát hiện xung đột, nên mỗi máy gửi đều có thể phát hiện xung đột trong quá trình truyền của mình, khi phát hiện xung đột nó đầu tiên truyền 32 bit jamming tuần tự và dừng việc truyền. Thật sự nó là 64 bit, 32 bit premble + 32 bit jamming

## 2. Token Ring

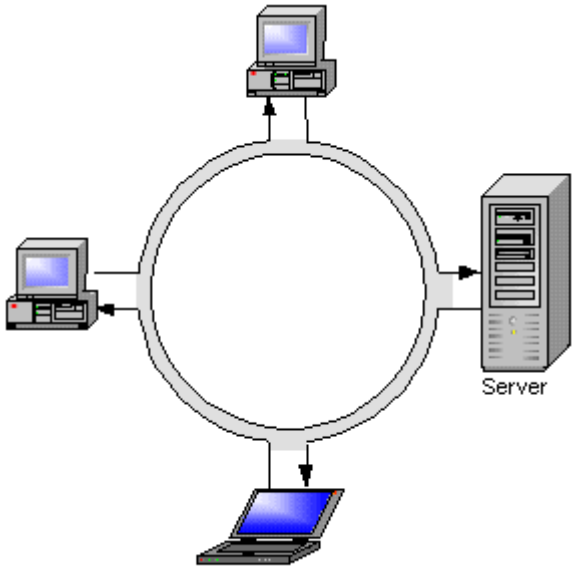
Cùng với Ethernet, Token Ring là một lớp quan trọng khác của mạng chia xẻ liên kết. Tuy nhiên, có nhiều vấn đề khó khăn trong Token Ring hơn là trong Ethernet.

Trước đây Token Ring định nghĩa bởi chuẩn IBM's Token Ring. Gần đây 802.5 là chuẩn định nghĩa bởi IEEE. Nhưng hầu hết các nguyên tắc tổng quát của Token Ring đều tương tự nhau giữa IBM và 802.5. Tuy nhiên chuẩn FDDI (Fiber Distributed Data Interface) là chuẩn mới nhất và nhanh nhất hiện nay.

Mạng Token Ring bao gồm một tập các nút nối trong một vòng. Dữ liệu luôn truyền theo hướng xác định vòng quanh vòng, mỗi nút nhận khung từ hàng xóm trên của nó và gửi chúng xuống hàng xóm bên dưới nó. Sơ đồ nối kết của Ring hoàn toàn trái ngược với sơ đồ nối kết Ethernet. Các nút tham gia nối kết trong mạng Token Ring chia sẽ chung một đường truyền vật lý.

Token Ring chia sẽ hai đặc trưng của Ethernet:

- Yêu cầu một thuật toán phân phối để điều khiển lúc một nút được phép truyền.
- Tất cả các nút trên vòng đều nhìn thấy các khung, mỗi nút xem xét địa chỉ trong header của khung và lưu lại một bảng sao của các khung khi các khung này đi qua nó.




Hình III-13.Mạng Token Ring

"Token" dùng để chỉ phương pháp truy xuất chia sẻ đường truyền. Nó thật sự chỉ là một chuỗi các bit đặc biệt, đi vòng quanh vòng. Mỗi nút trên vòng nhận và chuyển token. Khi một nút có dữ liệu cần truyền nhìn thấy token, nó chộp lấy token và chèn một khung vào trong vòng. Các nút còn lại trên vòng đơn giản chỉ chuyển khung này. Trước khi truyền dữ liệu các nút sẽ lưu trữ một bảng sao của khung sẽ truyền và sau đó sẽ chuyển khung này đến nút kế tiếp trong vòng. Lúc khung quay lại máy gửi, nút này nhận lại khung đó và trả lại token cho vòng.

**Giao thức điều khiển truy xuất đường truyền(MAC protocol)**

Card mạng cho một nút trong Token Ring chứa một receiver, một tranceiver, buffer.

Khi không có trạm nào truyền dữ liệu token đi vòng quanh vòng. Do đó, mỗi nút trên vòng phải có khả năng lưu trữ toàn bộ Token. Ví dụ token của 802.5 là 24 bit chiều dài.

Khi một token đi vòng quanh vòng, bất kỳ trạm nào có dữ liệu đều có thể chộp lấy token, giữ nó lại và bắt đầu gởi dữ liệu. Trong mạng 802.5, sự chộp lấy bằng cách chỉ thay đổi một bit trong byte thứ hai của token, 2 byte đầu tiên của

token được thay đổi bây giờ trở thành gói mang "lời chào hỏi". Khi một trạm có token nó có thể thực hiện gởi một hay nhiều gói.

Mỗi gói được truyền chứa địa chỉ của máy nhận. Mỗi nút cũng có thể truyền gói theo multicast hay broadcast. Khi mỗi gói đi qua mỗi nút, mỗi nút xem xét địa chỉ bên trong gói. Nếu là gói truyền đến nó, trạm này sẽ chép một bản sao vào trong buffer của nó khi gói đi qua card mạng, nhưng không di chuyển gói này ra khỏi vòng. Máy gửi có nhiệm vụ di chuyển gói ra khỏi vòng.

Một vấn đề cần giải quyết là bao nhiêu dữ liệu mà một nút được cho phép truyền mỗi lần nó có token, thời gian này được gọi là THT(token holding time). Nếu chúng ta cho rằng hầu hết các nút không có dữ liệu thì không hợp lý. THT được đặt cố định, nhưng thật vô lý trong trường hợp một nút bị giới hạn gửi chỉ một thông điệp và bắt buột phải đợi cho tới khi token đi quanh một vòng trước khi có cơ hội truyền tiếp.

Cách dễ dàng là một nút có thể gửi nhiều byte mỗi lần lúc nó token, điều này rất tốt khi nhận biết được trên vòng chỉ có một nút cần gửi dữ liệu, nhưng khả năng này không làm việc tốt lúc nhiều nút có dữ liệu gửi. Trong mạng 802.5 THT quy định là 10ms. Do đó các nút phải khéo léo khi sử dụng THT, trước khi đặt mỗi gói vào trong vòng, mỗi trạm phải kiểm tra khoảng thời gian dùng để truyền gói sẽ không vượt quá THT.

802.5 cung cấp một các thức thức truyền tin cậy, sử dụng 2 bit cuối gói, bit A và C được khởi tạo là 0. Lúc một trạm thấy một khung mà nó muốn nhận nó set bit A trong khung. Khi nó chép khung vào trong adaptor, nó set bit C, nếu máy gửi nhìn thấy khung quay trở lại với bit A vẫn là 0 thì nó sẽ biết không có máy nhận. Nếu bit A được đặt nhưng bit C thì không lý do là máy nhận không chấp nhận khung

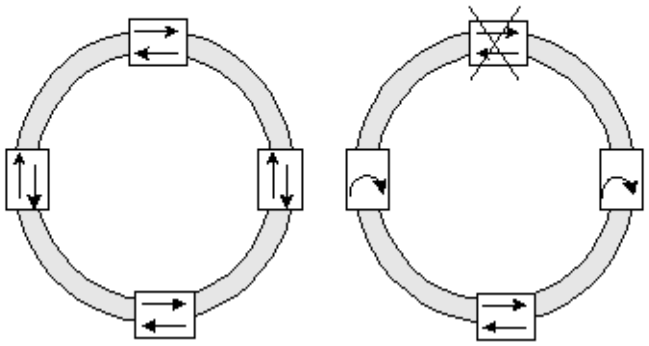
## 3. FDDI

FDDI (Fiber Distributed Data Interface) thì tương tự IBM và 802.5, tuy nhiên nó có một số điểm khác nhau bởi vì nó chạy trên cáp quang và nó thực hiện một số cách tân.

**Đặc điểm vật lý**

Nó bao gồm một vòng đôi, hai vòng truyền dữ liệu theo hai hướng ngược nhau, vòng thứ hai sẽ không được sử dụng nhưng nó sẽ trở nên hoạt động nếu vòng sơ cấp bị hỏng. Mạng FDDI vẫn hoạt động khi một đường cáp hay một trạm bị hỏng.

Bởi vì sự phí tổn của cấu hình vòng đôi. FDDI cho phép nút gắn vào mạng chỉ bởi một cáp đơn. Nó được gọi single attachment stations(SAS), kết nối đôi được gọi là Dual Attachment Stations.



Hình III-14. Mô hình mạng FDDI

Một thiết bị tập trung được sử dụng để gắn SAS vào vòng(sử dụng hai đường cáp đơn).

FDDI là một mạng 100 Mbps.

Giới hạn chuẩn 500 station.

Giới hạn chuẩn khoảng các là 2km giữa bất kỳ 2 trạm nào.

Toàn bộ mạng giới hạn 200 km của cáp quang, do vòng đôi nên nó tổng cộng chiếu dài chỉ là 100km.

Nó có thể chạy qua các môi trường vật lý khác nhau như cáp đồng trục hay cáp xoắn đôi.

FDDI sử dụng mã hoá 4B/5B.

**Thuật toán Time-Token**

THT của mỗi nút được xác định trước và gán ở một giá trị cố định. Thêm vào đó, để đảm bảo mỗi nút có cơ hội truyền trong một khoảng thời gian nào đó, ta đặt giới hạn trên của TRT(token ratation time) cho tất cả nút, gọi là target TRT và tất cả các nút đều chấp nhận thời gian TTRT này. Mỗi nút đo thời gian bởi sự di chuyển thành công của token. Ta goị là "Measured TRT".

If mesured-TRT > TTRT: token đến trễ và nút không truyền dữ liệu.

If mesured-TRT < TTRT: token đến sớm và nút được cho phép giữ token để truyền.

Có hai lớp truyền: đồng bộ và không đồng bộ. Lúc một nút có token nó được phép gởi dữ liệu đồng bộ, không cần quan tâm token đến sớm hay trễ (gởi âm thanh hay video). Ngược lại nó chỉ có thể gửi khi token đến sớm (các ứng dụng file). Nó sử dụng một bit để phân biệt đồng bộ và không đồng bộ.

## III.5. Địa chỉ vật lý (MAC address)

Mỗi host trên một Ethernet chỉ có một địa chỉ duy nhất có chiều dài 48 bit. Địa chỉ này được lưu trữ trên card mạng và có thể đọc tuần tự 6 số phân cách nhau bởi dấu ":"Để đảm bảo mỗi host có một địa chỉ duy nhất mỗi nhà sản xuất thiết bị Ethernet bị bắt buộc gán một mã trên các card mạng mà họ sản xuất.

Mỗi khung truyền trên Ethernet được nhận bởi tất cả các adapter nối đến Ethernet đó (kiểm tra địa chỉ để nhận hay không nhận).

Ngoài địa chỉ unicast, một địa chỉ bao gồm tất cả các bit 1 được xem là địa chỉ broadcast. Địa chỉ có bit đầu tiên là 1 nhưng không phải là broadcast thì được xem là multicast (một host có thể được lập trình trên adapter đó để có thể chấp nhận một vài địa chỉ multicast).

Tóm lại, một card giao tiếp mạng nhận tất cả khung và chỉ chấp nhận khung khi trên header của khung đó chứa địa chỉ của nó, địa chỉ multicast, địa chỉ broadcast, hay một khung vô tình.

## III.6. Một số công nghệ tầng liên kết dữ liệu khác

### III.6.1. Mạng không dây(Wireless Network)

Mạng không dây là một kỹ thuật gần đây phát triển mạnh. Các máy tính bên trong một toà nhà có thể sử dụng tia hồng ngoại để liên lạc với nhau hay người ta còn sử dụng sóng viba để xây dựng một mạng rộng lớn từ một lưới điều khiển của một số vệ tinh quỹ đạo thấp. 802.11 được thiết kế để sử dụng trong một khu vực địa lí giới hạn.

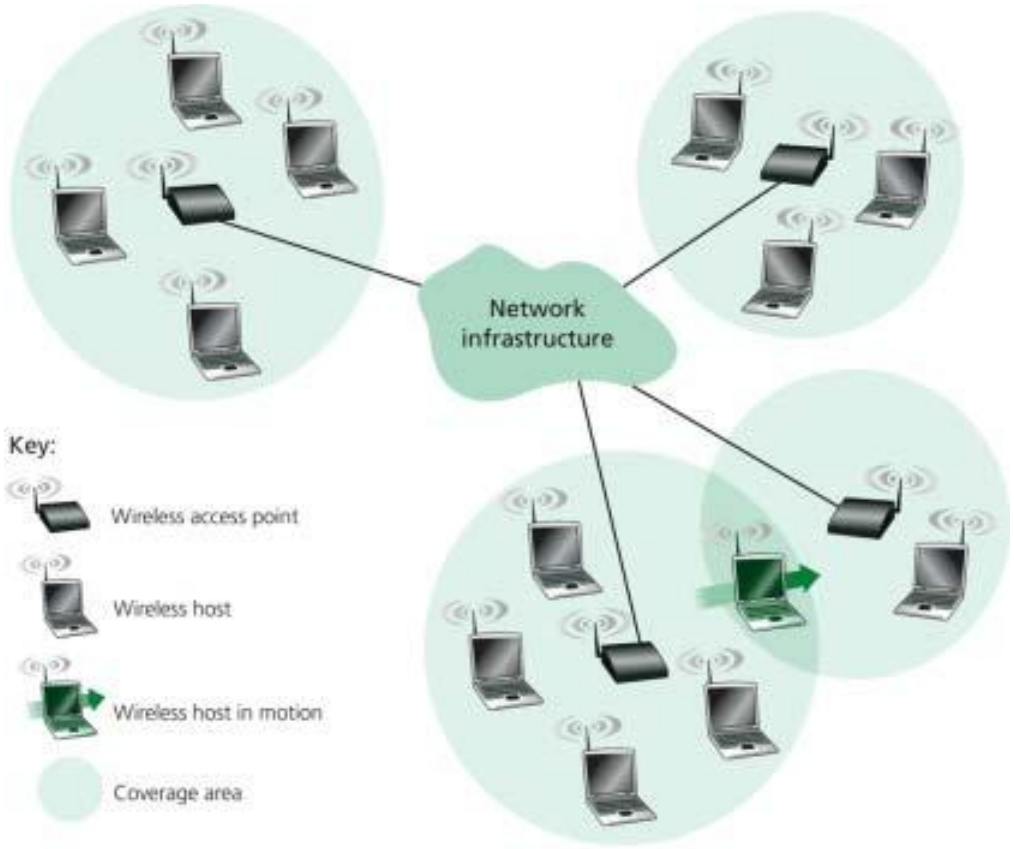
802.11 sử dụng 3 dạng đường truyền vật lý khác nhau:

- Sử dụng sóng vô tuyến
- Sử dụng sóng viba
- Sử dụng tia hồng ngoại.

Sóng vô tuyến được lan truyền qua một tần số rộng hơn bình thường, nhằm giảm tối thiểu tác động ảnh hưởng từ các thiết bị khác. **Frequency hopping** là một kỹ thuật sóng vô tuyến thực hiện truyền tín hiệu qua một dãy các tần số ngẫu nhiên, đầu tiên nó truyền ở tần số 1, rồi 2, rồi 3, nhưng dãy các tần số này thì không thật sự ngẫu nhiên, nó dùng thuật toán tạo ra số ngẫu nhiên giả. Các máy nhận sử dụng cùng thuật toán như là máy gửi và vì vậy hai máy có thể đồng bộ và truyền dữ liệu với nhau.

**Lan truyền trực tiếp (direct sequence):** mỗi bit trong khung truyền được thể hiện bởi nhiều bit trong tín hiệu truyền. Với mỗi bit muốn truyền máy gửi thực hiện phép XOR chuỗi bit đó với một chuỗi bit ngẫu nhiên.

Kỹ thuật truyền tia hồng ngoại truyền dựa trên sự khuyếch tán. Và thường nằm trong cự ly khoảng 10m và giới hạn bên trong một toà nhà.




Hình III-15. Ví dụ mạng không dây

**Quản lý xung đột**

Cách thức truyền của mạng không dây tương tự cách thức truyền của Ethernet. Một nút sẽ đợi cho đến khi liên kết rãnh trước khi truyền và nếu hai nút cùng truyền một lúc xung đột sẽ xuất hiện. Vấn đề xung đột trong mạng không dây phức tạp bởi vì không phải tất cả các nút luôn luôn ở trong phạm vi truyền của các nút khác.

**Thuật toán Multiple Access with Collision Avoidance (MACA)**

Máy gửi và máy nhận trao đổi các khung điều khiển với nhau trước khi máy gửi thực hiện truyền dữ liệu. Máy gửi truyền một khung Request to Send (RTS) đến máy nhận, khung RTS bao gồm một trường chỉ ra thời gian nó muốn chiếm giữ đường truyền (chiều dài của khung được truyền). Máy nhận đáp lại với khung Clear to Send(CTS), khung này đáp lại trường chiều dài của máy gửi, bất kỳ nút mà nó nhận thấy khung CTS thì nó biết nó không thể liên lạc với máy nhận, vì vậy nó không thể truyền trong khoảng thời gian này. Bất kỳ nút mà nó nhìn thấy khung, nhưng không thấy khung CTS thì nó có thể tự do liên lạc với máy nhận.

Hai vấn đề quan trọng trong mạng không dây

- Máy nhận gởi một ACK đến máy gửi thông báo thành công sau khi nhận khung, tất cả các nút phải đợi ACK trước khi truyền tiếp.
- Có hai hay nhiều nút nhận thấy liên kết trống và vì vậy sẽ truyền khung ở cùng một lúc, do đó các khung sẽ xung đột với nhau, 802.11 không hỗ trợ phát hiện xung đột nhưng nó sẽ phát hiện xung đột khi nó không nhận được khung CTS sau một khoảng thời gian nào đó. Trong trường hợp này chúng sẽ đợi một khoảng thời gian ngẫu nhiên trước khi truyền lại nó.

**Hệ thống phân phối (Distribution System)**

802.11 là một hệ thống phù hợp cho một mạng có cấu hình các nút đặc biệt, một nút trong mạng có thể bị giới hạn thông tin với một hay tất cả các nút khác trên mạng. Hơn nữa sự thuận lợi của mạng không dây là các nút tự do di chuyển, chúng không bị ràng buộc bởi dây dẫn, một tập các nút có thể thay đổi bất kỳ thời gian nào.

Các nút trong mạng không dây bên cạnh việc trao đổi thông tin tự do với các máy khác trong cùng một cấu trúc nó còn có thể trao đổi với các máy khác thông qua một thiết bị khác gọi là AP(Access Point). Thiết bị này sử dụng cáp để nối trực tiếp với một thiết bị gọi là distribution system. Các nút trong mạng có thể tự chọn riêng cho mình một AP.

Kỹ thuật chọn 1 AP được gọi là scanning thực hiện qua 4 bước:

- Gởi một khung thăm dò.
- Tất cả các AP trong phạm vi của máy gửi đáp lại với một khung trả lời khung thăm dò.
- Nút chọn một AP và gởi một khung giao thiệp.
- AP đáp lại với một khung trả lời giao thiệp.
- Các nút thực hiện cách này bất cứ lúc nào nó tham gia mạng, cũng như nó cảm thấy không cảm thấy "hạnh phúc" với AP hiện tại.
- AP có thể gởi một khung thông báo khả năng truy xuất của mình (tỉ lệ truyền hổ trợ bởi AP).

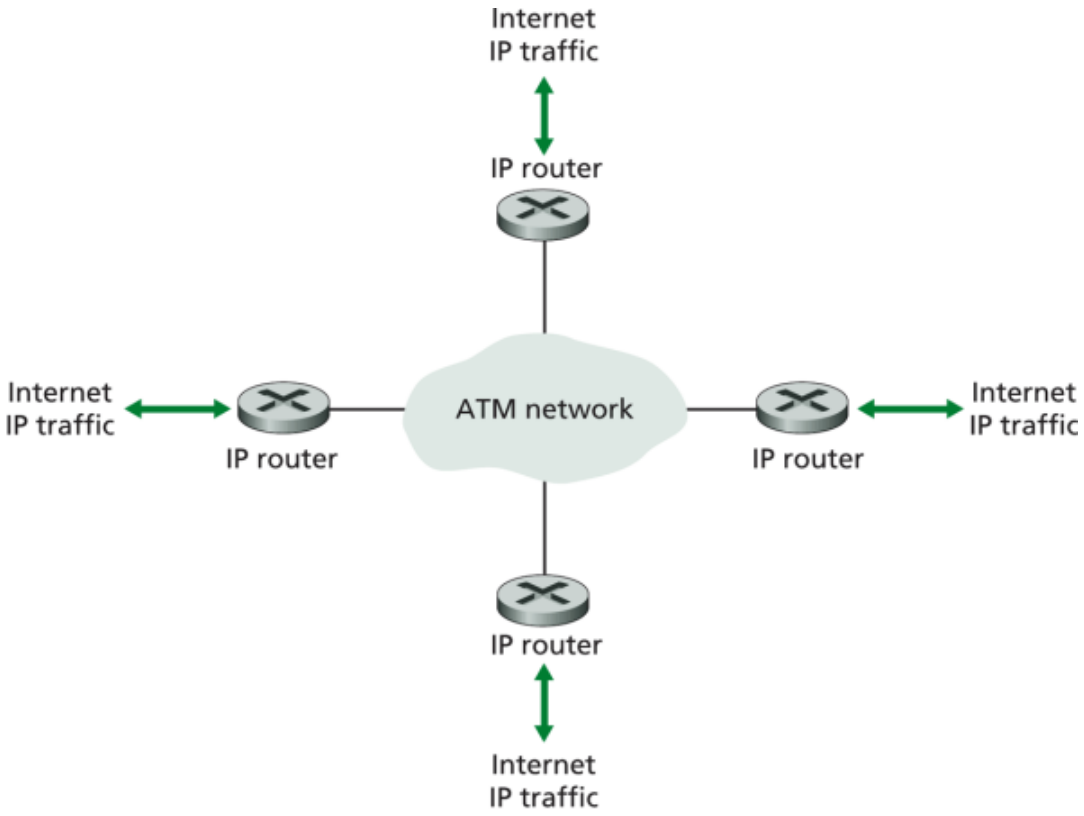
### III.6.2. ATM

Một công nghệ được quan tâm gần đây là ATM (Asychronous Tranfer Model). ATM là một công nghệ quan trọng trong những năm 1980 và đầu những năm 1990. ATM là tiếp cận theo dạng connection-oriented. Trong ATM giai đoạn thiết lập nối kết được gọi là signalling. Giao thức chính của ATM signalling là Q.2931. Ngoài khả năng tìm ra một đường đi xác định qua một mạng ATM, Q.2931 còn có nhiệm vụ cấp phát tài nguyên tại các chuyển mạch dọc kênh. Nó

đảm bảo một chất lượng phục vụ của kênh. Thật vậy, khả năng QoS cuả ATM là một trong nhữnh khả năng mạnh mẽ nhất.

Lúc một kênh ảo được thiết lập, nó cần thiết đặt địa chỉ nguồn trong thông điệp signalling. Trong ATM, địa chỉ có thể có ở một vài dạng, nhưng dạng chung nhất được sử dụng là E.164 và NSAP (Network Service Access Point), nó khác địa chỉ MAC sử dụng trong LAN.

Một điều mà làm ATM thật sự khác thường là các gói trong một mạng ATM có chiều dài cố định. Chiều dài của chúng là 53 byte bao gồm 5 byte header và 48 byte trọng tải, để phân biệt giữa các gói có chiều dài thay đổi và cố định người ta đưa ra một tên đặc biệt goị là tế bào (cell). ATM là một ví dụ chuẩn của mạng tế bào.




Hình III-16. Mạng ATM

**Cell**

Tất cả các công nghệ mạng mà chúng ta đã xem xét trước đây đều sử dụng các gói có chiều dài thay đổi. Gói có chiều dài thay đổi thì trói buột bên trong một vài giới hạn:

- Giới hạn thấp nhất: số lượng thông tin nhỏ nhất mà một gói có thể chứa mà một header không được tuỳ ý mở rộng.

- Giới hạn cao nhất: được đặt bởi nhiều yếu tố, ví dụ kích thước gói lớn nhất trong mạng FDDI xác định bao lâu mỗi trạm cho phép truyền mà không trả lại token và thật vậy nó xác định bao lâu mỗi trạm phải đợi cho token đến.

Cell, ngược lại giới hạn trên và dưới là cố định.

**Kích thước cell**

Gói có chiều dài thay đổi có một vài đặc trưng quan trọng:

- Nếu ta chỉ có một byte gửi, ta đặt nó trong gói có kích thước nhỏ nhất.
- Nếu chúng ta có một file lớn để gửi ta phân nó ra thành nhiều gói có kích thước lớn nhất để gửi.

Ta không cần thêm bất cứ thông tin gì trong trường hợp đầu, trong trường hợp thứ hai nó gia tăng hiệu quả băng truyền. Chúng ta cũng có thể giảm tối thiểu tổng số gói gửi bằng cách giảm tổng cộng hoạt động xử lý trên gói, điều này rất quan trọng trong một mạng có thông lượng cao bởi vì nhiều thiết bị mạng không giới hạn bao nhiêu bit trên 1 giây mà chúng có thể xử lý hơn là giới hạn số gói trên một giây mà chúng có thể xử lý.

Vậy tại sao phải sử dụng cell. Một lý do chính là nó thuận tiện được thi hành của phần cứng mạng. Bởi vì trong mạng điện thoại mỗi mạng điện thoại thường phục vụ 10.000 khách hàng, chiều dài cố định thì rất hữu ích nếu chúng ta muốn xây dựng các mạng nhanh, có tính khả mở. Có hai lý do:

- Xây dựng phần cứng là một nhiệm vụ dễ dàng, và nhiệm vụ xử lý mỗi gói thì dễ dàng khi biết chiều dài thật sự của chúng.
- Nếu tất cả các gói có cùng chiều dài, ta có thể có nhiều chuyển mạch. Tất cả chúng cùng làm một nhiệm vụ(xử lý song song).

Một đặc điểm quan trọng của truyền tế bào liên quan đến tổ chức hàng đợi. Khi ta lấy một gói từ hàng đợi và bắt đầu truyền nó, ta tiếp tục thực hiện thao tác này cho đến khi toàn bộ gói được truyền. Ví dụ, một mạng với một gói thay đổi, kích thước gói lớn nhất là 4KB và tốc độ truyền là 100Mbps, thời gian để truyền gói có kích thước lớn nhất là 327.69 micro giây, thật vậy một gói ưu tiên cao đến chỉ sau khi gói có kích thước lớn nhất được truyền sẽ ngồi đợi 327.68 micro giây để truy xuất liên kết, ngược lại nếu chuyển một cell 53 byte thời gian lâu nhất nó đợi là 4.24s điều này dường như không đáng kể nhưng nó dẫn đến tình trạng "bồn chồn" cho một số ứng dụng.

### III.6.3. X25

Được CCITT công bố lần đầu tiên vào 1970 lúc lĩnh vực viễn thông lần đầu tiên tham gia vào thế giới truyền dữ liệu với các đặc tính:

- X25 cung cấp quy trình kiểm soát luồng giữa các đầu cuối đem lại chất lương đường truyền cao cho dù chất lương đương dây truyền không cao.
- X25 được thiết kế cho cả truyền thông chuyển mạch lẫn truyền thông kiểu điểm nối điểm.
- Được quan tâm và tham gia nhanh chóng trên toàn cầu.

Trong X25 có chức năng dồn kênh (multiplexing) đối với liên kết logic (virtual circuits) chỉ làm nhiệm vụ kiểm soát lỗi cho các frame đi qua. Điều này làm tăng độ phức tạp trong việc phối hợp các thủ tục giữa hai tầng kề nhau, dẫn đến thông lượng bị hạn chế do tổng phí xử lý mỗi gói tin tăng lên. X25 kiểm tra lỗi tại mỗi nút trước khi truyền tiếp, điều này làm cho đường truyền có chất lượng rất cao gần như phi lỗi. Tuy nhiên do vậy khối lượng tích toán tại mỗi nút khá lớn, đối với những đường truyền của những năm 1970 thì điều đó là cần thiết nhưng hiện nay khi kỹ thuật truyền dẫn đã đạt được những tiến bộ rất cao thì việc đó trở nên lãng phí.

### III.6.4. Frame Relay

Mỗi gói tin trong mạng gọi là Frame, do vậy mạng gọi là Frame relay. Đặc điểm khác biệt giữa mạng Frame Relay và mạng X25 mạng Frame Relay là chỉ kiểm tra lỗi tại hai trạm gửi và trạm nhận còn trong quá trình chuyển vận qua các nút trung gian gói tin sẽ không được kiểm lỗi nữa. Do vậy thời gian xử lý trên mỗi nút nhanh hơn, tuy nhiên khi có lỗi thì gói tin phải được phát lại từ trạm đầu. Với độ an toàn cao của đường truyền hiện nay thì chi phí việc phát lại đó chỉ chiếm một tỷ lệ nhỏ nếu so với khối lượng tính toán được giảm đi tại các nút nên mạng Frame Relay tiết kiệm được tài nguyên của mạng hơn so với mạng X25.

Frame relay không chỉ là một kỹ thuật mà còn là thể hiện một phương pháp tổ chức mới. Với nguyên lý là truyền mạch gói nhưng các thao tác kiểm soát giữa các đầu cuối giảm đáng kể. Kỹ thuật Frame Relay cho phép thông lượng tối đa đạt tới 2Mbps và hiện nay nó đang cung cấp các giải pháp để tương nối các mạng cục bộ LAN trong một kiến trúc xương sống tạo nên môi trường cho ứng dụng multimedia.

# Chương IV. Giao thức tầng mạng

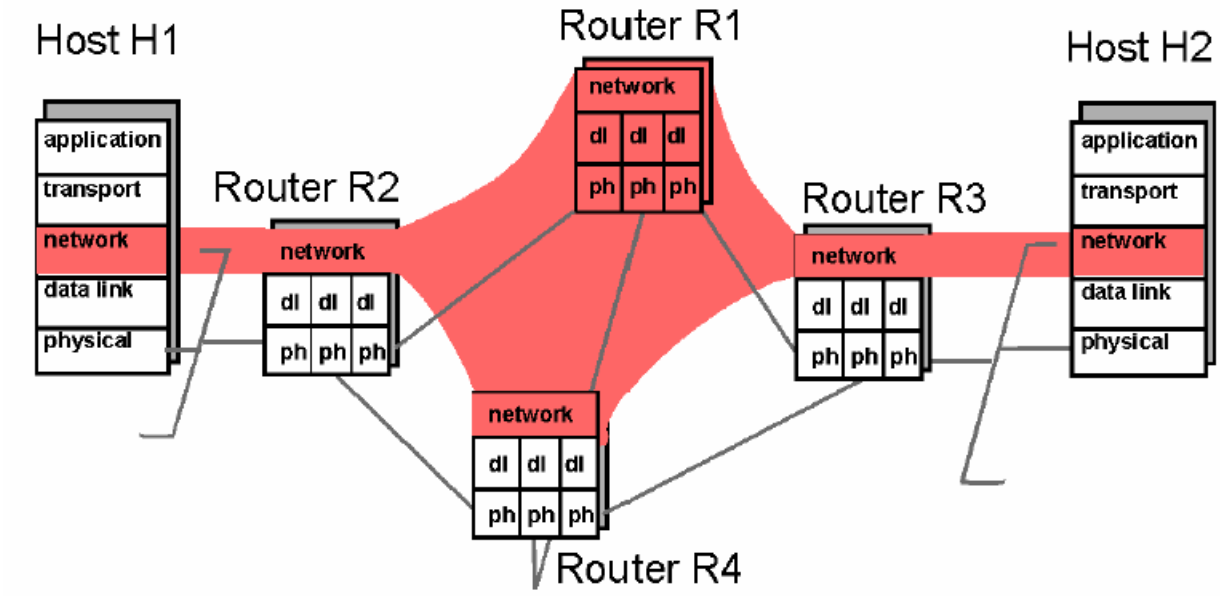
## IV.1. Chức năng của tầng mạng

### IV.1.1. Chức năng

Tầng mạng (Network layer) đảm bảo truyền tin thông suốt giữa hai nút đầu cuối trong mạng. Truyền các gói tin (packets) từ nơi gửi (sending host) tới nơi nhận (receiving host). Tầng mạng được cài đặt tại router và cả end system.

Chức năng chính:

- Chọn đường (path selection): có nhiều đường đi, gói tin sẽ đi theo đường nào?
- Chuyển mạch (switching, forwarding): chuyển gói tin từ cổng vào tới cổng ra của router một cách thích hợp.
- Thiết lập liên kết (call setup): một số kiến trúc mạng cần thiết lập kênh truyền trước khi truyền.




Hình IV-1. Tầng mạng

### IV.1.2. Dịch vụ cung cấp cho tầng giao vận

- Các dịch vụ phải độc lập với công nghệ được dùng trong mạng.
- Tầng giao vận phải độc lập với công nghệ được dùng trong mạng.

- Các địa chỉ mạng phải thống nhất để tầng iao vận có thể dùng cả mạng LAN và WAN

  *Có hai loại dịch vụ:*

  - Dịch vụ truyền tin liên kết (Connection Oriented Service)
  - Dich vụ truyền tin không liên kết (Connectionless Service)

  Sự khác nhau giữa hai dịch vụ:

| **Vấn đề** | **Dịch vụ có liên kết** | **Dịch vụ không liên kết** |
|---|---|---|
| Khởi động kênh | Cần thiết | Không |
| Địa chỉ đích | Chỉ cần lúc khởi động | Cần ở mọi gói tin |
| Thứ tự gói tin | Được đảm bảo | Không đảm bảo |
| Kiểm soát lỗi | Ở tầng mạng | Ở tầng giao vận |
| Điều khiển thông lượng | Ở tầng mạng | Ở tầng giao vận |
| Thỏa thuận tham số | Có | Không |
| Nhận dạng liên kết | Có | Không |

### IV.1.3. Tổ chức các kênh truyền tin trong mạng

#### 1. Kênh ảo (Virtual Circuit):

Tương đương kênh điện thoại trong tầng vật lý sử dụng trong mạng có liên kêt. Kênh ảo được thiết lập cho mỗi liên kết. Một khi đã được thiết lập thì các gói tin được chuyển đi tương tự trong mạng điện thoại cho đến khi liên kết bị hủy bỏ.

- Mỗi nút mạng chứa một kênh ảo.
- Khi một liên kết được khởi động một kênh ảo chưa dùng sẽ được chọn.
- Nút chọn kênh ảo chứa đường dẫn đến trạm tiếp theo và có số thấp nhất.

Khi gói tin khởi động đến nút đích, nút chọn kênh ảo có số thấp nhất thay thế số trong gói tin và chuyển vào trạm đích. Số kênh ảo nối với trạm đích có thể khác số kênh ảo mà trạm nguồn sử dụng.

#### 2. Mạng Datagram:

Tương đương với điện báo sử dụng trong mạng không liên kết. Trong mạng này không có tuyến đường nào được thiết lập. Các gói tin có thể đi theo nhiều đường khác nhau mà không nhất thiết theo một trình tự xác định. Thông tin vào là địa chỉ đích, thông tin ra là nút mạng phải tới.

Mạng Datagram phức tạp về điều khiển nhưng nếu kênh hỏng thì dễ dàng chuyển sang kênh mới.

Một số đặc trưng của mạng kênh ảo và datagram:

| Vấn đề | Mạng kênh ảo | Mạng datagram |
|---|---|---|
| Khởi động kênh | Cần thiết | Không |
| Địa chỉ hóa | Gói tin chỉ cần số kênh ảo | Gói tin phải có địa chỉ nguồn và địa chỉ đích |
| Thông tin tìm đường | Mỗi kênh ảo cần một vùng trong bảng | Không cần bất cứ thông tin nào |
| Tìm đường | Được thiết lập khi khởi động kênh ảo mới. Liên kết sẽ được duy trì cho cả phiên | Mỗi gói tin tìm đường độc lập.Phải tìm đường mỗi khi có gói tin đến nút mạng |
| Điều khiển | Kênh ảo qua nút hỏng sẽ bị hủy | Chỉ mất gói tin trong nút hỏng |
| Hỏng nút | Dễ khắc phục | Khó khắc phục |
| Độ phức tạp | Trong tầng mạng | Trong tầng giao vận |
| Thích hợp | Các dịch vụ liên kết | Các dịch vụ liên kết và không liên kết |

### IV.1.4. Tìm đường đi (định tuyến) trong mạng

Chức năng quan trọng nhất của tầng mạng là dẫn đường cho các gói tin từ trạm nguồn đến trạm đích. Thuật toán tìm đường là quy trình để quyết định chọn đường ra khỏi nút mạng nhằm gửi gói tin đi tiếp đến nút khác.

Yêu cầu của thuật toán tìm đường:

- Chính xác, ổn định, đơn giản và tối ưu.
- Thuật toán tìm đường phải có khả năng cập nhật lại cấu hình và đường vận chuyển để không phải khởi động lại mạng khi có một nút hỏng hoặc phải ngừng hoạt động của các máy trạm.

Các thuật toán chia làm hai nhóm:

- Nhóm không thích nghi (non adaptive): việc chọn đường không dựa vào việc đánh gia tình trạng mạng và cấu hình trong thời gian thực.
- Nhóm thích nghi (adaptive): việc tìm đường phải thích nghi với tình trạng mạng hiện tại.

### IV.1.5. Tắc nghẽn trong mạng

Khi có quá nhiều gói tin trong mạng hoặc một phần của mạng làm cho hiệu suất của mạng giảm đi vì các nút mạng không đủ khả năng lưu trữ, xử lý, gửi đi và

chúng bắt đầu bị mất các gói tin. Hiện tượng này gọi là sự tắc nghẽn (congestion) trong mạng.

Hàng đợi sẽ bị đầy (phải lưu tập tin, các bảng định tuyến,...) nếu khả năng xử lý của nút yếu hay thông tin vào nhiều hơn khả năng của đường ra.

Các biện pháp ngăn ngừa:

- Bố trí khả năng vận chuyển, lưu trữ, xử lý của mạng dư so với yêu cầu.
- Hủy bỏ các gói tin bị tắc nghẽn quá thời hạn.
- Hạn chế số gói tin vào mạng nhờ cơ chế cửa sổ (flow control).
- Chặn đường vào của các gói tin khi mạng quá tải.

## IV.2. Bộ định tuyến và các thiết bị kết nối mạng khác:

### IV.2.1. Bộ định tuyến (Router)

Trong môi trường gồm nhiều mạng gắn kết với nhau bằng nhiều giao thức và kiến trúc mạng khác nhau, bộ chuyển mạch (cầu nối) không thể truyền thông nhanh trong tất cả các đoạn mạng. Mạng có độ phức tạp như vậy cần một thiết bị không những biết địa chỉ mạng mỗi đoạn mạng mà còn quyết định tuyến đường tốt nhất để truyền dữ liệu và lọc các lưu lượng quảng bá trên các đoạn mạng cục bộ. Thiết bị như vậy gọi là bộ định tuyến (Router).

Hình IV-2. Router

Chức năng bộ định tuyến:

- Chuyển và định tuyến gói dữ liệu qua nhiều mạng dựa trên địa chỉ phân lớp mạng.
- Phân chia mạng lớn thành nhiều mạng nhỏ và kết nối các đoạn mạng với nhau.
- Lọc gói tin và giới hạn lưu lượng mạng, hoạt động như một rào cản an toàn giữa các đoạn mạng.
- Ngăn chặn tình trạng quảng bá vì router không chuyển tiếp gói tin dạng quảng bá.

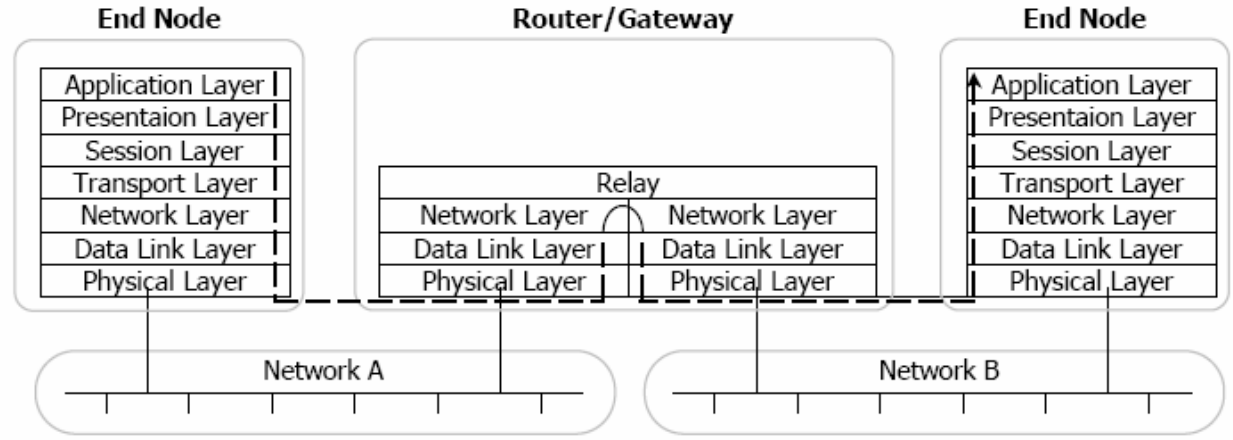
- Các bộ định tuyến có thể chia sẻ thông tin trạng thái và thông tin định tuyến với nhau, sử dụng thông tin này để bỏ qua các kết nối hỏng hoặc chậm.

**Nguyên lý hoạt động:**

Trong bộ định tuyến có một bảng định tuyến chứa các địa chỉ mạng. Tuy nhiên địa chỉ mạng có thể được lưu trữ tùy vào giao thức mạng đang chạy. Bộ định tuyến dùng bảng định tuyến để xác định địa chỉ đích cho dữ liệu nhận được. Bảng này liệt kê các thông tin sau:

- Địa chỉ mạng đã kết nối trực tiếp.
- Cách kết nối tới những mạng khác.
- Chi phí truyền dữ liệu qua các lộ trình đó.

Khi router nhận được gói dữ liệu truyền tới mạng ở xa, nó kiểm tra bảng định tuyến và chọn đường đi tối ưu (có chi phí thấp nhất) để gửi gói dữ liệu đến đích.




Hình IV-3. Kiến trúc Router trong mô hình OSI

**Truyền dữ liệu qua bộ định tuyến:**

Khi một trạm xác định cần gửi một gói dữ liệu tới một trạm trên một mạng khác. Công việc đầu tiên của trạm này là lấy địa chỉ vật lý của router (địa chỉ cổng kết nối ngầm định). Sau đó nó điền thông tin trong trường địa chỉ vật lý của gói dữ liệu bằng địa chỉ vậy lý của router và trường thông tin địa chỉ đích của tầng mạng (là địa chỉ IP nếu dùng TCP/IP) bằng địa chỉ của trạm đích.

Khi router kiểm tra địa chỉ đích, nó xác định xem nó có biết cách hay không chuyển tiếp gói tin đến chặng tiếp theo (next hop) là router kế tiếp trên đường đi, bằng cách kiểm tra địa chỉ. Nếu địa chỉ mạng đích nằm trong gói dữ liệu không có trong bảng định tuyến, router sẽ bỏ gói dữ liệu trừ khi nó được cấu hình đường đi mặc định. Ngược lại nếu địa chỉ mạng đích có trong bảng định tuyến, router thay

địa chỉ vật lý đích bằng địa chỉ vật lý của chặng tiếp theo và truyền gói dữ liệu đến đó.

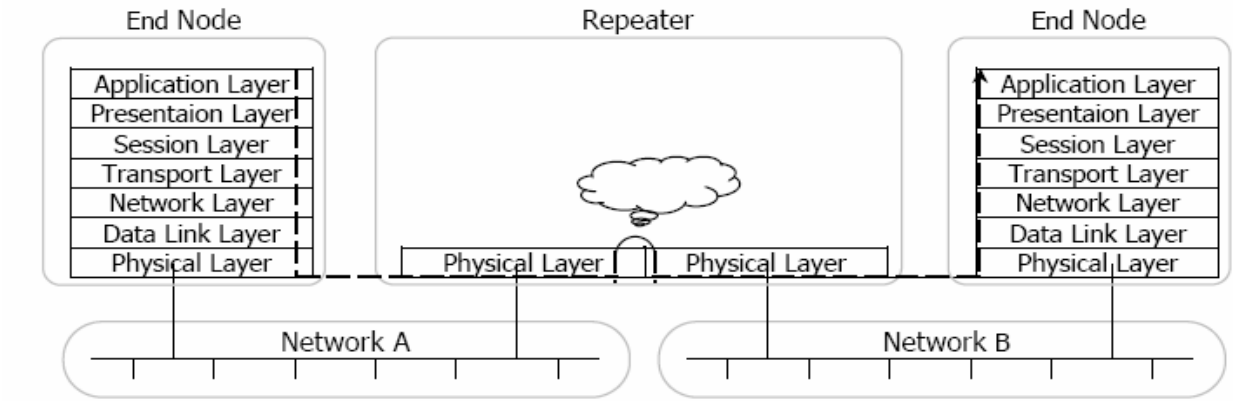
Như vậy, khi một gói tin truyền qua liên mạng, địa chỉ vật lý thay đổi nhưng địa chỉ của giao thức không đổi.

### IV.2.2. Bộ lặp (Repeater)

Bộ lặp thực hiện chức năng ở tầng vật lý dùng để khuyếch đại tín hiệu khi tín hiệu đi xa. Bộ lặp được sử dụng để kết nối các đoạn mạng lại với nhau. Bộ lặp nhận tín hiệu từ một đoạn mạng, tái tạo lại và truyền tín hiệu này đến đoạn mạng khác. Nhờ có bộ lặp mà tín hiệu bị suy yếu do phải truyền qua một đoạn cáp dài có thể trở lại dạng ban đầu và truyền đi được xa hơn.

Hình IV-4.Bộ lặp.

Tất cả các tín hiệu điện, bao gồm nhiễu điện từ và các lỗi khác cũng được lặp và khuyếch đại. Để bộ lặp hoat động, cả hai đoạn mạng nối với bộ lặp phải sử dụng cùng một phương pháp truy cập đường truyền.




Hình IV-5. Repeater trong mô hình OSI

### IV.2.3. Hub

Hub là thiết bị liên kết mạng được sử dụng làm trung tâm trong cấu trúc mạng có dạng hình sao (star). Mạng sao dùng sự phân chia tín hiệu trong Hub để đưa các tín hiệu ra các đường cáp khác nhau. Có 3 loại Hub thường sử dụng trong mạng là

- Hub chủ động: tái tạo và truyền tín hiệu giống như bộ lặp. Hub có nhiều cổng nên được gọi là bộ lặp đa cổng. Hub chủ động đưa các các tín hiệu mạnh hơn do đó cho phép đoạn cáp dài hơn. Đa phần các Hub là Hub chủ động.
- Hub thụ đông: hoặc động như các điểm kết nối, không tái tạo hay khuyếch đại tín hiệu.
- Hub lai: thích ứng với nhiều loại cáp khác nhau

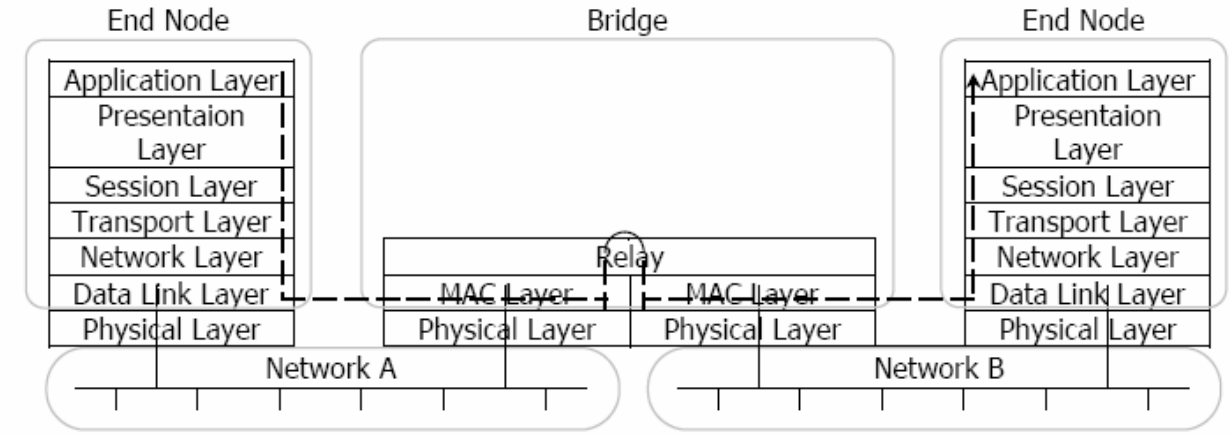
Hình IV-6.Hub

### IV.2.4. Cầu nối (Bridge)

Cầu nối là thiết bị hoạt động ở tầng liên kết dữ liệu, dùng để nối hai hay nhiều đoạn mạng (segment) của mạng LAN khác nhau.

Chức năng của cầu nối:

- Mở rộng khoảng cách phân đoạn mạng, tăng số lượng máy tính trên mạng.
- Lọc những gói dữ liệu để gửi đi hay không gửi đi cho đoạn nối, hoặc gửi trả lại nơi xuất phát.
- Phân chia mạng lớn thành nhiều mạng nhỏ nhằm cô lập lưu lượng, tăng tốc độ mạng. Nếu lưu lượng từ một nhóm máy tính trở nên quá tải và giảm hiệu xuất mạng thì cầu nối có thể cô lập máy tính hay bộ phận này.
- Kết nối các phương tiện truyền dẫn khác nhau.
- Kết nối các đoạn mạng sử dụng phương pháp truy cập khác nhau.




Hình IV-7.Bridge trong mô hình OSI

Nguyên lý hoạt động:

- Cầu nối không phân biệt giao thức này với giao thức khác, chỉ có nhiệm vụ lưu chuyển tất cả các giao thức trên mạng. Vì các giao thức đều có thể di chuyển qua cầu nối nên tùy thuộc vào từng máy quyết định chúng có thể nhận diện giao thức
- Cầu nối hoạt động trên nguyên tắc mỗi nút mạng có một địa chỉ riêng. Cầu nối chuyển gói dữ liệu dựa trên địa chỉ vật lý (MAC address) của nút đích. Khi dữ liệu truyền qua cầu nối, thông tin địa chỉ này sẽ được lưu trong RAM của cầu nối dùng để xây dựng bản địa chỉ dựa trên địa chỉ nguồn của gói tin.

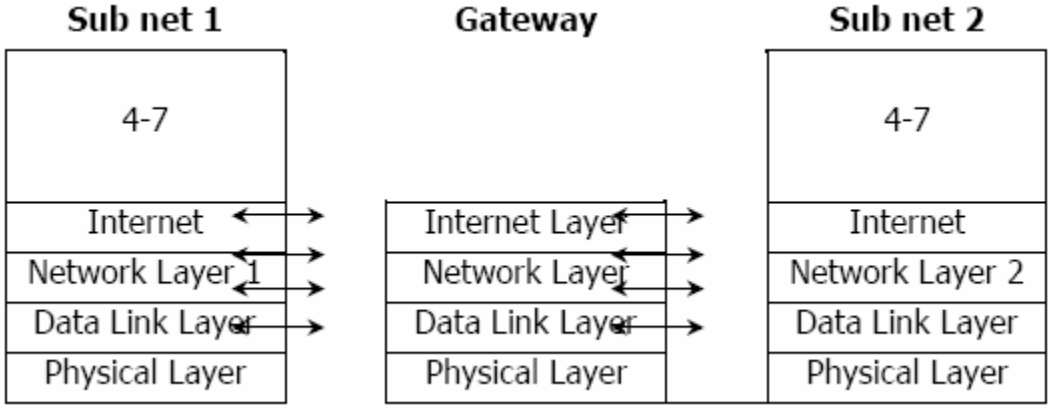
### IV.2.5. Bộ chuyển mạch (Switch)

Bộ chuyển mạch có chức năng giống cầu nối nhưng có nhiều port. Bộ chuyển mạch có thể kết nối một số mạng LAN riêng biệt và cung cấp khả năng lọc gói dữ liệu giữa chúng. Hiện nay, bộ chuyển mạch được sử dụng rộng rãi thay thế cho Hub.

Hình IV-8. Switch

### IV.2.6. Gateway

Gateway (cổng nối) hoạt động ở mức mạng, thực hiện việc ghép nối với WAN. Nguyên lý chung của nối kết này là tạo ra một tầng "liên mạng" (internet) trong tất cả các kiến trúc của mạng con tham gia nối kết. Tầng liên mạng thường là tầng con nằm ngay trên tầng 3 trong mô hình OSI.




Hình IV-9. Sơ đồ kiến trúc của gateway trong mô hình OSI.

Tầng con Internet được cài đặt trong tất cả các trạm cũng như trong các giao diện kết nối (gateway). Tầng này cung cấp dịch vụ truyền thông liên mạng với hai chức năng chính:

- Chuyển đổi các đơn vị dữ liệu của giao thức (Protocol Data Unit-PDU).
- Chọn đường đi cho các PDU này.

Các gói tin ở tầng con Internet lưu thông trong mạng theo phương pháp "đóng gói/tách gói". Khi một datagram được truyền từ mạng con này qua mạng con khác thông qua gateway thì nó được bổ sung vào hoặt tách ra các phần thông tin điều khiển cần thiết cho mạng con. Gateway có các giao thức xác định trước thường là nhiều giao thức, một gateway đa giao thức thường được chế tạo như các card có chứa các bộ xử lý riêng và cài đặt trên các máy tính hoặc thiết bị chuyên biệt.

## IV.3. Giao thức IP (IP Protocol)

Giao thức IP (Internet Protocol) hoạt động ở tầng mạng, cung cấp dịch vụ dữ liệu không liên kết (connectionless) cho nhiều giao thức liên kết dữ liệu khác. Đơn vị dữ liệu dùng trong IP là *datagram*, hay còn gọi là gói tin.

Chức năng chính của IP:

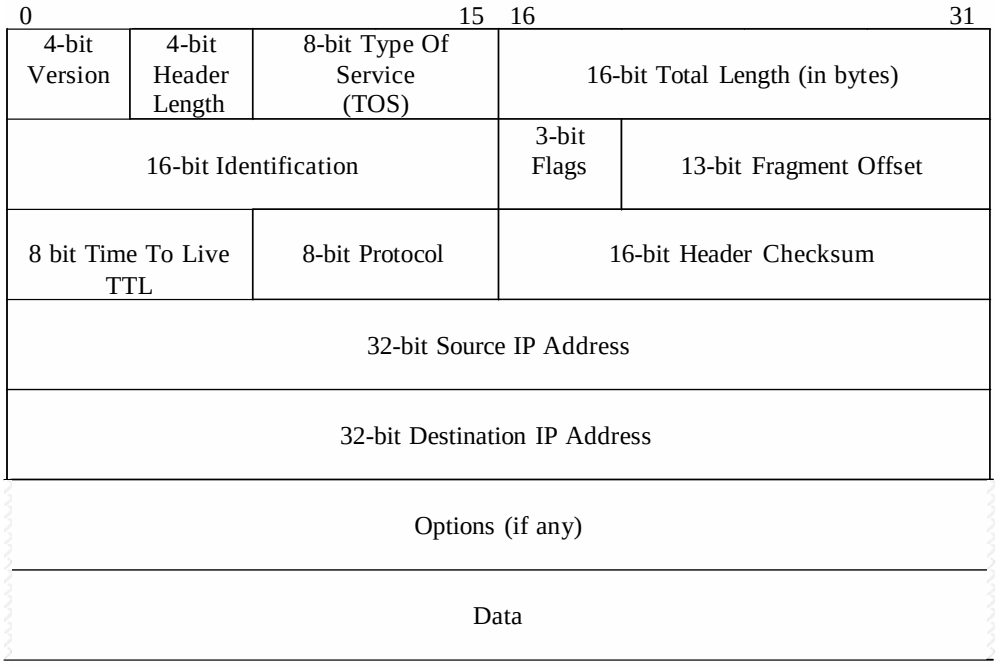
- Định nghĩa gói tin datagram là đơn vị dữ liệu cơ bản của việc truyền tin trên Internet.

- Xác định mô hình gán địa chỉ cho các gói tin và quản lý các quá trình trao đổi, xử lý các gói tin này.
- Chọn đường cho các datagram trên mạng.
- Phân đoạn và sắp xếp lại các gói tin.

Tính chất của giao thức IP

- Là giao thức hoạt động theo phương thức không nối kết.
- Không tin cậy: giao thức IP không có khả năng phát hiện và khắc phục lỗi, không quan tâm đến vấn đề dữ liệu có được nhận một cách chính xác không. Các gói dữ liệu có thể bị thất lạc, trùng lập, bị chậm hoặc không đúng thứ tự. Mỗi gói dữ liệu được xử lý độc lập và có thể gửi theo những đường định tuyến khác nhau.

### IV.3.1. Định dạng khung gói tin IP




Hình IV-10. Định dạng khung gói tin IP

Ý nghĩa các trường dữ liệu:

- *VER* (4 bits): chỉ version hiện hành của giao thức IP hiện được cài đặt, việc có chỉ số version cho phép có các trao đổi giữa các hệ thống sử dụng version cũ và hệ thống sử dụng version mới.
- *IHL* (4 bits): chỉ độ dài phần đầu (Internet header Length) của gói tin datagram, tính theo đơn vị từ ( 32 bits). Trường này bắt buột phải có

vì phần đầu IP có thể có độ dài thay đổi tùy ý. Độ dài tối thiểu là 5 từ (20 bytes), độ dài tối đa là 15 từ hay là 60 bytes.

- *Type of service* (8 bits): đặc tả các tham số về dịch vụ nhằm thông báo cho mạng biết dịch vụ nào mà gói tin muốn được sử dụng, chẳng hạn ưu tiên, thời hạn chậm trễ, năng suất truyền và độ tin cậy. Hình sau cho biết ý nghĩ của trường 8 bits này.

  - Precedence (3 bit): chỉ thị về quyền ưu tiên gửi datagram, nó có giá trị từ 0 (gói tin bình thường) đến 7 (gói tin kiểm soát mạng).
  - D (Delay) (1 bit): chỉ độ trễ yêu cầu trong đó (D = 0 gói tin có độ trễ bình thường, D = 1 gói tin độ trễ thấp)
  - T (Throughput) (1 bit): chỉ độ thông lượng yêu cầu sử dụng để truyền gói tin với lựa chọn truyền trên đường thông suất thấp hay đường thông suất cao.
    - T = 0 thông lượng bình thường và
    - T = 1 thông lượng cao
  - R (Reliability) (1 bit): chỉ độ tin cậy yêu cầu (R = 0 độ tin cậy bình thường, R = 1 độ tin cậy cao)
- *Total Length* (16 bits): chỉ độ dài toàn bộ gói tin, kể cả phần đầu tính theo đơn vị byte với chiều dài tối đa là 65535 bytes. Hiện nay giới hạn trên là rất lớn nhưng trong tương lai với những mạng Gigabit thì các gói tin có kích thước lớn là cần thiết.
- *Identification* (16 bits): cùng với các tham số khác (như Source Address và Destination Address) tham số này dùng để định danh duy nhất cho một datagram trong khoảng thời gian nó vẫn còn trên liên mạng.
- *Flags (3 bits):* liên quan đến sự phân đoạn (fragment) các datagram, Các gói tin khi đi trên đường đi có thể bị phân thành nhiều gói tin nhỏ, trong trường hợp bị phân đoạn thì trường Flags được dùng điều khiển phân đoạn và tái lắp ghép bó dữ liệu. Tùy theo giá trị của Flags sẽ có ý nghĩa là gói tin sẽ không phân đoạn, có thể phân đoạn hay là gói tin phân đoạn cuối cùng. Trường ***Fragment Offset*** cho biết vị trí dữ liệu thuộc phân đoạn tương ứng với đoạn bắt đầu của gói dữ liệu gốc. Ý nghĩa cụ thể của trường Flags là:

  - bit 0: reserved - chưa sử dụng, luôn lấy giá trị 0.
  - bit 1: (DF) = 0 (May Fragment) = 1 (Don't Fragment)
  - bit 2: (MF) = 0 (Last Fragment) = 1 (More Fragments)

- Fragment Offset (13 bits): chỉ vị trí của đoạn (fragment) ở trong datagram tính theo đơn vị 8 bytes, có nghĩa là phần dữ liệu mỗi gói tin (trừ gói tin cuối cùng) phải chứa một vùng dữ liệu có độ dài là bội số của 8 bytes. Điều này có ý nghĩa là phải nhân giá trị của Fragment offset với 8 để tính ra độ lệch byte.
- *Time to Live (8 bits)*: qui định thời gian tồn tại của gói tin trong mạng để tránh tình trạng một gói tin bị quẩn trên mạng. Thời gian này được cho bởi trạm gửi và được giảm đi (thường qui ước là 1 đơn vị) khi datagram đi qua mỗi router của liên mạng. Thời lượng này giảm xuống tại mỗi router với mục đích giới hạn thời gian tồn tại của các gói tin và kết thúc những lần lặp lại vô hạn trên mạng. Sau đây là 1 số điều cần lưu ý về trường ***Time To Live***:
  - Nút trung gian của mạng không được gởi 1 gói tin mà trường này có giá trị= 0.
  - Một giao thức có thể ấn định **Time To Live** để thực hiện cuộc ra tìm tài nguyên trên mạng trong phạm vi mở rộng.
  - Một giá trị cố định tối thiểu phải đủ lớn cho mạng hoạt động tốt.
- *Protocol (8 bits): chỉ giao thức tầng trên kế tiếp sẽ nhận vùng dữ liệu ở* trạm đích (hiện tại thường là TCP hoặc UDP được cài đặt trên IP). Ví dụ: **TCP** có giá trị trường **Protocol** là 6, **UDP** có giá trị trường **Protocol** là 17.
- Header Checksum (16 bits): Mã kiểm soát lỗi của header gói tin IP.
- Source Address (32 bits): Địa chỉ IP của máy nguồn.
- Destination Address (32 bits): Địa chỉ IP của máy đích.
- Options (độ dài thay đổi): Khai báo các lựa chọn do người gửi yêu cầu (tuỳ theo từng chương trình).
- Padding (độ dài thay đổi): Vùng đệm, được dùng để đảm bảo cho phần header luôn kết thúc ở một mốc 32 bits.
- *Data (độ dài thay đổi)*: Trên một mạng cục bộ như vậy, hai trạm chỉ có thể liên lạc với nhau nếu chúng biết địa chỉ vật lý của nhau. Như vậy vấn đề đặt ra là phải thực hiện ánh xạ giữa địa chỉ IP (32 bits) và địa chỉ vật lý (48 bits) của một trạm.

### IV.3.2. Phân mảnh và sắp xếp lại

Mỗi mạng đều có một maximum transmission unit (MTU), đây là kích thước lớn nhất mà một IP datagram có thể mang trong một khung. Chú ý rằng giá trị này thì nhỏ hơn kích thước gói lớn nhất trên mạng bởi vì IP datagram cần điều chỉnh cho phù hợp với khung trong tầng liên kết.

Lúc một gói gửi một IP datagram nó có thể chọn bất cứ kích thước nào mà nó muốn. Thông thường nó chọn bằng MTU của mạng mà host được nối kết trực tiếp. Sự phân mảnh sẽ được thực hiện nếu đường dẫn nguồn đi qua một mạng có MTU nhỏ hơn. Các giao thức vận chuyển ở trên IP sẽ truyền một gói có kích thước lớn hơn MTU cục bộ và host nguồn phải phân mảnh nó.

Sự phân mảnh thường xuất hiện ở các router lúc nó nhận một datagram và datagram này phải truyền qua một mạng có MTU nhỏ hơn kích thước của datagram nó nhận. Và sự sắp xếp xảy ra tại host đích nơi nó nhận datagram(các gói phải có cùng Id trong trường Ident), trường này được chọn bởi host gửi và nó định danh duy nhất trong số tất cả các datagram đến đích qua một khoảng thời gian nào đó (IP không cố gắng tìm lại khi sự phân mảnh bị lỗi).

Ví dụ một gói tin 4000 bytes và MTU là 1500:

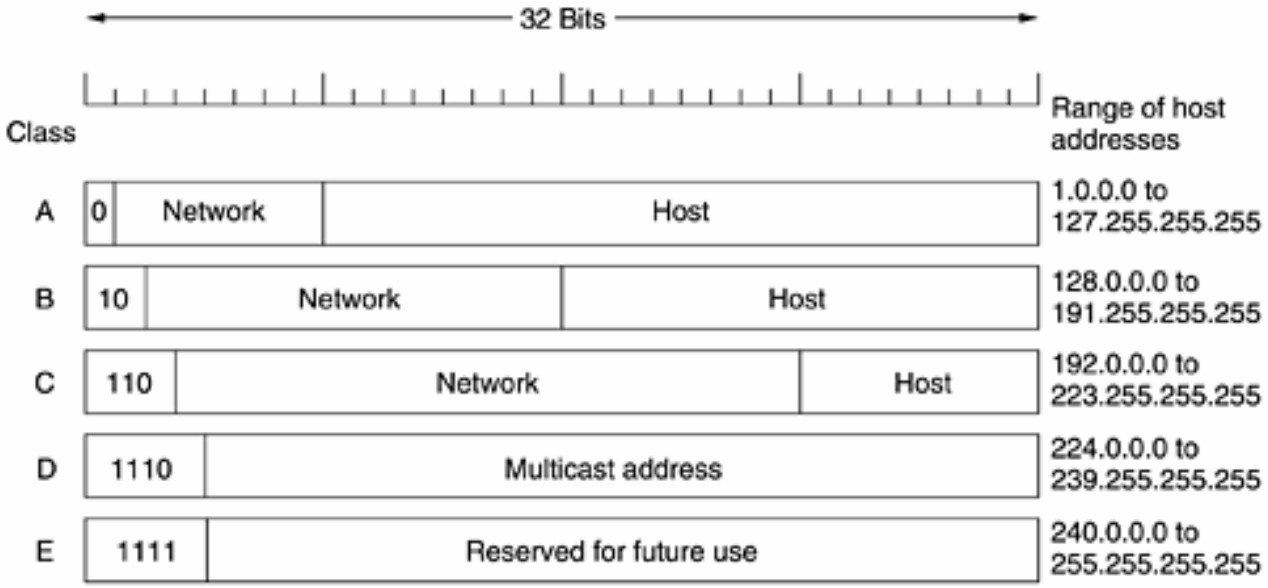
### IV.3.3. Địa chỉ IP

Sơ đồ địa chỉ hóa để định danh các trạm (host) trong liên mạng được gọi là địa chỉ IP 32 bits (32 bit IP address). Mỗi giao diện trong 1 máy có hỗ trợ giao thức IP đều phải được gán 1 địa chỉ IP (một máy tính có thể gắn với nhiều mạng do vậy có thể có nhiều địa chỉ IP). Địa chỉ IP gồm 2 phần: địa chỉ mạng (netid) và địa chỉ máy (hostid). Mỗi địa chỉ IP có độ dài 32 bits được tách thành 4 vùng (mỗi vùng 1 byte), có thể biểu thị dưới dạng thập phân, bát phân, thập lục phân hay nhị

phân. Cách viết phổ biến nhất là dùng ký pháp thập phân có dấu chấm (dotted decimal notation) để tách các vùng. Mục đích của địa chỉ IP là để định danh duy nhất cho một máy tính bất kỳ trên liên mạng.

Do tổ chức và độ lớn của các mạng con (subnet) của liên mạng có thể khác nhau, người ta chia các địa chỉ IP thành 5 lớp, ký hiệu là A, B, C, D và E. Trong lớp A, B, C chứa địa chỉ có thể gán được. Lớp D dành riêng cho lớp kỹ thuật multicasting. Lớp E được dành những ứng dụng trong tương lai.

Netid trong địa chỉ mạng dùng để nhận dạng từng mạng riêng biệt. Các mạng liên kết phải có địa chỉ mạng (netid) riêng cho mỗi mạng. Ở đây các bit đầu tiên của byte đầu tiên được dùng để định danh lớp địa chỉ (0 - lớp A, 10 - lớp B, 110 - lớp C, 1110 - lớp D và 11110 - lớp E).




Hình IV-11. Phân lớp địa chỉ IP

Khi sử dụng mạng cục bộ, không liên kết với mạng khác người sử dụng có thể gán tùy ý địa chỉ IP cho các trạm. Tuy nhiên với các site Internet thì địa chỉ IP phải được cung cấp bởi trung tâm quản lý thông tin mạng (NIC-Network Information Center).

Một số địa chỉ IP đặc biệt:

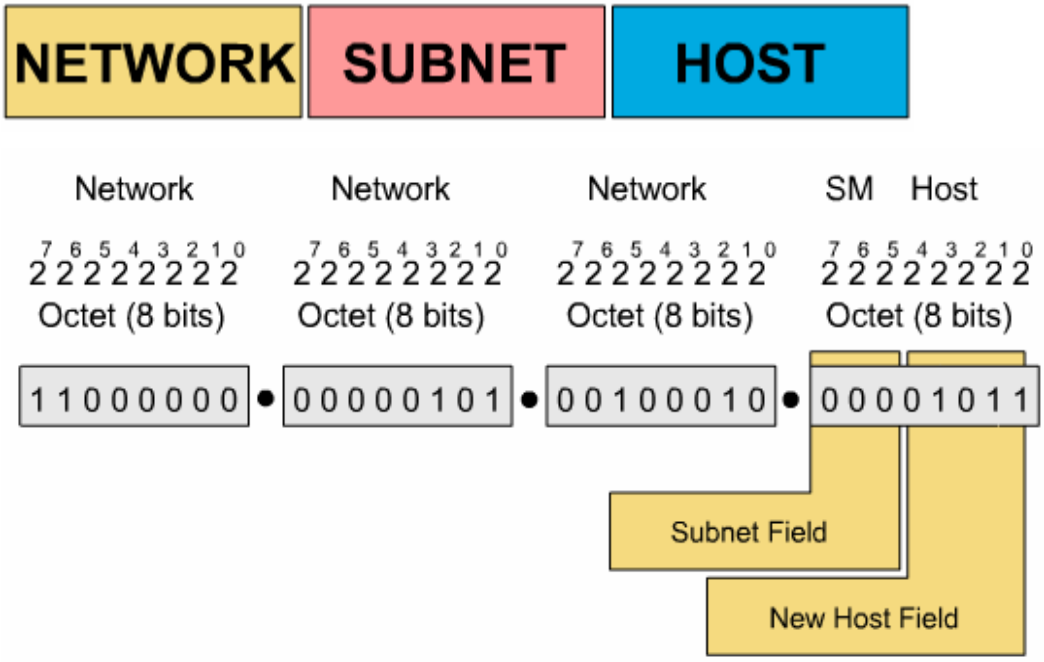
- Địa chỉ Loopback (127.x.x.x): tất cả các gói tin được gửi đến địa chỉ 127.0.0.0 đều được gửi trở lại máy tính.Địa chỉ loopback có thể được dùng như một địa chỉ kiểm tra nhanh xem phần mền TCP/IP có được cấu hình thích hợp. Trên hệ điều hành Windows thường dùng 127.0.0.1, Unix 127.0.0.*
- Địa chỉ quảng bá (broadcast address): địa chỉ này có các bit của phần hostID đều mang giá trị 1, được sử dụng khi muốn gửi gói tin đến tất cả

các máy của mạng con. Ví dụ địa chỉ 192.168.1.0 có địa chỉ quảng bá là 192.168.1.255.

**Mặt nạ mạng con(sunet mask):** là một số 32 bit bao gồm các bit cao = 1 và các bit thấp = 0. Các bit 1 quy định subnet, các bit 0 quy định địa chỉ host.từ subnet mask có thể xác định ranh giới giữa địa chỉ mạng và địa chỉ của interface (host). Thực hiện phép toán AND giữa địa chỉ IP và sunet mask sẽ cho địa chỉ mạng.

Ví dụ: địa chỉ IP lớp B 172.16.1.1, có mặt nạ 255.255.0.0 sẽ cho địa chỉ mạng là 172.16.0.0

**Mạng con (subnet):** để thuận lợi cho việc định tuyến dữ liệu trên mạng lớn, người ta thường tổ chức mạng IP theo cơ chế địa chỉ phân cấp, mỗi mạng được chia nhỏ thành nhiều mạng con. Mỗi mạng con chịu trách nhiệm cho việc chọn đường cho các gói tin IP trong mạng của mình, các gói tin này được nhận ra nhờ phần địa chỉ mạng. Trong các lớp mạng A, B, C thì phần địa chỉ mạng cố định. Tuy nhiên, để tạo sự linh hoạt khi phân chia mạng con thì địa chỉ mạng có thể mở rộng sang các bit của phần host, đó là kĩ thuật phân chia mạng con




Hình IV-12. Chia mạng con

### IV.3.4. Các bước hoạt động của giao thức IP

Khi giao thức IP được khởi động nó trở thành một thực thể tồn tại trong máy tính và bắt đầu thực hiện những chức năng của mình, lúc đó thực thể IP là cấu thành của tầng mạng, nhận yêu cầu từ các tầng trên nó và gửi yêu cầu xuống các tầng dưới nó.

Đối với thực thể IP ở máy nguồn, khi nhận được một yêu cầu gửi từ tầng trên, nó thực hiện các bước sau đây:

- Tạo một IP datagram dựa trên tham số nhận được.
- Tính checksum và ghép vào header của gói tin.
- Ra quyết định chọn đường: hoặc là trạm đích nằm trên cùng mạng hoặc một gateway sẽ được chọn cho chặng tiếp theo.
- Chuyển gói tin xuống tầng dưới để truyền qua mạng.

Đối với router, khi nhận được một gói tin đi qua, nó thực hiện các động tác sau:

1. Tính chesksum, nếu sai thì loại bỏ gói tin.
2. Giảm giá trị tham số Time-to-Live. nếu thời gian đã hết thì loại bỏ gói tin.
3. Ra quyết định chọn đường.
4. Phân đoạn gói tin, nếu cần.
5. Kiến tạo lại IP header, bao gồm giá trị mới của các vùng Time - to - Live, Fragmentation và Checksum.
6. Chuyển datagram xuống tầng dưới để chuyển qua mạng.

Cuối cùng khi một datagram nhận bởi một thực thể IP ở trạm đích, nó sẽ thực hiện bởi các công việc sau:

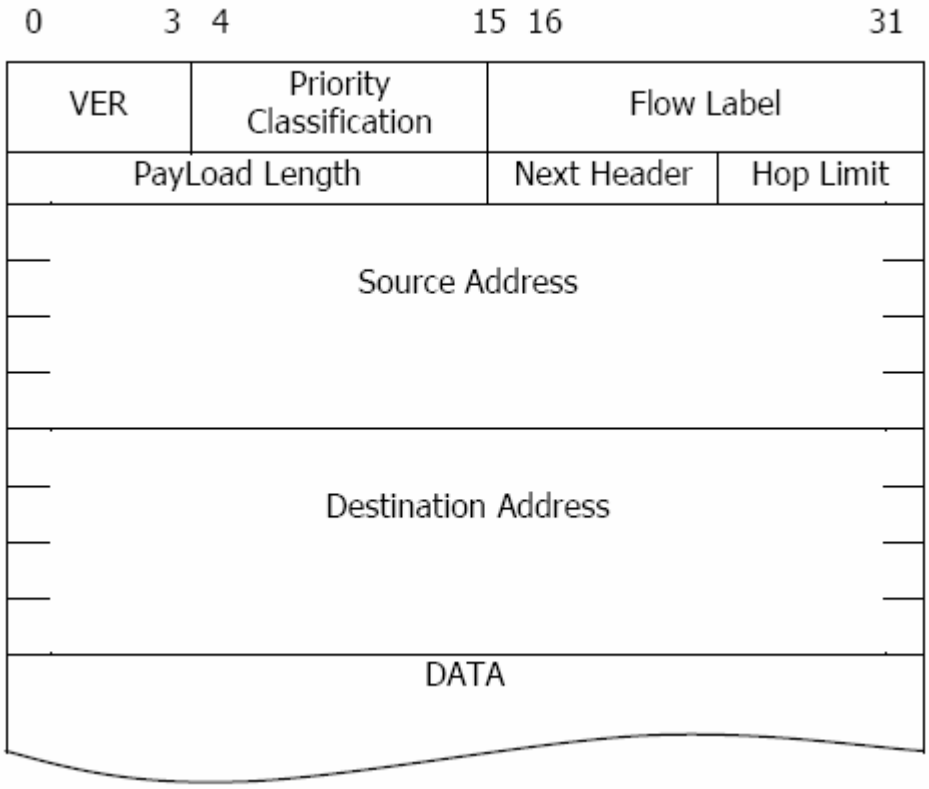
1. Tính checksum. Nếu sai thì loại bỏ gói tin.
2. Tập hợp các đoạn của gói tin (nếu có phân đoạn)
3. Chuyển dữ liệu và các tham số điều khiển lên tầng trên.

### IV.3.5. IPv6

Với sự phát triển nhanh chóng của Internet thì địa chỉ IP 32 bit không còn đáp ứng đủ cho nhu cầu sử dụng Internet. Để khắc phục điều này, phiên bản IPv6 (IP Next Generation) đang được phát triển. Phiên bản IPv6 có các thay đổi sau:

- Sử dụng 128 bit địa chỉ mạng thay vì 32 bit địa chỉ như phiên bản IPv4.
- Mở rộng phần Header cho ứng dụng và lựa chọn của khung tin.
- Hỗ trợ các loại dữ liệu video và audio.
- Có các giao thức mở rộng: cho phép bổ sung nhiều thông tin vào một datagram.

Định dạng khung header của IPv6:




Hình IV-13. Định dạng khung IPv6

## IV.4. Các giao thức liên quan đến IP

Để mạng với giao thức IP hoạt động được tốt người ta cần một số giao thức bổ sung, các giao thức này đều không phải là bộ phận của giao thức IP và giao thức IP sẽ dùng đến chúng khi cần.

- **Giao thức ARP (Address Resolution Protocol):** Ở đây cần lưu ý rằng các địa chỉ IP được dùng để định danh các host và mạng ở tầng mạng của mô hình OSI, và chúng không phải là các địa chỉ vật lý (hay địa chỉ MAC) của các trạm trên đó một mạng cục bộ (Ethernet, Token Ring.). Trên một mạng cục bộ hai trạm chỉ có thể liên lạc với nhau nếu chúng biết địa chỉ vật lý của nhau. Như vậy vấn đề đặt ra là phải tìm được ánh xạ giữa địa chỉ IP (32 bits) và địa chỉ vật lý của một trạm. *Giao thức ARP* đã được xây dựng để tìm địa chỉ vật lý từ địa chỉ IP khi cần thiết.
- **Giao thức RARP (Reverse Address Resolution Protocol):** Là giao thức ngược với *giao thức ARP*. Giao thức RARP được dùng để tìm địa chỉ IP từ địa chỉ vật lý.
- **Giao thức ICMP (Internet Control Message Protocol):** Giao thức này thực hiện truyền các thông báo điều khiển (báo cáo về các tình trạng các

lỗi trên mạng.) giữa các gateway hoặc một nút của liên mạng. Tình trạng lỗi có thể là: một gói tin IP không thể tới đích của nó, hoặc một router không đủ bộ nhớ đệm để lưu và chuyển một gói tin IP. Một thông báo ICMP được tạo và chuyển cho IP, IP sẽ "bọc" (encapsulate) thông báo đó với một IP header và truyền đến cho router hoặc trạm đích.

## IV.5. Giao thức định tuyến

Chúng ta cho rằng cả chuyển mạch và router không đủ thông tin về topology mạng để chúng có thể quyết định chọn đúng cổng cho các gói được output. Trong trường hợp chuyển mạch kênh, định tuyến là vấn đề chỉ cho các gói yêu cầu nối kết, còn tất cả các gói theo sau thì đi cùng đường dẫn như gói yêu cầu.

Trong mạng datagram(mạng IP), định tuyến là vấn đề của tất cả các gói. Một chuyển mạch hay một router cần phải xem xét các địa chỉ đích trong mỗi gói và rồi quyết định cổng tốt nhất mà gói có thể truyền. Chuyển mạch thực hiện quyết định dựa trên các thông tin trong bảng chuyển tiếp. Vấn đề cơ bản của quá trình chuyển tiếp là các chuyển mạch hay router lấy được thông tin trong các bảng này.

- Quá trình chuyển tiếp bao gồm lấy một gói, xem địa chỉ nguồn, tham khảo bảng và gửi gói đó theo hướng được xác định bởi dữ liệu trong bảng đó.
- Định tuyến là một quá trình xây dựng bảng.

Xem bảng sau, trong trường hợp bảng định tuyến có nghĩa là mạng số 10 có thể đến bởi router chặng tiếp theo có địa chỉ 171.69.245.10, trong khi bảng forwarding chứa thông tin chính xác như thế nào để chuyển gói chặng tiếp theo, gửi gói ra ngoài qua giao tiếp 0 với địa chỉ 8:0:2b:e4:b:1:2.

| NetworkNum | NextHop |
|---|---|
| 10 | 171.69.245.10 |

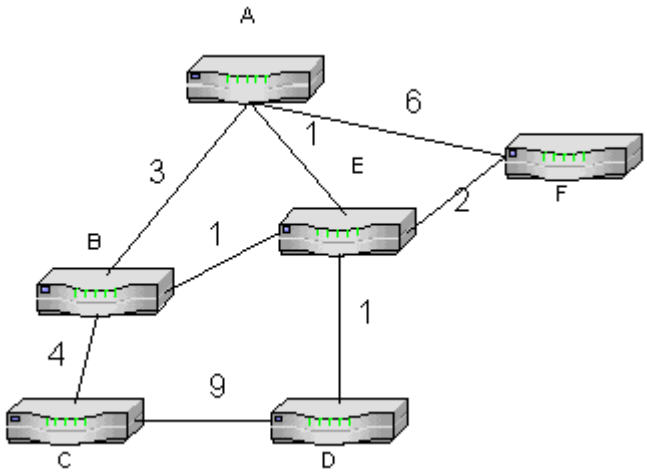
a)Bảng định tuyến

| NetworkNum | Interface | MAC address |
|---|---|---|
| 10 | If0 | 8:0:2b:e4:b:1:2 |

b)Bảng forwarding

### 1. Mạng là đồ thị:

Định tuyến là một bài toán của đồ thị, hình trên là một đồ thị thể hiện một mạng, một nút của đồ thị là các nhãn từ A đến F, các nhãn có thể là host, chuyển mạch, router hay một mạng. Trong trường hợp này chúng ta chỉ quan tâm các nút là router. Các cạnh của đồ thị tương ứng với một liên kết mạng. Mỗi cạnh được gán một trọng số(chi phí).




Hình IV-14.Mạng thể hiện như đồ thị

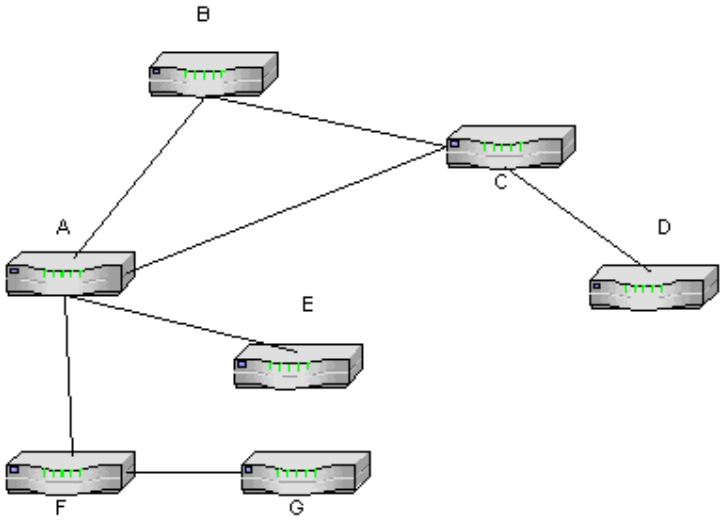
Vấn đề cơ bản của định tuyến là tìm được một đường đi có chi phí thấp nhất giữa hai nút(chi phí của đường đi bằng tổng chi phí của tất cả các cạnh trên đường đi).

Có 2 cách xây dựng định tuyến cho các nút:

- Tính tất cả các đường đi ngắn nhất và lưu trữ chúng trên mỗi nút.
- Thực hiện giao thức định tuyến tương ứng giữa tất cả các nút.

Chúng ta giả sử chi phí mỗi cạnh trong mạng có thể biết được, chúng ta xem xét hai lớp giao thức routing chính được sử dụng trong mạng: distance vector và link state.

**2. Định tuyến theo vector khoảng cách-Distance Vector(RIP):**




Hình IV-15. Ví dụ về định tuyến Distance Vector

**Ý tưởng:**

Mỗi nút xây dựng một mảng một chiều(vector) chứa khoảng cách(chi phí) đến tất cả các nút và phân phối vector đó với người hàng xóm của chúng. Để bắt đầu xây dựng, mỗi nút phải biết chi phí của các liên kết trực tiếp với người hàng xóm của chúng. Sau đó nó mới gán một chi phí xác định.

| Thoâng tin löu trõõ ôû Nuùt | Khoaûng caùch ñeán caùc nuùt | | | | | | |
|---|---|---|---|---|---|---|---|
| | A | B | C | D | E | F | G |
| A | 0 | 1 | 1 | ∞ | 1 | 1 | ∞ |
| B | 1 | 0 | 1 | ∞ | ∞ | ∞ | ∞ |
| C | 1 | 1 | 0 | 1 | ∞ | ∞ | ∞ |
| D | ∞ | ∞ | 1 | 0 | ∞ | ∞ | 1 |
| E | 1 | ∞ | ∞ | ∞ | 0 | ∞ | ∞ |
| F | 1 | ∞ | ∞ | ∞ | ∞ | 0 | 1 |
| G | ∞ | ∞ | ∞ | 1 | ∞ | 1 | 0 |

Bảng IV-1.Khởi tạo khoảng cách tại mỗi nút

Bảng trên trình bày thông tin khởi tạo về khoảng cách của từng nút đến tất cả các nút còn lại trong mạng.

Mỗi hàng trong bảng là một danh sách khoảng cách từ một nút đến tất cả các nút khác. Khởi tạo, mỗi nút đặt một chi phí là 1 cho tất cả các người hàng xóm của chúng và cho tất cả các nút khác. Thật vậy, lúc khởi tạo A có thể tin rằng nó có thể đi 1 bước tới B, nhưng không thể đến D. Bảng định tuyến lưu trữ ở A như sau:

| Destination | Cost | NextHop |
|---|---|---|
| B | 1 | B |
| C | 1 | C |
| D | ∞ | - |
| E | 1 | E |
| F | 1 | F |
| G | ∞ | - |

Bảng IV-2.Khởi tạo bảng định tuyến ở nút A

Tiếp theo mỗi nút gửi một thông điệp chứa danh sách khoảng cách cá nhân của nó trực tiếp đến các nút hàng xóm. Ví dụ nút F nói với nút A là nó có thể đến G với chi phí là 1; A biết nó có thể đến F với chi phí 1, nó cộng chi phí này với chi phí đến G từ F. Tổng chi phí là 2. Vậy A có thể đến G với chi phí là 2 qua F. Tương tự A có thể học từ C và biết rằng nó có thể đến D với chi phí là 2 qua C.

Lúc này A có thể cấp nhật bảng định tuyến với chi phí và chặng tiếp theo (nexthop) cho tất cả các nút trên mạng. Kết quả trong bảng sau:

| Destination | Cost | NextHop |
|---|---|---|
| B | 1 | B |
| C | 1 | C |
| D | 2 | C |
| E | 1 | E |
| F | 1 | F |
| G | 2 | F |

Bảng IV-3.Bảng định tuyến hoàn chỉnh ở nút A

Có hai tình huống khác nhau lúc một nút quyết định gửi bảng cập nhật routing đến hàng xóm của nó.

Cập nhật định kỳ: mỗi nút tự động gửi cập nhật sau một khoảng thời gian dù không có sự thay đổi, nó nhằm thông báo cho các nút khác là nó vẫn còn chạy, nó cũng đảm bảo rằng nó muốn lấy thông tin khác nếu người hàng xóm của nó bị hỏng.

Cập nhật phản ứng (triggered): xảy ra bất cứ lúc nào một nút nhận một cập nhật từ một người hàng xóm mà nó có sự thay đổi trong bảng routing.

Giả sử nút F phát hiện ra nút G sai. Đầu tiên F đặt khoảng cách mới tới G là không xác định và nó gởi thông tin này tới A, bởi vì A biết rằng nó có thể đi tới G 2 bước qua F , A cũng sẽ đặt khoảng cách tới G là không xác định, Tuy nhiên, với việc cập nhật kế tiếp từ , A sẽ học là C có thể đi 2 bước đến G. Thật vậy, A sẽ biết đến G với 3 bước qua C, nó sẽ cập nhật giá trị này vào bảng, lúc nó quảng cáo đến Khung, nút F sẽ học đến G 4 bước qua A. Để ngăn ngừa trường hợp này, ví dụ lúc liên kết từ A đến E bị hỏng, trong lần cập nhật tiếp theo, A quảng cáo một khoảng cách không xác định đến Ethernet, nhưng B và C quảng cáo 2 bước tới E. Dựa vào một khoảng thời gian, vấn đề có thể xảy ra, nút B nghe rằng nó có thể đến E hai bước từ C, vậy nó có thể đến Ethernet 3 bước và quảng cáo với A, nút kết luận rằng nó có thể đến E 4 bước và quảng cáo tới C ….vòng lặp này chỉ kết thúc khi khoảng cách tăng đến một số đủ lớn. Nghĩa là, không có nút nào thật sự biết E là nút không thể đến. Có một vài cách để giải quyết vấn đề này:

- Sử dụng một số nhỏ nhất để xác định khoảng cách, ví dụ chúng ta có thể quyết định số chặng lớn nhất qua một mạng nào đó sẽ không bao giờ lớn hơn 16.
- Split hozizon: lúc một nút gửi một routing cập nhật đến hàng xóm của nó, nó không gởi router mà nó học từ mỗi hàng xóm trở lại router đó. Ví dụ, nếu B có router(E,2,A) trong bảng của nó, và nó biết rằng nó học cái này từ router A, và vì vậy bất cứ lúc nào B gửi router cập nhật đến A, nó sẽ không gửi router(E,2). B thật sự gửi router đó về A, nhưng nó đặt một thông tin phủ nhận để đảm bảo rằng A không thể đến E từ B, ví dụ B gửi router(E, ) đến A.

| Thoâng tin löu tröõ ôû Nuùt | Khoaûng caùch ñeán caùc nuùt | | | | | | |
|---|---|---|---|---|---|---|---|
| | A | B | C | D | E | F | G |
| A | 0 | 1 | 1 | 2 | 1 | 1 | 2 |
| B | 1 | 0 | 1 | 2 | 2 | 2 | 3 |
| C | 1 | 1 | 0 | 1 | 2 | 2 | 2 |
| D | 2 | 3 | 1 | 0 | 3 | 2 | 1 |
| E | 1 | 2 | 2 | 3 | 0 | 2 | 3 |
| F | 1 | 2 | 2 | 2 | 2 | 0 | 1 |
| G | 2 | 3 | 2 | 1 | 3 | 1 | 0 |

Bảng IV-4.Khoảng cách hoàn chỉnh ở tất cả các nút

### 3. Định tuyến theo trạng thái kết nối-Link state(OSPF):

Thông đường theo trạng thái liên kết là một lớp thứ hai quan trọng của giao thức lộ trình. Mỗi nút cho rằng nó có khả năng tìm ra trạng thái liên kết với người hàng xóm của nó và chi phí của mỗi liên kết(chúng ta muốn cung cấp cho mỗi nút đầy đủ thông tin để có thể nó tìm ra một đường đi có chi phí nhỏ nhất đến bất cứ địa chỉ nào).

**Ý tưởng:**

Mỗi nút biết như thế nào để nối kết trực tiếp với hàng xóm của nó, và nếu chúng ta đảm bảo rằng toàn bộ những hiểu biết này được phổ biến đến tất cả các nút và rồi mỗi nút đủ kiến thức để xây dựng một sơ đồ mạng hoàn chỉnh. Đây rõ ràng là một điều kiện lý tưởng cho việc tìm đường đi ngắn nhất cho bất kỳ điểm nào trong mạng. Giao thức thông đường trạng thái liên kết dựa vào hai kỹ thuật chính:

- Đảm bảo sự phổ biến thông tin trạng thái liên kết.
- Tính toán đường đi từ tổng hợp tất cả các trạng thái liên kết mà nó biết.

**Reliable Flooding**

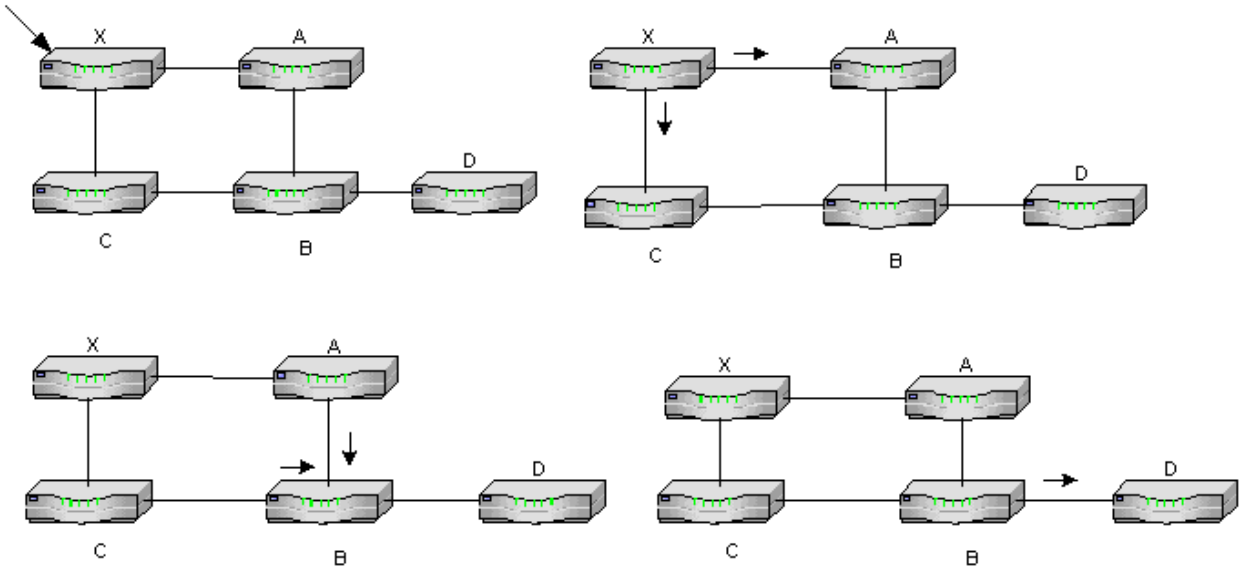
Đây là một quá trình nhằm đảm bảo tất cả các nút tham gia liên kết có một bản sao thông tin trạng thái liên kết từ tất cả các nút khác. "Flooding" có nghĩa rằng một nút gửi thông tin trạng thái liên kết ra tất cả các hàng xóm nối kết trực tiếp đến nó và mỗi nút nhận thông tin này tiếp tục chuyển ra tất cả các nút khác. Quá trình này tiếp tục cho tới khi chúng truyền thông tin đến toàn bộ mạng. Chính xác hơn, mỗi nút tạo một gói (LSP) chứa các thông tin sau:

- ID của nút tạo ra LSP
- Danh sách chi phí từ nó đến các hàng xóm nối kết trực tiếp.
- Một số thứ tự.

- Thời gian sống của gói.

Flooding làm việc theo cách sau:

Đầu tiên thực hiện truyền một LSP giữa các router nằm sát nhau(nó đảm bảo truyền bằng cách sử dụng cách thức truyền và hồi báo), tuy nhiên có nhiều bước cần đảm bảo flooding một LSP đến tất cả các nút trong mạng. Xem xét một nút X mà nó nhận bản sao của LSP từ host Y. X kiểm tra xem nó đã thật sự lưu trữ một bản sao LSP từ Y hay chưa, nếu chưa thì lưu trữ nó, ngược lại nó so sánh số thứ tự, nếu nó cho rằng bảng mới nhất thì nó thay thế cái củ, tiếp theo X gửi một bản sao LSP đó đến tất cả người hàng xóm ngoại trừ Y , và sau đó thông tin này sẽ đến tất cả các nút.




Hình IV-16. Flooding gói qua trạng thái liên kết.

Hình trên là một ví dụ chỉ ra một LSP bị flooding trong một mạng nhỏ.

Mỗi nút có thể sinh ra LSP theo hai cách:

- Theo một khoảng thời gian định sẳn,
- Thay đổi sơ đồ nối kết có thể là nguyên nhân một nút tạo ra một LSP mới(chỉ thực hiện khi có một nút mới tham gia nối kết hay một liên kết bị hỏng). Nó có thể phát hiện sự hỏng hóc bằng cách gửi một thông điệp thăm dò, nếu sau một khoảng thời gian không nhận được hồi báo nó xem như hàng xóm bị hỏng và tạo ra một LSP mới.

Một trong những mục tiêu thiết kế quan trọng của giao thức flooding là các thông tin mới nhất phải được flood đến tất cả các nút nhanh chóng, trong khi các thông tin cũ phải được di chuyển từ mạng và không cho phép lưu thông. Thêm vào đó nó giảm tổng phí giao thông trên mạng.

Một cách để làm giảm sự quá tải trên mạng là bằng cách tránh tạo ra LSP trừ khi thật sự cần thiết. Nó được thực hiện bằng cách gán một thời gian dài, thường là một vài giờ cho việc tạo ra một LSP mới.

Để đảm bảo rằng thông tin củ được thay thế bởi thông tin mới hơn, LSP mang một số thứ tự. Mỗi lần sinh ra một LSP mới, nó tăng số thứ tự lên 1, trường này tới 64 bit. Nếu một nút bị hỏng và nối kết lại nó gán số thứ tự này bằng 0. Nếu nút đó bị hỏng trong một thời gian dài, tất cả các LSP của nút sẽ bị xoá, ngược lại nếu nó nhận một bảng sao của chính nó với số thứ tự cao hơn, nó có thể gia tăng và sau đó sử dụng số thứ tự này.

LSP cũng mang một thời gian sống(time-to-live), nó dùng để đảm bảo rằng thông tin liên kết củ phải được di chuyển khỏi mạng. Một nút luôn luôn giảm TTL của một LSP mới nhận trước khi gửi nó cho tất cả các người hàng xóm.

**Tính toán đường đi**

Khi một nút có một bản sao của LSP từ các nút khác, nó có thể tạo ra một sơ đồ hoàn chỉnh của mạng và từ bảng đồ này nó có thể quyết định đường đi tốt nhất đến đích. Dựa vào thuật tóan Dijkstra, tưởng tượng rằng một nút lấy tất cả LSP mà nó nhận và xây dựng một đồ thị thể hiện đường đi trên mạng.

**Thuật toán:**

- N tập tất cả các nút trong đồ thị.
- l(i,j) chi phí cho cạnh(i,j)
- s chỉ nút hiện tại.
- C(n) chi phí đường đi từ s đến n
- M chỉ tập các nút
- Thuật toán tìm đường đi ngắn nhất:
  - M={s}
  - For each n in N-{s}

    C(n) = l(s,n)
  - While (N!=M)
    - M = M U {w} mà C(w) là giá trị nhỏ nhất trong tất cả w in (N-M)
    - For each n in (N-M)

      C(n) = MIN(C(n), C(w) + l(w,n))

Trong thực tế, mỗi chuyển mạch tính bảng table routing của nó từ các LSP, nó sử dụng thuật toán forward search. Mỗi chuyển mạch chứa hai danh sách

Tentative và Confirmed. Mỗi danh sách này chứa một tập các entry dạng <Destination, Cost, NextHop>. Thuật toán làm việc như sau:

1. Khởi tạo danh sách confirmed với một entry cho chính nó, với chi phí là 1.
2. Cho nút vừa thêm đến danh sách confirmed trong bước trước, gọi nút Next.
3. Cho mỗi hàng xóm của Next tính cost(chi phí) đến các hàng xóm này(bằng tổng chi phí từ chính nó đến Next và từ Next đến hàng xóm).
4. If hàng xóm hiện tại không có trong confirmed và tentative, thêm (Neighbor, Cost, NextHop) tới danh sách tentative
5. If hàng xóm hiện tại trên danh sách tentative, và chi phí hiện tại thấp hơn chi phí hiện tại, thay thế entry với (Neighbor, Cost, Nexthop).
6. If tentative rỗng, thì dừng lại, ngược lại lấy từ danh sách Tentative một entry chi phí thấp nhất và đặt nó vào danh sách Confirmed và chạy lại bước 2.

## IV.6. Định tuyến trên Internet

Do qui mô của mạng Intern là rất lớn, một nút không thể chứa tất cả các bản ghi cho mọi đích và việc cập nhật bảng dẫn đường tốn kém. Vì vậy mạng Internet được thành các hệ tự trị AS-Autonomous System, mỗi AS chứa nhiều mạng. Người quản trị mạng chịu trách nhiệm chọn giao thức định tuyến cho một AS bằng các giao thức định tuyến intra-AS (intra-AS routing protocol). Tiếp đó các gói dữ liệu được định tuyến giữa các AS khác nhau bằng giao thức định tuyến inter-AS (intra-AS routing protocol)

### 1. Intra-Autonomous System Routing protocol

Các giao thức tuyến intra-AS được dùng để cấu hình và duy trì các bảng định tuyến trong một hệ tự trị AS. Một khi có các bảng định tuyến này, các gói tin có thể tìm đường trong một hệ AS. Các giao thức này còn có tên gọi Interior Gateway Protocols (IGP).

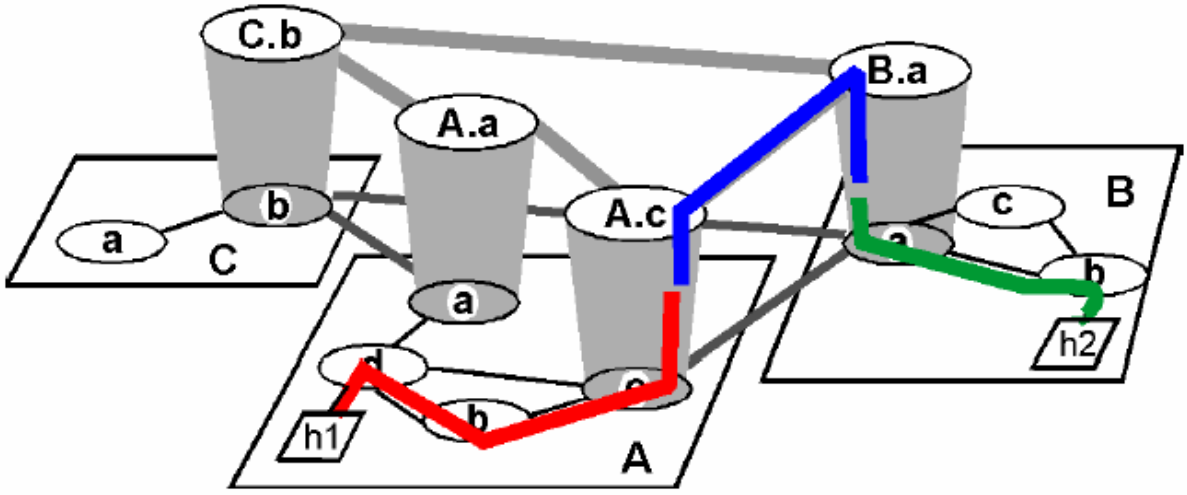
Một số giao thức định tuyến intra-AS:

- RIP: Routing Information Protocol
- OSPF: Open Shortest Path First
- IGRP: Interior Gateway Routing Protocol (của Cisco)

### 2. Inter-Autonomous System Routing protocol

Trong mỗi hệ tự trị, có các router đặc biệt gọi là **gateway router**.Các router này sử dụng intra-routing protocol với các router khác trong cùng AS và sử dụng inter-routing protocol với các gateway router của các AS khác. Một giao thức chuẩn phổ biến để định tuyến giữa các AS khác nhau là **Border Gateway Protocol-BGP**.

Mặc dù BGP trong các router có cách hoặc động tương tự theo kiểu giao thức giao thức định tuyến distance vector, nó có những đặc điểm như một giao thức vector chỉ đường (path vector protocol). Nguyên nhân là do BGP không thực hiệm việc quảng bá các thông tin về chi phí (như hop count,…) mà thực hiện quảng bá các thông tin về đường đi, ví dụ như tuần tự đường đi từ một AS này đến AS khác.

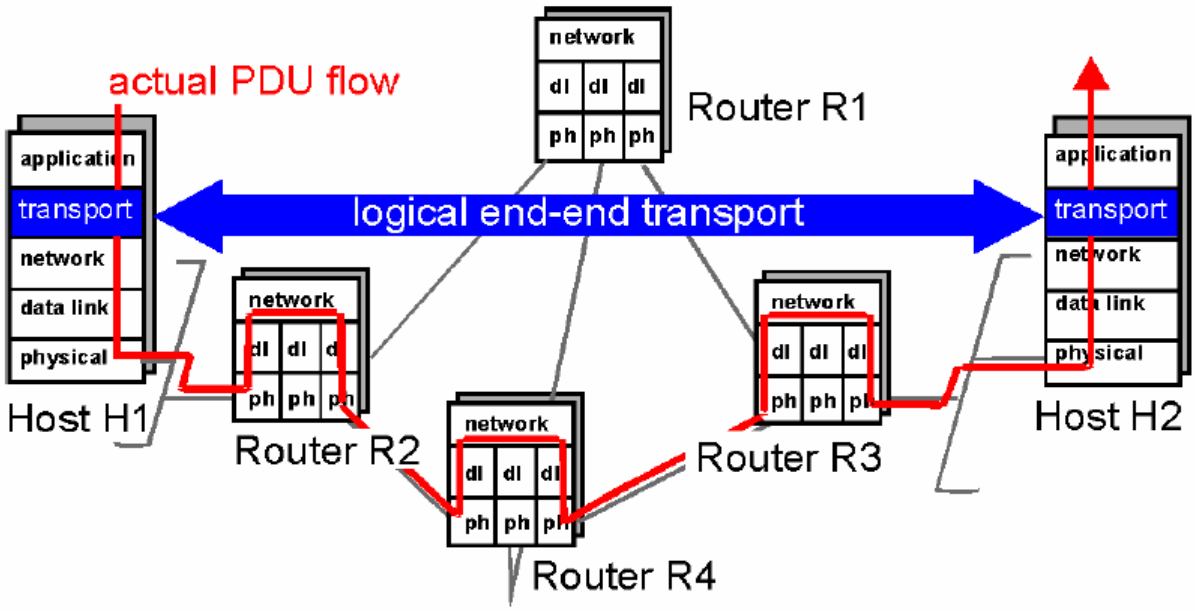



Hình IV-17. Định tuyến giữa các Autonomous System

# Chương V.Giao thức tầng giao vận

## V.1. Dịch vụ tầng vận chuyển

Tầng vận chuyển đóng vai trò quan trọng trong việc cung cấp các dịch vụ truyền thông trực tiếp đến các tiến trình ứng dụng tại các máy khác nhau. Các giao thức tầng ứng dụng cung cấp sự truyền thông logic (logical communication) giữa các tiến trình ứng dụng chạy ở các máy khác nhau. Truyền thông mức độ logic giữa các tiến trình ứng dụng có nghĩa là không kết nối về mặt vật lý (tại những vị trí khác nhau, kết nối thông qua nhiều router và các loại kết nối diện rộng khác,..). Các tiến trình sử dụng truyền thông logic được cung cấp bởi tầng vận chuyển để gửi thông điệp mà không cần quan tâm chi tiết đến hạ tầng vật lý bên dưới.




Hình V-1. Tầng vận chuyển cung cấp sự truyền thông logic

Các giao thức tầng vận chuyển được thực thi tại các trạm cuối (end system), không có tại các router. Tại phía gửi, tầng vận chuyển nhận thông điệp từ tầng ứng dụng, chia nhỏ và thêm vào các thông tin (header) của tầng mình và chuyển xuống tầng mạng bên dưới, nơi dữ liệu sẽ được đóng gói thành các gói tin. Tại nơi nhận, tầng vận chuyển nhận gói tin từ tầng mạng, loại bỏ các thông tin tầng vận chuyển (transport header), sắp xếp lại các thông điệp và chuyển cho các tiến trình ứng dụng bên trên.

Mô hình TCP/IP cung cấp hai giao thức tầng vận chuyển là UDP (User Datagram Protocol) và TCP (Transmission Control Protocol)

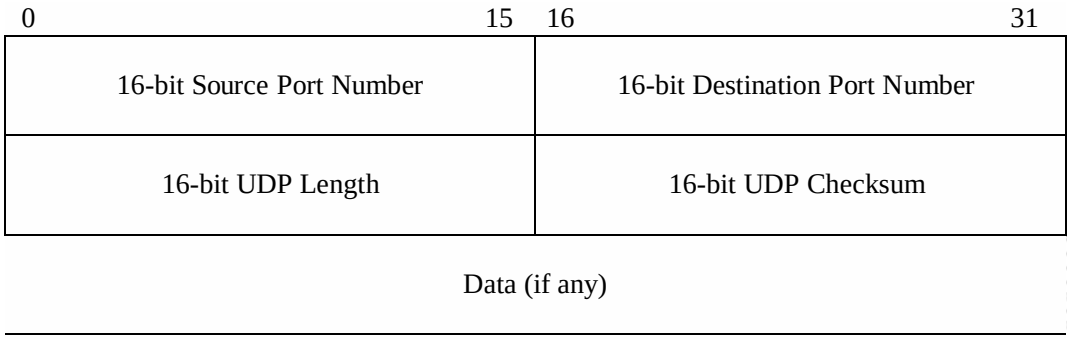
- UDP là giao thức không kết nối (connectionless) và không tin cậy (unreliable)
- TCP là giao thức hướng kết nối (connection-oriented) và tin cậy (reliable).

Khi thiết kế ứng dụng mạng, các nhà phát triển ứng dụng phải xác định rõ sử dụng UDP hay TCP.

## V.2. Giao thức không kết nối UDP

UDP-User Datagram Protocol cung cấp dịch vụ phi nối kết và không yêu cầu máy nhận thông báo rằng nó đã sẵn sàng cho việc nhận các thông điệp. Nó có thể mang dữ liệu ngay trong gói đầu tiên. Các ứng dụng sử dụng UDP thường quan tâm nhiều về tốc độ hơn là độ chính xác của dữ liệu.

**Port và Header**

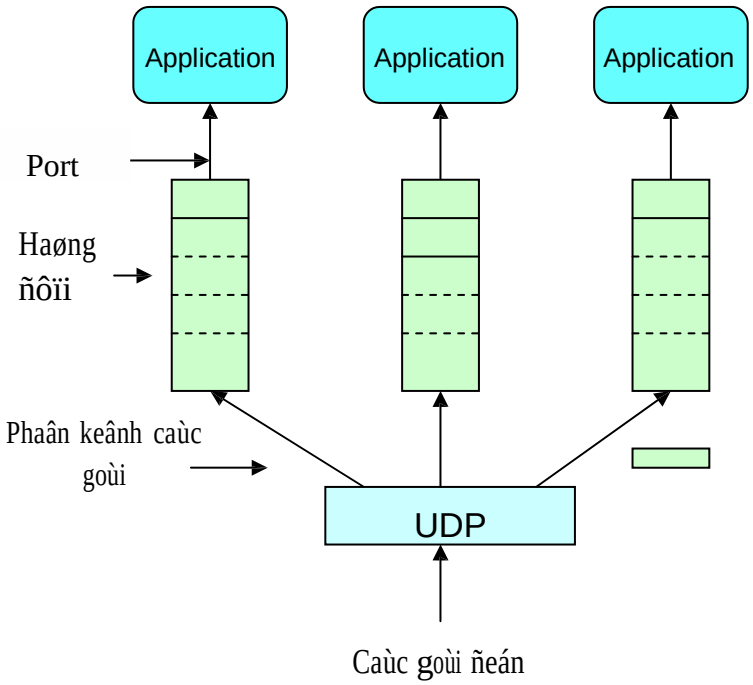



Hình V-2. Định dạng khung UDP

Một cách tiếp cận thông thường nhất(UDP) để trao đổi thông tin giữa các tiến trình ứng dụng là tiến trình xác định gián tiếp(không phải do OS gán) một ví trí ảo giữa hai tiến trình trên hai máy khác nhau để trao đổi thông tin, nó thường được gọi là port. Ý tưởng là máy gửi gửi thông tin qua một port và máy nhận nhận thông tin qua một port.

Để thực hiện chức năng phân kênh, mỗi header trong gói thông điệp của UDP chứa một định danh (port) của máy gửi và máy nhận. Trong hình minh hoạt định dạng khung UDP ở trên, mỗi port có giá trị 16 bit.

Vấn đề tiếp theo là như thế nào một tiến trình biết port mà nó muốn gửi 1 thông điệp. Một tiến trình client khởi tạo trao đổi thông tin với một tiến trình server, một khi liên lạc được với server, server có thể biết port của client và có thể đáp lại. Một số server nhận thông điệp ở một cổng cố định. Trong Internet, DNS(Domain Name Server)nhận thông điệp port 53 ở trên mỗi host.




Hình V-3. Hàng đợi thông điệp UDP

Minh họa trong hình trên, lúc một thông điệp được truyền đến, thông điệp được ở cuối hàng đợi. Nên khi hàng đợi đầy thông điệp sẽ bị loại bỏ. Không có kỹ thuật điều khiển luồn được sử dụng tại đây. Lúc một tiến trình ứng dụng muốn nhận một thông điệp nó lấy từ hàng đợi. Nếu hàng đợi rỗng tiến trình sẽ đợi cho đến khi thông điệp đến hàng đợi.

Mặc dù UDP không thực thi điều khiển luồn, đảm bảo phân phối, trật tự gói, nhưng nó cũng thực hiện kiểm tra lỗi khi truyền bằng cách sử dụng thuật toán checksum.

## V.3. Giao thức hướng kết nối TCP

Ngược lại với UDP, TCP-Transmission Control Protocol là một giao thức vận chuyển cung cấp dịch vụ tin cậy, connection-oriented, byte-stream.

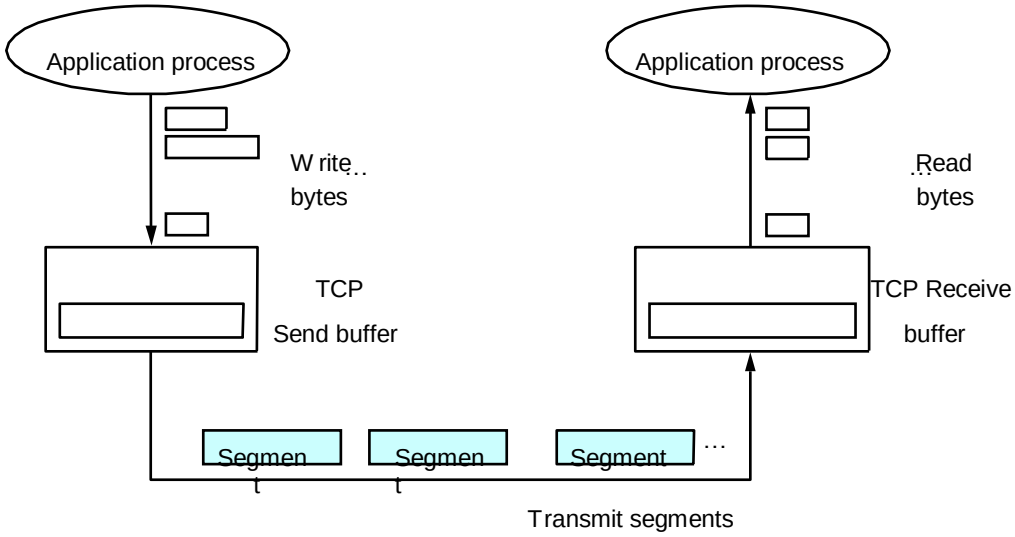
Dịch vụ này nâng cao hiệu quả của các ứng dụng bởi vì ứng dụng không cần lo lắng về lỗi hay thứ tự dữ liệu khi truyền. TCP có thể là một giao thức thỏa mãn tất cả những yêu cầu này.

- TCP là một giao thức full-duplex(có thể trao đổi thông tin hai chiều).
- TCP cũng gồm một kỹ thuật điều khiển luồn cho mỗi byte-stream mà nó cho phép máy nhận giới hạn dữ liệu máy gửi gửi trong một khoảng thời gian nào đó.

- TCP hỗ trợ kỹ thuật phân kênh mà nó cho phép nhiều chương trình ứng dụng trên bất kỳ máy có thể đồng thời trao đổi thông tin với các chương trình trên máy khác.
- TCP cũng thực hiện kỹ thuật điều khiển xung đột(không làm máy gửi quá tải máy nhận).

**1. Định dạng khung:**

TCP là một giao thức byte-oriented, điều này có nghĩa rằng máy gửi ghi các byte vào trong một nối kết TCP và máy nhận nhận được byte này từ nối kết TCP. Mặc dù "byte stream" được xem là dịch vụ TCP cung cấp cho các tiến trình ứng dụng. TCP không phải chính nó truyền các byte riêng biệt qua Internet, máy nguồn nhận các byte từ các tiến trình rồi tạo thành các gói có kích thước hợp lý, sau đó nó gửi các gói này đến đích. TCP của máy đích nhận các gói vào trong một buffer và tiến trình nới máy đích đọc các gói này lúc rảnh rỗi.



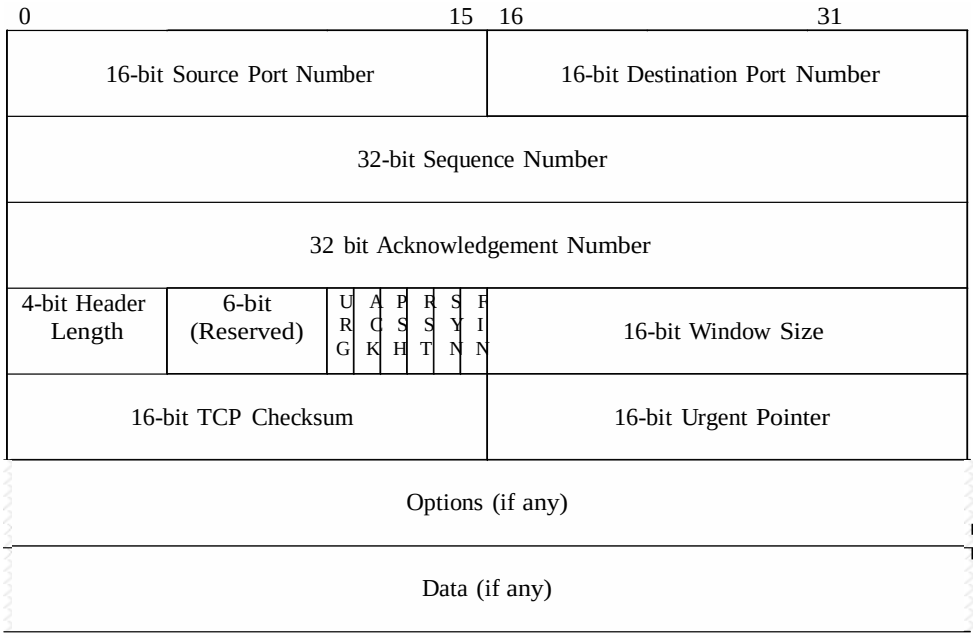

H

ình V-4. TCP quản lý một bit stream

Các gói được trao đổi giữa hai TCP được gọi là các đoạn, bởi vì mỗi đoạn mang một nhóm các byte. Câu hỏi đặt ra là như thế nào TCP quyết định đủ số byte để gửi vào trong một đoạn. TCP có 3 kỹ thuật để xây dựng truyền một đoạn:

- TCP chứa một biến maximum segment size(MSS) và nó gửi ngay một đoạn khi nó nhận đủ số byte từ các tiến trình.
- Các tiến trình yêu cầu thực hiện gửi.
- Sau một khoảng thời gian, nó sẽ gửi bất cứ đoạn đang có trong buffer.

Mỗi đoạn TCP chứa một header mô tả trong hình sau:



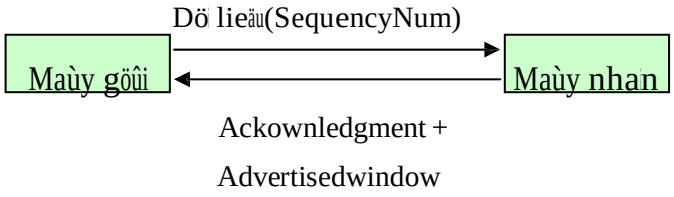

Hình V-5. Định dạng khung TCP

SrcPort và DstPort xác định port nguồn và port đích.

<SrcPort, SrcIPAddr, DstPort, DstIPAddr> xác định duy nhất cho một nối kết TCP.

Bởi vì TCP là một nối kết đến và đi, nó cho phép một nối kết giữa hai port được thiết lập, sử dụng để gửi và nhận dữ liệu và sau đó đóng lại và rồi một khoảng thời gian nào đó hai port như vậy khẩn cầu một nối kết thứ hai.

SequenceNum, Acknownledgment, AdvertiseWindow được sử dụng trong thuật toán cửa sổ trượt. Bởi vì TCP là một giao thức byte-oriented nên mỗi byte dữ liệu có một số thứ tự. Trường SequenceNum chứa số thứ tự của byte dữ liệu đầu tiên mang đoạn. Acknownledgment, AdvertiseWindow mang thông tin về dòng dữ liệu đi theo các hướng khác nhau.




Hình V-6. Minh họa đơn giản một tiến trình TCP

6 bit Flag thường được sử dụng để sắp đặt thông tin tin điều khiển giữa hai TCP. Nó bao gồm SYN, FIN, RESET, PUSH, URG, ACK.

- SYN và FIN dùng để thiết lập và kết thúc một nối kết.

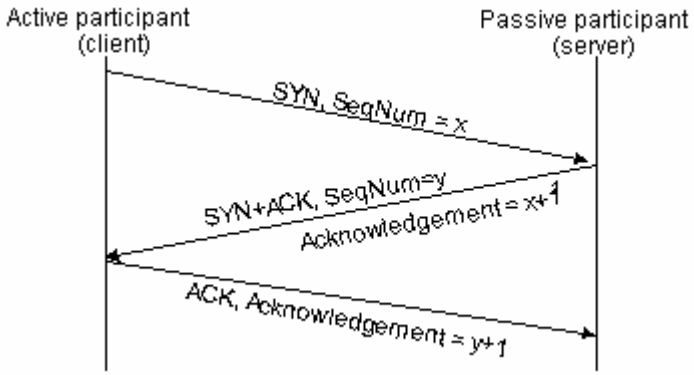
- ACK thiết lập để chỉ sự hồi báo.
- URG để chỉ đoạn chứa dữ liệu khẩn cấp.
- PUSH thiết bị gửi mong muốn một hoạt động push, nó muốn TCP máy nhận thông báo đến các tiến trình sự kiện này.
- RESET thiết bị nhận bị nhầm lẫn, ví dụ nó nhận một đoạn không mong đợi.
- CheckSum dùng để kiểm tra lỗi.

**2. Quá trình thiết lập và kết thúc kết nối:**

Một nối kết bắt đầu với một client thực hiện một hoạt động mở đến server. Cho rằng server chủ động mở nối kết trước, hai phía hứa hẹn với một thông điệp trao đổi để thiết lập nối kết. Chỉ sau khi giai đoạn thiết lập nối kết, hai phía mới bắt đầu gởi dữ liệu. Ngược lại, một khi không muốn trao đổi, nó đóng nối kết. Mỗi phía tự động đóng nối kết của mình.

**Thuật toán 3 cách bắt tay**

Thuật toán này bao gồm gửi 3 thông điệp giữa client và server. Minh họa trong hình sau:

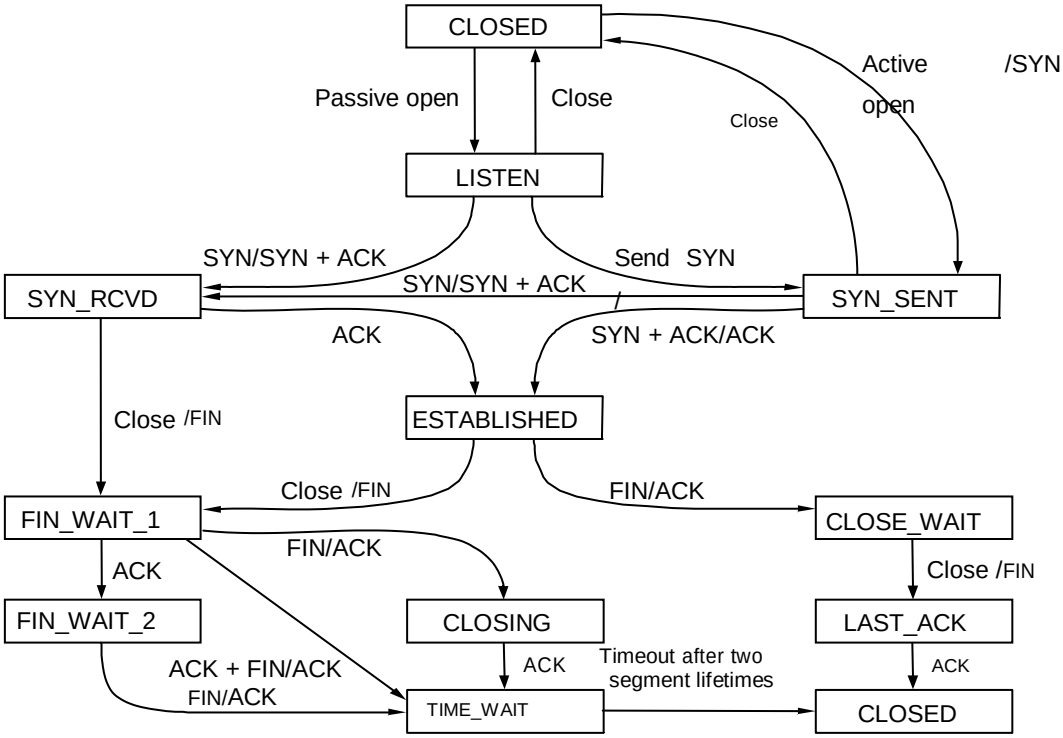



Hình V-7.Thuật toán ba cái bắt tay.

**Ý tưởng:**

Hai phía đồng ý nối kết trên một tập các thông số(tất cả các thông tin mà chúng muốn biết về nhau). Trong trường hợp mở nối kết, đầu tiên client gửi một thông điệp đến server với (flag = SYN, SequenceNum = x). Server đáp lại với một đoạn chứahồi báo(flag = ACK, ACK = x + 1) và trạng thái bắt đầu (flag = SYN, SequenceNum = y), Kết thúc client hồi báo với thông điệp (flag = ACK, ACK = y+1).

Lược đồ trạng thái chuyển tiếp:




Hình V-8. Hình lược đồ trạng thái chuyển tiếp.

Lược đồ này chỉ ra trạng thái yêu cầu để mở một nối kết và đóng một nối kết.

Có hai loại sự kiện gây ra trạng thái chuyển tiếp:

- Một đoạn đến từ TCP ngang hàng.
- Tiến trình ứng dụng cục bộ yêu cầu một hoạt động trên TCP.

Chú ý: Nếu một ACK từ client đến server bị mất(tương ứng với bước thứ ba của 3 cách bắt tay), nối kết vẫn thực hiện đúng. Bởi vì phía client đã thật sự ở trạng thái ESTABLISHED, vì vậy các tiến trình ứng dụng cục bộ có thể bắt đầu gởi dữ liệu. Mỗi đoạn dữ liệu này đặt cờ ACK, vì vậy server sẽ chuyển đến trạng thái ESTABLISHED lúc gói đầu tiên được nhận.

Tiến trình ứng dụng trên cả hai phía của nối kết phải tự đóng nữa nối kết. Nếu chỉ một phía đóng nối kết (có nghĩa là nó không còn dữ liệu để gửi) nhưng nó vẫn còn nhận dữ liệu từ phía kia.

Có ba khả năng xảy ra khi một phía đóng kết nối:

- Nó đóng trước phía kia:

  ESTABLISHED -> FIN_WAIT_1 -> FIN_WAIT_2 -> TIME_WAIT -> CLOSED

- Nó đóng sau phía kia:

ESTABLISHED ->CLOSE_WAIT -> LAST_ACK -> CLOSED.

- Hai phía cùng đóng

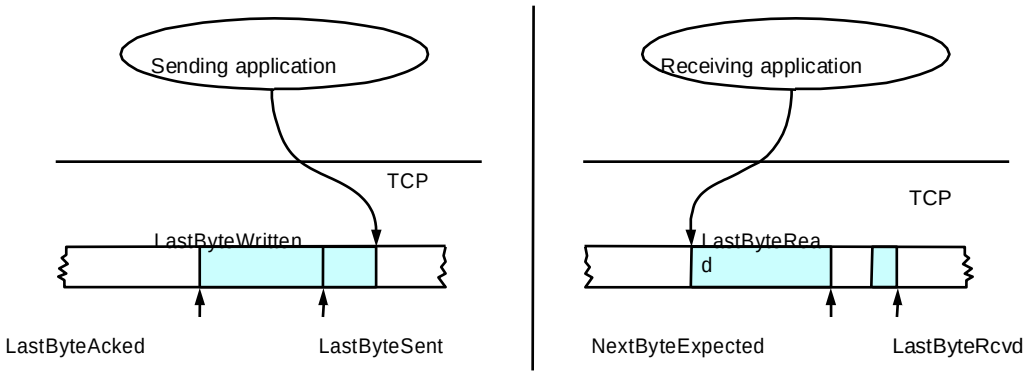
ESTABLISHED -> FIN_WAIT_1 -> CLOSING -> TIME_WAIT -> CLOSED.

**3. Điều khiển dòng truyền (Cửa sổ trượt):**

Mục đích của cửa sổ trượt:

- Đảm bảo phân phối dữ liệu tin cậy.
- Dữ liệu phân phối theo đúng trật tự
- Sử dụng điều khiển dòng giữa máy gửi và máy nhận.

Để có được kích thước cửa sổ thanh trượt cố định, máy nhận quảng cáo kích thước cửa sổ đến máy gửi. Nó được thực hiện bởi sử dụng trường AdvertiseWindow trong header TCP.




Hình V-9. Quan hệ giữa buffer gửi và buffer nhận.

**a) Phân phối tin cậy và thứ tự**

TCP bên phía gửi duy trì một buffer gửi. Buffer này được sử dụng lưu các dữ liệu đã gửi nhưng chưa có hồi báo, cũng như các dữ liệu được ghi bởi các ứng dụng nhưng chưa truyền. Bên phía nhận TCP duy trì một buffer nhận, buffer này lưu trữ dữ liệu đến thứ tự hay không thứ tự  mà các tiến trình ứng dụng chưa có cơ hội để đọc.

**b) Điều khiển luồng**

Trong giao thức cửa sổ trượt, kích thước của cửa sổ thiết lập dung lượng dữ liệu mà chúng có thể gửi mà không cần đợi hồi báo từ máy nhận. Thật vậy máy nhận có thể bóp nghẹt máy nhận bởi nó quảng cáo một cửa sổ mà nó lớn hơn dung lượng dữ liệu lưu trữ của buffer. Do đó kích thước cửa sổ trên máy nhận phải thỏa:

**LastByteRcvd - LastByteRead <= MaxRcvBuffer**

Để tránh quá tải trong buffer, nó phải quảng cáo kích thước cửa sổ:

**AdvertiseWindow = MaxRcvBuffer -( LastByteRcvd - LastByteRead)**

Nó thể hiện số không gian còn trống còn lại trong buffer.

TCP trên máy gửi lấy thông tin quảng cáo từ máy nhận. Nó phải đảm bảo rằng:

**LastByteSent - LastByteAcked <= AdvertisedWindow**

Máy gửi tính kích thước cửa sổ giới hạn dữ liệu gửi, phải đảm bảo:

**EffectiveWindow = AdvertisedWindow - (LastByteSent - LastByteAcked)**

Rõ ràng, EffectiveWindow phải lớn hơn không trước khi nguồn có thể gửi dữ liệu. Có khả năng, một đoạn đến hồi báo x byte, do đó cho phép máy gửi gia tăng LastByteAcked thêm x, nhưng bởi vì tiến trình tại các máy nhận không đọc bất kỳ dữ liệu, cửa sổ quảng cáo bây giờ giảm x byte so với thời gian trước. Trong trường hợp này, máy gửi có thể giải phóng buffer nhưng không tiếp tục gửi dữ liệu.

Máy gửi cũng đảm bảo rằng các tiến trình ứng dụng cục bộ không quá tải buffer gửi bằng cách giới hạn:

**LastByteWriten - LastByteAcked <= MaxSendBuffer.**

Nếu tiến trình gửi cố gắng viết y byte đến TCP nhưng

**LastByteWriten - LastByteAcked + y > MaxSendBuffer**

TCP sẽ khoá tiến trình gửi và không cho phép tạo ra dữ liệu.

## V.4. So sánh TCP và UDP

TCP là giao thức có liên kết, quản lý trạng thái liên kết và tin cậy. Tuy nhiên tốc độ truyền của TCP chậm hơn UDP vì phải có thời gian thiết lập, quản lý liên kết. Tùy vào yêu cầu cụ thể của ứng dụng mà sử dụng TCP hay UDP.

Một số các ứng dụng thực tế:

| **Ứng dụng** | **Giao thức ứng dụng** | **Giao thức vận chuyển** |
|---|---|---|
| Thư điện tử | SMTP | TCP |
| Truy cập từ xa | Telnet | TCP |
| Web | HTTP | TCP |
| Truyền File | FTP | TCP |
| Phân giải tên | DNS | thông thường là UDP |
| Giao thức định tuyến | RIP | thông thường là UDP |

# Chương VI. Giao thức tầng ứng dụng

## VI.1. Chức năng:

Chương trình ứng dụng (Applicationa) chạy trên các máy tính, trao đổi thông điệp (message) với các ứng dụng khác nhằm thực thi vai trò của ứng dụng. Khác với ứng dụng, **giao thức tầng ứng dụng (application-layer protocols)** là một thành phần của chương trình ứng dụng mạng, dùng để định nghĩa các quy tắc trao đổi thông điệp và giao tiếp với các dịch vụ được cung cấp bởi tầng dưới (chẳng hạn TCP hay UDP). Ví dụ như Web là một ứng dụng mạng cho phép người dùng lấy những "tài liệu" từ Web server theo yêu cầu. Ứng dụng Web gồm nhiều thành phần, bao gồm các chuẩn định dạng tài liệu (HTML,..), trình duyệt Web (Internet Explorer, Firefox,..), Web server (IIS, Apache,..) và một giao thức ứng dụng. Giao thức ứng dụng của web là HTTP (Hyper Text Transfer Protocol), định nghĩa thông điệp được truyền giữa Web server và trình duyệt như thế nào. Vì vậy HTTP chỉ là một thành phần của ứng dụng Web.

Giao thức tầng ứng dụng định nghĩa làm cách thức các tiến trình của ứng dụng trao đổi thông điệp với nhau.Cụ thể giao thức tầng ứng dụng định nghĩa:

- Các loại thông điệp cần trao đổi khác nhau, ví dụ như thông điệp yêu cầu (request message), thông điệp phản hồi (response message),…
- Cú pháp của các loại thông điệp, chẳng hạn các trường của thông điệp.
- Ý nghĩa của các trường.
- Các nguyên tắc quyến định lúc và cách thức gửi thông điệp yêu cầu hay phản hồi.

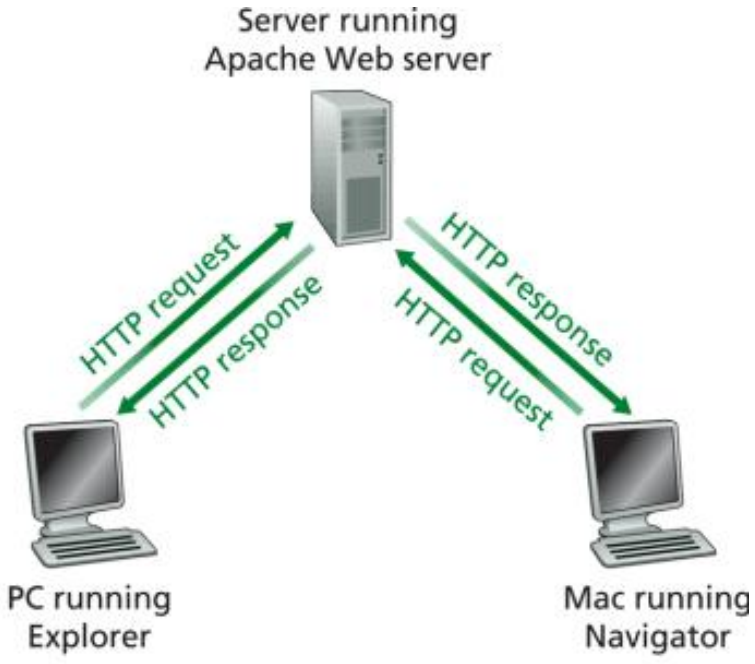
Các giao thức ứng dụng thường được đặc tả trong RFC và phổ biến rộng rãi. Tuy nhiên cũng có một số giao thức có bản quyền.

## VI.2. World Wide Web - HTTP

Hyper Text Transfer Protocol-Giao thức truyền siêu văn bản, sử dụng cho các dịch vụ truyền thông đa phương tiện WWW, dựa trên mô hình Client/Server. Dịch vụ WWW cho phép người sử dụng kết hợp văn bản, âm thanh, hình ảnh, hoạt hình tạo nên nguồn thông tin tư liệu. Đặc biệt ở đây là thông tin tư liệu trong WWW có dạng chủ yếu là HyperText-là dạng tư liệu chuẩn trong WWW. Về cơ bản đây là các file HTML-Hyper Text Markup Language.HTML sử dụng các thẻ (tag) để mô tả đối tượng chứa trong nó.Giao thức HTTP cho phép lấy và đọc nhanh các tài liệu này.

HTTP là giao thức truyền thông nhưng có thêm ưu điểm là thông tin tư liệu cần truy cập lại có chứa các liên kết với các đối tượng khác nằm khắp nơi trên mạng Internet. Phần mền cho Web server là chương trình điều khiển cho sự thu thập các tư liệu WWW trên một máy chủ. Để truy cập WWW cần phải có một trình duyệt (browser) chạy trên WWW client.

HTTP là giao thức Client/Server, được thiết kế để truyền các dạng dữ liệu siêu văn bản.Client yêu cầu truy cập web thông qua URL (URL request) và Server Gửi các đối tượng tới client thông quan phản hồi (response). HTTP là một giao thức không trạng thái, nghĩa là khi Server đáp ứng được yêu cầu dữ liệu của Client xong thì Server hủy bỏ kết nối đó để không tốn bộ nhớ cho sự kiện. Không trạng thái là yếu tố làm cho tốt độ truyền dẫn giữa Client và Server rất nhanh.

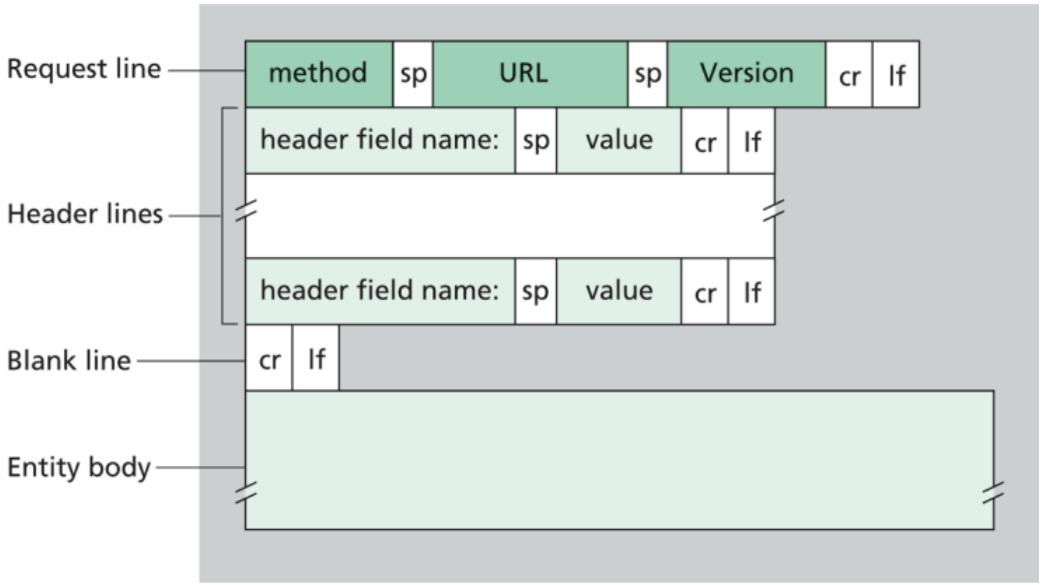



Hình VI-1. Mô hình hoạt động giao thức HTTP

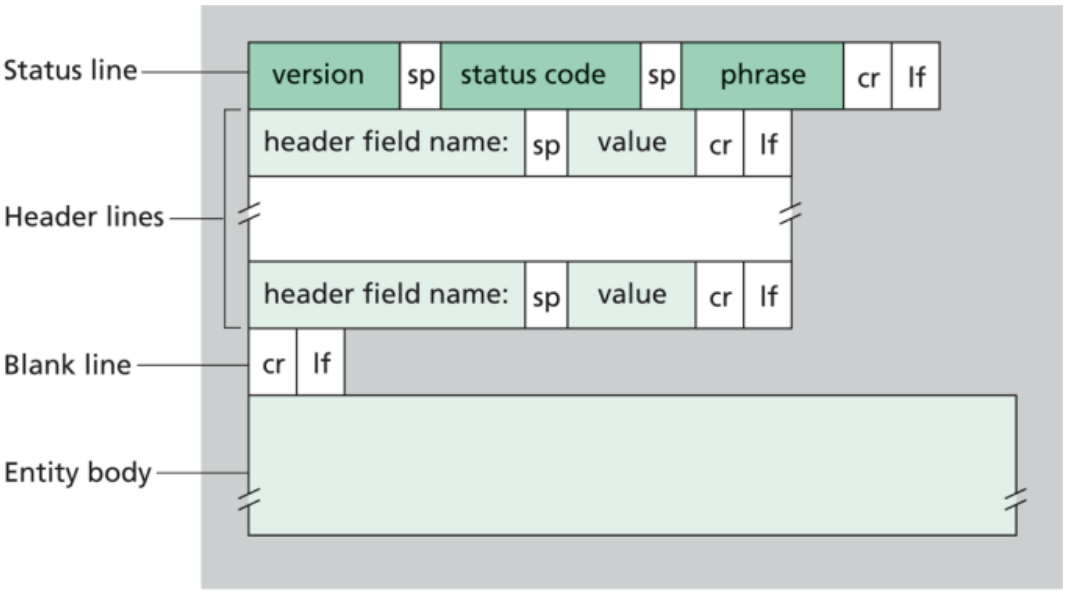
Các giai đoạn kết nối của HTTP:

- Mở kết nối: Client (browser) thiết lập liên kết tới web server (TCP connection) qua cổng 80 (mặc định). Server đồng ý kết nối (accept).
- Tạo yêu cầu: Client gửi thông điệp tới Server yêu cầu dịch vụ. Yêu cầu bao gồm các tiêu đề của HTTP, nó định nghĩa các phương thức được yêu cầu cho tác vụ và cung cấp thông tin về khả năng của Client (được theo sau dữ liệu gửi tới Server). Các phương thức HTTP điển hình là GET để nhận các đối tượng từ Server và POST để truyền dữ liệu cho đối tượng trên Server.

- Gửi đáp ứng: Server trả lời cho Client bao gồm các tiêu đề để trả lời mô tả trạng thái của các tác vụ (ví dụ thành công hay không thành công,..) theo sau dữ liệu thật sự.
- Ngắt kết nối.




Hình VI-2. Thông điệp HTTP Request




Hình VI-3. Thông điệp HTTP Response

Có hai kết nối HTTP:

- **Non-persistent HTTP**: Nhiều nhất là một đối tượng được truyền qua liên kết TCP (HTTP 1.0).

- **Persistent HTTP**: Cho phép nhiều đối tượng được truyền trên cùng một liên kết. Client phân tích, tìm ra và gửi yêu cầu tới tất cả các đối tượng ngay sau khi nhận được trang HTML ban đầu (base HTML).HTTP 1.1 sử dụng liên kết loại này ở chế độ mặc định.

## VI.3. Giao thức truyền File-FTP

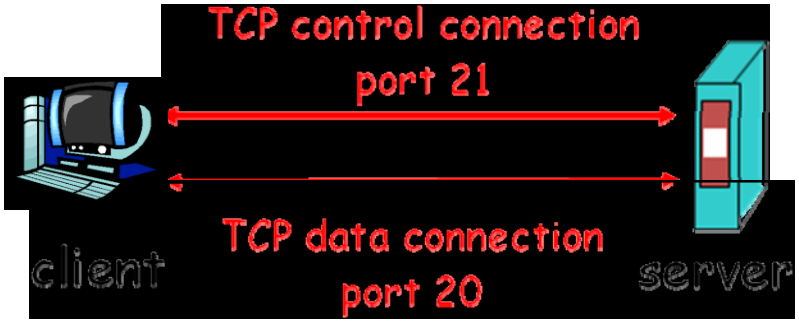
File Transfer Protocol-Giao thức truyền tập tin cho phép truyền tập tin giữa hai máy tính, quản lý các thư mục. FTP không được thiết kế để truy cập vào máy khác và chạy các chương trình ở máy đó. FTP giúp người sử dụng truy cập file và thư mục trên một máy chủ ở xa và thực hiện thao tác trên các thư mục như sau:

- Liệt kệ các file trên một thư mục cục bộ hay ở xa.
- Đổi tên và xóa tập tin (nếu có quyền).
- Tải các file về máy trạm hay truyền file đến máy ở xa (download/ upload).

FTP sử dụng đồng thời 2 liên kết TCP tại 2 cổng:

- TCP control connection, port 21: trao đổi các thông điệp điều khiển (commands, responses…).
- TCP data connection, port 20: truyền tải tệp.

Ngoài ra FTP lưu giữ trạng thái client trong phiên làm việc.




Hình VI-4. Mô hình hoạt động của FTP.

Quá trình trao đổi truyền tải:

- FTP server nghe tại cổng 21.
- FTP client yêu cầu kết nối với FTP server qua TCP tại cổng 21. Gửi user & password để đăng nhập.
- FTP server chấp nhận, liên kết điều khiển (control connection) được thiết lập. Quá trình trao đổi có thể bắt đầu.

- Khi server nhận được lệnh truyền tệp, nó mở liên kết dữ liệu (data connection) tới client, tệp được truyền qua liên kết này.
- Sau khi truyền xong một tệp, server ngắt liên kết dữ liệu (mỗi liên kết chỉ sử dụng để truyền một tệp).

## VI.4. Giao thức SMTP

Electronic Mail (viết tắt là e-Mail, thư điện tử) là một trong những dịch vụ thông tin phổ biến nhất trên Internet. Dịch vụ e-Mail giúp mọi người có thể trao đổi thông tin với nhau trên mạng Internet. Liên lạc bằng thư điện tử nhanh hơn, thuận tiện hơn và chi phí thấp hơn rất nhiều so với trao đổi thư từ qua đường bưu điện bình thường. Ngoài ra còn cho phép họ gởi cho nhau cả các loại tài liệu như : các văn bản, các báo cáo, các chương trình máy tính,… và nhiều thông tin khác.

Mỗi người sử dụng đều có một thư mục lưu trữ như trên máy server gọi là Mailbox. Tất cả các địa chỉ mail bao gồm hai phần được ngăn cách nhau bằng ký tự @ (ampersand). Tên miền có thể chia nhiều phần cách nhau bởi dấu chấm (.). Một địa chỉ Mail tiêu biểu có các phần như sau:

*Uername@ServerName.Type of Organization.Country*

Cấu trúc của một e-mail bao gồm các phần như sau:

- **Phần tiêu đề thư**

Phần này do các MTA (Messagn Transfer Agent) tạo ra và sử dụng, nó chứa các thông tin để chuyển nhận e-mail như địa chỉ của nơi nhận, địa chỉ của nơi gởi. Các hệ thống e-Mail cần những thông tin này để chuyển dữ liệu từ máy tính này sang máy tính khác. Cấu tạo phần này gồm nhiều trường (field), mỗi trường là một dòng văn bản ASCII chuẩn 7 bit như sau :<tên trường>:<nội dung của trường>.

Sau đây là một số trường thông tin thông dụng:

| Trường chức năng | Chức năng |
|---|---|
| DATE | Chỉ ngày giờ nhận mail |
| PROM | Chỉ địa chỉ người gởi |
| TO | Chỉ địa chỉ người nhận |
| CC | Chỉ địa chỉ những người nhận bản copy mail. Các người nhận thấy được địa chỉ của những người cùng nhận trong nhóm |
| BCC | Chỉ địa chỉ những người nhận bản sao chép của bức mail, nhưng từng người không biết những người nào sẽ nhận bức thư này. |

| | |
|---|---|
| REPLY-TO | Chứa cá thông tin để người nhận có thể nhận lại, thường nó chính là địa chỉ người gởi. |
| MESSAGE-ID | Định danh duy nhất, được sử dụng bởi hệ điều hành |
| SUBJECT | Chủ đề của nội dung thư |

Các trường trên là các trường chuẩn do giao thức SMTP quy định, ngoài ra trong phần header cũng có thể có thêm một số trường khác do chương trình e-Mail tạo ra nhằm quản lý các e-Mail riêng. Các trường này được bắt đầu ký tự X- và thông tin theo sau là cũng giống như ta thấy trên một trường chuẩn.

- **Phần nội dung**

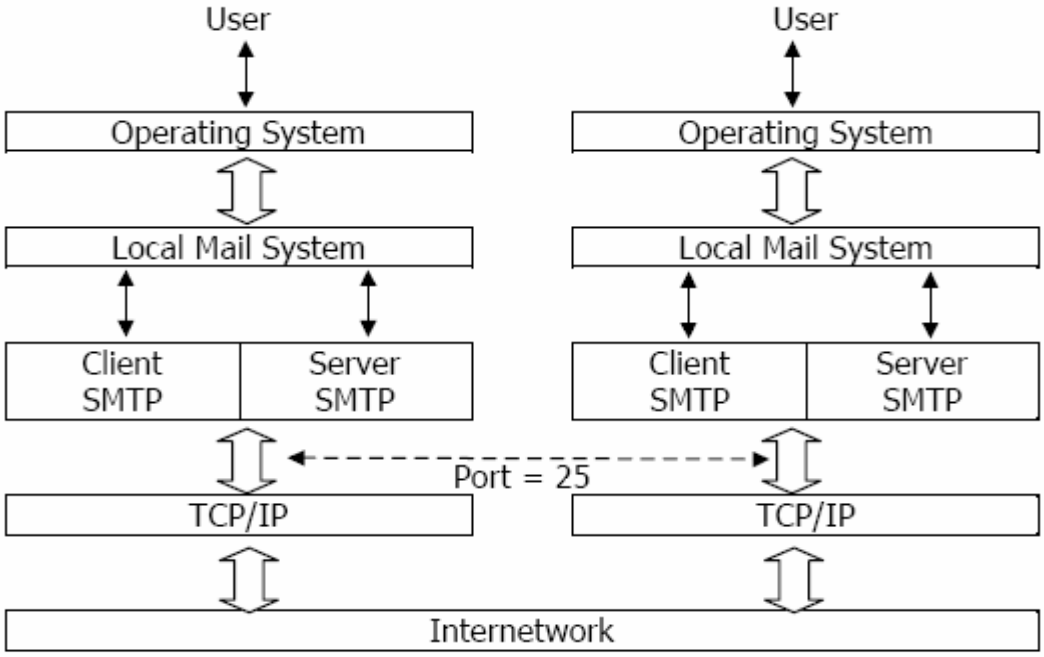
Để phân biệt phần tiêu đề và phần nội dung của e-mail, người ta quy ước ranh giới là một dòng trắng (chuỗi ký tự '\r\n'). kết thúc của dòng nội dung là chuỗi ký tự "\r\n.\r\n" .

Như vậy nội dung bức thư nằm trong khoảng giữa dòng trắng đầu tiên và ký tự kết thúc thư, và trong phần nội dung của bức thư không được phép tồn tại chuỗi ký tự kết thúc thư. Mặt khác do môi trường truyền thông là mạng Internet nên cá ký tự cấu thành phần thân của bức thư phải là các ký tự ASCII chuẩn.

### VI.4.1. Giao thức SMTP

SMTP (Simple Mail Transfer Protocol) là giao thức quy định về việc truyền mail chủ yếu dùng trong mạng Internet.

Mối quan hệ giữa SMTP và hệ thống Mail cục bộ như sau:




Hình VI-5. Quan hệ giữa SMTP và hệ thống Mail cục bộ.

Client liên quan đến thư đi, Server liên quan đến nhận thư. Hệ thống thư cục bộ hộp thư (mailbox) cho mỗi user. Mailbox có 2 phần: phần cục bộ và phần toàn cục.

Sau khi tháo bức thư trong khuôn dạng chuẩn, hệ thống mail cục bộ xác định tên người nhận ở hộp thư cục bộ hay phải gởi ra ngoài, để gởi bức thư Client SMTP phải biết địa chỉ IP của nơi nhận qua DNS và gởi qua cổng địa chỉ SMTP (25) để bắt đầu nối kết server SMTP nơi nhận. Khi mối nối đã được thiết lập, client bắt đầu chuyển thư đến Server bởi các lệnh của SMTP. SMTP dùng từ khóa như các lệnh để thực hiện thao tác chuyển giao mail. Một số lệnh chính của SMTP trong phiên việc giữa Client MTA và Server MTA như sau:

| **Lệnh** | **Tác dụng** |
|---|---|
| HELLO | Xưng danh với SMTP bên nhận, báo cho bện nhận biết bên gởi là ai. SMTP bên gởi gởi lệnh này đầu tiên cho SMTP bên nhận |
| MAIL | Khởi động một cuộc giao dịch mail mà mục đích cuối cùng là chuyển giao các mail tới một hay nhiều mailbox (nơi chứa mai nhận được) khác nhau. |
| RCPT | Nói rõ người nhận là ai |
| DATA | Các dòng lệnh DATA là dữ liệu của Mail. Đối với SMTP, chuỗi ký tự "CRLF.CRLF" báo nhận biết kết thúc nội dung bức mail. |
| RSET | Bỏ (Reset) cuộc giao dịch hiện tại. |
| NOOP | Yêu cấu SMTP bên nhận không làm gì ngoài việc trả về câu trả lời OK (dùng để kiểm tra). |
| QUIT | Yêu cầu SMTP nhận trả lời Ok và kết thúc phiên giao dịch hiện tại,=. |
| VRFY | Yêu cầu SMTP bên nhận kiểm tra người nhận là đúng, xác nhận các tham số gởi theo dòng kênh |
| SEND | Khởi động một cuộc giao dịch mà mail sẽ được gởi tới một hay nhiều thiết bị đầu cuối chứ không phải mailbox. |
| SOML | Khởi động một cuộc giao dịch mà mail sẽ được gởi tới một hay nhiều thiết bị đầu cuối hay mailbox. |
| SAML | Khởi động một cuộc giao dịch mà mail sẽ được gởi tới một hay nhiều thiết bị đầu cuối và mailbox |
| HELP | Yêu cầu SMTP bên nhận gởi thông tin giúp đỡ cho SMTP bên phát. |

| | |
|---|---|
| EXPN | Yêu cầu SMTP bên nhận gởi về danh sách những người nhận mail để có thể mở rộng việc chuyển mail cho các user khác. |
| TURN | Yêu cầu SMTP bên nhận gởi OK và đổi vai trò trở thành SMTP gởi. |

SMTP (trong RFC 821) ban đầu được thiết kế để cho phép các mail server chuyển đổi các mail message. Cơ chế chính được dùng để chuyển đổi các mail là phân đường các message quanh Internet. SMTP hoạt động trên mô hình lưu và truyền trong đó Client nắm các message cần để truyền đến server và gởi các lệnh đến server để báo cho server cách sử lý các message. Mail Client có thể là một mail server khác, nó có một hay nhiều các message phải truyền đến một server khác. Hầu hết các Internet Mail Client sử dụng SMTP để gởi message.

### *1. Quy tắc làm việc với SMTP*

1. Mỗi lệnh câu phân cách tham số theo sau bằng khoảng trắng và kết thúc bằng ký tựu CRLF. Mail đi từ SMTP gởi đến SMTP nhận và đến lượt SMTP nhận trở thành SMTP gởi để gởi mai đi tiếp cho đến khi chúng được giao vào Mailbox của người nhận.
2. Các lệnh SMTP phải diễn ra một cách tuần tự.
3. Việc đánh địa chỉ phải theo cách đánh địa chỉ của Internet

Giao thức SMTP quy định các Server MTA (ở đây SMTP bên phải) phải gởi tín hiệu phản hồi ACK sau mỗi lệnh mà nó nhận được từ Client MTA. Mỗi câu trả lời bên nhận đều mở đầu với một mã số theo sau mới là thông tin dạng text. Mỗi số mở đầu trong mã số có ý nghĩa khác nhau, nó chỉ ra rằng kết quả thực hiện thao tác là tốt (số 2) , thất bại (số 5), hay chưa hoàn thành (số 3).

### *2. Một số mã phản hồi thông dụng của SMTP*

220 Dịch vụ đã sẵn sàng

221 Đóng kết nối đã được sẵn sàng

250 Thao tác do Client MTA yêu cầu đã được hoàn thành.

234 Sẵn sàng nhận nội dung của mail

555 Thao tác yêu cầu không thực hiện được do không có Mailbox trên máy….

### *3. Phiên giao dịch SMTP*

Để hiểu cách dùng một số lệnh chúng ta xem xét qua ví dụ sau: bên gởi tên aa ở máy Samplel muốn gởi cho bb, cc ở máy Sample2, giả sử cc không có Mailbox tại Simple 2.

Bên gởi thực hiện một kết nối SMTP Server.

RECEIVER: 220 sample2 Simple mail Transfer Server ready

Khi được kết nối qua giao thức TCP/IP, máy nhận trả lời với mã 220 để báo cho máy gởi biết dịch vụ SMTP đã sẵn sàng.

SENDER: HELO sample1

Bên nhận đã sẵn sàng, bên gởi gởi HELLO và xưng tân người gởi.

RECEIVER: 250 sample2

trả với mã 250 báo cho biết bên nhận đã sẵn sàng.

SENDER: MAIL FROM:<>

Bên gởi dung lệnh MAIL để khởi động phiên giao dịch. Cú pháp trên cho bên nhận biết địa chỉ bên gởi (mailbox của bên gởi) để bên nhận thông báo lỗi nếu có về bên gởi.

RECEIVER: 250 OK

Trả lời với mã 250 cho biết đã chấp nhận.

SENDER: RCPT TO:<>

Bên gởi cho biết e-Mail đích.

RECEIVER: 250 OK

Trả lời với mã 250 cho biết đã chấp nhận.

SENDER: RCPT TO:<>

Muốn gởi bao nhiêu người dùng bấy nhiêu lệnh RCPT kèm theo địa chỉ nhận, nếu đúng sẽ trả lời về về mã 250 kèm theo OK

RECEIVER: 550 No such user here

Báo kèm theo mã 550 cho biết không có mailbox trên địa chỉ trên đối với người nhận.

SENDER: DATA

Báo cho bên nhận biết dữ liệu bắt đầu từ sau từ DATA.

RECEIVER: 354 Start mail input;end with <CRLF>,<CRLF>

Mã 354 báo cho biết đã sẵn sàng nhận mail, kết thúc mail với ký tự “CRLF,CRLF”

SENDER: bắt đầu thân của mail

SENDER: …

SENDER: (đến khi kết thúc gởi CRLF,CRLF)

RECEIVER: 250 OK

E-mail đã được chấp nhận.

SENDER: QUIT

Phát lệnh báo kết thúc phiên giao dịch

RECEIVER: 221 sample2 Server closing transmission chênnl

Mã 221 đóng kết nối đã thiết lập.

### *4. Giao thức mở rộng ESMTP*

SMTP có một hạn chế gây khó khăn trong việc truyền nhận mail là giới hạn tối đa kích thước nội dung một bức mail chỉ là 128KB. Do đó người ta đã cải tiến chuẩn SMTP thành một chuẩn mở rộng mới gọi là ESMTP, cho phép tăng giới hạn kích thước của mail lên 1MB.

Để xem xét Server MTA có theo chuẩn ESMTP hay không, thay vì dùng lệnh HELO ở đầu một cuộc giao dịch, Client MTA dùng lệnh mới EHLO, nếu Server thay thế chuẩn SMTP ở đa số các hệ thống

Chẳng hạnh để khởi động cuộc giao dịch với kích thước mail lên tới 1MB, sử dụng dòng lệnh sau:

MAIL FROM:<aa@sample1>SIZE=1000000

### VI.4.2. MIME

Từ khi MIME (Multipurpose Internet Mail Extention) được đưa ra, kiểu dữ liệu mà người dùng có thể gởi thông qua e-Mail được mở rộng. Ban đầu dữ liệu chỉ ở dạng text. Ngày nay, ta có thể gởi các tài liệu (file *.doc), cá file ảnh hay file âm thanh.

Để có thể phân phát các kiểu dữ liệu này, khuôn dạng các message trên Internet nên được mở rộng . MIME được phát triển cho mục đích này.

#### 1. *Cấu trúc message của MIME*

MIME không phải cho các ứng dung e-Mail mới, nhưng cho phép mở rộng khả năng e-Mail trên Internet trong khi vẫn dữ các ứng dụng giao vận và nền tảng hiện tại. Khuôn dạng MIME duy trì các cấu trúc message cơ bản với các phần Header và phần body (tham khảo RFC 822). Ví dụ về khuôn dạng của một tài liệu MIME như sau:

{Dòng này xác định MIME message}

MINE-Version:1.0

To:

Subject:Book CD

{Dòng này xác định đây là kiểu message hỗn hợp và các phần được phân tách nhau bởi đầu biên}

Content-Type: multipart/mixed;boundary=”---------6B9767D111AE”

X-Mozilla-Status: 0001

{Kết thúc phần header}

{Biên đầu tiên, thể hiện phần đầu của message}

----6B9767D111AE

{Đây là đoạn text, thể hiện các ký tự dạng US-ASCII}

Content-Type: text/plain;charset=us-ascii

Content-Transfer-Encoding:7bit

{Kết thúc phần header}

Davis,

I am----------

Thanks,

Davis

{phần sau là phần đánh dấu biên}

----------6B767D111AE

Content-Type: application/octet-stream

Content-Transfer –Encoding:base64

Content-Disposision:attachment;filename=”Sublic2.doc”

{Phần dưới đây là nội dung file}

0M8……

{Phần sau đây là biên kết thúc file}

--------6B767D111AE

### 2. *MIME version header*

MIME version header định dạng một message như một message MIME, và xác định server của MIME chuẩn để dịch message. Nếu không tìm thấy header, client sẽ đối xử với message theo khuôn dạng chuẩn trong RFC. Phiên bản hiện tại của MINM là 1.0. cú pháp MIME header version như sau:

MIME-Version: 1.0

- **Content Type header**

Content Type header xác định khuôn dạng file được gắn vào một đối tượng. Header báo cho MIME cách hiển thị hay thao tác trên thân của message. Content Type Header bao gồm tên của header, theo sau bởi MIME. Kiểu MIME theo sau hai tên và được cách biệt nhau bởi ký tự slash (/). Tên đầu tiên là tên kiểu và tên thứ 2 là tên phụ. Sau đây là các ví dụ của Content type header;

Content-Type: image/jpeg

Content-Type: image/gif

Content-Type: image/bup

Content-Type: image/mpeg

Content-Type: applicatipn/octet-stream

Ba ví dụ đầu tiên trong phần này, đối tượng là kiểu ảnh (cũng là kiểu nhị phân), kiểu con của nó là jpeg, gif, và bmp. Các file ảnh này được nhúng vào trong các message. Dòng thứ tư trong các ví dụ này đó là một file chương trình.

Các kiểu và kiểu con có thể được thiết lập bởi các tham số. Mỗi tham số bao gồm một tên tham số, theo sau bởi dấu bằng (=) và tiếp theo là giá trị tham số. Các tham số được tách biệt giữa kiểu và kiểu con, cũng như các tham số khác và được tách biệt nhau bằng dấu chấm phẩy. Ví dụ sau đây thể hiện một tập các tham số:

Content-Type: text/plain;charset=us-ascii

Kiểu đối tượng này báo cho người đọc message rằng các phần đi sau là dạng text và sử dụng các ký tự theo kiểu text.

Header này có thể hoàn toàn tùy chon. Nếu nó không được cung cấp thì message được đối xử như một chuỗi các ký tự ASCII.

- **Content Transfer Encoding Header**

Content transfer Encoding Header xác định mô hình mã hóa được sử dụng để nhúng đối tượng vào trong thân của message. Để nhúng một đối tượng nhị phân vào trong một thư điện tử, cần phải chuyển nó sang dạng ASCII, do vậy nó được biên dịch theo khuôn dạng RFC 822. Ví dụ một cú pháp header để mã hóa nội dung khi chuyển là Content-Transfer-Encoding Base64.

Tài liệu MIME định nghĩa 5 kiểu mã hóa, nhưng 3 kiểu mã hóa thể hiện đối tượng không được mã hóa. Mã hóa 7 bit thường được dùng cho các vùng text theo khuôn dạng MIME. Hai kiểu kia mã hóa theo kiểu 8 bit và nhị phân, chỉ được sử dụng khi chuyển thư không phải SMTP, do SMTP chỉ cho phép các ký tự ASCII theo kiểu mã hóa 7 bit. Hai mô hình mã hóa còn lại đó là quoted-printable và base65 để chuyển các đối tượng từ dạng nhị phân sang kiểu ASCII.

### 3. *Cấu trúc message MIME đa phần*

Một số các khả năng phổ biến của MINE đó là có một message đa phần. Bằng cách sử dụng message đa phần, ta có thể nhúng cả hình ảnh và âm thanh vào các message text hay xay dựng một ứng dụng về một đối tượng hoạt hình, nó bao gồm một số file cần thiết để chạy ứng dụng.

Cấu trúc message đa phần gồm nhiều message kết hợp vào trong thân của một message, mỗi message với thông tin header của nó thể hiện kiểu nội dung mà mô hình mã hóa. Các phần này được tách biệt bởi các dấu biên mà message chính định ra. Để hiểu chi tiết về cấu trúc của một message đa phần, xem RFC 1521.

### 4. *Mã hóa BASE64*

Thuật toán mã hóa Base64 được thiết kế để mô tả một chuỗi tùy ý các giá trị 8 bit mà con người không có khả năng đọc được thành các ký tự ASCII. Thuật toán mã hóa và giải mã đơn giản nhưng dữ liệu mã hóa sẽ lớn hơn dữ liệu nguồn 33%.

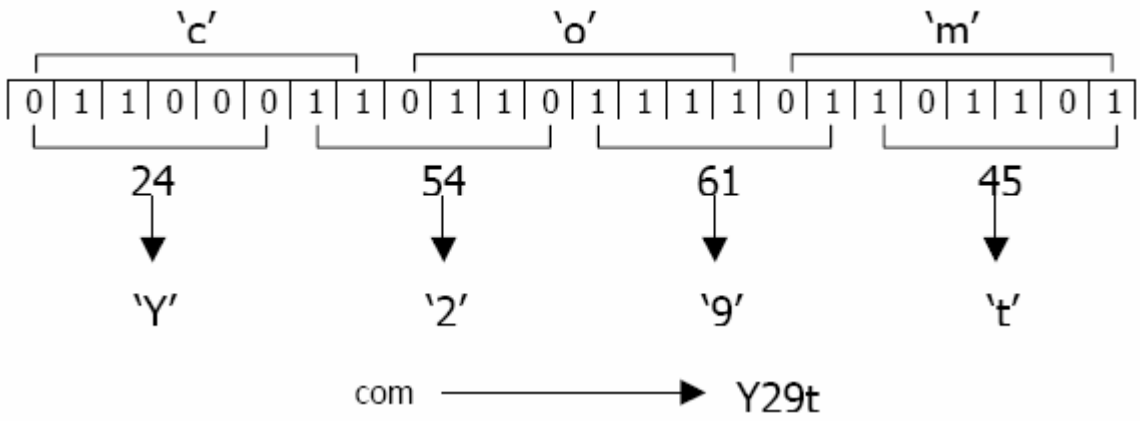
Một tập 65 ký tự AS-ASCII được dùng,cho phép 6 bit biểu diễn cho các ký tự có thể in được. (Ký tự 65, "=", là một ký tự sử lsy đặc biệt)

Tiến trình mã hóa biểu diễn nhóm 24 bít dữ liệu thành 4 ký tự mã hóa ở đầu ra. Tiến trình thực hiện từ trái sang phải, một nhóm 24 bit nhập được kết hợp từ nhóm 3 ký tự 8 bit. 24 bit đó được chia thành 4 ký tự 6 bit, mỗi nhóm được dịch thành một ký tự đơn dựa vào bảng mã Base64.

**Bảng mã Base64**

| Value | Encoding | Value | Encoding | Value | Encoding | Value | Encoding |
|---|---|---|---|---|---|---|---|
| 0 | A | 17 | R | 34 | i | 51 | Z |
| 1 | B | 18 | S | 35 | j | 52 | 0 |
| 2 | C | 19 | T | 36 | k | 53 | 1 |
| 3 | D | 20 | U | 37 | l | 54 | 2 |
| 4 | E | 21 | V | 38 | m | 55 | 3 |
| 5 | F | 22 | W | 39 | n | 56 | 4 |
| 6 | G | 23 | X | 40 | o | 57 | 5 |
| 7 | H | 24 | Y | 41 | p | 58 | 6 |
| 8 | I | 25 | Z | 42 | q | 59 | 7 |
| 9 | J | 26 | a | 43 | r | 60 | 8 |
| 10 | K | 27 | b | 44 | s | 61 | 9 |
| 11 | L | 28 | c | 45 | t | 62 | + |
| 12 | M | 29 | d | 46 | u | 63 | / |
| 13 | N | 30 | e | 47 | v | | |
| 14 | O | 31 | f | 48 | w | | |
| 15 | P | 32 | g | 49 | x | | |
| 16 | Q | 33 | h | 50 | y | | |

Ví dụ mô tả tiến trình mã hóa 3 ký tự nhập là "com":




Luồng dữ liệu được mã hóa đầu ra phải được biểu diễn bằng cá dòng có độ dài không lớn hơn 76 ký tự. Tất cả các ký tự xuống dòng hay các ký tự khác không có trong bảng mã Base64 đều được phần mềm giải mã bỏ qua.

Khi nhóm bit dòng nhập ít hơn 24 bít ( nghĩa là đến cuối của dữ liệu cần mã hóa) thì cần có xử lý đặc biệt. Khi có ít hơn 24bít dòng nhập thì các bits 0 được thêm vào phía bên phải nhóm bit để được đủ số 42 bít. Khi dòng nhập đã dủ 24 bít thì có các khả năng có thể xảy ra:

1. Phần cuối cùng của dữ liệu cần được mã hóa là 23 bít thì dữ liệu đầu ra cuối cùng sẽ là 4 ký tự đã mã hóa mà không có ký tự đệm"=".
2. Phần cuối cũng của dữ liệu cần mã hóa chính xác là 8 bít thì dữ liệu đầu ra cuối cùng sẽ là 2 ký tự đã mã hóa kèm theo 2 ký tự đệm "=" ở cuối.

Nếu phần cuối cùng của dữ liệu cần mã hóa chính xác là 16bít thì dữ liệu đầu ra cuối cùng sẽ gồm 3 ký tự đã mã hóa kèn theo với một ký tự đệm "=" ở cuối.

Bởi vì các ký tự đệm chỉ được thêm vào cuối của dữ liệu nên khi gặp bất kỳ một ký tự "=" nào thì hiển nhiên đã đến vị trí kết thúc của dữ liệu.

## VI.5. Các giao thức nhận mail:

### VI.5.1. Giao thức POP:

Người sử dụng có thể gởi thư bằng cách sử dụng SMTP, và có thể nhúng bất kỳ đối tượng nào vào trong message thông qua việc sử dụng khuôn mạng dạng MINE. Tuy nhiên, với SMTP, server để nhận được các message thư phải nối đến client và gởi tất cả các measage được phân phát cho client. Do đó, người sử dụng phải đăng ký tên máy dưới dạng tên địa chỉ Internet của người nhận.

SMTP được thiết kế trong trường hợp nhiều user sử dụng tất cả thời gian của họ kết nối đến một vài host và chạy một phiên đầu cuối. Giao thức không được thiết kế cho các tình huống thông dụng hiện nay, trong đó, hầu hết tất cả các user sử dụng e-mail kết nối hạn chế đến mail server đang giữ hộp thư. Người sử dụng

phải duy trì các message thư trên server và chuyển nó đến cho client khi client yêu cầu. Đây là mục đích trong thiết kế của POP.

POP (Post Office Protocol) được thiết kế bù đắp cho SMTP trong phần nhận các message. Những người thiết kế POP không gộp các chức năng gởi message và cho rằng SMTP tiếp tục được sử dụng để thực hiện các chức năng đó. Với giao thức POP, máy tính nhận được khởi tạo kết nối. Máy nhận kết nối đến mail server, login và nhận bất kỳ một mesage nào đang chờ. Do vậy máy gởi không cần biết gì về máy nhận trừ khi nó sử dụng login và password để dăng nhập. Ngày nay, hầu hết tất cả các mail client trên Internet mà bạn có thể sử dụng để kết hợp cả SMTP và POP.

### *1. Mô hình thông tin POP*

Trong mô hình lưu và phát, server mail cục bộ lưu các message đến khi các client nhận nó. POP client kết nối với server 110 của TCP. Để đăc nhập vào server, user sử dụng định danh (ID) và password. Sau khi đăng nhập thành công vào server, client có thể yêu server về các message mới đang sẵn sàng, lấy bất kỳ message nào mà server đang gởi hay đang xóa đi một message nào đó trên server.

Mô hình thông tin POP sử dụng 3 trạng thái giao tác để cung cấp chức năng này đến POP client:

- Trạng thái đặc quyền: Server kiểm tra quyền truy nhập của client (ID và password).
- Trạng thái giao tác: Client có thể nhận hay xóa message.
- Trạng thái cập nhập : Trạng thái này được chuyển đến ngay sau khi client tạo ra lệnh quit.

Trạng thái cập nhật là trạng thái cho pháp thao tác trên message. Khi client đang ở trên trạng thái giao tác, bạn có thể tạo ra lệnh reset để hủy bỏ tất cả các thao tác xóa trước đó (undo).

### *2. Chuẩn POP3*

Giao thức POP3 được cải biên từ giao thức POP. Nhiệm vụ của giao thức POP3 là lấy từ mailbox về khi nào người nhận muốn

Đặc điểm của hệ thống dùng POP là cho phép người sử dụng login vào POP server và nhận các mailbox của mình mà không cần phải login vào mạng mặc dù các mailbox thường nằm ở các Mail Server nằm trong mạng (thông thường muốn thâm nhập mạng ta phải có một account trên mạng và phải cung cấp password khi đăng nhập vào mạng). Người sử dụng có thể truy nhập POP Server bất cứ hệ thống nào trên mạng Interrnet, từ bất cứ UA nào dùng giao thức POP.

POP3 định nghĩa 3 giai đoạn tạo thành POP Session: Giai đoạn 1 là giai đoạn xác định tính hợp pháp của người nhận mail (Authorization); giai đoạn 2 là giai đoạn giao dịch giữa PC và POP Server (Transaction) và giai đoạn 3 là giai đoạn cập nhập thông tin (Update).

Sau khi thiết lập kết nối với Server, giai đoạn đầu Client sẽ cho Server biết nó là ai. nếu Client hợp pháp POP Server sẽ mở Mailbox và bắt đầu chuyển sang giai đoạn giao dịch. Giai đoạn giao dịch, chương trình sẽ yêu cầu POP3 Server cung cấp các thông tin như danh sách mail … hay yêu cầu gởi về cho nó một bức mail xác định nào đó. Giai đoạn cuối cũng sẽ cập nhập và đóng kết hiện hành.

Các lệnh thông dụng của giao thức POP3:

| **Lệnh** | **Ý nghĩa** |
|---|---|
| User | Cho biết tên của user cho POP Server |
| Pass | Yêu cầu một password cho người sử dụng trên Server |
| Quit | Đóng kết nối đã được thiết lập trước đó |
| Stat | POP Server trả về số lượng Mail có trong mailbox của người sử dụng cùng kích thước chúng |
| List | Trả về các ID và size của các message |
| Retr | Nhận một message từ mailbox (yêu cầu tham số là ID của mail cần nhận) |
| Dele | Đánh dấu một message để xóa ( yêu cầu tham số là ID của mail cần xóa) |
| Noop | POP Server trả về +OK nhưng không làm gì cả |
| Last | Yêu cầu POP Server trả về số Message đã truy nhập |
| Top | Liệt kê header của Mail |
| Rset | Hủy đánh dấu trên Message bị đánh dấu để xóa |

POP3 chỉ định nghĩa hai loại trả lời cho mỗi câu lệnh là : +OK để chỉ thao tác hoàn thành tốt và –ERR để báo có lỗi. Ví dụ cách dùng một số lệnh của POP3 như sau (các hàng sau dấu chấm phẩy để chú thích lệnh)

**Giai đoạnn 1: Nhận dạng user**

```
CLIENT: USER user01        ; cho biết tên user là user01
SERVER: +OK                ; báo thành công
CLIENT: PAS abc            ;cho biết Password là abc
```

SERVER: +OK user01's ; maildrop là 2 message (520octets)

**Giai đoạn 2: Trao đổi**

CLIENT: STAR ; số mail trong mailbox

SERVER: +OK 2 500 ; có 2 mail với tổng kích thước là 520

CLIENT: LIST ; Liệt kê các ID và kích thước của các mail

SERVER: +OK 2message (520 octets)

SERVER: 1 110 ; mail thứ 1 kích thước 110

SERVER: 2 410 ; mail thứ 2 kích thước 410

CLIENT: List 1 ;Cho thông tin về mail có ID là 1

SERVER: +OK 1 110

CLIENT: LIST 4

SERVER: -ERR no such message, only 2 message in maildrop

……

**Giai đoạn 3: Kết thúc**

CLIENT: q\QUIT ; đóng kết nối TCP hiện hành

SERVER: +OK dhdl POP3 server signing off

Chú ý rằng các message bị đánh dấu để xóa bằng lệnh DELE thực sự chưa bị xóa ngay để nếu sau đó ta có thể dùng lệnh phục hồi không xóa băng lệnh RSET, chúng chỉ thực sự bị xóa bỏ khỏi maildrop khi bước vào giai đoạn Update (khi gởi lệnh QUIT).

### V.5.1. Giao thức IMAP:

Không giống như POP3, hoạt động với giả thiết người dùng sẽ download thư điện tử về máy tính và xóa trên server, IMAP (Internet Mail Access Protocol), là giao thức cho phép các thư điện tử lưu trữ không giới hạn về thời gian trên server. IMAP cung cấp các cơ chế để đọc và thậm chí chia nhỏ thư, một đặc tính có lợi khi sử dụng kết nối tốc độ chậm. Vì hoạt động theo hướng thư điện tử sẽ không chuyển về lưu trữ trên máy tính người dùng, IMAP cho phép tạo, xóa và quản lý nhiều mail-box trên server.

## VI.6. Dịch vụ phân giải tên miền (DNS Services-Domain Name System Services)

Địa chỉ Internet 32 bit thỏa mãn yêu cầu kỹ thuật, nhưng phức tạp và khó nhớ đối với người dùng. Giải pháp đưa ra ở đây là dùng những tên gợi nhớ thay chổ địa chỉ số là tự nhiên và dễ nhớ đối với người sử dụng. Hơn nữa, dùng tin tin cậy hơn địa chỉ số vì địa chỉ số có thể thay đổi những tên luôn luôn dùng lại được. Do đó nảy sinh vấn đề cách đặt tên và ánh xạ địa chỉ IP với tên.

Trước đây trung tâm thông tin Internet NIC chịu trách nhiệm cấp phát và quản lý tên. Người ta dùng một file có tên host.txt trên Windows hoặc/etc/hosts trên Unix, tập tin này chứa tên của tất cả các mạng, router, host và địa chỉ IP tương ứng với chúng. Các tên được cấp phát không có mối liên hệ gì với nhau. Khi Internet phát triển, giải pháp này trở nên phức tạp không chấp nhận được về mặt quản lý.

Theo Paul Mockipetris, người thiết kế chính DNS, mục tiêu thiết kế bắt đầu của DNS là để thay thế các tập tin host phức tạp bằng một cơ sở dữ liệu phân tán nhẹ hơn có khả năng cung cấp một *không gian tên thứ bậc, sự quản lý phân tán, có bộ đệm cục bộ (caching), các kiểu mở rộng, kích thước cơ sở dữ liệu không giới hạn và có hiệu năng.*

DNS tương ứng với tầng 7 của mô hình OSI và dùng giao thức UDP hay TCP ở tầng dưới. Việc truy cập DNS thực hiện theo mô hình Client/Server. Hầu hết các hệ thống kết nối Internet đầu hỗ trợ DNS. Các địa chỉ DNS được định nghĩa trong tài liệu RFC 974, 1034, 1035. Dịch vụ cài đặt giao thức DNS phổ biến nhất BIND (Berkeley Internet Name Domain), được phát triển đầu tiên tại Berkeleycho hệ diều hành Unix.

DNS gồm 3 thành phần : **Namespace, các NameServer và Resover**

### V.5.2. Không gian tên miền

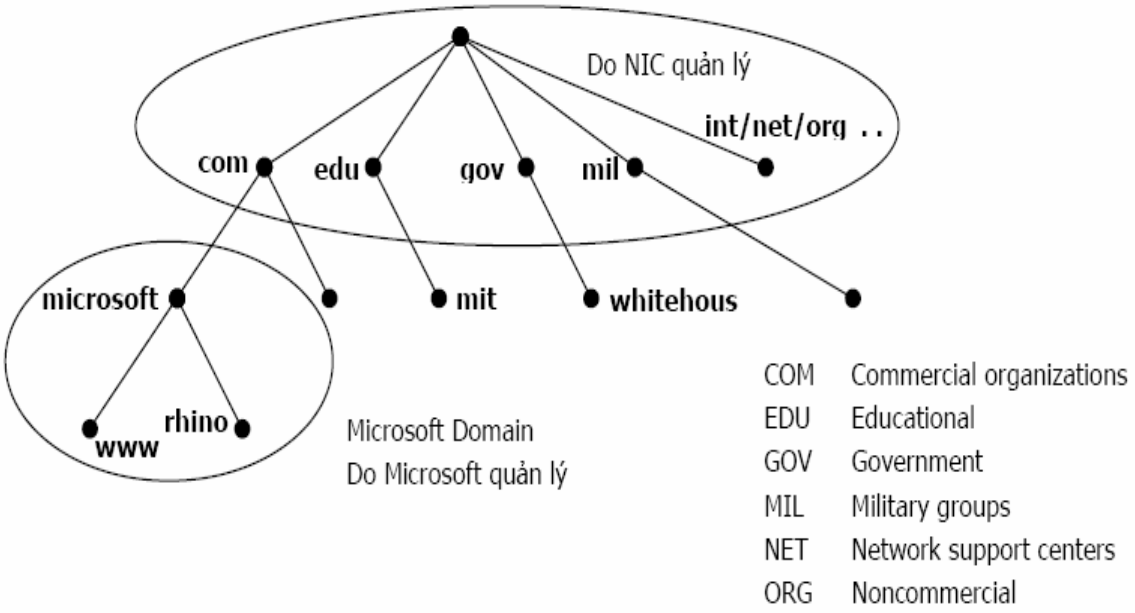
DNS tổ chức không gian tiên miền theo cấu trúc cây, trên cùng là gốc, rồi đến các nút cha, nút con… và cuối cùng là các nút lá.

Một máy tính trong mạng sẽ ứng với một nút của cây. Như ở trên, máy ở lá www sẽ có địa chỉ hoàn chỉnh www.microsoft.com. Mỗi nút trên cây biểu diễn một miền (domain) trong hệ thống DNS; mỗi miền lại có một hay nhiều miền con. Tại mỗi miền này đều phải có máy chủ DNS tương ứng quản lý hệ thống tên trong miền đo.

*Nút trên cây*: Mỗi nút có một tên tương ứng dài từ - đến 63 ký tự dưới 128 trong bảng mã ASCII. Các nút kề nhau không được có cùng tên. Mỗi nút có một tập (có thể rỗng) các *bản ghi tài nguyên* (Resource Record –RR) chứa thông tin đi kèm nút đó. Nhãn rỗng dành riêng cho nút gốc, ký hiệu bằng dấu chấm (.).

*Miền con*: Được tạo thành từ mỗi nút của không gian tên và các nút bên dưới có thể đi đến được các nút đó.

*Vùng:* Là một phần cây con của cây DNS được quản lý như một thực thể riêng. Vùng có thể bao gồm một miền hay một miền với một số miền con. Các miền con mức thấp hơn của một vùng lại có thể chia thành các vùng rời nhau.




Hình VI-6. Cấu trúc không gian tên miền DNS

*Tên miền của một nút:* là dãy các nhãn từ một nút trên cây đến gốc của cây. Các nhãn trong tên miền cách nhau bằng dấu chấm (.). *Tên miền tuyệt đối* kết thúc bằng dấu chấm và sẽ được phần mềm cục bộ ghép đầy đủ khi xử lý. Để đơn giản việc cài đặt, độ dài tên miền được giới hạn 255. Một miền là miền con của miền khác nếu tên miền đó chứa tên miền kia. Ví dụ A,B,C,D là miền con của các miền B,C,D,C,D,D, và miền gốc.

*Tên miền đầy đủ*: là tên các nút từ gốc lá của cây nối với nhau và phân cách bằng dấu chấm. Ví dụ mrp2.widgets.mfg.universal.co.uk

*Các miền mức định*: Miền gốc và các miền mức định của cây DNS do NIC quản lý. Các tên miền mứ định có thể chia ba loại.

- Các miền tổ chức (tên 3 ký tự): com, edu, gov…
- Các miền địa lý (các mã quốc gia, 2 ký tự): uk, vn, ca, fr…
- Miền in-addr-arpa: miền đặc biệt để ánh xạ địa chỉ thành tên.

Trách nhiệm quản lý không gian tên DNS dưới mức đỉnh được NIC ủy nhiệm cho các tổ chức khác. Các tổ chức này lại chia không gian tên phía dưới và ủy nhiệm xuống. Mô hình quản lý phân tầng cho phép DNS được quản lý tự trị bởi các tổ chức tham gia. Các đặt tên như vậy có tác dụng phân cấp quản lý vùng tên. Các tổ chức có thể tự tạo không gian tên riêng của mình trong mạng không phụ thuộc vào sự cho phép của NIC.

Vấn đề tên và vùng con được nhiều hãng lớn bổ sung và làm phong phú thêm bằng những phương pháp của riêng họ. Ví dụ Microsoft có WINS-Windows Internet Naming Service, IBM, có DDNS – Dynamic Domain Nam System.

- **Cú pháp tên miền**

Cú pháp cho tên miền sau đây cho phép phù hợp với nhiều ứng dung nhưmail, telnet,…

<domain>::<subdomain>|” ”

<subdomain>::=<label>|<subdomain>”.”<label>

<label>::=<letter>[[<ldh-str>]<let-dig>]

<ldh-str>::=<let-dig-hyp>|<let-hyp><ldh-str>

<let-dig-hyp>::=<let-dig>|” ”

<let-dig>:=<letter>|<digit>

<leter>::=ký tự từ A-Z, a-z

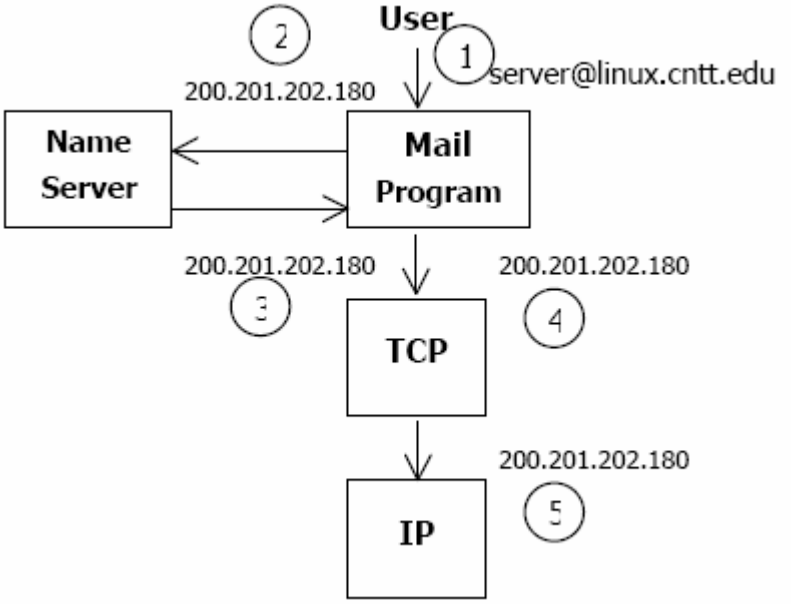
<digit>::=chữ số 0-9

### V.5.3. Máy chủ quản lý tên miền

Máy chủ quản lý tên (Name Server) quản lý cấu trúc cây của miền và các tập thông tin đi kèm. Máy chủ tên có thông tin đầy đủ về một số tập con gọi là vùng của không gian tên và các con trỏ đến các name server khác để lấy tin về một miền bất kỳ của cây miền. Các máy chủ tên có thông tin đầy đủ về một số phần của cây miền được gọi là có thẩm quyền (authoritative) về các phần đo. Một *vùng* (zone) là một đơn vị thông tin có thẩm quyền của cơ sở dữ liệu DNS. Trong thực tế, các máy chủ thường lưu tạm thời trong bộ đếm cấu trúc và thông tin các vùng về các vùng khác để tăng hiệu năng. Các máy chủ quản lý tên trong vùng trao đổi thông tin với nhau bằng Zone Transfer Protocol.

### V.5.4. Chương trình phân giải tên miền

Chương trình phân giải tên (resolver) là các chương trình hệ thống lấy thông tin từ nameserver để trả lời yêu cầu của những ứng dụng khách (client). Resolver phải có khả năng truy cập đến ít nhất một nameserver và dùng thông tin của nameserver đó trả lời trực tiếp câu hỏi hay để hỏi tiếp các nameserver khác. Chương trình người sử dụng có thể truy cập trực tiếp đến resolver, do đó không cần có một giao thức giữa resolver và chương trình người dùng.




Hình VI-7. Quá trình phân giải tên miền trong thực tế

# Tài liệu tham khảo

[1] Andrew S. Tanenbaum, **Computer Network**, Fourth Edition, Prentice Hill, 2003.

[2] James F. Kurose, Keith W.Ross, **A top-down approach featuring the Internet**, Addison Wesley, Third Edition, 2000.

[3] Nguyễn Tấn Khôi**, Giáo trình Mạng máy tính**, Đại học Bách khoa Đà Nẵng, 2004.

# Giáo trình mạng máy tính

Trang

**GIỚI THIỆU .....5**

**CHƯƠNG 1 - GIỚI THIỆU VỀ MẠNG MÁY TÍNH .....6**

*1.1 Lịch sử mạng máy tính .....6*
*1.2 Một số khái niệm cơ bản .....7*
*1.3 Mạng ngang hàng (Peer to Peer) và mạng có máy chủ (Server based) .....10*
*1.4 Các hệ điều hành mạng.....11*
*1.5 Các dịch vụ mạng .....12*
*1.6 Làm thế nào để trở thành một chuyên nghiệp viên về mạng máy tính?.....13*

**CHƯƠNG 2 - MÔ H Ì NH OSI.....17**

*2.1 Kiến trúc phân tầng và mô hình OSI (Open System Interconnect).....17*
*2.2 Ý nghĩa và chức năng của các tầng trong mô hình OSI .....19*
*2.3 Áp dụng mô hình OSI.....23*
*2.4 Mô tả các thành phần của khuôn dữ liệu (Frame) .....25*

**CHƯƠNG 3 - ĐƯỜNG TRUYỀN VẬT LÝ ..... 30**

*3.1 Truyền dữ liệu: tín hiệu tương tự (analogue) và tín hiệu số hoá (digital) ..... 30*

*3.2 Các đặc tính của đường truyền mạng ..... 31*

*3.3 Các mạng LAN: Baseband và Broadband ..... 32*

*3.4 Các loại cáp mạng ..... 33*

**CHƯƠNG 4 - CÁC GIAO THỨC MẠNG (PROTOCOLS) ..... 40**

*4.1 Giao thức (protocol) mạng là gì? ..... 40*

*4.2 Bộ giao thức TCP/IP (Transmission Control Protocol / Internet Protocol) ..... 41*

*4.3 Bộ giao thức IPX/SPX (Internetwork Packet Exchange / Sequenced Packet Exchange ) 44*

*4.4 Bộ giao thức Microsoft Network ( NETBIOS, NETBEUI, SMB) ..... 45*

*4.5 Một số Protocols khác ..... 47*

**CHƯƠNG 5 - CÁC HÌNH TRẠNG (TOPOLOGIES) CỦA MẠNG CỤC BỘ (LAN) ..... 49**

*5.1 Các đặc trưng cơ bản của mạng cục bộ (LAN) ..... 49*

*5.2 Các hình trạng LAN đơn giản ..... 51*

*5.3 Các hình trạng LAN hỗn hợp ..... 54*

*5.4 Các hệ thống giao vận mạng ..... 56*

*5.5 Kiến trúc Ethernet ..... 59*

*5.6 Mạng Token Ring ..... 64*

**CHƯƠNG 6 – GIỚI THIỆU WINDOWS 2000 ..... 70**

*6.1 Các phiên bản của Windows 2000 ..... 70*

*6.2 Một số đặc điểm mới của Windows 2000 ..... 71*

*6.3 Mô hình workgroup và mô hình domain trong Windows 2000 ..... 76*

**CHƯƠNG 7 – CÀI ĐẶT WINDOWS 2000 SEVER ..... 80**

*7.1 Cài đặt Windows 2000 Server ..... 80*

*7.2 Đăng nhập tới một Domain ..... 88*

*7.3 Các công cụ quản trị ..... 90*

*7.4 Hộp thoại bảo mật Windows 2000 ..... 90*

**CHƯƠNG 8 - QUẢN TRỊ TÀI KHOẢN NGƯỜI DÙNG ..... 93**

*8.1 Các loại tài khoản người dùng (user) ..... 93*

*8.2 Lập kế hoạch tài khoản người dùng ..... 94*

*8.3 Tạo tài khoản người dùng cục bộ và tài khoản người dùng miền ..... 97*

*8.4 Thiết lập hồ sơ người dùng (User Profile) ..... 106*

**CHƯƠNG 9 - QUẢN TRỊ TÀI KHOẢN NHÓM ..... 113**

*9.1. Các loại nhóm trong Windows 2000 ..... 113*
*9.2. Lập kế hoạch nhóm Local Domain và nhóm Global ..... 114*
*9.3. Tạo và xoá các nhóm ..... 114*
*9.4. Thêm các thành viên vào nhóm ..... 116*

**TÀI LIỆU THAM KHẢO ..... 121**

# GIỚI THIỆU

Yêu cầu có các tài liệu tham khảo cho sinh viên của khoa Công nghệ Thông tin - Trường Cao đẳng Công nghiệp 4 ngày càng trở nên cấp thiết. Việc biên soạn tài liệu này nằm trong kế hoạch xây dựng hệ thống giáo trình các môn học của Khoa.

Đề cương của giáo trình đã được thông qua Hội đồng Khoa học của Khoa và Trường. Mục tiêu của giáo trình nhằm cung cấp cho sinh viên một tài liệu tham khảo chính về môn học Mạng máy tính, trong đó giới thiệu những khái niệm căn bản nhất về hệ thống mạng máy tính, đồng thời trang bị những kiến thức và một số kỹ năng chủ yếu cho việc bảo trì và quản trị một hệ thống mạng. Đây có thể coi là những kiến thức ban đầu và nền tảng cho các kỹ thuật viên, quản trị viên về hệ thống mạng.

Tài liệu này có thể tạm chia làm 2 phần:

- Phần 1: từ chương 1 đến chương 5
- Phần 2: từ chương 6 đến chương 9

Phần 1, bao gồm những khái niệm cơ bản về hệ thống mạng (chương 1), nội dung chính của mô hình tham chiếu các hệ thống mở - OSI (chương 2), những kiến thức về đường truyền vật lý (chương 3), khái niệm và nội dung cơ bản của một số giao thức mạng thường dùng (chương 4) và cuối cùng là giới thiệu về các hình trạng mạng cục bộ (chương 5)

Phần 2, trình bày một trong những hệ điều hành mạng thông thường nhất hiện đang dùng trong thực tế: hệ điều hành mạng Windows 2000 Server. Ngoài phần giới thiệu chung, tài liệu còn hướng dẫn cách thức cài đặt và một số kiến thức liên quan đến việc quản trị tài quản người dùng.

Tham gia biên soạn giáo trình có:

- Giảng viên Nguyễn Văn Bình biên soạn chính các chương 1, 2, 5
- Giảng viên Tạ Duy Công Chiến biên soạn chính các chương 3, 4, 9
- Giảng viên Nguyễn Chí Hiếu biên soạn các chương 6, 7, 8.

Mặc dù đã có những cố gắng để hoàn thành giáo trình theo kế hoạch, nhưng do hạn chế về thời gian và kinh nghiệm soạn thảo giáo trình, nên tài liệu chắc chắn còn những khiếm khuyết. Rất mong nhận được sự đóng góp ý kiến của các thầy cô trong Khoa cũng như các bạn sinh viên và những ai sử dụng tài liệu này. Các góp ý xin gửi về Tổ Hệ thống máy tính – Khoa Công nghệ thông tin - Trường Cao đẳng Công nghiệp 4. Xin chân thành cảm ơn trước.

**Nhóm biên soạn**

Tháng 08/2004

# CHƯƠNG 1 - GIỚI THIỆU VỀ MẠNG MÁY TÍNH

## MỤC TIÊU CỦA CHƯƠNG

*Kết thúc chương này, sinh viên sẽ có thể:*

- Nắm sơ lược về lịch sử phát triển của mạng máy tính
- Hiểu được khái niệm mạng máy tính cũng như hai yếu tố cơ bản của nó là kiến trúc và môi trường truyền. Nắm được ba tiêu chí cơ bản để phân loại mạng máy tính và hình trạng tổng quan của mạng LAN.
- Nắm được hai mô hình mạng: *ngang hàng* (peer-to-peer) và *client/server*.
- Biết được một số hệ điều hành mạng thông dụng.
- Nắm được một số dịch vụ cơ bản có trên mạng.
- Những yêu cầu cần có để trở thành một chuyên nghiệp viên về mạng máy tính.

## 1.1 Lịch sử mạng máy tính

*Từ đầu những năm 60* đã xuất hiện các *mạng xử lý* trong đó các *trạm cuối* (terminal) thụ động được nối vào một máy xử lý trung tâm. Vì máy xử lý trung tâm làm tất cả mọi việc: quản lý các thủ tục truyền dữ liệu, quản lý sự đồng bộ của các trạm cuối v.v…, trong khi đó các trạm cuối chỉ thực hiện chức năng nhập xuất dữ liệu mà không thực hiện bất kỳ chức năng xử lý nào nên hệ thống này vẫn chưa được coi là *mạng máy tính.*

*Giữa năm 1968*, Cục các dự án nghiên cứu tiên tiến (ARPA – Advanced Research Projects Agency) của Bộ Quốc phòng Mỹ đã xây dựng dự án nối kết các máy tính của các trung tâm nghiên cứu lớn trong toàn liên bang, mở đầu là Viện nghiên cứu Standford và 3 trường đại học (Đại học California ở Los Angeless, Đại học California ở Santa Barbara và Đại học Utah). Mùa thu năm 1969, 4 trạm đầu tiên được kết nối thành công, đánh dấu sự ra đời của ARPANET. Giao thức truyền thông dùng trong ARPANET lúc đó đặt tên là NCP (Network Control Protocol).

*Giữa những năm 1970*, họ giao thức TCP/IP được Vint Cerf và Robert Kahn phát triển cùng tồn tại với NCP, đến năm 1983 thì hoàn toàn thay thế NCP trong ARPANET.

*Trong những năm 70*, số lượng các mạng máy tính thuộc các quốc gia khác nhau đã tăng lên, với các kiến trúc mạng khác nhau (bao gồm cả phần cứng lẫn giao thức truyền thông), từ đó dẫn đến tình trạng không tương thích giữa các mạng, gây khó khăn cho người sử dụng. Trước tình hình đó, vào *năm 1984* Tổ chức tiêu chuẩn hoá quốc tế ISO đã cho ra đời *Mô hình tham chiếu cho việc kết nối các hệ thống mở* (Reference Model for Open Systems Interconnection - gọi tắt là mô hình OSI). Với sự ra đời của OSI và sự xuất hiện của máy tính cá nhân, số lượng mạng máy tính tính trên toàn thế giới đã tăng lên nhanh chóng. Đã xuất hiện những khái niệm về các loại mạng LAN, MAN.

*Tới tháng 11/1986* đã có tới 5089 máy tính được nối vào ARPANET, và đã xuất hiện thuật ngữ "Internet".

*Năm 1987*, mạng xương sống (backborne) NSFnet (National Science Foundation network) ra đời với tốc độ đường truyền nhanh hơn (1,5 Mb/s thay vì 56Kb/s trong ARPANET) đã thúc đẩy sự tăng trưởng của Internet. Mạng Internet dựa trên NSFnet đã vượt qua biên giới của Mỹ.

*Đến năm 1990*, quá trình chuyển đổi sang Internet - dựa trên NSFnet kết thúc. NSFnet giờ đây cũng chỉ còn là một mạng xương sống thành viên của mạng Internet toàn cầu. Như vậy có thể nói lịch sử phát triển của Internet cũng chính là lịch sử phát triển của mạng máy tính.

## 1.2 Một số khái niệm cơ bản

### 1.2.1. Mạng máy tính là gì?

Ta có thể định nghĩa: mạng máy tính là một tập hợp các máy tính được nối kết với nhau bởi các *đường truyền vật lý* theo một *kiến trúc* nào đó.

Một cách cụ thể hơn ta có thể hiểu mạng máy tính bao gồm sự kết nối từ hai máy tính trở nên. Các máy tính này có thể giao tiếp với nhau, chia xẻ tài nguyên (các đĩa cứng, các máy in và các ổ đĩa CD-ROM v.v…), mỗi máy có thể truy xuất các máy ở xa hoặc các mạng khác để trao đổi các file, dữ liệu và thông tin hoặc cho phép các giao tiếp điện tử.

### 1.2.2. Các yếu tố của mạng máy tính.

Như đã định nghĩa ở trên, hai yếu tố căn bản của mạng máy tính là: *đường truyền vật lý* và *kiến trúc* mạng. Kiến trúc mạng bao gồm: *hình trạng* (topology) của mạng và *giao thức* (protocol) truyền thông. Đường truyền mạng (medium) bao gồm: loại có dây (wire): các loại cáp kim loại, cáp sợi quang, và loại không dây (wireless): tia hồng ngoại, sóng điện từ tần số radio v.v…. Chi tiết về các nội dung này sẽ được trình bày ở các chương sau.

### 1.2.3. Các tiêu chí phân loại mạng máy tính.

Dựa vào các tiêu chí khác nhau, người ta phân chia mạng máy tính thành các loại khác nhau. Sau đây là ba tiêu chí cơ bản.

a) Phân loại mạng dựa trên *khoảng cách địa lý,* có ba loại mạng:

- *Mạng cục bộ* (Local Area Network – LAN): là mạng được cài đặt trong một phạm vi tương đối nhỏ (trong một phòng, một toà nhà, hoặc phạm vi của một trường học v.v…) với khoảng cách lớn nhất giữa hai máy tính nút mạng chỉ trong khoảng vài chục km trở lại. Tổng quát có hai loại mạng LAN: *mạng ngang hàng* (peer to peer) và *mạng có máy chủ* (server based). Mạng server based còn được gọi là mạng "*Client / Server*" (Khách / Chủ).
- *Mạng đô thị* (Metropolitan Area Network – MAN): là mạng được cài đặt trong phạm vi một đô thị hoặc một trung tâm kinh tế - xã hội có bán kính khoảng 100 km trở lại.
- *Mạng diện rộng* (Wide Area network – WAN): phạm vi của mạng có thể vượt qua biên giới quốc gia và thậm chí cả lục địa. Cáp truyền qua đại dương và vệ tinh được dùng cho việc truyền dữ liệu trong mạng WAN.

- *Mạng toàn cầu* (Global Area Network – GAN): phạm vi của mạng trải rộng toàn Trái đất.

b) Phân loại mạng dựa trên *kỹ thuật chuyển mạch*, cũng có ba loại mạng:

- *Mạng chuyển mạch kênh* (circuit – switched networks): khi có hai thực thể cần trao đổi thông tin với nhau thì giữa chúng sẽ được thiết lập một "kênh" cố định và được duy trì cho đến khi một trong hai bên ngắt kết nối. Các dữ liệu chỉ được truyền theo con đường cố định này. Kỹ thuật chuyển mạch kênh được sử dụng trong các kết nối ATM (Asynchronous Transfer Mode) và dial-up ISDN (Integrated Services Digital Networks). Ví dụ về mạng chuyển mạch kênh là mạng điện thoại.

  Phương pháp chuyển mạch kênh có hai nhược điểm chính:

  - Phải tốn thời gian để thiết lập đường truyền cố định giữa hai thực thể.
  - Hiệu suất sử dụng đường truyền không cao, vì có lúc trên kênh không có dữ liệu truyền của hai thực thể kết nối, nhưng các thực thể khác không được sử dụng kênh truyền này.

- *Mạng chuyển mạch thông báo* (message – switched networks):

  *Thông báo* (message) là một đơn vị thông tin của người sử dụng có khuôn dạng được qui định trước. Mỗi thông báo có chứa vùng thông tin điều khiển trong đó có phần địa chỉ đích của thông báo.

  Trong mạng chuyển mạch thông báo, giữa hai thực thể truyền thông tồn tại nhiều đường truyền khác nhau. Căn cứ vào địa chỉ đích, các thông báo khác nhau có thể đến đích theo những con đường khác nhau.

  Phương pháp chuyển mạch thông báo có một số ưu điểm:

  - Hiệu suất sử dụng đường truyền cao, vì có thể phân chia giữa nhiều thực thể.
  - Mỗi nút mạng có thể lưu trữ thông báo cho đến khi kênh truyền rảnh mới gửi thông báo đi, do đó giảm được trình trạng tắc nghẽn mạng. v.v…

  Nhược điểm chính của phương pháp chuyển mạch thông báo là không hạn chế kích thước của các thông báo, do đó có thể dẫn đến phí tổn lưu trữ tạm thời cao. Kỹ thuật chuyển mạch thông báo thích hợp với các dịch vụ thông tin kiểu thư điện tử (Electronic Mail)

- *Mạng chuyển mạch gói* (packet - switched networks): mỗi thông báo được chia thành nhiều phần nhỏ hơn gọi là các *gói tin* (packet) có khuôn dạng qui định trước. Mỗi gói tin cũng có phần thông tin điều khiển chứa địa chỉ nguồn (sender) và địa chỉ đích (receiver) của gói tin. Các gói tin thuộc về một thông báo có thể truyền tới đích theo những con đường khác nhau.

  Kỹ thuật chuyển mạch gói về cơ bản giống kỹ thuật chuyển mạch thông báo, nhưng có hiệu quả hơn là phí tổn lưu trữ tạm thời tại mỗi nút giảm đi vì kích thước tối đa của các gói tin được giới hạn.

  Những khó khăn của kỹ thuật chuyển mạch gói cần giải quyết là: tập hợp các gói tin tại nơi nhận để tạo lại thông báo ban đầu cũng như xử lý việc mất gói.

Do có nhiều ưu điểm nên hiện nay mạng chuyển mạch gói được dùng phổ biến hơn các mạng chuyển mạch thông báo. Việc tích hợp cả hai kỹ thuật chuyển mạch kênh và thông báo trong một mạng thống nhất gọi là *mạng dịch vụ tích hợp số hoá* (Integrated Services Digital Networks – ISDN) đang là một trong những xu hướng phát triển của mạng ngày nay.

c) Phân loại mạng dựa trên *kiến trúc mạng* (topology và protocol). Ví dụ như mạng System Network Architecture (SNA) của IBM, mạng ISO (theo kiến trúc chuẩn quốc tế), mạng TCP/IP v.v….

### 1.2.4. Tổng quan về hình trạng mạng (topology) LAN

Hình trạng mạng chủ yếu thể hiện trong các mạng LAN. Mỗi chuẩn về LAN có các quy tắc riêng cho việc nối dây. Các quy tắc này định nghĩa việc kết nối đường truyền, những yêu cầu về phần cứng và cách thức sắp xếp các thành phần khác nhau. Có ba yếu tố xác định bản chất của một mạng LAN:

- Hình trạng mạng.
- Đường truyền.
- Kỹ thuật truy xuất đường truyền.

a) Hình trạng mạng (Topology)

Cách sắp đặt hình học (hoặc vật lý) sơ đồ nối dây mạng máy tính gọi là *hình trạng mạng* (topology). Có hai loại hình trạng:

- *Hình trạng vật lý* của một mạng mô tả con đường các cáp mạng được định tuyến. Nó không xác định kiểu của các thiết bị, phương pháp kết nối hoặc các địa chỉ trên mạng.
- *Hình trạng luận lý* của một mạng mô tả con đường mà mạng hoạt động trong khi truyền thông tin giữa các thiết bị khác nhau.

b) Hình trạng vật lý (Physical topology).

Cấu trúc vật lý đầy đủ của đường truyền mạng được gọi là *hình trạng vật lý*.

Hình trạng vật lý của một mạng được phân thành ba loại hình dạng hình học cơ bản: *bus, ring* hoặc *star*. Ba hình trạng này có thể kết hợp để tạo thành các hình trạng *hỗn hợp* (hybrid) như: *star-wired ring, star-wired bus* và *daisy chains* (Chi tiết về các hình trạng này sẽ được khảo sát ở chương 3 - "Topology").

Khi chọn một topology mạng vật lý, ta nên tập trung vào các đặc tính sau:

- Tính dễ dàng sắp đặt.
- Tính thuận tiện cho việc cấu hình lại.
- Việc chẩn đoán và sửa chữa các sự cố tương đối dễ dàng.
- Chi phí, hiệu suất, độ tin cậy, khả năng mở rộng mạng trong tương lai, kiểu và chiều dài của cáp mạng.

c) Hình trạng luận lý (Logical topology)

Hình trạng luận lý của mạng xác định các đặc tính truyền dữ liệu của nó, chẳng hạn như mô hình giao vận mạng. Đối với các mạng LAN, hai hình trạng luận lý thông thường nhất là *Ethernet* và *Token Ring*.

## 1.3 Mạng ngang hàng (Peer to Peer) và mạng có máy chủ (Server based)

### 1.3.1 Mạng ngang hàng (peer-to-peer network)

Các mạng peer-to-peer là một ví dụ rất đơn giản của các mạng LAN. Chúng cho phép mọi nút mạng vừa đóng vai trò là thực thể *yêu cầu* các dịch vụ mạng, vừa là các thực thể *cung cấp* các dịch vụ mạng. Phần mềm mạng peer-to-peer được thiết kế sao cho các thực thể ngang hàng thực hiện cùng các chức năng tương tự nhau.

Các đặc điểm của mạng peer-to-peer:

- Các mạng peer-to-peer còn được biết đến như các mạng **workgroup** (nhóm làm việc) và được sử dụng cho các mạng có 10 người sử dụng (user) làm việc trên mạng đó.
- Mạng peer-to-peer không đòi hỏi phải có người quản trị mạng (administrtor). Trong mạng peer-to-peer mỗi user làm việc như người quản trị cho trạm làm việc riêng của họ và chọn tài nguyên hoặc dữ liệu nào mà họ sẽ cho phép chia xẻ trên mạng cũng như quyết định ai có thể truy xuất đến tài nguyên và dữ liệu đó.

Các ưu điểm của mạng peer-to-peer:

- Đơn giản cho việc cài đặt.
- Chi phí tương đối rẻ.

Những nhược điểm của mạng peer-to-peer:

- Không quản trị tập trung, đặc biệt trong trường hợp có nhiều tài khoản cho một người sử dụng (user) truy xuất vào các trạm làm việc khác nhau.
- Việc bảo mật mạng có thể bị vi phạm với các user có chung username, password truy xuất tới cùng tài nguyên.
- Không thể sao chép dự phòng (backup) dữ liệu tập trung. Dữ liệu được lưu trữ rải rác trên từng trạm.

### 1.3.2 Mạng có máy chủ (Server based network / Client-Server network)

Mạng *server based* liên quan đến việc xác định vai trò của các thực thể truyền thông trong mạng. Mạng này xác định thực thể nào có thể tạo ra các *yêu cầu* dịch vụ và thực thể nào có thể *phục vụ* các yêu cầu đó (còn gọi là các thực thể *đáp ứng* yêu cầu dịch vụ). Các máy tính được gọi là các **file server** thực hiện việc xử lý dữ liệu và giao tiếp giữa các máy tính khác trong mạng. Các máy tính khác đó được gọi là các **workstation** (máy tính trạm).

Các mạng *server based* thường được sử dụng cho các mạng có 10 người sử dụng và thực hiện các công việc chuyên biệt sau:

- *File* và *Print Servers* - quản lý truy xuất của user tới các file và các máy in.
- *Application Servers* – máy chủ có nhiệm vụ cung cấp các ứng dụng, các phần mềm cho các máy trạm trong môi trường client/server.
- *Database Server* - máy chủ có cài đặt các hệ thống Cơ sở dữ liệu (DBMS) như SQL SERVER, Oracle, DB2 phục vụ cho các nhu cầu ứng dụng truy xuất dữ liệu trên mạng.
- *Communication Server* - máy chủ phục vụ cho công tác truyền thông, giao tiếp trên mạng như Web (Web Server), mail (mail Server), truyền nhận file (FTP server)…
- *Mail Servers* - hoạt động như một server ứng dụng, trong đó có các ứng dụng server và ứng dụng client, với dữ liệu được tải xuống từ server tới client.

Đặc điểm của mạng *server based*:

- Khó khăn trong việc cài đặt, cấu hình và quản trị hơn so với mạng peer-to-peer
- Cung cấp sự bảo mật tốt hơn cho các tài nguyên mạng.
- Dễ dàng hơn trong việc quản trị sao chép dự phòng dữ liệu (backup). Thậm chí có thể lập lịch cho công việc này thực hiện tự động.

## 1.4 Các hệ điều hành mạng

Cùng với việc ghép nối các máy tính thành mạng, cần thiết phải có các hệ điều hành được cài đặt trên từng máy tính có trong mạng. Trong đó có các hệ điều hành trên phạm vi toàn mạng có chức năng quản lý dữ liệu và tính toán, xử lý một cách thống nhất.

Những hệ điều hành dùng cho mạng máy tính cá nhân peer-to-peer bao gồm:

- Microsoft Windows for Workgroups 3.11
- Microsoft Windows 9X, ME
- Microsoft Windows NT Workstation
- Microsoft Windows 2000 Professional
- Microsoft Windows XP Professional
- Novell Netware Lite
- Linux for Workstation

Những hệ điều hành mạng máy tính cá nhân phổ biến nhất cho mạng server based bao gồm:

- Windows NT Server
- Windows 2000 Server và Advanced Server
- Unix (bao gồm cả Linux)
- Novell Netware

## 1.5 Các dịch vụ mạng

Các mạng kết nối hai hoặc nhiều hơn các máy tính với nhau để cung cấp một số phương pháp cho việc chia xẻ và truyền dữ liệu. Nhiều đặc điểm mà một mạng cung cấp được xem như các *dịch vụ* (services). Các dịch vụ thông thường nhất trên một mạng là: *thư điện tử* (email)*, in ấn, chia xẻ file, truy xuất Internet, quay số từ xa* (remote dial-in)*, giao tiếp*(communication) và *dịch vụ quản trị* (management service). Các mạng lớn có thể có những máy chủ (server) riêng, mỗi máy này thực hiện một trong các dịch vụ mạng. Với các mạng nhỏ hơn, tất cả các dịch vụ mạng được cung cấp bởi một hoặc vài máy chủ. (Một máy chủ có thể cung cấp nhiều dịch vụ mạng).

### 1.5.1 Các dịch vụ file và in ấn

Các dịch vụ file của một mạng có thể được sử dụng để chia xẻ các *phần mềm ứng dụng* như các chương trình xử lý văn bản, các cơ sở dữ liệu, các bảng tính hoặc các chương trình email. Các chương trình này được chạy trên một máy chủ trung tâm, có nghĩa là chúng không phải cài đặt cục bộ trên mọi máy tính. Chính điều này giảm bớt thời gian và chi phí cài đặt, cập nhật các file trên từng máy tính, vì mọi thứ được lưu trữ trong một vị trí trung tâm.

Các dịch vụ file cho phép các user chia xẻ dữ liệu và các tài nguyên khác nhanh và tiết kiệm. Email được gửi trong vài giây. Các file đa truyền thông (multimedia file) với kích thước lớn dễ dàng truyền qua mạng. Các web site có thể giúp chúng ta cập nhật thông tin mới nhất. Các tài nguyên quí hiếm như CD-ROM, fax modem, scanner v.v… có thể chia xẻ để dùng chung trên mạng.

Các máy in có thể dùng chung trên mạng nhờ các *dịch vụ in mạng*. Người quản trị mạng có thể cài đặt, quản trị, chẩn đoán và sửa các lỗi xảy ra trên các máy in mạng dễ dàng hơn do số lượng các máy in trong mạng giảm đi và công việc quản trị máy in mạng có thể được thực hiện trên chính máy tính mà người quản trị đang đăng nhập mà không cần trực tiếp đến từng máy in.

### 1.5.2 Sự bảo mật và quản trị được tập trung

Các file và chương trình trên một máy tính có thể được bảo vệ với các quyền chỉ cho các user nào được phép truy xuất và truy xuất ở mức nào. Các user chỉ cần đăng nhập với một tài khoản user hợp lệ sẽ cho phép họ truy xuất dữ liệu và tài nguyên mạng trong giới hạn quyền (permission) đã được cấp. Những tài nguyên mà một user có thể thấy trên mạng có thể bị ẩn đi đối với các user khác.

Các mạng cho phép các user truy xuất dữ liệu của họ từ bất kỳ máy tính nào trong mạng. Vì dữ liệu của họ được lưu trữ trên một máy tính chủ.

Việc sao chép dự phòng dữ liệu (backup) cũng trở nên dễ dàng hơn vì người quản trị chỉ cần backup một máy tính (máy chủ server). Chính việc lưu trữ các dữ liệu quan trọng trên một vị trí tập trung cho phép điều khiển và quản trị dữ liệu chặt chẽ hơn, tiết kiệm thời gian hơn so với việc lưu trữ dữ liệu trên mọi máy tính riêng lẻ.

### 1.5.3 Các dịch vụ thư điện tử (e-mail)

Việc chuyển e-mail giữa các user trên một mạng LAN hoặc giữa các user trên một mạng LAN và Internet được quản lý bởi các *dịch vụ thư tín* (mail service) mạng. Điều kiện để mọi người có thể giao tiếp trên mạng bằng e-mail là mỗi người phải có một địa chỉ e-mail.

### 1.5.4 Các dịch vụ giao tiếp (Communication services)

Các *dịch vụ giao tiếp* mạng cho phép các user bên ngoài kết nối tới mạng từ xa thông qua một đường dây điện thoại và một modem. Các dịch vụ này cũng cho phép các user trên mạng kết nối tới các máy hoặc mạng khác bên ngoài mạng LAN. Đa số các hệ điều hành mạng (Network Operating System – NOS) có các dịch vụ này bên trong, chẳng hạn:

- Windows NT 4.0 có Remote Access Server (RAS)
- Windows 2000 Server có Routing and Remote Access Server (RRAS)
- Netware có Network Access Server (NAS)

Các máy tính đang chạy các dịch vụ giao tiếp được gọi là các *máy chủ giao tiếp* (communication server) và chịu trách nhiệm quản lý các giao tiếp. Một khi user đã đăng nhập vào mạng từ xa và được xác nhận là hợp lệ thông qua máy chủ giao tiếp họ sẽ có các quyền truy xuất mà họ mong muốn giống như đang ngồi ở một máy tính trạm được kết nối vật lý trực tiếp với mạng đó (trừ trường hợp người quản trị hạn chế việc truy xuất khi đăng nhập từ xa).

### 1.5.5 Các dịch vụ Internet

Các *dịch vụ Internet* bao gồm các máy chủ World Wide Web (WWW) và các trình duyệt (browser), khả năng truyền file, sơ đồ định địa chỉ Internet, các bộ lọc bảo vệ. Các dịch vụ này là cần thiết đối với các mạng hiện nay để cho phép giao tiếp và chuyển đổi dữ liệu toàn cầu.

### 1.5.6 Các dịch vụ quản trị (Management services)

Các công việc quản trị mạng trở thành phức tạp hơn đối với các mạng có kích thước lớn, đặc biệt khi nó mở rộng qua các châu lục khác nhau (Các mạng WAN).

Các *dịch vụ quản trị* cho phép những người quản trị mạng quản trị tập trung các mạng lớn và phức tạp. Các công việc quản trị này bao gồm: *theo dõi và điều khiển lưu thông, cân bằng tải, chẩn đoán và cảnh báo các lỗi, quản trị tài nguyên, điều khiển và theo dõi sự cho phép, kiểm tra tính bảo mật, phân bố phần mềm, quản trị địa chỉ, backup và phục hồi dữ liệu.*

## 1.6 Làm thế nào để trở thành một chuyên nghiệp viên về mạng máy tính?

Có nhiều cách để trở thành một người chuyên nghiệp về mạng máy tính. Hoặc được học tập ở các trường đại học, cao đẳng hoặc lấy các bằng cấp thông qua việc học các khoá của các công ty và tham dự các kỳ thi. Một số văn bằng của các công ty bao

gồm: Microsoft Certified Systems Engineer, Novell Network Engineer hoặc các văn bằng của Cisco và Intel.

Một số lĩnh vực chuyên nghành về mạng máy tính là:

- Bảo mật mạng.
- Thiết kế Internet và Intranet.
- Quản trị mạng.
- Tích hợp dữ liệu và tiếng nói.
- Tính toán di dộng và từ xa.
- Tích hợp dữ liệu và cơ chế chống lỗi.
- Kiến thức sâu về các sản phẩm mạng của Microsoft cũng như của Netware.
- Kiến thức sâu về việc cấu hình và quản trị các thiết bị tìm đường (router)

Ngoài những kiến thức kỹ thuật sâu sắc (kỹ năng "cứng"), một người chuyên nghiệp về mạng máy tính cũng cần phải có các kỹ năng "mềm" tốt. Các kỹ năng này bao gồm:

- Kỹ năng quan hệ với khách hàng.
- Kỹ năng giao tiếp bằng lời và bằng văn bản.
- Vừa có khả năng làm việc độc lập vừa có khả năng làm việc tập thể.
- Có khả năng quản lý và lãnh đạo.
- Tính tin cậy cao.

# Câu hỏi ôn tập chương 1

1. Một số các máy tính phân bố trên một vùng địa lý rộng và được kết nối với nhau bằng các cáp và các thiết bị không dây là một ……

a. LAN b. MAN
c. WAN d. Virtual network.

2. Các thành phần cơ bản của kiến trúc mạng là ……(chọn 2)

a. Topology b. Form of the network
c. Protocols d. Physical Media

3. **Hai** mô hình mạng là …….

a. Wire b. Peer to peer
c. Wireless d. Server Based Network

4. Có **hai** loại hình trạng :

a. Physical topology
b. Simple topology
c. Complex topology
d. Logical topology

5. **Một** trong những đặc điểm của mạng LAN:

a. Khoảng cách xa nhất giữa hai trạm lớn hơn 100 km
b. Khoảng cách xa nhất giữa hai trạm vào khoảng vài chục km
c. Cả hai câu trên đều đúng.

6. Lịch sử mạng máy tính cũng chính là lịch sử của Internet

a. Đúng b. Sai

7. Những nhược điểm của mạng server-based là: (chọn 2)

a. Cài đặt phức tạp
b. Bảo mật kém
c. Không có cơ chế sao chép dữ liệu tập trung
d. Chi phí đắt hơn so với mạng peer-to-peer

8. Những nhược điểm của mạng peer to peer là: (chọn 2)

a. Cài đặt phức tạp
b. Bảo mật kém
c. Quản trị phức tạp
d. Không có cơ chế sao chép dữ liệu tập trung

9. Trong mạng peer-to-peer không tồn tại bất kỳ máy server nào.

a. Đúng b. Sai

10. Những dịch vụ thông thường nhất trên mạng là: (chọn 3 )

a. Dịch vụ File b. Dịch vụ Email
c. Dịch vụ thư mục d. Dịch vụ in
e. Dịch vụ chia xẻ

# CHƯƠNG 2 - MÔ HÌNH OSI

## MỤC TIÊU CỦA CHƯƠNG

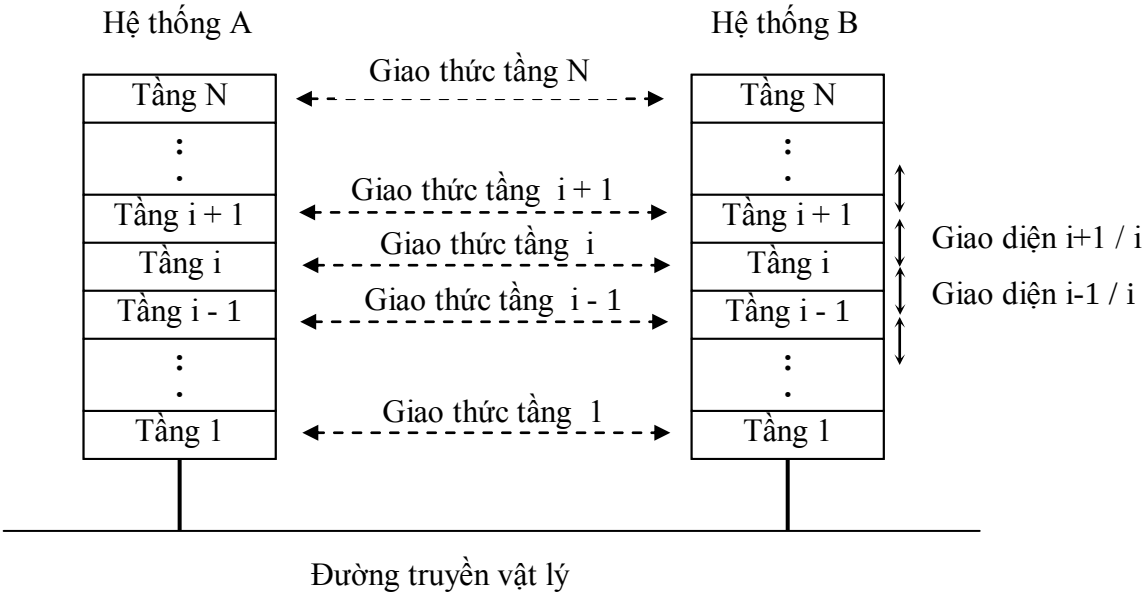
*Kết thúc chương này, sinh viên sẽ có thể:*

- Hiểu một cách khái quát về kiến trúc phân tầng mạng máy tính.
- Nắm được tổng quan về mô hình OSI
- Hiểu và nắm được ý nghĩa cũng như chức năng của các tầng trong mô hình OSI
- Áp dụng mô hình OSI trong việc phân tích một quá trình trong mạng máy tính.
- Hiểu được các thành phần của một khuôn dạng (frame) dữ liệu.

## 2.1 Kiến trúc phân tầng và mô hình OSI (Open System Interconnect)

### 2.1.1 Kiến trúc phân tầng

Để giảm độ phức tạp của việc thiết kế và cài đặt mạng, hầu hết các mạng máy tính hiện có đều được phân tích thiết kế theo quan điểm phân tầng (layering). Mỗi hệ thống thành phần của mạng được xem như một cấu trúc đa tầng, trong đó mỗi tầng được xây trên tầng trước nó. Số lượng các tầng cũng như tên và chức năng của mỗi tầng là tuỳ thuộc vào các nhà thiết kế. Tuy nhiên, trong hầu hết các mạng, mục đích của mỗi tầng là cung cấp một số *dịch vụ* nhất định cho tầng cao hơn. Hình 2.1 là một kiến trúc phân tầng tổng quát, với giả thiết A và B là hai hệ thống máy tính thành phần của mạng được nối với nhau.




*Hình 2.1* Minh hoạ kiến trúc phân tầng tổng quát

*Nguyên tắc của kiến trúc phân tầng là:*

- Mỗi hệ thống trong một mạng đều có cùng cấu trúc tầng (số lượng tầng, chức năng của mỗi tầng là như nhau).
- Sau khi xác định cấu trúc tầng, công việc kế tiếp là định nghĩa mối quan hệ (giao diện) giữa hai tầng kề nhau và mối quan hệ giữa hai tầng đồng mức ở hai hệ thống nối kết với nhau. Nếu một hệ thống mạng có N tầng thì tổng số các quan hệ (giao diện) cần phải xây dựng là 2*N –1.
- Trong thực tế, dữ liệu không được truyền trực tiếp từ tầng thứ i của hệ thống này sang tầng thứ i của hệ thống khác (trừ trường hợp tầng thấp nhất trực tiếp sử dụng đường truyền vật lý để truyền các chuỗi bít (0,1) từ hệ thống này sang hệ thống khác). Qui ước dữ liệu ở bên *hệ thống gửi* (sender) được truyền từ tầng trên xuống tầng dưới và truyền sang *hệ thống nhận* (receiver) bằng đường truyền vật lý và cứ thế đi ngược lên các tầng trên.

### 2.1.2 Tổng quan về mô hình OSI

Khi thiết kế mạng máy tính, các nhà thiết kế tự do lựa chọn kiến trúc riêng của mình. Từ đó dẫn đến tình trạng không tương thích giữa các mạng: phương pháp truy nhập đường truyền khác nhau, sử dụng họ giao thức khác nhau v.v… Sự không tương thích đó làm trở ngại cho sự tương tác của người sử dụng các mạng khác nhau. Nhu cầu trao đổi thông tin càng cao thì trở ngại đó càng lớn, đến mức không thể chấp nhận được đối với người sử dụng. Tình hình đó làm cho các nhà sản xuất và các nhà nghiên cứu, thông qua các tổ chức chuẩn hoá quốc gia và quốc tế cần phải xây dựng được một khung chuẩn về kiến trúc mạng để làm căn cứ cho các nhà thiết kế và chế tạo các sản phẩm về mạng.

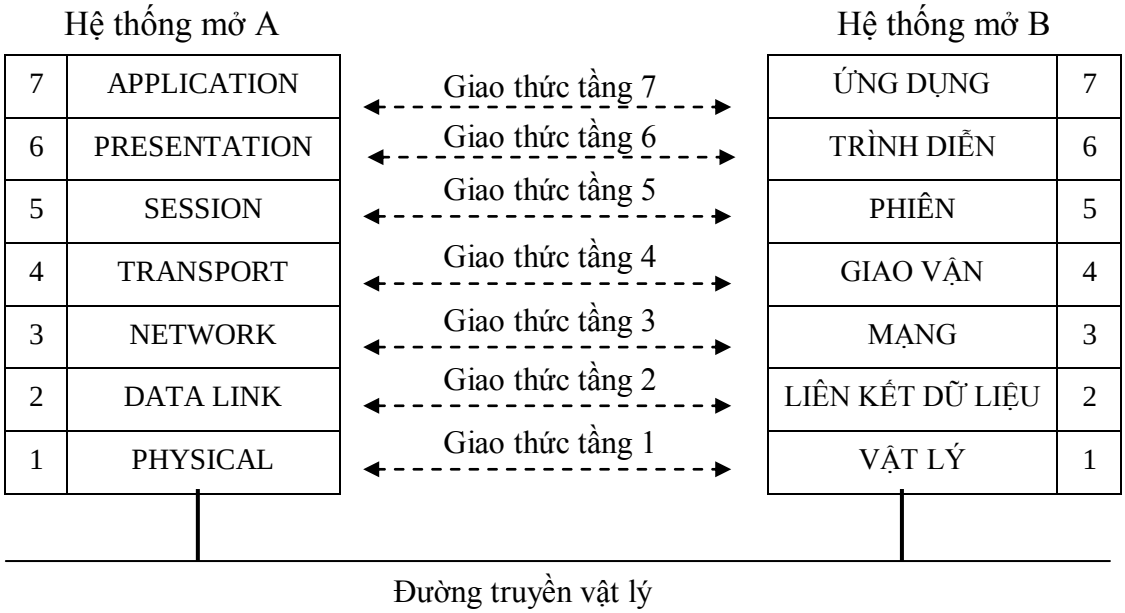
Vì lý do đó, Tổ chức tiêu chuẩn hoá quốc tế (International Organization for Standardization – ISO) đã lập ra một tiểu ban nhằm phát triển một khung chuẩn về kiến trúc mạng. Kết quả là vào năm 1984, mô hình tham chiếu OSI (Open System Interconnection Reference Model) ra đời.

Mô hình OSI là một tập các mô tả chuẩn cho phép các máy tính khác nhau giao tiếp với nhau theo cách *mở*. Từ "mở" ở đây nói lên khả năng 2 hệ thống khác nhau có thể kết nối để trao đổi thông tin với nhau nếu chúng tuân thủ mô hình tham chiếu và các chuẩn liên quan. Mô hình OSI phân chia kiến trúc mạng máy tính thành 7 tầng – tầng *Vật lý* (**Physical**), tầng *Liên kết Dữ liệu* (**Data Link**), tầng *Mạng* (**Network**), tầng *Giao vận* (**Transport**), tầng *Phiên* (**Session**), tầng *Trình diễn* (**Presentation**) và tầng *Ứng dụng* (**Application**). Mỗi tầng khác nhau có tập các chức năng riêng và chỉ giao tiếp với các tầng kề cận trên và dưới và giao tiếp với tầng đối diện (đồng mức) trên các máy tính khác. (Hình 2.2)

Từ khi có mô hình OSI, nhiều nhà sản xuất máy tính đã thay đổi kiến trúc mạng phân tầng của họ để tuân thủ các tầng của mô hình OSI. Ví dụ, các chức năng giao tiếp được phân chia thành một tập các tầng. Mỗi tầng thực hiện các chức năng cần thiết để giao tiếp với các hệ thống khác. Mỗi tầng dựa trên tầng kế tiếp bên dưới để thực hiện nhiều hơn các chức năng nguyên thuỷ (primitive function). Bản thân mỗi

tầng cũng cung cấp các dịch vụ cho tầng kế tiếp phía trên nó. Nói một cách khác tầng *N* sử dụng các dịch vụ của tầng *N-1* và cung cấp các dịch vụ cho tầng *N+1*.

Một cách lý tưởng, các tầng nên được định nghĩa sao cho những thay đổi trong một tầng không đòi hỏi những thay đổi trong các tầng khác. Nói một cách khác, ý tưởng của việc phân tầng là chia một vấn đề lớn thành một số các vấn đề nhỏ có thể quản lý được.




*Hình 2.2* Mô hình OSI 7 tầng

## 2.2 Ý nghĩa và chức năng của các tầng trong mô hình OSI

### 2.2.1 Tầng vật lý (Physical Layer)

Tầng *vật lý* là tầng thấp nhất trong mô hình OSI. Tầng này liên quan đến các qui tắc truyền dòng bit không có cấu trúc qua đường truyền vật lý. Tầng này định nghĩa:

- Cấu trúc mạng vật lý.
- Những mô tả về mặt cơ và điện cho việc sử dụng đường truyền.
- Các qui tắc mã hoá việc truyền các bit và các qui tắc định thời.

Tầng vật lý không bao gồm việc mô tả đường truyền và không cung cấp bất kỳ cơ chế kiểm soát lỗi nào.

Phần cứng kết nối mạng được coi là thuộc về tầng vật lý bao gồm:

- Các bộ giao tiếp mạng (Network Interface Card – NIC, Adapter, v.v…)
- Các bộ tập trung (Concentrator, Hub), các bộ chuyển tiếp (Repeater) dùng để tái sinh các tín hiệu điện.
- Các đầu nối (connector) cung cấp giao tiếp cơ để kết nối các thiết bị với đường truyền (các cáp, các đầu nối BNC – BayoNette Connector)

- Các bộ điều chế và giải điều chế (MODEM – MOdulation-DEModulation) thực hiện việc chuyển đổi giữa tín hiệu *số hoá* (digital) và tín hiệu *tương tự* (analog).

### 2.2.2 Tầng liên kết dữ liệu (Data Link Layer)

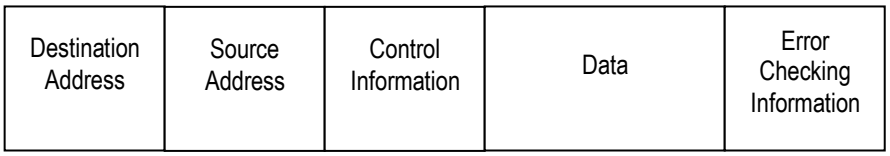
Tầng *liên kết dữ liệu* chịu trách nhiệm điều khiển tất cả các giao tiếp giữa tầng mạng bên trên nó và tầng vật lý bên dưới nó. Dữ liệu nhận được từ tầng mạng được phân chia thành các khối riêng biệt (khuôn dạng - *frame*), sau đó chúng được đưa tới tầng vật lý và cuối cùng truyền ra mạng. Mục đích chính của việc thực thi giao thức tầng liên kết dữ liệu là:

- Tổ chức các bit thuộc tầng vật lý thành các nhóm thông tin được gọi là các *khuôn dạng* (frame - giống như một byte, một frame là một dãy liên tục các bit được nhóm lại với nhau như một đơn vị dữ liệu)
- Phát hiện và sửa sai lỗi.
- Kiểm soát luồng dữ liệu.
- Định danh các máy tính trên mạng .

Tầng liên kết dữ liệu bổ sung thông tin điều khiển riêng của nó vào phía trước gói dữ liệu. Thông tin này bao gồm:

- Địa chỉ (vật lý) của máy nguồn và máy đích (Source address, Destination address) .
- Thông tin về chiều dài của frame.

Một khi dữ liệu được truyền trên mạng, tầng liên kết dữ liệu chờ thông tin phản hồi (Acknowledge –ACK) từ máy tính nhận, báo cho biết là nó đã nhận được tất cả các gói. Trái lại, các gói còn thiếu sẽ được truyền lại. Tầng liên kết dữ liệu không liên quan đến việc tại sao một gói không đến được đích, tầng này chỉ quan tâm đến sự kiện là, nếu một gói nào đó không đến đích thì nó phải được truyền lại. Như vậy tầng liên kết dữ liệu cung cấp các phương tiện đảm bảo sự tin cậy cho việc truyền thông tin.




*Hình 2.3* Một frame dữ liệu được đơn giản hoá

Các thiết bị kết nối mạng được xem như thuộc về tầng liên kết dữ liệu bao gồm:

- Bridges (Các cầu nối)
- Intelligent hubs (các hub thông minh)

Các chức năng của tầng liên kết dữ liệu bình thường được phân tách thành hai tầng con (sub-layer):

1. *Điều khiển truy xuất đường truyền* (Media Access Control - **MAC**)

   Tầng con ***MAC*** là lớp con phía dưới của tầng liên kết dữ liệu. Nó chịu trách nhiệm bổ sung địa chỉ vật lý của máy tính đích vào frame dữ liệu.

2. *Điều khiển liên kết lôgíc* (Logical Link Control – **LLC**)

   Tầng con ***LLC*** là lớp con phía trên của tầng liên kết dữ liệu và chịu trách nhiệm cung cấp một giao tiếp chung cũng như cung cấp tính tin cậy và các dịch vụ kiểm soát luồng dữ liệu. Nó thiết lập và duy trì liên kết cho việc truyền các frame dữ liệu từ thiết bị này tới thiết bị khác.

### 2.2.3 Tầng mạng (Network Layer)

Tầng mạng là tầng thứ ba của mô hình OSI. Mục tiêu chính của nó là *di chuyển dữ liệu tới các vị trí mạng xác định*. Để làm điều này, nó dịch các địa chỉ lôgíc thành địa chỉ vật lý tương ứng và sau đó quyết định con đường tốt nhất cho việc truyền dữ liệu từ máy gửi tới máy nhận. Điều này tương tự như công việc mà tầng liên kết dữ liệu thực hiện thông qua việc định địa chỉ thiết bị vật lý. Tuy nhiên, việc định địa chỉ của tầng liên kết dữ liệu chỉ hoạt động trên một *mạng đơn*. Tầng mạng mô tả các phương pháp di chuyển thông tin giữa *nhiều mạng độc lập* (và thường là không giống nhau) – được gọi là *liên mạng* (internetwork)

Ví dụ, các mạng cục bộ (LAN) Token Ring hoặc Ethernet có các kiểu địa chỉ khác nhau. Để kết nối hai mạng này, ta cần một cơ chế định địa chỉ giống nhau mà có thể được hiểu bởi cả hai loại mạng đó. Khả năng này được cung cấp bởi giao thức *chuyển đổi gói Internet* (Internet Packet Exchange – IPX) – một giao thức tầng mạng trong hệ điều hành Novell Netware.

Việc định địa chỉ của tầng liên kết dữ liệu để chuyển dữ liệu tới tất cả các thiết bị được gắn tới một mạng đơn và nhờ vào các thiết bị nhận để xác định xem dữ liệu có được truyền tới nó hay không. Trái lại, tầng mạng chọn một con đường xác định qua một liên mạng và tránh gửi dữ liệu tới các mạng không liên quan. Mạng thực hiện điều này bằng việc *chuyển mạch* (switching), *định địa chỉ* và các *giải thuật tìm đường*. Tầng mạng cũng chịu trách nhiệm đảm bảo ***định tuyến*** (routing) dữ liệu đúng qua một liên mạng bao gồm các mạng không giống nhau.

Một vấn đề có thể nảy sinh khi việc định tuyến dữ liệu qua một liên mạng không đồng dạng là sự khác nhau của kích thước gói dữ liệu mà mỗi mạng có thể chấp nhận. Một mạng không thể gửi dữ liệu trong các gói có kích thước lớn hơn kích thước của gói dữ liệu mà một mạng khác có thể nhận được. Để giải quyết vấn đề này, tầng mạng thực hiện một công việc được gọi là ***sự phân đoạn*** (segmentation). Với sự phân đoạn, một gói dữ liệu được phân tách thành các *gói* nhỏ hơn mà mạng khác có thể hiểu được - gọi là các ***packet***. Khi các gói nhỏ này đến mạng khác, chúng được ***hợp nhất*** (reassemble) thành gói có kích thước và dạng ban đầu. Toàn bộ sự *phân đoạn* và *hợp nhất* này xảy ra ở tầng mạng của mô hình OSI.

### 2.2.4 Tầng giao vận (Transport Layer)

Tầng giao vận nâng cấp các dịch vụ của tầng mạng. Công việc chính của tầng này là đảm bảo dữ liệu được gửi từ máy nguồn phải *tin cậy, đúng trình tự* và *không có*

*lỗi* khi tới máy đích. Để đảm bảo truyền dữ liệu *tin cậy*, tầng giao vận dựa trên cơ chế *kiểm soát lỗi* được cung cấp bởi các tầng bên dưới. Tầng này là cơ hội cuối cùng để sửa lỗi. Dữ liệu cùng với thông tin điều khiển mà tầng giao vận quản lý gọi là các *phân đoạn* (segment)

Tầng giao vận cũng chịu trách nhiệm *kiểm soát luồng dữ liệu.* Tốc độ truyền dữ liệu được xác định dựa trên khả năng mà máy đích có thể nhận các gói dữ liệu được gửi đến nó như thế nào. Dữ liệu ở máy gửi được phân chia thành các gói có kích thước tối đa mà loại mạng đó có thể quản lý. Chẳng hạn, một mạng Ethernet không thể điều khiển các gói có kích thước lớn hơn 1500 byte, vì thế tầng giao vận nhận dữ liệu và chia nó thành các gói 1500 byte. Mỗi gói con này được gắn một số trình tự, dùng để hợp nhất nó ở vị trí đúng bởi tầng giao vận của máy nhận. Công việc này được gọi là ***sắp xếp theo trình tự*** (sequencing).

Khi gói dữ liệu đến máy nhận, nó được hợp nhất theo đúng trình tự như lúc gửi. Sau đó một thông tin *báo nhận* (acknowledgement - ACK) được gửi quay trở lại máy gửi để báo cho nó biết rằng gói dữ liệu đã đến chính xác. Nếu có lỗi trong gói dữ liệu thì một yêu cầu truyền lại gói đó được gửi quay trở lại thay thế cho ACK. Nếu máy gửi ban đầu không nhận được thông tin ACK (hoặc yêu cầu truyền lại) trong một khoảng thời gian định trước, gói dữ liệu gửi được xem như bị thất lạc hoặc bị hư, khi đó nó sẽ được gửi lại.

Trong mạng TCP/IP, các chức năng TCP (Transmission Control Protocol) thuộc về tầng giao vận. Trong mạng Novell Netware sử dụng IPX/SPX thì giao thức SPX (Sequence Packet Exchange) hoạt động ở tầng giao vận.

### 2.2.5 Tầng phiên (hay Tầng giao dịch - Session Layer)

Tầng phiên quản lý các liên kết của user trên mạng để cung cấp các dịch vụ cho user đó. Ví dụ một người sử dụng đăng nhập vào một máy tính mạng để lấy file thì một phiên (hay một giao dịch / một liên kết) được thiết lập cho mục đích truyền file.

Tầng phiên tạo điều kiện thuận lợi cho việc giao tiếp giữa các hệ thống *yêu cầu* dịch vụ và các hệ thống *cung cấp* dịch vụ. các phiên giao tiếp được kiểm soát thông qua cơ chế *thiết lập, duy trì, đồng bộ hoá* và *quản lý* các phiên (hay còn gọi là cuộc hội thoại – dialogue) giữa các thực thể truyền thông. Tầng này cũng trợ giúp các tầng trên định danh và kết nối tới các dịch vụ có thể sử dụng trên mạng. Nếu một phiên giao tiếp bị ngắt, tầng phiên xác định vị trí để khởi tạo lại việc truyền phát một khi phiên giao tiếp đó được tái kết nối. Tầng phiên cũng chịu trách nhiệm xác định thời hạn của phiên giao tiếp. Nó xác định máy tính hoặc nút nào có thể truyền đầu tiên và truyền trong bao lâu.

Tầng phiên sử dụng thông tin địa chỉ lôgíc được cung cấp bởi các tầng bên dưới để định danh tên và địa chỉ của các máy chủ mà các tầng trên đòi hỏi.

### 2.2.6 Tầng trình diễn (Presentation Layer)

Tầng trình diễn quản lý cách thức dữ liệu được biểu diễn. Nó là trình dịch giữa ứng dụng và mạng. Có nhiều cách để biểu diễn dữ liệu, chẳng hạn như các bảng mã ASCII và EDBCDIC cho các file văn bản. Tầng trình diễn biến đổi dữ liệu sang một

định dạng mà mạng có thể hiểu được. Nó cũng chịu trách nhiệm *mã hoá* (encrypt) và *giải mã* (decrypt) dữ liệu - chẳng hạn như dữ liệu được mã hoá dữ liệu nó được gửi tới ngân hàng, nếu ta giao dịch trực tuyến với ngân hàng qua Internet.

### 2.2.7 Tầng ứng dụng (Application Layer)

Tầng ứng dụng chứa các giao thức và chức năng đòi hỏi bởi ứng dụng của người sử dụng để thực hiện các công việc truyền thông. Nó không liên quan đến các ứng dụng thực sự đang hoạt động như Microsoft Word hoặc Adobe Photoshop.

Các chức năng chung bao gồm:

- Các giao thức cung cấp các dịch vụ file từ xa, như các dịch vụ mở file, đóng file, đọc file, ghi file và chia xẻ truy xuất tới file.
- Các dịch vụ truyền file và truy xuất cơ sở dữ liệu từ xa.
- Các dịch vụ quản lý thông báo cho các ứng dụng thư điện tử.
- Các dịch vụ thư mục toàn cục để định vị tài nguyên trên mạng.
- Một cách quản lý đồng nhất các chương trình giám sát hệ thống và các thiết bị.
- v.v….

Nhiều dịch vụ này được gọi là *các giao tiếp lập trình ứng dụng* (Application Programming Interface – API). Các API là những thư viện lập trình mà người phát triển ứng dụng có thể sử dụng để viết các ứng dụng mạng.

## 2.3 Áp dụng mô hình OSI

Bảng sau đây tổng kết các chức năng của mô hình OSI:

| Tầng | Chức năng |
|---|---|
| Ứng dụng | Chuyển thông tin từ chương trình này tới chương trình khác. |
| Trình diễn | Điều khiển định dạng văn bản và hiển thị chuyển đổi mã. |
| Phiên | Thiết lập, duy trì và kết hợp các phiên truyền thông. |
| Giao vận | Đảm bảo phân phát chính xác dữ liệu. |
| Mạng | Tìm đường và quản lý việc truyền thông báo. |
| Liên kết Dữ liệu | Mã hoá, định địa chỉ và truyền thông tin. |
| Vật lý | Quản lý kết nối phần cứng |

Cách dễ nhất để xem xét mô hình OSI và áp dụng nó trong hoạt động mạng là tìm hiểu một quá trình cụ thể diễn ra trong mạng. Một trong những công việc được thực hiện nhiều lần trong một ngày trên hầu hết các mạng là đọc một thư điện tử (E-mail).

Sau khi người sử dụng đăng nhập vào trong mạng và khởi tạo chương trình e-mail, quá trình kiểm tra thư mới bắt đầu.

Đầu tiên *tầng ứng dụng* xác nhận yêu cầu (request) về thư thông qua một API chuẩn được xây dựng trong ứng dụng. Tầng ứng dụng nhận yêu cầu này và chuyển nó thành một yêu cầu dữ liệu được đọc từ máy chủ e-mail. Yêu cầu được chuyển tới *tầng trình diễn*.

*Tầng trình diễn* nhận yêu cầu và xác định xem nó nên được định dạng như thế nào theo kiểu mạng riêng mà yêu cầu đang hoạt động trên đó. Tầng này cũng xác định xem có bất kỳ đòi hỏi nào về *mã hoá* hay không. Dữ liệu sau khi được định dạng (và có thể được mã hoá) được truyền tới *tầng phiên*.

*Tầng phiên* nhận yêu cầu và gán một thẻ (token) dữ liệu tới nó. Thẻ này là một đơn vị dữ liệu điều khiển đặc biệt mà nó báo cho phần còn lại của mạng là người sử dụng có quyền truyền dữ liệu. Dữ liệu và thẻ được truyền tới *tầng giao vận.*

Khi tới *tầng giao vận,* dữ liệu và các thông tin điều khiển được chia thành các khối có kích thước có thể quản lý được. Nếu dữ liệu quá lớn để thích hợp trong một frame ở *tầng liên kết dữ liệu, tầng giao vận* sẽ phân chia dữ liệu thành các khối nhỏ hơn và gán một *số trình tự* (sequence number) hay *định danh* (identifier) cho mỗi khối. Sau đó từng khối được truyền tới *tầng mạng.*

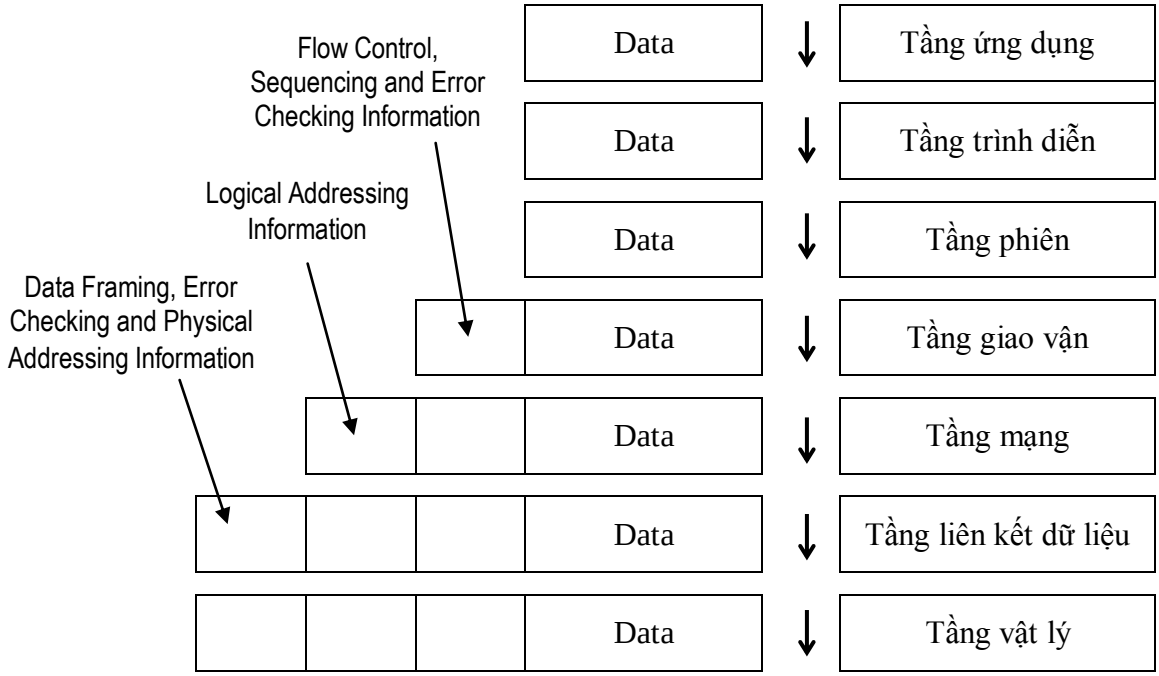
*Tầng mạng* bổ sung thông tin *địa chỉ lôgíc* tới dữ liệu mà nó nhận được từ *tầng giao vận* sao cho các tầng kế tiếp sẽ biết cả địa chỉ nguồn và đích của dữ liệu . Các khối dữ liệu tiếp theo được truyền cùng với thông tin định địa chỉ tới *tầng liên kết dữ liệu*.

Một khi dữ liệu đến được *tầng liên kết dữ liệu,* chúng được đóng gói thành các frame riêng rẽ. Mỗi frame này kèm theo giải thuật kiểm tra lỗi được biết như là **Frame Check Sequence (FCS) -** vùng để ghi mã kiểm soát lỗi – được chèn ở cuối mỗi frame. *Tầng liên kết dữ liệu* sau đó bổ sung thêm một header tới frame trước khi truyền nó tới *tầng vật lý*. Phần header này bao gồm *địa chỉ vật lý* của cả hai nút gửi và nút nhận.

Khi dữ liệu bắt đầu tới card giao tiếp mạng (NIC) ở *tầng vật lý,* nó được gửi ra mạng. *Tầng vật lý* không bổ sung bất kỳ thứ gì tới frame và tầng này cũng không quan tâm xem cái gì có trong frame. Nó đơn giản chỉ lấy dữ liệu (các bit) và truyền nó trên mạng.

Một khi các gói dữ liệu đến được nút nhận, chúng được lấy lại nhờ NIC của *tầng vật lý* bên hệ thống nhận và được truyền tiếp lên qua các tầng hệ thống đó. Mỗi một tầng dịch thông tin được bổ sung bởi các tầng tương ứng bên hệ thống gửi và sau đó truyền gói lên tầng bên trên cho tới khi cuối cùng gói đó được hợp nhất và *yêu cầu* được thực thi.

Nút nhận sau đó tạo ra một *đáp ứng* (response) và gửi nó quay trở lại nút gửi ban đầu đi theo trình tự chính xác như mô tả ở trên. Mỗi tầng kế tiếp của mô hình OSI bổ sung thông tin điều khiển, thông tin định dạng hay thông tin định địa chỉ tới dữ liệu mà nó điều khiển. Hệ thống nhận phiên dịch và sau đó sử dụng thông tin bổ sung khi nó đảo ngược tiến trình, truyền dữ liệu từ *tầng vật lý* lên tới *tầng ứng dụng.*




*Hình 2.4* Dữ liệu được truyền qua mô hình OSI

Bảng sau đây tổng kết đơn vị dữ liệu do các tâng quản lý:

| **Tầng** | **Đơn vị dữ liệu** |
|---|---|
| Tầng ứng dụng, trình diễn, phiên | Data |
| Tầng giao vận | Segment |
| Tầng mạng | Packet |
| Tầng liên kết dữ liệu | Frame |
| Tầng vật lý | Bit |

## 2.4 Mô tả các thành phần của khuôn dữ liệu (Frame)

Như ta đã thấy ở phần trên, dữ liệu khi truyền ngang qua mạng được phân tách thành những khối nhỏ, có kích thước phụ thuộc vào hình trạng lôgíc của mạng đó. Như đối với mạng Ethernet không thể sử dụng các khối dữ liệu lớn hơn 1500 byte. Các khối dữ liệu nhỏ này được gọi là các **frame** (khung hoặc khuôn dạng).

Có hai loại frame: **Ethernet** và **Token Ring** – tương ứng với tên hai loại mạng được sử dụng thông thường nhất.

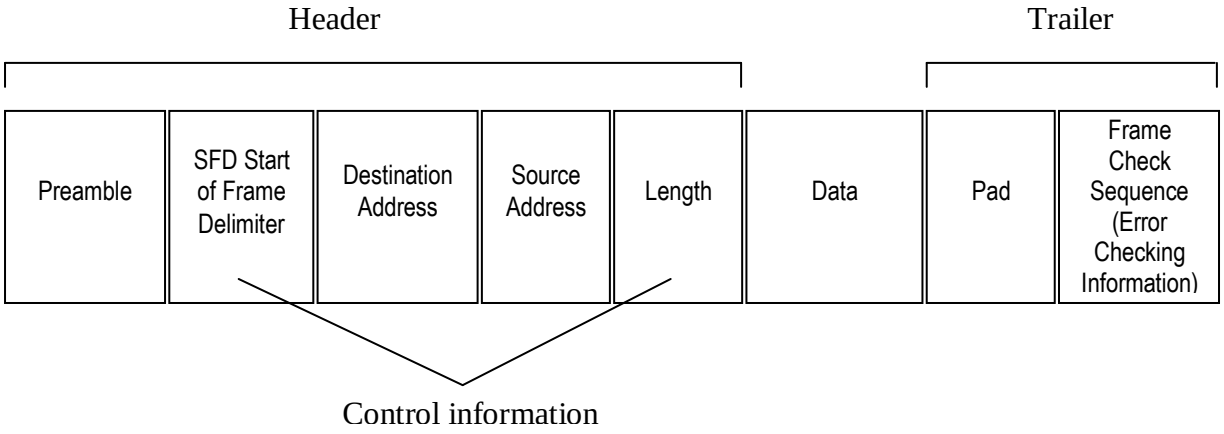
Công ty Xerox Corporation bắt đầu phát triển Ethernet vào năm 1970. Sau đó do liên kết giữa Xerox Corp. với DEC và Intel, Ethernet đã được cải tiến và hiện giờ có 4 công nghệ Ethernet chủ yếu đang được sử dụng – 10Base2, 10Base5, 10BaseT và 100BaseT.

Token Ring đã được phát triển bởi IBM vào năm 1980 và dựa trên liên kết giữa các nút với công nghệ vòng (ring): một thẻ bài (token) được truyền quanh các

nút. Một nút chỉ có thể truyền dữ liệu trên mạng sau khi nó nhận được thẻ bài. Cáp nối mạng hình thành một vòng (ring hoặc circle) và các tín hiệu dữ liệu được truyền chỉ theo một hướng quanh vòng.

Mặc dù về lý thuyết có thể truyền cả hai frame Ethernet và Token Ring trên cùng một mạng, nhưng điều này không thực hiện trong thực tế. Giao tiếp Ethernet không thể phiên dịch các frame Token Ring và trái lại. Một mạng luôn chỉ là Ethernet hoặc Token Ring chứ không thể đồng thời cả hai. Tuy nhiên có thể kết hợp các giao thức trên cùng trên một mạng. Chẳng hạn, có thể sử dụng cả hai bộ giao thức TCP/IP và IPX/SPX trên mạng mạng Ethernet, vì cả hai giao thức này cùng sử dụng một kiểu frame dữ liệu.

### 2.4.1 Một khuôn dữ liệu Ethernet điển hình



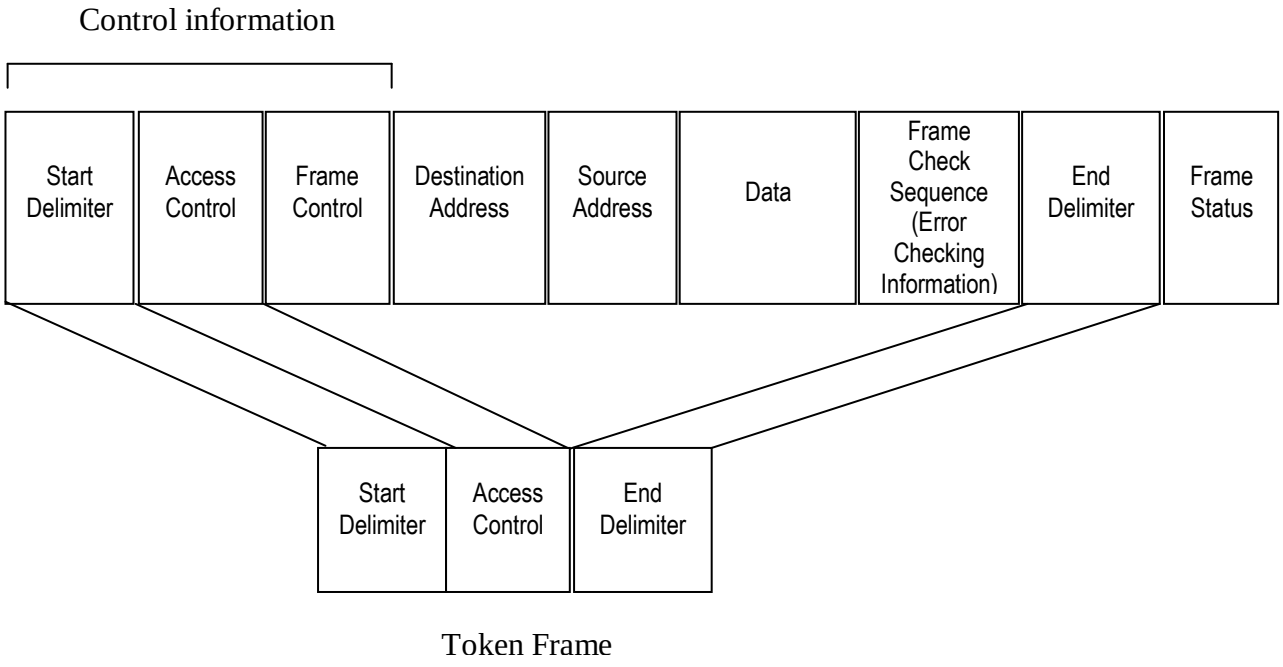

*Hình 2.5* Một khuôn dữ liệu Ethernet điển hình

Các thành phần của frame Ethernet 802.3 bao gồm:

- *Preamble* (Phần mở đầu)– Đánh dấu bắt đầu của toàn bộ frame, là tín hiệu thông báo tới mạng rằng dữ liệu đang truyền. (Vì trường này là một phần của quá trình giao tiếp, nên nó không được tính vào kích thước của frame)
- *Start of Frame Delimiter (SFD)* – Chứa thôngng tin khởi đầu của việc định địa chỉ frame.
- *Destination Address* – Chứa địa chỉ của nút đích.
- *Source Address* – Chứa địa chỉ của nút nguồn.
- *Length (LEN)* – Chứa chiều dài của gói.
- *Data* – Chứa dữ liệu được truyền từ nút nguồn.
- *Pad* – Được sử dụng để tăng kích thước của frame tới kích thước yêu cầu nhỏ nhất là 46 byte.

- *Frame Check Sequence (FCS)* – Cung cấp một giải thuật để xác định xem dữ liệu nhận được có chính xác hay không. Giải thuật được sử dụng thông thường nhất là **Cyclic Redundancy Check (CRC).**

### 2.4.2 Một khuôn dữ liệu Token Ring điển hình




*Hình 2.6* Một khuôn dữ liệu Token Ring điển hình

Các thành phần của frame Token ring 802.5 bao gồm:

- *Start Delimiter (SD)* – Báo hiệu bắt đầu gói. Nó là một trong ba trường tạo thành khuôn dạng Token Ring.
- *Access Control (AC)* – Chứa thông tin về độ ưu tiên của frame. Nó là trường thứ hai tạo thành khuôn dạng Token Ring.
- *Frame Control (FC)* – Định nghĩa kiểu của frame, được dùng trong Frame Check Sequence.
- *Destination Address* – Chứa địa chỉ của nút đích.
- *Source Address* – Chứa địa chỉ của nút nguồn.
- *Data* – Chứa dữ liệu được truyền từ nút nguồn, cũng có thể chứa thông tin quản lý và tìm đường.
- *Frame Check Sequence (FCS)* – Được sử dụng để kiểm tra tính toàn vẹn của frame.
- *End Delimiter (ED)* – Báo hiệu kết thúc frame. Nó là trường thứ ba của khuôn dạng Token Ring.

- *Frame Status (FS)* – Báo hiệu nút đích nhận dạng và sao chép đúng frame hay không.

### 2.4.3 Giới thiệu các chuẩn đặc tả mạng IEEE 802.x

Tổ chức tiêu chuẩn hoá Quốc tế (ISO) chịu trách nhiệm xây dựng mô hình OSI. Chính ISO cũng thông qua một tập các chuẩn được gọi là đề án "Project 802", được dùng để chuẩn hoá các thành phần vật lý của một mạng. Các chuẩn này do Viện Kỹ thuật Điện và Điện tử (Institute of Electrical and Electronic Engineers – IEEE) xây dựng, bao gồm các vấn đề liên quan đến khả năng kết nối, môi trường truyền mạng, các giải thuật kiểm tra lỗi, sự mã hoá và các công nghệ khác.

Bảng sau đây tổng quát hoá các chuẩn trong đề án "Project 802" :

| Chuẩn | Tên | Giải thích |
|---|---|---|
| 802.1 | Internetworking | Bao gồm việc định tuyến, tạo cầu nối, và các giao tiếp liên mạng. |
| 802.2 | Logical Link Control | Liên quan tới việc kiểm soát lỗi và kiểm soát luồng dữ liệu qua các frame. |
| 802.3 | Ethernet LAN | Bao gồm tất cả các dạng đường truyền và giao tiếp Ethernet |
| 802.4 | Token Bus LAN | Bao gồm tất cả các dạng đường truyền và giao tiếp Token Bus |
| 802.5 | Token Ring LAN | Bao gồm tất cả các dạng đường truyền và giao tiếp Token Ring |
| 802.6 | Metropolitan Area Network (MAN) | Bao gồm các công nghệ, định địa chỉ và các dịch vụ MAN |
| 802.7 | Broadband Technical Advisory Group | Bao gồm môi trường truyền, giao tiếp và các thiết bị khác cho mạng băng tần dải rộng. |
| 802.8 | Fibre-Optic Technical Advisory Group | Bao gồm đường truyền cáp quang và các công nghệ cho các loại mạng khác nhau. |
| 802.9 | Integrated Voice / Data Networks | Bao gồm sự tích hợp tiếng nói và dữ liệu qua một đường truyền mạng. |
| 802.10 | Network Security | Bao gồm các vấn đề về kiểm soát truy xuất mạng, sự mã hoá, xác nhận và các vấn đề bảo mật khác. |
| 802.11 | Wireless Networks | Các chuẩn cho mạng không dây. |
| 802.12 | High-Speed Networking | Bao gồm các công nghệ 100Mbs-plus, kể cả 100BaseVG-AnyLAN |

# Câu hỏi ôn tập chương 2

1. Mục tiêu của việc phân tích thiết kế các mạng máy tính theo quan điểm phân tầng là: (chọn 1)
   a. Để dễ dàng cho việc quản trị mạng
   b. Để giảm độ phức tạp của việc thiết kế và cài đặt mạng
   c. Đề nâng cấp hệ thống mạng dễ dàng hơn
   d. Không phải các lý do trên
2. Nếu một hệ thống mạng có 8 tầng thì tổng số các quan hệ (giao diện) cần phải xây dựng là …….
   a. 16 b. 24 c. 15 d. 22
3. Tầng …… của mô hình OSI có thể giao tiếp trực tiếp với tầng đối diện của hệ thống máy tính khác.
   a. Application b. Data link c. Network
   d. Physical. e. Transport
4. Những tầng nào của mô hình OSI cung cấp việc kiểm soát luồng dữ liệu?(chọn 3)
   a. Data-Link b. Transport c. Application
   d. Presentation e. Network
5. Một gói (packet) mạng bao gồm: (chọn 1)
   a. Một header, một body và một trailer
   b. Một địa chỉ của máy gửi và một thông báo
   c. Một chuỗi văn bản với thông tin định dạng
   d. Một URL tương ứng với một địa chỉ www.
6. Đơn vị dữ liệu do tầng Liên kết Dữ liệu quản lý là …….
   a. Bit b. Packet c. Frame d. Segment
7. Một Router làm việc ở tầng nào trong mô hình OSI?
   a. Data-Link b. Transport c. Application
   d. Presentation e. Network
8. Những vấn đề liên quan đến kiểm soát truy xuất mạng, mã hoá, xác nhận và bảo mật mạng thuộc chuẩn nào trong các chuẩn do IEEE 802.X xây dựng?
   a. 802.2 b. 802.3 c. 802.4
   d. 802.5 e. 802.10 f. 802.11
9. Tầng nào của mô hình OSI liên quan đến các dịch vụ hỗ trợ trực tiếp phần mềm truyền file, truy xuất cơ sở dữ liệu và e-mail.

a. Application b. Data link c. Network
d. Physical. e. Transport

10. Một cách tổng quát, dữ liệu có thể truyền trực tiếp từ một tầng của hệ thống gửi sang thẳng tầng đối diện (đồng mức) của hệ thống nhận trong mô hình OSI .
    a. Đúng b. Sai

# CHƯƠNG 3 - ĐƯỜNG TRUYỀN VẬT LÝ

## MỤC TIÊU CỦA CHƯƠNG

*Kết thúc chương này, sinh viên sẽ có thể:*

- Nắm được lý thuyết chung về các loại tín hiệu cũng như các đặc tính cơ bản của đường truyền mạng.
- Có những kiến thức và những thông số cơ bản về các loại cáp mạng.

## 3.1 Truyền dữ liệu: tín hiệu tương tự (analogue) và tín hiệu số hoá (digital)

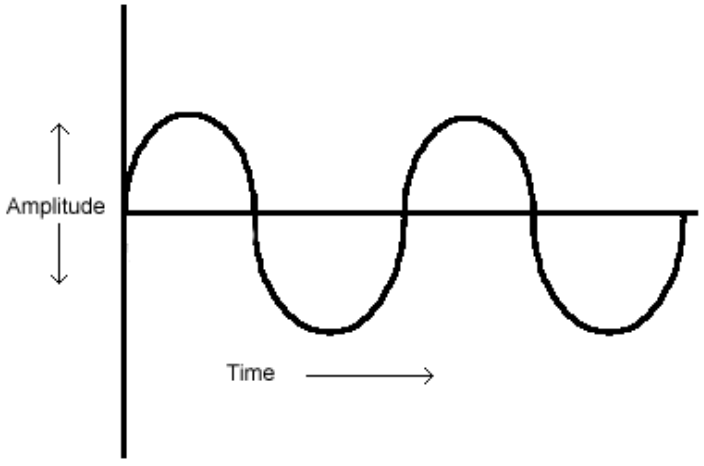
Tín hiệu truyền đi trên mạng hoặc là tương tự (analog), hoặc là số (digital)

### 3.1.1 Tín hiệu tương tự

Tín hiệu tương tự là tín hiệu bao gồm hàng loạt các sóng liên tục do sự biến đổi của điện áp. Nó cũng tương tự như quá trình truyền tín hiệu trên điện thoại. Tín hiệu tương tự không có khả năng loại bỏ nhiễu trên đường truyền trong quá trình truyền dữ liệu, và do đó nhiễu sẽ làm cho qua trình truyền dữ liệu không có tính chính xác cao.

Các đại lượng đặc trưng cho tín hiệu tương tự là: Biên độ và tần số. Đại lượng để đo tần số là Hz.

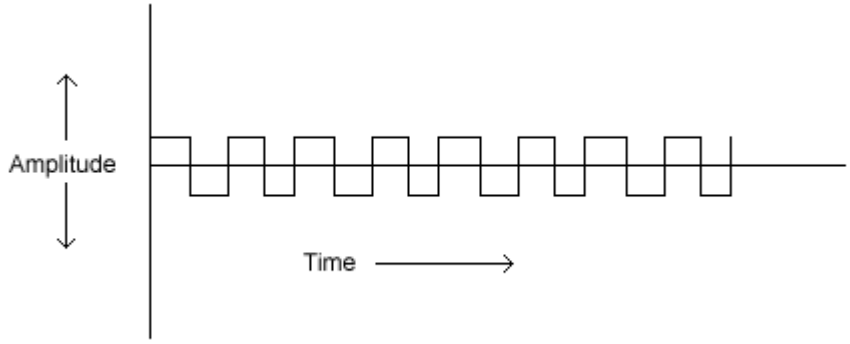
Một trong những vấn đề của tín hiệu tương tự đó là chúng bị *suy giảm*. Biên độ của tín hiệu sẽ tỷ lệ nghịch với khoảng cách mà tín hiệu truyền đi. Khi tín hiệu tương tự đi qua các thiết bị như HUB, hay Repeater thì biên độ của tín hiệu được khuyếch đại, nhưng nhiễu cũng vì vậy mà được khuyếch đại theo (Hình 3.1).




*Hình 3.1* Tín hiệu tương tự

### 3.1.2 Tín hiệu số

Tín hiệu số được tạo thành từ giá trị của các xung điện áp. Nhưng khi chúng đi qua các thiết bị như HUB hay Repeater thì chúng chỉ truyền hay lập lại các tín hiệu nguyên mẫu 1 hay 0 , quá trình này gọi là tái tạo lại. Tín hiệu số ít bị ảnh hưởng của nhiễu do đó có độ tin cậy cao hơn so với tín hiệu tương tự (Hình 3.2).



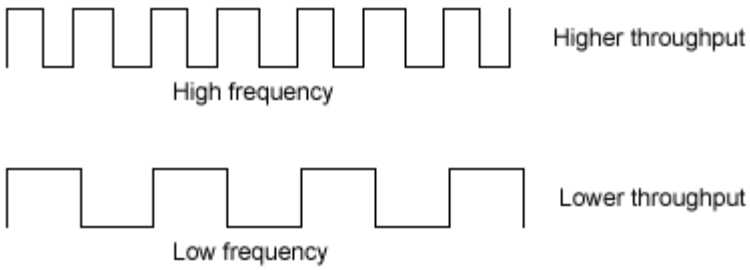

*Hình 3.2* Tín hiệu số

## 3.2 Các đặc tính của đường truyền mạng

Một số vấn đề cần quan tâm khi quyết định môi trường truyền thông trên mạng, bao gồm: dung lượng (throughput), băng thông (bandwidth), chi phí, kích thước, độ linh động, các thiết bị liên kết, và nhiễu.

*Dung lượng* (throughput hay capacity) là lượng dữ liệu đi qua đường truyền trong một đơn vị thời gian. Đơn vị là MegaBits/giây (Mbps). Dung lượng của mạng máy tính phụ thuộc vào khoảng cách địa lý và môi trường đang sử dụng.

*Băng thông* (bandwidth) là đại lượng dùng để đo sự sai biệt giữa tần số lớn nhất và tần số nhỏ nhất của môi trường truyền. Nó liên quan trực tiếp đến dung lượng của đường truyền, nếu một mạng máy tính đang hoạt động ở tần số 870MHz và 880Hz thì băng thông của nó là 10MHz. Thông thường băng thông là lượng dữ liệu thật sự đi qua đường truyền. Đơn vị đo là Hz.




So sánh tín hiệu số tần số cao và tần số thấp

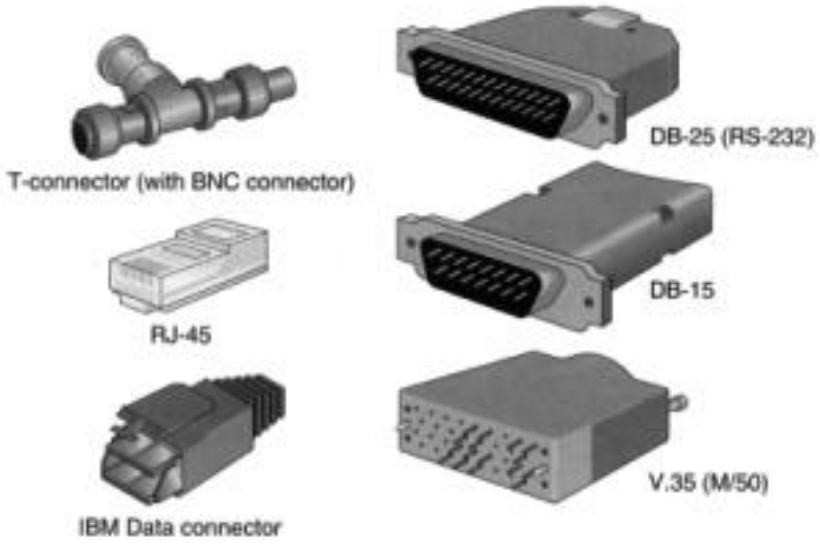
*Chi phí* là một trong các yếu tố quan trọng nó phụ thuộc vào một số các yếu tố như: chi phí cài đặt, chi phí cơ sở hạ tầng, chi phí bảo trì và hỗ trợ v.v...

*Kích thước* và quy mô của môi trường truyền thông mạng máy tính phụ thuộc vào số nút trên mỗi phân đoạn, số phân đoạn và chiều dài của mỗi phân đoạn. Việc chọn lựa cáp nào sẽ ảnh hưởng đến các yếu tố trên.

Số nút trên mỗi phân đoạn càng nhiều sẽ làm suy giảm tín hiệu trên đường truyền. Tín hiệu sau khi đi qua mỗi nút sẽ bị suy giảm và do đó dữ liệu nhận được ở nút sau có thể khác nút trước. Số nút trên mỗi phân đoạn và chiều dài tổng cộng của cả phân đoạn đều phụ thuộc vào dạng cáp đang dùng.

Một yếu tố khác cũng đáng quan tâm đó là *độ trễ* tín hiệu. Độ trễ là thời gian từ lúc tín hiệu được truyền đi cho đến khi nhận được tín hiệu. Ví dụ khi dùng MS Word để xử lý một văn bản được lấy trên server, khi người dùng nhấn Save trên thanh toolbar, thì độ trễ là thời gian được tính từ khi MS Word hiện ra thông báo đi qua mô hình OSI ra card mạng tới cáp, đi qua trường truyền dẫn , qua HUB/SWITCH/ROUTER tới card mạng trên server đi qua mô hình OSI và được chấp nhận bởi server. Lỗi trên đường truyền có thể xảy ra khi thời gian trễ là đủ lớn. Do đó mỗi dạng cáp thường hay qui định số phân đoạn và chiều dài tối đa cho một phân đoạn để tránh lỗi xảy ra.

*Thiết bị liên kết* (Connectors) là các thiết bị dùng để liên kết dây mạng với các nút trên mạng. Các nút này có thể là các trạm làm việc, các máy chủ, các máy in, HUB, Switchs, Routers. Có một số thiết bị như: BNC, T-Connector, RJ45. (Hình 3.3)




*Hình3.3* Một số thiết bị mạng

*Nhiễu điện từ*: bất kỳ hệ thống cáp nào cũng có nhiễu. Nhiễu càng nhiều thì càng ảnh hưởng đến chất lượng đường truyền. Có 2 nguyên nhân chính gây ra nhiễu đó là do điện và do tần số sóng âm thanh.

## 3.3 Các mạng LAN: Baseband và Broadband

Các mạng cục bộ chia làm hai loại: Mạng cục bộ băng thông cơ sở và mạng cục bộ băng thông rộng (Baseband và Broadband LAN).

a. *Mạng cục bộ băng thông cơ sở:* (Baseband LAN) là dạng mạng LAN chỉ cho phép truyền một dạng tín hiệu trên đường truyền hay nói khác đi chỉ có một kênh truyền ( tần số ) duy nhất hỗ trợ truyền số do đó nhanh hơn rất nhiều so với kỹ thuật truyền tín hiệu tương tự.

**Baseband Cable**

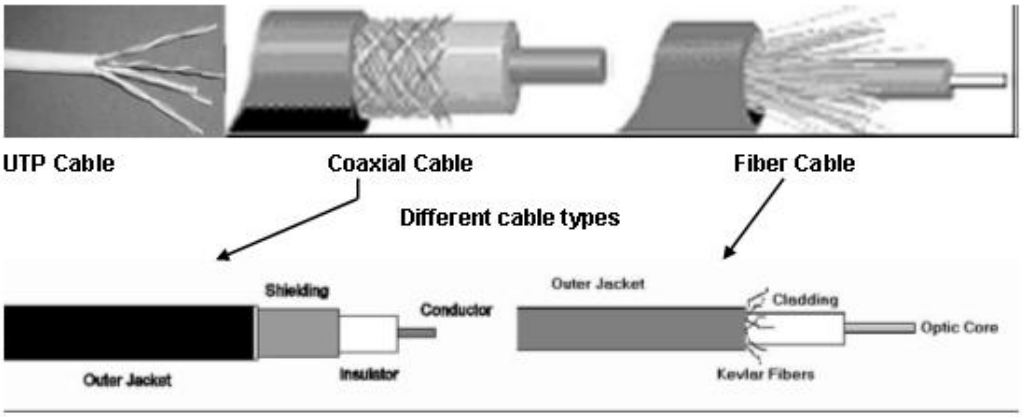
b. *Mạng cục bộ băng thông rộng*: (Broadband LAN) thông thường mạng cục bộ không thuộc loại này. Mạng cục bộ băng thông rộng thường sữ dụng cáp xoắn hay cáp cáp quang để tạo ra nhiều kênh truyền dữ liệu.

**Broadband Cable**

Ứng với mỗi kênh truyền sẽ có một tần số sóng khác nhau, nó sử dụng sóng âm thanh, tín hiệu truyền đi là tương tự do đó có thể xử lý các tín hiệu với các tần số khác nhau. Với băng thông rộng đường truyền được chia thành dãy tần số, mỗi tần số ứng với một loại dữ liệu , theo cách này thì các tính hiệu như âm thanh, hình ảnh. có thể truyền cùng một lúc. Mạng băng thông rộng thích hợp cho các bệnhviện và các viện đại học.

## 3.4 Các loại cáp mạng

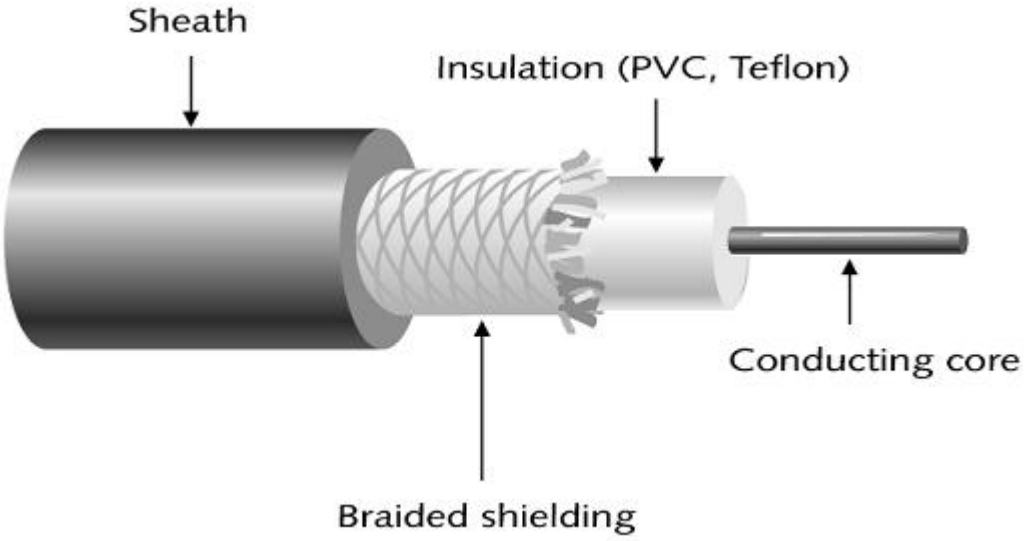
Các phương tiện nối mạng được chia làm hai nhóm: có quy định giới hạn và không quy định giới hạn . Phương tiên có quy định giới hạn thường là cáp, và các phương tiện không qui định là: sóng vô tuyến, laser, viba và tia hồng ngoại. Hệ thống cáp chia ra làm ba loại : *cáp đồng trục* (Coaxial), *cáp xoắn đôi* (twisted-pair) và *cáp sợi quang* (optical fiber)




**Transmission Media Connectors**

### 3.4.1 Cáp đồng trục (Coaxial cable)

Là loại cáp xuất hiện đầu tiên, gồm hai dây dẫn: một lõi bên trong và một lớp bọc ngoài. (Hình 3.4)




*Hình3.4* Cáp đồng trục

Cáp đồng trục chia ra làm hai loại

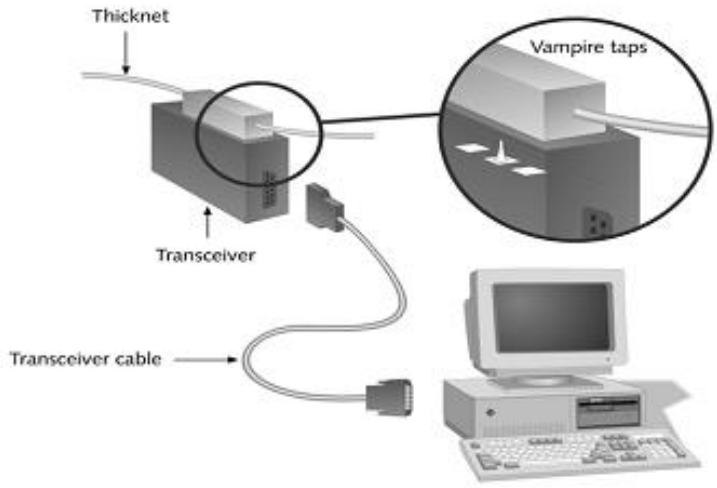
- Cáp đồng trục dày (Thick cable) - 10BASE-5
- Cáp đồng trục mảnh (Thin Cable) - 10BASE-2

Một số thông số kỹ thuật về 2 loại cáp này:

| **Cáp đồng trục mảnh (10BASE-2)** | **Giá trị** |
|---|---|
| Tốc độ truyền dữ liệu ( Max) | 10 Mbps |
| Số repeaters (Max) | 4 |
| Chiều dài tối đa cho 1 phân đoạn | 185 meters |
| Số trạm tối đa trên 1 phân đoạn | 30 |
| Số trạm tối đa | 90 |
| Khảng cách tối thiểu giữa hai trạm | 0.5m |

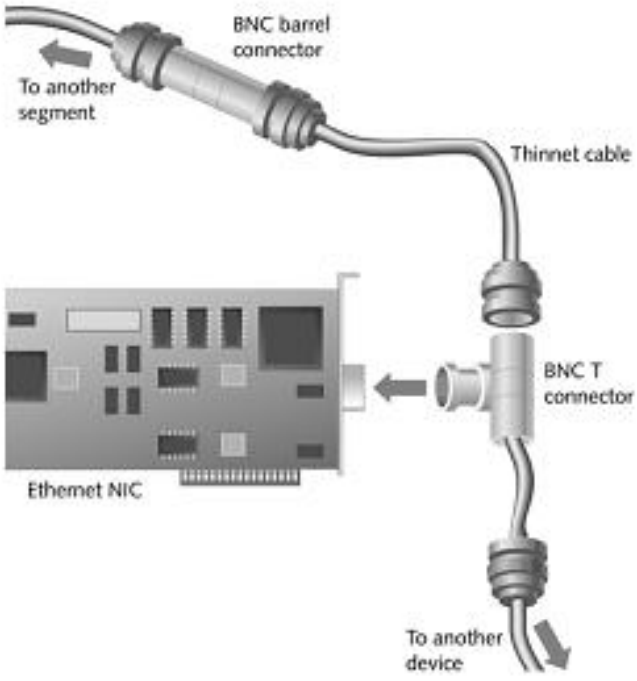
| **Cáp đồng trục dày ( 10BASE-5)** | **Giá trị** |
|---|---|
| Tốc độ truyền dữ liệu ( Max) | 10 Mbps |
| Số repeaters (Max) | 4 |
| Chiều dài tối đa cho 1 phân đoạn | 500 meters |
| Số trạm tối đa trên 1 phân đoạn | 50 |
| Số trạm tối đa | 300 |
| Khảng cách tối thiểu giữa hai trạm | Multiples of 2.5m |

Cáp đồng trục dày (RG-62) thường được dùng trong một mạng máy tính nó tạo thành các đường xương sống (backbone) trong hệ thống mạng (Hình 3.5)




*Hình 3.5* Sơ đồ mạng dùng cáp đồng trục dày

Cáp đồng trục mảnh (RG-58A/U) thường dùng để nối các trạm làm việc trên một mạng cục bộ (Hình 3.6).




*Hình 3.6* Sơ đồ mạng dùng cáp đồng trục mảnh

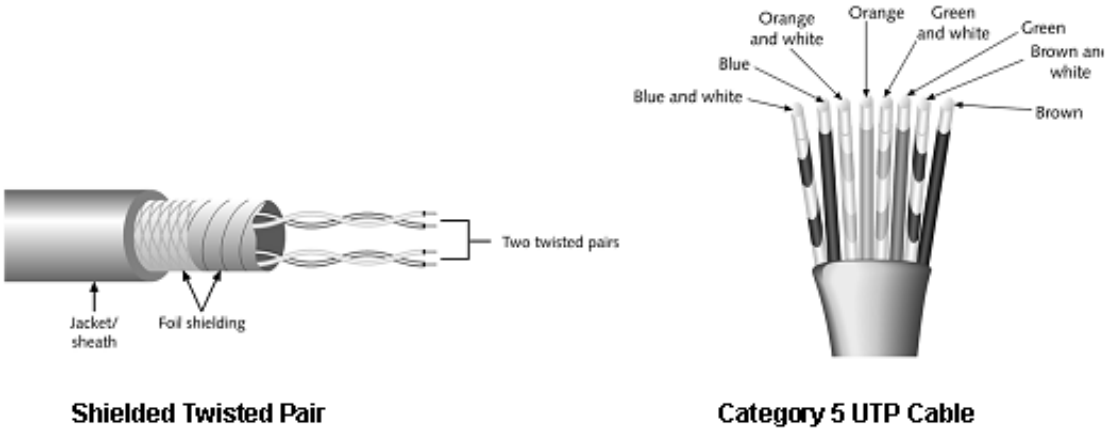
Cáp đồng trục **c**ó các tính chất sau:

- Bị ảnh hưởng của nhiễu bên ngoài và phải được bọc để làm giảm độ nhiễu ảnh hưởng đó.
- Khi khoảng cách mạng lớn, nó có thể thu lấy các nhiễu tạp âm và nhiễu từ xe cộ và các nguồn điện khác.
- Phát ra các tín hiệu khác.

### 3.4.2 Cáp xoắn đôi (Twisted Pair cable)

Có hai loại cáp xoắn đôi:

- Có bọc ngoài (Shielded Twisted Pair cable - STP)
- Không bọc ngoài (Unshielded Twisted Pair cable - STP). Riêng loại cáp dùng cho mạng Ethernet là loại cáp xoắn đôi không bọc ngoài hay còn gọi là cáp UTP (Hình 3.7).



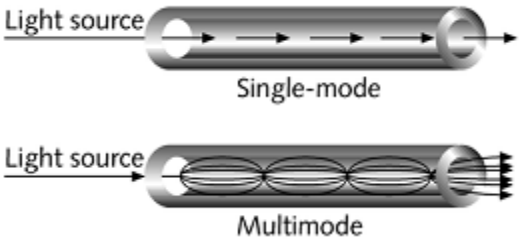

*Hình 3.7* Cáp xoắn đôi

Ngoài ra cáp UTP loại 5 còn gọi là cáp 10BASE-T

Cáp xoắn đôi có các tính chất sau

- Là hệ thống cáp kinh tế nhất
- Có thể dùng những đường cáp điện thoại có sẵn trong một số trường hợp
- Có chiều dài hạn chế
- Có thể bị ảnh hưởng bởi nhiễu bên ngoài

### 3.4.3 Cáp quang (Fibre-Optic cable)




Một số đặc điểm cơ bản của cáp sợi quang:

- Có nhiều kích cỡ khác nhau và chúng chuyển tải ánh sáng chớ không phải điện.
- Thường được dùng kết hợp với những loại cáp khác như là một đường nối kiểu xương sống giữa các server và các LAN

- Có ưu thế lớn về chiều dài cáp và tốc độ truyền nhanh hơn hẳn các loại cáp khác
- Không phát ra tín hiệu
- Không bị ảnh hưởng của nhiễu bên ngoài

Các thông số kỹ thuật của hệ thống cáp rất quan trọng, có thể kiểm tra theo 5 tính chất sau: Chiều dài - Hệ số suy giảm - Nhiễu chen ngang đầu cáp - Tạp nhiễu - Độ thất thoát

- **Việc nối cáp**

Việc chọn loại cáp là một điều quan trọng khi lắp đặt một mạng. Trong các loại cáp thì cáp quang là loại cáp an toàn nhất nhưng giá thành rất cao.

Bảng so sánh các tính năng của cáp

| Yếu tố so sánh | Cáp UTP | Cáp đồng trục | Cáp quang |
|---|---|---|---|
| Giá cả | Thấp | Trung bình | Cao |
| Băng Thông | Trung bình | Cao | Cực kỳ cao |
| Chiều dài | Hàng trăm feet | Hàng ngìn feet | Hàng dặm |
| Nhiễu | Khá nhiều | Thấp | Không có |
| Độ tin cậy | Cao | Cao | Rất cao |

- **Các thành phần của một mạng sử dụng cáp đồng trục 10BASE-2**

-Card giao tiếp 10BASE-2 : hầu hết tất cả đều hỗ trợ hệ thống cáp này. Card cho loại này phải có một đầu nối loại BNC để nối vào dường cáp chính . Trên đường cáp chính có gắn một đầu nối T-Connector để gắn vào một đầu nối BNC ở phía sau card . Nếu máy không có đĩa cứng thì phải gắn thêm một Boot ROM.

- Bộ tiếp sức (Repeater): là một thiết bị chọn thêm, dùng để nối 2 đoạn cáp chính và làm tăng tín hiệu truyền qua lại giữa chúng.
- Cáp: là loại cáp đồng trục có điện trở là 50 Ohm đường kính 0.2 inch
- Các đầu nối cáp kiểu BNC: được gắn vào hai đầu của khúc cáp
- Các đầu nối T-Connector kiểu BNC dùng để đưa tính hiệu vào và ra
- Các đầu nối thanh ngang kiểu BNC được dùng để nối hai khúc cáp lại với nhau
- Các Terminal gắn ở hai đầu cuối của đoạn mạng, có điện trở là 50 Ohm

Khi nối mạng bằng loại cáp này, phải tuân theo các quy tắc và hạn chế sau:

- Chiều dài của mỗi đoạn cáp chính tối đa là khoảng 185 mét
- Dùng các T-Connector để nối cáp với card mạng
- Chỉ dùng tối đa 4 repeater để nối kết 5 đoạn cáp mạng chính, trong đó chỉ có 3 đoạn là được dùng để nối với trạm làm việc, 2 đoạn còn lại chỉ dùng để nối đến những khoảng cách ở xa.
- Chiều dài tối đa của toàn mạng là 910 mét
- Tối đa có 30 nút trên mỗi đoạn mạng, các nút ở đây bào gồm: máy tính, server, repeater, router.

- **Các thành phần của một mạng khi dùng cáp xoắn đôi (10BASE-T hay là UTP)**

Các trạm làm việc được nối vào một HUB, có tác dụng làm khuyếch đại tín hiệu từ server tới và phát đi tiếp tới các máy khác trên mạng

** Các thành phần của một mạng dùng cáp UTP*

- Card giao tiếp mạng 10BASE-T
- Hub
- Cáp UTP

# Câu hỏi ôn tập chương 3

1. Công nghệ cáp đồng trục ..... hỗ trợ nhiều kênh, mỗi kênh chiếm khoảng 6 MHz.

a. Thick b. Baseband

c. Broadband d. Thin

2. Điều nào là không đúng khi nói về cáp sợi quang trong các điều sau?

a. It has a lower noise level

b. Light signals do not attenuate as quickly as electric signals

c. Light propagates more quickly through glass than electric signals

d. It is easy to wiretap

3. Việc tăng tốc độ truyền có thể tăng ảnh hưởng của nhiễu và vì vậy giá trị của tín hiệu.

a. Đúng b. Sai

3. Loại mội trường truyền nào trong các loại sau không phải là mội trường trường định hướng?

a. Twisted pair wire b. Coaxial cable

c. Fiber optic cable d. Microwave

4. Kỹ thuật chuyển từ dữ liệu số hoá sang tín hiệu tương tự gọi là .....

a. Manchester encoding b. Modulation

c. Multiplying d. Negotiation

5. Bạn chịu trách nhiệm bảo trì máy tính Microsoft Windows 2000 Server trên mạng công ty của mình. Card mạng trong server hiện thời được kết nối tới mạng. Bạn thấy có một đầu nối 15 chân ở phía sau của card giao tiếp mạng (NIC) đang nối tới một transceiver bên ngoài. Loại cáp nào được sử dụng cho kết nối mạng?

a. ThinNet coaxial (10Base2) b. ThickNet coaxial (10Base5)

c. Twisted-pair (10BaseT) cable d. Fiber-optic cable

6. Những loại cáp nào thuộc về công nghệ Ethernet 10 Mbps? (Chọn tất cả các câu trả lời đúng)

a. 10Base2 b. 10Base10 c. 10BaseTL

d. 10BaseUT e. 10BaseFL f. 10Base5

7. Hai loại cáp nào được sử dụng với đầu nối BNC connector và các thành phần terminator?

a. 10Base2 b. 10Base10

c. Thinnet d. 10BaseUT

# CHƯƠNG 4 - CÁC GIAO THỨC MẠNG (PROTOCOLS)

## MỤC TIÊU CỦA CHƯƠNG

*Kết thúc chương này, sinh viên sẽ có thể:*

- Hiểu được khái quát khái niệm giao thức mạng máy tính.
- Đặc điểm và nội dung các giao thức con của các bộ giao thức thông thường đang sử dụng: TCP/IP, IPX/SPX, MicroSoft Network. Có so sánh chúng với mô hình OSI.

## 4.1 Giao thức (protocol) mạng là gì?

*Tập hợp tất cả các quy tắc, quy ước để đảm bảo cho các máy tính trên mạng có thể giao tiếp với nhau gọi là giao thức*. Như vậy các máy trên mạng muốn giao tiếp với nhau thì phải có chung một giao thức.

Vai trò của giao thức là quan trọng, không thể thiếu.

Ví dụ một số giao thức như: TCP/IP, SPX/IPX, v.v...

Các dạng liên kết:

- Giao thức hướng kết nối và giao thức không kết nối (Connectionless & Connection- Oriented protocols)
- Giao thức có khả năng định tuyến và giao thức không có khả năng định tuyến (Routable & non - Routable protocols)

### 4.1.1 Giao thức hướng kết nối và giao thức không kết nối

- Đặc điểm của giao thức không kết nối:
  a. Không kiểm soát đường truyền
  b. Dữ liệu không bảo đảm đến được nơi nhận
  c. Dữ liệu thường dưới dạng datagrams

  Ví dụ: giao thức UDP của TCP/IP
- Đặc điểm của giao thức hướng kết nối:
  a. Ngược lại với giao thức không kết nối , kiểm soát được đường truyền
  b. Dữ liệu truyền đi tuần tự, nếu nhận thành công thì nơi nhận phải gởi tín hiệu ACK (ACKnowledge)

  Ví dụ: các giao thức TCP, SPX

### 4.1.2 Giao thức có khả năng định tuyến và giao thức không có khả năng định tuyến

- Giao thức có khả năng định tuyến

Là các giao thức cho phép đi qua các thiết bị liên mạng như Router để xây dựng các mạng lớn có qui mô lớn hơn

Ví dụ, các giao thức có khả năng định tuyến là: TCP/IP, SPX/IPX

- Giao thức không có khả năng định tuyến

Ngược với giao thức có khả năng định tuyến, các giao thức này không cho phép đi qua các thiết bị liên mạng như Router để xây dựng các mạng lớn.

Ví dụ về giao thức không có khả năng định tuyến là : NETBEUI

Hiện có 3 loại giao thức thường hay sử dụng:

- TCP/IP
- SPX/IPX (Novell Netware)
- Microsoft Network

## 4.2 Bộ giao thức TCP/IP (Transmission Control Protocol / Internet Protocol)

TCP/IP được thiết kế hoàn toàn độc lập với các phương pháp truy cập mạng, cấu trúc gói dữ liệu (data frame), môi trường truyền, do đó mà TCP/IP có thể dùng để liên kết các dạng mạng khác nhau như mạng LAN Ethernet, LAN Token Ring hay các dạng WAN như: Frame Relay, X.25

Hình 4.1 so sánh bộ giao thức TCP/IP với mô hình OSI.

TCP/IP là một lớp các giao thức ( protocol stack) bao gồm các giao thức sau:

### 4.2.1 FTP (File Transfer Protocol).

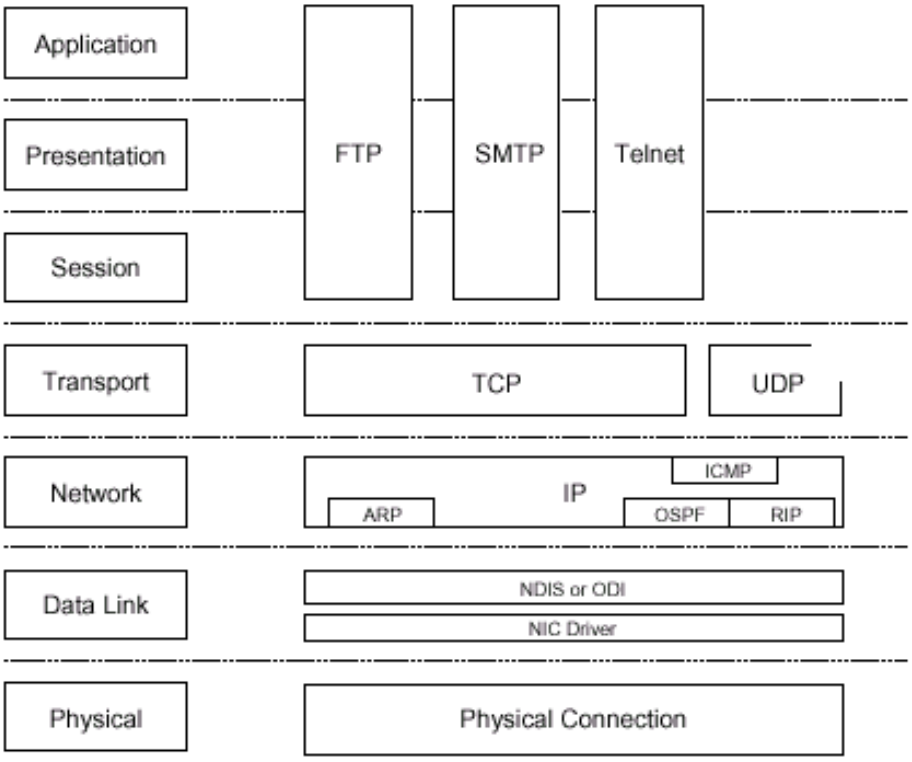
FTP cung cấp phương pháp truyền nhận file giữa các máy với nhau, nó cho phép người sử dụng có thể gởi một hay nhiều file từ máy mình lên hệ thống bất kỳ (upload) và nhận một hay nhiều file từ một hệ thống bất kỳ về máy mình (download)

### 4.2.2 Telnet

Với Telnet, người sử dụng có thể kết nối vào các hệ thống ở xa thông qua mạng Internet.

### 4.2.3 SMTP (Simple Mail Transfer protocol)

Là giao thức cho phép thực hiện dịch vụ truyền nhận mail trên mạng Internet.




*Hình 4.1* So sánh giao thức TCP/IP với mô hình OSI

### 4.2.4 TCP và UDP

Hai giao thức này đóng vai trò của tầng transport, có trách nhiệm tạo liên kết và dịch vụ kết nối dữ liệu (datagram communication service)

- TCP (Transmission Control Protocol) là giao thức chuyển giao chính trong TCP/IP. TCP cung cấp một đường truyền có độ tin cậy cao, là liên kết có định hướng (connection oriented protocol), khôi phục các gói dữ liệu bị mất trong qúa trình truyền. Quá trình truyền dữ liệu theo TCP là các byte, gói dữ liệu TCP bao gồm các thông tin sau

| **Thông tin** | **Chức năng** |
|---|---|
| Source Port | Thông tin về địa chỉ cổng (port) của máy gởi |
| Destination port | Thông tin về port của máy nhận |
| Chỉ số thứ tự | Chỉ số thứ tự tính từ byte đầu tiên trong dữ liệu TCP |
| ACK | Chỉ số byte mà người gởi nhận được từ người nhận |
| Window | Bộ đệm dữ liệu cho TCP |
| TCP Checksum | Xác định tính toàn vẹn dữ liệu trong TCP header và TCP data |

Một số port TCP thông dụng

| Số port | Dịch vụ |
|---|---|
| 20 | FTP ( Data) |
| 21 | FTP (Control) |
| 23 | Telnet |
| 80 | HTTP |
| 139 | NETBIOS |

- UDP (User Datagram protocol) là loại liên kết một một hay một nhiều, không định hướng (Connectionless), không có độ tin cậy cao, thường hay dùng khi dung lượng dữ liệu truyền tải trên mạng là nhỏ. Các thông tin trong UDP header bao gồm:

| Thông tin | Chức năng |
|---|---|
| Source Port | Thông tin về port của máy gởi |
| Destination port | Thông tin về port của máy nhận |
| TCP Checksum | Xác định tính toàn vẹn dữ liệu trong TCP header và TCP data |

Một số port UDP thông dụng:

| Số port | Dịch vụ |
|---|---|
| 53 | Domain name system |
| 137 | NETBIOS NAME |
| 138 | NETBIOS Datagram |
| 161 | SNMP |

### 4.2.5 Các giao thức IP, ARP, ICMP, RIP.

Đóng vai trò của tầng Internet có chức năng tìm đường (routing), nhận dạng địa chỉ (addressing), đóng gói (package)

- IP (Internet protocol) là dạng giao thức cho phép tìm đường (routable protocol), nhận dạng địa chỉ (addressing), phân tích và đóng gói. Một gói IP bao gồm IP header và IP payload, trong đó IP header bao gồm các thông tin sau:

| IP Header | Chức năng |
|---|---|
| Địa chỉ IP gởi | Thông tin về địa chỉ IP của máy gởi |
| Địa chỉ IP nhận | Thông tin về địa chỉ IP của máy nhận |
| Identification | Nhận dạng các mạng con nếu có trong địa chỉ IP |
| Checksum | Xác định tính toàn vẹn dữ liệu trong phần IP header |

- ARP (Address Resolution Protocol) có chức năng phân giải một địa chỉ IP thành một địa chỉ giao tiếp trên mạng.

- ICMP (Internet Control Message Protocol) có chức năng thông báo lại các lỗi xảy ra trong qua trình truyền dữ liệu.

### 4.2.6 NDIS (Network Driver Interface Specification) và ODI (Open Data Interface)

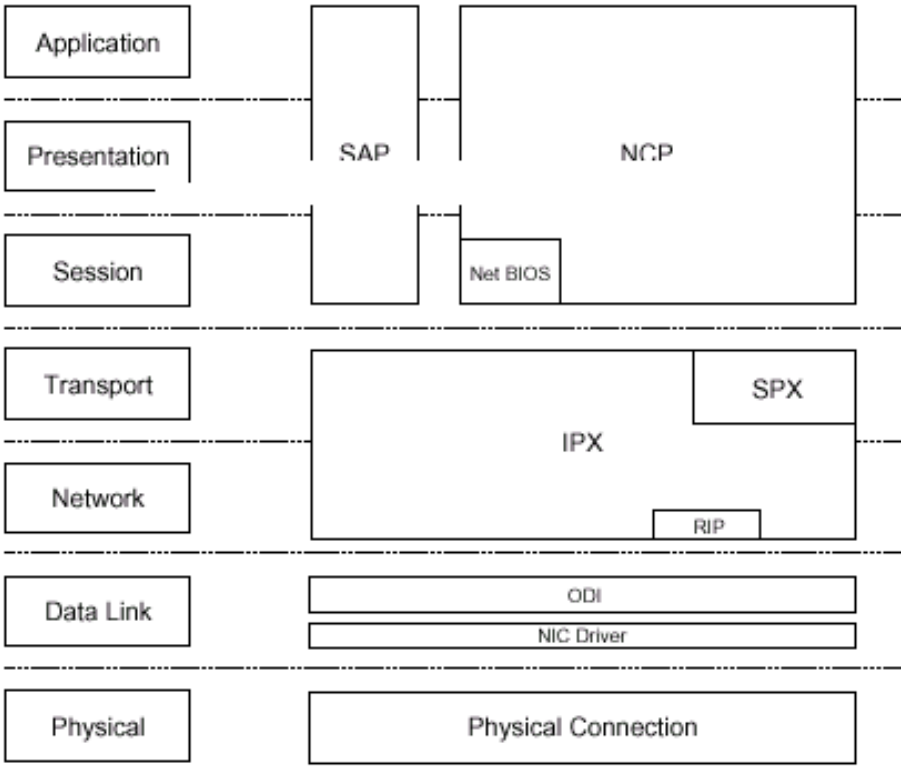
Hai giao thức này đóng vai trò của tầng DataLink, cho phép một card giao tiếp (interface card) có thể giao tiếp với nhiều giao thức khác nhau trên mạng.

- ODI được phát triển bởi Novell và Apple, ban đầu ODI driver được viết cho Novell và Macintosh

- NDIS được phát triển bởi Microsoft và 3 COM có các phiên bản như NDIS, NDIS2 và NDIS3. Các phiên bản cũ dùng cho Windows for workgroup, NT 3.5, còn các phiên bản mới dùng cho WinNT 4.0 hay Windows 2000.

## 4.3 Bộ giao thức IPX/SPX (Internetwork Packet Exchange / Sequenced Packet Exchange )

So sánh IPX/SPX với mô hình OSI (Hình 4.2)




*Hình 4.2* So sánh giao thức IPX/SPX với mô hình OSI

Cũng giống như TCP/IP, IPX/SPX là một lớp giao thức bao gồm các giao thức sau:

### 4.3.1 SAP (Service Advertising Protocol)

Là giao thức dùng để quảng cáo địa chỉ của server và các dịch vụ khác trên mạng như File servers và Print server dùng SAP.

### 4.3.2 NCP (Netware Core Protocol)

Xử lý quá trình tương tác giữa client và server, ví dụ như việc chia xẻ các tài nguyên trên mạng.

### 4.3.3 SPX (Sequenced Packet Exchange )

Cung cấp liên kết định hướng (connection oriented protocol) trên IPX.

### 4.3.4 RIP (Routing information Protocol)

Là giao thức tìm ra đường đi tốt nhất cho các gói dữ liệu.

### 4.3.5 IPX (Internetwork Packet Exchange)

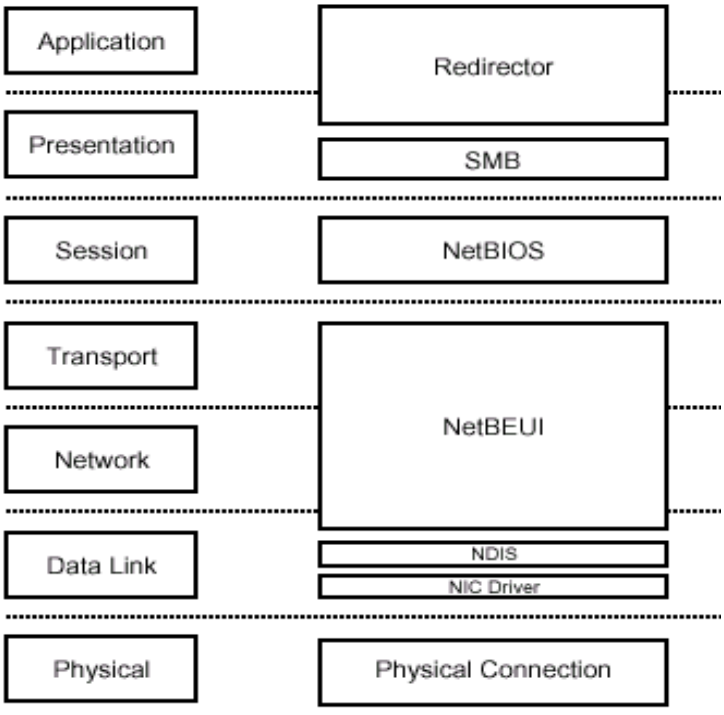
Là giao thức không định hướng, dùng để xác định địa chỉ mạng và tìm đường trên mạng IPX/SPX, IPX cung cấp dịch vụ về datagram.

### 4.3.6 ODI (Open Data Interface)

Giao thức này đóng vai trò của tầng DataLink, cho phép một card giao tiếp có thể giao tiếp với nhiều giao thức khác nhau trên mạng. ODI được phát triển bởi Novell và Apple, do đó ban đầu ODI driver được viết cho Novell và Macintosh

## 4.4 Bộ giao thức Microsoft Network ( NETBIOS, NETBEUI, SMB)

Microsoft Networking là sự kết hợp của IBM & Microsoft, nó là lớp các giao thức, so sánh với mô hình OSI ( Hình 4.3 )




*Hình 4.3* So sánh giao thức Microsoft Networking với mô hình OSI

NetBIOS : Network Basic Input Output System

NetBEUI : Network Extended User Interface

Microsoft Network bao gồm các giao thức sau:

### 4.4.1 Redirector

Giao thức này có tác dụng:

- Làm cho tài nguyên trên mạng trở thành cục bộ.
- Trực tiếp truy xuất tới tài nguyên trên các server tương ứng

### 4.4.2 SMB

Có chức năng tương tự như tầng biểu diễn, cung cấp liên kết ngang hàng giữa client và server, cho phép thành lập các mạng ngang hàng.

### 4.4.3 NetBIOS

Giao thức này dùng để thành lập phiên làm việc giữa các máy tính. Nó có các đặc điểm sau:

- Hoạt động tại tầng Session.
- Dùng tên có 15 ký tự để tự nhận dạng.
- Thành lập liên kết giữa 2 máy để truyền dữ liệu
- Cho phép liên kết không định hướng
- Dùng broadcast để định dạng các máy tính trên mạng.

Cơ chế hoạt động của NetBIOS bao gồm 4 phần :

- NetBIOS Interface
- NetBIOS Management
- NetBIOS Datagram
- NetBIOS Session

❖ NetBIOS Interface

Bao gồm các hàm API chuẩn cho phép các ứng dụng có thể gởi hay nhận thông tin từ server. NetBIOS Interface còn thực hiện chức năng NetBIOS trên TCP/IP.

❖ NetBIOS Management

Bao gồm những chức năng sau

. Đăng ký và hủy tên: cho phép các máy có thể đăng ký một tên nhận dạng trên mạng và sau đó xóa đi khi thoát khỏi mạng

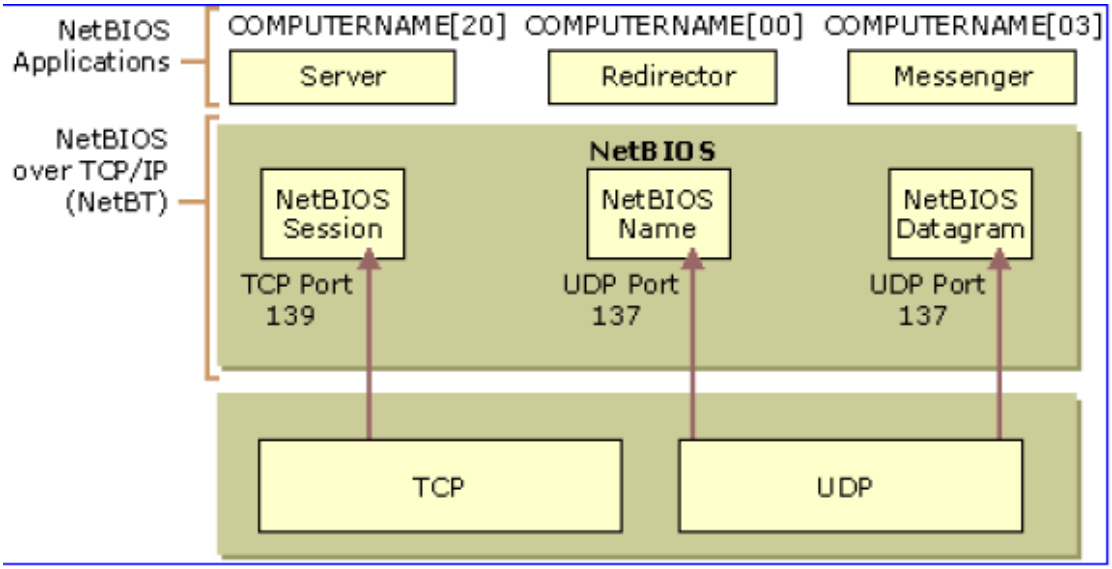
. Phân giải tên (Name Resolution): khi có một chương trình NetBIOS muốn giao tiếp với một chương trình NetBIOS khác, thì địa chỉ IP của chương trình này phải được phân giải thành NETBIOS name, NETBIOS trên TCP/IP sẽ thực hiện chức năng này.

❖ NetBIOS Datagram

Quản lý cách truyền các datagram theo liên kết không định hướng. Các datagram có thể truyền cho một người hay một nhóm người nào đó sử dụng cơ chế NetBIOS Name.

❖ NetBIOS Session

Quản lý cách truyền các datagram theo liên kết có định hướng và theo thứ tự có độ tin cậy cao. Nó sử dụng giao thức TCP để thành lập một liên kết và kết thúc khi cần thiết. Xem hình vẽ (Hình 4.4)




*Hình 4.4* Cơ chế NETBIOS

### 4.4.5 NetBEUI

- Là giao thức thích hợp cho các mạng LAN nhỏ từ 10 - 200 máy
- Nhanh, hiệu qủa, ít tốn vùng nhớ.

### 4.4.6 NDIS

Được phát triển bởi Microsoft và 3 COM có các phiên bản như NDIS, NDIS2 và NDIS3. Các phiên bản cũ dùng cho Windows for workgroup, NT 3.5, còn các phiên bản mới dùng cho WinNT 4.0 hay Windows 2000.

## 4.5 Một số Protocols khác

- DLC (Data Link Control): dùng để liên kết IBM mainframes và máy in của HP
- NFS ( Network File System) : là giao thức dùng trên UNIX
- SNA ( System Network Architecture) dùng trên máy IBM
- X-windows: tập các giao thức (MIT) dưới dạng Graphic để giao tiếp với người sử dụng trên Unix.

# Câu hỏi ôn tập chương 4

1. Mục nào trong các mục sau không phải là một thuộc tính TCP/IP trong một môi trường định tuyến?
   a. TCP/IP address b. Subnet mask
   c. Default gateway d. DNS server
2. Một mạng LAN, trong đó các máy tính được kết nối tới một HUB với cáp xoắn đôi, tốt nhất có thể được mô tả như:
   a. Một hình trạng star lôgíc
   b. Một hình trạng bus lôgíc và một hình trạng star vật lý.
   c. Một hình trạng ring hoặc loop.
   d. Một hình trạng bus vật lý.
3. Giao thức nào trong các giao thức sau không phải là một giao thức có thể định tuyến?
   a. FTP b. IP c. NetBEUI d. SMTP
4. Giao thức nào chuyển đổi datagrams mà không có thông tin ACK hoặc truyền đảm bảo?
   a. TCP b. ASP c. TCP/IP d. UDP
5. Một trong những khác nhau chính giữa NetBEUI và TCP/IP là:
   a. NetBEUI là định tuyến và TCP/IP là không định tuyến.
   b. NetBEUI là không định tuyến và TCP/IP là định tuyến.
   c. NetBEUI thì khó quản lý.
   d. TCP/IP cấu hình dễ dàng hơn so với NetBEUI.
6. Các yêu cầu tối thiểu cho việc định địa chỉ trong một mạng dựa trên giao thức TCP/IP?
   a. IP address, Subnet Mask, và default gateway.
   b. MAC address và subnet mask.
   c. IP address.
   d. IP address và subnet mask.
7. Những lợi ích mà TCP có so với UDP?
   a. TCP cho phép các gói lớn hơn được gửi qua mạng nhờ đó cải tiến hiệu suất ứng dụng.
   b. TCP có một cơ chế "gửi lại" để ngăn chặn việc mất gói dữ liệu.
   c. TCP sử dụng một header nhỏ hơn UDP.
   d. Không phải những điều ở trên.
8. Giao thức nào trong các giao thức giao vận sau được sử dụng cho việc chơi các trò chơi trên Internet?
   a. TCP b. IPX/SPX.
   b. NetBEUI d. UDP
9. Giao thức nào được sử dụng để gán các địa chỉ IP tĩnh?
   a. ARP b. Proxy ARP
   c. DHCP d. TCP/IP
10. Cái gì được sử dụng trong giao thức để tách host ID khỏi network ID?
    a. Network address b. Node address.
    c. Default gateway d. Subnet mask.

# CHƯƠNG 5 - CÁC HÌNH TRẠNG (TOPOLOGIES) CỦA MẠNG CỤC BỘ (LAN)

## MỤC TIÊU CỦA CHƯƠNG

*Kết thúc chương này, sinh viên sẽ có thể:*

- Nắm được các đặc trưng cơ bản của mạng cục bộ.
- Hiểu được các đặc điểm cũng như các ưu và nhược điểm của các hình trạng LAN đơn giản: *bus*, *star* và *ring*, cũng như đặc điểm của các hình trạng LAN hỗn hợp.
- Hiểu được ba kỹ thuật chuyển mạch: *kênh*, *thông báo* và *gói*; So sánh ba kỹ thuật chuyển mạch này.
- Nắm được nội dung cơ bản hai phương pháp truy xuất đường truyền: *CSMA/CD* và *Token Passing*.
- Nắm được các yếu tố (cả về lý thuyết và kỹ thuật cơ bản) tạo nên kiến trúc mạng Ethernet và mạng Token Ring

## 5.1 Các đặc trưng cơ bản của mạng cục bộ (LAN)

Trong mục 1.2.3 ở phần đầu tài liệu này, khi phân loại các mạng máy tính dựa trên yếu tố chính là khoảng cách địa lý, ta có các loại mạng như mạng cục bộ (LAN), mạng đô thị (MAN), mạng diện rộng (WAN) và mạng toàn cầu (GAN). Tuy nhiên khoảng cách địa lý giữa các trạm của mạng cũng chỉ là một trong các đặc trưng của mạng cục bộ. Còn có các đặc trưng khác (như tốc độ truyền, tỷ suất lỗi, …) cũng đóng vai trò quan trọng quyết định hiệu suất và sự phát triển của LAN.

Sau đây là một số đặc trưng cơ bản của LAN cho phép phân biệt LAN và các loại mạng khác, đặc biệt là với WAN.

### *5.1.1 Đặc trưng địa lý*

Cũng như đã được trình bày trong mục 1.2.3, mạng LAN là mạng được cài đặt trong một phạm vi tương đối nhỏ (trong một phòng, một toà nhà, hoặc phạm vi của một trường học v.v…) với khoảng cách lớn nhất giữa hai máy tính trạm chỉ trong khoảng vài chục ki-lô-met trở lại. Tuy nhiên giới hạn về khoảng cách này cũng chỉ có tính chất tương đối. Vì vậy, không thể chỉ lấy đặc trưng về địa lý để phân biệt LAN với các loại mạng khác.

### *5.1.2 Đặc trưng tốc độ truyền*

Mạng cục bộ có tốc độ truyền thường *cao hơn* so với mạng diện rộng (WAN). Hiện nay, tốc độ truyền của LAN có thể đạt tới 100 Mb/s.

### *5.1.3 Đặc trưng độ tin cậy*

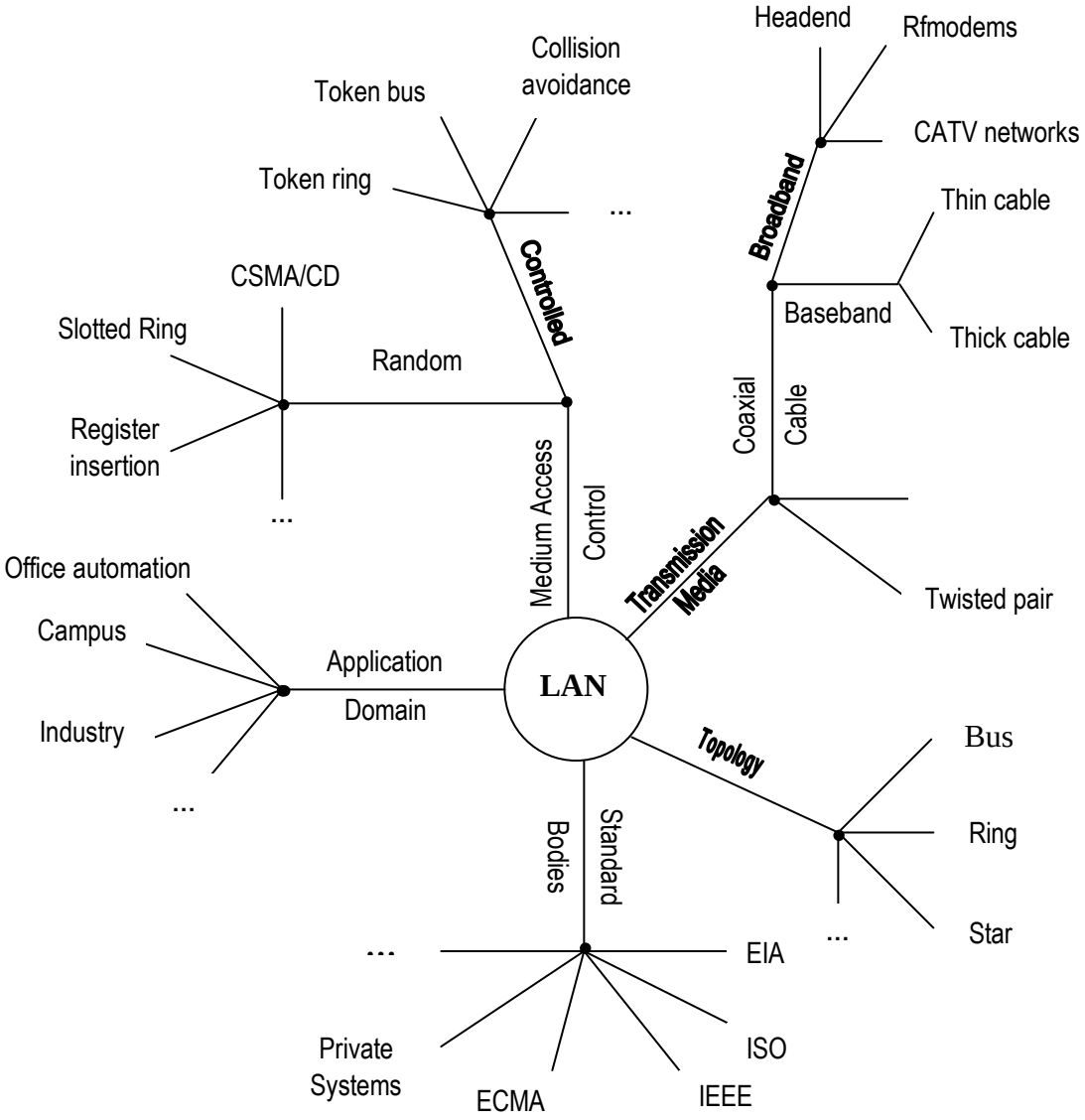
Tỷ suất lỗi (error rate) trên mạng LAN *thấp hơn* nhiều so với WAN: có thể đạt từ $10^{-8}$ đến $10^{-11}$.

### *5.1.4 Đặc trưng quản lý*

Mạng cục bộ thường là sở hữu riêng của một cá nhân hoặc tổ chức nào đó (trường học, doanh nghiệp, v.v…) do đó việc quản lý khai thác mạng hoàn toàn tập trung, thống nhất.

Tuy nhiên, với sự phát triển nhanh chóng của công nghệ mạng, các đặc trưng nói trên cũng chỉ có tính chất tương đối. Sự phân định giữa mạng cục bộ và mạng diện rộng sẽ ngày càng "mờ" hơn.

Hình 5.1 cho ta một sơ đồ tóm tắt các vấn đề cần xem xét khi tìm hiểu về mạng cục bộ.




*Hình 5.1* Sơ đồ tóm tắt những vấn đề liên quan đến mạng LAN

Những vấn đề liên quan đến đường truyền vật lý (Transmission media) đã được tìm hiểu ở chương 3. Chương này tập trung xem xét về hình trạng (topology) và kỹ thuật truy xuất đường truyền (Medium Access Control) LAN.

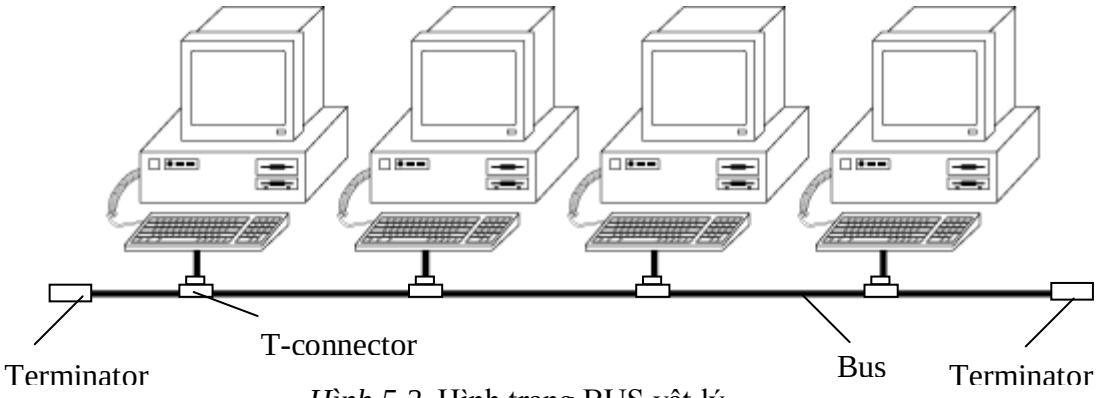
## 5.2 Các hình trạng LAN đơn giản

Như đã trình bày trong phần 1.2.4, mạng cục bộ có ba hình trạng đơn giản là *bus* (đường trục), *star* (hình sao), và *ring* (vòng). Sau đây ta sẽ lần lượt tìm hiểu các hình trạng này.

### 5.2.1 Hình trạng BUS

Một hình trạng *bus* vật lý (còn gọi là hình trạng *bus tuyến tính*) căn bản sử dụng một đường cáp chung dài gọi là đường *xương sống* (backborne hay bus). Đường cáp này còn được gọi là *đường truyền chính* (trunk line) hoặc *phân đoạn mạng* (network segment).

Có những đoạn cáp ngắn được gắn với đường xương sống bằng các *đầu nối* (tap) để kết nối với các thiết bị mạng (Các *tap* là những thiết bị cơ khí dùng để phân tách tín hiệu điện hoặc điện từ). Tuy nhiên các hình trạng bus hiện nay chủ yếu gắn các máy tính trực tiếp với đường truyền chính bằng đầu nối chữ T (T-connector). Đường truyền chính được kết thúc (terminate) ở hai đầu bằng các terminator để loại bỏ các tín hiệu trên dây sau khi nó truyền qua mọi thiết bị gắn với bus. Tất cả các nút (bao gồm máy chủ file, các máy trạm, và các thiết bị ngoại vi) được kết nối tới đường truyền chính đó (Hình 5.2).




*Hình 5.2* Hình trạng BUS vật lý

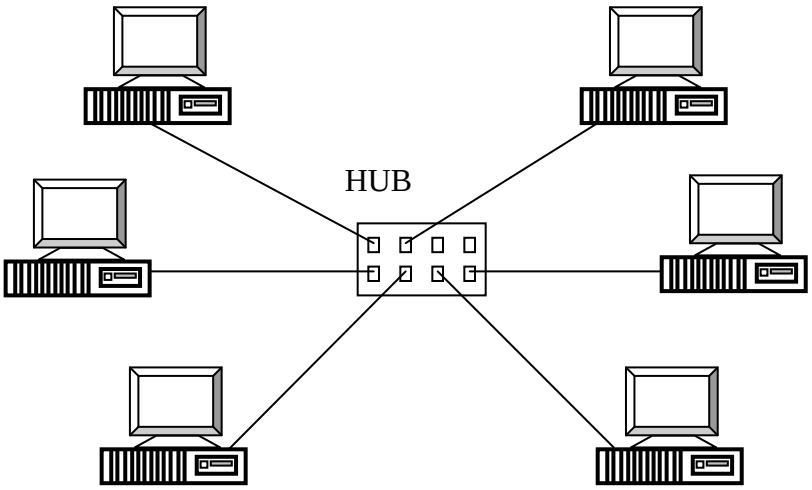
Đa số các hình trạng bus cho phép các tín hiệu điện hoặc điện từ lan truyền theo cả hai hướng

- *Ưu điểm của hình trạng* BUS*:*
  - Sử dụng các chuẩn đã được thiết lập, cài đặt tương đối dễ dàng.
  - Đòi hỏi đường truyền cáp ít hơn các hình trạng khác.
  - Cách bố trí dây rất đơn giản, dễ mở rộng và tin cậy.
- *Nhược điểm của hình trạng* BUS*:*

- Khó khăn trong việc cấu hình lại, đặc biệt khi khoảng cách và số các đầu nối vượt quá mức tối đa cho phép.
- Việc chẩn đoán và cô lập các lỗi khó khăn.
- Mạng sẽ không hoạ t động (down) khi có lỗi hoặc đứt cáp.

### 5.2.2 Hình trạng STAR

Mạng ở dạng hình sao có một *bộ xử lý trung tâm* (HUB) – còn gọi là bộ *chuyển tiếp nhiều cổng* (multiport repeater) hay *bộ tập trung* (concentrator) mà tất cả các nút (máy chủ file, các máy trạm, và các thiết bị ngoại vi) gắn với nó qua đường cáp (Hình 5.3). Các mạng hình sao có thể được lồng trong các mạng hình sao khác để tạo thành mạng hình cây hoặc mạng phân cấp




*Hình 5.3* Hình trạng STAR với HUB ở trung tâm

Dữ liệu trên mạng STAR truyền qua HUB trước khi tiếp tục tới đích. HUB quản lý và điều khiển tất cả các chức năng của mạng. HUB cũng hoạt động như một bộ chuyển tiếp luồng dữ liệu. Nó được sử dụng trong các mạng ARCnet, Token Ring, FDDI (Fiber Distributed Data Interface) và các mạng cục bộ 10BaseT với cáp xoắn đôi, cáp đồng trục hoặc cáp sợi quang. Những ví dụ điển hình của hình trạng STAR là các kiến trúc *mainframe* và *minicomputer*, trong đó máy chủ (host) là một bộ chuyển mạch (switch) tập trung. Trong mạng hình sao, nếu một cáp bị đứt, nó chỉ ảnh hưởng tới nút (máy trạm) nối tới HUB bằng cáp đó. Tuy nhiên nếu HUB bị hư thì toàn bộ phân đoạn mạng kết nối tới HUB đó sẽ ngừng hoạt động.

Đa số các mạng cục bộ Ethernet hiện nay đều sử dụng hình trạng STAR vì khả năng mở rộng và dễ dàng kết nối với các mạng khác. Chúng cũng dễ dàng cô lập các lỗi xảy ra với cáp mạng. Nhiều mạng bus và ring cũ cũng được nâng cấp để chuyển sang mạng hình sao.

❖ *Ưu điểm của hình trạng* STAR*:*

- Dễ cài đặt và cấu hình lại.

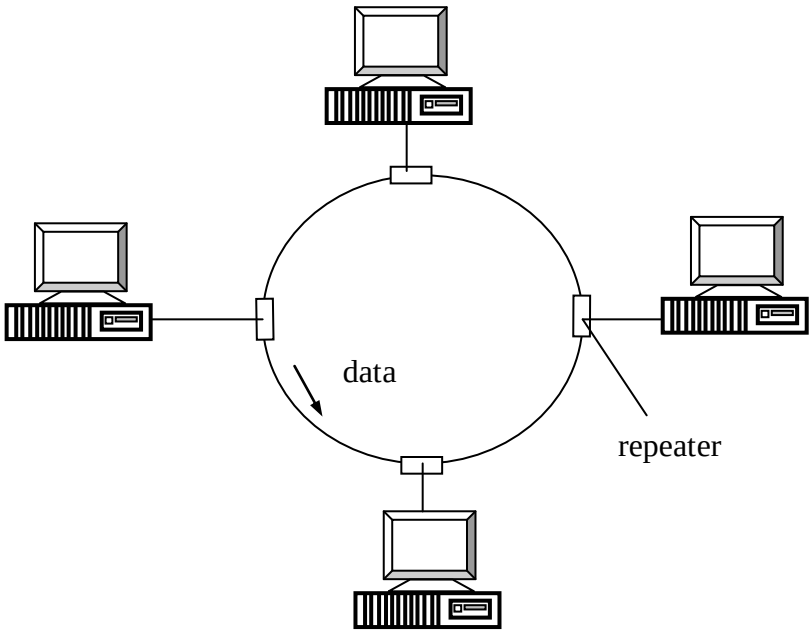
- Dễ giải quyết các sự cố.
- Lỗi đường truyền tự động cô lập phân đoạn mạng bị lỗi.
- Không cần phải ngắt mạng khi cần kết nối thêm hoặc tháo bỏ bớt các thiết bị mạng.

❖ *Nhược điểm của hình trạng* STAR*:*

- Đòi hỏi nhiều cáp hơn các hình trạng khác.
- Việc tồn tại một HUB tập trung (hoặc concentrator) đồng nghĩa với việc tồn tại khả năng ngừng hoạt động của toàn phân đoạn mạng khi HUB đó có sự cố.

### 5.2.3 Hình trạng RING

Một hình trạng RING vật lý là một hình trạng vòng (vòng kín liên kết điểm-điểm). Mỗi thiết bị kết nối trực tiếp tới vòng hoặc gián tiếp qua một thiết bị giao tiếp và cáp. Mỗi thiết bị hoạt động như một bộ chuyển tiếp (repeater), khuếch đại tín hiệu giữa các máy trạm.




*Hình 5.4* Hình trạng RING

Các tín hiệu điện hoặc điện từ được truyền từ thiết bị này tới thiết bị khác chỉ theo một hướng. Mỗi thiết bị kết hợp một thiết bị nhận ở cáp đến (receiver) và một thiết bị phát (transmitter) ở cáp đi. Các tín hiệu được lặp lại và tái sinh ở mỗi thiết bị sao cho sự suy hao là nhỏ nhất. Một ví dụ sử dụng hình trạng vòng là mạng cục bộ *Token Ring*. Loại mạng vòng này sử dụng việc *truyền thẻ bài* (token passing) để cho phép từng máy tính gửi dữ liệu trên mạng.

Một *thẻ bài* (token) là một gói dữ liệu nhỏ (3 byte) cho phép các nút truy xuất mạng. Nút (máy tính) gửi phải lấy thẻ bài và bổ sung thông tin địa chỉ, thông tin điều khiển riêng cùng với dữ liệu để hình thành một frame dữ liệu. Sau đó frame này được truyền trên mạng tới nút kế tiếp trong vòng. Nếu frame

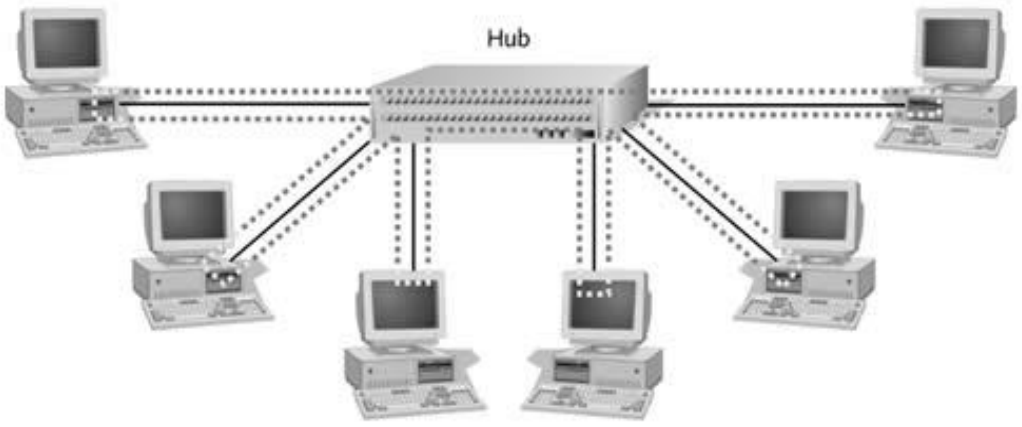
dữ liệu không phải dành cho nút kế tiếp thì nút này tái sinh lại tín hiệu và truyền tiếp nó trên mạng. Quá trình này tiếp tục cho đến khi nút nhận lấy được frame dữ liệu. Sau khi nhận được frame dữ liệu, nút nhận đáp lại nút gửi ban đầu bằng cách phát ra một đáp ứng truyền trên mạng cũng ở dạng một frame dữ liệu. Frame này di chuyển quanh mạng theo cùng hướng trước đây cho đến khi nó chạm tới nút gửi ban đầu. Khi đó frame này sẽ bị loại bỏ khỏi mạng, và một thẻ bài mới lại được sinh ra và truyền trên dây để cho một nút khác nhận nó, tạo frame dữ liệu và truyền tiếp v.v…. Quá trình này đảm bảo là ở bất kỳ thời điểm nào chỉ có thể có một nút truyền dữ liệu trên mạng .

- *Ưu điểm của hình trạng* RING*:*
  - Các lỗi về cáp xác định dễ dàng
  - Vòng đôi (Dual loop ring) có thể chống lỗi tốt.
- *Nhược điểm của hình trạng* RING*:*
  - Việc cài đặt, thay đổi và cấu hình lại khó khăn hơn hình trạng bus.
  - Lỗi về đường truyền trên các vòng đơn làm ngừng hoàn toàn hoạt động của mạng.
  - Các đầu nối khá đắt, đặc biệt là các đầu nối IBM (IBM connectors).

## 5.3 Các hình trạng LAN hỗn hợp

### 5.3.1 Star-Wired Ring

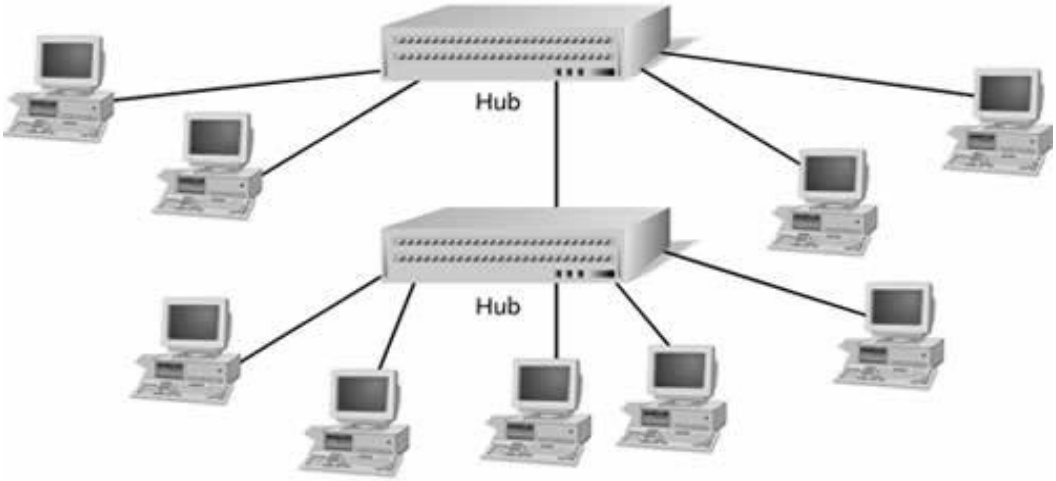
Một mạng hình trạng **star-wired ring** sử dụng cách sắp xếp vật lý của mạng *hình sao*, nhưng tích hợp phương pháp *truyền thẻ bài* (token passing). Dữ liệu được gửi quanh star theo một vòng khép kín. Điều này cho phép cơ chế chống lỗi tốt hơn mạng star và bổ sung thêm tính tin cậy của việc truyền thẻ bài. Những mạng vòng hiện nay thường sử dụng hình trạng hỗn hợp này. Trong hình 5.5 dưới đây, các đường nối liền nét đậm biểu diễn cáp vật lý kết nối hub và các trạm theo hình trạng STAR, trong khi các đường không liền nét biểu diễn vòng luận lý của hình trạng RING.




*Hình 5.5* Hình trạng mạng cục bộ Star-wired Ring

### 5.3.2 Star-Wired Bus

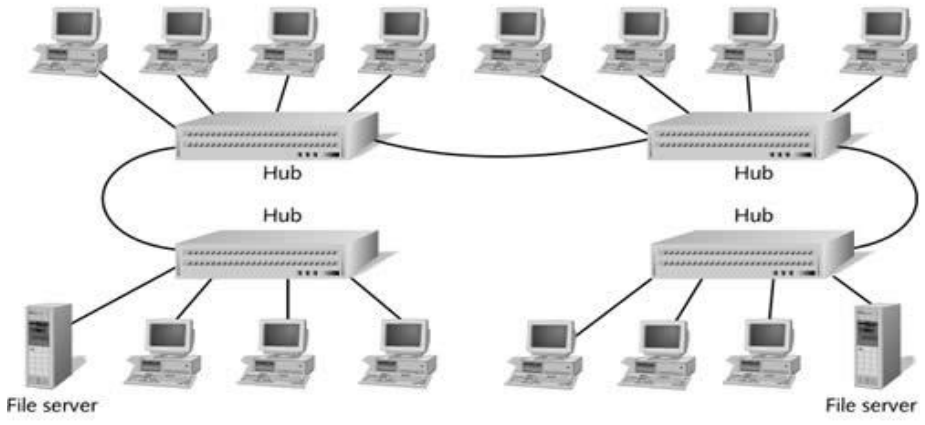
Một hình trạng **star-wired bus** là một dạng khác của hình trạng hỗn hợp. Các nhóm máy tính trạm được kết nối tới hub theo dạng *hình sao*, sau đó các hub được kết nối với nhau qua *đường trục đơn* (single bus). Điều này cho phép liên kết dễ dàng các phân đoạn mạng khác nhau và thường được sử dụng trong các mạng Ethernet và Fast Ethernet.




*Hình 5.6* Hình trạng mạng cục bộ Star-wired Bus

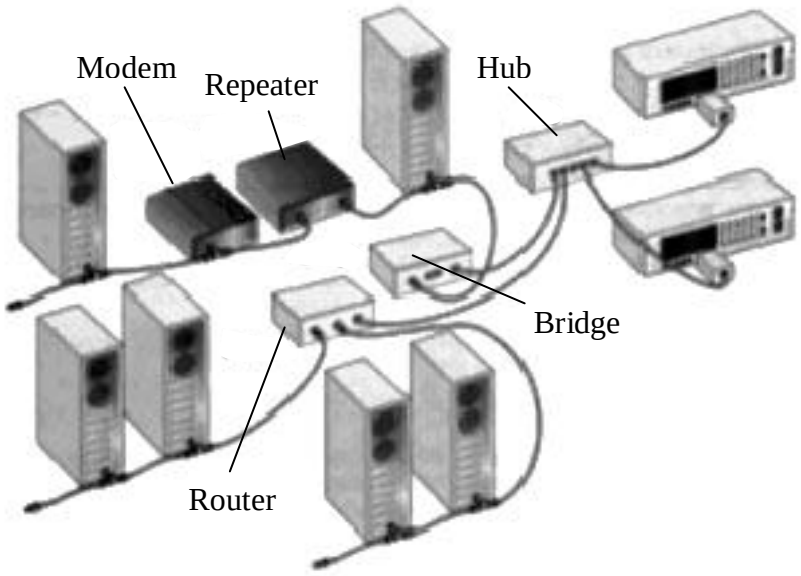
### 5.3.3 Daisy-Chained

Một mạng hình dạng *vòng hoa cúc* (daisy chain) thì tương tự như hình trạng star-wired bus. Các mạng sử dụng hình trạng star-wired bus hoặc star-wired ring có thể kết nối với nhau để hình thành một chuỗi vòng hoa phức tạp hơn. Đây là một kỹ thuật đơn giản mở rộng mạng LAN với chi phí bổ sung ít. Các quản trị mạng nên nhớ rằng, những hình trạng mạng đơn giản như Ethernet bị hạn chế về số phân đoạn có thể kết nối mà không bị mất tính toàn vẹn dữ liệu. Mặc dù về mặt vật lý rất dễ dàng mở rộng mạng, nhưng nếu chúng ta vượt quá số phân đoạn xác định, mạng của ta sẽ có lỗi.




*Hình 5.7* Một Daisy-chain có hai mạng cục bộ Star-wired Bus

## 5.4 Các hệ thống giao vận mạng




*Hình 5.8* Minh hoạ việc kết nối các thiết bị của mạng LAN (Hub, Repeater, Bridge, Router, Modem v.v….).

Hai hệ thống giao vận mạng phổ biến nhất là Ethernet và Token Ring. Những khái niệm cơ bản mà cả hai hình trạng lôgíc này sử dụng được trình bày ở phần dưới đây.

### 5.4.1 Kỹ thuật chuyển mạch (Switching)

Kỹ thuật chuyển mạch là một thành phần của hình trạng lôgíc mạng mà nó xác định cách thức các kết nối được tạo ra giữa các nút (hoặc trạm) trên mạng. Có ba kiểu chuyển mạch: *chuyển mạch kênh* (circuit switching); *chuyển mạch thông báo* (message switching); *và chuyển mạch gói* (packet switching). Mọi hệ thống giao vận mạng đều dựa trên một trong ba kiểu phương pháp chuyển mạch này. Nội dung về các kỹ thuật chuyển mạch này có thể xem lại ở mục 1.2.3. Phần tiếp theo chỉ trình bày những nét khái quát về các kỹ thuật này.

**1) Kỹ thuật chuyển mạch kênh (Circuit Switching)**

Trong kỹ thuật *chuyển mạch kênh*, một kết nối được thiết lập giữa hai nút mạng trước khi chúng khởi tạo việc truyền dữ liệu. Một tổng băng thông được dành riêng cho kết nối này và vẫn tiếp tục duy trì cho tới khi một trong hai thực thể kết thúc giao tiếp. Một khi kênh giao tiếp được thiết lập, toàn bộ dữ liệu sẽ tiếp tục đi theo cùng một con đường từ nút gửi tới nút nhận.

Kiểu chuyển mạch này không hiệu quả vì nó chiếm dụng băng thông cho trong suốt khoảng thời gian các nút kết nối.

**2) Kỹ thuật chuyển mạch thông báo (Message Switching)**

Kỹ thuật *chuyển mạch thông báo* và kỹ thuật *chuyển mạch kênh* có chung một đặc điểm là dữ liệu (toàn bộ thông báo) luôn luôn đi theo cùng một

đường. Tuy nhiên chuyển mạch thông báo *không duy trì một kết nối liên tục*. Khi một kết nối được tạo ra giữa hai thiết bị, dữ liệu được truyền tới thiết bị thứ hai, sau đó kết nối bị huỷ bỏ. Tiếp theo một kết nối được thiết lập giữa thiết bị thứ hai và thiết bị thứ ba. Một khi dữ liệu đã được truyền tới thiết bị thứ ba, kết nối đó được giải phóng. Quá trình cứ thế tiếp diễn cho đến khi dữ liệu tới đích cuối cùng. Kiểu chuyển mạch này sử dụng chương trình *lưu trữ* và *đẩy tới* (store and forward). Dữ liệu được đẩy đi từ một thiết bị này tới thiết bị kế tiếp, lưu trữ tại đó trước khi được đẩy tới thiết bị thứ ba. Kỹ thuật chuyển mạch thông báo đòi hỏi bộ nhớ lưu trữ tạm thời cao và những phí tổn xử lý tại các nút trung gian.

**3) Kỹ thuật chuyển mạch gói (Packet Switching)**

Như đã trình bày trong mục 1.2.3, kỹ thuật *chuyển mạch gói* ngắt dữ liệu thành những khối dữ liệu nhỏ, kích thước của nó có thể quản lý được - những khối này được gọi là các *gói* (packet) - trước khi chúng được truyền ngang qua mạng. Mỗi một gói có thể có con đường riêng qua mạng để tới đích cuối cùng của nó vì mỗi gói có cả hai địa chỉ nguồn và địa chỉ đích. Nói một cách khác, mỗi gói có thể tìm được kênh nhanh nhất tới đích ở bất kỳ thời điểm nào.

Nút đích trên mạng chuyển mạch gói nhận các gói và hợp nhất chúng lại theo đúng trình tự ban đầu dựa trên thông tin điều khiển bên trong gói. Kỹ thuật này tạo ra những phí tổn, mà nó không thích hợp cho việc truyền hình ảnh và âm thanh. Ưu điểm lớn nhất của kỹ thuật chuyển mạch gói là không tồn tại một con đường cố định trong khi dữ liệu được gửi từ một nút này tới nút kia và không đòi hỏi việc xử lý bởi các thiết bị trên đường truyền. Kỹ thuật chuyển mạch gói được sử dụng trong các mạng Ethernet, FDDI và Frame Relay.

### 5.4.2 Đa truy nhập có cảm nhận sóng mang / Phát hiện xung đột (Carrier Sense Multiple Access / Collision Detection - CSMA/CD)

Các hệ thống tranh chấp hoạt động dựa trên nguyên tắc: việc truy xuất đường truyền được thực hiện trên cơ sở thực thể nào chiếm dụng đường truyền đầu tiên sẽ được quyền truyền dữ liệu. Trước khi một trạm Ethernet truyền dữ liệu, nó lắng nghe kênh truyền có ở trạng thái tích cực hay không. Giao thức Ethernet thường được mô tả như giao thức "*lắng nghe trước khi truyền"* ("listen before talking"). Một kênh truyền được gọi là tích cực (activity), nếu như có bất kỳ tín hiệu đang được truyền bởi một trạm Ethernet nào đó. Sự xuất hiện của một tín hiệu truyền được gọi là *sóng mang* (carrier). Mỗi trạm có thể cảm nhận sự có mặt của một sóng mang.

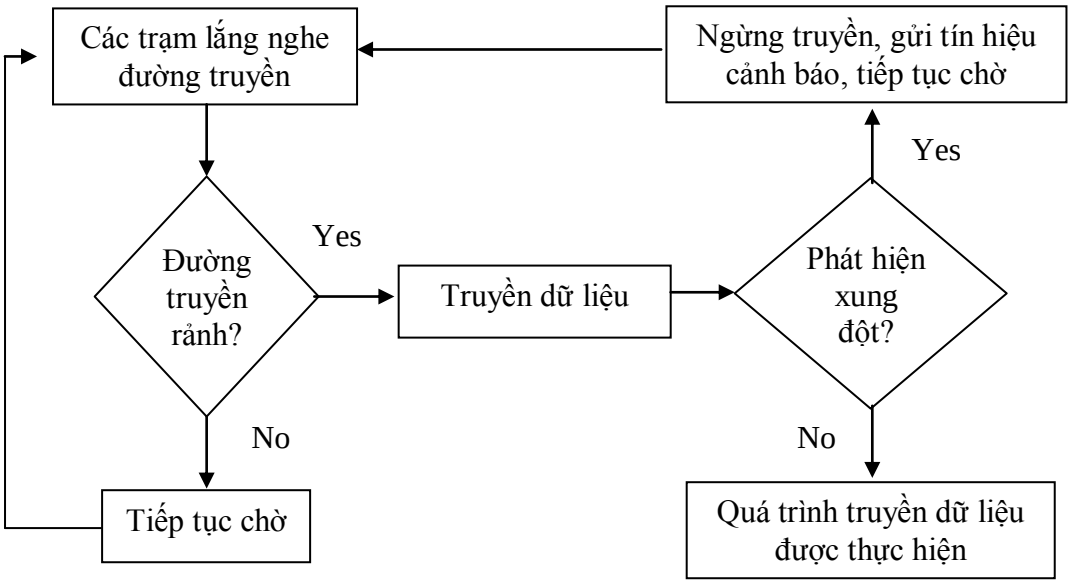
Nếu một trạm phát hiện kênh truyền đang ở trạng thái bận (trạng thái tích cực), trạm đó không thực hiện việc truyền dữ liệu. Sau khi bit cuối cùng của frame truyền qua, tầng *Ethernet Data Link* tiếp tục chờ tối thiểu 9,6 mili giây để tạo ra khoảng cách giữa các frame. Ở cuối thời điểm này, nếu một frame dữ liệu đang chờ để được truyền và nếu kênh truyền rảnh, quá trình truyền được khởi tạo. Nếu trạm không có dữ liệu để truyền, nó lại tiếp tục quá trình cảm nhận sóng mang ("Listen Before Talk" - LBT). Khoảng cách giữa các frame cung cấp thời gian hồi phục (recovery time) cho các trạm Ethernet khác.

Nếu một trạm vẫn cố truyền dữ liệu khi kênh truyền đang ở trạng thái bận, *sự đụng độ* (collision) xảy ra và kết quả là dữ liệu không đến được trạm đích hoặc nếu có đến thì cũng bị sai lệch. Nếu kênh truyền ở trạng thái rảnh (không một sóng mang nào được phát hiện), trạm đang lắng nghe có quyền truyền dữ liệu. Vì có nhiều trạm được kết nối tới kênh Ethernet sử dụng cơ chế cảm nhận sóng mang nên hệ thống này được gọi là *đa truy nhập có cảm nhận sóng mang* (Carrier Sense with Multiple Access - CSMA).

Một sự đụng độ cũng sẽ sẽ xảy ra nếu hai trạm quyết định truyền dữ liệu ở cùng một thời điểm mà kênh truyền không ở trạng thái tích cực. Những đụng độ xảy ra trong suốt quá trình hoạt động bình thường của mạng cục bộ Ethernet vì các trạm truyền dữ liệu chỉ dựa vào một sự kiện duy nhất: có tồn tại một sóng mang trên kênh truyền hay không.

Các trạm Ethernet giảm thiểu sự đụng độ bằng cách phát hiện những đụng độ khi chúng xảy ra. Vì thế thuật ngữ CSMA/CD mô tả cơ chế truy xuất đường truyền Ethernet, trong đó CD là viết tắt của Collision Detect (*phát hiện xung đột*). Cơ chế phát hiện xung đột này được gọi là "*nghe trong khi nói"* ("Listen While Talk" – LWT). Khi xảy ra xung đột các trạm (đang truyền dữ liệu ) ngừng việc truyền dữ liệu. Trạm đầu tiên phát hiện ra xung đột sẽ gửi một tín hiệu sóng mang đặc biệt tới tất cả các trạm kết nối tới mạng để cảnh báo sự kiện xung đột này. Sau khi một xung đột xảy ra, tất cả các trạm chờ đợi trong một thời đoạn ngẫu nhiên nào đó. Việc truyền chỉ xảy ra sau khi kết thúc thời đoạn này. Việc xử lý độ trễ truyền dẫn trước khi truyền có thể giảm đi những xung đột. Vì thế Ethernet không thích hợp cho các ứng dụng thời gian thực.

Giản đồ sau đây minh họa quá trình CSMA/CD.




*Hình 5.9* Quá trình CSMA/CD

## 5.5 Kiến trúc Ethernet

Sự mô tả về mạng Ethernet được xác định trong chuẩn IEEE 802.3. Về *giao thức,* mạng này sử dụng phương pháp CSMA/CD để truy xuất đường truyền. *Hình trạng* chính của Ethernet là đường trục bus tuyến tính, tuy nhiên mỗi thành phần của nó có thể là hình trạng star. (Star-wired bus)

### 5.5.1 Các loại cáp mạng Ethernet

Ethernet có thể hoạt động trên ba loại cáp khác nhau, mỗi loại có những hạn chế, yêu cầu và các thành phần riêng. Mạng Ethernet chủ yếu sử dụng cáp Ethernet chuẩn (Thicknet) và cáp Ethernet mảnh (Thinnet). Chi tiết về các loại cáp này xem lại phần *Coaxial cable* của chương 3.

Ngoài hai loại chính trên, hiện nay trong các mạng cục bộ Ethernet còn sử dụng loại cáp xoắn đôi không bọc kim loại (unshielded twisted-pair – UTP). Chi tiết về loại cáp này xem lại phần *Twisted Pair Cable* của chương 3.

Chuẩn Ethernet IEEE 802.3 mô tả ba loại cáp sử dụng trong mạng Ethernet là 10Base2, 10Base5 và 10Base-T (xem lại chương 3).

Mạng Ethernet là một lựa chọn tốt cho các mạng có lưu lượng đôi khi thay đổi mạnh. Mạng Ethernet không thích hợp cho các kiến trúc mạng cục bộ có yêu cầu tải ổn định.

Một ưu điểm của mạng Ethernet là khả năng sử dụng các giao thức khác, đặc biệt là giao thức TCP/IP (Transmission Control Protocol/Internet Protocol). Chính điều này làm cho mạng Ethernet dễ dàng cho việc truy xuất các minicomputer và các trạm công suất cao. Mạng Ethernet cũng là một chọn lựa tốt cho các mạng trong môi trường kỹ thuật, vì các nút trong môi trường này thường là các trạm cài đặt hệ điều hành UNIX sử dụng giao thức TCP/IP.

### 5.5.2 Phân đoạn mạng Ethernet

Một mạng Ethernet bao gồm các nút gắn tới đường trục bus của nó ở những cự ly khác nhau. Đường trục bus này thực sự là cáp chính dài của mạng Ethernet. Phần cáp chính này và các nút gắn tới nó được gọi là *phân đoạn mạng* Ethernet (Ethernet trunk segment).

Đa số các mạng Ethernet không thực thi một cáp dài. Thông thường cáp phân đoạn mạng được chia thành một dãy các cáp được kết nối qua các bộ chuyển tiếp(repater), cầu (bridge) và các bộ tìm đường (router).

Bảng ở phần 5.5.3 và 5.5.4 dưới đây là những mô tả chuẩn IEEE 802.3, trong đó cáp phân đoạn được giới hạn trong khoảng cách có thể truyền một tín hiệu. Cáp phân đoạn có chiều dài cực đại và bị hạn chế số nút có thể gắn tới nó. Phân đoạn mạng có thể được chia thành các đơn vị nhỏ hơn bằng việc sử dụng các đầu nối (connector). Phân đoạn mạng cáp đồng trục dày có chiều dài tối đa 500 mét (1640 feet) và có thể có tối đa 100 nút. Phân đoạn mạng cáp đồng trục mảnh có chiều dài tối đa 185 mét (607 feet) và có thể gắn tối đa 30 nút.

Một bộ chuyển tiếp (repeater) là một thiết bị dùng để mở rộng chiều dài của cáp phân đoạn mạng Ethernet. Các phân đoạn mạng bổ sung có thể mở rộng phân đoạn mạng Ethernet, tuy nhiên một phân đoạn mạng không thể được mở rộng vượt quá giới hạn xác định. Chú ý rằng mỗi nút cuối của một phân đoạn phải được gắn đầu nối terminator và một trong các nut phải được nối đất.

Mạng Ethernet không có một hub hoặc concentrator riêng như đối với hình trạng ring hoặc star. Mỗi cáp phân đoạn riêng rẽ đóng vai trò như một hub hoặc concentrator.

Một mạng Ethernet cũng có thể kết hợp các cáp Thinnet và Thicknet trong cùng một mạng. Tuy nhiên mỗi loại cáp có đặc tính kỹ thuật riêng và việc cài đặt mạng phải tuân theo các đặc tính của cả hai loại cáp này.

### 5.5.3 Các quy tắc nối cáp Ethernet mảnh (10Base2)

Các tham số cho cáp Ethernet mảnh (10Base2) được trình bày trong bảng dưới đây:

| **Các tham số cho cáp Ethernet mảnh (10Base2)** | **Giá trị** |
|---|---|
| Tốc độ cực đại của dữ liệu | 10 Mbps |
| Số repeater cực đại | 4 |
| Chiều dài cực đại cho phân đoạn cáp đồng trục | 185 mét |
| Số trạm cực đại / 1 phân đoạn | 30 |
| Tổng số trạm cực đại | 90 |
| Khoảng cách nhỏ nhất giữa các trạm | 0,5 mét |

### 5.5.4 Các quy tắc nối cáp Ethernet dày (10Base5)

Các tham số cho cáp Ethernet dày được trình bày trong bảng sau:

| **Các tham số cho cáp Ethernet dày (10base5)** | **Giá trị** |
|---|---|
| Tốc độ cực đại của dữ liệu | 10 Mbps |
| Số repeater cực đại | 4 |
| Chiều dài cực đại cho phân đoạn cáp đồng trục | 500 mét |
| Chiều dài cáp cực đại của transceiver | 50 mét |
| Chiều dài cực đại của phân đoạn mạng nối kết | 1500 mét |
| Số trạm cực đại / 1 phân đoạn | 100 |
| Tổng số trạm cực đại | 300 |
| Khoảng cách giữa các trạm | n*2,5 mét (n=1,2,3, …) |

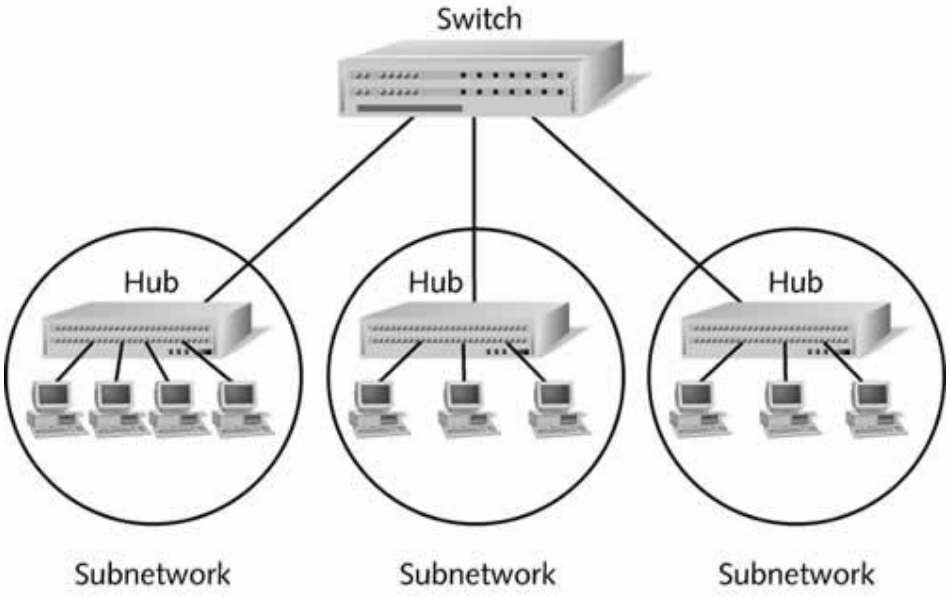
### 5.5.5 Mạng Ethernet dùng chung (Shared Ethernet)

Các mạng cục bộ Ethernet truyền thống gọi là mạng *Ethernet dùng chung*. Mạng này cung cấp tổng băng thông cố định được dùng chung giữa các thiết bị kết nối trên một phân đoạn. Hai nút mạng không thể gửi và nhận dữ liệu đồng thời, vì mạng Ethernet dùng chung này sử dụng một **hub** có chức năng nhận tín hiệu, sau đó khuếch đại và truyền lại tín hiệu đó tới mọi thiết bị.

### 5.5.6 Mạng Ethernet chuyển mạch (Switched Ethernet)

Mạng *Ethernet chuyển mạch* sử dụng một bộ chuyển mạch (**switch**) thay cho một hub. Switch này có thể phân tách một phân đoạn mạng thành các phân đoạn mạng độc lập nhỏ hơn. Mỗi phân đoạn nhỏ này có thể có lưu lượng riêng và cho phép nhiều nút truyền và nhận dữ liệu đồng thời. Như vậy, một mạng Ethernet chuyển mạch trở thành nhiều mạng *Ethernet dùng chung* độc lập, liên kết với nhau bởi switch. Điều này có nghĩa là băng thông được sử dụng hiệu quả hơn nhiều.

Mạng *Ethernet chuyển mạch* có những cải tiến đáng kể vì số các nút hoặc trạm đang tranh chấp đường truyền mạng ở bất kỳ khoảng thời gian nào được giảm đi rõ rệt. Chẳng hạn, nếu có 100 trạm trên mạng *Ethernet chuyển mạch,* mạng này có 100 máy tính đang cố giao tiếp cùng một lần. Vì mạng Ethernet sử dụng phương pháp CSMA/CD, khả năng xung đột là rất lớn. Tuy nhiên, nếu phân đoạn 100 trạm này được phân chia thành bốn phân đoạn độc lập (với số trạm ngang đều nhau) bằng việc sử dụng một switch, chỉ có 25 trạm tranh chấp đường truyền mạng. Điều này giảm thiểu khả năng xung đột một cách đáng kể.



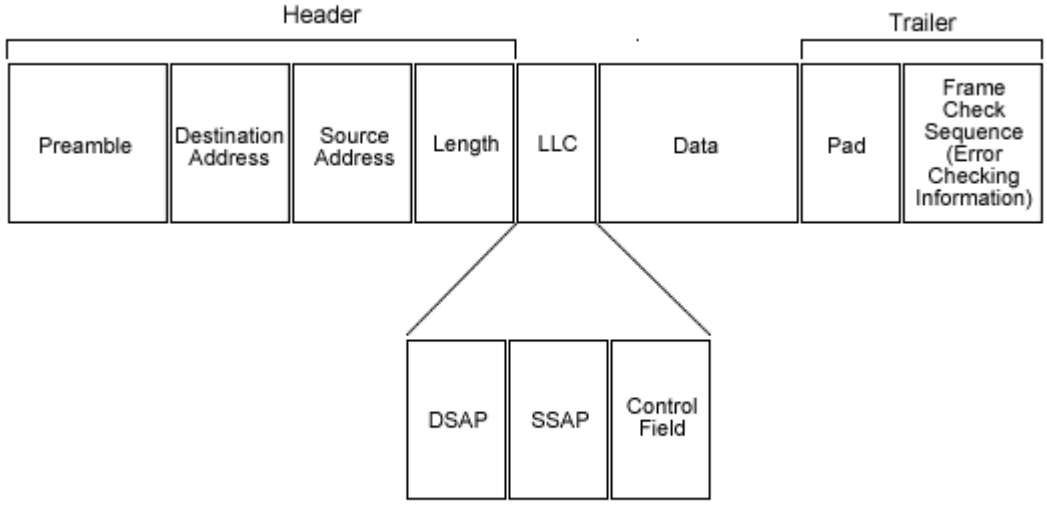

*Hình 5.10* Mạng Ethernet chuyển mạch

### 5.5.7 Các kiểu khuôn dạng Ethernet (Ethernet Frame Types)

Có bốn kiểu khuôn dạng dữ liệu khác nhau được sử dụng trong mạng Ethernet bao gồm **Ethernet 802.2**, **Ethernet 802.3**, **Ethernet II,** và **Ethernet SNAP** (Xem lại mục 2.3.1 giới thiệu về khuôn dạng Ethernet tổng quát) . Mỗi kiểu khuôn dạng có phần khác nhau và chúng đều có bốn trường chung: địa chỉ nguồn (*source addres),* địa chỉ đích (*destination address),* dữ liệu (*data)* và trường kiểm tra lỗi (*error-checking*). Các kiểu khuôn dạng Ethernet được sử dụng thông thường nhất là Ethernet 802.2 và Ethernet 802.3. Các khuôn dạng Ethernet có kích thước biến đổi từ tối thiểu 64 byte tới tối đa 1518 byte. (Mỗi khuôn dạng chứa thông tin *header* kích thước14 byte cộng với trường *Frame Check Sequence* chiều dài 4 byte. Phần *dữ liệu* của khuôn dạng có kích thước biến đổi từ 46 byte tới tối đa 1500 byte. Kích thước tổng cộng của frame được tính toán đơn giản bằng cách cộng kích thước của tất cả các trường – Nếu trường dữ liệu của frame nhỏ hơn 46 byte, frame sẽ được đệm thêm trường *pad* để kích thước tối thiểu của nó là 46 byte.

***a) 802.2***

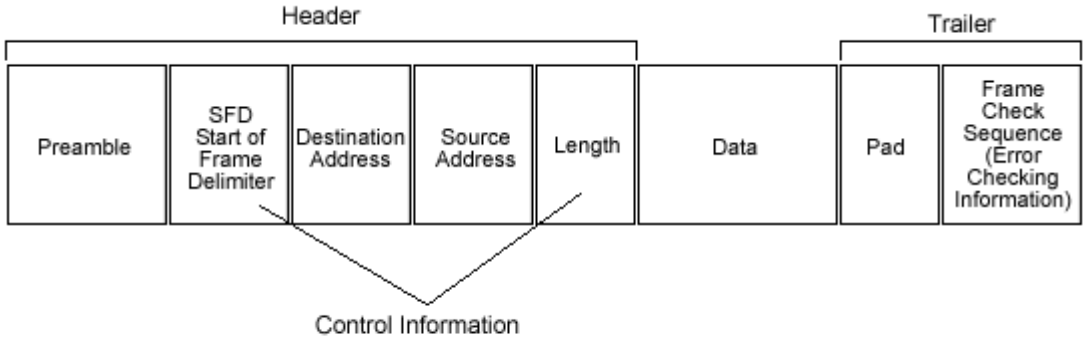
Khuôn dạng **Ethernet 802.2** là khuôn dạng mặc định được sử dụng cho mạng Novell Netware 4.x và hệ điều hành mạng cao hơn. Khuôn dạng này hỗ trợ giao thức IPX/SPX cũng như giao thức TCP/IP và là khuôn dạng Ethernet thông thường nhất được sử dụng ngày nay. Các khuôn dạng này chứa một *điểm truy nhập dịch vụ đích* (Destination Service Access Point - **DSAP)** và một *điểm truy nhập dịch vụ nguồn* (Source Service Access Point - **SSAP)**. Một *điểm truy nhập dịch vụ* (Service Access Point - SAP) định danh một nút hoặc quá trình bên trong, mà quá trình này sử dụng tầng con Logical Link Control của tầng Data Link. Mỗi quá trình xảy ra giữa nút nguồn và nút đích trên mạng có một SAP duy nhất.




*Hình 5.11* Một khuôn dạng Ethernet 802.2 điển hình

### *b) 802.3*

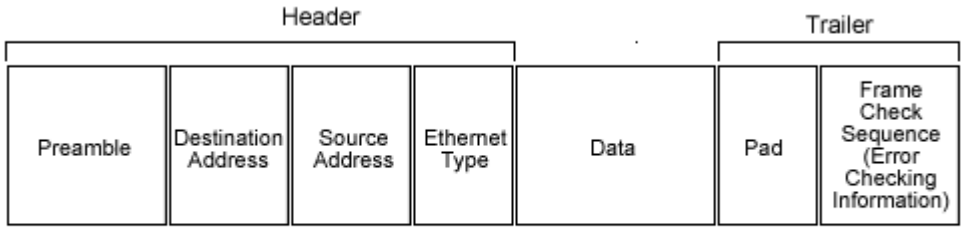
Kiểu khuôn dạng **Ethernet 802.3** là kiểu khuôn dạng Novell Netware ban đầu. Nó dùng cho các mạng đang sử dụng Novell Netware 3.12 và các phiên bản thấp hơn. Giống như Ethernet 802.2, kiểu khuôn dạng này cũng hỗ trợ giao thức IPX/SPX, nhưng nó không hỗ trợ các giao thức khác như TCP/IP. Không có các bit điều khiển (DSAP và SSAP) bên trong khuôn dạng 802.3.




*Hình 5.12* Một khuôn dạng Ethernet 802.3 điển hình

### *c) Ethernet II*

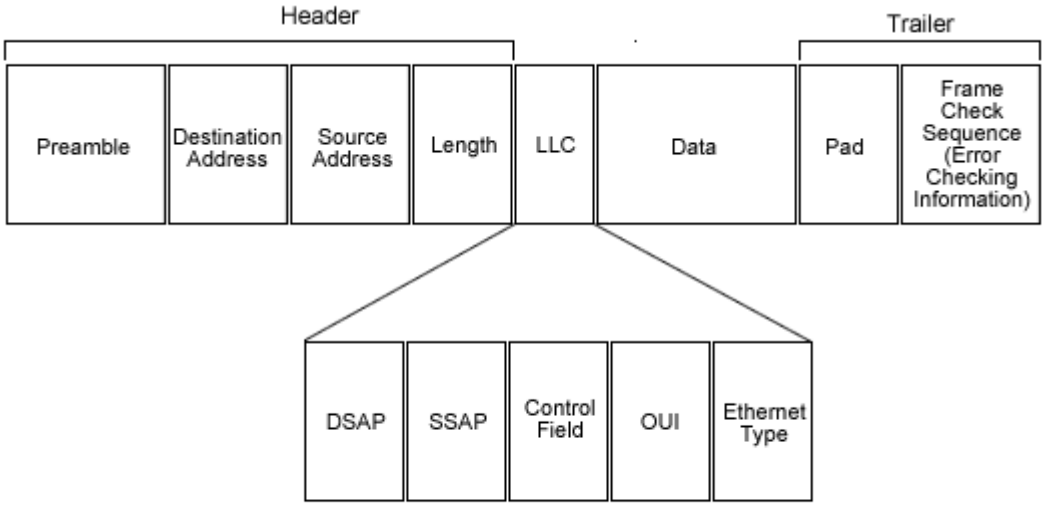
Ethernet II là kiểu khuôn dạng Ethernet đầu tiên được phát triển bởi DEC, Intel và Xerox. Nó được phát triển trước chuẩn IEEE 802. Nó tương tự khuôn dạng Ethernet 802.3, nhưng không chứa trường *length*. Thay thế, khuôn dạng Ethernet II chứa trường *Ethernet Type*, mà nó cho phép phân biệt việc sử dụng các giao thức IPX/SPX, TCP/IP và AppleTalk (Nội dung các giao thức này xem lại ở chương 4)




*Hình 5.13* Một khuôn dạng Ethernet II điển hình

### *d) Ethernet SNAP (Sub-Network Access Protocol)*

**Ethernet SNAP** là một sự điều chỉnh của khuôn dạng Ethernet 802.2 và Ethernet II. Kiểu khuôn dạng này sử dụng cùng các trường điều khiển như khuôn dạng 802.2 – *Destination Service Access Point (DSAP)* và *Source Service Access Point (SSAP)*. Nó cũng bổ sung trường *Ethernet Type* từ khuôn dạng Ethernet II cộng thêm một trường khác gọi là trường **Organisation ID (OUI)**. Trường này định danh kiểu mạng mà các khuôn dạng đó đang hoạt động. Ethernet SNAP thì thích hợp với các giao thức IPX/SPX, TCP/IP và AppleTalk, nhưng khuôn dạng này hiếm khi được sử dụng.




*Hình 5.13* Một khuôn dạng Ethernet SNAP điển hình

## 5.6 Mạng Token Ring

### 5.6.1 Kỹ thuật truyền thẻ bài (Token Passing)

Trong các hệ thống truyền thẻ bài, một frame dữ liệu nhỏ (token) được truyền lần lượt từ thiết bị này đến thiết bị khác. Một thẻ bài là một thông báo đặc biệt mà khi thiết bị nào lưu giữ nó, thiết bị đó tạm thời có quyền điều khiển đường truyền. Kỹ thuật truyền thẻ bài phân bố việc điều khiển truy xuất giữa các thiết bị mạng.

Mỗi thiết bị biết được thiết bị nào truyền thẻ bài tới nó cũng như thiết bị nào sẽ nhận thẻ bài do nó truyền đi (các thiết bị đứng trước và sau nó trong vòng lôgíc). Mỗi thiết bị định kỳ lấy quyền điều khiển thẻ bài, thực hiện nhiệm vụ của nó, và sau đó truyền thẻ bài cho thiết bị kế tiếp sử dụng. Các giao thức giới hạn mỗi thiết bị có thể kiểm soát thẻ bài trong bao lâu.

Tồn tại một số giao thức truyền thẻ bài. Hai chuẩn về mạng LAN truyền thẻ bài là *Token Bus* IEEE 802.4 và *Token Ring* 802.5. Mạng *Token Bus* sử dụng phương pháp điều khiển truy xuất bằng truyền thẻ bài và một hình trạng bus vật lý hoặc lôgíc, trong khi mạng *Token Ring* cũng sử dụng phương pháp điều khiển truy xuất bằng truyền thẻ bài nhưng hình trạng vật lý hoặc lôgíc là ring. Một chuẩn truyền thẻ bài khác (dùng cho các mạng LAN cáp sợi quang) được gọi là FDDI (Fibre-Distributed Data Interface).

Kỹ thuật truyền thẻ bài thì thích hợp cho các mạng có tải thay đổi mạnh theo thời gian chẳng hạn như các mạng truyền hình ảnh hoặc âm thanh số hoá hoặc các mạng có tải cao.

### 5.6.2 Kiến trúc Token Ring

Kiến trúc *Token Ring* tuân theo các chuẩn được tạo ra bởi IEEE 802.5 thuộc về một đề án có tên **Project 802.**

Hình trạng của *Token Ring* được sử dụng là star-wired ring, với ring được hình thành bởi hub. Các nút được gắn với ring (hoặc hub) tạo thành star. Mạng

*Token Ring* sử dụng phương pháp *xác định* (chứ không *ngẫu nhiên* như giao thức CSMA/CD) để truy xuất cáp. Thẻ bài – một khối bít xác định trước – cho phép một nút giao tiếp với cáp. Thẻ bài được truyền từ nút này tới nút kia cho tới khi một nút có yêu cầu truyền dữ liệu – quá trình này được gọi là *truyền thẻ bài* (**token passing**). Ta cần chú ý là phải tồn tại một vòng để thẻ bài di chuyển theo ở mọi thời điểm. Dữ liệu di chuyển trên vòng chỉ theo một hướng.

Mạng *Token Ring* có hai kiểu chính với tốc độ truyền dữ liệu là 4 và 16 Mbps, cả hai kiểu này đều dùng kỹ thuật truyền băng tần cơ sở. Cả hai kiểu mạng *Token Ring* đều có khả năng sử dụng cáp xoắn đôi không bọc kim loại, cung cấp khả năng tăng độ tin cậy cũng như mở rộng khoảng cách truyền tín hiệu.

### 5.6.3 Các thành phần của Token Ring

Có bốn thành phần cơ bản tạo nên mạng *Token Ring*: Token Ring NIC, Token Ring Multistation Access Unit (MAU), Cabling System, và Token Ring Network Connector.

**a) NIC của Token Ring**

Bảng mạch giao tiếp mạng (Network Interface Card - NIC) dùng cho *Token Ring* thì tương tự những NIC sử dụng với các loại mạng khác, chẳng hạn như Ethernet, nhưng được thiết kế đặc biệt cho phương pháp giao vận *Token Ring*. Ta không thể sử dụng NIC của một kiểu mạng này cho một kiểu mạng khác. Các NIC phải được kết nối qua một cáp tới *đơn vị truy xuất nhiều trạm (*Multistation Access Unit – MAU). MAU là một thiết bị tương đương với hub hoặc repeater của *Token Ring*. NIC của *Token Ring* có thông lượng là 4 Mbps hoặc 16 Mbps.

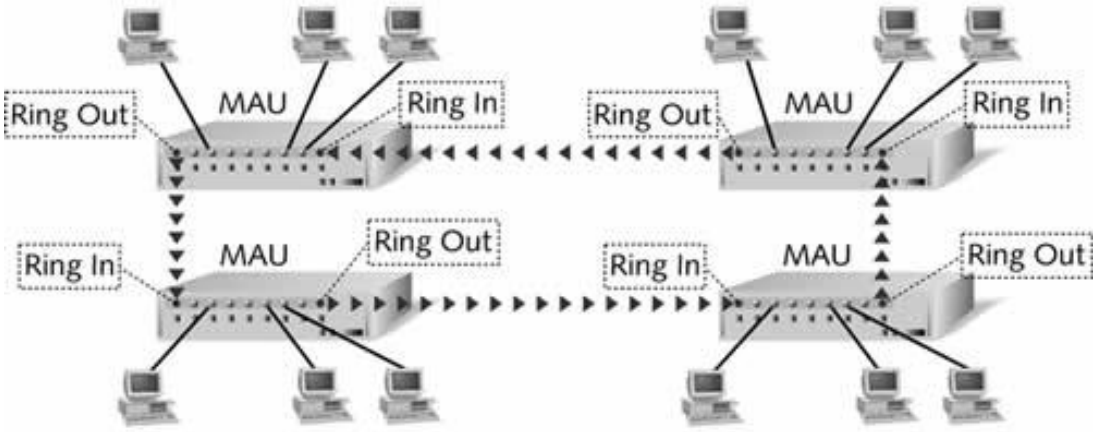
**b) MAU - Đơn vị truy xuất nhiều trạm của Token Ring**

*Đơn vị truy xuất nhiều trạm* được gọi là MAU (Multistation Access Unit ) hoặc là SMAU (Smart Multistation Access Unit). MAU cũng còn được tham chiếu như là một chuẩn 8228 (Đặc tả 8225 của IBM). MAU là một hub của mạng *Token Ring.*

Có 10 cổng trên một MAU 8228, tám cổng dùng cho kết nối các nút mạng, hai cổng còn lại được gọi là cổng *Ring-In* và cổng *Ring-Out*. Hai cổng này được sử dụng khi kết nối một dãy các MAU để duy trì tính toàn vẹn của vòng (Hình 5.14). *Ring-Out* là cổng xuất tín hiệu và *Ring-In* là cổng nhập tín hiệu. Nếu mạng chỉ có một MAU thì cổng *Ring-Out* và cổng *Ring-In* có thể được để nguyên (không kết nối). Nếu bất kỳ cổng nào trên MAU còn để trống, nó sẽ "*tự làm ngắn mạch*" để tạo nên một kết nối nhằm mục đích duy trì vòng.

Mỗi MAU có khả năng kết nối tối đa tám nút. Khi có nhiều hơn các nút được yêu cầu , nhiều MAU được kết nối bằng việc liên kết các cổng *Ring-In* và cổng *Ring-Out* của chúng. Các MAU được cài đặt trong một mạng có thể kết nối tối đa 72 nút khi sử dụng cáp xoắn đôi không bọc kim loại (Unshielded Twisted Pair - UTP) , hoặc tối đa 260 nút khi sử dụng cáp xoắn đội có bọc kim (Shielded Twisted Pair - STP).

Các MAU hoặc hub được nối với nhau để hình thành vòng. Các nút được kết nối tới MAU để tạo thành star của mạng.




*Hình 5.14* Nối kết các MAU Token Ring

### c) Hệ thống cáp

Có rất nhiều đặc tả cáp Token Ring khác nhau, bao gồm: IBM loại 1, IBM loại 2, IBM loại 3, IBM loại 5, IBM loại 6 và IBM loại 9. Bảng sau đây cho thấy các đặc tính của mỗi loại cáp này.

| Loại cáp IBM | Mô tả |
|---|---|
| **Loại 1** | ■ Hai cặp cáp xoắn với nhau, sau đó tất cả được bọc bên ngoài<br>■ Kích cỡ 22 AWG, được kiểm tra tới 16Mbps<br>■ Điện trở 150 Ohms ■ 0 % ở tần số 3-20Mhz<br>■ Độ suy hao 22dB / 1 km<br>■ Độ nhiễu (crosstalk) giữa các cặp phải nhỏ hơn 58dB<br>■ Sử dụng cho LAN : giữa các MAU và từ MAU tới vách tường |
| **Loại 2** | ■ Hai cặp xoắn với nhau và được bọc bên ngoài, sau đó hai cặp này được bọc cùng với bốn cặp dùng cho tiếng nói (cáp Unshielded Twisted Pair Category 3)<br>■ Kích cỡ 22 AWG, được kiểm tra tới 16Mbps<br>■ Điện trở 150 Ohms ■ 0 % ở tần số 3-20Mhz<br>■ Độ suy hao 22dB / 1 km<br>■ Độ nhiễu (crosstalk) giữa các cặp phải nhỏ hơn 58dB<br>■ Sử dụng cho LAN: đi xuyên qua các vách tường tới các trạm, mang tiếng nói, sử dụng cho mạng *token ring* và mạng Ethernet 10Base-T. |

| Loại cáp IBM | Mô tả |
|---|---|
| **Loại 3** | ■ Các cặp cáp xoắn không bọc (Unshielded Twisted Pair )<br>■ Dây có kích cỡ 22 AWG hoặc 24 AWG<br>■ Ít nhất 2 lần xoắn / 1 foot<br>■ Điện trở 100 Ohms ở tần số 256Khz - 2.3Mhz<br>■ Sử dụng cho LAN: nối khắp mạng *Token Ring* |
| **Loại 5** | ■ Hai cáp sợi quang *multimode*đường kính 62,5/125 micromet. (loại cáp đường kính 50/125 micromet và 100/140 micromet cũng được sử dụng)<br>■ Cáp đường kính 62,5/125 micromet là chuẩn thực tế cho FDDI<br>■ Độ suy hao: 3,75 dB/km khi sử dụng nguồn 850 nm<br>■ Độ suy hao: 1,5 dB/km khi sử dụng nguồn 1300 nm<br>■ Đường kính cáp 8,3/125 micromet cho cáp kiểu đơn<br>■ Các loại đầu nối: SMA, ST, và SC |
| **Loại 6** | ■ Hai cặp cáp xoắn với nhau, sau đó bọc bên ngoài<br>■ Cáp được bện 26 AWG<br>■ Điện trở 150 Ohms ■ 0 % ở tần số 3-20Mhz<br>■ Sử dụng cho LAN: dùng cho việc nối từ vách tường tới NIC của mỗi trạm, độ dài tối đa 30 mét. |
| **Loại 9** | ■ Hai cặp cáp xoắn với nhau, sau đó bọc bên ngoài<br>■ Cáp được bện hoặc liền khối 26 AWG<br>■ Điện trở 150 Ohms ■ 0 % ở tần số 3-20Mhz<br>■ Chấp nhận đầu nối RJ-45 (đường kính nhỏ hơn)<br>■ Sử dụng cho LAN: nối từ vách tường tới NIC của trạm |

Cáp bọc kim IBM loại 6 được sử dụng như cáp thích ứng (adapter) nối một trạm tới một MAU. Một đầu cáp có đầu nối tiếp 25 chân để kết nối tới NIC, và đầu cáp kia có một đầu nối dữ liệu IBM dùng để gắn tới hoặc một giá *faceplate* hoặc một MAU IBM 8228.

Cáp IBM loại 6 cũng có thể sử dụng làm cáp chắp nối (patch cable). Chiều dài của cáp loại 6 này biến đổi từ 2,5 mét đến 45 mét, với một đầu nối dữ liệu IBM ở mỗi đầu. Các cáp chắp nối này sau đó được nối với nhau để nối với cáp thích ứng hoặc tới MAU IBM 8228. Ví dụ, cáp chắp nối IBM loại 6 được sử dụng để gắn một nút tới một MAU. Cáp thích ứng chỉ dài 2,5 mét, nhưng khoảng cách tới MAU lớn hơn 2,5 mét. Một cáp chắp nối có thể được sử dụng để mở rộng khoảng cách, nó nối kết cáp thích ứng ở một đầu và MAU ở đầu kia. Cáp IBM loại 6 cũng được sử dụng để nối hai MAU.

Cáp IBM loại 9 được sử dụng chủ yếu khi cần phải đi dây trên trần nhà hoặc qua các khối bê tông. Nó có vỏ bọc bên ngoài đặc biệt và được sử dụng thay cho cáp IBM loại 1 và cáp IBM loại 2.

**d) Các đầu nối cáp Token Ring (Token Ring Connectors )**

Các đầu nối cáp mạng *Token Ring* về cơ bản có ba loại sau:

- Đầu nối dữ liệu cho cáp loại 1 và loại 2.
- Đầu nối điện thoại RJ-45 (8 chân) cho cáp loại 3
- Đầu nối điện thoại RJ-11 (4 chân) cho cáp loại 3

Chú ý rằng các đầu nối RJ thì chỉ dùng cho cáp loại 3. Trong đó RJ-45 được sử dụng rộng rãi hơn. Bổ sung thêm chú ý nữa, khi cáp IBM loại 3 được nối tới MAU, phải cần sử dụng một thiết bị lọc đường truyền loại 3. Thiết bị lọc này cũng cần cho cáp UTP.

### 5.6.4 Các quy tắc thiết kế việc nối cáp mạng Token Ring (IEEE 802.5)

Bảng sau đây tổng quát hoá các quy tắc thiết kế cho việc nối cáp mạng *Token Ring*:

| Các tham số *Token Ring* | Loại 1, 2 | Loại 3 |
|---|---|---|
| Số tối đa thiết bị / vòng | 260 | 96 |
| Tốc độ dữ liệu được kiểm tra | 16Mbps | 4Mbps |
| Khoảng cách tối đa từ trạm tới mạng cục bộ một MAU | 300m | 100m |
| Khoảng cách tối đa từ trạm tới mạng cục bộ nhiều MAU | 100m | 45m |
| Số tối đa các MAU / LAN | 12 | 2 |
| Khoảng cách tối đa từ MAU tới MAU | 200m | 120m |

### 5.6.5 Một số nguyên tắc cho việc đi cáp mạng Token Ring

Sau đây là những nguyên tắc chung cho việc nối cáp *Token Ring* :

1. Các trạm cách MAU 2,5 mét có thể được nối bằng cáp thích ứng 2,5 mét.
2. Các trạm cách MAU hơn 8 feet ( [redacted]50 mét) được nối bằng dây kéo dài.
3. Để tạo một vòng có nhiều MAU, nối một cáp chắp nối từ *Ring-Out* của MAU đầu tiên tới *Ring-In* của MAU thứ nhì. Tiếp tục như vậy cho tất cả các MAU cho tới MAU cuối cùng. Nối *Ring-Out* của MAU cuối cùng tới *Ring-In* của MAU đầu tiên.
4. Ta không thể nối các trạm tới các cổng *Ring-Out* và *Ring-In*. Các cổng *Ring-In* và *Ring-Out* chỉ được sử dụng cho việc nối kết giữa các MAU.
5. Các cáp chắp nối (cáp IBM loại 6) không nên ghép với nhau.
6. Cáp chắp nối (cáp IBM loại 6) không nên được sử dụng trong bất kỳ đường ống, trần nhà hoặc vùng thông khí nào. Có thể thay thế bằng cáp IBM loại 9, được xem như loại cáp rắn chắc.

# Câu hỏi ôn tập chương 5

1. Những phát biểu nào trong các phát biểu sau là đúng (chọn 1):
   a. Mạng LAN giống mạng Internet là không có chủ sở hữu và người quản trị.
   b. Mạng LAN có tốc độ truyền thường *cao hơn* so với mạng diện rộng (WAN)
   c. Mô hình OSI do ISO đưa ra chỉ có thể áp dụng cho mạng LAN.
   d. Mọi phát biểu trên đều đúng.
2. Các ưu điểm của các hình trạng STAR (choose 2):
   a. Dễ cài đặt và cấu hình b. Đòi hỏi ít cáp hơn các hình trạng khác
   c. Dễ phát hiện và sửa chữa các sự cố
3. Nhược điểm của hình trạng BUS (choose 2):
   a. Khó cài đặt và cấu hình hơn hình trạng STAR
   b. Đòi hỏi nhiều cáp hơn các hình trạng khác
   c. Khó mở rộng hơn các hình trạng khác
   d. Khó chẩn đoán và cô lập sự cố.
4. Ưu điểm của hình trạng RING (chọn 2):
   a. Các lỗi về cáp xác định dễ dàng
   b. Việc cài đặt, thay đổi và cấu hình lại dễ dàng hơn hình trạng bus.
   c. Vòng đôi (Dual loop ring) có thể chống lỗi tốt.
   d. Lỗi đường truyền trên vòng đơn không ngừng hoàn toàn hoạt động của mạng.
5. Đa số các mạng cục bộ Ethernet hiện nay đều sử dụng hình trạng …… vì khả năng mở rộng và dễ dàng kết nối với các mạng khác.
   a. STAR b. BUS c. RING
6. Mạng cục bộ Ethernet sử dụng (chọn 2)
   a. Hình trạng Star –wired – bus b. Hình trạng Star –wired – ring
   c. Giao thức truyền thẻ bài d. Giao thức CSMA/CD
7. CSMA/CD là một giao thức truy xuất đường truyền (chọn):
   a. Có điều khiển và xác định b. Ngẫu nhiên c. Cả hai
8. Dữ liệu (và cả thẻ bài ) trong các hình trạng RING di chuyển theo:
   a. Một chiều b. Cả hai chiều c. Quảng bá (broadcast)
9. Mỗi kiểu khuôn dạng (frame) Ethernet có các phần khác nhau nhưng chúng đều có **bốn** trường chung:
   a. Source addres b. Destination address c. Length
   d. Data e. Error-checking information
10. Phát biểu nào là đúng trong các phát biểu sau (chọn 1):
    a. Tổng số tối đa các trạm khi dùng cáp Ethernet dày (10Base5) là: 200 trạm
    b. Khoảng cách tối đa từ trạm tới LAN một MAU dùng cáp IBM loại 3 là 100 m
    c. Để mở rộng mạng *Token Ring* các cáp IBM loại 6 thường được ghép với nhau.

# CHƯƠNG 6 – GIỚI THIỆU WINDOWS 2000

## MỤC TIÊU CỦA CHƯƠNG

*Kết thúc chương này bạn có thể:*

- Biết được các phiên bản của Windows 2000
- Một số đặc điểm mới của Windows 2000
- Các mô hình làm việc trên Windows 2000

## 6.1 Các phiên bản của Windows 2000

Windows 2000 là hệ điều hành máy chủ được sử dụng phổ biến nhất hiện nay của Microsoft. Nó được xây dựng trên nền của kỹ thuật Windows NT, nhưng nó tin cậy, linh động, dễ phát triển, dễ quản lý và sử dụng hơn bất kỳ phiên bản nào trước kia của Windows. Gia đình Windows 2000 có bốn hệ điều hành: *Windows 2000 Professional, Windows 2000 Server*, *Windows 2000 Advanced Server* và *Windows 2000 Datacenter Server*. Chúng được tóm tắt trong bảng sau:

| Hệ điều hành | Mô tả |
|---|---|
| **Windows 2000 Professional** | Windows 2000 Professional thay thế cho Windows 95, Windows 98 và Windows NT 4.0 Workstation. Nó được thiết kế cho các loại máy tính cá nhân để bàn. |
| **Windows 2000 Server** | Windows 2000 Server có tất cả các đặc tính của Windows 2000 Professional, cộng thêm các dịch vụ quản lý mạng. Phiên bản này của Window 2000 rất lý tưởng đối với các dịch vụ file và máy in, dịch vụ Web và nhóm làm việc. |
| **Windows 2000 Advanced Server** | Windows 2000 Advanced Server có tất cả các đặc điểm của Windows 2000 Server, thêm các tính năng như có thể cho phép nhiều người dùng tài nguyên hệ thống cùng một lúc. Phiên bản này của Windows 2000 được thiết kế để quản lý cho các mạng xí nghiệp và các cơ sở dữ liệu chuyên dùng. |
| **Windows 2000 Datacenter Server** | Windows 2000 Datacenter Server có tất cả các đặc điểm của Windows 2000 Advanced Server, cộng thêm chức năng hỗ trợ nhiều bộ nhớ hơn và nhiều CPU trên một máy tính. Windows 2000 Datacenter Server là mạnh nhất trong gia Windows 2000. Nó được thiết kế để quản lý kho dữ liệu lớn, xử lý giao dịch trực tuyến và giả lặp mềm dẻo và các dự án hợp nhất máy chủ. |

## 6.2 Một số đặc điểm mới của Windows 2000

Mặc dù Windows 2000 được xây dựng trên nền tảng của Windows NT, nhưng nó có nhiều tính năng nổi bật hơn so với các phiên bản trước của Windows, bao gồm:

| Các đặc điểm | Mô tả |
|---|---|
| **Active Directory** | Active Directory là dịch vụ thư mục có thể phục vụ nhiều người dùng, được xây dựng từ cơ sở bằng cách sử dụng công nghệ chuẩn Internet, và tích hợp đầy đủ mức hệ điều hành. Active Directory đơn giản hoá việc quản trị và giúp cho người dùng dễ dàng tìm kiếm tài nguyên. Active Directory cung cấp nhiều đặc điểm và khả năng, bao gồm chính sách nhóm, nhiều người cùng làm việc mà không phức tạp, hỗ trợ nhiều giao thức thẩm định quyền, và sử dụng các chuẩn của Internet. |
| **Active Directory Service Interfaces (ADSI)** | ADSI là mô hình dịch vụ thư mục và là tập của các giao diện Component Object Service Model (COM). Nó cho phép các ứng dụng chạy trên các hệ điều hành Windows 95, Windows 98, Windows NT, và Windows 2000 truy xuất nhiều dịch vụ mạng trực tiếp, bao gồm Active Directory. Nó được cung cấp như một công cụ phát triển phần mềm (Software Development Kit - SDK). |
| **Asynchronous Transfer Mode (ATM)** | ATM là giao thức hướng nối kết và tốc độ cao, được thiết kế để truyền nhiều loại dữ liệu trên mạng. Nó thích hợp cho cả các mạng cục bộ (LAN) và các mạng diện rộng (WAN). Dùng ATM, có thể đồng thời truyền nhiều loại dữ liệu như: âm thanh, dữ liệu, hình ảnh, và video qua mạng. |
| **Certificate Services** | Sử dụng Certificate Services và các công cụ quản lý chứng nhận trong Windows 2000, bạn có thể triển khai các khoá công cộng của mình. Với khoá công cộng, bạn có thể hiện thực các kỹ thuật cơ bản chuẩn như khả năng đăng nhập thẻ thông minh, sự thẩm định quyền khách hàng (thông qua Secure Sockets Layer và Transport Layer Security), bảo mật thư điện tử, chữ ký điện tử và bảo mật kết nối (sử dụng Internet Protocol Security). |
| **Component Services** | Component Services là một tập hợp các dịch vụ cơ bản trên phần mở rộng của Component Object Model (COM) và trên Microsoft Transaction Server. Component Services cung cấp sự cải thiện luồng và bảo mật, quản lý giao dịch, đối tượng dùng chung, hàng đợi hợp thành, quản trị ứng dụng và đóng gói. |
| **Hỗ trợ hạn ngạch đĩa** | Bạn có thể dùng các hạn ngạch đĩa khi định dạng dung tích đĩa với hệ thống file NTFS, để giám sát và giới hạn khối lượng của không gian đĩa cho từng người dùng. Bạn có thể định nghĩa những đáp ứng khi người dùng sử dụng vượt qúa ngưỡng cho phép của họ. |

| Các đặc điểm | Mô tả |
|---|---|
| **Dynamic Host Configuration Protocol (DHCP) with Domain Name System (DNS) and Active Directory** | DHCP làm việc với DNS và Active Directory trên các mạng Internet Protocol (IP), giải phóng bạn khỏi việc gán và kiểm tra địa chỉ tĩnh. DHCP gán địa chỉ IP tự động đến các máy tính hoặc các nguồn tài nguyên khác kết nối tới mạng IP. |
| **Encrypting File System (EFS)** | EFS trong Windows 2000 bổ sung điều khiển truy xuất hiện có và thêm vào mức mới bảo vệ dữ liệu của bạn. Hệ thống mã hoá file thực thi như dịch vụ hệ thống tích hợp, làm nó dễ quản lý, khó bị thâm nhập và trong suốt với người sử dụng. |
| **Graphical Disk Management** | Disk Management là các công cụ đồ hoạ để quản lý đĩa cứng bao gồm nhiều đặc trưng mới, như hỗ trợ khối lượng động, quản lý đĩa trực tuyến, quản lý đĩa cục bộ và từ xa, Volume Mount Points. |
| **Group Policy (Một phần của Active Directory)** | Các chính sách có thể định nghĩa các hành động được phép và những cài đặt cho người sử dụng và máy tính. Trái với chính sách cục bộ, bạn có thể dùng chính sách nhóm để thiết lập các chính sách áp dụng cho các vị trí, miền hay tập tổ chức đã cho trong Active Directory. Quản lý dựa trên chính sách đơn giản hoá các thao tác nâng cấp hệ điều hành, cài đặt ứng dụng, hồ sơ người dùng, và khoá hệ thống màn hình. |
| **Indexing Service** | Chỉ mục dịch vụ cung cấp cách nhanh, dễ và bảo mật để người dùng tìm thông tin cục bộ hay trên mạng. Người dùng có thể dùng các câu truy vấn mạnh để tìm file trong các định dạng và ngôn ngữ khác nhau, qua lệnh Search của trình đơn Start hoặc qua các trang Hypertext Markup Language (HTML) mà chúng ta thấy trong các trình duyệt web. |
| **IntelliMirror** | IntelliMirror cung cấp các mức cao của việc điều khiển các hệ thống khách chạy trên hệ điều hành Windows 2000 Professional. Bạn có thể dùng IntelliMirror để định nghĩa các chính sách cơ bản tương ứng với công việc của người dùng, các thành viên nhóm và vị trí. Sử dụng các chính sách này nền màn hình Windows 2000 Professional được cấu hình tự động để làm quen với các yêu cầu của người dùng riêng biệt mỗi lần người dùng đăng nhập vào mạng, bất kể là người dùng đăng nhập từ đâu. |
| **Internet Authentication Service (IAS)** | IAS cung cấp một điểm tập trung để quản lý thẩm định quyền, quyền hạn, tài khoản và kiểm tra người dùng dial-up hoặc Virtual Private Network. IAS dùng giao thức Internet Engineering Task Force (IETF) gọi là Remote Authentication Dial-In User Service (RADIUS). |

| Các đặc điểm | Mô tả |
|---|---|
| **Internet Connection Sharing** | Với đặc điểm chia sẻ nối kết Internet của Network and Dial-Up Connections, bạn có thể sử dụng Windows 2000 để kết nối mạng gia đình của mình hoặc mạng văn phòng nhỏ tới Internet. Thí dụ, bạn phải có mạng gia đình để kết nối tới Internet bằng cách sử dụng kết nối dial-up. Bằng cách cho phép máy tính kết nối chia sẻ với Internet qua kết nối dial-up, bạn đang cung cấp cách thông dịch địa chỉ mạng, địa chỉ hoá, và các dịch vụ phân giải tên đối với tất cả các máy tính trên mạng của mình. |
| **Internet Information Services (IIS) 5.0** | Các đặc điểm mạnh trong Internet Information Services (IIS), như một phần của Microsoft Windows 2000 Server, làm nó dễ chia sẻ tài liệu và thông tin qua mạng intranet hoặc Internet. Dùng IIS, bạn có thể triển khai một cách linh hoạt và tin cậy các ứng dụng Web-based, và bạn có thể chuyển các dữ liệu và ứng dụng đang tồn tại tới Web. IIS bao gồm Active Server Pages và các đặc trưng khác. |
| **Hỗ trợ Internet Security (IPSec)** | Dùng IPSec để bảo mật giao tiếp bên trong mạng intranet và khởi tạo các giải pháp bảo mật Virtual Private Network trên Internet. IPSec được thiết kế bởi IETF và là chuẩn công nghiệp để mã hoá Transmission Control Protocol/Internet Protocol (TCP/IP). |
| **Hỗ trợ Kerberos V5 Protocol** | Kerberos V5 là giao thức thẩm định quyền mạng công nghiệp chuẩn. Với hỗ trợ Kerberos V5 việc sử lý đăng nhập nhanh và đơn giản cho người dùng truy xuất các nguồn tài nguyên của mạng, như các môi trường khác để hỗ trợ giao thức này. Sự hỗ trợ đối với Kerberos V5 bao gồm việc thêm các lợi ích như là thẩm định quyền lẫn nhau và uỷ nhiệm quyền thẩm định. |
| **Hỗ trợ Layer 2 Tunnelling Protocol (L2TP)** | L2TP là phiên bản bảo mật hơn Point-to-Point Tunnelling Protocol (PPTP) và được dùng để đường ống hoá, chỉ định địa chỉ và thẩm định quyền. |
| **Hỗ trợ Lightweight Directory Access Protocol (LDAP)** | LDAP là giao thức truy xuất chính Active Directory và là một chuẩn công nghiệp. Phiên bản LDAP 3 được thiết kế bởi IETF. |
| **Message queuing** | Tích hợp chức năng hàng đợi tin nhắn trong Windows 2000 giúp những người phát triển xây dựng và phát triển các ứng dụng làm nó chạy tin cậy hơn trên môi trường mạng. Các ứng dụng này có thể điều khiển các ứng dụng chạy trên các nền khác nhau như các hệ thống máy tính lớn và các hệ thống trên cơ sở UNIX. |
| **Microsoft Management Console (MMC)** | Dùng MMC để sắp xếp các công cụ quản lý và các quá trình bạn cần bên trong giao diện đơn. Bạn cũng có thể uỷ nhiệm các thao tác tới người dùng cụ thể bằng cách khởi tạo các màn hình điều khiển MMC cấu hình trước cho chúng. Màn hình điều khiển sẽ cung cấp các công cụ mà bạn lựa chọn cho người dùng. |

| Các đặc điểm | Mô tả |
|---|---|
| **Network Address Translation (NAT)** | NAT ẩn bên trong địa chỉ IP từ các mạng bên ngoài bằng cách truyền địa chỉ trong riêng tới địa chỉ ngoài chung. Điều này giảm thiểu chi phí việc đăng ký địa chỉ IP bằng cách cho phép bạn dùng địa chỉ IP bên trong chưa đăng ký, với việc truyền một số nhỏ của địa chỉ IP bên ngoài đã đăng ký. Nó cũng che dấu cấu trúc mạng bên trong, giảm sự rủi ro do những việc tấn công các hệ thống bên trong. |
| **Operating system migration, support, and integration** | Windows 2000 hợp nhất liền một khối với các hệ thống đang tồn tại và bao gồm sự hỗ trợ đối với các hệ điều hành Windows trước đây, như những đặc trưng mới để hỗ trợ các hệ điều hành chung khác. Windows 2000 cung cấp: thao tác giữa các phần với Windows NT Server 3.51 và 4.0; hỗ trợ cho các máy khách đang chạy nhiều loại hệ điều hành như Windows 3.x, Windows 95, Windows 98, và Windows NT Workstation 4.0; Máy tính lớn với khoảng cách kết nối trung bình, sử dụng các cổng giao dịch và hàng đợi S/390 và AS/400 qua Systems Network Architecture (SNA) Server; File Server cho máy Macintosh, cho phép máy khách Macintosh sử dụng giao thức TCP/IP (AppleTalk File Protocol (AFP) qua IP) để chia sẻ các file và truy cập chia sẻ trên máy chủ Windows 2000. |
| **Plug and Play** | Với Plug and Play, tổ hợp hỗ trợ của phần cứng và phần mềm, máy chủ có thể nhận biết và thích ứng với cấu hình phần cứng tự động thay đổi, không cần sự can thiệp và khởi động lại. |
| **Public key infrastructure (PKI) and smart card infrastructure** | Dùng Certificate Services và các công cụ quản lý chứng chỉ trong Windows 2000, bạn có thể triển khai cơ sở hạ tầng khoá công cộng. Với cơ sở hạ tầng khoá công cộng, bạn có thể hiện thực kỹ thuật cơ bản chuẩn như các khả năng đăng nhập thẻ thông minh, sự thẩm định quyền máy khách (qua Secure Sockets Layer và Transport Layer Security), bảo mật e-mail, chữ ký điện tử, và bảo mật kết nối (dùng Internet Protocol Security). Dùng Certificate Services, bạn có thể cài đặt và quản lý các chứng nhận quyền truy xuất mà nó cấp và thu hồi các chứng chỉ X.509V3. Cách thức này cho phép bạn không phụ thuộc vào các dịch vụ thẩm định quyền máy khách thương mại, mặc dù bạn có thể tích hợp việc thẩm định quyền máy khách thương mại bên trong cơ sở hạ tầng khoá công cộng của bạn nếu bạn chọn. |
| **Quality of Service (QoS)** | Dùng QoS, bạn có thể điều khiển các ứng dụng đã được phân phối trên băng thông mạng. Bạn có thể cho các ứng dụng quan trọng nhiều băng thông hơn, và các ứng dụng ít quan trọng ít băng thông hơn. Các dịch vụ tựa QoS và các giao thức cung cấp hệ thống phân phối thông tin trên mạng nhanh, bảo đảm, end-to-end. |

| Các đặc điểm | Mô tả |
|---|---|
| **Remote Installation Services (RIS)** | Với Remote Installation Services, bạn có thể cài đặt Windows 2000 Professional từ xa, mà không cần cài đặt trực tiếp trên mỗi máy khách. Các máy đích phải hoặc là hỗ trợ khởi động từ xa với Pre-Boot eXecution Environment (PXE) ROM, hoặc là phải được khởi động từ xa bằng đĩa mềm. Việc cài đặt cho nhiều máy khách trở nên đơn giản hơn nhiều. |
| **Removable Storage and Remote Storage** | Removable Storage làm nó dễ kiểm tra phương tiện lưu trữ có thể tháo dời và quản lý các thư viện phần cứng, như là các hộp ổ cứng nắp ngoài. Ổ cứng điều khiển từ xa dùng tiêu chuẩn mà bạn chỉ định để tự động việc sao chép các file ít sử dụng để di chuyển thiết bị truyền thông. Nếu không gian đĩa cứng bị giảm dưới mức xác định, Remote Storage xoá nội dung file chứa trên đĩa. Nếu file được dùng sau này thì nội dung của nó sẽ được tự động lấy lại từ nơi lưu trữ. Vì giá thành tính trên 1 MB của đĩa quang học và băng từ nhỏ hơn của ổ cứng, nên nó có thể giảm giá thành mạng của bạn. |
| **Routing and Remote Access service** | Routing and Remote Access service là dịch vụ tích hợp đơn mà các thiết bị đầu cuối kết nối từ các máy khách hoặc bằng dial-up hoặc bằng Virtual Private Network (VPN), hoặc thực hiện tìm đường (IP, IPX, and AppleTalk) hoặc cả hai. Với việc tìm đường và truy xuất từ xa, Windows 2000 server của bạn có thể hoạt động như dịch vụ truy xuất từ xa, máy chủ VPN , cổng vào hoặc tìm đường. |
| **Safe mode startup** | Với chế độ an toàn, bạn có thể khởi động Windows 2000 với tập tối thiểu các trình điều khiển và các dịch vụ, và do đó bạn sẽ thấy chuỗi các sự kiện lúc khởi động. Sử dụng chế độ an toàn, bạn có thể chuẩn đoán các vấn đề của các trình điều khiển và các thành phần khác mà bị ngăn cản bởi khởi động chuẩn. |
| **Cơ sở hạ tầng thẻ thông minh** | Dùng Certificate Services và các công cụ quản lý chứng chỉ trong Windows 2000, bạn có thể phát triển cơ sở hạ tầng khoá công cộng của bạn. Với chúng bạn có thể hiện thực các kỹ thuật chuẩn cơ sở như thẻ đăng nhập thông minh, thẩm định quyền máy khách (qua Secure Sockets Layer và Transport Layer Security), bảo mật thư điện tử, chữ ký điện tử, và bảo mật nối kết (dùng Internet Protocol Security). |
| **TAPI 3.0** | TAPI 3.0 hợp nhất IP và hệ thống điện thoại truyền thống để cho phép những nhà phát triển máy tính tạo thế hệ mới các ứng dụng hệ thống điện thoại máy tính để làm việc bằng Internet hay intranet trên hệ thống mạng điện thoại truyền thống. |

| Các đặc điểm | Mô tả |
|---|---|
| **Terminal Services** | Gia đình Windows 2000 Server chỉ cho phép những hệ điều hành máy chủ tích hợp các dịch vụ giả lặp đầu cuối. Dùng Terminal Services, người dùng có thể truy xuất các chương trình đang chạy trên các máy trạm từ nhiều thiết bị cũ hơn. Thí dụ, người dùng có thể truy xuất màn hình nền Windows 2000 Professional ảo và các ứng dụng trên nền Windows 32-bit từ phần cứng mà không thể chạy phần mềm cục bộ. Terminal Services cung cấp khả năng này cho cả các thiết bị của máy khách chạy hệ điều hành Windows và các hệ điều hành khác |
| **Mạng riêng ảo (Virtual Private Network - VPN)** | Bạn có thể cho phép người dùng sẵn sàng truy cập mạng ngay cả khi họ ở ngoài văn phòng và giảm giá truy xuất, bằng cách hiện thực VPN. Dùng VPN, người dùng có thể kết nối dễ dàng và bảo mật tới mạng công ty. Sự kết nối thông qua Internet Service Provider (ISP) cục bộ làm giảm thời gian kết nối. Với Windows 2000 Server, bạn có thể dùng các giao thức bảo mật hơn để tạo Virtual Private Networks, bao gồm: L2TP - một phiên bản bảo mật hơn của PPTP và IPSec - một giao thức cơ sở chuẩn để cung cấp các mức cao nhất việc bảo mật VPN. Dùng IPSec, mọi thứ trên lớp mạng có thể được mã hoá. |
| **Windows Media Services** | Dùng Windows Media Services, bạn có thể truyền đa phương tiện chất lượng cao cho người dùng Internet và intranet. |
| **Windows Script Host (WSH)** | Dùng WSH, bạn có thể tự động hoá các hành động như tạo nối tắt, kết nối và bỏ kết nối với máy chủ mạng. WSH phụ thuộc ngôn ngữ. Bạn có thể viết các kịch bản dưới những ngôn ngữ kịch bản thông thường như VBScript và JScript. |

## 6.3 Mô hình workgroup và mô hình domain trong Windows 2000

Sau khi kết nối máy tính của mình tới mạng, bạn có thể chia sẻ các file, các máy in, và thư điện tử với các máy tính khác. Có một vài khái niệm cơ bản cần biết để thiết kế cấu trúc file và cài đặt hệ thống của bạn.

**Workgroup hay Domain**

Khi cài đặt Windows 2000 Professional hoặc Server trong môi trường mạng, chúng có thể được cài đặt hoặc là **workgroup** hoặc là **domain.**

### a) Windows 2000 Workgroup

Windows 2000 *workgroup* là một nhóm máy tính mạng cùng chia sẻ tài nguyên như file dữ liệu, máy in. Nó là một nhóm lôgíc của các máy tính mà tất cả chúng có cùng tên nhóm. Có thể có nhiều nhóm làm việc (workgroups) khác nhau cùng kết nối trên một mạng cục bộ (LAN).

Workgroups cũng được coi là mạng peer-to-peer bởi vì tất cả các máy trong workgroup có quyền chia sẻ tài nguyên như nhau mà không cần sự chỉ định của Server. Mỗi máy tính trong nhóm tự bảo trì, bảo mật cơ sở dữ liệu cục bộ của nó. Điều này có nghĩa là, tất cả sự quản trị về tài khoản người dùng, bảo mật cho nguồn tài nguyên chia sẻ không được tập trung hoá. Bạn có thể kết nối tới một nhóm đã tồn tại hoặc khởi tạo một nhóm mới.

❖ *Ưu điểm của Windows 2000 Workgroup:*

- Workgroups không yêu cầu máy tính chạy trên hệ điều hành Windows 2000 Server để tập trung hoá thông tin bảo mật.
- Workgroups thiết kế và hiện thực đơn giản và không yêu cầu lập kế hoạch có phạm vi rộng và quản trị như domain yêu cầu.
- Workgroups thuận tiện đối với nhóm có số máy tính ít và gần nhau (<=10 máy).

❖ *Nhược điểm của Windows 2000 workgroup:*

- Mỗi người dùng phải có một tài khoản người dùng trên mỗi máy tính mà họ muốn đăng nhập.
- Bất kỳ sự thay đổi tài khoản người dùng, như là thay đổi password hoặc thêm tài khoản người dùng mới, phải được làm trên tất cả các máy tính trong workgroup. Nếu bạn quên bổ sung tài khoản người dùng mới tới một máy tính trong nhóm thì người dùng mới sẽ không thể đăng nhập vào máy tính đó và không thể truy xuất tới tài nguyên của máy tính đó.
- Việc chia xẻ thiết bị và file được xử lý bởi các máy tính riêng, và chỉ cho người dùng có tài khoản trên máy tính đó được được sử dụng.

### b) Windows 2000 Domain

Windows 2000 *domain* là một nhóm máy tính mạng cùng chia sẻ *cơ sở dữ liệu thư mục tập trung* (**central directory database**)**.** Thư mục dữ liệu chứa tài khoản người dùng và thông tin bảo mật cho toàn bộ Domain. Thư mục dữ liệu này được biết như là thư mục hiện hành (**Active Directory**).

Trong một Domain, thư mục chỉ tồn tại trên các máy tính được cấu hình như *máy điều khiển miền* (**domain controller**)**.** Một **domain controller là** một Server quản lý tất cả các khía cạnh bảo mật của Domain. Không giống như Windows 2000 workgroup, bảo mật và quản trị trong domain được tập trung hoá. Chỉ những máy tính đang chạy Windows 2000 Server mới có thể được thiết kế là các Domain controller.

Một domain không được xem như một vị trí đơn hoặc cấu hình mạng riêng biệt. Các máy tính trong cùng domain có thể ở trên một mạng LAN nhỏ hoặc có thể được đặt trong các nước khác nhau trên thế giới. Chúng có thể giao tiếp với nhau qua bất kỳ kết nối vật lý nào, như: dial-up, Integrated Services Digital Network (ISDN), fibre, Ethernet, Token Ring, Frame Relay, satellite, or leased lines.

❖ *Ưu điểm của Windows 2000 Domain:*

- Cho phép quản trị tập trung. Nếu người dùng thay đổi password của họ, thì sự thay sẽ được cập nhật tự động trên toàn Domain.
- Domain cung cấp quy trình đăng nhập đơn giản để người dùng truy xuất các tài nguyên mạng mà họ được phép truy cập.
- Domain cung cấp linh động để người quản trị có thể khởi tạo mạng rất rộng lớn.

Các miền Windows 2000 điển hình có thể chứa các kiểu máy tính sau :

| Kiểu máy tính | Mô tả |
|---|---|
| **Máy điều khiển miền (Domain controllers) – Windows 2000 Server** | Mỗi Domain controller cất trữ và bảo trì bản sao thư mục. Trong domain, tài khoản người dùng được tạo một lần, Windows 2000 ghi nó trong thư mục này. Khi người dùng đăng nhập tới máy tính trong domain, domain controller kiểm tra thư mục nhờ tên người sử dụng, mật khẩu và giới hạn đăng nhập. Khi có nhiều domain controllers, chúng định kỳ tái tạo thông tin thư mục của chúng. |
| **Các máy chủ thành viên (Member servers) – Windows 2000 Server** | Một *member server* là bất kỳ máy chủ nào mà không được cấu hình như là domain controller. Máy chủ không cất thông tin thư mục và không thể xác nhận domain người dùng. Các máy chủ cung cấp các tài nguyên chia sẻ như các thư mục dùng chung hay các máy in. |
| **Các máy tính trạm (Client computers) – Windows 2000 Professional** | Các máy tính trạm chạy một môi trường màn hình nền của người dùng và cho phép người dùng truy cập tới nguồn tài nguyên trong domain. |

Không giống như Workgroup, Domain phải tồn tại trước khi bạn tham gia vào nó. Việc tham gia vào Domain luôn yêu cầu người quản trị Domain cấp tài khoản cho máy tính của bạn tới domain đó. Tuy nhiên, nếu người quản trị cho bạn đúng đặc quyền, bạn có thể khởi tạo tài khoản máy tính của bạn trong quá trình cài đặt.

# Câu hỏi ôn tập chương 6

1. Chọn đúng **ba** hệ điều hành mạng theo liệt kê sau:

   a. DOS b. Win 2000 c. Win 9x

   d. Linux e. Novel NetWare

2. WINS được cấu hình ở đâu trong trạm làm việc khách? (chọn 1)
   a. Trong đặc tính của bộ điều hợp mạng.
   b. Trong sự thiết lập của modem.
   c. Trong các đặc tính của TCP/IP .
   d. Trong sự thiết lập máy khách của Microsoft.
3. Chọn lựa nào phù hợp nhất để dùng WINS?
   a. Windows 3.11 workstation
   b. Linux server
   c. Novel Server
   d. Windows 2000 workstation
4. WINS thuộc về tầng nào trong mô hình OSI?
   a. Application
   b. Presentation
   c. Session
   d. Transport
5. Windows 2000 Server được phát triển từ …….
   a. Windows NT 4.0 Enterprise Edition
   b. Windows NT 4.0 Server
   c. Windows NT 5.0 Server
   d. None of the others

6. Hệ điều hành nào trong các hệ điều điều hành sau được thiết kế để hỗ trợ nhiều bộ nhớ và CPU hơn trên một máy tính?

   a. Windows 2000 Professional
   b. Windows 2000 Server
   c. Windows 2000 Advanced Server
   d. Windows 2000 Data Center Server

7. Member server là Domain Controller?

   a. Đúng. b. Sai.

8. Ưu điểm của Windows 2000 Domain là không phải quản trị tập trung?

   a. Đúng. b. Sai.

9. Workgroups cũng được coi là mạng peer-to-peer ?

   a. Đúng. b. Sai.

# CHƯƠNG 7 – CÀI ĐẶT WINDOWS 2000 SEVER

## MỤC TIÊU CỦA CHƯƠNG

*Kết thúc chương này bạn có thể:*

- Nắm được lý thuyết chung của việc cài đặt Windows 2000 Server
- Nắm được yêu cầu phần cứng tối thiểu cho việc cài đặt Windows 2000 Server
- Nắm được các bước của quá trình cài đặt

## 7.1 Cài đặt Windows 2000 Server

### 7.1.1 Chuẩn bị cho việc cài đặt

Giống như cách cài đặt các phiên bản khác của Windows, Windows 2000 Server cũng hướng dẫn từng bước cho chúng ta cài đặt. Tuy nhiên trước khi cài đặt, cần phải xem xét trước một vài điểm về hệ thống, thể hiện trong bảng sau:

| **Hãy xem xét các điểm sau …** |
|---|
| Yêu cầu ổ cứng tối thiểu còn chưa sử dụng là: 2GB (Gigabytes). |
| Kiểm tra các phần cứng trong máy (network adapters, video drivers, sound cards, CD-ROM drives, PC cards v.v...) có tồn tại trong **Windows 2000 Hardware Compatibility List (HCL).** |
| Xác định phần ổ đĩa bạn sẽ cài Windows 2000 Server. |
| Chọn hệ thống file phù hợp với yêu cầu của bạn – **NTFS** hoặc **FAT16/FAT32.** Bạn nên chọn NTFS trừ khi bạn cần chạy nhiều hơn một hệ điều hành trên máy tính của bạn, hoặc máy tính của bạn cần sử dụng một vài phần mềm cũ (Xem xét nâng cấp phần mềm cũ sử dụng NTFS). |
| Lựa chọn kiểu per-seat hay per- server. Bạn có thể chuyển từ per-seat sang per-server, nhưng chiều ngược lại thi không được. |
| Chọn loại mạng bạn sẽ kết nối – Workgroup hay Domain. Nếu bạn đang kết nối domain, bạn cần thêm thông tin như là tên domain và tên tài khoản máy tính đã khởi tạo cho bạn. Với tài khoản quản trị và mật khẩu trong domain, bạn có thể khởi tạo tài khoản máy tính trong domain. |
| Chọn cài đặt mới hoặc nâng cấp từ Windows NT Server. Windows NT Workstation and Windows 9*x* không thể nâng cấp thành Windows 2000 Server. |
| Chọn phương pháp cài đặt: từ đĩa khởi động, CD-ROM hay mạng. |
| Chọn các thành phần bạn cần cài đặt, như Networking Services hay Microsoft Networking Service. |

### 7.1.2 Yêu cầu phần cứng tối thiểu

Máy tính của bạn phải phù hợp với yêu cầu phần cứng tối thiểu, trước khi bạn cài đặt Windows 2000 Server. Các yêu cầu được liệt kê theo bảng sau:

| Thành phần | Yêu cầu tối thiểu |
|---|---|
| Processor | 32-bit Pentium 133 MHz. |
| Không gian đĩa cứng còn trống | Ổ cứng tối thiểu còn trống là 671 MB (Đề nghị là 2 GB). |
| Bộ nhớ RAM | 64 MB đối với mạng có ít hơn 5 máy; 128 MB là yêu cầu tối thiểu với hầu hết các môi trường mạng. |
| Màn hình | Khả năng của màn hình VGA là 640 x 480 (đề nghị 1024 x 768). |
| Ổ đĩa CD-ROM | 12X hoặc đề nghị nhanh hơn; không yêu cầu khi cài đặt qua mạng. |
| Các ổ đĩa bổ sung | Đĩa mềm mật độ cao 3.5-inch, ngoại trừ máy bạn có thể khởi động từ CD-ROM. |
| Các thành phần tuỳ chọn | Chuột hay thiết bị trỏ khác. Đối với việc cài đặt qua mạng: một card mạng và hệ điều hành mạng dựa trên MS-DOS cho phép kết nối tới server chứa các file cài đặt Windows 2000. |

### 7.1.3 Các chương trình cài đặt Windows 2000 Server

Windows 2000 Server được cài đặt bằng cách sử dụng, hoặc là chương trình Winnt.exe hoặc Winnt32.exe, việc dùng chương trình cài đặt nào phụ thuộc vào hệ điều hành hiện tại đang sử dụng trên máy tính của bạn. Bạn cũng có thể sử dụng chương trình Setup.exe, nhưng thực sự nó thực hiện việc cài đặt trên Winnt.exe hoặc Winnt32.exe. Để cài đặt Windows 2000 Server trên máy tính đang chạy hệ điều hành MS-DOS hoặc Windows 3.x, bạn cần chạy file Winnt.exe từ thông số dòng lệnh của MS-DOS. Để cài trên các máy đang chạy hệ điều hành: Windows 95, Windows 98, Windows NT Workstation, Windows NT Server 3.51 hoặc Windows NT Server 4.0, bạn cho chạy file Winnt32.exe.

Windows 2000 Setup Program

Khi bạn thực thi chương trình Setup.exe, màn hình máy tính cho phép bạn cài đặt Windows 2000 Server, cài đặt các thành phần, các tùy chọn của đĩa CD, hoặc thoát khỏi chương trình cài đặt.

Nếu hệ thống của bạn cho phép chạy Autorun, Autorun gọi Setup.exe, chương trình này sẽ kiểm tra hệ thống của bạn. Nếu Setup xác định rằng máy tính của bạn đang chạy Windows NT Server 3.51, Windows NT Server 4.0, hoặc phiên bản trước Windows 2000 Server. Bạn cho phép máy hoặc nâng cấp hoặc cài đặt mới Windows 2000 Server. Nếu phiên bản trên hệ điều hành mới hơn Windows 2000 Server, Setup.exe sẽ không cho phép bạn cài đặt tiếp tục.

Winnt.exe Setup Program

Winnt.exe được sử dụng khi cài đặt từ máy đang chạy hệ điều hành MS-DOS hoặc Windows 3.x. Nó thường được sử dụng để cài đặt qua mạng cho máy trạm mạng MS-DOS. Winnt.exe thực hiện các bước sau:

- Khởi tạo thư mục tạm $WIN_NT$.~BT trên ổ đĩa và sao chép file khởi động cài đặt trên thư mục này.
- Khởi tạo thư mục tạm $WIN_NT$.~LS và sao chép các file Windows 2000 từ server vào thư mục này.
- Các dấu nhắc được sử dụng để khởi động lại hệ thống, trình đơn khởi động xuất hiện và quá trình cài đặt tiếp tục.

Winnt.exe cài đặt Windows 2000 Server và có thể được thực thi từ MS-DOS hoặc hệ điều hành Windows 16 bit từ thông số dòng lệnh. Có một số lựa chọn để thực thi chương trình Winnt.exe:

| Tuỳ chọn | Mô tả |
|---|---|
| /s[:*sourcepath*] | Định rõ vị trí nguồn của các file Windows 2000. Vị trí phải là đường dẫn đầy đủ. |
| /t[:*tempdrive*] | Chỉ thị việc cài đặt từ file tạm trên ổ đĩa định rõ và cài đặt Windows 2000 trên ổ đĩa đó. Nếu bạn không định rõ vị trí, việc cài đặt sẽ cố gắng thử định vị tới ổ cứng mặc định. |
| /u[:*answer file*] | Thực hiện cài đặt không giám sát. Việc trả lời file cung cấp trả lời tới một vài hoặc tất cả của lời nhắc trong suốt quá trình cài đặt. |
| /udf:id[,*UDF_file*] | Cho biết chỉ số nhận dạng mà quá trình cài đặt sử dụng để chỉ định làm thế nào sửa đổi Uniqueness Database File (UDF). Quá trình cài đặt nhắc bạn đưa đĩa chứa file $Unique$.udb. |
| /r[:*folder*] | Định rõ thư mục được cài đặt. Thư mục đó vẫn còn lại sau khi cài đặt xong. |
| /rx[:*folder*] | Định rõ thư mục lựa chọn để sao chép. Thư mục này bị xoá sau khi cài đặt xong. |
| /e | Định rõ lệnh thực thi tại lúc kết thúc cài đặt chế độ GUI. |
| /a | Cho phép lựa chọn khả năng truy xuất. |

Winnt32.exe Setup Program

Nếu máy tính của bạn sẽ cài Windows 2000 Server khi đang chạy các hệ điều hành: Windows 95, Windows 98, Windows NT Workstation, Windows NT Server 3.51 hoặc Windows NT Server 4.0, thì chương trình cài đặt Winnt32.exe sẽ được sử dụng để cài đặt. Bạn cũng có thể chạy Winnt32.exe từ thư mục gốc (chẳng hạn như \i386) trên đĩa

CD-ROM; hoặc thực thi Winnt32.exe từ thông số dòng lệnh từ Start Menu\run, khi hệ điều hành máy bạn đang chạy là Windows 95, Windows 98, hoặc Windows NT.

Nếu việc cài đặt Windows 2000 Server được cài đặt trên mạng, Winnt32.exe khởi tạo thư mục tạm $WIN_NT$.~LS và sao chép các file Windows 2000 Server từ server vào thư mục này. Thư mục tạm này được khởi tạo trên ổ đĩa đầu tiên mà nó đủ lớn, trừ khi bạn chọn /t. Việc này được gọi là *giai đoạn tiền sao chép* (Pre-Copy Phase) .

Các chọn lựa có thể được sử dụng với lệnh Winnt32.exe là:

| Tuỳ chọn | Mô tả |
|---|---|
| /s:*sourcepath* | Định rõ vị trí file nguồn Windows 2000. Để đồng thời sao chép file từ nhiều Server. Nếu bạn dùng nhiều /s, server đầu tiên phải sẵn sàng hoặc cài đặt sẽ thất bại. |
| /tempdrive:*drive_letter* | Điều khiển Setup đặt các file tạm trên phân hoạch xác định và cài đặt Windows 2000 trên ổ đó. |
| /Unattend or /u | Nâng cấp từ phiên bản trước của Windows 2000 trong chế độ cài đặt tự động. Tất cả các người dùng được lấy từ lần cài đặt trước, vì thế không có người dùng nào được thêm vào.<br>Dùng /unattend để tự động cài đặt xác nhận rằng bạn đang đọc và chấp nhận End-User License Agreement (EULA) cho Windows 2000. Trước khi dùng lựa chọn này để cài Windows 2000 với danh nghĩa là tổ chức khác hơn là bạn làm chủ, bạn phải xác nhận rằng người dùng cuối đã nhận, đọc và chấp nhận điều khoản của Windows 2000 EULA. OEMs có thể không định rõ khoá này trên máy nhượng lại từ những người dùng cuối. |
| /unattend[*num*][:*answer_file*] | Thực hiện làm tươi quá trình cài đặt trong chế độ cài đặt tự động. File trả lời cung cấp việc cài đặt với những mô tả tuỳ ý của bạn.. *Num* là số cộng thêm giữa thời gian cài đặt xong sao chép các file khi khởi động lại máy tính của bạn. Bạn có thể dùng số này trên bất kỳ máy tính đang chạy Windows NT hay Windows 2000. Trình lưu giữ *answer_file* là tên của file trả lời. |

| Tuỳ chọn | Mô tả |
|---|---|
| /copydir:*folder_name* | Khởi tạo và thêm danh mục bên trong danh mục mà các file Windows 2000 được cài đặt. Thí dụ, nếu danh mục nguồn chứa danh mục gọi là Private_drivers sửa đổi chỉ với vị trí (site) của bạn, bạn có thể gõ **/copydir:Private_drivers** để thực hiện việc sao chép danh mục tới danh mục Windows 2000 đã cài đặt của bạn. Do vậy vị trí danh mục mới sẽ là %systemroot%\Private_drivers. Bạn có thể dùng /copydir để tạo các thư mục bổ sung nếu bạn muốn. |
| /copysource:*folder_name* | Khởi tạo các thư mục tạm bên trong thư mục mà các file Windows 2000 được cài đặt. Thí dụ, nếu thư mục nguồn chứa thư mục gọi là Private_drivers sửa đổi chỉ với vị trí (site) của bạn, bạn có thể gõ **/copysource:Private_drivers** để thực hiện việc sao chép thư mục tới thư mục Windows 2000 đã cài đặt của bạn và sử dụng các file của nó trong suốt quá trình cài đặt. Do vậy vị trí thư mục mới sẽ là %systemroot%\Private_drivers. Khác với các thư mục được tạo bằng /copydir, các thư mục tạo bằng /copysource bị xoá sau khi quá trình cài đặt hoàn thành. |
| /cmd:*command_line* | Chỉ thị cài đặt tiến hành ra lệnh cụ thể trước giai đoạn kết thúc của quá trình cài đặt. Công việc này xuất hiện sau khi máy tính của bạn khởi động lại hai lần và sau khi cài đặt sưu tập thông tin cấu hình cần thiết, nhưng trước khi quá trình cài đặt hoàn thành. |
| /debug[*level*][:*filename*] | Tạo bản ghi gỡ rối mức danh nghĩa, thí dụ /debug4:C:\ Win2000.log. File mặc định là %systemroot%\Winnt32.log, với mức gỡ rối đặt là 2: Có các mức sau: 0-severe errors, 1-errors, 2-warnings, 3-information, và 4- chi tiết thông tin cho gỡ rối. Mỗi mức bao gồm các mức thấp hơn nó. |
| /udf:*id*[,*UDF_file*] | Biểu thị định danh mà quá trình cài đặt dùng để chỉ rõ việc sửa đổi và sự giải đáp file Uniqueness Database File (UDF) (see the /unattend entry). UDF ghi đè giá trị trong file giải đáp và xác định giá trị trong UDF được dùng. Thí dụ, /udf:RAS_user, Our_company.udb ghi đè việc cài đặt đã xác định cho định danh RAS_user trong file Our_company.udb. Nếu không có một UDF được xác định, Setup nhắc nhở người dùng đưa đĩa chứa file $Unique$.udb. |

| Tuỳ chọn | Mô tả |
|---|---|
| /syspart:*drive_letter* | Chỉ rõ rằng bạn có thể sao chép các fie bắt đầu cài đặt từ ổ cứng, đánh dấu đĩa hoạt động, và sau đó cài đặt đĩa trên máy tính khác. Khi bạn bắt đầu với máy tính đó, nó tự động khởi động với giai đoạn kế tiếp của quá trình cài đặt. Bạn phải luôn luôn sử dụng thông số /tempdrive với thông số /syspart.<br>Chọn /syspart khi chạy Winnt32.exe chỉ từ máy tính đang chạy Windows NT 3.51, Windows NT 4.0, hoặc Windows 2000. Nó không thể chạy từ Windows 9*x*. |
| /checkupgradeonly | Kiểm tra máy tính của bạn để nâng cấp tương thích với Windows 2000. Đối với Windows 9x, việc cài đặt tạo một báo cáo với tên là Upgrade.txt trong thư mục cài đặt Windows. Với việc nâng cấp từ Windows NT 3.51 hay 4.0, nó cất file báo cáo là Winnt32.log trong thư mục cài đặt. |
| /cmdcons | Thêm tùy trọn Recovery Console để hệ điều hành lựa chọn màn hình, sửa chữa lỗi cài đặt. |
| /m:*folder_name* | Định rõ rằng quá trình cài đặt sao chép các file thay thế từ vị trí luân phiên. Chỉ dẫn việc cài đặt xem vị trí luân phiên đầu tiên, và nếu các file có mặt, sử dụng chúng thay vì phải dùng các file từ vị trí mặc định. |
| /makelocalsource | Chỉ thị việc cài đặt sao chép tất cả các file nguồn cài đặt tới ổ cứng cục bộ của bạn. Sử dụng /makelocalsource khi cài đặt từ CD để cung cấp các file cài đặt. |
| /noreboot | Chỉ thị việc cài đặt không khởi động lại máy tính sau giai đoạn sao chép file của Winnt32 được hoàn thành để mà bạn có thể thực thi một lệnh khác. |

### 7.1.4 Các giai đoạn của quá trình cài đặt.

Có ba giai đoạn trong quá trình cài đặt Windows 2000 Server là: *Pre-Copy Phase*, *Text mode*, và *GUI mode*.

**a. Giai đoạn trước khi sao chép (Pre-Copy)**

Giai đoạn tiền sao chép của quá trình cài đặt là khi tất cả các file cần để cài đặt được sao chép vào thư mục tạm trên ổ cứng cục bộ. Khi Winnt.exe hoặc Winnt32.exe được dùng để cài Windows 2000 Server trên mạng, các file cài đặt được sao chép vào thư mục tạm $WIN_NT$.~LS trên ổ cứng. Quá trình cài đặt tiếp tục như là nó được thực hiện trên ổ cứng cục bộ.

Bạn có thể chọn không tạo đĩa mềm khởi động bằng cách chọn hộp chọn *Copy All Setup Files From The Setup CD To The Hard Drive*. Khi bạn lựa chọn tùy chọn này, thư mục $WIN_NT$.~BT được khởi tạo trên ổ cứng cục bộ. Thư mục này chứa các file mà có thể chứa trong 4 đĩa mềm.

**b. Chế độ văn bản (Text Mode)**

Sau quá trình Pre-Copy là phần Text mode. Bạn sẽ được nhắc các thông tin cần thiết để hoàn tất quá trình cài đặt. Sau khi bạn chấp nhận bản quyền, bạn chỉ định hay khởi tạo ổ đĩa cài đặt. Tất cả các file yêu cầu để cài đặt được sao chép từ thư mục tạm (hoặc CD-ROM).

- *Thỏa thuận bản quyền Windows 2000 Server*

Sự thoả thuận bản quyền Windows 2000 Server được trình bày trên nhiều trang. Bạn có thể dùng phím Page Down để xem hết văn bản, và nhấn phím F8 khi đọc hết để chấp nhận bản quyền này.

- *Cài đặt trên hệ điều hành đã tồn tại (Existing Installations)*

Nếu quá trình cài đặt nhận ra là đã tồn tại Windows 2000, nó sẽ hiển thị một danh sách cho phép bạn chọn sự cài đặt ( nhấn R để sửa chữa, hoặc Esc để cài đặt tiếp tục).

- *Partitions*

Quá trình cài đặt hiển thị tất cả các ổ cứng hiện hữu và phần ổ chưa sử dụng. Dùng phím Up, Down bạn có thể lựa chọn ổ cứng bạn muốn cài Windows 2000 Server. Tại thời điểm này bạn có thể xoá hoặc khởi tạo ổ đĩa.

- *File Systems*

Quá trình cài đặt cho phép bạn chọn để giữ file hệ thống như cũ hoặc cho phép bạn chuyển đổi nó thành NTFS. Nếu bạn không muốn thay đổi nó, chọn Leave Current File System Intact (default), nhấn Enter để tiếp tục.

Quá trình cài đặt khảo sát ổ cứng của bạn và sao chép các file cần cài đặt từ thư mục tạm tới thư mục cài đặt (mặc định là \WINNT).

**c. Chế độ giao diện đồ họa (GUI Mode)**

Ngay khi chế độ văn bản của quá trình cài đặt hoàn tất, máy tính khởi động lại và bắt đầu chế độ giao diện đồ hoạ. Phần này của quá trình cài đặt cho phép bạn chọn các thành phần để cài đặt. Nó cũng nhắc nhập mật khẩu của quản trị viên.

Có ba giai đoạn tạo thành GUI Mode

1. Lấy lại thông tin về máy tính của bạn
2. Cài đặt mạng Windows 2000 Server
3. Hoàn thành quá trình cài đặt.

❖ *Lấy lại thông tin về máy tính của bạn*

Giai đoạn đầu tiên này của GUI Mode bao gồm nhiều hộp thoại mà Windows 2000 Server dùng để thu thập thông tin cấu hình để cài đặt hệ thống. Trong suốt giai đoạn này, các đặc trưng bảo mật Windows 2000, các thiết bị và cấu hình được cài đặt. Bạn sẽ được nhắc các thông tin sau:

| Nội dung | Mô tả |
|---|---|
| **Regional Settings** | Windows 2000 hiển thị xác lập miền hiện hành. Bạn có thể thêm sự hỗ trợ ngôn ngữ, thay đổi vị trí xác lập của bạn đối với hệ thống, và cấu hình thiết lập mặc định tài khoản người dùng cũng được. |
| **Personalize Your Software** | Khi cấu hình hệ thống, bạn phải nhập tên mà Windows 2000 Server đã ghi nhớ. Ngoài ra bạn có thể thêm vào tên của tổ chức. Mặc dù đó chỉ là tuỳ chọn. |
| **Licensing Mode** | Bạn phải chọn phương pháp cấp phép Per Server hay Per Seat. Nếu bạn chọn Per Server, bạn phải nhập số cấp phép của Per Server. |
| **Computer Name and Administrator Password** | Bạn phải nhập vào tên máy tính (tên NetBIOS tối đa 15 ký tự) khi cài Windows 2000. Tên tự động tổng quát sẽ là 15 ký tự. Tên bạn nhập vào phải khác tên các máy tính khác, tên nhóm, tên miền đã nhập trên mạng. Tên máy tính mặc định được hiển thị. Bạn cũng có thể nhập mật khẩu quản trị đối với tài khoản người dùng quản trị cục bộ. Mật khẩu này có thể tới 127 ký tự. |
| **Optional Component Manager** | Optional Component Manager cho phép bạn thêm hoặc bỏ các thành phần bổ sung trong và sau quá trình cài đặt. |
| **Date and Time Settings** | Trong suốt quá trình cài đặt, nếu cần bạn phải chọn múi giờ tương ứng và điều chỉnh ngày và giờ,. |

❖ *Cài đặt mạng Windows 2000 Server*

Ngay sau quá trình thu thập thông tin, Setup sẽ trở lại màn hình cài đặt và bắt đầu khảo sát máy tính để tìm các card mạng đã cài đặt.

***** Cài đặt hoạt động mạng (Networking Settings)

Quá trình cài đặt mạng bắt đầu bằng việc hỏi bạn chọn kiểu cài đặt (Typical Settings), kiểu mặc định hay kiểu tuỳ thích (**Custom Settings**). Kiểu cài đặt mặc định cấu hình hệ thống những mặc định: *Client for Microsoft Networks, File and Print Sharing for Microsoft Networks,* và *Internet Protocol (TCP/IP) cấu hình như DHCP client.*

Các loại cài đặt tuỳ thích cho phép cấu hình theo ba mục sau:

| Cài đặt | Mô tả |
|---|---|
| **Clients** | Mặc định khách là **Client For Microsoft Networks**. Bạn có thể thêm **Gateway (and Client) Services for NetWare**. |
| **Services** | Mặc định dịch vụ là **File and Printer Sharing for Microsoft Networks**. Bạn có thể thêm **SAP Agent** và **QoS Packet Scheduler**. Bạn có thể sửa đổi cài đặt đối với File và Printer Sharing cho mạng Microsoft bằng chọn lấy dịch vụ và chọn Properties.<br>Điều này cho phép bạn tối ưu việc cài đặt dịch vụ tương thích với mạng LAN. |
| **Protocols** | Giao thức mặc định là **Transport Control Protocol/Internet Protocol (TCP/IP).** Bạn có thể thêm các giao thức, **NWLink IPX/SPX**, **NetBEUI**, **DLC**, **AppleTalk**, **Network Monitor Driver**, và các giao thức khác. Bạn có thể cũng sửa đổi việc cài đặt giao thức bằng cách chọn Properties. |

❖ *Hoàn thành quá trình cài đặt*

Phần cuối cùng của chế độ GUI là giai đoạn hoàn thành quá trình cài đặt, nó không yêu cầu bất kỳ sự tương tác người dùng nào. Nó thực hiện các thao tác sau:

| Công việc | Mô tả |
|---|---|
| Copying files | Thiết lập việc sao chép các file cần thiết tới thư mục cài đặt như các file phụ trợ và file hình ảnh. |
| Configuring the computer | Thiết lập việc khởi tạo trình đơn bắt đầu của bạn; các nhóm chương trình; cài đặt máy in, các dịch vụ, tài khoản quản trị, phông chữ, và đăng ký các thư viện động. |
| Saving the configuration | Thiết lập việc lưu trữ cấu hình, khởi tạo thư mục sửa chữa, đặt lại file Boot.ini. |
| Removing temporary files | Thiết lập việc dọn dẹp file và thư mục tạm đã khởi tạo và sử dụng trong quá trình cài đặt, như thư mục<br>$WIN_NT$.~LS. |

## 7.2 Đăng nhập tới một Domain

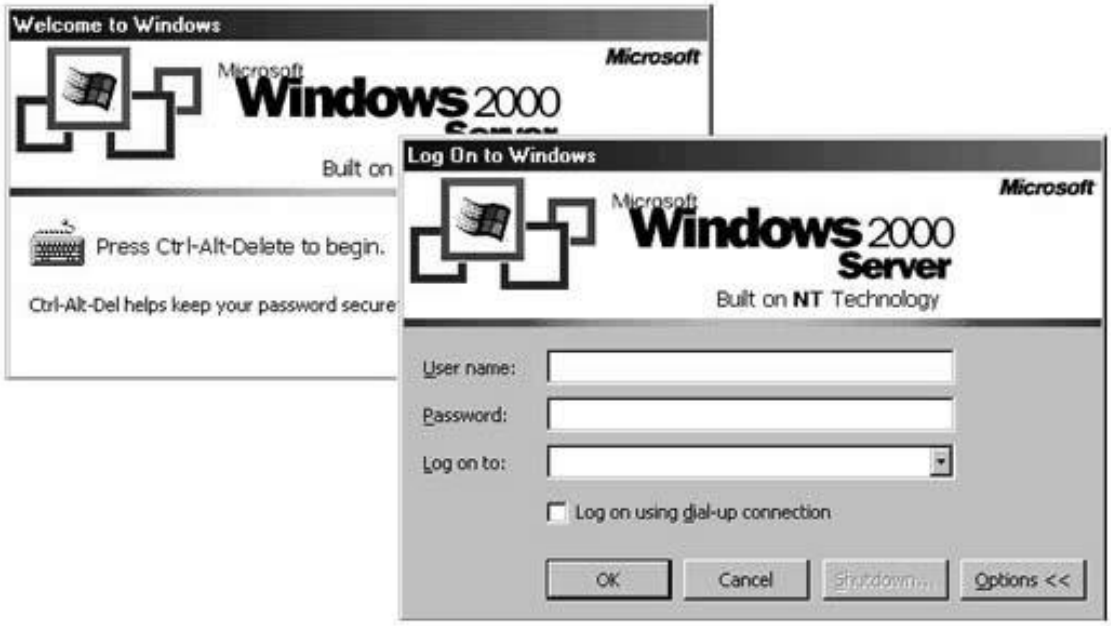
Bạn phải đăng nhập vào Windows 2000 để có thể truy xuất bất kỳ phần nào của hệ thống. Không giống như Windows 3.x hoặc Windows 9.x, bạn có thể truy xuất các file mà không cần đăng nhập tới mạng, bạn phải cung cấp thông tin đăng nhập đầu tiên trong Windows 2000.

Đăng nhập là quá trình nhận biết chính bạn tới máy tính bằng cách nhập tên và mật khẩu. Quá trình này nhận biết bạn như là người sử dụng hợp lệ và giúp duy trì sự bảo mật.

Để đăng nhập bạn phải cung cấp đúng tên và mật khẩu (user name and password), để kiểm tra định danh của bạn. Chỉ những người dùng hợp lệ mới có thể truy xuất tới nguồn tài nguyên và dữ liệu trên máy tính hoặc mạng.

Khi máy tính bắt đầu chạy Windows 2000 Server, nó sẽ hiển thị hộp thoại Welcome to Windows với lời nhắc nhấn **Ctrl+Alt+Delete** để đăng nhập.

Quá trình đăng nhập bắt đầu và đảm bảo rằng người dùng cung cấp đúng tên và mật khẩu tới hệ điều hành Windows khi bạn hoàn tất hộp thoại *Log On To Windows*.




Các lựa chọn trong hộp thoại Log on to Windows là:

| Tuỳ chọn | Mô tả |
|---|---|
| Hộp User Name | Mục này yêu cầu người dùng đăng nhập tên được cấp bởi người quản trị mạng. Để đăng nhập tới domain với tên người dùng, tài khoản người dùng phải lưu trữ tập trung trong thư mục hiện hành(Active Directory). |
| Hộp Password | Mật khẩu có phân biệt chữ hoa và chữ thường (case-sensitive). Các phần mật khẩu xuất hiện trên màn hình như là các dấu hoa thị (*) để đảm bảo bí mật. |
| Danh sách Log On To | Lựa chọn tên miền chứa tài khoản của bạn. Danh sách này chứa tất cả các miền trong cây miền. |
| Hộp kiểm tra Log On Using Dial-Up Connection | Cho phép người dùng kết nối tới miền máy chủ bằng cách dùng mạng dial-up, cho phép người dùng đăng nhập và thực hiện công việc từ vị trí ở xa. |

| | |
|---|---|
| Nút Shutdown | Đóng tất cả các file, lưu trữ tất cả dữ liệu của hệ điều hành, và chuẩn bị cho máy tính tắt an toàn. Trên các máy tính chạy hệ điều hành Windows 2000 Server, nút Shutdown không được đặt mặc định. |
| Nút Options | Dùng để đóng hoặc mở danh sách Log On To và hộp chọn Log On Using Dial-Up Connection. |

## 7.3 Các công cụ quản trị

Có một số công cụ quản trị sẵn có trên Windows 2000. Đa số các công cụ dùng wizard. Một số công cụ bao gồm: *Active Directory Users and Computers*; *Active Directory Domains and Trusts*; và snap-ins cho *DNS*, *DHCP* và *WINS*.

## 7.4 Hộp thoại bảo mật Windows 2000

Hộp thoại bảo mật Windows 2000 cung cấp một cách dễ dàng để truy xuất đến thông tin bảo mật. Nó hiển thị tài khoản người dùng đăng nhập hiện hành, miền hay máy tính mà người dùng được đăng nhập, ngày và thời gian người dùng đăng nhập. Thông tin này quan trọng đối với những người dùng có nhiều tài khoản. Thông qua nó ta xác định được ai có tài khoản chính, ai có tài khoản ưu tiên. Bạn truy cập vào hộp thoại bảo mật bằng cách nhấn **Ctrl+Alt+Delete** khi đăng nhập.

Bảng mô tả các nút nhấn trên hộp thoại Windows 2000 Security:

| Nút | Mô tả |
|---|---|
| **Lock Computer** | Cho phép người dùng bảo vệ máy tính không cần Log Off tất cả các chương trình đang chạy còn lại. Người dùng nên khoá máy tính của họ nếu không sử dụng. Người dùng có thể mở khoá lại bằng cách nhấn Ctrl+Alt+Delete và nhập đúng tên và mật khẩu. Người quản trị cũng có thể giải phóng khoá máy tính của người dùng hiện tại, tuy nhiên điều này là bắt ép đăng xuất (logoff) và dữ liệu có thể bị mất. |
| **Log Off** | Cho phép người dùng hiện tại đăng xuất và đóng tất cả các chương trình đang chạy. Hệ điều hành Windows 2000 vẫn đang chạy. |
| **Shut Down** | Cho phép người dùng đóng tất cả các file, cất tất cả dữ liệu hệ điều hành, và chuẩn bị cho máy tính có thể tắt máy một cách an toàn. |
| **Change Password** | Cho phép người dùng đổi mật khẩu tài khoản của họ. Họ phải biết mật khẩu cũ để khởi tạo mật khẩu mới. Đó là cách người dùng có thể thay đổi mật khẩu của họ. Các nhà quản trị nên yêu cầu những người dùng thay đổi mật khẩu chính của họ và nên tạo sự giới hạn mật khẩu như là phần của chính sách tài khoản. |

| Nút | Mô tả |
|---|---|
| **Task Manager** | Cung cấp danh sách những chương trình hiện tại đang chạy, xem xét hiệu suất sử dụng toàn bộ CPU và bộ nhớ, tổng quan mỗi chương trình, mỗi thành phần chương trình, hoặc hệ thống xử lý đang xử dụng CPU, bộ nhớ, trình quản lý tác vụ có thể được dùng để lựa chọn chương trình và dừng chương trình khi nó không đáp ứng. |
| **Cancel** | Đóng hộp thoại Windows Security. |

# Câu hỏi ôn tập chương 7

1. Khi cài đặt Windows 2000 Server ổ cứng yêu cầu còn trống tối thiểu là:
   a. 571 MB
   b. 671 MB
   c. 2 GB
2. Những hệ điều hành nào, trên đó khi cài đặt Windows 2000 Server phải sử dụng file Winnt32.exe ?
   a. Win 9X.
   b. Win NT 4.0 Workstation
   c. MS-DOS
   d. Win NT Server 4.0
   e. Windows 3.x
3. Thư mục nào sẽ được tạo mặc định khi bạn cài hệ điều hành Windows 2000 Server ?
   a. Windows
   b. WINNT
   c. None of the others
4. Chọn các quy tắc để đặt tên cho máy tính khi bạn cài hệ điều hành Windows 2000 Server .
   a. up to 15 characters
   b. different from all other computer, workgroup, or domain names.
   c. can contain asterisk characters.
5. Giao thức mặc định khi bạn cài đặt hệ điều hành Windows 2000 Server là …….
   a. IPX/SPX
   b. TCP/IP
   c. NetBEUI
   d. Apple Talk
6. Mật khẩu tối đa là bao nhiêu ký tự?
   a. 64
   b. 127
   c. 15
   d. 31

# CHƯƠNG 8 - QUẢN TRỊ TÀI KHOẢN NGƯỜI DÙNG

## MỤC TIÊU CỦA CHƯƠNG

*Kết thúc chương này bạn có thể:*

- Biết được các loại tài khoản người dùng
- Biết cách lập kế hoạch về tài khoản người dùng
- Tạo một số tài khoản người dùng và quản trị nó.

## 8.1 Các loại tài khoản người dùng (user)

Windows 2000 có một số loại tài khoản người dùng sau: *tài khoản cục bộ* ( local user accounts), *tài khoản miền* (domain user accounts), và *tài khoản cài đặt sẵn* (built-in user accounts). Với tài khoản cục bộ người dùng có thể đăng nhập vào máy tính riêng để truy xuất tài nguyên mạng trên máy tính đó. Với tài khoản miền, người dùng có thể đăng nhập tới miền để truy cập các nguồn tài nguyên mạng. Tài khoản cài đặt sẵn được dùng để thực hiện các tác vụ quản trị hoặc truy cập tới các nguồn tài nguyên mạng.

### 8.1.1 Tài khoản cục bộ

Tài khoản cục bộ được tạo trên những máy tính riêng biệt và cho phép người dùng đăng nhập vào máy tính và sử dụng tài nguyên chỉ trên máy tính đó. Tài khoản người dùng được khởi tạo trong những cơ sở dữ liệu bảo mật cục bộ và không tạo bản sao tới phần còn lại của miền. Trên các máy điều khiển miền (Domain Controller – DC) không có các tài khoản cục bộ, do vậy người dùng sẽ không được xác nhận trên miền và sẽ không được sử dụng tài nguyên miền. Các nhà quản trị miền không thể quản trị tài khoản cục bộ trừ khi họ kết nối riêng tới máy tính cục bộ để thực hiện các thao tác quản trị.

### 8.1.2 Tài khoản miền

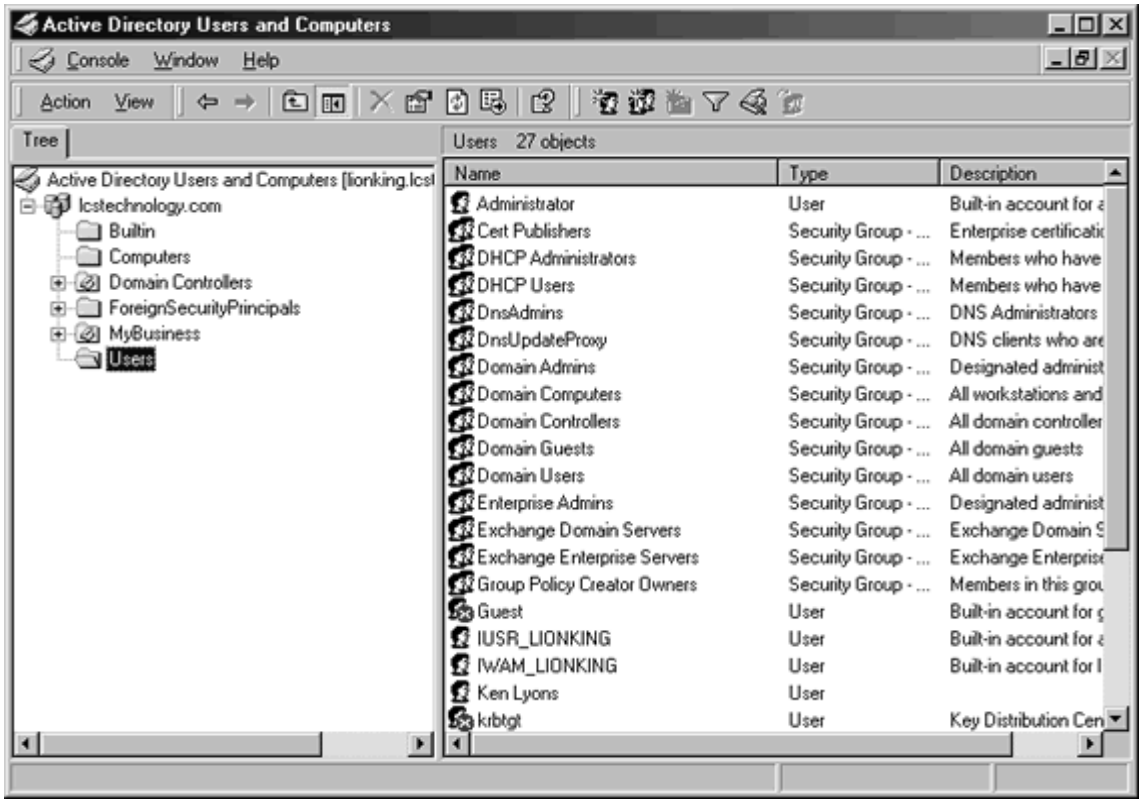
Tài khoản miền cho phép người dùng đăng nhập tới miền và truy xuất tới các tài nguyên ở bất kỳ đâu trên mạng. Người dùng cần nhập tên và mật khẩu của mình khi đăng nhập, việc kiểm tra tên và mật khẩu người dùng do DC đảm nhiệm. Khi một tài khoản được xác minh, Windows 2000 cấp một thẻ truy cập được dùng trong suốt phiên đăng nhập. Thẻ này chứa các thông tin về người dùng và tất cả các tài nguyên mà người dùng được phép truy cập.

Tài khoản miền được khởi tạo bên trong một container hoặc một đơn vị tổ chức (organizational unit – OU) trong bản sao của cơ sở dữ liệu Active Directory trên máy DC. Mỗi DC định kỳ tạo những bản sao về thông tin tài khoản người dùng mới tới tất cả các DC khác trong miền để xác nhận quyền truy cập của người dùng trên miền trong phiên đăng nhập.

### 8.1.3 Tài khoản cài đặt sẵn

Có một số tài khoản người dùng được tạo tự động khi Windows 2000 Server được cài đặt. Như tài khoản **Administrator** và **Guest**. Tài khoản Administrator được dùng để quản lý tất cả các máy tính và cấu hình miền cho các thao tác như là khởi tạo và sửa đổi

tài khoản người dùng và tài khoản nhóm, quản lý các chính sách bảo mật, khởi tạo máy in, và cấp phép và cấp quyền truy cập tài nguyên tới người dùng.




*Hình 8.1* Microsoft Management Console (MMC)
Active Directory Users and Computer

## 8.2 Lập kế hoạch tài khoản người dùng

Trước khi bạn cài đặt mạng, bạn cần phải lập kế hoạch người dùng, điều này rất quan trọng với mạng của bạn. Mọi thứ như là qui ước đặt tên người dùng phải hoàn tất trước khi tiến hành cài đặt.

### 8.2.1 Qui ước đặt tên

Qui ước đặt tên xác định mỗi user được nhận dạng duy nhất trong miền. Qui ước đặt tên nhất quán sẽ giúp bạn và người dùng nhớ nó khi đăng nhập.

Một vài điểm cần xem xét khi xác định qui ước đặt tên là:

| Consideration | Explanation |
|---|---|
| Các tài khoản người dùng cục bộ (Local user accounts) | Các tên tài khoản người dùng cục bộ phải duy nhất trên máy tính mà bạn tạo tài khoản cục bộ đó. |
| Các tài khoản người dùng miền (Domain user accounts) | Tên đăng nhập của người dùng phải duy nhất tới thư mục. Tên đầy đủ của người dùng cũng phải duy nhất trong Organisation Unit (OU) nơi bạn tạo tài khoản người dùng miền đó. |

| Consideration | Explanation |
|---|---|
| Nhiều nhất là 20 ký tự | Tên đăng nhập có thể dài tới 20 ký tự, bao gồm chữ hoa hoặc chữ thường. Dù trường dữ liệu có thể chấp nhận dài hơn, Windows 2000 chỉ lấy 20 ký tự đầu. |
| Các ký tự không hợp lệ | Bao gồm: " / \ [ ] : ; \| = , + * ? < > |
| Tên đăng nhập của người dùng không phân biệt ký tự hoa hay ký tự thường. | Bạn có thể dùng tổ hợp các ký tự kể cả ký tự đặc biệt để tạo tài khoản người dùng duy nhất. |
| Xét các nhân viên có cùng tên . | Nếu hai người dùng có cùng tên là John Smith, bạn có thể dùng tên của họ và thêm vào các ký tự hay ký số khác nhau để phân biệt. Thí dụ: Johns và Johnsm, hay Johns1 và Johns2. |
| Nhận dạng loại nhân viên. | Trong một số tổ chức có thể có nhiều loại nhân viên, ví dụ như nhân viên chính và nhân viên tạm tuyển. Để phân biệt nhân viên tạm, bạn có thể dùng ký tự T (Temp) làm tiếp đầu ngữ, ví dụ: T-Johns, cho John Smith. |
| Tính tương thích với hệ thống thư điện tử | Một số hệ thống thư điện tử có thể không chấp nhận một số ký tự như khoảng trắng hay dấu ngoặc ( "()" ) |

### 8.2.2 Những yêu cầu về mật khẩu (Password Requirements)

Mỗi tài khoản người dùng trên mạng Windows 2000 nên có mật khẩu để bảo vệ truy xuất tới domain hoặc máy tính cá nhân. Một vài quy tắc khi đặt mật khẩu là:

- Tài khoản quản trị phải có mật khẩu để ngăn sự đăng nhập bất hợp pháp.
- Quyết định xem nên để người quản trị hay người dùng điều khiển mật khẩu. Bạn có thể gán mật khẩu duy nhất đối với tài khoản người dùng và ngăn người dùng thay mật khẩu, hoặc bạn có thể cho phép người dùng nhập mật khẩu lần đầu họ đăng nhập. Người dùng nên điều khiển mật khẩu của bạn.
- Sử dụng mật khẩu phải khó đoán. Thí dụ, tránh sử dụng mật khẩu với những kết hợp rõ ràng, như tên thành viên gia đình.
- Mật khẩu có thể tới 14 ký tự, tối thiểu nên là 8 ký tự.
- Ba nhóm ký tự có thể dùng để đặt mật khẩu: Các ký tự hoa và ký tự thường, các ký số, và các ký tự khác.
- Tạo mật khẩu sau phải khác nhiều so với các mật khẩu trước.
- Chúng không được trùng với tên của người dùng hoặc chứa tên người dùng.

### 8.2.3 Hạn chế giờ đăng nhập và hạn chế trạm đăng nhập

Mặc định, mỗi tài khoản người dùng mới lúc khởi tạo không bị giới hạn giờ đăng nhập. Tạo ra các hạn chế này là do yêu cầu bảo mật của mạng. Nếu người dùng bao giờ cũng làm việc từ 9 giờ sáng đến 5 giờ chiều, từ thứ hai đến thứ sáu, thì việc truy cập ngoài giờ đó sẽ bị kiểm tra kỹ. Việc này sẽ giới hạn khả năng đối với những truy xuất không được phép. Cũng như vậy, nên xem xét việc giới hạn đăng nhập của user trên những máy tính xác định. Điều này giúp cho việc bảo mật mạng và giúp cho các nhà quản trị xác định chính xác người dùng có thể truy cập mạng ở đâu. Đối với tài khoản của các nhân viên tạm tuyển, thì nên có ngày kết thúc. Khi nhân viên đi khỏi công ty thì ngày sử dụng tài khoản của họ cũng nên hết hạn.

Các điểm cần nhớ khi xét đến giờ đăng nhập và giới hạn trạm làm việc:

- Giờ đăng nhập nên thiết lập cho người dùng chỉ yêu cầu truy cập tại thời gian cụ thể định trước, thí dụ chỉ cho phép các công nhân làm việc ca đêm truy cập mạng trong giờ làm của họ.
- Nên yêu cầu người dùng đăng nhập mạng từ máy tính của họ khi dữ liệu nhạy cảm được lưu giữ trên ổ cứng cục bộ của họ.

### 8.2.4 Bảng kế hoạch tài khoản người dùng

Để giúp cho công việc lập kế hoạch tài khoản người dùng dễ dàng, Microsoft đã phát triển phần mềm User Account Planning Worksheet. Để hoàn thiện công việc này bạn cần làm các bước sau:

- Ghi tên đầy đủ cho mỗi người dùng
- Định tên quy ước của bạn và ghi tên người dùng trên cơ sở này.
- Bao gồm cả tên công việc cho mỗi nhân viên
- Xác định mật khẩu cho mỗi người dùng (mật khẩu lúc khởi tạo)
- Ở cột vị trí Home Folder, ghi vị trí của nó là trên máy cục bộ hay máy chủ
- Ở cột giờ đăng nhập, điền giờ truy xuất cho mỗi người dùng
- Ghi dưới giới hạn trạm làm việc là yes nếu người dùng bị giới hạn và là no nếu không.

Bản kế hoạch hoàn thành sẽ có dạng như sau:

**User Accounts Planning Sheet**

**Qui ước đặt tên:** 3 ký tự đầu tiên của phần tên (first name), đi theo 3 ký tự đầu của phần họ (surname). Mật khẩu là ký tự đầu tiên của first name, theo sau là từ "password", cuối cùng là ký tự đầu của surname.

| Full Name | User Account | Description | Password Requirements | Home folder location | Logon hours | Workstation |
|---|---|---|---|---|---|---|
| John Smith | Johsmi | Vice President | Jpasswords | Server | 7.30 – 23.55 | N |
| Jim Jones | Jimjon | Temp | Jpasswordj | Server | 8.55 – | Y |

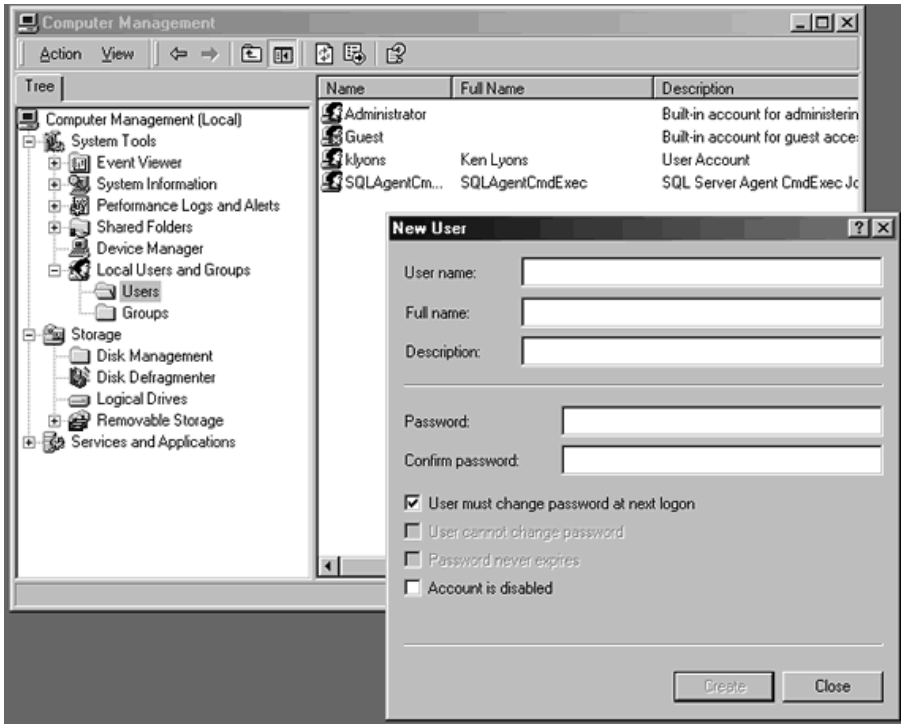
| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | 17.15 | |

## 8.3 Tạo tài khoản người dùng cục bộ và tài khoản người dùng miền

### 8.3.1 Tạo tài khoản người dùng cục bộ

Để tạo tài khoản người dùng, bạn sử dụng chương trình MMC *Local Users and Groups*. Bạn có thể tạo, xoá hoặc vô hiệu tài khoản người dùng trên máy cục bộ trong nhóm làm việc. Bạn không thể tạo tài khoản cục bộ trên domain controller.

1. Kích Start -> Programs -> Administrative Tools -> kích Computer Management.
2. Mở rộng mục Local Users and Groups, kích nút phải trên Users, và chọn New User.
3. Trong cửa sổ New User nhập các thông tin tài khoản user cục bộ như đã xác định trong giai đoạn lập kế hoạch.




Các mục chọn trong cửa sổ New User:

| Các tuỳ chọn | Mô tả |
|---|---|
| User Name | Tên phải duy nhất khi bạn nhập. Hộp thoại này là bắt buộc. |
| Full Name | Tên đầy đủ của người dùng. Hộp thoại này là tuỳ chọn. |
| Description | Các mô tả rất hữu ích để xác định người dùng, thí dụ như phòng ban hay nơi làm việc. Hộp thoại này là tuỳ chọn |
| User Must Change Password At Next Logon | Yêu cầu người dùng thay đổi mật khẩu của họ khi đăng nhập lần đầu. |

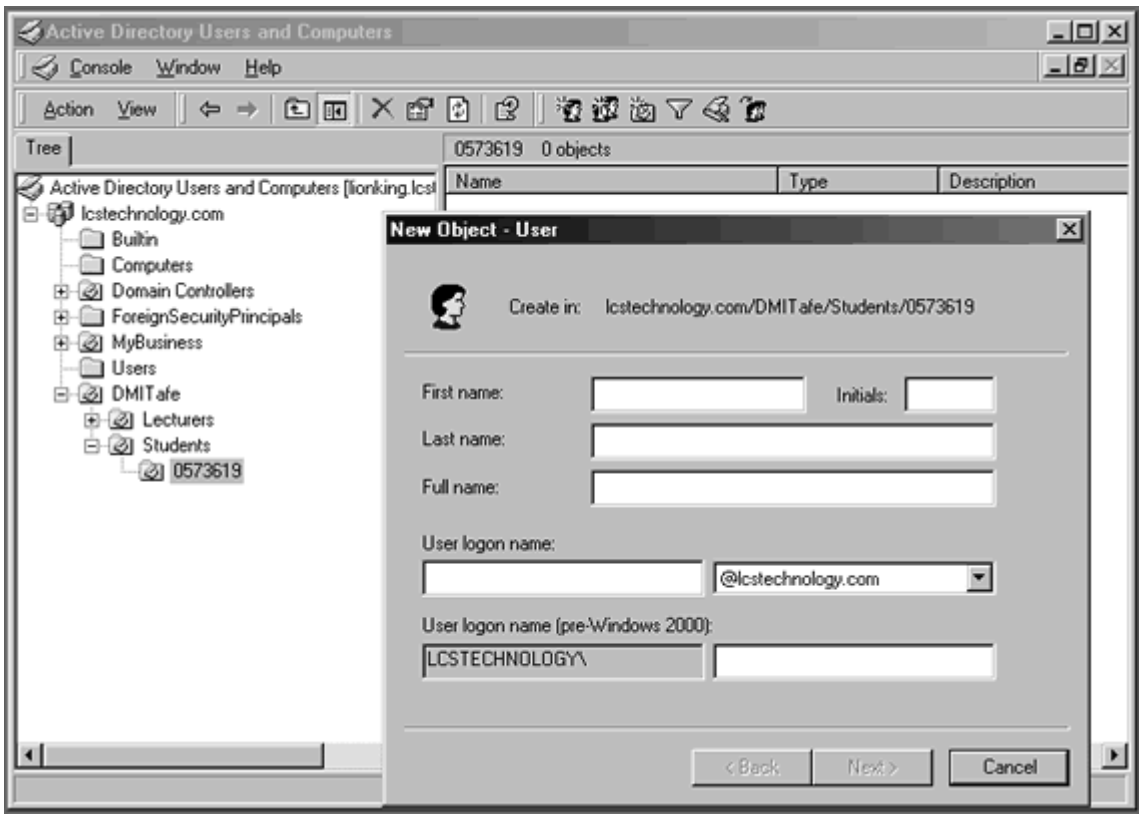
| Các tuỳ chọn | Mô tả |
|---|---|
| User Cannot Change Password | Chỉ cho phép nhà quản trị thay đổi mật khẩu. |
| Password Never Expires | Mật khẩu sẽ không bao giờ thay đổi. Người dùng phải thay đổi mật khẩu tại lần đăng nhập kế và ghi đè nên mục chọn mật khẩu không bao giờ đổi. |
| Account Is Disabled | Ngăn người dùng không cho dùng tài khoản của họ. |

### 8.3.2 Tạo tài khoản người dùng miền (Domain)

Để tạo tài khoản người dùng miền, bạn cần sử dụng chương trình *Active Directory Users and Computers*. Dùng chương trình này bạn có thể tạo, xoá hoặc vô hiệu tài khoản người dùng trên domain controller, hay tài khoản người dùng cục bộ trên bất kỳ máy tính nào trong miền.

Khi bạn tạo tài khoản người dùng miền, người dùng sẽ đăng nhập tới miền bằng tên mặc định. Tuy nhiên, bạn có thể lựa chọn bất kỳ miền nào để tạo tài khoản người dùng miền cho người dùng đó. Bạn phải chọn nơi cất trữ tài khoản mới đó. Bạn có thể tạo tài khoản người dùng miền trong nơi chứa người dùng mặc định hoặc ở nơi cất trữ miền. Thí dụ, nơi chứa (OU) gọi là DMITafe được khởi tạo. OU đó có thể chứa các OU khác, như Lecturers, Students, vân vân. Mỗi OU có thể có tài khoản người dùng đã được tạo.

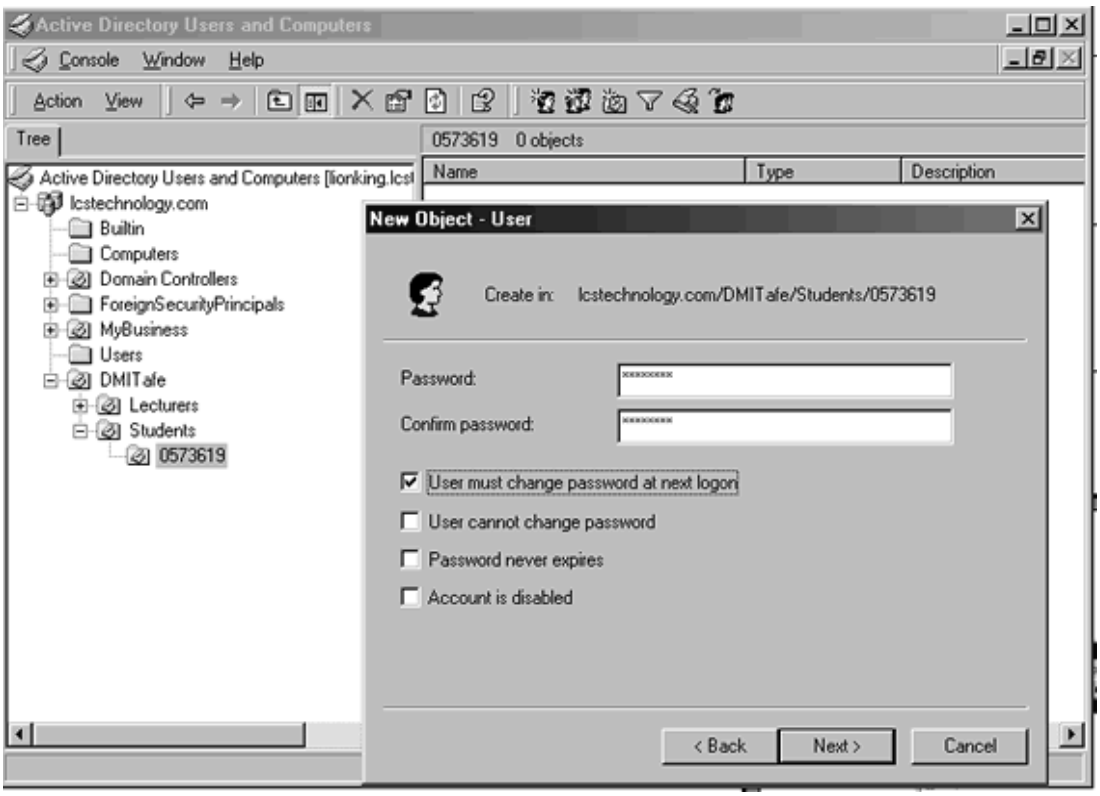
1. Kích Start -> Programs -> Administrative Tools -> Active Directory Users And Computers.
2. Chọn domain -> kích nút phải tại container Users -> New -> User
3. Trong cửa sổ *New Object – User* nhập các thông tin tài khoản user miền như đã xác định trong giai đoạn lập kế hoạch.



Các mục chọn trong hộp thoại New Object - User:

| Các tuỳ chọn | Mô tả |
|---|---|
| First Name | Tên người dùng hoặc họ tên, hộp thoại này yêu cầu bắt buộc phải nhập. |
| Initials | Tên viết tắt của người dùng, hộp thoại này bắt buộc. |
| Last Name | Họ của người sử dụng, hộp thoại này bắt buộc. |
| Full Name | Họ tên người dùng. Tên phải duy nhất trong nơi lưu giữ nó. Windows 2000 hoàn thiện mục chọn này nếu bạn nhập vào thông tin vào ba hộp thoại trên . Mục Create-In hiển thị tên này ở dạng đường dẫn tên phân biệt. |
| User Logon Name | Tên đăng nhập chứa trong hộp và danh sách xác định duy nhất người dùng trên mạng. Hộp thoại này bắt buộc và yêu cầu không được nhập trùng tên đã có trên miền. |
| User Logon Name (Pre-Windows 2000) | Dùng cho các phiên bản khác của Windows, như Windows NT 4.0 hay Windows NT 3.5.1. Hộp thoại này bắt buộc và yêu cầu không được nhập trùng tên đã có trên miền. |

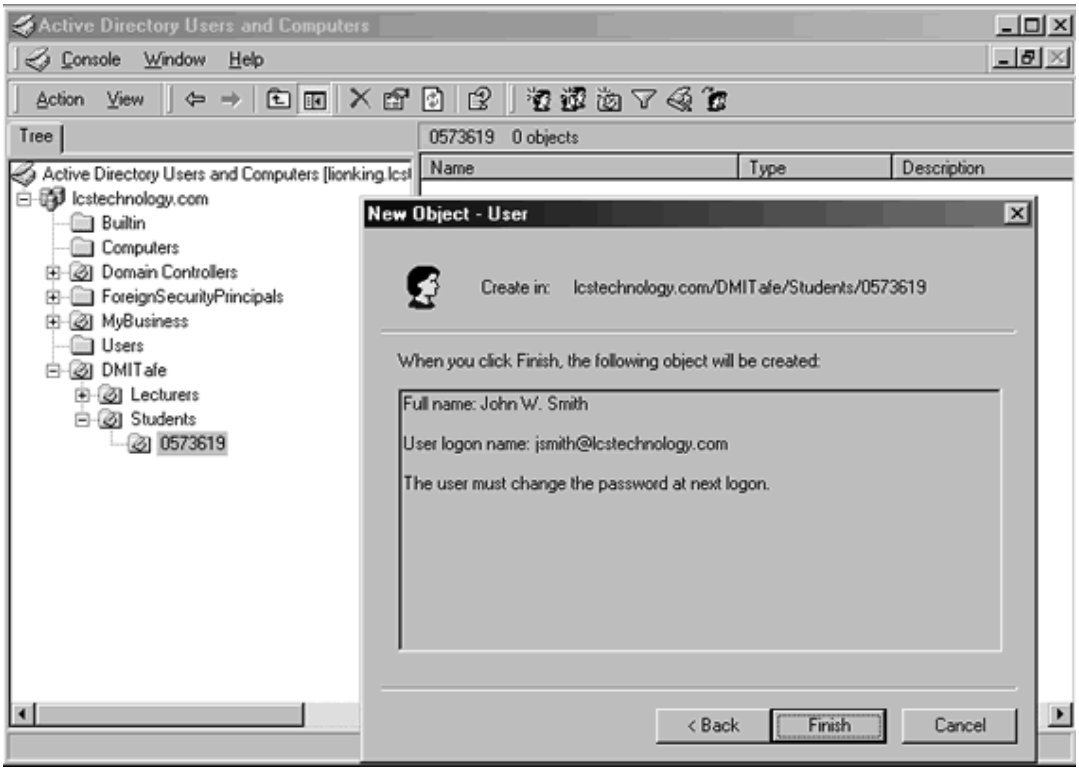
Khi những mục này đã hoàn thành, người quản trị nhấn vào nút Next, nó sẽ hiển thị tiếp hộp thoại Password Options.



Các mục chọn trong hộp thoại New Object – User Password Options :

| Các tuỳ chọn | Mô tả |
|---|---|
| Password | Mật khẩu được dùng để xác nhận quyền người dùng. Để bảo mật hơn bạn luôn gán mật khẩu. |
| Confirm Password | Xác nhận mật khẩu bằng cách nhập nó một lần nữa để đảm bảo rằng bạn đã gõ đúng mật khẩu. Hộp thoại này bắt buộc nếu bạn gán mật khẩu. |
| User Must Change Password At Next Logon | Yêu cầu người dùng thay đổi mật khẩu của họ lần đầu đăng nhập vào mạng. Điều này đảm bảo rằng chỉ người dùng mới biết mật khẩu của họ. |
| User Cannot Change Password | Chỉ những người quản trị mới được phép thay đổi mật khẩu. Chọn hộp kiểm này nếu bạn có nhiều hơn một người sử dụng cùng tài khoản miền hoặc để bảo trì điều khiển trên các mật khẩu tài khoản người dùng. |
| Password Never Expires | Mật khẩu sẽ không bao giờ thay đổi. Đối với tài khoản sử dụng miền bạn sẽ dùng chương trình hoặc dịch vụ Windows 2000. Mục User Must Change Password At Next Logon ghi đè nên mục Password Never Expires. |
| Account Is Disabled | Ngăn người dùng sử dụng tài khoản của họ. |

Sau khi điền vào hộp thoại Password Option, nhấn Next và sau đó là Finish để tạo tài khoản mới.



Mỗi tài khoản người dùng mới được tạo mặc định có thể thay đổi bằng cách nhắp đúp chuột vào người dùng mới trong trình đơn *Active Directory Users and Computers* và sau đó xác nhận các thuộc tính còn lại. Các thuộc tính này bao gồm các thuộc tính cá nhân và tài khoản, các mục chọn đăng nhập và thiết lập dial-in.

Các thuộc tính đó nên được điền đầy đủ thông tin.

Bảng sau mô tả các thuộc tính của người dùng:

| Tab | Mô tả |
|---|---|
| General | Chứa tên người dùng, hiển thị tên, mô tả, vị trí cơ quan, số điện thoại, địa chỉ e-mail, trang chủ và các trang Web bổ sung. |
| Address | Chứa địa chỉ đường phố , địa chỉ gửi thư đường bưu điện, mã vùng và mã nước. |
| Account | Chứa các thuộc tính tài khoản người dùng bao gồm: Tên đăng nhập, giờ đăng nhập, các máy được phép đăng nhập tới, các mục tài khoản, thời hạn kết thúc. |
| Profile | Thiết lập đường dẫn hồ sơ, đường dẫn kịch bản đăng nhập, thư mục gốc, thư mục tài liệu chia sẻ. |
| Telephones | Chứa số điện thoại bàn , điện thoại di động, số fax, giao thức Internet, và chỗ trống cho lời chú giải. |
| Organisation | Chứa các tiêu đề về người dùng như tên phòng ban, công ty, người quản lý, và các báo cáo trực tiếp. |
| Remote Control | Thiết lập điều khiển từ xa cho Terminal Services. |
| Terminal Services Profile | Cấu hình hồ sơ người dùng dịch vụ đầu cuối. |
| Member Of | Chứa các nhóm mà người sử dụng là thành viên. |
| Dial-In | Chứa các thuộc tính dial-in cho người dùng . |
| Environment | Cấu hình môi trường khởi động các dịch vụ đầu cuối. |
| Sessions | Thiết lập ngưỡng thời gian cho Terminal Services và các thiết lập lại kết nối. |

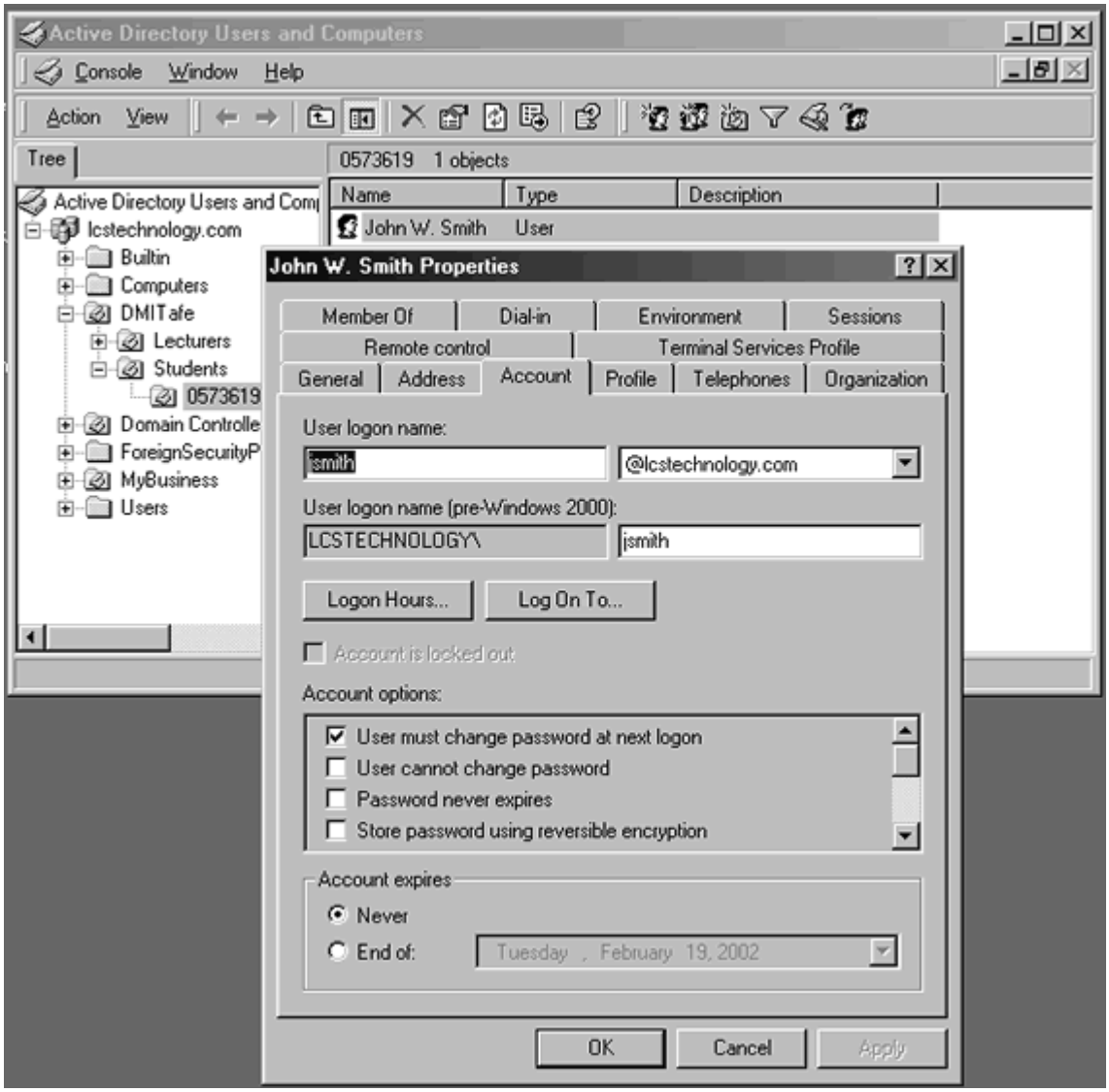
- Các thuộc tính cá nhân (Personal properties)

Bao gồm các trang (Tab) General, Address, Telephones, Organisation và cần được hoàn tất tương ứng với mỗi một tài khoản người dùng. Tương ứng với mỗi trường là một thuộc tính tìm kiếm.

- Các thuộc tính tài khoản (Account Properties)

Thuộc tính tài khoản người dùng được nhập qua trang Account. Một vài thuộc tính được tạo cùng thời gian với tài khoản người dùng miền. Tuy nhiên, các thuộc tính

thêm chỉ có hiệu lực khi bạn chọn lựa trang Account và hoàn tất các mục còn lại trong bảng.



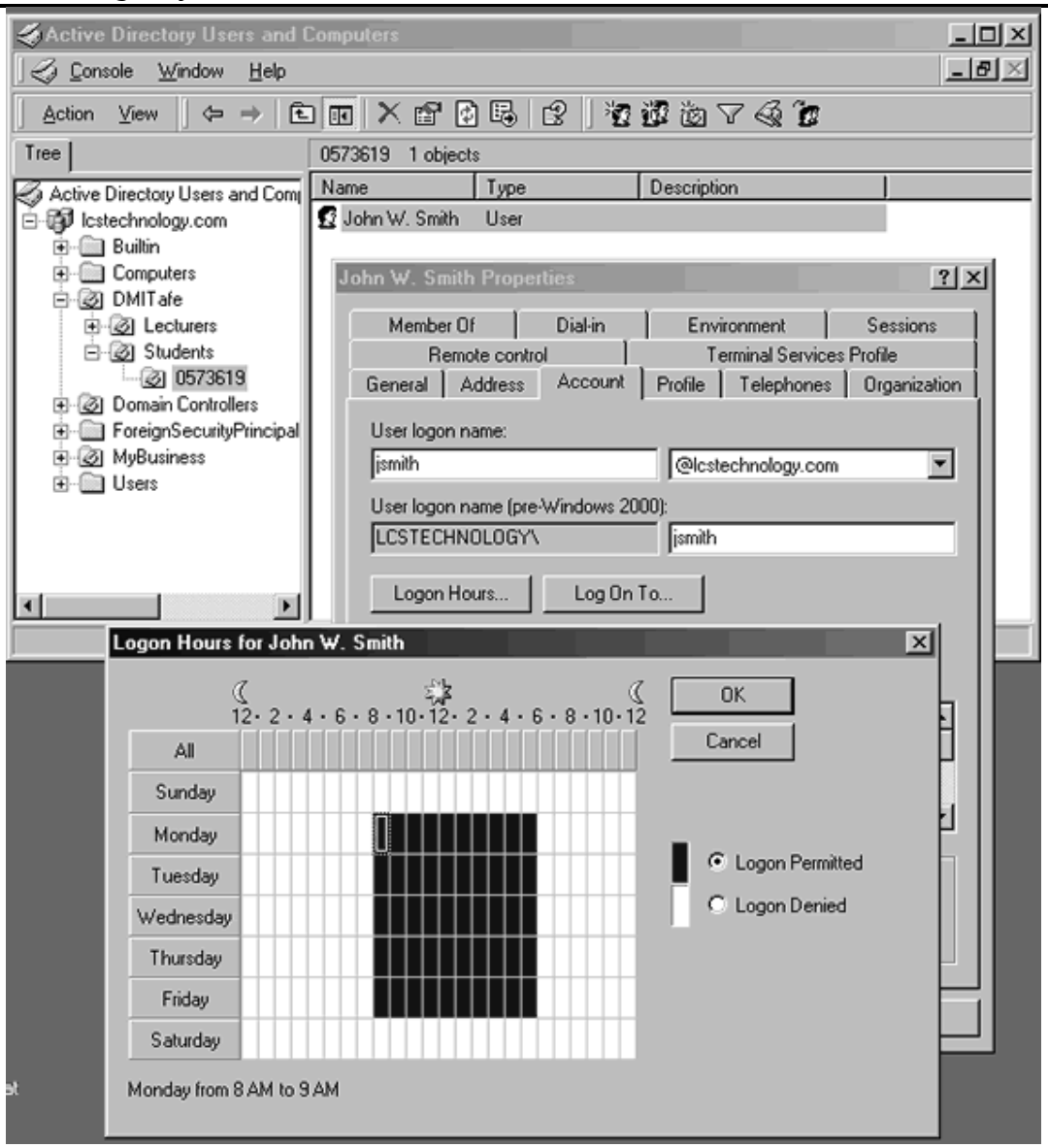

- Giờ đăng nhập( Logon Hours)

Thiết lập giờ đăng nhập trong hộp thoại Properties của bảng Account, nhấp chuột vào Logon Hours. Trên hộp thoại Logon Hours cho người dùng, hộp màu xanh chỉ định người dùng có thể đăng nhập, hộp màu trắng chỉ thị rằng người dùng không thể đăng nhập.

Để cho phép hay từ chối truy xuất cần làm những điều sau:

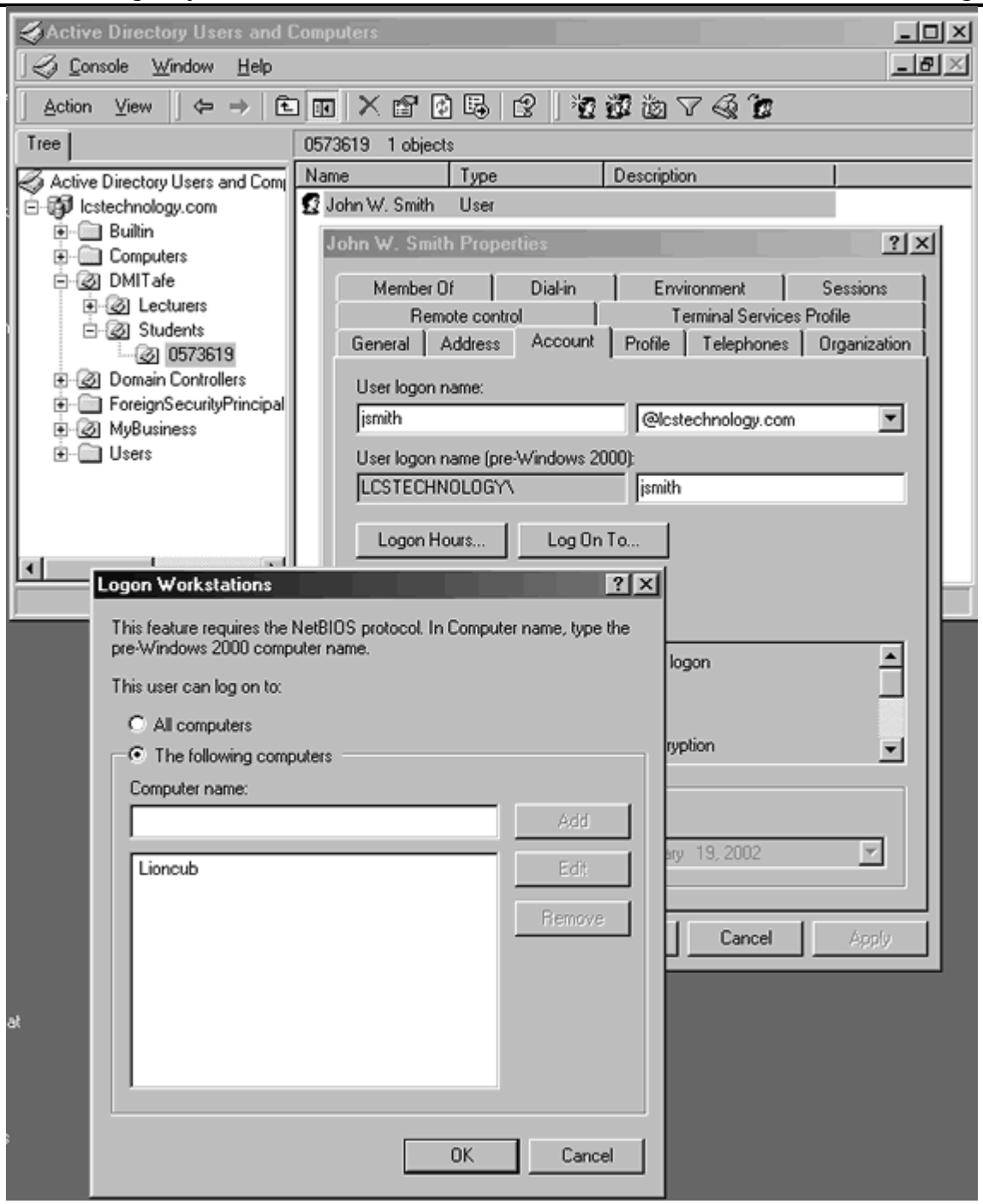
- Chọn các hình chữ nhật trên đó có các ngày và giờ bạn cho phép người dùng truy cập, chọn thời gian bắt đầu và thời gian kết thúc, và nhấp nút Logon Permitted.

- Chọn các hình chữ nhật trên đó có các ngày và giờ bạn không cho phép người dùng truy cập, chọn thời gian bắt đầu và thời gian kết thúc, và nhấp nút Logon Denied.



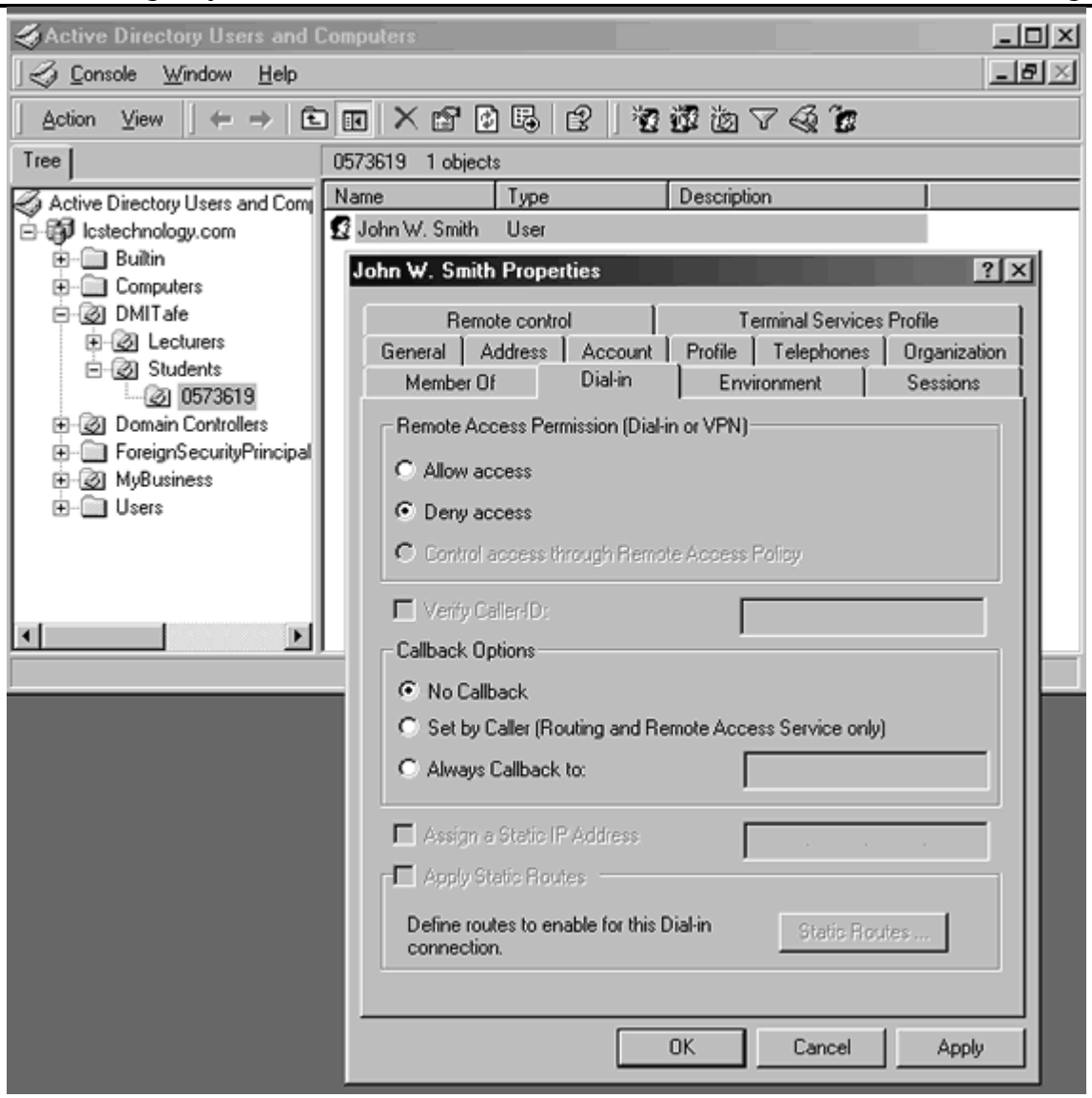

- Giới hạn các máy tính mà người dùng có thể đăng nhập tới

Cân nhắc xem người dùng có nên bị giới hạn đăng nhập tới các máy tính riêng hay không. Điều này rất cần cho việc bảo mật mạng và nó giúp người quản trị mạng biết chính xác người dùng truy cập mạng ở đâu. Để giới hạn người dùng truy cập tới máy tính khác ta chọn nút *Log On To…* trên trang Account và thêm tên các máy tính mà bạn cho phép người dùng đăng nhập tới.




- Xác nhận cho phép Dial-In

Các thiết lập xác nhận dial-in cho tài khoản người dùng được phép kết nối dial-in tới mạng từ xa. Để truy cập tới mạng, người dùng chạy chương trình Windows 2000 Remote Access Server (RAS). Người dùng được xác thực đồng thời là đang truy cập mạng nếu họ đã thực sự đăng nhập tới trạm đang kết nối tới mạng LAN.




Các mục chọn trong bảng Dial-In:

| **Các tuỳ chọn** | **Mô tả** |
|---|---|
| Allow Access | Quay số hoăc mạng ảo truy xuất từ xa cho người dùng. |
| Deny Access | Tắt dial-in hoặc truy xuất từ xa VPN cho người dùng. |
| Control Access Through Remote Access Policy | Cho phép người dùng truy cập từ xa. |
| Verify Caller-ID | Chỉ định số điện thoại mà người dùng phải quay vào. |

| Các tuỳ chọn | Mô tả |
|---|---|
| Callback Options | Các phương pháp gọi sau bao gồm:<br>*No Callback.* Dịch vụ RAS sẽ không gọi cho người dùng muốn gọi lại , mục này là mặc định.<br>*Set By Caller (Routing and Remote Access Service Only).* Người dùng cung cấp cho RAS số điện thoại để gọi lại. Công ty sẽ trả tiền cho mục này.<br>*Always Callback To.* Dịch vụ RAS dùng số điện thoại danh nghĩa cho người dùng gọi lại. Người dùng phải có số điện thoại danh nghĩa để kết nối với máy chủ. Dùng mục chọn này cho môi trường cần bảo mật cao. |
| Assign A Static IP Address | Định rõ những thiết lập cho hồ sơ dial-in nhóm ít quan tâm và gán địa chỉ TCP/IP tới người dùng này. |
| Apply Static Routes | Định rõ cấu hình tìm đường giới hạn trước để kết nối. |
| Static Routes | Cho phép xác định tìm đường tĩnh. |

## 8.4 Thiết lập hồ sơ người dùng (User Profile)

### 8.4.1 Khái niệm hồ sơ người dùng (User Profiles)

Hồ sơ người dùng bao gồm các thư mục và dữ liệu liên quan đến môi trường màn hình làm việc hiện tại của người dùng, những ứng dụng và dữ liệu cá nhân. Hồ sơ người dùng lưu tất cả các kết nối mạng được thiết lập khi người dùng đăng nhập tới máy tính, như là các mục trong trình Start và các ổ đĩa được ánh xạ tới các máy chủ mạng. Mỗi lần người dùng đăng nhập vào mạng, các thiết lập của họ sẽ giống như lần đăng nhập trước.

### 8.4.2 Ưu điểm của hồ sơ người dùng

- Cho phép nhiều người cùng sử dụng chung một máy tính, và mỗi người nhận được cài đặt màn hình riêng khi họ đăng nhập.
- Khi người dùng đăng nhập vào trạm làm việc của họ, họ sẽ nhận được màn hình như là khi họ đã thoát khỏi của phiên làm việc trước.
- Sự tuỳ biến của môi trường màn hình bởi một người sử dụng nào đấy sẽ không ảnh hưởng đến các thiết lập của người dùng khác.
- Các hồ sơ người dùng có thể được cất trên máy chủ để chúng có thể theo người dùng tới bất kỳ máy tính nào đang chạy Windows NT 4.0 hay Windows 2000 trên mạng. Hồ sơ này gọi là hồ sơ người dùng lang thang (*roaming user profiles).*
- Thiết lập ứng dụng được tiếp tục sử dụng, đó là các ứng dụng được xác nhận trên Windows 2000.
- Các nhà quản trị có thể khởi tạo hồ sơ người dùng mặc định, mà nó thích hợp với các công việc của người dùng đó.
- Bạn có thể thiết lập hồ sơ người dùng bắt buộc, hồ sơ đó không lưu giữ các thay đổi khi người dùng thiết lập màn hình. Người dùng có thể sửa đổi những thiết lập

màn hình của máy tính trong khi họ đăng nhập, nhưng không có thay đổi nào được lưu lại khi họ rời hệ thống. Hồ sơ bắt buộc được tải xuống từ máy tính cục bộ mỗi lần người dùng đăng nhập.

- Bạn có thể chỉ định người dùng mặc định bao gồm tất cả hồ sơ người dùng riêng biệt.

Có ba loại người dùng cá nhân: *hồ sơ người dùng cục bộ, hồ sơ người dùng lang thang* và *hồ sơ người dùng bắt buộc*.

### 8.4.3 Hồ sơ người dùng cục bộ

Hồ sơ người dùng cục bộ được tạo tự động lần đầu người dùng đăng nhập vào máy tính. Nó được cất trên ổ cứng cục bộ và bất kỳ sự thay đổi trên hồ sơ cục bộ sẽ được thể hiện trên máy tính đó. Hồ sơ người dùng cục bộ được cập nhật tự động bởi Windows 2000. Thí dụ, mỗi lần người dùng thay đổi trên màn hình, những thay đổi này được lưu giữ để lần đăng nhập tới sẽ được nạp nên giống như lần thoát trước.

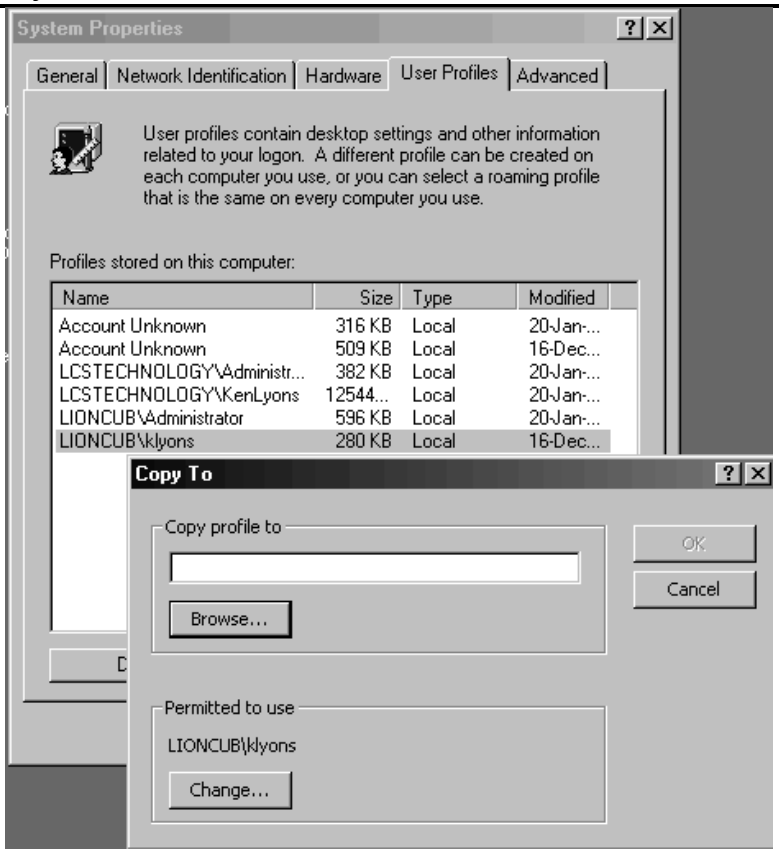
### 8.4.4 Hồ sơ người dùng lang thang (Roaming user profile)

Hồ sơ người dùng lang thang được tạo bởi người quản trị hệ thống và được cất trên máy chủ. Hồ sơ này có hiệu lực mỗi lần người dùng đăng nhập vào mạng ở bất kỳ máy tính nào. Mọi sự thay đổi trên màn hình của người dùng được cập nhật trên máy chủ và được bảo trì tự động. Sự khác nhau giữa hồ sơ cục bộ và lang thang chỉ là nơi lưu trữ. Hồ sơ lang thang được cất trên thư mục chia sẻ trong máy chủ để họ có thể truy cập từ bất kỳ máy nào trên mạng.

Lần đầu người dùng đăng nhập vào mạng, Windows 2000 sao chép tất cả các tài liệu của người dùng tới máy tính cục bộ. Từ thời gian này, khi người dùng đăng nhập tới máy tính, Windows 2000 sẽ so sánh với hồ sơ cất trữ cục bộ và hồ sơ lang thang. Nó chỉ chép lại những file có thay đổi. Việc này làm cho quá trình đăng nhập nhanh hơn.

- **Thiết lập hồ sơ người dùng lang thang**

1. Tạo mẫu hồ sơ người dùng với cấu hình thích hợp. Làm điều này bằng cách tạo tài khoản người dùng qua chương trình Active Directory Users and Computers, sau đó thoát ra và đăng nhập lại như người dùng mới. Cấu hình các thiết lập màn hình thích hợp và sau đó thoát ra khỏi tài khoản người dùng đó và đăng nhập lại như người quản trị.
2. Tạo thư mục dùng chung trên máy chủ, như : *\\server_name\profiles*.
3. Trong hộp thoại Properties của người dùng trên trang Profile, cung cấp đường dẫn tới thư mục dùng chung trong hộp Profile Path. (Sử dụng một đường dẫn Qui ước đặt tên chung (Universal Naming Convention - UNC) như là: *\\server_name\shared_folder_name\logon_name*).
   Bạn có thể gõ biến **%username%** thay vì tên đăng nhập. Khi người dùng sử dụng biến này, Windows 2000 tự động thay thế biến với tên tài khoản người dùng cho hồ sơ lang thang, nó hữu ích khi sao chép các tài khoản mẫu.
4. Sao chép mẫu hồ sơ người dùng tới thư mục dùng chung trên máy chủ và chỉ định những người dùng được phép sử dụng hồ sơ trong trang hồ sơ người dùng trong hộp thoại System Properties của Control Panel .




## 8.4.5 Hồ sơ người dùng bắt buộc (Mandatory user profile)

Hồ sơ người dùng bắt buộc là một loại hồ sơ lang thang đặc biệt chỉ đọc mà có thể thiết lập các chỉ định cá nhân đặc biệt hoặc gom nhóm người dùng. Chỉ những người quản trị hệ thống mới có thể thay đổi các hồ sơ bắt buộc. Hồ sơ bắt buộc được tải xuống máy người dùng mỗi lần người dùng đăng nhập vào mạng. Người dùng có thể thay đổi cấu hình màn hình của họ, nhưng khi thoát ra thì những thay đổi đó sẽ mất. Loại hồ sơ này không cập nhật.

Có một file ẩn trong hồ sơ này (*\\server_name\share\user_logon_name*) gọi là NTUSER.DAT, nó chứa các thiết lập hệ thống Windows 2000 áp dụng cho tài khoản người dùng cá nhân. File này cũng chứa các thiết lập môi trường người dùng. Bằng cách thay đổi tên của file NTUSER.DAT thành NTUSER.MAN, nó trở thành hồ sơ người dùng chỉ đọc.

## 8.4.5 Những thiết lập được lưu trữ trong hồ sơ người dùng

Bảng sau mô tả các thiết lập được lưu trữ trong hồ sơ người dùng. Các thiết lập này xác định môi trường màn hình của người dùng. Hồ sơ cục bộ được lưu trong thư mục *C:\Documents and Settings\user_logon_name*, ở đây C:\ là tên ổ cứng và *user_logon_name* là tên người dùng đăng ký khi đăng nhập vào hệ thống. Hồ sơ lang thang được lưu trên thư mục chia sẻ của máy chủ.

| Tham số | Nguồn |
|---|---|
| Toàn bộ những thiết lập được định nghĩa bởi user cho Windows Explorer | Windows Explorer |
| Các tài liệu do user lưu trữ | My Documents |
| Các file hình ảnh do user lưu giữ | My Pictures |

| Tham số | Nguồn |
|---|---|
| Các shortcuts cho các vị trí ưa thích trên Internet | Favourites |
| Bất kỳ một ổ đĩa mạng được ánh xạ do user tạo ra | Mapped network drive |
| Các liên kết tới các máy tính khác trên mạng | My Network Places |
| Các mục được lưu trữ trên màn hình Desktop và các Shortcut | Desktop contents |
| Toàn bộ các thiết lập font chữ và màu màn hình máy tính được định nghĩa bởi user. | Screen colours and fonts |
| Những thiết lập cấu hình được định nghĩa bởi user và dữ liệu của ứng dụng | Application data and registry hive |
| Những kết nối máy in mạng | Printer settings |
| Toàn bộ các thiết lập do user thực hiện trong Control Panel | Control Panel |
| Toàn bộ các thiết lập chương trình do user tạo ra ảnh hưởng đến môi trường Window của user, bao gồm Calculator, Clock, Notepad, và Paint | Accessories |
| Các thiết lập chương trình của mỗi user cho các chương trình được viết cho Windows 2000 và được thiết kế để theo dõi các cài đặt chương trình | Windows 2000-based programs |
| Bất kỳ bookmark nào được đặt trong hệ thống Help của Windows 2000 | Online user education bookmarks |

Bảng chứa nội dung của thư mục hồ sơ người dùng điển hình:

| Mục | Mô tả |
|---|---|
| Thư mục Application data * | Dữ liệu chương trình cụ thể, thí dụ từ điển tuỳ biến. Những người bán chương trình quyết định dữ liệu gì được cất trong thư mục hồ sơ người dùng. |
| Thư mục Cookies | Thông tin người dùng và các tham chiếu. |
| Thư mục Desktop | Các mục màn hình nền bao gồm các file, các shortcut, và các thư mục. |
| Thư mục Favourites | Các shortcut tới các vị trí ưa thích trên Internet. |
| Thư mục FrontPageTempDir | Thư mục tạm dùng bởi Microsoft Front Page. |
| Thư mục Local Settings * | Dữ liệu ứng dụng, lịch sử, các file tạm. Dữ liệu ứng dụng đi theo người dùng bằng hồ sơ người dùng lang thang. |
| Thư mục My Documents | Các tài liệu người dùng. |
| Thư mục My Pictures | Các mục ảnh người dùng. |
| Thư mục NetHood * | Shortcut tới các mục My Network Places. |

| Mục | Mô tả |
|---|---|
| Thư mục PrintHood * | Shortcut tới các thư mục máy in. |
| Thư mục Recent * | Shortcut tới các tài liệu và thư mục mới truy cập gần đây nhất. |
| Thư mục SendTo * | Shortcut tới các tài liệu xử lý hữu ích . |
| Thư mục Start Menu | Shortcut tới các mục chương trình. |
| Thư mục Templates | Các mục mẫu người dùng. |
| File NTUSER.DAT * | Lưu giữ những thiết lập đăng ký người dùng. |

### 8.4.6 Các thư mục đích (Home Folders)

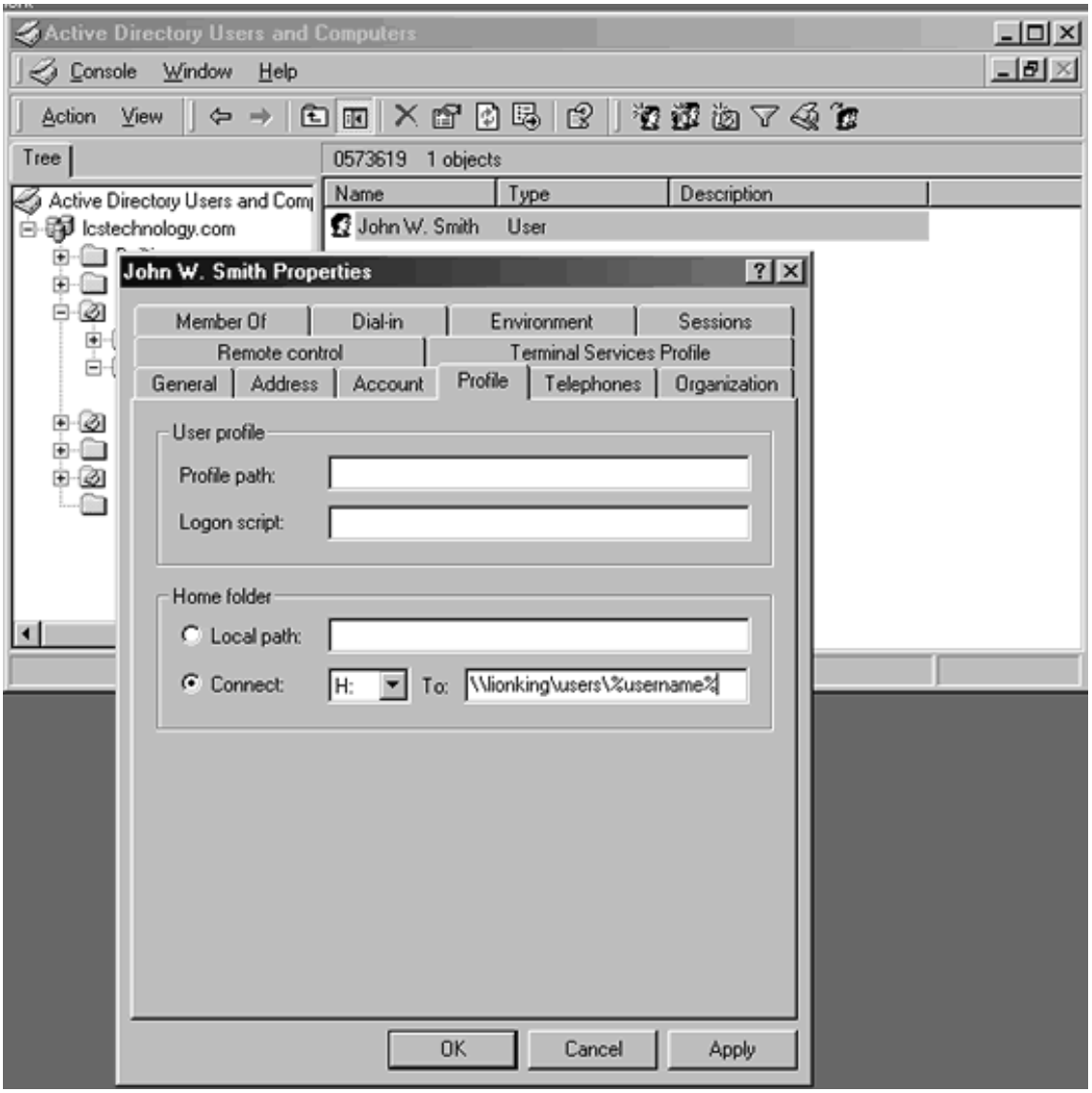
Thư mục đích (home) là thư mục để người dùng lưu giữ tài liệu. Bạn có thể lưu thư mục đích trên máy tính của bạn nhưng phổ biến hơn nó được lưu trên thư mục chia sẻ của máy chủ. Mặc dù các thư mục đích được hiện thực trên bảng Profile của hộp thoại Properties, chúng vẫn không được lưu như là một phần của hồ sơ lang thang. Cho nên, kích thước của thư mục đích không ảnh hưởng đến giao dịch trên mạng trong quá trình đăng nhập bởi vì nó không phải sao chép tới máy cục bộ. Đặt tất cả các thư mục đích trên một vị trí trung tâm của máy chủ làm cho các tác vụ quản trị như back up dữ liệu dễ dàng hơn.

- Ưu điểm của việc để các thư mục đích trên máy chủ
  - Người dùng có thể truy cập vào các thư mục đích từ bất kỳ máy trạm nào trên mạng.
  - Tập trung hoá việc back up và quản trị dữ liệu.
  - Các thư mục đích có thể được truy cập từ các máy chạy trên các hệ điều hành bất kỳ của Microsoft (bao gồm MS-DOS, Windows 95, Windows 98, và Windows 2000).
- Tạo các thư mục đích trên máy chủ

Để tạo thư mục đích cho tài khoản người dùng, bạn phải có quyền quản trị đối tượng mà tài khoản người dùng nhắm tới:

1. Tạo thư mục dùng chung để cất tất cả các thư mục trên máy chủ mạng. Các thư mục người dùng được lưu trên thư mục chia sẻ này.
2. Với thư mục chia sẻ, loại bỏ quyền mặc định Full Control từ nhóm Everyone, gán Full Control tới nhóm Users. (Việc này đảm bảo chỉ những người dùng xác thực với tài khoản người dùng miền mới có thể truy cập tới thư mục dùng chung).
3. Tại hộp thoại Properties của người dùng trong trình đơn Active Directories Users and Computers, chọn bảng Profile và sau đó tạo đường dẫn tới thư mục đích. Vì thư mục đích ở trên máy chủ, nhấn Connect định rõ ổ cứng để người dùng kết nối tới thư mục này. Trong hộp To, chỉ rõ tên UNC (địa chỉ đến một tập tin trong mạng cục bộ) cho thư mục, ví dụ, *\\server_name\shared_folder_ name\user_ logon_name*. Thay vì gõ

tên đăng nhập thực sự của người dùng, bạn gõ biến *%username%*. Hệ thống sẽ tự động tạo thư mục với tên đăng nhập của người dùng và gán các quyền cho người dùng. Thí dụ, gõ ***\\server_name\Users\%username%.***



# Câu hỏi ôn tập chương 8

1. Loại tài khoản nào cho phép người dùng đăng nhập vào Domain để truy cập các tài nguyên mạng?
   a. Local user accounts
   b. Default user accounts
   c. Domain user accounts
   d. Built-in user accounts
2. Loại tài khoản nào cho phép người dùng đăng nhập vào máy tính riêng biệt để truy xuất tài nguyên chỉ trên máy tính đó?
   a. Local user accounts
   b. Default user accounts
   c. Domain user accounts
   d. Built-in user accounts
3. Loại tài khoản nào cho phép người dùng thực hiện các tác vụ quản trị hoặc truy xuất các nguồn tài nguyên mạng ?
   a. Local user accounts
   b. Default user accounts
   c. Domain user accounts
   d. Built-in user accounts
4. Mỗi một Domain Controller định thời tái tạo bản sao tài khoản người dùng mới tới tất cả các Domain Controller khác trong toàn domain.
   a. Đúng
   b. Sai
5. Có hai loại Built-In User Accounts được tạo tự động khi cài đặt Windows 2000 Server là:
   a. Administrator account
   b. Guest account.
   c. User account
6. Trước khi tạo tài khoản người dùng cần xem xét những điều gì dưới đây:
   a. Naming Conventions
   b. Quantity user accounts
   c. Password Requirements
   d. Logon Hours and Workstation Restrictions
   e. User Account Planning Sheet
7. Người sử dụng không thể tự động thay đổi mật khẩu của mình. Chỉ những nhà quản trị mới có thể thay đổi được mật khẩu của người dùng.
   a. Đúng
   b. Sai
8. Người dùng có thể truy cập vào các thư mục đích từ bất kỳ máy trạm nào trên mạng.
   a. Đúng.
   b. Sai.
9. Chỉ những người quản trị hệ thống mới có thể thay đổi các hồ sơ bắt buộc.
   a. Đúng.
   b. Sai.
10. Một trong những ưu điểm của hồ sơ người dùng là cho phép nhiều người cùng sử dụng chung một máy tính, và khi họ đăng nhập vào mạng thì màn hình của họ được thiết lập giống như máy tính cá nhân của họ trong lần đăng nhập trước.
    a. Đúng
    b. Sai.

# CHƯƠNG 9 - QUẢN TRỊ TÀI KHOẢN NHÓM

## MỤC TIÊU CỦA CHƯƠNG

*Kết thúc chương này, sinh viên sẽ có thể:*

- Hiểu được cơ chế quản trị tài khoản user thông qua quản trị nhóm
- Nắm được các loại nhóm trong Windows 2000
- Biết cách lập kế hoạch tạo nhóm
- Nắm được các bước tạo, xoá và thêm các thành viên vào nhóm

## 9.1. Các loại nhóm trong Windows 2000

Nhóm bao gồm nhiều thành viên. Nhóm được dùng trong windows 2000 để đơn giản cho công việc quản trị mạng và dùng để gán quyền sử dụng cho một số tài nguyên trên mạng.

### 9.1.1 Các dạng nhóm (Type group)

Trong windows 2000, chia ra làm 2 dạng nhóm: *Nhóm Security* và *nhóm Distribution*. Cả hai dạng nhóm này đều được lưu trữ trên Active Directory nên chúng có thể truy cập từ bất kỳ nơi đâu trên hệ thống.

*Nhóm Security*: hệ thống windows 2000 chỉ sử dụng nhóm Security để cấp các quyền sử dụng tài nguyên trên hệ thống. Nhóm Security cũng có những đặc tính như nhóm Distribution.

*Nhóm Distribution*: dùng cho những mục đích không có tính bảo mật như gởi thông tin. Ta có thể đưa các thành viên vào trong một nhóm sau đó gởi thông tin đến nhóm này thì tất cả các thành viên đều nhận được thông tin .

### 9.1.2 Phạm vi của nhóm (Group Scopes)

Có 3 dạng: nhóm *Global* – nhóm *Domain Local* – nhóm *Universal*

*Nhóm Global*: chỉ bao gồm các thành viên trên một domain mà tạo ra nhóm này. Nó có thể truy cập vào bất kỳ tài nguyên nào trên các domain khác nhau thuộc cây domain hay rừng domain

*Nhóm Domain Local*: khác với nhóm Global, nhóm Domain Local có thể bao gồm nhiều thành viên trên các domain khác nhau, tuy nhiên chúng được tạo ra để truy cập vào các tài nguyên trên cùng domain nào mà tạo ra nhóm này.

*Nhóm Universal*: là sự kết hợp của nhóm Global và nhóm Domain Local, tuy nhiên chỉ hổ trợ cho những hệ thống mà chỉ toàn là Windows 2000 trở lên (Native mode)

### 9.1.3 Local Group

Nhóm Local được tạo trên các trạm làm việc sử dụng Windows 2000 hay trên các server thành viên của một mạng máy tính. Nhóm Local có đặc điểm sau:

- Chỉ chứa các tài khoản user trên máy tính trên đó nhóm Local được tạo ra.
- Không thể chứa các nhóm khác.

## 9.2. Lập kế hoạch nhóm Local Domain và nhóm Global

Một vấn đề quan trọng trong việc quản trị các nhóm là lập kế hoạch cho các nhóm trên. Sau đây là một số gợi ý.

- Gán tất cả các thành viên có chung một công việc vào Global group. Ví dụ tạo ra một nhóm có tên PGKETOAN và đưa tất cả các thành viên trong phòng này vào nhóm trên.

- Tạo Domain Local Group đối với các tài nguyên dùng chung trên hệ thống. Việc định dạng ra các tài nguyên dùng chung trên hệ thống để các thành viên có thể truy cập tới và tạo ra các Domain Local Group cho các tài nguyên này. Ví dụ như nếu công ty có một máy in màu, tạo ra domain local group có tên là PRINTCOLOR.

- Đưa tất cả các Global Group nào cần truy cập tài nguyên vào domain local group. Ví dụ đưa Global Group PGKETOAN vào trong domain local group PRINTCOLOR.

- Gán quyền truy cập tài nguyên vào domain local group. Ví dụ gán quyền truy cập máy in màu vào nhóm PRINTCOLOR để mọi thành viên có thể dùng máy in.

## 9.3. Tạo và xoá các nhóm

### 9.3.1 Tạo nhóm

Chọn Start → Programs → Administrative Tools → Active Directory users and computers (Hình 9.1)

Chọn tên domain → Users Container → new → Group (Hình 9.2)

Điền vào một số thông tin trong cửa sổ New Group như : tên nhóm, dạng nhóm, phạm vi của nhóm.

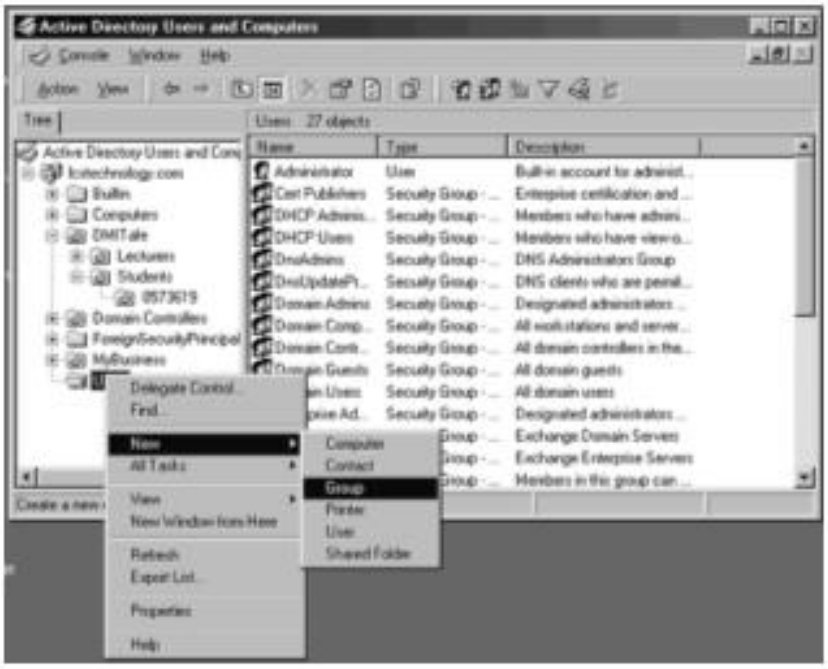
### 9.3.2 Xóa nhóm

Mỗi nhóm tạo ra đều có một SID (security Identifier), windows 2000 dùng SID để gán quyền cho các đối tượng.

Khi xóa nhóm thì các thành viên trong nhóm không bị xóa và tất cả các tài nguyên liên kết với nó cũng bị xóa theo

Để xóa nhóm, đơn giản chọn tên nhóm, nhấn chuột phải → delete

*Hình 9.1* Cách chọn Active Directory Service




*Hình 9.2* Cách chọn Group trong Active Directory

## 9.4. Thêm các thành viên vào nhóm

### 9.4.1 Built-in Group

Trong windows 2000 có một số các nhóm được tạo sẵn sau khi cài đặt xong. Đối với Windows NT 4.0 bao gồm các nhóm : Built-In Local, Built-in Global, System. Trong Windows 2000, các nhóm này được mở rộng và chia ra làm 4 nhóm: Predefine, Local, Global và Special Identifier .

- Nhóm định nghĩa trước (Predefined Group)

Nhóm này có phạm vi toàn cục, thường dùng để gom những tài khỏan người dùng có tính chất giống nhau. Theo mặc định Windows 2000 sẽ tự động đưa các thành viên vào một trong các nhóm thuộc Predefined Global. Người quản trị có thể đưa thêm một số thành viên vào Predefine Global, để thực hiện chế độ phân quyền cho các thành viên này.

Khi hệ thống là một domain, Windows 2000 sẽ tạo ra nhóm Predefined Global trong thư mục USERS trong Active Directory, các nhóm Predefined này không có quyền thừa kế, các nhóm này có quyền bằng cách đưa nhóm Global vào trong nhóm Domain Local hoặc có thể gán quyền trực tiếp trên chúng.

Sau đây là một số nhóm Prdefined Global

| **Predefined Global Group** | **Mô tả** |
|---|---|
| Domain Admins | Windows 2000 tự động đưa Domain Admins vào trong nhóm Domain Local có sẵn với tên là Administrators sao cho các thành viên trong Domain Admins có thể thực hiện công việc quản trị mạng trên hệ thống. Mặc định, người Administrator sẽ là thành viên thuộc nhóm này |
| Domain Guests | Windows 2000 tự động đưa Domain Guests vào nhóm Domain Local có sẵn với tên là Guests. Mặc định tài khoản Guest là thành viên thuộc nhóm này. |
| Domain Users | Windows 2000 tự động đưa Domain Users vào nhóm tự có Domain Local có tên Users. Mặc định, các tài khoản người dùng Administrator, Guest IUSR_*computername*, IWAM_ *computername*, Krbtgt, và TsInternet là những thành viên thuộc nhóm này. |
| Enterprise Admins | Người quản trị có thể đưa các thành viên vào nhóm Enterprise Admins để các thành viên này có quyền giám sát hệ thống. Sau đó đưa Enterprise Admins vào nhóm Domain Local có tên Administrators trong mỗi domain. Mặc định, người Administrator sẽ là thành viên thuộc nhóm này. |

- Các nhóm có sẵn (Built-in Groups)

Nếu như các nhóm Predefined có phạm vi toàn cục, thì các nhóm Built-in do Windows 2000 tạo ra có phạm vi cục bộ miền. Windows 2000 sẽ tạo ra nhóm Built-in Global trong thư mục BuiltIn trong Active Directory, các nhóm này có quyền trên toàn domain và trong Active Direcoty. Chúng có các quyền của nhóm Prdefined.

Sau đây là một số nhóm có sẵn (Built-in Groups)

| **Built-in Group** | **Mô tả** |
|---|---|
| Account Operators | Các thành viên có thể tạo, xóa, thay đổi các tài khỏan người dùng và các nhóm, tuy nhiên không thể thay đổi nhóm Administrators hay bất kỳ nhóm operators nào. |
| Administrators | Các thành viên có thể thực hiện tất cả các công việc quản trị trên tất cả Domain Controllers và chính trên domain đó. Mặc định, tài khoản Administrator và các nhóm toàn cục định nghĩa trước Domain Admins và Enterprise Admins là các thành viên. |
| Backup Operators | Các thành viên có thể thực hiện viêc lưu trữ (backup) và phục hồi trên Domain Controllers dùng Windows Backup. |
| Guests | Các thành viên chỉ có thể truy cập vào những tài nguyên cho phép; các thành viên không có quyền thay đổi các cài đặt về môi trường làm việc. Mặc định, các tài khoản user Guest, IUSR_*computername*, IWAM_*computername*, và TsInternet và nhóm toàn cục định nghĩa trước Domain Guests là các thành viên thuộc nhóm này. |
| Pre-Windows 2000 Compatible Access | Cho phép các thành viên có quyền đọc trong domain. Mặc định, chỉ có nhóm hệ thống Everyone pre-Windows 2000 là thành viên |
| Print Operators | Các thành viên có thể cài đặt và quản lý máy in trên mạng. |
| Replicator | Hổ trợ Chức năng nhân bản thư mục. |
| Server Operators | Các thành viên có thể chia xẻ các tài nguyên trên đĩa, lưu trữ, phục hồi các file trên một domain controller. |
| Users | Các thành viên có thể truy cập vào các tài nguyên của mình. Mặc định, các nhóm Authenticated Users và INTERACTIVE pre-Windows 2000 và nhóm toàn cục định nghĩa trước Domain Users là những thành viên của nhóm này. |

- Built-in Local Group

Trong tất cả các máy chạy Windows 2000 dù là server hay professional đều có nhóm Buitl-in Local. Chúng chỉ cho phép tất cả các thành viên trong nhóm này sử dụng tài nguyên trên chính máy đó, Các nhóm này được tạo trong thư mục Groups trong công cụ Local User Manager. Trên các máy domain controller không tồn tại nhóm Local và nhóm Built-in Local. Sau đây là các nhóm Built-in Local:

| Group | Mô tả |
|---|---|
| Administrators | Các thành viên có thể thực hiên công việc quản trị mạng trên máy tính này .Mặc định, Administrator là thành viên của nhóm. Khi có một server thành viên hoặc máy tính chạy Windows 2000 gia nhập vào một domain, Windows 2000 sẽ đưa nhóm toàn cục định nghĩa trước Domain Admins vào nhóm Administrators cục bộ. |
| Backup Operators | Các thành viên nhóm này có thể dùng Windows Backup để lưu trữ và phục hồi dữ liệu trên máy.. |
| Guests | Các thành viên chỉ có thể truy cập vào những tài nguyên cho phép; các thành viên không có quyền thay đổi các cài đặt về môi trường làm việc. Mặc định, Guest là thành viên. Khi có một server thành viên hoặc máy tính chạy Windows 2000 gia nhập vào một domain, Windows 2000 sẽ đưa nhóm toàn cục định nghĩa trước Domain Guests vào nhóm Guests cục bộ. |
| Power Users | Các thành viên có thể tạo và thay đổi các tài khoản user cục bộ trên máy tính cục bộ và chia xẻ các tài nguyên trên máy tính đó. |
| Replicator | Hổ trợ chức năng nhân bản thư mục. |
| Users | Các thành viên có thể truy cập vào các tài nguyên của mình. Mặc định, Windows 2000 sẽ đưa các tài khoản cục bộ được tạo ra trên máy vào trong nhóm Users . Khi có một server thành viên hoặc máy tính chạy Windows 2000 gia nhập vào một domain, Windows 2000 sẽ đưa nhóm nhóm toàn cục định nghĩa trước Domain Users vào nhóm Users cục bộ. |

- Nhóm định danh đặc biệt (Special Identifier Groups)

Mỗi máy tính chạy windows 2000 đều có các nhóm Special Identifier hay còn gọi các nhóm System.

Sau đây là các nhóm Special Identifier:

| Group | Mô tả |
|---|---|
| Anonymous Logon | Bao gồm bất kỳ tài khỏan người dùng mà Windows 2000 không xác nhận |
| Authenticated Users | Bao gồm tất cả tài khoản người dùng hợp lệ có tạo ra trong máy hay trong Active Directory. Dùng nhóm này để ngăn chặn quyền truy xuất bất hợp pháp của người dùng. |
| CREATOR OWNER | Bao gồm những người cho phép tạo ra các files hay thư mục. Nếu một thành viên thuộc nhóm Administrators tạo ra một tài nguyên nào đó thì tài nguyên đó thuộc quyền Administrators |
| Dialup | Bao gồm bất kỳ ai có thể kết nối vào mạng qua modem. |
| Everyone | Bao gồm tất cả mọi người đang truy cập vào máy tính. Theo mặc định nhóm này được gán quyền Full Control, do đó bất kỳ người nào cũng có toàn quyền trên bất kỳ tài nguyên nào của hệ thống. |
| Interactive | Bao gồm các tài khỏan cho phép người dùng có thể kết nối vào hệ thống. Các thành viên của nhóm này có thể truy cập vào bất kỳ máy nào tại bất kỳ nơi đâu. |
| Network | Bao gồm bất kỳ người nào có thể kết nối vào mạng để truy cập tài nguyên . |

# Câu hỏi ôn tập chương 9

1. Có ba phạm vi cho các nhóm được tạo ra trong domain là:

   a. Global groups b. Local groups
   c. Domain local groups d. Universal groups

2. Tên các nhóm có sẵn (built-in group) trong Windows 2000 là ..... (chọn 3)

   a. Users b. Administrators
   c. System d. Guests

3. Nhóm tài khoản nào mà Administrator có thể xoá trong các nhóm tài khoản sau:

   a. Users b. Guests
   c. Bult-in groups d. Created groups by the Administrator

4. Các nhóm nào trong các nhóm sau có thể chứa một số các tài khoản user từ một domain được nhóm lại với nhau.

   a. Global groups b. Local groups
   c. Domain local groups d. Universal groups

5. Những nhóm nào trong các nhóm sau đây được sử dụng để gán các quyền tới các tài nguyên.

   a. Global groups b. Local groups
   c. Domain local groups d. Universal groups

6. Những nhóm nào trong các nhóm sau đây được sử dụng để gán các quyền tới các tài nguyên liên quan trong nhiều domain.

   a. Global groups b. Local groups
   c. Domain local groups d. Universal group

# TÀI LIỆU THAM KHẢO

[1] DMIT – Network Maintenance Text Book, 2000
[2] MCSE Training Kit - Microsoft Windows 2000 Server / Microsoft Corporation. Microsoft Press, 2000.
[3] MCSE Training Kit – Networking Essentials Plus, 3rd ed. Microsoft press, 1999.
[4] Nguyễn Thúc Hải - Mạng máy tính và các hệ thống mở, Nhà xuất bản giáo dục, Hà nội, 1997.

# BÀI GIẢNG
# MÔN: **MẠNG MÁY TÍNH**

Biên soạn: ThS. Trần Bá Nhiệm

# GIỚI THIỆU MÔN HỌC

- Mục đích của môn học
  - Kiến thức cơ bản về mạng máy tính
  - Mô hình tham khảo OSI
  - Mô hình TCP/IP
- Thời lượng: 5 buổi học

# GIỚI THIỆU MÔN HỌC

- Nội dung môn học
  - Chương 1: Tổng quan về mạng máy tính
  - Chương 2: Cấu trúc của mạng
  - Chương 3: Phương tiện truyền dẫn và thiết bị mạng
  - Chương 4: Data link
  - Chương 5: TCP/IP
  - Chương 6: Khái niệm cơ bản về bảo mật mạng
  - Bài tập

# CHƯƠNG 1:
# TỔNG QUAN VỀ MẠNG MÁY TÍNH

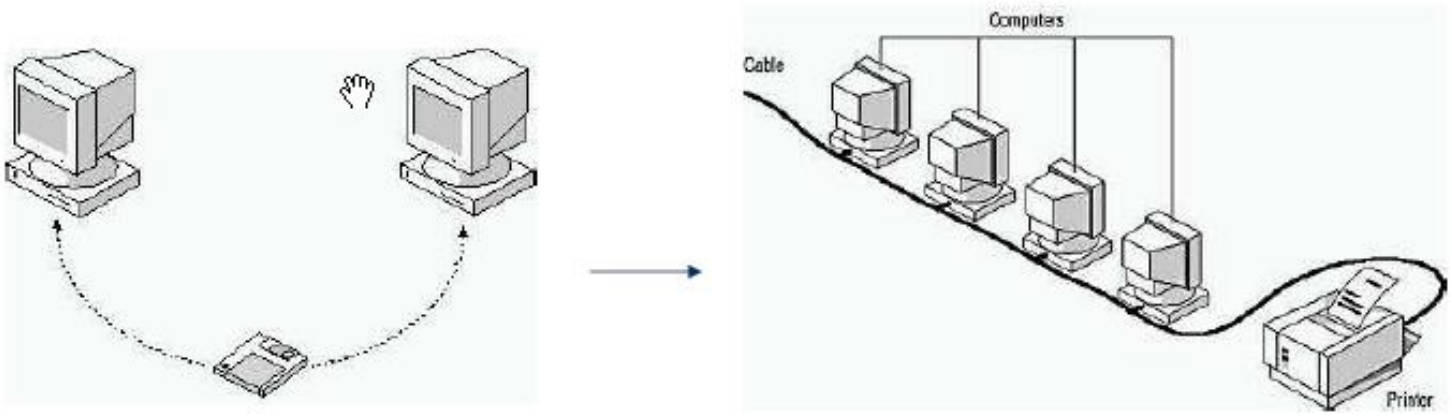
- Khái niệm về mạng máy tính
- Ứng dụng của mạng máy tính
- Phân loại mạng máy tính
- Mô hình OSI

# Khái niệm về mạng máy tính

- Một tập hợp của các máy tính độc lập được kết nối bằng một cấu trúc nào đó.
- Hai máy tính được gọi là kết nối nếu chúng có thể trao đổi thông tin.
- Kết nối có thể là dây đồng, cáp quang, sóng ngắn, sóng hồng ngoại, truyền vệ tinh…

# Ứng dụng của mạng máy tính

- Chia sẻ thông tin
- Chia sẻ phần cứng và phần mềm
- Quản lý tập trung

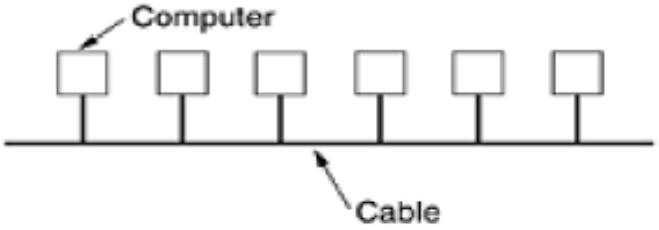


# Phân loại mạng máy tính

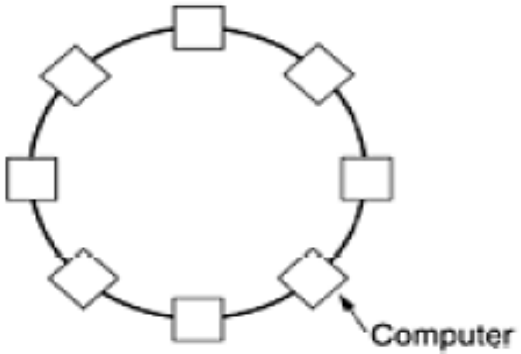
- Cách phân loại mạng máy tính được sử dụng phổ biến nhất là dựa theo khoảng cách địa lý của mạng: Lan, Man, Wan.
- Theo kỹ thuật chuyển mạch mà mạng áp dụng: mạng chuyển mạch kênh, mạng chuyển mạch thông báo, mạng chuyển mạch gói.
- Theo cấu trúc mạng: hình sao, hình tròn, tuyến tính…
- Theo hệ điều hành mà mạng sử dụng: Windows, Unix, Novell…

# LANs (Local Area Networks)

- Có giới hạn về địa lý
- Tốc độ truyền dữ liệu cao
- Tỷ lệ lỗi khi truyền thấp
- Do một tổ chức quản lý
- Sử dụng kỹ thuật Ethernet hoặc Token Ring
- Các thiết bị thường dùng trong mạng là Repeater, Brigde, Hub, Switch, Router.

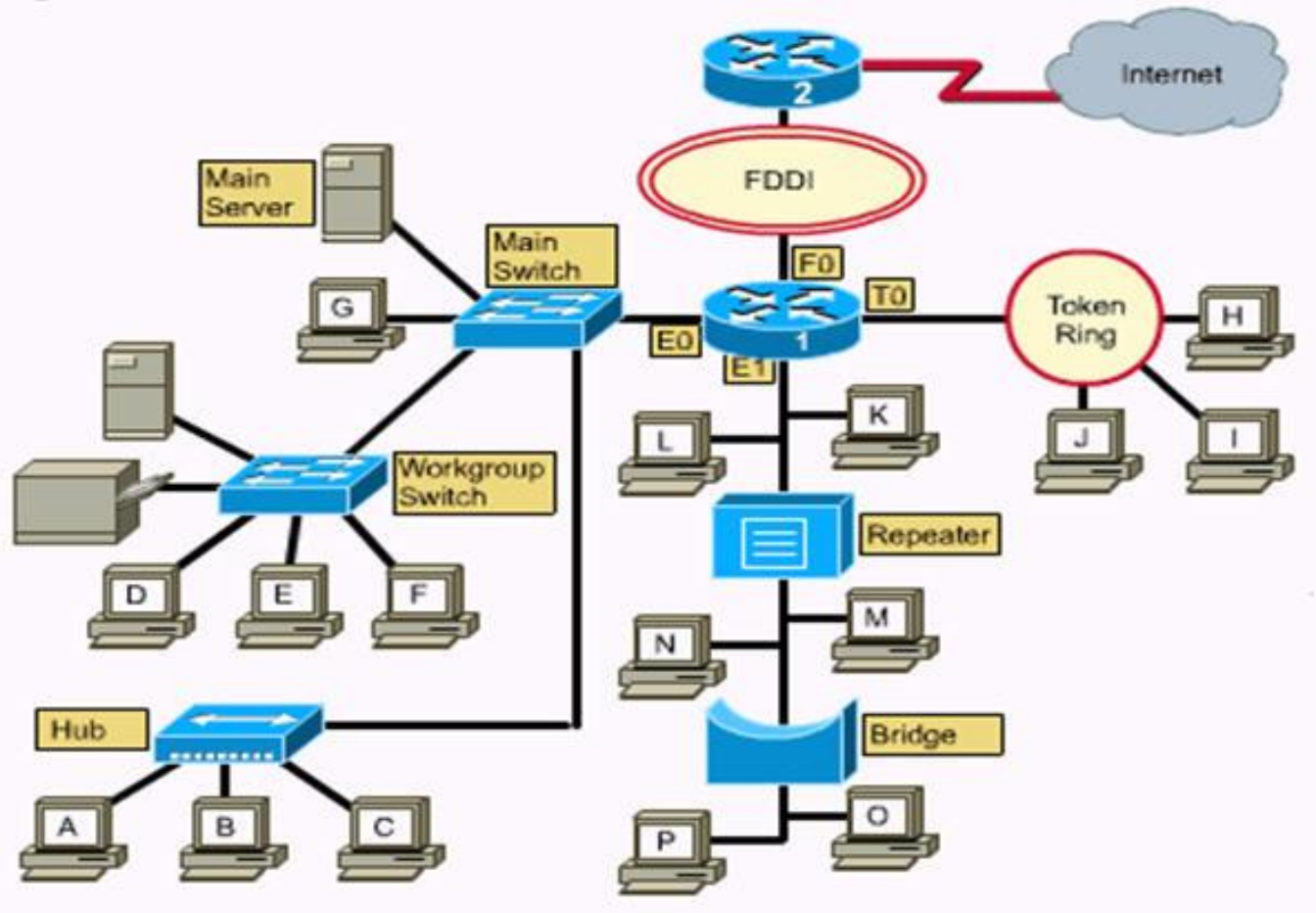



802.3 Ethernet



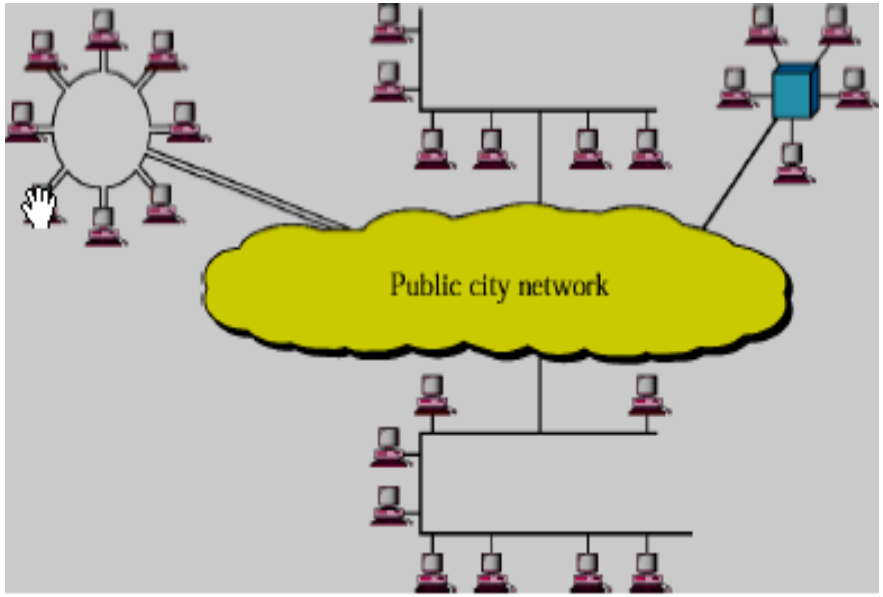

802.5 Token Ring

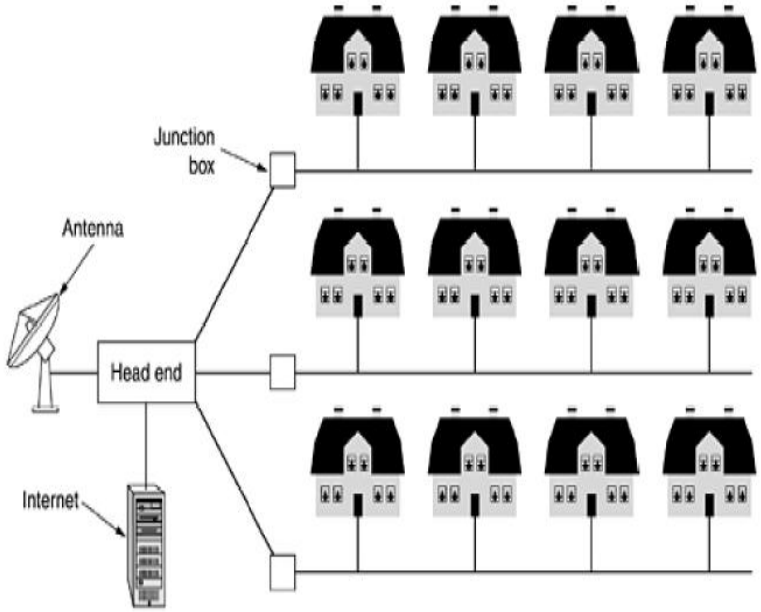
# LANs


Internet
2
FDDI
F0
T0
Token Ring
H
J
I
Main Server
Main Switch
G
E0
1
E1
K
L
Workgroup Switch
Repeater
D
E
F
M
N
Hub
Bridge
A
B
C
O
P

# MANs (Metropolitan Area Networks)

- Có kích thước vùng địa lý lớn hơn LAN
- Do một tổ chức quản lý
- Thường dùng cáp đồng trục hoặc cáp quang

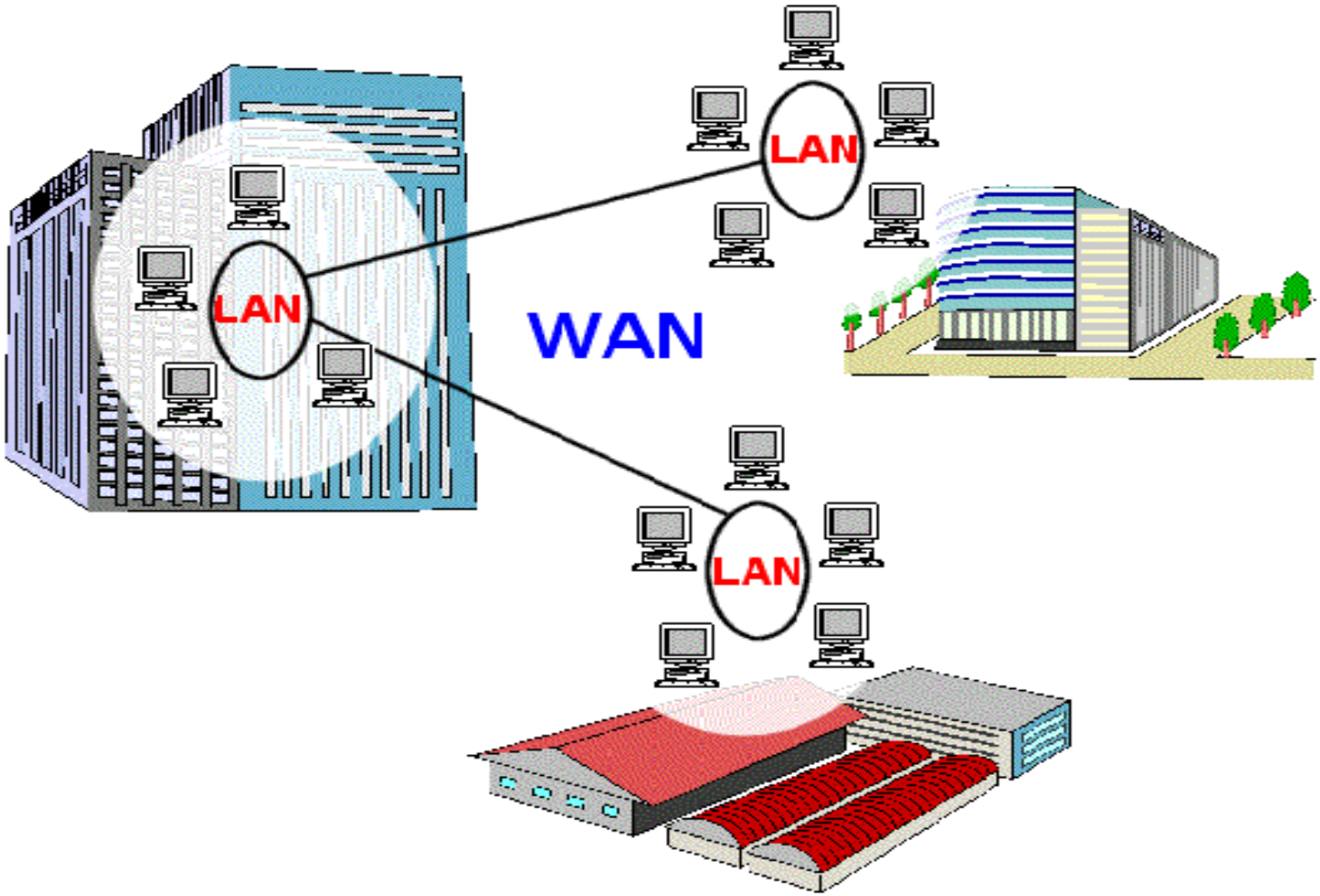


# WANs (Wide Area Networks)

- Là sự kết nối nhiều LAN
- Không có giới hạn về địa lý
- Tốc độ truyền dữ liệu thấp
- Do nhiều tổ chức quản lý
- Sử dụng các kỹ thuật Modem, ISDN, DSL, Frame Relay, ATM

# WANs (Wide Area Networks)



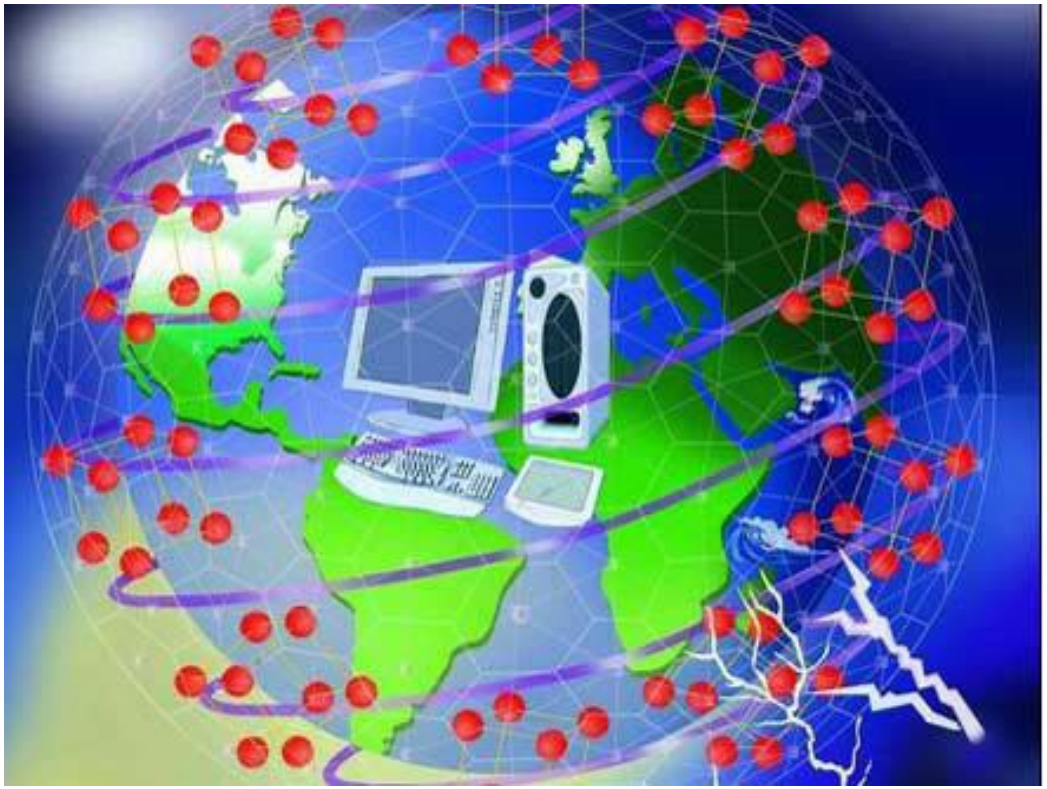
# Mạng không dây (Wireless Networking)

- Do tổ chức IEEE xây dựng và được tổ chức Wi-fi Alliance đưa vào sử dụng trên toàn thế giới.
- Có các tiêu chuẩn: chuẩn 802.11a, chuẩn 802.11b, chuẩn 802.11g (sử dụng phổ biến ở thị trường Việt Nam), chuẩn 802.11n (mới có).
- Thiết bị cho mạng không dây gồm 2 loại: card mạng không dây và bộ tiếp sóng/điểm truy cập (Access Point - AP).

# Mạng không dây

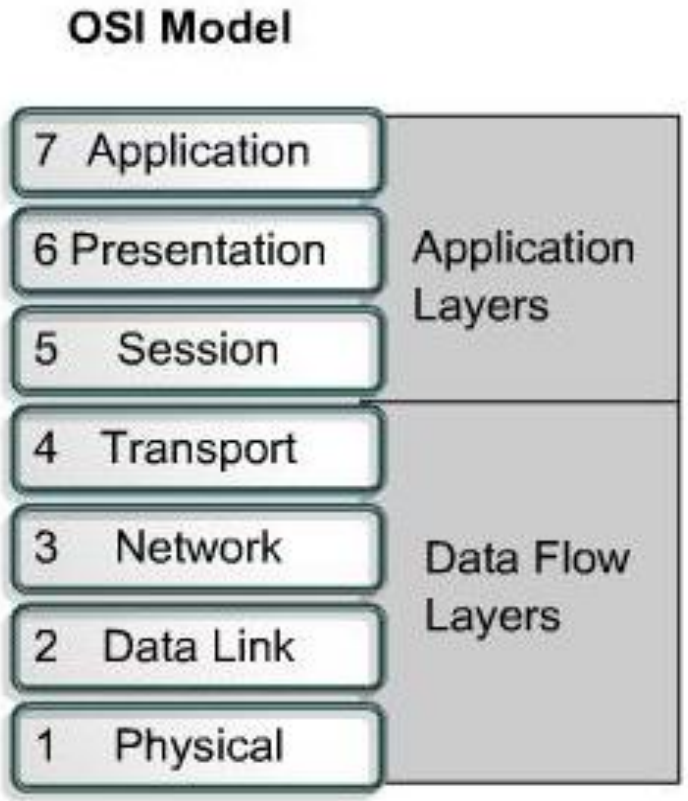
# Internet

Một hệ thống mạng của các máy tính được kết nối với nhau qua hệ thống viễn thông trên phạm vi toàn thế giới để trao đổi thông tin.

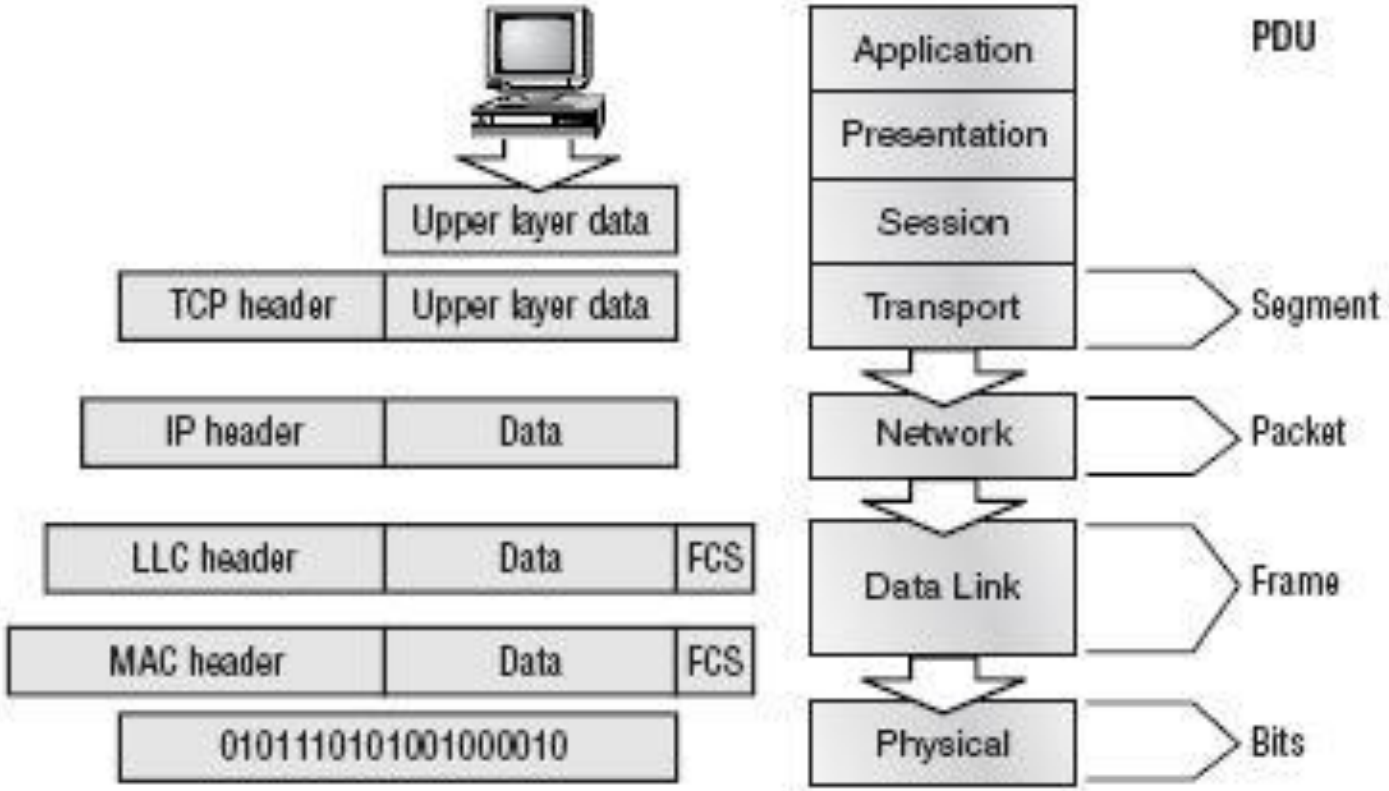


# Mô hình OSI
# (Open Systems Interconnection)

- Lý do hình thành: Sự gia tăng mạnh mẽ về số lượng và kích thước mạng dẫn đến hiện tượng bất tương thích giữa các mạng.
- Ưu điểm của mô hình OSI:
  - Giảm độ phức tạp
  - Chuẩn hóa các giao tiếp
  - Đảm bảo liên kết hoạt động
  - Đơn giản việc dạy và học

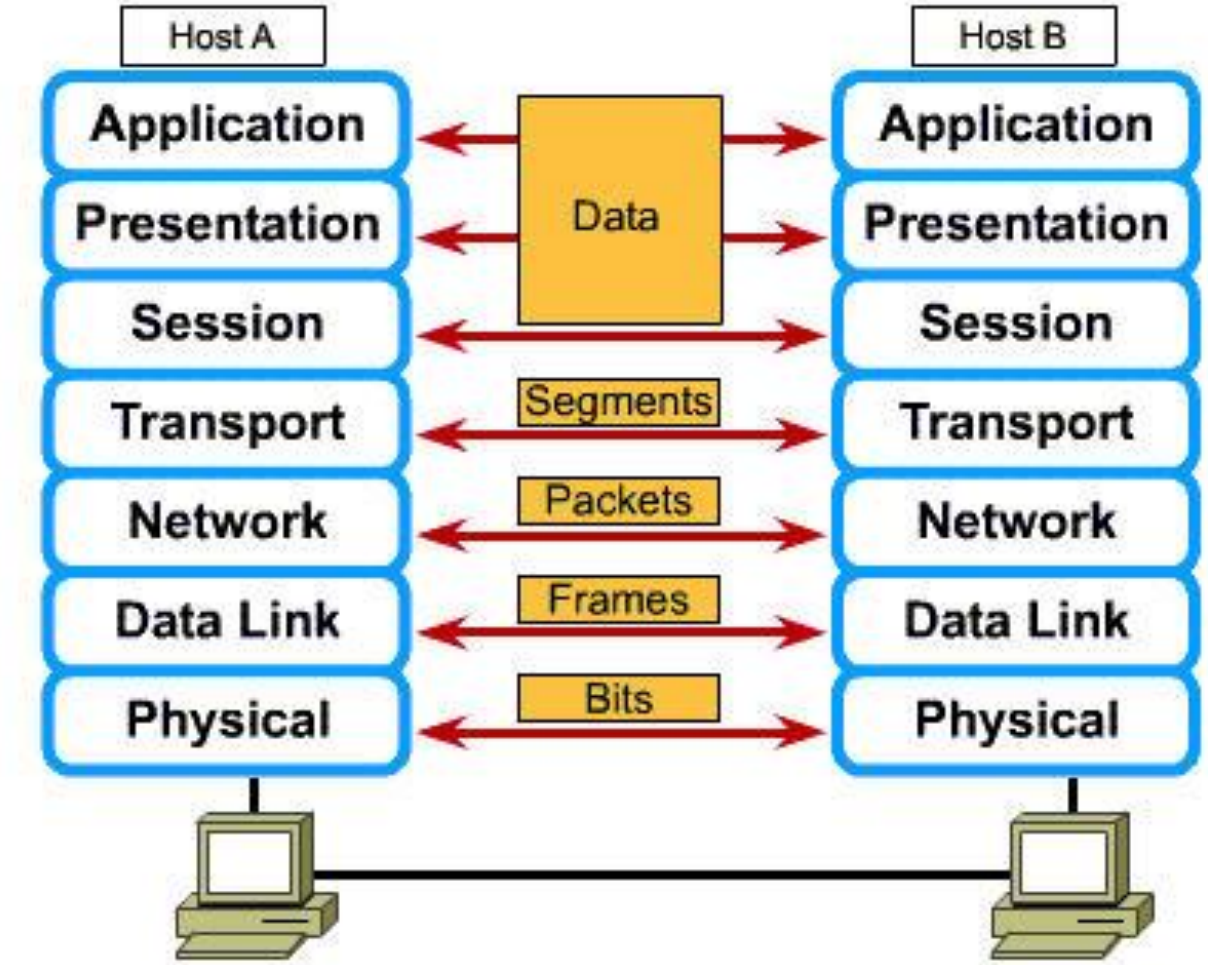


# Mô hình OSI

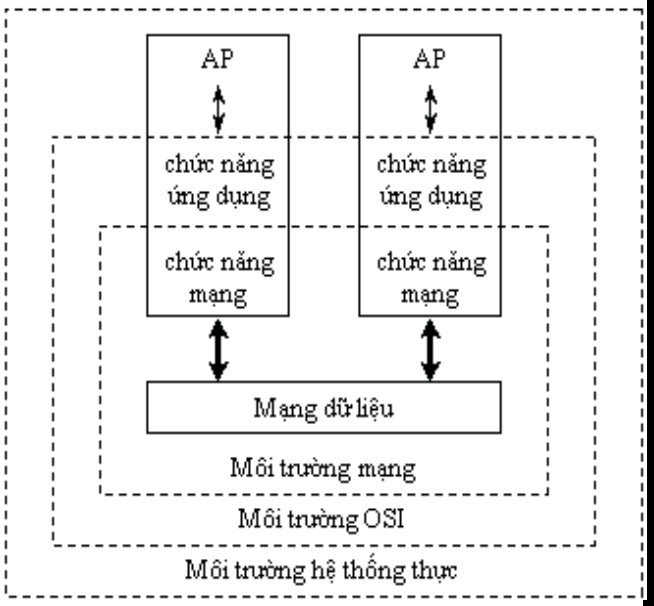


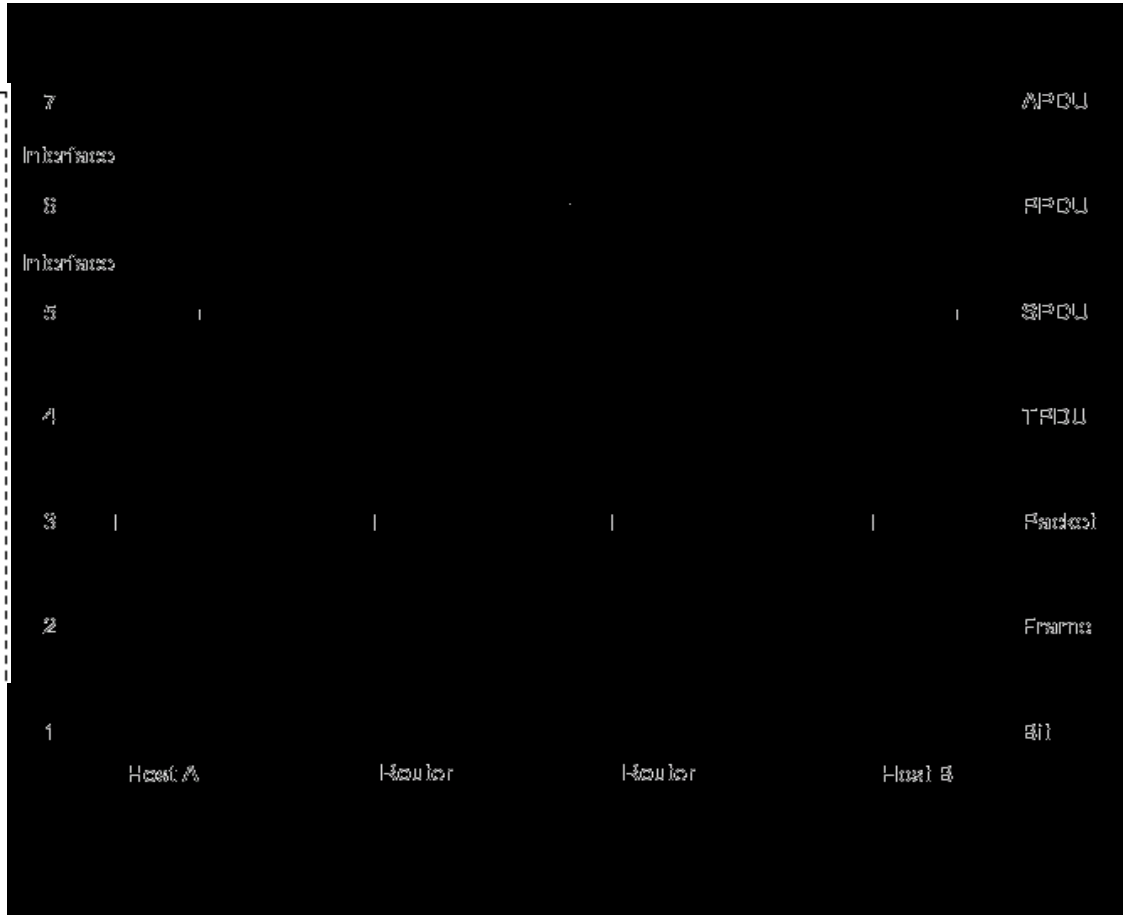

Đóng gói dữ liệu trên mạng

# Mô hình OSI


Host A
Host B
Application
Presentation
Session
Transport
Network
Data Link
Physical
Data
Segments
Packets
Frames
Bits
Application
Presentation
Session
Transport
Network
Data Link
Physical

# Mô hình OSI


AP
AP
chức năng ứng dụng
chức năng ứng dụng
chức năng mạng
chức năng mạng
Mạng dữ liệu
Môi trường mạng
Môi trường OSI
Môi trường hệ thống thực

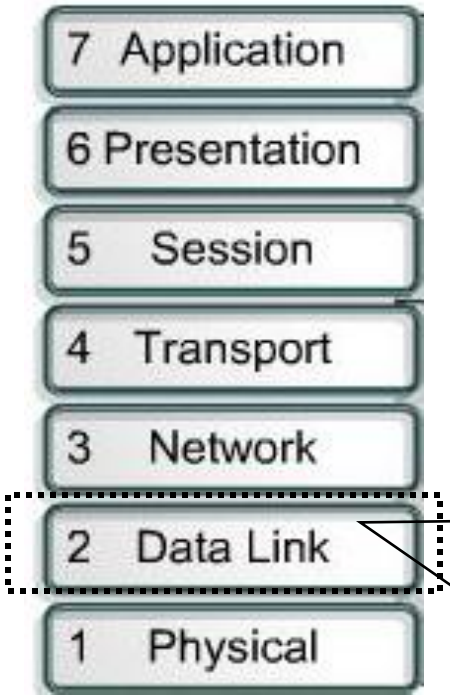

7
APDU
Interface
6
PPDU
Interface
5
SPDU
4
TPDU
3
Packet
2
Frame
1
Bit
Host A
Router
Router
Host B

# Mô hình OSI

**Truyền dẫn nhị phân**

- Dây, đầu nối, điện áp
- Tốc độ truyền dữ liệu
- Phương tiện truyền dẫn
- Chế độ truyền dẫn (simplex, half-duplex, full-duplex)

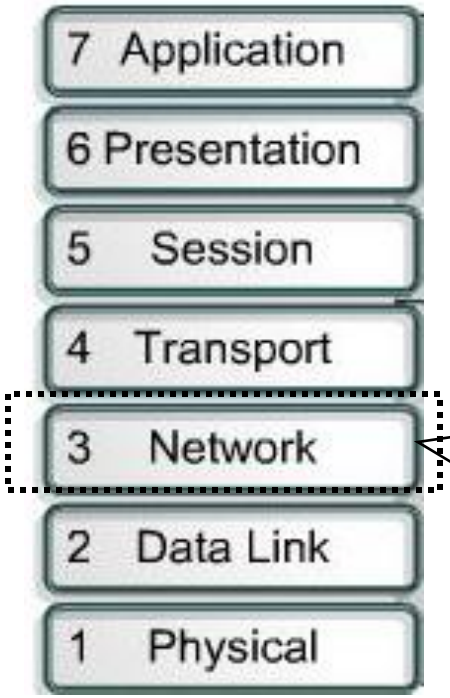
# Mô hình OSI




**Điều khiển liên kết, truy xuất đường truyền**

- Đóng Frame
- Ghi địa chỉ vật lý
- Điều khiển luồng
- Kiểm soát lỗi, thông báo lỗi

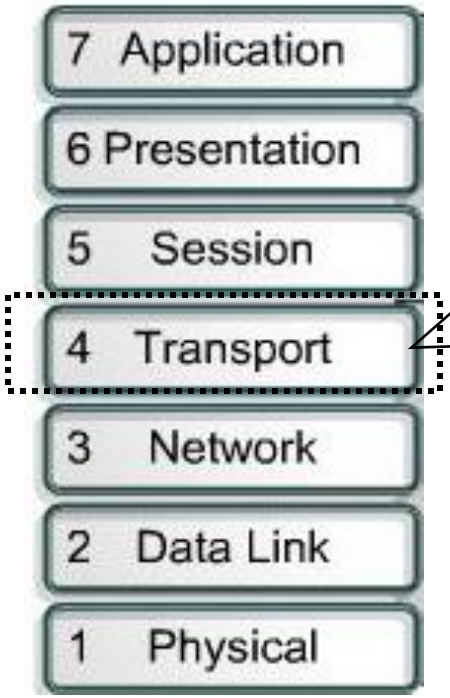
# Mô hình OSI




**Địa chỉ mạng và xác định đường đi tốt nhất**

- Tin cậy
- Địa chỉ luận lý, topo mạng
- Định tuyến (tìm đường đi) cho gói tin

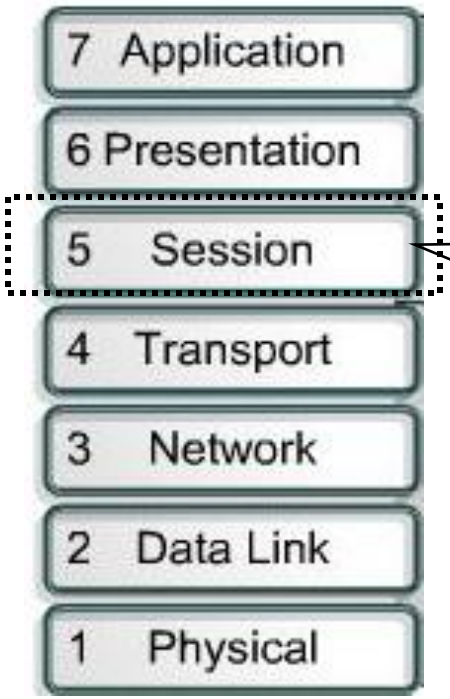
# Mô hình OSI




**Kết nối end-to-end**

- Vận chuyển giữa các host
- Vận chuyển tin cậy
- Thiết lập, duy trì, kết nối các mạch ảo
- Phát hiện lỗi, phục hồi thông tin và điều khiển luồng

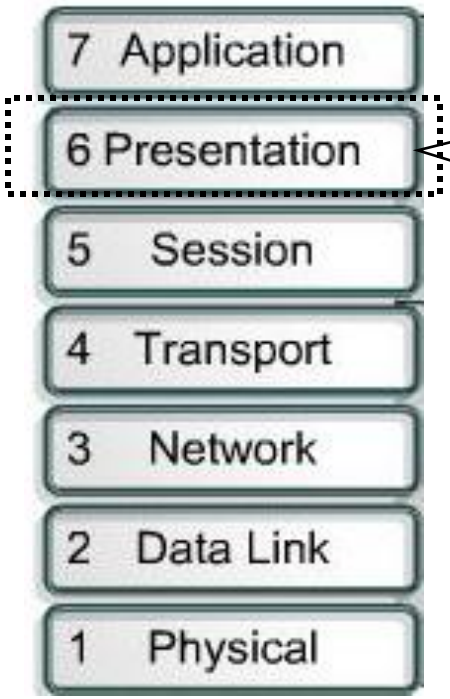
# Mô hình OSI




**Truyền thông liên host**

- Thiết lập, quản lý và kết thúc các phiên giữa các ứng dụng

# Mô hình OSI




**Trình bày dữ liệu**

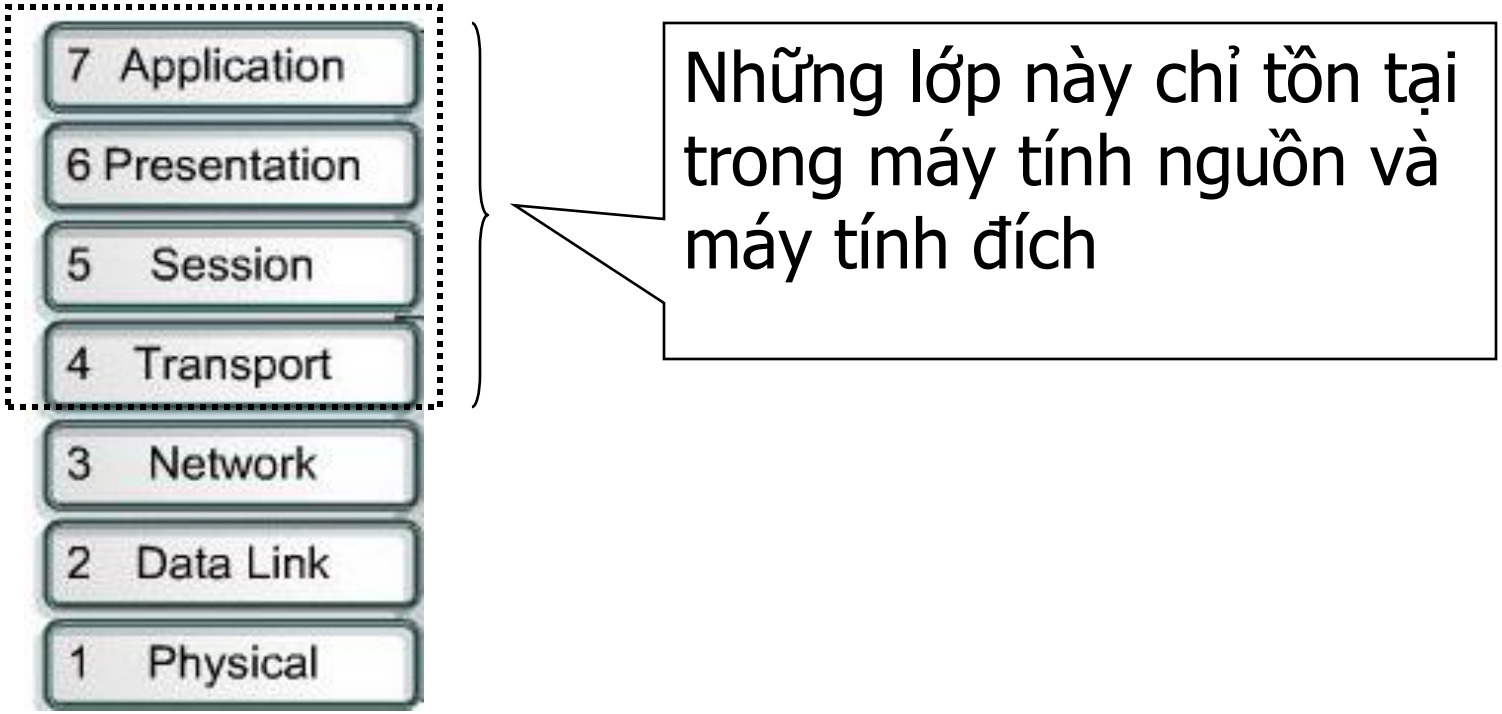
- Định dạng dữ liệu
- Cấu trúc dữ liệu
- Mã hóa
- Nén dữ liệu

# Mô hình OSI

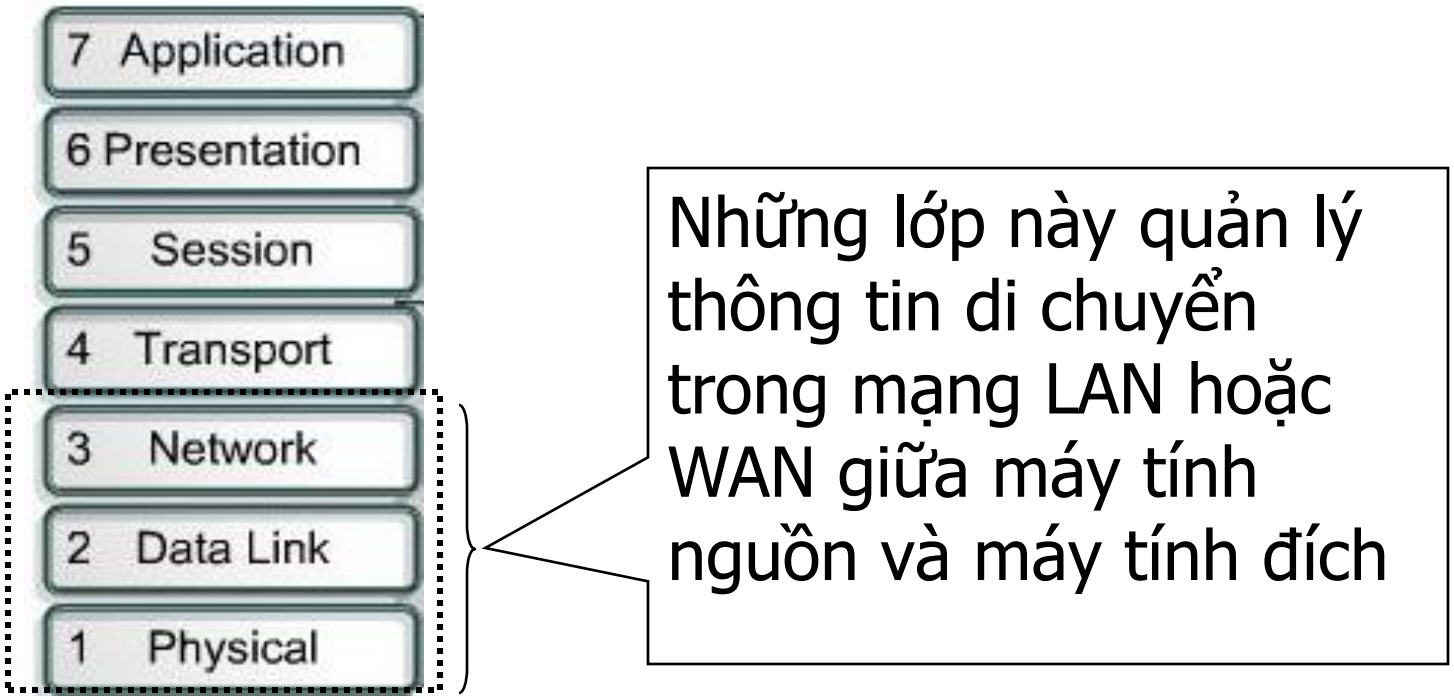
**Các quá trình mạng của ứng dụng**

- Xác định giao diện giữa người sử dụng và môi trường OSI
- Cung cấp các dịch vụ mạng cho các ứng dụng như email, truyền file…

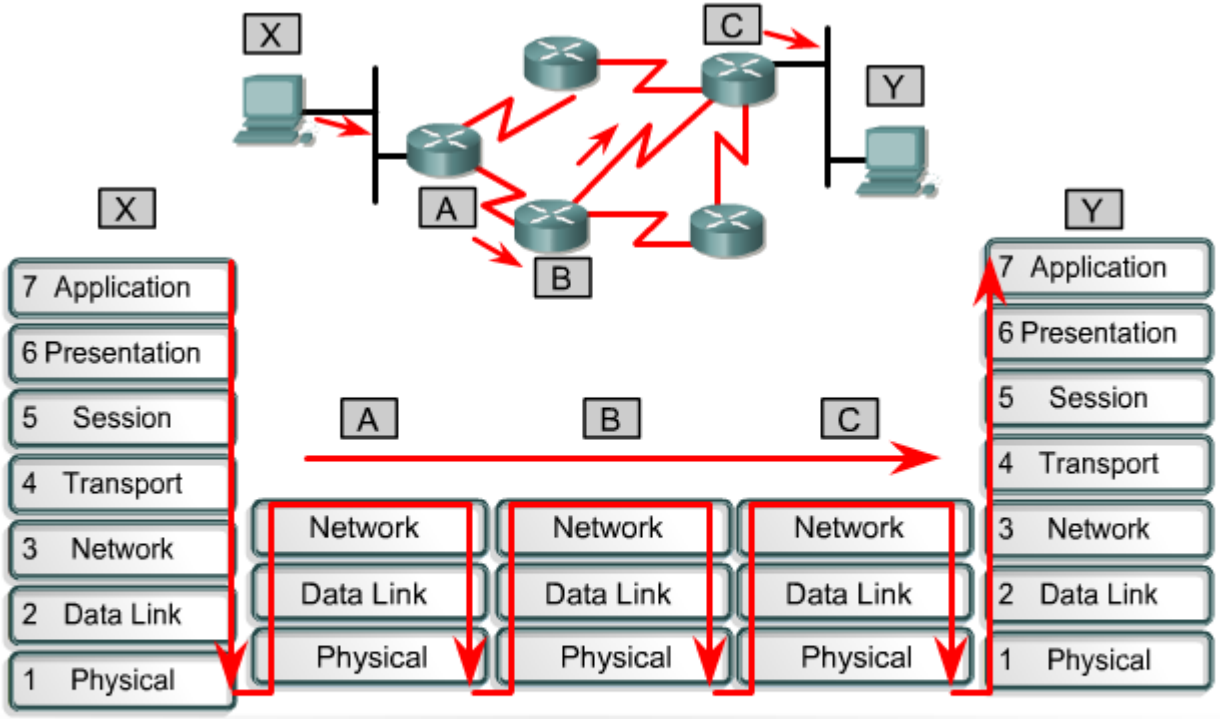
# Mô hình OSI


7 Application
6 Presentation
5 Session
4 Transport
3 Network
2 Data Link
1 Physical
Những lớp này chỉ tồn tại trong máy tính nguồn và máy tính đích

# Mô hình OSI


7 Application
6 Presentation
5 Session
4 Transport
3 Network
2 Data Link
1 Physical
Những lớp này quản lý thông tin di chuyển trong mạng LAN hoặc WAN giữa máy tính nguồn và máy tính đích

# Dòng dữ liệu trên mạng



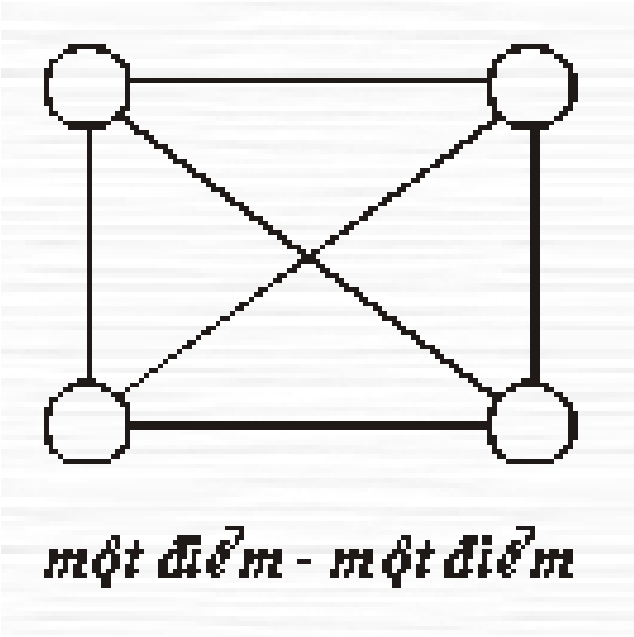

Data flow in a network focuses on layers one, two and three of the OSI model. This is after being transmitted by the sending host and before arriving at the receiving host.

# CHƯƠNG 2:
# CẤU TRÚC MẠNG (TOPOLOGY)

- Phương thức nối mạng
- Cấu trúc vật lý của mạng
- Giao thức truy cập đường truyền trên mạng LAN

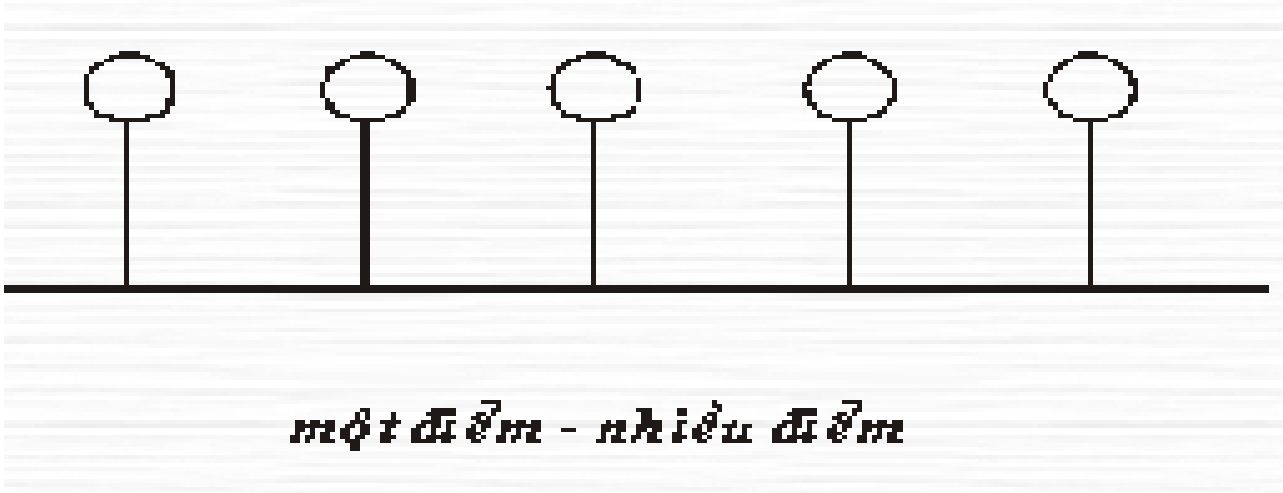
# Phương thức nối mạng

- Point-to-point (điểm – điểm): các đường truyền riêng biệt được thiết lập để nối các cặp máy tính lại với nhau.

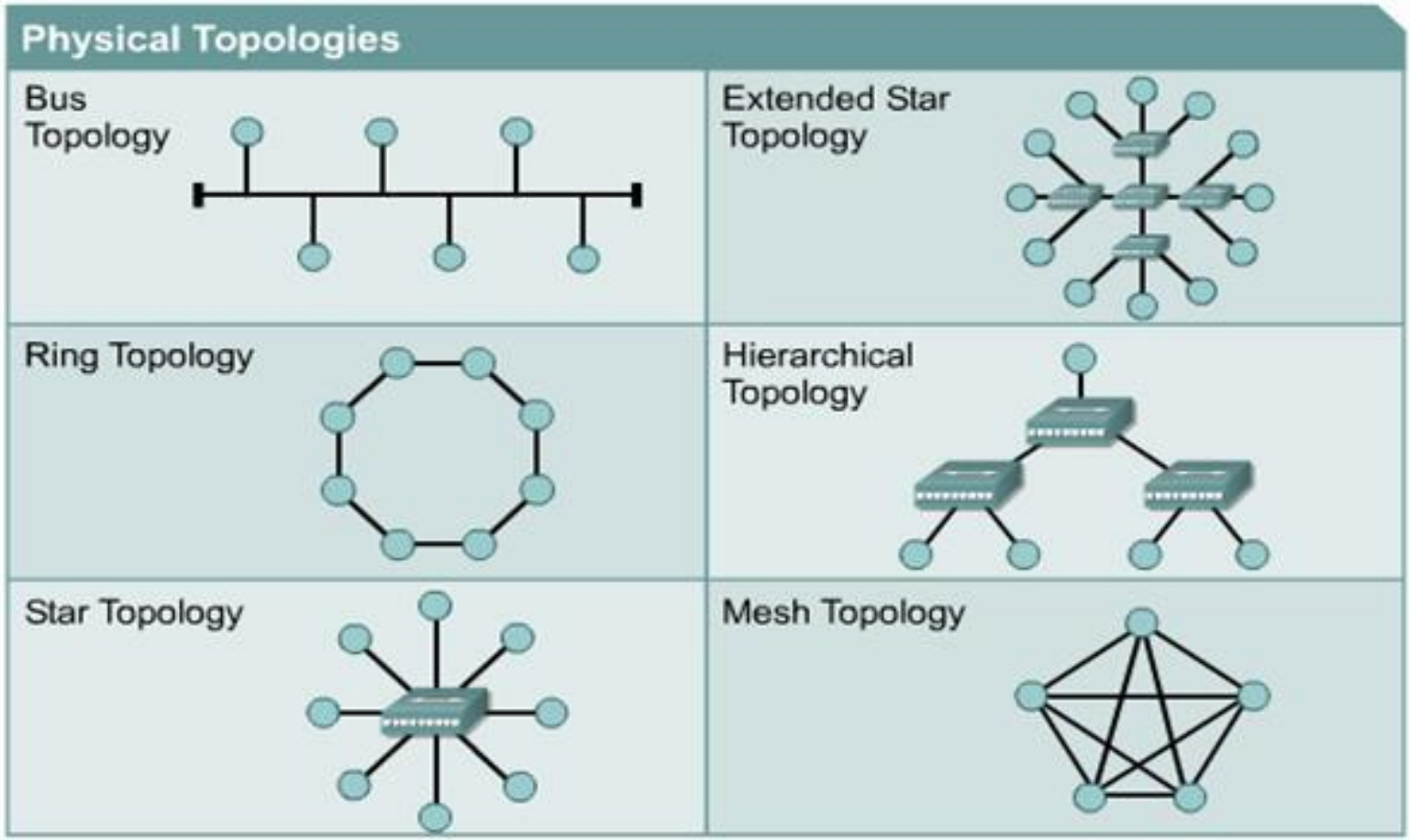


# Phương thức nối mạng

- Broadcast (một điểm - nhiều điểm): tất cả các trạm phân chia chung một đường truyền vật lý.



# Cấu trúc vật lý của mạng LAN

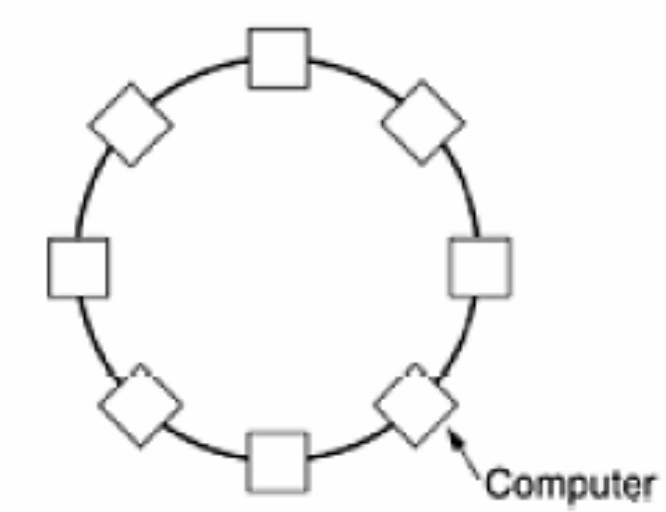


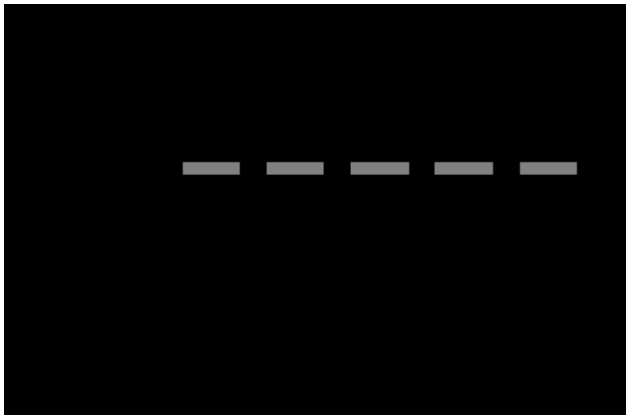
# Dạng đường thẳng (Bus Topology)

- Ưu điểm
  - Dễ dàng cài đặt và mở rộng
  - Chi phí thấp
  - Một máy hỏng không ảnh hưởng đến các máy khác.
- Hạn chế
  - Khó quản trị và tìm nguyên nhân lỗi
  - Giới hạn chiều dài cáp và số lượng máy tính
  - Hiệu năng giảm khi có máy tính được thêm vào
  - Một đoạn cáp backbone bị đứt sẽ ảnh hưởng đến toàn mạng

# Dạng vòng tròn (Ring Topology)

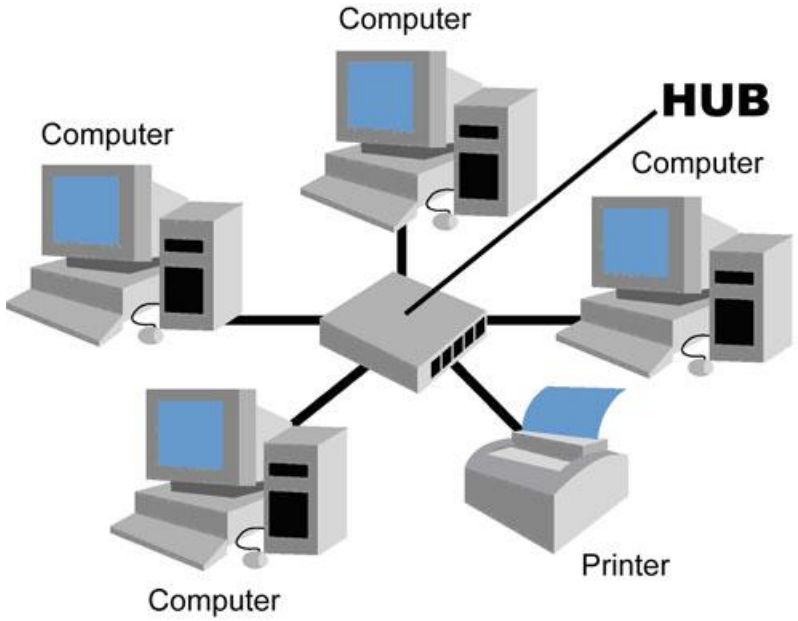
- Ưu điểm
  - Sự phát triển của hệ thống không tác động đáng kể đến hiệu năng
  - Tất cả các máy tính có quyền truy cập như nhau
- Hạn chế
  - Chi phí thực hiện cao
  - Phức tạp
  - Khi một máy có sự cố thì có thể ảnh hưởng đến các máy tính khác



# Dạng hình sao (Star Topology)

- Ưu điểm
  - Dễ dàng bổ sung hay loại bỏ bớt máy tính
  - Dễ dàng theo dõi và giải quyết sự cố
  - Có thể phù hợp với nhiều loại cáp khác nhau
- Hạn chế
  - Khi hub không làm việc, toàn mạng cũng sẽ không làm việc
  - Sử dụng nhiều cáp



# Giao thức truy cập đường truyền trên mạng LAN

Hai loại giao thức: ngẫu nhiên và có điều khiển

- Ngẫu nhiên
  - Giao thức chuyển mạch
  - Giao thức đường dây đa truy cập với cảm nhận va chạm
- Có điều khiển
  - Giao thức dùng thẻ bài vòng (Token Ring)
  - Giao thức dùng thẻ bài cho dạng đường thẳng (Token Bus)

# Giao thức truy cập đường truyền trên mạng LAN

- Giao thức chuyển mạch (yêu cầu và chấp nhận)

  Khi máy tính yêu cầu, nó sẽ được thâm nhập vào đường cáp nếu mạng không bận, ngược lại sẽ bị từ chối.

# Giao thức truy cập đường truyền trên mạng LAN

- Giao thức đường dây đa truy cập với cảm nhận va chạm (Carrier Sense Multiple Access/with Collision Detection)

  Gói dữ liệu chỉ được gởi nếu đường truyền rảnh, ngược lại mỗi trạm phải đợi theo một trong 3 phương thức:

  – Chờ đợi một thời gian ngẫu nhiên rồi lại bắt đầu kiểm tra đường truyền
  – Kiểm tra đường truyền liên tục cho đến khi đường truyền rảnh
  – Kiểm tra đường truyền với xác suất p (0<p<1)

# Giao thức truy cập đường truyền trên mạng LAN

- Giao thức dùng thẻ bài vòng (Token Ring)
  - Thẻ bài là một đơn vị dữ liệu đặc biệt có một bit biểu diễn trạng thái bận hoặc rảnh.
  - Thẻ bài chạy vòng quanh trong mạng.
  - Trạm nào nhận được thẻ bài rảnh thì có thể truyền dữ liệu.
- Giao thức dùng thẻ bài cho dạng đường thẳng (Token bus)

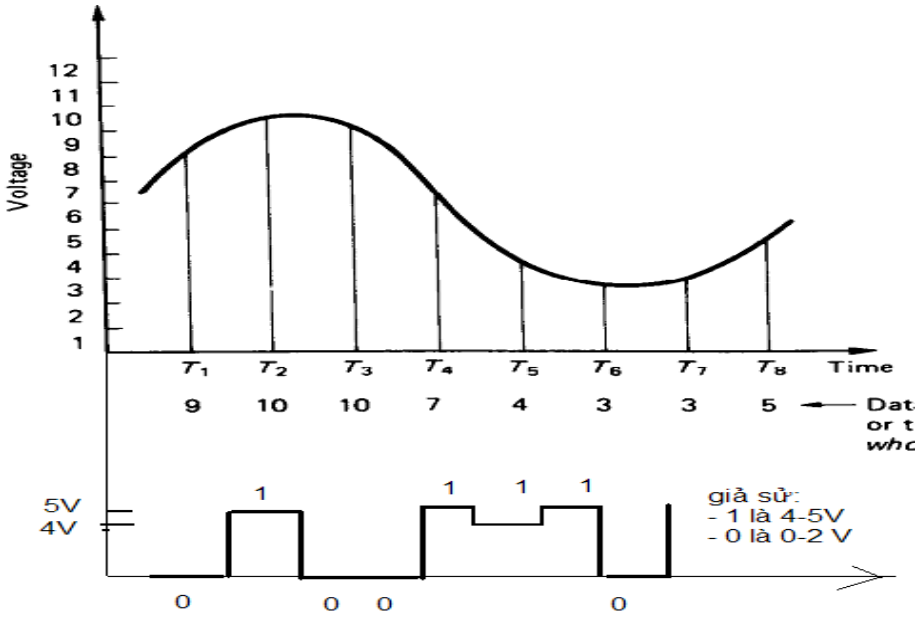
  Tạo ra một vòng logic (vòng ảo) và thực hiện giống Token Ring.

# CHƯƠNG 3:
# PHƯƠNG TIỆN TRUYỀN DẪN VÀ CÁC THIẾT BỊ LIÊN KẾT MẠNG

- Môi trường truyền dẫn
- Phương tiện truyền dẫn
- Các thiết bị liên kết mạng

# Môi trường truyền dẫn

- Là phương tiện vật lý cho phép truyền tải tín hiệu giữa các thiết bị.
- Hai loại phương tiện truyền dẫn chính:
  - Hữu tuyến
  - Vô tuyến
- Hệ thống sử dụng hai loại tín hiệu:
  - Digital
  - Analog



# Các đặc tính của phương tiện truyền dẫn

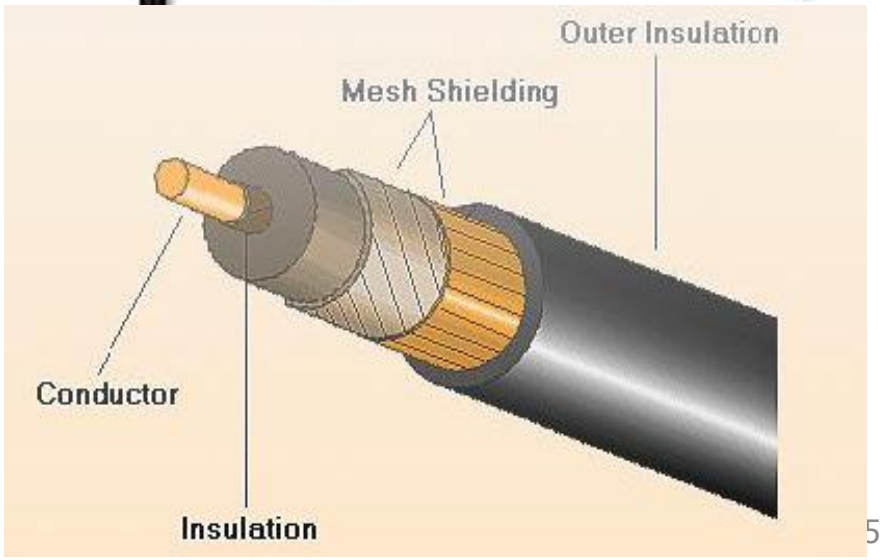
- Chi phí
- Yêu cầu cài đặt
- Băng thông (bandwidth).
- Băng tần (baseband, broadband)
- Độ suy dần (attenuation).
- Nhiễu điện từ (Electronmagnetic Interference - EMI)
- Nhiễu xuyên kênh (crosstalk)

# Phương tiện truyền dẫn

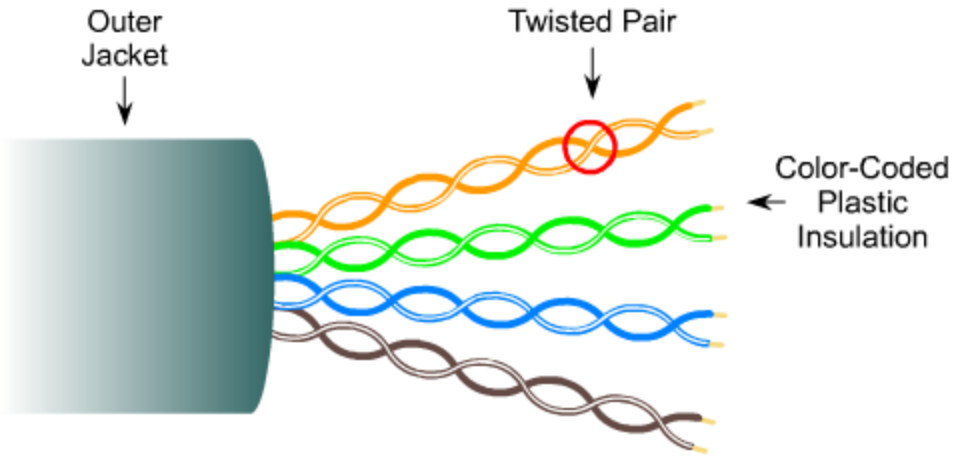
- Cáp đồng trục
- Cáp xoắn đôi
- Cáp quang
- Wireless

# Cáp đồng trục (coaxial)

- Cấu tạo
- Phân loại
  - Thinnet/Thicknet
  - Baseband/ Broadband
- Thông số kỹ thuật
  - Chiều dài cáp
  - Tốc độ truyền
  - Nhiễu
  - Lắp đặt/bảo trì
  - Giá thành
  - Kết nối

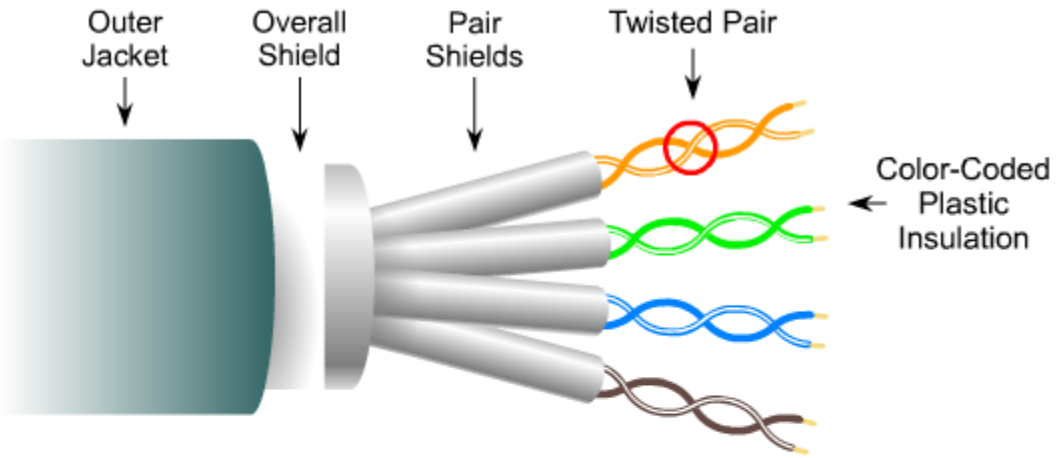


# Cáp xoắn đôi
# Unshielded Twisted Pair (UTP) Cable



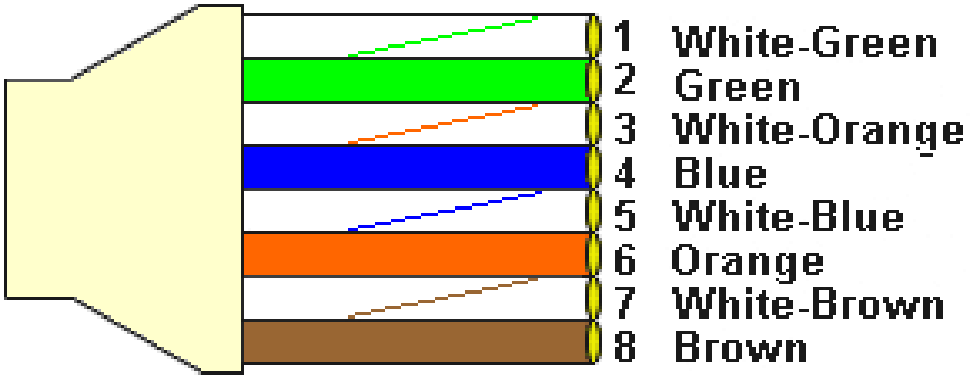

- Speed and throughput: 10 - 100 - 1000 Mbps (depending on the quality/category of cable)
- Average $ per node: Least Expensive
- Media and connector size: Small
- Maximum cable length: 100m

# Cáp xoắn đôi
# Shielded Twisted Pair (STP) Cable

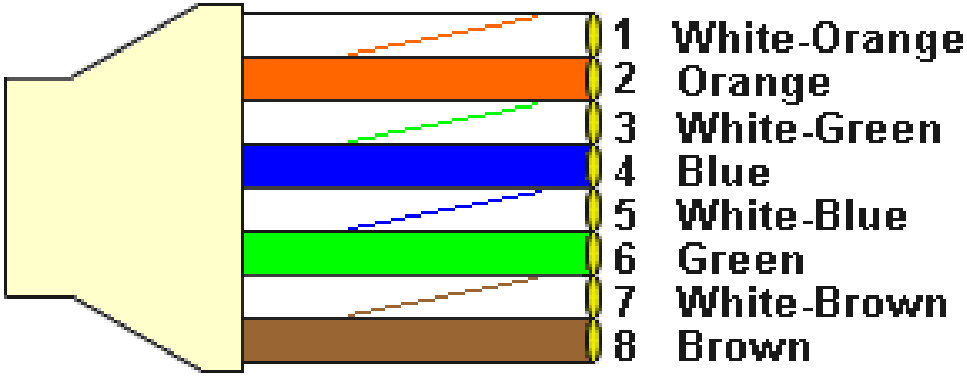



- Speed and throughput: 10 - 100 Mbps
- Average $ per node: Moderately Expensive
- Media and connector size: Medium to Large
- Maximum cable length: 100m

# Chuẩn cáp 568A & 568B

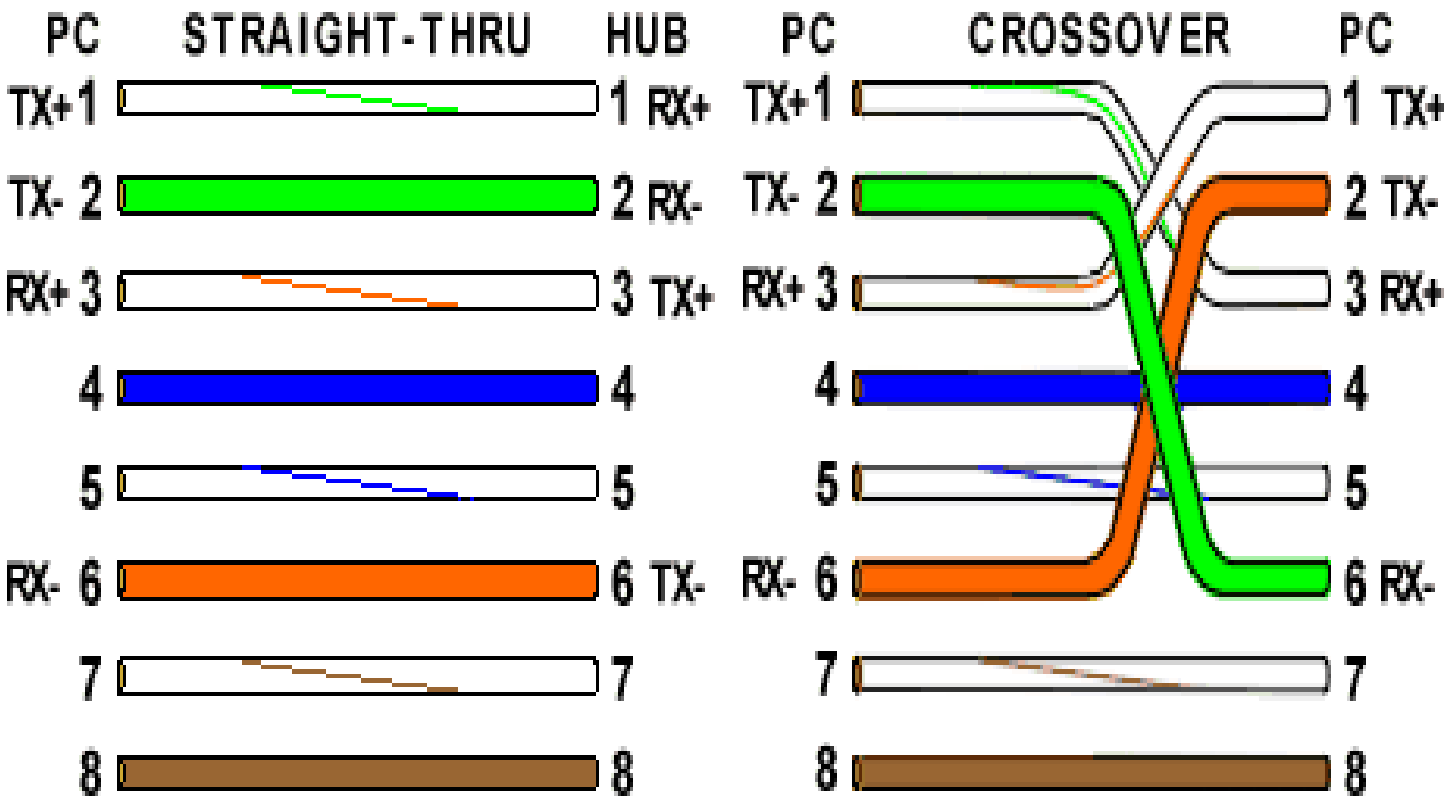



568A CABLE END



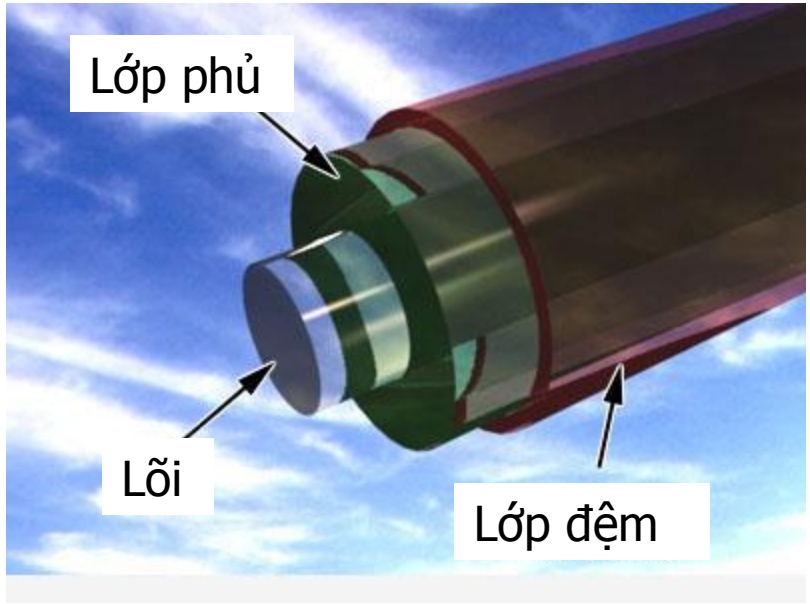

568B CABLE END

# Phương thức bấm Cáp

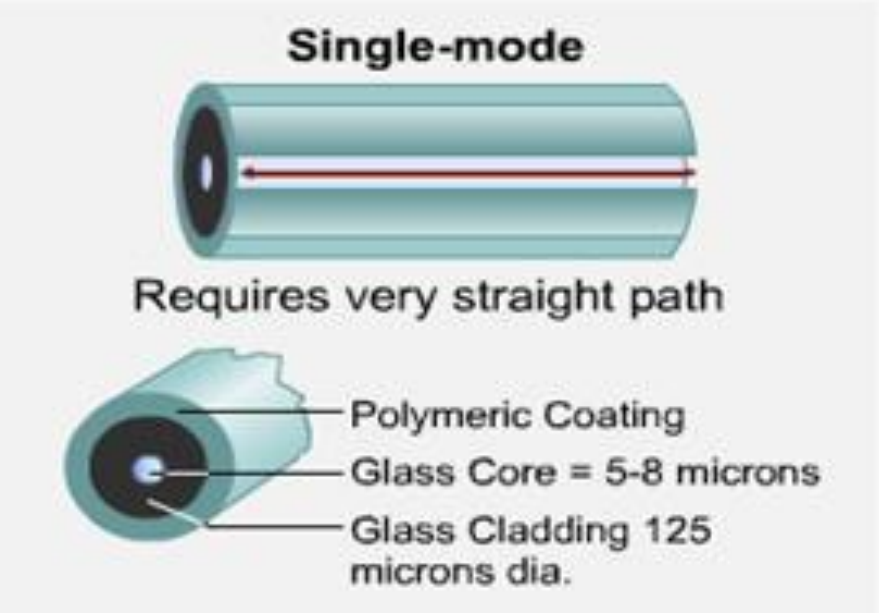


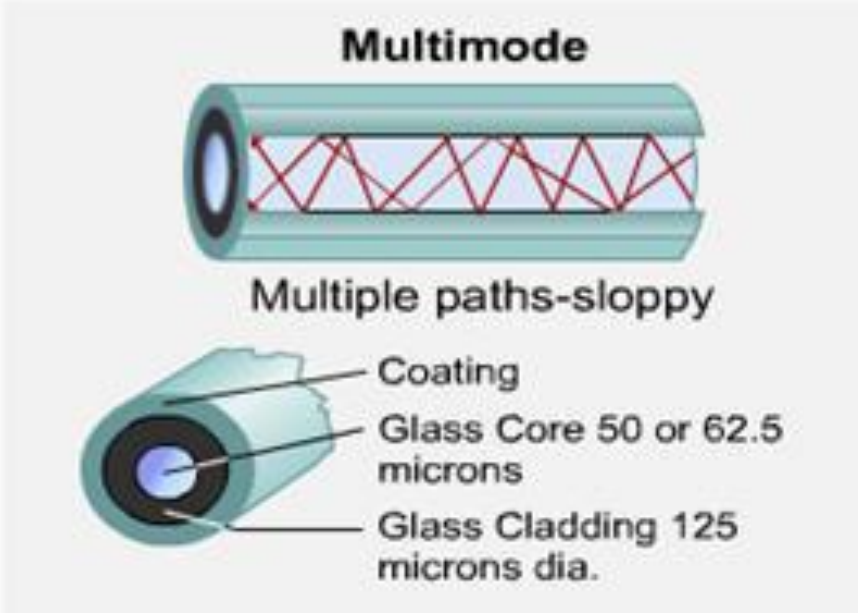
# Cáp quang (Fiber optic)

- Thành phần & cấu tạo
  - Dây dẫn
  - Nguồn sáng (LED, Laser)
  - Đầu phát hiện (Photodiode, photo transistor)
- Phân loại
  - Multimode stepped index
  - Multimode graded index
  - Single mode (mono mode)
- Thông số kỹ thuật
  - Chiều dài cáp
  - Tốc độ truyền
  - Nhiễu
  - Lắp đặt/bảo trì
  - Giá thành
  - Kết nối



# Cáp quang (Fiber optic)



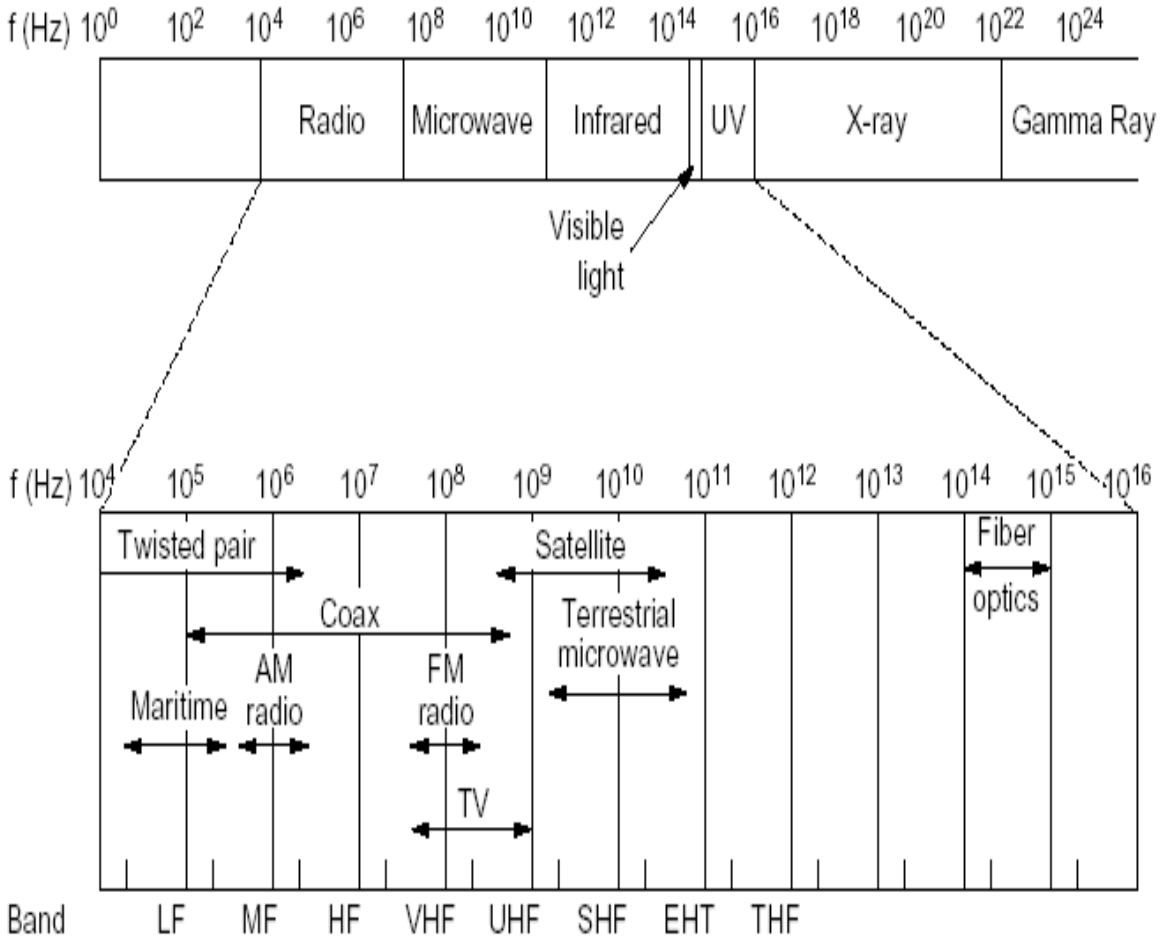



# Thông số cơ bản của các loại cáp

| Cáp | Chiều dài cáp tối đa | Tốc độ truyền | Lắp đặt | Nhiễu | Giá thành |
|---|---|---|---|---|---|
| UTP | 100 m | 10-100 Mbps | Dễ | Cao | Thấp nhất |
| STP | 100 m | 16-500 Mbps | Khá dễ | Thấp | Vừa phải |
| Thinnet | 185 m | 10 Mbps | Dễ | Thấp | Thấp |
| Thicknet | 500 m | 10 Mbps | Khó | Thấp | Cao |
| Fiber optics | 2000 m | 2 Gbps | Khó | Không | Đắt |

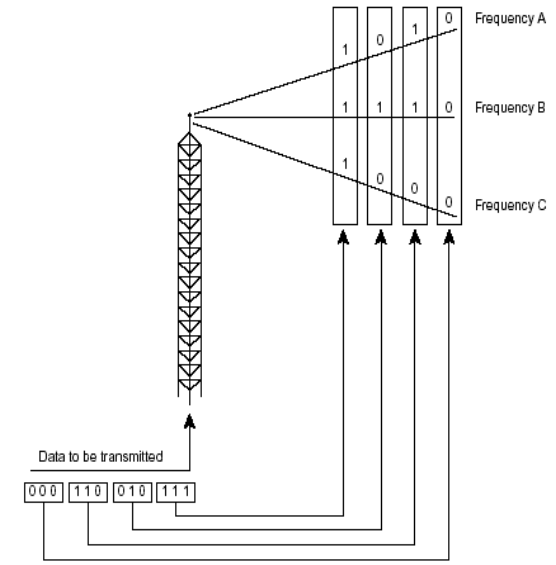
# Wireless

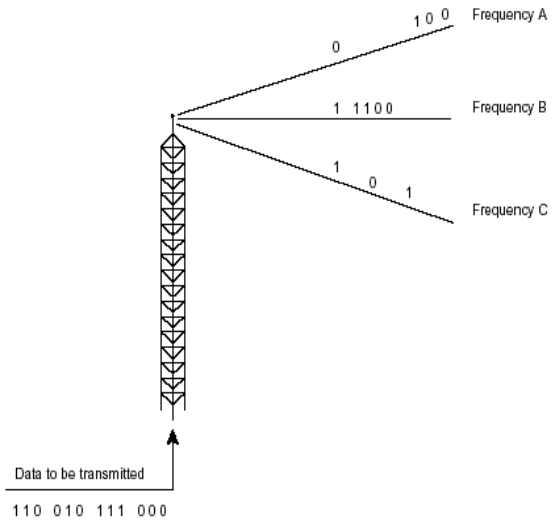
- Wireless?
- Các kỹ thuật
  - Radio
  - Microwave
  - Infrared
  - Lightwave



# Radio

- Đặc điểm
  - Tần số
  - Thiết bị: antenna, transceiver
- Phân loại
  - Single-Frequency
    - Low power
    - High power
  - Spread-Spectrum
    - Direct-sequence modulation
    - Frequency-hopping



# Microwave (sóng cực ngắn)

- Đặc điểm
- Phân loại
  - Terrestrial Microwave
  - Satellite Microwave
- Thông số

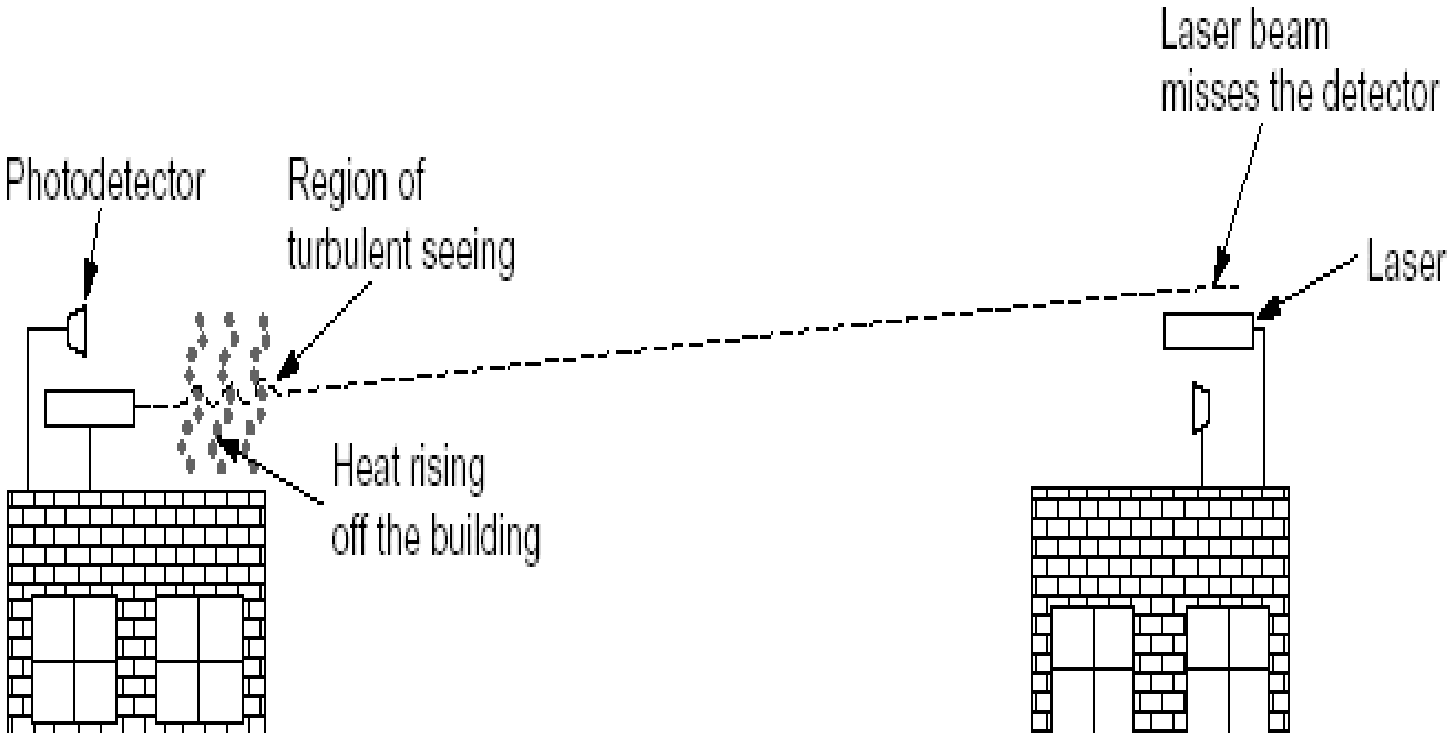
| | Terrestrial Microwave | Satellite Microwave |
|---|---|---|
| Tần số | 4-6 GHz, 21-23 GHz | 11-14 GHz |
| Khoảng cách tối đa | Phụ thuộc công suất và tần số phát (có thể vài chục km) | Toàn cầu |
| Tốc độ truyền | 1 – 10 Mbps | 1 – 10 Mbps |
| Lắp đặt / bảo trì | Khá khó | Khó |
| Nhiễu | Phụ thuộc thiết bị, thời tiết ... | Phụ thuộc thiết bị, thời tiết ... |
| Giá | Khá cao | Rất cao |
| Bảo mật | Thấp (thường được mã hoá) | Thấp (thường được mã hoá) |

# Infrared (Sóng hồng ngoại)

- Đặc điểm
- Phân loại
  - Point-to-point Infrared
  - Broadcast Infrared
- Thông số

| | Point-to-point Infrared | Broadcast Microwave |
|---|---|---|
| Tần số | 100-1000 GHz | 100 GHz - 1000 THz |
| Khoảng cách tối đa | Có thể vài km | Vài chục mét |
| Tốc độ truyền | 100 Kbps – 16 Mbps | Nhỏ hơn 1 Mbps |
| Lắp đặt / bảo trì | Vừa phải | Dễ |
| Nhiễu | Chống nhiễu điện, bị nhiễu ánh sáng | Chống nhiễu điện, bị nhiễu ánh sáng |
| Giá | Tuỳ thuộc thiết bị | Không cao |
| Bảo mật | Cao (do line-of-sight và độ dải sáng hẹp) | Thấp |

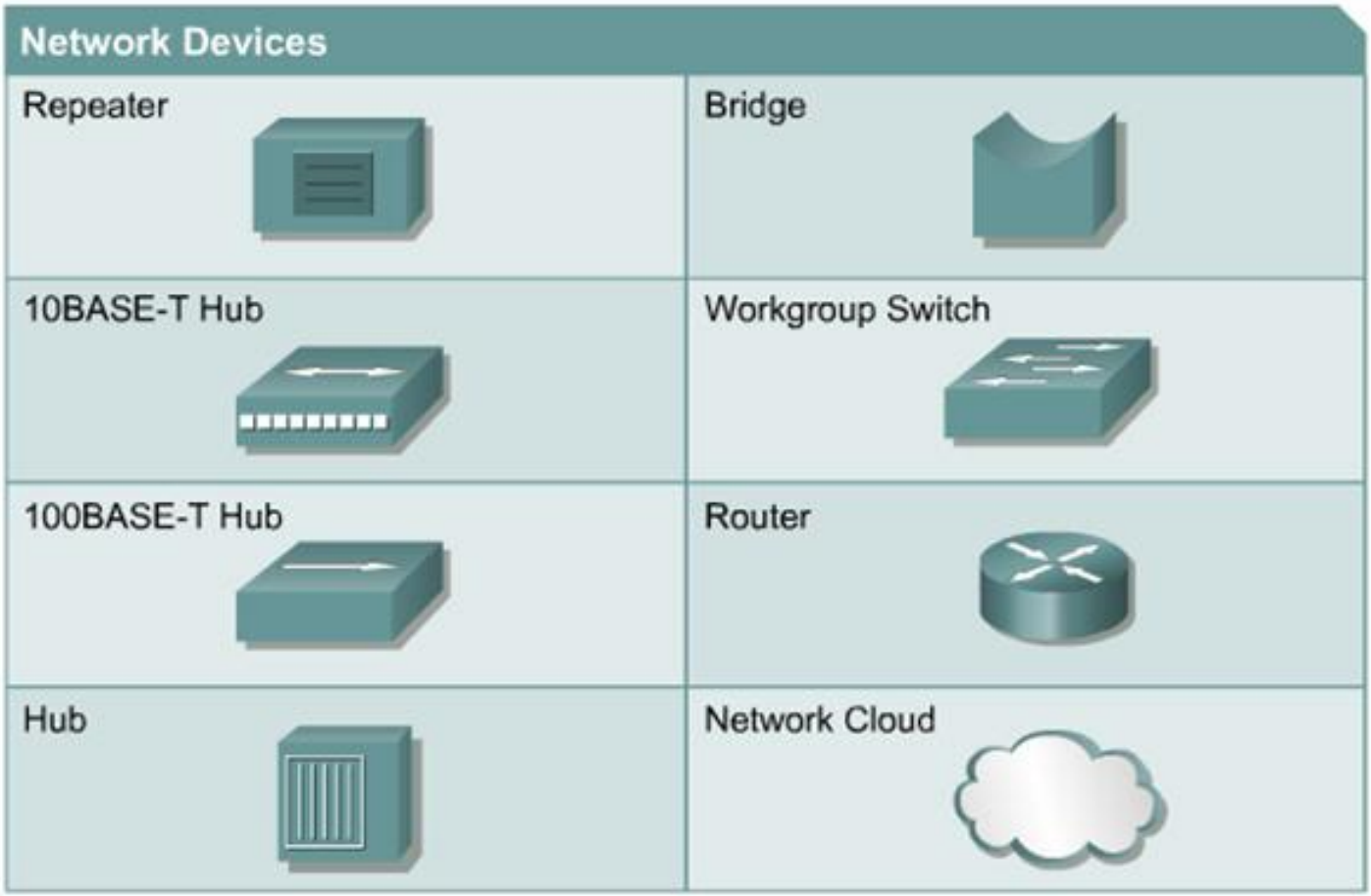
# Lightwave


Laser beam
misses the detector
Photodetector
Region of
turbulent seeing
Laser
Heat rising
off the building

# Các thiết bị liên kết mạng

- Card mạng (Network Interface Card - NIC)
- Modem
- Repeater (Bộ chuyển tiếp)
- Hub (Bộ tập trung)
- Bridge (Cầu nối)
- Switch (Bộ chuyển mạch)
- Router (Bộ định tuyến)
- Gateway (Cổng nối)

# Biểu diễn của các thiết bị mạng trong sơ đồ mạng



# Card mạng

- Kết nối giữa máy tính và cáp mạng để phát hoặc nhận dữ liệu với các máy tính khác thông qua mạng.
- Kiểm soát luồng dữ liệu giữa máy tính và hệ thống cáp.
- Mỗi NIC (Network Interface Adapter Card) có một mã duy nhất gọi là địa chỉ MAC (Media Access Control). MAC address có 6 byte, 3 byte đầu là mã số nhà sản xuất, 3 byte sau là số serial của card.

# Car

| Organizational Unique Identifier (OUI) | Vendor Assigned (NIC Cards, Interfaces) |
|---|---|
| 24 bits | 24 bits |
| 6 hex digits | 6 hex digits |
| 00 60 2F | 3A 07 BC |
| Cisco | particular device |

Internal network interface card

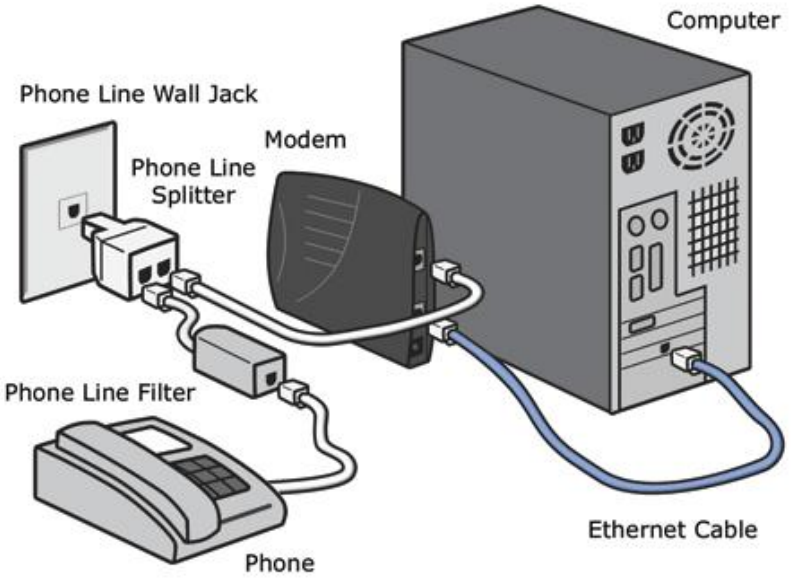
PCMCIA Network interface card

# Modem

- Là tên viết tắt của hai từ điều chế (MOdulation) và giải điều chế (DEModulation).
- Điều chế tín hiệu số (Digital) sang tín hiệu tương tự (Analog) để gởi theo đường điện thoại và ngược lại.
- Có 2 loại là Internal và External.

# Modem

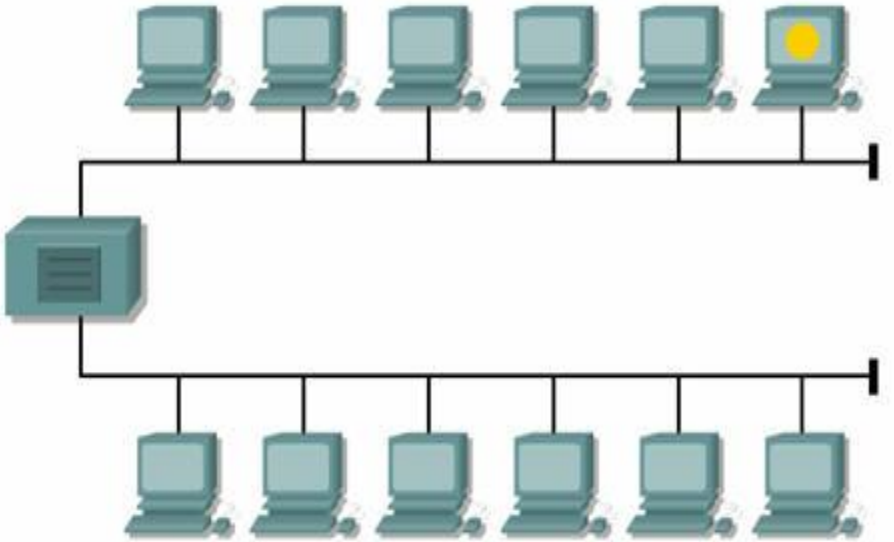
EDIMAX
ADSL ROUTER


Computer
Phone Line Wall Jack
Modem
Phone Line
Splitter
Phone Line Filter
Phone
Ethernet Cable

# Repeater (bộ chuyển tiếp)

- Khuếch đại, phục hồi các tín hiệu đã bị suy thoái do tổn thất năng lượng trong khi truyền.
- Cho phép mở rộng mạng vượt xa chiều dài giới hạn của một môi trường truyền.
- Chỉ được dùng nối hai mạng có cùng giao thức truyền thông.
- Hoạt động ở lớp Physical.

# Repeater (bộ chuyển tiếp)



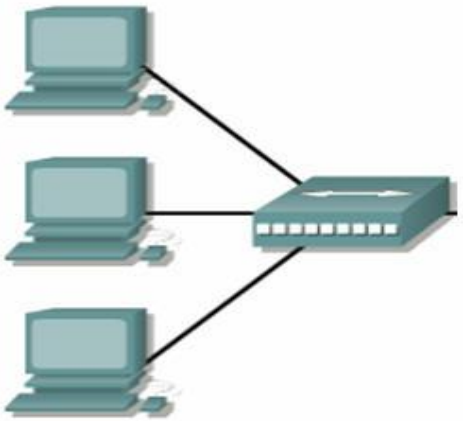
# Hub (bộ tập trung)

- Chức năng như Repeater nhưng mở rộng hơn với nhiều đầu cắm các đầu cáp mạng.
- Tạo ra điểm kết nối tập trung để nối mạng theo kiểu hình sao.
- Tín hiệu được phân phối đến tất cả các kết nối.
- Có 3 loại Hub: thụ động, chủ động, thông minh.

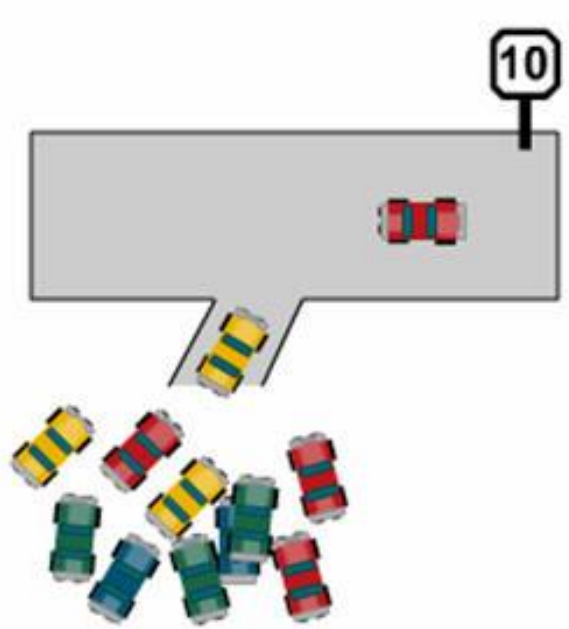
# Hub (bộ tập trung)

- Hub thụ động (Passive Hub): chỉ đảm bảo chức năng kết nối, không xử lý lại tín hiệu.
- Hub chủ động (Active Hub): có khả năng khuếch đại tín hiệu để chống suy hao.
- Hub thông minh (Intelligent Hub): là Hub chủ động nhưng có thêm khả năng tạo ra các gói tin thông báo hoạt động của mình giúp cho việc quản trị mạng dễ dàng hơn.

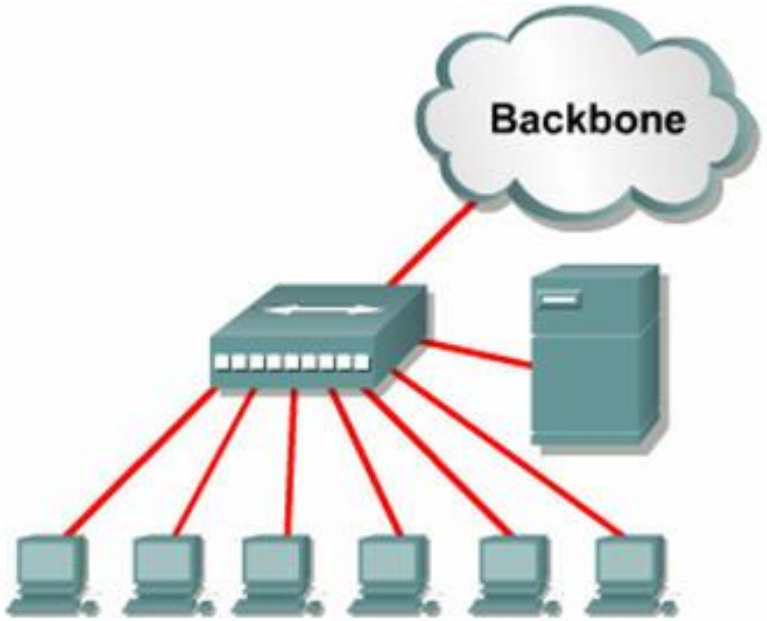
HUB



# Hub (bộ tập trung)




One device sending at a time

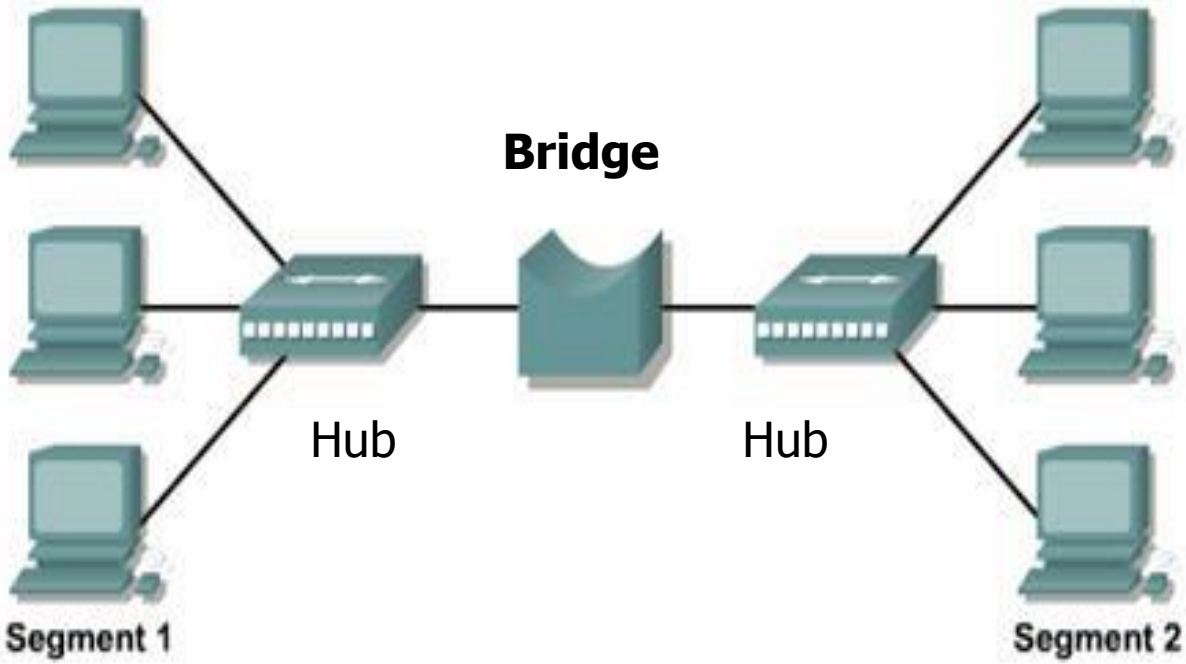



Each node shares 10 Mbps

# Bridge (cầu nối)

- Dùng để nối 2 mạng có giao thức giống hoặc khác nhau.
- Chia mạng thành nhiều phân đoạn nhằm giảm lưu lượng trên mạng.
- Hoạt động ở lớp Data Link với 2 chức năng chính là lọc và chuyển vận.
- Dựa trên bảng địa chỉ MAC lưu trữ, Brigde kiểm tra các gói tin và xử lý chúng trước khi có quyết định chuyển đi hay không.

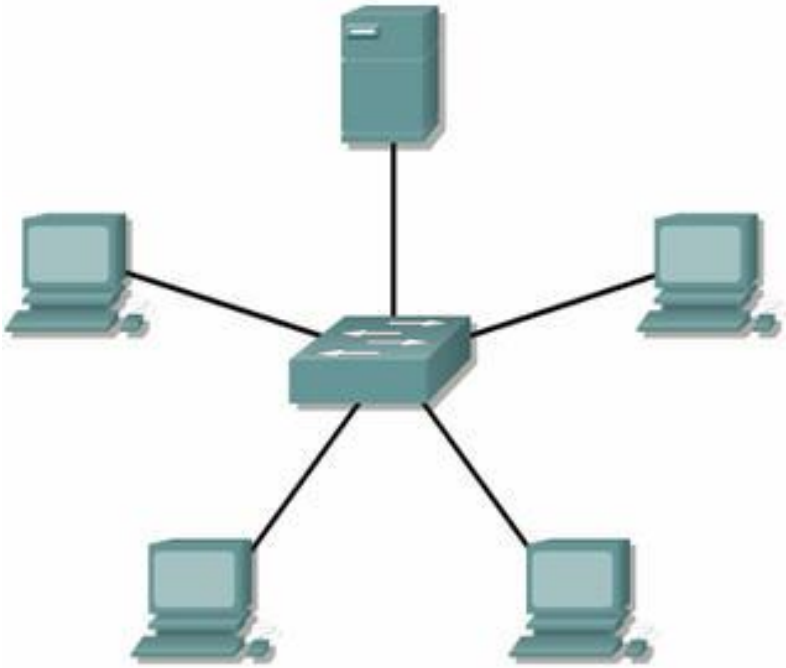
# Bridge (cầu nối)



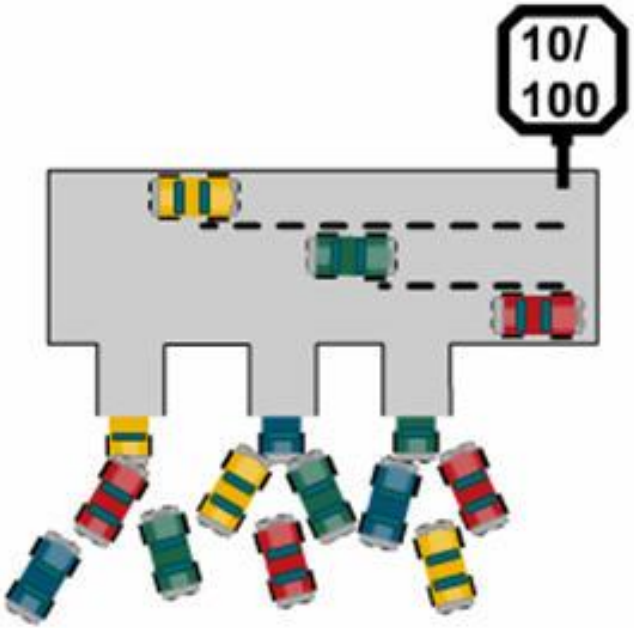
# Switch (bộ chuyển mạch)

- Là thiết bị giống Bridge và Hub cộng lại nhưng thông minh hơn.
- Có khả năng chỉ chuyển dữ liệu đến đúng kết nối thực sự cần dữ liệu này làm giảm đụng độ trên mạng.
- Dùng để phân đoạn mạng trong các mạng cục bộ lớn (VLAN).
- Hoạt động ở lớp Data Link.

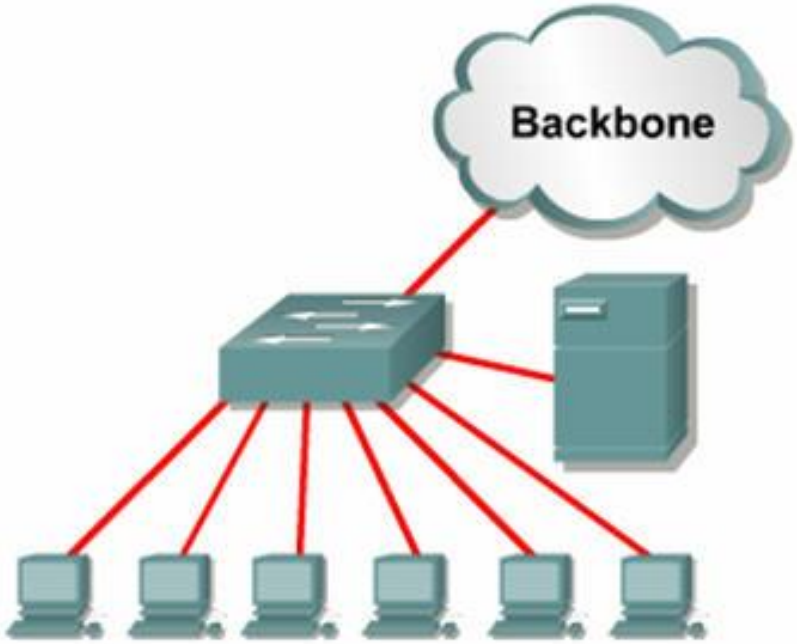
# Switch (bộ chuyển mạch)



# Switch (bộ chuyển mạch)




Multiple devices sending at the same time

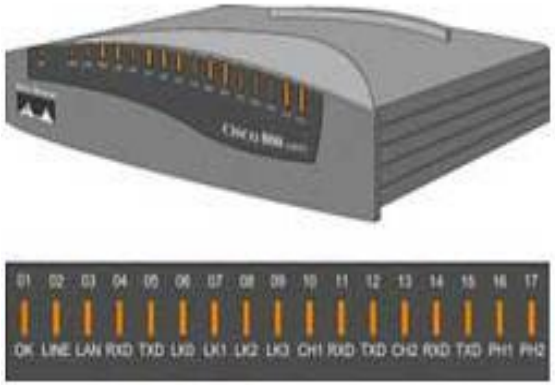


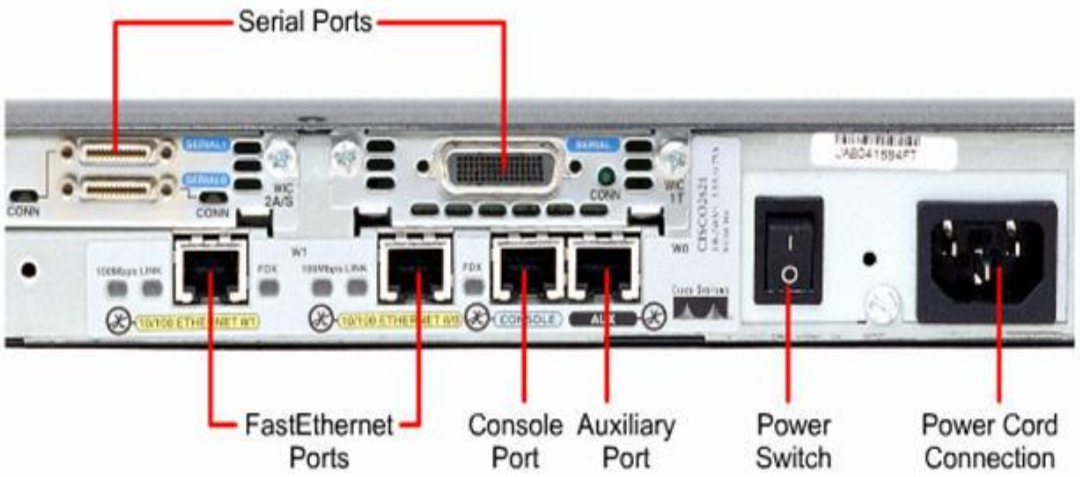

Each node has 10/100 Mbps

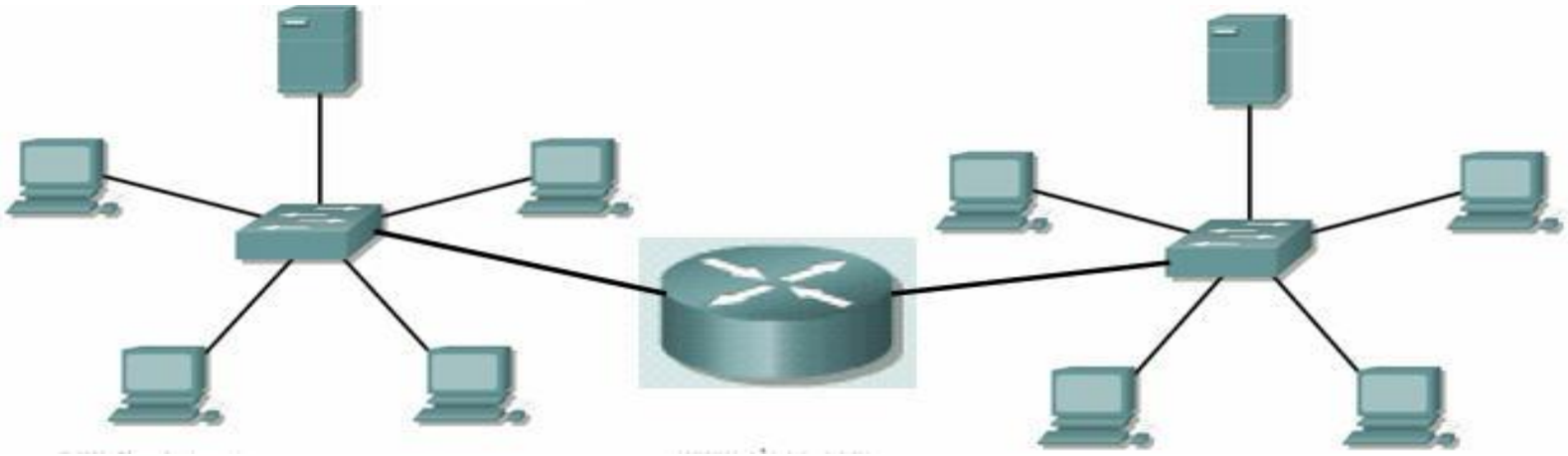
# Router (Bộ định tuyến)

- Dùng để ghép nối các mạng cục bộ lại với nhau thành mạng rộng.
- Lựa chọn đường đi tốt nhất cho các gói tin hướng ra mạng bên ngoài.
- Hoạt động chủ yếu ở lớp Network.
- Có 2 phương thức định tuyến chính:
  - Định tuyến tĩnh: cấu hình các đường cố định và cài đặt các đường đi này vào bảng định tuyến.
  - Định tuyến động:
    - Vectơ khoảng cách: RIP, IGRP, EIGRP, BGP
    - Trạng thái đường liên kết: OSPF

# Router (Bộ định tuyến)





# Gateway (Proxy - cổng nối)

- Thường dùng để kết nối các mạng không thuần nhất, chủ yếu là mạng LAN với mạng lớn bên ngoài chứ không dùng kết nối LAN – LAN.
- Kiểm soát luồng dữ liệu ra vào mạng.
- Hoạt động phức tạp và chậm hơn Router.
- Hoạt động từ tầng thứ 4→7

# CHƯƠNG 4: DATA LINK

- Điều khiển luồng (dòng)
- Phát hiện lỗi
- Xử lý lỗi

# Điều khiển luồng

- Là kỹ thuật nhằm đảm bảo rằng bên phát không làm tràn dữ liệu bên nhận
- Hai phương pháp được sử dụng:
  - Phương pháp dừng và chờ (Stop and Wait)
    - Đơn giản nhất,
    - Kém hiệu quả, chỉ có một khung tin được truyền tại một thời điểm
  - Phương pháp cửa sổ trượt –(Sliding Window Flow Control)
    - Hiệu quả
    - Cho phép truyền nhiều khung tin cùng một lúc trên kênh truyền

# Phương pháp dừng và chờ

- Truyền một gói tin và chờ báo nhận
  - Bên phát truyền một khung tin
  - Sau khi nhận được khung tin, bên nhận gửi lại xác nhận
  - Bên phát phải đợi đến khi nhận được xác nhận thì mới truyền khung tin tiếp theo
- Không hiệu quả
  - Bên nhận có thể dừng quá trình truyền bằng cách không gửi khung tin xác nhận
  - Tại một thời điểm chỉ có một khung tin trên đường truyền → chậm
  - Trường hợp độ rộng của kênh truyền lớn hơn độ rộng của khung tin thì nó tỏ ra cực kỳ kém hiệu quả.

# Phương pháp cửa sổ trượt

- Cho phép nhiều khung tin được truyền tại một thời điểm ->Truyền thông hiệu quả hơn.
- A và B được kết nối trực tiếp song công (full-duplex).
- B có bộ đệm cho n khung tin -> B có thể chấp nhận n khung tin, A có thể truyền n khung tin mà không cần đợi xác nhận từ bên B
- Mỗi khung tin được gán nhãn bởi một số thứ tự.
- B xác nhận khung tin đã được nhận bằng cách gửi xác nhận cùng với số thứ tự của khung tin tiếp theo mà nó mong muốn nhận

# Phương pháp cửa sổ trượt

- A duy trì danh sách các số thứ tự được phép gửi
- B duy trì danh sách số thứ tự chuẩn bị nhận

  - Gọi là cửa sổ của các khung tin

  - Điều khiển dòng cửa sổ trượt

# Phương pháp cửa sổ trượt

- Đối với đường truyền 2 chiều thì mỗi bên phải sử dụng hai cửa sổ:
  - Một cho phát và một cho nhận
  - Mỗi bên đều phải gửi dữ liệu và gửi xác nhận tới bên kia
- Số thứ tự được lưu trữ trong khung tin
  - Bị giới hạn, trường k bit thì số thứ tự được đánh số theo Module của $2^k$
  - Kích thước của cửa sổ không nhất thiết phải lấy là maximum ( ví dụ trường 3 bit, có thể lấy độ dài cửa sổ là 4)

# Phát hiện lỗi

- Lý do một hay nhiều bit thay đổi trong khung tin được truyền:
  - Tín hiệu trên đường truyền bị suy yếu
  - Tốc độ truyền
  - Mất đồng bộ
- Việc phát hiện ra lỗi để khắc phục, yêu cầu phát lại là cần thiết và vô cùng quan trọng trong truyền dữ liệu.

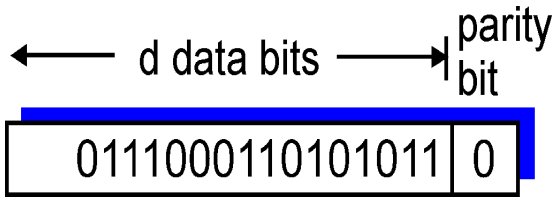
# Phát hiện lỗi: Parity Check

- Là kỹ thuật đơn giản nhất.
- Đưa một bit kiểm tra tính chẵn lẻ vào sau khối tin.
- Giá trị của bit này được xác định dựa trên số các số 1 là chẵn (even parity), hoặc số các số 1 là lẻ (odd parity).
- Lỗi sẽ không bị phát hiện nếu trong khung tin có 2 hoặc một số chẵn các bit bị đảo.
- Không hiệu quả khi xung nhiễu đủ mạnh.

# Kiểm tra Parity

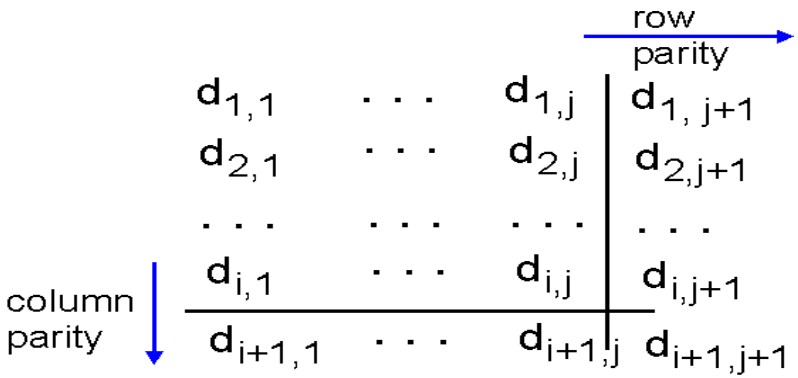
## Bit Parity đơn:

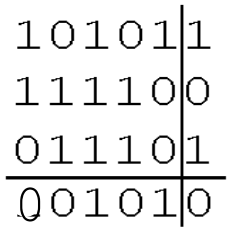
**phát hiện các lỗi bit**



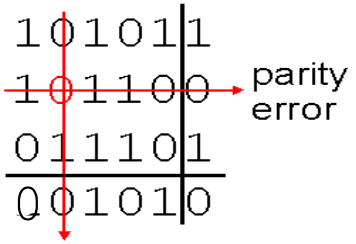

## Bit Parity 2 chiều:

**phát hiện & sửa các lỗi bit**




*no errors*




*correctable single bit error*

# Phát hiện lỗi: Cyclic redundancy Check (CRC)

Mô tả:

- Khối dữ liệu k bit
- Mẫu n+1 bit (n<k)
- Tạo ra dãy n bit gọi là dãy kiểm tra khung tin-FCS, Frame Check Sequence
- Tao ra một khung tin k+n bit
- Bên nhận khi nhận được khung tin sẽ chia cho mẫu, nếu kết quả là chia hết, việc truyền khung tin này là không có lỗi

# Phát hiện lỗi:
# CRC dưới dạng module của 2

M: Khối tin k bit

F: FCS n bit, n bit cuối của T

T: khung tin k+n bit

P: Mẫu n+1 bit, đây là một số chia được chọn trước.

Mục tiêu: xác định F để T chia hết cho P

$$T = 2^n M + F$$

# Phát hiện lỗi: Các bước tạo và kiểm tra CRC

- Các bước tạo CRC
  - Dịch trái M đi n bit
  - Chia kết quả cho P
  - Số dư tìm được là F
- Các bước kiểm tra CRC
  - Lấy khung nhận được (n+k) bit
  - Chia cho P
  - Kiểm tra số dư, nếu số dư khác 0, khung bị lỗi, ngược lại là không lỗi

# Phát hiện lỗi:
# CRC- Dạng đa thức nhị phân

Cách thứ 2 để biểu thị CRC là biểu diễn các giá trị như là một đa thức với các hệ số là số nhị phân, đây là các bit của số nhị phân. Gọi T(X), M(X), Q(X), P(X), R(X) là các đa thức tương ứng với các số nhị phân T, M, Q, P, R đã trình bày ở trên, khi đó CRC được biểu thị:

$$\frac{X^n M(X)}{P(X)} = Q(X) + \frac{R(X)}{P(X)}$$

$$T(X) = X^n M(X) + R(X)$$

# CRC- Dạng đa thức nhị phân

Một số đa thức P(X) tiêu biểu:

CRC-12: $X^{12}+X^{11}+X^3+X^2+X+1$ CRC-16: $X^{16}+X^{15}+X^2+1$

CRC-CCITT: $X^{16}+X^{12}+X^5+1$

CRC32: $X^{32}+X^{26}+X^{23}+X^{22}+X^{16}+X^{12}+X^{11}+X^{10}+X^8+X^7+X^5+X^4+X^2+X+1$

**Ví dụ:**

**Tạo CRC:**

1. Cho tin M=1010001101 (10 bit)

Mẫu P:110101 (6 bit)

FCS R: được tính theo phương pháp CRC v
sẽ có độ dài là 5 bit

2. Nhân M với $2^5$ ta được:

$M2^5$=101000110100000

3. Chia kết quả cho P:

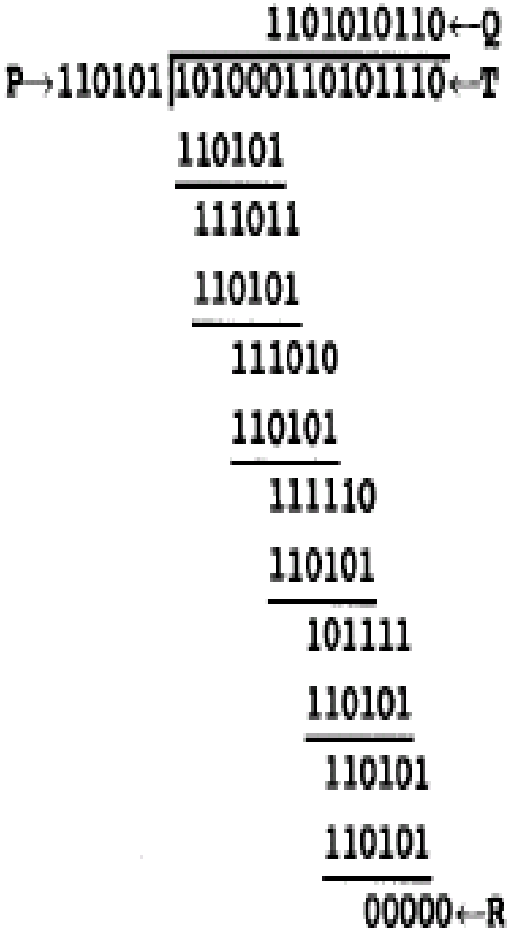
4. Số dư là: 01110, được đưa vào sau tin M

Ta có tin T, được truyền đi là:
101000110101110

```
                1101010110←Q
P→110101 |101000110100000←2^5M
         110101
          111011
          110101
            111010
            110101
              111110
              110101
                101100
                110101
                 110010
                 110101
                   01110←R
```

# CRC- Dạng đa thức nhị phân

- Kiểm tra CRC:
- Giả sử bên thu nhận được T, khi đó để kiểm tra là phép truyền có lỗi không ta chia T cho P, số dư là 00000, vậy ta kết luận phép truyền tin M, không có lỗi.



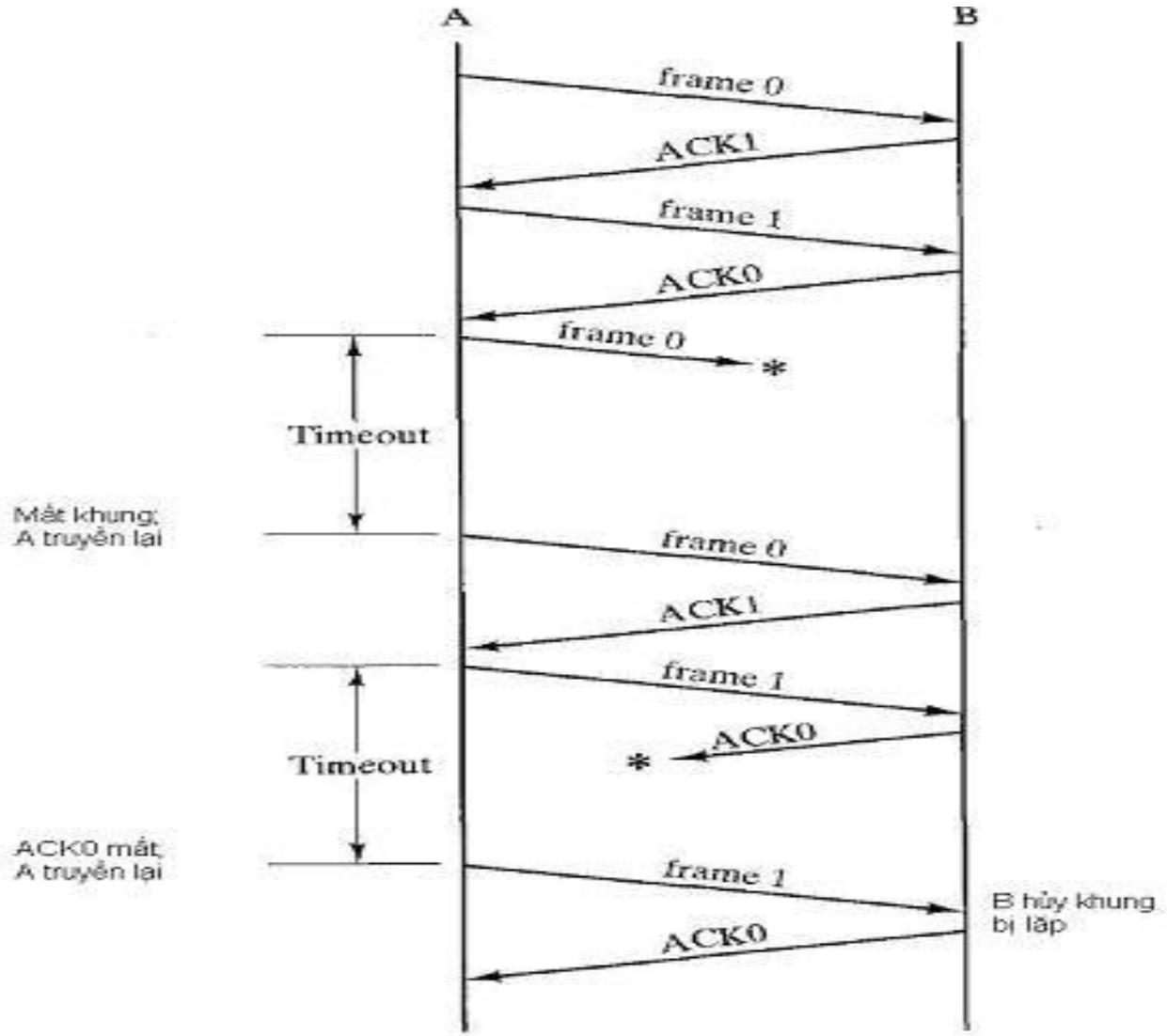
# Xử lý lỗi

- Lỗi: Mất khung, hỏng khung
- Kiểm soát lỗi:
  - Phát hiện lỗi
  - Báo nhận: khung tin tốt
  - Truyền lại khi hết thời gian định trước
  - Báo nhận: khung tin lỗi và truyền lại

# Xử lý lỗi: ARQ dừng và chờ

- Trên cơ sở kĩ thuật điều khiển luồng dừng-và-chờ
- Kiểm soát lỗi:
  - Khung tin tới bên nhận bị hỏng: Truyền lại, sử dụng đồng hồ đếm giờ time-out
  - Báo nhận bị hỏng: Time-out, bên phát gửi lại, sử dụng label 0/1 và ACK0/ACK1 phát hiện lỗi

# Xử lý lỗi: ARQ dừng và chờ



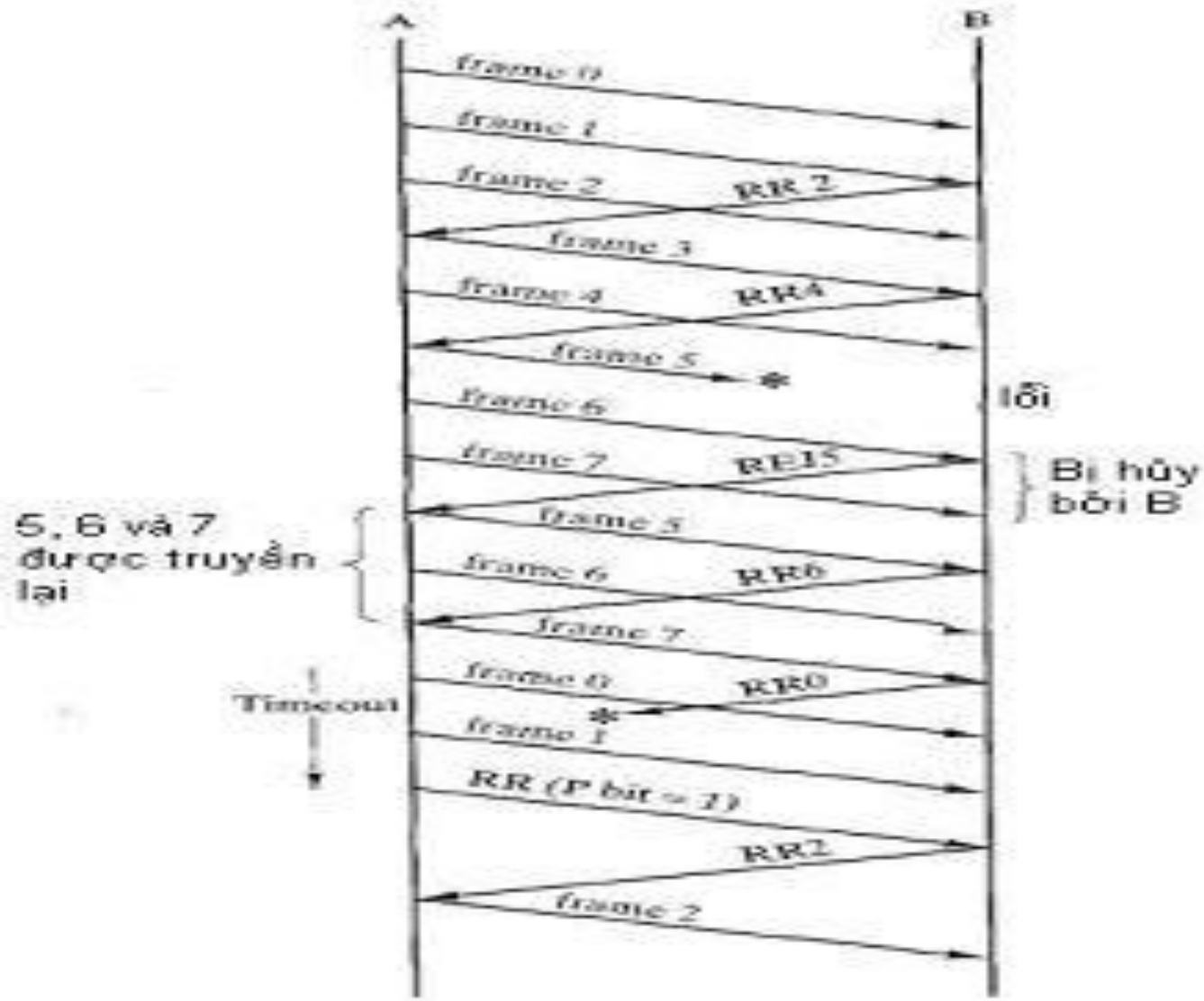
# Xử lý lỗi: ARQ Quay-lui-N

- Trên cơ sở kĩ thuật điều khiển luồng bằng Cửa sổ trượt
- Kiểm soát lỗi:
  - Khung hỏng:
    - Khung i-1 thành công, i lỗi, bên nhận gửi SREJ i, bên phát gửi lại
    - Khung i mất, i+1 được nhận không đúng trình tự, REJ i, bên gửi phát lại i và các khung sau đó
    - Chỉ khung i được truyền và bị mất, bên nhận không biết i đã được truyền đi, bên phát gửi time-out và gửi RR với P=1, khi bên phát nhận được RR từ bên nhận nó sẽ phát lại i

# Xử lý lỗi: ARQ Quay-lui-N

- RR hỏng:
  - B nhận khung i và gửi RR(i+1), RR(i+1) mất, A có thể nhận RR(>i+1) trước khi RR(i+1) time-out, và có nghĩa là khung i đã thành công.
  - RR(i+1) time-out, A cố gắng gửi RR với P-bit cho đến khi nhận được RR từ B một số lần nhất định, nếu vẫn không nhận được thì Khởi động lại giao thức
- Reject hỏng:
  - A time-out, A gửi RR với P=1 cho đến khi nhận được RRi từ B thì A sẽ gửi lại khung i

# Xử lí lỗi: ARQ Quay-lui-N



# Xử lý lỗi: ARQ Chọn-Hủy (Selective-Reject)

- Chỉ truyền lại những khung có báo nhận là lỗi (SREJ)
- Phải duy trì đủ bộ đệm độ lớn
- Đảm bảo tính logic phức tạp để gửi và nhận các khung theo đúng trình tự.
- ARQ Chọn-Hủy phải giải quyết được sự chồng chéo giữa cửa sổ gửi và nhận.

# Xử lý lỗi: ARQ Chọn-Hủy (Selective-Reject)

- Trạm A gửi các khung từ 0 đến 6 tới trạm B.
- Trạm B nhận tất cả 7 khung và báo nhận tích lũy với RR 7
- Vì lí do nào đó ví dụ như nhiễu làm RR 7 bị mất trên đường truyền.
- Đồng hồ ở A hết hạn và A truyền lại khung 0.
- B đã điều chỉnh trước cửa sổ nhận để có thể nhận các khung 7, 0, 1, 2, 3, 4 và 5. Do đó mà khung 7 được coi là bị mất và khung nhận được này là khung số 0 mới, và được chấp nhận bởi B.

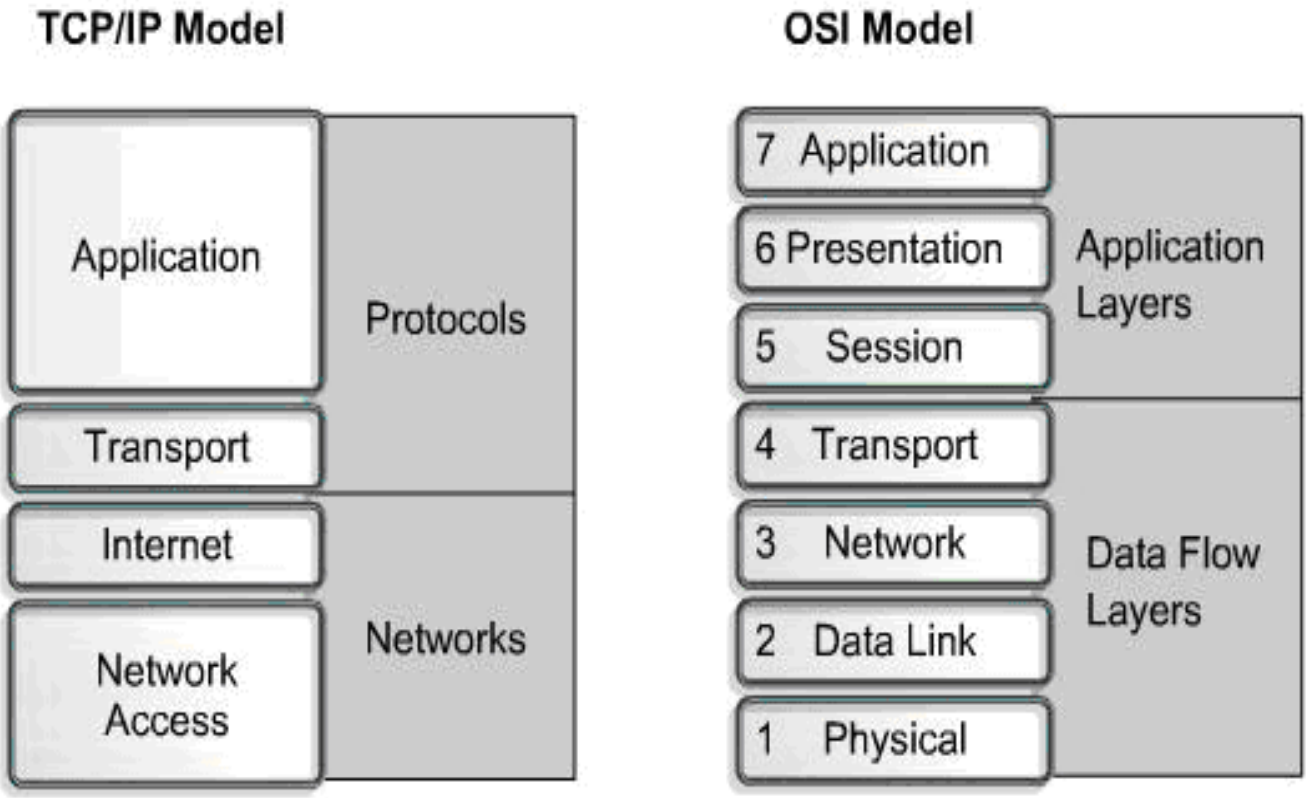
# CHƯƠNG 5: TCP/IP

- Khái niệm về TCP và IP
- Mô hình tham chiếu TCP/IP
- So sánh OSI và TCP/IP
- Các giao thức trong mô hình TCP/IP
- Chuyển đổi giữa các hệ thống số
- Địa chỉ IP và các lớp địa chỉ
- NAT
- Mạng con và kỹ thuật chia mạng con
- Bài tập

# Khái niệm về TCP và IP

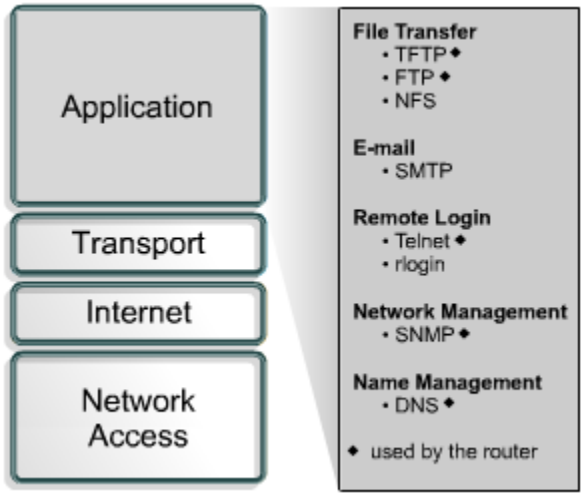
- TCP (Transmission Control Protocol) là giao thức thuộc tầng vận chuyển và là một giao thức có kết nối (connected-oriented).
- IP (Internet Protocol) là giao thức thuộc tầng mạng của mô hình OSI và là một giao thức không kết nối (connectionless).

# Mô hình tham chiếu TCP/IP



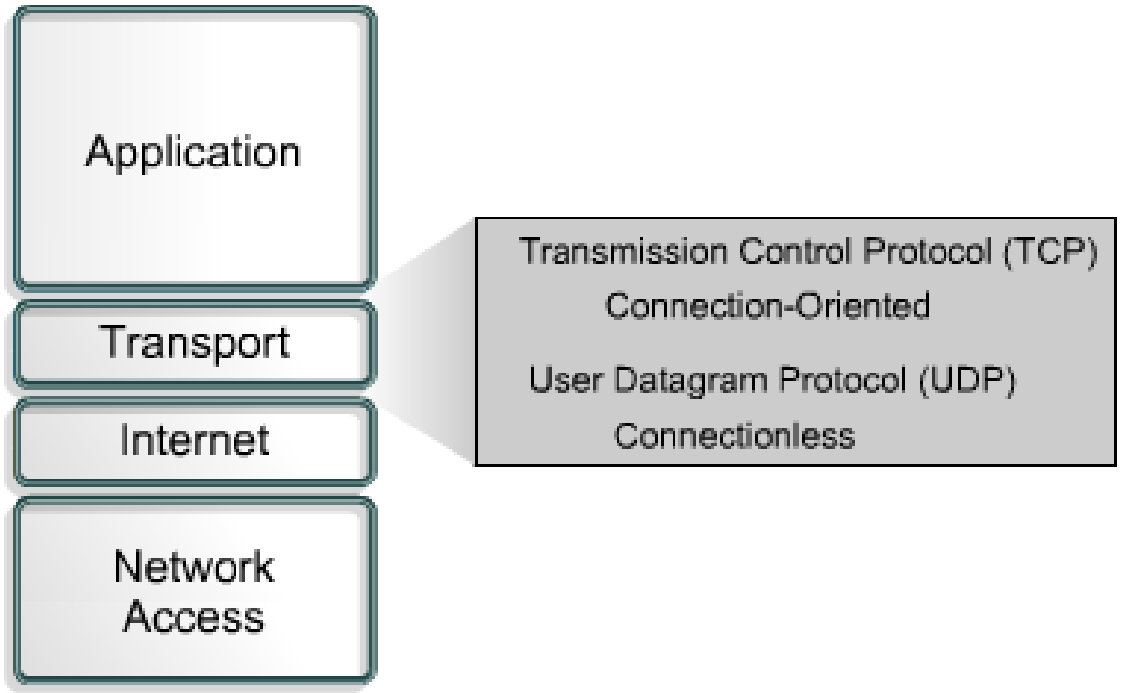
# Lớp ứng dụng

Kiểm soát các giao thức lớp cao, các chủ đề về trình bày, biểu diễn thông tin, mã hóa và điều khiển hội thoại. Đặc tả cho các ứng dụng phổ biến.



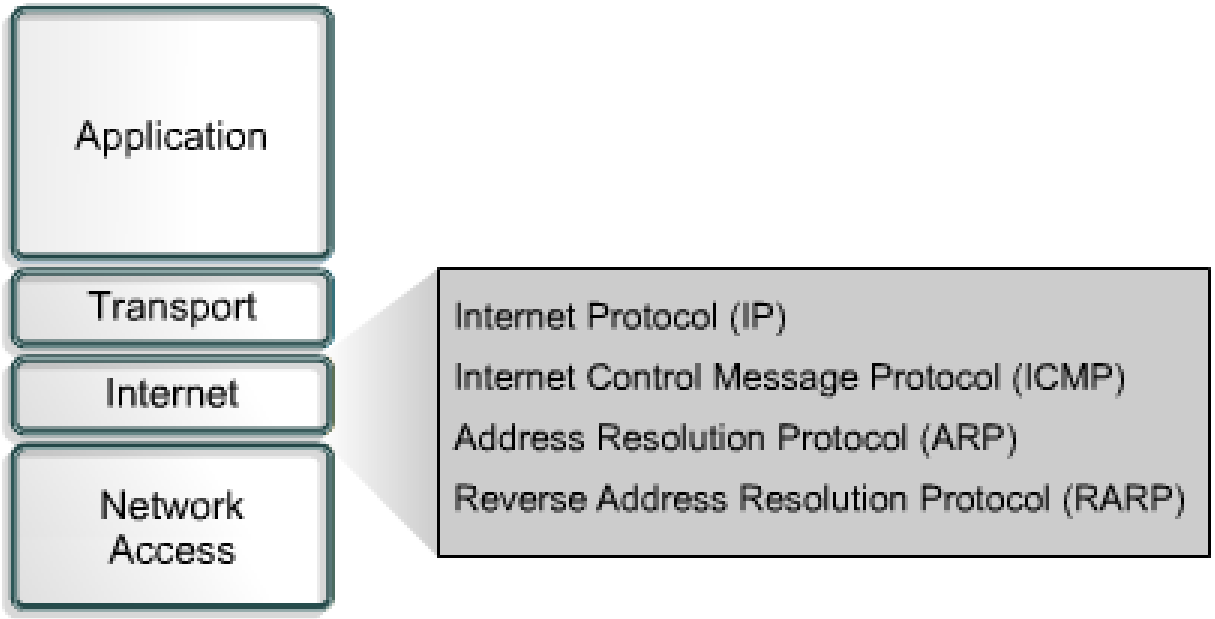
# Lớp vận chuyển

Cung ứng dịch vụ vận chuyển từ host nguồn đến host đích. Thiết lập một cầu nối luận lý giữa các đầu cuối của mạng, giữa host truyền và host nhận.



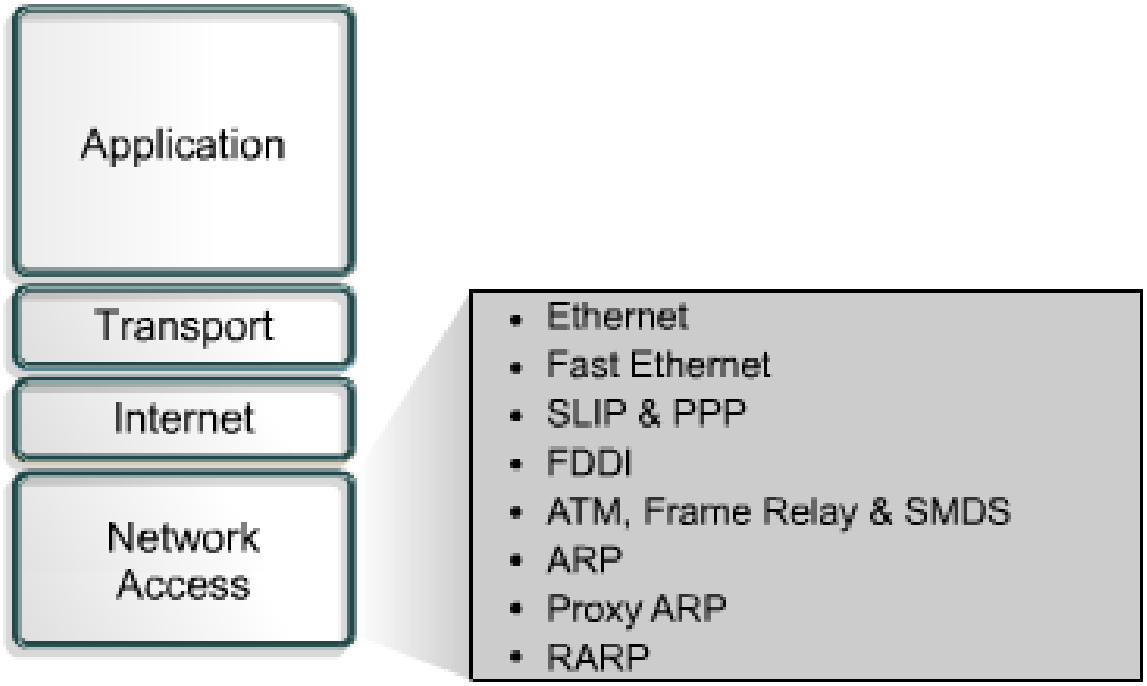
# Lớp Internet

Mục đích của lớp Internet là chọn đường đi tốt nhất xuyên qua mạng cho các gói dữ liệu di chuyển tới đích. Giao thức chính của lớp này là Internet Protocol (IP).



# Lớp truy nhập mạng

Định ra các thủ tục để giao tiếp với phần cứng mạng và truy nhập môi trường truyền. Có nhiều giao thức hoạt động tại lớp này

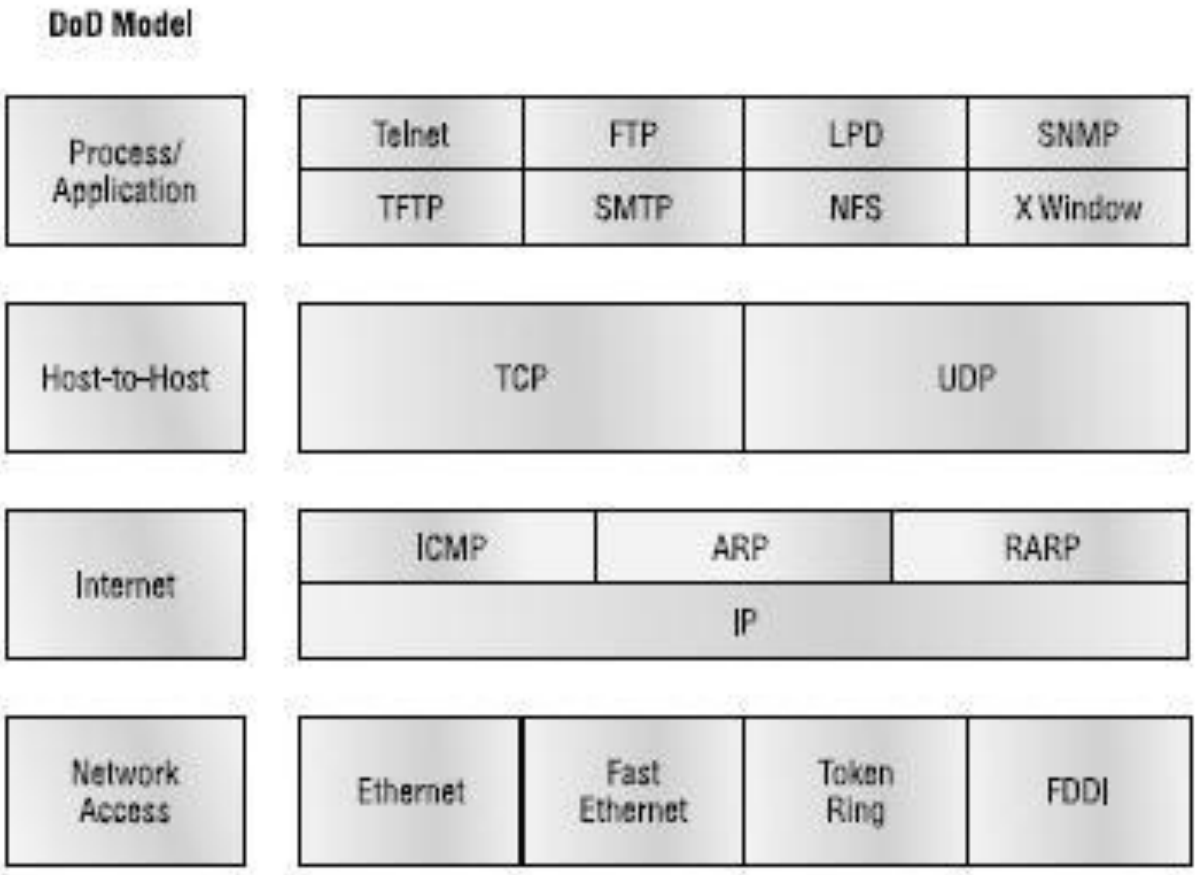


# So sánh mô hình OSI và TCP/IP

- Giống nhau
  - Đều phân lớp chức năng
  - Đều có lớp vận chuyển và lớp mạng.
  - Chuyển gói là hiển nhiên.
  - Đều có mối quan hệ trên dưới, ngang hàng.

- Khác nhau
  - TCP/IP gộp lớp trình bày và lớp phiên vào lớp ứng dụng.
  - TCP/IP gộp lớp vật lý và lớp liên kết dữ liệu vào lớp truy nhập mạng.
  - TCP/IP đơn giản vì có ít lớp hơn.
  - OSI không có khái niệm chuyển phát thiếu tin cậy ở lớp 4 như UDP của TCP/IP

# Các giao thức trong mô hình TCP/IP



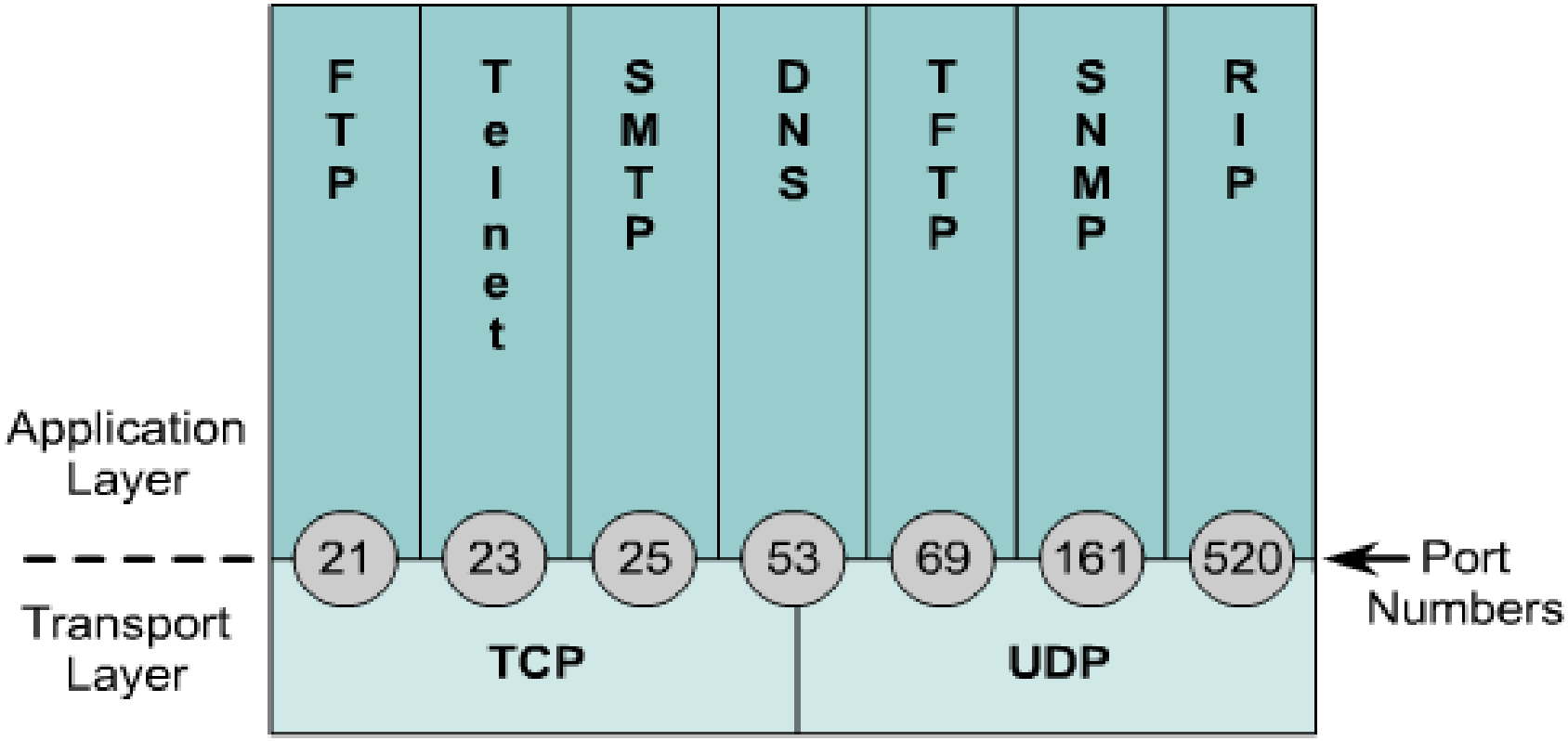
# Lớp ứng dụng

- FTP (File Transfer Protocol): là dịch vụ có tạo cầu nối, sử dụng TCP để truyền các tập tin giữa các hệ thống.
- TFTP (Trivial File Transfer Protocol): là dịch vụ không tạo cầu nối, sử dụng UDP. Được dùng trên router để truyền các file cấu hình và hệ điều hành.
- NFS (Network File System): cho phép truy xuất file đến các thiết bị lưu trữ ở xa như một đĩa cứng qua mạng.
- SMTP (Simple Mail Transfer Protocol): quản lý hoạt động truyền e-mail qua mạng máy tính.

# Lớp ứng dụng

- Telnet (Terminal emulation): cung cấp khả năng truy nhập từ xa vào máy tính khác. Telnet client là host cục bộ, telnet server là host ở xa.
- SNMP (Simple Network Management): cung cấp một phương pháp để giám sát và điều khiển các thiết bị mạng.
- DNS (Domain Name System): thông dịch tên của các miền (Domain) và các node mạng được công khai sang các địa chỉ IP.

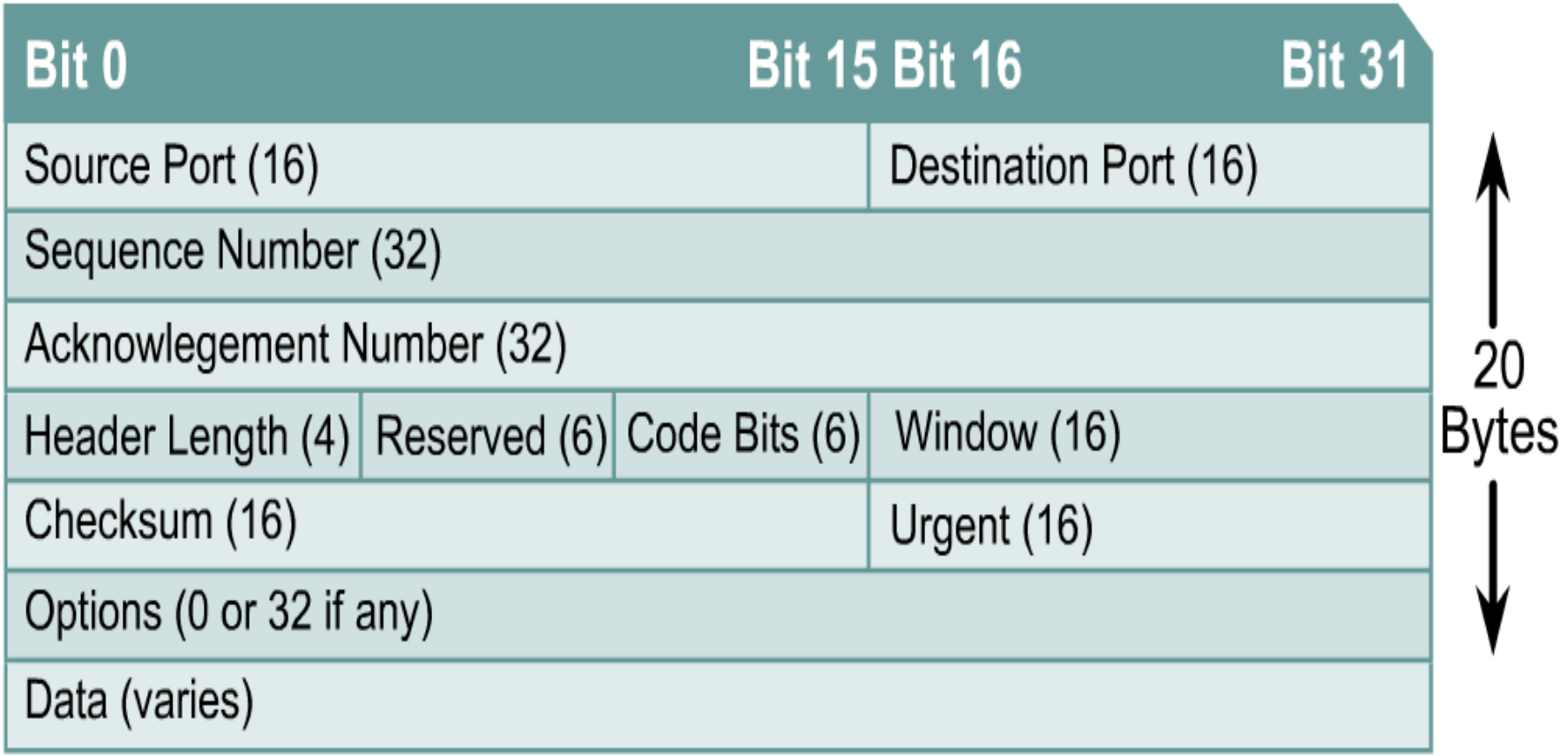
# Các cổng phổ biến dùng cho các giao thức lớp ứng dụng



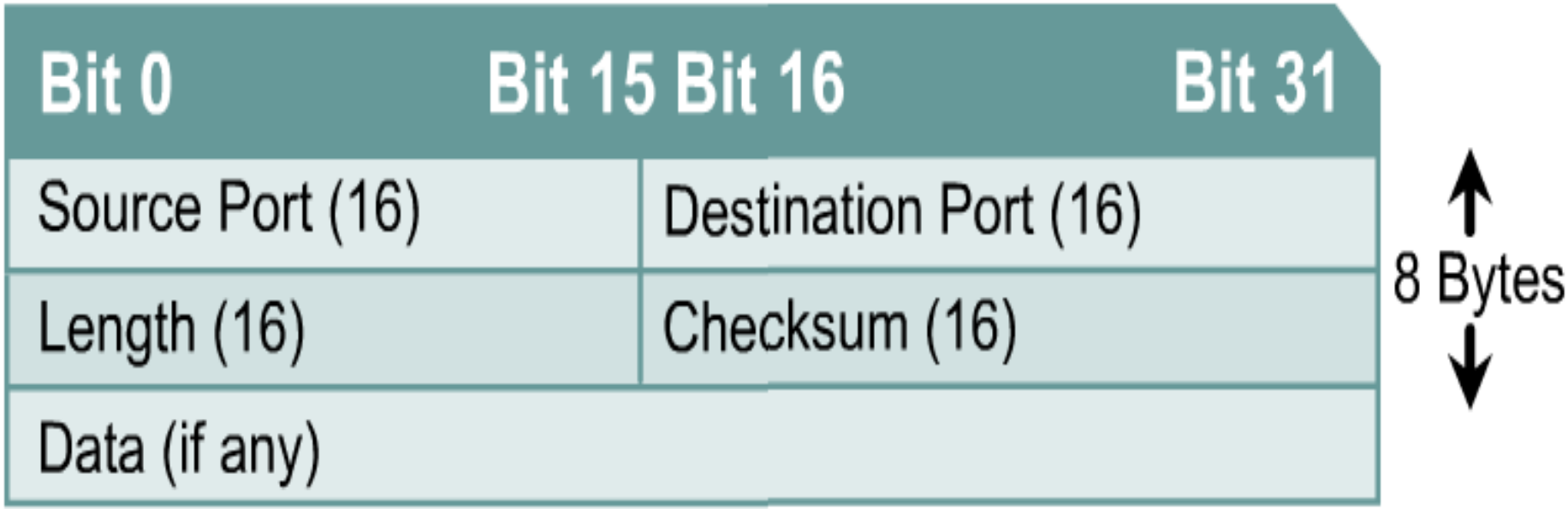
# Lớp vận chuyển

- TCP và UDP (User Datagram Protocol):
  - Phân đoạn dữ liệu ứng dụng lớp trên.
  - Truyền các segment từ một thiết bị đầu cuối này đến thiết bị đầu cuối khác
- Riêng TCP còn có thêm các chức năng:
  - Thiết lập các hoạt động end-to-end.
  - Cửa sổ trượt cung cấp điều khiển luồng.
  - Chỉ số tuần tự và báo nhận cung cấp độ tin cậy cho hoạt động.

# Khuôn dạng gói tin TCP



# Khuôn dạng gói tin UDP



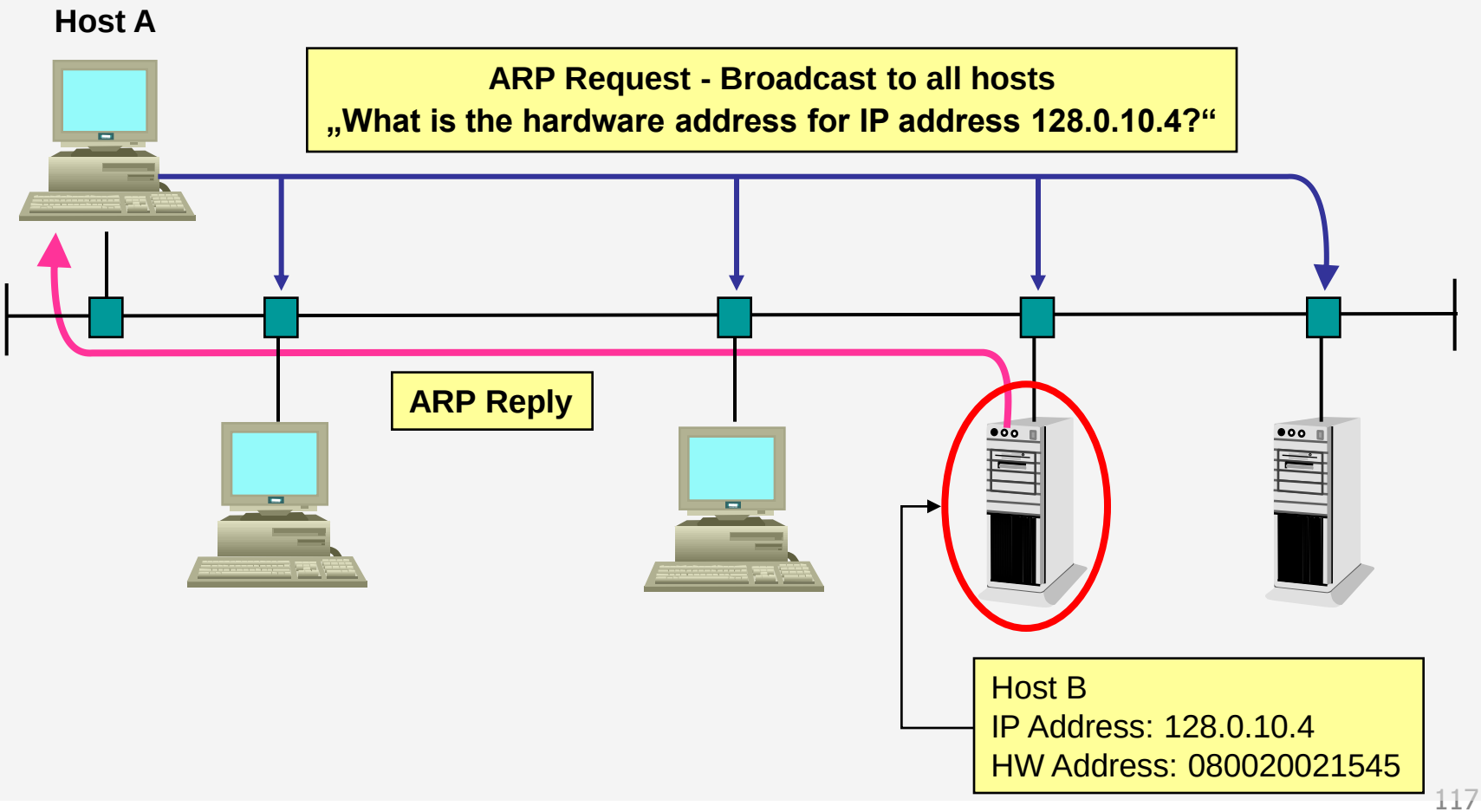
# Lớp Internet

- IP: không quan tâm đến nội dung của các gói nhưng tìm kiếm đường dẫn cho gói tới đích.
- ICMP (Internet Control Message Protocol): đem đến khả năng điều khiển và chuyển thông điệp.
- ARP (Address Resolution Protocol): xác định địa chỉ lớp liên kết số liệu (MAC address) khi đã biết trước địa chỉ IP.
- RARP (Reverse Address Resolution Protocol): xác định các địa chỉ IP khi biết trước địa chỉ MAC.

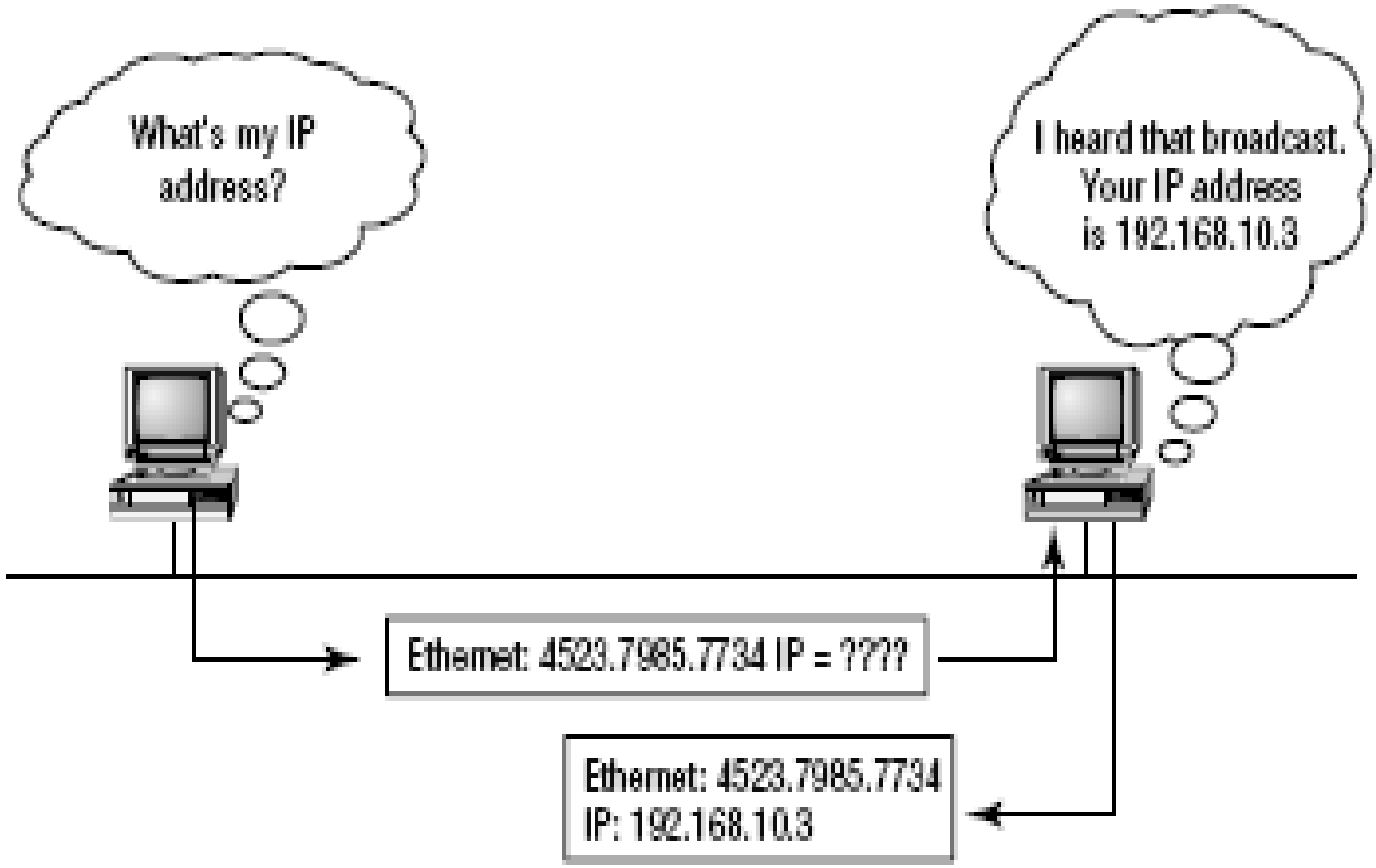
# Khuôn dạng gói tin IP

<table>
<tr><td>VER</td><td>IHL</td><td>Type of services</td><td colspan="2">Total lenght</td></tr>
<tr><td colspan="3">Identification</td><td>Flags</td><td>Fragment offset</td></tr>
<tr><td>Time to live</td><td>Protocol</td><td colspan="3">Header checksum</td></tr>
<tr><td colspan="5">Source address</td></tr>
<tr><td colspan="5">Destination address</td></tr>
<tr><td colspan="5">Options + Padding</td></tr>
<tr><td colspan="5">Data</td></tr>
</table>

# ARP


Host A
ARP Request - Broadcast to all hosts
„What is the hardware address for IP address 128.0.10.4?“
ARP Reply
Host B
IP Address: 128.0.10.4
HW Address: 080020021545

# RARP


What's my IP address?
I heard that broadcast. Your IP address is 192.168.10.3
Ethernet: 4523.7985.7734 IP = ????
Ethernet: 4523.7985.7734
IP: 192.168.10.3

# Lớp truy nhập mạng

- Ethernet
  - Là giao thức truy cập LAN phổ biến nhất.
  - Được hình thành bởi định nghĩa chuẩn 802.3 của IEEE (Institute of Electrical and Electronics Engineers).
  - Tốc độ truyền 10Mbps
- Fast Ethernet
- Gigabit Ethernet

# Chuyển đổi giữa các hệ thống số

- Hệ 2 (nhị phân): gồm 2 ký số 0, 1
- Hệ 8 (bát phân): gồm 8 ký số 0, 1, …, 7
- Hệ 10 (thập phân): gồm 10 ký số 0, 1, …, 9
- Hệ 16 (thập lục phân): gồm các ký số 0, 1, …, 9 và các chữ cái A, B, C, D, E, F

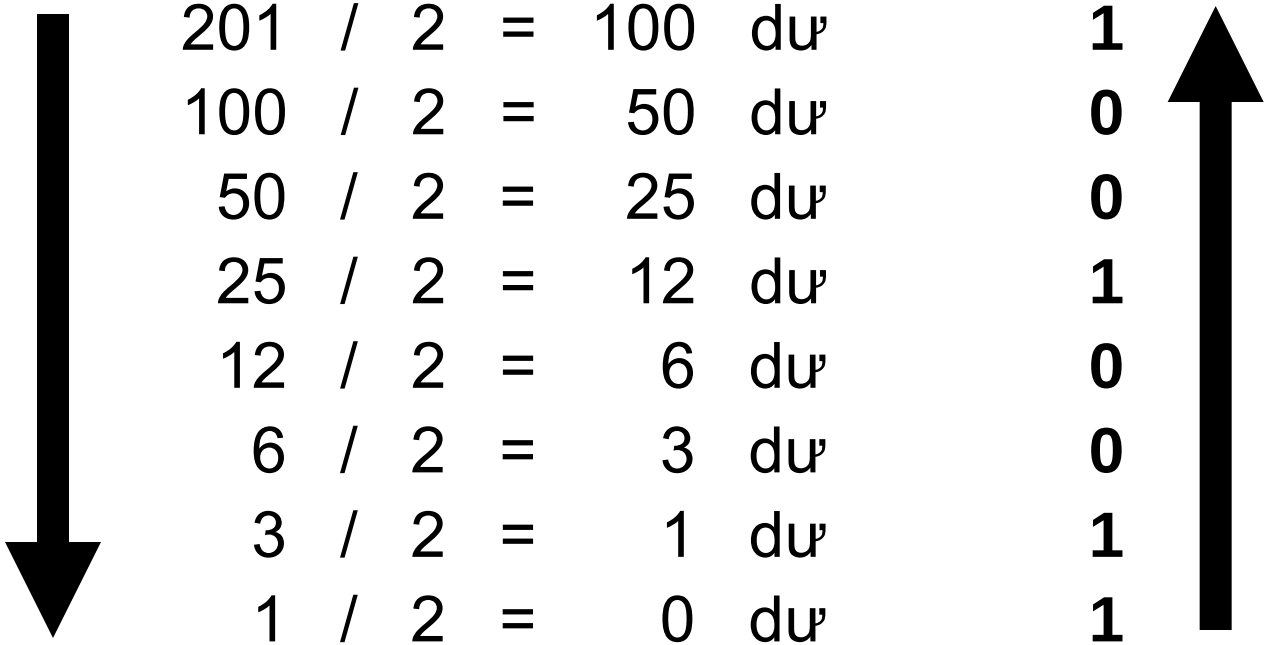
# Chuyển đổi giữa hệ nhị phân sang hệ thập phân

$$10110_2 = (1 \times 2^4) + (0 \times 2^3) + (1 \times 2^2) + (1 \times 2^1) + (0 \times 2^0) = 16 + 0 + 4 + 2 + 0 = 22$$

| | |
|---|---|
| Place Value | 128 64 32 16 8 4 2 1 |
| Base$^{Exponent}$ | $2^7 = 128$ $2^3 = 8$<br>$2^6 = 64$ $2^2 = 4$<br>$2^5 = 32$ $2^1 = 2$<br>$2^4 = 16$ $2^0 = 1$ |
| Number of Symbols | 2 |
| Symbols | 0, 1 |
| Rationale | Two-state (discrete binary) voltage systems made from transistors can be diverse, powerful, inexpensive, tiny and relatively immune to noise. |

# Chuyển đổi giữa hệ thập phân sang hệ nhị phân

**Đổi số $201_{10}$ sang nhị phân:**



| | | | | | | |
|---|---|---|---|---|---|---|
| 201 | / | 2 | = | 100 | dư | **1** |
| 100 | / | 2 | = | 50 | dư | **0** |
| 50 | / | 2 | = | 25 | dư | **0** |
| 25 | / | 2 | = | 12 | dư | **1** |
| 12 | / | 2 | = | 6 | dư | **0** |
| 6 | / | 2 | = | 3 | dư | **0** |
| 3 | / | 2 | = | 1 | dư | **1** |
| 1 | / | 2 | = | 0 | dư | **1** |

Khi thương số bằng 0, ghi các số dư theo thứ tự ngược với lúc xuất hiện, kết quả: **$201_{10} = 11001001_2$**

# Chuyển đổi giữa hệ nhị phân sang hệ bát phân và thập lục phân

- Nhị phân sang bát phân:
  - Gom nhóm số nhị phân thành từng nhóm 3 chữ số tính từ phải sang trái. Mỗi nhóm tương ứng với một chữ số ở hệ bát phân.
  - Ví dụ: $1'101'100_{(2)} = 154_{(8)}$
- Nhị phân sang thập lục phân:
  - Tương tự như nhị phân sang bát phân nhưng mỗi nhóm có 4 chữ số.
  - Ví dụ: $110'1100_{(2)} = 6C_{(16)}$

# Các phép toán làm việc trên bit

| A | B | A and B |
|---|---|---|
| 1 | 1 | 1 |
| 1 | 0 | 0 |
| 0 | 1 | 0 |
| 0 | 0 | 0 |

# Địa chỉ IP và các lớp địa chỉ

- Địa chỉ IP là địa chỉ có cấu trúc với một con số có kích thước 32 bit, chia thành 4 phần mỗi phần 8 bit gọi là octet hoặc byte.
- Ví dụ:
  - 172.16.30.56
  - 10101100 00010000 00011110 00111000.
  - AC 10 1E 38

# Địa chỉ IP và các lớp địa chỉ

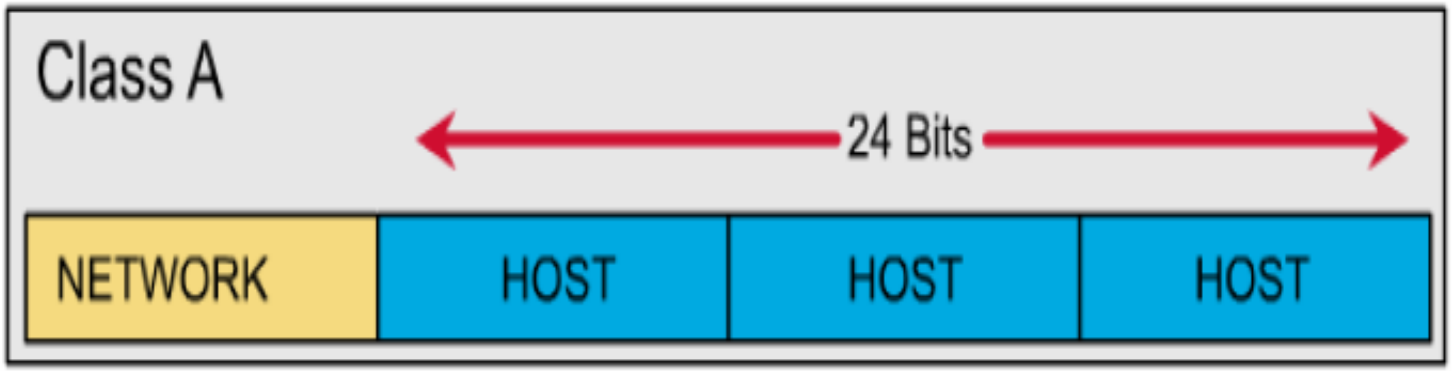
- Địa chỉ host là địa chỉ IP có thể dùng để đặt cho các interface của các host. Hai host nằm cùng một mạng sẽ có network_id giống nhau và host_id khác nhau.
- Khi cấp phát các địa chỉ host thì lưu ý không được cho tất cả các bit trong phần host_id bằng 0 hoặc tất cả bằng 1.
- Địa chỉ mạng (network address): là địa chỉ IP dùng để đặt cho các mạng. Phần host_id của địa chỉ chỉ chứa các bit 0. Ví dụ: 172.29.0.0
- Địa chỉ Broadcast: là địa chỉ IP được dùng để đại diện cho tất cả các host trong mạng. Phần host_id chỉ chứa các bit 1. Ví dụ: 172.29.255.255.

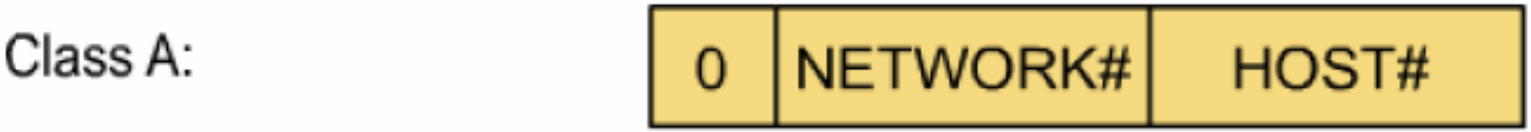
# Các lớp địa chỉ IP

Không gian địa chỉ IP được chia thành 5 lớp (class) A, B, C, D và E. Các lớp A, B và C được triển khai để đặt cho các host trên mạng Internet, lớp D dùng cho các nhóm multicast, còn lớp E phục vụ cho mục đích nghiên cứu.

# Lớp A (Class A)

Dành 1 byte cho phần network_id và 3 byte cho phần host_id.



# Lớp A (Class A)

- Bit đầu tiên của byte đầu tiên phải là bit 0. Dạng nhị phân của octet này là 0xxxxxxx
- Những địa chỉ IP có byte đầu tiên nằm trong khoảng từ 0 (=$00000000_{(2)}$) đến 127 (=$01111111_{(2)}$) sẽ thuộc lớp A.
- Ví dụ: 50.14.32.8.

# Lớp A (Class A)

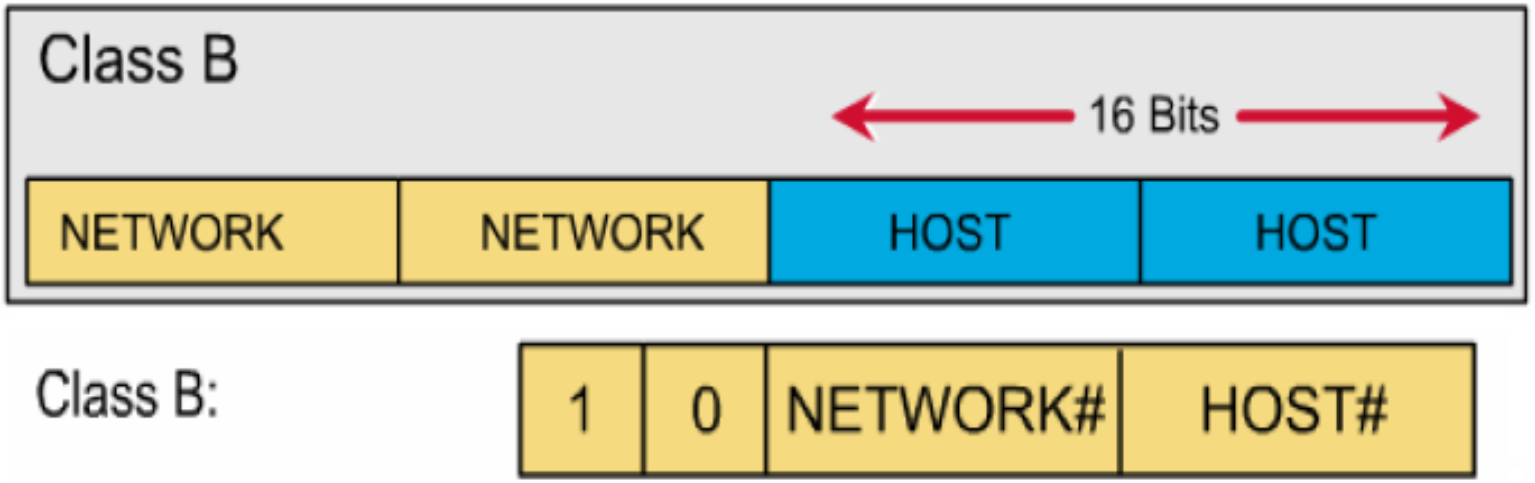
- Byte đầu tiên này cũng chính là network_id, trừ đi bit đầu tiên làm ID nhận dạng lớp A, còn lại 7 bit để đánh thứ tự các mạng, ta được 128 ($=2^7$) mạng lớp A khác nhau. Bỏ đi hai trường hợp đặc biệt là 0 và 127. Kết quả là lớp A chỉ còn 126 địa chỉ mạng, 1.0.0.0 đến 126.0.0.0.

# Lớp A (Class A)

- Phần host_id chiếm 24 bit, nghĩa là có $2^{24}$ = 16777216 host khác nhau trong mỗi mạng. Bỏ đi hai trường hợp đặc biệt (phần host_id chứa toàn các bit 0 và bit 1). Còn lại: 16777214 host.
- Ví dụ đối với mạng 10.0.0.0 thì những giá trị host hợp lệ là 10.0.0.1 đến 10.255.255.254.

# Lớp B (Class B)

Dành 2 byte cho phần network_id và 2 byte cho phần host_id.



# Lớp B (Class B)

- Hai bit đầu tiên của byte đầu tiên phải là 10. Dạng nhị phân của octet này là 10xxxxxx
- Những địa chỉ IP có byte đầu tiên nằm trong khoảng từ 128 (=$10000000_{(2)}$) đến 191 (=$10111111_{(2)}$) sẽ thuộc về lớp B
- Ví dụ: 172.29.10.1 .

# Lớp B (Class B)

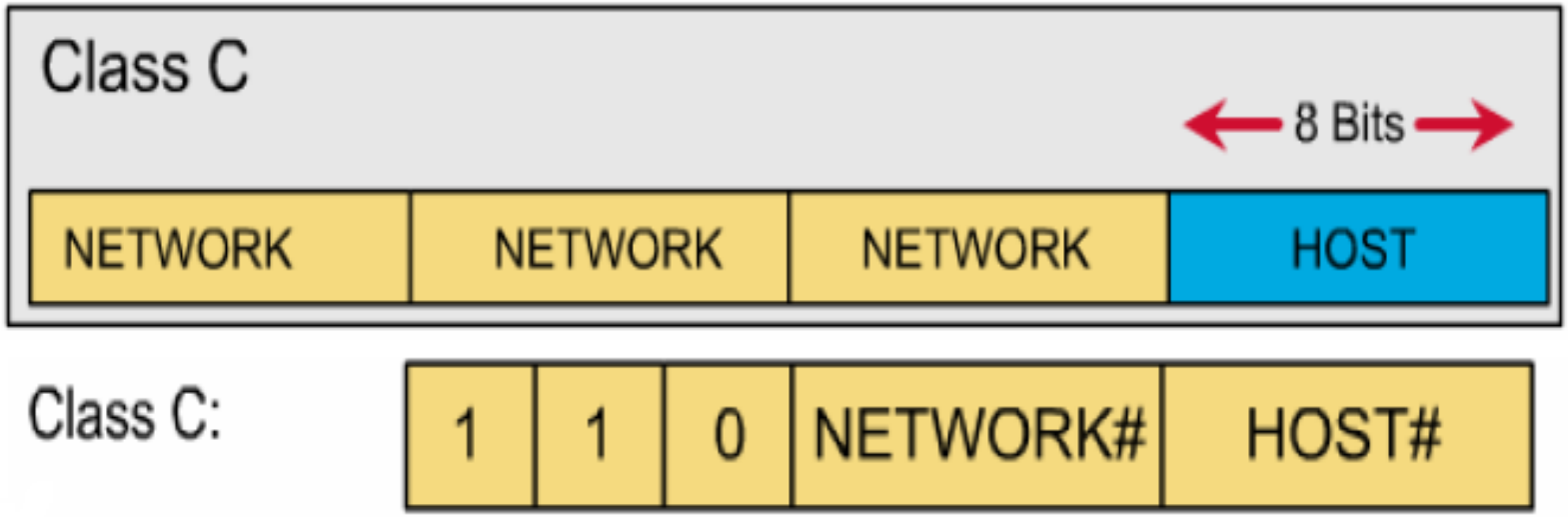
- Phần network_id chiếm 16 bit bỏ đi 2 bit làm ID cho lớp, còn lại 14 bit cho phép ta đánh thứ tự 16384 (=$2^{14}$) mạng khác nhau (128.0.0.0 đến 191.255.0.0).

# Lớp B (Class B)

- Phần host_id dài 16 bit hay có 65536 ($=2^{16}$) giá trị khác nhau. Trừ đi 2 trường hợp đặc biệt còn lại 65534 host trong một mạng lớp B.
- Ví dụ đối với mạng 172.29.0.0 thì các địa chỉ host hợp lệ là từ 172.29.0.1 đến 172.29.255.254.

# Lớp C (Class C)

Dành 3 byte cho phần network_id và 1 byte cho phần host_id.



# Lớp C (Class C)

- Ba bit đầu tiên của byte đầu tiên phải là 110. Dạng nhị phân của octet này là 110xxxxx
- Những địa chỉ IP có byte đầu tiên nằm trong khoảng từ 192 (=$11000000_{(2)}$) đến 223 (=$11011111_{(2)}$) sẽ thuộc về lớp C.
- Ví dụ: 203.162.41.235

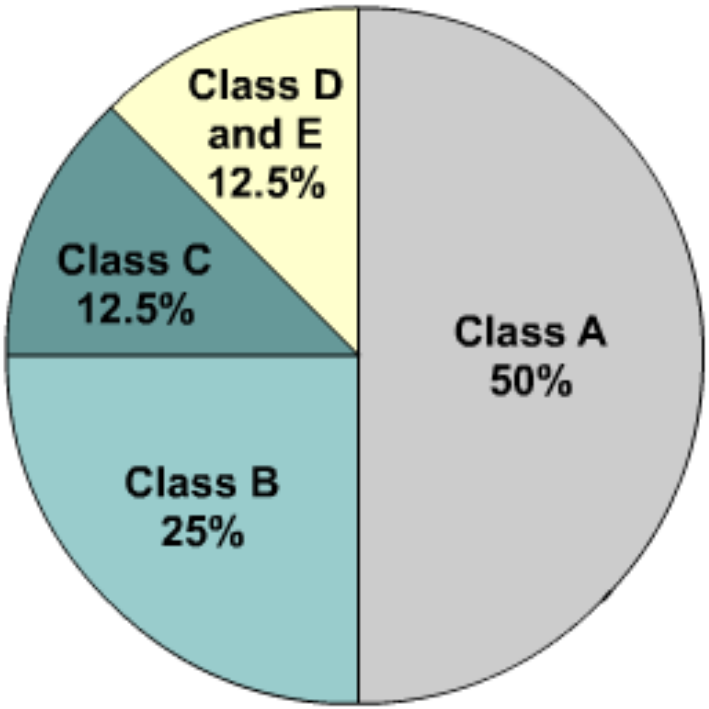
# Các lớp địa chỉ IP

| Address Class | Number of Networks | Number of Host per Network |
|---|---|---|
| A | 126 * | 16,777,216 |
| B | 16, 384 | 65,535 |
| C | 2,097,152 | 254 |
| D (Multicast) | N/A | N/A |

| IP Address Class | High Order Bits | First Octet Address Range | Number of Bits in the Network Address |
|---|---|---|---|
| Class A | 0 | 0 - 127 * | 8 |
| Class B | 10 | 128 - 191 | 16 |
| Class C | 110 | 192 - 223 | 24 |
| Class D | 1110 | 224 - 239 | 28 |

# Các lớp địa chỉ IP

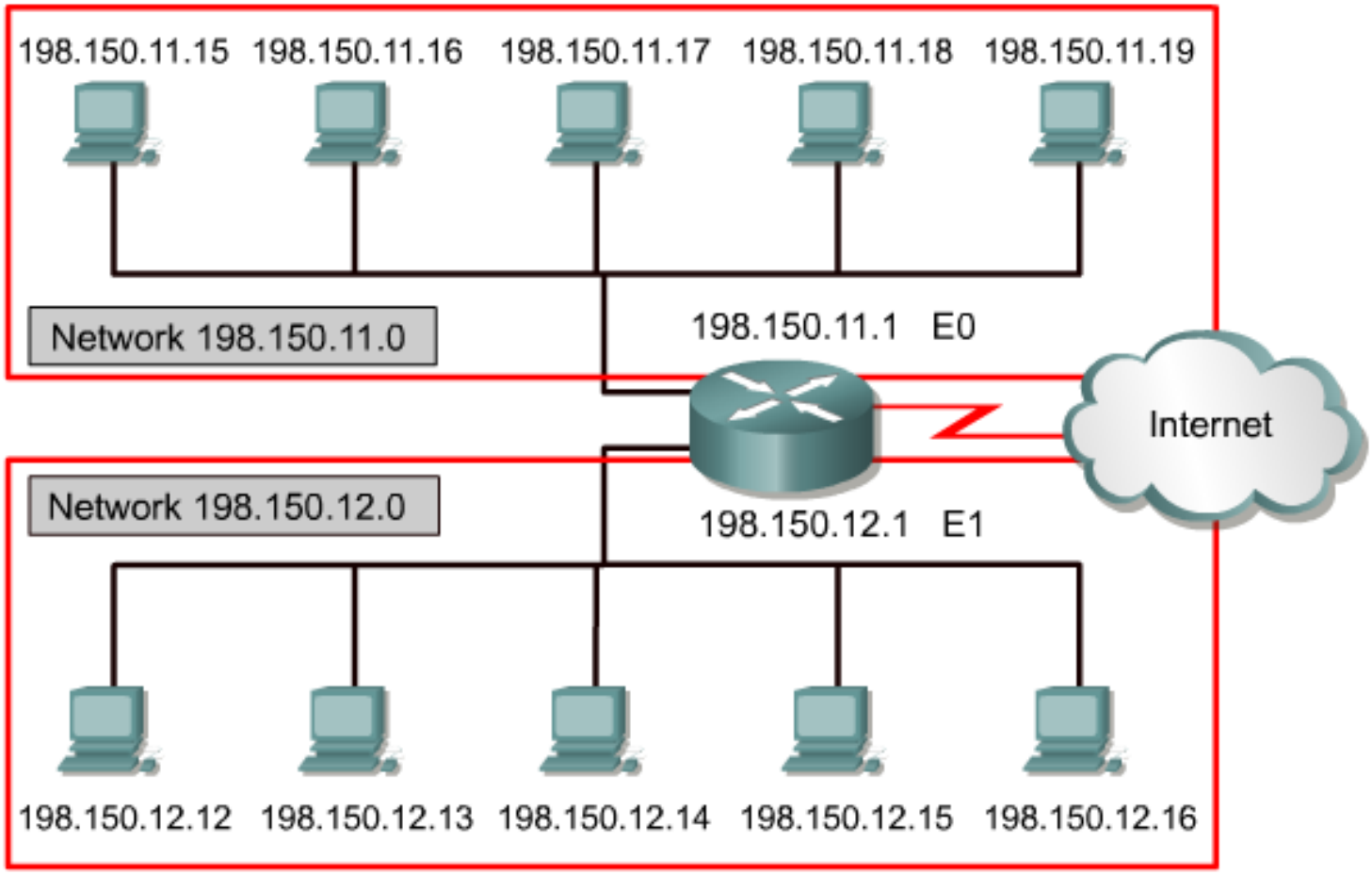
| IP address class | IP address range (First Octet Decimal Value) |
|---|---|
| Class A | 1-126 (00000001-01111110) * |
| Class B | 128-191 (10000000-10111111) |
| Class C | 192-223 (11000000-11011111) |
| Class D | 224-239 (11100000-11101111) |
| Class E | 240-255 (11110000-11111111) |



# Địa chỉ dành riêng

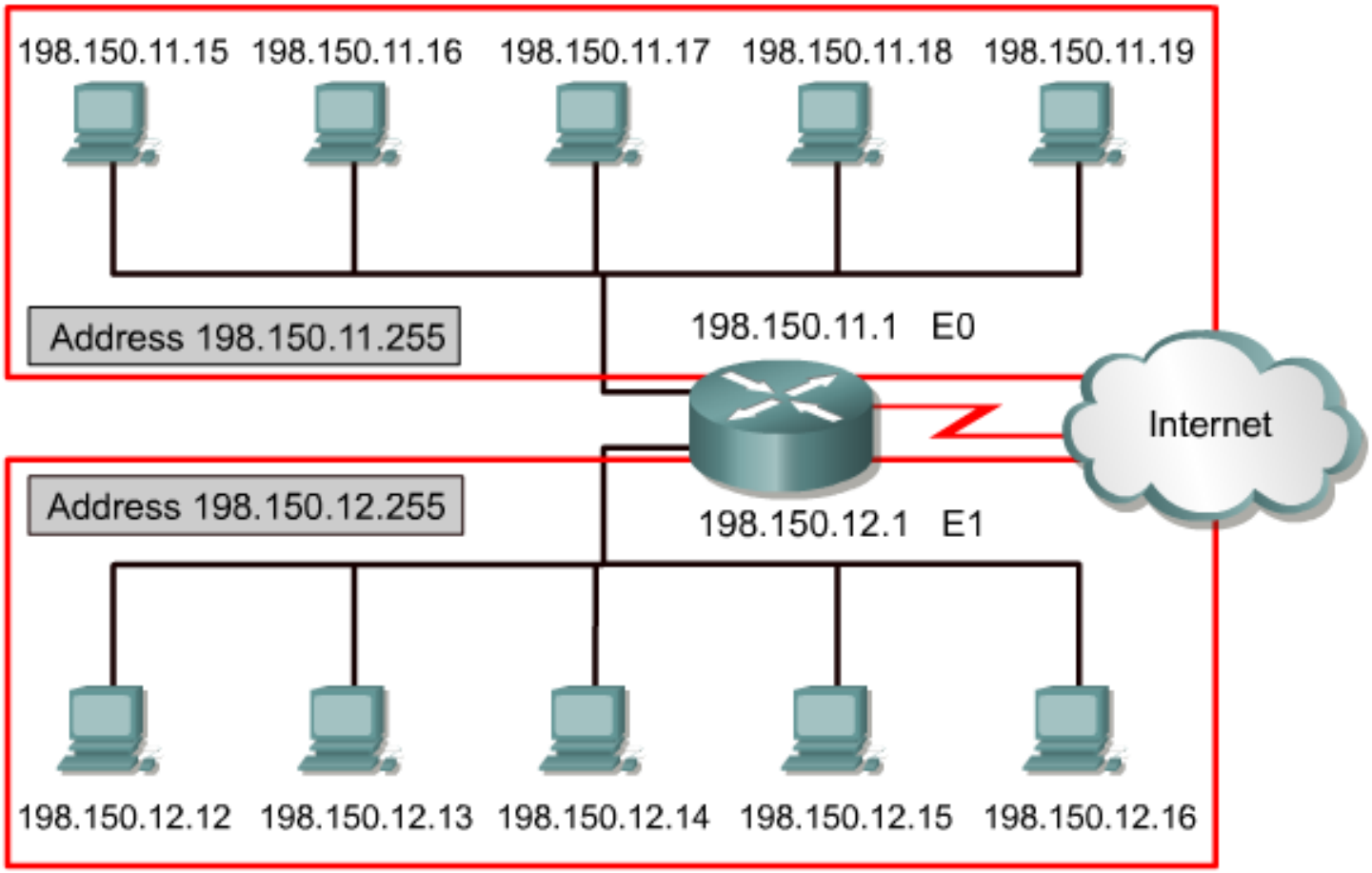
| Class | RFC 1918 internal address range |
|---|---|
| A | 10.0.0.0 to 10.255.255.255 |
| B | 172.16.0.0 to 172.31.255.255 |
| C | 192.168.0.0 to 192.168.255.255 |

# Các lớp địa chỉ IP




Địa chỉ mạng

# Các lớp địa chỉ IP




Địa chỉ broadcast

# Các lớp địa chỉ IP

| Lớp | Byte đầu tiên |
|---|---|
| A | 0xxxxxxx |
| B | 10xxxxxx |
| C | 110xxxxx |
| D | 1110xxxx |
| E | 11110xxx |

- 1.0.0.0 - 126.0.0.0 : Class A.
- 127.0.0.0 : Loopback network.
- 128.0.0.0 - 191.255.0.0 : Class B.
- 192.0.0.0 - 223.255.255.0 : Class C.

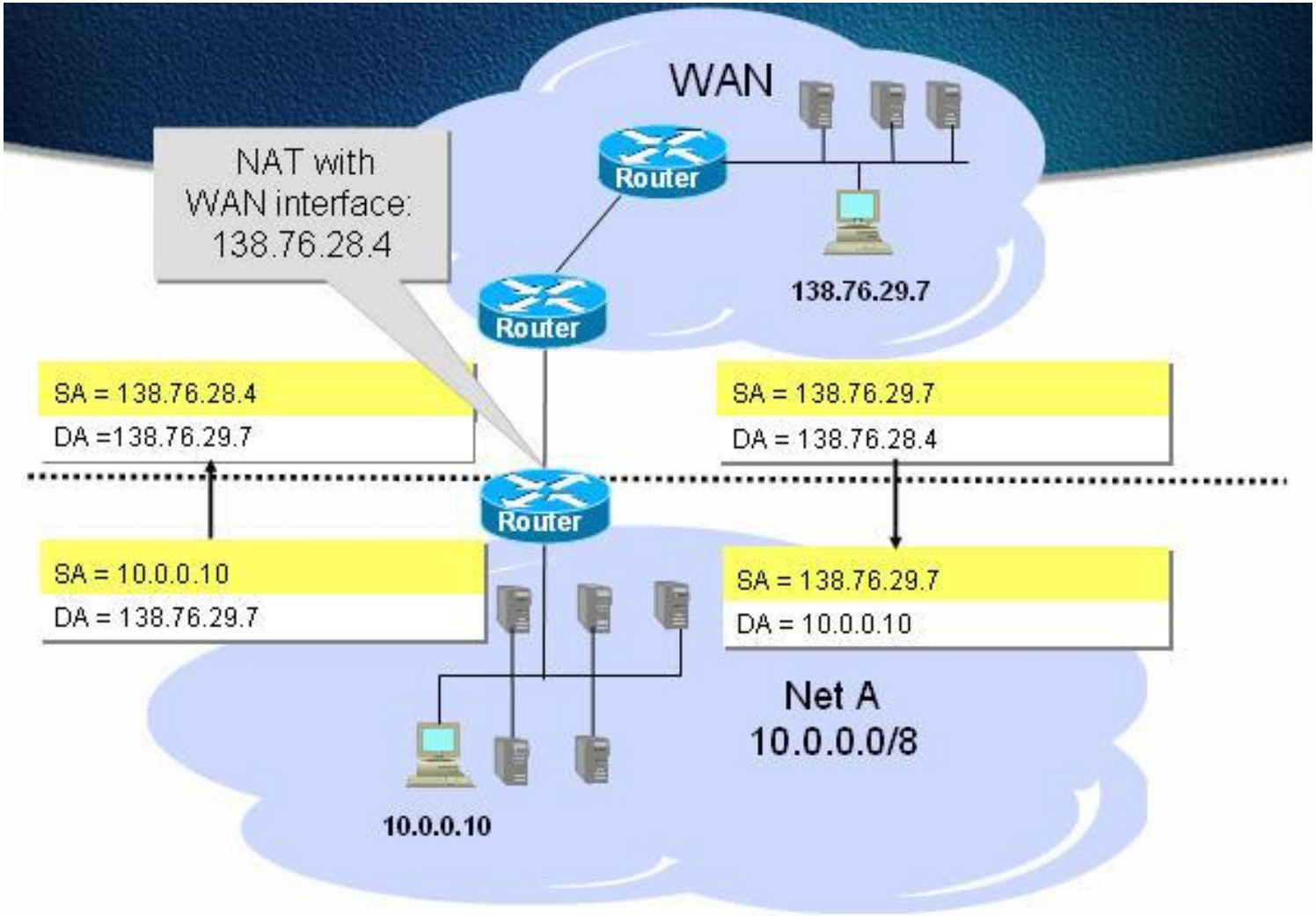
# NAT: Network Address Translation

- Được thiết kế để tiết kiệm địa chỉ IP.
- Cho phép mạng nội bộ sử dụng địa chỉ IP riêng.
- Địa chỉ IP riêng sẽ được chuyển đổi sang địa chỉ công cộng định tuyến được.
- Mạng riêng được tách biệt và giấu kín IP nội bộ.
- Thường sử dụng trên router biên của mạng một cửa.

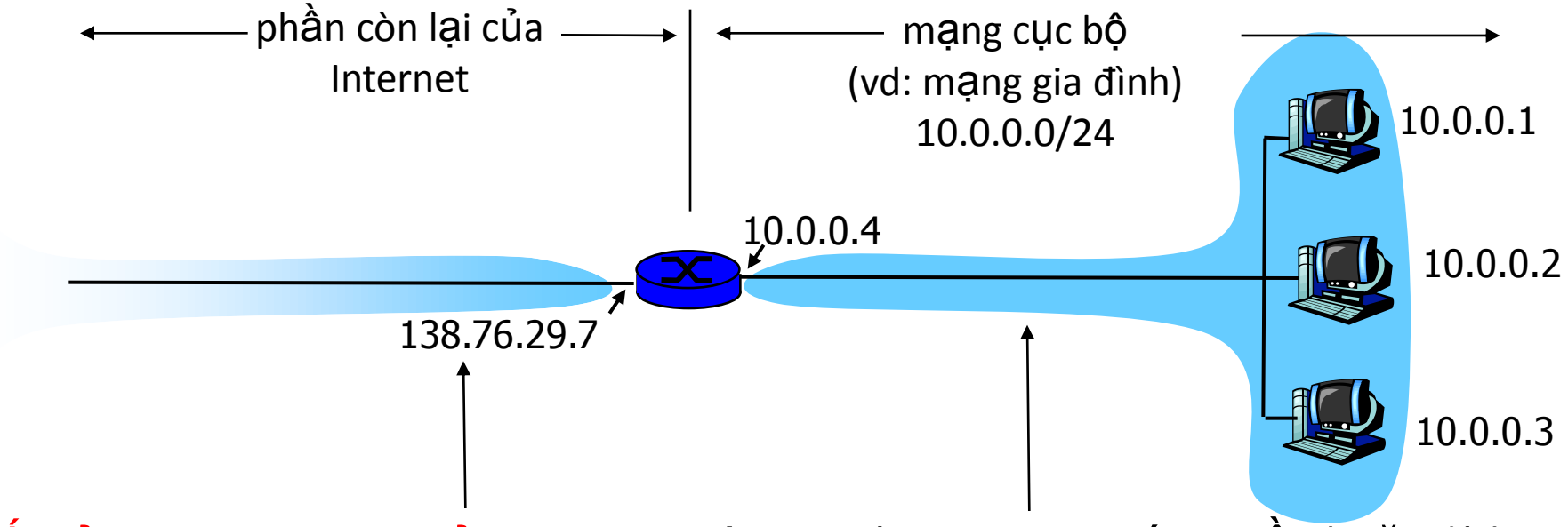
# NAT

- Địa chỉ cục bộ bên trong (Inside local address): Địa chỉ được phân phối cho các host bên trong mạng nội bộ.
- Địa chỉ toàn cục bên trong (Inside global address): Địa chỉ hợp pháp được cung cấp bởi InterNIC (Internet Network Information Center) hoặc nhà cung cấp dịch vụ Internet, đại diện cho một hoặc nhiều địa chỉ nội bộ bên trong đối với thế giới bên ngoài.
- Địa chỉ cục bộ bên ngoài (Outside local address): Địa chỉ riêng của host nằm bên ngoài mạng nội bộ.
- Địa chỉ toàn cục bên ngoài (Outside global address): Địa chỉ công cộng hợp pháp của host nằm bên ngoài mạng nội bộ.

# NAT


WAN
NAT with
WAN interface:
138.76.28.4
Router
Router
Router
138.76.29.7
SA = 138.76.28.4
DA =138.76.29.7
SA = 138.76.29.7
DA = 138.76.28.4
SA = 10.0.0.10
DA = 138.76.29.7
SA = 138.76.29.7
DA = 10.0.0.10
Net A
10.0.0.0/8
10.0.0.10

# NAT




*Tất cả* datagram *đi ra khỏi* mạng cục bộ có cùng một địa chỉ IP NAT là: 138.76.29.7, với các số hiệu cổng nguồn khác nhau

các Datagram với nguồn hoặc đích trong mạng này có địa chỉ 10.0.0/24

# NAT

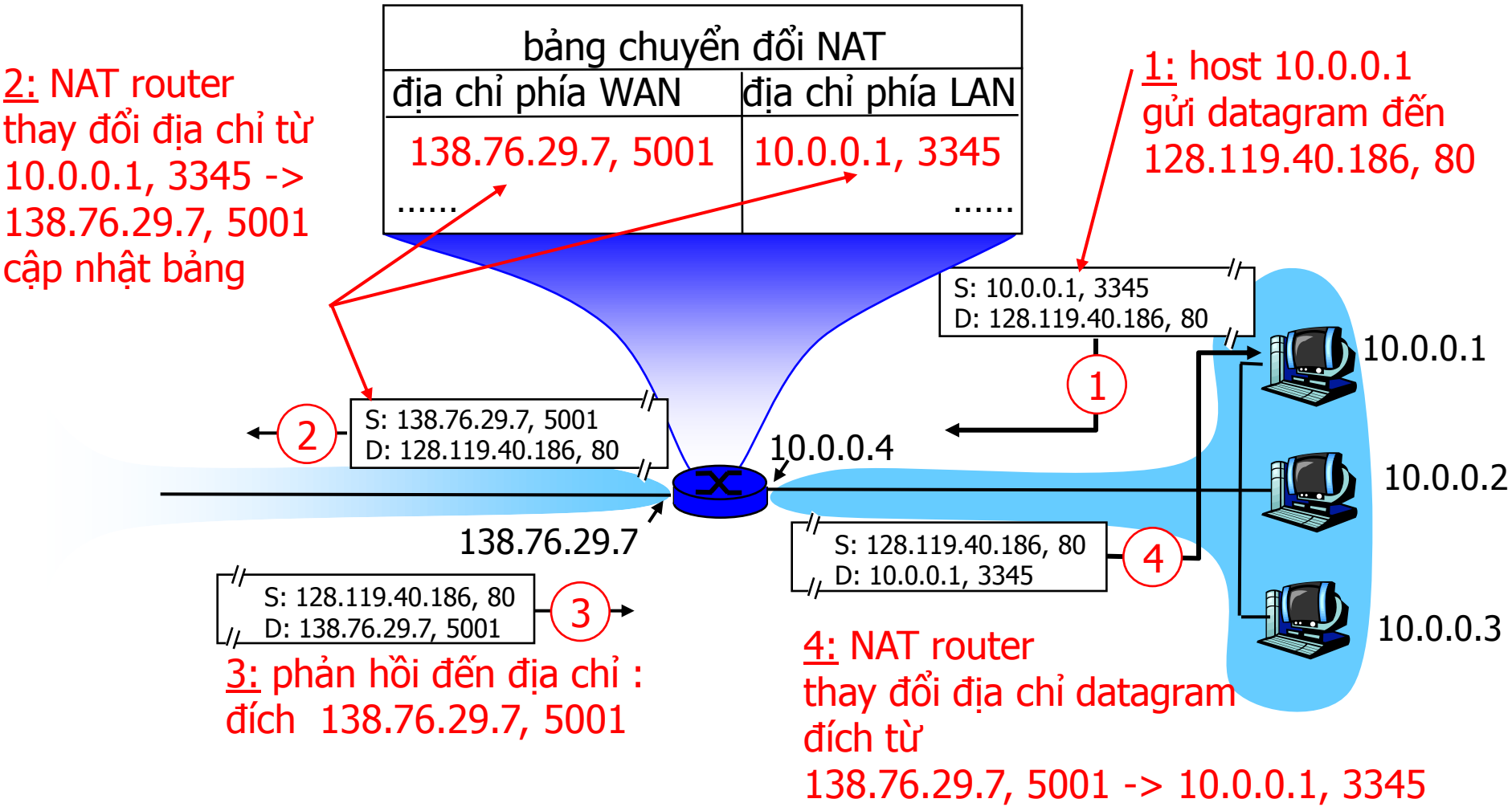
- Mạng cục bộ chỉ dùng 1 địa chỉ IP đối với bên ngoài:
  - không cần thiết dùng 1 vùng địa chỉ từ ISP: chỉ cần 1 cho tất cả các thiết bị
  - có thể thay đổi địa chỉ các thiết bị trong mạng cục bộ mà không cần thông báo với bên ngoài
  - có thể thay đổi ISP mà không cần thay đổi địa chỉ các thiết bị trong mạng cục bộ
  - các thiết bị trong mạng cục bộ không nhìn thấy, không định địa chỉ rõ ràng từ bên ngoài (tăng cường bảo mật)

# NAT

Hiện thực: NAT router phải:

- *các datagram đi ra:* thay thế (địa chỉ IP và số hiệu cổng nguồn) mọi datagram đi ra bên ngoài bằng (địa chỉ NAT IP và số hiệu cổng nguồn mới)
  - . . . các clients/servers ở xa sẽ dùng (địa chỉ NAT IP và số hiệu cổng nguồn mới) đó như địa chỉ đích
- *ghi nhớ (trong bảng chuyển đổi NAT)* mọi cặp chuyển đổi (địa chỉ IP và số hiệu cổng nguồn) sang (địa chỉ NAT IP và số hiệu cổng nguồn mới)
- *các datagram đi đến:* thay thế (địa chỉ NAT IP và số hiệu cổng nguồn mới) trong các trường đích của mọi datagram đến với giá trị tương ứng (địa chỉ IP và số hiệu cổng nguồn) trong bảng NAT

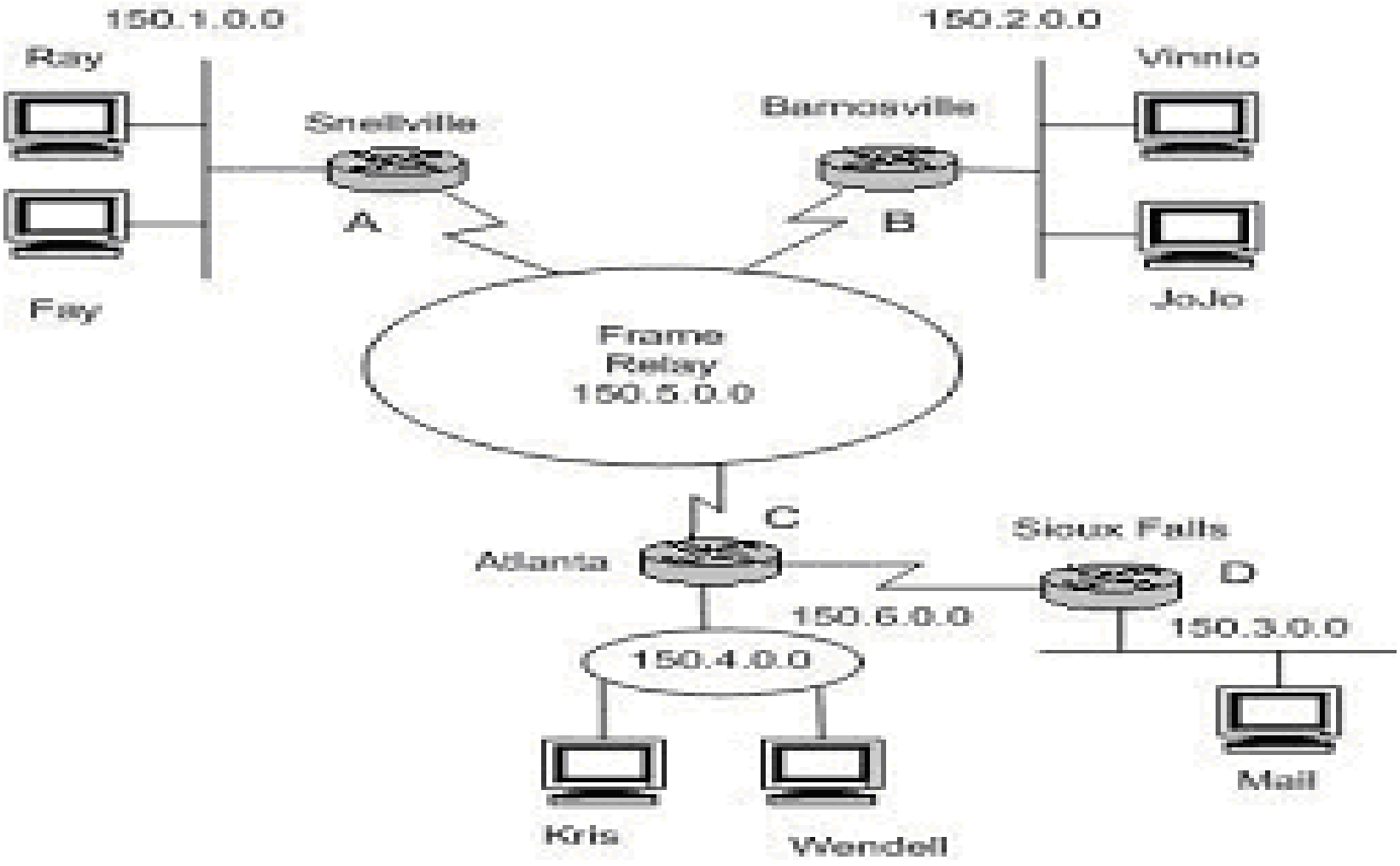
# NAT


bảng chuyển đổi NAT
địa chỉ phía WAN
địa chỉ phía LAN
138.76.29.7, 5001
10.0.0.1, 3345
.....
.....
2: NAT router thay đổi địa chỉ từ 10.0.0.1, 3345 -> 138.76.29.7, 5001 cập nhật bảng
1: host 10.0.0.1 gửi datagram đến 128.119.40.186, 80
S: 10.0.0.1, 3345
D: 128.119.40.186, 80
1
2
S: 138.76.29.7, 5001
D: 128.119.40.186, 80
10.0.0.4
138.76.29.7
10.0.0.1
10.0.0.2
10.0.0.3
S: 128.119.40.186, 80
D: 10.0.0.1, 3345
4
S: 128.119.40.186, 80
D: 138.76.29.7, 5001
3
3: phản hồi đến địa chỉ : đích 138.76.29.7, 5001
4: NAT router thay đổi địa chỉ datagram đích từ 138.76.29.7, 5001 -> 10.0.0.1, 3345

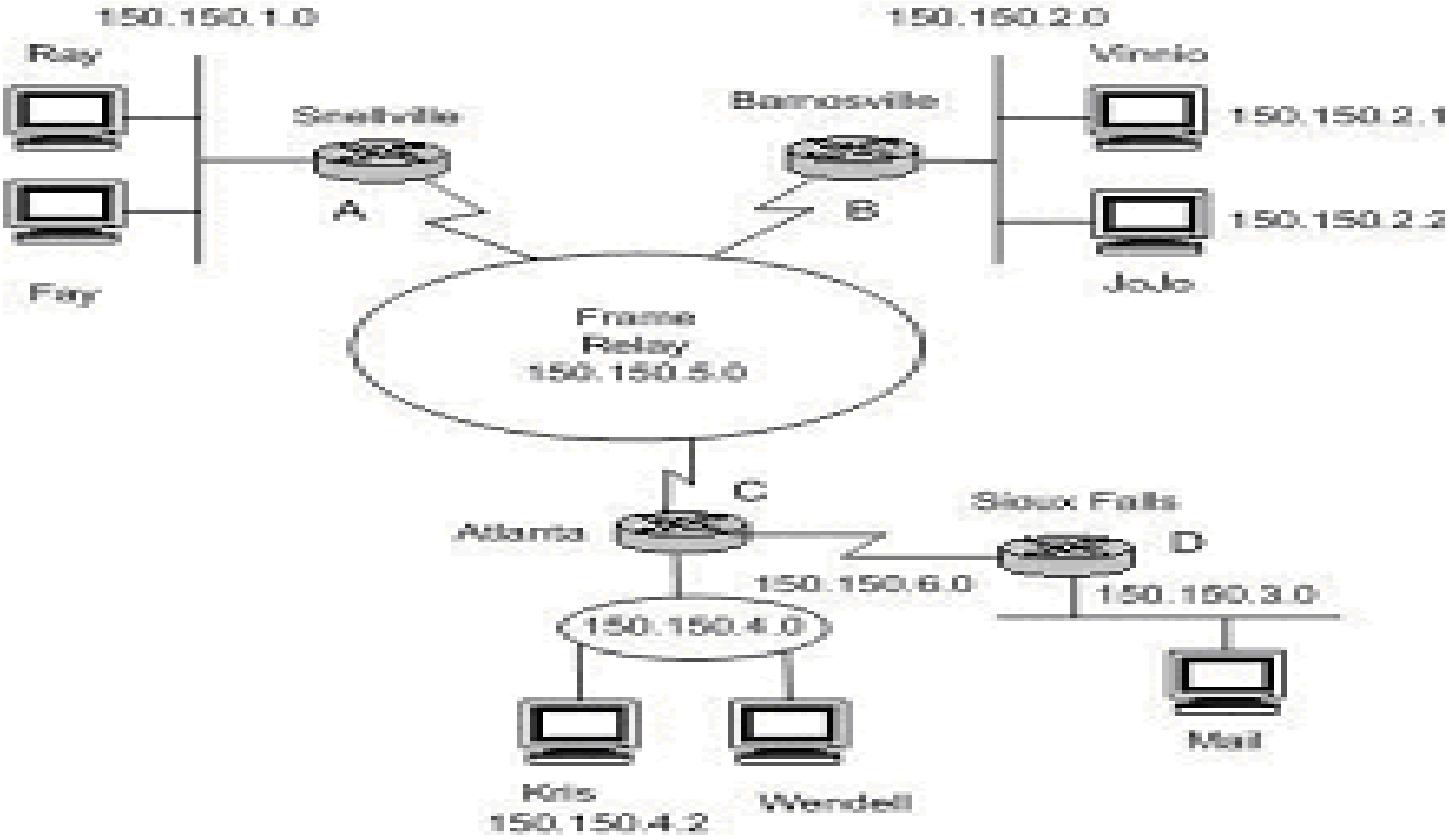
# NAT

- Trường số hiệu cổng 16-bit:
  - Cho phép 60000 kết nối đồng thời chỉ với một địa chỉ phía WAN
- NAT còn có thể gây ra tranh luận:
  - các router chỉ xử lý đến lớp 3
  - vi phạm thỏa thuận end-to-end
    - những người thiết kế ứng dụng phải tính đến khả năng NAT, vd: ứng dụng P2P
  - sự thiếu thốn địa chỉ IP sẽ được giải quyết khi dùng IPv6

# Mạng con

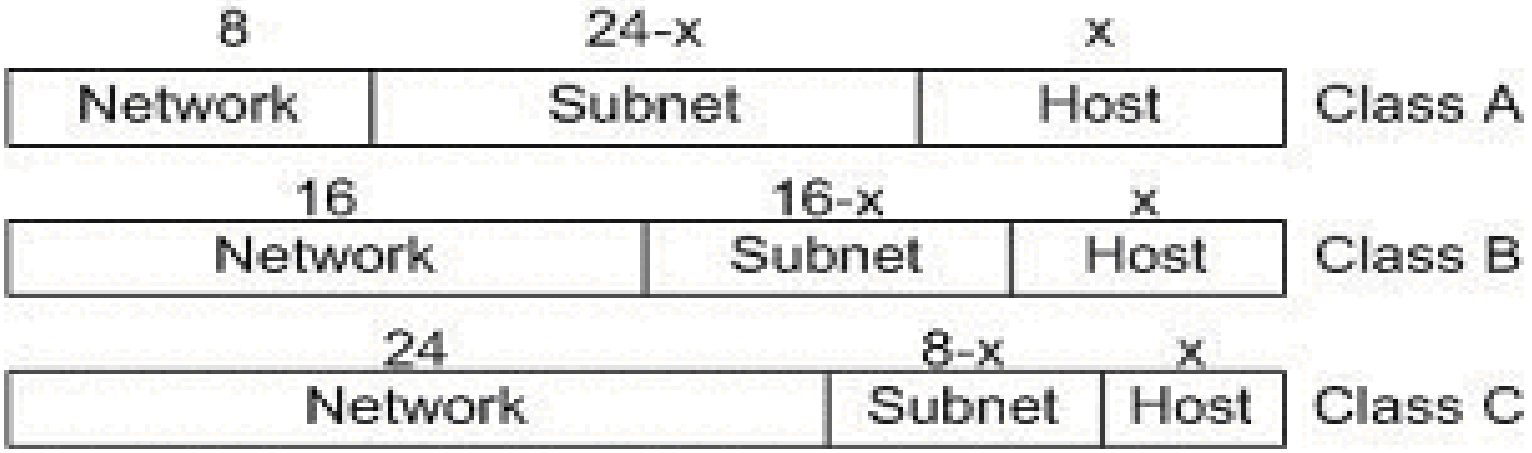

150.1.0.0
Ray
Fay
Snellville
A
150.2.0.0
Vinnie
Barnesville
B
JoJo
Frame
Relay
150.5.0.0
C
Atlanta
Sioux Falls
D
150.6.0.0
150.3.0.0
150.4.0.0
Mail
Kris
Wendell

# Mạng con


150.150.1.0
Ray
Snellville
A
Fay
150.150.2.0
Vinnie
Barnesville
B
150.150.2.1
150.150.2.2
JoJo
Frame
Relay
150.150.5.0
C
Atlanta
Sioux Falls
D
150.150.6.0
150.150.3.0
150.150.4.0
Mail
Kris
150.150.4.2
Wendell

# Kỹ thuật chia mạng con

- Mượn một số bit trong phần host_id ban đầu để đặt cho các mạng con
- Cấu trúc của địa chỉ IP lúc này sẽ gồm 3 phần: network_id, subnet_id và host_id.



# Kỹ thuật chia mạng con

- Số bit dùng trong subnet_id tuỳ thuộc vào chiến lược chia mạng con. Tuy nhiên số bit tối đa có thể mượn phải tuân theo công thức:

  **Subnet_id <= host_id - 2**

- Số lượng bit tối đa có thể mượn:
  - Lớp A: 22 (= 24 – 2) bit -> chia được $2^{22}$ = 4194304 mạng con
  - Lớp B: 14 (= 16 – 2) bit -> chia được $2^{14}$ = 16384 mạng con
  - Lớp C: 06 (= 8 – 2) bit -> chia được $2^{6}$ = 64 mạng con

# Kỹ thuật chia mạng con

- Số bit trong phần subnet_id xác định số lượng mạng con. Với số bit là x thì $2^x$ là số lượng mạng con có được.
- Ngược lại từ số lượng mạng con cần thiết theo nhu cầu, tính được phần subnet_id cần bao nhiêu bit. Nếu muốn chia 6 mạng con thì cần 3 bit ($2^3$=8), chia 12 mạng con thì cần 4 bit ($2^4$>=12).

# Một số khái niệm mới

- Địa chỉ mạng con (địa chỉ đường mạng): gồm cả phần network_id và subnet_id, phần host_id chỉ chứa các bit 0
- Địa chỉ broadcast trong một mạng con: tất cả các bit trong phần host_id là 1.
- Mặt nạ mạng con (subnet mask): tất cả các bit trong phần host_id là 0, các phần còn lại là 1.

# Quy ước ghi địa chỉ IP

- Nếu có địa chỉ IP như 172.29.8.230 thì chưa thể biết được host này nằm trong mạng nào, có chia mạng con hay không và có nếu chia thì dùng bao nhiêu bit để chia. Chính vì vậy khi ghi nhận địa chỉ IP của một host, phải cho biết subnet mask của nó
- Ví dụ: 172.29.8.230/255.255.255.0 hoặc 172.29.8.230/24 (có nghĩa là dùng 24 bit đầu tiên cho NetworkID).

# Kỹ thuật chia mạng con

- Thực hiện 3 bước:
  - Bước 1: Xác định lớp (class) và subnet mask mặc nhiên của địa chỉ.
  - Bước 2: Xác định số bit cần mượn và subnet mask mới, tính số lượng mạng con, số host thực sự có được.
  - Bước 3: Xác định các vùng địa chỉ host và chọn mạng con muốn dùng

# Bài tập 1

Cho địa chỉ IP sau: 172.16.0.0/16.

Hãy chia thành 8 mạng con và có tối thiểu 1000 host trên mỗi mạng con đó.

# Bước 1: Xác định class và subnet mask mặc nhiên

**Giải**:

- Địa chỉ trên viết dưới dạng nhị phân
  10101100.00010000.00000000.00000000
- Xác định lớp của IP trên:

  [redacted]ớp B
- Xác định Subnet mask mặc nhiên:

  [redacted]55.255.0.0

# Bước 2: Số bit cần mượn...

- Cần mượn bao nhiêu bit:

  N = 3, bởi vì:

  Số mạng con có thể: $2^3 = 8$.

  Số host của mỗi mạng con có thể:

  $2^{(16-3)} - 2 = 2^{13} - 2 > 1000$.

- Xác định Subnet mask mới:

  11111111.11111111.11100000.00000000

  hay 255.255.224.0

# Bước 3: Xác định vùng địa chỉ host

| STT | | | |
|---|---|---|---|
| 1 | 172.16.0.0 | 172.16.0.1 - 172.16.31.254 | 172.16.31.255 |
| 2 | 172.16.32.0 | 172.16.32.1 - 172.16.63.254 | 172.16.63.255 |
| … | … | | |
| 7 | 172.16.192.0 | | |
| 8 | 172.16.224.0 | 172.16.224.1 – 172.16.255.254 | 172.16.255.255 |

10101100.00010000.000**00000.00000001**
Đến
10101100.00010000.000**11111.11111111**

10101100.00010000.001**00000.00000001**
Đến
10101100.00010000.001**11111.11111110**

10101100.00010000.000**00000.00000000**

10101100.00010000.001**11111.11111111**

# Bài tập 2

Cho 2 địa chỉ IP sau:

192.168.5.9/28

192.168.5.39/28

- Hãy cho biết các địa chỉ network, host của từng IP trên?
- Các máy trên có cùng mạng hay không ?
- Hãy liệt kê tất cả các địa chỉ IP thuộc các mạng vừa tìm được?

# Địa chỉ IP thứ nhất: 192.168.5.9/28

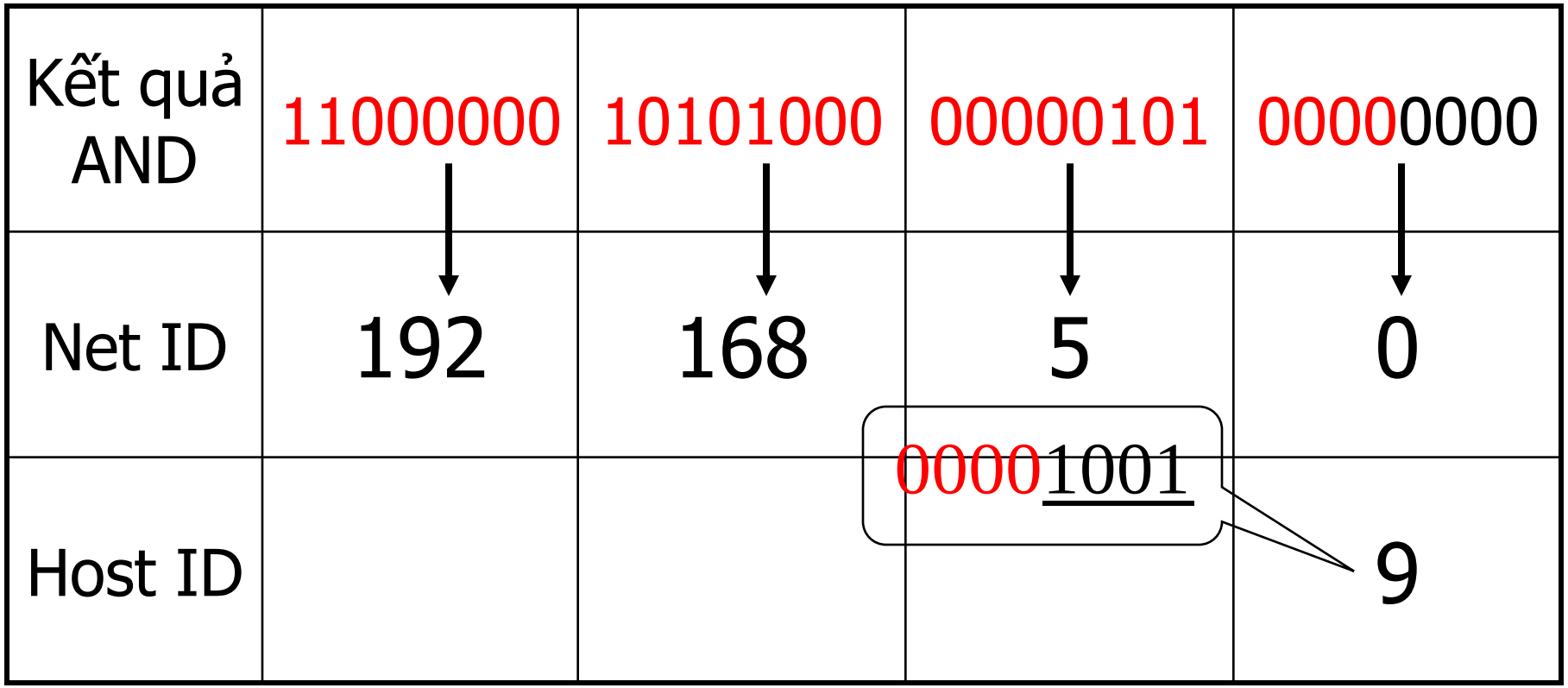
- Chú ý: 28 là số bit dành cho NetworkID
- Đây là IP thuộc lớp C
- Subnet mask mặc nhiên: 255.255.255.0

| IP (thập phân) | 192 | 168 | 5 | 9 |
|---|---|---|---|---|
| IP (nhị phân) | 11000000 | 10101000 | 00000101 | 00001001 |

# Thực hiện AND địa chỉ IP với Subnet mask

| | | | | |
|---|---|---|---|---|
| IP | 11000000 | 10101000 | 00000101 | 00001001 |
| Subnet mask | 11111111 | 11111111 | 11111111 | 11110000 |
| Kết quả AND | 11000000 | 10101000 | 00000101 | 00000000 |

# Chuyển IP sang dạng thập phân



# Địa chỉ IP thứ hai: 192.168.5.39/28

| IP | 192 | 168 | 5 | 39 |
|---|---|---|---|---|
| IP (nhị phân) | 11000000 | 10101000 | 00000101 | 00100111 |
| Subnet Mask | 11111111 | 11111111 | 11111111 | 11110000 |
| AND | 11000000 | 10101000 | 00000101 | 00100000 |
| Network ID | 192 | 168 | 5 | 32 |
| HostID | | | | 7 |

# Hai địa chỉ trên có cùng mạng?

- 192.168.5.9/28
- 192.168.5.39/28

**Kết luận:** Hai địa chỉ trên không cùng mạng

| | | | | |
|---|---|---|---|---|
| Net ID của địa chỉ thứ 1 | 192 | 168 | 5 | 0 |
| Net ID của địa chỉ thứ 2 | 192 | 168 | 5 | 32 |

# Liệt kê tất cả các địa chỉ IP

| Mạng tương ứng với IP | Vùng địa chỉ HostID với dạng nhị phân | Vùng địa chỉ HostID với dạng thập phân |
|---|---|---|
| 1 | 11000000.10101000.00000101.00000001<br>Đến<br>11000000.10101000.00000101.00001110 | 192.168.5.1/28<br>Đến<br>192.168.5.14/28 |
| 2 | 11000000.10101000.00000101.00100001<br>Đến<br>11000000.10101000.00000101.00101110 | 192.168.5.33/28<br>Đến<br>192.168.5.46/28 |

# Bài tập 3

Hãy xét đến một địa chỉ IP class B, **139.12.0.0**, với subnet mask là **255.255.0.0**. Một Network với địa chỉ thế này có thể chứa 65534 nodes hay computers. Đây là một con số quá lớn, trên mạng sẽ có đầy broadcast traffic. Hãy chia network thành 5 mạng con.

# Bước 1: Xác định Subnet mask

- Để chia thành 5 mạng con thì cần thêm 3 bit (vì $2^3 > 5$).
- Do đó Subnet mask sẽ cần: 16 (bits trước đây) + 3 (bits mới) = 19 bits
- Địa chỉ IP mới sẽ là **139.12.0.0/19** (để ý con số 19 thay vì 16 như trước đây).

# Bước 2: Liệt kê ID của các Subnet mới

| Subnet mask với dạng nhị phân | Subnet mask với dạng thập phân |
|---|---|
| 11111111.11111111.11100000.00000000 | 255.255.224.0 |

# NetworkID của bốn Subnets mới

| TT | Subnet ID với dạng nhị phân | Subnet ID với dạng thập phân |
|---|---|---|
| 1 | 10001011.00001100.00000000.00000000 | 139.12.0.0/19 |
| 2 | 10001011.00001100.00100000.00000000 | 139.12.32.0/19 |
| 3 | 10001011.00001100.01000000.00000000 | 139.12.64.0/19 |
| 4 | 10001011.00001100.01100000.00000000 | 139.12.96.0/19 |
| 5 | 10001011.00001100.10000000.00000000 | 139.12.128.0/19 |

# Bước 3: Cho biết vùng địa chỉ IP của các HostID

| TT | Dạng nhị phân | Dạng thập phân |
|---|---|---|
| 1 | 10001011.00001100.00000000.00000001<br>10001011.00001100.00011111.11111110 | 139.12.0.1/19 -<br>139.12.31.254/19 |
| 2 | 10001011.00001100.00100000.00000001<br>10001011.00001100.00111111.11111110 | 139.12.32.1/19 -<br>139.12.63.254/19 |
| 3 | 10001011.00001100.01000000.00000001<br>10001011.00001100.01011111.11111110 | 139.12.64.1/19 -<br>139.12.95.254/19 |
| 4 | 10001011.00001100.01100000.00000001<br>10001011.00001100.01111111.11111110 | 139.12.96.1/19 -<br>139.12.127.254/19 |
| 5 | 10001011.00001100.10000000.00000001<br>10001011.00001100.10011111.11111110 | 139.12.128.1/19 -<br>139.12.159.254/19 |

# Tính nhanh vùng địa chỉ IP

- n – số bit làm subnet
- Số mạng con: $S = 2^n$
- Số gia địa chỉ mạng con: $M = 2^{8-n}$ $(n \leq 8)$
- Byte cuối của IP địa chỉ mạng, ví dụ lớp C: (k-1)*M (với k=1,2,…)
- Byte cuối của IP host đầu tiên, ví dụ lớp C: (k-1)*M + 1 (với k=1,2,…)
- Byte cuối của IP host cuối cùng, ví dụ lớp C: k*M - 2 (với k=1,2,…)
- Byte cuối của IP broadcast, ví dụ lớp C: k*M - 1 (với k=1,2,…)

# Ví dụ tính nhanh vùng địa chỉ IP

- Cho địa chỉ: 192.168.0.0/24
- Với n=4 → M= 16 (= $2^{8-4}$) →
  - Network 1: 192.168.0.0. Host range: 192.168.0.1–192.168.0.14. Broadcast: 192.168.0.15
  - Network 2: 192.168.0.16. Host range: 192.168.0.17–192.168.0.30. Broadcast: 192.168.0.31
  - Network 3: 192.168.0.32. Host range: 192.168.0.33–192.168.0.46. Broadcast: 192.168.0.47
  - Network 4: 192.168.0.48. Host range: 192.168.0.49–192.168.0.62. Broadcast: 192.168.0.63

# Bài tập 4

- Cho địa chỉ IP: 102.16.10.107/12
  - Tìm địa chỉ mạng con? Địa chỉ host
  - Dải địa chỉ host có cùng mạng với IP trên?
  - Broadcast của mạng mà IP trên thuộc vào?

# Bước: Tính subnet mask

- 102.16.10.107/12 ➔
- Subnet mask: 11111111.1111**0000**.00000000.00000000
- Byte đầu tiên chắc chắn khi dùng phép toán AND ra kết quả bằng 102 → không cần đổi 102 sang nhị phân

# Trả lời câu hỏi 1: Địa chỉ mạng con?

- Xét byte kế tiếp là: 16 (10) → 00010000 (2)
- Khi AND byte này với Subnet mask, ta được kết quả là: 00010000 (2)
- Như vậy địa chỉ mạng con sẽ là:

**102.16.0.0/12**

- Như vậy địa chỉ host sẽ là:

**0.10.107**

# Trả lời câu hỏi 2: Dải địa chỉ host? Broadcast?

- Dải địa chỉ host sẽ từ:

01100110 00010000 00000000 00000001

**(hay 102.16.0.1/12)**

Đến:

01100110 00011111 11111111 11111110

**(hay 102.31.255.254/12)**

- Broadcast:

**102.31.255.255/12**

# Bài tập 5: Cho IP 172.19.160.0/21

- Chia làm 4 mạng con
- Liệt kê các thông số gồm địa chỉ mạng, dãy địa chỉ host, địa chỉ broadcast của các mạng con đó

# Giải BT 5

- Chia làm 4 mạng con nên phải mượn 2 bit
- Do /21 nên 2 byte đầu tiên của IP đã cho không thay đổi. Xét byte thứ 3
- 160 = 10100000$_{(2)}$
- Phần 2 bit 00 là nơi ta mượn làm subnet

# Giải BT 5 (tt)

- Xét byte thứ 3
- Mạng con thứ 1: $10100000_{(2)}$
- Mạng con thứ 2: $10100010_{(2)}$
- Mạng con thứ 3: $10100100_{(2)}$
- Mạng con thứ 4: $10100110_{(2)}$

# Giải BT 5 (tt)

| Địa chỉ mạng | Dải địa chỉ host | Địa chỉ broadcast |
|---|---|---|
| 172.19.160.0 | 172.19.160.1 đến 172.19.161.254 | 172.19.161.255 |
| 172.19.162.0 | 172.19.162.1 đến 172.19.163.254 | 172.19.163.255 |
| 172.19.164.0 | 172.19.164.1 đến 172.19.165.254 | 172.19.165.255 |
| 172.19.166.0 | 172.19.166.1 đến 172.19.167.254 | 172.19.167.255 |

# Bài tập 6: Cho IP 172.16.192.0/18

- Chia làm 4 mạng con
- Liệt kê các thông số gồm địa chỉ mạng, dãy địa chỉ host, địa chỉ broadcast của các mạng con đó

# Giải BT 6

- Chia làm 4 mạng con nên phải mượn 2 bit
- Do /18 nên 2 byte đầu tiên của IP đã cho không thay đổi. Xét byte thứ 3
- 192 = 11000000$_{(2)}$
- Phần 2 bit 00 là nơi ta mượn làm subnet

# Giải BT 6 (tt)

- Xét byte thứ 3
- Mạng con thứ 1: $11000000_{(2)}$
- Mạng con thứ 2: $11010000_{(2)}$
- Mạng con thứ 3: $11100000_{(2)}$
- Mạng con thứ 4: $11110000_{(2)}$

# Giải BT 6 (tt)

| Địa chỉ mạng | Dải địa chỉ host | Địa chỉ broadcast |
|---|---|---|
| 172.16.192.0 | 172.16.192.1 đến 172.16.207.254 | 172.16.207.255 |
| 172.16.208.0 | 172.16.208.1 đến 172.16.223.254 | 172.16.223.255 |
| 172.16.224.0 | 172.16.224.1 đến 172.16.239.254 | 172.16.239.255 |
| 172.16.240.0 | 172.16.240.1 đến 172.16.255.254 | 172.16.255.255 |

# CHƯƠNG 6: BẢO MẬT MẠNG

- Hiểu các nguyên lý của bảo mật mạng:
  - mật mã
  - chứng thực
  - tính toàn vẹn
  - khóa phân bố
- Bảo mật trong thực tế:
  - các firewall
  - bảo mật trong các lớp application, transport, network, data-link

# Bảo mật mạng là gì?

Sự bảo mật: chỉ có người gửi, người nhận mới "hiểu" được nội dung thông điệp

- người gửi mã hóa thông điệp
- người nhận giải mã thông điệp

Chứng thực: người gửi, người nhận xác định là nhận ra nhau

Sự toàn vẹn thông điệp: người gửi, người nhận muốn bảo đảm thông điệp không bị thay đổi (trên đường truyền hoặc sau khi nhận)

Truy cập & tính sẵn sàng: các dịch vụ phải có khả năng truy cập và sẵn sàng đối với các user

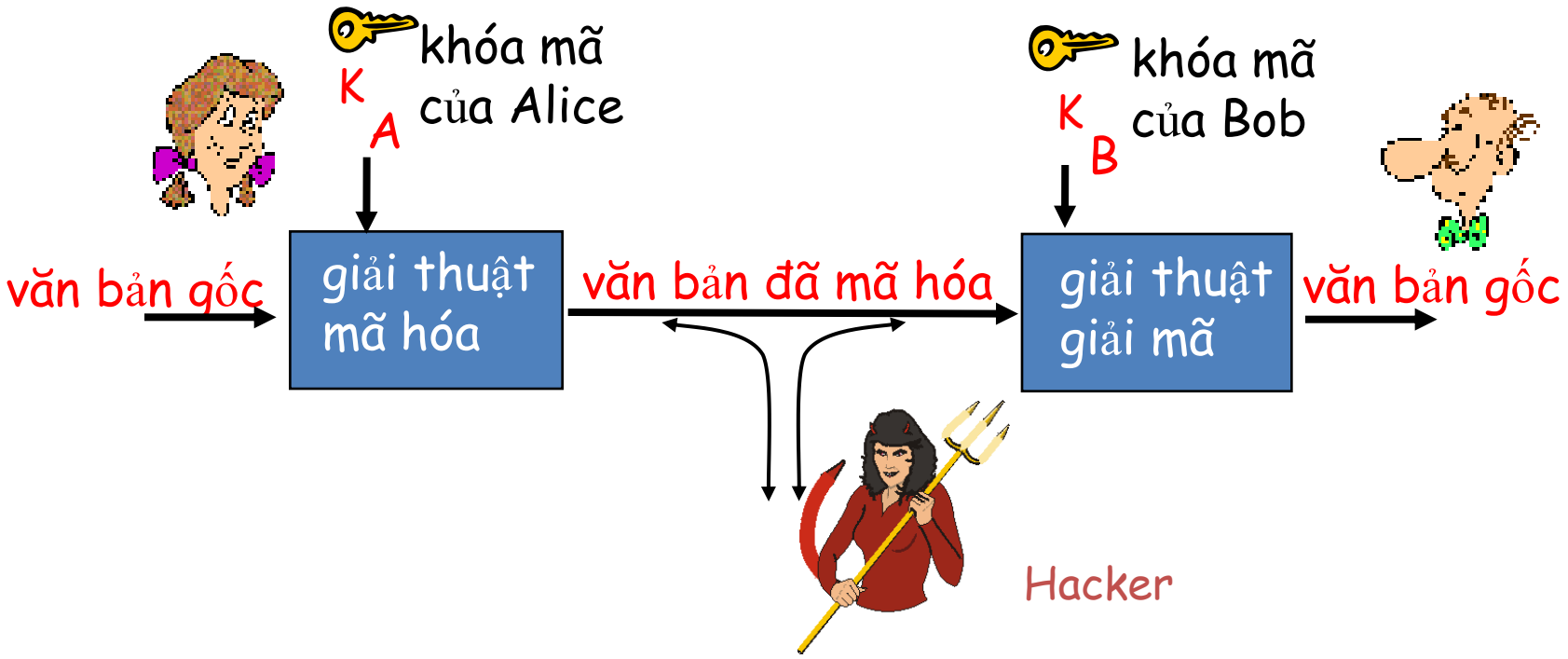
# Các đối tượng cần bảo mật

- Trình duyệt Web/server cho các giao dịch điện tử
- Client/Server ngân hàng trực tuyến
- DNS servers
- Các router trao đổi thông tin cập nhật bảng routing
- .v.v.

# Kẻ xấu có thể làm những việc gì?

- *nghe lén:* ngăn chặn các thông điệp
- kích hoạt *chèn* các thông điệp vào trong kết nối
- *giả danh:* có thể giả mạo địa chỉ nguồn trong gói (hoặc bất kỳ trường nào trong đó)
- *cướp:* "tiếp tục" kết nối hiện hành nhưng thay người gửi hoặc người nhận bằng chính họ
- *từ chối dịch vụ:* dịch vụ hiện tại bị người khác dùng (đồng nghĩa quá tải)
- .v.v.

# Các nguyên lý mã hóa



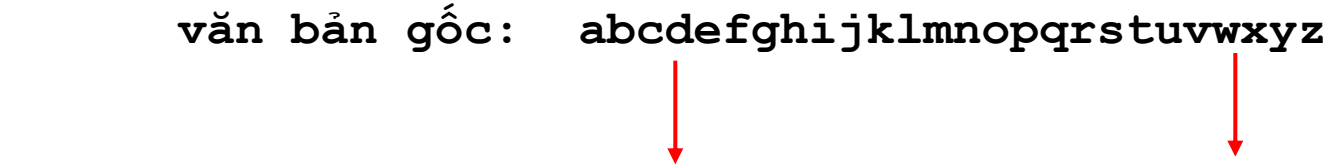

khóa đối xứng: khóa bên gửi và bên nhận giống nhau

khóa công cộng: khóa mã chung, khóa giải mã bí mật (riêng)

# Mã hóa khóa đối xứng

mật mã thay thế: thay thứ này thành thứ khác

– mã hóa ký tự đơn: thay thế từng ký tự một




ví dụ: văn bản gốc: Bob. i love you. Alice

mã hóa thành: nko. s gktc wky. mgsbc

- Bẻ khóa kiểu mã hóa đơn giản này dễ không?
  - ❑ brute force (khó như thế nào?)
  - ❑ khác?

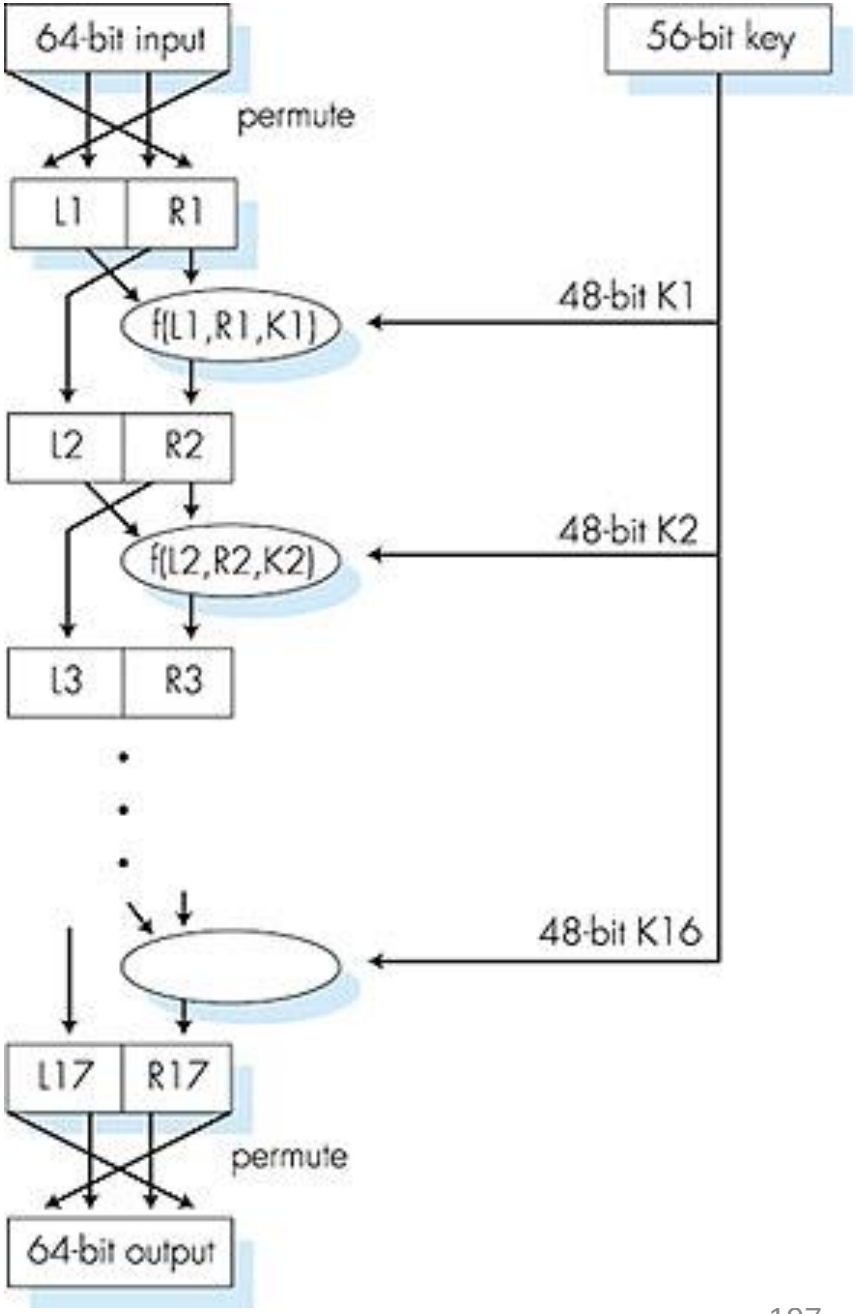
# Mã hóa khóa đối xứng: DES

## DES: Data Encryption Standard

- Chuẩn mã hóa của Hoa Kỳ [NIST 1993]
- Khóa đối xứng 56-bit, văn bản gốc vào 64-bit
- Bảo mật trong DES như thế nào?
  - chưa có cách tiếp cận "backdoor-cửa sau" để giải mã
- làm cho DES bảo mật hơn:
  - dùng 3 khóa tuần tự (3-DES) trong mỗi datum
  - dùng cơ chế liên kết khối mã

# Mã hóa khóa đối xứng: DES

DES hoạt động



# AES: Advanced Encryption Standard

- Chuẩn NIST khóa đối xứng mới (tháng 11-2001) thay thế cho DES
- Dữ liệu xử lý từng khối 128 bit
- Các khóa 128, 192 hoặc 256 bit
- Giải mã brute force (thử sai) tốn 1s với DES, tốn 149 tỷ tỷ năm với AES

# Mã hóa khóa công cộng

*khóa đối xứng*

- yêu cầu người gửi, người nhận phải biết khóa công cộng
- Làm sao biết khóa công cộng đó trong lần đầu tiên (đặc biệt với những người chưa bao giờ gặp trước)?

Mã hóa khóa công cộng

- tiếp cận khác hoàn toàn
- người gửi, người nhận không chia sẻ khóa công cộng
- khóa công cộng cho mọi người đều biết
- khóa giải mã riêng chỉ có người nhận biết

# Giải thuật mã hóa khóa công cộng

Yêu cầu:

1. cần $K_B^+(.)$ và $K_B^-(.)$ như sau:

$$K_B^-(K_B^+(m)) = m$$

2. cho khóa công cộng $K_B^+$, phải không thể tính toán ra được khóa riêng $K_B^-$

giải thuật RSA: Rivest, Shamir, Adelson

# Sự chứng thực

Mục tiêu: Bob muốn Alice "chứng thực" nhân dạng của cô đối với anh ta

Mô tả cách thức hiện thực: Alice nói "Tôi là Alice"

Thất bại sẽ xảy ra??

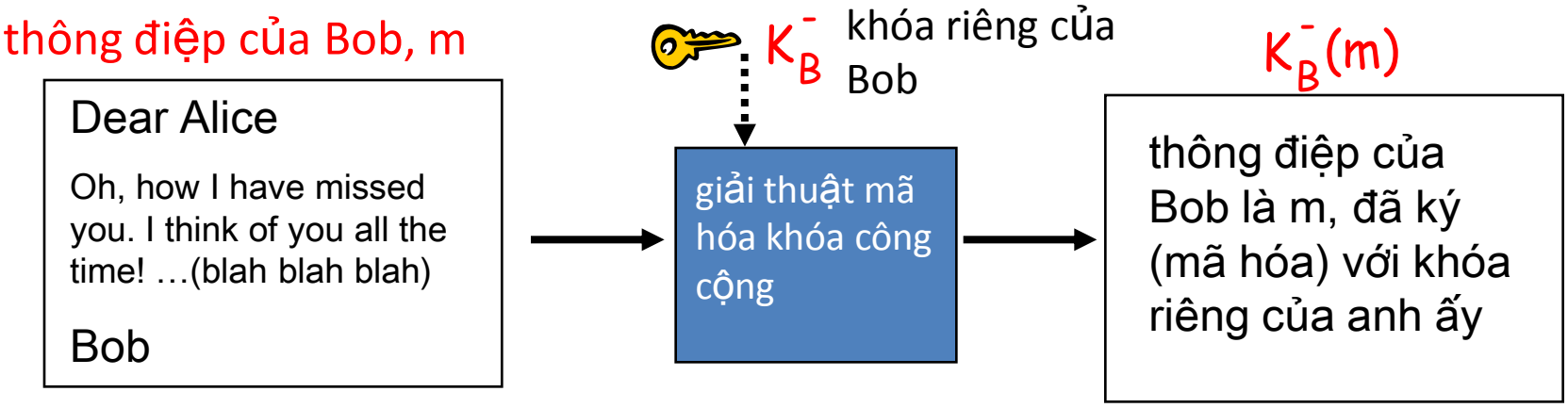
# Sự toàn vẹn

- Chữ ký số: Kỹ thuật mã hóa tương tự như các chữ ký bằng tay.
  - người gửi (Bob) đánh dấu (số hóa) tài liệu, thiết lập thuộc tính là người sở hữu/tạo lập tài liệu.
  - có thể kiểm tra, không thể làm giả: người nhận (Alice) có thể chứng thực với người khác là chỉ có Bob chứ ngoài ra không có ai (kể cả Alice) đã ký trên tài liệu đó.

# Chữ ký số

## Chữ ký số đơn giản cho thông điệp m:

- Bob ký m bằng cách mã hóa với khóa riêng của anh ấy $K_B^-$, tạo thống điệp "đã được ký", $K_B^-(m)$



# Chữ ký số (tt)

- Giả sử Alice nhận được m, với chữ ký số hóa là $K_B(m)$
- Alice kiểm tra m đã được ký bởi Bob bằng cách áp dụng khóa công cộng của Bob là $K_B$ cho $K_B(m)$ sau đó kiểm tra $K_B(K_B(m)) = m$.
- Nếu $K_B(K_B(m)) = m$, bất cứ ai đã ký m phải dùng khóa riêng của Bob

Alice kiểm tra:

- ✓ Bob đã ký m.
- ✓ Không có ai khác đã ký m.
- ✓ Bob đã ký m và không ký m'.

Không thể phủ nhận:

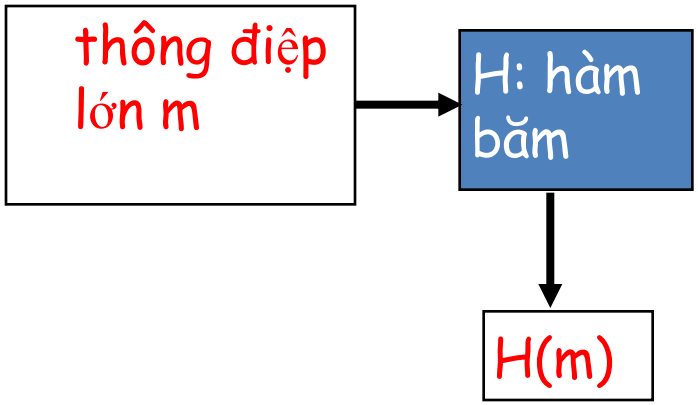
- ✓ Alice có thể giữ m và chữ ký $K_B(m)$ để chứng thực rằng Bob đã ký m.

# Phân loại thông điệp

Tính toán các thông điệp dài có chi phí đắt

Mục tiêu: "dấu tay" số hóa có kích thước cố định, dễ tính toán được

- áp dụng hàm băm H vào m, tính được phân loại thông điệp kích thước cố định, *H(m).*




Các đặc tính hàm băm:

- nhiều-một
- sinh ra phân loại thông điệp kích thước cố định ("dấu tay")
- cho phân loại thông điệp x, không thể tính toán để tìm m dùng x = H(m)

# Khóa phân bố và chứng chỉ

Vấn đề khóa đối xứng:

- Làm thế nào 2 thực thể cùng thiết lập khóa bí mật trên mạng?

Giải pháp:

- Trung tâm phân bố khóa (key distribution center-KDC) được tin cậy – hoạt động trung gian giữa các thực thể

Vấn đề khóa công cộng:

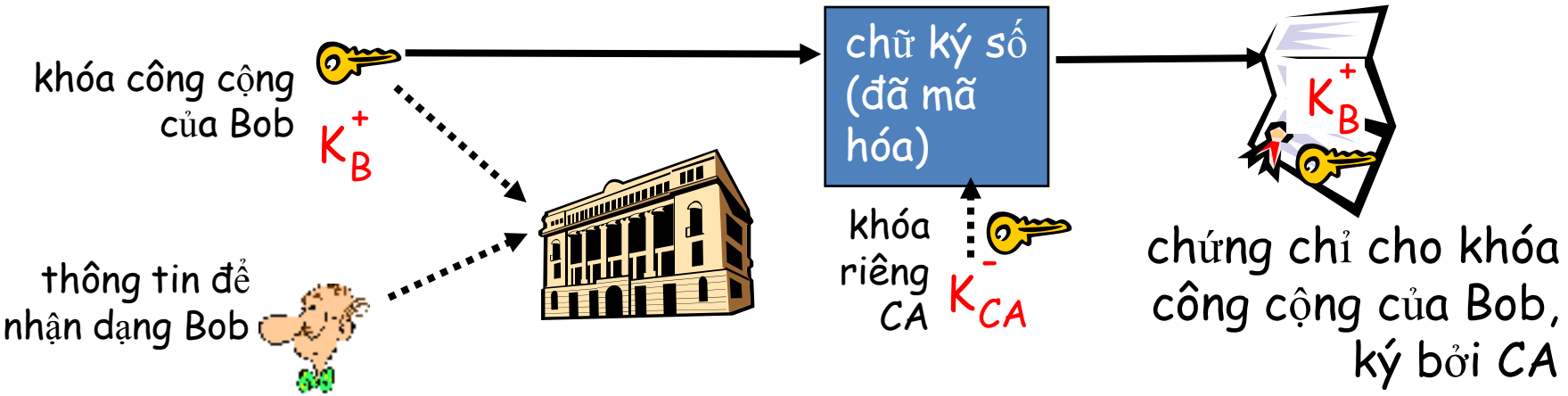
- Khi Alice lấy được khóa công cộng của Bob (từ web site, email, đĩa) làm sao biết khóa công cộng của Bob chứ không phải của Hacker?

Giải pháp:

- nơi cấp chứng chỉ (certification authority-CA) được tin cậy

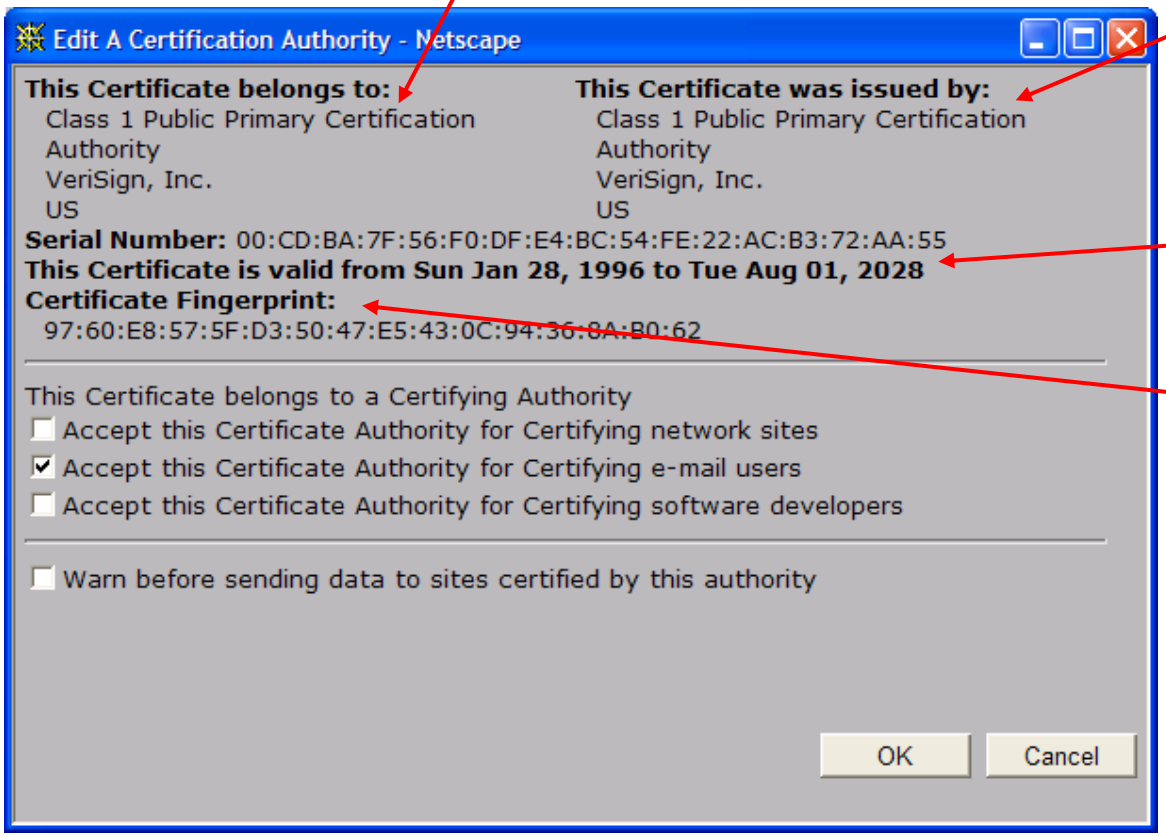
# Cấp chứng chỉ

- Certification authority (CA): gắn kết khóa công cộng với thực thể E nào đó.
- E (người, router) đăng ký khóa công cộng của họ với CA.
  - E cung cấp "bằng chứng để nhận dạng" cho CA.
  - CA tạo ra chứng chỉ ràng buộc E với khóa công cộng của nó.
  - chứng chỉ chứa khóa công cộng của E được ký số bởi CA – CA nói "đây là khóa công cộng của E"



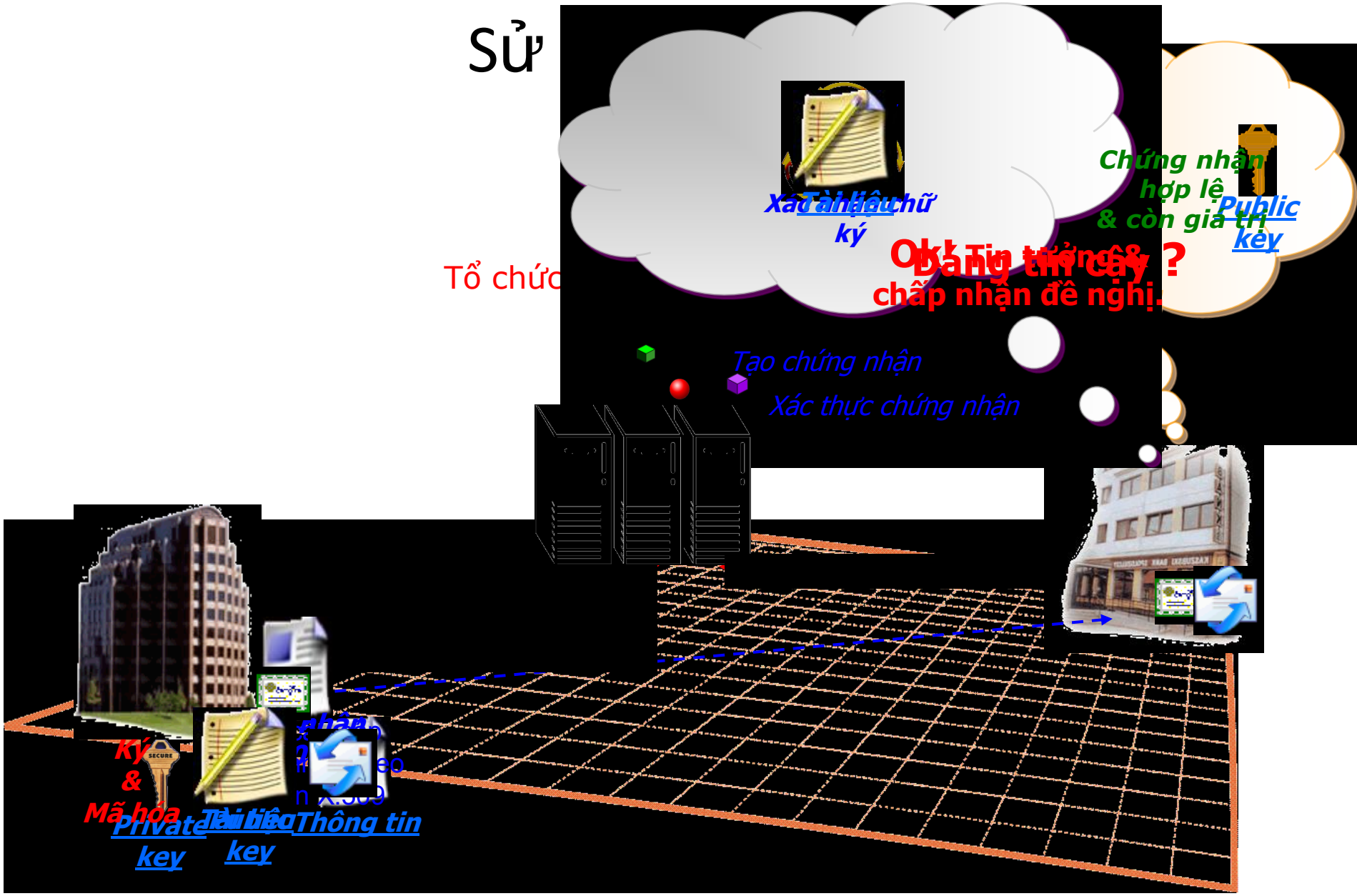
# Mô tả chứng chỉ

- Số thứ tự (duy nhất)
- thông tin về người sở hữu chứng chỉ, bao gồm giải thuật và chính giá trị khóa (không hiển thị ra)

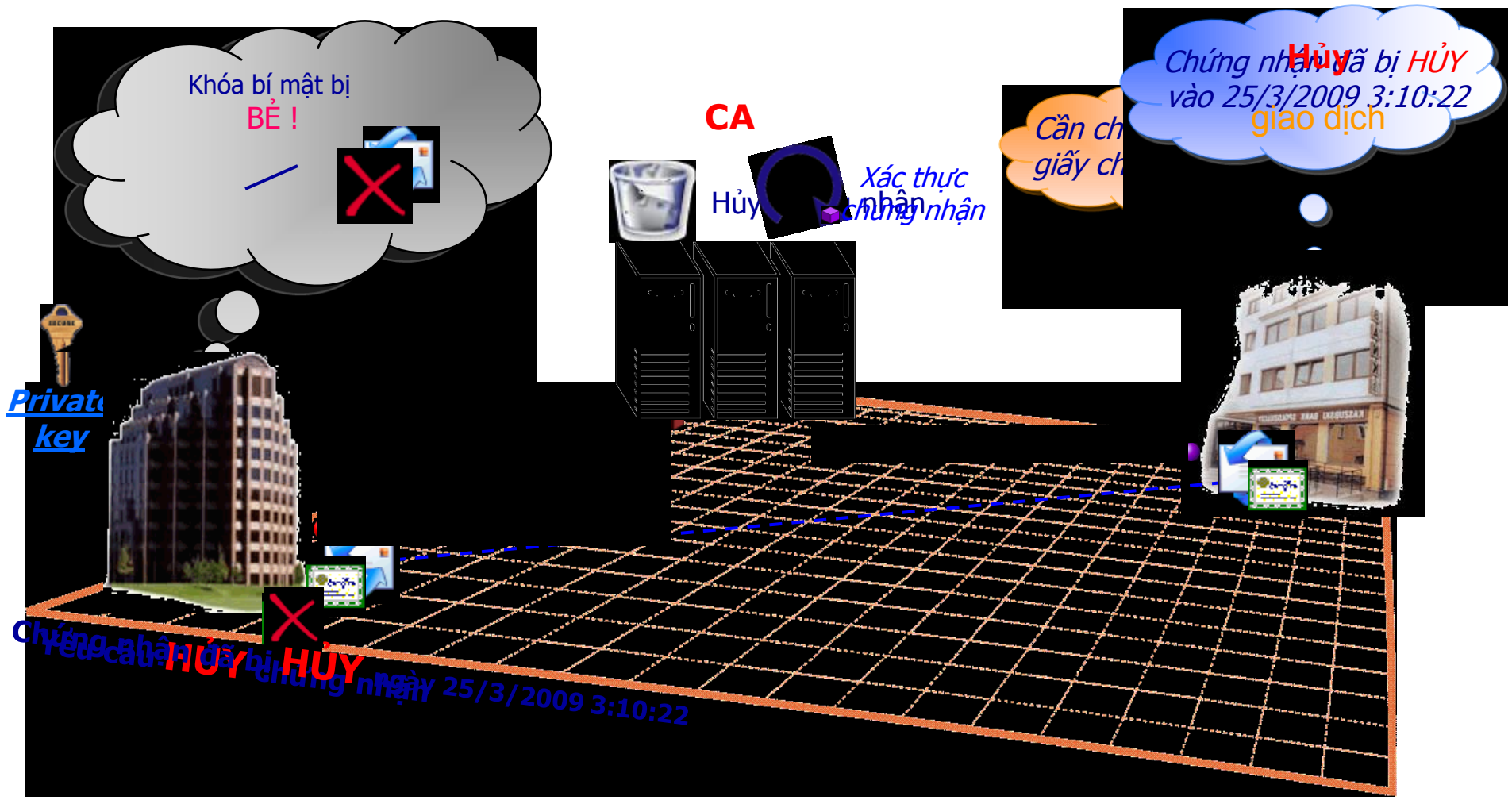



- thông tin về người phát hành chứng chỉ
- ngày kiểm tra tính hợp lệ
- chữ ký số bởi người phát hành chứng chỉ

# Sử


Tổ chức
Xác nhận chữ ký
Chứng nhận hợp lệ & còn giá trị
Public key
Ok! Tin tưởng & chấp nhận đề nghị.
Bảng thi cây ?
Tạo chứng nhận
Xác thực chứng nhận
Ký & Mã hóa
Private key
Thông tin

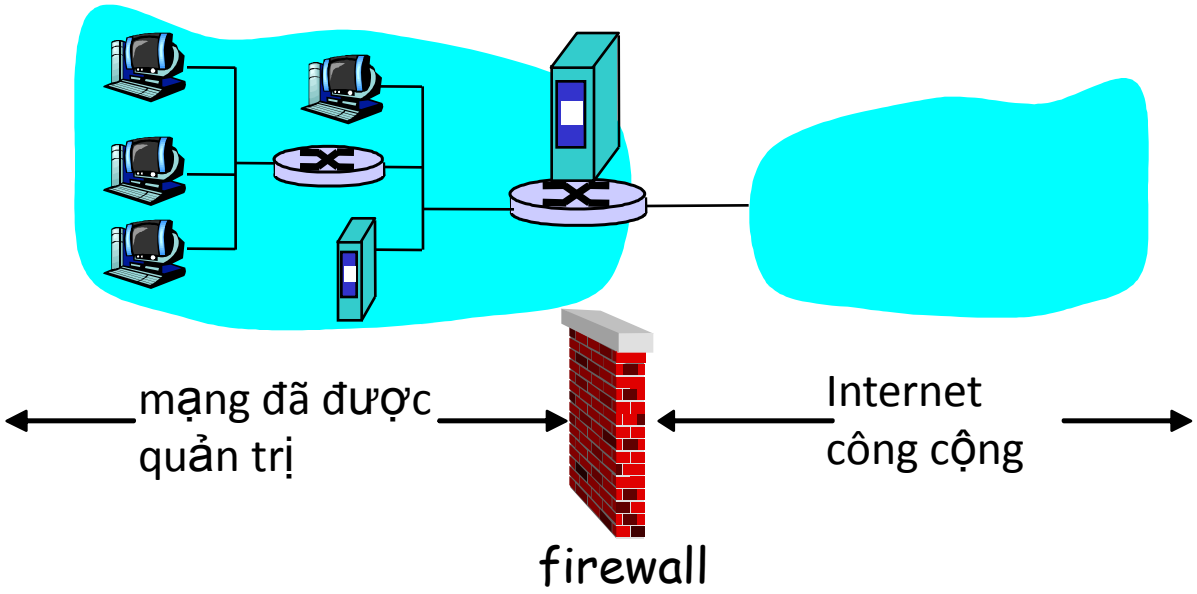
# Sử dụng chứng chỉ



# Các Firewall-Tường lửa

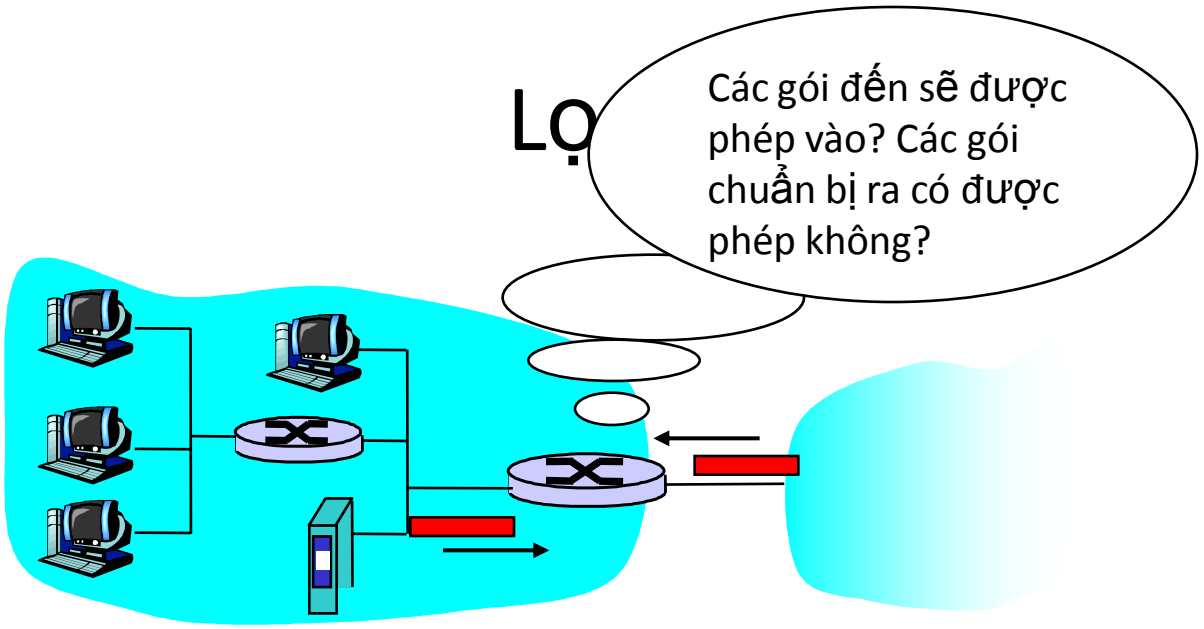
**firewall**

cô lập mạng nội bộ của tổ chức với Internet, cho phép một số gói được truyền qua, ngăn chặn các gói khác



# Firewall: Tại sao phải dùng?

- Ngăn chặn các cuộc tấn công từ chối dịch vụ Denial Of Service (DoS):
  - SYN flooding: kẻ tấn công thiết lập nhiều kết nối TCP "ảo", không còn tài nguyên cho các kết nối "thật"
- Ngăn chặn việc sửa đổi/truy cập bất hợp pháp các dữ liệu nội bộ.
  - Ví dụ: kẻ tấn công thay thế trang chủ của CIA bằng trang nào đó
- Chỉ cho phép các truy cập hợp pháp vào bên trong mạng (tập hợp các host/user được chứng thực)
- 2 kiểu firewall:
  - mức ứng dụng
  - lọc gói tin



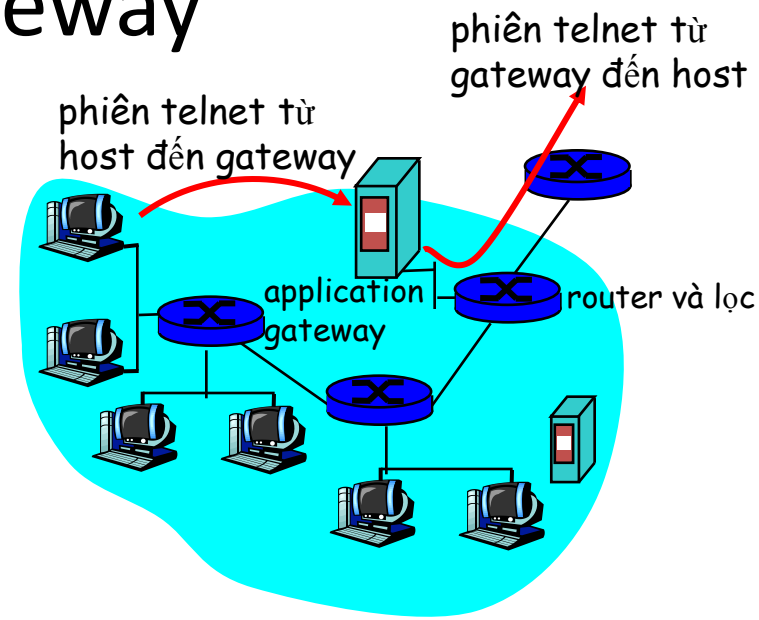

- mạng nội bộ kết nối với Internet thông qua router firewall
- router lọc từng gói một, xác định chuyển tiếp hoặc bỏ các gói dựa trên:
  - địa chỉ IP nguồn, địa chỉ IP đích
  - các số hiệu port TCP/UDP nguồn và đích
  - kiểu thông điệp ICMP
  - các bit TCP SYN và ACK

# Lọc gói tin

- Ví dụ 1: chặn các datagram đến và đi với trường giao thức IP = 17 và port nguồn hoặc đích = 23.
  - Tất cả các dòng UDP đến/đi và các kết nối telnet đều bị chặn lại.
- Ví dụ 2: chặn các đoạn Block TCP với ACK=0.
  - Ngăn chặn các client bên ngoài tạo các kết nối TCP với các client bên trong, nhưng cho phép các client bên trong kết nối ra ngoài.

# Các ứng dụng gateway

- Lọc các gói trên dữ liệu ứng dụng cũng như các trường IP/TCP/UDP.
- Ví dụ: cho phép chọn các user bên trong được telnet ra ngoài.




1. yêu cầu tất cả các user phải telnet thông qua gateway
2. với các user đã được cấp phép, gateway thiết lập kết nối với host đích. gateway tiếp vận dữ liệu giữa 2 kết nối.
3. Router lọc và chặn tất cả các kết nối telnet không xuất phát từ gateway.

# Các hạn chế của các firewall và gateway

- giả mạo IP: router không thể biết dữ liệu có thực sự đến từ nguồn tin cậy hay không
- nếu nhiều ứng dụng cần đối xử đặc biệt, mỗi cái sở hữu gateway riêng…
- phần mềm client phải biết cách tiếp xúc với gateway.
  - ví dụ: phải thiết lập địa chỉ IP của proxy trong trình duyệt Web
- các lọc thường dùng tất cả hoặc không có chính sách nào dành cho UDP
- sự cân bằng: mức độ truyền thông với bên ngoài và sự an toàn
- nhiều site bảo vệ mức cao vẫn phải chịu đựng sự tấn công

# Các loại tấn công và cách phòng chống

Phương thức:

- Trước khi tấn công: hacker tìm hiểu các dịch vụ đã hiện thực/hoạt động trên mạng
- Dùng `ping` để xác định các host nào có địa chỉ trên mạng
- Quét port: liên tục thử thiết lập các kết nối TCP với mỗi port (xem thử chuyện gì xảy ra)

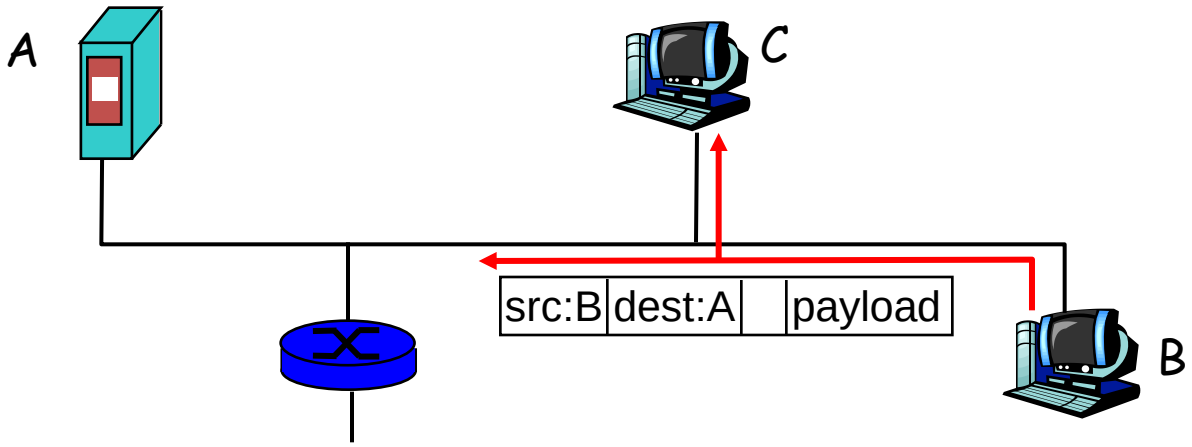
Biện pháp đối phó?

- Ghi nhận lưu thông vào mạng
- Quan tâm các hành vi nghi ngờ (các địa chỉ IP, port bị quét liên tục)

# Các mối đe dọa bảo mật Internet

## Packet sniffing: Nghe ngóng gói

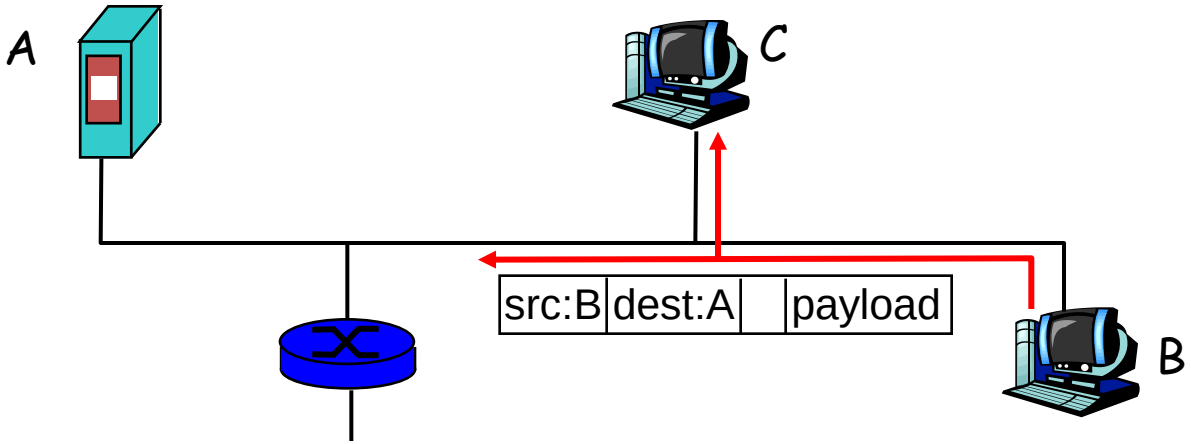
- NIC promiscuous (hỗn tạp) đọc tất cả các gói chuyển qua nó
- Có thể đọc tất cả các dữ liệu được mã hóa (như mật khẩu)
- Ví dụ: C nghe ngóng các gói của B



# Các mối đe dọa bảo mật Internet

## Packet sniffing: Biện pháp đối phó

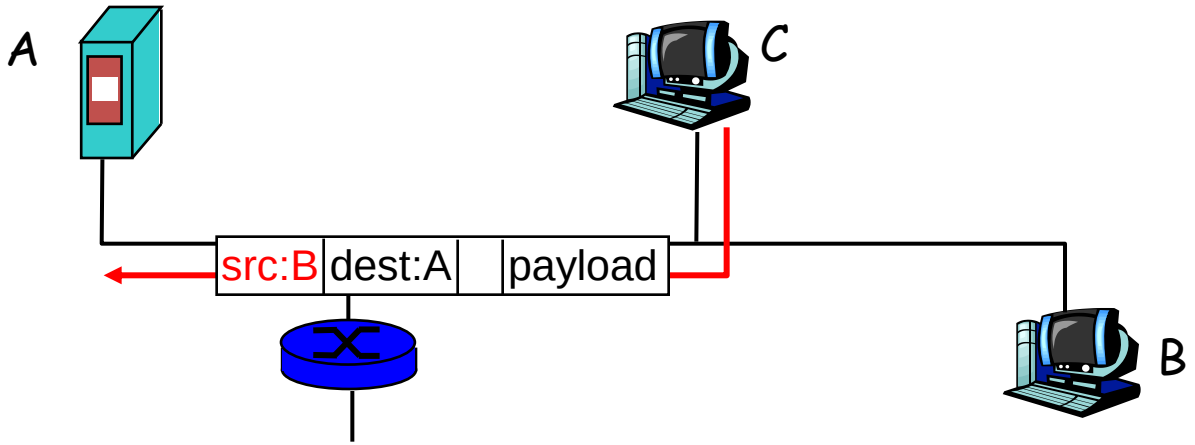
- Tất cả các host trong tổ chức chạy phần mềm kiểm tra định kỳ xem host có ở chế độ promiscuous
- 1 host mỗi đoạn của phương tiện truyền thông



# Các mối đe dọa bảo mật Internet

## IP Spoofing (giả mạo IP):

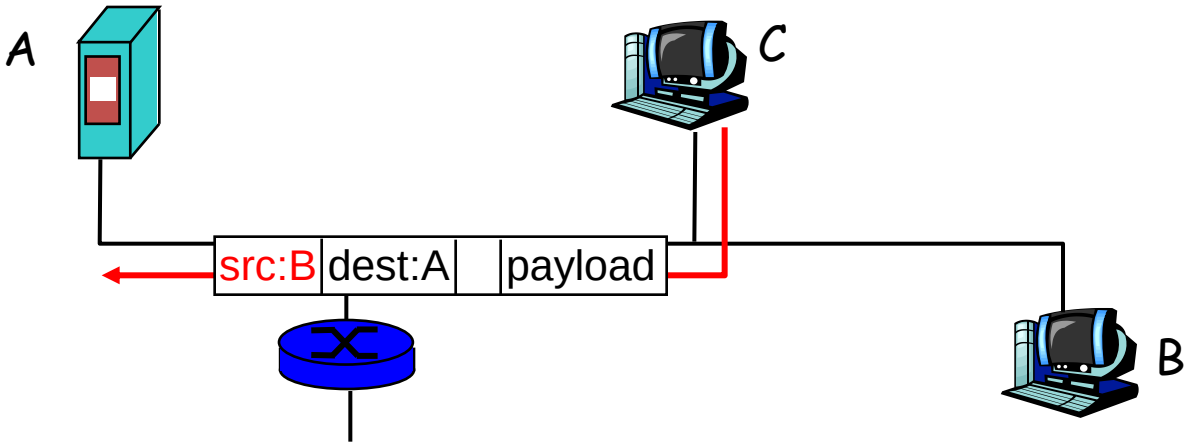
- Có thể sinh ra các gói IP "thô" trực tiếp từ ứng dụng, gán giá trị bất kỳ vào trường địa chỉ IP nguồn
- Bên nhận không thể xác định nguồn bị giả mạo
- Ví dụ: C giả mạo là B



# Các mối đe dọa bảo mật Internet

## IP Spoofing: lọc quyền vào

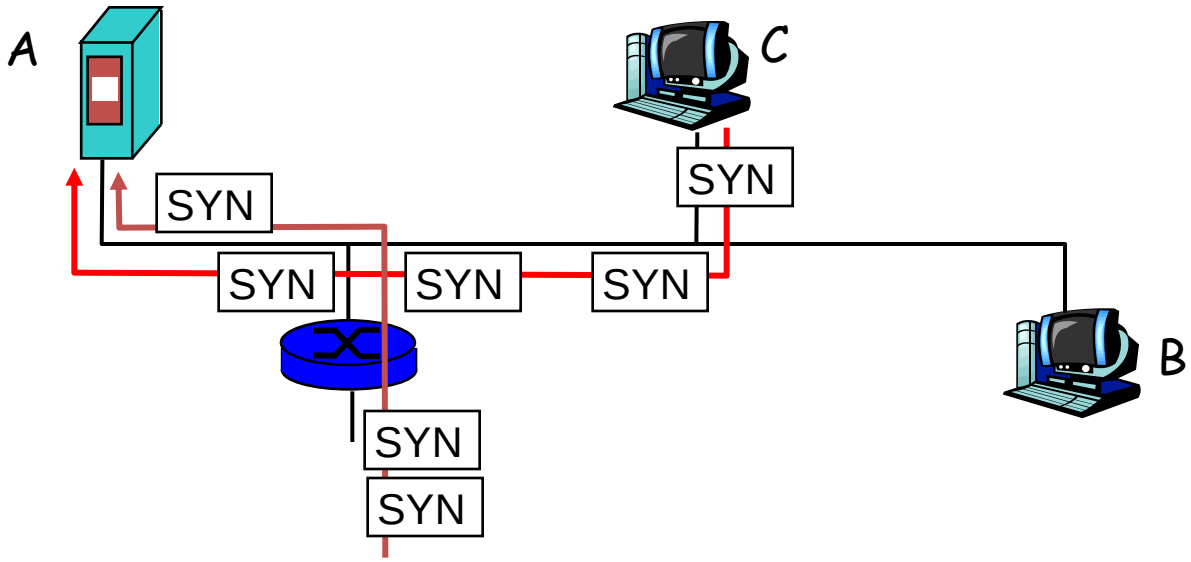
- Router sẽ không chuyển tiếp các gói đi với trường hợp các địa chỉ nguồn không hợp lệ
- Tuyệt vời, nhưng lọc như thế không thể áp dụng cho tất cả các mạng



# Các mối đe dọa bảo mật Internet

## Denial of Service (DoS):

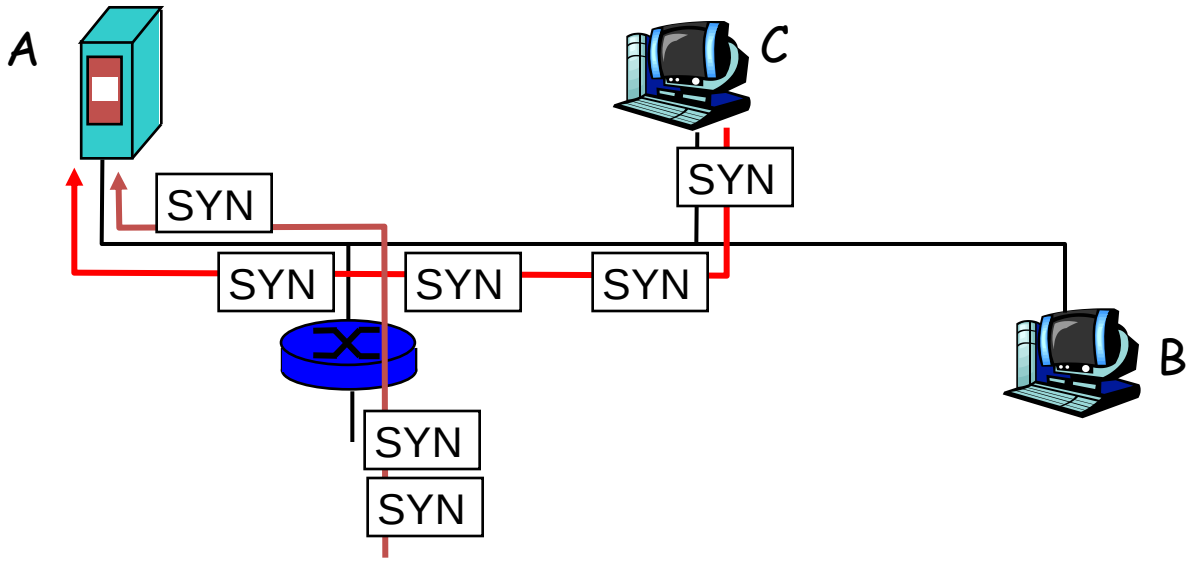
- Gây ra "ngập lụt" bằng các gói sinh ra bởi ý đồ xấu cho bên nhận
- Distributed DOS (DDoS): nhiều nguồn phối hợp làm "ngập lụt" bên nhận
- Ví dụ: C và các host ở xa tấn công SYN A



# Các mối đe dọa bảo mật Internet

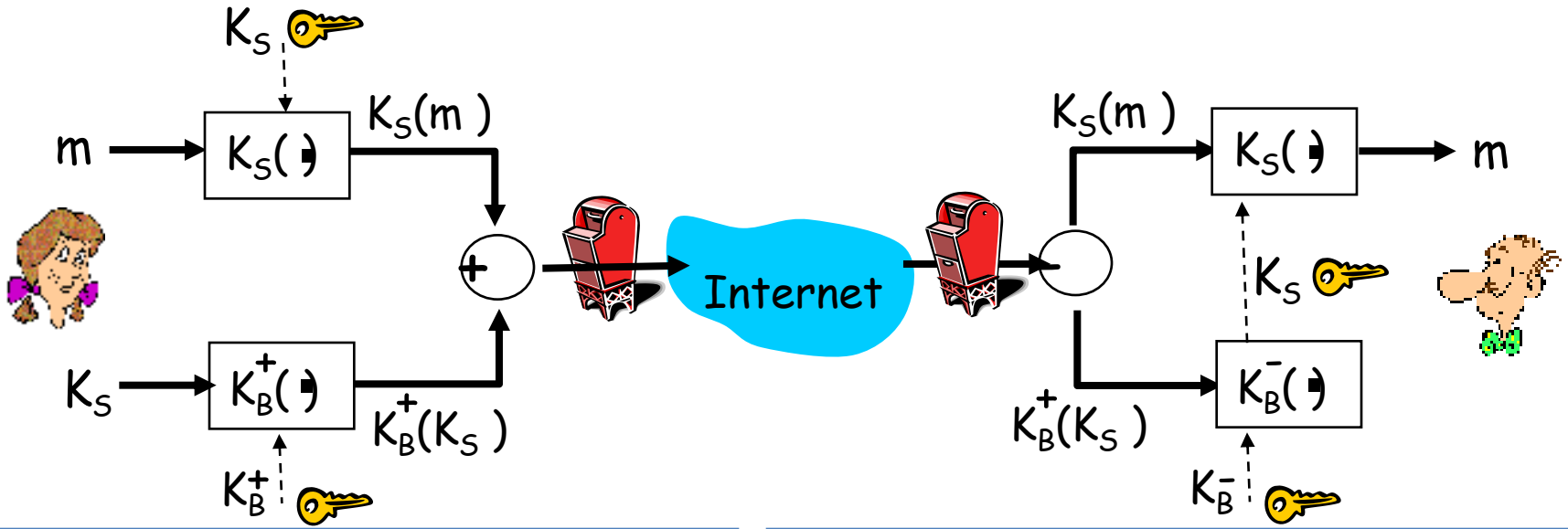
## Denial of Service (DoS): Biện pháp đối phó?

- Lọc ra trước các gói dùng làm "ngập lụt" (ví dụ: SYN)
- Theo dõi ngược lại nguồn gây ra "ngập lụt" (cơ chế giống máy phát hiện nói dối của Mỹ)



# Bảo mật e-mail

- Alice muốn gửi 1 e-mail bí mật, m, đến Bob.




Alice:

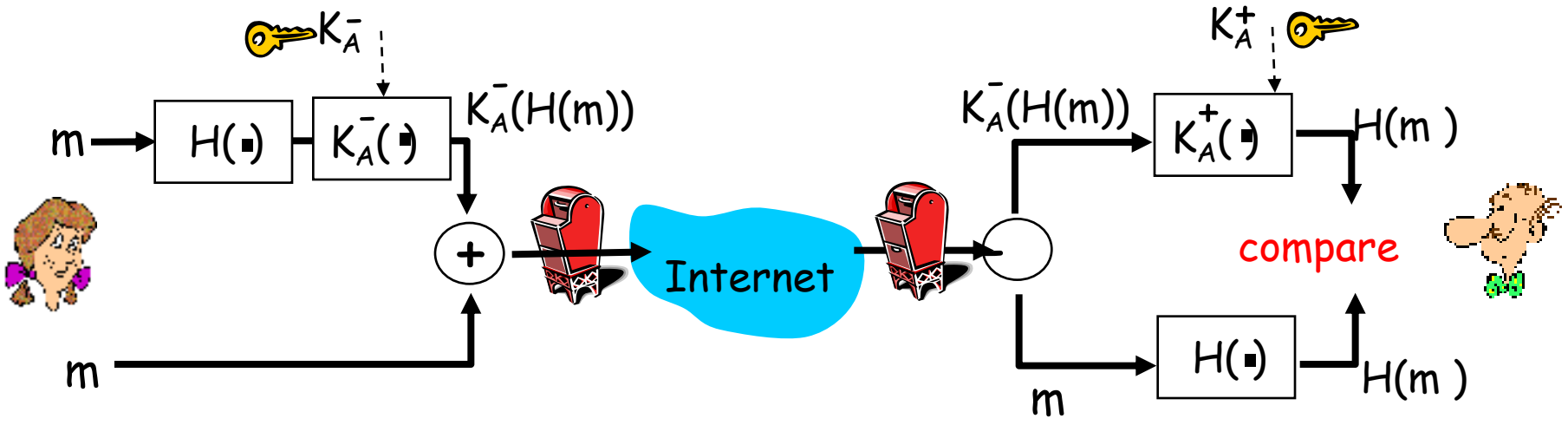
- sinh ra khóa riêng đối xứng ngẫu nhiên, $K_S$.
- mã hóa thông điệp với $K_S$
- cũng mã hóa $K_S$ với khóa công cộng của Bob.
- gửi cả $K_S(m)$ và $K_B(K_S)$ cho Bob.

Bob:

- dùng khóa riêng của anh ấy để giải mã và phục hồi $K_S$
- dùng $K_S$ để giải mã $K_S(m)$ và phục hồi m

# Bảo mật e-mail

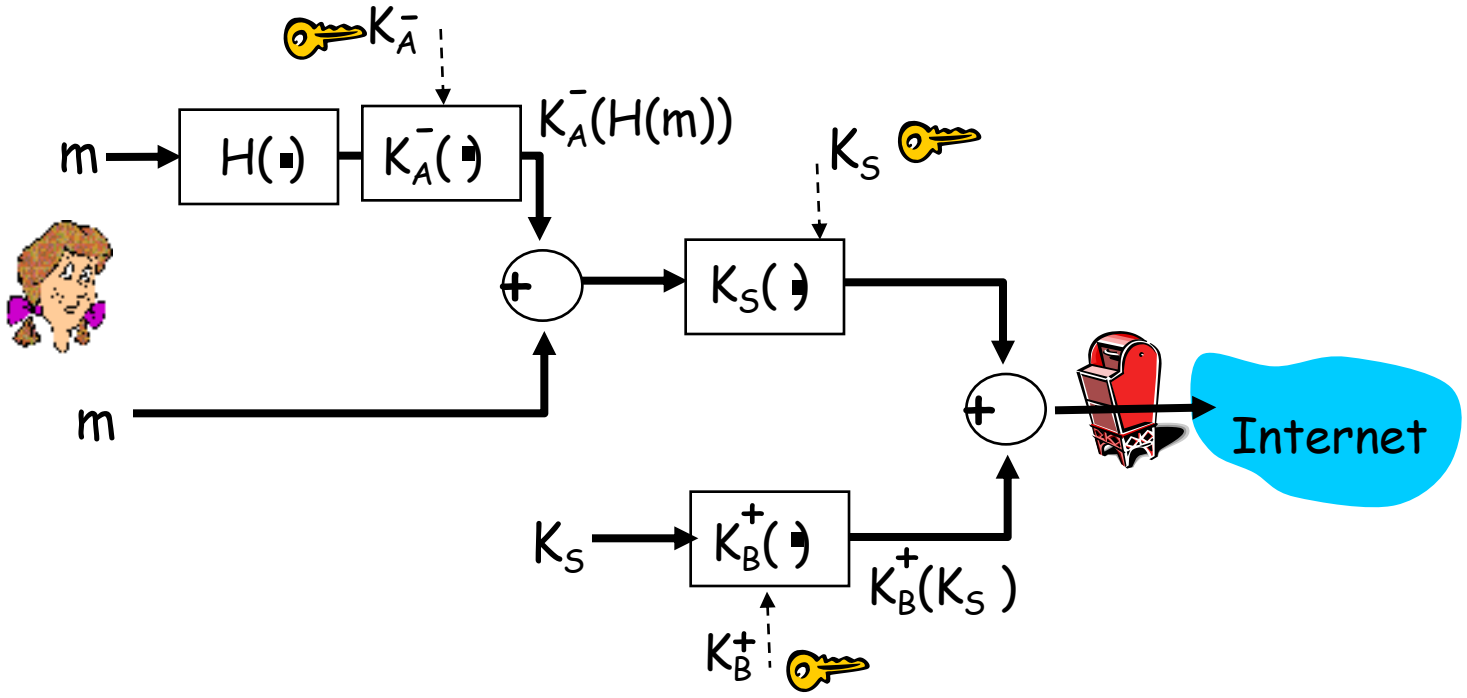
- Alice muốn cung cấp sự toàn vẹn thông điệp chứng thực người gửi.




- Alice ký số trên thông điệp.
- gửi cả thông điệp (dạng rõ ràng) và chữ ký số.

# Bảo mật e-mail

- Alice muốn cung cấp sự toàn vẹn thông điệp chứng thực người gửi → sự bí mật




Alice dùng 3 khóa: khóa riêng của cô ấy, khóa công cộng của Bob, khóa đối xứng vừa mới tạo

# Pretty good privacy (PGP)

- Chuẩn trên thực tế để mã hóa email Internet.
- Dùng mã hóa khóa đối xứng, khóa công cộng, hàm băm và chữ ký số như đã trình bày ở trước.
- Hỗ trợ đồng nhất, chứng thực người gửi, bí mật
- Người phát minh: Phil Zimmerman.

Một thông điệp đã được ký bằng PGP

```
---BEGIN PGP SIGNED MESSAGE---
Hash: SHA1

Bob:My husband is out of town
   tonight.Passionately yours, A

---BEGIN PGP SIGNATURE---
Version: PGP 5.0
Charset: noconv
yhHJRHhGJGhgg/12EpJ+lo8gE4vB3mqJ
   hFEvZP9t6n7G6m5Gw2
---END PGP SIGNATURE---
```

# Secure sockets layer (SSL)

- Bảo mật lớp transport với bất kỳ ứng dụng nào dựa trên TCP dùng các dịch vụ SSL
- Dùng giữa trình duyệt Web, các server trong thương mại điện tử
- Các dịch vụ bảo mật:
  - Chứng thực server
  - Mã hóa dữ liệu
  - Chứng thực client (tùy chọn)

- Chứng thực server:
  - Trình duyệt cho phép SSL chứa các khóa công cộng cho các CA được tin cậy
  - Trình duyệt yêu cầu chứng chỉ server, phát ra bởi CA được tin cậy
  - Trình duyệt dùng khóa công cộng của CA để trích ra khóa công cộng của server từ chứng chỉ
- Kiểm tra trong trình duyệt của bạn để thấy các CA được tin cậy

# SSL (tt)

Mã hóa phiên làm việc SSL :

- Trình duyệt sinh ra *khóa phiên đối xứng*, mã hóa nó với khóa công cộng của server, gửi khóa (đã mã hóa) cho server.
- Dùng khóa riêng, server giải mã khóa phiên
- Trình duyệt, server biết khóa phiên
  - Tất cả dữ liệu gửi vào trong TCP socket (do client hoặc server) được mã hóa bởi khóa phiên.

- SSL: cơ sở của IETF Transport Layer Security (TLS).
- SSL có thể dùng cho các ứng dụng không Web, như IMAP.
- Chứng thực client có thể hoàn thành với các chứng chỉ client

# IPSec: bảo mật lớp Network

- Bảo mật lớp Network:
  - host gửi mã hóa dữ liệu trong IP datagram
  - các đoạn TCP & UDP; các thông điệp ICMP & SNMP.
- Chứng thực lớp Network:
  - host đích có thể chứng thực địa chỉ IP nguồn
- 2 giao thức cơ bản:
  - authentication header (AH)
  - encapsulation security payload (ESP)
- Với cả AH và ESP, nguồn – đích bắt tay nhau:
  - tạo kênh logic lớp network gọi là một security association (SA)
- Mỗi SA theo 1 chiều duy nhất
- duy nhất xác định bởi:
  - giao thức bảo mật (AH hoặc ESP)
  - địa chỉ IP nguồn
  - ID của kết nối 32-bit

# Giao thức AH

- Hỗ trợ chứng thực nguồn, toàn vẹn dữ liệu, không tin cậy
- AH header được chèn vào giữa IP header, trường dữ liệu.
- Trường giao thức: 51
- Trung gian xử lý các datagram như bình thường

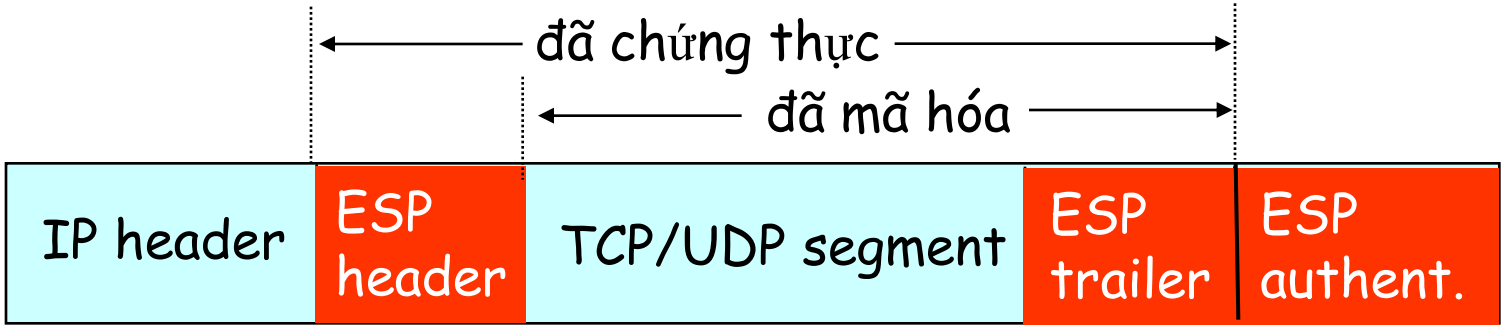
AH header chứa:

- Nhận dạng kết nối
- Dữ liệu chứng thực: thông điệp đã được ký từ nguồn được tính toán dựa trên IP datagram gốc
- Trường header kế tiếp: xác định kiểu của dữ liệu (vd: TCP, UDP, ICMP)

# Giao thức ESP

- Hỗ trợ toàn vẹn dữ liệu, chứng thực host, tính bí mật
- Mã hóa dữ liệu, ESP trailer
- Trường header kế tiếp nằm trong ESP trailer.

- Trường chứng thực ESP tương tự như của AH
- Protocol = 50.



# Bảo mật IEEE 802.11

- *Khảo sát:*
  - 85% việc sử dụng mà không có mã hóa/chứng thực
  - Dễ dàng bị phát hiện/nghe ngóng và nhiều loại tấn công khác!
- Bảo mật 802.11
  - Mã hóa, chứng thực
  - Thử nghiệm bảo mật 802.11 đầu tiên là Wired Equivalent Privacy (WEP): có thiếu sót
  - Thử nghiệm hiện tại: 802.11i

# Wired Equivalent Privacy (WEP):

- Chứng thực như trong giao thức *ap4.0*
  - host yêu cầu chứng thực từ access point
  - access point gửi 128 bit
  - host mã hóa dùng khóa đối xứng chia sẻ
  - access point giải mã, chứng thực host
- Không có cơ chế phân bố khóa
- Chứng thực: chỉ cần biết khóa chia sẻ

# Wi-Fi Protected Access (WPA)

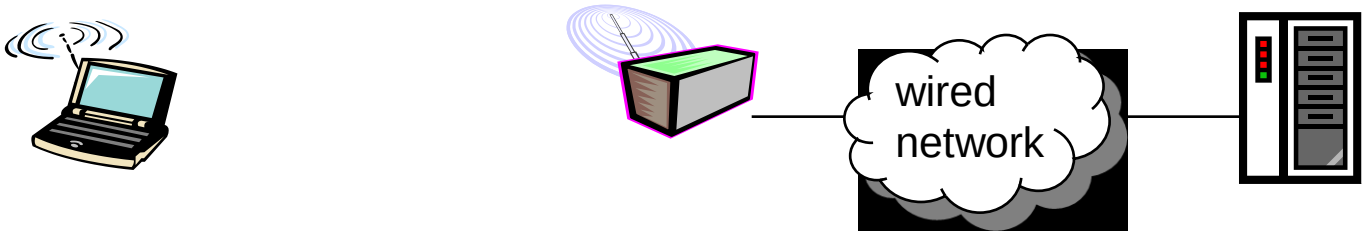
- Hai sự cải tiến chính so với WEP:
  - Mã hóa dữ liệu cải tiến thông qua giao thức Temporal Key Integrity Protocol (TKIP). TKIP scrambles key sử dụng thuật toán hashing và bằng đặc tính kiểm tra số nguyên, đảm bảo rằng Key sẽ không bị giả mạo.
  - Chứng thực người dùng, thông qua EAP.
- WPA là tiêu chuẩn tạm thời mà sẽ được thay thế với chuẩn IEEE 802.11i

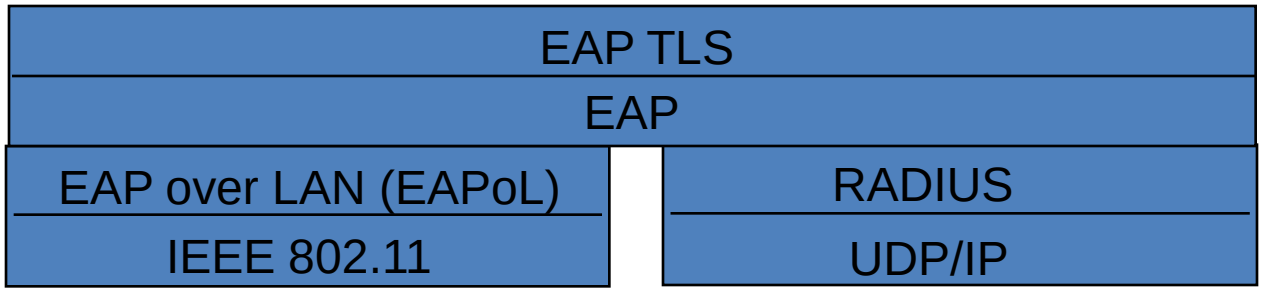
# 802.11i: cải tiến sự bảo mật

- Rất nhiều (và chắc chắn hơn) dạng mã hóa có thể
- Hỗ trợ phân bố khóa
- Dùng chứng thực server tách riêng khỏi AP

# EAP: Extensible Authentication Protocol

- EAP được gửi trên các "link" riêng biệt
  - mobile-đến-AP (EAP trên LAN)
  - AP đến server chứng thực (RADIUS trên UDP)



# TÀI LIỆU THAM KHẢO, ĐỊA CHỈ LIÊN LẠC


- Giáo trình Mạng máy tính, KS. Nguyễn Bình Dương, TS. Đàm Quang Hồng Hải
- Giáo trình hệ thống Mạng máy tính CCNA, Nguyễn Hồng Sơn
- CCNA: Cisco Certified Network Associate – Study Guide, Todde Lammle - 2007
- Computer Networking: A Top Down Approach Featuring the Internet, 3rd edition. Jim Kurose, Keith Ross. 2004.
- Computer Networks, 4th edition. Andrew S. Tanenbaum. 2003


- Địa chỉ liên lạc: Trần Bá Nhiệm – Khoa Mạng máy tính & Truyền thông – ĐH CNTT – 34 Trương Định, Q3, Tp.HCM. Email: tranbanhiem@yahoo.com

# Giáo trình nhập môn mạng máy tính

# MỤC LỤC

**Chương I Những khái niệm cơ bản của mạng máy tính ...6**

**I.** Định nghĩa mạng máy tính ..... 6

**II.** Phân loại mạng máy tính ..... 7

**II.1.** Dựa theo vị trí địa lý ..... 7

**II.2.** Dựa theo cấu trúc mạng ..... 7

II.2.1 Kiểu điểm - điểm (point - to - point) ..... 7

II.2.2 Kiểu khuyếch tán ..... 8

**II.3.** Dựa theo phương pháp chuyển mạch ..... 8

II.3.1 Mạng chuyển mạch kênh (Line switching network) ..... 8

II.3.2 Mạng chuyển mạch thông điệp (Message switching network) ..... 8

II.3.3 Mạng chuyển mạch gói (Packet switching network) ..... 9

**III.** So sánh giữa mạng cục bộ và mạng diện rộng ..... 9

**IV.** Các thành phần của mạng máy tính ..... 11

**IV.1.** Một số bộ giao thức kết nối mạng ..... 11

**IV.2.** Hệ điều hành mạng - NOS (*Network Operating System)* ..... 11

**V.** Các lợi ích của mạng máy tính ..... 12

**V.1.** Mạng tạo khả năng dùng chung tài nguyên cho các người dùng. ..... 12

**V.2.** Mạng cho phép nâng cao độ tin cậy. ..... 13

**V.3.** Mạng giúp cho công việc đạt hiệu suất cao hơn. ..... 13

**V.4.** Tiết kiệm chi phí. ..... 13

**V.5.** Tăng cường tính bảo mật thông tin. ..... 13

**V.6.** Việc phát triển mạng máy tính đã tạo ra nhiều ứng dụng mới ..... 13

**VI.** Các dịch vụ phổ biến trên mạng máy tính ..... 13

**Chương II Mô hình truyền thông .....15**

**I.** Sự cần thiết phải có mô hình truyền thông ..... 15

**II.** Các nhu cầu về chuẩn hóa đối với mạng ..... 16

**III.** Mô hình OSI (Open Systems Interconnection) ..... 17

**III.1.** Nguyên tắc sử dụng khi định nghĩa các tầng hệ thống mở ..... 17

**III.2.** Các giao thức trong mô hình OSI ..... 18

**III.3.** Các chức năng chủ yếu của các tầng của mô hình OSI. ..... 19

III.3.1 Tầng 1: Vật lý (Physical) ..... 19

III.3.2 Tầng 2: Liên kết dữ liệu (Data link) ..... 20

III.3.3 Tầng 3: Mạng (Network) ..... 20
III.3.4 Tầng 4: Vận chuyển (Transport) ..... 22
III.3.5 Tầng 5: Giao dịch (Session) ..... 23
III.3.6 Tầng 6: Trình bày (Presentation) ..... 23
III.3.7 Tầng 7: Ứng dụng (Application) ..... 24
IV. Quá trình chuyển vận gói tin ..... 24
IV.1. Quá trình đóng gói dữ liệu (tại máy gửi) ..... 24
IV.2. Quá trình truyền dữ liệu từ máy gửi đến máy nhận. ..... 26
IV.3. Chi tiết quá trình xử lý tại máy nhận ..... 26
V. Phương thức truyền tín hiệu ..... 27
VI. Mô hình TCP/IP ..... 27
VI.1. Tổng quan về bộ giao thức TCP/IP ..... 27
VI.2. So sánh TCP/IP với OSI ..... 29
VII. Các giao thức truy cập đường truyền trên mạng LAN ..... 30
VII.1. Giao thức chuyển mạch (yêu cầu và chấp nhận) ..... 30
VII.2. Giao thức đường dây đa truy cập với cảm nhận va chạm ..... 30
VII.3. Giao thức dùng thẻ bài vòng (Token ring) ..... 31
VII.4. Giao thức dung thẻ bài cho dạng đường thẳng (Token bus) ..... 31
VIII. Các phương tiện kết nối mạng liên khu vực (WAN) ..... 31
**Chương III Địa chỉ IP ..... 33**
I. Giao thức TCP/IP ..... 33
II. Địa chỉ IP ..... 33
II.1. Tổng quát ..... 33
II.2. Cấu trúc của các địa chỉ IP ..... 33
III. Một số khái niệm và thuật ngữ liên quan ..... 37
III.1. Các giao thức trong mạng IP ..... 38
III.2. Các bước hoạt động của giao thức IP ..... 38
IV. Giao thức điều khiển truyền dữ liệu TCP ..... 39
IV.1. Các bước thực hiện để thiết lập một liên kết TCP/IP: ..... 40
IV.2. Các bước thực hiện khi truyền và nhận dữ liệu ..... 41
IV.3. Các bước thực hiện khi đóng một liên kết ..... 42
IV.4. Một số hàm khác của TCP ..... 42
V. Giao thức UDP (User Datagram Protocol) ..... 44
VI. Địa chỉ IPv4 ..... 46

**VI.1.** Thành phần và hình dạng của địa chỉ IP ..... 46
**VI.2.** Các lớp địa chỉ IP ..... 46
**VII.** IPv6 ..... 48
**VII.1.** Giao thức liên mạng thế hệ mới (IPv6) ..... 48
**VII.2.** Một số đặc điểm mới của IPv6: ..... 48
**VII.3.** Kiến trúc địa chỉ trong IPv6: ..... 49
VII.3.1 Không gian địa chỉ: ..... 49
VII.3.2 Cú pháp địa chỉ: ..... 50
**Chương IV Thiết bị mạng ..... 51**
**I.** Môi trường truyền dẫn ..... 51
**I.1.** Khái niệm ..... 51
**I.2.** Tần số truyền thông ..... 51
**I.3.** Các đặc tính của phương tiện truyền dẫn ..... 51
**I.4.** Các kiểu truyền dẫn. ..... 52
**II.** Đường cáp truyền mạng ..... 52
**II.1.** Cáp xoắn cặp ..... 52
**II.2.** Cáp đồng trục ..... 53
**II.3.** Cáp sợi quang (Fiber - Optic Cable) ..... 54
**II.4.** Các yêu cầu cho một hệ thống cáp ..... 54
**III.** Đường truyền vô tuyến ..... 55
**III.1.** Sóng vô tuyến (radio) ..... 55
**III.2.** Sóng viba ..... 55
**III.3.** Hồng ngoại ..... 55
**IV.** Các kỹ thuật bấm cáp mạng ..... 56
**V.** Các thiết bị liên kết mạng ..... 57
**V.1.** Repeater (Bộ tiếp sức) ..... 57
**V.2.** Bridge (Cầu nối) ..... 58
**V.3.** Router (Bộ tìm đường) ..... 61
V.3.1 Các phương thức hoạt động của Router ..... 64
V.3.2 Một số giao thức hoạt động chính của Router ..... 64
**V.4.** Gateway (cổng nối) ..... 64
**V.5.** Hub (Bộ tập trung) ..... 65
**V.6.** Bộ chuyển mạch (*switch*) ..... 66
**Chương V Mô hình mạng ..... 67**

I. Kiến trúc mạng (Topology) ..... 67
II. Những cấu trúc chính của mạng cục bộ ..... 67
II.1. Dạng đường thẳng (Bus) ..... 67
II.2. Dạng vòng tròn (Ring) ..... 68
II.3. Dạng hình sao (Star) ..... 68
II.4. Mạng dạng kết hợp ..... 70
Chương VI Các dịch vụ của mạng diện rộng (WAN) ..... 71
I. Mạng chuyển mạch (Circuit Swiching Network) ..... 71
II. Mạng thuê bao (Leased line Network) ..... 73
III. Mạng chuyển gói tin (Packet Switching NetWork) ..... 74
IV. Mạng X25 ..... 75
V. Mạng Frame Relay ..... 76
VI. Mạng ATM (Cell relay) ..... 76
Chương VII CÁC DỊCH VỤ MẠNG THÔNG DỤNG ..... 78
I. DỊCH VỤ WEB ..... 78
I.1. Một số thuật ngữ cơ bản. ..... 78
I.2. Giới thiệu mô hình hoạt động của Web. ..... 80
II. DỊCH VỤ FTP ..... 81
II.1. Mô hình hoạt động của FTP ..... 81
II.2. Tập hợp các lệnh FTP ..... 81
III. E-MAIL. ..... 83
III.1. Mô hình hoạt động ..... 83
III.2. Các loại mail. ..... 83
III.3. Sử dụng WebMail. ..... 83

# Chương I Những khái niệm cơ bản của mạng máy tính

Mạng máy tính ngày nay đã phát triển một cách nhanh chóng và đa dạng. Hệ điều hành cùng các ứng dụng của mạng ngày càng phong phú, các lợi ích của mạng ngày càng được khẳng định. Mạng máy tính bao gồm rất nhiều loại, nhiều mô hình triển khai. Trong một mạng máy tính lại có nhiều thành phần cấu thành. Trước khi đi chi tiết về mạng máy tính, chúng ta sẽ tìm hiểu các khái niệm cơ bản của mạng máy tính.

## I. Định nghĩa mạng máy tính

*Mạng máy tính là một tập hợp các máy tính được nối với nhau bởi đường truyền theo một cấu trúc nào đó và thông qua đó các máy tính trao đổi thông tin qua lại với nhau.*

Đường truyền là hệ thống các thiết bị truyền dẫn có dây hay không dây dùng để chuyển các tín hiệu điện tử từ máy tính này đến máy tính khác. Các tín hiệu điện tử đó biểu thị các giá trị dữ liệu dưới dạng các xung nhị phân (on - off). Tất cả các tín hiệu được truyền giữa các máy tính đều thuộc một dạng sóng điện từ. Tùy theo tần số của sóng điện từ có thể dùng các đường truyền vật lý khác nhau để truyền các tín hiệu. Ở đây đường truyền được kết nối có thể là dây cáp đồng trục, cáp xoắn, cáp quang, dây điện thoại, sóng vô tuyến ... Các đường truyền dữ liệu tạo nên cấu trúc của mạng.

Hình I-1 Mạng máy tính

Với sự trao đổi qua lại giữa máy tính này với máy tính khác đã phân biệt mạng máy tính với các hệ thống thu phát một chiều như truyền hình, phát thông tin từ vệ tinh xuống các trạm thu thụ động... vì tại đây chỉ có thông tin một chiều từ nơi phát đến nơi thu mà không quan tâm đến có bao nhiêu nơi thu, có thu tốt hay không.

Đặc trưng cơ bản của đường truyền vật lý là giải thông. Giải thông của một đường chuyền chính là độ đo phạm vi tần số mà nó có thể đáp ứng được. Tốc độ truyền dữ liệu trên đường truyền còn được gọi là thông lượng của đường truyền - thường được tính bằng số lượng bit được truyền đi trong một giây (Bps). Thông lượng còn được đo bằng đơn vị khác là Baud (lấy từ tên nhà bác học - Emile Baudot). Baud biểu thị số lượng thay đổi tín hiệu trong một giây.

Ở đây Baud và Bps không phải bao giờ cũng đồng nhất. Ví dụ: nếu trên đường dây có 8 mức tín hiệu khác nhau thì mỗi mức tín hiệu tương ứng với 3 bit hay là 1 Baud tương ứng với 3 bit. Chỉ khi có 2 mức tín hiệu trong đó mỗi mức tín hiệu tương ứng với 1 bit thì 1 Baud mới tương ứng với 1 bit.

# II. Phân loại mạng máy tính

Có nhiều cách để phân biệt mạng máy tính nhưng người ta thường phân biệt mạng máy tính theo vị trí địa lý, cấu trúc mạng, phương pháp chuyển mạch.

## II.1. Dựa theo vị trí địa lý

Dựa vào phạm vi phân bổ của mạng người ta có thể phân ra các loại mạng như sau:

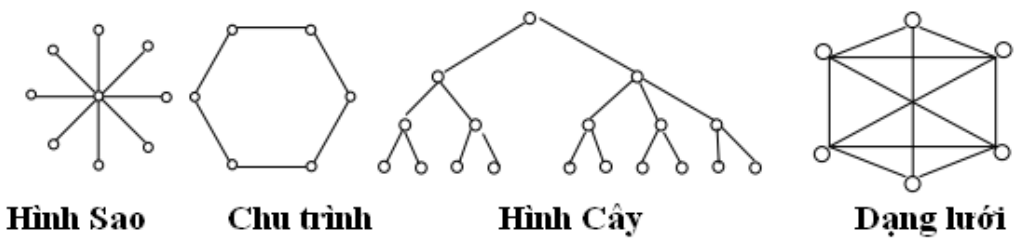
- **GAN (Global Area Network)** - Kết nối máy tính từ các châu lục khác nhau. Thông thường kết nối này được thực hiện thông qua mạng viễn thông và vệ tinh.
- **WAN (Wide Area Network)** - Mạng diện rộng, kết nối máy tính trong nội bộ các quốc gia hay giữa các quốc gia trong cùng một châu lục. Thông thường kết nối này được thực hiện thông qua mạng viễn thông. Các WAN có thể được kết nối với nhau thành GAN hay tự nó đã là GAN.
- **MAN (Metropolitan Area Network)** - Kết nối các máy tính trong phạm vi một thành phố hay giữa các thành phố với nhau.
- **LAN (Local Area Network)** - Mạng cục bộ, kết nối các máy tính trong một khu vực bán kính hẹp thông thường khoảng vài trăm mét. Kết nối được thực hiện thông qua các môi trường truyền thông tốc độ cao ví dụ cáp đồng trục thay cáp quang. LAN thường được sử dụng trong nội bộ một cơ quan/tổ chức... Các LAN có thể được kết nối với nhau thành WAN.

Trong các khái niệm nói trên, thường được sử dụng nhất hiện này là khái niệm Mạng diện rộng WAN và mạng cục bộ LAN.

## II.2. Dựa theo cấu trúc mạng

### II.2.1 Kiểu điểm - điểm (point - to - point)

Đường truyền nối từng cặp nút mạng với nhau. Thông tin đi từ nút nguồn qua nút trung gian rồi gởi tiếp nếu đường truyền không bị bận. Do đó, còn có tên là mạng lưu trữ và chuyển tiếp (store and forward).




Hình I-2 Cấu trúc điểm – điểm

### II.2.2 Kiểu khuyếch tán

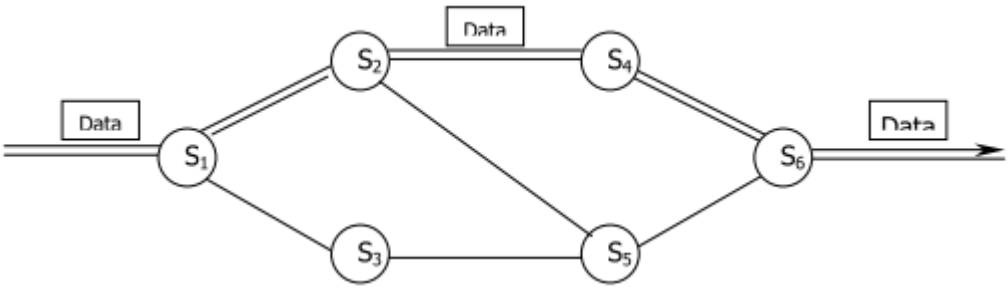
Bản tin được gởi đi từ một nút sẽ được tiếp nhận bởi các nút còn lại (còn gọi là broadcasting hay point to multipoint). Trong bản tin phải có vùng địa chỉ cho phép mỗi nút kiểm xem có phải tin của mình không và xử lý nếu đúng bản tin được gởi đến.

Hình I-3 Cấu trúc kiểu khuyếch tán

## II.3. Dựa theo phương pháp chuyển mạch

### II.3.1 Mạng chuyển mạch kênh (Line switching network)

Chuyển mạch kênh dùng trong mạng điện thoại. Một kênh cố định được thiết lập giữa cặp thực thể cần liên lạc với nhau. Mạng này có hiệu suất không cao vì có lúc kênh bỏ không.

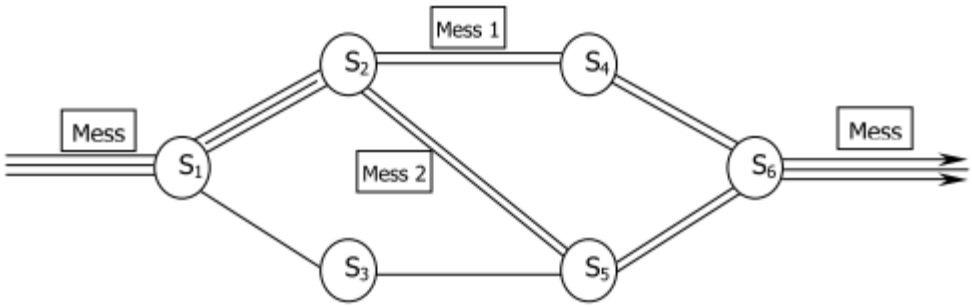



Hình I-4 Mạng chuyển mạch kênh

### II.3.2 Mạng chuyển mạch thông điệp (Message switching network)

Các nút của mạng căn cứ vào địa chỉ đích của "thông điệp" để chọn nút kế tiếp. Như vậy các nút cần lưu trữ và đọc tin nhận được, quản lý việc truyền tin. Trong trường hợp bản tin quá dài và nếu sai phải truyền lại. Phương pháp này giống như cách gởi thư thông thường.

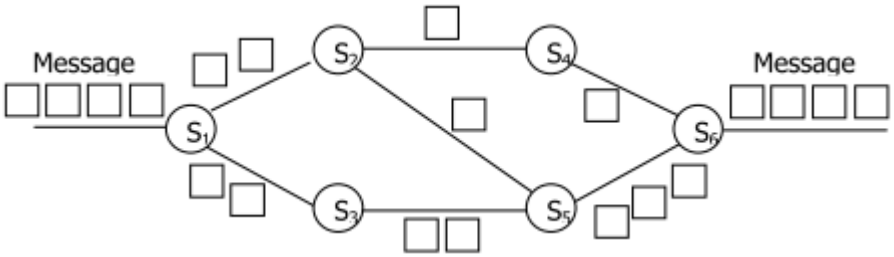
Mạng chuyển mạch thông báo thích hợp với các dịch vụ thông tin kiểu thư điện tử (Email) hơn là đối với các ứng dụng có tính thời gian thực vì tồn tại độ trễ nhất định do lưu trữ và xử lý thông tin điều khiển tại mỗi nút.




Hình I-5 Mạng chuyển mạch thông điệp

### II.3.3 Mạng chuyển mạch gói (Packet switching network)

Bản tin được chia thành nhiều gói tin (packet) có độ dài 512 bytes, phần đầu của gói tin thường là địa chỉ đích, mã để tập hợp các gói. Các gói tin của các thông điệp khác nhau có thể được truyền độc lập trên cùng một đường truyền. Vấn đề phức tạp ở đây là tạo lại bản tin ban đầu, đặc biệt là khi truyền trên các con đường khác nhau. Chuyển mạch gói mềm dẻo, hiệu suất cao. Sử dụng hai kĩ thuật chuyển mạch kênh và chuyển mạch gói trong cùng một mạng thống nhất gọi là mạng ISDN (Integrated Services Digital Network – Mạng thông tin số đa dịch vụ)




Hình I-6 Mạng chuyển mạch gói

## III. So sánh giữa mạng cục bộ và mạng diện rộng

Mạng cục bộ và mạng diện rộng có thể được phân biệt bởi: địa phương hoạt động, tốc độ đường truyền và tỷ lệ lỗi trên đường truyền, chủ quản của mạng, đường đi của thông tin trên mạng, dạng chuyển giao thông tin.

***Địa phương hoạt động***

Liên quan đến khu vực địa lý thì mạng cục bộ sẽ là mạng liên kết các máy tính nằm ở trong một khu vực nhỏ. Khu vực có thể bao gồm một tòa nhà hay là một khu nhà... Điều đó hạn chế bởi khoảng cách đường dây cáp được dùng để liên kết các máy tính của mạng cục bộ (Hạn chế đó còn là hạn chế của khả năng kỹ thuật của đường truyền dữ liệu). Ngược lại mạng diện rộng là mạng có khả năng liên kết các máy tính trong một vùng rộng lớn như là một thành phố, một miền, một đất nước, mạng diện rộng được xây dựng để nối hai hoặc nhiều khu vực địa lý riêng biệt.

***Tốc độ đường truyền và tỷ lệ lỗi trên đường truyền***

Do các đường cáp của mạng cục bộ đươc xây dựng trong một khu vực nhỏ cho nên nó ít bị ảnh hưởng bởi tác động của thiên nhiên (như là sấm chớp, ánh sáng...). Điều đó cho phép mạng cục bộ có thể truyền dữ liệu với tốc độ cao mà chỉ chịu một tỷ lệ lỗi nhỏ. Ngược lại với mạng diện rộng do phải truyền ở những khoảng cách khá xa với những đường truyền dẫn dài có khi lên tới hàng ngàn km. Do vậy mạng diện rộng không thể truyền với tốc độ quá cao vì khi đó tỉ lệ lỗi sẽ trở nên khó chấp nhận được.

Mạng cục bộ thường có tốc độ truyền dữ liệu từ 4 đến 16 Mbps và đạt tới 100 Mbps nếu dùng cáp quang. Còn phần lớn các mạng diện rộng cung cấp đường truyền có tốc độ thấp hơn nhiều như T1 với 1.544 Mbps hay E1 với 2.048 Mbps.

Đơn vị bps (Bit Per Second) là một đơn vị trong truyền thông tương đương với 1 bit được truyền trong một giây, ví dụ như tốc độ đường truyền là 1 Mbps tức là có thể truyền tối đa 1 Megabit trong 1 giây trên đường truyền đó.

Thông thường trong mạng cục bộ tỷ lệ lỗi trong truyền dữ liệu vào khoảng 1/107-108 còn trong mạng diện rộng thì tỷ lệ đó vào khoảng 1/106 - 107

### *Chủ quản và điều hành của mạng*

Do sự phức tạp trong việc xây dựng, quản lý, duy trì các đường truyền dẫn nên khi xây dựng mạng diện rộng người ta thường sử dụng các đường truyền được thuê từ các công ty viễn thông hay các nhà cung cấp dịch vụ truyền số liệu. Tùy theo cấu trúc của mạng những đường truyền đó thuộc cơ quan quản lý khác nhau như các nhà cung cấp đường truyền nội hạt, liên tỉnh, liên quốc gia. Các đường truyền đó phải tuân thủ các quy định của chính phủ các khu vực có đường dây đi qua như: tốc độ, việc mã hóa.

Còn đối với mạng cục bộ thì công việc đơn giản hơn nhiều, khi một cơ quan cài đặt mạng cục bộ thì toàn bộ mạng sẽ thuộc quyền quản lý của cơ quan đó.

### *Đường đi của thông tin trên mạng*

Trong mạng cục bộ thông tin được đi theo con đường xác định bởi cấu trúc của mạng. Khi người ta xác định cấu trúc của mạng thì thông tin sẽ luôn luôn đi theo cấu trúc đã xác định đó. Còn với mạng diện rộng dữ liệu cấu trúc có thể phức tạp hơn nhiều do việc sử dụng các dịch vụ truyền dữ liệu. Trong quá trình hoạt động các điểm nút có thể thay đổi đường đi của các thông tin khi phát hiện ra có trục trặc trên đường truyền hay khi phát hiện có quá nhiều thông tin cần truyền giữa hai điểm nút nào đó. Trên mạng diện rộng thông tin có thể có các con đường đi khác nhau, điều đó cho phép có thể sử dụng tối đa các năng lực của đường truyền hay nâng cao điều kiện an toàn trong truyền dữ liệu.

### *Dạng chuyển giao thông tin*

Phần lớn các mạng diện rộng hiện nay được phát triển cho việc truyền đồng thời trên đường truyền nhiều dạng thông tin khác nhau như: video, tiếng nói, dữ liệu... Trong khi đó các mạng cục bộ chủ yếu phát triển trong việc truyền dữ liệu thông thường. Điều này có thể giải thích do việc truyền các dạng thông tin như video, tiếng nói trong một khu vực nhỏ ít được quan tâm hơn như khi truyền qua những khoảng cách lớn.

Các hệ thống mạng hiện nay ngày càng phức tạp về chất lượng, đa dạng về chủng loại và phát triển rất nhanh về chất. Trong sự phát triển đó số lượng những nhà sản xuất từ phần mềm, phần cứng máy tính, các sản phẩm viễn thông cũng tăng nhanh với nhiều sản phẩm đa dạng. Chính vì vậy vai trò chuẩn hóa cũng mang những ý nghĩa quan trọng. Tại các nước các cơ quan chuẩn quốc gia đã đưa ra các những chuẩn về phần cứng và các quy định về giao tiếp nhằm giúp cho các nhà sản xuất có thể làm ra các sản phẩm có thể kết nối với các sản phẩm do hãng khác sản xuất.

# IV. Các thành phần của mạng máy tính

Mạng máy tính bao gồm các thiết bị phần cứng, các giao thức và các phần mềm mạng. Khi nghiên cứu về mạng máy tính, các vấn đề quan trọng cần được xem xét là giao thức mạng, cấu hình kết nối của mạng và các dịch vụ mạng.

## IV.1. Một số bộ giao thức kết nối mạng

1. TCP/IP

- Ưu thế chính của bộ giao thức này là khả năng liên kết hoạt động của nhiều loại máy tính khác nhau.
- TCP/IP đã trở thành tiêu chuẩn thực tế cho kết nối liên mạng cũng như kết nối Internet toàn cầu.

2. NetBEUI

- Bộ giao thức nhỏ, nhanh và hiệu quả được cung cấp theo các sản phẩm của hãng IBM, cũng như sự hỗ trợ của Microsoft.
- Bất lợi chính của bộ giao thức này là không hỗ trợ định tuyến và sử dụng giới hạn ở mạng dựa vào Microsoft.

3. IPX/SPX

- Đây là bộ giao thức sử dụng trong mạng Novell.
- Ưu thế: nhỏ, nhanh và hiệu quả trên các mạng cục bộ đồng thời hỗ trợ khả năng định tuyến.

4. DECnet

- Đây là bộ giao thức độc quyền của hãng Digital Equipment Corporation.
- DECnet định nghĩa mô hình truyền thông qua mạng LAN, mạng MAN và WAN. Hỗ trợ khả năng định tuyến

## IV.2. Hệ điều hành mạng - NOS (*Network Operating System)*

Cùng với sự nghiên cứu và phát triển mạng máy tính, hệ điều hành mạng đã được nhiều công ty đầu tư nghiên cứu và đã công bố nhiều phần mềm quản lý và điều hành mạng có hiệu quả như: *NetWare* của công ty NOVELL, LAN *Manager* của *Microsoft* dùng cho các máy *server* chạy hệ điều hành OS/2, LAN server của IBM (gần như đồng nhất với LAN *Manager*), *Vines* của *Banyan Systems* là hệ điều hành mạng dùng cho *server* chạy hệ điều hành UNIX, *Promise* LAN của *Mises Computer* chạy trên *card* điều hợp mạng độc quyền, *Windows for Workgroups* của *Microsoft*, LANtastic của *Artisoft, NetWare Lite* của *Novell*,....

Một trong những sự lựa chọn cơ bản mà ta phải quyết định trước là hệ điều hành mạng nào sẽ làm nền tảng cho mạng của ta, việc lựa chọn tuỳ thuộc vào kích cỡ của mạng hiện tại và

sự phát triển trong tương lai, còn tuỳ thuộc vào những ưu điểm và nhược điểm của từng hệ điều hành.

Một số hệ điều hành mạng phổ biến hiện nay:

- Hệ điều hành mạng UNIX: Đây là hệ điều hành do các nhà khoa học xây dựng và được dùng rất phổ biến trong giới khoa học, giáo dục. Hệ điều hành mạng UNIX là hệ điều hành đa nhiệm, đa người sử dụng, phục vụ cho truyền thông tốt. Nhược điểm của nó là hiện nay có nhiều *Version* khác nhau, không thống nhất gây khó khăn cho người sử dụng. Ngoài ra hệ điều hành này khá phức tạp lại đòi hỏi cấu hình máy mạnh (trước đây chạy trên máy *mini*, gần đây có SCO UNIX chạy trên máy vi tính với cấu hình mạnh).
- Hệ điều hành mạng *Windows* NT: Đây là hệ điều hành của hãng *Microsoft*, cũng là hệ điều hành đa nhiệm, đa người sử dụng. Đặc điểm của nó là tương đối dễ sử dụng, hỗ trợ mạnh cho phần mềm WINDOWS. Do hãng *Microsoft* là hãng phần mềm lớn nhất thế giới hiện nay, hệ điều hành này có khả năng sẽ được ngày càng phổ biến rộng rãi. Ngoài ra, *Windows* NT có thể liên kết tốt với máy chủ *Novell Netware*. Tuy nhiên, để chạy có hiệu quả, *Windows* NT cũng đòi hỏi cấu hình máy tương đối mạnh.
- Hệ điều hành mạng *Windows for Workgroup*: Đây là hệ điều hành mạng ngang hàng nhỏ, cho phép một nhóm người làm việc (khoảng 3-4 người) dùng chung ổ đĩa trên máy của nhau, dùng chung máy in nhưng không cho phép chạy chung một ứng dụng. Hệ dễ dàng cài đặt và cũng khá phổ biến.
- Hệ điều hành mạng *NetWare của Novell*: Đây là hệ điều hành phổ biến nhất hiện nay ở nước ta và trên thế giới trong thời gian cuối, nó có thể dùng cho các mạng nhỏ (khoảng từ 5-25 máy tính) và cũng có thể dùng cho các mạng lớn gồm hàng trăm máy tính. Trong những năm qua, *Novell* đã cho ra nhiều phiên bản của *Netware*: Netware 2.2, 3.11. 4.0 và hiện có 4.1. *Netware* là một hệ điều hành mạng cục bộ dùng cho các máy vi tính theo chuẩn của IBM hay các máy tính *Apple Macintosh*, chạy hệ điều hành MS-DOS hoặc OS/2.

  Hệ điều hành này tương đối gọn nhẹ, dễ cài đặt (máy chủ chỉ cần thậm chí AT386) do đó phù hợp với hoàn cảnh trang thiết bị hiện tại của nước ta. Ngoài ra, vì là một phần mềm phổ biến nên Novell Netware được các nhà sản xuất phần mềm khác hỗ trợ (theo nghĩa các phân mềm do các hãng phần mềm lớn trên thế giới làm đều có thể chạy tốt trên hệ điều hành mạng này).

# V. Các lợi ích của mạng máy tính

## V.1. Mạng tạo khả năng dùng chung tài nguyên cho các người dùng.

Vấn đề là làm cho các tài nguyên trên mạng như chương trình, dữ liệu và thiết bị, đặc biệt là các thiết bị đắt tiền, có thể sẵn dùng cho mọi người trên mạng mà không cần quan tâm đến vị trí thực của tài nguyên và người dùng.

Về mặt thiết bị, các thiết bị chất lượng cao thường đắt tiền, chúng thường được dùng chung cho nhiều người nhằm giảm chi phí và dễ bảo quản.

Về mặt chương trình và dữ liệu, khi được dùng chung, mỗi thay đổi sẽ sẵn dùng cho mọi thành viên trên mạng ngay lập tức. Điều này thể hiện rất rõ tại các nơi như ngân hàng, các đại lý bán vé máy bay...

### V.2. Mạng cho phép nâng cao độ tin cậy.

Khi sử dụng mạng, có thể thực hiện một chương trình tại nhiều máy tính khác nhau, nhiều thiết bị có thể dùng chung. Điều này tăng độ tin cậy trong công việc vì khi có máy tính hoặc thiết bị bị hỏng, công việc vẫn có thể tiếp tục với các máy tính hoặc thiết bị khác trên mạng trong khi chờ sửa chữa.

### V.3. Mạng giúp cho công việc đạt hiệu suất cao hơn.

Khi chương trình và dữ liệu đã dùng chung trên mạng, có thể bỏ qua một số khâu đối chiếu không cần thiết. Việc điều chỉnh chương trình (nếu có) cũng tiết kiệm thời gian hơn do chỉ cần cài đặt lại trên một máy.

Về mặt tổ chức, việc sao chép dữ liệu phòng hờ tiện lợi hơn do có thể giao cho chỉ một người thay vì mọi người phải tự sao chép phần của mình.

### V.4. Tiết kiệm chi phí.

Việc dùng chung các thiết bị ngoại vi cho phép giảm chi phí trang bị tính trên số người dùng. Về phần mềm, nhiều nhà sản xuất phần mềm cung cấp cả những ấn bản cho nhiều người dùng, với chi phí thấp hơn tính trên mỗi người dùng.

### V.5. Tăng cường tính bảo mật thông tin.

Dữ liệu được lưu trên các máy phục vụ tập tin (file server) sẽ được bảo vệ tốt hơn so với đặt tại các máy cá nhân nhờ cơ chế bảo mật của các hệ điều hành mạng.

### V.6. Việc phát triển mạng máy tính đã tạo ra nhiều ứng dụng mới

Một số ứng dụng có ảnh hưởng quan trọng đến toàn xã hội: khả năng truy xuất các chương trình và dữ liệu từ xa, khả năng thông tin liên lạc dễ dàng và hiệu quả, tạo môi trường giao tiếp thuận lợi giữa những người dùng khác nhau, khả năng tìm kiếm thông tin nhanh chóng trên phạm vi toàn thế giới,...

## VI. Các dịch vụ phổ biến trên mạng máy tính

- **Dịch vụ tập tin (File services)**

Cho phép chia sẻ tài nguyên thông tin chung, chuyển giao các tập tin dữ liệu từ máy này sang máy khác. Tìm kiếm thông tin và điều khiển truy nhập. Dịch vụ thư điện tử E_Mail (Electronic mail) cung cấp cho người sử dụng phương tiện trao đổi, tranh luận bằng thư điện tử. Dịch vụ thư điện tử giá thành hạ, chuyển phát nhanh, an toàn và nội dung có thể tích hợp các loại dữ liệu.

- **Dịch vụ in ấn**

Có thể dùng chung các máy in đắt tiền trên mạng. Cung cấp khả năng đa truy nhập đến máy in, phục vụ đồng thời cho nhiều nhu cầu in khác nhau. Cung cấp các dịch vụ FAX và quản lý được các trang thiết bị in chuyên dụng.

- **Các dịch vụ ứng dụng hướng đối tượng**

Sử dụng các dịch vụ thông điệp (Message) làm trung gian tác động đến các đối tượng truyền thông. Đối tượng chỉ bàn giao dữ liệu cho tác nhân (Agent) và tác nhân sẽ bàn giao dữ liệu cho đối tượng đích.

- **Các dịch vụ ứng dụng quản trị luồng công việc trong nhóm làm việc:**

Định tuyến các tài liệu điện tử giữa những người trong nhóm. Khi chữ ký điện tử được xác nhận trong các phiên giao dịch thì có thể thay thế được nhiều tiến trình mới hiệu quả và nhanh chóng hơn.

- **Dịch vụ cơ sở dữ liệu**

Là dịch vụ phổ biến về các dịch vụ ứng dụng, là các ứng dụng theo mô hình Client/Server. Dịch vụ xử lý phân tán lưu trữ dữ liệu phân tán trên mạng, người dùng trong suốt và dễ sử dụng, đáp ứng các nhu cầu truy nhập của người sử dụng.

# Chương II Mô hình truyền thông

## I. Sự cần thiết phải có mô hình truyền thông

Để một mạng máy tính trở một môi trường truyền dữ liệu thì nó cần phải có những yếu tố sau:

- Mỗi máy tính cần phải có một địa chỉ phân biệt trên mạng.
- Việc chuyển dữ liệu từ máy tính này đến máy tính khác do mạng thực hiện thông qua những quy định thống nhất gọi là giao thức của mạng.

Khi các máy tính trao đổi dữ liệu với nhau thì một quá trình truyền giao dữ liệu đã được thực hiện hoàn chỉnh. Ví dụ như để thực hiện việc truyền một file giữa một máy tính với một máy tính khác cùng được gắn trên một mạng các công việc sau đây phải được thực hiện:

- Máy tính cần truyền cần biết địa chỉ của máy nhận.
- Máy tính cần truyền phải xác định được máy tính nhận đã sẵn sàng nhận thông tin
- Chương trình gửi file trên máy truyền cần xác định được rằng chương trình nhận file trên máy nhận đã sẵn sàng tiếp nhận file.
- Nếu cấu trúc file trên hai máy không giống nhau thì một máy phải làm nhiệm vụ chuyển đổi file từ dạng này sang dạng kia.
- Khi truyền file máy tính truyền cần thông báo cho mạng biết địa chỉ của máy nhận để các thông tin được mạng đưa tới đích.

Điều trên đó cho thấy giữa hai máy tính đã có một sự phối hợp hoạt động ở mức độ cao. Bây giờ thay vì chúng ta xét cả quá trình trên như là một quá trình chung thì chúng ta sẽ chia quá trình trên ra thành một số công đoạn và mỗi công đoạn con hoạt động một cách độc lập với nhau. Ở đây chương trình truyền nhận file của mỗi máy tính được chia thành ba module là: Module truyền và nhận File, Module truyền thông và Module tiếp cận mạng. Hai module tương ứng sẽ thực hiện việc trao đổi với nhau trong đó:

- Module truyền và nhận file cần được thực hiện tất cả các nhiệm vụ trong các ứng dụng truyền nhận file. Ví dụ: truyền nhận thông số về file, truyền nhận các mẫu tin của file, thực hiện chuyển đổi file sang các dạng khác nhau nếu cần. Module truyền và nhận file không cần thiết phải trực tiếp quan tâm tới việc truyền dữ liệu trên mạng như thế nào mà nhiệm vụ đó được giao cho Module truyền thông.
- Module truyền thông quan tâm tới việc các máy tính đang hoạt động và sẵn sàng trao đổi thông tin với nhau. Nó còn kiểm soát các dữ liệu sao cho những dữ liệu này có thể trao đổi một cách chính xác và an toàn giữa hai máy tính. Điều đó có nghĩa là phải truyền file trên nguyên tắc đảm bảo an toàn cho dữ liệu, tuy nhiên ở đây có thể có một vài mức độ an toàn khác nhau được dành cho từng ứng dụng. Ở đây việc trao đổi dữ liệu giữa hai máy tính không phụ thuộc vào bản chất của mạng đang liên kết chúng. Những yêu cầu liên quan đến mạng đã được thực hiện ở module thứ ba là module tiếp cận mạng và nếu mạng thay đổi thì chỉ có module tiếp cận mạng bị ảnh hưởng.
- Module tiếp cận mạng được xây dựng liên quan đến các quy cách giao tiếp với mạng và phụ thuộc vào bản chất của mạng. Nó đảm bảo việc truyền dữ liệu từ máy tính này đến máy tính khác trong mạng.

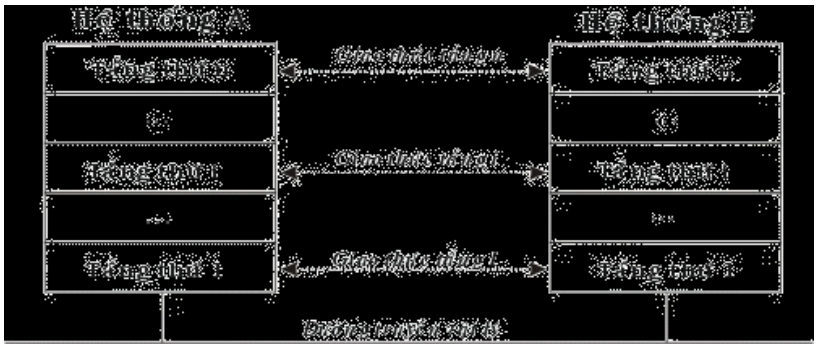
Như vậy thay vì xét cả quá trình truyền file với nhiều yêu cầu khác nhau như một tiến trình phức tạp thì chúng ta có thể xét quá trình đó với nhiều tiến trình con phân biệt dựa trên việc trao đổi

giữa các Module tương ứng trong chương trình truyền file. Cách này cho phép chúng ta phân tích kỹ quá trình file và dễ dàng trong việc viết chương trình.

Việc xét các module một cách độc lập với nhau như vậy cho phép giảm độ phức tạp cho việc thiết kế và cài đặt. Phương pháp này được sử dụng rộng rãi trong việc xây dựng mạng và các chương trình truyền thông và được gọi là phương pháp phân tầng (layer).

Nguyên tắc của phương pháp phân tầng là:

- Mỗi hệ thống thành phần trong mạng được xây dựng như một cấu trúc nhiều tầng và đều có cấu trúc giống nhau như: số lượng tầng và chức năng của mỗi tầng.
- Các tầng nằm chồng lên nhau, dữ liệu được chỉ trao đổi trực tiếp giữa hai tầng kề nhau từ tầng trên xuống tầng dưới và ngược lại.
- Cùng với việc xác định chức năng của mỗi tầng chúng ta phải xác định mối quan hệ giữa hai tầng kề nhau. Dữ liệu được truyền đi từ tầng cao nhất của hệ thống truyền lần lượt đến tầng thấp nhất sau đó truyền qua đường nối vật lý dưới dạng các bit tới tầng thấp nhất của hệ thống nhận, sau đó dữ liệu được truyền ngược lên lần lượt đến tầng cao nhất của hệ thống nhận.
- Chỉ có hai tầng thấp nhất có liên kết vật lý với nhau còn các tầng trên cùng thứ tư chỉ có các liên kết logic với nhau. Liên kết logic của một tầng được thực hiện thông qua các tầng dưới và phải tuân theo những quy định chặt chẽ, các quy định đó được gọi giao thức của tầng.



Hình II-1 Mô hình phân tầng

## II. Các nhu cầu về chuẩn hóa đối với mạng

Trong thực tế việc phân chia các tầng như trong mô hình trên thực sự chưa đủ. Trên thế giới hiện có một số cơ quan định chuẩn, họ đưa ra hàng loạt chuẩn về mạng tuy các chuẩn đó có tính chất khuyến nghị chứ không bắt buộc nhưng chúng rất được các cơ quan chuẩn quốc gia coi trọng.

Hai trong số các cơ quan chuẩn quốc tế là:

- **ISO (The International Standards Organization)** - Là tổ chức tiêu chuẩn quốc tế hoạt động dưới sự bảo trợ của Liên hợp Quốc với thành viên là các cơ quan chuẩn quốc gia với số lượng khoảng hơn 100 thành viên với mục đích hỗ trợ sự phát triển các chuẩn trên phạm vi toàn thế giới. Một trong những thành tựu của ISO trong lãnh vực truyền thông là mô hình hệ thống mở (Open Systems Interconnection - gọi tắt là OSI).

- **CCITT (Commité Consultatif International pour le Telegraphe et la Téléphone)** - Tổ chức tư vấn quốc tế về điện tín và điện thoại làm việc dưới sự bảo trợ của Liên Hiệp Quốc có trụ sở chính tại Geneva - Thụy sỹ. Các thành viên chủ yếu là các cơ quan bưu chính viễn thông các quốc gia. Tổ chức này có vai trò phát triển các khuyến nghị trong các lãnh vực viễn thông.

## III. Mô hình OSI (Open Systems Interconnection)

Mô hình OSI là một cơ sở dành cho việc chuẩn hoá các hệ thống truyền thông, nó được nghiên cứu và xây dựng bởi ISO. Việc nghiên cứu về mô hình OSI được bắt đầu tại ISO vào năm 1971 với mục tiêu nhằm tới việc nối kết các sản phẩm của các hãng sản xuất khác nhau và phối hợp các hoạt động chuẩn hoá trong các lĩnh vực viễn thông và hệ thống thông tin. Theo mô hình OSI chương trình truyền thông được chia ra thành 7 tầng với những chức năng phân biệt cho từng tầng. Hai tầng đồng mức khi liên kết với nhau phải sử dụng một giao thức chung.

Việc nghiên cứu về OSI được bắt đầu tại ISO vào năm 1971 với các mục tiêu nhằm nối kết các sản phẩm của các hãng sản xuất khác. Ưu điểm chính của OSI là ở chỗ nó hứa hẹn giải pháp cho vấn đề truyền thông giữa các máy tính không giống nhau. Hai hệ thống, dù có khác nhau đều có thể truyền thông với nhau một các hiệu quả nếu chúng đảm bảo những điều kiện chung sau đây:

- Chúng cài đặt cùng một tập các chức năng truyền thông.
  Các chức năng đó được tổ chức thành cùng một tập các tầng. các tầng đồng mức phải cung cấp các chức năng như nhau.
- Các tầng đồng mức khi trao đổi với nhau sử dụng chung một giao thức

Mô hình OSI tách các mặt khác nhau của một mạng máy tính thành bảy tầng theo mô hình phân tầng. Mô hình OSI là một khung mà các tiêu chuẩn lập mạng khác nhau có thể khớp vào. Mô hình OSI định rõ các mặt nào của hoạt động của mạng có thể nhằm đến bởi các tiêu chuẩn mạng khác nhau. Vì vậy, theo một nghĩa nào đó, mô hình OSI là một loại tiêu chuẩn của các chuẩn.

### III.1. Nguyên tắc sử dụng khi định nghĩa các tầng hệ thống mở

Sau đây là các nguyên tắc mà ISO quy định dùng trong quá trình xây dựng mô hình OSI

- Không định nghĩa quá nhiều tầng để việc xác định và ghép nối các tầng không quá phức tạp.
- Tạo các ranh giới các tầng sao cho việc giải thích các phục vụ và số các tương tác qua lại hai tầng là nhỏ nhất.
- Tạo các tầng riêng biệt cho các chức năng khác biệt nhau hoàn toàn về kỹ thuật sử dụng hoặc quá trình thực hiên.
- Các chức năng giống nhau được đặt trong cùng một tầng.
  Lựa chọn ranh giới các tầng tại các điểm mà những thử nghiệm trong quá khứ thành công.
- Các chức năng được xác định sao cho chúng có thể dễ dàng xác định lại, và các nghi thức của chúng có thể thay đổi trên mọi hướng.
- Tạo ranh giới các tầng mà ở đó cần có những mức độ trừu tượng khác nhau trong việc sử dụng số liệu.
- Cho phép thay đổi các chức năng hoặc giao thức trong tầng không ảnh hưởng đến các tầng khác.

- Tạo các ranh giới giữa mỗi tầng với tầng trên và dưới nó.

## III.2. Các giao thức trong mô hình OSI

Trong mô hình OSI có hai loại giao thức chính được áp dụng: giao thức có liên kết (connection - oriented) và giao thức không liên kết (connectionless).

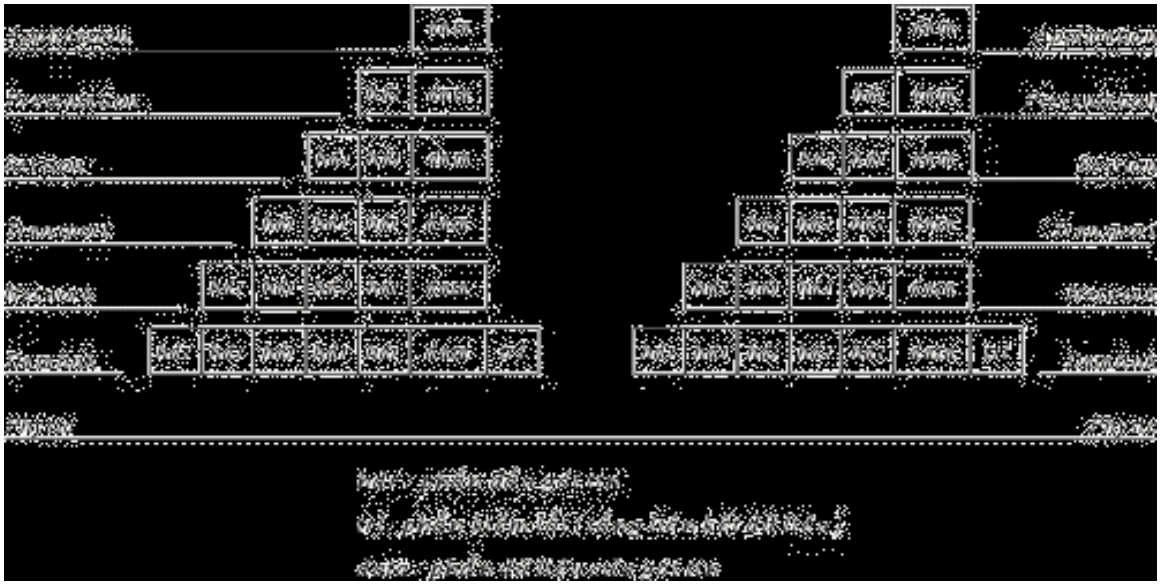
- *Giao thức có liên kết*: trước khi truyền dữ liệu hai tầng đồng mức cần thiết lập một liên kết logic và các gói tin được trao đổi thông qua liên kết náy, việc có liên kết logic sẽ nâng cao độ an toàn trong truyền dữ liệu.
- *Giao thức không liên kết*: trước khi truyền dữ liệu không thiết lập liên kết logic và mỗi gói tin được truyền độc lập với các gói tin trước hoặc sau nó.

Như vậy với giao thức có liên kết, quá trình truyền thông phải gồm 3 giai đoạn phân biệt:

- *Thiết lập liên kết (logic):* hai thực thể đồng mức ở hai hệ thống thương lượng với nhau về tập các tham số sẽ sử dụng trong giai đoạn sau (truyền dữ liệu).
- *Truyền dữ liệu*: dữ liệu được truyền với các cơ chế kiểm soát và quản lý kèm theo (như kiểm soát lỗi, kiểm soát luồng dữ liệu, cắt/hợp dữ liệu...) để tăng cường độ tin cậy và hiệu quả của việc truyền dữ liệu.
- *Hủy bỏ liên kết (logic):* giải phóng tài nguyên hệ thống đã được cấp phát cho liên kết để dùng cho liên kết khác.

Đối với giao thức không liên kết thì chỉ có duy nhất một giai đoạn truyền dữ liệu mà thôi.

Gói tin của giao thức: Gói tin (Packet) được hiểu như là một đơn vị thông tin dùng trong việc liên lạc, chuyển giao dữ liệu trong mạng máy tính. Những thông điệp (message) trao đổi giữa các máy tính trong mạng, được tạo dạng thành các gói tin ở máy nguồn. Và những gói tin này khi đích sẽ được kết hợp lại thành thông điệp ban đầu. Một gói tin có thể chứa đựng các yêu cầu phục vụ, các thông tin điều khiển và dữ liệu.



Hình II-2 Phương thức xác lập các gói tin trong mô hình OSI

Trên quan điểm mô hình mạng phân tầng tầng mỗi tầng chỉ thực hiện một chức năng là nhận dữ liệu từ tầng bên trên để chuyển giao xuống cho tầng bên dưới và ngược lại. Chức năng này thực chất là gắn thêm và gỡ bỏ phần đầu (header) đối với các gói tin trước khi chuyển nó đi. Nói cách khác, từng gói tin bao gồm phần đầu (header) và phần dữ liệu. Khi đi đến một tầng mới gói tin sẽ được đóng thêm một phần đầu đề khác và được xem như là gói tin của tầng mới, công việc trên tiếp diễn cho tới khi gói tin được truyền lên đường dây mạng để đến bên nhận.

Tại bên nhận các gói tin được gỡ bỏ phần đầu trên từng tầng tướng ứng và đây cũng là nguyên lý của bất cứ mô hình phân tầng nào.

***Chú ý:*** Trong mô hình OSI phần kiểm lỗi của gói tin tầng liên kết dữ liệu đặt ở cuối gói tin

## III.3. Các chức năng chủ yếu của các tầng của mô hình OSI.

### III.3.1 Tầng 1: Vật lý (Physical)

Tầng vật lý (Physical layer) là tầng dưới cùng của mô hình OSI là. Nó mô tả các đặc trưng vật lý của mạng: Các loại cáp được dùng để nối các thiết bị, các loại đầu nối được dùng , các dây cáp có thể dài bao nhiêu v.v... Mặt khác các tầng vật lý cung cấp các đặc trưng điện của các tín hiệu được dùng để khi chuyển dữ liệu trên cáp từ một máy này đến một máy khác của mạng, kỹ thuật nối mạch điện, tốc độ cáp truyền dẫn.

Tầng vật lý không qui định một ý nghĩa nào cho các tín hiệu đó ngoài các giá trị nhị phân 0 và 1. Ở các tầng cao hơn của mô hình OSI ý nghĩa của các bit được truyền ở tầng vật lý sẽ được xác định.

***Ví dụ:*** Tiêu chuẩn Ethernet cho cáp xoắn đôi 10 baseT định rõ các đặc trưng điện của cáp xoắn đôi, kích thước và dạng của các đầu nối, độ dài tối đa của cáp.

Khác với các tầng khác, tầng vật lý là không có gói tin riêng và do vậy không có phần đầu (header) chứa thông tin điều khiển, dữ liệu được truyền đi theo dòng bit. Một giao thức tầng vật lý tồn tại giữa các tầng vật lý để quy định về phương thức truyền (đồng bộ, phi đồng bộ), tốc độ truyền.

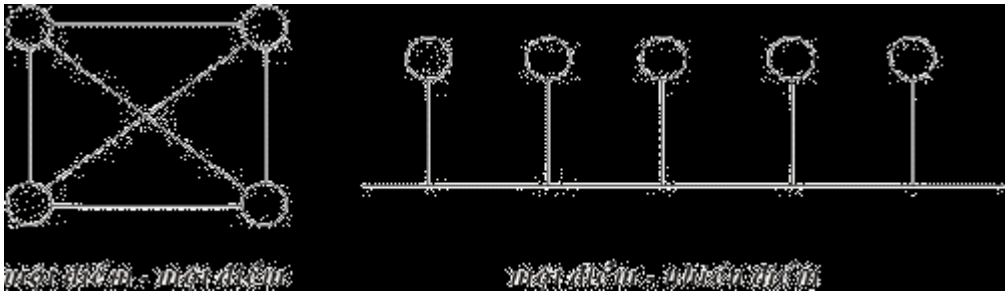
Các giao thức được xây dựng cho tầng vật lý được phân chia thành phân chia thành hai loại giao thức sử dụng phương thức truyền thông dị bộ (asynchronous) và phương thức truyền thông đồng bộ (synchronous).

- *Phương thức truyền dị bộ*: Không có một tín hiệu quy định cho sự đồng bộ giữa các bit giữa máy gửi và máy nhận, trong quá trình gửi tín hiệu máy gửi sử dụng các bit đặc biệt START và STOP được dùng để tách các xâu bit biểu diễn các ký tự trong dòng dữ liệu cần truyền đi. Nó cho phép một ký tự được truyền đi bất kỳ lúc nào mà không cần quan tâm đến các tín hiệu đồng bộ trước đó.
- *Phương thức truyền đồng bộ*: Sử dụng phương thức truyền cần có đồng bộ giữa máy gửi và máy nhận, nó chèn các ký tự đặc biệt như SYN (Synchronization), EOT (End Of Transmission) hay đơn giản hơn, một cái "cờ " (flag) giữa các dữ liệu của máy gửi để báo hiệu cho máy nhận biết được dữ liệu đang đến hoặc đã đến.

### III.3.2 Tầng 2: Liên kết dữ liệu (Data link)

Tầng liên kết dữ liệu (data link layer) là tầng mà ở đó ý nghĩa được gán cho các bít được truyền trên mạng. Tầng liên kết dữ liệu phải quy định được các dạng thức, kích thước, địa chỉ máy gửi và nhận của mỗi gói tin được gửi đi. Nó phải xác định cơ chế truy nhập thông tin trên mạng và phương tiện gửi mỗi gói tin sao cho nó được đưa đến cho người nhận đã định.

Tầng liên kết dữ liệu có hai phương thức liên kết dựa trên cách kết nối các máy tính, đó là phương thức "một điểm - một điểm" và phương thức "một điểm - nhiều điểm". Với phương thức "một điểm - một điểm" các đường truyền riêng biệt được thiết lập để nối các cặp máy tính lại với nhau. Phương thức "một điểm - nhiều điểm " tất cả các máy phân chia chung một đường truyền vật lý.



Hình II-3 : Các đường truyền kết nối kiểu "một điểm - một điểm" và "một điểm - nhiều điểm"

Tầng liên kết dữ liệu cũng cung cấp cách phát hiện và sửa lỗi cơ bản để đảm bảo cho dữ liệu nhận được giống hoàn toàn với dữ liệu gửi đi. Nếu một gói tin có lỗi không sửa được, tầng liên kết dữ liệu phải chỉ ra được cách thông báo cho nơi gửi biết gói tin đó có lỗi để nó gửi lại.

Các giao thức tầng liên kết dữ liệu chia làm 2 loại chính là các giao thức hướng ký tư và các giao thức hướng bit. Các giao thức hướng ký tự được xây dựng dựa trên các ký tự đặc biệt của một bộ mã chuẩn nào đó (như ASCII hay EBCDIC), trong khi đó các giao thức hướng bit lại dùng các cấu trúc nhị phân (xâu bit) để xây dựng các phần tử của giao thức (đơn vị dữ liệu, các thủ tục.) và khi nhận, dữ liệu sẽ được tiếp nhận lần lượt từng bit một.

### III.3.3 Tầng 3: Mạng (Network)

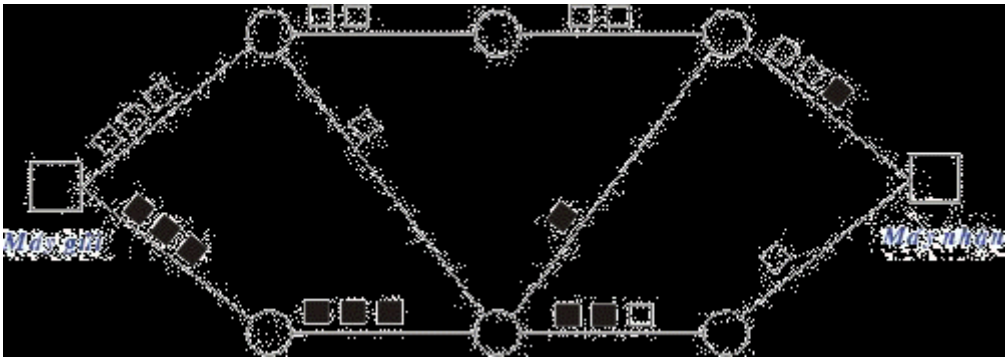
Tầng mạng (network layer) nhắm đến việc kết nối các mạng với nhau bằng cách tìm đường (routing) cho các gói tin từ một mạng này đến một mạng khác. Nó xác định việc chuyển hướng, vạch đường các gói tin trong mạng, các gói này có thể phải đi qua nhiều chặng trước khi đến được đích cuối cùng. Nó luôn tìm các tuyến truyền thông không tắc nghẽn để đưa các gói tin đến đích.

Tầng mạng cung các các phương tiện để truyền các gói tin qua mạng, thậm chí qua một mạng của mạng (network of network). Bởi vậy nó cần phải đáp ứng với nhiều kiểu mạng và nhiều kiểu dịch vụ cung cấp bởi các mạng khác nhau. hai chức năng chủ yếu của tầng mạng là chọn đường (routing) và chuyển tiếp (relaying). Tầng mạng là quan trọng nhất khi liên kết hai loại mạng khác nhau như mạng Ethernet với mạng Token Ring khi đó phải dùng một bộ tìm đường (quy định bởi tầng mạng) để chuyển các gói tin từ mạng này sang mạng khác và ngược lại.

Đối với một mạng chuyển mạch gói (packet - switched network) - gồm tập hợp các nút chuyển mạch gói nối với nhau bởi các liên kết dữ liệu. Các gói dữ liệu được truyền từ một hệ thống mở tới một hệ thống mở khác trên mạng phải được chuyển qua một chuỗi các nút. Mỗi nút nhận gói dữ liệu từ một đường vào (incoming link) rồi chuyển tiếp nó tới một đường ra (outgoing link) hướng đến đích của dữ liệu. Như vậy ở mỗi nút trung gian nó phải thực hiện các chức năng chọn đường và chuyển tiếp.

Việc chọn đường là sự lựa chọn một con đường để truyền một đơn vị dữ liệu (một gói tin chẳng hạn) từ trạm nguồn tới trạm đích của nó. Một kỹ thuật chọn đường phải thực hiện hai chức năng chính sau đây:

- Quyết định chọn đường tối ưu dựa trên các thông tin đã có về mạng tại thời điểm đó thông qua những tiêu chuẩn tối ưu nhất định.
- Cập nhật các thông tin về mạng, tức là thông tin dùng cho việc chọn đường, trên mạng luôn có sự thay đổi thường xuyên nên việc cập nhật là việc cần thiết.



Hình II-4 Mô hình chuyển vận các gói tin trong mạng chuyển mạch gói

Người ta có hai phương thức đáp ứng cho việc chọn đường là phương thức xử lý tập trung và xử lý tại chỗ.

- *Phương thức chọn đường xử lý tập trung* được đặc trưng bởi sự tồn tại của một (hoặc vài) trung tâm điều khiển mạng, chúng thực hiện việc lập ra các bảng đường đi tại từng thời điểm cho các nút và sau đó gửi các bảng chọn đường tới từng nút dọc theo con đường đã được chọn đó. Thông tin tổng thể của mạng cần dùng cho việc chọn đường chỉ cần cập nhập và được cất giữ tại trung tâm điều khiển mạng.
- *Phương thức chọn đường xử lý tại chỗ* được đặc trưng bởi việc chọn đường được thực hiện tại mỗi nút của mạng. Trong từng thời điểm, mỗi nút phải duy trì các thông tin của mạng và tự xây dựng bảng chọn đường cho mình. Như vậy các thông tin tổng thể của mạng cần dùng cho việc chọn đường cần cập nhập và được cất giữ tại mỗi nút.

Thông thường các thông tin được đo lường và sử dụng cho việc chọn đường bao gồm:

- Trạng thái của đường truyền.
- Thời gian trễ khi truyền trên mỗi đường dẫn.
- Mức độ lưu thông trên mỗi đường.
- Các tài nguyên khả dụng của mạng.

Khi có sự thay đổi trên mạng (ví dụ thay đổi về cấu trúc của mạng do sự cố tại một vài nút, phục hồi của một nút mạng, nối thêm một nút mới... hoặc thay đổi về mức độ lưu thông) các thông tin trên cần được cập nhật vào các cơ sở dữ liệu về trạng thái của mạng.

Hiện nay khi nhu cầu truyền thông đa phương tiện (tích hợp dữ liệu văn bản, đồ hoạ, hình ảnh, âm thanh) ngày càng phát triển đòi hỏi các công nghệ truyền dẫn tốc độ cao nên việc phát triển các hệ thống chọn đường tốc độ cao đang rất được quan tâm.

### III.3.4 Tầng 4: Vận chuyển (Transport)

Tầng vận chuyển cung cấp các chức năng cần thiết giữa tầng mạng và các tầng trên. nó là tầng cao nhất có liên quan đến các giao thức trao đổi dữ liệu giữa các hệ thống mở. Nó cùng các tầng dưới cung cấp cho người sử dụng các phục vụ vận chuyển.

Tầng vận chuyển (transport layer) là tầng cơ sở mà ở đó một máy tính của mạng chia sẻ thông tin với một máy khác. Tầng vận chuyển đồng nhất mỗi trạm bằng một địa chỉ duy nhất và quản lý sự kết nối giữa các trạm. Tầng vận chuyển cũng chia các gói tin lớn thành các gói tin nhỏ hơn trước khi gửi đi. Thông thường tầng vận chuyển đánh số các gói tin và đảm bảo chúng chuyển theo đúng thứ tự.

Tầng vận chuyển là tầng cuối cùng chịu trách nhiệm về mức độ an toàn trong truyền dữ liệu nên giao thức tầng vận chuyển phụ thuộc rất nhiều vào bản chất của tầng mạng. Người ta chia giao thức tầng mạng thành các loại sau:

- Mạng loại A: Có tỷ suất lỗi và sự cố có báo hiệu chấp nhận được (tức là chất lượng chấp nhận được). Các gói tin được giả thiết là không bị mất. Tầng vận chuyển không cần cung cấp các dịch vụ phục hồi hoặc sắp xếp thứ tự lại.
- Mạng loại B: Có tỷ suất lỗi chấp nhận được nhưng tỷ suất sự cố có báo hiệu lại không chấp nhận được. Tầng giao vận phải có khả năng phục hồi lại khi xảy ra sự cố.
- Mạng loại C: Có tỷ suất lỗi không chấp nhận được (không tin cậy) hay là giao thức không liên kết. Tầng giao vận phải có khả năng phục hồi lại khi xảy ra lỗi và sắp xếp lại thứ tự các gói tin.

Trên cơ sở loại giao thức tầng mạng chúng ta có 5 lớp giao thức tầng vận chuyển đó là:

- *Giao thức lớp 0 (Simple Class - lớp đơn giản)*: cung cấp các khả năng rất đơn giản để thiết lập liên kết, truyền dữ liệu và hủy bỏ liên kết trên mạng "có liên kết" loại A. Nó có khả năng phát hiện và báo hiệu các lỗi nhưng không có khả năng phục hồi.
- *Giao thức lớp 1 (Basic Error Recovery Class - Lớp phục hồi lỗi cơ bản)* dùng với các loại mạng B, ở đây các gói tin (TPDU) được đánh số. Ngoài ra giao thức còn có khả năng báo nhận cho nơi gửi và truyền dữ liệu khẩn. So với giao thức lớp 0 giao thức lớp 1 có thêm khả năng phục hồi lỗi.
- *Giao thức lớp 2 (Multiplexing Class - lớp dồn kênh)* là một cải tiến của lớp 0 cho phép dồn một số liên kết chuyển vận vào một liên kết mạng duy nhất, đồng thời có thể kiểm soát luồng dữ liệu để tránh tắc nghẽn. Giao thức lớp 2 không có khả năng phát hiện và phục hồi lỗi. Do vậy nó cần đặt trên một tầng mạng loại A.

- *Giao thức lớp 3 (Error Recovery and Multiplexing Class - lớp phục hồi lỗi cơ bản và dồn kênh)* là sự mở rộng giao thức lớp 2 với khả năng phát hiện và phục hồi lỗi, nó cần đặt trên một tầng mạng loại B.
- *Giao thức lớp 4 (Error Detection and Recovery Class - Lớp phát hiện và phục hồi lỗi)* là lớp có hầu hết các chức năng của các lớp trước và còn bổ sung thêm một số khả năng khác để kiểm soát việc truyền dữ liệu.

### III.3.5 Tầng 5: Giao dịch (Session)

Tầng giao dịch (session layer) thiết lập "các giao dịch" giữa các trạm trên mạng, nó đặt tên nhất quán cho mọi thành phần muốn đối thoại với nhau và lập ánh xa giữa các tên với địa chỉ của chúng. Một giao dịch phải được thiết lập trước khi dữ liệu được truyền trên mạng, tầng giao dịch đảm bảo cho các giao dịch được thiết lập và duy trì theo đúng qui định.

Tầng giao dịch còn cung cấp cho người sử dụng các chức năng cần thiết để quản trị các giao dịnh ứng dụng của họ, cụ thể là:

- Điều phối việc trao đổi dữ liệu giữa các ứng dụng bằng cách thiết lập và giải phóng (một cách lôgic) các phiên (hay còn gọi là các hội thoại - dialogues)
- Cung cấp các điểm đồng bộ để kiểm soát việc trao đổi dữ liệu.
- Áp đặt các qui tắc cho các tương tác giữa các ứng dụng của người sử dụng.
- Cung cấp cơ chế "lấy lượt" (nắm quyền) trong quá trình trao đổi dữ liệu.

Trong trường hợp mạng là hai chiều luân phiên thì nẩy sinh vấn đề: hai người sử dụng luân phiên phải "lấy lượt" để truyền dữ liệu. Tầng giao dịch duy trì tương tác luân phiên bằng cách báo cho mỗi người sử dụng khi đến lượt họ được truyền dữ liệu. Vấn đề đồng bộ hóa trong tầng giao dịch cũng được thực hiện như cơ chế kiểm tra/phục hồi, dịch vụ này cho phép người sử dụng xác định các điểm đồng bộ hóa trong dòng dữ liệu đang chuyển vận và khi cần thiết có thể khôi phục việc hội thoại bắt đầu từ một trong các điểm đó

Ở một thời điểm chỉ có một người sử dụng đó quyền đặc biệt được gọi các dịch vụ nhất định của tầng giao dịch, việc phân bổ các quyền này thông qua trao đổi thẻ bài (token). Ví dụ: Ai có được token sẽ có quyền truyền dữ liệu, và khi người giữ token trao token cho người khác thi cũng có nghĩa trao quyền truyền dữ liệu cho người đó.

Tầng giao dịch có các hàm cơ bản sau:

- *Give Token* cho phép người sử dụng chuyển một token cho một người sử dụng khác của một liên kết giao dịch.
- *Please Token* cho phép một người sử dụng chưa có token có thể yêu cầu token đó.
- *Give Control* dùng để chuyển tất cả các token từ một người sử dụng sang một người sử dụng khác.

### III.3.6 Tầng 6: Trình bày (Presentation)

Trong giao tiếp giữa các ứng dụng thông qua mạng với cùng một dữ liệu có thể có nhiều cách biểu diễn khác nhau. Thông thường dạng biểu diễn dùng bởi ứng dụng nguồn và dạng biểu diễn dùng bởi ứng dụng đích có thể khác nhau do các ứng dụng được chạy trên các hệ thống hoàn toàn khác nhau (như hệ máy Intel và hệ máy Motorola). Tầng trình bày (Presentation layer) phải chịu trách nhiệm chuyển đổi dữ liệu gửi đi trên mạng từ một loại biểu diễn này sang một loại

khác. Để đạt được điều đó nó cung cấp một dạng biểu diễn chung dùng để truyền thông và cho phép chuyển đổi từ dạng biểu diễn cục bộ sang biểu diễn chung và ngược lại.

Tầng trình bày cũng có thể được dùng kĩ thuật mã hóa để xáo trộn các dữ liệu trước khi được truyền đi và giải mã ở đầu đến để bảo mật. Ngoài ra tầng biểu diễn cũng có thể dùng các kĩ thuật nén sao cho chỉ cần một ít byte dữ liệu để thể hiện thông tin khi nó được truyền ở trên mạng, ở đầu nhận, tầng trình bày bung trở lại để được dữ liệu ban đầu.

### III.3.7 Tầng 7: Ứng dụng (Application)

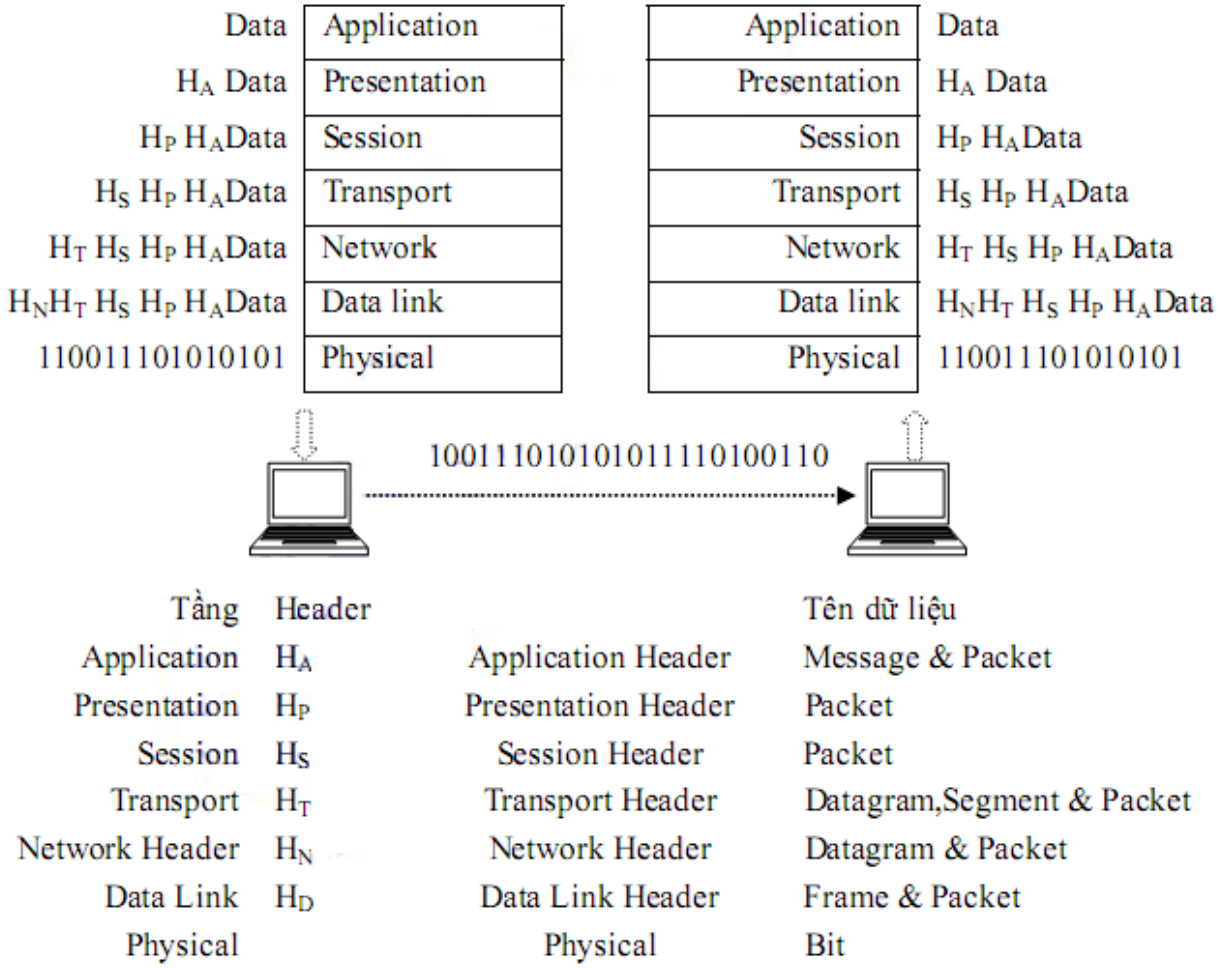
Tầng ứng dụng (Application layer) là tầng cao nhất của mô hình OSI, nó xác định giao diện giữa người sử dụng và môi trường OSI và giải quyết các kỹ thuật mà các chương trình ứng dụng dùng để giao tiếp với mạng.

Để cung cấp phương tiện truy nhập môi trường OSI cho các tiến trình ứng dụng, Người ta thiết lập các thực thể ứng dụng (AE), các thực thể ứng dụng sẽ gọi đến các phần tử dịch vụ ứng dụng (Application Service Element - viết tắt là ASE) của chúng. Mỗi thực thể ứng dụng có thể gồm một hoặc nhiều các phần tử dịch vụ ứng dụng. Các phần tử dịch vụ ứng dụng được phối hợp trong môi trường của thực thể ứng dụng thông qua các liên kết (association) gọi là đối tượng liên kết đơn (Single Association Object - viết tắt là SAO). SAO điều khiển việc truyền thông trong suốt vòng đời của liên kết đó cho phép tuần tự hóa các sự kiện đến từ các ASE thành tố của nó.

# IV. Quá trình chuyển vận gói tin

## IV.1. Quá trình đóng gói dữ liệu (tại máy gửi)

Đóng gói dữ liệu là quá trình đặt dữ liệu nhận được vào sau header (và trước trailer) trên mỗi lớp. Lớp Physical không đóng gói dữ liệu vì nó không dùng header và trailer. Việc đóng gói dữ liệu không nhất thiết phải xảy ra trong mỗi lần truyền dữ liệu của trình ứng dụng. Các lớp 5, 6, 7 sử dụng header trong quá trình khởi động, nhưng trong phần lớn các lần truyền thì không có header của lớp 5, 6, 7 lý do là không có thông tin mới để trao đổi.




| Tầng | Header | | Tên dữ liệu |
|---|---|---|---|
| Application | $H_A$ | Application Header | Message & Packet |
| Presentation | $H_P$ | Presentation Header | Packet |
| Session | $H_S$ | Session Header | Packet |
| Transport | $H_T$ | Transport Header | Datagram,Segment & Packet |
| Network Header | $H_N$ | Network Header | Datagram & Packet |
| Data Link | $H_D$ | Data Link Header | Frame & Packet |
| Physical | | Physical | Bit |

Hình II-5 Bổ sung phần đầu thông điệp & tên dữ liệu sử dụng

Các dữ liệu tại máy gửi được xử lý theo trình tự như sau:

- Người dùng thông qua lớp Application để đưa các thông tin vào máy tính. Các thông tin này có nhiều dạng khác nhau như: hình ảnh, âm thanh, văn bản…

- Tiếp theo các thông tin đó được chuyển xuống lớp Presentation để chuyển thành dạng chung, rồi mã hoá và nén dữ liệu.

- Tiếp đó dữ liệu được chuyển xuống lớp Session để bổ sung các thông tin về phiên giao dịch này.

- Dữ liệu tiếp tục được chuyển xuống lớp Transport, tại lớp này dữ liệu được cắt ra thành nhiều Segment và bổ sung thêm các thông tin về phương thức vận chuyển dữ liệu để đảm bảo độ tin cậy khi truyền.

- Dữ liệu tiếp tục được chuyển xuống lớp Network, tại lớp này mỗi Segment được cắt ra thành nhiều Packet và bổ sung thêm các thông tin định tuyến.

- Tiếp đó dữ liệu được chuyển xuống lớp Data Link, tại lớp này mỗi Packet sẽ được cắt ra thành nhiều Frame và bổ sung thêm các thông tin kiểm tra gói tin (để kiểm tra ở nơi nhận).

- Cuối cùng, mỗi Frame sẽ được tầng Vật Lý chuyển thành một chuỗi các bit, và được đẩy lên các phương tiện truyền dẫn để truyền đến các thiết bị khác.

## IV.2. Quá trình truyền dữ liệu từ máy gửi đến máy nhận.

Bước 1: Trình ứng dụng (trên máy gửi) tạo ra dữ liệu và các chương trình phần cứng, phần mềm cài đặt mỗi lớp sẽ bổ sung vào header và trailer (quá trình đóng gói dữ liệu tại máy gửi).

Bước 2: Lớp Physical (trên máy gửi) phát sinh tín hiệu lên môi trường truyền tải để truyền dữ liệu.

Bước 3: Lớp Physical (trên máy nhận) nhận dữ liệu.

Bước 4: Các chương trình phần cứng, phần mềm (trên máy nhận) gỡ bỏ header và trailer và xử lý phần dữ liệu (quá trình xử lý dữ liệu tại máy nhận).

Giữa bước 1 và bước 2 là quá trình tìm đường đi của gói tin. Thông thường, máy gửi đã biết địa chỉ IP của máy nhận. Vì thế, sau khi xác định được địa chỉ IP của máy nhận thì lớp Network của máy gửi sẽ so sánh địa chỉ IP của máy nhận và địa chỉ IP của chính nó:

- Nếu cùng địa chỉ mạng thì máy gửi sẽ tìm trong bảng MAC Table của mình để có được địa chỉ MAC của máy nhận. Trong trường hợp không có được địa chỉ MAC tương ứng, nó sẽ thực hiện giao thức ARP để truy tìm địa chỉ MAC. Sau khi tìm được địa chỉ MAC, nó sẽ lưu địa chỉ MAC này vào trong bảng MAC Table để lớp Datalink sử dụng ở các lần gửi sau. Sau khi có địa chỉ MAC thì máy gửi sẽ gởi gói tin đi.

- Nếu khác địa chỉ mạng thì máy gửi sẽ kiểm tra xem máy có được khai báo Default Gateway hay không.

+ Nếu có khai báo Default Gateway thì máy gửi sẽ gởi gói tin thông qua Default Gateway.

+ Nếu không có khai báo Default Gateway thì máy gởi sẽ loại bỏ gói tin và thông báo "Destination host Unreachable"

## IV.3. Chi tiết quá trình xử lý tại máy nhận

Bước 1: Lớp Physical kiểm tra quá trình đồng bộ bit và đặt chuỗi bit nhận được vào vùng đệm. Sau đó thông báo cho lớp Data Link dữ liệu đã được nhận.

Bước 2: Lớp Data Link kiểm lỗi frame bằng cách kiểm tra FCS trong trailer. Nếu có lỗi thì frame bị bỏ.

Sau đó kiểm tra địa chỉ lớp Data Link (địa chỉ MAC) xem có trùng với địa chỉ máy nhận hay không. Nếu đúng thì phần dữ liệu sau khi loại header và trailer sẽ được chuyển lên cho lớp Network.

Bước 3: Địa chỉ lớp Network được kiểm tra xem có phải là địa chỉ máy nhận hay không (địa chỉ IP) ? Nếu đúng thì dữ liệu được chuyển lên cho lớp Transport xử lý.

Bước 4: Nếu giao thức lớp Transport có hỗ trợ việc phục hồi lỗi thì số định danh phân đoạn được xử lý. Các thông tin ACK, NAK (gói tin ACK, NAK dùng để phản hồi về việc các gói tin đã được gởi đến máy nhận chưa) cũng được xử lý ở lớp này. Sau quá trình phục hồi lỗi và sắp thứ tự các phân đoạn, dữ liệu được đưa lên lớp Session.

Bước 5: Lớp Session đảm bảo một chuỗi các thông điệp đã trọn vẹn. Sau khi các luồng đã hoàn tất, lớp Session chuyển dữ liệu sau header lớp 5 lên cho lớp Presentation xử lý.

Bước 6: Dữ liệu sẽ được lớp Presentation xử lý bằng cách chuyển đổi dạng thức dữ liệu. Sau đó kết quả chuyển lên cho lớp Application.

Bước 7: Lớp Application xử lý header cuối cùng. Header này chứa các tham số thoả thuận giữa hai trình ứng dụng. Do vậy tham số này thường chỉ được trao đổi lúc khởi động quá trình truyền thông giữa hai trình ứng dụng.

# V. Phương thức truyền tín hiệu

Thông thường có hai phương thức truyền tín hiệu trong mạng cục bộ là dùng băng tần cơ sở (baseband) và băng tần rộng (broadband). Sự khác nhau chủ yếu giữa hai phương thức truyền tín hiệu này là băng tầng cơ sở chỉ chấp nhận một kênh dữ liệu duy nhất trong khi băng rộng có thể chấp nhận đồng thời hai hoặc nhiều kênh truyền thông cùng phân chia giải thông của đường truyền.

Hầu hết các mạng cục bộ sử dụng phương thức băng tần cơ sở. Với phương thức truyền tín hiệu này này tín hiệu có thể được truyền đi dưới cả hai dạng: tương tự (analog) hoặc số (digital). Phương thức truyền băng tần rộng chia giải thông (tần số) của đường truyền thành nhiều giải tần con trong đó mỗi dải tần con đó cung cấp một kênh truyền dữ liệu tách biệt nhờ sử dụng một cặp modem đặc biệt gọi là bộ giải / Điều biến RF cai quản việc biến đổi các tín hiệu số thành tín hiệu tương tự có tần số vô tuyến (RF) bằng kỹ thuật ghép kênh.

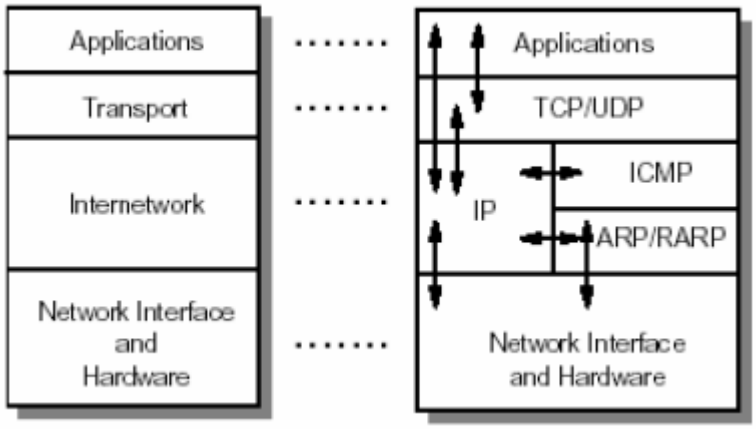
# VI. Mô hình TCP/IP

## VI.1. Tổng quan về bộ giao thức TCP/IP

TCP/IP là bộ giao thức cho phép kết nối các hệ thống mạng không đồng nhất với nhau. Ngày nay, TCP/IP được sử dụng rộng rãi trong các mạng cục bộ cũng như trên mạng Internet toàn cầu.

TCP/IP được xem là giản lược của mô hình tham chiếu OSI với bốn tầng như sau:

- Tầng liên kết mạng (Network Access Layer)
- Tầng Internet (Internet Layer)
- Tầng giao vận (Host-to-Host Transport Layer)
- Tầng ứng dụng (Application Layer)




Hình II-6 : Kiến trúc TCP/IP

**Tầng liên kết**:

Tầng liên kết (còn được gọi là tầng liên kết dữ liệu hay là tầng giao tiếp mạng) là tầng thấp nhất trong mô hình TCP/IP, bao gồm các thiết bị giao tiếp mạng và chương trình cung cấp các thông tin cần thiết để có thể hoạt động, truy nhập đường truyền vật lý qua thiết bị giao tiếp mạng đó.

**Tầng Internet**:

Tầng Internet (còn gọi là tầng mạng) xử lý qua trình truyền gói tin trên mạng. Các giao thức của tầng này bao gồm: IP (Internet Protocol), ICMP (Internet Control Message Protocol), IGMP (Internet Group Messages Protocol).

**Tầng giao vận**:

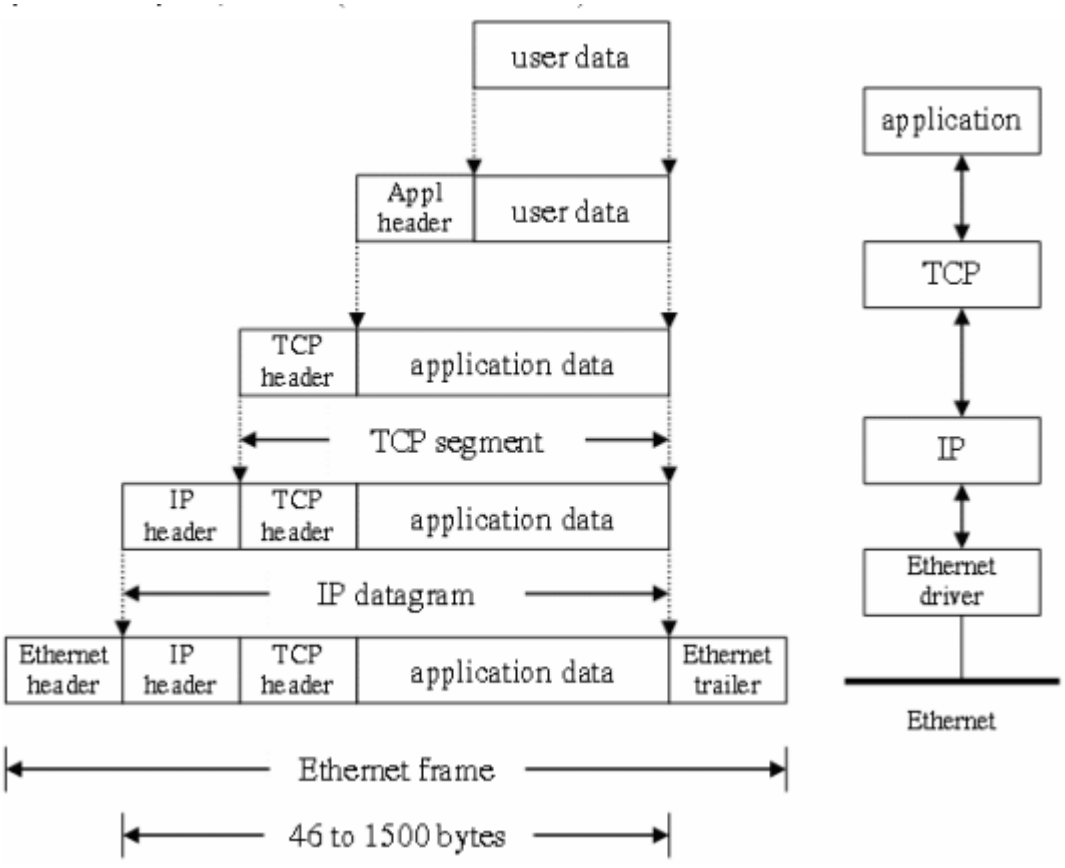
Tầng giao vận phụ trách luồng dữ liệu giữa hai trạm thực hiện các ứng dụng của tầng trên. Tầng này có hai giao thức chính: TCP (Transmission Control Protocol) và UDP (User Datagram Protocol)

TCP cung cấp một luồng dữ liệu tin cậy giữa hai trạm, nó sử dụng các cơ chế như chia nhỏ các gói tin của tầng trên thành các gói tin có kích thước thích hợp cho tầng mạng bên dưới, báo nhận gói tin,đặt hạn chế thời gian time-out để đảm bảo bên nhận biết được các gói tin đã gửi đi. Do tầng này đảm bảo tính tin cậy, tầng trên sẽ không cần quan tâm đến nữa.

UDP cung cấp một dịch vụ đơn giản hơn cho tầng ứng dụng. Nó chỉ gửi các gói dữ liệu từ trạm này tới trạm kia mà không đảm bảo các gói tin đến được tới đích. Các cơ chế đảm bảo độ tin cậy cần được thực hiện bởi tầng trên.

**Tầng ứng dụng:**

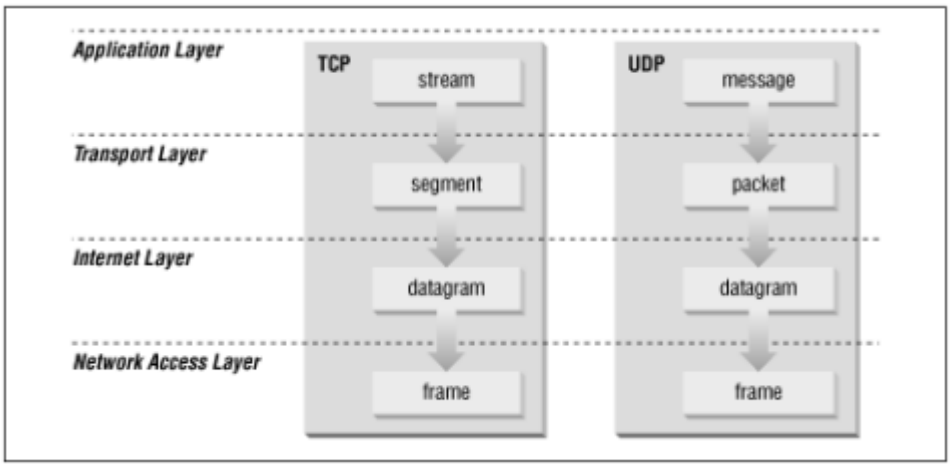
Tầng ứng dụng là tầng trên cùng của mô hình TCP/IP bao gồm các tiến trình và các ứng dụng cung cấp cho người sử dụng để truy cập mạng. Có rất nhiều ứng dụng được cung cấp trong tầng này, mà phổ biến là: Telnet: sử dụng trong việc truy cập mạng từ xa, FTP (File Transfer Protocol): dịch vụ truyền tệp, Email: dịch vụ thư tín điện tử, WWW (World Wide Web).




Hình II-7: Quá trình đóng/mở gói dữ liệu trong TCP/IP

Cũng tương tự như trong mô hình OSI, khi truyền dữ liệu, quá trình tiến hành từ tầng trên xuống tầng dưới, qua mỗi tầng dữ liệu được thêm vào một thông tin điều khiển được gọi là phần header. Khi nhận dữ liệu thì quá trình xảy ra ngược lại, dữ liệu được truyền từ tầng dưới lên và qua mỗi tầng thì phần header tương ứng được lấy đi và khi đến tầng trên cùng thì dữ liệu không còn phần header nữa. Hình vẽ sau cho ta thấy lược đồ dữ liệu qua các tầng. Trong hình vẽ này ta thấy tại các tầng khác nhau dữ liệu được mang những thuật ngữ khác nhau:

- Trong tầng ứng dụng dữ liệu là các luồng được gọi là stream.
- Trong tầng giao vận, đơn vị dữ liệu mà TCP gửi xuống tầng dưới gọi là TCP segment.
- Trong tầng mạng, dữ liệu mà IP gửi tới tầng dưới được gọi là IP datagram.
- Trong tầng liên kết, dữ liệu được truyền đi gọi là frame.




Hình II-8: Cấu trúc dữ liệu trong TCP/IP

## VI.2. So sánh TCP/IP với OSI

Mỗi tầng trong TCP/IP có thể là một hay nhiều tầng của OSI.

Bảng sau chỉ rõ mối tương quan giữa các tầng trong mô hình TCP/IP với OSI

| OSI | TCP/IP |
|---|---|
| Physical Layer và Data link Layer | Data link Layer |
| Network Layer | Internet Layer |
| Transport Layer | Transport Layer |
| Session Layer, Presentation Layer, Application Layer | Application Layer |

Sự khác nhau giữa TCP/IP và OSI chỉ là:

- Tầng ứng dụng trong mô hình TCP/IP bao gồm luôn cả 3 tầng trên của mô hình OSI
- Tầng giao vận trong mô hình TCP/IP không phải luôn đảm bảo độ tin cậy của việc truyền tin như ở trong tầng giao vận của mô hình OSI mà cho phép thêm một lựa chọn khác là UDP

# VII. Các giao thức truy cập đường truyền trên mạng LAN

Để truyền được dữ liệu trên mạng người ta phải có các thủ tục nhằm hướng dẫn các máy tính của mạng làm thế nào và lúc nào có thể thâm nhập vào đường dây cáp để gửi các gói dữ kiện. Ví dụ như đối với các dạng bus và ring thì chỉ có một đường truyền duy nhất nối các trạm với nhau, cho nên cần phải có các quy tắc chung cho tất cả các trạm nối vào mạng để đảm bảo rằng đường truyền được truy nhập và sử dụng một cách hợp lý.

Có nhiều giao thức khác nhau để truy nhập đường truyền vật lý nhưng phân thành hai loại: các giao thức truy nhập ngẫu nhiên và các giao thức truy nhập có điều khiển.

## VII.1. Giao thức chuyển mạch (yêu cầu và chấp nhận)

Giao thức chuyển mạch là loại giao thức hoạt động theo cách thức sau: một máy tính của mạng khi cần có thể phát tín hiệu thâm nhập vào mạng, nếu vào lúc này đường cáp không bận thì mạch điều khiển sẽ cho trạm này thâm nhập vào đường cáp còn nếu đường cáp đang bận, nghĩa là đang có giao lưu giữa các trạm khác, thì việc thâm nhập sẽ bị từ chối.

## VII.2. Giao thức đường dây đa truy cập với cảm nhận va chạm

Giao thức đường dây đa truy cập (Carrier Sense Multiple Access with Collision Detection hay CSMA/CD ) cho phép nhiều trạm thâm nhập cùng một lúc vào mạng, giao thức này thường dùng trong sơ đồ mạng dạng đường thẳng. Mọi trạm đều có thể được truy nhập vào đường dây chung một cách ngẫu nhiên và do vậy có thể dẫn đến xung đột (hai hoặc nhiều trạm đồng thời cùng truyền dữ liệu). Các trạm phải kiểm tra đường truyền gói dữ liệu đi qua có phải của nó hay không. Khi một trạm muốn truyền dữ liệu nó phải kiểm tra đường truyền xem có rảnh hay không để gửi gói dữ liệu của, nếu đường truyền đang bận trạm phải chờ đợi chỉ được truyền khi thấy đường truyền rảnh. Nếu cùng một lúc có hai trạm cùng sử dụng đường truyền thì giao thức phải phát hiện điều này và các trạm phải ngưng thâm nhập, chờ đợi lần sau các thời gian ngẫu nhiên khác nhau.

Khi đường cáp đang bận trạm phải chờ đợi theo một trong ba phương thức sau:

Trạm tạm chờ đợi một thời gian ngẫu nhiên nào đó rồi lại bắt đầu kiểm tra đường truyền.
Trạm tiếp tục kiểm tra đường truyền đến khi đường truyền rảnh thì truyền dữ liệu đi.
Trạm tiếp tục kiểm tra đường truyềnđến khi đường truyền rảnh thì truyền dữ liệu đi với xác suất p xác định trước ($0 < p < 1$).

Tại đây phương thức 1 có hiệu quả trong việc tránh xung đột vì hai trạm cần truyền khi thấy đường truyền bận sẽ cùng rút lui và chờ đợi trong các thời gian ngẫu nhiên khác nhau. Ngược lại phương thức 2 cố gắng giảm thời gian trống của đường truyền bằng các cho phép trạm có thể truyền ngay sau khi một cuộc truyền kết thúc song nếu lúc đó có thêm một trạm khác đang đợi thì khả năng xảy ra xung đột là rất cao. Phương thức 3 với giá trị p phải lựa chọn hợp lý có thể tối thiểu hóa được khả năng xung đột lẫn thời gian trống của đường truyền.

Khi lưu lượng các gói dữ liệu cần di chuyển trên mạng quá cao, thì việc đụng độ có thể xảy ra với sồ lượng lớn có gây tắc nghẽn đường truyền dẫn đến làm chậm tốc độ truyền tin của hệ thống.

### VII.3. Giao thức dùng thẻ bài vòng (Token ring)

Đây là giao thức truy nhập có điều khiển chủ yếu dùng kỹ thuật chuyển thẻ bài (token) để cấp phát quyền truy nhập đường truyền tức là quyền được truyền dữ liệu đi. Thẻ bài ở đay là một đơn vị dữ liệu đặc biệt, có kích thước và nội dung (gồm các thông tin điều khiển) được quy định riêng cho mỗi giao thức. Theo giao thức dùng thẻ bài vòng trong đường cáp liên tục có một thẻ bài chạy quanh trong mạng Thẻ bài là một đơn vị dữ liệu đặc biệt trong đó có một bit biểu diễn trạng thái sử dụng của nó (bận hoặc rỗi). Một trạm muốn truyền dữ liệu thì phải đợi đến khi nhận được một thẻ bài rảnh. Khi đó trạm sẽ đổi bit trạng thái của thẻ bài thành bận, nép gói dữ liệu có kèm theo địa chỉ nơi nhận vào thẻ bài và truyền đi theo chiều của vòng.

Vì thẻ bài chạy vòng quang trong mạng kín và chỉ có một thẻ nên việc đụng độ dữ liệu không thể xẩy ra, do vậy hiệu suất truyền dữ liệu của mạng không thay đổi.

Trong các giao thức này cần giải quyết hai vấn đề có thể dẫn đến phá vỡ hệ thống. Một là việc mất thẻ bài làm cho trên vòng không còn thẻ bài lưu chuyển nữa. Hai là một thẻ bài bận lưu chuyển không dừng trên vòng.

### VII.4. Giao thức dùng thẻ bài cho dạng đường thẳng (Token bus)

Đây là giao thức truy nhập có điều khiển trong để cấp phát quyền truy nhập đường truyền cho các trạm đang có nhu cầu truyền dữ liệu, một thẻ bài được lưu chuyển trên một vòng logic thiết lập bởi các trạm đó. Khi một trạm có thẻ bài thì nó có quyền sử dụng đường truyền trong một thời gian xác định trước. Khi đã hết dữ liệu hoặc hết thời đoạn cho phép, trạm chuyển thẻ bài đến trạm tiếp theo trong vòng logic.

Như vậy trong mạng phải thiết lập được vòng logic (hay còn gọi là vòng ảo) bao gồm các trạm đang hoạt động nối trong mạng được xác định vị trí theo một chuỗi thứ tự mà trạm cuối cùng của chuỗi sẽ tiếp liền sau bởi trạm đầu tiên. Mỗi trạm được biết địa chỉ của các trạm kề trước và sau nó trong đó thứ tự của các trạm trên vòng logic có thể độc lập với thứ tự vật lý. Cùng với việc thiết lập vòng thì giao thức phải luôn luôn theo dõi sự thay đổi theo trạng thái thực tế của mạng.

## VIII. Các phương tiện kết nối mạng liên khu vực (WAN)

Bên cạnh phương pháp sử dụng đường điện thoại thuê bao để kết nối các mạng cục bộ hoặc mạng khu vực với nhau hoặc kết nối vào Internet, có một số phương pháp khác:

- **Đường thuê bao (leased line)**. Đây là phương pháp cũ nhất, là phương pháp truyền thống nhất cho sự nối kết vĩnh cửu. Bạn thuê đường dây từ công ty điện thoại (trực tiếp hoặc qua nhà cung cấp dịch vụ). Bạn cần phải cài đặt một "*Chanel Service Unit*" (CSU) để nối đến mạng T, và một "*Digital Service Unit*" (DSU) để nối đến mạng chủ (primary) hoặc giao diện mạng.
- **ISDN (Integrated Service Digital Nework).** Sử dụng đường điện thoại số thay vì đường tương tự. Do ISDN là mạng dùng tín hiệu số, bạn không phải dùng một modem để nối với đường dây mà thay vào đó bạn phải dùng một thiết bị gọi là "*codec*" với modem có khả năng chạy ở 14.4 kbit/s. ISDN thích hợp cho cả hai trường hợp cá nhân và tổ chức. Các tổ chức có thể quan tâm hơn đến ISDN có khả năng cao hơn ("*primary*" ISDN) với tốc độ tổng cộng bằng tốc độ 1.544 Mbit/s của đường T1. Cước phí khi sử dụng ISDN được tính theo thời gian, một số trường hợp tính theo lượng dữ liệu được truyền đi và một số thì tính theo cả hai.

- **CATV link**. Công ty dẫn cáp trong khu vực của bạn có thể cho bạn thuê một "chỗ" trên đường cáp của họ với giá hấp dẫn hơn với đường điện thoại. Cần phải biết những thiết bị gì cần cho hệ thống của mình và độ rộng của dải mà bạn sẽ được cung cấp là bao nhiêu. Cũng như việc đóng góp chi phí với những khách hàng khác cho kênh liên lạc đó là như thế nào. Một dạng kỳ lạ hơn được đưa ra với tên gọi là mạng "lai" ("*hybrid" Network*), với một kênh CATV được sử dụng để lưu thông theo một hướng và một đường ISDN hoặc gọi số sử dụng cho đường trở lại. Nếu muốn cung cấp thông tin trên Internet, bạn phải xác định chắc chắn rằng "kênh ngược" của bạn đủ khả năng phục vụ cho nhu cầu thông tin của khách hàng của bạn.
- **Frame relay.** Frame relay "uyển chuyển" hơn đường thuê bao. Khách hàng thuê đường Frame relay có thể mua một dịch vụ có mức độ xác định - một "tốc độ thông tin uỷ thác" ("*Committed Information Rale" - CIR*). Nếu như nhu cầu của bạn trên mạng là rất "bột phát" (*burty*), hay người sử dụng của bạn có nhu cầu cao trên đường liên lạc trong suốt một khoảng thời gian xác định trong ngày, và có ít hoặc không có nhu cầu vào ban đêm - Frame relay có thể sẽ kinh tế hơn là thuê hoàn toàn một đường T1 (hoặc T3). Nhà cung cấp dịch vụ của bạn có thể đưa ra một phương pháp tương tự như là phương pháp thay thế đó là *Switched Multimegabit Data Service.*
- **Chế độ truyền không đồng bộ (Asynchoronous Trangfer Mode - ATM)**. ATM là một phương pháp tương đối mới đầu tiên báo hiệu cùng một kỹ thuật cho mạng cục bộ và liên khu vực. ATM thích hợp cho *real-time multimedia* song song với truyền dữ liệu truyền thống. ATM hứa hẹn sẽ trở thành một phần lớn của mạng tương lai.
- **Đường vi sóng (Microware links)**. Nếu cần kết nối vĩnh viễn đến nhà cung cấp dịch vụ nhưng lại thấy rằng đường thuê bao hay những lựa chọn khác là quá đắt, bạn sẽ thấy *microware* như là một lựa chọn thích hợp. Bạn không cần trả quá đắt cho cách này của *microware*, tuy nhiên bạn cần phải đầu tư nhiều tiền hơn vào lúc đầu, và bạn sẽ gặp một số rủi ro như tốc độ truyền đến mạng của bạn quá nhanh.
- **Đường vệ tinh (satellite links).** Nếu bạn muốn được chuyển một lượng lớn dữ liệu đặc biệt là từ những địa điểm từ xa thì đường vệ tinh là câu trả lời. Tầm hoạt động của những vệ tinh cùng vị trí địa lý với trái đất cũng tạo ra một sự chậm trễ (hoặc "bị che dấu") mà những người sử dụng Telnet có thể cảm nhận được.

# Chương III Địa chỉ IP

## I. Giao thức TCP/IP

Giao thức TCP/IP được phát triển từ mạng ARPANET và Internet và được dùng như giao thức mạng và vận chuyển trên mạng Internet. TCP (Transmission Control Protocol) là giao thức thuộc tầng vận chuyển và IP (Internet Protocol) là giao thức thuộc tầng mạng của mô hình OSI. Họ giao thức TCP/IP hiện nay là giao thức được sử dụng rộng rãi nhất để liên kết các máy tính và các mạng.

Hiện nay các máy tính của hầu hết các mạng có thể sử dụng giao thức TCP/IP để liên kết với nhau thông qua nhiều hệ thống mạng với kỹ thuật khác nhau. Giao thức TCP/IP thực chất là một họ giao thức cho phép các hệ thống mạng cùng làm việc với nhau thông qua việc cung cấp phương tiện truyền thông liên mạng.

## II. Địa chỉ IP

### II.1. Tổng quát

Nhiệm vụ chính của giao thức IP là cung cấp khả năng kết nối các mạng con thành liên kết mạng để truyền dữ liệu, vai trò của IP là vai trò của giao thức tầng mạng trong mô hình OSI. Giao thức IP là một giao thức kiểu không liên kết (connectionlees) có nghĩa là không cần có giai đoạn thiết lập liên kết trước khi truyền dữ liệu.

Sơ đồ địa chỉ hóa để định danh các trạm (host) trong liên mạng được gọi là địa chỉ IP 32 bits (32 bit IP address). Mỗi giao diện trong 1 máy có hỗ trợ giao thức IP đều phải được gán 1 địa chỉ IP (một máy tính có thể gắn với nhiều mạng do vậy có thể có nhiều địa chỉ IP). Địa chỉ IP gồm 2 phần: địa chỉ mạng (netid) và địa chỉ máy (hostid). Mỗi địa chỉ IP có độ dài 32 bits được tách thành 4 vùng (mỗi vùng 1 byte), có thể biểu thị dưới dạng thập phân, bát phân, thập lục phân hay nhị phân. Cách viết phổ biến nhất là dùng ký pháp thập phân có dấu chấm (dotted decimal notation) để tách các vùng. Mục đích của địa chỉ IP là để định danh duy nhất cho một máy tính bất kỳ trên liên mạng.

Do tổ chức và độ lớn của các mạng con (subnet) của liên mạng có thể khác nhau, người ta chia các địa chỉ IP thành 5 lớp, ký hiệu là A, B, C, D và E. Trong lớp A, B, C chứa địa chỉ có thể gán được. Lớp D dành riêng cho lớp kỹ thuật multicasting. Lớp E được dành những ứng dụng trong tương lai.

Netid trong địa chỉ mạng dùng để nhận dạng từng mạng riêng biệt. Các mạng liên kết phải có địa chỉ mạng (netid) riêng cho mỗi mạng. Ở đây các bit đầu tiên của byte đầu tiên được dùng để định danh lớp địa chỉ (0 - lớp A, 10 - lớp B, 110 - lớp C, 1110 - lớp D và 11110 - lớp E).

Ở đây ta xét cấu trúc của các lớp địa chỉ có thể gán được là lớp A, lớp B, lớp C.

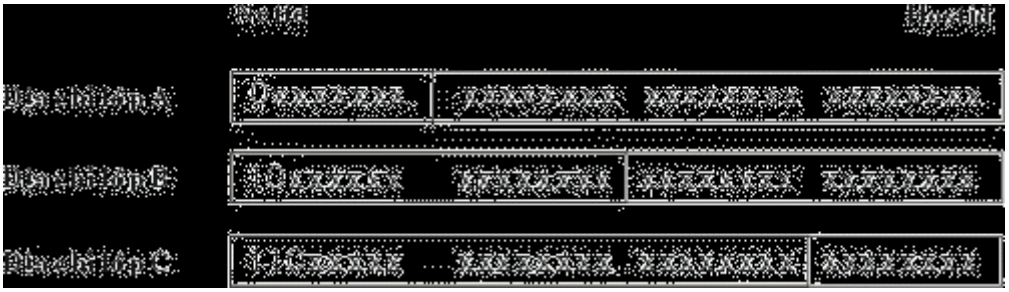
### II.2. Cấu trúc của các địa chỉ IP

Mạng lớp A: địa chỉ mạng (netid) là 1 Byte và địa chỉ host (hostid) là 3 byte.
Mạng lớp B: địa chỉ mạng (netid) là 2 Byte và địa chỉ host (hostid) là 2 byte.
Mạng lớp C: địa chỉ mạng (netid) là 3 Byte và địa chỉ host (hostid) là 1 byte.

Lớp A cho phép định danh tới 126 mạng, với tối đa 16 triệu host trên mỗi mạng. Lớp này được dùng cho các mạng có số trạm cực lớn.

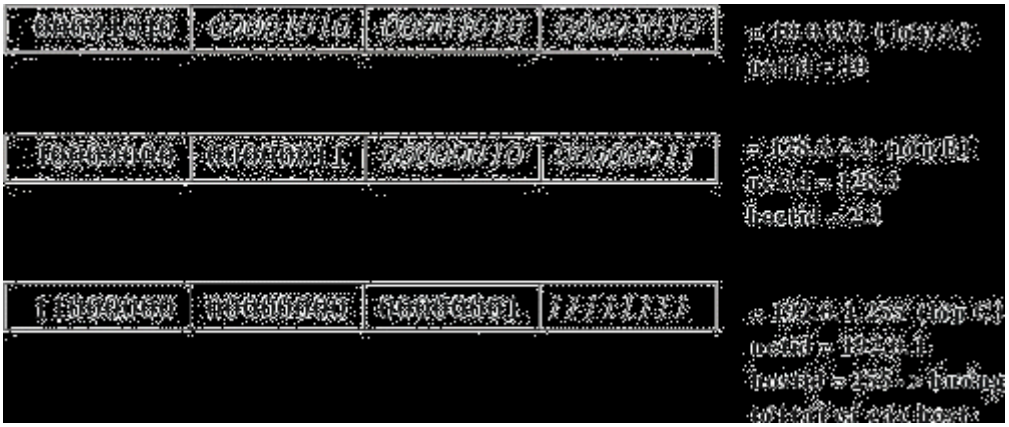
Lớp B cho phép định danh tới 16384 mạng, với tối đa 65534 host trên mỗi mạng.

Lớp C cho phép định danh tới 2 triệu mạng, với tối đa 254 host trên mỗi mạng. Lớp này được dùng cho các mạng có ít trạm.



Hình III-1: Cấu trúc các lớp địa chỉ IP

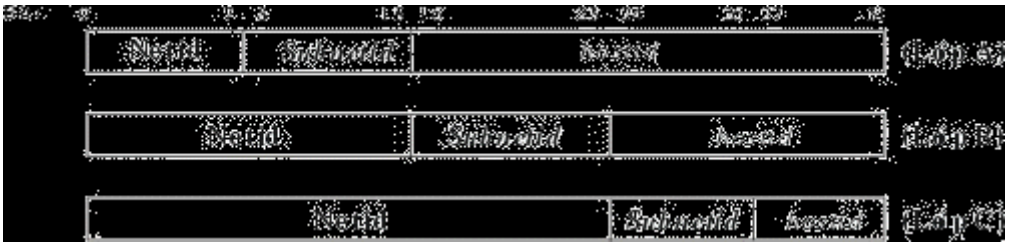
*Một số địa chỉ có tính chất đặc biệt*: Một địa chỉ có hostid = 0 được dùng để hướng tới mạng định danh bởi vùng netid. Ngược lại, một địa chỉ có vùng hostid gồm toàn số 1 được dùng để hướng tới tất cả các host nối vào mạng netid, và nếu vùng netid cũng gồm toàn số 1 thì nó hướng tới tất cả các host trong liên mạng



Hình III-2: Ví dụ cấu trúc các lớp địa chỉ IP

Cần lưu ý rằng các địa chỉ IP được dùng để định danh các host và mạng ở tầng mạng của mô hình OSI, và chúng không phải là các địa chỉ vật lý (hay địa chỉ MAC) của các trạm trên đó một mạng cục bộ (Ethernet, Token Ring.).

Trong nhiều trường hợp, một mạng có thể được chia thành nhiều mạng con (subnet), lúc đó có thể đưa thêm các vùng subnetid để định danh các mạng con. Vùng subnetid được lấy từ vùng hostid, cụ thể đối với lớp A, B, C như ví dụ sau:



Hình III-3: Ví dụ địa chỉ khi bổ sung vùng subnetid

Đơn vị dữ liệu dùng trong IP được gọi là gói tin (datagram), có khuôn dạng

Hình III-4: Dạng thức của gói tin IP

Ý nghĩa của thông số như sau:

- *VER* (4 bits)**:** chỉ version hiện hành của giao thức IP hiện được cài đặt, Việc có chỉ số version cho phép có các trao đổi giữa các hệ thống sử dụng version cũ và hệ thống sử dụng version mới.

- *IHL* (4 bits): chỉ độ dài phần đầu (Internet header Length) của gói tin datagram, tính theo đơn vị từ ( 32 bits). Trường này bắt buột phải có vì phần đầu IP có thể có độ dài thay đổi tùy ý. Độ dài tối thiểu là 5 từ (20 bytes), độ dài tối đa là 15 từ hay là 60 bytes.

- *Type of service* (8 bits): đặc tả các tham số về dịch vụ nhằm thông báo cho mạng biết dịch vụ nào mà gói tin muốn được sử dụng, chẳng hạn ưu tiên, thời hạn chậm trễ, năng suất truyền và độ tin cậy. Hình sau cho biết ý nghĩ của trường 8 bits này.

- Precedence (3 bit): chỉ thị về quyền ưu tiên gửi datagram, nó có giá trị từ 0 (gói tin bình thường) đến 7 (gói tin kiểm soát mạng).

- D (Delay) (1 bit): chỉ độ trễ yêu cầu trong đó

  - D = 0 gói tin có độ trễ bình thường

  - D = 1 gói tin độ trễ thấp

- T (Throughput) (1 bit): chỉ độ thông lượng yêu cầu sử dụng để truyền gói tin với lựa chọn truyền trên đường thông suất thấp hay đường thông suất cao.

  - T = 0 thông lượng bình thường và

  - T = 1 thông lượng cao

- R (Reliability) (1 bit): chỉ độ tin cậy yêu cầu

  - R = 0 độ tin cậy bình thường

  - R = 1 độ tin cậy cao

- *Total Length* (16 bits): chỉ độ dài toàn bộ gói tin, kể cả phần đầu tính theo đơn vị byte với chiều dài tối đa là 65535 bytes. Hiện nay giới hạn trên là rất lớn nhưng trong tương lai với những mạng Gigabit thì các gói tin có kích thước lớn là cần thiết.

- *Identification* (16 bits): cùng với các tham số khác (như Source Address và Destination Address) tham số này dùng để định danh duy nhất cho một datagram trong khoảng thời gian nó vẫn còn trên liên mạng.

- *Flags (3 bits):* liên quan đến sự phân đoạn (fragment) các datagram, Các gói tin khi đi trên đường đi có thể bị phân thành nhiều gói tin nhỏ, trong trường hợp bị phân đoạn thì trường Flags được dùng điều khiển phân đoạn và tái lắp ghép bó dữ liệu. Tùy theo giá trị của Flags sẽ có ý nghĩa là gói tin sẽ không phân đoạn, có thể phân đoạn hay là gói tin phân đoạn cuối cùng. Trường ***Fragment Offset*** cho biết vị trí dữ liệu thuộc phân đoạn tương ứng với đoạn bắt đầu của gói dữ liệu gốc. Ý nghĩa cụ thể của trường Flags là:

  - bit 0: reserved - chưa sử dụng, luôn lấy giá trị 0.

  - bit 1: (DF) = 0 (May Fragment) = 1 (Don't Fragment)

  - bit 2: (MF) = 0 (Last Fragment) = 1 (More Fragments)

- *Fragment Offset (13 bits)*: chỉ vị trí của đoạn (fragment) ở trong datagram tính theo đơn vị 8 bytes, có nghĩa là phần dữ liệu mỗi gói tin (trừ gói tin cuối cùng) phải chứa một vùng dữ liệu có độ dài là bội số của 8 bytes. Điều này có ý nghĩa là phải nhân giá trị của Fragment offset với 8 để tính ra độ lệch byte.

- *Time to Live (8 bits)*: qui định thời gian tồn tại (tính bằng giây) của gói tin trong mạng để tránh tình trạng một gói tin bị quẩn trên mạng. Thời gian này được cho bởi trạm gửi và được giảm đi (thường qui ước là 1 đơn vị) khi datagram đi qua mỗi router của liên mạng. Thời lượng này giảm xuống tại mỗi router với mục đích giới hạn thời gian tồn tại của các gói tin và kết thúc những lần lặp lại vô hạn trên mạng. Sau đây là 1 số điều cần lưu ý về trường ***Time To Live*****:**

  - Nút trung gian của mạng không được gởi 1 gói tin mà trường này có giá trị= 0.

  - Một giao thức có thể ấn định ***Time To Live*** để thực hiện cuộc ra tìm tài nguyên trên mạng trong phạm vi mở rộng.

  - Một giá trị cố định tối thiểu phải đủ lớn cho mạng hoạt động tốt.

- *Protocol (8 bits):* chỉ giao thức tầng trên kế tiếp sẽ nhận vùng dữ liệu ở trạm đích (hiện tại thường là TCP hoặc UDP được cài đặt trên IP). Ví dụ: **TCP** có giá trị trường **Protocol** là 6, **UDP** có giá trị trường **Protocol** là 17

- *Header Checksum (16 bits)*: Mã kiểm soát lỗi của header gói tin IP.

- *Source Address (32 bits)*: Địa chỉ của máy nguồn.

- Destination Address (32 bits): địa chỉ của máy đích

- *Options (độ dài thay đổi)*: khai báo các lựa chọn do người gửi yêu cầu (tuỳ theo từng chương trình).

- *Padding (độ dài thay đổi)*: Vùng đệm, được dùng để đảm bảo cho phần header luôn kết thúc ở một mốc 32 bits.

- *Data (độ dài thay đổi)*: Trên một mạng cục bộ như vậy, hai trạm chỉ có thể liên lạc với nhau nếu chúng biết địa chỉ vật lý của nhau. Như vậy vấn đề đặt ra là phải thực hiện ánh xạ giữa địa chỉ IP (32 bits) và địa chỉ vật lý (48 bits) của một trạm.

## III. Một số khái niệm và thuật ngữ liên quan

**Địa chỉ mạng (Network Address)**: là địa chỉ IP mà giá trị của tất cả các bits ở phần nhận dạng máy tính đều là 0, được sử dụng để xác định một mạng.

Ví dụ : 10.0.0.0; 172.18.0.0 ; 192.1.1.0

**Địa chỉ quảng bá (Broadcast Address)** : Là địa chỉ IP mà giá trị của tất cả các bits ở phần nhận dạng máy tính đều là 1, được sử dụng để chỉ tất cả các máy tính trong mạng.

Ví dụ : 10.255.255.255, 172.18.255.255, 192.1.1.255

**Mặt nạ mạng chuẩn (Netmask)** : Là địa chỉ IP mà giá trị của các bits ở phần nhận dạng mạng đều là 1, các bits ở phần nhận dạng máy tính đều là 0. Như vậy ta có 3 mặt nạ mạng tương ứng cho 3 lớp mạng A, B và C là :

- Mặt nạ mạng lớp A : 255.0.0.0
- Mặt nạ mạng lớp B : 255.255.0.0
- Mặt nạ mạng lớp C : 255.255.255.0

Ta gọi chúng là các mặt nạ mạng mặc định (Default Netmask)

Lưu ý : Địa chỉ mạng, địa chỉ quảng bá, mặt nạ mạng không được dùng để đặt địa chỉ cho các máy tính

Địa chỉ mạng 127.0.0.0 là địa chỉ được dành riêng để đặt trong phạm vi một máy tính. Nó chỉ có giá trị cục bộ ( trong phạm vi một máy tính). Thông thường khi cài đặt giao thức IP thì máy tính sẽ được gián địa chỉ 127.0.0.1. Địa chỉ này thông thường để kiểm tra xem giao thức IP trên máy hiện tại có hoạt động không.

**Địa chỉ dành riêng cho mạng cục bộ không nối kết trực tiếp Internet:** Các mạng cục bộ không nối kết trực tiếp vào mạng Internet có thể sử dụng các địa chỉ mạng sau để đánh địa chỉ cho các máy tính trong mạng của mình :
- Lớp A : 10.0.0.0
- Lớp B : 172.16.0.0 đến 172.32.0.0
- Lớp C : 192.168.0.0

**Ý nghĩa của Netmask**

Với một địa chỉ IP và một Netmask cho trước, ta có thể dùng phép toán AND BIT để tính ra được địa chỉ mạng mà địa chỉ IP này thuộc về. Công thức như sau :

Network Address = IP Address & Netmask

Ví dụ : Cho địa chỉ IP = 198.53.147.45 và Netmask = 255.255.255.0. Ta thực hiện phép toán AND BIT (&) hai địa chỉ trên:

| | Biểu diễn thập phân | Biểu diễn nhị phân |
|---|---|---|
| IP Address | 198.53.147.45 | 11000110 00110101 10010011 00101101 |
| Netmask | 255.255.255.0 | 11111111 11111111 11111111 00000000 |
| Network Address | 198.53.147.0 | 11000110 00110101 10010011 00000000 |

## III.1. Các giao thức trong mạng IP

Để mạng với giao thức IP hoạt động được tốt người ta cần một số giao thức bổ sung, các giao thức này đều không phải là bộ phận của giao thức IP và giao thức IP sẽ dùng đến chúng khi cần.

- ***Giao thức ARP (Address Resolution Protocol):*** Ở đây cần lưu ý rằng các địa chỉ IP được dùng để định danh các host và mạng ở tầng mạng của mô hình OSI, và chúng không phải là các địa chỉ vật lý (hay địa chỉ MAC) của các trạm trên đó một mạng cục bộ (Ethernet, Token Ring.). Trên một mạng cục bộ hai trạm chỉ có thể liên lạc với nhau nếu chúng biết địa chỉ vật lý của nhau. Như vậy vấn đề đặt ra là phải tìm được ánh xạ giữa địa chỉ IP (32 bits) và địa chỉ vật lý của một trạm. *Giao thức ARP* đã được xây dựng để tìm địa chỉ vật lý từ địa chỉ IP khi cần thiết.

- ***Giao thức RARP (Reverse Address Resolution Protocol)***: Là giao thức ngược với *giao thức ARP*. Giao thức RARP được dùng để tìm địa chỉ IP từ địa chỉ vật lý.

- ***Giao thức ICMP (Internet Control Message Protocol):*** Giao thức này thực hiện truyền các thông báo điều khiển (báo cáo về các tình trạng các lỗi trên mạng.) giữa các gateway hoặc một nút của liên mạng. Tình trạng lỗi có thể là: một gói tin IP không thể tới đích của nó, hoặc một router không đủ bộ nhớ đệm để lưu và chuyển một gói tin IP, Một thông báo ICMP được tạo và chuyển cho IP. IP sẽ "bọc" (encapsulate) thông báo đó với một IP header và truyền đến cho router hoặc trạm đích.

## III.2. Các bước hoạt động của giao thức IP

Khi giao thức IP được khởi động nó trở thành một thực thể tồn tại trong máy tính và bắt đầu thực hiện những chức năng của mình, lúc đó thực thể IP là cấu thành của tầng mạng, nhận yêu cầu từ các tầng trên nó và gửi yêu cầu xuống các tầng dưới nó.

Đối với thực thể IP ở máy nguồn, khi nhận được một yêu cầu gửi từ tầng trên, nó thực hiện các bước sau đây:

- Tạo một IP datagram dựa trên tham số nhận được.
- Tính checksum và ghép vào header của gói tin.
- Ra quyết định chọn đường: hoặc là trạm đích nằm trên cùng mạng hoặc một gateway sẽ được chọn cho chặng tiếp theo.
- Chuyển gói tin xuống tầng dưới để truyền qua mạng.

Đối với router, khi nhận được một gói tin đi qua, nó thực hiện các động tác sau:

1) Tính chesksum, nếu sai thì loại bỏ gói tin.

2) Giảm giá trị tham số Time - to Live. nếu thời gian đã hết thì loại bỏ gói tin.

3) Ra quyết định chọn đường.

4) Phân đoạn gói tin, nếu cần.

5) Kiến tạo lại IP header, bao gồm giá trị mới của các vùng Time - to -Live, Fragmentation và Checksum.

6) Chuyển datagram xuống tầng dưới để chuyển qua mạng.

Cuối cùng khi một datagram nhận bởi một thực thể IP ở trạm đích, nó sẽ thực hiện bởi các công việc sau:

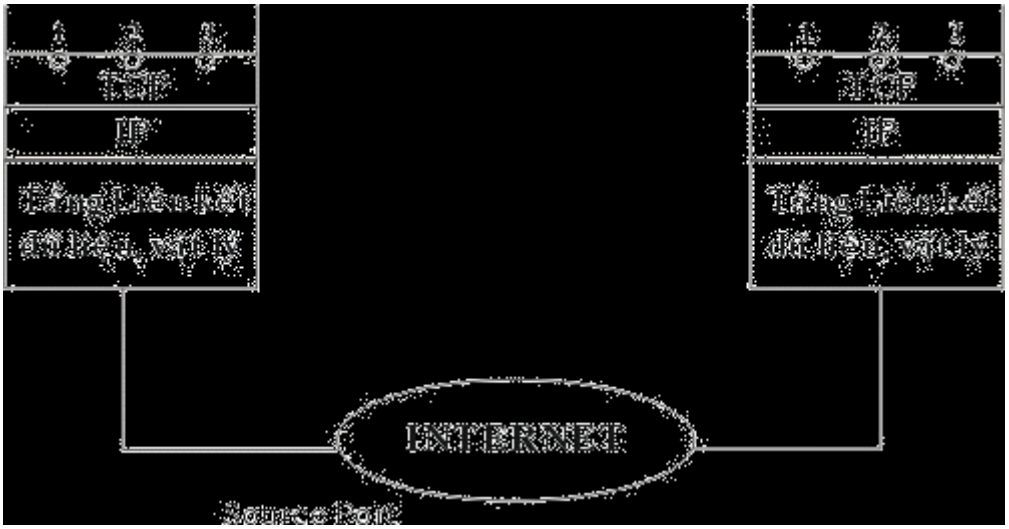
1) Tính checksum. Nếu sai thì loại bỏ gói tin.

2) Tập hợp các đoạn của gói tin (nếu có phân đoạn)

3) Chuyển dữ liệu và các tham số điều khiển lên tầng trên.

## IV. Giao thức điều khiển truyền dữ liệu TCP

TCP là một giao thức "có liên kết" (connection - oriented), nghĩa là cần phải thiết lập liên kết giữa hai thực thể TCP trước khi chúng trao đổi dữ liệu với nhau. Một tiến trình ứng dụng trong một máy tính truy nhập vào các dịch vụ của giao thức TCP thông qua một cổng (port) của TCP. Số hiệu cổng TCP được thể hiện bởi 2 bytes.



Hình III-5: Cổng truy nhập dịch vụ TCP

Một cổng TCP kết hợp với địa chỉ IP tạo thành một đầu nối TCP/IP (socket) duy nhất trong liên mạng. Dịch vụ TCP được cung cấp nhờ một liên kết logic giữa một cặp đầu nối TCP/IP. Một đầu nối TCP/IP có thể tham gia nhiều liên kết với các đầu nối TCP/IP ở xa khác nhau. Trước khi truyền dữ liệu giữa 2 trạm cần phải thiết lập một liên kết TCP giữa chúng và khi không còn nhu cầu truyền dữ liệu thì liên kết đó sẽ được giải phóng.

Các thực thể của tầng trên sử dụng giao thức TCP thông qua các hàm gọi (function calls) trong đó có các hàm yêu cầu để yêu cầu, để trả lời. Trong mỗi hàm còn có các tham số dành cho việc trao đổi dữ liệu.

## IV.1. Các bước thực hiện để thiết lập một liên kết TCP/IP:

Thiết lập một liên kết mới có thể được mở theo một trong 2 phương thức: chủ động (active) hoặc bị động (passive).

- Phương thức bị động, người sử dụng yêu cầu TCP chờ đợi một yêu cầu liên kết gửi đến từ xa thông qua một đầu nối TCP/IP (tại chỗ). Người sử dụng dùng hàm passive Open có khai báo cổng TCP và các thông số khác (mức ưu tiên, mức an toàn)

- Với phương thức chủ động, người sử dụng yêu cầu TCP mở một liên kết với một một đầu nối TCP/IP ở xa. Liên kết sẽ được xác lập nếu có một hàm Passive Open tương ứng đã được thực hiện tại đầu nối TCP/IP ở xa đó.

Bảng III-1 Lệt kê một vài cổng TCP phổ biến

| Số hiệu cổng | Mô tả |
|---|---|
| 0 | Reserved |
| 5 | Remote job entry |
| 7 | Echo |

| | |
|---|---|
| 9 | Discard |
| 11 | Systat |
| 13 | Daytime |
| 15 | Nestat |
| 17 | Quotd (quote odd day) |
| 20 | ftp-data |
| 21 | ftp (control) |
| 23 | Telnet |
| 25 | SMTP |
| 37 | Time |
| 53 | Name Server |
| 102 | ISO - TSAP |
| 103 | X.400 |
| 104 | X.400 Sending |
| 111 | Sun RPC |
| 139 | Net BIOS Session source |
| 160 - 223 | Reserved |

Khi người sử dụng gửi đi một yêu cầu mở liên kết sẽ được nhận hai thông số trả lời từ TCP.

- Thông số Open ID được TCP trả lời ngay lập tức để gán cho một liên kết cục bộ (local connection name) cho liên kết được yêu cầu. Thông số này về sau được dùng để tham chiếu tới liên kết đó. (Trong trường hợp nếu TCP không thể thiết lập được liên kết yêu cầu thì nó phải gửi tham số Open Failure để thông báo.)

- Khi TCP thiết lập được liên kết yêu cầu nó gửi tham số Open Sucsess được dùng để thông báo liên kết đã được thiết lập thành công. Thông báo này dược chuyển đến trong cả hai trường hợp bị động và chủ động. Sau khi một liên kết được mở, việc truyền dữ liệu trên liên kết có thể được thực hiện.

## IV.2. Các bước thực hiện khi truyền và nhận dữ liệu

Sau khi xác lập được liên kết người sữ dụng gửi và nhận dữ liệu. Việc gửi và nhận dữ liệu thông qua các hàm Send và receive.

- *Hàm Send:* Dữ liệu được gửi xuống TCP theo các khối (block). Khi nhận được một khối dữ liệu, TCP sẽ lưu trữ trong bộ đệm (buffer). Nếu cờ PUSH được dựng thì toàn bộ dữ liệu trong bộ đệm được gửi, kể cả khối dữ liệu mới đến sẽ được gửi đi. Ngược lại cờ PUSH không được dựng thì dữ liệu được giữ lại trong bộ đệm và sẽ gửi đi khi có cơ hội thích hợp (chẳng hạn chờ thêm dữ liệu nữa để gữi đi với hiệu quả hơn).

- *Hàm reveive*: Ở trạm đích dữ liệu sẽ được TCP lưu trong bộ đệm gắn với mỗi liên kết. Nếu dữ liệu được đánh dấu với một cờ PUSH thì toàn bộ dữ liệu trong bộ đệm (kể cả các dữ liệu được lưu từ trước) sẽ được chuyển lên cho người sữ dụng. Còn nếu dữ liệu đến không được đánh dấu với cờ PUSH thì TCP chờ tới khi thích hợp mới chuyển dữ liệu với mục tiêu tăng hiệu quả hệ thống.

Nói chung việc nhận và giao dữ liệu cho người sử dụng đích của TCP phụ thuộc vào việc cài đặt cụ thể. Trường hợp cần chuyển gấp dữ liệu cho người sử dụng thì có thể dùng cờ URGENT và đánh dấu dữ liệu bằng bit URG để báo cho người sử dụng cần phải sử lý khẩn cấp dữ liệu đó.

## IV.3. Các bước thực hiện khi đóng một liên kết

Việc đóng một liên kết khi không cần thiết được thực hiên theo một trong hai cách: *dùng hàm Close* hoặc dùng *hàm Abort*.

- *Hàm Close*: Yêu cầu đóng liên kết một cách bình thường. Có nghĩa là việc truyền dữ liệu trên liên kết đó đã hoàn tất. Khi nhận được một *hàm Close* TCP sẽ truyền đi tất cả dữ liệu còn trong bộ đệm thông báo rằng nó đóng liên kết. Lưu ý rằng khi một người sử dụng đã gửi đi một *hàm Close* thì nó vẫn phải tiếp tục nhận dữ liệu đến trên liên kết đó cho đến khi TCP đã báo cho phía bên kia biết về việc đóng liên kết và chuyển giao hết tất cả dữ liệu cho người sử dụng của mình.

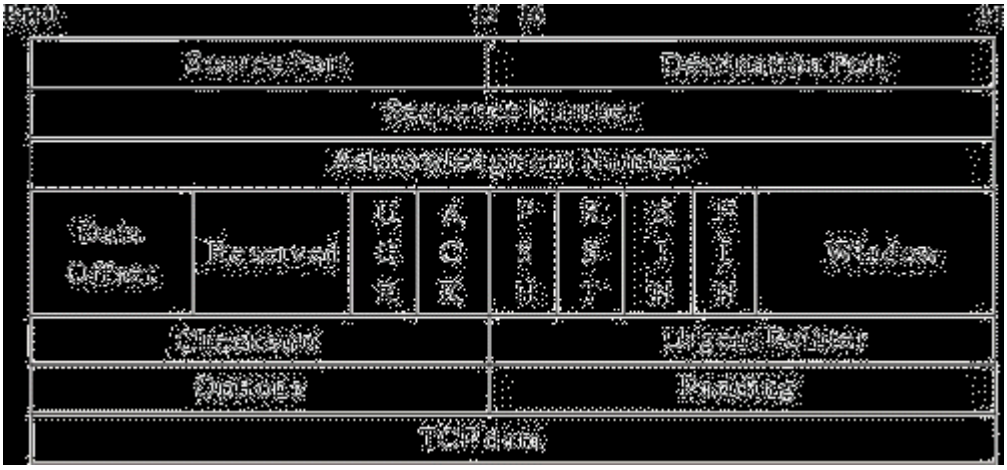
- *Hàm Abort*: Người sử dụng có thể đóng một liên kết bất và sẽ không chấp nhận dữ liệu qua liên kết đó nữa. Do vậy dữ liệu có thể bị mất đi khi đang được truyền đi. TCP báo cho TCP ở xa biết rằng liên kết đã được hủy bỏ và TCP ở xa sẽ thông báo cho người sử dụng cũa mình.

## IV.4. Một số hàm khác của TCP

- *Hàm Status*: cho phép người sử dụng yêu cầu cho biết trạng thái của một liên kết cụ thể, khi đó TCP cung cấp thông tin cho người sử dụng.

- *Hàm Error*: thông báo cho người sử dụng TCP về các yêu cầu dịch vụ bất hợp lệ liên quan đến một liên kết có tên cho trước hoặc về các lỗi liên quan đến môi trường.

Đơn vị dữ liệu sử dụng trong TCP được gọi là segment (đoạn dữ liệu), có các tham số với ý nghĩa như sau:



Hình III-6: Dạng thức của segment TCP

- Source Por (16 bits): Số hiệu cổng TCP của trạm nguồn.
- Destination Port (16 bit): Số hiệu cổng TCP của trạm đích.
- Sequence Number (32 bit): số hiệu của byte đầu tiên của segment trừ khi bit SYN được thiết lập. Nếy bit SYN được thiết lập thì Sequence Number là số hiệu tuần tự khởi đầu (ISN) và byte dữ liệu đầu tiên là ISN+1.
- Acknowledgment Number (32 bit): số hiệu của segment tiếp theo mà trạm nguồn đang chờ để nhận. Ngầm ý báo nhận tốt (các) segment mà trạm đích đã gửi cho trạm nguồn.
- Data offset (4 bit): số lượng bội của 32 bit (32 bit words) trong TCP header (tham số này chỉ ra vị trí bắt đầu của nguồn dữ liệu).
- Reserved (6 bit): dành để dùng trong tương lai
- Control bit (các bit điều khiển):
  - URG: Vùng con trỏ khẩn (Ucgent Poiter) có hiệu lực.
  - ACK: Vùng báo nhận (ACK number) có hiệu lực.
  - PSH: Chức năng PUSH.
  - RST: Khởi động lại (reset) liên kết.
  - SYN: Đồng bộ hóa số hiệu tuần tự (sequence number).
  - FIN: Không còn dữ liệu từ trạm nguồn.
- Window (16 bit): cấp phát credit để kiểm soát nguồn dữ liệu (cơ chế cửa sổ). Đây chính là số lượng các byte dữ liệu, bắt đầu từ byte được chỉ ra trong vùng ACK number, mà trạm nguồn đã sẵn sàng để nhận.
- Checksum (16 bit): mã kiểm soát lỗi cho toàn bộ segment (header + data)

- Urgemt Poiter (16 bit): con trỏ này trỏ tới số hiệu tuần tự của byte đi theo sau dữ liệu khẩn. Vùng này chỉ có hiệu lực khi bit URG được thiết lập.

- Options (độ dài thay đổi): khai báo các option của TCP, trong đó có độ dài tối đa của vùng TCP data trong một segment.

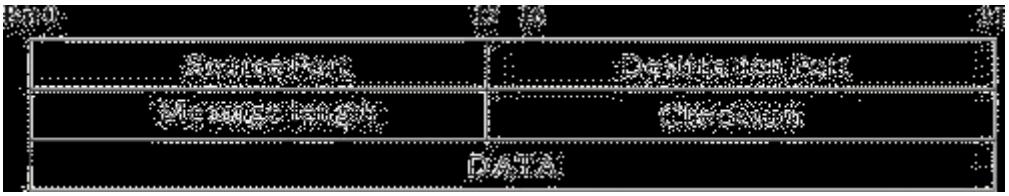
- Paddinh (độ dài thay đổi): phần chèn thêm vào header để đảm bảo phần header luôn kết thúc ở một mốc 32 bit. Phần thêm này gồm toàn số 0.

- TCP data (độ dài thay đổi): chứa dữ liệu của tầng trên, có độ dài tối đa ngầm định là 536 byte. Giá trị này có thể điều chỉnh bằng cách khai báo trong vùng options.

## V. Giao thức UDP (User Datagram Protocol)

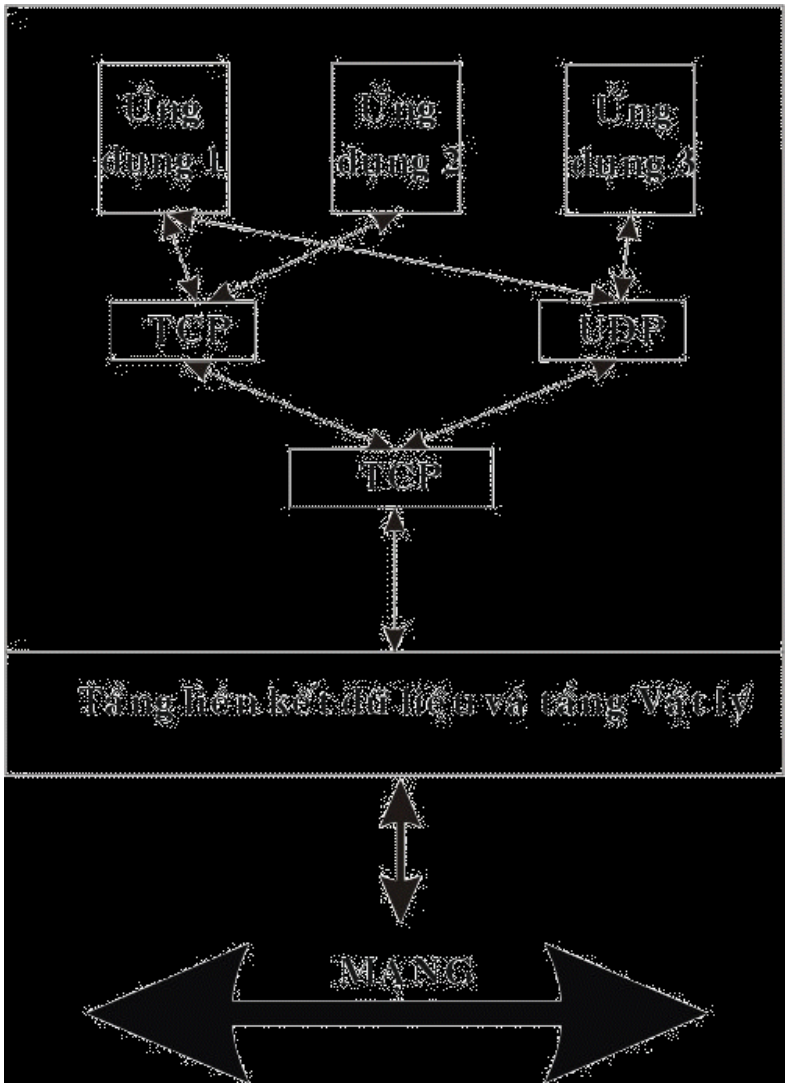
UDP (User Datagram Protocol) là giao thức theo phương thức không liên kết được sử dụng thay thế cho TCP ở trên IP theo yêu cầu của từng ứng dụng. Khác với TCP, UDP không có các chức năng thiết lập và kết thúc liên kết. Tương tự như IP, nó cũng không cung cấp cơ chế báo nhận (acknowledgment), không sắp xếp tuần tự các gói tin (datagram) đến và có thể dẫn đến tình trạng mất hoặc trùng dữ liệu mà không có cơ chế thông báo lỗi cho người gửi. Qua đó ta thấy UDP cung cấp các dịch vụ vận chuyển không tin cậy như trong TCP.

Khuôn dạng UDP datagram được mô tả với các vùng tham số đơn giản hơn nhiều so với TCP segment.



Hình III-7: Dạng thức của gói tin UDP

UDP cũng cung cấp cơ chế gán và quản lý các số hiệu cổng (port number) để định danh duy nhất cho các ứng dụng chạy trên một trạm của mạng. Do ít chức năng phức tạp nên UDP thường có xu thế hoạt động nhanh hơn so với TCP. Nó thường được dùng cho các ứng không đòi hỏi độ tin cậy cao trong giao vận.




Hình III-8: Mô hình quan hệ họ giao thức TCP/IP

# VI. Địa chỉ IPv4

## VI.1. Thành phần và hình dạng của địa chỉ IP

Địa chỉ IP đang được sử dụng hiện tại (IPv4) có 32 bit chia thành 4 Octet ( mỗi Octet có 8 bit, tương đương 1 byte ) cách đếm đều từ trái qua phải bit 1 cho đến bit 32, các Octet tách biệt nhau bằng dấu chấm (.), bao gồm có 3 thành phần chính.

Bit 1.....Bit 32

* Bit nhận dạng lớp ( Class bit )

* Địa chỉ của đường mạng ( Net ID )

* Địa chỉ của máy tính ( Host ID ).

Bit nhận dạng lớp (Class bit) để phân biệt địa chỉ ở lớp nào.

**1. Địa chỉ Internet biểu hiện ở dạng bit nhị phân:**

x y x y x y x y. x y x y x y x y. x y x y x y x y. x y x y x y x y

x, y = 0 hoặc 1.

Ví dụ:

| | | | | |
|---|---|---|---|---|
| **0** | **0 1 0 1 10.** | **0 1 1 1 1 0 1 1.** | **0 1 1 0 1 1 1 0.** | **1 1 1 0 0 0 0 0** |
| Bit nhận dạng | Octet 1 | Octet 2 | Octet 3 | Octet 4 |

**2. Địa chỉ Internet biểu hiện ở dạng thập phân:**

xxx.xxx.xxx.xxx

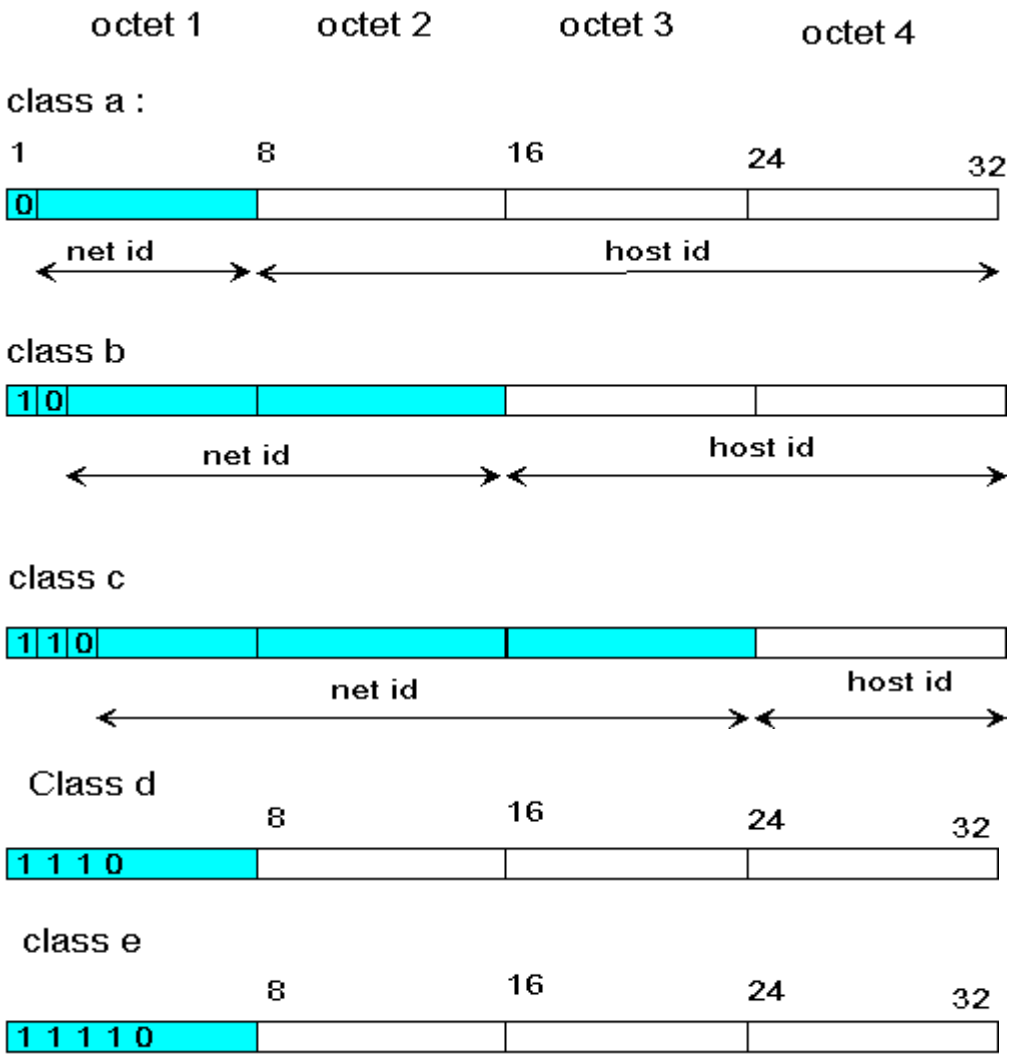
x là số thập phân từ 0 đến 9

Ví dụ: 146. 123. 110. 224

Dạng viết đầy đủ của địa chỉ IP là 3 con số trong từng Octet. Ví dụ: địa chỉ IP thường thấy trên thực tế có thể là 53.143.10.2 nhưng dạng đầy đủ là 053.143.010.002.

## VI.2. Các lớp địa chỉ IP

Địa chỉ IP chia ra 5 lớp A,B,C, D, E. Hiện tại đã dùng hết lớp A,B và gần hết lớp C, còn lớp D và E Tổ chức internet đang để dành cho mục đích khác không phân, nên chúng ta chỉ nghiên cứu 3 lớp đầu.




Qua cấu trúc các lớp địa chỉ IP chúng ta có nhận xét sau:

* Bit nhận dạng là những bit đầu tiên - của lớp A là 0, của lớp B là 10, của lớp C là 110.

* Lớp D có 4 bit đầu tiên để nhận dạng là 1110, còn lớp E có 5 bít đầu tiên để nhận dạng là 11110.

* Địa chỉ lớp A: Địa chỉ mạng ít và địa chỉ máy chủ trên từng mạng nhiều.

* Địa chỉ lớp B: Địa chỉ mạng vừa phải và địa chỉ máy chủ trên từng mạng vừa phải.

* Địa chỉ lớp C: Địa chỉ mạng nhiều, địa chỉ máy chủ trên từng mạng ít.

| Địa chỉ lớp | Vùng địa chỉ lý thuyết | Số mạng tối đa sử dụng | Số máy chủ tối đa trên từng mạng |
|---|---|---|---|
| A | Từ 0.0.0.0 đến 127.0.0.0 | 126 | 16777214 |
| B | Từ 128.0.0.0 đến 191.255.0.0 | 16382 | 65534 |
| C | Từ 192.0.0.0 đến 223.255.255.0 | 2097150 | 254 |

| | | | |
|---|---|---|---|
| D | Từ 224.0.0.0 đến 240.0.0.0 | Không phân | |
| E | Từ 241.0.0.0 đến 255.0.0.0 | Không phân | |

**Bảng III-2 Các lớp địa chỉ IP**

| Địa chỉ lớp | Vùng địa chỉ sử dụng | Bit nhận dạng | Số bit dùng để phân cho mạng |
|---|---|---|---|
| A | Từ 1 đến 127 | 0 | 7 |
| B | Từ 128.1 đến 191.254 | 10 | 14 |
| C | Từ 192.0.1 đến 223.255.254 | 110 | 21 |
| D | | 1110 | --- |
| E | | 11110 | --- |

**Bảng III-3 Bit nhận dạng các lớp**

Như vậy nếu chúng ta thấy 1 địa chỉ IP có 4 nhóm số cách nhau bằng dấu chấm, nếu thấy nhóm số thứ nhất nhỏ hơn 126 biết địa chỉ này ở lớp A, nằm trong khoảng 128 đến 191 biết địa chỉ này ở lớp B và từ 192 đến 223 biết địa chỉ này ở lớp C.

# VII. IPv6

## VII.1. Giao thức liên mạng thế hệ mới (IPv6)

Giao thức IPv4 đã được coi là nền tảng cho mạng Internet với những tính chất ưu việt của nó, tuy nhiên với sự bùng nổ về Internet giao thức IPv4 đã bộc lộ một số yếu điểm về tính năng, trong đó nổi bật là:

- Thiếu hụt về tính năng xác thực, an ninh của gói tin trên mạng. Khả năng mở rộng hạn chế.
- Thiếu hụt không gian địa chỉ. Với sự phát triển của mạng Internet, không gian địa chỉ IP có thể sử dụng thực sự là rất nhỏ do các địa chỉ lớp A được dành chủ yếu cho các công ty cung cấp dịch vụ lớn tại Mỹ và rất hạn chế trong việc cấp phát. Các địa chỉ lớp B nhanh chóng bị sử dụng hết do nó cung cấp số địa chỉ vừa phải. Hiện nay nhiều yêu cầu chỉ được đáp ứng bằng các địa chỉ lớp C với số địa chỉ rất hạn chế.
- Sự gia tăng số lượng các chỉ mục trong bảng định tuyến do cơ chế định tuyến không phân cấp dẫn đến yêu cầu nâng cấp các router và và định tuyến không hiệu quả.
- Ngày nay, với các nhu cầu kết nối vào mạng Internet của các dịch vụ khác như điện thoại di động, truyền hình số,… đòi hỏi giao thức IPv4 cần có các sửa đổi để đáp ứng các nhu cầu mới.

Trước những nhu cầu này, giao thức liên mạng thế hệ mới IPv6 đã ra đời nhằm thay thế cho IPv4, nhưng cho đến nay IPv6 vẫn chỉ mới chủ yếu là đang trong quá trình thử nghiệm và hoàn thiện. Trong khuôn khổ giáo trình cũng đề cập một cách tổng quát về giao thức liên mạng thế hệ mới IPv6.

## VII.2. Một số đặc điểm mới của IPv6:

- Khuôn dạng header mới: Header của IPv6 được thiết kế để giảm chi phí đến mức tối thiểu. Điều này đạt được bằng cách chuyển các trường lựa chọn sang các header

mở rộng được đặt phía sau của IPv6 header. Khuôn dạng mới của IPv6 tạo ra sự xử lý hiệu quả hơn tại các router.

− Header của IPv4 và IPv6 không thể xử lý chung. Một trạm hay một router phải cài đặt cả IPv4 và IPv6 để có thể xử lý được cả hai khuôn dạng header này. Header của IPv6 chỉ có kích thước gấp 2 lần header của IPv4 mặc dù không gian địa chỉ của IPv6 lớn gấp 4 lần không gian địa chỉ IPv4.

− Không gian địa chỉ lớn: IPv6 có địa chỉ nguồn và đích dài 128 bit. Mặc dù 128 bit có thể tạo ra hơn 3.4x1038 tổ hợp, không gian địa chỉ của IPv6 được thiết kế cho phép phân bổ địa chỉ và mạng con từ trục xương sống Internet đến từng mạng con trong một tổ chức.

− Hiện tại chỉ một lượng nhỏ các địa chỉ hiện đang được phân bổ để sử dụng bởi các trạm, vẫn còn dư thừa rất nhiều địa chỉ sẵn sàng cho việc sử dụng trong tương lai.

− Hiệu quả, phân cấp địa chỉ hóa và hạ tầng định tuyến: Các địa chỉ toàn cục của IPv6 được thiết kế để tạo ra mọt hạ tầng định tuyến hiệu quả, phân cấp và có thể tổng quát hóa dựa trên sự phân cấp thường thấy của các nhà cung cấp dịch vụ (ISP) trên thực tế.

− Hỗ trợ chất lượng dịch vụ (QoS) tốt hơn: Các trường mới trong header của IPv6 định ra cách thức xử lý và định danh trên mạng. Giao thông trên mạng được định danh nhờ trường gán nhãn luồng (Flow Label) cho phép router có thể nhận ra và cung cấp các xử lý đặc biệt đối với các gói tin thuộc về một luồng nhất định, một chuẩn các gói tin giữa nguồn và đích.

Do giao thông mạng được xác định trong header, các dịch vụ QoS có thể được thực hiện ngay cả khi phần dữ liệu được mã hóa theo IPSec.

− Khả năng mở rộng: IPv6 có thể dễ dàng mở rộng thêm các tính năng mới bằng việc thêm các header mới sau header IPv6.

## VII.3. Kiến trúc địa chỉ trong IPv6:

### VII.3.1 Không gian địa chỉ:

− IPv6 sử dụng địa chỉ có độ dài lớn hơn IPv4 (128 bit so với 32 bit) do đó cung cấp không gian địa chỉ lớn hơn rất nhiều. Trong khi không gian địa chỉ 32 bit của IPv4 cho phép khoảng 4 tỷ địa chỉ, không gian địa chỉ của

IPv6 có thể có khoảng 3.4x1038 địa chỉ. Số lượng điạc hỉ này rất lớn, hỗ trợ khoảng 6.5x1023 địa chỉ trên mỗi mét vuông bề mặt trái đất. Địa chỉ IPv6 128 bit được chia thành các miền phân cấp theo trật tự trên Internet.

Nó tạo ra nhiều mức phân cấp và linh hoạt trong địa chỉ hóa và định tuyến còn đang thiếu trong IPv4.

− Không gian địa chỉ IPv6 được chia trên cơ sở các bit đầu trong địa chỉ. Trường có độ dài thay đổi bao gồm các bit đầu tiên trong địa chỉ gọi là tiền tố định dạng (Format Prefix) FP.

− Ban đầu chỉ mới có 15% lượng địa chỉ được sử dụng, 85% còn lại để dùng trong tương lai.

− Các tiền tố định dạng từ 001 đến 111, ngoại trừ kiểu địa chỉ multicast (1111 1111) đều bắt buộc có định danh giao diện theo khuôn dạng EUI-64.

− Các địa chỉ dự trữ không lẫn với các địa chỉ chưa cấp phát. Chúng chiếm 1/256 không gian địa chỉ (FP = 0000 0000) và dùng cho các địa chỉ chưa chỉ định, địa chỉ quay vòng và các địa chỉ IPv6 có nhúng IPv4

### VII.3.2 Cú pháp địa chỉ:

Các địa chỉ IPv6 dài 128 bit, khi viết mỗi nhóm 16 bit được biểu diễn thành một số nguyên không dấu dưới dạng hệ 16 và được phân tách bởi dấu hai chấm (:),

Ví dụ: FEDC:BA98:7654:3210:FEDC:BA98:7654:3210

Trên thực tế địa chỉ IPv6 thường có nhiều số 0, ví dụ địa chỉ:

1080:0000:0000:0000:0008:0800:200C:417A. Do đó cơ chế nén địa chỉ được dùng để biểu diễn dễ dàng hơn các loại địa chỉ dạng này. Ta không cần viết các số 0 ở đầu mỗi nhóm, ví dụ 0 thay cho 0000, 20 thay cho 0020.

Địa chỉ trong ví dụ trên sẽ trở thành 1080:0:0:0:8:800:200C:417A.

Hơn nữa ta có thể sử dụng ký hiệu :: để chỉ một chuỗi số 0. Địa chỉ trong ví dụ trên sẽ trở thành: 1080::8:800:200C:417A. Do địa chỉ IPv6 có độ dài cố định, ta có thể tính được số các bit 0 mà ký hiệu đó biểu diễn.

Tiền tố địa chỉ IPv6 được biểu diễn theo ký pháp CIDR như IPv4 như sau:

IPv6-address/prefix length trong đó IPv6-address là bất kỳ kiểu biểu diễn nào, còn prefix length là độ dài tiền tố theo bit.

Ví dụ: biểu diễn mạng con có tiền tố 80 bit: 1080:0:0:0:8::/80.

Với node address: 12AB:0:0:CD30:123:4567:89AB:CDEF,

prefix: 12AB:0:0:CD30::/60 có thể viết tắt thành

12AB:0:0:CD30:123:4567:89AB:CDEF/60

# Chương IV Thiết bị mạng

## I. Môi trường truyền dẫn

### I.1. Khái niệm

Trên một mạng máy tính, các dữ liệu được truyền trên một môi trường truyền dẫn (transmission media), nó là phương tiện vật lý cho phép truyền tải tín hiệu giữa các thiết bị. Có hai loại phương tiện truyền dẫn chủ yếu:

- Hữu tuyến (bounded media)

- Vô tuyến (boundless media)

Thông thường hệ thống mạng sử dụng hai loại tín hiệu là: digital và analog.

### I.2. Tần số truyền thông

Phương tiện truyền dẫn giúp truyền các tín hiệu điện tử từ máy tính này sang máy tính khác. Các tín hiệu điện tử này biểu diễn các giá trị dữ liệu theo dạng các xung nhị phân (bật/tắt). Các tín hiệu truyền thông giữa các máy tính và các thiết bị là các dạng sóng điện từ trải dài từ tần số radio đến tần số hồng ngoại.

Các sóng tần số radio thường được dùng để phát tín hiệu LAN. Các tần số này có thể được dùng với cáp xoắn đôi, cáp đồng trục hoặc thông qua việc truyền phủ sóng radio.

Sóng viba (microware) thường dùng truyền thông tập trung giữa hai điểm hoặc giữa các trạm mặt đất và các vệ tinh, ví dụ như mạng điện thoại cellular.

Tia hồng ngoại thường dùng cho các kiểu truyền thông qua mạng trên các khoảng cách tương đối ngắn và có thể phát được sóng giữa hai điểm hoặc từ một điểm phủ sóng cho nhiều trạm thu. Chúng ta có thể truyền tia hồng ngoại và các tần số ánh sáng cao hơn thông qua cáp quang.

### I.3. Các đặc tính của phương tiện truyền dẫn

Mỗi phương tiện truyền dẫn đều có những tính năng đặc biệt thích hợp với mỗi kiểu dịch vụ cụ thể, nhưng thông thường chúng ta quan tâm đến những yếu tố sau:

- Chi phí

- Yêu cầu cài đặt

- Độ bảo mật

- Băng thông (bandwidth): được xác định bằng tổng lượng thông tin có thể truyền dẫn trên đường truyền tại một thời điểm. Băng thông là một số xác định, bị giới hạn bởi phương tiện truyền dẫn, kỹ thuật truyền dẫn và thiết bị mạng được sử dụng. Băng thông là một trong những thông số dùng để phân tích độ hiệu quả của đường mạng. Đơn vị của băng thông:

+ Bps (Bits per second-số bit trong một giây): đây là đơn vị cơ bản của băng thông.

+ KBps (Kilobits per second): 1 KBps=103 bps=1000 Bps

+ MBps (Megabits per second): 1 MBps = 103 KBps

+ GBps (Gigabits per second): 1 GBps = 103 MBps

+ TBps (Terabits per second): 1 TBps = 103 GBPS.

- Thông lượng (Throughput): lượng thông tin thực sự được truyền dẫn trên thiết bị tại một thời điểm.

- Băng tầng cơ sở (baseband): dành toàn bộ băng thông cho một kênh truyền, băng tầng mở rộng (broadband):cho phép nhiều kênh truyền chia sẻ một phương tiện truyền dẫn (chia sẻ băng thông).

- Độ suy giảm (attenuation): độ đo sự suy yếu đi của tín hiệu khi di chuyển trên một phương tiện truyền dẫn. Các nhà thiết kế cáp phải chỉ định các giới hạn về chiều dài dây cáp vì khi cáp dài sẽ dẫn đến tình trạng tín hiệu yếu đi mà không thể phục hồi được.

- Nhiễu điện từ (Electromagnetic interference - EMI): bao gồm các nhiễu điện từ bên ngoài làm biến dạng tín hiệu trong một phương tiện truyền dẫn.

- Nhiễu xuyên kênh (crosstalk): hai dây dẫn đặt kề nhau làm nhiễu lẫn nhau.

### I.4. Các kiểu truyền dẫn.

Có các kiểu truyền dẫn như sau:

- **Đơn công (Simplex)**: Trong kiểu truyền dẫn này, thiết bị phát tín hiệu và thiết bị nhận tín hiệu được phân biệt rõ ràng, thiết bị phát chỉ đảm nhiệm vai trò phát tín hiệu, còn thiết bị thu chỉ đảm nhiệm vai trò nhận tín hiệu. Truyền hình là một ví dụ của kiểu truyền dẫn này.
- **Bán song công (Half-Duplex)**: trong kiểu truyền dẫn này, thiết bị có thể là thiết bị phát, vừa là thiết bị thu. Nhưng tại một thời điểm thì chỉ có thể ở một trạng thái (phát hoặc thu). Bộ đàm là thiết bị hoạt động ở kiểu truyền dẫn này.
- **Song công (Full-Duplex)**: trong kiểu truyền dẫn này, tại một thời điểm, thiết bị có thể vừa phát vừa thu. Điện thoại là một minh họa cho kiểu truyền dẫn này.

## II. Đường cáp truyền mạng

Đường cáp truyền mạng là cơ sở hạ tầng của một hệ thống mạng, nên nó rất quan trọng và ảnh hưởng rất nhiều đến khả năng hoạt động của mạng. Hiện nay người ta thường dùng 3 loại dây cáp là cáp xoắn cặp, cáp đồng trục và cáp quang.

### II.1. Cáp xoắn cặp

Đây là loại cáp gồm hai đường dây dẫn đồng được xoắn vào nhau nhằm làm giảm nhiễu điện từ gây ra bởi môi trường xung quanh và giữa chúng với nhau.

Hiện nay có hai loại cáp xoắn là cáp có bọc kim loại ( STP - Shield Twisted Pair) và cáp không bọc kim loại (UTP -Unshield Twisted Pair).

- Cáp có bọc kim loại (STP): Lớp bọc bên ngoài có tác dụng chống nhiễu điện từ, có loại có một đôi giây xoắn vào nhau và có loại có nhiều đôi giây xoắn với nhau.
- Cáp không bọc kim loại (UTP): Tính tương tự như STP nhưng kém hơn về khả năng chống nhiễu và suy hao vì không có vỏ bọc.

STP và UTP có các loại (Category - Cat) thường dùng:

- Loại 1 & 2 (Cat 1 & Cat 2): Thường dùng cho truyền thoại và những đường truyền tốc độ thấp (nhỏ hơn 4Mb/s).
- Loại 3 (Cat 3): tốc độ truyền dữ liệu khoảng 16 Mb/s , nó là chuẩn cho hầu hết các mạng điện thoại.
- Loại 4 (Cat 4): Thích hợp cho đường truyền 20Mb/s.
- Loại 5 (Cat 5): Thích hợp cho đường truyền 100Mb/s.
- Loại 6 (Cat 6): Thích hợp cho đường truyền 300Mb/s.

Đây là loại cáp rẻ, dễ cài đặt tuy nhiên nó dễ bị ảnh hưởng của môi trường.

## II.2. Cáp đồng trục

Cáp đồng trục có hai đường dây dẫn và chúng có cùng một trục chung, một dây dẫn trung tâm (thường là dây đồng cứng) đường dây còn lại tạo thành đường ống bao xung quanh dây dẫn trung tâm (dây dẫn này có thể là dây bện kim loại và vì nó có chức năng chống nhiễu nên còn gọi là lớp bọc kim). Giữa hai dây dẫn trên có một lớp cách ly, và bên ngoài cùng là lớp vỏ plastic để bảo vệ cáp.

| ***Các loại cáp*** | ***Dây xoắn cặp*** | ***Cáp đồng trục mỏng*** | ***Cáp đồng trục dày*** | ***Cáp quang*** |
|---|---|---|---|---|
| ***Chi tiết*** | Bằng đồng, có 4 và 25 cặp dây (loại 3, 4, 5) | Bằng đồng, 2 dây, đường kính 5mm | Bằng đồng, 2 dây, đường kính 10mm | Thủy tinh, 2 sợi |
| ***Loại kết nối*** | RJ-25 hoặc 50-pin telco | BNC | N-series | ST |
| ***Chiều dài đoạn tối đa*** | 100m | 185m | 500m | 1000m |
| ***Số đầu nối tối đa trên 1 đoạn*** | 2 | 30 | 100 | 2 |
| ***Chạy 10 Mbit/s*** | Được | Được | Được | Được |
| ***Chạy 100 Mbit/s*** | Được | Không | Không | Được |
| ***Chống nhiễu*** | Tốt | Tốt | Rất tốt | Hoàn toàn |
| ***Bảo mật*** | Trung bình | Trung bình | Trung bình | Hoàn toàn |
| ***Độ tin cậy*** | Tốt | Trung bình | Tốt | Tốt |
| ***Lắp đặt*** | Dễ dàng | Trung bình | Khó | Khó |
| ***Khắc phục lỗi*** | Tốt | Dở | Dở | Tốt |
| ***Quản lý*** | Dễ dàng | Khó | Khó | Trung bình |
| ***Chi phí cho 1 trạm*** | Rất thấp | Thấp | Trung bình | Cao |
| ***Ứng dụng tốt nhất*** | Hệ thống Workgroup | Đường backbone | Đường backbone trong tủ mạng | Đường backbone dài trong tủ mạng hoặc các tòa nhà |

**Bảng IV-1** ***Tính năng kỹ thuật của một số loại cáp mạng***

Cáp đồng trục có độ suy hao ít hơn so với các loại cáp đồng khác (ví dụ như cáp xoắn đôi) do ít bị ảnh hưởng của môi trường. Các mạng cục bộ sử dụng cáp đồng trục có thể có kích thước trong phạm vi vài ngàn mét, cáp đồng trục được sử dụng nhiều trong các mạng dạng đường thẳng. Hai loại cáp thường được sử dụng là cáp đồng trục mỏng và cáp đồng trục dày trong đường kính cáp đồng trục mỏng là 0,25 inch, cáp đồng trục dày là

0,5 inch. Cả hai loại cáp đều làm việc ở cùng tốc độ nhưng cáp đồng trục mỏng có độ hao suy tín hiệu lớn hơn

Hiện nay có cáp đồng trục sau:

- RG -58,50 ohm: dùng cho mạng Thin Ethernet
- RG -59,75 ohm: dùng cho truyền hình cáp
- RG -62,93 ohm: dùng cho mạng ARCnet

Các mạng cục bộ thường sử dụng cáp đồng trục có dải thông từ 2,5 - 10 Mb/s, cáp đồng trục có độ suy hao ít hơn so với các loại cáp đồng khác vì nó có lớp vỏ bọc bên ngoài, độ dài thông thường của một đoạn cáp nối trong mạng là 200m, thường sử dụng cho dạng Bus.

## II.3. Cáp sợi quang (Fiber - Optic Cable)

Cáp sợi quang bao gồm một dây dẫn trung tâm (là một hoặc một bó sợi thủy tinh có thể truyền dẫn tín hiệu quang) được bọc một lớp vỏ bọc có tác dụng phản xạ các tín hiệu trở lại để giảm sự mất mát tín hiệu. Bên ngoài cùng là lớp vỏ plastic để bảo vệ cáp. Như vậy cáp sợi quang không truyền dẫn các tín hiệu điện mà chỉ truyền các tín hiệu quang (các tín hiệu dữ liệu phải được chuyển đổi thành các tín hiệu quang và khi nhận chúng sẽ lại được chuyển đổi trở lại thành tín hiệu điện).

Cáp quang có đường kính từ 8.3 - 100 micron, Do đường kính lõi sợi thuỷ tinh có kích thước rất nhỏ nên rất khó khăn cho việc đấu nối, nó cần công nghệ đặc biệt với kỹ thuật cao đòi hỏi chi phí cao.

Dải thông của cáp quang có thể lên tới hàng Gbps và cho phép khoảng cách đi cáp khá xa do độ suy hao tín hiệu trên cáp rất thấp. Ngoài ra, vì cáp sợi quang không dùng tín hiệu điện từ để truyền dữ liệu nên nó hoàn toàn không bị ảnh hưởng của nhiễu điện từ và tín hiệu truyền không thể bị phát hiện và thu trộm bởi các thiết bị điện tử của người khác.

Chỉ trừ nhược điểm khó lắp đặt và giá thành còn cao , nhìn chung cáp quang thích hợp cho mọi mạng hiện nay và sau này.

## II.4. Các yêu cầu cho một hệ thống cáp

- **An toàn, thẩm mỹ**: Tất cả các dây mạng phải được bao bọc cẩn thận, cách xa các nguồn điện, các máy có khả năng phát sóng để tránh trường hợp bị nhiễu. Các đầu nối phải đảm bảo chất lượng, tránh tình trạng hệ thống mạng bị chập chờn.
- **Đúng chuẩn**: Hệ thống cáp phải thực hiện đúng chuẩn, đảm bảo cho khả năng nâng cấp sau này cũng như dễ dàng cho việc kết nối các thiết bị khác nhau của các nhà sản xuất khác nhau. Tiêu chuẩn quốc tế dùng cho các hệ thống mạng hiện nay là EIA/TIA 568B.
- **Tiết kiệm và "linh hoạt" (flexible)**: Hệ thống cáp phải được thiết kế sao cho kinh tế nhất, dễ dàng trong việc di chuyển các trạm làm việc và có khả năng mở rộng sau này.

# III. Đường truyền vô tuyến

Khi dùng các loại cáp ta gặp một số khó khăn như cơ sở cài đặt cố định, khoảng cách không xa, vì vậy để khắc phục những khuyết điểm trên người ta dùng đường truyền vô tuyến. Đường truyền vô tuyến mang lại những lợi ích sau:

- Cung cấp nối kết tạm thời với mạng cáp có sẵn.

- Những người liên tục di chuyển vẫn nối kết vào mạng dùng cáp.

- Lắp đặt đường truyền vô tuyến ở những nơi địa hình phức tạp không thể đi dây được.

- Phù hợp cho những nơi phục vụ nhiều kết nối cùng một lúc cho nhiều khách hàng. Ví dụ như: Dùng đường vô tuyến cho phép khách hàng ở sân bay kết vào mạng để duyệt Internet.

- Dùng cho những mạng có giới hạn rộng lớn vượt quá khả năng cho phép của cáp đồng và cáp quang.

- Dùng làm kết nối dự phòng cho các kết nối hệ thống cáp.

Tuy nhiên, đường truyền vô tuyến cũng có một số hạn chế:

- Tín hiệu không an toàn.

- Dễ bị nghe lén.

- Khi có vật cản thì tín hiệu suy yếu rất nhanh.

- Băng thông không cao.

## III.1. Sóng vô tuyến (radio)

Sóng radio nằm trong phạm vi từ 10 KHz đến 1 GHz, trong miền này ta có rất nhiều dải tần ví dụ như: sóng ngắn, VHF (dùng cho tivi và radio FM), UHF (dùng cho tivi). Tại mỗi quốc gia, nhà nước sẽ quản lý cấp phép sử dụng các băng tần để tránh tình trạng các sóng bị nhiễu. Nhưng có một số băng tần được chỉ định là vùng tự do có nghĩa là chúng ta dùng nhưng không cần đăng ký (vùng này thường có dải tần 2,4 Ghz). Tận dụng lợi điểm này các thiết bị Wireless của các hãng như Cisco, Compex đều dùng ở dải tần này. Tuy nhiên, chúng ta sử dụng tần số không cấp phép sẽ có nguy cơ nhiễu nhiều hơn.

## III.2. Sóng viba

Truyền thông viba thường có hai dạng: truyền thông trên mặt đất và các nối kết với vệ tinh. Miền tần số của viba mặt đất khoảng 21-23 GHz, các kết nối vệ tinh khoảng 11-14 Mhz. Băng thông từ 1-10 MBps.

Sự suy yếu tín hiệu tùy thuộc vào điều kiện thời tiết, công suất và tần số phát. Chúng dễ bị nghe trộm nên thường được mã hóa.

## III.3. Hồng ngoại

Tất cả mạng vô tuyến hồng ngoại đều hoạt động bằng cách dùng tia hồng ngoại để truyền tải dữ liệu giữa các thiết bị. Phương pháp này có thể truyền tín hiệu ở tốc độ cao do dải thông cao của tia hồng ngoại. Thông thường mạng hồng ngoại có thể truyền với tốc độ từ 1-10 Mbps. Miền tần số từ 100 Ghz đến 1000 GHz. Có bốn loại mạng hồng ngoại:

- **Mạng đường ngắm**: mạng này chỉ truyền khi máy phát và máy thu có một đường ngắm rõ rệt giữa chúng.

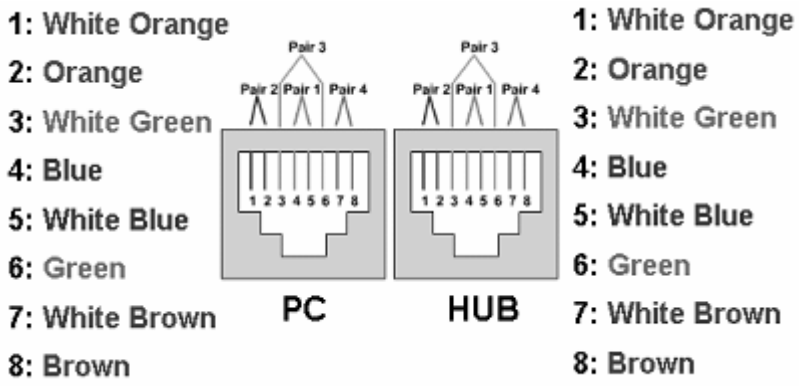
- **Mạng hồng ngoại tán xạ**: kỹ thuật này phát tia truyền dội tường và sàn nhà rồi mới đến máy thu. Diện tích hiệu dụng bị giới hạn ở khoảng 100 feet (35m) và có tín hiệu chậm do hiện tượng dội tín hiệu.

- **Mạng phản xạ**: ở loại mạng hồng ngoại này, máy thu-phát quang đặt gần máy tính sẽ truyền tới một vị trí chung, tại đây tia truyền được đổi hướng đến máy tính thích hợp.

- **Broadband optical telepoint**: loại mạng cục bộ vô tuyến hồng ngoại cung cấp các dịch vụ dải rộng. Mạng vô tuyến này có khả năng xử lý các yêu cầu đa phương tiện chất lượng cao, vốn có thể trùng khớp với các yêu cầu đa phương tiện của mạng cáp.

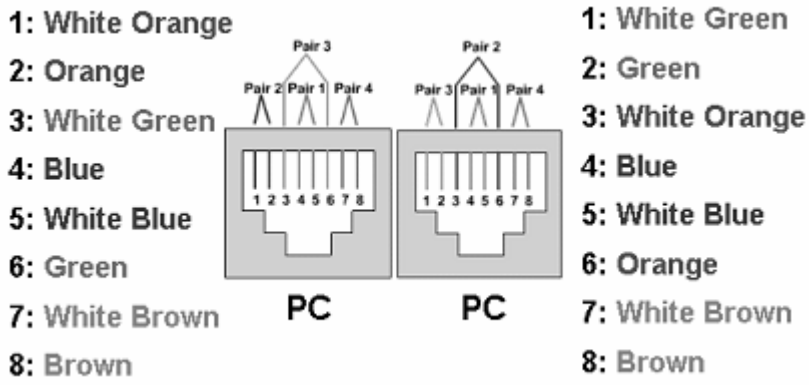
## IV. Các kỹ thuật bấm cáp mạng

- **Cáp thẳng (Straight-through cable)**: là cáp dùng để nối PC và các thiết bị mạng như Hub, Switch, Router… Cáp thẳng theo chuẩn 10/100 Base-T dùng hai cặp dây xoắn nhau và dùng chân 1, 2, 3, 6 trên đầu RJ45. Cặp dây xoắn thứ nhất nối vào chân 1, 2, cặp xoắn thứ hai nối vào chân 3, 6. Đầu kia của cáp dựa vào màu nối vào chân của đầu RJ45 và nối tương tự.




Hình IV-1: Cách đấu dây thẳng.

- **Cáp chéo (Crossover cable)**: là cáp dùng nối trực tiếp giữa hai thiết bị giống nhau như PC – PC, Hub – Hub, Switch – Switch. Cáp chéo trật tự dây cũng giống như cáp thẳng nhưng đầu dây còn lại phải chéo cặp dây xoắn sử dụng (vị trí thứ nhất đổi với vị trí thứ 3, vị trí thứ hai đổi với vị trí thứ sáu) .

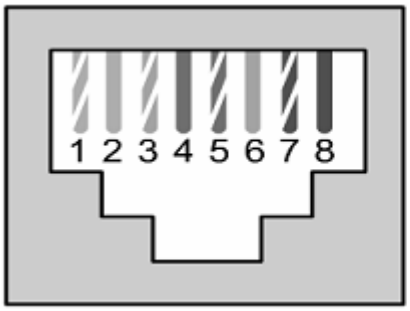



Hình IV-2: Cách đấu dây chéo.

- **Cáp Console**: Dùng để nối PC vào các thiết bị mạng chủ yếu dùng để cấu hình các thiết bị. Thông thường khoảng cách dây Console ngắn nên chúng ta không cần chọn cặp dây xoắn, mà chọn theo màu từ 1-8 sao cho dễ nhớ và đầu bên kia ngược lại từ 8-1.

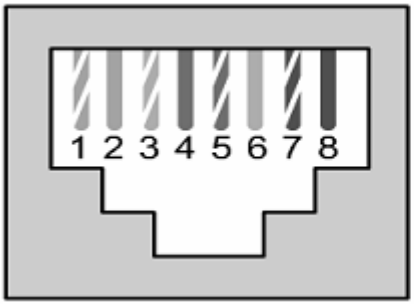
ANSI (Viện tiêu chuẩn quốc gia Hoa kỳ), TIA (hiệp hội công nghiệp viễn thông), EIA (hiệp hội công nghiệp điện tử) đã đưa ra 2 cách xếp đặt vị trí dây như sau:

- Chuẩn T568-A (còn gọi là Chuẩn A):




1. Trắng Xanh lá cây (White Green)
2. Xanh lá cây (Green)
3. Trắng Cam (White Orange)
4. Xanh đậm (Blue)
5. Trắng Xanh đậm (White Blue)
6. Cam (Orange)
7. Trắng Nâu (White Brown)
8. Nâu (Brown)

- Chuẩn T568-B (còn gọi là Chuẩn B):




1. Trắng Cam (White Orange)
2. Cam (Orange)
3. Trắng Xanh lá cây (White Green)
4. Xanh đậm (Blue)
5. Trắng Xanh đậm (White Blue)
6. Xanh lá cây (Green)
7. Trắng Nâu (White Brown)
8. Nâu (Brown)

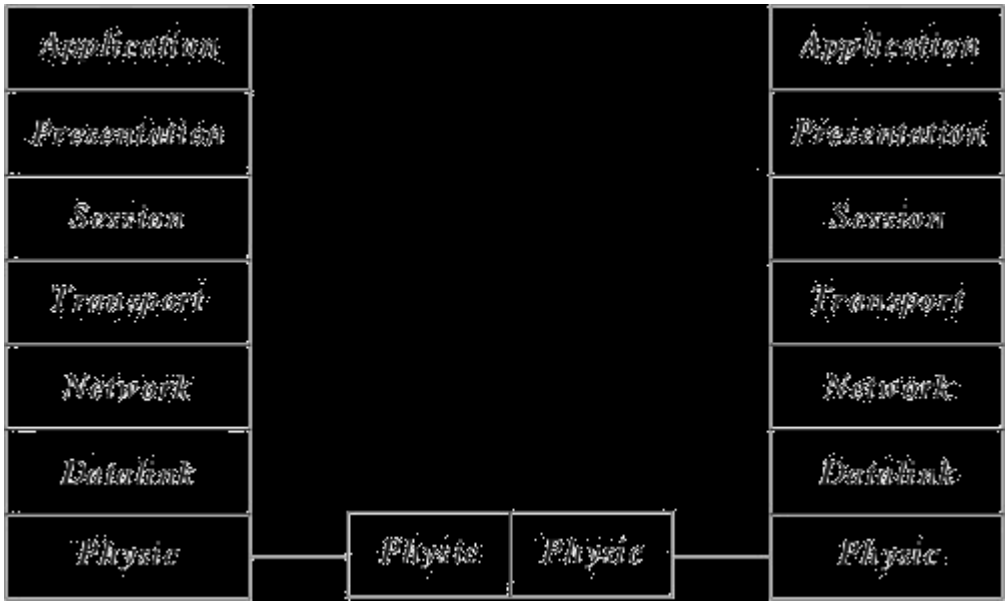
# V. Các thiết bị liên kết mạng

## V.1. Repeater (Bộ tiếp sức)

Repeater là loại thiết bị phần cứng đơn giản nhất trong các thiết bị liên kết mạng, nó được hoạt động trong tầng vật lý của mô hình hệ thống mở OSI. Repeater dùng để nối 2 mạng giống nhau hoặc các phần một mạng cùng có một nghi thức và một cấu hình. Khi Repeater nhận được một tín hiệu từ một phía của mạng thì nó sẽ phát tiếp vào phía kia của mạng.

Hình IV-3: Mô hình liên kết mạng của Repeater.

Repeater không có xử lý tín hiệu mà nó chỉ loại bỏ các tín hiệu méo, nhiễu, khuếch đại tín hiệu đã bị suy hao (vì đã được phát với khoảng cách xa) và khôi phục lại tín hiệu ban đầu. Việc sử dụng Repeater đã làm tăng thêm chiều dài của mạng.




Hình IV-4: Hoạt động của bộ tiếp sức trong mô hình OSI

Hiện nay có hai loại Repeater đang được sử dụng là Repeater điện và Repeater điện quang.

- Repeater điện nối với đường dây điện ở cả hai phía của nó, nó nhận tín hiệu điện từ một phía và phát lại về phía kia. Khi một mạng sử dụng Repeater điện để nối các phần của mạng lại thì có thể làm tăng khoảng cách của mạng, nhưng khoảng cách đó luôn bị hạn chế bởi một khoảng cách tối đa do độ trễ của tín hiệu. Ví dụ với mạng sử dụng cáp đồng trục 50 thì khoảng cách tối đa là 2.8 km, khoảng cách đó không thể kéo thêm cho dù sử dụng thêm Repeater.
- Repeater điện quang liên kết với một đầu cáp quang và một đầu là cáp điện, nó chuyển một tín hiệu điện từ cáp điện ra tín hiệu quang để phát trên cáp quang và ngược lại. Việc sử dụng Repeater điện quang cũng làm tăng thêm chiều dài của mạng.

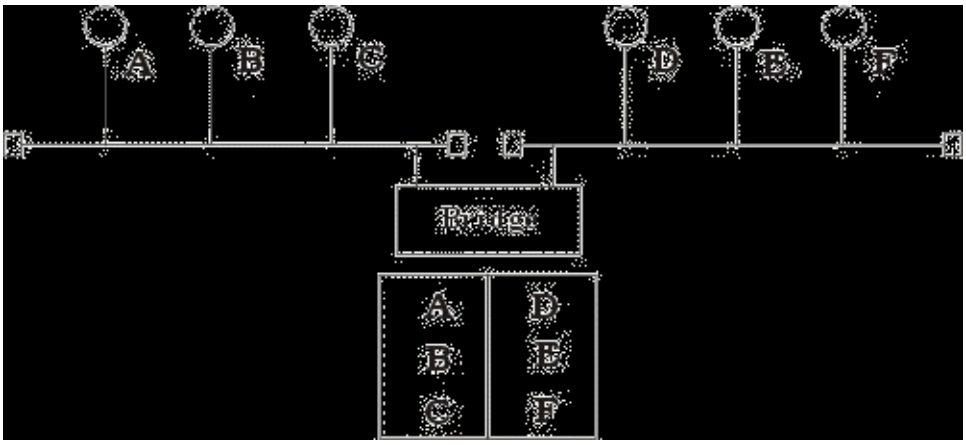
Việc sử dụng Repeater không thay đổi nội dung các tín hiện đi qua nên nó chỉ được dùng để nối hai mạng có cùng giao thức truyền thông (như hai mạng Ethernet hay hai mạng Token ring) nhưng không thể nối hai mạng có giao thức truyền thông khác nhau (như một mạng Ethernet và một mạng Token ring). Thêm nữa Repeater không làm thay đổi khối lượng chuyển vận trên mạng nên việc sử dụng không tính toán nó trên mạng lớn sẽ hạn chế hiệu năng của mạng. Khi lưa chọn sử dụng Repeater cần chú ý lựa chọn loại có tốc độ chuyển vận phù hợp với tốc độ của mạng.

## V.2. Bridge (Cầu nối)

Bridge là một thiết bị có xử lý dùng để nối hai mạng giống nhau hoặc khác nhau, nó có thể được dùng với các mạng có các giao thức khác nhau. Cầu nối hoạt động trên tầng liên kết dữ liệu nên không như bộ tiếp sức phải phát lại tất cả những gì nó nhận được thì cầu nối đọc được các gói tin của tầng liên kết dữ liệu trong mô hình OSI và xử lý chúng trước khi quyết định có chuyển đi hay không.

Khi nhận được các gói tin Bridge chọn lọc và chỉ chuyển những gói tin mà nó thấy cần thiết. Điều này làm cho Bridge trở nên có ích khi nối một vài mạng với nhau và cho phép nó hoạt động một cách mềm dẻo.

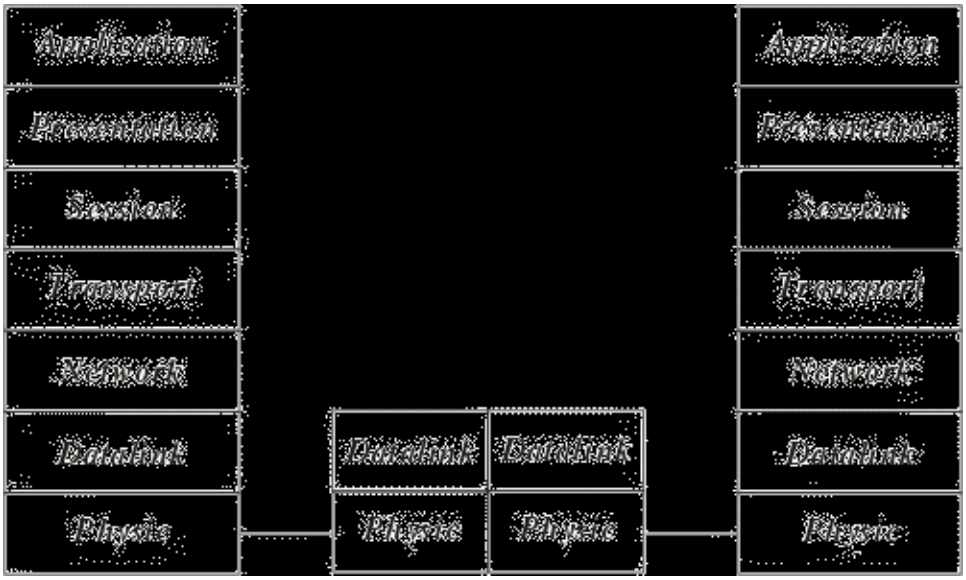
Để thực hiện được điều này trong Bridge ở mỗi đầu kết nối có một bảng các địa chỉ các trạm được kết nối vào phía đó, khi hoạt động cầu nối xem xét mỗi gói tin nó nhận được bằng cách đọc địa chỉ của nơi gửi và nhận và dựa trên bảng địa chỉ phía nhận được gói tin nó quyết định gửi gói tin hay không và bổ xung bảng địa chỉ.




Hình IV-5: Hoạt động của Bridge

Khi đọc địa chỉ nơi gửi Bridge kiểm tra xem trong bảng địa chỉ của phần mạng nhận được gói tin có địa chỉ đó hay không, nếu không có thì Bridge tự động bổ xung bảng địa chỉ (cơ chế đó được gọi là tự học của cầu nối).

Khi đọc địa chỉ nơi nhận Bridge kiểm tra xem trong bảng địa chỉ của phần mạng nhận được gói tin có địa chỉ đó hay không, nếu có thì Bridge sẽ cho rằng đó là gói tin nội bộ thuộc phần mạng mà gói tin đến nên không chuyển gói tin đó đi, nếu ngược lại thì Bridge mới chuyển sang phía bên kia. Ở đây chúng ta thấy một trạm không cần thiết chuyển thông tin trên toàn mạng mà chỉ trên phần mạng có trạm nhận mà thôi.



Hình IV-6: Hoạt động của Bridge trong mô hình OSI

Để đánh giá một Bridge người ta đưa ra hai khái niệm : Lọc và chuyển vận. Quá trình xử lý mỗi gói tin được gọi là quá trình lọc trong đó tốc độ lọc thể hiện trực tiếp khả năng hoạt động của

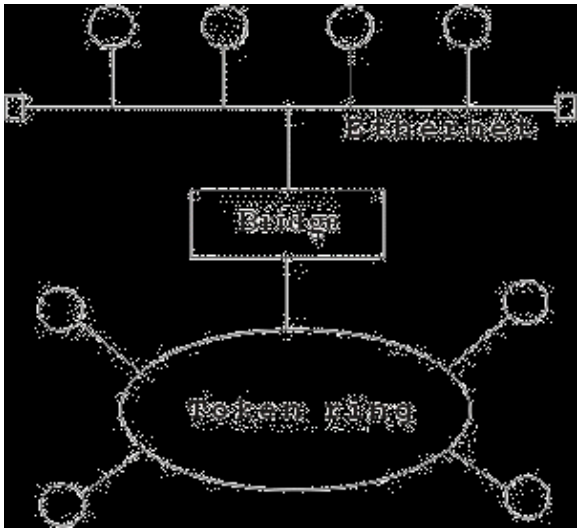
Bridge. Tốc độ chuyển vận được thể hiện số gói tin/giây trong đó thể hiện khả năng của Bridge chuyển các gói tin từ mạng này sang mạng khác.

Hiện nay có hai loại Bridge đang được sử dụng là Bridge vận chuyển và Bridge biên dịch. Bridge *vận chuyển* dùng để nối hai mạng cục bộ cùng sử dụng một giao thức truyền thông của tầng liên kết dữ liệu, tuy nhiên mỗi mạng có thể sử dụng loại dây nối khác nhau. Bridge vận chuyển không có khả năng thay đổi cấu trúc các gói tin mà nó nhận được mà chỉ quan tâm tới việc xem xét và chuyển vận gói tin đó đi.

Bridge biên dịch dùng để nối hai mạng cục bộ có giao thức khác nhau nó có khả năng chuyển một gói tin thuộc mạng này sang gói tin thuộc mạng kia trước khi chuyển qua

***Ví dụ :*** Bridge biên dịch nối một mạng Ethernet và một mạng Token ring. Khi đó Cầu nối thực hiện như một nút token ring trên mạng Token ring và một nút Enthernet trên mạng Ethernet. Cầu nối có thể chuyển một gói tin theo chuẩn đang sử dụng trên mạng Enthernet sang chuẩn đang sử dụng trên mạng Token ring.

Tuy nhiên chú ý ở đây cầu nối không thể chia một gói tin ra làm nhiều gói tin cho nên phải hạn chế kích thước tối đa các gói tin phù hợp với cả hai mạng. Ví dụ như kích thước tối đa của gói tin trên mạng Ethernet là 1500 bytes và trên mạng Token ring là 6000 bytes do vậy nếu một trạm trên mạng token ring gửi một gói tin cho trạm trên mạng Ethernet với kích thước lớn hơn 1500 bytes thì khi qua cầu nối số lượng byte dư sẽ bị chặt bỏ.

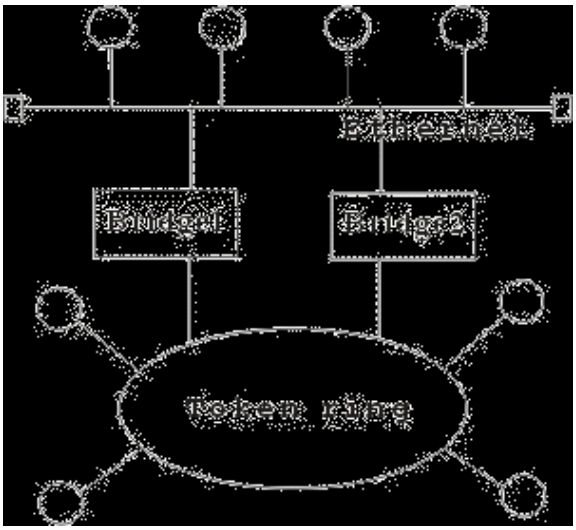


Hình IV-7: Ví dụ về Bridge biên dịch

Người ta sử dụng Bridge trong các trường hợp sau :

- Mở rộng mạng hiện tại khi đã đạt tới khoảng cách tối đa do Bridge sau khi sử lý gói tin đã phát lại gói tin trên phần mạng còn lại nên tín hiệu tốt hơn bộ tiếp sức.
- Giảm bớt tắc nghẽn mạng khi có quá nhiều trạm bằng cách sử dụng Bridge, khi đó chúng ta chia mạng ra thành nhiều phần bằng các Bridge, các gói tin trong nội bộ tùng phần mạng sẽ không được phép qua phần mạng khác.
- Để nối các mạng có giao thức khác nhau.

Một vài Bridge còn có khả năng lựa chọn đối tượng vận chuyển. Nó có thể chỉ chuyển vận những gói tin của nhưng địa chỉ xác định. Ví dụ : cho phép gói tin của máy A, B qua Bridge 1, gói tin của máy C, D qua Bridge 2.

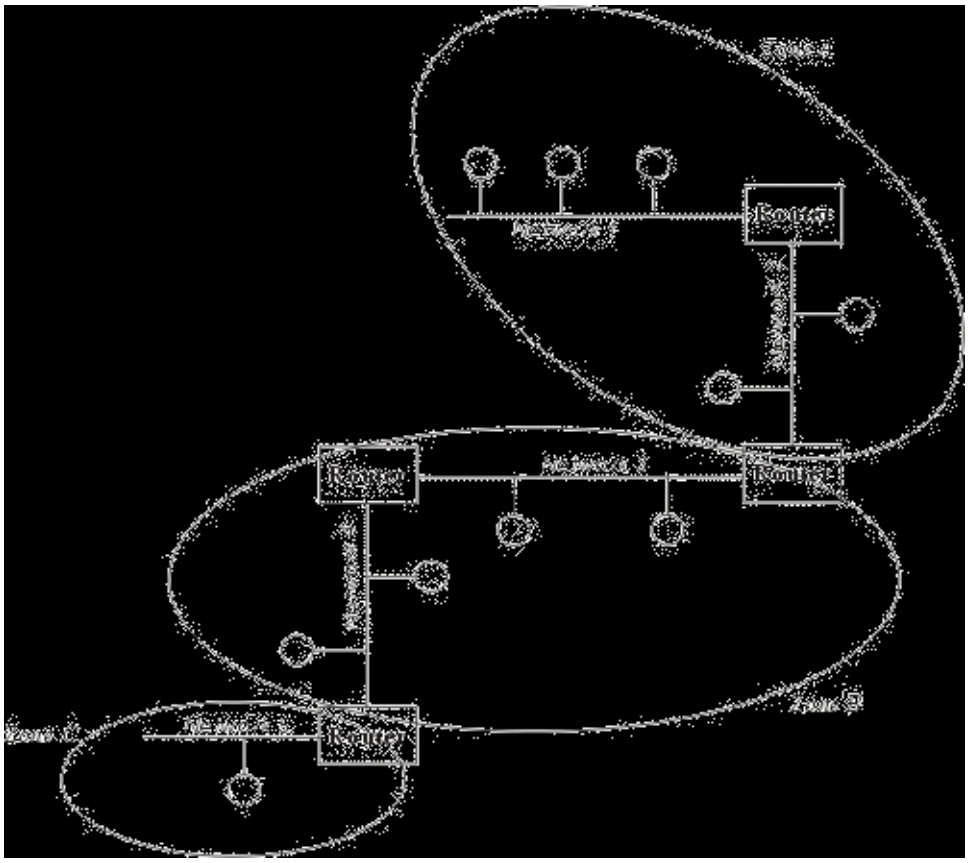


Hình IV-8: Liên kết mạng với 2 Bridge

Một số Bridge được chế tạo thành một bộ riêng biệt, chỉ cần nối dây và bật. Các Bridge khác chế tạo như card chuyên dùng cắïm vào máy tính, khi đó trên máy tính sẽ sử dụng phần mềm Bridge. Việc kết hợp phần mềm với phần cứng cho phép uyển chuyển hơn trong hoạt động của Bridge.

## V.3. Router (Bộ tìm đường)

Router là một thiết bị hoạt động trên tầng mạng, nó có thể tìm được đường đi tốt nhất cho các gói tin qua nhiều kết nối để đi từ trạm gửi thuộc mạng đầu đến trạm nhận thuộc mạng cuối. Router có thể được sử dụng trong việc nối nhiều mạng với nhau và cho phép các gói tin có thể đi theo nhiều đường khác nhau để tới đích.



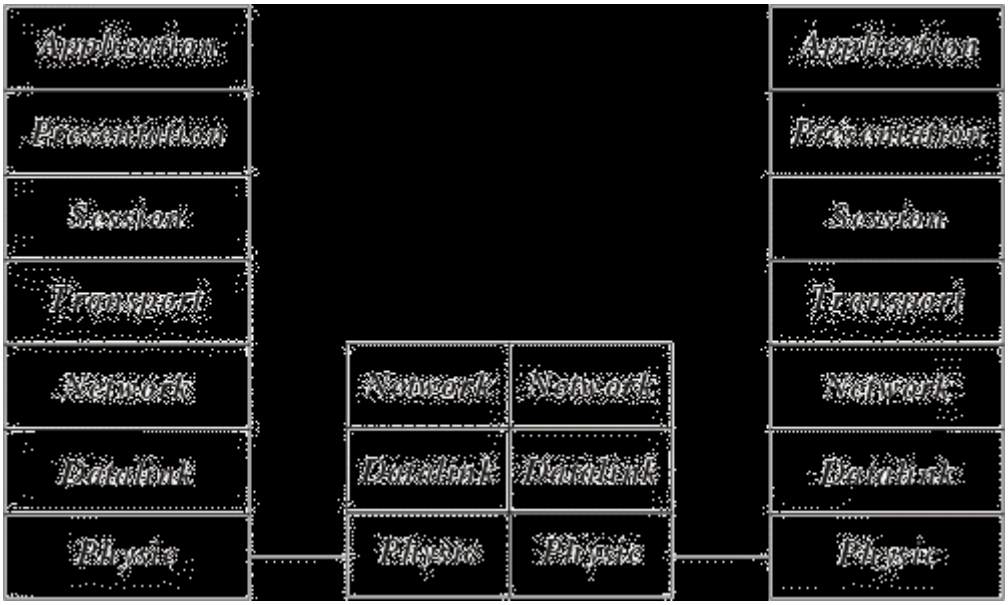
Hình IV-9: Hoạt động của Router.

Khác với Bridge hoạt động trên tầng liên kết dữ liệu nên Bridge phải xử lý mọi gói tin trên đường truyền thì Router có địa chỉ riêng biệt và nó chỉ tiếp nhận và xử lý các gói tin gửi đến nó mà thôi. Khi một trạm muốn gửi gói tin qua Router thì nó phải gửi gói tin với địa chỉ trực tiếp của Router (Trong gói tin đó phải chứa các thông tin khác về đích đến) và khi gói tin đến Router thì Router mới xử lý và gửi tiếp.

Khi xử lý một gói tin Router phải tìm được đường đi của gói tin qua mạng. Để làm được điều đó Router phải tìm được đường đi tốt nhất trong mạng dựa trên các thông tin nó có về mạng, thông thường trên mỗi Router có một bảng chỉ đường (Router table). Dựa trên dữ liệu về Router gần đó và các mạng trong liên mạng, Router tính được bảng chỉ đường (Router table) tối ưu dựa trên một thuật toán xác định trước.

Người ta phân chia Router thành hai loại là Router có phụ thuộc giao thức (The protocol dependent routers) và Router không phụ thuộc vào giao thức (The protocol independent router) dựa vào phương thức xử lý các gói tin khi qua Router.

- Router có phụ thuộc giao thức: Chỉ thực hiện việc tìm đường và truyền gói tin từ mạng này sang mạng khác chứ không chuyển đổi phương cách đóng gói của gói tin cho nên cả hai mạng phải dùng chung một giao thức truyền thông.
- Router không phụ thuộc vào giao thức: có thể liên kết các mạng dùng giao thức truyền thông khác nhau và có thể chuyển đôi gói tin của giao thức này sang gói tin của giao thức kia, Router cũng chấp nhận kích thước các gói tin khác nhau (Router có thể chia nhỏ một gói tin lớn thành nhiều gói tin nhỏ trước truyền trên mạng).

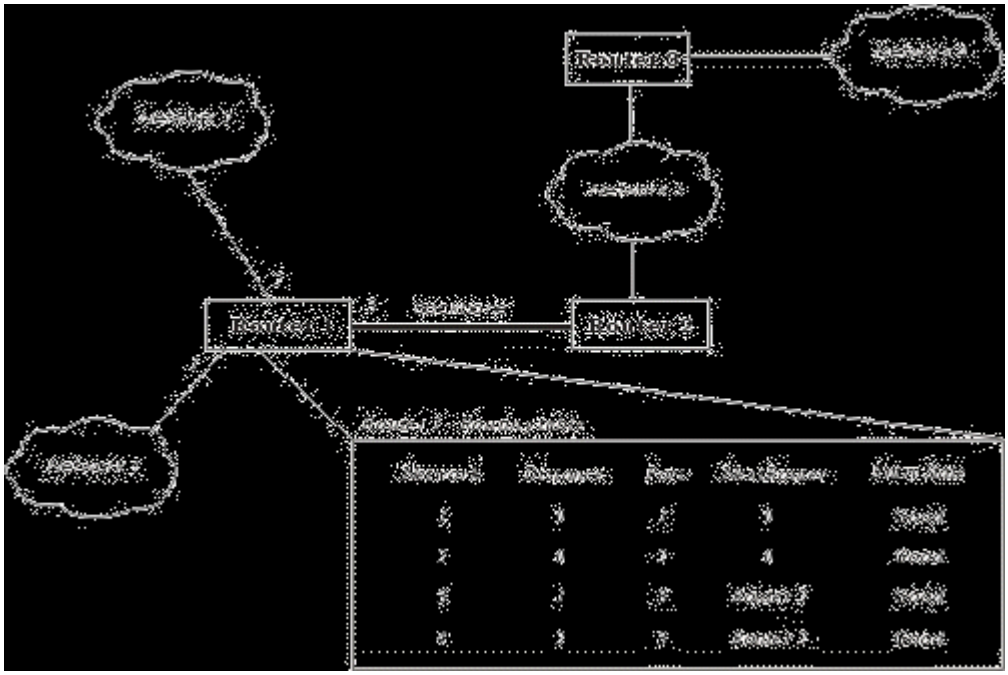


Hình IV-10: Hoạt động của Router trong mô hình OSI

Để ngăn chặn việc mất mát số liệu Router còn nhận biết được đường nào có thể chuyển vận và ngừng chuyển vận khi đường bị tắc.

Các lý do sử dụng Router :

- Router có các phần mềm lọc ưu việt hơn là Bridge do các gói tin muốn đi qua Router cần phải gửi trực tiếp đến nó nên giảm được số lượng gói tin qua nó. Router thường được sử dụng trong khi nối các mạng thông qua các đường dây thuê bao đắt tiền do nó không truyền dư lên đường truyền.
- Router có thể dùng trong một liên mạng có nhiều vùng, mỗi vùng có giao thức riêng biệt.
- Router có thể xác định được đường đi an toàn và tốt nhất trong mạng nên độ an toàn của thông tin được đảm bảo hơn.
- Trong một mạng phức hợp khi các gói tin luân chuyển các đường có thể gây nên tình trạng tắc nghẽn của mạng thì các Router có thể được cài đặt các phương thức nhằm tránh được tắc nghẽn.



Hình IV-11: Ví dụ về bảng chỉ đường (Routing table) của Router.

### V.3.1 Các phương thức hoạt động của Router

Đó là phương thức mà một Router có thể nối với các Router khác để qua đó chia sẻ thông tin về mạng hiện co. Các chương trình chạy trên Router luôn xây dựng bảng chỉ đường qua việc trao đổi các thông tin với các Router khác.

- **Phương thức véc tơ khoảng cách** : mỗi Router luôn luôn truyền đi thông tin về bảng chỉ đường của mình trên mạng, thông qua đó các Router khác sẽ cập nhật lên bảng chỉ đường của mình.
- **Phương thức trạng thái tĩnh** : Router chỉ truyền các thông báo khi có phát hiện có sự thay đổi trong mạng và chỉ khi đó các Router khác cập nhật lại bảng chỉ đường, thông tin truyền đi khi đó thường là thông tin về đường truyền.

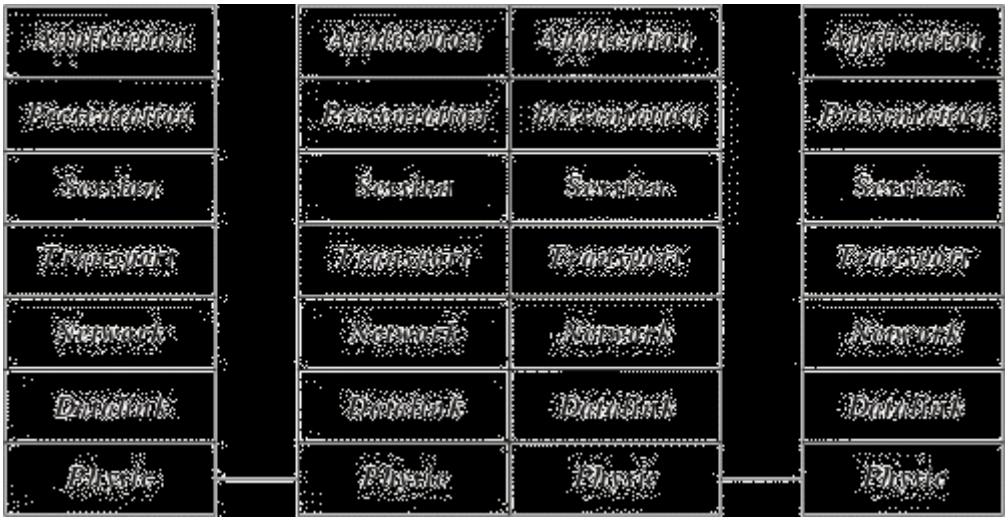
### V.3.2 Một số giao thức hoạt động chính của Router

- **RIP (Routing Information Protocol)** được phát triển bởi Xerox Network system và sử dụng SPX/IPX và TCP/IP. RIP hoạt động theo phương thức véc tơ khoảng cách.
- **NLSP (Netware Link Service Protocol)** được phát triển bởi Novell dùng để thay thế RIP hoạt động theo phương thức véctơ khoảng cách, mỗi Router được biết cấu trúc của mạng và việc truyền các bảng chỉ đường giảm đi..
- **OSPF (Open Shortest Path First)** là một phần của TCP/IP với phương thức trạng thái tĩnh, trong đó có xét tới ưu tiên, giá đường truyền, mật độ truyền thông...
- **OSPF-IS (Open System Interconnection Intermediate System to Intermediate System)** là một phần của TCP/IP với phương thức trạng thái tĩnh, trong đó có xét tới ưu tiên, giá đường truyền, mật độ truyền thông...

## V.4. Gateway (cổng nối)

Gateway dùng để kết nối các mạng không thuần nhất chẳng hạn như các mạng cục bộ và các mạng máy tính lớn (Mainframe), do các mạng hoàn toàn không thuần nhất nên việc chuyển đổi

thực hiện trên cả 7 tầng của hệ thống mở OSI. Thường được sử dụng nối các mạng LAN vào máy tính lớn. Gateway có các giao thức xác định trước thường là nhiều giao thức, một Gateway đa giao thức thường được chế tạo như các Card có chứa các bộ xử lý riêng và cài đặt trên các máy tính hoặc thiết bị chuyên biệt.



Hình IV-12: Hoạt động của Gateway trong mô hình OSI

Hoạt động của Gateway thông thường phức tạp hơn là Router nên thông suất của nó thường chậm hơn và thường không dùng nối mạng LAN -LAN.

## V.5. Hub (Bộ tập trung)

Hub thường được dùng để nối mạng, thông qua những đầu cắm của nó người ta liên kết với các máy tính dưới dạng hình sao.

Người ta phân biệt các Hub thành 3 loại như sau sau :

- **Hub bị động (Passive Hub)** : Hub bị động không chứa các linh kiện điện tử và cũng không xử lý các tín hiệu dữ liệu, nó có chức năng duy nhất là tổ hợp các tín hiệu từ một số đoạn cáp mạng. Khoảng cách giữa một máy tính và Hub không thể lớn hơn một nửa khoảng cách tối đa cho phép giữa 2 máy tính trên mạng (ví dụ khoảng cách tối đa cho phép giữa 2 máy tính của mạng là 200m thì khoảng cách tối đa giữa một máy tính và hub là 100m). Các mạng ARCnet thường dùng Hub bị động.
- **Hub chủ động (Active Hub)** : Hub chủ động có các linh kiện điện tử có thể khuyếch đại và xử lý các tín hiệu điện tử truyền giữa các thiết bị của mạng. Qúa trình xử lý tín hiệu được gọi là tái sinh tín hiệu, nó làm cho tín hiệu trở nên tốt hơn, ít nhạy cảm với lỗi do vậy khoảng cách giữa các thiết bị có thể tăng lên. Tuy nhiên những ưu điểm đó cũng kéo theo giá thành của Hub chủ động cao hơn nhiều so với Hub bị động. Các mạng Token ring có xu hướng dùng Hub chủ động.
- **Hub thông minh (Intelligent Hub)**: cũng là Hub chủ động nhưng có thêm các chức năng mới so với loại trước, nó có thể có bộ vi xử lý của mình và bộ nhớ mà qua đó nó không chỉ cho phép điều khiển hoạt động thông qua các chương trình quản trị mạng mà nó có thể hoạt động như bộ tìm đường hay một cầu nối. Nó có thể cho phép tìm đường

cho gói tin rất nhanh trên các cổng của nó, thay vì phát lại gói tin trên mọi cổng thì nó có thể chuyển mạch để phát trên một cổng có thể nối tới trạm đích.

## V.6. Bộ chuyển mạch (*switch)*

Chức năng chính của *switch* là cùng một lúc duy trì nhiều cầu nối giữa các thiết bị mạng bằng cách dựa vào một loại đường truyền xương sống (*backbone*) nội tại tốc độ cao. *Switch* có nhiều cổng, mỗi cổng có thể hỗ trợ toàn bộ *Ethernet* LAN hoặc Token Ring.

Bộ chuyển mạch kết nối một số LAN riêng biệt và cung cấp khả năng lọc gói dữ liệu giữa chúng.

Switch là thiết bị giống như bridge nhưng nhiều port hơn cho phép ghép nối nhiều đoạn mạng với nhau. Switch cũng dựa vào bảng địa chỉ MAC để quyết định gói tin nào đi ra port nào nhằm tránh tình trạng giảm băng thông khi số máy trạm trong mạng tăng lên. Switch cũng hoạt động tại lớp hai trong mô hình OSI. Việc xử lý gói tin dựa trên phần cứng (chip).

Khi một gói tin đi đến Switch (hoặc Bridge), Switch (hoặc Bridge) sẽ thực hiện như sau:

- Kiểm tra địa chỉ nguồn của gói tin đã có trong bảng MAC chưa, nếu chưa có thì nó sẽ thêm địa chỉ MAC này và port nguồn (nơi gói tin đi vào Switch (hoặc Bridge)) vào trong bảng MAC.

- Kiểm tra địa chỉ đích của gói tin đã có trong bảng MAC chưa:

+ Nếu chưa có thì nó sẽ gởi gói tin ra tất cả các port (ngoại trừ port gói tin đi vào).

+ Nếu địa chỉ đích đã có trong bảng MAC:

 Nếu port đích trùng với port nguồn thì Switch (hoặc Bridge) sẽ loại bỏ gói tin.

 Nếu port đích khác với port nguồn thì gói tin sẽ được gởi ra port đích tương ứng.

Chú ý:

- Địa chỉ nguồn và địa chỉ đích được nói ở trên đều là địa chỉ MAC.
- Port nguồn là Port mà gói tin đi vào.
- Port đích là Port mà gói tin đi ra.

# Chương V Mô hình mạng

## I. Kiến trúc mạng (Topology)

Hình trạng của mạng cục bộ thể hiện qua cấu trúc hay hình dáng hình học cuả các đường dây cáp mạng dùng để liên kết các máy tính thuộc mạng với nhau. Các mạng cục bộ thường hoạt động dựa trên cấu trúc đã định sẵn liên kết các máy tính và các thiết bị có liên quan.

Trước hết chúng ta xem xét hai phương thức nối mạng chủ yếu được sử dụng trong việc liên kết các máy tính là "một điểm - một điểm" và "một điểm - nhiều điểm ".

Với phương thức "một điểm - một điểm" các đường truyền riêng biệt được thiết lập để nối các cặp máy tính lại với nhau. Mỗi máy tính có thể truyền và nhận trực tiếp dữ liệu hoặc có thể làm trung gian như lưu trữ những dữ liệu mà nó nhận được rồi sau đó chuyển tiếp dữ liệu đi cho một máy khác để dữ liệu đó đạt tới đích.

Theo phương thức "một điểm - nhiều điểm " tất cả các trạm phân chia chung một đường truyền vật lý. Dữ liệu được gửi đi từ một máy tính sẽ có thể được tiếp nhận bởi tất cả các máy tính còn lại, bởi vậy cần chỉ ra địa chỉ đích của dữ liệu để mỗi máy tính căn cứ vào đó kiểm tra xem dữ liệu có phải dành cho mình không nếu đúng thì nhận còn nếu không thì bỏ qua.

Hình V-1 Các phương thức liên kết mạng

Tùy theo cấu trúc của mỗi mạng chúng sẽ thuộc vào một trong hai phương thức nối mạng và mỗi phương thức nối mạng sẽ có những yêu cầu khác nhau về phần cứng và phần mềm.

## II. Những cấu trúc chính của mạng cục bộ

### II.1. Dạng đường thẳng (Bus)

Trong dạng đường thẳng các máy tính đều được nối vào một đường dây truyền chính (bus). Đường truyền chính này được giới hạn hai đầu bởi một loại đầu nối đặc biệt gọi là terminator (dùng để nhận biết là đầu cuối để kết thúc đường truyền tại đây). Mỗi trạm được nối vào bus qua một đầu nối chữ T (T_connector) hoặc một bộ thu phát (transceiver). Khi một trạm truyền dữ liệu, tín hiệu được truyền trên cả hai chiều của đường truyền theo từng gói một, mỗi gói đều phải mang địa chỉ trạm đích. Các trạm khi thấy dữ liệu đi qua nhận lấy, kiểm tra, nếu đúng với địa chỉ của mình thì nó nhận lấy còn nếu không phải thì bỏ qua.

Sau đây là vài thông số kỹ thuật của topology bus. Theo chuẩn IEEE 802.3 (cho mạng cục bộ) với cách đặt tên qui ước theo thông số: tốc độ truyền tính hiệu (1,10 hoặc 100 Mb/s); BASE (nếu là Baseband) hoặc BROAD (nếu là Broadband).

- 10BASE5: Dùng cáp đồng trục đường kính lớn (10mm) với trở kháng 50 Ohm, tốc độ 10 Mb/s, phạm vi tín hiệu 500m/segment, có tối đa 100 trạm, khoảng cách giữa 2 tranceiver tối thiểu 2,5m (Phương án này còn gọi là Thick Ethernet hay Thicknet)

- 10BASE2: tương tự như Thicknet nhưng dùng cáp đồng trục nhỏ (RG 58A), có thể chạy với khoảng cách 185m, số trạm tối đa trong 1 segment là 30, khoảng cách giữa hai máy tối thiểu là 0,5m.

Dạng kết nối này có ưu điểm là ít tốn dây cáp, tốc độ truyền dữ liệu cao tuy nhiên nếu lưu lượng truyền tăng cao thì dễ gây ách tắc và nếu có trục trặc trên hành lang chính thì khó phát hiện ra.

Hiện nay các mạng sử dụng hình dạng đường thẳng là mạng Ethernet và G-net.

## II.2. Dạng vòng tròn (Ring)

Các máy tính được liên kết với nhau thành một vòng tròn theo phương thức "một điểm - một điểm ", qua đó mỗi một trạm có thể nhận và truyền dữ liệu theo vòng một chiều và dữ liệu được truyền theo từng gói một. Mỗi gói dữ liệu đều có mang địa chỉ trạm đích, mỗi trạm khi nhận được một gói dữ liệu nó kiểm tra nếu đúng với địa chỉ của mình thì nó nhận lấy còn nếu không phải thì nó sẽ phát lại cho trạm kế tiếp, cứ như vậy gói dữ liệu đi được đến đích. Với dạng kết nối này có ưu điểm là không tốn nhiều dây cáp, tốc độ truyền dữ liệu cao, không gây ách tắc tuy nhiên các giao thức để truyền dữ liệu phức tạp và nếu có trục trặc trên một trạm thì cũng ảnh hưởng đến toàn mạng.

Hiện nay các mạng sử dụng hình dạng vòng tròn là mạng Tocken ring của IBM.

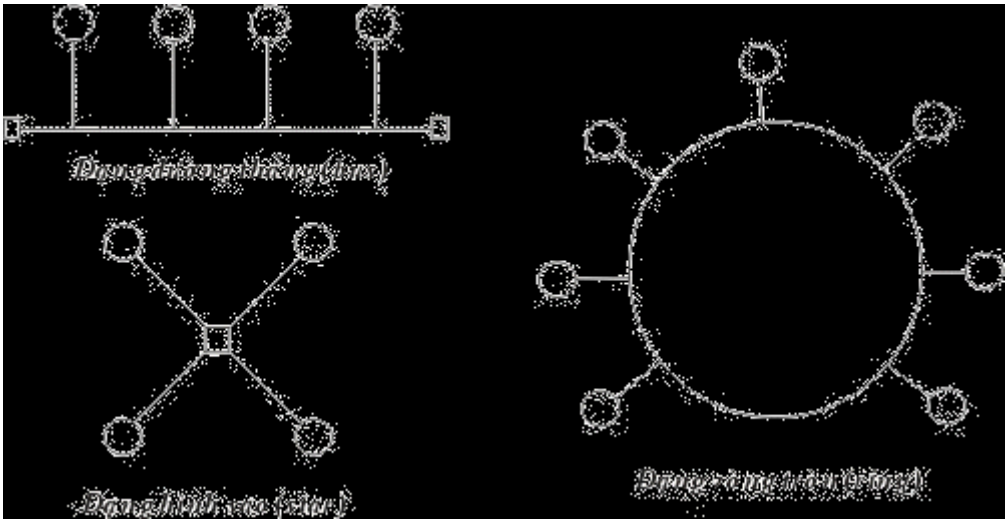
## II.3. Dạng hình sao (Star)

Ở dạng hình sao, tất cả các trạm được nối vào một thiết bị trung tâm có nhiệm vụ nhận tín hiệu từ các trạm và chuyển tín hiệu đến trạm đích với phương thức kết nối là phương thức "một điểm - một điểm ". Thiết bị trung tâm hoạt động giống như một tổng đài cho phép thực hiện việc nhận và truyền dữ liệu từ trạm này tới các trạm khác. Tùy theo yêu cầu truyền thông trong mạng , thiết bị trung tâm có thể là một bộ chuyển mạch (switch), một bộ chọn đường (router) hoặc đơn giản là một bộ phân kênh (Hub). Có nhiều cổng ra và mỗi cổng nối với một máy. Theo chuẩn IEEE 802.3 mô hình dạng Star thường dùng:

- 10BASE-T: dùng cáp UTP, tốc độ 10 Mb/s, khoảng cách từ thiết bị trung tâm tới trạm tối đa là 100m.
- 100BASE-T tương tự như 10BASE-T nhưng tốc độ cao hơn 100 Mb/s.

Ưu và khuyết điểm

- Ưu điểm: Với dạng kết nối này có ưu điểm là không đụng độ hay ách tắc trên đường truyền, lắp đặt đơn giản, dễ dàng cấu hình lại (thêm, bớt trạm). Nếu có trục trặc trên một trạm thì cũng không gây ảnh hưởng đến toàn mạng qua đó dễ dàng kiểm soát và khắc phục sự cố.
- Nhược điểm: Độ dài đường truyền nối một trạm với thiết bị trung tâm bị hạn chế (trong vòng 100 m với công nghệ hiện đại) tốn đường dây cáp nhiều, tốc độ truyền dữ liệu không cao.
- Hiện nay các mạng sử dụng hình dạng hình sao là mạng STARLAN của AT&T và S-NET của Novell.



Hình V-2 Các loại cấu trúc chính của mạng cục bộ.

| | **Đường thẳng** | **Vòng Tròn** | **Hình sao** |
|---|---|---|---|
| **Ứng dụng** | Tốt cho trường hợp mạng nhỏ và mạng có giao thông thấp và lưu lượng dữ liệu thấp | Tốt cho trường hợp mạng có số trạm ít hoạt động với tốc độ cao,không cách nhau xa lắm hoặc mạng có lưu lượng dữ liệu phân bố không đều. | Hiện nay mạng sao là cách tốt nhất cho trường hợp phải tích hợp dữ liệu và tín hiệutiếng.Các mạng đện thoại công cộng có cấu trúc này |
| **Độ phức tạp** | Tương đối không phức tạp | Đòi hỏi thiết bị tương đối phức tạp .Mặt khác việc đưa thông điệp đi trên tuyến là đơn giản, vì chỉ có 1 con đường, trạm phát chỉ cần biết địa chỉ của trạm nhận , các thông tin để dẫn đường khác thì không cần thiết | Mạng sao được xem là khá phức tạp . Các trạm được nối với thiết bị trung tâm và lần lượt hoạt động như thiết bị trung tâm hoặc nối được tới các dây dẫn truyền từ xa |
| **Hiệu suất** | Rất tốt dưới tải thấp có thể giảm hiệu suất rất mau khi tải tăng | Có hiệu quả trong trường hợp lượng lưu thông cao và khá ổn định nhờ sự tăng chậm thời gian trễ và sự xuống cấp so với các mạng khác | Tốt cho trường hợp tải vừa tuy nhiên kích thước và khả năng , suy ra hiệu suất của mạng phụ thuộc trực tiếp vào sức mạnh của thiết bị trung tâm. |
| **Tổng phí** | Tương đối thấp đặc biệt do nhiều thiết bị đã phát triển hòa chỉnh và bán sảm phẩm ở thị trường | Phải dự trù gấp đôi nguồn lực hoặc phải có 1 phương thức thay thế khi 1 nút không hoạt động nếu vẫn | Tổng phí rất cao khi làm nhiêm vụ của thiết bị trung tâm, thiết bị trung tâm ï không được dùng |

| | | | |
|---|---|---|---|
| | .Sự dư thừa kênh truyền được khuyến để giảm bớt nguy cơ xuất hiện sự cố trên mạng | muốn mạng hoạt động bình thường | vào việc khác .Số lượng dây riêng cũng nhiều. |
| **Nguy cơ** | Một trạm bị hỏng không ảnh hưởng đến cả mạng. Tuy nhiên mạng sẽ có nguy cơ bị tổn hại khi sự cố trên đường dây dẫn chính hoặc có vấn đề với tuyến. Vấn đề trên rất khó xác định được lại rất dễ sửa chữa | Một trạm bị hỏng có thể ảnh hưởng đến cả hệ thống vì các trạm phục thuộc vào nhau. Tìm 1 repeater hỏng rất khó ,vả lại việc sửa chữa thẳng hay dùng mưu mẹo xác định điểm hỏng trên mạng có địa bàn rôäng rất khó | Độ tin cậy của hệ thống phụ thuộc vào thiết bị trung tâm, .nếu bị hỏng thì mạng ngưng hoạt động Sự ngưng hoạt động tại thiết bị trung tâm thường không ảnh hưởng đến toàn bộ hệ thống . |
| **Khả năng mở rộng** | Việc thêm và định hình lại mạng này rất dễ.Tuy nhiên việc kết nối giữa các máy tính và thiết bị của các hãng khác nhau khó có thể vì chúng phải có thể nhận cùng địa chỉ và dữ liệu | Tương đối dễ thêm và bớt các trạm làm việc mà không phải nối kết nhiều cho mỗi thay đổi Giá thành cho việc thay đổi tương đối thấp | Khả năng mở rộâng hạn chế, đa số các thiết bị trung tâm chỉ chịu đựng nổi 1 số nhất định liên kết. Sự hạn chế về tốc độ truyền dữ liệu và băng tần thường được đòi hỏi ở mỗi người sử dụng. Các hạn chế này giúp cho các chức năng xử lý trung tâm không bị quá tải bởi tốc độ thu nạp tại tại cổng truyền và giá thành mỗi cổng truyền của thiết bị trung tâm thấp . |

**Bảng V-1** ***Bảng so sánh tính năng giữa các cấu trúc của mạng LAN***

## II.4. Mạng dạng kết hợp

- Kết hợp hình sao và tuyến (*star/Bus Topology*)

Cấu hình mạng dạng này có bộ phận tách tín hiệu (*spitter*) giữ vai trò thiết bị trung tâm, hệ thống dây cáp mạng có thể chọn hoặc *Ring Topology* hoặc *Linear Bus Topology.*

Lợi điểm của cấu hình này là mạng có thể gồm nhiều nhóm làm việc ở cách xa nhau, ARCNET là mạng dạng kết hợp *Star/Bus Topology*. Cấu hình dạng này đưa lại sự uyển chuyển trong việc bố trí đường dây tương thích dễ dàng đối với bất cứ toà nhà nào.

- Kết hợp hình sao và vòng *(Star/Ring Topology)*

Cấu hình dạng kết hợp *Star/Ring Topology*, có một "thẻ bài" liên lạc (*Token*) được chuyển vòng quanh một cái HUB trung tâm. Mỗi trạm làm việc (*workstation*) được nối với HUB - là cầu nối giữa các trạm làm việc và để tăng khoảng cách cần thiết.

# Chương VI Các dịch vụ của mạng diện rộng (WAN)

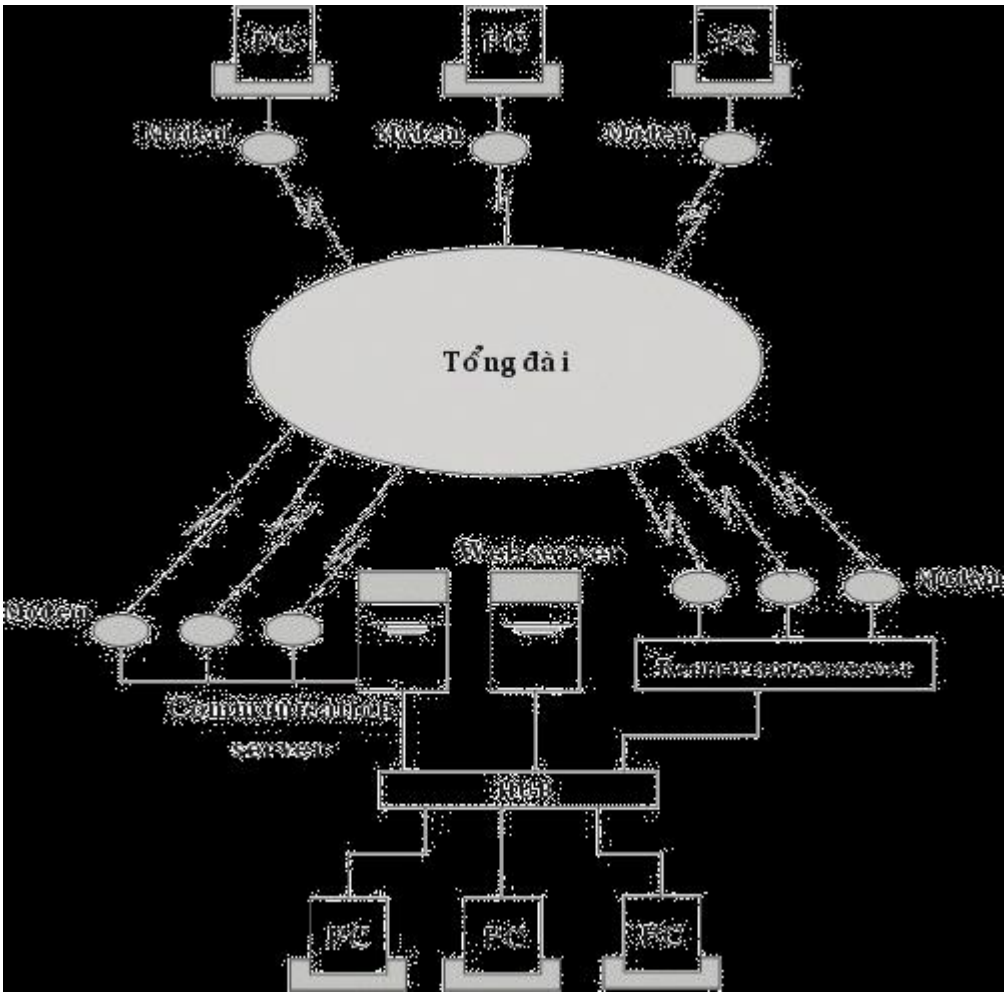
Hiện nay trên thế giới có nhiều dịch vụ dành cho việc chuyển thông tin từ khu vực này sang khu vực khác nhằm liên kết các mạng LAN của các khu vực khác nhau lại. Để có được những liên kết như vậy người ta thường sử dụng các dịch vụ của các mạng diện rộng. Hiện nay trong khi giao thức truyền thông cơ bản của LAN là Ethernet, Token Ring thì giao thức dùng để tương nối các LAN thông thường dựa trên chuẩn TCP/IP. Ngày nay khi các dạng kết nối có xu hướng ngày càng đa dạng và phân tán cho nên các mạng WAN đang thiên về truyền theo đơn vị tập tin thay vì truyền một lần xử lý.

Có nhiều cách phân loại mạng diện rộng, ở đây nếu phân loại theo phương pháp truyền thông tin thì có thể chia thành 3 loại mạng như sau:

- Mạng chuyển mạch (Circuit Swiching Network)
- Mạng thuê bao (Leased lines Network)
- Mạng chuyển gói tin (Packet Switching Network)

## I. Mạng chuyển mạch (Circuit Swiching Network)

Để thực hiện được việc liên kết giữa hai điểm nút, một đường nối giữa điểm nút này và điêm nút kia được thiết lập trong mạng thể hiện dưới dạng cuộc gọi thông qua các thiết bị chuyển mạch.



Hình VI-1*: Mô hình mạng chuyển mạch*

Một ví dụ của mạng chuyển mạch là hoạt động của mạng điện thoại, các thuê bao khi biết số của nhau có thể gọi cho nhau và có một đường nối vật lý tạm thời được thiết lập giữa hai thuê bao.

Với mô hình này mọi đường đều có thể một đường bất kỳ khác, thông qua những đường nối và các thiết bị chuyên dùng người ta có thể liên kết một đường tạm thời từ nơi gửi tới nơi nhận một đường nối vật lý, đường nối trên duy trì trong suốt phiên làm việc và chỉ giải phóng sau khi phiên làm việc kết thúc. Để thực hiện một phiên làm việc cần có các thủ tục đầy đủ cho việc thiết lập liên kết trong đó có việc thông báo cho mạng biết địa chỉ của nút nhận.

Hiện nay có 2 loại mạng chuyển mạch là chuyển mạch tương tự (analog) và chuyển mạch số (digital)

- *Chuyển mạch tương tự (Analog):* Việc chuyển dữ liệu qua mạng chuyển mạch tương tự được thực hiện qua mạng điện thoại. Các trạm sử dụng một thiết bị có tên là modem, thiết bị này sẽ chuyển các tín hiệu số từ máy tính sao tín hiệu tuần tự có trễ truyền đi trên mạng điện thoại và ngược lại.

Hình VI-2*: Mô hình chuyển mạch tương tự*

Khi sử dụng đường truyền điện thoại để truyền số liệu thì các chuẩn của modem và các tính chất của nó sẽ quyết định tốc độ của đường truyền. Cùng với các kỹ thuật chuyển đổi tín hiệu các tính năng mới như nén tín hiệu cho phép nâng tốc độ truyền dữ liệu lên rất cao.

| Loại | Tốc độ(bps) | Loại nén | Tốc độ thực tế (bps) |
|---|---|---|---|
| Bell 212A | 1200 | | |
| CCITT V22 | 1200 | | |
| CCITT V22 bis | 2400 | MNP Class 5 | 2400 - 3600 |
| CCITT V32 | 9600 | MNP Class 5, V42 bis | 9600 - 19200 |
| CCITT V32 bis | 14400 | MNP Class 5, V42 bis | 14400 - 33600 |

**Bảng VI-1*: Bảng kỹ thuật modem***

Các kỹ thuật nén thường dùng là MNP Class 5 và V42 bis, MNP Class 5 cho phép nén với tỷ lệ 1.5:1 và V42 bis nén với tỷ lệ 2:1. Tuy nhiên trên thực tế tỷ lệ nén có thể thay đổi dựa vào dạng dữ liệu được truyền.

- *Chuyển mạch số (Digital):* Đường truyền chuyển mạch số lần đầu tiên được AT&T thiệu vào cuối 1980 khi AT&T giới thiệu mạng chuyển mạch số Acnet với đường truyền 56 kbs. Việc sử dụng đường chuyển mạch số cũng đòi hỏi sử dụng thiết bị phục vụ truyền dữ liệu số (Data Service Unit - DSU) vào vị trí modem trong chuyển mạch tương tự. Thiết bị phục vụ truyền dữ liệu số có nhiệm vụ chuyển các tín hiệu số đơn chiều (unipolar) từ máy tính ra thành tín hiệu số hai chiều (bipolar) để truyền trên đường truyền.

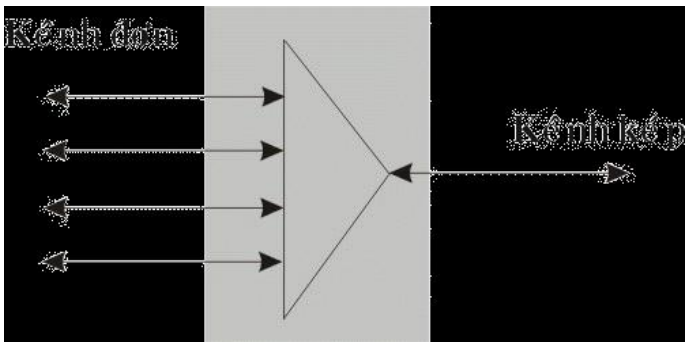
Hình VI-3*: Mô hình chuyển mạch số*

Mạng chuyển mạch số cho phép người sử dụng nâng cao tốc độ truyền (ở đây do khác biệt giữa kỹ thuật truyền số và kỹ thuật truyền tương tự nên hiệu năng của truyền mạch số cao hơn nhiều so với truyền tương tự cho dù cùng tốc độ), độ an toàn.

Vào năm 1991 AT&T giới thiệu mạng chuyển mạch số có tốc độ 384 Kbps. Người ta có thể dùng mạng chuyển mạch số để tạo các liên kết giữa các mạng LAN và làm các đường truyền dự phòng.

## II. Mạng thuê bao (Leased line Network)

Với kỹ thuật chuyển mạch giữa các nút của mạng (tương tự hoặc số) có một số lượng lớn đường dây truyền dữ liệu, với mỗi đường dây trong một thời điểm chỉ có nhiều nhất một phiên giao dịch, khi số lượng các trạm sử dụng tăng cao người ta nhận thấy việc sử dụng mạng chuyển mạch trở nên không kinh tế. Để giảm bớt số lượng các đường dây kết nối giữa các nút mạng người ta đưa ra một kỹ thuật gọi là ghép kênh.



Hình VI-4*: Mô hình ghép kênh*

Mô hình đó được mô tả như sau: tại một nút người ta tập hợp các tín hiệu trên của nhiều người sử dụng ghép lại để truyền trên một kênh nối duy nhất đến các nút khác, tại nút cuối người ta phân kênh ghép ra thành các kênh riêng biệt và truyền tới các người nhận.

Có hai phương thức ghép kênh chính là ghép kênh theo tần số và ghép kênh theo thời gian, hai phương thức này tương ứng với mạng thuê bao tuần tự và mạng thuê bao kỹ thuật số. trong thời gian hiện nay mạng thuê bao kỹ thuật số sử dụng kỹ thuật ghép kênh

theo thời gian với đường truyền T đang được sử dụng ngày một rộng rãi và dần dần thay thế mạng thuê bao tuần tự.

1. **Phương thức ghép kênh theo tần số**

Để sử dụng phương thức ghép kênh theo tần số giữa các nút của mạng được liên kết bởi đường truyền băng tần rộng. Băng tần này được chia thành nhiều kênh con được phân biệt bởi tần số khác nhau. Khi truyền dử liệu, mỗi kênh truyền từ người sử dụng đến nút sẽ được chuyển thành một kênh con với tần số xác định và được truyền thông qua bộ ghép kênh đến nút cuối và tại đây nó được tách ra thành kênh riêng biệt để truyền tới người nhận. Theo các chuẩn của CCITT có các phương thức ghép kênh cho phép ghép 12, 60, 300 kênh đơn.

Người ta có thể dùng đường thuê bao tuần tự (Analog) nối giữa máy của người sử dụng tới nút mạng thuê bao gần nhất. Khi máy của người sử dụng gửi dữ liệu thì kênh dữ liệu được ghép với các kênh khác và truyền trên đường truyền tới nút đích và được phân ra thành kênh riêng biệt trước khi gửi tới máy của người sử dụng. Đường nối giữa máy trạm của người sử dụng tới nút mạng thuê bao cũng giống như mạng chuyển mạch tuần tự sử dụng đường dây điện thoại với các kỹ thuật chuyển đổi tín hiệu như V22, V22 bis, V32, V32 bis, các kỹ thuật nén V42 bis, MNP class 5.

2. **Phương thức ghép kênh theo thời gian:**

Khác với phương thức ghép kênh theo tần số, phương thức ghép kênh theo thời gian chia một chu kỳ thời gian hoạt động của đường truyền trục thành nhiều khoảng nhỏ và mỗi kênh tuyền dữ liệu được một khoảng. Sau khi ghép kênh lại thành một kênh chung dữ liệu được truyền đi tương tự như phương thức ghép kênh theo tần số. Người ta dùng đường thuê bao là đường truyền kỹ thuật số nối giữa máy của người sử dụng tới nút mạng thuê bao gần nhất.

Hiện nay người ta có các đường truyền thuê bao như sau :

Đường T1 với tốc độ 1.544 Mbps nó bao gồm 24 kênh vớp tốc độ 64 kbps và 8000 bits điều khiển trong 1 giây.

## III. Mạng chuyển gói tin (Packet Switching NetWork)

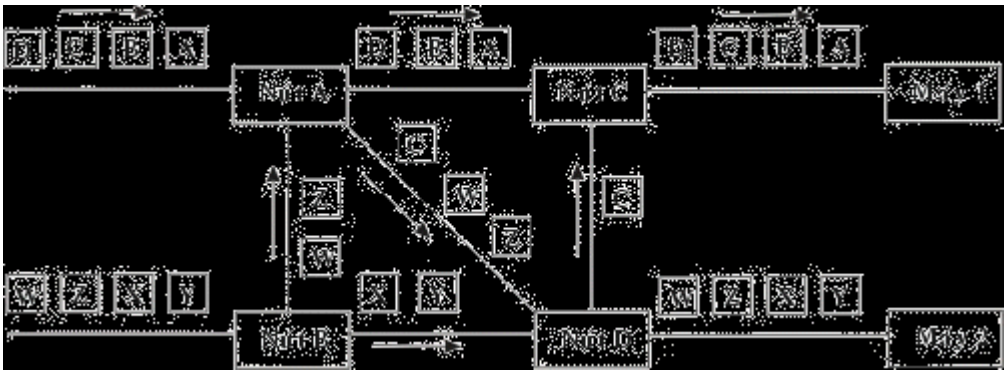
Mạng chuyển mạch gói hoạt động theo nguyên tắc sau : Khi một trạm trên mạng cần gửi dữ liệu nó cần phải đóng dữ liệu thành từng gói tin, các gói tin đó được đi trên mạng từ nút này tới nút khác tới khi đến được đích. Do việc sử dụng kỹ thuật trên nên khi một trạm không gửi tin thì mọi tài nguyên của mạng sẽ dành cho các trạm khác, do vậy mạng tiết kiệm được các tài nguyên và có thể sử dụng chúng một cách tốt nhất.

Người ta chia các phương thức chuyển mạch gói ra làm 2 phương thức:

Phương thức chuyển mạch gói theo sơ đồ rời rạc.
Phương thức chuyển mạch gói theo đường đi xác định.

1. **Phương thức chuyển mạch gói theo sơ đồ rời rạc:**

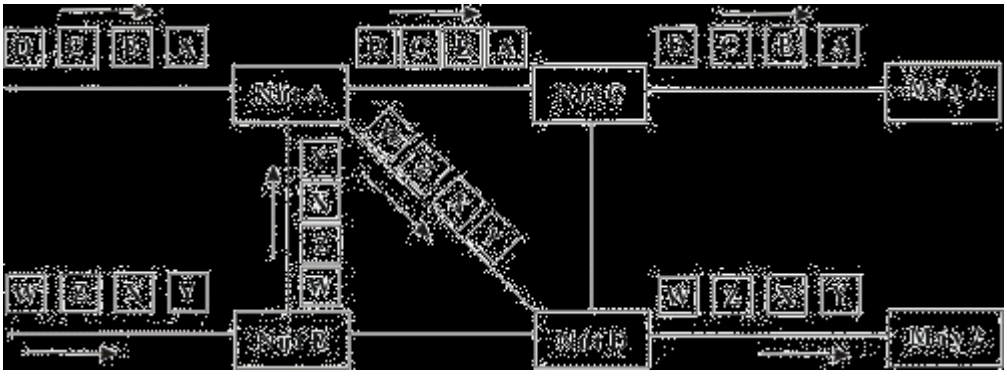
các gói tin được chuyển đi trên mạng một cách độc lập, mỗi gói tin đều có mang địa chỉ nơ i gửi và nơi nhận. Mỗi nút trong mạng khi tiếp nhận gói tin sẽ quyết định xenm đường đi của gói tin phụ thuộc vào thuật toán tìm đường tại nút và những thông tin về mạng mà nút đó có. Việc truyền theo phương thức này cho ta sự mềm dẻo nhất định do đường đi với mỗi gói tin trở nên mềm dẻo tuy nhiên điều này yêu cầu một số lượng tính toán rất lớn tại mỗi nút nên hiện nay phần lớn các mạng chuyển sang dùng phương chuyển mạch gói theo đường đi xác định.



Hình VI-5*: Ví dụ phương thức sơ đồ rời rạc.*

2. **Phương thức chuyển mạch gói theo đường đi xác định:**

Trước khi truyền dữ liệu một đường đi (hay còn gọi là đường đi ảo) được thiết lập giữa trạm gửi và trạm nhận thông qua các nút của mạng. Đường đi trên mang số hiệu phân biệt với các đường đi khác, sau đó các gói tin được gửi đi theo đường đã thiết lập để tới đích, các gói tin mang số hiệu củ đường ảo để có thể được nhận biết khi qua các nút. Điều này khiến cho việc tính toán đường đi cho phiên liên lạc chỉ cần thực hiện một lần.



Hình VI-6*: Ví dụ phương thức đường đi xác định*

## IV. Mạng X25

Được CCITT công bố lần đầu tiên vào 1970 lúc lĩnh vực viễn thông lần đầu tiên tham gia vào thế giới truyền dữ liệu với các đặc tính:

- X25 cung cấp quy trình kiểm soát luồng giữa các đầu cuối đem lại chất lương đường truyền cao cho dù chất lương đương dây truyền không cao.

- X25 được thiết kế cho cả truyền thông chuyển mạch lẫn truyền thông kiểu điểm nối điểm.
- Được quan tâm và tham gia nhanh chóng trên toàn cầu.

Trong X25 có chức năng dồn kênh (multiplexing) đối với liên kết logic (virtual circuits) chỉ làm nhiệm vụ kiểm soát lỗi cho các frame đi qua. Điều này làm tăng độ phức tạp trong việc phối hợp các thủ tục giữa hai tầng kề nhau, dẫn đến thông lượng bị hạn chế do tổng phí xử lý mỗi gói tin tăng lên. X25 kiểm tra lỗi tại mỗi nút trước khi truyền tiếp, điều này làm cho đường truyền chó chất lượng rất cao gần như phi lỗi. Tuy nhiên do vậy khối lượng tích toán tại mỗi nút khá lớn, đối với những đường truyền của những năm 1970 thì điều đó là cần thiết nhưng hiện nay khi kỹ thuật truyền dẫn đã đạt được những tiến bộ rất cao thì việc đó trở nên lãng phí

## V. Mạng Frame Relay

Mỗi gói tin trong mạng gọi là Frame, do vậy mạng gọi là Frame relay. Đặc điểm khác biệt giữa mạng Frame Relay và mạng X25 mạng Frame Relay là chỉ kiểm tra lỗi tại hai trạm gửi và trạm nhận còn trong quá trình chuyển vận qua các nút trung gian gói tin sẽ không được kiểm lỗi nữa. Do vậy thời gian xử lý trên mỗi nút nhanh hơn, tuy nhiên khi có lỗi thì gói tin phải được phát lại từ trạm đầu. Với độ an toàn cao của đường truyền hiện nay thì chi phí việc phát lại đó chỉ chiếm một tỷ lệ nhỏ nếu so với khối lượng tính toán được giảm đi tại các nút nên mạng Frame Relay tiết kiệm được tài nguyên của mạng hơn so với mạng X25.

Frame relay không chỉ là một kỹ thuật mà còn là thể hiện một phương pháp tổ chức mới. Với nguyên lý là truyền mạch gói nhưng các thao tác kiểm soát giữa các đầu cuối giảm đáng kể Kỹ thuật Frame Relay cho phép thông lượng tối đa đạt tới 2Mbps và hiện nay nó đang cung cấp các giải pháp để tương nối các mạng cục bộ LAN trong một kiến trúc xương sống tạo nên môi trường cho ứng dụng multimedia.

## VI. Mạng ATM (Cell relay)

Hiện nay kỹ thuật Cell Relay dựa trên phương thức truyền thông không đồng bộ (ATM) có thể cho phép thông lương hàng trăm Mbps. Đơn vị dữ liệu dùng trong ATM được gọi là tế bào (cell). các tế bào trong ATM có độ dài cố định là 53 bytes, trong đó 5 bytes dành cho phần chứa thông tin điều khiển (cell header) và 48 bytes chứa dữ liệu của tầng trên.

Trong kỹ thuật ATM, các tế bào chứa các kiểu dữ liệu khác nhau được ghép kênh tới một đường dẫn chung được gọi là đường dẫn ảo (virtual path). Trong đường dẫn ảo đó có thể gồm nhiều kênh ảo (virtual chanell) khác nhau, mỗi kênh ảo được sử dụng bởi một ứng dung nào đó tại một thời điểm.

ATM đã kết hợp những đặc tính tốt nhất của dạng chuyển mạch liên tục và dạng chuyển mạch gói, nó có thể kết hợp dải thông linh hoạt và khả năng chuyển tiếp cao tốc và có khả năng quản lý đồng thời dữ liệu số, tiếng nói, hình ảnh và multimedia tương tác.

Mục tiêu của kỹ thuật ATM là nhằm cung cấp một mạng dồn kênh, và chuyển mạch tốc độ cao, độ trễ nhỏ dáp ứng cho các dạng truyền thông đa phương tiện (multimecdia)

Chuyển mạch cell cần thiết cho việc cung cấp các kết nối đòi hỏi băng thông cao, tình trạng tắt nghẽn thấp, hổ trợ cho lớp dịch vụ tích hợp lưu thông dữ liệu âm thanh hình ảnh. Đặc tính tốc độ cao là đặc tính nổi bật nhất của ATM.

ATM sử dụng cơ cấu chuyển mạch đặc biệt: ma trận nhị phân các thành tố chuyển mạch (a matrix of binary switching elements) để vận hành lưu thông. Khả năng vô hướng (scalability) là một đặc tính của cơ cấu chuyển mạch ATM. Đặc tính này tương phản trực tiếp với những gì diễn ra khi các trạm cuối được thêm vào một thiết bị liên mạng như router. Các router có năng suất tổng cố định được chia cho các trạm cuối có kết nối với chúng. Khi số lượng trạm cuối gia tăng, năng suất của router tương thích cho trạm cuối thu nhỏ lại. Khi cơ cấu ATM mở rộng, mỗi thiết bị thu trạm cuối, bằng con đường của chính nó đi qua bộ chuyển mạch bằng cách cho mỗi trạm cuối băng thông chỉ định. Băng thông rộng được chỉ định của ATM với đặc tính có thể xác nhận khiến nó trở thành một kỹ thuật tuyệt hảo dùng cho bất kỳ nơi nào trong mạng cục bộ của doanh nghiệp.

Như tên gọi của nó chỉ rõ, kỹ thuật ATM sử dụng phương pháp truyền không đồng bộ (asynchronouns) các tề bào từ nguồn tới đích của chúng. Trong khi đó, ở tầng vật lý người ta có thể sử dụng các kỹ thuật truyền thông đồng bộ như SDH (hoặc SONET).

Nhận thức được vị trí chưa thể thay thế được (ít nhất cho đến những năm đầu của thế kỷ 21) của kỹ thuật ATM, hầu hết các hãng khổng lồ về máy tính và truyền thông như IBM, ATT, Digital, Hewlett - Packard, Cisco Systems, Cabletron, Bay Network,... đều đang quan tâm đặc biệt đến dòng sản phẩm hướng đến ATM của mình để tung ra thị trường. Có thể kể ra đây một số sản phẩm đó như DEC 900 Multiwitch, IBM 8250 hub, Cisco 7000 rounter, Cablectron, ATM module for MMAC hub.

Nhìn chung thị trường ATM sôi động do nhu cầu thực sự của các ứng dụng đa phương tiện. Sự nhập cuộc ngày một đông của các hãng sản xuất đã làm giảm đáng kể giá bán của các sản phẩm loại này, từ đó càng mở rộng thêm thị trường. Ngay ở Việt Nam, các dự án lớn về mạng tin học đều đã được thiết kế với hạ tầng chấp nhận được với công nghệ ATM trong tương lai.

# Chương VII CÁC DỊCH VỤ MẠNG THÔNG DỤNG

## I. DỊCH VỤ WEB

### I.1. Một số thuật ngữ cơ bản.

- **HTTP (Hypertext Transfer Protocol)**: là giao thức cho phép các máy tính giao tiếp qua Web và kết nối với nhau qua các siêu liên kết hyperlink.
- **HTML (Hypertext Markup Language)**: là ngôn ngữ định dạng dùng để tạo ra các trang Web giúp người dùng có thể đọc và truy cập từ bất kỳ máy nào trên mạng, dùng bất kỳ hệ điều hành nào.
- **WebPage**: là một trang tư liệu Web.
- **WebSite**: là tập hợp các trang Web của một tổ chức, một công ty, một web site có thể có nhiều Web Server.
- **Home page**: là trang Web đầu tin của một Web Site hoặc trang Web xuất hiện đầu tin khi khởi động Web Browser, đồng thời trang này chứa các liên kết tiêu biểu đến các trang Web còn lại.
- **HyperLink (link)**: là các mối liên kết giữa các tư liệu. Thông thường, trong một trang Web, các mối liên kết có màu xanh dương và được gạch dưới. Ngoài ra, bất kỳ một hình ảnh, văn bản nào khi di chuyển con trỏ chuột tới chuyển sang hình đều là các liên kết (link).
- **URL (Uniform Resource Locator)**: là đường dẫn chỉ tới một tập tin trong một máy chủ trên Internet. Chuỗi URL thường bao gồm: tên giao thức, tên máy chủ và đường dẫn đến tập tin trong máy chủ đó.

  Ví dụ: http://www.mait.vn/index.htm có nghĩa là: giao thức sử dụng http:// (Hypertext Transfer Protocol), tên máy chủ: www.mait.vn, đường dẫn và tên tập tin: index.htm. Lưu ý: đường dẫn sử dụng dấu "/" thay cho dấu "\".
- **IXP (Internet Exchange Provider)**: là nhà cung cấp đường truyền và cổng truy cập Internet.
- **ISP (Internet Service Provider)**: là nhà cung cấp dịch vụ Internet cho người dùng trực tiếp qua mạng điện thoại như là cấp quyền truy cập Internet, cung cấp các dịch vụ như Web, E-mail, Chat, Telnet…
- **ICP (Internet Content Provider)**: là nhà cung cấp thông tin lên Internet, thông tin được cập nhật định kỳ hay thường xuyên và thuộc nhiều lĩnh vực như thể thao, kinh tế giáo dục, chính trị, quân sự …

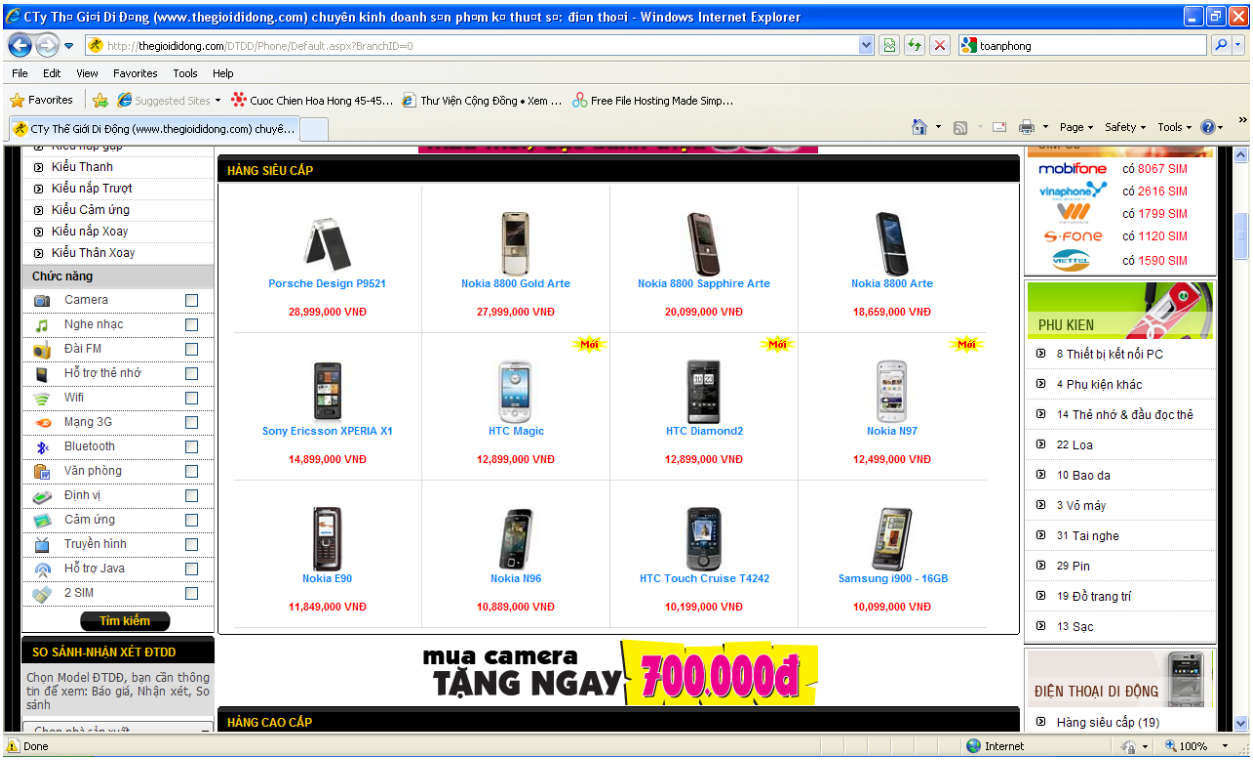
Các hoạt động chính trên Web.

- Duyệt Web tìm kiếm thông tin như số điện thoại, địa chỉ nhà, tin tức, tin dự báo thời tiết, bảng giá chứng khoán, các phần mềm miễn phí…
- Giải trí như nghe nhạc,xem phim, chơi game trên mạng.
- Trao đổi E-mail.
- Truy xuất và download các tập tin.
- Trao đổi thông tin (forum).
- Sắp xếp các chuyến đi du lịch như đặt vé máy bay, đăng ký phòng khách sạn...
- Giao dịch mua bán hàng qua mạng.

**Hình VII-1 Minh họa truy cập trang Web để tìm kiếm thông tin.**

**Hình VII-2 : Minh họa một trang Web dùng để đào tạo trực tuyến.**

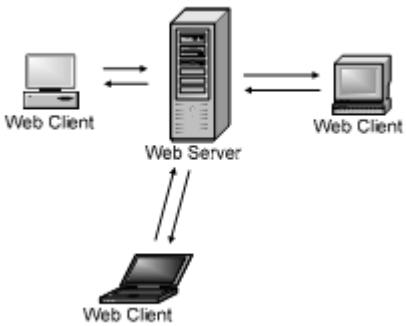
- Hội thảo từ xa.
- Quảng cáo sản phẩm.




**Hình VII-3 Minh họa Website giới thiệu sản phẩm**

## I.2. Giới thiệu mô hình hoạt động của Web.

Dịch vụ World Wide Web (viết tắt là www hoặc Web) là một dịch vụ cung cấp thông tin trên hệ thống mạng. Các thông tin này được lưu trữ dưới dạng siêu văn bản (hypertext) và thường được thiết kế bằng ngôn ngữ HTML (Hypertext Markup Language). Siêu văn bản là các tư liệu có thể là văn bản (text), hình ảnh tĩnh (image), hình ảnh động (video), âm thanh (audio)...., được liên kết với nhau qua các mối liên kết (link) và được truyền trên mạng dựa trên giao thức HTTP (Hypertext Transfer Protocol), qua đó người dùng có thể xem các tư liệu có liên quan một cách dễ dàng. Mô hình hoạt động:



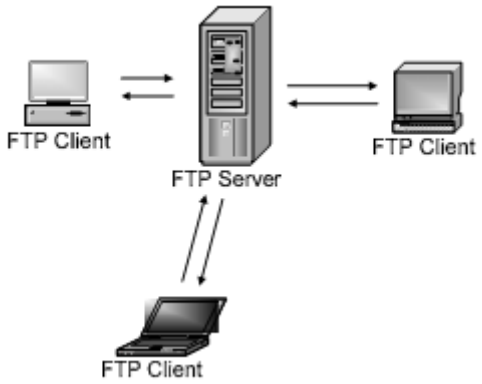

**Web server**: là một ứng dụng được cài đặt trên máy chủ trên mạng với chức năng là tiếp nhận các yêu cầu dạng HTTP từ máy trạm và tùy theo yêu cầu này máy chủ sẽ cung cấp cho máy trạm các thông tin web dạng HTML.

**Web Client**: là một ứng dụng cài trên máy trạm (máy của người dùng đầu cuối) gọi là Web Browser để gởi yêu cầu đến Web Server và nhận các thông tin phản hồi rồi hiện lên màn hình giúp người dùng có thể truy xuất được các thông tin trên máy Server. Một trong những trình duyệt Web (Web Browser) phổ biến nhất hiện nay là Internet Explorer.

# II. DỊCH VỤ FTP

## II.1. Mô hình hoạt động của FTP

FTP (File Transfer Protocol) là một dịch vụ cho phép ta truyền tải file giữa hai máy tính ở xa dùng giao thức TCP/IP. FTP cũng là một ứng dụng theo mô hình client-server, nghĩa là máy làm FTP Server sẽ quản lý các kết nối và cung cấp dịch vụ tập tin cho các máy trạm. Nói tóm lại FTP Server thường là một máy tính phục vụ cho việc quảng bá các tập tin cho người dùng hoặc là một nơi cho phép người dùng chia sẻ tập tin với những người dùng khác trên Internet. Máy trạm muốn kết nối vào FTP Server thì phải được Server cấp cho một account có đầy đủ các thông tin như: địa chỉ máy Server (tên hoặc địa chỉ IP), username và password. Phần lớn các FTP Server cho phép các máy trạm kết nối vào mình thông qua account anonymous (account anonymous thường được truy cập với password rỗng). Các máy trạm có thể sử dụng các lệnh ftp đã tích hợp sẵn trong hệ điều hành hoặc phần mềm chuyên dụng khác để tương tác với máy FTP Server.




**Hình VII-4: Mô hình hoạt động của FTP Server.**

## II.2. Tập hợp các lệnh FTP

| Lệnh | Chức năng |
|---|---|
| ! | Chạy chương trình command dos trên máy tính cục bộ |
| ? | Hiển thị giúp đỡ của các lệnh Ftp, lệnh này giống với lệnh Help. |
| Append | Chèn nội dung của một tập tin trên máy tính cục bộ vào cuối của một tập tin trên máy tính ở xa (máy FTP Server), dùng định dạng tập tin hiện tại. |
| Ascii | Đặt loại định dạng truyền file là ASCII, giá trị này là mặc định khi khởi tạo kết nối FTP. |
| Bell | Bật trạng thái chuông là on/off. Nếu là on thì sau mỗi lần lệnh truyền file hoàn thành thì máy phát ra tiếng chuông. Mặc định trạng thái này là off. |
| Binary | Đặt loại định dạng truyền file là binary. |
| Bye | Tắt kết nối với máy tính ở xa và thoát khỏi chương trình FTP. |
| Cd | Thay đổi thư mục hiện thành trên máy ở xa(Server). |
| Close | Ngừng phiên giao dịch với máy tính ở xa và trở về dòng lệnh |

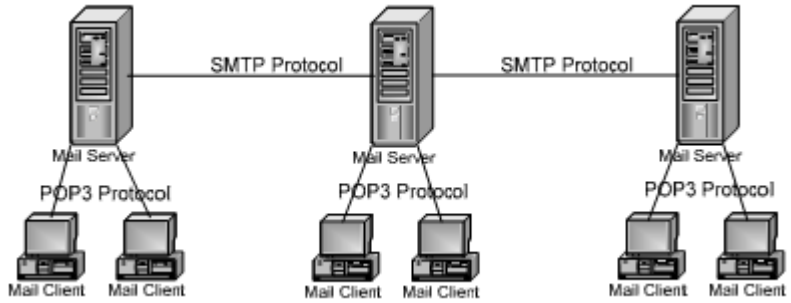
| | |
|---|---|
| | của chương trình ftp. |
| **Debug** | Bật trạng thái Debugg on/off. Nếu là on thì mỗi lệnh gởi đến máy tính ở xa thì chương trình sẽ in ra các thông báo. Mặc định là trạng thái là off. |
| **Delete** | Xoá tập tin trên máy tính ở xa. |
| **Dir** | Hiển thị danh sách các tập tin và thư mục con trong thư mục hiện tại. |
| **Disconnect** | Tắt kết nối với máy tính ở xa và trở về dòng lệnh FTP. |
| **Get** | Chép một tập tin từ máy tính ở xa về máy tính cục bộ, dùng định dạng truyền file hiện tại. |
| **Help** | Hiển thị giúp đỡ của các lệnh Ftp. |
| **Lcd** | Thay đổi thư mục hiện trên máy tính cục bộ. Mặc định là thư mục đang làm việc trên máy tính cục bộ. |
| **Ls** | Hiển thị danh sách các tập tin và thư mục con trong thư mục hiện tại. |
| **Mdelete** | Xóa nhiều tập tin cùng trên một máy tính ở xa. |
| **Mget** | Chép nhiều tập tin từ máy tính ở xa về máy tính cục bộ dùng định dạng truyền file hiện tại. |
| **mkdir** | Tạo thư mục trên máy tính ở xa. |
| **Mput** | Chép nhiều tập tin ở máy tính cục bộ lên máy tính ở xa dùng định dạng truyền file hiện tại. |
| **open** | Mở một kết nối đến máy FTP Server. |
| **Put** | Chép một tập tin ở máy tính cục bộ lên máy tính ở xa dùng định dạng truyền file hiện tại. |
| **Pwd** | Hiển thị thư mục hiện hành trên máy tính ở xa. |
| **Quit** | Tắt kết nối với máy tính ở xa và thoát khỏi chương trình FTP. |
| **Recv** | Chép một tập tin từ máy tính ở xa về máy tính cục bộ, dùng định dạng truyền file hiện tại. Tương tự như lệnh |
| **Rename** | Đổi tên tập tin, thư mục trên máy tính ở xa. |
| **Rmdir** | Xóa một thư mục ở xa. |
| **Send** | Chép một tập tin ở máy tính cục bộ lên máy tính ở xa dùng định dạng truyền file hiện tại. Tương tự như Put. |
| **Status** | Hiển thị các trạng thái lựa chọn của kết nối FTP. |

# III. E-MAIL.

## III.1. Mô hình hoạt động

E-mail (electronic mail) là thư điện tử, là một hình thức trao đổi thư từ nhưng thông qua mạng Internet. Dịch vụ này được sử dụng rất phổ biến và không đòi hỏi hai máy tính gởi và nhận thư phải kết nối online trên mạng..

Tại mỗi Mail Server thông thường gồm hai dịch vụ: POP3 (Post Office Protocol 3) làm nhiệm vụ giao tiếp mail giữa Mail Client và Mail Server, SMTP (Simple E-mail Transfer Protocol) làm nhiệm vụ giao tiếp mail giữa các máy Mail Server.




**Hình VII-5 : Mô hình hoạt động của Mail Server.**

Để sử dụng E-mail, người dùng cần có một account mail do nhà cung cấp dịch vụ Internet (ISP) cấp bao gồm các thông tin sau: địa chỉ mail (ví dụ: nvteo@hcm.vnn.vn), username, password và địa chỉ của Mail Server mà mình đăng ký. Sau đó chọn một chương trình Mail Client (Outlook Express, Eudora, Netscape...) và cấu hình các thông số trên vào chương trình đó. Từ đó bạn có thể sử dụng chương trình này để soạn thảo và gởi nhận mail một cách dễ dàng.

## III.2. Các loại mail.

Thông thường có hai loại mail thông dụng là WebMail và POP Mail. Webmail là loại mail mà hình thức giao dịch mail giữa Client và Server dựa trên giao thức Web (http), thông thường Webmail là miễn phí. Còn POP Mail là loại mail mà các Mail Client tương tác với MAIL SERVER bằng giao thức POP3. Mail loại này tiện lợi và an toàn hơn nên thông thường là phải đăng ký thuê bao với nhà cung cấp dịch vụ.

## III.3. Sử dụng WebMail.

Bạn muốn có một địa chỉ mail Internet để giao dịch với bạn bè trên thế giới, bạn có thể đến nhà cung cấp dịch vụ Internet để đăng ký hoặc tự tạo cho mình một địa chỉ mail miễn phí trên các Website nổi tiếng như Yahoo, Hotmail, Fpt, Vnn...

www.viet-ebook.co.cc

# GIÁO TRÌNH
# MẠNG MÁY TÍNH

Hà nội 11-2000

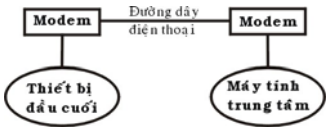
www.viet-ebook.co.cc

**Chương 1**

# Sơ lược lịch sử phát triển của mạng máy tính

Vào giữa những năm 50 khi những thế hệ máy tính đầu tiên được đưa vào hoạt động thực tế với những bóng đèn điện tử thì chúng có kích thước rất cồng kềnh và tốn nhiều năng lượng. Hồi đó việc nhập dữ liệu vào các máy tính được thông qua các tấm bìa mà người viết chương trình đã đục lỗ sẵn. Mỗi tấm bìa tương đương với một dòng lệnh mà mỗi một cột của nó có chứa tất cả các ký tự cần thiết mà người viết chương trình phải đục lỗ vào ký tự mình lựa chọn. Các tấm bìa được đưa vào một "thiết bị" gọi là thiết bị đọc bìa mà qua đó các thông tin được đưa vào máy tính (hay còn gọi là trung tâm xử lý) và sau khi tính toán kết quả sẽ được đưa ra máy in. Như vậy các thiết bị đọc bìa và máy in được thể hiện như các thiết bị vào ra (I/O) đối với máy tính. Sau một thời gian các thế hệ máy mới được đưa vào hoạt động trong đó một máy tính trung tâm có thể được nối với nhiều thiết bị vào ra (I/O) mà qua đó nó có thể thực hiện liên tục hết chương trình này đến chương trình khác.

Cùng với sự phát triển của những ứng dụng trên máy tính các phương pháp nâng cao khả năng giao tiếp với máy tính trung tâm cũng đã được đầu tư nghiên cứu rất nhiều. Vào giữa những năm 60 một số nhà chế tạo máy tính đã nghiên cứu thành công những thiết bị truy cập từ xa tới máy tính của họ. Một trong những phương pháp thâm nhập từ xa được thực hiện bằng việc cài đặt một thiết bị đầu cuối ở một vị trí cách xa trung tâm tính toán, thiết bị đầu cuối này được liên kết với trung tâm bằng việc sử dụng đường dây điện thoại và với hai thiết bị xử lý tín hiệu (thường gọi là Modem) gắn ở hai đầu và tín hiệu được truyền thay vì trực tiếp thì thông qua dây điện thoại.




*Hình 1.1. Mô hình truyền dữ liệu từ xa đầu tiên*

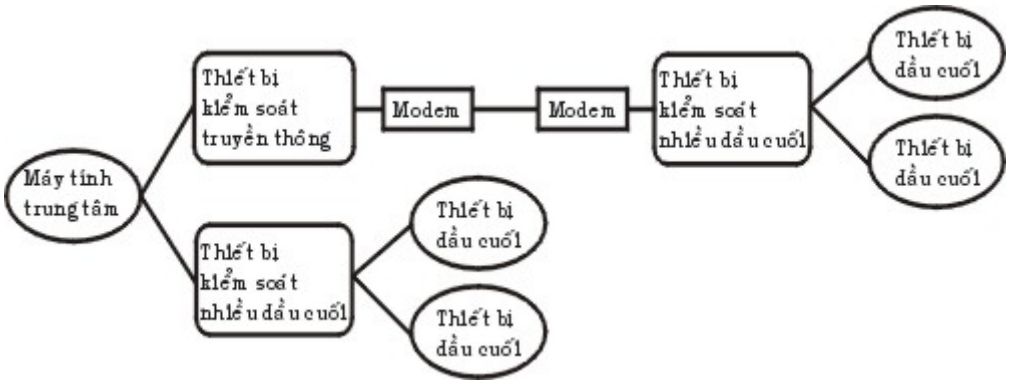
Những dạng đầu tiên của thiết bị đầu cuối bao gồm máy đọc bìa, máy in, thiết bị xử lý tín hiệu, các thiết bị cảm nhận. Việc liên kết từ xa đó có thể thực hiên thông qua những vùng khác nhau và đó là những dạng đầu tiên của hệ thống mạng.

Trong lúc đưa ra giới thiệu những thiết bị đầu cuối từ xa, các nhà khoa học đã triển khai một loạt những thiết bị điều khiển, những thiết bị đầu cuối đặc biệt cho phép người sử dụng nâng cao được khả năng tương tác với máy tính. Một trong những sản phẩm quan trọng đó là hệ thống thiết bị đầu cuối 3270 của IBM. Hệ thống đó bao gồm các màn hình, các hệ thống điều khiển, các thiết bị truyền thông được liên kết với các trung tâm tính toán. Hệ thống 3270 được giới thiệu vào năm 1971 và được sử dụng dùng để mở rộng khả năng tính toán của trung tâm máy tính tới các vùng xa. Để làm giảm nhiệm vụ truyền thông của máy tính trung tâm và số lượng các liên kết giữa máy tính trung tâm với các thiết bị đầu cuối, IBM và các công ty máy tính khác đã sản xuất một số các thiết bị sau:

- **Thiết bị kiểm soát truyền thông**: có nhiệm vụ nhận các bit tín hiệu từ các kênh truyền thông, gom chúng lại thành các byte dữ liệu và chuyển nhóm các byte đó tới máy tính trung tâm để xử lý, thiết bị này cũng thực hiện công việc ngược lại để chuyển tín hiệu trả lời của máy tính trung tâm tới các trạm ở xa. Thiết bị trên cho

phép giảm bớt được thời gian xử lý trên máy tính trung tâm và xây dựng các thiết bị logic đặc trưng.

- **Thiết bị kiểm soát nhiều đầu cuối**: cho phép cùng một lúc kiểm soát nhiều thiết bị đầu cuối. Máy tính trung tâm chỉ cần liên kết với một thiết bị như vậy là có thể phục vụ cho tất cả các thiết bị đầu cuối đang được gắn với thiết bị kiểm soát trên. Điều này đặc biệt có ý nghĩa khi thiết bị kiểm soát nằm ở cách xa máy tính vì chỉ cần sử dụng một đường điện thoại là có thể phục vụ cho nhiều thiết bị đầu cuối.




*Hình 1.2: Mô hình trao đổi mạng của hệ thống 3270*

Vào giữa những năm 1970, các thiết bị đầu cuối sử dụng những phương pháp liên kết qua đường cáp nằm trong một khu vực đã được ra đời. Với những ưu điểm từ nâng cao tốc độ truyền dữ liệu và qua đó kết hợp được khả năng tính toán của các máy tính lại với nhau. Để thực hiện việc nâng cao khả năng tính toán với nhiều máy tính các nhà sản xuất bắt đầu xây dựng các mạng phức tạp. Vào những năm 1980 các hệ thống đường truyền tốc độ cao đã được thiết lập ở Bắc Mỹ và Châu Âu và từ đó cũng xuất hiện các nhà cung cấp các dịnh vụ truyền thông với những đường truyền có tốc độ cao hơn nhiều lần so với đường dây điện thoại. Với những chi phí thuê bao chấp nhận được, người ta có thể sử dụng được các đường truyền này để liên kết máy tính lại với nhau và bắt đầu hình thành các mạng một cách rộng khắp. Ở đây các nhà cung cấp dịch vụ đã xây dựng những đường truyền dữ liệu liên kết giữa các thành phố và khu vực với nhau và sau đó cung cấp các dịch vụ truyền dữ liệu cho những người xây dựng mạng. ầ gười xây dựng mạng lúc này sẽ không cần xây dựng lại đường truyền của mình mà chỉ cần sử dụng một phần các năng lực truyền thông của các nhà cung cấp.

Vào năm 1974 công ty IBM đã giới thiệu một loạt các thiết bị đầu cuối được chế tạo cho lĩnh vực ngân hàng và thương mại, thông qua các dây cáp mạng các thiết bị đầu cuối có thể truy cập cùng một lúc vào một máy tính dùng chung. Với việc liên kết các máy tính nằm ở trong một khu vực nhỏ như một tòa nhà hay là một khu nhà thì tiền chi phí cho các thiết bị và phần mềm là thấp. Từ đó việc nghiên cứu khả năng sử dụng chung môi trường truyền thông và các tài nguyên của các máy tính nhanh chóng được đầu tư.

Vào năm 1977, công ty Datapoint Corporation đã bắt đầu bán hệ điều hành mạng của mình là "Attached Resource Computer ầ etwork" (hay gọi tắt là Arcnet) ra thị trường. Mạng Arcnet cho phép liên kết các máy tính và các trạm đầu cuối lại bằng dây cáp mạng, qua đó đã trở thành là hệ điều hành mạng cục bộ đầu tiên.

Từ đó đến nay đã có rất nhiều công ty đưa ra các sản phẩm của mình, đặc biệt khi các máy tính cá nhân được sử dụng một cánh rộng rãi. Khi số lượng máy vi tính trong một văn phòng hay cơ quan được tăng lên nhanh chóng thì việc kết nối chúng trở nên vô cùng cần thiết và sẽ mang lại nhiều hiệu quả cho người sử dụng.

ả gày nay với một lượng lớn về thông tin, nhu cầu xử lý thông tin ngày càng cao. Mạng máy tính hiện nay trở nên quá quen thuộc đối với chúng ta, trong mọi lĩnh vực như khoa học, quân sự, quốc phòng, thương mại, dịch vụ, giáo dục... Hiện nay ở nhiều nơi mạng đã trở thành một nhu cầu không thể thiếu được. ả gười ta thấy được việc kết nối các máy tính thành mạng cho chúng ta những khả năng mới to lớn như:

- **Sử dụng chung tài nguyên:** ả hững tài nguyên của mạng (như thiết bị, chương trình, dữ liệu) khi được trở thành các tài nguyên chung thì mọi thành viên của mạng đều có thể tiếp cận được mà không quan tâm tới những tài nguyên đó ở đâu.

- **Tăng độ tin cậy của hệ thống**: ả gười ta có thể dễ dàng bảo trì máy móc và lưu trữ (backup) các dữ liệu chung và khi có trục trặc trong hệ thống thì chúng có thể được khôi phục nhanh chóng. Trong trường hợp có trục trặc trên một trạm làm việc thì người ta cũng có thể sử dụng những trạm khác thay thế.

- **Nâng cao chất lượng và hiệu quả khai thác thông tin:** Khi thông tin có thể được sữ dụng chung thì nó mang lại cho người sử dụng khả năng tổ chức lại các công việc với những thay đổi về chất như:

    - Đáp ứng những nhu cầu của hệ thống ứng dụng kinh doanh hiện đại.
    - Cung cấp sự thống nhất giữa các dữ liệu.
    - Tăng cường năng lực xử lý nhờ kết hợp các bộ phận phân tán.
    - Tăng cường truy nhập tới các dịch vụ mạng khác nhau đang được cung cấp trên thế giới.

Với nhu cầu đòi hỏi ngày càng cao của xã hội nên vấn đề kỹ thuật trong mạng là mối quan tâm hàng đầu của các nhà tin học. Ví dụ như làm thế nào để truy xuất thông tin một cách nhanh chóng và tối ưu nhất, trong khi việc xử lý thông tin trên mạng quá nhiều đôi khi có thể làm tắc nghẽn trên mạng và gây ra mất thông tin một cách đáng tiếc.

Hiện nay việc làm sao có được một hệ thống mạng chạy thật tốt, thật an toàn với lợi ích kinh tế cao đang rất được quan tâm. Một vấn đề đặt ra có rất nhiều giải pháp về công nghệ, một giải pháp có rất nhiều yếu tố cấu thành, trong mỗi yếu tố có nhiều cách lựa chọn. ả hư vậy để đưa ra một giải pháp hoàn chỉnh, phù hợp thì phải trải qua một quá trình chọn lọc dựa trên những ưu điểm của từng yếu tố, từng chi tiết rất nhỏ.

Để giải quyết một vấn đề phải dựa trên những yêu cầu đặt ra và dựa trên công nghệ để giải quyết. ả hưng công nghệ cao nhất chưa chắc là công nghệ tốt nhất, mà công nghệ tốt nhất là công nghệ phù hợp nhất.

www.viet-ebook.co.cc

Chương 2

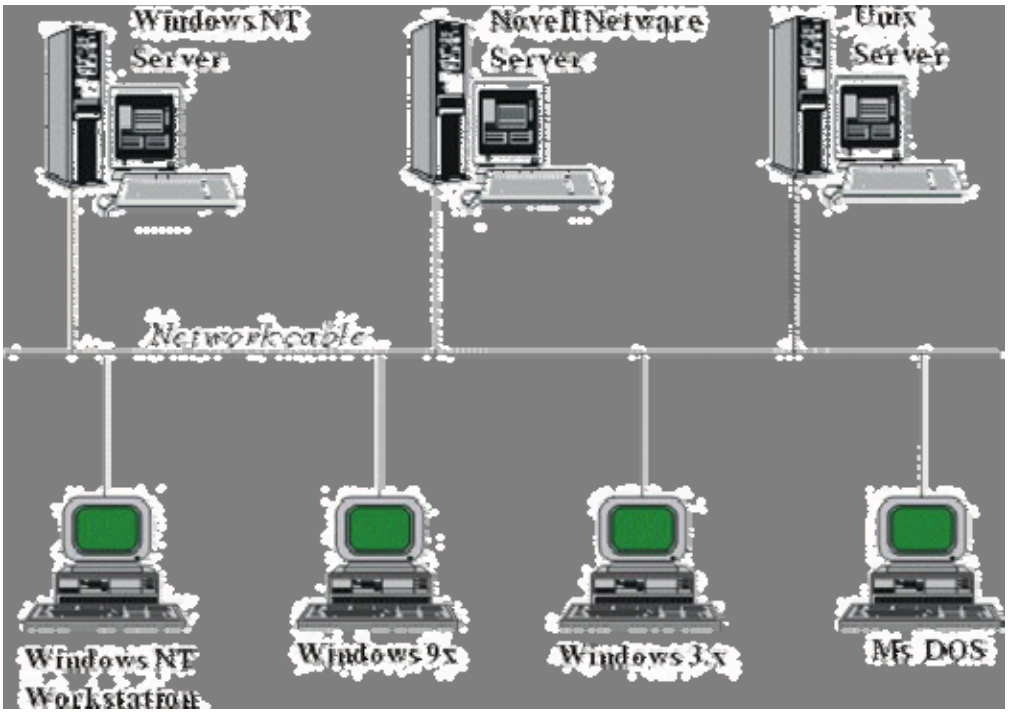
# Những khái niệm cơ bản của mạng máy tính

Với sự phát triển của khoa học và kỹ thuật, hiện nay các mạng máy tính đã phát triển một cách nhanh chóng và đa dạng cả về quy mô, hệ điều hành và ứng dụng. Do vậy việc nghiên cứu chúng ngày càng trở nên phức tạp. Tuy nhiên các mạng máy tính cũng có cùng các điểm chung thông qua đó chúng ta có thể đánh giá và phân loại chúng.

## I. Định nghĩa mạng máy tính

> *Mạng máy tính là một tập hợp các máy tính được nối với nhau bởi đường truyền theo một cấu trúc nào đó và thông qua đó các máy tính trao đổi thông tin qua lại cho nhau.*

Đường truyền là hệ thống các thiết bị truyền dẫn có dây hay không dây dùng để chuyển các tín hiệu điện tử từ máy tính này đến máy tính khác. Các tín hiệu điện tử đó biểu thị các giá trị dữ liệu dưới dạng các xung nhị phân (on - off). Tất cả các tín hiệu được truyền giữa các máy tính đều thuộc một dạng sóng điện từ. Tùy theo tần số của sóng điện từ có thể dùng các đường truyền vật lý khác nhau để truyền các tín hiệu. Ở đây đường truyền được kết nối có thể là dây cáp đồng trục, cáp xoắn, cáp quang, dây điện thoại, sóng vô tuyến ... Các đường truyền dữ liệu tạo nên cấu trúc của mạng. Hai khái niệm đường truyền và cấu trúc là những đặc trưng cơ bản của mạng máy tính.




*Hình 2.1: Một mô hình liên kết các máy tính trong mạng*

Với sự trao đổi qua lại giữa máy tính này với máy tính khác đã phân biệt mạng máy tính với các hệ thống thu phát một chiều như truyền hình, phát thông tin từ vệ tinh xuống các trạm thu thụ động... vì tại đây chỉ có thông tin một chiều từ nơi phát đến nơi thu mà không quan tâm đến có bao nhiêu nơi thu, có thu tốt hay không.

Đặc trưng cơ bản của đường truyền vật lý là giải thông. Giải thông của một đường chuyền chính là độ đo phạm vi tần số mà nó có thể đáp ứng được. Tốc độ truyền dữ liệu trên đường truyền còn được gọi là thông lượng của đường truyền - thường được tính bằng số lượng bit được truyền đi trong một giây (Bps). Thông lượng còn được đo bằng đơn vị khác là Baud (lấy từ tên nhà bác học - Emile Baudot). Baud biểu thị số lượng thay đổi tín hiệu trong một giây.

Ở đây Baud và Bps không phải bao giờ cũng đồng nhất. Ví dụ: nếu trên đường dây có 8 mức tín hiệu khác nhau thì mỗi mức tín hiệu tương ứng với 3 bit hay là 1 Baud tương ứng với 3 bit. Chỉ khi có 2 mức tín hiệu trong đó mỗi mức tín hiệu tương ứng với 1 bit thì 1 Baud mới tương ứng với 1 bit.

## II. Phân loại mạng máy tính

Do hiện nay mạng máy tính được phát triển khắp nơi với những ứng dụng ngày càng đa dạng cho nên việc phân loại mạng máy tính là một việc rất phức tạp. ả gười ta có thể chia các mạng máy tính theo khoảng cách địa lý ra làm hai loại: Mạng diện rộng và Mạng cục bộ.

- **Mạng cục bộ (Local Area Networks - LAN)** là mạng được thiết lập để liên kết các máy tính trong một khu vực như trong một toà nhà, một khu nhà.

- **Mạng diện rộng (Wide Area Networks - WAN)** là mạng được thiết lập để liên kết các máy tính của hai hay nhiều khu vực khác nhau như giữa các thành phố hay các tỉnh.

Sự phân biệt trên chỉ có tính chất ước lệ, các phân biệt trên càng trở nên khó xác định với việc phát triển của khoa học và kỹ thuật cũng như các phương tiện truyền dẫn. Tuy nhiên với sự phân biệt trên phương diện địa lý đã đưa tới việc phân biệt trong nhiều đặc tính khác nhau của hai loại mạng trên, việc nghiên cứu các phân biệt đó cho ta hiểu rõ hơn về các loại mạng.

## III. Sự phân biệt giữa mạng cục bộ và mạng diện rộng

Mạng cục bộ và mạng diện rộng có thể được phân biệt bởi: địa phương hoạt động, tốc độ đường truyền và tỷ lệ lỗi trên đường truyền, chủ quản của mạng, đường đi của thông tin trên mạng, dạng chuyển giao thông tin.

***Địa phương hoạt động*:** Liên quan đến khu vực địa lý thì mạng cục bộ sẽ là mạng liên kết các máy tính nằm ở trong một khu vực nhỏ. Khu vực có thể bao gồm một tòa nhà hay là một khu nhà... Điều đó hạn chế bởi khoảng cách đường dây cáp được dùng để liên kết các máy tính của mạng cục bộ (Hạn chế đó còn là hạn chế của khả năng kỹ thuật của đường truyền dữ liệu). ả gược lại mạng diện rộng là mạng có khả năng liên kết các máy tính trong một vùng rộng lớn như là một thành phố, một miền, một đất nước, mạng diện rộng được xây dựng để nối hai hoặc nhiều khu vực địa lý riêng biệt.

***Tốc độ đường truyền và tỷ lệ lỗi trên đường truyền*:** Do các đường cáp của mạng cục bộ đươc xây dựng trong một khu vực nhỏ cho nên nó ít bị ảnh hưởng bởi tác động của thiên nhiên (như là sấm chớp, ánh sáng...). Điều đó cho phép mạng cục bộ có thể truyền dữ liệu với tốc độ cao mà chỉ chịu một tỷ lệ lỗi nhỏ. ả gược lại với mạng diện rộng do phải

truyền ở những khoảng cách khá xa với những đường truyền dẫn dài có khi lên tới hàng ngàn km. Do vậy mạng diện rộng không thể truyền với tốc độ quá cao vì khi đó tỉ lệ lỗi sẽ trở nên khó chấp nhận được.

Mạng cục bộ thường có tốc độ truyền dữ liệu từ 4 đến 16 Mbps và đạt tới 100 Mbps nếu dùng cáp quang. Còn phần lớn các mạng diện rộng cung cấp đường truyền có tốc độ thấp hơn nhiều như T1 với 1.544 Mbps hay E1 với 2.048 Mbps.

(Ở đây bps (Bit Per Second) là một đơn vị trong truyền thông tương đương với 1 bit được truyền trong một giây, ví dụ như tốc độ đường truyền là 1 Mbps tức là có thể truyền tối đa 1 Megabit trong 1 giây trên đường truyền đó).

Thông thường trong mạng cục bộ tỷ lệ lỗi trong truyền dữ liệu vào khoảng $1/10^7$-$10^8$ còn trong mạng diện rộng thì tỷ lệ đó vào khoảng $1/10^6$ - $10^7$

***Chủ quản và điều hành của mạng:*** Do sự phức tạp trong việc xây dựng, quản lý, duy trì các đường truyền dẫn nên khi xây dựng mạng diện rộng người ta thường sử dụng các đường truyền được thuê từ các công ty viễn thông hay các nhà cung cấp dịch vụ truyền số liệu. Tùy theo cấu trúc của mạng những đường truyền đó thuộc cơ quan quản lý khác nhau như các nhà cung cấp đường truyền nội hạt, liên tỉnh, liên quốc gia. Các đường truyền đó phải tuân thủ các quy định của chính phủ các khu vực có đường dây đi qua như: tốc độ, việc mã hóa.

Còn đối với mạng cục bộ thì công việc đơn giản hơn nhiều, khi một cơ quan cài đặt mạng cục bộ thì toàn bộ mạng sẽ thuộc quyền quản lý của cơ quan đó.

***Đường đi của thông tin trên mạng:*** Trong mạng cục bộ thông tin được đi theo con đường xác định bởi cấu trúc của mạng. Khi người ta xác định cấu trúc của mạng thì thông tin sẽ luôn luôn đi theo cấu trúc đã xác định đó. Còn với mạng diện rộng dữ liệu cấu trúc có thể phức tạp hơn nhiều do việc sử dụng các dịch vụ truyền dữ liệu. Trong quá trình hoạt động các điểm nút có thể thay đổi đường đi của các thông tin khi phát hiện ra có trục trặc trên đường truyền hay khi phát hiện có quá nhiều thông tin cần truyền giữa hai điểm nút nào đó. Trên mạng diện rộng thông tin có thể có các con đường đi khác nhau, điều đó cho phép có thể sử dụng tối đa các năng lực của đường truyền hay nâng cao điều kiện an toàn trong truyền dữ liệu.

***Dạng chuyển giao thông tin:*** Phần lớn các mạng diện rộng hiện nay được phát triển cho việc truyền đồng thời trên đường truyền nhiều dạng thông tin khác nhau như: video, tiếng nói, dữ liệu... Trong khi đó các mạng cục bộ chủ yếu phát triển trong việc truyền dữ liệu thông thường. Điều này có thể giải thích do việc truyền các dạng thông tin như video, tiếng nói trong một khu vực nhỏ ít được quan tâm hơn như khi truyền qua những khoảng cách lớn.

Các hệ thống mạng hiện nay ngày càng phức tạp về chất lượng, đa dạng về chủng loại và phát triển rất nhanh về chất. Trong sự phát triển đó số lượng những nhà sản xuất từ phần mềm, phần cứng máy tính, các sản phẩm viễn thông cũng tăng nhanh với nhiều sản phẩm đa dạng. Chính vì vậy vai trò chuẩn hóa cũng mang những ý nghĩa quan trọng. Tại các nước các cơ quan chuẩn quốc gia đã đưa ra các những chuẩn về phần cứng và các quy định

về giao tiếp nhằm giúp cho các nhà sản xuất có thể làm ra các sản phẩm có thể kết nối với các sản phẩm do hãng khác sản xuất.

www.viet-ebook.co.cc

Chương 3

# Mô hình truyền thông

## I. Sự cần thiết phải có mô hình truyền thông

Để một mạng máy tính trở một môi trường truyền dữ liệu thì nó cần phải có những yếu tố sau:

- Mỗi máy tính cần phải có một địa chỉ phân biệt trên mạng.
- Việc chuyển dữ liệu từ máy tính này đến máy tính khác do mạng thực hiện thông qua những quy định thống nhất gọi là giao thức của mạng.

Khi các máy tính trao đổi dữ liệu với nhau thì một quá trình truyền giao dữ liệu đã được thực hiện hoàn chỉnh. Ví dụ như để thực hiện việc truyền một file giữa một máy tính với một máy tính khác cùng được gắn trên một mạng các công việc sau đây phải được thực hiện:

- Máy tính cần truyền cần biết địa chỉ của máy nhận.
- Máy tính cần truyền phải xác định được máy tính nhận đã saün sàng nhận thông tin
- Chương trình gửi file trên máy truyền cần xác định được rằng chương trình nhận file trên máy nhận đã saün sàng tiếp nhận file.
- ả ếu cấu trúc file trên hai máy không giống nhau thì một máy phải làm nhiệm vụ chuyển đổi file từ dạng này sang dạng kia.
- Khi truyền file máy tính truyền cần thông báo cho mạng biết địa chỉ của máy nhận để các thông tin được mạng đưa tới đích.

Điều trên đó cho thấy giữa hai máy tính đã có một sự phối hợp hoạt động ở mức độ cao. Bây giờ thay vì chúng ta xét cả quá trình trên như là một quá trình chung thì chúng ta sẽ chia quá trình trên ra thành một số công đoạn và mỗi công đoạn con hoạt động một cách độc lập với nhau. Ở đây chương trình truyền nhận file của mỗi máy tính được chia thành ba module là: Module truyền và nhận File, Module truyền thông và Module tiếp cận mạng. Hai module tương ứng sẽ thực hiện việc trao đổi với nhau trong đó:

- *Module truyền và nhận file* cần được thực hiện tất cả các nhiệm vụ trong các ứng dụng truyền nhận file. Ví dụ: truyền nhận thông số về file, truyền nhận các mẫu tin của file, thực hiện chuyển đổi file sang các dạng khác nhau nếu cần. Module truyền và nhận file không cần thiết phải trực tiếp quan tâm tới việc truyền dữ liệu trên mạng như thế nào mà nhiệm vụ đó được giao cho Module truyền thông.
- *Module truyền thông* quan tâm tới việc các máy tính đang hoạt động và saün sàng trao đổi thông tin với nhau. ả ó còn kiểm soát các dữ liệu sao cho những dữ liệu

này có thể trao đổi một cách chính xác và an toàn giữa hai máy tính. Điều đó có nghĩa là phải truyền file trên nguyên tắc đảm bảo an toàn cho dữ liệu, tuy nhiên ở đây có thể có một vài mức độ an toàn khác nhau được dành cho từng ứng dụng. Ở đây việc trao đổi dữ liệu giữa hai máy tính không phụ thuộc vào bản chất của mạng đang liên kết chúng. ả những yêu cầu liên quan đến mạng đã được thực hiện ở module thứ ba là module tiếp cận mạng và nếu mạng thay đổi thì chỉ có module tiếp cận mạng bị ảnh hưởng.

- *Module tiếp cận mạng* được xây dựng liên quan đến các quy cách giao tiếp với mạng và phụ thuộc vào bản chất của mạng. ả ó đảm bảo việc truyền dữ liệu từ máy tính này đến máy tính khác trong mạng.

ả hư vậy thay vì xét cả quá trình truyền file với nhiều yêu cầu khác nhau như một tiến trình phức tạp thì chúng ta có thể xét quá trình đó với nhiều tiến trình con phân biệt dựa trên việc trao đổi giữa các Module tương ứng trong chương trình truyền file. Cách này cho phép chúng ta phân tích kỹ quá trình file và dễ dàng trong việc viết chương trình.

Việc xét các module một cách độc lập với nhau như vậy cho phép giảm độ phức tạp cho việc thiết kế và cài đặt. Phương pháp này được sử dụng rộng rãi trong việc xây dựng mạng và các chương trình truyền thông và được gọi là phương pháp phân tầng (layer).

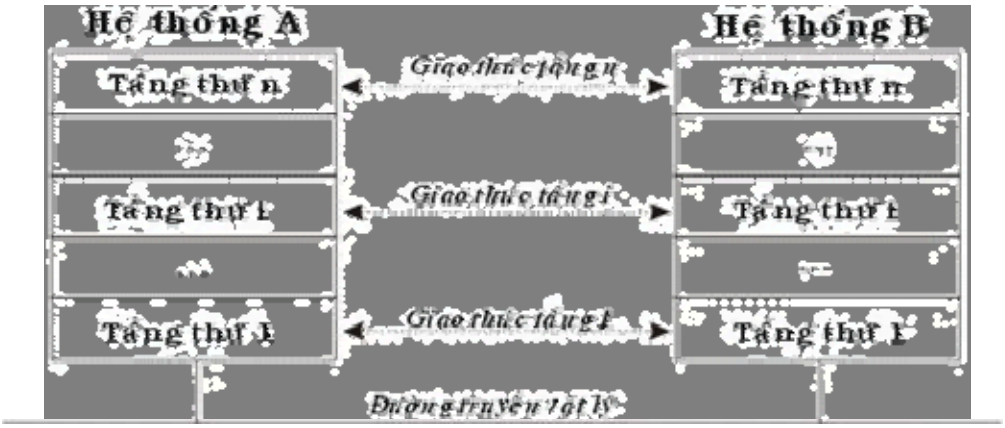
ả guyên tắc của phương pháp phân tầng là:

- Mỗi hệ thống thành phần trong mạng được xây dựng như một cấu trúc nhiều tầng và đều có cấu trúc giống nhau như: số lượng tầng và chức năng của mỗi tầng.

- Các tầng nằm chồng lên nhau, dữ liệu được chỉ trao đổi trực tiếp giữa hai tầng kề nhau từ tầng trên xuống tầng dưới và ngược lại.

- Cùng với việc xác định chức năng của mỗi tầng chúng ta phải xác định mối quan hệ giữa hai tầng kề nhau. Dữ liệu được truyền đi từ tầng cao nhất của hệ thống truyền lần lượt đến tầng thấp nhất sau đó truyền qua đường nối vật lý dưới dạng các bit tới tầng thấp nhất của hệ thống nhận, sau đó dữ liệu được truyền ngược lên lần lượt đến tầng cao nhất của hệ thống nhận.

- Chỉ có hai tầng thấp nhất có liên kết vật lý với nhau còn các tầng trên cùng thứ tư chỉ có các liên kết logic với nhau. Liên kết logic của một tầng được thực hiện thông qua các tầng dưới và phải tuân theo những quy định chặt chẽ, các quy định đó được gọi giao thức của tầng.




*Hình 3.1: Mô hình phân tầng gồm N tầng*

## II. Mô hình truyền thông đơn giản 3 tầng

ả ói chung trong truyền thông có sự tham gia của các thành phần: các chương trình ứng dụng, các chương trình truyền thông, các máy tính và các mạng. Các chương trình ứng dụng là các chương trình của người sử dụng được thực hiện trên máy tính và có thể tham gia vào quá trình trao đổi thông tin giữa hai máy tính. Trên một máy tính với hệ điều hành đa nhiệm (như Windows, Uả IX) thường được thực hiện đồng thời nhiều ứng dụng trong đó có những ứng dụng liên quan đến mạng và các ứng dụng khác. Các máy tính được nối với mạng và các dữ liệu được trao đổi thông qua mạng từ máy tính này đến máy tính khác.

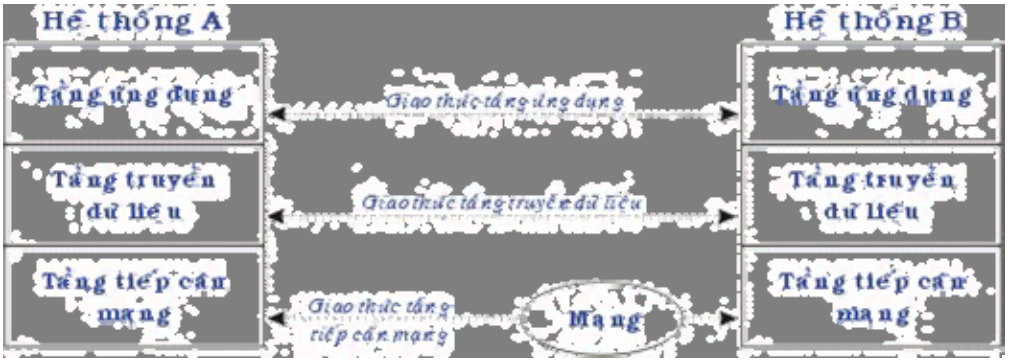
Việc gửi dữ liệu được thực hiện giữa một ứng dụng với một ứng dụng khác trên hai máy tính khác nhau thông qua mạng được thực hiện như sau: Ứng dụng gửi chuyển dữ liệu cho chương trình truyền thông trên máy tính của nó, chương trình truyền thông sẽ gửi chúng tới máy tính nhận. Chương trình truyền thông trên máy nhận sẽ tiếp nhận dữ liệu, kiểm tra nó trước khi chuyển giao cho ứng dụng đang chờ dữ liệu.

Với mô hình truyền thông đơn giản người ta chia chương trình truyền thông thành ba tầng không phụ thuộc vào nhau là: tầng ứng dụng, tầng chuyển vận và tầng tiếp cận mạng.

- ***Tầng tiếp cận mạng*** liên quan tới việc trao đổi dữ liệu giữa máy tính và mạng mà nó được nối vào. Để dữ liệu đến được đích máy tính gửi cần phải chuyển địa chỉ của máy tính nhận cho mạng và qua đó mạng sẽ chuyển các thông tin tới đích. ả goài ra máy gửi có thể sử dụng một số phục vụ khác nhau mà mạng cung cấp như gửi ưu tiên, tốc độ cao. Trong tầng này có thể có nhiều phần mềm khác nhau được sử dụng phụ thuộc vào các loại của mạng ví dụ như mạng chuyển mạch, mạng chuyển mạch gói, mạng cục bộ.

- ***Tầng truyền dữ liệu*** thực hiện quá trình truyền thông không liên quan tới mạng và nằm ở trên tầng tiếp cận mạng. Tầng truyền dữ liệu không quan tâm tới bản chất các ứng dụng đang trao đổi dữ liệu mà quan tâm tới làm sao cho các dữ liệu được trao đổi một cách an toàn. Tầng truyền dữ liệu đảm bảo các dữ liệu đến được đích và đến theo đúng thứ tự mà chúng được xử lý. Trong tầng truyền dữ liệu người ta phải có những cơ chế nhằm đảm bảo sự chính xác đó và rõ ràng các cơ chế này không phụ thuộc vào bản chất của từng ứng dụng và chúng sẽ phục vụ cho tất cả các ứng dụng.

- ***Tầng ứng dụng*** sẽ chứa các module phục vụ cho tất cả những ứng dụng của người sử dụng. Với các loại ứng dụng khác nhau (như là truyền file, truyền thư mục) cần các module khác nhau.




*Hình 3.2 Mô hình truyền thông 3 tầng*

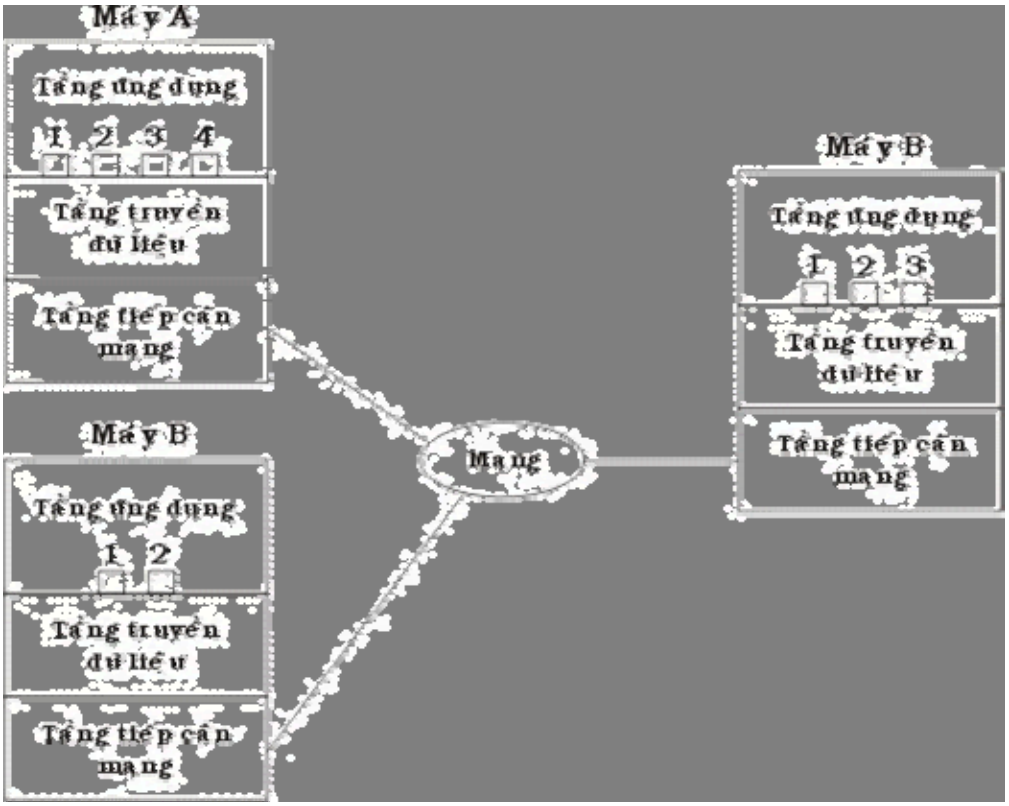
Trong một mạng với nhiều máy tính, mỗi máy tính một hay nhiều ứng dụng thực hiện đồng thời (Tại đây ta xét trên một máy tính trong một thời điểm có thể chạy nhiều ứng dụng và các ứng dụng đó có thể thực hiện đồng thời việc truyền dữ liệu qua mạng). Một ứng dụng khi cần truyền dữ liệu qua mạng cho một ứng dụng khác cần phải gọi 1 module tầng ứng dụng của chương trình truyền thông trên máy của mình, đồng thời ứng dụng kia cũng sẽ gọi 1 module tầng ứng dụng trên máy của nó. Hai module ứng dụng sẽ liên kết với nhau nhằm thực hiện các yêu cầu của các chương trình ứng dụng.

Các ứng dụng đó sẽ trao đổi với nhau thông qua mạng, tuy nhiên trong 1 thời điểm trên một máy có thể có nhiều ứng dụng cùng hoạt động và để việc truyền thông được chính xác thì các ứng dụng trên một máy cần phải có một địa chỉ riêng biệt. Rõ ràng cần có hai lớp địa chỉ:

- Mỗi máy tính trên mạng cần có một địa chỉ mạng của mình, hai máy tính trong cùng một mạng không thể có cùng địa chỉ, điều đó cho phép mạng có thể truyền thông tin đến từng máy tính một cách chính xác.

- Mỗi một ứng dụng trên một máy tính cần phải có địa chỉ phân biệt trong máy tính đo. ả ó cho phép tầng truyền dữ liệu giao dữ liệu cho đúng ứng dụng đang cần. Địa chỉ đó được gọi là điểm tiếp cận giao dịch. Điều đó cho thấy mỗi một ứng dụng sẽ tiếp cận các phục vụ của tầng truyền dữ liệu một cách độc lập.

- Các module cùng một tầng trên hai máy tính khác nhau sẽ trao đổi với nhau một cách chặt chẽ theo các qui tắc xác định trước được gọi là giao thức. Một giao thức được thể hiện một cách chi tiết bởi các chức năng cần phải thực hiện như các giá trị kiểm tra lỗi, việc định dạng các dữ liệu, các quy trình cần phải thực hiện để trao đổi thông tin.




*Hình 3.3 Ví dụ mô hình truyền thông đơn giản*

Chúng ta hãy xét trong ví dụ (như hình vẽ trên): giả sử có ứng dụng có điểm tiếp cận giao dịch 1 trên máy tính A muốn gửi thông tin cho một ứng dụng khác trên máy tính B có điểm tiếp cận giao dịch 2. Ứng dụng trên máy tính A chuyển các thông tin xuống tầng truyền dữ liệu của A với yêu cầu gửi chúng cho điểm tiếp cận giao dịch 2 trên máy tính B. Tầng truyền dữ liệu máy A sẽ chuyển các thông tin xuống tầng tiếp cận mạng máy A với yêu cầu chuyển chúng cho máy tính B (Chú ý rằng mạng không cần biết địa chỉ của điểm tiếp cận giao dịch mà chỉ cần biết địa chỉ của máy tính B). Để thực hiện quá trình này, các thông tin kiểm soát cũng sẽ được truyền cùng với dữ liệu.

Đầu tiên khi ứng dụng 1 trên máy A cần gửi một khối dữ liệu nó chuyển khối đó cho tầng vận chuyển. Tầng vận chuyển có thể chia khối đó ra thành nhiều khối nhỏ phụ thuộc vào yêu cầu của giao thức của tầng và đóng gói chúng thành các gói tin (packet). Mỗi một gói tin sẽ được bổ sung thêm các thông tin kiểm soát của giao thức và được gọi là phần đầu (Header) của gói tin. Thông thường phần đầu của gói tin cần có:

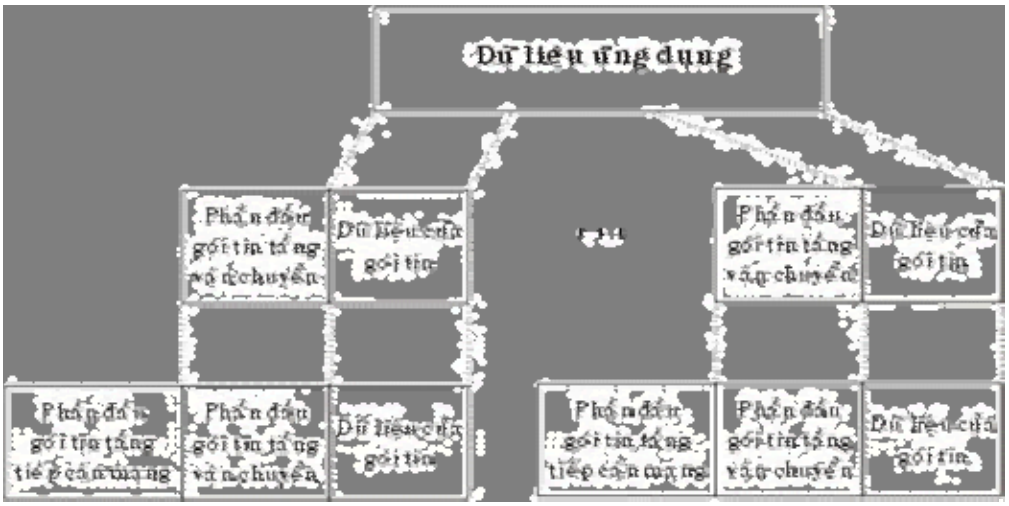
- ***Địa chỉ của điểm tiếp cận giao dịch nơi đến* (Ở đây là 3):** khi tầng vận chuyển của máy B nhận được gói tin thì nó biết được ứng dụng nào mà nó cần giao.

- ***Số thứ tự*** của gói tin, khi tầng vận chuyển chia một khối dữ liệu ra thành nhiều gói tin thì nó cần phải đánh số thứ tự các gói tin đó. ả ếu chúng đi đến đích nếu sai thứ tự thì tầng vận chuyển của máy nhận có thể phát hiện và chỉnh lại thứ tự. ả goài ra nếu có lỗi trên đường truyền thì tầng vận chuyển của máy nhận sẽ phát hiện ra và yêu cầu gửi lại một cách chính xác.

- ***Mã sửa lỗi*:** để đảm bảo các dữ liệu được nhận một cách chính xác thì trên cơ sở các dữ liệu của gói tin tầng vận chuyển sẽ tính ra một giá trị theo một công thức có

sãn và gửi nó đi trong phần đầu của gói tin. Tầng vận chuyển nơi nhận thông qua giá trị đó xác định được gói tin đó có bị lỗi trên đường truyền hay không.

Bước tiếp theo tầng vận chuyển máy A sẽ chuyển từng gói tin và địa chỉ của máy tính đích (ở đây là B) xuống tầng tiếp cận mạng với yêu cầu chuyển chúng đi. Để thực hiện được yêu cầu này tầng tiếp cận mạng cũng tạo các gói tin của mình trước khi truyền qua mạng. Tại đây giao thức của tầng tiếp cận mạng sẽ thêm các thông tin điều khiển vào phần đầu của gói tin mạng.




*Hình 3.4: Mô hình thiết lập gói tin*

Trong phần đầu gói tin mạng sẽ bao gồm địa chỉ của máy tính nhận, dựa trên địa chỉ này mạng truyền gói tin tới đích. ầ goài ra có thể có những thông số như là mức độ ưu tiên.

ầ hư vậy thông qua mô hình truyền thông đơn giản chúng ta cũng có thể thấy được phương thức hoạt động của các máy tính trên mạng, có thể xây dựng và thay đổi các giao thức trong cùng một tầng.

### III. Các nhu cầu về chuẩn hóa đối với mạng

Trong phần trên chúng ta đã xem xét một mô hình truyền thông đơn giản, trong thực tế việc phân chia các tầng như trong mô hình trên thực sự chưa đủ. Trên thế giới hiện có một số cơ quan định chuẩn, họ đưa ra hàng loạt chuẩn về mạng tuy các chuẩn đó có tính chất khuyến nghị chứ không bắt buộc nhưng chúng rất được các cơ quan chuẩn quốc gia coi trọng.

Hai trong số các cơ quan chuẩn quốc tế là:

- **ISO (The International Standards Organization) -** Là tổ chức tiêu chuẩn quốc tế hoạt động dưới sự bảo trợ của Liên hợp Quốc với thành viên là các cơ quan chuẩn quốc gia với số lượng khoảng hơn 100 thành viên với mục đích hỗ trợ sự phát triển các chuẩn trên phạm vi toàn thế giới. Một trong những thành tựu của ISO trong lãnh vực truyền thông là mô hình hệ thống mở (Open Systems Interconnection - gọi tắt là OSI).

- **CCITT (Commité Consultatif International pour le Telegraphe et la Téléphone) -** Tổ chức tư vấn quốc tế về điện tín và điện thoại làm việc dưới sự bảo trợ của Liên Hiệp Quốc có trụ sở chính tại Geneva - Thụy sỹ. Các thành viên chủ yếu là các cơ quan bưu chính viễn thông các quốc gia. Tổ chức này có vai trò phát triển các khuyến nghị trong các lãnh vực viễn thông.

## IV. Một số mô hình chuẩn hóa

### 1. Mô hình OSI (Open Systems Interconnection)

Mô hình OSI là một cơ sở dành cho việc chuẩn hoá các hệ thống truyền thông, nó được nghiên cứu và xây dựng bởi ISO. Việc nghiên cứu về mô hình OSI được bắt đầu tại ISO vào năm 1971 với mục tiêu nhằm tới việc nối kết các sản phẩm của các hãng sản xuất khác nhau và phối hợp các hoạt động chuẩn hoá trong các lĩnh vực viễn thông và hệ thống thông tin. Theo mô hình OSI chương trình truyền thông được chia ra thành 7 tầng với những chức năng phân biệt cho từng tầng. Hai tầng đồng mức khi liên kết với nhau phải sử dụng một giao thức chung. Trong mô hình OSI có hai loại giao thức chính được áp dụng: giao thức có liên kết (connection - oriented) và giao thức không liên kết (connectionless)

- ***Giao thức có liên kết*:** trước khi truyền dữ liệu hai tầng đồng mức cần thiết lập một liên kết logic và các gói tin được trao đổi thông qua liên kết náy, việc có liên kết logic sẽ nâng cao độ an toàn trong truyền dữ liệu.

- ***Giao thức không liên kết*:** trước khi truyền dữ liệu không thiết lập liên kết logic và mỗi gói tin được truyền độc lập với các gói tin trước hoặc sau nó.

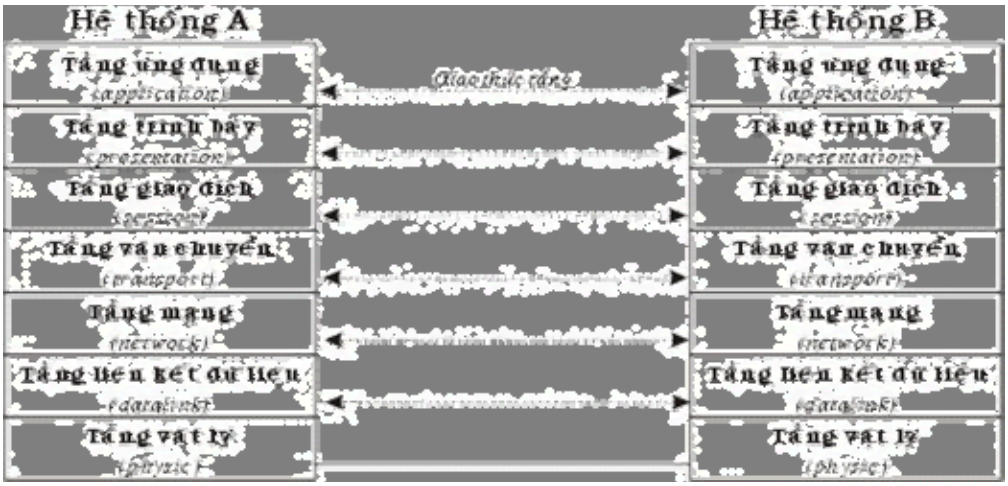
ả hiệm vụ của các tầng trong mô hình OSI:

- **Tầng ứng dụng (Application layer)**: tầng ứng dụng quy định giao diện giữa người sử dụng và môi trường OSI, nó cung cấp các phương tiện cho người sử dụng truy cập vả sử dụng các dịch vụ củ mô hình OSI.

- **Tầng trình bày (Presentation layer)**: tầng trình bày chuyển đổi các thông tin từ cú pháp người sử dụng sang cú pháp để truyền dữ liệu, ngoài ra nó có thể nén dữ liệu truyền và mã hóa chúng trước khi truyền đễ bảo mật.

- **Tầng giao dịch (Session layer)**: tầng giao dịch quy định một giao diện ứng dụng cho tầng vận chuyển sử dụng. ả ó xác lập ánh xa giữa các tên đặt địa chỉ, tạo ra các tiếp xúc ban đầu giữa các máy tính khác nhau trên cơ sở các giao dịch truyền thông. ả ó đặt tên nhất quán cho mọi thành phần muốn đối thoại riêng với nhau.

- **Tầng vận chuyển (Transport layer)**: tầng vận chuyển xác định địa chỉ trên mạng, cách thức chuyển giao gói tin trên cơ sở trực tiếp giữa hai đầu mút (end-to-end). Để bảo đảm được việc truyền ổn định trên mạng tầng vận chuyển thường đánh số các gói tin và đảm bảo chúng chuyển theo thứ tự.




*Hình 3.5: Mô hình 7 tầng OSI*

- **Tầng mạng (Network layer)**: tầng mạng có nhiệm vụ xác định việc chuyển hướng, vạch đường các gói tin trong mạng, các gói tin này có thể phải đi qua nhiều chặng trước khi đến được đích cuối cùng.

- **Tầng liên kết dữ liệu (Data link layer):** tầng liên kết dữ liệu có nhiệm vụ xác định cơ chế truy nhập thông tin trên mạng, các dạng thức chung trong các gói tin, đóng các gói tin...

- **Tầng vật lý (Phisical layer)**: tầng vật lý cung cấp phương thức truy cập vào đường truyền vật lý để truyền các dòng Bit không cấu trúc, ngoài ra nó cung cấp các chuẩn về điện, dây cáp, đầu nối, kỹ thuật nối mạch điện, điện áp, tốc độ cáp truyền dẫn, giao diện nối kết và các mức nối kết..

### 2. Mô hình SNA (Systems Netword Architecture)

Tháng 9/1973, Hãng IBM giới thiệu một kiến trúc mạng máy tính Sả A (System ả etwork Architecture). Đến năm 1977 đã có 300 trạm Sả A được cài đặt. Cuối năm 1978, số lượng đã tăng lên đến 1250, rồi cứ theo đà đó cho đến nayđã có 20.000 trạm Sả A đang được hoạt động. Qua con số này chúng ta có thể hình dung được mức độ quan trọng và tầm ảnh hưởng của Sả A trên toàn thế giới.

Cần lưu ý rằng Sả A không là một chuẩn quốc tế chính thức như OSI nhưng do vai trò to lớn của hãng IBM trên thị trường Cả TT nên Sả A trở thành một loại chuẩn thực tế và khá phổ biến. Sả A là một đặc tả gồm rất nhiều tài liệu mô tả kiến trúc của mạng xử lý dữ liệu phân tán. ả ó định nghĩa các quy tắc và các giao thức cho sự tương tác giữa các thành phần (máy tính, trạm cuối, phần mềm) trong mạng.

Sả A được tổ chức xung quanh khái niệm miền (domain). Một Sả A domain là một điểm điều khiển các dịch vụ hệ thống (Systems Services control point - SSCP) và nó sẽ điều khiển tất cả các tài nguyên đó, Các tài nguyên ở đây có thể là các đơn vị vật lý, các đơn vị logic, các liên kết dữ liệu và các thiết bị. Có thể ví SSCP như là "trái tim và khối óc" của Sả A. ả ó điều khiển Sả A domain bằng cách gói các lệnh tới một đơn vị vật lý, đơn vị vật lý này sau khi nhận được lệnh sẽ quản lý tất cả các tài nguyên trực tiếp với nó. đơn vị vật

lý thực sự là một "đối tác" của SSCP và chứa một tập con các khả năng của SSCP. Các Đơn vị vật lý đảm nhiệm việc quản lý của mỗi nút Sả A.

Sả A phân biệt giữa các nút miền con (Subarea node) và các nút ngoại vi (peripheral node).

- Một nút miền con có thể dẫn đường cho dữ liệu của người sử dụng qua toàn bộ mạng. ả ó dùng địa chỉ mạng và một số hiệu đường (router suember) để xác định đường truyền đi tới nút kế tiếp trong mạng.

- Một nút ngoại vi có tính cục bộ hơn. ả ó không dẫn đường giữa các nút miền con. Các nút được nối và điều khiển theo giao thức SDLC (Synchronous Data Link Control). Mỗi nút ngoại vi chỉ liên lạc được với nút miền con mà nó nối vào.

Mạng Sả A dựa trên cơ chế phân tầng, trước đây thì 2 hệ thống ngang hàng không được trao đổi trực tiếp. Sau này phát triển thành Sả A mở rộng: Lúc này hai tầng ngang hàng nhau có thể trao đổi trực tiếp. Với 6 tầng có tên gọi và chức năng tất như sau:

- **Tầng quản trị chức năng SNA (SNA Function Manegement)** Tầng này thật ra có thể chia tầng này làm hai tầng như sau:

- **Tầng dịch vụ giao tác (Transaction)** cung cấp các dịch vụ ứng dụng đến người dùng một mạng Sả A. ả những dịch vụ đó như : DIA cung cấp các tài liệu phân bố giữa các hệ thống văn phòng, Sả A DS (văn phòng dịch vụ phân phối) cho việc truyền thông bất đồng bộ giữa các ứng dụng phân tán và hệ thống văn phòng. Tầng dịch vụ giao tác cũng cung cấp các dịch vụ và cấu hình, các dịch vụ quản lý để điều khiển các hoạt động mạng.

- **Tầng dịch vụ trình diễn (Presentation Services):** tầng này thì liên quan với sự hiển thị các ứng dụng, người sử dụng đầu cuối và các dữ liệu hệ thống. Tầng này cũng định nghĩa các giao thức cho việc truyền thông giữa các chương trình và điều khiển truyền thông ở mức hội thoại.

- **Tầng kiểm soát luồng dữ liệu (Data flow control)** tầng này cung cấp các dịch vụ điều khiểnluồng lưu thông cho các phiên từ logic này đến đơn vị logic khác (LU - LU). ả ó thực hiện điều này bằng cách gán các số trình tự, các yêu cầu và đáp ứng, thực hiện các giao thức yêu cầu về đáp ứng giao dịch và hợp tác giữa các giao dịch gởi và nhận. ả ói chung nó yểm trợ phương thức khai thác hai chiều đồng thời (Full duplex).

- **Tầng kiểm soát truyền (Transmission control):** Tầng này cung cấp các điều khiển cơ bản của các phần tài nguyên truyền trong mạng, bằng cách xác định số trình tự nhận được, và quản lý việc theo dõi mức phiên. Tầng này cũng hỗ trợ cho việc mã hóa dữ liệu và cung cấp hệ thống hỗ trợ cho các nút ngoại vi.

- **Tầng kiểm soát đường dẫn (Path control):** Tầng này cung cấp các giao thức để tìm đường cho một gói tin qua mạng Sả A và để kết nối với các mạng Sả A khác, đồng thời nó cũng kiểm soát các đường truyền này.

- **Tầng kiểm soát liên kết dữ liệu (Data Link Control):** Tầng này cung cấp các giao thức cho việc truyền các gói tin thông qua đường truyền vật lý giữa hai node

và cũng cung cấp các điều khiển lưu thông và phục hồi lỗi, các hỗ trợ cho tầng này là các giao thức SDLC, System/370, X25, IEEE 802.2 và 802.5.

- **Tầng kiểm soát vật lý (Physical control):** Tầng này cung cấp một giao diện vật lý cho bất cứ môi trường truyền thông nào mà gắn với nó. Tầng nào định nghĩa các đặc trưng của tín hiệu cần để thiết lập, duy trì và kết thúc các đường nối vật lý cho việc hỗ trợ kết nối.

*Hình 3.6: Tương ứng các tầng các kiến trúc SNI và OSI*

www.viet-ebook.co.cc

**Chương 4**

# Mô hình kết nối các hệ thống mở

# Open Systems Interconection

Việc nghiên cứu về OSI được bắt đầu tại ISO vào năm 1971 với các mục tiêu nhằm nối kết các sản phẩm của các hãng sản xuất khác. Ưu điểm chính của OSI là ở chỗ nó hứa hẹn giải pháp cho vấn đề truyền thông giữa các máy tính không giống nhau. Hai hệ thống, dù có khác nhau đều có thể truyền thông với nhau một các hiệu quả nếu chúng đảm bảo những điều kiện chung sau đây:

Chúng cài đặt cùng một tập các chức năng truyền thông.

Các chức năng đó được tổ chức thành cùng một tập các tầng. các tầng đồng mức phải cung cấp các chức năng như nhau.

Các tầng đồng mức khi trao đổi với nhau sử dụng chung một giao thức

Mô hình OSI tách các mặt khác nhau của một mạng máy tính thành bảy tầng theo mô hình phân tầng. Mô hình OSI là một khung mà các tiêu chuẩn lập mạng khác nhau có thể khớp vào. Mô hình OSI định rõ các mặt nào của hoạt động của mạng có thể nhằm đến bởi các tiêu chuẩn mạng khác nhau. Vì vậy, theo một nghĩa nào đó, mô hình OSI là một loại tiêu chuẩn của các chuẩn.

## I. Nguyên tắc sử dụng khi định nghĩa các tầng hệ thống mở:

Sau đây là các nguyên tắc mà ISO quy định dùng trong quá trình xây dựng mô hình OSI

- Không định nghĩa quá nhiều tầng để việc xác định và ghép nối các tầng không quá phức tạp.
- Tạo các ranh giới các tầng sao cho việc giải thích các phục vụ và số các tương tác qua lại hai tầng là nhỏ nhất.
- Tạo các tầng riêng biệt cho các chức năng khác biệt nhau hoàn toàn về kỹ thuật sử dụng hoặc quá trình thực hiên.
- Các chức năng giống nhau được đặt trong cùng một tầng.
- Lựa chọn ranh giới các tầng tại các điểm mà những thử nghiệm trong quá khứ thành công.
- Các chức năng được xác định sao cho chúng có thể dễ dàng xác định lại, và các nghi thức của chúng có thể thay đổi trên mọi hướng.
- Tạo ranh giới các tầng mà ở đó cần có những mức độ trừu tượng khác nhau trong việc sử dụng số liệu.

- Cho phép thay đổi các chức năng hoặc giao thức trong tầng không ảnh hưởng đến các tầng khác.

- Tạo các ranh giới giữa mỗi tầng với tầng trên và dưới nó.

**II. Các giao thức trong mô hình OSI**

Trong mô hình OSI có hai loại giao thức chính được áp dụng: giao thức có liên kết (connection - oriented) và giao thức không liên kết (connectionless).

- *Giao thức có liên kết*: trước khi truyền dữ liệu hai tầng đồng mức cần thiết lập một liên kết logic và các gói tin được trao đổi thông qua liên kết náy, việc có liên kết logic sẽ nâng cao độ an toàn trong truyền dữ liệu.

- *Giao thức không liên kết*: trước khi truyền dữ liệu không thiết lập liên kết logic và mỗi gói tin được truyền độc lập với các gói tin trước hoặc sau nó.

ả hư vậy với giao thức có liên kết, quá trình truyền thông phải gồm 3 giai đoạn phân biệt:

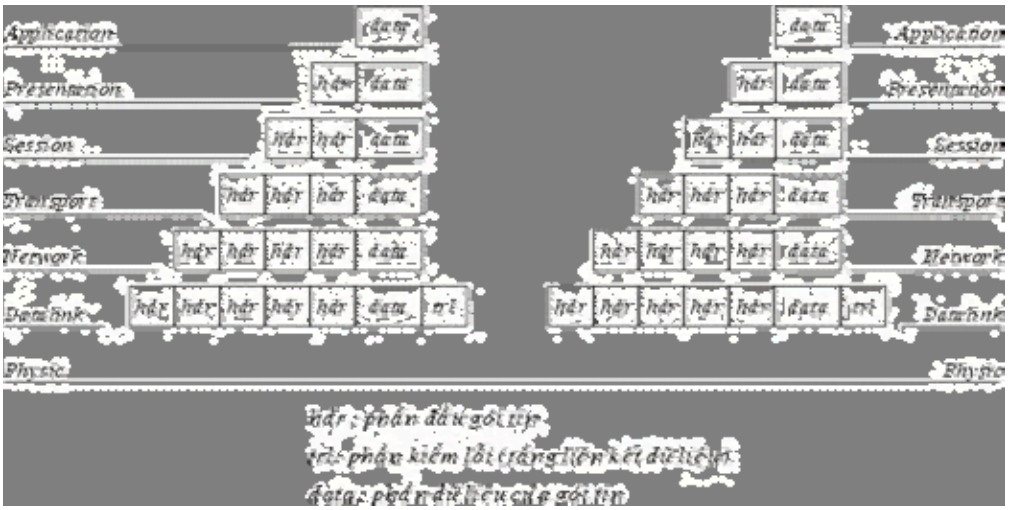
- *Thiết lập liên kết (logic):* hai thực thể đồng mức ở hai hệ thống thương lượng với nhau về tập các tham số sẽ sử dụng trong giai đoạn sau (truyền dữ liệu).

- *Truyền dữ liệu*: dữ liệu được truyền với các cơ chế kiểm soát và quản lý kèm theo (như kiểm soát lỗi, kiểm soát luồng dữ liệu, cắt/hợp dữ liệu...) để tăng cường độ tin cậy và hiệu quả của việc truyền dữ liệu.

- *Hủy bỏ liên kết (logic):* giải phóng tài nguyên hệ thống đã được cấp phát cho liên kết để dùng cho liên kết khác.

Đối với giao thức không liên kết thì chỉ có duy nhất một giai đoạn truyền dữ liệu mà thôi.

Gói tin của giao thức: Gói tin (Packet) được hiểu như là một đơn vị thông tin dùng trong việc liên lạc, chuyển giao dữ liệu trong mạng máy tính. ả hững thông điệp (message) trao đổi giữa các máy tính trong mạng, được tạo dạng thành các gói tin ở máy nguồn. Và những gói tin này khi đích sẽ được kết hợp lại thành thông điệp ban đầu. Một gói tin có thể chứa đựng các yêu cầu phục vụ, các thông tin điều khiển và dữ liệu.



*Hình 4.1: Phương thức xác lập các gói tin trong mô hình OSI*

Trên quan điểm mô hình mạng phân tầng tầng mỗi tầng chỉ thực hiện một chức năng là nhận dữ liệu từ tầng bên trên để chuyển giao xuống cho tầng bên dưới và ngược lại. Chức năng này thực chất là gắn thêm và gỡ bỏ phần đầu (header) đối với các gói tin trước khi chuyển nó đi. ả ói cách khác, từng gói tin bao gồm phần đầu (header) và phần dữ liệu. Khi đi đến một tầng mới gói tin sẽ được đóng thêm một phần đầu đề khác và được xem như là gói tin của tầng mới, công việc trên tiếp diễn cho tới khi gói tin được truyền lên đường dây mạng để đến bên nhận.

Tại bên nhận các gói tin được gỡ bỏ phần đầu trên từng tầng tướng ứng và đây cũng là nguyên lý của bất cứ mô hình phân tầng nào.

***Chú ý:*** Trong mô hình OSI phần kiểm lỗi của gói tin tầng liên kết dữ liệu đặt ở cuối gói tin

## III. Các chức năng chủ yếu của các tầng của mô hình OSI.

### Tầng 1: Vật lý (Physical)

Tầng vật lý (Physical layer) là tầng dưới cùng của mô hình OSI là. ả ó mô tả các đặc trưng vật lý của mạng: Các loại cáp được dùng để nối các thiết bị, các loại đầu nối được dùng , các dây cáp có thể dài bao nhiêu v.v... Mặt khác các tầng vật lý cung cấp các đặc trưng điện của các tín hiệu được dùng để khi chuyển dữ liệu trên cáp từ một máy này đến một máy khác của mạng, kỹ thuật nối mạch điện, tốc độ cáp truyền dẫn.

Tầng vật lý không qui định một ý nghĩa nào cho các tín hiệu đó ngoài các giá trị nhị phân 0 và 1. Ở các tầng cao hơn của mô hình OSI ý nghĩa của các bit được truyền ở tầng vật lý sẽ được xác định.

***Ví dụ:*** Tiêu chuẩn Ethernet cho cáp xoắn đôi 10 baseT định rõ các đặc trưng điện của cáp xoắn đôi, kích thước và dạng của các đầu nối, độ dài tối đa của cáp.

Khác với các tầng khác, tầng vật lý là không có gói tin riêng và do vậy không có phần đầu (header) chứa thông tin điều khiển, dữ liệu được truyền đi theo dòng bit. Một giao thức tầng vật lý tồn tại giữa các tầng vật lý để quy định về phương thức truyền (đồng bộ, phi đồng bộ), tốc độ truyền.

Các giao thức được xây dựng cho tầng vật lý được phân chia thành phân chia thành hai loại giao thức sử dụng phương thức truyền thông dị bộ (asynchronous) và phương thức truyền thông đồng bộ (synchronous).

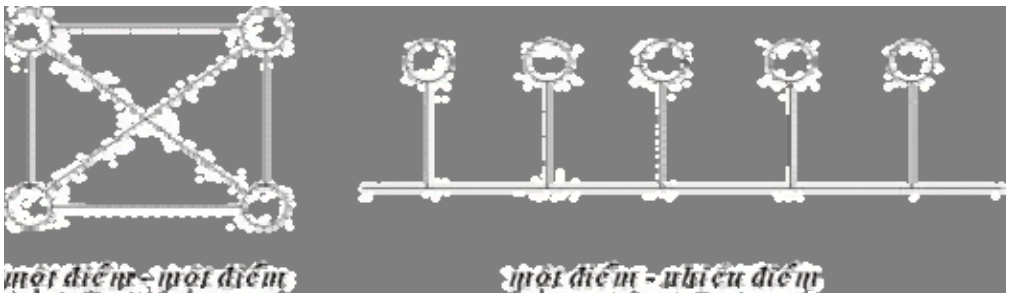
- *Phương thức truyền dị bộ*: không có một tín hiệu quy định cho sự đồng bộ giữa các bit giữa máy gửi và máy nhận, trong quá trình gửi tín hiệu máy gửi sử dụng các bit đặc biệt START và STOP được dùng để tách các xâu bit biểu diễn các ký tự trong dòng dữ liệu cần truyền đi. ả ó cho phép một ký tự được truyền đi bất kỳ lúc nào mà không cần quan tâm đến các tín hiệu đồng bộ trước đó.

- *Phương thức truyền đồng bộ*: sử dụng phương thức truyền cần có đồng bộ giữa máy gửi và máy nhận, nó chèn các ký tự đặc biệt như SYả (Synchronization), EOT (End Of Transmission) hay đơn giản hơn, một cái "cờ " (flag) giữa các dữ liệu của máy gửi để báo hiệu cho máy nhận biết được dữ liệu đang đến hoặc đã đến.

### Tầng 2: Liên kết dữ liệu (Data link)

Tầng liên kết dữ liệu (data link layer) là tầng mà ở đó ý nghĩa được gán cho các bít được truyền trên mạng. Tầng liên kết dữ liệu phải quy định được các dạng thức, kích thước, địa chỉ máy gửi và nhận của mỗi gói tin được gửi đi. ả ó phải xác định cơ chế truy nhập thông tin trên mạng và phương tiện gửi mỗi gói tin sao cho nó được đưa đến cho người nhận đã định.

Tầng liên kết dữ liệu có hai phương thức liên kết dựa trên cách kết nối các máy tính, đó là phương thức "một điểm - một điểm" và phương thức "một điểm - nhiều điểm". Với phương thức "một điểm - một điểm" các đường truyền riêng biệt được thiết lập để nối các cặp máy tính lại với nhau. Phương thức "một điểm - nhiều điểm " tất cả các máy phân chia chung một đường truyền vật lý.




*Hình 4.2: Các đường truyền kết nối kiểu "một điểm - một điểm" và "một điểm - nhiều điểm".*

Tầng liên kết dữ liệu cũng cung cấp cách phát hiện và sửa lỗi cơ bản để đảm bảo cho dữ liệu nhận được giống hoàn toàn với dữ liệu gửi đi. ả ếu một gói tin có lỗi không sửa được, tầng liên kết dữ liệu phải chỉ ra được cách thông báo cho nơi gửi biết gói tin đó có lỗi để nó gửi lại.

Các giao thức tầng liên kết dữ liệu chia làm 2 loại chính là các giao thức hướng ký tư và các giao thức hướng bit. Các giao thức hướng ký tự được xây dựng dựa trên các ký tự đặc biệt của một bộ mã chuẩn nào đó (như ASCII hay EBCDIC), trong khi đó các giao thức hướng bit lại dùng các cấu trúc nhị phân (xâu bit) để xây dựng các phần tử của giao thức (đơn vị dữ liệu, các thủ tục.) và khi nhận, dữ liệu sẽ được tiếp nhận lần lượt từng bit một.

### Tầng 3: Mạng (Network)

Tầng mạng (network layer) nhắm đến việc kết nối các mạng với nhau bằng cách tìm đường (routing) cho các gói tin từ một mạng này đến một mạng khác. ả ó xác định việc chuyển hướng, vạch đường các gói tin trong mạng, các gói này có thể phải đi qua nhiều chặng trước khi đến được đích cuối cùng. ả ó luôn tìm các tuyến truyền thông không tắc nghẽn để đưa các gói tin đến đích.

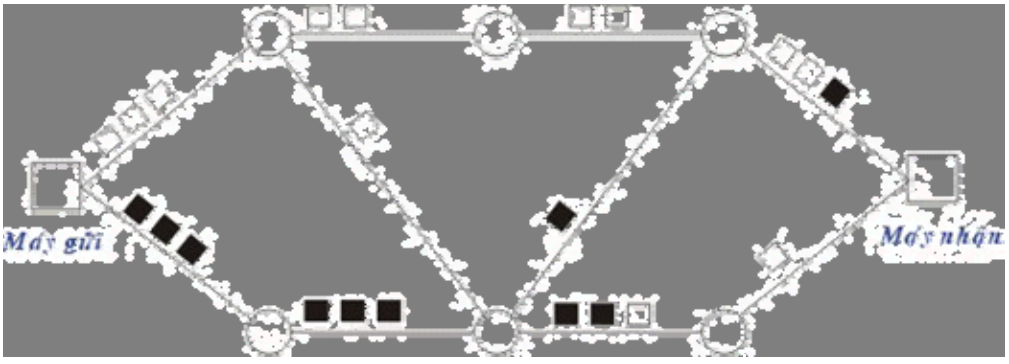
Tầng mạng cung các các phương tiện để truyền các gói tin qua mạng, thậm chí qua một mạng của mạng (network of network). Bởi vậy nó cần phải đáp ứng với nhiều kiểu mạng và nhiều kiểu dịch vụ cung cấp bởi các mạng khác nhau. hai chức năng chủ yếu của tầng mạng là chọn đường (routing) và chuyển tiếp (relaying). Tầng mạng là quan trọng nhất khi liên kết hai loại mạng khác nhau như mạng Ethernet với mạng Token Ring khi đó phải dùng một bộ tìm đường (quy định bởi tầng mạng) để chuyển các gói tin từ mạng này sang mạng khác và ngược lại.

Đối với một mạng chuyển mạch gói (packet - switched network) - gồm tập hợp các nút chuyển mạch gói nối với nhau bởi các liên kết dữ liệu. Các gói dữ liệu được truyền từ một hệ thống mở tới một hệ thống mở khác trên mạng phải được chuyển qua một chuỗi các nút. Mỗi nút nhận gói dữ liệu từ một đường vào (incoming link) rồi chuyển tiếp nó tới một đường ra (outgoing link) hướng đến đích của dữ liệu. ả hư vậy ở mỗi nút trung gian nó phải thực hiện các chức năng chọn đường và chuyển tiếp.

Việc chọn đường là sự lựa chọn một con đường để truyền một đơn vị dữ liệu (một gói tin chẳng hạn) từ trạm nguồn tới trạm đích của nó. Một kỹ thuật chọn đường phải thực hiện hai chức năng chính sau đây:

- Quyết định chọn đường tối ưu dựa trên các thông tin đã có về mạng tại thời điểm đó thông qua những tiêu chuẩn tối ưu nhất định.

- Cập nhật các thông tin về mạng, tức là thông tin dùng cho việc chọn đường, trên mạng luôn có sự thay đổi thường xuyên nên việc cập nhật là việc cần thiết.



*Hình 4. 3: Mô hình chuyển vận các gói tin trong mạng chuyển mạch gói*

ả gười ta có hai phương thức đáp ứng cho việc chọn đường là phương thức xử lý tập trung và xử lý tại chỗ.

- *Phương thức chọn đường xử lý tập trung* được đặc trưng bởi sự tồn tại của một (hoặc vài) trung tâm điều khiển mạng, chúng thực hiện việc lập ra các bảng đường đi tại từng thời điểm cho các nút và sau đó gửi các bảng chọn đường tới từng nút dọc theo con đường đã được chọn đó. Thông tin tổng thể của mạng cần dùng cho việc chọn đường chỉ cần cập nhập và được cất giữ tại trung tâm điều khiển mạng.

- *Phương thức chọn đường xử lý tại chỗ* được đặc trưng bởi việc chọn đường được thực hiện tại mỗi nút của mạng. Trong từng thời điểm, mỗi nút phải duy trì các thông tin của mạng và tự xây dựng bảng chọn đường cho mình. ả hư vậy các thông tin tổng thể của mạng cần dùng cho việc chọn đường cần cập nhập và được cất giữ tại mỗi nút.

Thông thường các thông tin được đo lường và sử dụng cho việc chọn đường bao gồm:

- Trạng thái của đường truyền.
- Thời gian trễ khi truyền trên mỗi đường dẫn.
- Mức độ lưu thông trên mỗi đường.
- Các tài nguyên khả dụng của mạng.

Khi có sự thay đổi trên mạng (ví dụ thay đổi về cấu trúc của mạng do sự cố tại một vài nút, phục hồi của một nút mạng, nối thêm một nút mới... hoặc thay đổi về mức độ lưu thông) các thông tin trên cần được cập nhật vào các cơ sở dữ liệu về trạng thái của mạng.

Hiện nay khi nhu cầu truyền thông đa phương tiện (tích hợp dữ liệu văn bản, đồ hoạ, hình ảnh, âm thanh) ngày càng phát triển đòi hỏi các công nghệ truyền dẫn tốc độ cao nên việc phát triển các hệ thống chọn đường tốc độ cao đang rất được quan tâm.

### Tầng 4: Vận chuyển (Transport)

Tầng vận chuyển cung cấp các chức năng cần thiết giữa tầng mạng và các tầng trên. nó là tầng cao nhất có liên quan đến các giao thức trao đổi dữ liệu giữa các hệ thống mở. ả ó cùng các tầng dưới cung cấp cho người sử dụng các phục vụ vận chuyển.

Tầng vận chuyển (transport layer) là tầng cơ sở mà ở đó một máy tính của mạng chia sẻ thông tin với một máy khác. Tầng vận chuyển đồng nhất mỗi trạm bằng một địa chỉ duy nhất và quản lý sự kết nối giữa các trạm. Tầng vận chuyển cũng chia các gói tin lớn thành các gói tin nhỏ hơn trước khi gửi đi. Thông thường tầng vận chuyển đánh số các gói tin và đảm bảo chúng chuyển theo đúng thứ tự.

Tầng vận chuyển là tầng cuối cùng chịu trách nhiệm về mức độ an toàn trong truyền dữ liệu nên giao thức tầng vận chuyển phụ thuộc rất nhiều vào bản chất của tầng mạng. ả gười ta chia giao thức tầng mạng thành các loại sau:

- Mạng loại A: Có tỷ suất lỗi và sự cố có báo hiệu chấp nhận được (tức là chất lượng chấp nhận được). Các gói tin được giả thiết là không bị mất. Tầng vận chuyển không cần cung cấp các dịch vụ phục hồi hoặc sắp xếp thứ tự lại.

- Mạng loại B: Có tỷ suất lỗi chấp nhận được nhưng tỷ suất sự cố có báo hiệu lại không chấp nhận được. Tầng giao vận phải có khả năng phục hồi lại khi xẩy ra sự cố.

- Mạng loại C: Có tỷ suất lỗi không chấp nhận được (không tin cậy) hay là giao thức không liên kết. Tầng giao vận phải có khả năng phục hồi lại khi xảy ra lỗi và sắp xếp lại thứ tự các gói tin.

Trên cơ sở loại giao thức tầng mạng chúng ta có 5 lớp giao thức tầng vận chuyển đó là:

- *Giao thức lớp 0 (Simple Class - lớp đơn giản)*: cung cấp các khả năng rất đơn giản để thiết lập liên kết, truyền dữ liệu và hủy bỏ liên kết trên mạng "có liên kết" loại A. ả ó có khả năng phát hiện và báo hiệu các lỗi nhưng không có khả năng phục hồi.

- *Giao thức lớp 1 (Basic Error Recovery Class - Lớp phục hồi lỗi cơ bản)* dùng với các loại mạng B, ở đây các gói tin (TPDU) được đánh số. ả goài ra giao thức còn có khả năng báo nhận cho nơi gửi và truyền dữ liệu khẩn. So với giao thức lớp 0 giao thức lớp 1 có thêm khả năng phục hồi lỗi.

- *Giao thức lớp 2 (Multiplexing Class - lớp dồn kênh)* là một cải tiến của lớp 0 cho phép dồn một số liên kết chuyển vận vào một liên kết mạng duy nhất, đồng thời có thể kiểm soát luồng dữ liệu để tránh tắc nghẽn. Giao thức lớp 2 không có khả năng phát hiện và phục hồi lỗi. Do vậy nó cần đặt trên một tầng mạng loại A.

- *Giao thức lớp 3 (Error Recovery and Multiplexing Class - lớp phục hồi lỗi cơ bản và dồn kênh)* là sự mở rộng giao thức lớp 2 với khả năng phát hiện và phục hồi lỗi, nó cần đặt trên một tầng mạng loại B.

- *Giao thức lớp 4 (Error Detection and Recovery Class - Lớp phát hiện và phục hồi lỗi)* là lớp có hầu hết các chức năng của các lớp trước và còn bổ sung thêm một số khả năng khác để kiểm soát việc truyền dữ liệu.

### Tầng 5: Giao dịch (Session)

Tầng giao dịch (session layer) thiết lập "các giao dịch" giữa các trạm trên mạng, nó đặt tên nhất quán cho mọi thành phần muốn đối thoại với nhau và lập ánh xa giữa các tên với địa chỉ của chúng. Một giao dịch phải được thiết lập trước khi dữ liệu được truyền trên mạng, tầng giao dịch đảm bảo cho các giao dịch được thiết lập và duy trì theo đúng qui định.

Tầng giao dịch còn cung cấp cho người sử dụng các chức năng cần thiết để quản trị các giao dịnh ứng dụng của họ, cụ thể là:

- Điều phối việc trao đổi dữ liệu giữa các ứng dụng bằng cách thiết lập và giải phóng (một cách lôgic) các phiên (hay còn gọi là các hội thoại - dialogues)

- Cung cấp các điểm đồng bộ để kiểm soát việc trao đổi dữ liệu.
- Áp đặt các qui tắc cho các tương tác giữa các ứng dụng của người sử dụng.
- Cung cấp cơ chế "lấy lượt" (nắm quyền) trong quá trình trao đổi dữ liệu.

Trong trường hợp mạng là hai chiều luân phiên thì nẩy sinh vấn đề: hai người sử dụng luân phiên phải "lấy lượt" để truyền dữ liệu. Tầng giao dịch duy trì tương tác luân phiên bằng cách báo cho mỗi người sử dụng khi đến lượt họ được truyền dữ liệu. Vấn đề đồng bộ hóa trong tầng giao dịch cũng được thực hiện như cơ chế kiểm tra/phục hồi, dịch vụ này cho phép người sử dụng xác định các điểm đồng bộ hóa trong dòng dữ liệu đang chuyển vận và khi cần thiết có thể khôi phục việc hội thoại bắt đầu từ một trong các điểm đó

Ở một thời điểm chỉ có một người sử dụng đó quyền đặc biệt được gọi các dịch vụ nhất định của tầng giao dịch, việc phân bổ các quyền này thông qua trao đổi thẻ bài (token). Ví dụ: Ai có được token sẽ có quyền truyền dữ liệu, và khi người giữ token trao token cho người khác thi cũng có nghĩa trao quyền truyền dữ liệu cho người đó.

Tầng giao dịch có các hàm cơ bản sau:

- *Give Token* cho phép người sử dụng chuyển một token cho một người sử dụng khác của một liên kết giao dịch.
- *Please Token* cho phép một người sử dụng chưa có token có thể yêu cầu token đó.
- *Give Control* dùng để chuyển tất cả các token từ một người sử dụng sang một người sử dụng khác.

### Tầng 6: Trình bày (Presentation)

Trong giao tiếp giữa các ứng dụng thông qua mạng với cùng một dữ liệu có thể có nhiều cách biểu diễn khác nhau. Thông thường dạng biểu diễn dùng bởi ứng dụng nguồn và dạng biểu diễn dùng bởi ứng dụng đích có thể khác nhau do các ứng dụng được chạy trên các hệ thống hoàn toàn khác nhau (như hệ máy Intel và hệ máy Motorola). Tầng trình bày (Presentation layer) phải chịu trách nhiệm chuyển đổi dữ liệu gửi đi trên mạng từ một loại biểu diễn này sang một loại khác. Để đạt được điều đó nó cung cấp một dạng biểu diễn chung dùng để truyền thông và cho phép chuyển đổi từ dạng biểu diễn cục bộ sang biểu diễn chung và ngược lại.

Tầng trình bày cũng có thể được dùng kĩ thuật mã hóa để xáo trộn các dữ liệu trước khi được truyền đi và giải mã ở đầu đến để bảo mật. ả goài ra tầng biểu diễn cũng có thể dùng các kĩ thuật nén sao cho chỉ cần một ít byte dữ liệu để thể hiện thông tin khi nó được truyền ở trên mạng, ở đầu nhận, tầng trình bày bung trở lại để được dữ liệu ban đầu.

### Tầng 7: Ứng dụng (Application)

Tầng ứng dụng (Application layer) là tầng cao nhất của mô hình OSI, nó xác định giao diện giữa người sử dụng và môi trường OSI và giải quyết các kỹ thuật mà các chương trình ứng dụng dùng để giao tiếp với mạng.

Để cung cấp phương tiện truy nhập môi trường OSI cho các tiến trình ứng dụng, ả gười ta thiết lập các thực thể ứng dụng (AE), các thực thể ứng dụng sẽ gọi đến các phần tử dịch vụ ứng dụng (Application Service Element - viết tắt là ASE) của chúng. Mỗi thực thể ứng dụng có thể gồm một hoặc nhiều các phần tử dịch vụ ứng dụng. Các phần tử dịch vụ ứng dụng được phối hợp trong môi trường của thực thể ứng dụng thông qua các liên kết (association) gọi là đối tượng liên kết đơn (Single Association Object - viết tắt là SAO). SAO điều khiển việc truyền thông trong suốt vòng đời của liên kết đó cho phép tuần tự hóa các sự kiện đến từ các ASE thành tố của nó.

www.viet-ebook.co.cc

**Chương 5**

# Các đặc tính kỹ thuật của mạng cục bộ

Trên thực tế mạng cục bộ là một hệ thống truyền dữ liệu giữa các máy tính với một khoảng cách tương đối hẹp, điều đó cho phép có những lựa chọn đa dạng về thiết bị . Tuy nhiên những lựa chọn đa dạng này lại bị hạn chế bởi các đặc tính kỹ thuật của mạng cục bộ, đó làø tập hợp các quy tắc chuẩn đã được quy ước mà tất cả các thực thể tham gia truyền thông trên mạng phải tuân theo để đảm bảo cho mạng hoạt động tốt. Các đặc tính chính của mạng cục bộ mà chúng ta nói tới sau đây là:

- Cấu trúc của mạng (hay topology của mạng mà qua đó thể hiện cách nối các mạng máy tính với nhau ra sao).
- Các nghi thức truyền dữ liệu trên mạng (các thủ tục hướng dẫn trạm làm việc làm thế nào và lúc nào có thể thâm nhập vào đường dây cáp để gửi các gói thông tin ).
- Các loại đường truyền và các chuẩn của chúng .
- Các phương thức tín hiệu

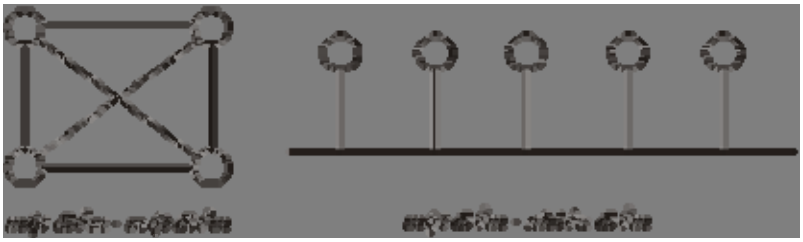
## I. Cấu trúc của mạng (Topology)

Hình trạng của mạng cục bộ thể hiện qua cấu trúc hay hình dáng hình học cuả các đường dây cáp mạng dùng để liên kết các máy tính thuộc mạng với nhau. Các mạng cục bộ thường hoạt động dựa trên cấu trúc đã định saün liên kết các máy tính và các thiết bị có liên quan.

Trước hết chúng ta xem xét hai phương thức nối mạng chủ yếu được sử dụng trong việc liên kết các máy tính là "một điểm - một điểm" và "một điểm - nhiều điểm ".

Với phương thức "một điểm - một điểm" các đường truyền riêng biệt được thiết lập để nối các cặp máy tính lại với nhau. Mỗi máy tính có thể truyền và nhận trực tiếp dữ liệu hoặc có thể làm trung gian như lưu trữ những dữ liệu mà nó nhận được rồi sau đó chuyển tiếp dữ liệu đi cho một máy khác để dữ liệu đó đạt tới đích.

Theo phương thức "một điểm - nhiều điểm " tất cả các trạm phân chia chung một đường truyền vật lý. Dữ liệu được gửi đi từ một máy tính sẽ có thể được tiếp nhận bởi tất cả các máy tính còn lại, bởi vậy cần chỉ ra địa chỉ đích của dữ liệu để mỗi máy tính căn cứ vào đó kiểm tra xem dữ liệu có phải dành cho mình không nếu đúng thì nhận còn nếu không thì bỏ qua.



*Hình 5.1: Các phương thức liên kết mạng*

Tùy theo cấu trúc của mỗi mạng chúng sẽ thuộc vào một trong hai phương thức nối mạng và mỗi phương thức nối mạng sẽ có những yêu cầu khác nhau về phần cứng và phần mềm.

## II. Những cấu trúc chính của mạng cục bộ

### 1. Dạng đường thẳng (Bus)

Trong dạng đường thẳng các máy tính đều được nối vào một đường dây truyền chính (bus). Đường truyền chính này được giới hạn hai đầu bởi một loại đầu nối đặc biệt gọi là *terminator* (dùng để nhận biết là đầu cuối để kết thúc đường truyền tại đây). Mỗi trạm được nối vào bus qua một đầu nối chữ T (T_connector) hoặc một bộ thu phát (transceiver). Khi một trạm truyền dữ liệu, tín hiệu được truyền trên cả hai chiều của đường truyền theo từng gói một, mỗi gói đều phải mang địa chỉ trạm đích. Các trạm khi thấy dữ liệu đi qua nhận lấy, kiểm tra, nếu đúng với địa chỉ của mình thì nó nhận lấy còn nếu không phải thì bỏ qua.

Sau đây là vài thông số kỹ thuật của topology bus. Theo chuẩn IEEE 802.3 (cho mạng cục bộ) với cách đặt tên qui ước theo thông số: tốc độ truyền tính hiệu (1,10 hoặc 100 Mb/s); BASE (nếu là Baseband) hoặc BROAD (nếu là Broadband).

- 10BASE5: Dùng cáp đồng trục đường kính lớn (10mm) với trở kháng 50 Ohm, tốc độ 10 Mb/s, phạm vi tín hiệu 500m/segment, có tối đa 100 trạm, khoảng cách giữa 2 tranceiver tối thiểu 2,5m (Phương án này còn gọi là Thick Ethernet hay Thicknet)

- 10BASE2: tương tự như Thicknet nhưng dùng cáp đồng trục nhỏ (RG 58A), có thể chạy với khoảng cách 185m, số trạm tối đa trong 1 segment là 30, khoảng cách giữa hai máy tối thiểu là 0,5m.

Dạng kết nối này có ưu điểm là ít tốn dây cáp, tốc độ truyền dữ liệu cao tuy nhiên nếu lưu lượng truyền tăng cao thì dễ gây ách tắc và nếu có trục trặc trên hành lang chính thì khó phát hiện ra.

Hiện nay các mạng sử dụng hình dạng đường thẳng là mạng Ethernet và G-net.

### 2. Dạng vòng tròn (Ring)

Các máy tính được liên kết với nhau thành một vòng tròn theo phương thức "một điểm - một điểm ", qua đó mỗi một trạm có thể nhận và truyền dữ liệu theo vòng một chiều và dữ liệu được truyền theo từng gói một. Mỗi gói dữ liệu đều có mang địa chỉ trạm đích, mỗi trạm khi nhận được một gói dữ liệu nó kiểm tra nếu đúng với địa chỉ của mình thì nó nhận lấy còn nếu không phải thì nó sẽ phát lại cho trạm kế tiếp, cứ như vậy gói dữ liệu đi được đến đích. Với dạng kết nối này có ưu điểm là không tốn nhiều dây cáp, tốc độ truyền dữ liệu cao, không gây ách tắc tuy nhiên các giao thức để truyền dữ liệu phức tạp và nếu có trục trặc trên một trạm thì cũng ảnh hưởng đến toàn mạng.

Hiện nay các mạng sử dụng hình dạng vòng tròn là mạng Tocken ring của IBM.

### 3. Dạng hình sao (Star)

Ở dạng hình sao, tất cả các trạm được nối vào một thiết bị trung tâm có nhiệm vụ nhận tín hiệu từ các trạm và chuyển tín hiệu đến trạm đích với phương thức kết nối là phương thức "một điểm - một điểm ". Thiết bị trung tâm hoạt động giống như một tổng đài cho phép thực hiện việc nhận và truyền dữ liệu từ trạm này tới các trạm khác. Tùy theo yêu cầu truyền thông trong mạng , thiết bị trung tâm có thể là một bộ chuyển mạch (switch), một bộ chọn đường (router) hoặc đơn giản là một bộ phân kênh (Hub). Có nhiều cổng ra và mỗi cổng nối với một máy. Theo chuẩn IEEE 802.3 mô hình dạng Star thường dùng:

- 10BASE-T: dùng cáp UTP, tốc độ 10 Mb/s, khoảng cách từ thiết bị trung tâm tới trạm tối đa là 100m.

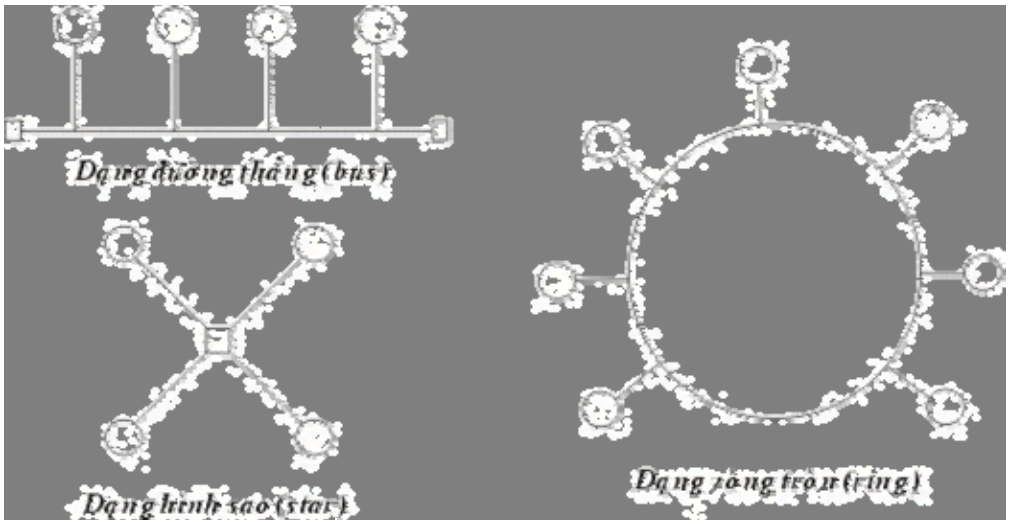
- 100BASE-T tương tự như 10BASE-T nhưng tốc độ cao hơn 100 Mb/s.

## *Ưu và khuyết điểm*

- *Ưu điểm:* Với dạng kết nối này có ưu điểm là không đụng độ hay ách tắc trên đường truyền, lắp đặt đơn giản, dễ dàng cấu hình lại (thêm, bớt trạm). ả ếu có trục trặc trên một trạm thì cũng không gây ảnh hưởng đến toàn mạng qua đó dễ dàng kiểm soát và khắc phục sự cố.

- *Nhược điểm:* Độ dài đường truyền nối một trạm với thiết bị trung tâm bị hạn chế (trong vòng 100 m với công nghệ hiện đại) tốn đường dây cáp nhiều, tốc độ truyền dữ liệu không cao.

Hiện nay các mạng sử dụng hình dạng hình sao là mạng STARLAả của AT&T và S-ả ET của ả ovell.




*Hình 5.2 : Các loại cấu trúc chính của mạng cục bộ.*

| | **Đường thẳng** | **Vòng Tròn** | **Hình sao** |
|---|---|---|---|
| Ứng dụng | Tốt cho trường hợp mạng nhỏ và mạng có giao thông thấp và | Tốt cho trường hợp mạng có số trạm ít hoạt động với tốc độ cao,không cách nhau xa lắm hoặc mạng có lưu lượng dữ | hiên nay mạng sao là cách tốt nhất cho trường hợp phải tích hợp dữ liệu và tín hiệutiếng.Các |

| | | | |
|---|---|---|---|
| | lưu lượng dữ liệu thấp | liệu phân bố không đều. | mạng đện thoại công cộng có cấu trúc này |
| Độ phức tạp | Tương đối không phức tạp | Đòi hỏi thiết bị tương đối phức tạp .Mặt khác việc đưa thông điệp đi trên tuyến là đơn giản, vì chỉ có 1 con đường, trạm phát chỉ cần biết địa chỉ của trạm nhận , các thông tin để dẫn đường khác thì không cần thiết | Mạng sao được xem là khá phức tạp . Các trạm được nối với thiết bị trung tâm và lần lượt hoạt động như thiết bị trung tâm hoặc nối được tới các dây dẫn truyền từ xa |
| Hiệu suất | Rất tốt dưới tải thấp có thể giảm hiệu suất rất mau khi tải tăng | Có hiệu quả trong trường hợp lượng lưu thông cao và khá ổn định nhờ sự tăng chậm thời gian trễ và sự xuống cấp so với các mạng khác | Tốt cho trường hợp tải vừa tuy nhiên kích thước và khả năng , suy ra hiệu suất của mạng phụ thuộc trực tiếp vào sức mạnh của thiết bị trung tâm. |
| Tổng phí | Tương đối thấp đặc biệt do nhiều thiết bị đã phát triển hòa chỉnh và bán sảm phẩm ở thị trường .Sự dư thừa kênh truyền được khuyến để giảm bớt nguy cơ xuất hiện sự cố trên mạng | Phải dự trù gấp đôi nguồn lực hoặc phải có 1 phương thức thay thế khi 1 nút không hoạt động nếu vẫn muốn mạng hoạt động bình thường | Tổng phí rất cao khi làm nhiêm vụ của thiết bị trung tâm, thiết bị trung tâm ï không được dùng vào việc khác .Số lượng dây riêng cũng nhiều. |
| ẩ guy cơ | Một trạm bị hỏng không ảnh hưởng đến cả mạng. Tuy nhiên mạng sẽ có nguy cơ bị tổn hại khi sự cố trên đường dây dẫn chính hoặc có vấn đề với tuyến. Vấn đề trên rất khó xác định được lại rất dễ sửa chữa | Mơt trạm bị hỏng có thể ảnh hưởng đến cả hệ thống vì các trạm phục thuộc vào nhau. Tìm 1 repeater hỏng rất khó ,vả lại việc sửa chữa thẳng hay dùng mưu mẹo xác định điểm hỏng trên mạng có địa bàn rôăng rất khó | Độ tin cậy của hệ thống phụ thuộc vào thiết bị trung tâm, .nếu bị hỏng thì mạng ngưng hoạt động Sự ngưng hoạt động tại thiết bị trung tâm thường không ảnh hươdng đến toàn bộ hệ thống . |
| Khả năng mở rộng | Việc thêm và định hình lại mạng này rất dễ.Tuy nhiên việc kết nối giữa các máy tính và thiết bị của các hãng khác nhau khó có thể vì chúng phải có thể nhận cùng | Tương đối dễ thêm và bớt các trạm làm việc mà không phải nối kết nhiều cho mỗi thay đổi Giá thành cho việc thay đổi tương đối thấp | Khả năng mở rộâng hạn chế, đa số các thiết bị trung tâm chỉ chịu đựng nối 1 số nhất định liên kết. Sự hạn chế về tốc độ truyền dữ liệu và băng tần thường được đòi hỏi ở mỗi người sử dụng. Các hạn chế này giúp cho các chức năng xử lý trung tâm không |

| | | | |
|---|---|---|---|
| | địa chỉ và dữ liệu | | bị quá tải bởi tốc độ thu nạp tại tại cổng truyền và giá thành mỗi cổng truyền của thiết bị trung tâm thấp . |

*Hình 6.4 : Bảng so sánh tính năng giữa các cấu trúc của mạng LAN*

## III. Phương thức truyền tín hiệu

Thông thường có hai phương thức truyền tín hiệu trong mạng cục bộ là dùng băng tần cơ sở (baseband) và băng tần rộng (broadband). Sự khác nhau chủ yếu giữa hai phương thức truyền tín hiệu này là băng tầng cơ sở chỉ chấp nhận một kênh dữ liệu duy nhất trong khi băng rộng có thể chấp nhận đồng thời hai hoặc nhiều kênh truyền thông cùng phân chia giải thông của đường truyền.

Hầu hết các mạng cục bộ sử dụng phương thức băng tần cơ sở. Với phương thức truyền tín hiệu này này tín hiệu có thể được truyền đi dưới cả hai dạng: tương tự (analog) hoặc số (digital). Phương thức truyền băng tần rộng chia giải thông (tần số) của đường truyền thành nhiều giải tần con trong đó mỗi dải tần con đó cung cấp một kênh truyền dữ liệu tách biệt nhờ sử dụng một cặp modem đặc biệt gọi là bộ giải / Điều biến RF cai quản việc biến đổi các tín hiệu số thành tín hiệu tương tự có tần số vô tuyến (RF) bằng kỹ thuật ghép kênh.

## IV. Các giao thức truy cập đường truyền trên mạng LAN

Để truyền được dữ liệu trên mạng người ta phải có các thủ tục nhằm hướng dẫn các máy tính của mạng làm thế nào và lúc nào có thể thâm nhập vào đường dây cáp để gửi các gói dữ kiện. Ví dụ như đối với các dạng bus và ring thì chỉ có một đường truyền duy nhất nối các trạm với nhau, cho nên cần phải có các quy tắc chung cho tất cả các trạm nối vào mạng để đảm bảo rằng đường truyền được truy nhập và sử dụng một cách hợp lý.

Có nhiều giao thức khác nhau để truy nhập đường truyền vật lý nhưng phân thành hai loại: các giao thức truy nhập ngẫu nhiên và các giao thức truy nhập có điều khiển.

### 1. Giao thức chuyển mạch (yêu cầu và chấp nhận)

Giao thức chuyển mạch là loại giao thức hoạt động theo cách thức sau: một máy tính của mạng khi cần có thể phát tín hiệu thâm nhập vào mạng, nếu vào lúc này đường cáp không bận thì mạch điều khiển sẽ cho trạm này thâm nhập vào đường cáp còn nếu đường cáp đang bận, nghĩa là đang có giao lưu giữa các trạm khác, thì việc thâm nhập sẽ bị từ chối.

### 2. Giao thức đường dây đa truy cập với cảm nhận va chạm (Carrier Sense Multiple Access with Collision Detection hay CSMA/CD )

Giao thức đường dây đa truy cập cho phép nhiều trạm thâm nhập cùng một lúc vào mạng, giao thức này thường dùng trong sơ đồ mạng dạng đường thẳng. Mọi trạm đều có thể được truy nhập vào đường dây chung một cách ngẫu nhiên và do vậy có thể dẫn đến xung đột (hai hoặc nhiều trạm đồng thời cùng truyền dữ liệu). Các trạm phải kiểm tra đường truyền gói dữ liệu đi qua có phải của nó hay không. Khi một trạm muốn truyền dữ liệu nó phải

kiểm tra đường truyền xem có rảnh hay không để gửi gói dữ liệu của, nếu đường truyền đang bận trạm phải chờ đợi chỉ được truyền khi thấy đường truyền rảnh. ả ếu cùng một lúc có hai trạm cùng sử dụng đường truyền thì giao thức phải phát hiện điều này và các trạm phải ngưng thâm nhập, chờ đợi lần sau các thời gian ngẫu nhiên khác nhau.

Khi đường cáp đang bận trạm phải chờ đợi theo một trong ba phương thức sau:

- Trạm tạm chờ đợi một thời gian ngẫu nhiên nào đó rồi lại bắt đầu kiểm tra đường truyền.
- Trạm tiếp tục kiểm tra đường truyền đến khi đường truyền rảnh thì truyền dữ liệu đi.
- Trạm tiếp tục kiểm tra đường truyềnđến khi đường truyền rảnh thì truyền dữ liệu đi với xác suất p xác định trước ($0 < p < 1$).

Tại đây phương thức 1 có hiệu quả trong việc tránh xung đột vì hai trạm cần truyền khi thấy đường truyền bận sẽ cùng rút lui và chờ đợi trong các thời gian ngẫu nhiên khác nhau. ả gược lại phương thức 2 cố gắng giảm thời gian trống của đường truyền bằng các cho phép trạm có thể truyền ngay sau khi một cuộc truyền kết thúc song nếu lúc đó có thêm một trạm khác đang đợi thì khả năng xảy ra xung đột là rất cao. Phương thức 3 với giá trị p phải lựa chọn hợp lý có thể tối thiểu hóa được khả năng xung đột lẫn thời gian trống của đường truyền.

Khi lưu lượng các gói dữ liệu cần di chuyển trên mạng quá cao, thì việc đụng độ có thể xảy ra với sồ lượng lớn có gây tắc nghẽn đường truyền dẫn đến làm chậm tốc độ truyền tin của hệ thống.

### 3. Giao thức dùng thẻ bài vòng (Token ring)

Đây là giao thức truy nhập có điều khiển chủ yếu dùng kỹ thuật chuyển thẻ bài (token) để cấp phát quyền truy nhập đường truyền tức là quyền được truyền dữ liệu đi. Thẻ bài ở đay là một đơn vị dữ liệu đặc biệt, có kích thuóc và nội dung (gồm các thông tin điều khiển) được quy định riêng cho mỗi giao thức. Theo giao thức dùng thẻ bài vòng trong đường cáp liên tục có một thẻ bài chạy quanh trong mạng Thẻ bài là một đơn vị dữ liệu đặc biệt trong đó có một bit biểu diễn trạng thái sử dụng của nó (bận hoặc rỗi). Một trạm muốn truyền dữ liệu thì phải đợi đến khi nhận được một thẻ bài rảnh. Khi đó trạm sẽ đổi bit trạng thái của thẻ bài thành bận, nép gói dữ liệu có kèm theo địa chỉ nơi nhận vào thẻ bài và truyền đi theo chiều của vòng.

Vì thẻ bài chạy vòng quang trong mạng kín và chỉ có một thẻ nên việc đụng độ dữ liệu không thể xảy ra, do vậy hiệu suất truyền dữ liệu của mạng không thay đổi.

Trong các giao thức này cần giải quyết hai vấn đề có thể dẫn đến phá vỡ hệ thống. Một là việc mất thẻ bài làm cho trên vòng không còn thẻ bài lưu chuyển nữa. Hai là một thẻ bài bận lưu chuyển không dừng trên vòng.

### 4. Giao thức dung thẻ bài cho dạng đường thẳng (Token bus)

Đây là giao thức truy nhập có điều khiển trong để cấp phát quyền truy nhập đường truyền cho các trạm đang có nhu cầu truyền dữ liệu, một thẻ bài được lưu chuyển trên một vòng logic thiết lập bởi các trạm đó. Khi một trạm có thẻ bài thì nó có quyền sử dụng đường truyền trong một thời gian xác định trước. Khi đã hết dữ liệu hoặc hết thời đoạn cho phép, trạm chuyển thẻ bài đến trạm tiếp theo trong vòng logic.

ả hư vậy trong mạng phải thiết lập được vòng logic (hay còn gọi là vòng ảo) bao gồm các trạm đang hoạt động nối trong mạng được xác định vị trí theo một chuỗi thứ tự mà trạm cuối cùng của chuỗi sẽ tiếp liền sau bởi trạm đầu tiên. Mỗi trạm được biết địa chỉ của các trạm kề trước và sau nó trong đó thứ tự của các trạm trên vòng logic có thể độc lập với thứ tự vật lý. Cùng với việc thiết lập vòng thì giao thức phải luôn luôn theo dõi sự thay đổi theo trạng thái thực tế của mạng.

## V. Đường cáp truyền mạng

Đường cáp truyền mạng là cơ sở hạ tầng của một hệ thống mạng, nên nó rất quan trọng và ảnh hưởng rất nhiều đến khả năng hoạt động của mạng. Hiện nay người ta thường dùng 3 loại dây cáp là cáp xoắn cặp, cáp đồng trục và cáp quang.

### 1. Cáp xoắn cặp

Đây là loại cáp gồm hai đường dây dẫn đồng được xoắn vào nhau nhằm làm giảm nhiễu điện từ gây ra bởi môi trường xung quanh và giữa chúng với nhau.

Hiện nay có hai loại cáp xoắn là cáp có bọc kim loại ( STP - Shield Twisted Pair) và cáp không bọc kim loại (UTP -Unshield Twisted Pair).

- Cáp có bọc kim loại (STP): Lớp bọc bên ngoài có tác dụng chống nhiễu điện từ, có loại có một đôi giây xoắn vào nhau và có loại có nhiều đôi giây xoắn với nhau.

- Cáp không bọc kim loại (UTP): Tính tương tự như STP nhưng kém hơn về khả năng chống nhiễu và suy hao vì không có vỏ bọc.

STP và UTP có các loại (Category - Cat) thường dùng:

- Loại 1 & 2 (Cat 1 & Cat 2): Thường dùng cho truyền thoại và những đường truyền tốc độ thấp (nhỏ hơn 4Mb/s).

- Loại 3 (Cat 3): tốc độ truyền dữ liệu khoảng 16 Mb/s , nó là chuẩn cho hầu hết các mạng điện thoại.

- Loại 4 (Cat 4): Thích hợp cho đường truyền 20Mb/s.

- Loại 5 (Cat 5): Thích hợp cho đường truyền 100Mb/s.

- Loại 6 (Cat 6): Thích hợp cho đường truyền 300Mb/s.

Đây là loại cáp rẻ, dễ cài đặt tuy nhiên nó dễ bị ảnh hưởng của môi trường.

### 2. Cáp đồng trục

Cáp đồng trục có hai đường dây dẫn và chúng có cùng một trục chung, một dây dẫn trung tâm (thường là dây đồng cứng) đường dây còn lại tạo thành đường ống bao xung quanh dây dẫn trung tâm (dây dẫn này có thể là dây bện kim loại và vì nó có chức năng chống nhiễu nên còn gọi là lớp bọc kim). Giữa hai dây dẫn trên có một lớp cách ly, và bên ngoài cùng là lớp vỏ plastic để bảo vệ cáp.

| *Các loại cáp* | *Dây xoắn cặp* | *Cáp đồng trục mỏng* | *Cáp đồng trục dày* | *Cáp quang* |
|---|---|---|---|---|
| *Chi tiết* | Bằng đồng, có 4 và 25 cặp dây (loại 3, 4, 5) | Bằng đồng, 2 dây, đường kính 5mm | Bằng đồng, 2 dây, đường kính 10mm | Thủy tinh, 2 sợi |
| *Loại kết nối* | RJ-25 hoặc 50-pin telco | Bả C | ả -series | ST |
| *Chiều dài đoạn tối đa* | 100m | 185m | 500m | 1000m |
| *Số đầu nối tối đa trên 1 đoạn* | 2 | 30 | 100 | 2 |
| *Chạy 10 Mbit/s* | Được | Được | Được | Được |
| *Chạy 100 Mbit/s* | Được | Không | Không | Được |
| *Chống nhiễu* | Tốt | Tốt | Rất tốt | Hoàn toàn |
| *Bảo mật* | Trung bình | Trung bình | Trung bình | Hoàn toàn |
| *Độ tin cậy* | Tốt | Trung bình | Tốt | Tốt |
| *Lắp đặt* | Dễ dàng | Trung bình | Khó | Khó |
| *Khắc phục lỗi* | Tốt | Dở | Dở | Tốt |
| *Quản lý* | Dễ dàng | Khó | Khó | Trung bình |
| *Chi phí cho 1 trạm* | Rất thấp | Thấp | Trung bình | Cao |
| *Ứng dụng tốt nhất* | Hệ thống Workgroup | Đường backbone | Đường backbone trong tủ mạng | Đường backbone dài trong tủ mạng hoặc các tòa nhà |

*Hình 5.3: Tính năng kỹ thuật của một số loại cáp mạng*

Cáp đồng trục có độ suy hao ít hơn so với các loại cáp đồng khác (ví dụ như cáp xoắn đôi) do ít bị ảnh hưởng của môi trường. Các mạng cục bộ sử dụng cáp đồng trục có thể có kích thước trong phạm vi vài ngàn mét, cáp đồng trục được sử dụng nhiều trong các mạng dạng đường thẳng. Hai loại cáp thường được sử dụng là cáp đồng trục mỏng và cáp đồng trục dày trong đường kính cáp đồng trục mỏng là 0,25 inch, cáp đồng trục dày là 0,5 inch. Cả hai loại cáp đều làm việc ở cùng tốc độ nhưng cáp đồng trục mỏng có độ hao suy tín hiệu lớn hơn

Hiện nay có cáp đồng trục sau:

- RG -58,50 ohm: dùng cho mạng Thin Ethernet
- RG -59,75 ohm: dùng cho truyền hình cáp
- RG -62,93 ohm: dùng cho mạng ARCnet

Các mạng cục bộ thường sử dụng cáp đồng trục có dải thông từ 2,5 - 10 Mb/s, cáp đồng trục có độ suy hao ít hơn so với các loại cáp đồng khác vì nó có lớp vỏ bọc bên ngoài, độ dài thông thường của một đoạn cáp nối trong mạng là 200m, thường sử dụng cho dạng Bus.

### 3. Cáp sợi quang (Fiber - Optic Cable)

Cáp sợi quang bao gồm một dây dẫn trung tâm (là một hoặc một bó sợi thủy tinh có thể truyền dẫn tín hiệu quang) được bọc một lớp vỏ bọc có tác dụng phản xạ các tín hiệu trở lại để giảm sự mất mát tín hiệu. Bên ngoài cùng là lớp vỏ plastic để bảo vệ cáp. ẩ hư vậy cáp sợi quang không truyền dẫn các tín hiệu điện mà chỉ truyền các tín hiệu quang (các tín hiệu dữ liệu phải được chuyển đổi thành các tín hiệu quang và khi nhận chúng sẽ lại được chuyển đổi trở lại thành tín hiệu điện).

Cáp quang có đường kính từ 8.3 - 100 micron, Do đường kính lõi sợi thuỷ tinh có kích thước rất nhỏ nên rất khó khăn cho việc đấu nối, nó cần công nghệ đặc biệt với kỹ thuật cao đòi hỏi chi phí cao.

Dải thông của cáp quang có thể lên tới hàng Gbps và cho phép khoảng cách đi cáp khá xa do độ suy hao tín hiệu trên cáp rất thấp. ẩ goài ra, vì cáp sợi quang không dùng tín hiệu điện từ để truyền dữ liệu nên nó hoàn toàn không bị ảnh hưởng của nhiễu điện từ và tín hiệu truyền không thể bị phát hiện và thu trộm bởi các thiết bị điện tử của người khác.

Chỉ trừ nhược điểm khó lắp đặt và giá thành còn cao , nhìn chung cáp quang thích hợp cho mọi mạng hiện nay và sau này.

### 4. Các yêu cầu cho một hệ thống cáp

- An toàn, thẩm mỹ: tất cả các dây mạng phải được bao bọc cẩn thận, cách xa các nguồn điện, các máy có khả năng phát sóng để tránh trường hợp bị nhiễu. Các đầu nối phải đảm bảo chất lượng, tránh tình trạng hệ thống mạng bị chập chờn.

- Đúng chuẩn: hệ thống cáp phải thực hiện đúng chuẩn, đảm bảo cho khả năng nâng cấp sau này cũng như dễ dàng cho việc kết nối các thiết bị khác nhau của các nhà sản xuất khác nhau. Tiêu chuẩn quốc tế dùng cho các hệ thống mạng hiện nay là EIA/TIA 568B.

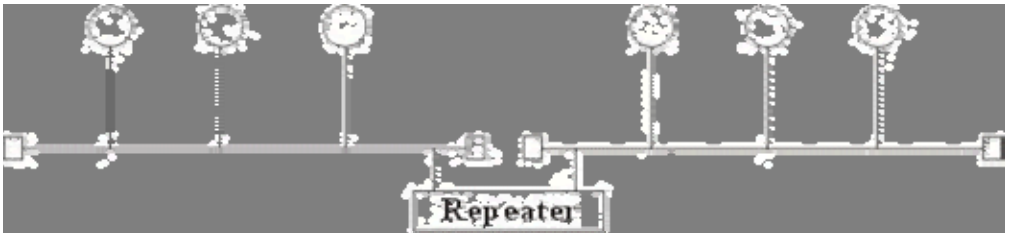
- Tiết kiệm và "linh hoạt" (flexible): hệ thống cáp phải được thiết kế sao cho kinh tế nhất, dễ dàng trong việc di chuyển các trạm làm việc và có khả năng mở rộng sau này.

**Chương 6**

# Các thiết bị liên kết mạng

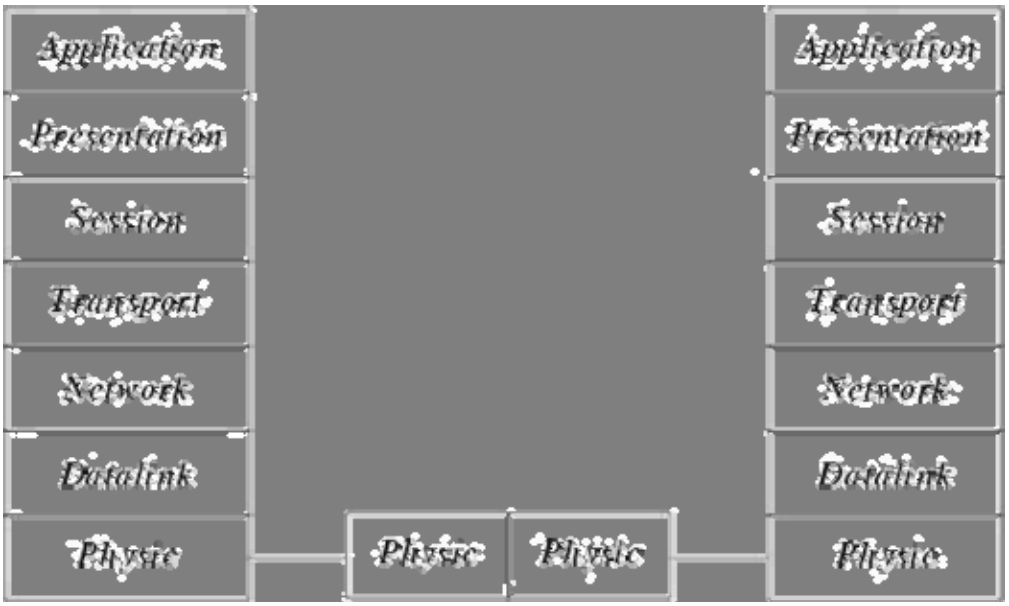
## I. Repeater (Bộ tiếp sức)

Repeater là loại thiết bị phần cứng đơn giản nhất trong các thiết bị liên kết mạng, nó được hoạt động trong tầng vật lý của mô hình hệ thống mở OSI. Repeater dùng để nối 2 mạng giống nhau hoặc các phần một mạng cùng có một nghi thức và một cấu hình. Khi Repeater nhận được một tín hiệu từ một phía của mạng thì nó sẽ phát tiếp vào phía kia của mạng.




*Hình 6.1: Mô hình liên kết mạng của Repeater.*

Repeater không có xử lý tín hiệu mà nó chỉ loại bỏ các tín hiệu méo, nhiễu, khuếch đại tín hiệu đã bị suy hao (vì đã được phát với khoảng cách xa) và khôi phục lại tín hiệu ban đầu. Việc sử dụng Repeater đã làm tăng thêm chiều dài của mạng.




*Hình 6.2: Hoạt động của bộ tiếp sức trong mô hình OSI*

Hiện nay có hai loại Repeater đang được sử dụng là Repeater điện và Repeater điện quang.

- ***Repeater điện*** nối với đường dây điện ở cả hai phía của nó, nó nhận tín hiệu điện từ một phía và phát lại về phía kia. Khi một mạng sử dụng Repeater điện để nối các phần của mạng lại thì có thể làm tăng khoảng cách của mạng, nhưng khoảng cách đó luôn bị hạn chế bởi một khoảng cách tối đa do độ trễ của tín hiệu. Ví dụ với

mạng sử dụng cáp đồng trục 50 thì khoảng cách tối đa là 2.8 km, khoảng cách đó không thể kéo thêm cho dù sử dụng thêm Repeater.

- ***Repeater điện quang*** liên kết với một đầu cáp quang và một đầu là cáp điện, nó chuyển một tín hiệu điện từ cáp điện ra tín hiệu quang để phát trên cáp quang và ngược lại. Việc sử dụng Repeater điện quang cũng làm tăng thêm chiều dài của mạng.

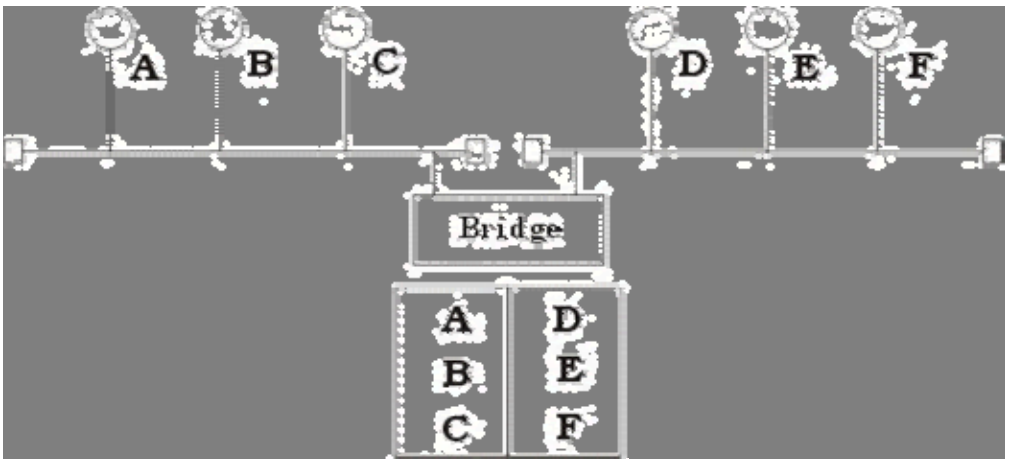
Việc sử dụng Repeater không thay đổi nội dung các tín hiện đi qua nên nó chỉ được dùng để nối hai mạng có cùng giao thức truyền thông (như hai mạng Ethernet hay hai mạng Token ring) nhưng không thể nối hai mạng có giao thức truyền thông khác nhau (như một mạng Ethernet và một mạng Token ring). Thêm nữa Repeater không làm thay đổi khối lượng chuyển vận trên mạng nên việc sử dụng không tính toán nó trên mạng lớn sẽ hạn chế hiệu năng của mạng. Khi lựa chọn sử dụng Repeater cần chú ý lựa chọn loại có tốc độ chuyển vận phù hợp với tốc độ của mạng.

## II. Bridge (Cầu nối)

Bridge là một thiết bị có xử lý dùng để nối hai mạng giống nhau hoặc khác nhau, nó có thể được dùng với các mạng có các giao thức khác nhau. Cầu nối hoạt động trên tầng liên kết dữ liệu nên không như bộ tiếp sức phải phát lại tất cả những gì nó nhận được thì cầu nối đọc được các gói tin của tầng liên kết dữ liệu trong mô hình OSI và xử lý chúng trước khi quyết định có chuyển đi hay không.

Khi nhận được các gói tin Bridge chọn lọc và chỉ chuyển những gói tin mà nó thấy cần thiết. Điều này làm cho Bridge trở nên có ích khi nối một vài mạng với nhau và cho phép nó hoạt động một cách mềm dẻo.

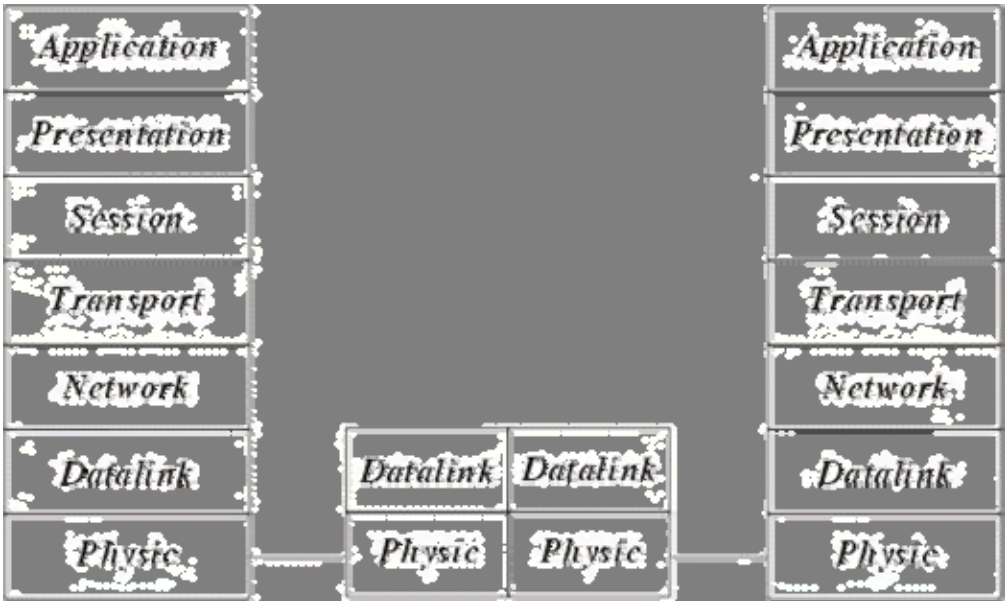
Để thực hiện được điều này trong Bridge ở mỗi đầu kết nối có một bảng các địa chỉ các trạm được kết nối vào phía đó, khi hoạt động cầu nối xem xét mỗi gói tin nó nhận được bằng cách đọc địa chỉ của nơi gửi và nhận và dựa trên bảng địa chỉ phía nhận được gói tin nó quyết định gửi gói tin hay không và bổ xung bảng địa chỉ.




*Hình 6.3: Hoạt động của Bridge*

Khi đọc địa chỉ nơi gửi Bridge kiểm tra xem trong bảng địa chỉ của phần mạng nhận được gói tin có địa chỉ đó hay không, nếu không có thì Bridge tự động bổ xung bảng địa chỉ (cơ chế đó được gọi là tự học của cầu nối).

Khi đọc địa chỉ nơi nhận Bridge kiểm tra xem trong bảng địa chỉ của phần mạng nhận được gói tin có địa chỉ đó hay không, nếu có thì Bridge sẽ cho rằng đó là gói tin nội bộ thuộc phần mạng mà gói tin đến nên không chuyển gói tin đó đi, nếu ngược lại thì Bridge mới chuyển sang phía bên kia. Ở đây chúng ta thấy một trạm không cần thiết chuyển thông tin trên toàn mạng mà chỉ trên phần mạng có trạm nhận mà thôi.




*Hình 6.4: Hoạt động của Bridge trong mô hình OSI*

Để đánh giá một Bridge người ta đưa ra hai khái niệm : Lọc và chuyển vận. Quá trình xử lý mỗi gói tin được gọi là quá trình lọc trong đó tốc độ lọc thể hiện trực tiếp khả năng hoạt động của Bridge. Tốc độ chuyển vận được thể hiện số gói tin/giây trong đó thể hiện khả năng của Bridge chuyển các gói tin từ mạng này sang mạng khác.

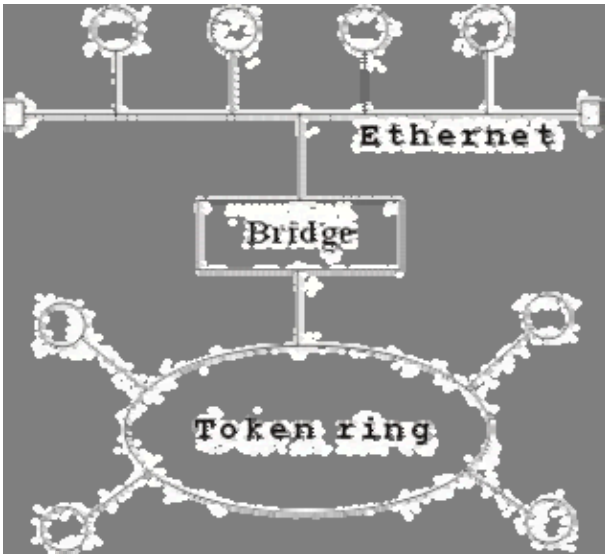
Hiện nay có hai loại Bridge đang được sử dụng là Bridge vận chuyển và Bridge biên dịch. Bridge *vận chuyển* dùng để nối hai mạng cục bộ cùng sử dụng một giao thức truyền thông của tầng liên kết dữ liệu, tuy nhiên mỗi mạng có thể sử dụng loại dây nối khác nhau. Bridge vận chuyển không có khả năng thay đổi cấu trúc các gói tin mà nó nhận được mà chỉ quan tâm tới việc xem xét và chuyển vận gói tin đó đi.

Bridge biên dịch dùng để nối hai mạng cục bộ có giao thức khác nhau nó có khả năng chuyển một gói tin thuộc mạng này sang gói tin thuộc mạng kia trước khi chuyển qua

***Ví dụ :*** Bridge biên dịch nối một mạng Ethernet và một mạng Token ring. Khi đó Cầu nối thực hiện như một nút token ring trên mạng Token ring và một nút Enthernet trên mạng Ethernet. Cầu nối có thể chuyển một gói tin theo chuẩn đang sử dụng trên mạng Enthernet sang chuẩn đang sử dụng trên mạng Token ring.

Tuy nhiên chú ý ở đây cầu nối không thể chia một gói tin ra làm nhiều gói tin cho nên phải hạn chế kích thước tối đa các gói tin phù hợp với cả hai mạng. Ví dụ như kích thước tối đa

của gói tin trên mạng Ethernet là 1500 bytes và trên mạng Token ring là 6000 bytes do vậy nếu một trạm trên mạng token ring gửi một gói tin cho trạm trên mạng Ethernet với kích thước lớn hơn 1500 bytes thì khi qua cầu nối số lượng byte dư sẽ bị chặt bỏ.




*Hình 6.5: Ví dụ về Bridge biên dịch*

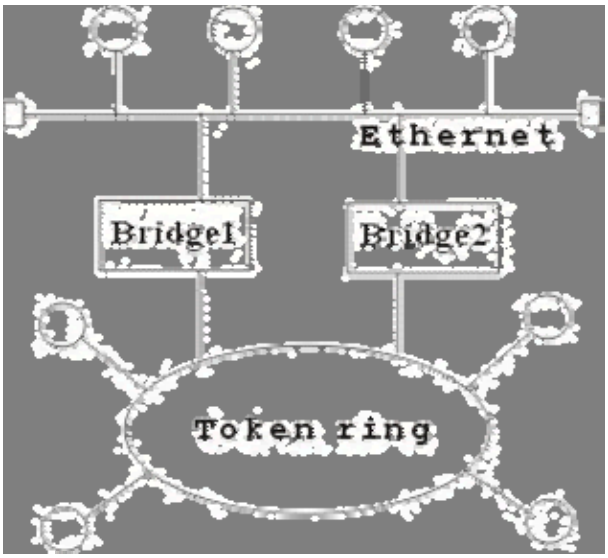
ầ gười ta sử dụng Bridge trong các trường hợp sau :

- Mở rộng mạng hiện tại khi đã đạt tới khoảng cách tối đa do Bridge sau khi sử lý gói tin đã phát lại gói tin trên phần mạng còn lại nên tín hiệu tốt hơn bộ tiếp sức.

- Giảm bớt tắc nghẽn mạng khi có quá nhiều trạm bằng cách sử dụng Bridge, khi đó chúng ta chia mạng ra thành nhiều phần bằng các Bridge, các gói tin trong nội bộ tùng phần mạng sẽ không được phép qua phần mạng khác.

- Để nối các mạng có giao thức khác nhau.

Một vài Bridge còn có khả năng lựa chọn đối tượng vận chuyển. ầ ó có thể chỉ chuyển vận những gói tin của nhưng địa chỉ xác định. Ví dụ : cho phép gói tin của máy A, B qua Bridge 1, gói tin của máy C, D qua Bridge 2.

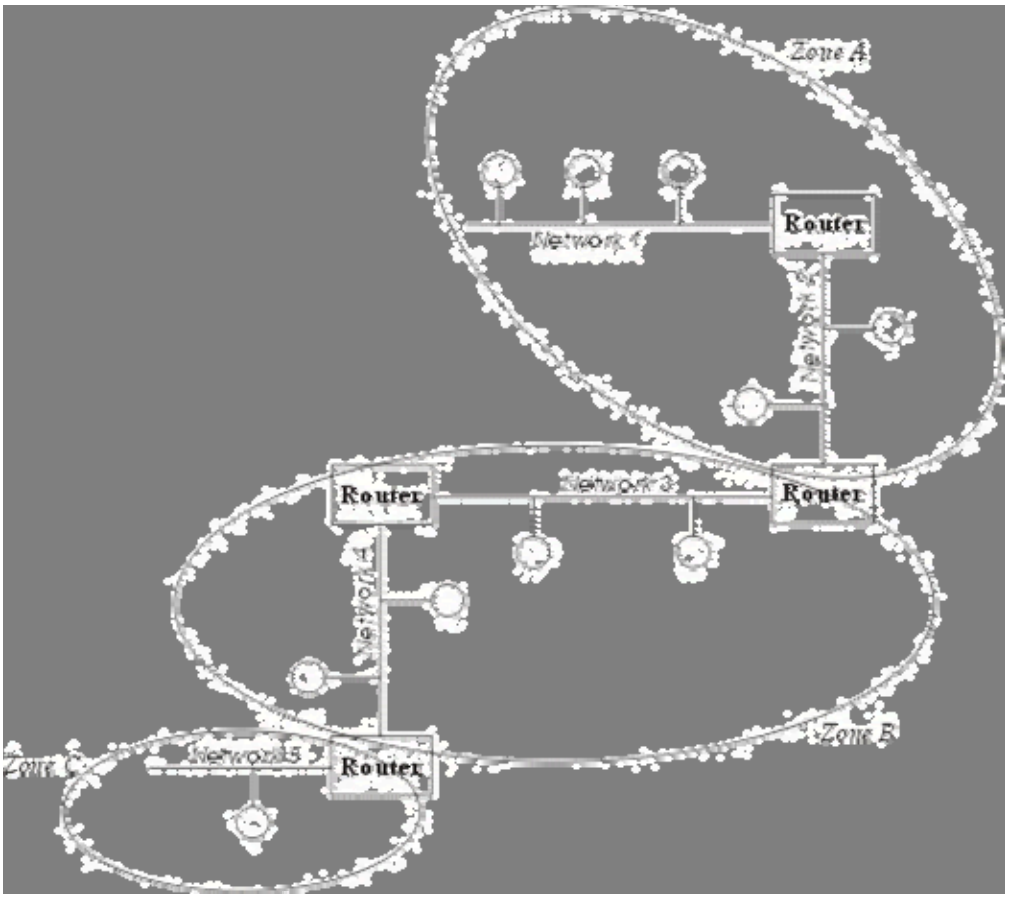



*Hình 6.6 : Liên kết mạng với 2 Bridge*

Một số Bridge được chế tạo thành một bộ riêng biệt, chỉ cần nối dây và bật. Các Bridge khác chế tạo như card chuyên dùng cắïm vào máy tính, khi đó trên máy tính sẽ sử dụng phần mềm Bridge. Việc kết hợp phần mềm với phần cứng cho phép uyển chuyển hơn trong hoạt động của Bridge.

**III. Router (Bộ tìm đường)**

Router là một thiết bị hoạt động trên tầng mạng, nó có thể tìm được đường đi tốt nhất cho các gói tin qua nhiều kết nối để đi từ trạm gửi thuộc mạng đầu đến trạm nhận thuộc mạng cuối. Router có thể được sử dụng trong việc nối nhiều mạng với nhau và cho phép các gói tin có thể đi theo nhiều đường khác nhau để tới đích.




*Hình 6.7: Hoạt động của Router.*

Khác với Bridge hoạt động trên tầng liên kết dữ liệu nên Bridge phải xử lý mọi gói tin trên đường truyền thì Router có địa chỉ riêng biệt và nó chỉ tiếp nhận và xử lý các gói tin gửi đến nó mà thôi. Khi một trạm muốn gửi gói tin qua Router thì nó phải gửi gói tin với địa chỉ trực tiếp của Router (Trong gói tin đó phải chứa các thông tin khác về đích đến) và khi gói tin đến Router thì Router mới xử lý và gửi tiếp.

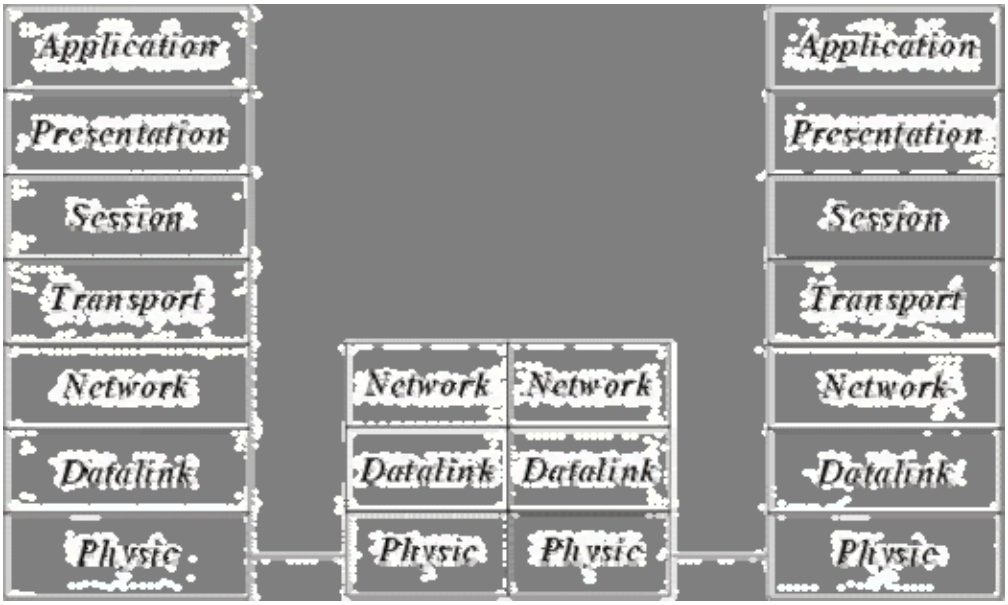
Khi xử lý một gói tin Router phải tìm được đường đi của gói tin qua mạng. Để làm được điều đó Router phải tìm được đường đi tốt nhất trong mạng dựa trên các thông tin nó có về mạng, thông thường trên mỗi Router có một bảng chỉ đường (Router table). Dựa trên dữ liệu về Router gần đó và các mạng trong liên mạng, Router tính được bảng chỉ đường (Router table) tối ưu dựa trên một thuật toán xác định trước.

ả gười ta phân chia Router thành hai loại là Router có phụ thuộc giao thức (The protocol dependent routers) và Router không phụ thuộc vào giao thức (The protocol independent router) dựa vào phương thức xử lý các gói tin khi qua Router.

- *Router có phụ thuộc giao thức:* Chỉ thực hiện việc tìm đường và truyền gói tin từ mạng này sang mạng khác chứ không chuyển đổi phương cách đóng gói của gói tin cho nên cả hai mạng phải dùng chung một giao thức truyền thông.

- *Router không phụ thuộc vào giao thức*: có thể liên kết các mạng dùng giao thức truyền thông khác nhau và có thể chuyển đôiø gói tin của giao thức này sang gói tin

của giao thức kia, Router cũng ù chấp nhận kích thước các gói tin khác nhau (Router có thể chia nhỏ một gói tin lớn thành nhiều gói tin nhỏ trước truyền trên mạng).




*Hình 6.8: Hoạt động của Router trong mô hình OSI*

Để ngăn chặn việc mất mát số liệu Router còn nhận biết được đường nào có thể chuyển vận và ngừng chuyển vận khi đường bị tắc.

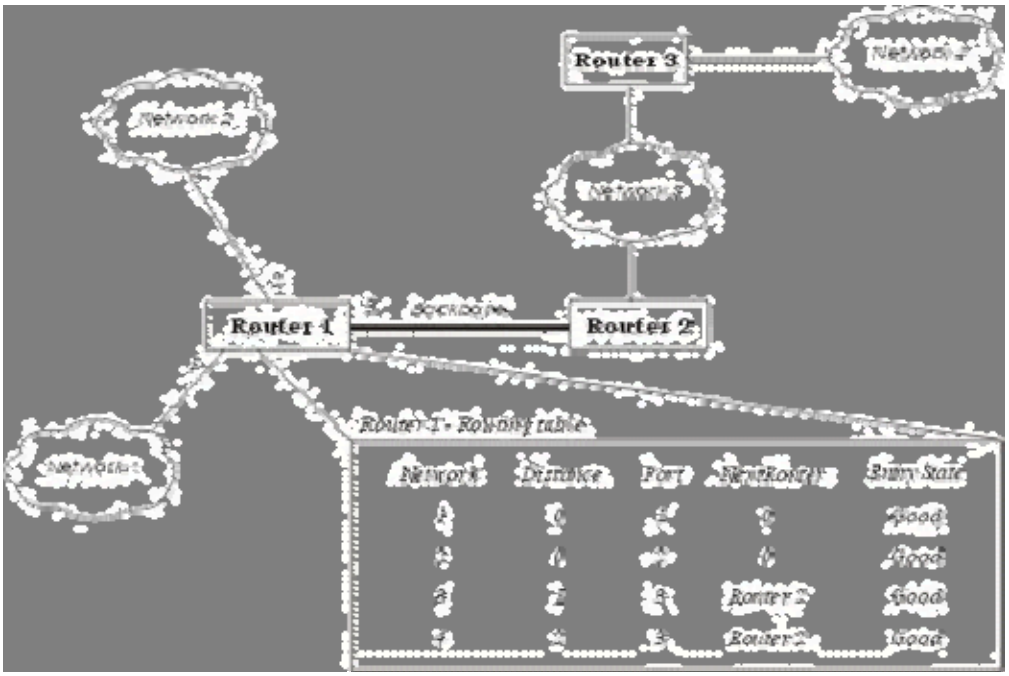
Các lý do sử dụng Router :

- Router có các phần mềm lọc ưu việt hơn là Bridge do các gói tin muốn đi qua Router cần phải gửi trực tiếp đến nó nên giảm được số lượng gói tin qua nó. Router thường được sử dụng trong khi nối các mạng thông qua các đường dây thuê bao đắt tiền do nó không truyền dư lên đường truyền.

- Router có thể dùng trong một liên mạng có nhiều vùng, mỗi vùng có giao thức riêng biệt.

- Router có thể xác định được đường đi an toàn và tốt nhất trong mạng nên độ an toàn của thông tin được đảm bảo hơn.

- Trong một mạng phức hợp khi các gói tin luân chuyển các đường có thể gây nên tình trạng tắc nghẽn của mạng thì các Router có thể được cài đặt các phương thức nhằm tránh được tắc nghẽn.




*Hình 6.9: Ví dụ về bảng chỉ đường (Routing table) của Router.*

## Các phương thức hoạt động của Router

Đó là phương thức mà một Router có thể nối với các Router khác để qua đó chia sẻ thông tin về mạng hiện co. Các chương trình chạy trên Router luôn xây dựng bảng chỉ đường qua việc trao đổi các thông tin với các Router khác.

- Phương thức véc tơ khoảng cách : mỗi Router luôn luôn truyền đi thông tin về bảng chỉ đường của mình trên mạng, thông qua đó các Router khác sẽ cập nhật lên bảng chỉ đường của mình.

- Phương thức trạng thái tĩnh : Router chỉ truyền các thông báo khi có phát hiện có sự thay đổi trong mạng vàchỉ khi đó các Routerkhác ù cập nhật lại bảng chỉ đường, thông tin truyền đi khi đó thường là thông tin về đường truyền.

## Một số giao thức hoạt động chính của Router

- *RIP(Routing Information Protocol)* được phát triển bởi Xerox ả etwork system và sử dụng SPX/IPX và TCP/IP. RIP hoạt động theo phương thức véc tơ khoảng cách.

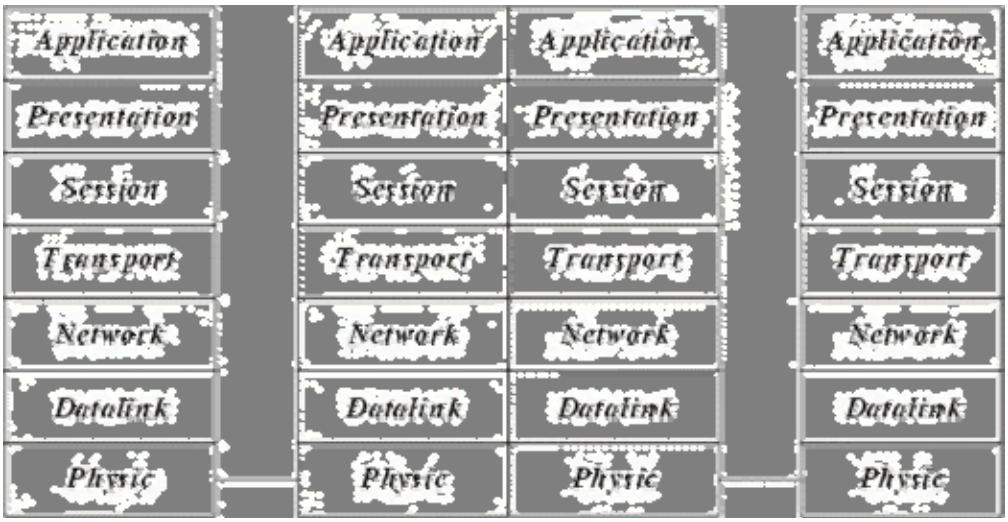
- *NLSP (Netware Link Service Protocol)* được phát triển bởi ả ovell dùng để thay thế RIP hoạt động theo phương thức véctơ khoảng cách, mỗi Router được biết cấu trúc của mạng và việc truyền các bảng chỉ đường giảm đi..

- *OSPF (Open Shortest Path First)* là một phần của TCP/IP với phương thức trạng thái tĩnh, trong đó có xét tới ưu tiên, giá đường truyền, mật độ truyền thông...

- *OSPF-IS (Open System Interconnection Intermediate System to Intermediate System)* là một phần của TCP/IP với phương thức trạng thái tĩnh, trong đó có xét tới ưu tiên, giá đường truyền, mật độ truyền thông...

## IV. Gateway (cổng nối)

Gateway dùng để kết nối các mạng không thuần nhất chẳng hạn như các mạng cục bộ và các mạng máy tính lớn (Mainframe), do các mạng hoàn toàn không thuần nhất nên việc chuyển đổi thực hiện trên cả 7 tầng của hệ thống mở OSI. Thường được sử dụng nối các mạng LAả vào máy tính lớn. Gateway có các giao thức xác định trước thường là nhiều giao thức, một Gateway đa giao thức thường được chế tạo như các Card có chứa các bộ xử lý riêng và cài đặt trên các máy tính hoặc thiết bị chuyên biệt.




*Hình 6.10: Hoạt động của Gateway trong mô hình OSI*

Hoạt động của Gateway thông thường phức tạp hơn là Router nên thông suất của nó thường chậm hơn và thường không dùng nối mạng LAả -LAả .

## V. Hub (Bộ tập trung)

Hub thường được dùng để nối mạng, thông qua những đầu cắm của nó người ta liên kết với các máy tính dưới dạng hình sao.

ả gười ta phân biệt các Hub thành 3 loại như sau sau :

- ***Hub bị động (Passive Hub) :*** Hub bị động không chứa các linh kiện điện tử và cũng không xử lý các tín hiệu dữ liệu, nó có chức năng duy nhất là tổ hợp các tín hiệu từ một số đoạn cáp mạng. Khoảng cách giữa một máy tính và Hub không thể lớn hơn một nửa khoảng cách tối đa cho phép giữa 2 máy tính trên mạng (ví dụ khoảng cách tối đa cho phép giữa 2 máy tính của mạng là 200m thì khoảng cách tối đa giữa một máy tính và hub là 100m). Các mạng ARCnet thường dùng Hub bị động.

- ***Hub chủ động (Active Hub) :*** Hub chủ động có các linh kiện điện tử có thể khuyếch đại và xử lý các tín hiệu điện tử truyền giữa các thiết bị của mạng. Qúa trình xử lý tín hiệu được gọi là tái sinh tín hiệu, nó làm cho tín hiệu trở nên tốt hơn, ít nhạy cảm với lỗi do vậy khoảng cách giữa các thiết bị có thể tăng lên. Tuy nhiên những ưu điểm đó cũng kéo theo giá thành của Hub chủ động cao hơn nhiều so với Hub bị động. Các mạng Token ring có xu hướng dùng Hub chủ động.

www.viet-ebook.co.cc

- ***Hub thông minh (Intelligent Hub):*** cũng là Hub chủ động nhưng có thêm các chức năng mới so với loại trước, nó có thể có bộ vi xử lý của mình và bộ nhớ mà qua đó nó không chỉ cho phép điều khiển hoạt động thông qua các chương trình quản trị mạng mà nó có thể hoạt động như bộ tìm đường hay một cầu nối. ả ó có thể cho phép tìm đường cho gói tin rất nhanh trên các cổng của nó, thay vì phát lại gói tin trên mọi cổng thì nó có thể chuyển mạch để phát trên một cổng có thể nối tới trạm đích.

**Chương 7**

# Giao thức TCP/IP

Giao thức TCP/IP được phát triển từ mạng ARPAả ET và Internet và được dùng như giao thức mạng và vận chuyển trên mạng Internet. TCP (Transmission Control Protocol) là giao thức thuộc tầng vận chuyển và IP (Internet Protocol) là giao thức thuộc tầng mạng của mô hình OSI. Họ giao thức TCP/IP hiện nay là giao thức được sử dụng rộng rãi nhất để liên kết các máy tính và các mạng.

Hiện nay các máy tính của hầu hết các mạng có thể sử dụng giao thức TCP/IP để liên kết với nhau thông qua nhiều hệ thống mạng với kỹ thuật khác nhau. Giao thức TCP/IP thực chất là một họ giao thức cho phép các hệ thống mạng cùng làm việc với nhau thông qua việc cung cấp phương tiện truyền thông liên mạng.

## I. Giao thức IP

### 1. Tổng quát

ả hiệm vụ chính của giao thức IP là cung cấp khả năng kết nối các mạng con thành liên kết mạng để truyền dữ liệu, vai trò của IP là vai trò của giao thức tầng mạng trong mô hình OSI. Giao thức IP là một giao thức kiểu không liên kết (connectionlees) có nghĩa là không cần có giai đoạn thiết lập liên kết trước khi truyền dữ liệu.

Sơ đồ địa chỉ hóa để định danh các trạm (host) trong liên mạng được gọi là địa chỉ IP 32 bits (32 bit IP address). Mỗi giao diện trong 1 máy có hỗ trợ giao thức IP đều phải được gán 1 địa chỉ IP (một máy tính có thể gắn với nhiều mạng do vậy có thể có nhiều địa chỉ IP). Địa chỉ IP gồm 2 phần: địa chỉ mạng (netid) và địa chỉ máy (hostid). Mỗi địa chỉ IP có độ dài 32 bits được tách thành 4 vùng (mỗi vùng 1 byte), có thể biểu thị dưới dạng thập phân, bát phân, thập lục phân hay nhị phân. Cách viết phổ biến nhất là dùng ký pháp thập phân có dấu chấm (dotted decimal notation) để tách các vùng. Mục đích của địa chỉ IP là để định danh duy nhất cho một máy tính bất kỳ trên liên mạng.

Do tổ chức và độ lớn của các mạng con (subnet) của liên mạng có thể khác nhau, người ta chia các địa chỉ IP thành 5 lớp, ký hiệu là A, B, C, D và E. Trong lớp A, B, C chứa địa chỉ có thể gán được. Lớp D dành riêng cho lớp kỹ thuật multicasting. Lớp E được dành những ứng dụng trong tương lai.

ả etid trong địa chỉ mạng dùng để nhận dạng từng mạng riêng biệt. Các mạng liên kết phải có địa chỉ mạng (netid) riêng cho mỗi mạng. Ở đây các bit đầu tiên của byte đầu tiên được dùng để định danh lớp địa chỉ (0 - lớp A, 10 - lớp B, 110 - lớp C, 1110 - lớp D và 11110 - lớp E).

Ơû đây ta xét cấu trúc của các lớp địa chỉ có thể gán được là lớp A, lớp B, lớp C

Cấu trúc của các địa chỉ IP như sau:

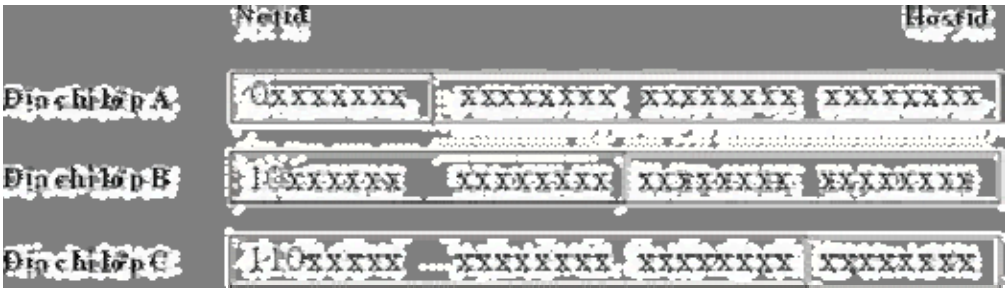
- Mạng lớp A: địa chỉ mạng (netid) là 1 Byte và địa chỉ host (hostid) là 3 byte.

- Mạng lớp B: địa chỉ mạng (netid) là 2 Byte và địa chỉ host (hostid) là 2 byte.
- Mạng lớp C: địa chỉ mạng (netid) là 3 Byte và địa chỉ host (hostid) là 1 byte.

Lớp A cho phép định danh tới 126 mạng, với tối đa 16 triệu host trên mỗi mạng. Lớp này được dùng cho các mạng có số trạm cực lớn.

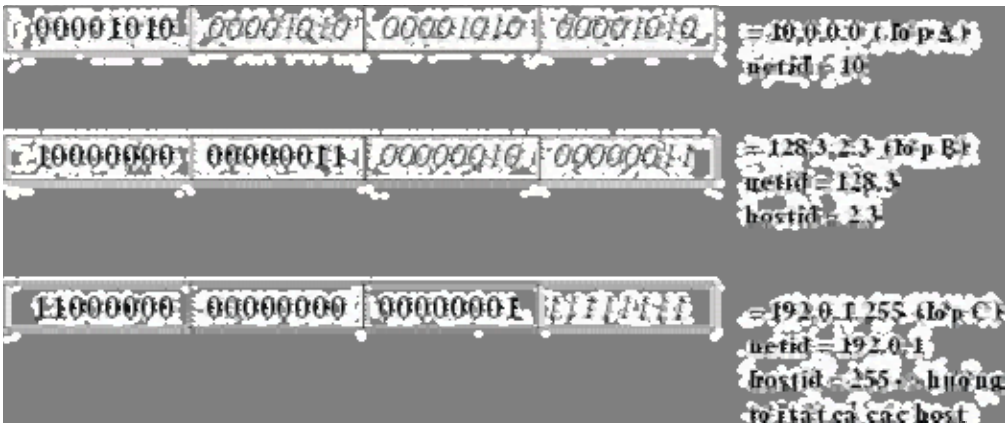
Lớp B cho phép định danh tới 16384 mạng, với tối đa 65534 host trên mỗi mạng.

Lớp C cho phép định danh tới 2 triệu mạng, với tối đa 254 host trên mỗi mạng. Lớp này được dùng cho các mạng có ít trạm.




*Hình 7.1: Cấu trúc các lớp địa chỉ IP*

*Một số địa chỉ có tính chất đặc biệt*: Một địa chỉ có hostid = 0 được dùng để hướng tới mạng định danh bởi vùng netid. ả gược lại, một địa chỉ có vùng hostid gồm toàn số 1 được dùng để hướng tới tất cả các host nối vào mạng netid, và nếu vùng netid cũng gồm toàn số 1 thì nó hướng tới tất cả các host trong liên mạng

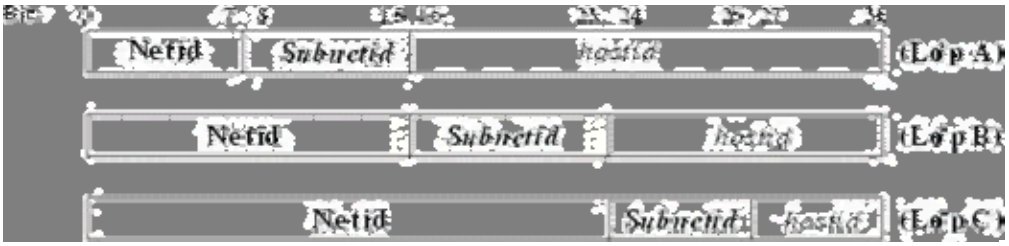



*Hình 7.2: Ví dụ cấu trúc các lớp địa chỉ IP*

Cần lưu ý rằng các địa chỉ IP được dùng để định danh các host và mạng ở tầng mạng của mô hình OSI, và chúng không phải là các địa chỉ vật lý (hay địa chỉ MAC) của các trạm trên đó một mạng cục bộ (Ethernet, Token Ring.).

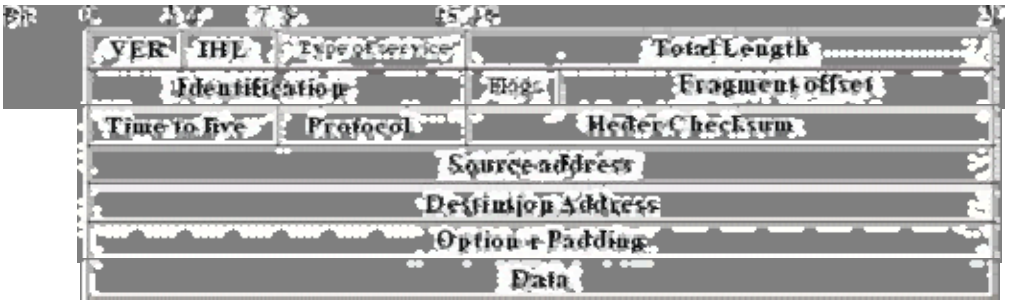
Trong nhiều trường hợp, một mạng có thể được chia thành nhiều mạng con (subnet), lúc đó có thể đưa thêm các vùng subnetid để định danh các mạng con. Vùng subnetid được lấy từ vùng hostid, cụ thể đối với lớp A, B, C như ví dụ sau:

www.viet-ebook.co.cc




*Hình 7.3: Ví dụ địa chỉ khi bổ sung vùng subnetid*

Đơn vị dữ liệu dùng trong IP được gọi là gói tin (datagram), có khuôn dạng




*Hình 7.4: Dạng thức của gói tin IP*

Ý nghĩa của thông số như sau:

- *VER* (4 bits): chỉ version hiện hành của giao thức IP hiện được cài đặt, Việc có chỉ số version cho phép có các trao đổi giữa các hệ thống sử dụng version cũ và hệ thống sử dụng version mới.

- *IHL* (4 bits): chỉ độ dài phần đầu (Internet header Length) của gói tin datagram, tính theo đơn vị từ ( 32 bits). Trường này bắt buột phải có vì phần đầu IP có thể có độ dài thay đổi tùy ý. Độ dài tối thiểu là 5 từ (20 bytes), độ dài tối đa là 15 từ hay là 60 bytes.

- *Type of service* (8 bits): đặc tả các tham số về dịch vụ nhằm thông báo cho mạng biết dịch vụ nào mà gói tin muốn được sử dụng, chẳng hạn ưu tiên, thời hạn chậm trễ, năng suất truyền và độ tin cậy. Hình sau cho biết ý nghĩ của trường 8 bits này.

- Precedence (3 bit): chỉ thị về quyền ưu tiên gửi datagram, nó có giá trị từ 0 (gói tin bình thường) đến 7 (gói tin kiểm soát mạng).

- D (Delay) (1 bit): chỉ độ trễ yêu cầu trong đó

  - D = 0 gói tin có độ trễ bình thường

  - D = 1 gói tin độ trễ thấp

- T (Throughput) (1 bit): chỉ độ thông lượng yêu cầu sử dụng để truyền gói tin với lựa chọn truyền trên đường thông suất thấp hay đường thông suất cao.
    - T = 0 thông lượng bình thường và
    - T = 1 thông lượng cao
- R (Reliability) (1 bit): chỉ độ tin cậy yêu cầu
    - R = 0 độ tin cậy bình thường
    - R = 1 độ tin cậy cao
- *Total Length* (16 bits): chỉ độ dài toàn bộ gói tin, kể cả phần đầu tính theo đơn vị byte với chiều dài tối đa là 65535 bytes. Hiện nay giới hạn trên là rất lớn nhưng trong tương lai với những mạng Gigabit thì các gói tin có kích thước lớn là cần thiết.
- *Identification* (16 bits): cùng với các tham số khác (như Source Address và Destination Address) tham số này dùng để định danh duy nhất cho một datagram trong khoảng thời gian nó vẫn còn trên liên mạng.
- *Flags (3 bits):* liên quan đến sự phân đoạn (fragment) các datagram, Các gói tin khi đi trên đường đi có thể bị phân thành nhiều gói tin nhỏ, trong trường hợp bị phân đoạn thì trường Flags được dùng điều khiển phân đoạn và tái lắp ghép bó dữ liệu. Tùy theo giá trị của Flags sẽ có ý nghĩa là gói tin sẽ không phân đoạn, có thể phân đoạn hay là gói tin phân đoạn cuối cùng. Trường ***Fragment Offset*** cho biết vị trí dữ liệu thuộc phân đoạn tương ứng với đoạn bắt đầu của gói dữ liệu gốc. Ý nghĩa cụ thể của trường Flags là:

    - bit 0: reserved - chưa sử dụng, luôn lấy giá trị 0.
    - bit 1: (DF) = 0 (May Fragment) = 1 (Don't Fragment)
    - bit 2: (MF) = 0 (Last Fragment) = 1 (More Fragments)
- *Fragment Offset (13 bits)*: chỉ vị trí của đoạn (fragment) ở trong datagram tính theo đơn vị 8 bytes, có nghĩa là phần dữ liệu mỗi gói tin (trừ gói tin cuối cùng) phải chứa một vùng dữ liệu có độ dài là bội số của 8 bytes. Điều này có ý nghĩa là phải nhân giá trị của Fragment offset với 8 để tính ra độ lệch byte.
- *Time to Live (8 bits)*: qui định thời gian tồn tại (tính bằng giây) của gói tin trong mạng để tránh tình trạng một gói tin bị quẩn trên mạng. Thời gian này được cho bởi trạm gửi và được giảm đi (thường qui ước là 1 đơn vị) khi datagram đi qua mỗi router của liên mạng. Thời lượng này giảm xuống tại mỗi router với mục đích giới hạn thời gian tồn tại của các gói tin và kết thúc những lần lặp lại vô hạn trên mạng. Sau đây là 1 số điều cần lưu ý về trường ***Time To Live***:

- ả út trung gian của mạng không được gởi 1 gói tin mà trường này có giá trị= 0.

- Một giao thức có thể ấn định ***Time To Live*** để thực hiện cuộc ra tìm tài nguyên trên mạng trong phạm vi mở rộng.

- Một giá trị cố định tối thiểu phải đủ lớn cho mạng hoạt động tốt.

- *Protocol (8 bits):* chỉ giao thức tầng trên kế tiếp sẽ nhận vùng dữ liệu ở trạm đích (hiện tại thường là TCP hoặc UDP được cài đặt trên IP). Ví dụ: **TCP** có giá trị trường **Protocol** là 6, **UDP** có giá trị trường **Protocol** là 17

- *Header Checksum (16 bits)*: Mã kiểm soát lỗi của header gói tin IP.

- *Source Address (32 bits)*: Địa chỉ của máy nguồn.

- *Destination Address (32 bits)*: địa chỉ của máy đích

- *Options (độ dài thay đổi)*: khai báo các lựa chọn do người gửi yêu cầu (tuỳ theo từng chương trình).

- *Padding (độ dài thay đổi)*: Vùng đệm, được dùng để đảm bảo cho phần header luôn kết thúc ở một mốc 32 bits.

- *Data (độ dài thay đổi)*: Trên một mạng cục bộ như vậy, hai trạm chỉ có thể liên lạc với nhau nếu chúng biết địa chỉ vật lý của nhau. ả hư vậy vấn đề đặt ra là phải thực hiện ánh xạ giữa địa chỉ IP (32 bits) và địa chỉ vật lý (48 bits) của một trạm.

### 2. Các giao thức trong mạng IP

Để mạng với giao thức IP hoạt động được tốt người ta cần một số giao thức bổ sung, các giao thức này đều không phải là bộ phận của giao thức IP và giao thức IP sẽ dùng đến chúng khi cần.

- *Giao thức ARP (Address Resolution Protocol):* Ở đây cần lưu ý rằng các địa chỉ IP được dùng để định danh các host và mạng ở tầng mạng của mô hình OSI, và chúng không phải là các địa chỉ vật lý (hay địa chỉ MAC) của các trạm trên đó một mạng cục bộ (Ethernet, Token Ring.). Trên một mạng cục bộ hai trạm chỉ có thể liên lạc với nhau nếu chúng biết địa chỉ vật lý của nhau. ả hư vậy vấn đề đặt ra là phải tìm được ánh xạ giữa địa chỉ IP (32 bits) và địa chỉ vật lý của một trạm. *Giao thức ARP* đã được xây dựng để tìm địa chỉ vật lý từ địa chỉ IP khi cần thiết.

- *Giao thức RARP (Reverse Address Resolution Protocol)*: Là giao thức ngược với *giao thức ARP*. Giao thức RARP được dùng để tìm địa chỉ IP từ địa chỉ vật lý.

- *Giao thức ICMP (Internet Control Message Protocol):* Giao thức này thực hiện truyền các thông báo điều khiển (báo cáo về các tình trạng các lỗi trên mạng.) giữa các gateway hoặc một nút của liên mạng. Tình trạng lỗi có thể là: một gói tin IP không thể tới đích của nó, hoặc một router không đủ bộ nhớ đệm để lưu và chuyển một gói tin IP, Một thông báo ICMP được tạo và chuyển cho IP. IP sẽ "bọc"

(encapsulate) thông báo đó với một IP header và truyền đến cho router hoặc trạm đích.

### 3. Các bước hoạt động của giao thức IP

Khi giao thức IP được khởi động nó trở thành một thực thể tồn tại trong máy tính và bắt đầu thực hiện những chức năng của mình, lúc đó thực thể IP là cấu thành của tầng mạng, nhận yêu cầu từ các tầng trên nó và gửi yêu cầu xuống các tầng dưới nó.

Đối với thực thể IP ở máy nguồn, khi nhận được một yêu cầu gửi từ tầng trên, nó thực hiện các bước sau đây:

- Tạo một IP datagram dựa trên tham số nhận được.
- Tính checksum và ghép vào header của gói tin.
- Ra quyết định chọn đường: hoặc là trạm đích nằm trên cùng mạng hoặc một gateway sẽ được chọn cho chặng tiếp theo.
- Chuyển gói tin xuống tầng dưới để truyền qua mạng.

Đối với router, khi nhận được một gói tin đi qua, nó thực hiện các động tác sau:

1) Tính chesksum, nếu sai thì loại bỏ gói tin.

2) Giảm giá trị tham số Time - to Live. nếu thời gian đã hết thì loại bỏ gói tin.

3) Ra quyết định chọn đường.

4) Phân đoạn gói tin, nếu cần.

5) Kiến tạo lại IP header, bao gồm giá trị mới của các vùng Time - to -Live, Fragmentation và Checksum.

6) Chuyển datagram xuống tầng dưới để chuyển qua mạng.

Cuối cùng khi một datagram nhận bởi một thực thể IP ở trạm đích, nó sẽ thực hiện bởi các công việc sau:

1) Tính checksum. ả ếu sai thì loại bỏ gói tin.

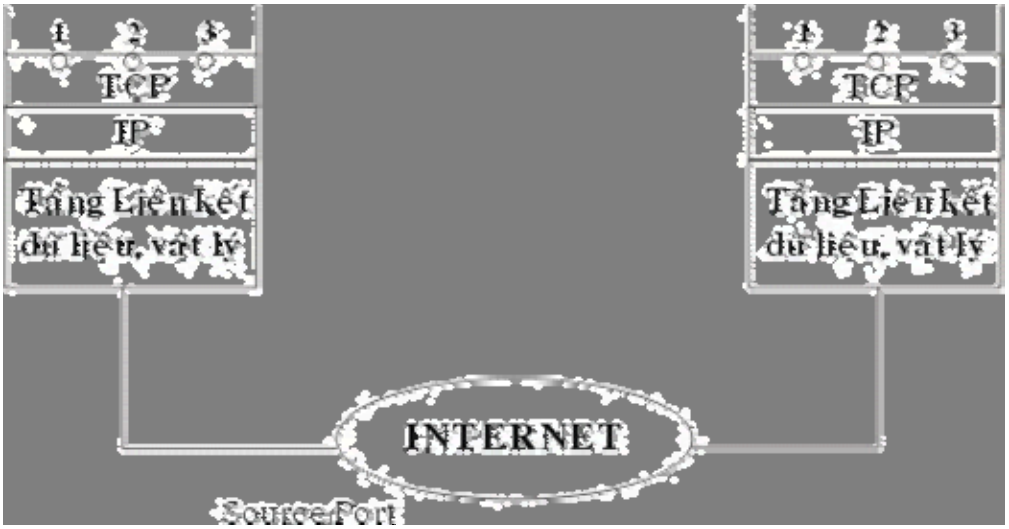
2) Tập hợp các đoạn của gói tin (nếu có phân đoạn)

3) Chuyển dữ liệu và các tham số điều khiển lên tầng trên.

## II. Giao thức điều khiển truyền dữ liệu TCP

TCP là một giao thức "có liên kết" (connection - oriented), nghĩa là cần phải thiết lập liên kết giữa hai thực thể TCP trước khi chúng trao đổi dữ liệu với nhau. Một tiến trình ứng

dụng trong một máy tính truy nhập vào các dịch vụ của giao thức TCP thông qua một cổng (port) của TCP. Số hiệu cổng TCP được thể hiện bởi 2 bytes.




*Hình 7.5: Cổng truy nhập dịch vụ TCP*

Một cổng TCP kết hợp với địa chỉ IP tạo thành một đầu nối TCP/IP (socket) duy nhất trong liên mạng. Dịch vụ TCP được cung cấp nhờ một liên kết logic giữa một cặp đầu nối TCP/IP. Một đầu nối TCP/IP có thể tham gia nhiều liên kết với các đầu nối TCP/IP ở xa khác nhau. Trước khi truyền dữ liệu giữa 2 trạm cần phải thiết lập một liên kết TCP giữa chúng và khi không còn nhu cầu truyền dữ liệu thì liên kết đó sẽ được giải phóng.

Các thực thể của tầng trên sử dụng giao thức TCP thông qua các hàm gọi (function calls) trong đó có các hàm yêu cầu để yêu cầu, để trả lời. Trong mỗi hàm còn có các tham số dành cho việc trao đổi dữ liệu.

*Các bước thực hiện để thiết lập một liên kết TCP/IP*: Thiết lập một liên kết mới có thể được mở theo một trong 2 phương thức: chủ động (active) hoặc bị động (passive).

- Phương thức bị động, người sử dụng yêu cầu TCP chờ đợi một yêu cầu liên kết gửi đến từ xa thông qua một đầu nối TCP/IP (tại chỗ). ả gười sử dụng dùng hàm passive Open có khai báo cổng TCP và các thông số khác (mức ưu tiên, mức an toàn)

- Với phương thức chủ động, người sử dụng yêu cầu TCP mở một liên kết với một một đầu nối TCP/IP ở xa. Liên kết sẽ được xác lập nếu có một hàm Passive Open tương ứng đã được thực hiện tại đầu nối TCP/IP ở xa đó.

**Bảng liệt kê một vài cổng TCP phổ biến.**

| Số hiệu cổng | Mô tả |
|---|---|
| 0 | Reserved |

| | |
|---|---|
| 5 | Remote job entry |
| 7 | Echo |
| 9 | Discard |
| 11 | Systat |
| 13 | Daytime |
| 15 | ả estat |
| 17 | Quotd (quote odd day |
| 20 | ftp-data |
| 21 | ftp (control) |
| 23 | Telnet |
| 25 | SMTP |
| 37 | Time |
| 53 | ả ame Server |
| 102 | ISO - TSAP |
| 103 | X.400 |
| 104 | X.400 Sending |
| 111 | Sun RPC |
| 139 | ả et BIOS Session source |
| 160 - 223 | Reserved |

Khi người sử dụng gửi đi một yêu cầu mở liên kết sẽ được nhận hai thông số trả lời từ TCP.

- Thông số Open ID được TCP trả lời ngay lập tức để gán cho một liên kết cục bộ (local connection name) cho liên kết được yêu cầu. Thông số này về sau được dùng để tham chiếu tới liên kết đó. (Trong trường hợp nếu TCP không thể thiết lập được liên kết yêu cầu thì nó phải gửi tham số Open Failure để thông báo.)

- Khi TCP thiết lập được liên kết yêu cầu nó gửi tham số Open Sucsess được dùng để thông báo liên kết đã được thiết lập thành công. Thông báo này dược chuyển đến trong cả hai trường hợp bị động và chủ động. Sau khi một liên kết được mở, việc truyền dữ liệu trên liên kết có thể được thực hiện.

*Các bước thực hiện khi truyền và nhận dữ liệu:* Sau khi xác lập được liên kết người sữ dụng gửi và nhận dữ liệu. Việc gửi và nhận dữ liệu thông qua các hàm Send và receive.

- *Hàm Send:* Dữ liệu được gửi xuống TCP theo các khối (block). Khi nhận được một khối dữ liệu, TCP sẽ lưu trữ trong bộ đệm (buffer). ả ếu cờ PUSH được dựng thì toàn bộ dữ liệu trong bộ đệm được gửi, kể cả khối dữ liệu mới đến sẽ được gửi đi. ả gược lại cờ PUSH không được dựng thì dữ liệu được giữ lại trong bộ đệm và sẽ gửi đi khi có cơ hội thích hợp (chẳng hạn chờ thêm dữ liệu nữa để gữi đi với hiệu quả hơn).

- *Hàm reveive*: Ở trạm đích dữ liệu sẽ được TCP lưu trong bộ đệm gắn với mỗi liên kết. ả ếu dữ liệu được đánh dấu với một cờ PUSH thì toàn bộ dữ liệu trong bộ đệm (kể cả các dữ liệu được lưu từ trước) sẽ được chuyển lên cho người sữ dụng. Còn nếu dữ liệu đến không được đánh dấu với cờ PUSH thì TCP chờ tới khi thích hợp mới chuyển dữ liệu với mục tiêu tăng hiệu quả hệ thống.

ả ói chung việc nhận và giao dữ liệu cho người sử dụng đích của TCP phụ thuộc vào việc cài đặt cụ thể. Trường hợp cần chuyển gấp dữ liệu cho người sử dụng thì có thể dùng cờ URGEả T và đánh dấu dữ liệu bằng bit URG để báo cho người sử dụng cần phải sử lý khẩn cấp dữ liệu đó.

*Các bước thực hiện khi đóng một liên kết:* Việc đóng một liên kết khi không cần thiết được thực hiên theo một trong hai cách: *dùng hàm Close* hoặc *dùng hàm Abort*.

- *Hàm Close*: yêu cầu đóng liên kết một cách bình thường. Có nghĩa là việc truyền dữ liệu trên liên kết đó đã hoàn tất. Khi nhận được một *hàm Close* TCP sẽ truyền đi tất cả dữ liệu còn trong bộ đệm thông báo rằng nó đóng liên kết. Lưu ý rằng khi một người sử dụng đã gửi đi một *hàm Close* thì nó vẫn phải tiếp tục nhận dữ liệu đến trên liên kết đó cho đến khi TCP đã báo cho phía bên kia biết về việc đóng liên kết và chuyển giao hết tất cả dữ liệu cho người sử dụng của mình.

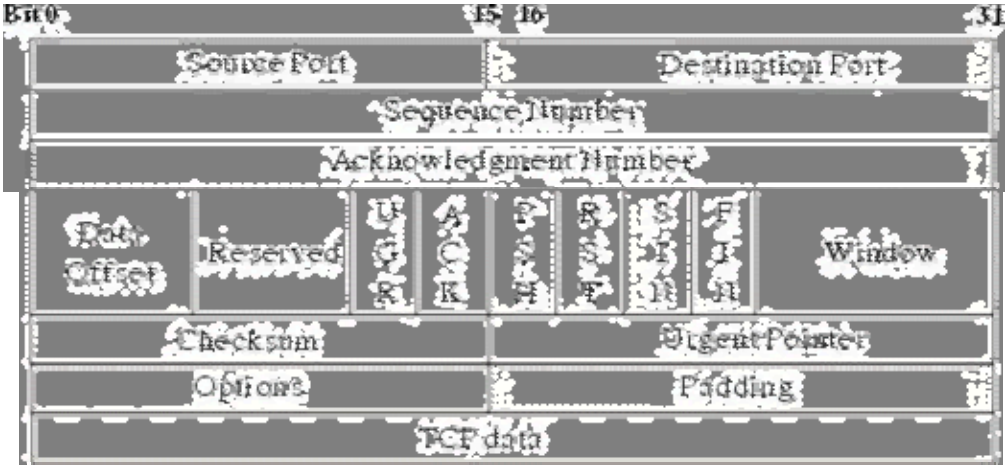
- *Hàm Abort*: ả gười sử dụng có thể đóng một liên kết bất và sẽ không chấp nhận dữ liệu qua liên kết đó nữa. Do vậy dữ liệu có thể bị mất đi khi đang được truyền đi. TCP báo cho TCP ở xa biết rằng liên kết đã được hủy bỏ và TCP ở xa sẽ thông báo cho người sử dụng cũa mình.

Một số hàm khác của TCP:

- *Hàm Status*: cho phép người sử dụng yêu cầu cho biết trạng thái của một liên kết cụ thể, khi đó TCP cung cấp thông tin cho người sử dụng.

- *Hàm Error*: thông báo cho người sử dụng TCP về các yêu cầu dịch vụ bất hợp lệ liên quan đến một liên kết có tên cho trước hoặc về các lỗi liên quan đến môi trường.

Đơn vị dữ liệu sử dụng trong TCP được gọi là segment (đoạn dữ liệu), có các tham số với ý nghĩa như sau:




*Hình 7.5: Dạng thức của segment TCP*

- Source Por (16 bits): Số hiệu cổng TCP của trạm nguồn.
- Destination Port (16 bit): Số hiệu cổng TCP của trạm đích.
- Sequence ả umber (32 bit): số hiệu của byte đầu tiên của segment trừ khi bit SYả được thiết lập. ả ếy bit SYả được thiết lập thì Sequence ả umber là số hiệu tuần tự khởi đầu (ISả ) và byte dữ liệu đầu tiên là ISả +1.
- Acknowledgment ả umber (32 bit): số hiệu của segment tiếp theo mà trạm nguồn đang chờ để nhận. ả gầm ý báo nhận tốt (các) segment mà trạm đích đã gửi cho trạm nguồn.
- Data offset (4 bit): số lượng bội của 32 bit (32 bit words) trong TCP header (tham số này chỉ ra vị trí bắt đầu của nguồn dữ liệu).
- Reserved (6 bit): dành để dùng trong tương lai
- Control bit (các bit điều khiển):
    - URG: Vùng con trỏ khẩn (Ucgent Poiter) có hiệu lực.
    - ACK: Vùng báo nhận (ACK number) có hiệu lực.
    - PSH: Chức năng PUSH.
    - RST: Khởi động lại (reset) liên kết.
    - SYả : Đồng bộ hóa số hiệu tuần tự (sequence number).
    - FIả : Không còn dữ liệu từ trạm nguồn.

- Window (16 bit): cấp phát credit để kiểm soát nguồn dữ liệu (cơ chế cửa sổ). Đây chính là số lượng các byte dữ liệu, bắt đầu từ byte được chỉ ra trong vùng ACK number, mà trạm nguồn đã saün sàng để nhận.

- Checksum (16 bit): mã kiểm soát lỗi cho toàn bộ segment (header + data)

- Urgemt Poiter (16 bit): con trỏ này trỏ tới số hiệu tuần tự của byte đi theo sau dữ liệu khẩn. Vùng này chỉ có hiệu lực khi bit URG được thiết lập.

- Options (độ dài thay đổi): khai báo các option của TCP, trong đó có độ dài tối đa của vùng TCP data trong một segment.

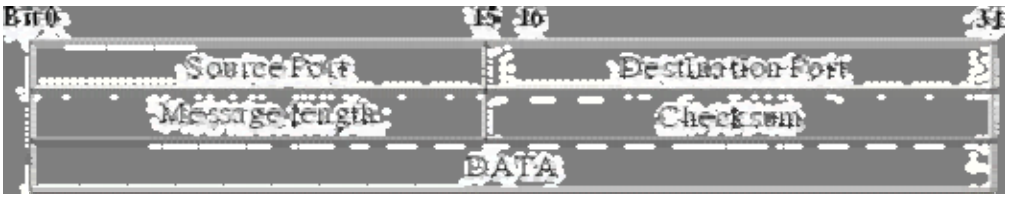
- Paddinh (độ dài thay đổi): phần chèn thêm vào header để đảm bảo phần header luôn kết thúc ở một mốc 32 bit. Phần thêm này gồm toàn số 0.

- TCP data (độ dài thay đổi): chứa dữ liệu của tầng trên, có độ dài tối đa ngầm định là 536 byte. Giá trị này có thể điều chỉnh bằng cách khai báo trong vùng options.

**III. Giao thức UDP (User Datagram Protocol)**

UDP (User Datagram Protocol) là giao thức theo phương thức không liên kết được sử dụng thay thế cho TCP ở trên IP theo yêu cầu của từng ứng dụng. Khác với TCP, UDP không có các chức năng thiết lập và kết thúc liên kết. Tương tự như IP, nó cũng không cung cấp cơ chế báo nhận (acknowledgment), không sắp xếp tuần tự các gói tin (datagram) đến và có thể dẫn đến tình trạng mất hoặc trùng dữ liệu mà không có cơ chế thông báo lỗi cho người gửi. Qua đó ta thấy UDP cung cấp các dịch vụ vận chuyển không tin cậy như trong TCP.

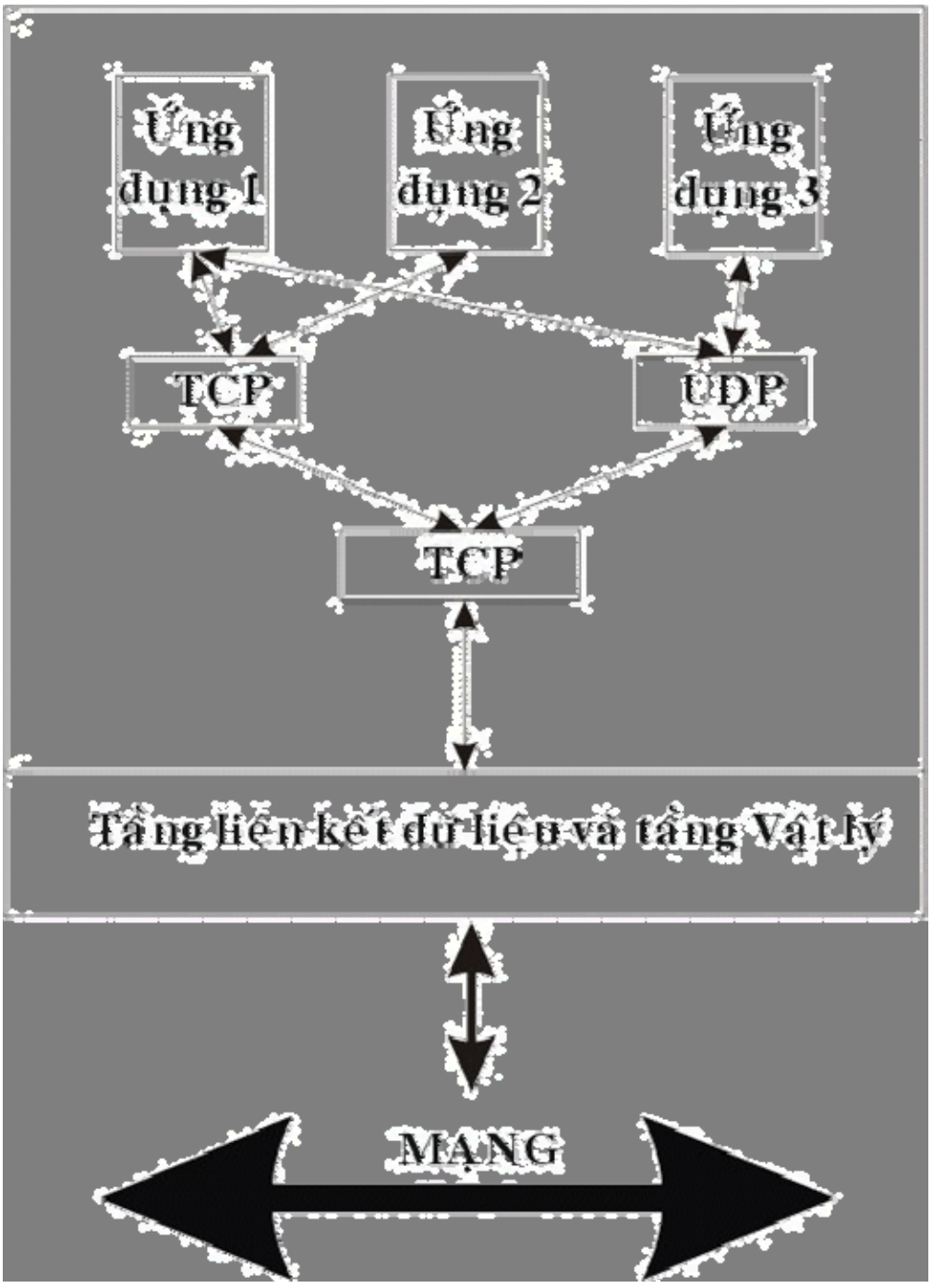
Khuôn dạng UDP datagram được mô tả với các vùng tham số đơn giản hơn nhiều so với TCP segment.




*Hình 7.7: Dạng thức của gói tin UDP*

UDP cũng cung cấp cơ chế gán và quản lý các số hiệu cổng (port number) để định danh duy nhất cho các ứng dụng chạy trên một trạm của mạng. Do ít chức năng phức tạp nên UDP thường có xu thế hoạt động nhanh hơn so với TCP. ả ó thường được dùng cho các ứng không đòi hỏi độ tin cậy cao trong giao vận.

www.viet-ebook.co.cc




*Hình 7.8: Mô hình quan hệ họ giao thức TCP/IP*

www.viet-ebook.co.cc

**Chương 8**

# Các dịch vụ của mạng diện rộng (WAN)

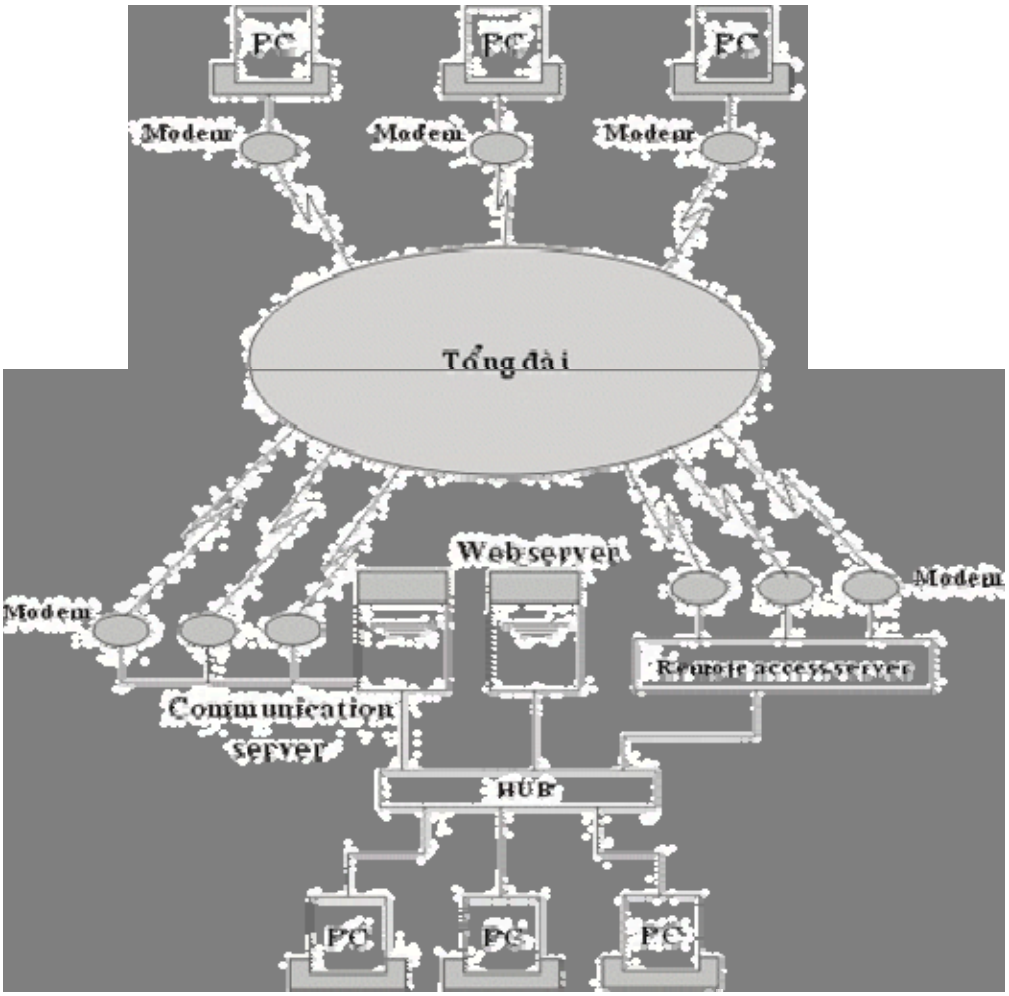
Hiện nay trên thế giới có nhiều dịch vụ dành cho việc chuyển thông tin từ khu vực này sang khu vực khác nhằm liên kết các mạng LAả của các khu vực khác nhau lại. Để có được những liên kết như vậy người ta thường sử dụng các dịch vụ của các mạng diện rộng. Hiện nay trong khi giao thức truyền thông cơ bản của LAả là Ethernet, Token Ring thì giao thức dùng để tương nối các LAả thông thường dựa trên chuẩn TCP/IP. ả gày nay khi các dạng kết nối có xu hướng ngày càng đa dạng và phân tán cho nên các mạng WAả đang thiên về truyền theo đơn vị tập tin thay vì truyền một lần xử lý.

Có nhiều cách phân loại mạng diện rộng, ở đây nếu phân loại theo phương pháp truyền thông tin thì có thể chia thành 3 loại mạng như sau:

- Mạng chuyển mạch (Circuit Swiching ả etwork)
- Mạng thuê bao (Leased lines ả etwork)
- Mạng chuyển gói tin (Packet Switching ả etwork)

## I. Mạng chuyển mạch (Circuit Swiching Network)

Để thực hiện được việc liên kết giữa hai điểm nút, một đường nối giữa điểm nút này và điêm nút kia được thiết lập trong mạng thể hiện dưới dạng cuộc gọi thông qua các thiết bị chuyển mạch.




*Hình 8.1: Mô hình mạng chuyển mạch*

Một ví dụ của mạng chuyển mạch là hoạt động của mạng điện thoại, các thuê bao khi biết số của nhau có thể gọi cho nhau và có một đường nối vật lý tạm thời được thiết lập giữa hai thuê bao.

Với mô hình này mọi đường đều có thể một đường bất kỳ khác, thông qua những đường nối và các thiết bị chuyên dùng người ta có thể liên kết một đường tạm thời từ nơi gửi tới nơi nhận một đường nối vật lý, đường nối trên duy trì trong suốt phiên làm việc và chỉ giải phóng sau khi phiên làm việc kết thúc. Để thực hiện một phiên làm việc cần có các thủ tục đầy đủ cho việc thiết lập liên kết trong đó có việc thông báo cho mạng biết địa chỉ của nút nhận.

Hiện nay có 2 loại mạng chuyển mạch là chuyển mạch tương tự (analog) và chuyển mạch số (digital)

- *Chuyển mạch tương tự (Analog):* Việc chuyển dữ liệu qua mạng chuyển mạch tương tự được thực hiện qua mạng điện thoại. Các trạm sử dụng một thiết bị có tên là modem, thiết bị này sẽ chuyển các tín hiệu số từ máy tính sao tín hiệu tuần tự có trể truyền đi trên mạng điện thoại và ngược lại.

*Hình 8.2: Mô hình chuyển mạch tương tự*

Khi sử dụng đường truyền điện thoại để truyền số liệu thì các chuẩn của modem và các tính chất của nó sẽ quyết định tốc độ của đường truyền. Cùng với các kỹ thuật chuyển đổi tín hiệu các tính năng mới như nén tín hiệu cho phép nâng tốc độ truyền dữ liệu lên rất cao.

| Loại | Tốc độ (bps)ä | Loại nén | Tốc độ thực tế (bps) |
|---|---|---|---|
| Bell 212A | 1200 | | |
| CCITT V22 | 1200 | | |
| CCITT V22 bis | 2400 | Mả P Class 5 | 2400 - 3600 |
| CCITT V32 | 9600 | Mả P Class 5, V42 bis | 9600 - 19200 |
| CCITT V32 bis | 14400 | Mả P Class 5, V42 bis | 14400 - 33600 |

*Hình 8.3: Bảng kỹ thuật modem*

Các kỹ thuật nén thường dùng là Mả P Class 5 và V42 bis, Mả P Class 5 cho phép nén với tỷ lệ 1.5:1 và V42 bis nén với tỷ lệ 2:1. Tuy nhiên trên thực tế tỷ lệ nén có thể thay đổi dựa vào dạng dữ liệu được truyền.

- *Chuyển mạch số (Digital):* Đường truyền chuyển mạch số lần đầu tiên được AT&T thiệu vào cuối 1980 khi AT&T giới thiệu mạng chuyển mạch số Acnet với đường truyền 56 kbs. Việc sử dụng đường chuyển mạch số cũng đòi hỏi sử dụng thiết bị phục vụ truyền dữ liệu số (Data Service Unit - DSU) vào vị trí modem trong chuyển mạch tương tự. Thiết bị phục vụ truyền dữ liệu số có nhiệm vụ chuyển các tín hiệu số đơn chiều (unipolar) từ máy tính ra thành tín hiệu số hai chiều (bipolar) để truyền trên đường truyền.

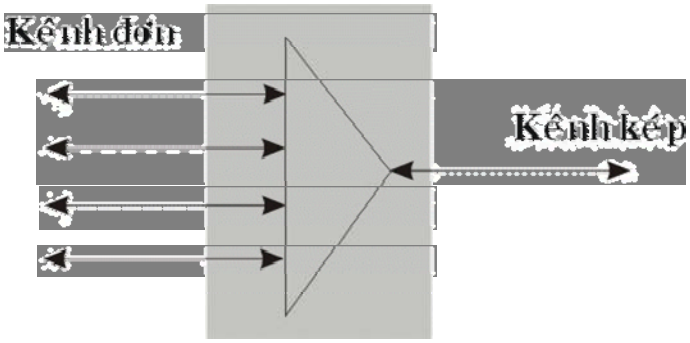
*Hình 8.3: Mô hình chuyển mạch số*

Mạng chuyển mạch số cho phép người sử dụng nâng cao tốc độ truyền (ở đây do khác biệt giữa kỹ thuật truyền số và kỹ thuật truyền tương tự nên hiệu năng của truyền mạch số cao hơn nhiều so với truyền tương tự cho dù cùng tốc độ), độ an toàn.

Vào năm 1991 AT&T giới thiệu mạng chuyển mạch số có tốc độ 384 Kbps. ả gười ta có thể dùng mạng chuyển mạch số để tạo các liên kết giữa các mạng LAả và làm các đường truyền dự phòng.

## II. Mạng thuê bao (Leased line Network)

Với kỹ thuật chuyển mạch giữa các nút của mạng (tương tự hoặc số) có một số lượng lớn đường dây truyền dữ liệu, với mỗi đường dây trong một thời điểm chỉ có nhiều nhất một phiên giao dịch, khi số lượng các trạm sử dụng tăng cao người ta nhận thấy việc sử dụng mạng chuyển mạch trở nên không kinh tế. Để giảm bớt số lượng các đường dây kết nối giữa các nút mạng người ta đưa ra một kỹ thuật gọi là ghép kênh.




*Hình 8.4: Mô hình ghép kênh*

Mô hình đó được mô tả như sau: tại một nút người ta tập hợp các tín hiệu trên của nhiều người sử dụng ghép lại để truyền trên một kênh nối duy nhất đến các nút khác, tại nút cuối người ta phân kênh ghép ra thành các kênh riêng biệt và truyền tới các người nhận.

Có hai phương thức ghép kênh chính là ghép kênh theo tần số và ghép kênh theo thời gian, hai phương thức này tương ứng với mạng thuê bao tuần tự và mạng thuê bao kỹ thuật số. trong thời gian hiện nay mạng thuê bao kỹ thuật số sử dụng kỹ thuật ghép kênh theo thời gian với đường truyền T đang được sử dụng ngày một rộng rãi và dần dần thay thế mạng thuê bao tuần tự.

### 1. Phương thức ghép kênh theo tần số

Để sử dụng phương thức ghép kênh theo tần số giữa các nút của mạng được liên kết bởi đường truyền băng tần rộng. Băng tần này được chia thành nhiều kênh con được phân biệt bởi tần số khác nhau. Khi truyền dữ liệu, mỗi kênh truyền từ người sử dụng đến nút sẽ được chuyển thành một kênh con với tần số xác định và được truyền thông qua bộ ghép kênh đến nút cuối và tại đây nó được tách ra thành kênh riêng biệt để truyền tới người nhận. Theo các chuẩn của CCITT có các phương thức ghép kênh cho phép ghép 12, 60, 300 kênh đơn.

ả gười ta có thể dùng đường thuê bao tuần tự (Analog) nối giữa máy của người sử dụng tới nút mạng thuê bao gần nhất. Khi máy của người sử dụng gửi dữ liệu thì kênh dữ liệu được

ghép với các kênh khác và truyền trên đường truyền tới nút đích và được phân ra thành kênh riêng biệt trước khi gửi tới máy của người sử dụng. Đường nối giữa máy trạm của người sử dụng tới nút mạng thuê bao cũng giống như mạng chuyển mạch tuần tự sử dụng đường dây điện thoại với các kỹ thuật chuyển đổi tín hiệu như V22, V22 bis, V32, V32 bis, các kỹ thuật nén V42 bis, Mả P class 5.

### 2.Phương thức ghép kênh theo thời gian:

Khác với phương thức ghép kênh theo tần số, phương thức ghép kênh theo thời gian chia một chu kỳ thời gian hoạt động của đường truyền trục thành nhiều khoảng nhỏ và mỗi kênh tuyền dữ liệu được một khoảng. Sau khi ghép kênh lại thành một kênh chung dữ liệu được truyền đi tương tự như phương thức ghép kênh theo tần số. ả gười ta dùng đường thuê bao là đường truyền kỹ thuật số nối giữa máy của người sử dụng tới nút mạng thuê bao gần nhất.

Hiện nay người ta có các đường truyền thuê bao như sau :

Đường T1 với tốc độ 1.544 Mbps nó bao gồm 24 kênh vớp tốc độ 64 kbps và 8000 bits điều khiển trong 1 giây.

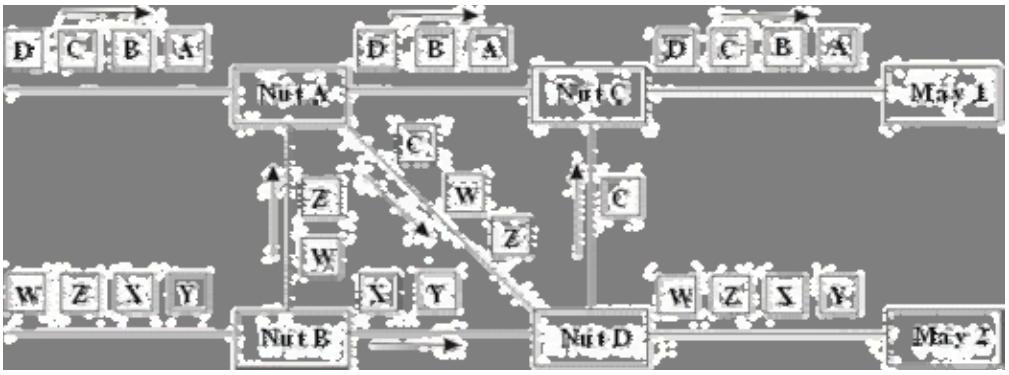
## III. Mạng chuyển gói tin (Packet Switching NetWork)

Mạng chuyển mạch gói hoạt động theo nguyên tắc sau : Khi một trạm trên mạng cần gửi dữ liệu nó cần phải đóng dữ liệu thành từng gói tin, các gói tin đó được đi trên mạng từ nút này tới nút khác tới khi đến được đích. Do việc sử dụng kỹ thuật trên nên khi một trạm không gửi tin thì mọi tài nguyên của mạng sẽ dành cho các trạm khác, do vậy mạng tiết kiệm được các tài nguyên và có thể sử dụng chúng một cách tốt nhất.

ả gười ta chia các phương thức chuyển mạch gói ra làm 2 phương thức:

- Phương thức chuyển mạch gói theo sơ đồ rời rạc.
- Phương thức chuyển mạch gói theo đường đi xác định.

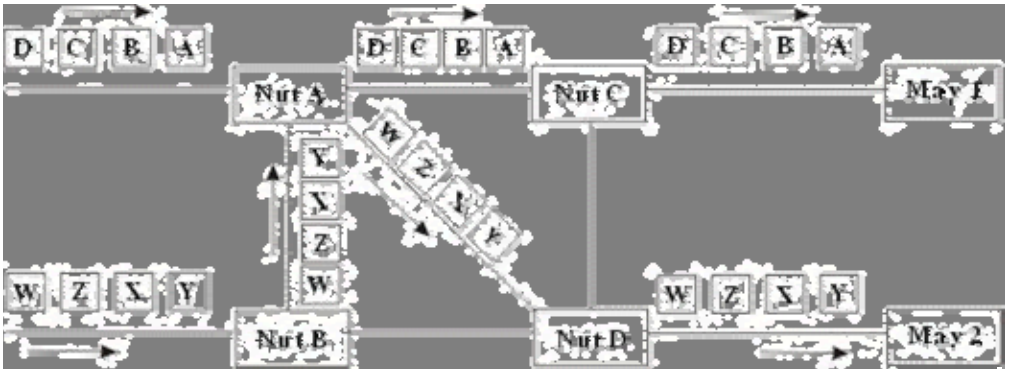
Với phương thức chuyển mạch gói theo sơ đồ rời rạc các gói tin được chuyển đi trên mạng một cách độc lập, mỗi gói tin đều có mang địa chỉ nơ i gửi và nơi nhận. Mỗi nút trong mạng khi tiếp nhận gói tin sẽ quyết định xenm đường đi của gói tin phụ thuộc vào thuật toán tìm đường tại nút và những thông tin về mạng mà nút đó có. Việc truyền theo phương thức này cho ta sự mềm dẻo nhất định do đường đi với mỗi gói tin trở nên mềm dẻo tuy nhiên điều này yêu cầu một số lượng tính toán rất lớn tại mỗi nút nên hiện nay phần lớn các mạng chuyển sang dùng phương chuyển mạch gói theo đường đi xác định.




*Hình 8.5: Ví dụ phương thức sơ đồ rời rạc.*

Phương thức chuyển mạch gói theo đường đi xác định:

Trước khi truyền dữ liệu một đường đi (hay còn gọi là đường đi ảo) được thiết lập giữa trạm gửi và trạm nhận thông qua các nút của mạng. Đường đi trên mang số hiệu phân biệt với các đường đi khác, sau đó các gói tin được gửi đi theo đường đã thiết lập để tới đích, các gói tin mang số hiệu củ đường ảo để có thể được nhận biết khi qua các nút. Điều này khiến cho việc tính toán đường đi cho phiên liên lạc chỉ cần thực hiện một lần.




*Hình 8.6: Ví dụ phương thức đường đi xác định*

### 1. Mạng X25

Được CCITT công bố lần đầu tiên vào 1970 lúc lĩnh vực viễn thông lần đầu tiên tham gia vào thế giới truyền dữ liệu với các đặc tính:

- X25 cung cấp quy trình kiểm soát luồng giữa các đầu cuối đem lại chất lương đường truyền cao cho dù chất lương đương dây truyền không cao.
- X25 được thiết kế cho cả truyền thông chuyển mạch lẫn truyền thông kiểu điểm nối điểm.
- Được quan tâm và tham gia nhanh chóng trên toàn cầu.

Trong X25 có chức năng dồn kênh (multiplexing) đối với liên kết logic (virtual circuits) chỉ làm nhiệm vụ kiểm soát lỗi cho các frame đi qua. Điều này làm tăng độ phức tạp trong việc phối hợp các thủ tục giữa hai tầng kề nhau, dẫn đến thông lượng bị hạn chế do tổng phí xử lý mỗi gói tin tăng lên. X25 kiểm tra lỗi tại mỗi nút trước khi truyền tiếp, điều này làm cho đường truyền chó chất lượng rất cao gần như phi lỗi. Tuy nhiên do vậy khối lượng tích toán tại mỗi nút khá lớn, đối với những đường truyền của những năm 1970 thì điều đó là cần thiết nhưng hiện nay khi kỹ thuật truyền dẫn đã đạt được những tiến bộ rất cao thì việc đó trở nên lãng phí

### 2. Mạng Frame Relay

Mỗi gói tin trong mạng gọi là Frame, do vậy mạng gọi là Frame relay. Đặc điểm khác biệt giữa mạng Frame Relay và mạng X25 mạng Frame Relay là chỉ kiểm tra lỗi tại hai trạm gửi và trạm nhận còn trong quá trình chuyển vận qua các nút trung gian gói tin sẽ không được kiểm lỗi nữa. Do vậy thời gian xử lý trên mỗi nút nhanh hơn, tuy nhiên khi có lỗi thì gói tin phải được phát lại từ trạm đầu. Với độ an toàn cao của đường truyền hiện nay thì chi phí việc phát lại đó chỉ chiếm một tỷ lệ nhỏ nếu so với khối lượng tính toán được giảm đi tại các nút nên mạng Frame Relay tiết kiệm được tài nguyên của mạng hơn so với mạng X25.

Frame relay không chỉ là một kỹ thuật mà còn là thể hiện một phương pháp tổ chức mới. Với nguyên lý là truyền mạch gói nhưng các thao tác kiểm soát giữa các đầu cuối giảm đáng kể Kỹ thuật Frame Relay cho phép thông lượng tối đa đạt tới 2Mbps và hiện nay nó đang cung cấp các giải pháp để tương nối các mạng cục bộ LAả  trong một kiến trúc xương sống tạo nên môi trường cho ứng dụng multimedia.

### 3. Mạng ATM (Cell relay)

Hiện nay kỹ thuật Cell Relay dựa trên phương thức truyền thông không đồng bộ (ATM) có thể cho phép thông lương hàng trăm Mbps. Đơn vị dữ liệu dùng trong ATM được gọi là tế bào (cell). các tế bào trong ATM có độ dài cố định là 53 bytes, trong đó 5 bytes dành cho phần chứa thông tin điều khiển (cell header) và 48 bytes chứa dữ liệu của tầng trên.

Trong kỹ thuật ATM, các tế bào chứa các kiểu dữ liệu khác nhau được ghép kênh tới một đường dẫn chung được gọi là đường dẫn ảo (virtual path). Trong đường dẫn ảo đó có thể gồm nhiều kênh ảo (virtual chanell) khác nhau, mỗi kênh ảo được sử dụng bởi một ứng dung nào đó tại một thời điểm.

ATM đã kết hợp những đặc tính tốt nhất của dạng chuyển mạch liên tục và dạng chuyển mạch gói, nó có thể kết hợp dải thông linh hoạt và khả năng chuyển tiếp cao tốc và có khả năng quản lý đồng thời dữ liệu số, tiếng nói, hình ảnh và multimedia tương tác.

Mục tiêu của kỹ thuật ATM là nhằm cung cấp một mạng dồn kênh, và chuyển mạch tốc độ cao, độ trễ nhỏ dáp ứng cho các dạng truyền thông đa phương tiện (multimecdia)

Chuyển mạch cell cần thiết cho việc cung cấp các kết nối đòi hỏi băng thông cao, tình trạng tắt nghẽn thấp, hổ trợ cho lớp dịch vụ tích hợp lưu thông dữ liệu âm thanh hình ảnh. Đặc tính tốc độ cao là đặc tính nổi bật nhất của ATM.

ATM sử dụng cơ cấu chuyển mạch đặc biệt: ma trận nhị phân các thành tố chuyển mạch (a matrix of binary switching elements) để vận hành lưu thông. Khả năng vô hướng (scalability) là một đặc tính của cơ cấu chuyển mạch ATM. Đặc tính này tương phản trực tiếp với những gì diễn ra khi các trạm cuối được thêm vào một thiết bị liên mạng như router. Các router có năng suất tổng cố định được chia cho các trạm cuối có kết nối với chúng. Khi số lượng trạm cuối gia tăng, năng suất của router tương thích cho trạm cuối thu nhỏ lại. Khi cơ cấu ATM mở rộng, mỗi thiết bị thu trạm cuối, bằng con đường của chính nó đi qua bộ chuyển mạch bằng cách cho mỗi trạm cuối băng thông chỉ định. Băng thông rộng được chỉ định của ATM với đặc tính có thể xác nhận khiến nó trở thành một kỹ thuật tuyệt hảo dùng cho bất kỳ nơi nào trong mạng cục bộ của doanh nghiệp.

ả hư tên gọi của nó chỉ rõ, kỹ thuật ATM sử dụng phương pháp truyền không đồng bộ (asynchronouns) các tề bào từ nguồn tới đích của chúng. Trong khi đó, ở tầng vật lý người ta có thể sử dụng các kỹ thuật truyền thông đồng bộ như SDH (hoặc SOả ET).

ả hận thức được vị trí chưa thể thay thế được (ít nhất cho đến những năm đầu của thế kỷ 21) của kỹ thuật ATM, hầu hết các hãng khổng lồ về máy tính và truyền thông như IBM, ATT, Digital, Hewlett - Packard, Cisco Systems, Cabletron, Bay ả etwork,... đều đang quan tâm đặc biệt đến dòng sản phẩm hướng đến ATM của mình để tung ra thị trường. Có thể kể ra đây một số sản phẩm đó như DEC 900 Multiwitch, IBM 8250 hub, Cisco 7000 rounter, Cablectron, ATM module for MMAC hub.

ả hìn chung thị trường ATM sôi động do nhu cầu thực sự của các ứng dụng đa phương tiện. Sự nhập cuộc ngày một đông của các hãng sản xuất đã làm giảm đáng kể giá bán của các sản phẩm loại này, từ đó càng mở rộng thêm thị trường. ả gay ở Việt ả am, các dự án lớn về mạng tin học đều đã được thiết kế với hạ tầng chấp nhận được với công nghệ ATM trong tương lai.

www.viet-ebook.co.cc

**Chương 9**

# Ví dụ một số mạng LAN và WAN

Hiện nay trên thế giới có rất nhiều mạng máy tính, chúng được sử dụng để phục vụ cho nhiều lĩnh vực khác nhau như nghiên cứu khoa học, truyền dữ liệu, kinh doanh. Vì vậy nên các mạng này cũng rất đa dạng về chủng loại. Trong phần này ta xem xét một số mạng LAả và WAả thông dụng.

## I. Mạng Novell NetWare

Được đưa ra bởi hãng ả ovell từ những năm 80 và đã được sử dụng nhiều trong các mạng cục bộ với số lượng ước tính hiện nay vào khoảng 50 -60%. Hệ điều hành mạng ả ovell ả etWare là một hệ điều hành có độ an toàn cao đặc biệt là với các mạng có nhiều người sử dụng. Hệ điều hành mạng ả etware khá phức tạp để lắp đặt và quản lý nhưng nó là một hệ điều hành mạng đang được dùng phổ biến nhất hiện nay. Hệ điều hành mạng ả ovell ả etWare được thiết kế như một hệ thống mạng *client-server* trong đó các máy tính được chia thành hai loại:

- ả hững máy têêính cung cấp tài nguyên cho mạng gọi là *server* hay còn gọi là máy chủ mạng.
- Máy sử dụng tài nguyên mạng gọi là *clients* hay còn gọi là trạm làm việc.

Các server (File server) của ả etware không chạy DOS mà bản thân ả etware là một hệ điều hành cho server điều đó đã giải phóng ả etware ra khỏi những hạn chế của DOS. Server của ả etware dùng một cấu trúc hiệu quả hơn DOS để tổ chức các tập tin và thư mục, với ả etware, chúng ta có thể chia mỗi ổ đĩa thành một hoặc nhiều tập đĩa (volumes), tương tự như các ổ đĩa logic của DOS. Các tập đĩa của ả ovell có tên chứ không phải là chữ cái. Tuy nhiên, để truy cập một tập đĩa của ả etware từ một trạm làm việc chạy DOS, một chữ cái được gán cho tập đĩa.

Với các hệ điều hành ả etware 3.x và 4.x các server phải được dành riêng, trong đó chúng ta không thể dùng một file server làm thêm việc cùa Workstation, tuy điều đó tốn kém hơn vì phải mua một máy tính để làm server nhưng nó có hiệu quả hơn vì máy tính server có thể tập trung để phục vụ mạng. Còn với ả etware 2.x thì có thể lưa chọn trong đó một file server có thể làm việc như một Workstation như hai tiến trình Server và Workstation tách tời nhau hoàn toàn.

Các trạm làm việc trên một mạng ả etware có thể là các máy tính DOS, chạy OS/2 hoặc các máy Macintosh. ả ếu mạng vừa có máy PC và Macintosh thì ả etware có thể là sự lựa chọn tốt.

Tất cả các phiên bản của ả etware đều có đặc trưng được gọi là tính chịu đựng sai hỏng của hệ (System Fault Tolerance SFT) được thiết kế để giữ cho mạng vẫn chạy ngay cả khi phần cứng có sai hỏng.

ả etWare là một hệ điều hành nhưng không phải là một hệ điều hành đa năng mà tập trung chủ yếu cho các ứng dụng truy xuất tài nguyên trên mạng, nó có một tập hợp xác định saün

các dịch vụ dành cho người sử dụng. Tại đây ả ovell ả etWare có một hệ thống các yêu cầu và trả lời mà Client và Server đều hiểu, nó bao gồm:

- ả hóm chương trình trên máy người dùng: Hệ điều hành trạm, các giao diện cho phép nhười sử dụng chi xuất các tài nguyên của mạng như là các tài nguyên của máy cục bộ, chương trình truyền số liệu qua mạng.
- Hệ điều hành trên máy máy chủ: Chương trình thực hiên từ DOS, Lưu các thông số của DOS, chuyển CPU của server qua chế độ protectied mode, quản lý việc sử dụng tài nguyên của mạng cho người sử dụng.
- Các tiện ích trên mạng: dành cho người sử dụng và người quản trị mạng.
- ả ovell ả etWare hỗ trợ các giao thức cơ bản sau:
- Giao thức truy xuất (Access Protocol) (Ethernet, Token Ring, ARCnet, Proả ET-10, FDDI)
- Giao thức trao đổi gói tin trên mạng (Internet Packet Exchange -IPX)
- Giao thức thông tin tìm đường (Routing Information Protocol - RIP)
- Giao thức thông báo dịch vụ (Sevice Advertising Protocol - SAP)
- Giao thức nhân ả etWare (ả etWare Core Protocol - ả CP) cho phép người dùng truy xuất vào file server

Do nhu cầu cần thích nghi với nhiều kiểu mạng và để dễ dàng nâng cấp và quản lý, ả ovell ả etWare cũng được chia thành nhiều tầng giao thức tương tự cấu trúc 7 tầng cuả hệ thống mở OSI.

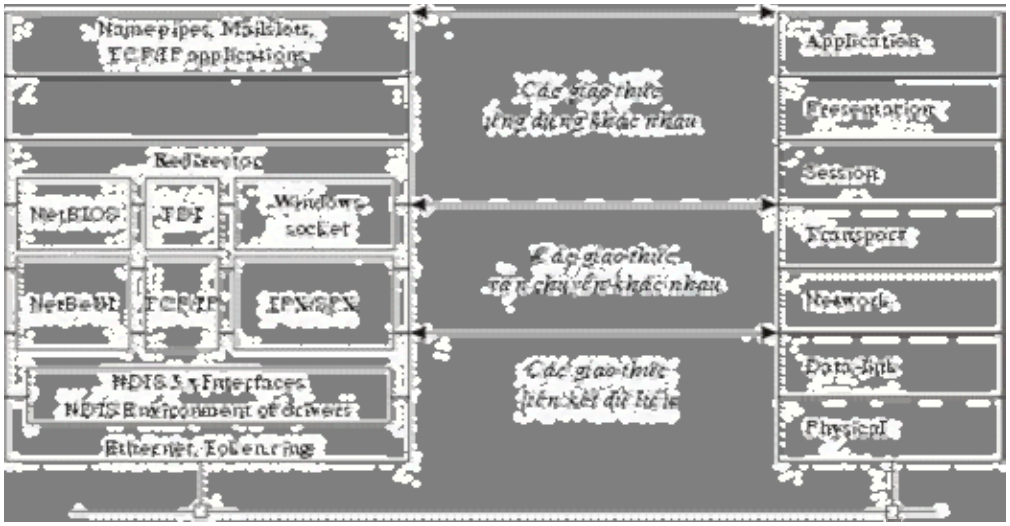
<table>
<tr><td>Tầng ứng dụng<br>(Application)</td><td rowspan="2">Giao thức<br>thông báo dịch vụ<br>(Service advertising<br>protocol - SAP)</td><td rowspan="2">Giao thức thông<br>tin tìm đường<br>(Routing Information<br>Protocol - RIP)</td><td rowspan="2">Giao thức<br>nhân NetWare<br>(NetWare core<br>protocol - NCP)</td></tr>
<tr><td>Tầng trình bày<br>(Presentation)</td></tr>
<tr><td>Tầng giao dịch<br>(Session)</td><td colspan="3">Hệ thống nhập xuất cơ bản trên mạng<br>(NetBIOS)</td></tr>
<tr><td>Tầng vận chuyển<br>(Transport)</td><td colspan="3">Trao đổi gói tin tuần tự<br>(Sequence Packet eXchange - SPX)</td></tr>
<tr><td>Tầng mạng<br>(Network)</td><td colspan="3">Trao đổi gói tin liên mạng<br>(Internet Packet Exchange - IPX)</td></tr>
<tr><td>Tầng liên kết dữ liệu<br>(Data link)</td><td colspan="3">Giao thức truy xuất và kỹ thuật mạng lưới<br>(Access protocol and wiring techniques)<br>(Chuẩn giao tiếp liên kết dữ liệu mở ODI)</td></tr>
<tr><td>Tầng vật lý<br>(Physical)</td><td colspan="3">Ethernet, Token Ring, ARCnet<br>cáp đồng trục, cáp trần xoắn cặp<br>(IEEE 802.X hoặc FDDI)</td></tr>
</table>

*Hình 9.1: Cấu trúc của Hệ điều hành Novell NetWare*

## II. Mạng Windows NT

Mạng dùng hệ điều hành **Windows NT** được đưa ra bởi hãng Microsoft với phiên bản mới nhất hiện nay là Windows ả T 5.0, cụm từ windows ả T được hiểu là công nghệ mạng trong môi trường Windows (Windows ả etwork Technology). Hiện mạng Windows ả T đang được đánh giá cao và được đua vào sử dụng ngày một nhiều. Windows ả T là một hệ điều hành đa nhiệm, đa xử lý với địa chỉ 32 bit bộ nhớ. ả goài việc yểm trơ các ứng dụng DOS, Windows 3.x, Win32 GUI và các ứng dụng dựa trên ký tự, Windows ả T còn bao gồm các thành phần mạng, cơ chế an toàn, các công cụ quản trị có khả năng mạng diện rộng, các phần mềm truy cập từ xa. Windows ả T cho phép kết nối với máy tính lớn, mini và máy Mac.

Hệ điều hành mạng Windows ả T có thể chay trên máy có một CPU cũng như nhiều CPU. Hệ điều hành mạng còn có đưa vào kỹ thuật gương đĩa qua đó sử dụng tốt hệ thống nhiều đĩa nâng cao năng lực hoạt động. Hệ điều hành mạng Windows ả T đảm bảo tránh được những người không được phép vào trong hệ thống hoặc thâm nhập vào các file và chương trình trên đĩa cứng. Hệ điều hành mạng Windows ả T cung cấp các công cụ để thiết lập các lớp quyền dành cho nhiều nhiệm vụ khác nhau làm cho phép xây dựng hệ thống an toàn một cách mềm dẻo. Windows ả T được thiết kế dành cho giải pháp nhóm (Workgroup) khi bạn muốn có kiểm soát nhiều hơn đối với mạng ngang hàng (như Windows For Workgroup, LAả tastic hay ả ovell lite). ả goài ra chức năng mới của Windows ả T server là mô hình vùng (Domain) được thiết lập cho các mạng lớn với khả năng kết nối các mạng toàn xí nghiệp hay liên kết các kết nối mạng với các mạng khác và những công cụ cần thiết để điều hành.




*Hình 9.2: Cấu trúc của Hệ điều hành Windows NT*

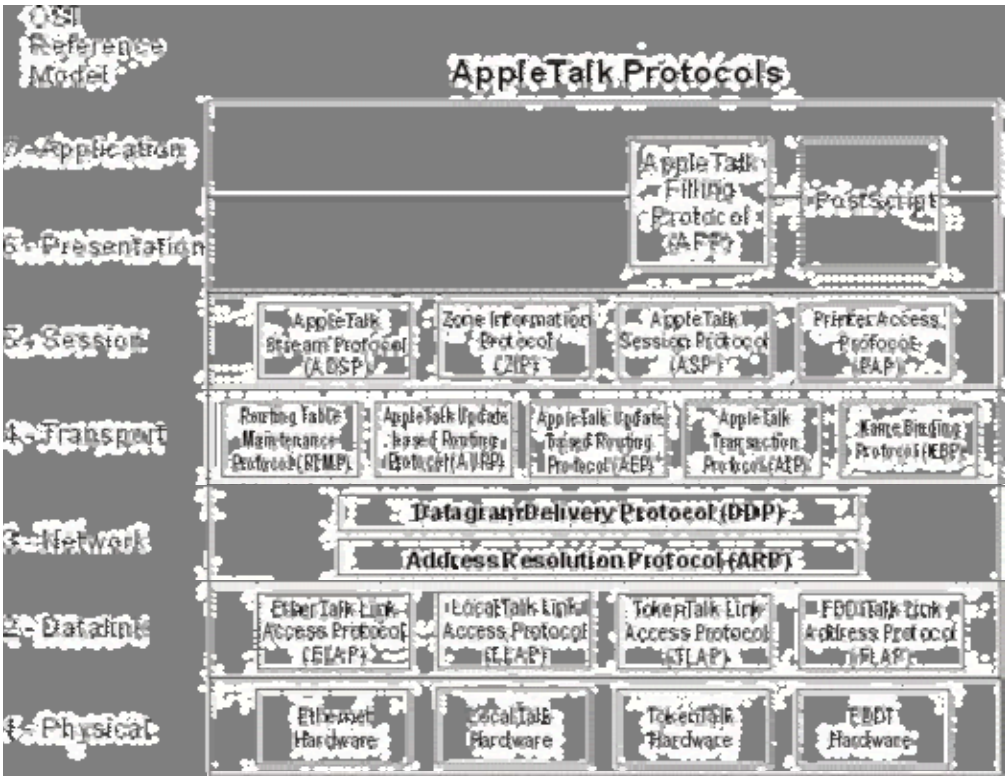
## III. Mạng Apple talk

Vào đầu những năm 1980, khi công ty máy tính Apple chuẩn bị giới thiệu máy tính Macintosh, các kỹ sư Apple đã thấy rằng mạng sẽ trở nên rất cần thiết. Họ muốn rằng mạng MAC cũng là một bước tiến mơi trong cuộc cách mạng về giao diện thân thiện người dùng do Apple khởi xướng. Với ý định như vậy, Apple xây dựng một giao thức mạng cho

họ máy Macintosh, và tích hợp giao thức trên vào máy tính để bàn. Cấu trúc mạng mới do Apple xây dựng được gọi là Apple Talk.

Mặc dù Apple Talk là giao thức mạng độc quyền của Apple, nhưng Apple cũng đã ấn hành nhiều tài liệu về Apple Talk trong cố gắng khuyến khích các nhà sản xuất phần mềm khác phát triển trên Apple Talk. ấ gày nay đã có nhiều sản phẩm thương mại trên nền Apple Talk như của ấ ovell, Microsoft.

Ban đầu **AppleTalk** chỉ cài đặt trên hệ thống cáp riêng của hãng là LocalTalk và có phạm vi ứng dụng rất hạn chế. Phiên bản đầu của Apple Talk được thiết kế cho nhóm người dùng cục bộ hay được gọi là *Apple Talk phase 1*. Sau khi tung ra thị trường 5 năm, số người dùng đã vượt quá 1,5 triệu người cài đặt, Apple nhận thấy những nhóm người dùng lớn đã vượt quá giới hạn của *Apple Talk phase 1*, nên họ đã nâng cấp giao thức. Giao thức đã được cải tiến được biết dưới cái tên *Apple Talk phase 2,* cải tiến khả năng tìm đường của Apple Talk và cho phép Apple Talk chạy trên những mạng lớn hơn.




*Hình 9.3: Cấu trúc của Hệ điều hành Appletalk*

Hãng Apple thiết kế Apple Talk độc lập với tầng liên kết dữ liệu. Apple hỗ trợ nhiều loại cài đặt của tầng liên kết dữ liệu, bao gồm *Ethernet, Token Ring, Fiber Distributed Data Interface* (FDDI), và *Local Talk*. Trên Apple Talk, Apple xem Ethernet như *ethertalk*, Token Ring như *tokentalk*, và FDDI như *fdditalk*.

**Các giao thức chính của mạng AppleTalk:**

- ***LLAP*** *(Local Talk Link Access)* là giao thức do Apple phát triển để hoạt động với cáp riêng của hãng (cũng được gọi là LocalTalk**)** dựa trên cáp xoắn đôi bọc kim

(STP), thích hợp với các mạng nhỏ, hiệu năng thấp. Tốc độ tối đa là 230,4 Kb/s và khoảng cách các đoạn cáp có độ dài giới hạn là 300m, số lượng trạm tối đa là 32.

- ***ELAP*** *(Ethertalk Link Access)* và *TLAP (tokentalk Link Access)* là các giao thức cho phép sử dụng các mạng vật lý tương ứng là Ethernet và Token Ring.

- ***AARP*** *(AppleTalk Addresss Resolution Protocol)* là các giao thức cho phép ánh xạ giữa các địa chỉ vật lý của Ethernet và Token Ring, là giao diện giữa các tầng cao của AppleTalk với các tầng vật lý của Ethernet và Token Ring.

- ***DDP*** *(Datagram Delivery Protocol)* là giao thức tầng Mạng cung cấp dịch vụ theo phương thức không liên kết giữa 2 sockets (để chỉ 1 địa chỉ dịch vụ; một tổ hợp của địa chỉ thiết bị, địa chỉ mạng và socket sẽ định danh 1 cách duy nhất cho môãi tiến trình). DDP thực hiện chức năng chọn đường (routing) dựa trên các bảng chọn đường cho RTMP bảo trì.

- ***RTMP*** *(Routing Table Maintenance protocol)* cung cấp cho DDP thông tin chọn đường trên phương pháp vector khoảng cách tương tự như RIP (Routing Information Protocol) dùng trong ả etware IPX/SPX.

- ***NBP*** *(Naming Binding Protocol)*: cho phép định danh các thiết bị bởi các tên lôgic (ngoài địa chỉ của chúng). Các tên này ẩn dấu địa chỉ tầng thấp đối với người sử dụng và đối với các tầng cao hơn.

- ***ATP*** *(AppleTalk Transaction Protocol)* là giao thức thức tầng vận chuyển hoạt động với phương thức không liên kết. Dich vụ vận chuyển này được cung cấp thông qua một hệ thống các thông báo nhận và truyền lại. Độ tin cậy cũa ATP dựa trên các thao tác (transaction) (một thao tác bao gồm một cặp các thao tác hỏi-đáp).

- ***ASP*** *(AppleTalk Section Protocol)* là giao thức tầng giao dịch của AppleTalk, cho phép thiết lập, duy trì và hủy bỏ các phiên liên lạc giữa người yêu cầu dịch vụ và người cung cấp dịch vụ.

- ***ADSP*** *(AppleTalk Data Stream Protocol)* là một giao thức phủ cả tầng vận chuyển và tầng giao dịch, có thể thay cho nhóm giao thức dùng với ATP.

- ***ZIP*** *(Zone Information Protocol)* là giao thức có chức năng tổ chức các thiết bị thành các vùng (zone) để làm giảm độ phức tạp của 1 mạng bằng cách giới hạn sự tương tác của người sử dụng vào đúng các thiết bị mà anh ta cần.

- ***PAP*** *(Printer Access protocol)* cũng là 1 giao thức của tầng giao dịch tương tự như ASP. ả ó không chỉ cung cấp các dịch vụ in như tên gọi mà còn yểm trợ các kiểu liên kết giữa người yêu cầu và người cung cấp dịch vụ.

- ***AFP*** *(AppleTalk Filling Protocol)* là giao thức cung cấp dịch vụ File và đảm nhận việc chuyển đổi cú pháp dữ liệu, bảo vệ an toàn dữ liệu (tương tự tầng trình bày trong mô hình OSI).

**IV. Mạng Arpanet**

Đây là mạng được thiết lập tại Mỹ vào giữa những năm 60 khi bộ quốc phòng Mỹ muốn có một mạng dùng để ra lệnh và kiểm soát mà có khả năng sống còn cao trong trường hợp có chiến tranh hạt nhân. ấ hững mạng sử dụng đường điện thoại thông thường vào lúc đó tỏ ra không đủ an toàn khi mà một đường dây hay một tổng đài bị phá hủy cũng có thể dẫn đến mọi cuộc nói chuyện hay liên lạc thông qua nó bị gián đoạn, việc đó còn đôi khi dẫn đến cắt rời liên lạc.

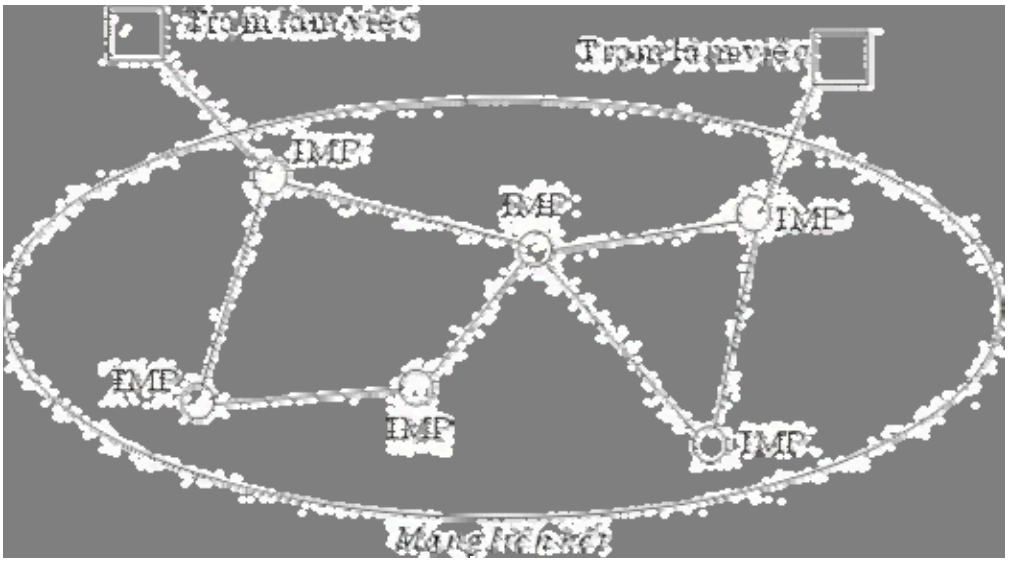
Để làm được điều này khi bộ quốc phòng Mỹ đưa ra chương trình ARPA (Advanced Research Projects Agency) với sự tham gia của nhiều trường đại học và công ty dưới sự quản lý của khi bộ quốc phòng Mỹ.

Vào đầu những năm 1960 những ý tưởng chủ yếu của chuyển mạch gói đã được Paul Baran công bố và sau khi tham khảo nhiều chuyên gia thì chương trình ARPA quyết định mạng tương lai của khi bộ quốc phòng Mỹ sẽ là mạng chuyển mạch gói và nó bao gồm một mạng liên kết và các trạm (host). Mạng liên kết bao gồm các máy tính dùng để liên kết các đường truyền dữ liệu được gọi là các điểm trung chuyển thôâng tin (IMP - Interface Message Processor).

Một IMP sẽ được liên kết với ít nhất là hai IMP khác với độ an toàn cao, các thông tin được chuyển trên mạng liên kết dưới dạng các gói dữ liệu tách rời, có nghĩa là khi có một số đường và nút bị phá hủy thì các gói tin tự động được chuyển theo những đường khác. Mỗi nút một máy tính của hệ thống bao gồm một trạm có được kết nối với một IMP trên mạng, nó gửi thông tin của mình đến IMP để rồi sau đó IMP sẽ phân gói, rồi lần lượt gửi các gói tin theo những đường mà nó lựa chọn để đến đích.

Tháng 10 năm 1968 ARPA quyết định lựa chọn hãng BBẩ một hãng tư vấn tại Cambridge, Massachsetts làm tổng thầu. Lúc đó BBẩ đã lựa chon máy DDP-316 làm IMP, các IMP được nối với đường thuê bao 56 Kbps từ các công ty điện thoại. Phần mềm được chia làm hai phần: phần liên kết mạng và phần cho nút, với phần mềm cho liên kết mạng bao gồm phần mềm tại các IMP đầu cuối và các IMP trung gian, các giao thức liên kết IMP với khả năng đảm bảo an toàn cao.

Phần mềm tại nút bao gồm phần mềm danh cho việc liên kết giữa nút với IMP, các giao thức giữa các nút với nhau trong quá trình truyền dữ liệu.



*Hình 9.4: Cấu trúc ban đầu của mạng ARPANET*

Vào tháng 10 năm 1969 mạng ARPAả ET bắt đầu được đưa vào hoạt động thử nghiệm với 4 nút là những trường đại học và trung tâm nghiên cứu tham gia chính vào dự án, mạng phát triển rất nhanh đến tháng 3 năm 1971 đã có 15 nút và tháng 9 năm 1972 đã có tới 35 nút. Các cải tiến tiếp theo cho phép nhiều trạm có thể liên kết với một IMP do vậy sẽ tiết kiệm tài nguyên và một trạm có thể liên kết với nhiều IMP nhằm tránh việc IMP hư hỏng làm gián đoạn liên lạc.

Cùng với việc phát triển các nút ARPA cũng dành ngân khoản cho phát triển các mạng truyền dữ liệu dùng kỹ thuật vệ tinh và dùng kỹ thuật radio. Điều đó cho phép thiết lập các nút tại những điểm các khoảng cách rất xa. Về các giao thức truyền thông thì sau khi thấy rằng các giao thức của mình không chạy được trên nhiều liên kết mạng vào năm 1974 ARPA đã đầu tư nghiên cứu hệ giao thức TCP/IP và dựa trên hợp đồng giữa BBả và Trường đại học tổng hợp Berkeley - California các nhà nghiên cứu của trường đại học đã viết rất nhiều phần mềm, chương trình quản trị trên cơ ở hệ điều hành Uả IX. Dựa trên các phần mềm mới về truyền thông trên cơ sở TCP/IP đã cho phép dễ dành liên kết các mạng LAả vào mạng ARPAả ET. Vào năm 1983 khi mạng đã hoạt động ổn định thì phần quốc phòng của mạng (gồm khoảng 160 IMP với 110 IMP tại nước Mỹ và 50 IMP ở nước ngoài, hàng trăm nút) được tách ra thành mạng MILả ETvà phần còn lại vẫn tiếp tục hoạt động như là một mạng nghiên cứu.

Trong những năm 1980 khi có nhiều mạng LAả được nối vào ARPAả ET để giảm việc tìm kiếm địa chỉ trên mạng người ta chia vùng các máy tính đưa tên các máy vào địa chỉ IP và xây dựng hệ quản trị cơ sở phân tán các tên các trạm của mạng Hệ cơ sở dữ liệu đó gọi là Dả S (Domain ả aming System) trong đó có chức mọi thông tin liên quan đến tên các trạm.

Vào năm 1990 với sự phát triển của nhiều mạng khác mà ARPAả ET là khởi xướng thì ARPAả ET đã kết thúc hoạt động của mình, tuy nhiên MILả ET vẫn hoạt động cho đến ngày nay.

## V. Mạng NFSNET

Vào cuối những năm 1970 khi Quỹ khoa học quốc gia Hoa kỳ (ả FS - The U.S. ả ational Science Foundation) thấy được sự thu hút của ARPAả ET trong nghiên cứu khoa học mà qua đó các nhà khoa học có thể chia sẻ thông tin hay cùng nhau nghiên cứu các đề án. Tuy nhiên việc sử dụng ARPAả ET cần thông qua bộ quốc phòng Mỹ với nhiều hạn chế và nhiều cơ sở nghiên cứu khoa học không có khả năng đó. Điều đó khiến ả FS thiết lập một mạng ảo có tên là CSả ET trong đó sử dụng các máy tính tại công ty BBả cho phép các nhà nghiên cứu có thể kết nối vào để tiếp tục nối với mạng ARPAả ET hay gửi thư điện tử cho nhau. Vào năm 1984 ả FS bắt đầu nghiên cứu tới việc thiết lập một mạng tốc độ cao dành cho các nhóm nghiên cứu khoa học nhằm thay thế mạng ARPAả ET, bước đầu ả FS quyết định xây dựng được đường trục truyền số liệu nối 6 máy tính lớn (Supercomputer) tại 6 trung tâm máy tính. Tại mỗi trung tâm máy tính lớn tại đây được nối với một máy mini loại LSI-11 và các máy mini được nối với nhau bằng đường thuê bao 56 Kbps tương tự như kỹ thuật đã sử dụng ở mạng ARPAả ET. Đồng thời ả FS cũng cung cấp ngân khoản cho khoảng 20 mạng vùng để liên kết với các máy tính lớn trên và qua đó tới các máy tính lớn khác. Toàn bộ mạng bao gồm mạng trục và các mạng vùng được gọi là ả FSả ET, mạng ả FS có được kết nối với mạng ARPAả ET.

Mạng ả FS được phát triển rất nhanh, sau một thời gian hoạt động đường trục chính được thay thế bằng đường cáp quang 448 Kbps và các máy IBM RS6000 được sử dụng làm công việc kết nối. Đến năm 1990 đường trục đã được nâng lên đến 1.5 Mbps.

Với việc phát triển rất nhanh và ả FS thấy rằng chính quyền không có khả năng tiếp tục tài trợ nhưng do các công ty kinh doanh không thể sử dụng mạng ả FSả ET (do bin cấm theo luật) nên ả FS yểm trợ các công ty MERIT, MCI, IBM thành lập một công ty không sinh lợi (nonprofit corporation) có tên là Aả S (Advanced ả etworks and Services) nhằm phát triển việc kinh doanh hóa mạng. ASả  tiếp nhận mạng ả FSả ET và bắt đầu nâng cấp đường trục lên từ 1.5 Mbps lên 45 Mbps để thành lập mạng Aả Sả ET.

Vào năm 1995 khi các công ty cung cấp dịch vụ liên kết phát triển khắp nơi thì mạng trục Aả Sả ET không còn cần thiết nữa và Aả Sả ET được bán cho công ty America Online. Hiện nay các mạng vùng của ả FS mua các dịch vụ truyền dữ liệu để liên kết với nhau, mạng ả FS đang sử dụng dịch vụ của 4 mạng truyền dữ liệu là PacBell, Ameritech, MFS, Sprint mà qua đó các mạng vùng ả FS có thể lựa chọn để kết nối với nhau.

**VI. Mạng Internet**

Cùng với sự phát triển của ả FSả ET và ARPAả ET nhất là khi giao thức TCP/IP đã trở thành giao thức chính thước duy nhất trên các mạng trên thì số lượng các mạng, nút muốn tham gia kết nối vào hai mạng trên đã tăng lên rất nhanh. Rất nhiều các mạng vùng được kết nối với nhau và còn liên kết với các mạng ở Canada, châu Aâu.

Vào khoảng giữa những năm 1980 người ta bắt đầu thấy được sự hình thành của một hệ thống liên mạng lớn mà sau này được gọi là Internet. Sự phát triển của Internet được tính theo cấp số nhân, nếu như năm 1990 có khoảng 200.000 máy tính với 3.000 mạng con thì năm 1992 đã có khoảng 1.000.000 máy tính được kết nối, đến năm 1995 đã có hàng trăm mạng cấp vùng, chục ngàn mạng con và nhiều triệu máy tính. Rất nhiều mạng lớn đang hoạt động cũng đã được kết nối vào Internet như các mạng SPAả , ả ASA network, HEPả ET, BITả ET, IBM network, EARả . Việc liên kết các mạng được thực hiện thông qua rất nhiều đường nối có tốc độ rất cao.

Hiện nay một máy tính được gọi là thành viên của Internet nếu máy tính đó có giao thức truyền dữ liệu TCP/IP, có một địa chỉ IP trên mạng và nó có thể gửi các gói tin IP đến tất cả các máy tính khác trên mạng Internet.

Tuy nhiên trong nhiều trường hợp thông qua một nhà cung cấp dịch vụ Internet người sử dụng kết nối máy của mình với máy chủ của nhà phục vụ và được cung cấp một địa chỉ tạm thời trước khi khai thác các tài nguyên của Internet. Máy tính của người đó có thể gửi các gói tin cho các máy khác bằng địa chỉ tạm thời đó và địa chỉ đó sẽ trả lại cho nhà cung cấp khi kết thúc liên lạc. Vì máy tính của người đó sử dụng trong thời gian liên kết với Internet cũng có một địa chỉ IP nên người ta vẫn coi máy tính đó là thành viên của Internet.

Vào năm 1992 cộng đồng Internet đã ra đời nhằm thúc đẩy sự phát triển của Internet và điều hành nó. Hiện nay Internet có 5 dịch vụ chính:

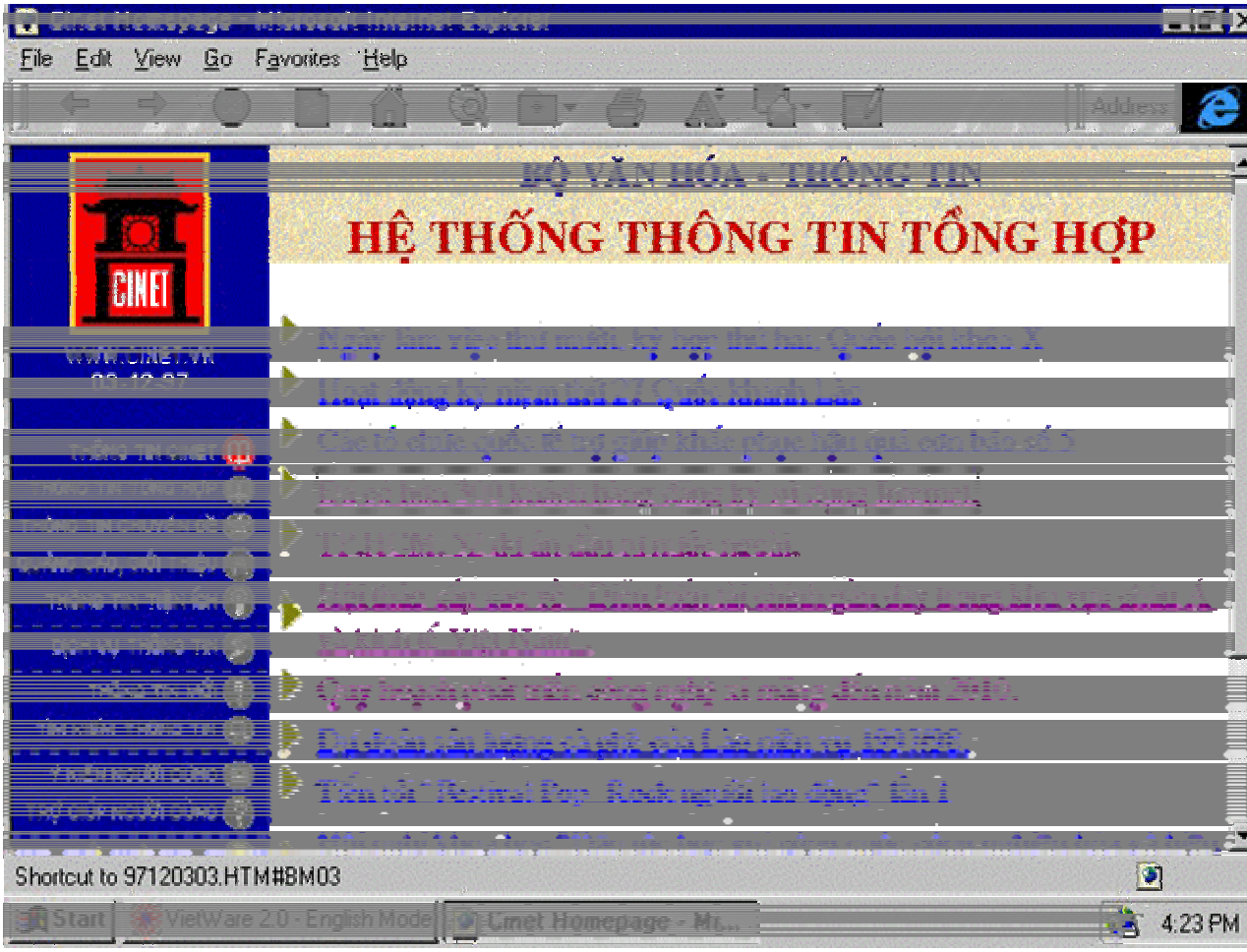
- **Thư điện tử** (Email): đây là dịch vụ đã có từ khi mạng ARPAả ET mới được thiết lập, nó cho phép gửi và nhận thư điến tử cho mọi thành viên khác trong mạng.

- **Thông tin mới** (ả ews): Các vân đề thời sự được chuyển thành các diễn đàn cho phép mọi người quan tâm có thể trao đổi các thông tin cho nhau, hiện nay hiện nay có hàng nghìn diễ đàn về mọi mặt trên Internet.

- **Đăng nhập từ xa** (Remote Login): Bằng các chương trình như Telnet, Rlogin người sử dụng có thể từ một trạm của Internet đăng nhập (logon) vào một trạm khác nếu như người đó được đăng ký trên máy tính kia.

- **Chuyển file** (File transfer): Bằng chương trình FTP người sử dụng có thể chép các file từ một máy tính trên mạng Internet tới một máy tính khác. ả gười ta có thể chép nhiều phần mềm, cơ sở dữ liệu, bài báo bằng cách trên.

- **Dịch vụ WWW** (World Wide Web): WWW là một dịch vụ đặc biệt cung cấp thông tin từ xa trên mạng Internet. Các tập tin siêu văn bản được lưu trữ trên máy chủ sẽ cung cấp các thông tin và dẫn đường trên mạng cho phép người sử dụng dễ dàng Truy cập các tập tin văn bản, đồ họa, âm thanh.




*Hình 9.5: Ví dụ một trang Web cho phép dễ dàng khai thác các trang Web khác*

ả gười sử dụng nhận được thông tin dưới dạng các trang văn bản, một trang là một đơn thể nằm trong máy chu. Đây là dịch vụ đang mang lại sức thu hút to lớn cho mạng Internet, chúng ta có thể xây dựng các trang Web bằng ngôn ngữ HTML (Hypertext Markup Language) với nhiều dạng phong phú như văn bản, hình vẽ, video, tiếng nói và có thể có

các kết nối với các trang Web khác. Khi các trang đó được đặt trên các máy chủ Web thì thông qua Internet người ta có thể xem được sự thể hiện của các trang Web trên và có thể xem các trang web khác mà nó chỉ đến.

Các phần mềm thông dụng được sử dụng hiện nay để xây dựng và duyệt các trang Web là Mosaic, ả avigator của ả etscape, Internet Explorer của Microsoft, Web Access của ả ovell.

www.viet-ebook.co.cc

**Chương 10 :**

# Giới thiệu về hệ điều hành mạng Windows NT

## I. Thế nào là một hệ điều hành mạng

Với việc ghép nối các máy tính thành mạng thì cần thiết phải có một hệ thống phần mềm có chức năng quản lý tài nguyên, tính toán và xử lý truy nhập một cách thống nhất trên mạng, hệ như vậy được gọi là hệ điều hành mạng. Mỗi tài nguyên của mạng như tệp, đĩa, thiết bị ngoại vi được quản lý bởi một tiến trình nhất định và hệ điều hành mạng điều khiển sự tương tác giữa các tiến trình và truy cập tới các tiến trình đó.

Căn cứ vào việc truy nhập tài nguyên trên mạng người ta chia các thực thể trong mạng thành hai loại chủ và khách, trong đó máy khách (Client) truy nhập được vào tài nguyên của mạng nhưng không chia sẻ tài nguyên của nó với mạng, còn máy chủ (Server) là máy tính nằm trên mạng và chia sẻ tài nguyên của nó với các người dùng mạng.

Hiện nay các hệ điều hành mạng thường được chia làm hai loại là hệ điều hành mạng ngang hàng (Peer-to-peer) và hệ điều hành mạng phân biệt (client/server).

Với hệ điều hành mạng ngang hàng mỗi máy tính trên mạng có thể vừa đóng vai trò chủ lẫn khách tức là chúng vừa có thể sử dụng tài nguyên của mạng lẫn chia sẻ tài nguyên của nó cho mạng, ví dụ: LAå tastic của Artisoft, å etWare lite của å ovell, Windows (for Workgroup, 95, å T Client) của Microsoft.

Với hệ điều hành mạng phân biệt các máy tính được phân biệt chủ và khách, trong đó máy chủ mạng (Server) giữ vai trò chủ và các máy cho người sử dụng giữ vai trò khách (các trạm). Khi có nhu cầu truy nhập tài nguyên trên mạng các trạm tạo ra các yêu cầu và gửi chúng tới máy chủ sau đó máy chủ thực hiện và gửi trả lời. Ví dụ các hệ điều hành mạng phân biệt: å ovell å etware, LAå  Manager của Microsoft, Windows å T Server của Microsoft, LAå  Server của IBM, Vines của Banyan System với server dùng hệ điều hành Unix.

## II. Hệ điều hành mạng Windows NT

Windows å T là hệ điều hành mạng cao cấp của hãng Microsoft. Phiên bản đầu có tên là Windows å T 3.1 phát hành năm 1993, và phiên bản server là Windows å T Advanced Server (trước đó là LAå  Manager for å T). å ăm 1994 phiên bản Windows å T Server và Windows å T Workstation version 3.5 được phát hành. Tiếp theo đó ra đời các bản version 3.51. Các phiên bản workstation có sử dụng để thành lập mạng ngang hàng; còn các bản server dành cho quản lý file tập trung, in ấn và chia sẻ các ứng dụng.

å ăm 1995, Windows å T Workstation và Windows å T Server version 4.0 ra đời đã kết hợp shell của người anh em Windows 95 nổi tiếng phát hành trước đó không lâu (trước đây shell của Windows å T giống shell của Windows 3.1) đã kết hợp được giao diện quen thuộc, dễ sử dụng của Windows 95 và sự mạnh mẽ, an toàn, bảo mật cao của Windows å T.

Windows å T có hai bản mà nó đi đôi với hai cách tiếp cận mạng khác nhau. Hai bản này gọi là Windows å T Workstation và Windows å T server. Với hệ điều hành chuẩn của å T ta có thể xây dựng mạng ngang hàng, máy chủ mạng và mọi công cụ quản trị cần thiết cho

một máy chủ mạng ngoài ra còn có thể có nhiều giải pháp về xây dựng mạng diện rộng. Cả hai bản Windows ả T station và Windows ả T server cùng được xây dựng trên cơ sở nhân ả T chung và các giao diện và cả hai cùng có những đặc trưng an toàn theo tiêu chuẩn C2. Windows ả T Wordstation được sử dụng để kết nối những nhóm người sử dụng nhỏ, thường cùng làm việc trong một văn phòng. Tuy nhiên với Windows ả T server ta có được một khả năng chống hỏng hóc cao, những khả năng cung cấp dịch vụ mạng lớn và những lựa chon kết nối khác nhau, Windows ả T Server không hạn chế về số người có thể thâm nhập vào mạng.

Với Windows ả T ta cũng có những công cụ quản trị từ xa vào mạng mà có thể thực hiện được việc quản trị từ những máy tính ở xa. ả ó thích hợp với tất cả các sơ đồ mạng BUS, STAR, RIả G và hỗn hợp.

Windows ả T là hệ điều hành có sức mạnh công nghiệp đầu tiên cho số lượng khổng lồ các máy tính IBM compatible. Windows ả T là một hệ điều hành thực sự dành cho người sử dụng, các cơ quan, các công ty xí nghiệp. Windows ả T là một hệ điều hành đa nhiệm, đa xử lý với địa chỉ 32 bit bộ nhớ. ả ó yểm trợ các ứng dụng DOS, Windows, Win32 GUI và các ứng dụng dựa trên ký tự. Windows ả T server là một hệ điều hành mạng hoàn chỉnh, nó nhanh chóng được thừa nhận là một trong những hệ điều hành tốt nhất hiện nay vì:

- Là hệ điều hành mạng đáp ứng tất cả các giao thức truyền thông phổ dụng nhất. ả goài ra nó vừa cho phép giao lưu giữa các máy trong mạng, vừa cho phép truy nhập từ xa, cho phép truyền file v.v... Windows ả T là hệ điều hành vừa đáp ứng cho mạng cục bộ (LAả ) vừa đáp ứng cho mạng diện rộng (WAả ) như Intranet, Internet.

- Windows ả T server hơn hẳn các hệ điều hành khác bởi tính mềm dẻo, đa dạng trong quản lý. ả ó vừa cho phép quản lý mạng theo mô hình mạng phân biệt (Clien/Server), vừa cho phép quản lý theo mô hình mạng ngang hàng (peer to peer).

- Windows ả T server đáp ứng tốt nhất các dịch vụ viễn thông, một dịch vụ được sử dụng rộng rãi trong tương lai.

- Windows ả T server cài đặt đơn giản, nhẹ nhàng và điều quan trọng nhất là nó tương thích với hầu như tất cả các hệ mạng, nó không đòi hỏi người ta phải thay đổi những gì đã có.

- Cho phép dùng các dịch vụ truy cập từ xa (Remote access service - RAS), có khả năng phụp vụ đến 64 cổng truy nhập từ xa (trong đó Lan manager 16 cổng).

- Đáp ứng cho cả các máy trạm Macintosh nối với Windows ả T server.

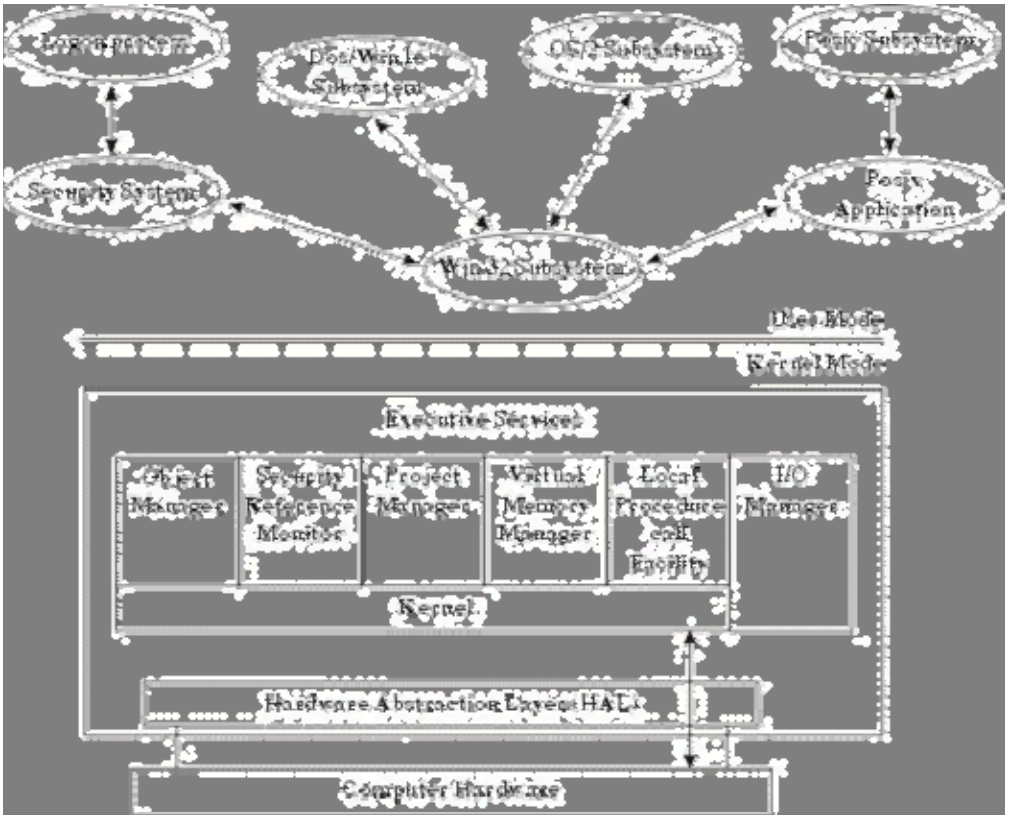
Windows ả T yểm trợ mọi nghi thức mạng chuẩn như ả etBUEI, IPX/SPX, TCP/IP và các nghi thức khác. Windows ả T cũng tương thích với những mạng thông dụng hiên nay như ả ovell ả etWare, Banyan VIả ES, và Microsoft LAả  Manager. Đối với mạng lớn và khả năng thâm nhập từ xa sản phẩm Windows ả T Server cũng cũng cấp các chức năng bổ xung nhu khả năng kết nối với máy tính lớn và máy MAC.

**III. Cấu trúc của hệ điều hành Windows NT**

Windows ả T được thiết kế sử dụng cách tiếp cận theo đơn thể (modular). Các đơn thể khác nhau (còn được gọi là các bộ phận, thành phần) của Windows ả T được trình bày trong hình 1 Các bộ phận của Windows ả T có thể chạy dưới hai chế độ: User (người sử dụng) và Kernel (cốt lõi của hệ điều hành). Khi một thành phần của hệ điều hành chạy dưới cốt lõi của hệ điều hành (Kernel), nó truy cập đầy đủ các chỉ thị máy cho bộ xử lý đó và có thể truy cập tổng quát toàn bộ tài nguyên trên hệ thống máy tính.

Trong Windows ả T: Executive Services, Kernel và HAL chạy dưới chế độ cốt lõi của hệ điều hành.

Hệ thống con (Subsystem) Win 32 và các hệ thống con về môi trường, chẳng hạn như DOS/Win 16.0S/2 và hệ thống con POSIX chạy dưới chế độ user. Bằng cách đặt các hệ thống con này trong chế độ user, các nhà thiết kế Windows ả T có thể hiệu chỉnh chúng dễ dàng hơn mà không cần thay đổi các thành phần được thiết kế để chạy dưới chế độ Kernel.




*Hình 10.1: Cấu trúc Windows NT*

**Các lớp chính của hệ điều hành WINDOWS NT SERVER gồm:**

- ***Lớp phần cứng trừu tượng (Hardware Astraction Layer - HAL):*** Là phần cứng máy tính mà cốt lõi của hệ điều hành (Kernel) có thể đươc ghi vào giao diện phần cứng ảo, thay vì vào phần cứng máy tính thực sự. Phần lớn cốt lõi của hệ điều hành sử dụng HAL để truy cập các tài nguyên máy tính. Điều này có nghĩa là cốt lõi của hệ điều hành và tất cả các thành phần khác phụ thuộc vào cốt lõi có thể dễ dàng xuất (Ported) thông qua Microsoft đến các nền ( Platform ) phần cứng khác. Một thành phân nhỏ trong cốt lõi của hệ điều hành, cũng như bộ quản lý ả hập / Xuất truy cập phần cứng máy tính trực tiếp mà không cần bao gồm HAL.

- ***Lớp Kernel cốt lõi của hệ điều hành):*** Cung cấp các chức năng hệ điều hành cơ bản được sử dụng bởi các thành phần thực thi khác. Thành phần Kernel tương đối nhỏ và cung cấp các thành phần cốt yếu cho những chức năng của hệ điều hành. Kernel chủ yếu chịu trách nhiệm quản lý luồng, quản lý phần cứng và đồng bộ đa sử lý.

- **Các thành phần Executive:** Là các thành phần hệ điều hành ở chế độ Kernel thi hành các dịch vụ như :

  - Quản lý đối tượng (object manager)
  - Bảo mật (security reference monitor)
  - Quản lý tiến trình (process manager)
  - Quản lý bộ nhớ ảo (virtual memory manager)
  - Thủ tục cục bộ gọi tiện ích, và quản trị nhập/xuất (I/O Manager)

## IV.Cơ chế quản lý của Windows NT

### *1. Quản lý đối tượng* (Object Manager):

Tất cả tài nguyên của hệ điều hành được thực thi như các đối tượng. Một đối tượng là một đại diện trừu tượng của một tài nguyên. ả ó mô tả trạng thái bên trong và các tham số của tài nguyên và tập hợp các phương thức (method) có thể được sử dụng để truy cập và điều khiển đối tượng.

Ví dụ một đối tượng tập tin sẽ có một tên tập tin, thông tin trạng thái trên file và danh sách các phương thức, như tạo, mở,đóng và xóa, đối tượng mô tả các thao tác có thể được thực hiện trên đối tượng file.

Bằng cách xử lý toàn bộ tài nguyên như đối tượng Windows ả T có thể thực hiện các phương thức giống nhau như: tạo đối tượng, bảo vệ đối tượng, giám sát việc sử dụng đối tượng (Client object) giám sát những tài nguyên được sử dụng bởi một đối tượng.

Việc quản lý đối tượng (Object Manager) cung cấp một hệ thống đặt tên phân cấp cho tất cả các đối tượng trong hệ thống. Do đó, tên đối tượng tồn tại như một phần của không gian tên toàn cục và được sử dụng để theo dõi việc tạo và sử dụng đối tượng.

Sau đây là một số ví dụ của loại đối tượng Windows ả T :

- Đối tượng Directory (thư mục).
- Đối tượng File (tập tin).
- Đối tượng kiểu object.
- Đối tượng Process (tiến trình).

- Đối tượng thread (luồng).
- Đối tượng Section and segment (mô tả bộ nhớ).
- Đối tượng Port (cổng).
- Đối tượng Semaphore và biến cố.
- Đối tượng liên kết Symbolic (ký hiệu).

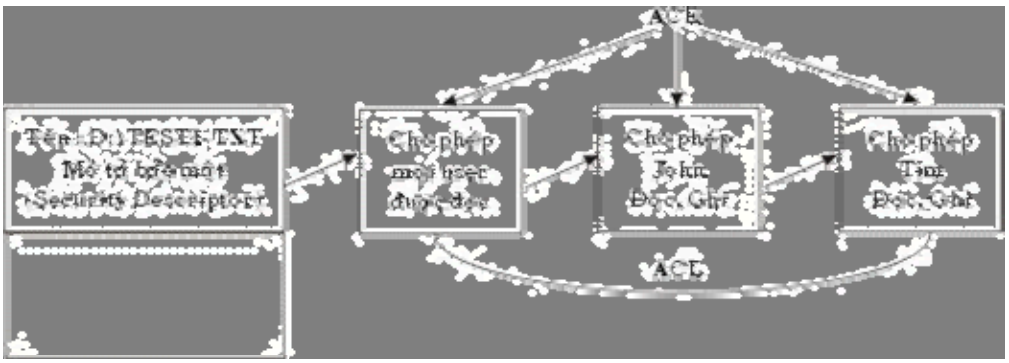
### *2. Cơ chế bảo mật* (SRM - Security Reference Monitor):

Được sử dụng để thực hiện vấn đề an ninh trong hệ thống Windows ả T. Các yêu cầu tạo một đối tượng phải được chuyển qua SRM để quyết định việc truy cập tài nguyên được cho phép hay không. SRM làm việc với hệ thống con bảo mật trong chế độ user. Hệ thống con này được sử dụng để xác nhận user login vào hệ thống Windows ả T.

Để kiểm soát việc truy cập, mỗi đối tượng Windows ả T có một danh sách an toàn (Access Control List - ACL). Danh sách an toàn của mỗi đối tượng gồm những phần tử riêng biệt gọi là Access Control Entry (ACE). Mỗi ACE chứa một SecurityID (SID: số hiệu an toàn) của người sử dụng hoặc nhóm. Một SID là một số bên trong sử dụng với máy tính Windows ả T mô tả một người sử dụng hoặc một nhóm duy nhất giữa các máy tính Windows ả T.

ả goài SID, ACE chứa một danh sách các hành động (action) được cho phép hoặc bị từ chối của một user hoặc một nhóm. Khi người sử dụng đăng nhập vào mạng Windows ả T, sau khi việc nhận dạng thành công, một Security Access Token (SAT) được tạo cho người dùng đó. SAT chứa SID của người dùng và SID của tất cả các nhóm người dùng thuộc mạng Windows ả T. Sau đó SAT hoạt động như một "passcard" (thẻ chuyển) cho phiên làm việc của người dùng đó và được sử dụng để kiểm tra tất cả hoạt động của người dùng.

Khi người dùng tham gia mạng truy cập một đối tượng, Security Reference Monitor kiểm tra bộ mô tả bảo mật của đối tượng xem SID liệt kê trong SAT có phù hợp với giá trị trong ACE không. ả ếu phù hợp, các quyền về an ninh được liệt trong ACE áp dụng cho người dùng đó.



*Hình 10.2: Ví dụ về danh sách an toàn (Access Control List).*

### *3. Quản lý nhập / xuất (I/O Manager) :*

Chịu trách nhiệm cho toàn bộ các chức năng nhập / xuất trong hệ điều hành Windows ả T. I/O Manager liên lạc với trình điều khiển của các thiết bị khác nhau.

**4. I/O *Manager:***

**S**sử dụng một kiến trúc lớp cho các trình điều khiển. Mỗi bộ phận điều khiển trong lớp này thực hiện một chức năng được xác định rõ. Phương pháp tiếp cận này cho phép một thành phần điều khiển được thay thế dễ dàng mà không ảnh hưởng phần còn lại của các bộ phận điều khiển.

*Hình 10.3:Các trình điều khiển thiết bị theo lớp của I / O Manager*

## V. Các cơ chế bảo vệ dữ liệu trong Windows NT

Cơ chế bảo vệ dữ liệu của Windows ả T gọi là fault tolerance, nó cho phép hệ thống khả năng tiếp tục làm việc và bảo toàn dữ liệu của hệ thống trong trường hợp một phần của hệ thống có sự cố hỏng hóc sai lệch. Trong Windows ả T cơ chế fault tolerance bao gồm các biện pháp sau:

- Chống cúp điện bất thường.
- Cung cấp khả năng bảo vệ hệ thống đĩa (fault tolerance disk subsystem).
- Cung cấp khả năng sao chép dự phòng (backup) từ băng từ.

Khả năng bảo vệ hệ thống đĩa của Windows ả T là RAID ø (viết tắt của Redundant Array of Inexpensiredisk). Thực chất RAID là một loạt các biện pháp để bảo vệ hệ thống đĩa. Các biện pháp trong RIAD được chia thành 6 mức sau:

- ***Mức 0*:** Đây là mức ứng với biện pháp chia nhỏ đĩa (disk striping). Thực chất nội dung của biện pháp này là phân chia dữ liệu thành khối và sau đó sắp xếp các khối dữ liệu theo thứ tự trong tất cả các đĩa thành 1 mảng.
- ***Mức 1*:** Mức này ứng với biện pháp disk Mirroring, biện pháp này cho phép tạo ra 2 đĩa giống nhau. ả ếu trong quá trình vận hành mạng một đĩa có sự cố thì hệ thống sử dụng dữ liệu của đĩa kia.
- ***Mức 2*:** Mức này ứng với biện pháp phân chia nhỏ đĩa bằng cách phân chia các file thành các byte và sắp xếp các byte sang nhiều đĩa. Mức này sử dụng mã sửa sai

(error correcting code) trong quá trình phân chia đĩa. ả ói chung biện pháp dùng ở mức này tốt hơn biện pháp dùng trong mức 1.

- ***Mức 3*:** Mức này sử dụng biện pháp giống mức 2. Tuy nhiên mã sửa sai (error correction code) chỉ sử dụng cho một đĩa. Không áp dụng cho nhiều đĩa như ở mức 2. ả gười ta thường dùng mức này để truy nhập vào một số ít file có dung tích lớn.

- ***Mức 4*:** Mức này sử dụng biện pháp giống ở mức 2 và 3 nhưng bằng phương pháp phân chia đĩa thành các khối lớn. Giống như mức 3 tất cả các mã sửa sai (error correction code) được hgi vào một đĩa và tách khỏi khối dữ liệu.

- ***Mức 5*:** Trong mức này người ta sử dụng biện pháp phân chia đĩa thành từng phần gọi là Striping with party. Biện pháp sử dụng ở mức này tương tự như ức 4, số liệu được phân nhỏ thành các khối lớn và sau đó ghi vào tất cả các đĩa. Các thông tin (party Infomation) được coi như các dữ liệu dùng tạm thời (data redundancy).

**Ngoài ra chúng ta còn có thể áp dụng các biện pháp bảo vệ dữ liệu trong Windows NT:**

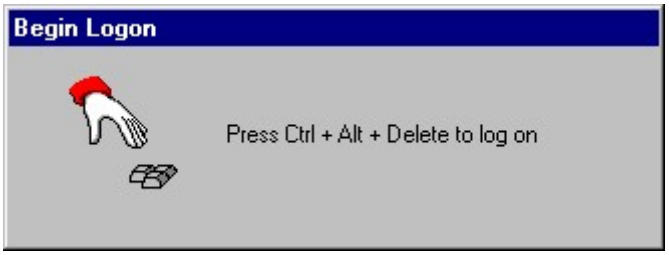
- ***Biện pháp Disk mirroring:*** Disk mirroring là cách sao tạm (redundant) lại đĩa hoặc partition. Biện pháp này bảo vệ dữ liệu tránh các sự cố bằng cách dưa ra chế độ thường xuyên backup đĩa hoặc partition. Hình dưới chỉ ra cách dùng biện pháp Mirroring:

- ***Disk Duplexing:*** Biện pháp dùng đĩa kép (Disk Duplexing) tường tự như disk mirroring chỉ khác là chúng dùng 2 disk controler. Diều này cho thên hả năng bảo vệ khi controler của một đĩa có sự cố. Trong khi đó biện pháp Mirror không thể khắc phục được tình huống này.

- ***Mirror Set:*** Các partition hoặc đĩa trong chế độ Mirror được tạo ra bằng cách lặp sao lại partition hoặc đĩa trên đĩa khác cùng một tên ổ đĩa được gán cho cả 2 partition. Ta có thể dùng establish Mirror trong menu Fault tolerance. ả ếu đĩa hoặc partition trong chế độ Mirror bị lỗi thì chế độ Mirror cần phải ngắt để thực hiện chế độ sao chép dự phòng vào một đĩa riệng. Sau đó sao backup trở lại.

## VI. Giới thiệu về hoạt động của Windows NT Server

Khi chúng ta khởi động Windows ả T Server hộp Begin logon sẽ hiện ra, server chờ đợi để chúng ta bấm Ctrl+Alt +Del để có thể tiếp tục hoạt động. Ở đây có điểm khác với các hệ điều hành DOS, Windows 95 là tổ hợp Ctrl+Alt +Del không phải là khởi động lại máy. Trong trường hợp này Windows ả T loại bỏ mọi chương trình Virus hay không có phép đang hoạt động trước khi bước vào làm việc.



*Hình 10.4: Thông báo gia nhập mạng*

Lúc này chúng ta sẽ thấy hộp Logon Information xuất hiện và yếu cầu chúng ta phải đánh đúng tên và mật khẩu thì mới được đăng nhập vào Server. ả ếu là người dùng mới thì phải được người quản trị khai báo tên và mật khẩu trước khi đăng nhập..

*Hình 10.5: Màn hình gia nhập mạng*

Cũng giống như màn hình nền của hệ điều hành Windows 95 khi muốn thực hiện các trình, gọi các menu hệ thống chúng ta dùng nút Start ở cuối màn hình

*Hình 10.6: Điểm khởi đầu của Windows*

Trước muốn kết thúc chương trình và tắt máy chúng ta phải bấm phím Start rồi chọn ShutDown, màn hình kết thúc sẽ hiện ra cho chúng ta lựa chon công yêu cầu về tắt hay khởi động lại.

*Hình 10.7: Màn hình thoát khỏi Windows*

**Chương 11**

# Hệ thống quản lý của mạng Windows NT

Các mạng máy tính hiện nay được thiết kế rất đa dạng và đang thực hiện những ứng dụng trên nhiều lĩnh vực của đời sống xã hội. Điều đó có nghĩa là các thông tin lưu trữ trên mạng và các thông tin truyền giao trên mạng ngày càng mang nhiều giá trị có ý nghĩa sống còn. Do vậy những người quản trị mạng ngày càng phải quan tâm đến việc bảo vệ các tài nguyên của mình.

Việc bảo vệ an toàn là quá trình bảo vệ mạng khỏi bị xâm nhập hoặc mất mát, khi thiết kế các hệ điều hành mạng người ta phải xây dựng một hệ thống quản lý nhiều tầng và linh hoạt giúp cho người quản trị mạng có thể thực hiện những phương án về quản lý từ đơn giản mức độ thấp cho đến phức tạp mức độ cao trong những mạng có nhiều người tham gia. Thông qua những công cụ quản trị đã được xây dựng saün người quản trị có thể xây dựng những cơ chế về an toàn phù hợp với cơ quan của mình.

Thông thường hệ thống mạng có những mức quản lý chính sau:

- **Mức quản lý việc thâm nhập mạng (Login/Password):** Mức quản lý việc thâm nhập mạng (Login/Password) xác định những ai và lúc nào có thể vào mạng. Đối với người quản trị và người sử dụng mạng, mức an toàn này dường như khá đơn giản mà theo đó mỗi người sử dụng (người sử dụng) có một tên login và mật khẩu duy nhất.

- **Mức quản lý trong việc quản lý sử dụng các tài nguyên của mạng:** Kiểm soát những tài nguyên nào mà người sử dụng được phép truy cập, sử dụng và sử dụng như thế nào.

- **Mức quản lý với thư mục và file:** Mức an toàn của file kiểm soát những file và thư mục nào người sử dụng được dùng trên mạng và được sử dụng ở mức độ nào

- **Mức quản lý việc điều khiển File Server:** Mức an toàn trên máy chủ kiểm soát ai có thể được thực hiện các thao tác trên máy chủ như bật, tắt, chạy các chương trình khác. ả gười ta cần có cơ chế như mật khẩu để bảo vệ.

## I. Quản lý các tài nguyên trong mạng

ả hư chúng ta đã biết, mạng LAả cung cấp các dịch vụ theo hai cách: qua cách chia sẻ tài nguyên theo nguyên tắc ngang hàng và thông qua những máy chủ trung tâm. Dù bất cứ phương pháp nào được sử dụng, vấn đề cần phải giải quyết là là giúp người sử dụng xác định được các tài nguyên có saün ở đâu để có thể sử dụng.

Các kỹ thuật sau đây đã được sử dụng để tổ chức tài nguyên mạng máy tính:

- Quản lý đơn lẻ từng máy chủ (stand-alone services).

- Quản lý theo dịch vụ thư mục (directory services).

- Quản lý theo nhóm (workgroups).

- Quản lý theo domain (domains).

### 1. Quản lý đơn lẻ từng máy chủ (Stand-alone Services)

Với cách quản lý này trong mạng LAå thường chỉ có một vài máy chủ, mỗi máy chủ sẽ quản lý tài nguyên của mình, mỗi người sử dụng muốn thâm nhập những tài nguyên của máy chủ nào thì phải khai báo và chịu sự quản lý của máy chủ đó. Mô hình trên phù hợp với những mạng nhỏ với ít máy chủ và khi có trục trặc trên một máy chủ thì toàn mạng vẫn hoạt động. Cũng vì trong mạng LAå chỉ có ít máy chủ, do đó người sử dụng không mấy khó khăn để tìm các tập tin, máy in và các tài nguyên khác của mạng (plotter, CDRom, modem...).

Việc tổ chức như vậy không cần những dịch vụ quản lý tài nguyên phức tạp. Tuy nhiên khi trong mạng có từ hai máy chủ trở lên vấn đề trở nên phức tạp hơn vì mỗi máy chủ riêng lẻ giữ riêng bảng danh sách các người sử dụng và tài nguyên của mình. Khi đó mỗi người sử dụng phải tạo lập và bảo trì tài khoản của mình ở hai máy chủ khác nhau mới có thể đăng nhập (logon) và truy xuất đến các máy chủ này. å goài ra việc xác định vị trí của các tài nguyên trong mạng cũng rất khó khăn khi mạng có qui mô lớn.

### 2. Quản lý theo dịch vụ thư mục (Directory Services)

Hệ thống các dịch vụ thư mục cho phép làm việc với mạng như là một hệ thống thống nhất, tài nguyên mạng được nhóm lại một cách logic để dễ tìm hơn. Giải pháp này có thể được dùng cho những mạng lớn. Ở đây thay vì phải đăng nhập vào nhiều máy chủ, người sử dụng chỉ cần đăng nhập vào mạng và được các dịch vụ thư mục cấp quyền truy cập đến tài nguyên mạng, cho dù được cung cấp bởi bất kể máy chủ nào.

å gười quản trị mạng chỉ cần thực hiện công việc của mình tại một trạm trên mạng mặc dù các điểm nút của nó có thể nằm trên cả thế giới. Hệ điều hành å etware 4.x cung cấp dịch vụ nổi tiếngï và đầy ưu thế cạnh tranh này với tên gọi ***Netware Directory Services (NDS).***

Giải pháp này thích hợp với những mạng lớn. Các thông tin của å DS được đặt trong một hệ thống cơ sở dữ liệu đồng bộ, rộng khắp được gọi là DIB (Data Information Base). Cơ sở dữ liệu trên quản lý các dữ liệu dưới dạng các đối tượng phân biệt trên toàn mạng. Các định nghĩa đối tượng sẽ được đặt trên các tập tin riêng của một số máy chủ đặc biệt, mỗi đối tượng có các tính chất và giá trị của mỗi tính chất. Đối tượng bao hàm tất cả những gì có tên phân biệt như å gười sử dụng, File server, Print server, group. Mỗi loại đối tượng có những tính chất khác nhau ví dụ như đối tượng å gười sử dụng có tính chất về nhóm mà người sử dụng đó thuộc, còn nhóm có các tính chất về người sử dụng mà nhóm đó chứa.

Việc thiết lập các dịch vụ như vậy cần được lập kế hoạch, thiết kế rất cẩn thận, liên quan đến tất cả các đơn vị phòng ban có liên quan. Loại mạng này có khuyết điểm là việc thiết kế, thiết lập mạng rất phức tạp, mất nhiều thời gian nên không thích hợp cho các mạng nhỏ.

### 3. Quản lý theo nhóm (Workgroup)

Các nhóm làm việc làm việc theo ý tưởng ngược lại với các dịch vụ thư mục. å hóm làm việc dựa trên nguyên tắc mạng ngang hàng (peer-to-peer network), các người sử dụng chia sẻ tài nguyên trên máy tính của mình với những người khác, máy nào cũng vừa là chủ

(server) vừa là khách (client). ả gười sử dụngĩ có thể cho phép các người sử dụng khác sử dụng tập tin, máy in, modem... của mình, và đến lượt mình có thể sử dụng các tài nguyên được các người sử dụng khác chia sẻ trên mạng. Mỗi cá nhân người sử dụng quản lý việc chia sẻ tài nguyên trên máy của mình bằng cách xác định cái gì sẽ được chia sẻ và ai sẽ có quyền truy cập. Mạng này hoạt động đơn giản: sau khi logon vào, người sử dụng có thể duyệt (browse) để tìm các tài nguyên có saün trên mạng.

Workgroup là nhóm logic các máy tính và các tài nguyên của chúng nối với nhau trên mạng mà các máy tính trong cùng một nhóm có thể cung cấp tài nguyên cho nhau. Mỗi máy tính trong một workgroup duy trì chính sách bảo mật và CSDL quản lý tài khoản bảo mật SAM (Security Account Manager) riêng ở mỗi máy. Do đó quản trị workgroup bao gồm việc quản trị CSDL tài khoản bảo mật trên mỗi máy tính một cách riêng lẻ, mang tính cục bộ, phân tán. Điều này rõ ràng rất phiền phức và có thể không thể làm được đối với một mạng rất lớn.

ả hưng workgroup cũng có điểm là đơn giản, tiện lợi và chia sẽ tài nguyên hiệu quả, do đó thích hợp với các mạng nhỏ, gồm các nhóm người sử dụng tương tự nhau.

Tuy nhiên Workgroup dựa trên cơ sở mạng ngang hàng (peer-to-peer), nên có hai trở ngại đối với các mạng lớn như sau:

- Đối với mạng lớn, có quá nhiều tài nguyên có saün trên mạng làm cho các người sử dụng khó xác định chúng để khai thác.

- ả gười sử dụng muốn chia sẻ tài nguyên thường sử dụng một cách dễ hơn để chia sẻ tài nguyên chỉ với một số hạn chế người sử dụng khác.

Điển hình cho loại mạng này là Windws for Workgroups, LAả tastic, LAả  Manager... Window 95, Windows ả T Workstation.

### 4. Quản lý theo vùng (Domain)

Domain mượn ý tưởng từ thư mục và nhóm làm việc. Giống như một workgroup, domain có thể được quản trị bằng hỗn hợp các biện pháp quản lý tập trung và địa phương. Domain là một tập hợp các máy tính dùng chung một nguyên tắc bảo mật và CSDL tài khoản người dùng (người sử dụng account). ả hững tài khoản người dùng và nguyên tắc an toàn có thể được nhìn thấy khi thuộc vào một CSDL chung và được tập trung.

Giống như một thư mục, một domain tổ chức tài nguyên của một vài máy chủ vào một cơ cấu quản trị. ả gười sử dụng được cấp quyền logon vào domain chứ không phải vào từng máy chủ riêng lẻ. ả goài ra, vì domain điều khiển tài nguyên của một số máy chủ, nên việc quản lý các tài khoản của người sử dụng được tập trung và do đó trở nên dễ dàng hơn là phải quản lý một mạng với nhiều máy chủ độc lập.

Các máy chủ trong một domain cung cấp dịch vụ cho các người sử dụng. Một người sử dụng khi logon vào domain thì có thể truy cập đến tất cả tài nguyên thuộc domain mà họ được cấp quyền truy cập. Họ có thể dò tìm (browse) các tài nguyên của domain giống như trong một workgroup, nhưng nó an toàn, bảo mật hơn.

Để xây dựng mạng dựa trên domain, ta phải có ít nhất một máy Windows ả T Server trên mạng. Một máy tính Windows ả T có thể thuộc vào một workgroup hoặc một domain, nhưng không thể đồng thời thuộc cả hai. Mô hình domain được thiết lập cho các mạng lớn với khả năng kết nối các mạng toàn xí nghiệp hay liên kết các kết nối mạng với các mạng khác và những công cụ cần thiết để điều hành.

Việc nhóm những người sử dụng mạng và tài nguyên trên mạng thành domain có lợi ích sau:

- Mã số của người sử dụng được quản lý tập trung ở một nơi trong một cơ sở dữ liệu của máy chủ, do vậy quản lý chặt chẽ hơn.
- Các nguồn tài nguyên cục bộ được nhóm vào trong một domain nên dễ khai thác hơn.

*Quản lý theo Workgroup và domain là hai mô hình mà Windows NT lựa chọn. Sự khác nhau căn bản giữa Workgroup và domain là trong một domain phải có ít nhất một máy chủ (máy chủ) và tài nguyên người sử dụng phải được quản lý bởi máy chủ đó.*

## II. Hệ thống quản lý trên Hệ điều hành mạng Windows NT Server

Windows ả T cung cấp những chức năng tuân theo chuẩn C2 (chuẩn về an toàn quốc tế) trong đó Windows ả T đảm bảo tránh được những người không được phép vào trong hệ thống hoặc thâm nhập vào các file và chương trình trên đĩa cứng. ả gười ta không thể thâm nhập vào được nếu không có mật khẩu đúng. và qua đó đã bảo vệ được các file. Windows ả T cung cấp công cụ để xây dựng các lớp quyền dành cho nhiều nhiệm vụ khác nhau nhằm xây dựng hệ thống an toàn một cách mềm dẻo.

ả hiều người sử dụng có thể có quyền vào một máy chủ Windows ả T. Một tài khoản của người sử dụng trên máy bao gồm tên, mật khẩu và nhiều tính chất được cho bởi người quản trị mạng. ả gười sử dụng có thể che các thư mục hay file của mình từ những người khác và cài đặt các thông số của File manager, Programe Manager, Control Panel một cách phù hợp.

Khi người dùng thâm nhập vào hệ thống thì tự động khởi động mọi thông số đã được lưu trữ từ trước. ả ếu người sử dụng có quyền cao hơn thì họ có thể chia sẻ hoặc ngừng các tài nguyên đang dùng chung trên mạng như máy in hay file hoặc họ có thể thay đổi quyền của những người dùng mạng khác khi thâm nhập vào mạng.

### 1. Mô hình Workgroup (nhóm) của mạng Windows NT

Mỗi người truy cập vào mạng Windows ả T tổ chức theo mô hình Workgroup cần phải đăng ký:

- Tên vào mạng
- Mật khẩu vào mạng

Dựa vào tên và mật khẩu đã cho, Windows ả T cung cấp cho người một số gọi là mã số của người sử dụng (user account). Mã số này được lưu dữ trong cơ sở dữ liệu là hệ thống

quản trị tài nguyên (SAM - Security Account Manager database). Hệ thống quản trị tài nguyên dùng để đảm bảo an toàn về tài nguyên trên mạng. ả gười vào mạng muốn truy nhập vào tài nguyên phải qua sự kiểm duyệt của hệ thống quản trị tài nguyên. Trong mô hình Workgroup mỗi máy trạm có một nguồn tài nguyên tương ứng với một hệ thống quản trị tài nguyên bảo vệ nó.

**Chú ý:** Mỗi người khai thác mạng phải nhớ nhiều mã số, vì ứng với mỗi máy trạm có một hệ thống quản trị tài nguyên riêng của nó.

### 2. Mô hình vùng (Domain)

Domain là một khái niệm rất cơ bản trong Windows ả T server, nó là hạt nhân để tổ chức các mạng có quy mô lớn.

Mỗi người tham gia trong Domain cần phải đăng ký thông tin sau:

- Tên Domain
- Tên người sử dụng
- Mật khẩu

Các thông tin này được lưu ở máy chủ dưới dạng một mã số, gọi là tài khoản người sử dụng (user account) và các mã số cũa người sử dụng trong một domain được tổ chức thành một cơ sở dữ liệu trên máy chủ. Khi người sử dụng muốn truy nhập vào một Domain người đó phải chọn tên Domain trong hộp thoại trên máy trạm. Máy trạm sẽ chuyển các thông tin về hệ thống quản trị tài nguyên (SAM - Security Account Manager database) của Domain để kiểm tra. Khi đó hệ thống quản trị tài nguyên trên máy chủ sẽ kiểm tra các thông tin này, nếu kết quả kiểm tra là đúng, người khai thác mới được quyền truy nhập vào tài nguyên của Domain.

Một máy Windows ả T mà không tham gia vào một Domain có nhược điểm sau:

- Máy trạm chỉ có thể cung cấp các mã số được tạo ra trên nó. ả ếu máy này bị hư hỏng thì những người khai thác mạng không thể truy nhập bằng mã số của họ. ả ếu máy này nằm trong một Domain nào đó thì các mã số này còn được lưu trong SAM của một Domain trên máy Máy chủ.
- Qua máy trạm không tham gia vào Domain, người khai thác mạng không thể truy nhập vào tài nguyên của Domain, mặc dù mã số của của người này có trong SAM của Domain

Trong một Domain thường có các loại máy thực hiện những công việc sau:

- Primary domain Controller (PDC), bao giờ cũng phải có để quản trị hệ thống các người sử dụng và các tài khoản trong Domain (hệ thống này gọi là cơ sở dữ liệu SAM - Security Account Manager của Domain). SAM trên máy chủ được thiết kế như hệ thống kiểm soát Domain. Trong một Domain chỉ có duy nhất một PDC.

- ả goài ra hệ thống còn có một hay nhiều máy làm Backup Domain Controller (BDC). Các BDC có thể dùng thay thế cho máy PDC trong trường hợp cần thiết, chẳng hạn máy PDC bị hư

ả gười quản trị Domain chỉ cần tạo tài khoản người sử dụng (user account) chỉ một lần trên máy Primary Domain Controller, thông tin được tự động copy đến các máy Backup Domain Controller.

### 3. Mô hình quan hệ giữa các Domain trong mạng Windows NT

Trong một mạng có thể có nhiều Domain nhưng một máy tính Windows ả T là thành viên của chỉ một domain tại mỗi thời điểm. Tuy nhiên, có một vài trường hợp đôi khi chúng ta cần truy cập tài nguyên trong những domain khác, để là được điều này hệ điều hành Windows ả T server cho phép giữa các Domain có thể tồn tại một quan hệ gọi là quan hệ tin cậy (trust relationship). Chúng ta có thể sử dụng quan hệ tin cậy giữa các Domain cho phép người dùng trên một Domain truy cập tài nguyên trong Domain khác.

Hai Domain A, B gọi là quan hệ tin cậy (trust relationship) mà trong đó Domain A tin cậy Domain B nếu giữa chúng có một mối liên kết sao cho người khai thác mạng của Domain B có thể truy nhập vào Domain A từ một máy trạm trong Domain B.

Từ góc độ của người quản trị mạng mục đích của việc thiết lập quan hệ tin cậy giữa các Domain là làm cho việc quản lý mạng trở lên đơn giản hơn bằng cách kết hợp các Domain vào một đơn vị quản lý. Trong quan hệ tin cậy các Domain được chia ra như sau:

- Domain được tin cậy (trusted domain)
- Domain tin cậy (trusting domain)

Một Domain là loại này hoặc loại kia *thông thường* phụ thuộc vào nó chứa mã số của người sử dụng (người sử dụng account) hay chỉ chứa tài nguyên (resource)

- Domain tin cậy (trusting domain) là Domain chứa tài nguyên.
- Domain được tin cậy (trusted domain) là Domain chứa mã số người sử dụng.

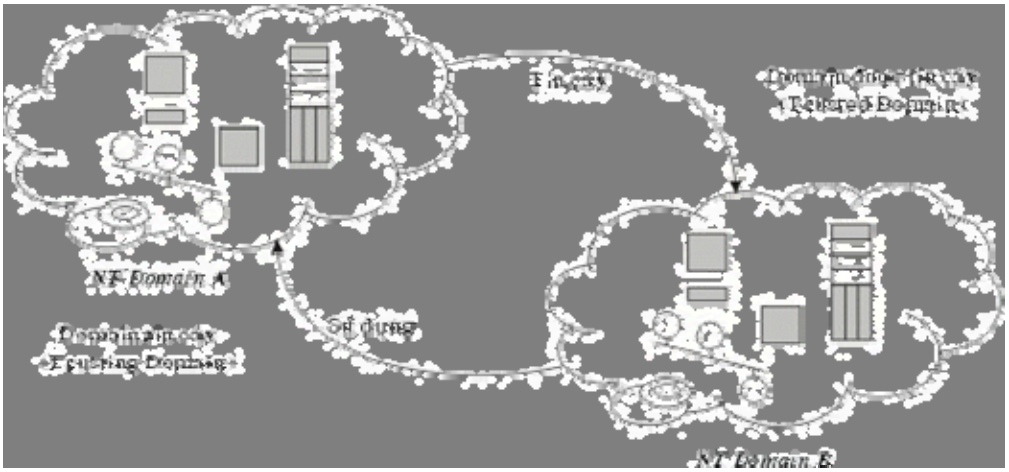
Khi người sử dụng truy nhập từ một máy trạm trong Domain tin cậy (trusting domain) vào Domain được tin cậy (trusted domain) thì quá trình kiểm soát diễn ra như sau:

- ả gười sử dụng phải cho mã số (mã số này ứng với tên, mật khẩu, tên domain cần truy nhập)
- Mã số được chuyển về máy chủ của Domain tin cậy.
- Máy chủ của Domain tin cậy chuyển mã số này sang Domain được tin cậy.
- Kết quả kiểm tra của máy chủ trong Domain được tin cậy diễn ra theo quá trình ngược lại.

**Ở đây chúng ta chú ý:**

- Việc liên kết giữa các Domain không có tính bắc cầu.

- Thông qua việc thiết lập mối quan hệ tin tưởng, chúng ta có thể sử dụng một tài khoản để truy xuất đến nhiều tài nguyên của nhiều Domain. Có thể quản trị nhiều Domain từ một vị trí tập trung.



*Hình 11.1: Mô hình tin cậy của các Domain trong mạng Windows NT*

### 4. Nhóm (group) trong Windows NT

Trong mạng Windows ả T khái niệm nhóm (group) là một trong những khái niệm quan trọng đối với công việc quản lý, điều hành mạng Windows ả T. ả hóm làm cho việc khai thác tài nguyên được dễ dàng thuận lợi và đơn giản hóa việc quản trị. Mỗi nhóm được đăng ký bởi một tài khoản (group account) và có các thành viên của nó. Các quyền đã được gán cho nhóm sẽ tự động gán cho các người sử dụng là thành viên của nhóm. Các tiện lợi của nhóm như sau:

- Quyền có thể được gán cho, hoặc hủy đi trên mọi thành viên của nhóm.

- Khi một người sử dụng bị loại ra khỏi nhóm, thì tự động bị mất các quyền đã được cấp khi còn trong nhóm.

Trong mạng Windows ả T người ta phân biệt phân biệt hai loại nhóm là nhóm toàn cục (global group) và nhóm cục bộ (local group).

### 5. Nhóm toàn cục (global group)

ả hóm toàn cục còn được gọi là nhóm vùng (domain group). Thành viên của nhóm là các người dùng cấp vùng (domain user). Họ ngược lại với người dùng cục bộ (local user) là người có phạm vi giới hạn trong máy tính mà họ được xác định. Thành viên của nhóm toàn cục được phép chuyển ra ngoài (export) một Domain khác. Phạm vi của nhóm toàn cục là toàn bộ vùng trên đó user dược xác định, và thấy được từ bất kỳ máy tính ả T nào trong vùng đó. Quyền có thể được gán cho nhóm toàn cục cho các tài nguyên trên một máy ả T Server hay ả T Workstation trong vùng.

Các tài khoản nhóm toàn cục được lưu ở PDC (Primary DomainController) của Domain, và được sao lưu đến các BDC (Backup Domain Controller) trong Domain đó.

ả hóm toàn cục có những đặc trưng sau:

- Thành viên của nhóm phải là các người sử dụng của domain (domain user account).
- ả hóm toàn cục có thể được gán quyền cho tài nguyên bất kỳ trong vùng mà chúng được xác định.
- ả hóm toàn cục có thể được gán quyền đến các tài nguyên trong vùng khác với vùng chúng được xác định khi quan hệ tin cậy (trust relationship) giữa các vùng có hiệu lực.
- Các thành viên của nhóm toàn cục có thể sử dụng nguồn tài nguyên trong vùng bất kỳ mà nhóm toàn cục có quyền.
- ả hóm toàn cục chỉ chứa mã số của người sử dụng trong Domain của nó. ả ó không thể chứa các nhóm cục bộ và nhóm toàn cục khác.

### 6. Nhóm cục bộ (local group)

ả hóm cục bộ, trái lại, được gán quyền cho nguồn tài nguyên trên máy ả T mà nó được xác định. ả ếu máy ả T là một phần của vùng, thì để tiện cho việc gán quyền, một nhóm cục bộ có thể chứa các tài khoản người dùng cấp vùng (domain user account) và các nhóm toàn cục trong Domain đó, nơi máy tính ả T là thành viên, hoặc những người dùng từ Domain được tin cậy. Các người dùng cấp vùng (domain user) có thể được gán quyền truy cập đến tài nguyên bất kỳ trong Domain đó.

ả ếu Windows ả T computer không nối với mạng thì các thành viên trong local group có thể được gán quyền để truy xuất đến tài nguyên trên máy tính mà trong đó các thành viên được tạo ra còn nếu Windows ả T computer nối vào mạng thì để tiện lợi cho việc phân quyền thì người quản trị mạng có thể đưa global group và domain user vào trong local group .

Có hai loại nhóm cục bộ: ***nhóm cục bộ trạm làm việc (workstation local group)*** và ***nhóm cục bộ vùng (domain local group).*** Một mạng làm việc theo cơ chế vùng bao gồm cả Windows ả T Server và Windows ả T Workstation việc hiểu rõ sự khác nhau giữa hai loại nhóm cục bộ là rất quan trọng.

#### *a. Nhóm cục bộ trạm làm việc (Workstation local group):*

ả hóm cục bộ trạm làm việc hiện diện trên Windows ả T Workstation trên đó chúng được tạo ra. Chúng được chứa trong dữ liệu SAM lưu trữ trên Windows ả T Workstation. Một người dùng cục bộ được tạo ra bằng công cụ *User Manager* của Windows ả T Workstation (khác với công cụ *User Manager for Domains* trên Windows ả T Server) có thể có quan hệ thành viên chỉ trong nhóm cục bộ của trạm làm việc đó. Một nhóm cục bộ trong một trạm làm việc chỉ có thể được dùng trên máy tính trên đó nhóm được tạo ra, và không thể làm việc rên bất kỳ máy Windows ả T nào khác.

ả hóm cục bộ trạm làm việc có thể chứa:

- Các tài khoản người dùng cục bộ từ trạm làm việc trên đó nó được xác định.
- Các tái khoản người dùng cấp vùng (domain user account) và các nhóm toàn cục từ vùng trong đó họ được xác định.
- Các tái khoản người dùng cấp vùng (domain user account) và các nhóm toàn cục từ các vùngï được ủy quyền.

### *b. Nhóm cục bộ vùng (Domain local group):*

**N**hóm cục bộ vùng hoạt động trên Windows ả T Server ở mức vùng, và được tạo ra bằng *User Manager for Domains* (trên Windows ả T Server). Các nhóm cục bộ vùng chỉ có thể hiện hữu trên máy Windows ả T Server tạo ra nó. Do đó, các nhóm cục bộ vùng có thể dùng để truy cập nguồn tài nguyên trên máy tính Windows ả T Server trong vùng đó, mà không dùng để truy cập nguồn tài nguyên trên máy tính Windows ả T Workstation trong vùng này. ả hóm cục bộ vùng không thể được gán quyền trên bộ điều khiển không có cấp vùng, thậm chí cả các máy chủ.

## III. Các mô hình Domain trong mạng Windows NT

Windows ả T máy chủ cung cấp 4 kiểu tổ chức domain gọi tắt là các mô hình domain (domain models). Dưới đây là 4 mô hình tổ chức của nó:

- Mô hình domain đơn (single domain)
- Mô hình domain chính (master domain)
- Mô hình multiple master domain
- Mô hình complete truts

### 1. Mô hình Domain đơn (single domain)

Mô hình domain đơn là mô hình trong mạng chỉ có một domain. Mô hình này thích hợp cho mạng ít người khai thác, cần quản lý tập trung. Mô hình đơn nói chung tương tự như mô hình workgroup, trong mô hình này người sử dụng có thể xem xét, khai thác tài nguyên theo cả mô hình workgroup và mô hình domain.

Loại mô hình này không có các quan hệ ủy quyền vì chỉ có một domain duy nhất, domain này cũng chứa CSDL SAM cho toàn bộ mạng và việc quản trị mạng có thể thực hiện từ một vị trí trung tâm.

Các tài khoản người dùng trong vùng (domain user account) và tài khoản nhóm trong vùng (domain group acconunt) có thể được xây dựng và có các quyền truy cập tài nguyên được gán trên các nhóm và người dùng riêng rẽ và có một phạm vi bao gồm tất cả các máy vi tính trong vùng.

Trong mô hình Domain đơn vấn đề an toàn dữ liệu, quản lý hệ thống được xem xét một cách tốt hơn so với Workgroup.

### 2. Mô hình Domain chính (Master domain)

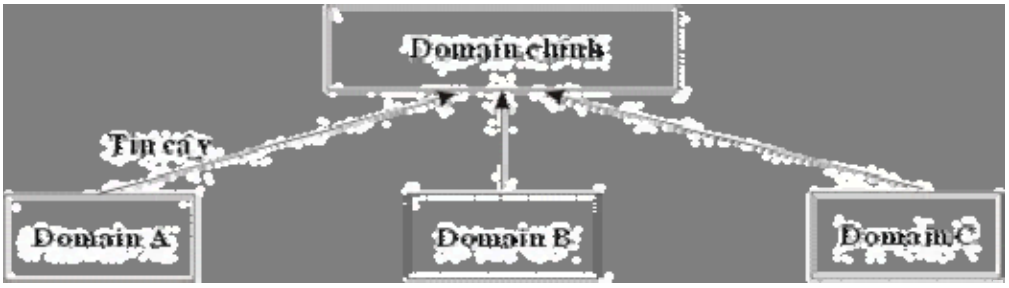
Mô hình Domain chính có thể được sử dụng cho các cơ quan khi họ muốn tổ chức mạng thành nhiều Domain tài nguyên (Resource domain) nhưng vẫn có những tiện lợi trong việc quản lý tập trung. Bằng cách phân chia tài nguyên mạng vào nhiều Domain, chúng ta sẽ tiện tổ chức và quản lý một lượng tài nguyên lớn. Một Domain chủ (master domain) được sử dụng để hổ trợ việc quản trị tập trung mà trong đó tất cả mã số của người sử dụng và mã số các nhóm toàn cục (global group) trên mạng được lưu giữ.

Đặc điểm của mô hình domain chính :

- Mô hình Master Domain là mô hình có nhiều Domain, trong đó có 1 Domain là Domain chính (premery domain). Mô hình này thích hợp cho mạng có số người dùng không quá lớn, nhưng cần phải phân chia thành các đơn vị nhỏ hơn nhưng việc quản lý được tiến hành tập trung.

- Trong mô hình này tất cả mã số của người khai thác mạng và mã số của các nhóm toàn cục (global group) đều chứa trên server trên Domain chính.

- Trong mô hình này tất cả các khác Domain đều tin cậy với Domain chính.




*Hình 11.2: Mô hình Domain chính*

Trong mô hình này mã số của người sử dụng quản lý tập trung và các nhóm toàn cục chỉ cần xác định một lần trong Domain chính. Tài nguyên được nhóm logic thành các đơn vị nhỏ hơn để có thể quản lý bởi từng Domain.

Mô hình Domain chính là mô hình quản lý tập trung vì vậy chiến lược phát triển mạng cần dựa vào các nhóm cục bộ và các nhóm toàn cục.

Mô hình này không những quản lý tập trung các mã số của người sử dụng mà còn cung cấp các dịch vụ như cài đặt phần mềm, sao chép backup cho tất cả các máy chủ trên mạng.

Tuy nhiên mô hình này có nhược điểm có thể gây ùn tắc nếu có quá nhiều nhóm và nhiều người dùng và các nhóm cục bộ cần phải xác định trong mỗi Domain mà chúng được sử dụng.

### 3. Mô hình nhiều Domain chính (muliple master domain)

Mô hình **nhiều Domain chính** (muliple master domain) có thể được sử dụng cho các tổ chức có nhiều khu vực và mỗi khu vực có nhiều bộ phận. Trong nhiều mạng kiểu như vậy, bộ phận điều hành riêng biệt cho mỗi khu vực muốn quản lý tập trung các tài nguyên mạng trong khu vực. Chúng ta xây dựng một Domain chủ (master domain) cho mỗi khu vực và chia các tài nguyên trong mỗi khu vực thành nhiều Domain tài nguyên (resoure domain) riêng biệt.

Trên mô hình này tồn tại các quan hệ sau:

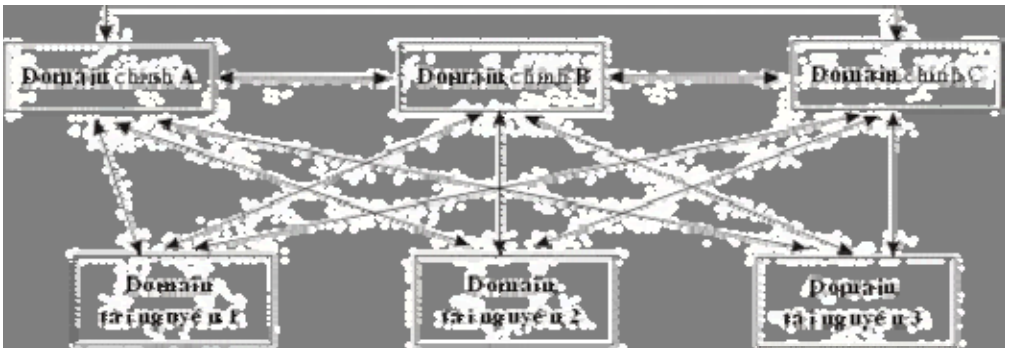
- Mỗi Domain chính quan hệ tin cậy hai chiều với các domain chính khác. Điều này cho phép mỗi Domain chính có thể quản lý các domain chính khác.

- Các Domain không phải là chính không có mã số của người sử dụng mà chỉ cung cấp tài nguyên trên mạng.

- Các Domain không phải là chính tin cậy đối với tất cả các Domain chính. ả hờ điều này mỗi mã số của người sử dụng sẽ được sử dụng trên tất cả các Domain chính và có được quyền truy nhập vào tài nguyên trong các tài nguyên trên các Domain khác của mạng.

Bằng cách phân chia tài nguyên mạng thành nhiều Domain, chúng ta có nhiều thuận lợi trong việc tổ chức quản lý một số lượng lớn các tài nguyên trong các đơn vị phù hợp.

Mô hình nhiều Domain chính có ưu điểm đối với mạng nhiều người dùng trong đó các tài nguyên được nhóm một cách logic theo công việc. Tuy nhiên các nhóm cục bộ và toàn cục phải xác định nhiều lần và mã số của người sử dụng phải chứa ở nhiều Domain chính .

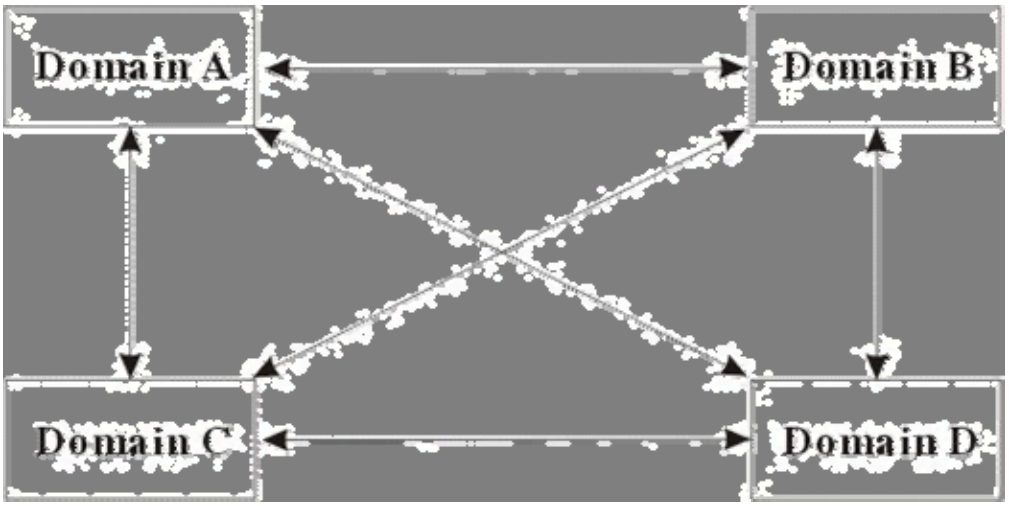


*Hình 11.3: Mô hình nhiều Domain chính*

### 4. Mô hình tin cậy hoàn toàn (complete trust)

Mô hình tin cậy hoàn toàn là mô hình mà trong đó mỗi Domain là quan hệ tin cậy 2 chiều với các Domain khác. Với mô hình này, người sử dụng có thể truy nhập vào bất kỳ Domain nào trên mạng từ một máy trạm nào đó.

Mô hình này có thể áp dụng với qui mô mạng tùy ý và phù hợp cho các cơ quan không có nhóm quản trị tập trung, nó cho phép không hạn chế số người khai thác mạng và số nhóm. Mỗi bộ phận trong đơn vị có thể kiểm soát được mã số của người sử dụng cũng như tài nguyên của bộ phận mình trong đó tài nguyên và mã số người sử dụng được nhóm thành một Domain.




*Hình 11.4: Mô hình nhiều Mô hình tin cậy hoàn toàn*

## IV. Các mặt hạn chế của những mô hình Domain

Mô hình vùng có một số kẽ hở về cấu trúc. ả hững hạn chế về domain được thảo luận ở đây nhằm mục đích giúp bạn thiết kế mạng chính xác và hoàn hảo.

- Domain ả T đơn điệu theo nghĩa là không có cách nào diễn tả quan hệ phân cấp hoặc nhóm tài nguyên trong một vùng đơn. ả gười dùng có thể sử dụng những quyền được ủy thác thể hiện các quan hệ giữa những vùng, nhưng đây là quan hệ sử dụng và không thích hợp cho việc tổ chức mạng dựa trên phạm vi địa lý, tài nguyên sở hữu, logic hoặc nền tảng sơ đồ tổ chức.

- Mô hình vùng Domain chính duy nhất theo Microsoft thích hợp cho các mạng ít hơn 40.000 người dùng và nhóm. Khi số người dùng và nhóm tăng lên, số quan hệ ủy quyền và chi phí quản lý quan hệ cũng tăng. ả ói cách khác chi phí quản lý mạng có thể tăng bất thình lình khi kích thước mạng tăng.

- ả gười dùng phải cẩn trọng về kẻ hở của quan hệ ủy quyền - đặc biệt quan hệ ủy quyền hai chiều. ả ếu không cẩn thận trong việc gán các quan hệ ủy quyền và không có kế hoạch đúng đắn, người sử dụng có thể kết thúc bằng một mô hình ủy quyền trọn vẹn, với tất cả những hạn chế của mô hình đi kèm.

- ả goài ra có một nguy cơ thực sự sẽ xảy ra là người cài đặt mạng có thể cài đặt một mạng hoạt động tốt trong thời gian ngắn còn khi mạng hoạt động dài hạn này sẽ ù nảy sinh vấn đề về mặt chính sách là ai ủy quyền cho ai.

www.viet-ebook.co.cc

**Chương 12**

# Cài đặt, quản trị, sử dụng mạng Windows NT

## I. Cài đặt hệ điều hành mạng Windows NT server

Trước khi cài đặt mạng Windows ả T thì cũng giống như cài các hệ điều hành khác chúng ta phải cắm card mạng vào máy, thiết lập mạng và đảm bảo nó được hoạt động tốt. Khi cài chúng ta có thể sử dụng phần mềm trên đĩa CD ROM (nếu máy của chúng ta là PC thì chúng ta sử dụng thư mục I386) hoặc chúng ta chép thư mục I386 lên đĩa cứng trước khi cài đặt. Để cài đặt Windows ả T ta và trong thư mục I386 và chạy lệnh "WIả ả T"

Chú ý trong trường hợp này chương trình sẽ yêu cầu chuẩn bị 3 đĩa mềm loại 1.44Mb để cài các chương trình khởi động cần thiết và trong quá trình cài đặt các đĩa mềm trên sẽ được sử dụng. ả ếu ta không muốn thì thực hiện lệnh "WIả ả T /B" và phải chỉ đường dẫn của chương trình nguồn như d:\I386.

**Yêu cầu về phần cứng cho việc cài đặt windows NT**

| Thiết bị phần cứng | Yêu cầu |
|---|---|
| Processor | Intel 486, Pentium, Pentium Pro, những hệ thống chạy trên RISC (Ex: MIPS R4x00, DEC?s Alpha AXP). Windows ả T hỗ trợ lên đến 4 CPU ở Mode Symmetriccal Multi-Processing |
| Display device | VGA hay những thiêt bị có độ phân giải cao hơn |
| Hard disk | Tối thiểu phải có 110 MB Hard Disk còn trống trong suốt quá trình cài đặt |
| Floppy disk | 31/2 inch hay 51/4 inch |
| CD-ROM | CD-ROM drive hay đĩa CD-ROM mà ta có thể truy xuất được thông qua đường mạng |
| ả etwork adapter | Một hay nhiều card mạng, card mạng không có cũng được nhưng chức năng mạng sẽ không có |
| Memory | ả T khuyến cáo ít nhất phải có 16 MB Ram cho cả hai hệ thống chạy trên Intel và RISC |

**Chương 13 :**

# Quản lý và khai thác File, thư mục trong mạng Windows NT

Trong số các tài nguyên của mạng chia sẻ cho người sử dụng thông tin lưu trữ trên đĩa cứng của các máy chủ là tài nguyên quan trọng nhất. Không phải ngẫu nhiên mà cái tên "File server" trở nên rất quen thuộc với những người dùng mạng giống như "ả etwork server". Tuy nhiên để làm sao có thể sử dụng, quản lý các tài nguyên đó một cách tốt nhất Windows ả T cung cấp cho chúng ta một cơ chế quản lý và phương thức khai thác. Thông thường chúng ta phải khai báo các tài nguyên trước khi chúng được người sử dụng khai thác. ả goài ra người sử dụng cũng được cung cấp quyền sử dụng một cách phù hợp.

## I. Cơ chế an toàn của File và thư mục trong Windows NT

***Quá trình truy cập tập tin (File hoặc thư mục)*** **trong Windows NT:** Khi một người sử dụng muốn truy cập một tập tin thì tất cả các thông tin về phương thức phục hồi giao dịch và phục hồi giao dịch khi bị lỗi sẽ được đăng ký bởi Log File Server. ả ếu giao dịch thành công, tập tin đó sẽ truy xuất được, ngược lại giao dịch sẽđược phục hồi. ả ếu có lỗi trong quá trình giao dịch, tiến trình giao dịch sẽ kết thúc.

Việc truy xuất tập tin (File hoặc thư mục) được quản lý thông qua các quyền truy cập (right), quyền đó sẽ quyết định ai có thể truy xuất và truy xuất đến tập tin đó với mức độ giới hạn nào. ả hững Quyền đó là Read, Execute, Delete, Write, Set Permission, Take Ownership.

**Trong đó:**

- **Read (R):** Được đọc dữ liệu, các thuộc tính, chủ quyền của tập tin.
- **Execute (X):** Được chạy tập tin.
- **Write (W):** Được phép ghi hay thay đổi thuộc tính.
- **Delete (D):** Được phép xóa tập tin.
- **Set Permission (P):** Được phép thay đổi quyền hạn của tập tin.
- **Take Ownership (O):** Được đặt quyền chủ sở hữu của tập tin.

**Bảng tóm tắt các mức cho phép**

| Permission | R | X | W | D | P | O |
|---|---|---|---|---|---|---|
| ả o Access | | | | | | |
| Read | X | X | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| Change | X | X | X | X | | |
| Full Control | X | X | X | X | X | X |
| Special Access | ? | ? | ? | ? | ? | ? |

Để đảm bảo an toàn khi truy xuất đến tập tin (File và thư mục)ă, chúng ta có thể gán nhiều mức truy cập (permission) khác nhau đến các tập tin thông qua các quyền được gán trên tập tin. Có 5 mức truy cập được định nghĩa trước liên quan đến việc truy xuất tập tin (File và thư mục) là: ả o Access, Read, Change, FullControl, Special Access. Special Access được tạo bởi người quản trị cho bất cứ việc chọn đặt sự kết hợp của R, X, W, D, P, O. ả hững người có quyền hạn Full Control, P, O thì họ có quyền thay đổi việc gán các quyền hạn cho Special Access.

- Khi một người quản trị mạng định dạng một partition trong Windows ả T, hệ thống sẽ mặc định có cấp cho quyền Full Control tới partition đó cho nhóm Everyone. Điều này có nghĩa không hạn chế truy xuất của tất cả người dùng.

- Tùy thuộc trên yêu cầu bảo mật cho các tập người quản lý sẽ cân nhắc việc xóa bỏ nhóm Everyone trong danh sách các quyền hạn sau khi định dạng hay hạn chế nhóm Everyone với quyền Read. ả ếu sự hạn chế này là cần thiết, người quản trị nên cấp quyền hạn Full Control cho nhóm Administrators tới partition gốc.

Ở đây quyền truy cập được gán cho người sử dụng và nhóm người sử dụng do vậy quyền truy cập của một người sử dụng được tính bởi quyền hạn người đó và các nhóm mà người đó là thành viên. Khi người dùng đó truy xuất tài nguyên, các quyền hạn của người dùng được tính theo lối sau:

- ả hững quyền hạn của ngươi dùng và các nhóm trùng nhau.

- ả ếu một trong những quyền là ả o Access thì quyền hạn chung là ả o Access.

- ả ếu những quyền hạn đã yêu cầu được liệt kê không rõ ràng trong danh sách các quyền hạn, yêu cầu truy xuất này là không chấp nhận.

Một người sử dụng thuộc hai nhóm, nếu một nhóm quyền hạn của người dùng là ả o Access, nó luôn được liệt kê đầu tiên trong danh sách Access Control List.

**Quyền sở hữu của các tập tin:** ả gười tạo ra tập tin đó có thể cho các nhóm khác hay người dùng khác khả năng làm quyền sở hữu. Administrator luôn có khả năng làm quyền sở hữu của các tập tin.

ả ếu thành viên của nhóm Administrator có quyền sở hữu một tập tin thì nhóm những Aministrator trở thành chủ nhân. ả ếu người dùng không phải là thành viên của nhóm Administrator có quyền sở hữu thì chỉ người dùng đó là chủ nhân.

ả hững chủ nhân của tập tin có quyền điều khiển của tập tin đó và có thể luôn luôn thay đổi các quyền hạn. Trong File Manager, dưới Security Menu, sau khi xuất hiện hộp thoại

Owner, chúng ta lựa chọn tập tin, chủ nhân hiện thời và nhấn nút Take Ownership, cho phép lập quyền sở hữu nếu được cấp quyền đó.

**Để có quyền sở hữu một tập tin chúng ta cần một trong những điều kiện sau:**

- Có quyền Full Control.
- Có những quyền Special Access bao gồm Take Ownership.
- Là thành viên của nhóm Administrator.

**II. Các thuộc tính của File và thư mục**

- **Archive:** Thuộc tính này được gán bởi hệ điều hành chỉ định rằng một File đã được sửa đổi từ khi nó được Backup. Các phần mềm Backup thường xóa thuộc tính lưu trữ đó. Thuộc tính lưu trữ này có thể chỉ định các File đã được thay đổi khi thực thi việc Backup.
- **Compress:** Chỉ định rằng các File hay các thư mục đã được nén hay nên được nén. Thông số này chỉ được sử dụng trên các partition loại ả TFS.
- **Hidden:** Các File và các thư mục có thuộc tính này thường không xuất hiện trong các danh sách thư mục.
- **Read Only:** Các File và các thư mục có thuộc tính này sẽ không thể bị xóa hay sửa đổi.
- **System:** Các File thường được cho thuộc tính này bởi hệ điều hành hay bởi chương trình OS setup. Thuộc tính này ít khi được sửa đổi bởi người quản trị mạng hay bởi các User.
- ả goài ra các File hệ thống và các thư mục còn có cả hai thuộc tính chỉ đọc và ẩn.

**Lưu ý:** Việc gán thuộc tính nén cho các File hay thư mục mà ta muốn Windows ả T nén sẽ xảy ra trong chế độ ngầm (background). Việc nén này làm giảm vùng không gian đĩa mà File chiếm chỗ. Có một vài thao tác chịu việc xử lý chậm vì các File nén phải được giải nén trước khi sử dụng. Tuy nhiên việc nén File thường xảy ra thường xuyên như là các File dữ liệu quá lớn mà có nhiều người dùng chia sẻ.

**III. Chia sẻ Thư mục trên mạng**

Không có một người sử dụng nào có thể truy xuất các File hay thư mục trên mạng bằng cách đăng nhập vào mạng khi không có một thư mục nào được chia se.

Việc chia sẻ này sẽ làm việc với bảng FAT và ả TFS file system. Để nâng cao khả năng an toàn cho việc chia sẻ, chúng ta cần phải gán các mức truy cập cho File và Thư mục.

Khi chúng ta chia sẻ một thư mục, thì chúng ta sẽ chia sẻ tất cả các File và các Thư mục con. ả ếu cần thiết phải hạn chế việc truy xuất tới một phần của cây thư mục, chúng ta phải

sử dụng việc cấp các quyền cho một user hay một nhóm đối với các Thư mục và các File đó.

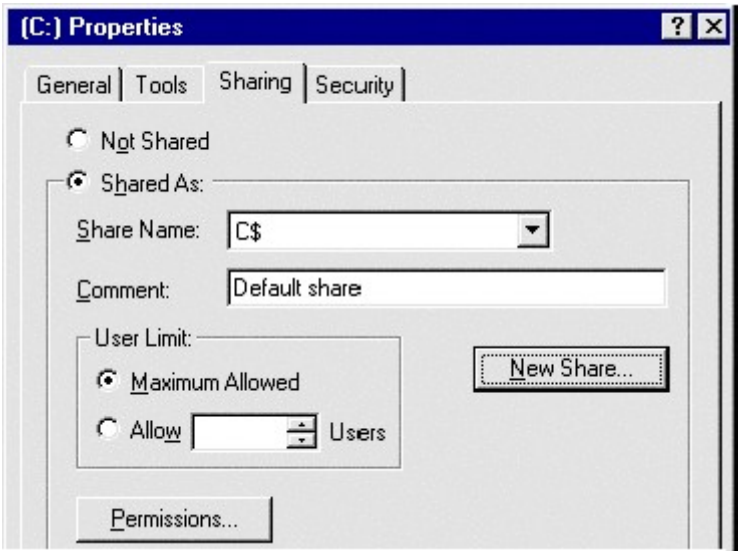
Để chia sẻ một Thư mục, ta phải Login như một thành viên của nhóm quản trị mạng hay nhóm điều hành server.

Tất cả các thủ tục chia sẻ thư mục được thực thi trong Windows ả T Explorer.

**Để chia sẻ một thư mục ta phải thực hiện các bước sau:**

- **Right-click** lên Thư mục đó trong Windows ả T Explorer. Hiện ra menu

- Click **Properties** trong Menu. Hiện ra hộp đối thoại sau:




- Chọn **Sharing tab** hiện ra hộp đối thoại sau:

- Chọn **Shared As** để kích hoạt việc chia sẻ.

- Đưa một tên cần chia sẻ vào hộp **Share name**. Mặc nhiên tên Thư mục được chọn sẽ hiện ra. Đưa dòng ghi chú liên quan đến việc chia sẻ thư mục đó vào hộp **Comment**

- Thiết lập giới hạn số lượng các user bằng cách gỏ một con số vào hộp **Allow**

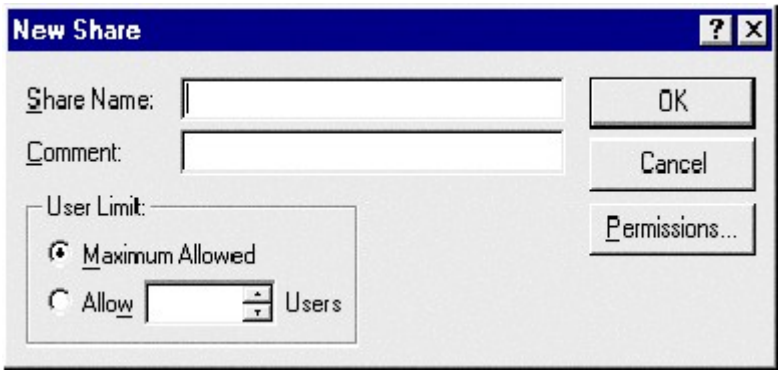
- ả ếu muốn hạn chế việc truy xuất thì click **Permissions button.**

- **Click OK.**

Sau khi một thư mục được chia sẻ Icon cho thư mục đó có 1 bàn tay chỉ định rằng thư mục đó đã được chia sẻ.

ả ếu chúng ta muốn thêm một chia sẻ mới với cùng một thư mục đã được chia sẻ (có thể với hai chia sẻ có hai quyền truy cập khác nhau), ta thực hiện các bước sau:

- **Right-click** vào thư mục đã được chia sẻ trong Windows ả T Explorer.
- Click **Properties** trong **Menu** rút gọn, hiện ra hộp đối thoại **Properties**
- Click **Sharing tab.**
- Click button **New Share** để tạo một sự chia sẻ mới, hiện ra hộp đối thoại sau

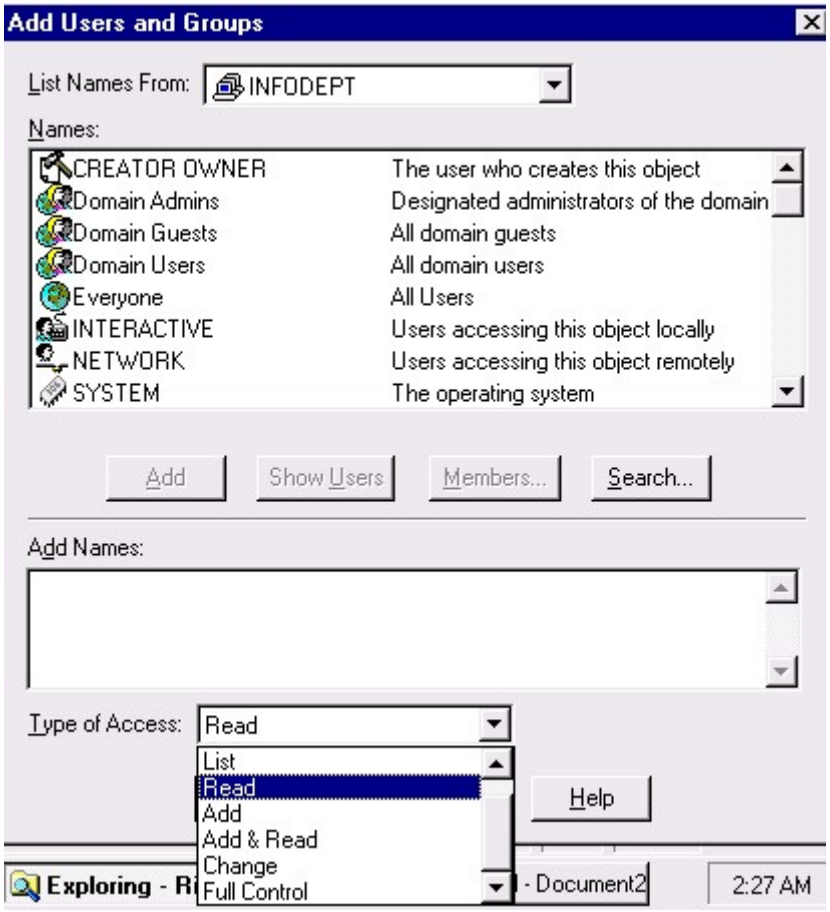



- Mỗi lần tạo một sự chia sẻ chúng ta phải đưa một tên mới cũng như những lời chú thích việc chia sẻ đó sẽ cho ai sử dụng.

**IV. Thiết lập quyền truy cập cho một người sử dụng hay một nhóm**

Để thiết lập các quyền truy cập đối với một thư mục đã được chia sẻ cho một người sử dụng hay một nhóm ta thực hiện:

- **Right-click** lên thư mục đó trong Windows ả T Explorer.
- Click **Properties** trong menu rút gọn**.**
- Chọn **Sharing** tab để hiện các tính chất của thư mục đó
- Click button **Permissions** trong **sharing tab** . Hiện ra Cửa sổ ***The Access Through Share Permissions.***
- Chọn button **Add**, hiện ra cửa sổ ***Add User and group.***




- Chọn một tên trong hộp ***Names*** và click button **Add.** Kết quả là tên đó được đưa vào hộp ***Add Names.***

- Chọn quyền truy xuất trong hộp ***Type of Access*** cho các tên đã chọn .

- Click button **OK.**

Khi chúng ta tạo một sự chia sẻ mới, quyền truy cập mặc nhiên cho nhóm **Everyone** là đầy đủ (**Full Control**). Giả sử rằng chúng ta sẽ gán giá trị mặc nhiên này cho quyền truy cập của thư mục và File. Khi cần thiết sẽ hạn chế việc truy xuất tới thư mục đó.

**Ở đây có một vài chú ý:**

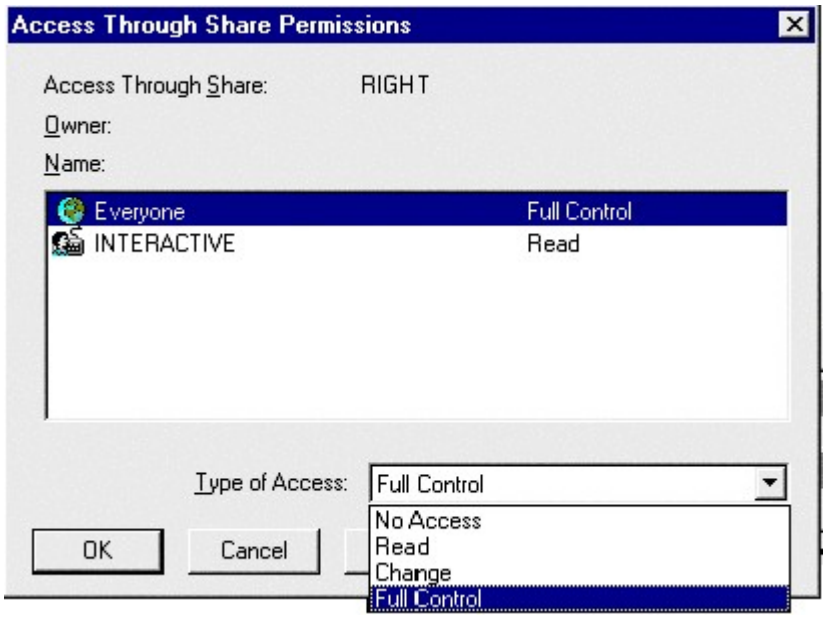
- Các người sử dụng thường chỉ cóù quyền đọc trong các thư mục chứa các chương trình ứng dụng vì họ không cần phải sửa đổi các File.

- Trong một vài trường hợp, các chương trình ứng dụng đòi hỏi các user chia sẻ một thư mục cho các File tạm thời. ẩ ếu thư mục đó nằm trong cùng thư mục chứa trình ứng dụng, chúng ta có thể cho phép user tạo hay xóa các File trong thư mục đó bằng việc gán quyền **Change**.

- Thông thường các người sử dụng cần quyền **Change** trong bất kỳ thư mục nào chứa các Files dữ liệu và chỉ trong các thư mục cá nhân của ho là có đầy đủ các quyền truy cậpï.

**Để sửa đổi các quyền truy cập đối với một thư mục đã được chia sẻ ta thực hiện:**

- **Right-click** lên thư mục được chia sẻ trong Windows ả T Explorer.
- Click **Properties**
- Click **Sharing** tab.
- Click button **Permissions** hiện ra cửa sổ ***Access Through Share Permissions*** sau:




- Chọn 1 tên trong hộp ***Name***
- Chọn một quyền khác trong hộp ***Type of Access*** mà ta muốn gán.
- Click **OK**.

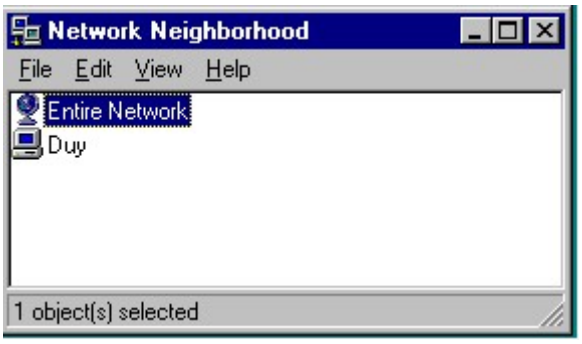
Thông qua việc chia sẻ một thư mục cho một user hay một nhóm cũng góp phần vào việc bảo đảm an toàn cho một thư mục không cho user khác hay nhóm khác truy xuất thư mục đó.

**V. Sử dụng các thư mục mạng**

Muốn sử dụng các thư mục mạng thì trước hết thư mục đó được cho phép chia sẻ, chúng ta phải liên kết thư mục mạng đó với tên một chữ cái tương ứng như một tên đĩa mạng (E,F ,G ,H I,...). Sau khi thư mục được chia sẻ đã kết nối với ký tự ổ đĩa mạng người dùng có thể truy cập thư mục được chia sẻ, các thư mục và file con của nó như là nó đang ở trên máy tính của mình .

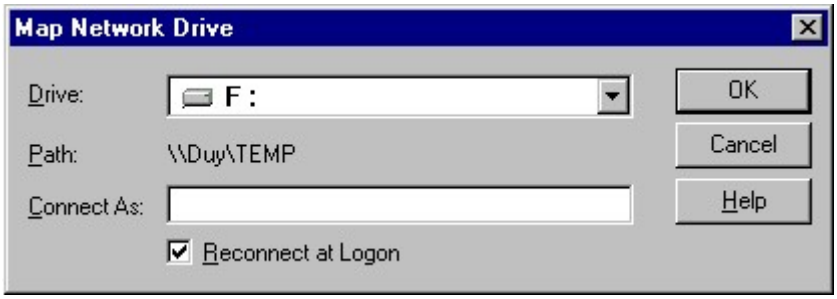
**Có thể dùng Network Neighborhood để thực hiện công việc trên như sau :**

- Click đúp trên **Network Neighborhood** để mở trình duyệt mạng.




- Duyệt qua **Network Neighborhood** để tìm nơi muốn liên kết.

- Click phải vào thư mục đã được chia sẻ mà chúng ta muốn truy cập và chọn **Map Network Drive** trong thực đơn **Options** ta thấy hộp **Map Network Drive** hiện ra




- Trong trường **Drive** của hộp thoại **Map Network Drive**, chọn ổ đĩa mạng chúng muốn liên kết với thư mục chia sẻ.

- ẩ ếu thấy cần, chọn Path và gõ vào tên theo tổng quát Uẩ C (Universal ẩ aming Convention - xem cấu trúc ở phần dưới) để sửa lại đường dẫn tới tài nguyên được chia sẻ. (Việc này chỉ thực hiện khi sử dụng ẩ etwork ẩ eighborhood.)

- ẩ ếu chúng ta không được quyền để truy cập vào tài nguyên chia sẻ trên nhưng trong cương vị người dùng khác thì chúng ta được quyền truy cập, trong trường hợp đó hãy gõ tên người dùng đó vào trường **Connect As**.

- Kích hoạt hộp kiểm tra **Reconnect at Logon** nếu muốn liên kết lâu dài, đó là loại kết nối được phục hồi mỗi lần chú ta đăng nhập vào mạng.

- Chọn **OK** để lưu các thông tin trên.

ẩ goài ra ta có thể dùng lệnh **NET USE** để thực hiện các công việc trên.

Lệnh ẩ ET USE dùng Universal ẩ aming Convention (Uẩ C) để truy cập các tài nguyên dùng chung. Tên Uẩ C bắt đầu bằng một dấu phân cách đặt biệt \\, dấu này chỉ sự bắt đầu của tên Uẩ C (tên Uẩ C có dạng "\\computer_name\share_name[\sub_directory]". ẩ ET USE được dùng đểû truy cập một nguồn tài nguyên dùng chung. Lệnh ẩ ET USE dùng bộ hướng dẫn mạng (ẩ etwork Redirector) trên máy tính ẩ T để thiết lập sự nối kết dùng nguồn tài nguyên chung.

Chúng ta có thể xem ai dùng các file dùng chung khi ta đang xem trạng thái của một file dùng chung, File Manager sẽ cung cấp cho ta các thông tin bằng dùng chọn Properties trong thực đơn File

| Đề mục | Nội dung |
|---|---|
| Total Opens | Tổng số các user đang làm việc với file đó |
| Total Locks | Tổng số các khóa trên file |
| Open By | Tên của người dùng đã mở file |
| For | Loại truy xuất mà người dùng đã mở file |
| Locks | Một số khóa mà người dùng đặt trên file |
| File ID | Con số nhận diện của file |

Khi chúng ta dùng Windows Explorer để xem các tài nguyên chúng ta có thì các ổ đĩa mạng xuất hiện và cho chúng ta khai thác.

www.viet-ebook.co.cc

**Chương 14 :**

# Sử dụng máy in trong mạng Windows NT

Hiện nay máy in trên mạng cũng là một tài nguyên việc chia sẻ của mạng cho người sử dụng. Tuy các máy in đang ngày càng rẻ đi nhưng với nhu cầu về chất lượng đang ngày một cao thì việc chia sẻ các máy in đắt tiền trên mạng vẫn đang cần thiết. Windows ả T là một hệ điều hành mạng mà bất kỳ máy tính Windows ả T nào cũng có thể cung cấp các dịch vụ in ấn cho người sử dụng trong mạng.

Khi chia sẻ một máy in trên mạng (cho nhiều người có thể cùng sử dụng) chúng ta cần phải giải quyết những vấn đề sau :

- Máy in không làm được 2 việc một lúc, nếu phải nhận cùng một lúc thì sẽ có va chạm, do vậy mạng phải có cơ chế sắp xếp công việc sao cho máy in có thể thực hiện một cách lần lượt các công việc in.

- Các công việc in được thực hiện bởi những người sử dụng khác nhau có thể cần những mức độ ưu tiên khác nhau và hệ thống quan lý in cần có khả năng thực hiện điều này.

## I. Cơ chế in trong mạng Windows NT

Thông thường máy in mạng được quản lý thông qua một máy chủ mà trên đó thực hiện nhiệm vụ quản lý các công việc in, máy chủ đó thường được gọi là máy chủ in (Print server) và chạy chương trình quản lý in. Windows ả T cho phép cài đặt máy in tại bất cứ đâu trên mạng, mỗi một máy có cài đặt Windows ả T đều có thể thực hiện nhiệm vụ máy chủ in. ả ó có thể quản lý máy in gắn trực tiếp vào nó hay một máy in gắn vào máy khác trên mạng.

Để giải quyết những vấn đề đặt ra với công việc in trên mạng Windows ả T sử dụng kỹ thuật gọi là Spooling mà chủ yếu như sau:

- Khi người sử dụng quyết định thực hiện một công việc in thì công việc in đó không trực tiếp gửi ra máy in mà nó được đặt trong một file tại máy chủ in. Ở đây việc thực hiện giống như hàng đợi rạp hát, nó là một vùng lưu trữ các công việc in và có nhiệm vụ ngăn chặn xung đột khi các user chi xuất đồng thời ra máy in.

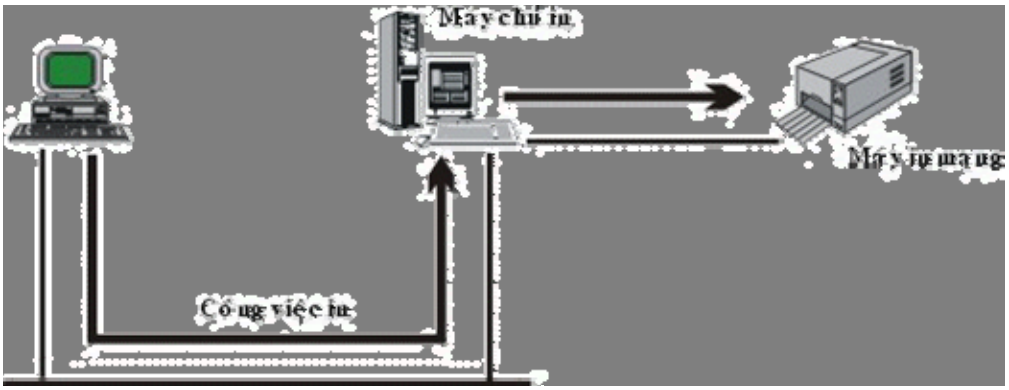
- Máy chủ in duy trì các hàng đợi để cất giữ các công việc in và đưa chúng tới máy in ngay khi có thể. Trong khi đó người sử dụng có thể làm tiếp công việc ngay khi công việc in được cất vào hàng đợi.

- Khi máy in rảnh máy chủ in sẽ chuyển lần lượt các công việc in đang đứng đợi trong hàng tới máy in. Tại đây máy chủ in phải có một khả năng lưu trữ dữ liệu lớn để có thể lưu trữ nhiều công việc in một lúc và cần phải có khả năng đáp ứng những yêu cầu đa dạng của các công việc in.

Để giải quyết vấn đề nẩy sinh với máy in trong mạng Windows ả T tiến hành phân biệt giữa máy in vật lý gọi là Printing device và một thực thể logic của máy in gọi là logic printer. Máy in logic được sử dụng để kiểm soát các tác vụ sau đây :

- Công việc in được gởi đi đâu.
- Công việc in ấn gởi đi khi nào.
- Thứ tự ưu tiên của các tác vụ in.

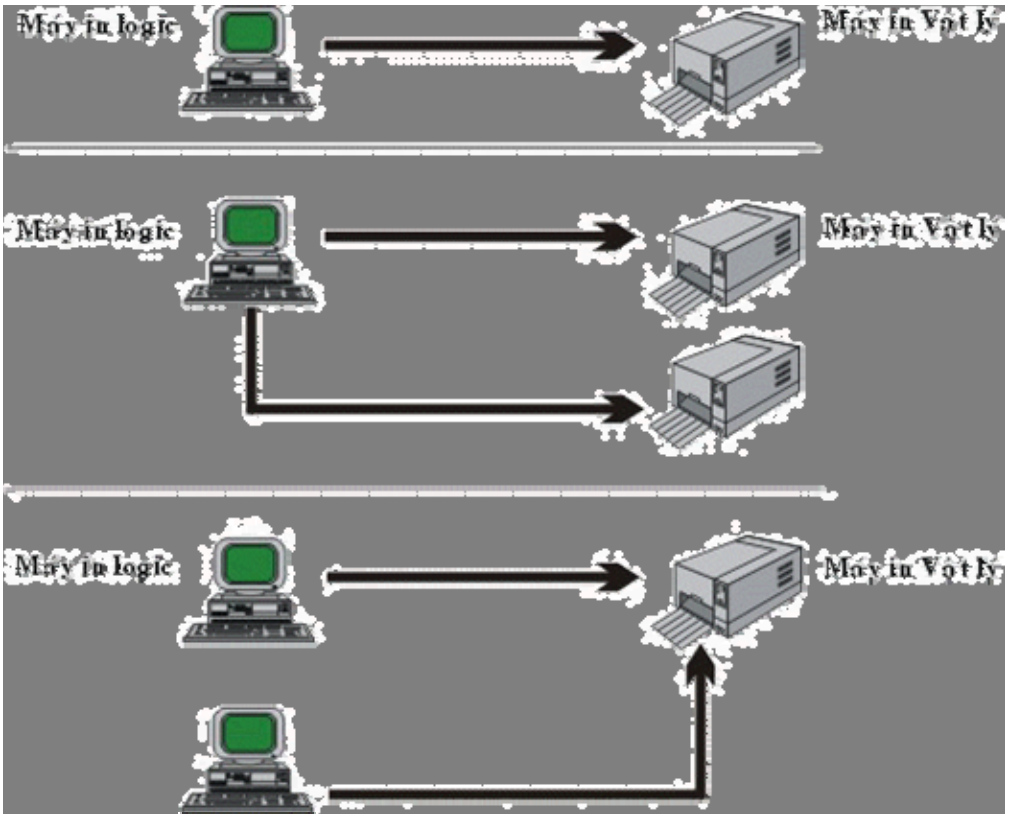
ả gười sử dụng in ra spool thông qua việc in ra máy in logic, họ sử dụng máy in logic như là máy in đang được gắn là máy của họ nhưng thực sự các dữ liệu được in ra máy in logic được chuyển cho mạng và qua đó đến máy chủ in trước khi được đưa ra máy in mạng.




*Hình 14.1: Máy chủ in và spool*

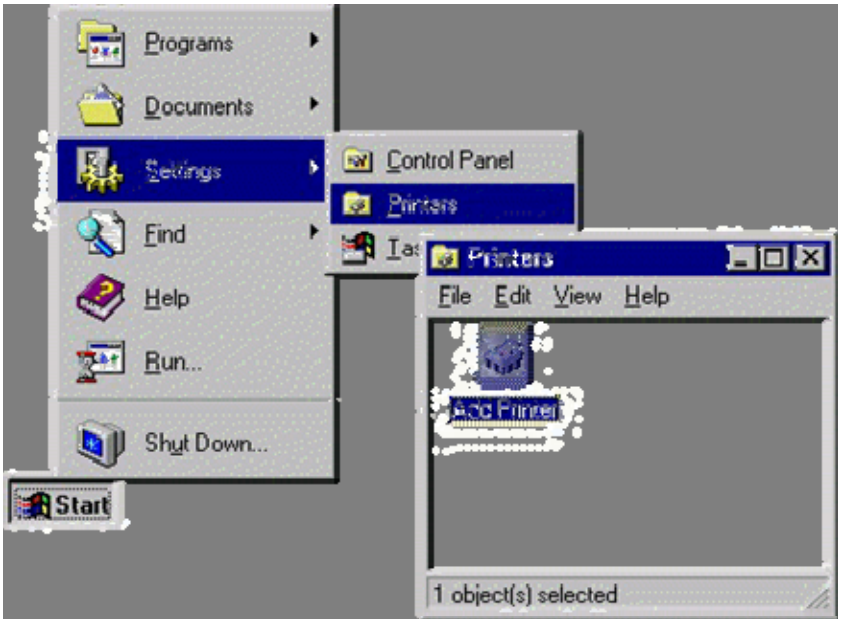
Máy chủ in sẽ liên kết các máy in logic với máy in vật lý, nó phải đảm bảo các công việc in phải được đưa đúng đến máy in vật lý. Tại đây có 3 trường hợp có thể đối với mối quan hệ giữa máy in logic và máy in vật lý

- Một máy in logic liên kết với một máy in vật lý.
- ả hiều máy in logic liên kết với một máy in vật lý.
- Một máy in logic liên kết với nhiều máy in vật lý.

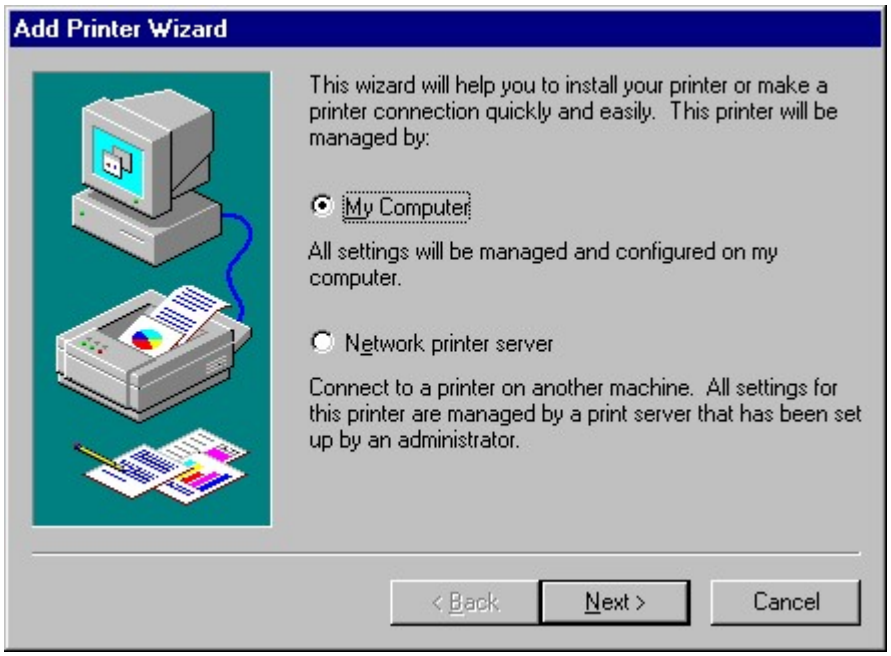



*Hình 14.2: Liên kết giữa máy in Logic và máy in vật lý*

ả ếu Server chưa cài đặt máy in logic, ta phải cài đặt máy in logic tương ứng với một máy in thực tế cho Server. Vào menu **Start**, chọn **Settings**, chọn **Printers**, chọn **Add Printer** như:




Hộp sau đó hộp hội thoại **Add printer** winzar hiện ra

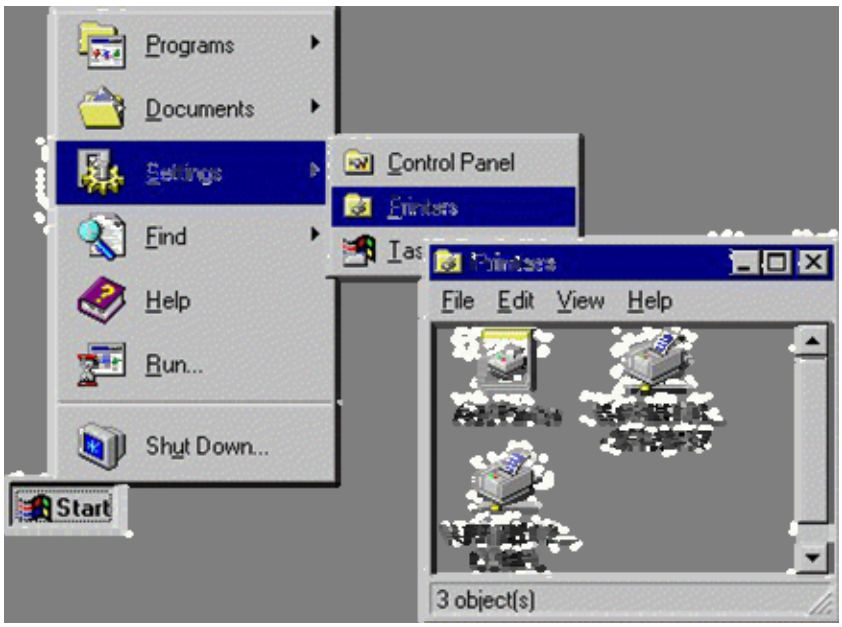



- Chọn My Computer nếu máy in của chúng ta không có card mạng và được nối trực tiếp vào Server.

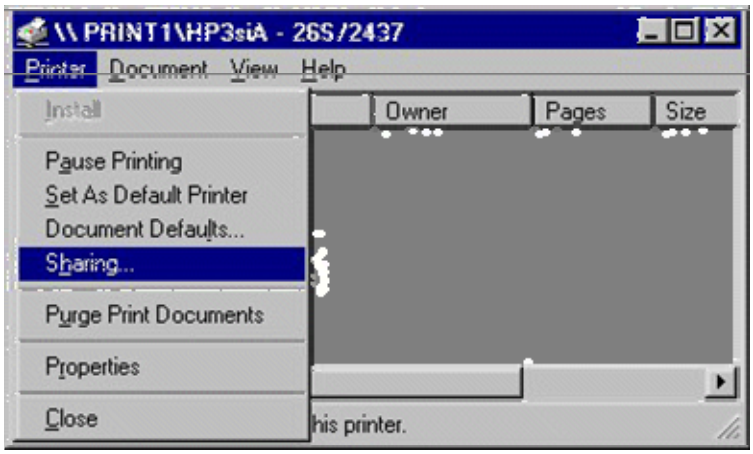
- Chọn ả etwork printer server nếu máy in của chúng ta nối trực tiếp vào mạng.

- Chọn ả ext, chọn cổng nối với máy in (thường là LPT1). Chọn tên hãng sản xuất và loại máy in ta đang dùng, chọn ả ext, ta phải trả lời thêm vài câu hỏi phụ như ta có muốn in trang test không? Có muốn đặt máy in này là ngầm định không?

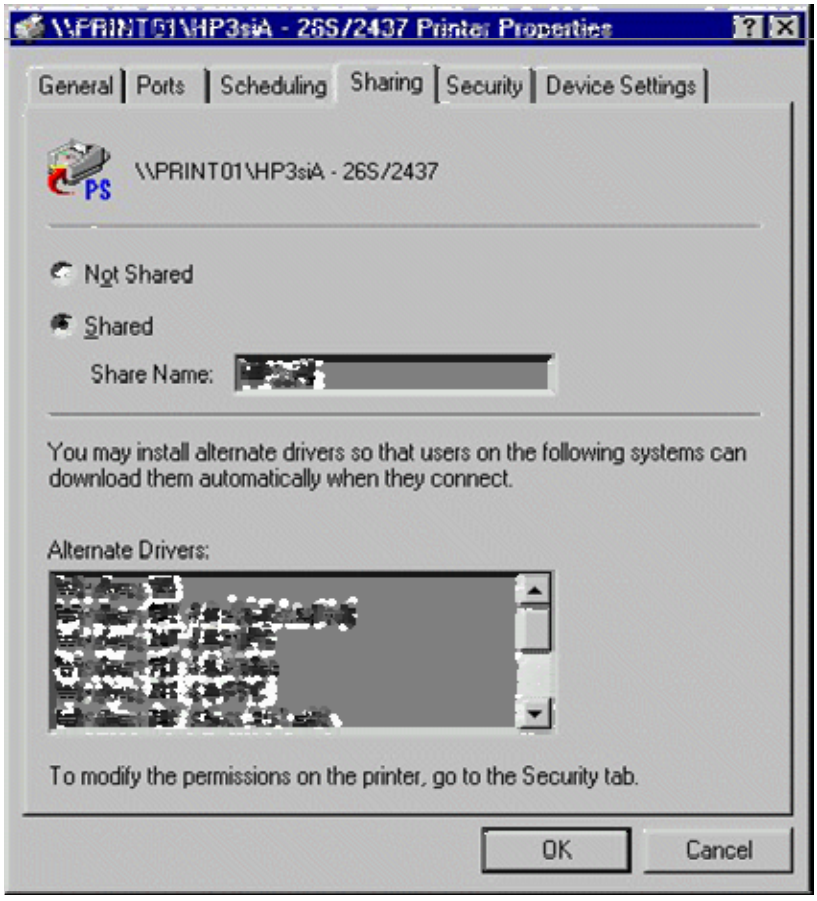
Sau khi cài đặt, chúng ta sẽ thấy xuất hiện thêm biểu tượng máy in mà vừa được cài đặt trong khung máy in. Chúng ta phải cho phép dùng chung máy in nàybằng cách lựa chọn máy in đó Trong khung Printers




- Ta nhắp chuột phải vào tên máy in đó, chọn **Sharing** như hình sau:




Khung **Printer properties** hiện ra cho chúng ta nhập các thông số như: tên máy in logic (Share namem), các tính chất khác như về an toàn. mà chúng ta muốn khi phục vụ mạng.




- Cuối cùng chọn **OK**, lúc này, ta sẽ thấy ở dưới biểu tượng máy in có bàn tay đỡ chứng tỏ máy in này đã được phép dùng chung. ấ ếu trên Server cài đặt nhiều loại máy in với nhiều chế độ khác nhau, ta có thể chọn máy in ngầm định bằng cách đánh dấu vào mục **Set As Default**.

- Để máy trạm có thể in được qua Server, nếu chưa cài đặt chúng ta phải cài máy in như sau: nhắp đúp vào tên Server có nối với máy in, khung **Shared Printers** sẽ hiện ra danh sách các máy in đã cài trên Server, chúng ta chọn tên máy in cần nối rồi bấm **OK**.

Quay trở lại khung màn hình **Print Manager** chúng ta nhìn thấy thông báo máy in này đã được phép sử dụng. Thoát ra khỏi **Print Manager** và chúng ta có thể in qua máy in mạng trên bất cứ một phần mềm nào trên Windows như Winword, Excel, v.v...

Bất kỳ máy tính Windows ả T có thể được cấu hình như là một **print server**. Tuy nhiên chỉ có những người là thành viên của những nhóm sau đây mới có quyền tạo ra các máy in:

- Administrator (ả T Worstation and Server).
- Server Operator (ả T Server).
- Print Operator (ả T Server).
- Power Users (ả T Worstation).

## II. Bảo mật của máy in

### Windows NT có các mức độ bảo mật trong in ấn như sau:

- **Quyền sở hửu máy in (Ownership) :** người sử dụng tạo ra một máy in chính là người chủ sở hửu máy in đó và có toàn quyền trên tất cả các thuộc tính của máy in logic. ả gười chủ sở hửu máy in có thể gán quyền cho những người dùng khác quản lý tài liệu hay toàn quyền điều khiển việc in ấn. Một người sử dụng có toàn quyền thì họ toàn quyền sở hửu máy in logic đó.

- **Quản lý thuộc tính máy in (Permissions):** quyền quản lý máy in bao gồm 4 quyền sau:

  - **No access:** không được phép truy cập.
  - **Print:** in
  - **Manage document:** quản lý văn bản, có khả năng thực hiện các thao tác: Điều khiển khởi đặt tài liệu, ả gừng, phục hồi, khởi động lại,và xóa các tài liệu.
  - **Full control:** toàn quyền điều khiển, thực hiện các quyền quản lý tài liệu và các quyền sau đây:
    - Thay đổi trật tự in ấn tài liệu.
    - ả gừng, tổng hợp lại,che dấu các máy in logic.
    - Thay đổi thuộc tính của máy in logic.
    - Hủy các máy in logic.
    - Thay đổi quyền của máy in logic

Có thể xem tài liệu ở máy in logic và quản lý chúng theo nhiều cách. ả gười sử dụng luôn quản lý được tất cả các tài liệu mà họ tạo ra. Để quản lý được các tài liệu của các người sử dụng khác, phải là người chủ sở hửu của máy in logic hay là thành viên của các nhóm:

- Administrator.
- Server Operator
- Print operator.

Bất kỳ một máy in nào cũng có thể làm việc trong môi trường mạng nhưng điều quan trọng là xem xét **chu kỳ làm việc (duty cycle)** của máy in. ả ghĩa là phải xem xét số lượng trang in tối đa mà máy in có thể in ra trong một khoảng thời gian nhất định.

Các máy in được thiết kế cho mạng thường có **chu kỳ làm việc (duty cycle)** cao. Các máy in có thể gắn vào bất cứ nơi đâu trên mạng. Công việc in không phù thuộc vào các thiết bị phần cứng hay các thiết bị kết nối mà do được quản lý bởi một **print server** và dữ liệu được chuyển vận trên mạng.

**Chương 15 :**

# Các dịch vụ mạng của Windows NT Server

Cũng như các hệ điều hành khác Windows ả T cũng có những ưu, khuyết điểm của nó, tuy nhiên Windows ả T hiện nay chinh phục được nhiều người dùng với những ưu điểm không thể chối cãi. Là hệ điều hành mạng cho phép tổ chức quản lý một cách chủ động theo nhiều mô hình khác nhau: peer-to-peer, clien/server. ả ó thích hợp với tất cả các kiến trúc mạng hiện nay như: hình sao (start), đường thẳng (bus), vòng (ring) và phức hợp. ả ó có một số đặc tính ưu việt bảo đảm thực hiện cùng lúc nhiều chương trình mà không bị lỗi. Bản thân Windows ả T đáp ứng được hầu hết các giao thức phổ biến nhất trên mạng và cũng hỗ trợ được rất nhiều những dịch vụ truyền thông trên mạng. ả ó vừa đáp ứng được cho mạng cục bộ (LAả ) và cho cả mạng diện rộng (WAả ).

Windows ả T cho phép dùng giao thức Windows ả T TCP/IP, vốn là một giao thức được sử dụng rất phổ biến trên hầu hết các mạng diện rộng và trên Internet. Giao thức TCP/IP dùng tốt cho nhiều dịch vụ mạng trên môi trường Windows ả T.

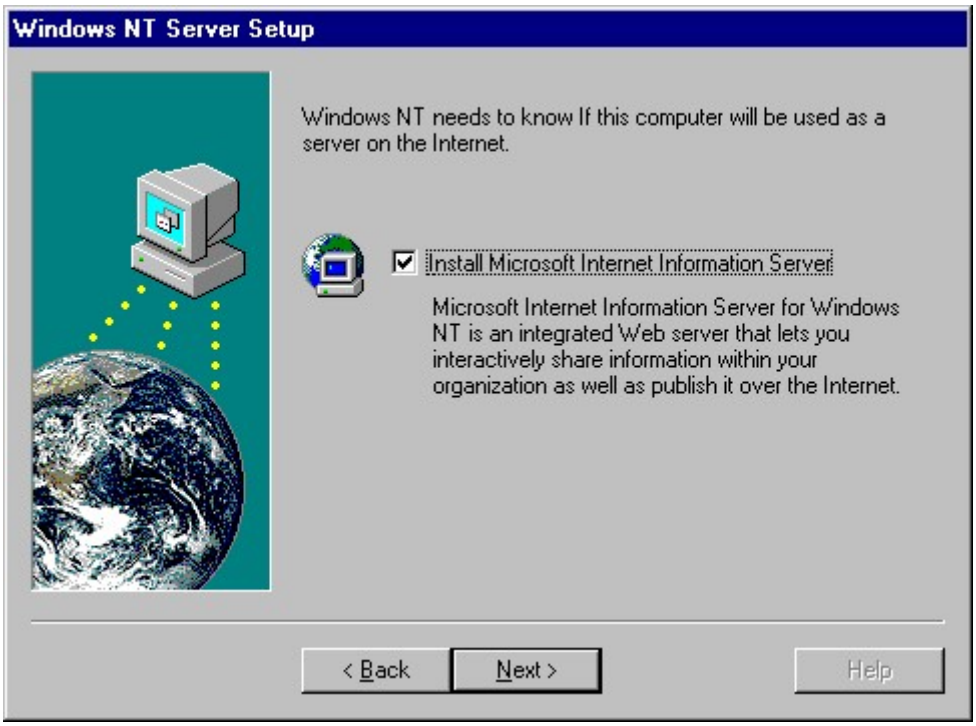
## I. Internet Information Server (IIS)

Internet Information Server là một ứng dụng chạy trên Windows ả T, tích hợp chặt với Windows ả T, khi cài đặt IIS, IIS có đưa thêm vào tiện ích màn hình kiểm soát (Performance monitor) một số mục như thống kê số lượng truy cập, số trang truy cập. Việc kiểm tra người dùng truy cập cũng dựa trên cơ chế quản lý người sử dụng của Windows ả T. Sau khi cài đặt IIS, trong thư mục InetSrv sẽ có các thư mục gốc tương ứng cho từng dịch vụ chọn cài đặt.

IIS bao gồm 3 dịch vụ: World Wide Web (WWW), chuyển file (FTP - File Transfer Protocol) và Gopher. Cả 3 dịch vụ này đều sử dụng kết nối theo giao thức TCP/IP.

### 1. Cài đặt dịch vụ Internet Information Server

Khi cài đặt hệ điều hành Windows ả T đến phần mạng Windows ả T sẽ hỏi chúng ta xem có cài đặt dịch vụ Internet Information Server hay không với hộp hội thoại




*Hình 15.1: Màn hình cài đặt của IIS*

Để thực hiện việc cài đặt chúng ta Click vào phím ả ext và Hệ thống sẽ bắt đầu cài đặt các dịch vụ Internet Information Server.

### 2. Các dịch vụ trong IIS

#### *a. WWW (World Wide Web) :*

Là một trong những dịch vụ chính trên Internet cho phép người sử dụng xem thông tin một cách dễ dàng, sinh động. Dữ liệu chuyển giữa Web Server và Web Client thông qua nghi thức HTTP (Hypertext Transfer Protocol).

ả gười quản trị có thể xem các thông tin như các người dùng đã truy cập, các trang được truy cập, các yêu cầu được chấp nhận, các yêu cầu bị từ chối. thông qua các file có thể được lưu dưới dạng cơ sở dữ liệu.

#### *b. FTP (File Transfer Protocol)*

Sử dụng giao thức TCP để chuyển file giữa 2 máy và cũng hoạt động theo mô hình Client/Server, khi nhận được yêu cầu từ client, đầu tiên FTP Server sẽ kiểm tra tính hợp lệ của người dùng thông qua tên và mật mã. ả ếu hợp lệ, FTP Server sẽ kiểm tra quyền người dùng trên tập tin hay thư mục được xác định trên FTP Server. ả ếu hợp lệ và hệ thống file là ả TFS thì sẽ có thêm kiểm tra ở mức thư mục, tập tin theo ả TFS. Sau khi tất cả hợp lệ, người dùng sẽ được quyền tương ứng trên tập tin, thư mục đó.

**Để sử dụng FTP có nhiều cách:**

- Sử dụng Web Browser.

- Sử dụng Command line.
- Sử dụng từ <Run> command trong Windows.

*c. Gopher*

Là một dịch vụ sử dụng giao diện menu để Gopher Client tìm và chuyển bất kỳ thông tin nào mà Gopher Server đã được cấu hình. Gopher cũng sử dụng kết nối theo giao thức TCP/IP.

**II. Dynamic Host Configuration Protocol (DHCP) :**

Trong một mạng máy tính, việc cấp các địa chỉ IP tĩnh cố định cho các host sẽ dẫn đến tình trạng lãng phí địa chỉ IP, vì trong cùng một lúc không phải các host hoạt động đồng thời với nhau, do vậy sẽ có một số địa chỉ IP bị thừa. Để khắc phục tình trạng đó, dịch vụ DHCP đưa ra để cấp phát các địa chỉ IP động trong mạng.

Trong mạng máy tính ả T khi một máy phát ra yêu cầu về các thông tin của TCPIP thì gọi là DHCP client, còn các máy cung cấp thông tin của TCPIP gọi là DHCP server. Các máy DHCP server bắt buộc phải là Windows ả T server.

Cách cấp phát địa chỉ IP trong DHCP: Một user khi log on vào mạng, nó cần xin cấp 1 địa chỉ IP, theo 4 bước sau :

- Gởi thông báo đến tất cả các DHCP server để yêu cầu được cấp địa chỉ.
- Tất cả các DHCP server gởi trả lời địa chỉ sẽ cấp đến cho user đó.
- User chọn 1 địa chỉ trong số các địa chỉ, gởi thông báo đến server có địa chỉ được chọn.
- Server được chọn gởi thông báo khẳng định đến user mà nó cấp địa chỉ.

**Quản trị các địa chỉ IP của DHCP server:** Server quản trị địa chỉ thông qua thời gian thuê bao địa chỉ (lease duration). Có ba phương pháp gán địa chỉ IP cho các Worstation :

- Gán thủ công.
- Gán tự động.
- Gán động .

Trong phương pháp gán địa chỉ IP thủ công thì địa chỉ IP của DHCP client được gán thủ công bởi người quản lý mạng tại DHCP server và DHCP được sử dụng để chuyển tới DHCP client giá trị địa chỉ IP mà được định bởi người quản trị mạng

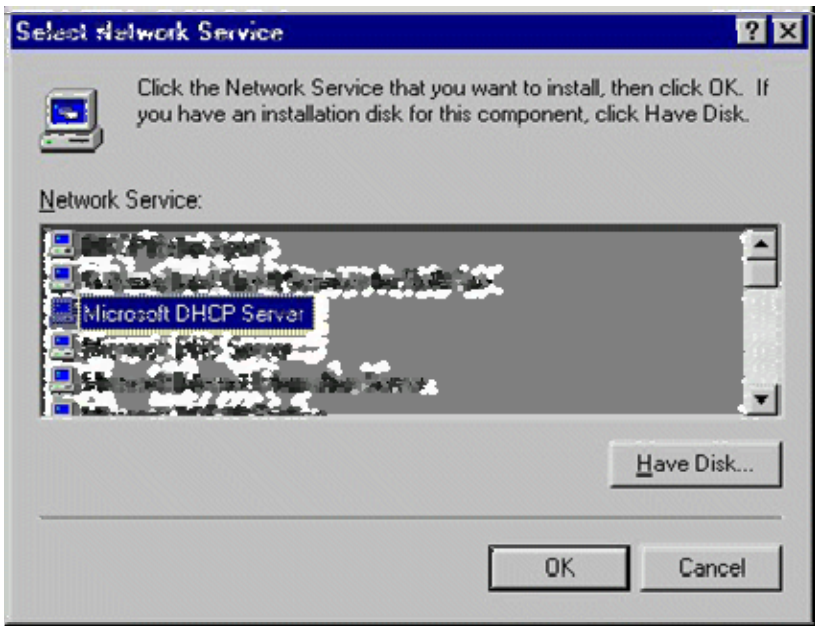
Trong phương pháp gán địa chỉ IP tự động DHCP client được gán địa chỉ IP khi lần đầu tiên nó nối vào mạng. Địa chỉ IP được gán bằng phương pháp này sẽ được gán vĩnh viễn cho DHCP client và địa chỉ này sẽ không bao giờ được sử dụng bởi một DHCP client khác

Trong phương pháp gán địa chỉ IP động thì DHCP server gán địa chỉ IP cho DHCP client tạm thời. Sau đó địa chỉ IP này sẽ được DHCP client sử dụng trong một thời gian đặc biệt. Đến khi thời gian này hết hạn thì địa chỉ IP này sẽ bị xóa mất. Sau đó nếu DHCP client cần nối kết vào mạng thì nó sẽ được cấp một địa chủ IP khác

Phương pháp gán địa chỉ IP động này đặc biệt hữu hiệu đối với những DHCP client chỉ cần địa chỉ IP tạm thời để kết nối vào mạng. Ví dụ một tình huống trên mạng có 300 users và sử dụng subnet là lớp C. Điều này cho phép trên mạng có 253 nodes trên mạng. Bởi vì mỗi computer nối kết vào mạng sử dụng TCP/IP cần có một địa chỉ IP duy nhất do đó tất cả 300 computer không thể đồng thời nối kết vào mạng. Vì vậy nếu ta sử dụng phương pháp này ta có thể sử dụng lại những IP mà đã được giải phóng từ các DHCP client khác.

Cài đặt DHCP chỉ có thể cài trên Windows ả T server mà không thể cài trên Client. Các bước thực hiện như sau:

- Login vào Server với tên Administrator .
- Click hai lần vào icon **Network** . Ta sẽ thấy hộp hội thoại **Network dialog box**




*Hình 15.2: Màn hình cài đặt của DHCP*

- Chọn tab **service** và click vào nút **Add** .
- Ta sẽ thấy một loạt các service của Windows ả T server nằm trong hộp hội thoại **Select Network Service**. Chọn **Microsoft DHCP server** từ danh sách các service được liệt kê ở phía dưới và nhấn **OK** và thực hiện các yêu cầu tiếp theo của Windows ả T.

Để cập nhật và khai thác DHCP server chúng ta chọn mục DHCP manager trong ả etwrok Administrator Tools.

**III. Dịch vụ Domain Name Service (DNS)**

Hiện nay trong mạng Internet số lượng các nút (host) lên tới hàng triệu nên chúng ta không thể nhớ hết địa chỉ IP được, Mỗi host ngoài địa chỉ IP còn có một cái tên phân biệt, Dẩ S là 1 cơ sở dữ liệu phân tán cung cấp ánh xạ từ tên host đếùn địa chỉ IP. Khi đưa ra 1 tên host, Dẩ S server sẽ trả về địa chỉ IP hay 1 số thông tin của host đó. Điều này cho phép người quản lý mạng dễ dàng trong việc chọn tên cho host của mình

**DNS server được dùng trong các trường hợp sau :**

- Chúng ta muốn có 1 tên domain riêng trên Interner để có thể tạo, tách rời các domain con bên trong nó.

- Chúng ta cần 1 dịch vụ Dẩ S để điều khiển cục bộ nhằm tăng tính linh hoạt cho domain cục bộ của bạn.

- Chúng ta cần một bức tường lửa để bảo vệ không cho người ngoài thâm nhập vào hệ thống mạng nội bộ của mình

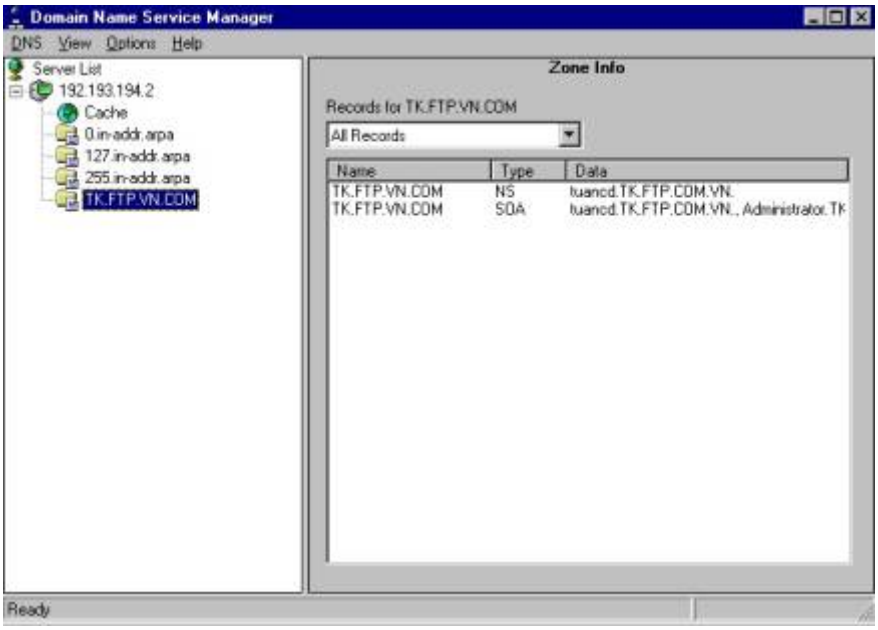
Có thể quản lý trực tiếp bằng các trình soạn thảo text để tạo và sửa đổi các file hoặc dùng Dẩ S manager để tạo và quản lý các đối tượng của Dẩ S như: Servers, Zone, Các mẫu tin, các Domains, Tích hợp với Win, .

Cài đặt Dẩ S chỉ có thể cài trên Windows ẩ T server mà không thể cài trên Client. Các bước thực hiện như sau:

- Login vào Server với tên **Administrator**.

- Click hai lần vào icon **Network**. Ta sẽ thấy hộp hội thoại **Network dialog box** tương tụ như trên và lựa chọn **Microsoft DNS Server**.

Để cập nhật và khai thác Dẩ S server chúng ta chọn mục **DNS manager trong Netwrok Administrator Tools**. Hộp hội thoại sau đây sẽ hiện ra



*Hình 15.3: Màn hình DNS Manager*

Mỗi một tập hợp thông tin chứa trong **DNS database** được coi như là **Resourse record**. ả những **Resourse record** cần thiết sẽ được liệt kê dươi đây:

| Tên Record | Mô tả |
|---|---|
| A (Address) | Dẫn đường một tên host computer hay tên của một thiết bị mạng khác trên mạng tới một địa chỉ IP trong Dả S zone |
| Cả AME () | Tạo một tên Alias cho tên một host computer trên mạng |
| MX () | Định nghĩa một sự trao đổi mail cho host computer đó |
| ả S (name server) | Định nghĩa tên server Dả S cho Dả S domain |
| PTR (Pointer) | Dẫn đường một địa chỉ IP đến tên host trong Dả S server zone |
| SOA (Start of authority) | Hiển thị rằng tên server Dả S này thì chứa những thông tin tốt nhất |

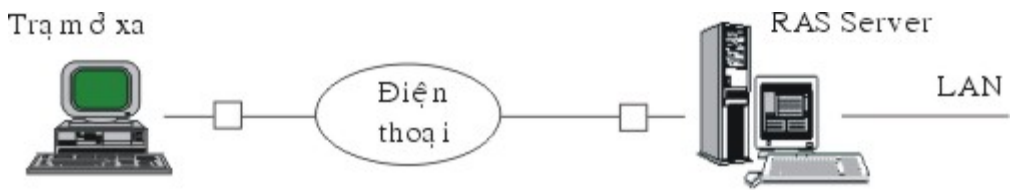
## IV. Remote Access Service (RAS)

ả goài những liên kết tại chỗ với mạng cục bộ (LAả ) các nối kết từ xa vào mạng LAả  hiện đang là những yêu cầu cần thiết của người sử dụng. Việc liên kết đó cho phép một máy từ xa như của một người sử dụng tại nhà có thể qua đường dây điện thoại thâm nhập vào một mạng LAả  và sử dụng tài nguyên của nó. Cách thông dụng nhất hiện nay là dùng modem để có thể truyền trên đường dây điện thoại.

Windows ả T cung cấp Dịch vụ Remote access Service cho phép các máy trạm có thể nối với tài nguyên của Windows ả T server thông qua đường dây điện thoại. RAS cho phép truyền nối với các server, điều hành các user và các server, thực hiện các chương trình khai thác số liệu, thiết lập sự an toàn trên mạng. .

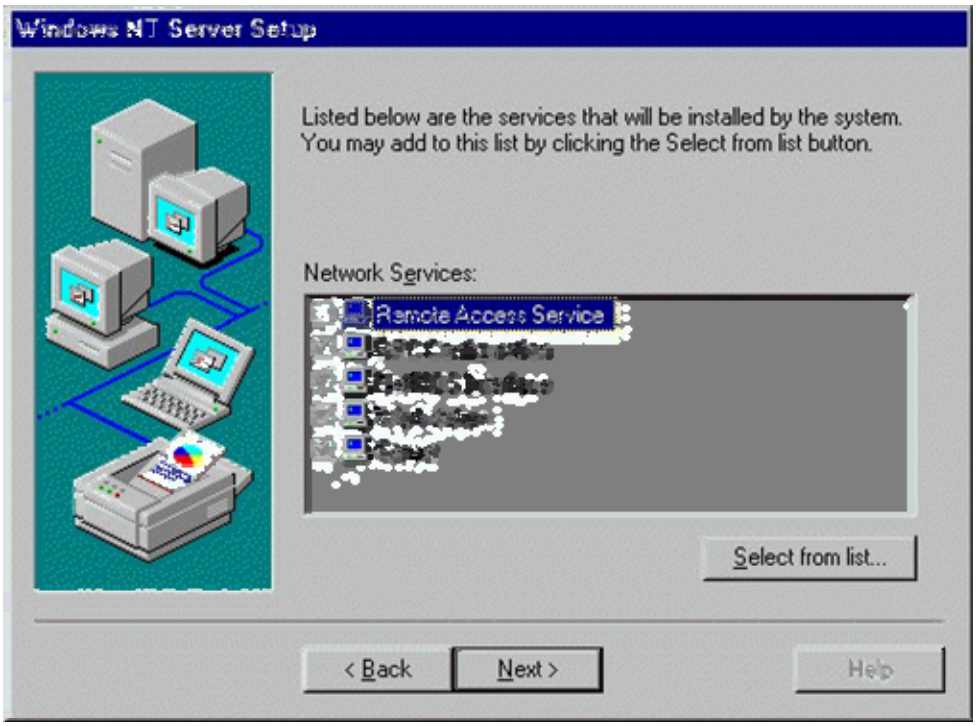
Máy trạm có thể được nối với server có dịch vụ RAS thông qua modem hoạc pull modem, cable null modem (RS232) hoặc X.25 network.

Khi đã cài đặt dịch vụ RAS, cần phải đảm bảo quyền truy nhập từ xa cho người sử dụng bằng tiện ích remote access amind để gán quyền hoặc có thể đăng ký người sử dụng ở remote access server. RAS cũng có cơ chế đảm bảo an toàn cho tài nguyên bằng cách kiểm soát các yếu tố sau: quyền sử dụng, kiểm tra mã số, xác nhận người sử dụng, đăng ký sử dụng tài nguyên và xác nhận quyền gọi lại.



*Hình 15.4: Mô hình truy cập từ xa bằng dịch vụ RAS*

Để cài đặt RAS chúng ta lựa chọn yêu cầu hộp Windows ả T server setup hiện ra lúc cài đặt hệ điều hành Windows ả T.




Với RAS tất cả các ứng dụng đều thực hiện trên máy từ xa, thay vì kết nối với mạng thông qua card mạng và đường dây mạng thì máy ở xa sẽ liên kết qua modem tới một RAS Server. Tất cả dữ liệu cần thiết được truyền qua đường điện thoại, mặc dù tốc độ truyền qua modem chậm hơn so với qua card mạng nhưng với những tác vụ của LAả  không phải bao giờ dữ liệu cũng truyền nhiều.

Với những khả năng to lớn của mình trong các dịch vụ mạng, hệ điều hành Windows ả T là một trong những hệ điều hành mạng tốt nhất hiện nay. Hệ điều hành Windows ả T vừa cho phép giao lưu giữa các máy trong mạng, vừa cho phép truy nhập từ xa, cho phép truyền file, vừa đáp ứng cho mạng cục bộ (LAả ) vừa đáp ứng cho mạng diện rộng (WAả ) như Intranet, Internet. Với những khả năng như vậy hiện nay hệ điều hành Windows ả T đã có những vị trí vững chắc trong việc cung cấp các giải pháp mạng trên thế giới.

HỌC VIỆN KỸ THUẬT QUÂN SỰ

TS VŨ MINH TIẾN (CHỦ BIÊN)
Th.S VŨ HỒNG GIANG, Th.S HOÀNG MINH TUẤN

# MẠNG MÁY TÍNH

**(Tài liệu dùng cho đào tạo Cao học các chuyên ngành Kỹ thuật và chuyên ngành Công nghệ Thông tin)**

LƯU HÀNH NỘI BỘ

NHÀ XUẤT BẢN QUÂN ĐỘI NHÂN DÂN
HÀ NỘI - 2002

*Chỉ đạo nội dung:*

BAN CHỈ ĐẠO NGHIÊN CỨU, BIÊN SOẠN, HOÀN THIỆN HỆ THỐNG TÀI LIỆU HUẤN LUYỆN, GIÁO TRÌNH, GIÁO KHOA - HỌC VIỆN KỸ THUẬT QUÂN SỰ.

Trưởng ban: Thiếu tướng, PGS-TS Nguyễn Đức Luyện

Phó trưởng ban: Đại tá, PGS-TS Phạm Huy Chương

Thư ký: Thượng tá, Th.S Nguyễn Văn Thàng

*Biên soạn:*

**Chủ biên:** TS Vũ Minh Tiến
**Tham gia biên soạn:** Th.S Vũ Hồng Giang, Th.S Hoàng Minh Tuấn

Quyết định ban hành
Số: 1374/QĐ-HV
Ngày 10 tháng 8 năm 2000

355 - 355.7
1412 - 2000
QĐND - 2001

# MỤC LỤC

MỤC LỤC ..... 5
LỜI NÓI ĐẦU ..... 9
**Chương 1**
GIỚI THIỆU MẠNG MÁY TÍNH ..... 10
1.1 Khái niệm mạng máy tính ..... 10
1.1.1. Định nghĩa ..... 10
1.1.2 Dịch vụ mạng ..... 11
1.2 Phân loại mạng máy tính ..... 15
1.2.1 Phân loại theo mô hình mạng ..... 15
1.2.2 Phân loại theo qui mô mạng ..... 17
1.2.3 Phân loại theo Tôpô mạng ..... 17
1.2.4 Phân loại theo hệ điều hành ..... 20
**Chương 2**
KIẾN THỨC CƠ SỞ CỦA MẠNG ..... 21
2.1 Môi trường truyền tin ..... 21
2.1.1 Các thông số cơ bản của đường truyền ..... 21
2.1.2 Vật tải truyền ..... 22
2.1.3 Tín hiệu trên đường truyền ..... 28
2.2 Sử lý các tập tin số ..... 38
2.2.1 Nguyên tắc kiểm tra lỗi ..... 38
2.2.2 Mã hoá và nén tin ..... 42
2.3 Máy tính và Khả năng truyền tin ..... 48
2.3.1 Cấu trúc máy tính ..... 48
2.3.2 Khả năng truyền tin của máy tính ..... 53
2.3.3 Nguyên tắc điều khiển thiết bị phần cứng trên Windows ..... 59
2.3.4 Card mạng (NIC) và cách nối ghép ..... 64
**Chương 3**
CÁC CHUẨN MẠNG ..... 66
3.1 Nhu cầu chuẩn hoá mạng ..... 66
3.2 Mô hình tham chiếu OSI ..... 67
3.2.1 Khái niệm về mô hình OSI 7 lớp ..... 67
3.2.2 Phương thức trao đổi thông tin trong mô hình OSI ..... 68
3.2.3 Tầng vật lý ..... 70

3.2.4 Tầng liên kết dữ liệu ..... 72
3.2.5 Tầng mạng ..... 81
3.2.6 Tầng vận chuyển ..... 88
3.2.7 Tầng phiên ..... 91
3.2.8 Tầng trình diễn ..... 92
3.2.9 Tầng ứng dụng ..... 93
3.3 Chuẩn IEEE 802 ..... 95

**Chương 4**

MẠNG CỤC BỘ LAN ..... 98
4.1 Tổng quan về mạng cục bộ ..... 98
4.2 Các phương pháp điều khiển truy nhập ..... 101
4.2.1 Phương pháp tranh chấp ..... 101
4.2.2 Phương pháp chuyển thẻ bài ..... 103
4.2.3 Phương pháp truy nhập ưu tiên theo yêu cầu ..... 106
4.3 Mạng Ethernet ..... 107
4.4 Mạng Token ring ..... 117
4.5 Hệ điều hành mạng ..... 123

**Chương 5**

CÁC BỘ GIAO THỨC CHUẨN ..... 127
5.1 Tổng quan về các giao thức ..... 127
5.2 Giao thức TCP/IP ..... 129
5.2.1 Tổng quan TCP/IP ..... 129
5.2.2 Giao thức TCP, UDP ..... 132
5.2.3 Giao thức IP ..... 135
5.2.4 Địa chỉ sử dụng trong TCP/IP ..... 138
5.3 Giao thức IPX/SPX ..... 141
5.4 Giao thức NETBEUI ..... 145
5.5 Các bộ giao thức khác ..... 146
5.5.1 Giao thức X25 ..... 146
5.5.2 Giao thức Frame relay ..... 148
5.5.3 Giao thức ATM ..... 149
5.5.4 Giao thức ISDN ..... 152

**Chương 6**

KẾT NỐI LIÊN MẠNG ..... 153
6.1 Các thiết bị kết nối liên mạng ..... 153
6.2 Các đường kết nối liên mạng ..... 160

6.3. Xác định hiệu năng mạng ..... 167
6.3.1. Xác định tốc độ mạng ..... 167
6.3.2. Tính theo từng loại mạng ..... 173
6.3.3. Đối với mạng truy nhập có điều khiển (Controlled access) ..... 175
6.3.4. Đối với mạng truy nhập ngẫu nhiên (Random access) ..... 178
6.3.5. Đối với mạng đa điểm - hai chiều đồng thời (multipoint-fult duplex) .. 179

**Chương 7**

INTERNET ..... 181
7.1. Lịch sử phát triển của Internet ..... 181
7.2. Cấu trúc của Internet ..... 186
7.2.1. Nhà cung cấp dịch vụ truy cập (IAP - Internet Access Provider) ..... 186
7.2.2. Nhà cung cấp dịch vụ thông tin Internet (ISP-Internet Service Provider) 186
7.2.3. Nhà cung cấp nội dung thông tin Internet (ICP) ..... 187
7.2.4. Người sử dụng Internet và phương thức truy cập ..... 188
7.2.5. Các tổ chức quản lý sự vận hành của Internet ..... 192
7.3. Công nghệ Internet ..... 192
7.3.1. Công nghệ triển khai áp dụng của IAP ..... 192
7.3.2. Công nghệ triển khai áp dụng của ICP ..... 193
7.3.3. Công nghệ triển khai áp dụng của ISP ..... 201
7.3.4. Các ví dụ minh hoạ thiết kế một số mạng ..... 203
7.4. Hệ thống các máy chủ ..... 205
7.4.1. Hệ thống máy chủ cung cấp các dịch vụ Internet ..... 206
7.4.2. Hệ thống máy chủ quản lý người dùng trong mạng ..... 206
7.4.3. Hệ thống máy chủ hỗ trợ chất lượng dịch vụ ..... 206
7.4.4. Hệ thống máy chủ bảo đảm an ninh và an toàn dữ liệu ..... 207
7.4.5. Hệ thống máy chủ giám sát và quản lý truy nhập ..... 208
7.4.6. Hệ thống máy chủ cung cấp dịch vụ truy cập từ xa ..... 208
7.4.7. Hệ thống máy chủ cung cấp các ứng dụng cơ sở dữ liệu ..... 209
7.4.8. Hệ thống máy chủ phục vụ in ấn ..... 209
7.4.9. Lựa chọn các máy tính làm máy chủ ..... 209
7.5. Các dịch vụ chính của Internet ..... 210
7.5.1. Thư tín điện tử (e-mail) ..... 210
7.5.2. Diễn đàn thông tin/NewsGroups ..... 211
7.5.3. Dịch vụ tuyền tệp FTP (File Transfer Protocol) ..... 213
7.5.4. Dịch vụ truy nhập máy chủ (Telnet) ..... 213
7.5.5. World Wide Web (WWW) ..... 213

7.6. Một số kiến thức liên quan ..... 214
7.6.1. QoS (Quality of Service) ..... 214
7.6.2. xDSL ..... 217
7.6.3. VoIP (Voice over IP) ..... 227
7.6.4. IP Routing ..... 233
**Chương 8**
AN NINH MẠNG ..... 241
8.1 Các hiểm hoạ trên mạng máy tính ..... 241
8.2 Các biện pháp bảo vệ và phòng ngừa ..... 247
8.2.1 Các chiến lược an toàn thông tin ..... 247
8.2.2 Các mức bảo vệ an toàn mạng ..... 249
**Tài liệu tham khảo ..... 255**

# LỜI NÓI ĐẦU

Sự phát triển của công nghệ thông tin (CNTT) đã dẫn đến cuộc cách mạng thứ 3 trong lịch sử văn minh loài người - Cách mạng thông tin. CNTT đã trở thành một nguồn lực quan trọng của mỗi quốc gia, cùng với tài lực và vật lực, CNTT trở thành 1 trong 4 nhân tố quyết định cho sự phát triển. Nền tảng cơ bản của CNTT là máy tính và sự kết nối giữa chúng tạo thành mạng. Mạng máy tính trong phạm vi nhỏ là mạng cục bộ, lớn hơn là mạng diện rộng thuộc một ngành, một quốc gia và lớn hơn nữa là mạng INTERNET kết nối các máy tính toàn cầu. Các mạng máy tính đã làm thay đổi một cách toàn diện phương thức sống, làm việc và sinh hoạt của con người, cũng như phương thức tổ chức và phát triển xã hội. Nhịp độ sử dụng ngày càng tăng các mạng máy tính để trao đổi thông tin, xử lý thông tin trong cuộc sống, trong các tổ chức và đặc biệt trong quân sự như các hệ thống điều khiển, chỉ huy, tính toán, viễn thông, tình báo... Mạng máy tính chính là một trong những giải pháp, phương tiện và mục tiêu hướng tới hiện đại hóa quân đội.

Giáo trình này cho một cách nhìn tổng quan về các mạng máy tính, các thiết bị nối ghép các mạng, các giao diện dùng trong hệ thống mạng đồng thời còn đề cập đến một số phương pháp xây dựng và quản lý các hệ thống xử lý tin lớn. Nó chủ yếu dùng để phục vụ cho học viên cao học các ngành không chuyên tin học có những khái niệm ban đầu về mạng máy tính. Tài liệu gồm 8 chương, giới thiệu những khái niệm cơ bản về mạng, kiến trúc phân tầng- mô hình OSI, môi trường truyền, tôpô mạng, các giải pháp truyền dữ liệu, một số giao thức chính thường sử dụng, các thiết bị kết nối mạng, các phương thức và giải pháp điều hành mạng, giới thiệu tổng quan một số khái niệm về mạng LAN, Internet và đề cập đến vấn đề an ninh, an toàn mạng.

Tập thể nhóm biên tập chân thành cảm ơn các cán bộ nghiên cứu và giảng dạy của Trung tâm Kỹ thuật điện tử-tin học (EIC), Công ty AIC, Phòng Sau đại học Học viện Kỹ thuật Quân sự, cùng các cơ quan hữu quan khác đã góp công sức và tạo điều kiện để tài liệu này đến được bạn đọc.

Do hạn chế về thời gian và kinh nghiệm, cuốn sách không thể tránh khỏi những thiếu sót nhất định. Vì vậy, rất mong nhận được ý kiến đóng góp của các bạn đồng nghiệp và đọc giả gần xa để có thể hoàn thiện hơn nữa cho lần tái bản sau.

*Hà Nội, tháng 4/2002*

**Vũ Minh Tiến**

# CHƯƠNG 1

# GIỚI THIỆU MẠNG MÁY TÍNH

## 1.1 Khái niệm mạng máy tính

### 1.1.1. Định nghĩa

Có rất nhiều các giải nghĩa khác nhau về mạng máy tính song một định nghĩa cơ bản nhất về mạng máy tính được phát biểu như sau: *Mạng máy tính là mạng bao gồm ít nhất hai máy tính được kết nối với nhau thông qua một đường truyền vật lý cho phép chúng chia sẽ dữ liệu và tài nguyên.* Tất cả các mạng máy tính lớn hiện nay đều xuất phát từ hệ thống đơn giản như vậy, ý tưởng kết nối hai máy tính qua đường truyền cáp có vẻ như bình thường nhưng đó lại là thành tựu quan trọng trong ngành truyền thông. Do các máy tính hiện nay trên thế giới có rất nhiều các chủng loại khác nhau, được dùng theo các cách khác nhau (chi tiết ở mục 2.3.1) và có thể nằm theo các cự ly khác nhau, cho nên để các máy tính truyền thông được với nhau phải liên quan đến nhiều công nghệ phức tạp.

Trong một mạng máy tính, các máy tính kết nối trên đường truyền vật lý này phải tuân theo một loạt các quy tắc truyền thông chung thì dữ liệu mới đến được đích và các máy tính gửi và nhận mới hiểu được nhau. Các quy tắc điều hành tiến trình truyền thông máy tính được gọi là giao thức [protocols].

Như vậy để hiểu kỹ hơn về mạng máy tính, chúng ta cần nghiên cứu kỹ các yếu tố cấu thành của mạng:

- Cách tổ chức chia sẻ tài nguyên (dịch vụ mạng).
- Cách tổ chức một đường vật lý (vật tải truyền).
- Các quy tắc truyền thông (giao thức).

Mạng máy tính ngày càng được sử dụng rộng rãi và đang đóng một vai trò quan trọng trong việc thúc đẩy sự phát triển nền kinh tế của nước ta. Tác dụng của mạng máy tính được tóm tắt như sau:

- Tận dụng tài nguyên chung (phần cứng, phần mềm và dữ liệu...)
- Chinh phục khoảng cách.
- Tăng chất lượng, hiệu quả trong khai thác và xử lý thông tin.

- Tăng độ tin cậy của hệ thống nhờ khả năng thay thế khi có sự cố với một nút hay một đoạn đường nào đó.

### 1.1.2 Dịch vụ mạng

Để có thể hiểu kỹ hơn về khả năng của mạng máy tính ta sẽ xem xét các dịch vụ mạng, đó là cách mà mạng máy tính cung cấp cho phép máy tính chia sẻ các tài nguyên của mình cho các máy tính khác. Các dịch vụ mạng phổ biến nhất là:

- Dịch vụ tập tin
- Dịch vụ in
- Dịch vụ thông điệp
- Dịch vụ thư mục
- Dịch vụ ứng dụng
- Dịch vụ cơ sở dữ liệu

**1. Các dịch vụ tập tin** [file services] cho phép các máy tính trên mạng chia sẻ các tập tin. Nhu cầu trao đổi các tập tin giữa các máy tính là rất cao, mặc dù vấn đề này có thể giải quyết bằng cách trao đổi các đĩa chứa các tập tin, song không mấy tiện dụng. Quan trọng hơn, người dùng cần chia sẻ dữ liệu trong các tập tin cơ sở dữ liệu chung, một công việc chỉ có thể thực hiện trên mạng. Đây chính lý do thúc đẩy việc kết mạng các máy tính cá nhân. Các dịch vụ tập tin bao gồm:

- Chuyển giao tập tin
- Lưu trữ tập tin
- Di trú dữ liệu
- Lưu dự phòng tập tin
- Đồng bộ hoá tiến trình cập nhật dữ liệu

Hầu hết các mạng máy tính đều có ít nhất một cơ chế lưu trữ tập tin tập trung nào đó. Có hai chế độ lưu trữ: Trực tuyến và ngoại tuyến. Lưu trữ trực tuyến là dữ liệu được lưu trữ trên các đĩa cứng và có thể truy cập theo nhu cầu. Lượng không gian đĩa cứng sẽ là giới hạn truy cập của các tập tin trên máy chủ. Đối với các mạng có cơ sở dữ liệu lớn có cách tiếp cận khác để lưu trữ tập tin đó là kho lưu trữ ngoài truyến [offline storage], bao gồm băng từ và đĩa quang. Sau khi dữ liệu được ghi ra băng từ hay đĩa quang, ta có thể tháo nó ra khỏi máy chủ để cất vào chỗ chứa. Những ai yêu cầu dữ liệu ngoài tuyến cần phải định danh băng từ hay đĩa chứa dữ liệu yêu cầu. Nếu trường hợp kho lưu trữ ngoài tuyến đáp ứng quá chậm, ta có thể dùng kỹ thuật kho lưu trữ cận tuyến [near-line storage]. Kho lưu trữ cận tuyến sử dụng một máy, có tên "máy phát theo yêu cầu" [jukebox] để tự động quản lý các số lượng băng từ hay đĩa quang. Máy phát này sẽ truy lục cuộn băng hay đĩa mà không cần có sự can thiệp của con người. Với kiểu kho lưu

trữ cận tuyến, chỉ cần chờ trong giây lát là có ngay các lượng dữ liệu khổng lồ, trong khi chi phí lại thấp hơn nhiều so với các ổ đĩa cứng.

**Đồng bộ hoá việc cập nhật tập tin:** Theo dạng thức đơn giản nhất, đồng bộ hoá tiến trình cập nhật tập tin [update synchroniszation] là một biện pháp bảo đảm tất cả mọi người dùng đều có bản sao mới nhất của tập tin. Các dịch vụ đồng bộ hoá tiến trình cập nhật tập tin có thể quản lý các tập tin bằng cách giám sát các tem ngày giờ để xác định tập tin nào được lưu cận nhất. Nhờ theo dõi người dùng truy cập tập tin, kèm với các tem ngày giờ, dịch vụ đó có thể cập nhật tất cả mọi bản sao tập tin theo phiên bản cận nhất. Tuy nhiên, việc đồng bộ hoá tiến trình cập nhật tập tin rất phức tạp vì không phải lúc nào cũng để mọi người dùng truy cập tất cả các tập tin theo thời gian thực. Việc đồng bộ hoá tiến trình cập nhật tập tin trở nên gây cấn hơn khi có thêm người dùng đồng thời chia sẻ các tập tin dữ liệu. Phải thiết lập các cơ chế để bảo đảm người dùng không vô tình ghi đè lên dữ liệu của nhau. Trong vài trường hợp, hệ thống đơn giản gán cờ cho các tập tin có nhiều đợt cập nhật xung đột và yêu cầu con người ra tay hoà giải những điểm khác biệt.

**2. Dịch vụ in**

Tiến trình in mạng là yếu tố thứ hai thúc đẩy ta cài đặt các mạng máy tính. Các ưu điểm của tiến trình in trên mạng có thể mô tả như sau:

Nhiều người có thể chia nhau dùng chung máy in- một khả năng đặc biệt hữu ích đối với các thiết bị đắt tiền, như các máy vẽ và máy in màu.

Các máy in có thể đặt bất kỳ đâu, chứ không chỉ đặt cạnh PC của người dùng.

Tiến trình in mạng dựa trên hàng đợi thường hiệu quả hơn so với in trực tiếp bởi trạm làm việc có thể bắt đầu làm việc trở lại ngay khi khối in được xếp hàng trên mạng.

Các dịch vụ in hiện đại có thể cho phép người dùng gửi các phiên truyền fax đến một máy chủ fax thông qua mạng.

Trong tập sách này, các dịch vụ in được định nghĩa như là những ứng dụng mạng điều khiển và quản lý việc truy cập các máy in, máy fax mạng, và các dịch vụ tương tự khác.

**3. Các dịch vụ thông điệp** bao gồm :

- Thư điện tử
- Thư thoại và thư điện tử tích hợp
- Các ứng dụng hướng đối tượng
- Các ứng dụng nhóm làm việc

**Thư điện tử** (hoặc e-mail) là công nghệ để chuyển giao các thông điệp giữa các máy tính nối mạng. Các hệ thư điện tử có thể phục vụ cho mọi đối tượng, từ một nhóm làm việc cục bộ, đến một công ty, hay toàn thế giới. Nhờ cài đặt các thiết bị định tuyến [routing devices] thư điện tử, ta có thể chuyển giao thư từ suôn sẻ và hữu hiệu giữa các mạng máy tính (LAN). Hệ thư điện tử khổng lồ nhất có lẽ nằm trên Internet, nó cho phép người dùng của hàng chục quốc gia trên thế giới trao đổi các thông điệp điện tử dễ dàng hơn so với việc gửi thư bằng giấy.

Dạng thư điện tử đầu tiên là gốc văn bản, hiện nay được phát triển kèm theo các hệ thống hỗ trợ nhúng âm thanh, đồ hoạ, và thậm chí các dữ liệu video. Các hệ thư điện tử hiện đại cũng cho phép các hệ khách di động "gọi đến" để gửi và nhận thư. Các công nghệ gửi thông điệp mới hệ thư thoại [voice mail] không chỉ đơn thuần là một hệ trả lời điện thoại đơn giản. Bởi bản thân các hệ thư thoại dựa vào máy tính, nên chúng có thể liên kết với các mạng và các dịch vụ thông điệp có thể quản lý dữ liệu thoại chung cuộc, điều này cho phép nhiều hệ thư thoại và thư điện tử tương hoạt và tự do trao đổi dữ liệu.

Ngày nay, người dùng điện thoại di động có thể gửi [forward] các thông điệp thư điện tử của mình cho hệ thư thoại. Sau đó, họ có thể gọi đến và để một hệ nhận dạng văn bản đọc các thông điệp bằng điện tử. Một cách khác, có thể dùng các thiết bị nhận dạng tiếng nói để đọc thư thoại của người dùng rồi chuyển đổi nó thành thông điệp thư điện tử gốc văn bản.

**Bản chất các ứng dụng hướng đối tượng là** có thể dùng các dịch vụ thông điệp như những công cụ trung gian cho phép các đối tượng trên mạng truyền thông. Để đạt được điều này, các ứng dụng dịch vụ thông điệp tác động như những tác nhân của các đối tượng. Đối tượng chỉ việc bàn giao dữ liệu cho một tác nhân, và rồi tác nhân này sẽ chịu trách nhiệm bàn giao dữ liệu cho đối tượng đích. Điều này khiến cho các đối tượng không cần phải có khả năng truyền thông với mọi đối tượng khác trên mạng

**Các ứng dụng nhóm làm việc** [workgroup applications] dùng các dịch vụ mạng để cải tiến việc truyền thông trong các nhóm làm việc. Có hai kiểu ứng dụng nhóm làm việc: ứng dụng quản trị luồng công việc và các tư liệu nối kết đối tượng:

- Các ứng dụng quản trị luồng công việc [workflow management applications] sẽ định tuyến các tư liệu và biểu mẫu điện tử giữa các người dùng trong nhóm làm việc. Khi các chữ ký điện tử đáng tin cậy được bổ sung vào tiến trình, ta có thể thay thế nhiều tiến trình vẫn thường được tiến hành trên giấy tờ truyền thống.
- Các tư liệu nối kết đối tượng: Các tư liệu không nhất thiết chỉ là những tập tin thuần văn bản. Các tư liệu hiện đại có thể chứa nhiều kiểu đối tượng khác nhau, kể cả văn

bản, đồ hoạ, âm thanh, tiếng nói, dữ liệu bảng tính, và video. Có thể kết hợp nhiều kiểu đối tượng khác nhau để xây dựng các tư liệu. Các đối tượng không chỉ đơn thuần là dữ liệu. Một đối tượng được nhúng trong tư liệu sẽ có một cấp độ thông minh cho phép nó chuyển các thông điệp đến hệ điều hành và đến các tư liệu khác.

**4. Dịch vụ thư mục**

Dịch vụ thư mục tích hợp mọi thông tin về các đối tượng trên mạng thành một cấu trúc thư mục chung. Các đối tượng mạng có thể tham khảo thư mục để định danh và trao đổi các thông điệp với các đối tượng khác trên mạng. Bản thân các đối tượng không cần biết địa chỉ, vị trí, hoặc dạng thức thông điệp cần thiết để truyền thông, dịch vụ thư mục sẽ cung cấp toàn bộ thông tin này.

Các dịch vụ thư mục có thể đơn giản hoá đáng kể các khối lượng công việc trên mạng. Giả sử một mạng có hai máy chủ tập tin và một máy chủ thư điện tử. Nếu không có dịch vụ thư mục, điều hành viên mạng phải quản lý các tài khoản người dùng trên các máy chủ đó một cách độc lập. Với các dịch vụ thư mục, họ có thể quản lý cả ba máy chủ chỉ bằng một cấu trúc thư mục.

Cấu trúc thư mục che giấu cấu trúc vật lý của mạng để tránh các ứng dụng và người dùng dòm ngó. Máy chủ in đơn giản là một thành phần của mạng, nó không phải là một dịch vụ do một máy tính cụ thể cung cấp.

**5 Các dịch vụ ứng dụng**

Các dịch vụ ứng dụng [application services] cho phép các ứng dụng huy động năng lực tính toán và các khả năng chuyên môn của các máy tính khác trên mạng. Ví dụ, các ứng dụng kinh doanh thường phải thực hiện các phép tính thống kê phức hợp vượt quá hoạt vi của hầu hết các PC để bàn. bình thường phải dùng máy tính lớn hay máy tính mini Unix để chạy phần mềm thống kê này. Nhờ sử dụng dịch vụ ứng dụng trên mạng ta có thể để kết chùm các máy tính PC thành một máy tính lớn (Máy tính song song) có hiệu năng tương đương hoặc cao hơn các máy tính lớn (Main-frame) đảm bảo giải quyết các bài toán lớn trên nền mạng máy tính PC.

Các máy chủ ứng dụng là một chiến lược hiệu quả để linh động hoá qui mô của một mạng. Có thể bổ sung các máy chủ ứng dụng mới khi các kiểu nhu cầu ứng dụng mới nảy sinh. Nếu cần thêm năng lực cho ứng dụng, ta chỉ cần nâng cấp máy chủ ứng dụng đó. Ví dụ, một máy chủ cơ sở dữ liệu có thể bành trướng từ một máy PC thành một hệ RISC đa bộ xử lý chạy unix mà không cần thay đổi nhiều (thậm chí không hề phải thay đổi) các máy PC khách.

**6 Các dịch vụ cơ sở dữ liệu**

Các dịch vụ cơ sở dữ liệu [database services] là ví dụ phổ biến nhất về các máy chủ ứng dụng. Do các máy chủ cơ sở cho phép thiết kế các ứng dụng theo các thành phần hệ khách và hệ chủ tách biệt, nên chúng thường được gọi là cơ sở dữ liệu khách/chủ [client/server databases]. Với cơ sở dữ liệu khách/chủ, ta có thể thiết kế các ứng dụng khách và ứng dụng phục vụ để vận dụng các khả năng chuyên môn của các hệ cơ sở dự liệu và hệ khách

Các cơ sở dữ liệu phân phối đang ngày càng phổ dụng. Chúng cho phép lưu trữ các phần của các cơ sở dữ liệu trên các máy chủ tách biệt, có thể đặt tại các vị trí địa lý khác nhau. Kỹ thuật này có tên là dữ liệu phân phối. Đối với người dùng nó giống như một cơ sở dữ liệu lôgic đơn lẻ, song lại đặt dữ liệu mà họ cần tại một vị trí dễ truy cập nhất. Ta phải áp dụng các cơ chế cơ sở dữ liệu đặc biệt để duy trì tính đồng bộ của dữ liệu trong các bản sao cơ sở dữ liệu. Các cơ sở dữ liệu có thể được sao lặp [replicated]; các bản sao hoàn chỉnh của cơ sở dữ liệu có thể được lưu trữ tại nhiều vị trí khác nhau. Khả năng này tạo ra một nhân tố dôi, bởi tai hoạ ắt không thể cùng lúc đổ ập lên tất cả mọi bản sao. Ngoài ra tính năng sao lặp cơ sở dữ liệu cũng cải thiện thời gian đáp ứng ứng dụng bởi người dùng có thể truy cập cục bộ cơ sở dữ liệu thay vì phải thông qua một WAN tương đối chậm.

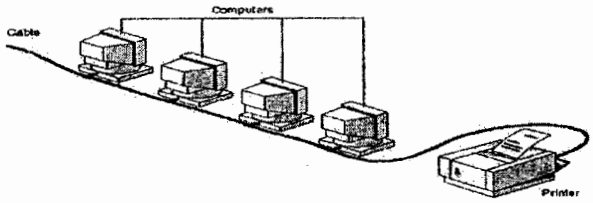
## 1.2 Phân loại mạng máy tính

### 1.2.1 Phân loại theo mô hình mạng

***Loại mạng bình đẳng*** hay còn gọi là mạng peer to peer (hình 1.1). Mạng bình đẳng là mạng trong đó các máy có vai trò ngang nhau trong quá trình khai thác tài nguyên, máy này có thể yêu cầu máy kia cung cấp tài nguyên và ngược lại. Không máy nào được coi là máy chủ hay máy trung tâm.

Trong môi trường mạng bình đẳng, người dùng trên từng PC chịu trách nhiệm việc điều hành và chia sẻ các tài nguyên PC của họ. (Tính năng này được gọi là điều hành nhóm làm việc hoặc điều hành phân tán).

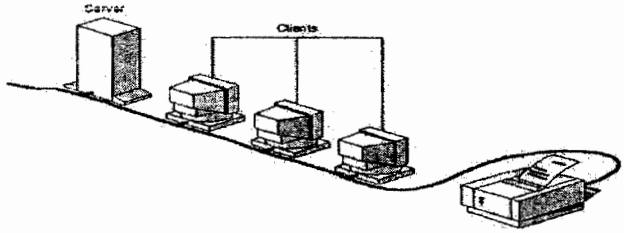
Các mạng bình đẳng rất phù hợp với các tổ chức nhỏ có số người dùng giới hạn và không đặt nặng vấn đề bảo mật. Cũng có thể dùng các mạng bình đẳng như một phương án tản quyền [decentralized] trong các tình huống ở đó việc điều hành máy chủ là một công việc không quá lớn hoặc quá phức tạp.




**Hình 1.1 Mô hình mạng bình đẳng (Peer to Peer).**

- ***Loại mạng theo mô hình khách/chủ*** (client/Server). Mạng client/ server (hình 1.2) là hệ thống mạng có ít nhất một máy gọi là máy chủ (Server), đó là máy có cài đặt phần mềm điều hành hệ thống của mạng, máy này có chức năng điều khiển và cung cấp, phân chia tài nguyên theo yêu cầu của máy khác. Điển hình của loại mạng này là mạng Novell. Dưới mô hình khách/phục vụ, các tài nguyên phần cứng có thể được tập trung trên tại máy chủ, và các máy khách có thể được thiết kế theo các cấu hình phần cứng tối thiểu.

Mô hình mạng khách/ phục vụ tỏ ra lý tưởng đối với các mạng lớn cần đến hệ bảo mật mạng. Dưới mô hình khách/chủ, một điều hành viên mạng có thể dễ dàng điều khiển việc truy cập các tài nguyên mạng. Thông qua hệ điều hành mạng, điều hành viên có thể giao hoặc thu hồi giấy phép [permission] truy cập các tập tin, máy in, và các tài nguyên khác trên máy chủ.




**Hình 1.2. Mô hình mạng khách chủ (Client/ server).**

***Loại mạng hỗn hợp*** ( Kết hợp mạng bình đẳng và mạng khách/ chủ). Mạng hỗn hợp là mạng mà trong quá trình khai thác tài nguyên các máy có lúc quan hệ với nhau bình đẳng, có lúc quan hệ với nhau theo kiểu khách chủ. Nhiều môi trường mạng sử dụng cả hai mô hình mạng. Ví dụ, một tổ chức có thể dùng đồng thời các hệ điều hành Netware khách/phục vụ của Novell và Windows for Workgroups bình đẳng của Microsoft. Các hệ điều hành vi tính mới như Microsoft Windows 95/98 hoặc Microsoft Windows 2000 sử dụng cả hai mô hình mạng.

### 1.2.2 Phân loại theo qui mô mạng

Nếu lấy khoảng cách địa lý làm yếu tố chính để phân loại thì ta có mạng cục bộ, mạng đô thị, mạng diện rộng

***Mạng cục bộ*** (Local Area Networks- LAN): Là mạng được cài đặt trong một phạm tương đối nhỏ như trong một toà nhà, trong một trường học...với khoảng cách giữa các máy tính nút mạng chỉ trong vòng vài chục ki-lô-mét trở lại.

***Mạng đô thị*** (Metropolitan Area Networks - MAN): là mạng được cài đặt trong phạm vi một đô thị hoặc một trung tâm kinh tế- xã hội có bán kính khoảng 100 ki-lô-mét trở lại.

***Mạng diện rộng*** (Wide Area Networks - WAN): là mạng được cài đặt có qui mô lớn nó được tạo thành nhờ ghép nối nhiều mạng LAN lại với nhau và phải sử dụng đến các thiết bị viễn thông, không có trong mạng cục bộ như brigde, getway, Modem...Mạng Internet, Intranet cũng là những hệ thống thuộc khái niệm mạng WAN.

### 1.2.3 Phân loại theo Tôpô mạng

***- Mạng trục ( Bus)*** : cấu trúc của mạng là dùng một BUS thông tin chung để trao đổi thông tin giữa các nút bất kỳ của mạng. Các nút thông tin (các trạm cuối) có thể thâm nhập ở bất cứ vị trí nào trên mạng. Do vậy BUS thông tin còn được gọi là trục hay xương sống của mạng. Điều khiển mạng có thể được thực hiện theo phương pháp tập trung (từ một nút chính) hay theo phương pháp phân bố. Xu hướng chính hiện nay là điều khiển theo phương pháp phân bố.

Mạng hình BUS được dùng phổ biến trong các LAN, như mạng TRANS-NET, ETHERNET, D-LINK,...

Ưu điểm của mạng hình BUS là:

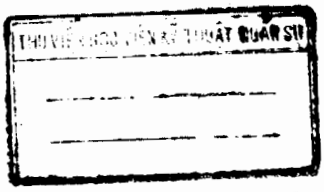
Các thiết bị của các nút thông tin có thể thao tác độc lập, sai hỏng của một máy không ảnh hưởng tới toàn mạng.

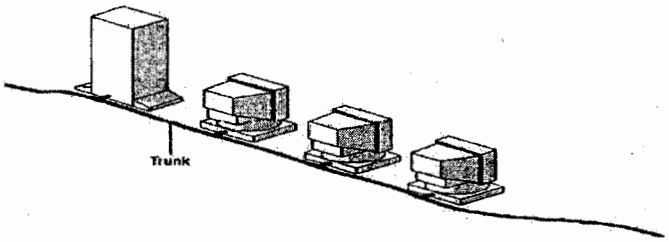
Mở rộng hay thu hẹp mạng có thể thực hiện một cách đơn giản.

Mạng BUS sử dụng ít dây nhất so với các mạng khác.

Nhược điểm của mạng hình BUS là:

- Nếu chỉ một điểm trên BUS bị hỏng thì toàn bộ thông tin của mạng sẽ dừng lại.
- Phương pháp thâm nhập mạng yêu cầu phức tạp hơn để đảm bảo tránh sự chồng chéo số liệu (collision of data) gây ra do nhiều trạm cùng phát số liệu đồng thời. Chính điều này đã hạn chế nút thông tin trên mạng.






**Hình 1.3. Mạng sơ đồ hình BUS**

Mạng hình BUS có thể dùng các loại dây nối như, cáp đồng trục, cáp sợi quang. Về phương pháp thâm nhập cho mạng hình BUS phải giải quyết vấn đề chồng chéo số liệu và giải quyết vấn đề nhiễu nên phần lớn các LAN kiểu BUS này sử dụng phương pháp thâm nhập CSMA/CD protocol (Carrier sence multiple access/ collision detection) hay phương pháp thâm nhập dùng token passing.

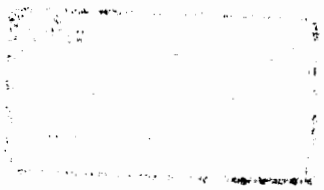
- ***Mạng hình sao (Star)*** : mạng hình sao bao gồm một trung tâm điều khiển và các nút thông tin. Các nút thông tin chính là các trạm đầu cuối, các máy vi tính... của mạng. Trung tâm điều khiển mạng điều phối mọi hoạt động trong mạng. Hiện nay người ta sử dụng trung tâm điều khiển như một đầu nối giữa các máy tính với nhau. HUB cũng chính là một trung tâm điều khiển.

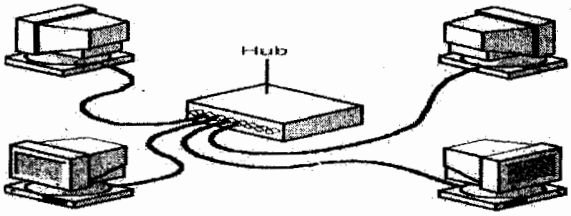
Mạng sao có các ưu điểm chính như sau:

- Hoạt động theo nguyên lý độc lập nên một trạm bị sai hỏng thì mạng vẫn hoạt động bình thường.
- Cấu trúc mạng đơn giản, các thuật toán điều khiển ổn định.
- Mạng có thể mở rộng hay thu hẹp khá thuận lợi và đơn giản.
- Mạng STAR tiếp nhận tất cả các phương thức thâm nhập mạng khác nhau.

Nhược điểm của mạng sao:

Khi trung tâm điều khiển có sự cố thì toàn mạng sẽ ngừng hoạt động. Mạng yêu cầu phải nối từng cặp dây từ trung tâm điều khiển tới các máy tính.



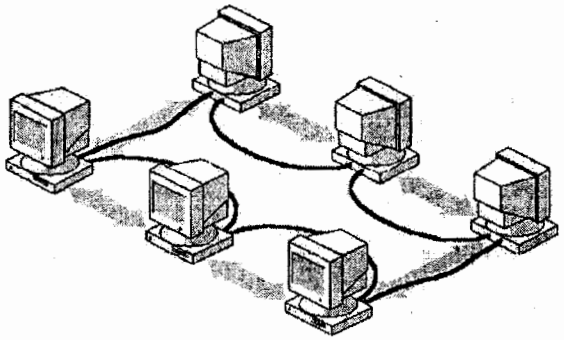



**Hình 1.4. Mạng hình sao**

***Mạng vòng (Ring)***: Các thiết bị đầu cuối hay các máy tính có thể được kết nối tại bất cứ vị trí nào trên BUS vòng tròn của mạng theo kiểu nối tiếp nhau. Vòng tròn này thực chất là một cáp thông tin nối khép kín không có điểm đầu, điểm cuối.

Ưu điểm của mạng vòng: Điều khiển hệ thống đơn giản và giảm nhiều khả năng chồng chéo thông tin vì thông tin chạy trên mạng theo một chiều duy nhất. Tiết kiệm dây dẫn hơn mạng Sao và khi qua mỗi nút thông tin thì các mạng được phục hồi và khuếch đại lên vì vậy khoảng cách giữa các nút thông tin có thể được tăng lên.

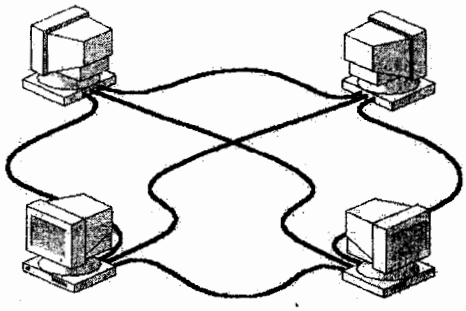
Nhược điểm của mạng vòng: Nếu một nút thông tin nào đó bị hỏng, nó ảnh hưởng tới toàn bộ các nút tiếp theo sau nó (theo chiều truyền của số liệu). Việc nối dây sẽ yêu cầu phức tạp hơn để bảo đảm cho các nút hoạt động tin cậy.



**Hình 1.5. Mạng hình vòng**

***Mạng hình lưới :*** Một mạng theo dạng lưới (hình 1.6) đảm bảo độ dự phòng và độ tin cậy cao hơn nhiều so với các cấu trúc khác. Trong cấu hình này, mỗi máy tính được nối tới mỗi máy tính khác bằng dây cáp riêng biệt. Cấu hình này cung cấp những đường dẫn dự phòng thông qua toàn bộ cấu trúc mạng, nên nếu có một đoạn cáp nào đó

bị hỏng, thì các cáp khác sẽ chịu trách nhiệm chuyển tải thông tin. Trong cấu hình này sẽ giảm nhẹ việc dò lỗi trên mạng và tăng độ tin cậy nhưng giá thành lắp đặt sẽ cao do chúng sử dụng nhiều dây cáp. Thường Mạng hình lưới thường được dùng kết hợp với các Tôpô mạng khác tạo ra các cấu trúc kết hợp (lai) khác nhau.



**Hình 1.6 Mạng hình lưới**

### 1.2.4 Phân loại theo hệ điều hành

Trong nhiều trường hợp người ta lấy tên của hệ điều hành mạng hoặc hệ điều hành môi trường sử dụng mạng làm tên của mạng. Hệ điều hành điểm - điểm (Peer to Peer) và Hệ điều hành khách chủ :

Hệ điều hàng theo mô hình khácli/chủ

- Mạng UNIX, Linux .....
- Novell NetWare
- Banyan VINES
- Open VMS
- IBM OS/2 LAN Server
- Microsoft Windows NT Server. Windows 2000...

Hệ điều hành theo mô hình bình đẳng:

- Novell Personal NetWare
- Microsoft Windows for Workgroups và Windows NT
- AppleTalk ( hệ mạng cho các máy tính Apple Macintosh)
- ArtisoftLANtastic...

# CHƯƠNG 2

# KIẾN THỨC CƠ SỞ CỦA MẠNG

## 2.1 Môi trường truyền tin

### 2.1.1 Các thông số cơ bản của đường truyền

**Độ suy hao:**

Tín hiệu trên đường dây bị suy giảm trong quá trình truyền tin. Để khắc phục ta dùng các bộ khuyếch đại. Độ suy giảm được tính bằng đơn vị decibel. Nếu điện thế ban đầu là $V_1$ và sau đó giảm xuống $V_2$ thì số decibel của độ suy hao được định nghĩa như sau:

$$S\,(decibel\quad) = 20\ \log_{10}\frac{V_1}{V_2}$$

Suy dần là lý do thứ hai mà các thiết kế cáp phải chỉ định các giới hạn về chiều dài chạy cáp. Khi cường độ tín hiệu tụt xuống dưới một số giới hạn nhất định, các thiết bị điện tử đang nhận tín hiệu sẽ khó lòng cô lập tín hiệu ban đầu với âm nhiễu hiện diện trong mọi phiên truyền điện tử.

**Độ nhiễu**

Điện từ trường trong môi trường truyền tin gây nhiễu cho các tín hiệu mang thông tin. Để khắc phục ta dùng các bộ lọc nhiễu. Để đặc trưng độ nhiễu trên đường dây, ta dùng tỷ số tín hiệu / tạp âm (Signal/Noise - S/N):

$$\frac{S}{N}(decibel\quad) = 10\ \log_{10}\frac{S}{N}$$

Tỉ lệ lỗi bít là một kết quả cho biết tỉ lệ của dữ liệu bị lỗi so với dữ liệu truyền đi, nó được tính bằng % bít lỗi so với tổng số bit truyền đi.

$$\text{Tỉ lệ lỗi bít} = \frac{\text{Số bít lỗi}}{\text{Tổng số bít truyền đi}}$$

Ví dụ: Một thông báo được truyền đi trên một đường với tỉ lệ lỗi bít là 1/500,000. Thông báo được truyền dẫn có 100 ký tự (mỗi ký tự có 8 bít), nó được tính toán là số thông báo trung bình được truyền đi trước khi có một lỗi bít được tìm thấy.

Số bít trong một thông báo

= 100 ký tự/thông báo X 8 bit/ký tự

= 800 bít/thông báo

Tỉ lệ lỗi bít = 1/500,000 → trung bình 1 bít lỗi được tìm thấy khi có 500,000 bít được truyền đi. Số thông báo trung bình được truyền đi trước khi có một lỗi bít được tìm thấy

= số bít trước khi tìm thấy lỗi / số ký tự trong một thông báo

= 500,000 bít / 800 bít/thông báo

= 635 thông báo

**Băng thông.**

Trong lĩnh vực mạng máy tính, thuật ngữ băng thông [bandwidth] có nghĩa là số đo công suất của một vật tải để truyền dữ liệu. Một vật tải có công suất cao sẽ có băng thông cao. Một vật tải có công suất hạn chế sẽ có băng thông thấp.

Có thể ví băng thông như các vòi nước. Nếu một vòi nước vườn đường kính nửa inch có thể tải luồng từ nhỏ giọt lên đến băng thông hai $cm^3$/ phút, thì có thể xem vòi nước đó có được băng thông hai $cm^3$ / phút. Tuy nhiên, một vòi rồng chữa cháy bốn inch có thể có một băng thông vượt quá mức 100 $cm^3$/phút.

Các tốc độ truyền số liệu thường được phát biểu dưới dạng các bit có thể truyền mỗi giây. Trên lý thuyết, một LAN Ethernet có thể truyền mỗi giây. Trên lý thuyết, một LAN Ethernet có thể truyền 10 triệu bit/giây và có một băng thông 10 Mbps..

Băng thông của một cáp phần nào được xác định bởi chiều dài cáp. Một đoạn cáp ngắn thường có băng thông lớn hơn một đoạn cáp dài, và là một lý do mà mọi thiết kế cáp chỉ định các chiều dài tối đa để chạy cáp. Nếu vượt quá các giới hạn này, các tín hiệu tần số cao nhất có thể bị hỏng và có thể bắt đầu xảy ra lỗi trong các tín hiệu dữ liệu.

**Nhiễu điện từ**

Nhiễu điện từ [electromagnetic interference-EMI] bao gồm các âm nhiễu điện từ bên ngoài làm biến dạng tín hiệu trong một vật tải. Khi nghe một đài phát thanh AM, ta thường nghe âm nhiễu do các động cơ hay tia chớp gây ra. Đây là một ví dụ về EMI. Vật tải mạng dễ bị nhiễm EMI hơn các vật tải khác.

### 2.1.2 Vật tải truyền

Vật tải truyền giúp truyền các tín hiệu điện tử từ máy tính này sang máy tính khác. Các tín hiệu điện tử này biểu diễn các giá trị dữ liệu theo dạng các xung nhị phân. Các tín hiệu [ đóng/ ngắt ] được truyền thông qua mạng bằng một tổ hợp các thiết bị điện tử [các cạc mạng, bộ tập chung cáp " hubs ",v.v...] và vật tải truyền cho đến khi chúng đến được máy tính đích cần thiết, ở đó chúng lại được chuyển đổi thành các tín hiệu dữ liệu bên trong máy tính nhận.

Tất cả các tín hiệu truyền giữa các máy tính đều bao gồm một dạng sóng điện từ nào đó, từ các tần số radio đến viba, và tia hồng ngoại (Tần số từ vài KHz đến vài THz). Chúng được chuyển đi theo đường cáp hoặc sóng vô tuyến

Các sóng tần số radio có thể được dùng với cáp điện (cáp xoắn đôi hay cáp đồng trục) hoặc thông qua việc phủ sóng radio. Các kỹ thuật truyền viba có thể được dùng cho các phiên truyền tập trung giữa các trạm đất và vệ tinh. Chúng cũng được dùng cho các phiên truyền trong tầm phát ngang trên mặt đất. Các sóng viba cũng có thể được dùng theo các dạng công suất thấp để phủ rộng các tín hiệu từ một trạm phát đến nhiều trạm thu. Các mạng điện thoại tế bào là những ví dụ về các hệ thống dùng các tín hiệu viba công suất thấp để phủ rộng các tín hiệu.

Tia hồng ngoại thường lý tưởng cho các kiểu truyền thông mạng. Tia hồng ngoại có thể được truyền trên các khoảng cách tương đối ngắn và có thể được phát sóng giữa hai điểm hoặc từ một điểm phủ sóng cho nhiều trạm thu. Có thể truyền tia hồng ngoại và các tần số ánh sáng cao hơn thông qua cáp quang.

**Vật tải cáp:** Có 4 loại cáp thường dùng trong mạng là cáp đồng trục, cáp xoắn đôi có màn chắn (STP), cáp xoắn đôi thường (UTP), cáp quang. Bảng 2.1 tóm tắt các đặc tính của bốn kiểu cáp này theo các tiêu chí giá thành, cách cài đặt, công suất (tốc độ truyền dữ liệu), độ suy dẫn, đặc tính EMI.

Bảng 2.1

**Một số đặc tính cáp truyền**

| *Kiểu cáp* | *Giá thành* | *Cài đặt* | *Công suất* | *Suy dần* | *EMI* |
|---|---|---|---|---|---|
| Đồng trục | Trung bình < Cat 5 UTP >Cat3UTP mỏng <STP dày >STP <sợi quang | Dễ lắp đặt Khó cấu hình lại | Thường 10Mbps | Thấp hơn SPT hay UPT; hạn chế trong vòng vài kilomet | ít nhạy cảm hơn UTP; song vẫn bị ảnh hưởng của EMI và nghe trộm |
| Xoắn cặp | Trung bình | Vừa | Thường là | hạn chế | ít nhạy cảm |

| | | | | | |
|---|---|---|---|---|---|
| có màng chắn STP | >UTP =đồng trục mỏng <đồng trục dày < sợi quang | phải/khá dễ; khó hơn UTP và đồng trục | 16Mbps; lên tới 500 Mbps | trong vòng vài trăm mét | hơn UTP; song vẫn bị ảnh hưởng của EMI và nghe trộm |
| Xoắn cặp trần UTP | Thấp nhất | Rẻ tiền/dễ | 1-100 Mbps với các đoạn chạy cáp 100met | Hạn chế trong vòng vài trăm mét | Nhạy cảm nhất với EMI và nghe trộm |
| Cáp quang | Cao nhất | Đắt tiền/khó | 10 Mbps đến 2 Gbps; thường là 100 Mbps | Thấp nhất phạm vi trong vòng hàng chục kilomet | Không cảm ứng với EMI và nghe trộm |

Có vài so sánh xem ra không đơn giản. Mặc dù cáp quang được coi là đắt tiền, song ta có thể kiến tạo một tuyến cáp quang dài nhiều kilométi. Để xây dựng một tuyến cáp đồng có chiều dài tương tự, ta phải cài đặt các bộ truyền lặp [repeaters] tại vài điểm dọc theo tuyến cáp để khuyếch đại tín hiệu. Các bộ truyền lặp này có thể vượt quá chi phí của tuyến cáp quang.

**Vật tải vô tuyến:** Bản thân cáp lệ thuộc vào các cơ sở cài đặt cố định và các khoảng cách trung bình. Khi các điểm cuối cách xa nhau hoặc khi các điểm đó di động, ta nên xét đến vật tải vô tuyến. Hiện tồn tại các kiểu vật tải vô tuyến sau:

- Radio
- Viba
- Tia hồng ngoại

Phần radio của quang phổ điện từ nằm trong phạm vi từ 10 KHz đến 1Ghz. Trong miền này, ta có rất nhiều băng tần, hoặc các miền tần số được chỉ định cho các mục tiêu cụ thể. Dưới đây là các băng tần quen thuộc:

- Sóng ngắn (shortwave)
- VHF (very High Frequency):
- UHF (Ultra High Frequency):

Có một số miền tần số không được khoanh vùng cấp phép, có nghĩa là chúng có thể được dùng tự do cho mục đích đã được chỉ định cho tần số đó. Uỷ ban truyền thông liên bang của Mỹ (FCC) đã chỉ định ba băng tần không cấp giấy chứng nhận: 902-928 MHz, và 5.72-5.85 GHz. 902 Mhz là miền dài nhất sẵn có và đã được dùng cho mọi thứ từ các điện thoại không dây cho đến việc điều khiển máy bay mô hình từ xa. Do miền 902 MHz khá đông đúc, nên nhiều hãng kinh doanh đang cố phát triển các thiết bị cho

băng tần 2.4 GHz ít đông hơn. Các thiết bị cho băng tần 5.72 GHz vẫn còn đắt tiền và ít được dùng.

Sử dụng một tần số không cấp chứng nhận thường là một nguy cơ cho người dùng và thường không bảo đảm sẽ là một kênh truyền thông rõ. Tuy nhiên, trang thiết bị dùng trong các dải tần này phải hoạt động theo mức công suất điều tiết để giới hạn miền và giảm bớt khả năng bị nhiễu.

Các phiên truyền radio có thể theo mọi hướng hay định hướng. Một trạm radio thường truyền một tín hiệu mọi hướng mà mọi đài radio trong vùng phủ sóng có thể nhận. Đôi lúc, có thể dùng một phiên truyền định hướng để hướng mọi công suất phiên truyền về phía một điểm cụ thể.

Ta dùng nhiều kiểu ăng-ten khác nhau, tuỳ theo mức truyền dự kiến và các đặc tính thu.

Tháp phủ sóng thường là loại phủ theo mọi hướng, mặc dù có thể điều chỉnh khuôn mẫu bức xạ cụ thể cho khớp với các hạn chế của FCC dành cho một nhà được cấp giấy chứng nhận cụ thể.

- Ăng-ten lưỡng cực nhận một miền các tần số khá rộng và định hướng vừa phải.
- Dây có chiều dài ngẫu nhiên có thể dùng để phát hoặc thu. Chiều dài ngẫu nhiên có nghĩa là chiều dài ăngten không được chọn cụ thể cho tần số đang phát hoặc thu. Ăng-ten trên đài radio AM/FM bình thường là loại dây có chiều dài ngẫu nhiên.
- Ăng ten chùm [beam antenna] dùng nhiều thành phần để tinh chỉnh ăngten theo một miền tần số cụ thể và theo sự định hướng. Một thiết kế chung của ăngten này có tên Yagi. Ăngten chùm được dùng để tạo một chùm khá tập trung có thể hướng đến một điểm thu cụ thể (mặc dù hiệu ứng không hoàn toàn định hướng, và hiện tượng rò tín hiệu theo mọi hướng).

**Radio Quang phổ trải**: Quang phổ trải [spread spectrum] là một kỹ thuật do giới quân sự phát triển đầu tiên để giải quyết một số vấn đề về truyền thông. Quang phổ trải cải tiến độ tin cậy, giảm bớt sự nhạy cảm với sự cố nhiễu và tắc nghẽn, ngoài ra nó cũng khó bị nghe trộm hơn so với radio tần số đơn.

Phiên truyền quang phổ trải sử dụng nhiều tần số để truyền các thông điệp. Hai kỹ thuật thường sử dụng đó là: điều biến chuỗi trực tiếp và lập chặng tần số.

Điều biến chuỗi trực tiếp [Direct sequence modulation ] tách các thông điệp ban đầu thành các phần có tên là chip, được truyền trên các tần số tách biệt. Để làm rối các tay nghe trộm, Có thể truyền dữ liệu "cò mồi" trên các tần số khác. Trạm thu đích sẽ biết các tần số nào là hợp lệ, và có thể cô lập các chip rồi ráp lại thông điệp. Khó lòng nghe trộm bởi không biết tần số chính xác, và kẻ nghe trộm cũng không thể cô lập các tần số đang tải dữ liệu thực. Kỹ thuật này có thể hoạt động trong các môi trường có các

hoạt động truyền khác bởi có thể chọn các loạt tần số khác nhau. Các hệ điều biến trực tiếp hoạt động ở mức 900 MHz thường hỗ trợ băng thông 2-6 Mbps.

Kỹ thuật lập chặng tần số [frequency hopping] chuyển các phiên truyền giữa các tần số đã có. Trạm phát và trạm thu phải duy trì tính đồng bộ thì kỹ thuật này mới làm việc. Có vài hệ thống truyền đồng thời trên nhiều tần số để gia tăng băng thông. Các hệ quang phổ thường hoạt động trong miền tần số không cấp phép. Các thiết bị 900 MHz là phổ dụng, song các thiết bị 2.4 GHz cũng đang sẵn có.

*Viba mặt đất:*

Kỹ thuật truyền thông viba mặt đất sử dụng các trạm phát và trạm thu mặt đất. Các tần số được dùng nằm trong miền gigahertz thấp, hạn chế tất cả các truyền thông liên lạc theo tầm phát ngang. Phiên truyền viba thường được tiến hành bằng một ăngten parabôn tạo ra một tín hiệu hẹp có độ định hướng cao. Một ăngten tương tự tại trạm thu sẽ chỉ cảm ứng với các tín hiệu trong tiêu điểm hẹp. Do trạm phát và trạm thu được tập trung cao, chúng phải được điều chỉnh cẩn thận để tín hiệu truyền thẳng hàng với trạm thu.

Sóng viba được dùng như một biện pháp để truyền các tín hiệu tại những nơi không thể chạy cáp. Nếu cần nối hai mạnh cách biệt bởi một con đường công cộng, bạn sẽ thấy không thể chạy cáp bên trên hay bên dưới con đường đó. Trong trường hợp như vậy, tuyến kết nối viba là một giải pháp lý tưởng.

Một số LAN hoạt động theo các tần số viba, hoạt động ở công suất thấp, và dùng các trạm phát và trạm thu không định hướng. Cách tiếp cận này là một cách để cho phép các trạm làm việc di dộng trong một môi trường văn phòng.

Trong nhiều trường hợp, kỹ thuật viba mặt đất sử dụng các tần số cấp phép. Phải có giấy phép của FCC, và trang thiết bị phải được các kỹ thuật viên được chứng nhận cài đặt và bảo trì.

Các hệ viba mặt đất hoạt động trong miền gigahertz thấp, thường ở mức 4-6 GHz và 21-23 GHz.

*Viba vệ tinh:*

Các hệ thống viba vệ tinh tiếp sóng phiên truyền thông qua các vệ tinh truyền thông hoạt động trong quỹ đạo địa tĩnh, cách 22,300 dặm trên Trái đất. Các vệ tinh quay theo quỹ đạo theo khoảng cách này luôn nằm cách tại một điểm cố định bên trên Trái đất.

Các trạm mặt đất sử dụng ăngten parabôn để truyền thông các vệ tinh. Các vệ tinh có thể truyền lại các tính hiệu trong các chùm tia rộng hoặc hẹp tuỳ theo vị trí nhận các tín hiệu. Khi đích nằm trên phía đối diện của trái đất, vệ tinh đầu tiên không thể truyền trực tiếp đến trạm thu và phải tiếp sóng tín hiệu thông qua một vệ tinh khác.

Do không cần cáp ta có thể thực thi kỹ thuật truyền thông viba vệ tinh với hầu hết các trạm từ xa và với các thiết bị di động, kể cả tàu bè ngoài khơi và xe cộ. Các khoảng cách dùng trong truyền thông vệ tinh dẫn đến hiện tượng thú vị: Do mọi tín hiệu phải đi 22,300 dặm đến vệ tinh và 22,300 dặm khi trở về trạm thu, thời gian cần để truyền một tín hiệu độc lập với khoảng cách. Thời gian để truyền một tín hiệu đến một trạm thu trong cùng trạng thái cũng bằng thời gian đến một trạm thu cách đó một phần ba đường vòng quanh thế giới. Thời gian để một tín hiệu đi đến đích của nó có tên là độ trễ lan truyền [propagation delay]. Các độ trễ thường gặp trong các phiên truyền vệ tinh là từ 0,5 đến 5 giây.

Kinh phí truyền vệ tinh rất đắt tiền. Chi phí xây dựng và phóng một vệ tinh có thể dễ dàng vượt trên một tỷ đôla. Trong hầu hết các trường hợp, các tổ chức chia nhau chi phí này, hoặc họ mua các dịch vụ từ một nhà cung cấp thương mại. AT&T, Hughes Network Services, và Scientific-Atlanta thuộc trong số các hãng kinh doanh các dịch vụ truyền thông gốc vệ tinh.

**Tia hồng ngoại liên điểm**

Các mạng liên điểm [point-to-point] hoạt động bằng cách tiếp sóng các tín hiệu tia hồng ngoại từ thiết bị này sang thiết bị kế tiếp.

Do các thiết bị phải được xác lập và đặt để cẩn thận, nên tia hồng ngoại liên điểm không phù hợp với các thiết bị di chuyển thường xuyên.

Có thể dùng các trạm phát lase công suất cao để truyền dữ liệu trong vài ngàn mét khi có thể áp dụng kỹ thuật truyền thông tầm phát ngang. Có thể dùng lase trong nhiều tình huống tương tự như các nối kết viba, mà không buộc phải có giấy phép FCC. Hãy xét khả năng dùng tia lase hồng ngoại để liên kết giữa các toà nhà, nhất là khi chúng bị khống chế bởi các quy định đường phố.

Tia hồng ngoại thường nằm trong phạm vi dưới mức ánh sáng thấy được và có miền tần số xấp xỉ 100GHz đến 1,000 THz.

**Tia hồng ngoại phủ rộng**

Thay vì tập trung phiên truyền vào các chùm tia kín, tia hồng ngoại phủ rộng phát tán phiên truyền để vài chạm thu thấy được chúng. Có ít nhất hai cách tiếp cận khả dĩ. Cách tiếp cận đầu tiên đó là dịch vụ một trạm phát tác hoạt [active] tại một cao điểm để nó có thể truyền cho mọi thiết bị. Cách tiếp cận thứ hai là đặt một chất phản chiếu trên trần nhà; các thiết bị truyền về phía trần ở đó các tín hiệu ánh sáng được phát tán đến các thiết bị khác trong phòng.

### 2.1.3 Tín hiệu trên đường truyền

Để có thể truyền thông trên mạng, bằng cách này hay cách khác các bít dữ liệu (các số 1 và số 0 ) phải đi qua các vật tải truyền từ máy gửi đến máy nhận, chúng được truyền đi theo một trong hai dạng: dạng số hoặc tương tự (analog). Thông tin analog là thông tin thay đổi liên tục và có thể đảm nhận nhiều giá trị khác nhau. Thông tin số hóa được định rõ đặc điểm bởi các trạng thái riêng rẽ.

Thông thường, thông tin trong một dạng phải được chuyển đổi thành một dạng khác. Điều này thường liên quan đến việc dùng một thuật mã hóa nào đó cho phép thông tin ban đầu khôi phục từ một tín hiệu sau khi đã nhận nó. Khi một tín hiệu số hóa hay tương tự (analog) thay đổi để chứa thông tin sẽ được truyền, tiến trình được gọi là điều chế [modulation] hay mã hóa [encoding].

**1.Truyền dẫn số.**

Hiện nay với tiến bộ của kỹ thuật số và máy tính các hệ thống chuyển mạch trung tâm điện thoại đang chuyển sang dùng truyền số và hầu hết các mạng máy tính đều dùng kỹ thuật phát tín hiệu số hóa. Những ưu việt của việc truyền số so với việc truyền tương tự là do chỉ gồm hai giá trị 0 và 1 nên giảm được các lỗi do suy hao và nhiễu đường truyền, tăng độ tin cậy và tốc độ truyền, nó dùng được cho cả việc đàm thoại, truyền số liệu, truyền thanh và truyền hình , giá thành thiết bị sử dụng ngày càng rẻ. Để truyền các tín hiệu số hiệu quả trên đường truyền người ta thường sử dụng phương pháp điều biến tín hiệu số để mã hoá dữ liệu số. Dưới đây mô tả hai phương pháp điều biến tín hiệu số: trạng thái hiện hành và trạng thái chuyển tiếp.

**Kỹ thuật mã hóa trạng thái hiện hành** [current state encoding] gán các trạng thái tín hiệu cụ thể để biểu thị từng giá trị dữ liệu khả dĩ. Tín hiệu được giám sát định kỳ để xác định trạng thái hiện hành của nó, từ đó có thể xác định một giá trị dữ liệu. Ví dụ, một điện áp +5V có thể biểu thị một số nhị phân 0, và một điện áp -5V có thể biểu thị một số nhị phân 1. Có thể dùng nhiều biến thể tín hiệu khác nhau. Đặc tính quan trọng đó là một trạng thái nhất định sẽ biểu thị cho một và chỉ một giá trị dữ liệu. Các kỹ thuật mã hóa dưới đây sử dụng kỹ thuật mã hóa trạng thái hiện hành:

- Đơn cực
- Lưỡng cực
- Lưỡng pha

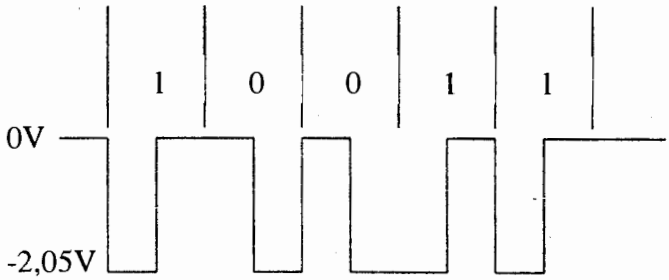
**Kỹ thuật mã hóa trạng thái chuyển tiếp** [state transition encoding] sử dụng các bước chuyển tiếp trong tín hiệu số hóa để biểu thị dữ liệu. Dưới đây là các cách để thực hiện:

- Một bước chuyển tiếp từ điện áp cao sang thấp luôn biểu thị một số nhị phân 1, và một bước chuyển tiếp từ điện áp thấp sang cao luôn biểu thị một số nhị phân 0.
- Một bước chuyển tiếp bất kỳ luôn biểu thị cho một số 1, và sự vắng mặt của một bước chuyển tiếp dự trù sẽ biểu thị một số 0.

Các thuật mã hóa dưới đây sử dụng kỹ thuật mã hóa chuyển tiếp trạng thái:

- BipolarAlternate Mark Inversion ( AMI )
- NonReturnto Zero ( NRZ )
- Manchester
- Differential Manchester
- Biphase Space ( FM0 )

Ví dụ thuật toán mã hoá Manchester hay sử dụng trong mạng Ethernet như hình 2.1



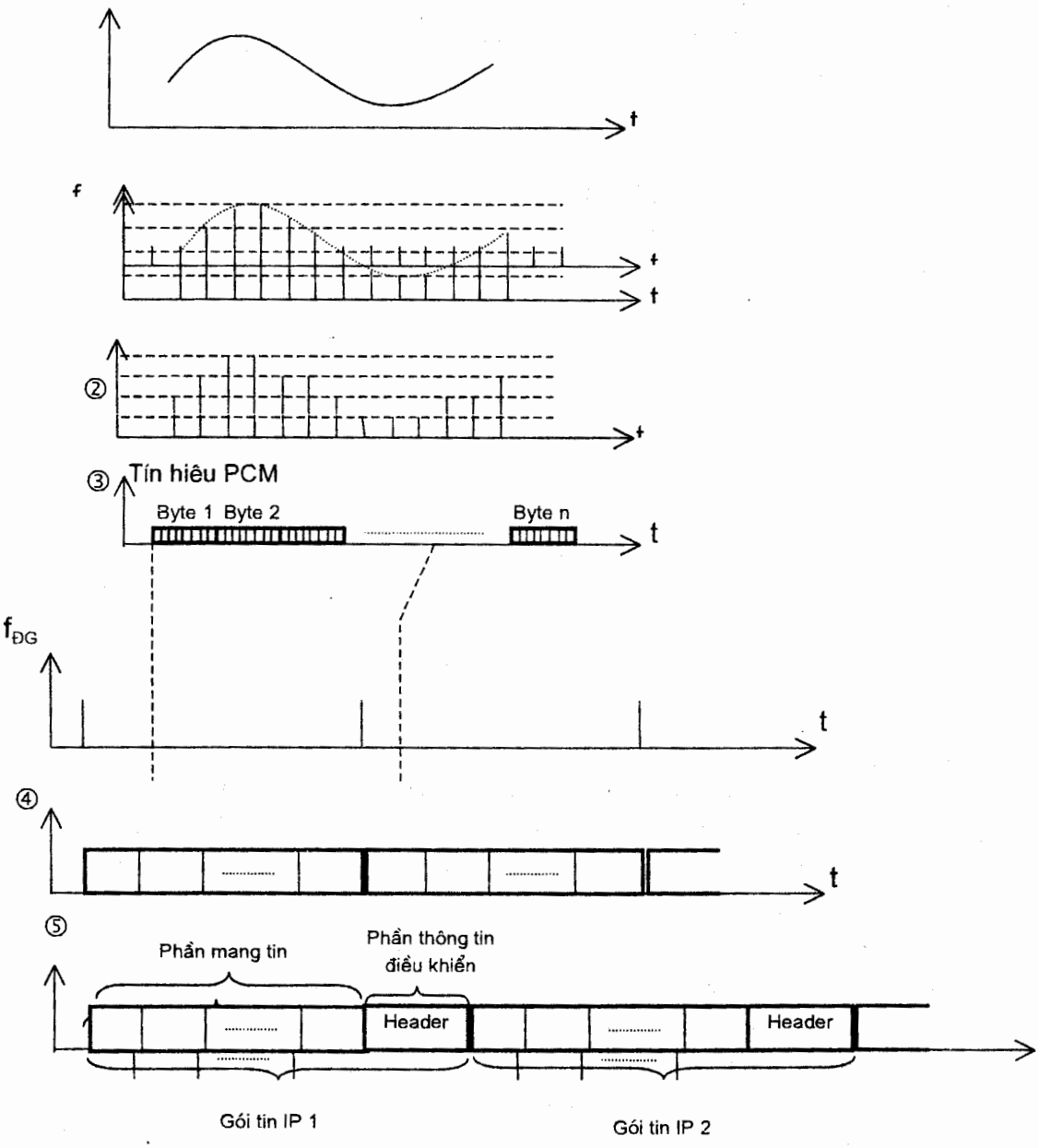

**Hình 2.1: Mã hoá Manchester**

**Mã PCM**

Mã PCM là phương pháp biến đổi tín hiệu tương tự của tiếng nói sang dạng tín hiệu số để có thể truyền đi qua đường truyền số. Quá trình biến đổi từ tiếng nói (tín hiệu tương tự) ra tín hiệu số PCM (các byte) và đóng gói chúng thành các gói tin IP truyền trên mạng (Công nghệ VOIP-Truyền tiếng nói qua mạng) được thể hiện trên hình 2.2 và hình 2.3 .Tần số lấy mẫu lượng tử là 8 Khz.

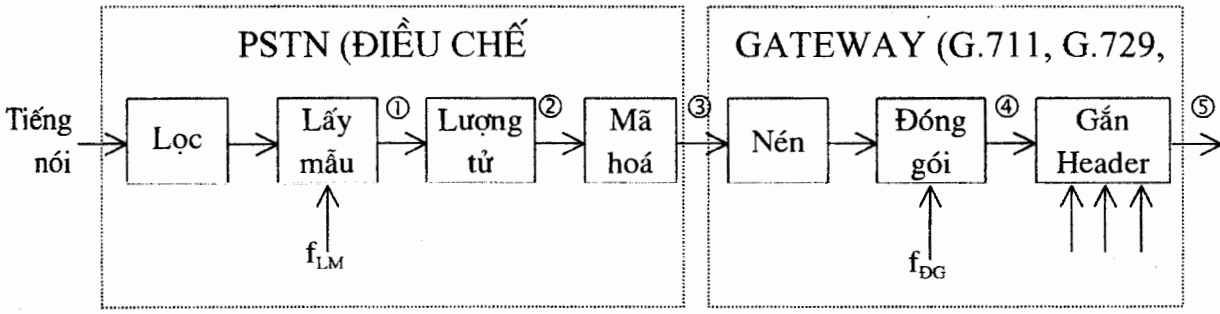
Lọc: nhằm hạn chế phổ tần của tín hiệu liên tục cần truyền: biến đổi Fourier của các tín hiệu liên tục thực tế là vô hạn theo biến tần số. Chính vì vậy, các tín hiệu liên tục cần truyền phải được lọc nhằm hạn chế phổ tới tần số cực đại W nào đó nhằm thoả mãn tiền đề về băng tần hạn chế của định lý lấy mẫu. Lấy mẫu: tín hiệu liên tục sau lọc được rời rạc hoá nhờ lấy mẫu tín hiệu liên tục bằng chuỗi xung nhịp có tần số $f_S$ = 8 Khz theo định lý lấy mẫu để có được các tín hiệu điều biên xung (PAM: Pulse Amplitude Modulation).

Lượng tử hoá: Sử dụng 256 mức để biểu diễn giá trị của từng xung PAM và quá trình này được gọi là lượng tử hoá. Các giá trị mức lượng tử ứng với các xung PAM được mã hoá bằng các tổ hợp mã nhị phân để truyền đi trên hệ thống truyền dẫn số. Sau khi được xử lý (nén) các Byte thông tin được đóng thành các gói tin.

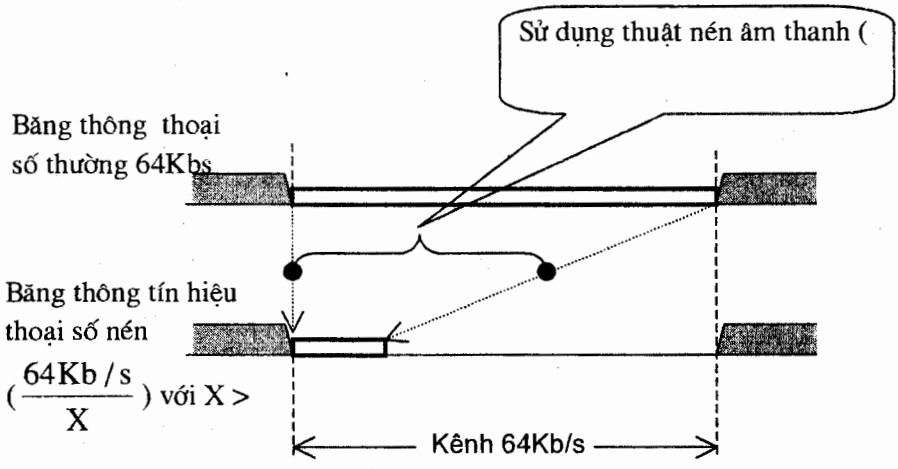



**Hình 2.2 Đồ thị mô tả quá trình biến đổi tiếng nói → gói tin IP**

Các gói có kích thước giống nhau, nó được "lấy mẫu" bởi một tần số cố định, độ dài của gói tin thường là 20ms, 40ms, 60ms hoặc 80ms tuỳ theo thiết bị của từng hãng, nhưng phổ biến nó được lấy là 20Byte. Các thông tin về địa chỉ đích, loại giao thức kế tiếp, số thứ tự của gói ... sẽ được điền và gắn vào gói tin. Header giống Header của gói IP thông thường. Từ hình 2.2 cho thấy, băng thông của tín hiệu PCM ở đầu ③ (băng thông 01 kênh thoại số thường) là 64Kb/s và băng thông của mỗi gói tin IP ở đầu ⑤ (băng thông của 01 kênh thoại số có sử dụng kỹ thuật sử lý số như nén) là 64Kbs/ X với X > 1. Như vậy thì 01 kênh thoại thường 64Kb/s có thể truyền được X kênh băng thông của 01 kênh thoại số có sử dụng kỹ thuật nén. Hình 2.4 cho ta thấy rõ điều này.




**Hình 2.3: Sơ đồ mô tả các khối tham gia quá trình**




**Hình 2.4 Băng thông kênh thoại số thường và kênh số nén.**

**Mạng truyền số công cộng:** Hiện nay theo phương pháp truyền số xuất hiện một loại các dịch vụ truyền số công cộng do bưu điện triển khai như các mạng thông dụng sau:

- X. 25
- Tiếp sóng khung.
- SONET [Synchronous Optical Network = Mạng cáp quang đồng bộ]
- ATM, ISDN

Bảng 2.2

**Các băng thông của các dịnh vụ mạng truyền số liệu**

| *Dịch vụ* | *Băng thông* |
|---|---|
| Dedicated 56 KB (DDS) | 56 Mbps |
| Switched 56 | 56 Mbps |
| X.25 | 56 Mbps |
| T1 | 1.544 Mbps |
| Switched T1 | 1.544 Mbps |
| Frame relay | 1.544 Mbps |
| SMDS | 1.544 Mbps |
| ISDN | 1.544 Mbps |
| EI (Europe) | 2.048 Mbps |
| T3 | 44.736 Mbps |
| ATM | 44.736 Mbps |

**2. Truyền dẫn tương tự (analog).**

Đây là phương phương pháp truyền đẫn đã tồn tại hàng trăm năm nay trên thế giới, các tín hiệu truyền trên các hệ thống truyền tin đặc biệt là hệ thống điện thoại hầu hết là tín hiệu tương tự. Phát tín hiệu tương tự thay đổi liên tục theo một hay nhiều giá trị. Các thay đổi về giá trị này có thể dược dùng để biểu thị dữ liệu. Các dạng sóng tương tự thường mang dạng sóng hình sin.

Các đặc tính định nghĩa một dạng sóng tương tự là: Tần số và biên độ và pha. Tần số là số đo khoảng cách giữa hai đỉnh tương tự trên các sóng kế cận. Tần số thường được đo bằng Hertz (Hz ). Biên độ là số đo cường độ của dạng sóng. Pha ( phase) tuy

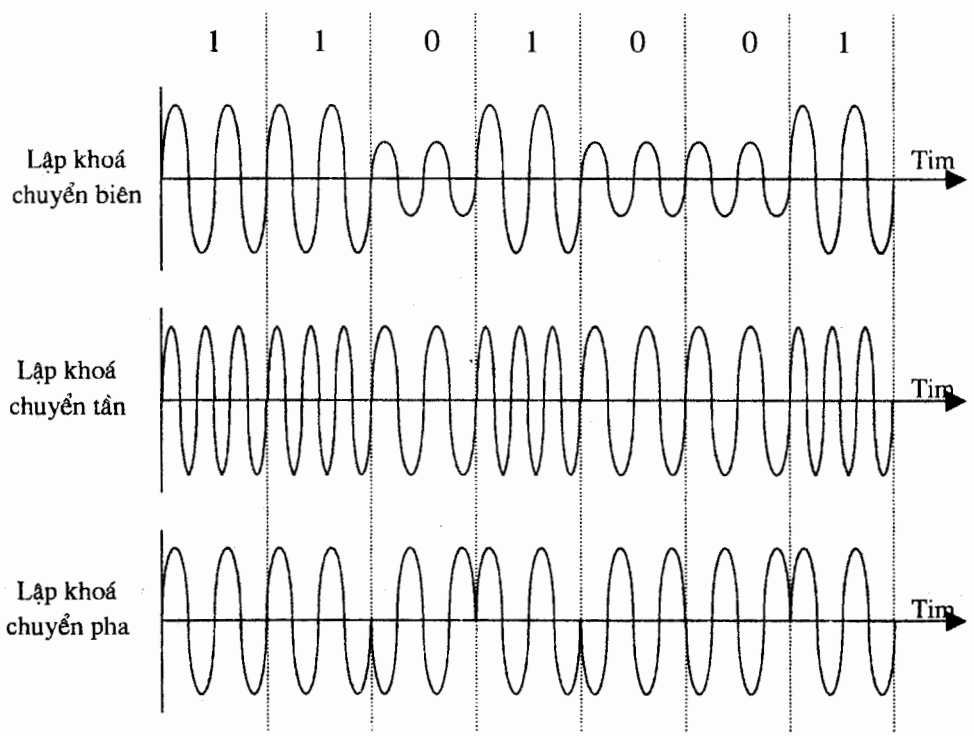
giống tần số và biên độ, song chúng không bắt đầu các bước chuyển tiếp của mình cùng một lúc.

Các tín hiệu số có thể truyền qua đường truyền tương tự nhờ các phương pháp mã hoá sau (hình 2.5).

**Điều chế theo biên độ:** [amplitue shift keying] là phương pháp điều chế trạng thái hiện hành qua đó các biên độ tín hiệu cụ thể được gán các giá trị dữ liệu 0,1. Ví dụ (hình 2.5) một tín hiệu biên độ cao có thể được gán một giá trị 1, trong khi một tín hiệu biên độ thấp được gán một giá trị 0.

**Điều chế theo tần số**: [frequency shift keying] cũng là một phương pháp điều chế trạng thái hiện hành. các giá trị tần số cụ thể được gán các giá trị dữ liệu cụ thể. Ví dụ, một tần số cao có thể biểu thị cho 0, trong một tàn số thấp có thể biểu thị cho 1.

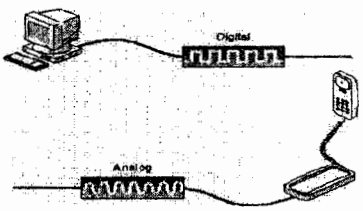
**Điều chế theo pha:** [phase shift keying] là phương pháp điều biến trạng thái chuyển tiếp. Ví dụ, một pha tham chiếu có thể biểu thị cho 0, trong khi một bước chuyển pha 180° sẽ biểu thị một giá trị 1.




**Hình 2.5 Các phương pháp mã tín hiệu.**

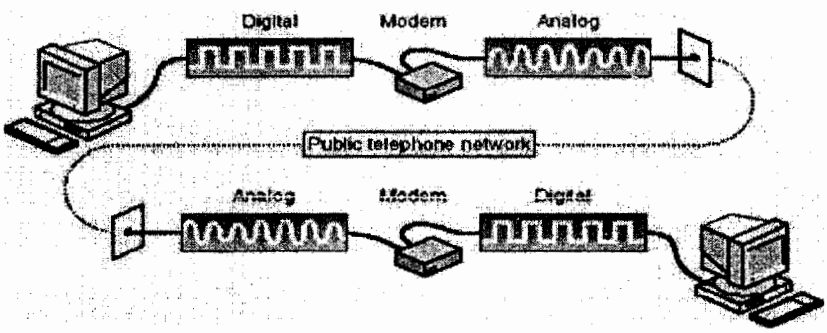
**3.Công nghệ modem**

Modem là một thiết bị giúp các máy tính thông tin được với nhau thông qua một đường điện thoại ở bên ngoài. Các máy tính không thể đơn giản đấu nối đến nhau bằng một đường điện thoại bên ngoài, bởi vì thông tin của máy tính là thông tin dưới dạng số (xung điện), một đường điện thoại chỉ gửi tín hiệu tương tự.




**Hình 2.6 Sự khác nhau giữa tín hiệu máy tính và điện thoại**

Hình 2.6 chỉ ra sự khác nhau giữa tín hiệu máy tính số và tín hiệu điện thoại tương tự. Hình 2.7 modem làm nhiệm vụ biến đổi tín hiệu số của máy tính thành tín hiệu tương tự và truyền trên đường điện thoại. Modem ở đầu kia làm nhiệm vụ thu và biến đổi tín hiệu tương tự thành tín hiệu số để cho máy tính sử dụng.




**Hình 2.7. Mô tả tín hiệu máy tính đến máy tính qua đường thoại**

**Chuẩn của modem:** Một tiêu chuẩn là cần thiết để cho các modem được chế tạo theo các công nghệ khác nhau có thể thông tin được với nhau.

- Tương thích Hayes

Năm 1980, công ty Hayes Microcomputer Products đưa ra loại modem gọi là Hayes Smartmodem. Smartmodem trở thành một tiêu chuẩn cho các modem khác, nhìn chung chỉ có các máy của IBM là phù hợp với chuẩn này. Bởi vì hầu hết các nhà cung cấp đều tuân theo chuẩn Hayes này lên gần đây tất cả các modem của mạng LAN đều có thể thông tin được với nhau.

Modem tương tích với chuẩn này có thể gửi và nhận dữ liệu ở tốc độ 300bit/s. Modem được chế tạo hiện nay thường có tốc độ 56,600bit/s hoặc cao hơn.

-Tiêu chuẩn quốc tế

Từ năm 1980, tổ chức viễn thông quốc tế (ITU) đã đưa ra tiêu chuẩn về modem. Đặc biệt là tiêu chuẩn V, bao gồm một số các chỉ dẫn về tiêu chuẩn. Tiêu chuẩn V22 ở tốc độ 2400bít/s cho phép một modem chỉ mất 18 giây để gửi một bức thư 1000 từ. Tiêu chuẩn V34 ở tốc độ 9600 bit/s cho phép modem có thể gửi cũng bức thư như vậy mà chỉ mất 4 giây, và tiêu chuẩn V42 ở tốc độ 14,400bit/s cho phép modem có thể gửi bức thư như vậy mà chỉ mất 3 giây.

**Đặc tính modem**

Tốc độ của một modem được đo bằng đơn vị bit/s hoặc đơn vị baud, hầu hết mọi người nhầm lẫn hai cách biểu diễn này.

Baud được xem là tốc độ sóng âm thanh mang một bit dữ liệu dao động qua đường điện thoại. Thuật ngữ này bắt nguồn từ tên điện báo của Pháp và kỹ sư Jean-Maurice-Emile Baudot. Trước năm 1980 tốc độ baud bằng tốc độ của modem. Vào thời điểm này 300 baud bằng 300bit/s.

Song với sự phát triển của công nghệ nén và mã hoá dữ liệu âm thanh được điều chế có thể mang nhiều hơn một bít dữ liệu. Sự khám phá này cho biết được rằng tốc độ bit có thể lớn hơn tốc độ baud. Ví dụ một modem điều chế ở tốc độ 2400 baud có thể gửi ở 9600 bit/s. Hiện nay thông số tốc độ của modem là bit/s.

Bảng 2.3

**Một số chuẩn Modem**

| *Loại chuẩn* | *bps* | *Năm công bố* | *Các loại modem* |
|---|---|---|---|
| V.22bis | 2400 | 1984 | |
| V.32 | 9600 | 1984 | |
| V.32bis | 14,400 | 1991 | |
| V.32terbo | 19,200 | 1993 | Will communicate only with another V.32terbo |
| V.FastClass (V.FC) | 28,800 | 1993 | |
| V.34 | 28,800 | 1994 | Improved V.FastClass. Backward-compatible with earlier V. modems |
| V.42 | 57,600 | 1995 | Backward-compatible with earlier V. modems—error-correction standard |
| V.90 | 56,600 | 1998 | 56K modem standard; resolved competition for standard between U.S. Robotic X2 and Rockwell K56 Flex standards. |

Một vài tiêu chuẩn công nghiệp của modem như V42 bis/MNP5 nén dữ liệu, có tốc độ truyền dẫn dữ liệu 57,600bit/s, và một vài modem có tốc độ cao hơn đến 76,800bit/s.

**Chủng loại modem**

Có nhiều loại modem khác nhau bởi vì có nhiều kiểu môi trường thông tin yêu cầu các phương pháp gửi dữ liệu khác nhau. Các môi trường này có thể được chia thành hai loại :

- Không đồng bộ
- Đồng bộ

Kiểu modem của mạng được sử dụng độc lập với môi trường là đồng bộ hay không đồng bộ

**3. Các phiên truyền băng tần rộng và băng tần cơ sở**

Có hai cách để phân bổ công suất của các vật tải truyền đó là: dùng các phiên truyền băng tần rộng và băng tần cơ sở. Băng tần cơ sở [baseband] dành chọn công suất của vật tải cho một kênh truyền thông. Băng tần rộng [broadband]cho phép hai hay nhiều kênh truyền thông dùng chung băng thông của vật tải truyền thông.

Băng tần cơ sở là chế độ hoạt động phổ dụng nhất. Ví dụ, hầu hết các LAN đều hoạt động trong chế độ băng tần cơ sở. Có thể dùng các tín hiệu số hoá lẫn tương tự để phát tín hiệu băng tần cơ sở.

Chúng ta đã có nhiều cơ hội làm quen với các phiên truyền băng tần rộng, ví dụ đường cáp tivi từ cần ăngten hoặc nhà cung cấp cáp chạy vào nhà là một dạng vật tải băng tần rộng. Nhiều tín hiệu tivi có thể dùng chung băng thông của cáp bởi mỗi tín hiệu được điều biên bằng một tần số được gán riêng biệt. Ta có thể dùng bộ rà chỉnh tivi để chọn kênh muốn xem bằng cách lựa tần số của nó. Kỹ thuật chia băng thông thành các băng tần này có tên là FDM (frequency-division multiplexing = ghép kênh phân theo tần số) và chỉ làm việc với các tín hiệu tương tự. Một kỹ thuật khác có tên TDM (time-division multiplexing = ghép kênh phân theo thời gian), hỗ trợ các tín hiệu số hoá, và được mô tả trong đoạn sau.

**Ghép Kênh**

Ghép kênh (multiplexing) là kỹ thuật cho phép các vật tải băng tần rộng hỗ trợ nhiều kênh dữ liệu. Ghép kênh thường được dùng trong nhiều tình huống:

➢ Khi băng thông vật tải đắt tiền. Một tuyến thuê bao cao tốc, như T1 hay T3, rất đắt tiền. Miễn là tuyến thuê bao có băng thông đủ, phương pháp ghép kênh có thể cho

phép cùng một tuyến chuyển tải máy tính lớn, LAN, đàm thoại, hội nghị video, và nhiều kiểu dữ liệu khác.

➢ Khi băng thông nhàn rỗi. Nhiều tổ chức đã cài đặt cáp quang chỉ được sử dụng một phần công suất. Với khả năng của mình, một sợi cáp quang có thể hỗ trợ hàng trăm megabit hoặc thậm chí gigabit hay thêm dung lượng dữ liệu.

➢ Khi cần truyền các dữ liệu lớn qua các kênh công suất thấp. Các kỹ thuật ghép kênh có thể chia luồng dữ liệu ban đầu thành vài kênh có băng thông thấp, mỗi kênh có thể truyền thông qua một vật tải có công suất thấp. Các tín hiệu có thể được tổ hợp lại ở bên nhận.

Ghép kênh có nghĩa là tổ hợp nhiều kênh dữ liệu để truyền trên một vật tải chung. Tản kênh [demultiplexing] có nghĩa là phục hồi các kênh riêng biệt ban đầu từ một tín hiệu đã ghép kênh.

Tiến trình ghép kênh và giải kênh được thực hiện bởi bộ ghép kênh [multiplexing]. Bộ này thường có hai khả năng. Trong tiếng Anh, đôi khi nó còn được gọi là mux.

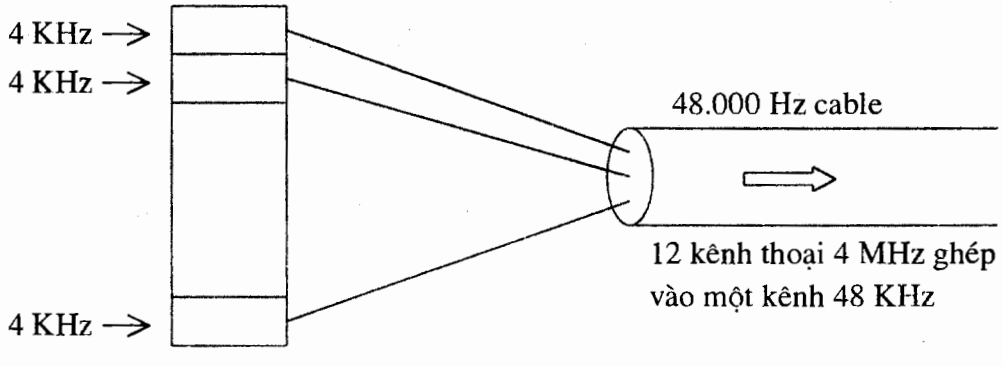
Hai kỹ thuật dưới đây được dùng để ghép kênh các tín hiệu:

➢ Ghép kênh phân theo tần số.

➢ Ghép kênh phân theo thời gian.

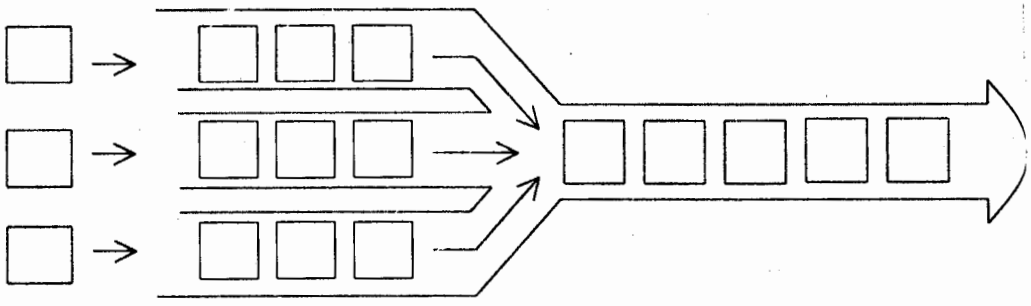
**Ghép kênh theo tần số**

Hình 2.8 minh hoạ kỹ thuật ghép kênh phân theo tần số (FDM). Kỹ thuật này làm việc bằng cách chuyển đổi mọi kênh dữ liệu sang dạng tương tự. Mỗi tín hiệu tương tự có thể được điều biến bởi một tần số riêng biệt (có tên tần số tải [carrier frequency]) để có thể phục hồi tín hiệu đó trong tiến trình giải kênh. Tại bên nhận, bộ giải kênh có thể chọn tần số tải thích hợp và dùng nó để trích tín hiệu dữ liệu của đó.




**Hình 2.8 Ghép kênh phân theo tần số (FDM)**

FDM có thể dùng trong các LAN băng tần rộng (một chuẩn cho Ethernet tồn tại). Một ưu điểm của FDM đó là: nó hỗ trợ tiến trình phát tín hiệu hai chiều trên cùng một đường cáp.



**Hình 2.9 Ghép kênh phân theo thời gian (TDM)**

Nếu cần phải dùng hiệu quả công suất của vận tải dữ liệu, ta có thể dùng một kỹ thuật phức tạp hơn, tên là ghép kênh phân theo thời gian thống kê [statistical timedivision multiplexing] (StatTDM). Bộ statmux dùng kỹ thuật khe thời gian, song lại phân bố các khe thời gian theo nhu cầu lưu thông trên các kênh riêng lẻ.

## 2.2 Sử lý các tập tin số

Chúng ta đang được chứng kiến sự phát triển vượt bậc của công nghệ số, hiện nay hầu hết các dạng thông tin đều có thể biểu diễn dưới dạng số (bit và byte) và chúng có thể được lưu trữ dưới dạng tập tin và được sử lý với rất nhiều các thuật toán thông minh khác nhau để tăng chất lượng và hiệu quả thông tin. Các Dịch vụ tập tin trong mạng máy tính có thể chuyển dữ liệu giữa các người sử dụng dưới dạng các tập tin. Ngày nay có khá nhiều kiểu dữ liệu số, bao gồm âm thanh, video, đồ hoạ văn bản ... Dữ liệu văn bản được coi là dạng dữ liệu đơn giản nhất nay cũng mang nhiều kiểu dáng kỳ lạ như siêu văn bản[hypertext] (chứa các nối kết điện tử đến các văn bản, tư liệu, hình ảnh, âm thanh, hay các kiểu dữ liệu khác). Trong phần này chúng ta sẽ xem xét một số kỹ thuật xử lý thông tin số để tăng hiệu quả truyền dữ liệu số trên mạng như kỹ thuật kiểm tra lỗi, mã hoá và các kỹ thuật nén tin.

### 2.2.1 Nguyên tắc kiểm tra lỗi

Trong việc truyền dẫn dữ liệu việc cần thiết nhất là có các biện pháp ngăn ngừa được các lỗi bít phát sinh do hiện tượng cảm ứng điện từ, vv..

Có hai phương pháp điều khiển lỗi:

- Kiểm tra chẵn lẻ
- CRC (kiểm tra vòng)

Một loại mã sửa lỗi hệ thống gọi là :

- Mã Hamming

### Kiểm tra chẵn lẻ

Kỹ thuật kiểm tra chẵn lẻ là một phương pháp để dò tìm lỗi bít nhờ một bít cho thêm vào (gọi là bit chẵn lẻ) nó được bổ xung thêm vào trong chuỗi bít truyền dẫn. Tại nơi nhận bộ thu sẽ xem xét chuỗi bít này và bít chẵn lẻ.

Có hai phương pháp bổ xung bit chẵn lẻ.

- Tương đương lẻ: bít 1 hoặc bít 0 sẽ được thêm tuỳ thuộc vào tổng giá trị các bit lẻ.
- Tương đương chẵn: bít 1 hoặc bít 0 sẽ được thêm tuỳ thuộc vào tổng giá trị các bit chẵn.
- Có hai phương pháp kiểm tra:
- Kiểm tra chẵn lẻ theo chiều ngang: kiểm tra theo hàng chuỗi bít được cấu tạo từ các ký tự
- Kiểm tra chẵn lẻ theo chiều dọc: kiểm tra theo chiều dọc chuỗi bít được cấu tạo từ khối dữ liệu.

Thông thường, cả hai phương pháp này được sử dụng kết hợp.

### Phương pháp kiểm tra vòng CRC

CRC là phương pháp truyền dẫn mà chuỗi bít được biểu diễn dưới dạng các hệ số của một đa thức và bổ xung vào đó mã dữ liệu kiểm tra (mã CRC), đó là số dư $R(x)$ được tính toán theo phương pháp số học "Cộng modulo 2 " trên các chuỗi bit dữ liệu của đa thức truyền $M(x)$ và đa thức sinh (tạo) $G(x)$. Dạng đa thức truyền sẽ có dạng sau:

$T(x) = x^cM(x) + R(x)$ Trong đó c- Số bit mã dữ liệu kiểm tra thêm vào.

Ta hãy xem một ví dụ về việc tính toán CRC:

Giả sử ta có chuỗi bit dữ liệu 110101 cần truyền đi, như vậy ta có đa thức truyền sẽ có dạng sau: $M(x) = x^5+x^4+x^2+1$. Nếu ta chọn số bit mã kiểm tra là 3 (c=3) và đa thức sinh chọn như sau: $G(x) = x^3+1$.

Các bước tính CRC sẽ như sau:

- Ta nhân $x^3$ với da thức $M(x)$ *ta có* $x^3M(x)/G(x) = x^8+x^7+x^5+x^3$ điều này tương đương với dịch chuỗi bít sang trái 3 bit.
- Như vậy ta sẽ có $x^3M(x) = Q(x^3) + R(x)*G(x)$
- Đa thức cần truyền đi T(x) sẽ có dạng sau:

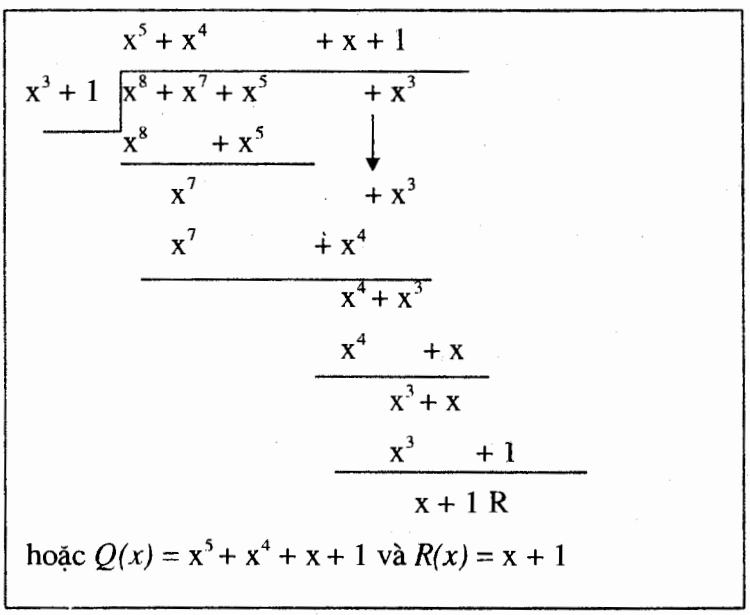
$T(x) = x^8 + x^7 + x^5 + x^3 + x + 1$

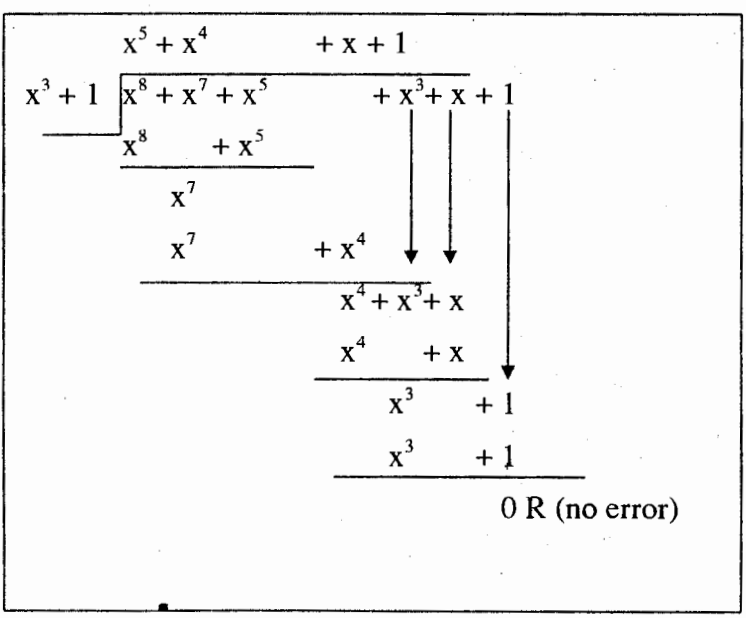
- Việc chuyển đổi từ dạng đa thức về dạng chuỗi bit được thực hiện như sau:

$(1)x^8 + (1)x^7 + (1)x^6 + (1)x^5 + (0)x^4 + (1)x^3 + (0)x^2 + (1)x^1 + (1)x^0$

- Chuỗi bit truyền đi là 110101011
- Việc kiểm tra CRC của bên nhận sẽ được thực hiện bằng cách chia đa thức nhận cho $G(x) = x^3+1$., nếu R(x)= 0 thì dữ liệu nhận được không bị lỗi.

Cách thực hiện phép sinh đa thức sẽ theo thuật toán cộng Modul 2 như sau:



Các đa thức sinh (khởi tạo) G(x) được sự dụng trong thực tế có dạng sau:

CRC 12 = $x^{12} + x^{11} + x^3 + x^2 + x + 1$

CRC 16 = $x^{16} + x^{15} + x^2 + 1$

CRC - CCITT = $x^{16} + x^{12} + x^5 + 1$

**Mã Hamming**

Mã Hamming là một kỹ thuật bổ xung thêm một bít thừa, gọi là mã Hamming, được bổ xung thêm vào để dò tìm và sửa lỗi. Sử dụng khoảng cách hamming (chiều dài của các bít này không giống với các bít thông tin), sẽ tiến hành dò và sửa lỗi:

- Nếu khoảng các hamming là m+1 hoặc dài hơn, m bit lỗi có thể được tìm thấy.
- Nếu khoảng cách hamming là 2n+1 hoặc dài hơn, n bít lỗi có thể được sửa.

Nếu dữ liệu truyền dẫn là ($m_3$, $m_2$, $m_1$, $m_0$) = (1010), sử dụng kỹ thuật mã Hamming ta có biểu thức của lỗi được tìm thấy như sau:

$c_0 = m_0 \oplus m_1 \oplus + m_3$

$c_1 = m_0 \oplus m_2 \oplus + m_3$

$c_2 = m_1 \oplus m_2 \oplus + m_3$

$c_0 = 0 \oplus 1 \oplus 1 = 0$

$c_1 = 0 \oplus 0 \oplus 1 = 1$

$c_2 = 1 \oplus 0 \oplus 1 = 0$

Giá trị mã (Hamming code) được tạo ra có dạng sau: $m_3\ m_2\ c_2\ m_1\ m_0\ c_1\ c_0$ - suy ra mã được tạo ra sẽ là 1010010.

Khi bên thu nhận được giá trị mã trên nó sẽ kiểm tra lỗi bằng cách các giá trị $p_0$, $p_1$, $p_2$

$p_0 = c_0 \oplus m_0 \oplus m_1 \oplus m_3$

$p_1 = c_1 \oplus m_0 \oplus m_2 \oplus m_3$

$p_2 = c_2 \oplus m_1 \oplus m_2 \oplus m_3$

Nếu $p_0 = p_1 = p_2 = 0$ thì giá trị mã nhận được sẽ không có lỗi, nếu chúng khác không thì giá trị nhận được có lỗi và vị trí bit lỗi nằm ở vị trí $p_2\ p_1\ p_0$. Ví dụ giá trị nhận được không phải chuỗi bit 1010010 mà là 1110010, ta sẽ có:

$p_0 = 0 \oplus 0 \oplus 1 \oplus 1 = 0$

$p_1 = 1 \oplus 0 \oplus 1 \oplus 1 = 1$

$p_2 = 0 \oplus 1 \oplus 1 \oplus 1 = 1$

Như vậy vị trí lỗi sẽ nằm ở bít số ($p_2\ p_1\ p_0$ = 110) số 6.

### 2.2.2 Mã hoá và nén tin

Các kỹ thuật mã hoá sử dụng một dạng trộn lẫn dữ liệu có thể đảo ngược để chuyển đạt dữ liệu thành không đọc được mà không có khoá. Khoá là một mã từ hoặc mã số cho phép phần mềm mã hoá/ giải mã trộn lẫn và thôi trộn lẫn dữ liệu.

Miễn là có thời gian, mọi kỹ thuật mã hoá đều có thể bị bẻ khoá. Các máy tính cao tốc có thể bẻ khoá nhiều mã bằng cách đơn giản thử các giá trị khoá khác nhau cho đến khi tìm được đúng khoá. Do đó, người ta đã nỗ lực tạo các thuật toán mã hoá tự hào là khó bị bẻ. Hai kỹ thuật chung đó là: khoá công khai và khoá riêng.

**Các khoá riêng**

Các khoá riêng [private key] sử dụng cùng một khoá để mã hoá và giải mã thông điệp. Phương pháp này có vài nhược điểm. Bên gửi và bên nhận phải bảo đảm thông báo cho nhau về khoá đó. Nếu khoá bị chặn, thông điệp sẽ bị tổn hại. Mỗi lần khoá thay đổi- các khoá riêng thường được thay đổi đề phòng chúng bị phá hoại-khoá mới phải được truyền thông và dễ bị phát hiện.

**Các khoá công khai**

Với kỹ thuật khoá công khai [public key], một khoá công khai được dùng để mã hoá các thông điệp, và sau đó một khoá riêng được dùng để giải mã. Khoá công khai được người dùng tạo bằng cách áp dụng một thuật toán cho khoá riêng, là khoá mà chỉ có bên nhận thông điệp mới biết.

Bên gửi sẽ dùng khoá công khai để mã hoá thông điệp và không biết hoặc không cần biết đến khoá riêng. Thực tế, những ai có khoá công khai của một người đều có thể mã hoá thông điệp cho người đó. Bên nhận sẽ giải mã thông điệp bằng cách tổ hợp khoá công khai với khoá riêng, và riêng chỉ có họ mới biết được khoá riêng đó.

Các thuật toán dùng để mã hoá khoá công khai cự kỳ phức tạp và kể cả siêu máy tính cũng khó lòng tìm ra đúng khoá trong một quãng thời gian hợp lý (ví dụ, cả đời bạn). Tuy vậy, các nhà tạo mã chưa bao giờ vượt qua nổi các tay bẻ khoá mã, và các kỹ thuật mã hoá phức tạp hơn vẫn không ngừng được phát triển.

**Phương pháp nén và giải nén**

Trước đây, kiểu dữ liệu được sử dụng trong việc truyền dẫn là các các dữ liệu kiểu ký tự đơn giản nhưng ngày nay dữ liệu rất đa dạng, có chứa nhiều ảnh tĩnh và video. Đây là kết quả làm tăng kích cỡ dữ liệu và làm tăng mật độ lưu thông trên mạng cả hai vấn đề này đều làm cho giá thành thông tin tăng lên. khi truyền dẫn tín hiệu âm thanh số các tín hiệu này phải truyền dẫn ở tốc độ 64 kbits/s. Do đó, việc nén dữ liệu là một vấn đề quan trọng trong những trường hợp mà dữ liệu gốc gây ra nhiều bất lợi về giá thành.

Nén dữ liệu số được ứng dụng cho cho nhiều kiểu dữ liệu số đa dạng như âm thanh, ảnh tĩnh và video (TV pictures), điều này đặc biệt hiệu quả và có ích đối với hầu hết các loại hình thông tin giải rộng và thông tin yêu cầu tốc độ truyền dẫn lớn. Trường hợp ảnh TV, ví dụ ảnh động có thể tạo ra bằng cách gửi 30 khung trong một giây, nhưng nếu chúng được số hoá thì ở tốc độ truyền dẫn 100Mbit/s hoặc hơn nữa chất lượng hình ảnh vẫn như vậy. Tuy nhiên trong việc phân tích tỉ mỉ bức ảnh thì nền và các đặc tính khác của nó không thay đổi thường xuyên. Điều này có nghĩa là các bức ảnh phía sau nhận được từ sự thay đổi một số thành phần của bức ảnh phía trước. Nội dung thông tin không suy giảm đáng kể bằng việc chỉ gửi đi các phần này. Hơn nữa để việc nén có hiệu quả có thể thực hiện bằng phương pháp employing (nén chuyển động) đó là phương pháp dựa vào hình dạng của vật thể và chuyển động của các vật thể hiện tại.

Đối với hệ thống thông tin di động thì phạm vi tần số đã được giới hạn trước do vậy tín hiệu âm thanh có thể được nén ở tốc độ 11.2 kbit/s. Hiện nay các ứng dụng này còn có thể được nén ở tốc độ chỉ bằng một nửa, nén tín hiệu đến 5,6 kbit/s.

Phương pháp nén và giải nén dữ liệu được trình diễn như sau.

**1.Nén theo Mã Huffman**

Mã huffman là một phương pháp nén được khám phá bởi D.A.Huffman, đó là phương pháp thay thế các ký tự và các chuỗi dữ liệu tìm thấy bằng các mã ngắn hơn.

Hãy quan sát xem chuỗi ký tự R={vuxzvvyyzuvyzvzuyvuu} được mã hoá như thế nào. Năm ký hiệu được tìm thấy trong chuỗi ký tự là x, y, z, u, v. Ba bít sẽ được dùng để biểu diễn cho mỗi ký tự này nghĩa là 60 bit sẽ được dùng để biểu diễn cho 20 ký tự.

Ví dụ phương pháp biểu diễn bình thường

| | |
|---|---|
| X | 000 |
| Y | 001 |
| Z | 010 |
| U | 011 |
| V | 100 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| V | U | X | Z | V | V | Y | Y | Z | U |
| 100 | 011 | 000 | 010 | 100 | 100 | 001 | 001 | 010 | 011 |
| V | Y | Z | V | Z | U | Y | V | U | U |
| 100 | 001 | 010 | 100 | 010 | 011 | 001 | 100 | 011 | 011 |

Mã Huffman được phân phát theo xác suất của "tần số xuất hiện" (một giá trị có thể tìm được bằng việc chia tổng số ký hiệu cho thời gian mỗi ký hiệu suất hiện trong chuỗi ký hiệu đó). Nhìn chung với chuỗi ký hiệu có dạng $M = \{a_1, a_2, .., a_M\}$, khả năng

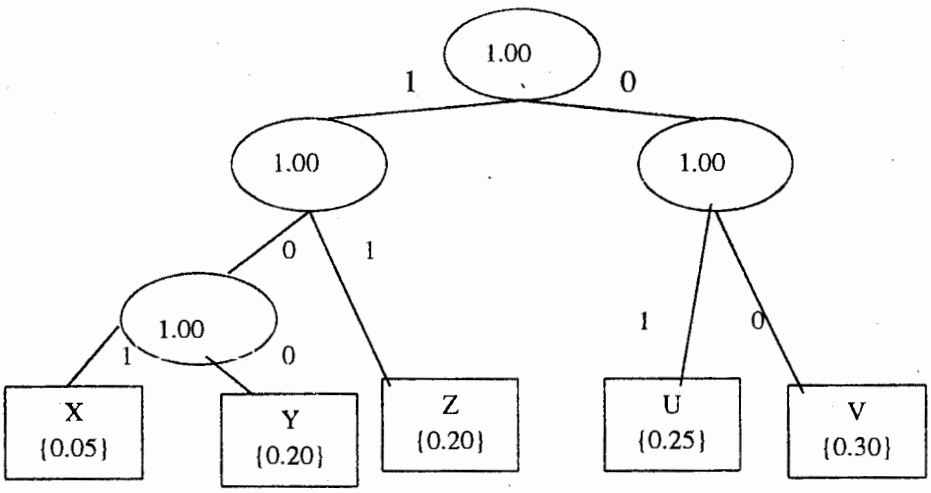
xảy ra (tần số xuất hiện) với một lần xuất hiện được biểu diễn là $P(a_i)$. Trong ví dụ cụ thể trên ta có kết quả tần số sự cố của tất cả các ký hiệu trong chuỗi kí hiệu R.

| Kí hiệu | Số lần xuất hiện | Tần số xuất hiện |
|---|---|---|
| X | 1 | 0.05 |
| Y | 4 | 0.20 |
| Z | 4 | 0.20 |
| U | 5 | 0.25 |
| V | 6 | 0.30 |

Cơ chế làm việc của mã Huffman, với các ký hiệu không xuất hiện thường xuyên (có tần số xuất hiện thấp) sẽ được phân phối một mã có chiều dài bít dài, với những ký hiệu xuất hiện thường xuyên (tần số xuất hiện cao) sẽ được phân phối các bít ngắn.

Cấu trúc mã Huffman cho các kí tự sẽ như sau:

| Kí tự | Chuỗi bit |
|---|---|
| X | 101 |
| Y | 100 |
| Z | 11 |
| U | 01 |
| V | 00 |




**Hình 2.10. Cây Huffman**

Sản phẩm của mã Huffman :

1. Sắp xếp theo chiều giảm dần của tần số xuất hiện. Nó đóng vai trò là ký hiệu ở vị trí đầu tiên trong trường hợp các ký hiệu có tần số xuất hiện giống nhau.

2. Các ký hiệu với tần xuất xuất hiện nhỏ nhất và các ký hiệu có tần xuất xuất hiện nhỏ nhất tiếp theo sẽ tạo thành các nút của cây, và một nút mới sẽ được thiết lập. Nút này có được từ tổng tần xuất xuất hiện của hai ký hiệu. Cành cây từ nút này sẽ hướng tới ký hiệu có tần xuất xuất hiện thấp nhất và có nhãn là 1, cành cây khác sẽ có nhãn là 0.

3. Trở về việc tạo nút trong bước hai giống như một mã mới, bước hai được tiếp tục làm lại cho tới khi không có một nút mới được tạo ra.

4. Nút đứng đầu sẽ là nút gốc

Hình 2.10 cho thấy dùng mã Huffman cho chuỗi ký hiệu R có thể dùng 45 bit để biểu diễn cho 20 ký tự.

Mã Huffman dùng để nén các loại dữ liệu kiểu ký tự. Hiện nay mã Huffman được sử dụng trong JPEG, MPEG và các phương pháp nén khác.

Khuôn dạng mới của chuỗi kí tự theo mã Huffman có dạng sau:

| V | U | X | Z | V | V | Y | Y | Z | U |
|---|---|---|---|---|---|---|---|---|---|
| 00 | 01 | 101 | 11 | 00 | 00 | 100 | 100 | 11 | 01 |

| V | Y | Z | V | Z | U | Y | V | U | U |
|---|---|---|---|---|---|---|---|---|---|
| 00 | 100 | 11 | 00 | 11 | 01 | 100 | 00 | 01 | 01 |

**2. Nén JPEG (Joint Photographic coding Expert Group)**

JPEG là một tiêu chuẩn được dùng phổ biến trên thế giới dùng để nén và giải nén các bức ảnh thông qua việc số hoá màu sắc và độ sáng tối, thông thường nó dựa vào một phương pháp nén không thuận nghịch (DCT: biến đổi hàm Cosin rời rạc) (một phương pháp thuận nghịch hiện có).

Phương pháp này có tỉ số nén rất cao (từ 1/8 đến 1/100), nó được dùng để truyền tải ảnh màu trên Internet.

JPEG bao gồm hai kiểu nén dữ liệu.

Nén thuận nghịch: Sau khi giải mã dữ liệu mã hoá, có sự phục hồi lại hoàn toàn khuôn dạng gốc.

Nén không thuận nghịch: Sau khi giải mã dữ liệu mã hoá không có sự phục hồi lại hoàn toàn khuôn dạng cũ tuy nhiên hình ảnh quan sát được sẽ hầu như không có gì khác cả.

Thêm nữa JPEG còn có một phương pháp nén khác cho các ảnh tĩnh gọi là LZW, phương pháp này được sử dụng cho ảnh GIF (Graphics Interchange Format). Tuy nhiên phương pháp này là một kỹ thuật cao cấp.

**3. Nén MPEG (Motion Pictures Coding Expert Group)**

MPEG là một tiêu chuẩn nén và giải nén âm thanh và hình ảnh video nó được tiêu chuẩn hoá bởi ISO và IEC (International Electrotechnical Commission).

MPEG cho một khả năng nén cao với chất lượng cao, nhưng nó sẽ chiếm thời gian phục hồi nén, thời gian phục hồi lại này thường phải nhờ phần cứng.

Tiêu chuẩn hoá việc mã hoá MPEG được chia làm 4 cấp gọi là MPEG 1, MPEG 2, MPEG 4, MPEG 7.

**MPEG 1** : đã được tiêu chuẩn hoá bởi ITU-T từ năm 1992. Sử dụng tiêu chuẩn này ta có thể nén ảnh video đến 1.5 Mbit/s.

**MPEG 2**: đã được tiêu chuẩn hoá bởi ITU-T từ năm 1994. Sử dụng tiêu chuẩn này ta có thể nén ảnh TV vào khoảng 3-6Mbít/s, và nén ảnh chi tiết, ảnh TV có độ nét cao vào khoảng 10-20 Mbit/s.

**MPEG 4:** Với phạm vi tốc độ truyền dẫn từ vài kbit/s đến nhiều kbit/s MPEG 4 có thể được sử dụng cho thông tin di động.

**MPEG 7:** được triển khai sau và được mường tượng để sử dụng cho các phương tiện tìm kiếm tốc độ cao cho loại hình thông tin đa phương tiện.

**4. Nén Mã FAX**

Fax là công nghệ và thiết bị để truyền dẫn dữ liệu kiểu văn bản, hình ảnh, vv.

Tiêu chuẩn quốc tế của Fax đối với việc sử dụng cho đường truyền tương tự là G3, và G4 là tiêu chuẩn sử dụng cho đường truyền tốc độ cao giống như đường ISDN. Trong Fax, dữ liệu như văn bản hoặc hình ảnh .v.v được xem giống như hình ảnh ta quét (scan), sau đó nó sẽ được mã hoá bằng phương pháp CODEC. ở giai đoạn này số lượng dữ liệu sẽ rất lớn nếu bức ảnh chỉ được mã hoá giống hệt nó. MH, MR, MMR, run-length, vv.. là một vài công nghệ nén và mã được dùng trong mã Fax.

**MH (Modified Huffman)** là phương pháp nén mã Fax đã được tiêu chuẩn hoá bởi ITU-T. Đây là phương pháp nén được xây dựng sau ý tưởng mã Huffman, và tin vào sự liên tiếp của các tín hiệu đen và trắng. Mỗi đường quét được xử lý riêng biệt, gọi là "phương pháp mã hoá một thứ nguyên" (one-dimensional encoding method).

**MR (Modified READ):** MR được tiêu chuẩn hoá bởi ITU-T, và nó là một phương pháp mã hoá Fax mang lại tỉ số nén cao hơn so với phương pháp MH. Đây là

phương pháp mã hoá hai thứ nguyên, phương pháp này dựa trên sự tương quan giữa các đường quét theo hướng dọc, nó hiệu quả hơn so với phương pháp mã hoá một thứ nguyên.

**MMR (Modified Modified READ:** MMR là phương pháp nén mã hoá, phương pháp này chỉ tiến hành hiệu chỉnh một phần do vậy nó đem lại hiệu quả cao hơn so với phương pháp MR

**Run-Length :**Phương pháp mã hoá run-length biểu diễn các phần tử giống nhau được tìm thấy dưới dạng số lần phần tử đó lặp lại. Sử dụng phương pháp này dữ liệu như "xxxxxyyyyxxxxxxx" được biểu diễn như sau "05x04y07x".

## 2.3 Máy tính và Khả năng truyền tin

### 2.3.1 Cấu trúc máy tính

Nguồn gốc của máy tính xuất phát từ các bàn tính ra đời ở thế kỷ 18 và đến nay thay cho chúng các loại calculator đã là một công cụ tính toán phổ cập. Tiếp theo là các máy tính cơ khí hoạt động chưa có bộ nhớ, chưa chạy theo chương trình và vào giữa thế kỷ 20 máy tính điện tử hoạt động theo chương trình được chế tạo thuộc họ máy Von Newmann. Các lệnh của máy chỉ thực hiện theo chế độ tuần tự. Các máy này đã phải trải qua 4 thế hệ là điện tử, bán dẫn, IC, và VLSI.

Bảng 2.4

**Lịch sử phát triển của các hệ máy tính**

| Năm | Các thời kỳ xử lý | Mục đích chính | Ví dụ | Công nghệ |
|---|---|---|---|---|
| 1950-1960 | Xứ lý lô | Tiết kiệm chi phí | Dùng trong tính toán và thiết kê kỹ thuật | Thế hệ thứ 2- (bóng điện tử) |
| 1970 | Xử lý trung tâm | Tiết kiệm chi phí và hiệu quả nội bộ | Lưu trữ dữ liệu.<br>mô phỏng quá trình kiểm soát sản phẩm. | Thế hệ thứ 3 (IC)<br>*Hệ thống đĩa.<br>*Hệ thống thiết bị đầu cuối chuyển tải dữ liệu |
| 1980 | xử lý phân tán | Tiết kiệm chi phí và phục vụ khách hàng. | Cơ sở dữ liệu thời gian thực<br>Siêu xử lý | Thế hệ thứ 3,5 (LSI)<br>*Máy tính mini.<br>*Cơ sở dữ liệu với đĩa |

| | | | | |
|---|---|---|---|---|
| | | | | dung lượng lớn. |
| 1990 | Xử lý phân tán | Tự động hoá văn phòng và dịch vụ thông tin | Hệ thống thư tín điện tử.<br>Thông tin các nhân<br>Thông tin gia đình | Thế hệ thứ 4 (VLSI)<br>*Ngôn ngữ cấp cao<br>*Truyền dữ liệu số |
| 2000 | Mạng và xử lý khách chủ | Làm ra lợi nhuận và dịch vụ toàn diện | *Tái xử lý quá trình kinh doanh<br>*Truyền dữ liệu thời gian thực<br>*Rôbốt trong gia đình | Thế hệ thứ 5 (linh kiện mới)<br>*Ngôn ngữ tự nhiên<br>*Truyền thông đa phương tiện<br>*Mạng liên kết |

Hiện nay loài người đang lỗ lực nghiên cứu chế tạo máy tính thế hệ 5 là loại máy tính không thuộc họ Von Newmann. Nó xử lý song song, có bộ nhớ hoạt động theo nguyên tắc liên hợp chứ không theo nguyên tắc đánh địa chỉ, có cấu trúc xử lý trí thức. Tiến triển của các hệ máy tính được trình bày trong bảng 2.4

Từ trước đến nay đã có nhiều cuộc cách mạng trong công nghiệp chế tạo máy tính điện tử. Đầu tiên là vào những năm 50, khi thị trường máy tính bắt đầu hình thành. Lúc đầu chỉ vài chục máy tính lớn (Mainframe), sau đó trên thị trường phát triển lên hàng ngàn chiếc.

Cuộc cách mạng thứ 2 là vào những năm 60, khi phát hiện ra rằng một máy tính có thể hội thoại với các máy tính khác qua đường điện thoại. Và từ đó đến nay các máy tính hội thoại với nhau liên tục phát triển.

Vào những năm 1970 có hai cuộc cách mạng xảy ra đồng thời. Một là sự ra đời của vi xử lý đã giảm đáng kể giá máy tính. Hai là các hãng chế tạo máy tính đã phát triển các kiến trúc mạng toàn diện cho việc nối ghép các máy tính của họ qua các thiết bị truyền thông.

Trong những năm 1980 thị trường máy tính cá nhân (PC), mạng cục bộ và workstation phát triển rầm rộ.

Thập niên 90 là thập niên của mạng máy tính toàn cầu. Các cấu trúc mạng đã được phát triển từ những năm 70 nay mới có đủ điều kiện để phát huy tác dụng. Các loại máy tính mạng mới (NC) ra đời với cấu trúc phần cứng đơn giản, tận dụng tài

nguyên trên mạng và là một đối thủ cạch tranh chính với máy tính PC trong tương lai gần.

Nừu CPU và bộ nhớ là trái tim và bộ não của máy tính thì linh hồn của nó là hệ điều hành và các phần mềm ứng dụng. Linh hồn máy cũng trải qua nhiều giai đoạn.

Đầu tiên máy tính chỉ làm được từng chức năng đơn lẻ là giai đoạn máy tính xử lý đơn năng. Dần dần nó phát triển lên mức thực hiện đa năng rồi đến mức xử lý tập trung và hiện nay đang phát triển ở mức xử lý phân tán. Vào cuối thập kỷ này máy tính có thể có mức xử lý thông minh cao nhưng cũng còn xa với mức thông minh của con người.

Chi phí cho phần cứng ngày càng giảm và giá của các phần mềm ngày càng tăng. Trong vòng 3 thập kỷ gần đây giá máy tính cứ 3 năm lại giảm một nửa. Phần mềm ngày càng đắt và nhất là phần mềm có đặc thù ứng dụng riêng.

**Các loại máy tính họ máy tính họ Von Newmann.**

- **Máy tính lớn (Mainframe) và máy tính MINI:**

Hai hãng chế tạo máy tính lớn và máy tính mini mạnh nhất thế giới ngày nay là IBM (International Business Machine) và DEC (Digital Equipment Corporation) .Các loại máy IBM main frame tiêu biểu như :

*Các máy lớn*: System/ 370, S/ 3090, S/ 4300, ES/ 9370(1990),RS6000..

*Các máy bậc trung*: System/ 360(1965), System Application/ 400(1988)

*Các hệ điều hành* cho các máy lớn: VM, VSE, MVS và các máy trung: OS/ 400

Hiện nay IBM đang đưa ra các kiến trúc SAA ( System Application Architecture) là một tập các thủ tục để đảm bảo độ tương thích giữa các dòng họ máy tính của hãng. Đây cũng là một kế hoạch lớn của IBM nhằm phát triển hệ thống phần mềm trong những năm 1990.

- ***Các máy vi tính(PC) :***

Các máy vi tính phát triển có sức mạnh ngày càng cao. Có ba loại workstation phổ cập nhất đang cạnh tranh nhau và được chế tạo hàng loạt là:

- Họ IBM PS/2 và tương đương.
- Các máy Macintosh
- Các trạm làm việc UNIX.

Các máy vi tính được chế tạo từ các họ vi xử lý của các hãng Intel, Motorola và một số hãng khác. Hiện nay người ta chia bộ sử lý trung tâm CPU ra làm 2 loại:

- CPU với tập lệnh đầy đủ CISC ( Complex instruction Set Computing): intel 8086, 80x86, Pentium, MC 680x0. . .

- CPU với tập lệnh rút gọi RISC ( Reduced instruction Set Computing): MC 88000, SPARC, DECchip 21064. . .

So sánh giữa hai bộ lệnh của CISC và RISC ta thấy:

| CISC | RISC |
|---|---|
| 20% số lệnh thường được dùng | Chỉ có các lệnh hay dùng nhất |
| 80% số lệnh ít dùng | |
| Các lệnh có độ phức tạp cao | Các lệnh đơn giản |
| CPU phức tạp do đó hoạt động chạm | CPU đơn giản nên hoạt động nhanh |

Do giá thành rẻ và khả năng máy tính ngày càng lớn nên thị trường máy vi tính ngày càng phát triển. Tuy nhiên các máy lớn vẫn có một số lợi thế so với các máy tính như:

- Khả năng hoạt động với số lượng lớn terminal.
- Khả năng xử lý hữu hiệu các cơ sở dữ liệu lớn.
- Khả năng bảo mật các dữ liệu tốt hơn.

Do những đặc điểm nêu trên nên xu thế phát triển hiện nay là phối hợp các chủng loại máy tạo thành một mạng máy tính tổng thể để phát huy được sức mạnh của từng loại máy.

**Sự phát triển của phần mềm**

Một cấu trúc máy tính gồm các phần chính sau:

- Phần cứng kể cả các thiết bị ngoại vi
- Phần mềm cơ sở – BIOS
- Hệ điều hành
- Các chương trình ứng dụng

Cừu trúc phần cứng một máy vi tính cơ bản điều bao gồm một bộ xử lý trung tâm (CPU), bộ nhớ động (RAM), Bộ nhớ chương trình (ROM) và các IC logich hỗ trợ khác như : bộ đệm, bộ tạo xung nhịp đồng hồ, bộ giãi mã. Bộ Vi sử lý trung tâm CPU là đầu não của mọi hoạt đông của máy tính nó hoạt đông theo một chương trình cho trước được nạp vào ROM hoặc RAM. Các tín hiệu vật lý trao đổi giữa CPU với các IC loghíc khác được thông qua ba luồng ( BUS ) thông tin chính lá BUS địa chỉ, BUS số liệu và BUS điều khiển. Tuỳ theo từng loại CPU sử dụng trong máy vi tính mà số lượng các bit thông tin trong từng BUS này khác nhau vị dụ đối với CPU 80286 số bit ở BUS số liệu là 16 bit, đối với CPU 80586 số bit ở BUS số liệu là 64 bit ...BUS địa chỉ giúp cho CPU quản lý và điều khiển được hàng Gbyte bộ nhớ và hơn 65000 các thiết bị ngoại vi khác nhau, BUS Số liệu giúp cho CPU đọc các chươnng trình đưới dạng mã máy, lưu trữ và

trao đổi số liệu từ RAM, ROM, gửi và nhận các tín hiệu số từ các thiết bị ngoại vi mà máy tính quản lý. BUS điều khiển.dùng để phân biệt trạng thái và các chế độ làm việc của CPU như chế độ đọc mã lệnh, chế độ làm việc với bộ nhớ ( Đọc hoặc ghi), chế độ làm việc với ngoại vi ...

Trước kia hệ điều hành và các chương trình ứng dụng phát huy được hết các khả năng của phần cứng. Nhưng ngày nay với các chip vi xử lý như intel 586, Pentium Motorola 68040 với đường BUS dữ liệu 64 Bít thì hạn chế cho người sử dụng lại chính là ở hệ điều hành. Nói cách khác phần cứng đã đi trước phần mềm. Điều này cũng dễ hiểu do khi một bộ vi xử lý mạnh mới ra đời cần có thời gian để các chuyên gia phần mềm thiết kế và sử dụng hệ điều hành chạy trên nó và tiếp đến mới là các chương trình ứng dụng.

*Các hệ điều hành máy tính:*

Hệ điều hành máy tính làm nhiệm vụ nối ghép giữa phần cứng với các chương trình ứng dụng. Nó có một số chức năng chính như sau:

- Quản lý các tài nguyên như bộ nhớ thời gian CPU
- Điều hành việc thực hiện các chương trình ứng dụng
- Quản lý các tệp chứa trong đĩa cứng và đĩa mềm
- Quản lý người sử dụng
- Hỗ trợ các thiết bị ngoại vi

Hiện nay các hệ điều hành sau đã trở thành hàng chuẩn cho nhiều phần mềm ứng dụng:

- MS-DOS, Windows: cho họ vi xử lý intel 80x86
- MacOS: cho họ Motorola 680x0
- OS/2: cho họ intel 80x86
- UNIX,Linux: không phụ thuộc vào họ vi xử lý

Các hệ điều hành của mainframe IBM như VM (Virtual Machine), MVS (Multiple Virtual System), VSE (Virtual Strorage extended), OS/400 cho máy IBM AS/400. VMS (Virtual Memory System) cho các máy tính mainframe VAX 9000, mini VAX 2000, 3000, 6000 và VAX station. DEC đang cho ra hệ điều hành OSF/1 là một hệ điều hành UNIX hiện đại dùng cho thập kỷ 90.

MS DOS có nhiều hạn chế như đơn nhiệm, một người sử dụng nhưng có nhiều lợi thế như rẻ tiền và được chạy trên với hầu hết các máy vi tính, laptop, notebook và có nhiều chương trình ứng dụng đã được sản xuất hàng loạt. Sự kết hợp với MS-Window

có các chức năng đa nhiệm và phối ghép đồ hoạ GUI ( Graphic user Interfase) được bổ xung làm nó càng có sức hấp dẫn người sử dụng.

MacOS là hệ điều hành cho các máy Macintosh và rất phù hợp cho các ứng dụng ẩn loát. Nó là hệ điều hành phổ biến thứ hai sau MS DOC. Khả năng đồ hoạ của nó rất phát triển mà Microsoft bây giờ mới đưa vào MS-Windows.

OS/2 được hãng IBM và hãng Microsoft đưa ra năm 1987 là sản phẩm tiếp theo sau MS-DOS. Nó là hệ điều hành đa nhiệm một người sử dụng có đồ hoạ và nhiều khả năng giống Unix. Các chương trình ứng dụng của OS/2 còn chưa nhiều. Trong tương lai, kết hợp với MS-DOS/MS-Windows, nó sẽ đạt tới khả năng gần UNIX và chiếm được nhiều ứng dụng trong các hệ thống xuất bản.

UNIX đã trở thành chuẩn công nghiệp và được dùng ở nhiều hệ thống lớn. Nó là hệ diều hành đa nhiệm nhiều người sử dụng. UNIX được viết trên C và đi cùng với C nó được sử dụng rộng rãi để phát triển các chương trình ứng dụng từ workstation đến mainframe. UNIX có một số ưu thế như sau:

- Là hệ xử lý đa nhiệm, nhiều người sử dụng có khả năng hội thoại qua ống (pipes), dùng chung bộ nhớ (shared memory), semaphones, bộ nhớ ảo v .v. . .
- Có khả năng định hướng vào/ ra ( Input/ Output Redirection)
- Có các thủ tục giao diện mạng như TCp/IP, NFS
- Có các shell chuyên dùng cho các ứng dụng khác nhau như Bourne shell cho các trường đại học và Viện nghiên cứu khoa học, C-shell, Kron shell trên nguyên lý WIMP (Window, Icons, Menues và Poiting devices ) cho các người sử dụng như NeXTStep, Motif, Open Destop, Open look.

Mặc dù chưa có nhiều ưu điểm nhưng UNIX cũng còn một số nhược điểm như:

- Chưa có một hệ UNIX chuẩn tuyệt đối. Vì có quá nhiều loại UNIX nên các chương trình ứng dụng cũng phụ thuộc nhiều các chủng loại UNIX và phần cứng kèm theo.
- Quá nhiều GUI Shell khác nhau, chưa có một chuẩn độc nhất nên các chương trình ứng dụng phụ thuộc nhiều vào Shell nó chọn.
- Sử dụng phức tạp đòi hỏi phải có chuyên gia xử lý lỗi, bảo trì, cài đặt thiết bị, phần mềm mới, kết nạp thêm người sử dụng v.v...

### 2.3.2 Khả năng truyền tin của máy tính

Bất kể một loại máy tính nào được sản xuất hiện nay cũng đều có khả năng truyền tin của nó với các thiết bị ngoại vi hay máy tính khác. Việc trao đổi số liệu lưu trữ trên đĩa cứng của nó với các máy tính PC khác hoặc thiết bị ngoại vi được thực hiện qua các phương thức sau:

- Qua đĩa mềm, đĩa CD, đĩa cứng .. bằng phương pháp vận chuyển thủ công.
- Qua cổng truyền tin nối tiếp không đồng bộ (Cổng COM) theo giao diện RS232.
- Qua cổng truyền tin song song hay còn gọi là cổng máy in.
- Qua đường kết nối mở (SLOT) trên bo mạch chủ của PC.

**Phương thức truyền tin nối tiếp:**

Trên mỗi máy tính PC thường được sản xuất sẵn hai cổng nối tiếp RS232 (Serial –COM1 ,COM2 ). Đây là các cổng truyên tin nối tiếp theo nguyên tắc dị bộ.

Bảng 2.5

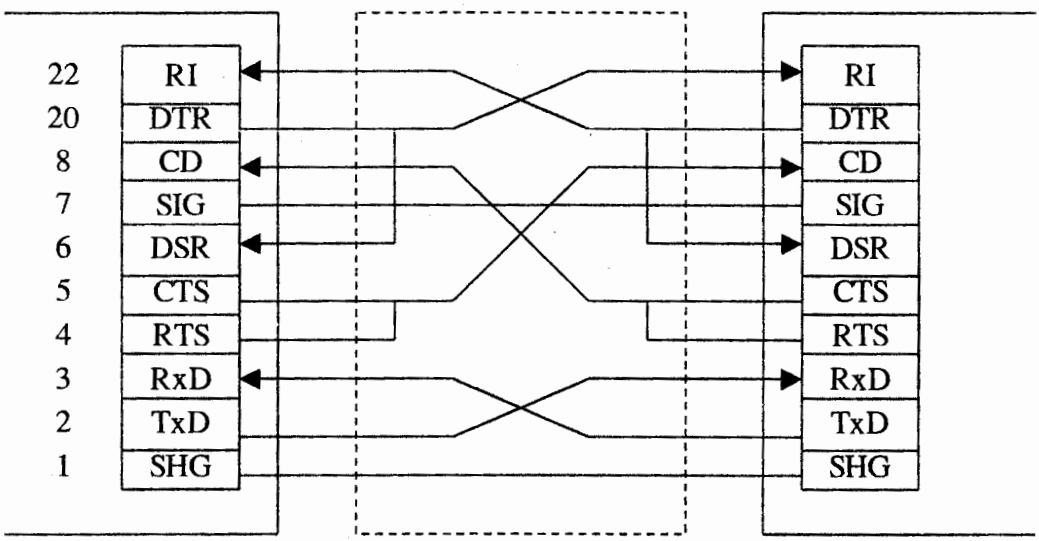
**Mô tả sơ đồ đấu nối các chân của cổng RS232**

| CHÂN | CHỨC NĂNG | TÊN GỌI | VỊ TRÍ |
|---|---|---|---|
| (TxD) | Kênh truyền số liệu | Transmit Data | 2 |
| (RxD) | Kênh nhận số liệu | Receive Data | 3 |
| ( RST) | Tín hiệu yêu cầu phát | Request to Send | 4 |
| (CTS) | Sẵn sàng cho phát | Clear to Send | 5 |
| (DSR) | Số liệu sẵn sàng | Data Set Ready | 6 |
| (GND) | Chân tiếp đất | Ground | 7 |
| (CD) | Có tín hiệu đồng bộ | Data Carrier Detect | 8 |
| (DTR) | Thiết bị đầu cuối sẵn sàng | Data Terminal Ready | 20 |
| (RI) | Chỉ thị báo chuông gọi | Ring Indicator | 22 |

Hai tín hiệu quan trọng nhất của cổng COM là tín hiệu TxD và tín hiệu RxD. TxD là số liệu số nối tiếp phát đi từ máy tính ra thiết bị ngoại vị và RxD là tín hiệu phát từ ngoại vị vào máy tính . Các tín hiệu này được pháp đị với các tộc độ khác nhau từ 300 đến 115000 bit/ giây do người sử dụng lập trình với tín hiệu vật lý tương ứng là bít 0 ứng với mức +12V , bit 1 ứng với mức -12V. Các tín hiệu còn lại trên cổng COM là các tín hiệu điều khiển trợ giúp như tín hiệu DTR báo cho máy tính biết thiết bị ngoại vị đã sẵn sàng làm việc, tín hiệu RTS báo cho ngoại vi biết máy tính chuẩn bị phát số liệu. Toàn bộ các thông số của cổng COM được điều khiển thông qua các cổng địa chỉ trong thanh ghi của IC 8050

Cổng COM thường được dùng để truyền số liệu trực tiếp giữa hai máy tính PC với nhau trên khoảng cách đến 30m hoặc sử dụng kết nối với thiết bị điều chế và giải điều chế ( MODEM) để truy nhập trên khoảng cách lớn với một máy tính PC khác hoặc mạng máy tính thông qua mạng điện thoại công cộng hoặc đường truyền riêng (Xem mục 2.1.3) .

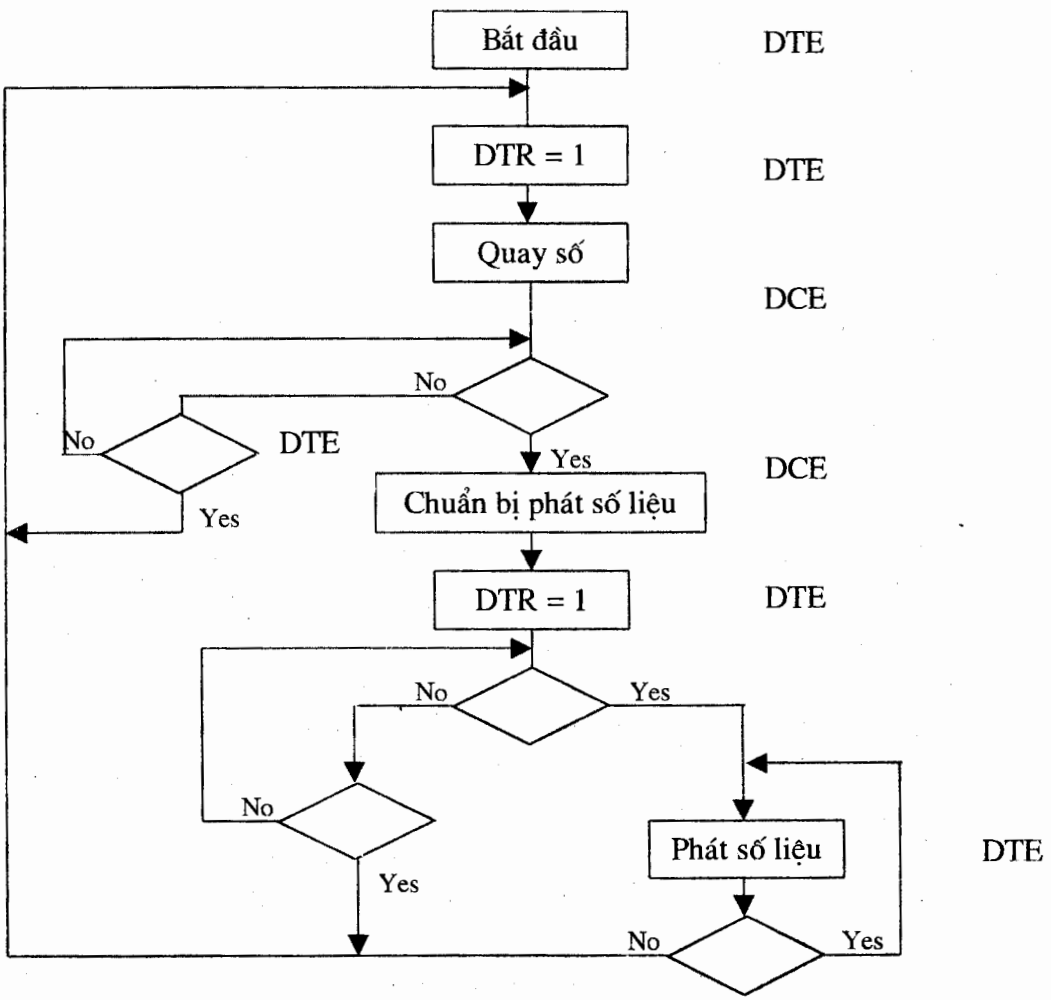
Hình 2.11 nêu phương thức đấu nối truyền số liệu giữa hai máy tính qua cổng RS232:




**Hình 2.11 Nối ghép hai máy tính qua cổng RS232**

Cách kết nối và thủ tục giao tiếp giữa máy tính (DTE) với Modem (DCE) qua cổng RS232 có thể mô tả tóm tắt như sau (hình 2.12):

Khi máy tính sẵn sàng (tương ứng với chân số 20 DTR=1) thì Modem cũng sẵn sàng (ứng với DSR=1). Modem sẽ kiểm tra tín hiệu trên đường dây, nếu phát hiện tháy có tín hiệu nhận (CD=1) ở chân số 8 thì thiết bị đầu cuối sẽ chuyển yêu cầu được gửi số liệu (Request To Send - RTS=1) từ chân số 4 tới Modem. Modem đã sẵn sàng để nhận số liệu nên sẽ gửi tín hiệu cho phép gửi (Clear To Send - CTS=1) lại cho thiết bị đầu cuối.




**Hình 2.12 Thủ tục trao đổi giữa máy tính và Modem**

Kết nối được thiết lập thông qua việc người sử dụng quay số gọi máy tính ở xa và đợi trả lời. Máy tính sẽ nối nếu không bận. Chuông dừng và người sử dụng nghe được trả lời. Khi đó, người sử dụng bấm vào nút dữ liệu (Data button), thiết bị đầu cuối được nối lên đường dây (ứng với DTR=1) và Modem tại chỗ sẽ trả lời sẵn sàng (ứng với Data Set Ready - DSR=1). Lúc này đèn báo kết nối đã được thiết lập. Khi có cuộc gọi, Modem của máy tính (Modem được gọi) reo chuông (RI=1), giả sử máy tính đã sẵn sàng nhận cuộc gọi (DTR=1), nó trả lời bằng cách đặt RTS=1. Điều này có hai hiệu ứng:

- Modem được gọi gửi tín hiệu mang (Carrier) đến Modem gọi để báo cuộc gọi được chấp nhận.
- Sau thời gian trễ, Modem được gọi đặt CTS=1 để máy tính có thể bắt đầu gửi số liệu. Máy tính gửi lời mời tới thiết bị đầu cuối rồi chuẩn bị nhận trả lời của người sử dụng, bằng cách đặt tín hiệu báo chưa sẵn sàng (DTS Off). Kết quả là chuông sẽ ngừng (Tone Off).

Khi Modem gọi (Calling Modem) kiểm tra thấy mất tín hiệu sóng mang (Carrier), nó đặt CD Off. Thiết bị đầu cuối gửi yêu cầu được chuyển số liệu (RTS=1) và Modem sẽ báo cho phép chuyển số liệu (CTS=1). Người sử dụng gõ bản tin trả lời (đèn hiển thị).

Khi quá trình gửi/nhận tin hoàn thành, cả hai tín hiệu sáng mang (Carrier) sẽ được ngắt (Switch Off), cuộc gọi kết thúc.

**Phương thức truyền tin qua cổng máy in** ( hay còn gọi là các cổng song song - parallel): Trên PC thông thường có từ 1 đến 3 cổng truyền tin song song ( LPT1, LPT2, LPT3 ) thường ghép với máy in hoặc truyền số liệu giữa hai máy tính với khoảng cách gần ( dưới 5m). Ưu điểm của phương pháp truyền song song là đạt tốc độ truyền cao thích hợp với các quá trình diễn ra nhanh tuy nhiên không thể truyền đi xa và khó kiểm tra độ chính xác của dữ liệu. Đầu ra của cổng song song được sử dụng JACK 25 chân gắn sau máy tính, bao gồm 8 đường số liệu phát ra và đọc vào giữa máy tính và thiết bị ngoại vi, 4 đường điều khiển phát ra từ máy tính và 4 đường đọc vào máy tính từ thiết bị ngoại vi. Mức tín hiệu trên các đường này tương ứng Bit 0 - +5V, Bit 1 - 0 V.Cổng song song được điều khiển bởi 3 cổng logich như sau :Cổng đọc phát số liệu có địa chỉ BASE_LPT1. Cổng phát điều khiển có địa chỉ BASE_LPT1.+2 và cổng đọc trạng thái có địa chỉ BASE_LPT1.+1. Việc điều khiển cổng song song ngoài các thủ tục thông thường của ROM BIOS chúng ta sử dụng chúng như những cổng vào ra thông thường.

**Phương thức ghép nối qua SLOT máy tính..**

Đây là phương thức ghép nối song song cho khả năng điều khiển tối đa nhất từ máy tính tới thiết bị ngoại vi. SLOT có 4 kiểu cấu trúc sau: ISA, EISA, kênh nhỏ (Micro Channel), PCI. Mỗi loại có cấu trúc vật lý khác nhau.

**Cấu trúc ISA:** là cấu trúc sử dụng trong máy tính IBM, máy tính XT và AT, cũng như trong tất cả máy tính bắt chước chúng. Nó cho phép cắm các cạc phần cứng thêm vào hệ thống bằng cách thức chèn vào khe mở rộng. ISA đã mở rộng từ đường 8 bit lên đường 16 bit trong năm 1984 khi IBM giới thiệu máy tính IBM PC/AT. ISA quy cho khe mở rộng chính nó (1 khe 8 bit hoặc 1 khe 16 bit). Khe 8 bit không tồn tại ngắn hơn khe 16 bit và trên thực tế gồm có 2 khe. Một cạc 8 bit có thể cắm vào khe 16 bit nhưng khe 16 bit không thể cắm vào khe 8 bit.

ISA đã là cấu trúc chuẩn của máy tính cá nhân trước khi Compaq và vài công ty riêng phát triển kênh EISA.

**Cấu trúc EISA** là kênh chuẩn được giới thiệu năm 1988 trên 9 công ty máy tính: AST Research, Compaq, Epson, Hewlett-Packard, NEC, Olivetti, Tandy, Wyse Technology, và Zenith. EISA đưa ra đường dữ liệu 32 bit và duy trì sự tương thích với ISA,

Bảng 2.6

**Sơ đồ chân của SLOT**

SLOT Chuẩn SLOT Mở rộng

| B | No | A | | B | No | A |
|---|---|---|---|---|---|---|
| GND | 1 | -I/O CH CK | | -MEM CS16 | 1 | SBHE |
| RESET DRV | 2 | SDD7 | | -I/O CS 16 | 2 | LA23 |
| + 5Vdc | 3 | SDD6 | | IRQ10 | 3 | LA22 |
| IRQ2 | 4 | SDD5 | | IRQ11 | 4 | LA21 |
| -5Vdc | 5 | SDD4 | | IRQ12 | 5 | LA20 |
| DRQ2 | 6 | SDD3 | | IRQ13 | 6 | LA19 |
| -12Vdc | 7 | SDD2 | | IRQ14 | 7 | LA18 |
| OWS | 8 | SDD1 | | -DACK0 | 8 | LA17 |
| +12Vdc | 9 | SDD0 | | DRQ0 | 9 | -MEMR |
| GND | 10 | -I/O CH RDY | | -DACK5 | 10 | -MEMW |
| SMEMW | 11 | AEN | | DRQ5 | 11 | SD08 |
| SMEMR | 12 | SA19 | | -DACK6 | 12 | SD09 |
| -IOW | 13 | SA18 | | DRQ6 | 13 | SD10 |
| -IOR | 14 | SA17 | | -DACK7 | 14 | SD11 |
| -DACK3 | 15 | SA16 | | DRQ7 | 15 | SD12 |

| | | | | | | |
|---|---|---|---|---|---|---|
| DRQ3 | 16 | SA15 | | +5Vdc | 16 | SD13 |
| -DACK1 | 17 | SA14 | | -MASTER | 17 | SD14 |
| DRQ1 | 18 | SA13 | | GND | 18 | SD15 |
| -REFRESH | 19 | SA12 | | | | |
| CLK | 20 | SA11 | | | | |
| IRQ7 | 21 | SA10 | | | | |
| IRQ6 | 22 | SA9 | | | | |
| IRQ5 | 23 | SA8 | | | | |
| IRQ4 | 24 | SA7 | | | | |
| IRQ3 | 25 | SA6 | | | | |
| -DACK2 | 26 | SA5 | | | | |
| T/C | 27 | SA4 | | | | |
| BALE | 28 | SA3 | | | | |
| +5Vdc | 29 | SA2 | | | | |
| OSC | 30 | SA1 | | | | |
| GND | 31 | SA0 | | | | |

**Cấu trúc kênh nhỏ (Micro Channel):** IBM giới thiệu chuẩn này vào năm 1988 vào thời gian đó nó được tách ra từ chuẩn PS/2. Cấu trúc Micro Channel không tương thích về điện và vật lý với kênh ISA. Không giống như kênh ISA, chức năng Micro Channel vừa kênh 16 bit vừa kênh 32 bit và có thể là không phụ thuộc vào nhiều kênh chính của bộ vi lý chính.

**Chuẩn PCI:** Đó là kênh cục bộ 32 bit sử dụng trong đa số máy tính Pentium và trong máy Apple Power Macintosh. Hiện thời cấu trúc kênh PCI phù hợp hầu hết đòi hỏi của chi tiết cấu trúc một máy tính cá nhân.

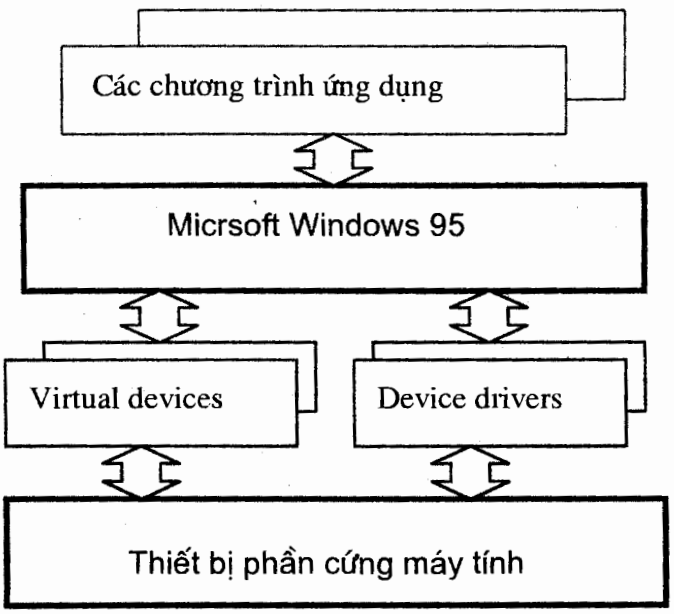
Theo phương pháp này ta sẽ thiết kế một CARD phần cứng cấm trên SLOT của máy tính để tạo các giao diện điều khiển và truyền tin khác nhau tuỳ theo mục đích sử dụng ví dụ như CARD mạng, CARD màn hình... SLOT máy tính đã chuẩn bị đầy đủ 3 BUS thông tin chính của máy tính như BUS số liệu( 16 đường D) - D15), BUS Địa chỉ 24 đường ( A0- A23 ), BUS điều khiển bao gồm các tín hiệu điều khiển dọc ghi, trạng thái và các tín hiệu ngắt,truy nhập trực tiếp bộ nhớ DMA. Thông thường việc điều khiển thiết bị phần cứng phải đảm bảo yếu tố thời gian thực vì vậy việc trao đổi số liệu giữa máy tính và thiết bị ngoại vi thường sử dụng các ngắt cứng và phương pháp truy nhập bộ nhớ trực tiếp DMA . Trên SLOT PC đã chuẩn bị sẵn 14 đường tín hiệu ngắt IRQ (IRQ2 - IRQ14).Khi có tín hiệu ngắt Bộ xử lý trung tâm sẽ dừng việc sử lý tuần tự theo chương trình đã định sẵn để thực hiện chương trình phục vụ ngắt cho chính IRQ đó. Chương trình sử lý ngắt sẽ được lập trình trước để phục vụ ngay cho các tình huống trao đổi thông tin giữa máy tính và ngoại vi. Các tín hiệu IRQ được sắp xếp sử lý ưu

tiên theo thứ tự nhỏ dần , IRQ0 có thứ tự ưu tiên cao nhất. Phần mềm điều khiển chuyên dụng cho CARD phần cứng thường do các nhà sản xuất CARD cung cấp dưới dạng các trình điều khiển thiết bị (Device drivers), chúng thường được viết trên ngôn ngữ máy hoặc ngôn ngữ trợ giúp bậc thấp (ASSEMBLE) để tăng tốc độ sử lý.

### 2.3.3 Nguyên tắc điều khiển thiết bị phần cứng trên Windows

Điều khiển thiết bị phần cứng trong Hệ điều hành (HĐH) đơn nhiệm như DOS là một việc tương đối đơn giản, chúng ta có thể can thiệp trực tiếp các thiết bị phần cứng thông qua các ngắt, các cổng vào ra để điều khiển chúng mà không ảnh hưởng đến toàn bộ hệ thống. Nhưng trong HĐH đa nhiệm như Windows 95, việc điều khiển các thiết bị phần cứng phức tạp hơn nhiều do việc phải đáp ứng hoạt động của nhiều ứng dụng cùng một lúc. Môi trường điều hành của Windows 95 bao gồm các thiết bị phần cứng của máy tính và các thành phần phần mềm sau: (Hình 2.13)

- Trình quản lý máy ảo (VMM32.VXD)
- Các thiết bị ảo (các file .VxD)
- Các chương trình điều khiển thiết bị 16- và 32-bit trong chế độ bảo vệ cho các thiết bị ngoại vi.
- Các thư viện liên kết động 16- và 32-bit (như USER.EXE và USER32.DLL).
- Các ứng dụng của Windows và các ứng dụng khác.




**Hình 2.13 Mô hình điều khiển phần cứng của Windows**

Bộ quản lý máy ảo VMM là lõi của HĐH, nó cung cấp các hàm dịch vụ (thường gọi là dịch vụ) cho phép tạo, và quản lý các máy ảo (ứng dụng luôn được thực thi trên một máy ảo). Các thiết bị ảo hỗ trợ các thiết bị độc lập với VMM bằng cách quản lý các thiết bị phần cứng của máy tính và hỗ trợ phần mềm. Các thiết bị ảo quản lý phần mềm cũng như phần cứng máy tính để đảm bảo rằng không một ứng dụng nào phá vỡ hoạt động của một ứng dụng khác. Các thư viện liên kết động của Windows cung cấp các hàm và các tài nguyên đồ hoạ mà tất cả các ứng dụng của Windows sử dụng.

**Các máy ảo (Virtual Machines)**

Một máy ảo là một phiên làm việc bao gồm một ứng dụng, hỗ trợ phần mềm (như ROM_BIOS, và MS-DOS), bộ nhớ và các thanh ghi CPU. VMM có thể tạo nhiều máy ảo. Máy ảo được tạo đầu tiên, gọi là máy ảo hệ thống, bao gồm các ứng dụng Windows 16-bit, các ứng dụng Win32 và các thread được tạo bởi các ứng dụng Win32. Các máy ảo khác được tạo cho các ứng dụng của MS-DOS khi các ứng dụng này bắt đầu được thực hiện.

Các ứng dụng MS-DOS trong một máy ảo được thực hiện trong chế độ giả lập 8086 (được gọi là chế độ V86). Trong chế độ V86, các ứng dụng chạy tương tự như khi chúng chạy trên một bộ xử lý Intel 8086 hoặc tương thích (chế độ thực - Real-mode). Điều này có nghĩa là một ứng dụng MS-DOS vẫn có thể chạy tốt trong một máy ảo mà không cần sửa đổi. Chế độ V86 cũng cho phép thực hiện các ứng dụng của chế độ bảo vệ (protected-mode) trong một máy ảo.

Mỗi một máy ảo có vùng địa chỉ, các cổng vào ra và bảng vector ngắt riêng. VMM cũng ánh xạ ROM-BIOS, MS-DOS, các chương trình điều khiển thiết bị, và các chương trình thường trú với vùng địa chỉ của máy ảo để các ứng dụng có thể truy nhập các hàm hệ thống của MS-DOS và các chương trình con của ROM-BIOS.

**Bộ quản lý máy ảo - VMM (Virtual Machine Manager)**

VMM là một hệ điều hành 32-bit chế độ bảo vệ. Nhiệm vụ chính của nó là tạo, thực hiện, giám sát và kết thúc các máy ảo. VMM cung cấp các dịch vụ để quản lý bộ nhớ, các nhiệm vụ, các ngắt và các lỗi. VMM làm việc với các thiết bị ảo, các thư viện liên kết động ở chế độ bảo vệ, cho phép các thiết bị ảo ngăn chặn các ngắt và các lỗi để điều khiển các truy nhập của một ứng dụng tới các thiết bị phần cứng và các phần mềm đã được cài đặt. Cả VMM và các thiết bị ảo chạy trong một vùng địa chỉ đơn 32-bit tại mức ưu tiên 0 (được gọi là vòng 0). Hệ thống tạo hai bảng mô tả toàn cục (GDT-Global Description Table), một bảng cho mã lệnh, một bảng cho dữ liệu, và sử dụng các bảng mô tả này trong các thanh ghi phân đoạn CS, DS, SS, và ES. Cả hai bảng mô tả đều có

địa chỉ cơ sở là 0 và một có giới hạn là 4 gigabytes, do vậy tất cả các thanh ghi đoạn trỏ tới cùng một vùng bộ nhớ. VMM và các thiết bị ảo không bao giờ thay đổi các thanh ghi này.

VMM cung cấp các thread đơn, đa nhiệm được ưu tiên. Nó thực hiện nhiều ứng dụng đồng thời bằng cách chia xẻ thời gian của CPU giữa các máy ảo mà trong các máy ảo đó các ứng dụng được thực hiện.

Khi bắt đầu hoạt động, VMM tạo và khởi tạo máy ảo hệ thống. Đầu tiên, chương trình WIN.COM nạp file VMM32.VXD, file này chứa VMM và các thiết bị ảo ngầm định. VMM được nạp vào vùng bộ nhớ mở rộng (được cấp phát bằng một trình điều khiển XMS), nó tự khởi tạo chính nó và các thiết bị ảo, sau đó chuyển sang thực hiện trong chế độ bảo vệ. Khi khởi tạo, các thiết bị ảo cài đặt các thủ tục callback cho các ngắt và xử lý các lỗi, cấp phát bộ nhớ cho các tài nguyên cần thiết của máy ảo hệ thống. Thiết bị ảo hỗ trợ giao diện (Shell), thường là thiết bị ảo được khởi tạo cuối cùng, bắt đầu Windows trong máy ảo hệ thống bằng cách nạp hạt nhân của Windows, KRNL386.EXE. Hạt nhân của HĐH nạp tất cả các phần cần thiết khác của Windows.

**Các thiết bị ảo**

Một thiết bị ảo là một chương trình 32-bit quản lý một tài nguyên hệ thống, chẳng hạn như một thiết bị phần cứng hoặc phần mềm đã được cài đặt, cho phép nhiều ứng dụng sử dụng tài nguyên đó tại cùng một thời điểm. Windows sử dụng các thiết bị ảo để cho phép xử lý đa nhiệm các ứng dụng của Windows. Các thiết bị ảo làm việc kết hợp với Windows để xử lý các ngắt, và thực hiện các thao tác vào ra cho một ứng dụng cụ thể mà không phá vỡ sự hoạt động của các ứng dụng khác.

Các thiết bị ảo hỗ trợ tất cả các thiết bị phần cứng của một máy tính, bao gồm bộ điều khiển ngắt lập trình được (PIC); đồng hồ thời gian thực; truy nhập trực tiếp bộ nhớ (DMA); bộ điều khiển đĩa; các cổng nối tiếp, song song; bàn phím và bộ hiển thị.

Rất nhiều thiết bị phần cứng sử dụng các ngắt để báo hiệu khi dữ liệu đã sẵn sàng hoặc thiết bị đã sẵn sàng hoạt động. Các thiết bị ảo hiếm khi trực tiếp chặn các ngắt cứng này. Thay vào đó, một thiết bị ảo dựa vào thiết bị ảo điều khiển ngắt lập trình được (VPICD) để xử lý các ngắt cứng. Thiết bị ảo này cài đặt thủ tục callback, thủ tục này sẽ được gọi bởi VPICD khi một ngắt cứng xảy ra. Thủ tục callback thường phục vụ ngắt của thiết bị hoặc yêu cầu VPICD phản hồi ngắt đó tới ROM BIOS hoặc mã lệnh khác phục vụ thiết bị. Một thiết bị ảo cũng có thể đăng ký các thủ tục callback để quản lý các pha khác của quá trình xử lý ngắt ví dụ như thực hiện lệnh iret. Các thiết bị ảo không được sửa đổi các mô tả trong bảng mô tả ngắt (IDT-Interupt Description Table).

Hầu hết các thiết bị phần cứng cung cấp bản đồ bộ nhớ hoặc các thanh ghi vào ra để thông qua đó các ứng dụng có thể đặt chế độ làm việc cho thiết bị và đọc hoặc ghi

dữ liệu. Các thiết bị ảo thường lưu lại các truy nhập tới các thanh ghi này để lưu giữ sự thay đổi trạng thái của thiết bị và để tái tạo lại việc đọc hoặc ghi dữ liệu. Nếu một thiết bị phần cứng sử dụng các bộ nhớ đệm, ví dụ như bộ nhớ video cho bộ hiển thị, thì thiết bị ảo của thiết bị phần cứng đó thường chiếm quyền sở hữu một vùng bộ nhớ vật lý để ngăn không cho hệ thống sử dụng vùng bộ nhớ đó nữa. Thiết bị ảo đó cũng sẽ ánh xạ bộ nhớ để ngăn không cho các ứng dụng đang chạy trong chế độ nền sau ghi đè lên các nội dung hiện thời.

Nhiều thiết bị phần cứng có ROM BIOS hoặc các chương trình con tương ứng (thường được gọi là API) để thiết lập và ghi lại trạng thái của thiết bị. Trong hầu hết các trường hợp, các ứng dụng gọi các chương trình con này bằng cách sử dụng một ngắt mềm. Các thiết bị ảo thường cài đặt các thủ tục callback để chặn các ngắt mềm này. Điều này cho phép thiết bị ảo hoặc tái tạo lại hành động được yêu cầu hoặc chuẩn bị các tham số của lời gọi cho việc thực hiện trong chế độ V86. Các tham số được chuẩn bị (được gọi là bản dịch hoặc bản đồ API) được yêu cầu khi một ứng dụng trong chế độ bảo vệ gửi một địa chỉ tới ROM BIOS hoặc một trình điều khiển thiết bị chạy trong chế độ V86.

**Ngắt và xử lý lỗi**

VMM quản lý tất cả các ngắt và xử lý lỗi cho các thiết bị ảo. Thủ tục xử lý lỗi của VMM nhận được điều khiển bất cứ khi nào một ngắt hoặc lỗi xảy ra, ví dụ khi một ứng dụng thực hiện một ngắt mềm, có gắng truy nhập tới một cổng vào ra được bảo vệ, hoặc cố gắng truy nhập tới một phân đoạn, một trang bộ nhớ không có sẵn hay được bảo vệ. Thủ tục xử lý lỗi của VMM gọi các thủ tục callback đã được cài đặt trước bởi các thiết bị ảo, cho phép các thủ tục này xử lý ngắt hoặc lỗi.

**Xử lý đa nhiệm**

VMM sử dụng một lược đồ lát cắt thời gian và quyền ưu tiên thực hiện để thực hiện các nhiệm vụ đa nhiệm theo thứ tự ưu tiên cho các máy ảo. VMM cấp phát các lát cắt thời gian cho các máy ảo có quyền ưu tiên cao nhất. Các máy ảo có quyền ưu tiên thấp hơn không nhận được các lát cắt thời gian. VMM gán quyền ưu tiên thực hiện cho một máy ảo khi nó tạo máy ảo đó. VMM và các thiết bị ảo có thể thường xuyên tăng hoặc giảm thứ tự ưu tiên thực hiện để chuyển đổi sự thực hiện giữa các máy ảo. VMM thường tăng quyền ưu tiên thực hiện cho một máy ảo cần phục vụ một sự kiện của thiết bị có mức ưu tiên cao, ví dụ như một ngắt cần phải được phục vụ tức thời.

**Các trình điều khiển thiết bị (Device drivers)**

Một trình điều khiển thiết bị trong Windows là một thư viện liên kết động (Dynamic-Link Librarie - DLL) được Windows sử dụng để tương tác với một thiết bị phần cứng, chẳng hạn như bàn phím hoặc màn hình. Thay vì truy nhập trực tiếp tới một

thiết bị phần cứng, Windows nạp trình điều khiển cho thiết bị đó và gọi các hàm trong trình điều khiển thiết bị để thực hiện các tác động trên thiết bị đó. Mỗi trình điều khiển thiết bị cung cấp một tập hợp các hàm chức năng; Windows gọi các hàm chức năng này để hoàn thành một hành động đối với thiết bị đó, chẳng hạn như vẽ một vòng tròn hoặc dịch mã quét của một phím được bấm. Các hàm chức năng của một trình điều khiển thiết bị cũng bao gồm các mã lệnh đặc trưng cần thiết của thiết bị để thực hiện các hành động trên thiết bị đó.

Windows yêu cầu các trình điều khiển thiết bị cho hiển thị màn hình, bàn phím, và các cổng truyền thông thông thường (như cổng nối tiếp và cổng song song). Các trình điều khiển thiết bị khác cũng có thể được yêu cầu nếu người dùng bổ sung thêm các thiết bị mới vào hệ thống.

**Các thông báo hệ thống (System Message)**

Windows 95 quản lý và điều khiển các ứng dụng thông qua một tập hợp các "thông báo hệ thống". Các thông báo hệ thống cung cấp cách thức để báo cho tất cả các ứng dụng cũng như các thành phần khác của hệ thống những thay đổi có thể ảnh hưởng đến hoạt động và sự truy nhập tới các tài nguyên hệ thống của chúng.

Các ứng dụng và các thành phần khác của hệ thống cũng có thể định nghĩa các thông báo của riêng chúng và sử dụng các thông báo đó để phục vụ cho việc thông báo về các kiểu sự kiện khác nhau.

### 2.3.4 Card mạng (NIC) và cách nối ghép

Vai trò của Cạc mạng (NIC) là:

- Chuẩn bị dữ liệu từ máy tính đưa vào cáp mạng.
- Gửi dữ liệu cho máy tính khách.
- Điều khiển luồng dữ liệu giữa máy tính và hệ thống cáp.
- Thu nhận dữ liệu đến từ cáp và biên dịch lại nó thành ra các byte mà bộ xử lý trung tâm của máy tính có thể hiểu được.

Các cạc mạng chứa đựng phần cứng và chương trình *firmware* (phần mềm cất giữ tệp lệnh thi hành nằm trong phần bộ nhớ chỉ đọc, ROM) thực hiện điều khiển liên kết Logic và hàm điều khiển truy cập truyền thông trong tầng liên kết dữ liệu của mô hình OSI (3 em phần .2.4)

**Chuẩn bị dữ liệu:** Trước khi dữ liệu có thể gửi lên trên mạng, cạc mạng cần phải thay đổi nó từ khuôn dạng máy tính có thể hiểu được thành khuôn dạng có thể truyền lên trên cáp mạng. Thí dụ như sử dụng trong máy tính cá nhân IBM nguyên bản, được biết là bus dữ liệu 8 bit bởi vì chúng có thể chuyển 8 bit kế tiếp nhau. Máy tính IBM PC/AT sử dụng buses 16 bit, điều đó nghĩa là nó có thể chuyển 16 bit kế tiếp nhau.

Ngày nay máy tính được chế tạo sử dụng buses 32 bit. Khi dữ liệu di chuyển trên buses máy tính, tức là nó như di chuyển song song bởi vì 32 bit di chuyển xuyên suốt bên canh nhau. ta có thể minh hoạ buses 32 bit như 32 con đường lớn với 32 chiếc ô tô di chuyển bên canh nhau (di chuyển song song), mỗi xe chở 1 bit dữ liệu.

Cạc mạng nhận dữ liệu song song từ máy tính và sắp xếp lại nó để cho nó chảy xuyên suốt theo thứ tự bit một trên đường cáp mạng.

**Địa chỉ mạng:** Trong việc bổ xung thêm dữ liệu, Cạc mạng cũng sẽ báo cho biết vị trí của nó, hoặc địa chỉ, để phân biệt nó với tất cả các cạc khác trên mạng. một chuẩn địa chỉ dã được định ra cho mỗi nhà sản xuất Cạc mạng. Nhà sản xuất kiểm soát các địa chỉ bên trong con chip trên cạc bởi quá trình hiểu là "burning" địa chỉ bên trong cạc. Với tiến trình đó, mỗi NIC có duy nhất một địa chỉ trên mạng.

Bởi vì thường thì dữ liệu di chuyển nhanh trên bus hoặc cáp hơn là cạc mạng có thể sử lý, dữ liệu được gửi đến bộ đệm của cạc, phần dành riêng của RAM. ở đây nó được giữ tạm thời trong lúc vừa truyền vừa nhận dữ liệu.

**Truyền và điều khiển dữ liệu**

Trên thực tế, trước khi Cạc Mạng gửi dữ liệu lên mạng, nó thực hiện việc trao đổi các thông tin đối thoại với NIC thu :

- Kích thước lớn nhất khối dữ liệu được gửi.
- Tổng số dữ liệu được gửi trước khi nhận tín hiệu xác nhận quay trở lại.
- Khoảng thời gian giữa các đoạn dữ liệu truyền.
- Tổng số thời gian đợi trước khi xác nhận gửi.
- Có bao nhiêu dữ liệu mà mỗi cạc có thể giữ trước khi tràn bộ nhớ.
- Tốc độ truyền dữ liệu.

Nếu một NIC hiện đại, nhanh, tinh xảo hơn muốn truyền thông với môt NIC cũ, chậm, cả hai muốn tìm kiếm tốc độ truyền chung thì có thể làm phù hợp. Một vài NICs hiện đại có mạch kết hợp cho phép cạc nhanh điều chỉnh đến tốc độ của cạc chậm.

**Lựa chọn và cài đặt cấu hình:**

Cạc ghép nối mạng thường có cấu hình lựa chọn đến mức là thiết lập thứ tự cho cạc đúng chức năng. Lựa chọn cấu hình ở ví dụ dưới đây:

- Ngắt.
- Địa chỉ cổng vào ra (I/O) cơ sở.
- Địa chỉ bộ nhớ cơ sở.
- Máy thu phát.

Đường yêu cầu ngắt là đường cứng bên ngoài thiết bị như cổng I/O, bàn phím, ổ đĩa, và NICs có thể gửi lệnh ngắt hoặc yêu cầu 1 dịch vụ đến bộ vi xử lý của máy tính.

Khi mà NIC gửi các yêu cầu đến máy tính, nó sử dụng lệnh ngắt - là tín hiệu điện gửi đến CPU của máy tính. Mỗi một thiết bị trong máy tính phải sử dụng đường yêu cầu ngắt khác nhau. Đường ngắt được định rõ khi mỗi thiết bị được cấu hình.

Trong hầu hết các trường hợp, IRQ3 và IRQ5 có thể sử dụng cho NIC, ta có thể sử dụng công cụ chuẩn đoán để xác định rõ IRQ đó hiện tại đã sử dụng.

# CHƯƠNG 3

# CÁC CHUẨN MẠNG

## 3.1 Nhu cầu chuẩn hoá mạng

Như trong mục 2.3.1 đã giới thiệu tổng quan về đa chủng loại máy tính và mạng máy tính và các hệ điều hành máy tính hiện nay trên thế giới. Với các kiến trúc mạng được phát triển bởi các nhà sản xuất đơn lẻ thì chúng thường được thiết kế cho các sản phẩm của riêng họ, không nhằm mục dích liên kết với các nhà sản xuất khác (Ví dụ mạng của IBM thời gian đầu nhưng năm 1970). Tình trạng này dẫn tới mỗi mạng máy tính chỉ có thể đi theo một dòng sản phẩm của riêng nhà sản xuất nào đó bao gồm cả phần cứng và phần mềm và mạng máy tính sẽ không thể phát triển được như ngày hôm nay.

Để có thể kết nối các mạng máy tính với nhau đòi hỏi phải mạng phải có kiến trúc mở, phân tầng và được tiêu chuẩn hoá nhằm liên kết các sản phẩm và các hệ thống khác nhau. Hoạt động của Mạng là điều hành quá trình gửi dữ liệu từ máy tính này sang máy tính khác. Quá trình phức tạp này có thể được phân đoạn thành những nhiệm vụ riêng biệt theo chuỗi liên tục. Máy tính gửi phải :

- Nhận dạng được dữ liệu.
- Chia cắt dữ liệu thành những khúc nhỏ để dễ quản lý.
- Thêm thông tin điều khiển vào mỗi khúc dữ liệu để xác định vị trí của dữ liệu và để xác định địa chỉ của cái máy thu.
- Thêm thông tin thời gian và thông tin kiểm tra lỗi.
- Đặt dữ liệu lên mạng và gửi nó tới đích.

Các phần mềm mạng hoạt động trong rất nhiều các cấp độ khác nhau tại máy tính gửi và máy tính nhận. Tại mỗi cấp độ (mức) hoặc mỗi tác nghiệp được điều khiển bởi một hoặc nhiều giao thức, những giao thức này là những đặc tả tiêu chuẩn cho sự định dạng và di chuyển dữ liệu. Khi các máy tính gửi và máy tính nhận được tuân theo cùng một giao thức, thì sự truyền thông sẽ được đảm bảo. Với sự tăng trưởng nhanh của phần cứng và phần mềm kết nối mạng thúc đẩy nhu cầu cấp bách là tạo ra các giao thức chuẩn cho phép phần cứng và phần mềm của những nhà cung cấp khác nhau liên lạc được với nhau. Trong chương này chúng ta sẽ xem xét hai chuẩn phổ cập hiện nay là mô hình liên kết mở OSI (Open System Inteconnection) và chuẩn IEEE 802.

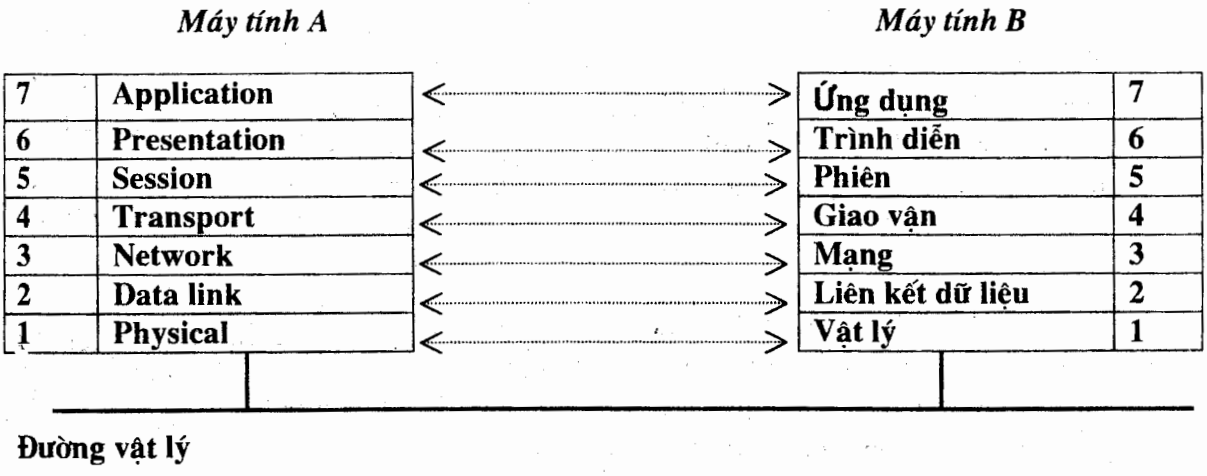
## 3.2 Mô hình tham chiếu OSI

Năm 1977 tổ chức ISO (International Organization for Standardization- Tổ chức quốc tế về tiêu chuẩn hoá) và năm 1978 tổ chức CCITT (International Telegraph and telephone Consultative Committee- Hội đồng tư vấn về điện thoại và điện tín quốc tế) khởi đầu quá trình nghiên cứu về mô hình liên kết mở OSI (Open System Inteconnection) để sử dụng làm chuẩn cho mạng máy tính. Vào năm 1984, ISO và CCITT hợp tác khuyến nghị một chuẩn chung cho mạng máy tính căn cứ trên sự nhất trí của quốc tế - Đó là mô hình tham chiếu OSI.

Mô hình OSI là mô hình tốt nhất được biết tới và thường được sử dụng rộng rãi để tham khảo trực quan về môi trường kết nối mạng. Các nhà sản xuất thường dựa vào mô hình tham chiếu OSI khi thiết kế những sản phẩm mạng. OSI mô tả cách thức: Làm sao phần cứng và phần mềm mạng làm việc được cùng nhau bên trong các lớp để tạo ra các phiên truyền thông. Mô hình cũng giúp đỡ để dò các lỗi mạng.

### 3.2.1 Khái niệm về mô hình OSI 7 lớp

Mô hình OSI chia các giao thức truyền thông thành bẩy tầng. Mỗi tầng giải quyết một phần hẹp của tiến trình truyền thông. Hình 3.1 minh họa các tầng của mô hình OSI.




**Hình 3.1. Mô hình OSI 7 tầng**

**Chức năng của từng mức:**

- Tầng một (Vật lý): Cung cấp các phương tiện truyền tin, thủ tục khởi động, duy trì và huỷ bỏ các liên kết vật lý cho phép truyền các dòng dữ liệu ở dạng bit.
- Tầng hai (Liên kết dữ liệu): Cung cấp phương tiện để truyền thông tin qua liên kết vật lý đảm bảo tin cậy, gửi các khối dữ liệu (frame) với các cơ chế đồng bộ, kiểm soát lỗi và kiểm soát luồng dữ liệu.
- Tầng ba (Mạng): Chọn đường truyền tin trong mạng, thực hiện kiểm soát luồng dữ liệu, khắc phục sai sót và cắt/ hợp dữ liệu.
- Tầng bốn (Giao vận): Thực hiện việc truyền dữ liệu giữa hai đầu mút (end to end), thực hiện việc kiểm soát lỗi và kiểm soát luồng dữ liệu, thực hiện ghép kênh và cắt / hợp dữ liệu.
- Tầng năm (Phiên): Cung cấp phương tiện quản lý truyền thông giữa các ứng dụng; thiết lập, duy trì, đồng bộ hoá và huỷ bỏ các phiên truyền thông giữa các ứng dụng
- Tầng sáu (Trình diễn): Chuyển đổi cú pháp dữ liệu để đáp ứng yêu cầu truyền dữ liệu của các ứng dụng qua môi trường OSI, mã hoá và nén dữ liệu.
- Tầng bảy ( ứng dụng): Là giao diện để người sử dụng có thể truy nhập được vào môi trường OSI, đồng thời cung cấp các dịch vụ thông tin phân tán.

### 3.2.2 Phương thức trao đổi thông tin trong mô hình OSI

Trong kiến trúc phân tầng như ở mô hình OSI ở mỗi tầng có hai quan hệ : theo chiều ngang và theo chiều dọc. Các qui tắc, qui ước để hội thoại với nhau giữa các lớp đồng mức theo quan hệ theo chiều ngang (quan hệ đồng mức qua đường truyền thông ảo) được định nghĩa là **giao thức** (Protocol). Quan hệ theo chiều dọc là quan hệ giữa các tầng kề nhau trong cùng một máy và ta gọi lớp giữa hai tầng kề nhau trong mô hình OSI là **giao diện.**

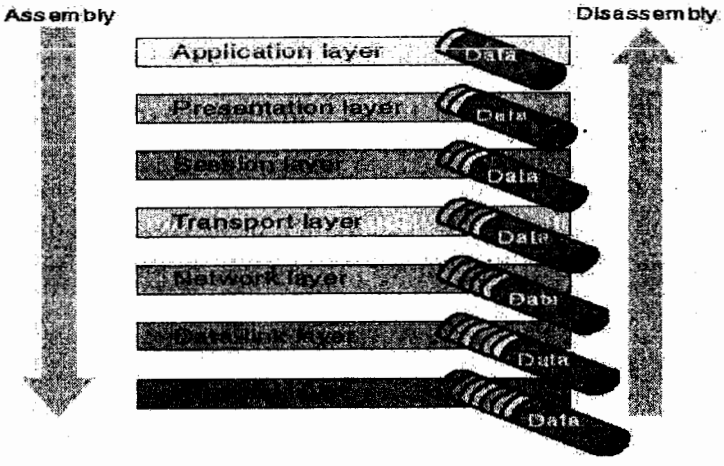
Mô hình OSI tách tiến trình truyền thông thành các tầng. Mỗi tầng chọn lựa các giao thức khác nhau để giải quyết các nhu cầu của một môi trường truyền thông cụ thể. Các giao thức này được "xếp ngăn" chồng lên nhau cho đến khe hoàn tất khả năng truyền thông. Như vậy, ngăn xếp giao thức là một loạt các giao thức xếp tầng, tương thích, được thực thi trên một máy tính cụ thể. Ngăn xếp giao thức là một loạt các giao thức phân cấp kết hợp để thực hiện một tiến trình truyền thông hoàn chỉnh. Mỗi tầng vận dụng các dịch vụ do tầng bên dưới nó cung cấp, đồng thời cung cấp các dịch vụ cho tầng bên trên nó. Về hình thức, tầng n phục vụ tầng N + 1, và tầng N -1 phục vụ tầng N.

Hình 3.2 mô tả quá trình phát sinh đường truyền của một thông điệp bắt đầu tại tầng ứng dụng. Thông điệp di chuyển dọc xuống ngăn xếp giao thức, thông qua vật tải mạng, và di chuyển dọc lên ngăn xếp giao thức của máy tính nhận. Nếu tầng chuyển tải trong máy tính nhận hiểu được các giao thức dùng trong tầng chuyển tải đã phát sinh thông điệp, thì thông điệp đó có thể bàn giao.

Nếu ngăn xếp giao thức trên hai máy tính tương thích, các kiểu máy tính khác nhau có thể truyền thông. Ví dụ, TCP/IP sẵn dùng cho hầu hết các máy tính và các hệ điều hành hiện hành. Nếu cả hai trạm làm việc Macintosh và Unix đều chạy TCP/IP, máy Mac có thể truy cập các tập tin trên trạm làm việc Unix.

**Cách truyền thông của các tầng đồng mức**

Để truyền thông với các tầng cùng mức [peer layer] trong một máy tính khác, mỗi tầng giao thức bổ sung thông tin riêng của mình vào gói tin đang gửi. Thông tin này xuất hiện dưới dạng một phần đầu (Header), được bổ sung vào đầu các gói tin ( xem Hình 3.2). Các phần đầu được bổ sung khi đang chuẩn bị thông điệp (gói tin) để truyền (assembly), và chúng được bên nhận gỡ bỏ (disassembly) sau khi đã sử dụng thông tin trong phần đầu. dữ liệu của mỗi tầng bao gồm phần đầu và dữ liệu của tầng cao hơn kế cận. Do mỗi tầng có một dạng thức dữ liệu khác nhau, nên các thuật ngữ khác nhau thường được dùng để đặt tên cho dữ liệu tại mỗi tầng. Bảng 3.1 tóm tắt các thuật ngữ này theo tầng.




**Hình 3.2. Đường di chuyển của một gói tin**

Có hai phương thức để truyền dữ liệu trong mô hình OSI là có kết nối và không kết nối.

***Truyền dữ liệu kết nối***: một kênh liên lạc logic được thiết lập và được thảo thuận trước khi truyền dữ liệu về tốc độ truyền, kiểu đấu nối terminal,... Khi truyền dữ liệu hoàn thành việc đấu nối kết thúc. Trong kiểu truyền dữ liệu này có các tính chất sau:

- Cần thiết lập một kênh logic (Yêu cầu kết nối, truyền dữ liệu và huỷ bỏ kết nối).
- Dữ liệu được truyền với một độ tin cậy cao.
- Kiểm soát trình tự truyền bằng việc bảo đảm trình tự truyền dữ liệu.
- Kiểm soát luồng bằng việc kiểm soát sự tắc nghẽn trên mạng.

Bảng3.1

**Tên gói dữ liệu tại các tầng trong mô hình OSI**

| ***Tầng*** | ***Tên gói dữ liệu*** |
|---|---|
| ứng dụng | Thông điệp (và gói tin ) |
| Trình diễn | Gói tin |
| Phiên | Gói tin |
| Giao vận | Gam Dữ liệu, phân đoạn (và gói tin ) |
| Mạng | Gam Dữ liệu (và gói tin ) |
| Liên kết dữ liệu | Khung ( và gói tin) |
| Vật lý | Bit ( và gói tin) |

***Truyền dữ liệu không kết nối***: một bên truyền dữ liệu một cách độc lập mà không cần thiết phải thiết lập một kênh liên kết. Trong kiểu truyền này có các tính chất sau:

- Không cần thiết lập kênh logic.
- Cần có thêm thông tin về việc truyền vào dữ liệu truyền.
- Dữ liệu được truyền có độ tin cậy thấp. (Không có báo lại khi có lỗi truyền).

Truyền dữ liệu có kết nối phù hợp cho việc truyền dữ liệu trong thời gian dài, liên tục nhận và truyền một khối lượng lớn dữ liệu. Truyền dữ liệu không kết nối phù hợp cho các liên lạc rải rác và độc lập.

### 3.2.3 Tầng vật lý

Tầng vật lý là tầng thấp nhất trong mô hình tham chiếu OSI và làm việc thông qua các mạch truyền dẫn bao gồm các phương tiện vật lý (Chi tiết xem phần 2.1) như cáp đồng trục, cáp sợi quang,v.v.. để đảm bảo việc truyền các đơn vị bít từ tầng liên kết dữ liệu chuyển xuống. Trong tầng vất lý các thuộc tính điện liên quan đến sự biểu diễn các bít (các mức thế hiệu) và tốc độ truyền các bít, thuộc tính cơ liên quan đến các tính chất vật lý của giao diện với một đường truyền. Ngoài ra còn các thuộc tính chức năng chỉ ra các chức năng được thực hiện bởi các phần tử của giao diện vật lý, giữa một hệ

thống và đường truyền. Thuộc tính thủ tục liên quan đến giao thức điều khiển việc truyền các xâu bit qua đường truyền vật lý.

Tầng vật lý thực hiện các hoạt động vật lý mà các thực thể dữ liệu đòi hỏi để truyền và nhận dữ liệu giữa các thực thể liên kết dữ liệu kế tiếp trong một hệ thống mở. Các hoạt động mà tầng vật lý thực hiện cho các thực thể liên kết dữ liệu để cung cấp dịch vụ vật lý như:

- Kích hoạt (thiết lập) các kết nối vật lý nghĩa là làm cho việc truyền dữ liệu giữa các thực thể sử dụng dịch vụ vật lý được thực hiện.
- Truyền dữ liệu giữa những thực thể sử dụng dịch vụ vật lý qua kết nối vật lý đã được kích hoạt.
- Xoá các kết nối vật lý khi các thực thể không sử dụng

*Các tham số chủ yếu khi thiết kế mức vật lý*:

- Độ dài đường truyền
- Loại cáp sử dụng
- Tốc độ thông tin yêu cầu
- Số nối vào mạng và Tôpô của mạng
- Kênh thông tin cần dùng ( kênh cơ sở hay kênh băng rộng)

Các chuẩn cho tầng vật lý

Các chuẩn cho tầng vật lý phải bao gồm các phần tử giao thức giữa các thực thể và các đặc tả của giao diện với đường truyền. Trong các chuẩn này hai thiết bị thường được sử dụng là *thiết bị đầu cuối dữ liệu* DTE (Data Terminal Equipment) và *thiết bị cuối kênh dữ liệu* DCE (Data Circuit-Terminating Equipment).

DTE dùng để chỉ các máy tính hoặc terminal của người sử dụng cuối. Trong DTE có các ứng dụng (chương trình, dữ liệu) của người sử dụng. Mạng máy tính sẽ cho phép nối các DTE và phân chia tài nguyên giữa các DTE với nhau cũng như trao đổi dữ liệu và lưu trữ những thông tin dùng chung.

DCE dùng để nối các DTE với các đường truyền thông. DCE có thể là Modem, transducer, Multiplexer,...máy tính (nút mạng). DCE có thể cài đặt trong DTE hoặc để ngoài, nhiệm vụ của nó như nhau, đều dùng để biểu diễn dữ liệu của người sử dụng thành dạng tín hiệu chấp nhận được theo đường truyền hoặc từ đường truyền vào DTE.

***Một số khuyến nghị chuẩn thường dùng:***

Có ba kiểu tiêu chuẩn được CCITT khuyến nghị sử dụng:

- Chuẩn loại V- Chuẩn cho giao diện giữa DTE và DCE sử dụng đường tương tự (Analog).
- Chuẩn loại X- Chuẩn cho giao diện giữa DTE và DCE sử dụng đường số (Digital).

- Chuẩn loại I- Chuẩn cho giao diện đường đa dịch vụ ISDN.

Ví dụ: Khuyến nghị chuẩn V24/RS-232-c: Dùng để định nghĩa giao diện tầng vật lý giữa DTE và DCE, đây là hai chuẩn của CCITT và EIA. Các chuẩn này qui định dùng đầu nối 25 chân (25-pin connector) do vậy cần dùng cáp 25 sợi để nối DTE và DCE. Chuẩn này qui định mức điện áp nhỏ hơn -3V và lớn hơn +3V tương ứng với các tín hiệu số nhị phân 0 và 1. Tốc độ tín hiệu qua giao diện không vượt quá 20 Kb/s và với khoảng dưới 15 m. Chuẩn này nếu sử dùng truyền theo phương thức đồng bộ cần phải có tín hiệu đồng hồ để đồng bộ hoá các bít. Nếu một Modem đồng bộ được dùng thì cả hai chức năng điều chế và giải điều chế đều đòi hỏi một tín hiệu đồng hồ để thực hiện mã và giải mã tín hiệu. Vì vậy Modem cần cung cấp đồng hồ "gửi" và "nhận" cho các mạch điều khiển giao diện trong các DTE. Trường hợp dùng Modem không đồng bộ sẽ không cần đồng hồ trong Modem. Trường hợp khoảng cách giữa các thiết bị quá gần, cho phép hai DTE có thể truyền tín hiệu trực tiếp cho nhau. Khi đó các mạch RS-232-C vẫn có thể được dùng như không cần có mặt DCE nữa. Từ năm 1987, RS-232-C được đổi tên là EIA-232-D. Nhược điểm chính của chuẩn này là sự hạn chế về tốc độ và khoảng cách.

Khuyến nghị chuẩn RS-449/422-A/423-A: RS-449 định nghĩa các đặc trưng cơ, chức năng và thủ tục. RS-449 tương tự RS-232-C và có thể liên tác với chuẩn cũ, nó giữ nguyên các mạch cũ của RS-232-C và thêm vào 10 mạch mới. Tương tự như RS-232C các mạch trong RS-449 thực hiện việc truyền tin dựa trên các cặp "tác động-phản ứng" như DTE thực hiện Request to Send, sau đó đợi DCE trả lời Clear to Send. RS-449 dùng đầu nối 37 chân cho giao diện cơ bản và dùng đầu nối 9 chân riêng biệt nếu có kênh phụ. Thực tế có nhiều trường hợp chỉ có một số ít chân được dùng. RS-422-A và RS-433-A định nghĩa các đặc trưng điện mới của chuẩn RS-449. RS-449-A sử dụng phương thức truyền không cân bằng và có thể đạt tốc độ cao hơn 100 Kb/s ở 1200 m và tới 10 Mb/s ở 12 m.

Khuyến nghị loại X của CCITT: Có nhiều hệ thống sử dụng các khuyến nghị loại X của CCITT cho tầng vật lý. X21 chấp nhận các chế độ truyền cân bằng và không cân bằng và có cùng giới hạn, khoảng cách như trong RS-422-A và RS-423-A. X21 thể hiện tính mềm dẻo và hiệu quả hơn so với RS-232-C và RS-449.

### 3.2.4 Tầng liên kết dữ liệu

Tầng nối kết dữ liệu nhận các gói tín dữ liệu có tên là khung [frames] từ các tầng phía trên. Chức năng chính của tầng nối kết dữ liệu là tháo rời các khung này thành các bit để truyền và rồi kiến tạo lại các khung từ các bit nhận được.

Tầng nối kết dữ liệu thực hiện các công việc sau

- Điều khiển việc truy cập vật tải mạng
- Định danh các thiết bị trên mạng
- Định nghĩa tôpô logic của mạng
- Điều khiển luồng dữ liệu
- Điều khiển và kiểm tra lỗi.

**Điều khiển truy cập vật tải**

Mọi kênh vật tải vào một thời điểm chỉ phục vụ một tín hiệu. Nếu hai máy tính truyền trên kênh cùng một lúc, các tín hiệu của chúng sẽ gây nhiễu cho nhau, cũng giống như âm nhiễu khi hai người nói cùng một lúc. Tính năng điều khiển truy cập vật tải sẽ điều khiển việc truy cập vật tải để không xảy ra sự cố gây nhiễu. Có ba dạng điều khiển truy cập vật tải (Chi tiết xem mục 4.3):

+ Tranh chấp là phương pháp điều khiển truy nhập chấp nhận xung đột khi mọi máy tính đều có khả năng truyền trên mạng.

+ Chuyển thẻ bài [token passing] là phương pháp vận dụng một khung có tên là thẻ bài [token], luân chuyển quanh mạng. Một máy tính muốn truyền phải đợi cho đến khi nhận được khung thẻ bài, vào lúc này nó mới được phép truyền. Khi máy tính truyền xong, nó chuyển khung thẻ bài cho trạm kế tiếp trên mạng

+ Dò báo là một phương pháp điều khiển truy cập sử dụng một thiết bị trung tâm để điều tiết toàn bộ việc truy cập mạng. Dò báo là phương pháp điều khiển truy cập phổ dụng nhất trên các mạng máy tính lớn.

**Định địa chỉ**

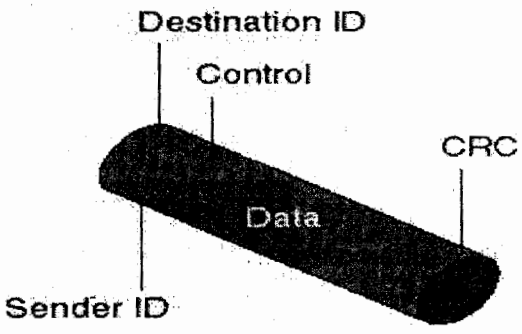
Tầng nối kết dữ liệu duy trì các địa chỉ vật lý của thiết bị mạng cho phép gửi các thông điệp đến một thiết bị cụ thể trện mạng. Các địa chỉ được dùng có tên là các địa chỉ thiết bị vật lý [physical device addresses], là những địa chỉ duy nhất kết hợp với phần cứng nối mạng trong máy tính. Trong hầu hết các trường hợp các địa chỉ thiết bị vật lý được cài cứng bởi nhà sản xuất vào cạc mạng khi chế tạo cạc.

Các chuẩn áp dụng cho một mạng cụ thể sẽ xác định dạng thức của địa chỉ. Do dạng thức địa chỉ kết hợp với phương pháp điều khiển truy cập vật tải đang dùng, nên các địa chỉ thiết bị vật lý thường được gọi là các địa chỉ MAC (Media Access Control).

Địa chỉ thiết bị thực tế không được dùng để định tuyến một thông điệp đến một thiết bị cụ thể. Các khung trên các mạng LAN thường được truyền cho tất cả các thiết bị trên mạng. Mỗi thiết bị đọc từng khung đó để xác định địa chỉ thiết bị mà khung đó sẽ đến. Nếu địa chỉ đích của khung khớp với địa chỉ vật lý riêng của thiết bị, phần còn lại của khung sẽ được chấp nhận. Nếu các địa chỉ không khớp, phần còn lại của khung sẽ được bỏ qua.

**Khung tin và đồng bộ hoá phiên truyền**

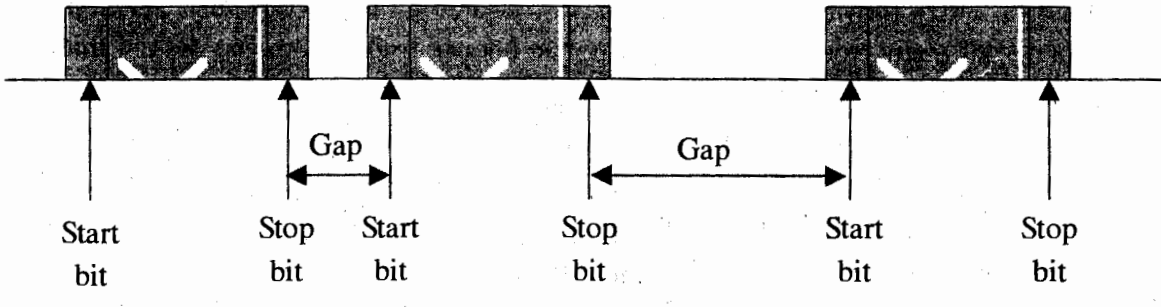
Tầng vật lý phải đồng bộ hoá các phiên truyền bit giữa các thiết bị gửi và nhận. Tuy nhiên, tầng nối kết dữ liệu tác động lên dữ liệu sau khi lắp ráp các bit thành các khung tin và nó sẽ phải đảm bảo rằng các bit này là không có lỗi, nếu kiểm tra có lỗi nó sẽ thông báo cho bên phát để giữ lại. Cấu trúc cơ bản của một khung tin (Hình 3.3) bao gồm địa chỉ MAC của thiết bị nhận(Distination ID) và địa chỉ MAC của thiết bị gửi, (Sender ID), các thông tin điều khiển gói tin (Control), Sô liệu (DATA) và thông tin kiểm tra lỗi của khung tin (CRC).




**Hình 3.3 Cấu trúc cơ bản của một khung tin**

Tại tầng liên kết dữ liệu, các phiên truyền khung phải được đồng bộ hoá. Có các cơ chế đồng bộ sau:

- Di bộ
- Đồng bộ
- Đẳng thời




**Hình 3.4: Mô hình truyền không đồng bộ**

**Truyền dị bộ**

Truyền dị bộ [asynchronous transmission] không dùng cơ chế tính giờ để đồng bộ hoá các thiết bị gửi và nhận. Thay vì thế, nó dùng cơ chế đồng bộ bit để đồng bộ hoá các thiết bị theo mỗi khung được truyền. Mỗi khung bắt đầu bằng một bit bắt đầu (START) cho phép thiết bị nhận đồng bộ với tín hiệu truyền. Các thông điệp được giữ ở mức ngắn để các thiết bị gửi và nhận không bị cuốn dạt ra khỏi cơ chế đồng bộ hoá trong thời gian của thông điệp. Truyền dị bộ thường được dùng để truyền dữ liệu ký tự và rất phù hợp với các môi trường ở đó các ký tự được truyền theo các quãng thời gian không đều, như khi người dùng nhập dữ liệu ký tự.

Hình 3.4 minh hoạ cấu trúc điển hình để truyền dữ liệu ký tự theo phương pháp dị bộ. Khung này có bốn thành phần:

- Một bit bắt đầu. Các tín hiệu mà một khung đang bắt đầu và cho phép thiết bị nhận tự đồng bộ hoá .
- Các bit dữ liệu. Bao gồm bảy hay tám bit khi dữ liệu ký tự đang được truyền
- Một bit kiểm tra chẵn lẻ. Được tuỳ chọn dùng như một phương pháp sơ bộ để phát hiện các lỗi truyền.
- Một hoặc 2 bit dừng. Phát tín hiệu cuối khung dữ liệu.

Các kỹ thuật kiểm tra chẵn lẻ có thể phát hiện các lỗi ảnh hưởng đến một bit. Tuy nhiên, chúng không thể phát hiện các lỗi ảnh hưởng đến hai hay nhiều bit.

Truyền dị bộ là một công nghệ đơn giản và rẻ tiền, thích hợp cho việc truyền các khung nhỏ theo các quãng thời gian không đều. Tuy nhiện, do phải bổ sung các bit khởi đầu, bit dừng, và bit tương đồng vào mỗi ký tự truyền, nên phần điều hành chung của truyền dị bộ ở mức cao, khoảng 20 đến 30 phần trăm. Điều này lãng phí băng thông và khiến phương pháp truyền dị bộ trở nên không phù hợp khi phải truyền các lượng dữ liệu lớn.

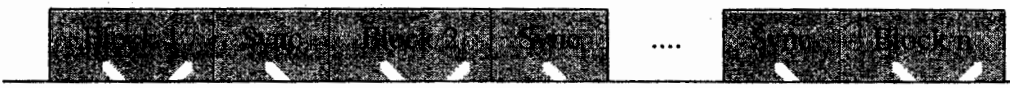
Truyền dị bộ thường được dùng trong truyền thông giữa các máy PC và trạm cuối với máy chủ . Trong các môi trường này, dữ liệu thường thuộc bản chất hướng ký tự và gián đoạn rất thích hợp với kỹ thuật truyền dị bộ. Trong cả hai trường hợp, việc áp dụng phương pháp truyền dị bộ nói chung tỏ ra thoả đáng vì giảm được giá thành mà kết quả vẫn cao.

**Truyền đồng bộ**

Việc truyền thông có thể tiến hành hiệu quả hơn bằng cách đồng bộ hoá các đồng hồ trên các thiết bị truyền và nhận. Tiến trình đồng hoá hoá này được tiến hành theo 2 cách:

- Bằng cách truyền tín hiệu đồng bộ hoá kèm với dữ liệu. Có một số kỹ thuật mã hóa dữ liệu tự tính giờ để bảo đảm việc chuyển tiếp tín hiệu với từng bit được truyền.
- Bằng cách dùng một kênh truyền thông riêng để tải các tín hiệu đồng bộ (xung nhịp), một kỹ thuật có thể vận hành với mọi kỹ thuật mã hóa tín hiệu.

Hình 3.5 minh hoạ hai cấu trúc của thông điệp kết hợp với truyền đồng bộ.



**Hình 3.5: Mô hình truyền tin đồng bộ**

Cả hai kiểu truyền đều bắt đầu bằng một chuỗi các tín hiệu đồng bộ (synch), để thông báo cho bên nhận biết đầu của một khung. Các tín hiệu synch thường vận dụng một khuôn mẫu bit không thể xuất hiện đâu đó trong thông điệp, nhằm bảo đảm chúng luôn tách biệt và bên nhận cũng dễ nhận ra.

Có thể truyền nhiều kiểu dữ liệu khác nhau. Có hai kiểu dữ liệu: hướng ký tự và hướng bit. có thể truyền nhiều ký tự hoặc các chuỗi bit dài trong chỉ một khung dữ liệu. Do bên truyền và bên nhận vẫn duy trì tình trạng đồng bộ trong phiên truyền, nên các khung có thể rất dài. Ví dụ ta xem xét một giao thức hướng Bit -HDLC (High level Data Link Control) là là giao thức bậc cao cho tầng 2 tầng liê kết dữ liệu. Giao thức phát triển theo 2 khuyến nghị ISO 3309 và ISO 4335, dựa trên cơ sở của SDLC. HDLC hỗ trợ cho việc liên kết điểm - điểm, điểm - nhiều điểm, có khả năng khai thác song công hoàn toàn (Full duplex)

Khác với giao thức hướng ký tự, giao thức HDLC quản lý dữ liệu dưới dạng các frame. Sau đây là hai cấu trúc frame cơ bản của HDLC (Hình 3.6.): Khuôn dạng chuẩn và mở rộng, giữa hai dạng này có một khác biệt nhỏ. Đối với dạng chuẩn các trường Address, Control, FSC có độ lớn 8 bit, đối với dạng mở rộng các trường tương ứng này có độ lớn gấp đôi (16 bit). Thực chất frame kiểm soát cũng là một frame nhưng trường thông tin của nó không có.

Mô tả các trường như sau:

Trường Flag: Dùng để đồng bộ và phân cách frame. Các frame bắt đầu và kết thúc bằng các flag. , hi thu trạm thu bắt buộc phải tìm các flag này. Flag còn dùng để đồng bộ các frame. Một flag có thể sử dụng vừa để kết thúc mộtt frame vừa để bắt đầu một frame tiếp theo.

Trường Address: Trường địa chỉ chứa địa chỉ trạm đích của frame (trạm thứ cấp)

Trường Control: (còn gọi là trường Command) Trường lệnh kiểm soát chứa các lệnh - commands (đối với các trạm sơ cấp) và trả lời - Resôonses (đối với trạn thứ cấp) và các số thứ tự frame (SEQuence number). Trường Control được sử dụng ở trạm sơ cấp để thông báo cho trạm thứ cấp biết thao tác (operation) nào cần được tiến hành. Trạm thứ cấp sử dụng trong trường hợp này để trả lời cho trạm sơ cấp.

| Flag | Address | Control | Datas | FCS | Flag |
|---|---|---|---|---|---|
| 01111110 | 8/16 bit | 8/16 bit | * | 16/32 bit | 01111110 |
| | Frame Header | | | | |

a- Frame đầy đủ

| Flag | Address | Control | FCS | Flag |
|---|---|---|---|---|
| 01111110 | 8/16 bit | 8/16 bit | 16/32 bit | 01111110 |
| | Frame Header | | | |

b- Frame kiểm soát

**Hình 3.6 Cấu trúc frame của HDLC**

Trường information: Trường thông tin (thường là bội số các byte), trường này là một dãy bit nhị phân bất kỳ. Tuy nhiên thông thường trường này bao gồm bội số các byte (8 bit)

Để phân biệt với các flag, trong trường này, các bit 0 được chèn vào sau 5 bit 1 liên tiếp (kể cả đối với FCS). Phía thu sẽ tự bỏ đi các bit 0 ngay sau 5 bit 1 liên tiếp.Trường FCS: (Frame Check Sequence): Trường kiểm tra.

Khi các khung trở nên dài, phương pháp kiểm tra lỗi chẵn lẻ [parity] không còn thích hợp để phát hiện các lỗi. Nếu xảy ra lỗi, nhiều bit sẽ bị ảnh hưởng, và các kỹ thuật kiểm tra chẵn lẻ ắt không thể báo cáo đúng đắn các lỗi. Kỹ thuật được dùng với cơ chế truyền đồng bộ đó là CRC (cyclic redundancy check = kiểm tra độ dôi chu kỳ- Chi tiết xem 2.2.2). Bên truyền dùng một thuật toán để tính một giá trị CRC tóm tắt toàn bộ giá trị các bit dữ liệu, và rồi giá trị này được chắp vào khung dữ liệu. Bên nhận dùng cùng thuật toán đó, tính lại CRC, và so sánh CRC trong khung với giá trị đã tính toán. Nếu các giá trị ăn khớp, khung hầu như chắc chắn không gặp lỗi.

Khuôn mẫu bit cuối [end bit pattern] tất nhiên ám chỉ cuối một khung. Giống như các bit synch, khuôn mẫu bit cuối thường là một khuôn mẫu không thể xuất hiện trong thân của khung dữ liệu, để bên nhận không nhầm lẫn.

Khi các tuyến nối kết truyền đồng bộ ở tình trạng không tải (không truyền dữ liệu), các bit chèn thêm [fill bits] thường được truyền để duy trì tính đồng bộ của các thiết bị, nhờ vậy không cần phải tái đồng bộ hoá các thiết bị khi truyền một khung mơi.

Cơ chế truyền thông đồng bộ có nhiều ưu điểm so với truyền dị bộ. Các bit điều hành chung (synch, CRC, và end) chỉ chiếm một phần nhỏ của khung dữ liệu chung, khiến việc sử dụng băng thông của phương pháp truyền đồng bộ trở nên hiệu quả hơn nhiều. Tính năng đồng bộ hoá cho phép các hệ thống vận dụng các tốc độ cao vào cải tiến kỹ thuật phát hiện lỗi.

Nhược điểm của phương pháp truyền thông đồng bộ xoay quanh chi phí cao, sở dĩ như vậy là vì phải áp dụng hệ mạch phức hợp hơn. Kết quả là, phương pháp truyền đồng bộ chủ yếu được dùng khi buộc phải truyền các lượng dữ liệu lớn.

Truyền đồng bộ thường được dùng trong môi trường truyền thông giữa các máy tính lớn, cũng như để đạt được các mức hiệu quả cao trên các LAN. Ví dụ, cả Ethernet lẫn Token Ring đều vận dụng các tín hiệu tự đồng bộ thời gian.

**Truyền Đẳng Thời**

*Truyền đẳng thời (isochronous transmission)* sử dụng một thiết bị chung cung cấp một tín hiệu tính giờ (đồng bộ thời gian) mà tất cả các thiết bị trên mạng cùng chia sẻ. Thiết bị tính giờ tạo các khe thời gian [time slots]. Các thiết bị có dữ liệu để truyền sẽ giám sát mạng và chèn dữ liệu vào các khe thời gian mở khi chúng sẵn dùng. Một khe thời gian nhất định có thể được điền bằng nhiều khung, theo dung lượng. Phương pháp truyền đẳng thời là tất định, bảo đảm các tốc độ truyền, và có phần điều hành chung ở mức thấp. Tuy nhiên, kỹ thuật này dẫn đến nguy cơ sự cố xảy ra tập trung tại một điểm.

**Các dịch vụ liên kết**

Các dịch vụ liên kết mạng cung cấp nhiều chức năng:

- Điều khiển luồng [flow control] xác định lượng dữ liệu có thể truyền trong một thời hạn nhất định. Chức năng điều khiển luồng ngăn cấm thiết bị truyền không được làm ngập bên nhận. Có thể áp dụng tính năng này tại vài cấp giao thức, kể cả tầng con LLC.
- Điều khiển lỗi [error control] phát hiện các lỗi trong các khung nhận và yêu cầu truyền lại các khung. Điều khiển lỗi là một chức năng của tầng con LLC.
- Điều khiển chuỗi [sequence control] cho phép các bên nhận tái lắp ráp các khung dữ liệu theo thứ tự ban đầu của chúng. Kích cỡ khung thường bị hạn chế, do đó cần phải phân mảnh gói tin và tái hợp để truyền các thông điệp lớn. Điều khiển chuỗi là chức năng của tầng mạng.

Có ba kiểu dịch vụ liên kết cung cấp các cách phối hợp khác nhau của các dịch vụ trên đây:

- Các dịch vụ phi liên kết không báo nhận [unacknowledged connectionless service]. Không cung cấp chức năng điều khiển luồng, điều khiển lỗi, hay điều khiển chuỗi. Khi cần, các dịch vụ này phải được cung cấp bởi các tầng

giao thức cao hơn. Các dịch vụ phi liên kết không báo nhận thường cung cấp khả năng vận hành cao khi việc truyền thông mạng được mặc nhận là đáng tin cậy ( như trên hầu hết các LAN)

➢ Các dịch vụ hướng -liên kết [connection -oriented services]. Cung cấp các chức năng điều khiển luồng, điệu khiển lỗi, và điều khiển chuỗi thông qua việc dùng các tín hiệu báo nhận. Các dịch vụ hướng - liên kết chiếm mức điều hành chung cao, làm giảm khả năng vận hành, nhưng lại cải tiến độ tin cậy ở những mức độ tin cậy của mạng có vấn đề ( Như trên hầu hết các WAN).

➢ Các dịch vụ phi liên kết có báo nhận [acknowledged connec-tionless services]. Dùng các tín hiệu báo nhận [acknowless service]. Dùng các tín hiệu báo nhận [acknowledgments] để cung cấp các chức năng điều khiển lỗi và điều khiển luồng trên các tuyến liên kết liên điểm [point-to-point connections].

**Điều khiển luồng tại tầng Con LLC**

Dịch vụ điều khiển luồng ngăn cấm các thiết bị truyền chạy nhanh làm ngập các thiết bị nhận. Hai kỹ thuật chung của cơ chế điều khiển luồng là: điều khiển luồng có tốc độ bảo đảm [guaranteed rate flow control] và điều khiển luồng cửa sổ [window flow control].

**** Điều khiển luồng có tốc độ bảo đảm***

Trong kỹ thuật điều khiển luồng có tốc độ bảo đảm, các thiết bị gửi và nhận thương lượng một tốc độ truyền mà cả hai cùng chấp nhận được. Tốc độ truyền này thường giữ ổn định trong suốt cả phiên truyền.

Để bảo đảm nhận đúng đắn các khung, một số giao thức yêu cầu bên nhận báo đã nhận từng khung khi được xử lý. Nếu không phát hiện lỗi, nó sẽ trả về cho bên truyền một khung báo nhận [acknowlegment frame], chỉ thị cho nó gửi khung kế tiếp. Nếu phát hiện các lỗi, bên nhận phải tiến hành một trong hai việc: gửi một yêu cầu truyền lại, hoặc đơn giản chờ cho đến khi bên truyền tính hết giờ và truyền lại khung.

Tóm lại, kỹ thuật điều khiển luồng có tốc độ bảo đảm mặc nhận bên nhận sử lý một đơn vị thông điệp (bit hoặc khung) cho mỗi đơn vị được truyền. Kiểu tiếp cận khá cứng nhắc này thường không vận dụng thật hiệu quả các khả năng của kênh vật tải, thiết bị truyền và thiết bị nhận.

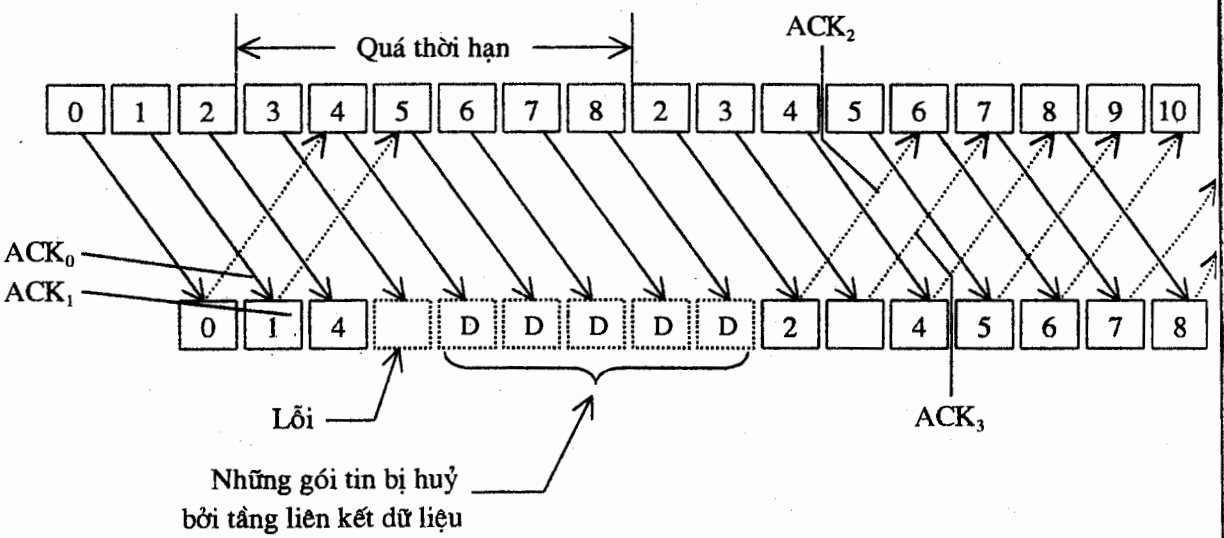
**** Điều Khiển Luồng Cửa Sổ***

Kỹ thuật *lập vùng đệm [buffering]* cho phép các bên truyền và bên nhận hoạt động linh hoạt hơn. Các vùng đệm là vùng bộ nhớ có thể nhận dữ liệu từ mạng và lưu giữ nó cho đến khi bên nhận có thể xử lý dữ liệu và phát tín hiệu báo nhận.

*Lập cửa sổ [windowing]* là một kỹ thuật cho phép bên truyền gửi vài khung giữ liệu trước khi nhận tín hiệu báo nhận của bên nhận. Có thể lập vùng đệm cho vài khung trong thiết bị nhận khi chúng được xử lý. Thuật ngữ *cửa sổ [window]* ở đây ám chỉ lượng khung mà một thiết bị truyền thông có thể gửi mà không cần nhận tín hiệu báo nhận.

- Điều khiển luồng cửa sổ tĩnh *[static window flow control]* hạn chế kích cỡ cửa sổ theo một số lượng khung cụ thể, thường được định nghĩa bởi số lượng khung có thể vừa trong vùng đệm nhập liệu của thiết bị nhận. Nếu kích cỡ cửa sổ là 7, bên truyền có thể có tới bảy khung đang chờ. Tuy nhiên, không thể truyền khung thứ tám cho đến khi một trong các khung đang chờ được báo nhận (xem hình 3.7).

Điều khiển luồng cửa sổ động *[dynamic window flow control]* cải thiện hiệu năng bằng cách cho phép các thiết bị truyền thông điều chỉnh kích cỡ cửa sổ. Kỹ thuật này còn có các thuật ngữ khác như: cửa sổ *trôi [floating]* hay cửa sổ *trượt [sliding]*. Kỹ thuật cửa sổ động cho phép bên nhận gửi đi một *khung điều tiết [chokeframe]* dưới dạng dung lượng gần sát vùng đệm nhập liệu của nó. Khung điều tiết này phát tín hiệu cho bên truyền biết để chậm lại. Sau khi bên truyền điều chỉnh tốc độ truyền chậm lại, nó lại tăng tốc độ truyền cho đến khi nhận được một khung điều tiết khác. Theo cách này, ta có thể tối ưu hoá việc sử dụng băng thông.




**Hình 3.7 Điều khiển luồng của sổ tĩnh**

**Điều Khiển Lỗi**

Hai điều kiện lỗi LLC có thể tồn tại:

- Khi phát hiện các lỗi CRC
- Khi không nhận được các tín hiệu báo nhận dự kiến (Quá thời gian đợi qui định)

Như đã nêu trên đây, các khung dữ liệu đồng bộ kết hợp chặt chẽ với một trường CRC, có thể được dùng để phát hiện các lỗi truyền. Khi một thiết bị nhận phát hiện ra một lỗi CRC, nó có thể truyền một NAK (*negative acknowledgment = tín hiệu báo phủ nhận*) yêu cầu truyền lại khung đó. Khi các dịch vụ báo nhận, bên truyền mong đợi các khung ACK (acknowledgment = tín hiệu báo nhận ) từ bên nhận cho mỗi khung ( hoặc một nhóm khung trong giao thức lập cửa sổ ). Khi quãng thời gian đã định hết hạn mà không gặp tín hiệu báo nhận, bên truyền mặc nhận khung đã bị mất và sẽ truyền lại nó.

### 3.2.5 Tầng mạng

Như đã nêu ở phần trên, tầng nối kết dữ liệu đảm trách việc truyền thông giữa các thiết bị trên cùng một mạng. Các địa chỉ thiết bị vật lý được dùng để định danh các khung dữ liệu, và mỗi thiết bị chịu trách nhiệm giám sát mạng và nhận các khung để gửi cho thiết bị đó.

Tầng mạng liên quan đến việc truyền thông với các thiết bị trên các mạng tách biệt về lôgic, được liên kết để hình thành các liên mạng [internetwork]. Do các liên mạng có thể rất lớn và có thể dược kiến tạo từ các kiểu mạng khác nhau, nên tầng mạng vận dụng các thuật toán quyết định tuyến để hướng các gói tin từ các mạng nguồn đến các mạng đích.

Thành phần chính của tầng mạng đó là mỗi mạng trong liên mạng được gán một địa chỉ mạng, có thể dùng nó để định tuyến các gói tin. Để giúp hiểu rõ bản chất của các địa chỉ này và cách dùng chúng để định tuyến các gói tin, ta sẽ xem xét các phần sau:

- Định địa chỉ
- Trạm chuyển
- Các thuật toán định tuyến
- Các dịch vụ liên kết

**1. Định địa chỉ**

Các địa chỉ mạng vật lý *(MAC)* định danh duy nhất một thiết bị cụ thể trên mạng dưới dạng một nguồn hay đích của một khung. Tầng mạng sử dụng hai kiểu địa chỉ bổ sung sau:

➢ Các địa chỉ mạng lôgic [*Logical network addresses*], để định tuyến các gói tin theo các mạng cụ thể trên liên mạng. Một trong những công việc mà chuyên viên

cài đặt mạng phải hoàn thành đó là đảm bảo mỗi địa chỉ mạng phải duy nhất trên một liên mạng nhất định.

➢ Các địa chỉ dịch vụ [*Service addresses*], định tuyến các gói tin theo các tiến trình cụ thể đang chạy trên các thiết bị đích. Các hệ điều hành trên hầu hết các máy tính có thể cùng luc chạy vài tiến trình. Khi một gói tin đến, bạn phải xác định tiến trình nào trên máy tinh sẽ nhận dữ liệu trong gói tin đó. Để thực hiện, bạn gán các địa chỉ dịch vụ, chúng sẽ định danh các giao thức và các tiến trình của tầng phía trên. Các địa chỉ dịch vụ này được gộp với các địa chỉ mạng lôgic và vật lý trong khung dữ liệu. ( Có vài giao thức gọi các địa chỉ dịch vụ là ổ cắm [ *sockets*] hoặc cổng [ *ports*]).

**2. Trạm chuyển**

Trong liên mạng ta có thể dùng các kỹ thuật sau để định tuyến các thông điệp :

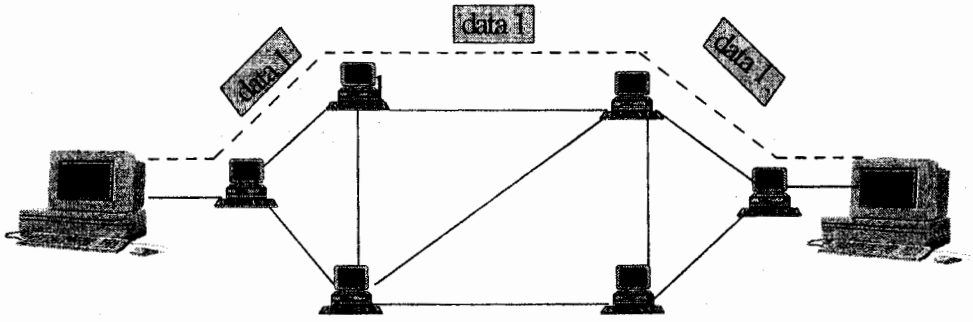
➢ Chuyển mạch

➢ Chuyển thông điệp

➢ Chuyển gói tin

***Chuyển mạch***

Kỹ thuật *chuyển mạch* [*Circuit swiching*] thiết lập một đường truyền luôn giữ cố định trong khi liên kết (xem hình 3.8 ). Kỹ thuật chuyển mạch cung cấp cho các thiết bị một đường truyền chuyên trách và một băng thông xác định

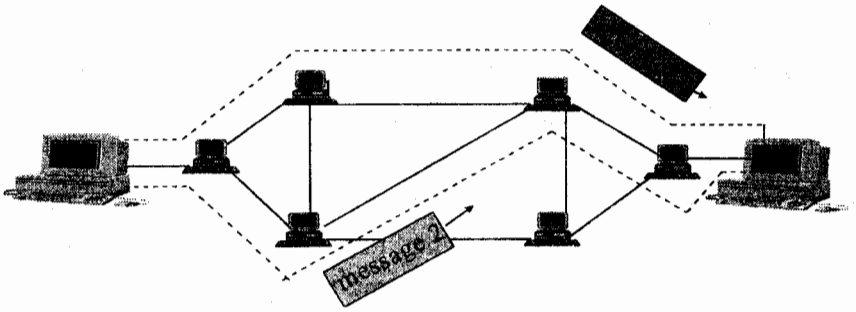



**Hình 3.8. Chuyển mạch kênh**

Phương pháp chuyển mạch kênh có hai nhược điểm chính: một là phải tiêu tốn thời gian để thiết lập con đường (kênh truyền) cố định giữa hai thiết bị cần truyền, hai là do lượng lưu thông khác không thể chia sẻ dường truyền chuyên trách đó, nên băng thông có thể vận dụng không hiệu quả và do các mạng chuyển mạch phải có sự thặng dư băng thông, nên chi phí xây dựng cũng vì thế mà tăng cao.

**- Chuyển thông điệp**

Kỹ thuật *chuyển thông điệp* [*Message swiching*] xem mỗi thông điệp như một thực thể độc lập có thông tin địa chỉ mô tả đích của thông điệp. Thông tin này được dùng tại mỗi trạm chuyển kế tiếp trong tuyến đường của nó. Trạm chuyển thông điệp được lập trình theo thông tin liên quan đến các trạm chuyển khác trong mạng, và có thể được chuyển gửi các thông điệp đến các đích của chúng. Chúng cũng có thể được lập trình theo thông tin về các tuyến đường hiệu quả nhất. Tuỳ theo các điều kiện mạng, các thông điệp khác nhau có thể được gửi thông qua mạng theo các tuyến đường khác nhau, xem hình 3.9.




**Hình 3.9. Chuyển mạch thông điệp**

Kỹ thuật chuyển thông điệp sẽ chuyển giao thông điệp hoàn chỉnh từ trạm chuyển này sang trạm chuyển kế tiếp, ở đó thông điệp được lưu trữ trước khi được chuyển gửi vào lần sau. Do mỗi thông điệp được lưu trữ trước khi tiếp tục được gửi đến trạm chuyển kế tiếp, nên kiểu mạng này thường được gọi là mạng lưu - và -chuyển gửi [ Store-and-forward]. Trạm chuyển thông điệp thường là các máy tính đa dụng. Chúng phải được trang bị một kho lưu trữ ( thường là các ổ đĩa cứng) có đủ dung lượng để cho phép lưu trữ các thông điệp cho đến khi có thể chuyển gửi .

Thư điện tử là một ứng dụng chung của kỹ thuật chuyển thông điệp. Khi bàn giao thư, có thể được phép trễ trong một thời gian nhất định , không như các yêu cầu khi hai máy tính đang trao đổi dữ liệu theo thời gian thực. Phương pháp chuyển thông điệp dùng các thiết bị tương đối rẻ tiền để chuyển gửi các thông điệp và vẫn có thể hoạt động tốt với các kênh truyền thông tương đối chậm. Các ứng dụng khác để chuyển thông điệp bao gồm các ứng dụng nhóm như luồng công việc [workflow ], lên lịch [ calendaring ] , và phần nhóm [ groupware ].

Chuyển thông điệp có vài ưu điểm như :

- Hiệu suất sử dụng đường truyền cao vì đường truyền không bị chiếm dụng độc quyền mà được phân chia giữa nhiều thiết bị mạng.
- Trạm chuyển thông điệp ( nút mạng) có thể lưu trữ các thông điệp cho đến khi một kênh rỗi mới truyền, giảm bớt độ nhạy cảm với sự tắc nghẽn mạng.

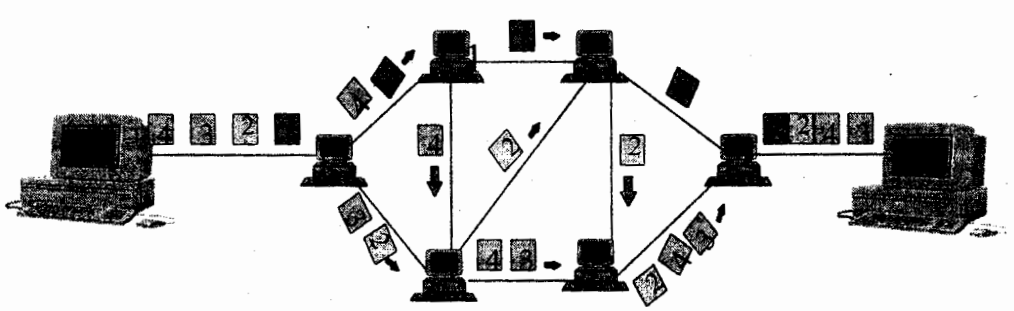
- Có thể dùng các mức ưu tiên thông điệp để quản lý lượng lưu thông trên mạng.
- Phương pháp định địa chỉ quảng bá sử dụng băng thông mạng hiệu quả hơn bằng cách bàn giao các thông điệp cho nhiều đích.

Nhược điểm chính của việc chuyển thông điệp đó là có độ trễ truyền tin cao do việc phải lưu trữ tạm thời và độ dài của thông diep lớn vì thế không phù hợp với các ứng dụng thời gian thực, bao gồm truyền thông dữ liệu,video, audio.

***- Chuyển gói tin***

Trong các phương pháp chuyển gói tin [packet swiching], các thông điệp được chia thành các gói tin nhỏ hơn. Mỗi gói tin bao gồm thông tin địa chỉ nguồn và đích để có thể độc lập định tuyến chúng riêng lẻ thông qua liên mạng. Như mô tả hình 3.9, các gói tin tạo thành một thông điệp có thể theo các tuyến đường rất khác nhau thông qua liên mạng.

Phương pháp chuyển gói tin có vẻ rất giống với kỹ thuật chuyển thông điệp. Đặc tính để phân biệt đó là các gói tin được hạn chế theo một kích cỡ cho phép các thiết bị chuyển quản lý toàn bộ dữ liệu gói tin trong bộ nhớ, mà không cần lưu trữ dữ liệu tạm thời trên đĩa. Do đó, phương pháp chuyển gói tin định tuyến các gói tin thông qua mạng nhanh và hiệu quả hơn nhiều so với phương pháp chuyển thông điệp.



**Hình 3.10. Mạng chuyển mạch gói**

Hiện có vài phương pháp chuyển gói tin. Dưới đây đề cập hai trong số các phương pháp này:

➢ Gam dữ liệu

➢ Mạch ảo.

*Chuyển gói tin gam dữ liệu*

Các dịch vụ gam dữ liệu [ datagram service ] xem mỗi gói tin như một thông điệp độc lập. Mỗi gói tin được định tuyến độc lập thông qua liên mạng, và mỗi nút chuyển [ swich node] sẽ quyết định nên dùng phân đoạn nào cho bước kế tiếp trong tuyến đường của gói tin. Khả năng này cho phép các trạm chuyển bỏ qua các phân đoạn bận rộn và tiến hành các bước khác để tăng tốc các gói tin thông qua mạng (hình 3.10). Các gam dữ liệu thường được dùng trên các mạng LAN

Phương pháp chuyển gói tin phù hợp với nhu cầu truyền các thông điệp lớn theo kích cỡ khung tương đối nhỏ mà tầng vật lý có thể đảm đương. Tầng mạng chịu trách nhiệm phân nhỏ các thông điệp của các tầng phía trên thành các gam dữ liệu nhỏ hơn thích hợp với tầng vật lý. Tầng mạng cùng chịu trách nhiệm kiến tạo lại các thông điệp từ các gam dữ liệu khi nhận chúng.

*Chuyển gói tin mạch ảo*

Các mạch ảo [virtual circuit] hoạt động bằng cách thiết lập một tuyến liên kết hình thức giữa hai thiết bị trong truyền thông. Khi các thiết bị bắt đầu một phiên truyền thông, chúng đàm phán các tham số truyền thông, đường truyền mạng, vân vân. Cuộc đàm phán này thiết lập một mạch ảo, một đường truyền được định nghĩa kỹ lưỡng thông qua liên mạng qua đó các thiết bị sẽ truyền thông với nhau. Mạch ảo này thường giữ nguyên hiệu lực cho đến khi các thiết bị ngưng truyền thông.

Các mạch ảo được phân biệt thông qua một tuyến liên kết lôgic. ảo có nghĩa là mạng ứng sử như thể một mạch vật lý chuyên trách được thiết lập giữa các thiết bị đang truyền thông. Cho dù không tồn tại một mạch vật lý như vậy, mạng vẫn tạo bề ngoài một tuyến liên kết vật lý miễn là còn liên quan đến các thiết bị tại các đầu của mạch. Các mạch ảo thường được dùng phối hợp với các dịch vụ hướng - liên kết,

Các ưu điểm của phương pháp chuyển gói tin

Phương pháp chuyển gói tin tối ưu hoá việc dùng băng thông bằng cách cho phép nhiều thiết bị định tuyến các gói tin thông qua cùng những kênh trên mạng. Vào một thời điểm nhất định, một trạm chuyển có thể đang định tuyến các gói tin đến vài thiết bị đích khác nhau, điều chỉnh các tuyến đường theo yêu cầu để đạt được hiệu năng khả dĩ tốt nhất vào lúc đó.

Do các thông điệp không được lưu dữ toàn bộ tại các trạm chuyển trước khi chuyển gửi, nên các độ trễ truyền sẽ ngắn hơn đáng kể so với trường hợp chuyển thông điệp.

Tuy các thiết bị chuyển không buộc phải trang bị các ổ đĩa cứng có dung lượng lớn, song chúng cần một lượng bộ nhớ thời gian thực đáng kể. Ngoài ra, chúng phải có đủ năng lực xử lý để chạy các giao thức định tuyến phức tạp hơn mà phương pháp

chuyển gói tin yêu cầu. Trong số các điểm phức tạp mới, có nhu cầu nhận dạng khi các gói tin bị thất lạc để có thể yêu cầu truyền lại.

**3. Thuật toán định tuyến**

Định tuyến có nghĩa là chuyển gửi các thông điệp thông qua các nút mạng (thiết bị chuyển). Trong vài trường hợp, thông tin định tuyến được lập trình vào trong các thiết bị chuyển (Nút chuyển). Tuy nhiên, các nút chuyển lập trình sẵn không thể điều chỉnh theo các điều kiện mạng thay đổi. Do đó, hầu hết các thiết bị định tuyến đều có khả năng phát hiện các tuyến đường thông qua liên mạng và lưu trữ thông tin định tuyến trong các bảng định tuyến.

Các bảng định tuyến không những lưu trữ thông tin đường truyền. Chúng còn lưu trữ các giá trị ước tính thời gian kéo dài để gửi một thông điệp thông qua một tuyến đường nhất định. Giá trị ước tính thời gian này được gọi là đơn vị trọng lượng của một đường truyền cụ thể. Có vài phương pháp để ước tính giá trị đơn vị trọng lượng định tuyến (giá thành), như sau:

➢ Số đếm bước nhảy [ hop count] mô tả số lượng bộ định tuyến mà một thông điệp sẽ băng qua trước khi đạt đến đích của nó. Nếu mặc nhận tất cả các bước nhảy đều có cùng thời lượng, đường truyền tối ưu chính là đường truyền có số bước nhảy nhỏ nhất.

➢ Số đếm nhịp [tic count] là giá trị ước tính thời gian thực tế, ở đó nhịp là đơn vị thời gian như các thực thi định tuyến định nghĩa.

Sau khi thiết lập các mức trọng lượng, bộ định tuyến có thể chọn các tuyến đường, tĩnh hoặc động, như sau:

➢ Phương pháp chọn tuyến đường tĩnh sử dụng các tuyến đường đã được điều hành viên mạng lập.

➢ Phương pháp chọn tuyến đường động sử dụng thông tin trọng lượng định tuyến để chọn tuyến đường có hiệu quả nhất cho một gói tin nhất định. Khi các điều kiện mạng thay đổi và được phản ánh trong các bảng định tuyến, bộ định tuyến có thể chọn các tuyến đường khác nhau để duy trì các mức đơn vị trọng lượng thấp.

Ta sẽ xem xét hai phương pháp phát hiện định tuyến - định tuyến véc tơ cự ly [distance vector routing] và định tuyến trạng thái nối kết [ link - state routing].

*** Định tuyến véc tơ cự ly**

Các bộ định tuyến véc tơ cự ly quảng cáo sự hiện diện của chúng với các bộ định tuyến khác trên mạng. Theo định kỳ, mỗi bộ định tuyến trên mạng quảng bá thông tin trong bảng định tuyến của nó. Các bộ định tuyến khác có thể dùng thông tin này để cập các bảng định tuyến riêng của mình và tự tính lại các đơn vị trọng lượng từ nó tới các

các nút khác trong mạng. Ví dụ trong liên mạng có 3 nút S1, S2, S3. S1 nối với S2, S2 nối với S3. Giả sử nút S3 biết được rằng S2 kề nó chỉ cách có 1 bước nhảy và nó nhận được thông tin thông báo quảng bá trên mạng từ S2 là cạnh S2 có nút S1 cách S2 bằng 2 bước nhảy vì vậy S3 sẽ biết được để đến S1 thông qua nút S2 sẽ là ba bước nhảy và nó sẽ cập nhật thông tin mới vào bảng định tuyến riêng của nó.

Định tuyến véctơ cự ly là một thuật toán hiệu quả, song chưa hẳn là hữu hiệu. Do các thay đổi có thể dao động thông qua các bộ định tuyến trên mạng, nên phải mất một thời gian để tất cả các bộ định tuyến trên mạng biết được đã xảy ra một thay đổi. Ngoài ra, các đợt quảng bá thông tin định tuyến thường xuyên sẽ tạo ra các mức lưu thông cao có thể phương hại đến khả năng vận hành trên các mạng lớn.

*** Định tuyến trạng thái nối kết**

Định tuyến trạng thái nối kết [link - state] giảm bớt được lượng lưu thông mạng cần thiết để cập nhật các bảng định tuyến. Các bộ định tuyến mới được gắn vào mạng có thể yêu cầu thông tin định tuyến từ một bộ phận định tuyến lân cận.

Sau khi các bộ định tuyến trao đổi thông tin định tuyến về mạng, các bộ định tuyến sẽ chỉ quảng bá các thông điệp khi có thay đổi. Các thông điệp này chứa thông tin về trạng thái của từng tuyến nối kết mà bộ định tuyến đó thiết lập với các bộ định tuyến khác trên mạng. Do các bộ định tuyến giữ cho nhau cập nhật, nên không cần phải thường xuyên tiến hành cập nhật thông tin định tuyến trên toàn mạng.

**4. Các dịch vụ liên kết**

Tầng mạng cũng cung cấp các dịch vụ hướng-liên kết, bao gồm các kỹ thuật điều khiển luồng, phát hiện lỗi và phát tín hiệu báo nhận. Các tín hiệu báo nhận mạng (network acknowledgments) được dùng để cung cấp tính năng điều khiển luồng, phát hiện lỗi và điều khiển chuỗi gói tin.

*Điều khiển luồng của tầng mạng*

Tầng nối kết dữ liệu quản lý tính năng điều khiển luồng dựa trên các khả năng của các thiết bị đang truyền thông. Tầng mạng quản lý tính năng điều khiển luồng để tránh tình trạng tắc nghẽn trên mạng. Tầng mạng xác định số lượng gói tin sẽ gửi thông qua một tuyến đường nhất định. Nhờ định tuyến các gói tin vòng qua các tuyến nối kết đang bận, băng thông mạch sẽ được dùng hiệu quả hơn và tình trạng tắc nghẽn cũng giảm bớt. Vì lý do này, kỹ thuật điều khiển luồng mạng thường được gọi là *điều khiển tình trạng tắc nghẽn.*

Kỹ thuật điều khiển luồng của tầng mạng có thể cho phép các thiết bị thương lượng một tốc độ dữ liệu bảo đảm. Cũng có thể sử dụng các cửa sổ tĩnh và động.

Các thiết bị nhận có thể điều khiển tình trạng tắc nghẽn bằng cách trì hoãn trước khi gửi tín hiệu báo nhận. Trong các tình huống này, bên gửi có thể mặc nhận gói tin đã thất lạc và được truyền lại. Để phòng việc truyền lại không cần thiết, một số giao thức đã định nghĩa các gói tin phát tín hiệu tình trạng tắc nghẽn và cho phép các thiết bị nhận yêu cầu rõ rệt các độ trì hoãn trong khi truyền.

*Điều khiển lỗi của tầng mạng*

Có thể phát hiện nhiều điều kiện lỗi tại tầng mạng. Các lỗi trong dữ liệu thường được phát hiện bằng các thuật toán CRC. Do thông tin phần đầu gói tin thay đổi theo mỗi bước nhảy (các địa chỉ thay đổi), nên các giá trị CRC phải được mỗi bộ định tuyến tính toán lại.

Tuy tầng mạng có thể thực thi kỹ thuật phát hiện tình trạng thất lạc và nhân bản các gói tin, song tầng chuyển tải thường điều quản các chức năng này.

*Điều khiển chuỗi gói tin*

Các mạng chuyển gói tin có thể định tuyến các gói tin bằng cách thay đổi các tuyến đường. Kết quả là, các gói tin của một thông điệp có thể đến đích cuối cùng không theo thứ tự. Trường hợp này có thể xảy ra cho các dịch vụ hướng-liên kết và gam dữ liệu. Ta có thể cấu hình tầng mạng để điều quản tính năng điều khiển chuỗi gói tin, mặc dù chức năng này thường do tầng vận chuyển đảm nhận.

### 3.2.6 Tầng vận chuyển

Tầng giao vận có nhiệm vụ đảm bảo chuyển giao dữ liệu từ nơi gửi tới nơi nhận an toàn và hiệu suất cao, các giao thức tầng thấp hơn đảm trách việc bàn giao các thông điệp giữa các thiết bị vật lý cụ thể. Tuy nhiên, tầng chuyển tải liên quan tới việc bàn giao các thông điệp giữa các tiến trình đang chạy trên các thiết bị đó. Mỗi khi có một thiết bị đang dùng hệ điều hành đa nhiệm và nhiều tiến trình có thể đang chạy trên thiết bị đó, thì nhất thiết các thông điệp phải được bàn giao từ một tiến trình trên thiết bị truyền sang đúng tiến trình trên thiết bị đang nhận.

Tầng giao vận cho phép các giao thức tầng phía trên giao tiếp với mạng, song lại che giấu các chi tiết phức tạp của tác vụ mạng. Một trong số các chức năng của tầng giao vận đó là tách nhỏ các thông điệp lớn thành các phân đoạn phù hợp với khả năng bàn giao của mạng và thực thi các thủ tục để bảo đảm các phân đoạn đó bàn giao đáng tin cậy cho các thiết bị đích của chúng.

Sau đây ta xem xét một số chức năng chính của tầng giao vận:

**1. Định địa chỉ**

Tính năng định địa chỉ của tầng giao vận liên quan đến việc bàn giao các thông điệp của một tiến trình cụ thể trên một máy tính sang đúng tiến trình đang chạy trên máy tính đích. Các thông điệp có thể được định danh theo hai cách:

*Mã số định danh liên kết* (connection identifier _ CID) còn gọi là *ổ cắm* (socket) hoặc *cổng* (port), tùy theo các thực thi giao thức cụ thể. Mã số định danh liên kết gắn nhãn mỗi cuộc liên lạc và cho phép một tiến trình liên lạc với các tiến trình đang chạy trên các thiết bị khác. Mỗi cuộc liên lạc đều được gán một mã số. Một dịch vụ, chạy tại các cấp OSI cao hơn, sẽ định danh các phiên truyền thông bằng các mã số CID cho phép tầng giao vận điều hướng tính năng định địa chỉ tầng thấp hơn và bàn giao các thông điệp theo yêu cầu.

*Mã số định địa giao dịch* được dùng khi hai thiết bị tham gia nhiều đợt trao đổi dữ liệu. *Dấu định danh giao dịch* được dùng khi cuộc trao đổi là một sự kiện một lần, bao gồm một yêu cầu và một đáp ứng.

Chuyển đổi địa chỉ /tên

Các địa chỉ mạng luôn là những số nhị phân, thường có chiều dài là 32 bit. Có thể diễn tả các con số này theo hệ ký hiệu thập phân để giúp ta dễ dàng định danh. Tuy nhiên, các con số này không nhận dạng được dưới dạng các từ mà con người thường sử dụng để đặt tên cho các thiết bị mạng. Có vài giao thức mạng đã giải quyết vấn đề này, các tên này được một dịch vụ trên mạng phiên dịch thành các địa chỉ mạng bằng số. Tiến trình phiên dịch này có thể thực hiện bởi các thiết bị mạng riêng lẻ hoặc một máy chủ tên trung tâm (Domain name server). Cụ thể:

*Phân giải địa chỉ/ Tên do bên yêu cầu dịch vụ bắt đầu.*

Theo phương pháp này, một thiết bị yêu cầu thông tin địa chỉ sẽ quảng bá một gói tin yêu cầu thông tin về một tên,địa chỉ, hay dịch vụ cụ thể. Thiết bị tương ứng với tên, địa chỉ, hay dịch vụ đó sẽ đáp ứng bằng thông tin cần thiết.

*Phân giải địa chỉ/ Tên do bên cung cấp dịch vụ bắt đầu*

Phương pháp này sử dụng một máy chủ thư mục trung tâm (Domain name server) thu nhập thông tin do các thiết bị trên mạng quảng bá. Các thiết bị yêu cầu tên hay thông tin địa chỉ có thể yêu cầu nó từ máy chủ thư mục.

### 2. Phát triển phân đoạn

Khi các thông điệp từ các giao thức cấp cao hơn vượt kích cỡ mà một ngăn xếp giao thức cho phép đối với một phân đoạn, tầng giao vận sẽ chia các thông điệp ngoài biến thành các phân đoạn có kích cỡ thích hợp. Tầng giao vận cũng tái hợp các phân đoạn đến thành các dạng thức thông điệp mà các tầng phía trên yêu cầu.

Tầng giao vận cũng có thể tổ hợp nhiều thông điệp nhỏ thành chỉ một phân đoạn để cải thiện hiệu năng của mạng. Mỗi thành phần thông điệp được định danh bằng mã số định danh liên kết( CID). CID này cho phép tầng giao vận của thiết bị nhận bàn giao từng thông điệp cho đúng tiến trình.

**3. Các dịch vụ liên kết**

Chất lượng dịch vụ mạng tại tầng giao vận tuỳ thuộc vào từng loại mạng. CCITT và ISO đã định nghĩa 3 loại mạng sau đây:

- Mạng loại A: có tỷ lệ lỗi và sự cố có báo hiệu chấp nhận được. Các gói tin được giả thiết không bị mất. Tầng giao vận không cần cung cấp các dịch vụ phục hồi hoặc xắp sếp lại thứ tự.
- Mạng loại B: có lệ lỗi chấp nhận được nhưng tỷ lệ sự cố có báo hiệu lại không chấp nhận được. Tầng giao vận phải có khả năng phục hồi lại khi xẩy ra lỗi hoặc sự cố.
- Mạng loại C: có tỷ lệ lỗi không chấp nhận được. Tầng giao vận phải có khả năng phục hồi lỗi và sắp xếp thứ tự các gói tin.

Tầng giao vận cung cấp các cơ chế giao thức khác nhau để thực hiện chất lượng dịch vụ yêu cầu bởi thực thể sử dụng dịch vụ vận chuyển. Có thể phân giao thức tầng giao vận theo các lớp sau đây:

- *Lớp 0*: (Mạng loại A) được gọi là lớp đơn giản, lớp này thiết lập kết nối để cung cấp các chức năng trao đổi, truyền dữ liệu và thống kê lỗi giao thức.
- *Lớp 1*: (Mạng loại B) lớp này cung cấp chức năng khắc phục lỗi xoá rồi lập lại kết nối để khắc phục lỗi. Lớp này còn được gọi là lớp khắc phục lỗi cơ bản.
- *Lớp 2*: (Mạng loại A) để bổ xung cho các chức năng cung cấp bởi lớp 0, lớp này cung cấp các chức năng ghép nhiều kết nối giao vận thành một kết nối mạng. Lớp này còn được gọi là lớp nhân ghép.
- *Lớp 3*: (Mạng loại B) để bổ xung cho chức năng cung cấp bởi lớp 2, lớp này cung cấp các chức năng khắc phục bằng cách xoá rồi lại khôi phục kết nối từ đầu. Nó cũng được gọi là lớp nhân ghép kênh/ khắc phục lỗi.
- *Lớp 4*: (Mạng loại C) đây là lớp thủ tục giao vận phức tạp nhất để bổ xung cho chức năng cung cấp bởi lớp 3, lớp này cung cấp các chức năng chữa lỗi khi các khâu kiểm tra trước đó bỏ sót, giải quyết vấn đề mất gói tin và gói tin hỏng, giải quyết các yêu cầu khởi động lại.

Ví dụ một số dịch vụ có thể được thực hiện tại tầng giao vận :

*Kết chuỗi phân đoạn*

Kết chuỗi phân đoạn (segment sequencing) là một dịch vụ hướng nối kết do tầng giao vận đảm trách. Khi các thông điệp lớn được chia thành các phân đoạn để giao vận, tầng giao vận phải tái kết chuỗi các phân đoạn khi nhận chúng, trước khi tái lắp ráp thông điệp ban đầu.

*Điều khiển lỗi*

Nếu các phân đoạn bị mất trong khi truyền, hoặc các phân đoạn có các ID phân đoạn trùng lặp, tầng giao vận phải bắt đầu tính năng phục hồi lỗi.Các chiến lược để điều khiển lỗi bao gồm:

- Các mã số chuỗi phân đoạn duy nhất.
- Các mạch ảo, chỉ cho phép dùng một mạch ảo cho một phiên truyền.
- Các giá trị hết giờ được gỡ bỏ ra khỏi các phân đoạn mạng đã được định tuyến sai và đã nằm lại trên mạng vượt quá một thời điểm đã định.

### 3.2.7 Tầng phiên

Tầng phiên làm việc quản lý các phiên làm việc giữa hai máy tính bằng cách thiết lập, quản lý và kết thúc các phiên truyền thông.

Các phiên làm việc thường có ít nhất ba giai đoạn:

- Thiết lập tuyến liên kết: Bên yêu cầu dịch vu sẽ yêu cầu bắt đầu một dịch vụ. Trong tiến trình xác lập, phiên truyền thông được thiết lập, và các quy tắc được thoả thuận.
- Chuyển giao dữ liệu. Do các quy tắc được thoả thuận trong khi xác lập, nên mỗi bên của phiên làm việc sẽ biết nội dung mong đợi. Phiên truyền thông sẽ hữu hiệu, và các lỗi cũng dễ phát hiện.
- Giải phóng tuyến kết. Khi hoàn tất phiên làm việc.

**Thiết lập tuyến liên kết**

Các công việc có thể được tiến hành vào lúc bắt đầu một phiên làm việc:

- Chỉ định các dịch vụ cần thiết
- Thẩm định quyền truy nhập người dùng và các thủ tục bảo mật khác
- Thương thảo các giao thức và các tham số giao thức
- Thông báo các ID liên kết
- Thiết lập kiểu điều khiển, cũng như công nhận cách đánh số và các thủ tục truyền lại.

**Chuyển giao dữ liệu**

Sau khi thiết lập tuyến liên kết, các thiết bị có liên quan có thể bắt đầu cuộc làm việc. Ngoài việc trao đổi dữ liệu, các thiết bị này có thể trao đổi các tín hiệu báo nhận và các dữ liệu điều khiển khác quản lý cuộc làm việc.

Tầng phiên làm việc cũng có thể liên kết các giao thức để bắt đầu lại các cuộc làm việc bị gián đoạn. Sau khi thiết lập một cuộc làm việc chính thức, các thiết bị nhận dạng một tuyến liên kết bị mất mỗi khi tuyến liên kết đó không được chính thức giải phóng Do đó, một thiết bị sẽ nhận ra một tuyến liên kết bị mất khi nó không thể nhận một tín hiệu báo nhận dự kiến hoặc phiên truyền dữ liệu.

Trong một thời hạn nhất định, hai thiết bị có thể tái nhập phiên làm việc đã bị gián đoạn nhưng chưa được giải phóng.

**Giải phóng tuyến liên kết**

Đây là tiến trình trình tự để đóng phiên truyền thông và giải phóng các tài nguyên của bên cung cấp dịch vụ.

### 3.2.8 Tầng trình diễn

Tầng trình diễn sử lý cú pháp, hoặc các quy tắc văn phạm, cần thiết cho phiên truyền thông giữa hai máy tính. Nó có mục đích đảm bảo cho các hệ thống cuối có thể truyền thông có kết quả ngay cả khi chúng sử dụng các biểu diễn dữ liệu khác nhau. Các dịch vụ của tầng trình diễn:

**Phiên dịch dữ liệu:**

Một mục tiêu quan trọng cần giải quyết khi thiết kế các mạng đó là cho phép các kiểu máy tính khác nhau trao đổi dữ liệu. Tuy mục tiêu này khó có thể được giải quyết triệt để, song việc vận dụng hiệu quả các kỹ thuật phiên dịch dữ liệu có thể giúp nhiều kiểu máy tính truyền thông với nhau. Có bốn dạng phiên dịch dữ liệu: thứ tự bit, thứ tự byte, mã ký tự, và cú pháp tập tin.

*Thứ tự bit:* Khi số nhị phân được truyền thông qua một mạng, chúng được gửi đi theo từng bit một. Hãy xét số nhị phân 10110010. Máy tính truyền có thể bắt đầu tại một trong hai đầu của con số:

+ Nó có thể bắt đầu tại MSD (most-significant digit- chữ số quan trọng nhất), là chữ số có giá trị cao nhất, và gửi một 1 trước.

+ Nó có thể bắt đầu tại LSD (least-significant digit- chữ số ít quan trọng nhất), là chữ số có giá trị thấp nhất, và gửi một 0 trước.

Trừ phi các thiết bị gửi và nhận đồng ý với các quy ước thứ tự bit, chúng sẽ thay đổi các giá trị của các số nhị phân đang truyền.

*Phiên dịch thứ tự Byte:* Logic tương tự cũng áp dụng cho thứ tự Byte. Các giá trị phức hợp thường phải được biểu thị bằng nhiều byte, nhưng các máy tính khác nhau

thường dùng các quy ước khác nhau về việc sẽ truyền byte nào trước. Các bộ vi xử lý Intel bắt đầu bằng byte ít quan trọng nhất. Do chúng bắt đầu tại đầu nhỏ, nên được gọi là kết đầu nhỏ [little endian]. Các bộ vi sử lý Motorola bắt đầu bằng byte quan trọng nhất, nên được gọi là kết đầu to [big endian]. Để hoà hợp những khác biệt này, ta cần phải có tính năng phiên dịch thứ tự Byte.

*Phiên dịch mã ký tự:* Hầu hết các máy tính đều dùng một trong các lược đồ đánh số nhị phân dưới đây để biểu thị các bộ ký tự:

- ASCII ( Amerian Standard Code for information interchange - mã chuẩn của Hoa kỳ để hoán đổi thông tin) có 8 bit được dùng để biểu thị các ký tự tiếng Anh trên tất cả các máy tính và hầu hết các máy tính mini.
- EBCDIC (extended Binary Coded Decimal Interchange Code - mã hoán đổi thập phân mã hoá nhị phân mở rộng] được dùng để biểu thị cho các ký tự tiếng Anh trên máy tính lớn IBM.
- Shift-JIS, được dùng để biểu thị các ký tự tiếng Nhật
- Mã UNICODE mã chuẩn dạng 16 bit dùng để biểu diễn các ký tự của hầu hết các quốc gia trên thế giới.

*Phiên dịch cú pháp tập tin:* Khi các dạng thức tập tin khác nhau giữa các máy tính đòi hỏi phải phiên dịch. Dưới đây là một số tình huống yêu cầu phiên dịch dạng thức tập tin:

+ Sao các tập tin giữa máy Macintosh và PC DOS. Các tập tin Macintosh thực tế bao gồm hai tập tin hữu quan có tên dữ liệu [data fork] và tài nguyên [resource fork]. Trong khi đó, các tập tin PC chỉ bao gồm một tập tin đơn lẻ.

+ Chép các tập tin giữa các máy PC DOS và các trạm làm việc Unix.

Một khi thực hiện đúng đắn, các kỹ thuật phiên dịch này có thể hoàn toàn thông suốt. Ví dụ, NetWare cho phép người dùng DOS, Macintosh, và Unix chia sẻ cùng các tập tin trên một máy chủ NetWare bằng cách dùng một tính năng có tên hỗ trợ không gian tên [name space support].

**Mã hoá và nén tin**

Tầng trình diễn thực hiện các kỹ thuật mã hoá và nén tin để tăng hiệu quả trong truyền thông và đảm bảo an toàn cho dữ liệu truyền thông trên mạng. một số kỹ thuật chi tiết xem mục 2.2.3

### 3.2.9 Tầng ứng dụng

Tầng ứng dụng liên quan đến tiến trình cung cấp các dịch vụ trên mạng, các dịch vụ mạng này bao gồm: dịch vụ tập tin, dịch vụ in, dịch vụ cơ sở dữ liệu, và các dịch vụ khác như trong phần 1.1.2 Người ta thường hiểu lầm rằng tầng ứng dụng chịu trách

nhiệm chạy các ứng dụng người dùng như các trình xử lý văn bản. Không phải vậy. Tuy nhiên, tầng ứng dụng cũng cung cấp một giao diện qua đó các ứng dụng có thể truyền thông với mạng.

Tầng ứng dụng thực hiện hai chức năng có liên quan đến việc sử dụng các dịch vụ trên mạng. Một liên quan đến việc thông báo các dịch vụ hiện có và một liên quan đến việc dùng các dịch vụ.

**Thông báo các dịch vụ**

Để thông tin cho các hệ khách về các dịch vụ sẵn có, tầng ứng dụng loan báo các địa chỉ dịch vụ này với mạng. Các địa chỉ này cung cấp cơ chế cho phép các hệ khách liên lạc với các dịch vụ.

**Các phương pháp dùng dịch vụ**

Các hệ khách có thể truy cập các dịch vụ bằng ba phương pháp sau:

- Ngắt lệnh gọi OS
- Tác vụ từ xa
- Cộng tác

*Ngắt lệnh gọi OS*

Các ứng dụng trên các hệ khách yêu cầu các dịch vụ bằng cách đặt các lệnh gọi dịch vụ vào các hệ điều hành (OS) cục bộ của mình. Lệnh gọi dịch vụ là một thủ tục chính thức được xác lập bởi các thiết kế viên của hệ điều hành cung cấp một giao diện với các chương trình mà hệ điều hành đó hỗ trợ. Khi một hệ khách được cấu hình để hoạt động trên mạng, ngắt lệnh gọi sẽ chặn các yêu cầu dịch vụ. Các lệnh gọi dịch vụ yêu cầu các tài nguyên cục bộ sẽ được chuyển gửi đến OS của hệ khách. Các lệnh gọi dịch vụ yêu cầu các tài nguyên mạng sẽ được chuyển giao đến mạng, ở đó chúng được chuyển gửi đến máy chủ thích hợp. Ngắt lệnh gọi OS cho phép một hệ khách vận dụng các dịch vụ mạng kể cả khi OS không có khả năng nối mạng vốn có.

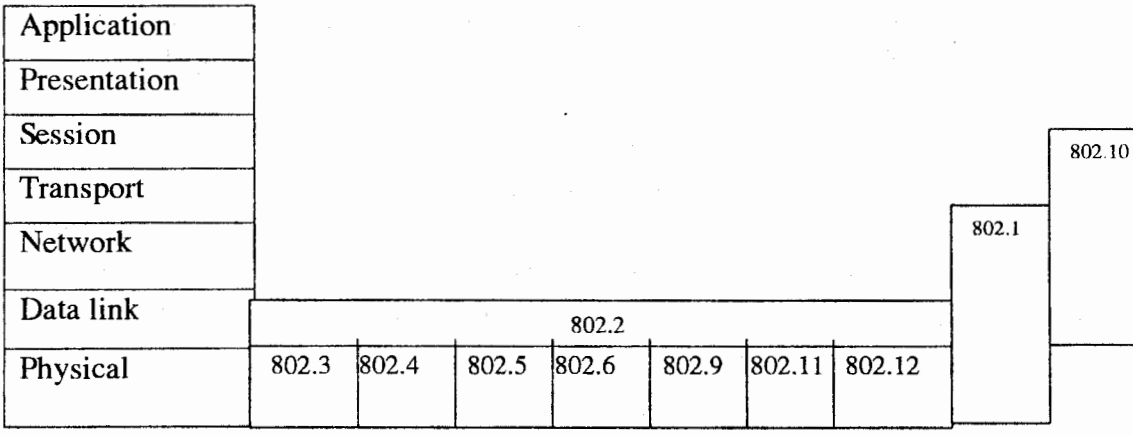
*Tác vụ từ xa*

Khi OS khách có cài sẵn khả năng mạng, nó có thể truy cập máy chủ bằng tác vụ từ xa. OS khách giao tiếp trực tiếp với mạng. Đối với máy chủ, các yêu cầu của OS khách cũng chẳng khác gì các yêu cầu của các hệ riêng trên máy chủ. Nói cách khác, máy chủ không trực tiếp nhận biết sự tồn tại riêng biệt của các hệ khách.

*Điện toán cộng tác*

Có vài hệ điều hành trên máy khách và máy phục vụ cao cấp đến nỗi khó lòng phân biệt ranh giới giữa chúng. Các hệ điều hành làm việc với nhau để phối hợp cách dùng các tài nguyên trên hai máy tính tương ứng. nó không chỉ gồm các máy tính chỉ biết truy cập các dịch vụ của nhau. Thay vì thế, các máy tính tham gia vào lĩnh vực điện toán hợp tác sẽ góp chung tất cả các tài nguyên của chúng. Ví dụ, một máy tính có

thể bắt đầu một tiến trình trên một máy tính khác để vận dụng vài chu kỳ xử lý tự do. Điều này yêu cầu các hệ điều hành tham gia phải có khả năng hợp tác cao.




**Hình 3.11. Mối quan hệ giữa các chuẩn IEEE 802 và mô hình OSI**

## 3.3 Chuẩn IEEE 802

IEEE (institute of Electrical and Electronic Engineers - viện thiết kế điện và điện tử) là một tổ chức chuyên nghiệp lớn nhất thế giới và có ảnh hưởng rất quan trọng đối với việc xây dựng các chuẩn. Uỷ ban 802 của IEEE đã phát triển một loạt các chuẩn cho mạng cục bộ LAN và mạng diện rộng WAN. Các chuẩn này đã được thừa nhận và đã được ISO tái công bố dưới dạng các chuẩn ISO 802.

Mười hai tiểu ban đã xem xét các chuẩn 802. ( Một tiểu ban thứ mười ba đã được đề nghị để phát triển chuẩn 100BASEX.) Hình 3.11 minh hoạ vị trí của mỗi chuẩn trong Mô hình tham khảo OSI.

**IEEE 802.2**

Chuẩn IEEE 802.2 định nghĩa một tầng con LLC tương đương với tầng 2 - Liên kết dữ liệu được các giao thức tầng phía dưới khác sử dụng. Do các giao thức tầng phía dưới sử dụng chỉ một tầng giao thức LLC đơn lẻ, nên các giao thức tầng mạng có thể có được thiết kế độc lập với tầng vật lý của mạng và các thực thi tầng con MAC.

LLC chắp vào các gói tin một phần đầu định danh các giao thức tầng phía trên, kết hợp với khung. Phần đầu cũng khai báo các tiến trình là nguồn và đích của mỗi gói tin.

**IEEE 802.3**

Chuẩn IEEE 802.3 định nghĩa một mạng phát sinh từ mạng Ethernet, thoạt đầu được phát triển bởi các hãng Digital, Intel, và Xerox. Chuẩn này định nghĩa các đặc tính liên quan đến tầng con MAC của tầng nối kết dữ liệu và tầng vật lý OSI. Ngoài một chi tiết khác biệt nhỏ-kiểu khung- các chức năng IEEE 802.3 Ethernet giống y hệt DIX Ethernet v.2. Thậm chí hai chuẩn có thể cùng tồn tại trên cùng một hệ cáp, tuy các thiết bị dùng chuẩn này không thể truyền thông trực tiếp với các thiết bị dùng chuẩn kia.

Tầng con MAC dùng dạng truy cập tranh chấp có tên CSMA/CD. Kỹ thuật này giảm bớt tình trạng va chạm bằng cách mỗi thiết bị lắng chờ mạng để xác định nó đã yên hay chưa ( "cảm ứng tần số tải"); một thiết bị chỉ gắng truyền khi mạng yên lặng. Điều này giúp giảm bớt song không loại hẳn các sự cố va chạm bởi các tín hiệu phải mất một thời gian nhất định để loan truyền qua mạng. Khi các thiết bị truyền, chúng tiếp tục lắng chờ, do đó chúng có thể phát hiện một va chạm nếu nó xảy ra. Khi một va chạm xảy ra, tất cả các thiết bị ngưng truyền và gửi một tín hiệu "đang kẹt" để thông báo cho tất cả các trạm về sự cố va chạm. Sau đó, mỗi thiết bị đợi một lượng ngẫu nhiên trước khi gắng truyền lại. Tổ hợp bảo vệ này làm giảm bớt đáng kể các sự cố va chạm trên tất cả ngoại trừ các mạng bận rộn nhất.

Phần định nghĩa tầng vật lý mô tả phương pháp phát tín hiệu ( Cả băng tần cơ sở lẫn băng tần rộng đều sẵn có), các tốc độ dữ liệu, vật tải, và các tôpô. Vài biến thể tầng vật lý cũng được định nghĩa. Mỗi biến thể được đặt tên theo một quy ước quy định tốc độ phát tín hiệu (1 hay 10) Mbps, chế độ băng tần cơ sở (BASE) hoặc băng tần rộng (BROAD), và một chỉ định các đặc tính vật tải.

Danh sách các chủng loại 802.3 được mô tả chi tiết ở mục 4.4

**IEEE 802.4**

Chuẩn 802.4 mô tả một mạng có tôpô buýt vật lý điều khiển việc truy cập vật tải theo cơ chế thẻ bài. Chuẩn đã được thiết kế để thoả các nhu cầu của các hệ thống tự động hoá về công nghiệp nhưng lại ít được phổ dụng. Cả hai cấu hình băng tần cơ sở lẫn băng tần rộng (dùng cáp đồng trục 75Ohm) đều sẵn có.

**IEEE 802.5**

Chuẩn IEEE 802.5 xuất xứ từ mạng TokenRing của IBM, sử dụng tôpô lôgic vòng khâu và cơ chế điều khiển truy cập vật tải gốc thẻ bài. Tốc độ dữ liệu 1,4, và 16 Mbps đã được định nghĩa. Chuẩn IEEE 802.5 không mô tả một hệ đấu cáp. Hầu hết các thực thi đều dứ trên hệ cáp IBM, sử dụng cáp xoắn cặp được đấu dây theo hình sao vật lý.

**IEEE 802.6**

Chuẩn IEEE 802.6 mô tả một chuẩn MAN tên DQDB (Distributed Queue Dual Bus = buýt đôi có hàng đợi phân phối). Không chỉ là một công nghệ mạng dữ liệu, DQDB rất thích hợp với các phiên truyền dữ liệu, tiếng, và video. Mạng dựa trên cáp quang theo cấu hình tôpô buýt đôi. Lượng lưu thông trên mỗi buýt là một chiều. Khi hoạt động theo từng cặp, hai buýt cung cấp một cấu hình dung lỗi. Băng thông được phân bổ bằng các khe thời gian, và các chế độ đồng bộ và dị bộ đều được hỗ trợ.

**IEEE 802.9**

Chuẩn IEEE 802.9 hỗ trợ một kênh dị bộ 10Mbps, cùng với 96 kênh 64Kbps (tổng băng thông 6 Mbps) có thể chuyên trách các luồng dữ liệu cụ thể. Tổng băng thông là 16 Mbps. Chuẩn này có tên là Ethernet đẳng thời (isoEnet) và được thiết kế cho các cơ sở có lượng lưu thông gián đoạn và quan trọng về thời gian.

**IEEE 802.11**

IEEE 802.11 là một chuẩn cho các LAN vô tuyến, hiện đang phát triển. Một phương pháp CSMA/CD đã được chứng nhận, nhưng chuẩn chung cuộc vẫn đang chờ giải quyết.

**IEEE 802.12**

Chẩn IEEE 802.12 dựa trên một đề nghị 100Mbps của các hãng IBM, AT&T và HewlettPackard được gọi là 100VGAnyLAN, mạng này dựa trên một tôpô đấu dây hình sao và phương pháp truy cập gốc tranh chấp qua đó các thiết bị phát tín hiệu cho ổ cái đấu dây về một nhu cầu truyền dữ liệu. Các thiết bị chỉ có thể truyền khi được ổ cái giao giấy phép. Chủ trương của chuẩn này là cung cấp một mạng cao tốc có thể hoạt động trong các môi trường hỗn hợp Ethernet và Token Ring bằng cách hỗ trợ cả hai kiểu khung.

# CHƯƠNG 4

# MẠNG CỤC BỘ LAN

## 4.1 Tổng quan về mạng cục bộ

Mạng cục bộ (Local area network-LAN) là một nhóm các máy tính và các thiết bị truyền thông mạng được kết nối với nhau trong một khu vực địa lý nhỏ, như toà cao ốc hay trụ sở làm việc của các cơ quan, công ty.

Các LAN thường có các đặc tính sau:

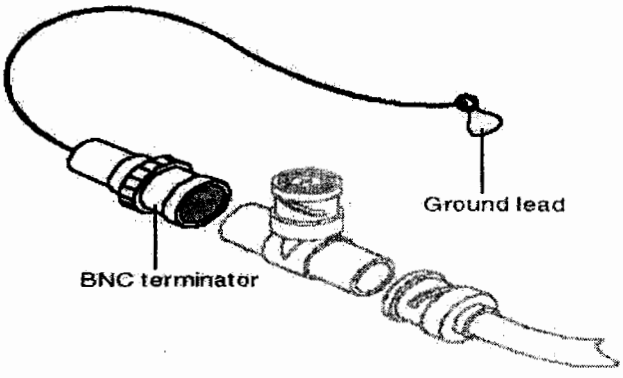
+ Chuyển giao dữ liệu với tốc độ nhanh
+ Thuộc loại mạng có tỷ lệ lỗi thấp.
+ Tồn tại trong một khu vực địa lý giới hạn
+ Công nghệ tương đối rẻ tiền.

Mạng LAN được kết nối theo nhiều kiểu khác nhau song tuân thủ theo hai mô hình mạng chính là mạng chủ tớ ( Clien/server) và mô hình bình đẳng (Peer To Peer). Hình dạng mạng được phân theo tôpô vật lý và tôpô logích.

**Tôpô vật lý**

Theo sơ dồ kết nối vật lý giữa các máy tính, mạng LAN có các dạng kết nối sau:

*Dạng BUS tuyến tính (linear bus topology)* : (Hình 1.3) Là một thiết kế đơn giản với một đoạn cáp chung, được gọi là BUS. Mọi thiết bị trên mạng cục bộ đều được nối với BUS tuyến tính này và dùng chung môi trường truyền thông duy nhất đó. Hai đầu của BUS được nối thiết bị đầu cuối (Terminator – hình 4.1)




**Hình 4.1 Đầu cuối cáp trong cấu hình BUS**

Dạng BUS tuyến tính thật đơn giản và tiết kiệm. Bất kỳ thiết bị nào nối mạng bị hư hỏng đều không ảnh hưởng gì đến hoạt động của mạng, nhưng nếu đường cáp bị đứt

thì mạng sẽ bị ngắt làm hai và làm ngưng trệ mạng. Trên các mạng lớn dùng BUS tuyến tính rất khó định vị các chỗ hỏng của cáp.

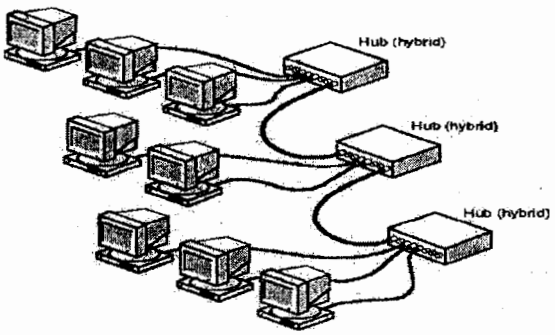
*Dạng hình sao (star topology)*: (Hình 1.4) Nối các trạm làm việc PC với một điểm trung tâm bằng một đoạn cáp riêng biệt. Điểm trung tâm chính là một "hộp nối" (hub), thực chất là một bộ xử lý dồn kênh. Nó được nối với một đoạn cáp tuyến tính dùng chung. Thông thường, mỗi hub có thể nối được từ 4 đến 24 máy. Cấu trúc này có ưu điểm là độ ổn định cao, dễ phát hiện lỗi, hoạt động của toàn mạng có tính an toàn cao, khi một đường dây nào hỏng thì chỉ có máy nối với đường dây đó không vào mạng được còn toàn mạng vẫn hoạt động bình thường. Việc mở rộng dễ dàng bằng việc chồng Hub. Đây cũng là cách nối phổ biến nhất hiện nay.

*Dạng nối vòng (ring topology)* (Hình 1.5) : Cũng giống như dạng hình sao, nó là tổ hợp các đoạn cáp riêng và dùng chung. Các đoạn cáp riêng tỏa ra từ một "bộ dồn kênh nối tâm" (central wiring concentrator). Các tín hiệu điều khiển được truyền từ trạm này tới trạm khác, theo một vòng kín. Vòng đó là một phần thiết kế logic của mạng cục bộ, nhưng về vật lý nó không biểu hiện. Mặt khác, cũng như trong dạng hình sao phân tán, các thông báo đều được truyền từ vị trí trung tâm đến các trạm. Phương pháp này có ưu điểm là tốc độ truy nhập cao, ít xảy ra đụng độ, tuy nhiên cấu trúc mạng phức tạp, việc quản lý mạng đòi hỏi cao hơn.

*Dạng hỗn hợp* : Thường được áp dụng trong những mạng LAN có phạm vi trải rộng trên một khu vực tương đối rộng. Ví dụ như trong một tòa nhà, một khu trường, các văn phòng của các Bộ, Ngành v.v. Một trong các dạng hỗn hợp đó là dạng Bus/Star. Với tôpô dạng này thường được áp dụng một đoạn cáp nối các switch/hub với nhau gọi là đường trục backbone và từ các hub tỏa ra các máy trạm được áp dụng cấu trúc dạng hình sao. Đối với các mạng thông thường người ta thường sử dụng các cáp đồng trục loại mỏng (thin coaxial cable) hoặc cáp đồng trục béo (thick coaxial cable) để kết nối đường trục Backbone (nối giữa các switch/hub). Tuy nhiên, khi yêu cầu tốc độ được quan tâm nhiều hơn, hoặc khi các tham số về khoảng cách giữa các máy trong LAN mà cáp đồng trục không đáp ứng được người ta thường sử dụng cáp sợi quang để nối đường trục backbone này. Ngày nay các dạng hay được áp dụng nhất là dạng hình sao và dạng hỗn hợp bus/star (hình 4.2).

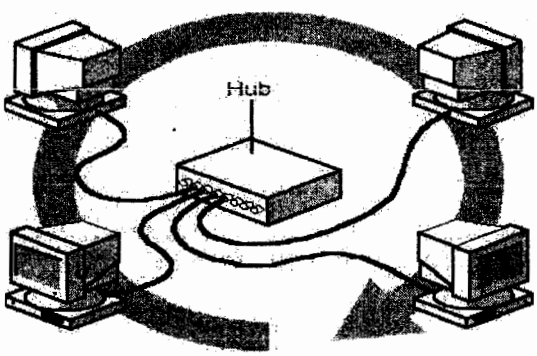
### Tôpô Lôgic

Ngoài việc xây dựng một tôpô vật lý, mạng còn có một tôpô lôgic mô tả đường truyền mà một tín hiệu phải theo trên mạng. Tầng nối kết dữ liệu của mô hình OSI sẽ điều quản tôpô lôgic. Tôpô vật lý và lôgic của một mạng cũng có thể giống hay khác nhau.




**Hình 4.2 Cấu hình kết hợp bus-star**

Token Ring là ví dụ điển hình nhất về một mạng có tôpô vật lý và lôgic khác nhau. Mỗi máy tính truyền các tín hiệu đến các trạm thu trên máy tính kế tiếp. Theo cách này, các tín hiệu di chuyển qua từng trạm trên hệ đấu cáp, cuối cùng hoàn tất cuộc hành trình trở về trạm đã phát chúng. Hãy nhớ lại, tôpô lôgic mô tả cách thức mà các tín hiệu di chuyển trên mạng. Ta có thể hiểu tại sao cắc mạng Token Ring lại có một tôpô vòng khâu lôgic.

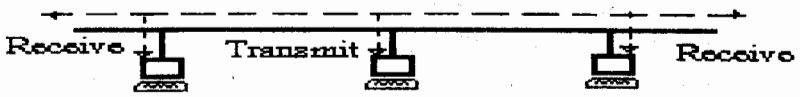



**Hình 4.3. Một vòng khâu logic dạng một hình sao vật lý.**

Tuỳ nhiên, các mạng Token Ring không hề được đấu dây vật lý trong các vòng khâu. Thay vì thế, người ta dùng các ổ cái, và mỗi máy tính được đấu cáp với ổ cái. Hình 4.3 nêu cách bố trí các máy tính và đường cáp. Lưu ý cách đấu các đường cáp trong ổ cái để phía trạm phát của máy tính nối với trạm thu của máy tính kế tiếp. Điều này giống hệt như mối quan hệ lôgic trong hình 4.3, và tôpô lôgic vẫn là một vòng khâu.

Tuy nhiên, do cách tổ chức mà từng máy tính được đấu cáp riêng lẻ với ổ cái, nên tôpô vật lý của Token Ring là một hình sao.

Ethernet đồng trục là một ví dụ về mạng trục ở đó mọi trạm được nối với mọi trạm khác trong một tôpô vật lý đa điểm. Ngoài ra, mọi trạm Ethernet truyền các tín hiệu đến mọi trạm khác, kết quả là một tôpô lôgic bus. Do đó, Ethernet đồng trục có một dạng bus vật lý và một bus lôgic (xem hình 4.4).




**Hình 4.4. Ethernet đồng trục vừa là BUS vật lý vừa là Logic**

Mạng Ethernet sủ dụng bộ tập chung HUB và cáp UTP (10 BASET-ta sẽ xem chi tiết ở mục sau) là một mạng vật lý hình sao đồng thời cũng là một bus lôgic.

## 4.2 Các phương pháp điều khiển truy nhập

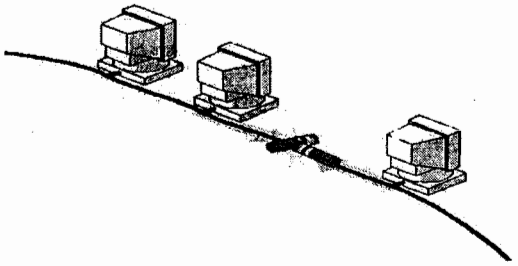
Mọi kênh vật tải chỉ có thể hỗ trợ mỗi lần một tín hiệu. Nếu hai máy tính truyền trên kênh cùng một lúc, các tín hiệu của chúng sẽ gây nhiễu cho nhau, cũng giống như âm nhiễu khi hai người nói cùng một lúc. Tính năng điều khiển truy cập vật tải sẽ điều khiển việc truy cập vật tải để không xảy ra sự cố gây nhiễu.

Đoạn này đề cập ba dạng điều khiển truy cập vật tải:

+ Tranh chấp
+ Chuyển thẻ bài
+ Sử lý ưu tiên theo yêu cầu

### 4.2.1 Phương pháp tranh chấp

Với dạng điều khiển truy cập gốc tranh chấp [contention-based access control], mọi máy tính đều có thể truyền bất kỳ lúc nào. Hệ thống bị hỏng khi hai máy tính gắng truyền cùng một lúc, trong trường hợp đó sẽ xảy ra một xung đột (xem hình 4.5). Cuối cùng, khi mạng quá bận, hầu hết các lần thử truyền đều dẫn đến xung đột, và việc truyền thông có thể kém hiệu quả.



**Hình 4.5 Xung đột trên cáp mạng**

Do đó, người ta thường thiết lập các cơ chế để giảm thiểu các hiệu ứng xung đột. Một trong những cơ chế đó là gửi sóng mang [carrier sensing], qua đó mỗi máy tính lắng nghe mạng trước khi thử truyền. Nếu mạng đang bận máy tính sẽ hoãn việc truyền cho đến khi mạng lắng dịu. Chiến lược đơn giản "nghe trước khi nói" này có thể giảm bớt đáng kể các xung đột.

Một cơ chế khác đó là phát hiện sóng mang [carrier detection]. Với chiến lược này, các máy tính tiếp tục kiểm tra mạng khi chúng truyền. Nếu máy tính phát hiện tín hiệu khác gây nhiễu tín hiệu mà nó đang gửi, nó sẽ ngưng truyền. Như vậy cả hai máy tính sẽ đợi trong một quãng thời gian ngẫu nhiên rồi gắng truyền lại. Trừ phi mạng thật bận rộn, kỹ thuật phát hiện xung đột cùng với kỹ thuật gửi song mang có thể quản lý một lượng phiên truyền lớn.

Cả hai cơ chế này được dùng chung với nhau để hình thành giao thức dùng trong tất cả các kiểu Ethernet, có tên CSMA/CD (Carrier Sense Multiple Access with collision Detection = đa truy cập gửi sóng mang có phát hiện xung đột)

Mạng LocalTalk của Apple dùng giao thức CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance sử dụng các kỹ thuật bổ sung để giảm bớt hơn nữa các khả năng xung đột.

Dưới đây tóm tắt các đặc tính của phương pháp điều khiển truy cập tranh chấp:

- Các hệ thống tranh chấp thuần tuý cho phép tất cả các trạm tiến hành phiên truyền tuỳ thích.
- Các va chạm luôn xảy ra tại một cấp nào đó trên các mạng gốc - tranh chấp, với số lượng gia tăng theo tỷ lệ thuận khi các phiên truyền gia tăng.
- CSMA/CD và CSMA/CA là hai giao thức giảm bớt sự tổn hại do các va chạm gây ra.

Trong phương pháp này thì nếu một trạm nào đó có nhu truy nhập vào bus thì trước hết nó phải " lắng nghe" xem trên bus có rỗi hay không. Nếu bus rỗi thì truyền dữ liệu đi, nếu bus bận (busy) nghĩa là trên bus đã có trạm khác đang truyền tin thì nó "chờ". Việc "chờ" theo các giải thuật sau đây:

- Trạm tạm thời ngừng truyền cho tới một thời gian ngẫu nhiên nào đó lại tiếp tục 'nghe' đường truyền. Ưu điểm là tránh được xung đột, nhược điểm là có thể có thời gian chết sau mỗi cuộc truyền.
- Trạm tiếp tục 'nghe' đến khi thấy đường truyền rỗi thì lại truyền dữ liệu đi với xác xuất bằng 1. Ưu điểm là tránh được thời gian chết, nhược điểm là khả năng xung đột cao.

➢ Trạm tiếp tục 'nghe' đến khi đường truyền rỗi thì truyền đi với xác xuất P xác định trước (0<P<1). Ưu điểm là khả năng xảy ra xung đột ít nhất, nhược điểm là phải lựa chọn P hợp lý để tránh cả thời gian xung đột và thời gian trễ.

Lý do xảy ra xung đột là do độ trễ truyền dẫn trên bus, cũng có thể có hai (hoặc nhiều hơn) trạm cùng kiểm tra và phát hiện môi trường truyền đang rỗi và chúng phát khung tin gần như đồng thời. Để khắc phục người ta dùng phương pháp CSMA/CD nghĩa là trong lúc truyền vẫn nghe để phát hiện xung đột. Thiết bị đầu tiên có phát hiện xung đột sẽ phát một tín hiệu đặc biệt (Jamming signal) để yêu cầu tất cả các thiết bị dừng việc phát dữ liệu. Các thiết bị sẽ đợi một thời gian ngẫu nhiên và sau đó phát lại.

Tuy bề ngoài các phương pháp tranh chấp có vẻ như không ổn do sự tổn hại mà các va chạm gây ra, song phương pháp tranh chấp (nhất là CSMA/CD) là phương pháp điều khiển truy cập vật tải phổ dụng nhất trên các LAN theo dạng Ethernet. Phương pháp CSMA/CD nói chung là một phương pháp khá đơn giản, do vậy Card mạng sử dụng phương pháp này khá rẻ. Phương pháp này phù hợp với các loại dữ liệu phát ngẫu nhiên (bursty) và kích thước khung tin nhỏ. Nhưng khi lưu lượng tăng thì số lần xung đột tăng và hiệu năng của mạng Lan giảm một cách đáng kể và do các va chạm xảy ra vào những lúc không ngờ, nên không có gì bảo đảm một máy tính nào đó sẽ có khả năng truyền vào một thời điểm nhất định. Các mạng dựa trên giải pháp này thường được mệnh danh là theo xác suất [probalistic] bởi cơ may mà một máy tính được phép truyền không thể đoán

### 4.2.2 Phương pháp chuyển thẻ bài

Phương pháp truyền thẻ bài [token passing] vận dụng một khung có tên là thẻ bài [token], luân chuyển quanh mạng. Một máy tính muốn truyền phải đợi cho đến khi nhận được khung thẻ bài, vào lúc này nó mới được phép truyền. Khi máy tính truyền xong, nó chuyển khung thẻ bài cho trạm kế tiếp trên mạng. Có vài chuẩn mạng sử dụng phương pháp điều khiển truy cập chuyền thẻ bài:

- Token Ring, được định nghĩa bởi chuẩn IEEE 802.5 được dùng phổ dụng nhất.
- Token bus (Chuẩn IEEE 802.4) cũng sử dụng phương pháp chuyền thẻ bài. Chuẩn này ít khi được thực thi.
- FDDI là chuẩn mạng sợi quang 100 Mbps dùng phương pháp chuyền thẻ bài và vòng khâu [rings] tương tự như Token Ring 802.5.

Ta xem nguyên tắc làm việc cụ thể của các phương pháp này

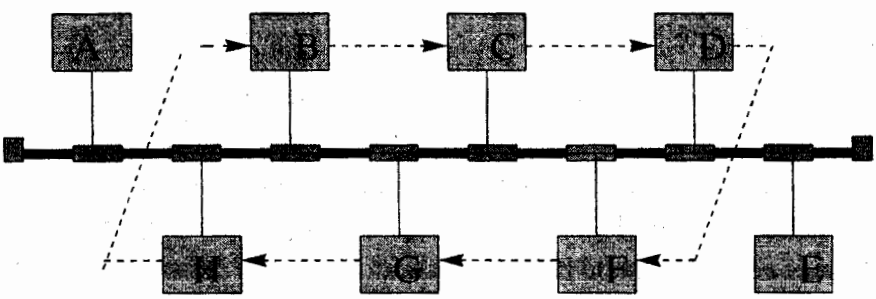
*Token bus* là phương pháp truy nhập đường truyền có điều khiển, token ở đây là một đơn vị dữ liệu đặc biệt có kích thước và nội dung gồm các thông tin điều khiển

được qui định riêng (Token). Một token được lưu chuyển trên vòng logic thiết lập bởi các trạm có nhu cầu truyền để cấp phát đường truyền mà ở đó vòng logic độc lập vớic87 vòng vt lý hực (Hình 4.6). Khi oken đến rạm nào hì rạm đó được quyền ruyền dữ liệu vào bus rong mộ khe hời gian xác định. Khi số liệu được ruyền hế hoặc hế khe hời gian qui định hì rạm đó phải chuyển oken đến rạm iếp heo só. Theo phương pháp này hì cần giải quyế mộ số vấn đề sau:

- Thiế lt p vòng logic gồm những rạm có nhu cầu ruyền số liệu, mỗi rạm được xác định heo mộ chuỗi hứ ự mà rạm cuối cùng sẽ nối với rạm đầu iên.
- Mỗi rạm phải biế địa chỉ của rạm ngay rước và kế sau nó.
- Các rạm không có nhu cầu ruyền hì nằm ngoài vòng logic và chúng có nhiệm vụ nhn dữ liệu.

Như vt y là vòng logic phải được hiế lt p rong rạng hái hực ế, nghĩa là cần có khả năng bổ xung thêm được hoặc loại bỏ một hay nhiều trạm ra khỏi vòng logic, quản lý việc đức vòng logic, trùng địa chỉ các trạm, khởi tạo lại vòng logic.v.v...

Để bổ xung thêm một trạm (hoặc nhiều trạm) vào vòng logic phải được định kỳ xem xét, nếu có nhu cầu truyền thì được nối vào vòng logic bằng cách khi chuyển token đi thì đồng thời gửi thông báo"tìm trạm đứng sau" để mời trạm có địa chỉ giữa nó và trạm kế tiếp nó có nhu cầu tham gia nhập vòng.




**Hình 4.6. Token bus**

——————— Đường truyền vật lý

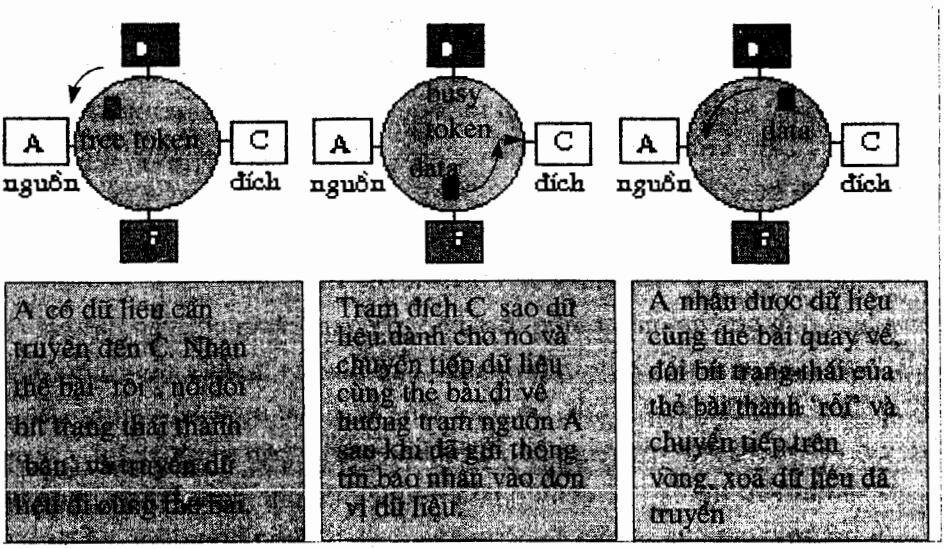
- - - - - - - - - - - - - - - Vòng logic

Khi một trạm gửi token đi nó phải giải quyết các tình huống sau để trách lỗi:

- Nghe xem trạm kế tiếp có làm việc không. Nếu không thấy làm việc thì phải tìm cách với qua trạm đó đến trạm tiếp theo để tránh đứt vòng logic.
- Nếu có một trạm nào đó cũng có thẻ bài thì nó chuyển sang trạng thái nghe bị động để chờ dữ liệu hoặc thẻ bài đến.

Việc khởi tạo lại vòng logic được thực hiện khi một hay nhiều trạm phát hiện trên bus mất token sau một khoảng thời gian định trước (gọi là Time out). Lúc đó trạm phát hiện sẽ gửi thông báo yêu cầu token đến trạm được chỉ định để lập một token mới.

*Token ring* sử dụng thẻ (token) để chiếm quyền được truyền. Một thiết bị trong vòng mạng chỉ được truyền dữ liệu khi nó có thẻ. Thẻ được truyền trong mạng vòng lần lượt từ thiết bị này đến thiết bị khác. Khi một thiết bị thu được thẻ, nó có thể truyền dữ liệu lên mạng nếu có, hoặc truyền thẻ cho thiết bị tiếp theo nếu không có dữ liệu cần truyền. Tuy nhiên việc truy nhập của mọi thiết bị đều được đảm bảo chứ không cầu may như phương pháp CSMA/CD.




**Hình 4.7 Hoạt động của mạng Token ring**

Khi một trạm muốn truyền dữ liệu, nó thu thẻ và gán thẻ này vào phần điều khiển (header) của khung tin và truyền đi trong vòng cho đến khi khung tin đến được đích. Sau đó, thẻ được trạm thu truyền vào vòng để đến trạm phát nhằm thông báo rằng khung tin đã đến đích. trạm phát sẽ tạo ra một thẻ mới và phát vào vòng. Trong một vòng lớn với các gói tin nhỏ, thời gian để trả lại thẻ vào vòng có thể lớn hơn nhiều so với thời gian truyền tin. Để tăng tính hiệu quả của token vòng phương pháp giải phóng thẻ sớm (early token vòng) được sử dụng. Thẻ được giải phóng ngay sau khi trạm phát xong một khung tin. Nếu trạm muốn phát nhiều hơn một khung tin, thì nó phải đưa thông tin ưu tiên vào khung tin thứ nhất, để yêu cầu được sử dụng tiếp thẻ. Các thiết bị khác có thể ghi đè thông tin ưu tiên này khi chúng thu và phát lại khung tin.

Sự phức tạp của phương pháp truy nhập dùng thẻ là ở chỗ nó phải được hệ thống quản lý. Trạm đầu tiên truy nhập vào vòng sẽ là thiết bị quản lý, mặc dù tất cả các trạm khác cũng có khả năng trở thành thiết bị quản lý. Hình 4.7. mô tả sự hoạt động của mạng token ring.

***Fiber Distributed Data Interface (FDDI):*** Phương pháp FDDI sử dụng phương pháp truy nhập dùng thẻ có định thời gian. Khi một thiết bị có thẻ, nó có thể giữ thẻ trong một thời gian nhất định, thời gian này do người quản trị mạng đặt thông qua trạm quản lý (Station management- SMT). Trong vòng FDDI có thể có nhiều hơn một khung tin bởi vì thiết bị truyền giải phóng thẻ trong khi các khung của nó vẫn chạy trong vòng. Có 2 chế độ truy nhập trong FDDI: dị bộ và đồng bộ. Chế độ dị bộ là phương pháp truyền ngẫu nhiên. Chế độ này phù hợp với truyền dữ liệu, nhưng không phù hợp với các dịch vụ nhạy cảm với thời gian thực như video chẳng hạn. Các card mạng FDDI đồng bộ cho phép người quản trị mạng giành một phần cố định giải thông cho các thiết bị có thông tin nhậy cảm với thời gian. Phần giải thông còn lại sẽ được thiết bị khác chia sẻ bằng chế độ dị bộ.

**So sánh phương pháp tranh chấp và chuyền thẻ bài.**

Với tư cách là một cơ chế điều khiển truy cập, phương pháp chuyền thẻ bài dường như có vẻ trội vượt hơn phương pháp tranh chấp. Tuy nhiên, ta thấy rằng cho đến nay Ethernet vẫn là chuẩn LAN thống lĩnh, nó đã chứng tỏ được sự xuất chúng của mình trong khi phối hợp chặt chẽ với phương pháp điều khiển truy cập tranh chấp.

Phương pháp chuyền thẻ bài yêu cầu phải có nhiều cơ chế điều khiển phức tạp thì mới làm việc tốt. Phần cứng của phương pháp này cũng đắt tiền hơn đáng kể so với các cơ chế tranh chấp. Do các mạng chuyền thẻ bài được thiết kế với độ tin cậy cao, nên việc xây dựng các khả năng chẩn đoán và chỉnh sự cố mạng vào trong phần cứng mạng là lẽ đương nhiên. Điều này lại càng làm tăng chi phí của các mạng chuyền thẻ bài. Chúng ta phải quyết định có nên bỏ thêm chi phí để đổi lấy độ tin cậy bổ sung đó hay không. Trái lại, tuy các mạng chuyền thẻ bài thực hiện tốt hơn các mạng gốc-tranh chấp khi gặp các lượng lưu thông cao, song các mạng tranh chấp lại có khả năng vận hành vượt trội dưới các điều kiện mức tải nhẹ. Tiến trình chuyền thẻ bài vòng quanh (và các tác vụ bảo trì khác) đã ăn lấn vào băng thông xẵn có. Kết quả là, một Ethernet 10Mbps và một Token Ring 16-Mbps thực hiện gần tương đương nhau dưới các điều kiện mức tải nhẹ, trong khi giá thành của Ethernet lại thấp hơn nhiều.

### 4.2.3 Phương pháp truy nhập ưu tiên theo yêu cầu

Đây là một phương pháp điều khiển truy cập sử dụng một thiết bị trung tâm để điều tiết toàn bộ việc truy cập mạng. Nó là phương pháp điều khiển truy cập phổ dụng nhất trên các mạng máy tính lớn.

Thiết bị trung tâm, có tên là thiết bị chính [primary], sẽ yêu cầu dữ liệu từ các thiết bị khác trên mạng, có tên thiết bị thứ cấp [Secondaries]. Nó sẽ quét các cổng để tìm ra thiết bị có nhu cầu truyền dữ liệu. Thiết bị trung tâm cho phép truy nhập dựa trên mức ưu tiên và vị trí của cổng trong vòng quét. Mỗi thiết bị chỉ được phép truyền truyền một khung tin trong một vòng quét.

Phương pháp truy nhập ưu tiên theo yêu cầu (Demand Priority Protocol- DPP) bảo đảm mỗi thiết bị đều được quyền truy cập mạng một cách hợp lý và tỏ ra thích hợp khi dùng với dữ liệu quan trọng về thời gian. Thực tế, kỹ thuật truy nhập ưu tiên theo yêu cầu mang nhiều ưu điểm của phương pháp chuyển thẻ bài, như:

- Truy nhập theo định kỳ
- Gán được các mức ưu tiên
- Tránh được các va chạm

Một điểm khác biệt quan trọng giữa phương pháp này và chuyển thẻ bài đó là: kỹ thuật Demand Priority tập trung hóa quyền điều khiển, tính năng tập trung này có thể là một ưu điểm theo góc nhìn quản lý, song sự cố lại có tiềm năng xảy ra tập trung tại chỉ một điểm. Nếu cơ chế điều khiển trung tâm bị hỏng, mạng sẽ ngưng hoạt động. Phương pháp chuyển thẻ bài sử dụng các chức năng điều khiển phân phối hơn do đó ít bị hỏng tập trung tại một điểm.

Do phương pháp truy nhập ưu tiên theo yêu cầu tập trung điều khiển, nên các thiết bị thứ cấp không thể truyền thông trực tiếp với các thiết bị thứ cấp khác. Thay vì thế, chúng phải dùng thiết bị chính làm trung gian. Vả lại, do thiết bị chính phải quyết hỏi từng thiết bị thứ cấp-bất kể thiết bị thứ cấp có dữ liệu để truyền hay không-nên tiến trình quét hỏi cũng lãng phí các lượng băng thông lớn. Điều này có thể dẫn đến các độ trễ quá mức khi có vài thiết bị thứ cấp đợi trong lúc các thiết bị khác đang được dò báo.

## 4.3 Mạng Ethernet

Thoạt đầu, Ethernet được phát triển bởi các hãng Xerox, Digital, và Intel vào đầu những năm 1970. Hiện nay Ethernet trở thành cấu trúc mạng LAN thông dụng nhất trên thế giới. Ethernet dùng phương pháp truy cập tranh chấp CSMA/CD, nó tuân theo định chuẩn IEEE 802.3 và hỗ trợ tốc độ truyền dữ liệu trên mạng từ 10-100 Mbps.

Ethernet chủ yếu sử dụng băng tần cơ sở và có dạng hình trục hoặc hình sao. Ethernet thường được dùng trên các mạng có lượng lưu thông nhẹ đến trung bình.

Card Ethernet có thể có một, hai, hoặc có thể có ba đầu nối dưới đây:

➢ Các đầu nối BNC hỗ trợ cáp đồng trục.

➢ Các đầu nối RJ45 hỗ trợ hệ cáp 10BASET (UTP).

➢ Các đầu nối DIX được dùng để nối các bộ thu phát bên ngoài.

Giới hạn 1,024 nút (các địa chỉ vật lý) cho mỗi địa chỉ mạng vẫn tồn tại trên mạng Ethernet. Các địa chỉ được IEEE gán cho hãng kinh doanh theo ba byte đầu của một địa chỉ gồm sáu byte. Hãng kinh doanh chịu trách nhiệm việc gán phần còn lại của địa chỉ và đảm bảo các ID duy nhất.

Các kiểu khung Ethernet

Để có thể truyền thông tin thành công qua mạng Ethernet, các nút mạng gửi và nhận phải thoả thuận trước về cấu trúc của thông tin sẽ truyền. Nút gửi phải tổ chức thông tin theo cách thức trật tự và có thể tiên đoán được để nút nhận có thể tìm và diễn dịch thông tin được truyền. Cách bố trí thông tin theo trật tự di chuyển qua một mạng Ethernet được xem là khung Ethernet (Ethernet frame –hình 4.8).

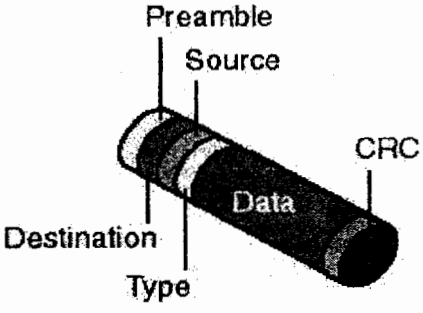
Các kiểu khung Ethernet khác nhau mô tả các chuẩn khác nhau để chỉ định cấu trúc giao thức. Hiện có bốn kiểu khung Ethernet. Cùng kiểu khung Ethernet phải được nạp trên cả hệ phục vụ và các hệ khách truy cập thì phiên truyền thông đúng đắn mới có thể diễn ra. Bốn kiểu khung sẵn có là

- ETHERNET 802.3 ( còn gọi là ETHERNET thô),
- ETHERNET 802.2,
- ETHERNET SNAP,
- ETHERNET II.

ETHERNET thô ( 802.3 ) đã được phát triển trước khi chuẩn IEEE 802.3 được hoàn thành và công bố. ETHERNET 802.3 không dành một trương để chỉ định các giao thức có thể chứa trong gói tin. Do thiếu trường này, nên ETHERNET 802.3 đã thành một sản phẩm hầu như đặc thù của riêng hệ điều hành NetWare 2.2 và NetWare 3.x của Novell. Các tính năng chung của chuẩn ETHERNET 802.3 bao gồm:

- Một kích cỡ khung giữa 64 và 1,518 byte.
- Một lời tựa trong dòng đầu tiên của phần đầu (nó chứa các số 1 và 0 thay thế để đồng bộ hoá các trạm truyền thông).
- Một trường SFD (Start Frame Delimiter - dấu định biên khởi đầu khung) chỉ định đầu khung tin.
- Một trường sáu byte chỉ định địa chỉ của trạm mà gói tin đang được gửi tới.

- Một địa chỉ phát sinh nêu rõ hệ khách; hệ phục vụ, hoặc bộ định tuyến nơi gửi gói tin lần chót.
- Một trường hai byte chỉ định chiều dài phần dữ liệu của gói tin, và chiều dài không được lớn hơn 1,500 byte.
- Một trường dữ liệu phải dài hơn 46 byte và ngắn hơn 1,500 byte.
- Một Cyclical Redundancy Check (CRQ) hoặc Frame Check Sequence bốn byte, giúp đảm bảo dữ liệu truyền hợp lệ.




**Hình 4.8 Một dạng khung ETHERNET II**

ETHERNET 802.2 tuân thủ đầy đủ chuẩn IEEE 802.3. Nó kiểu khung ngầm định được dùng trong các mạng NetWare 3.12 và NetWare 4. x. Các tính năng chung của chuẩn ETHERNET 802.2 là:

- Tất cả các trường đều giống với định chuẩn 802.3
- Ba trường bổ sung Logical Link Control ( LLC ), dài một byte, tác động như một phần đầu 802.3
- Một kích cỡ khung giữa 64 và 1,518 bytes
- ETHERNET SNAP ( SupNetwork Address Protocol - giao thức địa chỉ mạng con) tuân thủ đầy đủ chuẩn ETHERNET 802.2 và thực tế được xem một bản tăng cường cho định chuẩn 802.2. Các tình năng chung của chuẩn ETHERNET SNAP là:
- Hai trong số các trường LLC, chứa dữ liệu cố định nêu rõ một gói tin SNAP

Một trường LLC thứ ba được xem như trường kiểu, cho phép gói tin tải các giao thức cấp cao khác nằm trong cấu trúc khung, do đó bảo đảm tính tương thích và các hệ điều hành mạng có thể tải các giao thức trên các kiểu vật tải khác, như Token Ring.

Các kiểu khung ETHERNET II hỗ trợ TCP/IP. Các tính năng chung của kiểu khung ETHERNET II (hình 4.8) là:

- Một trường Preamble để chỉ sự bắt đầu của khung tin.
- Một trường sáu byte chỉ địa chỉ của trạm đích mà gói tin được gửi tới.

- Một trường sáu byte chỉ định địa chỉ của trạm nguồn mà gói tin được gửi đi.
- Một trường kiểu gói tin nằm ngay sau trường địa chỉ nguồn, là vị trí của trường chiều dài gói tin trong khung và giao thức mạng sử dụng của gói tin như IP, IPX..
- Một trường dữ liệu phải dài từ 46 - 1,500 byte.
- Một Cyclical Redundancy Check (CRC) để kiểm tra dữ liệu truyền hợp lệ.

Bảng 4.1 mô tả một ví dụ cụ thể về một khung tin Ethernet theo chuẩn ETHERNET II. Trường "type" 0x0800 chỉ ra gói tin theo giao thức IP packet và đưa vào ghép nối (Ethernet frame).

Mặc dù có sẵn bốn kiểu khung ETHERNET, chỉ nên nạp kiểu khung cần dùng trên hệ máy mạng.

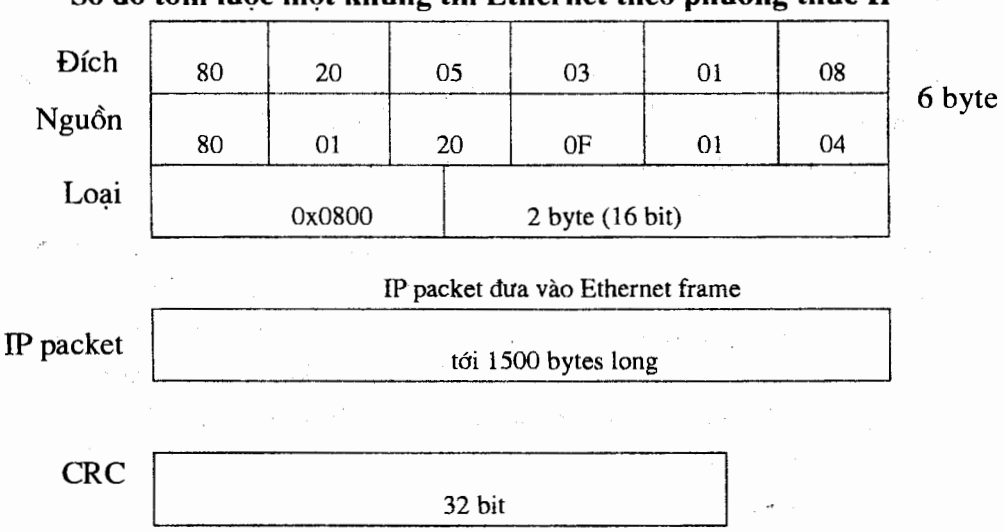
Sau đây sẽ xem xét một số định chuẩn của mạng Ethernet:

**10BASE2**

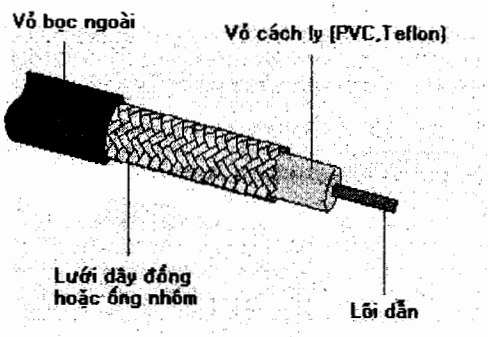
Tôpô cáp 10BASE2 (Thinnet- cáp gầy) thường dùng bộ thu phát cài sẵn trên card mạng (NIC) để điều khiển các tín hiệu vào/ra trên mạng. Hệ cáp Thinnet có thể dùng loại cáp đồng trục RG-58A/U hoặc RG-58C/U (hình 4.9), Một đặc tính của kiểu đấu cáp này là các đầu cáp phải được kết thúc bằng một đầu nối đặc biệt có tên là đầu kết [terminator]. Đầu kết có gắn một điện trở khớp với đặc tính của cáp 50 Ohms. Điện trở này ngăn cấm các tín hiệu một khi đến cuối cáp sẽ không nẩy ngược lại và gây nhiễu. Đầu nối T – connetor (hình 4.10) gắn trực tiếp vào đầu nối BNC trên NIC. Phải dùng một đầu kết nối mát trên một đầu của phân đoạn mạng.

Bảng 4.1

**Sơ đồ tóm lược một khung tin Ethernet theo phương thức IP**



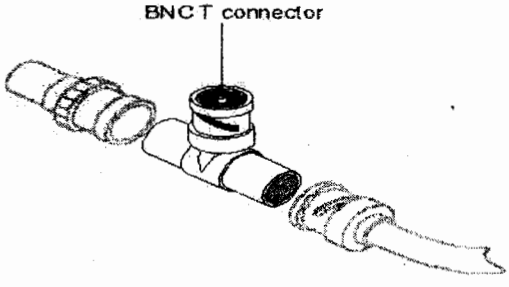
Bộ thu phát là một thiết bị nhận tín hiệu số hoá từ nút và phiên dịch nó để truyền thông trên hệ cáp rải tần cơ sở. Các NIC hỗ trợ cáp Thinnet hoặc 10BASE-T thường gắn sẵn các bộ thu phát. Các bộ thu phát bên ngoài được dùng cho Thick Ethernet mặc dù cũng có thể dùng nó cho Thinnet và UTP.




**Hình 4.9 Cáp đồng trục gầy RG-58 A/U b**

Các Ưu điểm củ2 10BASE

Giá cả là ưu điểm chính củ2 việc dùng 10BASE . Thường được sử dụng khi một phân đoạn cáp bất kỳ trên mạng không phải chạy x2 hơn 185 mét, 10BASE cũng tương đối đơn giản khi nối. Mỗi nút mạng nối trực tiếp với cáp mạng bằng một đầu nối T gắn với NIC.




**Hình 4.10 Đầu nối T-BNC connector**

Để trách sự cố trên mạng 10BASE t2 phải tuân thủ các quy tắc dùng 10BASE . như s2u:

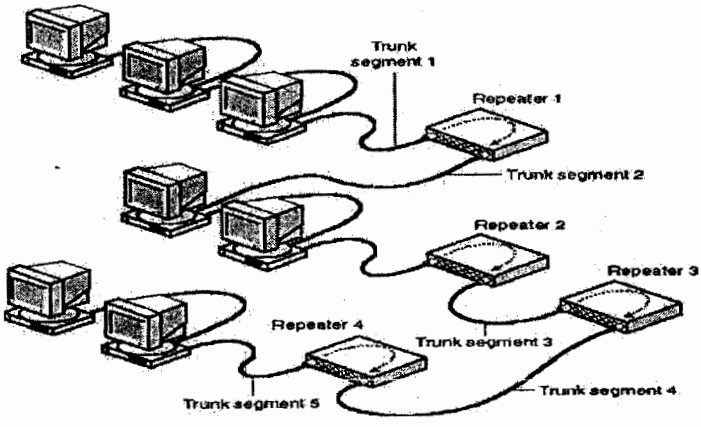
- ➢ Khoảng cách cáp tối thiểu giữ2 các máy tính phải là 0.5 mét.
- ➢ Đầu nối T phải được nối trực tiếp với NIC.
- ➢ Không thể vượt quá giới hạn phân đoạn mạng tối đa là 185 mét.
- ➢ Tổng thể sơ đồ đấu cáp mạng không thể vượt quá 925 mét.

➢ Số nút tối đa trên mỗi phân đoạn mạng là 30 (quy định này gồm tất cả các máy tính và các bộ truyền lặp).

➢ Một đầu kết terminator 50 ohm phải được dùng trên từng đầu của các bus, với chỉ một trong các đầu kết đấu mát hoặc có đây mát gắn nó với đinh ốc giữ vỏ ổ cắm điện.

➢ Mỗi mạng không thể có trên năm phân đoạn. Các phân đoạn có thể nối tối đa *bốn bộ truyền lặp, và chỉ ba trong số năm phân đoạn có thể có các nút mạng – Người ta* thường gọi qui tắc này là qui tắc 543 (hình 4.11).

Chuẩn IEEE 802.3 của Thinnet là 10BASE2. Chuẩn này mô tả một mạng dải tần cơ sở 10Mbps, có chiều dài phân đoạn tối đa khoảng 200 mét (giới hạn thực tế, như đã nêu là 185 mét).



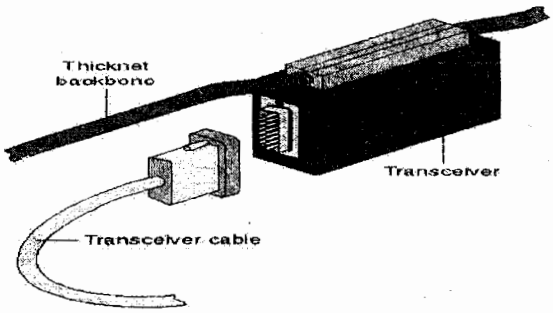

**Hình 4.11 Mạng 10BASE2 với 5 đoạn (Segment)-10BASE5**

Tôpô cáp 10BASE5 (Thicknet-Cáp béo) dùng một bộ thu phát bên ngoài để gán với card giao tiếp mạng (xem Hình 4.12). NIC gắn với bộ thu phát bên ngoài thông qua cáp Attachment Universal Interface (AUI) đấu vào đầu nối DIX trên lưng card. Bộ thu phát bên ngoài sẽ ngoạm chặt cáp Thicknet. Cũng như Thinnet, mỗi phân đoạn mạng cũng phải được kết thúc tại cả hai đầu, có một đầu dùng đầu kết nối mát. Hình 4.13 có nêu các thành phần của một mạng Thicknet.

Ưu điểm chính của 10BASE5 là khả năng vượt quá các hạn chế cáp ứng dụng cho 10BASE2. Tuy nhiên, nó cũng đặt ra các hạn chế cho riêng mình, mà ta cần phải xem xét khi cài đặt hoặc chỉnh sự cố một mạng 10BASE5.

Cũng như các mạng 10BASE2, cân nhắc đầu tiên khi cài đặt một mạng 10BASE5

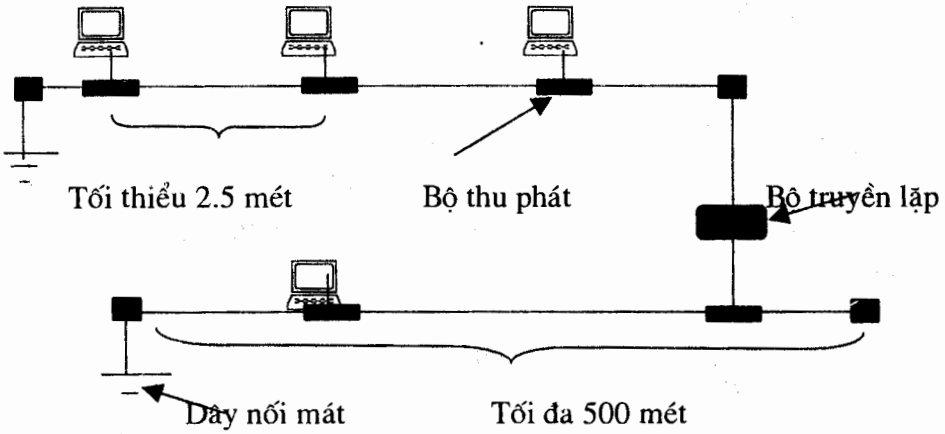
chính là các nguyên tắc chỉ đạo và các quy tắc đấu cáp đã thiết lập.




**Hình 4.12. Bộ thu pháp bên ngoài của 10BASE5**

Có vài nguyên tắc bổ xung, cùng với quy tắc 543, phải được tuân thủ trong các mạng Think Ethernet:

- Khoảng cách cáp tối thiểu giữa các bộ thu phát là 2.5 mét.
- Không được quá chiều dài phân đoạn mạng tối đa là hoặc 500 mét
- Toàn bộ sơ đồ đấu cáp mạng không thể vượt quá 2,500 mét
- Một đầu của phân đoạn mạng có kết thúc phải được nối mát
- Các đoạn nối từ bộ thu phát tới NIC có thể ngắn theo yêu cầu, nhưng không thể dài hơn 50 mét .
- Các phân đoạn cáp được cắt và nối bằng " mối ngoạm "[Vampire Tap] phải xuất xứ từ chung một cuộn cáp để bảo đảm từng đoạn nối sẽ tải hệ cáp điện đồng nhất với đoạn kia.
- Số nút tối đa cho mỗi phân đoạn mạng là 100. ( Bao gồm tất cả các máy tính và các bộ truyền lặp ).




**Hình 4.13. Hai phân đoạn dùng hệ cáp 10 BASE5**

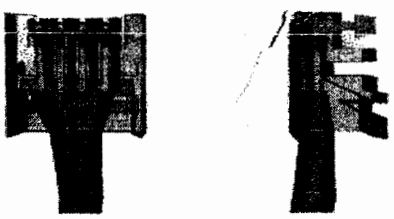
10BASE5 đòi hỏi cáp có trở kháng 50 ohm. Cáp RC-8 và RCA-11, 50-ohm được dùng với Ethernet-10BASE5

Chuẩn IEEE 802.3 của Thicknet là 10 BASE5. Chuẩn này mô tả một mạng dài tần cơ sở 10 Mbps, có thể có các phân đoạn dài tới 500 mét. Có thể phối hợp cáp Thinnet và Thicknet để mở rộng khoảng cách của tôpô mạng Ethernet.

**10 BASE-T**

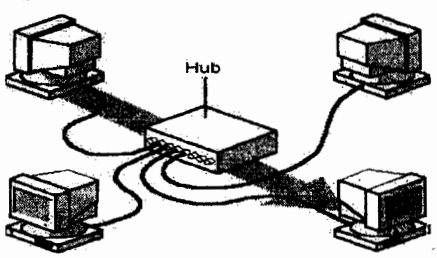
Xu hướng đấu dây các mạng Ethernet đó là dùng cáp xoắn cặp trần (UTP ). Cáp UTP hoặc 10 BASE-T là một trong ba thực thi phổ dụng nhất của Ethernet. Nó dựa trên chuẩn IEEE 802.3. Cáp UTP không có màng chắn tết bím. Các cặp dây này thường được mã hoá màu để phân biệt các cặp dây (hình 4.14).

Có vài lý do khiến cáp xoắn cặp trở thành phổ dụng, song lý do quan trọng nhất vẫn là giá thành thấp. Cáp xoắn cặp vừa rẻ tiền khi cài đặt vừa có mức chi phí thấp nhất trong mọi loại cáp. Một sợi cáp xoắn cơ bản bao gồm hai sợi dây đồng xoắn với nhau. Các vòng xoắn là phần quan trọng trong đặc tính của cáp xoắn cặp. Kỹ thuật xoắn làm giảm bớt độ nhạy của cáp đối với EMI và cũng giảm bớt xu hướng để cáp bức xạ gây nhiễu tần số radio gây nhiễu các thành phần điện tử và các đường cáp lân cận. Các tín hiệu bị bức xạ từ các sợi dây xoắn có khuynh hướng khử nhau. (Các ăng ten, được thiết kế nhằm bức xạ các tín hiệu tần số radio, bao gồm các sợi dây song song, chứ không phải xoắn).



**Hình 4.14 Cáp UTP và đầu nối RJ 45**

Hệ cáp 10 BASE-T được đấu dây theo tôpô hình sao. Nó vận hành theo lôgic, giống như một bus tuyến tính. Cáp dùng các đầu nối RJ 45 để nối giữa card giao tiếp mạng (có các giắc cắm RJ 45 cài sau lưng card) với các ổ cắm RJ 45 của một bộ tập trung [hub] (hình 4.15).




**Hình 4.15 Cấu hình 10BASET**

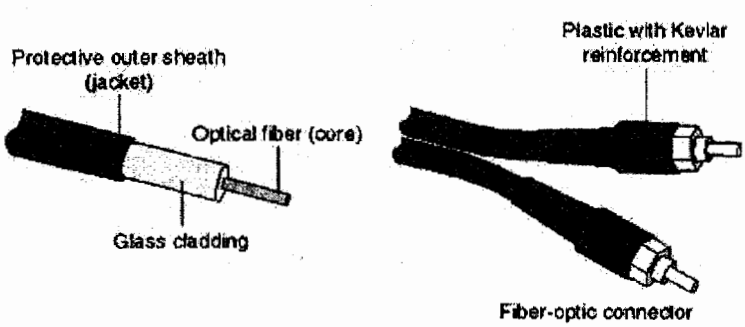
Hệ đấu dây hình sao của 10 BASE-T có vài ưu điểm, nhất là trong các mạng lớn. Trước tiên, mạng đáng tin cậy hơn và dễ quản lý hơn bởi các mạng 10 BASE-T dùng bộ tập trung Hub. Các Hub "thông minh" ở chỗ chúng định tuyến trao đổi dữ liệu trên mạng vòng qua một phân đoạn cáp bị hỏng và có thể phát hiện các phân đoạn cáp hỏng. Điều này tạo thuận lợi cho việc định vị và sửa chữa các phân đoạn cáp bị hỏng. 10 BASE-T cho phép thiết kế và xây dựng từng phân đoạn trên LAN, dễ ràng tăng số máy khi mạng cần nâng cấp thêm. Như vậy, 10 BASE-T linh hoạt hơn các khả năng đấu cáp khác trên LAN.

Khi thiết kế một mạng 10 BASE-T phải tuân thủ các quy tắc sau:

- Số lượng tối đa các máy tính trên mạng là 1,024
- Hệ cáp được dùng phải là 8 sợi (4 đôi) thuộc loại UTP 3,4 hoặc 5 và có mức trợ kháng là 85 đến 115 ohms, ở 10 MHz.
- Số nút tối đa là 512, và chúng có thể nối vào ba phân đoạn bất kỳ, với năm là số phân tuyến tối đa sẵn có.
- Chiều dài tối đa của phân đoạn cáp từ NIC tới Hub là 100 mét. Nếu tăng thêm độ dài của đoạn cáp ta phải dùng thêm bộ lặp

Theo EIA/TIA-568B RJ-45 sơ đồ đấu nối giữa cáp UTP 4 đôi và đầu nối RJ 45 được mô tả như sau:

| | |
|---|---|
| - Đôi 2 được nối với chốt 1 và 2 đầu nối RJ 45: | |
| + Chốt 1 bắt vào dây có màu: | Trắng/Da cam |
| + Chốt 2 bắt vào dây có màu: | Da cam |
| - Đôi 3 được nối với chốt 3 và 6 đầu nối RJ 45: | |
| + Chốt 3 bắt vào dây có màu: | Trắng/Xanh lá cây |
| + Chốt 6 bắt vào dây có màu: | Xanh lá cây |




**Hình 4.16 Cấu trúc cáp quang**

**10BASEFL**

Đây là chuẩn mạng Ethernet do IEEE ban hành qui định việc sử dụng cáp quang (Fiber-optic hình 4.16) cho việc đấu nối giữa các máy tính trên mạng vẫn trên nền tốc độ chuẩn 10 Mbps và sử dụng băng tần cơ sở. Lý do chính để sử dụng mạng 10BASEFL tăng khoảng cách kết nối giữa các máy tính hoặc các bộ lặp (đặt tại các toà nhà khác nhau) trong mạng. Khoảng cách tối đa cho một phân đoạn mạng 10BASEFL là 2000 mét.

**Các chuẩn mạng 100-Mbps (IEEE Standards)**

Do nhu cầu phát triển của thông tin, nhiều loại hình mới yêu cầu băng thông rộng và tốc độ truyền dữ liệu cao trên mạng như : Truyền ảnh , Video, hệ thống lưu trữ văn bản lớn, hệ thống trợ giúp thiết kế CAD-CAM... Các chuẩn mạng Ethernet mới ra đời với tốc độ 100 Mbps nhằm bù đắp hạn chế về tốc độ của các mạng Ethernet truyền thống 10 Mbps. Hai chuẩn mới hiện đang có nhu cầu sử dụng cao là:

- 100BaseVG-AnyLAN Ethernet.
- 100BaseX Ethernet (Fast Ethernet- Ethernet tốc độ cao).

Cả hai loại này đều tương thích với với hệ thống đấu cáp của chuẩn 10BASET, điều đó có nghĩa chúng cho phép nâng cấp trên nền hệ thống 10BASE-T đã tồn tại cũ.

**100VG-AnyLAN**

Mạng 100VG-AnyLAN sử dụng cộng nghệ mạng trộn giữa kiến trúc Ethernet và Token ring. Ban đầu nó được phát triển bởi công ty Hewlett-Packard và hiện nay được định nghĩa lại trong chuẩn IEEE 802.12, nó qui định các chuẩn cho việc truyền các khung tin 802.3 Ethernet và gói tin 602.5 token ring. Nó có các kiểu tên gọi khác nhau như sau: 100VG-AnyLAN , 100BaseVG, VG, AnyLAN.

Các đặc trưng của 100VG-AnyLAN như sau:

- Tốc độ tối thiểu của mạng 100 Mbps.
- Cấu trúc tôpô vật lý hình sao, cáp đấu nối có thể dùng UTP loại 3,4,5 hoặc cáp quang đấu nối tới HUB trung tâm. Trong câu hình này HUB và Cạc mạng phải là loại chuyên dụng dùng riêng cho 100VG-AnyLAN.
- Cho phép sử dụng cả phương thức truy nhập ưu tiên theo nhu cầu cho hai mức ưu tiên thấp và cao.
- Tại HUB có cung cấp khả năng lọc địa chỉ khung tin để tăng khả năng bảo vệ riêng của người sử dụng mạng.
- Hỗ trợ cả khung Ethernet và gói tin của mạng Token ring (Ta sẽ đề cập đến ở phần sau)
- Chiều dài tối đa của phân đoạn cáp từ NIC tới Hub là 250 mét.

**100BaseX Ethernet**

Chuẩu này thường gọi Ethernet tốc độ cao. Đây là chuẩn bổ xung cho các chuẩn Ethernet hiện hành, nó sử dụng cáp UTP hoặc STP theo phương thức truy nhập CSMA/CD trong cấu trúc hình sao (vật lý) - Bus (Logích) tương tự như 10BASET tất cả các cáp đều được nối tới Hub, tốc độ mạng 100 Mbps, sử dụng băng tần cơ sở.

100BaseX có ba loại hình chính:

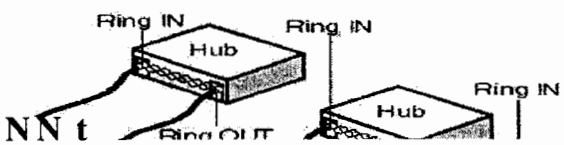
- 100BaseT4 ( Sử dụng cáp 4-đôi loại 3, 4, hoặc 5 UTP)
- 100BaseTX (Sử dụng cáp 2-đôi loại 5 UTP or STP- tương tự UTP có thêm màng chắn kim loại)
- 100BaseFX (Cáp quang 2-nhánh fiber-optic cable).

## 4.4 Mạng Token ring

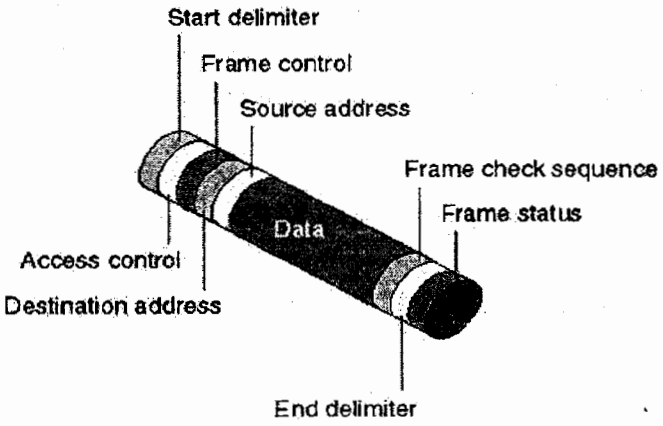
Token Ring dùng kiến trúc chuyền thẻ bài tuân thủ chuẩn IEEE 802.5. Xét về vật lý, tôpô theo cấu hình sao, song về lôgic lại dùng một vòng khâu để chuyền thẻ bài từ trạm này sang một trạm khác. Mỗi nút phải được gắn với một bộ tập kết có tên MSAU hoặc MAU ( multistation access unit = bộ truy cập đa trạm ). Như hình 4.17 các MAU thường có 10 đầu nối, 8 trong số này chấp nhận các cáp đến các máy trạm hoặc máy chủ, các đầu nối khác được gán nhãn RI ( ring in = vòng đến ) và RO (ring out = vòng ra). Các đầu nối RI và RO được dùng để nối nhiều MAU tạo thành các mạng lớn hơn.

Card giao tiếp mạng Token Ring có thể chạy ở mức 4 Mbps hoặc 16 Mbps sử dụng băng tần cơ sở. Card 16 Mbps có thể được cấu hình để chạy ở mức 4 hoặc 16 Mbps. Tất cả các card trên một vòng khâu mạng nhất định phải đang chạy cùng tốc độ.

**MAU**




**Hình 4.17 Đấu nối giữa các MAU trong cấu hình Token ring**




**Hình 4.18 Cấu trúc khung tin của token ring**

Cấu trúc khung tin trong Token ring được biểu diễn ở hình 4.18, các trường cụ thể được mô tả ở bảng 4.2

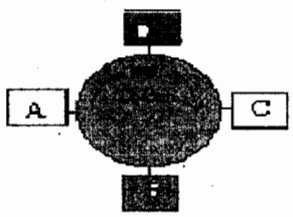
Bảng 4.2

**Các trường cụ thể**

| *Tên trường* | *Mô tả* |
|---|---|
| Start delimiter | Báo bắt đầu khung tin. |
| Access control | Chỉ báo mức ưu tiên của khung tin và loại khung là thẻ bài hay là một khung. |
| Frame control | Chứa các thông tin truy nhập điều khiển dùng cho tất cả các máy tính trên mạng hoặc các thông tin riêng cho một máy cụ thể. |
| Destination address | Địa chỉ máy nhận gói tin. |
| Source address | Địa chỉ máy gửi gói tin. |
| Information, or data | Dữ liệu gửi trên mạng. |
| Frame check sequence | Thông tin kiểm tra lỗi CRC |
| End delimiter | Báo kết thúc khung tin |
| Frame status | Thông báo trạng thái gói tin đã được nhận, bản sao (copied) hoặc đang đến đích. |

Mỗi nút trong mạng Token ring đều tác động như một bộ truyền lặp nhận thẻ bài và các khung dữ liệu từ láng riềng gần nhất NAUN (nearest active upstream neighbor). Sau khi nút xử lý một khung, khung sẽ truyền xuôi tiếp đến nút gắn kế cận. Khi một nút nhận được một khung đúng địa chỉ của mình nó sẽ sử lý số liệu gửi kèm và thay đổi 2 bit trong trường trạng thái của khung báo là dữ liệu đã được đọc bởi nó và nó sẽ gửi khung này đi tới nút kế tiếp sau. Mỗi khung tin thực hiện ít nhất một chuyến lưu chuyển quanh hết vòng khâu. Sau đó, trở về nút phát sinh, tại đây nút gửi nhận ra rằng khung dữ liệu đã được đọc thành công và không gửi tiếp khung này đi một lần nữa nó sẽ giải phóng thẻ bài cho nút sau nêu không có nhu cầu truyền dữ liệu tiếp. Các trạm làm việc có vấn đề sẽ gửi một " phao tiêu" để định danh một địa chỉ của sự cố tiềm ẩn. (hình 4.18)

Cũng như các NIC Ethernet, địa chỉ nút trên từng NIC Token được cài đặt tại nhà chế tạo và duy nhất cho từng card. Trong vài trương hợp, địa chỉ nút có thể bị ghi đè bởi các chỉ lệnh phần mềm. Có thể cài đặt tối đa hai card Token Ring trong một nút bất kỳ và được định nghĩa. là chính hay dự phòng trong máy.




**Hình 4.18. Hoạt động của một Token Ring**

*Hệ cáp Token Ring*

Các mạng Token Ring truyền thông dùng cáp xoắn cặp có màng chắn. Dưới đây là các kiểu cáp IBM chuẩn của Token Ring:

- Loại 1. Một màng chắn tết bím bao quanh hai cặp dây đồng đặc xoắn. Loại 1 được dùng để nối các trạm cuối với các panel phân phối cáp, hoặc nối giữa các tủ đấu dây khác nhau nằm cùng toà nhà. Loại 1 sử dụng hai STP thuộc loại 22 AWG lõi đặc để dùng cho các phiên truyền cấp dữ liệu cao và dài bên trong các bức tường của toà nhà.
- Loại 2. dùng tổng cộng sáu cặp xoắn: hai cặp là STP (để nối mạng), bốn cặp là UTP (cho các hệ điện thoại). Cáp này được dùng cho cùng mục tiêu như Loại 1, song cho phép gộp cả cáp tiếng lẫn dữ liệu vào chỉ một đoạn chạy cáp.
- Loại 3. Loại 3 có cặp dây đồng xoắn trần với tối thiểu hai vòng xoắn/inch, được dùng như một tuỳ chọn thay thế cho cáp Loại 1 và Loại 2 bởi giá thành thấp. Nó có bốn UTP dây24 AWG lõi đặc dùng cho các mạng hoặc cho các hệ điện thoại. Không thể dùng Loại 3 cho các mạng Token Ring 16Mbps. Nó được chủ

yếu dùng cho các phiên truyền cấp dữ liệu thấp, dài bên trong các bức tường. Các tín hiệu không di chuyển nhanh bằng cáp Loại 1 bởi Loại 3 không có màng chắn như của Loại 1.

- Loại 5. Cáp quang chỉ được dùng trên vòng khâu chính. Loại 5 có thể dùng hai sợi quang 100um hoặc 140um trong một cáp bao.
- Loại 6. Một màng chắn tết bím bao quanh hai cặp xoắn dây đồng nhiều sợi kết tao. Nó được tạo bằng hại STP, Cáp này hỗ trợ các đoạn chạy cáp ngắn hơn Loại 1, song linh hoạt hơn bởi các dây dẫn có lõi nhiều sợi.
- Loại 8. Dùng một STP đơn lẻ, dây 26 AWG lõi nhiều sợi và được thiết kế để chủ yếu dùng dưới thảm.
- Loại 9. Cũng giống như cáp loại 6 ngoại trừ được thiết kế với tính năng chống cháy để dùng trong các cơ sở đầy. Nó dùng hai STP, dây 26 AWG lõi đặc và được dùng cho các đoạn chạy cáp dài bên trong các bức tường toà nhà.

Hệ cáp Token Ring được dùng để nối các hệ khách với MSAU, hoặc nối một MSAU với một MSAU khác. Các cáp nối giữa các MSAU có tên là cáp nhánh [patch cables]. Với cáp nhánh, ta cũng có thể dùng loại IBM Loại 6.

Khi kết nối mạng Token Ring phải bảo đảm tiến hành theo các bước sau:

- Khởi tạo từng cổng trong MSAU bằng cách dùng công cụ xác lập đi kèm MSAU trước khi nối một cáp.
- Nếu dùng nhiều MSAU, nối cổng RO của từng MSAU với cổng RI của MSAU kế tiếp trong vòng lặp. Về vật lý, điều này phải hoàn tất một vòng tròn hoặc vòng khâu.
- Phải tuân thủ nhiều nguyên tắc khác nhau khi cấu hình các Token Ring.

*Các nguyên tắc dưới đây áp dụng cho mạng Token Ring cơ động loại nhỏ:*

- Khoảng cách cáp nhánh tối thiểu giữa hai MSAU là 2.5 m. và tối đa là
- Khoảng cách cáp vá tối đa giữa hai MAU là 45m.
- Khoảng cách cáp nhánh tối đa nối tất cả các MAU là 120m.
- Khoảng cách cáp adaptor tối đa giữa một MAU và một nút là 45 m.
- Tối đa 72 nút trên 1 hub (MAU)
- Tối đa 12 MAU
- Cáp Loại 6

*Một hệ cáp IBM có định lớn bao gồm:*

- Tối đa 260 nút trên 1 MAU
- Tối đa 33 MAU
- Cáp Loại 1 hoặc Loại 2

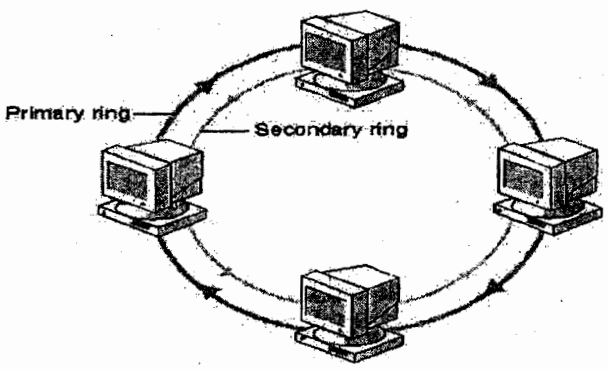
**FDDI**

Fiber Distributed Data Interface là một chuẩn LAN, giống như Token Ring; nó tuân thủ chuẩn IEEE 802.5 để truy cập mạng. FDDI tải các phiên truyền thông LAN do tia lasez và LED phát sinh thông qua cáp quang. Cáp quang chủ yếu bao gồm thuỷ tinh tinh khiết được kéo thành một lõi, được bao bởi một tầng thuỷ tinh khác có tên là lớp lót. LED gửi các tín hiệu xuyên qua lõi cáp này, và lớp lót chứa các tín hiệu này theo lõi. Tín hiệu trên từng sợi chỉ có thể mỗi lần đi theo một hướng. Bó sợi cho phép LED gửi các bội tín hiệu cùng một lúc.

Không như Token Ring và các card giao tiếp mạng hữu quan của nó thường truyền dữ liệu qua mạng theo các tốc độ 4 hoặc 15 Mbps, FDDI chuyển giao thông tin ở tốc độ 100 Mbps. Ngoài ra, FDDI được cấu trúc để tận dụng ưu điểm của hai vòng khâu thay vì một (hình 4.19). Cấu trúc Dual Counter Rotating [hai vòng khâu quay ngược] này cho phép FDDI chuyển giao dữ liệu qua một vòng khâu trong khi tiến hành lưu dự phòng và các dịch vụ khác trên vòng khâu thứ hai. Ngoài ra, FDDI dùng nhiều thẻ bài và có khả năng bỏ qua các trạm mạng được chỉ định có mức ưu tiên thấp, do đó nó có thể cung cấp dịch vụ nhanh hơn cho các trạm mạng có ưu tiên cao.

Cũng như LAN Token Ring, FDDI dùng một thẻ bài để chuyển giao các khung dữ liệu vòng quanh mạng. Sau khi khung dữ liệu được xử lý bởi đúng trạm mạng, thẻ bài được chuyển tiếp đến nút mạng gắn kế tiếp.

Vòng khâu thứ hai trong mạng FDDI sẽ quay theo hướng ngược lại với vòng khâu thứ nhất. Dạng quay ngược này sẽ cho phép mạng bù đắp một chỗ đứt trong sợi cáp. Nếu một vòng khâu trong mạng bị hỏng do một sự cố tại một trong các trạm mạng, các trạm nằm trên một trong hai phía của chỗ đứt có thể cô lập chỗ đứt trong sợi cáp bằng cách hình thành một vòng khâu đơn lẻ (thu gó ) từ các cổng riêng của chúng, như minh họa trong hình 4.19.




**Hình 4.19 Cấu trúc mạng FDDI**

Mỗi trạm mạng có thể được gắn với một trong hai vòng khâu hoặc với cả hai vòng khâu, tuỳ theo lớp của trạm được nối.

Một phương pháp khác để cô lập các nút lỗi trong mạng đó là dùng các bộ tập kết đấu dây. Về lý thuyết, các bộ tập kết đấu dây hoạt động giống như MSAU Token Ring. Chúng tác động như những thiết bị đấu cáp tập trung cho các mạng. Tuy nhiên, không như các MSAU, các bộ tập kết đấu dây có thể truyền thông với các trạm và xác minh tính nguyên vẹn của tuyến giao kết trạm bộ tập kết.

*Các ưu điểm của việc dùng FDDI*

- Khả năng cô lập một chỗ bị đứt trong cáp và tiếp tục truyền thông mạng đã khiến FDDI trở thành một phương án đấu cáp cực kỳ tin cậy. FDDI còn có vài ưu điểm khác.
- FDDI khắc phục vài sự cố về khả năng vận hành thường gặp trên các mạng Token Ring truyền thống bằng cách thực thi một chuẩn cung cấp tính năng truy cập mạng hợp lý và đúng lúc.
- Độ tin cậy tăng là một ưu điểm của FDDI. Độ tin cậy này có vài dạng, bao gồm:
  - An toàn thông tin. Cáp quang khó câu dây nghe trộm.
  - An toàn vật lý. Cáp quang bền hơn các kiểu đấu cáp khác.
  - An toàn điện. Cáp quang không bị nhiễu điện và không dẫn điện.
- FDDI cũng có thể truyền các gói tin mạng trên cáp của nó trên các khoảng cách dài hơn nhiều so với các kiểu đấu cáp khác. Ví dụ, trên một đường cáp quang không có các chỗ cong hoặc chỗ đứt có thể làm giảm tính nguyên vẹn của phiên truyền, thông tin có thể di chuyển hàng trăm dặm.
- FDDI cũng có cài sẵn khả năng quản trị ba lĩnh vực của mạng, bao gồm:
  - Ring Management ( RMT ). Chịu trách nhiệm về việc tìm và giải quyết các lỗi trong vòng khâu mạng
  - Conection Management ( CMT ). Chịu trách nhiệm về việc điều khiển các trạm tự chèn vào mạng hoặc tự tháo bỏ ra khỏi mạng
  - Station Management ( SMT ). Tạo cho các chương trình đặc biệt cấp cao giám sát vòng nối

*Các nhược điểm của việc dùng FDDI*

Hai nhược điểm chính của FDDI trong mạng: một là, do tính phức tạp và sự mới mẻ của công nghệ FDDI, nên cần có chuyên môn cao để cài đặt và sau đó bảo trì mạng FDDI; và hai là, mặc dù giá thành của bản thân cáp có thể so sánh với hệ cáp UTP, song các bộ tập kết và các adaptor LAN tương đối đắt. Do đó, chi phí chung của một

mạng FDDI dành cho LAN theo một quy mô bất kỳ có thể nhanh chóng trở thành khá cao.

## 4.5 Hệ điều hành mạng

Máy tính không thể làm việc khi không có hệ điều hành, một mạng máy tính không thể thao tác khi không có hệ điều hành mạng. Hệ điều hành mạng phụ thuộc vào nhà cung cấp, nó có thể là một phần mềm mạng độc lập bao gồm cả hai chức năng hề điều hành máy tính và hệ điều hành mạng hoặc là tích hợp với các hệ điều hành có sẵn trên máy tính. Novell's NetWare là một hệ điều hành mạng quen thuộc và được nhiều người ưa chuộng là một ví dụ điển hình về hệ điều hành mạng độc lập trên máy tính đảm bảo cả hai chức năng quản lý mạng và quản lý bản thân máy tính.

Phần mềm hệ điều hành mạng được tích hợp vào trong một số hệ điều hành máy tính được mọi người ưa chuộng bao gồm Windows 2000 Server/Windows 2000 Professional, Windows NT Server/Windows NT Workstation, Windows 98, Windows 95, và AppleTalk.

Hệ điều hành của máy tính kết hợp qua lại giữa máy tính và chương trình hoặc các ứng dụng - đang chạy. Nó điều khiển sự phân phối và sử dụng tài nguyên phần cứng như:

- Bộ nhớ RAM.
- Thời gian sử dụng CPU.
- Truy nhập không gian đĩa.
- Thiết bị ngoại vi.

Trong môi trường mạng, máy chủ cung cấp các tài nguyên mạng cho các máy trạm trên mạng và phần mềm mạng của máy trạm sẽ biến các tài nguyên này thành tài nguyên mà máy trạm có thể sử dụng được. Hệ điều hành mạng và các phần mềm mạng ở các máy trạm làm việc nhịp nhàng với nhau sao cho các tiến trình và các chức năng mạng được vận hành trôi chảy. Các đặc tính chính của hệ điều hành mạng là hệ điều hành đa nhiệm, nó có khả cung cấp phương tiện cho phép máy tính xử lý nhiều tiến trình (nhiệm vụ ) trong cùng một thời điểm

Phần mềm mạng có hai thành phần chính :

- Phần mềm mạng trên máy trạm.
- Phần mềm mạng trên máy chủ

***Phần mềm mạng trên máy trạm.***

Trong chế độ hoạt động một mình khi người sử dụng gõ một lệnh yêu cầu máy tính thực hiện một nhiệm vụ nào đó, yêu cầu này thông qua mạng bus nội tại của máy

chuyển tới CPU để thực hiện và gửi kết quả ra cho người sử dụng trên màn hình máy tính. Trong môi trường mạng khi người sử dụng có yêu cầu sử dụng một tài nguyên trên mạng thì yêu cầu này được định hướng lại và chuyển tiếp từ bus nội tại của nó lên trên mạng tới máy chủ. Phần mềm máy chủ sẽ kiểm tra yêu cầu và kiểm tra quyền truy nhập hợp pháp của người sử dụng nêu được quyền nó sẽ thực hiện và gửi kết quả theo đường mạng tới máy tính yêu cầu các chức năng định hướng và chuyển tiếp yêu cầu và quản lý các quá trình này do phần mềm mạng trên máy trạm đảm nhiệm hoàn toàn tự động và người sử dụng không hề phải quan tâm các tài nguyên sử dụng này là tại chỗ hay trên mạng.

***Phần mềm mạng trên máy chủ***

Với phần mềm máy chủ, các người sử dụng ở các máy khác có thể chia sẻ dữ liệu chung và bao gồm cả thiết bị ngoại vi máy in, máy vẽ, thư mục. Phần mềm trên máy chủ có các chức năng chính sau:

**1. Chia sẻ tài nguyên:**

Khái niệm chia sẻ dùng để mô tả các tài nguyên chung trên mạng cho phép mọi người trên mạng đều được truy nhập đến. Nhiều hệ điều hành mạng không chỉ cho phép chia sẻ mà còn xác định rõ mức độ chia sẻ. Bao gồm:

- Cho phép các người sử dụng khác nhau có các mức độ quyền truy nhập khác nhau tới các tài nguyên mạng.
- Điều phối quá trình truy nhập tài nguyên sao cho đảm bảo rằng cùng một thời điểm không thể có hai người cung truy nhập vào một tài nguyên.

**2. Quản lý người sử dụng**

Hệ điều hành mạng cho phép người quản lý mạng xác định bất cứ người sử dụng nào hoặc nhóm người sử dụng nào sẽ được phép truy cập tài nguyên mạng. Người quản trị mạng có thể sử dụng hệ điều hành mạng để:

- Tạo quyền cho người sử dụng, Sử dụng hệ diều hành mạng giám sát việc truy nhập mạng, xác định người đang sử dụng mạng.
- Cho phép hoặc từ chối quyền sử dụng trên mạng.
- Xoá bỏ người sử dụng từ danh sách sử dụng để hệ điều hành mạng có thể kiểm soát được.

Đối với mạng lớn nhiều người sử dụng, để dễ cho người quản trị mạng, các hệ điều hành mạng thường có chức năng phân thành các nhóm người sử dụng, trong một nhóm thì mọi người đều có quyền sử dụng như nhau.

**3. Quản lý mạng**

Một vài hệ điều hành mạng cao cấp có bao gồm các công cụ quản lý giúp đỡ người quản trị mạng giám sát được các trạng thái mạng. Nếu vấn đề phát sinh trên

mạng, công cụ quản lý có thể phát hiện ra dấu hiệu của sự cố và biểu diễn chúng dưới dạng bản đồ, hoặc các định dạng khác. Với công cụ đó, người quản trị mạng có thể tác động kịp thời và chính xác để hiệu chỉnh, trước khi mạng bị treo.

***Các hệ điều hành mạng điển hình***

- **Hệ điều hành Novell:** Hệ điều hành mạng NetWare gồm ứng dụng cho máy chủ và máy trạm. Ứng dụng cho máy trạm thiết kế để chạy trên nền nhiều hệ điều hành máy trạm. Ứng dụng cho máy chủ có thể truy cập qua người sử dụng từ máy trạm chạy MS-DOS, Microsoft Windows (phiên bản 3.*x*, 95, and 98, và Windows NT), OS/2, AppleTalk, or UNIX. Thường NetWare là hệ điều hành mạng được lựa chọn trong môi trường hỗn hợp các hệ điều hành. Trong mạng nhỏ, NetWare có thể đắt tiền và phức tạp với nhà kỹ thuật mạng thiếu kinh nghiệm cho việc cài đặt và quản trị. Phiên bản 3.2 của Netware là hệ điều hành 32 bit hỗ trợ cho Windows (phiên bản 3.*x*, 95, and 98 và Windows NT), UNIX, Mac OS, và môi trường MS-DOS. Với phiên bản 4.11 Netware, Novell giới thiệu là hệ điều hành mạng mới, dịch vụ chỉ dẫn Novell. Phiên bản 5.0, phiên bản gần đây nhất được phát hành, có tích hợp LAN, WAN và các ứng dụng mạng, mạng Intranet và Internet vào trong một mạng toàn cầu.

Dịch vụ thư mục Novell (NSD) cung cấp dịch vụ tên, bảo mật, chọn đường, thông báo, quản lý, xuất bản web, file và dịch vụ in. Sử dụng cấu trúc thư mục X500, nó quản lý tất cả các tài nguyên mạng, kể cả người sử dụng, nhóm sử dụng, máy in, máy chủ.

- **Hệ điều hành mạng Microsoft**

Được chia làm hai loại tương ứng với hai mô hình mạng :

- Mạng bình đẳng: Windows 9x, Windows 2000
- Mạng chủ / tớ : Windows 2000, Windows NT..

**Windows NT** cũng giống như hệ điều hành NetWare, Windows NT tổng hợp trong nó cả hệ điều hành - Hệ điều hành mạng và hệ điều hành máy tính. Bao gồm hai thành phần : Windows NT Server chạy trên máy chủ để quản lý chức năng trên mạng và tài nguyên mạng, Windows NT Workstation chạy trên các máy trạm cung cấp cho các máy trạm các chức năng mạng.

Windows NT làm việc trong chế độ domain. Mỗi một Domain là tập hợp các máy tính cùng chia sẻ một cơ sở dữ liệu chung và có cùng một mức độ bảo mật. Mỗi domain đều có tên riêng. Bên trong mỗi một domain nhất thiết phải có một máy được chỉ định làm máy chủ quản lý điều khiển Domain chính (PDC), nó chịu trách nhiệm về các dịch vụ thư mục và kiểm tra quyền truy nhập của người sử dụng. Các dịch vụ thư mục của Windows NT có thể thực hiện bởi nhiều cách khác nhau như sử dụng tài khoản người dùng hoặc cơ sở dữ liệu bảo mật.

Có bốn chế độ domain sau:

- **Domain** đơn : Một máy chủ đơn quản lý cơ sở dữ liệu tài khoản người dùng và bảo mật.
- Chế độ đơn chủ: Một mạng chủ có thể có vài domain nhưng chỉ có một domain được chỉ định là chủ và quản lý cơ sở dữ liệu tài khoản người dùng và bảo mật.
- **Chế độ đa chủ (Multiple-master):** Một mạng có nhiều chủ sẽ bao gồm nhiều domain nhưng cơ sở dữ liệu tài khoản người dùng được quản lý bởi nhiều máy chủ. Chế độ này chỉ sử dụng trong một tổ chức rất lớn.
- **Chế độ tin cậy hoàn toàn (Complete-trust)** có nghĩa là **trên mạng** có nhiều Domain song không có một Domain riêng nào được chỉ định là chủ. Tất cả các Domain hoàn toàn tin tưởng lẫn nhau.

**- Hệ điều hành UNIX cho mạng LAN**

UNIX nói chung là một hệ điều hành đa nhiệm, đa người sử dụng. Hai phiên bản được nhiều người ưa thích là Linux và Sun Microsystem's Solaris. Một hệ thống UNIX thường thường được lắp ghép giữa một máy tính trung tâm và nhiều người sử dụng thiết bị đầu cuối riêng lẻ. Nó là mạng độc lập, thiết kế đặc trưng cho mạng lớn, cũng có vài ứng dụng cho máy tính cá nhân. UNIX làm việc tốt trên máy tính đơn và bởi vì nó có khả năng chạy đa nhiệm nên nó cũng thực hiện tốt trong môi trường mạng.

UNIX thích nghi cao với môi trường khách/chủ. Nó có thể được sử dụng như hệ điều hành trong một máy chủ khi cài đặt phần mềm file-server. và với vai trò là máy chủ UNIX thể đáp ứng lại yêu cầu từ máy trạm. Phần mềm file-server ngày càng trở thành một ứng dụng phổ biến chạy cho máy tính đa nhiệm.

Một máy trạm trong hệ điều hành UNIX có thể là máy tính UNIX hoặc các máy tính khác chạy trên nền MS-DOS, OS/2, Microsoft Windows, hoặc Macintosh. Một file của người điều khiển sẽ có khả năng làm kho dữ liệu máy trạm và gọi ra file của UNIX như thể họ lấy ra trong định dạng ban đầu.

# CHƯƠNG 5

# CÁC BỘ GIAO THỨC CHUẨN

## 5.1 Tổng quan về các giao thức

Để thiết kế một toà nhà. Trước tiên, kiến trúc sư đưa ra một bản phác mô tả bản chất chung của toà nhà. Sau đó, kiến trúc sư, có thể làm việc với một chuyên viên về ngành kinh doanh nhà cụ thể, phát triển các bản thiết kế mô tả mọi chi tiết của toà nhà đó. Cuối cùng, một toà nhà thực tế được xây dựng.

Các giao thức là những bản thiết kế về cách nối mạng- các phần mô tả thật chi tiết tất cả các chức năng tại một tầng truyền thông nhất định. Tuy nhiên, trừ phi giao thức đó được diễn tả trong phần cứng và phần mềm, nó không thể đưa ra làm việc. Ba giai đoạn diễn ra trước khi giao thức thực sự làm việc

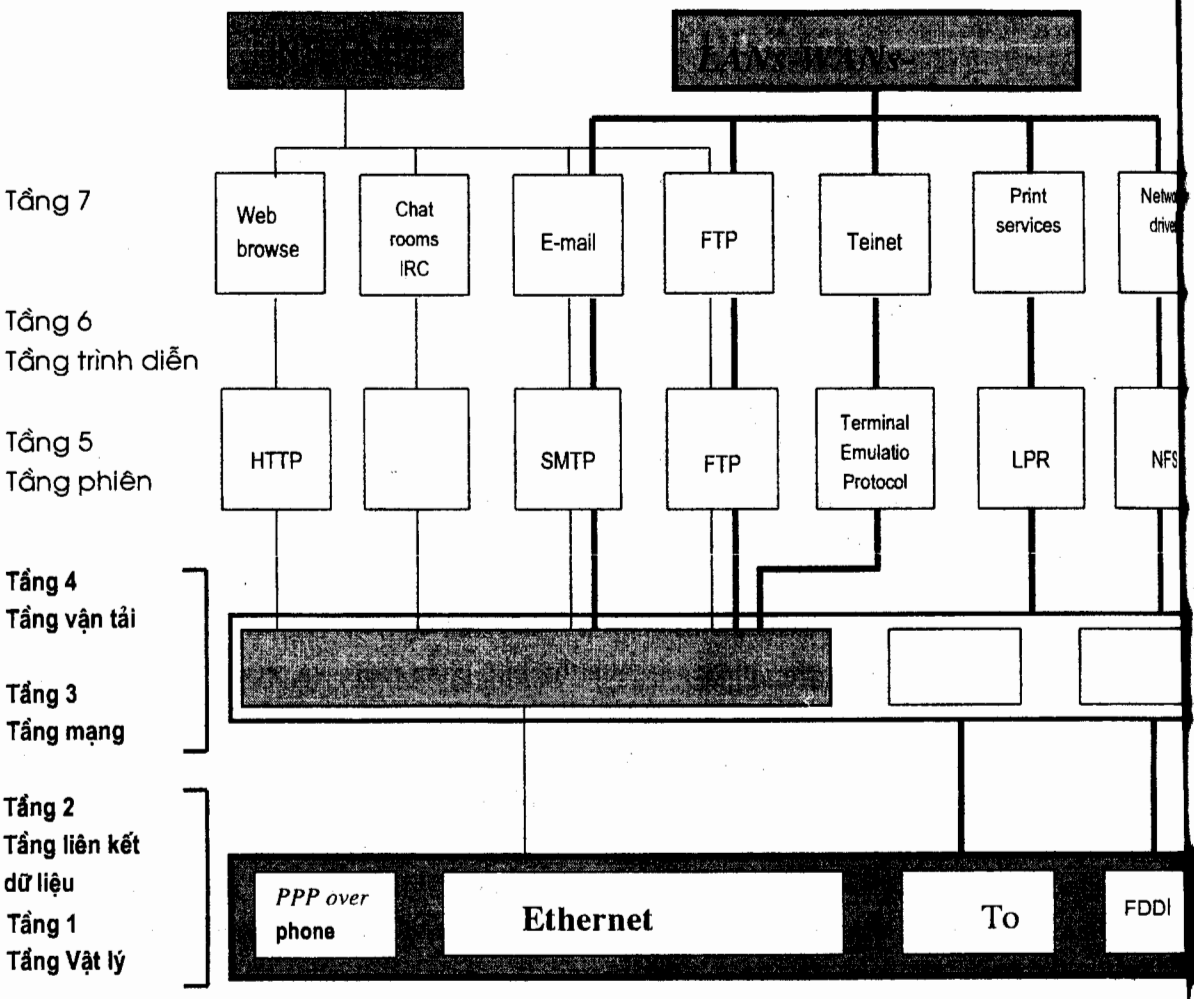
- Một mô hình mô tả chức năng chung của giao thức đó.
- Bản thân giao thức được định nghĩa thật chi tiết.
- Giao thức phải được các nhà thiết kế phần mềm và phần cứng nhận thức trong các sản phẩm thực tế.

Tiến trình phiên dịch một giao thức thành phần cứng và phần mềm có thể là một việc khó, các nhà thiết kế khác nhau thường gặp khó khăn trong việc đưa trang thiết bị của họ tương tác mà không phải tiến hành một kiểu chỉnh sửa nào đó, nhất là trong các giai đoạn tiên khởi của tuổi thọ giao thức. Cuối cùng, việc thực thi một giao thức trở thành khá thông lệ, nhưng phải luôn thẩm tra mọi cuộc trắc nghiệm tính tương thích đã được thực hiện trên một mẩu thiết bị mới.

Do các nhà thiết kế và điều hành viên đã gặp nhiều sự cố khi gắng tương kết các thiết bị chạy các giao thức khác nhau, nên nhiều tổ chức có xu hướng thiên về các hệ thống mở. Hệ thống mở [Open systems] là những loạt các chuẩn phần cứng và phần mềm có thể áp dụng chung xuyên suốt ngành công nghiệp để giảm bớt các khó khăn trong truyền thông.

Mô hình tham chiếu OSI đã được dùng như một chiến lược để phát triển các hệ thống mở, và một số hãng kinh doanh đã thiết kế lại các bộ giao thức hiện có để khiến chúng tương thích hơn với mô hình OSI. Các tổ chức khác-ví dụ điển hình là cộng đồng TCP/IP- cho rằng họ đã có sẵn một bộ giao thức mang tính chức năng cao mà thực tế đã mang tính mở - ở chỗ chúng luôn sẵn dùng cho mọi người trong ngành công nghiệp.

Kết quả là, sự tác động của mô hình OSI đã hạn chế ở mức sản phẩm của một số nhà chế tạo.




**Hình 5.1 Tổng quan các giao thức mạng so với mô hình OST**

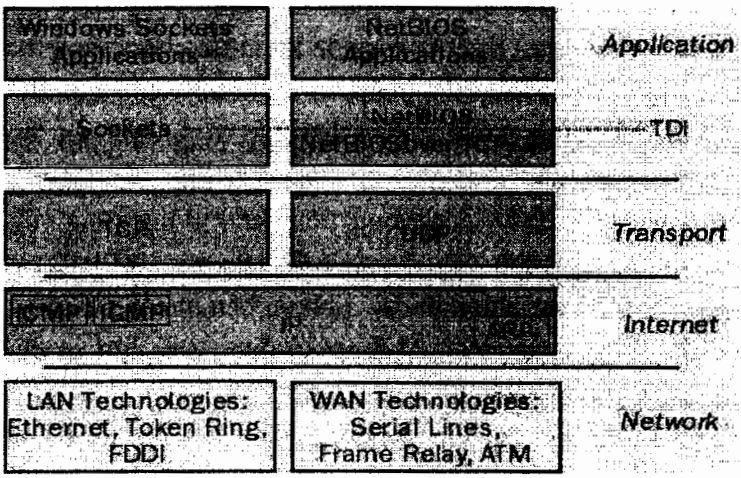
Hình 5.1 mô tả một cách khá tổng quát vị trí của các giao thức và các phần mềm dịch vụ mạng được dùng phổ biến hiện nay trên các mạng LAN, WAN và Internet so với mô hình tham chiếu OSI. Trong chương này sẽ trình bày kỹ ba giao thức cơ bản hiện nay trên mạng là các giao thức TCP/IP, IPX/SPX, NETBEUI.

## 5.2 Giao thức TCP/IP

### 5.2.1 Tổng quan TCP/IP

Thoạt đầu, bộ giao thức TCP/IP (còn gọi là bộ giao thức Internet) được phát triển bởi DoD ( Bộ quốc phòng Mỹ) để cung cấp dịch vụ trên các liên mạng lớn, kết hợp nhiều kiểu máy tính khác nhau. Trong những năm gần đây, các giao thức TCP/IP ngày càng phổ biến và trở thành các giao thức mạng phổ dụng nhất hiện hành, được sử dụng trong hầu hết các mạng LAN, WAN và nó là bộ giao thức chuẩn của mạng Internet. Hình 5.2 minh hoạ cụ thể mối quan hệ giữa các giao thức trong bộ TCP/IP và các tầng của Mô hình tham khảo OSI. TCP/IP được thiết kế để làm việc dựa trên các chuẩn đã thiết lập như Ethernet. TCP/IP giao tiếp được với phần lớn các công nghệ của tầng vật lý và tầng nối kết dữ liệu.

Giao thức TCP/IP cung cấp cho mạng khả năng kết nối tất cả các trạm (host) và các vị trí khác nhau, cung cấp một tiêu chuẩn cho việc trao đổi thông tin giữa các máy và sự liên lạc giữa các mạng. TCP/IP là một giao thức bao gồm 4 lớp: lớp ứng dụng, lớp vận chuyển, lớp mạng (Internet) và lớp giao diện với cạc mạng, như trong hình 5.2.




**Hình 5.2 Mô hình 4 lớp**

Lớp ứng dụng là lớp trên cùng trong mô hình 4 lớp của TCP/IP, đó là các phần mềm truy nhập mạng. Lớp này tương ứng với lớp phiên, lớp trình diễn và lớp ứng dụng trong mô hình OSI. Một vài tiện ích và dịch vụ của TCP/IP chạy ở lớp ứng dụng này. Các tiện ích và dịch vụ này bao gồm (hình 5.1- Chi tiết được mô tả trong chương 7):

- HTTP là giao thức được sử dụng phần lớn đối với thông tin WWW. Window2000 với trình duyệt Internet Explorer được coi như là client HTTP và Internet Information Server (IIS) được coi như là server.
- FTP là một dịch vụ internet dùng để thuyên chuyển file từ máy tính này sang máy tính khác. Trình duyệt Internet Explorer và tiện ích dùng dòng lệnh FTP cả hai đều được coi như là client FTP.
- SMTP là một giao thức máy chủ cung cấp dịch vụ sử dụng để chuyển thư điện tử. IIS có thể gửi thông báo sử dụng giao thức SMTP.
- Telnet là một giao thức mô phỏng thiết bị đầu cuối được sử dụng để thâm nhập từ xa vào máy chủ khác trên mạng. Telnet giúp cho người sử dụng có thể chạy các chương trình từ xa và các thủ tục đơn giản. Với Telnet ta có thể dễ dàng hoạt động trong môi trường mạng không đồng nhất. Windows 2000 bao gồm cả hai : client và server Telnet.
- DNS - Hệ thống tên miền là một giao thức và dịch vụ trên mạng TCP/IP nó cho phép phân cấp thứ bậc trên mạng và định vùng máy chủ dễ dàng bằng việc sử dụng các tên thân thiện hơn mà không phải nhớ các địa chỉ IP.
- SNMP cho phép quản lý các nút mạng như các máy chủ, trạm làm việc, bộ định tuyến, cầu nối, và hubs từ một máy chủ trung tâm. SNMP cũng có thể được sử dụng như một thiết bị ở xa để kiểm tra chất lượng mạng, dò tìm các lỗi hoặc các truy nhập không hợp pháp, và kiểm tra việc sử dụng mạng.

Phần mềm TCP/IP cung cấp hai giao diện lập trình cho ứng dụng mạng (API) để sử dụng dịch vụ của giao thức TCP/IP:

**Winsock.** Windows 2000 là phương tiện được dùng rộng rãi với việc sử dụng Sockets cho giao diện lập trình ứng dụng (API). Sockets API là một tiêu chuẩn cho phép truy nhập gói dữ liệu và phiên từ các dịch vụ bên ngoài TCP/IP.

**NetBIOS.** Một tiêu chuẩn API đã được sử dụng như một cơ chế trao đổi và sử lý thông tin trong môi trường windows.

Lớp vận chuyển: Giao thức vận chuyển cung cấp thông tin về phiên giữa máy tính và định nghĩa kiểu dịch vụ vận chuyển như TCP- giao thức có liên kết hoặc UDP-giao thức không liên kết. TCP/IP là một giao thức có liên kết nó được ứng dụng cho các mô hình truyền dữ liệu với số lượng lớn trong cùng một thời gian. Nó cũng được ứng dụng cho dịch vụ yêu cầu sự xác nhận trở lại của nơi nhận. UDP là kiểu giao thức không liên kết và nó không đảm bảo về việc phân phối các gói dữ liệu đến đích 100 %. UDP được ứng dụng cho các dịch vụ truyền dữ liệu với số lượng nhỏ trong cùng một thời gian. Lớp vận chuyển trong mô hình TCP/IP cũng gần giống với lớp vận chuyển trong mô hình OSI.

Lớp Internet.: Các giao thức internet được gói gọn thành các gói dữ liệu nhỏ (IP) và được đưa đến các nơi cần thiết nhờ các thuật toán định đường. Chức năng định đường của lớp Internet giúp cho các máy chủ có thể hoạt động liên kết với các mạng khác. Lớp Internet tương đối giống với lớp mạng trong mô hình OSI. Có 5 giao thức được bổ xung trong lớp này :

- Giao thức phân giải địa chỉ (ARP-Address Resolution Protocol ), nó cung cấp địa chỉ vật lý của các trên mạng.
- Giao thức phân giải địa chỉ đảo (RARPReverse Address Resolution Protocol ), nó cung cấp địa chỉ đảo ở các máy chủ tiếp nhận. (Mặc dù Microsoft không bổ xung giao thức RARP, nhưng nó vẫn có trong các hệ thống khác có liên quan đến máy tính).
- Giao thức điều khiển thông điệp Internet(ICMP- Internet Control Message Protocol), giao thức này có nhiệm vụ gửi các thông báo chuẩn đoán lỗi và các tình huống bất thường liên quan với giao thức IP.
- Giao thức quản lý nhóm Internet (IGMP), nó cung cấp thông tin chính xác về định tuyến do các nhóm đưa ra.
- Giao thức Internet (IP), làm nhiệm vụ cung cấp địa chỉ lôgíc và định đường cho các gói dữ liệu.

**Lớp giao diện mạng.**

Lớp giao diện mạng luôn có ở một mô hình cơ bản nhất. Trong các mạng cục bộ LAN, các mạng cấp đô thị MAN, mạng diện rộng WAN, và mô hình quay số như Ethernet, Token Ring, phân phối dữ liệu bằng cáp (FDDI), và ARCnet, chúng có khác nhau về cáp, tín hiệu, và giải mã dữ liệu. Lớp giao diện mạng tương ứng với hai lớp liên kết dữ liệu và lớp vật lý của mô hình OSI. Lớp giao diện mạng làm nhiệm vụ gửi và nhận các khung, đó là các gói dữ liệu mang thông tin được truyền dẫn trên mạng. Lớp giao diện mạng chịu trách nhiệm đưa các khung vào mạng để truyền đi và nhận lại nó từ mạng.

**Công nghệ TCP/IP WAN.**

Có hai phạm trù của WAN được hỗ trợ bởi TCP/IP:

- Đường truyền nối tiếp bao gồm kiểu quay số tương tự, đường tín hiệu số, và đường cho thuê riêng. TCP/IP điều khiển các gói tin qua đường truyền nối tiếp bằng cách sử dụng một trong hai giao thức SLIP hoặc PPP. Server của Windows 2000 hỗ trợ cả hai loại giao thức này với các bộ định tuyến và dịch vụ truy nhập từ xa. PPP có tính an toàn và khả năng dò tìm lỗi tốt hơn so với SLIP, giao thức này được khuyến khích dùng cho thông tin kiểu đường nối tiếp.

- Mạng chuyển mạch gói như: mạng X25, trễ khung, và kiểu truyền dẫn không đồng bộ (ATM).

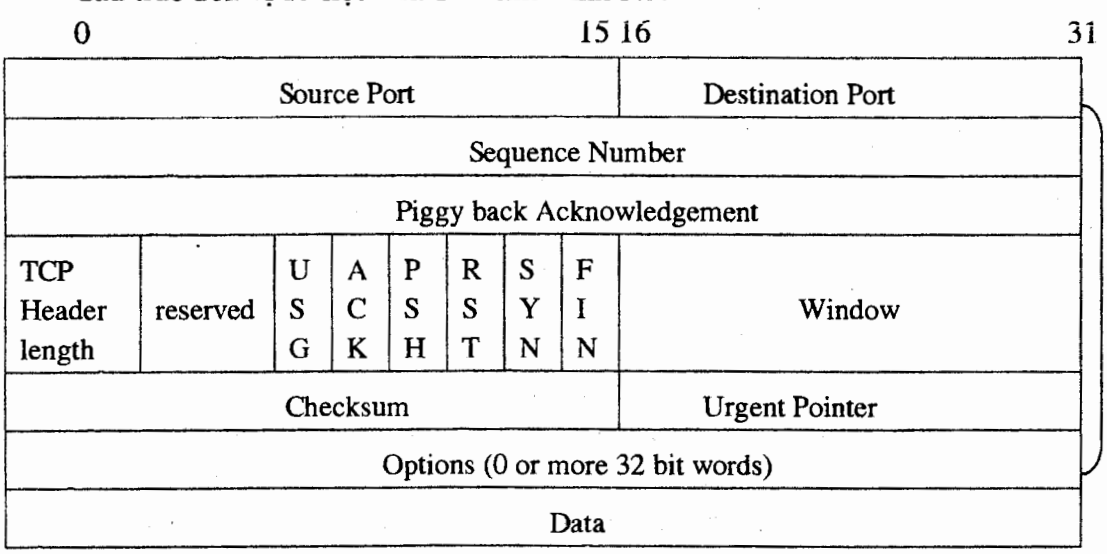
### 5.2.2 Giao thức TCP, UDP

TCP (Transmission Control Protocol ) là một giao thức liên mạng, tương ứng với tầng chuyển tải của OSI.TCP cung cấp khả năng chuyển tải hướng giao kết, song công đầy đủ. Khi không cần điều hành một tiến trình chuyển tải hướng giao kết, UDP (Used Datagram Protocol - Giao thức chuyển gam dữ liệu người dùng) có thể được đưa ra thay cho TCP ở cấp chuyển tải (Liên máy chủ). TCP và UDP hoạt động tại cùng một tầng.

TCP tương ứng với SPX trong môi trường Netware.TCP duy trì một tuyến giao kết logic giữa các hệ máy tính gửi và nhận. Theo cách này, tính nguyên vẹn của phiên truyền được duy trì. TCP nhanh chóng phát hiện mọi sự cố trong phiên truyền và ra tay hành động để chỉnh lý. Bù lại, TCP lại không chạy nhanh bằng UDP.

TCP còn cung cấp tính năng phân mảnh và lắp ráp lại thông điệp, đồng thời có thể chấp nhận các thông điệp có chiều dài bất ký từ các giao thức tầng phía trên. TCP phân mảnh các luồng thông điệp thành các phân đoạn mà IP có thể điều quản. Khi được dùng với IP, TCP bổ sung dịch vụ hướng giao kết và tiến hành đồng bộ hoá phân đoạn, bổ sung các số chuỗi tại cấp byte.

Cấu trúc đơn vị dữ liệu của TCP như hình 5.3:




**Hình 5.3 Cấu trúc dữ liệu TCP**

Ngoài việc phân mảnh thông điệp, TCP có thể duy trì nhiều cuộc thoại [conversation] với các giao thức tầng phía trên và có thể cải thiện việc sử dụng băng thông mạng bằng cách tổ hợp nhiều thông điệp vào chung một phân đoạn. Mỗi tuyến giao kết mạch ảo được gán một ID giao kết có tên là cổng [port] để định danh các gam dữ liệu kết hợp với tuyến giao kết đó.

UDP là một giao thức tầng chuyển tải phi giao kết, nó không cung cấp các tín hiệu báo nhận thông điệp; thay vì thế, nó đơn giản chuyển tải các gam dữ liệu. Cũng như TCP, UDP vận dụng các địa chỉ cổng để bàn giao các gam dữ liệu. Tuy nhiên, các địa chỉ cổng này không kết hợp với các mạch ảo mà chỉ đơn thuần định danh các tiến trình xử lý của máy chủ cục bộ. UDP được ưa dùng hơn TCP khi khả năng bàn giao đáng tin cậy không quan trọng bằng khả năng vận hành cao hoặc phải giữ phần điều hành chung của mạng ở mức thấp. Do UDP không cần thiết lập, bảo trì, và đóng các tuyến giao kết, hoặc điều khiển luồng dữ liệu, nên nói chung nó chạy nhanh hơn TCP. UDP được dùng trong giao thức quản trị mạng chuẩn SNMP (Simple Network Management Protocol) của các mạng TCP/IP. UDP cho phép SNMP cung cấp tính năng quản trị mạng với phần điều hành chung mạng ở mức tối thiểu.

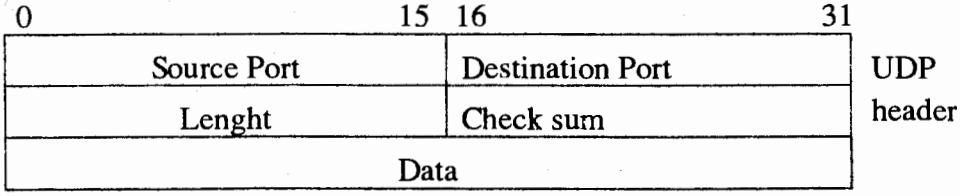
TCP được ấn định bằng một dãy số trên mỗi đoạn truyền đi (hình 5.3). Dòng dữ liệu này có chiều dài tuỳ ý được phân thành những đoạn không vượt quá 64KB và máy chủ khi nhận được các đoạn này vẫn phân biệt được chúng. Một sự xác nhận sẽ được gửi trả lại khi có một máy chủ khác tiếp nhận dữ liệu này. Đối với mỗi đoạn gửi đi, máy chủ tiếp nhận sẽ phải phản hồi một tín hiệu xác nhận (ACK) mà không có một mức ưu tiên nào cả. Nếu sau lần gửi đó không nhận được tín hiệu phản hồi ACK thì dữ liệu đó sẽ lại tiếp tục được gửi lại. Nếu đoạn dữ liệu thu được bị lỗi thì máy chủ tiếp nhận sẽ huỷ bỏ nó khi đó ACK sẽ không được gửi và máy chủ gửi sẽ gửi lại đoạn dữ liệu đó.

TCP header tối thiểu là 20 bytes và chỉ có một dạng .

- Source port và Destination Port là các cổng thâm nhập dịch vụ lớp giao vận. TCP có số lượng các cổng trong khoảng 0 cho đến $2^{16}-1$. Các cổng có số nằm trong khoảng từ 0 tới 1023 là được biết đến nhiều nhất vì các cổng này được sử dụng cho việc truy nhập tới các dịch vụ tiêu chuẩn.
- Sequence Number là số thứ tự của các byte dữ liệu được gửi đi.
- Piggy back Acknowledgement là số thứ tự của các byte dữ liệu đang chờ thu.(thông số này chỉ được xác định khi cờ ACK = 1.)
- TCP header length: độ dài của TCP header một đơn vị tương ứng với 32 bit.

- Reserved: dành cho sau này (đặt là Zero).
- URG: Cờ phải xử lý trước các số liệu khác.
- ACK: Cờ biên nhận số liệu đã thu đúng.
- PSH: Cờ chuyển số liệu (push), không cần chờ đầy
  - Nếu chờ PUSH = 1 thì toàn bộ dữ liệu trong bộ đệm gửi, kể cả khối dữ liệu mới, sẽ được gửi đi ngay bằng một hay nhiều segment liên tiếp.
  - Ngược lại cờ PUSH = 0 thì dữ liệu được dữ lại trong bộ đệm gửi và sẽ gửi đi khi có cơ hội thích hợp, chẳng hạn chờ thêm dữ liệu nữa để có thể gửi đi các segment lớn hơn, hiệu quả hơn.
  - Tại trạm đích, dữ liệu đến sẽ được TCP lưu trong bộ đệm nhận gắn với mỗi liên kết. Nếu dữ liệu đến được đánh dấu với một cờ PUSH thì toàn bộ dữ liệu trong bộ đệm ( kể cả dữ liệu được lưu từ trước) sẽ được chuyển lại cho người sử dụng. Còn dữ liệu đến với PUSH = 0 thì TCP chờ đến khi thích hợp mới chuyển dữ liệu đi, với mục tiêu tăng hiệu quả của hệ thống.
- RST: Cờ huỷ bỏ kết nối do lỗi phần mềm hoặc cứng.
- SYN: Cờ đồng bộ để thiết lập kết nối.
- FIN: Cờ để kết thúc kết nối.
- Window: để điều khiển thông lượng và quản lý buffer.
- Checksum: 2 byte kiểm tra để đảm bảo thu nhận đúng phần đầu của TCP.
- Urgent Point có giá trị khi URG = 1, để chỉ ra đoạn dữ liệu khẩn cấp. Trường hợp cần chuyển gấp dữ liệu cho người sử dụng thì ta dùng cờ URGENT (URG = 1) để báo cho người sử dụng cần xử lý khẩn cấp dữ liệu đó với Urgent Pointer xác định vị trí kết thúc vùng dữ liệu khẩn.
- Options: tuỳ ý, ví dụ để thông báo kích thước buffer.

Cấu trúc đơn vị dữ liệu của UDP là đơn giản như hình 5.4.




**Hình 5.3 Cấu trúc dữ liệu UDP**

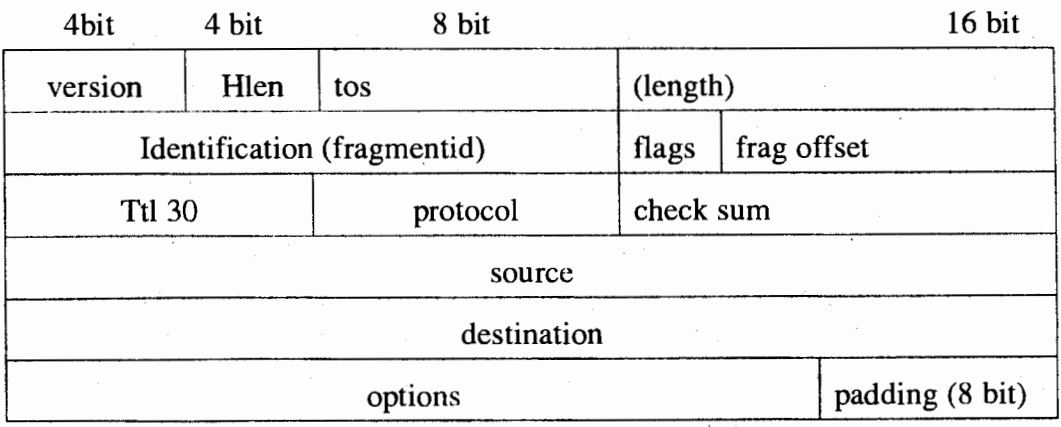
UDP là giao thức không liên kết, nó không đảm bảo gì về việc phân phối các gói dữ liệu. Trường dữ liệu checksum trong UDP là không bắt buộc, UDP được ứng dụng để đáp ứng các yêu cầu về việc tiếp nhận dữ liệu mà không cần sự xác nhận trở lại.

### 5.2.3 Giao thức IP

Giao thức IP (Internet Protocol) là một giao thức phi giao kết [connectionless] cung cấp dịch vụ gam dữ liệu, và các gói tin IP thường được gọi là các gam dữ liệu IP [IP datagrams]. IP là một giao thức chuyển gói tin thực hiện tiến trình định địa chỉ và chọn tuyến đường. Một phần đầu IP được chắp vào các gói tin, được các giao thức cấp thấp hơn truyền theo dạng các khung. IP định tuyến các gói tin thông qua các liên mạng bằng cách vận dụng các bảng định tuyến động được tham chiếu tại mỗi bước nhảy [hop]. Các phần xác định tuyến đường được tiến hành bằng cách tham khảo thông tin thiết bị mạng vật lý và logic, như được ARP (Address Resolution Protocol - giao thức phân giải địa chỉ) cung cấp.

Khi qua các môi trường liên kết dữ liệu khác nhau có kích thước tối đa của gói tin khác nhau, ta phải chia gói tin IP thành các gói nhỏ. Quá trình gộp chúng trở lại (reassembly) sẽ được thực hiện khi bên thu nhận được bản tin. Ví dụ, một gói tin dài 2000 byte được đưa vào mạng Ethernet, vì dạng bản tin Ethernet có độ dài cực đại chỉ là 1500 byte, ta sẽ phải cắt gói tin 2000 byte đó thành hai bản tin ngắn. IP cũng thực hiện tính năng kiểm tra lỗi trên dữ liệu phần đầu bằng một tổng trị kiểm [checksum], mặc dù dữ liệu của các tầng phía trên không được kiểm tra lỗi.

Một IP datagram gồm có các phần header và phần dữ liệu. Phần header có một phần cố định gồm 20 byte và một phần tuỳ ý độ rộng thay đổi. Cấu trúc phần đầu của gói tin IP hình 5.4:




**Hình 5.4 Cấu trúc đầu dẫn gói tin IP**

Ý nghĩa của các trường được thể hiện như bảng sau:

➢ Trường Type of Service: Trường này chứa các thông tin về quyền ưu tiên của việc truyền datagram và các ảnh hưởng có thể xảy ra trong quá trình truyền các datagram. Trường này có độ dài là 8 bit. IP chuẩn không yêu cầu chỉ ra các hành động cụ thể dựa trên giá trị của trường Type of Service. IP chỉ định sử dụng nó trong việc thiết lập các tuỳ chọn cho các mạng con mà nó sẽ truyền qua trong bước nhảy tới. Một vài máy và router không quan tâm đến giá trị cảu trường này trong khi một số khác lại dựa vào đây để quyết định đường truyền.

➢ Trường Total Length: Trường này chứa độ dài của datagram (bao gồm cả header và data) đo bằng byte (8 bit). Do số bit của trường này là 16 do đó độ dài lớn nhất có thể là 65535 byte. IP chuẩn yêu cầu tất cả các máy phải có khả năng nhận datagram có độ dài tới 576 byte.

➢ Trường phân đoạn (Fragment fields): Các trường Identification, Flags, Fragment Offset đóng một vai trò quan trọng trong quá trình phân đoạn (ở máy phát) và ghép nối (ở máy nhận). Trường Identification có độ dài là 16 bit. Nội dung của nó cho phép máy nhận biết các phân đoạn của datagram có cùng một datagram hay không.

➢ Trường Flags: Có 3 bit, Bit 0 để dự trữ, bit 1 = 0 thông báo đăng phân đoạn, ngược lại bit 1 = 1 là không phân đoạn, bit 2 =0 thông báo gói tin này là phân đoạn cuối ngược lại nếu bit 2=1 thì cho biết còn các phân đoạn khác tiếp theo. Người gửi thông tin có thể dùng bit 1 để cho phép phân đoạn datagram hay không. Nếu router không thể truyền nguyên cả một datagram mà bit này được thiết lập bằng 1 thì datagram đó sẽ bị loại bỏ và sẽ có một thông báo lỗi gửi đến máy phát. Bất kỳ một người quản trị mạng nào cũng có thể sử dụng cách này để kiểm tra độ lớn của các datagram có thể được truyền trên các phần khác nhau trên mạng Internet. Khi router phân đoạn các datagram, mỗi phân đoạn bao gồm 8 byte. 8 byte này được gọi là Fragment block. Trường Fragment Offset nói lên vị trí của đoạn dữ liệu phân đoạn này so với lúc bắt đầu phân đoạn datagram. Đơn vị đo chính là Fragment block.

➢ Trường Fragment Offset: Có độ dài 13 bit, do đó nó có thể đánh số từ 0 cho tới 8192 Fragment block, tương ứng từ 0 cho tới 65528 byte. Giả sử router thực hiện phân đoạn datagram có identification = 314, dữ liệu chứa 3000 byte chia làm 3 datagram, mỗi datagram chứa Header và 1000 byte (125 Fragment block) sữ liệu, thì các trường Flags, Identification Offset sẽ là:

| | ID | *Flags* | *Fragment Offset* |
|---|---|---|---|
| Fragment 1 | 314 | 100 | 0 block from start |
| Fragment 2 | 314 | 100 | 125 block (1000 byte) from start |
| Fragment 3 | 314 | 100 | 250 block (2000 byte) from start |

➢ Time-to-live: (TTL) chứa số giây lớn nhất có thể (nhiều nhất là 255 giây) mà datagram được cho phép tồn tại trong mạng trước khi tới đích. Bất cứ một datagram nào đó không tới được đích trong bảng thời gian của TTL đều loại bỏ. Trên thực tế không có một cách chính xác nào để theo dõi được trường thời gian này. TTL được cài đặt như một máy đếm đơn giản và khi đi truyền qua router thì được giảm đi 1. Tuy nhiên nó sẽ được giảm đi nhiều hơn khi được truyền với tốc độ chậm. Giá trị default của TTl được xác định bằng xấp xỉ hai lần đường truyền dài nhất trên mạng mà datagram có thể được truyền. Đường truyền dài nhất này đôi khi được gọi là bán kính của mạng.

➢ Protocol: Trường này có độ dài 8 bit dùng để xác định giao thức nào ở lớp trên sẽ là giao thức nhận datagram. TCP là 6 còn UDP là 17.

➢ Header checksum: Trường này có độ dài là 16 bit được tính toán dựa trên các trường khác trên IP header. Trường Checksum được cập nhật liên tục khi truyền datagram vì trường Time-to-live thay đổi tại các router.

➢ Địa chỉ nguồn và địa chỉ đích: Trường địa chỉ của IP bao gồm 32 bit, cấu tạo của trường địa chỉ nói sau, có 4 lớp địa chỉ A, B, C, D. Lưu ý là địa chỉ mạng theo dạng OSI cho phép trường này có thể có độ dài thay đổi, tuy nhiên độ dài cố định cho phép việc đánh địa chỉ, truyền dữ liệu, cài đặt dễ dàng và nhanh hơn nhiều.

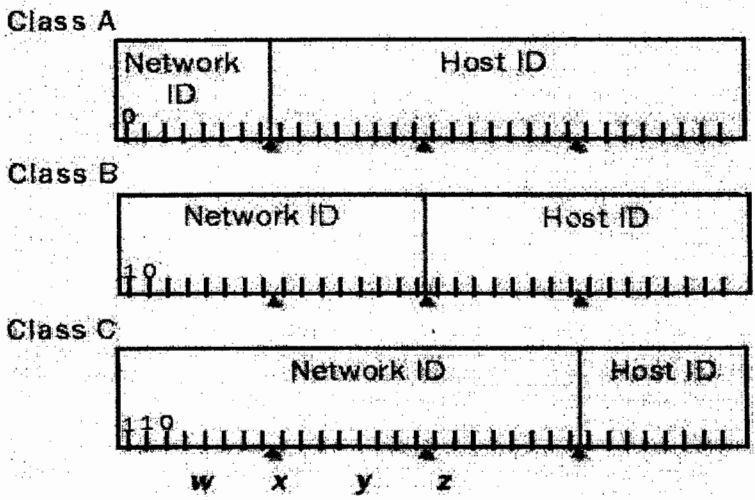
➢ Các trường lựa chọn: IP dành 40 byte cho một hay nhiều trường lựa chọn, các trường lựa chọn này được tạo ra bởi các ứng dụng truyền thông (communication applications).

### 5.2.4 Địa chỉ sử dụng trong TCP/IP

Ba kiểu thông tin địa chỉ dưới đây được dùng trên các liên mạng TCP/IP:

- Địa chỉ vật lý. Được tầng vật lý và tầng nối kết dữ liệu sử dụng.
- Các địa chỉ IP. Cung cấp các ID máy chủ và mạng logic. Các địa chỉ IP bao gồm bốn con số thường được diễn tả theo dạng thập phân có chấm. Ví dụ, 134.135.100.13 là một địa chỉ IP.

- Các tên nút Logic. Định danh các máy chủ cụ thể bằng các ID tên miền. Chúng giúp ta dễ nhớ hơn so với các địa chỉ IP toàn con số. Ví dụ, MYHOST.COM là một tên nút logic [logical node name].




**Hình 5.5 Địa chỉ IP của các lớp**

**Địa chỉ IP** là địa chỉ Internet được phân phối bởi InterNIC, cơ quan này là một tổ chức hành chính của Internet. Các địa chỉ IP được cấu trúc từ 32 bit dữ liệu và được chia thành các lớp. Bao gồm 5 lớp A, B, C, D và E, tương ứng với người sử dụng đầu cuối khác nhau..Lớp D và E dùng cho các mục đích riêng (thông tin quảng bá). Cấu trúc các lớp A, B, C, được mô tả ở hình 5.5.

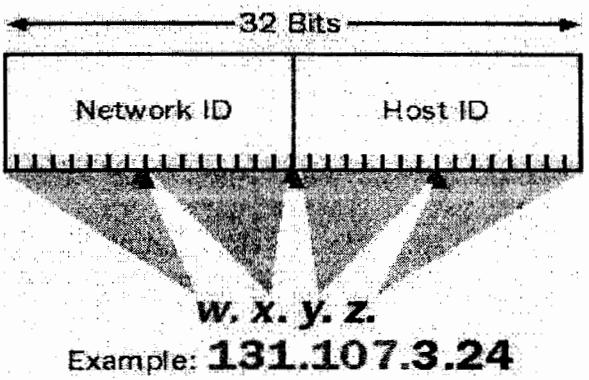
Địa chỉ IP được chia làm hai thành phần số hiệu mạng (Network ID) và số hiệu máy tính (Host ID).

- Số hiệu mạng dùng để phân biệt các máy tính TCP/IP có nằm trong cùng một mạng vật lý không. Tất cả các máy tính nằm trong cùng một mạng vật lý phải được định nghĩa cùng một số hiệu mạng để đảm bảo truyền thông giữa chúng với nhau.
- Số hiệu máy tính dùng để xác định nó trong một mạng cụ thể. Số hiệu máy tính phải là duy nhất trong một mạng có số hiệu mạng xác định

Có hai cách biểu diễn một địa chỉ IP – kí hiệu cơ số hai và kí hiệu thập phân có dấu chấm. Như trong hình 5.6, mỗi địa chỉ IP dài 32 bit và chia làm 4 đoạn 8 bit. Mỗi đoạn 8 bít này được hiểu như một octets.

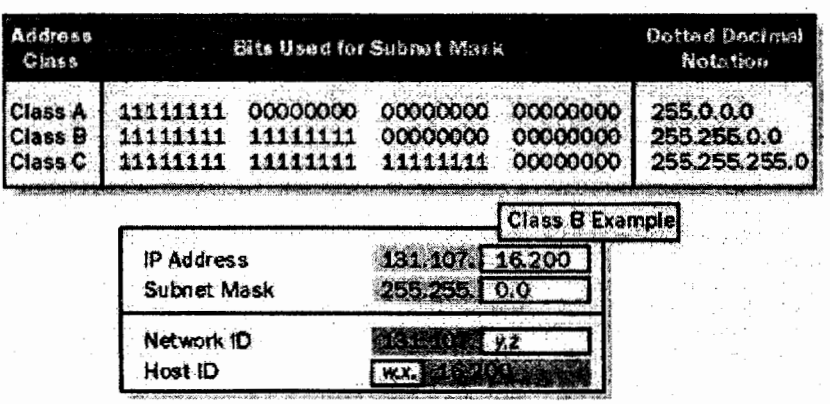
Ví dụ địa chỉ IP: 192.169.123.132 Viết dưới dạng mã cơ số hai là

11000000.10101000.01111011.10000100. Mã thập phân được chia ra bởi các dấu chấm thập phân như là các octet trong cách biểu diễn bằng cơ số hai. Các octet này miêu tả số thập phân từ 0 đến 255, và gồm 32 bit để định danh mạng và máy chủ như hình 5.6




**Hình 5.6 Ví dụ một địa chỉ IP cụ thể**

Mỗi máy tính trên mạng TCP/IP đều yêu cầu có một mặt nạ mạng con (SUBNET MASK) để phân cấp thành các mạng con, giá trị mặt nạ mạng có hai khả năng hoặc là bằng giá trị mặc định khi mạng không có nhu cầu chia thành các mạng con, hoặc giá trị lựa chọn khi mạng được chia thành các mạng con. Một mặt nạ mạng con là một địa chỉ 32 bit sử dụng để ngăn chặn hoặc lọc các địa chỉ IP nhằm phân biệt ID mạng từ ID của máy chủ. Đây là một việc cần thiết để TCP/IP quyết định xem đây là địa chỉ IP của một mạng nội hạt hay là địa chỉ IP của một mạng ở xa.




**Hình 5.7 Ví dụ về bộ lọc phân cấp dưới được sử dụng ở lớp B**

Giá trị mặc định của mặt nạ mạng con phụ thuộc vào địa chỉ lớp của IP, xem hình 5.7.

Lớp A cho phép định danh mạng với số máy chủ rất lớn. Lớp mạng A sử dụng một mặt nạ mạng con mặc định là 255.0.0.0 và có giá trị từ 0-126 cho phần đầu tiên.

Lớp B cho phép ta định danh mạng với kích cỡ trung bình và lớn. Lớp mạng B sử dụng một mặt nạ mạng con mặc định là 255.255.0.0 và có giá trị từ 128-191 cho phần đầu tiên.

Lớp C cho phép định danh các mạng nhỏ như mạng LANs. Lớp mạng C sử dụng một mặt nạ mạng con mặc định là 255.255.255.0 và có giá trị từ 192-223 cho phần đầu tiên.

Nguyên tắc định địa chỉ IP: Mặc dù không có tiêu chuẩn cho việc ấn định địa chỉ IP như thế nào, nhưng chắc chắn việc ấn định địa chỉ IP phải hợp lý với IDs của mạng và IDs của máy chủ. Có một vài nguyên tắc chung khi ấn định IDs của mạng và IDs của máy chủ:

- ID mạng không thể là 127. Đây là ID dự phòng cho chu trình vòng lặp và chức năng chuẩn đoán.
- Các bít ID của mạng và của máy tính không thể tất cả đều là 1. Nếu tất cả các bit được đặt là 1, địa chỉ này được hiểu như một địa chỉ phát quảng bá trên toàn mạng chứ không phải là một địa chỉ ID của máy tính.
- Các bít ID của mạng và của máy tính không thể tất cả đều là 0. Nếu tất cả các bit được đặt là 0 thì địa chỉ đó cho biết đây là "một mạng duy nhất".
- ID của máy tính phải là duy nhất trong một mạng nhất định.
- ID của mạng phải là duy nhất đối với mạng diện rộng. Nếu ta liên kết đến mạng Internet công cộng, bạn phải biết được ID của mạng mà bạn muốn vào.

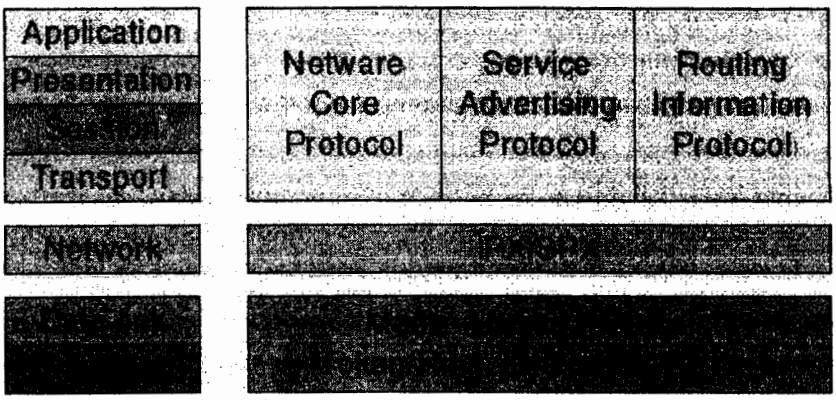
Tất cả các máy tính TCP/IP, bao gồm cả bộ định tuyến cũng yêu cầu một địa chỉ ID duy nhất. Địa chỉ ID của bộ định tuyến là địa chỉ IP có cấu hình giống như một trạm làm việc được mặc định là cổng gatewary.

## 5.3 Giao thức IPX/SPX

Giống như TCP/IP, NOVELL cung cấp một bộ giao thức đặc biệt cho Netware. Có 5 giao thức chính sử dụng bằng Netware là:

- Giao thức truy nhập phương tiện MAP
- Giao thức Chuyển mạch gói liên mạng/ chuyển mạch gói tuần tự (IPX/SPX)
- Giao thức thông tin chọn đường (RIP)

- Giao thức quảng bá dịch vụ (SAP)
- Giao thức mã Netware (NCP)




**Hình 5.8 So sánh giữa NetWare và mô hình tham chiếu OSI**

Hình 6.5 cho ta sơ đồ của các giao thức Netware so sánh với mô hình tham chiếu OSI. Trong thực tế, không có sự tương quan trực tiếp giữa ranh giới của hai kiến trúc đang tồn tại này. Các giao thức này tuân theo nguyên tắc bọc bì thư và đặc biệt là các giao thức mức cao hơn như NCP, SAP, RIP được bọc bởi IPX/SPX và giao thức MAP đến lượt mình lại bao IPX/SPX.

Giao thức truy nhập phương tiện (MAP): định địa chỉ ở từng nút trên một mạng NetWare network. Các địa chỉ này được cài đặt trên phần cứng hoặc cạc mạng NIC.

Giao thức này có trách nhiệm thiết lập phần đầu (header) trên mỗi gói dữ liệu, mỗi phần đầu gói tin bao gồm mã nguồn và mã đích. Sau khi gói dữ liệu được truyền trên mạng và đến cạc mạng, cạc mạng sẽ kiểm tra địa chỉ, nếu địa chỉ của chúng trùng với địa chỉ đích của gói dữ liệu, hoặc nếu gói dữ liệu là một thông báo công cộng thì NIC sẽ sao chép gói dữ liệu này và gửi nó lên ngăn xếp giao thức.

IPX/SPX

Giao thức trao đổi gói tin IPX (Internetwork Packet exchange protocol) là một giao thức tầng mạng cung cấp dịch vụ phi giao kết (gam dữ liệu). (IPX đã được phát triển từ giao thức XNS do hãng Xerox đề xuất). Với tư cách là một giao thức tầng mạng, IPX chịu trách nhiệm về tiến trình định tuyến liên mạng và duy trì các địa chỉ logic mạng. Tiến trình định tuyến sử dụng giao thức RIP (sẽ mô tả sau) để tiến hành chọn các tuyến đường. IPX dựa trên các địa chỉ vật lý phần cứng tìm thấy tại các tầng phía dưới để cung cấp tính năng định địa chỉ thiết bị mạng. Nó cũng sử dụng các

sockets hoặc các địa chỉ dịch vụ tầng phía trên, để bàn giao các gói tin cho các đích sau của chúng.

IPX xác định hai kiểu địa chỉ:

**Địa chỉ liên mạng:** Địa chỉ này là của các segment trên mạng, nhận biết bằng số của mạng được ấn định trong suốt quá trình cài đặt.

**Địa chỉ nút nội bộ:** Địa chỉ này được xử lý bên trong một nút nó được nhận biết bằng số của socket.

Các giao thức IPX chỉ được sử dụng trên các mạng với các Netware server và nó thường được cài đặt với các giao thức khác phù hợp với nó như TCP/IP. Netware hoạt động theo hướng sử dụng TCP/IP như là một tiêu chuẩn.

Giao thức trao đổi gói tin tuần tự SPX (Sequenced packet exchange) là một giao thức tầng chuyển tải mở rộng IPX để cung cấp dịch vụ hướng giao kết có khả năng bàn giao đáng tin cậy. Khả năng bàn giao đáng tin cậy được bảo đảm bằng cách truyền lại các gói tin trong trường hợp bị lỗi. SPX xuất xứ từ một giao thức SPX tương tự trong bộ giao thức mạng XNS.

SPX thiết lập các mạng ảo có tên các tuyến giao kết [connection]. Số hiệu giao kết của mỗi tuyến giao kết xuất hiện trong phần đầu SPX. Tiến trình của một tầng phía trên có thể kết hợp với nhiều số hiệu giao kết. SPX được dùng trong các tình huống cần truyền dữ liệu đáng tin cậy. SPX lập chuỗi các gói tin dữ liệu. Việc thất lạc các gói tin hoặc các gói tin không đến theo thứ tự mà chúng đã được gửi đều được phát hiện ngay lập tức. Ngoài ra, SPX còn cung cấp tính năng dồn kênh giao kết, được dùng trong môi trường tin. Ví dụ, nhiều chương trình kế toán yêu cầu các dịch vụ của SPX để bảo đảm dữ liệu được truyền chính xác.

**Giao thức thông tin bộ định tuyến** RIP (Router information Protocol) dùng phương pháp phát hiện tuyến đường theo vectơ cự ly để xác định các tuyến đếm bước nhảy đến các thiết bị khác cũng như IPX, RIP đã được phát triển từ một giao thức tương tự trong bộ giao thức XNS. RIP được thực thi dưới dạng một dịch vụ tầng phía trên và được gán một ổ cắm (địa chỉ dịch vụ). RIP trực tiếp dựa vào IPX và thực hiện các chức năng tầng mạng. Một trường dữ liệu phụ được thêm vào trong gói dữ liệu để giải quyết việc chọn ra một con đường nhanh nhất để tới đích. Trong việc quảng bá các gói dữ liệu RIP cho phép:

- Các trạm làm việc có thể định vị một con đường nhanh nhất đến số mạng cần.
- Các bộ định tuyến có thể yêu cầu thông tin định tuyến từ một bộ định tuyến khác để cập nhật chúng vào bảng định tuyến bên trong của nó.

- Các bộ định tuyến có thể đáp ứng các yêu cầu định tuyến từ các trạm làm việc và các bộ định tuyến khác.
- Các bộ định tuyến có thể chắc chắn rằng các bộ định tuyến khác có trong cấu hình của liên mạng.
- Các bộ định tuyến có thể dò tìm được thay đổi trong cấu hình của liên mạng.

**Giao thức các dịch vụ nối kết mạng NLSP** (Network Link Services Protocol ) là một giao thức định tuyến trạng thái nối kết, xuất xứ từ một giao thức ISO có tên ISIS (intermediate system-to-in-termediate system). NLSP là một giao thức mới có trong NetWare 4.1 và cung cấp khả năng tương thích về trước với các bộ định tuyến IPX dùng RIP. NLSP có các thuật toán định tuyến trội vượt để định tuyến các gói tin đi qua một liên mạng một cách hiệu quả hơn. Hệ phục vụ tập tin NetWare 4.1 dùng NLSP sẽ duy trì một bản đồ liên mạng trong RAM và chỉ truyền bá các chi tiết thay đổi trên mạng. Điều này cho phép hệ phục vụ thực hiện các phép tính chính xác để tìm ra tuyến đường tốt nhất. Nhờ chỉ quảng bá các chi tiết thay đổi trên mạng, NLSP đã giảm thiểu được lượng lưu thông quá mức trên mạng do IPX RIP gây ra. NetWare 4.1 cho phép chọn dùng NLSP hoặc là IPX RIP truyền thống.

**Giao thức lõi NetWare NCP** (NetWare Core Protocol) cung cấp nhiều lệnh gọi hàm hỗ trợ các dịch vụ mạng, như dịch vụ tập tin, in, quản lý tên, khoá tập tin, và đồng bộ hoá. Phần mềm khách NetWare giao tiếp với NCO để truy cập các dịch vụ NetWare. NCP là một giao thức cấp cao cài sẵn trong lõi hệ điều hành NetWare. Giao thức này bao gồm các khía cạnh của phiên làm việc, phần trình bày và các tầng ứng dụng của Mô hình tham khảo OSI. NCP có ngôn ngữ thu nhỏ riêng mà các lập trình viên vận dụng khi viết các ứng dụng cho môi trường NetWare. Các lệnh NPC chủ yếu giải quyết việc truy cập các tập tin và thư mục trên hệ phục vụ tập tin. Các lệnh NCP được phân loại dưới dạng một yêu cầu hoặc một đáp ứng. Một yêu cầu NCP được gửi từ một hệ khách đến một hệ phục vụ. Một đáp ứng NCP được gửi từ hệ phục vụ trả về hệ khách.

Mọi yêu cầu và mọi đáp ứng đòi hỏi phải có một tín hiệu báo nhận. Điều này thường được gọi là hiệu ứng đối chuyền [ping-pong effect]. Trong vài trường hợp, chuỗi yêu cầu/ đáp ứng tuỳ thuộc vào một lời đáp từ hệ khách hay hệ phục vụ.

**Giao thức quảng cáo dịch vụ** SAP (Service Advertising Protocol) được các hệ phục vụ NetWare dùng để quảng cáo các dịch vụ của chúng trên mạng. Mỗi hệ phục vụ tự định danh mỗi phút một lần bằng cách truyền một gói tin SAP. Người dùng SAP cũng có thể yêu cầu thông tin về dịch vụ bằng cách truyền một gói tin truy vấn dịch vụ. Các thực thi SAP lấy thông tin địa chỉ dịch vụ từ thông tin phần đầu IPX. Với SAP việc

thêm vào hay gỡ bỏ các dịch vụ trên mạng sẽ được thực hiện động. Một gói dữ liệu SAP bao gồm:

- Thông tin điều hành - Chỉ rõ các thao tác mà gói dữ liệu sẽ thực thi
- Kiểu dịch vụ - Chỉ rõ các kiểu dịch vụ được cung cấp bởi server
- Tên server - Chỉ rõ tên của server quảng bá
- Địa chỉ mạng - Chỉ rõ số của mạng của server quảng bá.
- Địa chỉ nút - Chỉ rõ số của nút của server quảng bá.
- Địa chỉ socket - Chỉ rõ số của socket của server quảng bá
- Tổng số các bước nhảy đến server - Chỉ rõ số bước nhảy đến server quảng bá.
- Phạm vi hoạt động chỉ rõ kiểu yêu cầu
- Thông tin thêm cho thông tin về một hoặc nhiều server hoạt động trong lĩnh vực hoặc phạm vi này.

## 5.4 Giao thức NETBEUI

Hầu hết các dịch vụ và ứng dụng chạy trên các hệ thống dùng Windows đều sử dụng giao diện NetBIOS (Hệ thống vào ra cơ sở của mạng) hoặc truyền thông liên quá trình IPC. NetBIOS đã được phát triển trên mạng LAN và mở ra một giao diện tiêu chuẩn cho các ứng dụng sử dụng để truy nhập giao thức mạng tại lớp chuyển vận cho cả hai loại thông tin kết nối có liên kết và kết nối không liên kết. Giao diện NetBIOS đang sử dụng cho NetBEUI, NWLink, và TCP/IP. NetBIOS yêu cầu một địa chỉ IP và tên NetBIOS để nhận dạng duy nhất một máy tính.

NetBIOS thực hiện 4 chức năng sơ cấp:

- Phân giải tên NetBIOS mỗi trạm làm việc trên một mạng đều có một hoặc nhiều tên. NetBIOS duy trì một bảng tên và các biệt hiệu. Tên đầu tiên trong bảng là tên duy nhất của NIC. Chọn lựa các tên người sử dụng có thể dùng các tên thân thiện với người sử dụng và hệ thống vẫn nhận dạng được. NetBIOS sau đó sẽ bổ xung tên như yêu cầu.
- Dịch vụ gói dữ liệu NetBIOS. Chức năng này cho phép một thông báo được gửi đến nhiều tên, một nhóm tên, hoặc tất cả người sử dụng trên mạng. Tuy nhiên vì không sử dụng kiểu kết nối điểm - điểm nên không có sự bảo đảm thông báo sẽ đến được đích của nó.
- Dịch vụ phiên NetBIOS. Đây là dịch vụ mở một kết nối kiểu điểm - điểm giữa hai trạm làm việc trên mạng. Một trạm làm việc khởi xướng một cuộc gọi đến một trạm làm việc khác và mở kết nối. Bởi vì cả hai trạm làm việc này ngang hàng nhau nên cả hai có thể nhận và gửi dữ liệu đồng thời.

➢ NetBIOS NIC/trạng thái phiên. Đây là chức năng tạo thông tin về NIC vùng, mạng NIC khác, và các phiên đang hoạt động hiện tại nên một số phần mềm ứng dụng sử dụng NetBIOS.

**NetBEUI**

NetBEUI là chữ viết tắt của NetBIOS Extended User Interface. Ban đầu NetBIOS và NetBEUI có quan hệ chặt chẽ với nhau và được xem như một giao thức. Tuy nhiên một vài mạng khác sử dụng NetBIOS ở giao thức của lớp phiên, vì vậy mà nó có thể được sử dụng với giao thức của lớp chuyển vận. NetBIOS (hệ thống vào/ ra cơ bản của mạng) là một giao diện LAN ở lớp phiên của IBM mà hoạt động như một giao diện ứng dụng mạng. NetBIOS cung cấp công cụ cho một chương trình để thiết lập một phiên với một chương trình khác qua mạng, bởi vì nhiều chương trình ứng dụng hỗ trợ nó.

NetBEUI là giao thức ở lớp chuyển vận, nó nhỏ, nhanh và hiệu quả, nó cung cấp cho tất cả các sản phẩm của Microsoft Network. Nó có từ giữa năm 1980 và đã cung cấp cho sản phẩm mạng đầu tiên của Microsoft là MS-NET.

Ưu điểm của NetBEUI là ngăn xếp của nó nhỏ (điều quan trọng cho máy tính chạy trên MS-DOS), tốc độ truyền dữ liệu trên mạng là trung bình, và tương thích với tất cả các mạng cơ bản của Microsoft.

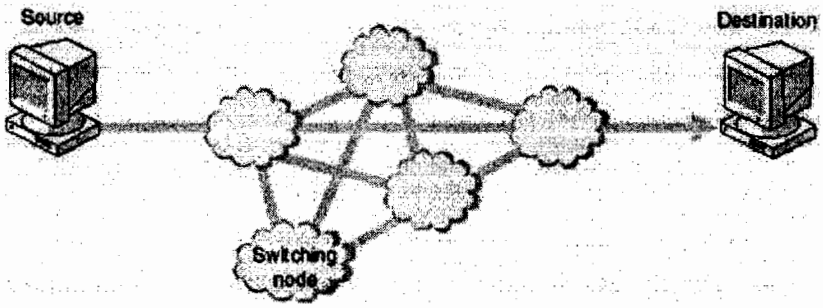
Nhược điểm của NetBEUI là nó không hỗ trợ cho việc định tuyến. Nó cũng giới hạn ở các mạng cơ bản của Microsoft. NetBEUI là một giải pháp tốt và kinh tế cho các mạng nhỏ kiểu peer-to-peer ở đó tất cả các trạm làm việc sử dụng hệ điều hành Microsoft.

## 5.5 Các bộ giao thức khác

### 5.5.1 Giao thức X25

X25 là một giao thức được sử dụng trong mạng chuyển mạch gói. Mạng chuyển mạch gói được sinh ra để phục vụ các dịch vụ chuyển mạch nhằm thiết lập các kết nối đầu cuối ở xa đến các hệ thống máy chủ lớn.

Một mạng chuyển mạch gói X25 như chỉ ra trong hình 5.9 sử dụng các bộ chuyển mạch, các mạch dẫn, các bộ định tuyến có sẵn để cung cấp một tuyến đường ngắn nhất. Các bộ này có thể thay đổi một cách nhanh chóng tuỳ thuộc vào sự cần thiết và những thứ sẵn có, chúng được vẽ như những đám mây.



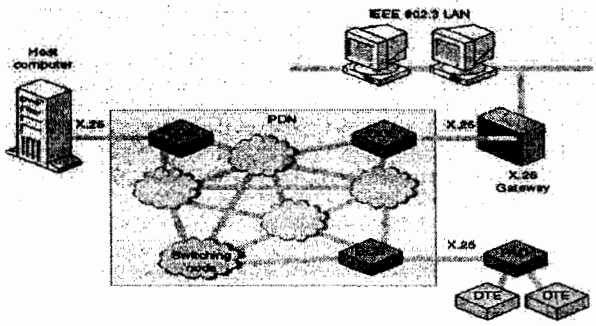

**Hình 5.9 Mạng chuyển mạch gói X25**

Thời kì đầu X25 sử dụng đường điện thoại để truyền dẫn dữ liệu. Phương tiện này không đáng tin cậy do có các lỗi tần số, vì vậy X25 đã phải dùng thêm các bộ kiểm tra lỗi ở bên ngoài. Do hậu quả của việc sử dụng các bộ kiểm tra lỗi và việc truyền lại nên X25 chậm.

Ngày nay giao thức X25 được định nghĩa là giao diện giữa một máy chủ hoặc thiết bị khác hoạt động theo kiểu chuyển mạch gói đồng bộ và mạng số liệu công cộng PDN thông qua một đường truyền riêng hoặc một đường cho thuê. Giao diện này là một giao diện kiểu DTE/DCE (thiết bị đầu cuối số liệu/thiết bị truyền thông tin).

Ví dụ về cấu trúc của DTE bao gồm:

- Một máy chủ với giao diện X25.
- Một bộ đóng và mở gói (PAD) bộ này nhận các ký tự không đồng bộ được đưa tới từ các đầu cuối tốc độ thấp và tập hợp chúng thành các gói dữ liệu để truyền dẫn qua mạng. Bộ PAD mở các gói nhận được từ mạng và phân phát đến các đầu cuối.
- Một cổng gateway giữa PDN và một mạng LAN hay WAN.




**Hình 5.10 Các ví dụ của DTEs**

Trong việc cài đặt các giao thức của mạng WAN, X25 được kết hợp chặt chẽ trong mạng chuyển mạch gói tạo lên các dịch vụ chuyển mạch. Các dịch vụ chuyển mạch này thiết lập các kết nối từ các trạm đầu cuối (DTE) xa đến các hệ thống máy chủ lớn (host computer). Mạng này sẽ bị tắc nghẽn mỗi khi có nhiều gói dữ liệu được vận chuyển đến cùng một vị trí trên mạng. Đường dẫn giữa các nút là một mạch ảo trông giống như một đường đơn, liên tục, đây là một kết nối logic tới một lớp cao hơn.

Mỗi gói dữ liệu có thể đi theo các tuyến đường khác nhau để tới đích. Sau khi các gói dữ liệu đến chúng sẽ được lắp ráp lại thành gói dữ liệu ban đầu.

Một gói bao gồm 128 byte dữ liệu; tuy nhiên địa chỉ nguồn và đích có thể làm cho kích thước của các gói dữ liệu khác nhau và nó vượt quá 128 byte. Theo lý thuyết giao thức X25 có thể hỗ trợ lớn nhất là 4095 mạng ảo đồng thời qua một đường vật lý giữa một nút và mạng X25. Tốc độ truyền dữ liệu của X25 là 64 Kbit/s.

Giao thức X25 làm việc tại lớp vật lý, lớp liên kết dữ liệu và lớp mạng của mô hình tham chiếu OSI. Nó có từ giữa năm 1979 và được dùng để gỡ rối, nó là một môi trường mạng ổn đinh. Tuy nhiên nó có hai thiếu sót:

- Việc lưu và gửi là nguyên nhân làm cho cơ cấu bị chậm. Với kiểu chuyển mạch này sẽ tạo ra thời gian trễ khoảng 6 ms và không hiệu quả đối với các dữ liệu kiểu khối lớn. Tuy nhiên với kiểu truyền dẫn kiểu mạch lật Flip-Flop trễ này có thể trông thấy.
- Cần một bộ nhớ đệm lớn để lưu và gửi dữ liệu.

X25 và TCP/IP đồng thời có thể sử dụng làm giao thức của mạng chuyển mạch gói. Tuy nhiên có một vài sự khác sau giữa chúng:

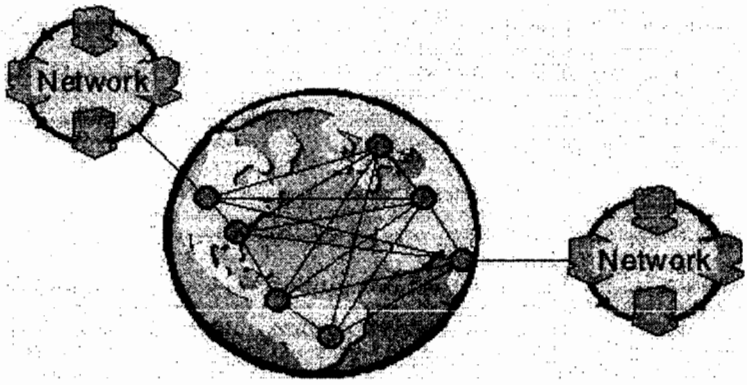
- TCP/IP chỉ kiểm tra lỗi đầu cuối - đầu cuối và điều khiển lưu lượng; X25 không kiểm lỗi từ nút này đến nút kia
- Công việc bù đối với mạng TCP/IP là hoàn toàn thụ động, TCP/IP có nhiều phức tạp trong việc điều khiển lưu lượng.
- X25 yêu cầu sự chặt chẽ về các mức đường và điện, TCP/IP được thiết kế để vận chuyển qua nhiều phương tiện khác nhau, với nhiều kiểu đường dịch vụ.

### 5.5.2 Giao thức Frame relay

Giống như mạng thông tin phát triển theo hướng số hoá và dùng môi trường truyền dẫn sợi quang các công nghệ mới đang xuất hiệu thoả mãn yêu cầu kiểm tra lỗi bít ít hơn so với phương pháp chuyển mạch gói tương tự thời kỳ đầu.

Frame relay là một ưu điểm của công nghệ chuyển mạch gói đó là: nhanh, độ dài thay đổi, số hoá. Với công nghệ này thì việc thiết kế X25 không cần dùng nhiều các bộ kiểm tra lỗi vì môi trường truyền dẫn là sợi quang.

Frame relay được chỉ ra trong hình 5.11 là một hệ thống theo kiểu điểm-điểm sử dụng một đường chuyển mạch ảo để truyền dẫn các khung có độ dài thay đổi ở lớp liên kết dữ liệu. Dữ liệu này được vận truyển từ một mạng và thông qua một đường cho thuê để tới mạng frame relay và được chuyển đến mạng đích.




**Hình 5.11 Frame relay sử dụng một hệ thống điểm -điểm**

Các mạng Frame relay rất được ưu chuộng bởi vì chúng nhanh hơn các hệ thống chuyển mạch khác ở thao tác chuyển mạch cơ bản. Bởi vì frame relay dùng đường dẫn ảo PVC, vì vậy toàn bộ các đường dẫn từ đầu cuối tới đầu cuối đều được biết trước. Không cần có thêm các thiết bị frame relay làm nhiệm vụ tháo gói và lắp ráp gói, hoặc cung cấp một đường đi tốt nhất.

Các mạng Frame relay cũng cung cấp một độ rộng băng tần cần thiết và khách hành có thể chọn lựa kiểu truyền dẫn.

Công nghệ Frame relay yêu cầu một bộ định tuyến hoặc một cầu Frame relay có đủ khả năng để vận chuyển dữ liệu qua mạng. Một bộ định tuyến Frame relay cần ít nhất một cổng WAN để kết nối mạng frame relay với các cổng khác của LAN.

### 5.5.3 Giao thức ATM

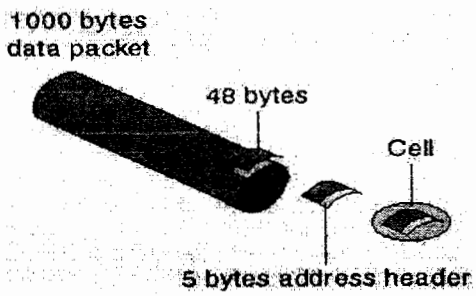
Công nghệ truyền dẫn không đồng bộ ATM là một ưu điểm bổ xung của công nghệ chuyển mạch gói, nó cung cấp một tốc độ truyền dữ liệu cao với việc gửi đi các gói tin có kích cỡ không đổi thông qua băng tần rộng và băng tần cơ sở của LANs và WANs. ATM có thể phù hợp với các loại hình sau:

- Thoại
- Số liệu
- Fax
- Video thời gian thực
- Audio chất lượng cao
- Hình ảnh
- Truyền dữ liệu đa Mbit

CCITT đã định nghĩa ATM vào năm 1988 như một phần của mạng số liên kết đa dịch vụ băng rộng B-ISDN. Độ rộng băng tần của ATM có thể được gán một cách linh hoạt tuỳ thuộc vào sự phát triển của thông tin trên mạng. Nó đều có thể thích ứng với môi trường LAN và WAN và nó có thể truyền dẫn dữ liệu ở tốc độ rất cao (155 Mbít/s đến 622 Mbit/s hoặc cao hơn).

**Công nghệ ATM**

ATM là một tế bào được truyền tải trong mạng băng rộng, tế bào của nó gồm 53 byte. Hình 5.12 là cấu trúc của tế bào ATM. Tế bào này có 48 byte chứa thông tin ứng dụng và 5 byte thêm vào phần đầu của tế bào. Ví dụ ATM muốn chia gói dữ liệu gồm 1000 byte thành 21 khung và đặt mỗi khung dữ liệu này vào trong một tế bào. Các gói này là đồng dạng nhau.




**Hình 5.12 Dạng khung tin ATM**

Các thiết bị của mạng có thể chuyển mạch, định đường và vận chuyển các khung có kích cỡ giống nhau này nhanh hơn là các khung có kích cỡ ngẫu nhiên. Với các tế bào có kích cỡ tiêu chuẩn sẽ làm giảm công việc xử lý dữ liệu tại các bộ nhớ đệm. Kích cỡ của các tế bào giống nhau cũng giúp cho kế hoạch ứng dụng băng rộng.

ATM có tốc độ lưu lượng lên tới 1,2Gbit/s. Hiện nay nhờ sử dụng cáp quang tốc độ này có thể được trải ra ở 622 Mbít/s. Hầu hết các đường ATM phục vụ cho mục đích thương mại đều sử dụng tốc độ 155Mbit/s. ATM có thể được sử dụng trong mạng LAN và WAN.

**Thành phần của ATM** hiệu nay chỉ giới hạn ở một số nhà cung cấp. Tất cả các phần cứng của mạng ATM đều phải tương thích với ATM. Các phương tiện hiện nay muốn tương thích với ATM đều phải có các thiết bị mở rộng để thay thế. Đây là lý do tại sao ATM không được áp dụng và được triển khai nhanh. Tuy nhiên ATM được một số hãng khác nhau cung cấp:

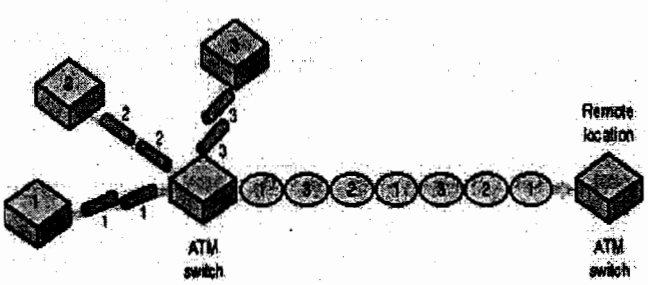
- Bộ định tuyến và chuyển mạch cho nối kết các dịch vụ trên toàn cầu.
- Trục chính (backbone) kết nối các mạng LAN bên trong một tổ chức hoặc cơ quan lớn.
- Các bộ chuyển mạch và các bộ chuyển đổi phục vụ cho việc kết nối các máy tính để bàn với đường ATM tốc độ cao để có thể chạy các ứng dụng đa phương tiện.

**Phương tiện truyền dẫn của ATM** ATM không tự bị giới hạn bởi các kiểu phương tiện truyền dẫn khác nhau. Nó có thể sử dụng các phương tiện truyền dẫn hiện có cho các hệ thống thông tin khác nhau:

- Cáp đồng trục
- Cáp xoắn
- Cáp sợi quang.

Tuy nhiên các phương tiện mạng truyền thống hiện nay không hỗ trợ tất cả các khả năng của ATM. Một tổ chức gọi là ATM Forum giới thiệu các giao diện vật lý cho ATM như sau:

- FDDI (100Mbit/s)
- Kênh quang (155Mbit/s)
- SONET OC3 (155Mbit/s)
- T3 (45Mbit/s).
- Các giao diện khác bao gồm frame relay và X25




**Hình 5.13 Ghép các gói dữ liệu ở đầu vào bộ ghép kênh của chuyển mạch ATM**

**Các bộ chuyển mạch ATM** Các thiết bị chuyển mạch ATM là thiết bị đa cổng, nó có thể hoạt động theo hai dạng thức sau:

- Như Hub gửi chuyển tiếp dữ liệu từ một máy tính đến một máy tính khác ở trong cùng một mạng

➢ Như một bộ định tuyến để chuyển tiếp dữ liệu tốc độ cao đến các mạng ở xa.

Trong một vài kiến trúc mạng như Ethernet và Token Ring, trong một thời điểm chỉ có một máy tính được phép truyền dữ liệu. Trong hình 5.13 cả ba bộ định tuyến router cùng cung cấp dữ liệu vào bộ chuyển mạch ATM vào cùng một thời điểm.

Công nghệ ATM yêu cầu một phần cứng chuyên dụng và một độ rộng băng tần đặc biệt. Các ứng dụng hỗ trợ cho video hoặc thoại chiếm hầu hết trong các môi trường mạng nó làm thất bại những cố gắng của người sử dụng trong việc sử dụng mạng cho mục đích thương mại bình thường. ATM yêu cầu phải có một sự thành thạo trong việc sử dụng nó.

### 5.5.4 Giao thức ISDN

Mạng số đa dịch vụ (ISDN) có tính năng như một mạng LAN số, nó hỗ trợ cả thoại, dữ liệu và hình ảnh. Mục tiêu đầu tiên của ISDN là phát triển các đường đến từng nhà và từng nơi buôn bán bằng hệ thống dây điện thoại. ISDN đã thực thi kế hoạch thay đổi các mạch điện thoại hiện tại từ dạng tương tự sang dạng số. Kế hoạch này đã và đang được tiến hành trên toàn thế giới.

Tốc độ cơ bản của ISDN: Độ rộng băng của nó được chia thành 3 kênh số chính. Hai kênh trong số này truyền dẫn ở tốc độ 64 kbít/s. Kênh thứ ba truyền dẫn ở tốc độ 16kbit/s.

Các kênh 64kbít/s được biết giống như là các kênh cơ sở kiểu B. Các kênh này mang thông tin thoại, số liệu và hình ảnh. Kênh chậm hơn 16kbit/s gọi là kênh D. kênh D mang thông tin báo hiệu và dữ liệu quản lý đường. Tốc độ cơ sở của dịch vụ ISDN gọi là 2B+D.

Một máy tính kết nối tới dịch vụ ISDN có thể sử dụng cả hai kênh B đồng thời cho một luồng dữ liệu 128 kbit/s.

Tốc độ sơ cấp của ISDN sử dụng toàn bộ độ rộng băng tần của đường T1 bằng việc cung cấp 23 kênh B ở 64kbit/s và một kênh D ở 64 kbit/s. Kênh D được sử dụng cho báo hiệu và quản lý.

Trong chiến lược sử dụng dịch vụ ISDN ta nên cân nhắc việc chọn lựa tốc độ cơ sở hay tốc độ sơ cấp tuỳ thuộc lưu lượng dữ liệu. ISDN là sự số hoá cho mạng PSTN và dịch vụ quay số. Nó không phải được thiết kế cho các dịch vụ đáp ứng 24 giờ như T1 hay dịch vụ có độ rộng băng yêu cầu giống như frame relay.

# CHƯƠNG 6

# KẾT NỐI LIÊN MẠNG

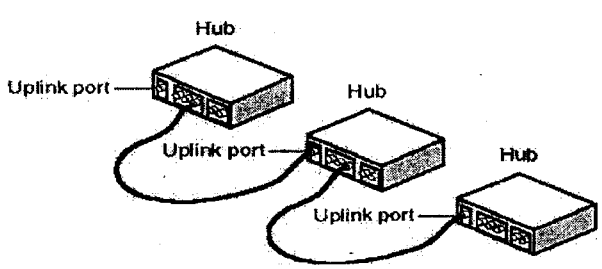
## 6.1 Các thiết bị kết nối liên mạng

Sau một thời gian khai thác sử dụng một mạng LAN do xu thế phát triển thường xuất hiện các nhu cầu mở rộng mạng LAN như bổ xung một số máy vào mạng, mở rộng khoảng cách, kết nối hai mạng LAN với nhau hay kết nối mạng LAN với một mạng diện rộng lớn hơn như mạng WAN hay mạng Internet. Hiển nhiên một mạng không thể mở rộng bằng cách thêm máy tính và kéo dài đây cáp do các giới hạn về kiến trúc vật lý và cấu hình mạng vì thế để đáp ứng nhu cầu nâng cấp mở rộng mạng ta phải sử dụng các thành phần liên kết mạng như sau:

- HUB.
- Bộ lặp (Repeaters).)
- Cầu nối (Bridges).)
- Bộ định tuyến (Routers).
- Bộ định tuyến cầu (Brouters).
- Cổng kết nối (Gateways).

**HUB**

Trong các chương trước đã đề cập cách sử dụng các Hub như là thiết bị kết nối trung tâm trong mạng hình sao cũng như trong mạng Token ring. Hub còn có khả năng sử dụng như là một thiết bị mở rộng kích cỡ mạng bằng các kết nối bổ xung các Hub vào mạng LAN như hình 6.1 mô tả phương pháp bổ xung Hub cho mạng 10BASET, phương pháp này được sử dụng khá phổ biến để tăng số lượng các trạm làm việc trên mạng tuy nhiên nó không thể kết nối một mạng LAN vào mạng WAN.



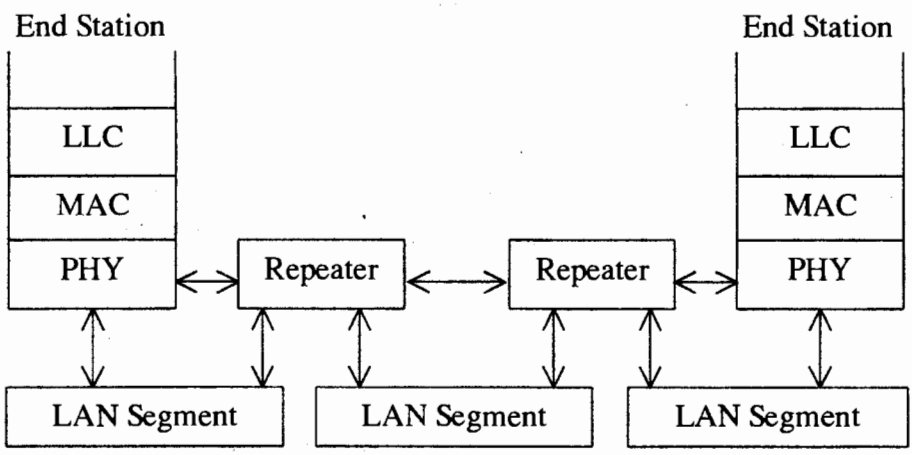

**Hình 6.1 Ethernet hubs kết nối thành chuỗi**

Sơ đồ đấu nối cáp UTP giữa hai Hub khác với việc đấu nối từ Hub tới máy tính, Cách đấu nối được thể hiện như sau:

| ***Đầu chuẩn*** | ***Đầu còn lại*** |
|---|---|
| Chốt 1: Trắng/Da cam | Chốt 1: Trắng/Xanh lá cây |
| Chốt 2: Da cam | Chốt 2: Xanh lá cây |
| Chốt 3: Trắng/Xanh lá cây | Chốt 3: Trắng/Da cam |
| Chốt 4: Xanh nước biển | Chốt 4: Xanh nước biển |
| Chốt 5: Trắng/ Xanh nước biển | Chốt 5: Trắng/ Xanh nước biển |
| Chốt 6: Xanh lá cây | Chốt 6: Da cam |
| Chốt 7: Trắng/Nâu | Chốt 7: Trắng/Nâu |
| Chốt 8: Nâu | Chốt 8: Nâu |

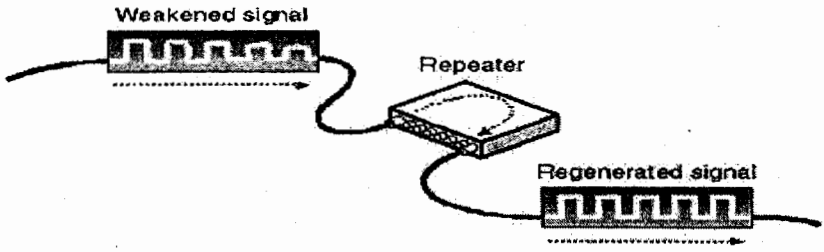
## Bộ phát lặp

Tín hiệu được truyền dọc theo chiều dài cáp nối và nó sẽ bị suy hao, nếu khoảng cách quá dài bên thu có khả năng nhận sai tín hiệu. Trong trường hợp này bộ phát lặp được sử dụng với mục đích khuyếch đại lại tín hiệu vật lý trên đường truyền và như vậy Bộ phát lặp làm việc tại lớp vật lý theo mô hình tham chiếu OSI, hình 6.2




**Hình 6.2 bộ phát lặp trong mô hình tham chiếu OSI**

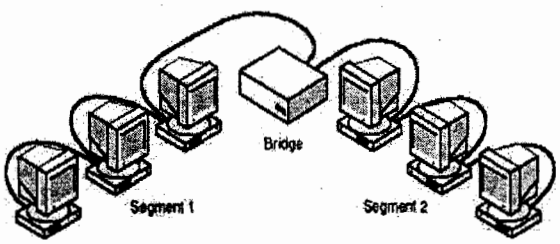
Hình 6.3 biểu diễn phương thức hoạt động của bộ phát lặp, nó tiếp nhận tín hiệu yếu từ một phân đoạn mạng này, tái tạo lại và chuyển nó tới một phân đoạn khác của mạng.




**Hình 6.3 Khuếch đại tín hiệu trong bộ phát lặp**

Bộ phát lặp chỉ hỗ trợ cho cùng một phương thức truy nhập mạng, nó không thể kết nối hai đoạn mạng có phương pháp truy nhập khác nhau ví dụ như mạng 802.3 LAN (Ethernet) và 802.5 LAN (Token Ring). Bộ phát lặp cũng không thể phiên dịch các gói tin và lọc gói tin. Hai phương thức truy nhập hay sử dụng bộ phát lặp là CSMA/CD token passing.

Bộ phát lặp là phương thức rẻ tiền nhất để mở rông một mạng theo hai hình thức: khoảng cách (lý do chính) và có thể tăng cả số lượng máy trạm làm việc. Tuy nhiên do không có tính năng lọc và loại trừ các gói tin không cần thiết giữa các đoạn mạng vì vậy khi số lượng máy tính ở các đoạn mạng tăng thì vẫn ảnh hưởng đến lượng lưu thông trên mạng. Không nên dùng bộ lặp để mở rộng một mạng đã có tải lới hoặc mạng yêu cầu lọc gói tin hai có từ hai phương thức truy nhập trở lên.




**Hình 6.4 Bộ cầu nối kết nối hai mạng**

**Bộ cầu nối**

Cũng giống như bộ phát lặp, bộ cầu nối có thể kết nối nhiều phân đoạn mạng LAN hay nhiều các nhóm làm việc LAN khác nhau vào với nhau. Hình 6.4 mô tả việc việc ghép nối hai đoạn mạng khác nhau trong một mạng bằng bộ cầu nối. Hơn nữa bộ cầu nối còn có thể chia một mạng thành các tuyến mạng độc lập. Bộ cầu nối có thể sử dụng để:

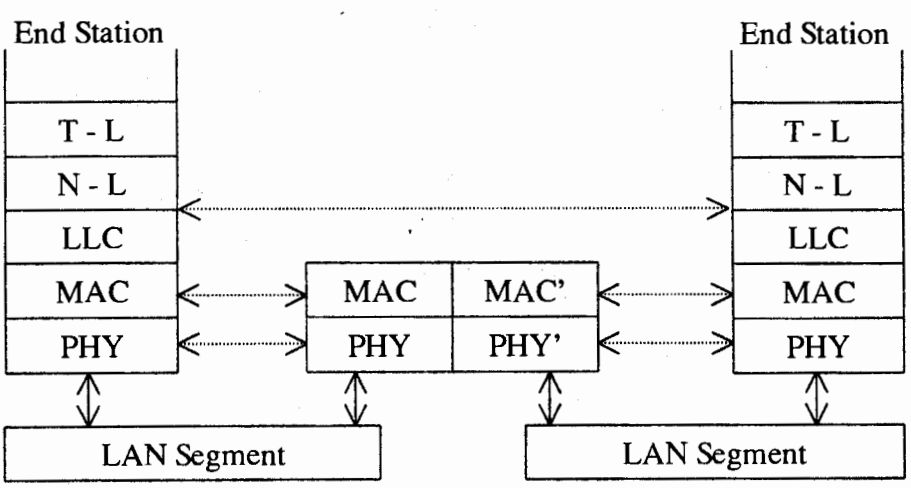
- Tăng chiều dài của một đoạn mạng

- Tăng số lượng máy tính trên mạng
- Giảm sự quá tải trên mạng do quá nhiều máy tính đấu vào mạng
- Chia một mạng đang quá tải thành hai mạng riêng để giảm tải trên mỗi đoạn mạng giúp cho mạng làm việc hiệu quả hơn

Cầu nối làm việc tương ứng với lớp 2- Lớp liên kết dữ liệu trong mô hình OSI (hình 6.5).

Như ta đã biết lớp liên kết dữ liệu được chia thành 2 lớp con: lớp điều khiển liên kết LLC và lớp điều khiển truy nhập MAC. Bộ cầu nối làm việc tại lớp MAC vì thế còn hay được gọi là bộ cầu nối MAC, nó làm việc như sau:

- Lắng nghe thông tin trên mọi hướng của mạng
- Kiểm tra địa chỉ nguồn và địa chỉ đích của mỗi một gói tin (địa chỉ vật lý)
- Xây dựng bảng đụnh tuyến đường đưới dạng thông tin chỉ dẫn
- Chuyển tiếp gói tin theo các nguyên tắc sau:
  - Nếu địa chỉ đích không có trong bảng định tuyến, nó sẽ chuyển tiếp gói tin này tới tất cả các phân đoạn của mạng.
  - Nếu địa chỉ đích có trong bảng định tuyến, nó sẽ chuyển tiếp gói tin này tới phân đoạn chứa địa chỉ đích.



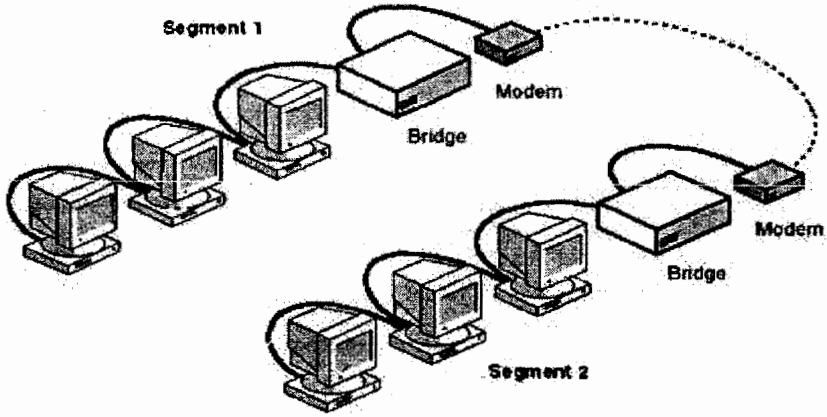

**Hình 6.5 Bộ cầu nối trong mô hình tham chiếu OSI**

Bộ cầu nối làm việc theo nguyên tắc mỗi một nút mạng phải có địa chỉ riêng của nó, cầu nối sẽ chuyển tiếp gói tin trên cơ sở địa chỉ của nút đích. Thông thường các bộ cầu nối có các cấp độ thông minh khác nhau trong việc định luồng chuyển tiếp số liệu. Tất cả luồng thông tin đều được chuyển qua cầu nối, các thông tin về địa chỉ của các

máy tính trên mạng sẽ được lưu trong RAM của cầu nối và được nó sử dụng để xây dựng bảng định tuyến và phân phân biệt xem máy tính nào thuộc phân đoạn nào của mạng

Vì bộ cầu nối là một công cụ rất mạnh trong việc mở rộng và phân đoạn hoá mạng nên nó thường được sử dụng trong các mạng lớn mà các mạng này thường có nhu cầu truy nhập từ xa qua mạng điện thoại. Bình thường chỉ cần một cầu nối cho hai đoạn mạng, tuy nhiên khi khi có hai mạng LAN riêng biệt nằm ở các khoảng cách xa nhau vẫn có thể nối chung thành một một mạng, để thực hiện điều này cần hai bộ cầu nối xa được nối với nhau các Modem đồng bộ sử dụng đường thoại riêng như hình 6.6

Sự khác nhau giữa cầu nối và bộ lặp ở chỗ bộ cầu nối làm việc ở mức hai trong mô hình OSI, điều đó có nghĩa nó thông minh hơn bộ phát lặp và có thể xử lý được một số tính chất của dữ liệu, cũng giống như bộ lặp bộ cầu nối tái tạo lại số liệu song nó tái tạo lại ở mức gói tin vì thế có thể gửi các gói tin này tới một khoảng cách xa nhờ các phương tiện truyền dài. Bộ cầu nối cung cấp cho mạng hiệu năng tốt hơn là bộ lặp vì cầu nối có thể chia mạng thành các phân đoạn nhỏ ví dụ như một mạng Ethernet lớn có thể chia thành hai phân đoạn kết nối với nhau qua bộ cầu nối, mỗi một mạng mới có ít lượng gói tin vận chuyển hơn và ít bị xung đột hơn.

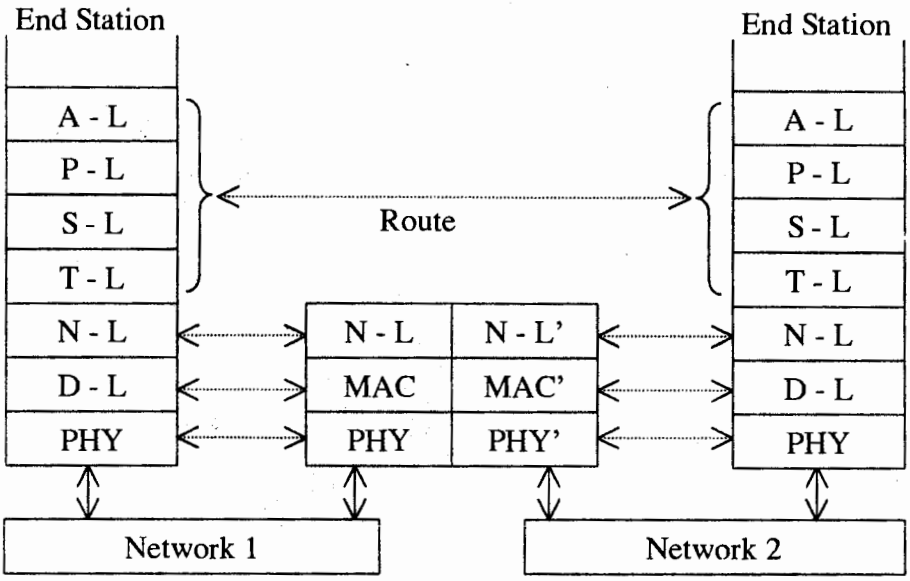



**Hình 6.6 Bộ cầu nối xa**

Việc cài đặt bộ cầu nối có thể như một thiết bị đứng độc lập hoặc có thể cài đặt bên trong máy chủ. Nếu hệ điều hàng mạng cho phép có dùng một hoặc nhiều cạc mạng NIC làm cầu nối trong của mạng. Các nhà quản trị mạng thích dùng giải pháp cầu nối vì:

- Đơn giản và trong suốt đối với người sử dụng
- Cơ động và dễ ghép nối

- Giá thành vừa phải.




**Hình 6.7 Bộ định tuyến trong mô hình OSI**

**Bộ định tuyến**

Trong môi trường chứa nhiều đoạn mạng cùng với các kiểu kiến trúc và giao thức khác nhau bộ cầu nối có thể không thích hợp cho việc đảm bảo liên lạc tốc độ cao trên tất cả các đoạn mạng. Tổng thể một mạng không chỉ cần một thiết bị phân biệt các địa chỉ mạng trên từng phân đoạn mà còn cần phải thực hiện tìm một tuyến đường đi tốt nhất cho việc gửi dữ liệu và lọc các luồng thông tin quảng bá tới phân đoạn mạng tại chỗ. Thiết bị đáp ứng yêu cầu này chính là bộ định tuyến (Router).

Bộ định tuyến làm việc tại lớp mạng trong mô hình OSI (hình 6.7), điều đó có nghĩa là nó có thể chuyển mạch và tìm đường cho các gói tin thông qua liên mạng.

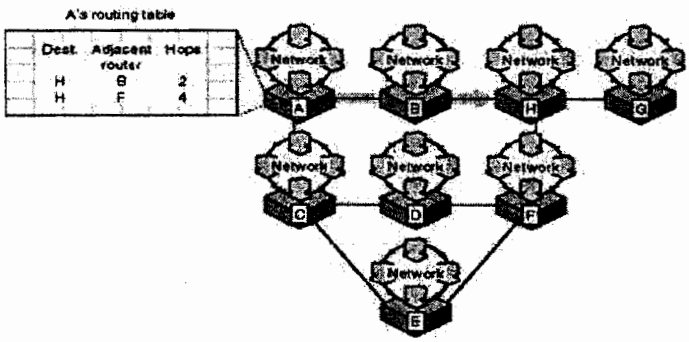
Để thức hiện việc đó, bộ đính tuyến trao đổi các thông tin đặc chủng về giao thức giữa các mạng riêng biệt. Router đọc thông tin định địa chỉ của liên mạng trong các gói tin và với chức năng ở lớp mạng (khác với bộ cầu nối) nó có thể bổ xung thêm thông tin để tăng chất lượng chuyển giao gói tin mặc dù các tính năng như bộ cầu nối nó vẫn đảm bảo.

Bộ định tuyến luôn duy trì bảng định tuyết riêng của mình, nó thường chứa các địa chỉ mạng, địa chỉ máy tính mạng, thậm chí cả kiến trúc mạng mỗi khi có cơ hội. Để

thực hiện việc định địa chỉ đích cho các gói tin đến trong bảng định tuyến sẽ bao gồm các nội dung sau:

- Tất cả các địa chỉ mạng hiện có
- Thủ tục kết nối với các mạng khác
- Các tuyến đường kết nối giữa các bộ định tuyến.
- Mức độ tổn phí (giá thành) của thông tin khi qua các tuyến đường ấy

Hình 6.8 cho ví dụ Router sử dụng bảng định tuyến của mình để chọn đường đi tốt nhất.




**Hình 6.8 Ví dụ các Router trong liên mạng**

Bộ định tuyến cũng phải có địa chỉ riêng, chúng chỉ cần hiểu địa chỉ mạng để có thể liên lạc được với các Router khác và các địa chỉ NIC của mạng nội tại . Chúng không nói chuyện với các máy tính mạng khác. Khi router nhận được các gói tin có địa chỉ mạng xa, nó sẽ chuyển chúng cho router quản lý mạng xa ấy. Chi tiết về cách tìm đường của router sẽ đề cập ở phần sau.

**Brouters**

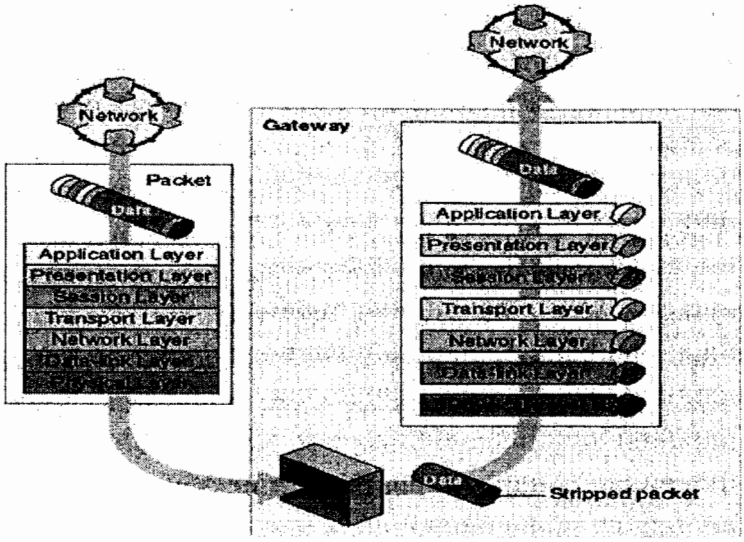
Brouter, như tên gọi Brigde- router, nó là thiết bị tổ hợp cả hai cầu nối và bộ định tuyến. Brouter có thể làm việc như một bộ định tuyến cho một giao thức cụ thể hoặc là cầu nối cho mọi loại giao thức

**Cổng kết nối**

Cổng để kết nối hai hệ thống không sử dụng cùng một kiểu sau:

- Giao thức kết nối truyền thông
- Cấu trúc định dạng cơ sở dữ liệu
- Ngôn ngữ
- Kiến trúc mạng

Cổng kết nối làm việc tại tất cả các lớp của mô hình OSI như hình 6.9




**Hình 6.9 Cổng nối trong mô hình OSI**

Thoạt đầu, thuật ngữ gateway được dùng trong bộ giao thức Internet để chỉ bộ định tuyến. Ngày nay, cổng nối gateway thường ám chỉ một hệ thống hoạt động tại các cấp trên cùng của mô hình OSI (Tầng phiên làm việc, Phiên trình bày, ứng dụng), cho phép truyền thông giữa các hệ giao thức tầng phía trên không giống nhau. Có thể thực thi gateway dưới dạng phần mềm, phần cứng, hoặc tổ hợp cả hai.

## 6.2 Các đường kết nối liên mạng

Trong phần này chúng ta sẽ xem xét các dịch vụ nối kết khác nhau mà chúng ta có thể dùng với các phần cứng kết nối liên mạng đã được miêu tả ở phần trên..

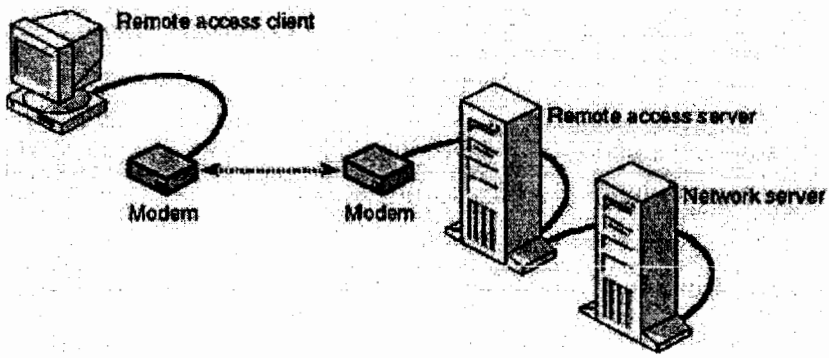
**Đường điện thoại**

Có hai loại đường điện thoại được sử dụng cho việc kết nối mạng qua modem: Đường quay số và đường thuê riêng. Đường quay số là đường điện thoại thông dụng nhưng tốc độ của chúng thấp và yêu cầu người sử dụng phải thao tác đấu nối bằng tay, nó không đáng tin cậy cho việc truyền dữ liệu. Tuy nhiên, nó vẫn được một số công ty sử dụng để truyền file và cập nhật cơ sở dữ liệu-thời gian ít. Đường thuê riêng cách này cho phép bạn kết nối toàn bộ thời gian. Bạn không phải dùng bất cứ một sự chuyển mạch nào cho việc kết nối. Chất lượng của đường loại này cao hơn so với đường điện thoại chỉ truyền dẫn tiếng nói. Phạm vi tốc độ của nó từ 56kbit/s đến 45 Mbit/s hoặc cao hơn.

**Dịch vụ truy nhập từ xa (RAS)**

Người sử dụng có thể yêu cầu thông tin từ nhiều mạng khác chứ không phải chỉ ở một mạng. Nhiều hệ thống mạng có thể cung cấp các dịch vụ đó, gọi là dịch vụ truy cập từ xa (RAS). Việc thiết lập đấu nối cần có hai dịch vụ: RAS và dịch vụ clien giống như mạng quay số (DUN). Máy chủ hoặc máy tính trạm sử dụng dịch vụ RAS để nối một máy tính ở xa với mạng bằng việc sử đụng đường điện thoại và quay số đến qua modem. Mặt khác DUN là dịch vụ mà máy tính ở xa sử dụng để kết nối đến máy chủ server RAS. Hai dịch vụ này đều cung cấp một khả năng mở rộng mạng nó có hiệu quả đối với mạng LAN và WAN. Bởi vì nhiều dịch vụ Internet cung cấp việc truy nhập qua đường điện thoại. Một vài máy tính và mạng LAN có thể nối kết vào nhau qua mạng điện thoại chuyển mạch công cộng PSTN, mạng chuyển mạch gói, mạng dịch vụ số ISDN

Hình 6.10 chỉ ra việc kết nối một client ở xa đến server của một mạng sử dụng RAS.




**Hình 6.10 Cách kết nối máy tính từ xa tới mạng**

**Đấu nối RAS:** Đấu nối vật lý đến server RAS có thể dùng một vài phương tiện vận chuyển khác nhau như sau:

- Mạng chuyển mạch điện thoại công cộng (PSTN) Đây là dịch vụ được hiểu như là hệ thống điện thoại công cộng
- Mạng chuyển mạch gói X25. Đây là mạng chuyển mạch gói sử dụng kiểu quay số hoặc là đấu nối trực tiếp.
- Mạng số đa dịch vụ (ISDN) Đây là dịch vụ cung cấp đường truy nhập tốc độ cao, nhưng giá thành đắt hơn nhiều so với dịch vụ quay số. Một đấu nối ISDN yêu cầu một card ISDN đặt bên trong modem.

**Giao thức RAS:** RAS hỗ trợ 3 giao thức đấu nối. Cũ nhất năm 1984 là giao thức SLIP tuy nhiên nó có một số thiếu sót. SLIP không hỗ trợ địa chỉ IP động hoặc giao thức IPX hoặc NetBEUI, nó không thể đăng nhập thông tin mật mã, và nó chỉ hỗ trợ các RAS client. Giao thức điểm-điểm (PPP) khắc phục được những giới hạn của SLIP. Với việc thêm TCP/IP, nó hỗ trợ các giao thức IPX, NetBEUI, AppleTalk và DECnet. Nó cũng hỗ trợ mật mã bằng password. Giao thức PPTP (Point-to-Point Tunneling Protocol) là một phần của công nghệ mạng riêng ảo (VPN). Giống như PPP nó không bị tách bạch giữa các giao thức. PPTP cung cấp một sự truyền dẫn an toàn qua mạng TCP/IP bởi vì nó đấu nối bằng mật mã. Giao thức này hỗ trợ đa giao thức VPN. Sử dụng PPTP các client ở xa có thiết lập một kết nối tới server RAS hoặc mạng Internet. PPTP cung cấp một đường đến bộ định tuyến IP, IPX, hoặc NetBEUI gói giao thức PPP sẽ qua một mạng TCP/IP. Bằng việc gói gọn thành các gói không giống nhau, các gói giao thức sẽ được gửi đi thông qua mạng TCP/IP. WAN ảo đượng hỗ trợ thông qua các mạng công cộng giống như mạng Internet.

Sử dụng RAS để đấu nối sẽ không có được sự chọn lựa tốt nhất cho việc mở rộng mạng. Nhưng nó cung cấp nhiều cơ hội và đặc trưng mà ở các cách khác không thể có. Đây là điều quan trọng để biết được khi nào ta chọn lựa RAS và khi nào chọn lựa một cái khác.

Chỉ sử dụng RAS khi ta xác định rõ độ rộng băng tần của mình không lớn hơn 128 kbit/s và không yêu cầu việc kết nối toàn bộ thời gian hoặc để giá cả hệ thống giảm xuống. Không dùng RAS nếu độ rộng băng tần n hơn khả năng cung cấp của một modem không đồng bộ hoặc nếu dành toàn bộ thời gian để kết nối.

**Tổng quan về WAN**

Mạng LAN làm việc tốt nhưng nó có nhiều hạn chế về khoảng cách và vật lý. LAN không thích hợp cho thông tin thương mại. Với việc sử dụng các thành phần kết nối liên mạng như bộ cầu nối, một router và cùng với việc cung cấp dịch vụ truyền thông một LAN có thể mở rộng hoạt động từ một máy chủ cục bộ đến một mạng diện rộng có khả năng hỗ trợ truyền thông dữ liệu khắp cả thành phố, quốc gia và thậm trí trên toàn thế giới.

Hầu như các mạng WAN được tập hợp từ các mạng LAN và các thiết bị truyền thông khác được nối kết với nhau bằng các đường thông tin gọi là các "WAN links". Các WAN links bao gồm:

- Mạng chuyển mạch gói.
- Cáp quang.
- Truyền dẫn viba.
- Đường vệ tinh.

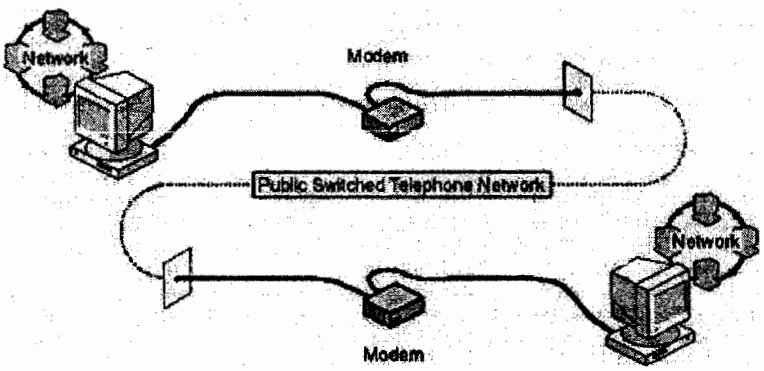
- Hệ thống cáp đồng trục TV.

Thông tin truyền giữa các LAN sử dụng một trong các công nghệ sau:

- Tương tự.
- Số.
- Chuyển mạch gói.

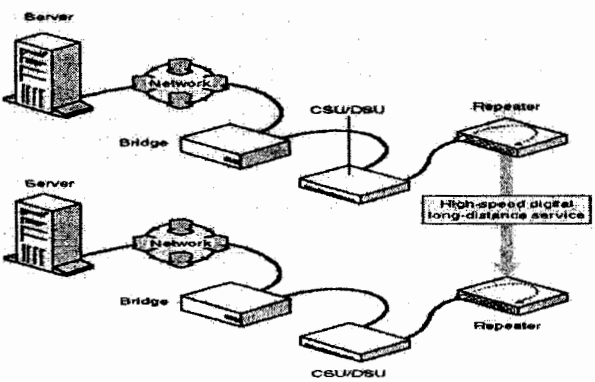
### Nối kết tương tự

**Đường quay số:** Do mạng PSTN được làm để thông tin tiếng nói theo kiểu cơ bản nên tốc độ của nó rất chậm; việc dùng modem quay số vào đường tương tự có thể càng làm cho chúng chậm hơn. Hình 6.11 chỉ ra một kết nối theo kiểu quay số. Bởi vì mạng PSTN là mạng chuyển mạch mạch nên việc kết nối chất lượng cao là việc không thể có.




**Hình 6.11 Kết nối hai mạng LAN qua PSTN**

**Đường tương tự chuyên dụng:** Không giống như đường quay số phải thao tác lại sau mỗi lần đấu nối. Đường tương tự chuyên dụng (hoặc cho thuê) sẽ mở tất cả mọi lúc. Một đường cho thuê sẽ nhanh hơn và đáng tin cậy hơn so với đường quay số.




**Hình 6.12 Kết nối mạng qua đường số DDS**

tốc độ dữ liệu được biết như là DS-0. Tốc độ 1,544 Mbít/s là DS-1. DS-1 có thể được ghép vào nhau để có được một tốc độ truyền dẫn lớn hơn như DS-1C, DS-2, DS-3 và DS-4. Các tốc độ truyền dẫn này được cho trong bảng 6.1.

Cáp đồng có thể được dùng cho T1, T2. T3 và T4 yêu cầu một phương tiện có tần số cao hơn như sóng viba hoặc cáp sợi quang.

Bảng 6.1

**Tốc độ truyền dẫn số**

| *Loại tín hiệu* | *Sóng mang* | *Kênh T-1* | *Kênh tiếng* | *Tốc độ dữ liệu (Mbps)* |
|---|---|---|---|---|
| DS-0 | N/A | N/A | 1 | 0.064 |
| DS-1 | T1 | 1 | 24 | 1.544 |
| DS-1C | T-1C | 2 | 48 | 3.152 |
| DS-2 | T2 | 4 | 96 | 6.312 |
| DS-3 | T3 | 28 | 672 | 44.736 |
| DS-4 | T4 | 168 | 4032 | 274.760 |

**Dịch vụ T3** và các đường phân cấp cho thuê của T3 có thể cung cấp các dịch vụ thoại và dữ liệu ở các cấp độ khác nhau từ 6Mbit/s đến 45 Mbit/s. Đây là các đường cho thuê có dung lượng cao nhất hiệu nay. T3 và phân đoạn T3 được thiết kế để truyền tải dữ liệu tốc độ cao trong một phạm vi lớn giữa 2 điểm cố định. Một đường T3 có thể được dùng để thay thế cho vài đường T1.

**Dịch vụ chuyển mạch 56:** Hai công ty điện thoại ở cách xa nhau thường sử dụng dịch vụ chuyển mạch 56. Sử dụng dịch vụ để truyền dẫn dữ liệu từ mạng LAN tới mạng LAN số ở tốc độ 56 kbít/s. Chuyển mạch 56 chỉ là một mạch chuyển mạch thuộc một dạng của DDS 56 kbit/s. Ưu điểm của chuyển mạch 56 là nó được sử dụng theo nhu cầu, bằng cách ấy có thể loại trừ được các phí tổn của đường chuyên dụng. Mỗi máy tính sử dụng dịch vụ này phải trang bị một CSV/DSV có thể quay số đến các vùng chuyển mạch 56 khác.

**Mạch chuyển mạch gói**

Công nghệ chuyển mạch gói rất nhanh, thuận tiện và tin cậy, nó được sử dụng để truyền dữ liệu ở các vùng mạng rộng như thành phố, quốc gia, hoặc các thị trấn. Các gói tin được gửi từ những người gửi khác nhau và từ nhiều đường kênh nhau. Các dữ liệu ban đầu được đóng vào trong các gói, mỗi gói đều được đánh dấu một địa chỉ đích và các thông tin khác. Các gói này sẽ được gửi tới các mạng. Mỗi gói tin sẽ được chuyển mạch một cách riêng rẽ. Hai gói tin từ một nguồn tin có thể đi theo hai đường

hoàn toàn khác nhau để tới cùng một đích. Cho dù mỗi gói dữ liệu được vận chuyển đến theo một đường truyền dẫn khác nhau và các gói dữ liệu đến ở các thời gian khác nhau hoặc trình tự khác nhau thì các máy tính tiếp nhận vẫn tập hợp lại được các thông báo đầu tiên.

Chuyển mạch trực tiếp các gói dữ liệu thông qua việc nối kết và các đường dẫn gọi là kết nối kiểu any-to-any. Tổng đài của các mạng này sẽ đọc thông tin ở đầu mỗi gói dữ liệu để định ra một con đường ngắn nhất va chuyển chúng đi ngay lập tức. Kích thước của các gói dữ liệu rất nhỏ. Nếu có một lỗi nào đó trong quá trình truyền dẫn thì dữ liệu này sẽ được truyền lại. Như vậy việc truyền lại một gói dữ liệu nhỏ sẽ thuận lợi hơn là truyền một gói lớn. Với các gói nhỏ thì thời gian ưu tiên chuyển mạch sẽ ngắn hơn.

Sử dụng mạng chuyển mạch gói ta có thể gửi đi lượng dữ liệu lớn thay vì nạp tất cả dữ liệu này lên một đường truyền.

Chuyển mạch gói rất nhanh và hiệu quả. Các công việc quả lý lưu lượng mạng, định đường tập hợp và phân phát các gói dữ liệu có thể được giao cho một số máy tính và phần mềm thông minh để xử lý. Mạng chuyển mạch gói đem lại sự kinh tế bởi vì có đường dẫn tốc độ cao. Nhưng chỉ phải trả một phần kinh phí cho việc sử dụng tốc độ này.

**Mạch ảo:** Có rất nhiều mạng chuyển mạch gói sử dụng mạch ảo. Các mạch ảo này là các nối kết theo kiểu nối kết logic giữa hai máy tính gửi và nhận. Các mạch này được chỉ định một độ rộng băng tần yêu cầu nhưng không có sự kết nối với nhau bằng cáp hoặc một sự kết nối vĩnh viễn nào, Các kết nối này được thiết lập trước khi hai máy tiến hành trao đổi thông tin với nhau. Một thông tin đồng ý với việc thiết lập này sẽ được sử dụng để duy trì kết nối này. Các thông số này bao gồm thông tin về kích cỡ của thông báo và thông tin về đường đi của dữ liệu. Các thông số đó bao gồm:

- Thông tin xác nhận
- Điều khiển lưu lượng
- Điều khiển lỗi

Các mạch ảo này được duy trì tạm thời tới cuối cuộc đàm thoại hoặc có thể được cố định cho việc thông tin giữa các máy tính.

**Chuyển mạch mạch ảo (SVCs).** Trong SVCs việc nối kết người sử dụng máy tính cuối cùng sẽ sử dụng một tuyến đường đặc biệt của mạng này. Tuyến đường này sẽ được duy trì tới khi việc kết nối chấm rứt. Đó là những kết nối giống như kiểu Điểm - Đa điểm.

**Mạch ảo cố định (PVCs).** Rất giống kiểu đường cho thuê, nó là kiểu đường cố định nhưng là đường ảo, khách hàng chỉ phải trả tiền cho thời gian sử dụng đường này.

**Gửi dữ liệu thông qua một WAN.**

Có một số công nghệ rất thông dụng mà ta nên cân nhắc để sử dụng trong môi trường của mạng WAN, nó bao gồm:

- X25
- Trễ khung
- Truyền dẫn không đồng bộ ATM
- Mạng số hoá liên kết đa dịch ISDN
- Giao diện dữ liệu phân phối trong cáp quang (FDDI)
- Mạng quang đồng bộ SONET
- Dịch vụ chuyển mạch số đa Mbit (SMDS).

## 6.3. Xác định hiệu năng mạng

### 6.3.1. Xác định tốc độ mạng

Hiệu năng của mạng được xác định bởi 3 tham số chính là thông lượng, độ trễ và độ tin cậy của mạng. Ba tham số này được xác định bởi nhiều phương pháp khác nhau, thông thường người ta xác định 3 tham số đó dựa trên các tiêu chuẩn có sẵn, hoặc qua các thiết bị đo. Các căn cứ để xác định các thông số này dựa vào các chuẩn của nhà sản xuất và đặc tính kỹ thuật của từng loại mạng. Ví dụ: thông lượng là giá trị đo tốc độ truyền và nhận thành công số lượng lớn nhất các bít, các ký tự hoặc các khung tin trong một đơn vị thời gian. Thông lượng của mạng bị ảnh hưởng bởi nhiều yếu tố như: độ trễ, cỡ khung tin, tỷ lệ lỗi, cơ chế kiểm soát luồng dữ liệu, độ dài đường truyền, v.v.. Tốc độ mạng là tốc độ truyền tối đa dữ liệu trong mạng mà đặc tính kỹ thuật của mạng đó cho phép. Thông lượng luôn có giá trị nhỏ hơn tốc độ mạng. Mạng nào có độ lớn của thông lượng càng sát với tốc độ mạng thì mạng đó có hiệu suất truyền càng cao. (Đơn vị của thông lượng và của tốc độ mạng đều là bit/giây). Ngoài độ tin cậy, ba tham số của mạng là thông lượng, độ trễ và tốc độ mạng luôn có sự ảnh hưởng tới nhau. Ba tham số này cùng các tham số khác ảnh hưởng tới hiệu năng của mạng.

Tốc độ mạng phụ thuộc nhiều vào đường truyền. Các yếu tố ảnh hưởng tới việc truyền khung tin (hoặc gói tin) trong mạng là kích cỡ khung (gói), tỷ lệ lỗi, thời gian truyền v.v...Các yếu tố này có quan hệ mạt thiết với nhau làm ảnh hưởng tới tốc độ truyền của mạng và tốc độ vật lý của đường truyền.

Trong các tham số của mạng có 2 tham số trực tiếp tác động tới tối ưu hoá mạng là tham số độ trễ (T) và tham số thông lượng (L).

Trễ toàn mạng được tính bởi công thức $T = T_f + 2\ T_d$ . Trong đó $T_f$ là thời gian khung, $T_d$ là thời gian trễ của đường truyền. Nếu tốc độ mạng là B, độ dài của khung tin sẽ là n/B, khoảng thời gian truyền của một khung tin đến một khung kế tiếp là $(n/B)+t_i$. Còn thời gian trả lời khi nhận được khung tin, thời gian lưu trữ và thời gian xử lý khứ hồi rất nhỏ so với thời gian truyền và thời gian trễ trên đường truyền. Thời gian trễ trên đường truyền là tỷ lệ giữa độ dài đường truyền và tốc độ vật lý của đường truyền $T_d = d/V$;

Thông lượng đường truyền là tỷ lệ giữa số lượng tin cần truyền của một khung tin trên tổng thời gian truyền và xử lý truyền khung tin đó:

$$L = \frac{k}{T} \tag{6-1}$$

Trong đó: T là độ trễ, k là số bít thông tin dữ liệu trong một khung tin.

Công thức (6-1) chưa có lỗi của đường truyền. Nếu đường truyền có lỗi rõ ràng độ trễ sẽ tăng. Lúc đó thông lượng được tính theo công thức:

$$L = \frac{k}{mT} \tag{6-2}$$

Trong đó: m là số lần truyền lại khung tin khi đường truyền có lỗi.

Công thức (6-2) có tỷ lệ lỗi đường truyền qua số lần truyền lại. Thông lượng trong công thức này chỉ có số bít thông tin dữ liệu (k) trong một khung (theo đúng định nghĩa), các bít thông tin điều khiển của khung được truyền trong mạng chưa được xét đến.

Cách tính lưu lượng băng thông như sau:

$$Lưu\ lượng\ băng\ thông = \frac{Thông\ lượng}{Tốc\ độ\ mạng} = \frac{n\left(\frac{d}{V} + \frac{n}{B}\right)}{B}$$

Thông lượng: $$L = n\left(\frac{d}{V} + \frac{n}{B}\right) = nT \tag{6-3}$$

Trong đó: n- là cỡ khung tin, V- tốc độ môi trường truyền, d- độ dài đường truyền, B- tốc độ mạng.

Công thức (6-3) không xét đến tỷ lệ lỗi đường truyền. Tính thông lượng của hệ thống qua tốc độ truyền các bít thông tin có công thức:

$$L = \frac{i(n-c)(1-P)}{\frac{in}{B} + t_i} \qquad (6\text{-}4)$$

Trong đó: i- số bít thông tin của một kí tự; n- cỡ khung tin; c- số bít điều khiển làm khung; P- xác xuất bít lỗi trong mỗi khung; B- tốc độ mạng; $t_i$- khoảng cách giữa 2 khung tin.

Công thức (6-4) tính cỡ khung tin, tính các bít điều khiển của khung, xét đến xác suất lỗi của 1 khung tin. Công thức này bỏ qua tham số độ trễ.

Thời gian truyền là một trong những yếu tố quan trọng nhất ảnh hưởng tới quá trình truyền tin. Tổng thời gian truyền một khung tin theo cơ chế truyền có báo nhận là:

$$T = \sum T_i = T_a + T_f + T_l + 2T_d + T_p$$

Trong đó: $T_f$- thời gian truyền khung; $T_a$- thời gian trả lời; $T_p$- thời gian xử lý khứ hồi- trễ thao tác; $T_d$- là thời gian trễ trên đường truyền; Tl- trễ lưu trữ.

Bản chất của quá trình truyền tin cho thấy nếu tốc độ của đường truyền là B, phục vụ yêu cầu truyền loại hình thông tin dịch vụ nào đó, độ dài của khung tin là n thì thời gian khung tin chiếm giữ đường truyền sẽ là n/B. Gọi khoảng thời gian giữa hai khung tin là $t_i$. *Vậy thời gian chiếm dụng đường truyền của một khung tin đến khung tin tiếp* sau là: $\frac{n}{B} + t_i$.

Do thời gian trả lời, thời gian lưu trữ và thời gian xử lý khứ hồi rất nhỏ so với thời gian truyền và thời gian trễ trên đường truyền, nên độ trễ của mạng theo thời gian truyền, những thời gian gây trễ khác không xét tới nhằm giảm tính phức tạp khi phân tích, đánh giá độ trễ của mạng. Độ trễ của mạng được xác định theo công thức sau:

$$T = T_f + 2T_d; \quad với \quad T_f = \frac{n}{B} + t_i \quad và \quad T_d = \frac{d}{V} \qquad (6\text{-}5)$$

Để quá trình truyền tin thành công, người ta thiết kế các thủ tục truyền tin có báo

đáp-trả lời (acknowledge), khi có lỗi khung tin không đến đích, thủ tục mạng yêu cầu truyền lại (ACK). Mỗi lần truyền lại như vậy thời gian truyền tăng lên. Vì vậy dù truyền một tập tin trong nhiều lần khác nhau sẽ cho kết quả khác nhau. Nếu gọi số lần truyền là m, thì thời gian truyền sẽ là mT, khi đó công thức (6-2) sẽ là:

$$L = \frac{k}{mT} = \frac{k}{m\left(n/B + t_i + 2d/V\right)} \tag{6-6}$$

Xác suất truyền thành công khung tin để xác đinh cách tính số lần truyền thành công khung tin như sau: nếu xác suất khung tin bị mất hoặc bị huỷ là P thì xác suất không lỗi của khung tin sẽ là 1-P. Trong trường hợp bị lỗi, khung tin không đến đích, do đó có yêu cầu truyền lại khung tin này, như vậy sẽ làm tăng lưu lượng khung tin trên mạng. Nếu khung được truyền lại một lần sau đó nhận đúng, xác suất truyền lại sẽ là P(1-P). Nếu truyền lại một lần vẫn không thành công thì phải tiếp tục được truyền lại x lần. Xác suất truyền lại x lần sẽ là $P^x(1-P)$. Khi đó số khung tin phải truyền lại x lần sẽ là $xP^x(1-P)$.

Tổng số lần truyền lại sẽ là: $$m^* = \sum_{x=1}^{\infty} xP^x = \frac{P}{1-P}$$

Nếu E là tỷ lệ bít lỗi trong mỗi khung n. Xác suất một khung truyền đúng sẽ là $(1-E)^n$, như vậy xác suất truyền một khung bị lỗi sẽ là: $P = 1-(1-E)^n$. Số lần truyền lại sẽ là:

$$m^* = \sum_{x=1}^{\infty} xP^x = \frac{P}{1-P} = \frac{1-(1-E)^n}{(1-E)^n}$$

Một khung tin được truyền ít nhất 1 lần, nếu không bị lỗi dù một lần cũng thành công. Trong thực tế đường truyền luôn có một tỷ lệ lỗi nhất định. Khung tin không thể truyền một lần mà có thể phải truyền lại, số lần truyền một khung tin thành công sẽ là một lần truyền cộng với số lần truyền lại:

$$m = 1 + m^* = 1 + \frac{1-(1-E)^n}{(1-E)^n} \tag{6-7}$$

Thay (6-7) vào biểu thức (6-6) cho công thức tính thông lượng:

$$L = \frac{k}{\left[1 + \frac{1-(1-E)^n}{(1-E)^n}\right]\left(n/B + t_i + 2d/V\right)} \tag{6-8}$$

Công thức (6-8) chỉ ra sự tương quan giữa độ trễ, khoảng cách truyền, tốc độ của môi trường truyền, tỷ lệ bít lỗi, tốc độ truyền dữ liệu của mạng, cỡ khung tin, số lượng tin được đóng gói trong một khung, khoảng cách giữa hai khung tin và thông lượng. Công thức (6-8) được xây dựng trên cơ sở công thức (6-2). Vì vậy, thông lượng ở đây là thông lượng của khung tin có tỷ lệ 100% tin cần truyền. Từ đây cho thấy muốn mạng đạt thông lượng L, tốc độ mạng phải đạt giá trị tối thiểu nào đó phù hợp. Với lập luận như vậy và lấy giá trị B từ (6-8) sẽ nhận được công thức sau:

$$B = \frac{nVL\left[1 + \frac{1-(1-E)^n}{(1-E)^n}\right]}{Vk - \left(t_i LV + 2dL\right)\left[1 + \frac{1-(1-E)^n}{(1-E)^n}\right]} \tag{6-9}$$

Thực tế tại một thời điểm trong mạng ngoài các bít thông tin trong khung còn các bít điều khiển làm khung nên số lượng tin truyền trong mạng sẽ lớn hơn số thông tin cần truyền. Chính vì vậy, để đảm bảo chất lượng của dịch vụ thông tin với thông lượng là L và độ trễ T nào đó, tốc độ mà mạng yêu cầu cho dịch vụ này phải đạt giá trị $B_y$ mà $B_y$ phải lớn hơn B một lượng nào đó đảm bảo tốc độ truyền các bít thông tin dữ liệu và thông tin điều khiển của khung tin trong mạng.

Quá trình hình thành khung tin để truyền trong mạng sẽ thấy k luôn luôn nhỏ hơn n, thông tin cần truyền luôn ít hơn thông tin thực truyền ở trên mạng, bởi giao thức tạo khung tin chỉ đóng gói k bít thông tin thuộc tập tin cần truyền vào mỗi khung tin theo "chuẩn" do giao thức mạng qui định. Mỗi khung tin ngoài k bít cần truyền còn có C bít điều khiển làm "khung". Nên số bít trong khung n = C+k . Như vậy, thực chất sẽ có một lượng bít "phí tổn" do giao thức đóng khung thông tin làm 'tăng tải' cho đường truyền, cho nên tốc độ mạng trong công thức (6-9) mới thể hiện thông lượng khi trên đường truyền chỉ có các bít tin cần truyền (k).

Hệ số k là số bít dữ liệu cần truyền của khung, C là số các bít điều khiển của

khung. Vậy tỷ lệ các bít cần truyền so với tỷ lệ các bít thực tế trên đường truyền của 01 khung tin là: $\frac{k}{C+k}$. Tính theo tỷ lệ% thì số các bít cần truyền trên các bít thực truyền là: $\frac{k}{C+k}100\%$.

Nếu F là "phí tổn" do giao thức đóng khung thông tin, F phải là hiệu của 100% với tỷ lệ đã tính ở trên, khi đó sẽ được:

$$F = \left(100\% - \frac{k}{C+k}100\%\right) = \left(1 - \frac{k}{n}\right)100\% \qquad (6\text{-}10)$$

**Để tính tốc độ "hao phí" dựa vào lập luận như sau:**

Tỷ lệ truyền không có "hao phí" là 100% sẽ đạt tốc độ truyền là B.

Khi tỷ lệ truyền có "hao phí" là F thì tốc độ mạng chỉ còn BF.

Vậy sẽ có tốc độ mạng "hao phí" là: $B_F = \frac{FB}{100\%}$ (6-11)

Như vậy, ***tốc độ mạng do thực tế yêu cầu phải là tổng tốc độ mạng phục vụ và tốc độ mạng "hao phí"***.

$$B_y = B + B_f = B + \frac{FB}{100\%} = \frac{nLV\left[1 + \frac{1-(1-E)^n}{(1-E)^n}\right]\left(2 - \frac{k}{n}\right)}{Vk - \left(t_i LV + 2dL\right)\left[1 + \frac{1-(1-E)^n}{(1-E)^n}\right]} \qquad (6\text{-}12)$$

Trong đó: By- Tốc độ mạng yêu cầu thực tế cần đạt cho thông lượng L; L- Thông lượng trung bình của loại hình dịch vụ yêu cầu được phục vụ; k- Lượng thông tin cần truyền trong một khung tin; n- Kích cỡ khung tin; E- Tỷ lệ bít lỗi; d- Khoảng cách giữa hai trạm xa nhất; V- Vận tốc của môi trường truyền; ti- Thời gian giữa hai khung tin liền nhau.

Tuy 6-12 đã xét đến khung tin trong quá trình truyền nhưng chưa xét đến cơ chế và phương pháp thâm nhập đường truyền của khung tin. Mỗi loại mạng khác nhau có cơ chế và phương pháp thâm nhập mạng khác nhau. Các cơ chế và phương pháp đó đều ảnh hưởng nhất định đến thông lượng và tốc độ mạng. Cần xem xét thêm về cơ chế

kiểm soát luồng dữ liệu và phương pháp thâm nhập mạng.

### 6.3.2. Tính theo từng loại mạng

**a) Đối với mạng kiểm soát luồng dữ liệu bằng cơ chế cửa sổ** (Window mechanism)

Mạng kiểm soát luồng dữ liệu bằng cơ chế cửa sổ phụ thuộc nhiều vào kích cỡ cửa sổ, cửa sổ được xác định bởi một giới hạn trên và một giới hạn dưới. Giới hạn trên là giá trị xác định khung tin đầu tiên nằm trong giới hạn cửa sổ, giới hạn dưới là giá trị xác định khung tin cuối cùng trong khung cửa sổ được phép đi qua giao diện. Kích cỡ cửa sổ (W) cho mỗi hướng truyền xác định số lượng các khung tin tối đa tại một thời điểm được nằm trong cửa sổ và chỉ các khung tin đó được truyền đi. Lượng tin trong khung cần truyền là k, với cơ chế cửa sổ, số lượng tin truyền đi sẽ là Wk. Tương tự như vậy nếu số lần truyền lại là m*, với cơ chế cửa sổ, số lần truyền lại sẽ là Wm*. Như vậy từ (6-7) được thay đổi phù hợp hơn trong mạng dùng cơ chế cửa sổ theo công thức sau:

$$m_w = 1 + m^* = 1 + \frac{\left[1-(1-E)^n\right]W}{(1-E)^n} \qquad (6\text{-}13)$$

Thay (6-13) vào (6-12) sẽ nhận được công thức xác định tốc độ cho mạng dùng cơ chế kiểm soát bằng cửa sổ là:

$$B_w = \frac{nVL\left\{1 + \frac{\left[1-(1-E)^n\right]W}{(1-E)^n}\right\}\left(2 - \frac{k}{n}\right)}{kWV - \left(t_i LV + 2dL\right)\left\{1 + \frac{\left[1-(1-E)^n\right]W}{(1-E)^n}\right\}} \qquad (6\text{-}14)$$

Công thức (6-14) được phát triển từ công thức tổng quát (6-12) cho riêng mạng dùng cơ chế kiểm soát bằng cửa sổ. Từ (6-14) qua phép biến đổi toán học sẽ nhận được công thức tính thông lượng (6-15).

Ngoài các tham số đã giải thích ở phần trên, W là kích cỡ cửa sổ của mạng. Công thức này khác công thức tính thông lượng của tất cả các tài liệu đã có ở chỗ thông lượng trong mạng có tính đến giá trị "hao phí" tốc độ mạng, khi mạng phải truyền cùng một lúc cả thông tin hữu ích do dịch vụ yêu cầu và thông tin làm khung do giao thức mạng qui định.

$$L_w = \frac{kWVB}{\left\{1 + \frac{\left[1-(1-E)^n\right]W}{(1-E)^n}\right\}\left[nV\left(2-\frac{k}{n}\right) + (t_i V + 2d)B\right]} \quad (6\text{-}15)$$

Các tham số trong (6-14), (6-15) thể hiện các mối tương quan về khả năng phục vụ của mạng dùng cơ chế cửa sổ. Trong đó kích cỡ cửa sổ ngầm định bằng 2, hoặc được thay đổi theo thủ tục phụ tới 127. Trong các tham số trên kích cỡ cửa sổ và tỷ lệ bít lỗi là hai tham số tạo nên sự biến thiên lớn nhất cho tốc độ mạng và cho thông lượng của mạng. Tham số khoảng cách giữa hai trạm xa nhất và tham số vận tốc vật lý của môi trường truyền có sự biến thiên rất nhỏ trong công thức phân tích mạng dùng cơ chế cửa sổ. Thông thường các giải pháp thay đổi tốc độ mạng và thông lượng qua tỷ lệ bít lỗi sẽ rất phức tạp vì việc đó còn phụ thuộc vào nhiều khâu khác nhau. Đối với mạng loại này dùng giải pháp thay đổi kích cỡ cửa sổ sẽ mang lại hiệu qủa cao. Các biện pháp tìm kích cỡ cửa sổ tối ưu có thể được khảo sát qua các tham số mạng trong (6-14); (6-15).

**b) Đối với mạng kiểm soát luồng dữ liệu bằng cơ chế xếp hàng** (Queueing mechanism)

Mạng có cơ chế xếp hàng kiểm soát luồng dữ liệu có số lượng các khung trong hệ thống là:

$$X = \lambda S + \frac{\lambda^2 S^2}{2(1-\lambda S)} \quad (6\text{-}16)$$

Trong đó: S- Thời gian truyền trung bình; λ-Tốc độ đến trung bình của các khung tin.

Số lượng khung tin trong hàng đợi là X, theo nguyên tắc của cơ chế kiểm soát luồng dữ liệu khả năng truyền lại cũng tăng lên X lần, tương tự như khả năng truyền lại trong mạng dùng phương pháp kiểm soát luồng dữ liệu bằng cơ chế cửa sổ, khi đó từ (6-7) cho biết số lần truyền lại trong mạng dùng phương pháp kiểm soát bằng cơ chế xếp hàng như sau:

$$m_x = 1 + m^* = 1 + \frac{\left[1-(1-E)^n\right]X}{(1-E)^n} \quad (6\text{-}17)$$

Tương tự như mạng dùng phương pháp kiểm soát luồng dữ liệu bằng cơ chế cửa sổ, số lượng thông tin trong hàng đợi sẽ là Xk. Từ đây, cũng nhận được cách tính thông lượng với sự thay đổi số lượng các bít truyền, điều đó dẫn tới sự thay đổi tương ứng của tốc độ mạng cho phù hợp với sự thay đổi của thông lượng và cho công thức (6-18).

$$B_x = \frac{nVL\left\{1 + \frac{\left[1-(1-E)^n\right]X}{(1-E)^n}\right\}\left(2 - \frac{k}{n}\right)}{kXV - (t_i LV + 2dL)\left\{1 + \frac{\left[1-(1-E)^n\right]X}{(1-E)^n}\right\}} \qquad (6\text{-}18)$$

Thay (6-16) vào công thức (6-18) sẽ cho công thức (6-19). Công thức (6-19) cho biết mối tương quan giữa các tham số cơ bản trong mạng dùng phương pháp kiểm soát luồng dữ liệu bằng cơ chế xếp hàng, đồng thời còn cho biết hiệu năng của mạng đó qua việc phân tích, khảo sát (6-19).

$$B_x = \frac{nVL\left\{1 + \frac{\left[1-(1-E)^n\right]\left[\lambda S + \frac{\lambda^2 S^2}{2(1-\lambda S)}\right]}{(1-E)^n}\right\}\left(2 - \frac{k}{n}\right)}{kV\left[\lambda S + \frac{S^2\lambda^2}{2(1-\lambda S)}\right] - (t_i LV + 2dL)\left\{1 + \frac{\left[1-(1-E)^n\right]\left[\lambda S + \frac{S^2\lambda^2}{2(1-\lambda S)}\right]}{(1-E)^n}\right\}} \qquad (6\text{-}19)$$

Ngoài tham số tỷ lệ bít lỗi, các tham số thời gian truyền trung bình, tốc độ đến trung bình của các khung tin và sự thay đổi số lượng các khung tin trong hàng đợi làm cho tốc độ mạng theo cơ chế xếp hàng biến đổi lớn. Như các mạng khác, mạng theo cơ chế xếp hàng cũng bị chi phối bởi tỷ lệ bít lỗi.

### 6.3.3. Đối với mạng truy nhập có điều khiển (Controlled access)

Mạng dùng phương pháp truy nhập có điều khiển điển hình là mạng Token Bus, Token Ring và Collision Avoidance (tránh xung đột). Đối với mạng loại này thường dùng các "thẻ bài", khi nhận được "thẻ bài" trạm truyền có thể "gửi" thông tin vào

đường truyền.

Mạng truy nhập có điều khiển bị ảnh hưởng bởi nhiều yếu tố, trong đó hiệu năng của mạng (performance) là yếu tố ảnh hưởng đáng kể. Nếu hiệu năng của mạng là U, mạng đạt hiệu năng 100% thì U=1. Khi đó thông lượng của mạng sẽ bằng tốc độ đường truyền mà mạng có. Điều này khó xảy ra! Thông thường U luôn nhỏ hơn 1.

Nếu giá trị hiệu năng mà mạng chưa đạt tới là 1-U, tương ứng với giá trị đó, tốc độ của mạng sẽ là By(1-U). (6-12) thể hiện tốc độ mạng đạt thông lượng trung bình cho dịch vụ khi hiệu năng ở mức 100%. Khi mạng không đạt hiệu năng 100% rõ ràng tốc độ mạng phải thêm một lượng By(1-U) mới bảo đảm đạt thông lượng trung bình cho dịch vụ, như vậy công thức (6-12) sẽ được cộng thêm tốc độ mạng suy giảm do hiệu năng của mạng gây ra. Tốc độ mạng khi đó sẽ là:

$$B_p = B_y + B_y(1-U) = \frac{nLV\left[1+\frac{1-(1-E)^n}{(1-E)^n}\right]\left(2-\frac{k}{n}\right)(2-U)}{Vk-\left(t_i LV+2dL\right)\left[1+\frac{1-(1-E)^n}{(1-E)^n}\right]} \qquad (6\text{-}20)$$

Công thức (6-20) dùng chung cho các mạng truy nhập có điều khiển.

**** Ứng dụng cho mạng TOKEN RING***

Hiệu năng U của mạng Token Ring có biểu thức chung là:

$$U = \frac{1}{1+a/N} \quad với\ a<1 \quad và \quad U = \frac{1}{a\left(1+1/N\right)} \quad với\ a>1\ ; \quad a = \frac{d/V}{n/B_y}$$

Trong đó: N - số lượng các trạm trong vòng, a - hệ số truyền.

Thay U vào (6-20) nhận được (6-21) với a < 1 và (6-22) với a >1.

$$B_{ct} = \frac{nLV\left[1 + \frac{1-(1-E)^n}{(1-E)^n}\right]\left(2 - \frac{k}{n}\right)\left(2 - \frac{1}{1 + dB_y / nVN}\right)}{Vk - (t_i LV + 2dL)\left[1 + \frac{1-(1-E)^n}{(1-E)^n}\right]} \quad (6\text{-}21)$$

$$B_{ct} = \frac{nLV\left[1 + \frac{1-(1-E)^n}{(1-E)^n}\right]\left(2 - \frac{k}{n}\right)\left[2 - \frac{1}{dB_y / nV\left(1 + 1/N\right)}\right]}{Vk - (t_i LV + 2dL)\left[1 + \frac{1-(1-E)^n}{(1-E)^n}\right]} \quad (6\text{-}22)$$

Lưu ý: khi khảo sát theo các công thức này, đầu tiên cần tính giá trị a. Nếu a < 1, khảo sát- phân tích mạng theo (6-21), ngược lại khi a > 1 khảo sát - phân tích mạng theo (6-22). Trường hợp giá trị a=1 (6-21) và (6-22) bằng nhau.

*** *Ứng dụng cho mạng FDDI:***

Mạng FDDI, có giá trị hiệu năng của mạng là:

$$U = \frac{N(TTRT - T_l)}{N(TTRT - T_l) + (N+1)T_l + T_t} \quad (6\text{-}23)$$

Thay giá trị này vào (6-20), nhận được công thức (6-24) như sau:

$$B_{cf} = \frac{nLV\left[1 + \frac{1-(1-E)^n}{(1-E)^n}\right]\left(2 - \frac{k}{n}\right)\left[2 - \frac{N(TTRT - T_l)}{N(TTRT - T_l) + (N+1)T_l + T_t}\right]}{Vk - (t_l LV + 2dL)\left[1 + \frac{1-(1-E)^n}{(1-E)^n}\right]}$$

Trong đó : TTRT- Thời gian luân phiên quay TOKEN: TTRT=4+$T_l$; $T_l$- Thời gian phát triển vòng: $T_l$ =$dt_l$+$NS_t$; d- Độ dài của vòng; $S_t$- Số trạm phát triển trong vòng; $t_l$- Trễ đường truyền / một mét dài; $T_t$- Thời gian truyền TOKEN; N- Số lượng các trạm trong vòng.

### 6.3.4. Đối với mạng truy nhập ngẫu nhiên (Random access)

Phương pháp truy nhập ngẫu nhiên bao gồm CSMA, CSMA/CD, Slotted Ring, Register Insertion. Điển hình và đại diện cho phương pháp truy nhập ngẫu nhiên là phương pháp CSMA/CD. Phương pháp này có nhiều ưu điểm so với phương pháp truy nhập có điều khiển ở tính đơn giản và hoạt động đạt hiệu quả cao trong trường hợp tải nhẹ. Nhưng tính chất ngẫu nhiên trong truy nhập làm cho hiệu năng của mạng phụ thuộc rất nhiều vào số lượng các trạm được kết nối vào mạng.

Các mạng truy nhập ngẫu nhiên khi tăng số lượng trạm sẽ đồng nghĩa với tăng xung đột, như vậy chắc chắn làm tăng số lần truyền lại, nên tốc độ mạng cũng cần tăng theo để đảm bảo cho mạng đạt giá trị thông lượng trung bình mà dịch vụ yêu cầu.

Từ đó có hệ quả sau: nếu mạng có N trạm, trường hợp truy nhập ngẫu nhiên cao nhất là tất cả các trạm tham gia truy nhập vào mạng cùng một thời điểm. Chắc chắn xung đột sẽ xảy ra, khi mạng dùng thủ tục tự động yêu cầu trả lời (ACK), mỗi lần va chạm, mạng sẽ yêu cầu truyền lại một lần. Nếu N trạm cùng có yêu cầu truyền lại thì số lần truyền thành công khung tin phải là:

$$m = 1 + m^* = 1 + N\left[\frac{1-(1-E)^n}{(1-E)^n}\right] \qquad (6\text{-}25)$$

Công thức này được xây dựng từ công thức (6-7), trong trường hợp số lần truyền lại tăng N lần so với trường hợp bình thường, công thức tính tốc độ mạng cũng biến đổi tương ứng [*thay (6-25) vào (6-12)*]:

$$B_r = \frac{nLV\left\{1+N\left[\frac{1-(1-E)^n}{(1-E)^n}\right]\right\}\left(2-\frac{k}{n}\right)}{Vk-\left(t_i LV+2dL\right)\left\{1+N\left[\frac{1-(1-E)^n}{(1-E)^n}\right]\right\}} \qquad (6\text{-}26)$$

Trong đó: ngoài các tham số đã giải thích ở trên, N là số lượng các trạm truy nhập ngẫu nhiên vào mạng.

Phân tích (6-26) cho thấy yêu cầu về tốc độ mạng tăng khi số lượng trạm truy nhập

ngẫu nhiên tăng, khi đó tốc độ mạng sẽ đảm bảo thông lượng trung bình của dịch vụ trong trường hợp mạng có một tỷ lệ lỗi bít nào đó. (6-26) hợp lý hơn các công thức tính tốc độ mạng đã có trước đây là công thức này đã tính đến tốc độ mạng "hao phí" do giao thức đóng gói khung tin tạo nên và số lần truyền lại ngẫu nhiên có tính đến số lượng truyền lại với khả năng ngẫu nhiên cao nhất có thể xảy ra khi cùng lúc toàn bộ số lượng các trạm trong mạng truy nhập vào đường truyền.

### 6.3.5. Đối với mạng đa điểm - hai chiều đồng thời (multipoint-fult duplex)

Giao thức hướng ký tự và giao thức hướng bít sử dụng các ứng dụng kiểu đa điểm-hai chiều đồng thời. Các ứng dụng này hay được dùng trong các mạng có máy chủ với một vài trạm đầu cuối hoặc trong mạng bình đẳng.

Tính chất đa điểm-hai chiều đồng thời cho thấy: ngoài các lỗi ngẫu nhiên, tốc độ mạng còn phụ thuộc vào số lượng trạm tham gia truy nhập. Nếu có N trạm trong mạng, để đạt được thông lượng yêu cầu, tốc độ mạng phải tăng N lần tương ứng với số lượng trạm truyền-nhận thông tin đồng thời trong mạng, cùng với sự tăng số lần truyền lại do lỗi va chạm gây ra (như mạng truy nhập ngẫu nhiên).

$$B_m = \frac{nLV\left\{1 + N\left[\frac{1-(1-E)^n}{(1-E)^n}\right]\right\}\left(2 - \frac{k}{n}\right)N}{Vk - (t_i LV + 2dL)\left\{1 + N\left[\frac{1-(1-E)^n}{(1-E)^n}\right]\right\}} \qquad (6\text{-}27)$$

So sánh (6-27) với (6-26) cho thấy (6-27) tăng hơn N lần so với (6-26) điều này hoàn toàn đúng vì tính chất truy nhập ngẫu nhiên tương đương với truy nhập hai chiều đồng thời. Hai mô hình này khác nhau ở tính chất đa điểm đồng thời với tính chất điểm - điểm, điểm- đa điểm.

***Ví dụ :***

Yêu cầu thông lượng trung bình của một loại hình dịch vụ cho mạng đa điểm hai chiều đồng thời là 1 Mbit/s, tỷ lệ bit lỗi 10-7, khoảng cách giữa hai trạm xa nhất d= 10.000 m. Môi trường truyền sử dụng cáp xoắn đôi có tốc độ trung bình đạt 2.108 m/s. Giả thiết rằng $t_i$=0

- Xác định tốc độ mạng để đáp ứng thông lượng cho dịch vụ, trường hợp N=2. ?
- Xác định tốc độ mạng để đáp ứng thông lượng cho dịch vụ, trường hợp N= 10. ?
- Xác định số lượng trạm tối ưu trong trường hợp mạng có tốc độ truyền 10 Mbit/s ?

*Giải :*

Để đơn giản cho quá trình khảo sát, chọn điều kiện: kích cỡ khung tin cố định n=1024 bit và k =816 bit. Thay thế các số liệu vào công thức (6-27) ta được $B_m \approx 3,47$ Mbit/s. Như vậy chỉ cần mạng đạt tốc độ 3,47 Mbit/s sẽ bảo đảm phục vụ cho dịch vụ có yêu cầu thông lượng 1 Mbit/s.

Cùng điều kiện như trên, thay các số liệu đã cho vào công thức (6-27) ta sẽ có giá trị tối ưu về tốc độ mạng là: $B_m \approx 3,47$ Mbit/s. Như vậy trong trường hợp số lượng trạm tăng lên gấp 5 lần mới đáp ứng được yêu cầu phục vụ cho cùng một dịch vụ thông tin.

Cho giá trị tốc độ mạng $B_m$=10 Mbit/s. Thay các số liệu đã cho, với n = 1024 bit và k= 816 bit vào công thức (6-27) sẽ xác định được số lượng các trạm tối ưu cho tốc độ và thông lượng mạng yêu cầu. (Điều kiện N>0). Qua tính toán sẽ được $N \approx 5,76$, làm tròn số N =5. Như vậy, đáp ứng các giá trị thông lượng trung bình 1 Mbit/s và tốc độ mạng 10 Mbit/s, mạng kết nối truy nhập tới 5 trạm làm việc sẽ đạt giá trị tối ưu về hiệu suất truyền.

Có thể dùng chương trình máy tính để phân tích, khảo sát mạng, với nhiều tham số biến thiên theo yêu cầu khác nhau của người thiết kế mạng hoặc quản trị mạng sẽ cho kết quả tối ưu đầy đủ hơn trong xác định hiệu năng mạng .

# CHƯƠNG 7

# INTERNET

Internet là một mạng máy tính có phạm vi và qui mô toàn cầu. Hiện tại có hàng chục triệu máy tính tham gia mạng Internet và có hàng trăm triệu người trên thế giới hàng ngày truy nhập vào mạng Internet. Điều này cho thấy Internet đã, đang và sẽ còn phát triển mạnh mẽ. Để góp phần thúc đẩy sự phát triển này giáo trình muốn dành một chương riêng nói về Internet. Các nội dung được đề cập trong chương này bao gồm :

- *Lịch sử phát triển của Internet,*
- *Cấu trúc của mạng Internet,*
- *Công nghệ Internet,*
- *Hệ thống các máy chủ,*
- *Các dịch vụ Internet, và*
- Một số kiên thức liên quan.

## 7.1. Lịch sử phát triển của Internet

Khi nói về Internet người ta luôn nghĩ đó là một mạng toàn cầu với rất nhiều lợi ích và phục vụ chung cho tất cả nhân loại. Không ai nghĩ rằng Internet lại được sinh ra từ sự đối đầu giữa Liên xô và Mỹ. Dưới đây là những con số và sự kiện liên quan đến lịch sử phát triển của Internet.

Bảng 7.1

**Lịch sử phát triển Internet**

| *Năm* | **Sự kiện** |
|---|---|
| **1957** | - Liên xô phóng tàu vũ trụ Sputnik mở đầu cho thời đại thông tin viễn thông thế giới.<br>- Mỹ đáp lại bằng cách thành lập "Viện nghiên cứu các Dự án cao cấp" ARPA (Advanced Research Projects Agency) |
| **1962** | - Paul Baran, RAND, mô tả mạng mạch gói (packet-switch networks) trong bài báo "On Distributed Communications Networks" |
| **1967** | - Tại hội thảo về các nguyên lý Hệ điều hành, ACM (Association for Computing Machinery - Hiệp Hội Máy tính) lần đầu tiên đưa ra mô hình mạng mạch gói. |
| **1969** | - Thiết lập mạng ARPANET - mạng máy tính đầu tiên được thiết lập |

| | |
|---|---|
| | theo nguyên tắc mạch gói. Máy chủ đầu tiên được xây dựng thông qua công ty môi giới BBN và đặt tại Trường đại học Tổng hợp California (UCLA - University of California). ARPA giao việc nghiên cứu ARPANET cho BBN, UCLA, Viện nghiên cứu Stanford (SRI - Stanford Research Institute), Trường đại học Tổng hợp Utah (UU - University of Utah). Có thể coi đây là thời điểm sinh ra Internet.<br>- 04 máy chủ; |
| **1970** | - Mạng ARPANET bắt đầu sử dụng giao thức NCP (Network Control Protocol). |
| **1971** | - 23 máy chủ;<br>- ARPA được chuyển sang nằm trong Bộ quốc phòng Mỹ (DOD - Department of Defence) và có tên mới là DARPA (Defence Advandced Research Projects Agency). DARPA tập trung nghiên cứu các công nghệ viễn thông, vô tuyến và công nghệ mạng mạch gói<br>- Ray Tomlinson của BBN (Bolt, Bernak & Newman) lần đầu tiên phát minh ra chương trình thư tín điện tử (E-mail program) trên mạng phân tán. |
| **1973** | - Mạng ARPANET thiết lập liên kết đầu tiên với nước Anh và Nauy.<br>- Phát hiện ra một số nhược điểm của NCP. DARPA quyết định cần thay đổi về căn bản các nguyên lý của mạng ARPANET.<br>- Trên 23 máy chủ |
| **1974** | - Tại trường đại học Harvard, Robert Metcalfe trong luận án tiến sĩ của mình lần đầu tiên đưa ra công nghệ Ethernet.<br>- Vinton Cerf và Bob Kahn trong bài báo "A protocol for Packet Network Intercommunications" lần đầu tiên thiết kế và mô tả giao thức TCP (Transmission Control Protocol). Như vậy Vinton Cerf và Bob Kahn là cha đẻ của dòng họ giao thức TCP/IP nổi tiếng hiện nay.<br>- DARPA đưa ra một loạt các chức năng của các giao thức mới là tiền thân của TCP/IP sau này.<br>- TCP/IP chính thức được tung ra vào khoảng cuối 1974 đầu 1975.<br>- Cuối 1974, hãng BBN công bố Telnet - phần mềm cho phép các máy tính truy nhập trực tiếp vào các mạng máy tính lớn (Mainframe). Có thể coi Telnet là phiên bản thương mại đầu tiên bắt nguồn từ ARPANET.<br>- 62 máy chủ. |
| **1975** | - Bộ quốc phòng Mỹ (DOD - Department of Defence) đưa ARPANET vào đội hình của DCA – Defence Communication Agency - Ban truyền thông Bộ quốc phòng Mỹ. DCA có nhiệm vụ triển khai các vấn đề về mạng |

| | |
|---|---|
| | trong bộ quốc phòng. Như vậy, ARPANET chính là tiền thân của Mạng số liệu quốc phòng Mỹ (DDN – Defence Data Network) sau này. |
| **1976** | - AT&T Bell Labs nghiên cứu và phát triển UUCP (UUCP - Unix To Unix Copy), chương trình copy file của UNIX.<br>- Trên 111 máy chủ. |
| **1978** | - Tom Truscott và Steve Bellovin thiết lập mạng USENET, sử dụng UUCP nối mạng giữa trường Đại học Tổng hợp Duke và Trường đại học North Carolina.<br>- Lần đầu tiên truy nhập thành công vào mạng ARPANET từ xa (Mobile Location) sử dụng TCP/IP. |
| **1980** | - Tổ chức khoa học quốc gia NSF (National Science Foundation) thành lập CSNET (Computer Science Network) với mục đích nối các mạng của tất cả các tổ chức khoa học). Máy chủ đầu tiên của CSNET được dặt tại công ty BBN, đại học Cambridge, bang Massachuset. ARPANET là mạng đầu tiên gia nhập CSNET. Như vậy NSF là người chủ đầu tiên của Internet sau này. |
| **1980 - 1981** | Một loạt các mạng rộng được thiết lập:<br>- BitNet (Because It's Time Network)<br>- EARN (European Academic Research Network)<br>- EUNET (European Unix Network)<br>- 213 máy chủ |
| **1982** | - DOD (Department of Defence) chính thức công bố từ bỏ NCP và đưa TCP/IP làm giao thức duy nhất cho ARPANET. Danh từ "Internet" xuất hiện bắt nguồn từ chữ IP (Internet Protocol) tượng trưng cho các mạng máy tính toàn cầu.<br>- DOD công bố rằng, bắt đầu từ 1-1-1983, tất cả các thành phần của ARPANET bắt buộc phải sử dụng TCP/IP. TCP/IP chính thức được coi là một chuẩn và có cơ hội để phát triển nhanh chóng.<br>- 235 máy chủ. |
| **1983** | - Trường đại học Winconsin lần đầu tiên phát triển lý thuyết về Name Servers, lý thuyêt cho phép đặt tên các máy trong mạng thay cho việc dùng mã số trước kia.<br>- Trường đại học California tạI Berkeley tung ra thị trường bản Unix 4.2 sử dụng TCP/IP. Bắt đầu từ đây toàn bộ các phiên bản của UNIX đều sử dụng TCP/IP tạo tiền đề cho sự bùng nổ của TCP/IP.<br>- ARPANET tách làm hai mạng: |

| | |
|---|---|
| - | ▫ DDN (Defence Data Network - hay còn được gọi là Milnet).<br>▫ DARPA Internet – chính là ARPANET cũ.<br>- 562 máy chủ. |
| **1984** | - DNS (Domain Name Server) được chính thức áp dụng.<br>- Thành lập mạng JUNET (Japan Unix Network) sử dụng UUCP.<br>- 1.024 máy chủ. |
| **1985** | - NSF quyết định mở rộng phạm vi của mình bằng cách đầu tư xây dựng Backbone với tốc độ 56 Kbps để nối 5 trung tâm máy tính lớn nhất nước Mỹ (1. Supercomputer Center, San Diego - 2. National Center for Atmospheric Research, Boulder, CO - 3. National Center for Supercomputing Applications, Urbana, IL - 4. Pisttburgh Supercomputer Center - 5. Cornell Theory Center, Ithaca, NY). Đây là Internet Backbone đầu tiên.<br>- Bùng nổ Internet.<br>- 2/1986: 2.308 máy chủ<br>- 11/1986: 5.000 máy chủ<br>- Mạng USENET sử dụng NNTP (Network News Transfer Protocols)<br>- Craig Partridge phát minh công nghệ MX (Mail Exchanger) cho phép non-IP-host thiết lập địa chỉ E-mail. |
| **1987** | - Các công ty Merit, IBM và MCI thành lập ANS (Advandced Network & Services). ANS là công ty nghiên cứu không lợi nhuận có nhiệm vụ điều hành NSFNET.<br>- 28.174 máy chủ. |
| **1988** | - Sự kiện "Internet Virus" làm hỏng 6.000 máy chủ<br>- 56.000 máy chủ |
| **1989** | - 100.000 máy chủ.<br>- NSFnet nâng cấp Backbone thành T1 (1544 Mbps)<br>- Bang Ohio thành lập liên kết giữa CompuServe và Internet. |
| **1990** | - ARPANET chấm dứt sự tồn tại.<br>- Thành lập Electronic Frontier Foundation. Người thành lập: Mitch Kapor.<br>- 313.000 máy chủ. |
| **1991** | - Thành lập CIX (Commercial Internet eXchange).<br>- Công ty Thinking Machines tung ra WAIS (Wide Area Information Service).<br>- Trường đại học Minnesota đưa ra Gopher. |

| | |
|---|---|
| | - Thành lập NREN (National Research & Education Network).<br>- 01/1991 : 376.000 máy chủ<br>- 10/1991 : 617.000 máy chủ |
| **1992** | - CERN công bố World Wide Web.<br>- 1.000.000 máy chủ<br>- NSFNET nâng cấp Backbone lên T3, có tốc độ 44736 Mbps.<br>- NSF sáng lập InterNIC.<br>- MBone - Multicast Backbone lần đầu tiên được sử dụng.<br>- 1.136.000 máy chủ |
| **1993** | - Nhà trắng tham gia Internet. Địa chỉ: president@whitehouse.gov<br>- Thông qua điều lệ về Cơ sở hạ tầng thông tin Quốc gia.<br>- Giới kinh doanh và Thông tin đại chúng bắt đầu chú ý đến Internet.<br>- 2.056.000 máy chủ. |
| **1994** | - Multimedia làm cho WWW và Gopher phát triển rực rỡ.<br>- Kỷ niệm 25 năm Internet.<br>- Nhà trắng và Quốc hội Mỹ thiết lập Information Server.<br>- Bắt đầu xuất hiện mua bán, kinh doanh trên Internet.<br>- 3.864.000 máy chủ. |
| **1995** | - 6.642.000 máy chủ.<br>- NSF không giữ quyền kiểm soát NSFNET và thành lập dự án xây dựng vBNS (Very-High-Speed-Backbone-Network-Service). Có thể dự đoán vBNS là tương lai của Internet hiện tại.<br>- Internet trong quá trình chuyển giao sang các công ty thương mại.<br>- Công bố NC - Network Computer |
| **1996** | - 15.000.000 máy chủ |
| **1997-đến nay** | - Trên 30.000.000 máy chủ và còn tiếp tục tăng nhanh.<br>- Hầu hết các đường truyền Internet hiện nay được thực hiện bởi các đường trục Backbone của các nhà ISP độc lập như MCI, AT&T, Sprint, UUnet, BBN planet, ANS v.v.<br>- Cộng đồng Internet ngày nay đang cố gắng thiết lập một giao thức TCP/IP mới để cho phép có hàng tỷ địa chỉ thay vì việc hệ thống bị giới hạn địa chỉ như hiện nay. Vấn đề nảy sinh là chưa biết hai hệ thống địa chỉ cũ và mới sẽ có thể làm việc ở cùng một thời điểm trong thời gian chuyển tiếp hay không ? |

| | |
|---|---|
| | - Thành lập NREN (National Research & Education Network).<br>- 01/1991 : 376.000 máy chủ<br>- 10/1991 : 617.000 máy chủ |
| **1992** | - CERN công bố World Wide Web.<br>- 1.000.000 máy chủ<br>- NSFNET nâng cấp Backbone lên T3, có tốc độ 44736 Mbps.<br>- NSF sáng lập InterNIC.<br>- MBone - Multicast Backbone lần đầu tiên được sử dụng.<br>- 1.136.000 máy chủ |
| **1993** | - Nhà trắng tham gia Internet. Địa chỉ: president@whitehouse.gov<br>- Thông qua điều lệ về Cơ sở hạ tầng thông tin Quốc gia.<br>- Giới kinh doanh và Thông tin đại chúng bắt đầu chú ý đến Internet.<br>- 2.056.000 máy chủ. |
| **1994** | - Multimedia làm cho WWW và Gopher phát triển rực rỡ.<br>- Kỷ niệm 25 năm Internet.<br>- Nhà trắng và Quốc hội Mỹ thiết lập Information Server.<br>- Bắt đầu xuất hiện mua bán, kinh doanh trên Internet.<br>- 3.864.000 máy chủ. |
| **1995** | - 6.642.000 máy chủ.<br>- NSF không giữ quyền kiểm soát NSFNET và thành lập dự án xây dựng vBNS (Very-High-Speed-Backbone-Network-Service). Có thể dự đoán vBNS là tương lai của Internet hiện tại.<br>- Internet trong quá trình chuyển giao sang các công ty thương mại.<br>- Công bố NC - Network Computer |
| **1996** | - 15.000.000 máy chủ |
| **1997-đến nay** | - Trên 30.000.000 máy chủ và còn tiếp tục tăng nhanh.<br>- Hầu hết các đường truyền Internet hiện nay được thực hiện bởi các đường trục Backbone của các nhà ISP độc lập như MCI, AT&T, Sprint, UUnet, BBN planet, ANS v.v.<br>- Cộng đồng Internet ngày nay đang cố gắng thiết lập một giao thức TCP/IP mới để cho phép có hàng tỷ địa chỉ thay vì việc hệ thống bị giới hạn địa chỉ như hiện nay. Vấn đề nảy sinh là chưa biết hai hệ thống địa chỉ cũ và mới sẽ có thể làm việc ở cùng một thời điểm trong thời gian chuyển tiếp hay không ? |

## 7.2. Cấu trúc của Internet

*Cấu trúc của Internet được thể hiện như hình 7.1.*

Từ sơ đồ thể hiện trên hình 7.1. cho thấy có 04 đối tượng cấu thành nên Internet, bao gồm :

- *Nhà cung cấp dịch vụ truy cập Internet - IAP (Internet Access Provider),*
- *Nhà cung cấp dịch vụ Internet - ISP (Internet Service Provider),*
- *Nhà cung cấp nội dung thông tin - ICP (Internet Content Provider), và*
- *Người sử dụng.*

Ngoài 4 đối tượng trên đây còn cần kể đến các tổ chức quản lý Internet (InterNIC).

### 7.2.1. Nhà cung cấp dịch vụ truy cập (IAP - Internet Access Provider)

Đó là các cơ quan, các tổ chức đảm trách việc xây dựng, cung cấp và quản lý các đường truyền viễn thông : như đường truyền Internet tốc độ cao xuyên lục địa, xuyên quốc gia và các đường thuê bao số hoặc tương tự (Analog) tới các nhà cung cấp dịch vụ thông tin, các nhà cung cấp nội dung thông tin hoặc thậm chí tới tận người sử dụng đầu cuối. Nhờ các đường truyền này mà thông tin trên Internet có thể di chuyển tới bất cứ địa danh nào trên thế giới, miễn là nơi này có đường truyền viễn thông được lắp đặt và đã đưa vào vận hành. Các công việc cụ thể của tổ chức này bao gồm :

*Xây dựng cung cấp và quản lý hạ tầng truyền thông Internet,*

*Quản lý các Internet Gateway,*

*Cấp phát và quản lý băng thông và đường truyền tới các thuê bao ISP, ICP hoặc người sử dụng đầu cuối, và.Giám sát và bảo đảm sự vận hành của các đường truyền viễn thông.*

### 7.2.2. Nhà cung cấp dịch vụ thông tin Internet (ISP-Internet Service Provider)

Đó là các cơ quan, các tổ chức đảm trách việc cung cấp các dịch vụ Internet (ISP). Các dịch vụ này bao gồm 05 dịch vụ cơ bản :

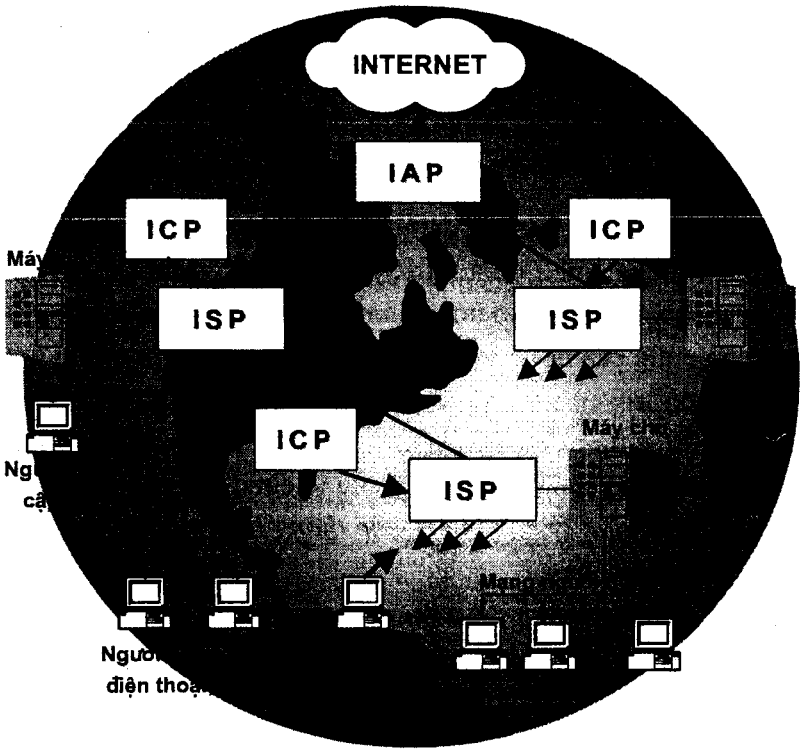
- *Thư tín điện tử (E-Mail),*
- *Diễn đàn thông tin (NewGroups),*
- *Dịch vụ truyền tệp FTP (File Transfers Protocols),*

- *Truy nhập vào máy chủ (Telnet), và*
- *World Wide Web (WWW).*

Để cung cấp các dịch vụ Internet các ISP cần phải tiến hành các công việc bao gồm:

- *Xây dựng một mạng đảm nhận vai trò cung cấp các dịch vụ Internet,*
- *Tổ chức quản lý cung cấp các dịch vụ thông tin theo yêu cầu (cơ bản gồm 05 dịch vụ nói trên), và*

*Tổ chức biên tập và cấp phát thông tin giống như vai trò của nhà cung cấp nội dung thông tin ICP (chi tiết về ICP xin xem phần tiếp theo).*




**Hình 7.1. Sơ đồ minh hoạ cấu trúc của Internet**

### 7.2.3. Nhà cung cấp nội dung thông tin Internet (ICP)

Việc phát triển nội dung thông tin trên Internet được các ICP đảm nhận. ICP là một tổ chức hoặc cá nhân sau khi đã đăng ký và được cấp phép họ có thể tự phát triển nội dung thông tin đã đăng ký và đưa vào khai thác sử dụng trên Internet. Các thông tin này có thể hội nhập vào bên trong mạng của một ISP theo các hình thức *thuê chỗ* trên

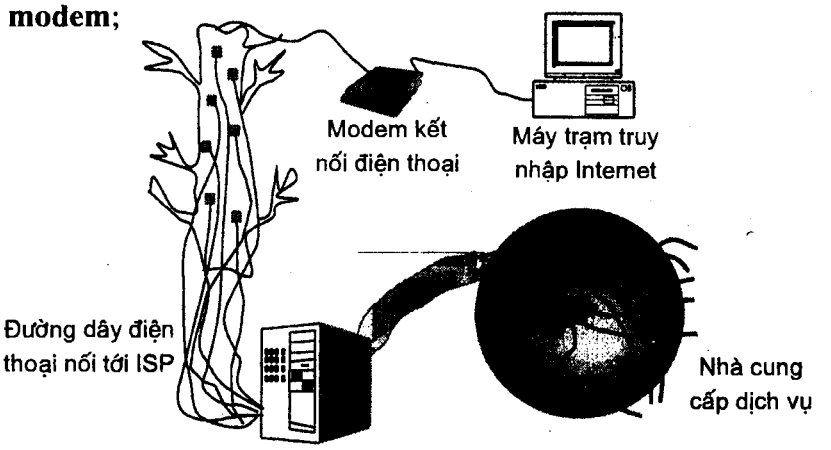
máy chủ, *thuê cổng mạng để đặt máy chủ*, hoặc *thuê đường thuê bao tốc độ cao* kết nối tới mạng thông tin nội tại, nơi sản sinh ra các thông tin cung cấp của ICP.

Việc cập nhật mới các thông tin do chính các thành viên của ICP đảm nhận. Các thông tin này có thể cập nhật gián tiếp định kỳ theo tuần, tháng, quý hoặc khi xét thấy cần thiết thông qua việc truyền thông *gửi / nhận* (qua điện thoại hoặc các đường thuê bao khác) hoặc cũng có thể *thao tác trực tiếp trên các máy chủ* chứa tin hoặc *thông qua mạng kết nối tốc độ cao* đến máy chủ chứa nội dung thông tin.

ICP cũng có thể định ra các chính sách bán, miễn phí một số phần hoặc miễn phí toàn bộ các nội dung thông tin họ cung cấp. Ngoài ra việc bán thông tin trên mạng cũng có thể được chính các ISP tự phát triển dựa trên các ứng dụng do họ tạo ra trên môi trường Internet. Khi này để lấy được thông tin người sử dụng thường được yêu cầu điền các số liệu trong các mẫu biểu riêng biệt. Các mẫu biểu này chứa các thông tin như *tên người mua, số điện thoại, địa chỉ và quan trọng nhất là số tài khoản thanh toán điện tử...*

### 7.2.4. Người sử dụng Internet và phương thức truy cập

Mọi sự phát triển của các thành phần trên đây (IAP, ISP và ICP) sẽ trở nên vô nghĩa nếu Internet không có sự tham gia của người sử dụng thông tin. Đáng mừng là ngày nay việc gia tăng người sử dụng thông tin trên mạng Internet đang và sẽ còn phát triển như vũ bão. Hàng trăm triệu người đang trực tiếp khai thác thông tin trên mạng này. Có thể phân loại người sử dụng Internet ra các nhóm sau đây (phụ thuộc vào phương thức truy nhập của họ): **Nhóm người sử dụng Internet thông qua điện thoại quay số và modem;**



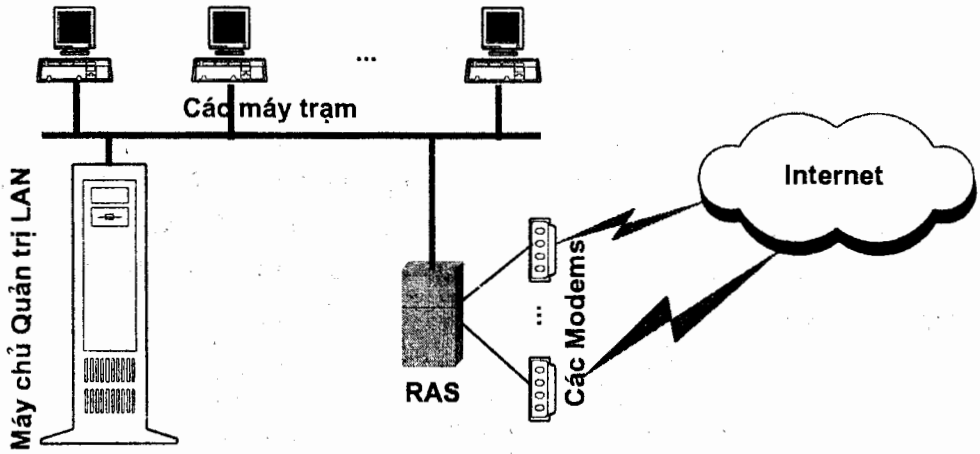

**Hình 7.2. Truy nhập Internet thông qua điện thoại/modem nối trực tiếp với máy tính**

Mỗi máy tính muốn sử dụng Internet cần được trang bị một modem và một trung kế điện thoại. Người sử dụng cần thiết lập dịch vụ mạng quay số (Dial Up Networking). Đăng nhập mạng thông qua một tài khoản (account) do ISP cấp, bao gồm tên đăng nhập và mật khẩu (hình 7.2).

Giao thức được thiết lập tại máy người sử dụng là TCP/IP Dial Up. Khi kết nối người sử dụng không cần chỉ ra IP của máy mình. Một dịch vụ cung cấp IP động DHCP đã được thực hiện từ mạng ISP. Dịch vụ này sẽ cấp cho máy kết nối Internet một địa chỉ IP trong suốt phiên làm việc.

***Nhóm người sử dụng Internet thông qua mạng LAN có máy chủ cung cấp dịch vụ truy cập từ xa RAS;***

Đây là phương thức truy nhập Internet của cộng đồng người dùng trong một mạng LAN có máy chủ cung cấp dịch vụ truy nhập từ xa RAS (Remote Access Server). Cộng đồng người sử dụng này có thể sử dụng chung một tài khoản truy cập Internet. Có thể minh hoạ phương thức truy cập này như thể hiện trên hình 7.3. dưới đây :




**Hình 7.3. Truy nhập Internet từ LAN thông RAS**

Các modems một đầu được nối với RAS, đầu kia nối với các trung kế thoại; RAS có thể là một thiết bị chuyên dụng như Lantronix LRS 8, 16 Ports, Cisco 2508/2509 (8 Ports/16 Ports)..., hoặc là một máy chủ có cắm thêm các Card mở rộng số lượng cổng COM (MultiPorts)...

Phương thức này cho phép người sử dụng thực hiện việc truy cập Internet từ bất cứ máy trạm nào trong mạng. Sau khi khai báo xong tài khoản truy cập, RAS sẽ kích hoạt modems kết nối tới Internet và nếu kết nối thành công sẽ cho phép người dùng truy cập Internet. Phương thức này cho phép số lượng người truy cập đồng thời tối đa là bằng số

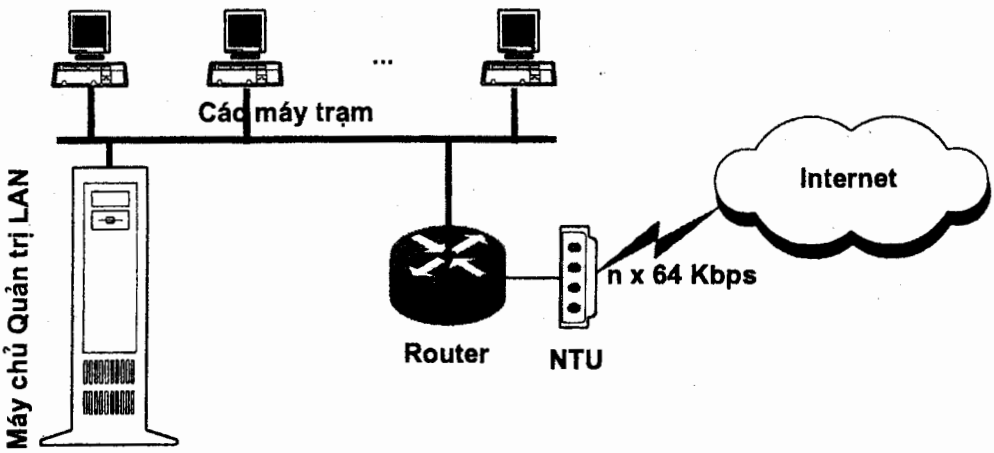
modems kết nối với RAS. Ngoài ra điểm khác biệt so với phương thức đầu là người sử dụng trên các máy trạm không cần phải nối máy tính với modem và trung kế điện thoại.

Với cộng đồng người sử dụng loại này, giao thức được thiết lập tại máy người sử dụng là TCP/IP Dial Up. Khi kết nối người sử dụng không cần chỉ ra IP của máy mình. Một dịch vụ cung cấp IP động DHCP đã được thực hiện từ mạng ISP. Dịch vụ này sẽ cấp cho máy kết nối Internet một địa chỉ IP trong suốt phiên làm việc.

***Nhóm người sử dụng Internet trực tiếp;***

Thường áp dụng cho một tổ chức đã có kết nối mạng LAN nội bộ (xem hình 7..4.). Trên cơ sở này có thể bổ sung thêm các thiết bị Router và NTU (Network Terminator Unit). Router một đầu được nối trực tiếp với mạng LAN (thông thường thông qua các bộ Hub/Switch tốc độ cao) đầu kia được nối với NTU. Về phần mình NTU một đầu nối với Router, đầu kia nối với đường truyền thông Leased Line hoặc Frame Relay ... Tốc độ của các đường thuê bao riêng thường là bội của băng thông cơ bản 64 Kbps.

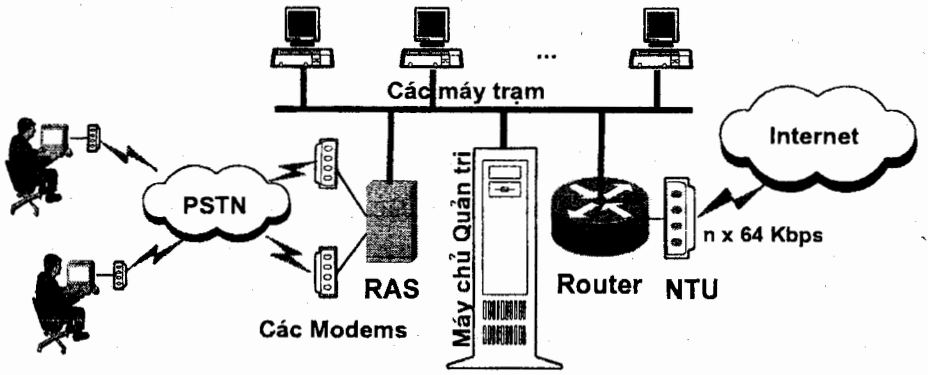
Phương thức này cho phép người sử dụng truy nhập trực tiếp vào Internet 24/24h mà không cần sử dụng modems dưới bất cứ hình thức nào. Tốc độ truy cập phụ thuộc vào băng thông được cấp cho đường Leased Line. Các Router có thể là của Cisco, như Cisco Router 2509/2511/3640. Các bộ NTU có thể là NTU 560 của NET hoặc DataCraft 560 của DataCraf.




**Hình 7..4. Truy nhập Internet từ trực tiếp**

Nhóm người sử dụng loại này còn bao gồm các thành viên của các mạng ISP và ICP (nếu mạng ICP cũng có Router và NTU như nêu trên).

Đối với mạng như thế này thường được InterNIC quốc gia cấp cho một vài địa chỉ IP tĩnh. Các IP này được gán cho các máy làm các dịch vụ Server. Các máy khác trong mạng chỉ cần thiết lập giao thức TCP thông thường (địa chỉ động hoặc tĩnh) và khi truy cập Internet sẽ được mạng ISP cấp một địa chỉ IP động.




**Hình 7..5. Truy nhập Internet thông qua LAN tại văn phòng**

***Nhóm người sử dụng Internet từ xa thông qua mạng LAN tại văn phòng;***

Đây là hình thức được sinh ra từ hai phương án trên (tận dụng khả năng của RAS và Router). Phương thức truy cập này được minh hoạ trên hình 7..5.

Hình thức này là một phương án hay. Nó cho phép người sử dụng vừa có thể truy cập Internet tại cơ quan lại vừa có thể truy cập Internet tại nhà.

Với hình thức này RAS được tổ chức như một Server dùng riêng cho cơ quan. Nó cấp quyền truy nhập từ xa vào mạng LAN của cơ quan rồi từ đó thông qua Router kết nối tới Internet.

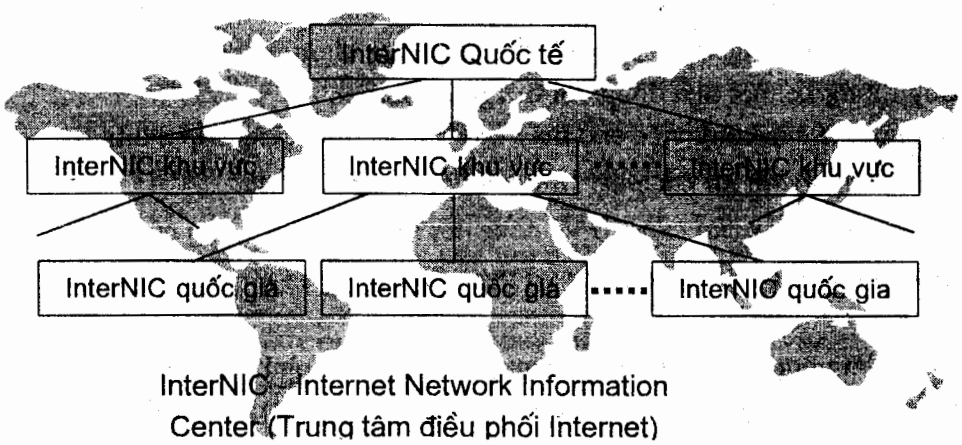
Giao thức được thiết lập tại máy người sử dụng ở xa là TCP/IP Dial Up. Khi kết nối tới mạng văn phòng người sử dụng có thể không cần chỉ ra IP của máy mình (*nếu mạng văn phòng đã thiết lập dịch vụ DHCP*). Việc tiếp tục truy nhập ra Internet sẽ được dịch vụ DHCP của mạng ISP cấp cho máy kết nối Internet một địa chỉ IP trong suốt phiên làm việc.

### 7.2.5. Các tổ chức quản lý sự vận hành của Internet

Để quản lý Internet người ta đã thành lập ra các cơ quan chức năng để quản lý mạng Internet (được thể hiện như trên *hình 7..6.*).

Nhiệm vụ chính của các InterNIC là điều phối quản lý và cấp phép sử dụng các địa chỉ IP mạng, các tên miền là thành viên trong khu vực quản lý của mình.

- InterNIC quốc tế quản lý các InterNIC khu vực.
- InterNIC khu vực quản lý các InterNIC quốc gia.
- InterNIC quốc gia quản lý các IAP, ISP, ICP.
- Các ISP về phần mình quản lý các thuê bao trực thuộc.




**Hình 7.6. Sơ đồ quản lý vận hành của Internet**

## 7.3. Công nghệ Internet

### 7.3.1. Công nghệ triển khai áp dụng của IAP

Để cung cấp các dịch vụ truy cập Internet nói riêng và liên lạc truyền số liệu nói chung IAP cần thiết phải thực hiện việc xây dựng hệ thống các thiết bị chuyển mạch số liệu trên toàn bộ khu vực địa lý cần đáp ứng việc phục vụ cung cấp các nhu cầu truyền tải dữ liệu. Thường thì các hệ thống này được thiết kế theo kiểu phân cấp : *Lớp chuyển mạch trục chính (bao phủ trên toàn vùng và có thể áp dụng chuyển mạch ATM), lớp chuyển mạch phân cấp* từ tổng đài chuyển mạch khu vực tới các tổng đài chuyển mạch gói địa phương ... Các thiết bị chuyển mạch cần hỗ trợ các dịch vụ như chuyển mạch ATM, Frame Relay, Cell Relay, liên kết mạng LAN và các dịch vụ kênh thuê bao riêng.

### 7.3.2. Công nghệ triển khai áp dụng của ICP

Như đã biết, nhiệm vụ chính của ICP là biên tập và phát triển thông tin phát hành ở dạng Web để cung cấp cho người dùng Internet. Vì vậy công nghệ áp dụng cho việc triển khai cung cấp nội dung thông tin sẽ định hướng vào : *Công nghệ áp dụng cho mạng, công nghệ biên tập thông tin và công nghệ phát hành thông tin*;

a. Công nghệ áp dụng cho mạng.

Việc áp dụng công nghệ cho mạng cần phải tuân thủ nguyên tắc : không phụ thuộc vào cấu hình phần cứng. Ngoài ra cần phải cân nhắc đến khả năng đáp ứng việc cung cấp thông tin trên mạng từ đó tính đến việc lựa chọn băng thông trong nội bộ mạng và băng thông kết nối hoà đồng với thế giới Internet.

Xét trên thực tế của công việc cho thấy có 03 hình thức cung cấp thông tin :

- *Thuê chỗ đặt thông tin tại các máy chủ của bất kỳ một ISP nào*
- *Thuê chỗ đặt một máy chủ của ICPvà cổng nối máy chủ với mạng của ISP*
- *Đặt máy chủ ở mạng nội bộ cơ quan và thuê đường truyền tốc độ cao nối vào mạng nội bộ.*

Với hai trường hợp đầu công nghệ mạng sẽ hoàn toàn phụ thuộc vào ISP và do họ thiết lập. Riêng trường hợp thứ ba cần quan tâm đến các thiết bị và giao thức truyền thông áp dụng trên mạng.

Trong thế giới của Internet giao thức mạng cần tuân thủ là TCP/IP. Việc cần quan tâm là cấu trúc mạng và băng thông cấp phối từ máy chủ tới người dùng truy cập. Băng thông này phụ thuộc vào 03 yếu tố : *Tốc độ xử lý thông tin của máy chủ, tốc độ truyền tải thông tin từ máy chủ qua đường truyền thông nội bộ tới thiết bị kết nối liên mạng* (Router) và cuối cùng là *bản thân băng thông của đường thuê bao riêng từ Router đi Internet.*

Một mạng ICP cỡ nhỏ thông thường cần có ít nhất một Server Web đủ mạnh, một tô - pô mạng hình sao và tốc độ trên đường truyền nội bộ là 100 Mbps. Đường thuê bao riêng tốc độ nên đạt ít nhất là 64 Kbps.

Đối với các ICP cỡ trung bình và lớn có thể triển khai thêm các thiết bị sao cho mỗi máy tính có thể chỉ đảm nhận một trong các dịch vụ : *Web, E-Mail, FTP, News, Telnet...*

Cuối cùng điều cần lưu ý là cấu trúc mạng lựa chọn nên là cấu trúc mở để tiện nâng cấp và mở rộng sau này.

b. Công nghệ biên tập thông tin.

Việc sản xuất thông tin cần các yếu tố : Trình biên soạn Web, các bộ Web Server và các công cụ phát triển lập trình ứng dụng trên Web.

*Biên tập các trang Web*

Khi nói đến việc biên tập Web, theo truyền thống chúng ta sẽ nghĩ ngay đến ngôn ngữ HTML (HyperText Make Up Language) và các công cụ đồ hoạ thiết kế các hoạ tiết cho Web... Việc phát triển Web có thể độc lập trên ngôn ngữ này, tuy nhiên nên lựa chọn một môi trường thân thiện hơn thay vì sử dụng ngôn ngữ này. Ngày nay FrontPage của Microsoft là giải pháp đang được lựa chọn và được xem là tối ưu hơn cả.

Đối với các Web Server có thể hướng tới một trong hai lựa chọn đó là Netscape Enterprise Server hoặc Internet Information Server. Việc lựa chọn trình Server nào là tuỳ thuộc vào giải pháp của ICP cung cấp thông tin. Thông thường người sử dụng đầu cuối có hai lựa chọn hoặc sử dụng Netscape Navigator hoặc sử dụng IE của Microsoft. Vì vậy khi biên tập Web cần chọn những lệnh, những hiệu ứng hỗ trợ chung cho cả hai.

Mặc dù HTML là ngôn ngữ Web đã được thừa nhận, song công nghệ biên tập Web lại gắn chặt với việc xây dựng các trang Web tĩnh mà những người thiết kế Web có kinh nghiệm đã từng rất quen thuộc.

Vấn đề đặt ra là công nghệ nào đáp ứng việc xây dựng các trang Web có nội dung thường xuyên thay đổi và cập nhật ?

Với sự phát triển của công nghệ phần mềm việc thiết kế các trang Web động nói trên đã và đang được thực hiện một cách có hiệu quả bằng các công nghệ mới : công nghệ ASP, công nghệ Java hoặc công nghệ PHP. Trong khuôn khổ của cuốn sách này chúng tôi muốn đề cập hai công nghệ đã và đang được hầu hết các ICP áp dụng, đó là :

- Công nghệ ASP.
- Công nghệ JAVA.

*1. Công nghệ ASP*

ASP (Active Server Page) là công nghệ xây dựng trang Web động của Microsoft. Công nghệ này có các đặc tính cơ bản sau đây :

- Cho phép tạo một giao diện tương tác giữa web Server với người sử dụng, tạo và chạy các ứng dụng Web Server động truy cập tới cơ sở dữ liệu trên Server.
- Các mã ASP thường được kết hợp với một số ngôn ngữ Script phổ biến như JavaScript hay VbScript nhằm tăng hiệu năng sử dụng và tạo nên sự linh hoạt trong lập trình. VBScript là ngôn ngữ mặc định của ASP, khi sử dụng ngôn ngữ Script khác bắt buộc phải định nghĩa ngôn ngữ ở đầu trang bằng dòng <%@LANGGUAGE= 'tên ngôn ngữ'%>.
- Các chức năng được thực hiện bằng ASP sẽ được Web Server nhận biết bằng file có phần mở rộng là ".asp". Cũng giống như với HTML, các thẻ được bắt

đầu và kết thúc bằng cặp "< />", một đoạn mã asp bắt đầu và kết thúc bởi cặp thẻ "<% %>". Các thẻ HTML có thể được thực thi trong các file .asp tương đương như trong các file .html và trong đó các đoạn mã ASP có thể xuất hiện bất kỳ đâu. Điều này thể hiện sự gắn bó chặt chẽ giữa ASP và HTML tạo nên sự linh hoạt, uyển chuyển trong việc thể hiện các tương tác của website. Khi một file .asp được kích hoạt bởi một người truy cập ở phía client thì mọi quá trình xử lý file .asp đó sẽ diễn ra trên server thay vì trên client, webserver sẽ làm mọi việc cần thiết và trả về cho trình duyệt trên client một file kết quả dạng HTML.

- Mỗi khi có một người sử dụng thông qua trình duyệt Web như Internet Explore hay Nestcape Navigator... gửi yêu cầu tới một file .asp ở phía máy chủ, các Script trong file .asp đó sẽ được thực thi trên Server và sau đó gửi trả kết quả về cho Browser đó. Kết quả mà Web Server trả về cho Browser sau khi thực hiện một file .asp luôn luôn là một trang HTML.

Các ASP được xây dựng dựa trên hình thức giống như các ngôn ngữ lập trình hướng đối tượng, đồng thời ASP có cũng có các đối tượng của riêng nó đi kèm như: *Request, Response, Application, Server, Session*. Không những vậy, ASP còn có thể tận dụng được các ActiveX Components như: *Database access, Content Linking, Collaboration Data Object, Browser Capabilities, File Access*... cũng như các component được cung cấp từ nhiều nhà cung cấp khác nhau dưới dạng các file .dll. Những đối tượng, những đặc điểm này của ASP đã đem lại những lợi ích xác thực, cho phép tạo ra những Website thương mại hấp dẫn, có tương tác qua lại với người sử dụng chứ không chỉ chứa những nội dung tĩnh đơn thuần. Các đối tượng của ASP bao gồm :

- *Response Object:* là công cụ để gửi thông tin tới *User*, là đại diện cho phần thông tin trả về cho Web Browser. Hoàn toàn có thể sử dụng đối tượng này để viết lên màn hình, định hướng các trang, tạo các *Cookies*.
- *Request Object:* cho phép lấy thông tin qua một *HTTP Request* và có thể sử dụng *Request Object* để đọc *URL*, truy cập thông tin từ một form, đọc *Cookie* và các *HTTP Header*.
- *Application Object:* được sử dụng để điều khiển các đặc tính liên quan đến việc khởi động và dừng ứng dụng cũng như việc lưu trữ các thông tin có thể được truy cập bởi các ứng dụng nói chung.
- *Server Object:* cho phép thực thi một chuỗi các ứng dụng một chuỗi các tác vụ nói chung như ánh xạ một đường dẫn ảo tới một đường dẫn vật lý và tạo thể hiện của một thành phần.
- *Sesion Object:* được sử dụng để lưu trữ thông tin về từng *user* đã truy cập vào website.

*2. Công nghệ Java*

Như đã biết Java là công nghệ phát triển Web của Sun Microsystems. Công nghệ này có các đặc tính cơ bản dưới đây :

➢ *Java là ngôn ngữ hướng đối tượng thuần tuý*

Khác với một số ngôn ngữ hướng đối tượng như C++, Java là ngôn ngữ hướng đối tượng thuần tuý. Tất cả các thao tác, các công cụ hay các chức năng tự xây dựng đều được thực thi thông qua hành vi của các đối tượng cụ thể.

➢ *Java là ngôn ngữ có tính linh hoạt cao*

Có thể nói rằng đây chính là một trong những điểm nổi bật nhất của Java so với các ngôn ngữ khác. Một chương trình Java có thể chạy trên mọi loại máy chỉ với điều kiện có cài trình thông dịch Java. Đầu tiên, mã nguồn Java được trình biên dịch Java dịch sang một loại mã đặc thù được gọi là mã "*byte code*". Sau đó, mã *byte* này vào lúc chạy sẽ được trình thông dịch Java dịch lại một lần nữa và chạy trên máy ảo của Java. Một chương trình Java có thể chạy trên bất kỳ máy nào có cài đặt máy ảo Java.

➢ *Java là ngôn ngữ có hiệu năng cao*

Hiệu năng của chương tình Java còn được cải thiện đáng kể nhờ khả năng xử lý đa tuyến đoạn. Java cho phép trong khi lập trình có thể tạo ra nhiều tuyến đoạn đồng hành để giải quyết nhiều việc cùng một lúc. Kỹ thuật đa tuyến đoạn cũng được vận dụng để giải quyết vấn đề của Java là dọn dẹp bộ nhớ một cách tự động.

➢ *Java là môi trường xử lý phân tán*

Chương trình Java có thể thực thi với các đối tượng định vị trên các máy khác nhau phân tán trên mạng. Bên cạnh đó, các cơ chế truyền thông điệp giữa các đối tượng Java cũng rất thuận tiện cho lập trình phân tán.

*Java là môi trường an toàn*

Ngôn ngữ Java có tính an toàn cao bằng một mô hình với bốn tầng bảo vệ. Người sử dụng đầu cuối trên mạng sẽ không phải lo tới chuyện bị Virus xâm nhập khi thực thi một ứng dụng Java hay chạy một Applet.

Có thể nói so với các ngôn ngữ lập trình khác thì Java là một ngôn ngữ khá toàn diện và thân thiện. Trong khuôn khổ của cuốn sách này sẽ đề cập tới mảng lập trình Web với công nghệ Java mà điển hình là công nghệ Applet, JSP và Servlet:

*Applet*

Applet là một ứng dụng được viết bằng Java mà có thể chạy trực tiếp trên trình duyệt của máy khách khi nó được gắn vào một file văn bản HTML. Một Applet khi chạy trên trình duyệt có khả năng tạo ra rất nhiều điều hấp dẫn và đó cũng chính là một trong những điểm mạnh của Java. Tuy nhiên, theo như "*tôn chỉ*" đã nói ở trên thì Java

là ngôn ngữ có tính an toàn cao, vì vậy ứng dụng ký sinh phải chịu một số các ràng buộc:

- Ứng dụng Applet không thể đọc hay ghi tập tin trên đĩa cứng của máy khách trừ khi có sự cho phép từ phía người dùng.
- Ứng dụng Applet không thể kết nối với một máy chủ nào khác trừ máy chủ mà từ đó nó xuất phát.
- Ứng dụng Applet không thể tự kích hoạt bất cứ một chương trình nào trên máy khách.
- Ứng dụng Applet không được phép nạp xuống máy khách chương trình ở dạng mã đặc thù của máy khách. Chẳng hạn, nếu đang dùng Windows, một Applet sẽ không thể nạp các tập tin .dll xuống máy của người sử dụng.

*Servlet*

- Servlet là một công nghệ dựa trên nền Java được lựa chọn để mở rộng và nâng cao hiệu năng của một Web Server. Servlet hoạt động trên Web Server và nó cung cấp một thành phần cơ sở, một phương thức độc lập với Platform để xây dựng các ứng dụng web cơ bản mà không bị ảnh hưởng bởi những hạn chế của các CGI.
- Servlet có quyền truy cập tới toàn bộ các API của Java bao gồm cả các JDBC API được sử dụng để truy cập tới cơ sơ dữ liệu xí nghiệp. Ngoài ra, Servlet cũng có thể truy cập tới thư viện các đặc trưng của HTTP và tất cả những thuận lợi của ngôn ngữ lập trình Java bao gồm tình khả chuyển, hiệu năng cao, độ an toàn cao...
- Các Servlet độc lập với Platform, 100% các module hoạt động trên Server và phù hợp với cơ cấu của Web Server.

*JSP (Java Sever Page)*

- JSP là một công nghệ cho phép những người phát triển và thiết kế Web có thể phát triển các Website một cách nhanh chóng và duy trì Website đó dễ dàng.
- Công nghệ JSP tạo khả năng phát triển các ứng dụng trên Web mà độc lập với Platform.
- Công nghệ JSP tách rời giao diện người sử dụng với việc tạo nội dung cho một Website, điều này tạo khả năng cho người thiết kế có thể thay đổi toàn bộ thiết kế về giao diện hay cách bố trí các trang mà không phải thay đổi nội dung động.
- JSP sử dụng các thẻ như XML và các Scriptlet được viết bằng ngôn ngữ Java để tóm lược lại logic đã tạo nên nội dung cho một trang. Thêm vào đó, một ứng dụng logic có thể được đặt trong các tài nguyên trên server (ví dụ như kiến trúc JavaBean) mà một trang Web có thể truy cập bằng cách sử dụng các thẻ và các

Scriptlet này. Tất cả các thẻ kể cả thẻ HTML hay XML đều được truyền trở về trang phản hồi một cách trực tiếp. Bằng cách tách rời logic của các trang với các thiết kế, sự hiển thị đồng thời hỗ khả năng thiết kế dựa trên các thành phần có thể sử dụng lại, JSP đã làm cho nó hoạt động nhanh hơn và dễ dàng hơn các ứng dụng trên Web trước đây.

➢ JSP là sự mở rộng của Java Servlet API. Cùng với Servlet, JSP cung cấp một thay đổi hấp dẫn tới các dạng khác của các Script hay các chương trình Web động mà bị hạn chế bởi sự phụ thuộc vào Platform, đồng thời nâng cao hiệu năng của hệ thống, tách rời sự thể hiện với logic, tạo sự dễ dàng cho người quản trị, có thể mở rộng vào môi trường xí nghiệp và quan trọng nhất là dễ dàng sử dụng.

***Tổ chức hệ thống thư điện tử và các chuẩn giao thức liên quan***

*Tổ chức hệ thống thư điện tử* :

Việc tổ chức hệ thống thư tín điện tử đòi hỏi phải có phần mềm Mail Server. Hiện nay có rất nhiều hệ thống Mail Server được biết đến trong môi trường Internet. Tuy nhiên thịnh hành nhất vẫn là Netscape Mail Server và Microsoft Exchange. Các phần mềm này có thể cài trên các máy Server riêng biệt hoặc cài chung với máy cung cấp dịch vụ Web.

Các công việc chính bao gồm :

➢ Thu thập các hồ sơ của các users đăng ký sử dụng dịch vụ.

Những tham số quan trọng nhất cần phải có là *tên, mật khẩu và dung lượng đĩa* cần sử dụng.

➢ Cài đặt và cấu hình hệ thống phần mềm Mail Server.

Tuỳ theo từng phần mềm Mail Server mà quá trình cài đặt và cấu hình có thể khác nhau, tuy nhiên quan trọng nhất trong phần này cần phải khai báo là :

- Địa chỉ IP của Mail Server;
- Giao thức E-Mail được dùng;
- Cấp phép sử dụng dịch vụ E-Mail cho người dùng.

*Hướng dẫn sử dụng các dịch vụ Mail tương ứng của ICP.*

- Thông báo cho các user về tài khoản E-Mail đã cấp;
- Các cách thiết lập phần mềm để sử dụng dich vụ E-Mail. Bao gồm các thông tin như: *địa chỉ IP của máy chủ cung cấp dịch vụ E-Mail, giao thức được áp dụng cho dịch vụ.*

***Các chuẩn giao thức liên quan* :**

Có 04 công đoạn liên quan đến việc gửi và nhận thư :

- *SMTP Client*: thu nhận các thông tin mà người sử dụng nhập vào như là: địa chỉ của người nhận, nội dung bức thư,..., mã hoá dữ liệu rồi gửi vào mailbox của SMTP Server.
- *SMTP Server*: thực chất đây là mail server mà tại đây người gửi có thuê bao.
- *POP3 Server*: đây là mail server nhận thư từ SMTP Server.
- POP3 Client: lấy thông tin từ POP3 Server, giải mã chúng để hiện nội dung của bức thư cho người nhận.

*Để hiểu rõ về bản chất của việc gửi / nhận thư giáo trình sẽ đề cập một cách cô đọng nhất đến các chuẩn giao thức liên quan :*

*1. Chuẩn giao thức SMTP*

SMTP là viết tắt của tập hợp từ Simple Mail Transfer Protocol (*giao thức gửi thư đơn giản*). Là một giao thức truyền thư hiệu quả và tin cậy, chúng được phát triển cho các hệ thống mạng sử dụng họ giao thức TCP/IP. Một đặc điểm quan trọng của SMTP là khả năng chuyển tiếp các thư qua các môi trường dịch vụ giao vận. Một dịch vụ giao vận cung cấp một môi trường truyền thông liên tiến trình (InterProcess Communication Environment – IPCE).

*SMTP được thiết kế dựa trên cơ sở của mô hình liên lạc như sau*:

- Khi bên gửi có một yêu cầu truyền thư thì nó sẽ thực hiện một kênh liên lạc hai chiều với bên nhận. Kênh liên lạc hai chiều này cho phép hai bên có thể thực hiện gửi thông tin qua lại với nhau. Bên nhận có thể là đích cuối hoặc là một đích trung gian.
- Bên gửi sẽ tạo ra các lệnh gửi cho bên nhận, do đó khi nhận được các lệnh này thì bên nhận sẽ gửi lại các trả lời. Mỗi lần một kênh liên lạc được thực hiện thì bên gửi sẽ gửi lệnh MAIL để chỉ ra bên gửi thư, nếu bên nhận chấp nhận thư thì nó sẽ gửi lại OK để trả lời. Sau đó bên gửi sẽ gửi lệnh RCPT để chỉ ra bên nhận thư.
- Nếu bên nhận có thể nhận thư cho người nhận thì nó sẽ gửi lại trả lời OK, nếu không nó sẽ gửi trả lời không chấp nhận người nhận đó.
- SMTP cung cấp cơ cấu truyền thư, cho phép host của người gửi làm việc trực tiếp với host của người nhận khi hai host này được liên kết đến cùng một dịch vụ giao vận, hoặc qua một hoặc nhiều SMTP-server trung gian trong trường hợp host nguồn và đích không liên kết đến cùng một dịch vụ giao vận. Để có thể cung cấp khả năng chuyển tiếp thì SMTP-server phải được cung cấp tên của host đích cuối giống như là tên của mailbox định gửi tới.
- Các lệnh và câu trả lời được xây dựng từ một tập các ký tự ASCII. Khi dịch vụ giao vận cung cấp một kênh truyền 8-bit thì chỉ có 7-bit được sử dụng còn

bit cao nhất sẽ được xóa về 0. Các tham số được biểu diễn trong một dấu nháy kép và một cặp dấu ngoặc nhọn như: "tuanhm-it@aic.com.vn".

*Các thủ tục của SMTP* bao gồm :

- *Thủ tục Mail*, bao gồm 03 bước : *xác định* người muốn gửi thư, đưa ra *đường dẫn* đến người nhận và *nhận và lưu trữ* dữ liệu của thư.
- *Thủ tục Forwarding*, chuyển tiếp thư đến các địa chỉ liên quan.
- *Thủ tục mailing* và *sending* : thủ tục *mailing* là thủ tục chuyển thư đến các hộp thư (mailbox) của người sử dụng còn thủ tục *sending* là thủ tục chuyển thư đến các trạm đầu cuối (terminal).
- *Thủ tục openning* và *closing* là các thủ tục mở và đóng một kênh truyền thư giữa các máy chủ.
- *Thủ tục Domain*, là thủ tục thay đổi địa chỉ trống bằng tên host. Tên host được thay thế bởi domain là host được chỉ định, các phần tử trong tên host đứng cách nhau bởi dấu chấm.
- *Thủ tục thay đổi vai trò (changing roles)*, là thủ tục thay đổi giữa vai trò gửi và nhận thư.

*2. Chuẩn giao thức POP3*

POP3 là viết tắt của tập hợp từ Post Office Protocol Version 3 (Giao thức bưu điện văn phòng phiên bản 3) được dùng cho phép các workstation truy cập đến các maildrop ở trên server host. Thông thường dịch vụ POP3 được sử dụng cho phép một workstation lấy thư từ một server khác.

*Cơ chế làm việc của POP3 như sau :*

- Ban đầu, Server host sẽ bắt đầu với dịch vụ POP3 bằng cách "*lắng nghe*" ở trên TCP thông qua cổng 110. Khi Client muốn sử dụng dịch vụ nó sẽ thiết lập một kiên kết TCP với Server host.
- Sau khi việc kết nối đã được thiết lập, POP3 Server sẽ gửi một lời chào mừng. Client và POP3 Server sẽ trao đổi lệnh và các phản hồi trở lại cho tới khi quá trình kết nối đó kết thúc hoặc bị ngắt.

Câu lệnh trong POP3 bao gồm phần từ khoá và tiếp theo là một hoặc nhiều đối số. Các phản hồi trong POP3 bao gồm các trạng thái chỉ thị (status indicator). Mọi phản hồi trở lại đều được kết thúc bởi cặp CRLF.

*Các phiên làm việc của POP3 :*

Được tiến hành thông qua một số trạng thái. Khi TCP thực hiện kết nối xong thì POP3 server sẽ gửi một lời chào mừng và phiên làm việc bắt đầu với trạng thái AUTHORIZATION. Trong giai đoạn này Client đã được kết nối với POP3 Server. Sau khi Client đã hoàn thành kết nối, Server sẽ tiến hành tìm kiếm Maildrop của Client và

thực hiện trả lại thông tin phản hồi. Tiếp theo là phiên làm việc với trạng thái TRANSACTION. Trong giai đoạn này Client sẽ có các yêu cầu tác động lên POP3 Server. Sau khi Client nhận được kết quả, nó sẽ đưa ra lệnh QUIT. Khi đó phiên làm việc sẽ bắt đầu với trạng thái UPDATE: POP3 Server sẽ thoát khỏi sự đòi hỏi của TRANSACTIONs và kết nối TCP sẽ được đóng lại.

c. Công nghệ phát hành thông tin.

Việc phát hành thông tin như thế nào cho khoa học và mang lại nhiều lợi nhuận là cả một nghệ thuật. Nhìn chung cần phải khảo sát một cách kỹ càng cách thức khai thác thông tin từ phía người sử dụng để từ đó áp dụng phân loại thông tin, chia nhỏ đến mức vừa phải nhằm tránh cảm giác nhàm chán hoặc khó khai thác.

Công nghệ phát hành tin cần quan tâm đến các khía cạnh dưới đây :

- Thiết kế một trang chủ : gọn, nhẹ có tĩnh mỹ thuật cao;
- Các mục tin cần được phân cấp một cách hợp lý tránh tình trạng quá vụn vặt hoặc quá phức tạp;
- Kết hợp hài hoà giữa việc bố trí văn bản chữ và việc thể hiện đồ hoạ và các hiệu ứng trong các trang;
- Nên có các mục *tìm kiếm thông tin, diễn đàn trao đổi* và *tin nóng* ...
- Phân trang trên nguyên tắc một trang Web người dùng không mất quá 30s để tải đầy đủ các nội dung về máy mình...
- Đối với những mục tin nội bộ hoặc mục tin với mục đích kinh doanh cần phát triển các ứng dụng hướng tới mục đích quản lý, giám sát và thu cước phí dựa trên nguyên tắc *thâm nhập phải được kiểm soát và trả phí* (thông thường trình quản lý sẽ đưa ra một mẫu biểu đòi hỏi người sử dụng phải tự hoàn tất trước khi họ có thể kiết xuất thông tin).

### 7.3.3. Công nghệ triển khai áp dụng của ISP

Khác với các ICP nhiệm vụ của một ISP bao gồm toàn bộ công việc của ICP ngoài ra còn thêm các nhiệm vụ riêng đó là *cung cấp các dịch vụ Internet.*

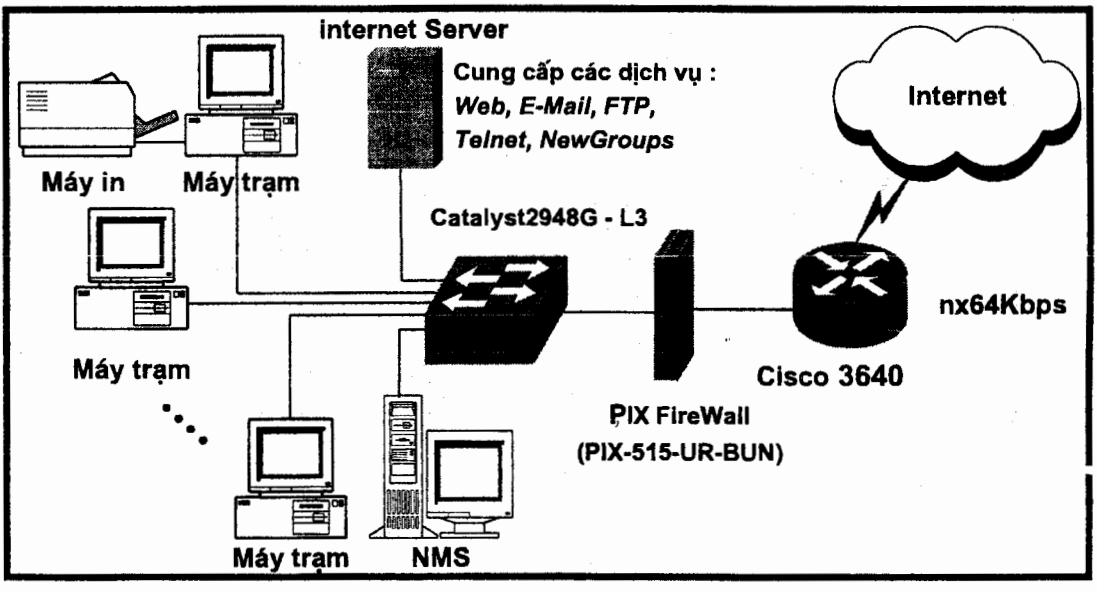
Vì vậy đối với các ISP nhất thiết phải có mạng riêng của mình và đường thuê bao kết nối tốc độ cao tới Internet.

ISP phục vụ một lượng lớn các thuê bao Internet vì thế bên cạnh việc sử dụng các máy chủ mạnh là thì các thiết bị kết nối mạng cũng cần có hiệu năng mạnh tương xứng.

Có thể tóm lược những nét chính sau đây :

- Sử dụng các máy chủ có cấu hình mạnh dùng để cung cấp các dịch vụ Internet và có thể sử dụng mỗi máy đảm nhận riêng một dịch vụ;

- Sử dụng giao thức mạng là TCP/IP;
- Sử dụng tô-pô mạng là tô-pô hình sao và cấu trúc mở;
- Dùng Switch tốc độ Gbps trên mạng cung cấp các dịch vụ;
- Ngoài Router tốc độ cao kết nối với Internet cần có thêm thiết bị phục vụ truy cập từ xa RAS (Remote Access Server). Thiết bị này cần thoả mãn đáp ứng các nhu cầu truy cập qua modem quay số điện thoại và cả những nhu cầu kết nối tốc độ cao đối với các tổ chức cá nhân có mong muốn kết nối tốc độ cao thông qua Router và đường thuê bao số tốc độ cao;
- Cần có các hệ thống bức tường lửa (Firewall) để ngăn chặn các truy nhập không hợp pháp hoặc không đủ thẩm quyền hoặc sự cố tấn công mạng;
- Cần có các thiết bị làm nhiệm vụ tải trước dữ liệu (caching);
- Đối với các ISP cỡ lớn cần có thêm đường kết nối Internet dự phòng để khắc phục các rủi do khi có sự cố đối với đường kết nối Internet.




**Hình 7.7. Sơ đồ thiết kế mạng ICP thông thường**

### 7.3.4. Các ví dụ minh hoạ thiết kế một số mạng

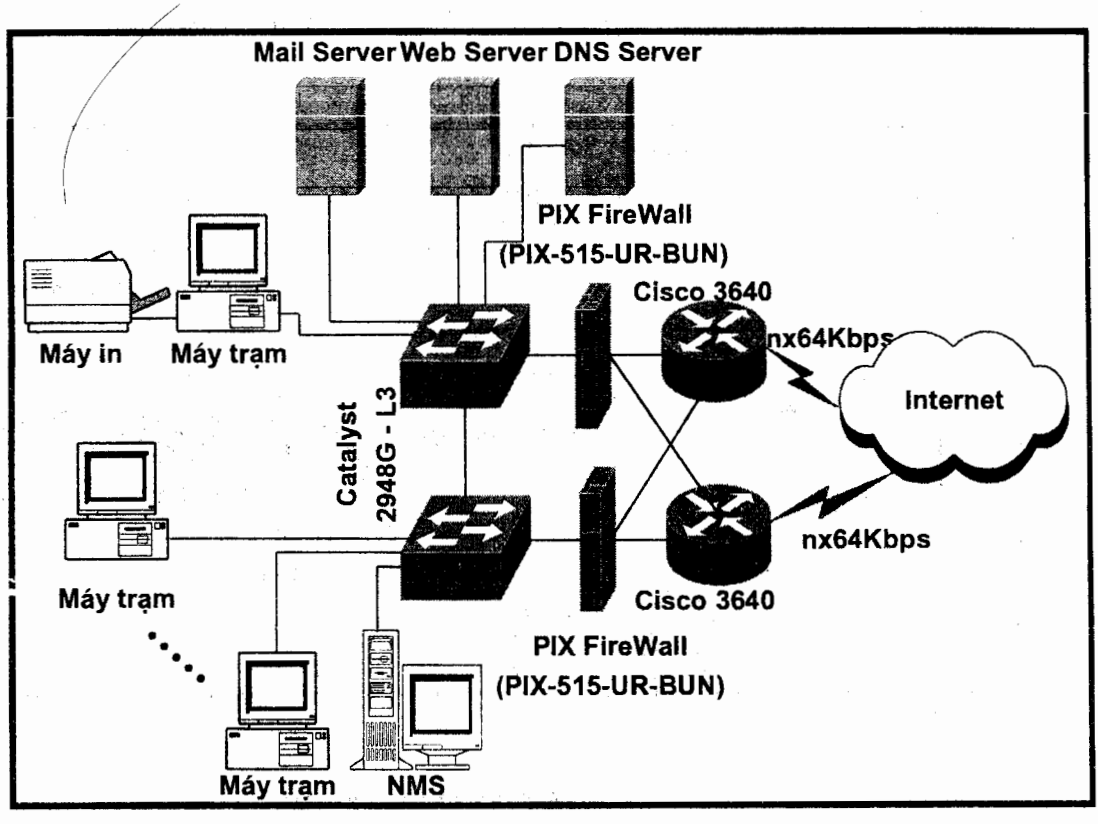
Dưới đây là một vài thiết kế minh hoạ :

*Ví dụ 1 :* Sơ đồ thiết kế mạng ICP thông thường (*xem hình 7.7*)

Tất cả các dịch vụ Internet cơ bản được một máy chủ đảm trách (*Internet Server*) bao gồm : *Dịch vụ Web, Dịch vụ FTP, Dịch vụ E-Mail, Dịch vụ Telnet và Dịch vụ NewGroups*.

- Các thiết bị đều nối về Switch tốc độ cao (1 Gbps). Như vậy các máy đều có giao diện Card mạng tốc độ 1 Gbps tương ứng.
- Firewall là thiết bị phần cứng chuyên dụng, bên trong đã tích hợp hệ thống phần mềm Firewall cần thiết.
- Firewall nằm giữ Router của mạng và mạng. Một cổng được kết nối với Router, một cổng được nối với Switch và như vậy tốc độ vào và ra của Firewall là như nhau (đều là tốc độ 1 Gbps).

Có thể bỏ Firewall nếu không xét đến tính an toàn bảo mật, hoặc coi như đã có Firewall ở mức quốc gia.




**Hình 7.8. Sơ đồ mạng ICP có đường dự phòng & mỗi máy chủ làm một nhiệm vụ**

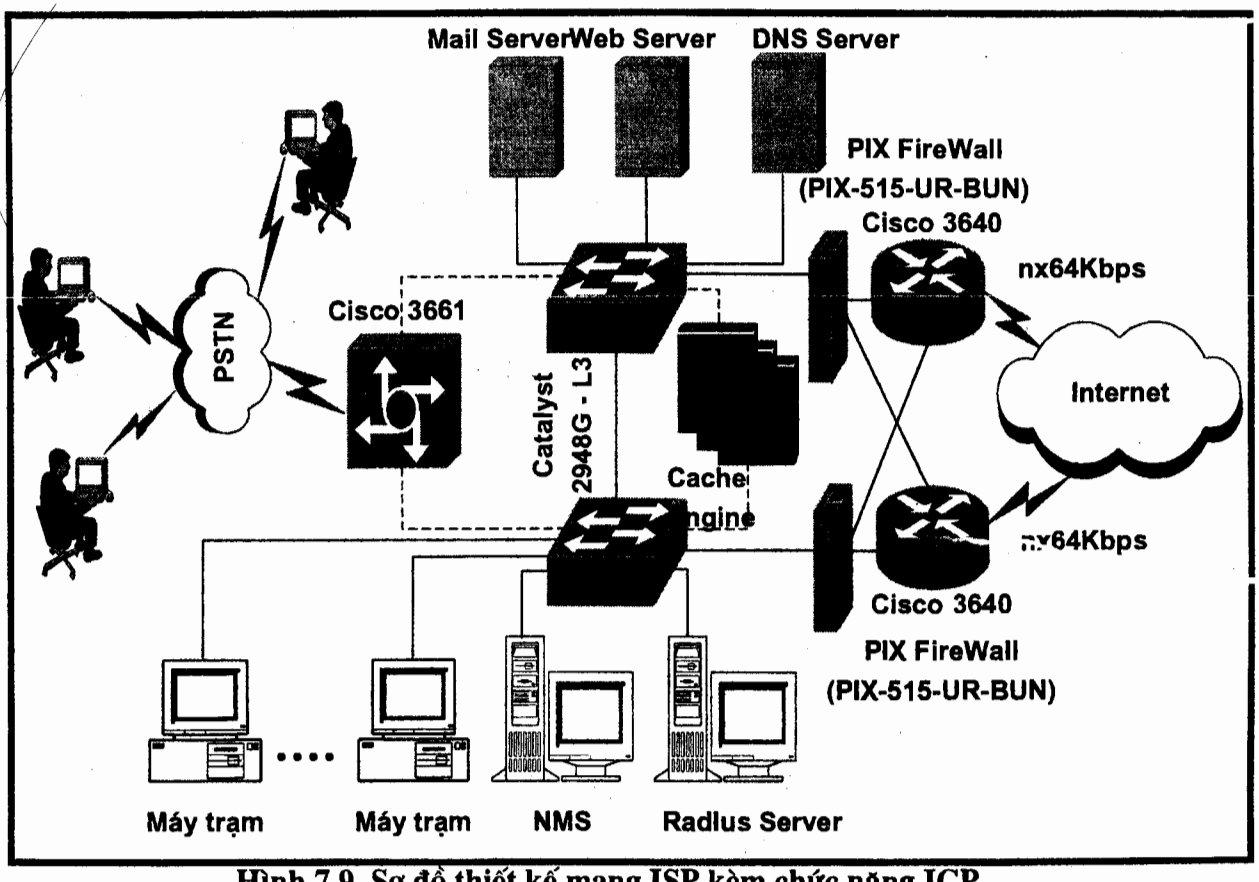
*Ví dụ 3 :* Sơ đồ thiết kế mạng ICP có đường thuê bao dự phòng ngoài ra Web, Mail và DNS Server được chạy trên các máy riêng biệt (*xem hình 7.8.*)

Ví dụ này hoàn toàn *giống với ví dụ 1* ngoại trừ một điều ở đây sử dụng thêm 1 tuyến dự phòng bao gồm :

- Bổ sung một đường thuê bao riêng (*leased line nx64 Kbps*),
- Bổ sung thêm 1 Router,
- Bổ sung thêm 1 Gbps Switch và hai Switch này nối trực tiếp với nhau.

Với phương án này khi có 1 đường thuê bao riêng bị trục trặc, đường kia vẫn sẽ đảm nhận việc truy cập của người sử dụng Internet (tất nhiên băng thông sẽ nhỏ hơn) trong khi chờ đợi khắc phục các sự cố đường truyền. Mỗi dịch vụ Internet được thiết lập riêng rẽ trên một máy chủ.

*Ví dụ 4 :* Sơ đồ thiết kế mạng ISP kèm chức năng ICP với công nghệ hiện đại (*xem hình 7.9.*)




**Hình 7.9. Sơ đồ thiết kế mạng ISP kèm chức năng ICP**

Đây là một thiết kế áp dụng các công nghệ tiên tiến ở thời điểm hiện tại. Về cơ bản nó là sự bổ sung kế thừa của phương án mạng ICP như đã nêu trong ví dụ 3. Mạng được bổ sung thêm một số thiết bị sau :

- Thiết bị cung cấp dịch vụ truy cập từ xa (RAS),
- Thiết bị tải trước dữ liệu (Caching Engine).

Mạng này một phía cho phép cộng đồng người sử dụng Internet thông qua Router và Firewall thâm nhập các Server cung cấp thông tin Internet của mạng ISP. Phía bên kia cho phép các thuê bao Internet (sử dụng modem và điện thoại) của ISP truy nhập vào các kho thông tin này thông qua RAS và có thể từ đây dẫn đến các máy chủ cung cấp thông tin Internet khác trên toàn thế giới (đi qua Firewall và Router). RAS trong sơ đồ này là loại đã tích hợp các modems số ngay trong thiết bị.

## 7.4. Hệ thống các máy chủ

Internet vận hành và ngày càng mang lại những hiệu quả to lớn cho nhân loại là nhờ hệ thống các dịch vụ mà nó đáp ứng nhu cầu không ngừng gia tăng của cộng đồng người sử dụng. Mỗi dịch vụ cung cấp được gọi là Server. Các máy cung cấp các dịch vụ Server này được gọi là máy Server hay còn được gọi dưới một tên khác là Host và được hiểu là máy chủ. Xét về các chức năng thực sự mà các máy tính này đảm nhiệm thì cụm từ được dùng một cách ưa chuộng hiện nay là "*máy chủ*" là hoàn toàn không chính xác. Bởi vì chúng là các *máy phục vụ* - một chức năng hoàn toàn khác hẳn so với tên gọi của nó. Tuy nhiên giáo trình này sẽ không bàn đến tính chính xác của tên gọi mà sẽ tập chung vào tìm hiểu các chức năng đích thực của hệ thống các máy chủ trên Internet. Chúng là những thành phần quan trọng và không thể thiếu được trong Internet. Tuỳ theo chức năng cung cấp dịch vụ mà hệ thống máy chủ có thể được phân loại như sau :

- Hệ thống máy chủ cung cấp các dịch vụ Internet,
- Hệ thống máy chủ quản lý người dùng trong mạng,
- Hệ thống máy chủ hỗ trợ chất lượng dịch vụ,
- Hệ thống máy chủ bảo đảm an ninh và an toàn dữ liệu,
- Hệ thống máy chủ giám sát và quản lý truy nhập,
- Hệ thống máy chủ cung cấp dịch vụ truy cập từ xa,
- Hệ thống máy chủ cung cấp các ứng dụng cơ sở dữ liệu, và
- Hệ thống máy chủ phục vụ in ấn.

### 7.4.1. Hệ thống máy chủ cung cấp các dịch vụ Internet

Các dịch vụ quen thuộc đối với cộng đồng người sử dụng Internet bao gồm : *E-Mail, FTP, NewGroups, Telnet* và quan trọng nhất là *World Wide Web (WWW)*. Nhìn chung khi nhu cầu cung cấp dịch vụ ISP và ICP chưa lớn các dịch vụ này có thể được thiết lập trên một máy tính có cấu hình đủ mạnh. Tuy nhiên trên thực tế vì cả lý do an toàn lẫn chất lượng dịch vụ đòi hỏi ngày càng cao các dịch vụ này nên được cài đặt riêng rẽ trên từng máy tính. Như vậy hệ thống máy chủ sẽ bao gồm : *máy chủ cung cấp dịch vụ E-Mail, máy chủ cung cấp dịch vụ truyền File, máy chủ cung cấp tin tức, máy chủ cung cấp dịch vụ Telnet và máy chủ cung cấp dịch vụ Web.*

### 7.4.2. Hệ thống máy chủ quản lý người dùng trong mạng

Dù là một mạng LAN thông thường hay là mạng Internet thì hệ thống mạng nào cũng cần có máy chủ quản lý cộng đồng người sử dụng mạng trực tiếp của mình. Việc quản lý được phản ánh thông qua việc cấp tài khoản, cấp quyền truy nhập và sử dụng tài nguyên, cấp quyền quản lý và cấp phát các dịch vụ .... Ví dụ với các mạng công nghệ Windows NT được biết đến là các máy chủ quản lý domain chính PDC (Primary Domain Controller) và máy chủ quản lý tài khoản sao lưu BDC (Backup Domain Controllerr). Với các mạng NT nói trên hệ thống máy chủ quản trị Domain có thể là rất nhiều và được tổ chức dưới các mô hình rất khác nhau và mô hình thường được áp dụng nhiều nhất là mô hình Domain uỷ quyền...

### 7.4.3. Hệ thống máy chủ hỗ trợ chất lượng dịch vụ

Chất lượng Internet tốt hay chưa tốt phụ thuộc rất nhiều vào các *máy chủ hỗ trợ chất lượng dịch vụ*. Các máy chủ này bao gồm các thành phần chính như : máy chủ *quản trị tên miền DNS* (Domain Name Service), máy chủ *uỷ quyền* (proxy), máy chủ làm nhiệm vụ *Caching (tải trước)*dữ liệu ...

- Máy chủ quản trị tên miền lưu giữ một cơ sở dữ liệu tên miền là các bảng địa chỉ IP tương ứng với các tên mà các máy trên Internet được đặt. Tên và IP được cấp phát và quản lý bởi các tổ chức có tên là InterNIC (InterNIC quốc tế, InterNIC khu vực và InterNIC quốc gia). Nhiệm vụ đích thực của máy chủ DNS là việc thông dịch các tên bí danh thành các địa chỉ IP để từ đó có thể biết được luồng truy nhập sẽ đến máy chủ nào trong số các máy chủ trên Internet.
- Máy chủ uỷ quyền Proxy được ra đời xuất phát từ hai nguyên nhân chính : an toàn thông tin và nhu cầu truy cập nhanh. Để khắc phục các sự cố tấn

công trên mạng (điều này thường xuyên xảy ra) thường ở biên của mạng (cổng giao lưu giữa trong mạng và bên ngoài) được đặt một máy chủ uỷ quyền. Máy này có nhiệm vụ là người đại diện cho mạng cung cấp và kiểm duyệt các dịch vụ vào ra trong mạng. Các thông tin vào ra mạng được đặc trưng bởi địa chỉ IP của máy này trong khi các máy cung cấp dịch vụ Internet đích thực nằm phía trong mạng không để lộ các thông tin về IP... Ngoài ra Proxy Server còn làm nhiệm vụ *caching* dữ liệu để tăng hiệu quả truy cập Internet.

- Máy chủ làm nhiệm vụ *Caching* được thiết lập trong các mạng ISP lớn. Với các mạng này việc máy chủ đảm nhiệm chức năng uỷ quyền kèm chức năng *caching* dữ liệu sẽ không còn thích hợp xét về góc độ tốc độ đáp ứng dịch vụ. Các nhiệm vụ chủ yếu của nó bao gồm : *tải trước các thông tin* mà người dùng có thể yêu cầu về máy (và do đó khi truy cập Internet nhiều khi các dữ liệu thay vì phải sục sạo ở nhiều nơi có thể được lấy ngay từ máy chủ *Caching* này), *tối ưu hoá* việc sử dụng băng thông và *tăng cường giám sát nội dung thông tin*. Hiện nay Cisco đã đưa ra thiết bị chuyên dụng có hiệu năng rất cao có tên gọi là Cache Engine CE 550.

### 7.4.4. Hệ thống máy chủ bảo đảm an ninh và an toàn dữ liệu

Đối với các ISP chuyên nghiệp việc bảo đảm an toàn và an ninh thông tin luôn được đặt lên hàng đầu. Xuất phát từ lý do này trong các mạng ISP, máy chủ Firewall luôn luôn đảm bảo chỗ đứng của mình. Chức năng chính của Firewall là *ngăn chặn các truy cập bất hợp pháp* dưới mọi hình thức, *theo dõi quản lý và phân tích* những hiện tượng tấn công mạng bất hợp pháp, *thống kê* tần suất truy cập, *thiết lập các địa chỉ cấm* truy cập và *bảo vệ mạng nội bộ khỏi bị tấn công từ bên ngoài* (bằng việc so sánh các packet bên trong, bên ngoài với các dòng của một bảng. Truy nhập chỉ được cho phép khi trong bảng chỉ ra như vậy).

Thông thường có thể sử dụng một máy tính (cài đặt hệ điều hành Unix hoặc Windows NT) để cài đặt các phần mềm Firewall quản trị an ninh mạng như *Raptor Firewall* hoặc *CheckPoint Firewall*... Tuy nhiên với sự phát triển của công nghệ, ngày nay đã xuất hiện những thiết bị chuyên dụng đảm nhận công việc này (tích hợp cả phần cứng và phần mềm *Firewall* ngay trong thiết bị) ví dụ PIX Firewall (PIX-515-BUN). Ưu điểm của nó là đầu vào và đầu ra cùng một tốc độ cao Gbps (do thiết bị được chế tạo gồm 1 cửa vào và một cửa ra độc lập nhau, khác hẳn với việc áp dụng máy tính làm Firewall khi đó vào và ra đều chung một cửa là thông qua máy tính).

### 7.4.5. Hệ thống máy chủ giám sát và quản lý truy nhập

Việc theo dõi các truy nhập vào ra trên mạng được đảm trách bằng máy chủ NMS (Network Mangement Station). Máy này được cài đặt phần mềm giám sát quản trị mạng theo dõi các liên kết, các gói tin, các luồng dữ liệu theo thời gian thực để có thể phát hiện ra các nguy cơ mất thông tin hoặc bị tấn công... Ngoài ra nếu các đường truyền cung cấp dịch vụ truy nhập từ xa có băng thông ở tốc độ E1 có thể cài đặt thêm các hệ thống phần mềm (ví dụ như Merit) nó dựa trên luồng tín hiệu từ tổng đài (ví dụ tổng đài E10) để nhận biết số điện thoại kết nối và chúng được ghi vào một tệp .LOG, từ đây có thể phát triển một chương theo dõi sự kết nối của các thuê bao. Khả năng ghi lại số điện thoại của người sử dụng kết nối cho phép dễ dàng tìm ra người đó khi có sự cố liên quan xảy ra (ví dụ như bị lộ thông tin)...

### 7.4.6. Hệ thống máy chủ cung cấp dịch vụ truy cập từ xa

Có rất nhiều thiết bị đảm nhận vai trò cung cấp dịch vụ từ xa RAS, trong đó có cả các máy tính (sau khi đã bổ sung các giao diện kết nối modems). Tuy nhiên vì nhiệm vụ của hệ thống máy chủ này là cung cấp và bảo đảm đường truyền kết nối qua điện thoại cho nên đối với các mạng ISP chuyên nghiệp thường hay tìm đến giải pháp sử dụng các thiết bị chuyên dụng phục vụ cho công việc này.

Trong một loạt các thiết bị có thể đáp ứng của các hãng như Cisco, Lantronix, Intel ... việc lựa chọn thiết bị nào là một câu hỏi kiểm chứng chuyên môn đối với những nhà thiết kế mạng. Trên thực tế vấn đề cần quan tâm luôn là : *tin cậy, dễ mở rộng nâng cấp, dễ lắp đặt và gọn nhẹ*. Trong khi một RAS Server luôn đòi hỏi một đầu kết nối với mạng và đầu kia kết nối với modems và đường điện thoại và do đó sẽ chẳng gọn nhẹ chút nào nếu như RAS Server luôn đi kèm với hàng chục hoặc thậm chí hàng trăm modems bên ngoài cùng những bó dây nối nguồn và nối tín hiệu và rất nhiều các bộ nắn dòng (adapter) v.v. Vì vậy giải pháp hữu hiệu sẽ là giải pháp chọn lựa các RAS Server đã tích hợp các modems bên trong thiết bị (ví dụ CISCO AS5301)...

### 7.4.7. Hệ thống máy chủ cung cấp các ứng dụng cơ sở dữ liệu

Càng ngày nhu cầu khai thác Internet càng đòi hỏi đáp ứng các dịch vụ chất lượng ngày một cao hơn. Từ việc truy cập tìm kiếm thông tin thông thường như gửi thư đàm thoại, multimedia đến những dịch vụ cao cấp hơn như kinh doanh, mua bán. Từ chỗ ban đầu Web chỉ bao gồm các kho CSDL phi cấu trúc (ở dạng .html) đến nay đã có không ít các hệ thống dữ liệu ở dạng cấu trúc, được phát triển dựa trên các hệ thống

máy chủ cung cấp các dịch vụ CSDL dựa trên công nghệ Web (web based). Sẽ là không hiệu quả nếu như để cho máy chủ cung cấp dữ liệu Web đảm nhận vai trò cung cấp các dịch vụ CSDL (chức năng của máy chủ Database). Vì vậy một loại hình máy chủ mới xuất hiện chuyên làm chức năng cung cấp các dịch vụ CDSL. Máy chủ này được gọi là Database Server (Host).

Database Server có thể được cài đặt các hệ quản trị CSDL lớn như : Oracle, Informix hoặc trung bình và nhỏ như Microsoft SQL Server.

Một yêu cầu xuất phát từ người sử dụng đến Web site. Máy chủ Web sẽ cung cấp thông tin Web và có thể sai khiến các máy khác làm các dịch vụ khác mà người sử dụng đòi hỏi được cung cấp. Sau khi gửi các lệnh đến các DataBase Server máy chủ Web đợi thông tin xử lý từ các DataBase Server này rồi kiết xuất ở các khuôn dạng dữ liệu gửi html trả cho trình duyệt đã yêu cầu. Đây là một trong những giải pháp làm tăng hiệu năng cung cấp các dịch vụ của Internet.

### 7.4.8. Hệ thống máy chủ phục vụ in ấn

Cũng giống như việc quản trị người dùng trong mạng, việc in ấn trong mạng nào cũng nên uỷ nhiệm cho các máy chủ nào đó đảm nhận công việc này một cách độc lập. Sẽ không thú vị nếu làm việc trên một máy có gắn với máy in và do đó luôn phải bận rộn bởi những phiền hà do những người xung quanh in tài liệu qua máy in gắn với máy tính đang làm việc. Việc lựa chọn máy chủ làm máy in có rất nhiều giải pháp như : gắn máy in vào một máy tính riêng và thiết lập nó với chức năng in ấn, hoặc trang bị máy in có card mạng bên trong chuyên làm nhiệm vụ in trên mạng hoặc chọn thiết bị có tên là print server cho phép nối một vài máy in vào thiết bị này. Chọn lựa giải pháp nào sẽ tuỳ thuộc vào người thiết kế mạng và khả năng đáp ứng kinh phí.

### 7.4.9. Lựa chọn các máy tính làm máy chủ

Việc chọn cấu hình máy tính là rất quan trọng. Một mặt phải chọn được máy tính cấu hình thích hợp với quy mô mạng hiện tại và nhiệm vụ của từng máy, mặt khác phải tính đến khả năng phát triển của mạng trong tương lai để có thể nâng cấp và mở rộng việc cung cấp dịch vụ khi cần thiết. Các tiêu chuẩn chính được đưa ra để lựa chọn một máy tính làm máy chủ bao gồm: *tốc độ, cấu trúc BUS, số CPU, bộ nhớ RAM và Cache, khả năng hỗ trợ các hệ điều hành, tính ổn định, khả năng mở rộng và công nghệ - kỹ thuật bảo đảm an toàn dữ liệu.*

Hiện nay có quá nhiều các hãng cung cấp các loại máy tính để đảm nhận các vai trò cung cấp dịch vụ. Lựa chọn máy của hãng nào, theo công nghệ nào là tuỳ ở các

phân tích tài liệu kỹ thuật công nghệ của chủng loại máy ở thời điểm thiết kế. Tuy nhiên nếu xét trên góc độ an toàn và độ tin cậy nên hướng tới các giải pháp thiết bị dựa trên hệ điều hành có độ an toàn và cấp độ bảo mật cao (Unix hoặc Linux).

Ngoài ra, hiện nay hướng nghiên cứu tính toán song song ở trong nước và trên thế giới cũng đã cho ra đời những siêu máy tính rẻ tiền dựa trên hai công nghệ : *công nghệ kết chùm các máy vi tính* và *công nghệ SCI* (Scalable Coherent Interface) với hệ điều hành Linux. Các *siêu máy tính này* thực chất được nối với nhau trên một mạng Ethernet (đối với công nghệ cluster) hoặc mạng SCI. Theo số liệu được biết **các nhóm** nghiên cứu trong nước *đã cho ra đời siêu máy tính với công nghệ kết chùm 16 máy vi tính* rẻ tiền đạt được tốc độ **3,6 GFlops** và *Siêu máy tính theo công nghệ SCI với 4 máy vi tính* rẻ tiền đạt được tốc độ **1,86 GFlops**. Điều đặc biệt là với các công nghệ này hoàn toàn có thể triển khai cung cấp các dịch vụ Internet, bao gồm : Web, E-Mail, FTP, News, Telnet, Firewall ... Tất cả các dịch vụ này được phục vụ song song và trong suốt đối với người dùng. Việc ứng dụng kết quả nghiên cứu này là sẽ một thách thức đối với các nhà thiết kế mạng trong nước nói chung và mạng ISP nói riêng trong những năm tới...

## 7.5. Các dịch vụ chính của Internet

### 7.5.1. Thư tín điện tử (e-mail)

Dịch vụ thư tín điện tử là dịch vụ cho phép gửi và nhận thư thông qua mạng Internet. Khi sử dụng dịch vụ này người sử dụng có cơ hội làm quen, trao đổi thông tin, gửi và nhận thư trực tiếp với hàng trăm triệu người trên thế giới đang tham gia vào cộng đồng Internet. *E-mail* là dịch vụ đơn giản nhất nhưng cũng là dịch vụ có số người tham gia đông nhất trên Internet. Cũng giống như hệ thống gửi thư bưu điện, đó là nếu muốn gửi thư cho một ai đó, cần phải cung cấp địa chỉ của người nhận, trong đó có tên và nơi ở. Và ngược lại, nếu muốn nhận thư từ người khác, cũng phải cung cấp một tên và nơi ở xác định để thư có thể đến mà không sợ bị nhầm địa chỉ.

Trong hệ thống thư tín điện tử, nếu muốn gửi và nhận thư, cần có một tài khoản trong hệ thống này. Mỗi tài khoản này sẽ ứng với một người sử dụng trong hệ thống thư. Bởi vậy, mỗi tài khoản này sẽ có một số hiệu và nó chính là địa chỉ thư điện tử. Một địa chỉ sẽ gồm hai phần: *userid@domain* với *domain* là tên máy tính chứa hệ thống thư (coi như một bưu điện) và *userid* là tên tài khoản trong hệ thống này. Để đảm bảo tính bảo mật, mỗi tài khoản này phải có một mật khẩu riêng để hạn chế người khác không thâm nhập vào tài khoản của mình.

### 7.5.2. Diễn đàn thông tin/NewsGroups

Cùng với sự ra đời của email, dịch vụ nhóm tin (lúc đầu là Maillist sau phát triển thành NewsGroups) đã phát triển và trở thành phần không thể thiếu được của Internet. Đây thực sự là một diễn đàn thông tin công cộng mà trên đó, người sử dụng có thể trao đổi và thảo luận về mọi chủ đề. Tập hợp các nhóm thảo luận này có liên quan đến hàng triệu người trên khắp thế giới. Mỗi nhóm quay quanh một chủ đề như: công nghệ máy tính, hội hoạ, âm nhạc hay những tin nóng mang tính thời sự như xu hướng hội nhập phát triển kinh tế của các khu vực, tình hình chiến sự,... thậm chí cả những truyện đùa hoặc công thức pha chế món ăn...

Vì nội dung thảo luận phong phú như vậy, cho nên NewGroups đã lôi cuốn hàng triệu người từ khắp nơi trên thế giới tham gia, trao đổi, tranh luận và học hỏi. Hiện tại có hơn 28,000 diễn đàn trao đổi thông tin trên Internet, trung bình mỗi ngày có hơn 200,000 thông tin được đưa lên mạng.

Dịch vụ NewsGroups được hình thành từ Mạng lưới nhóm tin Usenet. Năm 1978, Tom Truscott và Steve Bellovin, sinh viên trường đại học Duke và North California đã móc nối hai máy tính bằng đường điện thoại. Chương trình này được viết trên hệ điều hành Unix 7.0. Năm 1981, hệ thống này được sinh viên trường đại học Berkley hoàn chỉnh và phổ biến rộng rãi. Năm 1986, do số lượng tin ngày càng nhiều, người ta đã đặt ra giao thức vận chuyển truyền tin NNTP (Network News Transfer Protocol). Giao thức này đơn giản hoá việc trao đổi tin tức, tin tức được truyền đi mau lẹ và hữu hiệu hơn và người đọc có thể lựa chọn tin để đọc một cách dễ dàng. Năm 1987, trường đại học Toronto đã cải thiện và hoàn chỉnh.

Mạng lưới nhóm tin tồn tại trên toàn cầu và không phải là mạng Internet. Dữ liệu của các nhóm tin được lưu trữ và quản lý bởi chương trình NewsServer. Người sử dụng có thể ngồi ở một client và sử dụng phần mềm NewsGroups client để đọc thông tin trên diễn đàn. Mỗi khi thực hiện lệnh để đọc một mẩu tin, newsgroups client yêu cầu newsgroups server cung cấp.

Để mạng lưới này hoạt động, hàng ngàn máy chủ chứa tin được nối với nhau và sử dụng chung một giao thức NNTP. Thông tin được lưu trữ tại các server và gọi là news site. Hiện nay có hơn 10,000 news site với hơn hai triệu rưỡi thành viên. Mỗi site được điều hành bởi một người gọi là người quản trị tin tức News admin.

Mỗi nhóm tin được đặt một tên. Tên này bao gồm hai hoặc nhiều phần, phân cách nhau bởi dấu chấm. Phần đầu là lĩnh vực (hierachy) mà nhóm tin thuộc về. Chẳng hạn, những người mới sử dụng Internet còn bỡ ngỡ về những kiến thức trên mạng và họ có một nhóm tin để tham khảo và thảo luận với tên là news.newusers.questions. Như vậy,

news là lĩnh vực về nhóm tin, newusers dành cho những người mới vào mạng và question là nhóm tin gồm những thắc mắc và hỏi đáp dành cho đối tượng này.

NewsGroup được tổ chức theo cấu trúc hình cây, cấp cao nhất có hai loại: *Maintream* và *Alternative*.

*Maintream* chứa những chủ đề tin được tải trên các news server:

| | |
|---|---|
| comp | công nghệ máy tính |
| misc | các chủ đề chung |
| news | về chính usenet |
| rec | tiêu khiển, nghệ thuật,... |
| sci | ngành khoa học |
| soc | nhóm tin xã hội |
| talk | chủ đề gây tranh cãi |

*Alternative* chứa những chủ đề tin mà người quản trị tin sẽ xem xét có nên chứa chúng hay không phụ thuộc vào dung lượng nhớ của server:

| | |
|---|---|
| alt | cho phép lựa chọn những chủ đề khác nhau |
| biz | thương mại, quảng cáo |
| ddn | mạng dữ liệu mật |
| bionet | sinh học |

...

Những người tham gia dịch vụ NewsGroups có thể gửi (Post) những bài tin (Article) của mình vào những nhóm thảo luận. Những thông tin này được lưu trong một máy chủ chứa tin (News server). Việc kiểm soát những bài tin và nhóm tin do người quản trị tin tức (News admin) của máy chủ đó quản lý. Người này có thể định hạn của mỗi bài tin, tức là sau một thời gian là bao nhiêu lâu, các bài tin đó sẽ hết hạn và được xóa khỏi máy chủ chứa tin. Một người tham gia dịch vụ này có thể được đọc các bài tin từ các nhóm tin, cùng trao đổi và học hỏi bằng cách gửi các bài lên các nhóm tin và phúc đáp một bài tin nào đó (follow-up). Và mỗi người sử dụng có thể được đọc thông tin từ các máy chủ khác nhau mà họ được phép truy nhập.

### 7.5.3. Dịch vụ tuyền tệp FTP (File Transfer Protocol)

FTP là dịch vụ cho phép sao chép thông tin (theo cả hai chiều) từ các "kho" dữ liệu trên Internet với máy tính cá nhân.

Nếu máy tính cá nhân đã hoà nhập mạng Internet, nhờ FTP người sử dụng có thể kết nối tới bất kì máy chủ nào trong hệ thống đó, xem được danh sách các file trong các thư mục của máy chủ. Thực hiện các file đó (đọc nội dung, chạy chương trình,...).

Từ đó, người sử dụng có thể chọn các file mình cần, sao chép (download) các file đó về máy tính cá nhân của mình. Ngược lại, nếu FTP Server cho phép ghi thì người sử dụng cũng có thể truyền file từ máy tính cá nhân của mình tới máy chủ.

### 7.5.4. Dịch vụ truy nhập máy chủ (Telnet)

Dịch vụ Telnet cho phép người sử dụng có thể truy nhập vào các máy chủ lớn (Mainframe, Midrange hay Mini). Khi đó, máy tính cá nhân của người sử dụng sẽ đóng vai trò như một trạm đầu cuối (terminal) làm việc trên máy chủ ở xa.

Các terminal sẽ sử dụng hoàn toàn các thiết bị và tài nguyên của các máy tính lớn. Điều này có ý nghĩa vô cùng to lớn. Dịch vụ Telnet đã nối kết thế giới Internet, thế giới máy PC và thế giới của các máy tính lớn. Các máy tính lớn đã và còn đóng vai trò quan trọng trong nghiên cứu khoa học và áp dụng các thành tựu khoa học mới. Đó đó, Telnet sẽ còn là dịch vụ không thể thiếu được của Internet.

### 7.5.5. World Wide Web (WWW)

WWW là dịch vụ mới nhưng phát triển nhanh nhất của Internet. Hiện tại số lượng các Web Server đã vượt lên đến hàng triệu.

Thông tin từ các Web Server được truy cập theo các trang gọi là trang Web. Trên trang Web có đủ các loại dữ liệu như chữ, đồ hoạ, âm thanh, video. Điều đặc biệt nhất của thông tin Web là khái niệm *Siêu văn bản (Hypertext)* hoặc *Siêu phương tiện (Hypermedia)*. *Hypertext* hoặc *Hypermedia* là các văn bản hay đồ hoạ bình thường nhưng có thêm một tính năng rất đặc biệt. Khi người sử dụng kích chuột vào các vị trí "siêu" đó, sẽ xuất hiện các trang Web khác. Khả năng tự động kết nối này làm cho Web trở nên trong suốt đối với các kho dữ liệu và làm cho nó trở thành dịch vụ phát triển với tốc độ nhanh nhất. Các *HyperText* hay *HyperMedia* chính là điểm kết nối thông tin trên Internet rất thuận tiện. Người sử dụng có thể tạo ra các trang Web cho riêng mình, trên đó xếp đặt các "siêu" kết nối với bất kì vị trí nào mong muốn. Các trang thông tin mà từ đó xuất phát để truy nhập các thông tin khác được gọi là *Trang chủ* (*Home Page*).

## 7.6. Một số kiến thức liên quan

### 7.6.1. QoS (Quality of Service)

**1. Giới thiệu**

Thuật ngữ QoS là viết tắt của tập hợp từ Quality of Service (Chất lượng dịch vụ). Chất lượng dịch vụ là nói đến khả năng của một mạng cung cấp dịch vụ tốt hơn cho sự lưu thông mạng đã chọn trên các công nghệ khác nhau, bao gồm Frame Relay, Asynchronous Transfer Mode (ATM), Ethernet và các mạng theo chuẩn 802.1, SONET và các mạng định tuyến IP. Mục đích chính của QoS là cấp quyền ưu tiên như băng thông tận hiến (dedicated), độ lệch trễ jitter và suy hao điều khiển và cải tiến các đặc tính hao tổn. Một đặc tính quan trọng khác là ưu tiên cung cấp cho một hoặc nhiều *luồng** nhưng vẫn bảo đảm các *luồng* khác hoạt động tốt. Các công nghệ QoS cung cấp những khối cơ bản sẽ được áp dụng cho các ứng dụng thương mại trong tương lai ở mạng WAN, Campus và các mạng của các nhà cung cấp dịch vụ.

**2. Những khái niệm của QoS**

Về cơ bản, QoS cho phép mạng cung cấp các dịch vụ tốt hơn cho các *luồng* nhất định. Điều này được thực hiện bằng việc tăng sự ưu tiên cho *luồng* này và giới hạn sự ưu tiên của *luồng* khác. Khi sử dụng các công cụ quản lý các sự cố nghẽn mạng, hãy thử tăng độ ưu tiên bằng việc đẩy vào hàng đợi và bảo quản các hàng đợi vào những tuyến đường khác. Công cụ quản lý hàng đợi dùng để tránh tắc nghẽn sẽ tăng độ ưu tiên bằng việc chia nhỏ các *luồng* có độ ưu tiên thấp hơn trước các *luồng* có độ ưu tiên cao hơn. Khống chế và sắp đặt độ ưu tiên cho một *luồng* bằng việc hạn chế thông lượng các *luồng* khác. Các công cụ liên kết hiệu quả hạn định *các luồng lớn* thành *các luồng nhỏ* dễ được chấp nhận.

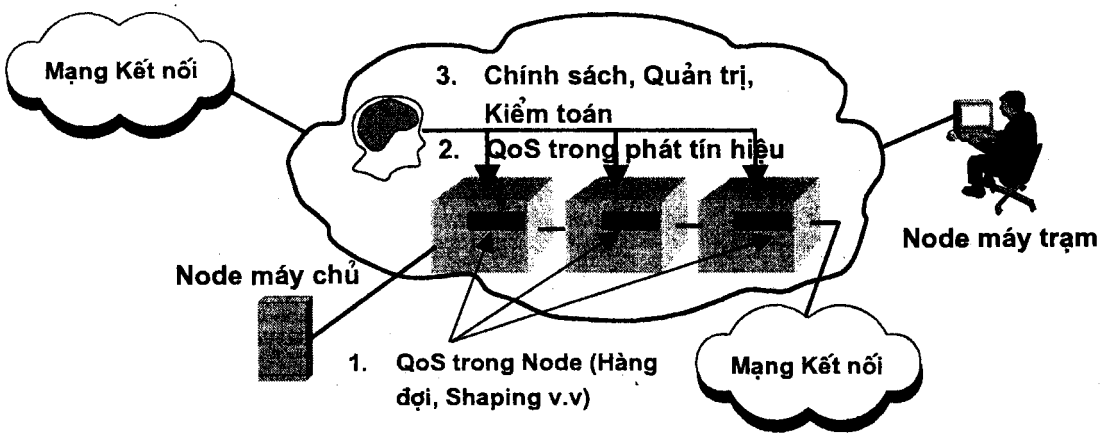
Các công cụ QoS có thể làm nhẹ bớt các vấn đề tắc nghẽn. Tuy nhiên điều gì sẽ xảy ra nếu có quá nhiều lưu lượng truyền tải trên băng thông được cung cấp ? Trong những trường hợp như vậy, QoS cũng đành bó tay.

**3. Kiến trúc QoS cơ bản**

Kiến trúc cơ bản gồm 03 thành phần để thực hiện QoS (*Hình 7.10.*) :

- Nhận diện QoS và tạo các kỹ thuật phối hợp QoS từ đầu này tới đầu khác giữa các phần tử của mạng;
- QoS bên trong một phần tử mạng riêng lẻ (chẳng hạn, hàng đợi, lịch đợi và các công cụ tạo mẫu liên lạc)

- Các chức năng kiểm toán, quản trị và chính sách QoS để điều khiển và quản trị lưu thông từ điểm tới điểm dọc theo mạng.




**Hình 7.10. Ba thành phần chính khi thực hiện *một QoS cơ bản***

**4. Xác nhận và đánh dấu QoS**

Xác nhận và phân loại được hoàn tất thông qua sự phân loại và hạn chế.

***Sự Phân loại***

Để cung cấp một dịch vụ ưu tiên cho một kiểu truyền tải thì trước hết nó cần được *xác nhận* và tiếp theo gói tin có thể sẽ được *đánh dấu*. Hai công việc này tạo ra sự phân loại. Khi gói tin được xác nhận nhưng không bị đánh dấu thì phân loại đó được gọi là *trên một chặng (hop) cơ bản*. Điều này được áp dụng khi phân loại chỉ gắn liền với thiết bị mà nó hiện diện và không được chuyển sang Router tiếp theo. Nó xảy ra với hàng đợi ưu tiên (Priority Queuing - PQ) và hàng đợi theo yêu cầu khách hàng (Custom Queuing - CQ). Khi các gói tin được đánh dấu để sử dụng trên diện rộng, các bits ưu tiên IP có thể được đặt.

Các phương pháp thông thường của việc xác nhận *luồng* bao gồm danh sách điều khiển truy nhập ALC (acccess control list), định tuyến dựa trên chính sách, tốc độ truy nhập cam kết CAR (committed access rate) và nhận dạng ứng dụng chạy trên mạng NBAR (network-based application recognition).

**5. QoS bên trong một phần tử mạng riêng lẻ**

Các công cụ chính bao gồm :

- Công cụ quản lý tắc nghẽn,
- Công cụ quản lý hàng đợi,
- Công cụ quản lý hiệu quả liên kết, và
- Công cụ quản lý *chính sách* và *shaping*.

*Công cụ quản lý tắc nghẽn*

Vì sự tràn ngập tự nhiên của truyền tải âm thanh, hình ảnh và dữ liệu, đôi khi một lượng truyền tải vượt quá tốc độ của đường truyền. Khi ấy Router sẽ làm gì ? Phải chăng nó sẽ đệm (buffer) lưu lượng truyền tải trong một hàng đợi riêng và cho phép gói vào đầu sẽ là gói ra đầu tiên ? Hoặc phải chăng nó thường xuyên đặt các gói vào các hàng đợi khác và/hoặc hàng đợi dịch vụ nào đó ? Các công cụ quản lý tắc nghẽn là nhằm giải quyết các câu hỏi này. Các công cụ quản lý tắc nghẽn bao gồm : *hàng đợi ưu tiên (PQ), hàng đợi theo yêu cầu của khách hàng (CQ), hàng đợi chất tải hợp lý (WFQ) và hàng đợi chất tải hợp lý dựa theo lớp (CBWFQ).*

*Công cụ quản lý hàng đợi*

Bởi vì các hàng đợi không có kích thước xác định, chúng có thể chứa đầy và tràn ra. Khi một hàng đợi đầy các gói bổ sung sẽ không chen được vào hàng đợi và sẽ bị bỏ rơi. Đây gọi là rớt đuôi. Hiện tượng rớt đuôi là vì Router không thể ngăn cản gói tin này khỏi bị bỏ rơi (ngay cả khi nó có độ ưu tiên cao). Bởi vậy cần có một cơ chế để thực hiện hai điều :

1. Đảm bảo hàng đợi không bị đầy và do vậy sẽ có chỗ cho các gói tin có độ ưu tiên cao;
2. Cho phép xắp xếp tiêu chuẩn các gói tin có độ ưu tiên thấp hơn bị rớt trước khi các gói tin có độ ưu tiên cao hơn cũng bị rớt (nếu phải vậy).

Cơ chế *phát hiện trước tải nặng một cách ngẫu nhiên* (WRED) cung cấp cả hai đặc tính này.

*Công cụ quản lý hiệu quả liên kết*

Thỉnh thoảng các liên kết tốc độ thấp thể hiện sự ra đời của các gói tin nhỏ hơn. Ví dụ trễ do đặt gói tin vào đường truyền của một gói tin 1500 bytes trên đường truyền 56 Kbps là 214 ms. Nếu một gói âm thanh đi sau gói tin lớn này, thời gian trễ của gói âm thanh có thể vượt ngưỡng ngay cả khi gói tin lớn đã ra khỏi Router! Chia nhỏ và chèn trên đường truyền cho phép gói lớn này được phân đoạn thành các gói nhỏ hơn xen kẽ với gói âm thanh. Việc chèn gói cũng quan trọng không kém việc chia nhỏ và không có lý do gì để sau khi đã chia nhỏ gói tin lớn trên lại để gói âm thanh đi sau các gói đã chia nhỏ này.

Một hiệu quả khác là việc loại bỏ quá nhiều các bits overhead. Ví dụ RTF header (Header của giao thức thời gian thực - Real Time Protocol) có tới 40 bytes header. Với lượng chất tải ít chẳng hạn 20 bytes, khi ấy phần overhead gấp đôi nội dung chất tải. Nén RTF header là biện pháp để giảm header và do vậy tăng kích cỡ quản lý.

*Công cụ quản lý shaping truyền tải và chính sách truyền tải*

*Shaping* thường dùng để tạo *luồng* truyền tải mà nó giới hạn tiềm năng của toàn bộ băng thông của *luồng* này. Điều này được sử dụng nhiều lần để tránh sự cố tràn như đã đề cập trong các phần trên. Ví dụ nhiều công nghệ mạng sử dụng Frame Relay trong Hub. Trong trường hợp này, trạm trung tâm thông thường có liên kết băng thông cao (chẳng hạn T1), trong khi trạm ở xa có liên kết băng thông thấp (chẳng hạn 384 Kbps). Lúc này hoàn toàn có thể xảy ra truyền tải từ trạm trung tâm làm tràn đường truyền băng thông thấp ở đầu cuối khác. *Shaping* là cách hoàn hảo để dẫn tốc độ gần với 384 Kbps nhằm tránh hiện tượng tràn đường truyền ở xa. Trong truyền tải nêu trên tốc độ đã được thiết lập được lưu giữ tạm thời cho truyền thông về sau nhằm để duy trì tốc độ đã được thiết lập.

Chính sách truyền tải *cũng giống như* Shaping, *nhưng nó khác một cách rất quan trọng : truyền tải nào vượt quá vận tốc được thiết lập sẽ không được lưu giữ tạm và do đó sẽ bị biến mất.*

### 7.6.2. xDSL

**Tổng quan**

*Digital Subscriber Line (*DSL*)* là công nghệ modem mà nó sử dụng đường dây điện thoại đã có sẵn để truyền tải dữ liệu có băng thông cao như multimedia, hình ảnh tới những người thuê bao dịch vụ.

Thuật ngữ *xDSL* một trong các công nghệ xuất phát từ DSL, bao gồm :

- Công nghệ ADSL,
- Công nghệ VDSL,
- Công nghệ HDSL,
- Công nghệ HDSL-2,
- Công nghệ SDSL,
- Công nghệ G.SHDSL và
- Công nghệ IDSL.

*xDSL* đã gây ra sự chú ý đặc biệt của những người thực hiện và cung cấp dịch vụ bởi vì nó hứa hẹn việc cung cấp các tốc độ truy cập dữ liệu băng thông cao tới những khu vực phân tán ở xa với giá thành tương đối thấp và vẫn dựa trên hạ tầng viễn thông hiện thời.

Các dịch vụ *xDSL* là các truy cập mạng công cộng, mạng điểm nối điểm hoặc mạng tận hiến (dedicated) trên cáp dẫn đôi dây, xoắn, bằng đồng tại các khu vực giữa một đầu là văn phòng trung tâm của các nhà cung cấp dịch vụ mạng (NSP) và một

đầu là khách hàng, hoặc tại khu vực bên trong các toà nhà cao tầng hoặc bên trong các mạng Campus.

Hiện nay tiêu điểm chính của công nghệ *xDSL* là phát triển và triển khai các công nghệ *ADSL* và *VDSL*. Vì vậy giáo trình này sẽ tập trung vào hai công nghệ nói trên.

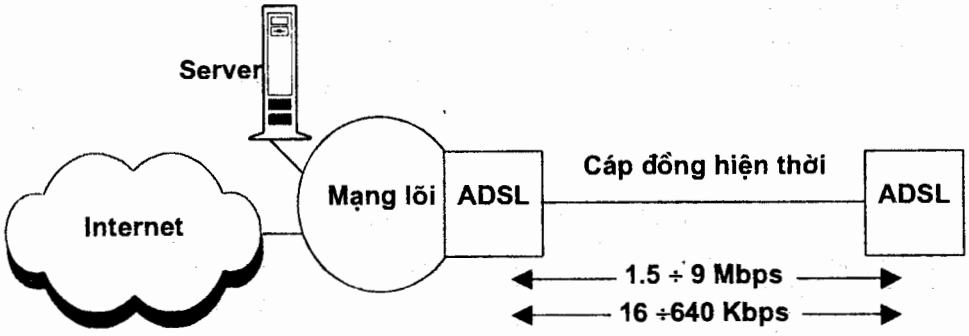
**ADSL là gì ?**

Thuật ngữ ADSL là viết tắt của tập hợp từ **Asymmetric Digital Subscriber Line** (Đường thuê bao số phi đối xứng). Công nghệ *ADSL* cho phép băng thông của luồng dữ liệu tải từ văn phòng NSP về phía khách hàng lớn hơn băng thông đi từ phiá khách hàng tới văn phòng NSP.

Tính phi đối xứng này đã nảy sinh ý tưởng mở rộng dịch vụ cho các mạng Internet/Intranet như xem video theo yêu cầu, truy nhập mạng LAN từ xa..., dựa trên thực tế là người sử dụng thường muốn lấy thông tin về càng nhanh càng tốt trong khi luồng thông tin gửi yêu cầu đi có thể không cần nhanh (và không nhiều) như vậy.

*ADSL* truyền tải nhiều hơn 6Mbps tới một thuê bao và nhiều nhất là 640 kbps cho cả hai chiều (xem hình 7.11.). Các tốc độ nói trên gấp 50 lần so với việc truy nhập thông thường qua điện thoại trong khi không cần phải thay đổi hệ thống cáp dẫn tín hiệu của hệ thống điện thoại hiện có.

*ADSL* thực sự biến mạng thông tin công cộng hiện hành từ chỗ bị giới hạn bởi các tín hiệu âm thanh, văn bản và đồ hoạ phân giải thấp trở thành một hệ thống đầy tiềm năng với những ứng dụng đa phương tiện, bao gồm video hoàn toàn động tới mọi nhà trong thế kỷ này.




**Hình 7.11. Kết nối ADSL**

*ADSL* sẽ đóng vai trò chủ yếu trong những thập kỷ tới ngay khi các công ty điện thoại chấp nhận những thị trường mới để phân phát thông tin ở khuôn dạng đa phương tiện hoặc video. Lắp đặt cáp băng thông rộng sẽ mất tới hàng chục năm mới tiếp cận tất cả các thuê bao trong tương lai. Sự thành công của các dịch vụ mới có thể sẽ phụ thuộc

vào cách tiếp cận với nhiều khách hàng ngay cả trong những năm đầu tiên. Với việc đưa ra các phim, truyền hình, các catalog ảnh, các đĩa CD-ROM đặt ở xa kết hợp với các mạng LAN và Internet tại nhà, tại văn phòng, *ADSL* sẽ tạo ra những thị trường ổn định, sinh lợi cho các công ty điện thoại và cũng vậy cho các nhà cung cấp các ứng dụng.

**Các khả năng của ADSL**

Một vòng *ADSL* nối một modem *ADSL* tại một đầu cuối của đường dây diện thoại có thể tạo ra 03 kênh thông tin - một kênh tải về (*downstream*) với vận tốc cao, một kênh hai chiều với vận tốc trung bình và một kênh dịch vụ điện thoại cơ bản. Kênh dịch vụ điện thoại cơ bản được tách từ modem số bằng các bộ lọc, bởi vậy bảo đảm dịch vụ điện thoại cơ bản không bị ngắt, thậm chí nếu *ADSL* bị hỏng. Kênh tốc độ cao trong dải 1.5 ÷ 6.1 Mbps và kênh hai chiều với tốc độ trong dải 16 ÷ 640 Kbps. Mỗi kênh có thể chia nhỏ thành các kênh có tốc độ thấp hơn.

Các modem *ADSL* cung cấp tốc độ phù hợp với chuẩn hệ thống số T1 của Bắc Mỹ 1.544 Mbps và E1 của châu Âu 2.048 Mbps (*xem bảng 7.1.*) và có thể mua được với các dải tốc độ khác và dung lượng khác. Cấu hình tối thiểu cung cấp được 1.5 hoặc 2.0 Mbps cho các luồng về và 16 kbps cho kênh hai chiều; các cấu hình khác cung cấp tốc độ 6.1 Mbps à 64 kbps hai chiều. Các sản phẩm với tốc độ luồng về đạt đến 8 Mbps và 640 kbps cho cả hai chiều đi và về hiện cũng đã sẵn có các modems *ADSL* thích hợp với việc truyền tải trên ATM với các tốc độ tuỳ biến và khả năng bù lấp các overhead ATM giống như mạng IP.

Tốc độ dữ liệu của luồng về phụ thuộc vào một số yếu tố, bao gồm chiều dài của cáp đồng, tiêu chuẩn dây, sự rẽ mạch và các bộ couple. Suy giảm trên đường dây là do tăng chiều dài và giảm đường kính dây. Bỏ qua những rẽ mạch *ADSL* thực hiện như nêu trên *bảng 7.2.*

Bảng 7.1

**Tốc độ đường xuống và đường hai chiều**

| *Downstream Bearer Channels* | *Duplex Bearer Channels* |
|---:|---:|
| n x 1.536 Mbps 1.536 Mbps | C Channel 16 Kbps |
| 3.072 Mbps | 64 Kbps |
| 4.608 Mbps | Optional Channels 160 Kbps |
| 6.144 Mbps | 384 Kbps |
| n x 2.048 Mbps 2.048 Mbps | 544 Kbps |
| 4.096 Mbps | 576 Kbps |

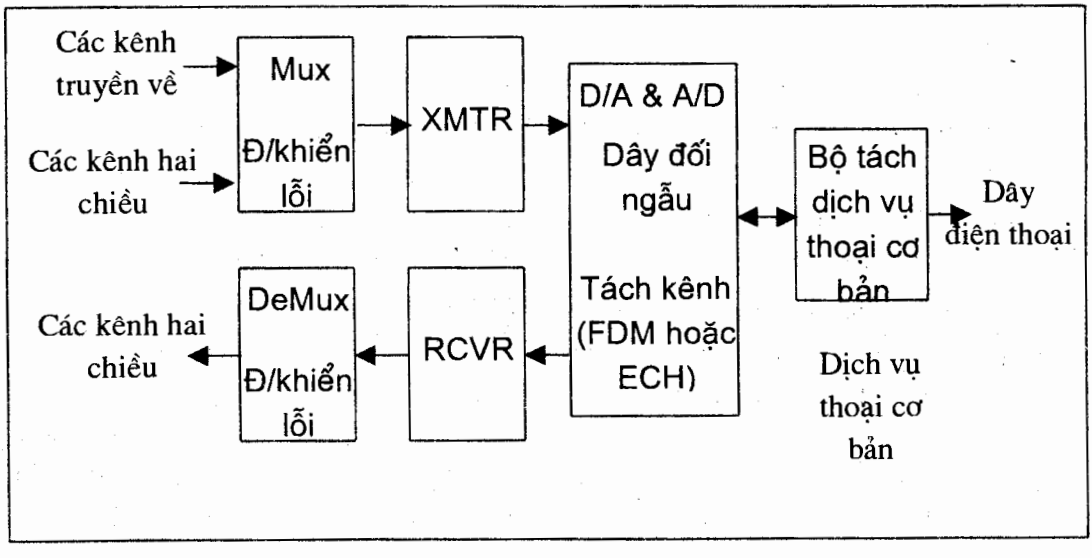
Bảng 7.2

**Khả năng của thiết bị vật lý ADSL**

| Tốc độ dữ liệu (Mbps) | Đường kính dây (AWG) | Khoảng cách (feet) | Đường kính dây (mm) | Khoảng cách (km) |
|---|---|---|---|---|
| 1.5 or 2 | 24 | 18,000 | 0.5 | 5.5 |
| 1.5 or 2 | 26 | 15,000 | 0.4 | 4.6 |
| 6.1 | 24 | 12,000 | 0.5 | 3.7 |
| 6.1 | 26 | 9,000 | 0.4 | 2.7 |

**Công nghệ ADSL**

*ADSL* phụ thuộc vào việc xử lý tín hiệu số tiên tiến và việc tạo ra các thuật toán nén đủ nhiều thông tin trong đôi dây cáp. Các tiến bộ mới được yêu cầu trong khi chuyển đổi như các bộ lọc tương tự và các bộ biến đổi A/D. Đường dây điện thoại dài sẽ có thể suy hao các tín hiệu ở tần số 1 MHz (cận ngoài của băng tần được sử dụng bởi *ADSL*) nhiều nhất là 90 dB, bắt buộc các phần analog của *ADSL* làm việc rất nhiều để thu được vùng động, lớn, tách các kênh và đảm bảo tạp âm thấp.




**Hình 7.12. Đầu cuối mạng nhận ADSL**

Nhìn từ ngoài *ADSL* trông rất đơn giản các đường dữ liệu đồng bộ trong suốt ở các tốc độ khác nhau trên các đường dây điện thoại ban đầu. Bên trong, tất cả các

transistors đều làm việc - đó là điều thần kỳ của kỹ thuật modem. Hình 7.12. giới thiệu một đầu cuối của mạng nhận *ADSL*.

Để tạo nhiều kênh, các modems ADSL chia băng thông sẵn có của đường điện thoại bằng một trong hai cách - ghép bộ chia đa tần (FDM) hoặc loại bỏ tiếng vọng như thể hiện trên hình 7.13. FDM sẽ gán băng cho dữ liệu đi và băng khác cho dữ liệu về. Đường dữ liệu về sau đó được chia bởi việc ghép TDM (time-division multiplexing) thành một hoặc nhiều kênh tốc độ cao. Đường dữ liệu lên cũng được ghép tương ứng với các kênh tốc độ thấp. Loại bỏ tiếng vọng được gán cho băng lên để gối lên băng về và tách thành hai bằng các phương pháp loại bỏ tiếng vọng nội tại là kỹ thuật đã được biết của các modems chuẩn V.32 và V.34. Với một trong hai kỹ thuật này *ADSL* tách một vùng 4 kHz thành dịch vụ thoại cơ bản ở đầu cuối DC của băng.

Một modem *ADSL* tổ chức một dòng dữ liệu gộp được tạo bởi việc ghép các kênh về, các kênh hai chiều và các kênh duy trì đồng thời vào các khối và đính kèm mã hiểu chỉnh lỗi cho mỗi khối. Bộ thu sau đó sẽ hiệu chỉnh các lỗi xảy ra trong quá trình truyền tải tới giới hạn được cho bởi mã và độ dài khối.

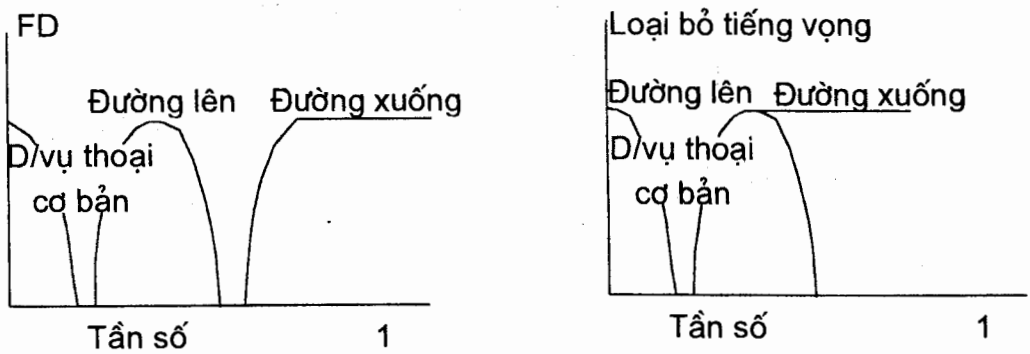
Thiết bị cũng có thể là một lựa chọn cho người sử dụng tạo các khối lớn bằng việc chèn dữ liệu vào các khối nhỏ; nó cho phép bộ nhận hiệu chỉnh mọi tổ hợp lỗi trong một khoảng bít đặc biệt. Điều này đã mở ra việc truyền hiệu quả cả cho dữ liệu lẫn tín hiệu video.

**VDSL**

Thuật ngữ *VDSL* là viết tắt của tập hợp từ **Very-high-rate Digital Subscriber Line** (Đường thuê bao số tốc độ truyền tải cực cao). Nói một cách đơn giản *VDSL* truyền dữ liệu tốc độ cao trên cáp điện thoại bằng đồng với dải tốc độ phụ thuộc vào chiều dài thực tế của cáp dẫn. Tốc độ tối đa của luồng tải về trong khoảng 51÷ 55 Mbps với độ dài dây là 300m. Khi độ dài dây là 1500m tốc độ luồng về có thể đạt 13 Mbps. Tốc độ luồng đi cũng như model *ADSL* sẽ là phi đối xứng đạt từ 1.6 ÷ 2.3 Mbps. Cả hai kênh dữ liệu sẽ được tách theo tần số của các băng tần sử dụng cho dịch vụ điện thoại và các mạng dịch vụ tích hợp số ISDN, cho phép các nhà cung cấp dịch vụ ghép chồng *VDSL* trên các dịch vụ đang tồn tại. Tại thời điểm hiện tại hai kênh tốc độ cao cũng đã được tách theo tần số. Ngay cả các nhu cầu nảy sinh các kênh đi với tốc độ cao hoặc tốc độ đối xứng các hệ thống *VDSL* có thể cần sử dụng việc loại bỏ tiếng vọng.

**Công nghệ VDSL**

Công nghệ *VDSL* giống với *ADSL* rất nhiều điểm, mặc dù *ADSL* cần phải đối mặt với nhiều lĩnh vực thay đổi lớn và rất phức tạp. VDSL cần phải thấp hơn về giá thành và điện năng tiêu thụ và với những giả định trên VDSL có thể được thực hiện cho việc ghép các kênh đi (*upstream*).




**Hình 7.13. ADSL sử dụng FDM và loại bỏ tiếng vọng để chia băng thông sẵn có thành các dịch vụ**

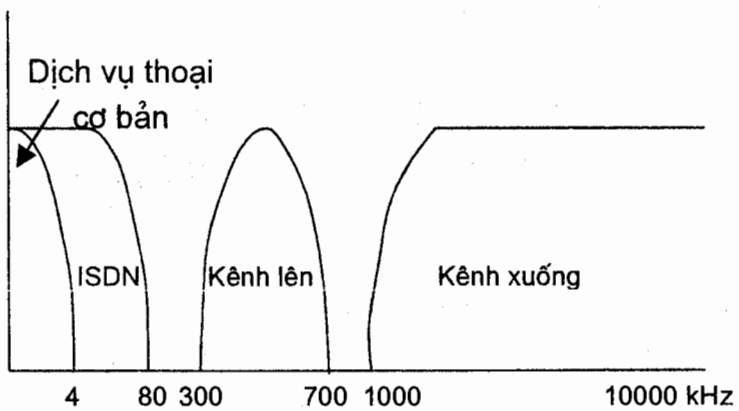
***Chọn mã đường***

Bốn loại mã đã được đề xuất cho *VDSL* :

- CAP (*Carierless Amplitude modulation/phase modulation - Điều biên không sóng mang*) - Một phiên bản điều biên bốn trạng thái triệt tiêu sóng mang (QAM). Với các cấu hình kết thúc mạng (NT) thụ động, CAP được sử dụng khoá dịch pha bốn trạng thái (QPSK) cho đường lên và một kiểu của TDMA cho việc ghép kênh (Mặc dù CAP không loại FDM tiếp cận với việc ghép kênh lên).
- DTM (*Discrete Multitone* - Đa tần rời rạc) - Một hệ thống đa sóng mang sử dụng các phép biến đổi Fourier rời rạc để tạo và giải điều chế các sóng mang cá nhân. Với các cấu hình NT thụ động, DTM sử dụng FDM cho việc ghép kênh lên (mặc dù DTM không loại bỏ chiến lược ghép kênh TDMA).
- DWMT (*Discret Wavelet Multitone - Đa tần sóng con rời rạc*) - Một hệ thống đa sóng mang sử dụng các phép biến đổi sóng con để tạo và giải điều chế các sóng mang cá nhân. DWMT cũng sử dụng FDM cho việc ghép các đường lên, nhưng cũng cho phép TDMA.
- SLC (Simple Line Code - Mã đường đơn giản) - Một phiên bản phát tín hiệu băng tần bốn mức mà nó lọc băng cơ bản và khôi phục nó ở máy thu. Đối với các cấu hình NT thụ động, SLC giống với việc sử dụng TDMA để ghép kênh lên mặc dù FDM cũng có thể tồn tại.

**Tách kênh**

Các phiên bản trước đây của *VDSL* sử dụng việc ghép kênh chia tần để tách các kênh về khỏi các kênh đi và tách cả hai khỏi dịch vụ thoại cơ bản và ISDN như thể hiện trên hình 7.14. Việc loại bỏ tiếng vọng có thể được yêu cầu bởi các hệ thống ra đời sau này đặc trưng bởi tốc độ dữ liệu đối xứng. Khoảng cách thực tế theo tần số sẽ được duy trì giữa kênh dữ liệu thấp nhất và dịch vụ thoại cơ bản để cho phép các bộ tách dịch vụ thoại cơ bản một cách đơn giản và hiệu quả. Trong thực tế các kênh về được định vị trên các kênh lên.




**Hình 7.14. Phiên bản trước đây của VDSL sử dụng FDM để tách kênh về khỏi các kênh lên và cả hai khỏi dịch vụ thoại cơ bản và ISDN**

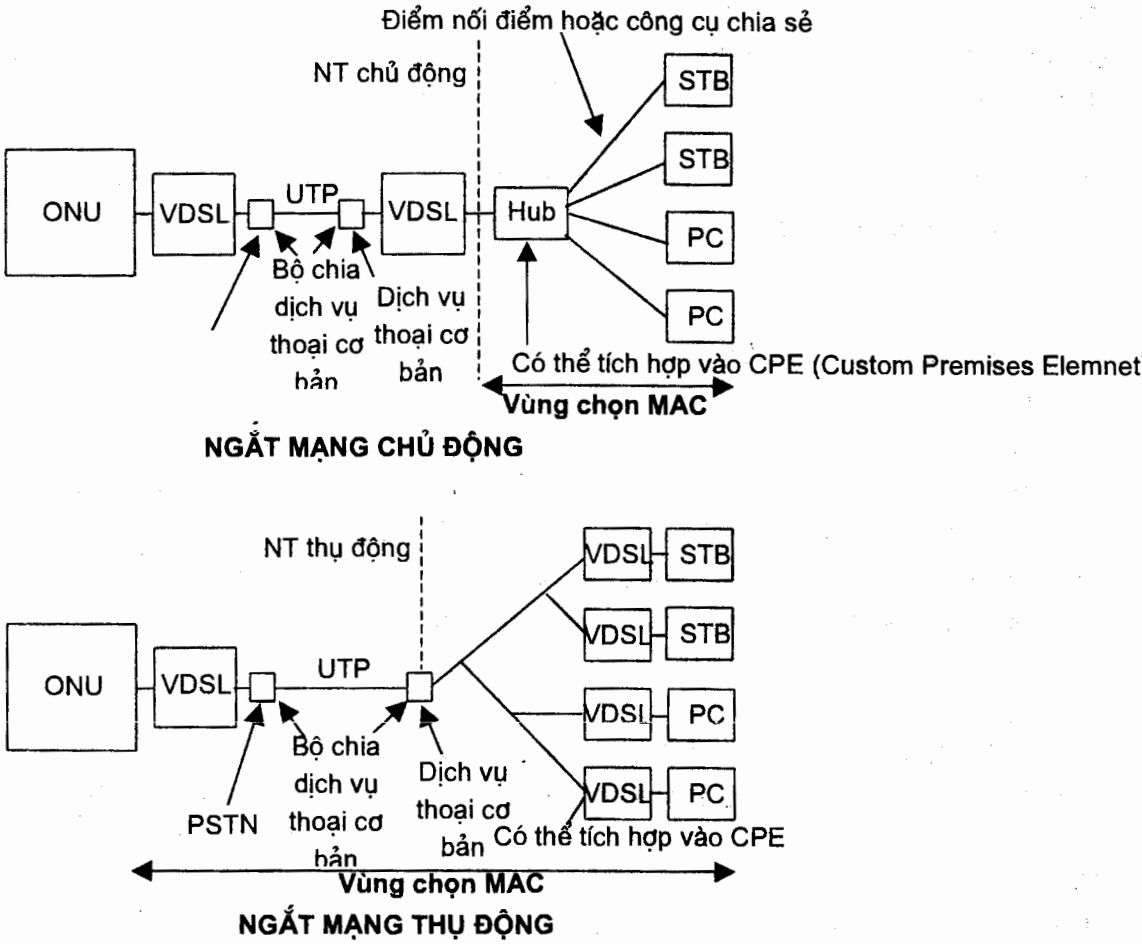
***Điều khiển sửa lỗi trước (FEC-Forward Error Control)***

FEC sẽ không nghi ngờ việc sử dụng dạng mã của Reed Solomon và việc chèn không bắt buộc để hiệu chỉnh những xuất hiện đột ngột của lỗi gây nên bởi xung lực của tạp âm. Cấu trúc này sẽ rất giống với *ADSL* như được định nghĩa trong chuẩn T1.413. Một câu hỏi còn tồn tại là không biết phần overhead của FEC (khoảng 8%) sẽ được lấy khỏi dung lượng tải hoặc được thêm vào như một tín hiệu ngoài băng ? Trước đây giảm dung lượng tải nhưng duy trì khoảng định mức, ngược lại về sau giữ lại tải định mức nhưng cho phép giảm một chút trong khoảng. *ADSL* đặt over head của FEC bên ngoài băng.

**Ghép kênh lên**

Nếu giả định bộ VDSL có kết thúc mạng (Network Termination - NT), khi ấy các công cụ ghép các tế bào của kênh lên hoặc các kênh dữ liệu từ nhiều CPE vào một luồng lên riêng rẽ trở thành nhiệm vụ của mạng giả định. Bộ VDSL đơn giản thể hiện

dòng số liệu thô từ hai hướng. Như minh hoạ trên hình 7.15., một kiểu của mạng giả định bao gồm một hình sao kết nối từng CPE vào HUB chuyển mạch hoặc ghép kênh; như vậy một HUB có thể được tích hợp vào bộ VDSL giả định.




**Hình 7.15. Các phương pháp ngắt mạng thụ động và chủ động**

Trong cấu hình NT thụ động, mỗi CPE có một bộ VDSL liên kết. Lúc này các kênh lên từ một CPE cần phải chia sẻ dây dẫn chung. Mặc dù một hệ thống phát hiện xung đột có thể được sử dụng, nhưng để băng thông được bảo đảm cần một trong hai giải pháp. Giải pháp thứ nhất cần đến thủ tục chuyển nhượng tế bào trong các Frame của kênh xuống được sinh ra ở ONU hoặc cấp xa hơn, mạng chứa một vài bits mà nó cấp truy nhập cho một CPE đặc biệt trong một chu kỳ định trước cho việc nhận Frame. Một CPE được cấp có thể gửi một tế bào của kênh lên trong chu kỳ này. Thiết bị truyền trong CPE này cần bật lên, gửi phần mở đầu để quy định cho máy thu ONU, gửi tế bào

này và sau đó tự tắt. Thủ tục này cần chèn đủ *độ im lặng* (enough silence) để cho phép đường dây rung chuông rõ ràng. Một sự giải thích của thủ tục này là sử dụng khoảng 77 (cơ số 8) để truyền tế bào 53 (cơ số 8).

Phương pháp thứ hai chia kênh lên thành các băng tần và gán một băng cho CPE. Phương pháp này có lợi thế là tránh mọi MAC với overhead liên kết của nó (mặc dù bộ ghép multiplexor cần phải được xây dựng trong ONU), nhưng một trong hai sẽ ngăn chặn tốc độ dữ liệu đang có tới bất kỳ 1 CPE nào hoặc bắt đảm trách lược đồ ghép kênh nghịch đảo động mà nó cho phép CPE gửi nhiều hơn sự chia sẻ của nó trong một chu kỳ. Mới đây người ta đã thấy một sự phân phát lớn giống như thủ tục MAC, nhưng không mất băng thông liên kết với việc phát hiện và xoá sóng mang cho mỗi một tế bào.

**Các công nghệ DSL khác**

**HDSL**

Thuật ngữ *HDSL* là viết tắt của tập hợp từ **High-speed Digital Subscriber Line** (**Đường thuê bao số tốc độ truyền tải cao**). Đây là công nghệ được phát triển bởi Bellcore. Các công nghệ *HDSL/T1/E1* đã được hình thành chuẩn bởi ANSI của Mỹ và bởi ETSI của châu Âu. Chuẩn ANSI cho phép truyền thông tốc độ T1 trên 2 cặp dây với 784 Kbps cho mỗi một cặp. Các chuẩn ETSI tồn tại cả hai gồm hệ thống 2 cặp với tốc độ E1, mỗi cặp truyền tải 1168 Kbps và hệ thống 3 cặp E1 với tốc độ 784 Kbps cho mỗi cặp.

*HDSL* trở nên ưa chuộng bởi vì nó là cách tốt nhất cho việc cung cấp tốc độ T1 hoặc E1 trên các dây dẫn đồng xoắn cặp đôi thay vì kỹ thuật đã được sử dụng trong một thời gian dài là *đảo ngược mặt nạ luân phiên AMI* (Alternative Mark Inversion). *HDSL* sử dụng băng thông ít hơn và không đòi hỏi các bộ lặp tín hiệu tới vùng CSA. Bằng việc sử dụng tính tương đương của đường tự thích nghi và điều chế 2B1Q, *HDSL* truyền tải 1,544 Mbps hoặc 2,048 Mbps trong vùng dải thông từ 80 nast đến 1,5 MHz đòi hỏi bởi AMI. (AMI vẫn là thủ tục mã hoá được dùng chủ yếu cho T1).

Dịch vụ T1 có thể được thiết lập trong một ngày với chi phí nhỏ hơn 1000 USD để cài đặt modem ở đầu cuối của mỗi đường. Lắp đặt theo AMI giá thành đắt hơn nhiều và mất nhiều thời gian hơn bởi vì nó đòi hỏi phải lắp đặt các bộ lặp tín hiệu giữa các thuê bao và đầu trung kế CO. Phụ thuộc vào chiều dài của dây mà giá có thể cộng thêm cho các bộ lặp tín hiệu có thể lên đến 5000 USD và mất hơn 1 tuần lắp đặt.

*HDSL* sử dung đắt hơn tại những nơi có hệ thống điện thoại theo cơ chế tổ ong. Đường truyền từ trạm cơ sở đến trung kế CO sử dụng *HDSL* chiếm trên 50% giá lắp đặt. Hiện nay một phần lớn các đường T1 mới đã được cung cấp luồng T1.

*HDSL* cũng có hạn chế. Trước hết nó hiện không cung cấp cho dịch vụ thoại tương tự, bởi vì nó sử dụng băng thoại. Thứ hai, *ADSL* đạt được tốc độ lớn hơn so với *HDSL* bởi vì tính phi đối xứng của *ADSL* là có tính toán đến việc một phía dành cho thoại trong khi *HDSL* lại giữ lại cả hai đầu.

**HDSL-2**

*HDSL-2* là một chuẩn nổi trội và hứa hẹn một sự lựa chọn của *HDSL*. Mục đích của nó là chào bán các dịch vụ đối xứng ở các tốc độ T1 sử dụng một đôi dây dẫn đơn thay vì hai đôi. Điều này sẽ cho phép nó tiếp cận với khách hàng có tiềm năng lớn hơn. Nó cũng sẽ đòi hỏi sự điều chế tích cực hơn, khoảng cách ngắn hơn (khoảng 10000 fít) và chất lượng đường dây điện thoại tốt hơn.

Hầu như thiết bị SDSL (*Symmetric Digital Subscriber Line - Đường thuê bao số đối xứng*) trên thị trường ngày nay sử dụng mã đường 2B1Q được phát triển bởi mạng tích hợp dịch vụ số ISDN. Các công ty của Bell đã nhấn mạnh rằng việc sử dụng SDSL ở các tốc độ lớn hơn 768 Kbps có thể gây ra nhiễu cho các dịch vụ thoại và các dịch vụ khác mà chúng đang đảm trách trên cáp dẫn bằng đồng.

Lợi thế lớn nhất của *HDSL-2* là chúng được phát triển để phục vụ như một chuẩn theo đó các thiết bị của các nhà cung cấp khác có thể cùng vận hành. Nghĩa là nó được thiết kế không giao tiếp với các dịch vụ khác. Tuy nhiên *HDSL-2* chỉ có 1 tốc độ đó là dịch vụ chỉ ở 1,5 Mbps.

**SDSL**

*SDSL* là phiên bản *thích ứng* tốc độc của *HDSL* và giống như *HDSL* nó là đối xứng. Nó cho phép băng thông của kênh đi về (từ văn phòng của nhà cung cấp dịch vụ mạng NSP đến trạm của khách hàng) cũng giống như băng thông đường lên từ phía thuê bao tới NSP. *SDSL* chỉ hỗ trợ dữ liệu trên một đường đơn và không hỗ trợ các cuộc gọi tương tự. *SDSL* sử dụng sự mã hoá 2B1Q và có thể truyền tải tới 1,54 Mbps đi và đến thuê bao hoặc có thể cấu hình để bao hàm một vùng băng thông có sẵn đạt đến tốc độ 1,45 Mbps.

Tính đối xứng của *SDSL* bao hàm : kết hợp đặc tính luôn truy nhập (mà nó loại bỏ việc thiết lập cuộc gọi), làm cho nó thích ứng với công nghệ mạng WAN cho những văn phòng thương mại và chi nhánh cỡ nhỏ và vừa, và có thể thay đổi khi đủ điều kiện thành các dịch vụ như Frame Relay và các đường thuê bao riêng. Bởi vì truyền tải là đối xứng do vậy các dịch vụ như truyền File, Web Hosting và các ứng dụng học thuật từ xa có thể sẽ mang lại hiệu quả bằng việc thực thi theo công nghệ *SDSL*.

**G.SHDSL**

G.SHDSL là một chuẩn thiết lập trên phiên bản đa tốc độ của *HDSL-2* và đưa ra các dịch vụ đối xứng. Lợi thế của *HDSL-2* là chúng được phát triển để phục vụ như một chuẩn theo đó các thiết bị của các nhà cung cấp khác có thể cùng vận hành và rằng nó được thiết kế chỉ với một tốc độ T1. *HDSL-2* là một phần trong lần phát hành thứ hai của chuẩn được biết đến với tên *G.SHDSL* và cũng đã được ITU phê chuẩn. *G.SHDSL* được xây dựng trong lúc *HDSL-2* chào hàng các tốc độ đối xứng 2,3 Mbps.

**IDSL**

Thuật ngữ *IDSL* là viết tắt của tập hợp từ ISDN Digital Subscriber Line (Đường thuê bao số ISDN). Đây là công nghệ pha tạp giữa ISDN và xDSL. Nó giống như ISDN ở chỗ sử dụng một cặp dây dẫn đơn để truyền tải dữ liệu hai chiều ở tốc độ 128 Kbps và ở khoảng cách trong vùng RRD. Giống như ISDN, ISDL sử dụng mã đường 2B1Q để cho phép sự vận hành trong suốt thông qua các giao diện 'U' của ISDN. Người sử dụng khi đó vẫn có thể tiếp tục sử dụng các CPE đang tồn tại (Bộ chỉnh dòng ISDN BRI, các cầu và các routers ) để tạo các kết nối CO (Trung kế).

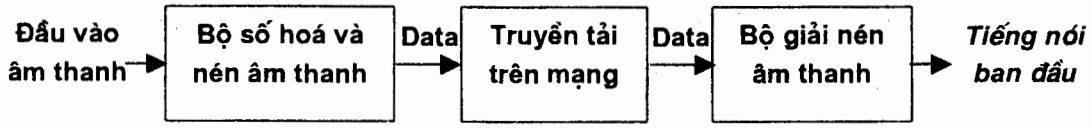
Sự khác biệt lớn là sóng mang. Không giống ISDN, ISDL không kết nối thông qua bộ chuyển mạch thoại. Một phần mới của thiết bị truyền thông dữ liệu ngắt kết nối IDSL và tách nó ra khỏi Router hoặc Data Switch. Đây là một đặc tính chủ yếu bởi vì việc quá tải tại các bộ chuyển mạch ở văn phòng trung tâm bởi người sử dụng dữ liệu là vấn đề ngày càng nghiêm trọng của các công ty điện thoại.

Hạn chế của IDSL là ở chỗ khách hàng không còn được cung cấp các dịch vụ tín hiệu hoặc thoại nữa. Nhưng với các ISP, những người không cung cấp dịch vụ thoại công cộng thì IDSL là một phương pháp hữu ích để sử dụng các dịch quay số đặt hàng truy nhập Internet tốc độ cao.

### 7.6.3. VoIP (Voice over IP)

*Định nghĩa* : Là dịch vụ điện thoại mà nội dung các cuộc đàm thoại được truyền tải thông qua hệ thống truyền tải của các mạng IP.

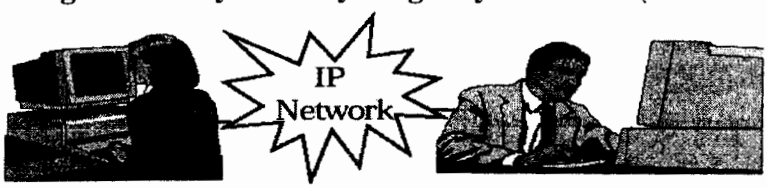
Với sự phát triển của công nghệ thông tin ngày nay hầu hết các thông tin đều có thể được truyền tải trên các hệ thống mạng mà trong đó cũng không loại trừ các dữ liệu là tiếng nói (đàm thoại, nhạc và kể cả hình ảnh ...). Tiếng nói vận hành trên các hệ thống này được thực hiện theo nguyên lý như được thể hiện trên hình 7.16.




**Hình 7.16. Sơ đồ truyền tải tiếng nói trên mạng**

Ngoài ra về khía cạnh an ninh đôi khi người ta còn áp dụng việc mã hoá và giải mã trong quá trình truyền tải. Nguyên lý này đã coi tiếng nói là một loại dữ liệu và do vậy hoàn toàn có thể truyền tải trên mạng giống như bất kỳ một dữ liệu nào khác. Từ nguyên lý trên đây ngày nay các dịch vụ VoIP dưới đây đã được triển khai xây dựng :

**Truyền tải tiếng nói từ máy tính này sang máy tính khác (hình 7.17);**

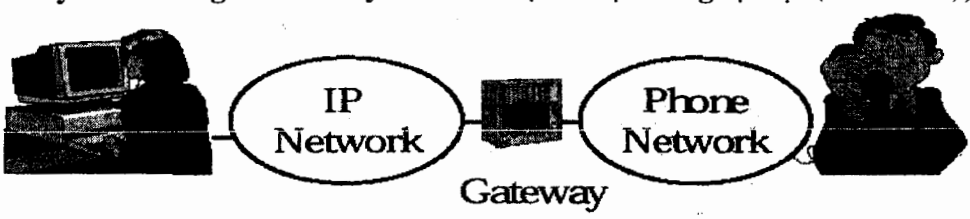



**Hình 7.17. Mô hình tuyền tải tiếng nói từ PC đến PC**

Khi này mỗi máy tính cần được trang bị thêm những thiết bị sau :

- Card xử lý âm thanh (Sound Card) kèm tai nghe;
- Một phần mềm điện thoại như Cuseeme, InternetPhone ...
- Có thể trang bị cả Camera nếu dịch vụ này được thiết lập.

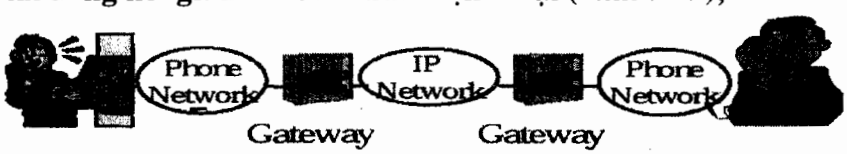
**Truyền tải tiếng nói từ máy tính tới điện thoại và ngược lại (hình 7.18);**




**Hình 7.18. Mô hình tuyền tải tiếng nói giữa PC và thuê bao điện thoại**

Khi này đòi hỏi phải có một gateway kết nối giữa mạng máy tính IP và mạng điện thoại. Đây thực chất là là dùng một Router kết nối tới tổng đài (PBX) của mạng điện thoại.

**Truyền tải tiếng nói giữa các thuê bao điện thoại (*hình 7.19*);**



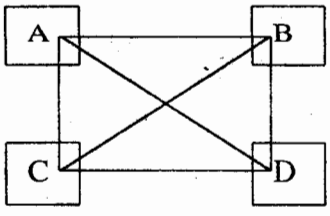

**Hình 7.19. Mô hình tuyền tải tiếng nói giữa các thuê bao điện thoại**

Khi này đòi hỏi phải có nhiều gateway để kết nối giữa mạng máy tính IP với các mạng điện thoại. Mạng IP khi này có thể là mạng Intranet hoặc Internet. Mạng điện thoại có thể là tổng đài riêng của cơ quan hoặc các bộ chuyển mạch sóng mang.

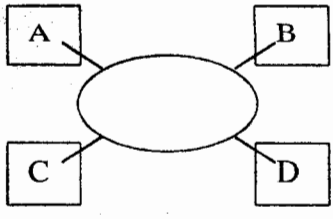
*1. Lợi điểm khi sử dụng VoIP.*

➢ Số đường liên kết giảm

Hình 7.20 minh hoạ số đường liên kết của mạng điện thoại thông thường và mạng điện thoại VoIP.




*a. Mạng điện thoại thường*




*b. Mạng VoIP*

**Hình 7.20. Sơ đồ liên kết của mạng điện thoại thường và mạng VoIP**

- Số liên kết của mạng điện thoại thường là $n \times (n-1)$ liên kết;
- Số liên kết của mạng VoIP là $n$.

➢ Cước phí trên mạng điện thoại thông thường tính theo cự ly và thời gian gọi trong khi cước phí trên mạng VoIP lại chỉ được coi như nội hạt do vậy sẽ rẻ hơn rất nhiều (nhất là khi gọi đi quốc tế).

➢ Có thể rễ ràng thay đổi lộ trình gọi do vậy tin cậy hơn;

➢ Không bị giới hạn trong băng thông 64 kbps như trong mạng điện thoại thông thường do vậy có thể rễ ràng cung cấp các dịch vụ với chất lượng cao.

*2. Các ứng dụng có thể xây dựng.*

➢ *Ứng dụng VoIP trên mạng PC cho phép cung cấp các dịch vụ :*

- Hội thảo có sử dụng tài liệu;
- Trợ giúp trực tiếp;
- Đặt hàng và xắp xếp từ xa.

➢ *Ứng dụng VoIP để xây dựng mạng giao dịch Quốc tế;*

➢ *Xây dựng một mạng VoIP cho hệ thống điện thoại riêng gọi là Intranet Telephone;*

➢ *Internet Fax;*

*3. Sự cần thiết phải có các dịch vụ QoS.*

Chất lượng dịch vụ (Quality of Services - QoS) luôn là điểm cần quan tâm đối với hệ thống thoại bất kỳ và mạng VoIP cũng không phải là ngoại lệ.

Trong mạng VoIP chất lượng âm thanh bị ảnh hưởng trực tiếp bởi 02 yếu tố chủ yếu :

- Mất một số gói tin; Gói tin bị mất gây ra hiện tượng âm thanh bị cắt xén hoặc bị bỏ qua. Các thuật toán mã hoá chuẩn công nghiệp có thể hiệu chỉnh tới 30ms của đoạn âm thanh bị mất. Do vậy các mẫu âm thanh tải trong một gói tin âm thanh nên là các mẫu có độ dài 20 ms. Chỉ có như vậy các thuật toán hiệu chỉnh mới có thể mang lại hiệu quả. Trong trường hợp xấu nhất cũng chỉ có thể mất một gói trong toàn bộ thời gian giao tiếp.
- Các gói tin bị trễ. Gói tin bị trễ có thể gây ra một trong các hiện tượng như giảm chất lượng âm thanh và do vậy độ suy hao của âm thanh sẽ lớn từ đầu cuối này tới đầu cuối khác, hoặc mất gói tin nếu độ trễ thay đổi. Nếu độ suy hao từ đầu cuối này tới đầu cuối khác quá lớn (ví dụ 250 ms), giao tiếp bắt đầu trở lên khó nghe và có những tạp âm như sóng đài. Nếu độ trễ thay đổi sẽ có thể xuất hiện nguy cơ tràn vùng đệm giữ các số liệu lệch trễ (jitter buffer) ở thời điểm nhận. Loại bỏ sự rớt âm và trễ là hoàn toàn cưỡng bức khi có các truyền tải Fax hoặc modems trên mạng IP. Nếu gói tin bị mất trong quá trình truyền tải của Fax hoặc modems các modems sẽ quay lại để đồng bộ lại.

Để có thể phân tích được nguyên nhân mất hoặc trễ gói tin cần thiết phải có đầy đủ kiến thức để hiểu tại sao chất lượng dịch vụ (QoS) lại liên quan đến mọi lĩnh vực của một mạng chuyên nghiệp. Bao gồm :

- Chất lượng mạng (Network Quality); Các gói tin có thể bị chia nhỏ nếu chất lượng mạng thấp, nếu mạng bị nghẽn hoặc nếu độ trễ thay đổi quá nhiều trên mạng. Chất lượng mạng thấp có thể dẫn đến các phiên giao dịch thường xuyên bị ngắt dịch vụ, bởi vậy có thể mất các kết nối về mặt vật lý hoặc logic. Vì thế khi thiết kế và triển khai một mạng VoIP cần phải nhận thức rằng cấu hình mạng logic và vật lý cần đặc biệt ổn định để từ đó đưa ra những phương pháp thích hợp cho việc thiết kế một mạng truyền tải âm thanh.
- Tắc nghẽn của mạng (Network Congestion); Tắc nghẽn mạng có thể dẫn đến hai khả năng : *gói tin bị mất* và *gói tin thay đổi độ trễ*. Gói tin bị mất từ việc tắc nghẽn mạng thông thường do các vùng đệm truyền tin bị đầy ở cửa ra nào đó trong mạng. Khi các liên kết hoặc các kết nối tiến gần tới việc sử dụng 100% tài nguyên, các hàng đợi đang được phục vụ đã đầy. Khi một hàng đợi đầy, một gói mới cố chen vào hàng đợi sẽ bị từ chối. Điều này có thể xảy ra trên các bộ chuyển mạch

Ethernet của các mạng Campus, đặc biệt trong mạng cung cấp dịch vụ Frame Relay.

- Độ trễ và lệch trễ (Delay and Jitter).

➢ *Độ trễ* (Delay) là khoảng thời gian gói tin đi từ điểm nhận đến điểm gửi và còn được gọi dưới một thuật ngữ "end-to-end delay" (khoảng trễ từ điểm đến điểm). *Độ trễ* gồm 02 thành phần : *Độ trễ cố định* của mạng (fixed network delay) và *độ trễ biến thiên* của mạng (variable network delay).

➢ *Lệch trễ* (Jitter) là khoảng lệch (delta) hoặc hiệu giữa hai giá trị trễ của hai gói tin âm thanh liền nhau trong dòng tin âm thanh gửi trên mạng.

➢ *Độ trễ* cố định của mạng nên được xem xét ở thời điểm thiết kế ban đầu của mạng VoIP. Chuẩn G.114 của Hiệp hội viễn thông Quốc tế (ITU) nêu rõ rằng *độ trễ* một chiều là 150ms được xem như tín hiệu âm thanh ở chất lượng cao. Trên thực tế đã cho thấy rằng có sự khác biệt không đáng kể nếu *độ trễ* cố định của mạng là 200ms. Độ trễ cố định của mạng bao gồm : *Độ trễ lan truyền* tín hiệu giữa đầu gửi và đầu nhận, *độ trễ do mã hoá âm thanh* và *thời gian đóng gói* của các bộ codecs VoIP khác nhau. Các tính toán về độ trễ lan truyền cho thấy hầu như giá trị này đạt ở mức 0.0063ms/km. Chẳng hạn bộ codec G.729A có độ trễ mã hoá là 25ms (02 frame mỗi frame 10ms cộng với 5ms cho phần header và 20ms trễ do đóng gói).

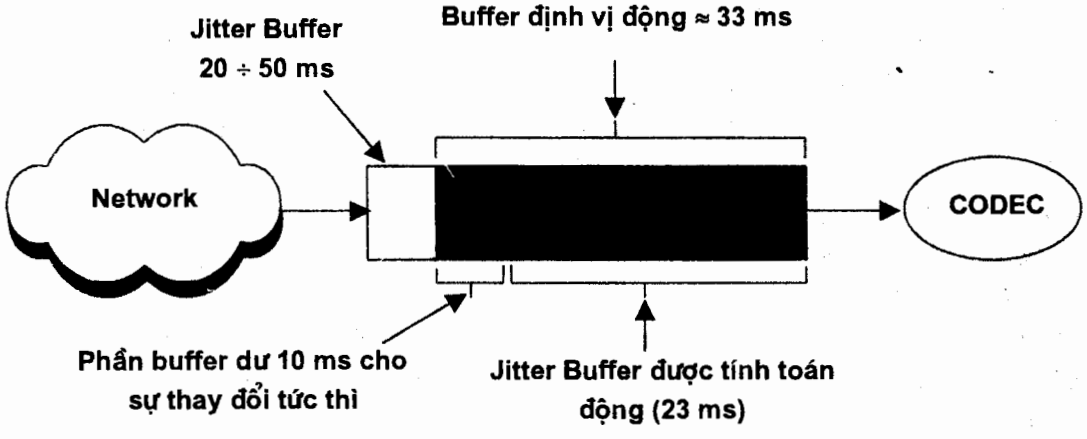
➢ Các hàng đợi tắc nghẽn ở đường ra và các độ trễ theo hàng trên giao diện mạng có thể gây ra độ trễ gói biến thiên. Không kể đến sự ưu tiên hoặc hoặc độ suy hao thấp do xếp hàng (Low-Latency Queuing - LLQ), số lần trễ do xếp hàng bằng với số lần *trễ do đặt gói tin vào đường truyền (serialization delay)* khi việc sử dụng liên kết đạt tới 100%. *Độ trễ do đặt gói tin vào đường truyền* là một chức năng bất biến của *vận tốc liên kết* (link speed) và *kích cỡ của gói tin*. Như nêu trong bảng 7.3., một gói lớn hơn và *vận tốc liên kết* nhỏ hơn thì *độ trễ do đặt gói tin vào đường truyền* lớn hơn. Khi biết được tỷ lệ này nó có thể được xem xét biến thiên (động) bởi một gói dữ liệu lớn hơn có thể đi vào *hàng đợi rồi* trước một gói âm thanh ở bất kỳ thời điểm nào. Nếu gói âm thanh cần phải đợi gói dữ liệu được đặt vào đường truyền, độ trễ gây ra bởi gói âm thanh là bản thân *độ trễ do đặt gói tin vào đường truyền* cộng với *độ trễ do đặt gói tin vào đường truyền* của gói dữ liệu đứng trước nó. Các kỹ thuật liên kết chia mảnh và chèn (Link Fragmentation and Interleave) có thể được hình thành sao cho giá trị trễ là không đổi. Bởi vì tắc nghẽn mạng có thể gặp phải ở bất kỳ thời điểm nào trong mạng, các vùng đệm có thể chiếm ngay lập tức. Sự sử dụng vùng đệm tức thời này có thể dẫn đến sự sai lệch số lần trễ giữa các gói trong cùng một luồng âm thanh. Sự sai lệch này (còn gọi là lệch

trễ) là sự thay đổi thời gian ước tính một gói sẽ xuất hiện so với thời gian khi nó thực sự được nhận. Để triệt tiêu những sai lệch trễ giữa các gói âm thanh giao tiếp, các đầu cuối của VoIP sử dụng các vùng đệm lệch trễ (Jitter Buffer) để hướng những khác biệt về lệch trễ thành giá trị không đổi sao cho âm thanh chuyển qua nhịp nhàng.

Bảng 7.3

**Độ trễ theo thứ tự xắp xếp là một hàm của tốc độ liên kết và kích cỡ của gói**

| Tốc độ liên kết | Kích cỡ của gói | | | | | |
|---|---|---|---|---|---|---|
| | 64 Bytes | 128 Bytes | 256 Bytes | 512 Bytes | 1024 Bytes | 1500 Bytes |
| 56 kbps | 9 ms | 16 ms | 36 ms | 72 ms | 144 ms | 214 ms |
| 64 kbps | 8 ms | 8 ms | 32 ms | 64 ms | 128 ms | 187 ms |
| 128 kbps | 4 ms | 4 ms | 16 ms | 32 ms | 64 ms | 93 ms |
| 256 kbps | 2 ms | 2 ms | 8 ms | 16 ms | 32 ms | 46 ms |
| 512 kbps | 1 ms | 1 ms | 4 ms | 8 ms | 16 ms | 23 ms |
| 768 kbps | 0,640 ms | 1.28 ms | 2.56 ms | 5.12 ms | 10.24 ms | 15 ms |




**Hình 7.21. Vùng đệm Jitter thích ứng**

➢ Các thiết bị đầu cuối của mạng VoIP sử dụng bộ xử lý tín hiệu số (Digital Signal Processor) có áp dụng các thuật toán để điều chỉnh Jitter buffer trong khoảng 20 ÷ 50 ms như được minh hoạ trên hình 7.21.

➢ Kích cỡ thực tế của buffer thay đổi từ 20 ÷ 50 ms dựa trên độ trễ đã quy định của mạng cho gói âm thanh. Những thuật toán này phân tích thời gian trễ được ghi trong vùng header của gói tin âm thanh trong giao thức truyền thông thời gian thực (Real-time Transport Protocol - RTP) để tính ra độ trễ mong muốn và hiệu chỉnh Jitter buffer phù hợp.

Khi jitter buffer thích ứng được hình thành, phần buffer dư 10 ms được cấu hình cho những độ trễ gói thay đổi. Chẳng hạn nếu một dãy các gói đang đi vào jitter buffer với thời gian trễ được ghi trong phần header của giao thức RTP là 23 ms trong tổng thể Jitter Buffer của mạng, thì kích cỡ của Jitter buffer thay đổi nhiều nhất là 33 ms (22+10 = 33 ms) . Nếu phần Jitter lớn hơn 10 ms như chỉ ra ở trên gói tin sẽ bị chia nhỏ ra.

### 7.6.4. IP Routing

Các giao thức định tuyến theo IP (IP Routing) là các giao thức động. Các cuộc gọi được định tuyến động bởi Router được tính tự động trong các khoảng thời gian như nhau bởi phần mềm cài đặt trong các thiết bị định tuyến. Nó tương phản với sự định tuyến tĩnh mà tại đó các Routers được thiết lập bởi người quản trị mạng và không thay đổi cho đến khi người quản trị thay đổi chúng. Một bảng định tuyến IP chứa các cặp địa chỉ đến của các chặng tiếp theo được sử dụng để cho phép định tuyến động. Một sự ghi nhận trong bảng này có thể được thông dịch như sau : tới mạng có địa chỉ ví dụ là 129.100.0.0, gửi gói tin đến ngoại vi Ethernet 0 (E0). IP Routing chỉ ra lược đồ dữ liệu IP chuyển đi trong liên mạng, mỗi chặng (hop) một lần. Bởi vậy, tuyến tổng thể không được biết đến tại thời điểm đầu của hành trình. Thay vì thế, tại mỗi lần dừng, địa chỉ đến tiếp theo lại được tính bằng việc đối sánh địa chỉ đến bên trong lược đồ dữ liệu với bảng tiếp nhận tại bảng định tuyến của node hiện thời.

Mỗi sự can dự của node trong quá trình định tuyến được giới hạn bằng việc chuyển tiếp các gói tin nhờ vào các thông tin bên trong. Các node không giám sát các gói tin lấy từ đâu, đi tới địa chỉ cuối cùng nào và cũng không cung cấp các báo cáo lỗi, phản hồi lại cho nơi gửi những bất thường xảy ra trong việc định tuyến. Công việc này được giao phó cho giao thức khác của Internet Protocol đó là giao thức ICMP (Internet Control-Message Protocol - Giao thức điều khiển thông báo Internet). Giao thức này là một giao thức Internet, thuộc lớp mạng. Nó cung cấp các gói thông tin thông báo về các báo cáo lỗi và các thông tin khác, đánh giá việc xử lý gói tin IP để phản hồi lại nơi gửi.

**Các giao thức bên trong và bên ngoài**

Các giao thức định tuyến chủ yếu được chia làm hai loại : giao thức cổng đợi bên trong IGP (Interior Gateway Protocol) và giao thức cổng đợi bên ngoài EGP (Exterior Gateway Protocol). Các giao thức định tuyến bên trong bao gồm giao thức thông tin định tuyến RIP (Routing Information Protocol), Hello, giao thức định tuyến cổng đợi bên trong IGRP và giao thức mở đường ngắn nhất đầu tiên OSPFP (Open Shortest Path First Protocol ). Giao thức bên trong được dùng cho các mạng định tuyến mà nó được giám sát bằng các cách quản trị thông thường. Trong khi giao thức định tuyến bên ngoài bao gồm EGP và giao thức cổng biên BGP (Border Gateway Protocol) được sử dụng để trao đổi thông tin định tuyến giữa các mạng không chia sẻ sự quản trị thông thường.

RIP là giao thức định tuyến được sử dụng bởi quá trình định tuyến trong hệ thống. Rất nhiều mạng sử dụng RIP; Nó làm việc tốt đối với các mạng nhỏ, biệt lập và tô pô đơn giản.Hello is giao thức định tuyến cũ trước đây được sử dụng trên đường backbone của mạng nghiên cứu khoa học NFS. IGRP tập trung vào các mạng lớn với tô-pô phức tạp và các phần có đặc tính trễ và băng thông khác nhau.. EGP là giao thức bên ngoài, nó là giao thức gốc và vẫn được sử dụng chủ yếu trong mạng dữ liệu quân sự Mỹ DDN và mạng nghiên cứu khoa học quốc gia NFS. BGP là giao thức định tuyến bên ngoài mới ra đời. Nó giải quyết một vài lỗi của EGP. Trong khuôn khổ giáo trình này sẽ đề cập tương đối chi tiết về giao thức thông tin định tuyến RIP.

**Routing information Protocol (RIP)**

Giao thức thông tin định tuyến RIP (Routing Information Protool) là một trong những giao thức lâu đời nhất trong tất cả các giao thức định tuyến. RIP cũng là một trong những giao thức rất rễ nhầm bởi vì tính đa dạng của RIP và những giao thức định tuyến giống RIP đã được sinh ra. Một số trong số các giao thức đó thậm chí được sử dụng cùng tên ! RIP và vô số các giao thức giống RIP khác đã được hình thành trên một bộ các thuật toán sử dụng các vector khoảng cách để so sánh về mặt toán học các tuyến đường nhằm xác định đường tối ưu tới mọi địa chỉ đích. Những thuật toán này ra đời từ nghiên cứu học thuật trong năm 1957. Những phiên bản chuẩn mở ngày nay của RIP đôi khi đã qui RIP như là giao thức thông tin định tuyến IP và được chính thức định nghĩa trong hai tài liệu : Request For Coments (RFC) 1058 và Internet Standard (STD) 56. Khi mạng dựa trên IP trở nên nhiều hơn và kích cỡ lớn hơn, các lực lượng triển khai thiết kế Internet (Internet Engineering Task Force - IETF) thấy rõ RIP cần được nâng cấp. Do đó IETF đã phát hành RFC 1388 vào tháng 01-1993 và RFC 1723 vào tháng 11-1994 mà nó mô tả RIP 2 (phiên bản thứ hai của RIP). Những tài liệu RFC đã mô tả những sự mở rộng khả năng của RIP nhưng không loại bỏ các phiên bản trước đây của RIP. RIP 2 đã cho phép các thông báo RIP mang nhiều thông tin hơn, được

phép sử dụng cơ chế xác nhận đơn giản cho bảng an toàn cập nhật. Quan trọng hơn là RIP 2 đã hỗ trợ mặt nạ cho các mạng con (subnet) - một đặc tính quan trọng chưa có ở RIP.

*Quá trình cập nhật tuyến đường của RIP*

RIP gửi thông báo cập nhật tuyến đường ở những khoảng thời gian xác định và khi tô pô của mạng thay đổi. Khi Router nhận được một cập nhật tuyến đường (bao gồm những thay đổi cho một sự tiếp nhận) nó cập nhật lại bảng định tuyến để phản ánh tuyến đường mới. Giá trị đo cho đường này được tăng lên 1 đơn vị và người gửi được chỉ ra như một chặng (hop) tiếp theo. RIP router chỉ duy trì các tuyến đường tốt nhất hay còn gọi là tuyến đường ngắn hơn (tuyến đường với giá trị đo nhỏ hơn).

Sau khi đã cập nhật bảng định tuyến của mình, Router phát đi các sửa đổi về tuyến đường để thông báo cho các routers mạng khác biết sự thay đổi này. Những cập nhật này là được gửi độc lập với những cập nhật xắp lịch thường xuyên do các Routers RIP gửi đi.

*Đơn vị đo tuyến đường của RIP*

RIP sử dụng một đơn vị đo tuyến đường riêng rẽ (đếm chặng) để đo khoảng cách giữa mạng nguồn và mạng đích. Mỗi chặng trong đường từ nguồn đến đích được gán giá trị đếm là một chặng, nói chung được tính là 1 đơn vị. Khi Router nhận một cập nhật tuyến đường mà nó chứa sự tiếp nhận của một mạng đích mới hoặc một mạng đích thay đổi, Router thêm 1 vào giá trị đo được chỉ ra trong hồ sơ cập nhật và tiếp nhận mạng đó trong bảng định tuyến. Địa chỉ IP của người gửi này được sử dụng như chặng tiếp theo.

*Các đặc tính ổn định của RIP*

RIP ngăn chặn sự lặp lại của tuyến đường khỏi sự kéo dài vô hạn định bằng việc giới hạn thực hiện số các chặng được phép trong một con đường từ nguồn đến đích. Số tối đa các chặng trong một đường là 15. Nếu một Router nhận một cập nhật tuyến đường chứa sự tiếp nhận mới hoặc tiếp nhận thay đổi và nếu việc tăng đơn vị đo lên 1 gây ra cho đơn vị đo trở thành không xác định (nghĩa là giá trị bằng 16) thì địa chỉ đích của mạng được xem như không thể tới. Việc mất tính ổn định này là do nó bị giới hạn đường kính tối đa của một mạng RIP là nhỏ hơn 16 chặng (hop).

RIP bao gồm một số đặc tính ổn định khác mà nó chung cho nhiều giao thức định tuyến khác. Những đặc tính này được thiết kế để cung cấp tính ổn định, bất chấp những thay đổi nhanh chóng, đầy tiềm năng của các tô-pô mạng. Ví dụ, RIP thực hiện sự phân tầng và giữ các cơ chế để tránh các thông tin định tuyến không chính xác khỏi các thông tin hiện đang truyền tải trên mạng.

*Các bộ đếm thời gian của RIP*

RIP sử dụng nhiều bộ đếm thời gian để điều chỉnh hiệu năng của nó. Chúng bao gồm một bộ đếm cập nhật tuyến đường, một bộ đếm thời gian vượt ngưỡng của tuyến đường định tuyến và một bộ đếm tràn đường. Bộ đếm cập nhật tuyến đường tính giờ cho khoảng thời gian giữa các cập nhật tuyến đường định kỳ. Thông thường nó được đặt là 30s, với một lượng thời gian nhỏ đã được bổ sung ngẫu nhiên mỗi khi bộ đếm reset. Điều này được làm để ngăn chặn tắc nghẽn có thể xảy ra khi tất cả các Routers đồng thời cập nhật tới Router hàng xóm của mình. Mỗi sự tiếp nhận trong bảng định tuyến có một bộ đếm thời gian vượt ngưỡng của tuyến đường truyền với nó. Khi bộ đếm thời gian vượt ngưỡng của tuyến đường hết hạn, tuyến đường này được đánh dấu là không hợp lệ nhưng vẫn được giữ lại trong bảng đến khi bộ đếm tràn đường hết hạn.

*Khuôn dạng các gói tin*

Phần dưới đây tập chung vào việc minh hoạ khuôn dạng của các gói tin IP RIP và IP RIP 2. Mỗi minh hoạ đều kèm theo mô tả các trường.

*Khuôn dạng gói tin IP RIP*

| 1 byte trường lệnh | 1 byte trường số phiên bản | 2 byte trường Zero (0) | 2 byte trường AFI | 2 byte trường Zero (0) | 4 byte trường địa chỉ IP | 4 byte trường Zero (0) | 4 byte trường Zero (0) | 4 byte trường đơn vị đo |
|---|---|---|---|---|---|---|---|---|

**Hình 7.22. Khuôn dạng gói tin IP RIP**

Một gói tin IP RIP bao gồm 9 trường (*xem hình 7.22.*), nội dung các trường :

- ***Trường lệnh*** : Chỉ ra khi nào gói được yêu cầu hoặc được đáp lại. Yêu cầu này hỏi rằng một Router gửi tất cả hoặc một phần bảng định tuyến của nó. Sự đáp lại này có thể là một cập nhật định tuyến thường lệ tự nguyện hoặc một sự trả lời cho một yêu cầu. Các sự đáp lại chứa những tiếp nhận bảng định tuyến. Các gói có nhiều RIP được sử dụng để vận chuyển thông tin từ các bảng định tuyến lớn.
- ***Trường số hiệu phiên bản*** : Trường này chỉ ra phiên bản của RIP được sử dụng. Trường này có thể báo hiệu sự khác biệt tiềm ẩn của các phiên bản không tương thích.
- ***Trường Zero*** : Trường này thực chất không sử dụng bởi RFC 1058 RIP; nó đã được bổ sung chỉ để cung cấp tính tương thích với các chuẩn trước đây thể hiện sự đa dạng của RIP. Tên của nó xuất phát từ việc giá trị ngầm định của nó là 0.
- ***Trường xác nhận họ địa chỉ AFI (Address-Family Identifier)*** : Chỉ ra địa chỉ của một họ đang được sử dụng. RIP được thiết kế để truyền thông tin định

tuyến cho một vài giao thức khác nhau. Mỗi một tiếp nhận có một số hiệu xác nhận họ địa chỉ để chỉ ra kiểu địa chỉ đang ghi. AFI cho IP là 2.

- ***Trường địa chỉ IP*** : Chỉ ra địa chỉ IP của tiếp nhận.
- ***Trường đơn vị đo*** : Chỉ ra bao nhiêu chặng (Routers) đã đi qua trong hành trình đến đích. Giá trị này ở khoảng từ 1 đến 15 đối với một đường hợp lệ hoặc 16 đối với đường không đến được.

***Lưu ý*** : Có tới 25 trường hợp cho các trường *AFI, địa chỉ* và *đơn vị đo* là được phép trong một gói RIP IP riêng rẽ. (25 địa chỉ đích có thể được liệt kê trong một gói RIP riêng rẽ).

*Khuôn dạng gói tin IP RIP 2*

| 1 byte trường lệnh | 1 byte trường số phiên bản | 2 byte trường không sử dụng | 2 byte trường AFI | 2 byte trường tuyến đích | 4 byte trường địa chỉ mạng | 4 byte trường mặt nạ mạng | 4 byte trường Chặng tiếp theo | 4 byte trường đơn vị đo |
|---|---|---|---|---|---|---|---|---|

**Hình 7.23. Khuôn dạng gói tin IPRIP 2**

Tham số kỹ thuật của IP RIP 2 (được mô tả trong RFC 1723) cho phép bao gồm nhiều thông tin trong các gói RIP và cung cấp một cơ chế xác nhận đơn giản mà nó không được hỗ trợ bởi IP RIP. Hình 7.23. giới thiệu khuôn dạng đầy đủ của gói tin IP RIP 2. Một gói tin IP RIP 2 chứa các trường tương tự như IP RIP. Dưới đây là tổng hợp các mô tả về khuôn dạng gói tin IP RIP 2 :

- ***Trường lệnh*** : giống như mô tả trong IP RIP.
- ***Trường số hiệu phiên bản*** : Trường này chỉ ra phiên bản của RIP được sử dụng. Trường này được đặt giá trị là 2
- ***Trường không sử dụng*** : Có giá trị đặt là 0
- ***Trường xác nhận họ địa chỉ AFI (Address-Family Identifier)*** : Chỉ ra địa chỉ của một họ đang được sử dụng. Chức năng các trường AFI của RIP 2 xác nhận theo RFC 1508 với một ngoại lệ : Nếu AFI cho sự tiếp nhận đầu tiên trong thông báo là 0xFFFF, phần còn lại của tiếp nhận chứa thông tin xác nhận. Hiện nay kiểu của sự xác nhận chỉ đơn giản là mật khẩu.
- ***Trường tuyến đích (Route tag)*** : Cung cấp một phương pháp phân biệt giữa tuyến bên trong (được nghiên cứu bởi RIP) và tuyến bên ngoài (được nghiên cứu từ các giao thức khác).
- ***Trường địa chỉ IP*** : Chỉ ra địa chỉ IP của tiếp nhận.
- ***Trường Subnet Mask*** : Chứa subnet mask cho tiếp nhận. Nếu trường này bằng 0, không có subnet mask nào được chỉ định cho tiếp nhận.

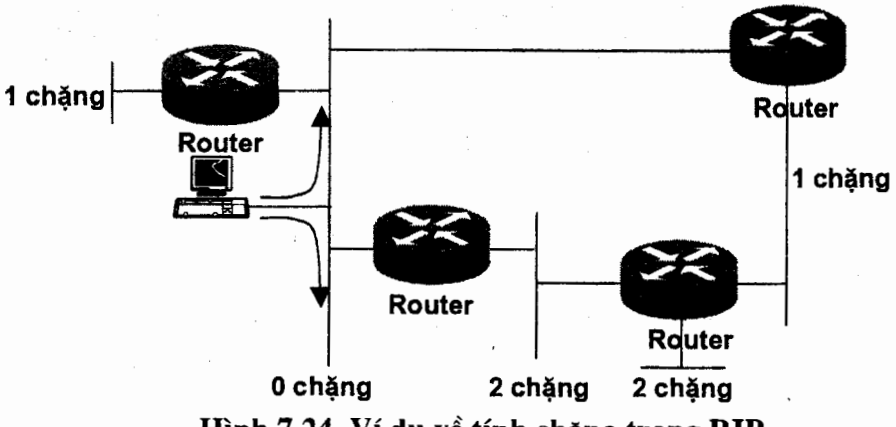
➢ ***Trường chặng tiếp theo*** : Chỉ ra địa chỉ IP của chặng tiếp theo cho tiếp nhận sẽ gửi đến.

➢ ***Trường đơn vị đo*** : Chỉ ra bao nhiêu chặng (Routers) đã đi qua trong hành trình đến đích. Giá trị này ở khoảng từ 1 đến 15 đối với một đường hợp lệ hoặc 16 đối với đường không đến được.

***Lưu ý*** : Có tới 25 trường hợp cho các trường *AFI, địa chỉ* và *đơn vị đo* là được phép trong một gói RIP IP riêng rẽ. Nghĩa là 25 sự tiếp nhận bảng định tuyến có thể được liệt kê trong một gói RIP riêng rẽ. Nếu AFI chỉ ra một thông báo xác nhận thì chỉ 25 sự tiếp nhận bảng định tuyến có thể được chỉ ra.

*Cấu hình một giao thức RIP*

RIP sử dụng việc quảng bá các gói tin dữ liệu tuân thủ giao thức UDP (User Datagram Protocol) để trao đổi thông tin. Mỗi Router gửi các cập nhật thông tin định tuyến sau mỗi chu kỳ 30s; tiến trình này được gọi dưới thuật ngữ "*Quảng cáo*". Nếu một Router không nhận một cập nhật từ các Router khác trong khoảng thời gian 180s hoặc nhiều hơn, nó đánh dấu các tuyến đường được phục vụ bởi *Router không cập nhật* như là không sử dụng. Nếu không cập nhật trong khoảng 240s, Router này sẽ huỷ tất cả các cửa vào của bảng định tuyến. Đơn vị đo mà RIP sử dụng để ước lượng giá trị các con đường là *số chặng*. Số chặng là số các Routers đi ngang qua trong một đường. Mạng nối trực tiếp có đơn vị đo là 0 (*xem hình 7.24.*); một mạng không đến được có đơn vị đo là 16. Chính vì đơn vị đo quá ít ỏi này làm cho giao thức RIP không phù hợp với các mạng lớn. Nếu Router có đường dẫn mạng mặc định, RIP sẽ *quảng cáo* một tuyến đường mà nó nối Router tới một địa chỉ mạng ảo (địa chỉ 0.0.0.0). Địa chỉ mạng 0.0.0.0 không tồn tại; RIP sẽ xem 0.0.0.0 như một mạng để thực hiện các đặc tính định tuyến mặc định.

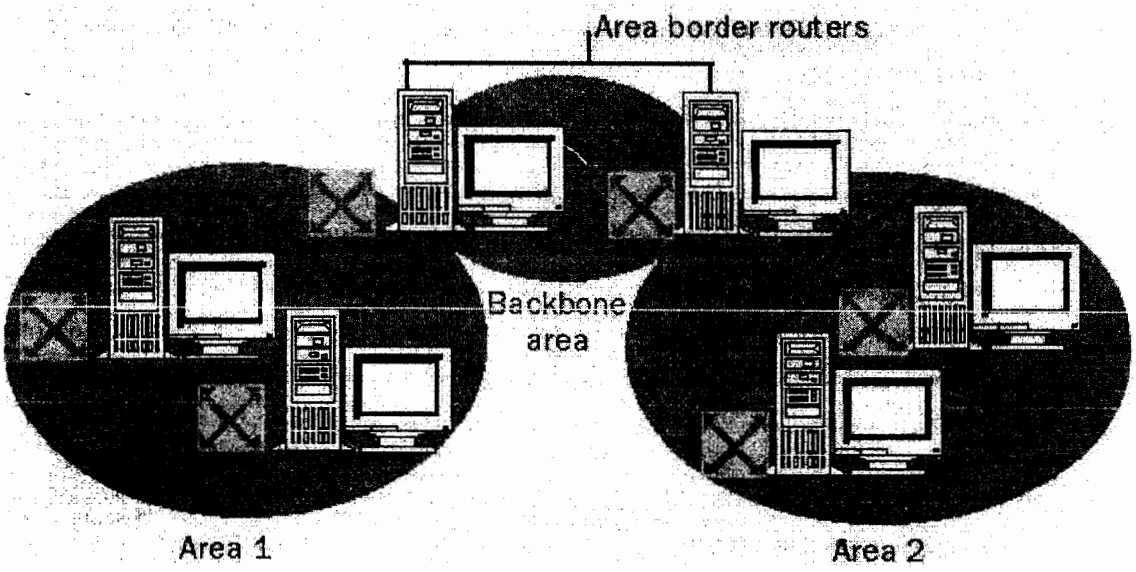



**Hình 7.24. Ví dụ về tính chặng trong RIP**

**2. Giao thức mở đường dẫn ngắn nhất đầu tiên(OSPFP).**

OSPFP là một giao thức định tuyến theo trạng thái đường nó cho phép các route trao đổi thông tin và tạo ra một lược đồ hình mạng cho phép tính toán được các đường dẫn ngắn nhất đến mỗi mạng. Trong lúc dữ liệu về trạng thái đường thay đổi thì các bảng định đường sẽ được tính toán lại. Nếu kích cỡ của bảng dữ liệu tăng thì thời gian cho các route tính toán cũng phải tăng. OSPF chia liên mạng thành các vùng. Các vùng này sẽ liên kết đến các vùng khác qua một backbone (đó là những đường nối kết và phần cứng nối kết dùng để truyền dữ liệu với tốc độ cao) của vùng. Một backbone trong OSPF là một bộ định tuyến, nó được đấu nối tới backbone của vùng. Các backbone này không chỉ đấu nối tới một vùng mà được nối tới nhiều vùng. Tuy nhiên, giữa các backbone này không có các đường truyền tốc độ cao. Các backbone này có tất cả các đường nối tới tất cả các backbone khác ở trong một vùng mạng.

Mỗi route chỉ lưu một cơ sở dữ liệu về trạng thái đường cho tất cả các vùng mạng mà nó có thể nối tới. Các đường tốc độ cao làm nhiệm vụ nối backbone của vùng này với backbone của vùng khác, như chỉ ra trong hình 7.25.




**Hình 7.25 Thiết kế một vùng OSPF cơ bản**

Mô hình OSPF là tốt nhất đối với kiểu mạng có kích cỡ cực kỳ lớn, nhiều đường, liên mạng IP động giống như kiểu công ty hay một tổ chức, hoặc các liên mạng có quy mô rộng lớn. Để quản lý các route và các đường kết nối phải tuân thủ:

- Bảo đảm rằng ABRs trong vùng phải là các cặp thích hợp mà đường ra chung của nó là route của vùng.

- Bảo đảm rằng các bộ lọc định tuyến trên ABR không quá bị giới hạn. các bộ lọc định tuyến bên ngoài là các bảng định tuyến ngoài được lựa chọn trong hộp thoại OSPF Routing Protocol Properties.
- Bảo đảm rằng tất cả các ABRs đều được đấu nối vật lý đến backbone hoặc đấu nối logic đến backbone đó bằng việc sử dụng một đường ảo. Các đường này không nên quay lại các route đã đi qua, điều này có nghĩa rằng các route đấu nối tới hai vùng sẽ không đi qua cùng một backbone này.

# CHƯƠNG 8

# AN NINH MẠNG

Mục tiêu của việc kết nối mạng là để nhiều người sử dụng từ những vị trí địa lý khác nhau, có thể dùng chung những tài nguyên, đặc biệt là tài nguyên thông tin. Do đặc điểm của nhiều người sử dụng và phân tán về mặt địa lý nên việc bảo vệ các tài nguyên đó tránh khỏi sự mất mát, xâm phạm (vô tình hay hữu ý) phức tạp hơn rất nhiều so với trường hợp máy tính đơn lẻ, một người sử dụng. Để việc đảm bảo thông tin đạt kết quả cao, chúng ta phải lường trước được càng nhiều càng tốt các khả năng xâm phạm, các sự cố rủi ro đối với thiết bị và tài nguyên trên mạng. Xác định càng chính xác các nguy cơ trên, càng quyết định được tốt các giải pháp phù hợp để giảm thiểu các thiệt hại.

Internet có những kỹ thuật tuyệt vời cho phép mọi người truy nhập, khai thác, chia sẻ thông tin. Nhưng nó cũng là nguy cơ chính dẫn đến thông tin bị hư hỏng hoặc phá huỷ hoàn toàn.

Để bảo vệ cho các mạng nội bộ (LAN, Intranet) khi kết nối vào Internet hay kết nối với nhiều mạng nội bộ khác có những độ an toàn, bảo mật khác nhau, người ta thường phải bổ xung thêm các giải pháp kỹ thuật an toàn mạng và ban hành các chính sách bảo mật thông tin cụ thể.

## 8.1 Các hiểm hoạ trên mạng máy tính

Khi xây dựng một hệ thống bảo vệ, vấn đề đầu tiên mà ta cần quan tâm là ta cần phải bảo vệ những gì. Trong một hệ thống thông tin mạng nói chung, đó chính là dữ liệu, tài nguyên và danh tiếng của ta.

**Dữ liệu:**

Có ba đặc tính sau rất quan trọng đối với dữ liệu:

- Tính bảo mật: Chỉ những người có quyền mới được biết.
- Tính toàn vẹn: Không bị hư hỏng, bị sửa đổi hay mất mát.
- Tính kịp thời: Sẵn sàng bất cứ lúc nào cần.

**Tài nguyên:**

Chúng ta phải tiêu tốn nhiều thời gian và tiền bạc cho tài nguyên và ta có quyền quyết định chúng phải sử dụng như thế nào. Tài nguyên của máy tính không phải là tài

nguyên thiên nhiên, nó có giới hạn và không được lãng phí hay phá huỷ nếu không được sử dụng.

**Danh tiếng**

Khi một kẻ tấn công xuất hiện trên Internet với định danh của chúng ta, thì bất kỳ điều gì người đó làm thì cũng liên quan đến chúng ta. Nếu như người bị tấn công là một công ty lớn hay các cơ quan trong bộ máy nhà nước thì vấn đề uy tín trở nên rất quan trọng. Trong trường hợp người quản trị hệ thống chỉ biết được sau khi chính hệ thống của mình được dùng làm bàn đạp để tấn công vào các hệ thống khác thì tổn thất về uy tín là không thể tính được và để lại hậu quả lâu dài.

**Các đối tượng tân công mạng- Hacker:** Thuật ngữ "hacker" thực ra không phải lúc nào cũng mang ý nghĩa tiêu cực. Đúng ra là nó hàm ý chỉ một người nào đó rất kiên trì, cố gắng phá vỡ cái gì đó và đoán xem nó làm việc như thế nào. Bởi vì hầu hết những người thực hiện "hacking" đều là các thần đồng trong lĩnh vực khoa học máy tính. Tuy nhiên, mục đích trong phần này thì "hacker" được ám chỉ như là những kẻ phá hoại.

Một kẻ phá hoại thường muốn truy nhập vào hệ thống mạng vì một lý do này hay lý do khác. Sau đây là một số lý do có thể:

- Chỉ để tò mò giải trí.
- Để xem xét chung chung.
- Để ăn cắp các tài nguyên máy tính như thời gian của bộ CPU.
- Để ăn cắp các bí mật thương mại, quốc gia hoặc các thông tin độc quyền khác.
- Phát động chiến tranh thông tin trên mạng, làm tê liệt mạng.

Trong mọi trường hợp bất kể vì lý do gì thì đằng sau cuộc tấn công, thông tin mà kẻ phá hoại muốn lấy nhất là tệp /passwd- thông tin mật khẩu. Tuy nhiên, các thông tin mật khẩu trong tệp /passwd đều được mã hoá, nhưng điều này không có nghĩa là mật khẩu vẫn an toàn. "Hacker" có thể dùng chương trình *Bộ giải mã mật khẩu* (Password Cracker) để cố đoán các mật khẩu trong tệp đó bằng cách so sánh chúng với các từ trong một từ điển hoặc Brouce Force (tất nhiên phương pháp này không hiệu quả). Mức độ thành công của chương trình giải mật khẩu tuỳ thuộc vào tài nguyên của CPU, vào chất lượng của từ điển và vào việc người dùng có một bản sao của tệp /passwd.

Các hình thức tấn công phá hoại trên mạng :

Có rất nhiều kiểu tấn công vào các hệ thống và cũng có nhiều cách để phân loại các tấn công này, sau đây đề cập đến một số kiểu tấn công chính sau:

**1.Tấn công trực tiếp:** Phần lớn các cuộc tấn công vào hệ thống là trực tiếp. Một phương pháp tấn công cổ điển là dò cặp tên người dùng và mật khẩu

(username/password). Đây là phương pháp khá đơn giản, dễ thực hiện và không đòi hỏi một điều kiện đặc biệt nào để bắt đầu. Kẻ tấn công có thể sử dụng những thông tin như tên người dùng, ngày sinh, địa chỉ, số nhà....để đoán mật khẩu. Một số chương trình có thể lấy được dễ dàng từ Internet để giải mã các mật khẩu đã mã hoá của hệ thống, chúng có khả năng thử các tổ hợp các từ trong một từ điển lớn theo những quy tắc do người dùng tự định nghĩa. Trong một số trường hợp, khả năng thành công của phương pháp có thể lên tới 30%.

Một phương pháp khác là sử dụng các lỗ hỏng bảo mật do lỗi chương trình ứng dụng và bản thân hệ điều hành. Đây là phương pháp đã được sử dụng từ những vụ tấn công đầu tiên và vẫn tiếo tục được sử dụng để chiếm quyền truy nhập. Khi đã chiếm được quyền truy nhập, kẻ tấn công có thể sử dụng nhiều kỹ thuật để phá hoại mạng như xoá các tập tin, làm treo máy chủ, ăn cắp thông tin...

**2.Nghe trộm:** Có một số kiểu tấn công cho phép kẻ tấn công lấy được thông tin mà không cần sử dụng máy tính một cách trực tiếp. Phần lớn những kẻ ăn cắp thông tin đều cố gắng truy cập vào hệ thống máy tính bằng cách dò tìm tên người dùng và mật khẩu. Cách dễ nhất để lấy thông tin là đặt máy nghe trộm trên mạng.Việc nghe trộm thường được tiến hành ngay sau khi kẻ tấn công đã chiếm được quyền truy nhập vào hệ thống thông qua các chương trình cho phép đưa cạc giao tiếp mạng (Network Interface Card - NIC) vào chế độ nhận toàn bộ thông tin lưu truyền trên mạng hoặc cài các con rệp (Tjrojan) vào mạng như là một cổng cung cấp thông tin ra các mạng hoặc thùng thư điện tử bên ngoài..

**3. Giả mạo địa chỉ:** Việc giả mạo đia chỉ IP có thể được thực hiện thông qua việc sử dụng khả năng dẫn đường trực tiếp (source - routing). Với cách tấn công này, kẻ tấn công gửi các gói tin IP tới mạng bên trong một địa chỉ IP giả mạo, đồng thời chỉ rõ đường dẫn mà các gói tin IP phải gửi đi.

**4.Vô hiệu hoá các chức năng của hệ thống (denial of service):**

Vô hiệu hoá các chức năng của hệ thống là một kiểu tấn công nhằm làm tê liệt hệ thống không cho nó thực hiện các chức năng của nó. Đây là kiểu tấn công không thể ngăn chặn được vì những phương tiện tổ chức tấn công cũng chính là các phương tiện để làm việc và truy cập thông tin tên mạng.

**5.Tấn công vào yếu tố con người:**

Kẻ tấn công có thể liên lạc với người quản trị hệ thống, giả làm một người sử dụng để yêu cầu thay đổi mật khẩu, thay đổi quyền truy nhập của mình đối với hệ thống, hoặc thậm chí thay đổi một số cấu hình của hệ thống để thực hiện các phương pháp tấn công khác. Với kiểu tấn công này, không một thiết bị nào có thể ngăn chặn

một cách hữu hiệu, và chỉ có một cách giáo dục người sử dụng mạng nội bộ về những yêu cầu bảo mật để đề cao cảnh giác với những hiện tượng đáng nghi.

Dưới đây đề cập đến đến một số ác hình thức tấn công phá hoại điển hình trên mạng LAN và Internet:

**Tấn công kiểu từ chối dịch vụ - Denial of Service**

Hộp thư điện tử thường là mục tiêu chính của tấn công kiểu này. Tấn công được thực hiện bằng một chương trình gửi thư liên tục đến hộp thư cần phá hoại cho đến khi hộp thư không thể nhận thêm thư. Hiện nay, kiểu tấn công *DoS* thường nhằm vào các *Web Server* lớn với mục đích phá hoại dịch vụ cung cấp của Website. Virus Worm năm 1988 là một vụ tấn công đầu tiên của dạng *DoS*. Nó đã gây ra một vụ đình trệ tệ hại trên các mạng máy tính bằng cách gửi đi hàng triệu gói tin, chiếm băng thông của đường truyền và thiệt hại ước tính nhiều triệu USD.

Một biến thể khác của tấn công kiểu DoS là tấn công DoS kiểu phân tán (*Distributed Denial of Service - DDoS*). Kẻ tấn công sẽ dùng nhiều máy tính bên ngoài đồng loạt tấn công *DoS* gây ra tắc nghẽn trầm trọng và rất khó truy tìm thủ phạm. Ví dụ như vụ tấn công vào các site thương mại có tiếng như *Yahoo*, *Ebay* vào tháng 2 năm 2000 do một *hacker* người Canada, sử dụng nhiều máy chủ đồng thời truy cập. Để chống tấn công kiểu này, ngoài những biện pháp tự bảo vệ còn phải có sự cộng tác chung. Các chủ sở hữu những *server* mạnh cần quản lý *server* sao cho không để những *hacker* lợi dụng. Một số *firewall* cho phép đặt hữu hạn số lượng kết nối với các host trong mạng. Điều này làm giảm đáng kể khả năng tấn công.

Có thể nói, bất kỳ dịch vụ nào có sự truy cập của người sử dụng theo thời gian đều có thể trở thành mục tiêu của tấn công *DoS*.

**Chặn bắt gói tin (Network Packet Sniffing)**

Những chương trình chặn bắt gói tin có thể chặn lại một gói tin bất kỳ trong mạng và hiển thị nội dung của gói tin một cách dễ đọc nhất. Hai đầu của kết nối có thể không thể biết được là gói tin của mình đã bị xem trộm. Đây là công cụ ưa thích của những người quản trị mạng dùng để kiểm tra mạng. Khi mạng nội bộ được kết nối vào Internet, một kẻ khả nghi bên ngoài dùng packet sniffer có thể dễ dàng chặn gói tin được gửi đến một máy nào đó trong mạng. Và dễ dàng nghe trộm thông tin.

**Giả mạo địa chỉ IP**

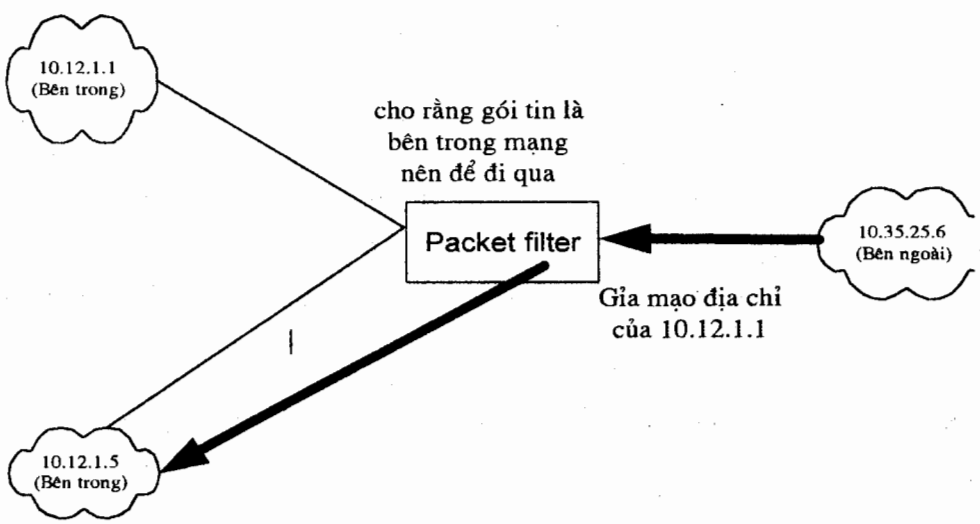
Một phương thức thường được sử dụng khác là giả mạo địa chỉ *IP*. Kẻ tấn công sử dụng địa chỉ *IP* nào đó được tin là hợp lệ, không bị nghi ngờ. Bởi địa chỉ *IP* là duy nhất nhưng lại không phải là gắn với duy nhất một máy. Khi ai đó muốn đều có thể sử dụng *IP* mình thích mà không cần bất kỳ sự chứng thực nào. Như trong pha gửi thư theo giao thức *SMTP*, mục người gửi không có một hạn chế nào là phải dùng đúng tên thật của

máy gửi hay *IP* của địa chỉ nguồn. Giả mạo *IP* được sử dụng trong trường hợp mà *firewall* sử dụng một tập luật lọc gói tin dựa vào địa chỉ *IP*. Cho người dùng *X* đi qua mà không cho người dùng *Y* đi qua. Hay còn gọi là *Host-based filtering*. *Y* nếu muốn thì có thể giả mạo tên của *X* để vượt qua *firewall*. Vì thế không thể tin tưởng vào địa chỉ *IP* và chỉ nên dùng tại mức cơ bản của *firewall*.

Trong ví dụ hình 8.1 một hệ thống bên ngoài ghi lại địa chỉ *IP* của nó là *10.12.1.1*, giống như địa chỉ của một máy bên trong mạng. Nếu *firewall* sử dụng việc lọc gói tin chỉ dựa trên địa chỉ *IP* mà không nhìn vào đường truyền vật lý thì gói tin giả mạo vẫn có thể đi qua được *firewall*.

**Xáo trộn và phát lại thông tin**

Các thông tin truyền đi có thể bị chặn lại và bị thay đổi nội dung rồi mới được gửi đến cho bên nhận (*replay attack*). Tuy nhiên, việc này sẽ khó thực hiện đối với các mạng truyền quảng bá đến tất cả các máy trạm nhưng dễ dàng thực hiện trong mạng kiểu lưu trữ và chuyển tiếp. Ngoài ra, các thông tin bị chặn lại trên đường truyền còn có




**Hình 8.1 Tấn công GM địa chỉ**

thể được lưu trữ lại và gửi đi vào các thời điểm khác làm cho bên nhận có thể không nhận ra được sự thay đổi nhưng thực chất thông tin nhận được là hoàn toàn sai lệch. Việc mã hoá thông tin không thể chống lại kiểu tấn công này bởi việc truyền lại các thông tin có thể dùng là các thông tin lấy trộm được từ chính tài nguyên của hệ thống thậm chí đối với các kẻ phá hoại không mục đích chúng không cần hiểu hay dịch được các thông tin mà chúng thực hiện truyền lại.

**Một số phương pháp tấn công khác**

Hầu hết các phương pháp tấn công trên đều thực hiện do chính người sử dụng hệ thống, chúng lợi dụng quyền của người sử dụng thực hiện chương trình để tiến hành một trong các phá hoại như trên. Nếu các mức kiểm soát truy nhập thực hiện đúng và cơ chế kiểm tra chứng thực thâm nhập hệ thống ổn định thì các tấn công này sẽ rất khó thực hiện. Tuy nhiên vấn đề này thường rất khó đối với người quản trị hệ thống để đảm bảo rằng mọi cơ chế hoạt động đều luôn đúng như vậy.

Đối với những người sử dụng bất hợp pháp một phương cách đơn giản để thâm nhập vào hệ thống lấy thông tin đó là việc đoán mật khẩu hoặc sử dụng các chương trình dò mật khẩu của những người sử dụng đã biết hoặc lợi dụng các sơ hở của người sử dụng để lấy trộm được mật khẩu. Với kiểu tấn công này không một thiết bị nào có thể ngăn chặn một cách hữu hiệu, và chỉ có một cách giáo dục người sử dụng mạng nội bộ về những yêu cầu bảo mật để đề cao cảnh giác với những hiện tượng đáng nghi đồng thời yêu cầu người sử dụng biết chọn lựa một mật khẩu tốt với độ dài thích hợp. Nói chung yếu tố con người là một điểm yếu trong bất kỳ một hệ thống bảo vệ nào, và chỉ có sự giáo dục cộng với tinh thần hợp tác từ phía người sử dụng mới có thể nâng cao được độ an toàn của hệ thống bảo vệ.

Cùng với các phương thức lấy thông tin bằng truy nhập trực tiếp còn có một vài phương pháp tinh vi khác khá phổ biến đặc biệt đối với các hệ thống có đưa ra các dịch vụ truy nhập công cộng. Các phương pháp đó là:

*Sử dụng virus máy tính:*

Là một chương trình gắn vào chương trình hợp lệ khác và có khả năng lây lan nó vào các môi trường đích mỗi khi chương trình hợp lệ được chạy. Sau khi virus đã nhiễm vào hệ thống nó sẽ thực hiện phá hoại mỗi khi nó muốn thông thường là phá hoại theo thời gian định trước. Đúng như tên gọi của nó, một trong những hành động của virus đó là lây lan bản thân nó vào tất cả các chương trình mà nó tìm thấy trong môi trường hệ thống. Chúng chuyển từ máy này sang máy khác mỗi khi chương trình được sao chép bất kể qua mạng hay qua thiết bị lưu trữ vật lý.

*Sử dụng chương trình worm:*

Là chương trình lợi dụng điều kiện dễ dàng cho phép chạy các tiến trình từ xa trong hệ phân tán. Các điều kiện này có thể tồn tại một cách tình cờ hoặc có chủ ý. Một số các chương trình *Internet Worm* đã lợi dụng đặc tính kết hợp cả có chủ ý và tình cờ cho phép chạy chương trình từ xa trong hệ thống *BSD UNIX* để phá hoại hệ thống.

*Sử dụng chương trình trojan:*

Những chương trình đưa ra cho người sử dụng hệ thống sử dụng bề ngoài thực hiện một chức năng bình thường nhưng thực chất là thực hiện việc phá hoại ẩn sau đó. Một ví dụ khá phổ biến về loại chương trình này đó là 'spoof login' là chương trình bề

ngoài vẫn hiển thị các dòng lệnh yêu cầu người sử dụng nhập tên truy nhập và mật khẩu của hệ thống không khác gì bình thường nhưng thực chất nó thực hiện lưu trữ các giá trị đó vào một file trong hệ thống để sử dụng trái phép.

## 8.2 Các biện pháp bảo vệ và phòng ngừa

An toàn thông tin trên mạng là một công việc vô cùng khó khăn phức tạp do nhiều người sử dụng, phân tán về mặt địa lý và trong môi trường mạng phức tạp. Nó đòi hỏi phải sử dụng nhiều giải pháp khác nhau từ cơ bản đến phức tạp, tuỳ theo lượng thông tin cần bảo vệ và khả năng cho phép của từng hệ thống cụ thể .

### 8.2.1 Các chiến lược an toàn thông tin

Khi xây dựng các hệ thống bảo vệ, có một số nguyên tắc sau mà chúng ta phải tuân theo:

**Quyền hạn tối thiểu - Least Privilege**

Nguyên tắc nền tảng trong an toàn (không chỉ cho an toàn mạng) là quyền hạn tối thiểu (Least Privilege). Về cơ bản, nguyên tắc này là bất kỳ một đối tượng nào chỉ nên có những quyền hạn nhất định mà đối tượng đó cần phải có để thực hiện các nhiệm vụ của mình và chỉ như vậy. Quyền hạn tối thiểu là nguyên tắc quan trọng để hạn chế sự phô bày mà kẻ bên ngoài có thể tấn công và hạn chế sự phá huỷ do các vụ tấn công gây ra.

**Đơn giản:**

Việc đặt ra yêu cầu đơn giản cho hệ thống bảo vệ có hai lý do chính:

- Dễ hiểu : Khi một hệ thống thiết kế đơn giản ta dễ dàng hiểu được hệ thống có hoạt động như ta mong muốn không.
- Ít lỗi : Một hệ thống càng phức tạp càng chứa nhiều lỗi. Ngay cả khi hệ thống không có lỗi và không có các lỗ hổng bảo mật, thì hệ thống phức tạp cũng sẽ làm phức tạp quá trình phân tích và xử lý các vấn đề trong những tình huống không định trước.

Các hệ thống Firewall thường được xây dựng trên những hệ điều hành đã được sửa đổi, loại bỏ những chức năng không cần thiết, các công cụ trợ giúp người sử dụng, các công cụ phát triển. Một số Firewall còn loại bỏ hầu như toàn bộ các công cụ quản trị từ xa, tất cả các thao tác của người quản trị phải được thực hiện tại bàn giao tiếp người-máy (console).

**Bảo vệ theo chiều sâu** (Defense in depth):

Một nguyên tắc khác của an toàn là bảo vệ theo chiều sâu. Không nên chỉ phụ thuộc vào một chế độ an toàn dù nó có mạnh như thế nào. Ta nên lắp đặt nhiều cơ chế an toàn để chúng có thể hỗ trợ lẫn nhau. Một Firewall có rất nhiều lớp, nếu trường hợp lớp thứ nhất có vấn đề thì chúng ta sẽ được các lớp tiếp theo bảo vệ.

**Nút thắt - choke point:**

Một nút thắt buộc những kẻ tấn công phải đi qua một cửa khẩu hẹp mà chúng ta có thể kiểm soát và điều khiển được. Firewall là một cấu trúc nằm giữa hệ thống nội bộ và Internet như một nút thắt. Bất kỳ kẻ nào có ý định tấn công từ Internet đều phải đi qua cửa khẩu này, chúng ta có thể theo dõi và phản ứng lại chúng. Tuy nhiên một nút thắt sẽ trở nên vô dụng nếu có những con đường khác không đi qua nó. Không nhất thiết phải tấn công Firewall trong khi có rất nhiều đường dial-up không được bảo vệ.

**Đường nối yếu nhất - Weakest Link**

Những kẻ tấn công thông minh luôn tìm các điểm yếu nhất trong hệ thống để tấn công vào đó. Do đó, chúng ta cần nhận thức được điểm yếu nhất để có phương thức bảo vệ. Thông thường, chúng ta quan đến những kẻ tấn công từ mạng hơn là những kẻ tiếp cận hệ thống, bởi vậy an toàn về mặt vật lý được coi là điểm yếu nhất trong hệ thống của chúng ta.

**Hỏng an toàn - Fail safe stance**

Nguyên tắc của hỏng an toàn (Fail safe stance) là nếu hệ thống có hỏng thì nó nên hỏng theo một cách nào đó mà vẫn loại bỏ được sự truy nhập bất hợp pháp của những kẻ tấn công. Tất nhiên, điều này cũng ngăn trở việc truy nhập của người dùng hợp pháp cho đến khi hệ thống được khôi phục lại. Trong nguyên tắc này, có hai quy tắc cơ bản mà chúng ta có thể áp dụng cho các quyết định về biện pháp an toàn. Đó là :

- Mặc định từ chối (Default deny Stance): Chú trọng vào những gì chúng ta cho phép và ngăn cản tất cả những cái còn lại. Default deny Stance có chiều hướng chấp nhận theo quan điểm an toàn. Nó là một hệ thống an toàn nên những gì chúng ta không biết sẽ không thể tấn công chúng ta. Đây là lựa chọn của những người làm an toàn nhưng không hiển nhiên đối với người sử dụng.
- Mặc định cho phép (Default permit Stance): Chú trọng vào những gì chúng ta ngăn cấm và cho phép tất cả những cái còn lại. Hầu hết những người sử dụng và các nhà quản lý đều lựa chọn quy tắc này. Mọi thứ được cho phép bằng cách ngầm định còn các dịch vụ, hoạt động rắc rối cụ thể sẽ bị ngăn cản.

**Tính toàn cục**

Để đạt được hiệu quả cao, hầu hết các hệ thống an toàn đòi hỏi phải có tính toàn cục của các hệ thống cục bộ (hay cá nhân). Nếu một kẻ nào đó có thể dễ dàng bẻ gẫy một cơ chế an toàn thì chúng có thể thành công bằng cách tấn công hệ thống tự do của

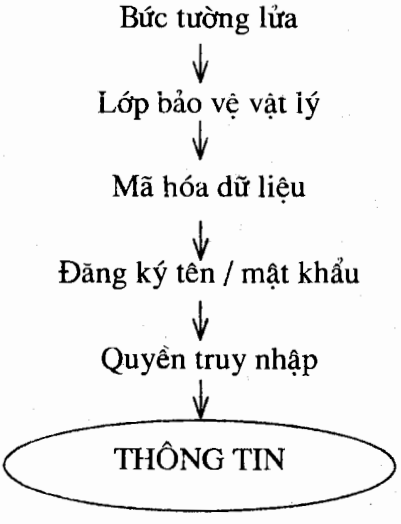
ai đó và sau đó tấn công hệ thống nội bộ từ bên trong. Có rất nhiều hình thức làm hỏng an toàn hệ thống và chúng ta cần được báo lại những hiện tượng là xảy ra có thể kiên quan đến an toàn của hệ thống cục bộ.

**Tính đa dạng của việc bảo vệ**

Sự đa dạng của các hệ thống mạng bên trong có thể tăng khả năng bảo vệ mạng. Nếu mạng bên trong bao gồm các hệ thống giống nhau, một lỗi chung trong hệ điều hành hoặc một trình ứng dụng có thể làm cho toàn bộ mạng bị tấn công theo cùng một phương pháp. Tuy nhiên, sự đa dạng trong mạng cùng đồng nghĩa với sự phức tạp khi quản lý các hệ thống khác nhau, đồng thời tăng chi phí trang bị phần cứng và phần mềm.

### 8.2.2 Các mức bảo vệ an toàn mạng

Vì không có một giải pháp bảo vệ mạng an toàn tuyệt đối nên người ta phải sử dụng đồng thời nhiều mức bảo vệ khác nhau tạo thành nhiều lớp rào chắn đối với các hoạt động xâm phạm . Việc bảo vệ thông tin trên mạng chủ yếu là bảo vệ thông tin cất giữ trong các máy tính , trong các máy chủ của mạng . Do đó ngoài một số biện pháp nhằm chống thất thoát thông tin trên đường truyền , ta phải xây dựng các mức " rào chắn " từ ngoài vào trong cho các hệ thống kết nối vào mạng . Mô hình như ở hình 8.2




**Hình 8.2 Các mức bảo vệ an toàn**

**Quyền truy nhập ( Access Right ):** Lớp bảo vệ này nhằm kiểm soát việc truy nhập tài nguyên mạng và quyền hạn trên tài nguyên đó . Cụ thể là việc quản lý được

tiến hành ở mức truy nhập tệp .Việc xác lập các quyền này được quyết định bởi người quản trị mạng (supervisor ).

**Đăng ký tên / mật khẩu :(login /password ):**

Mỗi người sử dụng muốn được vào sử dụng mạng đều phải đăng ký tên /mật khẩu .Nếu người ngoài không biết tên/mật khẩu thì không thể truy nhập vào mạng được .Nói chung phương pháp này đơn giản ,hiệu quả. Nhưng nếu không cẩn thận như ta đã trình bày ở phần trên để kẻ thâm nhập biết tên / mật khẩu thì có thể gây nguy hiểm. Phương pháp này không mấy hiệu quả với những kẻ quá hiểu biết về hệ thống.

**Mã hoá dữ liệu (data encryption ):**

Phương pháp này nhằm mục đích biến đổi dữ liệu từ dạng nhận thức được đến dạng không nhận thức được theo một thuật toán nào đó và sẽ được biến đổi ngược lại ở trạm nhập .

**Lớp bảo vệ vật lý ( Physical protection ):**

Lớp này nhằm ngăn cản các truy nhập vật lý bất hợp pháp vào hệ thống . Thường dùng các biện pháp như cấm tuyệt đối không cho người không có phận sự vào phòng máy ,dùng ổ khoá trên máy tính , khoá bàn phím , dùng các trạm không sử dụng ổ đĩa mềm hoặc các biện pháp dùng khoá cứng ...

**Bức tường lửa ( Firewall ) :**

Để bảo vệ an toàn và ngăn chặn từ xa một máy tính hay cả mạng nội bộ (intranet),người ta dùng hệ thống đặc biệt gọi là bức tường lửa .Đây là biện pháp tương đối phổ biến để bảo vệ các mạng nội bộ ,nó ngăn chặn các thâm nhập trái phép và thậm chí có thể "lọc"bỏ các gói tin mà không muốn gửi đi hoặc nhận vào vì những lý do nào đó .

**1. *Bức tường lửa***

Bức tường lửa là cổng chắn giữa mạng nội bộ với thế giới bên ngoài ( internet ) mục đích của bức tường lửa là tạo nên lớp vỏ bao quanh một mạng để bảo vệ các máy bên trong mạng , tránh các mối đe doạ khác nhau từ bên ngoài . cơ chế làm việc của bức tường lửa là dựa trên việc kiểm tra các gói dữ liệu IP lưu truyền giữa máy chủ và trạm làm việc .

Các mối đe doạ mà bức tường lửa có thể chống lại bao gồm :

- Chống lại các cuộc thâm nhập từ xa đến các nguồn thông tin khi không được phép .
- Từ chối các dịch vụ đưa thông tin vào mạng nội bộ với mục đích làm rối loạn hệ thống .
- Không cho phép thâm nhập ra ngoài khi cần thiết .
- Chống lại sự giả danh để thâm nhập mạng từ bên ngoài .

- Các thành phần thường gặp trong bức tường lửa là :
- Bộ định tuyến ( router ) với bộ lọc gói ( packet filtering )
- Pháo đài bảo vệ ( pháo đài bảo vệ ) để cung cấp cơ chế an toàn cho phép thâm nhập ra ngoài .
- Các phần mềm quản lý an ninh chạy trên máy chủ bảo vệ như hệ quản lý xác thực (authentication ), cấp quyền(authorization ) và kế toán (accounting).

**Bộ lọc gói tin ( packet filtering )**

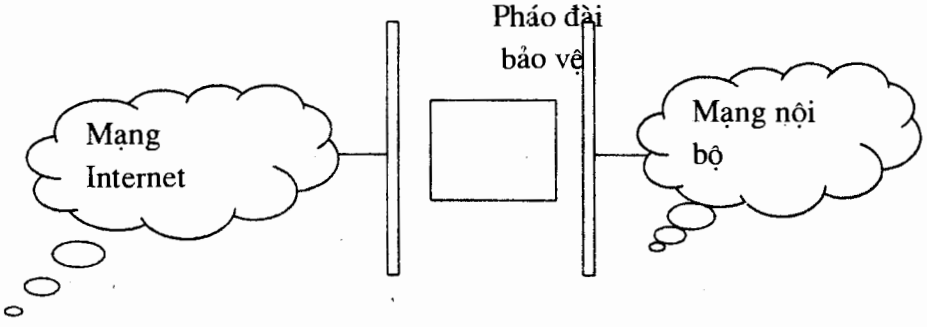
Nó cho phép hay ngăn cấm các gói tin khi chúng chuyển từ mạng này đến mạng khác . trong bộ lọc gói tin ta phải cài đặt một tập các qui tắc chỉ định gói tin loại nào sẽ được phép ( đi qua ) và loại bị ngăn cấm ( không cho đi qua ) . Bộ lọc gói tin có thể cài đặt trên một bộ định tuyến ( router ) hay trên một máy chủ. Mỗi gói tin chứa đựng những thông tin :

- Địa chỉ nguồn IP , địa chỉ đích IP
- Giao thức sử dụng TCP/ UDP
- Cổng nguồn của TCP/ UDP, cổng đích của TCP/ UDP

Ngoài ra Router biết được giao diện mà gói tin đến và giao diện nào mà router phải định hướng gói tin đi . Thực tế các server cung cấp các dịch vụ internet tại một vị trí nhất định cho phép router khoá hay mở đối với các loại kết nối bằng cách chỉ định số cổng thích hợp ( ví dụ TCP cổng 23 cho các kết nối Telnet , trong bộ qui tắc được chỉ định cho Packet filtering .

**Pháo đài bảo vệ ( Bastionhost ):**

Việc hạn chế gói tin đi vào mạng nội bộ của bộ lọc gói tin cũng làm việc hạn chế việc thâm nhập các dịch vụ Internet của các máy trong mạng nội bộ . Lúc này cần có cơ chế an toàn cho phép thâm nhập dịch vụ bên ngoài, đó là *pháo đài bảo vệ*. Hình 8.3




**Hình 8.3 Pháo đài bảo vệ**

Để cho phép thâm nhập bức tường lửa phải có hai lớp rào chắn. Rào chắn phía ngoài ngăn các gói tin đi vào trừ các gói tin được phép đi vào *pháo đài bảo vệ* và các gói tin cho clients ở trên *pháo đài bảo vệ* . Rào chắn phía trong ngăn cản các gói tin đi ra , trừ các gói tin từ pháo đài bảo vệ .

Có hai cách để người sử dụng chạy phần mềm client trên pháo đài bảo vệ :

- Cách thứ nhất : người sử dụng dùng dịch vụ từ xa ( Telnet ) để tiếp xúc với *pháo đài bảo vệ* rồi từ bộ phiên dịch lệch ( commad interpreter ) chạy phần mềm client . Cách này kinh tế và an toàn , nhưng cần cơ chế phụ để chuyển tin vào từ *pháo đài bảo vệ* về máy tính và người sử dụng.
- Cách thứ hai: Có sự biến đổi phần mềm client để chạy trên máy người sử dụng và nó phải tự động tiếp xúc với *pháo đài bảo vệ*.

Với cách này thì người sử dụng không cần tài khoản trên *pháo đài bảo vệ*, không cần Login trước khi thâm nhập Sever ở xa và không cần biết cú pháp của bộ dịch lệnh trên *pháo đài bảo vệ*. Bất lợi và tốn kém ,mỗi máy tính người sử dụng cần một chương trình client đặc biệt cho mỗi dịch vụ và *pháo đài bảo vệ* cần phần mềm đặc biệt để truyền tin máy tính người sử dụng cũng như Server trên Internet

*Pháo đài bảo vệ* phải được bảo mật cao để giảm đến mức thấp nhất các tổn thương do kẻ tấn công gây ra. Thường nó lộ trên Internet và là điểm kết nối chính cho người sử dụng toàn mạng nội bộ tới Internet và cũng là nơi đối mặt chính của bức tường lửa với những kẻ tấn công vì vậy nó thường được cài đặt nhiều chế độ bảo vệ khác nhau như độ lọc gói, dịch vụ uỷ quyền (proxyservices)

**Những mối đe doạ Firewall không thể chống lại :**

Virus và các chương trình Trojan horse: Firewall không thể chống lại các virus hoặc các chương trình kiểu *trojan horse*. Hiển nhiên thấy rằng các *virus* có thể tràn lan mà không đếm xỉa gì đến việc có sử dụng *firewall* hay không. Một *firewall* không thể biết được (không cần thiết) biết bên trong gói tin có nội dung như thế nào. Việc chống lại *virus* là do ý thức của người sử dụng, có tuân thủ những quy tắc tối thiểu cho việc chống virus hay không.

Tấn công từ bên trong: Vai trò chính của *firewall* là chặn thông tin từ bên ngoài đi tới. Với việc tấn công từ bên trong, việc phát hiện ra và ngăn chặn không phải là điều dễ dàng. Chỉ trong trường hợp mạng được chia càng nhỏ, sự tấn công giữa các bộ phận vì thế có thể giảm xuống. Một điều hiển nhiên là những sự tấn công từ bên trong thường gây thiệt hại nghiêm trọng hơn rất nhiều và khó phát hiện hơn các tấn công từ bên ngoài. Đây là vấn đề tin cậy nội bộ.

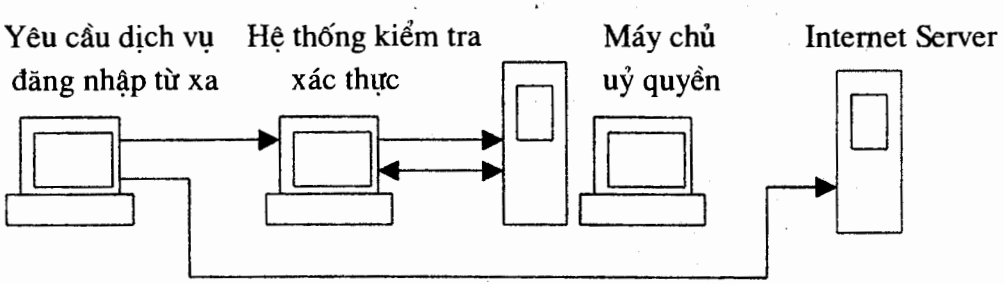
Có thể nói *firewall* bảo vệ được rất nhiều nhưng không phải là tất cả. Một sự an ninh tin cậy chỉ có được khi kết hợp *firewall* với nhiều yếu tố khác, đặc biệt là ý thức

bảo vệ của bản thân người sử dụng hệ thống. Không nên cho rằng, khi cài đặt thành công một *firewall* là mạng máy tính đã hoàn toàn yên ổn. Điều này cũng giống như khi ta tin rằng chỉ cần người bảo vệ là có thể tránh khỏi mọi vụ trộm trong toà nhà.

**2. Dịch vụ uỷ quyền (proxy services):**

Để an toàn, tránh tự do truy nhập giữa Internet và các máy chủ của mạng nọi bộ, ta cung cấp một máy chủ đơn truy nhập Internet cho tất cả mọi người sử dụng.Tuy nhiên, đây không phải là giải pháp tốt nhất, bởi vì máy chủ đó "không rõ ràng " với người sử dụng và không thể đảm bảo an toàn cho một máy với nhiều người sử dụng, đặc biệt đối với những người sử dụng muốn truy nhập thông tin từ xa.

Ví dụ một dịch vụ Proxy trên cổng ứng dụng (Application Gateway):




**Hình 8.4 Dịch vụ Proxy**

Với Proxy người sử dụng nghĩ là tương tác trức tiếp với các dịch vụ Internet. Proxy cho phép người sử dụng muốn truy nhập Internet từ chính hệ thống của họ, chúng cũng không cho phép các gói tin ngang qua trực tiếp giữa Internet và hệ thống người sử dụng. Các hệ thống Proxy cũng không ngăn ngừa người sử dụng làm mất tác dụng và không an toàn của máy chủ bảo vệ vì bây giờ máy uỷ quyền tự động tương tác với máy chủ bảo vệ thay vì người sử dụng giao dịch trực tiếp với máy chủ bảo vệ. Cơ chế lọc của bộ lọc gói tin phối hợp kiểm soát với cơ chế "uỷ quyền " cung cấp một khả năng an toàn và uyển chuyển

Hệ thống mạng có chức năng lọc gói tin, ngăn các kết nối bằng Telnet vào hệ chỉ trừ một chủ duy nhất –TELNET- muốn kết nối vào hệ thống phải được thực hiện các bước sau:

- Thực hiện dịch vụ đăng nhập từ xa tới cổng ứng dụng Telnet, rồi cho biết tên của máy chủ bên trong cần truy cập.
- Gateway kiểm tra địa chỉ IP nơi xuất phát của người truy cập rồi cho phép hoặc từ chối tuỳ theo chế độ an ninh của hệ thống .

- Người truy cập phải vượt qua được hệ thống kiểm tra xác thực.
- Proxy Services tạo một kết nối giữa cổng truyền (Gateway) và máy chủ cần truy cập rồi liên kết lưu thông giữa người truy cập và máy chủ trên Internet.

# TÀI LIỆU THAM KHẢO

[1] Nguyễn Thúc Hải. ***Mạng máy tính và các hệ thống mở***. NXB giáo dục. 1997.

[2] Nguyễn Gia Hiểu. ***Mạng máy tính***. NXB thống kê.1999.

[3] Vũ Hồng Giang. ***Một phương pháp phân tích mạng máy tính***. Tạp chí bưu chính viễn thông- các công trình nghiên cứu- triển khai công nghệ thông tin và viễn thông. 12/1999.

[4] Nguyễn Tiến, Đặng Xuân Hường, Nguyễn Văn Hoài. ***Giáo trình căn bản về mạng***. NXB Giáo dục. 1999.

[5] Bohdan O. Szuprowicz. ***Multimedia Networking***. McGraw- Hill, Inc.

[6] Thomas Case, Laray Smith. ***Managing Local Area Networks***. McGraw- Hill. 1995A.

[7] Michael Duck, Peter Bishop, Richard Read. ***Data Communication for Engineers***. Addison Wesley Longman. 1996.

[8] Warwick Ford. ***Computer Communications Security***. Prentice-Hall, Inc. 1994.

[9] Fred Halsall. ***Data Communications, Computer Networks and Open Systems***. Addison-Wesley Publishing Company. Fourth Edition. 1996.

[10] Gil Held, Ray sarch. ***Data communications***. Third Edition. McGraw - Hill, Inc. 1995. 371-398.

[11] Warren Hioki. ***Telecommunications***. Prentice-Hall, Inc. Second Edition. 1995. 272-275, 297-325.

[12] Robertazzi Thomas G. ***Computer Networks and Systems***- queueing theory and performance evaluation. Springer- Verlag. 1995.

[13] David A. Stamper. ***Local area Networks***. Addison Wesley Longman, Inc. Second Edition. 1997.

[14] William Stallings. ***Data and Computer Communications***- USA. Prentice- Hall. Inc. 1997.

[15] William Stallings. ***Local Networks***. Macmilan Publishing Company, a division of Macmillan. Inc. 1987.

# Mục lục


**CHƯƠNG 1 - GIỚI THIỆU CHUNG ---- 7**

1.1 MẠNG TRUYỀN THÔNG VÀ CÔNG NGHỆ MẠNG ---- 7
1.1.1 Giới thiệu chung ---- 7
1.1.2 Mạng máy tính ---- 9
1.1.3. Phân loại mạng máy tính ---- 13
1.1.4 Địa chỉ mạng, định tuyến, tính tin cậy, tính liên tác và an ninh mạng ---- 23
1.1.5 Chuẩn mạng ---- 25
1.2 MÔ HÌNH OSI ---- 26
1.2.1 Mô hình ---- 27
1.2.2 Chức năng các tầng ---- 32
1.2.3 Bộ giao thức TCP/IP – Mô hình Internet ---- 43
1.3 PHƯƠNG PHÁP TIẾP CẬN ---- 44

**CHƯƠNG 2 - TẦNG ỨNG DỤNG ---- 45**

2.1 GIAO THỨC TẦNG ỨNG DỤNG ---- 45
2.1.1 Giao thức tầng ứng dụng ---- 46
2.1.2 Các yêu cầu của ứng dụng ---- 51
2.1.3 Dịch vụ của các giao thức giao vận Internet ---- 53
2.1.4 Một số ứng dụng phổ biến ---- 56
2. 2 WORLD WIDE WEB: HTTP ---- 57
2.2.1 Tổng quan về HTTP ---- 58
2.2.2 Kết nối liên tục và không liên tục (persistent / nonpersistent) ---- 61
2.2.3 Khuôn dạng thông điệp HTTP ---- 63
2.2.4 Tương tác giữa người dùng Hrver-server ---- 67
2.2.5 GET có điều kiện (Conditional GET) ---- 69
2.2.6 Web cache ---- 71
2.2.7 Web động ---- 73
2.3 TRUYỀN FILE (FILE TRANSFER) FTP ---- 82
2.3.1 Các lệnh FTP (FTP Commands) ---- 84
2.4 - THƯ TÍN ĐIỆN TỬ (E-mail) TRÊN INTERNET ---- 85
2.4.1 SMTP ---- 87

2.4.2 So sánh SMTP với HTTP ---- 90
2.4.3 Khuôn dạng thư và chuẩn MIME ---- 91
2.4.4 Giao thức truy nhập mail. ---- 97
2. 5 DỊCH VỤ TÊN MIỀN - DNS. ---- 102
2.5.1 Các dịch vụ của DNS ---- 103
2.5.2 Cơ chế hoạt động của DNS ---- 105
2.5.3 Bản ghi DNS ---- 112
2.5.4 Thông điệp DNS ---- 113
2.6 CÁC ỨNG DỤNG THEO KIẾN TRÚC NGANG HÀNG ---- 115
2.6.1 Nhắn tin tức thì ---- 117
2.6.6. Kiến trúc Hệ thống MSN. ---- 121
2.6.3 Kiến trúc chia sẻ file ngang hàng Gnutella ---- 128
2.7 LẬP TRÌNH SOCKET ---- 134
2.7.1 Các hàm thao tác trên Socket ---- 135
2.7.2 Ví dụ một chương trình client/server đơn giản ---- 138
2.7.3 Web server đơn giản ---- 140

**CHƯƠNG 3 - TẦNG GIAO VẬN ---- 148**

3.1 DỊCH VỤ VÀ NGUYÊN TẮC CỦA TẦNG GIAO VẬN ---- 148
3.1.1 Quan hệ giữa tầng giao vận và tầng mạng ---- 150
3.1.2 Tổng quan về tầng giao vận trong Internet. ---- 152
3.2 DỊCH VỤ DỒN KÊNH, PHÂN KÊNH ---- 153
3.3 UDP – GIAO THỨC KHÔNG HƯỚNG NỐI ---- 158
3.3.1 Cấu trúc UDP segment ---- 162
3.3.2 UDP checksum ---- 162
3.4 CÁC NGUYÊN TẮC TRUYỀN DỮ LIỆU TIN CẬY ---- 164
3.4.1 Xây dựng giao thức truyền dữ liệu tin cậy ---- 165
3.4.2 Giao thức truyền dữ liệu tin cậy liên tục (Pipeline) ---- 175
3.4.3 Go-back-N (GBN) ---- 178
3.4.4 Giao thức lặp lại có lựa chọn (Selective Repeat) ---- 184
3.5 TCP – GIAO THỨC GIAO VẬN HƯỚNG NỐI ---- 189
3.5.1 Kết nối TCP ---- 190
3.5.2 Cấu trúc TCP Segment ---- 193
3.5.3 Số thứ tự và Số biên nhận ---- 195
3.5.4 Telnet: Một ví dụ về số thứ tự và số biên nhận ---- 196
3.5.5 Truyền dữ liệu tin cậy ---- 199



3.5.6 Kiểm soát lưu lượng ---- 205
3.5.7 Quản lý kết nối TCP ---- 207
3.6 KIỂM SOÁT TẮC NGHẼN TRONG TCP ---- 211

**CHƯƠNG 4 - TẦNG MẠNG ---- 216**

4.1 CÁC MÔ HÌNH DỊCH VỤ CỦA TẦNG MẠNG ---- 216
4.1.1 Mô hình dịch vụ mạng ---- 218
4.1.2 Nguồn gốc của dịch vụ chuyển mạch gói và chuyển mạch ảo. ---- 223
4.2 CÁC NGUYÊN LÝ ĐỊNH TUYẾN ---- 224
4.2.1. Thuật toán định tuyến link state. ---- 227
4.2.2. Thuật toán Distance vector. ---- 231
4.3 ĐỊNH TUYẾN PHÂN CẤP ---- 236
4.4 INTERNET PTOTOCOL ---- 238
4.4.1 Địa chỉ IPv4 ---- 240
4.4.2 Chuyển datagram từ nguồn tới đích: vấn đề địa chỉ và định tuyến ---- 248
4.4.3 Khuôn dạng gói dữ liệu IP ---- 251
4.4.4 Phân mảnh (Fragmentation) và Hợp nhất (Reassembly) gói tin IP ---- 254
4.4.5 Giao thức kiểm soát lỗi ICMP (Internet Control Message Protocol) ---- 258
4.5 ĐỊNH TUYẾN TRÊN INTERNET ---- 259
4.5.1 Định tuyến trong một miền (Intra-AS routing) (Định tuyến nội miền) ---- 260
4.5.2 Định tuyến giữa các miền (Inter-AS routing) (Định tuyến liên miền) ---- 264
4.6 CẤU TẠO CỦA THIẾT BỊ ĐỊNH TUYẾN (ROUTER) ---- 264
4.6.1 Cổng vào (Input port) ---- 266
4.6.2 Kết cấu chuyển (Switching fabric) ---- 268
4.6.3 Cổng ra (Output port) ---- 270
4.6.4 Hàng đợi ở router ---- 270
4.7 IPv6 ---- 273
4.7.1 Định dạng gói tin IPv6 ---- 273
4.7.2 Chuyển từ IPv4 sang IPv6 ---- 276
4.8 CƠ CHẾ DỊCH CHUYỂN ĐỊA CHỈ (NAT) ---- 279
4.9 KIỂM SOÁT TẮC NGHẼN ---- 285
4.9.1 Các nguyên lý Kiểm soát tắc nghẽn. ---- 286
4.9.2 Chính sách ngăn chặn tắc nghẽn ---- 289
4.9.3 Kiểm soát tắc nghẽn trong mạch ảo ---- 290
4.9.4 Kiểm soát tắc nghẽn trong mạng chuyển mạch gói. ---- 292
4.9.5 Cắt tải ---- 293

CHƯƠNG 5 -TẦNG LIÊN KẾT DỮ LIỆU ----------295

5.1 CÁC KHÁI NIỆM CHUNG, DỊCH VỤ CỦA TẦNG DATALINK----------295
5.1.1 Những dịch vụ của tầng liên kết dữ liệu----------296
5.1.2 Bộ điều hợp (Adapter)----------300
5.2 KỸ THUẬT PHÁT HIỆN VÀ SỬA LỖI----------302
5.2.1 Kiểm tra tính chẵn lẻ----------304
5.2.2 Phương pháp tính tổng kiểm tra (checksum) ----------306
5.2.3 Kiểm tra dư thừa vòng (CRC)----------306
5.2.4 Sửa lỗi bằng mã Hamming ----------309
5.3. GIAO THỨC ĐA TRUY CẬP VÀ MẠNG CỤC BỘ----------313
5.3.1 Giao thức phân chia kênh truyền (channel partitioning) ----------317
5.3.2 Giao thức truy cập ngẫu nhiên (random access) ----------318
5.3.3 Giao thức truy cập lần lượt (Taking – turns) ----------326
5.3.4 Mạng cục bộ LAN (Local Area Network) ----------327
5.4 ĐỊA CHỈ LAN VÀ ARP ----------328
5.4.1 Địa chỉ LAN----------329
5.4.2. Giao thức giải mã địa chỉ (ARP)----------331
5.5. ETHERNET----------336
5.5.1 Những khái niệm cơ bản của Ethernet----------338
5.2.2 CSMA/CD: Giao thức đa truy cập của Ethernet----------342
5.5.3 Những công nghệ Ethernet ----------345
5.6 HUB, BRIDGE VÀ SWITCH----------349
5.6.1 Hub----------349
5.6.2 Bridge----------351
5.6.3. Switch----------360
5.8. MẠNG LAN KHÔNG DÂY ----------363
5.8.1 Giới thiệu chung----------363
5.8.2 Lớp giao thức IEEE 802.11----------366
5.8.3 Một số vấn đề hay gặp đối với mạng không dây----------369
5.9. PPP – GIAO THỨC ĐIỂM NỐI ĐIỂM ----------371
5.9.1 Khuôn dạng gói gữ liệu (Frame PPP)----------373
5.9.2 Giao thức điều khiển đường truyền PPP (LCP) và kiểm soát mạng ----------375
5.10 MẠNG RIÊNG ẢO (VPN)----------378
5.10.1 Các mạng riêng ảo truyền thống ----------378
5.10.2 Mô phỏng giả dây dẫn (Pseudowire Emulation Overview) ----------381
**TÀI LIỆU THAM KHẢO** ----------387

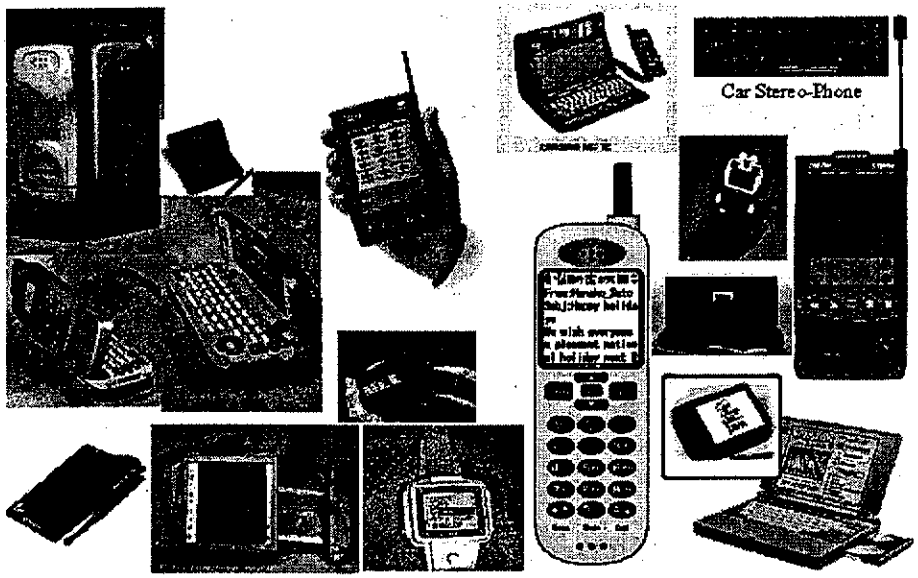


# Chương 1
# GIỚI THIỆU CHUNG

## 1.1 MẠNG TRUYỀN THÔNG VÀ CÔNG NGHỆ MẠNG

### 1.1.1 Giới thiệu chung

**Truyền thông máy tính (computer communications)** là quá trình truyền dữ liệu từ thiết bị này sang thiết bị khác. Trước đây chúng ta thường hiểu thiết bị là máy tính, nhưng ngày nay thiết bị (end-system, device) không chỉ đơn thuần là máy tính mà bao gồm nhiều chủng loại thiết bị khác, ví dụ điện thoại di động, máy tính PAM,... (Xem Hình 1.1). Số lượng các kiểu thiết bị có khả năng lấy thông tin từ Internet ngày càng tăng. Một từ phổ biến có nghĩa tương tự như vậy là truyền dữ liệu. Mặc dù hai cụm từ này có thể sử dụng thay thế cho nhau, một số người coi thuật ngữ dữ liệu (data) chỉ bao gồm những sự kiện đơn giản và thô (chưa được xử lý), và sử dụng thuật ngữ thông tin (information) để chỉ việc tổ chức những sự kiện này thành dạng thông tin có nghĩa đối với con người.




**Hình 1.1 Các thiết bị có khả năng kết nối Internet**

Khái niệm **mạng (networking)** chỉ khái niệm kết nối các thiết bị lại với nhau nhằm mục đích chia sẻ thông tin. Khái niệm mạng liên quan đến nhiều vấn đề, bao gồm:

**Giao thức truyền thông (protocol)**: mô tả những nguyên tắc mà tất cả các thành phần mạng cần tuân thủ để có thể trao đổi được với nhau;

**Topo (mô hình ghép nối mạng/hình trạng mạng)**: mô tả cách thức nối các thiết bị với nhau.

**Địa chỉ**: mô tả cách thức định vị một đối tượng trên mạng.

**Định tuyến (routing)**: mô tả cách thức dữ liệu truyền từ thiết bị này sang thiết bị khác trên mạng.

**Tính tin cậy (reliability)**: giải quyết tính toàn vẹn của dữ liệu, đảm bảo dữ liệu nhận được chính xác như dữ liệu gửi đi.

**Khả năng liên tác (interoperability)**: chỉ mức độ các sản phẩm phần mềm và phần cứng của các hãng sản xuất khác nhau có thể làm việc cùng nhau.



**An ninh (security)**: đảm bảo an toàn hoặc bảo vệ tất cả các thành phần của mạng.

**Chuẩn (standard)**: thiết lập các quy tắc và luật lệ cụ thể cần phải tuân theo.

Trên thực tế, khái niệm mạng xuất hiện ở nhiều kiểu ứng dụng khác nhau. Ví dụ, trong công nghiệp giải trí, các công ty truyền thanh, truyền hình, và công ty cáp đều có những mạng độc lập riêng của mình với nhiều trạm phát. Thông qua những mạng này, các chương trình tin tức, thể thao, điện ảnh, phim truyện... được dùng chung giữa các trạm phát. Mạng truyền thông ra đời sớm nhất và phổ biến nhất là mạng điện thoại. Khi nói đến mạng điện thoại, người ta muốn nhắc đến hệ thống điện thoại kiểu cũ (plain old telephone system - POTS) hoặc mạng điện thoại chuyển mạch công cộng (PSTN – public switched telephone network). Mạng PSTN mô tả hệ thống điện thoại truyền thống dựa trên tín hiệu tương tự được sử dụng để truyền tiếng nói. Một mạng truyền thông khá quen thuộc ngày nay là mạng máy tính Internet - là một tập hợp các mạng, hay mạng mạng.

## 1.1.2 Mạng máy tính

Mạng bao gồm nhiều thành phần, các thành phần được nối với nhau theo một cách thức nào đó và cùng sử dụng chung một ngôn ngữ:

Các thiết bị đầu cuối (end system) kết nối với nhau tạo thành mạng có thể là các máy tính (computer) hoặc các thiết bị khác. Ngày càng có nhiều loại thiết bị có khả năng kết nối vào mạng máy tính như điện thoại di động, PDA, ti vi...

Môi trường truyền (media) thực hiện việc truyền dẫn các tín hiệu vật lý. Môi trường truyền có thể là các loại dây dẫn (cáp), sóng (đối với các mạng không dây).

Giao thức (protocol) là quy tắc quy định cách thức trao đổi dữ liệu giữa các thực thể.

Nói chung, ba khái niệm trên đưa đến một định nghĩa chuẩn về mạng máy tính như sau:

Mạng máy tính là tập hợp các máy tính và các thiết bị phụ trợ khác sử dụng chung một nhóm giao thức để chia sẻ tài nguyên thông qua các phương tiện truyền thông mạng.

### Các thành phần mạng: thiết bị, nút, máy tính

Theo nghĩa chung nhất, thuật ngữ **thiết bị** (device) chỉ bất cứ một thực thể phần cứng nào, chẳng hạn các thiết bị đầu cuối, máy in, máy tính, hoặc một thiết bị phần cứng đặc biệt liên quan đến mạng, ví dụ máy chủ (server), repeater (bộ lặp), bridge (cầu), switch, router (bộ định tuyến), và rất nhiều thiết bị đặc biệt khác. Tất cả các kiểu thiết bị này sẽ được thảo luận chi tiết ở các chương sau.

Nói chung có nhiều phương pháp gán cho thiết bị mạng một định danh duy nhất, thường thì thiết bị được chính hãng sản xuất gắn một số nhận dạng duy nhất. Việc này tương tự như việc in số seri trên tivi hoặc các đồ dùng điện tử khác. Ví dụ mỗi card Ethernet được hãng sản xuất gán cho một địa chỉ duy nhất - địa chỉ này không trùng với bất kỳ card Ethernet nào khác.

Khi mô tả các thành phần mạng, cần phân biệt giữa khái niệm thiết bị (device) và máy tính (computer). Nếu xét ở khía cạnh thiết bị máy tính thường được gọi là host (hoặc server) hay trạm làm việc (workstation) (cũng còn được gọi là desktop hay client). Thuật ngữ này thường dùng để chỉ những hệ thống máy tính có cài đặt hệ điều hành riêng của mình (ví dụ Windows, UNIX). Vì vậy workstation có thể là máy tính cá nhân như máy Apple Macintosh, hoặc bất cứ máy tính họ Intel nào (thường được gọi là IBM-PC); cũng có thể là một workstation đồ họa (ví dụ các workstation đồ họa được sản xuất bởi Sun Microsystems, Silicon Graphics, IBM, Hewlett-Packard, Compaq Computer Corporation), một superminicomputer như Compaq's VAX hay một hệ thống IBM AS/400, một super-microcomputer như Compaq's Alpha; hoặc có thể là một máy tính lớn (mainframe) như IBM ES-9000.

### Phương tiện và các giao thức truyền thông mạng

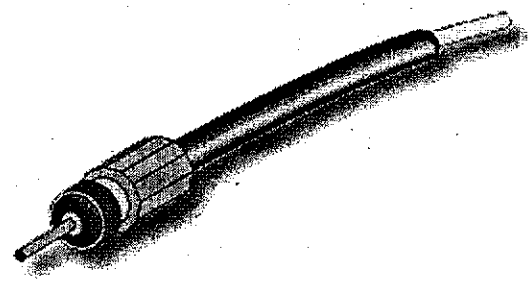
Để chia sẻ thông tin và sử dụng dịch vụ trên mạng, các thành phần của mạng phải có khả năng truyền thông được với nhau. Để đáp ứng được yêu cầu này, chúng ta phải xét tới hai tiêu chí cụ thể của mạng: khả năng



liên kết (connectivity) và ngôn ngữ (language). Khả năng liên kết chỉ đường truyền hoặc kết nối vật lý giữa các thành phần; ngôn ngữ chỉ một bảng từ vựng cùng các quy tắc truyền thông mà các thành phần phải tuân thủ.

### Phương tiện truyền thông (media)

Môi trường vật lý sử dụng để kết nối các thành phần của mạng thường được gọi là môi trường truyền thông (medium, media). Môi trường truyền thông mạng được chia thành hai loại: cáp (cable) và không dây (wireless). Ví dụ, cáp truyền thông có thể là cáp xoắn đôi (twisted-pair), cáp đồng trục (coaxial), và cáp sợi quang (fiber-optic cable)... Truyền thông không dây có thể là sóng radio (gồm sóng cực ngắn hay việc truyền thông qua vệ tinh), bức xạ hồng ngoại. Các môi trường truyền thông mạng được thảo luận chi tiết trong chương 5.



**Hình 1.2 Môi trường truyền: Sợi cáp quang**

**Giao thức (Protocols).** Ngôn ngữ được sử dụng bởi các thực thể mạng gọi là giao thức truyền thông mạng. Các bên truyền thông "hiểu nhau" do giao thức định nghĩa một ngôn ngữ chung giữa các thành phần mạng. Từ ý nghĩa khái quát này có thể hiểu giao thức truyền thông mạng là các thủ tục, quy tắc hoặc các đặc tả chính thức đã được chấp nhận nhằm xác định hành vi và ngôn ngữ trao đổi giữa các bên. Nói chung trong cuộc sống hàng ngày, chúng ta cũng áp dụng những quy tắc nào đó. Ví dụ, khi đi đến những nơi đòi hỏi tính trang trọng, mọi người phải tuân theo những nghi thức đặc biệt về ăn mặc (ví dụ nam giới phải mặc áo vét có thắt caravat). Nhưng khi đến các quán ăn bình dân thì không cần ăn mặc trang trọng như vậy. Trong mạng và truyền thông máy tính, giao thức mạng là bản đặc tả chính thức quy định cách thức "xử sự" của các thực thể tham gia truyền thông. Ở đây khái

niệm thực thể bao gồm cả thiết bị phần cứng cũng như tiến trình phần mềm. Giao thức mạng cũng định nghĩa khuôn dạng dữ liệu được trao đổi giữa các bên. Nói một cách ngắn gọn, giao thức mạng định nghĩa bảng từ vựng và các quy tắc áp dụng truyền thông dữ liệu.

Không có môi trường truyền, không thể trao đổi thông tin giữa các thực thể mạng; không có ngôn ngữ chung, không thể hiểu được nhau. Vì vậy, đường truyền cung cấp môi trường để thực hiện truyền thông, trong khi đó ngôn ngữ chung đảm bảo hai bên truyền thông hiểu được nhau. Điều này cũng giống như cuộc nói chuyện điện thoại giữa một người chỉ nói được tiếng Ý với một người chỉ nói được tiếng Nga. Nếu không có đường điện thoại (đường truyền mạng) cho cuộc nói chuyện thì hai người không thể nói chuyện được với nhau (không thể trao đổi dữ liệu). Đã có đường điện thoại rồi, lúc này hai người có thể nói và nghe thấy giọng nói của nhau (truyền dữ liệu được thực hiện) nhưng họ không giao tiếp được với nhau vì không ai trong số họ hiểu được ngôn ngữ của người kia - họ nói chuyện bằng hai thứ tiếng khác nhau.

Ví dụ TCP/IP là một giao thức mạng quen thuộc - một trong những giao thức của bộ giao thức TCP/IP (Transmission Control Protocol/Internet Protocol) TCP/IP được coi là xương sống của Internet. Tuy tên gọi TCP/IP chỉ gồm hai giao thức cụ thể là TCP và IP nhưng thường được sử dụng để chỉ nhóm gồm nhiều giao thức khác ngoài TCP và IP. Tập hợp các giao thức này được gọi là bộ giao thức TCP/IP. Có thể kể đến một số giao thức trong bộ giao thức TCP/IP như FTP (Transfer Protocol) định nghĩa cách chuyển file; HTTP (the Hypertext Transport Protocol) được dùng cho World Wide Web (WWW), định nghĩa cách các server cần phải truyền các tài liệu (trang Web) tới các client (Web browser) như thế nào. Ngoài ra cũng phải kể đến ba giao thức được sử dụng cho thư điện tử (email) là Post Office Protocol (POP), Simple Mail Transfer Protocol (SMTP) và Internet Mail Access Protocol (IMAP). Ngày nay các mạng sử dụng rất nhiều giao thức khác nhau từ đơn giản đến phức tạp. Có thể nói các giao thức là "keo dán" ràng buộc mạng máy tính lại với nhau bởi vì chúng định nghĩa cách thực hiện các hoạt động cụ thể.

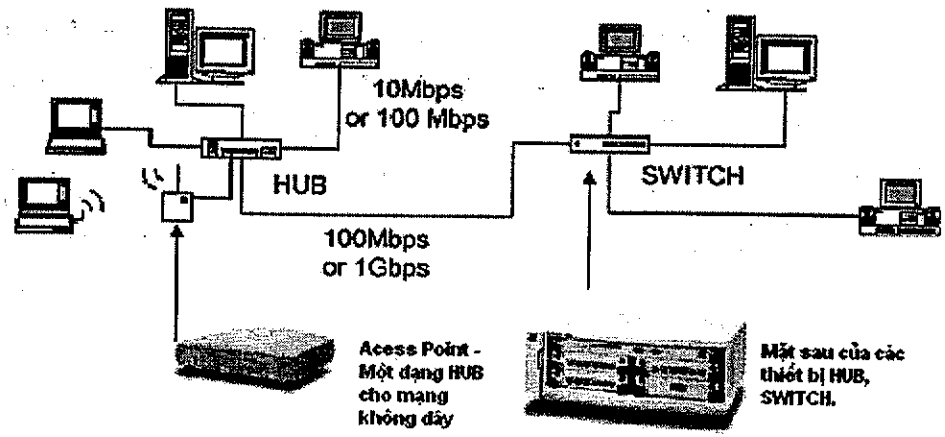
Một số bộ giao thức khác có thể kể đến là **AppleTalk** - bộ giao thức mạng của công ty Apple Computer, đầu tiên chỉ sử dụng cho các máy tính



Macintosh, không thể phục vụ cho các hệ điều hành khác; bộ giao thức của Hệ điều hành **Windows 2000** của Microsoft; **DECnet** của Digital Equipment Corporation (hiện giờ là Compad) - sử dụng giao thức mạng Digital Network Architecture (DNA). DECnet được thiết kế cho các máy VAX hoặc Alpha chạy dưới hệ điều hành Open-VMS, hoặc cho các hệ thống DEC dùng hệ điều hành DEC trước đây, ví dụ như RSX-11M, RT-11, RSTS/E cũng như một số hệ điều hành phổ biến khác như MS-DOS, Windows, và một vài biến thể của Unix. Mạng máy tính đôi khi cũng được đặt tên theo giao thức chúng dùng. Ví dụ, một mạng gồm các thiết bị hỗ trợ Apple Talk thường được gọi là một mạng Apple Talk. Tương tự, mạng TCP/IP là mạng của các thiết bị được liên kết với nhau và sử dụng bộ giao thức TCP/IP để truyền thông.

## 1.1.3. Phân loại mạng máy tính

Có rất nhiều kiểu mạng máy tính khác nhau. Việc phân loại chúng thường dựa trên các đặc điểm chung. Ví dụ, mạng máy tính thường được phân loại theo vùng địa lý (diện hoạt động) (ví dụ: mạng cục bộ, mạng diện rộng,...); theo topo (mô hình ghép nối mạng) (ví dụ: điểm-điểm (point-to-point) hay broadcast); hoặc theo kiểu đường truyền thông mà mạng sử dụng và cách chuyển dữ liệu đi (ví dụ mạng chuyển mạch ảo, hay chuyển mạch gói).




Hình 1.3 Một mạng LAN đơn giản

***Phân loại mạng theo diện hoạt động***

Nếu phân loại theo diện hoạt động, mạng máy tính có thể được phân chia thành:

Mạng cục bộ (Local Area Network - LAN);

Mạng diện rộng (Wide Area network - WAN);

Mạng đô thị (Metropolitan Area network - MAN);

Mạng toàn cầu (Global Area network - GAN);

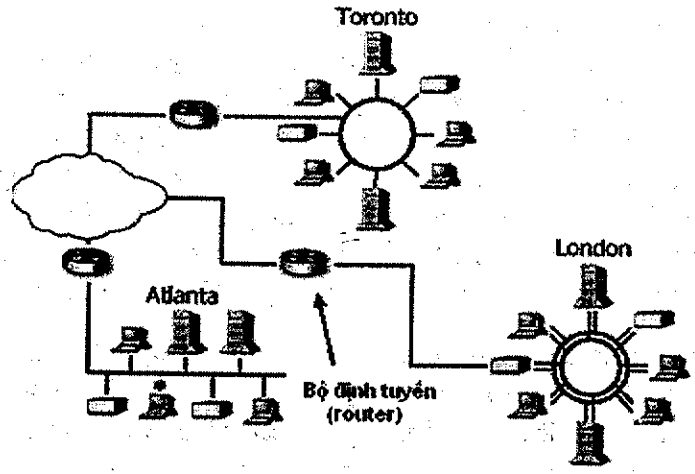
Mạng cá nhân (Personal Area network - PAN);

Mạng lưu trữ (Storage Area Network - SAN).

***Mạng cục bộ (LAN)*** liên kết các tài nguyên máy tính trong một vùng địa lý có kích thước hạn chế. Đó có thể là một phòng, vài phòng trong một tòa nhà, hoặc vài tòa nhà trong một khu nhà. Cụm từ "kích thước hạn chế" không được xác định cụ thể nên một số người xác định phạm vi của mạng LAN bằng cách định bán kính nằm trong khoảng vài chục mét đến vài km. IEEE (Institute of Electrical and Electronics Engineers) xác định bán kính của mạng LAN nhỏ hơn 10km. Ví dụ về một số công nghệ mạng LAN: Ethernet/802.3, Token Ring, mạng FDDI (Fiber Distributed Data Interface).

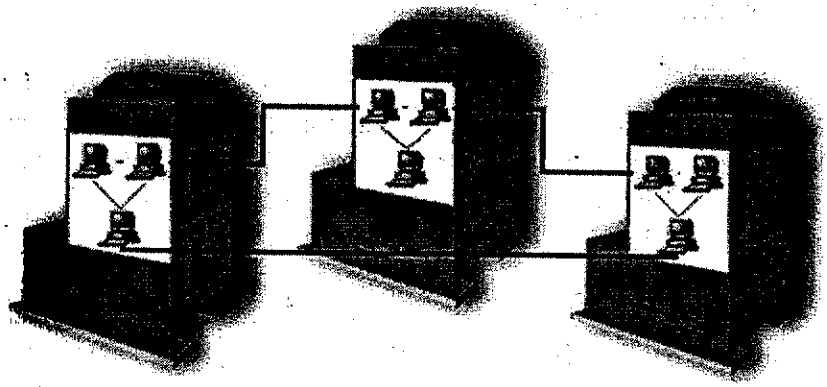
***Mạng diện rộng (WAN)*** liên kết các tài nguyên máy tính trong một vùng địa lý rộng (có bán kính trên 100km) như thị xã, thành phố, tỉnh/bang, quốc gia. Có thể coi mạng WAN gồm nhiều mạng LAN khác nhau. Ví dụ một số công nghệ mạng WAN: ISDN (Integrated Services Data Network), frame relay, SMDS (Switched Multimegabit Data Service) và ATM (Asynchronous Transfer Mode).






**Hình 1. 4 Mạng WAN - kết hợp của nhiều mạng LAN qua các router**

Một số người phân biệt kỹ hơn giữa mạng LAN và WAN. Do vậy xuất hiện phân loại ***Mạng đô thị (MAN)***. MAN liên kết các tài nguyên máy tính trong một thành phố. Giả sử có một công ty kinh doanh có nhiều tòa nhà trong tỉnh/thành phố. Mỗi tòa nhà có một mạng LAN riêng, những mạng LAN này được kết nối với nhau, kết quả ta có một mạng MAN vì tất cả các tòa nhà là ở trong cùng một tỉnh/thành phố. Nhìn chung, MAN được dùng để chỉ các mạng có diện hoạt động lớn hơn LAN nhưng nhỏ hơn WAN.



**Hình 1. 5 Mạng MAN - kết hợp nhiều mạng LAN trong một khu vực địa lý**

Một loại mạng nữa là **Mạng cá nhân (PAN)**, chỉ mạng máy tính nhỏ sử dụng trong gia đình. Giá máy tính ngày càng rẻ làm cho số gia đình có

nhiều máy tính ngày càng tăng nhanh, dẫn đến nhu cầu xuất hiện mạng PAN vì người ta nhận ra ưu điểm của việc kết nối các máy tính trong gia đình. Ví dụ, có thể nối các máy tính trong nhà đến cùng một máy in, không cần phải mua máy in cho mỗi máy tính. PAN cũng cho phép cả gia đình sử dụng một máy làm file server chứa tất cả phần mềm ứng dụng và dữ liệu người dùng; có thể truy cập đến server này từ bất cứ máy nào nối với mạng gia đình. PAN cũng giúp các thành viên trong gia đình truy cập đến bất cứ tài nguyên nào được dùng chung trong gia đình từ các vị trí khác nhau trong nhà.

***Mạng toàn cầu (GAN)*** là mạng của các mạng WAN, trải rộng trên phạm vi toàn cầu. Ví dụ, nhiều công ty xuyên quốc gia hoạt động trên nhiều nước trên thế giới. Việc kết nối mạng của các công ty con lại với nhau tạo thành mạng GAN. Mạng toàn cầu Internet cũng là một mạng GAN đặc biệt.

### *Phân loại mạng theo mô hình ghép nối*

Một cách khác để phân loại mạng là theo topo - mô hình ghép nối mạng, hay còn gọi là hình trạng mạng. Topo mạng gần giống như bản đồ đường phố. Nó mô tả chi tiết cách thức kết nối các thành phần chính của mạng (các nút) và các đường truyền. Có thể so sánh topo mạng với bản thiết kế của một ngôi nhà, trong đó hệ thống điện, sưởi, điều hòa, và nước được tích hợp với nhau trong một thiết kế chung nhất, hoàn chỉnh. Có 3 chiến lược kết nối tổng quát: điểm-điểm (point-to-point), broadcast (điểm-nhiều điểm) và multidrop (đa chặng).

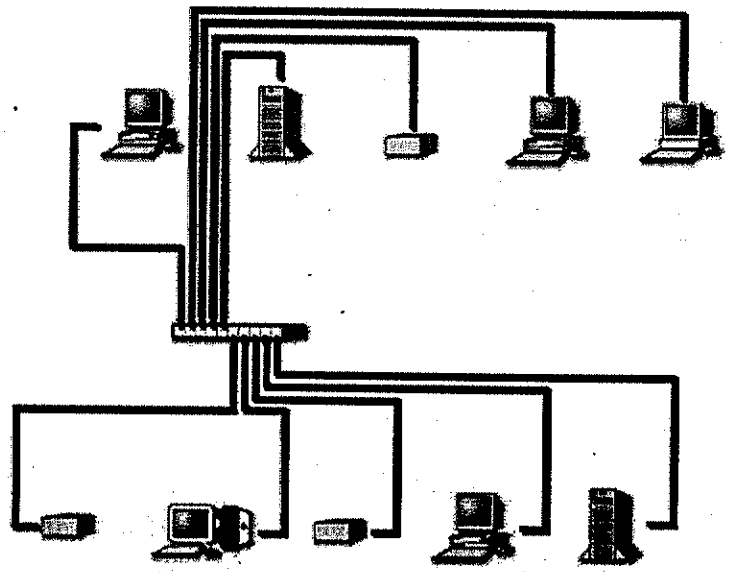
### *Mô hình điểm-điểm (point-to-point)*

Mạng point-to-point gồm nhiều nút, mỗi nút chỉ có thể liên lạc với nút liền kề qua đường liên kết trực tiếp. Mạng point-to-point có thể bao gồm hàng ngàn nút, mỗi nút nối trực tiếp với một số nút nào đó. Nếu một nút cần liên lạc với nút không liền kề, nó buộc phải liên lạc gián tiếp thông qua chuỗi các nút khác. Đầu tiên, nút nguồn chuyển thông điệp tới nút liền kề với mình. Sau đó thông điệp này sẽ được chuyển tuần tự qua dãy các nút liền kề nhau cho đến khi đến được nút đích. Việc chuyển dữ liệu thông qua nút liền kề đến một nút khác thường được gọi là bridging hoặc routing (định tuyến) – tùy thuộc vào kỹ thuật truyền tin (bridging được thảo luận trong chương 5; routing được thảo luận trong chương 4). Có một số topo mạng dựa trên mô hình point-to-point. Xét hai dạng topo mạng point-to-point phổ biến: star (hình sao) và tree (dạng cây).



### Star (Hình sao)

Đặc điểm chính của mạng hình sao là có một hub xử lý trung tâm – hub này là trung tâm truyền tin cho tất cả các nút. Cấu hình mạng hình sao đơn giản được minh họa trong hình 1.6. Để các nút có thể truyền thông cho nhau, tất cả dữ liệu phải được chuyển qua hub. Do đó khi hub ngừng hoạt động thì toàn bộ mạng sụp đổ. Hình 1.6 minh họa một mạng 10BASE-T (một dạng Ethernet), gồm các nút được nối trực tiếp với một Ethernet switch thông qua một cáp xoắn đôi trần (UTP – unshielded twisted-pair cable). (Mạng 10BASE-T, switched Ethernet và cáp UTP được thảo luận chi tiết trong chương 5).

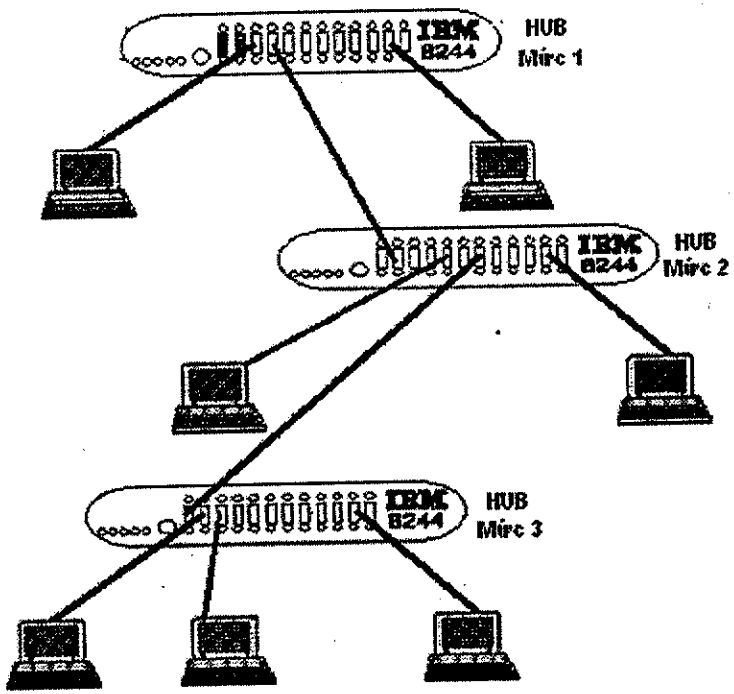


**Hình 1. 6 Các thiết bị nối vào một HUB duy nhất. Mô hình sao**

### Tree (Cây)

Mô hình cây là mô hình phân cấp, gồm một nút gốc hoặc một hub nối đến các nút mức hai hoặc hub mức hai. Các thiết bị ở mức hai lại được nối đến các thiết bị ở mức ba, mức ba được nối đến các thiết bị ở mức bốn... Mạng hình cây đơn giản được minh họa trên hình 1.7. Kiến trúc mạng IEEE 802.12, hay còn gọi là 100VG-AnyLAN, áp dụng mô hình này trong đó các hub được sắp thành tầng tạo thành mô hình phân cấp. Mô hình cây được minh họa trong hình 1.7.

THƯ VIỆN TRƯỜNG ĐHSPKT
SKV 057729




Hình 1. 7 Mô hình cây

*Mô hình điểm - nhiều điểm (Broadcast)*

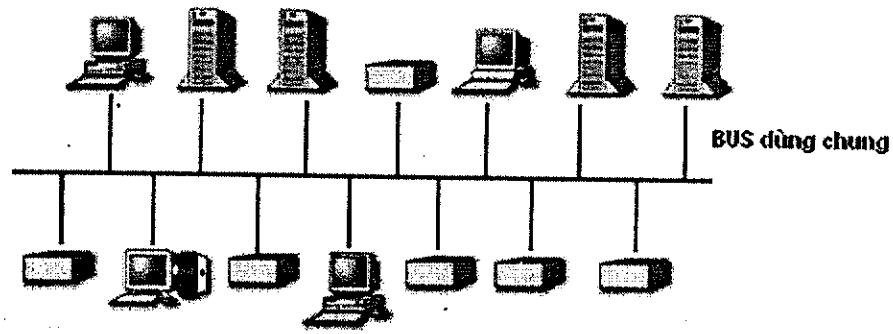
Mô hình này gồm các nút dùng chung một kênh truyền thông. Khác với mô hình điểm - điểm, dữ liệu từ một máy gửi đi sẽ được truyền đến tất cả các nút tham gia kênh truyền dùng chung. Các máy sẽ kiểm tra xem liệu chúng có phải là đích đến của thông điệp nhận được hay không bằng cách kiểm tra địa chỉ đến (destination address) của thông điệp. (Khái niệm địa chỉ sẽ được thảo luận trong phần tiếp theo). Các máy không phải là đích của thông điệp sẽ bỏ qua thông điệp. Chỉ có nút đích của thông điệp mới tiếp nhận thông điệp. Điều này cũng tương tự như một lớp học gồm nhiều sinh viên và một giáo viên. Nếu giáo viên đưa ra một câu hỏi, tất cả sinh viên đều nghe thấy câu hỏi nhưng chỉ sinh viên được giáo viên chỉ định mới trả lời câu hỏi này. Môi trường dùng chung ở đây chính là không khí, câu hỏi của giáo viên là một dạng thông điệp, lan truyền trong không khí và đến tai tất cả các sinh viên (các nút).



Mô hình điểm - nhiều điểm có một số dạng topo phổ biến, đó là bus và ring. Các hệ thống truyền thông vệ tinh cũng dựa trên mô hình điểm - nhiều điểm.

**Bus**

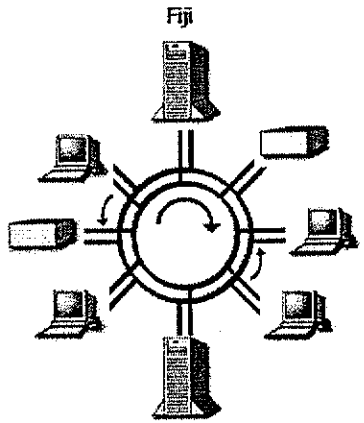
Một cấu hình bus điển hình được minh họa trong hình 1.8. Rõ ràng topo dạng bus thuộc mô hình điểm - nhiều điểm: các nút mạng được nối đến cùng một kênh truyền. Ví dụ điển hình về mạng có topo dạng bus là mạng Ethernet đồng trục (xem chương 5).




Hình 1.8 Mạng Ethernet với Bus dùng chung

**Ring**

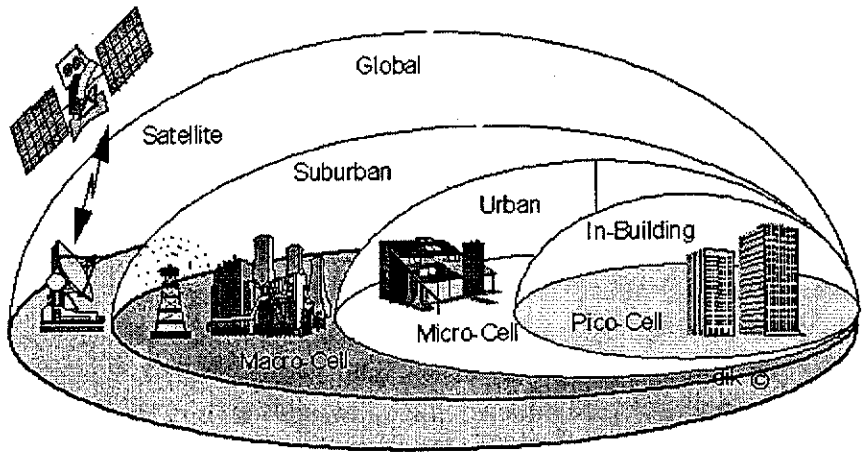
Trong cấu hình ring, tất cả các nút được nối đến một vòng – môi trường truyền thông dùng chung. Trong topo dạng ring truyền thống, thông điệp được truyền lần lượt qua các nút trên vòng. Phụ thuộc vào công nghệ sử dụng, hướng truyền có thể thuận hay nghịch chiều kim đồng hồ. Chú ý rằng mặc dù dữ liệu được chuyển từ nút nọ đến nút kia, ring vẫn không phải là một topo thuộc mô hình điểm - điểm vì các nút dùng chung một kênh truyền. Vì vậy, về mặt logic, trong topo dạng ring tất cả các nút dùng chung một kênh truyền, nhưng về mặt vật lý, việc truyền thông thuộc mô hình điểm - điểm. Trường hợp này cũng giống như topo dạng bus và tất cả các hệ thống điểm - nhiều điểm khác, mạng dạng ring cần một số phương pháp để quản lý việc truy cập vòng đồng thời.




Hình 1.9 Mạng FDDI có topo dạng Ring

## Vệ tinh

Trong hệ thống truyền thông vệ tinh, việc truyền dữ liệu từ một ăng-ten trên mặt đất đến vệ tinh thường là mô hình điểm-điểm. Tuy nhiên, tất cả các nút nằm trong mạng đều có thể nhận được dữ liệu từ vệ tinh truyền xuống - vệ tinh phát quảng bá xuống một hoặc nhiều trạm trên mặt đất. Do đó, các hệ thống truyền thông vệ tinh được xếp vào mô hình điểm - nhiều điểm (broadcast). Ví dụ, rất nhiều trường học ở Mỹ có khả năng nhận tin từ vệ tinh. Bất cứ chương trình giáo dục nào được phát quảng bá qua hệ thống vệ tinh đều được các trường học thu được bằng cách điều chỉnh thiết bị nhận đến một tần số thích hợp. Mạng vệ tinh được minh họa trên hình 1.10.




Hình 1. 10 Vệ tinh và các khu vực phủ sóng



Trong mô hình điểm - nhiều điểm có rất nhiều kiểu truyền thông điệp khác nhau:

**unicast** - chỉ có một thiết bị nhận thông điệp.

**multicast** - một nhóm thiết bị nhận thông điệp. Chính tầng network của thiết bị nhận sẽ kiểm tra xem thiết bị nhận đó có nằm trong nhóm nhận thông điệp không.

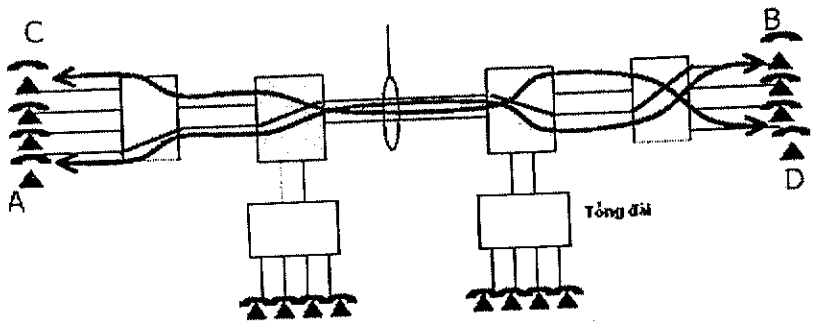
**broadcast** - tất cả các thiết bị trong mạng nhận thông điệp. Thông điệp broadcast là một thông điệp multicast đặc biệt.

Một đặc điểm khác của mô hình điểm - nhiều điểm là khái niệm tranh chấp (contention). Do tất cả các nút cùng dùng chung một kênh truyền, chúng phải "tranh nhau" kênh truyền khi có nhu cầu gửi giữ liệu. Do vậy mạng dựa trên mô hình broadcast cần giải quyết vấn đề nhiều nút muốn truyền dữ liệu tại cùng một thời điểm. Rất nhiều giao thức được đưa ra để giải quyết tranh chấp giữa các nút và sẽ được trình bày trong chương 5.

### *Phân loại mạng theo kiểu chuyển*

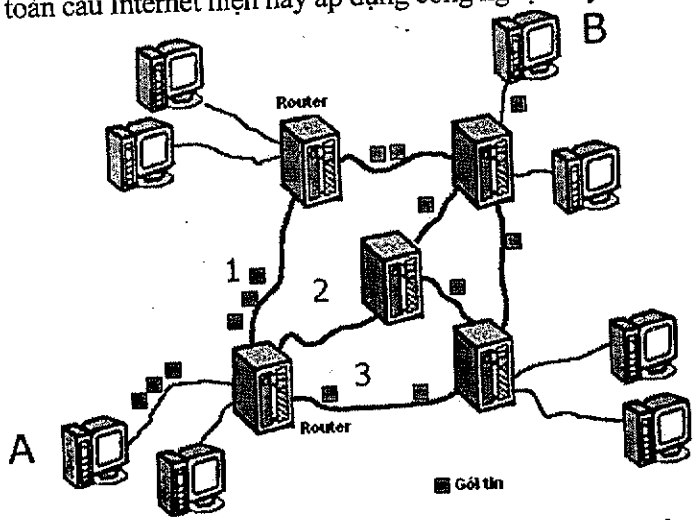
Ngoài việc phân loại theo diện hoạt động và topo, mạng còn được phân loại theo kiểu truyền thông mà chúng sử dụng, cùng với cách dữ liệu được truyền đi. Hai phân loại điển hình là mạng chuyển mạch ảo (virtual circuit-switched) và mạng chuyển gói (packet-switched).

Trong mạng ***chuyển mạch ảo (circuit-switched)***, phải thiết lập mạch vật lý giữa nút nguồn và đích trước khi chuyển dữ liệu thực sự. Mạch này tồn tại trong suốt thời gian chuyển dữ liệu. Mạng điện thoại công cộng là một ví dụ về mạng chuyển mạch ảo. Khi gọi điện thoại, một đường truyền vật lý trực tiếp được thiết lập giữa máy điện thoại của người gọi và máy điện thoại của người nhận. Đường truyền này là một kết nối điểm - điểm, liên kết các bộ chuyển mạch (switch) trong các tổng đài của công ty điện thoại lại với nhau. Sau khi đã được thiết lập, đường truyền chỉ dành riêng để truyền dữ liệu cho cuộc gọi hiện thời. Sau khi truyền xong dữ liệu (cuộc gọi kết thúc), mạch được giải phóng và có thể được cấp phát cho cuộc gọi khác. Như vậy, chuyển mạch làm tăng khả năng chia sẻ đường truyền (link) vì cùng một mạch có thể được sử dụng cho nhiều quá trình truyền khác nhau, mặc dầu không cùng một thời điểm.




Hình 1.11 Mạng điện thoại - chuyển mạch ảo

Trong ***mạng chuyển gói (packet-switched network)***, thông điệp đầu tiên được chia thành những đơn vị nhỏ hơn gọi là gói (packet), sau những packet lần lượt được gửi tới nút nhận qua mạng lưới các thiết bị chuyển mạch trung gian (switch). Packet là một đơn vị dữ liệu nhỏ nhất có thể truyền trên mạng. Mỗi packet mang thông tin về địa chỉ nút nhận cùng số thứ tự của mình. Khi packet đến thiết bị trung gian, thiết bị này căn cứ vào địa chỉ đích của packet để quyết định xem sẽ chuyển packet đi theo hướng nào để đến được thiết bị kế tiếp. Do cấu hình của toàn bộ hệ thống có thể thay đổi nên các packet của cùng một thông điệp có thể đến đích theo những tuyến đường khác nhau. Điều này cũng giống như việc gửi thư. Khi nhận được thư, bưu cục sẽ căn cứ vào địa chỉ người nhận để chuyển đến nơi thích hợp. Mạng toàn cầu Internet hiện nay áp dụng công nghệ chuyển mạch gói này.




Hình 1.12 Mạng chuyển mạch gói – các gói tin đi theo nhiều tuyến đường khác nhau từ A đến B



## 1.1.4 Địa chỉ mạng, định tuyến, tính tin cậy, tính liên tác và an ninh mạng

Khái niệm mạng máy tính liên quan đến nhiều yếu tố, trong đó có địa chỉ, định tuyến, tính tin cậy, tính liên tác, và an ninh mạng. Phần dưới đây trình bày ngắn gọn về những yếu tố này.

### Địa chỉ (Address)

Khái niệm địa chỉ liên quan đến việc gán cho mỗi nút mạng một địa chỉ duy nhất - cho phép các thiết bị khác định vị được nó. Điều này giống như địa chỉ của một ngôi nhà - tên phố sẽ chỉ cho biết khu vực cần đi đến, số nhà xác định chính xác nhà cần đến. Một ví dụ khác là hệ thống điện thoại. Mỗi điện thoại có mã vùng và một số (địa chỉ). Mã vùng cung cấp thông tin về vị trí vùng của điện thoại, còn số điện thoại là số xác định duy nhất máy điện thoại trong vùng. Hệ thống các thiết bị chuyển mạch trong công ty điện thoại được lập trình để tạo nên một kênh truyền giữa hai thiết bị. Về thực chất mã vùng lại được phân cấp thành mã quốc gia và mã khu vực.

### Routing - Định tuyến

Định tuyến xác định tuyến đường mà dữ liệu sẽ đi qua trong quá trình chuyển từ nút nhận đến nút gửi. Chức năng định tuyến được thực hiện bởi một thiết bị phần cứng đặc biệt: router (thiết bị định tuyến). Việc lựa chọn tuyến đường tốt nhất phải dựa trên một tiêu chuẩn cụ thể - được gọi là độ đo (metric). Các độ đo định tuyến phổ biến là: khoảng cách, số chặng (hop) và băng thông.

### Tính tin cậy

Tính tin cậy chỉ tính toàn vẹn dữ liệu - đảm bảo dữ liệu nhận được giống hệt dữ liệu gửi đi. Mạng máy tính không phải là hệ thống không có lỗi. Trong thực tế, lỗi có thể xuất hiện trên tất cả các môi trường truyền. Vì vậy cần phải thiết kế sao cho hệ thống có khả năng xử lý lỗi. Một trong những phương pháp điển hình là thêm thông tin dư thừa vào dữ liệu chuyển đi sao cho phía nhận phát hiện được lỗi (nếu có). Khi phát hiện ra lỗi, phía

nhận có thể: (1) yêu cầu truyền lại dữ liệu bị lỗi, hoặc (2) kiểm tra xem dữ liệu đúng là gì và sửa lại dữ liệu bị lỗi. Cách thứ nhất là sửa lỗi bằng cách yêu cầu truyền lại, cách thứ hai là tự sửa lỗi. Để sửa được lỗi, phải dò tìm lỗi. Việc tự sửa lỗi nói chung khó thực hiện. Hầu hết các mạng ngày nay đều được thiết kế có khả năng phát hiện lỗi (error detection). Có hai cách để phát hiện lỗi thông dụng là kiểm tra bit chẵn/lẻ và mã dư thừa vòng (CRC – Cyclic Redundancy Check). Hai kỹ thuật này được trình bày trong chương 5.

**Tính liên tác (interoperability)**

Tính liên tác (interoperability) chỉ khả năng các sản phẩm (phần cứng và phần mềm) của các hãng sản xuất khác nhau có thể giao tiếp được với nhau trong mạng. Trong thời kì hoàng kim của các mạng độc quyền (của tư nhân, hãng sản xuất, hoặc một tổ chức), không cần phải quan tâm đến tính liên tác, miễn là các thành phần cấu thành mạng đều là sản phẩm và giao thức của cùng một hãng sản xuất. Khi hãng sản xuất thứ ba phát triển ứng dụng có tính năng được cải tiến hơn ứng dụng của hãng sản xuất độc quyền, hãng sản xuất thứ ba phải được sự đồng ý của nhà sản xuất độc quyền - tức là hãng sản xuất thứ ba phải trả phí bản quyền. Ngày nay, với bộ giao thức "mở" TCP/IP, các hãng sản xuất - những người viết và bán các ứng dụng dựa trên TCP/IP được tự do làm những điều họ muốn, không phải lo ngại về việc vi phạm bản quyền. Hầu hết các hãng sản xuất máy tính đều cố gắng để sản phẩm của mình tương thích với sản phẩm của hãng sản xuất khác.

**An ninh**

An ninh mạng chỉ việc bảo vệ mọi thứ trong mạng, bao gồm dữ liệu, phương tiện truyền thông và các thiết bị. An ninh mạng còn bao gồm các chức năng quản trị, các công cụ kỹ thuật và thiết bị như các sản phẩm mã hóa, các sản phẩm kiểm soát truy cập mạng (ví dụ: tường lửa firewall - thiết bị phần cứng đặc biệt bảo vệ mạng với thế giới bên ngoài). An ninh mạng cũng bao gồm việc định ra những chính sách sử dụng tài nguyên mạng, kiểm tra xem tài nguyên mạng có được sử dụng phù hợp với chính sách đã định trước hay không, quy định và kiểm tra chỉ những người có đủ quyền mới được sử dụng các tài nguyên đó…



## 1.1.5 Chuẩn mạng

Chuẩn mạng định nghĩa các giao tiếp phần cứng, giao thức truyền thông, kiến trúc mạng... Chuẩn mạng thiết lập những quy tắc hay các quy ước cụ thể mà các bên tham gia truyền thông cần tuân thủ. Chúng làm tăng khả năng giao tiếp giữa sản phẩm phần cứng và phần mềm của các hãng sản xuất khác nhau. Chuẩn được xây dựng thông qua các tổ chức chuẩn hóa. Những tổ chức này được chia thành bốn loại chính: (a) quốc gia, (b) vùng, (c) quốc tế và (d) ngành/hiệp hội thương mại/hiệp hội nghề. Thành viên của tổ chức chuẩn thường là đại diện của chính phủ, viện nghiên cứu và hãng sản xuất. Quá trình xây dựng chuẩn phải đảm bảo được tính thống nhất, vì vậy thường kéo dài, đôi khi phải mất nhiều năm mới cho ra đời được một chuẩn chính thức. Quá trình này cũng bị ảnh hưởng bởi các yếu tố khác như kinh tế, chính trị.

**Chuẩn chính thức (De jure standard)**

Chuẩn chính thức được công nhận bởi những tổ chức chuẩn hóa chuyên nghiệp. Ví dụ, những giao thức về modem được xây dựng bởi Hiệp hội truyền thông quốc tế (International Telecommunications Union – ITU), hay chuẩn EIA/TIA-568 dùng cho Commercial Building Telecommunications Wiring được xây dựng bởi Electronic Idustries Association - EIA và Telecommunications Inustries Association – TIA, hoặc các chuẩn cho mạng cục bộ được xây dựng bởi Institute for Electrical and Electronic Engineers – IEEE. (Các chuẩn này sẽ được trình bày chi tiết trong các chương sau).

**Chuẩn thực tế (De facto standard)**

Chuẩn thực tế là chuẩn tồn tại trong thực tế chứ không phải do các tổ chức chuẩn hóa xây dựng nên. Chúng được phát triển thông qua sự chấp nhận của toàn ngành đối với chuẩn nào đó của một hãng nhà sản xuất cụ thể. Ví dụ một chuẩn thực tế là Network File System (NFS) - giao thức chia sẻ file của hãng Sun Microsystems. Sun đã công khai đặc tả của giao thức này, do đó những nhà sản xuất khác có thể tự do triển khai. Kết quả NFS được sử dụng rộng rãi và được coi như một chuẩn thực tế. Hiện tại, NFS được cài đặt trên rất nhiều hệ thống UNIX khác nhau (Sun, IBM, Silicon Gracphics, Compaq, và HP), cũng như các hệ thống dựa trên Macintosh và Intel. Một chuẩn thực tế khác là Java - ngôn ngữ lập trình Web được phát triển bởi hãng Sun Microsystems.

### Chuẩn riêng của hãng

Chuẩn của hãng quy định những yêu cầu cụ thể của một nhà sản xuất nào đó. Những đặc tả này không được công khai, chỉ được tuân theo và chấp nhận bởi chính hãng sản xuất đề nghị ra nó. Trong thời kì đầu của mạng, các chuẩn của hãng thống trị. Mặc dầu ngày nay những chuẩn như vậy không còn được tán thành nữa song chúng vẫn tồn tại rất nhiều. Được biết đến nhiều nhất phải kể đến các chuẩn của IBM (ví dụ: SNA - kiến trúc hệ thống mạng của IBM, giao thức IPX của Novell - dựa trên giao thức XNS của Xerox). Chuẩn riêng của hãng trói buộc khách hàng vào giải pháp của một nhà sản xuất cụ thể, làm cho họ gặp khó khăn khi sử dụng sản phẩm (phần cứng hoặc phần mềm) của các hãng sản xuất khác.

### Chuẩn hiệp hội

Chuẩn hiệp hội tương tự như chuẩn chính thức theo nghĩa chúng là sản phẩm của quá trình chuẩn hóa. Điểm khác nhau là quá trình lập kế hoạch và chuẩn hóa những chuẩn này không chịu sự quản lý của các tổ chức chuẩn hóa chuyên nghiệp. Thay vào đó, đặc tả cho các chuẩn được thiết kế và thỏa thuận bởi nhóm các nhà sản xuất thành lập nên hiệp hội, với một mục đích cụ thể: đạt được mục tiêu chung. Những nhà sản xuất này cam kết hỗ trợ cho các chuẩn được phát triển bởi hiệp hội, và phát triển những sản phẩm tuân theo chuẩn này. Ví dụ về các chuẩn hiệp hội như Fast Ethernet, Asynchronous Transfer Mode (ATM Forum) hay Gigabit Ethernet.

## 1.2 MÔ HÌNH OSI

Tổ chức ISO (International Standards Organization) được thành lập năm 1971 với mục đích xây dựng các tiêu chuẩn quốc tế. Một trong các chuẩn ISO định nghĩa các mặt của truyền thông mạng là mô hình OSI - Open Systems Interconnection (Mô hình liên kết giữa các hệ thống mở). Đây là mô hình cho phép bất cứ hai hệ thống nào (cho dù khác nhau) có thể truyền thông với nhau mà không cần quan tâm đến kiến trúc bên dưới của chúng. Các giao thức của riêng một hãng sản xuất thường ngăn ngừa việc truyền thông giữa hai hệ thống không cùng một kiểu. Mô hình OSI ra đời



với mục đích cho phép hai hệ thống bất kì truyền thông với nhau mà không cần thay đổi bất cứ phần cứng hoặc phần mềm nào bên dưới. Mô hình OSI không phải là một giao thức; nó là một mô hình để nhận biết và thiết kế một kiến trúc mạng linh động, vững chắc và có khả năng liên tác. Chú ý ISO là tên tổ chức; OSI là một mô hình.

### 1.2.1 Mô hình

Mô hình OSI được phân tầng với mục đích thiết kế các hệ thống mạng cho phép tất cả các kiểu hệ thống máy tính khác nhau có thể truyền thông với nhau. Mô hình gồm 7 tầng riêng biệt nhưng có liên quan đến nhau, mỗi tầng định nghĩa một phần của quá trình truyền thông tin trên mạng. Những quy tắc cơ bản của mô hình OSI là nền tảng cơ bản để nghiên cứu chi tiết truyền thông dữ liệu.

Thực ra trong cuộc sống, chúng ta gặp khá nhiều ví dụ về việc phân tầng. Giả sử người A viết thư gửi cho người B. Sau khi viết thư xong, A cho thư vào phong bì, dán kín, ghi địa chỉ của B, dán tem và nhét bức thư vào hộp thư ở bưu điện. Giữa A và B, đơn vị dữ liệu trao đổi là các lá thư. Bức thư có thể xem là dữ liệu thực sự trong khi phong bì thư có thể xem là một loại tiêu đề chứa các thông tin điều khiển. Hệ thống bưu điện (bao gồm nhiều bưu cục – là các trạm trung gian mà bức thư sẽ đi qua) chịu trách nhiệm chuyển bức thư tới địa chỉ của B. Với ví dụ này tầng dưới (hệ thống bưu điện) sẽ cung cấp dịch vụ chuyển thư cho tầng trên (A và B). A và B chỉ quan tâm đến nội dung bức thư, khuôn dạng thư, ngôn ngữ viết trong thư... mà không cần quan tâm đến làm thế nào để thư có thể chuyển tới B. Đây chính là ưu điểm của việc phân tầng: tầng trên sử dụng dịch vụ của tầng dưới nhưng không cần quan tâm đến cách thức thực hiện dịch vụ đó.

### Kiến trúc phân tầng

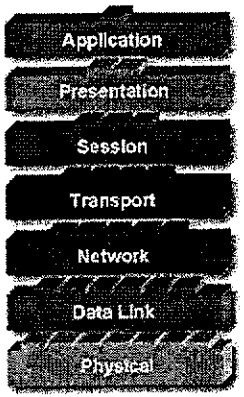
Mô hình OSI gồm 7 tầng (Hình 1.13):

Tầng vật lý (Physical layer)

Tầng liên kết dữ liệu (Datalink layer)

Tầng mạng (Network layer)

Tầng giao vận (Transport layer)
Tầng phiên (Session layer)
Tầng trình diễn (Presentation layer)
Tầng ứng dụng (Application layer).




**Hình 1.13 Bảy tầng trong mô hình OSI**

## *Trong lịch sử* LỊCH SỬ MÔ HÌNH 7 TẦNG

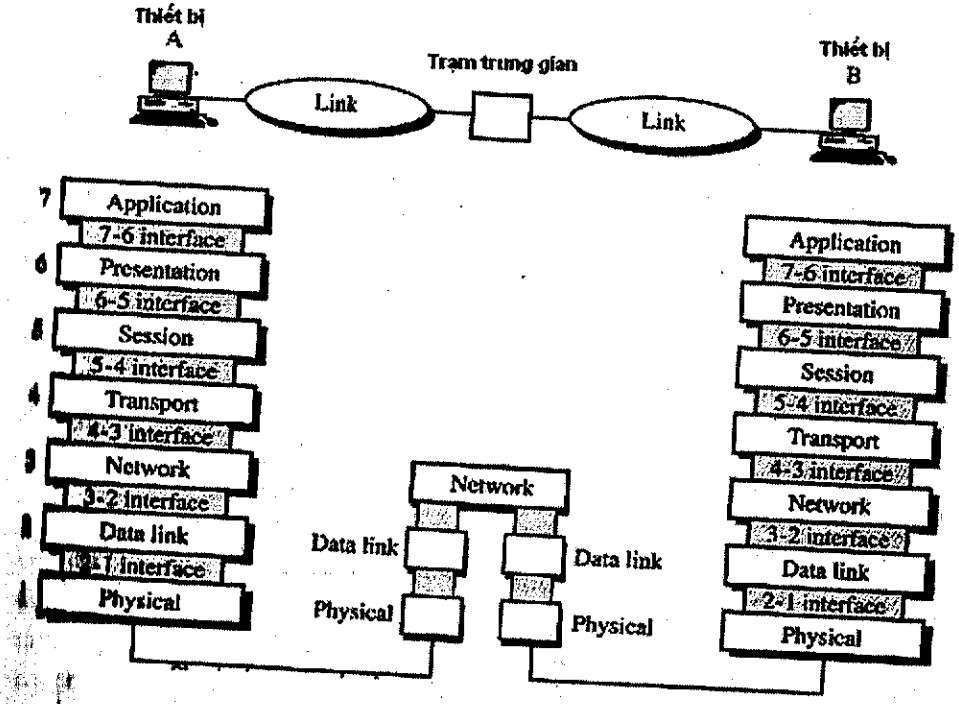
Phần lớn công việc thiết kế mô hình OSI được thực hiện bởi hai nhà nghiên cứu Mike Canepa và Charlie Bachman tại công ty Honeywell Information Systems. Mục tiêu của nhóm nghiên cứu này là phát triển một hệ thống nguyên mẫu cùng một bản kế hoạch phát triển sản phẩm. Nửa đầu thập niên 70, nhóm tập trung vào thiết kế cơ sở dữ liệu có hỗ trợ truy cập từ xa – và do đó cần tới một kiến trúc truyền thông phân tán nhưng có cấu trúc. Sau khi có những nghiên cứu về kiến trúc mạng SNA của IBM, các giao thức đề xuất cho mạng ARPANET, nhóm đã phát triển kiến trúc hệ thống phân tán (DSA – Distributed Systems Architecture) - tiền thân của mô hình 7 tầng ngày nay.

Trong khi đó, Cơ quan chuẩn hóa Anh quốc đề nghị Tổ chức chuẩn quốc tế (ISO) ban hành một kiến trúc chung cho truyền thông phân tán. Theo yêu cầu này, ISO thành lập tiểu ban Kết nối các Hệ thống mở (Open Systems Interconnection – OSI) và yêu cầu Cơ quan chuẩn hóa Hoa Kỳ (ANSI) đưa ra một đề xuất cho phiên họp đầu tiên của OSI.

Bachman và Canepa tham dự những phiên họp đầu tiên với ANSI và đã trình bày mô hình bảy tầng của mình và ngay lập tức mô hình này được lựa chọn để đề xuất cho tiểu ban OSI. Vào tháng 3/1978, khi tiểu ban OSI họp tại Washington, Bachman đã trình bày mô hình của mình. Với một sự nhất trí cao, tiểu ban đã chấp nhận kiến trúc phân tầng này đáp ứng đầy đủ phần lớn các yêu cầu và có khả năng mở rộng để thỏa mãn các yêu cầu mới. Phiên bản đầu tiên của mô hình này được công bố vào tháng 3/1978. Phiên bản kế tiếp (với một vài chỉnh sửa) công bố vào tháng 6/1979 và tiếp tục được chỉnh sửa thêm.



Hình 1.14 minh họa mối quan hệ giữa các tầng khi thông điệp được gửi từ thiết bị A đến thiết bị B. Khi đi từ A đến B, thông điệp có thể đi qua nhiều nút trung gian khác. Những nút trung gian này thường chỉ liên quan đến 3 tầng đầu của mô hình OSI. Khi phát triển mô hình, các nhà thiết kế đã phân tích quá trình truyền dữ liệu ra những chức năng cơ bản nhất, và nhóm những chức năng có mục đích (sử dụng) liên quan đến nhau vào các nhóm riêng - còn gọi là tầng (layer). Mỗi tầng đều có chức năng, nhiệm vụ xác định. Bằng cách xác định và khoanh vùng các chức năng trong mô hình, nhà thiết kế đã đưa ra một kiến trúc đạt được cả tính toàn diện và linh hoạt. Quan trọng nhất, mô hình OSI tạo ra tính trong suốt hoàn toàn giữa hai hệ thống không tương thích với nhau.




**Hình 1.13 Mô hình OSI**

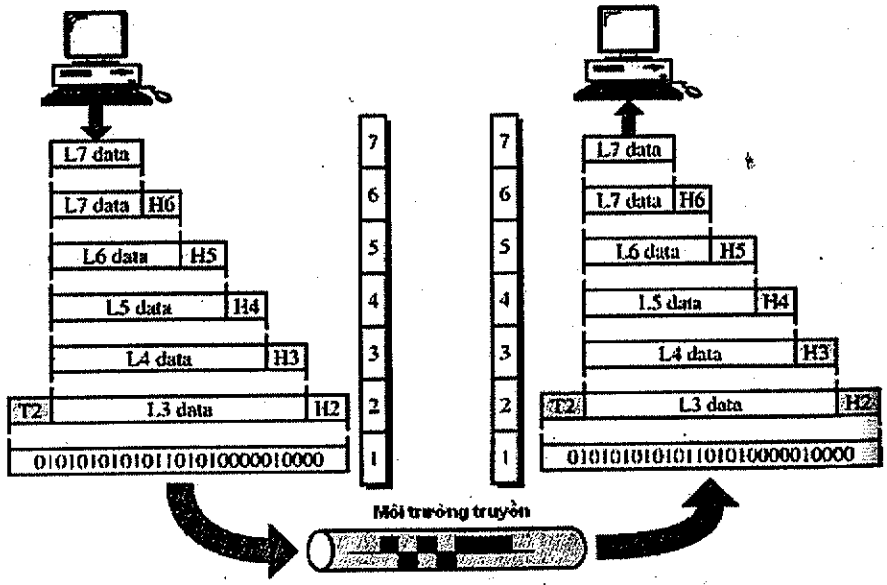
### tiến trình ngang hàng (peer-to-peer)

Tại thiết bị đầu cuối, mỗi tầng sử dụng các dịch vụ do tầng bên dưới cấp. Ví dụ, tầng 3 sử dụng các dịch vụ do tầng 2 cung cấp và đến lượt

mình lại cung cấp dịch vụ cho tầng 4. Giữa các máy tính, tầng N trên một thiết bị giao tiếp với tầng N trên thiết bị khác. Việc giao tiếp này được tiến hành theo các quy tắc và quy ước đã được thỏa thuận trước-gọi là giao thức.

Tại tầng vật lý, truyền thông diễn ra trực tiếp: A gửi một luồng bit đến B dưới dạng tín hiệu. Tuy nhiên tại các tầng cao hơn trên máy A, dữ liệu được chuyển dần xuống các tầng bên dưới, đến máy B và tiếp tục đi ngược lên các tầng cao hơn (của B). Mỗi tầng trong máy gửi (A) thêm các thông tin của mình vào thông điệp nhận được từ phía trên rồi sau đó chuyển toàn bộ gói dữ liệu xuống tầng phía dưới. Các thông tin được thêm vào này - được gọi là header (tiêu đề chèn trước) và trailer (tiêu đề chèn sau) - là các thông tin điều khiển được thêm vào đầu hay cuối gói dữ liệu. Header được thêm vào thông điệp tại mỗi tầng 6, 5, 4, 3, và 2; trailer được thêm vào tại tầng 2.

Tại tầng 1, gói dữ liệu được chuyển thành dạng tín hiệu có thể truyền đi tới máy nhận. Tại thiết bị nhận, các tiêu đề được lấy ra dần dần trong quá trình chuyển dữ liệu lên trên. Ví dụ, tầng 2 loại bỏ các tiêu đề của tầng 2 và chuyển phần còn lại (dữ liệu) cho tầng 3. Tầng 3 loại bỏ các tiêu đề tầng 3 và chuyển phần dữ liệu cho tầng 4...




**Hình 1. 14 Dữ liệu được chuyển dọc theo các tầng đi xuống phía dưới**



## Giao diện giữa các tầng

Trên cùng một máy tính, hai tầng kề nhau trao đổi dữ liệu với nhau qua các giao diện (interface). Giao diện định nghĩa cách thức và khuôn dạng dữ liệu trao đổi giữa hai tầng kề nhau trên cùng một thiết bị. Định nghĩa giao diện giữa các tầng một cách rõ ràng cho phép thay đổi cách thức triển khai tại một tầng mà không ảnh hưởng đến các tầng khác.

Trong thuật ngữ mạng, người ta thường gọi giao diện giữa các tầng là điểm truy cập dịch vụ (Service Access Point – SAP) vì tầng trên yêu cầu dịch vụ của tầng dưới thông qua giao diện.

## Tổ chức các tầng

Có thể chia bảy tầng vào ba nhóm. Nhóm tầng hỗ trợ mạng gồm ba tầng: vật lý, liên kết dữ liệu và mạng chịu trách nhiệm về các mặt liên quan đến khía cạnh vật lý khi truyền dữ liệu từ thiết bị này sang thiết bị khác (ví dụ: đặc tả điện, các kết nối vật lý, định địa chỉ vật lý, định thời gian truyền và tính tin cậy). Tầng phiên, trình diễn, và ứng dụng thuộc nhóm tầng hỗ trợ người dùng; chúng tạo ra khả năng liên tác giữa các hệ thống phần mềm khác nhau. Tầng 4 - tầng giao vận đảm bảo việc chuyển dữ liệu đầu cuối (end-to-end) tin cậy, trong khi tầng 2 đảm bảo việc truyền dữ liệu tin cậy trên một đường truyền vật lý riêng lẻ. Nói chung, các tầng trên của mô hình OSI thường được triển khai qua phần mềm trong khi nhóm các tầng dưới được triển khai bằng sự kết hợp của cả phần cứng lẫn phần mềm. Tầng vật lý hầu như được triển khai bởi phần cứng.

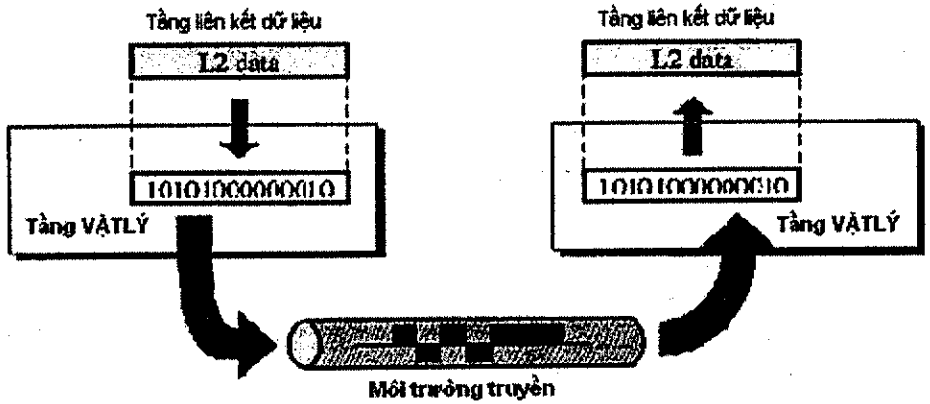
Hình 1.15 mô tả tổng quan các tầng trong mô hình OSI. Trong hình vẽ, (dữ liệu) L7 là đơn vị dữ liệu tại tầng 7, (dữ liệu) L6 là đơn vị dữ liệu tại tầng 6,... Trong thuật ngữ mạng người ta gọi Li là đơn vị dữ liệu giao thức tầng i (iPDU – Protocol Data Unit). Đối với tầng thứ i+1, dữ liệu tầng i truyền cho được gọi là đơn vị dữ liệu dịch vụ (service data unit – SAP). Nói chung PDU chứa SAP và một số thông tin tiêu đề khác. Quá trình được bắt đầu tại tầng 7 (tầng ứng dụng), sau đó chuyển xuống các tầng dưới. Tại mỗi tầng ngoại trừ tầng 7 và tầng 1, header được chèn thêm vào đơn vị dữ liệu. Tại tầng 2, ngoài header, trailer cũng được thêm vào đơn vị dữ liệu. Khi đi qua tầng vật lý (tầng 1), đơn vị dữ liệu (đã định khuôn dạng) được chuyển thành tín hiệu vật lý và truyền đi qua môi trường vật lý.

Tại nơi nhận, tín hiệu vật lý đến tầng 1 và được chuyển ngược lại thành chuỗi bit. Các đơn vị dữ liệu sau đó sẽ được chuyển dần từ tầng 1 lên các tầng trên trong mô hình OSI. Tại mỗi tầng, các header và trailer được thêm vào khối dữ liệu ở tầng tương ứng bên máy gửi được lấy ra. Khi đến tầng 7, thông điệp đã ở dạng dữ liệu phù hợp và ứng dụng có thể sử dụng.

## 1.2.2 Chức năng các tầng

Trong phần này, chúng ta sẽ mô tả chi tiết chức năng của từng tầng trong mô hình OSI.

**Tầng vật lý**




**Hình 1. 15 Vị trí, vai trò của tầng vật lý**

Tầng vật lý thực hiện các chức năng cần thiết để truyền luồng bit dữ liệu đi qua môi trường vật lý. Nó giải quyết những vấn đề liên quan đến đặc điểm kỹ thuật về cơ và điện giữa card ghép nối (interface) với môi trường truyền dẫn. Nó cũng xác định các thủ tục, chức năng mà thiết bị vật lý và thiết bị giao tiếp cần phải tuân thủ. Hình 1.16 minh họa mối quan hệ giữa tầng vật lý với môi trường truyền dẫn và tầng liên kết dữ liệu.

Trong ví dụ chuyển thư, tầng vật lý liên quan đến công nghệ chuyển thư, chẳng hạn là xe đạp, máy bay, tàu hỏa, tàu thủy... dùng chuyên chở các túi thư. Tầng liên kết dữ liệu chuyển lá thư cho tầng vật lý và hy vọng tầng vật lý chuyển lá thư sang phía bên kia của kênh truyền.



Tầng vật lý liên quan đến:

**Đặc điểm vật lý của môi trường (thiết bị) giao tiếp và truyền thông**: Tầng vật lý xác định đặc điểm/đặc tính giao diện giữa thiết bị và môi trường truyền dẫn. Nó cũng xác định kiểu môi trường truyền dẫn thông tin (xem chương 5).

**Biểu diễn bit**: Dữ liệu tầng vật lý là luồng bit liên tục (các chuỗi 0 và 1). Để truyền đi, bit phải được mã hóa thành tín hiệu điện hoặc quang. Tầng vật lý xác định phương thức mã hóa (các bit 0 và 1 được chuyển thành tín hiệu như thế nào).

**Tốc độ dữ liệu:** Tốc độ truyền dẫn - số bit được gửi đi trong một đơn vị thời gian. Nói cách khác, tầng vật lý xác định khoảng thời gian để truyền đi một bit.

**Đồng bộ hóa các bit**: Máy gửi và nhận phải được đồng bộ hóa ở mức bit. Nói cách khác, đồng hồ của máy gửi và nhận phải được đồng bộ hóa.

**Cấu hình đường truyền**: Tầng vật lý liên quan đến việc kết nối các thiết bị vào môi trường truyền thông. Trong cấu hình điểm-điểm (point-to-point), hai thiết bị được nối với nhau qua một đường truyền riêng. Trong cấu hình điểm-nhiều điểm (multipoint), một đường truyền được nhiều thiết bị dùng chung.

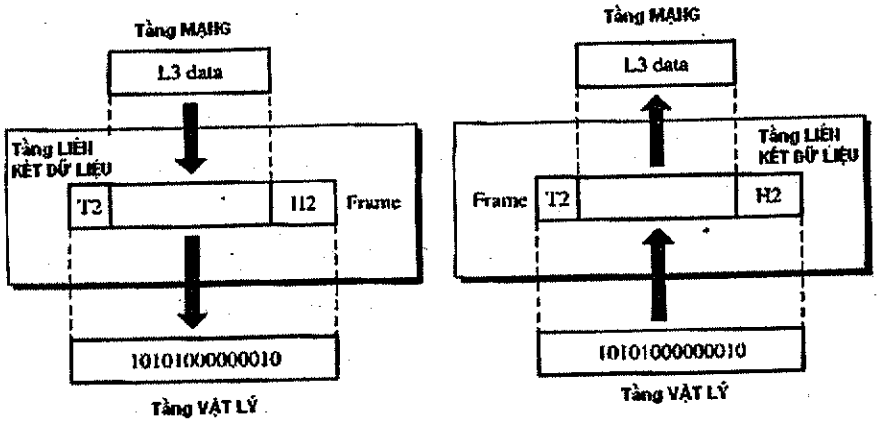
**Topo (Mô hình ghép nối) vật lý**: Topo vật lý xác định cách nối các thiết bị với nhau để tạo thành mạng. Có thể sử dụng topo dạng lưới (mesh topology) (mỗi thiết bị được nối với tất cả các thiết bị còn lại), topo dạng sao (star topology) (mỗi thiết bị được nối với một thiết bị trung tâm), topo dạng vòng (ring topology) (mỗi thiết bị được nối với một thiết bị bên cạnh, cứ như vậy tạo thành vòng), hay topo dạng bus (mỗi thiết bị được nối đến một đường truyền chung).

**Chế độ truyền dẫn**: Tầng vật lý xác định hướng truyền dữ liệu giữa hai thiết bị: đơn công (simplex), bán song công (half-duplex), hay song công (full-duplex). Trong chế độ đơn công, một thiết bị chỉ có thể gửi hoặc nhận dữ liệu. Chế độ đơn công là truyền thông một chiều. Trong chế độ bán song công, thiết bị có thể gửi và nhận dữ liệu, nhưng không phải tại cùng một thời

điểm. Trong chế độ song công, thiết bị có thể nhận và gửi dữ liệu tại cùng một thời điểm.

### Tầng liên kết dữ liệu

Nhiệm vụ của tầng liên kết dữ liệu là truyền thông giữa hai nút nối trực tiếp với nhau. Nó biến tầng vật lý không tin cậy thành đường truyền tin cậy cho tầng mạng bên trên. Hình 1.17 minh họa mối quan hệ giữa tầng liên kết dữ liệu với tầng mạng và tầng vật lý.




**Hình 1.16 Vị trí, vai trò của tầng liên kết dữ liệu**

Tầng liên kết dữ liệu chịu trách nhiệm:

**Framing – Đóng gói dữ liệu**: Tầng liên kết dữ liệu chia luồng bit nhận được từ tầng mạng thành các đơn vị dữ liệu gọi là frame.

**Định địa chỉ vật lý**: Nếu gói dữ liệu được chuyển đến thiết bị khác trong mạng, tầng liên kết dữ liệu thêm vào tiêu đề của frame địa chỉ vật lý của nơi nhận (địa chỉ đích) và có thể địa chỉ vật lý của nơi gửi (địa chỉ nguồn). Nếu gói dữ liệu được chuyển đến các thiết bị bên ngoài mạng, địa chỉ nhận sẽ là địa chỉ của thiết bị trung gian kết nối mạng ra bên ngoài.

**Kiểm soát lưu lượng**: Nếu tốc độ nhận dữ liệu nhỏ hơn tốc độ gửi dữ liệu, tầng liên kết dữ liệu phải thực hiện kỹ thuật kiểm soát lưu lượng để ngăn ngừa tình trạng quá tải tại nơi nhận.

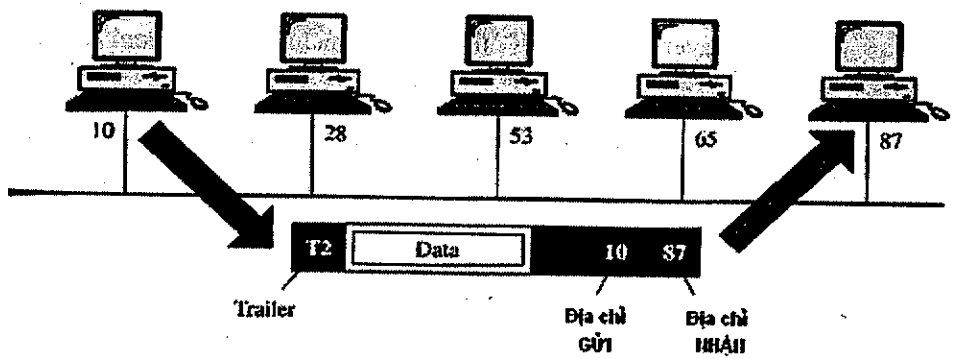
**Kiểm soát lỗi**: Tầng liên kết dữ liệu làm tăng tính tin cậy của tầng vật lý bằng cách sử dụng kỹ thuật phát hiện và truyền lại các frame bị lỗi



hoặc bị mất. Nó cũng sử dụng kỹ thuật xử lý các frame trùng lặp. Kiểm soát lỗi thường được thực hiện bằng cách thêm một trailer vào phần cuối của frame.

**Kiểm soát truy cập**: Khi nhiều thiết bị dùng chung đường truyền, các giao thức ở tầng liên kết dữ liệu sẽ quyết định thiết bị nào được quyền sử dụng đường truyền tại một thời điểm xác định.

Trong hình 1.18, nút có địa chỉ vật lý 10 gửi frame đến nút có địa chỉ vật lý 87. Hai nút này được nối với nhau qua đường truyền dùng chung. Ở tầng liên kết dữ liệu, header của frame chứa các địa chỉ vật lý. Phần còn lại của header chứa các thông tin cần thiết cho tầng liên kết dữ liệu. Trailer thường chứa các bit dư thừa để kiểm soát lỗi.



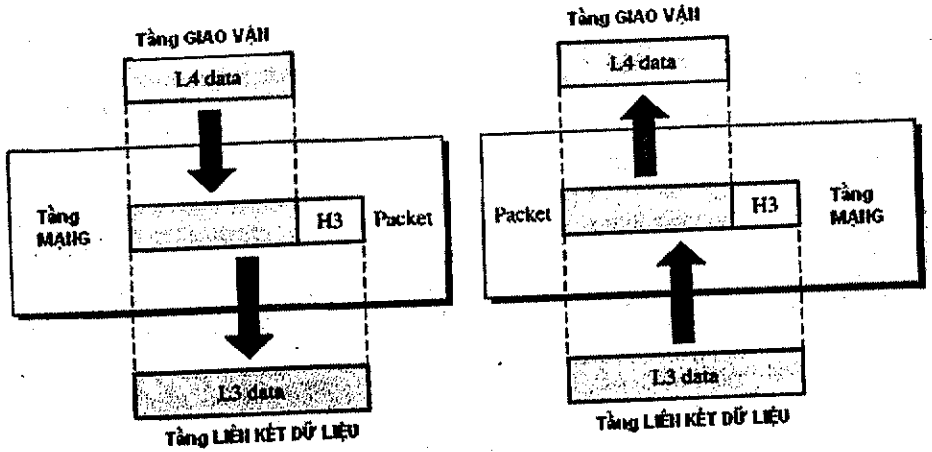

**Hình 1. 17 Ví dụ về địa chỉ của tầng liên kết dữ liệu**

Hãy xét tiếp ví dụ chuyển thư. Sau khi thu thập thư tại hòm thư, nhân viên bưu chính thực hiện việc phân loại thư ra hai nhóm: nhóm thứ nhất gồm các thư gửi tới địa chỉ nằm trong vùng do bưu cục quản lý, nhóm thứ hai chuyển ra phía ngoài. Đối với nhóm thứ hai, nhân viên bưu cục đặt tất cả thư trong một túi thư lớn và chuyển cho bưu cục cấp cao hơn. Các túi thư có thể xem là các "frame". Hơn thế nữa, địa chỉ trên túi thư sẽ cho phép thư được chuyển đến bưu cục cấp cao thích hợp.

### Tầng mạng

Tầng mạng chịu trách nhiệm chuyển gói dữ liệu từ nơi gửi đến nơi nhận, gói dữ liệu có thể phải đi qua nhiều mạng (các chặng trung gian). Tầng liên kết dữ liệu thực hiện truyền gói dữ liệu giữa hai thiết bị trong cùng một mạng, còn tầng mạng đảm bảo gói dữ-liệu sẽ được chuyển từ nơi gửi đến đúng nơi nhận.

Nếu hai thiết bị nằm trên cùng một môi trường truyền thì rõ ràng không cần tầng mạng. Tuy nhiên, nếu hai thiết bị ở trên hai mạng khác nhau, và giữa chúng có nhiều thiết bị kết nối trung gian thì cần phải có tầng mạng để thực hiện việc chuyển dữ liệu từ nguồn đến đích. Hình 1.19 minh họa mối quan hệ giữa tầng mạng với tầng giao vận và liên kết dữ liệu.




Hình 1.18 Vị trí tầng mạng

Tầng mạng có nhiệm vụ:

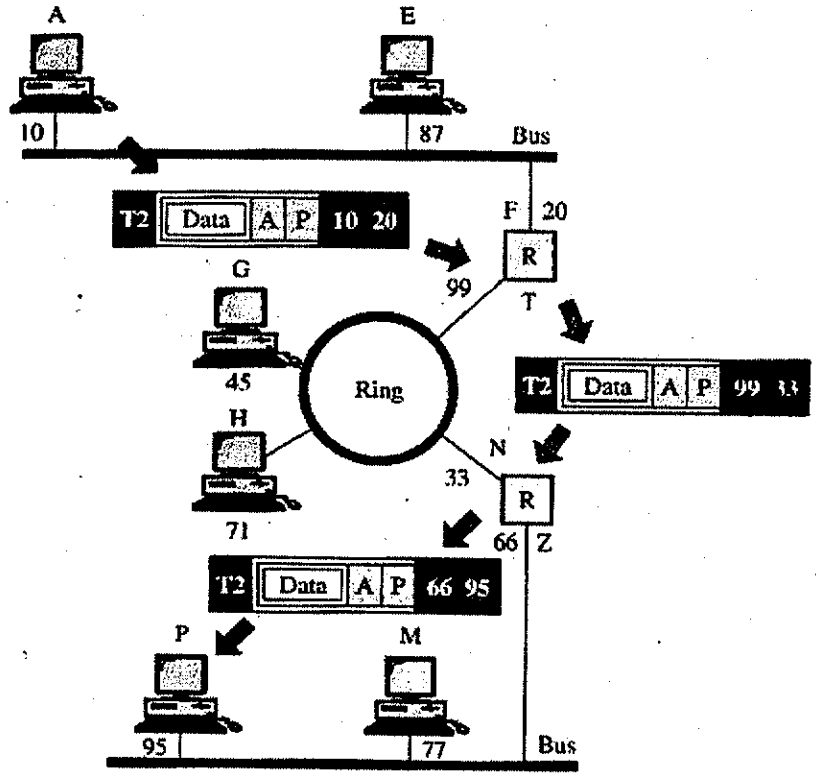
**Định địa chỉ logic**: Địa chỉ vật lý của tầng liên kết dữ liệu chỉ giải quyết được vấn đề định địa chỉ cục bộ trên một mạng nhỏ. Nếu gói dữ liệu được chuyển sang mạng khác, cần có hệ thống địa chỉ khác để phân biệt giữa hệ thống gửi và hệ thống nhận. Tầng mạng bổ sung thêm tiêu đề - có chứa địa chỉ logic của thiết bị nhận và thiết bị gửi vào mỗi gói dữ liệu gửi đi.

**Định tuyến**: Khi mạng hoặc các nút riêng rẽ nối với nhau tạo thành một liên mạng (mạng của các mạng), các thiết bị kết nối trung gian (router hoặc gateway) phải xác định tuyến đường (định tuyến) cho gói dữ liệu để chúng đến được đích.

Giả sử trong Hình 1.18, dữ liệu được gửi từ nút có địa chỉ mạng A với địa chỉ vật lý 10 trong một mạng cục bộ tới nút có địa chỉ mạng P với địa chỉ vật lý 95 trong mạng cục bộ khác. Do hai thiết bị thuộc hai mạng khác nhau, chúng ta không thể chỉ sử dụng địa chỉ vật lý vì địa chỉ vật lý chỉ có tác dụng trong mạng cục bộ. Cái chúng ta cần ở đây là một địa chỉ toàn



thể để có thể chuyển packet giữa các mạng khác nhau. Địa chỉ logic có đặc điểm này. Gói dữ liệu tại tầng mạng chứa địa chỉ logic - địa chỉ này không thay đổi khi packet đi từ nơi gửi đến nơi nhận (A và P). Địa chỉ logic không thay đổi khi gói dữ liệu đi từ mạng này sang mạng khác; ngược lại địa chỉ vật lý thay đổi khi packet đi từ mạng này sang mạng khác. Trong hình vẽ, R là router – kiểu thiết bị này sẽ được mô tả kỹ trong chương 3.

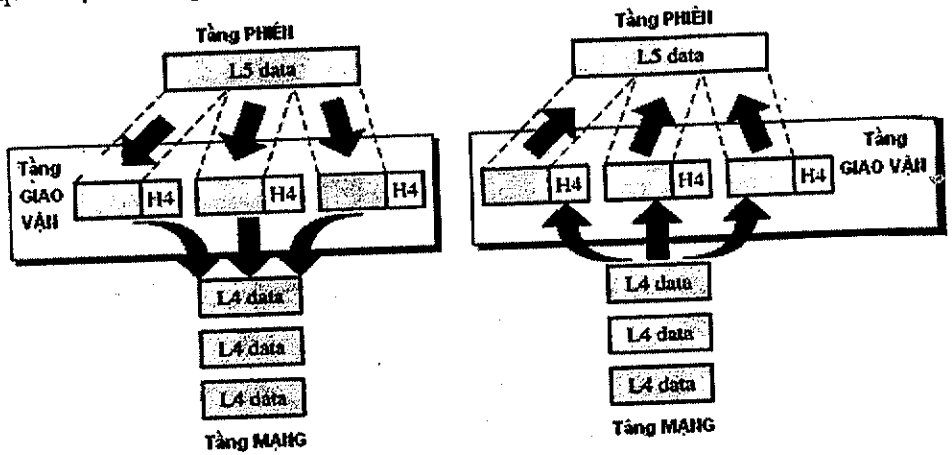



Hình 1.19 Ví dụ về địa chỉ tầng mạng

Các bưu cục sẽ cung cấp dịch vụ giống với tầng mạng. Trong mỗi bưu cục sẽ có một "bảng định tuyến" cho phép bưu tá xác định nơi cần chuyển tiếp bức thư đến. Bức thư sẽ được chuyển đến trạm kế tiếp (bưu cục hay địa chỉ nhận) nhờ vào dịch vụ của tầng liên kết dữ liệu. Rõ ràng rằng thư được chuyển trên các chặng có thể bằng những phương thức hoàn toàn khác nhau (bằng ô tô, máy bay...). Điểm khác biệt duy nhất giữa mạng bưu chính và mạng máy tính là topo của mạng bưu chính gần như không thay đổi theo thời gian, do vậy việc định tuyến gần như là "tĩnh".

## Tầng giao vận

Tầng giao vận chịu trách nhiệm chuyển toàn bộ thông điệp từ nơi gửi đến nơi nhận. Tầng mạng chuyển từng gói dữ liệu riêng lẻ từ nơi gửi đến nơi nhận mà không quan tâm đến quan hệ giữa các gói dữ liệu. Tầng mạng xử lý mỗi gói dữ liệu một cách độc lập mà không quan tâm các gói có thuộc vào cùng một thông điệp hay không. Nói cách khác, tầng giao vận đảm bảo gửi thông điệp đến nơi nhận một cách toàn vẹn. Hình 1.21 minh họa mối quan hệ của tầng giao vận với tầng mạng và tầng phiên.




**Hình 1. 20 Quan hệ giữa tầng giao vận, tầng phiên và tầng mạng**

Tầng giao vận tạo ra một kết nối logic giữa hai cổng đầu cuối: tất cả các gói dữ liệu của cùng một thông điệp được truyền theo đường kết nối đó. Có ba giai đoạn của kết nối: thiết lập kết nối, truyền dữ liệu, giải phóng kết nối. Do phải truyền tất cả các gói dữ liệu trên một kết nối, tầng giao vận còn phải kiểm soát thứ tự truyền, lưu lượng, phát hiện và sửa lỗi.

Tầng giao vận chịu trách nhiệm:

**Địa chỉ cổng (port number)**: Các máy tính thường chạy nhiều chương trình tại cùng một thời điểm. Vì vậy việc chuyển thông điệp không chỉ là truyền dữ liệu từ một máy tính này đến một máy tính khác mà phải chuyển thông điệp từ tiến trình cụ thể trên máy tính này đến tiến trình cụ thể trên máy tính khác. Header được thêm vào tại tầng giao vận phải chứa thông tin về một kiểu địa chỉ - địa chỉ cổng hay địa chỉ tiến trình. Sau khi tầng mạng chuyển gói dữ liệu tới thiết bị nhận, tầng giao vận ở phía nhận phải chuyển toàn bộ thông điệp đến đúng tiến trình nhận.

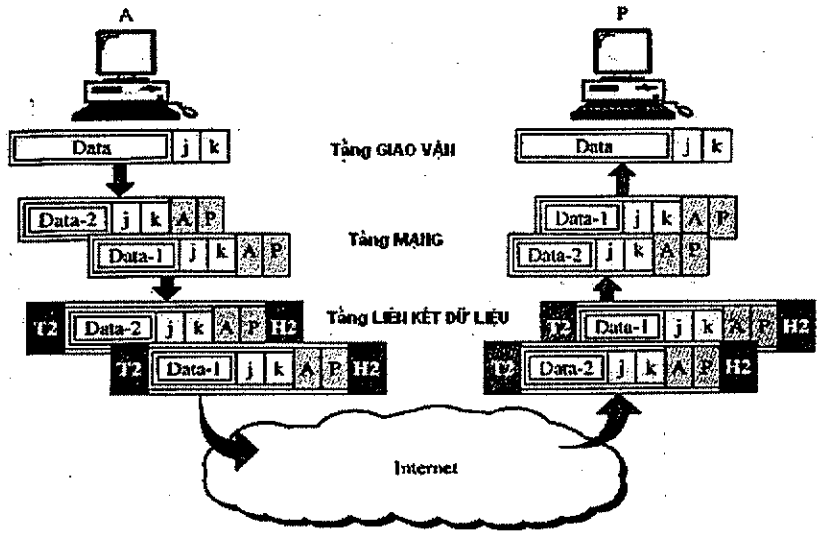


**Phân mảnh và tái hợp nhất**: Mỗi thông điệp được chia thành các đoạn (segment) nhỏ, được truyền độc lập với nhau. Mỗi segment có một số thứ tự cho phép tầng giao vận phía nhận ghép các segment lại thành thông điệp hoàn chỉnh hay phát hiện segment nào bị mất trong khi truyền.

**Kiểm soát kết nối**: Tầng giao vận có thể hướng nối hoặc không hướng nối. Thực thể giao vận không hướng nối xử lý segment như một gói dữ liệu độc lập và chuyển nó đến tầng giao vận của máy nhận. Một tầng giao vận hướng nối thực hiện kết nối với tầng giao vận của máy nhận trước, sau đó mới chuyển các gói dữ liệu đi. Sau khi tất cả dữ liệu được chuyển đi, kết nối được giải phóng.

**Kiểm soát lưu lượng**: Giống như tầng liên kết dữ liệu, tầng giao vận chịu trách nhiệm kiểm soát lưu lượng. Tuy nhiên, việc kiểm soát lưu lượng được thực hiện ở thiết bị đầu cuối chứ không phải trên một đường truyền vật lý.

**Kiểm soát lỗi**: Giống tầng liên kết dữ liệu, tầng giao vận chịu trách nhiệm kiểm soát lỗi. Tuy nhiên việc kiểm soát lỗi ở tầng này được thực hiện tại các thiết bị đầu cuối chứ không phải trên đường truyền trung gian. Tầng giao vận ở phía gửi đảm bảo rằng toàn bộ thông điệp đến tầng giao vận phía nhận là không bị lỗi (hỏng, mất, dư thừa). Việc khắc phục lỗi thường được thực hiện bằng cách yêu cầu truyền lại.



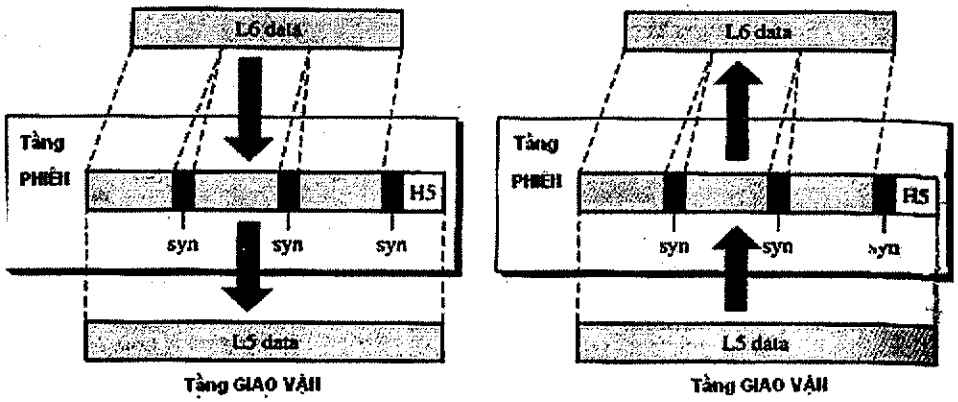

**Hình 1. 21 Ví dụ về tầng giao vận**

Hình 1.20 minh họa tầng giao vận. Dữ liệu đến từ các tầng trên có địa chỉ cổng là j (của ứng dụng gửi) và k (của ứng dụng nhận). Do kích thước dữ liệu lớn hơn khả năng xử lý của tầng mạng, dữ liệu được chia thành hai gói nhỏ, mỗi gói dữ liệu vẫn chứa địa chỉ cổng j và k. Tiếp theo, tại tầng mạng, địa chỉ mạng (A và P) được thêm vào mỗi packet. Các gói dữ liệu có thể đi theo các tuyến đường khác nhau, đến nơi nhận có thể không theo đúng thứ tự. Hai gói dữ liệu được chuyển đến tầng mạng của nơi nhận, tại đây header của tầng mạng được lấy ra khỏi gói dữ liệu. Hai gói dữ liệu tiếp tục được chuyển lên tầng giao vận, tại đây chúng được ghép lại để chuyển lên tầng trên.

Hệ thống bưu cục không có tầng giao vận. Trong ví dụ chuyển thư, tầng giao vận sẽ được triển khai ở người gửi và người nhận thư. Giả sử A gửi thư cho B mỗi ngày một lá thư. Hệ thống bưu cục có thể làm mất, hay gửi trễ một lá thư nào đó. B có thể phát hiện ra điều đó nếu A ghi ngày tháng viết thư trong mỗi lá thư. Nếu B không nhận thư của một ngày nào đó trong một khoảng thời gian tương đối dài, B có thể cho rằng thư đó bị mất và yêu cầu A gửi lại. Nói chung đây sẽ là cơ chế hoạt động của tầng giao vận.

## Tầng phiên

Các dịch vụ của ba tầng đầu (vật lý, liên kết dữ liệu, và mạng) chưa đủ để hai tiến trình trên hai thiết bị có thể truyền thông. Tầng phiên đóng vai trò "kiểm soát viên" hội thoại (dialog) của mạng với nhiệm vụ thiết lập, duy trì và đồng bộ hóa tính liên tác giữa hai bên.




Hình 1. 22 Vai trò của tầng phiên



Tầng phiên chịu trách nhiệm về:

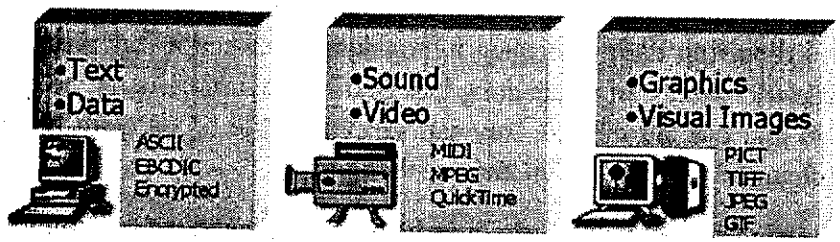
**Kiểm soát hội thoại**: Tầng phiên cho phép hai thực thể (tiến trình) cùng tham gia vào một cuộc hội thoại. Nó cho phép truyền thông giữa hai tiến trình được thực hiện hoặc theo chế độ bán song công hoặc song công. Ví dụ, hội thoại giữa một thiết bị đầu cuối với một mainframe có thể theo kiểu bán song công.

Đồng bộ hóa: Tầng phiên cho phép một tiến trình thêm các mốc (trong thuật ngữ mạng gọi là ***điểm đồng bộ - synchronization point***) vào luồng dữ liệu. Ví dụ, nếu hệ thống cần gửi đi một file có 2000 trang, cứ sau 100 trang nên chèn thêm các điểm đồng bộ để đảm bảo rằng việc nhận từng cụm 100 trang được thực hiện độc lập. Trong trường hợp này nếu như có lỗi khi đang truyền đi trang 523, việc truyền lại sẽ được bắt đầu từ trang 501, không cần phải truyền lại các trang từ 1 đến 500. Hình 1.23 minh họa mối quan hệ giữa tầng phiên và tầng trình diễn.

Trong một công ty nào đó có hai thư ký - một người chuyên nhận thư và một người chuyên gửi thư. Hai người thư ký này đóng vai trò tầng giao vận. Người thư ký trưởng phụ trách cả hai thư ký này đóng vai trò tầng phiên.

## Tầng trình diễn

Tầng trình diễn thực hiện biểu diễn cú pháp và ngữ nghĩa các thông tin được trao đổi giữa hai hệ thống.



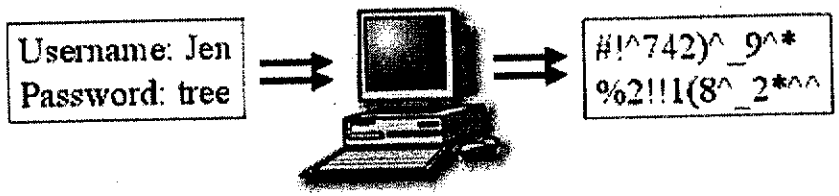

Hình 1. 23 Nhiệm vụ của tầng trình diễn

Tầng trình diễn có nhiệm vụ:

**Phiên dịch (Translation)**: Tiến trình trên hai thiết bị trao đổi các thông tin dưới dạng chuỗi kí tự, số,... Các thông tin này sau đó được chuyển

thành chuỗi bit trước khi truyền. Do các hệ thống máy tính khác nhau sử dụng các hệ thống mã hóa khác nhau, tầng trình diễn chịu trách nhiệm chuyển đổi giữa các cách mã hóa khác nhau. Tầng trình diễn tại phía gửi chuyển thông tin theo khuôn dạng của mình thành thông tin theo khuôn dạng chung. Tầng trình diễn tại máy nhận sẽ chuyển thông tin trong khuôn dạng chung thành thông tin theo khuôn dạng của máy nhận.

**Mã hóa**: Hệ thống phải có khả năng đảm bảo tính bí mật khi chuyển những thông tin quan trọng. Do vậy phía gửi sẽ biến đổi thông tin ban đầu thành một dạng khác và gửi nó đến phía nhận – đây là công việc mã hóa. Phía nhận thực hiện quá trình ngược lại biến thông điệp nhận được thành dạng ban đầu. Quá trình này được gọi là giải mã.




**Hình 1. 24 Mã hóa dữ liệu**

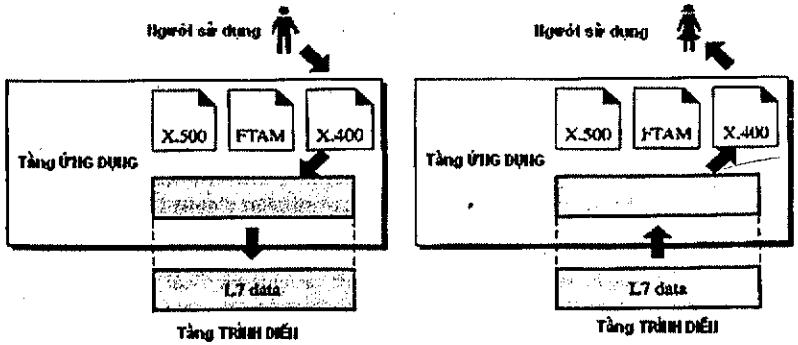
**Nén**: Nén dữ liệu làm giảm số lượng bit trên đường truyền. Nén dữ liệu ngày càng trở nên quan trọng, đặc biệt trong việc truyền các dữ liệu đa phương tiện âm thanh, hình ảnh.

### Tầng ứng dụng

Tầng ứng dụng cho phép người dùng (con người hay phần mềm) truy cập vào mạng bằng cách cung cấp giao diện người sử dụng, hỗ trợ các dịch vụ như gửi thư điện tử, truy cập và chuyển file từ xa, quản lý CSDL dùng chung và một số dịch vụ khác về thông tin.

Hình 1.26 minh họa mối quan hệ giữa tầng ứng dụng với người dùng và với tầng trình diễn. Có rất nhiều ứng dụng có sẵn, ở đây chỉ đề cập đến 3 ứng dụng: X.400 (dịch vụ xử lý thông điệp), X.500 (dịch vụ thư mục), và dịch vụ truy cập, chuyển và quản lý file (FTAM). Người dùng trong ví dụ dưới đây dùng X.400 để gửi đi một thông điệp điện tử. Chú ý rằng tầng ứng dụng sẽ tạo ra dữ liệu thực sự chứ không có các thông tin tiêu đề.






**Hình 1. 25 Tầng ứng dụng**

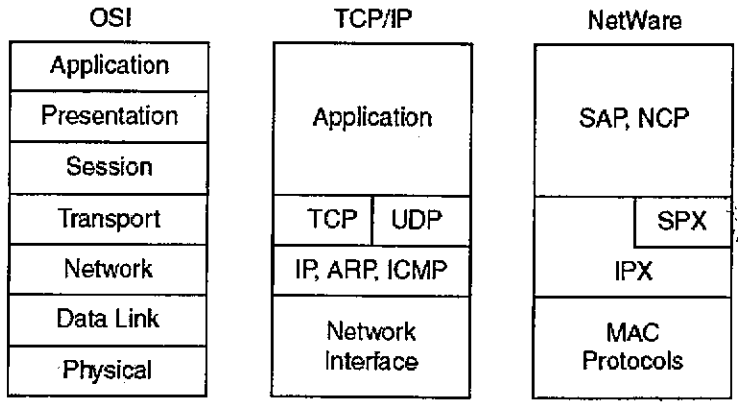
Tầng ứng dụng cung cấp các dịch vụ:

**Thiết bị đầu cuối ảo của mạng**: Thiết bị đầu cuối ảo là phiên bản phần mềm của thiết bị đầu cuối vật lý, cho phép người dùng đăng nhập vào một máy từ xa.

**Quản lý, truy cập và chuyển file**: Ứng dụng cho phép người dùng truy cập file (để viết hoặc đọc dữ liệu), lấy file, quản lý hoặc kiểm soát các file trên máy tính khác.

**Các dịch vụ khác**: Ứng dụng thư tín điện tử cho phép hai người trao đổi thư điện tử với nhau, ứng dụng Web cho phép người sử dụng xem trang Web được lưu trữ trên các server... Số lượng các ứng dụng mạng tăng lên rất nhanh.

## 1.2.3 Bộ giao thức TCP/IP – Mô hình Internet

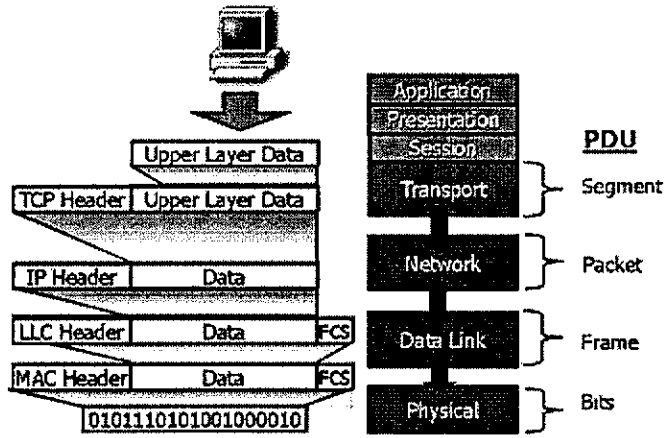



**Hình 1.26 Đối chiếu mô hình OSI, mô hình Internet và NetWare**

Bộ giao thức TCP/IP (được sử dụng trên Internet) ra đời trước khi có mô hình OSI. Các tầng trong bộ giao thức TCP/IP không giống hệt các tầng trong mô hình OSI. Bộ giao thức TCP/IP có 5 tầng: vật lý, liên kết dữ liệu, mạng, giao vận và ứng dụng. Bốn tầng đầu tiên cung cấp các chuẩn vật lý, giao tiếp mạng, liên mạng và chức năng giao vận tương ứng với 4 tầng đầu tiên trong mô hình OSI. Tuy nhiên 3 tầng trên cùng trong mô hình OSI được nhập thành tầng ứng dụng trong mô hình Internet (Hình 1.27).

TCP/IP là giao thức phân cấp, được tạo thành bởi các module độc lập, mỗi module cung cấp một chức năng nhất định, tuy nhiên các module này không nhất thiết phải độc lập với nhau. Mô hình OSI xác định rõ chức năng nào thuộc về tầng nào; trong khi đó các tầng của bộ giao thức TCP/IP chứa các giao thức tương đối độc lập với nhau, nhưng các giao thức này vẫn có thể kết hợp với nhau tùy thuộc nhu cầu hệ thống. Thuật ngữ "phân cấp" mang nghĩa mỗi giao thức ở tầng trên được hỗ trợ bởi một hoặc nhiều giao thức ở tầng dưới.

Tại tầng giao vận, mô hình Internet có hai giao thức: Transmission Control Protocol (TCP) và User Datagram Protocol (UDP). Tại tầng mạng là giao thức Internetworking Protocol, thường được gọi là IP.




**Hình 1. 27 Dữ liệu đi từ trên xuống trong mô hình INTERNET**

## 1.3 PHƯƠNG PHÁP TIẾP CẬN

Trong giáo trình này chúng ta sẽ giới thiệu về các công nghệ mạng theo cách tiếp cận các tầng từ trên xuống. Đầu tiên chúng ta sẽ học về tầng ứng dụng, giao vận, mạng và cuối cùng là liên kết dữ liệu. Chúng ta sẽ sử dụng mô hình Internet làm trọng tâm.



# Chương 2
# TẦNG ỨNG DỤNG

## 2.1 GIAO THỨC TẦNG ỨNG DỤNG

Sự phồng phú của các ứng dụng mạng chính là động lực phát triển của mạng máy tính. Có lẽ nếu không có chúng thì cũng sẽ không có các giao thức mạng. Trong hơn ba mươi năm qua, có nhiều phát minh đột phá trong việc phát triển các ứng dụng mạng. Bắt đầu từ thập niên 80, những ứng dụng đơn giản tương tác với người dùng qua chế độ lệnh (text-based) đã trở nên phổ biến như truy cập máy tính từ xa (telnet), thư điện tử (email), truyền file (ftp), nhóm thông tin (newsgroup), và trò chuyện từ xa (chat). Hiện nay, những ứng dụng đa phương tiện phức tạp hơn như World Wide Web, điện thoại trực tuyến, hội thảo từ xa, chia sẻ file... đã ngày càng trở nên quen thuộc.

Mặc dù chương trình ứng dụng mạng có nhiều loại khác nhau, có thể có nhiều thành phần tương tác với nhau, nhưng "lõi" của chúng là phần mềm. Phần mềm ứng dụng mạng được cài đặt phân tán trên các **thiết bị đầu cuối (end-system)** như máy tính, điện thoại di động... Ví dụ, với Web, có hai phần mềm tương tác với nhau: phần mềm trình duyệt trong máy tính của người dùng (PC, Mac, hay trạm làm việc) và phần mềm Web server.

Trong thuật ngữ hệ điều hành, việc kết nối được thực hiện giữa các **tiến trình** (process) chứ không phải giữa các chương trình phần mềm. Tiến trình là một chương trình chạy trên thiết bị đầu cuối. Khi các tiến trình chạy trên cùng một thiết bị, chúng sẽ kết nối, trao đổi dữ liệu với nhau thông qua cơ chế truyền thông liên tiến trình (interprocess communication). Chính hệ điều hành của thiết bị sẽ kiểm soát cơ chế này. Trong cuốn sách này chúng

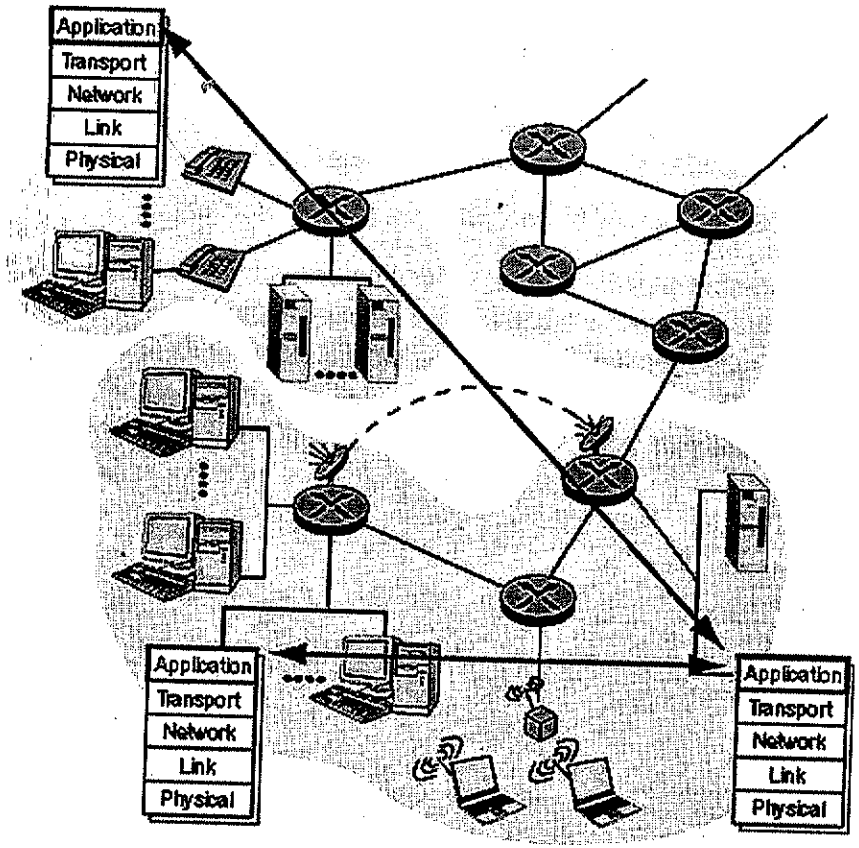
ta không quan tâm đến cách thức tiến trình trên cùng một máy tính kết nối với nhau như thế nào, mà chỉ quan tâm đến việc kết nối giữa các tiến trình trên những thiết bị khác nhau (và có thể trên những hệ điều hành khác nhau). Việc kết nối như vậy sẽ được thực hiện bằng cách trao đổi thông điệp qua mạng máy tính. Tiến trình gửi sẽ tạo và gửi thông điệp qua mạng, tiến trình nhận sẽ nhận thông điệp (message) và có thể phản hồi lại bằng cách gửi một thông điệp trả lời (xem Hình 2.1). Ứng dụng mạng có các giao thức định nghĩa khuôn dạng, thứ tự trao đổi các thông điệp cũng như hành vi của mỗi bên khi nhận được thông điệp.

Tầng ứng dụng là nơi đơn giản nhất để bắt đầu nghiên cứu về giao thức. Chúng ta sẽ làm quen với một vài ứng dụng cũng như các giao thức giữa chúng. Điều này giúp ta hiểu rõ hơn về giao thức.

## 2.1.1 Giao thức tầng ứng dụng

Cần phân biệt ứng dụng mạng và giao thức tầng ứng dụng. Giao thức tầng ứng dụng chỉ là một phần (cho dù là phần quan trọng) của ứng dụng mạng. Ví dụ Web - ứng dụng mạng cho phép người dùng lấy các đối tượng từ Web server bao gồm nhiều thành phần, như tiêu chuẩn định dạng văn bản (HTML), trình duyệt Web (Netscape Navigator hay Microsoft Internet Explorer), Web server (Apache, Microsoft, và Netscape server), và giao thức tầng ứng dụng. Giao thức tầng ứng dụng của Web–HTTP (HyperText Transfer Protocol [RFC 2616]), định nghĩa cách thức chuyển thông điệp giữa Web client (trình duyệt) và Web server. Như vậy HTTP chỉ là một phần của ứng dụng Web. Một ví dụ khác là ứng dụng thư điện tử. Thư điện tử cũng có nhiều thành phần, bao gồm mail server có chức năng như một hòm thư, mail reader cho phép người dùng đọc và gửi thư, chuẩn định nghĩa cấu trúc của thư điện tử và giao thức tầng ứng dụng định nghĩa cách thức chuyển thông điệp giữa mail server và mail reader, cũng như ý nghĩa của một số trường trong thư (ví dụ các tiêu đề thư: người nhận, người gửi...). Giao thức tầng ứng dụng cho thư điện tử là SMTP (Simple Mail Transfer Protocol [RFC 821]). Do đó, SMTP chỉ là một phần (cho dù quan trọng) của ứng dụng thư điện tử.






**Hình 2.1 Các ứng dụng trên mạng**

Như đã nói ở trên, giao thức tầng ứng dụng định nghĩa cách thức truyền thông điệp giữa các tiến trình ứng dụng chạy trên các thiết bị khác nhau. Nó xác định:

Kiểu thông điệp trao đổi, ví dụ như thông điệp yêu cầu hay thông điệp trả lời.

Cú pháp của thông điệp, ví dụ các trường trong thông điệp cũng như cách xác định chúng.

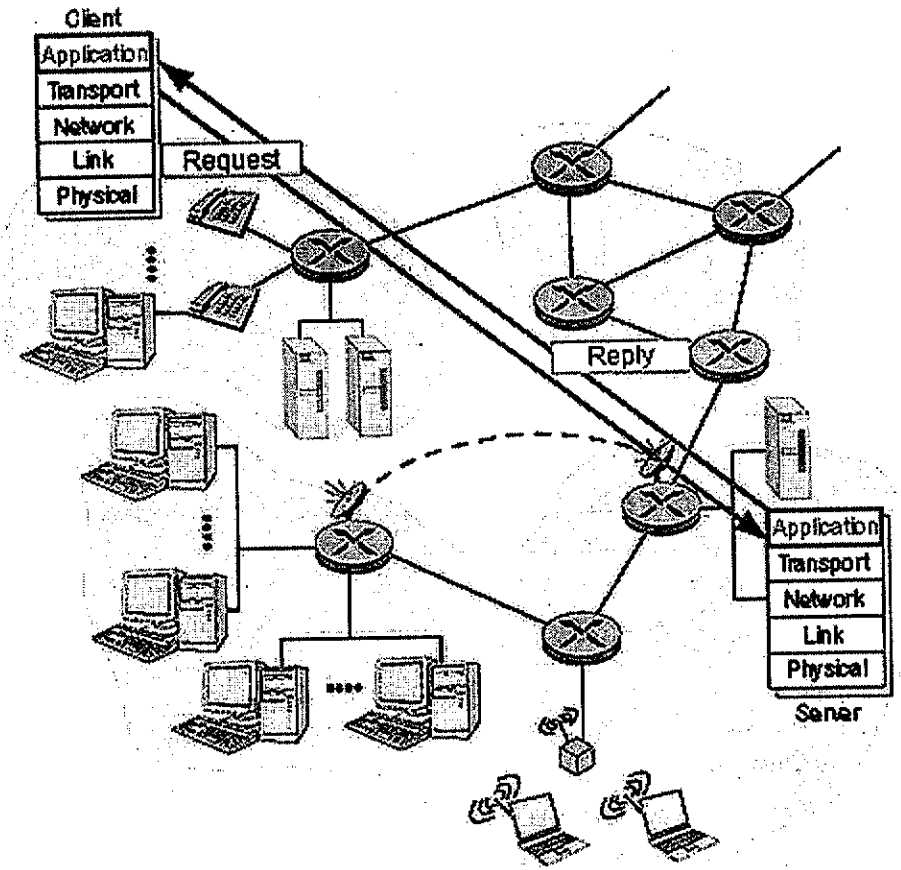
Ý nghĩa của các trường.

Qui tắc xác định khi nào và như thế nào tiến trình gửi và trả lời thông điệp.

Nhiều giao thức tầng ứng dụng được đặc tả trong các RFC. Ví dụ, đặc tả của HTTP là HTTP RFC. Nếu người thiết kế trình duyệt tuân theo các qui tắc của HTTP RFC, trình duyệt sẽ có thể lấy được trang Web từ bất kỳ Web server nào tuân theo các qui tắc HTTP RFC.

### Mô hình Khách hàng / Người phục vụ (Client/Server)

Giao thức ứng dụng mạng thường chia ra hai phần hay hai phía, phía client và phía server (Xem Hình 2.2). Phía client trong thiết bị này liên lạc với phía server trong thiết bị khác. Ví dụ, trình duyệt Web là phía client, và Web server là phía server của HTTP. Trong ứng dụng thư điện tử, mail server gửi thư là phía client và mail server nhận thư là phía server của SMTP.



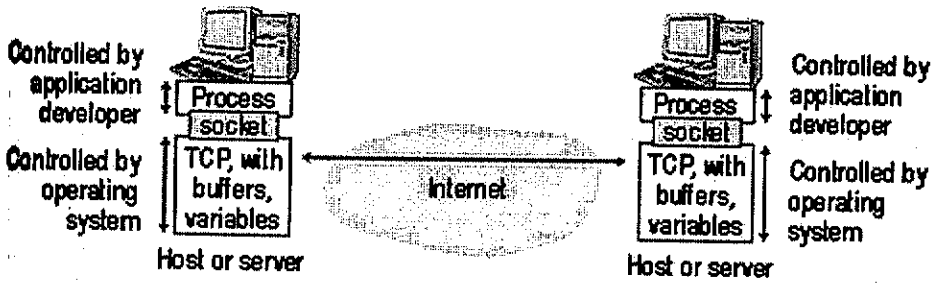

Hình 2.2 Tương tác client/server



Trong nhiều ứng dụng, máy tính sẽ thực hiện cả phần client và phần server của ứng dụng. Ví dụ xét phiên làm việc Telnet giữa máy A và máy B. (Telnet là ứng dụng đăng nhập từ xa). Nếu máy A bắt đầu trước (có nghĩa là người dùng ở máy A đăng nhập vào máy B), khi đó máy A chạy phía client và máy B chạy phía server của ứng dụng. Mặt khác, nếu máy B bắt đầu trước thì máy B chạy phía client của ứng dụng. Một ví dụ khác, FTP - được dùng để truyền file giữa hai máy. Sau khi thiết lập phiên làm việc FTP giữa hai máy tính, mỗi máy đều có thể truyền file tới máy kia trong suốt phiên làm việc. Tuy nhiên giống như hầu hết các ứng dụng mạng, máy nào bắt đầu trước được coi là client. Hơn nữa, máy tính có thể chạy cả phía client và server tại cùng một thời điểm. Ví dụ, mail server chạy phía client của SMTP khi gửi thư và chạy phía server của SMTP khi nhận thư.

### Truyền thông giữa các tiến trình

Ứng dụng bao gồm hai tiến trình trên hai thiết bị khác nhau và liên lạc với nhau qua mạng. Hai tiến trình liên lạc với nhau bằng cách gửi và nhận thông điệp qua socket của chúng. Socket có thể xem như "cửa" của tiến trình vì tiến trình nhận và gửi thông điệp thông qua "cửa". Khi muốn gửi thông điệp tới tiến trình khác, tiến trình đẩy thông điệp cần gửi qua "cửa" với giả định rằng thực thể giao vận nằm bên kia "cửa" sẽ chuyển thông điệp đến "cửa" của tiến trình nhận.




Hình 2.3 Tiến trình ứng dụng, socket và giao thức giao vận

Hình 2.3 minh hoạ truyền thông qua socket giữa hai tiến trình trên Internet. (Tầng giao vận trên hình 2.3 là TCP, mặc dù ở đây có thể sử dụng giao thức khác như UDP). Qua hình vẽ ta thấy socket là giao diện giữa tầng ứng dụng và tầng giao vận trong máy tính. Nó được xem là API (giao diện lập trình ứng dụng) giữa ứng dụng và mạng. Người thiết kế ứng dụng kiểm

soát mọi khía cạnh phía bên trên socket – là tầng ứng dụng - nhưng chỉ có khả năng kiểm soát rất ít tầng giao vận phía dưới socket. Với tầng giao vận, người lập trình ứng dụng chỉ có thể kiểm soát được: (1) chọn giao thức giao vận nào và (2) xác định một vài tham số ở tầng giao vận như độ lớn bộ đệm và kích thước tối đa của gói tin. Khi người lập trình lựa chọn giao thức giao vận nào, ứng dụng được tạo ra sử dụng tầng giao vận ứng với giao thức đó. Chúng ta sẽ xem xét tỉ mỉ về socket trong phần sau.

**Địa chỉ tiến trình**

Để gửi thông điệp cho tiến trình trên máy tính khác thì tiến trình gửi phải xác định được tiến trình nhận. Tiến trình được xác định qua hai phần: (1) tên hay địa chỉ của máy tính, và (2) định danh xác định tiến trình trên máy tính nhận.

Đầu tiên chúng ta hãy xét địa chỉ máy tính. Trong ứng dụng Internet, máy tính được xác định qua địa chỉ IP. Địa chỉ IP sẽ được học trong chương 4. Bây giờ chúng ta chỉ cần biết địa chỉ IP là một số 32 bit dùng để xác định duy nhất một thiết bị (chính xác hơn, nó xác định duy nhất giao diện (interface) của thiết bị kết nối vào Internet). Vì địa chỉ IP của thiết bị mang tính xác định duy nhất, nên việc phân phối địa chỉ IP được quản lý chặt chẽ. Mạng ATM có một chuẩn địa chỉ khác. ITU-T lấy số điện thoại làm địa chỉ, gọi là địa chỉ E.164 [ITU 1997] sử dụng trên mạng ATM.

Ngoài địa chỉ thiết bị nhận, phía gửi phải thêm vào thông tin giúp phía nhận chuyển tiếp thông điệp cho tiến trình phù hợp (vì trong máy tính nhận có thể có nhiều tiến trình đồng thời hoạt động). Thông tin này là cổng phía nhận (destination port). Các giao thức tầng ứng dụng phổ biến đều được gán số hiệu cổng (port number) là một số cụ thể. Ví dụ, tiến trình Web server (giao thức HTTP) sử dụng cổng 80. Tiến trình mail server (giao thức SMTP) sử dụng cổng 25. Danh sách các cổng cho tất cả giao thức thường gặp trên Internet được liệt kê trong RFC 1700. Khi xây dựng ứng dụng mạng mới thì ứng dụng đó phải được đăng kí một số hiệu cổng mới.

**Chương trình giao tiếp người dùng (user agent)**

Trước khi bắt đầu trình bày các giao thức tầng ứng dụng, chúng ta phải nói tới khái niệm user agent. User agent là giao diện giữa người dùng



và ứng dụng mạng. Ví dụ trong ứng dụng Web, user agent là chương trình trình duyệt như Netscape Navigator hay Microsoft Internet Explorer. Trình duyệt cho phép người dùng xem trang Web, duyệt trên Web, cung cấp dữ liệu vào các form, tương tác với Java... Trình duyệt là phía client trong giao thức HTTP. Do đó khi kích hoạt, trình duyệt là tiến trình cung cấp giao diện cho người dùng, thay mặt người dùng nhận và gửi thông điệp qua socket, hiển thị thông điệp trả lời cho người dùng xem (chẳng hạn diễn dịch các mã HTML). Trong ứng dụng thư điện tử, user agent là mail reader, cho phép người dùng soạn và đọc thư. Một số phần mềm mail reader (như Eudora, Netscape Messenger, Microsoft Outlook) với hệ giao tiếp đồ hoạ có thể chạy trên PC, Mac. Mail reader chạy trên PC là phía client của giao thức tầng ứng dụng SMTP khi gửi thư và phía client của giao thức lấy thư (POP3 hoặc IMAP (xem phần 2.4)), khi nhận thư từ mail server.

## 2.1.2 Các yêu cầu của ứng dụng

Socket là giao diện giữa tiến trình ứng dụng và thực thể giao vận. Ứng dụng gửi thông điệp qua "cửa". Ở sau cánh cửa thực thể giao vận có trách nhiệm chuyển thông điệp qua mạng máy tính tới "cửa" tiến trình nhận. Nhiều kiểu mạng, kể cả Internet, có nhiều kiểu giao thức giao vận khác nhau. Khi thiết kế ứng dụng, bạn phải lựa chọn một giao thức giao vận có sẵn nào đó. Bạn thực hiện lựa chọn này như thế nào? Đầu tiên cần nghiên cứu các dịch vụ được các giao thức giao vận cung cấp, và sau đó sẽ chọn giao thức đáp ứng đầy đủ nhất các yêu cầu của mình. Điều này tương tự như việc chọn tàu hoả hay máy bay để di chuyển giữa hai thành phố (như Hà Nội và Huế). Bạn phải chọn một trong hai phương tiện và mỗi phương tiện cung cấp một dịch vụ khác nhau. (Ví dụ, tàu hoả giá rẻ trong khi máy bay tiết kiệm thời gian).

Ứng dụng đòi hỏi dịch vụ gì của giao thức giao vận? Về đại thể chúng ta có thể phân loại theo ba nhóm: mất mát dữ liệu, băng thông, và thời gian.

**Mất mát dữ liệu (Data loss)**

Một số ứng dụng như thư điện tử, truyền file, truy cập từ xa, truyền các đối tượng Web, và ứng dụng tài chính đòi hỏi dữ liệu phải được truyền

chính xác và đầy đủ, tức là không được mất dữ liệu. Đặc biệt, mất mát file dữ liệu hoặc dữ liệu trong các giao dịch tài chính có thể gây nên hậu quả nghiêm trọng. Tuy nhiên một số ứng dụng khác như ứng dụng đa phương tiện (real-time audio/video hay stored audio/video) chấp nhận mất mát dữ liệu. Trong các ứng dụng kiểu này, mất mát dữ liệu có thể gây nên một số nhiễu trong dữ liệu đa phương tiện – nhưng điều này có thể chấp nhận được trong giới hạn nào đó. Ảnh hưởng do mất mát dữ liệu tới chất lượng ứng dụng cũng như số lượng cho phép các gói dữ liệu bị mất phụ thuộc vào chính ứng dụng và phương pháp mã hoá.

**Băng thông (bandwith)**

Để hoạt động hiệu quả, một số ứng dụng phải truyền dữ liệu với một tốc độ nhất định. Ví dụ, ứng dụng gọi điện thoại qua Internet (Internet telephony) mã hoá âm thanh với tốc độ 32Kbs, thì sau đó dữ liệu tạo ra phải được chuyển tới ứng dụng nhận với tốc độ trên. Nếu không có đủ băng thông cần thiết, ứng dụng cần phải mã hoá âm thanh với tốc độ khác hay phải kết thúc - bởi vì nếu không đủ băng thông thì ứng dụng không thể đáp ứng yêu cầu người sử dụng. Những ứng dụng đa phương tiện hiện nay là ứng dụng phụ thuộc vào băng thông (bandwidth sensitive), nhưng trong tương lai ứng dụng đa phương tiện sẽ sử dụng các kỹ thuật mã hoá thích nghi để mã hoá tốc độ cho phù hợp với dải tần hiện có.

**Thời gian (timing)**

Những ứng dụng thời gian thực (real-time) mang tính chất tương tác, như Internet telephone, hội thảo qua điện thoại, hay các trò chơi nhiều người tham gia cùng một lúc (multiplayer game) yêu cầu những ràng buộc chặt chẽ về thời gian trong việc trao đổi dữ liệu. Ví dụ, những ứng dụng này đòi hỏi độ trễ (delay) từ tiến trình gửi đến tiến trình nhận không vượt quá vài trăm phần nghìn giây. Độ trễ lớn trong ứng dụng Internet telephony khiến cuộc đàm thoại bị đứt đoạn giữa chừng. Trong trò chơi nhiều người cùng tham gia hay trong môi trường tương tác ảo, độ trễ từ lúc đưa ra yêu cầu cho đến khi nhận được kết quả phản ứng từ môi trường (ví dụ, từ một người chơi khác) lớn sẽ làm giảm tính chân thực của trò chơi. Đối với ứng dụng không tính đến yếu tố thời gian thực, người ta vẫn mong muốn có một độ trễ thấp, song không có ràng buộc chặt chẽ đối với độ trễ.



Hình 2.4 tóm tắt các yếu tố như độ tin cậy, băng thông, và các đòi hỏi về thời gian của một số ứng dụng Internet phổ biến. Hình 2.4 chỉ phác hoạ một vài đòi hỏi quan trọng của những ứng dụng Internet này. Ở đây chúng ta không có đầy đủ các phân loại hoàn chỉnh, nhưng cũng đủ để nhận biết một vài đặc trưng quan trọng nhất để phân loại ứng dụng.

| Ứng dụng | Mất mát dữ liệu | Băng tần | Thời gian |
|---|---|---|---|
| File transfer | Không | Elastic | Không |
| E-mail | Không | Elastic | Không |
| Web Documents | Không | Elastic (few Kbps) | Không |
| Real-time Audio/Video | Chấp nhận mất mát | Audio: Few Kbps - 1Mb<br>Video: 10Kb-5 Mb | Có: 100s of msec |
| Stored Audio/Video | Chấp nhận mất mát | Same as Above | Có: Few Seconds |
| Interactive games | Chấp nhận mất mát | Few Kbps - 10Kb | Có: 100s of msec |
| Financial Applications | Không | Elastic | Có hoặc Không |

**Hình 2.4 Các yêu cầu cho một số ứng dụng**

## 2.1.3 Dịch vụ của các giao thức giao vận Internet

Internet (và nói chung TCP/IP) cung cấp hai giao thức giao vận cho tầng ứng dụng: UDP và TCP. Khi xây dựng ứng dụng cho Internet, một trong những quyết định đầu tiên mà nhà thiết kế phải đưa ra là sử dụng UDP hay TCP. Mỗi giao thức cung cấp một kiểu phục vụ khác nhau cho ứng dụng.

**TCP**

Đặc trưng của giao thức TCP là hướng kết nối và cung cấp dịch vụ truyền dữ liệu tin cậy. Khi sử dụng giao thức giao vận TCP, ứng dụng sẽ nhận được cả hai loại dịch vụ này.

### *Dịch vụ hướng nối (connection oriented)*

TCP client và TCP server trao đổi các thông tin điều khiển với nhau trước khi truyền dữ liệu ứng dụng. Quá trình "bắt tay" giữa client và server như vậy cho phép cả hai bên sẵn sàng xử lý các gói dữ liệu. Sau quá trình này, xuất hiện một đường kết nối TCP (TCP connection) giữa socket của hai tiến trình. Đây là **kết nối hai chiều (song công – full duplex)** vì cho phép hai tiến trình có thể đồng thời gửi và nhận thông điệp. Khi ứng dụng kết thúc việc gửi thông điệp, nó đóng kết nối lại. Dịch vụ này chỉ là hướng kết nối chứ không phải mạch ảo (virtual circuit) bởi vì hai tiến trình được kết nối một cách lỏng lẻo. Trong chương 3, chúng ta sẽ thảo luận chi tiết về dịch vụ hướng nối và cách thực hiện chúng.

### *Dịch vụ giao vận tin cậy*

Tiến trình gửi có thể sử dụng TCP để truyền dữ liệu chính xác và đúng thứ tự. Gửi đi một luồng byte qua socket, tiến trình ứng dụng có thể tin tưởng TCP sẽ chuyển luồng byte này đến socket nhận, không bị lỗi hay trùng lặp byte.

TCP cũng có cơ chế kiểm soát tắc nghẽn, cơ chế này đáp ứng cho cả Internet chứ không phải cho hai tiến trình truyền thông với nhau. Kỹ thuật kiểm soát tắc nghẽn của TCP là giảm tốc độ gửi dữ liệu của mỗi tiến trình (client hay server) khi mạng bị tắc nghẽn. Đặc biệt, như chúng ta sẽ thấy trong chương 3, cơ chế kiểm soát tắc nghẽn của TCP cố gắng giới hạn mỗi kết nối TCP để chia sẻ công bằng băng thông giữa các tiến trình.

Giới hạn tốc độ truyền có thể không thoả mãn với các ứng dụng audio và video theo thời gian thực, những ứng dụng đòi hỏi phải có một băng thông tối thiểu. Hơn nữa, ứng dụng thời gian thực chấp nhận mất mát dữ liệu và không thực sự cần đến một dịch vụ giao vận tin cậy hoàn toàn. Vì các lý do đó, các ứng dụng thời gian thực thường chạy trên nền UDP.

Bây giờ chúng ta trình bày một số dịch vụ mà TCP không cung cấp. Thứ nhất, TCP không bảo đảm một tốc độ truyền tối thiểu. Tiến trình gửi không được phép truyền với bất kỳ tốc độ nào nó đề nghị, tốc độ này được kiểm soát bởi cơ chế kiểm soát tắc nghẽn của TCP. Đôi khi cơ chế này khiến tiến trình gửi phải gửi với tốc độ trung bình tương đối thấp. Thứ hai, TCP không đưa ra bất kỳ sự bảo đảm nào về độ trễ. Khi tiến trình gửi chuyển dữ liệu cho socket TCP, dữ liệu cuối cùng sẽ đến được socket nhận nhưng TCP



không bảo đảm dữ liệu sau bao lâu mới tới được đích. Với những quan sát trên môi trường Internet thực, có thể phải chờ vài giây thậm chí đến vài phút để TCP gửi thành công một thông điệp (ví dụ một trang Web HTML từ Web server đến Web client). Nói tóm lại, TCP bảo đảm việc truyền tất cả dữ liệu một cách chính xác, nhưng không bảo đảm về tốc độ truyền và độ trễ.

### Dịch vụ UDP

UDP là giao thức giao vận khá đơn giản với mô hình phục vụ tối thiểu. UDP không hướng nối, nghĩa là không có giai đoạn "bắt tay" trước khi hai tiến trình bắt đầu trao đổi dữ liệu. UDP không cung cấp dịch vụ truyền tin cậy. Khi tiến trình gửi chuyển thông điệp qua cổng UDP, UDP không đảm bảo thông điệp sẽ đến được cổng tiến trình nhận. Hơn nữa, các thông điệp đến đích có thể không đúng thứ tự.

Mặt khác, UDP không có cơ chế kiểm soát tắc nghẽn, vì vậy tiến trình gửi có thể đẩy dữ liệu ra cổng UDP với tốc độ bất kì. Mặc dù không phải tất cả dữ liệu đều tới được đích, nhưng phần lớn dữ liệu có thể tới được. Ứng dụng thời gian thực thường lựa chọn UDP ở tầng giao vận. Giống TCP, UDP không bảo đảm về độ trễ.

Hình 2.5 trình bày các giao thức giao vận của các ứng dụng mạng phổ biến. Thư điện tử, truy cập từ xa, Web, và truyền file sử dụng TCP do TCP cung cấp dịch vụ truyền dữ liệu tin cậy, bảo đảm rằng mọi dữ liệu sẽ tới được đích.

| Ứng dụng | Giao thức ứng dụng | Giao thức giao vận |
|---|---|---|
| Thư điện tử | SMTP [RFC 821] | TCP |
| Truy cập từ xa | Telnet [RFC 854] | TCP |
| Web | HTTP [RFC 2068] | TCP |
| Truyền file | FTP [RFC 959] | TCP |
| Remote File Server | NFS | UDP hoặc TCP |
| Streaming Multimedia | Giao thức riêng, không công bố (ví dụ Real Networks) | UDP hoặc TCP |
| Điện thoại Internet | Giao thức riêng, không công bố (ví dụ Vocaltec) | Thường là UDP |

**Hình 2.5 Các ứng dụng phổ biến và giao thức giao vận tương ứng**

Chúng ta cũng thấy rằng điện thoại qua Internet chạy trên nền UDP. Mỗi phía của ứng dụng này cần gửi dữ liệu qua mạng với tốc độ tối thiểu nào đó (Xem Hình 2.5). Hơn nữa, ứng dụng điện thoại qua Internet chấp nhận mất mát dữ liệu, vì thế chúng không cần dịch vụ truyền tin cậy của TCP.

Như đã lưu ý trước, TCP và UDP đều không bảo đảm về thời gian. Điều này có nghĩa là ứng dụng có ràng buộc về thời gian không thể chạy trên mạng ngày nay? Câu trả lời chắc chắn là không - Internet đã có một kế hoạch cho ứng dụng kiểu này trong nhiều năm tới.

### 2.1.4 Một số ứng dụng phổ biến

Các kiểu ứng dụng mạng ngày càng đa dạng và phong phú. Chúng ta sẽ tập trung nghiên cứu một số ứng dụng quan trọng thường gặp. Trong chương này chúng ta sẽ trình bày khá chi tiết bốn ứng dụng phổ biến: Web, truyền file, thư điện tử và dịch vụ tên miền (DNS). Web là ứng dụng đầu tiên là vì Web cực kỳ phổ biến và giao thức tầng ứng dụng của nó - HTTP, tương đối đơn giản và minh hoạ nhiều đặc trưng cơ bản của giao thức. Sau đó là ứng dụng truyền file, bởi vì ứng dụng này có nhiều đặc điểm trái ngược với HTTP. Chúng ta cũng sẽ nghiên cứu thư điện tử, một trong những ứng dụng xuất hiện đầu tiên và thông dụng nhất của Internet. Thư điện tử ngày nay sử dụng nhiều giao thức tầng ứng dụng. Web, truyền file, và thư điện tử đều yêu cầu dịch vụ truyền tin cậy, không có yêu cầu ràng buộc thời gian và yêu cầu về băng thông. Do vậy ba ứng dụng này sử dụng TCP ở tầng giao vận. Ứng dụng thứ tư là DNS (Domain Name System) cung cấp dịch vụ chỉ dẫn. Người dùng không tương tác trực tiếp với DNS mà yêu cầu dịch vụ DNS gián tiếp thông qua ứng dụng khác (ví dụ Web, truyền file, và thư điện tử). DNS minh hoạ cách thức triển khai một cơ sở dữ liệu phân tán trên mạng. Cả bốn ứng dụng trên không có yêu cầu chặt chẽ về thời gian. Các ứng dụng yêu cầu về thời gian được trình bày trong chương 6.





Tháng 4/1994, Marc Andreesen, chuyên viên máy tính (người sau này tạo ra trình duyệt Mosaic tại trường đại học Illinois•bang Urbana) cùng với Jim Clark - người sáng lập công ty Silicon Graphic (là cựu giáo sư Stanford) sáng lập tập đoàn truyền thông Nestcape. Nestcape sau đó tuyển dụng nhiều người trong nhóm dự án Mosaic ở trường đại học Illinois và cho ra đời phiên bản Beta của trình duyệt Nivigator 1.0 vào tháng 10 năm 1994. Trong những năm sau, Nestcape đã cải tiến đáng kể trình duyệt của mình, phát triển phần mềm Web server, commerce server, mail server, proxy server, mail reader và nhiều sản phẩm phần mềm ứng dụng khác. Netscape là một trong những công ty kinh doanh trên Internet đổi mới và thành công nhất trong giữa thập niên 90. Tháng 1 năm 1995, Barksdale trở thành tổng giám đốc của Nestcape và vào tháng 8, Nestcape bắt đầu bán cổ phiếu của mình trên thị trường .

Microsoft khởi đầu tương đối chậm trong lĩnh vực Internet khi đưa ra trình duyệt đầu tiên của mình - Internet Explorer 1.0 vào tháng 8 năm 1995. Internet Explorer cồng kềnh và chạy chậm nhưng Microsoft đã đầu tư lớn vào đây để đến năm 1997, Microsoft và Nestcape trở thành "kỳ phùng địch thủ" cạnh tranh thị trường trình duyệt. Ngày 11 tháng 6 năm 1997, Nestcape công bố phiên bản trình duyệt 4.0 và vào ngày 30 tháng 10 Microsoft đưa ra trình duyệt phiên bản 4.0. Tại thời điểm đó, khó có thể xác định chất lượng của trình duyệt nào tốt hơn và Microsoft - với sự thống trị của hệ điều hành Windows liên tục giành thêm được nhiều thị phần. Vào năm 1997, Nestcape mắc phải một số sai lầm nghiêm trọng trong đó có việc đầu tư rất lớn vào trình duyệt hỗ trợ JAVA. Trong suốt năm 1998, Nescape tiếp tục để mất thị phần trình duyệt Web và cả các sản phẩm khác. Cuối năm 1998 American Online đã mua lại Netscape. Marc Andreesen và các cộng sự ban đầu rời bỏ Netscape.

## 2.2 WORLD WIDE WEB: HTTP

Cho đến những năm 1990, Internet chỉ được sử dụng trong các cơ quan nghiên cứu, trường đại học với các dịch vụ đơn giản như truy cập từ xa, truyền file, nhận và gửi thư điện tử. Mặc dù những ứng dụng này đã (và vẫn) cực kỳ phổ biến - nhưng về cơ bản Internet vẫn chỉ được biết tới trong cộng đồng nghiên cứu. Vào đầu thập niên 90, ứng dụng quan trọng nhất của Internet - World Wide Web xuất hiện, và nhanh chóng được mọi người chấp nhận. Nó thay đổi cách thức tương tác giữa con người và môi trường làm việc. Chính điều này đã giúp đưa Internet từ một trong rất nhiều mạng thông tin (ví dụ mạng trực tuyến Prodigy, American Online hay Compuserve, hệ

thống thông tin quốc gia: Minitee/Tranpac ở Pháp, Private X25, Rrame Relay) thành một mạng thống nhất duy nhất.

Lịch sử phát triển của công nghệ viễn thông ảnh hưởng lớn đến xã hội loài người. Công nghệ đầu tiên là điện thoại - được phát minh vào năm 1870. Điện thoại cho phép hai người nói chuyện trực tiếp mà không cần ở trong cùng một vùng. Nó có những ảnh hưởng cả tốt lẫn xấu đến xã hội. Công nghệ tiếp theo là truyền thanh, truyền hình - ra đời vào những năm 1920-1930. Nó giúp con người thu nhận một lượng thông tin rất lớn bằng âm thanh và hình ảnh, và tác động lớn đến xã hội. Có lẽ công nghệ thứ ba làm thay đổi cuộc sống và công việc của con người chính là Web. Sức lôi cuốn của Web đối với con người là ở chỗ Web hoạt động theo yêu cầu (on demand). Nghĩa là có thể nhận được thông tin cần thiết vào các thời điểm cần thiết. Điều này khác so với công nghệ quảng bá (truyền thanh, truyền hình) chỉ phát đi những nội dung có sẵn tại những thời điểm định trước. Ngoài ra Web có nhiều đặc điểm lý thú khác. Ai cũng có thể dễ dàng trở thành các nhà xuất bản; các siêu liên kết và các công cụ tìm kiếm giúp ta tìm kiếm qua nhiều trang Web. Các hình ảnh đồ hoạ và hoạt hình "khuấy động" thị giác. Các thành phần khác như: Form, Java applet, Active X cho phép tương tác tới các Website khác.

## 2.2.1 Tổng quan về HTTP

Hyper Text Transfer Protocol (HTTP) - giao thức tầng ứng dụng của Web - là trái tim của Web. HTTP được triển khai trên cả hai phía client và server. Các tiến trình client và server trên các hệ thống đầu cuối khác nhau giao tiếp với nhau thông qua việc trao đổi các thông điệp HTTP. HTTP quy định cấu trúc thông điệp cũng như cách thức trao đổi thông điệp giữa client và server. Trước khi nói về HTTP, chúng ta hãy nói lại các thuật ngữ về Web.

**Trang Web** (Webpage - hay còn gọi là một tập tin) chứa các đối tượng (Object). Đơn giản đối tượng chỉ là một file như file HTML, file ảnh JPEG, file ảnh GIF, file java applet, một đoạn âm thanh... Đối tượng được xác định qua địa chỉ URL. Trang Web chứa một file HTML cơ sở và tham

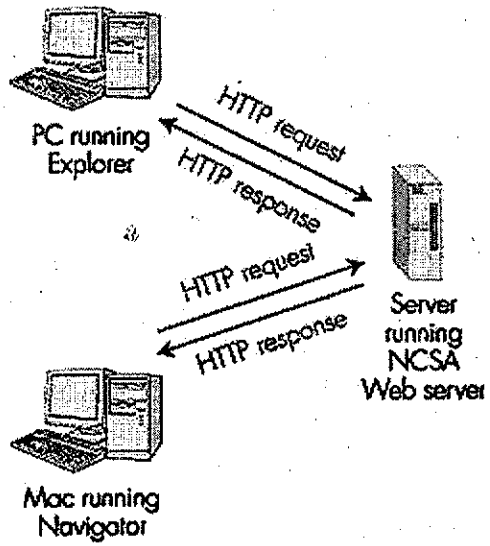


chiếu đến các đối tượng khác. Ví dụ một trang Web chứa một file HTML văn bản và 5 đối tượng ảnh JPEG, khi đó trang Web có 6 đối tượng: 1 file văn bản HTML và 5 file ảnh. File HTML cơ sở này tham chiếu đến các đối tượng khác thông qua địa chỉ URL. Mỗi địa chỉ URL có hai thành phần: tên của máy chủ và vị trí của đối tượng trên máy chủ. Đây là một địa chỉ URL

**www. someschool. edu/somedepartment/picture. gif**

www.someschool.edu là tên máy chủ và somedepartment/picture.gif là đường dẫn đối tượng.

**Trình duyệt** (Browser) - chương trình giao tiếp người dùng của ứng dụng Web cho phép hiển thị trang Web. Browser là phía client của giao thức HTTP. Hiện nay có rất nhiều phần mềm trình duyệt nhưng phổ biến nhất là Nestcape Communication và Microsoft Internet Explorer. Web server lưu giữ các đối tượng Web và được xác định qua địa chỉ URL. Phần mềm Web server là phía server của giao thức HTTP. Một số phần mềm Web server phổ biến là Apache, Microsoft Internet Information Server và Nestcape Enterprise Server.




**Hình 2.6. Tương tác client/server**

HTTP xác định cách thức trình duyệt yêu cầu trang Web từ Web server cũng như cách thức server gửi trang Web được yêu cầu tới trình

duyệt. Dưới đây chúng ta sẽ nói rõ hơn về quá trình trao đổi giữa client và server. Hình 2.6 minh họa quá trình này. Khi người dùng yêu cầu một đối tượng (ví dụ kích chuột vào một siêu liên kết), browser sẽ gửi thông điệp HTTP tới server yêu cầu đối tượng đó. Server nhận được yêu cầu và trả lời bằng cách gửi lại một thông điệp trả lời chứa đối tượng được yêu cầu. Cho tới những năm 1997, phần lớn các trình duyệt Web và Web server tuân thủ phiên bản HTTP 1.0 (đặc tả trong RFC 1945). Từ năm 1998 một số browser và Web server sử dụng phiên bản 1.1 theo khuyến nghị RFC 2616. Phiên bản mới này tương thích với phiên bản 1.0, nghĩa là Web server dùng phiên bản 1.1 có thể "nói chuyện" được với trình duyệt sử dụng phiên bản 1.0 và ngược lại.

Cả phiên bản 1.0 và 1.1 đều sử dụng TCP làm giao thức ở tầng giao vận phía dưới. HTTP client khởi tạo một kết nối TCP tới HTTP server. Sau khi thiết lập được kết nối, cả tiến trình browser và Web server đều truy cập tới TCP thông qua sòcket. Như đã nói ở phần 2.1, socket là "cửa" giữa tiến trình ứng dụng và thực thể TCP. Client gửi thông điệp yêu cầu qua socket. Server nhận thông điệp yêu cầu này và gửi thông điệp trả lời qua socket. Sau khi gửi thông điệp qua socket thì thông điệp nằm ngoài tầm "kiểm soát" của client và chính thực thể TCP chịu trách nhiệm chuyển nó sang phía bên kia. Trong phần 2.1 chúng ta thấy rằng TCP cung cấp dịch vụ truyền tin cậy cho HTTP, như vậy thông điệp của tiến trình client sẽ được chuyển tải nguyên vẹn đến server và ngược lại. Đến đây ta đã thấy được ưu điểm của kiến trúc phân tầng. HTTP không giải quyết việc mất mát dữ liệu mà việc này là trách nhiệm của TCP và các tầng bên dưới.

TCP sử dụng cơ chế tránh tắc nghẽn, cơ chế này sẽ được nghiên cứu chi tiết ở chương 3. Ở đây chúng ta chỉ cần biết rằng khi kết nối TCP mới khởi tạo cơ chế này đòi hỏi tốc độ truyền dữ liệu tương đối thấp nhưng sẽ tăng nhanh khi trên mạng không có tắc nghẽn. Giai đoạn bắt đầu với tốc độ thấp gọi là giai đoạn bắt đầu chậm (slow start).

Một chú ý quan trọng là server gửi các đối tượng được yêu cầu cho client mà không ghi lại bất kỳ một thông tin nào về trạng thái của client. Nếu client yêu cầu lại cùng một đối tượng thì server sẽ không thể trả lời cho client rằng đối tượng đó vừa được gửi cho client, server sẽ gửi lại cho client đối tượng đó như thể nó không biết việc gửi lần trước. HTTP server không nhớ các thông tin về client, vì thế HTTP được gọi là giao thức không trạng thái.



## 2.2.2 Kết nối liên tục và không liên tục (persistent / nonpersistent)

HTTP hỗ trợ cả hai cách kết nối liên tục và không liên tục. HTTP 1.0 sử dụng kết nối không liên tục. Chế độ mặc định của HTTP 1.1 là kết nối liên tục.

**Kết nối không liên tục (nonpersistent)**

Ta hãy xét các bước client thực hiện để yêu cầu trang Web từ server trong trường hợp sử dụng kết nối không liên tục. Giả sử trang Web có chứa một file HTML cơ sở và 10 file ảnh JPEG, đồng thời cả 11 đối tượng này cùng ở trên một server, địa chỉ của file HTML này là:

**www. someschool. edu/somedepartment/home. index**

Các bước thực hiện như sau:

HTTP client khởi tạo một kết nối TCP tới server có địa chỉ là **www.someschool.edu**. Cổng 80 là cổng được HTTP server sử dụng để "lắng nghe" các yêu cầu lấy trang Web từ client thông qua giao thức HTTP.

HTTP client gửi thông điệp yêu cầu qua socket tới thực thể TCP đã được kết nối ở bước trước. Thông điệp bao gồm đường dẫn **somedepartment/home.index** (ý nghĩa thông điệp sẽ được giải thích ở dưới).

HTTP server nhận được thông điệp yêu cầu từ socket, lấy đối tượng **somedepartment/home.index** trong bộ nhớ của mình (ổ cứng hoặc RAM), đặt đối tượng này vào trong một thông điệp trả lời và gửi đi qua socket.

HTTP server yêu cầu thực thể TCP kết thúc kết nối (nhưng nó không đóng lại thực sự cho đến khi client nhận được thông điệp).

HTTP client nhận được thông điệp trả lời, kết nối được đóng lại. Thông điệp chỉ ra rằng nó chứa một đối tượng là file HTML. Client sẽ lấy file đó ra từ thông điệp trả lời. File HTML tham chiếu đến 10 đối tượng ảnh JPEG.

4 bước đầu được lặp lại cho mỗi đối tượng ảnh được tham chiếu trong file HTML.

Khi nhận được thông điệp trả lời có chứa trang Web, browser sẽ hiển thị trang Web. Các browser khác nhau thì có thể có các cách hiển thị khác nhau đối với cùng một trang Web. HTTP không ảnh hưởng gì đối với cách hiển thị trang Web của client. Các đặc tả trong HTTP chỉ định nghĩa giao thức truyền thông giữa tiến trình client và server mà thôi.

Các bước ở trên sử dụng cách kết nối không liên tục vì sau khi gửi đi một đối tượng thì server sẽ đóng kết nối TCP lại, kết nối không được sử dụng để lấy các đối tượng khác. Lưu ý rằng mỗi kết nối TCP chuyển duy nhất một thông điệp yêu cầu và một thông điệp trả lời, như vậy trong ví dụ trên, client yêu cầu toàn bộ đối tượng trên trang Web thì sẽ có thể có tới 11 kết nối TCP được thiết lập.

Trong ví dụ trên, chúng ta không hề nói đến việc client nhận được 10 file ảnh JPEG qua 10 liên kết TCP riêng rẽ hay một số file được nhận qua cùng một kết nối. Trên thực tế, người dùng có thể cấu hình cho trình duyệt điều khiển mức độ song song của các kết nối. Chế độ mặc định của trình duyệt thường là từ 5 đến 10 kết nối TCP song song và mỗi kết nối kiểm soát một cặp thông điệp yêu cầu / trả lời. Nhưng nếu người dùng không thích thì có thể đặt số kết nối song song tối đa là 1, trong trường hợp này 10 kết nối được thiết lập riêng lẻ. Trong chương sau chúng ta sẽ thấy rằng cách kết nối song song làm giảm thời gian nhận được kết quả từ client.

**Kết nối liên tục**

Có một vài nhược điểm trong kết nối không liên tục: Thứ nhất, khi kết nối mới được tạo ra, phía client và server phải tạo ra vùng đệm TCP (buffer) cũng như lưu giữ các biến TCP. Điều này chính là gánh nặng cho server khi có nhiều client cùng yêu cầu một lúc.

Với cách kết nối liên tục, server không đóng liên kết TCP sau khi gửi thông điệp trả lời. Các thông điệp yêu cầu và trả lời sau đó (giữa cùng một client và server) được gửi qua cùng một kết nối. Trong ví dụ trên, toàn bộ đối tượng trong trang Web (một file HTML và 10 file ảnh JPEG) được truyền nối tiếp nhau trên cùng một kết nối TCP. Ngoài ra, có thể các trang Web khác trên cùng server có thể được truyền qua một kết nối TCP. Thông thường thì HTTP server đóng liên kết khi liên kết không được sử dụng trong một khoảng thời gian nào đó.



Chế độ làm việc mặc định của phiên bản HTTP 1.1 là gửi liên tục. Trong trường hợp này, HTTP client gửi yêu cầu khi nhận được một tham chiếu (ví dụ một siêu liên kết, hay tham chiếu đến file ảnh) vì vậy client có thể gửi các yêu cầu liên tiếp. Khi nhận được yêu cầu thì server sẽ gửi các đối tượng nối tiếp nhau.

## 2.2.3 Khuôn dạng thông điệp HTTP

Các đặc tả HTTP 1.0 (RFC 1945) và HTTP 1.1 (RFC 2016) đặc tả khuôn dạng thông điệp HTTP. Có hai kiểu khuôn dạng HTTP: thông điệp yêu cầu và thông điệp trả lời.

**Thông điệp yêu cầu HTTP (HTTP request message)**

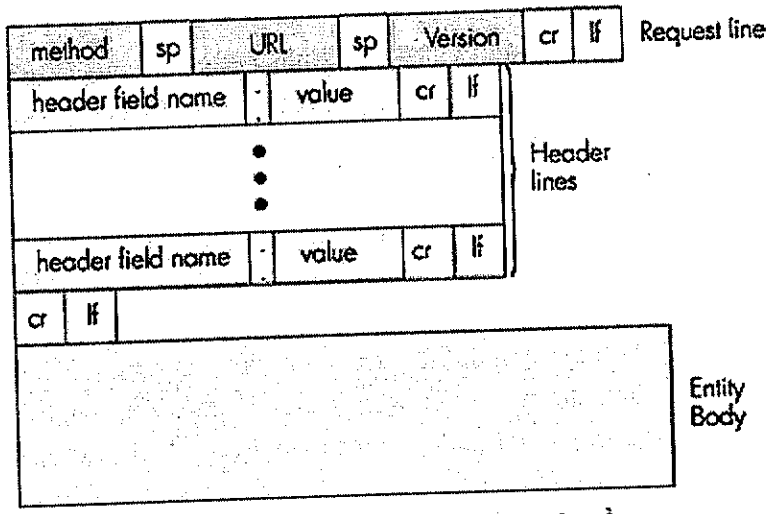
Một thông điệp yêu cầu thường có dạng sau:

```
GET /somedir. page. html HTTP/1.1
Host: www. someschool. edu
Connection:close
User-agent:Mozzilla /4.0
Accept- language:Fr
(extra carry return line feed)
```

Trước hết ta thấy rằng thông điệp được viết bằng mã ASCII - vì thế bất kỳ máy tính thông thường nào cũng có thể đọc được. Thứ hai, thông điệp gồm 5 dòng và mỗi dòng đều kết thúc bởi cặp ký tự đặc biệt Carriage Return (CR=13h) và Line Feed (LF=10h). Trên thực tế một thông điệp có thể có nhiều dòng hơn. Dòng đầu tiên của thông điệp được gọi là **dòng yêu cầu (request line)**, các dòng sau gọi là **tiêu đề (header)**. Dòng yêu cầu có 3 trường: trường method, trường địa chỉ URL và trường phiên bản HTTP. Trường method nhận một trong ba giá trị: GET, POST và HEAD. Phần lớn các yêu cầu sử dụng phương thức GET. Phương thức này được trình duyệt sử dụng để yêu cầu đối tượng có địa chỉ URL. Trong ví dụ trên thì trình duyệt yêu cầu đối tượng **somedir/page.html**. Trường phiên bản xác định phiên bản giao thức HTTP (trong ví dụ là 1.1).

Bây giờ hãy xét các trường trong tiêu đề. **Host: www.someschool.edu** là địa chỉ của máy tính có chứa đối tượng được yêu cầu. Ý nghĩa của trường Connection: close là trình duyệt yêu cầu server không sử dụng cách kết nối liên tục và yêu cầu server đóng kết nối lại sau khi đã gửi đi đối tượng được yêu cầu. Mặc dù client sử dụng phiên bản HTTP 1.1 nhưng lại không sử dụng kết nối liên tục. Trường **User-agent** xác định phần mềm trình duyệt của người sử dụng. Phần mềm trình duyệt ở đây là Mozzilla, một sản phẩm của hãng Nestcape. Trường này rất quan trọng vì server có thể gửi các bản khác nhau của cùng một đối tượng đến các trình duyệt khác nhau (các bản đối tượng này đều được xác định qua cùng một địa chỉ URL duy nhất). Cuối cùng là trường **Accept language**, trong ví dụ này người sử dụng yêu cầu bản tiếng Pháp của đối tượng - nếu server có bản này. Trong trường hợp không có thì server gửi đi bản mặc định.

Hình 2.7 minh hoạ khuôn dạng chung của thông điệp yêu cầu.




**Hình 2.7 Khuôn dạng thông điệp yêu cầu**

Khuôn dạng tổng quát của thông điệp có thêm trường **Entity Body** sau các dòng tiêu đề. Trường này không được sử dụng trong phương thức **GET** nhưng được sử dụng trong phương thức **POST**. HTTP client sử dụng phương thức **POST** khi người dùng điền vào một form - ví dụ khi muốn tìm kiếm qua máy tìm kiếm Google. Với phương thức **POST** người dùng vẫn yêu cầu trang Web nhưng nội dung cụ thể phụ thuộc vào nội dung điền trong form. Nếu giá trị của trường method là **POST** thì phần entity body sẽ chứa nội dung mà người dùng điền vào form. Phương thức **HEAD** cũng tương tự



như phương thức **POST**. Khi nhận được yêu cầu với phương thức **POST**, server sẽ gửi lại thông điệp HTTP trả lời nhưng không gửi đối tượng được yêu cầu. Thường người ta sử dụng phương thức **HEAD** để gỡ lỗi.

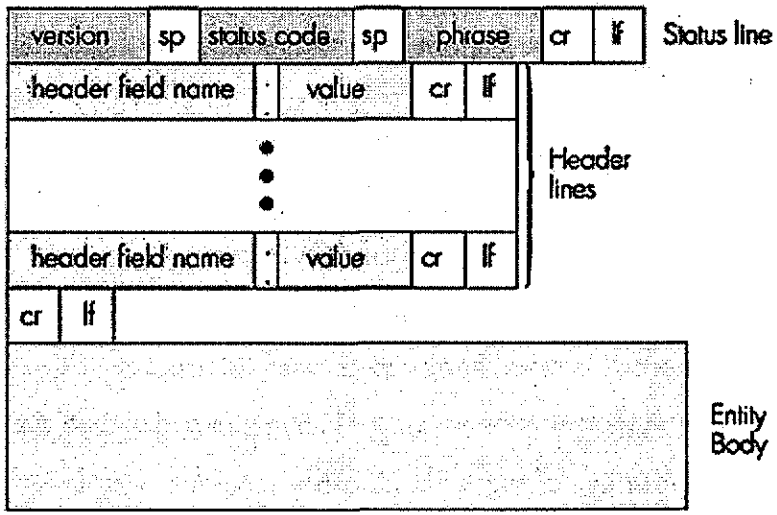
### Thông điệp trả lời (HTTP response massage)

Sau đây là một ví dụ về thông điệp trả lời, thông điệp này có thể là trả lời cho thông điệp yêu cầu trên.

```
HTTP /1.1  200 OK
Connection:close
Date: Thu, 06 Aug 1998 12:00:15 GMT
Server Apache/1. 3. 0 (unix)
Last modified:Mon, 22 Jun 1998 09:23:24 GMT
Connect lenght:6821
Connect type:text/html

( data data . . . . . )
```

Thông điệp trên gồm có 3 phần: Dòng đầu tiên là dòng trạng thái (status line), 6 dòng tiêu đề và cuối cùng là **phần thân (Entity body)** chứa đối tượng được yêu cầu (là phần **data data...**). Dòng trạng thái có 3 trường: trường phiên bản của giao thức, mã trạng thái và trường trạng thái thông điệp trả lời. Trong ví dụ này thì dòng trạng thái cho biết server sử dụng phiên bản HTTP 1.1 và trạng thái là sẵn sàng (server đã nhận được yêu cầu và gửi đối tượng được yêu cầu).




**Hình 2.8 Khuôn dạng thông điệp trả lời**

Trường **Connection: close** báo cho client biết server sẽ đóng kết nối sau khi gửi đi thông điệp. Trường **Date:** cho biết thời gian khi server tạo ra thông điệp và gửi đi, chú ý rằng đây không phải là thời gian khi đối tượng được tạo ra hay lần cuối cùng đối tượng được cập nhật. Đó là thời điểm mà server tìm thấy đối tượng trong hệ thống file của mình, chèn đối tượng vào thông điệp trả lời và gửi đi. Trường **Server** cho biết thông điệp trả lời này được tạo ra từ phần mềm Web server Apache, ý nghĩa của nó giống với trường **User agent** trong thông điệp yêu cầu. Trường **Last modified** là thời gian cuối cùng đối tượng được cập nhật. Ta sẽ nghiên cứu kĩ hơn về trường này nhưng chú ý rằng nó có vai trò quan trọng đối với cả client và Web cache (proxy server). **Content lenght:** cho biết độ dài của đối tượng được gửi. **Content type** xác định kiểu của đối tượng là file văn bản HTML (kiểu của đối tượng được đặt ở đây chứ không phải trong phần mở rộng của tên file).

Chú ý khi nhận được một thông điệp yêu cầu HTTP 1.0, server cũng sẽ không sử dụng kết nối liên tục ngay cả khi server dùng phiên bản 1.1. Server sẽ đóng kết nối ngay sau khi gửi đối tượng. Điều này cần thiết vì client sử dụng phiên bản HTTP 1.0 sẽ chờ server đóng kết nối lại.

Khuôn dạng chung của một thông điệp trả lời được minh hoạ trên Hình 2.8. Khuôn dạng này tương thích với ví dụ trên. Tuy nhiên cần phải nói thêm về mã trạng thái (status code) và ý nghĩa của chúng. Mã trạng thái cùng với cụm từ đi sau cho biết kết quả đáp ứng yêu cầu. Sau đây là một vài giá trị thông dụng và ý nghĩa của chúng:

**200 OK**: Yêu cầu được đáp ứng và dữ liệu được yêu cầu nằm trong thông điệp.

**301 Moved permanetly**: cho biết đối tượng đã được chuyển và địa chỉ URL mới của đối tượng được đặt trong trường **Location:** của thông điệp trả lời, phần mềm tại client sẽ tự động lấy đối tượng tại địa chỉ URL mới (đây là hiện tượng redirection thường gặp khi duyệt Web).

**400 Bad Request**: server không hiểu được yêu cầu từ client

**404 Not found**: đối tượng không còn được lưu trên server

**505 HTTP version not support**: server không hỗ trợ giao thức của client

Trong phần này chúng ta đã trình bày một số trường trong tiêu đề của thông điệp HTTP. HTTP (đặc biệt là bản 1.1) định nghĩa rất nhiều



trường có thể được browser, Web server và Web cache chèn vào trong thông điệp. Ở trên chúng ta mới đề cập đến một phần nhỏ, chi tiết có thể xem trong các đặc tả của HTTP.

Làm thế nào để trình duyệt cũng như server biết được phải chèn trường nào vào tiêu đề thông điệp? Thông điệp yêu cầu phụ thuộc vào chức năng trình duyệt cũng như phiên bản HTTP (HTTP 1.0 không thể tạo ra thông điệp kiểu HTTP1.1). Người sử dụng có thể định cấu hình cho trình duyệt.

## 2.2.4 Tương tác giữa người dùng và Hrver-server

Như đã nói trên, HTTP server không lưu giữ trạng thái. Điều này đơn giản hoá kiến trúc và làm tăng hiệu suất hoạt động của server. Tuy nhiên server muốn phân biệt người dùng không chỉ vì muốn hạn chế sự truy cập mà còn vì muốn phục vụ theo định danh người dùng. HTTP có 2 cơ chế để server phân biệt người dùng: Authentication và cookies.

**Authentication (Kiểm chứng)**

Nhiều server yêu cầu người dùng phải cung cấp tên (username) và mật khẩu (password) để có thể truy cập được vào tài nguyên trên máy chủ. Yêu cầu này được gọi là kiểm chứng. HTTP có các mã trạng thái và trường để thực hiện quá trình kiểm chứng. Giả sử client yêu cầu một đối tượng từ server và server yêu cầu client cung cấp tên và mật khẩu. Đầu tiên client vẫn gửi một thông điệp yêu cầu thông thường. Server sẽ trả lời với thông điệp có phần thân rỗng và trường mã trạng thái là **401 Authentication required.** Trong thông điệp trả lời này có trường **www-Authenticate**: xác định phương thức kiểm chứng mà người dùng phải thực hiện, thông thường là đưa tên và mật khẩu. Nhận được thông điệp này, client yêu cầu người dùng cung cấp tên và mật khẩu. Sau đó, client sẽ gửi lại thông điệp yêu cầu có trường **Authoziration:** trong tiêu đề, trường này chứa tên và mật khẩu của người dùng.

Sau khi nhận được đối tượng đầu tiên, client tiếp tục gửi tên và mật khẩu trong các thông điệp kế tiếp (thường thì cho đến khi người dùng đóng trình duyệt lại. Khi trình duyệt còn mở, tên và mật khẩu được lưu lại trong

cache để người dùng không phải đánh lại nữa). Theo cách này server có thể phân biệt các người dùng khác nhau. HTTP phân biệt người dùng khá lỏng lẻo và không khó để vượt qua. Chúng ta sẽ nghiên cứu thêm về vấn đề bảo mật và sơ đồ xác nhận người dùng trong chương sau.

**Cookie**

Cookie là kỹ thuật khác được sử dụng để ghi lại dấu vết của người truy cập. Nó được đặc tả trong RFC 2109. Ví dụ lần đầu tiên người dùng truy cập vào một server nào đó có sử dụng cookie. Thông điệp trả lời của server có trường **Set-cookies:** trong tiêu đề, cùng với một chuỗi ký tự do Web server tạo ra.

Ví dụ **Set-cookies:1678453**. Khi nhận được thông điệp trả lời, client xác định được trường **Set-cookies** và chuỗi ký tự đi kèm, trình duyệt sẽ thêm một dòng vào cuối file cookie (là một file đặc biệt nằm trên máy client). Dòng này thường là dòng chứa tên máy chủ và chuỗi ký tự cookie. Giả sử một tuần sau, client gửi thông điệp yêu cầu đến server, client sẽ tự động chèn trường **Cookies:** trong tiêu đề của thông điệp yêu cầu với giá trị là chuỗi giá trị cookie lưu trong file cookie. Trong ví dụ trên, tiêu đề chứa trường **cookies** là **Cookie:1678453.** Theo cách này, server không xác định được tên của người dùng (user name) nhưng xác định được user này chính là người đã truy cập một tuần trước đó.

Web server sử dụng cookie cho nhiều mục đích:

Nếu server yêu cầu kiểm chứng nhưng không muốn đòi hỏi người dùng đăng nhập qua tên và mật khẩu thì có thể sử dụng cookie cho mỗi lần người dùng truy cập vào server.

Server sử dụng cookie nếu muốn ghi nhớ các hoạt động của người dùng, phục vụ mục đích quảng cáo.

Nếu user mua hàng trên mạng (mua một đĩa CD chẳng hạn) thì server sử dụng cookie để ghi lại những gì mà user đã mua. Đó chính là các cửa hàng ảo.

Sử dụng cookie gây khó khăn cho người dùng không có máy cố định mà truy cập vào server từ nhiều máy khác nhau. Server sẽ coi đó là những người dùng phân biệt.



## 2.2.5 GET có điều kiện (Conditional GET)

Lưu giữ lại các đối tượng đã từng được lấy, Web cache có thể làm giảm thời gian chờ từ khi gửi yêu cầu đến khi nhận đối tượng và làm giảm lưu lượng thông tin truyền trên Internet. Web cache được triển khai trên trình duyệt hay các cache server. Chúng ta sẽ nghiên cứu network cache ở phần sau. Trong phần này ta chỉ quan tâm đến cache tại trình duyệt.

Mặc dù Web cache làm giảm thời gian chờ nhận đối tượng nhưng vấn đề nẩy sinh là bản sao của đối tượng được lưu giữ trên client có thể đã "cũ", nói cách khác đối tượng trên server có thể đã thay đổi từ khi client lấy đối tượng đó về. Tuy nhiên HTTP có cơ chế cho phép sử dụng cache trong khi vẫn đảm bảo đối tượng trong cache chưa bị "cũ". Cơ chế này chính là **GET có điều kiện (conditional GET)**. Một thông điệp HTTP được gọi là có điều kiện nếu: (1) thông điệp sử dụng phương thức GET và (2) thông điệp có trường **If-modified-since** trong tiêu đề. Ví dụ, trình duyệt yêu cầu một đối tượng từ server mà trong cache của nó chưa có:

**GET /fruit/banana.gif HTTP/1. 0**
**User-agent:Mozilla/4. 0**

Sau đó server gửi thông điệp trả lời kèm với đối tượng

**HTTP /1.0 200 OK**
**Date: wed 12 aug 1998 15:38:29**
**Server : Apache/1. 3. 0 (Unix)**
**Last-modified: mon, 22 jun 1998 09:23:24**
**Content-type:image/gif**
**(data data. . . . . )**

Trình duyệt hiển thị đối tượng đồng thời lưu lại đối tượng trong cache cục bộ cùng với thời gian trong trường **Last-modified** kèm theo đối tượng.

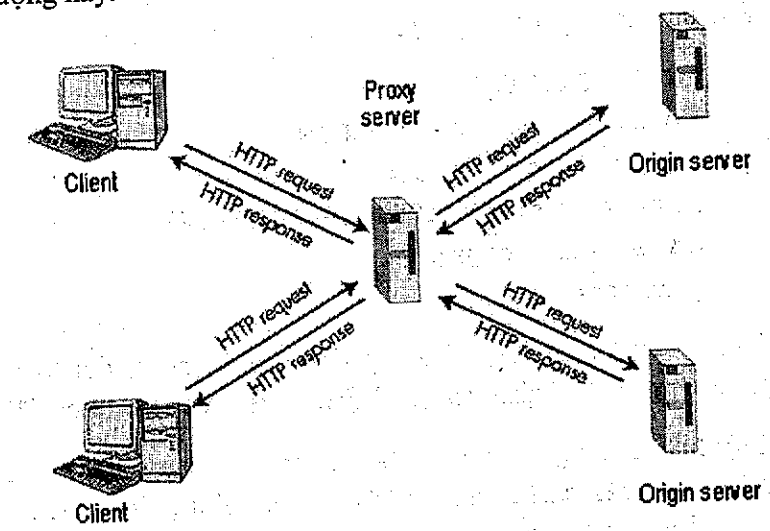
Một tuần sau, người sử dụng lại yêu cầu đối tượng này và đối tượng vẫn còn được lưu trên cache. Nhưng trên server đối tượng có thể đã bị thay đổi trong thời gian một tuần nên trình duyệt phải thực hiện kiểm tra bằng cách gửi một thông điệp GET có điều kiện, cụ thể browser gửi đi:

**GET /fruit/kiwi. gif HTTP/1. 0**
**User-agent: Mozilla /4. 0**
**If-modified-since: Mon, 22 Jun 1998 09:23:24**

Chú ý giá trị trường **If-modified-since:** là giá trị của trường **Last-modified:** trong tiêu đề mà server đã gửi cho client tuần trước. Thông điệp **GET** có điều kiện yêu cầu server chỉ gửi đối tượng cho client nếu như đối tượng đó bị thay đổi sau thời gian được chỉ ra trên. Giả sử đối tượng đó không thay đổi gì từ 9 giờ 23 phút 24 giây ngày 22 tháng 6 năm 1998 thì server sẽ gửi cho client thông điệp:

**HTTP /1.0 304 Not modified**
**Date : wed, 19 Aug 1998 15:39:29**
**Server: Apache /1. 3. 0 (Unix)**
**(empty entity body)**

Thông điệp trả lời này không kèm theo đối tượng. Việc gửi kèm đối tượng chỉ làm lãng phí đường truyền và làm tăng thời gian client phải chờ để nhận được đối tượng, đặc biệt khi đối tượng có kích thước lớn. Giá trị trường trạng thái là **304 Not modified** báo cho client biết đối tượng mà client lưu trong cache giống đối tượng gốc tại server, do đó client có thể sử dụng lại đối tượng này.




**Hình 2.9 Client yêu cầu đối tượng thông qua cache**



## 2.2.6 Web cache

**Web cache (proxy server) là thực thể đáp ứng yêu cầu từ client. Máy tính làm nhiệm vụ Web cache có ổ đĩa riêng lưu trữ bản sao các đối tượng đã từng được yêu cầu. Như minh hoạ trên**

Hình 2.9, người sử dụng có thể cấu hình trình duyệt sao cho tất cả các yêu cầu đều được gửi đến Webcache trước (việc này tương đối đơn giản với các trình duyệt của Microsoft và Nescape). Khi đó tất cả yêu cầu của trình duyệt về một đối tượng nào đó sẽ được chuyển đến Webcache trước. Giả sử trình duyệt yêu cầu đối tượng là một file ảnh có địa chỉ là **http://www.someschool.edu/campus.gif**

- Trình duyệt khởi tạo một kết nối TCP tới Webcache và gửi yêu cầu tới Webcache
- Webcache sẽ kiểm tra và tìm đối tượng, nếu tìm được thì Webcache sẽ gửi đối tượng cho client qua kết nối TCP đã được thiết lập.
- Nếu Webcache không có đối tượng đó thì nó sẽ khởi tạo một kết nối tới server thật chứa đối tượng, ở đây là **www.someschool.edu**. Sau đó Webcache gửi thông điệp yêu cầu tới cho server này thông qua kết nối TCP vừa khởi tạo. Sau khi nhận được yêu cầu từ Webcache, server sẽ gửi lại đối tượng cho Webcache
- Khi nhận được đối tượng, Webcache sẽ lưu lại bản sao của đối tượng và gửi đối tượng trong thông điệp HTTP trả lời cho máy client (thông qua kết nối TCP đã được thiết lập trước đó).

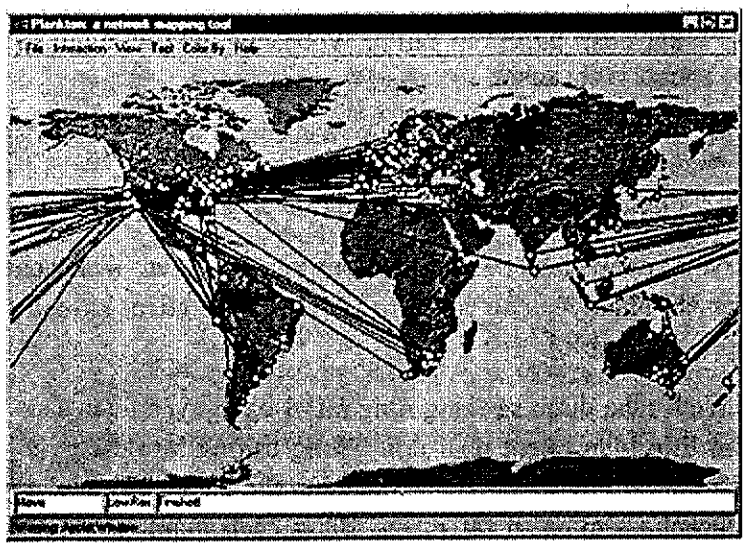
Như vậy Webcache vừa là client vừa là server. Webcache đóng vai trò server khi nhận yêu cầu và trả lời, đóng vai trò client khi gửi yêu cầu và nhận thông điệp trả lời.

Webcache được sử dụng rộng rãi vì ba nguyên nhân sau: Webcache làm giảm thời gian client phải đợi. Trong trường hợp cache có đối tượng được yêu cầu thì đối tượng này sẽ ngay lập tức được chuyển cho client. Thứ hai, Webcache làm giảm tải mạng. Bằng cách giảm tải đường truyền ra mạng Internet, cơ quan không cần phải nâng cấp đường truyền và giảm chi

phí. Webcache làm giảm lượng thông tin Web trao đổi trên Internet, do đó tăng hiệu suất hoạt động của tất cả các ứng dụng. Năm 1998, theo thống kê hơn 75% thông tin được truyền trên mạng là ứng dụng Web, vì vậy giảm tải Web cải thiện đáng kể hiệu suất toàn bộ Internet. Thứ ba, mạng Internet với nhiều Webcache giúp cho việc nhanh chóng phát tán thông tin - thậm chí ngay cho những nhà cung cấp thông tin có tốc độ server chậm hay tốc độ kết nối chậm. Nếu một nhà cung cấp có một nội dung cần phổ biến thì nội dung này ngay lập tức được chuyển đến các Webcache và yêu cầu của người dùng từ mọi nơi được đáp ứng nhanh chóng.

**Cache liên hợp (Cooperative caching)**

Có thể kết hợp nhiều Webcache đặt ở các vị trí khác nhau trên mạng nhằm nâng cao hiệu suất tổng thể. Ví dụ, cache của một cơ quan có thể được cấu hình sao cho các yêu cầu của nó được gửi tới cache của nhà cung cấp dịch vụ Internet cấp quốc gia (backbone ISP). Khi đó nếu cache của cơ quan không có đối tượng được yêu cầu thì nó sẽ gửi thông điệp yêu cầu HTTP đến cache của ISP. Cache ở ISP sẽ tìm đối tượng trong hệ thống lưu trữ của mình hoặc tại chính server có lưu giữ đối tượng. Sau đó nó sẽ gửi đối tượng trong thông điệp trả lời HTTP tới cache của cơ quan. Cache của cơ quan lại gửi đối tượng tới trình duyệt yêu cầu. Mỗi lần đối tượng khi qua cache đều được sao chép lại trong cache.



**Hình 2.10 NLANR caching**



Một ví dụ về hệ thống cache liên hợp là hệ thống cache NLANR. Hệ thống này có nhiều máy làm nhiệm vụ Webcache ở Mỹ, cung cấp dịch vụ cho các Webcache của các tổ chức và các khu vực trên toàn thế giới. Mô hình phân cấp của hệ thống này được mô tả trong Hình 2.10. Cache này lấy đối tượng từ cache khác bằng cách kết hợp sử dụng giao thức HTTP và ICP (Internet Caching Protocol). ICP là giao thức ở tầng ứng dụng cho phép cache nhanh chóng xác định một cache khác có đối tượng nào đó hay không, và nếu có thì cache có thể sử dụng giao thức HTTP để lấy đối tượng về. ICP được sử dụng rộng rãi trên rất nhiều hệ thống cache liên hợp.

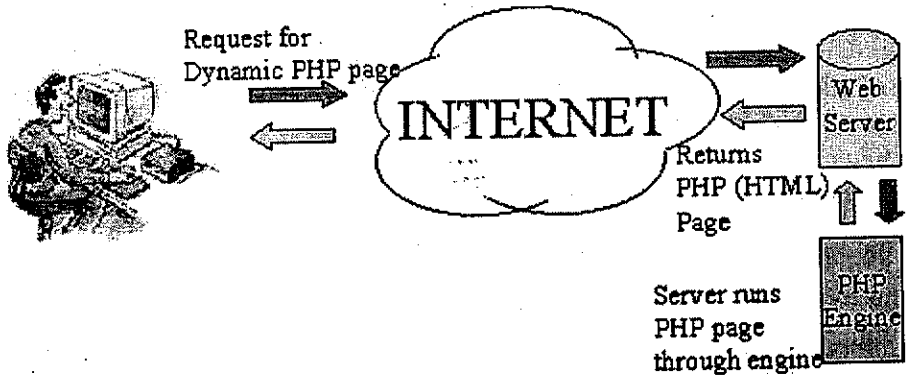
Một kiểu liên hợp khác là cụm cache (cache cluster), thường đặt trên cùng một mạng LAN. Cache được thay thế bởi cụm cache khi một cache duy nhất không đáp ứng hiệu quả trong trường hợp quá nhiều yêu cầu hay khi dung lượng thiết bị nhớ hạn chế. Tuy nhiên khi trình duyệt yêu cầu một đối tượng thì vấn đề nảy sinh là yêu cầu được gửi đến cache nào trong cụm cache. Vấn đề này có thể được giải quyết bằng cách tìm kiếm theo hàm băm (hash routing). Đơn giản nhất, trình duyệt thực hiện phép "băm" trên địa chỉ URL, trình duyệt sẽ căn cứ vào kết quả để gửi yêu cầu đến một trong các cache trong cụm. Nếu tất cả trình duyệt dùng cùng một thuật toán băm, đối tượng không bao giờ được lưu trên các cache khác nhau trong cụm. Nếu đối tượng thực sự được lưu trữ trong cụm thì trình duyệt luôn có thể gửi yêu cầu đến cache thích hợp. Tìm kiếm theo hàm băm là cốt lõi của giao thức Cache Array Routing (CARP).

Webcache là vấn đề lớn và phức tạp. Trong vài năm gần đây có nhiều nghiên cứu và sản phẩm về cache. Hướng nghiên cứu là xây dựng cache có khả năng xử lý được luồng âm thanh và hình ảnh. Cache sẽ đóng một vai trò quan trọng để Internet trở thành cơ sở hạ tầng cung cấp các dịch vụ hỗ trợ đa phương tiện theo yêu cầu (on demand).

## 2.2.7 Web động

Trong phần trên, chúng ta nói về trang Web tĩnh – là một file HTML cụ thể nằm trên Web server. Trong phần này chúng ta sẽ trình bày về Web động và Web tích cực. Một trang Web động không tồn tại dưới dạng một file cố định trên Web server. Trang Web động chỉ được server tạo ra khi

nhận được một yêu cầu cụ thể từ trình duyệt Web. Khi nhận được một yêu cầu, Web server sẽ chạy một chương trình ứng dụng nào đó để tạo ra nội dung một văn bản. Sau đó văn bản này được trả về cho trình duyệt.




**Hình 2.11 Ví dụ về Web động, Web server sử dụng công nghệ PHP**

Web tích cực (active Web) là loại văn bản có chứa chương trình. Chương trình này có khả năng tính toán và hiển thị thông tin. Khi trình duyệt yêu cầu, server sẽ gửi cho trình duyệt một văn bản có đính kèm chương trình. Trình duyệt sẽ chạy chương trình này tại máy tính cục bộ của mình, chương trình có thể tương tác với người sử dụng, tự động cập nhật thông tin theo nhu cầu người sử dụng. Do vậy nội dung trang Web tích cực không bất biến mà thay đổi khi chương trình tương ứng thực thi. Cơ chế Web động có ưu nhược điểm riêng so với Web tĩnh truyền thống.

Rõ ràng ưu điểm chính của Web tĩnh là tính đơn giản, tiện dụng và tin cậy. Sau khi được tạo ra, trang Web tĩnh có một định dạng cố định và bất biến. Trình duyệt có thể nhanh chóng hiển thị một trang Web tĩnh, và có thể tăng hiệu suất hệ thống bằng cách sử dụng cơ chế cache.

Nhược điểm của Web tĩnh là thiếu tính linh hoạt. Khi phải thay đổi, chúng ta phải chỉnh sửa lại mỗi trang Web tĩnh. Điều này không được làm tự động mà phải làm thủ công. Do đó trang Web tĩnh không thích hợp khi cần cung cấp các thông tin biến đổi thường xuyên.

Ưu điểm chính của Web động là khả năng hiển thị ngay lập tức thông tin hiện thời từ phía server. Những thông tin thay đổi thường xuyên, chẳng hạn dự báo thời tiết, giá các loại cổ phiếu,... có thể được một chương trình ứng dụng ở phía server sinh ra và chuyển cho trình duyệt khi có yêu cầu.



Triển khai Web động được thực hiện ở phía server. Phía client yêu cầu một trang Web động giống như khi yêu cầu một trang Web tĩnh. Đối với client, một trang Web động không khác gì một trang Web tĩnh. Do Web tĩnh hay Web động đều theo định dạng HTML, nên client không thể biết thông điệp trả về là server lấy từ file nằm trên ổ cứng hay là kết quả của một chương trình.

Nhược điểm chính của Web động là chi phí cài đặt tương đối cao và không linh hoạt khi phải hiển thị những thông tin hay thay đổi. Giống như Web tĩnh, một khi thông điệp được server sinh ra và chuyển cho trình duyệt thì nội dung thông điệp là cố định. Nếu mỗi lần thông tin thay đổi, trình duyệt phải cập nhật lại để lấy nội dung mới.

Xây dựng và bảo trì các Web server có khả năng tương tác động khá tốn kém, do ngoài khả năng phải lập trình thì máy tính làm Web server phải có cấu hình mạnh, ngoài ra phải tăng cường khả năng bảo mật của hệ thống. Việc tạo ra trang Web động cũng tốn nhiều thời gian hơn (do phía server phải chạy chương trình với mỗi yêu cầu từ client).

Đối với Web động, cho dù thông điệp trả lời chỉ được tạo ra khi có nhu cầu, nhưng thông tin trong đó vẫn có thể bị lạc hậu nhanh chóng. Ưu điểm chính của Web tích cực so với Web động chính là khả năng cập nhật thông tin liên tục do khả năng Web tích cực có khả năng tương tác trực tiếp với server để cập nhật thông tin. Ví dụ một trang Web hiển thị giá của thị trường chứng khoán có thể tự động cập nhật giá các loại cổ phiếu mà không cần bất kỳ sự can thiệp nào từ phía người dùng.

Nhược điểm chính của Web tích cực là chi phí xây dựng và khả năng an ninh hệ thống. Vì phải tải và sau đó thực thi một chương trình từ server, nên phải có khả năng đảm bảo chương trình này không làm gì có hại trên máy tính client.

Chủ yếu việc triển khai Web động được thực hiện ở phía server, server phải có bổ sung thêm khả năng chạy một chương trình ứng dụng nào đó để tạo ra nội dung một trang Web khi có yêu cầu từ trình duyệt. Mỗi một kiểu trả lời phải có một chương trình ứng dụng riêng. Do đó server phải có khả năng chuyển yêu cầu đến từ trình duyệt cho chương trình ứng dụng cụ thể.

## Chuẩn CGI (Common Gateway Interface)

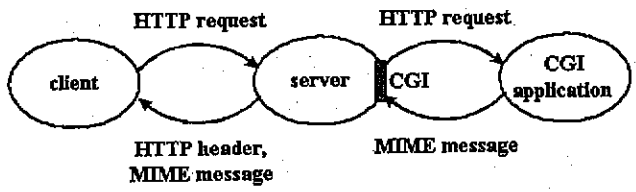
CGI là một trong những công nghệ đã từng được sử dụng rất rộng rãi khi xây dựng Web động. Chuẩn CGI quy định cách thức Web server tương tác với chương trình ứng dụng (chương trình CGI). Hình 2.12 minh họa cơ chế hoạt động của CGI.

Trên phần lớn Web server, cơ chế CGI được cài đặt như sau. Trong thư mục gốc cài đặt Web server, có thư mục cgi-bin. Khi client yêu cầu một file nào đó nằm trong thư mục cgi-bin thì Web server sẽ không gửi file được yêu cầu mà phải thực thi file này và kết quả của quá trình thực thi sẽ được gửi cho trình duyệt. Chương trình được gọi để thực thi ở đây có thể là một file khả thi hoặc một đoạn mã script (bằng Perl).

Giả sử bạn gõ **http://computer.howstuffworks.com/cgi-bin/search.pl** trên trình duyệt. Web server nhận thấy rằng file **search.pl** nằm trong thư mục cgi-bin, do vậy nó thực thi **search.pl** (là một Perl script) và sau đó gửi kết quả cho trình duyệt.

Bạn hoàn toàn có thể viết một đoạn script và thử cơ chế CGI, miễn là:

- Bạn biết một ngôn ngữ lập trình, chẳng hạn C hay PERL
- Bạn có quyền truy cập vào Web server có hỗ trợ CGI.




Hình 2.12 Vị trí của CGI

## Một chương trình CGI đơn giản

Trong phần trước, chúng ta đã xem một ví dụ trang Web tĩnh đơn giản như sau:

```
<html>
 <body>
  <h1>Hello there!</h1>
 </body>
</html>
```



Nếu có quyền truy cập tới thư mục cgi-bin trên một Web server có hỗ trợ CGI, bạn có thể thử đoạn mã đơn giản được viết bằng ngôn ngữ lập trình C sau đây. Kết quả thực hiện của chương trình này tương đương với trang Web tĩnh ở trên.

```
#include <stdio.h>
int main()
{
 printf("Content-type: text/html\n\n");
 printf("<html>\n");
 printf("<body>\n");
 printf("<h1>Hello there!</h1>\n");
 printf("</body>\n");
 printf("</html>\n");
 return 0;
}
```

Dịch file mã nguồn này thành file **simplest.cgi** và đặt trong thư mục cgi-bin. Giả sử trình duyệt yêu cầu file **simplest.cgi** thì chương trình CGI tại server sẽ sinh ra một trang Web có dòng chữ "Hello there".

Chú ý rằng bắt buộc phải có dòng **printf("Content-type: text/html\n\n")** vì **"Content-type: text/html\n\n"** luôn là dòng đầu tiên Web server gửi cho trình duyệt.

Ưu điểm chính của chương trình CGI là tạo ra nội dung động – nghĩa là kết quả của mỗi lần chạy là khác nhau. Chương trình C sau đây minh họa điều này.

```
#include <stdio.h>
int incrementcount()
{
 FILE *f;
 int i;
 f=fopen("count.txt", "r+");
 if (!f)
 {
   sleep(1);
   f=fopen("count.txt", "r+");
   if (!f)
     return -1;
 }

 fscanf(f, "%d", &i);
 i++;
```

```
  fseek(f,0,SEEK_SET);
  fprintf(f, "%d", i);
  fclose(f);
  return i;
}

int main()
{
  printf("Content-type: text/html\n\n");
  printf("<html>\n");
  printf("<body>\n");
  printf("<h1>The current count is: ")
  printf("%d</h1>\n", incrementcount());
  printf("</body>\n");
  printf("</html>\n");
  return 0;
}
```

Sau đó dịch file này thành file **counter.cgi**. Tạo ra file **count.txt** có chứa số **0** trong đó và đặt cả hai file này vào thư mục cgi-bin. Sau đó thử kiểm tra bằng cách kích vào link **http://computer.howstuffworks.com/cgi-bin/count.cgi** một số lần. Mỗi lần sẽ hiện ra một kết quả khác nhau.

File **count.txt** giữ giá trị hiện thời của biến **count**, và hàm **incrementcount()** làm tăng biến **count** trong file **count.txt**. Hàm này mở file **count.txt**, đọc giá trị biến count, tăng biến count lên một sau đó ghi lại giá trị mới vào file.

### Form: Gửi thông tin đến trình duyệt

Chúng ta thấy rằng chương trình CGI tương đối đơn giản. Web server chỉ gọi một chương trình CGI để thực thi và sau đó kết quả được gửi lại cho trình duyệt. Bây giờ chúng ta xem cách thức làm sao để trình duyệt gửi được thông tin cho chương trình CGI. Cách thức đơn giản ở đây chính là HTML form.

Để hiểu thế nào là form, chúng ta thử tạo ra một file HTML đơn giản có tên **simpleform.htm** với nội dung như sau

```
<html>
<body>
 <h1>A super-simple form<h1>
 <FORM METHOD=GET ACTION="http://computer.howstuffworks.com/
```



```
cgi-bin/simpleform.cgi">
 Enter Your Name:
 <input name="Name" size=20 maxlength=50>
 <P>
 <INPUT TYPE=submit value="Submit">
 <INPUT TYPE=reset value="Reset">
 </FORM>
</body>
</html>
```

File HTML này bạn đặt trong thư mục cgi-bin của Web server. Nếu để ý kỹ, bạn sẽ thấy trong đoạn mã HTML sử dụng phương thức GET để gửi đến CGI script có địa chỉ **http://computer.howstuffworks.com/cgi-bin/simpleform.cgi**. Trong form có vùng văn bản để người dùng đưa dữ liệu vào và hai nút chuẩn kiểu Submit và Reset.

File **Simpleform.cgi** được tạo ra bằng chương trình C đơn giản **simpleform.c** sau:

```
#include <stdio.h>
#include <stdlib.h>
int main()
{
 printf("Content-type: text/html\n\n");
 printf("<html>\n");
 printf("<body>\n");
 printf("<h1>The value entered was: ")
 printf("%s</h1>\n", getenv("QUERY_STRING"));
 printf("</body>\n");
 printf("</html>\n");
 return 0;
}
```

Và sau khi biên dịch được đặt trong thư mục cgi-bin. Chương trình này sẽ lấy giá trị được trình duyệt gửi về qua form để rồi hiển thị nó.

## Các kỹ thuật phía Server

Một phương pháp giúp Web server tạo nội dung động là các công nghệ phía server (server side technology). Ngày nay có khá nhiều công nghệ như vậy.

**ASP** (*Active Server Pages*): Là công nghệ của Microsoft, có phần mở rộng là .asp.

**PHP** (*Personal Home Pages*): Công nghệ mã nguồn mở, phần mở rộng là php or.php3 (phụ thuộc vào cấu hình server).

**JSP** (*Java Server Pages*): Dựa trên ngôn ngữ lập trình Java, có phần mở rộng là .jsp.

Với những công nghệ trên, dễ dàng cài đặt và bảo trì cho một Website lớn. Người phát triển chỉ cần gắn các đoạn mã (phía server) vào các trang HTML. Đoạn mã này được đưa cho trình biên dịch tương ứng để từ những câu lệnh sinh ra các đoạn mã HTML và sau đó trang HTML được gửi về cho trình duyệt. Chú ý rằng trình duyệt sẽ không biết về đoạn mã được gắn bên trong trang Web, trình duyệt chỉ nhận được một trang Web với mã HTML thuần túy do server gửi về.

Chúng ta thử lấy PHP làm ví dụ. Yêu cầu của trình duyệt tới một trang PHP sẽ được Web server chuyển cho bộ biên dịch PHP (cùng với các dữ liệu có liên quan). Bộ biên dịch PHP sẽ chạy đoạn mã PHP để sinh ra nội dung HTML và chuyển kết quả này cho Web server. Web server tiếp tục chuyển kết quả nhận được cho trình duyệt yêu cầu. Trình duyệt chỉ nhận được mã HTML, hiển thị chúng mà không biết cách thức Web server tạo ra trang HTML.

### Một chương trình PHP đơn giản

Tạo ra một file **hello.php** có nội dung sau và đặt trong thư mục chủ cài đặt PHP của Web server (**DOCUMENT_ROOT**)

```
<html>
 <head>
  <title>PHP Test</title>
 </head>
 <body>
 <?php echo '<p>Hello World</p>'; ?>
 </body>
</html>
```

Sử dụng trình duyệt để truy cập vào file hello.php này (gõ **http://Webserver//hello.php** trên thanh địa chỉ của trình duyệt). Nếu phía server cấu hình PHP chính xác thì phía trình duyệt sẽ nhận được kết quả sau:



```
<html>
 <head>
  <title>PHP Test</title>
 </head>
 <body>
 <p>Hello World</p>
 </body>
</html>
```

Chương trình trên cực kỳ đơn giản. Nó chỉ hiển thị dòng chữ "**Hello World**" trên trình duyệt bằng cách sử dụng lệnh **echo( )** của PHP.

Điểm quan trọng trong ví dụ này là các thẻ PHP đặc biệt. Trong ví dụ này ta sử dụng thẻ <?php để xác định điểm khởi đầu và thẻ ?> đánh dấu điểm kết thúc của một đoạn mã PHP. Đoạn mã PHP có thể được đặt vào bất kỳ đâu trong file mã nguồn PHP và đoạn mã này sẽ được trình biên dịch PHP xử lý.

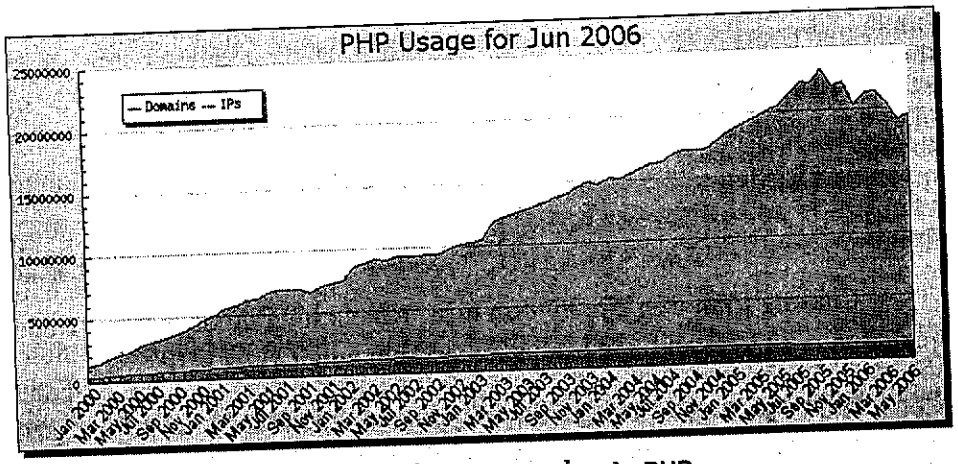
## *Lịch sử PHP*

PHP được Rasmus Lerdorf công bố chính thức từ khoảng mùa thu năm 1994. Trước đó Rasmus đã sử dụng chương trình này để kiểm soát số người truy cập vào Website cá nhân của mình. Phiên bản PHP đầu tiên được công bố vào đầu năm 1995 và được xem là viết tắt của Personal Home Page. Nó chỉ bao gồm một bộ phân tích cực kỳ đơn giản với một vài macro, một vài tiện ích để hỗ trợ xây dựng một Website cá nhân có guessbook và counter. Bộ phân tích được viết lại vào giữa năm 1995 và trở thành phiên bản PHP/FI 2. Module FI thực hiện việc tạo ra file HTML từ một dữ liệu cho trước. Rasmus đã kết hợp module Form Interperter và thêm các hỗ trợ mSQL. Bắt đầu từ đó, công nghệ PHP được sử dụng cực kỳ rộng rãi và được nhiều người cùng bắt tay phát triển cùng.

Rất khó đưa ra các dự đoán thật chính xác, nhưng vào khoảng cuối năm 1996, có khoảng 15000 Website sử dụng PHP/FI. Đến giữa năm 1997, số lượng này tăng lên 50000. Tại thời điểm này, PHP không còn là dự án mang tính "ngẫu hứng" của Rasmus nữa mà trở thành một dự án có tổ chức với nhiều người cùng tham gia phát triển. Bộ phân tích được Zeev Suraski và Andi Gutmans viết lại từ đầu – và trở thành cơ sở cho PHP3. PHP3 – bên cạnh khá nhiều tiện ích của PHP/FI – cũng được viết lại và bổ sung khá nhiều phần.

Đến tháng 10/2000, PHP3 và PHP4 được cài đặt trên 3300000 Website (so với con số 3800000 Website cài IIS). Phiên bản 4 sử dụng cơ chế Zend để nâng cao hiệu suất. Tháng 12/2004, phiên bản 5 ra đời với nhiều tính năng nổi bật

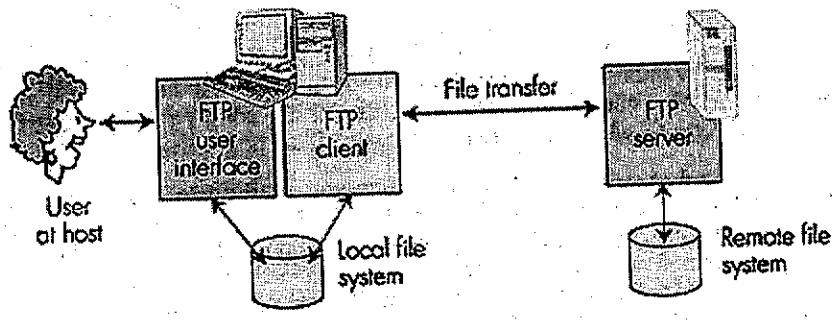
Hình 2.13 minh họa tốc độ phát triển của PHP




Hình 2.13 Tốc độ phát triển của PHP

## 2.3 TRUYỀN FILE (FILE TRANSFER) FTP

FTP (File Transfer Protocol) là giao thức truyền file giữa các máy tính. Giao thức này xuất hiện từ những năm 1971 (khi Internet vẫn chỉ là một dự án thử nghiệm) nhưng vẫn còn được sử dụng rộng rãi cho đến tận ngày nay. FTP được đặc tả trong RFC 959. Hình 2.14 minh hoạ các dịch vụ của FTP.



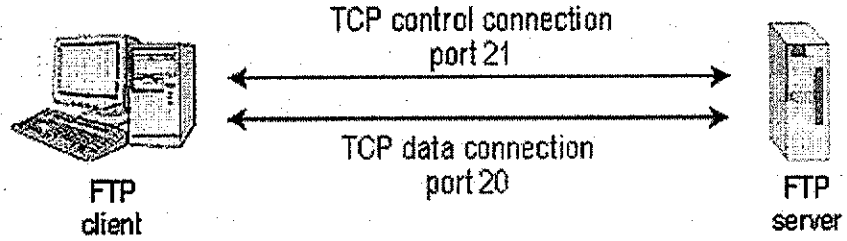

Hình 2.14 FTP cho phép trao đổi file giữa hai máy tính

Trong phiên làm việc của FTP, người dùng làm việc trên máy tính của mình và trao đổi file với một máy tính khác. Để truy cập tới máy tính khác, người dùng phải đăng nhập bằng cách cung cấp định danh người dùng



và mật khẩu. Sau khi những thông tin này được kiểm chứng thì công việc truyền file từ hệ thống file trên máy tính của mình đến hệ thống file ở đầu kia mới có thể được thực hiện.

Như mô tả trên Hình 2.15, người dùng tương tác với FTP thông qua chương trình giao tiếp người dùng của FTP. Đầu tiên người dùng đánh tên máy tính cần truyền file. Tiến trình FTP ở client khởi tạo một kết nối TCP tới tiến trình FTP server, sau đó người dùng đưa các thông tin về tên và mật khẩu để server kiểm chứng. Sau khi được server xác định, người dùng mới có thể thực hiện việc trao đổi file giữa hai hệ thống file.




Hình 2.15 FTP gồm hai đường: kiểm soát và dữ liệu

HTTP và FTP đều là giao thức truyền file và có rất nhiều đặc điểm chung như cả hai đều sử dụng các dịch vụ của TCP. Tuy vậy hai giao thức này có những điểm khác nhau cơ bản. Điểm khác nhau nổi bật nhất là FTP sử dụng hai kết nối TCP song song, một đường truyền thông tin điều khiển (control connection) và một đường truyền dữ liệu (data connection). Các thông tin điều khiển như thông tin định danh người dùng, mật khẩu truy nhập, lệnh thay đổi thư mục, lệnh "put" hoặc "get" file giữa hai máy tính được trao đổi qua đường truyền thông tin điều khiển. Đường truyền dữ liệu để truyền file dữ liệu thực sự. Vì FTP phân biệt luồng thông tin điều khiển với luồng dữ liệu nên nó được gọi là gửi thông tin điều khiển out-of-band. Giao thức RTSP dùng để truyền âm thanh và hình ảnh liên tục cũng sử dụng cách gửi thông tin điều khiển kiểu out-of-band. Như đã nói, HTTP gửi tiêu đề của thông điệp và file dữ liệu trên cùng một kết nối TCP. Vì vậy mà HTTP được gọi là gửi thông tin điều khiển in-band. Trong phần tiếp theo ta sẽ thấy rằng SMTP - giao thức gửi thư điện tử cũng sử dụng truyền thông tin điều khiển kiểu in-band. Đường truyền thông tin điều khiển và đường truyền dữ liệu của giao thức FTP được minh hoạ trong Hình 2.15.

Khi người dùng bắt đầu một phiên làm việc FTP, đầu tiên FTP sẽ thiết lập một đường kết nối thông tin điều khiển TCP qua cổng 21. Phía client của giao thức FTP gửi thông tin về định danh người dùng và mật khẩu cũng như lệnh thay đổi thư mục qua kết nối này. Khi người dùng có một yêu cầu trao đổi file (truyền từ/đến máy người dùng), FTP mở một kết nối TCP để truyền dữ liệu qua cổng 20. FTP truyền đúng một file qua kết nối này và ngay sau khi truyền xong thì đóng kết nối lại. Nếu trong cùng phiên làm việc, người dùng có yêu cầu truyền file thì FTP sẽ mở một kết nối khác. Như vậy với FTP, luồng thông tin điều khiển được mở và tồn tại trong suốt phiên làm việc của người dùng, nhưng mỗi kết nối dữ liệu được tạo ra cho mỗi một yêu cầu truyền file (kết nối dữ liệu là không liên tục).

Trong suốt phiên làm việc, FTP server phải giữ lại các thông tin về trạng thái của người dùng, đặc biệt phải kết hợp các thông tin điều khiển với tài khoản của người dùng. Server cũng lưu giữ thư mục hiện thời mà người dùng truy cập cũng như cây thư mục của người dùng. Ghi lại các thông tin trạng thái của mỗi phiên làm việc hạn chế đáng kể tổng số phiên làm việc đồng thời. HTTP không lưu giữ trạng thái nên không phải ghi lại bất kì thông tin nào về trạng thái người dùng.

### 2.3.1 Các lệnh FTP (FTP Commands)

Lệnh (yêu cầu) từ client đến server và kết quả (trả lời) từ server tới client được gửi thông qua kết nối điều khiển và được mã hoá bằng bảng mã ASCII 7 bit. Do vậy giống như lệnh HTTP, người ta có thể đọc được lệnh FTP. Trường hợp các lệnh viết liên tục thì cặp ký tự CR (carriage return) và LF (line feed) được sử dụng để phân biệt các lệnh (và trả lời). Mỗi câu lệnh chứa 4 kí tự ASCII in hoa, một số lệnh có tham số. Sau đây là một số câu lệnh hay gặp:

**USER username:** sử dụng để gửi thông tin định danh người dùng cho server

**PASS password:** dùng để gửi password cho server

**LIST:** dùng để yêu cầu server gửi một danh sách các file trong thư mục hiện thời. Danh sách này được gửi thông qua một kết nối dữ liệu TCP

**RETR filename:** dùng để lấy một file từ thư mục hiện thời (trên máy ở xa)

**STOR filename:** dùng để tải một file vào thư mục hiện thời (trên máy ở xa)



Thông thường có quan hệ 1-1 giữa lệnh của người dùng và lệnh của FTP. Ứng với mỗi lệnh từ client là một trả lời của server. Câu trả lời là một mã 3 chữ số và có thể có một thông báo kèm theo. Điều này tương tự như trường mã trạng thái trong thông điệp trả lời HTTP. Dưới đây là một số câu trả lời thường gặp:

331 username OK, password requiered

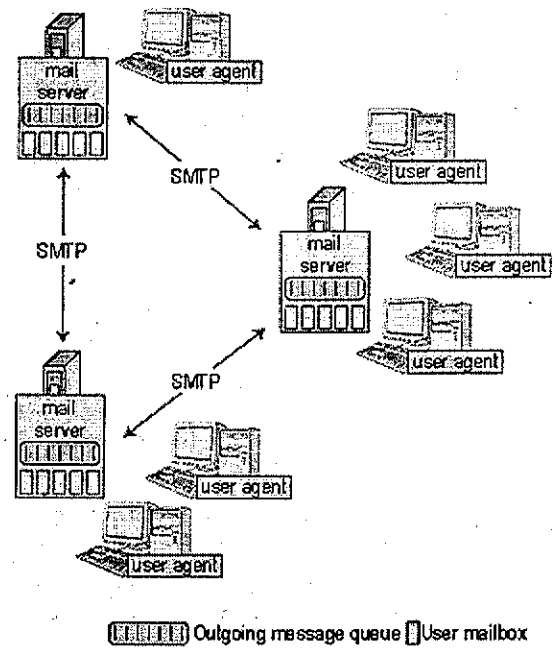
125 connection already open; Transfer staring

425 can't open data connection

452 error writing file

Chi tiết về FTP có thể tham khảo tại khuyến nghị RFC 959

## 2.4 THƯ TÍN ĐIỆN TỬ (E-mail) TRÊN INTERNET




**Hình 2.16 Mô hình hệ thống email đơn giản**

Cùng với Web, thư điện tử là một trong những ứng dụng Internet thông dụng nhất. Gần giống thư tín thông thường, e-mail là dịch vụ không

đòi hỏi đồng bộ - nghĩa là mọi người gửi và đọc thư khi thấy thuận tiện, không cần theo kế hoạch trước. Nhưng khác với thư tín thường, e-mail nhanh, dễ gửi và chi phí thấp. Hơn nữa, những thông điệp e-mail ngày nay có thể chứa đựng các hyperlink, văn bản định dạng HTML, hình ảnh, âm thanh và cả video. Trong phần này, chúng ta sẽ khảo sát các giao thức trao đổi thư thuộc tầng ứng dụng trên Internet.

Hình 2.16 minh hoạ hệ thống mail trên Internet gồm có 3 thành phần chính: user agent, mail server và SMTP (Simple Mail Transfer Protocol). Để tiện theo dõi, chúng ta sẽ lấy ví dụ Alice gửi e-mail cho Bob để mô tả 3 thành phần trên. Chương trình giao tiếp người dùng cho phép đọc, hồi âm, gửi, lưu giữ và soạn thảo các thư (user agent dành cho e-mail còn được gọi là mail reader – trình đọc thư. Mặc dù vậy, trong cuốn sách này, chúng ta sẽ tránh sử dụng thuật ngữ đó). Khi Alice soạn thảo xong thư, user agent của Alice sẽ gửi thư tới mail server của Alice, tại đây thư được đặt vào trong hàng đợi để gửi ra ngoài. Khi Bob muốn đọc thư, user agent của Bob sẽ lấy thư trên hộp thư (mail box) của Bob tại mail server. Trong những năm cuối thập kỷ 90, các user agent có giao diện đồ họa GUI (Graphic User Interface) khá thông dụng, chúng cho phép người dùng có thể xem và soạn thảo các thư có gắn tài liệu đa phương tiện. Hiện nay, những phần mềm soạn e-mail thông dụng là Eudora, Microsoft Outlook và Nescape Messenger. Có nhiều chương trình user agent có giao diện dựa trên nền văn bản gõ lệnh như là mail, pine và elm.

## *Trong lịch sử* HOTMAIL

Tháng 12/1995, Sabeer Bhatia và Jack Smith đề nghị Draper Fisher Jurvetson - một nhà đầu tư mạo hiểm phát triển một hệ thống email miễn phí trên nền Web. Ý tưởng là cung cấp miễn phí tài khoản (hòm thư) và việc truy cập tới hòm thư có thể thực hiện thông qua Web. Khi đó bất kỳ ai truy cập được vào Internet – dù ở nhà hay ở cơ quan - đều có khả năng đọc và gửi thư. Hơn thế nữa, hình thức này khá tiện dụng đối với người dùng hay phải di chuyển. Draper Fisher Jurvetson tài trợ cho Bhatia and Smith lập công ty Hotmail đổi lấy 15% giá trị công ty. Với 3 nhân viên làm cả ngày và 12 đến 14 nhân viên bán công nhật trả lương bằng cổ phiếu của chính công ty, Hotmail đã phát triển và cung cấp dịch vụ đầu tiên vào tháng 7 năm 1996. Sau một tháng họ có 100000 người sử dụng dịch vụ. Số lượng người sử dụng tăng lên nhanh chóng – và tất cả người sử dụng đều phải đọc banner quảng cáo trong email. Tháng 12/1997, chưa đầy 18 tháng sau khi khai trương, Hotmail có 12 triệu người sử dụng và đã được Microsoft mua lại với giá 400 triệu đôla.

Có hai yếu tố quan trọng trong thành công của Hotmail: sự tiên phong và khả năng tự quảng cáo. Hotmail là "người tiên phong" vì Hotmail là công ty đầu tiên cung cấp dịch vụ Web mail. Các công ty khác, sử dụng ý tưởng của Hotmail - đều đi sau Hotmail sáu tháng. Email là một ví dụ điển hình về sự tự quảng cáo. Khi nhận được thư từ dịch vụ Yahoo, người nhận sẽ biết được về Yahoo.



Máy chủ phục vụ thư (Mail server) là thành phần cốt lõi trong hệ thống e-mail. Mỗi người có một hộp thư đặt trên mail server. Hộp thư của Bob quản lý, lưu giữ các thư gửi tới Bob. Thư được tạo ra tại user agent của người gửi, được gửi tới mail server của người gửi, rồi tới mail server của người nhận – và cuối cùng được chuyển vào hộp thư của người nhận. Khi Bob muốn truy cập vào hộp thư của mình, mail server chứa hộp thư của Bob sẽ kiểm chứng Bob (thông qua username và password). Mail server của Alice cần phải xử lý khi mail server của Bob gặp sự cố. Nếu không thể gửi thư cho mail server của Bob, mail server của Alice sẽ giữ những thư đó trong hàng đợi gửi thông điệp và sẽ cố gắng gửi lại thông điệp. Quá trình gửi lại được tiến hành thường xuyên 30 phút một lần trong năm ngày. Và sau đó, nếu vẫn không thành công thì server sẽ huỷ bỏ thư và gửi thư báo cho người gửi (Alice).

SMTP (Simple Mail Transfer Protocol) là giao thức gửi thư điện tử của tầng ứng dụng. SMTP sử dụng dịch vụ truyền dữ liệu tin cậy của TCP để truyền thư từ mail server của người gửi đến mail server của người nhận. Giống các giao thức khác ở tầng ứng dụng, SMTP có 2 phía: phía client, trên mail server của người gửi và phía server, trên mail server của người nhận. Tất cả các mail server đều chạy cả hai phía client và server của SMTP. Mail server đóng vai trò client khi gửi thư, đóng vai trò server khi nhận thư.

### 2.4.1 SMTP

SMTP là trái tim của dịch vụ gửi thư trên Internet và được đặc tả trong RFC 821. SMTP truyền các thông điệp (thư) từ mail server của người gửi đến mail server của người nhận. SMTP ra đời trước HTTP khá lâu (RFC đặc tả SMTP có từ năm 1982 và SMTP đã xuất hiện trước đó một thời gian dài). Mặc dù có nhiều ưu điểm nên được tất cả mail server trên Internet sử dụng, SMTP vẫn là một công nghệ cũ nên chắc chắn có những đặc tính "lạc hậu". Ví dụ SMTP đòi hỏi phần thân của tất cả các thông điệp e-mail phải mã hoá theo bảng mã ASCII 7 bit. Sự hạn chế này là do trong những năm đầu thập kỷ 80, với số đường truyền ít ỏi, không ai gửi thư cùng với những phần đính kèm lớn, hay gửi kèm các file hình ảnh, âm thanh có kích thước

lớn. Nhưng trong kỷ nguyên đa phương tiện ngày nay, việc giới hạn mã ASCII 7 bit là một hạn chế lớn vì dữ liệu đa phương tiện nhị phân phải được chuyển sang mã ASCII trước khi được gửi đi qua SMTP và sau đó lại phải giải mã thành mã nhị phân sau khi thư đến đích. Trong mục 2.3 ta đã biết rằng HTTP không yêu cầu dữ liệu đa phương tiện phải mã hoá sang mã ASCII trước khi truyền.

Để minh hoạ hoạt động cơ bản của SMTP, hãy xét ví dụ sau: giả sử Alice muốn gửi cho Bob một thông điệp ASCII đơn giản:

Đầu tiên, Alice sử dụng user agent của mình, đánh địa chỉ e-mail của Bob (bob@somechool.edu), soạn e-mail và yêu cầu user agent gửi thư đi.

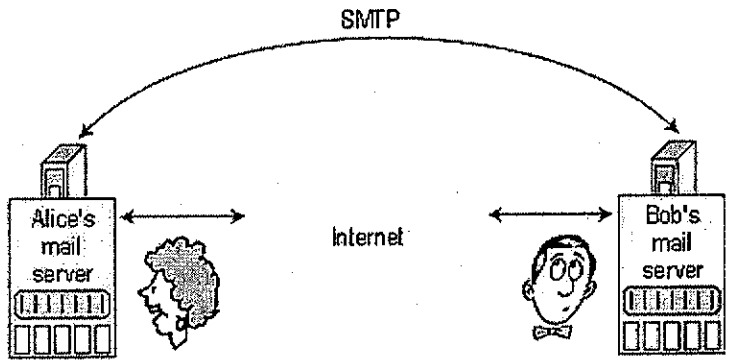
User agent của Alice gửi thư tới mail server của Alice. Tại đây thư được đặt vào hàng thư đợi gửi.

SMTP client chạy trên mail server của Alice thấy thư trong hàng đợi. Nó tạo kết nối TCP tới SMTP server trên mail server của Bob.

Sau giai đoạn khởi tạo 3 bước, SMTP client gửi thư của Alice qua kết nối TCP.

Tại mail server của Bob, SMTP server nhận thư và đặt thư vào mail box của Bob.

Cuối cùng, khi thuận tiện Bob sẽ sử dụng user agent của mình để đọc thư.




**Hình 2.17 Thư được gửi từ mail server của Alice đến mail server của Bob**



Kịch bản này được minh hoạ trên Hình 2.17. Một điểm quan trọng cần chú ý là SMTP không sử dụng mail server trung gian để gửi thư - ngay cả khi mail server gửi và nhận ở xa nhau. Ví dụ nếu mail server của Alice đặt ở Hồng Kông và mail server của Bob ở Mobile tiểu bang Alabama, thì giữa hai mail server ở Hồng Kông và Mobile vẫn có đường kết nối TCP trực tiếp. Đặc biệt nếu mail server của Bob bị hỏng thì thư vẫn còn trong mail server của Alice và đợi cho lần gửi sau. Thông điệp không được gửi qua mail server trung gian.

Bây giờ chúng ta có thể xem chi tiết cách thức các mail server gửi thư bằng SMTP. Chúng ta sẽ thấy rằng SMTP có nhiều đặc điểm tương tự như những quy tắc trong giao tiếp trực diện của con người. Đầu tiên, SMTP client (chạy trên mail server gửi) thiết lập kết nối TCP với cổng 25 tại SMTP server (chạy trên mail server nhận). Trong trường hợp server không làm việc, client sẽ cố gắng thử lại lần sau. Ngay khi kết nối được thiết lập, server và client thực hiện một vài thủ tục bắt tay. Quá trình này tương tự như hai người tự giới thiệu về bản thân trước khi tiến hành nói chuyện. Trong thủ tục trao đổi, SMTP client thông báo với SMTP server địa chỉ e-mail người gửi và địa chỉ email người nhận. Ngay sau quá trình giới thiệu, client sẽ gửi thư bằng dịch vụ truyền dữ liệu tin cậy của TCP. Sau đó, client sẽ lặp lại các bước này khi vẫn còn thông điệp khác để gửi tới server, còn nếu không, client yêu cầu TCP đóng kết nối lại.

Ví dụ sau là đoạn "hội thoại" giữa client (C) và server (S). Tên máy tính client là crepes.fr và server là hamburger.edu. Dòng hội thoại mở đầu bằng chữ C: là đoạn hội thoại client gửi qua socket TCP và dòng hội thoại bắt đầu với chữ S: là đoạn hội thoại server gửi đi thông qua socket TCP. Đoạn hội thoại bắt đầu ngay sau khi thiết lập được kết nối TCP:

```
S: 220 hambuger.edu
C: HELO crepes.fr
S: 250 Hello crepes. fr, pleased to meet you
C: MAIL FROM: <alice@crepes. fr>
S: 250 alice@crepes. fr... Sender ok
C: RCPT TO: <bob@hamburger. edu>
S: 250 bob@hamburger. edu ...Recipient ok
C: DATA
S: 354 Enter mail, end with ". " On a line by itself
C: Do you like ketchup?
C: How about pickles ?
C: .
S: 250 Message accepted for delivery
C: QUIT
S: 221 hambuger. edu closing connection.
```

Trong ví dụ trên, client gửi một thông điệp ("Do you like ketchup? How about pickles?") từ mail server crepes.fr tới mail server hamburger.edu. Client sử dụng 5 câu lệnh: HELO (viết tắt của HELLO), MAIL FROM, RCPT TO, DATA và QUIT. Ý nghĩa của những câu lệnh này có thể đoán được qua tên gọi của nó. Server gửi trả kết quả thực hiện mỗi lệnh, kết quả này chứa một mã trạng thái và một lời giải thích tiếng Anh. Ở đây SMTP sử dụng kết nối liên tục: Nếu có nhiều thư để gửi tới cùng một mail server thì mail server gửi sẽ gửi tất cả các thư trên cùng một kết nối TCP. Với mỗi thông điệp, client bắt đầu tiến trình gửi bằng lệnh HELO crepes.fr và chỉ gửi lệnh QUIT sau khi gửi tất cả thư.

Độc giả nên sử dụng Telnet để xem một đoạn hội thoại trực tiếp với SMTP server. Sử dụng telnet serverName 25 trong đó serverName là tên mail server. Khi đó bạn đã thiết lập kết nối TCP giữa máy tính của bạn và mail server. Sau khi đánh lệnh này, bạn sẽ nhận được ngay lập tức mã trả lời 220 từ server. Sau đó hãy sử dụng các lệnh SMTP: HELO, MAIL FROM, RCPT TO, DATA, QUIT ở những thời điểm tương ứng. Nếu bạn telnet qua SMTP server của ai đó, bạn có thể gửi tới họ theo cách này (không phải dùng user agent).

## 2.4.2 So sánh SMTP với HTTP

Chúng ta hãy cùng so sánh vắn tắt hai giao thức SMTP và HTTP. Cả hai giao thức đều được sử dụng để gửi file giữa các máy tính. HTTP chuyển file hoặc đối tượng từ Web server tới Web client (trình duyệt Web), SMTP chuyển file (là thông điệp thư điện tử) giữa các mail server. Khi truyền file cả 2 giao thức HTTP và SMTP cùng sử dụng kết nối liên tục. Điểm khác biệt cơ bản giữa hai giao thức là HTTP là giao thức kiểu kéo (Pull protocol) – client "kéo" thông tin từ server về. Phía nhận (client) là phía thiết lập kết nối TCP. SMTP lại là giao thức theo kiểu đẩy (Push protocol) – client "đẩy" thông tin lên server. Phía gửi (client) là phía thiết lập kết nối TCP trước.

Ngoài dữ liệu văn bản, thông điệp còn có thể chứa các kiểu dữ liệu khác như âm thanh, hình ảnh. HTTP đặt các đối tượng này trong các thông điệp riêng rẽ để gửi. Với SMTP tất cả các đối tượng này được đặt trong cùng một thư điện tử.



## 2.4.3 Khuôn dạng thư và chuẩn MIME

Khi Alice gửi thư cho Bob, Alice sẽ đặt thư vào phong bì, ghi rõ địa chỉ gửi và địa chỉ nhận, nhân viên bưu điện sẽ đóng dấu ngày tháng vào phong bì. Thư điện tử cũng giống như vậy, bên cạnh nội dung bức thư (phần thân) cũng cần có địa chỉ người gửi, địa chỉ người nhận. Những thông tin phụ trợ này sẽ được đặt trong các dòng tiêu đề. Các dòng tiêu đề và phần thân của thư được tách biệt với nhau bằng cặp ký tự CR-LF. RFC 822 đặc tả đầy đủ các dòng tiêu đề cũng như ý nghĩa của chúng. Giống HTTP, tiêu đề gồm từ khoá, theo sau là dấu hai chấm (":") và một giá trị nào đó. Với SMTP có một số trường bắt buộc, một số trường không bắt buộc. Tiêu đề phải có trường **From:** và trường **To:** Một số trường như **Subject:** có thể có hoặc không. Lưu ý rằng những trường này khác những lệnh SMTP mà chúng ta đã đề cập trong mục 2.4.1 (mặc dù chúng cũng có "From" và "To"). Các lệnh là một phần trong giai đoạn khởi tạo của SMTP trong khi các trường nằm ngay trong thư.

Một bức thư thường có tiêu đề như sau:

```
From: alice@crepes. fr
To: bob@hamburger. edu
Subject: Searching for the meaning of life
```

Sau phần tiêu đề thông điệp là một dòng trống, tiếp đến là thân thông điệp (dạng mã ASCII). Như đã nói ở trên, thông điệp kết thúc bằng một dòng chỉ chứa một dấu chấm câu. Bạn nên sử dụng Telnet để gửi tới mail server một thông điệp có chứa một vài dòng tiêu đề, bao gồm dòng tiêu đề **Subject:** Có thể thử điều này bằng cách telnet vào một mail server: telnet serverName 25 trong đó serverName là tên (hoặc địa chỉ IP) của máy tính.

### Mở rộng MIME cho dữ liệu không thuộc dạng ASCII

Phần tiêu đề thông điệp được đặc tả trong RFC 822 phù hợp cho việc gửi văn bản nhưng lại không đầy đủ để gửi thư chứa nội dung đa phương tiện (multimedia) - là thư có đính kèm ảnh, audio, video hoặc các thư chứa các ký tự khác tiếng Anh. Để gửi dữ liệu không thuộc dạng văn bản ASCII, user agent gửi phải gửi thêm một số trường trong tiêu đề của

thư. Những trường này được đặc tả trong RFC 2045 và RFC 2046, là phần mở rộng MIME (Multipurpose Internet Mail Extension) cho RFC 822.

Hai trường MIME hỗ trợ multimedia là **Content-Type**: và **Content-Transfer-Encoding**. Trường **Content-Type** cho phép phía nhận thực hiện các thao tác thích hợp trên thư nhận được. Ví dụ, nếu chỉ ra thân thông điệp chứa ảnh JPEG, user agent nhận có thể gửi thân thông điệp tới chương trình giải nén JPEG. Để gửi thông điệp văn bản không mã hoá theo bảng mã ASCII (ví dụ văn bản tiếng Trung Quốc, Nhật Bản), người ta phải mã hoá nó theo bảng mã ASCII để không làm ảnh hưởng tới SMTP. Trường **Content-Transfer-Encoding**: xác định phần thân thông điệp đã được mã hoá theo bảng mã ASCII và phương pháp mã hoá được sử dụng. Vì vậy khi user agent nhận được một thông điệp với hai tiêu đề trên, đầu tiên nó sử dụng giá trị của tiêu đề **Content-Transfer-Encoding**: để chuyển đổi thân thông điệp về dạng ban đầu (không theo định dạng ASCII) và sau đó sử dụng trường **Content-Type** để xác định thao tác thực hiện kế tiếp.

Xét ví dụ sau, giả sử Alice muốn gửi một ảnh JPEG cho Bob. Để thực hiện điều này, Alice sử dụng phần mềm Eudora, đánh địa chỉ email của Bob, chủ đề của e-mail và chèn ảnh JPEG vào thân thông điệp. Sau khi hoàn tất việc soạn thảo, Alice nhấn nút "Send". Sau đó, user agent của Alice tạo ra một thông điệp MIME có nội dung sau:

```
From: alice@crepes. fr
To: bob@hamburger. edu
Subject: Picture of yummy crepe.
MIME-Version: 1. 0
Content-Transfer-Encoding: base64
Content-Type: Image/jpeg

(base64 encoded data .....
.....
.... base64 encoded data )
```

Với thông điệp MIME trên, chúng ta thấy rằng user agent của Alice mã hoá ảnh JPEG sử dụng kỹ thuật mã hoá base64. Đây là một trong những kỹ thuật mã hoá chuẩn trong MIME [RFC 2045] để biến đổi sang định dạng mã ASCII 7 bit.



Khi Bob đọc thư, user agent của Bob xử lý thông điệp MIME này. Thấy trường **Content-Transfer-Encoding: base64**, nó thực hiện giải mã thân thông điệp đã được mã hoá bằng kỹ thuật base64. Trường **Content-Type: image/jpeg** giúp cho user agent của Bob xác định rằng thân của thông điệp phải được giải nén theo chuẩn JPEG. Cuối cùng, thông điệp chứa trường **MIME-Version:** xác định phiên bản MIME đang được sử dụng. Lưu ý rằng, thông điệp cũng phải tuân theo khuyến nghị RFC 822/SMTP.

Theo đặc tả MIME trong khuyến nghị RFC 2046, trường **Content-Type:** có khuôn dạng sau:

**Content-Type: type/subtype; parmeters**

Phần tham số (parameters) đi sau dấu chấm phẩy có thể không bắt buộc. Trong khuyến nghị RFC 2046, trường Content-Type được sử dụng để xác định kiểu dữ liệu trong phần thân của thông điệp MIME, gồm hai giá trị: kiểu dữ liệu và kiểu con. Sau phần kiểu và kiểu con là phần tham số. Nói chung, kiểu cao nhất (top-level) được sử dụng để khai báo kiểu dữ liệu chung, kiểu con (subtype) xác định định dạng đặc biệt trong kiểu dữ liệu chung. Các tham số bổ nghĩa cho kiểu và không ảnh hưởng tới bản chất kiểu dữ liệu. Tập hợp tham số phụ thuộc vào kiểu và kiểu con.

Được thiết kế để có thể mở rộng, số lượng các cặp type/subtype và những tham số đi kèm trong MIME ngày càng tăng. Để bảo đảm là tập hợp này phát triển có trình tự, được đặc tả rõ ràng, MIME cần thiết lập quá trình đăng ký với IAAN (Internet Assigned Numbers Authority) là cơ quan đăng ký trung tâm. Tiến trình đăng ký kiểu dữ liệu được đặc tả trong khuyến nghị RFC 2048.

Hiện nay, mới có định nghĩa cho bảy nhóm dữ liệu chính. Với mỗi kiểu lại có một danh sách các kiểu con và danh sách này đang tăng lên hàng năm. Dưới đây là 5 nhóm dữ liệu chính:

**Văn bản (Text)**: Kiểu văn bản được sử dụng để xác định thân thông điệp chứa thông tin dạng văn bản. Một kiểu con thường gặp là plain (trơn). Văn bản trơn không có lệnh hay chỉ dẫn định dạng khuôn dạng và do đó không cần phần mềm đặc biệt nào để hiển thị. Nếu nhìn tiêu đề MIME của thư trong hộp thư, bạn có thể sẽ thấy trên tiêu đề có trường **text/plain;**

**charset="us-ascii"** hay **text/plain; charset="ISO-8859-1"**. Những tham số này xác định bộ mã mà thông điệp sử dụng. Một kiểu con khác cũng rất thông dụng là text/html. Kiểu con *html* yêu cầu mail server thông dịch những thẻ HTML gắn trong thông điệp. Điều này cho phép user agent nhận hiển thị thông điệp dưới dạng một trang Web (với font, hyperlink, applet).

**Ảnh (Image)**: Kiểu ảnh được dùng để xác định thân thông điệp là ảnh. Hai kiểu con thông dụng là image/gif và image/jpeg. Với kiểu con image/gif, muốn hiển thị ảnh, user agent phải giải nén ảnh GIF.

**Âm thanh (Audio)**: Kiểu audio yêu cầu nội dung được gửi ra thiết bị audio (speaker hoặc telephone). Kiểu con thông dụng là basic (mã theo luật μ 8-bit cơ sở) và 32kadpcm (định dạng 32kps được đặc tả trong RFC 1911).

**Video**: Kiểu video có kiểu con là mpeg và quicktime.

**Kiểu ứng dụng (Application)**: Kiểu ứng dụng dành cho dữ liệu không thuộc bất kỳ kiểu nào khác. Nó thường được áp dụng cho loại dữ liệu phải qua một ứng dụng khác xử lý trước khi người nhận có thể sử dụng được. Ví dụ khi người gửi gắn một tài liệu MS Word vào thông điệp E-mail, user agent đặt giá trị application/msword vào trường type/subtype. Khi user agent thấy giá trị application/msword trong trường type/subtype, nó khởi động ứng dụng MS Winword và chuyển phần thân thông điệp MIME cho ứng dụng Word. Một kiểu con quan trọng khác là octerstream. Kiểu con này thường được dùng khi thân thông điệp chứa dữ liệu nhị phân tuỳ ý. Khi nhận kiểu con này, mail reader sẽ yêu cầu người nhận lựa chọn để lưu thông điệp trên đĩa xử lý sau.

Có một kiểu MIME đặc biệt quan trọng là kiểu **multipart**. Thông điệp e-mail cũng như trang Web có thể chứa nhiều đối tượng (như văn bản, ảnh, applet). Web gửi mỗi đối tượng trong một thông điệp trả lời độc lập nhưng thư điện tử đặt tất cả các đối tượng trong cùng một thông điệp. Đặc biệt, khi thông điệp đa phương tiện có nhiều đối tượng thì thông điệp đó có kiểu là **multipart/mixed**. Khi nhận được một thông điệp mà trường **content-type** có giá trị **multipart/mixed,** user agent nơi nhận biết thông điệp nhận được chứa nhiều đối tượng. Khi nhận được thông điệp như vậy, user agent phải xác định rõ:



Điểm đầu và điểm cuối của đối tượng.

Cách mã hoá các đối tượng không theo bảng mã ASCII.

Kiểu của mỗi đối tượng.

Công việc này được thực hiện nhờ ký tự phân cách giữa các đối tượng và trường **Content-type, Content-Transfer-Encoding** đứng trước mỗi đối tượng trong thông điệp. Xét ví dụ sau: Giả sử Alice muốn gửi thông điệp bao gồm một đoạn văn bản ASCII, một ảnh JPEG và cuối cùng là một đoạn văn bản ASCII cho Bob. Sử dụng user agent của mình, Alice đánh một đoạn văn bản, chèn ảnh JPEG sau đó đánh tiếp đoạn văn bản còn lại. Kết quả là user agent của Alice tạo ra một thông điệp như sau:

```
From: alice@crepes. fr
To: bob@hamburger. edu
Subject: Picture of yummy crepe with commentary
MIME-Version: 1. 0
Content-Type: multipart/mixed; Boundary=StartOfNextPart
--StartOfNextPart
Dear Bob,
Please find a picture of an absolutely scrumption crepe.
--StartOfNextPart
Content-Transfer-Encoding: base64
Content-Type: image/jpeg
base64 encoded data ....
.....
..... base64 encoded data
--StartOfNextPart
Let me know if you would like the recipe.
```

Qua thông điệp trên chúng ta thấy rằng trường **Content-Type**: trong tiêu đề xác định cách thức phân cách các phần khác nhau trong cùng một thông điệp. Việc phân cách được bắt đầu bằng 2 dấu gạch ngang (--) và kết thúc bằng cặp ký tự CRLF.

**Nhận thông điệp**

Thông điệp e-mail bao gồm nhiều phần, lõi của thông điệp là phần thân chứa dữ liệu thực sự được chuyển từ người gửi đến người nhận. Với

thông điệp nhiều phần, thân thông điệp gồm nhiều phần và trước mỗi phần có một hoặc vài trường xác định kiểu. Đứng trước thân thông điệp là cặp CRLF và một số trường. Những trường như **From:**, **To:**, và **Subject:** được đặc tả trong RFC 822 và những trường như **Content-type:** và **Content-Transfer-Encoding:** là tiêu đề MIME. Nhưng chính mail server nhận thông điệp cũng chèn vào thông điệp một số trường khác, ví dụ **Received:** ở đầu thông điệp. Trường này xác định tên của SMTP server gửi thông điệp ("from"), tên của SMTP server nhận thông điệp ("by") và thời gian khi thông điệp tới đích. Người đọc sẽ đọc được thông điệp như sau:

**Received: from crepes. fr by hamburger. edu; 12 Oct 98 15:27:39 GMT**
**From: alice@crepes. fr**
**To: Bob@hamburger. edu**
**Subject: Picture of yummy crepe.**
**MIME-Version: 1. 0**
**Content-Transfer-Encoding: base64**
**Content-Type: image/jpeg**

**base64 encoded data .....**
**.....**
**..... base64 encoded data**

Thực ra tất cả mọi người khi dùng e-mail đều nhìn thấy trường **Received:** đứng trước thông điệp e-mail (trường này có thể nhìn thấy trực tiếp trên màn hình hoặc khi in thư). Có thể có những thông điệp có nhiều trường **Received:** và trường **Return-Path**: phức tạp. Đó là vì thông điệp này có thể được chuyển tiếp (forward) qua nhiều mail server trước khi đến tay người nhận. Ví dụ nếu Bob cấu hình mail server của mình (hamburger.edu) gửi chuyển tiếp tất cả các thư của Bob tới sush.jp, khi đó tất cả các thư của Bob khi lấy từ sush.jp sẽ có những trường sau:

Received: from hamburger. edu by sushi. jp; Oct 98 15:30:01 GMT

Received: from crepes. fr by hamburger. edu; 12 Oct 98 15:27:39 GMT

Những trường này cho phép người nhận theo dõi vết đường đi của thư qua nhiều SMTP server cũng như thời gian thư tới mỗi server.



## 2.4.4 Giao thức truy nhập mail

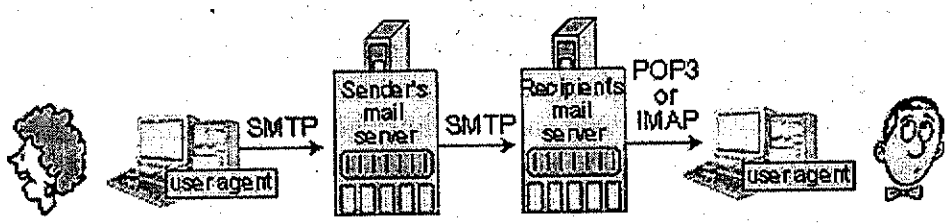
Mỗi khi SMTP gửi thư từ mail server của Alice tới mail server của Bob, thư được đặt trong mail box của Bob. Từ trước tới giờ, chúng ta chấp nhận giả thiết để đọc thư, Bob phải đăng nhập vào mail server và sử dụng một chương trình đọc thư (mail reader) nào đó cài ngay trên mail server. Tới tận đầu những năm 90, mọi người vẫn thực hiện như vậy. Nhưng ngày nay mọi người thường đọc thư qua một user agent chạy trên máy tính cá nhân của mình. Chạy user agent trên máy tính cá nhân, người sử dụng có được nhiều tính năng cao cấp, kể cả việc gửi và nhận những thông điệp đa phương tiện.

Giả sử Bob (người nhận) chạy user agent của mình trên máy tính cá nhân. Có thể cài đặt mail server ngay trên máy tính cá nhân của Bob. Tuy nhiên cách này có nhiều nhược điểm. Mail server quản lý nhiều mailbox, thực hiện cả chức năng client và server của SMTP. Nếu cài mail server trên máy tính cá nhân của Bob thì PC đó lúc nào cũng phải bật và kết nối vào Internet để có thể nhận thư mới (mà thư thì có thể đến bất cứ lúc nào). Điều này không thực tế với đa số người sử dụng Internet. Thông thường, người sử dụng chạy chương trình user agent trên máy tính cá nhân, truy cập vào hộp thư trên một mail server dùng chung (mail server này luôn luôn kết nối tới Internet và được chia sẻ giữa nhiều người dùng khác). Mail server thường được ISP của người dùng (là trường đại học hoặc công ty) quản lý.

Do user agent chạy trên máy tính cá nhân và mail server được quản lý bởi các ISP nên cần có một giao thức cho phép user agent và mail server trao đổi với nhau. Đầu tiên chúng ta xét trường hợp thư được tạo ra tại PC của Alice được chuyển tới mail server của Bob như thế nào. Công việc này có thể được thực hiện một cách đơn giản bằng việc user agent của Alice trao đổi trực tiếp với mail server của Bob bằng giao thức SMTP. User agent của Alice sẽ khởi tạo một kết nối TCP tới mail server của Bob, gửi những lệnh khởi tạo SMTP, tải thư lên bằng lệnh DATA và sau đó đóng kết nối lại. Cách tiếp cận này hoàn toàn có thể thực hiện được nhưng ít khi được dùng vì nó không hỗ trợ trường hợp mail server phía nhận bị trục trặc. Trên thực tế, user agent gửi khởi tạo SMTP để tải thư của Alice tới chính mail server

của Alice (chứ không phải là mail server của người nhận thư). Mail server của Alice sau đó sẽ thiết lập một phiên làm việc SMTP tới mail server của Bob để gửi tiếp thư tới mail server của Bob. Nếu mail server của Bob ngừng làm việc thì mail server của Alice sẽ giữ thư lại và sau đó cố gắng gửi lại. RFC SMTP có những lệnh để gửi tiếp thư qua nhiều SMTP server.

Vậy user agent chạy trên máy tính cá nhân của Bob lấy thông điệp trong hộp thư trên mail server của Bob như thế nào ? Giải pháp là phải có một giao thức lấy thư cho phép chuyển thư từ mail server của Bob tới máy tính cục bộ. Hiện nay có 2 giao thức lấy thư thông dụng là **POP3 (Post Office Protocol - Version 3)** và **IMAP (Internet Mail Access Protocol)**. Dưới đây, chúng ta sẽ trình bày cả hai giao thức này. Lưu ý rằng user agent của Bob không thể sử dụng SMTP để lấy thư bởi vì lấy thư giống như việc "kéo" trong khi SMTP là một giao thức "đẩy". Hình 2.18 minh hoạ về việc gửi và nhận thư. SMTP được dùng để chuyển thư giữa các mail server hay giữa user agent của người gửi và mail server của người gửi. POP3 hay IMAP được dùng để chuyển thư từ mail server tới user agent của người nhận.




**Hình 2.18 Giao thức email và các thực thể truyền thông**

## POP3

POP3 được đặc tả trong RFC 1939 là giao thức lấy thư cực kỳ đơn giản và có rất ít chức năng. POP3 được khởi tạo khi user agent (client) tạo kết nối TCP tới mail server (server) qua cổng 110. Sau khi thiết lập được kết nối TCP, POP3 gồm 3 giai đoạn: kiểm chứng, tiến hành xử lý và cập nhật. Trong giai đoạn kiểm chứng đầu tiên, user agent sử dụng tên và mật khẩu để xác nhận người sử dụng. Trong giai đoạn tiến hành xử lý thứ hai, user agent tiến hành lấy thư. Nó có thể đánh dấu các thư để xoá hay hủy bỏ việc đánh



dấu xoá. Giai đoạn ba - cập nhật, xảy ra sau khi client ra lệnh quit để kết thúc phiên làm việc POP3. Tại thời điểm đó mail server xoá tất cả thư được đánh dấu.

Trong giai đoạn xử lý, user agent gửi lệnh và server trả lời kết quả thực hiện của mỗi lệnh đó. Mỗi lệnh có hai trạng thái kết quả: +OK thông báo lệnh vừa gửi được thực hiện đúng và –ERR thông báo lệnh vừa gửi không thực hiện được.

Giai đoạn kiểm chứng có 2 lệnh là **user <username>** và **pass <password>**. Để minh hoạ hai lệnh này bạn nên Telnet trực tiếp qua một server POP3 sử dụng cổng 110 để thực hành. Giả sử mail server là tên mail server, bạn có thể làm như sau:

```
telnet mail server 110
+OK POP3 server ready
user alice
+OK
pass hungry
+OK user successfully logged on
```

Nếu bạn đánh sai một lệnh thì server POP3 sẽ đáp lại bằng một thông điệp –ERR.

Người sử dụng có thể cấu hình user agent ở một trong hai chế độ "tải và xoá" ("download and delete") hay "tải và giữ" ("download và keep"). Chuỗi lệnh được user agent gửi phụ thuộc vào cấu hình này. Trong chế độ đầu, user agent sẽ phát ra chuỗi lệnh **list, retr** và **dele**. Giả sử người dùng có 2 thông điệp trong hộp thư của mình. Trong đoạn hội thoại dưới đây C: (client) là user agent và S: (server) là mail server. Khi đó giai đoạn xử lý công việc sẽ như sau:

```
C: list
S: 1 498
S: 2 912
S: .
C: retr 1
S: (blah blah ...
```

S: .....
S: ..... blah)
S:.
C: dele 1
C: retr 2
S: (blah blah ....
S: .....
S: .....blah)
S:.
C: dele 2
C: quit
S: +OK POP3 server signing off

Đầu tiên, user agent yêu cầu mail server liệt kê kích thước của tất cả thư lưu trữ trong hộp thư. Sau đó, user agent lấy và xoá từng thư trong hộp thư. Lưu ý rằng sau giai đoạn kiểm chứng người dùng chỉ còn 4 câu lệnh là **list, retr, dele** và **quit**. Cú pháp của các lệnh này được đặc tả trong RFC 1939. Sau khi xử lý lệnh quit, server POP3 vào giai đoạn cập nhật và xoá thư 1, 2 trong mailbox.

Trong chế độ này, khi Bob lấy thư từ những địa điểm khác nhau, thư của Bob sẽ nằm rải rác trên nhiều máy. Đặc biệt, nếu Bob đã lấy thư từ máy tính ở nhà thì sau đó sẽ không thể đọc lại thư đó trên máy tính ở cơ quan. Trong chế độ thứ hai "download and keep", user agent vẫn để lại thư trên mail server sau khi đã tải về. Khi đó Bob vẫn có thể đọc thư từ nhiều máy khác nhau.

Trong phiên làm việc POP3 giữa user agent và mail server, server POP3 sẽ ghi nhớ một vài thông tin trạng thái – ví dụ các thư đã bị đánh dấu xoá. Tuy nhiên server POP3 không chuyển thông tin trạng thái giữa các phiên làm việc khác nhau. Ví dụ không có thư nào được đánh dấu xoá ở đầu mỗi phiên làm việc. Điều này làm đơn giản công việc xây dựng một server POP3.

## IMAP

Sau khi tải thư về từ máy tính cá nhân, Bob có thể tạo những thư mục chứa thư và chuyển thư vào trong các thư mục đó. Sau đó Bob có thể



xoá, chuyển thư giữa các thư mục hay tìm kiếm thư theo tên người gửi và chủ đề thư. Phương thức như vậy bất tiện với người sử dụng muốn đọc thư từ nhiều nơi vì họ thích duy trì phân cấp thư mục trên mail server để có thể truy cập được từ bất kỳ máy tính nào. POP3 không đáp ứng được yêu cầu này.

IMAP (đặc tả trong RFC 2060) có thể giải quyết vấn đề này. Giống POP3, IMAP cũng là giao thức lấy thư. Nó có nhiều đặc tính phức tạp hơn POP3. IMAP được thiết kế cho phép người dùng thao tác trên những hộp thư ở xa một cách dễ dàng. IMAP cho phép Bob tạo những thư mục thư khác nhau trong mailbox. Bob có thể đặt thư vào trong thư mục hay dịch chuyển thư từ thư mục này đến những thư mục khác. IMAP cũng có lệnh cho phép tìm kiếm trên thư mục theo tiêu chí xác định. IMAP phức tạp hơn POP3 nhiều vì server IMAP phải duy trì hệ thống thư mục cho mọi người dùng. Những thông tin trạng thái như thế phải được mail server lưu giữ cho tất cả các phiên làm việc. Nên nhớ rằng POP3 server không lưu giữ trạng thái của mỗi người dùng sau khi phiên làm việc kết thúc.

IMAP có một đặc tính quan trọng là có những lệnh cho phép user agent chỉ lấy một số thành phần trong thư. Ví dụ: user agent có thể lấy phần tiêu đề hoặc một phần trong thư có nhiều phần. Điều này rất có ích khi kết nối giữa useragent và mail server chậm, người dùng có thể không cần tải tất cả thư trong hộp thư của mình. Đặc biệt có thể tránh tải những thư chứa nội dung âm thanh hay hình ảnh có kích thước lớn.

Phiên làm việc IMAP gồm 3 giai đoạn: giai đoạn thiết lập kết nối giữa client (user agent) và IMAP server, giai đoạn server chấp nhận kết nối và giai đoạn tương tác client/server. Tương tác client/server của IMAP tương tự nhưng phong phú hơn nhiều tương tác trong POP3. Server luôn ở một trong bốn trạng thái. Trong trạng thái **chưa kiểm chứng (nonauthenticated)** là trạng thái khởi đầu, khi đó người dùng phải đăng nhập hệ thống trước khi thực hiện các lệnh. Trạng thái **đã kiểm chứng (authenticated)**, người dùng phải chọn một thư mục trước khi gửi lệnh. Trong trạng thái **lựa chọn (selected)**, người dùng có thể sử dụng những lệnh có thể tác động tới thông điệp (như lấy, xoá, chuyển thư). Cuối cùng là trạng thái **thoát (logout)**, khi kết thúc phiên làm việc. Bạn có thể đọc tất cả về IMAP tại [IMAP 1999].

**HTTP**

Ngày nay, nhiều người sử dụng Webmail - dịch vụ có thể truy cập email qua trình duyệt (Hotmail hay Yahoomail). Khi đó, user agent là trình duyệt Web thông thường và mọi người kết nối tới hộp thư của mình trên mail server qua HTTP. Khi Bob muốn đọc thư, thư được gửi từ mail server của Bob tới trình duyệt nhờ giao thức HTTP chứ không phải là giao thức POP3 hay IMAP. Khi người gửi (Alice) có một tài khoản (account) trên mail server muốn gửi thư, thư sẽ được gửi từ trình duyệt của Alice tới mail server nhờ giao thức HTTP chứ không sử dụng SMTP. Tuy nhiên, mail server đó vẫn gửi và nhận thư với những mail server khác bằng giao thức SMTP. Giải pháp truy cập mail kiểu như vậy vô cùng thuận tiện cho người sử dụng hay phải di chuyển. Họ chỉ cần sử dụng một trình duyệt để gửi và nhận thư. Trình duyệt đó có thể ở một quán café Internet, ở nhà của bạn bè, ở khách sạn với Web TV... Giống IMAP người dùng có thể tổ chức thư của mình trong hệ thống thư mục trên mail server. Sự thật là, e-mail dựa trên Web ngày càng thuận tiện và dần dần thay thế POP3 và IMAP trong những năm tới. Nhược điểm chính yếu của nó là chậm, bởi vì server và client ở xa, giao tiếp giữa chúng phải thông qua CGI.

## 2.5 DỊCH VỤ TÊN MIỀN - DNS

Cá nhân mỗi con người có thể được xác định theo nhiều cách. Ví dụ, chúng ta có thể được nhận biết qua tên trong giấy khai sinh, bằng số chứng minh thư nhân dân. Dù có nhiều cách nhận biết để phân biệt mọi người nhưng lựa chọn phương thức nhận biết phụ thuộc vào hoàn cảnh. Ví dụ công an sử dụng số chứng minh thư nhân dân chứ không sử dụng tên. Bình thường mọi người thích nhớ tên nhau hơn là số chứng minh thư.

Giống con người, máy tính trên Internet cũng có thể được xác định bằng nhiều cách. Tên máy tính (host name) là một cách, ví dụ cnn.com, www.yahoo.com, gais.umass.edu hay surf.eurecom.fr. Những tên đó tương đối dễ nhớ đối với con người. Tuy nhiên tên máy tính cung cấp ít thông tin về vị trí trên Internet của máy tính (Tên máy tính surf.eurecom.fr chỉ cho



chúng ta biết máy tính đó ở nước Pháp vì kết thúc bằng đuôi .fr, ngoài ra không còn thông tin nào khác). Hơn nữa tên máy tính bao gồm nhiều ký tự - cả chữ cái và chữ số - có độ dài thay đổi nên router khó có thể xử lý được. Vì lý do đó, máy tính được xác định thông qua địa chỉ IP. Địa chỉ IP được thảo luận chi tiết trong chương 4. Địa chỉ IP gồm có 4 byte và có cấu trúc phân cấp, giá trị mỗi byte lại được đổi ra số thập phân (0-255) và cách nhau bằng dấu chấm (ví dụ 121.23.45.5). Địa chỉ IP phân cấp vì khi duyệt địa chỉ từ trái qua phải, chúng ta nhận được thêm nhiều thông tin xác định về vị trí của máy tính trên Internet (Vị trí ở trong mạng của các mạng, trong một mạng...). Điều này tương tự khi xét địa chỉ bưu điện từ dưới lên, chúng ta nhận được nhiều thông tin về địa chỉ đó.

### 2.5.1 Các dịch vụ của DNS

Có hai cách để xác định một máy tính: dựa vào tên máy tính hoặc địa chỉ IP. Con người thích sử dụng tên máy dễ nhớ, trong khi router lại sử dụng địa chỉ IP có cấu trúc phân cấp và độ dài cố định (dễ xử lý). Để dung hoà giữa hai cách, chúng ta cần một dịch vụ chỉ dẫn để chuyển đổi tên máy tính sang địa chỉ IP và đây chính là nhiệm vụ của hệ thống tên miền trên Internet (DNS). DNS là (1) Cơ sở dữ liệu phân tán được đặt trên một hệ thống phân cấp các máy phục vụ tên (nameserver) và (2) Giao thức thuộc tầng ứng dụng cho phép máy tính và máy chủ tên trao đổi thông tin phục vụ mục đích xác định địa chỉ IP. Máy chủ tên miền thường là các máy UNIX c cài đặt phần mềm Berkely Internet Name Domain (BIND). Giao thức DNS chạy trên nền UDP với số hiệu cổng là 53.

Thông thường DNS được các giao thức tầng ứng dụng khác như HTTP, SMTP và FTP sử dụng để xác định địa chỉ IP từ tên máy tính do người dùng đưa vào. Chuyện gì xảy ra khi trình duyệt (HTTP client) trên máy tính của người sử dụng yêu cầu đối tượng có địa chỉ URL là www.someschool.edu/index.html. Để gửi được thông điệp HTTP yêu cầu tới Web server thì máy tính của người sử dụng phải xác định được địa chỉ IP của www.someschool.edu. Điều này được thực hiện như sau: máy tính của người sử dụng chạy phía client của ứng dụng DNS. Trình duyệt sẽ lấy ra tên

máy tính (www.someschool.net) từ địa chỉ URL và chuyển nó cho phần mềm client của DNS. DNS client gửi một truy vấn (query) chứa tên máy tính tới DNS server. DNS client sẽ nhận được một thông điệp trả lời từ DNS server chứa địa chỉ IP cần xác định. Sau đó trình duyệt sẽ mở một kết nối TCP tới tiến trình HTTP server trên máy tính có địa chỉ IP vừa được xác định.

Rõ ràng các ứng dụng Internet sử dụng DNS hoạt động chậm đi. Tuy nhiên, địa chỉ IP đã được xác định thường được ghi tạm (cache) trong một name server DNS ở gần và như vậy làm giảm tải cho hệ thống DNS cũng như độ trễ của ứng dụng.

Bên cạnh dịch vụ xác định địa chỉ IP từ tên máy, DNS cung cấp một số dịch vụ quan trọng sau:

**Dịch vụ đặt bí danh cho máy tính (Host aliasing):**

Máy tính có tên phức tạp có thể có một hoặc nhiều bí danh (alias). Ví dụ tên máy tính relay1.west-coast.enterprise.com có thể có hai bí danh là www.enterprise.com và enterprise.com. Trong trường hợp này, relay1.west-coast.enterprise.com là tên đầy đủ (canonical name). Tên bí danh thường dễ nhớ hơn tên đầy đủ. Một ứng dụng có thể yêu cầu DNS xác định tên đầy đủ cũng như địa chỉ IP của một tên bí danh.

**Dịch vụ đặt bí danh cho mail server (Mail server aliasing):**

Hiển nhiên địa chỉ email cần dễ nhớ. Ví dụ nếu Bob có tài khoản trên Hotmail, địa chỉ của Bob có thể chỉ đơn giản là bob@hotmail.com. Tuy nhiên tên máy tính của máy phục vụ thư tại Hotmail phức tạp và vì thế khó nhớ hơn so với hotmail.com (Ví dụ tên đầy đủ có thể là relay1.west-coast.hotmail.com). Ứng dụng có thể sử dụng DNS để xác định tên đầy đủ của một bí danh cũng như địa chỉ IP của máy tính đó. Trên thực tế, DNS cho phép mail server và Webserver của các công ty có tên (bí danh) giống nhau, ví dụ: Webserver và mail server của một công ty có thể cùng là enterprise.com.

**Phân tán tải (load distribution):**

DNS thực hiện việc phân tán tải cho các server, đặc biệt là các Web server "nhân bản" (replicated) (là các server có nội dung giống hệt nhau).



Những site có nhiều người truy cập như cnn.com được đặt trên nhiều server giống hệt nhau. Mỗi server là một hệ thống đầu cuối (end system) khác nhau, có địa chỉ IP khác nhau. Đối với các server giống hệt nhau như vậy, một nhóm địa chỉ IP sẽ gắn với tên đầy đủ của một máy nào đó. Cơ sở dữ liệu DNS chứa toàn bộ nhóm địa chỉ IP đó. Khi client gửi truy vấn DNS để xác định địa chỉ IP thì server sẽ gửi toàn bộ nhóm địa chỉ IP đó nhưng server thay đổi thứ tự các địa chỉ IP trong nhóm. Thông thường client gửi thông điệp HTTP tới máy tính có địa chỉ IP được liệt kê đầu tiên trong nhóm. Sự hoán chuyển vị trí các địa chỉ IP mà DNS thực hiện đã phân tải cho các server. Việc hoán vị của DNS cũng được áp dụng cho email khi nhiều mail server có chung bí danh.

DNS được đặc tả trong RFC 1034, RFC 1035 và cập nhật trong một số RFC khác. DNS là hệ thống phức tạp và chúng ta chỉ nghiên cứu một vài khía cạnh của nó.

## Trong lịch sử

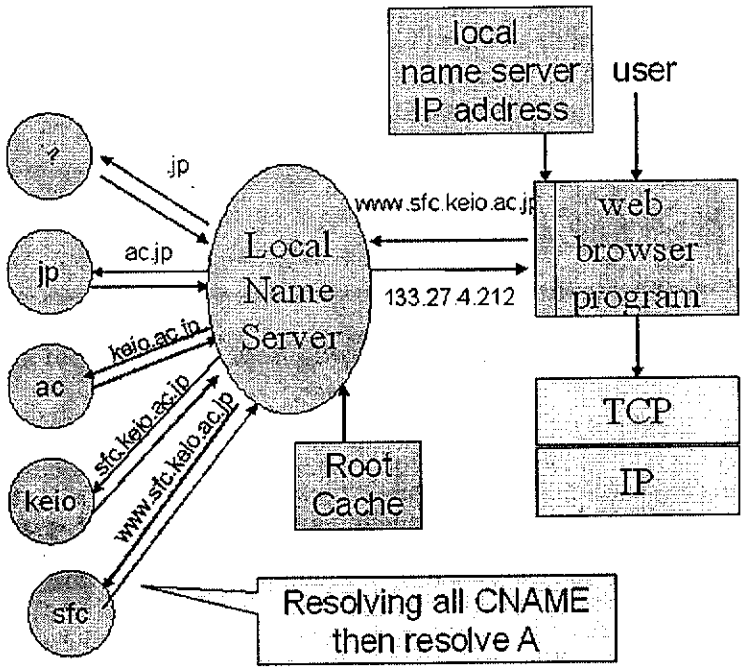
***DNS: Một dịch vụ mạng quan trọng hoạt động trên mô hình client/server.***

Giống HTTP, FTP hay SMTP, giao thức DNS nằm ở tầng ứng dụng vì (1) nó hoạt động giữa hai thực thể truyền thông đầu cuối sử dụng mô hình client/server và (2) sử dụng một giao thức giao vận end-to-end ở tầng giao vận phía dưới để trao đổi thông điệp DNS giữa hai phía đầu cuối. Tuy nhiên vai trò của DNS khác các ứng dụng Web, FTP hay Email nhiều. DNS không phải ứng dụng được người dùng trực tiếp sử dụng mà DNS chỉ cung cấp một dịch vụ Internet cực kỳ thiết yếu cho các ứng dụng: chuyển đổi tên máy tính sang địa chỉ IP. Trước đây trong mục 1.2 chúng ta thấy rằng sự phức tạp trong kiến trúc của Internet được đặt tại "lớp vỏ" của mạng. DNS được triển khai trên các máy tính đầu cuối là một minh chứng rõ ràng cho nguyên lý thiết kế này.

## 2.5.2 Cơ chế hoạt động của DNS

Bây giờ, chúng ta trình bày tổng quan cách thức hoạt động của DNS, tập trung vào dịch vụ xác định địa chỉ IP từ tên máy tính. Với client, DNS là

một "hộp đen". Client gửi thông điệp truy vấn DNS vào hộp đen đó, trong thông điệp chứa tên máy cần xác định địa chỉ IP. Với hệ điều hành Unix, gethostname() là một hàm mà ứng dụng có thể gọi để gửi thông điệp truy vấn. Sau một khoảng thời gian nào đó - từ vài phần nghìn giây đến vài chục giây, client nhận được thông điệp trả lời của DNS chứa địa chỉ IP cần xác định. Vì vậy, với client thì DNS là một dịch vụ xác định IP đơn giản và dễ hiểu. Nhưng "hộp đen" triển khai dịch vụ đó thực sự phức tạp, bao gồm nhiều máy chủ tên (nameserver) đặt khắp nơi trên thế giới và một giao thức ở tầng ứng dụng xác định cách thức trao đổi thông tin giữa các nameserver và giữa nameserver với máy tính.




**Hình 2.19 Ứng dụng sử dụng dịch vụ của DNS**

Để triển khai DNS, người ta có thể đưa ra một kiến trúc đơn giản sau: có một name server chứa tất cả các ánh xạ tên và địa chỉ IP. Theo thiết kế tập trung này, client chỉ cần gửi tất cả các truy vấn tới nameserver duy nhất và nameserver này sẽ trực tiếp trả lời mọi truy vấn. Mặc dù tính đơn giản của thiết kế này rất hấp dẫn nhưng nó hoàn toàn không thích hợp cho



Internet với số lượng lớn và ngày càng nhiều máy tính. Thiết kế tập trung như vậy nảy sinh một số vấn đề sau:

**Điểm hỏng duy nhất (A single point of failure)** nếu nameserver duy nhất ngừng làm việc cũng có nghĩa là toàn bộ Internet ngừng hoạt động.

**Khối lượng công việc (Traffic volume)**: Một nameserver duy nhất phải xử lý tất cả các truy vấn DNS (cho tất cả các thông điệp yêu cầu từ hàng triệu máy tính trên toàn cầu).

**Cơ sở dữ liệu tập trung ở xa (distant centralized database)**: Nameserver duy nhất không thể gần tất cả các client. Nếu nameserver đặt ở NewYork thì tất cả truy vấn từ Úc phải chuyển tới phía bên kia trái đất và có thể qua một đường kết nối chậm và tắc nghẽn. Hậu quả là các ứng dụng phải chịu độ trễ lớn.

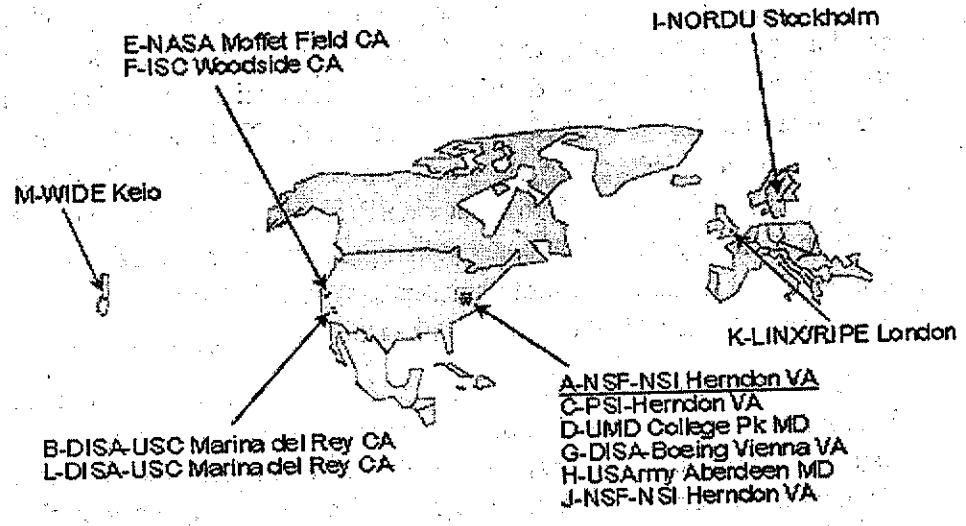
**Bảo trì (maintenance):** Namserver phải ghi nhớ thông tin về tất cả các máy tính trên Internet. Khi đó cơ sở dữ liệu sẽ cực kỳ lớn và nameserver phải cập nhật thường xuyên thông tin cho mọi máy tính mới cũng như phải giải quyết các vấn đề kiểm chứng và xác nhận khi người dùng sử dụng cơ sở dữ liệu tập trung.

Tóm lại, cơ sở dữ liệu tập trung trên một nameserver duy nhất không phù hợp khi quy mô hệ thống lớn. Do đó, DNS được thiết kế phân tán. Trên thực tế DNS là một ví dụ tuyệt vời về triển khai cơ sở dữ liệu phân tán trên Internet. Để giải quyết vấn đề quy mô, DNS sử dụng nhiều nameserver tổ chức phân cấp và phân tán trên toàn cầu. Không có nameserver nào chứa tất cả tên và địa chỉ IP các máy tính trên Internet, những thông tin này được phân tán trên nhiều nameserver. Có ba loại nameserver: local nameserver, root nameserver và authoritative nameserver. Các nameserver đó trao đổi thông tin với nhau và với các máy tính khác.

**Local nameserver**: Mỗi ISP như trường đại học, công ty đều có local nameserver (còn được gọi là default name server). Khi máy tính trong cơ quan tạo ra một thông điệp truy vấn DNS thì đầu tiên thông điệp đó được gửi tới local name server của tổ chức. Địa chỉ IP của local name server phải được cấu hình trong máy tính (Trong Win 95/98, bạn có thể tìm thấy địa chỉ IP của local name server bằng cách mở Control Panel, sau đó chọn Network,

chọn TCP/IP, rồi chọn cấu hình DNS). Local name server thường "gần" với client, trong trường hợp tại cơ quan của một tổ chức, nó có thể ở trên cùng mạng LAN với máy tính client. Với ISP phục vụ kết nối từ nhà thì khoảng cách giữa name server và các máy tính client chỉ là vài router. Nếu máy tính yêu cầu xác định địa chỉ IP của một máy tính khác trong cùng một ISP thì local name server có thể ngay lập tức xác định được địa chỉ IP cần thiết. Ví dụ nếu máy tính surf.eurecom.fr yêu cầu địa chỉ IP của baie.eurecom.fr thì local name server ở eurecom ngay lập tức có thể đưa ra địa chỉ IP mà không phải liên hệ với bất kỳ name server nào khác.

**Rootname server**: Trên Internet có 13 rootname server, hầu hết đặt tại Bắc Mỹ. Vị trí các root name server vào thời điểm tháng 02/1998 được minh hoạ trên Hình 2.18. Khi local name server không thể trả lời truy vấn của một máy tính (bởi vì nó không có thông tin của máy tính được yêu cầu) thì local name server sẽ đóng vai trò client DNS và gửi câu hỏi truy vấn tới một trong số các root name server. Nếu root name server có thông tin của máy tính được hỏi, nó sẽ gửi một thông điệp DNS hồi âm tới local name server và sau đó thông tin này được local name server gửi trả lời cho máy tính yêu cầu. Nhưng root name server có thể không có thông tin của máy tính đó. Trong trường hợp này, root name server biết được địa chỉ IP của name server quản lý máy tính đó.

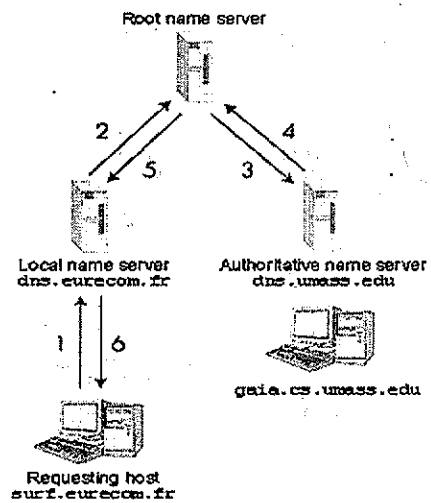



**Hình 2.20 Các root name server trên thế giới**



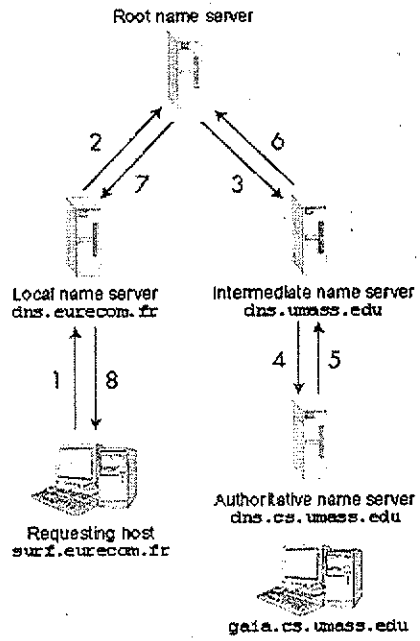
**Authoriative name server**: Mỗi máy tính phải đăng ký tới một Authoritative name server. Thông thường authoriative name server của một máy tính là name server trong miền ISP của máy tính đó (thực tế mỗi máy tính phải có ít nhất hai authoritative name server, để đề phòng trường hợp một name server bị hỏng). Có thể định nghĩa, Authoriative name server của một máy tính là nameserver luôn lưu trữ bản ghi DNS cho phép xác định địa chỉ IP của máy tính đó từ tên. Khi authoritative name server nhận được truy vấn từ root nameserver, nó sẽ gửi một thông điệp DNS trả lời chứa ánh xạ được yêu cầu. Sau đó, root server gửi ánh xạ đó tới local nameserver và local nameserver lại tiếp tục gửi ánh xạ đó tới máy tính yêu cầu. Nhiều nameserver vừa là local vừa là authoriative nameserver.

Xét ví dụ đơn giản sau. Giả sử máy tính surf.eurecom.fr muốn có địa chỉ IP của máy tính gaia.cs.umas.edu, giả sử nameserver của miền Eurecom là dns.eurecom.com.fr và authoriative nameserver cho gaia.cs.umas.edu là dns.umass.edu. Như đã trình bày trong Hình 2.20, đầu tiên máy tính surf.eurecom.fr gửi một thông điệp truy vấn tới local name server của nó là dns.eurecom.fr. Thông điệp đó chứa tên máy tính cần xác định địa chỉ IP, là gaia.cs.umass.edu. Local name server gửi thông điệp tới root name server. Root nameserver gửi tiếp thông điệp tới nameserver có thể xác định tất cả các máy tính trong miền umass.edu, ví dụ là dns.umass.edu. Sau đó, authoriative name server này gửi kết quả cho surf.eurecom.fr thông qua root name server và local name server. Trong ví dụ này, để xác định được địa chỉ có 6 thông điệp DNS được trao đổi: 3 thông điệp yêu cầu và 3 thông điệp trả lời.




**Hình 2.21 Các truy vấn DNS**

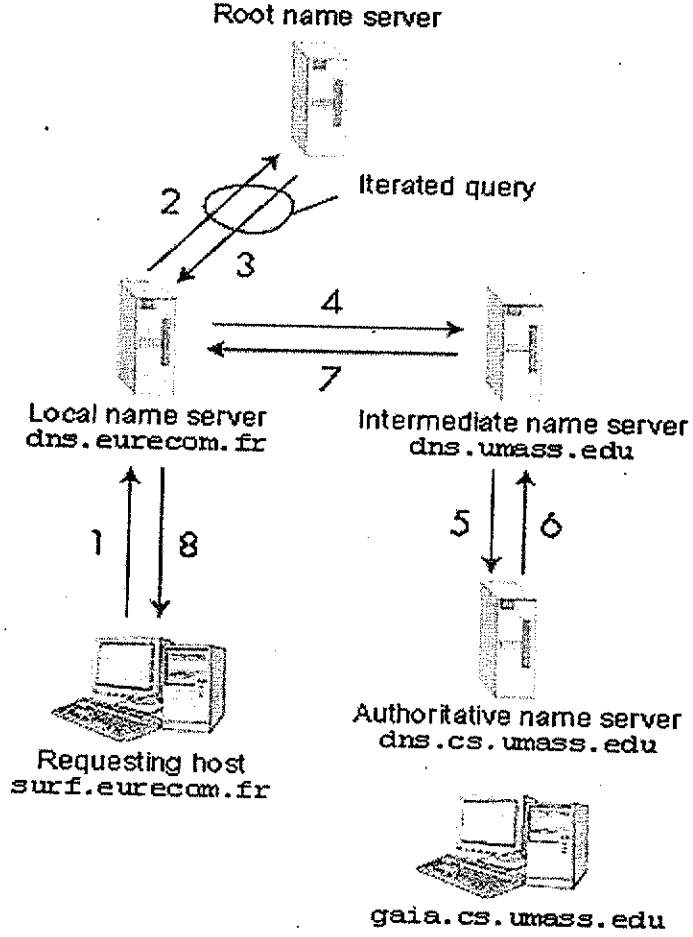
Giả thiết root name server biết địa chỉ IP của authoriative name server của mọi máy tính như trên có thể không đúng. Với tên một máy tính, root nameserver có thể chỉ biết được địa chỉ IP của một name server trung gian mà chính name server trung gian này mới biết được địa chỉ IP của authoriative nameserver của máy tính đó. Để minh họa điều này vẫn xét ví dụ máy tính surf.eurecom.fr cần xác định địa chỉ IP của gaia.cs.umass.edu. Giả sử trường Đại học Massachusets (Univ of Massachusets) có name server cho toàn bộ trường đại học, đó là dns.umass.edu. Ta cũng giả sử tiếp rằng mỗi khoa trong trường đại học này có name server riêng, quản lý tên cho tất cả các máy tính trong khoa đó. Khi root name server nhận được yêu cầu xác định địa chỉ IP cho một tên máy tính có tận cùng là umass.edu, nó sẽ gửi yêu cầu tới name server dns.umass.edu. Name server này gửi tất cả các yêu cầu có tên máy tính tận cùng là cs.umass.edu cho authoritative name server quản lý tất cả máy tính có tên tận cùng là cs.umass.edu. Authoriative name server này (dns.cs.umass.edu) gửi kết quả tới name server trung gian (dns.umass.edu) và name server này sẽ gửi tiếp kết quả tới root name server. Root name server sẽ gửi tiếp kết quả tới local name server của máy tính yêu cầu. Trong ví dụ này, 8 thông điệp DNS được gửi (Hình 2.21). Thực ra có thể có nhiều hơn 8 thông điệp DNS được trao đổi vì có thể có nhiều name server trung gian ở giữa root name server và authoriative name server.




Hình 2. 22 Các truy vấn DNS



Trong ví dụ trên, tất cả các truy vấn được gọi là đệ quy (recursive query). Khi máy tính hay name server A gửi thông điệp yêu cầu tới name server B, name server B sẽ thay mặt A nhận thông điệp chứa kết quả và sau đó gửi kết quả tới A. Tuy nhiên DNS cho phép các truy vấn tương tác (iterative query) ở bất kì giai đoạn nào trong quá trình từ máy tính yêu cầu đến authoriative name server. Khi name sever A gửi một truy vấn tương tác tới name server B, nếu name server B không có ánh xạ được yêu cầu, nó sẽ gửi cho A thông điệp trả lời chứa địa chỉ IP của name server kế tiếp trên chuỗi, giả sử là name sever C. Sau đó name server A trực tiếp gửi thông điệp yêu cầu tới name server C.




Hình 2. 23 Các truy vấn đệ quy và tương tác

Các truy vấn trong dãy truy vấn liên tiếp có thể là tương tác hoặc đệ quy như minh hoạ trên Hình 2. 23. Thông thường tất cả các truy vấn - ngoại trừ truy vấn từ local name server tới root name server là đệ quy, truy vấn tới root name server thường là tương tác (bởi vì root name server phải xử lý một lượng lớn các yêu cầu nên cần làm giảm số lượng truy vấn tới root name server).

Một đặc tính quan trọng của DNS là lưu trữ tạm thời các bản ghi DNS (**DNS caching**). Trên thực tế, DNS lưu trữ tạm thời (cache) để làm giảm độ trễ cũng như làm giảm số thông điệp DNS trao đổi trên mạng. Ý tưởng này rất đơn giản: Khi nhận được ánh xạ DNS của máy tính nào đó, bên cạnh việc gửi tiếp thông điệp, name server sẽ lưu ánh xạ này vào bộ nhớ cục bộ (ổ đĩa cứng hay RAM). Với ánh xạ tên máy - địa chỉ IP được lưu trữ sẵn, nếu có một truy vấn khác yêu cầu địa chỉ IP của cùng tên máy mà name server vừa lưu trữ, nameserver sẽ xác định ngay được địa chỉ IP mong muốn, kể cả khi nó không là authoritiative name server cho máy tính đó. Để khắc phục tình trạng lưu trữ thông tin cũ, thông tin được lưu trữ tạm thời sẽ bị xoá bỏ sau một khoảng thời gian (thường là hai ngày).

## 2.5.3 Bản ghi DNS

Name server lưu giữ các bản ghi tài nguyên (resource record) cho các ánh xạ Tên máy / Địa chỉ IP. Mỗi thông điệp trả lời DNS chứa một hay nhiều bản ghi tài nguyên. Trong phần này chúng ta sẽ nói qua về bản ghi tài nguyên và thông điệp DNS. Về chi tiết, bạn có thể xem trong DNS RFC [RFC 1034, RFC 1035].

Bản ghi tài nguyên gồm 4 trường sau::

(Name, Value, Type, TTL)

TTL là thời gian tồn tại của bản ghi tài nguyên, dùng để xác định thời điểm có thể xoá bản ghi tài nguyên khỏi bộ nhớ lưu trữ. Trong các bản ghi ví dụ dưới đây, chúng ta bỏ qua trường TTL. Ý nghĩa của trường Name và Value phụ thuộc vào trường Type:



Nếu Type = A thì Name là tên máy và Value là địa chỉ IP của máy đó. Bản ghi kiểu A là ánh xạ Tên máy - Địa chỉ IP chuẩn. Ví dụ, (relay1.bar.foo.com, 145.37.93.126, A) là một bản ghi Type A.

Nếu Type = NS thì Name là một miền (như là foo.com) và Value là tên máy của authoriative name server của các máy tính trong miền đó. Bản ghi này thường được sử dụng để gửi tiếp các truy vấn DNS. Ví dụ 1 bản ghi Type NS: (foo.com, dns.foo.com, NS)

Nếu Type = CNAME thì Value là tên đầy đủ của máy có tên bí danh nằm trong Name. Bản ghi kiểu này cho phép xác định tên đầy đủ của một máy tính từ tên bí danh. Ví dụ một bản ghi CNAME: (foo.com, relay1.bar.foo.com, CNAME).

Nếu Type = MX thì Value là tên máy của mail server có tên bí danh nằm trong Name. Ví dụ, bản ghi kiểu MX (foo.com, mail.bar.foo.com, MX). Bản ghi MN cho phép mail server có tên bí danh đơn giản.

Nếu một name server là authoritiative name server cho một máy tính nào đó thì name server sẽ chứa bản ghi kiểu A của máy tính đó (ngay cả nếu name server đó không là authoritiative name server thì có thể nó chứa bản ghi kiểu A trong bộ nhớ cache của nó). Nếu name server không là authoritiative name server của máy tính được hỏi thì nó sẽ chứa một bản ghi kiểu NS cho miền của máy tính này, và nó cũng có một bản ghi kiểu A xác định địa chỉ IP của name server của miền này đặt trong trường Value của bản ghi NS. Ví dụ, root name server không là authoritiative name server cho máy tính gaia.cs.umass.edu, root server sẽ có một bản ghi cho miền chứa umass.edu ví dụ (umass.edu, dns.umass.edu, NS). Root server đó đồng thời cũng có một bản ghi kiểu A cho phép xác định địa chỉ IP của name server dns.umass.edu, chẳng hạn (dns.umass.edu, 128.119.40.111, A).

## 2.5.4 Thông điệp DNS

Có hai loại thông điệp DNS: thông điệp yêu cầu và thông điệp trả lời. Cả hai kiểu thông điệp này có chung khuôn dạng minh hoạ trên Hình 2.22.

Ý nghĩa các trường trong thông điệp như sau:

12 byte đầu tiên là phần tiêu đề. Phần tiêu đề có một số trường. Trường đầu tiên là một định danh 16 bit cho mỗi thông điệp yêu cầu. 16 bit định danh này được ghi lại vào thông điệp trả lời, cho phép client xác định được đấy là câu trả lời cho thông điệp yêu cầu nào. Có nhiều cờ trong trường cờ (mỗi cờ ứng với một bit). **Cờ truy vấn (query/reply flag)** xác định thông điệp là yêu cầu (0) hay là trả lời (1). **Cờ authoritiative** được đặt trong thông điệp trả lời khi name server là authoriative name server của tên máy tính cần xác định địa chỉ IP. **Cờ mong muốn đệ quy (recursive-desired query)** được đặt khi client (máy tính hay name server) mong muốn name server thực hiện truy vấn đệ quy khi nó không có bản ghi đó. **Cờ chấp nhận đệ quy (recursion-available flag)** được đặt trong thông điệp trả lời nếu name server đó hỗ trợ đệ quy. Trong phần tiêu đề cũng có 4 trường số lượng, các trường này xác định số lượng các bản ghi trong 4 phần dữ liệu sau phần tiêu đề.

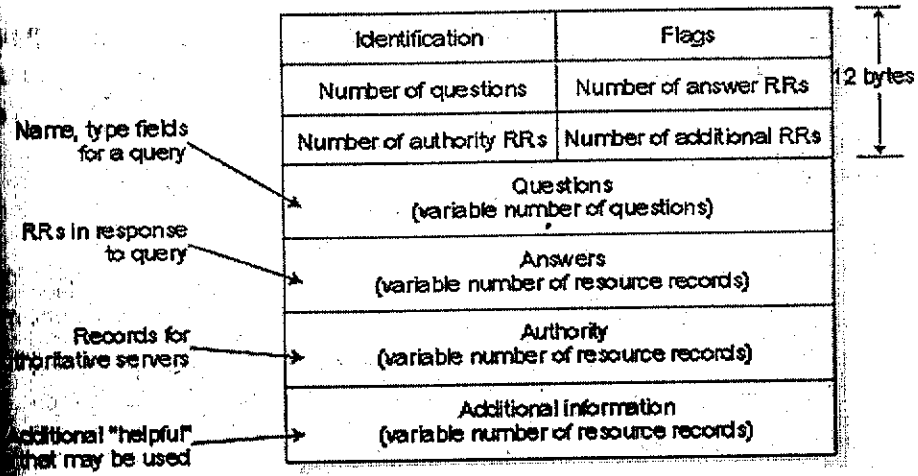
Phần câu hỏi (Question session) chứa thông tin về các câu hỏi được tạo ra. Nó bao gồm (1) trường tên chứa tên đang được hỏi và (2) trường kiểu xác định kiểu câu hỏi cho tên máy tính đó (Kiểu A cho tên máy tính, kiểu MX cho mail server).

Trong thông điệp trả lời từ server name, phần trả lời (answer section) chứa các bản ghi tài nguyên cho tên được yêu cầu trước đó. Chú ý rằng mỗi bản ghi tài nguyên có 4 trường: Type (A, NS, CNAME, MX), Name, Value, TTL. Thông điệp trả lời có thể có nhiều bản ghi tài nguyên vì tên máy tính có thể ứng với nhiều địa chỉ IP.

Mục thẩm quyền (authority section) chứa các bản ghi của các authoritative server.

Mục phụ trợ (additional section) chứa các bản ghi "hữu ích" khác. Ví dụ trường trả lời trong thông điệp trả lời một truy vấn MX sẽ chứa tên đầy đủ của mail server có tên bí danh đặt ở trong Name. Phần phụ trợ có thể chứa một bản ghi kiểu A cung cấp địa chỉ IP cho chính mail server đó.






**Hình 2. 24 Khuôn dạng thông điệp DNS**

Các phần trên mô tả cách thức lấy dữ liệu trong cơ sở dữ liệu DNS. làm thế nào để đưa được dữ liệu vào cơ sở dữ liệu? Cho tới gần đây, dung của server DNS được cấu hình tĩnh, ví dụ, thông qua file cấu hình người quản trị hệ thống tạo ra. Gần đây, lựa chọn UPDATE được đưa giao thức DNS cho phép dữ liệu được tự động thêm vào hay xoá bỏ cơ sở dữ liệu thông qua thông điệp DNS. RFC 2136 đặc tả quá trình nhật động của DNS.

## CÁC ỨNG DỤNG THEO KIẾN TRÚC NGANG HÀNG

Tháng 5/1999, Shawn Fanning và Sean Parker sáng lập ra công ty ster Inc và đã mở ra một cuộc Cách mạng trong ngành công nghệ thông Tại thời điểm đó, Napster là dịch vụ chia sẻ file ngang hàng duy nhất mạng Internet.

Chính nhu cầu chia sẻ các loại phần mềm không bản quyền thúc đẩy ra đời các cộng đồng ảo có tổ chức nhưng lại kết nối lỏng lẻo trên rnet. Napster không chỉ đáp ứng nhu cầu tìm kiếm và chia sẻ các file âm c mà còn hình thành nên một cộng đồng ảo trên đó. Tham gia vào cộng

đồng này, một người có thể dễ dàng nén các đĩa CD âm nhạc ra file MP3 để chia sẻ với những người khác.

## Trong lịch sử

Năm 1999, Shawn Fanning công bố chương trình đầu tiên (thực hiện sau vài tháng) đáp ứng được nhu cầu một nhóm nhỏ bạn bè. Nói chung mỗi người đều có nhiều các file nhạc (MP3) trong ổ cứng trên máy tính cá nhân, máy tính cá nhân đều có kết nối Internet. Vấn đề ở đây là làm thế nào tìm được file mà người sử dụng (NSD) muốn kiếm theo một tiêu chí nào đó (Tên bài hát / Ca sỹ / Nhạc sỹ/ Album...). Chương trình mà Fanning viết có thể kiểm soát được những thông tin như vậy.

Ở server trung tâm, Chương trình của Fanning kiểm soát những file mà hệ thống có thể cung cấp và vị trí chính xác của file (tức là địa chỉ máy tính chứa file). Khi người dùng kết nối vào hệ thống (bằng phần mềm của Fanning), danh sách tất cả các file mà người dùng muốn chia sẻ sẽ được cập nhật lên server trung tâm (chú ý là chỉ danh sách các file, còn các file thực sự vẫn nằm trên máy tính đầu cuối – gọi là nút). Khi NSD muốn tìm kiếm file nào đó, từ hệ thống CSDL của mình, server trung tâm sẽ trả về cho NSD danh sách các máy tính có chứa file cần tìm. NSD chỉ việc liên lạc trực tiếp đến máy tính có file để xin tải về.

Mạng Napster – với khả năng hỗ trợ tìm kiếm và tải file MP3 với khối lượng lớn – đã phát triển với tốc độ cực kỳ nhanh, hình thành một cộng đồng 30 triệu NSD chia sẻ 2,8 tỷ file trước khi chấm dứt hoạt động theo phán quyết của Tòa án Hoa Kỳ.

Khởi đầu từ năm 2003, RIAA (Hiệp hội âm nhạc Hoa Kỳ) đã có chiến lược mới để kiểm soát mạng P2P. Sau khi RIAA thua tại Tòa Thượng thẩm Liên bang khi ISP Verizon không cung cấp thông tin về khách hàng thuê bao, RIAA bắt đầu thu thập thông tin về hành vi của người sử dụng (chứ không phải ISP hay nhà cung cấp phần mềm P2P). Tháng 9/2003, RIAA đã đưa ra tòa 261 người chia sẻ các file nhạc bất hợp pháp, ngày nay số lượng vụ kiện kiểu này hàng năm là 13000.

Giờ đây, sau nhiều cố gắng của Hiệp hội công nghiệp thu âm Hoa Kỳ (RIAA), Quốc hội Hoa Kỳ đã đưa ra những điều khoản quy định việc chia sẻ, hạn chế việc tự do chia sẻ các phần mềm hợp pháp trên các mạng ngang hàng.

Người ta thường xem Kỷ nguyên Mạng ngang hàng bắt đầu với Napster, tuy nhiên ta thấy những phần mềm nhắn tin (Yahoo Messenger) đã



manh nha ý tưởng này. Nhắn tin là một hình thức lai tạp – vừa tận dụng tính tức thời của hệ thống điện thoại lại vừa có tính kiểm soát của hệ thống thư tín điện tử.

Nói chung, ứng dụng P2P có các đặc điểm sau:

- **Chia sẻ các tài nguyên và dịch vụ phân tán**. Trong mạng P2P, các nút thành viên vừa đóng vai trò client, vừa đóng vai trò server; nghĩa là vừa là nhà cung cấp nhưng cũng là người tiêu thụ các tài nguyên (Tài nguyên ở đây có thể là thông tin, file, năng lực tính toán...).

- **Không tập trung**. Không có điểm tập trung nào đóng vai trò điều phối chung của toàn bộ hệ thống. Truyền thông giữa các nút diễn ra trực tiếp, không có nút nào kiểm soát được tất cả các nút khác. Ở đây có sự phân biệt giữa mạng P2P thuần túy (các nút hoàn toàn bình đẳng với nhau) và mạng P2P lai tạp (các nút không còn bình đẳng hoàn toàn, có một nhóm nút sẽ đóng vai trò kiểm chứng và tìm kiếm theo chỉ mục). Kiểu lai tạp kết hợp giữa mạng P2P thuần túy và mô hình client/server truyền thống.

- **Tự trị**. Mỗi nút trong mạng P2P tự quyết định khi nào tham gia mạng và mức độ đóng góp chia sẻ cho cộng đồng.

Các ứng dụng P2P có thể phân loại vào 3 nhóm sau đây:

- Nhắn tin tức thì (Instant messaging)

- Chia sẻ file

- Tính toán mạng lưới

Việc phân chia nhóm như vậy cũng chưa rõ ràng và ranh giới giữa các nhóm còn mập mờ, và biến đổi rất nhanh chóng.

### 2.6.1 Nhắn tin tức thì

Ngày nay Nhắn tin tức thì (IM - Instant Messaging) được sử dụng cực kỳ rộng rãi do có khả năng truyền thông điệp tức thời (giống điện thoại) một cách có kiểm soát (giống email) và khả năng duy trì đồng thời nhiều cuộc hội thoại. Các dịch vụ IM như I-seek-you (ICQ), MSN Messenger của

Microsoft, AOL Instant Messenger® (AIM), Yahoo Messenger (YIM) trở nên cực kỳ thông dụng (đặc biệt với giới trẻ) khi các dịch vụ này tích hợp thêm nhiều tính năng như truyền file, chia sẻ dữ liệu, tương tác đa phương tiện...

## Chức năng của IM

Cho đến năm 2000, không có một giao thức chuẩn nào quy định cách thức hoạt động của các hệ thống IM. RFC2778 "A model for Presence and Instant Messaging" và RFC2779 "Instant Messaging/Presence Protocol" đưa ra tập hợp các hướng dẫn hình thành nên cấu hình cơ bản cho một hệ thống IM. Các phần mô tả sau đây chủ yếu dựa trên các khuyến nghị RFC2778 và RFC2779.

**Dịch vụ Hiển thị Thông tin (Presence Service)** là dịch vụ quan trọng nhất trong hệ thống IM, xác định có thể liên lạc được với một đối tượng hay không và trạng thái của đối tượng đó. Ngoài ra, dịch vụ này còn cung cấp các cơ chế đảm bảo tính riêng tư, chẳng hạn lựa chọn một nhóm đối tượng được phép nhìn thấy trạng thái của mình và được quyền gửi thông điệp tới.

**Dịch vụ chuyển phát tin nhắn.** Là các tiện ích cho phép chuyển phát các tin nhắn (có thể dưới dạng văn bản hay âm thanh) giữa những người sử dụng trên mạng IM.

**Các dịch vụ bổ trợ**. Bên cạnh các dịch vụ cơ sở trên, các hệ thống IM bổ sung rất nhiều tính năng mới để thu hút khách hàng. Các dịch vụ bổ trợ được liệt kê trong RFC2778 và RFC2779.

## Các thành phần của IM

**IM Server**. Cung cấp các dịch vụ IM như hiển thị thông tin, cảnh báo, đăng ký tài khoản, và nhắn tin. Người sử dụng (qua phần mềm Client) phải kết nối với Server để có trạng thái trực tuyến (online) trong mạng IM. Mạng IM có thể gồm nhiều server cùng làm việc với nhau để cung cấp khả năng mở rộng trong trường hợp có nhiều client cùng kết nối.



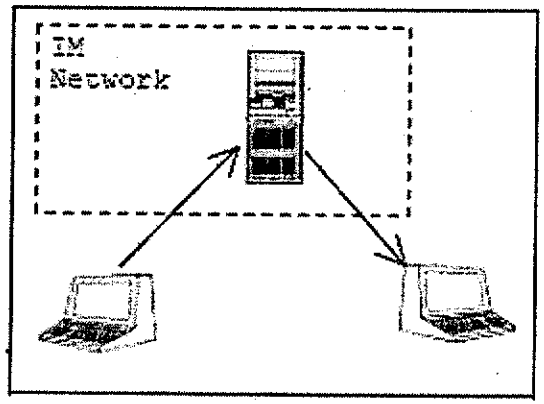
Truyền thông giữa các server thường "trong suốt", vì người sử dụng nói chung không biết được mình kết nối đến những server nào. Server của các mạng IM lớn thường được đặt tại các công ty sở hữu mạng IM.

**IM Client**. Phần mềm client là "điểm giao tiếp" của người sử dụng với mạng IM. Sau khi cài đặt trên máy tính, NSD có thể sử dụng IM client để kết nối và sử dụng các dịch vụ do IM server cung cấp. Client cũng được sử dụng để lưu trữ các thông tin cục bộ của người sử dụng (chẳng hạn mật khẩu, tên truy cập phục vụ mục đích tự động truy cập hay nhật ký hội thoại).

## Mô hình kết nối

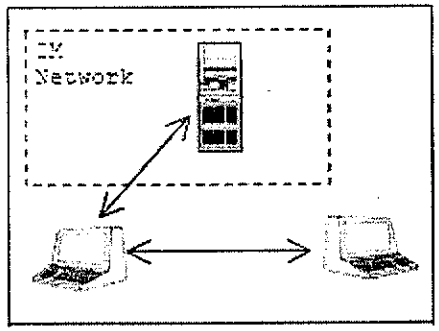
Có hai mô hình cơ sở được áp dụng trên các mạng IM

**Client-Server hay kiểu tập trung.** Tất cả thông tin trao đổi trên mạng đều phải đi qua server, có nghĩa là hai client không kết nối trực tiếp được với nhau mà kết nối gián tiếp qua server (Xem Hình 2.25)




Hình 2.25 Mô hình kết nối IM kiểu tập trung

**Peer-to-Peer hay kiểu phân tán.** Dữ liệu được trao đổi trực tiếp giữa các client (không đi qua server). Kiểu kết nối này thường được sử dụng khi truyền file (để làm giảm tải cho server). Server trong mạng kiểu này chỉ làm nhiệm vụ kiểm soát trạng thái các client và giúp các client trao đổi trực tiếp với nhau. Kiểu kết nối này được minh họa trên Hình 2.26.




Hình 2.26 Mô hình IM kiểu phân tán

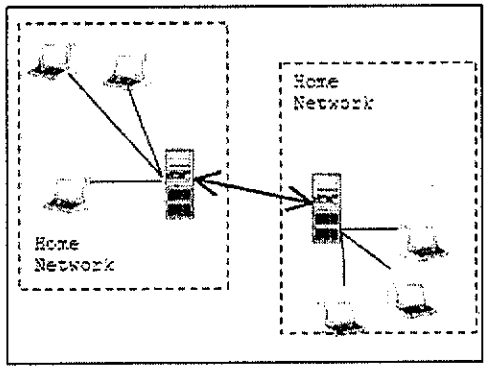
## Cấu hình Server

Để tăng khả năng mở rộng, hệ thống IM có thể sử dụng một hay nhiều Server.

**Kiến trúc một Server.** Mọi dịch vụ IM đều thực hiện trên một server duy nhất (tạo tài khoản, kiểm chứng người sử dụng và các dịch vụ khác). Kiến trúc này dễ bảo trì server và tăng cường khả năng bảo mật, nhưng khó mở rộng hệ thống.

**Kiến trúc nhiều Server.** Phần lớn các mạng IM lớn đều sử dụng nhiều server. Các server thường được chia thành hai loại: Nhân bản và Dịch vụ phân tán.

Trong kiểu thứ nhất, mỗi server có thể thực hiện được tất cả các dịch vụ IM. Các server giống hệt nhau (nên được gọi là nhân bản) và được kết nối với nhau. Các client "đăng ký" đến một server "nhà" và "nói chuyện" với client thuộc server "nhà" khác. Kiến trúc Jabber theo kiểu này.




Hình 2. 27 Kiến trúc nhiều Server nhân bản



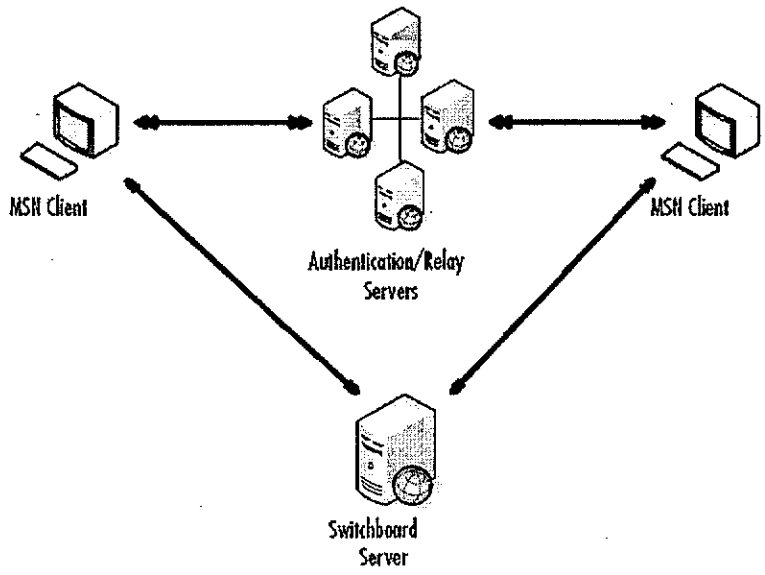
Trong kiểu thứ hai, các dịch vụ khác nhau được cài đặt trên các server khác nhau. Một server có thể cung cấp dịch vụ đăng ký tài khoản và đăng nhập hệ thống, trong khi chức năng truyền tin nhắn và thông báo được cài đặt trên các server khác.

Kiến trúc MSNP cung cấp nhiều server kiểm chứng đặt tại miền messenger.hotmail.com. Sau khi đăng nhập vào miền này, client được chuyển hướng tới một trong các server kiểm chứng. Sau khi kiểm chứng thành công, client có thể được chuyển kết nối sang một trong các server thực hiện nhiệm vụ cảnh báo. Client sẽ kết nối với server nào phụ thuộc vào vị trí địa lý của server hay tải của server.

## 2.6.6. Kiến trúc Hệ thống MSN

Hai hệ thống IM được sử dụng rộng rãi nhất hiện nay là AIM và MSN trong khi ICQ đứng thứ 5 trong danh sách. AIM và ICQ được quản lý bởi AOL Time Warner và sử dụng giao thức OSCAR (Open System for Communications in Real-time) trong khi MSN được Microsoft quản lý và sử dụng giao thức MSNP (MSN Protocol).

### MSN Protocol (MSNP)




Hình 2. 28 Kiến trúc MSN

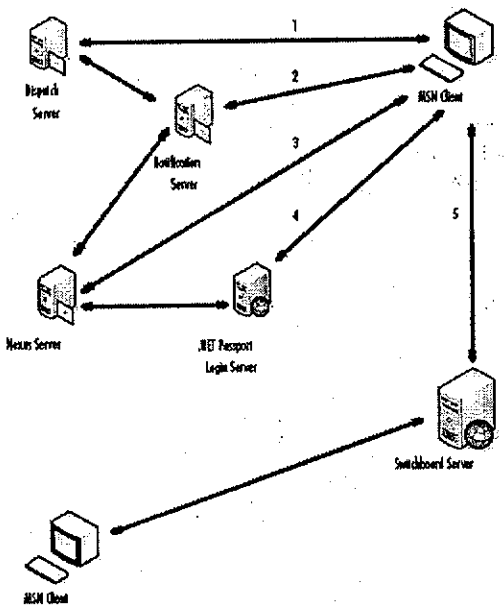
Server và Client trong mạng MSN trao đổi các lệnh được mã hóa theo chuẩn UTF-8 qua TCP socket.

Ở đây có ba kiểu server: Dispatch Server (DS), Notification Server (NS) và Switchboard Server (SS).

Nhiệm vụ chính của DS là thỏa thuận sử dụng phiên bản giao thức nào với client, sau đó sẽ xác định server NS nào kiểm soát người sử dụng. Sau khi xác định, địa chỉ NS được chuyển cho client.

NS là thành phần quan trọng nhất trong mạng IM. Sau khi kiểm chứng để đăng nhập thành công, Client và NS phải đồng bộ với nhau về trạng thái cũng như trao đổi các thông tin dị bộ. Một số sự kiện trao đổi giữa client và NS là khi thay đổi trạng thái (trực tuyến, ngoại tuyến hoặc rảnh rỗi), yêu cầu làm việc với SS (trình bày trong phần sau). Ngoài ra một vài thông báo khác cũng có thể trao đổi giữa NS và client (chẳng hạn thông báo có thư mới).

SS là thành phần trợ giúp client tạo các phiên hội thoại, chuyển tin nhắn giữa các client. Mỗi một cuộc hội thoại sẽ mở một kết nối từ client tới SS. Khi Client 1 muốn nói chuyện với Client 2, Client 1 sẽ gửi yêu cầu tới NS, NS sẽ gán cho Client 1 một SS nào đó (SS 1), đồng thời gửi thông báo tới NS của Client 2, NS này sẽ yêu cầu Client 2 kết nối tới SS 1 để nhận tin nhắn từ Client 1.




**Hình 2.29 Minh họa các bước của MSNP**



Sau đây chúng ta thử phân tích một số hoạt động của giao thức MSNP.

Trong quá trình hoạt động, người sử dụng MSN thực hiện 2 bước sau: Đăng nhập vào hệ thống (lấy danh sách bạn bè và trạng thái của từng bạn bè) và sau đó Gửi và Nhận tin nhắn.

Đầu tiên client (MSN) mở một kết nối TCP tới địa chỉ 64.4.13.58 ở port 1863. Sau khi thiết lập kết nối, client và server sẽ thỏa thuận với nhau sử dụng phiên bản nào của giao thức. MSN client gửi thông điệp sau chứa danh sách các giao thức client có thể sử dụng được:

**VER 0 MSNP7 MSNP6 MSNP5 MSNP4 CVRO**

Trong giao thức MSNP, trường "trial id" được khởi tạo là 0 và được gửi đi trong tất cả các thông điệp, cứ sau mỗi thông điệp, giá trị "trial id" được tự động tăng lên 1. Server trả lời kiểu như sau:

VER 0 MSNP7 MSNP6 MSNP5 MSNP4

Khi đó Client và Server thỏa thuận được giao thức sẽ sử dụng. Kế tiếp client hỏi server phương pháp mã hóa khi kiểm chứng.

INF 1

Khác Yahoo, MSN không gửi mật khẩu dưới dạng nguyên không mã hóa. MSN sẽ mã hóa mật khẩu để mật khẩu không bị lộ trên đường truyền. Server trả lời bằng thông điệp sau:

INF 1 MD5

Ở đây MD5 là phương pháp bảo mật mà server hỗ trợ. Kế tiếp client gửi username cho server

USR 2 MD5 I venky_dude@hotmail.com

Server sẽ kiểm tra xem có thông tin gì về người dùng này hay không. Nếu có Server sẽ gửi thông điệp kiểu sau cho client:

XFR 2 NS 64.4.13.55:1863 0

Ở đây server báo cho client biết phải liên lạc với Notification Server (NS) có địa chỉ 64.4.13.55 và cổng 1863. Sau đó Client và server đóng kết nối này, client sẽ mở kết nối với NS mới nhận được (64.4.13.55).

(client) VER 3 MSNP7 MSNP6 MSNP5 MSNP4 CVRO
(server) VER 3 MSNP7 MSNP6 MSNP5 MSNP4
(client) INF 4
(server) INF 4 MD5
(client) USR 5 MD5 I venky_dude@hotmail.com

Sau đó NS server biết được các thông tin về người dùng định đăng nhập. Server sẽ trả lời như sau:

USR 5 MD5 S 989048851.1851137130

Chuỗi "989048851.1851137130" là giá trị Hash theo kiểu MD5. Nó là một hàm băm do server tạo ra và được sử dụng cho mục đích kiểm chứng. Client sẽ gửi server mật khẩu đã được mã hóa theo MD5. Client sẽ gửi hàm băm được tính tạo thành từ chuỗi trên kết hợp với mật khẩu của mình cho server, chẳng hạn: **3b7926d277068ec49576a0c40598ff21**.

**USR 6 MD5 S 3b7926d277068ec49576a0c40598ff21**

Nếu mật khẩu này đúng, server sẽ trả lời dạng sau:

**USR 6 OK venky_dude@hotmail.com venkat**

Từ cuối cùng là tên của người sử dụng. Trong SMNP7, server có thể gửi một vài thông tin bổ trợ, chẳng hạn thông tin về người dùng và mã kiểm chứng (tương tự cookie) sử dụng cho các mục đích khác.

**MSG Hotmai Hotmail 362**
**MIME-Version: 1.0**
**Content-Type: text/x-msmsgspro file; charset=UT**
**LoginTime: 1011252477**
**EmailEnabled: 1**
**MemberIdHigh: 84736**
**MemberIdLow: - 1434729391**
**lang _preference: 103**
**preferredEmai l: venky_dude@hotmail.com**
**country: IN**
**PostalCode:**
**Gender: M**
**Kid:0**
**Age: 22**
**sid: 517**
**kv: 2**
**MSPAuth:**
**2AAAAAAADU0p4uxxxJtDJozJSlUTS0i7YpwnC9PUHRv56YKxxxCTWmg$S**

Giờ đây người sử dụng đã đăng nhập hệ thống, nhưng vẫn ở trong trạng thái không trực tuyến, để chuyển trạng thái, client sẽ gửi lệnh sau:



CHG 7 NLN

Người dùng không gửi ngay lệnh này vì có thể người sử dụng muốn đăng nhập hệ thống nhưng dưới chế độ ẩn. Trong thông điệp Server trả lời có liệt kê danh sách các "bạn bè" ở trạng thái khác nhau, chẳng hạn:

**CHG 7 NLN**
**ILN 7 NLN btxxxe@hotmail.com nick**
**ILN 7 AWY wmpyxxx@msn.com mike**
**ILN 7 BSY tehpxxpxx@hotmail.com yeaxxx**
**MSG Hotmail Hotmail 223**
**MIME-Version: 1.0**
**Content-Type: text/x-msmsgsinitialemailnotification; charset=UTF-8**
**Inbox-Unread: 293**
**Folders-Unread: 0**
**Inbox-URL: /cgi-bin/HoTMaiL**
**Folders-URL: /cgi-bin/folders**
**Post-URL: http://www.hotmail.com**

Để có danh sách các bạn bè, client có thể sử dụng lệnh:

**LST 9 RL**

Nhận được lệnh này, server sẽ gửi cho client danh sách các "bạn bè", ví dụ:

**LST 9 RL 69 1 19 venky_dude@hotmail.com venkat**
**LST 9 RL 69 2 19 puxxxxx@hotmail.com PUJA**
**LST 9 RL 69 3 19 vancxxxxx@hotmail.com ramachandran**
**LST 9 RL 69 4 19 moxxxxx@hotmail.com chandramouli**
**LST 9 RL 69 5 19 v_n_xxxxx@hotmail.com Narayanaswamy**
**LST 9 RL 69 6 19 dexxxxx@hotmail.com Venkatesh**
**LST 9 RL 69 7 19 lousydxxxxx@hotmail.com DKV**

**LST 9 RL 69 8 19 hexxxxxr@hotmail.com Hetchar%20Ramachandran**
**LST 9 RL 69 9 19 ambxxxxx@hotmail.com Aiyer**
**LST 9 RL 69 10 19 suxxx@hotmail.com Ganesh**
**LST 9 RL 69 11 19 deexxxxx@hotmail.com Deepak**
**LST 9 RL 69 12 19 anilxxxxx@hotmail.com anil**
**LST 9 RL 69 13 19 dixxxxx@hotmail.com <Diamond>**
**LST 9 RL 69 14 19 nvxxxx@hotmail.com giri**
**LST 9 RL 69 15 19 shxxx@hotmail.com Hari**
**LST 9 RL 69 16 19 radhikashuxxxxx@hotmail.com radhika**
**LST 9 RL 69 17 19 eskaxxxxx@hotmail.com kannan**
**LST 9 RL 69 18 19 shaxxxxx@hotmail.com Shankar**
**LST 9 RL 69 19 19 puneetagarxxxxx@hotmail.com puneet**

Cứ mỗi khi có một người bạn chuyển sang trạng thái trực tuyến, NS sẽ gửi thông điệp kiểu sau cho client:

**NLN 10 NLN deaxxxx@hotmail.com Venkatesh**

Khi một người bạn thoát khỏi mạng (không trực tuyến), NS gửi thông điệp kiểu sau:

**FLN 10 FLN deaxxxx@hotmail.com**

Như vậy, người sử dụng đã đăng nhập thành công vào mạng MSN, sau đó người sử dụng có thể gửi và nhận các tin nhắn.

NSD chỉ có thể tham gia hội thoại trong hai trường hợp sau: NSD khởi tạo cuộc hội thoại với ai đó hoặc ai đó khởi tạo cuộc hội thoại với NSD.

**NSD khởi tạo cuộc hội thoại**

Tất cả các cuộc hội thoại đều diễn ra qua SS. Client gửi lệnh sau yêu cầu địa chỉ IP của Switchboard server

**XFR 9 SB**

NS gửi thông điệp trả lời chứa địa chỉ IP, cổng của SS cùng với mã CKI. CKI là phương pháp bảo mật mà client phải sử dụng khi liên lạc với SS.

XFR 9 SB 64.4.13.88:1863 CKI 989487642.2070896604

Kế tiếp Client sẽ tạo ra một kết nối mới tới SS có địa chỉ vừa nhận được (**64.4.13.88**). Chú ý rằng client vẫn duy trì kết nối tới NS, kết nối này chỉ được đóng khi NSD thoát khỏi hệ thống. Sau khi kết nối thành công, chúng ta gửi lệnh sau cho SS:

USR 1 venky_dude@hotmail.com 989487642.2070896604

Nếu CKI đúng, SS sẽ gửi cho chúng ta lệnh tương tự sau:

USR 1 OK venky_dude@hotmail.com venkat

Sau đó, NSD có thể "gọi" bạn bè để tham gia hội thoại thông qua lệnh sau

CAL 2 deadxxx@hotmail.com



Thông điệp trả lời từ Server sẽ định danh phiên hội thoại (session id). Định danh này sẽ được chuyển tiếp cho NSD sẽ tham gia hội thoại.

CAL 2 RINGING 11717653

Khi NSD khác trả lời thông điệp và sẵn sàng hội thoại, SS gửi lệnh sau cho client:

JOI deadlee@hotmail.com Venkatesh

Lệnh này chứng tỏ NSD khác đã tham gia hội thoại và sẵn sàng gửi/nhận các tin nhắn.

NSD nhận yêu cầu hội thoại từ NSD khác

Khi NSD 1 được NSD 2 mời "hội thoại" thì NS của NSD 1 gửi thông điệp sau cho client của NSD 1:

RNG 11742066 64.4.13.74:1863 CKI 989495494.750408580 deaxxxx@hotmail.com Venkatesh

Thông điệp này chứa session id, địa chỉ IP và cổng của SwitchBoard, mã hash CKI và tên người dùng khởi tạo cuộc nói chuyện.

NSD kết nối đến SS và gửi lệnh sau:

ANS 1 venky_dude@hotmail.com 989495494.750408580 11742066

Ở đây, NSD gửi tên đăng nhập, mã CKI và session ID mà server đã gửi

Server trả lời:

IRO 1 1 1 deaxxxx@hotmail.com Venkatesh

ANS 1 OK

Bây giờ hai bên có thể tiến hành hội thoại với nhau. Trước khi nhận và gửi thông điệp, chúng ta sẽ xem cách thức client xây dựng thông điệp như thế nào.

Tiêu đề thông điệp có khuôn dạng sau:

**MIME-Version: 1.0**
**Content-Type: text/plain; charset=UTF-8**
**X-MMS-IM-Format: FN=Microsoft%20Sans%20Serif; EF=; CO=0; CS=0; PF=22**

Khuôn dạng thông điệp được gửi đi:

```
MSG 2 N 137
MIME-Version: 1.0
Content-Type: text/plain; charset=UTF-8
X-MMS-IM-Format: FN=Microsoft%20Sans%20Serif; EF=; CO=0; CS=0; PF=22
hello
```

2 là "trial id", giá trị này được tự động tăng lên 1 sau mỗi thông điệp gửi đi, 137 là độ dài toàn bộ thông điệp Thông điệp trả lời có khuôn dạng tương tự:

```
MSG deaxxxx@hotmail.com Venkatesh 137
MIME-Version: 1.0
Content-Type: text/plain; charset=UTF-8
X-MMS-IM-Format: FN=Microsoft%20Sans%20Serif; EF=; CO=0; CS=0; PF=22
Hello
```

## 2.6.3 Kiến trúc chia sẻ file ngang hàng Gnutella

Gnutella lúc đầu được phát triển tại AOL, sau đó tách ra và được nhiều người phát triển. Hiện tại có khá nhiều hệ thống kế thừa kiến trúc này, chẳng hạn LimeWire, BearShear, Gnucleus, XoloX, và Shareaza.

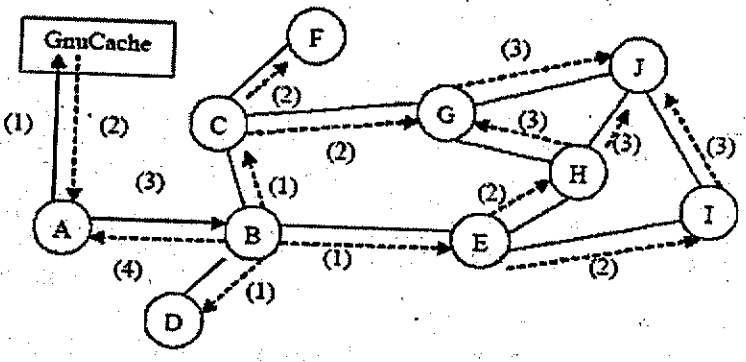
### Kiến trúc Gnutella

Gnutella không có một server chỉ mục trung tâm như Napster. Mạng Gnutella gồm các nút ngang hàng nhau (peer), có thể đối một kết nối trực tiếp với nhau. Các nút này còn được gọi là servent, vì vừa đóng vai trò client (khi yêu cầu nút khác) lẫn server (khi đáp ứng yêu cầu từ nút khác). Các nút có bản ghi thông tin chỉ mục về toàn bộ (hoặc một phần) hệ thống.

Muốn gia nhập mạng Gnutella, nút phải xác định được địa chỉ một nút đã nằm trong mạng Gnutella. Điều này có thể thực hiện bằng cách sử dụng GnuCache – lưu giữ địa chỉ một số nút luôn luôn kết nối vào mạng Gnutella. Sau đó, nút muốn gia nhập gửi thông điệp **GNUTELLA CONNECT** tới các nút đã nằm trong mạng Gnutella. Nếu chấp nhận, nút nhận được



thông điệp yêu cầu sẽ gửi thông điệp **GNUTELLA OK** (nếu không chấp nhận có thể gửi thông điệp bất kỳ, có khá nhiều lý do từ chối kết nối, chẳng hạn do quá tải kết nối). Sau khi kết nối vào mạng, nút gửi các thông điệp "**ping**" tới các "hàng xóm" để tìm kiếm thêm các nút khác. Do bản chất động của mạng (các nút có thể thoát khỏi mạng bất kỳ lúc nào) nên một nút thường giữ kết nối với nhiều nút khác (để tránh trường hợp nếu kết nối với một nút duy nhất, nút này thoát khỏi mạng sẽ kéo theo nút mất kết nối với mạng). Khi nhận được thông điệp "**ping**", nút gửi thông điệp "**pong**" trả lời và thông điệp này phải đi theo đúng tuyến đường của thông điệp ping tương ứng.




**Hình 2.30 Ví dụ về mạng Gnutella**

Thông điệp này chứa thông tin chi tiết của nút, chẳng hạn địa chỉ IP, ...hiệu port, số lượng file và khối lượng (tính theo byte) được chia sẻ. Mạng ...utella không có server chỉ mục trung tâm mà mỗi nút duy trì chỉ mục ...g của mình. Để tìm kiếm file, nút sẽ gửi truy vấn tới tất cả các nút "hàng ...". Khi nhận được truy vấn từ hàng xóm, nút sẽ kiểm tra dữ liệu cục bộ ... mình để xem có đáp ứng được hay không. Trong trường hợp có thể đáp ... được, nút gửi thông điệp **queryHit** cho nút đang tiến hành tìm kiếm. ... không đáp ứng được, nút chuyển tiếp thông điệp tới các hàng xóm của ...h. Chú ý trong trường hợp nút tạo thông điệp **queryHit** nằm đằng sau ...wall, nút tìm kiếm không thể tạo kết nối TCP tới được, khi đó, nút tìm ... phải gửi thông điệp **Put** tới nút chứa dữ liệu. Nút này sẽ tạo đường kết ...TTP tới nút tìm kiếm. Việc truyền file được thực hiện nhờ giao thức ...P.

Vì các nút sẽ gửi quảng bá thông điệp, nên để tránh tình trạng làm "tràn ngập" mạng, trong tiêu đề mỗi thông điệp có trường TTL (Time-to-Live), giá trị của trường này sẽ được giảm đi một tại mỗi nút. Tại nút nào mà trường này có giá trị 0, nút sẽ xóa thông điệp tương ứng. Điều này khiến một thông điệp không thể lưu chuyển mãi mãi trên mạng. Mỗi nút phải ghi nhớ định danh thông điệp và trường dữ liệu của mỗi thông điệp nhận được để tránh tình trạng gửi trùng lặp thông điệp. Kế tiếp chúng ta sẽ mô tả giao thức Gnutella.

## *Trong Lịch sử*

**Kazaa, một trong những mạng chia sẻ file "lấy lừng" nhất thế giới, vừa chấp nhận trả 100 triệu USD để dàn xếp vụ kiện bản quyền với ngành công nghiệp nhạc số và điện ảnh của Mỹ.**

Theo thỏa thuận, chủ sở hữu của Kazaa - Sharman Networks sẽ trả cho 4 hãng đĩa đại gia là Universal Musicm Sony BMG, EMI và Warner Music hơn 100 triệu USD, cùng lời cam kết sẽ "hoạt động hợp pháp". Hiệp hội Điện ảnh Hoa Kỳ cho biết Sharman sẽ tiếp tục duy trì Kazaa và triển khai thêm nhiều công nghệ mới để ngăn chặn việc phát tán trái phép các nội dung có bản quyền trên mạng . Kazaa đã phải tiến hành dàn xếp tại 2 địa điểm cùng một lúc: một là tại Úc, nơi tòa án đã ra phán quyết rằng Sharman Networks vi phạm bản quyền. Vụ kiện kia là tại California, và hai người sáng lập ra Kazaa là Niklas Zennstrom và Janus Friis đều bị buộc tội đồng phạm.

Sau khi bán lại Kazaa cho Sharman Networks vào năm 2002, Zennstrom và Friis đã cùng nhau tạo ra Skype - phần mềm gọi điện Internet thông dụng nhất hiện nay. Sau đấy, họ lại tiếp tục bán Skype cho eBay đổi lấy 2,6 tỷ USD tiền mặt và cổ phiếu.

**Biểu tượng là chính**

Ngành công nghiệp âm nhạc đã theo đuổi một chính sách pháp lý quyết liệt nhằm tiêu diệt nạn ăn cắp bản quyền qua mạng Internet. RIAA (Hiệp hội ghi âm Hoa Kỳ) đã đệ đơn kiện một loạt mạng chia sẻ file như Kazaa và Grokster cùng hàng chục cá nhân vi phạm. Nỗ lực của họ càng được khuyến khích khi năm ngoái, Tòa án Tối cao Hoa Kỳ tuyên bố các nhà cung cấp nội dung có quyền kiện những hãng công nghệ tiếp tay cho nạn xâm phạm bản quyền. Cùng lúc, những dịch vụ nhạc số hợp pháp như iTunes cũng ăn nên làm ra một cách bất ngờ, khiến cho người dùng nguôi ngoai "nỗi nhớ" mạng P2P. Thật ra, theo giới phân tích, vụ dàn xếp chỉ mang ý nghĩa biểu tượng là chính, bởi Kazaa đã qua thời kỳ đỉnh cao của nó. "Ngày nay, hầu như rất ít người còn dùng Kazaa. Đã xuất hiện nhiều dịch vụ ưu việt hơn, nhưng đây là một chiến thắng pháp lý mang tính biểu tượng cho RIAA", chuyên gia Jonathan Arber nhận định.

Năm ngoái, doanh thu đĩa CD lậu đạt tới 4,5 tỷ USD, tức là cứ 3 đĩa CD được bán thì lại có hơn 1 chiếc là đĩa lậu. Số lượng bản nhạc bị download trái phép là 20 tỷ, tức là bình quân mỗi người trên trái đất download tới 3 bài.



Giả sử NSD A muốn kết nối tới mạng Gnutella để tìm kiếm file (Xem Hình 2.30). A gửi thông điệp truy vấn tới hàng xóm của mình – là B. Đầu tiên B kiểm tra xem có phải đây là lần đầu tiên mình nhận thông điệp này hay không. B nếu có dữ liệu cần tìm sẽ gửi thông điệp **queryHit** tới A. B giảm trường TTL trong tiêu đề thông điệp đi 1, và gửi tiếp thông điệp đến C, D và E. C, D, và E tiếp tục thực hiện các thao tác tương tự và chuyển thông điệp tới F, G, H, và I. 4 NSD này sẽ thực hiện thao tác tương tự để chuyển thông điệp tới J. Giả sử H là nút đầu tiên chuyển tiếp thông điệp tới J, khi đó các thông điệp giống như vậy do G và I chuyển cho J sẽ bị J loại bỏ (vì J đã nhận được thông điệp như thế rồi). Bây giờ, giả sử J có dữ liệu mà A cần, J sẽ gửi thông điệp **queryHit** tới A (thông điệp này đi theo đúng tuyến đường cũ nhưng theo chiều ngược lại, từ J, qua H, qua E, B rồi đến A). Sau đó A có thể kết nối trực tiếp đến J để tải dữ liệu về theo giao thức HTTP.

## Khuôn dạng thông điệp của giao thức Gnutella

Các thông điệp của giao thức Gnutella được chia thành 5 kiểu: **Ping, Pong, Query, QueryHit,** và **Push**.

**Ping**: Được sử dụng để phát hiện các nút trên mạng. Một nút khi nhận được một thông điệp Ping có thể trả lời bằng một hoặc nhiều thông điệp Pong.

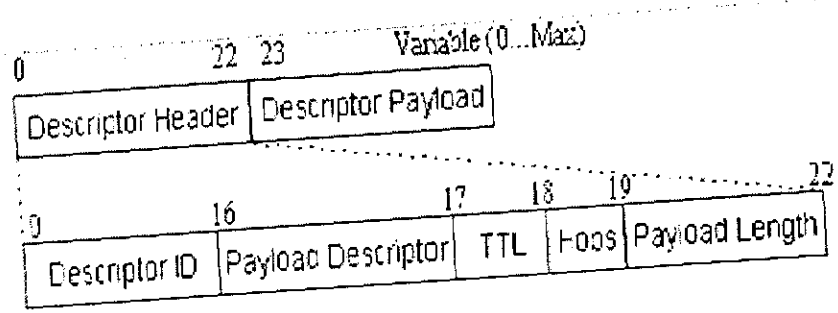
**Pong**. Thông điệp trả lời cho Ping. Chứa địa chỉ và các thông tin của nút (chẳng hạn danh sách các file chia sẻ).

**Query**. Là thông điệp phục vụ mục đích tìm kiếm trên mạng. Nếu nhận được truy vấn mà có dữ liệu đáp ứng được, nút gửi thông điệp QueryHit trả lời.

**QueryHit**. Là thông điệp trả lời thông điệp Query. Thông điệp này cung cấp các thông tin cần thiết để phía tìm kiếm có thể tải file.

**Push**. Được các nút đằng sau firewall sử dụng khi muốn chuyển dữ liệu cho nút khác.

## Các thông tin tiêu đề




**Hình 2.31 Khuôn dạng tổng quát của thông điệp GNUTELLA**

Hình 2.31 minh họa tiêu đề gồm 5 trường của một thông điệp Gnutella tổng quát:

- **Descriptor ID (Định danh thông điệp)** xác định duy nhất một thông điệp trên mạng.
- **Payload Descriptor (Dữ liệu)** Xác định kiểu thông điệp (0x00 cho Ping, 0x01 cho Pong, 0x40 cho Push, 0x80 cho Query, and 0x81 cho QueryHit).
- **TTL** Số chặng mà thông điệp có thể lan tỏa trên mạng.
- **Hops**: Số chặng mà thông điệp đã đi qua (tổng của giá trị này với giá trị TTL là giá trị TTL khởi đầu).
- **Payload Length**: Độ dài của trường dữ liệu.

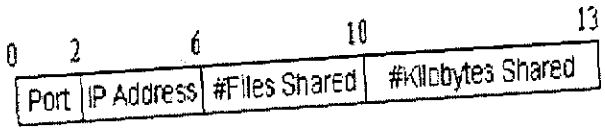
## Mô tả trường dữ liệu

Có năm kiểu trường dữ liệu khác nhau (ứng với 5 kiểu thông điệp).

### 1. Ping

Thông điệp Ping không có trường dữ liệu.

### 2. Pong




**Hình 2.32 Khuôn dạng thông điệp PONG**



Dữ liệu trong thông điệp Pong có bốn phần (Hình 2.32).Thông điệp Pong được gửi để trả lời thông điệp Ping. Một thông điệp Ping có thể có nhiều thông điệp Pong trả lời.

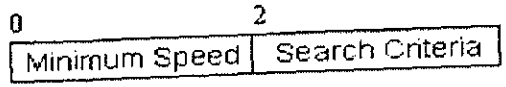
**Port**: số hiệu cổng host chấp nhận kết nối.

**IP Address**: địa chỉ IP của nút.

**#Files Shared**: Số lượng file mà host chia sẻ.

**#Kilobytes Shared**: Số lượng KB host đã chia sẻ.

### 3. Query

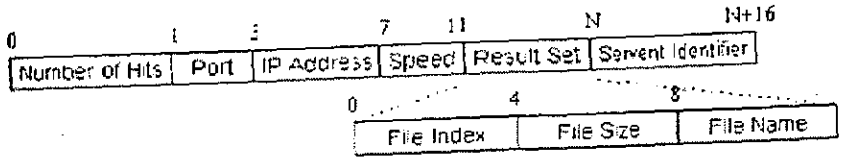



**Hình 2.33 Khuôn dạng thông điệp Query**

Là thông điệp truy vấn, gồm hai phần: Minimum Speed và Search Criteria.

**Minimum Speed**: Tốc độ cực tiểu (đơn vị KB/s) mà nút có thể đáp ứng với thông điệp.

**Search Criteria**: Tiêu chí tìm kiếm, độ dài của trường này bị giới hạn bởi giá trị trường Payload Length trong tiêu đề thông điệp.




**Hình 2.34 Khuôn dạng thông điệp QueryHit**

**4. Thông điệp QueryHit** trả lời cho thông điệp Query. Thông điệp này được nút có thể đáp ứng yêu cầu gửi cho nút có yêu cầu. Định danh thông điệp trong tiêu đề thông điệp QueryHit trùng với định danh thông điệp của thông điệp Query tương ứng. Điều này cho phép nút nhận có thể xác định kết quả trả lời ứng với câu hỏi truy vấn nào.

**Number of Hits**: Số lượng các câu trả lời trong Result Set.

**Port**: Số hiệu cổng mà nút có thể chấp nhận các kết nối.

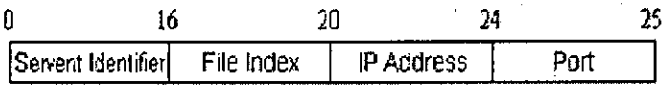
**IP Address**: địa chỉ IP của nút tương ứng

**Speed**: tốc độ (KB/s) của nút.

**Result Set**: Tập hợp các kết quả thỏa mãn câu truy vấn. Tập hợp này bao gồm các bản ghi liên tục nhau, mỗi bản ghi gồm tên file, kích thước file và đường dẫn đến file.

**Servent Identifier**: là chuỗi 16-byte xác định nút duy nhất trên mạng.

**5. Push (0x40)**




**Hình 2.35 Khuôn dạng thông điệp PUSH**

Thông điệp Push được sử dụng bởi nút yêu cầu đề nghị nút có dữ liệu nhưng ở phía sau firewall khởi tạo kết nối trước.

**Servent Identifier**: chuỗi 16-byte xác định nút được đề nghị chuyển file có đường dẫn đặt ở File_Index. Định danh này phải giống với định danh trong thông điệp QueryHit tương ứng.

**File Index**: xác định file được đề nghị gửi.

**Port**: Số hiệu cổng mà nút có thể chấp nhận các kết nối.

**IP Address**: địa chỉ IP của nút tương ứng.

## 2.7 LẬP TRÌNH SOCKET

Phần này giới thiệu quá trình phát triển ứng dụng mạng. Trong các phần trước, chúng ta đã biết phần lớn các ứng dụng mạng gồm hai phía: Client và Server. Hai phía trao đổi với nhau bằng cách gửi và nhận các thông điệp qua Socket. Phần này sẽ giới thiệu các bước chính trong quá trình



phát triển các ứng dụng mạng. Sau đó chúng ta sẽ giới thiệu một chương trình Web server rất đơn giản.

### 2.7.1 Các hàm thao tác trên Socket

Đầu tiên, chương trình phía server phải chạy và lắng nghe trên một cổng nào đó để đợi phía client kết nối tới. Nếu mọi việc diễn ra bình thường (kết nối thành công), cả hai phía đều có hai thể hiện của lớp Socket và dữ liệu sẽ được truyền qua hai socket này.

Để mở socket MyClient, phía client sẽ thực hiện khai báo và sau đó sử dụng phương thức tạo mới Socket như sau:

```
Socket MyClient;
try {
        MyClient = new Socket("Machine name", PortNumber);

catch (IOException e) {
        System.out.println(e);
```

Trong đó **Machine name** là tên (hoặc địa chỉ IP) của máy tính server, và **PortNumber** là số hiệu cổng mà tiến trình server đang chạy "lắng nghe" (đợi kết nối từ client). Chú ý các port từ 0-1023 được sử dụng cho các ứng dụng đặc biệt (HTTP, FTP, SMTP) nên bạn hãy lựa chọn cổng có số hiệu lớn hơn 1023.

Phía server sẽ mở socket bằng cách sau:

```
ServerSocket MyService;
try {
        MyServerice = new ServerSocket(PortNumber);

catch (IOException e) {
        System.out.println(e);
```

Phía server cần phải khởi tạo đối tượng của lớp **ServerSocket** với mục đích lắng nghe và chấp nhận kết nối đến từ client.

```
Socket clientSocket = null;
```

```
try {
        serviceSocket = MyService.accept();
}
catch (IOException e) {
        System.out.println(e);
}
```

### Tạo đối tượng Input Stream ở phía client

Phía client phải sử dụng lớp DataInputStream tạo input với mục đích nhận thông điệp trả lời từ server:

```
DataInputStream input;
try {
        input = new DataInputStream(MyClient.getInputStream());
}
catch (IOException e) {
        System.out.println(e);
}
```

Lớp **DataInputStream** cho phép bạn đọc từng dòng văn bản hoặc các đối tượng thuộc kiểu cơ bản trong ngôn ngữ lập trình Java (chẳng hạn read, readChar, readInt, readDouble, và readLine).

Ở phía server, cũng sử dụng lớp **DataInputStream** để nhận thông điệp từ client:

```
DataInputStream input;
try {
    input = new DataInputStream(serviceSocket.getInputStream());
}
catch (IOException e) {
  System.out.println(e);
}
```

### Tạo output stream

Phía client có thể sử dụng lớp **PrintStream** hoặc **DataOutputStream** của java.io để gửi thông điệp cho server.

```
PrintStream output;
try {
        output = new PrintStream(MyClient.getOutputStream());
```



```
}
catch (IOException e) {
        System.out.println(e);
}
```

Lớp **PrintStream** có phương thức để hiển thị các kiểu dữ liệu cơ bản của Java dưới dạng văn bản (Chẳng hạn các phương thức Write hoặc Println), còn lớp **DataOutputStream** có thể được sử dụng như sau:

```
DataOutputStream output;
try {
        output = new DataOutputStream(MyClient.getOutputStream());
}
catch (IOException e) {
        System.out.println(e);
}
```

Lớp **DataOutputStream** cũng cho phép viết các kiểu dữ liệu cơ bản trong Java (ví dụ phương thức writeBytes).

Lớp **PrintStream** được phía server sử dụng để gửi thông điệp cho client.

```
PrintStream output;
try {
        output = new PrintStream(serviceSocket.getOutputStream());

catch (IOException e) {
        System.out.println(e);
```

### Đóng kết nối

Phải đóng output và input stream trước khi đóng socket.

Ở phía client:

```
try {
        output.close();
        input.close();
        MyClient.close();

catch (IOException e) {
        System.out.println(e);
```

```
}
```

Ở phía server:

```
try {
        output.close();
        input.close();
        serviceSocket.close();
        MyService.close();
}
catch (IOException e) {
        System.out.println(e);
}
```

## 2.7.2 Ví dụ một chương trình client/server đơn giản

Ví dụ đơn giản này minh họa một ứng dụng server/client đơn giản. Client sẽ gửi cho Server một chuỗi, Server sẽ gửi phản hồi chuỗi này cho Client. Trong ví dụ này sử dụng địa chỉ máy tính là **localhost** (ứng với địa chỉ IP **127.0.0.1**), khi đó cả server và client chạy trên cùng một máy tính.

Đây là mã nguồn của Server.java:

```
import java.lang.*;
import java.io.*;
import java.net.*;
class     Server {
          public static void main(String args[]) {
                    String data = "Toobie ornaught toobie";
                    try {
                         ServerSocket srvr = new ServerSocket(1234);
                         Socket skt = srvr.accept();
                         System.out.print("Server has connected!\n");
                              PrintWriter out =
                              new PrintWriter(skt.getOutputStream(),true);
                              System.out.print("Sending string: '" + data +
"'\n");
                              out.print(data);
                              out.close();
```



```
                              skt.close();
                              srvr.close();
                    }
                    catch(Exception e) {
                              System.out.print("Whoops!     It     didn't
work!\n");
                    }
          }
}
```

Khối chương trình chính nằm trong khối **try{}**. Đối tượng **ServerSocket** được khởi tạo để lắng nghe cổng 1234. Sau khi khởi tạo, đối tượng Socket sử dụng phương thức **accept()** của lớp **ServerSocket** để đợi client kết nối đến. Phương thức này trả lại một đối tượng của lớp **Socket (skt)** – đối tượng này đóng vai trò "đầu mút" truyền thông ở phía server. **skt.getOutputStream()** trả lại output stream qua đó server có thể gửi thông điệp tới client, và **skt.getInputStream()** trả lại input stream qua đó server có thể nhận thông điệp từ client. Ví dụ này tạo ra đối tượng **PrintWriter** sử dụng output stream để đơn giản hóa việc kết xuất và gửi dữ liệu (đặt trong biến data) tới client (**out.print(data)**).

Đây là mã chương trình **Client.java**:

```
import java.lang.*;
import java.io.*;
import java.net.*;
class Client {
        public static void main(String args[]) {
        try {
                Socket skt = new Socket("localhost", 1234);
                BufferedReader in = new BufferedReader(new
                InputStreamReader(skt.getInputStream()));
                System.out.print("Received string: '");
                while (!in.ready()) {}
                        System.out.println(in.readLine());
                        System.out.print("'\n");
                        in.close();
                }
        catch(Exception e) {
                System.out.print("Whoops! It didn't work!\n");
        }
        }
}
```

Chúng ta thấy khối chương trình chính của client cũng nằm trong khối **try{}**. Một đối tượng của lớp Socket được tạo ra để kết nối tới server. Ở đây, client sẽ kết nối tới server có địa chỉ localhost ở cổng 1234 – cổng mà server đang lắng nghe. Sau khi được tạo ra, socket cũng hoạt động tương tự như đối tượng lớp ServerSocket trong file Server.java. Tiếp theo, input stream được tạo ra và là dữ liệu để khởi tạo một đối tượng thuộc lớp BufferedReader. Dữ liệu được đọc từ lớp này và hiển thị lên màn hình.

## 2.7.3 Web server đơn giản

Trong phần này chúng ta sẽ phân tích và phát triển ứng dụng Web server rất đơn giản. Chương trình của chúng ta khi thực thi sẽ đợi yêu cầu từ trình duyệt và nếu có đối tượng được yêu cầu sẽ gửi đối tượng cho trình duyệt. Đối với ứng dụng Web, trình duyệt (client) luôn là phía thiết lập kết nối trước và sau đó gửi yêu cầu HTTP. Phía server không có nhiệm vụ kết nối với client, tuy nhiên cả hai phía đều có khả năng đóng kết nối. Chẳng hạn, khi NSD nhấn nút Stop trên trình duyệt thì có thể khiến trình duyệt kết thúc việc tải file về và sau đó đóng kết nối TCP lại.

### HTTP Request

Như chúng ta đã nói trong phần 2.2, yêu cầu HTTP có ba thành phần chính

- Phương thức / Phiên bản giao thức
- Tiêu đề của thông điệp yêu cầu
- Thân yêu cầu

Mỗi yêu cầu HTTP có thể sử dụng một trong các phương thức sau: GET, POST, HEAD, OPTIONS, PUT, DELETE, TRACE, trong đó GET và POST là thông dụng nhất. Sau phần phương thức là URL – địa chỉ của tài nguyên, địa chỉ này thường là địa chỉ tương đối so với thư mục root của Web server. Phần tiêu đề thường chứa các thông tin về môi trường của trình duyệt (tên, phiên bản trình duyệt; hệ điều hành của máy client...). Các tiêu đề cách nhau bằng ký tự xuống dòng (CR-LF).



### HTTP Response

Thông điệp trả lời của HTTP gồm 3 phần sau

- Trạng thái giao thức / Mô tả trạng thái
- Tiêu đề của thông điệp
- Thân thông điệp

Ứng dụng Web server trình bày ở đây gồm ba lớp chính:

- **HttpServer**
- **Request**
- **Response**

Chương trình chính được cài đặt trong lớp **HttpServer**. Phương thức main() của lớp này sẽ tạo ra một đối tượng **HttpServer** và sau đó gọi phương thức await để đợi một yêu cầu từ client (trên một cổng nào đó), xử lý yêu cầu và sau đó gửi kết quả cho client. Đối tượng **HtttpServer** sẽ đợi cho đến khi nhận được lệnh **Shutdown**.

Web server này rất đơn giản, chỉ gửi các đối tượng tĩnh (các file HTML, file ảnh). Nó không chấp nhận tiêu đề (chẳng hạn ngày tháng, cookie) từ trình duyệt.

### Lớp HttpServer

Lớp **HttpServer** biểu diễn đối tượng Web server và có thể phục vụ các yêu cầu đối tượng tĩnh là các file nằm trong thư mục được xác định bởi biến tĩnh **WEB_ROOT** và các thư mục con của thư mục này. **WEB_ROOT** được khởi tạo như sau:

```
public static final String WEB_ROOT =
        System.getProperty("user.dir") + File.separator  + "Webroot";
```

Để yêu cầu đối tượng tĩnh, đánh địa chỉ kiểu như sau trong thanh địa chỉ của trình duyệt:

```
http://machineName:port/staticResource
```

Nếu yêu cầu này được gửi từ một máy tính khác máy tính chạy chương trình Web server, thì machimeName là địa chỉ IP của máy tính chạy Web server; còn nếu hai chương trình chạy trên cùng một máy tính thì machineName có thể là **localhost** hoặc **127.0.0.1**. Port là **8080** và

**staticResource** là tên file được yêu cầu (file này phải nằm trong thư mục WEB_ROOT).

Ví dụ, nếu hai chương trình chạy trên cùng một máy tính và trình duyệt muốn yêu cầu file **index.html** nằm trong thư mục **WEB_ROOT** thì gõ địa chỉ sau:

```
http://localhost:8080/index.html
```

Để ngừng hoạt động của server, có thể từ trình duyệt gửi lệnh **SHUTDOWN** cho server

```
http://localhost:8080/SHUTDOWN
```

Lệnh **SHUTDOWN** được cài đặt bằng một biến tĩnh bên trong lớp **HttpServer**:

```
private static final String SHUTDOWN_COMMAND = "/SHUTDOWN";
```

Chúng ta xét phương thức await sau đây:

```
public void await() {
        ServerSocket serverSocket = null;
        int port = 8080;
        try {
                serverSocket =  new ServerSocket(port, 1,
                InetAddress.getByName("127.0.0.1"));
        }
        catch (IOException e) {
                e.printStackTrace();
                System.exit(1);
        }

  // Vòng lặp, được sử dụng để đợi kết nối từ server.
        while (!shutdown) {
                Socket socket = null;
                InputStream input = null;
                OutputStream output = null;
                try {
                        socket = serverSocket.accept();
                        input = socket.getInputStream();
                        output = socket.getOutputStream();

                        // Tạo và sau đó phân tích đối tượng Request
                        Request request = new Request(input);
```



```
                        request.parse();

                        // Tạo đối tượng Response
                        Response response = new
Response(output);
                        response.setRequest(request);
                        response.sendStaticResource();

                        // Đóng kết nối
                        socket.close();

                        //Kiểm tra xem yêu cầu đến từ client có là
                        lệnh shutdown hay không

        request.getUri().equals(SHUTDOWN_COMMAND);
                }
                catch (Exception e) {
                        e.printStackTrace();
                        continue;
                }
        }
```

Phương thức **await** bắt đầu bằng cách tạo một đối tượng thuộc lớp **ServerSocket** và đặt nó trong vòng lặp **while**.

```
rverSocket= new ServerSocket(port, 1, InetAddress.getByName("127.0.0.1"));

ợi kết nối
ile (!shutdown) {
```

Đoạn mã bên trong vòng lặp while bắt đầu bằng phương thức **ept** của lớp **ServerSocket**, trả lại kết quả là yêu cầu HTTP nhận được ổng 8080:

```
ket = serverSocket.accept();
```

Khi nhận được yêu cầu, phương thức **await** tạo ra đối tượng io.InputStream và java.io.OutputStream từ đối tượng Socket i.

```
ut = socket.getInputStream();
put = socket.getOutputStream();
```

Phương thức **await** cũng tạo ra đối tượng **Request** và gọi phương thức **parse** để phân tích yêu cầu HTTP.

```
Request request = new Request(input);
request.parse();
```

Kế tiếp, tạo ra đối tượng **Response** và khởi tạo cho đối tượng này nhờ đối tượng Request và sau đó sử dụng phương thức **sendStaticResource** để gửi đối tượng.

```
Response response = new Response(output);
response.setRequest(request);
response.sendStaticResource();
```

Cuối cùng, đóng Socket và sử dụng phương thức **getUri** của lớp **Request** để kiểm tra xem yêu cầu có phải là lệnh kết thúc **SHUTDOWN** hay không.

```
// Đóng socket
socket.close();
//Kiểm tra có phải là lệnh SHUTDOWN không
shutdown = request.getUri().equals(SHUTDOWN_COMMAND);
```

#### Phân tích lớp Request

Lớp **Request** thực hiện việc biểu diễn và xử lý yêu cầu HTTP. Đối tượng của lớp này được khởi tạo từ đối tượng của lớp Socket để thực hiện việc truyền thông với Client.

Lớp **Request** có hai phương thức chính: **parse** và **getUri**. Phương thức **parse** phân tích dữ liệu thô trong yêu cầu HTTP. Nó sử dụng phương thức **parseUri** để lấy ra URL. Phương thức **parseUri** đặt giá trị URL vào biến uri. Phương thức **getUri** trả lại URL của thông điệp yêu cầu HTTP.

Chú ý rằng thông điệp HTTP yêu cầu gồm ba phần: dòng yêu cầu, các tiêu đề và thân thông điệp. Tuy nhiên trong ví dụ này, chúng ta chỉ quan tâm đến dòng yêu cầu (dòng này gồm ba phần: từ khóa là tên phương thức yêu cầu, tên đối tượng và cuối cùng là phiên bản giao thức HTTP; các phần cách nhau bằng dấu cách). Ví dụ

```
GET /index.html HTTP/1.1
```

là yêu cầu file **index.html** bằng phương thức **GET**.

Phương thức **parse** đọc toàn bộ luồng byte từ socket InputStream, sau đó chuyển cho đối tượng và sau đó lưu giữ luồng byte này trong một bộ đệm. Bộ đệm này sau đó được dùng để khởi tạo cho đối tượng **request** của



lớp **StringBuffer**. Đối tượng này sau đó được chuyển sang kiểu **String** để phương thức **parseUri** có thể phân tích

```
public void parse() {
        // Đọc các ký tự từ socket
        StringBuffer request = new StringBuffer(2048);
        int i;
        byte[] buffer = new byte[2048];
        try {
                i = input.read(buffer);
        }
        catch (IOException e) {
                e.printStackTrace();
                i = -1;
        }
        for (int j=0; j<i; j++) {
                request.append((char) buffer[j]);
        }

        System.out.print(request.toString());
        uri  = parseUri(request.toString());
```

Sau đó phương thức **parseUri** sẽ lấy địa chỉ URL từ dòng yêu cầu bằng cách trích chuỗi nằm giữa hai dấu cách đầu tiên.

```
rivate String parseUri(String requestString) {
        int index1, index2;
        index1 = requestString.indexOf(' ');
        if (index1 != -1) {
                index2 = requestString.indexOf(' ', index1 + 1);
                 if (index2 > index1)
                        return  requestString.substring(index1  +  1,
ndex2);
        }
        return null;
```

#### hân tích lớp Response

Lớp **Response** biểu diễn thông điệp HTTP trả lời, có thể sử dụng ối tượng thuộc lớp **OutputStream** để khởi tạo như sau:

```
ublic Response(OutputStream output) {
 this.output = output;
```

Đối tượng **Response** sẽ được lớp **HttpServer** khởi tạo bằng việc gán đối tượng **OutputStream** được tạo ra từ socket.

Lớp **Response** có hai phương thức: **setRequest** và **sendStaticResource**. Phương thức **setRequest** sẽ gán đối tượng **Request** cho đối tượng **Response**.

```
public void setRequest(Request request) {
  this.request = request;
}
```

Nhiệm vụ của phương thức **sendStaticResource** là gửi đối tượng tĩnh, chẳng hạn file HTML

```
public void sendStaticResource() throws IOException {
        byte[] bytes      = new byte[BUFFER_SIZE];
        FileInputStream fis = null;
        try {
                File file      =    new    File(HttpServer.WEB_ROOT,
request.getUri());
                if (file.exists()) {
                        fis    = new FileInputStream(file);
                        int ch = fis.read(bytes, 0, BUFFER_SIZE);
                        while (ch != -1) {
                        output.write(bytes, 0, ch);
                        ch = fis.read(bytes, 0, BUFFER_SIZE);
                        }
                }
                else { Không tìm thấy file
                        String errorMessage = "HTTP/1.1 404 File
                        Not Found\r\n"      +      "Content-Type:
                        text/html\r\n" +
                        "Content-Length: 23\r\n" + "\r\n" +
                        "<h1>File Not Found</h1>";
                        output.write(errorMessage.getBytes());
                }
        }
        catch (Exception e) {
                System.out.println(e.toString() );
        }
        finally {
                if (fis != null)
                fis.close();
        }
}
```



Phương thức **sendStaticResource** rất đơn giản, sử dụng tham số là đường dẫn đầy đủ của thư mục gốc (**WEB_ROOT**) và tên file yêu cầu khởi tạo đối tượng file thuộc lớp **java.io.File**.

```
File file = new File(HttpServer.WEB_ROOT, request.getUri());
```

Đầu tiên sẽ kiểm tra xem file như vậy có tồn tại không. Nếu tồn tại, phương thức **sendStaticResource** sẽ tạo ra một đối tượng thuộc lớp java.io.FileInputStream từ đối tượng **File**. Kế tiếp sẽ sử dụng phương thức **read** của lớp **FileInputStream** để ghi luồng byte lên **OutputStream**. Nội dung của đối tượng tĩnh được gửi cho trình duyệt dưới dạng dữ liệu thô.

```
If (file.exists()) {
        fis    = new FileInputStream(file);
        int ch = fis.read(bytes, 0, BUFFER_SIZE);
        while (ch != -1) {
                output.write(bytes, 0, ch);
                ch = fis.read(bytes, 0, BUFFER_SIZE);
        }
}
```

Nếu file không tồn tại, phương thức **sendStaticResource** gửi thông báo lỗi cho trình duyệt

```
String errorMessage = "HTTP/1.1 404 File Not Found\r\n" +
  "Content-Type: text/html\r\n" +
  "Content-Length: 23\r\n" +
  "\r\n" +
  "<h1>File Not Found</h1>";

output.write(errorMessage.getBytes());
```

# Chương 3
# TẦNG GIAO VẬN

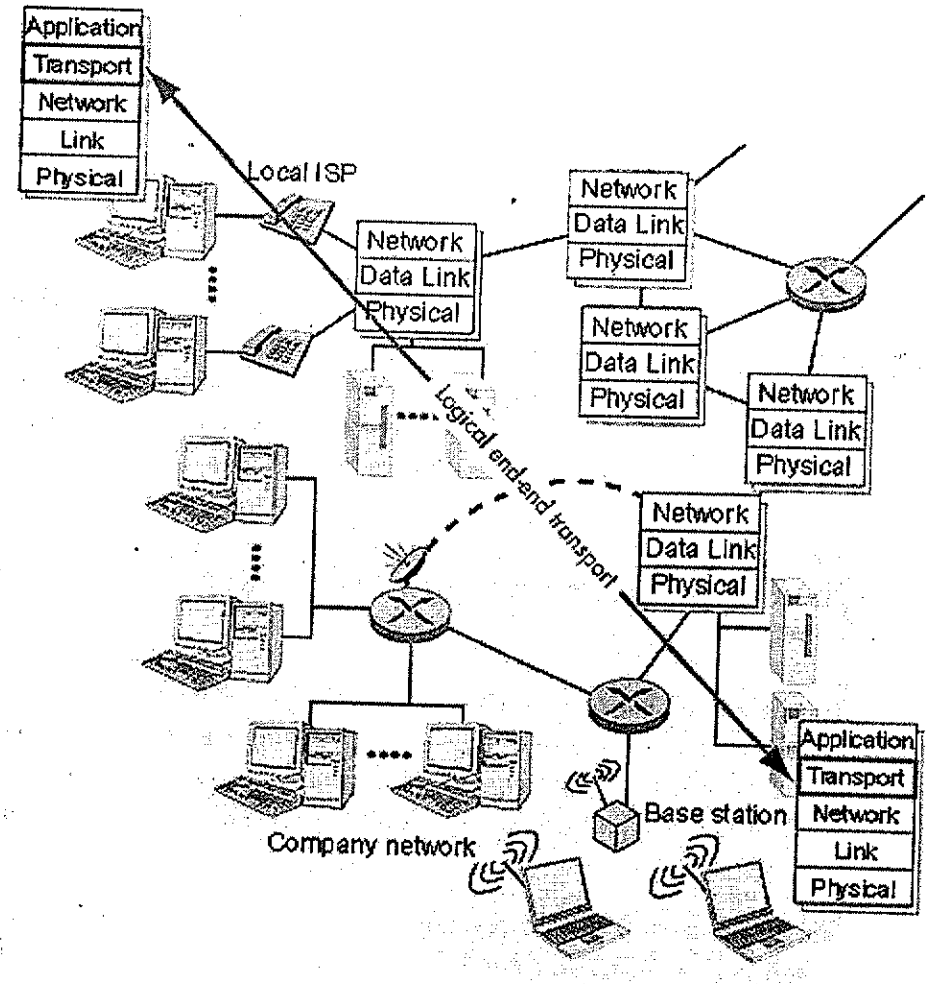
## 3.1 DỊCH VỤ VÀ NGUYÊN TẮC CỦA TẦNG GIAO VẬN

Nằm giữa tầng ứng dụng và tầng mạng, tầng giao vận là tầng trung tâm trong kiến trúc phân tầng với nhiệm vụ cung cấp dịch vụ truyền thông giữa các tiến trình ứng dụng chạy trên các máy tính khác nhau. Chương này nghiên cứu tất cả dịch vụ của tầng giao vận cũng như các nguyên tắc cơ bản thực hiện điều này theo nhiều cách tiếp cận khác nhau. Chúng ta sẽ xem cách thức dịch vụ này được cài đặt trong các giao thức. Tầng giao vận của Internet có hai giao thức quan trọng là TCP và UDP.

Hai chương trước đã nói về vai trò và những dịch vụ mà tầng giao vận cung cấp, vậy cho đến bây giờ, chúng ta đã biết gì về tầng giao vận?

Giao thức tầng giao vận cung cấp một kênh truyền logic (ảo) giữa các tiến trình ứng dụng chạy trên máy tính khác nhau. Gọi là logic vì không tồn tại một đường truyền vật lý thực sự giữa hai tiến trình. Các tiến trình ứng dụng sẽ sử dụng đường truyền ảo này để trao đổi thông điệp mà không phải bận tâm về cơ sở hạ tầng của môi trường vật lý thực sự. Hình 3.1 minh hoạ điều này.






**Hình 3.1 Tầng giao vận cung cấp dịch vụ truyền thông logic cho các tiến trình ứng dụng**

Trên Hình 3.1, tầng giao vận nằm trên các thiết bị đầu cuối chứ không phải ở các router. Router hoạt động ở tầng mạng.

Ở phía gửi, thực thể giao vận chèn thông điệp mà nó nhận được từ tiến trình ứng dụng vào các 4-PDU (là đơn vị dữ liệu của giao thức tầng giao vận – Protocol Data Unit). Công việc được thực hiện bằng cách chia thông điệp thành nhiều đoạn nhỏ, bổ sung vào đầu mỗi đoạn tiêu đề của tầng giao vận để tạo ra gói dữ liệu của tầng giao vận (4-PDU). Sau đó tầng giao vận truyền gói dữ liệu (4-PDU) xuống tầng mạng, tại đây mỗi gói này được đặt

trong gói dữ liệu của tầng mạng (3-PDU). Ở phía nhận, tầng giao vận nhận gói dữ liệu từ tầng mạng, loại bỏ phần tiêu đề của gói dữ liệu 4-PDU, ghép chúng lại thành một thông điệp hoàn chỉnh và chuyển cho tiến trình ứng dụng nhận.

Trên mạng máy tính có thể có nhiều giao thức giao vận khác nhau, cung cấp cho ứng dụng các dịch vụ với chất lượng khác nhau.

Tất cả giao thức tầng giao vận đều cung cấp dịch vụ **dồn kênh (multiplex)** và **phân kênh (demultiplex)**, điều này sẽ nói cụ thể trong các phần sau. Như đã nói trong phần 2.1, ngoài dịch vụ dồn kênh/ phân kênh, tầng giao vận còn có thể cung cấp các dịch vụ khác cho tiến trình ứng dụng như truyền dữ liệu tin cậy, đảm bảo băng thông hay giới hạn độ trễ.

### 3.1.1 Quan hệ giữa tầng giao vận và tầng mạng

Tầng giao vận nằm ở trên tầng mạng. Nếu giao thức tầng giao vận cung cấp đường truyền logic giữa tiến trình chạy trên các máy tính khác nhau, thì giao thức tầng mạng cung cấp đường truyền giữa các máy tính. Điểm khác biệt nhỏ này tuy khó nhận biết nhưng rất quan trọng, xét ví dụ dưới đây.

Giả sử có hai nhà: một ở Hà Nội, một ở Huế trong mỗi nhà có 12 đứa trẻ là anh em họ với nhau. Hàng tuần chúng trao đổi thư cho nhau, mỗi thư được đặt trong một phong bì riêng và được dịch vụ bưu chính gửi đi theo địa chỉ ghi trên phong bì. Hàng tuần mỗi nhà sẽ nhận 144 lá thư từ nhà bên kia (bọn trẻ có thể tiết kiệm được tiền nếu chúng sử dụng email). Ở mỗi nhà có một đứa trẻ chịu trách nhiệm thu thập và phân phát thư - An trong nhà phía tây, Bình trong nhà phía đông. Mỗi tuần, An lấy thư từ bọn trẻ trong nhà mình và chuyển cho nhân viên bưu cục - người thường xuyên ghé qua nhà để lấy và chuyển thư. Khi nhận thư từ nhân viên bưu tá, An chuyển tiếp thư cho người nhận. Bình cũng sẽ thực hiện công việc tương tự.

Trong ví dụ trên, dịch vụ bưu chính cung cấp đường truyền logic giữa hai nhà - chuyển thư từ nhà này đến nhà kia, chứ không phải từ người



này đến người kia. Còn An và Bình cung cấp đường truyền logic giữa từng người trong hai nhà. Đối với lũ trẻ, An và Bình là dịch vụ chuyển thư mặc dù An và Bình chỉ là một phần (phần đầu mút) của cả hệ thống chuyển thư. Qua ví dụ này ta hiểu được quan hệ giữa tầng giao vận và tầng mạng:

Máy tính (hay thiết bị đầu cuối) = Ngôi nhà.

Tiến trình = Từng người trong ngôi nhà.

Thông điệp ứng dụng = Thư trong phong bì.

Giao thức tầng mạng = Dịch vụ bưu chính (gồm nhân viên bưu chính).

Giao thức tầng giao vận = An và Bình.

Trong ví dụ trên, An và Bình thực hiện công việc phân phát thư tại chính ngôi nhà của chúng, nhưng không thực hiện những việc như sắp xếp thư tại các bưu cục (là các trạm trung chuyển trên đường đi) hay gửi thư từ bưu cục này tới bưu cục khác. Tương tự, giao thức tầng giao vận chỉ hoạt động ở các thiết bị đầu cuối. Tại thiết bị đầu cuối, giao thức tầng giao vận chuyển dữ liệu từ tiến trình ứng dụng xuống tầng mạng và ngược lại nhưng không biết thông điệp được truyền đi như thế nào trong tầng mạng. Trên hình 3.1, các router không xử lý bất kỳ thông tin tiêu đề nào mà tầng giao vận chèn vào bên cạnh thông điệp ứng dụng.

Giả sử An và Bình đi vắng, Hạnh và Phúc làm thay. Nhưng thật tiếc hai đứa trẻ này còn quá nhỏ, không làm việc được cẩn thận như An và Bình. Chúng làm mất thư. Tương tự như vậy, mạng máy tính có thể có nhiều giao thức giao vận, mỗi giao thức cung cấp các dịch vụ với chất lượng khác nhau cho chương trình ứng dụng.

Dịch vụ mà An và Bình cung cấp phụ thuộc vào dịch vụ của bưu điện. Ví dụ nếu bưu điện không đảm bảo thời gian chuyển thư giữa hai nhà thì An và Bình cũng sẽ không đảm bảo được thời gian chuyển thư giữa những người trong hai nhà. Tương tự, dịch vụ của giao thức tầng giao vận cung cấp sẽ phụ thuộc vào dịch vụ của tầng mạng bên dưới. Nếu giao thức tầng mạng không đảm bảo thời gian trễ hay đảm bảo về băng thông cho gói dữ liệu 4-PDU trong quá trình gửi giữa các máy tính, thì giao thức tầng giao vận cũng không thể cung cấp những dịch vụ này khi gửi thông điệp giữa các tiến trình ứng dụng.

Tuy nhiên, tầng giao vận vẫn có thể cung cấp những dịch vụ mà tầng mạng không cung cấp. Những dịch vụ như thế được nghiên cứu ngay trong chương này, ví dụ giao thức tầng giao vận cung cấp dịch vụ truyền dữ liệu tin cậy cho tầng ứng dụng ngay cả khi tầng mạng không đáng tin cậy - làm mất, gửi lỗi hay gửi trùng lặp dữ liệu. Một dịch vụ khác sẽ nghiên cứu trong chương 7 (An ninh mạng) là khả năng mã hoá thông điệp của tầng giao vận để đảm bảo thông điệp không bị đọc trộm, trong khi tầng mạng không thực hiện được điều này.

### 3.1.2 Tổng quan về tầng giao vận trong Internet

Trong mạng Internet hay mạng TCP/IP có hai giao thức ở tầng giao vận: UDP và TCP. **UDP** (User Datagram Protocol) cung cấp dịch vụ truyền không tin cậy, không hướng nối và **TCP** (Transmission Control Protocol) cung cấp dịch vụ tin cậy, hướng nối cho ứng dụng. Người viết ứng dụng phải lựa chọn một trong hai giao thức này cho ứng dụng của mình.

Để đơn giản, trong mô hình Internet ta coi 4-PDU là một segment. Tuy vậy, nhưng trong các khuyến nghị RFC thì 4-PDU được coi là **segment** đối với TCP và **datagram** đối với UDP. Nói chung thuật ngữ **datagram** thường sử dụng cho PDU ở tầng mạng nhưng trong một quyển sách nhập môn như thế này, nói chung ít xảy ra nhầm lẫn khi sử dụng thuật ngữ segment cho cả TCP PDU và UDP PDU.

Trước khi tiếp tục, chúng ta nói qua về tầng mạng của Internet (Tầng mạng sẽ được nghiên cứu chi tiết trong chương 4). Giao thức của tầng mạng là IP (Internet Protocol). IP cung cấp đường truyền logic giữa các máy tính và mô hình dịch vụ của nó theo kiểu **cố gắng tối đa (best effort delivery service)**. Nghĩa là IP cố gắng gửi các segment giữa các máy tính – hay thiết bị đầu cuối khác nhau - với hết khả năng của mình nhưng không đảm bảo điều này. Nói cụ thể hơn, IP không đảm bảo về thứ tự truyền, về tính toàn vẹn của dữ liệu trong segment. Chính vì thế người ta xem IP là dịch vụ không tin cậy. Mỗi máy tính có một địa chỉ IP xác định. Trong chương này ta chỉ cần biết mỗi máy tính cần có một địa chỉ IP xác định duy nhất.



Nhiệm vụ chính của UDP và TCP là mở rộng dịch vụ IP - truyền dữ liệu giữa hai thiết bị đầu cuối - thành dịch vụ truyền dữ liệu giữa hai tiến trình chạy trên thiết bị đầu cuối. Việc mở rộng từ truyền dữ liệu giữa các máy tính (host-to-host) đến truyền dữ liệu giữa các tiến trình (process-to-process) được gọi là quá trình dồn kênh (multiplex) và phân kênh (demultiplex). Vấn đề này sẽ nghiên cứu ở phần sau. UDP và TCP kiểm soát tính toàn vẹn (hay tính đúng đắn) của dữ liệu nhờ trường phát hiện lỗi đặt trong tiêu đề gói dữ liệu. UDP chỉ cung cấp dịch vụ phân phối dữ liệu giữa hai tiến trình và kiểm tra lỗi. Tương tự IP, UDP là dịch vụ không tin cậy, không đảm bảo dữ liệu được truyền đi một cách đúng đắn giữa các tiến trình. UDP được trình bày kỹ trong phần 3.1.

Ngoài phân kênh, dồn kênh, TCP còn cung cấp một số dịch vụ khác cho ứng dụng. Dịch vụ đầu tiên và quan trọng nhất là truyền dữ liệu tin cậy (reliable data transfer). Các cơ chế điều khiển lưu lượng, đánh số thứ tự, số thứ tự biên nhận, bộ định thời sẽ giúp TCP đảm bảo dữ liệu được truyền từ tiến trình gửi đến tiến trình nhận chính xác và đúng thứ tự. Như vậy giao thức TCP đã biến dịch vụ truyền không tin cậy giữa các thiết bị đầu cuối (IP) thành dịch vụ truyền dữ liệu tin cậy giữa các tiến trình.

Giao thức cung cấp dịch vụ truyền dữ liệu tin cậy và kiểm soát tắc nghẽn rất phức tạp. Các phần từ 3.4 đến 3.8 trình bày nguyên tắc chung của các dịch vụ trên và giao thức TCP. Cách tiếp cận của chương này là giới thiệu xen kẽ các nguyên lý cơ bản với giao thức TCP. Ví dụ chúng ta nói tổng quan cách thức cung cấp dịch vụ truyền dữ liệu tin cậy sau đó mới nghiên cứu TCP thực hiện điều này như thế nào. Chúng ta sẽ bắt đầu bằng công việc dồn kênh/phân kênh với dữ liệu từ tầng ứng dụng.

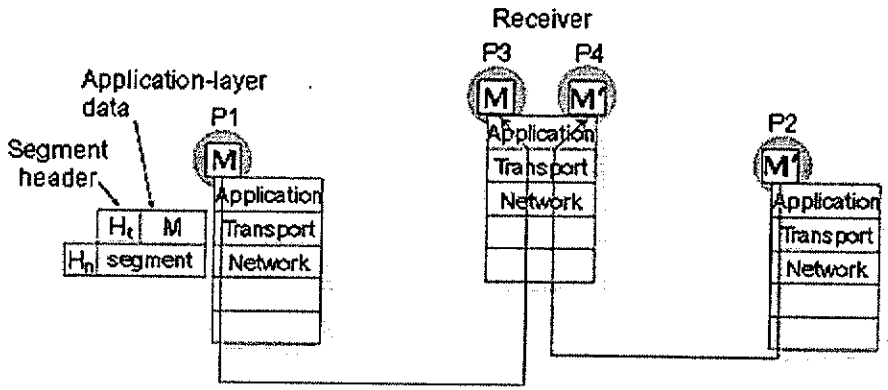
## 3.2 DỊCH VỤ DỒN KÊNH, PHÂN KÊNH

Phần này chúng ta sẽ nghiên cứu về công việc dồn kênh và phân kênh trong mạng. Để đơn giản, chúng ta chỉ nói đến các dịch vụ của tầng giao vận trong mô hình Internet. Tuy nhiên cần nhấn mạnh rằng - đây là dịch vụ cần thiết đối với tất cả các mô hình kết nối mạng.

Mặc dù dồn kênh/ phân kênh không phải là một trong những dịch vụ quan trọng nhất của tầng giao vận, nhưng nó cực kỳ cần thiết. Để hiểu tại sao như vậy, ta thấy rằng IP truyền dữ liệu giữa hai thiết bị đầu cuối, mỗi thiết bị có một địa chỉ IP nhất định. IP không truyền dữ liệu giữa các tiến trình ứng dụng chạy trên các máy tính. Mở rộng việc gửi - từ máy tính đến máy tính - tới từ tiến trình đến tiến trình là công việc dồn kênh và phân kênh.

Tại máy tính nhận, tầng giao vận nhận gói dữ liệu (hay còn gọi là segment) từ tầng mạng ngay phía dưới và có trách nhiệm gửi dữ liệu bên trong segment này tới tiến trình ứng dụng thích hợp trên máy tính. Giả sử lúc nào đó máy tính của bạn đang tải trang Web xuống, chạy một phiên FTP và hai phiên Telnet cùng một lúc. Như vậy bạn đang chạy 4 tiến trình ứng dụng: 2 tiến trình Telnet, 1 tiến trình FTP, và 1 tiến trình HTTP. Khi tầng giao vận trong máy tính của bạn nhận được dữ liệu từ tầng mạng chuyển lên, nó phải gửi dữ liệu trong đó tới 1 trong 4 tiến trình trên. Việc đó diễn ra như thế nào?

Mỗi segment của tầng giao vận có trường xác định tiến trình nhận dữ liệu. Tầng giao vận bên nhận sẽ sử dụng trường này để xác định rõ tiến trình nhận và gửi dữ liệu trong segment tới tiến trình đó. Công việc chuyển dữ liệu trong segment tới đúng tiến trình ứng dụng được gọi là phân kênh. Tại thiết bị gửi, tầng giao vận nhận dữ liệu từ nhiều tiến trình ứng dụng khác nhau, tạo segment chứa dữ liệu cùng với một số thông tin tiêu đề và cuối cùng chuyển segment xuống tầng mạng. Quá trình trên được gọi là dồn kênh. Hình 3.2 minh hoạ cả hai quá trình này.




Hình 3.2 Dịch vụ dồn kênh, phân kênh

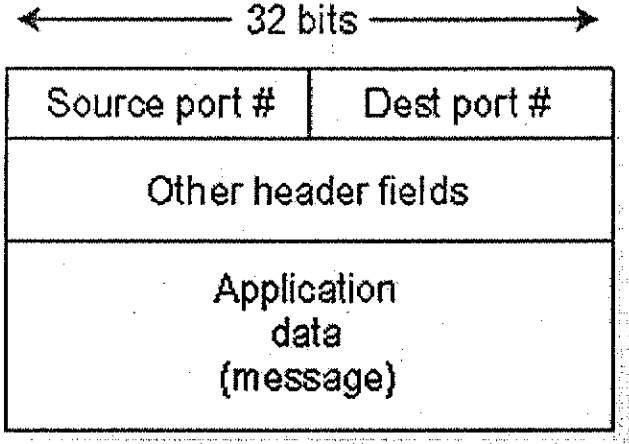


Để hiểu rõ hơn về dịch vụ dồn kênh, ta quay lại ví dụ trước. Mỗi đứa trẻ được xác định qua tên. Khi Bình nhận được thư từ người đưa thư, cậu bé sẽ thực hiện quá trình phân kênh bằng cách đọc tên trên phong bì thư để chuyển cho đúng người nhận. Còn An thực hiện quá trình dồn kênh khi thu thập thư từ mọi người và chuyển cho người đưa thư.

UDP và TCP thực hiện việc dồn kênh và phân kênh nhờ hai trường đặc biệt ở đầu segment: trường định danh cổng tiến trình gửi (nguồn – source port number) và trường định danh cổng tiến trình nhận (đích – destination port number). Hai trường này được minh họa trên Hình 3.3. Chúng xác định một tiến trình ứng dụng duy nhất chạy trên máy tính. Tất nhiên UDP và TCP còn có nhiều trường khác mà chúng ta sẽ nghiên cứu sau.

Khái niệm số hiệu cổng đã được giới thiệu qua trong chương 2. Nó là một con số 16 bit, nhận giá trị từ 0 tới 65535. Giá trị từ 0 đến 1023 là các giá trị đặc biệt và được sử dụng rất hạn chế, chỉ dành cho các ứng dụng thông dụng như HTTP, FTP sử dụng. HTTP sử dụng cổng 80, FTP sử dụng cổng 21. Danh sách các cổng thông dụng có thể tham khảo trong RFC 1700. Khi xây dựng một ứng dụng mới, phải xác định số hiệu cổng cho ứng dụng này.

Mỗi ứng dụng chạy trên thiết bị đầu cuối có số hiệu cổng nhất định. Với vậy vấn đề đặt ra là tại sao mỗi segment ở tầng giao vận đều có trường số hiệu cổng nguồn và đích. Một thiết bị đầu cuối có thể chạy đồng thời hai tiến trình cùng kiểu, như vậy số hiệu cổng đích chưa đủ để phân biệt các tiến trình. Giả sử Web server chạy tiến trình HTTP xử lý các thông điệp yêu cầu; khi Web server phục vụ nhiều yêu cầu cùng một lúc (điều này hết sức thông thường) thì server sẽ chạy nhiều tiến trình trên cổng 80. Để gửi dữ liệu đến tiến trình nhận, phải xác định số hiệu cổng của phía gửi (cổng nguồn).

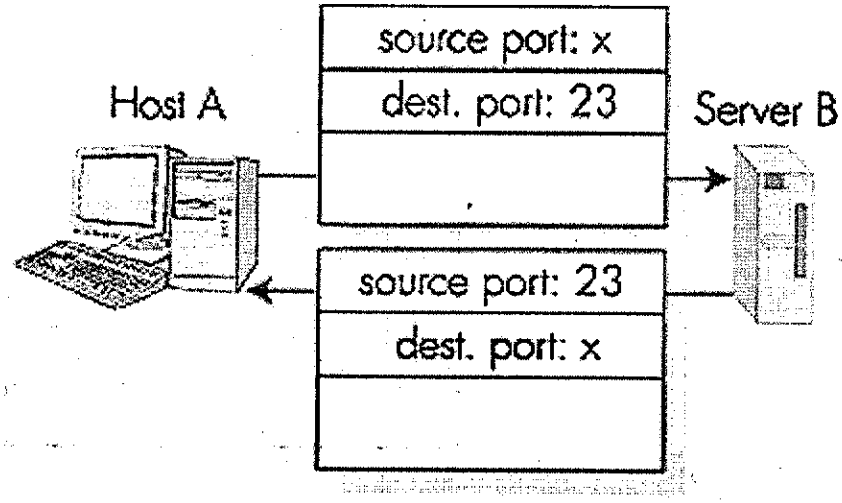



**Hình 3.3 Trường địa chỉ tiến trình gửi, tiến trình nhận trong gói dữ liệu segment**

Cổng nguồn được tạo ra như thế nào? Nhận giá trị bao nhiêu? Để trả lời câu hỏi này hãy nhớ lại rằng ứng dụng mạng sử dụng kiến trúc khách hàng/ người phục vụ. Thông thường máy tính nào khởi đầu trước đóng vai trò client, máy tính kia đóng vai trò server. Xét ví dụ một tiến trình ứng dụng có số hiệu cổng là 23 (số hiệu cổng của ứng dụng Telnet server). Hãy quan sát segment ở tầng giao vận khi rời client (là máy tính chạy chương trình Telnet client) chuyển tới server. Số hiệu cổng nguồn và đích của segment này là bao nhiêu? Số hiệu cổng đích chính là số hiệu cổng tiến trình nhận - 23. Còn số hiệu cổng nguồn - ở phía client – là một giá trị chưa được sử dụng bởi tiến trình nào, được phần mềm giao vận chạy trên máy tính client xác định tự động. Giả sử phía client chọn số hiệu cổng là x thì mỗi segment được gửi tới ứng dụng Telnet có cổng nguồn là x, cổng đích là 23. Khi segment tới, server căn cứ vào số hiệu cổng để chuyển dữ liệu trong segment tới đúng tiến trình ứng dụng nhận. Cổng đích 23 xác định tiến trình Telnet, cổng nguồn x để xác định một tiến trình gửi cụ thể.

Segment truyền từ server tới client sẽ ngược lại. Cổng nguồn bây giờ sẽ là cổng của ứng dụng có giá trị 23, còn cổng đích sẽ là x (là số hiệu cổng nguồn trong segment gửi từ client tới server). Khi segment tới, client cũng sẽ căn cứ vào số hiệu cổng nguồn và đích để gửi dữ liệu trong segment tới đúng tiến trình ứng dụng. Hình 3.4 minh hoạ quá trình trên.

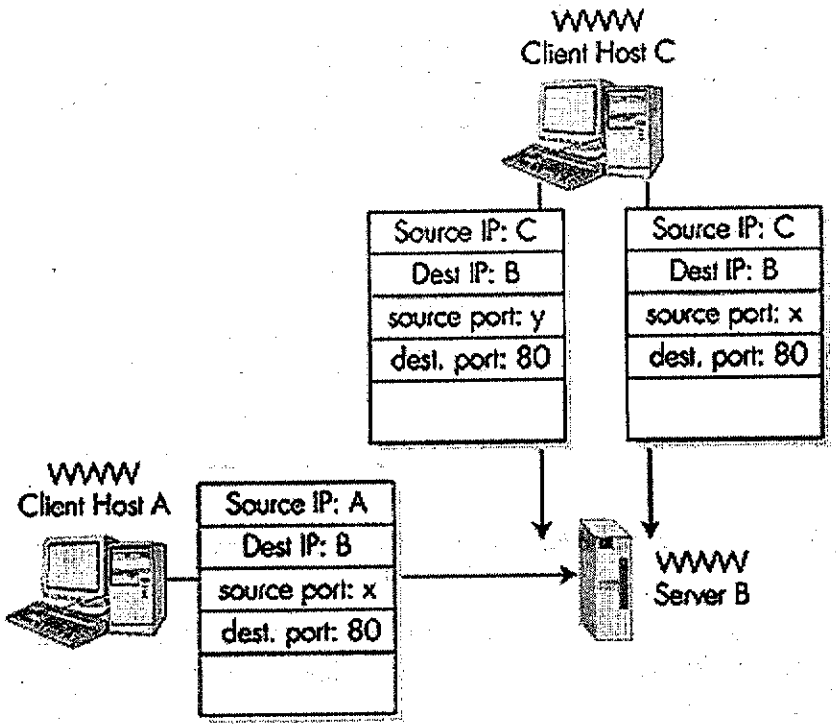





**Hình 3.4 Sử dụng số hiệu cổng nguồn và cổng đích trong trình ứng dụng khách/chủ**

Chuyện gì xảy ra nếu có hai client khác nhau cùng thiết lập phiên làm việc tới một server và mỗi client đều chọn cổng nguồn là x? Điều này rất dễ xảy ra với những Web server có nhiều người truy cập, phải phục vụ nhiều yêu cầu. Bên server phải phân kênh segment như thế nào khi hai phiên làm việc có cùng cặp số hiệu cổng? Khi đó server phải sử dụng địa chỉ IP trong gói dữ liệu IP (datagram) chứa segment. Trên Hình 3.5, máy C có hai phiên làm việc và máy A có một phiên làm việc HTTP tới cùng server B. Cả ba máy A,B,C đều có địa chỉ IP phân biệt lần lượt là A, B, C. Máy C sử dụng hai cổng nguồn (x,y) khác nhau cho hai kết nối HTTP tới B. A chọn số hiệu cổng nguồn độc lập với C nên nó có thể gán cổng nguồn x cho kết nối HTTP của mình. Tuy nhiên, máy chủ B vẫn có thể thực hiện phân kênh hai đối segement có cặp cổng giống nhau do địa chỉ IP nguồn khác nhau. Tóm lại, bên nhận sử dụng cả ba giá trị (địa chỉ IP nguồn, số hiệu cổng nguồn, số hiệu cổng đích) để xác định tiến trình ứng dụng nhận.

Sau khi xét tầng giao vận thực hiện việc dồn kênh và phân kênh các tiến trình ứng dụng như thế nào, chúng ta sẽ nghiên cứu một trong các giao thức giao vận của Internet - UDP. Trong phần này chúng ta sẽ thấy ngoài hai dịch vụ dồn kênh và phân kênh, UDP gần như không cung cấp dịch vụ nào khác.




**Hình 3.5 Hai client cùng số hiệu cổng đích truyền thông với cùng một server**

## 3.3 UDP – GIAO THỨC KHÔNG HƯỚNG NỐI

Trong phần này ta sẽ nghiên cứu cơ chế hoạt động của UDP. Độc giả cần nhớ lại khái quát về dịch vụ UDP trình bày trong phần 2.1.

Bạn sẽ làm gì nếu muốn xây dựng một giao thức giao vận cực kỳ đơn giản - một giao thức giao vận "rỗng"? Khi đó, thực thể giao vận phía gửi nhận thông điệp từ tiến trình ứng dụng và chuyển xuống tầng mạng; thực thể giao vận phía nhận chuyển thông điệp tầng mạng đưa lên tới chương trình ứng dụng tương ứng. Tầng giao vận chỉ cung cấp dịch vụ dồn kênh/phân kênh bằng cách chuyển dữ liệu đến từ tầng mạng tới đúng tiến trình ứng dụng nhận.

UDP đặc tả trong RFC 768 là giao thức giao vận cực kỳ đơn giản. Như vậy, bên cạnh chức năng dồn kênh/phân kênh, UDP có thêm cơ chế phát hiện lỗi đơn giản. Có thể nói nếu sử dụng UDP thì gần như ứng dụng làm việc trực



tiếp với tầng mạng IP. UDP lấy thông điệp từ tiến trình ứng dụng, chèn thêm một số trường tiêu đề, trong đó có hai trường địa chỉ cổng nguồn và đích cho dịch vụ dồn kênh/phân kênh để tạo nên gói dữ liệu segment. Gói segment sau khi tạo ra được chuyển xuống tầng mạng. Tầng mạng đặt segment này trong gói dữ liệu IP datagram và ***cố gắng*** gửi gói IP datagram tới máy tính nhận. Nếu segment tới đích, UDP sử dụng số hiệu cổng và địa chỉ IP của tiến trình nhận để truyền dữ liệu trong segment tới đúng tiến trình ứng dụng nhận. Chú ý UDP không đòi hỏi thực thể bên gửi và bên nhận phải liên kết trước khi trao đổi dữ liệu. Vì thế UDP được xem là dịch vụ **không hướng nối hay không liên kết trước (connectionless)**.

DNS là một giao thức tầng ứng dụng chạy trên nền UDP. Khi muốn truy vấn, DNS tạo thông điệp truy vấn DNS, chuyển thông điệp tới socket. UDP bổ sung một số trường vào đầu mỗi thông điệp để tạo ra UDP segment rồi gửi segment này xuống tầng mạng. Tầng mạng sẽ đóng gói UDP segment này trong IP datagram và gửi datagram tới đích (name server). Sau đó, DNS bên gửi đợi trả lời. Nếu không nhận được câu trả lời (điều này có thể xảy ra khi các tầng dưới làm mất thông điệp yêu cầu hay thông điệp trả lời) thì DNS gửi lại yêu cầu hoặc báo cho ứng dụng biết là không nhận được câu trả lời. Các đặc tả DNS cho phép DNS chạy trên nền TCP nhưng trong thực tế DNS thường chạy trên UDP.

So với UDP, TCP có vẻ có nhiều ưu điểm hơn: TCP cung cấp dịch vụ truyền dữ liệu tin cậy trong khi UDP không làm được. Tuy nhiên trên thực tế nhiều ứng dụng lại sử dụng UDP với các lý do sau đây:

**Không có giai đoạn thiết lập kết nối:** TCP sử dụng cơ chế "bắt tay" ba bước trước khi bắt đầu truyền dữ liệu thực sự. UDP không cần cơ chế này trước khi truyền dữ liệu. Vì thế UDP sẽ không phải chịu thời gian trễ để thiết lập đường truyền. Đây chính là nguyên nhân DNS chạy trên UDP chứ không phải là TCP. DNS sẽ chạy chậm nếu sử dụng TCP. HTTP sử dụng TCP vì các đối tượng Web cần được tải về chính xác – do đó yêu cầu một đường truyền tin cậy. Nhưng như đã trình bày trong phần 2.2, giai đoạn thiết lập đường truyền trong TCP gây nên một thời gian trễ cho ứng dụng HTTP (tình trạng "world wide wait").

**Không duy trì trạng thái kết nối.** TCP ghi nhớ trạng thái kết nối trên hệ thống đầu cuối. Trạng thái kết nối bao gồm vùng đệm (buffer) của bên nhận và bên gửi, các tham số kiểm soát tắc nghẽn, số tuần tự phát và số

biên nhận. Nó giúp TCP triển khai dịch vụ truyền tin tin cậy và cơ chế kiểm soát tắc nghẽn. Trong phần 3.5 ta sẽ hiểu ý nghĩa các trạng thái này. UDP không phải lưu giữ những thông tin như vậy. Do đó nếu phía server sử dụng UDP thì có khả năng phục vụ đồng thời nhiều client hơn.

**Tiêu đề gói dữ liệu nhỏ.**: Tiêu đề của TCP segment là 20 byte trong khi UDP chỉ có 8 bytes.

**Không kiểm soát tốc độ gửi**. TCP có cơ chế kiểm soát tắc nghẽn, điều chỉnh tốc độ gửi khi xảy ra tắc nghẽn. Cơ chế điều chỉnh này có thể ảnh hưởng tới những ứng dụng thời gian thực – là những ứng dụng chấp nhận mất mát dữ liệu (trong phạm vi nào đó) nhưng lại đòi hỏi phải có một tốc độ truyền tối thiểu. Tốc độ truyền dữ liệu của UDP chỉ bị giới hạn bởi tốc độ sinh dữ liệu của ứng dụng, khả năng máy tính nguồn (CPU, tốc độ đồng hồ), và tốc độ truy cập mạng. Chú ý rằng bên nhận không nhất thiết phải nhận toàn bộ dữ liệu. Khi mạng bị tắc nghẽn, một phần dữ liệu có thể bị mất do tràn vùng đệm ở router. Tốc độ nhận có thể bị giới hạn do tắc nghẽn ngay cả khi tốc độ gửi không bị giới hạn.

| Ứng dụng | Giao thức tầng ứng dụng | Tầng giao vận tương ứng |
|---|---|---|
| Thư điện tử | SMTP | TCP |
| Truy cập từ xa | Telnet | TCP |
| Web | HTTP | TCP |
| Truyền file | FTP | TCP |
| File server | NFS | thường là UDP |
| Đa phương tiện | Phụ thuộc vào hãng sản xuất | thường là UDP |
| Điện thoại qua Internet | Phụ thuộc vào hãng sản xuất | thường là UDP |
| Quản lý mạng | SNMP | thường là UDP |
| Định tuyến | RIP | thường là UDP |
| Tên miền | DNS | thường là UDP |

**Hình 3.6 Các ứng dụng thông dụng và giao thức giao vận tương ứng**



Hình 3.6 liệt kê một số ứng dụng phổ biến và giao thức giao vận của chúng. Email, truy cập từ xa, Web và truyền file chạy trên nền TCP vì chúng cần đến dịch vụ truyền dữ liệu tin cậy. Tuy nhiên có một số ứng dụng khác thích hợp với UDP hơn TCP. Giao thức cập nhật bảng định tuyến RIP (sẽ học trong chương 4) sử dụng UDP, bởi vì việc cập nhật được thực hiện định kỳ (thường khoảng 5 phút một lần), cho nên dù cập nhật bị mất nhưng sẽ có cập nhật mới sau một khoảng thời gian ngắn. UDP được sử dụng để gửi dữ liệu quản trị mạng (SNMP). Trong trường hợp này UDP thích hợp hơn TCP vì các tiến trình quản trị mạng thường hoạt động khi mạng có sự cố không thể truyền dữ liệu chính xác hay cơ chế kiểm soát tắc nghẽn không làm việc. DNS sử dụng UDP, do đó có thể tránh được thời gian trễ trong giai đoạn thiết lập kết nối.

Ngày nay UDP thường được các ứng dụng đa phương tiện như điện thoại Internet, hội thảo từ xa, các ứng dụng thời gian thực sử dụng. Các ứng dụng như thế có thể chấp nhận mất mát, lỗi trên một phần dữ liệu, vì thế truyền dữ liệu tin cậy không phải là tiêu chí quan trọng nhất đánh giá sự thành công của ứng dụng. Hơn nữa các ứng dụng thời gian thực không thích ứng được với cơ chế kiểm soát tắc nghẽn của TCP. Do đó chúng thường lựa chọn UDP ở tầng giao vận.

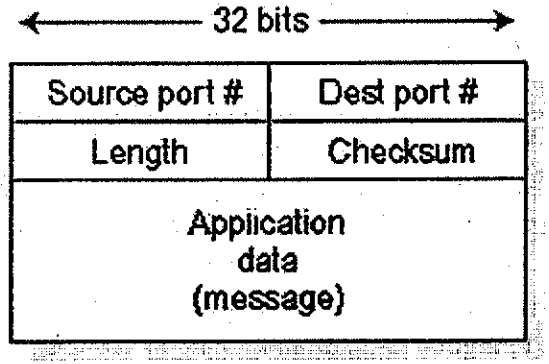
Hiện nay mặc dù đã triển khai trong thực tế, song việc các ứng dụng đa phương tiện sử dụng UDP gây ra nhiều tranh cãi. Như đã nói ở trên, UDP không kiểm soát được tắc nghẽn nên mạng rất dễ bị tắc nghẽn – khi đó chỉ rất ít thông tin được chuyển. Nếu tất cả mọi người đều xem phim trực tuyến thì các gói tin sẽ bị tràn bộ đệm ở các router – và khi đó thì chẳng ai xem được gì cả. Thiếu cơ chế kiểm soát tắc nghẽn có thể sẽ là một vấn đề nghiêm trọng đối với UDP. Người ta đã đưa ra nhiều cơ chế đòi hỏi tất cả các thực thể - kể cả UDP - thực hiện một cơ chế kiểm soát lưu lượng thích nghi.

Trước khi trình bày về cấu trúc UDP, cần chú ý rằng tuy sử dụng UDP nhưng ứng dụng vẫn có thể có một đường truyền tin cậy. Điều này được thực hiện bằng cách đảm bảo tính tin cậy ngay trong bản thân ứng dụng (bằng các cơ chế đánh số thứ tự, truyền lại). Công việc này sẽ làm ứng dụng cồng kềnh và phức tạp. Tuy nhiên ưu điểm là ứng dụng có thể truyền thông tin cậy với tốc độ không bị cơ chế kiểm soát tắc nghẽn của TCP khống chế. Ngày nay một số phần mềm chuyên dụng đa phương tiện sử

dụng cơ chế đánh số thứ tự và truyền lại ngay trong chương trình ứng dụng để giảm bớt việc mất dữ liệu.

### 3.3.1 Cấu trúc UDP segment

Cấu trúc UDP segment, đặc tả trong RFC 768 được minh hoạ trên Hình 3.7. Dữ liệu của ứng dụng nằm trong trường dữ liệu của UDP datagram. Ví dụ đối với DNS, trường dữ liệu chứa thông điệp yêu cầu hay thông điệp trả lời. Tiêu đề UDP có bốn trường, độ lớn mỗi trường là hai byte. Như đã nói ở phần trước, số hiệu cổng cho phép thiết bị gửi chuyển dữ liệu tới đúng tiến trình chạy trên thiết bị nhận (chức năng phân kênh). Trường Checksum được bên nhận sử dụng để kiểm tra trong segment có lỗi hay không. Trên thực tế, kể cả tiêu đề của gói dữ liệu IP cũng được tính checksum. Nguyên tắc cơ bản của cơ chế phát hiện và sửa lỗi được trình bày trong phần 5.1. Trường độ dài (Length) cho biết độ dài (tính theo byte) của toàn bộ gói dữ liệu UDP segment - kể cả phần tiêu đề.




**Hình 3.7 Cấu trúc gói UDP datagram**

### 3.3.2 UDP checksum

UDP checksum được sử dụng để phát hiện lỗi. Checksum được tính như sau: tính giá trị bù một của tổng các từ 16 bit trong segment, giá trị nhận được được đặt vào trường checksum trong gói dữ liệu UDP segment. Có thể



tìm hiểu phương thức triển khai trong RFC 1071 và hiệu quả trên dữ liệu thực trong [Stone 1998 và Stone 2000]. Giả sử có ba từ 16 bit sau đây:

0110011001100110

0101010101010101

0000111100001111

Tổng hai từ đầu là:

0110011001100110

0101010101010101

1011101110111011

Cộng từ thứ ba vào, ta có:

1011101110111011

0000111100001111

1100101011001010

Cách lấy bù một là đảo 0 thành 1 và 1 thành 0. Vì vậy kết quả phép lấy bù một của 1100101011001010 là 0011010100110101 và đó chính là giá trị checksum. Tại phía nhận, tất cả bốn từ (kể cả checksum) được cộng lại. Nếu dữ liệu không có lỗi thì tổng nhận được là 1111111111111111. Nếu có một bit nào đó bằng 0 thì ta biết dữ liệu nhận được có lỗi.

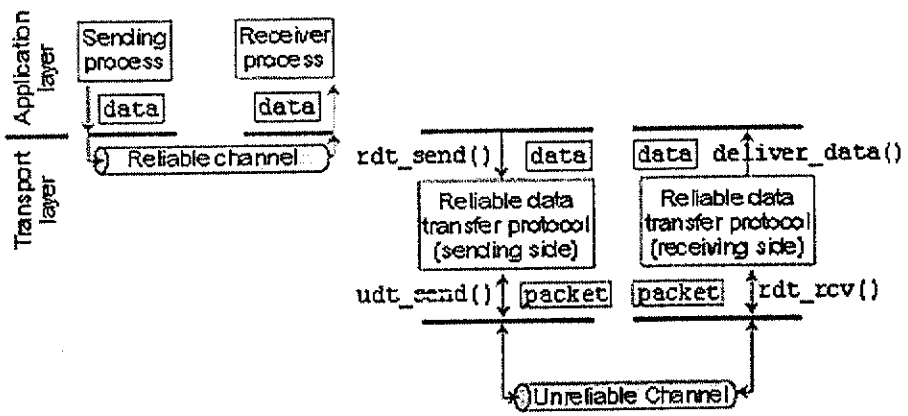
Bạn có thể hỏi tại sao UDP tính checksum – trong khi một vài giao thức tầng liên kết dữ liệu (kể cả giao thức Ethernet thông dụng) cũng có cơ chế kiểm tra lỗi. Lí do là chưa chắc tất cả các kết nối (link - đường truyền vật lý thực sự) giữa thiết bị gửi và thiết bị nhận đều có cơ chế kiểm tra lỗi – có thể một trong các kết nối đó sử dụng giao thức không cung cấp việc kiểm tra lỗi. Mặc dù UDP có thể phát hiện được lỗi nhưng nó không làm gì khi phát hiện ra lỗi. Có thể nó sẽ loại bỏ segment bị lỗi, có thể nó sẽ chuyển segment bị lỗi cho ứng dụng nhận cùng với một thông điệp cảnh báo.

TCP cung cấp đường truyền tin cậy – do đó hiển nhiên triển khai nó phức tạp hơn UDP rất nhiều. Trước khi tìm hiểu về TCP, trong phần sau chúng ta sẽ trình bày nguyên tắc chung để xây dựng một đường truyền tin cậy. TCP sẽ áp dụng đúng những nguyên tắc này khi triển khai.

## 3.4 CÁC NGUYÊN TẮC TRUYỀN DỮ LIỆU TIN CẬY

Phần này trình bày tổng quan dịch vụ truyền dữ liệu tin cậy. Dịch vụ này không chỉ nằm ở tầng giao vận mà còn có thể nằm ở tầng liên kết dữ liệu hay tầng ứng dụng. Có thể nói truyền dữ liệu tin cậy là một trong những vấn đề quan trọng nhất của mạng. Trong phần kế tiếp về TCP, chúng ta sẽ nghiên cứu cách thức TCP áp dụng các nguyên tắc chung được trình bày ở đây như thế nào.

Hình 3.8 là sơ đồ cấu trúc của quá trình truyền dữ liệu tin cậy. Tầng dưới cung cấp dịch vụ truyền tin cậy cho các thực thể ở tầng trên. Trên đường truyền tin cậy này, dữ liệu không bị lỗi (bit 0 biến thành bit 1 hoặc ngược lại), không bị mất và được nhận theo đúng thứ tự gửi. Đây chính là dịch vụ mà TCP cung cấp cho các ứng dụng Internet.




**Hình 3.8 Dịch vụ truyền dữ liệu tin cậy: Mô hình và Triển khai**

Để thực hiện công việc này, người ta cần đến những giao thức truyền dữ liệu tin cậy. Nguyên nhân là tầng phía dưới của giao thức tin cậy là không tin cậy. Ví dụ TCP là giao thức truyền dữ liệu tin cậy nằm ở phía trên giao thức truyền không tin cậy (IP) giữa hai thiết bị đầu cuối trên mạng.



Để đơn giản trong trường hợp này chúng ta coi tầng phía dưới là một đường truyền điểm nối điểm (point-to-point) không tin cậy.

Trong phần này, chúng ta sẽ xây dựng dần giao thức truyền dữ liệu tin cậy giữa phía gửi và phía nhận theo độ phức tạp tăng dần của kênh truyền bên dưới. Hình 3.8b minh hoạ điều này. Thực thể gửi sẽ nhận dữ liệu từ phía trên chuyển xuống qua hàm **rdt_send()** (Ở đây rdt là viết tắt của "reliable data transfer" và **_send** chỉ rõ đây là phía gửi của giao thức rdt. Bước đầu tiên khi xây dựng một giao thức nào đó là chọn cho nó một cái tên dễ nhớ!). Phía nhận sử dụng hàm **rdt_rcv()** để lấy gói dữ liệu từ đường truyền. Để chuyển dữ liệu lên tầng trên, phía nhận sử dụng hàm **deliver_data()**. Trong phần này, chúng ta sử dụng thuật ngữ **"packet"** thay thế "segment" với ý nghĩa là đơn vị dữ liệu giao thức - PDU. Ý tưởng trình bày trong phần này không chỉ áp dụng cho tầng giao vận mà còn áp dụng chung cho toàn mạng máy tính, vì thế sử dụng thuật ngữ **"packet"** thích hợp hơn.

Trong phần này chỉ nghiên cứu trường hợp dữ liệu truyền theo một hướng từ nơi gửi đến nơi nhận. Trường hợp dữ liệu truyền theo hai hướng là một vấn đề không khó về mặt lý thuyết nhưng triển khai cụ thể tương đối phức tạp. Mặc dù dữ liệu chỉ được truyền theo một hướng nhưng các bên truyền thông trong giao thức rdt cần truyền dữ liệu theo cả hai hướng (xem Hình 3.8) bởi vì ngoài các gói dữ liệu thực sự, chúng còn phải trao đổi các gói dữ liệu chứa thông tin điều khiển. Cả bên gửi và bên nhận đều sử dụng hàm **udt_send()** để gửi dữ liệu đến phía bên kia (udt là viết tắt của unreliable data transfer).

### 3.4.1 Xây dựng giao thức truyền dữ liệu tin cậy

Bây giờ chúng ta sẽ từng bước nghiên cứu các giao thức với độ phức tạp tăng dần để cuối cùng đi đến giao thức truyền dữ liệu không lỗi. Chúng ta sẽ mô tả trạng thái của phía nhận và phía gửi bằng kỹ thuật máy hữu hạn trạng thái (**finite state machine – FSM**)

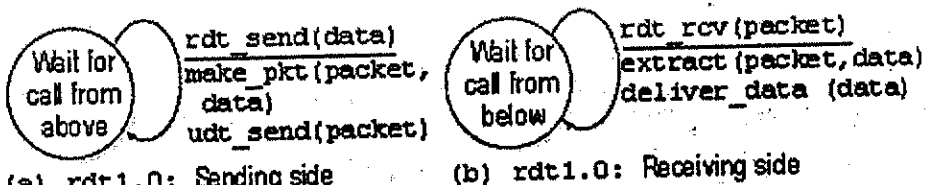
Truyền dữ liệu tin cậy trên kênh truyền tin cậy hoàn toàn: giao thức rdt 1.0.

Giao thức đầu tiên, đơn giản nhất được đưa ra - rdt 1.0 sử dụng kênh truyền tin cậy ở phía dưới. Giao thức rdt 1.0 cực kỳ đơn giản, FSM của bên gửi và bên nhận đều chỉ có một trạng thái (xem Hình 3.9). Mũi tên trong sơ đồ chỉ sự chuyển trạng thái của giao thức (mặc dù mỗi FSM trong Hình 3.9 chỉ có một trạng thái, vẫn cần đến sự chuyển trạng thái để quay về chính trạng thái cũ). Sự kiện kích hoạt việc chuyển trạng thái được đặt phía trên đường kẻ nằm ngang, đó là nhãn sự kiện. Phía bên dưới đường kẻ nằm ngang là những hành động mà thực thể phải thực hiện ngay khi sự kiện đó xảy ra (thực hiện trước khi thực thể chuyển sang trạng thái mới).

Với rdt 1.0, việc gửi đơn giản chỉ là nhận dữ liệu từ tầng trên thông qua sự kiện **rdt_send(data)**, tạo ra gói dữ liệu (bằng hành động **make_data (packet,data)**) và gửi gói dữ liệu (packet) lên kênh truyền. Trên thực tế, sự kiện **rdt_send(data)** là kết quả của một thủ tục (ví dụ khi ứng dụng phía trên sử dụng hàm rdt_send()) .

Ở phía nhận, rdt nhận gói dữ liệu **(packet)** từ kênh truyền bằng sự kiện **rdt_rcv(packet)**, lấy dữ liệu ra khỏi gói dữ liệu (bằng hành động **extract (packet,data)**) và đưa dữ liệu lên tầng trên. Trên thực tế, sự kiện **rdt_rcv(packet)** là kết quả của một thủ tục (ví dụ khi ứng dụng phía trên sử dụng hàm **rdt_rcv()**).

Trong giao thức đơn giản này, không có sự khác biệt giữa dữ liệu **(data)** với gói dữ liệu **(packet)**. Như vậy, tất cả packet đều được truyền từ phía gửi cho phía nhận. Với kênh truyền tin cậy, phía nhận không cần thiết phải phản hồi cho phía gửi vì nó chắc rằng không có chuyện gì xảy ra. Chú ý rằng, chúng ta đã giả thiết phía nhận có thể nhận dữ liệu với tốc độ phía gửi gửi. Vì vậy, phía nhận không cần yêu cầu phía gửi gửi chậm lại.




**Hình 3.9 Giao thức cho kênh truyền tin cậy hoàn toàn**

Truyền dữ liệu tin cậy trên kênh truyền có lỗi bit: giao thức rdt 2.0.



Một dạng kênh truyền thực tế hơn là gói dữ liệu trên kênh truyền có thể bị lỗi. Thường bit bị lỗi trên đường truyền vật lý của mạng. Tuy nhiên, chúng ta giả thiết rằng tất cả các gói dữ liệu truyền đi đều đến được đích và theo đúng thứ tự gửi mặc dù các bit trong gói dữ liệu có thể bị lỗi.

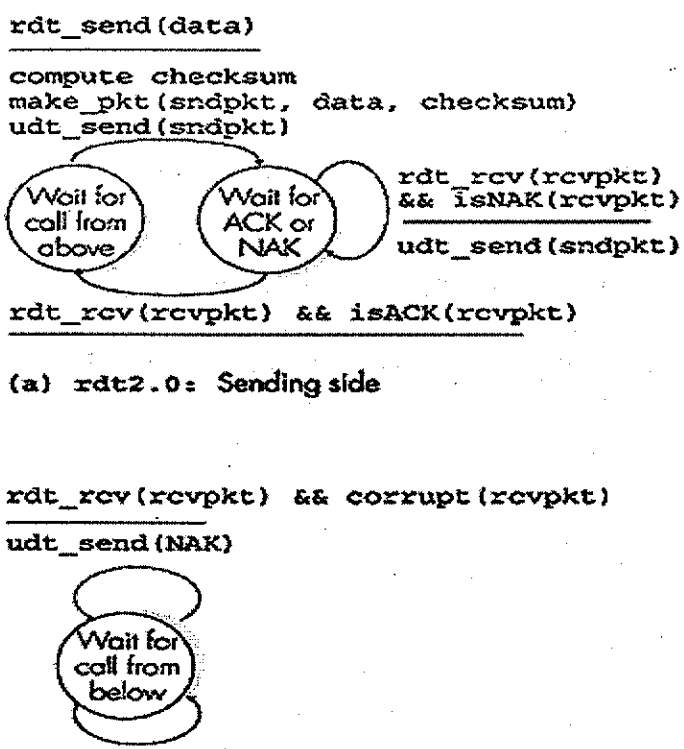
Trước khi tiếp tục, xét ví dụ sau. Giả sử bạn đọc một bài chính tả cho ai đó qua điện thoại. Thông thường, người chép sẽ nói "Xong rồi" sau khi đã nghe, hiểu và ghi lại một câu chính tả. Nếu câu nói của bạn bị nhiễu, người kia nghe không rõ thì họ sẽ yêu cầu bạn nhắc lại. Giao thức truyền tin này sử dụng **phản hồi tích cực** (positive acknowledgement) ("Xong rồi") **hay phản hồi tiêu cực** (negative acknowledgement) ( "Gì cơ ?"). Những thông điệp điều khiển này cho phép bên nhận báo cho bên gửi biết dữ liệu nào nhận đúng, dữ liệu nào bị lỗi và yêu cầu truyền lại dữ liệu bị lỗi. Trong mạng máy tính, giao thức truyền tin cậy dựa trên cơ chế truyền lại như vậy được gọi là các giao thức **ARQ (Automatic Repeat reQuest)**.

Các giao thức ARQ cần phải có ba khả năng sau để xử lý trong trường hợp dữ liệu có lỗi:

***Phát hiện lỗi (error detection)***: là cơ chế cho phép bên nhận phát hiện được khi nào trong gói dữ liệu có bit bị lỗi. Trong phần trước, ta thấy UDP sử dụng trường Internet checksum cho mục đích này. Trong chương V, chúng ta sẽ xem xét chi tiết một số kỹ thuật phát hiện và thậm chí có thể sửa được lỗi. Còn bây giờ chúng ta chỉ cần biết rằng những kỹ thuật như vậy yêu cầu ngoài việc gửi dữ liệu gốc, bên gửi còn phải tạo ra và gửi kèm một lượng dữ liệu dư thừa (nhưng phụ thuộc vào dữ liệu gốc). Các bit dư thừa này được đặt trong trường checksum của gói dữ liệu rdt 2.0.

***Phản hồi từ phía nhận (receiver feedback):*** Khi phía gửi và phía nhận nằm trên các thiết bị đầu cuối khác nhau - có thể cách nhau hàng nghìn km, cách duy nhất để phía gửi biết được kết quả gửi là phía nhận gửi thông tin phản hồi thông báo tình trạng nhận cho phía gửi. Báo nhận đúng (đôi khi gọi là báo nhận tích cực) ACK và báo nhận sai NAK trong ví dụ trên chính là các thông tin phản hồi. Giao thức rdt 2.0 yêu cầu phía nhận gửi phản hồi các thông điệp ACK hay NAK cho phía gửi. Gói dữ liệu phản hồi chỉ cần sử dụng một bit, ví dụ giá trị 0 ứng với NAK và giá trị 1 ứng với ACK.

*Truyền lại (retransmission)*: gói dữ liệu bị lỗi sẽ được bên gửi truyền lại.




**Hình 3.10 Giao thức cho kênh truyền có lỗi bit**

Hình 3.10 là FSM của phía gửi và nhận trong giao thức rdt 2.0 với cơ chế phát hiện lỗi, phản hồi (ACK, NAK) và truyền lại.

Trong giao thức rdt 2.0, phía gửi có hai trạng thái. Ở trạng thái thứ nhất, phía gửi đợi dữ liệu từ tầng trên. Trong trạng thái thứ hai, phía gửi đợi phản hồi ACK hoặc NAK từ phía nhận. Nếu nhận được ACK (rdt_rcv(rcvpkt ) & isACK(rcvpkt) trong Hình 3.10 tương ứng với sự kiện này), phía gửi biết được gói dữ liệu chuyển đến đích an toàn, vì vậy nó trở về trạng thái đợi dữ liệu từ tầng trên để chuyển tiếp. Nếu nhận được NAK,



phía gửi gửi lại gói dữ liệu rồi quay lại trạng thái đợi phản hồi ACK hoặc NAK cho gói dữ liệu vừa gửi lại. Chú ý rằng khi phía gửi ở trong trạng thái chờ phản hồi (ACK hoặc NAK), nó không thể nhận thêm dữ liệu từ tầng trên đưa xuống. Nó chỉ chấp nhận dữ liệu mới khi nhận được ACK và chuyển trạng thái. Phía gửi sẽ không gửi dữ liệu mới cho đến khi nó chắc chắn rằng phía nhận đã nhận đúng gói dữ liệu đã gửi. Giao thức rdt 2.0 với hành vi như vậy thuộc kiểu **dừng và chờ (stop and wait)**.

FSM bên nhận trong giao thức rdt 2.0 chỉ có một trạng thái duy nhất. Khi nhận được gói dữ liệu (packet), phía nhận gửi thông điệp phản hồi ACK hoặc NAK, phụ thuộc vào gói dữ liệu đã nhận có lỗi hay không. Trong Hình 3.10, rdt_rcv (rcvpkt) && corrups(rcvpkt) tương ứng với sự kiện gói dữ liệu nhận được bị lỗi.

Giao thức rdt 2.0 vẫn còn nhược điểm: chúng ta chưa tính đến khả năng chính gói ACK hoặc NAK có lỗi. (Trước khi tiếp tục bạn hãy thử nghĩ cách cải tiến giao thức này). Chúng ta cần tạo checksum cho chính gói phản hồi (ACK hoặc NAK) để bên gửi (lúc này đóng vai trò bên nhận) có khả năng phát hiện lỗi trong chính gói phản hồi. Vấn đề ở đây là khi nhận được một gói phản hồi bị lỗi – phía gửi không thể xác định nó là ACK nay NAK, do đó không xác định được gói dữ liệu nó gửi tới đích có bị lỗi hay không. Trong trường hợp này, bên gửi sẽ phải làm gì ?

Có ba giải pháp xử lý ACK hoặc NAK bị lỗi:

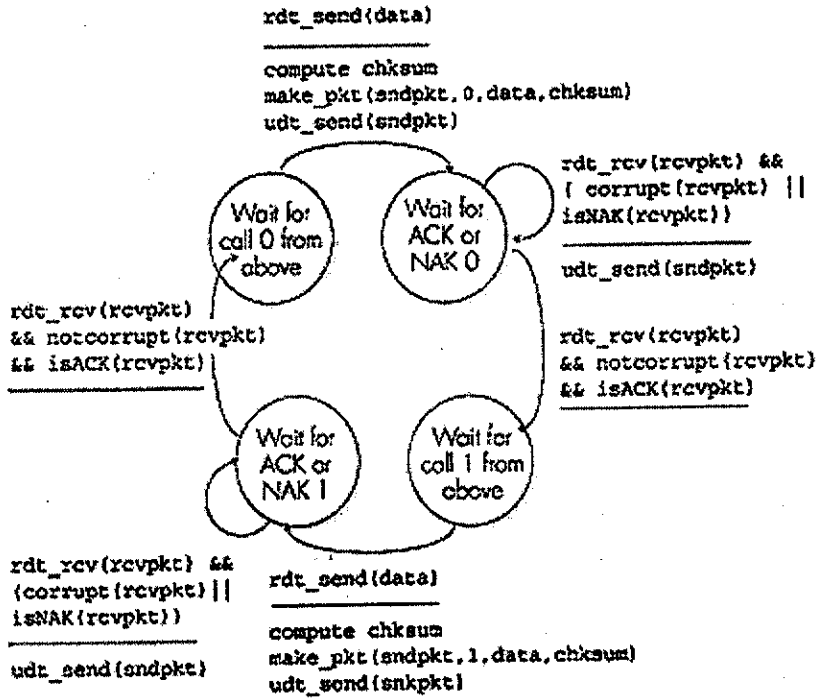
Giải pháp thứ nhất, người đọc trong ví dụ đọc chính tả lúc nãy sẽ làm gì trong trường hợp này? Nếu không hiểu câu phản hồi "Xong rồi" hay "Gì cơ" thì họ có thể hỏi "Bạn nói gì?" (một dạng thông điệp điều khiển khác). Nếu nghe được, người bên kia sẽ lặp lại câu phản hồi. Nhưng chuyện gì xảy ra nếu chính câu "Bạn nói gì?" có lỗi? Khi đó phía nhận - do không xác định được câu có lỗi đó là một phần trong bài chính tả hay là yêu cầu nhắc lại câu phản hồi - nên có thể phản hồi lại bằng câu "Bạn nói gì?". Dĩ nhiên, câu trả lời này cũng có thể bị lỗi. Rõ ràng giải pháp này đã đi vào ngõ cụt.

Giải pháp thứ hai là thêm vào trường checksum một số bit để không những cho phép phía nhận phát hiện mà còn sửa được các bit lỗi. Đây hoàn toàn có thể là giải pháp trung gian cho những kênh truyền có lỗi – nhưng không xử lý được trường hợp toàn bộ gói dữ liệu (packet) bị mất.

Giải pháp thứ ba, phía gửi truyền lại gói dữ liệu nếu phát hiện lỗi trong gói phản hồi (ACK hoặc NAK). Tuy nhiên, phương pháp này có thể

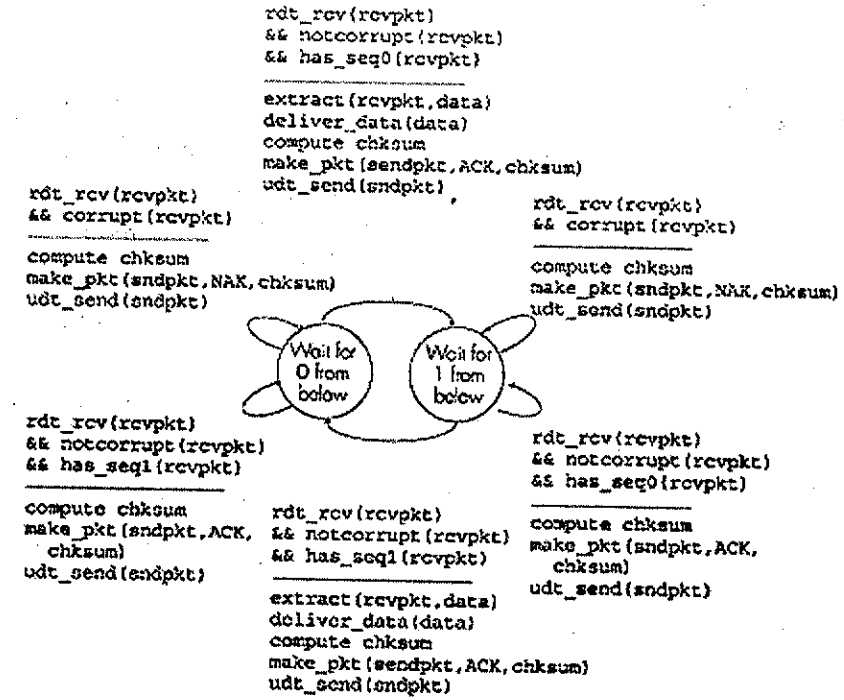
dẫn đến **sự trùng lặp dữ liệu (duplicate packet)**. Phía nhận không biết được ACK/NAK mà nó gửi phản hồi có bị lỗi trên đường truyền không. Vì thế nó không xác định được gói dữ liệu vừa nhận được là gói dữ liệu mới hay gói cũ (sẽ bị trùng lặp).

Giải pháp đơn giản nhất cho vấn đề này (sẽ được áp dụng cho nhiều giao thức, kể cả TCP) là thêm trường số thứ tự cho gói dữ liệu (packet), phía gửi đánh số thứ tự các gói dữ liệu và đặt giá trị này vào trường số thứ tự (sequence number). Phía nhận chỉ cần kiểm tra số thứ tự để xác định gói dữ liệu nhận được là gói mới hay gói truyền lại. Với giao thức **stop and wait** đơn giản, chỉ cần một bit số thứ tự. Bên nhận có thể xác định bên gửi truyền lại gói dữ liệu đã gửi lần trước (số thứ tự của gói dữ liệu nhận được trùng với số thứ tự với gói dữ liệu nhận được lần trước) hay gói dữ liệu mới (có số thứ tự khác nhau, tăng lên theo module 2). Vì chúng ta vẫn giả định toàn bộ gói dữ liệu (packet) không bị mất trên kênh truyền, nên trong gói phản hồi (ACK/NAK) không cần chỉ ra số thứ tự của gói dữ liệu mà chúng biên nhận. Phía gửi biết rằng gói ACK/NAK (có thể bị lỗi hoặc không) là biên nhận cho gói dữ liệu gần nhất nó gửi.




Hình 3.11 FSM của phía gửi trong rdt 2.1

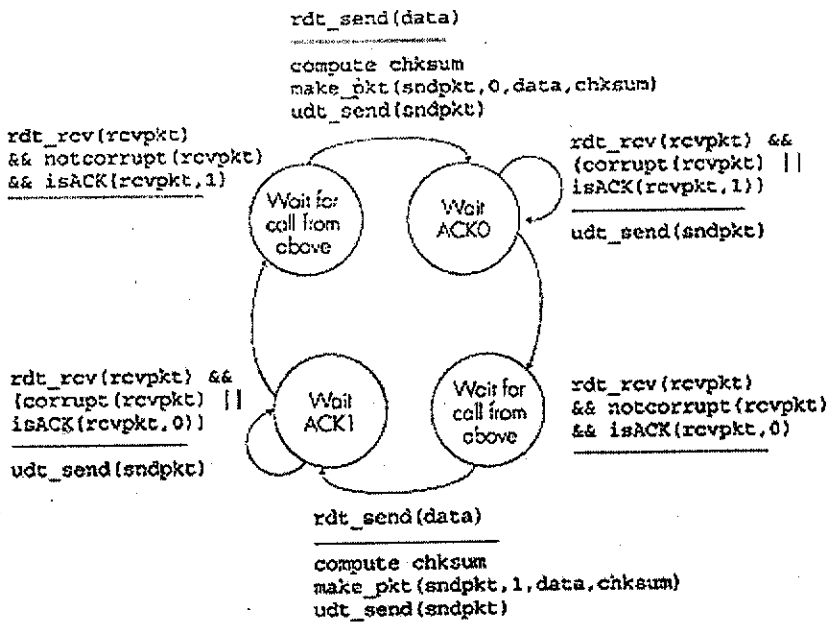




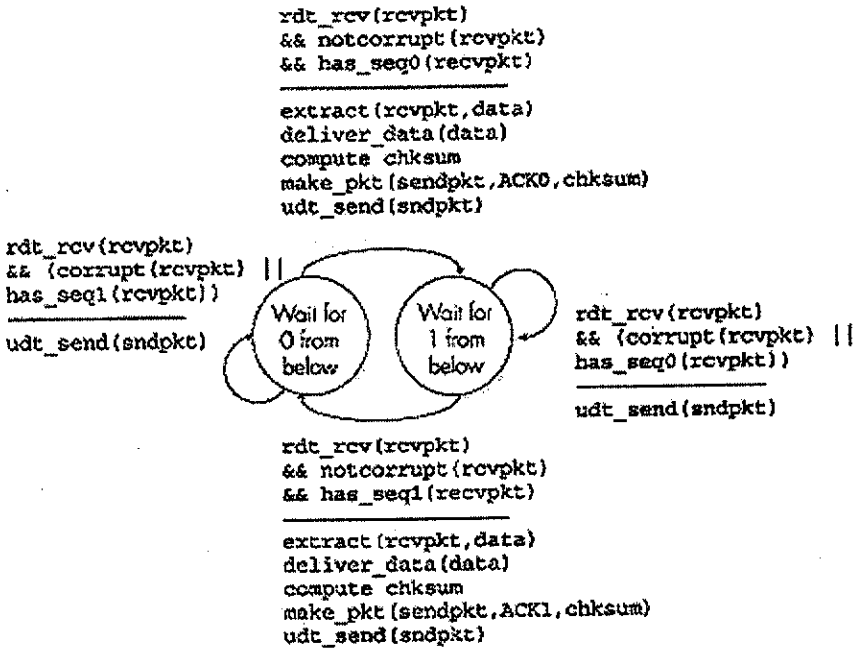

Hình 3.12 FSM của phía nhận trong rdt 2.1

Hình 3.11 và Hình 3.12 là FSM của bên gửi và nhận trong giao thức rdt 2.1 – phiên bản mới của rdt 2.0. Trong rdt 2.1, FSM của bên gửi và nhận đều có số trạng thái tăng gấp đôi. Đó là vì trạng thái giao thức phải biểu diễn gói dữ liệu được gửi (bởi bên gửi) và gói dữ liệu được đợi (tại bên nhận) có số thứ tự là 0 hay 1. Chú ý rằng các hành động trong trạng thái gói dữ liệu có số thứ tự 0 được gửi (phía gửi) hoặc được mong đợi (phía nhận) ngược với trạng thái gói dữ liệu có số thứ tự 1 được gửi hay được đợi.

Giao thức rdt 2.1 sử dụng cả biên nhận đúng (ACK) và biên nhận sai (NAK). NAK được gửi khi nhận được gói dữ liệu bị lỗi hay không đúng số thứ tự. Chúng ta có thể không cần sử dụng NAK: thay vì việc gửi NAK, chúng ta gửi ACK cho gói dữ liệu cuối cùng đã được nhận đúng. Nếu nhận hai ACK cho cùng một gói dữ liệu (hiện tượng **trùng ACK – duplicate ACK**) bên gửi xác định được bên nhận không nhận đúng gói dữ liệu sau gói dữ liệu đã biên nhận ACK hai lần. TCP sử dụng sự kiện "3 lần nhận được ACK trùng nhau" ("triple duplicate ACKs") để kích hoạt việc gửi lại. rdt 2.2 là giao thức truyền dữ liệu tin cậy trên kênh truyền có bit lỗi không sử dụng NAK, minh hoạ trên Hình 3.13 và Hình 3.14.




Hình 3.13 FSM của phía gửi trong rdt 2.2




Hình 3.14 FSM của phía nhận trong rdt 2.1



## *Truyền dữ liệu tin cậy trên kênh truyền mà dữ liệu bị mất, lỗi: rdt 3.0.*

Dữ liệu trên kênh truyền không những bị lỗi mà còn có thể bị mất, đây là tình huống khá phổ biến trong mạng máy tính ngày nay, kể cả Internet. Lúc này giao thức cần phải giải quyết hai vấn đề: làm thế nào để phát hiện gói dữ liệu bị mất và làm gì khi mất gói dữ liệu. Sử dụng cơ chế phát hiện lỗi nhờ checksum, số thứ tự, biên nhận ACK và truyền lại gói dữ liệu - đã được phát triển trong giao thức rdt 2.2 - cho phép chúng ta giải quyết được vấn đề thứ hai. Để giải quyết vấn đề thứ nhất, chúng ta cần một cơ chế mới.

Có nhiều giải pháp xử lý việc mất mát dữ liệu. Ở đây chúng ta trình bày giải pháp lựa chọn bên gửi là nơi phát hiện và xử lý việc mất dữ liệu. Giả sử phía gửi gửi đi gói dữ liệu nhưng chính gói dữ liệu đó hoặc biên nhận ACK cho nó bị mất trên đường truyền. Trong cả hai trường hợp, bên gửi đều không nhận được biên nhận cho gói dữ liệu đã gửi. Giải pháp được đưa ra là sau khi gửi một khoảng thời gian nào đó mà không nhận được biên nhận ACK (có thể gói dữ liệu bị mất) thì bên gửi sẽ truyền lại.

Nhưng phía gửi phải đợi trong bao lâu để chắc chắn rằng gói dữ liệu đã bị mất? Ít nhất phía gửi phải đợi trong khoảng thời gian để gói tin đi đến được phía nhận, phía nhận xử lý gói tin và thông tin biên nhận quay lại. Trong nhiều mạng, rất khó dự đoán và ước lược thời gian này. Lý tưởng là phải xử lý việc mất gói tin ngay khi có thể, đợi một khoảng thời gian dài đồng nghĩa với việc chậm trễ khi xử lý gói tin bị mất. Trên thực tế, phía gửi sẽ chọn một khoảng thời gian đợi nào đó, mặc dù không đảm bảo chắc chắn là gói tin có bị mất hay không. Nếu không nhận được ACK trong khoảng thời gian này, bên gửi sẽ gửi lại gói dữ liệu. Chú ý rằng, nếu gói dữ liệu đến trễ, phía gửi sẽ gửi lại gói dữ liệu - ngay cả khi gói dữ liệu đó và cả ACK đều không bị mất. Điều này gây ra trùng lặp dữ liệu tại phía nhận. Tuy nhiên, giao thức rdt 2.2 đã có đủ khả năng (nhờ số thứ tự) để ngăn chặn sự trùng lặp dữ liệu.

Đối với phía gửi, truyền lại là giải pháp "vạn năng". Phía gửi không xác định được gói dữ liệu bị mất, gói biên nhận ACK bị mất hay chỉ đơn giản là chúng bị trễ. Trong mọi trường hợp, hành động của nó là giống nhau:

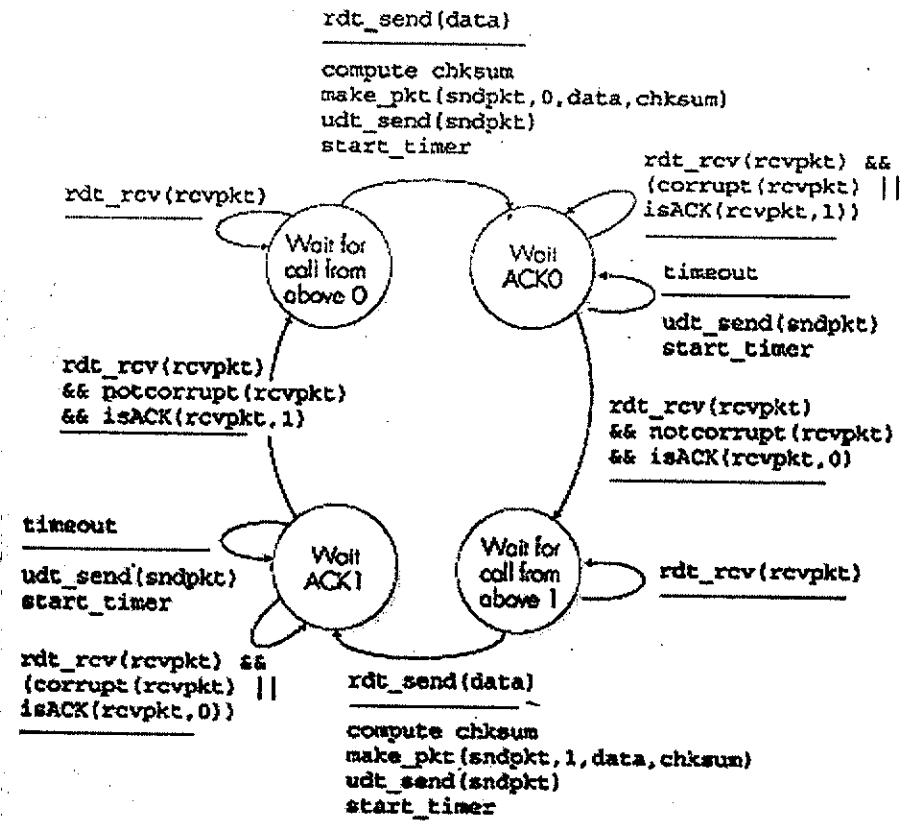
truyền lại. Để thực hiện cơ chế truyền lại theo thời gian, một bộ định thời đếm ngược (countdown timer) được sử dụng để nhắc phía gửi thời gian đợi đã hết. Do vậy, phía gửi phải có khả năng (1) khởi tạo timer mỗi khi gửi gói dữ liệu (gói dữ liệu gửi lần đầu hay gói dữ liệu được truyền lại), (2) phản ứng với ngắt của timer (đưa ra những hành động thích hợp) và (3) dừng timer.

Sự trùng lặp các gói dữ liệu do phía gửi tạo ra, sự mất mát các gói dữ liệu (cả gói dữ liệu lẫn gói biên nhận) gây khó khăn cho phía gửi khi xử lý các gói biên nhận ACK. Nếu nhận được ACK, làm thế nào để phía gửi biết được ACK đó là biên nhận cho gói dữ liệu gửi đi gần đây nhất, hay là ACK biên nhận cho gói dữ liệu nào đó đã gửi từ trước nhưng đến trễ? Giải pháp là ta thêm vào gói ACK trường **số thứ tự biên nhận (acknowledge number)**. Giá trị của trường này – do phía nhận tạo ra - là số thứ tự của chính gói dữ liệu cần được biên nhận. Bằng cách kiểm tra giá trị trường biên nhận, phía gửi có thể xác định được số thứ tự của gói dữ liệu được biên nhận.

Hình 3.15 là FSM của bên gửi trong giao thức rdt 3.0 – giao thức truyền dữ liệu trên kênh truyền có thể có lỗi hoặc bị mất dữ liệu. Hình 3.16 minh họa sự vận hành của giao thức trong một số trường hợp. Thời gian dịch chuyển theo chiều từ trên xuống. Thời điểm nhận gói dữ liệu chậm hơn thời điểm gửi gói dữ liệu vì tính đến thời gian gói dữ liệu lan tỏa trên đường truyền. Trong Hình 3.16b-d, ngoặc vuông xác định thời điểm timer được thiết lập và thời điểm "timeout". Vì số thứ tự của gói dữ liệu thay đổi lần lượt giữa 0 và 1 nên đôi khi giao thức rdt 3.0 được gọi là giao thức một bit luân chuyển (alternate bit protocol).

Chúng ta đã điểm qua các thành phần chính cho một giao thức truyền số liệu. Checksum, số thứ tự phát, bộ định thời (timer), các gói biên nhận ACK và NAK đều cực kỳ cần thiết và đóng vai trò quan trọng trong quá trình hoạt động của giao thức. Đến bây giờ chúng ta đã có một giao thức truyền dữ liệu tin cậy thực sự hoạt động được.

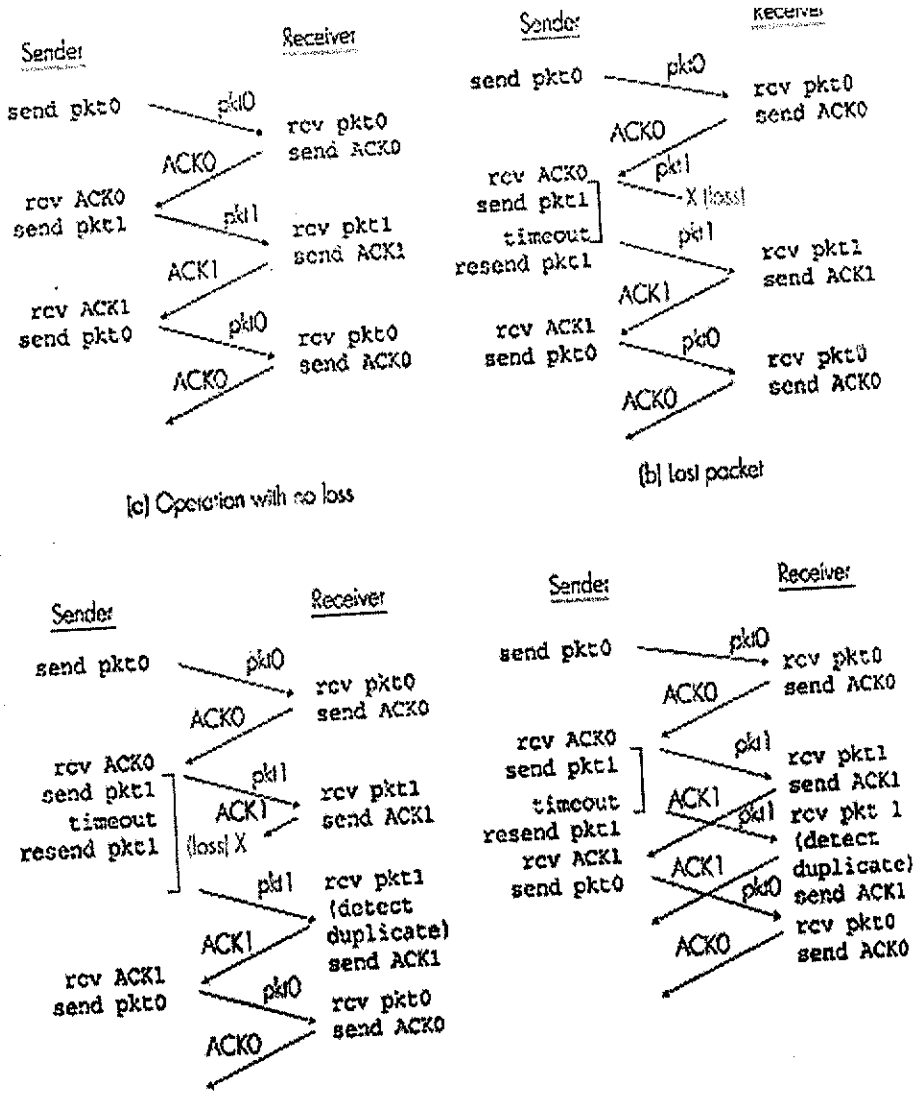





**Hình 3.15 FSM của bên gửi trong rdt 3.0**

## 3.4.2 Giao thức truyền dữ liệu tin cậy liên tục (Pipeline)

Mặc dù hoạt động đúng nhưng không phải ai cũng vừa lòng với hiệu suất của rdt3.0, đặc biệt trong các mạng cao tốc ngày nay. Cốt lõi vấn đề hiệu suất của giao thức rdt 3.0 chính là hành vi dừng và chờ (stop and wait). Nguyên tắc của giao thức kiểu "Dừng và Chờ" như sau: sau khi phát một gói dữ liệu, thiết bị phát dừng phát (stop) để chờ nhận phản hồi từ thiết bị nhận về kết quả nhận số liệu (wait). Nếu kết quả nhận tốt (biên nhận ACK), bên phát được quyền phát tiếp. Nếu kết quả nhận sai (biên nhận NAK), bên phát phải gửi lại gói dữ liệu.




**Hình 3.16 Ví dụ hoạt động của giao thức rdt 3.0**

Để ước lượng hiệu suất của giao thức **stop and wait**, xét trường hợp lý tưởng với hai thiết bị đầu cuối, một ở bờ biển phía đông, một ở bờ biển phía tây nước Mỹ. Thời gian trễ giữa hai thiết bị (dù tín hiệu lan truyền với tốc độ ánh sáng) là $P_{prop}$ xấp xỉ 15 ms. Giả sử rằng hai thiết bị được kết nối bằng đường truyền tốc độ C (1 gigabit/s). Kích thước của gói dữ liệu SP là

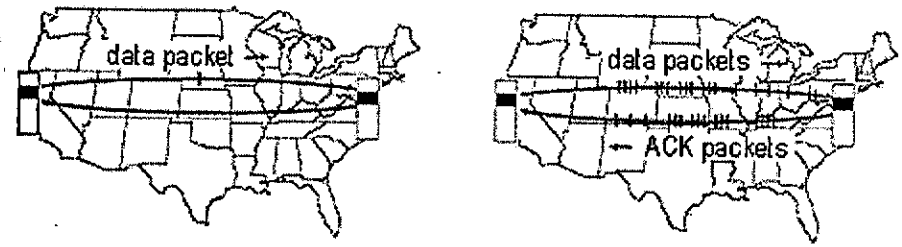


1Kbyte/packet, thời gian cần thiết để truyền toàn bộ gói dữ liệu trên kênh truyền tốc độ 1 Gbps được tính bởi công thức:

$$T_{trans} = \frac{SP}{C} = \frac{8Kbit/packet}{1Mbit/sec} = 8\ ms$$

Với giao thức **stop and wait**, nếu phía gửi bắt đầu gửi gói dữ liệu tại thời điểm t = 0 thì tại thời điểm t = 8 microsecond, bit cuối cùng mới được bên gửi đẩy ra đường truyền. Tiếp theo phải mất 15 ms để cả gói dữ liệu đi từ phía gửi sang phía nhận (xem Hình 3.17a) như vậy bit cuối cùng của gói dữ liệu đến đích tại thời điểm t = 15.008ms. Để đơn giản, ta giả thiết gói ACK có cùng độ dài với gói dữ liệu và phía nhận gửi ngay gói ACK khi nhận được bit cuối cùng của gói dữ liệu. Như vậy bit cuối cùng của gói ACK được truyền tới đích tại thời điểm t = 30.016 ms. Trong khoảng thời gian 30.016ms, phía gửi chỉ hoạt động (gửi hoặc nhận) trong 0.016 ms. Nếu định nghĩa **Hiệu suất (utilization)** của phía gửi (hay kênh truyền) là tỷ lệ thời gian phía gửi hoạt động (gửi dữ liệu trên kênh truyền), chúng ta có hiệu suất $U_{sender}$ cực thấp:

$$U_{sender} = \frac{.008}{30.016} = 0.00015$$




(a) A stop-and-wait protocol in operation (b) A pipelined protocol in operation

**Hình 3.17**

Điều đó có nghĩa là phía gửi chỉ hoạt động trong khoảng 0.15 phần trăm thời gian. Theo cách tính khác, phía gửi gửi 1 Kbyte trong 30,016 millisecond tương đương với tốc độ truyền là 33 Kbyte/s thấp hơn nhiều so với tốc độ có thể là 1 Gigabit/s. Người quản trị mạng "bất hạnh" này phải trả một số tiền khổng lồ để thuê đường truyền 1 Gigabit/s nhưng cuối cùng chỉ nhận được một đường truyền có tốc độ 33 Kbyte/s. Đây là một ví dụ sống động minh hoạ việc phần mềm có thể giới hạn các khả năng của phần cứng bên dưới. Trong trường hợp này chúng ta đã bỏ qua thời gian xử lý của các

giao thức tầng dưới ở cả phía gửi và phía nhận cũng như thời gian xử lý và thời gian trễ của gói tin tại các router trung gian. Nếu tính cả những yếu tố này, hiệu suất hoạt động thực sự sẽ còn thấp hơn nữa.

Giải pháp cho vấn đề hiệu suất sẽ là cho phép phía gửi gửi đồng thời nhiều gói dữ liệu mà không cần phải đợi ACK (xem Hình 3.17b). Có thể hình dung các gói dữ liệu nối tiếp nhau trên đường truyền từ phía gửi đến phía nhận giống như nước chảy trong một đường ống. Vì thế kỹ thuật gửi liên tiếp này được gọi là **kỹ thuật đường ống (pipeline)**. Kỹ thuật nầy làm tăng hiệu suất của giao thức lên nhiều lần, tuy nhiên nó đòi hỏi những yêu cầu sau:

Khoảng số thứ tự phải tăng, bởi vì mỗi gói dữ liệu được truyền đi (không tính các gói dữ liệu truyền lại) phải có một số thứ tự duy nhất. Trên đường truyền có thể có đồng thời nhiều gói dữ liệu đã gửi nhưng chưa được biên nhận.

Phía gửi và phía nhận có thể phải có bộ đệm (buffer) cho nhiều gói dữ liệu. Ít nhất phía gửi có vùng đệm cho các gói dữ liệu đã được truyền đi nhưng chưa được biên nhận. Phía nhận cũng có thể cần vùng đệm cho cả các gói dữ liệu đã nhận đúng, như sẽ trình bày dưới đây.

Yêu cầu về khoảng số thứ tự cần thiết cũng như về vùng đệm phụ thuộc vào cách giao thức xử lý việc mất dữ liệu, dữ liệu bị lỗi, bị trễ. Có hai cách tiếp cận chính được trình bày ở đây: **Quay lại N (Go-back-N)** và **Lặp lại có lựa chọn (SelectiveRepeat)**.

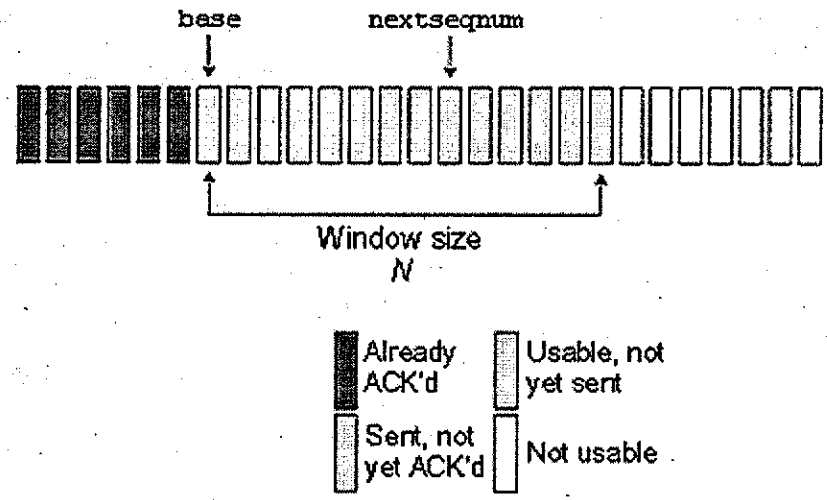
## 3.4.3 Go-back-N (GBN)

Trong giao thức **Go-back-N**, phía gửi được phép truyền đi đồng thời nhiều gói dữ liệu mà không phải đợi biên nhận. Tuy nhiên tổng số gói dữ liệu bị giới hạn bởi giá trị N - tổng số gói dữ liệu tối đa chưa được biên nhận trong đường ống. Hình 3.18 là khoảng số thứ tự trong giao thức **Go-back-N**. Định nghĩa **base** là số thứ tự của gói dữ liệu đã được truyền đi lâu nhất chưa được biên nhận và **nextseqnum** là số thứ tự nhỏ nhất chưa được sử dụng (là số thứ tự của gói tiếp theo sẽ gửi). Có bốn khoảng số thứ tự như sau: Khoảng [0,base-1] ứng với số thứ tự của các gói dữ liệu đã được truyền đi



và đã được biên nhận. Khoảng [base, nextseqnum-1] ứng với các gói dữ liệu đã được gửi đi nhưng chưa được biên nhận. Khoảng [nextseqnum, base +N-1] có thể được sử dụng làm số thứ tự cho các gói sẽ được gửi nếu như có dữ liệu từ tầng trên chuyển xuống. Khoảng từ [base+N] trở lên chưa được sử dụng cho đến khi các gói tin đợi biên nhận được biên nhận.

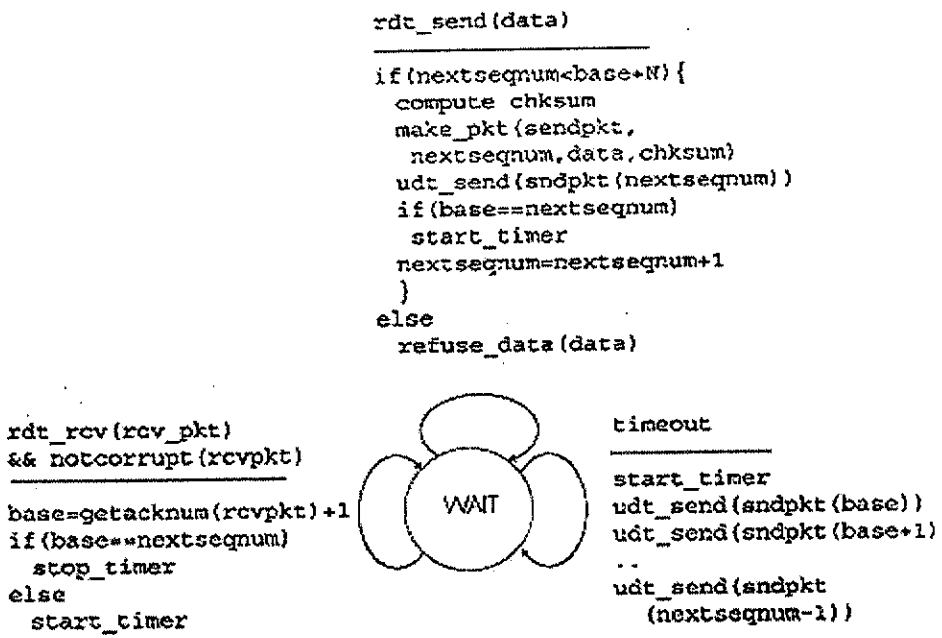
Trong Hình 3.18, khoảng số thứ tự cho phép của những gói dữ liệu đã được gửi nhưng chưa được biên nhận có thể xem là một "cửa sổ" kích thước N nằm trong phạm vi số thứ tự. Khi giao thức vận hành, cửa sổ này có thể "trượt" trên toàn bộ khoảng số thứ tự. Vì vậy, N thường được xem là **độ lớn cửa sổ (window size)** và giao thức GBN là giao thức **cửa sổ trượt (sliding-window)**. Tại sao ngay từ đầu chúng ta phải giới hạn số lượng tối đa các gói dữ liệu được gửi mà chưa cần biên nhận bởi giá trị N. Tại sao không để giá trị N này là vô hạn. Chúng ta sẽ thấy trong phần 3.5, kiểm soát lưu lượng là một trong những lý do bắt buộc ta phải đặt giới hạn phía gửi.



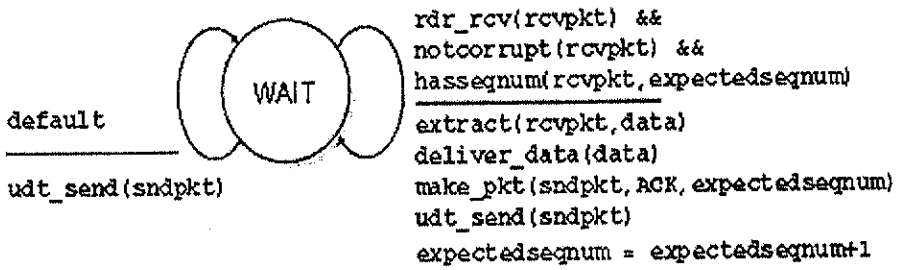

**Hình 3.18 Khoảng số thứ tự của bên gửi trong giao thức Go-Back-N**

Trên thực tế, số thứ tự được đặt trong một trường có độ dài cố định trong tiêu đề của gói dữ liệu Nếu k là độ lớn trường số thứ tự (tính theo bit) của gói dữ liệu thì khoảng số thứ tự sẽ là $[0,2^k-1]$. Vì khoảng số thứ tự bị giới hạn, nên tất cả các thao tác trên số thứ tự sẽ được thực hiện theo module $2^k$ (khoảng số thứ tự có thể xem là một vòng tròn với $2^k$ giá trị, sau giá trị $2^k$-1 là giá trị 0). Giao thức rdt 3.0 chỉ sử dụng 1 bit làm số thứ tự nên khoảng số

thứ tự là [0,1]. Trong phần 3.5 chúng ta sẽ thấy trường số thứ tự của TCP là 32 bit, và TCP đánh số thứ tự đến từng byte - chứ không phải cho các gói.




**Hình 3.19 FSM mở rộng của bên gửi trong GBN**




**Hình 3.20 FSM mở rộng của bên nhận trong GBN**

Hình 3.19 và Hình 3.20 là FSM mở rộng của phía gửi và phía nhận trong giao thức GBN chỉ sử dụng ACK, không sử dụng NAK. Gọi là **FSM mở rộng (extended FSM)** vì chúng ta thêm vào các biến (base và nextseqnum - giống như biến trong ngôn ngữ lập trình), các lệnh và hành động có điều kiện liên quan đến các biến này.

Trong giao thức GBN, phía gửi phải đáp ứng ba sự kiện sau:



*Có dữ liệu từ trên chuyển xuống*: khi rdt_send() được phía trên sử dụng để chuyển dữ liệu xuống, phía gửi phải kiểm tra xem cửa sổ đã đầy chưa (tức là đã có N gói dữ liệu gửi đi chưa được biên nhận không). Nếu cửa sổ chưa đầy, phía gửi tạo ra và sau đó gửi gói dữ liệu đồng thời cập nhật các biến. Nếu cửa sổ đầy, phía gửi không chấp nhận dữ liệu từ tầng trên và thông báo cửa sổ đã đầy. Khi đó, tầng trên sẽ phải gửi lại. Trên thực tế, phía gửi sẽ đưa dữ liệu vào vùng đệm (nhưng chưa gửi ngay) hoặc có cơ chế đồng bộ (sử dụng semaphore hay cờ) chỉ cho phép tầng ứng dụng sử dụng rdt_send() khi cửa sổ chưa đầy.

*Nhận được một ACK*: trong giao thức GBN, giá trị biên nhận mang tính tích lũy, nghĩa là nếu biên nhận gói tin có số thứ tự n thì toàn bộ gói dữ liệu có số thứ tự nhỏ hơn hoặc bằng n đều đã được phía nhận nhận đúng. Chúng ta sẽ quay lại vấn đề này khi xem xét phía nhận trong giao thức GBN.

*Hết thời gian đợi (timeout)*: tên giao thức - "Go-Back-N" bắt nguồn từ hành vi của phía gửi khi dữ liệu bị mất hay bị trễ. Giống như trong giao thức stop and wait, timer được sử dụng để xử lý việc mất gói dữ liệu hay gói phản hồi. Khi hết thời gian đợi (timeout), phía gửi sẽ gửi lại tất cả các gói dữ liệu đã được gửi đi trước đó nhưng chưa được biên nhận. Trong Hình 3.19, phía gửi chỉ sử dụng duy nhất một timer, có thể xem là timer của gói dữ liệu đã được truyền đi lâu nhất nhưng chưa được biên nhận. Nếu ACK nào đó được nhận nhưng vẫn còn gói dữ liệu gửi đi chưa được biên nhận thì timer sẽ được khởi động lại. Nếu tất cả các gói dữ liệu đã gửi đều được biên nhận thì có thể ngừng timer.

Các hành động của phía nhận trong giao thức GBN đơn giản. Nếu nhận được đúng gói dữ liệu và gói này đúng thứ tự thì phía nhận gửi ACK cho gói nhận được và chuyển dữ liệu trong gói dữ liệu này lên trên. Trong tất cả các trường hợp còn lại, phía nhận loại bỏ gói dữ liệu và gửi lại ACK cho gói dữ liệu đúng thứ tự cuối cùng nó nhận được. Chú ý rằng gói dữ liệu được chuyển lên tầng trên một lần duy nhất nên nếu gói dữ liệu thứ k được nhận và chuyển lên trên thì nghĩa là tất cả các gói dữ liệu có số thứ tự nhỏ hơn k cũng đã được chuyển lên. Sử dụng ACK tích lũy là sự lựa chọn tuyệt vời cho giao thức GBN.

Trong giao thức GBN, bên nhận loại bỏ gói tin không theo thứ tự. Dường như lãng phí khi loại bỏ gói tin đã nhận đúng nhưng không đúng thứ tự, nhưng có vài nguyên nhân cho hành vi trên. Bên nhận phải chuyển dữ liệu lên tầng trên theo đúng thứ tự. Giả sử gói tin N đang được đợi nhận nhưng gói tin thứ (N+1) lại đến trước. Trong trường hợp ấy, để dữ liệu chuyển lên hợp lệ, bên nhận có thể lưu tạm gói tin (N+1) và chỉ chuyển gói tin này lên tầng trên sau khi đã nhận đúng gói tin thứ N. Tuy nhiên theo quy tắc truyền lại của bên gửi, nếu gói tin thứ N bị mất thì gói tin này và cả gói tin N+1 sẽ được truyền lại. Như vậy, bên nhận có thể loại bỏ gói tin N+1. Ưu điểm của giải pháp này là bên nhận triển khai vùng đệm (buffer) đơn giản bởi không cần lưu lại các gói tin không đúng thứ tự. Nếu bên gửi phải ghi nhớ các cận của cửa sổ (base, base+N) và vị trí **nextseqnum** trong cửa sổ, thì bên nhận chỉ phải nhớ số thứ tự của gói tin hợp lệ tiếp theo. Giá trị này được giữ trong biến **expectedseqnum** (số thứ tự được mong đợi) (xem Hình 3.20). Tất nhiên, nhược điểm của việc loại bỏ gói tin đã nhận đúng (nhưng không theo thứ tự) là khi truyền lại gói tin có thể bị mất hay lỗi, do đó phải truyền đi truyền lại nhiều lần.

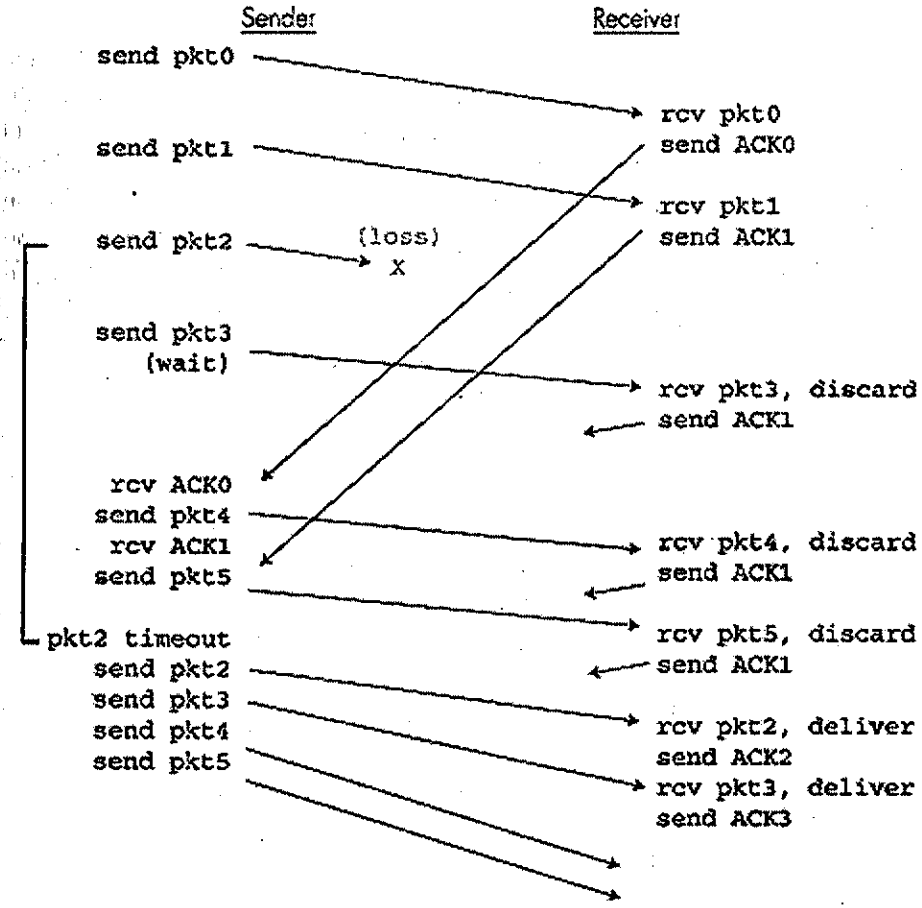
Hình 3.21 là một ví dụ hoạt động của giao thức GBN trong trường hợp cửa sổ có độ lớn bốn gói tin. Với độ lớn này, bên gửi sẽ chỉ được gửi các gói tin từ 0 đến 3 nhưng sau đó phải đợi biên nhận cho các gói tin này trước khi tiếp tục gửi tiếp. Khi nhận được các ACK liên tiếp nhau (ví dụ ACK0 và ACK1), cửa sổ sẽ trượt về phía trước, bên gửi có thể truyền gói tin mới (lần lượt là pkt4 và pkt5). Ở phía bên nhận, gói tin số 2 bị mất, do đó gói tin 3,4,5 gửi đến không theo đúng thứ tự và bị loại bỏ.

Với GBN, có một chú ý quan trọng là triển khai GBN tương tự FSM mở rộng (Hình 3.19). Hình thức triển khai bao gồm nhiều thủ tục khác nhau, mỗi thủ tục thực hiện một nhóm các hành động nào đó đáp lại các sự kiện khác nhau có thể xảy ra. Với lập trình hướng sự kiện (**event-based programming**), các thủ tục sẽ được gọi khi sự kiện tương ứng xuất hiện. Ở phía bên gửi, sự kiện có thể là: (1) thực thể tầng trên truyền dữ liệu xuống qua thủ tục rdt_send(), (2) ngắt khi thời gian đợi hết và (3) tầng dưới chuyển dữ liệu lên qua hàm rdt_rcv( ).

Chú ý rằng giao thức GBN kết hợp hầu hết các kỹ thuật mà chúng ta sẽ gặp khi nghiên cứu TCP trong mục 3.5: số thứ tự, số biên nhận tích luỹ, checksum, timeout và việc truyền lại. Trong thực tế, TCP là giao thức "tựa" GBN. Tuy nhiên có sự khác biệt giữa GBN và TCP. Nhiều phiên bản TCP



lưu lại các segment không theo thứ tự nhận đúng. Trong phương án nâng cấp TCP, sử dụng biên nhận có lựa chọn [RFC 258] cho phép bên nhận có thể biên nhận tuỳ ý một gói tin không theo thứ tự (chứ không sử dụng giá trị biên nhận tích luỹ). Biên nhận có lựa chọn chính là lớp giao thức gửi liên tiếp thứ hai mà chúng ta sẽ nghiên cứu dưới đây: **lặp lại có lựa chọn (selective repeat - SR)** . Có thể xem TCP là sự kết hợp của cả hai giao thức GBN và SR.

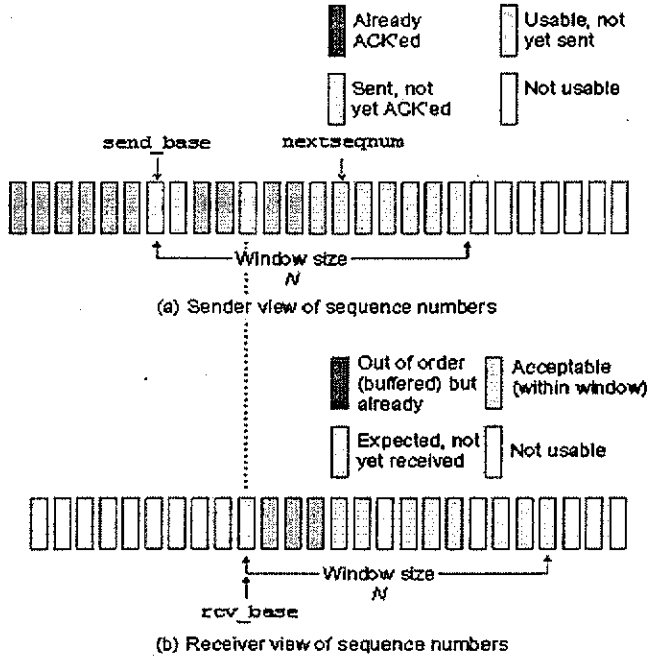



**Hình 3.21 Giao thức Go-Back N trong quá trình hoạt động**

### 3.4.4 Giao thức lặp lại có lựa chọn (Selective Repeat)

Giao thức GBN cho phép bên gửi "đổ tràn đường truyền" bằng các gói tin như trong Hình 3.17 và do đó khắc phục được hiệu suất thấp của giao thức **stop and wait**. Tuy nhiên trong một vài tình huống, chính hiệu suất của giao thức GBN cũng cực thấp. Ví dụ khi kích thước cửa sổ và thời gian truyền một gói tin lớn, có thể có nhiều gói tin ở trên đường truyền. Một gói tin bị lỗi có thể khiến GBN phải truyền lại nhiều gói tin mà trong một số trường hợp là không cần thiết. Nếu trong ví dụ đọc chính tả của chúng ta, nếu mỗi từ bị lỗi phải đọc lại khoảng 1000 từ đứng trước (kích thước cửa sổ là 1000 từ) thì tốc độ đọc sẽ rất chậm.

Giao thức lặp lại có lựa chọn (**SR - Selective Repeat**) tránh việc truyền lại không cần thiết bằng cách bên gửi chỉ truyền lại các gói tin mà nó cho là có lỗi (hoặc mất). Để truyền lại từng gói tin cần thiết, bên nhận cần biên nhận cho từng gói tin nhận đúng. Giao thức này vẫn sử dụng kích thước cửa sổ là N để giới hạn tổng số gói tin chưa được biên nhận trên đường truyền. Tuy nhiên khác với GBN, bên gửi sẽ nhận được biên nhận ACK cho một số gói tin trong cửa sổ. Hình 3.22 là không gian số thứ tự của phía gửi SR. Hình 3.23 mô tả chi tiết hành động của bên gửi trong giao thức SR.




**Hình 3.22 Khoảng số thứ tự của bên gửi và bên nhận**



Bên nhận Selective Repeat sẽ biên nhận cho bất kỳ gói tin nhận đúng, cho dù không theo đúng thứ tự. Gói tin không đúng thứ tự vẫn được lưu giữ lại cho đến khi tất cả các gói tin còn thiếu (gói tin có số thứ tự nhỏ hơn) được chuyển đến, khi đó tất cả các gói tin sẽ được chuyển lên tầng trên theo đúng thứ tự.

**Hình 3.23 tóm tắt các hoạt động khác nhau của bên nhận trong SR.**

**Hình 3.25 là một ví dụ hoạt động của SR trong trường hợp mất gói tin. Trong**

Hình 3.25, bên nhận sẽ lưu giữ tạm gói tin 3,4 và gửi chúng cùng với gói tin 2 lên tầng trên khi gói tin 2 được chuyển đến.

***1. Dữ liệu nhận được từ phía trên***

Khi nhận được dữ liệu từ phía trên, bên gửi SR kiểm tra số thứ tự sẽ gửi. Nếu số thứ tự sẽ gửi nằm trong cửa sổ gửi, dữ liệu được đóng gói và gửi đi, ngược lại thì dữ liệu được lưu giữ trong bộ đệm hoặc gửi trả lên tầng trên để gửi sau, giống GBN.

***2. Hết thời gian đợi - Timeout***

Timer lại được sử dụng để phát hiện mất gói tin. Tuy nhiên, mỗi gói tin gửi đi có một timer riêng, bởi vì chỉ có duy nhất một gói tin được gửi lại khi hết thời gian đợi. Có thể sử dụng đồng hồ hệ thống giữ vai trò đồng bộ cho các timer.

***3. Nhận được ACK***

Nếu nhận được ACK, bên gửi đánh dấu gói tin đã được chuyển đúng. Nếu số thứ tự của gói tin vừa được biên nhận bằng send_base, cánh cửa sổ sẽ trượt tới gói tin có số thứ tự nhỏ nhất chưa được biên nhận. Nếu cửa sổ di chuyển và còn các gói tin chưa được truyền thì các gói tin đó sẽ được gửi.

**Hình 3.23 Sự kiện và phản ứng của bên gửi**

1) Nhận đúng gói tin với số thứ tự trong khoảng **[rcv_base,rcv_base+N-1**. Trong trường hợp này, gói tin nhận được nằm trong cửa sổ nhận. Bên nhận gửi biên nhận cho gói tin này. Nếu gói tin đó chưa được nhận từ trước, nó sẽ được ghi lại trong bộ đệm. Nếu gói tin đó có số thứ tự bằng với cận dưới của cửa sổ nhận (rcv_base trong hình 3.22) thì nó cùng các gói tin có số thứ tự liên tiếp đã lưu giữ từ trước (bắt đầu từ rcv_base) được chuyển lên tầng trên. Cửa sổ nhận sẽ trượt về phía trước một khoảng bằng với khoảng số gói tin đã chuyển lên tầng trên. Với ví dụ trên hình 3.25 khi nhận được gói tin có số thứ tự rcv_base=2 thì gói tin này cùng với gói tin rcv_base+1 và gói tin rcv_base+2 được chuyển lên tầng trên.

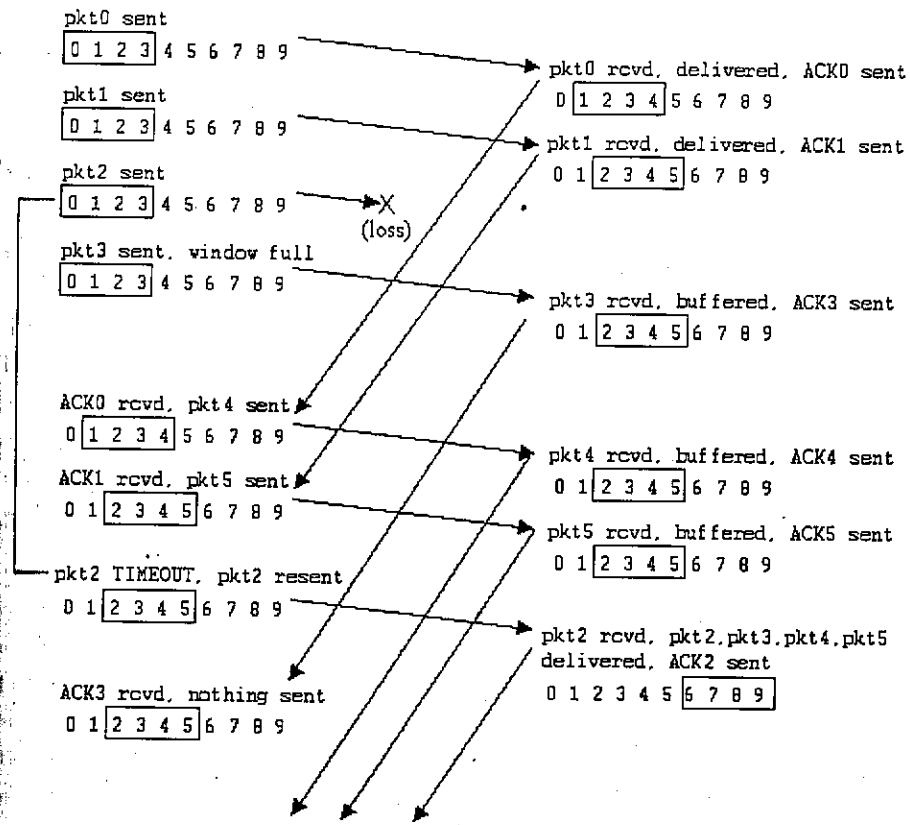
2. Nhận được gói tin với số thứ tự trong **[rcv_base-N,rcv_base-1]**. Trong trường hợp này, gửi biên nhận lại cho gói tin (mặc dù đã biên nhận từ trước).

3. ***Các trường hợp khác***. Bỏ qua gói tin đó.

**Hình 3.24 Sự kiện và phản ứng của bên nhận**

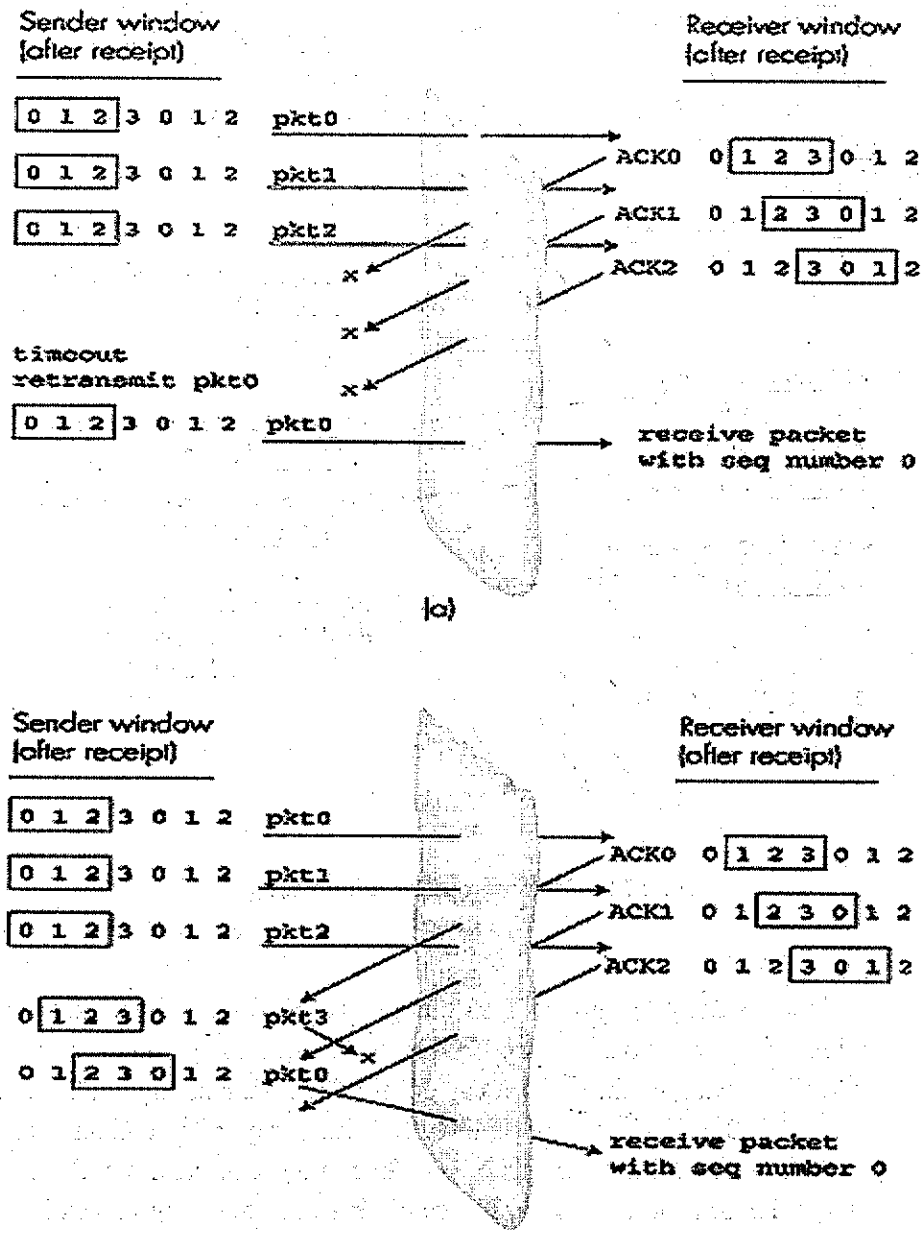
Chú ý rằng ở trong bước hai trong Hình 3.23 bên nhận phải biên nhận lại (chứ không được bỏ qua) cho gói tin đến với số thứ tự nhỏ hơn giá trị biên của cửa sổ hiện thời. Điều này hết sức cần thiết. Ví dụ với không gian số thứ tự của bên gửi và bên nhận như trong Hình 3.22, nếu không nhận được ACK từ bên nhận xác nhận gói tin send_base đã được nhận, bên gửi sẽ gửi lại gói tin send_base, mặc dù rõ ràng rằng (với chúng ta, chứ không phải bên gửi) bên nhận đã nhận được gói tin đó. Nếu bên nhận không biên nhận gói tin này, cửa sổ bên gửi có thể sẽ không bao giờ trượt tới phía trước. Ví dụ này minh hoạ một đặc điểm quan trọng của giao thức SR (và nhiều giao thức tương tự khác). Sự xác định của bên gửi và bên nhận về cái gì đã được nhận, cái gì chưa được nhận không phải luôn luôn giống nhau. Với giao thức SR, điều này có nghĩa là cửa sổ bên gửi và bên nhận không bao giờ trùng khớp nhau.






**Hình 3.25 SR trong quá trình hoạt động**

Thiếu sự đồng bộ giữa cửa sổ bên gửi và bên nhận có thể gây hậu quả nghiêm trọng trong trường hợp khoảng số thứ tự nhỏ. Ví dụ điều gì có thể xảy ra với khoảng số thứ tự là 4, các gói tin được đánh số là 0, 1, 2 và 3, bằng lớn cửa sổ là 3. Giả sử các gói tin từ 0, 1, 2 được truyền đi và nhận chính xác tại phía bên nhận. Bên nhận gửi biên nhận cho 3 gói tin này. Khi đó, cửa sổ bên nhận tiến lên các gói tin thứ 4,5 và 6 với số thứ tự tương ứng là 3, 0, và 1. Bây giờ xem xét hai trường hợp. Trường hợp đầu tiên (Hình 3.26a) , ACK của 3 gói tin đầu tiên bị mất, bên gửi truyền lại các gói tin đó. Khi đó bên nhận nhận được tiếp theo gói tin có số thứ tự 0 - lại chính là gói tin 0 đầu tiên được gửi ban đầu.




**Hình 3.26 Khi khoảng số thứ tự nhỏ: Truyền lại hay gói mới ?**



Trong trường hợp thứ hai (Hình 3.26b), ACK cho ba gói tin được huyển đi thành công. Như vậy cửa sổ bên gửi sẽ trượt về phía trước và gửi i các gói tin 4, 5, và 6 với số thứ tự tương ứng là 3, 0, 1. Nếu gói tin với số ứ tự 3 bị mất, lúc ấy gói tin có số thứ tự 0 đến, gói tin này chứa dữ liệu ới (không phải gói tin 0 truyền lại).

Rõ ràng có một bức "màn chắn" giữa bên gửi và bên nhận vì bên hận không thể "nhìn" thấy hành động từ bên gửi. Bên nhận chỉ quan sát ược gói tin nào nó nhận được hay gửi đi. Hai trường hợp trong inh 3.26 là tương tự nhau. Không có phương pháp nào phân biệt được gói được truyền lại hay gói 5 được truyền lần đầu tiên. Rõ ràng nếu kích thước a sổ nhỏ hơn khoảng số thứ tự một đơn vị thì hệ thống không còn làm ệc đúng đắn. Nhưng độ lớn cửa sổ nên là bao nhiêu? Người ta chứng minh ợc rằng độ lớn cửa sổ phải bé hơn hoặc bằng một nửa khoảng số thứ tự với ao thức SR.

Chúng ta giả thiết môi trường truyền không tin cậy ở dưới dẫn đến ệc các gói tin có thể bị giữ lại trên đường truyền. Đây là việc ít khi xảy ra i kênh truyền giữa phía gửi và phía nhận là một môi trường vật lý thực sự. ỳ nhiên khi kênh truyền này lại là một mạng máy tính thì việc một gói tin giữ lại trên kênh truyền hoàn toàn có thể xảy ra. Hệ quả của nó là xuất n một gói tin với số thứ tự hay số biên nhận là x trong khi cả cửa sổ nhận gửi đều không chứa x. Trong trường hợp này, kênh truyền bị coi là một đệm, có thể tuỳ ý phát lại gói tin ở bất cứ thời điểm nào. Vì số thứ tự có được sử dụng lại nên trong một số trường hợp sẽ xảy ra hiện tượng trùng gói tin. Trong thực tế phải bảo đảm số thứ tự không được sử dụng lại cho khi bên gửi có thể tương đối chắc chắn về gói tin với số thứ tự x được trước đấy không còn tồn tại trong mạng. Điều này được thực hiện với thiết một gói tin không thể "tồn tại" trên mạng trong một khoảng thời n lớn hơn một khoảng thời gian cố định nào đấy. Thời gian "sống" lớn t của gói tin xấp xỉ là 3 phút với mạng TCP cao tốc [RFC 1323]. Có iều phương thức đánh số thứ tự để tránh việc xuất hiện lại gói tin.

## TCP – GIAO THỨC GIAO VẬN HƯỚNG NỐI

Sau khi đã nghiên cứu những nguyên lý cơ bản của truyền dữ liệu tin , chúng ta sẽ bàn đến TCP – một giao thức tầng giao vận của Internet với tính hướng nối và tin cậy. Chúng ta sẽ thấy rằng để có thể cung cấp dịch

vụ truyền dữ liệu tin cậy, TCP áp dụng rất nhiều nguyên lý mà chúng ta đã đề cập ở phần trước, bao gồm cơ chế phát hiện lỗi, truyền lại, biên nhận tích lũy, timer, trường tiêu đề cho số thứ tự và số biên nhận. TCP được đặc tả trong các khuyến nghị RFC 793, RFC 1122, RFC 1323, RFC 2018, RFC 2581.

### 3.5.1 Kết nối TCP

Chức năng dồn kênh, phân kênh và phát hiện lỗi của TCP giống UDP. Tuy nhiên TCP và UDP có nhiều điểm khác biệt. Điểm khác nhau cơ bản nhất là UDP không hướng nối còn TCP hướng nối. UDP không hướng nối do có thể gửi dữ liệu mà không cần phải thiết lập trước đường truyền. TCP hướng nối vì trước khi tiến trình ứng dụng có thể bắt đầu gửi dữ liệu tới tiến trình khác, hai tiến trình này phải có thủ tục "bắt tay" với nhau, nghĩa là chúng phải gửi một số gói segment đặc biệt để xác định các tham số đảm bảo cho quá trình truyền dữ liệu. Trong giai đoạn thiết lập kết nối TCP, hai bên sẽ khởi tạo nhiều biến trạng thái TCP cho kết nối (xem mục 3.7).

"Kết nối" TCP không phải kết nối thực sự giữa hai điểm đầu mút (end-to-end) giống như mạch TDM hay FDM trong mạng chuyển mạch kênh. Nó cũng không phải là mạch ảo bởi vì trạng thái kết nối nằm hoàn toàn trên hệ thống đầu cuối. Giao thức TCP chỉ hoạt động trên thiết bị đầu cuối và không hoạt động trên các thiết bị trung gian (switch, bridge, router). Trong thực tế, các router trung gian chỉ có thể thấy các datagram, không nhìn thấy các kết nối.

Kết nối TCP cung cấp đường truyền dữ liệu **hai hướng** (song công – **full duplex**). Nếu có kết nối TCP giữa tiến trình A chạy trên một máy tính và tiến trình B chạy trên máy tính khác, khi đó dữ liệu ứng dụng có thể truyền từ A tới B cùng lúc với dữ liệu truyền từ B sang A. Kết nối TCP luôn luôn thuộc kiểu điểm nối điểm, giữa một bên gửi và một bên nhận (point to point). Chế độ truyền "multicasting" (tiến trình gửi có thể gửi đồng thời một thông điệp tới nhiều tiến trình nhận) không thực hiện được trong TCP.

Bây giờ ta hãy nhìn xem kết nối TCP được thiết lập như thế nào? Giả sử có tiến trình đang chạy trên một máy tính muốn khởi tạo đường



truyền tới tiến trình trong một máy tính khác. Nhớ lại rằng tiến trình nào khởi tạo kết nối là tiến trình khách (client) và tiến trình kia là tiến trình phục vụ (server). Đầu tiên tiến trình ứng dụng client yêu cầu thực thể TCP của mình thiết lập đường kết nối tới tiến trình nào đó trên server. Chương trình java thực hiện điều này bằng cách sử dụng mã:

Socket clientSocket = new Socket ("hostname" ,port number);

Sau đó thực thể giao vận trong máy client thiết lập kết nối TCP tới thực thể TCP trên máy phục vụ. Chúng ta sẽ thảo luận chi tiết thủ tục thiết lập đường truyền ở cuối mục này. Bây giờ chúng ta chỉ cần biết là đầu tiên máy khách sẽ gửi một gói tin TCP đặc biệt, máy server trả lời bằng một gói TCP đặc biệt thứ hai và cuối cùng client trả lời lại bằng một gói TCP đặc biệt thứ ba. Hai gói TCP đầu tiên không tải, có nghĩa là không có dữ liệu thực sự từ tầng ứng dụng, chỉ bắt đầu từ gói thứ ba mới mang dữ liệu. Vì ba gói dữ liệu đặc biệt này được trao đổi giữa hai máy tính trước khi kết nối, thủ tục thiết lập kết nối này còn được gọi là giai đoạn **bắt tay ba bước (three way handshake)**.

**Trong lịch sử Vinton Clef,Robert Kahn,và TCP/IP.**

Đầu những năm 1970, mạng chuyển mạch gói bắt đầu phát triển mạnh mẽ, và mạng APPAnet, tiền thân của Internet - chỉ là một trong các kiểu mạng như vậy. Mỗi kiến trúc mạng đều có giao thức riêng của mình. Hai nhà nghiên cứu, Vinton Cerf và Robert Kahn, nhận thấy tầm quan trọng của việc kết nối các mạng lại với nhau, đã cùng nhau phát triển giao thức liên mạng với tên gọi TCP/IP (viết tắt của Transmission Control Protocol/Internet Protocol). Mặc dù lúc đầu Cerf và Kahn xem giao thức này là một thực thể duy nhất, nhưng ngay sau đó nó được tách ra thành hai phần riêng biệt, hoạt động độc lập với nhau là TCP và IP. Cerf và Kahn đã công bố về TCP/IP vào 5/1974 trong IEEE Transacsions on Communications Technology.

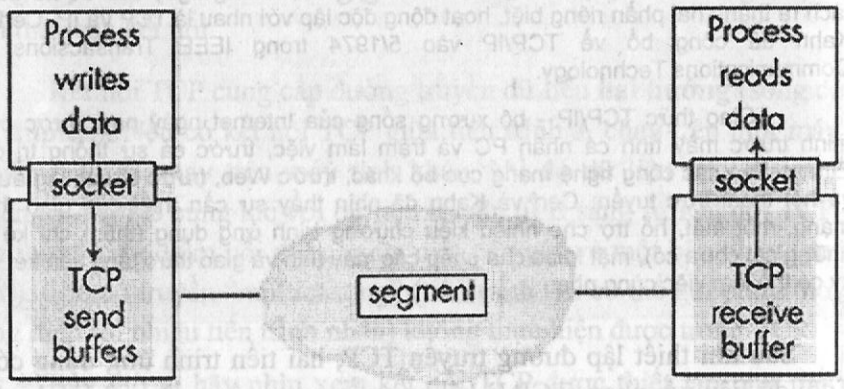
Giao thức TCP/IP - bộ xương sống của Internet ngày nay, được phát minh trước máy tính cá nhân PC và trạm làm việc, trước cả sự thống trị của Ethernet và các công nghệ mạng cục bộ khác, trước Web, trước streaming audio và hội thoại trực tuyến. Cerf và Kahn đã nhìn thấy sự cần thiết của giao thức mạng, một mặt, hỗ trợ cho nhiều kiểu chương trình ứng dụng (thậm chí kể cả những cái chưa có), mặt khác cho phép các máy tính và giao thức tầng liên kết bất kỳ có thể làm việc cùng nhau.

Sau khi thiết lập đường truyền TCP, hai tiến trình ứng dụng có thể trao đổi dữ liệu với nhau. TCP là kênh truyền song công nên máy tính có thể gửi và nhận đồng thời. Xét quá trình gửi dữ liệu từ tiến trình client tới tiến

trình server. Tiến trình client sẽ "đổ" luồng dữ liệu qua socket ("cửa" của tiến trình - xem mục 2.6). Khi đã qua cửa, tiến trình gửi sẽ không kiểm soát được dữ liệu mà chính thực thể TCP chạy trên máy client sẽ chịu trách nhiệm kiểm soát. Trong Hình 3.27, TCP đẩy dữ liệu vào bộ đệm gửi **(send buffer)**, một trong các bộ đệm được khởi tạo trong quá trình thiết lập kết nối. Sau đó TCP sẽ lấy và gửi dần dữ liệu trong bộ đệm gửi. Tuy nhiên, đặc tả TCP không xác định tường minh khi nào TCP phải gửi dữ liệu trong bộ đệm. Thường nó chỉ yêu cầu TCP "gửi khi thuận tiện". Lượng dữ liệu ứng dụng lớn nhất có thể đặt trong một segment giới hạn bởi MMS (maximum segement size). Giá trị MMS phụ thuộc vào chính phần mềm triển khai TCP (thường là hệ điều hành) và có thể cấu hình được. Các giá trị MMS phổ biến thường là 1500 byte, 536 byte hay 512 byte. (Độ lớn của segment thường được giới hạn để tránh hiện tượng phân mảnh IP, một hiện tượng sẽ được đề cập trong chương sau). Chú ý MMS là lượng dữ liệu ứng dụng lớn nhất trong segment, chứ không phải là kích thước lớn nhất của segment TCP bao gồm cả tiêu đề (header).

Thực thể TCP gói dữ liệu cùng với TCP header trong TCP segment. TCP segment được chuyển xuống dưới tầng mạng và được đặt trong gói tin của tầng mạng (IP datagram) để gửi qua mạng. Ở phía nhận, thực thể TCP sẽ đặt dữ liệu vào bộ đệm nhận **(receiver buffer)** của kết nối TCP. Ứng dụng sẽ đọc dòng dữ liệu này từ bộ đệm. Mỗi kết nối đều có bộ đệm gửi và bộ đệm nhận. Bộ đệm gửi và nhận cho dữ liệu được minh hoạ trên Hình 3.27.

Chú ý rằng bộ đệm, các biến trạng thái, và socket tạo thành kết nối TCP chỉ nằm trên hai thiết bị đầu cuối chứ không nằm trên các thiết bị trung gian (router, hub, switch...).




**Hình 3.27 Bộ đệm của thực thể TCP**



### 3.5.2 Cấu trúc TCP Segment

Sau khi đã nói qua về TCP, bây giờ chúng ta sẽ xem xét cấu trúc gói dữ liệu TCP (TCP segment). TCP segment bao gồm các trường tiêu đề và trường dữ liệu. Trường dữ liệu chứa một phần dữ liệu ứng dụng. Như đã nói ở trên, giá trị MMS giới hạn độ lớn trường dữ liệu của segment. Khi TCP gửi một file lớn - ví dụ file ảnh trong trang Web, nó phải chia file thành các đoạn có kích thước MMS (ngoại trừ đoạn cuối cùng có độ lớn bé hơn hoặc bằng MMS). Tuy nhiên độ lớn dữ liệu của các ứng dụng tương tác thường nhỏ hơn MMS. Ví dụ, với ứng dụng đăng nhập từ xa (Telnet), trường dữ liệu trong TCP segment thường chỉ là 1 byte. Độ lớn trường tiêu đề của TCP là 20 byte (của UDP là 12 byte). Segment được Telnet gửi có thể chỉ có 21 byte.

Hình 3.28 minh hoạ cấu trúc TCP segment. Tương tự UDP, tiêu đề TCP bao gồm trường số hiệu cổng nguồn, số hiệu cổng đích để thực hiện dịch vụ dồn, phân kênh dữ liệu cho các ứng dụng bên trên và trường Checksum. Tuy nhiên tiêu đề của TCP segment còn có các trường sau:

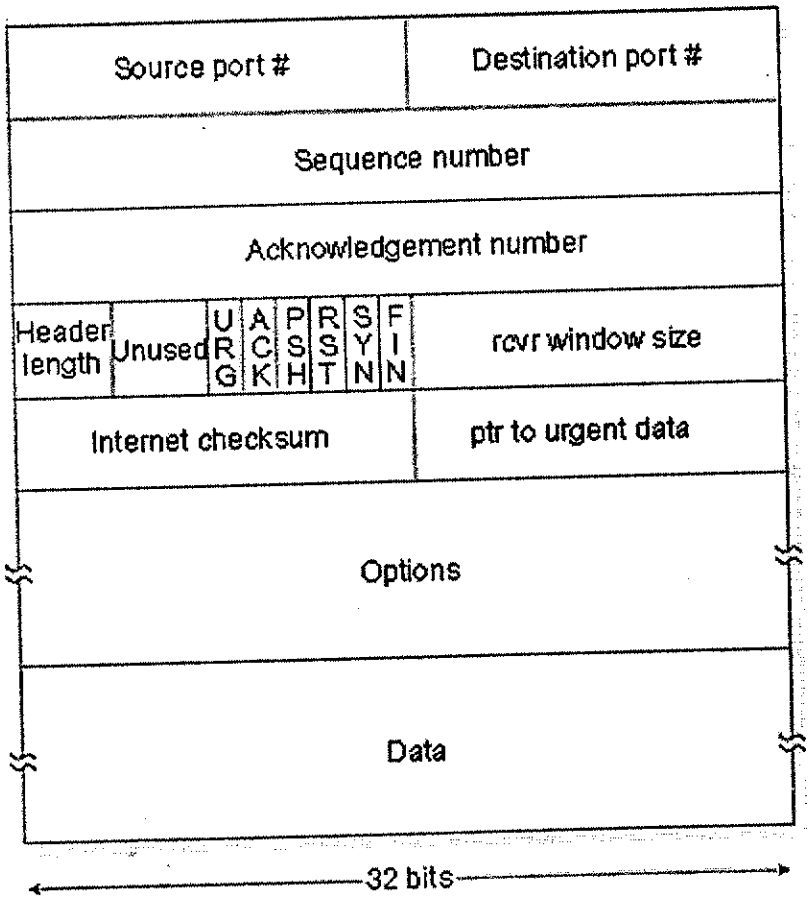
Trường **số thứ tự (sequence number)** 32 bit và trường **số biên nhận (acknowledge number)** 32 bit được bên gửi và bên nhận sử dụng trong việc cung cấp dịch vụ truyền dữ liệu tin cậy, sẽ được đề cập kĩ hơn trong phần dưới đây.

Trường **độ lớn cửa sổ (window size)** 16 bit được sử dụng để kiểm soát lưu lượng. Đấy chính là số lượng dữ liệu tối đa (tính theo byte) mà bên nhận có thể chấp nhận được.

Trường **độ dài tiêu đề (length field)** 4 bit xác định độ dài của tiêu đề TCP theo đơn vị là các từ 32 bit. Tiêu đề TCP có thể có độ dài thay đổi phụ thuộc trường option (Nếu trường option rỗng, thì chiều dài của tiêu đề TCP là 20 byte).

Trường **option** là tuỳ chọn, có thể thay đổi tuỳ ý. Trường này được sử dụng khi bên gửi, bên nhận có thể thương lượng về giá trị MMS hoặc giá trị gia tăng của cửa sổ trong mạng cao tốc. Lựa chọn nhãn thời gian (timestamping) cũng được định nghĩa. Xem RFC 854 và RFC 1323 để biết thêm chi tiết.

Trường cờ (**flag**) gồm 6 bit. Bit **ACK** được sử dụng để chỉ ra rằng giá trị đặt trong trường biên nhận là đúng. Các bit **RST**, **SYN** và **FIN** được sử dụng trong việc thiết lập hay đóng kết nối. Khi bit **PSH** được bật, thì đây là dấu hiệu để yêu cầu bên nhận phải chuyển dữ liệu lên tầng trên ngay lập tức. Cuối cùng, bit **URG** được dùng để báo hiệu dữ liệu trong segment được thực thể tầng trên phía gửi tạo ra là "khẩn cấp". Vị trí byte cuối cùng của dữ liệu khẩn cấp được xác định bởi con trỏ dữ liệu khẩn 16 bit (ptr to urgent data). TCP phải báo cho tầng trên biết có dữ liệu khẩn và đặt con trỏ vào cuối dữ liệu khẩn (Trong thực tế, PSH, URG và con trỏ dữ liệu khẩn không được sử dụng)



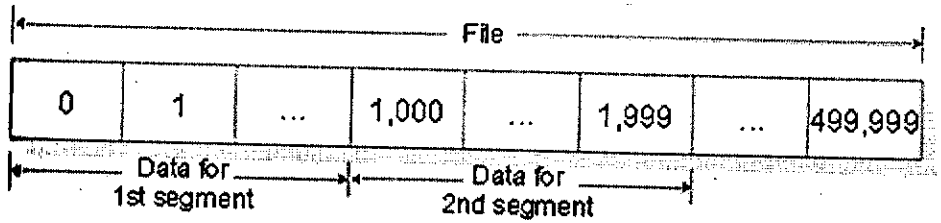

Hình 3.28 Cấu trúc gói dữ liệu TCP



## 3.5.3 Số thứ tự và Số biên nhận

Hai trong số những trường quan trọng nhất của tiêu đề TCP segment là trường số thứ tự và trường số biên nhận. Trước khi nói đến những trường này được sử dụng để cung cấp đường truyền dữ liệu tin cậy như thế nào, chúng ta cần nói đến những trường này nhận giá trị gì.

TCP xem dữ liệu là dòng các byte không có cấu trúc nhưng có thứ tự và TCP sẽ đánh số thứ tự cho từng byte của dòng dữ liệu này. Mỗi segment có một số thứ tự, là số thứ tự của byte đầu tiên của segment. Xét ví dụ sau: Giả sử có tiến trình trên máy A muốn gửi dòng dữ liệu tới tiến trình trên máy B thông qua kết nối TCP. Thực thể TCP trên máy A sẽ đánh số thứ tự cho từng byte trong dòng dữ liệu. Giả sử dòng dữ liệu này chứa file có kích thước 500.000 byte, giá trị MMS là 1000 byte, và byte đầu tiên của dòng dữ liệu được đánh số thứ tự 0. Trong Hình 3.29, TCP sẽ tạo ra 500 segment từ dòng dữ liệu này. Segment đầu tiên có số thứ tự 0, segment thứ hai có số thứ tự là 1000 , segment thứ ba có số thứ tự là 2000,.... Mỗi số thứ tự như vậy được chèn vào trường số thứ tự trong tiêu đề của TCP segment tương ứng.




Hình 3.29 Chia nhỏ file dữ liệu vào các TCP segment

Số biên nhận phức tạp hơn số thứ tự. Vì TCP là kênh truyền song công nên A có thể nhận được dữ liệu từ B trong khi nó gửi dữ liệu tới B (trên cùng kết nối TCP). Mỗi segment đến từ máy B có một số thứ tự cho dòng dữ liệu đi từ B sang A. ***Số biên nhận mà máy A đặt trong segment của nó sẽ là số thứ tự của byte tiếp theo mà máy A đang chờ máy B gửi tới.*** Để có thể hiểu rõ hơn chúng ta xét ví dụ sau: Giả sử rằng máy A đã nhận được tất cả các byte từ byte số 0 đến byte số 535 máy B gửi đến và giả sử máy A cũng gửi một segment tới máy B. Trong trường hợp này, máy A đợi byte thứ 536 và toàn bộ các byte tiếp theo trong dòng dữ liệu từ máy B. Khi

đó máy A đặt giá trị 536 vào trường số biên nhận của segment mà nó gửi tới máy B.

Một ví dụ khác, giả sử rằng máy A đã nhận được một segment từ máy B bao gồm byte 0 đến byte 535 và một segment khác bao gồm byte 900 đến byte 1000. Vì lý do nào đó, máy A không nhận được byte thứ 536 đến byte 899. Trong trường hợp này, máy A sẽ vẫn đợi byte thứ 536 (và các byte tiếp theo) để tạo lại dòng dữ liệu của máy B. Do đó, trong segment tiếp theo bên A gửi cho bên B, trường số biên nhận vẫn chứa giá trị 536. TCP biên nhận tất cả các byte cho đến byte đầu tiên chưa nhận được (còn thiếu trong dòng dữ liệu), cho nên có thể nói TCP biên nhận kiểu **tích luỹ (cummulative acknowledgement)**.

Ví dụ cuối cùng đưa ra vấn đề quan trọng nhưng đơn giản. Bên A nhận được segment thứ ba (byte thứ 900 đến 1.000) trước khi nhận được segment thứ hai (byte thứ 536 đến byte 899). Khi đó segment thứ ba đến không theo đúng thứ tự. Vấn đề ở đây sẽ là máy tính sẽ làm gì khi nó nhận được một segment không đúng thứ tự trong kết nối TCP ? Rất thú vị, các đặc tả RFC TCP không đưa ra bất cứ một quy tắc nào để giải quyết. Chính người lập trình phần mềm TCP sẽ đưa ra cách giải quyết. Về cơ bản, có hai lựa chọn: (1) Bên nhận ngay lập tức loại bỏ các byte không đúng thứ tự hoặc (2) bên nhận giữ lại các byte không đúng thứ tự và chờ đến khi nhận được các byte thiếu, tạo thành dòng dữ liệu liên tục. Rõ ràng giải pháp sau có hiệu quả hơn nếu đánh giá theo hiệu suất mạng, trong khi đó giải pháp thứ nhất đơn giản hóa việc cài đặt TCP. Trong quyển sách nhập môn này, chúng ta sẽ coi TCP phía nhận loại bỏ các segment không đúng thứ tự.

Trong Hình 3.30 chúng ta mặc định số thứ tự khởi tạo bắt đầu từ số 0. Nhưng trên thực tế, cả hai phía kết nối TCP đều chọn ngẫu nhiên giá trị số thứ tự khởi tạo ban đầu. Điều này sẽ giảm thiểu xác suất có một gói tin của một kết nối đã kết thúc giữa hai máy tính tồn tại quá lâu trên mạng và bị hiểu nhầm là một segment hợp lệ của một kết nối khác giữa chính hai máy tính đấy.

## 3.5.4 Telnet: Một ví dụ về số thứ tự và số biên nhận

Telnet đặc tả trong khuyến nghị RFC 854 là giao thức đăng nhập từ xa phổ biến ở tầng ứng dụng. Nó chạy trên nền TCP và được thiết kế để làm



việc giữa một cặp máy bất kỳ. Không giống các ứng dụng trao đổi dữ liệu đề cập trong chương hai, Telnet là ứng dụng mang tính tương tác. Chúng ta thảo luận ví dụ Telnet ở đây để có thể hiểu rõ hơn số thứ tự và số biên nhận của TCP.

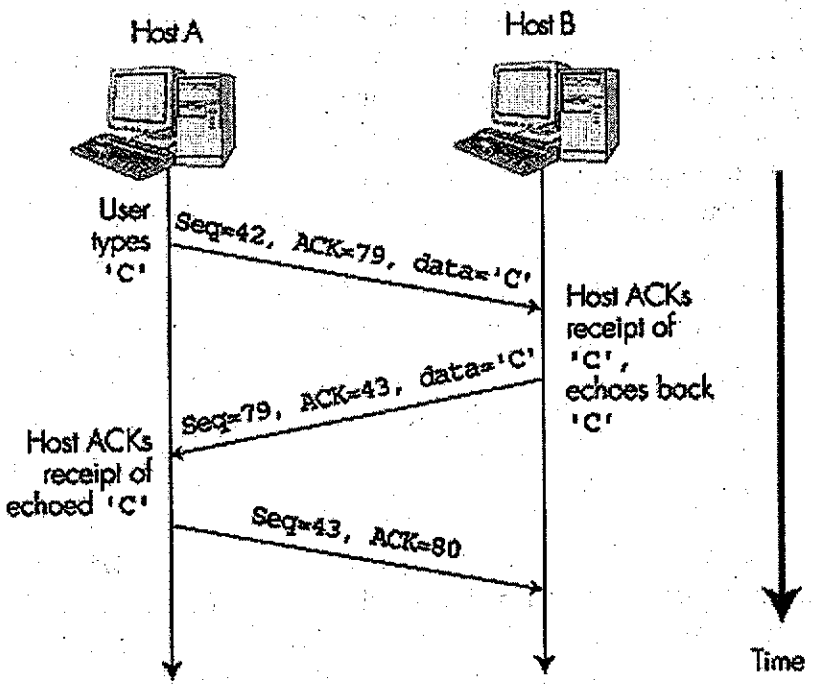
Giả sử máy A thiết lập một phiên Telnet với máy B. Máy A thiết lập phiên làm việc nên đóng vai trò client, máy B đóng vai trò server. Mỗi ký tự được người dùng gõ vào (tại phía client A) sẽ được gửi tới máy B; B sẽ gửi lại A bản sao của kí tự đó. Sau đó A sẽ hiển thị ký tự đó trong màn hình Telnet của người sử dụng. Tín hiệu "echo back" được sử dụng để chắc chắn rằng kí tự mà người sử dụng nhìn thấy đã được nhận và xử lý tại máy tính ở xa. Như vậy mỗi kí tự sẽ được truyền qua mạng hai lần trong khoảng thời gian người dùng gõ phím tới khi ký tự được hiển thị trên màn hình của người sử dụng.

Bây giờ giả sử rằng người sử dụng gõ một phím bất kì, chẳng hạn là 'C'. Hãy kiểm tra xem các TCP segment được trao đổi giữa client và server. Trên Hình 3.31, chúng ta coi số thứ tự bắt đầu của client là 42 và của server là 79. Như đã nói trên, số thứ tự của segment chính là số thứ tự của byte đầu tiên trong trường dữ liệu. Khi đó, segment đầu tiên được gửi từ phía client sẽ có số thứ tự là 42; segment đầu tiên được gửi từ phía server sẽ có số thứ tự là 79. Số biên nhận là số thứ tự của byte tiếp theo trong dòng dữ liệu đang đợi nhận. Như vậy, ngay sau khi kết nối TCP được thiết lập - nhưng trước dữ liệu thực sự được gửi, bên client sẽ đợi byte có số thứ tự 79 và bên server sẽ đợi byte có số thứ tự 42. Trên hình 3.31 ba segment đã được trao đổi. Segment đầu tiên được client gửi tới server, chứa một byte mã ASCII của ký tự 'C' trong trường dữ liệu. Trường số thứ tự của segment đầu tiên nhận giá trị 42. Vì client chưa nhận được bất kỳ dữ liệu nào từ server, nên trường số biên nhận trong segment này nhận giá trị 79.

Segment thứ hai được server gửi cho client. Có hai điểm chú ý với segment này, đầu tiên server biên nhận cho dữ liệu vừa nhận được. Với giá trị 43 trong trường số biên nhận, server báo cho client rằng nó nhận đúng tất cả các byte có số thứ tự không vượt 42 và bây giờ đang chờ nhận byte thứ 43. Thứ hai là segment này sẽ chứa lại kí tự 'C' (phản hồi lại). Lúc ấy trường dữ liệu của segment thứ hai chứa mã ASCII của ký tự 'C'. Giá trị

trường số thứ tự của segment thứ hai này là 79 - là số thứ tự của byte đầu tiên trong dòng dữ liệu chuyển từ server sang client. Chú ý rằng biên nhận cho dữ liệu từ client tới server được đặt ngay trong segment chứa dữ liệu từ server tới client. Đây gọi là biên nhận **ghép đuôi (piggybacking).**

Segment thứ ba được gửi từ client tới server. Mục đích duy nhất của nó là biên nhận dữ liệu nhận được từ server (chú ý segment thứ hai chứa dữ liệu là kí tự 'C' từ server tới client). Segment thứ ba có trường dữ liệu rỗng (biên nhận không đi kèm với dữ liệu gửi đến server). Trường số biên nhận của segment này nhận giá trị 80 vì client đã nhận được tất cả các byte có số thứ tự không vượt 79 và đang đợi byte có số thứ tự 80. Có lẽ bạn nghĩ thật không bình thường khi segment này cũng có số thứ tự khi nó chẳng chứa dữ liệu. Nhưng tiêu đề TCP có trường số thứ tự, nên phải đặt giá trị nào đó vào trong trường này.




**Hình 3.31 Số thứ tự và số biên nhận trong ví dụ Telnet**



## 3.5.5 Truyền dữ liệu tin cậy

Dịch vụ tầng mạng của Internet không tin cậy: IP không đảm bảo việc chuyển datagram, không đảm bảo gửi datagram đúng thứ tự cũng như không đảm bảo tính toàn vẹn dữ liệu. Với dịch vụ IP, datagram có thể bị tràn tại bộ đệm router và do đó không bao giờ đến được đích, dữ liệu có thể đến không đúng thứ tự hay các bit trong datagram có thể bị lỗi. Bởi vì segment của tầng giao vận được đặt trong IP datagram để truyền qua mạng nên segment của tầng giao vận cũng có thể phải gặp những vấn đề nêu trên.

TCP tạo ra đường truyền dữ liệu tin cậy trên dịch vụ không tin cậy của IP. Dịch vụ truyền dữ liệu tin cậy của TCP đảm bảo dòng dữ liệu tới tiến trình nhận không có lỗi, liên tục, không trùng lặp dữ liệu, đúng thứ tự. Có nghĩa là dòng byte nhận được giống hệt dòng byte gửi đi. Mục này nghiên cứu cách thức cung cấp dịch vụ truyền dữ liệu tin cậy của TCP. Chúng ta sẽ thấy rằng dịch vụ truyền dữ liệu tin cậy của TCP sử dụng rất nhiều nguyên lý cơ bản đã nghiên cứu trong mục 3.4.

Hình 3.32 minh hoạ 3 sự kiện chính liên quan đến việc truyền hay truyền lại dữ liệu tại phía bên gửi TCP. Để đơn giản, chúng ta coi kết nối TCP giữa hai máy A và B chuyển dữ liệu từ máy A tới máy B. Tại phía gửi (máy A), thực thể TCP lấy dữ liệu của tầng ứng dụng, đóng gói trong các segment và chuyển xuống tầng mạng. Do đó nhận dữ liệu từ tầng ứng dụng, đóng gói dữ liệu trong các segment và gửi segment đi chính là sự kiện quan trọng đầu tiên mà thực thể TCP bên gửi phải xử lý. Ngay sau khi chuyển segment cho IP, TCP khởi động timer cho segment đó. Thời gian đợi hết (timeout) gây ra một ngắt tại máy A. TCP phản ứng với sự kiện timeout, đây đơn giản là sự kiện thứ hai mà bên gửi TCP phải xử lý bằng cách truyền lại segment gây ra ngắt thời gian.

Sự kiện thứ ba mà bên gửi TCP phải xử lý là nhận được một segment biên nhận (ACK) từ bên gửi (chính xác hơn là một segment chứa giá trị trường biên nhận ACK hợp lệ). Ở đây, thực thể TCP phía gửi phải quyết định đó là ACK lần đầu tiên nhận được (tức là biên nhận cho một segment đã gửi nhưng chưa được biên nhận) hay chỉ là ACK trùng lặp (biên nhận lại một gói tin đã từng được biên nhận). Trong trường hợp thứ nhất thì bên gửi sẽ biết rằng tất cả các byte có số thứ tự không vượt giá trị biên nhận được nhận được đã được gửi thành công. Khi đó, bên gửi có thể cập nhật biến trạng thái TCP kiểm soát số thứ tự của byte cuối cùng mà nó cho rằng đã được nhận chính xác và theo đúng thứ tự tại phía bên nhận.

## Trên thực tế

TCP cung cấp đường truyền tin cậy bằng cách sử dụng ACK và timer giống như trong mục 3.4. TCP biên nhận cho dữ liệu đã được nhận chính xác, và truyền lại segment nếu cho rằng segment hay biên nhận tương ứng của nó bị mất hoặc có lỗi. Phiên bản hiện thời của TCP cũng có cơ chế NAK ẩn, đấy là cơ chế truyền lại nhanh của TCP khi nhận được ba ACK cho cùng một segment được gửi. TCP sử dụng số thứ tự cho phép bên nhận xác định segment bị mất hoặc trùng lặp. Cái này tương tự như trường hợp giao thức truyền dữ liệu tin cậy của chúng ta. TCP không chắc chắn được segment hay biên nhận của nó bị lỗi, bị mất hay chỉ đến trễ, nó xử lý giống hệt nhau: truyền lại.

TCP cũng thực hiện việc gửi liên tục (cơ chế đường ống), cho phép bên gửi có thể gửi nhiều segment mà chưa cần nhận biên nhận ngay. Cơ chế này cho phép nâng cao hiệu suất của đường truyền. Số lượng tối đa các segment được gửi chưa cần biên nhận phụ thuộc vào cơ chế kiểm soát lưu lượng và kiểm soát tắc nghẽn của TCP. Cả hai cơ chế này đều được nghiên cứu trong các phần sau.

Để hiểu về phản ứng của bên gửi khi nhận được ACK trùng lặp, đầu tiên chúng ta phải xét tại sao bên nhận gửi ACK trùng lặp. Bảng 3.1 tóm tắt các chính sách chung của thực thể TCP nhận. Khi nhận được segment có số thứ tự lớn hơn số thứ tự đang được mong đợi, bên nhận phát hiện có đoạn trống trong dòng dữ liệu - nghĩa là thiếu segment. Vì TCP không sử dụng biên nhận phủ định (NAK) nên bên nhận không thể gửi biên nhận phủ định. Thay vào đó, nó biên nhận lại byte đúng thứ tự cuối cùng mà nó nhận được (tạo ra ACK trùng lặp). Nếu bên gửi TCP nhận được 3 ACK trùng lặp cho cùng một segment, nó sẽ cho rằng segment ngay sau segment được biên nhận ba lần bị mất. Trong trường hợp này, TCP thực hiện cơ chế truyền lại nhanh **(fast retransmit)** [RFC 258], gửi lại segment bị cho là mất trước khi timer của segment đó hết hạn (kết thúc).

```
/*assume sender is not constrained by TCP flow or
congestion control,that data from above is less than MSS in
size, and that data transfer is in one direction only
*/
sendbase=initial_sequence number /*see Figure 3.18*/
nextseqnum=initial_sequence number
```



```
 loop (forever) {
   switch(event)

vent: data received from application above
reate TCP segment with sequence number nextseqnum
          start timer for segment nextseqnum
          pass segment to IP
          nextseqnum=nextseqnum+length(data)
reak;  /* end of event data received from above */

vent: timer timeout for segment with sequence number y
          retransmit segment with sequence number y
          compute new timeout interval for segment y
          restart timer for sequence number y
          break;  /* end of timeout event */

ent: ACK received, with ACK field value of y
 (y > sendbase) {/* cumulative ACK of all date up to y */
ncel all timers for segments with sequence numbers < y
ndbase=y
             }
e { /* a duplicate ACK for already ACKed segment */
rement number of duplicate ACKs received for y
(number of duplicate ACKs received for y==3) {
                /* TCP fast retransmit */
                resend segment with sequence number y
                restart timer for segment y
             }
ak; /* end of ACK received event */
* end of loop forever */
```

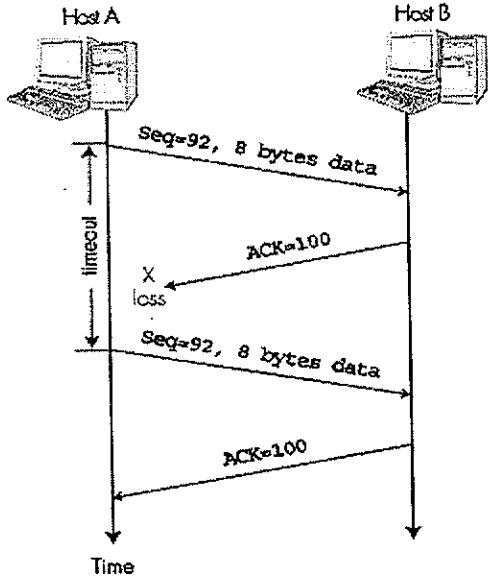
**Hình 3.31 Bên gửi của TCP**

| Sự kiện | Hành động tiếp nhận của TCP |
|---|---|
| gment đến có số thứ tự là số thứ mong muốn. Tất cả dữ liệu đến thứ tự mong muốn đã được biên n. Không có khoảng trống trong liệu nhận được | Trì hoãn ACK. Đợi segment đúng thứ tự tiếp theo trong khoảng thời gian 500ms. Nếu segment này không xuất hiện mới gửi ACK |
| gment đến có số thứ tự là số thứ mong muốn. Segment đến trước ng đợi gửi biên nhận. Không có ảng trống trong dữ liệu nhận được | Ngay lập tức gửi đi ACK tích lũy duy nhất biên nhận cho cả hai segment đúng thứ tự. |

| | |
|---|---|
| Segment không đúng thứ tự đến, có số thứ tự cao hơn số thứ tự mong muốn nhận. Phát hiện có khoảng trống dữ liệu. | Ngay lập tức gửi đi ACK trùng lặp và chỉ ra số thứ tự của byte mong muốn nhận tiếp theo. |
| Segment đến lấp đầy một phần hoặc toàn bộ khoảng trống trong dữ liệu nhận được | Ngay lập tức gửi đi ACK biên nhận cho đoạn dữ liệu đúng thứ tự liên tục lớn nhất nhận được |

Hình 3.32

## Một vài trường hợp tiêu biểu



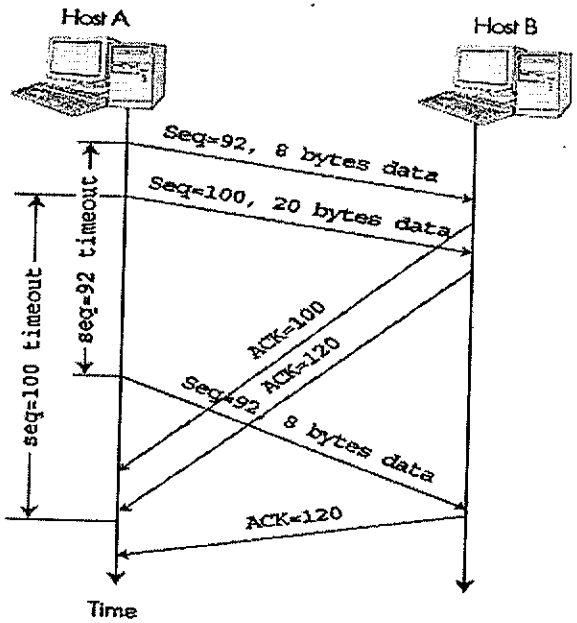

Hình 3.33 Truyền lại vì mất ACK

Chúng ta kết thúc trình bày ở đây để xem xét vài trường hợp đơn giản. Hình 3.33 mô tả trường hợp máy tính A gửi một segment tới máy tính B. Giả sử segment này có số thứ tự là 92 và có 8 byte dữ liệu. Sau khi gửi, máy A chờ segment ACK với giá trị biên nhận 100 từ máy B. Mặc dù segment gửi từ máy A đã đến máy B nhưng ACK gửi từ máy B đến máy A bị mất. Trong trường hợp này, khi hết thời gian đợi, máy A truyền lại một segment giống hệt cho B. Dĩ nhiên khi nhận được segment truyền lại, máy B sẽ phát hiện sự trùng lặp nhờ trường số thứ tự. Vì vậy thực thể TCP trên máy B sẽ loại bỏ segment truyền lại.



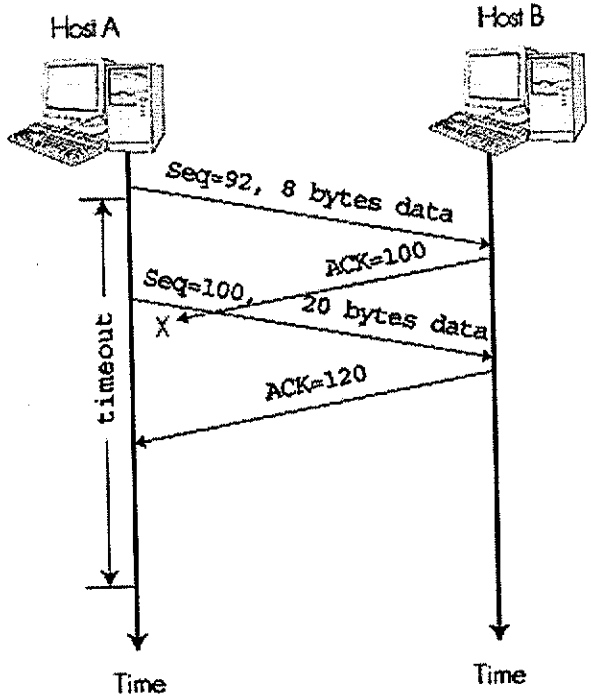
Trong trường hợp thứ hai, máy A gửi hai segment liên tiếp. Segment đầu tiên có số thứ tự là 92 và 8 byte dữ liệu, segment thứ hai có số thứ tự là 100 và 20 byte dữ liệu. Giả sử cả hai segment này đều đến máy B nguyên vẹn và máy B gửi biên nhận ACK riêng rẽ cho từng segment. ACK cho segment đầu tiên có số biên nhận là 100 và cho segment thứ hai là 120. Lại giả sử rằng cả hai ACK đều không đến được máy A trước khi hết thời gian đợi của segment đầu tiên. Khi hết thời gian đợi, máy A gửi lại segment đầu tiên có số thứ tự 92. Vậy máy A có gửi lại segment thứ hai không ? Theo quy tắc mô tả trên, máy A chỉ gửi lại segment thứ hai nếu hết thời gian đợi trước khi ACK có số biên nhận 120 hoặc lớn hơn đến. Vì vậy, như minh hoạ trên hình 3.33, nếu ACK thứ hai không mất và đến trước timeout của segment thứ hai thì máy A sẽ không phải gửi lại segment thứ hai .

Trong trường hợp thứ ba và cũng là trường hợp cuối cùng, giả sử máy tính A gửi hai segment giống như trong ví dụ hai. ACK của segment đầu tiên bị mất, nhưng trước khi hết thời gian đợi của segment đầu tiên, máy A nhận được ACK có số biên nhận 120 - do đó máy A hiểu rằng máy B đã nhận được tất cả các byte đến tận byte thứ 119, vì vậy máy A không phải gửi lại segment nào trong hai segment. Trường hợp này được minh hoạ trong Hình 3.34.




Hình 3.34 Segment không cần truyền lại vì ACK đến trước khi hết thời gian đợi

Mặc dù trong phần trước chúng ta đã nói TCP là giao thức kiểu Go-Back-N vì các giá trị biên nhận mang tính tích luỹ và bên nhận không biên nhận cho các segment đã nhận đúng nhưng không theo số thứ tự. Kết quả là (xem Hình 3.31 và Hình 3.18) TCP bên gửi chỉ cần ghi nhớ số thứ tự nhỏ nhất của byte đã được gửi nhưng chưa được biên nhận (**sendbase**) và số thứ tự cho byte tiếp theo sẽ được gửi đi (**nextseqnum**). Tuy nhiên cần lưu ý rằng mặc dù thành phần truyền dữ liệu tin cậy của TCP giống Go-Back-N, nhưng không phải giống hoàn toàn. Để phân biệt một số điểm khác nhau giữa TCP và Go-Back-N, chúng ta hãy xem điều gì sẽ xảy ra khi bên gửi gửi các segment liên tiếp 1, 2,..., N, tất cả segment này đều được nhận đúng thứ tự và không có lỗi. Giả sử ACK của segment n<N bị mất nhưng ACK của N-1 segment còn lại đến bên nhận trước khi hết thời gian đợi của từng segment. Trong trường hợp này, Go-Back-N sẽ truyền lại không chỉ packet n mà còn là tất cả những gói tin sau n+1, n+2, ..., N. TCP sẽ truyền lại nhiều nhất là segment thứ n. Thậm chí TCP sẽ không truyền lại segment thứ n nếu ACK cho segment thứ n+1 đến trước khi hết thời gian đợi (timeout) của segment thứ n.



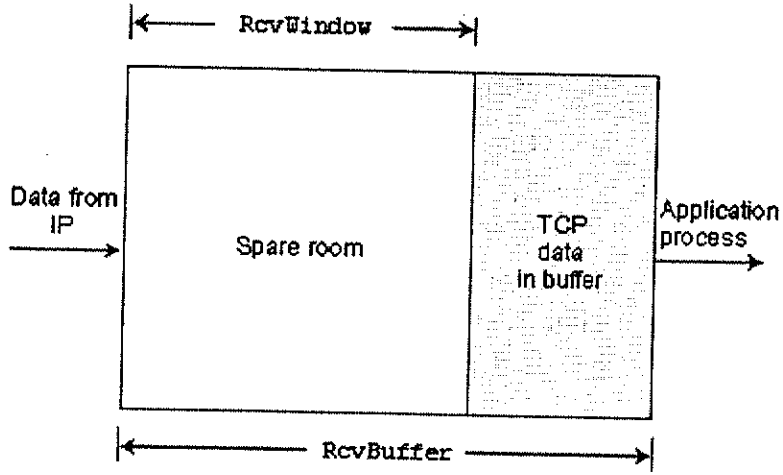

**Hình 3.35 ACK tích luỹ tránh việc truyền lại segment đầu tiên**



Gần đây có một số đề xuất [RFC 2018] mở rộng cơ chế biên nhận của TCP cho giống kiểu giao thức Selective Repeat. Ý tưởng chính trong những đề xuất này là cung cấp cho bên gửi những thông tin tường minh về segment nào đã được nhận đúng và segment nào chưa nhận được.

## 3.5.6 Kiểm soát lưu lượng

Nhắc lại rằng, thiết bị đầu cuối ở mỗi phía của kết nối TCP đều có bộ đệm dữ liệu (buffer). Khi nhận được đúng một dòng byte liên tục (đúng thứ tự), TCP sẽ đặt dòng byte này vào bộ đệm nhận (receive buffer). Tiến trình ứng dụng nhận sẽ đọc dữ liệu từ bộ đệm này, nhưng không nhất thiết là phải đọc ngay khi dữ liệu đến. Có thể tiến trình ứng dụng nhận phải thực hiện nhiều tác vụ khác nên chưa đọc ngay dữ liệu trong bộ đệm. Nếu ứng dụng đọc dữ liệu chậm thì bên gửi có thể làm tràn bộ đệm nhận do dữ liệu được gửi quá nhiều và quá nhanh. Chính vì lý do này TCP cung cấp dịch vụ **kiểm soát lưu lượng (flow control)** để tránh hiện tượng bên gửi làm tràn bộ đệm bên nhận. Kiểm soát lưu lượng là quá trình làm tương thích (matching) về tốc độ: tương thích giữa tốc độ gửi và tốc độ nhận . Như đã lưu ý ở phần trước, bên gửi TCP cũng bị giới hạn do tắc nghẽn trong mạng IP, đây chính là cơ chế **kiểm soát tắc nghẽn (congestion control)** của TCP. Mặc dù kiểm soát lưu lượng giống kiểm soát tắc nghẽn (hạn chế tốc độ gửi của bên gửi), tuy nhiên chúng được thực hiện với những mục đích khác nhau. Nhiều người coi hai thuật ngữ này tương đương nhau, vì vậy người đọc nên xem kỹ để phân biệt hai trường hợp.




**Hình 3.36 Biến receive window và bộ đệm nhận**

Để cung cấp cơ chế kiểm soát lưu lượng, TCP bên gửi sử dụng biến **receive window**. Đây là giá trị mà bên nhận báo cho bên gửi biết độ lớn vùng đệm còn rỗi của mình. Trong kết nối hai hướng, ở mỗi phía kết nối có một giá trị **receive window** riêng. Giá trị **receive window** thay đổi trong thời gian kết nối. Chúng ta hãy nghiên cứu giá trị receive window trong ví dụ truyền file. Giả sử máy A gửi một file lớn tới máy B qua kết nối TCP. Máy B sẽ khởi tạo bộ đệm cho kết nối này với độ lớn **RcvBuffer**. Tiến trình ứng dụng trên B đọc dữ liệu từ bộ đệm. Chúng ta định nghĩa một số biến sau:

**LastByteread** = số thứ tự của byte cuối cùng trong dòng dữ liệu mà tiến trình ứng dụng trong máy B đọc từ buffer

**LastByteRcvd** = số thứ tự byte cuối cùng trong dòng dữ liệu đến từ mạng và được để trong receive buffer trên máy B

Vì TCP không cho phép tràn bộ đệm nên:

**LastByteRcvd – LastByteread <= RcvBuffer**

Receive window là giá trị RcvWindow, là độ lớn vùng đệm rỗi:

**RcvWindow =RcvBuffer - [LastByteRcvd - LastByteread ]**

Bởi vì độ lớn vùng đệm rỗi thay đổi theo thời gian nên giá trị **RcvWindow** cũng biến đổi. Biến **RcvWindow** được minh hoạ trong Hình 3.35.

Kết nối sử dụng biến **RcvWindow** để cung cấp dịch vụ kiểm soát lưu lượng như thế nào? Máy B báo cho máy A độ lớn vùng rỗi trong bộ đệm của mình bằng cách đặt giá trị **RcvWindow** hiện thời vào trong trường **window** của tất cả các segment gửi tới A. Ban đầu máy B thiết lập **RcvWindow=RcvBuffer.** Rõ ràng để đạt được điều này thì máy B phải kiểm soát vài biến kết nối .

Máy A cũng có hai biến **LastByteSent** và **LastByteAcked**. Độ lệch giữa hai biến này, **LastByteSent – LastByteAcked** là số lượng dữ liệu chưa được biên nhận mà A gửi qua kết nối. Bằng cách khống chế số lượng dữ liệu chưa được biên nhận nhỏ hơn giá trị RcvWindow, A đảm bảo không làm tràn bộ đệm tại B. Do vậy trong suốt thời gian kết nối, A phải đảm bảo:

**LastByteSent – LastByteAcked ≤RcvWindow**



Một vấn đề kỹ thuật nhỏ nẩy sinh ở đây. Giả sử bộ đệm ở máy B đầy, có nghĩa là RcvWindow = 0. Sau khi thông báo tới máy A là RcvWindow = 0, máy B không có gì để gửi tới máy A. Khi tiến trình ứng dụng ở máy B lấy dữ liệu lên làm cho bộ đệm rỗng thì TCP không gửi segment mới cùng với giá trị RcvWindow mới tới máy A – TCP chỉ gửi segment tới A khi có dữ liệu hoặc ACK để gửi. Bởi vậy, máy A sẽ không bao giờ được thông báo đã có thêm khoảng trống trong bộ đệm ở B. Máy A bị "khoá" và không thể truyền thêm dữ liệu. Để giải quyết vấn đề này, đặc tả TCP yêu cầu máy A tiếp tục gửi segment với một byte dữ liệu khi receive window của máy B bằng 0. Những segment này sẽ được B biên nhận. Khi bộ đệm bắt đầu có vùng rỗng thì trong gói biên nhận sẽ có cả giá trị khác 0 của RcvWindow.

Khác TCP, UDP không có cơ chế kiểm soát lưu lượng. Để hiểu vấn đề này, chúng ta hãy xem thực thể UDP gửi các segment từ tiến trình trên máy A tới tiến trình trên máy B. UDP sẽ đặt các segment (chính xác hơn là dữ liệu trong segment) vào trong một hàng đợi có độ lớn hữu hạn ứng với socket nào đó ("cửa" của tiến trình). Tiến trình đọc lần lượt từng segment trong hàng đợi. Nếu tốc độ đọc của tiến trình không đủ nhanh thì hàng đợi bị tràn và các segment đến sau sẽ bị mất.

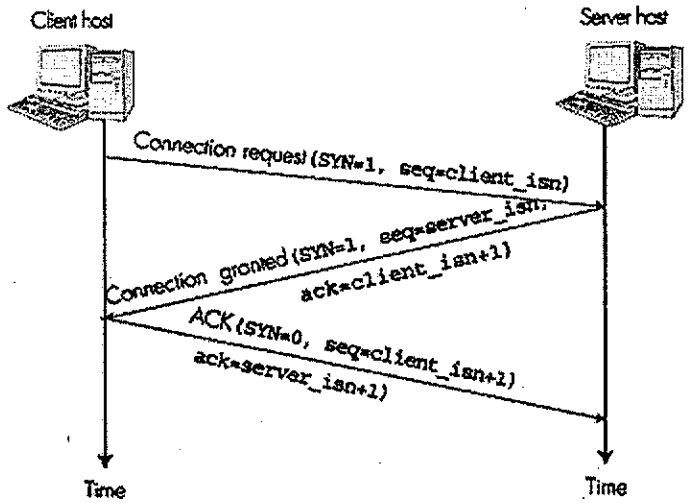
## 3.5.7 Quản lý kết nối TCP

Trong phần này chúng ta xem xét một kết nối TCP được thiết lập và giải phóng như thế nào. Mặc dù đây là vấn đề không hấp dẫn nhưng lại quan trọng bởi vì giai đoạn thiết lập kết nối TCP ảnh hưởng lớn đến độ trễ (chẳng hạn như khi duyệt Web). Bây giờ chúng ta xem một kết nối TCP được thiết lập như thế nào? Giả sử tiến trình chạy trên máy client muốn khởi tạo một kết nối tới tiến trình trên server. Đầu tiên tiến trình ứng dụng trên client yêu cầu thực thể TCP của nó (client) thiết lập một kết nối tới một tiến trình trên server. Sau đó thực thể TCP client khởi tạo kết nối TCP tới thực thể TCP trên server qua những bước sau:

**Bước 1:** Đầu tiên phía TCP client gửi một segment đặc biệt tới TCP server. Segment đặc biệt này không chứa dữ liệu của tầng ứng dụng nhưng cờ SYN (một bit thuộc trường cờ (flag)) trong phần tiêu đề được đặt giá trị bằng 1. Vì thế đôi khi segment đặc biệt này được gọi là SYN segment. Ngoài ra

TCP client chọn số thứ tự ban đầu (client_isn) và đặt giá trị này vào trường số thứ tự của SYN segment. Segment này được đặt trong IP datagram để gửi tới server.

**Bước 2**: Khi IP datagram chứa TCP segment đến server (nếu đến được) thì server lấy SYN segment ra khỏi datagram, phân phối bộ đệm và các biến TCP phục vụ kết nối đồng thời gửi đi một segment đặc biệt thông báo chấp nhận kết nối từ client. Segment này cũng không chứa dữ liệu của tầng ứng dụng. Tuy nhiên nó chứa ba thông tin quan trọng trong phần tiêu đề. Thứ nhất bit SYN sẽ được thiết lập giá trị 1. Thứ hai, trường biên nhận trong tiêu đề nhận giá trị client_isn+1. Cuối cùng, server chọn số thứ tự bắt đầu của mình (server_isn) và đặt giá trị này vào trường số thứ tự trong tiêu đề của segment. Với segment chấp nhận kết nối, server ngụ ý "đã nhận được từ client gói SYN yêu cầu thiết lập kết nối với số thứ tự bắt đầu từ client_isn. Chấp nhận thiết lập kết nối này. Số thứ tự của server bắt đầu từ server_isn". Đôi khi đây được gọi là SYNACK segment.

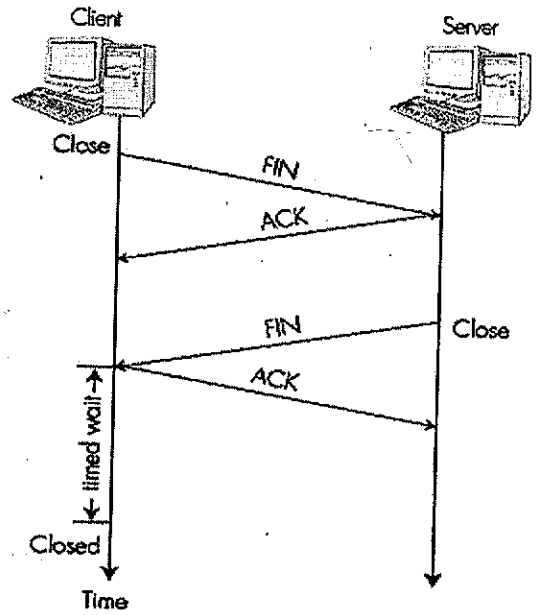



**Hình 3.37 Giai đoạn bắt tay ba bước trong thiết lập đường truyền của TCP**

**Bước 3**: Khi nhận được segment chấp nhận kết nối, client cũng khởi tạo bộ đệm và các biến phục vụ kết nối. Client gửi segment thứ ba biên nhận cho segment chấp nhận kết nối của server (bằng cách đặt giá trị server_isn+1 vào trường số biên nhận trong tiêu đề của TCP segment). Bit SYN được đặt giá trị 0 vì kết nối đã được thiết lập.



Sau khi thực hiện xong ba bước này thì client và server có thể trao đổi các segment chứa dữ liệu. Bit SYN trong các segment sau được đặt giá trị 0. Như vậy, để thiết lập được kết nối hai máy phải trao đổi ba segment (xem Hình 3.37). Vì thế thủ tục kết nối được xem là **quá trình bắt tay ba bước (three way handshake)**.

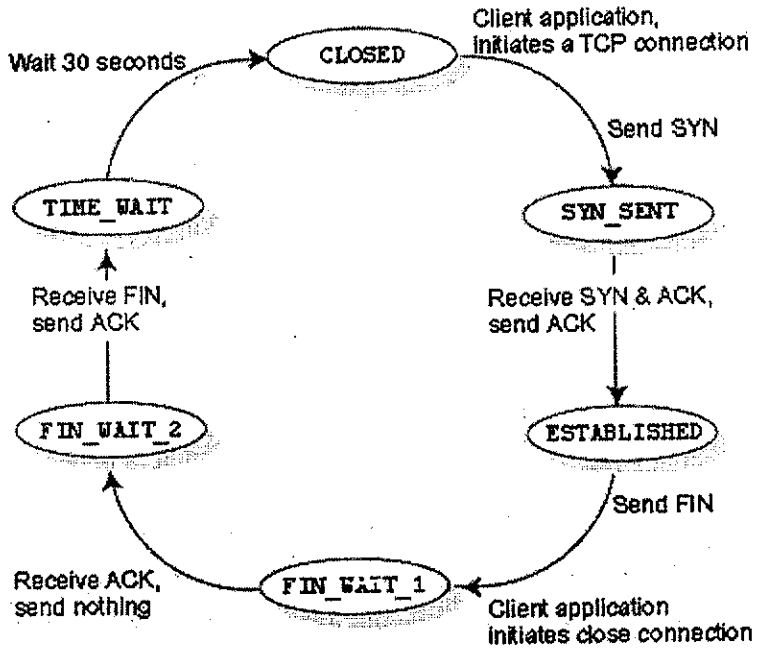



**Hình 3.38 Kết thúc kết nối TCP**

Bây giờ chúng ta xét đến việc đóng kết nối TCP. Cả hai tiến trình tham gia kết nối TCP đều có thể kết thúc kết nối. Khi kết nối đóng lại thì các tài nguyên phục vụ kết nối (bộ đệm và các biến TCP) trong máy được giải phóng. Ví dụ client quyết định đóng kết nối (Hình 3.38). Tiến trình ứng dụng client sẽ đưa ra lệnh đóng. Khi đó TCP client gửi một segment TCP đặc biệt đến tiến trình server. Đây là FIN segment vì cờ FIN trong segment này được đặt giá trị 1. Khi server nhận được segment FIN, nó sẽ gửi lại cho client một segment ACK biên nhận segment FIN của client. Kế tiếp server gửi lại một segment kết thúc FIN (có cờ FIN được đặt giá trị 1). Cuối cùng client gửi segment ACK biên nhận segment FIN của server. Tại thời điểm này thì tất cả tài nguyên trên hai máy đều được giải phóng.

Trong suốt thời gian kết nối TCP, giao thức TCP chạy trên mỗi máy chuyển qua các trạng thái TCP (TCP state). Hình 3.39 minh hoạ quá trình

thay đổi trạng thái TCP xảy ra bên phía client. TCP client bắt đầu ở trạng thái đóng (CLOSED). Ứng dụng bên phía client khởi tạo một kết nối TCP. Điều này đòi hỏi TCP client gửi SYN segment tới TCP server. Sau khi gửi SYN segment, TCP client chuyển sang trạng thái SYN_SENT. Trong trạng thái SYN_SENT, TCP client đợi SYNACK segment (biên nhận cho SYN segment của mình). Khi nhận được segment này, TCP client chuyển sang trạng thái ESTABLISHED. Ở trạng thái ESTABLISHED, TCP client có thể gửi và nhận TCP segment chứa dữ liệu (là dữ liệu thực sự do ứng dụng tạo ra).




**Hình 3.39 Dòng trạng thái của TCP**

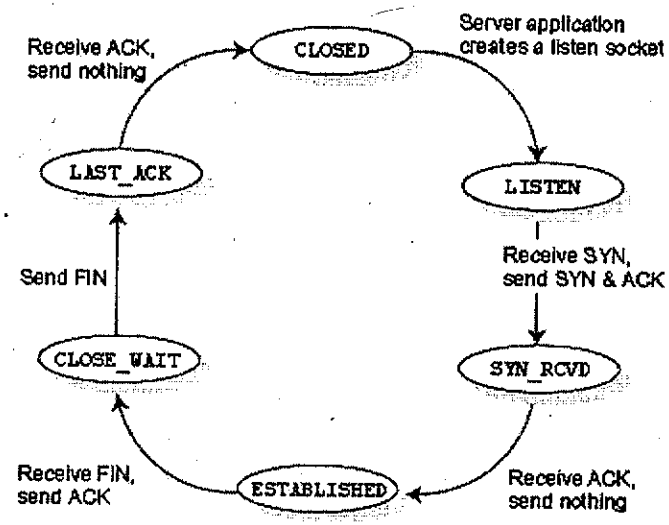
Giả sử ứng dụng client quyết định đóng kết nối (server tương tự). Khi đó TCP client gửi FIN segment và chuyển sang trạng thái FIN_WAIT_1. Trong trạng thái này, TCP client đợi segment biên nhận từ phía server. Sau khi nhận được segment này, TCP client chuyển sang trạng thái FIN_WAIT_2. Trong trạng thái FIN_WAIT_2, TCP client đợi FIN segment từ server. Sau khi nhận segment này, TCP client gửi segment ACK biên nhận tới server và chuyển sang trạng thái TIME_WAIT. Trong trạng thái TIME_WAIT, TCP client có thể gửi lại biên nhận ACK trong trường hợp ACK trước bị mất. Thời gian đợi ở trạng thái TIME_WAIT phụ thuộc



vào phần mềm triển khai TCP, nhưng thường nhận các giá trị 30 giây, một phút, hai phút. Sau khi hết thời gian đợi, kết nối chính thức được đóng và tất cả tài nguyên phía client (bao gồm cả số hiệu cổng) được giải phóng.

Hình 3.40 minh hoạ quá trình thay đổi trạng thái xảy ra ở TCP server. Giả sử client yêu cầu kết thúc trước.

Trong hai sơ đồ biến đổi trạng thái vừa nghiên cứu, chúng ta đã tìm hiểu về cơ chế thiết lập và giải phóng đường truyền của TCP.




**Hình 3.40 Các trạng thái của kết nối TCP**

## 3.6 KIỂM SOÁT TẮC NGHẼN TRONG TCP

Trong các phần trước, chúng ta đã nghiên cứu cách thức TCP cung cấp dịch vụ truyền tin tin cậy giữa hai tiến trình chạy trên những thiết bị đầu cuối khác nhau. Một dịch vụ cực kỳ quan trọng khác của TCP là cơ chế kiểm soát tắc nghẽn. Cơ chế này của TCP chỉ dựa vào các thiết bị đầu cuối chứ không dựa vào cơ chế kiểm soát tắc nghẽn của tầng mạng vì tầng IP không cung cấp cho TCP các thông tin minh bạch khi có tắc nghẽn. Trước khi đi sâu vào chi tiết, chúng ta hãy xem xét chung về cơ chế kiểm soát tắc nghẽn của TCP và mục tiêu kiểm soát tắc nghẽn của TCP khi nhiều kết nối TCP cùng chia sẻ một đường truyền bị tắc nghẽn.

Kết nối TCP kiểm soát tốc độ truyền của mình bằng cách giới hạn số lượng các segment đã gửi nhưng chưa được biên nhận. Định nghĩa w là số lượng cho phép các segment chưa cần biên nhận, thường được coi như **kích thước cửa sổ của TCP (TCP window)**. Lý tưởng là kết nối TCP cho phép truyền với tốc độ tối đa có thể (càng nhiều segment chưa biên nhận càng tốt) chừng nào chưa xảy ra hiện tượng mất segment do bị tắc nghẽn. Nói chung kết nối TCP bắt đầu với giá trị w tương đối nhỏ và sau đó "thăm dò" kênh truyền còn rỗi không bằng cách tăng dần giá trị w. Kết nối TCP tiếp tục được tăng w cho đến khi xảy ra mất dữ liệu (sự kiện hết thời gian đợi - timeout hay nhận được các biên nhận trùng lặp). Khi đó TCP sẽ giảm w tới một giá trị "an toàn" và sau đó lại bắt đầu "thăm dò" kênh truyền rồi bằng cách tăng dần giá trị w.

## Tổng quan về kiểm soát tắc nghẽn của TCP

Trong mục 3.5 chúng ta đã thấy mỗi kết nối TCP có bộ đệm gửi, bộ đệm nhận và một vài biến (LastByteRead, RcvWin...). Cơ chế kiểm soát tắc nghẽn của TCP bổ sung thêm hai biến nữa: **congestion window** (cửa sổ tắc nghẽn) và **threshold** (ngưỡng). Cửa sổ tắc nghẽn, ký hiệu là CongWin biểu thị số lượng dữ liệu tối đa mà người gửi có thể gửi qua kết nối. Như vậy khối lượng dữ liệu được gửi không được vượt quá CongWin và RcvWin, tức là:

Last ByteSent - LastByteAcked $\leq$ min {CongWin,RcvWin}.

Ngưỡng ký hiệu là **threshold** sẽ ảnh hưởng tới quá trình tăng của CongWin như trình bày dưới đây.

Chúng ta hãy xem giá trị CongWin tăng trong suốt kết nối TCP như thế nào. Để tập trung vào cơ chế kiểm soát tắc nghẽn (khác với kiểm soát lưu lượng), chúng ta giả thiết rằng bộ đệm nhận đủ lớn để có thể bỏ qua các hạn chế của cửa sổ nhận. Trong trường hợp này, số lượng dữ liệu gửi chưa cần được biên nhận chỉ bị giới hạn bởi CongWin. Chúng ta cũng giả thiết rằng phía gửi cần gửi nhiều dữ liệu.

Sau khi thiết lập kết nối TCP giữa hai hệ thống đầu cuối, tiến trình ứng dụng bên gửi chuyển dữ liệu tới bộ đệm gửi của TCP. TCP chia dữ liệu thành các khối với kích thước MMS, đặt các khối dữ liệu trong TCP



segment, và chuyển segment xuống tầng mạng để gửi đi. Cửa sổ tắc nghẽn của TCP điều tiết số lượng segment được gửi. Ban đầu, CongWin nhận giá trị 1 MMS, TCP gửi segment đầu tiên và được biên nhận. Nếu segment này được biên nhận trước khi timeout, phía gửi tăng CongWin lên 1 MMS và gửi đi hai segment. Nếu những segment này được biên nhận trong thời gian đợi của chúng, CongWin lại được tăng thêm 1 MMS cho mỗi segment được biên nhận. Khi đó CongWin mới là 4 MMS và phía gửi gửi đi bốn segment. Thủ tục này được thực hiện liên tục cho tới khi (1) CongWin vượt ngưỡng (threshold) hay (2) không nhận được biên nhận trong thời gian chờ biên nhận.

Trong giai đoạn này, cửa sổ tắc nghẽn (CongWin) tăng theo hàm số mũ. Ban đầu nó nhận giá trị 1 MSS, sau đó tăng lên 2 MMS, 4 MMS, 8 MMS.... Đây là giai đoạn **khởi đầu chậm (slow start)** vì giá trị cửa sổ khởi đầu với giá trị nhỏ (1 MMS). Tuy vậy giá trị cửa sổ tăng khá nhanh.

Giai đoạn slow-start kết thúc khi CongWin vượt ngưỡng. Khi đó giá trị CongWin sẽ tăng tuyến tính chứ không còn tăng theo hàm số mũ. Tức là nếu CongWin = w, sau khi nhận được biên nhận cho w segment, giá trị CongWin sẽ tăng lên 1, CongWin = w+1. Đây là giai đoạn **tránh tắc nghẽn (congestion avoidance)**.

Giai đoạn tránh tắc nghẽn tiếp tục khi vẫn nhận được biên nhận trong thời gian đợi. Tuy nhiên giá trị cửa sổ cũng như tốc độ gửi dữ liệu không thể tăng mãi. Đến lúc nào đó sẽ xảy ra sự cố mất gói dữ liệu ở router. Điều này dẫn đến sự kiện timeout ở phía gửi. Lúc này giá trị ngưỡng (threshold) nhận giá trị bằng một nửa CongWin, CongWin được đặt bằng 1 MMS. Bên gửi sẽ tiếp tục tăng nhanh giá trị CongWin theo hàm số mũ cho đến khi nó vượt ngưỡng.

Tóm lại:

Khi cửa sổ tắc nghẽn chưa vượt ngưỡng, cửa sổ sẽ tăng theo hàm mũ.

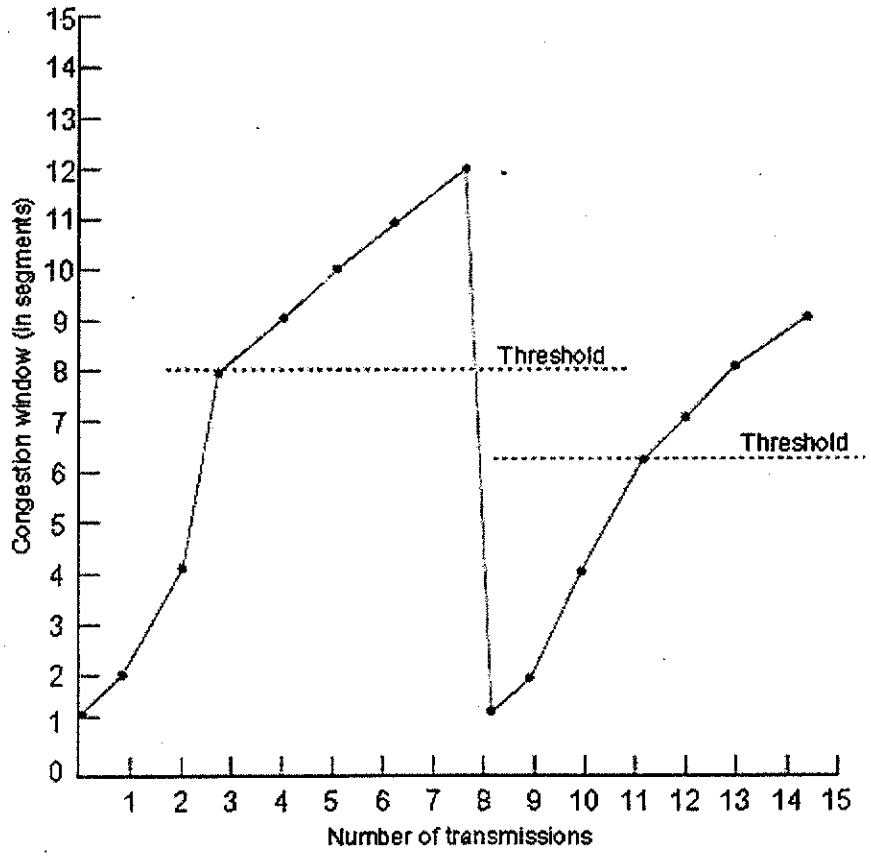
Khi cửa sổ tắc nghẽn vượt ngưỡng, cửa sổ sẽ tăng tuyến tính.

Khi hết thời gian đợi, giá trị ngưỡng bằng một nửa giá trị cửa sổ tắc nghẽn hiện thời và cửa sổ tắc nghẽn nhận giá trị 1.

Nếu bỏ qua giai đoạn slow-start, chúng ta sẽ thấy TCP tăng độ lớn cửa sổ theo cấp số cộng khi mạng chưa bị tắc nghẽn và giảm độ lớn cửa sổ

theo cấp số nhân (chia 2) ngay khi mạng bị tắc nghẽn. Vì vậy, TCP được coi là thuật toán **AIMD (additive-increase, multiplicative-decrease)**.

Giá trị độ lớn cửa sổ tắc nghẽn của TCP được minh hoạ trong Hình 3.41. Trong hình này, ngưỡng ban đầu bằng 8 MSS. Cửa sổ tắc nghẽn tăng nhanh theo luỹ thừa 2 trong giai đoạn slow-start và đạt ngưỡng tại t=3. Giá trị cửa sổ tắc nghẽn tăng tuyến tính đến khi xuất hiện mất mát dữ liệu. Giả sử khi dữ liệu bị mất, cửa sổ tắc nghẽn có giá trị 12 MMS. Ngưỡng mới được đặt bằng 0.5 CongWin = 6 MSS và cửa sổ tắc nghẽn bằng 1 MMS. Quá trình lại được tiếp tục. Thuật toán kiểm soát tắc nghẽn này do V.Jacobson đề xuất. Hiện nay có nhiều biến thể của thuật toán Jacobson (xem RFC 2581).




**Hình 3.41 Cửa sổ kiểm soát tắc nghẽn**



## Tahoe, Reno và Vegas

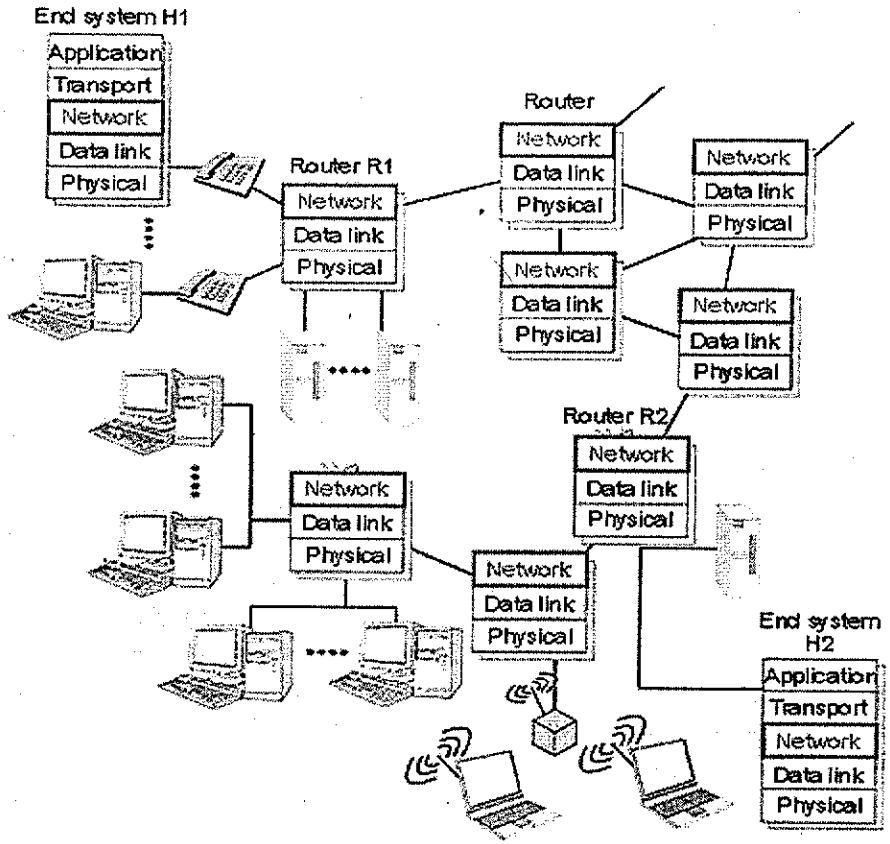
Thuật toán kiểm soát tắc nghẽn của TCP ở đây được gọi là **Tahoe**. Một vấn đề với thuật toán Tahoe là khi một segment bị mất, người gửi có thể phải đợi trong một khoảng thời gian dài để gửi lại. Vì vậy một biến thể của Tahoe gọi là **Reno** đã được triển khai trong phần lớn các hệ điều hành. Giống Tahoe, Reno đặt độ lớn cửa sổ tắc nghẽn bằng 1 khi timeout (hết thời gian của bộ định thời). Tuy nhiên Reno có cơ chế truyền lại nhanh mà chúng ta đã khảo sát trong mục 3.5. Phía gửi sẽ gửi lại gói tin đã nhận được biên nhận trùng lặp ba lần liên tiếp ngay cả khi chưa hết thời gian đợi của gói tin này. Reno cũng sử dụng cơ chế khôi phục nhanh (fast recovery). Hiện nay phần lớn thực thể TCP sử dụng thuật toán Reno. Tuy nhiên có nhiều thuật toán cải tiến đáng kể hiệu suất của Reno – như **Vegas**.

# Chương 4
# TẦNG MẠNG

## 4.1 CÁC MÔ HÌNH DỊCH VỤ CỦA TẦNG MẠNG

Như đã trình bầy trong chương trước, tầng giao vận cung cấp dịch vụ truyền thông giữa hai tiến trình đang chạy trên hai máy tính khác nhau. Để cung cấp được dịch vụ này, tầng giao vận phải sử dụng dịch vụ cung cấp đường truyền giữa hai máy tính của tầng mạng. Nói cụ thể hơn, tầng mạng chuyển gói tin (segment) của tầng giao vận từ máy tính này đến máy tính khác. Tại máy tính gửi, tất cả các segment của tầng giao vận được chuyển xuống tầng mạng. Nhiệm vụ của tầng mạng là chuyển những segment này đến máy tính đích và gửi tới thực thể nào đó ở tầng giao vận bên trên. Công việc chuyển segment từ tầng giao vận máy tính nguồn đến tầng giao vận máy tính đích của tầng mạng chính là nội dung của chương này. Chúng ta sẽ thấy rằng không giống tầng giao vận, tầng mạng gồm nhiều máy tính và các router trung gian. Vì thế, giao thức tầng mạng là một trong những giao thức phức tạp nhất.






**Hình 4.1 Một mô hình mạng đơn giản**

Hình 4.1 minh hoạ một mạng đơn giản với hai máy tính (H1 và H2) và một số router trên đường truyền giữa H1 và H2. Tầng mạng ở máy tính gửi thực hiện bước gửi đầu tiên trên toàn bộ hành trình của gói tin. Ví dụ nếu H1 gửi gói tin đến H2 thì tầng mạng trên H1 sẽ truyền gói tin này đến router gần nhất: R2. Tại máy tính nhận (chẳng hạn H2), tầng mạng sẽ nhận gói tin từ router gần nó nhất (trong trường hợp này là R2) và chuyển lên cho tầng giao vận tại H2. Vai trò chính của router là chuyển gói tin từ một đầu vào nào đó (input) tới một đầu ra nào đó (output). Chú ý rằng các tầng trên của tầng mạng (giao vận, ứng dụng) không hoạt động tại các router trong Hình 4.1 bởi vì router không cần thiết phải chạy các giao thức ở tầng giao vận hay tầng ứng dụng (ngoại trừ các mục đích kiểm soát).

Vai trò của tầng mạng đơn giản chỉ là chuyển gói tin từ máy tính gửi đến máy tính nhận. Vì thế, tầng mạng có ba chức năng quan trọng sau đây:

*Xác định đường đi (Path determination)*: Tầng mạng phải xác định các router trung gian hay tuyến đường (path) mà gói tin được truyền từ nơi gửi đến nơi nhận. Thuật toán xác định tuyến đường như vậy gọi là "**thuật toán định tuyến**" (routing algorithm). Thuật toán định tuyến sẽ quyết định đường đi của các gói tin từ máy tính nhận đến máy tính gửi (trong ví dụ là máy tính H1 và máy tính H2). Trọng tâm của chương này là các thuật toán định tuyến. Trong phần 4.2, chúng ta sẽ nghiên cứu lý thuyết của thuật toán định tuyến, tập trung vào hai kiểu thuật toán: *Link state* và *Distance vector*. Chúng ta sẽ thấy độ phức tạp của thuật toán định tuyến phụ thuộc vào số lượng router trên đường truyền. Điều này dẫn đến định tuyến phân cấp, một chủ đề được trình bày trong phần 4.3.

***Chuyển mạch (Switching)***: Khi gói tin đến đầu vào, router phải quyết định gửi gói tin đến đầu ra thích hợp nào. Ví dụ, gói tin từ máy H1 đến router R1 sẽ phải được chuyển đến router kế tiếp trên đường tới H2. Trong phần 4.6 chúng ta sẽ nghiên cứu hoạt động của router và quá trình chuyển một gói tin từ đầu vào đến đầu ra trong một router diễn ra như thế nào.

***Thiết lập đường truyền (Call setup)***: Trong phần trước trình bày về TCP, chúng ta thấy rằng hai thực thể truyền thông phải có một giai đoạn "bắt tay" trước khi trao đổi dữ liệu thực sự. Điều này cho phép bên gửi và bên nhận thiết lập các thông tin trạng thái cần thiết (ví dụ, số thứ tự khởi đầu, độ lớn cửa sổ). Với một số kiến trúc mạng khác (ví dụ ATM) đòi hỏi các router trên tuyến đường từ nguồn đến đích phải "bắt tay" nhau trước khi bắt đầu truyền dữ liệu thực sự. Trong tầng mạng, quá trình này được gọi là thiết lập đường truyền (*call setup*). Chúng ta sẽ thấy tầng mạng trong kiến trúc Internet không đòi hỏi công việc này.

Tuy nhiên, trước khi đi sâu vào chi tiết các khái niệm và triển khai của tầng mạng, chúng ta sẽ xem xét tổng quát những kiểu dịch vụ khác nhau của tầng mạng.

### 4.1.1 Mô hình dịch vụ mạng

Khi tầng giao vận ở thiết bị gửi chuyển các gói tin xuống tầng mạng, liệu tầng giao vận có thể tin cậy tầng mạng chuyển gói tin này đến đích không? Liệu khi gửi nhiều gói tin, chúng có được chuyển đến tầng giao vận của thiết bị nhận theo đúng thứ tự không ? Vận tốc gửi các gói tin có được xác định trước không? Tầng mạng có phản hồi lại các thông tin liên quan đến tắc nghẽn không? Mô hình dịch vụ mạng sẽ trả lời những câu hỏi này và nhiều vấn đề khác.



**Chuyển mạch gói (datagram) và chuyển mạch ảo (virtual circuit)**

Có lẽ điểm trừu tượng quan trọng nhất mà tầng mạng che dấu các tầng trên là việc có sử dụng **mạch ảo (Virtual Circuit - VC)** hay không. Về khía cạnh nào đó mạch ảo tương tự mạng điện thoại truyền thống (mặc dù mạng điện thoại sử dụng mạch thực). Có ba giai đoạn trong chuyển mạch ảo:

***Thiết lập mạch ảo***: trong cả giai đoạn thiết lập, phía gửi thông báo địa chỉ nhận với tầng mạng, yêu cầu tầng mạng thiết lập VC. Tầng mạng xác định tuyến đường giữa bên gửi và bên nhận, tức là chuỗi các cung đường (hay đường kết nối - link) cũng như các thiết bị chuyển mạch (switch – nút trung gian) mà tất cả các gói dữ liệu sẽ đi qua. Giai đoạn này yêu cầu việc cập nhật bảng định tuyến và dự trữ tài nguyên trong mỗi thiết bị chuyển mạch.

***Truyền dữ liệu***: Sau khi thiết lập, dữ liệu có thể được chuyển trong VC.

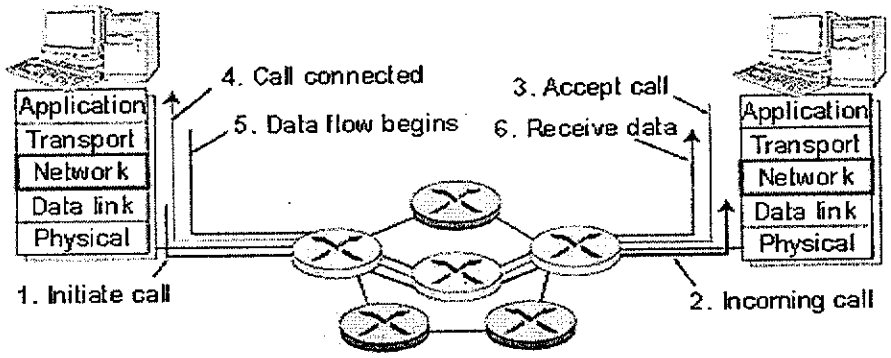
***Giải phóng mạch ảo***: Giai đoạn này bắt đầu khi phía gửi (hoặc phía nhận) báo cho tầng mạng yêu cầu đóng VC. Tầng mạng sẽ thông báo cho thiết bị đầu cuối bên kia cũng như các thiết bị chuyển mạch trên VC để cập nhật lại các bảng định tuyến, giải phóng tài nguyên.

Có sự khác biệt tuy nhỏ - nhưng quan trọng giữa thiết lập VC ở tầng mạng và thiết lập kết nối ở tầng giao vận (giai đoạn bắt tay 3 bước của TCP). Thiết lập kết nối ở tầng giao vận chỉ liên quan đến các thiết bị đầu cuối ở trên hai đầu mút. Hai thiết bị đồng ý thiết lập kết nối và thoả thuận các thông số của kết nối (ví dụ số thứ tự khởi tạo, độ lớn cửa sổ kiểm soát lưu lượng). Hai thiết bị đầu cuối này sẽ nhận biết được về sự kết nối ở tầng giao vận, nhưng các thiết bị chuyển mạch ở giữa thì không. Trái lại trong tầng mạng của mạng chuyển mạch ảo, tất cả các thiết bị chuyển mạch giữa hai thiết bị đầu cuối đều tham gia vào quá trình thiết lập mạch ảo, và do đó đều nhận biết được tất cả các VC đi qua.

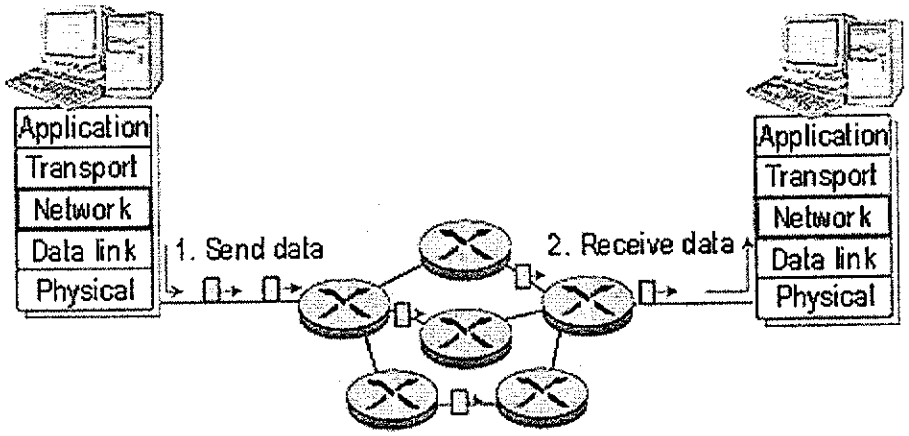
Thông điệp trao đổi giữa các thiết bị đầu cuối yêu cầu khởi tạo hay kết thúc mạch ảo hay thông điệp trao đổi giữa các thiết bị chuyển mạch yêu cầu thiết lập VC (để cập nhật bảng chuyển mạch) được gọi là **thông điệp báo hiệu (signaling message)**. Giao thức được sử dụng để trao đổi những thông điệp này là **giao thức báo hiệu (signaling protocol)**. Quá trình thiết lập VC được minh hoạ trong Hình 4.2. ATM, Frame Relay và X.25 là ba kiến trúc mạng sử dụng chuyển mạch ảo.

Trong mạng chuyển mạch gói, khi muốn gửi gói tin, thiết bị đầu cuối đặt vào gói tin địa chỉ thiết bị nhận và sau đó chuyển gói tin

vào mạng. Như minh hoạ trong Hình 4.3, không có giai đoạn thiết lập VC nào. Những thiết bị trung chuyển trong mạng chuyển mạch gói (được gọi là bộ định tuyến - router trên Internet) không duy trì bất kỳ trạng thái nào về VC vì không có VC. Thiết bị trung chuyển sẽ định tuyến gói tin đến đích bằng cách xác định địa chỉ đích, tìm kiếm trên bảng định tuyến và chuyển tiếp gói tin theo hướng đến đích (giống việc chuyển thư bình thường trong hệ thống bưu điện). Vì bảng định tuyến có thể được cập nhật liên tục, nên các gói tin được gửi từ thiết bị đầu cuối này đến thiết bị đầu cuối khác có thể đi theo nhiều tuyến đường khác nhau và đến đích không theo thứ tự. Mạng Internet công cộng ngày nay sử dụng dịch vụ chuyển mạch gói.




**Hình 4.2 Mô hình dịch vụ chuyển mạch ảo**




**Hình 4.3 Mô hình chuyển mạch gói**



Để chuyển gói tin của tầng giao vận, tầng mạng thường đưa ra dịch vụ chuyển mạch ảo hoặc dịch vụ chuyển mạch gói nhưng không bao giờ cung cấp cả hai dịch vụ này. Ví dụ, dịch vụ của mạng ATM là VC trong khi mạng Internet cung cấp dịch vụ chuyển mạch gói.

Một thuật ngữ tương đương của mạch ảo (VC) và mạch gói (Datagram) tương ứng là dịch vụ hướng nối (connection-oriented) và dịch vụ không hướng nối (connectionless). Dịch vụ chuyển mạch ảo được xếp vào lớp dịch vụ hướng nối vì phải thiết lập và kết thúc kết nối cũng như việc duy trì thông tin trạng thái của kết nối tại tất cả thiết bị chuyển mạch. Dịch vụ chuyển mạch gói được xếp vào lớp dịch vụ không hướng nối. Cả hai nhóm thuật ngữ đều có ưu điểm cũng như nhược điểm và đều được sử dụng phổ biến trong các tài liệu về mạng. Trong quyển sách này, chúng ta sử dụng thuật ngữ "dịch vụ chuyển mạch ảo" và "dịch vụ chuyển mạch gói" cho tầng mạng và sử dụng thuật ngữ "dịch vụ hướng nối" và "dịch vụ không hướng nối" cho tầng giao vận. Điểm khác biệt này sẽ giúp người đọc hiểu được những dịch vụ khác nhau của 2 tầng này.

Bảng 4.1 tổng kết những nét chính của mô hình dịch vụ Internet và kiến trúc mạng ATM. Chúng ta không đi sâu vào những khía cạnh chi tiết của mô hình dịch vụ ở đây. Kiến trúc hiện nay của Internet chỉ cung cấp duy nhất dịch vụ chuyển mạch gói, một dịch vụ theo kiểu **cố gắng tối đa (best-effort)**. Như minh hoạ trong bảng 4.1, dịch vụ này cũng giống với việc không cung cấp bất kỳ dịch vụ nào cả.

| Kiến trúc mạng | Mô hình dịch vụ | Đảm bảo băng thông | Đảm bảo không mất | Thứ tự | Độ trễ | Kiểm soát tắc nghẽn |
|---|---|---|---|---|---|---|
| Internet | Cố gắng tối đa | Không | Không | Không | Không | Không |
| ATM | CBR | Có | Có | Có | Có | Không có tắc nghẽn |
| ATM | VBR | Có | Có | Có | Có | Không có tắc nghẽn |
| ATM | ABR | Bảo đảm tốc độ nhỏ nhất | Không | Có | Có | Không có tắc nghẽn |
| ATM | UBR | Không | Không | Có | Có | Không |

**Bảng 4. 1**

Mạng không đảm bảo thời gian gửi các gói tin giống nhau, các gói tin không được đảm bảo đến đích theo đúng thứ tự, và thậm chí không đảm bảo gói tin đến được đích. Với định nghĩa này, một mạng không chuyển bất kỳ gói tin nào đến đích cũng được phân loại theo kiểu cố gắng tối đa (ví dụ mạng Internet công cộng hay bị tắc nghẽn).

Chúng ta hãy chuyển sang mô hình dịch vụ ATM. Ở đây, chúng ta sẽ tập trung vào mô hình dịch vụ đã được Diễn đàn ATM [ATM Forum] chuẩn hoá. Kiến trúc ATM cung cấp nhiều kiểu dịch vụ khác nhau (tức là chuẩn ATM có nhiều mô hình dịch vụ). Trong phạm vi cùng một mạng, những kết nối khác nhau có thể được cung cấp những lớp dịch vụ khác nhau.

**Dịch vụ truyền với tốc độ cố định - Constant bit rate (CBR)**: là mô hình dịch vụ ATM đầu tiên được chuẩn hoá, ở đây có thể thấy được vai trò các công ty điện thoại đằng sau ATM. Dịch vụ mạng CBR là sự lựa chọn lý tưởng cho việc truyền dữ liệu đa phương tiện (ví dụ điện thoại số) theo thời gian thực với tốc độ truyền cố định. Mục tiêu của dịch vụ CBR là làm cho kết nối mạng trông giống như một đường kết nối thực sự (bằng dây đồng hay cáp quang) giữa bên gửi và bên nhận. Trong dịch vụ CBR, các gói tin ATM (trong thuật ngữ ATM là các **tế bào ATM – ATM cell**) được truyền qua mạng với một độ trễ nào đó (được gọi là cell transfer delay, CTD). Biến thiên của độ trễ ( "jitter" hay cell – delay variation, CDV), tỷ lệ các cell bị mất hay đến trễ (cell – lost rate, CLR) được đảm bảo không vượt quá một giá trị ngưỡng. Tốc độ truyền tối đa của mỗi kết nối được xác định trước (pick cell rate, PCR) và bên gửi có thể gửi dữ liệu với tốc độ này. Các giá trị PCR, CTD, CDV và CLR đã được máy tính gửi và mạng ATM thoả thuận trước trong giai đoạn thiết lập kết nối CBR.

Lớp dịch vụ ATM thứ hai là **dịch vụ truyền với tốc độ không xác định (Unspecified bit rate - UBR)**. Không giống dịch vụ CBR (đảm bảo tốc độ, độ trễ, mất mát dữ liệu), UBR không đảm bảo những điều này ngoại trừ việc gửi các cell theo đúng thứ tự. Như vậy dịch vụ UBR giống mô hình dịch vụ cố gắng tối đa của Internet. Dịch vụ UBR không cung cấp thông tin phản hồi cho bên gửi về việc các cell có đến được đích hay không. Với mạng UBR, tính tin cậy của truyền dữ liệu được triển khai trong các giao thức ở tầng cao hơn. Dịch vụ UBR phù hợp với những ứng dụng truyền dữ liệu không cần tốc độ truyền cố định như email, newsgroup.



Nếu UBR được xem như một dịch vụ theo kiểu cố gắng tối đa thì **dịch vụ truyền với tốc độ có sẵn (available rate bit - ABR)** có thể phân loại vào nhóm dịch vụ theo kiểu cố gắng tối đa nhưng ưu việt hơn. Hai tính năng bổ sung quan trọng nhất của dịch vụ ABR là:

Tốc độ truyền cell nhỏ nhất (MRC) được đảm bảo cho kết nối ABR. Tuy nhiên, khi tài nguyên của mạng rỗi, bên gửi có thể gửi với tốc độ cao hơn MCR.

Có phản hồi về tắc nghẽn từ tầng mạng. Mạng ATM có thể cung cấp thông tin phản hồi cho bên gửi (là bit thông báo tắc nghẽn hay tốc độ gửi thấp) để bên gửi điều chỉnh tốc độ gửi.

ABR không đảm bảo một băng thông tối thiểu, nhưng cố gắng truyền dữ liệu nhanh nhất có thể. Như vậy, ABR phù hợp với các ứng dụng truyền dữ liệu yêu cầu độ trễ nhỏ (ví dụ duyệt Web).

Mô hình ATM cuối cùng là **dịch vụ truyền với tốc độ biến đổi (variable bit rate - VBR)**. Trong dịch vụ VBR thời gian thực, tỷ lệ mất gói dữ liệu, độ trễ có thể chấp nhận được thỏa thuận trước giống dịch vụ CBR. Tuy nhiên, tốc độ gửi thực sự được phép thay đổi theo các tham số do người dùng đưa vào. Điều này cho phép sử dụng tài nguyên có hiệu quả hơn, nhưng xét theo các tiêu chí về mất mát dữ liệu, độ trễ thì VBR tương tự CBR.

Có thể tìm hiểu kỹ hơn về ATM trong ATM Forum's Traffic Management Specification 4.0 [ATM Forum 1996].

## 3.1.2 Nguồn gốc của dịch vụ chuyển mạch gói và chuyển mạch ảo

Lịch sử phát triển mô hình dịch vụ mạng Internet và ATM phản ánh nguồn gốc của chúng. Với khái niệm trọng tâm là mạch ảo và dịch vụ CBR là dịch vụ đầu tiên, ATM rõ ràng xuất phát từ mạng điện thoại truyền thống (sử dụng "mạch thực"). Các định nghĩa sau này về lớp dịch vụ UBR và ABR đã ghi nhận tầm quan trọng của việc phát triển các ứng dụng truyền dữ liệu. Với kiến trúc VC và trọng tâm hỗ trợ truyền dữ liệu theo thời gian thực cùng

với sự bảo đảm về hiệu năng hệ thống (thậm chí kể cả với dịch vụ ABR), tầng mạng phức tạp hơn rất nhiều so với mô hình Internet theo kiểu cố gắng tối đa. Mạng điện thoại đặt tính phức tạp vào bên trong mạng vì mạng này kết nối các thiết bị đầu cuối câm (dump device), ví dụ các máy điện thoại quay số.

Ngược lại mạng toàn cầu Internet phát sinh từ nhu cầu kết nối các máy tính (được xem là thiết bị đầu cuối thông minh) với nhau. Với thiết bị đầu cuối phức tạp, kiến trúc Internet lựa chọn mô hình dịch vụ mạng đơn giản nhất có thể và đặt các chức năng phụ trợ (ví dụ như truyền dữ liệu tin cậy), cũng như các ứng dụng mạng ở tầng cao hơn triển khai trên các thiết bị đầu cuối. Điều này ngược với mô hình mạng điện thoại, và kết quả là: Mô hình dịch vụ mạng của Internet không đảm bảo bất kỳ một dịch vụ nào do vậy có thể dễ dàng kết nối các mạng sử dụng những công nghệ kết nối rất khác nhau (ví dụ vệ tinh, Ethernet, cáp quang, sóng vô tuyến). Các công nghệ này có tốc độ và tỷ lệ mất mát dữ liệu khác nhau. Kết nối các mạng IP được thảo luận chi tiết trong mục 4.4.

Như chúng ta đã thấy trong chương 2, những ứng dụng như thư điện tử, Web, và thậm chí cả dịch vụ của tầng mạng như DNS được triển khai trên các máy tính (là thiết bị đầu cuối). Các dịch vụ mới có thể nhanh chóng được sử dụng rộng rãi thông qua các giao thức tầng ứng dụng.

Tuy nhiên có sự tranh cãi lớn trong cộng đồng Internet về việc cải tiến kiến trúc của tầng mạng để hỗ trợ các ứng dụng đa phương tiện thời gian thực.

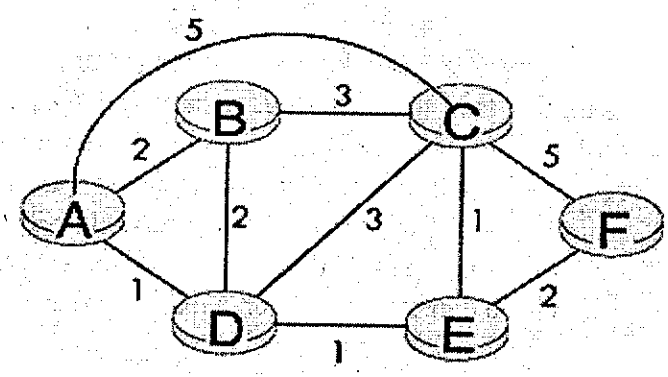
## 4.2 CÁC NGUYÊN LÝ ĐỊNH TUYẾN

Để truyền gói dữ liệu từ máy tính gửi đến máy tính nhận, tầng mạng phải quyết định đường đi hoặc các router mà gói dữ liệu phải đi qua. Dù mạng chuyển mạch gói (các gói tin khác nhau có thể đi theo các tuyến đường khác nhau) hay mạng mạch ảo (tất cả các gói tin được truyền trên cùng một tuyến đường định trước) thì tầng mạng đều phải xác định đường đi cho gói tin. Đây là công việc của các giao thức định tuyến ở tầng mạng.



Trái tim của giao thức định tuyến là thuật toán xác định đường đi cho gói tin – thuật toán định tuyến. Mục tiêu của thuật toán định tuyến hết sức đơn giản: với một tập hợp router cùng với liên kết giữa các router, thuật toán định tuyến phải xác định đường đi tốt nhất từ thiết bị nguồn đến thiết bị đích. Đường đi tốt đơn giản có thể là đường đi có giá nhỏ nhất. Tuy nhiên trong thực tế chúng ta sẽ thấy các vấn đề liên quan đến chính sách (policy) – ví dụ router X thuộc tổ chức Y không được chuyển tiếp các gói tin được tạo ra từ mạng của tổ chức Z-có thể làm phức tạp các thuật toán của router lên nhiều.

Người ta thường sử dụng đồ thị để xây dựng các thuật toán định tuyến như minh hoạ trên Hình 4.3. Trong chương này chúng ta sử dụng kỹ thuật biểu diễn sơ đồ mạng dưới dạng đồ thị. Ở đây, nút (node) của đồ thị biểu diễn router - điểm quyết định việc định tuyến gói tin - và những đoạn thẳng ("cung" trong lý thuyết đồ thị) nối các nút biểu diễn đường truyền vật lý thực sự giữa các router. Cung được đặc trưng bởi đại lượng "giá" (cost) là chi phí của việc gửi gói tin qua đường truyền tương ứng. Giá có thể phản ánh mức tắc nghẽn trên đường truyền (thời gian trễ trung bình) hoặc khoảng cách vật lý thực sự giữa hai router (ví dụ, đường truyền xuyên đại dương sẽ có giá cao hơn đường truyền giữa các khu vực trên đất liền). Để đơn giản, chúng ta coi mỗi cung trên đồ thị có một giá và không quan tâm đến việc xác định giá bằng cách nào.




**Hình 4.4 Ví dụ một mô hình mạng**

Với mô hình đồ thị, vấn đề tìm kiếm tuyến đường từ nguồn đến đích có chi phí thấp nhất yêu cầu xác định chuỗi các cung sao cho:

- Cung đầu tiên trong chuỗi xuất phát từ nguồn.
- Đích của cung cuối cùng trong chuỗi là đích.
- Với mọi i, cung thứ i và i-1 cùng kết nối vào một nút.

Với đường đi có giá nhỏ nhất, tổng chi phí tất cả các cung trên tuyến đường là nhỏ nhất. Chú ý nếu tất cả các cung có giá như nhau thì đường đi có giá nhỏ nhất cũng là đường đi ngắn nhất giữa nguồn và đích.

Ví dụ như trong Hình 4.4, đường đi có giá nhỏ nhất giữa nút A (nguồn) và nút C (đích) là đường ADEC.

Một bài tập đơn giản: hãy trình bày cách tìm đường đi có giá thấp nhất từ A đến F. Phần lớn mọi người sẽ tìm bằng cách kiểm tra Hình 4.3, lần theo các router từ A đến F qua nhiều con đường và tự thuyết phục rằng đường đi mà mình chọn có giá nhỏ nhất so với tất cả các đường khác. (Có tất cả 12 tuyến đường khác nhau nối A và F). Quá trình xác định như thế là ví dụ của thuật toán định tuyến tập trung - chạy trong bộ não của bạn với đầy đủ thông tin về mạng. Nói chung, chúng ta có thể phân loại thuật toán định tuyến vào hai kiểu: toàn cục hay phân tán.

**Thuật toán định tuyến toàn cục (global)** xác định đường đi với giá thấp nhất giữa nguồn và đích bằng cách sử dụng tất cả thông tin về tổng thể mạng. Đầu vào của thuật toán là tất cả các nút, cung và giá của các cung. Rõ ràng router phải bằng một cách nào đó thu được các thông tin này trước khi bước vào giai đoạn tính toán thực sự. Thuật toán có thể được chạy tại một nơi (thuật toán định tuyến tập trung) hoặc chạy tại nhiều nơi. Tuy nhiên điểm phân biệt chính yếu là thuật toán định tuyến toàn cục phải có trước đầy đủ thông tin về đồ thị mạng. Trong thực tế, thuật toán như vậy được gọi là thuật toán **link state** vì thuật toán phải biết được giá của mỗi liên kết trên mạng. Chúng ta sẽ nghiên cứu thuật toán global link state trong mục 4.2.1.

Trong **thuật toán phân tán**, xác định đường đi có giá thấp nhất được thực hiện dần dần theo cách thức phân tán. Không nút nào có đầy đủ thông tin về giá của tất cả các liên kết trên mạng. Ban đầu mỗi nút chỉ biết về giá của các cung có kết nối trực tiếp với nó. Sau đó, thông qua các bước tính toán và trao đổi thông tin với các nút hàng xóm (hai nút được gọi là hàng xóm nếu giữa chúng có một đường kết nối vật lý trực tiếp và trong



thuật ngữ đồ thị gọi là hai đỉnh kề nhau), nút sẽ dần dần xác định được đường đi có giá nhỏ nhất đến một tập hợp đích nào đó. Chúng ta sẽ nghiên cứu thuật toán định tuyến phân tán - thuật toán **distance vector** trong mục 4.2.2. Được gọi là thuật toán distance vector bởi vì nút không biết được đường đi cụ thể đến đích mà chỉ biết đến nút hàng xóm trên đường đến đích và tổng giá của đường đi đến đích.

Một kiểu phân loại thuật toán thứ hai là theo tính chất tĩnh hay động. Trong thuật toán định tuyến tĩnh, tuyến đường thay đổi rất ít theo thời gian, thường là kết quả do con người tác động (ví dụ đặt lại cấu hình cho bảng định tuyến trong router). Thuật toán định tuyến động cho phép thay đổi các tuyến đường khi lưu lượng mạng hay kiến trúc liên kết mạng bị thay đổi. Thuật toán động có thể được chạy định kỳ hoặc gửi thông điệp trực tiếp khi cấu trúc mạng hay giá các cung bị thay đổi. Thuật toán động có thể xử lý được khi mạng thay đổi nhưng lại nảy sinh các vấn đề mới như định tuyến lặp (mục 4.2.2).

Thuật toán định tuyến thường được sử dụng trong Internet gồm hai kiểu chính: thuật toán global link state tĩnh và thuật toán distance vector động. Chúng ta sẽ phân tích những thuật toán này lần lượt trong mục 4.2.1 và mục 4.2.2. Những thuật toán định tuyến khác sẽ được nói qua trong mục 4.2.3.

## 4.2.1. Thuật toán định tuyến Link state

Trong thuật toán Link state, cấu trúc mạng và giá của tất cả các liên kết đều phải được xác định trước. Đây là dữ kiện đầu vào của thuật toán link state. Trong thực tế, điều này được thực hiện bằng cách mỗi nút sẽ gửi thông báo quảng bá về định danh của mình và giá các cung liên kết trực tiếp đến nó tới tất cả các router khác trên mạng. Việc quảng bá rộng rãi trạng thái liên kết có thể được thực hiện ngay khi nút không biết về đầy đủ các nút khác trên mạng. Ban đầu nút chỉ biết được thông tin về các hàng xóm của mình cũng như giá các cung đến các hàng xóm. Nhưng sau đó nó sẽ xác định được topo của phần còn lại của mạng khi nhận những thông báo quảng bá từ các nút khác. (Trong chương 5, chúng ta thấy các router hàng xóm trao

đổi thông tin với nhau như thế nào). Kết quả của việc quảng bá trạng thái liên kết là tất cả các nút có thể đầy đủ thông tin về tổng thể mạng. Sau đó mỗi nút đều có thể chạy thuật toán Link state và xác định đường đi có giá thấp nhất tới mọi nút.

Thuật toán Link state được trình bày ở đây là thuật toán Dijkstra (đặt theo tên của người phát minh ra). Thuật toán Dijkstra xác định đường đi có giá thấp nhất từ một nút nguồn (không mất tổng quát, giả sử là A) đến tất cả các nút khác trên mạng. Thuật toán Dijkstra có nhiều bước và sau ***k*** bước sẽ xác định được đường đi có giá thấp nhấp tới ***k*** nút đích. Chúng ta định nghĩa một số ký hiệu sau:

***c(i, j)***: giá liên kết từ nút i đến nút j. Nếu nút i và nút j không có đường kết nối trực tiếp thì $c(i, j) = \infty$. Để đơn giản, chúng ta coi c(i, j) = c(j, i).

***D(v)***: giá hiện tại thấp nhất của tuyến đường đi từ nút nguồn đến nút v.

***P(v)***: nút phía trước nút v (hàng xóm của v) trên tuyến đường hiện có giá thấp nhất từ nguồn tới nút v.

*N*: tập hợp của các nút đã xác định được đường đi ngắn nhất.

Thuật toán Link state gồm có bước khởi tạo cho vòng lặp. Số các bước bằng tổng số nút trên mạng. Khi kết thúc, thuật toán sẽ xác định được đường đi ngắn nhất từ nút nguồn đến tất cả các nút khác trên mạng.

**Thuật toán Link state (LS):**

```
Khởi tạo:
    N = {A}
    for (tất cả các nút v)
        if v kề A
            thì D(V) = c(A, v)
        else D(v) = ∞

Repeat
    Tìm w không ở trong N có D(w) nhỏ nhất
    Bổ sung w vào N
    Cập nhật D(v) cho tất cả v kề với w và không nằm trong N:
        D(v) = min ( (D(v), D(w) + c(w, v) )
     /* Giá mới đến v khác giá cũ đến v hoặc biết được giá đường đi ngắn nhất
     đến w cộng với giá từ w đến v */
Until tất cả các nút nằm trong N
```



| Bước | N | D(b), p(B) | D(C), p(C) | D(D), p(D) | D(E), p(E) | D(F), p(F) |
|---|---|---|---|---|---|---|
| 0 | A | 2, A | 5.A | 1, A | ∞ | ∞ |
| 1 | AD | 2, A | 4, D | | 2, D | ∞ |
| 2 | ADE | 2, A | 3, E | | | 4, E |
| 3 | ADEB | | 3, E | | | 4, E |
| 4 | ADEBC | | | | | 4, E |
| 5 | ADEBCF | | | | | |

Bảng 4.2 Bảng trạng thái các bước cho mạng minh hoạ trên hình 4.4

Xét đồ thị mạng trong Hình 4.4 và tính đường đi có giá thấp nhất từ A đến tất cả các nút khác. Bảng 4.2 cho thấy các kết quả tính của thuật toán, mỗi dòng trong bảng ứng với trạng thái của thuật toán sau khi kết thúc một bước. Sau đây chúng ta sẽ phân tích một số bước đầu tiên:

**Trong bước khởi tạo**, giá hiện tại thấp nhất của đường đi từ A đến các nút hàng xóm B, C và D tương ứng là 2, 5, và 1. Chúng ta có một chú ý nhỏ ở đây, giá đến C được đặt là 5 (ngay sau đây chúng ta sẽ thấy đây không phải là đường đi tốt nhất) vì đây là giá của đường nối trực tiếp từ A đến C. Giá đến E và F được đặt là vô cùng vì giữa A và E, F không có đường kết nối trực tiếp.

**Trong bước đầu tiên** chúng ta tìm kiếm trên những nút chưa được đưa vào tập N và xác định nút có giá đến thấp nhất. Đó là nút D với giá là 1 và do đó D được bổ sung vào N. Dòng 12 của thuật toán LS được thực hiện để cập nhật D(v) cho tất cả các nút v, kết quả nhận được được trình bày trong dòng thứ 2 (bước 1) trong bảng 4.2. Giá của đường đi đến B không đổi. Giá đường đi đến C (nhận giá trị 5 trong bước khởi tạo trước) qua D có giá trị nhỏ hơn là 4. Đây là đường tốt hơn được chọn và nút phía trước của C trên đường đi ngắn nhất từ A sẽ là D. Tương tự vậy, giá đường đi đến E (qua D) được tính là 2 và bảng được cập nhật tương ứng.

**Trong bước thứ hai**, đường đi đến nút B và E đều có giá thấp nhất và chúng ta bổ sung E vào tập N (Bây giờ N chứa A, D và E). Giá đến các nút chưa nằm trong N (gồm B, C và F) được cập nhật trong dòng 12 của thuật toán LS, kết quả là dòng 3 của bảng 4.2.

....

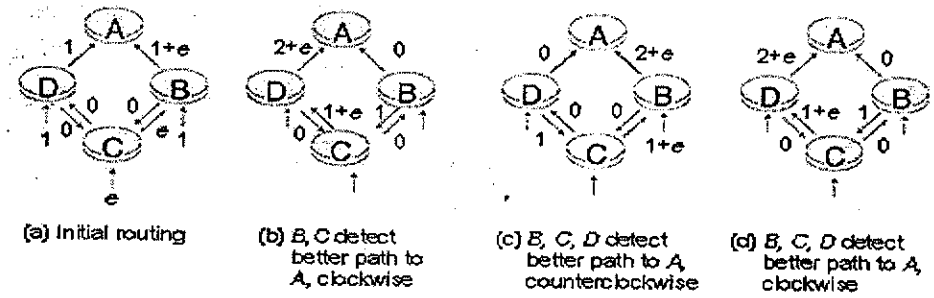
Khi thuật toán LS kết thúc, với mỗi nút chúng ta xác định được nút ngay trước nó trên tuyến đường có giá thấp nhất xuất phát từ nguồn. Với mỗi nút phía trước, chúng ta lại có nút phía trước nữa... Cuối cùng chúng ta xác định được toàn bộ đường đi từ nguồn đến tất cả các nút đích.

Độ phức tạp tính toán của thuật toán này bằng bao nhiêu? Với n nút (không kể nút nguồn), để tìm đường đi có giá thấp nhất từ nguồn đến tất cả các đích, khối lượng tính toán là bao nhiêu trong trường hợp xấu nhất? Trong vòng lặp đầu tiên, chúng ta cần kiểm tra qua tất cả n nút để xác định nút w có giá nhỏ nhất không nằm trong n; trong vòng lặp thứ hai, chúng ta cần kiểm tra n – 1 nút để xác định giá thấp nhất; trong vòng lặp thứ ba là n-2 nút ... Tổng số các nút mà chúng ta cần phải kiểm tra qua tất cả các bước là $n(n+1)/2$ và theo đó chúng ta có thể nói rằng thuật toán Link state có độ phức tạp là $O(n^2)$. (Thuật toán này có thể được cải tiến bằng cách sử dụng cấu trúc dữ liệu HEAP, độ phức tạp chỉ còn theo hàm logarit của n).

Trước khi kết thúc trình bày về thuật toán LS, chúng ta hãy xét ví dụ minh họa một cấu hình mạng giống như trên Hình 4.5. Giá của mỗi liên kết (cung) bằng tải hiện tại trên nó (như thế giá sẽ là độ trễ mà gói tin phải chịu). Trong trường hợp này giá không có tính chất đối xứng, nghĩa là c(A, B) chỉ bằng c(B, A) nếu tải trên cả hai hướng AB là như nhau. Giả sử hai nút B và D gửi một đơn vị dữ liệu, nút C gửi khối lượng dữ liệu là e tới A. Định tuyến ban đầu được minh hoạ trên Hình 4.5(a), giá của mỗi cung ứng với tải trên cung đó.

Trong bước tiếp theo của thuật toán LS, nút C (với giá liên kết cơ bản đã được xác định trong Hình 4.5a) nhận thấy đường đi đến A theo chiều kim đồng hồ có giá là 1, trong khi theo chiều ngược lại có giá là 1+e. Do đó, đường đi đến A có giá thấp nhất của C bây giờ là theo chiều kim đồng hồ. Tương tự, B nhận thấy đường đi đến A có giá thấp nhất mới cũng theo chiều kim đồng hồ, kết quả được trình bày trong Hình 4.5b. Trong bước tiếp theo, nút B, C và D nhận thấy đường đi đến A ngược chiều kim đồng hồ có giá là 0 và tất cả các nút định lại tuyến đường theo ngược chiều kim đồng hồ. Trong bước tiếp theo B, C và D lại thay đổi việc định tuyến theo chiều kim đồng hồ.






**Hình 4.5 Xung đột định tuyến**

Làm sao có thể ngăn ngừa sự dao động như trên (điều này luôn xuất hiện với những thuật toán chọn độ tắc nghẽn hoặc thời gian trễ làm giá cho đường truyền). Một giải pháp được đưa ra là định giá cho đường truyền không phụ thuộc vào tải trên đường đi - một giải pháp khó có khả năng chấp nhận vì mục tiêu của định tuyến là tránh những đường truyền hay tắc nghẽn (có độ trễ cao). Một giải pháp khác là làm thế nào để tất cả các router không chạy thuật toán LS tại cùng một thời điểm. Giải pháp này dường như hợp lý hơn vì chúng ta hy vọng rằng thậm chí nếu các router có chạy thuật toán LS với cùng chu kỳ, thì thuật toán sẽ đưa ra những kết quả khác nhau tại mỗi nút.

## 4.2.2. Thuật toán Distance vector

Nếu thuật toán LS sử dụng thông tin về toàn bộ trạng thái mạng, thuật toán Distance vector (DV) là thuật toán lặp, không đồng bộ và phân tán. Thuật toán được xem là phân tán vì mỗi nút nhận thông tin từ những nút hàng xóm có đường kết nối trực tiếp, thực hiện các bước tính toán và phân tán kết quả tính toán tới tất cả các nút hàng xóm. Tính lặp được thể hiện ở chỗ quá trình này được thực hiện liên tục cho đến khi không còn thông tin được trao đổi giữa các cặp hàng xóm (chúng ta sẽ thấy đây là thuật toán tự kết thúc – nó tự dừng chứ không cần một tín hiệu kết thúc). Thuật toán không đòi hỏi các nút không được hoạt động trong khi trao đổi với những nút khác – đây chính là đặc điểm không đồng bộ. Chúng ta sẽ thấy thuật toán với các đặc điểm dị bộ, lặp, tự kết thúc, và phân tán thú vị và đáng quan tâm hơn so với thuật toán tập trung.

Cấu trúc dữ liệu chính trong thuật toán DV là **bảng khoảng cách (distance table)** được đặt ở mỗi nút. Trong bảng khoảng cách, mỗi hàng ứng với một nút đích trên mạng và mỗi cột ứng với một nút hàng xóm có đường kết nối trực tiếp đến. Giả sử nút X muốn định tuyến đến đích Y qua nút hàng xóm Z. Trong bảng khoảng cách của nút X, $D^X(Y, Z)$ là tổng của giá đường liên kết trực tiếp giữa X và Z - c(X, Z) với giá đường đi bé nhất từ Z đến Y. Đó là:

$$D^X(Y, Z) = c(X, Z) + \min_w\{D^Z(Y, w)\}$$

Biểu thức $\min_w$ trong đẳng thức trên được lấy trên tất cả các hàng xóm của Z (kể cả X, như chúng ta sẽ thấy dưới đây).

Đẳng thức giúp chúng ta hình dung ý tưởng của thuật toán DV - mỗi nút phải biết được giá nhỏ nhất của đường đi từ tất cả các hàng xóm của nó đến bất kỳ đích nào. Và khi giá nhỏ nhất đến đích nào đó thay đổi, nút phải báo cho tất cả các hàng xóm biết.

Trước khi trình bày thuật toán DV, xét kiến trúc mạng và bảng khoảng cách của nút E trên Hình 4.6. Đây là bảng khoảng cách của nút E sau khi thuật toán DV hội tụ. Hãy nhìn vào dòng đầu tiên với đích đến là A.

Rõ ràng giá đường kết nối trực tiếp đến A từ E phải là 1, do đó $D^E(A, A) = 1$.

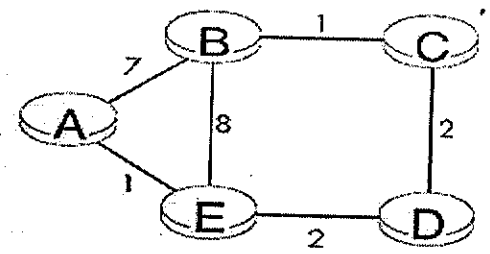
Bây giờ hãy chú ý đến giá trị của $D^E(A, D)$ – giá đường đi từ E đến A qua D. Trường này trong bảng khoảng cách là giá của đường đi từ E đến D (2) cộng với giá đường đi nhỏ nhất từ D đến E. Chú ý rằng giá thấp nhất của đường đi từ D đến A là 3 - đường đi qua E! Do vậy giá thấp nhất từ E đến A qua D là 5. Chúng ta không quan tâm - mặc dù có thể băn khoăn ở đây - là đường đi từ E đến A qua D lại quay lại E.

Tương tự, trường trong bảng khoảng cách với đường đi qua B: $D^E(A, B) = 14$. Hãy chú ý rằng tại sao ở đây không phải là 15?

Các vòng tròn trong bảng khoảng cách là giá nhỏ nhất của đường đi đến các đích (ứng với các hàng). Cột ứng với vòng tròn xác định nút tiếp theo trên đường đi đến đích có giá thấp nhất. Từ đó có thể dễ dàng xây dựng bảng định tuyến cho mỗi nút (với một đích cụ thể nào đó, cần gửi gói tin ra theo đường ra nào).



Trong khi trình bày bảng vector cho nút E ở trên, chúng ta vẫn có được một cái nhìn toàn cục, biết được giá của tất cả các liên kết trên mạng. Thuật toán DV phân tán được trình bày ở đây không sử dụng đến những thông tin tổng thể như vậy.




| destination | $D^E()$ | cost to destination via A | B | D |
|---|---|---|---|---|
| | A | ① | 14 | 5 |
| | B | 7 | 8 | ⑤ |
| | C | 6 | 9 | ④ |
| | D | 4 | 11 | ② |

Hình 4.6

**Thuật toán distance vector(DV)**

Tại mỗi nút X:

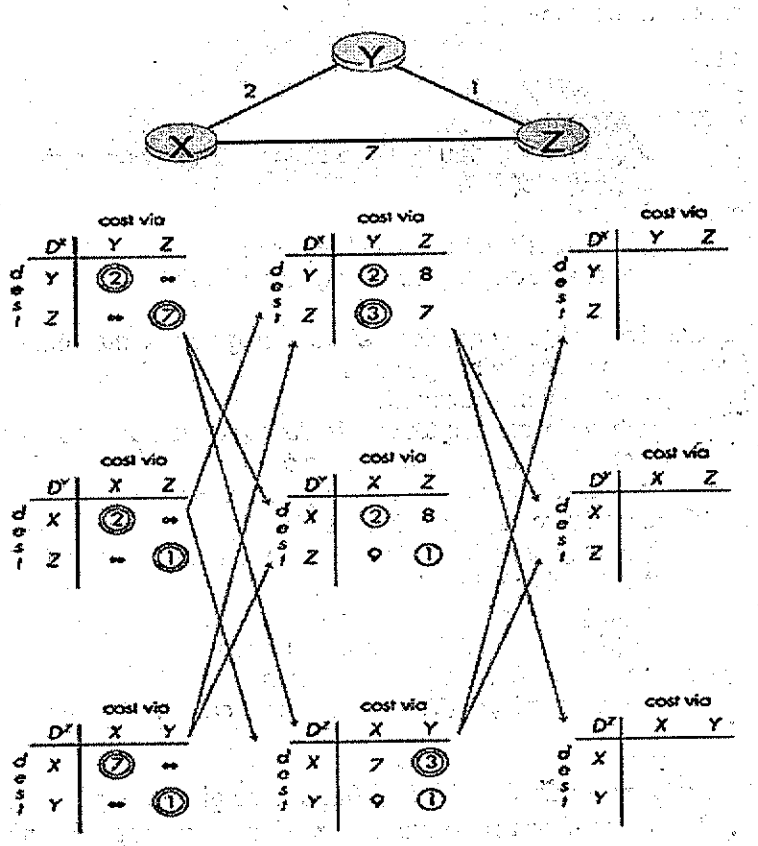
```
1:Khởi tạo:
2:      for (tất cả các nút kề với v)
3:              D^X(*, v) = ∞ /* dấu "*" là để chỉ cho tất cả các hàng*/
4:              D^X(v, v) = c(X, v)
5:      for (tất cả các đích Y)
6:              gửi min_w D(Y, w) đến mỗi hàng xóm
7:              /* w chạy trong tập các hàng xóm của X*/
8:Lặp
9:      Đợi cho đến khi (thấy giá liên kết đến hàng xóm V thay đổi hoặc nhận
        được sự cập nhật của hàng xóm V)
        if (c(X, V) thay đổi một lượng d)
                /* thay đổi giá của tất cả các đường đi đến đích qua v bằng d*/
                /* chú ý: d có thể dương hoặc âm*/
                for (tất cả các đích y: D^X(y, V) = D^X(y, V) + d
        else if ( nhận được cập nhật từ V đến Y)
                /* đường đi ngắn nhất từ V đến nút nào đó Y thay đổi*/
                /* V đã gửi giá trị mới của min_w D^V(Y, w)*/
                /* gọi giá trị mới nhận được là "newval"*/
                for (đích y): D^X(Y, V) = c(X, V) + newval
        if (chúng ta có min_w D^X(Y, w) mới cho đích Y nào đó)
                gửi giá trị min_w D^X(Y, w) mới đến tất cả các hàng xóm.
Mãi mãi
```

Thật vậy, mỗi nút sẽ chỉ biết thông tin về giá đường liên kết tới nút hàng xóm cũng như thông tin nó nhận được từ những hàng xóm này. Thuật toán Distance vector chúng ta sẽ nghiên cứu còn được gọi là thuật toán

Bellman–Ford. Nó được áp dụng trong nhiều giao thức định tuyến trong thực tế, bao gồm: Internet BGP, ISO IDRP, Novell IPX và mạng ARPAnet.

Bước mấu chốt nằm từ dòng 15 đến 21, ở đó nút cập nhật bảng khoảng cách khi nhận được sự thay đổi về giá của liên kết đến hàng xóm hoặc nhận được thông tin cập nhật từ hàng xóm. Một bước quan trọng khác là dòng 24, ở đó nút gửi cập nhật đến tất cả các hàng xóm nếu đường đi có giá nhỏ nhất đến đích nào đó bị thay đổi.

Hình 4.7 minh hoạ hoạt động của thuật toán DV cho mạng đơn giản gồm 3 nút. Hoạt động của thuật toán được thực hiện một cách đồng bộ: tất cả các nút đồng thời nhận được thông điệp từ hàng xóm của chúng, tính toán bảng khoảng cách mới và báo cho các hàng xóm về sự thay đổi giá đường đi ngắn nhất. Sau khi nghiên cứu ví dụ này, bạn có thể nghĩ rằng thuật toán hoạt động đúng trong chế độ không đồng bộ - việc tính toán và cập nhật sự thay đổi của mỗi nút có thể diễn ra tại bất kỳ thời điểm nào.




**Hình 4.7 Ví dụ về thuật toán Distance Vecto**



Các ô khoanh tròn trong Hình 4.7 ứng với giá nhỏ nhất đến đích nào đó nằm trong hàng tương ứng. Khoanh hai vòng tròn biểu diễn giá nhỏ nhất mới được xác định (trong dòng 4 hoặc dòng 21 của thuật toán DV). Khi đó các thông tin cập nhật sẽ được gửi đến các nút hàng xóm (dòng 24 của thuật toán DV) - ứng với mũi tên giữa các cột trong Hình 4.7.

Cột ngoài cùng bên trái trong Hình 4.7 là các bảng khoảng cách của nút X, Y và Z sau bước khởi tạo.

Bây giờ hãy xem làm thế nào để nút X tính lại bảng khoảng cách (cột giữa của Hình 4.7) sau khi nhận được thông tin cập nhật từ nút Y và Z. Khi nhận được cập nhật từ Y và Z, X thực hiện dòng 21 của thuật toán DV:

$$D^X(Y, Z) = c(X, Z) + \min_w D^Z(Y, w)$$
$$= 7 + 1$$
$$= 8$$
$$D^X(Z, Y) = c(X, Y) + \min_w D^Y(Z, w)$$
$$= 2 + 1$$
$$= 3$$

X biết giá trị $\min_w D^Z(Y, w)$ và $\min_w D^Y(Z, w)$ vì nút Z và Y gửi những giá trị này đến X (và X cũng nhận được theo dòng 10 của thuật toán DV). Việc tính lại bảng khoảng cách của Y và Z ở cột giữa trong Hình 4.7 được thực hiện tương tự.

Giá trị $D^X(Z, Y) = 3$ có nghĩa là giá nhỏ nhất từ X đến Z giảm từ 7 xuống 3. Do đó, X gửi cập nhật đến Y và Z để thông báo cho chúng giá thấp nhất mới đến Z. Chú ý X không cần cập nhật cho Y, Z về giá của nó đến Y vì giá trị này không bị thay đổi. Khi Y tính lại bảng khoảng cách không phát hiện ra thay đổi, do đó Y không gửi cập nhật đến X và Z.

Quá trình nhận cập nhật từ hàng xóm, tính lại bảng khoảng cách và cập nhật các thay đổi đến hàng xóm được thực hiện cho đến khi không còn thông điệp nào được trao đổi. Trong trường hợp này vì không có thông tin cập nhật được gửi nên các nút không phải tính lại bảng khoảng cách và thuật toán ở trạng thái không hoạt động: tất cả các nút ở trạng thái đợi trong dòng 9 của thuật toán DV. Thuật toán DV sẽ ở trong trạng thái không hoạt động cho đến khi giá của một liên kết nào đó thay đổi.

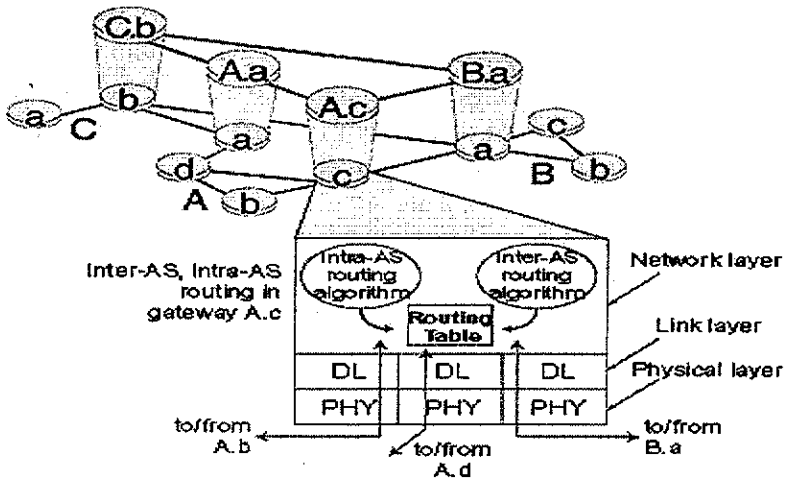
## 4.3 ĐỊNH TUYẾN PHÂN CẤP

Trong các phần trước, chúng ta đã thấy mạng là tập hợp các router liên kết với nhau. Tất cả các router sẽ giống nhau nếu như đều sử dụng cùng một thuật toán định tuyến để xác định đường đi trên toàn bộ hệ thống mạng.

Trong thực tế, mô hình mạng như vậy và việc xem các router giống hệt nhau cùng thực hiện một thuật toán định tuyến quá đơn giản với hai lý do quan trọng sau:

**Phạm vi (scale)**: Khi số lượng các router lớn, khối lượng thông tin phải tính toán, lưu trữ và trao đổi giữa các bảng chứa thông tin định tuyến trên mỗi router (ví dụ các cập nhật về đường đi ngắn nhất) cũng trở nên cực lớn. Mạng Internet ngày nay bao gồm hàng triệu router liên kết với nhau và hơn 50 triệu máy tính. Lưu trữ thông tin về tất cả các máy tính cũng như các router đòi hỏi một lượng bộ nhớ khổng lồ. Các thông tin trao đổi cập nhật giữa các router sẽ "ngốn" toàn bộ băng thông của đường truyền. Thuật toán distance vector trên hàng triệu router chắc chắn sẽ không bao giờ hội tụ. Do đó nảy sinh ra nhu cầu làm giảm độ phức tạp trong việc xác định đường đi trên một mạng lớn như Internet.

**Quản trị (Administrative automomy)**: Mặc dù các nhà thiết kế thường bỏ qua yêu cầu của các tổ chức - chẳng hạn khả năng lựa chọn thuật toán định tuyến hay che dấu cấu trúc mạng bên trong của tổ chức với bên ngoài – nhưng trên thực tế đây là những vấn đề quan trọng. Lý tưởng mà nói, một tổ chức phải giữ khả năng quản trị và kiểm soát mạng máy tính của mình nhưng vẫn có khả năng kết nối với các mạng bên ngoài.

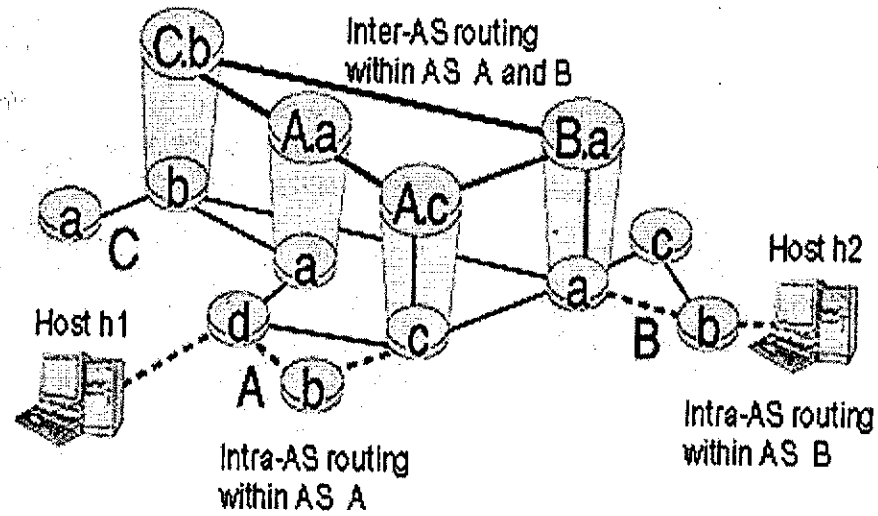



Hình 4.8 Ví dụ miền tự quản



Cả hai vấn đề trên đều có thể giải quyết bằng cách nhóm các router thành các vùng hay **Miền tự quản (Autonomous System - AS)**. Các router trong cùng AS sử dụng cùng một thuật toán định tuyến (ví dụ như thuật toán LS hay DV) và biết đầy đủ về nhau (giống trường hợp đã trình bày ở trước). Thuật toán định tuyến chạy trong mỗi AS được gọi là **intraautonomous system routing protocol**. Dĩ nhiên cần phải kết nối các AS với nhau – và vì thế một số router trong AS có thêm nhiệm vụ định tuyến gói tin ra ngoài AS (đích nằm trong một AS khác). Các router định tuyến gói tin ra phía ngoài như vậy được gọi là gateway router. Để định tuyến gói tin đi giữa các AS (có thể phải đi qua nhiều AS trên toàn bộ tuyến đường), các gateway router phải biết cách xác định đường đi giữa các AS. Thuật toán định tuyến được sử dụng tại các gateway router là interautonomous system routing protocol.

Nói tóm lại, vấn đề phạm vi và quản trị được giải quyết bằng cách sắp xếp router vào các miền tự quản (AS). Tất cả router trong một AS sử dụng cùng một thuật toán định tuyến. Các gateway router trên mỗi AS sử dụng thuật toán interautonomous system routing để định tuyến giữa các AS. Vấn đề phạm vi được giải quyết ở chỗ mỗi router chỉ cần biết về các router khác trong cùng AS và gateway router của AS đó (chứ không cần phải biết tất cả các router). Vấn đề quản trị được giải quyết vì tổ chức có thể lựa chọn sử dụng bất kỳ thuật toán định tuyến intra-AS nào - miễn là thuật toán inter-AS mà nó sử dụng có khả năng liên kết với các AS khác.




Hình 4.9 Ví dụ định tuyến phân cấp

Trên Hình 4.9 có ba AS: A, B và C. Miền A có 4 router: A.a, A.b, A.c, và A.d, sử dụng cùng một thuật toán intra-AS của miền A. Bốn router này đều có đầy đủ các thông tin về nhau cũng như các liên kết trong miền A. Tương tự miền B có 3 và miền C có 2 router. Các thuật toán intra-AS trong các miền A, B, C không nhất thiết giống nhau. Các gateway router là A.a, A.c, B.a, và C.b. Ngoài các thuật toán intra-AS để trao đổi với các router trong miền, bốn gateway router này phải sử dụng thuật toán inter-AS để định tuyến giữa các AS. Về mặt topo, chúng sử dụng giao thức inter-AS, được minh họa bằng các đường kết nối mầu đen đậm ở mức cao hơn. Các đường kết nối này có thể là đường kết nối vật lý thực sự (giữa A.c và B.a), có thể là đường ảo (ví dụ giữa A.c và A.a). Trên hình vẽ chúng ta cũng thấy A.c sử dụng cả intra-AS để định tuyến với A.b, A.d và inter-AS để định tuyến với B.a

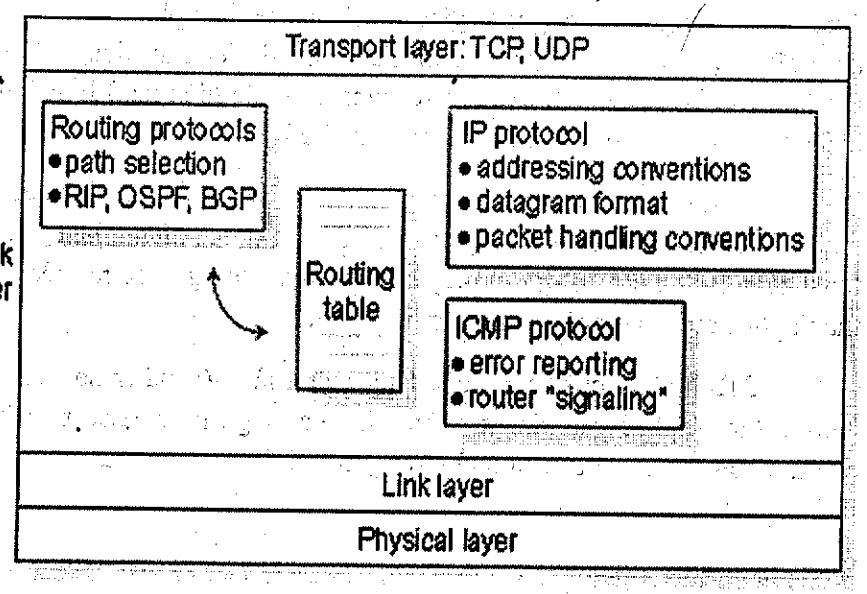
Giả sử máy tính h1 nối với router A.d cần gửi gói tin tới máy tính h2 trong AS B, như trên Hình 4.9. Bảng định tuyến tại A.d cho biết, router A.c chịu trách nhiệm gửi gói tin ra bên ngoài AS. Gói tin từ A.d tới router đầu tiên A.c sử dụng giao thức định tuyến intra-AS của A. Có một điểm cực kỳ quan trọng cần chú ý là router A.d không cần biết gì về cấu trúc nội tại trong miền B và C và cũng như topo giữa ba miền A, B và C. Router A.c nhận gói tin, xác định đích của gói tin đó nằm ngoài miền A (miền B), bảng định tuyến của inter-AS sẽ xác định rằng để gửi tới miền B thì phải chuyển tới B.a. Khi gói tin tới B.a, giao thức inter-AS xác định rằng gói tin này tới máy tính nào đó trong miền B và chuyển cho giao thức intra-AS của B. Cuối cùng router B.a chuyển gói tin đó tới máy tính đích h2 sử dụng giao thức intra-AS của B. Trong Hình 4.9, các giao thức intra-AS của A và B là các đường kẻ đứt, giao thức inter-AS giữa các miền là đường kẻ đậm.

## 4.4 INTERNET PROTOCOL

Trong các phần trước, chúng ta đã trình bày các nguyên lý chung của tầng mạng mà chưa nói đến bất kỳ một kiến trúc mạng cụ thể nào. Chúng ta cũng nói tới các mô hình dịch vụ khác nhau của tầng mạng, các thuật toán định tuyến xác định đường đi giữa thiết bị gửi và thiết bị nhận, phân cấp hệ thống mạng để giải quyết vấn đề phạm vi. Trong phần này,



chúng ta sẽ nói tới tầng mạng của Internet – mà một phần trong đó được xem là tầng IP. Chúng ta sẽ thấy IP chỉ là một phần (dù là phần quan trọng) trong kiến trúc tầng mạng của Internet (xem Hình 4.10).




**Hình 4.10 Vị trí và các thành phần của Tầng mạng**

Như đã nói trong trong phần 4.1, tầng mạng của Internet sử dụng dịch vụ chuyển mạch gói (datagram) chứ không phải dịch vụ chuyển mạch ảo (VC). Tại máy gửi, khi nhận được một segment từ tầng giao vận, tầng mạng đặt segment trong gói dữ liệu IP (IP datagram) với các trường địa chỉ gửi, địa chỉ nhận... và gửi datagram này tới router đầu tiên trên đường tới đích. Điều này tương tự như một người sau khi viết thư, bỏ lá thư vào phong bì ghi địa chỉ người nhận và thả phong bì thư vào hộp thư. Tầng mạng của Internet cũng giống như hệ thống bưu điện đều không có bất kỳ một sự liên hệ trước nào với bên nhận trước khi chuyển "bưu kiện" (datagram hay lá thư) tới phía nhận. Hơn nữa, như đã nói trong phần 4.1, tầng mạng của Internet và bưu điện sẽ chỉ cung cấp một dịch vụ kiểu "cố gắng tối đa", nghĩa là không có bất kỳ đảm bảo nào về việc gói tin có đến đích hay không, đến trong một khoảng thời gian bao lâu hay đến theo đúng thứ tự gửi.

Trong Hình 4.10, tầng mạng trong kiểu mạng chuyển mạch gói giống như mạng Internet có ba thành phần chính:

Thành phần thứ nhất là giao thức mạng: xác định địa chỉ tầng mạng; ý nghĩa các trường trong datagram (là gói dữ liệu - PDU của tầng mạng); hành động của router và thiết bị đầu cuối khi nhận được datagram. Giao thức mạng trong Internet gọi là giao thức Internet hay phổ biến hơn là giao thức **IP**. Hiện nay có hai phiên bản giao thức IP được sử dụng. Các phần 4.4.1 đến 4.4.4 nói về IPv4 (được sử dụng chủ yếu hiện nay) [RFC 701] và phần 4.7 nói tới IPv6 (được đưa ra để thay thế IPv4).

Thành phần thứ hai của tầng mạng là bộ phận xác định đường đi: xác định tuyến đường của datagram trên đường đi tới đích. Phần 4.2 nói về thuật toán tạo ra các bảng định tuyến như vậy. Chúng ta sẽ nghiên cứu các thành phần của bộ định tuyến trong phần 4.5.

Thành phần cuối cùng của tầng mạng là chức năng báo lỗi và khả năng trả lời một số yêu cầu về thông tin của tầng mạng. Giao thức báo lỗi của Internet – ICMP được nói đến trong mục 4.4.5.

## 4.4.1 Địa chỉ IPv4

Đầu tiên chúng ta sẽ nói về địa chỉ IPv4. Mặc dù vấn đề địa chỉ tương đối đơn giản song mối quan hệ giữa địa chỉ và giao thức tầng mạng lại quan trọng.

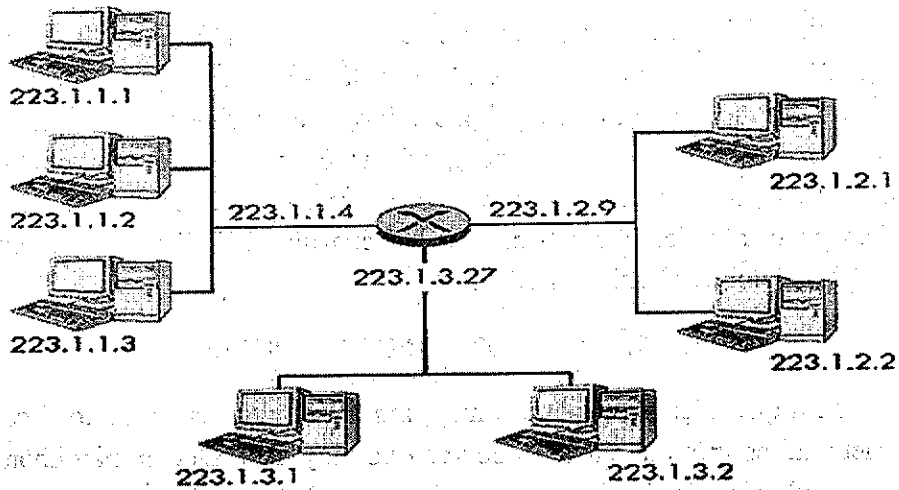
Trước khi thảo luận về địa chỉ IP, chúng ta hãy xét máy tính và router nối vào mạng như thế nào. Máy tính thường có một đường kết nối duy nhất vào hệ thống mạng mà qua đó thực thể IP trong máy tính sẽ sử dụng khi gửi datagram. Nằm giữa máy tính và đường kết nối vật lý là một **giao diện ghép nối (interface)**. Ngược lại router khác hoàn toàn máy tính. Công việc của router là chuyển một datagram từ kết nối (incoming link) này tới kết nối khác (outgoing link). Router có thể có nhiều kết nối, và bộ phận nằm giữa router với kết nối cũng được gọi là giao diện. Như vậy router có nhiều giao diện, mỗi giao diện ứng với một kết nối. Vì tất cả các máy tính và router đều phải có khả năng gửi và nhận IP datagram nên mỗi giao diện phải có một địa chỉ IP. Do đó địa chỉ IP ứng với giao diện chứ không phải với máy tính hay router.



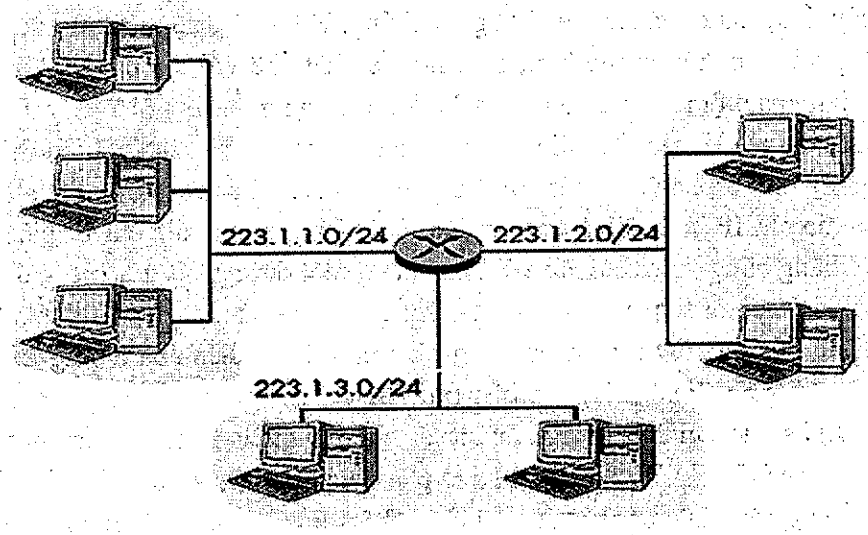
Địa chỉ IP có độ dài 32 bit (4 byte) và do đó không gian địa chỉ có $2^{32}$ địa chỉ. Địa chỉ IP được viết theo ký pháp **dấu chấm thập phân (dotted-decimal notation)** vì mỗi byte của địa chỉ được viết dưới dạng thập phân và phân cách với các byte khác bằng ký tự chấm (.). Xét địa chỉ IP 193.32.216.9. 193 là số thập phân ứng với nhóm 8 bít đầu của địa chỉ, 32 là số thập phân ứng với nhóm 8 bít thứ hai của địa chỉ... Bởi vậy địa chỉ 193.32.216.9 đổi ra hệ nhị phân sẽ là:

**11000001 00100000 11011000 00001001.**

Mỗi giao diện ghép nối của máy tính hay router trên mạng toàn cầu Internet phải có một địa chỉ IP được xác định duy nhất. Địa chỉ này không thể chọn một cách tùy ý mà phụ thuộc vào "mạng" mà nó kết nối vào. Trong ngữ cảnh này, thuật ngữ "mạng" không có ý là một cấu trúc tổng thể gồm các máy tính, router và các liên kết giữa chúng. Hiện tại thuật ngữ này được sử dụng với ý nghĩa cụ thể hơn, có quan hệ chặt chẽ với địa chỉ IP. Hình 4.11 minh họa một router có 3 giao diện được sử dụng để kết nối 7 máy tính. Quan sát địa chỉ IP của giao diện ứng với mỗi máy tính và router. Giao diện của 3 máy tính ở phần trên bên trái trong Hình 4.11 và router nối với chúng đều có địa chỉ IP là 223.1.1.xxx.: nghĩa là 24 bit đầu của địa chỉ IP giống nhau. Chúng cũng được kết nối với nhau bằng một đường kết nối vật lý duy nhất (trong trường hợp này là môi trường quảng bá sử dụng cáp Ethernet) mà không cần qua bất kỳ router trung gian nào. Giao diện của những máy tính này và giao diện phía trên bên trái của router tạo nên **mạng IP (IP network)** hay đơn giản là **mạng**. 24 bit địa chỉ đầu giống nhau là phần mạng trong cấu trúc địa chỉ IP, 8 bit còn lại là phần máy tính (host) của địa chỉ IP. Chính mạng này cũng có một địa chỉ là 22.3.1.1.0/24 trong đó kí hiệu /24 là **mặt nạ mạng (network mask)** với ý nghĩa 24 bit đầu tiên của địa chỉ 32 bit xác định địa chỉ mạng. Những bit này cũng được xem là **tiền tố mạng (network prefix)**. Mạng 22.3.1.1.0/24 gồm giao diện của 3 máy tính (223.1.1.1; 223.1.1.2; 223.1.1.3) và một giao diện của router (223.1.1.4). Bất kỳ máy tính nào nối với mạng 223.2.2.0/24 đều phải có địa chỉ dưới dạng 223.1.1.xxx. Trên Hình 4.11 còn có hai mạng khác: 223.1.2.0/24 và 223.1.3.0/24 . Hình 4.12 minh hoạ 3 mạng IP trong Hình 4.11.




Hình 4.11




Hình 4.12

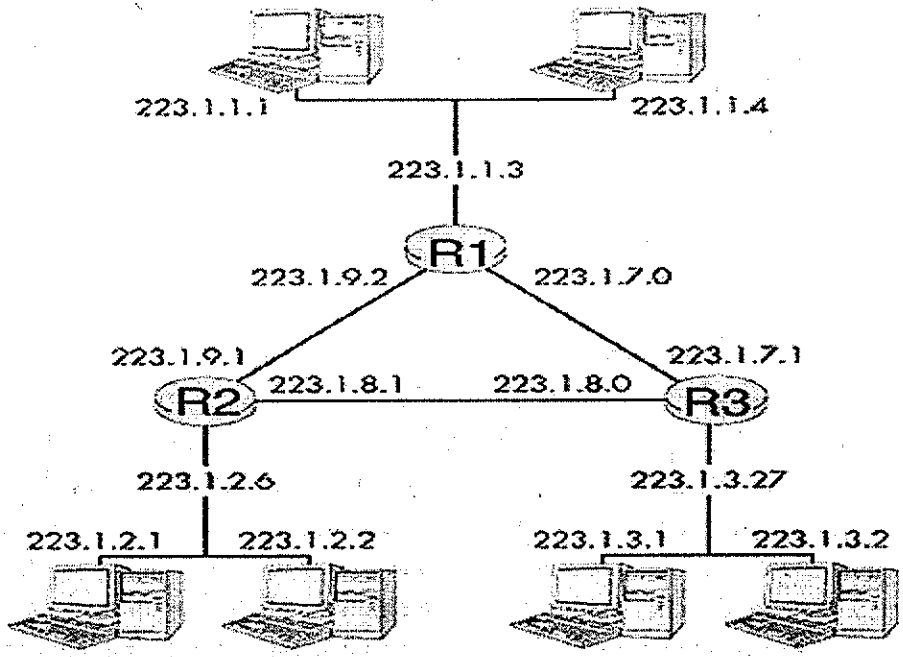
Định nghĩa IP về "mạng" không chỉ với phân đoạn mạng Ethernet nối nhiều máy tính với một router. Trên Hình 4.13 ba router đôi một nối với nhau qua các đường liên kết điểm tới điểm (point-to-point). Mỗi router có ba giao diện, hai giao diện kết nối tới hai router kia và một giao diện dành cho kết nối quảng bá với các máy tính. Có bao nhiêu mạng IP ở đây? Ba mạng 223.1.1.0/24, 223.1.2.0/24 và 223.1.3.0/24 tương tự các mạng nói tới trong



Hình 4.11. Nhưng chú ý có thêm 3 mạng nữa trong Hình 4.13 mạng 223.1.9.0/24 cho hai giao diện nối router R1 và R2, mạng 223.1.8.0/24 cho hai giao diện nối router R2 và R3 và mạng 223.1.7.0/24 ứng với hai giao diện nối router R3 và R1

Với một hệ thống liên mạng gồm nhiều router và máy tính, chúng ta có thể sử dụng một công thức để xác định các mạng trong hệ thống. Chúng là loại bỏ tất cả giao diện của các máy tính và router. Khi đó sẽ tạo ra các mạng cô lập, mỗi mạng cô lập đó được coi là một mạng IP. Áp dụng cách thức này trong ví dụ trên Hình 4.13, chúng ta có 6 mạng IP tách biệt. Mạng toàn cầu Internet gồm hàng triệu hệ thống mạng như vậy. Ký pháp mạng và địa chỉ mạng có vai trò then chốt trong kiến trúc định tuyến Internet. Sau khi đã có định nghĩa về mạng, chúng ta tiếp tục trình bày chi tiết về địa chỉ IP. Kiến trúc địa chỉ Internet đầu tiên đưa ra 4 lớp địa chỉ minh họa trên Hình 4.14. Lớp địa chỉ thứ năm, bắt đầu bằng 11110 được dự trữ cho việc sử dụng sau này. Với lớp địa chỉ A, 8 bit đầu là địa chỉ mạng và 24 bit cuối là địa chỉ cho giao diện (máy tính) trong mạng. Như thế có $2^7$ mạng lớp A (bit đầu tiên trong 8 bit địa chỉ mạng luôn nhận giá trị 0), mỗi mạng lớp A lại có thể có $2^{24}$ giao diện. Lớp B có $2^{14}$ mạng, mỗi mạng có $2^{16}$ giao diện. Lớp địa chỉ C dùng 24 bit làm địa chỉ mạng và chỉ có 8 bit làm địa chỉ máy. Lớp D dự trữ làm địa chỉ multicast.

Bốn lớp địa chỉ trình bày trên hiện tại không còn được áp dụng trong kiến trúc địa chỉ IP nữa. Điều kiện phần mạng của địa chỉ IP có độ dài là một, hai hoặc ba byte không hợp lý khi số lượng các tổ chức với mạng cỡ nhỏ hay trung bình ngày càng tăng. Mạng lớp C (/24) chỉ có thể có $2^8 - 2 = 254$ máy tính (2 trong số $2^8$ địa chỉ được dự trữ cho một số mục đích khác) - một số lượng quá nhỏ với nhiều tổ chức. Tuy nhiên, mạng lớp B (/16) có thể tới 65.634 máy tính lại là quá lớn. Một tổ chức với 2000 máy tính phải sử dụng địa chỉ lớp B (/16). Với kiểu gán địa chỉ như vậy thì không gian địa chỉ lớp B sẽ nhanh chóng bị cạn kiệt nhưng không gian địa chỉ lại không được sử dụng hiệu quả. Ví dụ, tổ chức sử dụng địa chỉ lớp B cho 2000 máy tính thì sẽ có khoảng 63000 địa chỉ còn lại bị lãng phí trong khi đáng ra có thể phân phối cho các tổ chức khác.




**Hình 4.13 Có 6 mạng IP**

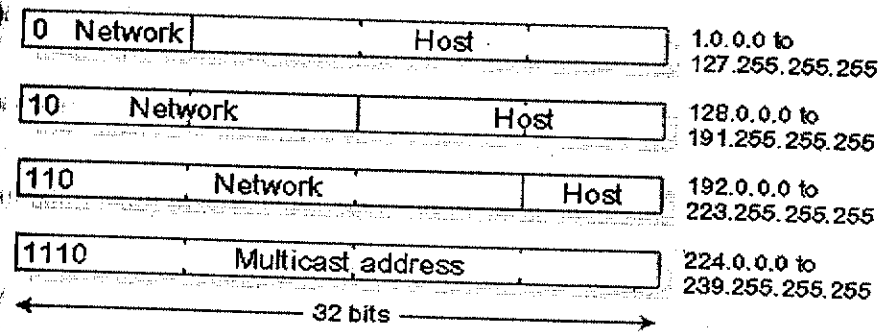
Năm 1993, IETF chuẩn hóa **Định tuyến liên miền không phân lớp (Classless interdomain routing - CIDR-** phát âm là "cider") [RFC 1519]. Với cơ chế không phân lớp, phần mạng của địa chỉ IP có thể có độ dài tùy ý, không nhất thiết phải là 8, 16 hay 24 bit. Khuôn dạng của một địa chỉ không phân lớp sẽ là **a.b.c.d/x**, trong đó x là số lượng bit dùng để làm địa chỉ mạng. Trong ví dụ trước, tổ chức cần không gian địa chỉ cho 2000 máy tính chỉ cần một không gian 2.048 địa chỉ dưới dạng a.b.c.d/21, cho phép 63000 địa chỉ còn lại được phân phối cho các tổ chức khác. Trong trường hợp này, 21 bit đầu tiên xác định địa chỉ mạng của tổ chức và tất cả địa chỉ IP của máy tính trong tổ chức đều phải có phần địa chỉ mạng giống nhau. 11 bit còn lại xác định cụ thể máy tính nào trong tổ chức. Trên thực tế, tổ chức có thể tiếp tục chia 11 bit đó trong thủ tục **tạo mạng con (subnetting)** [RFC 950] để tạo ra các mạng con bên trong mạng a.b.c.d/21.



## *Trên thực tế*

Ví dụ trình bày việc một ISP kết nối 8 tổ chức vào mạng Internet minh họa việc phân phối địa chỉ không phân lớp có thể đáp ứng khả năng định tuyến phân cấp như thế nào. Giả sử như trong hình 4.19, ISP Fly-By-Night quảng cáo với thế giới bên ngoài là nó có thể gửi các datagram đến các máy có 20 bit địa chỉ đầu trùng với 200.23.16.0/20. Thế giới bên ngoài không cần biết trong không gian địa chỉ 200.23.16.0/20 thực tế có 8 tổ chức con, mỗi tổ chức có hệ thống mạng riêng. Khả năng sử dụng một tiền tố mạng (prefix) quảng cáo cho nhiều mạng được gọi là **nhóm đường (route aggregation hay route summarization)**.

Nói chung nhóm đường hoạt động tốt khi không gian địa chỉ được cấp phát cho ISP và sau đó ISP cấp phát tiếp cho các tổ chức khách hàng. Nhưng chuyện gì xảy ra nếu địa chỉ không được phân phối theo cách thức phân cấp? Chẳng hạn tổ chức 1 không chấp nhận dịch vụ với chất lượng thấp của ISP Fly-By-Night và quyết định lựa chọn ISP mới là ISPs-R-Us? Như minh họa trên Hình 4.15, ISPs-R-Us có không gian địa chỉ là 199.31.0.0/16, nhưng không gian địa chỉ IP của tổ chức 1 lại nằm bên ngoài không gian địa chỉ này. Sẽ làm gì ở đây ? Chắc chắn, tổ chức 1 có thể cấu hình lại tất cả router và máy tính để có địa chỉ IP trong miền địa chỉ của ISPs–R –Us. Nhưng đây là giải pháp tốn kém, và trong tương lai rất có thể tổ chức 1 lại lựa chọn một ISP mới. Giải pháp ở đây sẽ là cho phép tổ chức 1 giữ lại địa chỉ 200.23.18.0/23. Trong trường hợp này, như trong hình 4.15, Fly-By-Night-ISP tiếp tục quảng cáo không gian địa chỉ 200.23.16.0/20 và ISPs-R-Us tiếp tục quảng cáo không gian địa chỉ 199.31.0.0/16. Tuy nhiên ISPs-R-U bây giờ cũng quảng cáo không gian địa chỉ cho tổ chức 1: 200.23.18.0/23. Khi những router khác trong Internet nhận được quảng cáo không gian địa chỉ 200.23.16.0/20 (từ Fly-By-Night-ISP) và 200.23.18.0/23 (từ ISPs–R-Us) và muốn định tuyến tới một địa chỉ nào đó trong 200.23.18.0/23, chúng sẽ sử dụng **quy tắc địa chỉ tiền tố dài nhất (longest prefix rule)** để định tuyến tới ISPs-R-Us, vì ISPs-R-Us quảng cáo địa chỉ có tiền tố dài nhất ứng với địa chỉ đích.




**Hình 4.14 Cấu trúc địa chỉ mạng với 4 lớp A,B,C và D**

### Gán địa chỉ cho mỗi giao diện

Sau khi biết được địa chỉ IP, bạn có thể hỏi bằng cách nào máy tính nhận được địa chỉ IP? Địa chỉ IP có hai phần: Phần mạng và phần máy tính. Phần máy tính của địa chỉ có thể được cấp phát theo nhiều cách như sau:

**Cấu hình bằng tay.** Địa chỉ IP được người quản trị hệ thống cấu hình vào máy tính (thường trong file cấu hình).

**Giao thức cấu hình địa chỉ động (Dynamic host configuartion protocol -DHCP)** [RFC 2131]. DHCP là phiên bản mở rộng của giao thức BOOTP [RFC 1542]. Với DHCP, khi máy DHCP phục vụ (server) trong mạng (mạng cục bộ chẳng hạn) nhận yêu cầu DHCP từ một máy khách, nó sẽ phân phối (gán) một địa chỉ IP cho máy khách yêu cầu. DHCP được sử dụng rộng rãi trong mạng cục bộ hay truy cập Internet từ nhà (kết nối modem với ISP).

Để có địa chỉ mạng không đơn giản. Người quản trị mạng phải liên lạc với ISP của mình. ISP đã được phân phối một không gian địa chỉ tương đối lớn và sẽ cấp một phần trong không gian địa chỉ này cho tổ chức thuê bao. Ví dụ ISP được phân phối không gian địa chỉ 200.23.16.0/20. Đến lượt mình ISP chia không gian địa chỉ này thành 8 không gian địa chỉ nhỏ hơn và cấp phát 8 không gian này cho các tổ chức thuê bao như dưới đây (để tiện theo dõi, phần mạng trong địa chỉ được gạch chân)

Không gian địa chỉ của ISP: 11001000 00010111 00010000 00000000 200.2.3.16.0/20

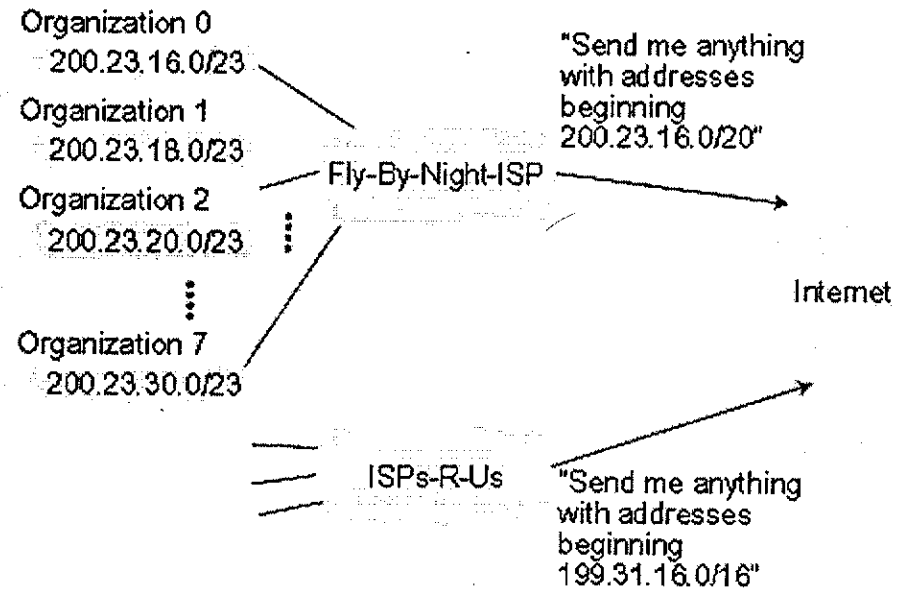
Tổ chức 0 11001000 00010111 00010000 00000000 200.23.16.0/23

Tổ chức 1 11001000 00010111 00010010 00000000 200.23.18.0/23

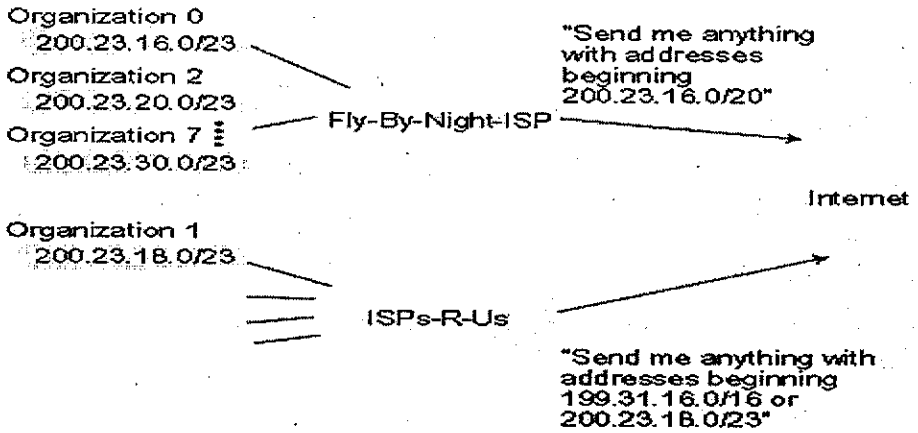
Tổ chức 7 11001000 00010111 00010100 0000000 200.23.30.0/23

Vậy làm thế nào để ISP nhận được không gian địa chỉ? Địa chỉ IP được tổ chức ICANN (The Internet Corporation for Assigned Names and Numbers) [ICANN 2000] quản lí theo các nguyên tắc chỉ đạo ghi trong RFC 2050. Vai trò của tổ chức phi lợi nhuận ICANN không chỉ cấp phát địa chỉ IP mà còn quản trị các root DNS server. Nó chịu trách nhiệm đặt tên miền cũng như giải quyết các tranh chấp về tên miền. Hiện nay việc phân phối địa chỉ IP được cơ quan đăng kí Internet cấp vùng quản lý. Giữa năm 2000, có 3 cơ quan đăng kí như vậy: American Registry for Internet Number (**ARIN**) cho châu Mĩ và một số phần của châu Phi. Reseaux IP Europeans (**RIPE**) cho châu Âu và một số nước chung quanh và Asia Pacific Network Information Center (**APNIC**) cho khu vực châu Á.

Các máy tính có khả năng di động (mobile) có thể thay đổi mạng theo cách động (khi di chuyển) hoặc tĩnh (theo thời gian). Khi định tuyến, phải xác định mạng trước và sau đó mới tới máy tính trong mạng, nên địa chỉ IP của máy tính di động sẽ phải thay đổi khi máy tính thay đổi mạng. Các kỹ thuật xử lý trường hợp này đang được phát triển [RFC 2002, RFC 2131].



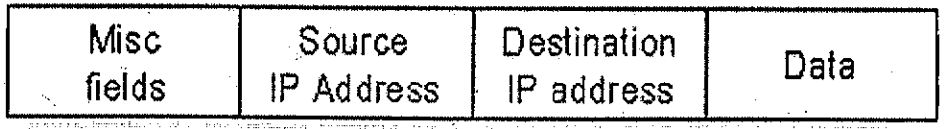

**Hình 4.15 Ví dụ 2 ISP**




Hình 4.16

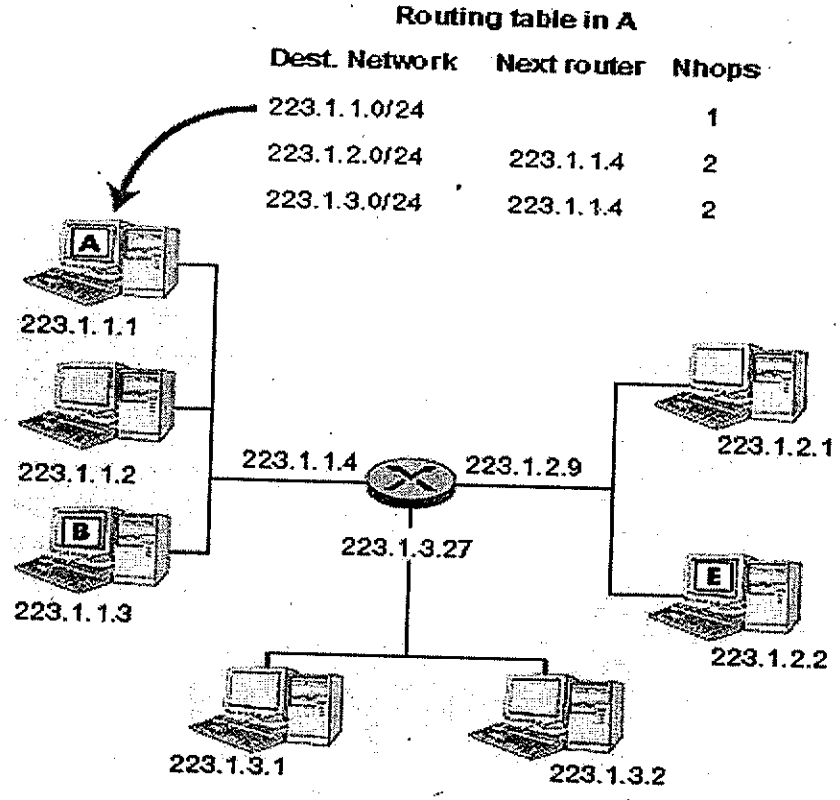
## 4.4.2 Chuyển datagram từ nguồn tới đích: vấn đề địa chỉ và định tuyến

Giờ đây khi đã có định nghĩa về giao diện, mạng cũng như các hiểu biết cơ bản về địa chỉ IP, chúng ta hãy thử xem máy tính và các router chuyển một gói tin IP (IP datagram) từ nơi gửi đến nơi nhận như thế nào. Để đơn giản, ta coi khuôn dạng chung của gói tin IP giống như trong Hình 4.17. Mỗi IP datagram có trường địa chỉ gửi và trường địa chỉ nhận. Máy tính gửi sẽ điền vào trường địa chỉ gửi 32 bit địa chỉ IP của mình và điền vào trường địa chỉ nhận 32 bit địa chỉ IP của máy tính nhận (giống như các trường FROM và TO trên phong bì thư). Trường dữ liệu của datagram thường là gói TCP hoặc UDP segement. Khuôn dạng gói dữ liệu IP được thảo luận chi tiết trong các phần sau.




Hình 4.17 Khuôn dạng chung gói dữ liệu tầng mạng



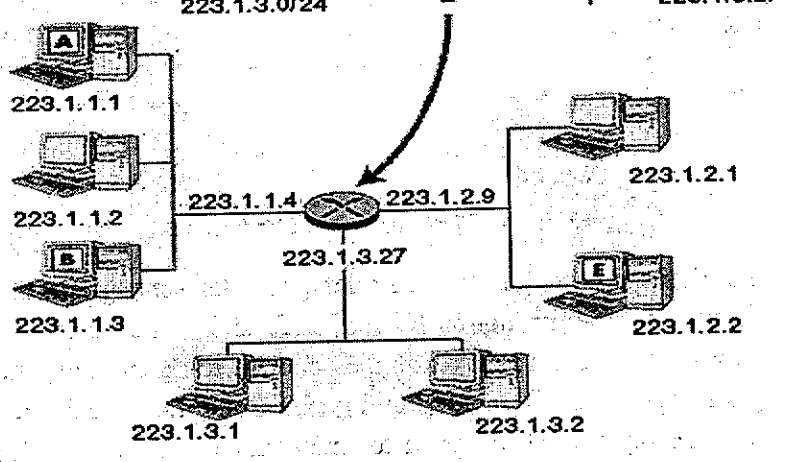



Hình 4.18 Ví dụ định tuyến từ A đến B

Sau khi máy tính gửi tạo ra IP datagram, tầng mạng làm thế nào để gửi datagram từ máy tính nguồn tới máy tính đích? Câu trả lời phụ thuộc vào việc máy tính nguồn và máy tính đích có nằm trong cùng một mạng hay không (thuật ngữ "mạng" sử dụng giống như trong 4.4.1). Đầu tiên giả sử máy tính A muốn gửi IP datagram tới máy tính B nằm trong cùng mạng 223.1.1.0/24 với A. Điều này được thực hiện như sau: đầu tiên thực thể IP trong máy A dò trong bảng định tuyến cục bộ của mình (xem Hình 4.18) và tìm thấy hàng 223.1.1.0/24 trùng với các bit đầu (địa chỉ mạng) trong địa chỉ IP của máy B. Bảng định tuyến chỉ ra rằng số lượng các thiết bị trung gian để đến mạng 223.1.1.0 là 1, nghĩa là B nằm trong cùng một mạng với A. Do đó máy A có thể gửi trực tiếp đến B mà không cần qua các router trung gian. Sau đó máy A chuyển gói dữ liệu IP cho tầng liên kết dữ liệu để chuyển gói dữ liệu đó tới B (công việc của tầng liên kết dữ liệu chuyển dữ liệu giữa hai thiết bị nối trực tiếp với nhau sẽ được trình bày trong chương 5).

Xét tiếp trường hợp máy A gửi gói dữ liệu tới máy E nằm trên mạng khác. A dò trên bảng định tuyến của mình và thấy 223.1.1.0/24 có địa chỉ mạng trùng với phần mạng trong địa chỉ IP của E. Vì số lượng các thiết bị trung gian là 2, nên máy A biết máy đích nằm trên mạng khác và do đó sẽ phải chuyển qua router trung gian. Ngoài ra bảng định tuyến tại A cũng cho biết để gửi tới E, đầu tiên A phải gửi gói dữ liệu tới địa chỉ IP 223.1.1.4 – là địa chỉ IP của giao diện router nằm trên cùng một mạng với A. Thực thể IP trong máy A chuyển gói dữ liệu xuống tầng liên kết dữ liệu và yêu cầu chuyển tới địa chỉ IP 223.1.1.4. Một chú ý rất quan trọng ở đây là mặc dù gói dữ liệu IP được gửi tới giao diện của router (qua tầng liên kết dữ liệu), địa chỉ đích trong gói dữ liệu vẫn là địa chỉ đích cuối cùng (địa chỉ E) chứ không phải là địa chỉ router trung gian.

| Dest. Network | Next router | Nhops | Interface |
|---|---|---|---|
| 223.1.1.0/24 | – | 1 | 223.1.1.4 |
| 223.1.2.0/24 | – | 1 | 223.1.2.9 |
| 223.1.3.0/24 | – | 1 | 223.1.3.27 |




**Hình 4.19 Chuyển dữ liệu từ A đến E**

Khi gói dữ liệu tới router thì trách nhiệm chính của router là chuyể gói dữ liệu hướng tới đích cuối cùng. Như minh họa trong Hình 4.19, rout tìm trên bảng định tuyến và thấy hàng 223.1.2.0/24 trùng với phần mạng đ chỉ IP của E. Như vậy gói dữ liệu phải được chuyển đến giao diện của rout có địa chỉ IP là 223.1.2.9. Vì số lượng các thiết bị trung gian giữa router v đích là 1, nên router biết rằng đích (E) nằm trên cùng một mạng với gi diện ứng với địa chỉ 223.1.2.9, vì thế router chuyển gói dữ liệu tới giao d (cổng) này, và sau đó gói dữ liệu được chuyển trực tiếp tới E.



Chú ý rằng trong Hình 4.19, các hàng trong cột "next router" là rỗng vì mỗi mạng (223.1.1.0/24, 223.1.2.0/24, và 223.1.3.0/24) được kết nối trực tiếp với router. Trong trường hợp này, chúng không cần phải đi qua các router trung gian để đến đích. Tuy nhiên nếu máy A và máy E cách nhau 2 router thì trong trong bảng định tuyến của router đầu tiên trên tuyến đường từ A tới E, dòng tương ứng với đích E sẽ chỉ ra phải qua 2 chặng nữa mới tới được đích và phải chỉ ra địa chỉ IP của router thứ hai trên tuyến đường. Router đầu tiên sẽ chuyển gói dữ liệu tới router thứ hai nhờ vào giao thức của tầng liên kết dữ liệu giữa hai router. Kế đó router thứ hai sẽ chuyển gói dữ liệu tới máy đích nhờ giao thức tầng liên kết dữ liệu giữa router thứ hai và máy đích.

Định tuyến cho gói dữ liệu trên mạng Internet tương tự việc người lái xe hỏi đường cảnh sát giao thông tại mỗi bùng binh. Trên đường di chuyển từ nguồn tới đích, gói dữ liệu sẽ đi qua nhiều router. Tại mỗi router, gói tin dừng lại và "hỏi" router đi đường nào để tới đích. Trừ khi router trên cùng mạng với máy tính đích, về cơ bản, bảng định tuyến trong router sẽ nói với gói dữ liệu: "Tôi không biết chính xác đi đến đích như thế nào, nhưng tôi biết hướng tới nó là đi theo đường này". Sau đó gói dữ liệu sẽ được gửi đi trên đường kết nối này để đến một router khác và lại hỏi tiếp tục hỏi đường.

Rõ ràng bảng định tuyến của router đóng vai trò then chốt trong việc định tuyến gói tin qua mạng Internet. Nhưng làm thế nào để cấu hình và bảo trì bảng định tuyến trong một hệ thống liên mạng cực lớn với nhiều tuyến đường giữa đích và nguồn (như trong mạng Internet). Rõ ràng bảng định tuyến phải được cấu hình sao cho các gói dữ liệu được đi theo tuyến đường tốt nhất từ nguồn tới đích. Chính các thuật toán định tuyến đã nói tới trong mục 4.2 thực hiện công việc định tuyến và cập nhật bảng định tuyến. Thuật toán định tuyến của Internet được trình bày trong mục 4.5.

## 4.3 Khuôn dạng gói dữ liệu IP

Sau đây là các trường trong gói dữ liệu IPv4:

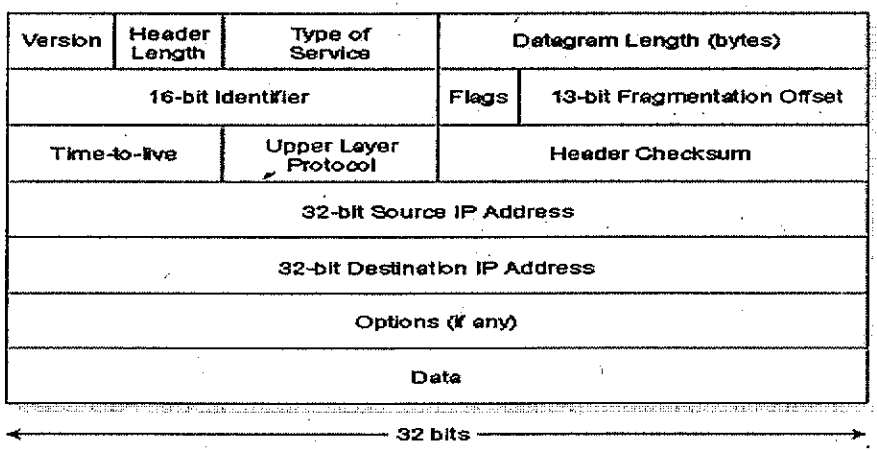
***Phiên bản (version):*** Trường 4 bit này xác định phiên bản giao thức của gói dữ liệu. Qua trường phiên bản, router mới xác định được ý nghĩa các trường còn lại của gói dữ liệu IP. Các phiên bản IP khác nhau sử dụng các khuôn dạng dữ liệu khác nhau. Khuôn dạng gói dữ liệu IP hiện tại - IPv4

- được minh họa trong Hình 4.20. Khuôn dạng gói dữ liệu IPv6 được trình bày trong phần 4.7.

***Độ dài tiêu đề (Header length):*** Gói dữ liệu IPv4 có thể có nhiều trường mang tính lựa chọn (không bắt buộc phải có). 4 bit này được dùng để xác định vị trí bắt đầu của dữ liệu thực sự trong gói dữ liệu IP. Tuy nhiên phần lớn gói dữ liệu IP không chứa các trường lựa chọn nên tiêu đề của gói dữ liệu thường cố định là 20 byte.

***Kiểu dịch vụ (Type of service – TOS)***: Trường kiểu dịch vụ (TOS) giúp phân biệt các kiểu khác nhau của gói dữ liệu IP, để từ đó có thể xử lý theo những cách khác nhau. Ví dụ khi mạng quá tải, cần phân biệt được gói dữ liệu chứa thông tin kiểm soát mạng (ICMP) với gói dữ liệu thực sự (thông điệp HTML) hay giữa datagram chứa dữ liệu thời gian thực (ứng dụng điện thoại qua Internet) với datagram không chứa dữ liệu thời gian thực (ứng dụng FTP). Gần đây Cisco (công ty chiếm thị phần router lớn nhất) đã sử dụng 3 bit đầu tiên của trường TOS để định nghĩa các mức dịch vụ khác nhau mà router có thể cung cấp. Các mức dịch vụ cụ thể được người quản trị router thiết lập theo những tiêu chí của tổ chức.

***Độ dài gói dữ liệu (datagram length)***: đây là tổng độ dài của gói dữ liệu IP (cả phần tiêu đề lẫn phần dữ liệu) tính theo byte. Độ dài trường này là 16 bit nên về lý thuyết kích thước tối đa của gói dữ liệu IP là 65.535 byte. Tuy nhiên, hiếm khi kích thước gói dữ liệu vượt quá 1500 byte và thường giới hạn là 576 byte.




**Hình 4.20 Khuôn dạng gói dữ liệu IP**



***Định danh, cờ và vị trí phân đoạn (Identifier, Flags, Fragmention Offset).*** 3 trường này được sử dụng khi phân mảnh gói IP (fragmentation), một chủ đề chúng ta sẽ xem xét chi tiết dưới đây. Chú ý phiên bản mới của IP (IPv6) không cho phép phân mảnh gói dữ liệu tại các router.

***Thời gian tồn tại (Time-to-live-TTL):*** Trường thời gian tồn tại (TTL) được sử dụng để bảo đảm gói dữ liệu không thể lưu chuyển mãi mãi trong mạng (nguyên nhân có thể do định tuyến lặp nên các gói tin truyền lòng vòng theo một chu trình). Trường này bị giảm đi một (-1) mỗi lần gói tin đi qua router. Nếu trường TTL bằng 0, router sẽ loại bỏ gói tin.

***Giao thức (Protocol):*** Trường này chỉ được sử dụng khi gói dữ liệu IP đến được máy tính đích. Giá trị của trường này xác định giao thức tầng giao vận ở máy tính đích sẽ nhận được phần dữ liệu trong gói dữ liệu IP. Ví dụ giá trị 6 có ý nghĩa phần dữ liệu cần chuyển tới thực thể TCP, giá trị 17 có ý nghĩa phần dữ liệu phải chuyển đến thực thể UDP. RFC 1700 liệt kê các giá trị này. Chú ý rằng vai trò của trường giao thức trong gói dữ liệu IP tương tự vai trò trường số hiệu cổng trong segment của tầng giao vận. Trường giao thức được xem là điểm nối giữa tầng mạng và tầng giao vận cũng như trường số hiệu cổng là điểm nối giữa tầng giao vận với ứng dụng cụ thể. Trong chương 5 chúng ta cũng sẽ thấy trong frame của tầng liên kết dữ liệu cũng có một trường đặc biệt để nối với tầng mạng.

***Checksum của tiêu đề (Header checksum)***: Trường checksum trong tiêu đề giúp router phát hiện lỗi trong tiêu đề gói dữ liệu IP được gửi đến. Giá trị checksum được tính bằng cách xem phần tiêu đề là một chuỗi các từ hai byte, cộng các từ này lại và sau đó lấy bù một. Như đã thảo luận trong phần 3.3, số bù một của tổng này được gọi là Internet checksum. Router tính lại Internet checksum cho mỗi gói dữ liệu IP nhận được và có thể phát hiện ra lỗi nếu như giá trị checksum tính lại khác giá trị checksum trong gói dữ liệu. Router thường loại bỏ những gói dữ liệu bị lỗi. Chú ý rằng router phải tính lại checksum, trường TTL và có thể một số trường khác. RFC 1071 trình bày phương thức tính checksum nhanh. Một vấn đề thường được đặt ra ở đây là tại sao TCP/IP thực hiện kiểm tra lỗi ở cả tầng giao vận lẫn tầng mạng? Có nhiều nguyên nhân của việc này. Thứ nhất: các router không bắt buộc phải kiểm tra lỗi, vì vậy tầng giao vận không thể dựa vào tầng mạng để làm việc này. Thứ hai: TCP/UDP và IP không nhất thiết nằm trong cùng một nhóm giao thức. TCP có thể chạy trên giao thức khác (ví dụ ATM) và IP có thể chuyển dữ liệu không phải là TCP hay UDP segment.

*Địa chỉ IP nguồn và đích:* Những trường này là 32 bit địa chỉ IP của máy tính gửi và máy tính nhận. Tầm quan trọng của địa chỉ đích là rõ ràng. Trong phần 3.2 chúng ta thấy rằng địa chỉ IP máy gửi (cùng với số hiệu cổng nguồn và đích) được máy nhận sử dụng để hướng dữ liệu ứng dụng tới socket phù hợp.

*Lựa chọn (Option):* Các trường này cho phép mở rộng tiêu đề IP. Phần lựa chọn trong tiêu đề hiếm khi được sử dụng. Sự tồn tại của phần lựa chọn trong tiêu đề làm phức tạp việc xử lý các gói tin vì tiêu đề của gói dữ liệu có phần lựa chọn không có độ dài cố định, do đó không xác định được vị trí bắt đầu của dữ liệu thực sự. Như vậy thời gian xử lý gói dữ liệu IP tại mỗi router có thể khác nhau. Đây là nhược điểm của các mạng hiệu suất cao. Vì thế, IPv6 sẽ loại bỏ các trường lựa chọn.

*Dữ liệu (payload):* Cuối cùng là trường quan trọng nhất - trường dữ liệu. Thông thường trường dữ liệu của gói IP là gói dữ liệu của tầng giao vận (TCP hay UDP segment). Tuy nhiên, trường dữ liệu có thể là các kiểu dữ liệu khác, ví dụ thông điệp ICMP (sẽ được trình bày trong phần 4.4.5).

## 4.4.4 Phân mảnh (Fragmentation) và Hợp nhất (Reassembly) gói tin IP

Trong chương 5 chúng ta sẽ thấy không phải tất cả các giao thức của tầng liên kết dữ liệu đều có khả năng truyền các gói tin (packet) có cùng độ lớn. Một vài giao thức có khả năng gửi những gói tin lớn trong khi một vài giao thức chỉ có thể gửi những gói tin nhỏ. Ví dụ, gói tin của mạng Ethernet có độ lớn lên tới 1500 byte, trong khi gói tin trên những liên kết ở mạng diện rộng có độ lớn không được vượt quá 576 byte. Số lượng dữ liệu tối đa của gói tin trên một đường truyền vật lý được định nghĩa là **MTU (maximum transfer unit)**. Gói dữ liệu IP được đặt trong gói dữ liệu của tầng liên kết dữ liệu giữa hai router kế tiếp nhau trên đường truyền. Vì thế giá trị MTU của giao thức ở tầng liên kết dữ liệu giới hạn độ dài gói tin IP. Giới hạn kích thước gói tin IP không phải là vấn đề lớn. Vấn đề ở đây là kết nối giữa các router dọc theo tuyến đường từ nơi gửi đến nơi nhận có thể sử dụng các giao thức liên kết dữ liệu khác nhau có giá trị MTU khác nhau.



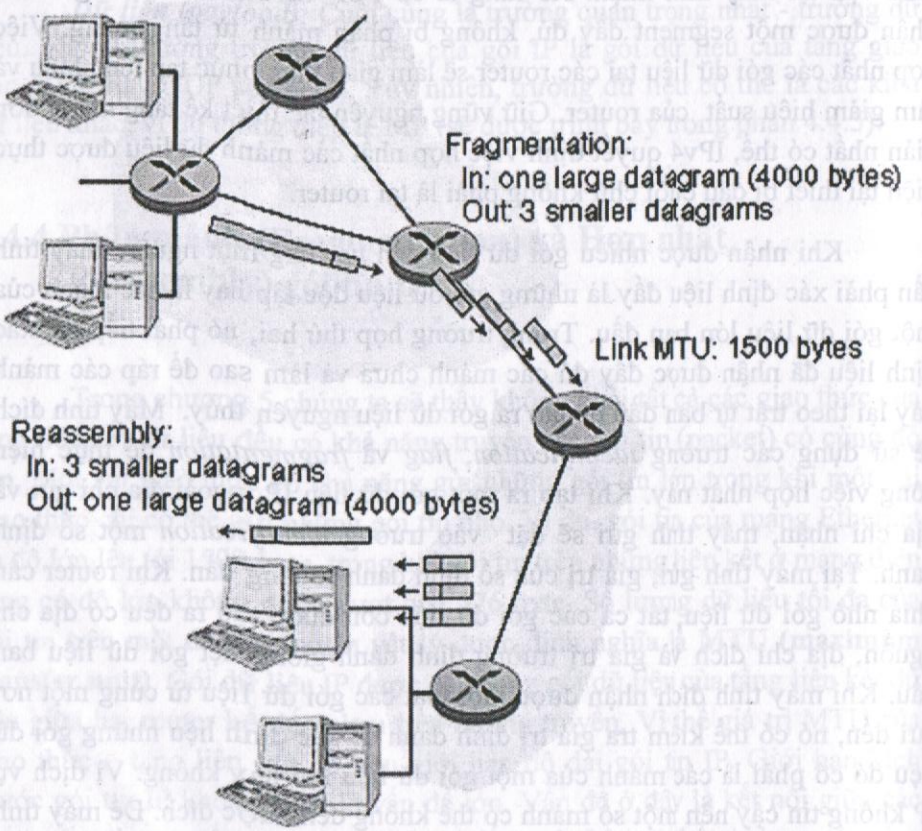
Để hiểu vấn đề rõ hơn, xét router với nhiều kết nối, mỗi kết nối có một giao thức liên kết dữ liệu khác nhau với giá trị MTU khác nhau. Giả sử khi nhận được gói dữ liệu đến từ kết nối nào đó, căn cứ vào địa chỉ đích, router kiểm tra bảng định tuyến để xác định cần gửi gói tin đi ra theo kết nối nào. Tuy nhiên đường kết nối ra ngoài này có giá trị MTU nhỏ hơn độ dài gói dữ liệu IP. Làm thế nào router có thể đặt gói tin IP lớn trong gói tin của tầng liên kết dữ liệu có kích thước nhỏ hơn? Giải pháp cho vấn đề này là phân mảnh (fragmentation) dữ liệu trong gói dữ liệu IP thành nhiều gói dữ liệu IP nhỏ hơn và sau đó gửi những gói dữ liệu nhỏ hơn này trên đường kết nối. Mỗi gói dữ liệu IP nhỏ này được coi là một mảnh (fragment).

Các mảnh tách rời này cần được ráp lại trước khi chuyển lên tầng giao vận tại máy tính nhận. Rõ ràng là cả TCP và UDP đều mong muốn nhận được một segment đầy đủ, không bị phân mảnh từ tầng mạng. Việc hợp nhất các gói dữ liệu tại các router sẽ làm giao thức phức tạp lên nhiều và làm giảm hiệu suất của router. Giữ vững nguyên tắc thiết kế tầng mạng đơn giản nhất có thể, IPv4 quyết định việc hợp nhất các mảnh dữ liệu được thực hiện tại thiết bị đầu cuối chứ không phải là tại router.

Khi nhận được nhiều gói dữ liệu đến từ cùng một nguồn, máy tính cần phải xác định liệu đấy là những gói dữ liệu độc lập hay là các mảnh của một gói dữ liệu lớn ban đầu. Trong trường hợp thứ hai, nó phải tiếp tục xác định liệu đã nhận được đầy đủ các mảnh chưa và làm sao để ráp các mảnh này lại theo trật tự ban đầu để tạo ra gói dữ liệu nguyên thủy. Máy tính đích sẽ sử dụng các trường *identification*, *flag* và *fragmentation* để thực hiện công việc hợp nhất này. Khi tạo ra một gói dữ liệu IP, ngoài địa chỉ gửi và địa chỉ nhận, máy tính gửi sẽ đặt vào trường *identification* một số định danh. Tại máy tính gửi, giá trị của số định danh sẽ tăng dần. Khi router cần chia nhỏ gói dữ liệu, tất cả các gói dữ liệu con được tạo ra đều có địa chỉ nguồn, địa chỉ đích và giá trị trường định danh giống hệt gói dữ liệu ban đầu. Khi máy tính đích nhận được một loạt các gói dữ liệu từ cùng một nơi gửi đến, nó có thể kiểm tra giá trị định danh để xác định liệu những gói dữ liệu đó có phải là các mảnh của một gói dữ liệu lớn hay không. Vì dịch vụ IP không tin cậy nên một số mảnh có thể không đến được đích. Để máy tính nhận có thể chắc chắn là đã nhận được mảnh cuối cùng của gói dữ liệu ban đầu, thì trường cờ của mảnh cuối cùng phải có giá trị 0, trong khi trường cờ

của các mảnh khác có giá trị 1. Tương tự để máy nhận xác định được liệu có mất mảnh nào không (và để ghép các mảnh theo đúng thứ tự), trường Offset được sử dụng để xác định vị trí của mảnh trong gói dữ liệu IP ban đầu.

Xét ví dụ trên Hình 4.21. Một gói dữ liệu có độ lớn 4000 byte đến router và phải gửi qua đường liên kết có MTU là 1500 byte. Điều này có nghĩa rằng 3980 byte dữ liệu trong gói dữ liệu ban đầu phải được tách ra thành ba mảnh phân biệt (mỗi mảnh trở thành một gói dữ liệu IP độc lập). Giả sử trong gói dữ liệu ban đầu giá trị trường định danh là 777. Giá trị các trường trong ba phân mảnh này được chỉ ra trong Bảng 4.3




Hình 4.21 Phân mảnh và hợp nhất gói dữ liệu IP



Dữ liệu của gói IP chỉ được chuyển lên tầng giao vận tại máy tính nhận khi tầng IP tái tạo hoàn chỉnh gói dữ liệu IP ban đầu. Nếu một số mảnh dữ liệu bị mất, không đến được đích, thì toàn bộ gói dữ liệu sẽ bị loại bỏ và không được chuyển lên tầng giao vận. Nhưng như đã nghiên cứu trong chương trước, nếu sử dụng TCP ở tầng giao vận, thì thực thể TCP sẽ khắc phục mất mát do phía gửi sẽ gửi lại gói dữ liệu ban đầu.

| Fragment | Bytes | ID | Offset | Flag |
|---|---|---|---|---|
| 1 | 1480 byte trong trường dữ liệu | identification=777 | offset=0 (dữ liệu bắt đầu từ byte thứ 0) | flag=1 (còn mảnh nữa) |
| 2 | 1480 byte trong trường dữ liệu | identification=777 | offset=1480 (dữ liệu bắt đầu từ byte thứ 1480) | flag=1 (còn mảnh nữa) |
| 3 | 1020 byte (=3980 - 1480 - 1480) trong trường dữ liệu | identification=777 | offset=2960 (dữ liệu bắt đầu từ byte thứ 2960) | flag=0 (đây là mảnh cuối cùng) |

Bảng 4.3 Ví dụ phân mảnh gói tin

Phân mảnh và hợp nhất khiến nhiệm vụ xử lý gói tin tại router (tạo ra các mảnh) và thiết bị nhận (hợp nhất các mảnh) phức tạp hơn. Vì thế người ta cố gắng giảm thiểu việc phân mảnh dữ liệu. Điều này thường được thực hiện bằng cách giới hạn độ lớn gói dữ liệu của tầng giao vận (TCP hay UDP segment) bởi một giá trị tương đối nhỏ. Khi đó việc phân mảnh trở nên không cần thiết. Vì phần lớn các giao thức liên kết dữ liệu hỗ trợ IP có MTU tối thiểu là 536 byte, có thể loại bỏ hoàn toàn việc phân mảnh nếu đặt giá trị MSS là 536 byte với 20 byte tiêu đề của gói TCP và 20 byte tiêu đề của gói IP. Đây chính là lý do hầu hết các gói TCP khi truyền khối lượng lớn dữ liệu (chẳng hạn FTP) có độ dài từ 512 đến 536 byte (Khi duyệt WEB, bạn sẽ thấy thường khoảng 500 byte dữ liệu đến cùng một lần).

Nếu gói TCP được lồng trong gói IP và cả hai gói TCP và IP đều không có trường tùy chọn (option) thì gói dữ liệu IP sẽ có 40 byte tiêu đề, phần còn lại là dữ liệu ứng dụng.

### 4.4.5 Giao thức kiểm soát lỗi ICMP (Internet Control Message Protocol)

ICMP được các máy tính đầu cuối, router và các cổng (gateway) sử dụng để trao đổi các thông tin tầng mạng với nhau. ICMP được đặc tả trong RFC 792. ICMP được sử dụng chủ yếu cho việc báo lỗi. Ví dụ khi chạy một phiên Telnet, FTP, hoặc HTTP, bạn có thể gặp một thông điệp như "Destination network unreachable" (*Không đến được mạng đích).* Thông điệp này có do thực thể ICMP ở router tạo ra. Khi không tìm được đường dẫn đến máy tính đích, router sẽ tạo ra và gửi thông báo ICMP kiểu 3 tới máy tính của bạn với mục đích thông báo lỗi. Máy tính nhận được thông báo lỗi ICMP sẽ trả lại mã lỗi cho thực thể TCP đang cố gắng kết nối tới máy tính đích. Đến lượt lượt mình, TCP trả lại mã lỗi cho ứng dụng (là phiên làm việc FTP, HTTP...).

ICMP thường được coi là một phần của IP, nhưng về mặt kiến trúc lại nằm trên IP, bởi vì thông báo ICMP được đặt trong gói IP, giống như TCP hay UDP segment nằm trong trường dữ liệu (payload) của gói dữ liệu IP. Tương tự, khi nhận được một gói tin IP với trường *protocol* xác định giao thức ICMP, tầng mạng của máy tính nhận sẽ chuyển phần dữ liệu (là thông điệp ICMP) lên thực thể ICMP, giống như đã làm với TCP hay UDP.

Thông báo ICMP có trường kiểu (type) và trường mã (code), và chứa 8 byte đầu tiên của gói dữ liệu IP gây ra lỗi (nguyên nhân để tạo ra thông báo ICMP). Do đó phía gửi có thể xác định được gói tin nào gây ra lỗi. Một số kiểu thông điệp ICMP tiêu biểu được minh họa trên Hình 4.22. Chú ý rằng thông báo ICMP không chỉ được sử dụng để báo lỗi. Chương trình ping rất thông dụng gửi thông báo ICMP kiểu 8, mã 0 tới máy tính nào đó, máy tính nhận được yêu cầu ICMP sẽ gửi lại một thông báo ICMP phản hồi với kiểu 0, mã 0.



| ICMP Type | Code | Description |
|---|---|---|
| 0 | 0 | echo reply (to ping) |
| 3 | 0 | destination network unreachable |
| 3 | 1 | destination host unreachable |
| 3 | 2 | destination protocol unreachable |
| 3 | 3 | destination port unreachable |
| 3 | 6 | destination network unknown |
| 3 | 7 | destination host unknown |
| 4 | 0 | source quench (congestion control) |
| 8 | 0 | echo request |
| 9 | 0 | router advertisement |
| 10 | 0 | router discovery |
| 11 | 0 | TTL expired |
| 12 | 0 | IP header bad |

**Hình 4.22 Các kiểu thông điệp ICMP hay gặp**

Chương trình ***Traceroute*** cho phép bạn xác định tất cả các router trên một tuyến đường giữa bất kỳ hai thiết bị đầu cuối nào. Chương trình Traceroute cũng sử dụng các thông báo của ICMP để xác định tên và địa chỉ của các router giữa nguồn và đích. Chương trình Traceroute trong máy tính nguồn sẽ gửi đi một loạt các gói dữ liệu IP tới máy tính đích. Gói IP đầu tiên có trường TTL nhận giá trị 1, gói thứ hai là 2, gói thứ ba là 3,... Máy tính nguồn đặt timer cho mỗi gói IP gửi đi. Khi gói IP thứ n đến router thứ n, router này thấy trường TTL của gói dữ liệu nhận giá trị 0, nên theo nguyên tắc của giao thức IP, router sẽ loại bỏ gói dữ liệu và gửi thông điệp cảnh báo ICMP (kiểu 11 mã 0). Trong thông điệp cảnh báo này có tên và địa chỉ IP của router. Khi nhận được thông báo ICMP, máy tính nguồn xác định được thời gian khứ hồi đến router thứ n (nhờ timer) cũng như tên, và địa chỉ IP của router đó.

## 4.5 ĐỊNH TUYẾN TRÊN INTERNET

Sau khi đã nghiên cứu về địa chỉ Internet và giao thức IP, bây giờ chúng ta nói tới các giao thức định tuyến của Internet – là các giao thức xác

định tuyến đường đi từ nguồn tới đích. Chúng ta sẽ thấy rằng các giao thức định tuyến của Internet được triển khai dựa trên những nguyên tắc mà chúng ta đã nói tới: link state và distance vector trong phần 4.2, miền tự trị (AS) trong phần 4.3.

Mạng Internet toàn cầu ngày nay là sự kết hợp lỏng lẻo của nhiều mạng bao gồm các ISP khu vực, quốc gia và quốc tế. Trong phần 4.3 chúng ta thấy rằng tập hợp các router cùng nằm dưới một một sự quản trị - ít nhất về mặt kỹ thuật - tạo thành miền tự trị (AS). Mỗi AS lại có thể bao gồm nhiều mạng (ở đây chúng ta sẽ sử dụng thuật ngữ "mạng" với ý nghĩa giống trong phần 4.4). Điểm phân biệt quan trọng nhất giữa các giao thức định tuyến của Internet là liệu chúng được sử dụng để định tuyến trong một miền hay giữa các miền với nhau. Phần 4.5.1 giới thiệu giao thức định tuyến trong một miền và phần 4.5.2 giới thiệu các giao thức định tuyến giữa các miền.

## 4.5.1 Định tuyến trong một miền (Intra-AS routing) (Định tuyến nội miền)

Giao thức định tuyến Intra-AS được sử dụng để cấu hình và duy trì bảng định tuyến trong tất cả các router thuộc cùng một miền. Những giao thức định tuyến kiểu này được gọi là **giao thức định tuyến nội miền (interior gateway protocol)**. Trên Internet có 3 giao thức định tuyến nội miền được sử dụng rộng rãi: **RIP** (Routing Information Protocol), **OSPF** (Open Shortest Path First) và **EIGRP** (Cisco's propriety Enhanced Interior Gateway Routing Protocol).

### RIP (Routing Information Protocol)

RIP là một trong những giao thức định tuyến nội miền đầu tiên. Nó được triển khai trong một chương trình được gọi là ***routed*** trong phần lớn các hệ thống UNIX. RIP có một số đặc điểm sau:

**Định tuyến nội miền**: Cho phép các router trong một miền trao đổi thông tin với nhau.

**Đo khoảng cách bằng chặng**: Giá đường đi giữa hai thiết bị đầu cuối được xác định bằng số lượng các router trung gian trên đường đi đó. Độ



dài tối đa của một tuyến đường là 15, nghĩa là đường kính tối đa của một miền là 15 router.

**Truyền thông không tin cậy**: RIP sử dụng UDP để chuyển thông điệp.

**Gửi quảng bá (broadcast) và multicast:** RIP được sử dụng chủ yếu trên mạng cục bộ (LAN) hỗ trợ công nghệ truyền quảng bá (mạng Ethernet). RIP v1 sử dụng cách truyền quảng bá khi truyền giữa hai router. RIP v2 cho phép truyền theo chế độ multicast.

**Thuật toán distance vector**. RIP sử dụng thuật toán distance vector. Các router hàng xóm trao đổi bảng định tuyến cho nhau 30s một lần trong các thông điệp RIP (RIP response message, RIP advertisement), mỗi thông điệp chứa tối đa 25 địa chỉ đích tới.

**Các máy tính có thể thụ động nhận thông tin từ các router**. RIP cho phép các thiết bị đầu cuối (chủ yếu là máy tính) lắng nghe và cập nhật bảng định tuyến. Điều này đặc biệt hữu dụng với các mạng có nhiều router. Khi đó máy tính trong mạng có thể dễ dàng xác định được router cần chuyển tới.

Chú ý rằng router gửi một thông điệp RIP liệt kê các mạng mà nó có thể kết nối tới. Khi nhận được một quảng cáo như vậy, thực thể RIP (phần mềm) trên router sử dụng những thông tin này để cập nhật lại bảng định tuyến của mình. Mỗi một trường trong thông điệp quảng cáo là một cặp:

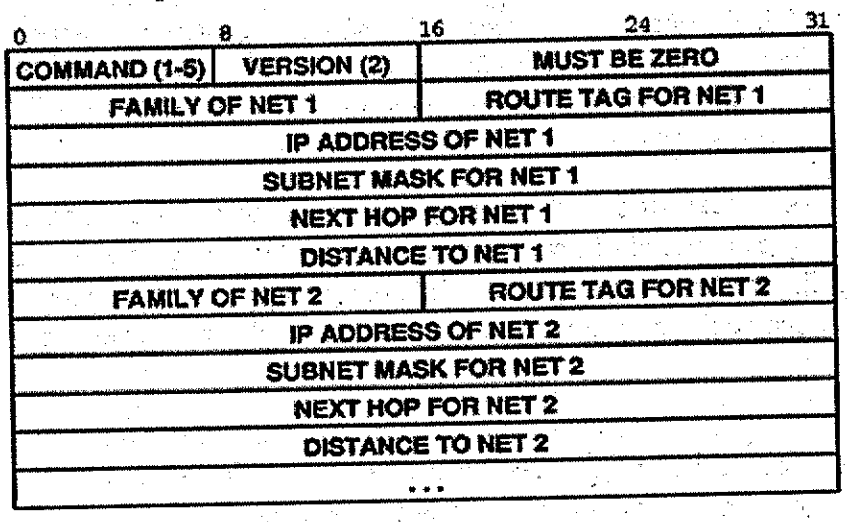
(địa chỉ mạng đích **n**, khoảng cách **r**)

trong đó khoảng cách **r** là số lượng các router trung gian từ router gửi thông điệp tới đích có địa chỉ mạng là **n**. Khi nhận được một thông điệp, giả sử router nhận không có đường đi tới đích được quảng cáo trong thông điệp hoặc có đường đi đến đích nhưng giá lớn hơn, router sẽ cập nhật bảng định tuyến để sử dụng tuyến đường vừa mới nhận được quảng cáo (điểm đầu tiên trên tuyến đường này chính là router gửi quảng cáo).

Ưu điểm chính của RIP là tính đơn giản. RIP không đòi hỏi cấu hình nhiều. Người quản trị chỉ cần bật máy lên, cho phép router trao đổi thông tin với nhau, sau một thời gian ngắn, router sẽ tự xây dựng được bảng định tuyến cho mình.

Tổ chức có thể lựa chọn một router trong miền làm router ngầm định, thường là router nối với ISP. Sau đó RIP sẽ thực hiện việc quảng cáo cho router ngầm định này. Sau đó các gói tin gửi ra phía ngoài sẽ được gửi qua router ngầm định tới ISP.

Hình 4.23 minh họa khuôn dạng thông điệp cập nhật RIP. Mỗi trường trong thông điệp ứng với một địa chỉ đích, mặt nạ mạng của địa chỉ đích (do đó có thể sử dụng địa chỉ không phân lớp CIDR), khoảng cách tới đích và nút kế tiếp trên đường tới đích.




**Hình 4.23 Khuôn dạng gói dữ liệu RIP**

### *OSPF – Open Shartest Path First*

RIP có một số nhược điểm của thuật toán distance vector. Độ dài của thông điệp có thể lớn do phải liệt kê toàn bộ danh sách các địa chỉ đích và khoảng cách tới đó. Khi nhận được thông điệp, router nhận phải lấy ra từng trường, so sánh trong bảng định tuyến, như vậy thời gian xử lý thông điệp trong mỗi router lớn, gây ra một độ trễ nào đó. Do vậy RIP chỉ phù hợp với các mạng có kích cỡ nhỏ.

Khi một tổ chức mạng tương đối lớn, người ta cần phải đưa ra giao thức phù hợp hơn. IETF đưa ra OSPF với các đặc điểm sau:



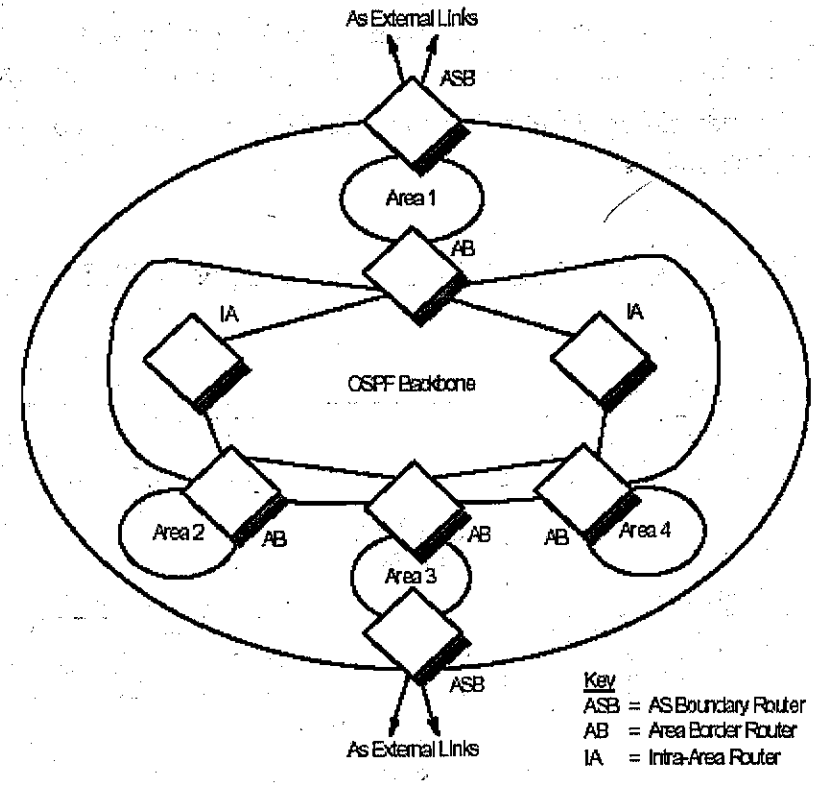
**Định tuyến nội miền**: Cho phép trao đổi thông tin giữa các router trong một miền.

**Hỗ trợ phân mạng và CIDR.** Bên cạnh địa chỉ IP 32 bit là mặt nạ 32 bit. Do đó OSPF hỗ trợ việc phân mạng, chia mạng to ra các mạng con.

**Trao đổi các thông tin đã được kiểm chứng.** Hai router trao đổi thông điệp OSPF với nhau có thể tiến hành thủ tục kiểm tra để xác định mình nhận được thông điệp từ đúng phía bên kia. Điều này ngăn ngừa được tin tặc tiến hành các cuộc tấn công bằng phương pháp giả mạo.

**Sử dụng thuật toán Link state.**

**Hỗ trợ phân cấp trong miền.** Ưu điểm chính của OSPF là cho phép tiếp tục phân một miền thành nhiều miền con.




**Hình 4.24 OSPF cho phép chia miền con**

### 4.5.2 Định tuyến giữa các miền (Inter-AS routing) (Định tuyến liên miền)

Giao thức BGP (Border Gateway Protocol v4) (xem đặc tả RFC 1771, 1772, 1773) được xem là một chuẩn ngầm định *de facto* trong định tuyến liên miền trên Internet ngày nay. Nhiệm vụ của nó là định tuyến giữa các miền được quản trị độc lập với nhau.

**BGP (Border Gateway Protocol)**

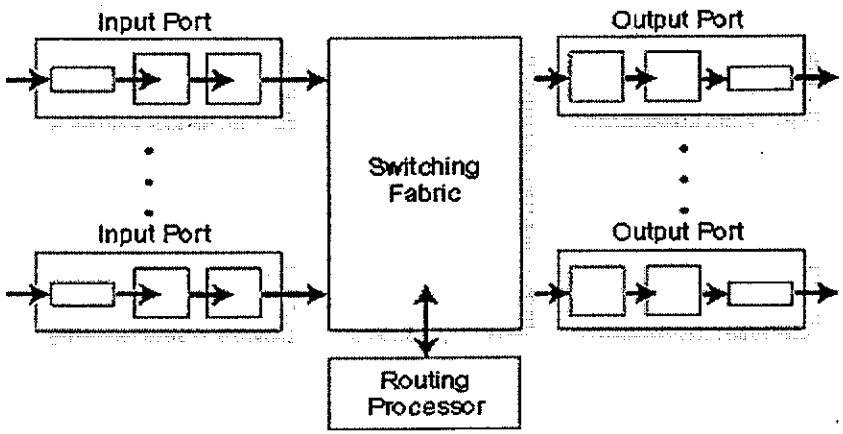
BGP là giao thức liên miền chủ yếu được sử dụng hiện nay. BGP có những đặc điểm sau:

**Định tuyến liên miền.** BGP cho phép cung cấp các thông tin định tuyến giữa các miền. Mỗi tuyến đường được xem là một chuỗi các AS liên tiếp nhau.

**Hỗ trợ việc thiết lập chính sách (policy).** Người quản trị có thể áp dụng những chính sách nào đó, ví dụ hạn chế việc quảng cáo ra phía ngoài.

**Truyền thông tin cậy.** Hai thực thể BGP sử dụng kết nối TCP để trao đổi thông điệp.

## 4.6 CẤU TẠO CỦA THIẾT BỊ ĐỊNH TUYẾN (ROUTER)




Hình 4.25 Kiến trúc bộ định tuyến



Các phần trước trình bầy về các mô hình dịch vụ của tầng mạng, các thuật toán định tuyến xác định đường đi cho các gói tin trên mạng cũng như các giao thức gắn với các thuật toán ấy. Trong phần này, chúng ta sẽ nói đến một chủ đề quan trọng khác - chức năng chuyển mạch của bộ định tuyến – công việc thực sự để chuyển một datagram từ liên kết này tới liên kết kia. Chỉ nghiên cứu các khía cạnh về mặt kiểm soát và dịch vụ của tầng mạng cũng giống như nghiên cứu một công ty mà chỉ tìm hiểu cơ chế quản lý của công ty và các quan hệ với bên ngoài. Để hiểu rõ về công ty, người ta phải xem xét đến công nhân. Trong tầng mạng, công việc thực sự của việc truyền gói tin chính là việc chuyển gói tin từ liên kết này tới liên kết kia của router. Trong mục này chúng ta sẽ nghiên cứu router thực hiện công việc này như thế nào.

Một cách tổng thể, kiến trúc chung của router được minh họa trong Hình 4.25. Bốn thành phần chính của router được xác định như sau:

**Cổng vào (Input port).** Cổng vào của router thực hiện một số chức năng: chức năng của tầng vật lý (hộp ngoài cùng cổng vào và cổng ra); chức năng của tầng liên kết dữ liệu (là các hộp ở giữa đối với cả đường vào và đường ra) cần thiết để làm việc được với tầng liên kết dữ liệu ở đầu bên kia của kết nối; chức năng tìm kiếm và chuyển (hộp trong cùng của cổng vào và cổng ra). Gói tin từ cổng vào sẽ đi qua kết cấu chuyển để tới cổng ra phù hợp. Các gói tin chứa thông tin điều khiển (chứa thông tin điều khiển của các giao thức RIP, OSPF, BGP) sẽ được chuyển từ cổng vào đến bộ xử lý của router.

**Kết cấu chuyển (Switching fabric).** Kết cấu chuyển nối cổng vào của router tới cổng ra. Kết cấu chuyển nằm hoàn toàn trong router – là một mạng chuyển mạch nằm bên trong router mạng.

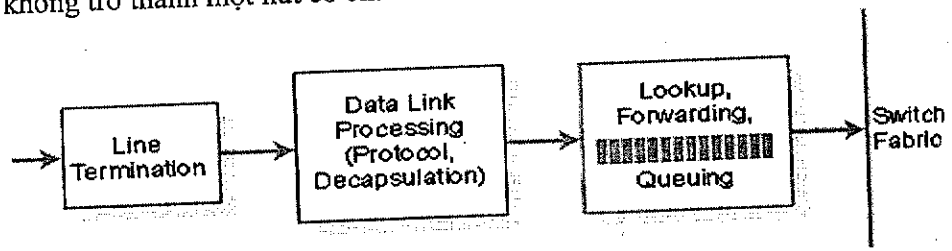
**Cổng ra (output port)** Cổng ra nhận những gói dữ liệu gửi tới nó qua kết cấu chuyển và sau đó truyền gói dữ liệu này trên đường nối ra ngoài. Nó cũng thực hiện chức năng của tầng liên kết dữ liệu và tầng vật lý.

**Bộ xử lý (Routing Processor)** Bộ xử lý router thực hiện các giao thức định tuyến, (ví dụ các giao thức đã nói trong phần 4.5), duy trì bảng định tuyến, và thực hiện một số chức năng quản trị mạng.

Dưới đây chúng ta sẽ nghiên cứu các thành phần này một cách kỹ lưỡng hơn.

### 4.6.1 Cổng vào (Input port)

Hình 4.26 minh họa chi tiết các chức năng của cổng vào. Như đã nói ở trên, chức năng kết thúc tín hiệu trên đường truyền (line termination) và xử lý liên kết dữ liệu ứng với tầng vật lý và tầng liên kết dữ liệu của một đường truyền vật lý thực sự với router. Chức năng tìm kiếm và chuyển tiếp của cổng vào đóng vai trò trung tâm trong việc chuyển của bộ định tuyến. Trong nhiều router, cổng vào chính là nơi xác định cổng ra cho một gói dữ liệu. Cổng ra được xác định nhờ các thông tin lưu trong bảng định tuyến. Mặc dù bảng định tuyến được bộ xử lý tạo ra, song mỗi cổng vào đều có một bảng sao chép bảng định tuyến và cập nhật khi cần thiết. Nhờ vậy, quyết định chuyển đến cổng ra nào có thể được thực hiện cục bộ ở tại cổng vào, mà không cần đến bộ xử lý trung tâm. Điều này khiến bộ xử lý sẽ không trở thành một nút cổ chai của router.




**Hình 4.26 Cấu trúc cổng vào của Router**

Với những router mà khả năng xử lý ở cổng vào còn hạn chế, cổng vào sẽ chuyển gói dữ liệu tới bộ xử lí. Bộ xử lý sẽ tìm kiếm trên bảng định tuyến để xác định cổng ra thích hợp. Người ta thường áp dụng giải pháp này trong trường hợp router là một trạm làm việc hay một máy tính. Khi đó, bộ xử lí của router là bộ xử lý của trạm làm việc hay của máy tính. Cổng vào sẽ là card mạng (ví dụ card Ethernet).

Với bảng định tuyến xác định trước, tìm kiếm trên bảng định tuyến tương đối đơn giản. Duyệt toàn bộ bảng định tuyến để xác định hàng nào có địa chỉ phù hợp nhất với địa chỉ đích của gói dữ liệu, trong trường hợp không tìm thấy thì sử dụng cổng mặc định (Trong phần 4.4.1, chúng ta thấy



rằng địa chỉ phù hợp nhất là địa chỉ có tiền tố mạng dài nhất trùng với phần mạng của địa chỉ đích). Tuy nhiên triển khai trong thực tế lại không đơn giản như thế. Điều phức tạp nhất là router trên các trục chính (backbone router) phải hoạt động ở tốc độ cao, có khả năng thực hiện hàng triệu phép tra cứu mỗi giây. Thực sự người ta mong muốn tốc độ xử lý ở cổng vào phải ngang với tốc độ đường truyền (line speed), có nghĩa là tốc độ xử lý phải nhỏ hơn tốc độ đến của các gói tin. Như vậy gói tin có thể được xử lý xong trước khi gói tin kế tiếp đến.

Để hoạt động ở tốc độ cao không thể sử dụng phương pháp tìm kiếm tuyến tính trên bảng định tuyến, hợp lý hơn là lưu giữ giá trị của bảng định tuyến trong cấu trúc dữ liệu dạng cây. Mỗi mức trong cây ứng với vị trí một bit trong địa chỉ đích. Để tìm kiếm một địa chỉ, bắt đầu từ "gốc" của cây. Nếu bit địa chỉ đầu tiên là 0 thì địa chỉ cần tìm nằm trong cây con trái, ngược lại nằm trong cây con phải. Tiếp tục duyệt cây con bằng cách sử dụng các bit còn lại. Bit kế tiếp bằng 0, tìm trên cây con trái, bit kế tiếp bằng 1 tìm trên cây con phải. Người ta sẽ tìm kiếm bảng định tuyến trong N bước, N là số lượng bit trong địa chỉ.

Thậm chí với N = 32 (địa chỉ IP 32 bit), tốc độ tìm kiếm bằng kỹ thuật duyệt nhị phân chưa đủ nhanh để đáp ứng yêu cầu định tuyến trên các đường trục chính của Internet. Ví dụ tốc độ truy cập bộ nhớ là 40ns. Đã có một số kỹ thuật nâng cao tốc độ này. Bộ nhớ đánh địa chỉ theo nội dung (CAM – Content Addressable Addressing) cho phép địa chỉ IP 32 bit được biểu diễn trong CAM, và các trường tương ứng với địa chỉ đó được xác định trong khoảng thời gian cố định. Dòng router CISCO 8500 [Cisco 8500 1999] có 64K CAM cho mỗi cổng vào. Kỹ thuật khác làm tăng tốc độ tra cứu là lưu giữ các địa chỉ vừa được truy cập trong bộ nhớ cache có tốc độ truy cập nhanh. Vấn đề cần quan tâm ở đây là độ lớn của cache.

Khi xác định được cổng ra, gói dữ liệu sẽ được chuyển đến qua kết cấu chuyển. Tuy nhiên, gói dữ liệu tạm thời có thể bị "phong tỏa" chưa được chuyển qua kết cấu (có thể do các gói dữ liệu khác đang sử dụng kết cấu chuyển). Một gói dữ liệu bị phong tỏa phải xếp hàng ở cổng vào và đợi được lên lịch chuyển qua kết cấu tại một thời điểm nào đó.

# *Trong lịch sử*

## Công ty Cisco: thống trị thị trường mạng

Tháng giêng năm 2000, Công ty Cisco có 23000 công nhân và trị giá 360 tỉ đôla. Cisco hiện thống trị thị trường router, và hiện nay đang nhanh chóng chiếm lĩnh thị trường điện thoại qua Internet cạnh tranh quyết liệt cùng với các công ty thiết bị điện thoại như Lucent, Alcatel, Nothern Telcom và Siemens. Cisco được khởi đầu như thế này ? Bắt đầu từ năm 1984 trong phòng tiếp khách của một căn hộ tại Silicon Valley.

Khi làm việc ở đại học Stanford, Len Bosak cùng vợ là Sandy Lerner nẩy ra ý tưởng sản xuất và bán router Internet cho các viện nghiên cứu và trường đại học. Sandy Lerner đưa ra tên gọi của công ty "Cisco" (viết tắt của SanFrancisco) và bà cũng thiết kế biểu tượng cho công ty. Ban đầu tổng hành dinh của công ty đặt ngay tại phòng khách của họ. Hai vợ chồng phải sử dụng thẻ tín dụng trong công việc kinh doanh và phải làm thêm công việc tư vấn vào ban đêm. Cuối năm 1986, doanh thu của Cisco lên tới 250000USD/tháng - một kết quả không tồi với công ty được cấp vốn chỉ bằng thẻ tín dụng mà không có sự hùn vốn nào. Cuối năm 1987 Cisco huy động được 2 triệu đô từ Sequoia Capital đổi lấy việc kiểm soát 1/3 công ty. Vài năm tiếp theo Cisco tiếp tục phát triển và giành ngày càng nhiều thị phần. Cùng thời điểm đó, quan hệ giữa vợ chồng Bosak, Lener với đội ngũ quản lý của Cisco bắt đầu trục trặc. Cisco niêm yết trên thị trường cổ phiếu vào năm 1990. Cùng năm đó, Cisco sa thải Lerner và Bosak về hưu.

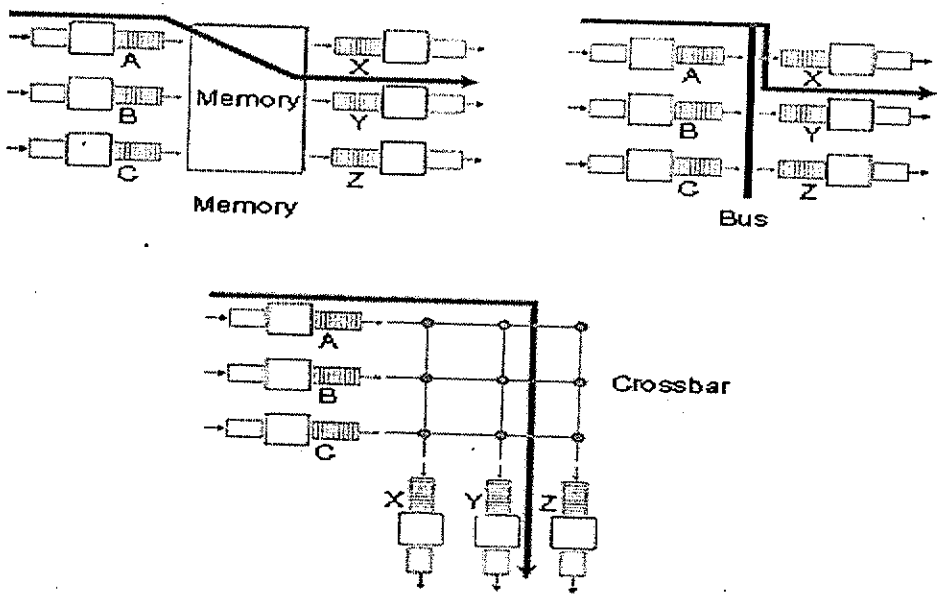
## 4.6.2 Kết cấu chuyển (Switching fabric)

Kết cấu chuyển nằm ở trung tâm của router. Gói dữ liệu chuyển từ cổng vào đến cổng ra qua kết cấu chuyển. Việc chuyển được thực hiện bằng nhiều cách như minh họa trên Hình 4.27

**Chuyển qua bộ nhớ**: Các router đơn giản nhất thuộc thế hệ đầu tiên thường chính là các máy tính truyền thống, việc chuyển từ cổng vào tới cổng ra được thực hiện dưới sự điều khiển trực tiếp của CPU. Cổng vào và cổng ra chỉ là các thiết bị vào ra truyền thống trong hệ điều hành. Khi nhận được một gói dữ liệu, cổng vào sẽ sử dụng ngắt để báo cho CPU. Sau đó gói dữ liệu được sao chép vào bộ nhớ của vi xử lý. Bộ vi xử lý lấy địa chỉ đích từ tiêu đề gói tin, tìm cổng ra trong bảng định tuyến và sao chép gói dữ liệu vào bộ đệm của cổng ra.



Nhiều router hiện đại cũng thực hiện việc chuyển qua bộ nhớ. Điểm khác biệt chính ở chỗ việc xác định địa chỉ đích và việc lưu trữ (chuyển) gói dữ liệu vào vị trí phù hợp trong bộ nhớ được thực hiện bởi bộ xử lý trên mạch cổng vào. Router chuyển qua bộ nhớ, theo một cách nào đó giống hệ thống nhiều bộ xử lý với bộ nhớ dùng chung, bộ xử lí trên cổng vào sẽ đặt gói dữ liệu vào bộ nhớ của một cổng ra thích hợp. Dòng router Cisco Catalyst 8500 và đòng Bay Network Accelar 1200 chuyển gói dữ liệu qua bộ nhớ dùng chung.




Hình 4.27 Kết cấu chuyển

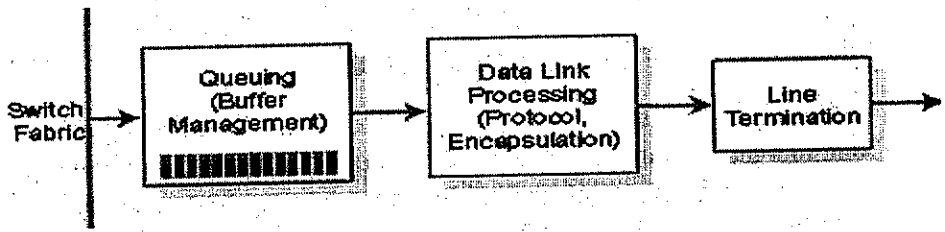
**Chuyển qua bus**. Cổng vào chuyển thẳng gói tin tới cổng ra qua một đường bus dùng chung mà không cần bộ xử lí của router can thiệp (chú ý là khi chuyển qua bộ nhớ, gói tin phải qua bus hệ thống để đến hay đi khỏi bộ nhớ). Mặc dù bộ xử lí của router không liên quan đến việc chuyển trên bus, song do bus dùng chung, tại một thời điểm chỉ cho phép một gói tin được truyền dẫn trên bus. Một gói tin đến cổng vào và thấy bus đang bị chiếm dụng bởi gói tin khác sẽ tạm thời bị chặn lại, đưa vào hàng đợi ở cổng vào. Vì tất cả các gói tin đều phải truyền qua một bus duy nhất, tốc độ chuyển của router bị giới hạn bởi tốc độ bus. Với công nghệ băng thông của bus vượt qua 1Gbit/s, chuyển mạch qua bus đủ hiệu quả với các router hoạt động ở mức tổ chức (ví dụ mạng cục bộ). Dòng Cissco 1900 chuyển mạch các gói qua bus 1Gbps.

**Chuyển mạch qua một liên mạng**. Một cách khắc phục hạn chế của bus dùng chung duy nhất là sử dụng một mạng liên kết phức tạp, giống các kĩ thuật được sử dụng để kết nối những bộ xử lí trong hệ thống đa bộ xử lý.

Hình 4.27 minh họa một mạng liên kết sử dụng 2N bus để nối N cổng vào với N cổng ra. Một gói tin đến từ một cổng vào sẽ được chuyển dọc theo bus nằm ngang gắn với cổng vào cho tới khi gặp giao điểm với bus nằm dọc gắn với cổng ra tương ứng. Nếu bus nằm dọc đó rỗi, gói tin sẽ được chuyển trên bus dọc đó tới cổng ra cần đến. Trong trường hợp ngược lại, gói tin tạm thời bị chặn lại và xếp hàng tại cổng vào. Dòng Cisco 12000 Family sử dụng công nghệ này.

## 4.6.3 Cổng ra (Output port)

Quá trình xử lí tại cổng ra được minh họa trên Hình 4.28: lấy gói dữ liệu đã được lưu trữ trong bộ đệm của cổng ra và truyền qua đường liên kết ra. Các chức năng xử lí giao thức liên kết dữ liệu và kết thúc đường truyền là chức năng tầng liên kết dữ liệu và tầng vật lí để làm việc với đầu vào bên kia của đường truyền vật lý. Chức năng quản lí vùng đệm và hàng đợi được sử dụng khi tốc độ dữ liệu mà kết cấu chuyển chuyển tới nhanh hơn tốc độ gửi đi của cổng ra.




**Hình 4.28 Cấu trúc cổng ra**

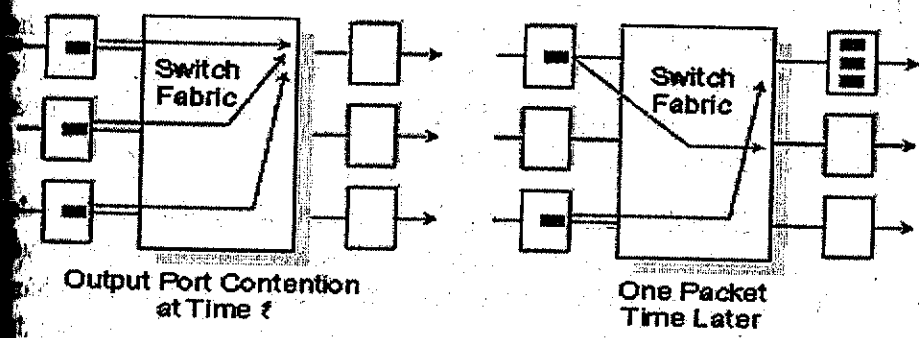
## 4.6.4 Hàng đợi ở router

Nếu nhìn vào chức năng, cấu hình của cổng vào, cổng ra trong Hình 4.27, rõ ràng hàng đợi của các gói tin có thể được hình thành tại cả cổng vào và cổng ra. Chúng ta sẽ trình bày chi tiết về hàng đợi vì khi hàng đợi lớn, bộ



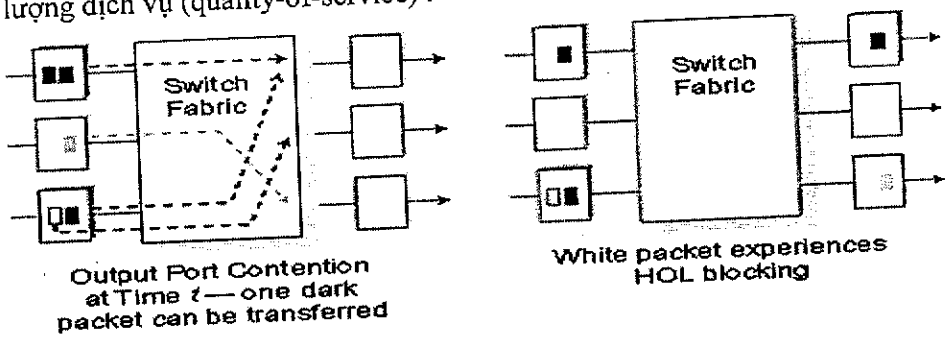
đệm của router sẽ đầy lên và xảy ra hiện tượng mất gói tin (tràn bộ đệm). Trong các phần trước, chúng ta đã nói mơ hồ rằng gói tin bị mất đâu đó "trong mạng" hay "tại router". Chính tại các hàng đợi của router, gói tin bị mất. Trên thực tế, vị trí gói tin bị mất (cổng vào hay cổng ra) phụ thuộc vào tải của mạng, tốc độ tương đối giữa kết cấu chuyển và đường truyền.

Giả sử tốc độ đường truyền vào và ra bằng nhau, và có $n$ cổng vào, $n$ cổng ra. Nếu tốc độ chuyển của kết cấu chuyển lớn hơn tốc độ đường truyền $n$ lần thì chắc chắn không có hàng đợi tại cổng vào. Bởi trong tình huống xấu nhất, tất cả n đường vào cùng nhận được gói tin, kết cấu chuyển có khả năng truyền n gói tin từ cổng vào tới cổng ra. Nhưng điều gì có thể xảy ra tại cổng ra? Giả sử tốc độ kết cấu chuyển vẫn nhanh hơn tốc độ đường truyền n lần. Trong trường hợp xấu nhất, tất cả gói tin từ n cổng vào cùng đến một cổng ra. Mỗi lần cổng ra chỉ có thể gửi đi một gói tin duy nhất, do đó n gói tin sẽ phải xếp hàng tại cổng ra để đợi truyền. Khi số lượng gói tin xếp hàng vượt qua độ lớn bộ đệm, các gói tin đến sau sẽ bị mất. Hàng đợi tại cổng ra được minh hoạ trong Hình 4.29. Tại thời điểm t, tất cả các cổng vào đều nhận được một gói tin và phải chuyển tới cổng ra trên cùng bên phải. Giả sử tốc độ ba đường truyền là như nhau và tốc độ kết cấu chuyển nhanh hơn tốc độ đường truyền ba lần. Sau một đơn vị thời gian (thời gian cần thiết để nhận hay gửi một gói tin ), cả 3 gói tin được chuyển tới cổng ra và xếp hàng để đợi truyền đi. Trong một đơn vị thời gian tiếp theo, một gói tin được truyền đi trên đường truyền ra. Cùng lúc đấy, lại có thêm hai gói tin khác chuyển tới cổng ra trên cùng và do đó sẽ phải xếp hàng.




**Hình 4.29 Mất gói tin tại Router**

Bộ điều phối (**scheduler**) tại cổng ra phải chọn một gói tin trong hàng đợi để truyền đi. Có thể sử dụng một cơ chế đơn giản như First-Come-First-Served (Người đến trước được phục vụ trước-FCFS) hay cơ chế hàng đợi có trọng số (WFQ – weighted fair queuing) phức tạp hơn, cho phép chia sẻ một cách tương đối công bằng đường truyền ra giữa các kết nối đầu cuối khác nhau. Bộ điều phối có vai trò quyết định trong trong việc bảo đảm chất lượng dịch vụ (quality-of-service) .




**Hình 4.30 Ví dụ về tắc nghẽn**

Nếu kết cấu chuyển không đủ nhanh (so với tốc độ cổng vào) để chuyển ngay lập tức tất cả các gói tin qua, hàng đợi sẽ xuất hiện tại cổng vào, vì khi đó các gói tin sẽ phải xếp hàng đợi đến lượt chuyển qua kết cấu chuyển tới cổng ra. Để minh hoạ xét chuyển mạch qua một liên mạng trong Hình 4.30 và giả sử (1) tốc độ của tất cả các liên kết bằng nhau, (2) thời gian gói tin chuyển từ cổng vào tới cổng ra bằng thời gian cổng vào nhận được một gói tin và (3) các gói tin được chuyển từ cổng vào tới cổng ra theo thứ tự đến (FCFS). Nhiều gói tin có thể được truyền đồng thời miễn là cổng ra của chúng khác nhau. Tuy nhiên nếu hai gói tin xếp đầu hàng đợi trên hai cổng vào khác nhau cùng hướng tới một cổng ra thì một gói tin sẽ bị chặn lại tại cổng vào (phải xếp hàng trong hàng đợi) vì tại một thời điểm kết cấu chuyển chỉ có thể chuyển đi một gói tin.

Trong Hình 4.30 ta thấy hai gói tin (tô đen) đứng đầu hai hàng đợi cùng hướng tới cổng ra phía trên bên phải. Giả sử kết cấu chuyển sẽ chuyển gói tin từ hàng đợi phía trên bên trái trước. Khi đó gói tin màu đen ở hàng đợi phía dưới bên trái sẽ phải đợi. Nhưng không chỉ có gói tin này phải đợi mà còn gói tin màu trắng xếp hàng sau nó cũng phải đợi - mặc dù các gói tin này hướng tới cổng ra khác. Đây là hiện tượng head-of-the-line (HOL)



blocking. [Karol 1997] đã chứng minh rằng [illegible]
hàng đợi tăng lên vô hạn ngay cả khi tốc độ đến của các gói tin trên cổng vào bằng 58% tốc độ tối đa. [McKeowwn 1997b] đưa ra nhiều giải pháp ngăn chặn HOL.

## 4.7 IPv6

Đầu những năm 1990, Internet Engineering Task Force bắt đầu nỗ lực phát triển giao thức mạng thay thế IPv4. Nguyên nhân đầu tiên cho nỗ lực này là không gian địa chỉ IP 32 bit đã bắt đầu cạn kiệt trong khi số lượng những mạng mới và những nút mạng được kết nối vào Internet (cần cấp phát một địa chỉ IP duy nhất) tăng lên đáng kể. Để giải quyết nhu cầu có không gian địa chỉ IP lớn hơn, giao thức mạng IPv6 đã được phát triển. Những người thiết kế IPv6 cũng chọn lọc các tính năng, cải tiến nhiều đặc điểm khác của IPv4 dựa trên cơ sở những kinh nghiệm thực tế của IPv4.

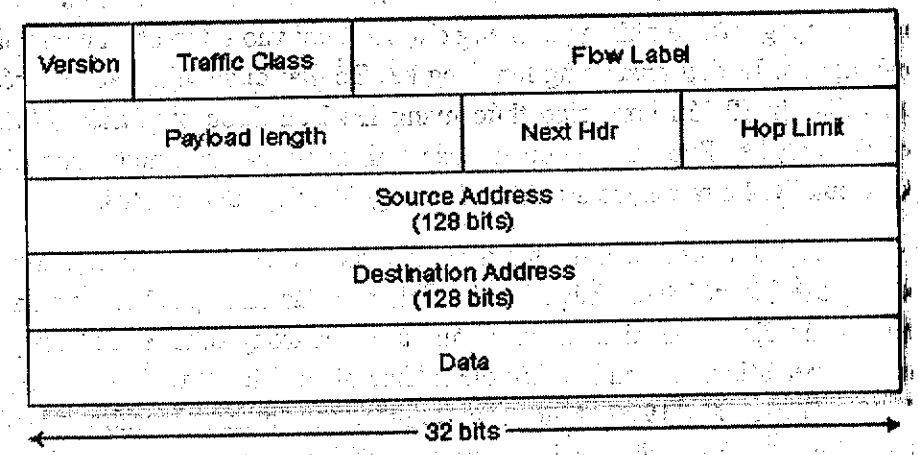
Người ta chưa thống nhất được khi nào địa chỉ IPv4 cạn kiệt (khi đó không thể kết nối thêm bất kỳ máy tính nào vào mạng). Căn cứ trên xu hướng cấp địa chỉ IP hiện tại hai nhóm làm việc trong IETF's Address Life time Expectations đưa ra hai thời điểm khác nhau là 2008 và 2018 [Solenky 1996]. Trong năm 1996, American Registry for Internet Number (ARIN) thông báo tất cả các địa chỉ IPv4 lớp A, 62% lớp B và 37% lớp C đã được phân phối [ARIN 1996]. Mặc dù những đánh giá và các con số dự đoán trên cho thấy còn có nhiều thời gian cho tới khi không gian địa chỉ IPv4 hết, song đã đến lúc triển khai một công nghệ mới trên một quy mô rộng lớn, và do đó "Next Generation IP" (thế hệ IP mới) [Brander 1996:RFC1752] đã bắt đầu triển khai.

### 4.7.1 Định dạng gói tin IPv6

Khuôn dạng gói dữ liệu IPv6 được minh họa trên hình Hình 4.31. Điểm thay đổi quan trọng nhất của IPv6 chính là khuôn dạng gói tin.

*Mở rộng khả năng đánh địa chỉ.* IPv6 tăng kích thước địa chỉ IP từ 32 bit lên 128 bit. Nó đảm bảo khả năng không bị thiếu địa chỉ IP. Với không gian 128 bit, có thể đánh địa chỉ cho đến từng hạt cát có trên trái đất. Bên cạnh địa chỉ duy nhất (unicast) và địa chỉ đa đích (multicast), IPv6 còn có một dạng địa chỉ mới gọi là "anycast address", cho phép một gói tin với địa chỉ đích thuộc kiểu "anycast address" có thể được chuyển tới một nhóm các máy tính (đặc điểm này sẽ được sử dụng ví dụ khi gửi thông điệp HTTP GET tới nhiều site phụ chứa cùng một tài liệu nào đấy).

*Tiêu đề có độ dài cố định 40 byte.* Một số trường IPv4 mang tính chất tùy chọn. Tổng độ dài tiêu đề cố định cho phép xử lí các gói dữ liệu IPv6 nhanh hơn.




**Hình 4.31 Khuôn dạng địa chỉ IPv6**

*Gắn nhãn luồng (flow label) và độ ưu tiên (priority).* IPv6 không có định nghĩa cho "flow" một cách rõ ràng. Các khuyến nghị RFC 1752 và RFC 2460 cho phép gắn nhãn cho các gói tin thuộc về cùng một "flow". Các gói tin này đòi hỏi được xử lý một cách đặc biệt, như các dịch vụ thời gian thực với chất lượng tốt hơn. Ví dụ, các dữ liệu đa phương tiện có thể xem như một luồng liên tục. Dữ liệu các ứng dụng truyền thống, như truyền file, E-mail không được xem như một luồng. Có thể dữ liệu của những người có độ ưu tiên cao (ví dụ người trả phí cao hơn) cũng có thể coi như một luồng. Rõ ràng ở đây những người thiết kế IPv6 đã dự đoán được nhu cầu phân biệt giữa các luồng dữ liệu ngay cả khi chưa định nghĩa chính xác được luồng là gì. Tiêu đề IPv6 cũng có trường Traffic Class 8 bit. Trường này giống



trường TOS (Tyte of Service) trong IPv4 có thể được sử dụng cho những gói n có quyền ưu tiên trong một luồng, hoặc cho những ứng dụng có độ ưu iên cao (ví dụ gói tin ICMP).

So sánh khuôn dạng gói dữ liệu IPv4 (Hình 4.20) và IPv6 (Hình 31), ta thấy gói IPv6 có cấu trúc đơn giản hơn. Sau đây là một số trường rong gói dữ liệu IPv6:

**Phiên bản (version).** Trường 4-bit này xác định phiên bản IP của ói dữ liệu. Rõ ràng gói IPv6 có giá trị "6" trong trường này. Chú ý không hải đặt giá trị "4" trong trường này thì gói dữ liệu là IPv4.

**Traffic class.** Trường 8-bit này giống trường TOS trong IPv4

**Nhãn luồng (Flow label).** Trường 20 bit này xác định một luồng hứa gói dữ liệu.

**Độ lớn dữ liệu (Payload length).** Độ lớn (tính theo byte) của phần ữ liệu không tính tiêu đề.

**Next header.** Trường này xác định giao thức ở tầng phía trên sẽ hận dữ liệu (ví dụ tới TCP hoặc UDP). Trường này giống trường Protocol ủa IPv4.

**Hop limit.** Giá trị của trường này sự giảm đi 1 khi đi qua mỗi router. Nếu giá trị này bằng 0, gói dữ liệu bị loại bỏ.

**Địa chỉ nguồn và đích (source and destination addresss).** Khuôn dạng 128-bit địa chỉ IPv6 được đặc tả trong RFC 2373.

**Dữ liệu (data).** Khi gói tin IPv6 tới đích, các tiêu đề sẽ bị loại bỏ và phần dữ liệu này sẽ được chuyển đến thực thể ở tầng phía trên.

Có một số trường trong IPv4 không xuất hiện trong IPv6 nữa.

**Phân mảnh, Hợp nhất gói tin.** IPv6 không cho phép phân mảnh và hợp nhất gói tin tại các router trung gian. Nếu một gói dữ liệu IPv6 quá lớn để có thể gửi đi trên một đường liên kết ra của router, router sẽ loại bỏ gói tin này và gửi một thông báo lỗi ICMP "Packet Too Big" tới bên gửi. Sau đó bên gửi gửi lại dữ liệu, sử dụng các gói dữ liệu có kích thước nhỏ hơn. Việc

phân mảnh và hợp nhất các gói tin IP chiếm nhiều thời gian xử lý của router. Thực hiện những công việc này tại các thiết bị đầu cuối sẽ làm tăng tốc độ truyền trên mạng.

**Checksum**. Do tầng giao vận (ví dụ, TCP và UDP) và các giao thức liên kết dữ liệu (ví dụ Ethenet) đã thực hiện kiểm tra lỗi, chức năng này không cần thiết trong tầng mạng nên được bỏ đi. Vấn đề xử lý nhanh các gói tin IP cực kỳ quan trọng. Khi nói về IPv4 trong phần 4.4.1, chúng ta đã thấy giá trị trường TTL trong tiêu đề của IPv4 giảm đi một khi đi qua mỗi router, nên giá trị trường checksum trong tiêu đề IPv4 cần phải được tính lại tại các router. Như vậy, giống như phân mảnh và hợp nhất, việc này khiến thời gian xử lý gói IPv4 lâu hơn.

***ICMP cho IPv6***

Trong phần 4.4, giao thức ICMP được sử dụng để thông báo lỗi và cung cấp một số các thông tin hạn chế tới thiết bị đầu cuối (ví dụ lệnh ping). Một phiên bản mới của ICMP được đặc tả cho IPv6 trong khuyến nghị RFC 2463. Bên cạnh các kiểu và mã cũ, ICMPv6 cũng đưa thêm vào nhiều kiểu và mã mới. Ví dụ kiểu mã lỗi "Packet Too Big" hay "Unrecognized IPv6 option".

## 4.7.2 Chuyển từ IPv4 sang IPv6

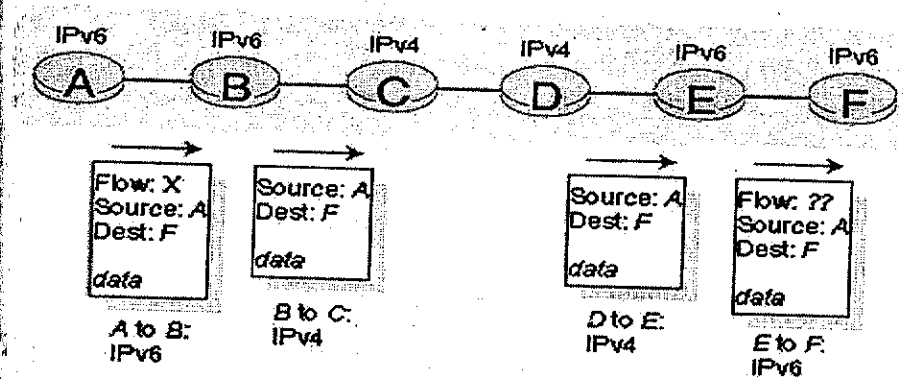
Chúng ta đã xem xét các chi tiết kỹ thuật của IPv6, bây giờ chúng ta sẽ xét tới một vấn đề rất thực tiễn: làm thế nào để chuyển mạng toàn cầu Internet hiện tại – đang sử dụng IPv4 sang sử dụng IPv6? Vấn đề ở chỗ trong khi các hệ thống mới IPv6 có khả năng tương thích ngược tức là có thể gửi, chuyển, nhận các gói dữ liệu IPv4 thì các hệ thống cũ đang được sử dụng lại không có khả năng xử lý gói dữ liệu IPv6. Người ta đã đưa ra một số giải pháp.

Giải pháp thứ nhất là lựa chọn một thời điểm nào đó, tắt tất cả máy để nâng cấp lên IPv6. Việc chuyển đổi công nghệ quan trọng gần đây nhất (từ NCP sang TCP cho giao thức giao vận tin cậy) cách đây 20 năm. Ngay



cả thời điểm đó [RFC 801], khi Internet còn rất nhỏ và vẫn còn được quản trị bởi một nhóm nhỏ các chuyên gia, người ta cũng không thể chọn được một thời điểm như vậy. Giải pháp này ngày nay sẽ đòi hỏi sự tham gia của hàng trăm triệu máy tính và hàng triệu người quản trị mạng – rõ ràng là không thể. RFC 1933 đưa ra hai giải pháp (có thể sử dụng đồng thời hay dùng riêng rẽ) để dần dần tích hợp các thiết bị sử dụng IPv6 vào thế giới IPv4 (dĩ nhiên mục tiêu dài hạn vẫn là chuyển tất cả các thiết bị sử dụng IPv4 sang IPv6).

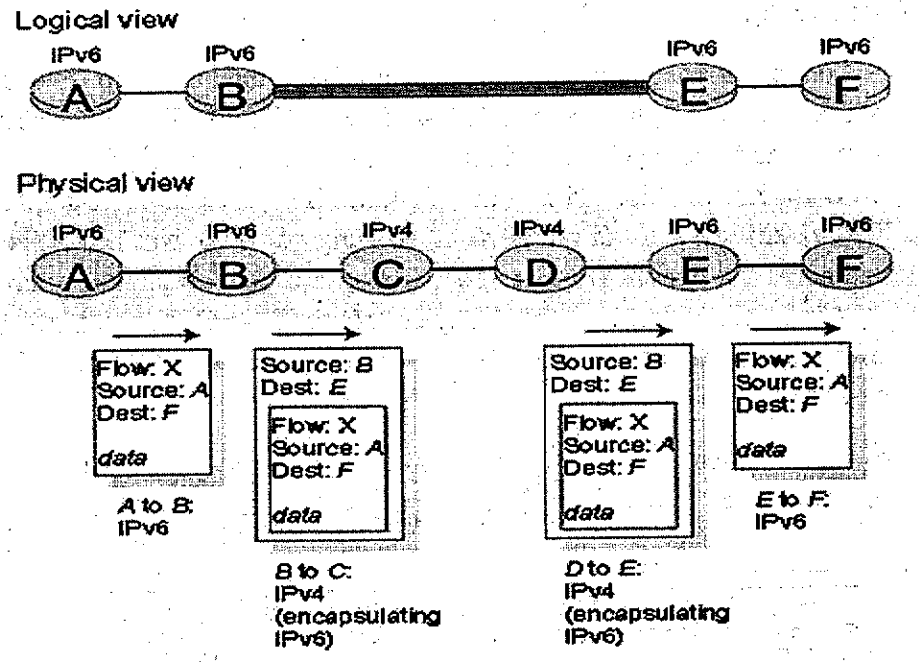
Có thể giải pháp đơn giản nhất để đưa vào các thiết bị hỗ trợ IPv6 là **dual-stack**, các thiết bị triển khai cả IPv4 và IPv6. Thiết bị IPv6/IPv4 như vậy được đặc tả trong RFC 1933 có khả năng nhận và gửi cả hai gói dữ liệu IPv4 và IPv6. Khi trao đổi với một nút IPv4, nút IPv6/IPv4 sử dụng gói dữ liệu IPv4 và khi trao đổi với nút IPv6, sẽ sử dụng gói IPv6. Nút IPv4/IPv6 cần phải có cả hai địa chỉ IPv6 và IPv4. Chúng cần phải có khả năng xác định được một nút có khả năng IPv6 hay chỉ hỗ trợ IPv4. Có thể giải quyết vấn đề này nhờ Hệ thống tên miền DNS (Domain Name Server) (xem trong chương 2).




**Hình 4.32 Giải pháp dual-stack**

Trong giải pháp trên, nếu cả bên gửi và bên nhận chỉ hỗ trợ IPv4 thì giữa chúng chỉ có thể trao đổi gói dữ liệu IPv4. Do đó có thể hai nút có khả năng IPv6 chỉ có thể trao đổi gói dữ liệu IPv4 với nhau. Trong Hình 4.32,giả sử nút A hỗ trợ IPv6 muốn gửi một gói dữ liệu IP tới nút F cũng hỗ trợ IPv6. Nút A và B có thể trao đổi gói tin IPv6 với nhau. Tuy nhiên, nút B phải tạo gói dữ liệu IPv4 để gửi tới C. Chắc chắn một số trường tiêu đề của gói IPv6

được sao chép vào trường tiêu đề của gói dữ liệu IPv4 và phải thực hiện việc đổi địa chỉ. Tuy nhiên, khi chuyển từ IPv6 sang IPv4, sẽ có một số trường đặc thù trong IPv6 sẽ không có trong IPv4 (ví dụ trường flow). Các thông tin trong các trường này sẽ bị mất. Cho dù E và F có thể trao đổi gói dữ liệu IPv6, gói dữ liệu IPv4 từ D tới E không có đầy đủ tất cả các thông tin trong gói dữ liệu IPv6 nguyên thủy được gửi từ A.




**Hình 4.33 Giải pháp đường ống**

Giải pháp thứ hai được nêu ra trong khuyến nghị RFC 1933 là giải pháp **đường ống (tunneling)**. Giải pháp này cho phép khắc phục được vấn đề nêu trên, cho phép E nhận gói IPv6 nguyên bản từ A. Sau đây trình bày ý tưởng cơ bản của giải pháp này. Giả sử hai nút IPv6 (ví dụ B và E trong Hình 4.33) muốn gửi gói IPv6 cho nhau, nhưng giữa chúng là các router chỉ hỗ trợ IPv4. Các router IPv4 nằm giữa hai router IPv6 là một **đường ống**, như minh hoạ trong Hình 4.33. Hai nút IPv6 ở hai đầu của đường ống (B chẳng hạn) đặt toàn bộ gói dữ liệu IPv6 vào trong trường dữ liệu (payload) của gói dữ liệu IPv4. Gói dữ liệu IPv4 này có địa chỉ đích là nút IPv6 ở đầu



kia đường ống (ví dụ là E) và được gửi tới nút đầu tiên trong đường ống (C). Các router IPv4 trong đường ống sẽ định tuyến gói dữ liệu IPv4 giống như bất kỳ gói dữ liệu IPv4 nào mà không biết được gói dữ liệu IPv4 đó chứa gói dữ liệu IPv6. Nút IPv6 phía bên kia đường ống nhận được gói IPv4, xác định trong đó có gói IPv6, lấy gói IPv6 ra, và sau đó chuyển tiếp gói IPv6 như thể nó nhận thẳng gói IPv6 từ phía bên kia.

Vậy khi nào IPv6 có bước đột phá thực sự vào mạng Internet toàn cầu. Thực tế hiện nay các ISP Bắc Mỹ không có dự định mua thiết bị có hỗ trợ IPv6 vì ít khách hàng đòi hỏi điều này. Nhu cầu sử dụng IPv6 chủ yếu xuất phát từ châu Âu và châu Á.

Rõ ràng cực kỳ khó khăn để thay đổi các giao thức của tầng mạng. Từ đầu những năm 90, rất nhiều giao thức mới của tầng mạng đã được đưa ra nhưng vẫn chưa được áp dụng thực sự trong thực tế. Thực vậy, thay đổi giao thức tầng mạng giống như thay đổi móng của một ngôi nhà. Sẽ rất khó thực hiện nếu không phá hủy hoàn toàn ngôi nhà hoặc ít nhất tạm thời bố trí những người sinh sống trong đó đến các địa điểm khác. Mặt khác, Internet chứng kiến sự phát triển nhanh chóng các giao thức tầng ứng dụng. Một ví dụ hiển nhiên là HTTP và WEB. Đưa ra những giao thức ứng dụng mới giống như việc thêm một lớp sơn mới cho ngôi nhà - nó thực sự dễ dàng, và nếu bạn chọn một màu hấp dẫn, những người xung quanh sẽ bắt chước làm theo bạn. Tóm lại, trong tương lai chúng ta có thể kỳ vọng thấy được sự thay đổi tầng mạng của Internet, nhưng những thay đổi này sẽ diễn ra rất chậm so với những thay đổi tại tầng ứng dụng.

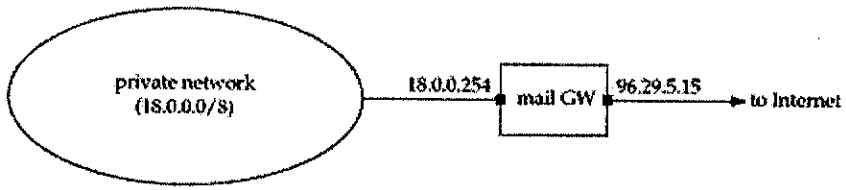
## 4.8 CƠ CHẾ DỊCH CHUYỂN ĐỊA CHỈ (NAT)

Trong trường hợp tổ chức có nhu cầu kết nối nhiều máy tính vào mạng nhưng lại chỉ được cấp phát một lượng nhỏ địa chỉ IP chính thức, vậy làm thế nào để tất cả các máy tính trong mạng có thể truy cập Internet ? NAT là một trong các giải pháp để thực hiện điều này. RFC 1918 xác định một số địa chỉ IP đặc biệt gọi là địa chỉ riêng (Hình 4.34). Gói tin có địa chỉ trong dải địa chỉ này sẽ không được router chuyển ra phía ngoài.

| Khối | Dải địa chỉ |
|---|---|
| 10.0.0.0/8 | 10.0.0.1 – 10.255.255.255 |
| 172.16.0.0/12 | 172.16.0.0 – 172.31.255.255 |
| 192.168.0.0/16 | 192.168.0.0 – 192.168.255.255 |

**Hình 4.34 Các địa chỉ riêng**

Dĩ nhiên nếu tổ chức không có nhu cầu kết nối ra Internet thì sử dụng bất kỳ địa chỉ IP nào cũng được. Trước khi có RFC 1918, mọi tổ chức đều có khuynh hướng chọn một lớp địa chỉ bất kỳ. Trong Hình 4.35, tổ chức chọn địa chỉ 18.0.0.0/8. Tuy nhiên giả sử sau đó tổ chức muốn cài đặt Mail server để máy tính ở trong mạng nội bộ có thể gửi và nhận thư với bên ngoài. Để nối với các máy tính bên trong mạng nội bộ, mail server sử dụng địa chỉ 18.0.0.254. Để kết nối ra ngoài Internet, mail server sử dụng địa chỉ 96.29.5.15 thực xác định duy nhất trên Internet.




**Hình 4.35 Ví dụ một tổ chức dùng Gateway Mail Server**

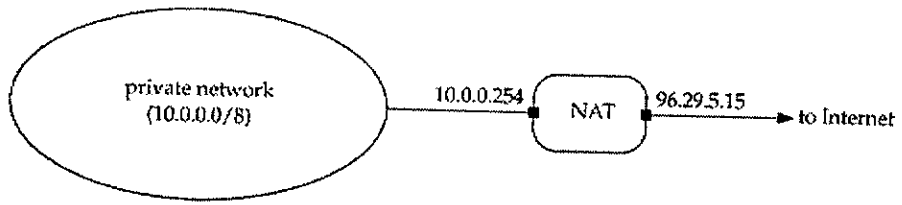
Bây giờ giả sử người trong cơ quan muốn gửi email đến ai đó ở MIT. Vấn đề ở đây là địa chỉ thật của MIT là 18.0.0.0/8. Do đó mail gateway sẽ chuyển ngược thư vào lại mạng nội bộ, chứ không chuyển tới miền mit.edu. Vấn đề này sẽ không còn nữa nếu cơ quan sử dụng địa chỉ riêng.

Một ưu điểm khác của NAT là cho phép cấu hình mạng của cơ quan không phụ thuộc vào bất kỳ ISP nào cả.

Trước khi đi sâu vào chi tiết, chúng ta sẽ tìm hiểu qua cơ chế Dịch chuyển địa chỉ mạng NAT (Network Address Translation). Cơ chế này được cài đặt trên router nối ra ngoài của mạng. Nếu chúng ta thay thế mail gateway trên Hình 4.35 bằng một router có hỗ trợ cơ chế NAT và đánh lại



địa chỉ cho các máy tính bên trong là địa chỉ 10.0.0.0/8, chúng ta được Hình 4.36. Chúng ta quay lại ví dụ trên, giả sử máy 10.0.0.1 bên trong mạng riêng muốn gửi email đến địa chỉ 18.7.7.76. Kết nối TCP này không thể được thiết lập do mail server ở MIT không thể gửi lại gói tin phản hồi đến địa chỉ 10.0.0.1




**Hình 4.36 Mạng riêng với Router có hỗ trợ cơ chế NAT**

Về mặt lý thuyết, gói tin gửi từ 10.0.0.1 sẽ đến được MIT server. Nhưng trên thực tế, các router và mail server thường loại bỏ các gói tin có địa chỉ gửi là địa chỉ riêng với mục đích phòng ngừa tấn công từ chối dịch vụ (DoS) hay các thư rác.

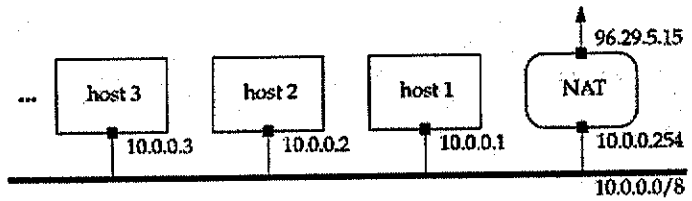
Chính vì vậy gói tin trước khi rời mạng riêng, địa chỉ gửi trong gói tin phải được thay đổi để bên kia có thể gửi thông điệp phản hồi.

NAT hoạt động theo một trong ba chế độ sau:

1. **Cơ chế tĩnh**. Mỗi máy tính trong mạng riêng khi truy cập đến Internet sẽ có một địa chỉ thật. NAT chỉ thực hiện việc ánh xạ từ địa chỉ ảo vào địa chỉ thực và ngược lại.
2. **Cơ chế vòng**. Tất cả các máy tính trong mạng riêng sử dụng chung một nhóm địa chỉ chính thức. Ví dụ mạng riêng với 300 máy tính được cấp phát một dải 32 địa chỉ thật. Khi một máy tính trong mạng riêng muốn kết nối với một máy tính bên ngoài, nó sẽ được gán cho một địa chỉ thực tạm thời. Sau khi kết nối kết thúc, địa chỉ vừa được cấp phát sẽ được thu hồi để cấp cho máy tính có nhu cầu khác. Hiển nhiên khi hết các địa chỉ thật, các máy khác có nhu cầu cũng không được kết nối.

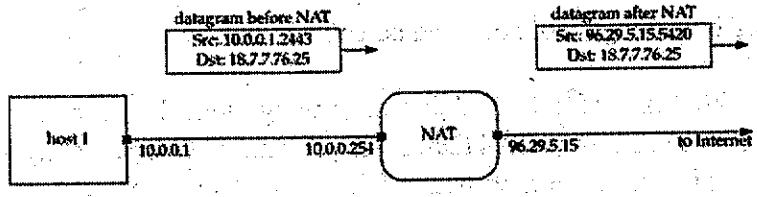
**Cơ chế chuyển địa chỉ theo cổng (PAT)**. Đây là cơ chế được sử dụng rộng rãi nhất. Cơ chế này được sử dụng khi có một địa chỉ thật duy

nhất dùng chung cho cả tổ chức. Khi đó địa chỉ port gửi của mỗi gói tin được thay bằng một giá trị xác định duy nhất. Giá trị này sẽ được sử dụng để khi nhận một gói tin, router biết phải chuyển tiếp nó cho máy tính nào trong mạng riêng.Để hiểu rõ cơ chế hoạt động của PAT, chúng ta minh họa mạng riêng ở Hình 4.36 thành Hình 4.37.




**Hình 4.37 Ví dụ về mạng sử dụng cơ chế PAT**

Giả sử Host 1 muốn thiết lập kết nối với email server của MIT có địa chỉ 18.7.7.76 thông qua proxy 2443 Hình 4.38 minh họa đường đi của gói tin IP chứa TCP SYN segment gửi tới MIT email server qua hai chặng: chặng thứ nhất từ Host 1 đến Router và chặng thứ hai từ router đến MIT server. Cơ chế PAT được sử dụng để biến đổi gói tin này giữa hai chặng




**Hình 4.38 Gói tin từ Host 1 đến router và được chuyển tiếp**

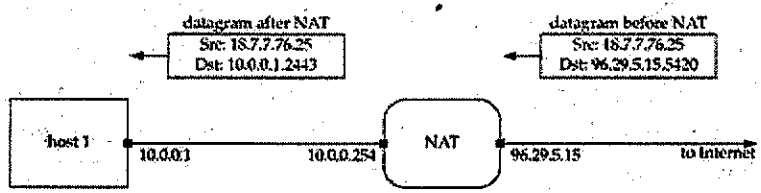
Đầu tiên gói tin được gửi từ Host 1 có địa chỉ gửi là địa chỉ riêng (**10.0.0.1**) và port gửi là **2443**. Sau khi đi qua router, địa chỉ gửi của gói tin là **96.29.5.15** và port gửi là **5420**.

MIT's mail server thấy kết nối này đến từ **96.29.5.15:5420** và sẽ gửi thông điệp trả lời đến socket này.

Chúng ta thấy gói tin trả lời trong Hình 4.39. Chú ý rằng, khi đến router gói tin này có địa chỉ nhận là **96.29.5.15:5420** còn địa chỉ nguồn là



phía mail server của MIT. Router sẽ kiểm tra địa chỉ **96.29.5.15:5420** trong bảng PAT và thấy gói tin này phải được chuyển tiếp tới **10.0.0.1:2443**. Phía bên trái của Hình 4.39 minh họa gói tin sau khi đã được router biến đổi địa chỉ gửi theo cơ chế PAT.




**Hình 4.39 Gói tin trả lời được NAT biến đổi**

Giả sử tại cùng thời điểm Host 1 gửi, một máy tính khác trong mạng riêng, chẳng hạn Host 2 với địa chỉ **10.0.0.2** cũng gửi email tới MIT, khi đó NAT sẽ ánh xạ địa chỉ gửi của Host 2 vào **96.29.5.15** nhưng sẽ sử dụng một địa chỉ cổng khác, ví dụ **7322**. Do vậy khi nhận được gói tin có địa chỉ đích **96.29.5.15:7322**, NAT biết rằng cần chuyển gói tin này đến Host 2 (**10.0.0.2**).

Ưu điểm của NAT là hoàn toàn rõ ràng. Thứ nhất, nó làm tiết kiệm không gian địa chỉ IP đã sắp cạn kiệt, một mạng riêng khá lớn cũng chỉ cần một địa chỉ thật. Thứ hai là tổ chức có thể cấp phát địa chỉ riêng cho các máy tính trong cơ quan của mình và thực hiện ánh xạ địa chỉ tại router kết nối ra ngoài, do đó có sự độc lập với ISP. Nếu tổ chức muốn chuyển sang nhà cung cấp dịch vụ ISP khác thì chỉ cần cấu hình lại bảng NAT mà không cần gán lại địa chỉ IP cho các máy tính trong tổ chức. Như vậy, NAT là giải pháp rất phù hợp với tổ chức quy mô nhỏ.

Tuy nhiên, NAT cũng có nhiều nhược điểm. Trong phần trên, chúng ta thấy rằng dường như NAT chỉ là sự ánh xạ rất đơn giản giữa địa chỉ riêng và địa chỉ thật. Tuy nhiên có khá nhiều công việc trong quá trình ánh xạ. Thứ nhất địa chỉ IP gửi bị thay đổi trong trường tiêu đề nên giá trị trong trường checksum cũng phải tính lại. Thứ hai, router phải kiểm tra xem gói tin chứa TCP segment hay UDP segment, và sau đó phải thay đổi số hiệu cổng và checksum trong tiêu đề của TCP (hay UDP) segment. Như vậy,

router hỗ trợ NAT đã "vi phạm" cơ chế phân tầng do đã kiểm tra bên trong gói dữ liệu IP.

Có rất nhiều ứng dụng, chẳng hạn ftp sử dụng nhiều kết nối. FTP client gửi lệnh **PORT x y** tới FTP server để yêu cầu FTP server mở một kết nối tới socket địa chỉ IP **x** và cổng **y**. Địa chỉ và số hiệu cổng này được chuyển dưới dạng mã ASCII bên trong thông điệp ở tầng ứng dụng. Như vậy NAT phải biết điều này vì hai lí do. Thứ nhất, NAT phải ánh xạ lại địa chỉ riêng của client gửi đến server và NAT phải ghi nhớ (để có thể ánh xạ lại trong trường hợp có xung đột với cổng NAT đã gán khác). Thứ hai NAT phải xác định chính xác socket (IP/port) của máy tính trong mạng riêng đang đợi kết nối từ phía FTP server ở bên ngoài.

Để thực hiện điều này, NAT router phải kiểm tra gói tin TCP để xem nó có chứa lệnh **PORT** của ftp không. Nếu có, không những chúng ta phải thay đổi tiêu đề TCP segment mà còn phải thay đổi cả độ dài gói tin (đổi **10.0.0.1** thành **96.29.5.15** khiến độ dài trường dữ liệu trong TCP segment tăng thêm 2 byte). Khi độ dài trường dữ liệu thay đổi, các giá trị biên nhận (ACK) cũng phải thay đổi theo. Chẳng hạn như trong ví dụ trên, nếu byte cuối cùng mà client (bên trong mạng riêng) gửi có số thứ tự là n. Tuy nhiên do NAT router bổ sung thêm dữ liệu ở trong TCP segment nên byte cuối cùng của gói tin này có số thứ tự là n+2. Phía server sẽ trả lại giá trị biên nhận ACK là n+3 (hy vọng byte kế tiếp nhận được có số thứ tự là n+3). Khi đó NAT router phải đổi giá trị biên nhận ACK này thành n+1 khi chuyển tiếp cho client. Không chỉ thế NAT router phải ghi nhớ sự biến đổi này trong suốt phiên kết nối.

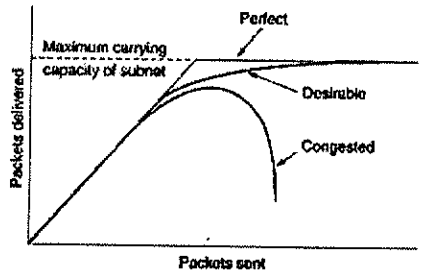
Chế độ thụ động của FTP có thể khắc phục vấn đề này. Trong chế độ này, phía client sẽ khởi tạo cả kết nối điều khiển lẫn kết nối dữ liệu. Khi đó, NAT router không cần biến đổi dữ liệu bên trong gói tin. Khi client muốn mở một kết nối dữ liệu tới server, nó sẽ gửi lệnh PASV yêu cầu server lắng nghe trên một cổng nào đó mà client chỉ định.

NAT có thể xử lý với ftp và một số rất ít các giao thức thông dụng khác nhưng có thể NAT làm hỏng các giao thức ở tầng ứng dụng do người dùng đặt ra nếu những giao thức này đặt địa chỉ cổng bên trong trường dữ liệu ứng dụng.



## 4.9 KIỂM SOÁT TẮC NGHẼN

Như chúng ta đã nói trong chương 3, hiện tượng tắc nghẽn là tại một thời điểm có quá nhiều gói tin đến cùng một phân đoạn mạng (hay một router) và hệ quả của tắc nghẽn là hiệu suất của hệ thống giảm nghiêm trọng. Trong Hình 4.40, chúng ta thấy rằng nếu tổng số gói tin trong mạng nhỏ hơn năng lực chuyển của mạng thì tất cả các gói tin đều sẽ được chuyển đến đích và số lượng gói tin truyền thành công bằng số lượng gói tin được gửi. Tuy nhiên khi lưu lượng gửi tăng nhanh, các router không kịp chuyển tiếp, các gói tin bắt đầu bị mất (do thiếu bộ đệm). Đến một giới hạn nào đó, hiệu suất hệ thống sụt giảm nghiêm trọng.




**Hình 4.40 Đồ thị minh họa tắc nghẽn**

Có nhiều tình huống dẫn đến tắc nghẽn. Chẳng hạn tại router, khi tất cả các gói tin đến từ nhiều cổng vào khác nhau nhưng lại cùng được chuyển đến một cổng ra, xuất hiện hàng đợi tại cổng ra này, do bộ đệm hữu hạn nên các gói tin đến sau có thể bị mất. Một số nghiên cứu cũng đã chứng minh được rằng, cho dù kích thước bộ đệm của router lớn vô cùng, tình trạng tắc nghẽn cũng không thể được giải quyết mà còn có xu hướng ngày càng xấu đi vì các gói tin nằm ở cuối hàng đợi chưa được chuyển đi, tại phía gửi do không nhận được ACK (sự kiện timeout) nên sau một thời gian sẽ tự động truyền lại gói tin (gửi trùng lặp). Các gói tin này sau đó lại "nằm xếp hàng" tại các router trên tuyến đường tới đích.

Tốc độ xử lý của CPU chậm cũng có thể là nguyên nhân gây tắc nghẽn. Nếu router không xử lý đủ nhanh, hàng đợi có thể xuất hiện tại router

(ngay cả khi công suất đường truyền vẫn chưa đạt tới cực đại). Tương tự, đường truyền có băng thông nhỏ cũng có thể gây ra tắc nghẽn. Nâng cấp đường truyền mà không nâng cấp router (hoặc ngược lại) không thể khắc phục được toàn bộ vấn đề, mà chỉ dịch chuyển "nút cổ chai" từ vị trí này trên mạng sang vị trí khác. Vấn đề ở đây là sự không cân đối giữa các phần khác nhau của hệ thống. Vấn đề chỉ được khắc phục hoàn toàn nếu đảm bảo được tính cân bằng trong hệ thống.

Ở đây chúng ta lại nhấn mạnh đến sự khác biệt giữa kiểm soát tắc nghẽn và điều khiển lưu lượng. Kiểm soát tắc nghẽn đảm bảo mạng máy tính có khả năng trung chuyển được khối lượng thông tin định trước. Điều này là vấn đề toàn cục, liên quan đến hành vi của tất cả các máy tính, các router. Ngược lại, điều khiển lưu lượng tập trung vào đường kết nối giữa hai đầu mút của truyền thông với mục đích kiểm soát để bên gửi không gửi quá tốc độ xử lý của bên nhận. Thông thường, phía nhận sẽ gửi thông báo phản hồi về tình trạng phía bên mình cho bên gửi.

Đôi khi hai khái niệm này không được phân biệt rõ ràng vì thuật toán kiểm soát tắc nghẽn cũng vận hành bằng cách gửi các thông báo phản hồi đến các nút trong mạng thông báo tình trạng tắc nghẽn. Do thế, nút gửi sẽ được yêu cầu gửi chậm lại khi hoặc mạng bị tắc nghẽn, hoặc khi nút nhận không kịp xử lý lượng dữ liệu gửi tới.

Chúng ta sẽ trình bày mô hình tổng quát xử lý tắc nghẽn, sau đó sẽ giới thiệu cách thức ngăn chặn để không xảy ra tắc nghẽn và sau đó là các thuật toán động – được sử dụng để khắc phục khi tắc nghẽn xuất hiện.

## 4.9.1 Các nguyên lý Kiểm soát tắc nghẽn

Đối với vấn đề tắc nghẽn, có hai chiến lược xử lý: Đóng và Mở. Giải pháp Mở là đưa ra một thiết kế đảm bảo tắc nghẽn không thể xảy ra. Quan trọng nhất trong giải pháp này là quyết định có chấp nhận một phiên truyền thông mới hay không ? Quyết định khi nào loại bỏ và loại bỏ gói tin nào ? Tuy nhiên tất cả các quyết định này được đưa ra không phụ thuộc vào trạng thái hiện thời của mạng.



Ngược lại, giải pháp Đóng dựa trên ý tưởng phản hồi và gồm ba giai đoạn:

1. Kiểm soát hệ thống để phát hiện thời điểm và vị trí xảy ra tắc nghẽn.
2. Chuyển thông tin cảnh báo về nơi có thể xử lý.
3. Điều chỉnh hệ thống để xử lý vấn đề.

Có rất nhiều tiêu chí khác nhau để kiểm soát tắc nghẽn. Thông dụng nhất là tỷ lệ phần trăm các gói tin bị loại bỏ do thiếu bộ đệm; độ lớn trung bình của hàng đợi; số lượng các gói tin không nhận được phản hồi và bị truyền lại; độ trễ trung bình của gói tin. Trong những trường hợp trên, những độ đo này tăng nghĩa là tắc nghẽn bắt đầu xuất hiện.

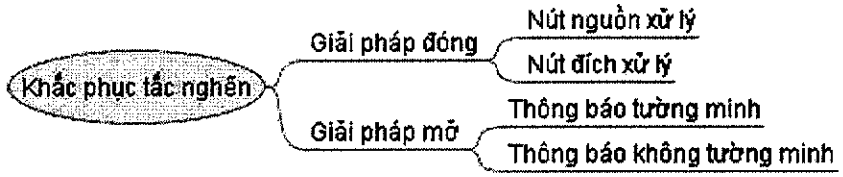
Bước phản hồi thứ hai là chuyển thông điệp cảnh báo từ nơi phát hiện tắc nghẽn đến nơi có thể đưa ra các hành động khắc phục. Một cách đơn giản là các router phát hiện ra tắc nghẽn gửi các gói tin đặc biệt đến tất cả các máy tính trên mạng thông báo về tình trạng tắc nghẽn. Rõ ràng nhược điểm của giải pháp này là phát sinh thêm các gói tin tại thời điểm đã có quá nhiều gói tin trên mạng (do tắc nghẽn).

Tuy nhiên người ta có thể đặt một trường nào đó bên trong mỗi gói tin và router sẽ thay đổi giá trị của trường này khi tắc nghẽn vượt qua một ngưỡng nào đó. Khi phát hiện tắc nghẽn, router sẽ thiết lập giá trị ở trường báo hiệu tắc nghẽn trong mỗi gói tin đi qua nó để cảnh báo các "hàng xóm".

Một phương pháp khác là các máy tính và router định kỳ gửi các thông điệp thăm dò với mục đích hỏi về tình trạng tắc nghẽn. Sau đó những thông tin nhận được có thể được router sử dụng để chuyển các gói tin vòng qua những khu vực đang bị tắc nghẽn. Điều này tương tự hệ thống cảnh báo tắc đường ở Mỹ. Trên một số trục xa lộ của nước Mỹ, có máy bay trực thăng bay để phát hiện xem có tắc đường không và những thông tin này sẽ được phát qua radio trên một số tần số cố định. Người lái xe có thể nghe được những thông tin này và chuyển hướng đi (không đi qua khu vực bị tắc).

Trong tất cả các phương pháp phản hồi, người ta hy vọng khi nhận được các thông tin báo hiệu tắc nghẽn, các máy tính trên mạng giảm bớt việc gửi tin để làm giảm tắc nghẽn. Có rất nhiều thuật toán kiểm soát tắc

nghẽn, và được phân loại như trong Hình 4.41.Giải pháp đóng được chia thành hai loại: Nút gửi thông tin sẽ xử lý tắc nghẽn và Nút nhận thông tin sẽ xử lý tắc nghẽn. Giải pháp mở cũng được chia thành hai loại: Tường minh (có thông báo tường minh gửi tới các nút trên mạng thông báo về tình trạng tắc nghẽn) và Không tường minh (các nút tự rút ra tình trạng tắc nghẽn qua các trạng thái cục bộ của mình – chẳng hạn như có quá nhiều gói tin phải gửi lại).



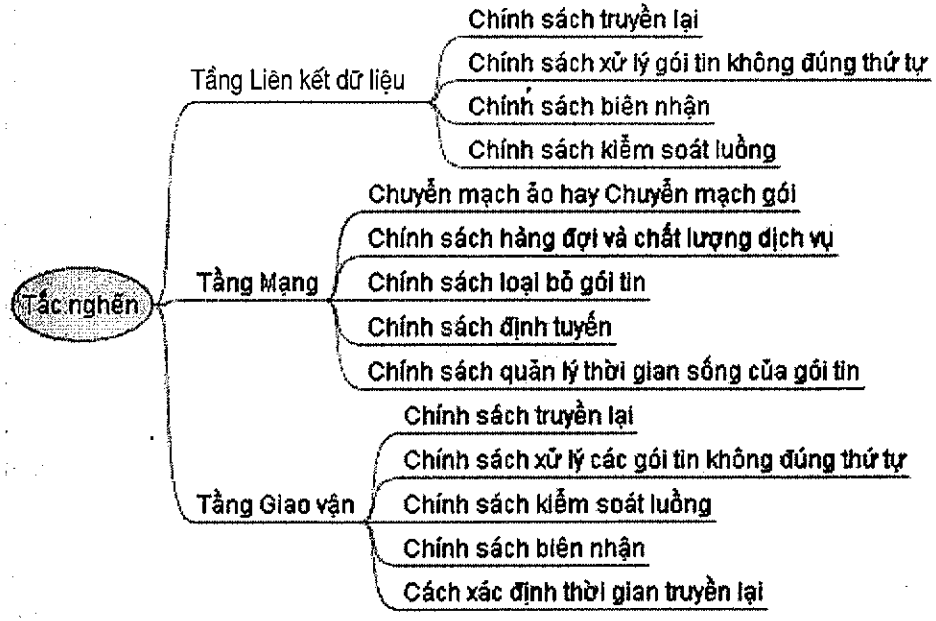

**Hình 4.41 Phân loại các giải pháp xử lý tắc nghẽn**

Nguyên nhân của tắc nghẽn là tại một thời điểm, tải lớn hơn năng lực xử lý của các tài nguyên mạng. Như vậy sẽ có hai giải pháp: Tăng tài nguyên cho mạng hoặc giảm tải. Có nhiều cách thức làm tăng tài nguyên, chẳng hạn nâng cấp đường truyền, sử dụng thêm các kết nối dự trữ... ; tuy nhiên không phải lúc nào cũng làm được điều này. Do vậy giải pháp khắc phục duy nhất là giảm tải. Có khá nhiều phương pháp để thực hiện điều này: có thể từ chối dịch vụ đối với một số người dùng (không đưa thêm dữ liệu vào mạng nữa), hay yêu cầu tất cả người dùng giảm lượng dữ liệu gửi vào mạng...

Những phương thức kể trên sẽ được nghiên cứu trong các phần sau. Đối với chuyển mạch ảo, những phương thức này được áp dụng ở tầng mạng, còn đối với chuyển mạch gói, những phương thức này lại có thể được cài đặt ở tầng giao vận.



## 4.9.2 Chính sách ngăn chặn tắc nghẽn




**Hình 4.42 Các chính sách ngăn chặn tắc nghẽn ở các tầng khác nhau**

Chúng ta bắt đầu xét giải pháp mở. Tư tưởng của chiến lược này là ngăn chặn không cho tắc nghẽn xuất hiện chứ không đợi đến lúc tắc nghẽn xuất hiện mới khắc phục. Mục tiêu này đạt được bằng các áp dụng nhiều chính sách khác nhau ở các tầng khác nhau. Trong Hình 4.42 chúng ta thấy các chính sách ở các tầng liên kết dữ liệu, mạng và giao vận ảnh hưởng đến tắc nghẽn.

Đầu tiên chúng ta xét đến tầng liên kết dữ liệu. Chính sách truyền lại xác định phía gửi sau bao lâu sẽ gửi lại gói tin chưa nhận được biên nhận. Rõ ràng nếu đặt thời gian timeout quá bé và sử dụng thuật toán Go-Back-N thì số lượng gói tin phía gửi đưa vào mạng lớn hơn rất nhiều so với hệ thống có timeout lớn và sử dụng thuật toán Selective Repeat. Một vấn đề liên quan mật thiết là chính sách lưu tạm thời dữ liệu ở phía nhận. Nếu phía nhận loại bỏ tất cả các gói dữ liệu đến không đúng thứ tự, các gói này sẽ được gửi lại

lần nữa và do đó làm tăng tổng số lượng gói tin truyền qua mạng. Rõ ràng thuật toán Selective Repeat có hiệu quả hơn Go-Back-N.

Chính sách biên nhận cũng ảnh hưởng đến tắc nghẽn. Nếu phía nhận gửi biên nhận cho mỗi gói tin nhận được thì số lượng gói tin biên nhận sẽ rất lớn. Tuy nhiên nếu biên nhận được dồn lại và gửi kèm cùng với các thông tin khác, hệ thống cũng tiết kiệm được đường truyền và góp phần làm giảm tắc nghẽn.

Ở tầng mạng, quyết định sử dụng chuyển mạch gói hay chuyển mạch ảo cũng ảnh hưởng đến việc kiểm soát tắc nghẽn vì một vài thuật toán chỉ có thể sử dụng trên mạch ảo. Chính sách hàng đợi và chất lượng dịch vụ liên quan đến việc tại mỗi đường ra (hay đường vào) của router có thể có một hay nhiều hàng đợi. Điều này cũng liên quan đến thứ tự ưu tiên khi xử lý các gói tin. Chính sách loại bỏ gói tin là quy tắc xác định gói tin nào sẽ bị loại bỏ trong trường hợp không đủ bộ đệm. Một chính sách tốt sẽ giúp làm giảm tắc nghẽn.

Một thuật toán định tuyến tốt giúp làm giảm tình trạng tắc nghẽn trên mạng bằng cách phân chia đều các gói tin trên tất cả các đường truyền. Một thuật toán không tốt có thể gửi quá nhiều gói tin qua một đường truyền đã bị tắc nghẽn. Cuối cùng, thời gian sống của gói tin (từ khi gửi cho đến khi bị xóa) cũng đóng vai trò quan trọng. Nếu thời gian này quá dài, các gói tin có thể lưu chuyển trên mạng quá lâu, nhưng nếu thời gian này quá dài, gói tin sẽ bị xóa trước khi đến đích, và do đó sẽ phải truyền lại.

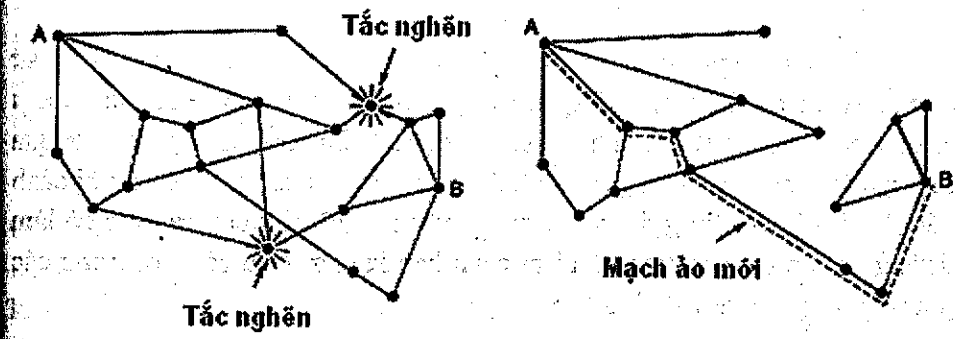
Vấn đề ở tầng giao vận cũng tương tự như ở tầng liên kết dữ liệu. Tuy nhiên xác định khoảng thời gian timeout phức tạp hơn rất nhiều vì giữa bên gửi và bên nhận có thể có nhiều router trung gian.

## 4.9.3 Kiểm soát tắc nghẽn trong mạch ảo

Trong mạch ảo thường sử dụng chiến lược mở: ngăn ngừa không cho tắc nghẽn xảy ra. Ở đây chúng ta sẽ mô tả một vài phương pháp kiểm soát động được sử dụng trong các mạng ảo.



Một kỹ thuật được sử dụng khá phổ biến là kiểm soát việc thiết lập kết nối mới. Khi bắt đầu tắc nghẽn, không mạch ảo nào được thiết lập cho đến khi hết tắc nghẽn. Như vậy, việc thiết lập kết nối ở tầng giao vận sẽ không thể thực hiện được. Ưu điểm của giải pháp này là tính đơn giản và dễ cài đặt. Trong mạng điện thoại truyền thống, khi một tổng đài rơi vào tình trạng quá tải, hệ thống thực hiện kiểm soát việc thiếp lập kết nối mới không cho phép kết nối qua tổng đài này.




**Hình 4.43 (a) Mạng bị tắc nghẽn (b) Mạng không có tắc nghẽn do mạch ảo từ A đến B vòng qua khu vực bị tắc nghẽn**

Một giải pháp khác là cho phép thiết lập mạch ảo, nhưng định tuyến mạch này không đi qua khu vực bị tắc nghẽn, như ví dụ trong Hình 4.43 Giả sử một nút gắn với router A muốn thiết lập kết nối tới nút gắn với router B. Bình thường, kết nối này sẽ được thực hiện qua một vài router đang bị tắc nghẽn. Để tránh trường hợp này, chúng ta vẽ lại hình trạng mạng như trong Hình 4.43b, loại bỏ các router bị tắc nghẽn và các đường truyền liên quan. Đường đứt nét là tuyến mạch ảo mới tránh khỏi khu vực tắc nghẽn.

Một chiến lược khác liên quan đến mạch ảo là nút sẽ "thương lượng" với hệ thống mạng để đạt được một "thỏa thuận" trước khi thiết lập mạch ảo. Thỏa thuận này bao gồm khối lượng, khuôn dạng và chất lượng dịch vụ của mạch ảo. Để đảm bảo thực hiện đúng thỏa thuận, hệ thống mạng thường thực hiện việc dự trữ tài nguyên dọc theo tuyến đường mạch ảo được thiết lập. Tài nguyên có thể là bảng định tuyến, bộ đệm, băng thông đường truyền của router. Do mỗi mạch ảo đều được đảm bảo những tài nguyên cần thiết, tắc nghẽn không bao giờ xuất hiện.

Quá trình dự trữ tài nguyên này có thể chỉ được thực hiện khi mạng bị tắc nghẽn hay là một thủ tục trong hoạt động bình thường của hệ thống. Nhược điểm của hệ thống này là lãng phí tài nguyên. Đó là cái giá cho việc thực hiện kiểm soát tắc nghẽn.

## 4.9.4 Kiểm soát tắc nghẽn trong mạng chuyển mạch gói

Trong mạng chuyển mạch gói, các router kiểm soát hiệu suất sử dụng của các đường truyền đi qua. Ví dụ mỗi đường truyền sẽ có một biến u (nằm trong khoảng [0,1]) là hiệu suất sử dụng đường truyền. Nếu u vượt qua một ngưỡng nào đó, đường truyền tương ứng chuyển sang trạng thái bị cảnh báo. Mỗi một gói tin gửi qua đường truyền này sẽ bị kiểm tra xem có làm đường truyền ở trong trạng thái bị cảnh báo không. Nếu có, một trong các phương pháp sau đây sẽ được áp dụng.

### Bit cảnh báo

Kiến trúc DECNET thực hiện việc cảnh báo bằng cách thiết lập một bit đặc biệt trong tiêu đề gói tin (giống kiến trúc Frame Relay). Khi gói tin đến đích, thực thể giao vận ở nút đích sẽ sao giá trị bit này vào gói tin biên nhận. Khi nhận được, phía gửi sẽ giảm tốc độ truyền.

Chừng nào còn ở trong trạng thái cảnh báo, router tiếp tục thiết lập giá trị bit cảnh báo. Sau một thời gian, các nút gửi nhận được các gói tin biên nhận có thiết lập bit cảnh báo và phải giảm tốc độ gửi dữ liệu. Quá trình giảm này tiếp tục cho đến khi không nhận được các gói tin có chứa dấu hiệu cảnh báo.

### Gói tin báo tắc nghẽn

Thuật toán trình bày trên nhờ phía nhận phản hồi cho phía gửi giảm tốc độ truyền. Tại sao router không thông báo trực tiếp tình trạng tắc nghẽn cho các nút ? Trong giải pháp này, router sẽ gửi một gói tin báo nghẽn cho phía gửi (địa chỉ nhận của gói báo nghẽn được xác định nhờ trường địa chỉ gửi của gói tin bình thường). Gói tin bình thường được đánh dấu (bằng cách



thiết lập một trường nào đó trong tiêu đề gói tin) và chuyển tiếp bình thường tới đích. Mục đích của việc đánh dấu là không phát sinh thêm các gói tin báo nghẽn do gói tin bình thường sinh ra khi đến các router khác.

Khi nhận được gói tin báo nghẽn, nút gửi phải giảm tốc độ truyền tới địa chỉ đích cụ thể đi X%. Có thể các gói tin gửi đến cùng địa chỉ đích này cũng khiến phát sinh ra các gói tin báo nghẽn, nên phía gửi sẽ bỏ qua các gói tin báo nghẽn trong một khoảng thời gian nào đó. Sau đó, phía gửi tiếp tục kiểm tra xem có nhận được gói tin báo nghẽn nào không. Nếu có, nó lại tiếp tục giảm tốc độ gửi vì trên đường truyền đến đích chắc chắn xuất hiện tắc nghẽn. Nút gửi có thể tăng tốc độ gửi trong trường hợp không nhận được gói tin báo nghẽn trong một khoảng thời gian đủ lâu.

Bằng cách điều chỉnh các tham số truyền (chẳng hạn độ lớn cửa sổ), nút có thể làm giảm tốc độ truyền. Thông thường, khi nhận được gói tin báo nghẽn đầu tiên, tốc độ truyền giảm 50%, lần nhận gói tin báo nghẽn thứ hai khiến tốc độ truyền giảm xuống còn 25%... Tuy nhiên tốc độ truyền tăng từ từ để tránh sự tái xuất hiện của tắc nghẽn.

Có khá nhiều phiên bản của thuật toán này. Chẳng hạn một router có thể có nhiều mức ngưỡng khác nhau. Phụ thuộc vào mức ngưỡng nào, router có thể gửi các gói tin báo nghẽn ở các mức độ khác nhau.

## 4.9.5 Cắt tải

Nếu không phương pháp nào trình bày trên khắc phục hoàn toàn tắc nghẽn, router có thể sử dụng một phương pháp rất mạnh: cắt tải. Khi có quá nhiều gói tin đến router và router không thể xử lý hết, router sẽ xóa bỏ một số gói tin. Điều này cũng tương tự để đảm bảo an toàn cho mạng lưới điện vào những ngày hè (khi nhu cầu điện lớn hơn lượng điện có thể cung cấp), một vài khu vực sẽ bị cắt điện.

Router có thể loại bỏ ngẫu nhiên các gói tin, nhưng thông thường router loại bỏ theo một chiến lược nào đó. Chiến lược này phụ thuộc vào ứng dụng đang chạy. Ví dụ đối với ứng dụng truyền file (FTP), gói tin cũ có

ích hơn gói tin mới, vì chẳng hạn nếu loại bỏ gói tin 6 và giữ lại các gói tin từ 7 đến 10 có thể sẽ khiến tất cả gói tin từ 6-10 phải gửi lại nếu phía nhận không chấp nhận các gói tin đến không theo thứ tự. Như vậy nếu file gồm 12 gói tin, loại bỏ gói 6 sẽ khiến phải truyền lại gói 7 đến 12 nhưng loại bỏ gói 10 thì chỉ cần truyền lại gói 10 đến 12. Tuy nhiên với ứng dụng đa phương tiện thì gói tin mới có ích hơn gói tin cũ.

Đối với nhiều ứng dụng, một số gói tin có tầm quan trọng hơn các gói tin khác. Chẳng hạn với một số thuật toán nén phim đôi khi gửi toàn bộ frame (chứa hình ảnh) trong một gói tin và các gói tin sau chỉ lưu lại các khác biệt so với frame ban đầu. Do vậy, ở đây nếu phải loại bỏ một gói tin thì nên loại bỏ gói tin chứa các gói tin biến đổi chứ không nên loại bỏ gói tin chứa một frame hoàn chỉnh.

Để cài đặt chiến lược loại bỏ thông minh, ứng dụng phải đánh dấu các gói tin ở các độ ưu tiên (thể hiện sự quan trọng) khác nhau. Khi đó, tại các router, các gói tin ít quan trọng sẽ bị loại bỏ trước.

**Phát hiện sớm ngẫu nhiên (Random Early Detection)**

Rõ ràng xử lý tắc nghẽn ngay khi phát hiện ra sẽ có hiệu quả hơn nhiều nếu trì hoãn xử lý rồi sau đó mới khắc phục. Thuật toán thực hiện điều này – RED (Random Early Detection) – thực hiện loại bỏ các gói tin trước khi router sử dụng hết các bộ đệm. Trong một số giao thức ở tầng giao vận (chẳng hạn TCP), phía gửi khi bắt đầu thấy mất gói tin (không nhận được biên nhận) sẽ bắt đầu giảm tốc độ gửi. Ý tưởng của điều này là TCP được sử dụng trên mạng có dây (tỷ lệ lỗi thấp) nên nếu gói tin bị mất thì nguyên nhân lớn nhất là thiếu bộ đệm ở router. Điều này có thể được sử dụng để tránh tắc nghẽn.

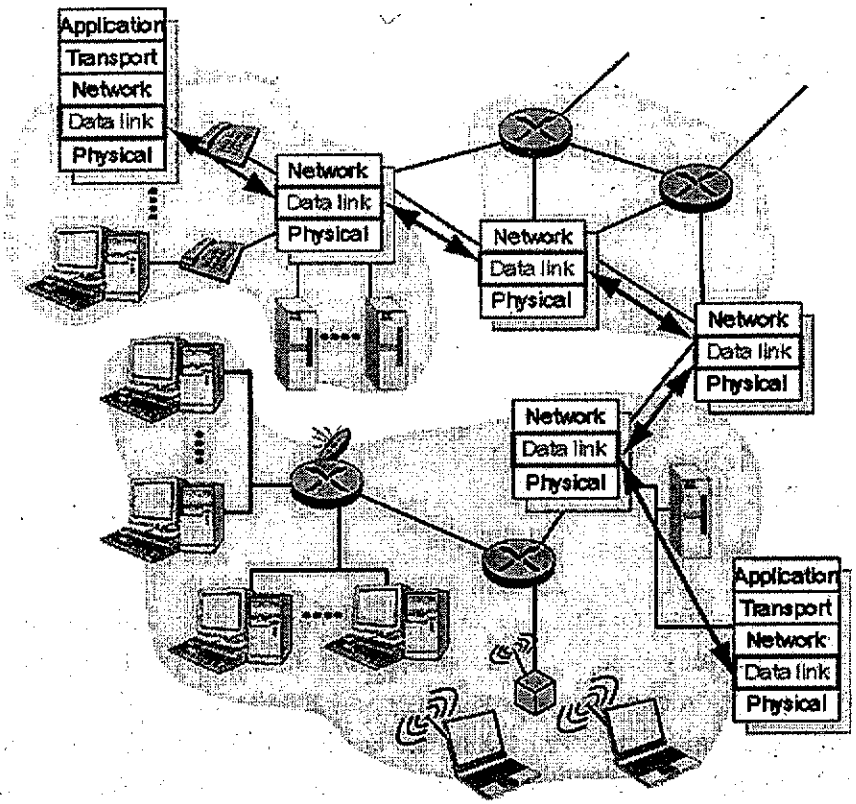
Nếu router ngăn ngừa trước khi tắc nghẽn thực sự xảy ra thì tắc nghẽn sẽ không xảy ra ở mức độ nghiêm trọng. Để xác định khi nào bắt đầu xảy ra tắc nghẽn, độ dài hàng đợi trung bình của mỗi đường truyền được gán một mức ngưỡng nào đó. Nếu vượt quá ngưỡng này, chắc chắn tắc nghẽn bắt đầu xuất hiện và router thực hiện loại bỏ gói tin.



# Chương 5
# TẦNG LIÊN KẾT DỮ LIỆU

## 5.1 CÁC KHÁI NIỆM CHUNG, DỊCH VỤ CỦA TẦNG DATALINK

Ở chương trước chúng ta đã biết tầng mạng cung cấp dịch vụ truyền thông giữa hai máy tính. Ví dụ trong Hình 5.1 đường truyền thông này bắt đầu từ máy nguồn qua lần lượt các router và kết thúc ở máy đích. Để thuận tiện, chúng ta coi cả máy tính và router là các **nút (node)** vì ở đây nút là router hay máy tính không phải là vấn đề quan trọng và kênh truyền thông kết nối giữa hai nút liền kề trên toàn bộ đường truyền thông được gọi là **đường liên kết,** hay **đường truyền (link)**. Để gói dữ liệu (datagram) đi từ máy tính nguồn tới máy tính đích, gói dữ liệu phải được chuyển trên mỗi đường liên kết. Chương này tập trung vào tầng liên kết dữ liệu với nhiệm vụ truyền gói dữ liệu trên một đường liên kết (đường truyền vật lý). Đầu tiên chúng ta sẽ phân loại và nghiên cứu những dịch vụ của tầng liên kết dữ liệu. Từ phần 5.2 đến phần 5.4 là các nguyên lý quan trọng của những giao thức cung cấp các dịch vụ này (ví dụ nhận lỗi và sửa lỗi, giao thức đa truy cập được sử dụng để chia sẻ đường truyền vật lý duy nhất giữa các nút và địa chỉ mức liên kết dữ liệu). Chúng ta sẽ thấy nhiều kiểu công nghệ kết nối khác nhau được sử dụng để nối hai nút, từ phần 5.5 đến phần 5.10 chúng ta sẽ nghiên cứu chi tiết kiến trúc và giao thức của các kiểu kết nối.




**Hình 5.1 Vị trí của tầng liên kết dữ liệu**

## 5.1.1 Những dịch vụ của tầng liên kết dữ liệu

Giao thức tầng liên kết dữ liệu được sử dụng để truyền gói dữ liệu trên một môi trường vật lý. Giao thức tầng liên kết dữ liệu định nghĩa khuôn dạng đơn vị dữ liệu trao đổi giữa các nút ở mỗi đầu của đường truyền, cũng như những công việc các nút thực hiện khi nhận và gửi những đơn vị dữ liệu này. Trong chương 1 chúng ta đã biết rằng đơn vị dữ liệu của tầng liên kết dữ liệu là frame và mỗi frame tầng liên kết dữ liệu chứa một gói dữ liệu tầng mạng. Công việc của giao thức tầng liên kết dữ liệu khi gửi và nhận frame gồm: phát hiện lỗi, truyền lại, điều khiển lưu lượng và truy cập ngẫu nhiên.



Giao thức tầng liên kết dữ liệu gồm: Ethernet, token ring, FDDI và PPP; đôi khi ATM và frame relay có thể cũng được coi là giao thức tầng liên kết dữ liệu. Chúng ta sẽ nghiên cứu chi tiết những giao thức này trong nửa chương sau.

Nếu nhiệm vụ của tầng mạng là chuyển gói dữ liệu của tầng giao vận từ máy gửi tới máy nhận thì giao thức của tầng liên kết dữ liệu có nhiệm vụ chuyển gói dữ liệu tầng mạng giữa hai nút kế tiếp trên đường truyền. Một đặc điểm quan trọng của tầng liên kết dữ liệu là gói dữ liệu tầng mạng có thể được xử lí bởi các giao thức liên kết dữ liệu khác nhau trên đường truyền. Ví dụ, gói dữ liệu này có thể được chuyển bởi giao thức Ethernet trên đường truyền đầu tiên, bởi PPP ở đường truyền cuối cùng và frame relay trên các đường truyền ở giữa. Chú ý quan trọng là các giao thức liên kết dữ liệu khác nhau có thể cung cấp những dịch vụ khác nhau. Giao thức tầng liên kết dữ liệu không nhất thiết phải cung cấp dịch vụ truyền tin cậy. Vì vậy tầng mạng phải tính đến khả năng hoạt động trên nhiều kiểu dịch vụ liên kết dữ liệu khác nhau.

Để hiểu rõ quan hệ của tầng liên kết dữ liệu với tầng mạng như thế nào xét ví dụ sau. Giả sử một đại lý du lịch phải sắp xếp cho khách du lịch đi từ KS Hilton, Hà Nội đến Ngọ Môn, Huế. Đầu tiên khách du lịch sẽ đi xe buýt đến sân bay Nội Bài, bay bằng máy bay của Hàng không Việt Nam đến Huế và đi taxi từ sân bay Phú Bài, Huế đến Ngọ Môn. Sau khi đại lý du lịch tiến hành đặt chỗ, thì chính công ty xe buýt chịu trách nhiệm đưa khách du lịch từ Hilton đến Nội Bài, Hàng không Việt Nam chịu trách nhiệm từ Nội Bài đến sân bay Phú Bài và hãng taxi từ sân bay Huế đến Ngọ Môn. Mỗi một trong ba chặng này được xem là một lần chuyển trực tiếp giữa các "nút" kế tiếp. Rõ ràng ba chặng đường sẽ được các công ty khác nhau phụ trách. Trong ví dụ trên có thể xem khách du lịch là datagram (gói tin của tầng mạng), chặng đường tương ứng với một đường truyền vật lý, phương tiện đi lại trên chặng đường là giao thức cho đường truyền vật lý và đại lý du lịch chính là giao thức định tuyến ở tầng mạng.

Dịch vụ cơ bản của bất kì tầng liên kết dữ liệu nào là chuyển gói dữ liệu của tầng mạng giữa hai nút kế tiếp, song cụ thể dịch vụ này được thực hiện như thế nào lại phụ thuộc vào giao thức tầng liên kết dữ liệu sử dụng

trên đường truyền đó. Nói chung giao thức tầng liên kết dữ liệu có thể cung cấp những dịch vụ sau:

**Đóng gói dữ liệu (frame) và truy cập đường truyền (link access):** Phần lớn các giao thức tầng liên kết dữ liệu đặt gói dữ liệu tầng mạng vào trong gói dữ liệu tầng liên kết dữ liệu (frame) trước khi truyền lên trên đường truyền. Frame gồm trường dữ liệu là gói dữ liệu của tầng mạng cùng với một số trường tiêu đề khác. Chú ý frame có thể có cả trường tiêu đề đầu và cuối (header và trailer). Giao thức tầng liên kết dữ liệu xác định khuôn dạng của frame cũng như giao thức truy cập kênh truyền (cách thức truyền). Với đường truyền kiểu point-to-point có một phía gửi và một phía nhận thì giao thức truy cập đường truyền khá đơn giản (gần như không tồn tại) - bên gửi có thể gửi frame bất cứ lúc nào đường truyền rỗi. Trường hợp phức tạp hơn xảy ra khi nhiều nút cùng chia sẻ đường truyền duy nhất: đây là vấn đề đa truy cập. Giao thức đa truy cập được nghiên cứu trong phần 5.3. Chúng ta sẽ thấy các giao thức liên kết dữ liệu khác nhau sẽ có những khuôn dạng dữ liệu khác nhau (chú ý gói dữ liệu của tầng liên kết dữ liệu được gọi là frame). Trong phần 5.3, chúng ta sẽ thấy tiêu đề frame thường chứa trường **địa chỉ vật lí** của nút, (địa chỉ này khác địa chỉ IP).

**Dịch vụ truyền tin cậy.** Nếu cung cấp dịch vụ truyền tin cậy, giao thức tầng liên kết dữ liệu bảo đảm chuyển chính xác gói dữ liệu tầng mạng trên một đường truyền. Trong chương 3 chúng ta thấy rằng giao thức tầng giao vận (TCP) cũng cung cấp dịch vụ truyền tin cậy. Tương tự như trong tầng giao vận, truyền tin cậy ở tầng liên kết dữ liệu được thực hiện qua cơ chế báo nhận và truyền lại (xem phần 3.4). Dịch vụ truyền tin cậy ở tầng liên kết dữ liệu thường được sử dụng trên đường truyền có tỉ lệ lỗi cao (ví dụ trên đường truyền không dây). Mục đích là sửa lỗi ngay trên đường truyền bị lỗi chứ không phải truyền lại dữ liệu từ thiết bị gửi tới thiết bị nhận bởi giao thức tầng giao vận hoặc tầng ứng dụng. Tuy nhiên tầng liên kết dữ liệu không cần cung cấp dịch vụ truyền tin cậy cho các đường truyền ít lỗi (ví dụ cáp quang). Vì vậy phần lớn các giao thức tầng liên kết dữ liệu phổ biến không cung cấp dịch vụ truyền tin cậy.

**Kiểm soát lưu lượng.** Khả năng lưu trữ tạm thời (buffer) các frame tại các nút trên mỗi phía của đường truyền không phải là vô hạn. Đây sẽ là



vấn đề khi tốc độ tới của các frame nhanh hơn tốc độ nút nhận có thể xử lí được. Nếu không kiểm soát lưu lượng, bộ đệm phía nhận có thể bị tràn và frame sẽ bị mất. Giống như tầng giao vận, tầng liên kết dữ liệu cung cấp cơ chế kiểm soát lưu lượng để ngăn chặn phía phát gửi quá khả năng nhận của phía thu.

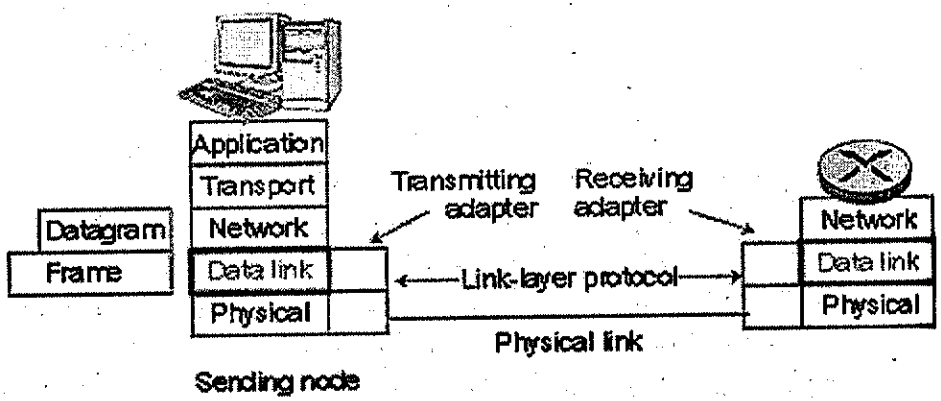
**Phát hiện lỗi.** Nút nhận có thể nhận bit 0 trong khi phía gửi gửi bit 1 hay ngược lại. Nguyên nhân bit bị lỗi có thể do tín hiệu bị suy hao hay nhiễu điện từ. Nhiều giao thức tầng liên kết dữ liệu cung cấp cơ chế phát hiện lỗi. Điều này được thực hiện bằng cách phía gửi sẽ thiết lập một số bit phát hiện lỗi trong frame và phía nhận thực hiện việc kiểm tra lỗi. Dịch vụ phát hiện lỗi rất phổ biến trong nhiều giao thức tầng liên kết dữ liệu. Trong chương 3 và chương 4 chúng ta thấy tầng giao vận và tầng mạng trên Internet cũng có khả năng phát hiện lỗi. Tuy nhiên phát hiện lỗi trong tầng liên kết dữ liệu phức tạp hơn rất nhiều và do vậy thường được triển khai bằng phần cứng.

**Sửa lỗi.** Sửa lỗi cũng tương tự phát hiện lỗi. Tuy nhiên không chỉ phát hiện được lỗi có khả năng mà phía nhận còn có khả năng xác định chính xác vị trí lỗi xuất hiện trong frame (và do đó có thể sửa được những lỗi này). Phát hiện và sửa lỗi được nghiên cứu trong phần 5.2.

**Bán song công và song công (Half duplex, full duplex).** Trong chế độ truyền song công, hai phía của đường truyền có thể đồng thời truyền dữ liệu. Trong chế độ truyền bán song công, tại một thời điểm thiết bị không thể cùng truyền và nhận.

Như nói trên, nhiều dịch vụ của tầng liên kết dữ liệu giống dịch vụ của tầng giao vận, chẳng hạn cả hai tầng đều có dịch vụ truyền tin cậy. Mặc dù cơ chế thực hiện dịch vụ truyền tin cậy ở cả hai tầng giống nhau (xem phần 3.4), nhưng hai dịch vụ truyền tin cậy này không giống nhau. Giao thức tầng giao vận cung cấp dịch vụ truyền tin cậy giữa hai tiến trình trên cơ sở đầu cuối (end-to-end). Giao thức tầng liên kết dữ liệu cung cấp dịch vụ truyền tin cậy giữa hai nút có một đường truyền vật lý trực tiếp. Tương tự với dịch vụ kiểm soát lưu lượng và phát hiện lỗi.

## 5.1.2 Bộ điều hợp (Adapter)



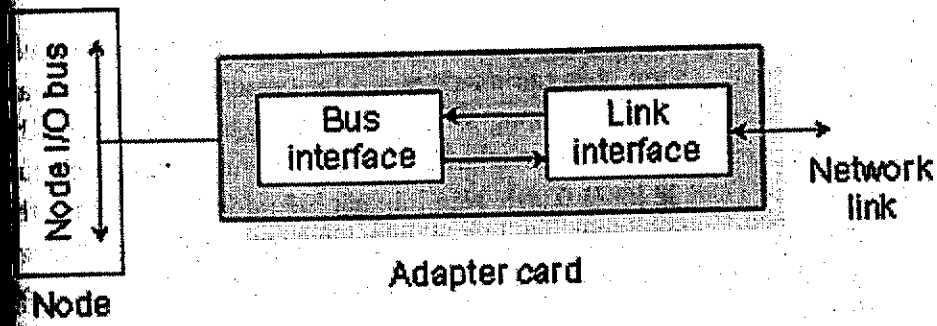

**Hình 5.2 Tầng liên kết dữ liệu được triển khai tại adapter**

Với phần lớn đường truyền, giao thức tầng liên kết dữ liệu được triển khai trên **adapter**. Adapter là bo mạch (hoặc card PCMCIA) có RAM, chip DSP, giao diện ghép nối (interface) với bus máy tính và giao diện ghép nối với đường truyền. Adapter cũng thường được coi là card giao tiếp mạng hay gọi tắt là card mạng (**NIC - Network Interface Card**). Như minh họa trên Hình 5.2, tầng mạng trên nút gửi (máy tính hoặc router) chuyển gói dữ liệu tầng mạng (datagram) xuống adapter để gửi sang phía bên kia đường truyền. Adapter đặt datagram trong frame, sau đó truyền frame qua đường truyền. Adapter phía bên kia (phía nhận) nhận frame, lấy và chuyển datagram lên tầng mạng. Nếu giao thức tầng liên kết dữ liệu cung cấp dịch vụ phát hiện lỗi thì adapter gửi đặt thêm một số bit phát hiện lỗi và adapter nhận thực hiện việc kiểm tra lỗi. Nếu giao thức tầng liên kết dữ liệu cung cấp dịch vụ truyền tin cậy thì những kĩ thuật cho dịch vụ truyền tin cậy (ví dụ số thứ tự, bộ định thời, biên nhận) được cài đặt ngay trên adapter. Nếu giao thức tầng liên kết dữ liệu cung cấp dịch vụ truy cập ngẫu nhiên (phần 5.3) thì giao thức này cũng được triển khai trên adapter.

Adapter là đơn vị bán tự trị. Ví dụ, adapter có thể nhận frame, xác định liệu frame có bị lỗi không và nếu có thì loại bỏ frame mà không thông



ão cho thiết bị. Khi nhận được frame đến từ môi trường vật lý (chẳng hạn rd mạng), adapter chỉ thông báo cho thiết bị (chính xác là CPU của thiết ) khi adapter muốn chuyển gói dữ liệu datagram trong frame tới tầng mạng ủa thiết bị. Việc này sẽ được thực hiện thông qua ngắt phần cứng nterrupt). Tương tự, khi nút gửi gói dữ liệu đến adapter, có thể coi adapter ược uỷ quyền để chuyển gói dữ liệu sang nút kế tiếp. Mặt khác, adapter hông là đơn vị tự trị hoàn toàn. Mặc dù chúng ta coi adapter là "hộp đen" ư minh họa trên Hình 5.3, adapter vẫn nằm trong máy tính, dùng chung guồn điện và bus - do đó vẫn nằm dưới sự điều khiển của máy tính.




**Hình 5.3 Kiến trúc Adapter**

Thành phần chính của adapter là giao diện ghép nối bus và giao diện hép nối đường truyền. Giao diện bus chịu trách nhiệm truyền thông với nút hứa adapter (chính xác hơn là với CPU). Nó truyền dữ liệu cùng thông tin iều khiển giữa nút và card mạng. Giao diện đường truyền (link interface) ó trách nhiệm triển khai giao thức tầng liên kết dữ liệu. Bên cạnh chức năng đóng gói (framing) và bóc tách (de-framing) gói dữ liệu, card mạng có hể cung cấp dịch vụ phát hiện lỗi, truy cập ngẫu nhiên và các chức năng khác của tầng liên kết dữ liệu. Nó chứa các mạch truyền và nhận (circuitry). Với những công nghệ phổ biến ở tầng liên kết dữ liệu – ví dụ như Ethernet, giao diện đường truyền được triển khai trên các chip. Chip được sản xuất đại trà và bán rộng rãi, do đó, adapter Ethernet rẻ - thường không quá 10 USD.

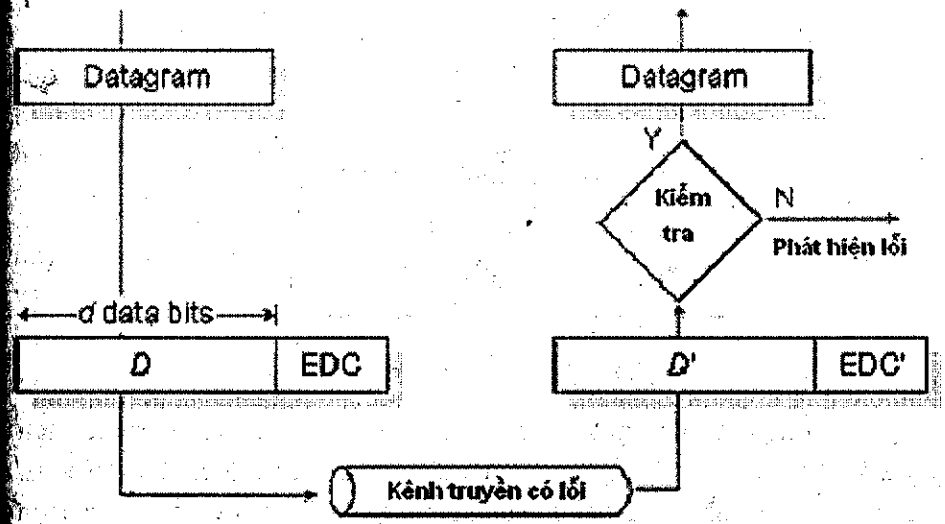
## 5.2 KỸ THUẬT PHÁT HIỆN VÀ SỬA LỖI

Các đường điện thoại bình thường (truyền tín hiệu tương tự trên đường dây đồng) có tỷ lệ lỗi tương đối cao. Việc thay thế hệ thống này rất khó thực thi vì quá tốn kém. Bên cạnh đó mạng không dây có tỷ lệ lỗi cao hơn rất nhiều so với mạng có dây. Do vậy nếu cơ sở truyền thông của chúng ta vẫn dựa trên mạng điện thoại bình thường cũng như việc mạng không dây ngày càng phổ biến thì các nhà nghiên cứu vẫn phải nghiên cứu các phương thức để xử lý lỗi trên đường truyền.

Về đặc điểm xuất hiện lỗi, người ta thấy rằng lỗi có xu hướng xuất hiện theo cụm chứ không phải các lỗi riêng lẻ. Tại sao đặc điểm này quan trọng khi tìm giải pháp phòng chống lỗi ? Chúng ta xét thử ví dụ sau. Khi truyền, dữ liệu thường được gửi theo khối. Giả sử kích thước trung bình của khối là 1000 bit và tỷ lệ lỗi là 0.001. Nếu lỗi xuất hiện độc lập với nhau thì trung bình mỗi khối đều có lỗi. Nhưng nếu lỗi xuất hiện thành cụm 100 bit thì trung bình trong 100 khối sẽ có từ 1 đến 2 khối bị lỗi. Nói chung lỗi theo cụm khó sửa hơn lỗi riêng lẻ.

Một trong các dịch vụ mà tầng liên kết dữ liệu cung cấp là **phát hiện (detection) và sửa (correct) lỗi** ở mức bit – cho phép phát hiện và trong một số trường hợp có thể sửa các bit bị lỗi trong frame của tầng liên kết dữ liệu gửi giữa hai nút kế tiếp. Trong chương 3 chúng ta đã thấy dịch vụ phát hiện lỗi cũng được triển khai ở tầng giao vận. Trong phần này, chúng ta sẽ nghiên cứu một vài kỹ thuật đơn giản nhất trong việc phát hiện và sửa lỗi bit. Ở đây chúng ta chỉ trình bày hết sức sơ lược với mục tiêu giúp độc giả hình dung ra một vài kỹ thuật được áp dụng trong một số giao thức tầng liên kết dữ liệu thông dụng.Hình 5.4 minh hoạ ý tưởng của việc triển khai dịch vụ phát hiện lỗi. Tại nút gửi, dữ liệu D được sử dụng để xác định các bit phát hiện và sửa lỗi EDC. Dữ liệu cần bảo vệ không chỉ gồm gói dữ liệu datagram tầng mạng chuyển xuống mà còn các trường khác trong tiêu đề frame như trường địa chỉ, trường số thứ tự... Cả D và EDC cùng được gửi đến nút nhận trong cùng một frame. Bên kia sẽ nhận được chuỗi bit là D' và EDC'. Chú ý rằng, D' và EDC' có thể không giống D và EDC vì trên kênh truyền có thể có lỗi.



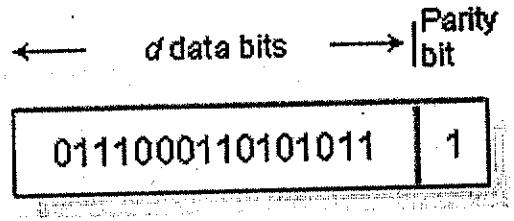



**Hình 5.4 Kiểm tra và phát hiện lỗi**

Phía nhận phải xác định liệu D' có chính là D được phía bên kia gửi hay không trong trường hợp nhận được cả D' và EDC'. Tại phía nhận, kết quả kiểm tra frame có lỗi không rất quan trọng (xem Hình 5.4). Chú ý rằng ở đây chúng ta xác định có ***phát hiện được lỗi*** không chứ không phải là ***có lỗi hay không***). Kỹ thuật phát hiện và sửa lỗi không phải luôn luôn cho phép phía nhận xác định được có lỗi hay không: sẽ có những trường hợp sử dụng bit phát hiện lỗi nhưng không có khả năng phát hiện khi xuất hiện lỗi, nghĩa là phía nhận sẽ không biết rằng thông tin nhận được bị lỗi. Hậu quả là phía nhận có thể chuyển gói dữ liệu bị lỗi lên tầng mạng, hoặc không biết rằng nội dung của một vài trường nào đó trong tiêu đề frame bị lỗi. Vì thế chúng ta mong muốn lựa chọn phương pháp có xác suất không phát hiện được lỗi nhỏ nhất có thể. Nói chung, các kĩ thuật phát hiện và sửa lỗi tinh vi (xác suất không phát hiện được lỗi khi có lỗi rất nhỏ) thường đòi hỏi nhiều thời gian tính toán (xác định EDC từ D), số lượng bit dư thừa lớn (EDC lớn) và tại phía nhận việc kiểm tra mất nhiều thời gian.

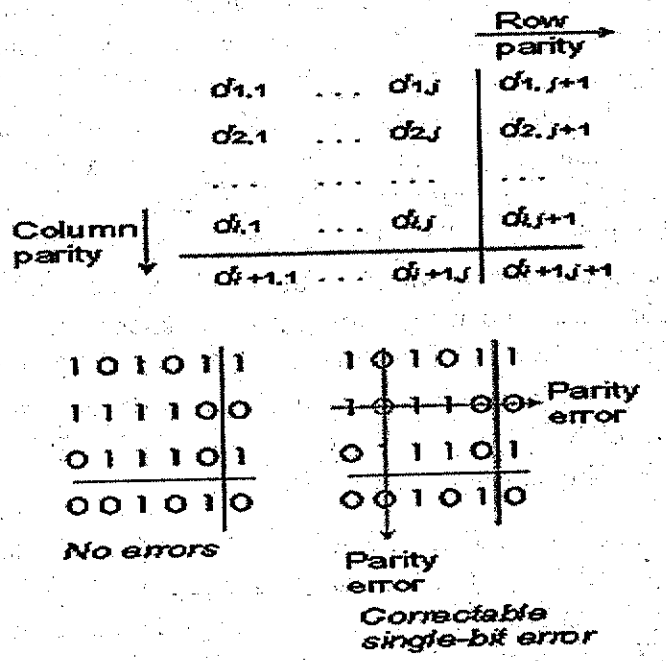
Bây giờ chúng ta sẽ xem xét một số kỹ thuật phát hiện lỗi đơn giản: bit chẵn lẻ (để minh họa ý tưởng của công việc); tính tổng (checksum) - được sử dụng ở tầng giao vận và bit dư thừa vòng - được sử dụng ở tầng liên kết dữ liệu. Kế tiếp chúng ta sẽ trình bày về mã Hamming, một phương pháp đơn giản nhưng có khả năng sửa được lỗi.

## 5.2.1 Kiểm tra tính chẵn lẻ




Hình 5.5 Kiểm tra tính chẵn lẻ

Phương pháp đơn giản nhất để phát hiện lỗi là sử dụng một **bit chẵn lẻ (parity bit)**. Giả sử thông tin D được gửi trong Hình 5.5 có d bit. Nếu sử dụng bit chẵn lẻ chẵn, bên gửi bổ sung một bit và giá trị bit này được chọn sao cho tổng số số bit 1 trong d+1 bit (d bit thông tin gốc D và một bit chẵn lẻ) là chẵn. Với bit chẵn lẻ lẻ, giá trị bit chẵn lẻ được chọn sao cho tổng số số bit 1 là một số lẻ. Hình 5.5 minh hoạ ví dụ bit chẵn lẻ chẵn, và bit chẵn lẻ (EDC) được đặt trong một trường khác với trường dữ liệu.




Hình 5.6 Kiểm tra chẵn lẻ hai chiều



Việc kiểm tra tại phía nhận cũng tương đối đơn giản. Phía nhận chỉ cần đếm số bit 1 trong d+1 bit nhận được. Nếu tổng số đếm được là một số lẻ trong khi sử dụng số chẵn lẻ chẵn thì phía nhận biết rằng ít nhất đã xuất hiện một bit bị lỗi. Chính xác hơn, tổng số các bit bị lỗi là một số lẻ.

Điều gì sẽ xảy nếu số bit bị lỗi là một số chẵn? Trong trường hợp này rõ ràng bên nhận không phát hiện được lỗi. Nếu xác suất bit bị lỗi thấp và giả định các bit bị lỗi xuất hiện độc lập với nhau thì khả năng một gói dữ liệu có nhiều bit bị lỗi sẽ cực kỳ thấp. Trong trường hợp này, có thể chỉ cần sử dụng một bit chẵn lẻ. Tuy nhiên, các thực nghiệm đã chỉ ra rằng lỗi không xuất hiện độc lập mà thường theo từng "cụm" (burst). Khi đó xác suất lỗi không bị phát hiện trong frame sử dụng một bit chẵn lẻ là 50%. Rõ ràng cần phải có phương pháp khác mạnh hơn. Nhưng trước khi nghiên cứu các phương pháp phát hiện lỗi được sử dụng trong thực tế, chúng ta hãy xét một phương pháp khác dựa trên bit chẵn lẻ có khả năng sửa được lỗi.

Hình 5.6 minh họa việc cải tiến phương pháp bit chẵn lẻ thông qua mảng hai chiều. Ở đây d bit trong D được sắp xếp vào bảng i dòng và j cột. Sau đó bên gửi xác định giá trị bit chẵn lẻ cho tất cả các dòng và cột. (i+j+1) bit chẵn lẻ được tạo ra này sẽ là các bit phát hiện và sửa lỗi của frame.

Bây giờ, giả sử rằng trên đường truyền có một bit duy nhất trong d bit thông tin gốc bị lỗi. Với phương pháp chẵn lẻ hai chiều, sẽ xuất hiện mâu thuẫn trong cả hàng và cột chứa bit bị lỗi. Khi đó phía nhận không những chỉ phát hiện có lỗi mà còn có thể xác định được vị trí bit bị lỗi (và do đó sửa được) thông qua chỉ số hàng và cột của bit đó.

Hình 5.6 chỉ ra ví dụ, bit có giá trị 1 tại vị trí (1,1) bị lỗi và bị chuyển thành 0. Lỗi mà sẽ được phía nhận phát hiện và sửa lại. Mặc dù, ở đây chúng ta chỉ quan tâm đến d bit thông tin, nhưng một bit lỗi trong các bit chẵn lẻ kiểm tra cũng sẽ bị phát hiện. Phương pháp này cũng có thể phát hiện được (nhưng không sửa được) khi có 2 bit bị lỗi trong gói dữ liệu.

Khả năng phía nhận vừa phát hiện vừa sửa được lỗi được gọi là FEC (Forward Error Correction). Những kĩ thuật này thường được sử dụng phổ biến trong các thiết bị lưu trữ âm thanh như đĩa CD nhạc. Trong môi trường mạng, kĩ thuật FEC có thể được sử dụng một mình, hoặc cùng với kĩ thuật

ARQ đã được nghiên cứu trong chương 3. Ưu điểm của kỹ thuật FEC là cho phép phía gửi không phải truyền lại (do phía nhận sửa được các thông tin bị lỗi). Có lẽ quan trọng hơn là phía nhận sửa được lỗi ngay khi nhận được. Điều này tránh thời gian đợi khi phía gửi phải truyền lại gói dữ liệu. Ưu điểm này được áp dụng trong các ứng dụng thời gian thực.

## 5.2.2 Phương pháp tính tổng kiểm tra (checksum)

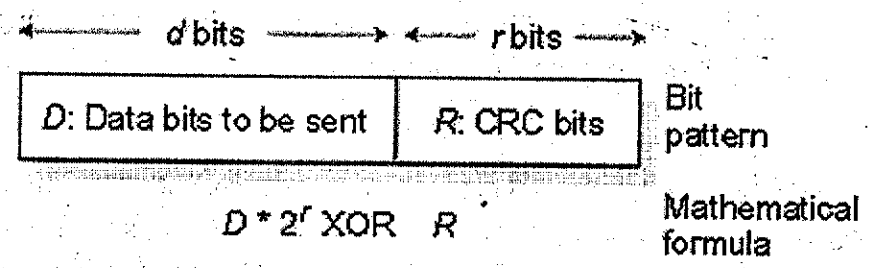
Trong kỹ thuật checksum, d bit dữ liệu trong Hình 5.4 được xem là dãy liên tiếp các số nguyên có độ dài k bit. Trong kỹ thuật checksum đơn giản, người ta tính tổng tất cả các số nguyên k bit này và sử dụng kết quả tính được làm các bit phát hiện lỗi. Phương pháp Internet checksum dựa trên hướng tiếp cận này - luồng dữ liệu được coi dãy liên tiếp các số nguyên 16 bit và Internet checksum là giá trị bù một của tổng các số nguyên 16 bit. Như đã trình bày trong phần 3.3.2, phía nhận tính lại checksum trên dữ liệu nhận được và kiểm tra xem nó có trùng với checksum trong gói dữ liệu nhận được hay không. RFC 1071 nêu chi tiết thuật toán Internet checksum cũng như phương thức triển khai. Trong giao thức TCP/IP, Internet checksum được tính toán trên tất cả các trường (kể cả trường tiêu đề và dữ liệu). Trong những giao thức khác, ví dụ như XTP [Strayer 1992], có cả checksum cho các trường tiêu đề và checksum cho toàn bộ gói dữ liệu.

McAuley [McAuley 1994] và Feldmeier [Feldmeier 1995] mô tả cách triển khai bằng phần mềm việc tính toán checksum.

## 5.2.3 Kiểm tra dư thừa vòng (CRC)

Kĩ thuật phát hiện lỗi được sử dụng rộng rãi trên mạng máy tính ngày nay dựa trên mã CRC. Mã CRC còn được gọi là mã đa thức vì có thể xem dãy các bit được gửi như một đa thức với hệ số nhận nhận giá trị 0 hoặc 1 và thao tác trên dãy bit này giống như thực hiện phép toán trên đa thức.






Hình 5.7 Mã dư thừa vòng

Mã CRC hoạt động như sau. Giả sử phía gửi muốn gửi d bit dữ liệu D. Đầu tiên hai bên phải thống nhất trước **đa thức sinh (generator)** ký hiệu là G có (r+1) bit. Bit có trọng số cao nhất của G phải nhận giá trị 1. Ý tưởng chính của mã CRC được minh họa trên Hình 5.7. Căn cứ vào dữ liệu nguyên thủy D, bên gửi sẽ xác định dữ liệu dư thừa R gồm r bit. Sau đó ghép R với D thu được (d+r) bit. R được chọn sao cho đa thức ứng với (d+r) bit này chia hết cho G. Phép chia ở đây được thực hiện theo module 2. Phía nhận thực hiện quá trình kiểm tra lỗi CRC khá đơn giản: chia d+r bit nhận được cho G. Nếu phần dư khác 0 thì phía nhận xác định xuất hiện lỗi, nếu không dữ liệu được chấp nhận là đúng.

Tất cả các tính toán trên CRC được thực hiện theo module 2 nhưng không nhớ trong phép cộng và không mượn trong phép trừ. Điều này có nghĩa là phép cộng giống phép trừ và cả hai tương đương với việc thực hiện phép XOR trên các toán hạng. Ví dụ:

1011 XOR 0101 =1110

1001 XOR 1101 =0100

Tương tự, chúng ta cũng có:

1011 - 0101 = 1110

1001 - 1101 = 0100

Phép nhân và phép chia cũng giống như thuật toán trên cơ số 2 nhưng các phép cộng và trừ đều không nhớ. Giống như khi thao tác trên các số nhị phân, phép nhân với $2^k$ là dịch sang trái k vị trí. Do vậy với D và R, kết quả $D*2^r$ XOR R là d+r bit minh họa trên Hình 5.7. Chúng ta sẽ sử dụng các đặc điểm đại số của mẫu d+r bit này trong phần trình bày dưới đây.

Vấn đề quan trọng là làm sao bên gửi xác định được R. Chúng ta muốn xác định R sao cho tồn tại n thỏa mãn:

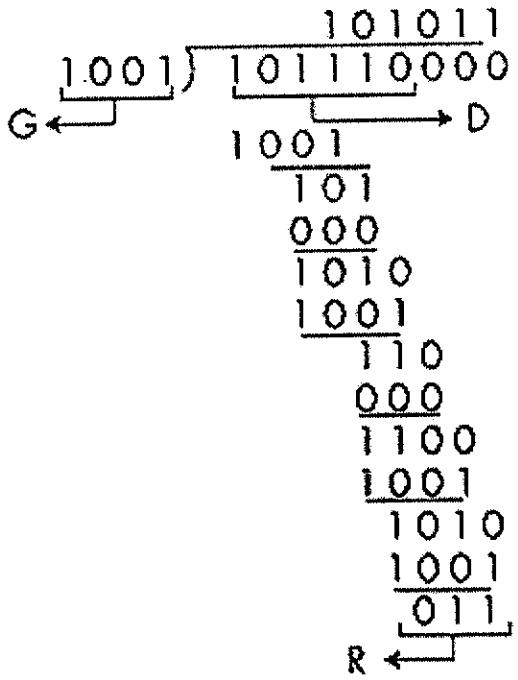
$$D * 2^r \text{ XOR } R = nG$$

Nghĩa là, chúng ta muốn chọn R sao cho G chia cho $D*2^r$ XOR R không có số dư. Nếu chúng ta thực hiện phép XOR R (là phép cộng theo module 2 không nhớ) cả hai vế của phương trình trên, chúng ta nhận được:

$$D * 2^r = nG \text{ XOR } R$$

Đẳng thức này cho chúng ta biết nếu chúng ta chia $D*2^r$ cho G, giá trị phần dư chính là R. Nói cách khác, có thể xác định R như sau:

$$R = \text{số dư } D * 2^r / G$$




**Hình 5.8 Ví dụ tính toán CRC**

Hình 5.8 minh hoạ kết quả tính toán cho trường hợp D=101110, d=6, G=1001, r=3. Chín bit được truyền trong trường hợp này là 101110 011.



Các chuẩn quốc tế định nghĩa các đa thức sinh (G) 8, 12, 16, 32 bit. CRC 8 bit được sử dụng trong 5 byte tiêu đề của tế bào ATM. CRC-32 trong nhiều giao thức sử dụng đa thức sinh sau:

$$G_{CRC-32} = 100000100110000010001110110110111$$

Các chuẩn CRC có thể phát hiện lỗi cụm với độ lớn nhỏ hơn r+1 bit hay số các bit bị lỗi là một số lẻ. Hơn nữa với một số giả định nào đó, lỗi cụm lớn hơn r+1 bit có thể được phát hiện với xác suất $1-0.5^r$. Lí thuyết mã CRC và thậm chí những mã có tính năng mạnh hơn vượt quá phạm vi của cuốn sách này.

## 5.2.4 Sửa lỗi bằng mã Hamming

Với môi trường truyền có tỷ lệ lỗi thấp, thì phát hiện được lỗi và sau đó yêu cầu truyền lại sẽ đem lại hiệu quả cao hơn. Để hiểu nguyên nhân điều này, chúng ta xét ví dụ sau. Giả sử trên môi trường truyền các lỗi xuất hiện riêng lẻ và tỷ lệ lỗi là $10^{-6}$ bit. Để sửa được lỗi cho các khối dữ liệu 1000 bit, chúng ta phải cung cấp thêm 10 bit kiểm tra. Như vậy tổng số lượng bit dư thừa là 10000 bit. Còn nếu chỉ để phát hiện khối có lỗi hay không, trong mỗi khối chỉ cần thêm 1 bit chẵn lẻ, và khi phát hiện được lỗi thì phía nhận yêu cầu bên kia gửi lại (gửi thêm 1 khối 1001 bit), nên tổng lượng bit dư thừa chỉ là 2001 - nhỏ hơn rất nhiều so với 10000. Do đó trong môi trường kiểu này, phát hiện lỗi và yêu cầu truyền lại hiệu quả hơn là trực tiếp sửa được lỗi.

Các phương pháp sửa lỗi được sử dụng chủ yếu trên kênh truyền không dây – là môi trường có tỷ lệ lỗi rất cao so với môi trường cáp đồng trục hay cáp quang.

### Gửi lặp

Gửi lặp mỗi bit nhiều lần cũng là một cách thức để khắc phục lỗi. Giả sử với cách gửi lặp 3 lần, để gửi đi bit 1, phía gửi sẽ gửi đi "111". Nếu nhận được 3 bit không hoàn toàn giống nhau thì chắc chắn có lỗi. Nếu kênh truyền có độ tin cậy rất cao có thể đảm bảo tối đa 1 bit lỗi trong bộ ba mã hóa, thì khi nhận được bộ "001", "010" hay "100" ta có thể xem chúng ứng

với bit 0; trong khi các bộ ba "110", "101" và "011" ứng với bit 1. Phương pháp mã hóa kiểu như trên cho phép phía nhận có thể khôi phục lại thông tin đúng, cho dù trên kênh truyền xảy ra lỗi – đây là khả năng sửa lỗi.

Tuy nhiên hiệu suất của phương pháp gửi lặp rất thấp do làm giảm băng thông đường truyền đi ba lần. Nếu số lần gửi lặp tăng (để có thể phát hiện và sửa được nhiều lỗi hơn) thì hiệu suất cũng giảm theo.

**Mã Hamming**

Nếu có nhiều bit sửa lỗi được đặt trong thông điệp và bố trí các bit này một cách hợp lý sao cho các vị trí bit lỗi khác nhau tạo ra những kết quả khác nhau thì chúng ta hoàn toàn xác định được các bit bị lỗi nằm ở đâu. Trong một thông điệp 7 bit, có thể có 7 vị trí có lỗi, do đó chỉ cần 3 bit để xác định thông điệp có lỗi hay không và nếu có thì vị trí của lỗi.

Hamming đã nghiên cứu các phương pháp mã hóa trước đó để tìm hiểu một khái niệm tổng quát. Ông bắt đầu với việc tính toán số bit dữ liệu và số bit dư thừa trong một thông điệp. Chẳng hạn với phương pháp bit chẵn lẻ, thông điệp là một ký tự ASCII 7 bit sẽ được mô tả là mã có dạng (8,7) nghĩa là trong 8 bit có 7 bit dữ liệu thực sự. Ví dụ trong phương pháp mã lặp nêu trên thì mã có dạng (3,1).

Hamming cũng chú ý đến vấn đề có nhiều bit bị lỗi, và đưa ra định nghĩa "khoảng cách"– sau này được gọi là khoảng cách Hamming để định nghĩa sự khác biệt giữa hai từ khóa. Mã chẵn lẻ có khoảng cách là 2 vì không thể phát hiện được 2 lỗi. Mã lặp (3,1) có khoảng cách là 3 vì nếu lỗi ở cả 3 bit thì kết quả là một từ mã hợp lệ khác (000 -> 111 hay 111 -> 000). Mã lặp (4,1) (mỗi bit được lặp 4 lần) có khoảng cách là 4, do đó hoàn toàn có thể phát hiện được tình huống có 2 bit trong từ bị lỗi.

Hamming quan tâm đến hai vấn đề: làm thế nào để tăng khoảng cách cho phương pháp mã nhưng giữ được lượng bit dư thừa thấp nhất có thể. Trong những năm 1940, ông đã đưa ra nhiều phương pháp khác nhau cải tiến các hệ mã hiện thời với ý tưởng chính là xen kẽ các bit chẵn lẻ sao cho chúng không chỉ kiểm soát dữ liệu mà còn kiểm soát lẫn nhau.

Ở đây chúng ta sẽ xét mã hóa Hamming (7,4) được đưa ra vào năm 1950. Cứ mỗi cụm 4 bit (D) trong thông điệp sẽ chèn thêm 3 bit kiểm tra chẵn lẻ (P). Phương pháp này sẽ sửa được bất kỳ lỗi 1 bit nào và có thể phát hiện tất cả lỗi 2 bit.



Giá trị mỗi bit kiểm tra phụ thuộc vào giá trị một số bit trong từ mã và chính vị trí của bit kiểm tra sẽ xác định nó phụ thuộc vào những bit nào.

Hình 5.9 minh họa cách xác định vị trí của bit kiểm tra và thuật toán tính những bit kiểm tra này.

Tất cả các bit ở vị trí là lũy thừa của 2 đều là bit kiểm tra (các bit ở vị trí 1,2,4,8..)

Tất cả các bit ở vị trí còn lại là dữ liệu thực sự cần gửi đi (các vị trí 3,5,6,7,9…

Vị trí 1: Bỏ qua 1 bit, kiểm tra 1 bit, bỏ qua 1 bit, kiểm tra 1 bit

Vị trí 2: Kiểm tra 1 bit, bỏ qua 2 bit, kiểm tra 2 bit, bỏ qua 2 bit, kiểm tra 2 bit

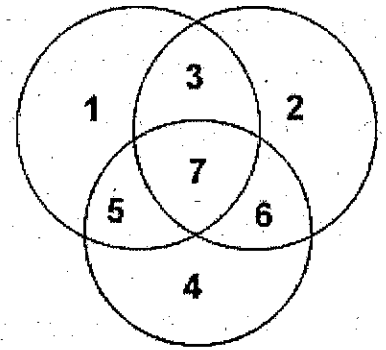
Vị trí 4: Kiểm tra 3 bit, bỏ qua 4 bit, kiểm tra 4 bit, bỏ qua 4 bit, kiểm tra 4 bit

Vị trí 8: Kiểm tra 7 bit, bỏ qua 8 bit, kiểm tra 8 bit, bỏ qua 8 bit, kiểm tra 8 bit

| 7 | 6 | 5 | 4 | 3 | 2 | 1 | |
|---|---|---|---|---|---|---|---|
| **D** | **D** | **D** | **P** | **D** | **P** | **P** | Từ mã 7 bit |
| D | - | D | - | D | - | P | Bit kiểm tra |
| D | D | - | - | D | P | - | Bit kiểm tra |
| D | D | D | P | - | - | - | Bit kiểm tra |

**Hình 5.9 Vị trí các bit kiểm tra và những bit nó kiểm soát**

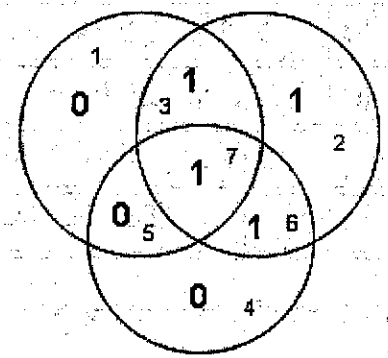
Chúng ta sẽ giải thích tại sao đặt bit kiểm tra vào các vị trí đó? Xét Hình 5.10, chúng ta thấy 3 bit kiểm tra (1,2,4) có liên quan đến các bit (3,5,6,7). Trong sơ đồ ven này, mỗi vòng tròn có một bit kiểm tra và 3 bit dữ liệu và tổng của 4 bit trong mỗi vòng tròn phải bằng 0. Với 4 bit dữ liệu, chúng ta có thể dễ dàng lựa chọn 3 bit kiểm tra thỏa mãn điều kiện này.




**Hình 5. 10 Quan hệ giữa bit kiểm tra và các bit dữ liệu**

Có thể chứng minh sự thay đổi của 1 trong 7 bit (1-7) sẽ làm thay đổi 3 bit kiểm tra một cách duy nhất. Ví dụ nếu bit 7 thay đổi thì cả 3 bit kiểm tra cũng thay đổi, nhưng nếu bit 6 thay đổi thì chỉ bit 2 và 4 mới thay đổi. Và nếu chính bit kiểm tra thay đổi thì chỉ có duy nhất bit này bị thay đổi, các bit còn lại không bị ảnh hưởng gì. Như vậy có thể dễ dàng xác định trực tiếp vị trí bit bị lỗi bằng cách kiểm tra ba vòng tròn.

Sự ảnh hưởng của lỗi duy nhất đến 3 bit kiểm tra phụ thuộc vào vị trí bit lỗi.




**Hình 5.11 Cách xác định lỗi dựa vào sơ đồ ven**

Giả sử bên gửi gửi chuỗi (1 1 0 0 1 1 0) và trên đường truyền, bit 5 bị lỗi (0 sang 1). Ở phía bên nhận, lỗi ở vị trí trên (bit 5) có thể được sửa bằng cách kiểm tra xem những bit kiểm tra nào bị tác động bởi bit lỗi.



Hình 5.12 minh họa điều này.

| 7 | 6 | 5 | 4 | 3 | 2 | 1 | | | |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 0 | 1 | 1 | 0 | Từ mã 7 bit | | |
| 1 | - | 1 | - | 1 | - | 0 | Tổng chẵn | **Sai !** | 1 |
| 1 | 1 | - | - | 1 | 1 | - | Tổng chẵn | **Đúng !** | 0 |
| 1 | 1 | 1 | 0 | - | - | - | Tổng chẵn | **Sai !** | 1 |

**Hình 5.12 Cách xác định vị trí bit bị lỗi**

Như vậy bit lỗi là 101 bằng 5. Qua ví dụ này, ta thấy bất kỳ lỗi nào cũng có thể được sửa bằng cách tương tự.

Mã Hamming tạo ra đúng 16 từ mã hợp lệ trong 128 từ có độ dài 7 bit có thể. 16 từ mã hợp lệ này được sắp xếp sao cho khoảng cách tối thiểu giữa 2 từ bất kỳ là 3 (Hình 5.13)

| | 7 6 5 4 3 2 1 | | 7 6 5 4 3 2 1 |
|---|---|---|---|
| 0 | 0 0 0 **0** 0 **0** 0 | 8 | 1 0 0 **1** 0 **1** 1 |
| 1 | 0 0 0 **0** 1 **1** 1 | 9 | 1 0 0 **1** 1 **0** 0 |
| 2 | 0 0 1 **1** 0 **0** 1 | A | 1 0 1 **0** 0 **1** 0 |
| 3 | 0 0 1 **1** 1 **1** 0 | B | 1 0 1 **0** 1 **0** 1 |
| 4 | 0 1 0 **1** 0 **1** 0 | C | 1 1 0 **0** 0 **0** 1 |
| 5 | 0 1 0 **1** 1 **0** 1 | D | 1 1 0 **0** 1 **1** 0 |
| 6 | 0 1 1 **0** 0 **1** 1 | E | 1 1 1 **1** 0 **0** 0 |
| 7 | 0 1 1 **0** 1 **0** 0 | F | 1 1 1 **1** 1 **1** 1 |

**Hình 5.13 Các từ mã Hamming hợp lệ**

## 5.3. GIAO THỨC ĐA TRUY CẬP VÀ MẠNG CỤC BỘ

Trong phần mở đầu của chương, chúng ta đã thấy rằng có hai kiểu kết nối mạng: kiểu truyền điểm nối điểm (point-to-point) và kiểu truyền

quảng bá (broadcast). Trên đường truyền điểm nối điểm có duy nhất một bên gửi và một bên nhận. Nhiều giao thức tầng liên kết dữ liệu được thiết kế cho đường truyền điểm nối điểm như PPP (Point-to-Point Protocol) và HDLC. Kiểu truyền thứ hai - kiểu quảng bá cho phép có nhiều nút gửi và nút nhận cùng kết nối đến kênh truyền dùng chung duy nhất. Khi bất kỳ nút nào đó truyền đi một frame, kênh truyền sẽ quảng bá frame này và tất cả các nút khác đều nhận được bản sao của frame. Ethernet - công nghệ quảng bá được sử dụng rộng rãi nhất - sẽ được nghiên cứu chi tiết trong phần 5.5. Trong phần này, chúng ta sẽ nghiên cứu một trong những vấn đề quan trọng nhất của tầng liên kết dữ liệu: làm thế nào để điều phối việc truy cập vào kênh truyền chung của nhiều nút - vấn đề **đa truy cập (multiple access problem)**. Kênh truyền quảng bá thường được sử dụng trên mạng cục bộ - là mạng giới hạn trong một khu vực địa lý.

Chúng ta đã quá quen thuộc với công nghệ quảng bá trong hệ thống phát thanh truyền hình. Nhưng hệ thống này chỉ phát quảng bá một chiều (nghĩa là một nút cố định – là ăngten - truyền dữ liệu đến nhiều nút nhận), trong khi các nút trên kênh truyền quảng bá trong mạng máy tính có thể vừa gửi vừa nhận. Có thể xét ví dụ tương tự trong một bữa tiệc, mọi người cùng nhau tụ họp trong một đại sảnh (không khí cung cấp môi trường quảng bá) để nói chuyện với nhau. Ví dụ thứ hai là lớp học - nơi giáo viên và sinh viên cùng nhau chia sẻ môi trường quảng bá duy nhất.Vấn đề chính trong cả hai trường hợp này là việc quyết định ai sẽ là người được nói (nghĩa là được truyền trên kênh truyền). Với con người, chúng ta đã có những quy tắc giao tiếp theo phép lịch sự để chia sẻ kênh truyền chung:

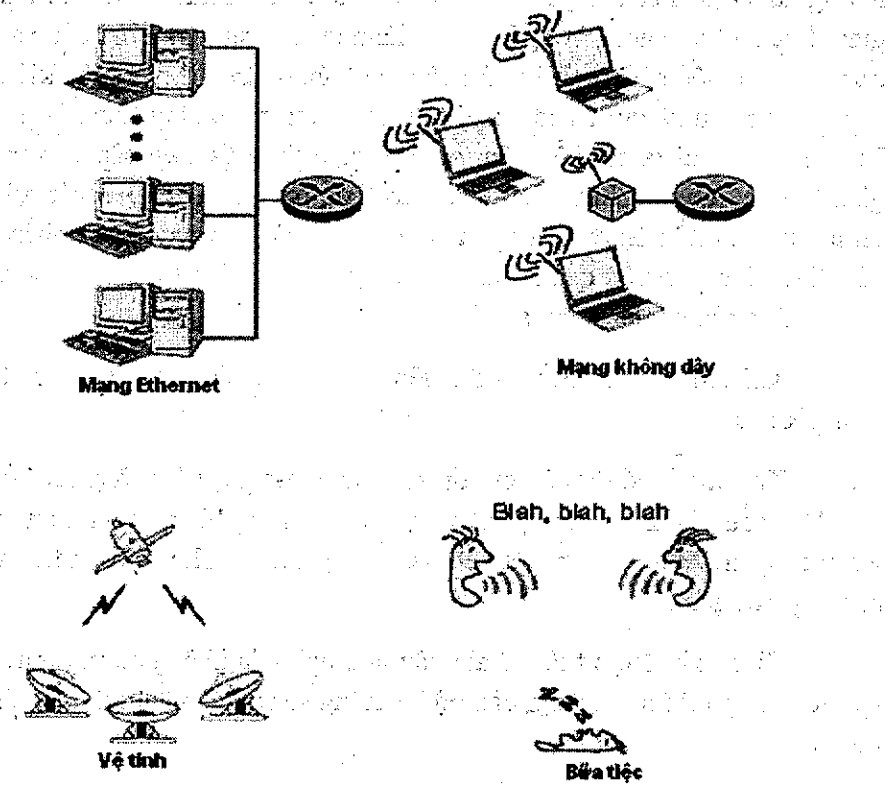
"Mỗi người đều có cơ hội nói"
"Im lặng cho đến khi bạn được quyền nói"
"Không được quyền nói suốt"
"Giơ tay yêu cầu nếu muốn nói"
"Đừng ngắt lời ai đó đang nói "
"Đừng ngủ khi ai đó đang nói"

Tương tự như vậy, mạng máy tính cũng có những giao thức - gọi là giao thức đa truy cập **(multiple access protocol)** – cho phép các nút điều chỉnh việc truyền thông của mình trên kênh truyền quảng bá dùng chung. Như minh họa trên Hình 5.14, giao thức đa truy cập rất cần thiết trong nhiều kiểu môi trường mạng: mạng không dây, mạng có dây và mạng vệ tinh.

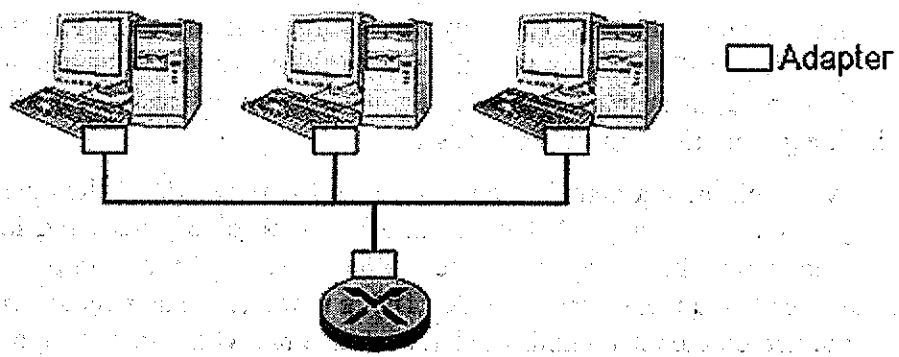


Hình 5.15 là ví dụ một kênh truyền quảng bá chia sẻ kênh truyền ùng chung. Mặc dù mỗi máy tính truy cập kênh truyền qua adapter, trong hần này chúng ta sẽ xem máy tính như một nút đóng vai trò vừa nhận lẫn ửi. Trên thực tế, hàng trăm hoặc thậm chí hàng nghìn nút có thể trực tiếp uyền thông trên một kênh truyền quảng bá.

Vì tất cả các nút đều có khả năng truyền frame nên rất có thể nhiều út truyền frame tại cùng một thời điểm. Khi đó, tất cả các nút cùng lúc hận được nhiều frame, nghĩa là các frame được truyền sẽ **xung đột collide)** với nhau tại tất cả các nút nhận. Thông thường khi xung đột xảy ra, hông nút nào có thể nhận chính xác bất kỳ frame nào vì tín hiệu trong các ame đan xen vào nhau hoàn toàn. Vì thế tất cả các frame liên quan đến ung đột đều bị mất, và có thể coi kênh truyền dùng chung không được sử ng trong khoảng thời gian xảy ra xung đột. Rõ ràng khi nhiều nút thường uyên muốn truyền frame, xác suất xảy ra xung đột sẽ tăng và phần lớn ăng thông của kênh truyền bị lãng phí.




**Hình 5.14 Chia sẻ kênh truyền dùng chung**




Hình 5.15 Mạng Ethernet quảng bá

Để bảo đảm hiệu suất của kênh truyền quảng bá đạt giá trị tối đa khi nhiều nút muốn gửi dữ liệu, bằng cách nào đó phải có cơ chế phối hợp giữa những nút có nhu cầu truyền. Cơ chế phối hợp này chính là trách nhiệm của giao thức đa truy cập. Trong ba mươi năm qua, hàng nghìn bài báo và hàng trăm luận án tiến sĩ đã nghiên cứu về giao thức đa truy cập. Nhiều kiểu giao thức khác nhau đã được triển khai trên các công nghệ tầng liên kết dữ liệu. Tuy nhiên người ta có thể phân loại các giao thức đa truy cập vào ba lớp: giao thức **phân chia kênh truyền**, giao thức **truy cập ngẫu nhiên** và giao thức **truy cập lần lượt**. Chúng ta sẽ xem xét các lớp này trong phần dưới đây. Trên kênh truyền quảng bá với tốc độ R b/s, giao thức đa truy cập lý tưởng sẽ có những đặc điểm sau:

Khi chỉ có một nút có dữ liệu gửi đi, nút đó được gửi với thông lượng R bps.

Khi M nút có dữ liệu gửi đi, mỗi nút được gửi với thông lượng R/M bps. Yêu cầu này không có nghĩa rằng mỗi nút trong M nút luôn luôn truyền với tốc độ tức thời R/M mà đây chỉ là tốc độ trung bình xác định trong một khoảng thời gian.

Giao thức được triển khai phân tán, nghĩa là không có một nút đóng vai trò điều phối (nếu không toàn bộ hệ thống sẽ sụp đổ nếu nút điều phối bị hỏng).

Giao thức phải đơn giản để chi phí cài đặt không cao.

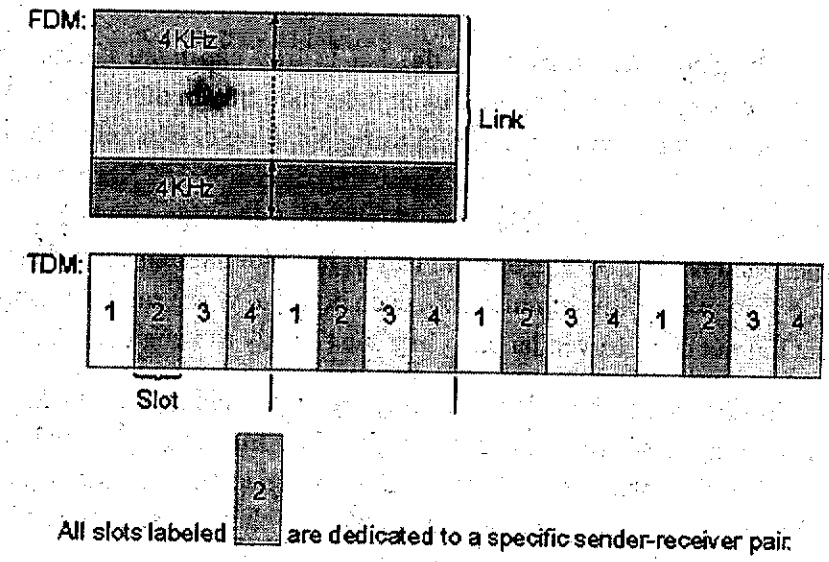


## 5.3.1 Giao thức phân chia kênh truyền (channel partitioning)

Phân kênh theo thời gian (TDM) và theo tần số (FDM) là hai kỹ thuật có thể được sử dụng để phân chia băng thông kênh truyền cho các nút tham gia truyền thông. Giả sử kênh truyền có N nút và tốc độ truyền của kênh là Rbps. TMD chia thời gian thành các khoảng (time frame) (độc lập với đơn vị dữ liệu frame ở tầng data-link) và sau đó lại chia mỗi khoảng thời gian thành N khe thời gian (time slot). Mỗi khe thời gian được cấp phát cho một nút. Khi có dữ liệu cần gửi, nút truyền các bit dữ liệu của mình trong khe thời gian đã được cấp phát. Thường khoảng thời gian được chọn sao cho một frame dữ liệu có thể truyền trọn vẹn trong một khe thời gian.

Hình 5.16minh hoạ TDM đơn giản cho 4 nút. Trong bữa tiệc điều này tương tự như quy định mỗi người chỉ được nói trong từng khoảng thời gian quy định. Vì thế ai cũng có cơ hội để nói.

Ưu điểm chính của TDM là loại trừ xung đột và đảm bảo công bằng: mỗi nút có được tốc độ truyền riêng R/N bps trong mỗi khoảng thời gian. Tuy nhiên, xuất hiện hai nhược điểm: tốc độ truyền trung bình của mỗi nút bị giới hạn R/N bps và nút chỉ được truyền trong khoảng thời gian của mình ngay cả khi nó là nút duy nhất có nhu cầu gửi. (Trong ví dụ bữa tiệc của chúng ta mọi người đều muốn nghe một vị khách nào đó nói thì vị khách đó chỉ được nói trong khoảng thời gian được cấp phát của mình). Rõ ràng, TDM không phải là một giao thức đa truy cập tốt cho bữa tiệc kiểu này.




Hình 5.16 Ví dụ TDM cho 4 nút

Nếu TDM chia kênh truyền theo thời gian thì FDM chia kênh truyền R bps ra các tần số khác nhau (mỗi tần số có băng thông R/N) và mỗi nút được cấp phát một dải tần số. Vì thế, FDM tạo ra N kênh truyền nhỏ R/Nbps từ kênh truyền lớn R bps. Ưu nhược điểm của FDM giống TDM, tức là cũng loại bỏ được xung đột và phân chia công bằng dải tần giữa N nút. Tuy nhiên, nhược điểm là tốc độ gửi của nút bị giới hạn ngay cả khi chỉ có duy nhất một nút có nhu cầu gửi dữ liệu.

Giao thức phân chia kênh truyền thứ ba là **chia mã (CDMA – Code Division Multiple Access)**. Nếu TDM và FDM cấp phát khoảng thời gian và tần số cho các nút thì CDMA cấp phát cho mỗi nút một mã khác nhau. Sau đó nút sử dụng mã duy nhất này để mã hoá dữ liệu gửi đi. CDMA cho phép nhiều nút gửi đồng thời và các nút nhận tương ứng nhận đúng dữ liệu gửi cho mình (miễn là nó biết được mã của nút gửi). CDMA đã được sử dụng trong hệ thống quốc phòng nhờ đặc tính chống nhiễu và bây giờ bắt đầu được áp dụng phổ biến cho mục đích dân sự, đặc biệt trong đa truy cập kênh truyền không dây.

## 5.3.2 Giao thức truy cập ngẫu nhiên (random access)

Kiểu giao thức đa truy cập thứ hai là truy cập ngẫu nhiên. Trong giao thức truy cập ngẫu nhiên, nút truyền luôn luôn truyền dữ liệu với tốc độ cao nhất của kênh truyền R bps. Khi có xung đột, các nút liên quan đến xung đột sẽ truyền lại frame cho đến khi frame đến đích an toàn. Nhưng khi biết có xung đột, nút không cần thiết truyền lại frame ngay lập tức, mà đợi một thời gian ngẫu nhiên nào đó trước khi truyền lại. Mỗi nút liên quan đến xung đột chọn thời gian đợi ngẫu nhiên một cách độc lập, vì thế sau mỗi xung đột xác suất hai nút cùng truyền lại cùng một lúc (lại xảy ra xung đột) sẽ giảm.

Có đến hàng trăm giao thức truy cập ngẫu nhiên, tuy nhiên trong phần này chúng ta sẽ trình bầy một vài giao thức truy cập ngẫu nhiên được sử dụng phổ biến nhất - giao thức ALOHA và giao thức đa truy cập cảm nhận sóng mang (CSMA). Sau đó, trong phần 5.5 chúng ta sẽ nghiên cứu chi tiết về Ethernet - công nghệ sử dụng CSMA cực kỳ phổ biến.



### *Slotted ALOHA*

Chúng ta bắt đầu nghiên cứu một trong số những giao thức đa truy cập đơn giản nhất: slotted ALOHA. Chúng ta giả định như sau:

- Tất cả frame có chính xác L bit.

- Thời gian được chia thành các khoảng L/R s (phải là khoảng thời gian đủ để truyền một frame).

- Nút bắt đầu truyền frame tại đầu mỗi khoảng thời gian.

- Tất cả các nút được đồng bộ hoá sao cho mỗi nút đều xác định được khi nào là đầu của khoảng thời gian.

- Nếu có nhiều frame xung đột trong khoảng thời gian nào đó thì tất cả các nút đều phát hiện sự kiện xung đột ngay trong khoảng thời gian đó.

Gọi p là xác suất ($0 \le p \le 1$). Hoạt động của slotted ALOHA trong mỗi nút như sau:

- Khi có frame mới cần gửi, nút sẽ đợi đến thời điểm đầu của khoảng thời gian kế tiếp và gửi toàn bộ frame trong khoảng thời gian đó.

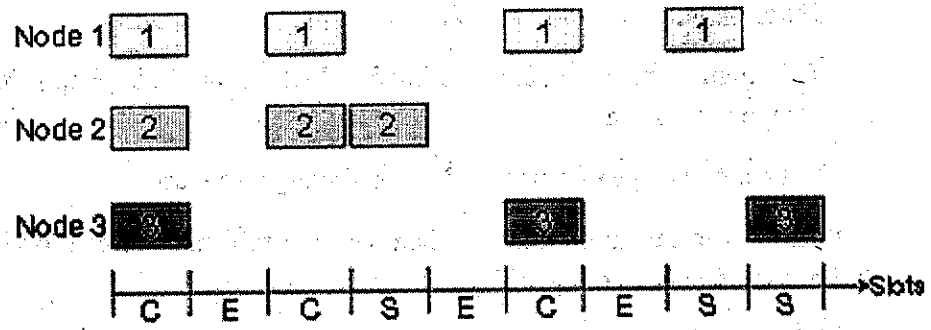
- Nếu không xảy ra xung đột, nút truyền thành công frame và vì vậy không cần thiết phải truyền lại (nút có thể chuẩn bị frame mới để truyền, nếu có).

- Nếu có xung đột, nút phát hiện xung đột ngay trong khoảng thời gian và sẽ truyền lại frame trong khoảng thời gian tiếp theo với xác suất p cho đến khi frame được truyền thành công.

Truyền lại với xác suất p giống như việc tung đồng xung: biến cố mặt ngửa ứng với việc truyền lại xảy ra với xác suất p. Biến cố mặt sấp ứng với việc "bỏ qua khoảng thời gian này và tung lại đồng xu trong khoảng thời gian kế tiếp" xảy ra với xác suất (1- p). Mỗi nút liên quan đến xung đột tung đồng xu độc lập với nhau.

Slotted ALOHA có nhiều ưu điểm. Không giống phân chia kênh truyền, nút tích cực duy nhất (nghĩa là nút có nhu cầu gửi dữ liệu) liên tục gửi frame ở tốc độ cao nhất của kênh truyền. Slotted ALOHA là một thuật

toán phân tán vì mỗi nút khi phát hiện ra xung đột sẽ quyết định khi nào truyền lại một cách độc lập. (Tuy nhiên slotted ALOHA đòi hỏi phải có cơ chế đồng bộ trên tất cả các nút).




**Hình 5.17 Ví dụ giao thức Slotted ALOHA**

Slotted ALOHA hoạt động tốt khi chỉ có một nút ở trạng thái tích cực, nhưng hiệu suất của nó bằng bao nhiêu khi có nhiều nút tích cực? Có hai yếu tố phải tính đến ở đây. Thứ nhất như trong Hình 5.17 khi có nhiều nút ở trạng thái tích cực sẽ xuất hiện nhiều khoảng thời gian xung đột và do đó kênh truyền bị lãng phí. Thứ hai sẽ có một số khoảng thời gian "rỗng" vì trong khoảng thời gian này tất cả các nút tích cực đều dừng lại đợi (kết quả của chính sách truyền theo xác suất). Chỉ trong những những khoảng thời gian "không bị lãng phí" sẽ có duy nhất một nút truyền thành công. Khoảng thời gian này gọi là khoảng thời gian thành công. Hiệu suất của giao thức được định nghĩa là tỷ lệ các khoảng thời gian truyền thành công trong trường hợp có nhiều nút tích cực, mỗi nút cần gửi đi nhiều frame. Rõ ràng rằng nếu không có cơ chế điều khiển truy cập và nút truyền lại ngay sau mỗi lần xung đột, hiệu suất sẽ bằng 0. Slotted ALOHA có hiệu suất lớn hơn 0 nhưng bằng bao nhiêu?

Bây giờ ta sẽ xác định hiệu suất tối đa của slotted ALOHA. Để đơn giản chúng ta thay đổi giao thức một chút và giả thiết rằng mỗi nút truyền frame trong mỗi khoảng thời gian với xác suất p (tức là mỗi nút luôn có một frame để gửi đi và frame này được gửi đi với xác suất p cho dù đây là frame mới hay frame phải gửi lại). Đầu tiên giả sử có N nút. Xác suất thành công của một khoảng thời gian nào đó là xác suất chỉ có một nút duy nhất truyền



và N-1 nút còn lại không truyền. Xác suất một nút nào đó truyền là p; xác suất mà các nút còn lại không truyền là $(1- p)^{N-1}$. Do vậy xác suất để một nút nào đó truyền trong khi các nút khác không truyền là $p(1-p)^{N-1}$. Vì có N nút, nên xác suất để có khoảng thời gian thành công bằng $Np(1-p)^{N-1}$.

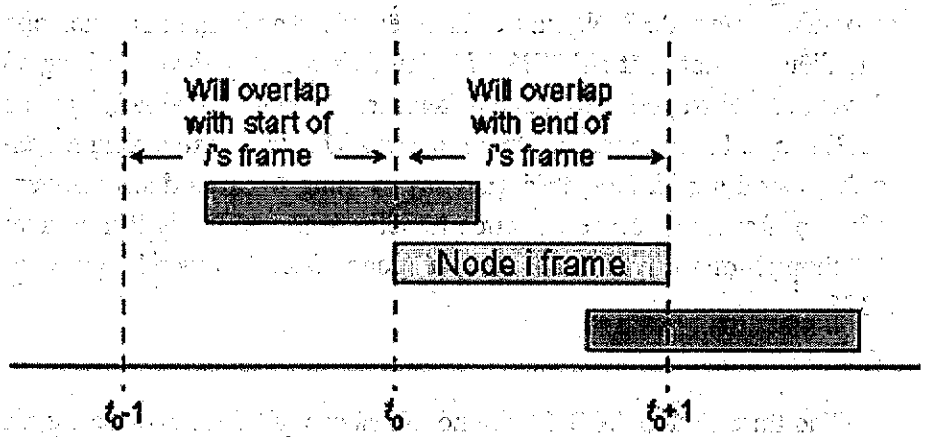
Do đó khi có N nút tích cực, hiệu suất của slotted ALOHA là $Np(1-p)^{N-1}$. Để đạt được hiệu suất lớn nhất, chúng ta phải xác định $p^*$ sao cho biểu thức này đạt giá trị lớn nhất. Và để đạt được hiệu suất lớn nhất khi có nhiều nút tích cực, chúng ta phải tính giới hạn của $Np^*(1-p^*)^{N-1}$ khi N tiến tới vô cùng. Áp dụng các công cụ toán học, chúng ta sẽ xác định được hiệu suất lớn nhất của giao thức là $1/e = 0.37$. Nghĩa là, khi nhiều nút cùng ở trạng thái tích cực thì trong điều kiện tốt nhất chỉ 37% thời gian đường truyền được sử dụng có ích. Vì vậy, tốc độ truyền hiệu quả của kênh truyền không phải là R bps mà chỉ là 0,37R bps. Phân tích tương tự chỉ ra rằng 37% thời gian đường truyền không được sử dụng và 26% thời gian xảy ra xung đột trên đường truyền. Như vậy một frame nào đó có thể được truyền với tốc độ tối đa R nhưng về tổng thể thông lượng truyền thành công của toàn bộ kênh truyền không vượt qua 0.37R.

***ALOHA***

Giao thức slotted ALOHA đòi hỏi tất cả các nút đồng bộ việc truyền tại đầu mỗi khoảng thời gian. Giao thức ALOHA đầu tiên thực sự là giao thức không chia khoảng thời gian, hoàn toàn phân tán. Trong giao thức này, khi có dữ liệu cần gửi đi, ngay lập tức nút truyền toàn bộ frame vào kênh truyền dùng chung. Nếu frame được truyền xung đột với frame từ các nút khác, thì ngay sau khi truyền cho xong frame, nút sẽ ngay lập tức truyền lại frame với xác suất p. Ngược lại nút đợi trong một khoảng thời gian truyền frame. Sau quá trình chờ đợi, nút truyền frame với xác suất là p, hoặc đợi (không làm gì cả) trong khoảng thời gian truyền frame với xác suất (1-p).

Để xác định được hiệu suất cực đại của ALOHA xét trên một nút duy nhất, chúng ta cũng giả định như trong trường hợp slotted ALOHA thời gian truyền frame là một đơn vị thời gian. Tại bất kì thời gian nào, xác suất để nút truyền frame là p. Giả sử frame này bắt đầu truyền tại thời điểm $t_0$. Như minh họa trong Hình 5.18, để frame này được truyền thành công thì không nút nào được bắt đầu truyền trong khoảng thời gian $[t_0 - 1, t_0]$. Nếu

không tín hiệu của những frame này sẽ xung đột với các tín hiệu đầu tiên của frame đang xét. Xác suất để tất cả các nút khác không được bắt đầu truyền trong khoảng thời gian này là $(1-p)^{N-1}$. Tương tự không nút nào được bắt đầu truyền trong khi nút đang xét đang truyền. Xác suất của điều này cũng là $(1-p)^{N-1}$. Vì vậy xác suất nút nào đó truyền thành công là $p(1-p)^{2(N-1)}$. Bằng cách lấy giới hạn như trong trường hợp slotted ALOHA, chúng ta thấy rằng hiệu suất lớn nhất của giao thức ALOHA là 1/2e - bằng một nửa của slotted ALOHA. Đây là cái giá phải trả cho giao thức ALOHA hoàn toàn phân tán.




**Hình 5.18 Các frame đan xen vào nhau trong ALOHA**

### *CSMA - Đa truy cập cảm nhận sóng mang*

Trong cả hai giao thức ALOHA và slotted ALOHA, quyết định truyền của nút được đưa ra độc lập với các nút khác. Cụ thể hơn, một nút không để ý tới việc liệu có nút khác đang truyền khi nó bắt đầu truyền hay không và nút cứ truyền kể cả khi có nút khác truyền (gây xung đột). Tương tự trong ví dụ buổi tiệc, giao thức ALOHA giống như hành vi của vị khách bất lịch sự cứ liên tục nói bất chấp việc có người đang nói hay không. Xã hội loài người có những quy tắc ứng xử cho phép xử sự một cách lịch sự và làm giảm "xung đột" giữa nhiều người nói chuyện. Đặc biệt, có hai quy tắc quan trọng cho một cuộc đối thoại của người lịch sự:

**Nghe trước khi nói**: nếu có ai đang nói, hãy đợi đến khi họ nói xong. Trong mạng máy tính, điều này được gọi là **cảm nhận sóng mang (carrier sense)** - nút lắng nghe kênh truyền trước khi truyền. Nếu có frame đang được truyền trên kênh truyền thì nút sẽ chờ (backs off) một khoảng thời gian ngẫu nhiên và lại tiếp tục lắng nghe kênh truyền. Lúc này nếu kênh truyền được cảm nhận là rỗi thì nút bắt đầu việc truyền frame. Trong trường hợp ngược lại, nút lại đợi một khoảng thời gian ngẫu nhiên khác và lặp lại quá trình này.

**Nếu có ai đó bắt đầu nói cùng lúc thì hãy tạm ngừng (Nghe trong khi nói)**: Trong mạng máy tính điều này được gọi là **phát hiện xung đột (collision detection)** - nút đang truyền vẫn phải tiếp tục lắng nghe kênh truyền trong khi đang truyền. Nếu phát hiện có nút khác truyền xen vào, nút sẽ dừng truyền và sử dụng giao thức nào đó để quyết định khi nào nên thử truyền tiếp.

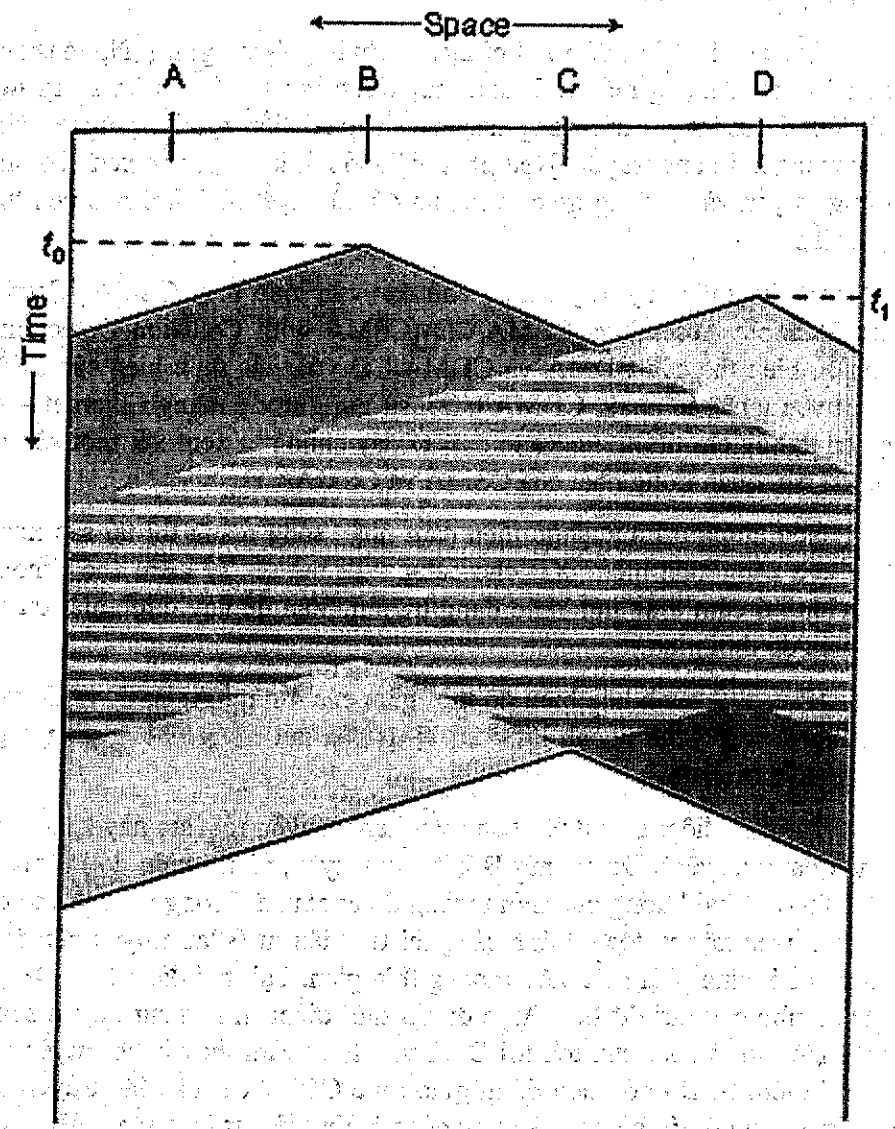
Hai quy tắc này là ý tưởng chủ đạo của giao thức CSMA (Carrier Sense Multiple Access) và CSMA/CD (CSMA with Collision Detection). Có nhiều biến thể của CDMA và CDMA/CD với việc thực hiện các chiến lược truyền lại khác nhau. CDMA/CD - sử dụng trong mạng Ethernet – sẽ được trình bày chi tiết trong phần 5.5. Ở đây chúng ta xem xét một số đặc trưng cơ bản quan trọng nhất của CSMA và CSMA/CD.

Nếu tất cả các nút thực hiện cảm nhận sóng mang thì tại sao xung đột có khả năng xuất hiện? Xét cho cùng, một nút sẽ "tự kiềm chế" không truyền khi nó cảm thấy nút khác đang truyền. Vấn đề này được giải quyết bằng biểu đồ thời gian.

Hình 519 minh họa biểu đồ thời gian của 4 nút ( A, B, C, và D) với bus dùng chung. Trục hoành biểu thị vị trí của nút trong không gian, trục tung mô tả thời gian.

Tại thời điểm $t_0$, nút B nhận thấy kênh truyền rỗi (lúc này không có nút nào đang truyền). Do đó nút B bắt đầu truyền, và tín hiệu do B truyền lan tỏa theo cả hai hướng của môi trường dùng chung. Trong thực tế cho dù vận tốc truyền xấp xỉ tốc độ ánh sáng thì tín hiệu từ B lan truyền đến một điểm nào đó cũng phải mất một khoảng thời gian. Tại thời điểm $t_1$ ( $t_1 > t_0$ ) nút D có nhu cầu gửi dữ liệu. Mặc dù tại thời điểm $t_1$, B đang truyền song các tín hiệu từ B chưa lan tỏa tới D và vì vậy D cảm thấy kênh truyền rỗi vào thời điểm $t_1$. Do đó, theo đúng giao thức CDMA, D bắt đầu truyền dữ liệu. Ngay sau đó, tín hiệu từ B xung đột với tín hiệu từ D. Hiển nhiên rằng độ trễ lan tỏa (propagation delay) giữa hai đầu mút của kênh truyền dùng

chung - thời gian để tín hiệu lan truyền từ đầu này đến đầu kia kênh truyền đóng vai trò quyết định trong hiệu suất hoạt động của kênh truyền. Thời gian trễ này càng lớn, xác suất một nút không phát hiện được có nút khác đang truyền cũng càng lớn.

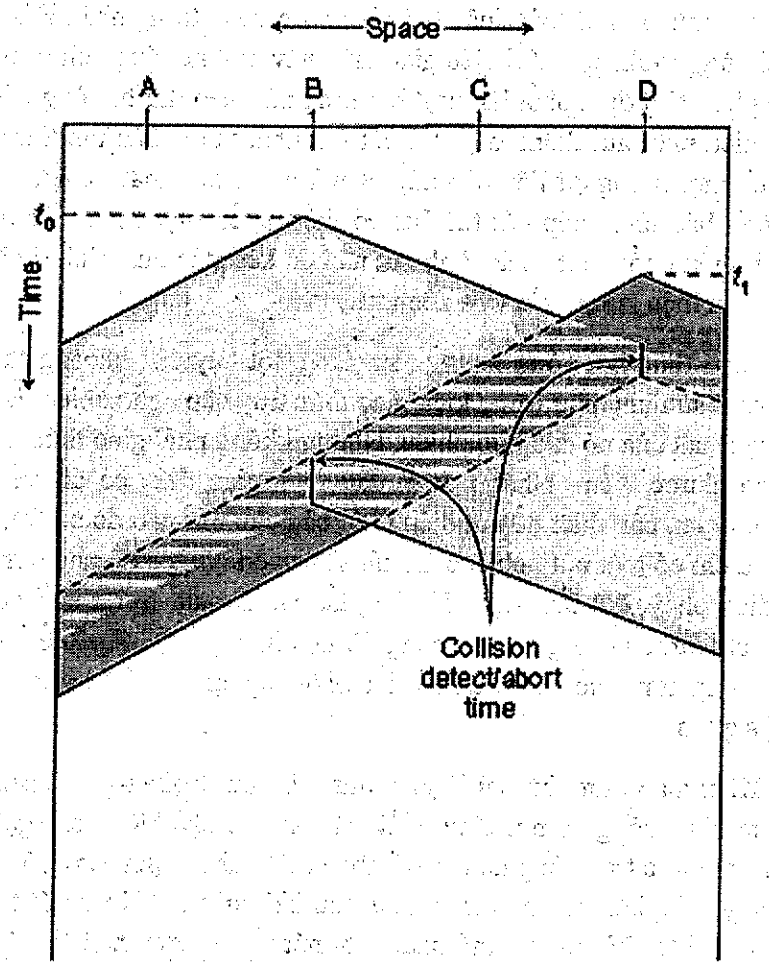



**Hình 5.19 Biểu đồ thời gian của 4 nút sử dụng CSMA**



Trong Hình 5.19 các nút không thực hiện phát hiện xung đột, cả nút B và D tiếp tục truyền toàn bộ frame ngay cả khi có xung đột. Nếu thực hiện công việc phát hiện xung đột, nút sẽ ngừng truyền ngay khi phát hiện xung đột.

Hình 5.20 tương tự như Hình 5.19 chỉ khác là cả hai nút ngừng truyền ngay sau khi phát hiện có xung đột. Rõ ràng đưa khả năng phát hiện xung đột vào giao thức đa truy cập sẽ làm tăng hiệu suất của giao thức do các nút không cố gắng tiếp tục gửi frame đã bị lỗi. Giao thức Ethernet chúng ta sẽ nghiên cứu trong phần 5.5 là giao thức CSMA có phát hiện xung đột.




**Hình 5.20 CSMA có phát hiện xung đột**

### 5.3.3 Giao thức truy cập lần lượt (Taking – turns)

Hai tính chất mà tất cả các giao thức đa truy cập muốn có là (1) khi chỉ có một nút tích cực, nút này có thể chiếm toàn bộ đường truyền nghĩa là truyền với băng thông tối đa R bps và (2) khi M nút tích cực, mỗi nút có băng thông trung bình R/M bps.

Giao thức ALOHA và CSMA có tính chất đầu tiên nhưng không có tính chất thứ hai. Điều này đã thúc đẩy các nhà nghiên cứu xây dựng một lớp các giao thức khác – kiểu lần lượt. Giống như kiểu truy cập ngẫu nhiên, có rất nhiều giao thức kiểu lần lượt, và mỗi giao thức này lại có nhiều biến thể. Ở đây, chúng ta sẽ thảo luận hai giao thức quan trọng nhất. Đầu tiên là **kiểu hỏi vòng (polling)**. Với kiểu giao thức này một nút được chọn đóng vai trò điều phối. Nút điều phối lần lượt hỏi từng nút theo thứ tự vòng tròn. Đầu tiên nút điều phối gửi thông điệp tới nút thứ nhất thông báo nút thứ nhất có thể truyền một lượng dữ liệu nào đấy. Sau khi nút thứ nhất truyền, nút điều phối thông báo cho phép nút thứ hai có thể truyền một lượng dữ liệu nào đó... Nút điều phối có thể xác định nút nào đó kết thúc quá trình dữ liệu khi không có tín hiệu lan truyền trên kênh truyền.

Giao thức hỏi vòng loại trừ sự xung đột hay các khoảng thời gian không được sử dụng như trong kiểu giao thức truy cập ngẫu nhiên. Điều này khiến hiệu suất của nó cao hơn nhiều. Nhưng không phải giao thức hỏi vòng không có nhược điểm. Nhược điểm đầu tiên, giao thức có độ trễ vòng - lượng thời gian cần thiết để nút điều phối báo cho nút nào đó có thể truyền. Ví dụ nếu chỉ có một nút tích cực thì nút sẽ truyền với tốc độ nhỏ hơn R bps, vì nút điều phối phải lần lượt hỏi vòng tất cả các nút, trong mỗi vòng nút tích cực chỉ được phép gửi một lượng dữ liệu hạn chế. Nhược điểm thứ hai, nghiêm trọng hơn nhiều, là nếu nút điều phối gặp sự cố thì toàn bộ hệ thống cũng bị sụp đổ.

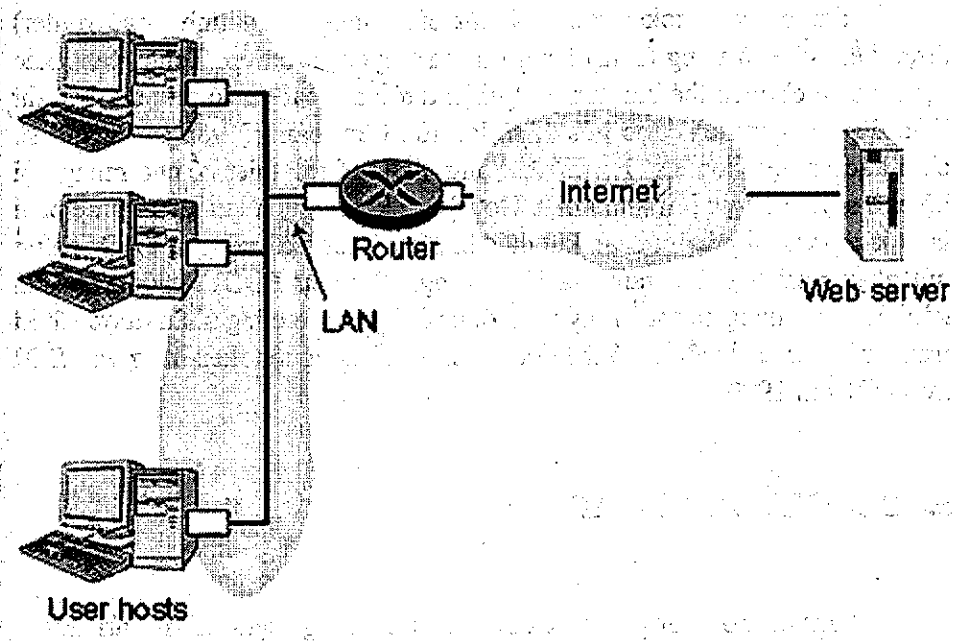
Kiểu giao thức thứ hai là giao thức **thẻ bài (token–passing)**. Trong giao thức này không có nút điều phối. Một frame đặc biệt được gọi là **thẻ bài (token)** được trao đổi giữa các nút theo một thứ tự định trước. Ví dụ, nút thứ nhất gửi thẻ bài tới nút thứ hai, nút thứ hai gửi thẻ bài tới nút thứ ba... nút thứ N gửi thẻ bài tới nút thứ nhất. Khi nút nhận được thẻ bài, nó chỉ giữ thẻ bài khi có dữ liệu cần truyền, nếu không nó sẽ ngay lập tức chuyển thẻ



bài tới nút kế tiếp. Nếu nút có frame để truyền, khi nhận được thẻ bài, nó gửi đi lượng dữ liệu được phép và sau đó chuyển thẻ bài tới nút kế tiếp. Giao thức thẻ bài được triển khai phân tán và có hiệu suất cao. Nhưng nó cũng có nhiều vấn đề cần giải quyết. Ví dụ, một nút gặp sự cố có thể làm toàn bộ hệ thống sụp đổ. Hoặc nếu một nút tình cờ không chuyển tiếp hay làm mất thẻ bài thì cần có cơ chế đưa thẻ bài mới vào lưu thông.

### 5.3.4 Mạng cục bộ LAN (Local Area Network)

Những giao thức đa truy cập được sử dụng trên nhiều loại kênh truyền quảng bá khác nhau. Chúng được sử dụng cho kênh truyền vệ tinh hay môi trường không dây (các nút truyền trên cùng một dải tần số).




**Hình 5.21 Máy tính người dùng truy cập máy dịch vụ Web Internet thông qua LAN. Kênh truyền quảng bá giữa máy tính người dùng và router gồm một "đường truyền"**

Mạng cục bộ LAN là mạng máy tính giới hạn trong một khu vực địa lý, ví dụ trong một toà nhà hoặc trong khuôn viên trường đại học. Thông

thường khi truy cập Internet từ trường đại học hay cơ quan, hầu hết mọi người truy cập thông qua mạng LAN. Khi đó máy tính của người dùng là một nút trong mạng LAN và mạng LAN cung cấp khả năng truy cập tới Internet thông qua router, như minh hoạ trong Hình 5.21. Mạng LAN là kênh truyền duy nhất giữa tất cả các máy tính và router; do đó nó cần tới giao thức tầng liên kết dữ liệu và giao thức đa truy cập. Tốc độ truyền R của hầu hết các mạng LAN rất cao. Tốc độ mạng LAN trước năm 1980 là 10Mbps, ngày nay là 100Mbps và trong tương lai sẽ là 1Gbps.

Vào những năm 80 và đầu những năm 90, có hai kiểu công nghệ mạng LAN phổ biến trên thị trường. Công nghệ thứ nhất là mạng cục bộ Ethernet (được biết đến là 802.3 LAN [IEEE 802.3) sử dụng giao thức truy cập ngẫu nhiên. Công nghệ thứ hai dựa trên công nghệ thẻ bài gồm công nghệ token–ring và FDDI. Công nghệ Ethernet được trình bày chi tiết trong phần 5.4 vì đây là công nghệ chủ đạo ngày nay.

Trong mạng token–ring, N nút của mạng (máy tính hoặc router) được kết nối vào vòng (ring) bằng đường truyền trực tiếp. Topo mạng xác định thứ tự chuyển thẻ bài. Khi nút nhận được thẻ bài và có nhu cầu gửi dữ liệu, dữ liệu (frame) được gửi đi sẽ lan tỏa trên toàn bộ vòng. Nút gửi sẽ chịu trách nhiệm loại bỏ frame trên vòng. FDDI được thiết kế cho mạng nội bộ cho một khu vực lớn (vài $km^2$). Do vậy sẽ không hiệu quả nếu frame phải lan tỏa ngược lại phía gửi sau khi đã đến đích. Trong công nghệ FDDI chính nút nhận phải loại bỏ frame ra khỏi vòng. (thực sự FDDI không phải là kênh truyền quảng bá thuần tuý vì không phải nút nào cũng nhận được bất kì frame nào được truyền). Có thể đọc thêm về công nghệ token–ring và FDDI trong [3Com 1999].

## 5.4 ĐỊA CHỈ LAN VÀ ARP

Như đã nói trong phần trước, các nút trong mạng LAN gửi frame cho nhau trên kênh truyền quảng bá dùng chung. Điều này nghĩa là khi một nút trong mạng LAN truyền frame, mọi nút khác kết nối tới mạng LAN đều có khả năng nhận được frame. Tuy nhiên mỗi nút trong mạng LAN không muốn gửi frame tới tất cả các nút khác mà chỉ muốn gửi tới một nút cụ thể nào đó trong mạng LAN. Để thực hiện điều này, các nút trong mạng LAN

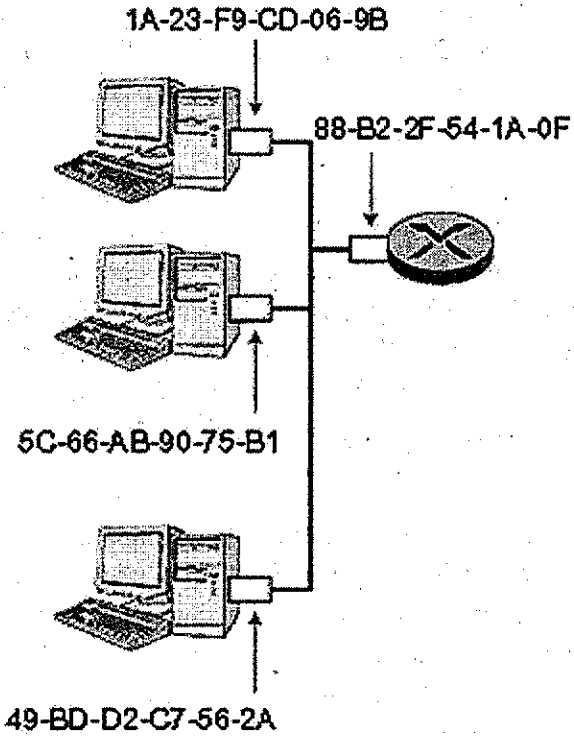


phải có khả năng xác định địa chỉ của nhau khi gửi frame, nghĩa là mỗi nút cần có một địa chỉ trong mạng LAN và trong gói tin tầng liên kết dữ liệu (frame) cần có trường chứa địa chỉ nút đích. Như vậy khi nhận được frame, nút có thể xác định liệu frame đó có phải gửi cho mình không.

Nếu địa chỉ đích của frame trùng với địa chỉ LAN của mình, nút nhận sẽ lấy gói dữ liệu tầng mạng từ frame tầng liên kết dữ liệu và chuyển gói dữ liệu này lên tầng mạng phía trên.

Nếu địa chỉ đích không trùng với địa chỉ nút nhận, đơn giản nút sẽ loại bỏ frame nhận được.

### 5.4.1 Địa chỉ LAN




**Hình 5.22 Mỗi adapter có một địa chỉ LAN duy nhất**

Thực sự, không phải nút (máy tính) có địa chỉ LAN mà chính adapter mới có địa chỉ LAN. Điều này được minh hoạ trong Hình 5.22. Địa chỉ LAN có nhiều tên gọi khác nhau: địa chỉ vật lý (physical address), địa chỉ Ethernet, địa chỉ MAC (media access control). Với hầu hết các mạng LAN (kể cả mạng Ethernet và thẻ bài), địa chỉ LAN có độ dài 6 byte (có thể có $2^{48}$ địa chỉ). 6 byte địa chỉ này được biểu diễn dưới dạng thập lục phân, mỗi byte ứng với một cặp số thập lục phân. Địa chỉ mạng LAN của adapter mang giá trị cố định, được ghi cứng vào ROM của adapter trong quá trình sản xuất.

Một điểm thú vị là hai adapter bất kỳ có địa chỉ LAN khác nhau. Thoạt tiên điều này dường như khó có thể thực hiện được vì nhiều công ty khác nhau có thể sản xuất adapter. Làm thế nào để địa chỉ adapter sản xuất ở Đài Loan khác với địa chỉ adapter sản xuất tại Bỉ? Điều này có được là do IEEE quản lý không gian địa chỉ vật lý. Khi muốn sản xuất adapter, công ty phải mua một phần không gian địa chỉ gồm $2^{24}$ địa chỉ với một mức phí nào đó. IEEE cấp từng khối $2^{24}$ địa chỉ bằng cách cố định 24 bit đầu của địa chỉ vật lí và công ty có thể tùy ý gán 24 bit sau cho bất kỳ sản phẩm nào của mình.

Địa chỉ vật lý của adapter có cấu trúc phẳng (đối lập với cấu trúc phân cấp) và không thay đổi cho dù có mang adapter đi đâu chăng nữa. Mỗi máy tính xách tay với một card Ethernet luôn có cùng một địa chỉ vật lý cho dù ở bất kỳ ở đâu. Điều này ngược với địa chỉ IP có cấu trúc phân cấp (gồm địa chỉ mạng và địa chỉ máy tính). Địa chỉ IP của nút sẽ thay đổi khi chuyển sang mạng khác. Địa chỉ vật lý của adapter giống như số chứng minh thư nhân dân của một người – không phân cấp và luôn luôn không thay đổi bất kể người đó ở đâu.

Như đã nói, khi adapter muốn gửi frame đến adapter nào đó nằm trên cùng mạng LAN, adapter gửi sẽ đặt địa chỉ nhận vào trong frame. Khi nhận được frame, adapter đích loại bỏ các tiêu đề của frame và gửi dữ liệu lên tầng phía trên. Tất cả các adapter khác trong LAN cũng đều nhận được frame. Tuy nhiên các adapter này sẽ loại bỏ frame (không gửi gói dữ liệu lên trên). Như vậy, các adapter sẽ không làm gián đoạn CPU trung tâm khi chúng nhận được dữ liệu dành cho nút khác. Tuy nhiên, đôi khi adapter gửi



muốn gửi tới tất cả các adapter khác trên mạng LAN. Khi đó adapter sử dụng một địa chỉ đặc biệt: địa chỉ quảng bá trong frame gửi đi. Đối với mạng cục bộ sử dụng địa chỉ 6 byte (như là LAN Ethernet và token-passing) thì địa chỉ quảng bá là chuỗi 48 bit 1 (FF-FF-FF-FF-FF-FF trong hệ 16).

### Nguyên lý: Giữ các tầng độc lập với nhau

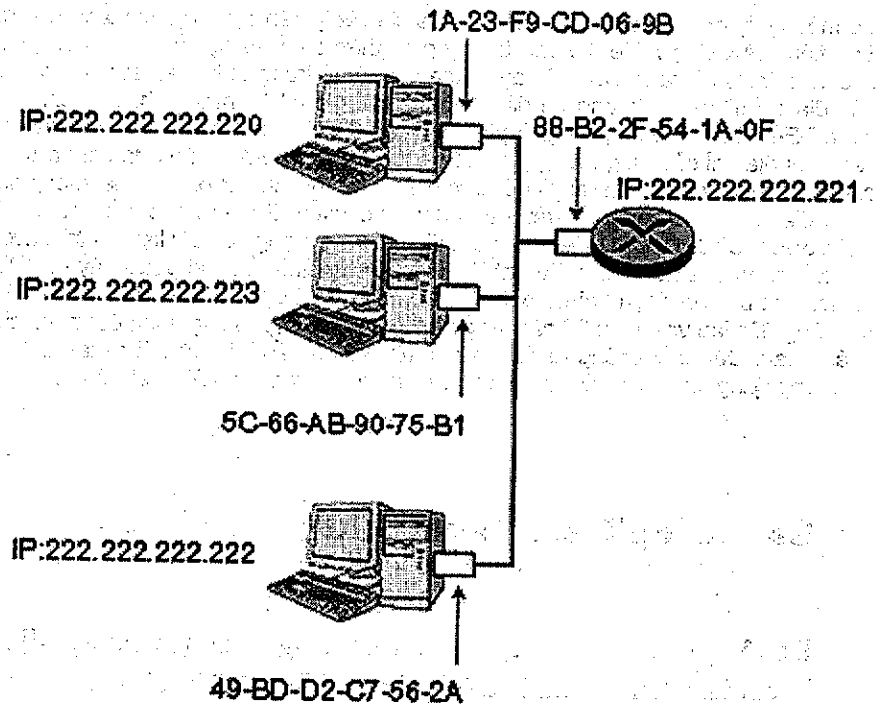
Có một vài lý do vì sao mỗi nút đều có địa chỉ vật lý bên cạnh địa chỉ tầng mạng. Đầu tiên, LAN được thiết kế cho bất kỳ giao thức tầng mạng nào chứ không chỉ cho giao thức IP và Internet. Thay vì địa chỉ vật lý trung tính, nếu adapter được gán địa chỉ IP thì nó không dễ dàng hỗ trợ các giao thức mạng khác (ví dụ IXP hoặc DECNET). Thứ hai, nếu adapter sử dụng địa chỉ tầng mạng thay cho địa chỉ vật lý thì địa chỉ của tầng mạng phải được lưu trữ trong RAM của adapter và phải cấu hình lại khi di chuyển (hay khởi động) adapter. Một lựa chọn khác là không sử dụng địa chỉ của adapter và yêu cầu adapter chuyển dữ liệu trong mỗi frame nó nhận được tới CPU. CPU kiểm tra xem địa chỉ tầng mạng của dữ liệu có trùng với địa chỉ mạng của nó không. Tuy nhiên vấn đề nảy sinh với giải pháp này là CPU sẽ liên tục bị gián đoạn khi có bất kỳ frame nào lan truyền trên LAN. Tóm lại, để các tầng độc lập với nhau thì các tầng có thể có những phương pháp đánh địa chỉ khác nhau. Đến đây chúng ta đã thấy có tới 3 kiểu đánh địa chỉ: tên máy tính ở tầng ứng dụng, địa chỉ IP ở tầng mạng và địa chỉ vật lý ở tầng liên kết dữ liệu

## 5.4.2. Giao thức giải mã địa chỉ (ARP)

Do tồn tại cả hai kiểu địa chỉ: địa chỉ tầng mạng (chẳng hạn địa chỉ IP) và địa chỉ tầng liên kết dữ liệu (địa chỉ vật lý) nên chắc chắn cần phải có một phương thức biến đổi giữa chúng. Đối với Internet, đây là công việc của giao thức giải mã địa chỉ ARP [RFC 826]. Tất cả máy tính và router trên LAN đều có **module ARP**.

Để hiểu rõ hơn về ARP, xét mạng minh họa trên Hình 5.23. Mỗi nút trong mạng có địa chỉ IP duy nhất và adapter của nút có một địa chỉ vật lý. Địa chỉ IP được viết dưới dạng ký pháp dấu chấm thập phân và địa chỉ LAN được viết dưới dạng ký pháp thập lục phân. Bây giờ, giả sử rằng nút có địa chỉ IP 222.222.222.220 muốn gửi gói dữ liệu IP đến nút có địa chỉ IP 222.222.222.222. Để thực hiện công việc này, nút gửi phải chuyển cho adapter của nó không chỉ gói dữ liệu IP mà cả địa chỉ vật lý của nút nhận

(222.222.222.222). Khi nhận được gói dữ liệu IP và địa chỉ LAN, adapter của nút gửi sẽ tạo ra frame tầng liên kết dữ liệu chứa địa chỉ vật lý của nút nhận và gửi frame đó trên LAN. Nhưng làm thế nào để nút gửi xác định địa chỉ vật lý của nút có địa chỉ IP là 222.222.222.222? Nó sẽ đưa cho module ARP địa chỉ IP 222.222.222.222, sau đó module ARP trả lại địa chỉ vật lý tương ứng với địa chỉ IP được hỏi, là 49-DB-D2-C7-56-2A.




**Hình 5.23 Mỗi nút trong mạng LAN có một địa chỉ IP, mỗi adapter của nút có một địa chỉ mạng LAN**

Do vậy chúng ta thấy rằng ARP đã xác định địa chỉ vật lý từ địa chỉ IP. Trong khía cạnh nào đó, chức năng này tương tự DNS (đã nghiên cứu trong mục 2.5), DNS xác định địa chỉ IP từ tên máy tính. Tuy nhiên sự khác biệt rất lớn giữa hai dịch vụ này là DNS chuyển đổi tên mọi máy tính trên Internet. Ngược lại ARP chỉ chuyển đổi địa chỉ IP cho những nút trên cùng mạng LAN. Nếu một nút ở Hà Nội cố gắng dùng module ARP để xác định địa chỉ vật lý của một nút ở Huế thì chắc chắn module ARP sẽ trả lại một mã lỗi.



Bây giờ chúng ta xét module ARP làm việc như thế nào. Module ARP trong mỗi nút chứa một bảng ARP trong RAM của mình. Mỗi hàng của bảng là một ánh xạ giữa địa chỉ IP và địa chỉ vật lý.

Hình 5.24 minh họa bảng ARP của nút 222.222.222.220. Với mỗi ánh xạ trong bảng ARP có trường "thời gian sống" (TTL) cho chính ánh xạ đó, xác định thời gian tồn tại của ánh xạ trong bảng. Chú ý rằng bảng này không nhất thiết phải chứa tất cả các ánh xạ cho mọi nút trên LAN, ánh xạ có thể dần dần được thêm vào bảng. Thời gian sống của một ánh xạ thường là 20 phút kể từ khi ánh xạ được đưa vào bảng ARP.

| IP address | LAN address | TTL |
|---|---|---|
| 222.222.222.221 | 88-B2-2F-54-1A-0F | 13:45:00 |
| 222.222.222.223 | 5C-66-AB-90-75-B1 | 13:52:00 |

**Hình 5. 24 Bảng ARP của nút 222.222.222.220**

Bây giờ, giả sử nút 222.222.222.220 muốn gửi gói dữ liệu IP đến một nút trên LAN. Nút gửi cần xác định địa chỉ vật lý từ địa chỉ IP của nút nhận. Công việc này đơn giản nếu bảng ARP của nút gửi chứa ánh xạ của nút nhận. Nhưng nếu bảng ARP đó không chứa ánh xạ tương ứng cho nút nhận thì sao? Giả sử nút có địa chỉ IP 222.222.222.220 muốn gửi gói dữ liệu tới nút 222.222.222.222. Khi đó nút gửi phải sử dụng giao thức ARP để giải mã địa chỉ. Đầu tiên, nút gửi tạo ra một gói đặc biệt gọi là **gói ARP (ARP packet)**. Trong gói ARP có trường chứa địa chỉ IP và địa chỉ vật lý của nút gửi, nút nhận. Cả gói truy vấn và trả lời ARP đều có chung khuôn dạng. Mục đích của gói truy vấn ARP là hỏi tất cả các nút khác trên LAN để xác định địa chỉ vật lý ứng với địa chỉ IP.

Trở lại ví dụ trên, nút 222.222.222.220 gửi gói truy vấn ARP đến adapter và yêu cầu adapter gửi tới tất cả các nút trên mạng LAN, có nghĩa là sử dụng địa chỉ quảng bá FF-FF-FF-FF-FF-FF. Adapter đặt gói ARP trong frame tầng liên kết dữ liệu, với địa chỉ đích của frame là địa chỉ quảng bá và gửi frame vào mạng LAN. Nó cũng giống như việc giáo viên vào lớp hỏi to "Sinh viên nào có tên là Trần Văn X hãy báo số thẻ sinh viên". Câu nói này lan tỏa khắp lớp học (được quảng bá), tất cả các sinh viên đều nghe thấy

nhưng chỉ có sinh viên Trần Văn X mới trả lời. Frame chứa truy vấn ARP được tất cả các adapter trên LAN nhận (do sử dụng địa chỉ quảng bá) và mỗi adapter gửi gói ARP trong frame lên bộ xử lý trung tâm của mình. Sau đó mỗi nút tự kiểm tra xem địa chỉ IP của mình có giống với địa chỉ IP đích trong gói ARP không. Chỉ có duy nhất nút phù hợp mới gửi gói ARP trả lời chứa ánh xạ yêu cầu. Sau đó nút gửi truy vấn (222.222.222.220) có thể cập nhật bảng ARP và gửi đi gói dữ liệu IP.

Có hai điểm cần chú ý trong giao thức ARP. Thứ nhất, thông điệp truy vấn ARP được gửi quảng bá trong khi thông điệp trả lời ARP được gửi trong frame bình thường. Thứ hai, ARP hoạt động theo kiểu "cắm vào là chạy" (plug and play) vì bảng ARP của nút được xây dựng tự động, không cần người quản trị thiết lập cấu hình. Và nếu một nút dừng kết nối với LAN thì ánh xạ tương ứng của nó cũng bị xoá khỏi bảng sau một khoảng thời gian nào đấy.

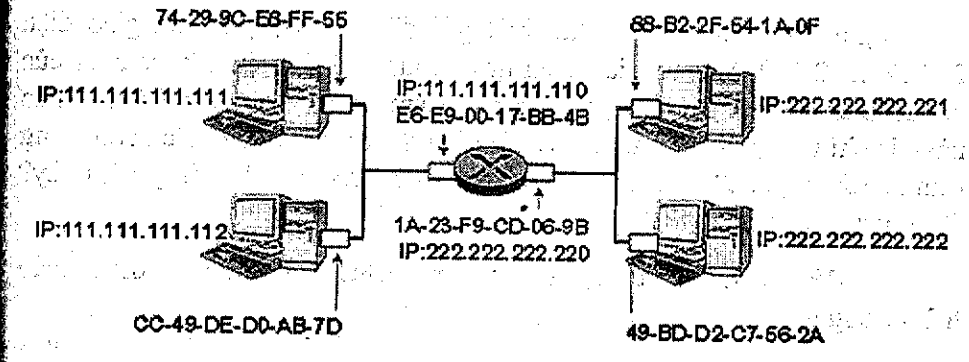
### Gửi gói dữ liệu đến nút không nằm trong LAN

Chúng ta đã hình dung rõ ràng hoạt động của ARP khi một nút gửi gói dữ liệu đến nút khác nằm trong cùng mạng LAN. Bây giờ hãy xét tình huống phức tạp hơn khi nút muốn gửi dữ liệu tới nút nằm ngoài mạng LAN. Chúng ta xét ví dụ minh họa trên Hình 5.25 gồm hai mạng LAN kết nối với nhau qua router.

Có một số điểm cần chú ý trong Hình 5.25. Đầu tiên nút chia ra làm hai kiểu: máy tính và router. Mỗi máy tính có duy nhất một địa chỉ IP và một adapter. Như đã nói tới trong phần 4.4, mỗi giao diện ghép nối của router có một địa chỉ IP riêng. Mỗi giao diện của router cũng có module ARP (trong router) và adapter. Router trong Hình 5.25 có hai giao diện nên có hai địa chỉ IP, hai module ARP và hai adapter. Dĩ nhiên, mỗi adapter có một địa chỉ vật lý riêng.

Cũng chú ý rằng tất cả giao diện kết nối vào mạng LAN 1 có địa chỉ IP dạng 111.111.111.xxx và kết nối vào mạng LAN 2 có địa chỉ IP dạng 222.222.222.xxx. Trong ví dụ này, 3 byte đầu tiên của địa chỉ IP xác định địa chỉ mạng trong khi đó byte cuối cùng xác định nút cụ thể nào trong mạng (chính xác hơn là adapter).






**Hình 5.25 Hai mạng LAN kết nối với nhau qua router**

Bây giờ, giả sử rằng máy tính 111.111.111.111 muốn gửi gói dữ liệu IP đến máy tính 222.222.222.222. Như thường lệ, máy tính gửi sẽ chuyển gói dữ liệu xuống adapter của mình. Nhưng máy tính gửi cũng cần phải chỉ cho adapter biết địa chỉ vật lý đích thích hợp. Adapter sẽ dùng địa chỉ vật lý nào ? Có phải là địa chỉ vật lý của máy tính 222.222.222.222 - 49-BD-D2-C7-56-2A không? Hiển nhiên nếu adapter gửi sử dụng địa chỉ vật lý này thì chắc chắn không một adapter nào của LAN 1 sẽ gửi gói dữ liệu IP lên tầng mạng của mình, vì địa chỉ đích của frame không phù hợp với địa chỉ vật lý của bất kỳ adapter nào trên LAN 1, do đó gói dữ liệu sẽ mất.

Nếu quan sát trên Hình 5.25, chúng ta thấy rằng để gửi gói dữ liệu từ nút 111.111.111.111 đến nút khác trên LAN 2, đầu tiên gói dữ liệu phải được gửi đến giao diện router 111.111.111.110. Như đã thảo luận trong phần 4.4, bảng định tuyến của máy tính 111.111.111.111 sẽ chỉ ra rằng để đi đến máy tính 222.222.222.222, thì đầu tiên gói dữ liệu cần được gửi tới router (chính xác hơn là adapter của router) có địa chỉ 111.111.111.110. Như vậy, địa chỉ vật lý đích của frame là địa chỉ vật lý của giao diện router có địa chỉ 111.111.111.110 tức là E6-E-00-17-BB-4B. Làm thế nào máy tính gửi xác định được địa chỉ vật lý của 111.111.111.110?. Tất nhiên là bằng cách sử dụng ARP. Sau khi xác định được địa chỉ vật lý, nút gửi sẽ tạo ra frame và gửi frame vào LAN 1. Adapter của router trên LAN 1 sẽ nhận frame tầng liên kết dữ liệu gửi cho nó, và sẽ chuyển gói IP lên tầng mạng của router. Gói dữ liệu IP đã được chuyển từ máy tính nguồn đến router. Bây giờ, router phải xác định giao diện để gửi dữ liệu đi tiếp. Như đã nêu trong phần 4.4, công việc này được thực hiện bằng cách tra cứu bảng định tuyến của router.

Bảng định tuyến của router cho biết gói dữ liệu cần gửi qua giao diện 222.222.222.220. Sau đó giao diện này sẽ gửi gói dữ liệu đến adapter của nó, adapter này đặt gói dữ liệu trong một frame mới và gửi vào LAN 2. Lúc này địa chỉ vật lý đích trong frame gửi đi là địa chỉ vật lý của đích cuối cùng (nút 222.222.222.222). Làm thế nào router có được địa chỉ vật lý đích này? Tất nhiên là dựa vào ARP.

ARP cho Ethernet được đặc tả trong RFC 826 và có thể tham khảo thêm trong RFC 1180.

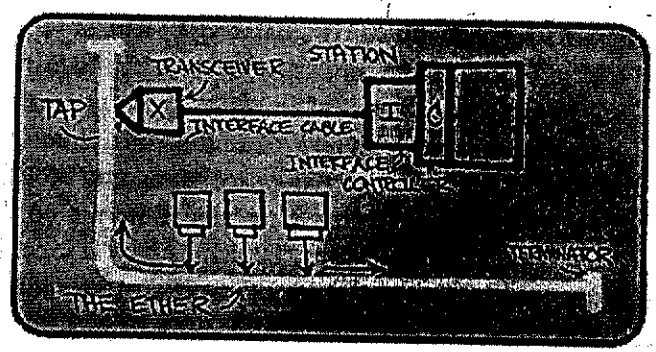
## 5.5. ETHERNET

Hiện nay Ethernet thống trị thị trường mạng cục bộ. Mới chỉ đầu những năm 1980 đến đầu những năm 1990, Ethernet còn có nhiều đối thủ khác như FDDI, token-ring, ATM. Một số công nghệ đã thành công trong việc chiếm lĩnh một thị phần nào đó trong vài năm. Nhưng từ khi ra đời vào giữa những năm 70, Ethernet liên tục phát triển để rồi dần dần chiếm lĩnh phần lớn thị phần. Ngày nay, Ethernet là công nghệ vượt xa các công nghệ LAN khác và khả năng này khó có thể bị đảo lộn trong tương lai gần.

Có rất nhiều lý do dẫn đến sự thành công của Ethernet. Thứ nhất, Ethernet là mạng cục bộ tốc độ cao được triển khai rộng rãi đầu tiên. Được triển khai tương đối sớm nên các nhà quản trị mạng lập tức trở nên quen thuộc với Ethernet (ưu điểm, các đặc tính...) - và ngại chuyển sang những công nghệ LAN mới. Thứ hai token-ring, FDDI và ATM phức tạp và đắt hơn Ethernet. Thứ ba, lý do chính đáng nhất để sử dụng các công nghệ LAN khác (FDDI hay ATM) là do công nghệ mới có tốc độ cao hơn, tuy nhiên Ethernet luôn luôn "phản công" lại bằng cách liên tục nâng cấp tốc độ. Ethernet dạng chuyển mạch được phát minh vào đầu những năm 90 với tốc độ rất cao. Cuối cùng vì Ethernet quá phổ biến, nên phần cứng Ethernet (đặc biệt là card mạng) cũng hết sức phổ biến và rẻ. Giá cả thấp này cũng do giao thức đa truy cập của Ethernet - CSMA/CD hoàn toàn phân tán nên có thiết kế đơn giản.

Kiến trúc Ethernet (Hình 5.26) được Bob Metcalf và David Boggs đưa ra vào khoảng giữa những năm 70.






**Hình 5.26 Thiết kế đầu tiên của Ethernet**

### Ngày xưa

**Bob Metcalfe và Ethernet**

Khi còn là nghiên cứu sinh ở trường đại học Harvard vào đầu những năm 1970, Bob Metcalfe làm việc cho ARRAnet tại MIT và đã thực sự ấn tượng về công trình của Abramson về giao thức truy cập ngẫu nhiên. Sau khi hoàn thành luận án tiến sỹ và ngay trước khi bắt đầu công việc mới ở Xero Palo Alto Research Center (Xerox PARC), Bob đã tới thăm Abrasmon và các đồng nghiệp tại trường đại học Hawaii trong 3 tháng và nhìn tận mắt Alohanet. Tại Xero PARC, Metcalfe đã làm quen với máy tính Alto (về khía cạnh nào đó có thể coi là tiền thân của máy tính cá nhân PC vào đầu thập niên 80). Metcalfe đã nhận thức được nhu cầu kết nối mạng cho các máy tính này với một chi phí không đắt. Nên với những kiến thức về ARPNet, Alohanet và giao thức truy cập ngẫu nhiên, Metcalfe và đồng nghiệp David Bogg đã phát minh ra Ethernet.

Kiến trúc Ethernet đầu tiên của Metcalfe và Bogg hoạt động với tốc độ 2.94 Mbps và có thể kết nối 256 máy trong phạm vi 1 dặm. Metcalfe và Bogg đã thành công trong việc kết nối các máy tính Alto. Sau đó Metcalfe đi đầu trong việc xây dựng liên minh giữa Xerox, Digital và Intel để thiết lập chuẩn Ethernet với tốc độ 10 Mbps và được IEEE thông qua. Năm 1979 Metcalfe thành lập công ty riêng là 3Com, với mục tiêu phát triển và thương mại hóa các công nghệ mạng, kể cả công nghệ Ethernet. Cụ thể 3Com đã bán sản phẩm card mạng Ethernet cho các máy tính IBM PC ngày càng trở nên phổ biến. Metcalfe rời 3Com khi 3Com có 2000 nhân viên, trị giá 400 triệu đô la thu nhập. Tháng 1 năm 2000, 3Com có vốn lên tới 15 tỷ USD và 13.000 công nhân.

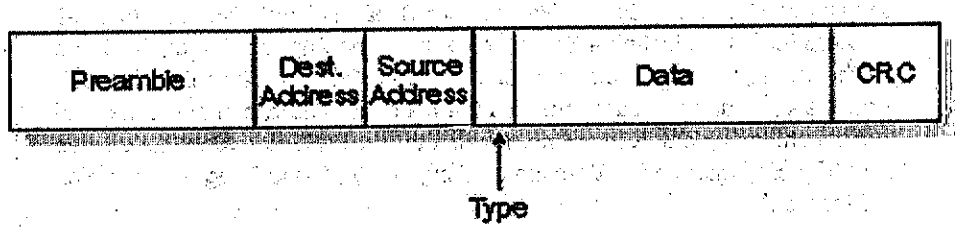
## 5.5.1 Những khái niệm cơ bản của Ethernet

Ngày nay Ethernet xuất hiện dưới nhiều hình thức. Mạng cục bộ Ethernet có thể có topo dạng bus hay dạng sao. Mạng cục bộ Ethernet có thể sử dụng cáp đồng trục hay cáp quang. Hơn nữa, Ethernet có thể truyền dữ liệu với các tốc độ khác nhau: 10Mbps, 100Mbps hay 1Gbps. Nhưng dù là Ethernet kiểu nào, tất cả các công nghệ Ethernet đều có một số đặc trưng quan trọng sau đây:

***Cấu trúc frame Ethernet***

Các công nghệ Ethernet khác nhau đều có chung cấu trúc frame. Cho dù công nghệ Ethernet sử dụng cáp đồng trục hay cáp quang, chạy với tốc độ 10Mbps, 100Mbps hay 1Gbps thì cấu trúc frame đều như nhau.

Frame Ethernet được minh hoạ trong Hình 5.27. Kiến thức về khuôn dạng frame Ethernet sẽ giúp chúng ta hiểu kỹ về Ethernet. Chúng ta xét việc gửi gói dữ liệu IP giữa hai máy tính trên cùng một mạng cục bộ Ethernet (Chú ý rằng Ethernet cũng có thể mang các gói dữ liệu tầng mạng khác IP). Giả sử A là adapter gửi có địa chỉ vật lý AA-AA-AA-AA-AA-AA và adapter nhận B có địa chỉ vật lý là BB-BB-BB-BB-BB-BB.




**Hình 5.27 Khuôn dạng gói tin Ethernet**

Adapter gửi đặt gói dữ liệu (IP datagram) trong frame Ethernet và gửi frame này xuống tầng vật lý. Adapter nhận sẽ nhận frame từ tầng vật lý, lấy ra gói dữ liệu IP và chuyển lên tầng mạng phía trên. Ở đây chúng ta chỉ nghiên cứu 6 trường trong frame Ethernet:

**Trường dữ liệu (từ 46 đến 1500 byte):** trường này chứa gói dữ liệu IP, MTU (Maximum Transfer Unit) của Ethernet là 1500 byte. Điều này có nghĩa là nếu gói dữ liệu IP vượt quá 1500 byte thì máy tính phải chia nhỏ gói dữ liệu ra (xem 4.4.4). Kích thước tối thiểu của trường này là 46 byte.



Điều này có nghĩa là nếu gói dữ liệu nhỏ hơn 46 byte, trường dữ liệu phải được "chèn" thêm một số dữ liệu giả cho đủ 46 byte. Khi bên gửi chèn thêm dữ liệu vào thì tầng mạng ở bên nhận cũng nhận được cả gói dữ liệu IP lẫn dữ liệu được chèn thêm vào, khi đó nó phải sử dụng trường độ dài trong gói dữ liệu IP để loại bỏ phần thêm vào.

**Địa chỉ đích (6 byte):** Trường này chứa địa chỉ vật lý của adapter nhận (chẳng hạn BB-BB-BB-BB-BB-BB). Khi adapter B nhận bất kỳ frame nào, nó sẽ kiểm tra địa chỉ đích của frame. Nếu địa chỉ đích là BB-BB-BB-BB-BB-BB (địa chỉ của chính nó), hoặc địa chỉ quảng bá LAN (FF-FF-FF-FF-FF-FF) thì adapter mới chuyển gói tin datagram trong trường dữ liệu lên tầng mạng. Nếu không adapter sẽ loại bỏ frame (trong trường hợp này frame được gửi tới một adapter khác).

**Địa chỉ nguồn (6 byte):** Trường này chứa địa chỉ vật lý của adapter gửi frame, trong ví dụ này là AA-AA-AA-AA-AA-AA.

**Trường kiểu (2 byte):** Trường này cho phép Ethernet hỗ trợ nhiều giao thức tầng mạng khác nhau. Cần chú ý rằng máy tính có thể sử dụng nhiều giao thức tầng mạng (không chỉ có IP). Trên thực tế, máy tính nào đó có thể hỗ trợ nhiều giao thức tầng mạng và sử dụng các giao thức khác nhau cho những ứng dụng khác nhau. Vì thế khi nhận được một frame Ethernet, adapter B cần xác định giao thức tầng mạng nào sẽ nhận nội dung của trường dữ liệu. Những giao thức tầng mạng như IP, Novell IPX hoặc AppleTalk đều có một mã định danh (là một số) đã được chuẩn hóa. Hơn nữa, giao thức ARP cũng có một định danh. Trường kiểu tương tự trường protocol trong gói dữ liệu IP hay trường số hiệu cổng trong tầng giao vận; mục đích của tất cả các trường này là kết hợp giao thức ở tầng dưới với giao thức ở tầng trên nó.

**Mã kiểm tra dư thừa vòng (Cyclic Redundancy Check -CRC) (4 byte).** Như đã nêu trong phần 5.2.3, mục đích của trường CRC là cho phép adapter phát hiện liệu có lỗi nào trong frame nhận được hay không. Có nhiều nguyên nhân lỗi bit, chẳng hạn suy hao năng lượng điện từ của tín hiệu; tỏa nhiệt trong card Ethernet hay cáp mạng. Việc phát hiện lỗi được thực hiện như sau: Khi tạo ra frame Ethernet, máy tính A tính giá trị trường CRC dựa trên trường dữ liệu thực sự. Công việc kiểm tra tại B xem dữ liệu

thực sự và CRC có mâu thuẫn không được gọi là **CRC check**. Nếu việc kiểm tra CRC thất bại (nghĩa là nếu giá trị trường CRC không phù hợp với phần dữ liệu) thì máy tính B xác định trong frame có lỗi.

**Lời mở đầu (preamble) (8 byte)**: Frame Ethernet bắt đầu với trường preamble 8 byte, trong đó bảy byte đầu tiên có giá trị là 10101010; byte thứ tám có giá trị 10101011. Bảy byte đầu tiên của phần mở đầu làm nhiệm vụ "đánh thức" adapter nhận và đồng bộ hoá đồng hồ bên gửi với đồng hồ bên nhận. Tại sao các đồng hồ lại không đồng bộ hoá ? Chú ý rằng adapter A truyền frame với tốc độ 10Mbps, 100Mbps hay 1Gbps phụ thuộc vào kiểu Ethernet. Tuy nhiên, adapter A chưa chắc đã truyền frame với tốc độ xác định mà với tốc độ nào đó. Adapter nhận có thể chốt đồng hồ của adapter A bằng cách chốt tất cả các bit trong bảy byte đầu tiên. Hai bit cuối cùng trong byte thứ 8 (hai bit 1 liên tiếp nhau) báo cho adapter B biết rằng "dữ liệu quan trọng" chuẩn bị đến. Khi máy tính B thấy hai bit 1 liên tiếp nhau, nó biết rằng 6 byte tiếp theo là địa chỉ đích. Adapter có thể phát hiện frame đã được truyền xong khi không thấy dòng điện.

***Dịch vụ không hướng nối, không tin cậy***

Tất cả công nghệ Ethernet cung cấp cho tầng mạng **dịch vụ không hướng nối**. Nghĩa là khi adapter A muốn gửi gói dữ liệu đến adapter B, adapter A sẽ đặt gói dữ liệu trong frame và gửi frame đó vào LAN mà không cần "bắt tay" trước với adapter B. Dịch vụ không kết nối ở tầng 2 này tương tự với dịch vụ IP ở tầng 3 và dịch vụ UDP ở tầng 4.

Công nghệ Ethernet cung cấp **dịch vụ không tin cậy** cho tầng mạng. Cụ thể, khi nhận được frame từ adapter A, adapter B sẽ không gửi phản hồi cho A. Adapter A không thể xác định liệu frame nó truyền đi có được nhận đúng hay không. Nếu phát hiện lỗi khi kiểm tra CRC, adapter B sẽ loại bỏ frame. Chính điều này giúp Ethernet đơn giản và rẻ. Nhưng dòng dữ liệu chuyển tới tầng mạng có thể bị gián đoạn.

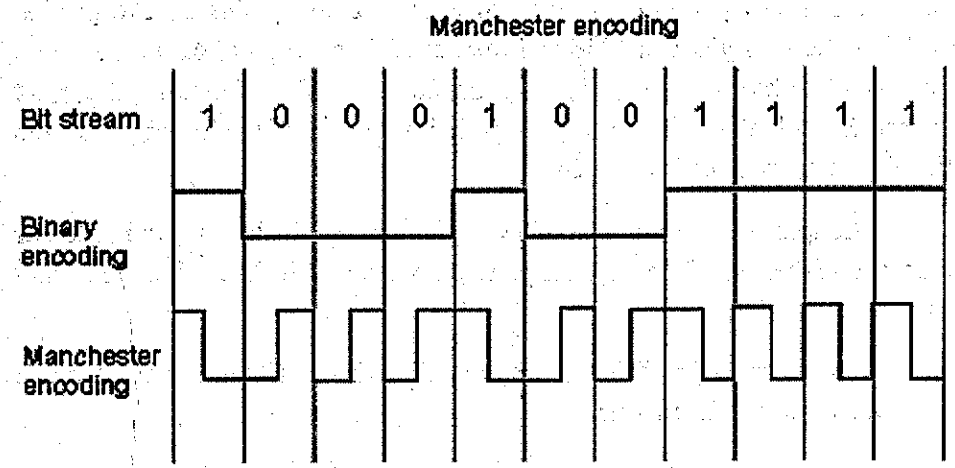
Nếu có sự gián đoạn do một số frame Ethernet bị loại bỏ, giao thức tầng ứng dụng tại máy B có phát hiện được sự gián đoạn đó không ? Như đã trình bày trong chương 3, điều này phụ thuộc việc ứng dụng sử dụng UDP hay TCP. Nếu ứng dụng dùng UDP thì giao thức tầng ứng dụng trong máy B



sẽ không phát hiện được gián đoạn trong dữ liệu. Mặt khác, nếu ứng dụng dùng TCP thì thực thể TCP trong máy B sẽ không gửi biên nhận cho những dữ liệu đã bị loại bỏ, do vậy thực thể TCP trong máy A sẽ gửi lại. Chú ý rằng khi TCP gửi lại dữ liệu, thì cuối cùng dữ liệu cũng sẽ đi qua các adapter Ethernet. Và như vậy Ethernet truyền lại dữ liệu. Tuy nhiên Ethernet không biết rằng nó đang truyền lại mà coi rằng đó là một gói dữ liệu mới.

***Giải tần cơ sở và mã hoá Manchester***

Ethernet sử dụng băng tần cơ sở (baseband) nghĩa là adapter gửi tín hiệu số trực tiếp vào kênh truyền dùng chung. Card giao diện không dịch chuyển tín hiệu sang dải tần số khác như trong ASDL và các hệ thống cáp modem. Ethernet sử dụng mã hoá Manchester (Hình 5.28). Trong phương pháp mã hoá Manchester, mỗi bít ứng với một quá trình chuyển trạng thái (transition): bit 1 chuyển từ trên xuống dưới, bit 0 chuyển từ dưới lên trên. Lý do sử dụng mã hoá Manchester là đồng hồ của adapter gửi và nhận không đồng bộ hoàn toàn với nhau. Khi xuất hiện sự chuyển ngay trong phần giữa mỗi bit, máy tính nhận có thể đồng bộ đồng hồ của nó với đồng hồ của máy tính gửi. Sau khi đồng hồ của adapter nhận được đồng bộ hoá, phía nhận có thể thu được tín hiệu của mỗi bit và xác định nó là 0 hay 1. Mã hoá Manchester được sử dụng nhiều trong tầng vật lý chứ không phải trong tầng liên kết dữ liệu.




**Hình 5.28 Mã hóa Manchester**

## 5.2.2 CSMA/CD: Giao thức đa truy cập của Ethernet

Các nút trên mạng cục bộ Ethernet được kết nối qua một kênh truyền quảng bá dùng chung, vì vậy khi adapter gửi đi một frame, tất cả các adapter trên LAN đều nhận được frame. Như chúng ta đã đề cập trong phần 5.3, Ethernet dùng thuật toán đa truy cập CSMA/CD. Chú ý rằng CSMA/CD sử dụng các cơ chế sau:

- Adapter có thể bắt đầu truyền tại bất kì thời điểm nào, nghĩa là không chia khoảng thời gian.

- Adapter không bao giờ truyền frame khi thấy có adapter khác đang truyền (cảm nhận sóng mang).

- Adapter đang truyền chấm dứt truyền ngay khi phát hiện ra adapter khác cũng đang truyền (phát hiện xung đột).

- Trước khi cố gắng thử truyền lại, adapter đợi một khoảng thời gian ngẫu nhiên tương đối nhỏ.

Những cơ chế này giúp hiệu suất của CSMA/CD được cải thiện đáng kể so với slotted ALOHA khi vận hành trong môi trường LAN. Trong thực tế, nếu thời gian để tín hiệu lan truyền giữa hai nút là rất nhỏ thì hiệu suất của CSMA/CD có thể đạt tới 100%. Nhưng chú ý rằng cơ chế thứ hai và thứ ba kể trên yêu cầu adapter Ethernet có khả năng (1) cảm nhận được khi nào thì có một adapter khác đang truyền và (2) phát hiện xung đột trong khi truyền. Adapter Ethernet thực hiện hai nhiệm vụ này bằng việc đo mức điện áp trước và trong khi truyền.

Adapter dùng giao thức CSMA/CD không cần kết hợp với adapter khác trên Ethernet. Trên một adapter, giao thức CSMA/CD làm việc như sau:

- Adapter nhận PDU tầng mạng, tạo ra frame Ethernet và đặt frame vào trong bộ đệm của adapter.

- Nếu adapter cảm nhận kênh truyền rỗi (không có năng lượng tín hiệu trên kênh truyền) thì adapter bắt đầu truyền. Nếu adapter thấy kênh truyền bận, nó sẽ đợi cho đến khi không phát hiện được năng lượng tín hiệu và sau đó bắt đầu truyền.



- Trong khi truyền, adapter kiểm tra xem có năng lượng tín hiệu đến từ adapter khác hay không. Nếu sau khi đã truyền xong frame mà không phát hiện được năng lượng trên đường truyền thì có thể xem frame được truyền thành công.

- Nếu adapter phát hiện năng lượng tín hiệu từ adapter khác trong khi đang truyền thì lập tức nó dừng lại không truyền và gửi đi tín hiệu báo nhiễu 48 bit (jam signal).

Sau khi dừng phát và gửi tín hiệu báo nhiễu, adapter sẽ thực hiện thuật toán **exponential backoff**. Khi truyền frame nào đó, nếu thấy frame đó bị xung đột n lần liên tiếp, adapter chọn một giá trị ngẫu nhiên K trong khoảng $(0,1,2.,..2^m - 1)$ với $m = \min(n,10)$. Sau đó adapter sẽ đợi K*512 trước khi quay lại bước 2.

Sau đây chúng ta sẽ giải thích về giao thức CSMA/CD. Mục đích của tín hiệu báo nhiễu là bảo đảm tất cả các adapter đang truyền khác đều phát hiện ra xung đột. Xét ví dụ sau: giả sử adapter A bắt đầu truyền đi một frame và ngay trước khi tín hiệu từ A tới được adapter B, adapter B bắt đầu truyền. Do vậy B chỉ truyền được vài bit trước khi dừng lại không truyền tiếp. Vài bit này sẽ lan tỏa được đến A, nhưng chúng không tạo đủ năng lượng để A có thể phát hiện xung đột. Để đảm bảo A phát hiện được xung đột, B phải truyền thêm tín hiệu báo nhiễu dài khoảng 48 bit.

Tiếp theo ta xét tới thuật toán exponetial backoff. Cần chú ý rằng thời gian để truyền đi một bit rất nhỏ: với tốc độ Ethernet 10Mbps, thời gian này là 0,1 microsecond. Xét ví dụ sau: giả sử adapter lần đầu tiên truyền đi một frame và trong khi truyền phát hiện có xung đột. Sau đó adapter sẽ chọn K=0 với xác suất 0,5 và chọn K=1 với xác suất 0,5. Nếu adapter chọn K=0 thì ngay lập tức nó sẽ nhảy đến bước 2 sau khi truyền đi tín hiệu báo nhiễu. Nếu adapter chọn K=1 thì nó sẽ đợi 51,2 microsecond trước khi quay lại bước 2. Sau xung đột lần thứ hai, K được chọn ngẫu nhiên giữa các giá trị (0,1,2,3) với xác suất bằng nhau, sau ba xung đột K sẽ được chọn ngẫu nhiên giữa các giá trị (0,1,2,…,7) với xác suất bằng nhau, sau nhiều hơn

mười xung đột K được chọn ngẫu nhiên giữa các giá trị (0,1,2,...,1023) với xác suất bằng nhau. Như vậy tổng số giá trị mà K có thể lựa chọn tăng theo luỹ thừa cơ số 2 với số mũ là số lần xung đột cho (cho đến khi N=10).

Chuẩn Ethernet ấn định giới hạn khoảng cách giữa hai nút bất kỳ. Giới hạn này bảo đảm rằng nếu adapter A chọn giá trị K thấp hơn giá trị K của tất cả các adapter khác liên quan đến xung đột trong pha trước thì A có thể truyền đi frame mà không bị xung đột nữa.

Tại sao lại sử dụng thuật toán exponetial backoff ? Tại sao không chọn K trong khoảng {0,1,2,3,4,5,6,7} sau mọi xung đột. Lý do sau khi adapter gặp xung đột lần đầu tiên, nó không hình dung được có bao nhiêu adapter liên quan đến xung đột đó. Nếu chỉ có một số lượng nhỏ adapter thì chắc chắn K sẽ được chọn trong một tập hợp hạn chế. Ngược lại, nếu có nhiều adapter liên quan thì K được chọn trong một tập hợp lớn hơn. Bằng cách tăng kích cỡ của tập hợp sau mỗi xung đột, adapter sẽ thích nghi được với nhiều hoàn cảnh.

Chúng ta cần chú ý thêm rằng mỗi lần adapter chuẩn bị frame mới để gửi đi, nó sử dụng thuật toán CSMA/CD nói trên. Cụ thể adapter không quan tâm tới bất kỳ xung đột nào trước đó. Do vậy, rất có khả năng adapter với frame mới có thể truyền xen vào trong khi một vài adapter khác đang trong trạng thái exponetial backoff.

***Hiệu suất Ethernet***

Khi chỉ có một nút có frame để truyền, nút đó có thể truyền với tốc độ tối đa (10Mbps, 100Mbps hoặc 1Gbps). Tuy nhiên nếu nhiều nút cùng truyền thì tốc độ truyền thành công (effective rate) của kênh truyền có thể giảm đi đáng kể. Chúng ta định nghĩa **hiệu suất (efficiency)** của Ethernet là tỉ lệ thời gian không có xung đột trên kênh truyền khi có nhiều nút tích cực, mỗi nút cần truyền nhiều frame trong một khoảng thời gian dài. Để xác định hiệu suất gần đúng của Ethernet, giả sử $t_{prop}$ là thời gian lớn nhất năng lượng tín hiệu lan tỏa giữa hai adapter. Giả sử $t_{trans}$ là thời gian để truyền đi một frame Ethernet với độ lớn cực đại (xấp xỉ 1,2 ms với Ethernet 10 Mbps). Có thể xem [Lam 1980] và [Bertsekas 1991] để xác định công thức tính. Ở đây chúng ta sử dụng công thức:



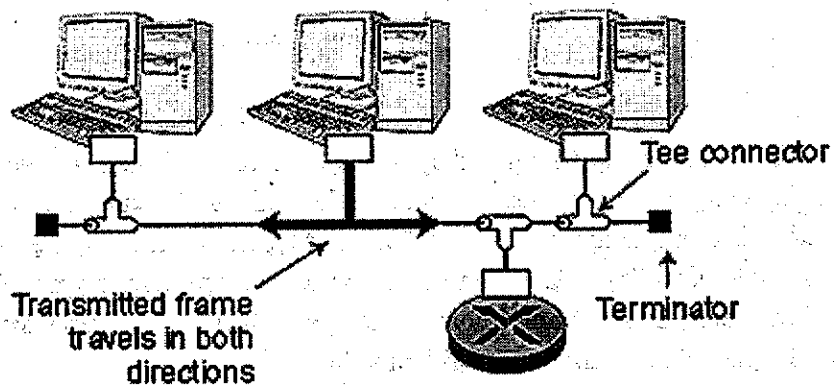
$$\text{Efficiency} = \frac{1}{1 + 5t_{prop}/t_{trans}}$$

Từ công thức này chúng ta thấy nếu $t_{prop}$ đạt tới 0 thì hiệu suất đạt tới 1. Điều này cũng rất hợp lý: nếu thời gian trễ là 0 thì các nút xung đột sẽ lập tức bỏ dở mà không lãng phí kênh truyền. Khi $t_{trans}$ trở lên rất lớn, hiệu suất đạt tới 1. Điều này cũng hiển nhiên vì khi frame có được kênh truyền nó sẽ chiếm dụng kênh truyền trong khoảng thời gian dài, như vậy kênh truyền hầu như lúc nào cũng trong trạng thái làm việc.

## 5.5.3 Những công nghệ Ethernet

Phần lớn những công nghệ Ethernet phổ biến ngày nay là **10Base2** sử dụng cáp đồng trục gầy (thin coaxial cable) có topo dạng bus, tốc độ truyền là 10Mbps; **10BaseT** sử dụng cáp đồng trục, topo hình sao, tốc độ truyền là 10 Mbps; **100BaseT** sử dụng dây đồng xoắn, topo hình sao, tốc độ truyền là 100Mbps; Gigabyte Ethernet sử dụng cả sợi quang hay dây đồng xoắn, truyền với tốc độ 1Gbps. Những công nghệ Ethernet này được chuẩn hoá bởi IEEE 802.3. Vì thế LAN Ethernet thường được gọi là 802.3 LAN.

Trước khi tiếp tục, chúng ta cần nói về **bộ tiếp sức (repeater)** - được sử dụng phổ biến trong mạng LAN cũng như các đường truyền trên khoảng cách xa. Repeater là thiết bị tầng vật lý xử lý trên từng bit riêng lẻ chứ không phải trên frame. Khi tín hiệu (biểu diễn bit 0 hoặc 1) đến từ một cổng, repeater thường tái tạo lại tín hiệu này bằng cách gia tăng cường độ năng lượng của tín hiệu và gửi tín hiệu đó qua tất cả các cổng còn lại. Repeater được sử dụng rộng rãi trong LAN để mở rộng phạm vi địa lý. Cần chú ý rằng trong Ethernet, repeater không có khả năng cảm nhận sóng mang hay thực hiện bất kỳ một chức năng nào của CSMA/CD, repeater chỉ tái tạo và gửi tín hiệu đến từ một cổng ra tất cả các cổng khác, kể cả trong trường hợp các cổng kia cũng đang có tín hiệu để truyền.



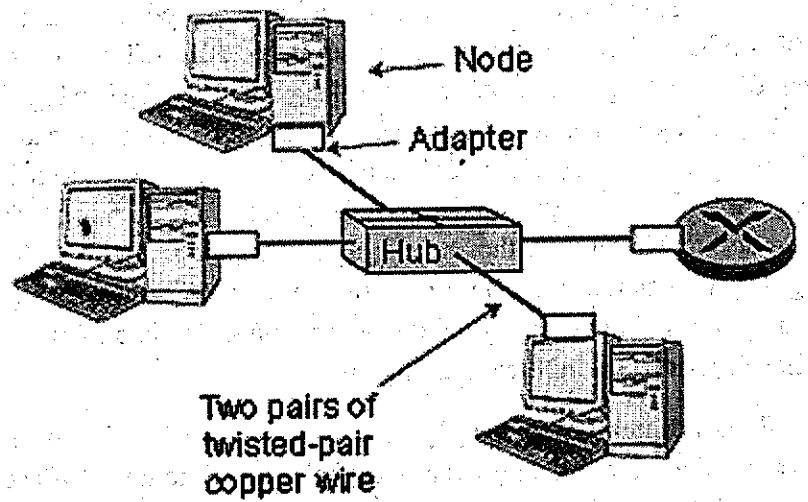

**Hình 5.29 Ethernet 10Base2**

10Base2 là một công nghệ Ethernet rất phổ biến. "10" trong 10Base2 có nghĩa là tốc độ truyền trong công nghệ này là 10 Mbps. "2" có ý nghĩa khoảng cách tối đa giữa hai trạm không có repeater ở giữa không vượt quá 200m. Hình 5.29 minh họa mạng Ethernet 10Base2. 10Base2 có topo dạng bus, các nút (chính xác hơn là các adapter) được kết nối trực tiếp vào một môi trường dùng chung – cáp đồng trục gầy (là loại cáp tương tự như cáp truyền hình nhưng mỏng và nhẹ hơn). Khi adapter gửi đi một frame, frame sẽ được truyền qua đầu nối chữ T (T connector). Sau đó frame sẽ lan tỏa theo hai hướng của dây dẫn. Trên đường đi, mỗi adapter sẽ nhận được một bản sao của frame (chính xác hơn là các adapter thu được các tín hiệu của frame). Khi đến điểm cuối cùng của dây dẫn, tất cả các tín hiệu sẽ bị terminator hấp thụ (triệt tiêu). Chú ý rằng, do tất cả adapter đều có khả năng nhận mọi frame nên 10Base2 rõ ràng là môi trường quảng bá.

Nếu không có repeater, độ dài tối đa của bus là 185m. Nếu bus có độ dài lớn hơn, suy hao tín hiệu sẽ làm hệ thống hoạt động không chính xác. Ngoài ra nếu không có repeater, số lượng tối đa các nút là 30. Người ta sử dụng repeater để nối các đoạn 10Base2 liên tiếp nhau, mỗi đoạn có thể có 30 máy và dài 185m. Chỉ có thể sử dụng tối đa 4 repeater – do đó có 5 đoạn 10Base2.








**Hình 5.30 Topo dạng sao 10BaseT và 100BaseT**

10BaseT và 100BaseT là hai công nghệ tương tự nhau. Điểm khác biệt quan trọng nhất là tốc độ truyền của 10BaseT là 10Mbps trong khi tốc độ truyền của Ethernet 100BaseT là 100Mbps. 10BaseT và 100BaseT là công nghệ được sử dụng rất phổ biến hiện nay. Chúng có topo dạng sao, như minh họa trên Hình 5.30. Trong topo hình sao có một thiết bị trung tâm được gọi là **hub** (đôi khi gọi là **bộ tập trung - concentrator**). Adapter trên mỗi nút có kết nối trực tiếp đến hub. Kết nối này gồm hai cặp dây đồng xoắn đôi, một để truyền và một để nhận. Tại mỗi đầu của kết nối có một connector (bộ nối) RJ-45 - giống như connector RJ-45 được sử dụng cho điện thoại thông thường. Chữ "T" trong 10BaseT và 100BaseT là viết tắt của "Twisted pair". Đối với 10BaseT và 100BaseT, khoảng cách tối đa giữa adapter và hub là 100m, vì vậy độ dài lớn nhất giữa hai nút là 200m. Chúng ta sẽ trình bày trong phần sau, khoảng cách này có thể được tăng nếu sử dụng các thiết bị như hub, bridge, switch.

Về bản chất, hub là repeater vì khi nhận được tín hiệu từ adapter, hub sẽ gửi tín hiệu đó đến tất cả các adapter khác. Theo cách này, mỗi adapter có thể (1) cảm nhận kênh truyền để xác định liệu kênh truyền có rỗi không và (2) phát hiện xung đột trong khi đang truyền dữ liệu. Nhưng hub được dùng phổ biến do có khả năng trợ giúp việc quản trị mạng. Ví dụ, nếu

adapter trục trặc và tiếp tục gửi frame Ethernet (gọi là jabbering adapter) thì mạng 10Base2 Ethernet sẽ sụp đổ vì không adapter nào có khả năng truyền thông nữa. Nhưng điều này không xảy ra với mạng 10BaseT vì hub sẽ phát hiện vấn đề và ngưng kết nối tới adapter đang trục trặc. Tính năng này có tính chất tự động, có nghĩa là không cần sự can thiệp bằng tay của người quản trị mạng. Hơn thế nữa, hầu hết hub có thể thu thập và báo cáo thông tin đến máy tính có kết nối trực tiếp đến hub. Máy tính kiểm tra này sẽ sử dụng giao diện đồ hoạ hiển thị các thông tin trạng thái của hub như băng thông, tỉ lệ xung đột, kích thước trung bình của frame v.v. Người quản trị mạng có thể sử dụng thông tin này không chỉ để kiểm tra và khắc phục lỗi mà còn để lập kế hoạch phát triển LAN trong tương lai.

Nhiều adapter Ethernet ngày nay là adapter 10/100 Mbps. Tức là chúng ta có thể sử dụng được dùng cả hai kiểu Ethernet: 10BaseT và 100BaseT. 100BaseT, đặc trưng của nó là sử dụng loại cáp xoắn kiểu 5 (loại cáp chất lượng cao với nhiều vỏ). Khác 10Base2 và 10BaseT, 100BaseT không sử dụng phương pháp mã hoá Manchester mà sử dụng phương pháp 4B5B có hiệu suất cao hơn: mỗi nhóm 5 chu kỳ đồng hồ được sử dụng để mã hóa 4 bit và cung cấp đủ thông tin cho phép đồng bộ hoá đồng hồ.

Chú ý rằng cả hai công nghệ 10BaseT và 100BaseT đều có thể sử dụng cáp quang, Cáp quang thường được sử dụng để kết nối đến hub. Giá thành của cáp quang cao do giá thành connector nhưng ưu điểm là khả năng chống nhiễu tuyệt vời. Chuẩn IEEE 802 cho phép LAN có thể trải rộng trên vùng địa lí lớn nếu sử dụng cáp quang để nối các nút nằm trên trục chính (backbone).

***Gigabit Ethernet***

Gigabit Ethernet là sự mở rộng của chuẩn Ethernet 10BaseT và 100BaseT. Với tốc độ truyền dữ liệu dạng thô là 1000 Mbps, Gigabit Ethernet vẫn duy trì khả năng tương thích hoàn toàn với các thiết bị Ethernet kiểu cũ. Chuẩn Gigabit Ethernet (IEEE802.3x), thực hiện các công việc sau:

- Sử dụng khuôn dạng frame Ethernet chuẩn (Hình 5.27), tương thích với công nghệ 10BaseT và 100BaseT. Điều này cho phép dễ dàng tích hợp Gigabit Ethernet vào các cơ sở đã cài đặt các thiết bị Ethernet



- Cho phép đường truyền point-to-point cũng như kênh truyền quảng bá dùng chung. Đường truyền poit-to-point dùng switch (xem phần 5.6) trong khi kênh truyền quảng bá sử dụng hub giống 10BaseT và 100BaseT. Trong thuật ngữ Gigabit Ethernet, hub được gọi là "buffered distributors".

- Sử dụng CSMA/CD cho kênh truyền quảng bá dùng chung. Để đạt được hiệu suất mong muốn, khoảng cách lớn nhất giữa các nút bị hạn chế chặt chẽ.

- Kênh truyền point-to-point có đặc tính song công, mỗi hướng truyền với tốc độ 1 Gbps.

- Giống 10BaseT và 100BaseT, Ethernet Gigabit có topo dạng sao với hub hoặc switch ở trung tâm (switch Ethernet sẽ được thảo luận trong phần 5.6). Gigabit Ethernet thường được sử dụng trên các backbone (trục chính) kết nối nhiều mạng cục bộ Ethernet 10BaseT và 100BaseT. Gigabit Ethernet có thể sử dụng loại cáp 5UTP hoặc cáp quang.

## 5.6 HUB, BRIDGE VÀ SWITCH

Cơ quan - các công ty, trường đại học – có đặc điểm gồm nhiều bộ phận con, mỗi bộ phận có mạng cục bộ Ethernet riêng. Tất nhiên, cơ quan muốn kết nối mạng cục bộ của các bộ phận. Trong mục này chúng ta nghiên cứu một số hướng tiếp cận để kết nối các LAN với nhau. Chúng ta sẽ nghiên cứu ba hướng tiếp cận: sử dụng hub, bridge và switch.

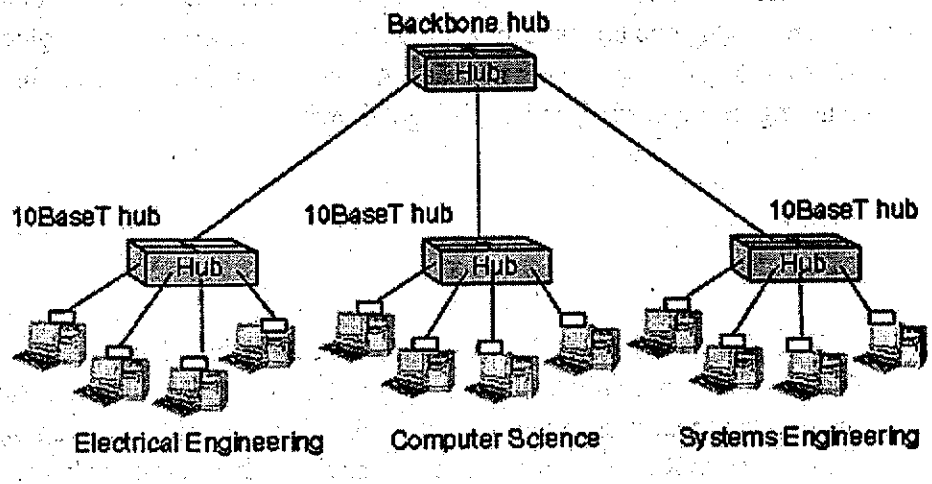
### 5.6.1 Hub

Cách đơn giản nhất để kết nối LAN là sử dụng hub. Hub là thiết bị đơn giản sao chép tín hiệu đến từ một cổng ra tất cả các cổng còn lại. Bản chất của hub là repeater, thao tác trên bit, vì thế chúng là thiết bị ở tầng vật lý. Khi bit đi vào một cổng, hub sẽ truyền bit này qua tất cả các cổng khác.

Hình 5.31 minh họa kết nối mạng LAN của ba khoa trong một trường đại học qua hub. Mỗi khoa có một mạng Ethernet 10BaseT để cán bộ và sinh viên của khoa sử dụng. Mỗi máy tính của khoa kết nối điểm nối điểm đến hub. Hub thứ tư, được gọi là backbone hub (hub trục chính) có kết nối điểm nối điểm đến các hub của khoa được sử dụng để liên kết LAN của ba khoa. Thiết kế được chỉ ra trong Hình 5.31là **thiết kế hub nhiều tầng (multi-tier hub design)** vì các hub được tổ chức trong hệ thống phân cấp. Có thể tạo thiết kế nhiều tầng - ví dụ, một tầng dành cho cấp Khoa, một tầng dành cho các trường trong trường đại học lớn (ví dụ: Trường công nghệ, trường kinh tế ...) và một tầng ứng với mức cao nhất của trường.

Trong thiết kế nhiều tầng, chúng ta coi toàn bộ mạng liên kết với nhau là mạng cục bộ LAN và coi mỗi phân mạng LAN ứng với một khoa (nghĩa là hub của khoa và các máy tính nối tới hub đó) là **LAN segment**. Chú ý rằng tất cả LAN segment trong Hình 5.31 thuộc về cùng một vùng xung đột, nghĩa là bất cứ lúc nào nhiều nút trên LAN truyền dữ liệu tại cùng một thời điểm thì sẽ phát sinh xung đột và tất cả những nút liên quan bắt đầu quá trình "exponential backoff".

Mạng cục bộ cấp khoa liên kết tới hub trục chính có nhiều ưu điểm. Đầu tiên và quan trọng nhất, nó cung cấp môi trường truyền thông giữa các khoa với nhau. Thứ hai, nó mở rộng khoảng cách tối đa giữa bất cứ cặp nút nào trên LAN. Ví dụ, với 10BaseT khoảng cách lớn nhất giữa nút và hub là 100m; vì thế trong LAN segment, khoảng cách lớn nhất giữa hai nút lên tới 200m.




**Hình 5.31 Kết nối qua hub**



Nếu kết nối qua hub, khoảng cách tối đa này có thể được mở rộng vì khoảng cách giữa các hub kết nối trực tiếp với nhau có thể là 100m khi sử dụng cáp xoắn đôi (và khoảng cách này sẽ tăng khi dùng cáp quang). Ưu điểm thứ ba là thiết kế nhiều tầng giảm nguy cơ sụp đổ của toàn hệ thống. Giả sử nếu bất kỳ hub của khoa nào đó bị trục trặc, hub trục chính có thể phát hiện vấn đề và phong tỏa kết nối tới hub khoa đó, như vậy các khoa còn lại vẫn có thể tiếp tục hoạt động và truyền thông trong khi hub bị lỗi không hoạt động.

Tuy vậy hub cũng có nhược điểm. Đầu tiên và có lẽ quan trọng nhất là khi sử dụng hub trung tâm, miền xung đột của mạng cục bộ của từng khoa trở thành miền xung đột chung của toàn bộ hệ thống. Xét ví dụ minh họa trên Hình 5.31. Trước khi kết nối ba khoa, mạng cục bộ mỗi khoa có băng thông cực đại là 10Mbps, vì vậy thông lượng toàn bộ tối đa của 3 LAN là 30Mbps. Nhưng khi mạng LAN của ba khoa được kết nối vào hub trung tâm, tất cả máy tính của ba khoa thuộc về cùng một miền xung đột, và thông lượng bị giảm xuống 10Mbps.

Hạn chế thứ hai là nếu các khoa khác nhau sử dụng các công nghệ Ethernet khác nhau thì không có khả năng để kết nối chúng vào hub trung tâm. Ví dụ, nếu một khoa sử dụng 10BaseT và các khoa còn lại sử dụng 100BaseT, thì không thể kết nối chúng với nhau vì hub về bản chất là repeater.

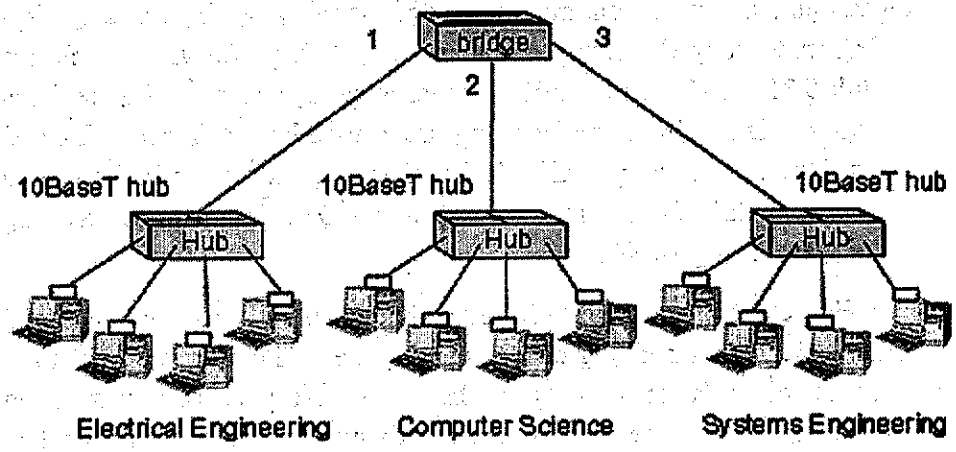
Hạn chế thứ ba là mỗi công nghệ Ethernet (10Base2, 10BaseT, 100BaseT, ...) có giới hạn về số nút, khoảng cách tối đa giữa hai máy tính trong miền xung đột và số tầng tối đa trong thiết kế nhiều tầng. Những hạn chế này hạn chế tổng số máy tính có thể kết nối đến mạng cục bộ cũng như phạm vi địa lí của mạng cục bộ nhiều tầng.

## 5.6.2 Bridge

Khác với hub (là thiết bị tầng vật lý), bridge có thể xử lý trên frame Ethernet, vì vậy nó là thiết bị tầng 2. Thực tế, bridge chính là thiết bị chuyển mạch gói thực hiện việc chuyển và lọc frame căn cứ trên địa chỉ vật lý. Khi

frame đến từ một cổng nào đó của bridge, bridge không gửi frame đến tất cả các cổng khác. Bridge sẽ xác định địa chỉ đích tầng 2 (địa chỉ vật lý) của frame và chuyển frame đến cổng duy nhất dẫn về đích.

Hình 5.32 minh họa ba khoa trong ví dụ trước kết nối tới bridge. Ba chữ số bên cạnh bridge là số thứ tự các cổng của bridge. Khi các khoa được kết nối qua bridge như trong hình 5.27 chúng ta vẫn coi mạng kết nối toàn bộ là LAN và mạng của mỗi khoa là LAN segment giống như ở phần trước. Nhưng khác với thiết kế hub nhiều tầng trong hình 5.26, mỗi LAN segment bây giờ là một miền xung đột đã được cô lập.




**Hình 5.32 Kết nối bằng Bridge**

Bridge có thể khắc phục nhiều vấn đề của hub. Thứ nhất, bridge cho phép truyền thông giữa các khoa trong khi cô lập miền xung đột của mỗi khoa. Thứ hai, bridge có thể kết nối các công nghệ LAN khác nhau (Ethernet 10Mbps và 100Mbps chẳng hạn). Thứ ba, không bị giới hạn về khoảng cách tối đa trong mạng cục bộ khi sử dụng bridge để kết nối các LAN segment. Về lý thuyết mà nói sử dụng bridge có thể xây dựng một mạng LAN trải rộng trên toàn thế giới.

### Bridge Fowarding và Filtering (chuyển tiếp và lọc)

**Lọc (Filtering)** là khả năng xác định liệu sẽ chuyển tiếp frame đến cổng nào đó hay loại bỏ luôn frame. **Chuyển tiếp (Fowarding)** là khả năng xác định cổng kế tiếp để chuyển frame đi. Bridge thực hiện hai chức năng



này nhờ **bảng bridge (bridge table)**. Mỗi hàng trong bảng ứng với một nút đích trên mạng LAN. Tuy vậy bảng bridge không nhất thiết phải chứa tất cả các hàng cho mọi nút trong mạng. Mỗi hàng trong bảng bridge gồm có (1) địa chỉ vật lý của nút, (2) cổng bridge có thể dẫn đến nút đó, (3) thời điểm thiết lập hàng đó trong bảng. Ví dụ về bảng bridge cho LAN trong Hình 5.32 được chỉ ra trong Hình 5.33. Mặc dù quá trình chuyển frame có vẻ tương tự quá trình chuyển gói dữ liệu datagram trong chương 4, nhưng chúng ta sẽ thấy ngay chúng hoàn toàn khác nhau. Ở đây, chú ý rằng địa chỉ bridge sử dụng là địa chỉ vật lý chứ không phải là địa chỉ của tầng mạng (IP). Chúng ta cũng thấy ngay bảng bridge được xây dựng khác với bảng định tuyến.

| Address | Interface | Time |
|---|---|---|
| 62-FE-F7-11-89-A3 | 1 | 9:32 |
| 7C-BA-B2-B4-91-10 | 3 | 9:36 |
| .... | .... | .... |

**Hình 5.33 Một phần bảng bridge cho LAN trong hình 5.26**

Để hiểu chức năng lọc và chuyển tiếp làm việc như thế nào, giả sử frame với địa chỉ đích DD-DD-DD-DD-DD-DD đến bridge từ cổng x. Bridge tìm kiếm trên bảng lọc hàng ứng với địa chỉ vật lý DD-DD-DD-DD-DD-DD để tìm ra cổng y tương ứng - là cổng sẽ dẫn đến nút có địa chỉ đích DD-DD-DD-DD-DD-DD. Chúng ta sẽ thấy điều gì sẽ xảy ra nếu không có giao diện y như thế trong bảng:

- Nếu x = y, thì frame đến từ segment chứa adapter DD-DD-DD-DD-DD-DD. Không cần chuyển frame đến bất kỳ cổng nào khác, bridge thực hiện chức năng lọc bằng cách loại bỏ frame.

- Nếu x ≠ y thì frame cần được gửi đến segment nào đó qua cổng y. Bridge thực hiện chức năng chuyển tiếp bằng cách đặt frame vào bộ đệm ra của cổng y.

Những quy tắc đơn giản này cho phép bridge cô lập các miền xung đột của các LAN segment khác nhau. Những quy tắc này cũng cho phép hai cặp thiết bị trên hai segment khác nhau truyền đồng thời mà không bị xung đột.

Xét những qui tắc này cho mạng minh họa trên Hình 5.32 và bảng bridge tương ứng trên Hình 5.33. Giả sử frame với địa chỉ đích 62-EF-F7-11-89-A3 được gửi đến bridge qua cổng 1. Bridge kiểm tra bảng và thấy rằng đích nằm trên LAN segment được kết nối đến cổng 1 (là mạng LAN của khoa Electrical Engineering). Điều này có nghĩa là frame thực sự đã được quảng bá trên LAN segment này. Do vậy bridge sẽ lọc frame (nghĩa là, loại bỏ frame – vì thực sự máy tính đích cũng đã nhận được frame này rồi). Giả sử frame với địa chỉ đích như vậy đến từ cổng 2. Bridge lại kiểm tra bảng và thấy rằng đích nằm ở trên hướng ứng với cổng 1, do đó bridge chuyển frame ra cổng 1. Rõ ràng rằng nếu bảng bridge đầy đủ và chính xác, bridge cho phép truyền thông giữa các khoa nhưng cô lập các miền xung đột.

Khi có frame để gửi chuyển tiếp, hub (hoặc repeater) gửi frame lên trên đường truyền mà không quan tâm xem có thiết bị nào khác đang chiếm dụng đường truyền không. Trái lại, bridge sẽ sử dụng thuật toán CSMA/CD trong phần 5.3 khi cần gửi đi frame. Tức là bridge sẽ không truyền ngay nếu như có nút khác trên LAN segment cũng đang truyền; hơn nữa, bridge cũng sử dụng thuật toán exponential backoff khi có xung đột. Vì vậy, cổng của bridge hoạt động giống như adapter của nút. Nhưng về mặt kỹ thuật mà nói, bridge không phải là adapter vì chúng không có địa chỉ vật lý. Chú ý rằng adapter của nút luôn luôn chèn địa chỉ vật lý của nó vào trường địa chỉ nguồn trong tất cả các frame nó gửi đi. Điều này cũng đúng cho adapter của router. Ngược lại bridge không thay đổi địa chỉ nguồn của frame.

Một tính năng quan trọng của bridge là khả năng kết nối các LAN segment sử dụng những công nghệ Ethernet khác nhau. Ví dụ nếu trong Hình 5.32, khoa Electrical Engineering sử dụng Ethernet 10BaseT, Khoa Computer Science sử dụng Ethernet 100BaseT và khoa System Engineering sử dụng Ethernet 10BaseT thì bridge có thể kết nối cả 3 segment trên. Với bridge Ethernet Gigabit có thể sử dụng đường truyền 1 Gbps nối tới router. Như chúng ta đã đề cập ban đầu, hub không có tính năng có thể kết nối các công nghệ với tốc độ truyền khác nhau.

Khi sử dụng bridge làm thiết bị kết nối, thì về lý thuyết LAN không bị giới hạn bởi phạm vi địa lý. Trên lý thuyết chúng ta có thể xây dựng mạng LAN trải rộng toàn cầu bằng kết nối các hub qua bridge. Theo thiết kế



này, mỗi hub là một miền xung đột và do đó LAN không bị giới hạn. Tuy nhiên sau đây chúng ta sẽ thấy rằng trong mạng lớn người ta sẽ kết nối qua router, chứ không sử dụng bridge.

**Tự học (Self-Learning)**

Đặc tính tuyệt vời (nhất là đối với những người quản trị mạng) của bridge là khả năng tự học. Bảng lọc của bridge được xây dựng tự động mà không cần bất cứ sự can thiệp nào từ phía người quản trị. Nói cách khác, bridge có khả năng tự học. Khả năng này được thực hiện như sau:

Bảng bridge khởi đầu là rỗng.

Khi frame đến cổng nào đó và địa chỉ đích của frame không có trong bảng, thì bridge sẽ chuyển frame đến bộ đệm ra của tất cả các cổng còn lại (tại mỗi cổng, frame được truyền lên LAN segment nhờ CSMA/CD)

Khi nhận được frame, bridge lưu trữ: (1) địa chỉ vật lý trong trường địa chỉ nguồn của frame, (2) cổng nhận được frame, (3) thời gian hiện tại. Như vậy bridge ghi nhớ được vị trí LAN segment của nút gửi. Nếu nút nào đó trong LAN gửi frame qua bridge thì bridge sẽ xác định được cổng để đi đến nút đó.

Khi địa chỉ đích của frame có trong bảng, thì bridge chuyển frame đến cổng thích hợp.

Bridge sẽ xoá địa chỉ trong bảng nếu adapter có địa chỉ đó không tiếp tục gửi frame trong khoảng thời gian xác định. Theo cách này, nếu PC được thay thế bởi PC khác (với adapter khác) thì địa chỉ vật lý của PC trước sẽ bị bridge xoá.

Xét quá trình tự học của bridge trong Hình 5.32 và bảng bridge tương ứng trong Hình 5.33. Giả sử rằng tại thời điểm 9:39 bridge nhận được một frame có địa chỉ gửi là 01-12-23-45-56 đến cổng 2. Giả sử, địa chỉ này chưa có trong bảng, bridge sẽ bổ sung một hàng mới trong bảng như chỉ ra trên Hình 5.34.

- Tiếp tục với ví dụ này, giả sử rằng "tuổi thọ" của mỗi hàng trong bảng là 60 phút và máy tính với địa chỉ 62-FE-F7-11-89-A3 không gửi đi

bất kỳ frame nào qua bridge trong khoảng thời gian từ 9:32 đến 10:32 thì lúc 10:32, bridge sẽ xóa địa chỉ này khỏi bảng.

Bridge là thiết bị theo kiểu **"cắm vào là chạy" (plug and play)** bởi vì nó không cần sự can thiệp của người quản trị mạng. Người quản trị mạng chỉ cần cắm connector vào các cổng của bridge. Người quản trị mạng không cần thiết lập cấu hình cho bảng bridge trong thời gian cài đặt hay khi máy tính tách khỏi LAN segment. Do đặc tính này, bridge được xem là trong suốt (transparent).

| Địa chỉ MAC | Interface | Time |
|---|---|---|
| 01-12-23-34-45-56 | 2 | 9:39 |
| 62-FE-F7-11-89-A3 | 1 | 9:32 |
| 7C-BA-B2-B4-91-10 | 3 | 9:36 |
| .... | .... | .... |

**Hình 5.34 Bảng lọc của bridge**

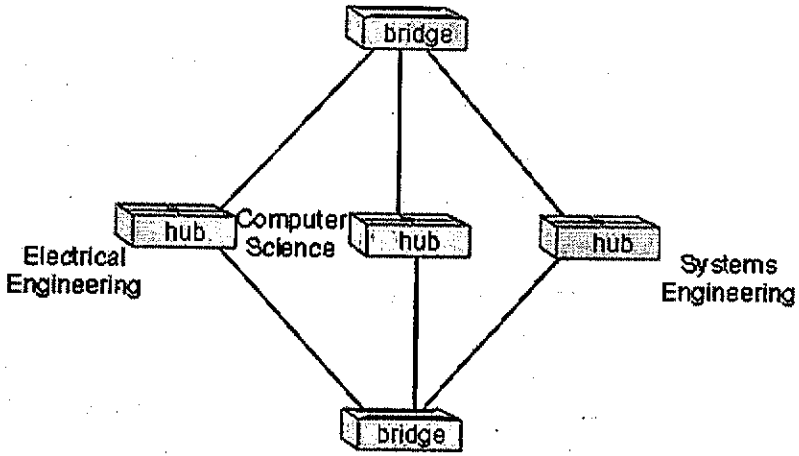
### *Spanning tree*

Nếu hoàn toàn kết nối LAN segment theo kiểu phân cấp thì khi hub hoặc bridge gần đỉnh bị hỏng, thì một phần lớn LAN sẽ không được kết nối. Chính vì lý do này người ta thường xây dựng mạng với nhiều đường nối giữa các LAN segment. Một ví dụ về mạng như thế được minh hoạ trong Hình 5.35.

Nhiều đường dư thừa giữa các LAN segment làm giảm khả năng sụp đổ của toàn bộ hệ thống. Nhưng có nhiều đường dẫn giữa các segment cũng sẽ phát sinh ra nhiều vấn đề - một frames có thể di chuyển vòng quanh hay được nhân bản lên nhiều lần trong mạng cục bộ. Để hình dung ra điều này, giả sử bảng bridge trong hình 5.30 rỗng và máy tính trong khoa Electrical Engineering gửi frame đến máy tính trong khoa Computer Science. Khi frame đến hub Electrical Engineering, hub sẽ sinh ra hai bản sao của frame và gửi mỗi bản đến hai bridge. Khi mỗi bridge nhận được frame, nó sẽ tạo ra 2 bản sao của frame, một bản gửi đến hub của khoa System Engineering và



bản kia đến hub của khoa Computer Science. Vì cả hai bridge cùng làm như vậy, sẽ có 4 frame giống hệt nhau trong LAN. Frame có thể được nhân bản liên tục nếu bridge không biết nút nhận nằm ở đâu (chú ý rằng để địa chỉ vật lý của máy tính nhận có trong bảng lọc, thì trước đó máy tính nhận phải gửi đi một frame qua bridge). Trong trường hợp này, số bản sao của frame gốc tăng theo hàm số mũ, làm tràn ngập toàn bộ mạng.




**Hình 5.35 Kết nối dư thừa**

Để ngăn ngừa những tình huống nêu trên, bridge sử dụng giao thức **spanning tree**. Trong giao thức spanning tree, bridge truyền thông với bridge khác trên LAN để xác định spanning tree, nghĩa là, một tập con của topo ban đầu không có vòng lặp. Sau khi xác định được spanning tree, bridge chỉ kết nối với các cổng phù hợp để tạo spanning tree từ topo ban đầu. Ví dụ trong hình 5.30, spanning tree được hình thành bằng cách bridge phía trên phong tỏa kết nối cổng kết nối đến Eletrical Engineering và bridge phía dưới phong tỏa cổng kết nối đến System Engineering. Với các cổng bị phong tỏa và loại bỏ được các vòng lặp, frame sẽ không lặp và nhân bản. Nếu khi nào đó một liên kết trong spanning tree bị lỗi, bridge có thể kết nối lại giao diện đã bị phong tỏa, kích hoạt thuật toán spanning tree lần nữa và xác định spanning tree mới.

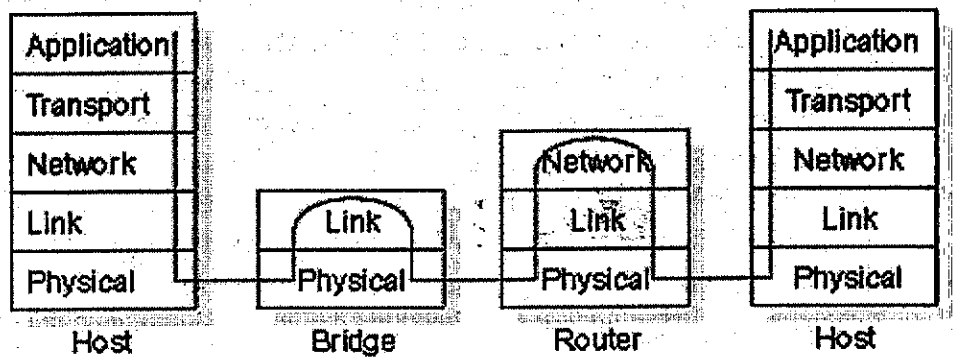
### *Phân biệt Bridge và Router*

Như đã trình bày trong chương 4, router là thiết bị chuyển mạch gói theo kiểu store-and-forward và chuyển gói tin theo địa chỉ tầng mạng. Mặc

dù cũng là thiết bị chuyển mạch kiểu store-and-forward, nhưng điểm khác biệt cơ bản giữa bridge với router là bridge sử dụng địa chỉ vật lý. Như vậy router là thiết bị chuyển mạch gói ở tầng 3 trong khi bridge là thiết bị chuyển mạch gói ở tầng 2.

Người quản trị mạng sẽ phải lựa chọn giữa bridge và router khi cài đặt thiết bị kết nối. Ví dụ, với hệ thống mạng trong Hình 5.32, người quản trị mạng có thể lựa chọn router thay vì lựa chọn bridge. Thật vậy, router cũng sẽ cô lập ba miền xung đột trong khi vẫn cho phép truyền thông giữa các khoa. Như vậy cả bridge và router đều có thể làm thiết bị kết nối. Vậy ưu và nhược điểm giữa chúng là gì ?

Đầu tiên ta xét về bridge. Như đã đề cập trên, bridge là thiết bị kiểu "cắm vào là chạy" - tính năng được tất cả các nhà quản trị mạng ưa thích. Bridge cũng có tốc độ lọc và chuyển gói dữ liệu cao – như minh họa trên Hình 5.35, bridge chỉ phải xử lý gói dữ liệu của tầng 2 trong khi router phải xử lý gói dữ liệu của tầng 3. Mặt khác, giao thức spanning tree hạn chế topo của toàn bộ mạng. Điều này có nghĩa là tất cả các frame chỉ được chuyển trên spanning tree, thậm chí khi có nhiều đường dẫn trực tiếp (nhưng bị phong tỏa) giữa nguồn và đích. Sự hạn chế của spanning tree cũng tập trung vào khả năng tải trên đường truyền spanning tree khi nó có thể đã được lan truyền đến tất cả các đường truyền khác của mạng cũ. Hơn nữa bridge không đưa ra bất cứ sự bảo vệ nào để chống lại sự phát ra hàng loạt - nếu máy tính bị lỗi và truyền đi một luồng frame Ethernet liên tục, bridge sẽ chuyển tất cả những frame này khiến toàn bộ mạng có thể bị sụp đổ.




**Hình 5.36 Luồng đi của gói dữ liệu trong máy tính, bridge và router**

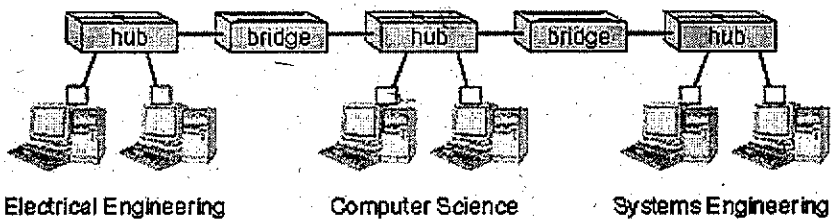


Bây giờ xét đến ưu và nhược điểm của router. Nói chung địa chỉ mạng thường phân cấp (không phẳng như địa chỉ vật lý), gói dữ liệu chắc chắn không quay vòng lại qua router ngay cả khi có nhiều đường đi (Thực sự gói dữ liệu có thể quay vòng nếu cấu hình bảng định tuyến của router bị đặt sai, nhưng như chúng ta đã học trong chương 4, IP sử dụng trường TTL trong tiêu đề gói dữ liệu để hạn chế chuyện này). Vì vậy, gói dữ liệu không bị giới hạn chuyển trong spanning tree, nó có thể sử dụng đường dẫn tốt nhất giữa nguồn và đích. Các router không bị giới hạn trong spanning tree nên Internet có thể có topo cực kỳ phong phú, ví dụ nhiều đường truyền giữa châu Âu và Bắc Mỹ. Một đặc tính quan trọng khác của router là tạo ra "firewall" (bức tường lửa) chống lại sự phát tán liên tục (quảng bá storm) ở tầng 2. Có lẽ yếu điểm duy nhất của router là không có khả năng "cắm vào là chạy"- cần cấu hình địa chỉ IP cho chúng và các máy tính kết nối đến chúng. Hơn nữa, thời gian xử lý gói tin của router thường lâu hơn bridge vì chúng phải xử lí các trường tiêu đề của tầng 3.

Với cả ưu và nhược điểm như đã thảo luận trên, vậy khi nào mạng sử dụng bridge, khi nào sử dụng router? Thông thường một mạng nhỏ gồm vài trăm máy tính nằm trên một số LAN segment chỉ cần sử dụng Bridge. Nhưng với những mạng lớn gồm hàng nghìn máy tính sẽ cần tới nhiều router bên trong mạng (bên cạnh bridge). Những router này cung cấp khả năng cô lập mạnh hơn, kiểm soát việc gửi tràn ngập.

***Kết nối LAN segment qua các trục chính (backbone)***

Lại xét ví dụ kết nối mạng Ethernet trong 3 khoa trên Hình 5.37 với bridge. Thiết kế này sử dụng hai bridge, mỗi bridge có hai cổng. Bridge thứ nhất kết nối hai khoa Electrical Engineering và Computer Sciense. Bridge kia kết nối khoa Computer Science với Systems Engineering. Mặc dù, bridge hai cổng rất phổ biến do giá rẻ và đơn giản, nhưng mô hình thiết kế trong Hình 5.37 không được ưa chuộng. Có hai lý do, thứ nhất, nếu hub của Computer Science bị hỏng thì máy tính ở hai khoa Electrical Engineering và Systems Engineering không thể trao đổi được với nhau. Thứ hai truyền thông giữa hai khoa Electrical Engineering và System Engineering phải thông qua Computer Science, dễ gây xung đột trong LAN segment của Computer Science.

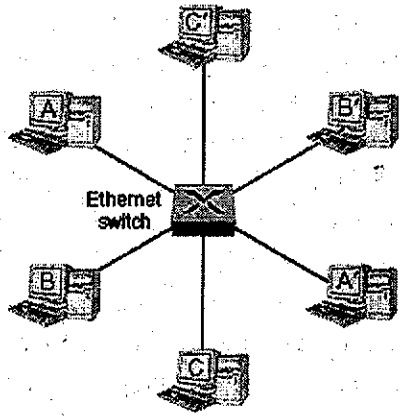



**Hình 5.37 Kết nối không có backbone**

Một nguyên tắc quan trọng định hướng dẫn việc kết nối các LAN segment khác là sử dụng đường trục chính (backbone) – là một mạng có kết nối trực tiếp đến tất cả các LAN segment. Khi LAN có một trục chính thì mỗi cặp LAN segment có thể truyền thông mà không cần thông qua LAN segment thứ ba. Trong thiết kế ở hình 5.37, bridge ba cổng đóng vai trò một backbone.

## 5.6.3. Switch

Cho đến giữa những năm 90 ba loại thiết bị kết nối mạng cục bộ được sử dụng chủ yếu là: hub (repeater), bridge, router. Gần đây, một thiết bị trở nên rất thông dụng là switch Ethernet. Switch Ethernet được hỗ trợ bởi ngành công nghiệp sản xuất thiết bị mạng. Về thực chất, switch là là bridge nhiều cổng có hiệu suất cao. Giống bridge, switch chuyển và lọc frame căn cứ vào địa chỉ vật lý đích, tự động xây dựng bảng lọc khi có frame đi qua. Điểm khác biệt quan trọng nhất giữa bridge và switch là bridge có ít cổng (từ 2 đến 4) trong khi switch có thể có nhiều cổng hơn.



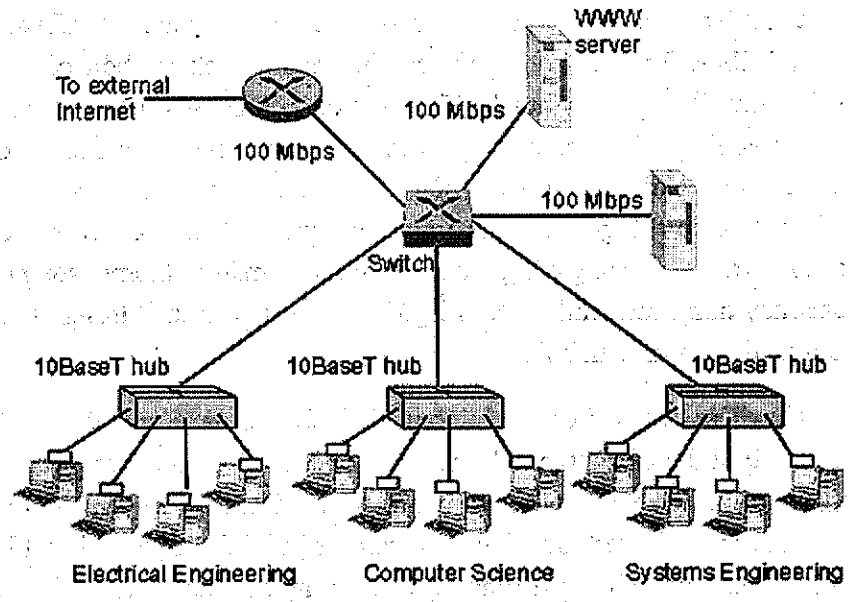

**Hình 5.38 Switch Ethernet cung cấp truy cập Ethernet dành riêng đến 6 máy tính**



Có thể mua switch có các cổng với tốc độ khác nhau 10 Mbps, 100 Mbps và 1Gbps. Ví dụ, một người có thể mua switch có bốn cổng 100 Mbps, hai mươi cổng 10 Mbps hoặc switch có bốn cổng 100 Mbps và một cổng 1 Gbps. Dĩ nhiên, nhiều cổng và tốc độ truyền của cổng càng cao thì switch càng đắt. Nhiều switch vận hành trong chế độ song công hoàn toàn, nghĩa là chúng có thể gửi và nhận frame tại cùng một thời điểm trên cùng một cổng. Với switch song công (cùng với bộ card mạng Ethernet song công trên các máy tính), máy tính A có thể gửi file đến máy tính B trong khi máy tính B gửi file đến máy tính A.

Ưu điểm của switch nhiều cổng là ở chỗ dễ dàng kết nối trực tiếp giữa các máy tính với switch. Khi có đường kết nối trực tiếp song công với switch, máy tính có thể truyền (và nhận) frame ở tốc độ truyền tối đa của adapter, đặc biệt adapter máy tính luôn cảm nhận kênh truyền rỗi và không bao giờ bị xung đột. Trong trường hợp này, máy tính được xem có **đường dùng riêng (dedicated link)**. Trên Hình 5.38 switch Ethernet cung cấp đường dùng riêng cho 6 máy tính. Các đường truy cập dùng riêng này cho phép đồng thời A gửi file đến A' trong khi B đang gửi file đến B' và C đang gửi đến C'. Nếu mỗi máy tính sử dụng adapter card 10 Mbps thì toàn bộ băng thông của hệ thống là 30 Mbps. Nếu A và A' có adapter 100 Mbps và những máy tính còn lại có adapter 10 Mbps, thì băng thông có thể lên tới 120 Mbps.

Hình 5.39 minh họa cách kết nối một trường đại học với nhiều khoa và một một số server quan trọng qua hub, switch và router. Trên Hình 5.39 mỗi khoa là một LAN segment sử dụng hub 10 Mbps. Vì mỗi hub có kết nối đến switch nên các khoa hoàn toàn có khả năng trao đổi dữ liệu với nhau. Server cho dịch vụ Web và email đều có đường dùng riêng 100 Mbps đến switch. Cuối cùng router sẽ kết nối toàn bộ hệ thống ra Internet, và router cũng có đường dùng riêng 100 Mbps đến switch. Chú ý switch này có ít nhất 3 cổng 10 Mbps và 3 cổng 100 Mbps.




**Hình 5.39 Mạng cơ quan sử dụng phối hợp hub, switch và router**

***Chuyển mạch xuyên suốt (Cut – Through)***

Ngoài việc có nhiều cổng, hỗ trợ nhiều môi trường và tốc độ truyền khác nhau, có chức năng quản trị mạng, các nhà sản xuất switch Ethernet thường quảng cáo sản phẩm của mình có khả năng gửi **xuyên suốt** (**cut-through**) chứ không phải kiểu store-and-forward như router và bridge. Khác biệt giữa store-and-forward và cut-through không lớn. Xét một gói dữ liệu chuyển qua thiết bị chuyển mạch (có thể là router, bridge hoặc switch). Gói tin đến switch từ một cổng nào đó và cần chuyển ra một cổng nào đó. Tại bộ đệm ở cổng ra của gói tin có thể có nhiều gói tin khác đang chờ chuyển. Khi đó store-and-forward và cut-through giống nhau. Hai công nghệ chuyển mạch này chỉ khác nhau khi bộ đệm cổng ra rỗng.

Khi gửi gói tin tới thiết bị chuyển kiểu store-and-forward, thiết bị sẽ thu và lưu trữ **toàn bộ** gói tin trước khi chuyển lên đường ra. Trong trường hợp bộ đệm ở cổng ra rỗng, phải thu thập toàn bộ gói tin rồi mới được chuyển đi (store and forward), việc này sẽ góp phần làm tăng thời gian trễ. Giới hạn độ trễ này là L/R, trong đó L là độ dài của gói tin và R là tốc độ truyền của cổng đến. Chú ý rằng gói tin chỉ chịu độ trễ này nếu bộ đệm cổng ra rỗng trước khi toàn bộ gói tin đến switch.

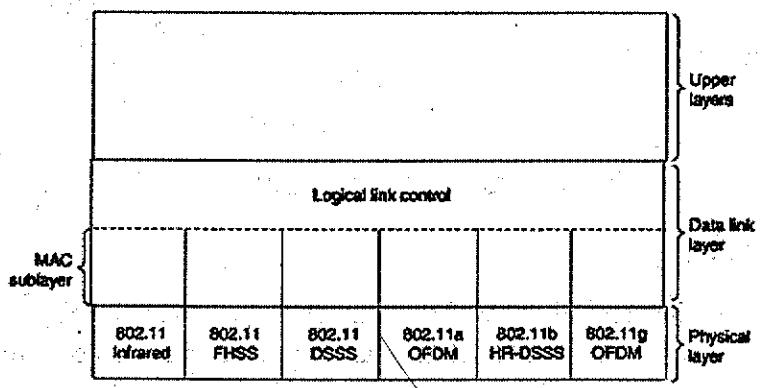


Với chuyển mạch kiểu cut-through, nếu buffer rỗng trước khi toàn bộ gói tin đến, switch có thể bắt đầu gửi đi phần trước trong khi đang nhận phần sau của gói tin. Tất nhiên trước khi truyền gói tin trên cổng ra, phải xác định được trường địa chỉ đích. (Thời gian trễ này không thể tránh khỏi đối với tất cả các loại chuyển mạch vì switch phải xác định cổng ra thích hợp). Tóm lại, trong chuyển mạch kiểu cut-through, gói tin không cần được "lưu trữ" đầy đủ trước khi chuyển tiếp đi mà gói tin sẽ được chuyển ngay khi cổng ra rỗi. Nếu cổng ra nối với mạng đa truy cập có chung môi trường truyền với những máy tính khác (ví dụ nối đến hub) thì switch phải "lắng nghe" để kiểm tra kênh truyền có rỗi không trước khi chuyển.

## 5.8. MẠNG LAN KHÔNG DÂY

### 5.8.1 Giới thiệu chung

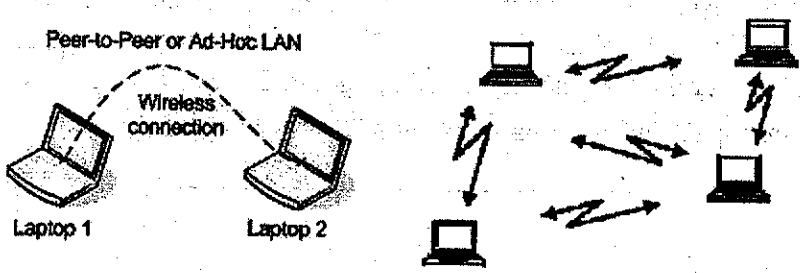
Các đặc tả về mạng LAN không dây ứng với tầng vật lý và tầng liên kết dữ liệu trong mô hình OSI. Thường tầng vật lý ở đây xác định việc sử dụng kênh truyền nào cũng như độ lớn của tín hiệu. Các chuẩn WLAN được IEEE đặc tả trong họ giao thức IEEE 802.11 chủ yếu sử dụng tia hồng ngoại hoặc dải phổ tự do. Dải phổ này còn được gọi là dải ISM (Industry, Science, Medicine) dùng trong các ứng dụng công nghiệp, khoa học và y tế.




**Hình 5.40 Vị trí các tầng con trong mạng LAN không dây**

Chuẩn 802.11 đưa ra năm 1997 xác định ba kỹ thuật truyền được sử dụng ở tầng vật lý. Kỹ thuật hồng ngoại (giống như trong các thiết bị điều khiển tivi từ xa). Hai kỹ thuật còn lại sử dụng sóng radio có bước sóng ngắn là công nghệ FHSS và DSSS. Băng tần hai công nghệ này là băng tần tự do (2.4GHz ISM). Tốc độ truyền theo những công nghệ này tương đối thấp (1-2 Mbps) và có phạm vi phủ sóng khả bé (để giảm thiểu xung đột). Đến năm 1999, hai kỹ thuật mới có tốc độ cao hơn được đưa ra là OFDM và HR-DSSS với tốc độ 54Mbps, 11Mbps tương ứng. Chú ý rằng các kỹ thuật này ứng với tầng Vật lý (Hình 5.40).

Nhiệm vụ của tầng liên kết dữ liệu ở đây là tổ chức việc truy cập đường truyền, đồng bộ hóa frame, kiểm soát tài nguyên. Cơ chế truy cập thực hiện chức năng điều phối phân tán (DCF – Distributed Coordination Function) được cài đặt ở tất cả các trạm (máy tính) có thiết bị thu phát không dây. Có hai kiểu thiết bị chính: Trạm di động (mobile station, chẳng hạn laptop) và Điểm truy cập (Access Point - AP, có nhiệm vụ chuyển tiếp dữ liệu giữa các trạm di động hay giữa trạm di động với mạng LAN cố định). Có hai kiểu kết nối của mạng LAN không dây: kiểu có cơ sở hạ tầng và kiểu không có cơ sở hạ tầng (adhoc).




Hình 5.41 Mạng Adhoc LAN

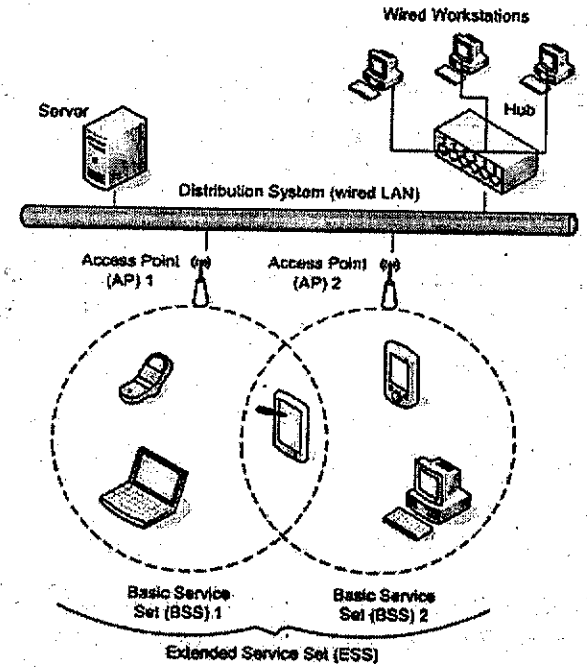
## Adhoc WLAN

Trong kiểu kết nối adhoc, hai trạm kết nối trực tiếp với nhau không qua AP (Hình 5.41).Trong kiểu kết nối này, các trạm làm việc có thể đóng vai trò server để chuyển tiếp dữ liệu. Hai trạm làm việc vẫn có thể trao đổi dữ liệu ngay cả khi chúng không nhận tín hiệu trực tiếp từ nhau.



## WLAN có cơ sở hạ tầng

Trong kiểu kết nối này (Hình 5.42), hai trạm chỉ có thể trao đổi dữ liệu với nhau qua AP. Thông thường, AP được đính vào tường (trong một văn phòng) và có kết nối với mạng LAN cố định. Bên cạnh chức năng chính là trung chuyển các gói tin giữa các trạm và giữa trạm với mạng LAN có dây, AP có thể thực hiện chức năng điều phối điểm (point coordinating function - PCF) cho phép truyền thông giữa các nút dựa trên việc cấp phát tài nguyên tài nguyên (thời gian, băng thông...).




Hình 5.42 Mạng LAN có cấu trúc

Đa phần tầng MAC trong họ giao thức IEEE WLAN có cơ chế truy cập tương tự mạng Ethernet. Ethernet sử dụng đa truy cập sóng mang có phát hiện xung đột (CSMA/CD). Tuy nhiên đối với mạng không dây, việc phát hiện xung đột không hiệu quả do độ suy hao năng lượng của tín hiệu theo khoảng cách rất lớn. Thay vì sử dụng cơ chế phát hiện, đa phần các mạng không dây sử dụng cơ chế tránh xung đột (collision avoidance). Ý tưởng chính của cơ chế này là đảm bảo giữa hai lần truyền gói tin liên tiếp phải có một khoảng thời gian tối thiểu.

## 5.8.2 Lớp giao thức IEEE 802.11

Trong họ giao thức 802.11, tầng MAC xác định cách thức phân phối kênh truyền – tức là tại một thời điểm, nút nào được quyền truyền dữ liệu. Tầng phía trên của MAC – tầng LLC (Logical Link Control) có nhiệm vụ "che dấu" các đặc điểm khác nhau của tầng MAC với tầng mạng.

### Tầng con Medium Access Control (MAC)

Chức năng chính của mạng LAN là chia sẻ tài nguyên giữa các máy tính trong một khu vực nhỏ, do vậy giống như Ethernet, nhiệm vụ của tầng MAC là xác định cụ thể từng giao diện của các máy tính trên mạng. Bên cạnh chức năng chính tổ chức truy cập kênh truyền và cơ chế điều phối đa truy cập, MAC còn có một số chức năng chính sau đâu:

**Cấu hình Mạng.** Đối với mạng LAN có dây, cấu hình mạng chính là topo mạng và đã được xác lập bằng cách nối dây. Tuy nhiên đối với mạng không dây, đây lại là việc quan trọng vì phải ghép nối các máy tính thành các "nhóm" có thể định danh được.

**Truy cập kênh truyền.** Đối với mạng LAN, cơ chế truy cập môi trường truyền nhanh, tin cậy và công bằng hết sức cần thiết.

### Đặc tả tầng MAC theo IEEE 802.11

Chức năng truy cập kênh truyền của mạng LAN không dây khá tương đồng với mạng Ethernet. Đặc tả này có một vài chức năng để đảm bảo tính an ninh, và sẽ được bổ sung thêm một vài tính năng để sau này có thể tích hợp được với mạng điện thoại không dây.

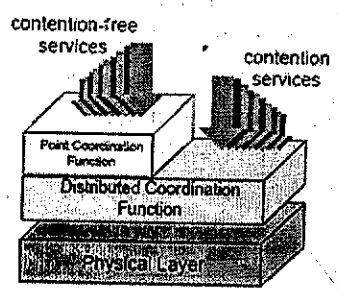
### Cấu hình mạng

Chuẩn IEEE 802.11 định nghĩa BSA (Basic Servive Area) là một khu vực có thể có nhiều máy tính (trạm) di động. Các máy tính trong BSA được gọi là Service Set (BSS). Các trạm làm việc trong BSS được kết nối với Access Point (AP). Nhiều BSS kết nối với nhau thành Distributed System (SS) để tạo thành Extended Service Set (ESS). Tất cả các trạm trong



cùng BSS sử dụng chung một tốc độ truyền (Basic Rate Set) và một cấu trúc gói dữ liệu PDU (xem minh họa Hình 5.42)

### Truy cập kênh truyền trong IEEE 802.11




**Hình 5.43 Cơ chế điều phối DCF**

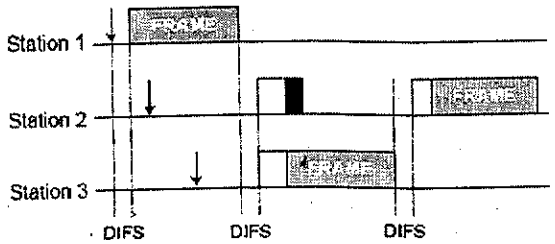
Chuẩn IEEE 802.11 định nghĩa cả tầng MAC lẫn tầng vật lý (Hình 5.40). Tầng MAC cung cấp hai dịch vụ: dịch vụ truy cập có tranh chấp (*Distributed Coordination Function - DCF*) và dịch vụ truy cập không tranh chấp (cài đặt ở *Point Coordination Function* - PCF). Những dịch vụ này được triển khai trên nền tầng vật lý, che dấu hết các đặc tính kỹ thuật của tầng vật lý đối với tầng mạng (Hình 5.43).

DCF là phương pháp chủ yếu trong họ IEEE 802.11 và sử dụng cơ chế *đa truy cập kênh truyền có tránh tắc nghẽn* (CSMA/CA). PCF được cài đặt trên nền DCF và dựa trên cơ chế hỏi vòng. Cơ chế này cho phép một trạm đóng vai trò trung tâm lần lượt "hỏi" các trạm trong mạng có muốn truyền dữ liệu không.

### Distributed Coordination Function (DCF)

Trước khi truyền frame, trạm phải "lắng nghe" kênh truyền để xem có trạm khác chiếm dụng kênh truyền hay không. Nếu kênh truyền rỗi trong một khoảng thời gian lớn hơn Distributed InterFrame Space (DIFS) thì trạm được phép truyền (Hình 5.44). Nếu ngược lại (môi trường truyền bị chiếm dụng), việc truyền của trạm bị trì hoãn đến phiên truyền tiếp theo. Khoảng thời gian trì hoãn này (backoff time) được lựa chọn một cách ngẫu nhiên và được sử dụng để khởi tạo cho backoff timer. Giá trị bộ định thời này giảm khi kênh truyền được cảm nhận là rỗi, sẽ giữ nguyên trong trường hợp kênh truyền bận và sẽ được giảm về 0 (reset) khi kênh truyền rỗi trong khoảng

thời gian lớn hơn DIFS. Ví dụ, trên Hình 5.44, chúng ta thấy rằng backoff timer của trạm 2 bị dừng lại trong khi trạm 3 đang truyền. Giá trị timer này sẽ được đặt về 0 sau khi trạm 3 truyền xong một khoảng thời gian DIFS. Trạm 2 sẽ được phép truyền khi backoff timer của mình nhận giá trị 0. Giá trị backoff time cũng được chia khoảng. Cụ thể hơn, giá trị này là một số nguyên ngẫu nhiên nằm trong khoảng (0, CW-1), trong đó CW (*Contention Window*) là độ lớn cửa sổ backoff (Backoff Window). Trong lần thử truyền đầu tiên, *CW* = *CW*min và cứ sau mỗi lần truyền thử, giá trị này tăng gấp đôi cho đến khi đạt đến giá trị *CW*max.




**Hình 5.44 Cơ chế tránh tắc nghẽn**

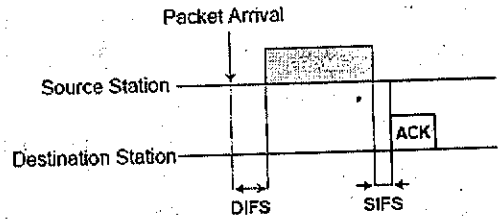
Theo chuẩn, giá trị của *CW*min và *CW*max phụ thuộc vào tầng vật lý phía dưới. Ví dụ, với công nghệ FHSS ở tầng Vật lý, giá trị của *CW*min và *CW*max tương ứng là 16 và 1024.

Rõ ràng hoàn toàn có khả năng tại cùng một thời điểm có nhiều trạm có nhu cầu truyền tin, khi đó xung đột chắc chắn xuất hiện. Với CSMA/CA trạm không có khả năng phát hiện xung đột bằng cách lắng nghe môi trường truyền giống như trong cơ chế CSMA/CD của mạng Ethernet. Do đó, để chắc chắn truyền thành công, phía nhận phải gửi phản hồi tích cực. Sau khi nhận đúng một frame, phía nhận đợi một khoảng thời gian Short InterFrame Space (SIFS) và gửi lại frame biên nhận ACK. Để ưu tiên việc gửi frame biên nhận hơn việc gửi frame dữ liệu bình thường khác, giá trị SIFS bé hơn DIFS (xem Hình 5.45). Nếu phía nhận không nhận được ACK, gói tin gửi đi sẽ bị coi là mất và sau một khoảng thời gian sẽ được gửi lại. Để phát hiện lỗi, người ta cũng sử dụng cơ chế CRC trình bày trong phần trước.

Sau khi phát hiện được frame bị lỗi (do xung đột hay lỗi trên môi trường truyền), trạm phải đợi ít nhất một khoảng thời gian bằng *Extended InterFrame Space* (EIFS) trước khi khởi động thuật toán backoff. Cụ thể, DCF phải sử dụng giá trị EIFS mỗi khi tầng vật lý báo cho tầng MAC frame



bắt đầu truyền không thể gửi thành công. Giá trị EIFS cũng được sử dụng để đồng bộ trạm làm việc với trạng thái của môi trường truyền (bận hay rỗi).




**Hình 5.45 Gửi biên nhận khi nhận được frame dữ liệu**

## 5.8.3 Một số vấn đề hay gặp đối với mạng không dây

Trong phần này, chúng ta nêu một số vấn đề nảy sinh trong mạng không dây, đây là những đặc điểm cơ bản khác với mạng có dây:

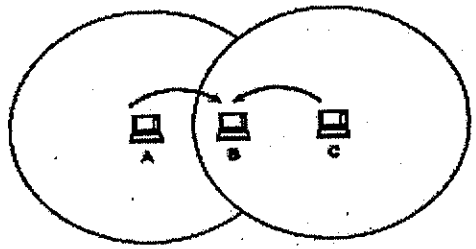
- Không có tiêu chí cụ thể để xác định phạm vi môi trường truyền. Có nghĩa là không thể xác định được phạm vi mà nút nằm trong đó chắc chắn nhận được frame, nằm ngoài phạm vi đó sẽ không nhận được.

- Môi trường truyền có thể bị nhiễu vì tín hiệu bên ngoài.

- Độ tin cậy kém môi trường có dây.

- Độ trễ trên môi trường truyền không cố định.

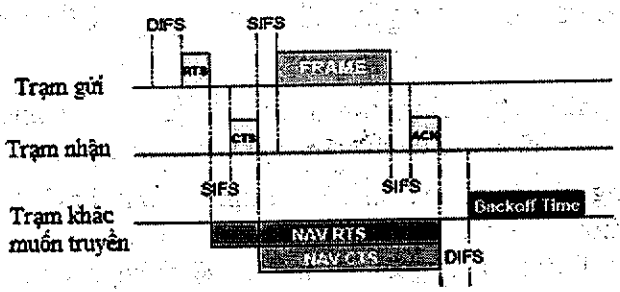
- Trong môi trường không dây, và cơ chế truy cập ngẫu nhiên dựa vào cảm nhận kênh truyền, những đặc tính nêu trên có thể gây nên những hiện tượng phức tạp, chẳng hạn "trạm ẩn" (hidden station) hay "trạm lộ" (exposed-station).




**Hình 5.46 Vấn đề trạm ẩn**

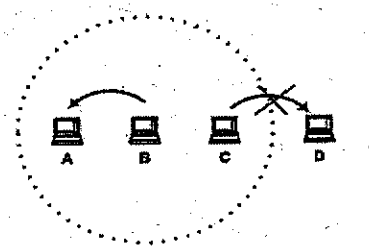
Hình 5.46 minh họa tình huống "trạm ẩn". Trạm B nằm giữa miền phủ sóng của A và C. Nhưng A và C không gửi trực tiếp dữ liệu được tới nhau. Giả sử trong lúc A bắt đầu gửi dữ liệu tới B thì C cũng có dữ liệu gửi tới B. Khi C thực hiện cảm nhận môi trường truyền thì tất nhiên không phát hiện dữ liệu do A gửi, vì vậy C coi kênh truyền rỗi và bắt đầu truyền. Tín hiệu từ A và C khi đến B sẽ bị xung đột

Vấn đề trạm ẩn này có thể khắc phục bằng cách bổ sung thêm vào cơ chế DCF cơ bản cơ chế cảm nhận ảo (*virtual carrier sensing*). Khi đó hệ thống có hai frame điều khiển: Request To Send (RTS) và Clear To Send (CTS). Trước khi truyền, trạm gửi sẽ gửi frame RTS tới trạm nhận để thông báo mình sẽ gửi frame dữ liệu (Hình 5.47). Khi nhận được frame RTS, trạm nhận sẽ gửi frame CTS. Chỉ khi nhận được CTS, bên gửi mới truyền đi dữ liệu.




**Hình 5.47 Cơ chế báo gửi và báo nhận**

Cả hai frame RTS và CTS đều được truyền trong những khoảng thời gian đủ để truyền đi một frame, nên tất cả các trạm trong vùng phủ sóng đều có thể nhận được các frame kiểu này và cập nhật giá trị *Network Allocation Vector* (NAV) tương ứng. Khi NVA dương, trạm không được gửi dữ liệu. Bằng cách sử dụng cơ chế RTS/CTS, trạm có thể nhận biết được sự truyền của các "trạm ẩn" cũng như khoảng thời gian truyền này.




**Hình 5.48 Trạm lộ**



Hình 5.48 minh họa tình huống "trạm lộ". Giả sử trạm A và C đều có thể nghe trạm B, nhưng trạm A không nghe được trạm C. Giả sử lúc B đang truyền cho A thì C nhận được một frame để truyền tới D. Rõ ràng C cảm nhận kênh truyền và thấy kênh truyền bận (do B truyền tới A), C sẽ trì hoãn việc truyền tới D, mặc dù việc này sẽ không gây xung đột tại A, điều này làm giảm thông lượng hệ thống.

## 5.9. PPP – GIAO THỨC ĐIỂM NỐI ĐIỂM

Phần trước chúng ta đã nói về kênh truyền quảng bá. Phần này chúng ta sẽ nghiên cứu giao thức liên kết dữ liệu cho kênh truyền điểm nối điểm (point-to-point) - giao thức PPP. PPP là giao thức được sử dụng chủ yếu khi người dùng truy cập Internet từ nhà thông qua đường điện thoại quay số, do đó PPP là một trong những giao thức tầng liên kết dữ liệu được sử dụng nhiều nhất nhất ngày nay. Giao thức quan trọng thứ hai là HDLC (High Level Data-Link Control [Spragins 1991]. Giao thức PPP được trình bầy tương đối đơn giản với mục đích khảo sát một số tính năng quan trọng nhất của lớp giao thức điểm nối điểm ở tầng liên kết dữ liệu.

Giao thức PPP [RFC 1661; RFC 2153] là giao thức tầng liên kết dữ liệu trên kênh truyền nối trực tiếp giữa hai nút - mỗi nút ở một đầu của đường truyền. Đường truyền PPP có thể là đường điện thoại quay số (ví dụ kết nối modem 56k), đường truyền SONET/SHD, kết nối X.25 hoặc mạch ISDN. Như đã nói trên, PPP chủ yếu được lựa chọn để kết nối máy tính gia đình đến ISP thông qua đường dây điện thoại. Trước khi đi sâu vào chi tiết của PPP, hãy điểm qua một số qui tắc chính mà IETF đã đặt ra cho mọi thiết kế của PPP [RFC 1547]:

**Đóng gói gói tin (Framing)**: phía gửi trong giao thức PPP phải có khả năng lấy gói tin ở tầng mạng, đặt nó trong frame tầng liên kết dữ liệu. Phía nhận xác định được vị trí bắt đầu và kết thúc của frame cũng như vị trí gói tin tầng mạng trong frame.

**Tính trong suốt**: Giao thức PPP không được đặt ra bất kỳ hạn chế nào trên gói dữ liệu tầng mạng. Tức là nó có khả năng chuyển đi bất kỳ gói dữ liệu tầng mạng nào.

**Hỗ trợ nhiều giao thức tầng mạng**: Giao thức PPP phải có khả năng hỗ trợ nhiều giao thức tầng mạng (ví dụ, IP và DECnet) trên cùng đường truyền vật lí tại cùng một thời điểm. Điều này cũng giống như giao thức IP có khả năng phân kênh cho nhiều giao thức giao vận khác nhau (ví dụ, TCP và UDP ). Như vậy PPP cũng cần có một cơ chế để thực thể PPP phía nhận xác định được cần chuyển gói dữ liệu trong frame cho thực thể tầng mạng nào.

**Hỗ trợ nhiều kiểu đường truyền**: Ngoài khả năng hỗ trợ nhiều giao thức ở tầng cao hơn, PPP phải có khả năng vận hành trên nhiều kiểu đường truyền khác nhau bao gồm đường truyền tuần tự (truyền lần lượt từng bit một) hoặc song song (truyền nhiều bit cùng một lần), đồng bộ (truyền tín hiệu đồng hồ cùng với bit dữ liệu) hoặc dị bộ, truyền với tốc độ chậm hoặc cao, tín hiệu điện tử hoặc quang học.

**Phát hiện lỗi**: PPP phía nhận có khả năng phát hiện liệu có lỗi bit trong frame nhận được hay không.

**Thời gian kết nối**: PPP phải có khả năng phát hiện đường truyền bị lỗi ở mức link (ví dụ, không có khả năng để truyền dữ liệu từ phía gửi sang phía nhận) và phải thông báo tình trạng lỗi này cho tầng mạng.

**Thoả thuận địa chỉ tầng mạng**: PPP phải cung cấp cơ chế cho phép hai thực thể tầng mạng tham gia truyền thông (IP) có thể học hay đặt cấu hình địa chỉ tầng mạng cho nhau.

**Đơn giản**: Người ta đòi hỏi PPP đáp ứng nhiều yêu cầu ngoài những yêu cầu nêu trên. Một trong những yêu cầu quan trọng nhất là "tính đơn giản". Hiện nay hơn 50 RFC định nghĩa những khía cạnh "đơn giản" của giao thức này.

Tuy vậy các đặc tả trong thiết kế PPP không yêu cầu:

**Sửa lỗi**: PPP cần phát hiện được lỗi bit nhưng không cần phải sửa lỗi.

**Kiểm soát lưu lượng**: PPP phía nhận được hy vọng có khả năng nhận frame với tốc độ cao nhất của tầng vật lí phía dưới. Nếu tầng mạng không thể nhận với tốc độ này thì việc loại bỏ gói tin hay yêu cầu bên kia truyền chậm lại là trách nhiệm của các tầng cao hơn. Khi đó tầng cao hơn sẽ



yêu cầu thực thể tương đương phía bên kia giảm tốc độ tạo ra dữ liệu gửi cho PPP.

**Đánh số thứ tự**: PPP không được yêu cầu chuyển frame đến phía nhận theo đúng thứ tự gửi.

**Đường truyền đa điểm**: PPP vận hành trên những đường truyền với một phía gửi và một phía nhận duy nhất. Một số giao thức tầng liên kết dữ liệu khác (ví dụ, HDLC) cho phép nhiều nút nhận trên cùng một đường truyền (giống Ethernet).

## 5.9.1 Khuôn dạng gói dữ liệu (Frame PPP)

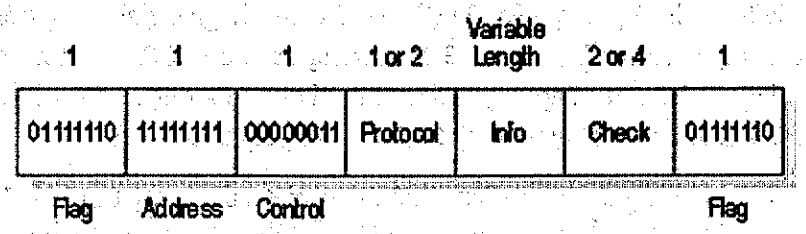
Hình 5.49 minh họa frame PPP giống frame HDLC [RFC 1662]

Frame PPP bao gồm những trường sau:

**Trường cờ**: Mọi frame PPP bắt đầu và kết thúc bằng một byte cờ có giá trị 01111110.

**Trường địa chỉ**: giá trị duy nhất của trường này là *11111111*.

**Trường điều khiển**: giá trị duy nhất của trường này là 00000011. Bởi vì cả hai trường địa chỉ và điều khiển đều mang những giá trị cố định, điều này giải thích vì sao những trường này được định nghĩa đầu tiên. Khuyến nghị PPP [RFC 1662] nói rõ rằng những giá trị này "có thể được định nghĩa sau này". Bởi vì những trường này mang giá trị cố định, PPP cho phép phía gửi không cần gửi byte địa chỉ và byte điều khiển, do đó tiết kiệm được hai byte tiêu đề trong frame PPP.




**Hình 5.49 Khuôn dạng frame dữ liệu PPP**

**Trường giao thức (protocol)**: Trường giao thức cho PPP xác định giao thức tầng trên sẽ nhận dữ liệu trong frame PPP. Khi nhận được frame PPP, bên nhận sẽ kiểm tra xem frame có lỗi không và sau đó chuyển phần dữ liệu trong gói tin cho giao thức thích hợp. RFC 1700 định nghĩa mã 16 bit cho các giao thức được sử dụng cùng với PPP. Giao thức IP (dữ liệu trong frame PPP là gói dữ liệu IP datagram) ứng với giá trị 21h, giao thức AppleTalk là 29h, DFCnet là 27h, giao thức điều khiển đường truyền PPP là C021h và giao thức điều khiển IP là 8021. Giao thức IP Control được PPP sử dụng khi kích hoạt kênh truyền lần đầu tiên để cấu hình IP giữa các thiết bị trên hai đầu kênh truyền.

**Thông tin**: Trường này chứa gói tin được giao thức tầng mạng gửi đi trên đường truyền PPP (là IP datagram với giao thức IP). Độ dài lớn nhất của trường thông tin này là 1500 byte, mặc dù giá trị này có thể thay đổi lúc đặt cấu hình cho đường truyền.

**Tổng kiểm tra (Checksum)**: Trường checksum được sử dụng để phát hiện các bit bị lỗi trong frame nhận được. Nó là mã CRC 2 hoặc 4 byte giống như trong giao thức HDLC.

***Chèn byte (Byte stuffing)***

Trước khi kết thúc việc trình bầy về PPP frame, chúng ta hãy xét vấn đề phát sinh khi trong gói dữ liệu của giao thức tầng mạng lại có một byte giống byte cờ đánh dấu điểm bắt đầu và kết thúc của frame. Điều gì xảy ra nếu phát hiện thấy có byte cờ với giá trị 01111110 ở giữa gói tin trong trường thông tin. Bên nhận sẽ cho rằng đây là điểm kết thúc của frame PPP - mặc dù trên thực tế không phải như vậy.

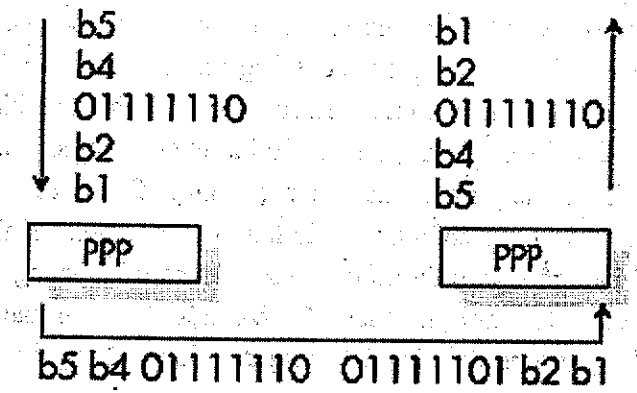
Một cách để giải quyết vấn đề này là cấm các giao thức tầng trên gửi dữ liệu chứa byte cờ. Yêu cầu về tính trong suốt của PPP đã nêu ở trên không chấp nhận giải pháp này. Giải pháp thay thế - được PPP cũng như nhiều giao thức khác áp dụng là kỹ thuật **chèn byte (byte stuff)**.

PPP định nghĩa byte điều khiển đặc biệt có giá trị 01111101 làm nhiệm vụ đánh dấu. Nếu byte cờ - 01111110 - xuất hiện trong frame (trừ vị trí mở đầu và kết thúc của frame), PPP đặt byte đánh dấu trước byte cờ. Như vậy nó đã "chèn" thêm một byte điều khiển để đánh dấu rằng byte 01111110



không phải là cờ mà là dữ liệu thực. Bên nhận thấy 01111110 đứng trước 01111101 nên biết được 01111101 không phải là cờ mà là dữ liệu, nên nó sẽ tự động loại bỏ byte đánh dấu 01111110 được phía nhận chèn vào bên cạnh dòng dữ liệu thực.

Hình 5.50 minh hoạ chèn byte trong PPP. Tương tự như thế, nếu chính byte đánh dấu cũng xuất hiện trong dòng dữ liệu thực sự thì nó cũng cần được đánh dấu.




**Hình 5.50 Chèn byte trong byte**

## 5.9.2 Giao thức điều khiển đường truyền PPP (LCP) và kiểm soát mạng

Trong phần trước, chúng ta đã thấy PPP đóng khung dữ liệu được gửi đi trên đường truyền. Nhưng đường truyền được khởi tạo như thế nào khi máy tính hoặc router ở một phía của đường truyền bật trước? Quá trình khởi tạo, duy trì, báo lỗi và đóng đường truyền PPP được thực hiện nhờ giao thức điều khiển đường truyền (LCP –Link Control Protocol) và các giao thức điều khiển mạng của PPP.

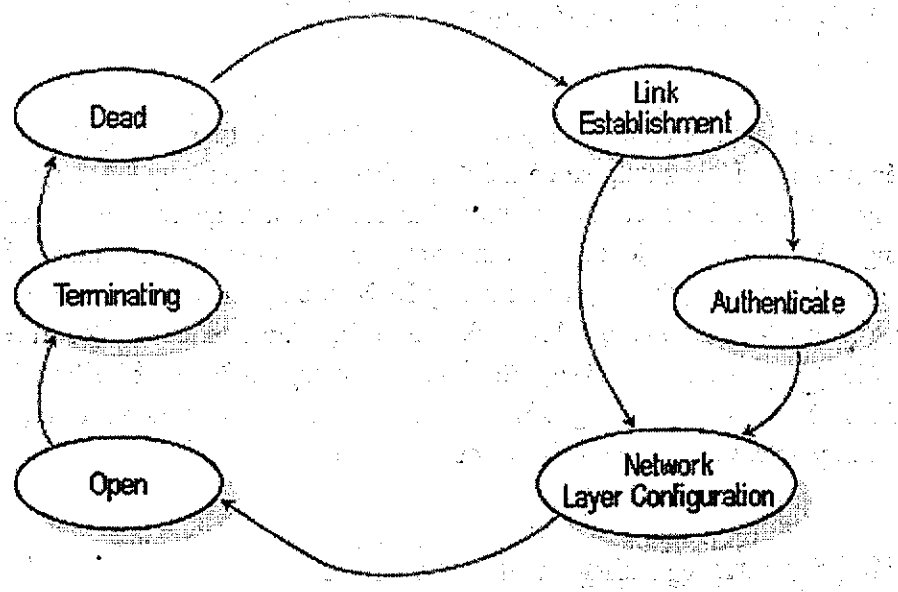
Trước khi trao đổi bất kì dữ liệu nào trên đường truyền PPP giao thức (mỗi phía ở một đầu đường truyền) phải thực hiện nhiều công việc nặng tự đặt trọng để thiết lập cấu hình cho đường truyền, điều này cũng ng truyền PPP.

thực thể TCP bên gửi và bên nhận thực hiện bắt tay ba bước (xem phần 3.5) để đặt các tham số của kết nối TCP trước khi trao đổi TCP segment. Hình 5.51 minh hoạ biểu đồ chuyển trạng thái của giao thức LCP để đặt cấu hình, duy trì và kết thúc đường truyền PPP.

Đường truyền PPP bắt đầu và kết thúc trong trạng thái đóng (dead). Khi phát sinh sự kiện như phát hiện sóng mang hay người quản trị mạng tác động để chỉ tầng vật lí sẵn sàng sử dụng, PPP bước sang trạng thái thiết lập đường truyền (link establishment). Trong trạng thái này, một phía của đường truyền gửi tùy chọn cấu hình mong muốn qua frame yêu cầu cấu hình LCP (là frame PPP có giá trị trường protocol ứng với giao thức LCP và trường information chứa nội dung cấu hình yêu cầu). Sau đó phía bên kia trả lời với frame ***configure-ack*** (chấp nhận tất cả các lựa chọn), frame ***configure-nak*** (hiểu nhưng không chấp nhận các lựa chọn) hoặc frame ***configure-reject*** (không thể ghi nhận hoặc chấp nhận các lựa chọn để đàm phán). Tùy chọn cấu hình LCP bao gồm kích thước tối đa của frame trên đường truyền, giao thức kiểm chứng được sử dụng (nếu cần) và một tùy chọn xác định có bỏ qua việc sử dụng trường địa chỉ và trường điều khiển trong frame PPP hay không.

Sau khi đường truyền được thiết lập, thỏa thuận xong các tuỳ chọn của đường truyền và kiểm chứng thành công, hai phía của đường truyền PPP sẽ trao đổi các gói tin kiểm soát của tầng mạng. Nếu IP chạy phía trên PPP, giao thức điều khiển IP [RFC 1332] được sử dụng để thiết lập cấu hình cho module giao thức IP tại mỗi đầu của đường truyền PPP. Gói tin IPCP được đặt trong frame PPP. IPCP cho phép hai module IP thay đổi hoặc đặt cấu hình địa chỉ IP hay thỏa thuận có nén gói dữ liệu IP không. Những giao thức kiểm soát mạng tương tự được đưa ra cho những giao thức tầng mạng khác như DECnet [RFC 1762] và AppleTalk [RFC 1378]. Sau khi cấu hình xong tầng mạng, PPP có thể bắt đầu gửi gói tin của tầng mạng - đường truyền ở trạng thái mở và dữ liệu bắt đầu chuyển trên đường truyền PPP. Các frame yêu cầu phản hồi và frame trả lời phản hồi LCP có thể được hai phía của đường truyền trao đổi để kiểm tra trạng thái đường truyền.






**Hình 5.51 Sơ đồ chuyển trạng thái của LCP**

Đường truyền PPP được duy trì cho đến khi gói tin LCP yêu cầu kết thúc được gửi đi. Nếu frame LCP yêu cầu kết thúc (terminate-request) từ một phía kết nối được trả lời bởi frame LCP chấp nhận kết thúc (terminate-ack) từ phía bên kia thì đường truyền bước vào trạng thái đóng.

Tóm lại, PPP là giao thức tầng liên kết dữ liệu cho hai thiết bị ở hai đầu của một đường truyền kiểu point-to-point, trao đổi các frame chứa gói dữ liệu của tầng mạng. Những chức năng chủ yếu của PPP là:

**Đóng gói dữ liệu**: Phương thức đặt gói dữ liệu trong frame PPP; xác định vị trí bắt đầu và kết thúc của frame; và phát hiện lỗi trong frame.

**Giao thức điều khiển đường truyền**: khởi tạo, duy trì và kết thúc đường truyền PPP.

**Giao thức điều khiển mạng**: một nhóm giao thức, mỗi giao thức ứng với một giao thức mạng ở tầng trên, cho phép module tầng mạng tự đặt cấu hình trước khi gói dữ liệu tầng mạng bắt đầu chuyển qua đường truyền PPP.

## 5.10 MẠNG RIÊNG ẢO (VPN)

Mục đích của mạng riêng ảo (Virtual Private Network - VPN) là cho phép một người dùng ở ngoài có thể đăng nhập được vào mạng LAN cục bộ thông qua mạng Internet như thể máy tính của người dùng đang nằm trong mạng LAN. Khi đó, mặc dù người dùng ở phía ngoài mạng LAN nhưng vẫn có thể sử dụng các dịch vụ trong mạng LAN không khác gì các máy tính đang nằm bên trong mạng LAN. Một trường hợp khác là tổ chức có nhiều địa điểm khác nhau, và mỗi địa điểm có một mạng LAN cục bộ riêng. Tổ chức muốn kết nối hai mạng LAN này lại với nhau để tạo thành một mạng LAN duy nhất. Công nghệ VPN có thể đáp ứng điều này.

### 5.10.1 Các mạng riêng ảo truyền thống

Phần này trình bày một vài kiến trúc VPN ở tầng Liên kết Dữ liệu và tầng Mạng.

#### VPN ở tầng Liên kết dữ liệu (tầng 2)

Trong thời kỳ đầu, khách hàng sẽ cài đặt hệ thống VPN bằng cách thuê bao các đường truyền riêng từ nhà cung cấp dịch vụ để kết nối hệ thống mạng cục bộ nằm trên nhiều địa điểm khác nhau.

Từ khi ra đời vào năm 1990, Frame Relay là công nghệ VPN "thống trị". Frame Relay cho phép nhà cung cấp dịch vụ tuy vẫn sử dụng đường truyền chia sẻ bình thường nhưng có thể cung cấp một băng thông thỏa thuận trước với khách hàng. Điều này được thực hiện bằng cách cấp phát "mạch ảo" trên kênh truyền dùng chung cho mỗi khách hàng (chứ không phải bằng cách phân chia kênh truyền). Mạch ảo ở đây được gọi là PVC (Permanent Virtual Circuit). Bằng cách cấu hình PVC, định danh kết nối ở tầng liên kết dữ liệu (Data-Link Connection Identifiers - DLCI) được thiết lập qua nhiều thiết bị khác nhau. Điều này sẽ tạo ra một "đường ống" cho phép dữ liệu của người sử dụng được truyền trên một đường dùng riêng cố định được cấp phát từ trước qua mạng dùng chung của nhà cung cấp dịch vụ.



Dịch vụ của nhà cung cấp dịch vụ chỉ cung cấp các kết nối ở tầng 2 chứ không liên quan đến tầng 3 (do đó gọi là VPN ở tầng 2). Ưu điểm của kiến trúc này là cho phép khách hàng độc lập trong việc thiết kế, định tuyến, đánh địa chỉ ở tầng 3.

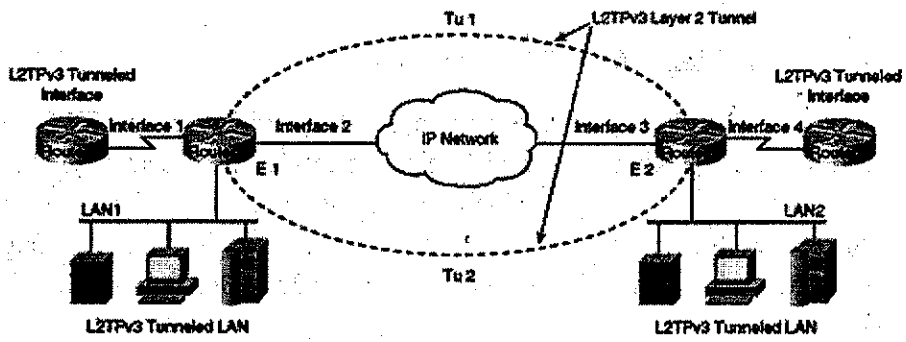
Sự độc lập của Fram Relay với giao thức mạng ở tầng 3 là yếu tố quan trọng để lựa chọn FR là công nghệ kết nối các mạng LAN từ nhiều địa điểm khác nhau. Hiện nay, nhiều nhà cung cấp dịch vụ hỗ trợ VPN trên nền ATM hoặc lai ghép cả ATM lẫn Frame Relay.

#### VPN ở tầng 3

Hiện nay công nghệ VPN chủ đạo ở tầng 3 là IP Security (IPsec) và MPLS Border Gateway Protocol (BGP). Những công nghệ này cho phép ứng dụng truy cập vào mạng Internet, mạng nội bộ hay mạng externet qua các đường kết nối an toàn.

Trong công nghệ VPN ở tầng 3, nhà cung cấp dịch vụ cho thuê bao các đường dùng riêng hay kết nối PVC giữa khách hàng và điểm truy cập dịch vụ (Point Of Presence – POP) gần nhất vào mạng của nhà cung cấp.

Hình 5.52 minh họa mô hình MPLS VPN cơ bản

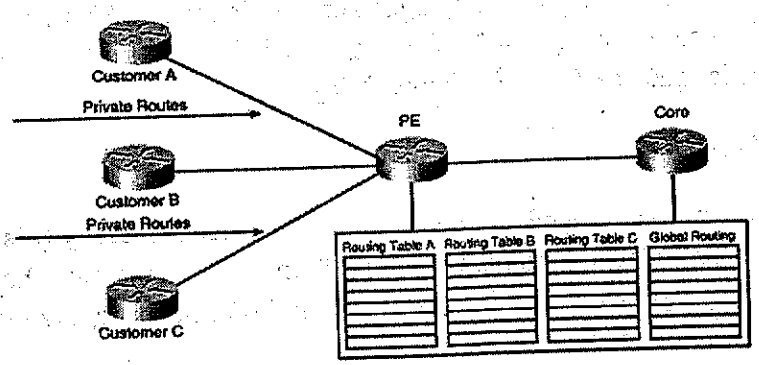



**Hình 5.52 Mạng riêng với địa chỉ IP riêng**

Trong công nghệ MPLS VPN, router ở phía khách hàng kết nối ngang hàng với router của nhà cung cấp dịch vụ. Khi muốn chuyển thông tin trong mạng riêng, router khách hàng sẽ cung cấp các thông tin và yêu cầu

định tuyến cho router của nhà cung cấp dịch vụ. Bên cạnh bảng định tuyến toàn cục, router của nhà cung cấp dịch vụ có bảng định tuyến riêng cho mỗi khách hàng

Trong Hình 5.53, không phải tất cả mạng riêng của khách hàng được chuyển qua bảng định tuyến toàn cục.




**Hình 5.53 Quan hệ giữa router khách hàng và router nhà cung cấp dịch vụ**

Thông qua VPN ở tầng 3, khách hàng có thể sử dụng tạo ra các đường kết nối an toàn trực tiếp từ khu vực này sang khu vực mạng khác trên nền mạng Internet toàn cầu với sự hỗ trợ của các ISP.

### Các vấn đề của kiến trúc VPN truyền thống

VPN ở tầng 3 cũng có nhiều hạn chế. Ví dụ với giao thức MPLS chỉ hỗ trợ duy nhất IP. Khách hàng phải nhường quyền kiểm soát việc định tuyến của mình cho nhà cung cấp dịch vụ. Thứ hai, router của nhà cung cấp dịch vụ (PE) có thể bị quá tải. Để hỗ trợ khả năng mở rộng của hệ thống, nhà cung cấp dịch vụ phải sử dụng các router có cấu hình mạnh – và do đó đắt tiền.

Như đã nói ở trên, các dịch vụ kết nối ở tầng 2 tạo ra các đường truyền điểm nối điểm để xây dựng VPN. Để hỗ trợ truyền thông ở tầng 3, phải xây dựng thêm một mạng ở tầng 3. Kết quả của điều này là nhà cung cấp dịch vụ phải có hai mạng tách rời cho cả tầng 2 lẫn tầng 3 – một vấn đề khó khăn và tốn kém.



Một vấn đề của dịch vụ ở tầng 2 [illegible] độ tối đa (ATM với đường truyền OC48) không thể theo kịp với tốc độ ngày càng tăng của công nghệ mạng cục bộ (Ethernet). Do vậy nhà cung cấp dịch vụ phải tìm cách nâng cao hiệu suất và giảm chi phí quản lý. Điều này có thể đạt được bằng cách cho phép nhiều kết nối ở tầng 2 có thể được thiết lập qua trục IP/MPLS dùng chung.

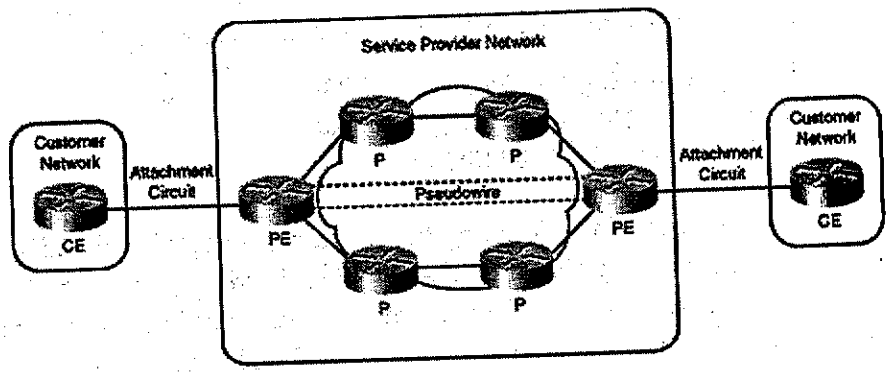
## 5.10.2 Mô phỏng giả dây dẫn (Pseudowire Emulation Overview)

Mục tiêu của cơ chế này là "tái tạo" các đặc điểm của dịch vụ chuyển mạch ở tầng 1 và tầng 2 (chẳng hạn TDM hay Frame Relay) trên nền tảng mạch chuyển mạch gói (PSN). Cơ chế này gửi các gói PDU giữa máy tính của khách hàng thông qua mạng của nhà cung cấp dịch vụ. Đối với khách hàng, cơ chế giả dây dẫn hoàn toàn trong suốt, nghĩa là khách hàng hoàn toàn không biết "mạch ảo" mà mình sử dụng được triển khai trên nền tảng chuyển mạch gói của nhà cung cấp dịch vụ.

Động lực thúc đẩy sự phát triển của công nghệ này là mong muốn hội tụ các công nghệ mạng cho phép triển khai một số dịch vụ mà trước đây chỉ có trên mạng chuyển mạch ảo trên công nghệ chuyển mạch gói.

### Mô hình tham chiếu

Hình 5.54 minh họa mô hình tham chiếu của kiến trúc mô phỏng dây dẫn.




**Hình 5.54 Mô hình giả dây dẫn**

Các thiết bị ở phía nhà cung cấp dịch vụ (PE) nằm trong miền quản trị. Nhiệm vụ của miền này là cung cấp dịch vụ mô phỏng giả dây dẫn cho các thiết bị ở phía khách hàng thuộc cùng một miền quản trị.

Kết nối giữa PE và CE được thực hiện bằng mạch nối (attachment circuit) – có thể là cổng Etthernet, Ethernet VLAN, PPP session hay kết nối High-Level Data Link Control (HDLC), định danh kết nối Frame Relay (DLCI), định danh mạch ảo ATM.

"Giả dây dẫn" là một mạch ảo giữa hai PE để kết nối hai mạch nối. Mạch ảo này có thể được thiết lập thủ công hay tự động (qua cơ chế báo tín hiệu). Sau khi đã có một "giả dây dẫn" giữa hai PE, các frame dữ liệu nguyên thủy từ các mạch nối được đặt trong các gói dữ liệu của mạch ảo truyền từ đầu này sang đầu kia. Khi nhận được PDU mạch ảo, PE sẽ lấy ra frame ban đầu và gửi cho mạch nối.

Các thiết bị của nhà cung cấp (P) tạo nên hệ thống chuyển mạch gói ở giữa và hoàn toàn trong suốt với khách hàng. P cũng không "nhận biết" được luồng truyền thông "giả dây dẫn" và điều này giúp việc thiết kế mạng đơn giản hơn. Mạng trung tâm sẽ không phức tạp vì chỉ tập trung vào khía cạnh định tuyến và chuyển tiếp dữ liệu sao cho đạt hiệu suất cao nhất. Khi đó mạng cũng dễ mở rộng hơn và có thể cung cấp được nhiều mạch "giả dây dẫn hơn". Ở đây chúng ta cũng thấy lại quan điểm tổ chức mạng ở "lõi" hệ thống càng đơn giản càng tốt và độ phức tạp nên chuyển ra phía ngoài.

## Giao thức và kiến trúc hệ thống

Giao thức của kiến trúc mô phỏng giả dây dẫn có ba tầng:

- Giao thức của Tầng chuyển mạch gói PSN
- Giao thức bao bọc dữ liệu của giả dây dẫn
- Giao thức của tầng dữ liệu (payload)

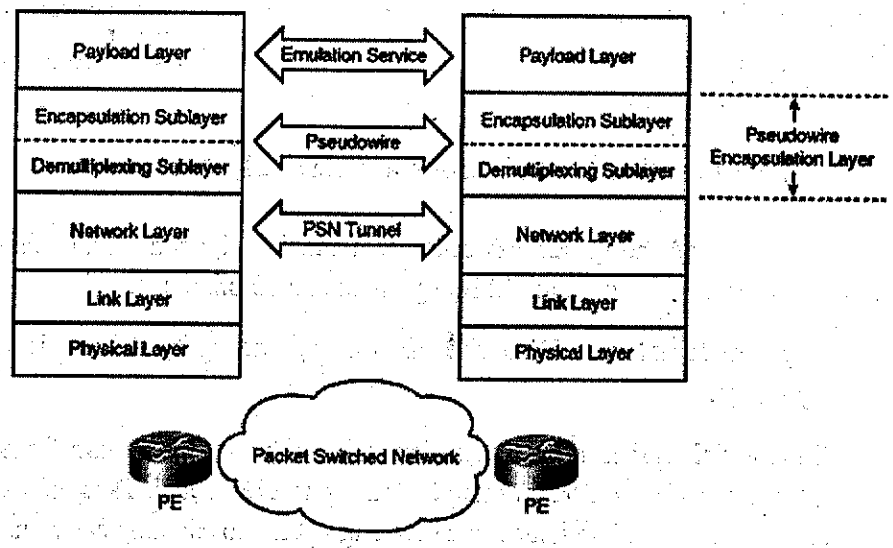
Tầng PSN quy định các thông tin về địa chỉ mạng của các thiết bị PE, ở đây có thể sử dụng giao thức địa chỉ IPv4, IPv6, hoặc nhãn MPLS. Các thiết bị mạng sử dụng tầng PSN để xác định tuyến đường chuyển tiếp của các gói tin trên mạch "giả dây dẫn". Bạn có thể hình dung mạch giả dây dẫn này như một đường ống tạo thành từ công nghệ chuyển mạch gói.



Tầng bao bọc dữ liệu bao gồm hai tầng con: tầng phân kênh và tầng bao bọc dữ liệu. Nhiệm vụ của tầng phân kênh là phân biệt các đường "giả dây dẫn" khác nhau cùng được thiết lập trên cùng một "đường ống" từ mạng chuyển mạch gói. Trong mỗi đường ống, mỗi giả dây dẫn có một định danh phân kênh duy nhất. Tầng bao bọc dữ liệu có nhiệm vụ đặt thêm một số thông tin về dữ liệu, những thông tin này sẽ được PE đầu kia sử dụng để loại bỏ để tạo ra frame ban đầu (từ payload) trước khi chuyển tiếp cho mạch nối đến CE.

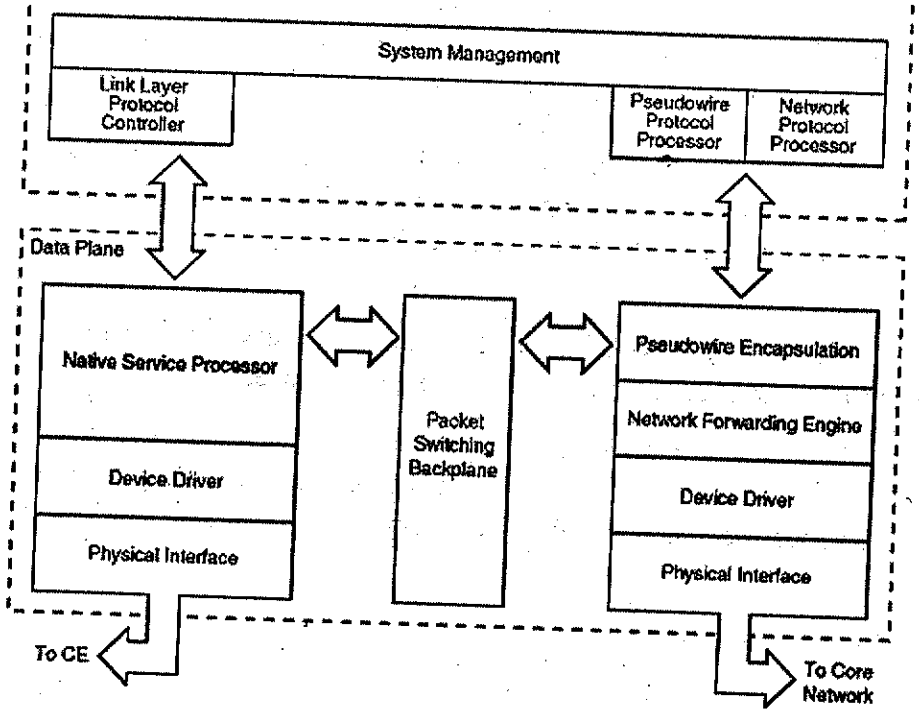
Tầng dữ liệu payload tải các kiểu dữ liệu giả dây dẫn khác nhau, có thể là frame Ethernet, ATM cell hay Frame Relay packet.

Hình 5.55 minh họa quan hệ của các tầng giả dây dẫn trên hai thiết bị PE. Mỗi tầng trên mỗi PE tương tác với tầng ngang cấp của phía PE bên kia thông qua các tầng bên dưới, và đến lượt mình lại cung cấp dịch vụ cho tầng cao hơn.




**Hình 5.55 Mô hình các tầng trong "Giả dây dẫn"**

PE đóng vai trò cực kỳ quan trọng trong kiến trúc. Trên thực tế, truyền thông giữa hai mạch nối diễn ra chủ yếu qua PE. Hình 5.56 minh họa kiến trúc của PE.




**Hình 5.56 Kiến trúc PE (Thiết bị của nhà cung cấp dịch vụ)**

Kiến trúc hệ thống của PE được chia thành hai phần chính: phần điều khiển và phần dữ liệu. Phần dữ liệu gồm có các bộ phận sau:

- **Physical interfaces**: Điều chế các tín hiệu tương tự thành bit và ngược lại.
- **Device drivers**: là tầng trung gian, với nhiệm vụ tạo ra các frame (phụ thuộc vào môi trường truyền) cho giao diện vật lí. Tầng nên sẽ che dấu các đặc điểm khác nhau của tầng vật lí cho các tầng cao hơn.
- **Native service processor** và **Pseudowire encapsulation**: Thực hiện biến đổi các gói dữ liệu (sẽ được trình bày kỹ hơn ở phần sau).
- **Network forwarding engine**: Khi nhận được dữ liệu từ bộ phận pseudowire encapsulation cùng với địa chỉ mạng đích, bộ phận



network forwarding engine tìm kiếm địa chỉ này trong các bảng chuyển tiếp. Nếu tìm thấy một giao diện ra, nó sẽ gói gói dữ liệu này trong một frame có cấu trúc phù hợp để gửi trên giao diện vừa tìm thấy. Nếu không tìm thấy, gói tin bị loại bỏ.

Phần điều khiển gồm các thành phần sau:

- **Link layer protocol controller**: Thực hiện giao thức báo hiệu trên đường truyền, chẳng hạn Frame Relay Local Management Interface (LMI) hay ATM Integrated Local Management Interface (ILMI), với mục đích thiết lập các mạch nối.
- **Pseudowire protocol processor** và **network protocol processor:** Tương ứng thực hiện các thủ tục báo hiệu trong giao thức "giả dây dẫn" và giao thức định tuyến. Các thiết bị PE sử dụng các thủ tục này để thiết lập các "giả dây dẫn" và tuyến đường để chuyển dữ liệu (xem Hình 5.56). Các thể lấy được các thông tin dùng để chuyển tiếp gói tin thông qua các thủ tục báo hiệu

**Xử lý các gói tin từ dịch vụ ban đầu**

Trong một số trường hợp, các gói dữ liệu của mạch nối có thể được chuyển tiếp ngay cho tầng giả dây dẫn. Tuy nhiên trong một số trường hợp, gói tin nguyên thủy này cần phải được xử lý trước khi áp dụng cơ chế bao bọc dữ liệu của giao thức "giả dây dẫn".

Thông thường, chúng ta phải áp dụng các thủ tục xử lý gói tin khác nhau cho các kiểu mạch nối khác nhau. Thậm chí cùng một kiểu nhưng các cấu hình khác nhau cũng có thể dẫn đến các thủ tục xử lý khác nhau.

The native service processor (NSP) xử lý bất kỳ gói tin nào truyền qua nó theo một cách thức phù hợp. Ví dụ khi nhận được một gói tin của giao thức PPP dưới dạng một frame HDLC, NSP loại bỏ các tiêu đề của HDLC sao cho phần dữ liệu của giao thức PPP có thể đặt trong khuôn dạng không phụ thuộc vào môi trường truyền. Khi gói dữ liệu của tầng "giả dây dẫn" chứa dữ liệu PPP đến thiết bị PE ở phía đầu kia, phần dữ liệu này sẽ được chuyển cho bộ phận NSP trước khi loại bỏ các tiêu đề của gói tin "giả

dây dẫn". Khi đó NSP biết rằng trường dữ liệu này cần phải đặt trong trường dữ liệu của giao thức PPP để gửi đi tiếp.

### Xử lý việc bao bọc dữ liệu ở tầng giả mã dây

Sau khi qua giai đoạn xử lý gói tin ban đầu, trường dữ liệu có thể được bao bọc theo khuôn dạng của giao thức giả mã dây. NSP có thể sử dụng thêm một số thông tin đặc thù của trường dữ liệu để chuyển qua cho pseudowire encapsulation processor (PEP)

Các thông tin điều khiển này được sử dụng để báo hiệu cho từng gói tin (cần thiết đối với một số kiểu dịch vụ). Ngoài các thông tin này, quá trình bao bọc có thể đặt thêm các thông tin về thời gian cho truyền thông theo thời gian thực hoặc các thông tin đánh số thứ tự giúp phía nhận phát hiện các gói tin không đúng thứ tự.

### Truyền thông qua mạng PSN

Phụ thuộc vào kiến trúc của PSN, chúng ta có thể sử dụng IP hoặc MPLS để gửi gói tin của tầng giả dây dẫn. Kiến trúc PSN không chỉ xác định cách thức bao bọc gói tin ở tầng mạng mà còn xác định khuôn dạng của bộ phân kênh của giả dây dẫn. Ví dụ nếu IP là giao thức tầng mạng của PSN, thì trong trường Upper layer của gói tin IP sẽ xác định cần gửi gói tin này cho bộ phân kênh nào.



# Tài liệu tham khảo


[1]. J. Kurose and K. Ross, ***Computer Networking: A Top-Down Approach Featuring the Internet***", Addison-Wesley, 3rd edition, May 2004.

[2]. Andrew S. Tanenbaum, **Computer Networks**, *Prentice Hall PTR, 2004*

[3]. S.Keshav, *An Engineering Approach to Computer Networking*, Addison-Wesley, 2003

[4]. Jean Walrand, ***Communication Networks: A first cost***, second edition, McGraw Hill, 2003

[5]. Douglas E. Comer, *Computer Networks and Internet with Internet Application*, 3rd edi, Prentice Hall, 2003.

[6]. Michael A. Gallo and William M. Hancock, ***Computer Communications and Network Technologies***, Brooks/Cole Thomson Learning, 2003

[7]. William Stalling, ***Data and Computers Communications***, 6th edition, Prentice Hall, 2003.

[8]. Behrouz A. Forouzan, ***Data Communications and Networking***, McGraw Hill, 2003

[9]. Ramesh Subramanian and Brian D. Goodman, ***Peer To Peer Computing The Evolution Of A Disruptive Technology***, IDEA Group Publishing, 2006

[10]. Wei Luo, *Layer 2 VPN Architectures*, Cisco Press, 2006

# Bài giảng MẠNG MÁY TÍNH

GV: NGUYỄN HÀ HUY CƯỜNG

# Mạng máy tính

## Tổng quan về mạng máy tính

# Nội dung

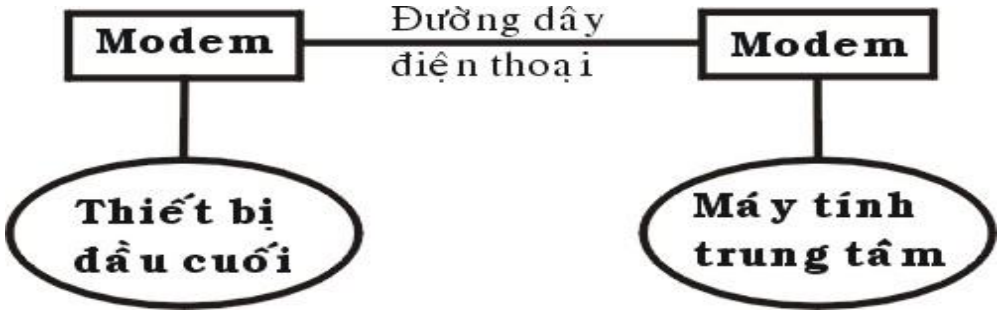
- Lịch sử phát triển của mạng máy tính
- Khái niệm mạng máy tính
- Mạng ngang hàng, mạng dựa vào phục vụ (server)
- Phần cứng/Phần mềm mạng
- Các kiểu mạng

# Lịch sử phát triển của mạng máy tính

- Vào giữa những năm 50 những thế hệ máy tính đầu tiên việc nhập liệu rất phức tạp phải thông qua các tấm bìa mà người viết chương trình đã đục lỗ sẵn.
- Thông qua thiết bị đọc các tấm bìa thông tin được đưa vào máy tính.
- Các thiết bị đọc bìa và máy in được thể hiện như thiết bị I/O của máy tính
- Sau một thời gian các máy tính được đưa vào hoạt động như máy tính trung tâm có thể được kết nối với nhiều thiết bị I/O.

# Lịch sử phát triển của mạng máy tính

- Cùng với sự phát triển của những ứng dụng trên máy tính các phương pháp nâng cao khả năng giao tiếp với máy tính trung tâm cũng đã được đầu tư nghiên cứu rất nhiều.
- Vào giữa những năm 60 một số nhà chế tạo máy tính đã nghiên cứu thành công những thiết bị truy cập từ xa tới máy tính của họ.
- Một trong những phương pháp truy cập từ xa được thực hiện thông qua đường dây điện thoại và hai thiết bị xử lý tín hiệu (Modem).

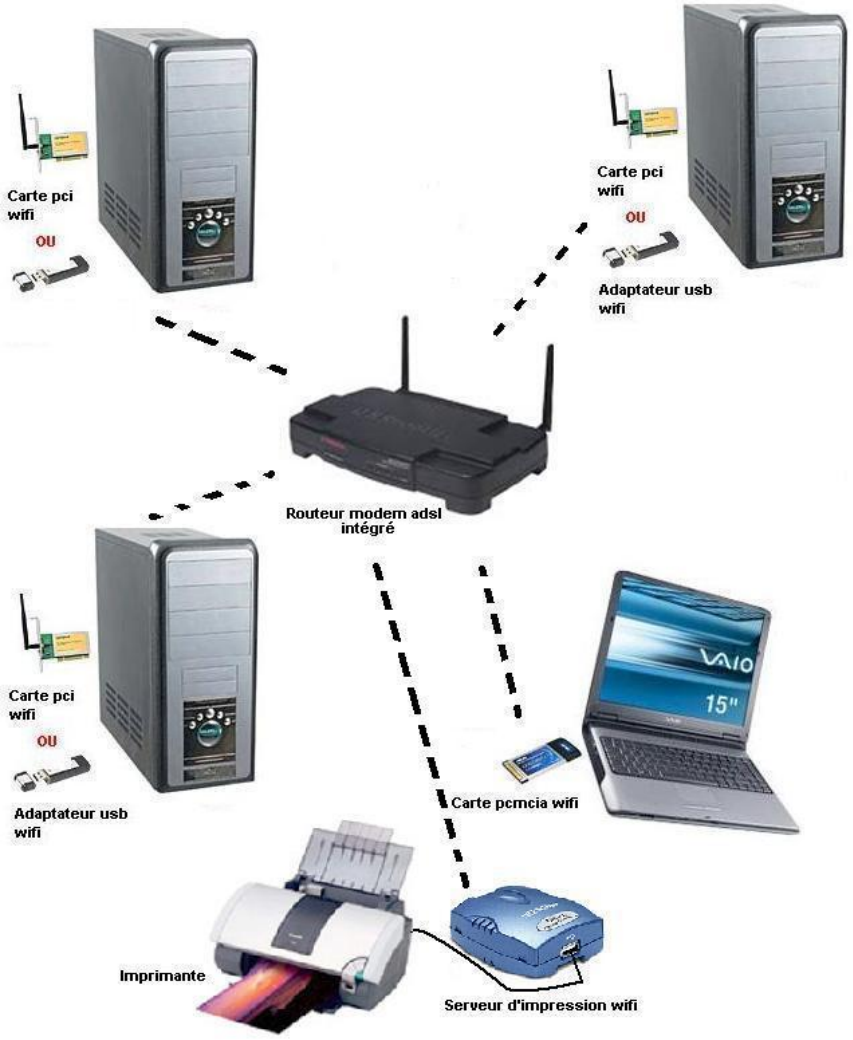


# Lịch sử phát triển của mạng máy tính

- Vào giữa những năm 1970, các thiết bị đầu cuối sử dụng những phương pháp liên kết qua đường cáp nằm trong một khu vực đã được ra đời.
- Với những ưu điểm từ nâng cao tốc độ truyền dữ liệu và qua đó kết hợp khả năng tính toán của các máy tính lại với nhau.
- Vào những năm 1980 các hệ thống đường truyền tốc độ cao đã được thiết lập ở Bắc Mỹ và Châu Âu.
- Vào năm 1974 công ty IBM đã giới thiệu một loạt các thiết bị đầu cuối được chế tạo cho lĩnh vực ngân hàng và thương mại, thông qua các dây cáp mạng các thiết bị đầu cuối có thể truy cập cùng một lúc vào một máy tính dùng chung.
- Với thời đại bùng nổ thông tin hiện nay, ở nhiều nơi mạng đã trở thành một nhu cầu không thể thiếu.

# Khái niệm mạng máy tính

- Định nghĩa: Mạng máy tính là một tập hợp các máy tính được nối với nhau theo một cấu trúc và một phương tiện truyền thông nào đó sao cho chúng có thể chia sẽ và trao đổi thông tin với nhau.




*Một mô hình liên kết các máy tính trong mạng*

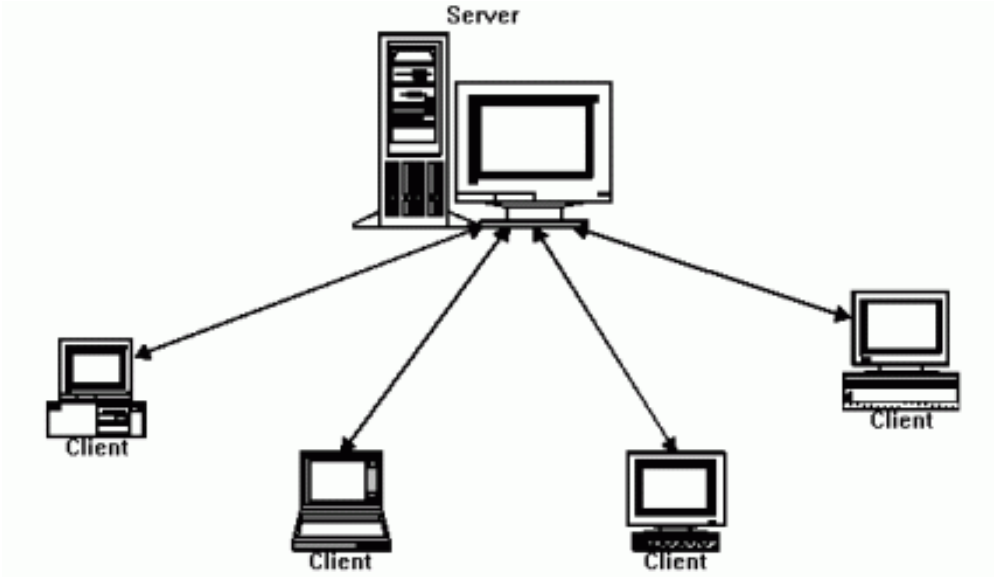
# Khái niệm mạng máy tính

Ưu điểm:

- **Sử dụng chung tài nguyên:** như dữ liệu, phần cứng, phần mềm, CPU → tiết kiệm chi phí
- **Tăng độ tin cậy của hệ thống**: Người ta có thể dễ dàng bảo trì máy móc và lưu trữ (backup) các dữ liệu chung
- **Nâng cao chất lượng và hiệu quả khai thác thông tin:**
  - Quản lý dữ liệu tập trung và đồng nhất.
  - Tăng cường năng lực xử lý
  - Tăng cường truy nhập tới các dịch vụ mạng khác nhau đang được cung cấp trên thế giới.

# Thí dụ - Tiết kiệm chi phí

- Phòng máy nối mạng 20 máy thực tập cần 20 đĩa cứng, phần mềm tương ứng.
- Nếu thông qua máy chủ (server) có thể chia sẽ, dùng chung đĩa cứng và phần mềm. Các máy trạm (không cần đĩa cứng) khi khởi động thông qua kỹ thuật BootROM cho phép tải phần mềm và dùng chung đĩa cứng của máy chủ.



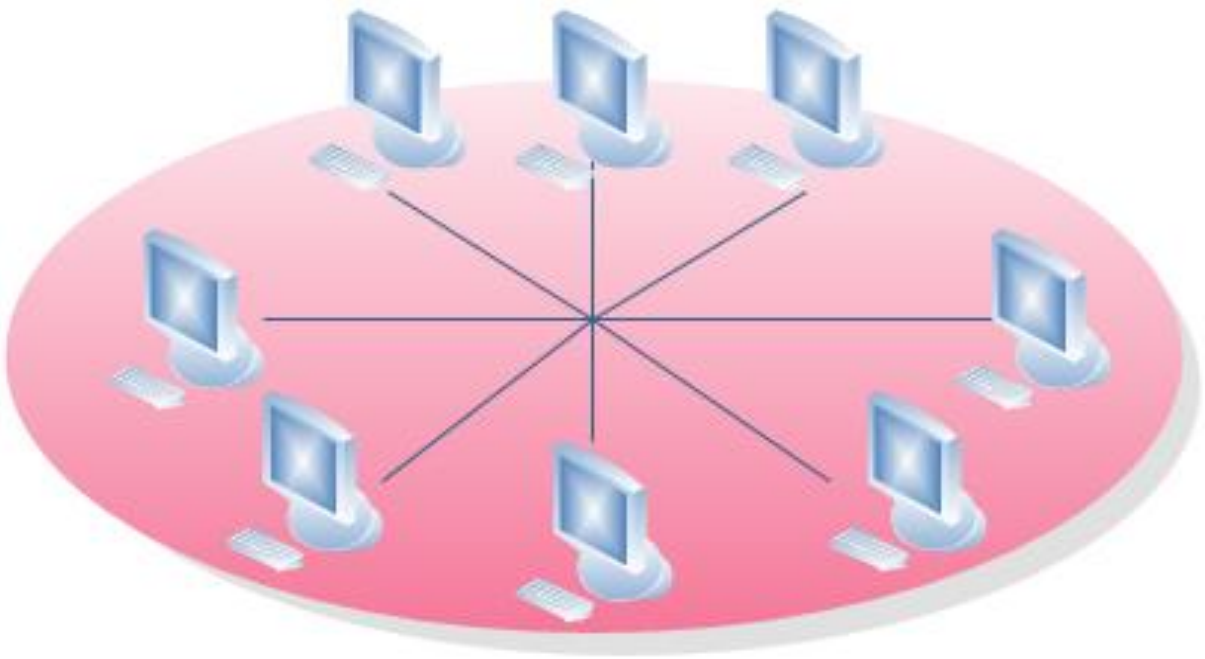
# KIẾN TRÚC MẠNG MÁY TÍNH

- Kiến trúc mạng máy tính thể hiện cách nối các máy tính với nhau và tập hợp các qui tắc, qui ước mà tất cả các máy tính tham gia truyền thông trên mạng phải tuân theo để đảm bảo hệ thống mạng hoạt động tốt.
- Cách nối các máy tính, các thiết bị ngoại vi, các thiết bị mạng trong một hệ thống mạng được gọi là cấu trúc hình học.
- Còn tập hợp các qui tắc, qui ước truyền thông được gọi là giao thức. Cấu trúc hình học của mạng và các giao thức là hai khái niệm rất cơ bản của mạng máy tính.

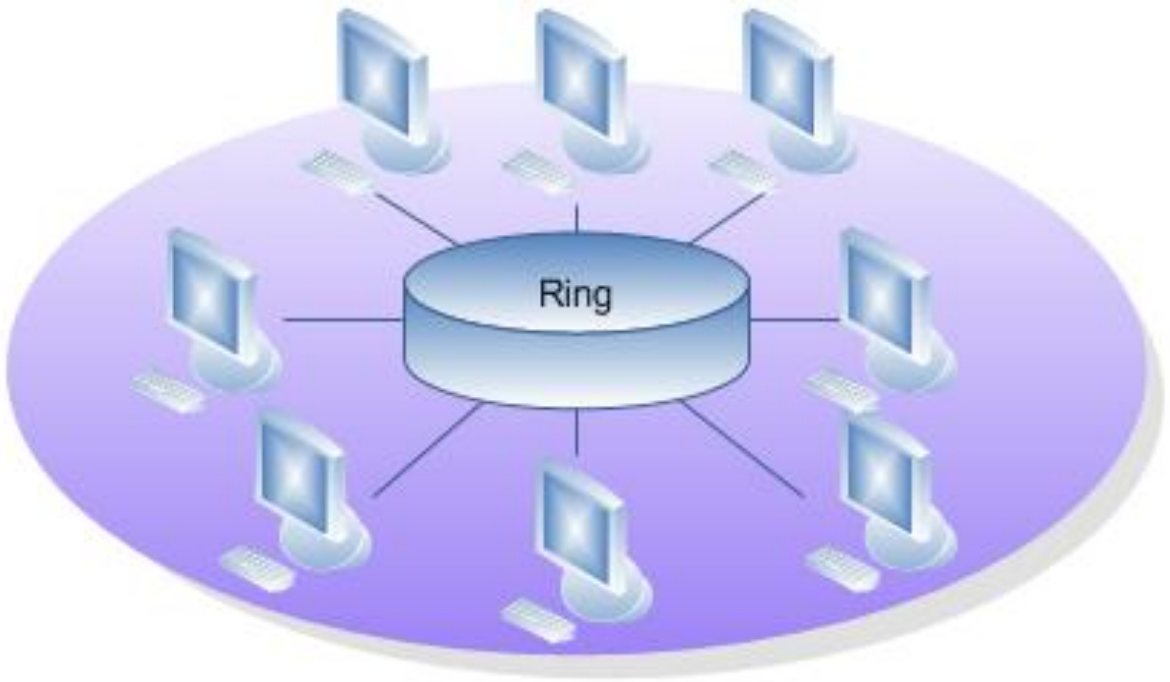
# Cấu trúc hình học(Topology)

- Mạng kiểu hình sao (Star type)
- Mạng kiểu tuyến Bus (Bus type)
- Mạng kiểu vòng (Ring type)
- Mạng kiểu cây (Tree type)
- Mạng kiểu lưới (Mesh type)

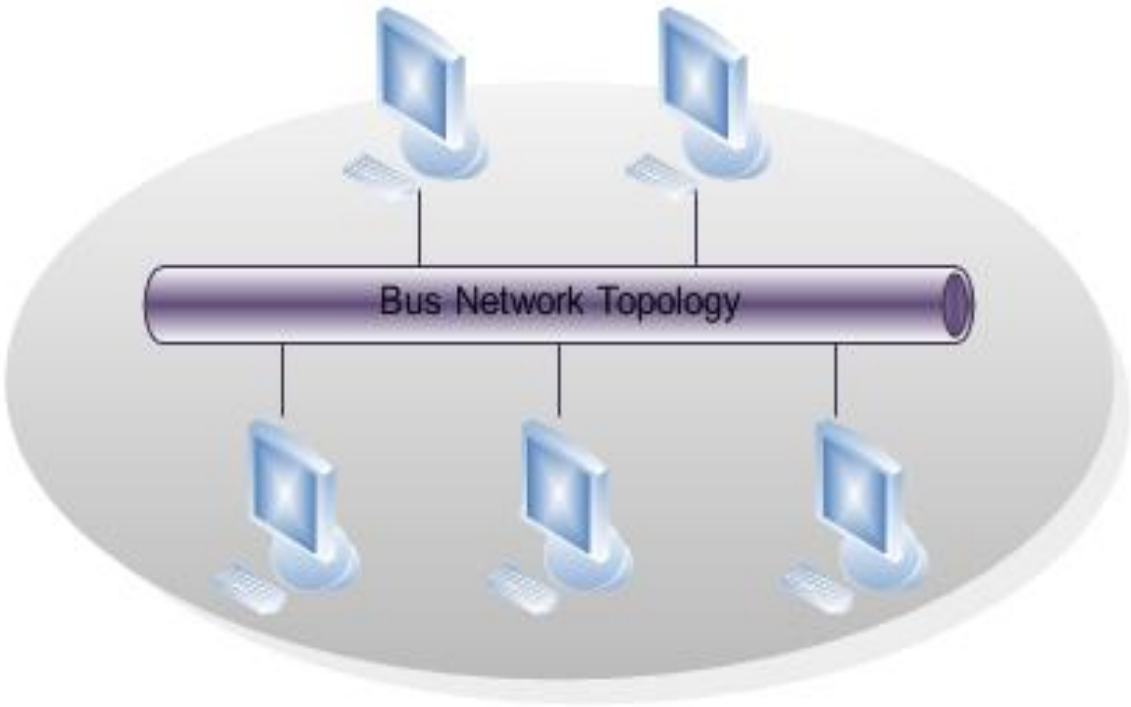
# Star Topology



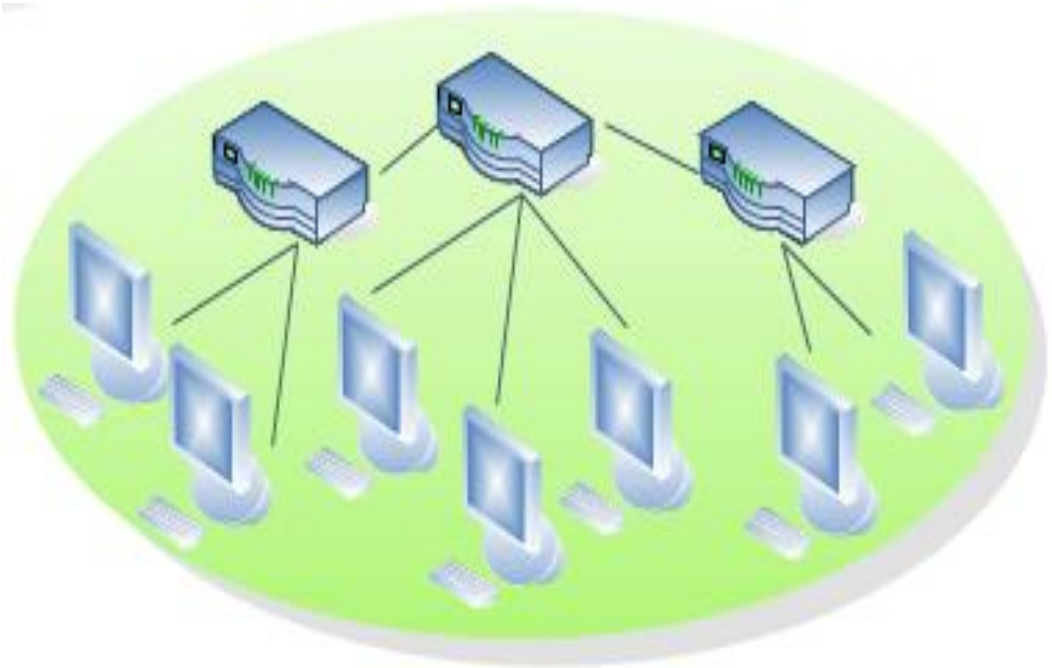
# Ring Topology



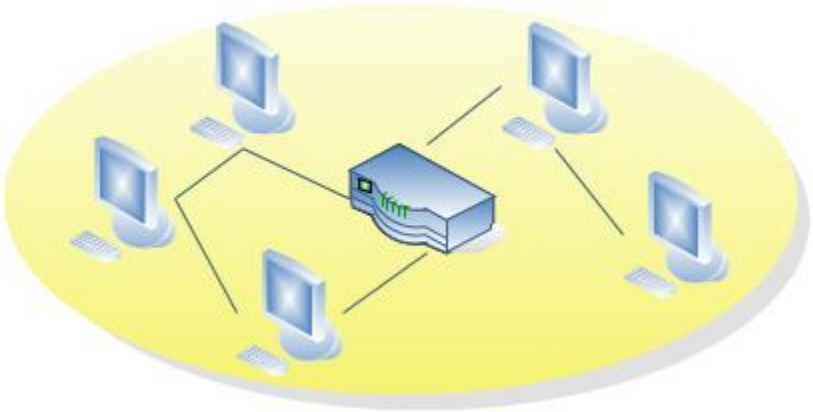
# Bus Topology



# Tree Topology



# Mesh Topology



# PHÂN BIỆT MẠNG MÁY TÍNH

- Phân loại mạng theo phương thức kết nối mạng được sử dụng chủ yếu trong liên kết mạng.
- Phân loại mạng theo chức năng.
- Phân loại mạng máy tính theo vùng địa lý.
- Phân loại mạng máy tính theo kiến trúc mạng (tôpô).

# Phân loại Phân loại mạng theo chức năng  thức kết nối mạng

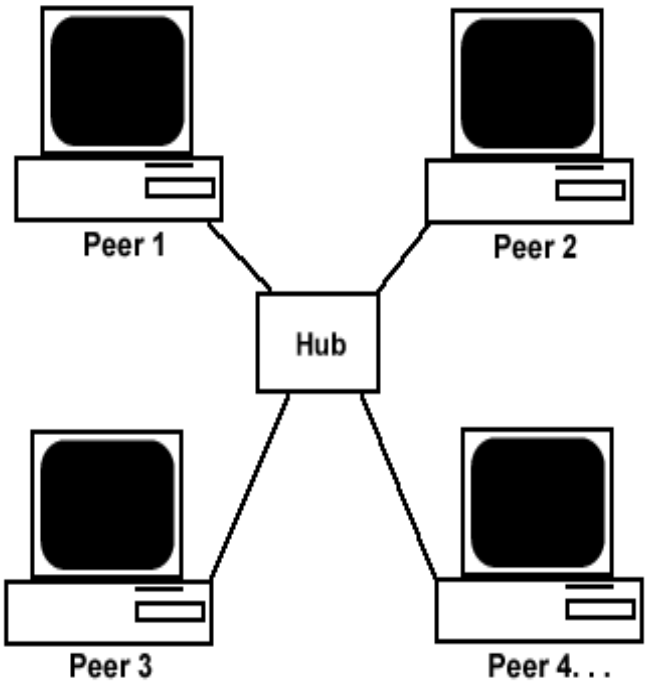
- Phương thức kết nối mạng được sử dụng chủ yếu trong liên kết mạng: có hai phương thức chủ yếu, đó là điểm - điểm và điểm - nhiều điểm.

# Phân loại mạng theo chức năng

- Mạng ngang hàng/mạng server
- Trong mạng có 2 loại máy tính
  - Server (máy chủ-máy phục vụ)
  - Workstation/client (máy trạm/máy khác)
- Server là máy cung cấp, chia sẽ các tài nguyên dùng chung trên mạng
- Workstation là máy sử dụng các tài nguyên dùng chung trên mạng

# Mạng ngang hàng – peer to peer

- Còn gọi là mạng workgroup
- Các máy trên mạng đều có vai trò như nhau
- Ưu điểm: Đơn giản, dễ cài đặt, chi phí rẻ → thích hợp với mạng nhỏ (10 – 20 máy)
- Khuyết:
  - Quản lý tập tin kém, không đồng nhất (có thể tồn tại nhiều phiên bản trên nhiều máy)
  - An toàn và bảo mật kém

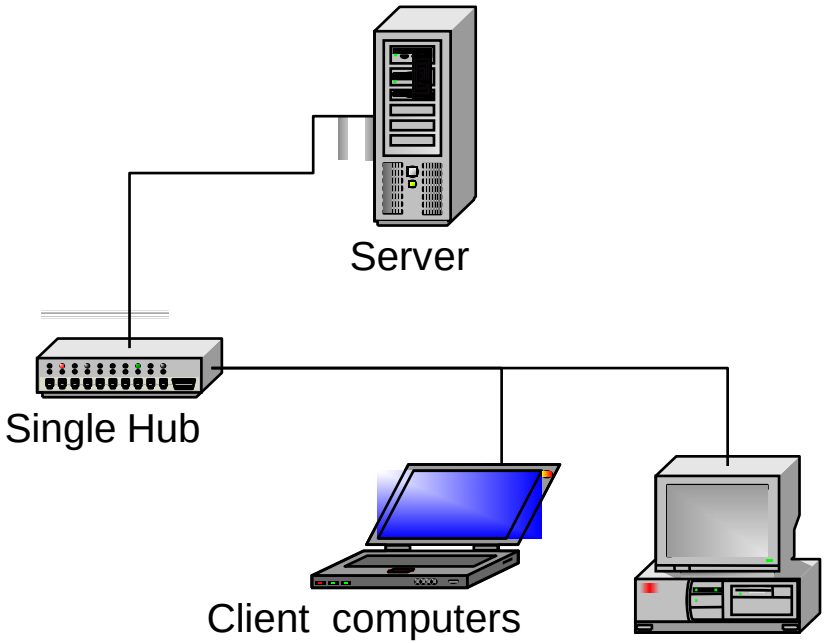


# Mạng dựa vào máy chủ phục vụ

- Dùng 1 hay nhiều server chuyên dụng.
- Quản trị mạng:
  - Quản lý chia sẻ các tài nguyên dùng chung trên mạng
  - Hệ thống an toàn bảo mật
  - Quản lý và phân quyền người dùng trên mạng
  - Bảo trì mạng
  - Cấp tài tài khoản người dùng (account) và mật khẩu truy cập (password) và phân quyền người dùng (role) như cho phép truy cập dữ liệu, ghi dữ liệu, ...
- Mạng này cần một người quản trị

# Mạng dựa vào máy chủ phục vụ

- Ưu điểm:
  - Sử dụng cho mạng lớn (quản lý nhiều máy)
  - Quản lý tập trung đồng nhất trên các server chuyên dụng
  - Hệ thống an toàn, bảo mật cao
  - Giảm chi phí phần mềm
- Khuyết điểm:
  - Khó cài đặt, quản lý (đối với mạng lớn)
  - Chi phí cao hơn do: chi phí server, người quản trị/bảo trì



# Một số dạng máy chủ phục vụ

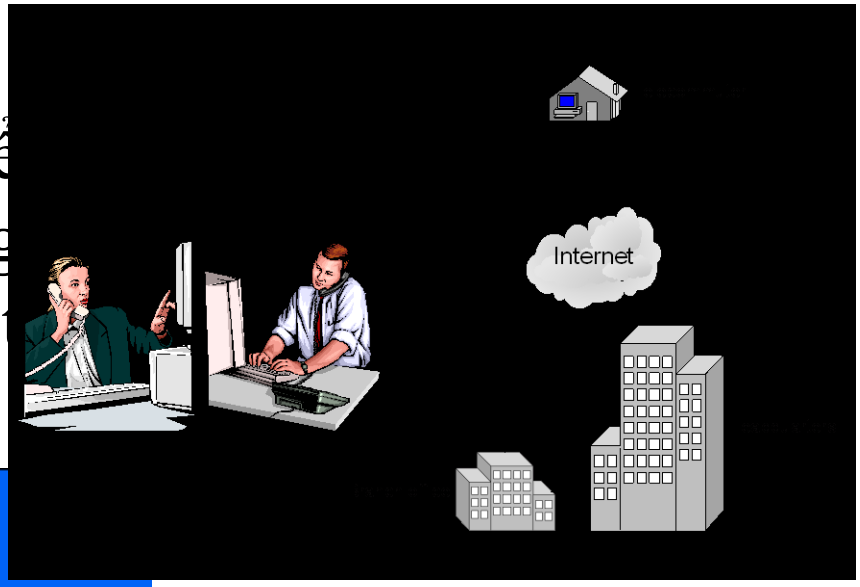
- File server: Chia sẻ các tập tin dùng chung
- Application server: Chia sẻ dùng chung phần mềm
- Database server: Chia sẻ dùng chung cơ sở dữ liệu
- Web server: Máy chủ phục vụ web
- Mail server: Máy chủ phục vụ gởi nhận thư điện tử
- Printer server: Chia sẻ máy in
- Chat server: Cho phép nhiều người tham gia vào chat như Yahoo Messager
- Máy server có thể có nhiều chức năng trên

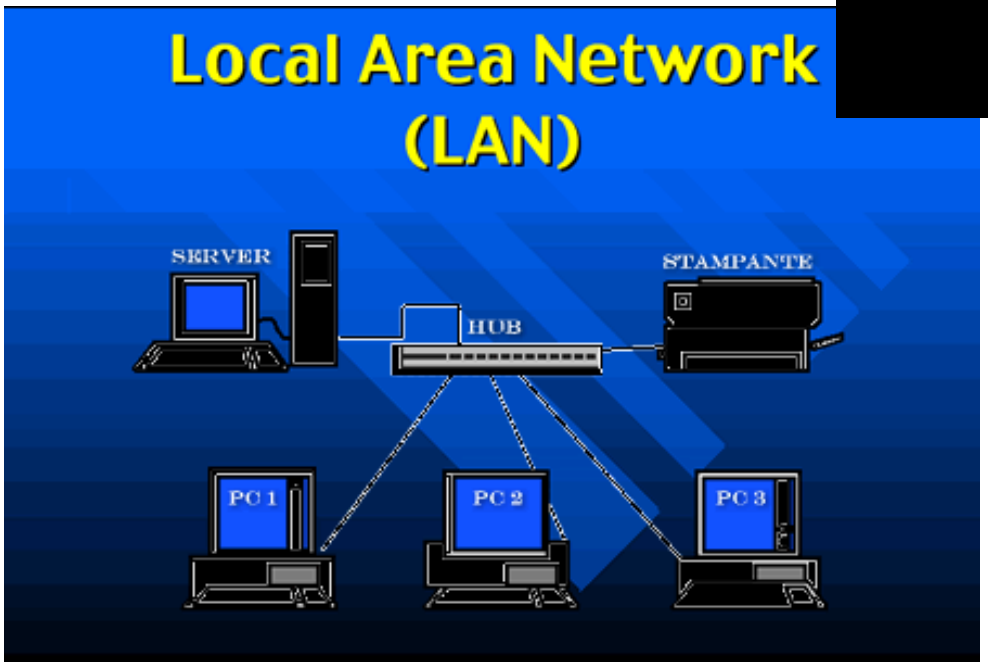
# Phân biệt theo vị trí địa lý

- Dựa vào phạm vi hoạt động người ta chia ra làm 4 kiểu mạng:
  - Mạng cục bộ (Local Area Networks – LAN)
  - Mạng đô thị băng thông rộng (Metro Area Networks – MAN)
  - Mạng diện rộng (Wide Area Networks – WAN)
  - Mạng toàn cầu (Global Area Networks- GAN)

# Mạng LAN

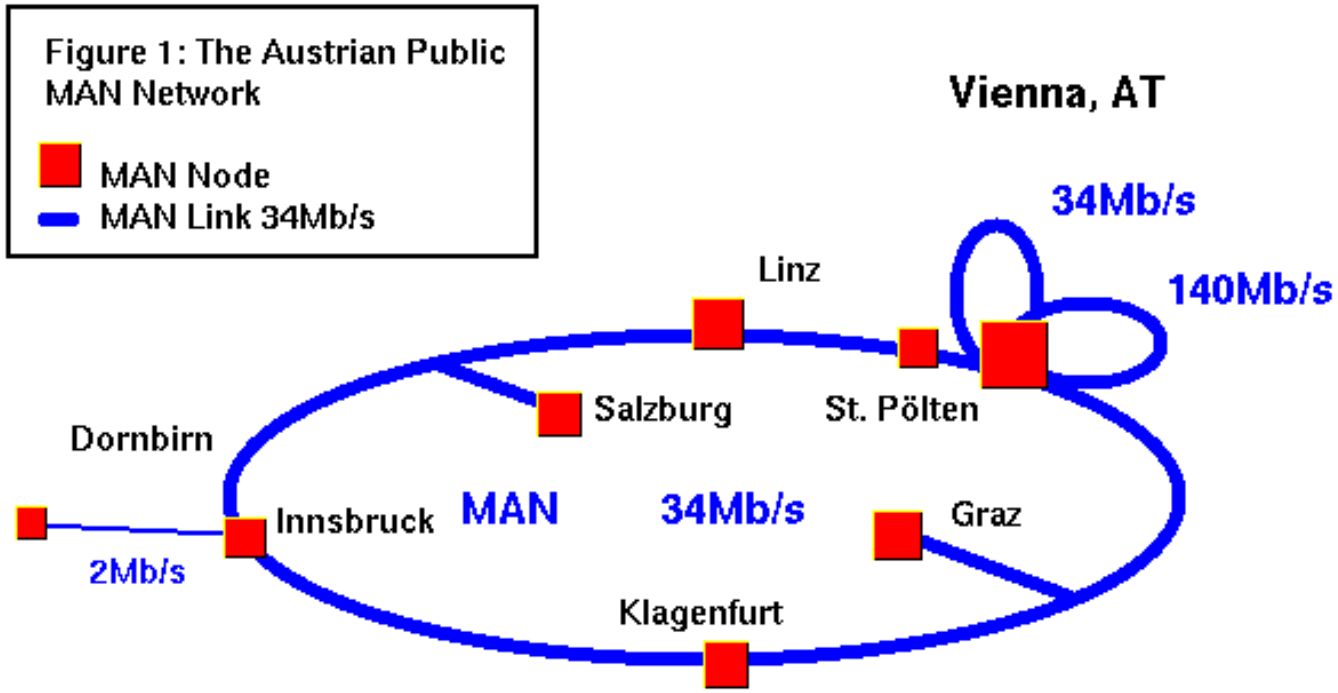
- Là mạng được thiết lập để liên kết các máy tính trong một khu vực như trong một toà nhà, một khu nhà.



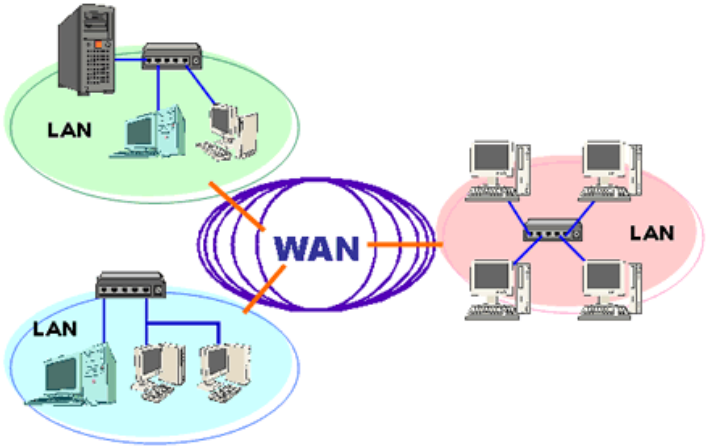
# Mạng MAN

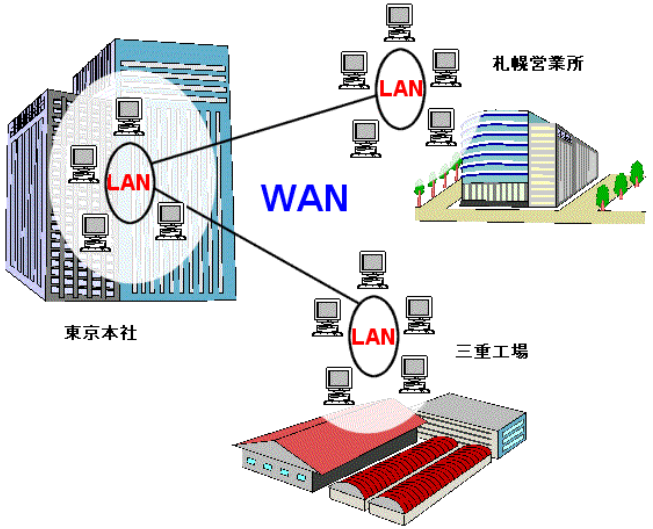
- Là mạng đô thị băng thông rộng, phạm vi hoạt động trong thành phố, đô thị,... (<100km)



# Mạng WAN

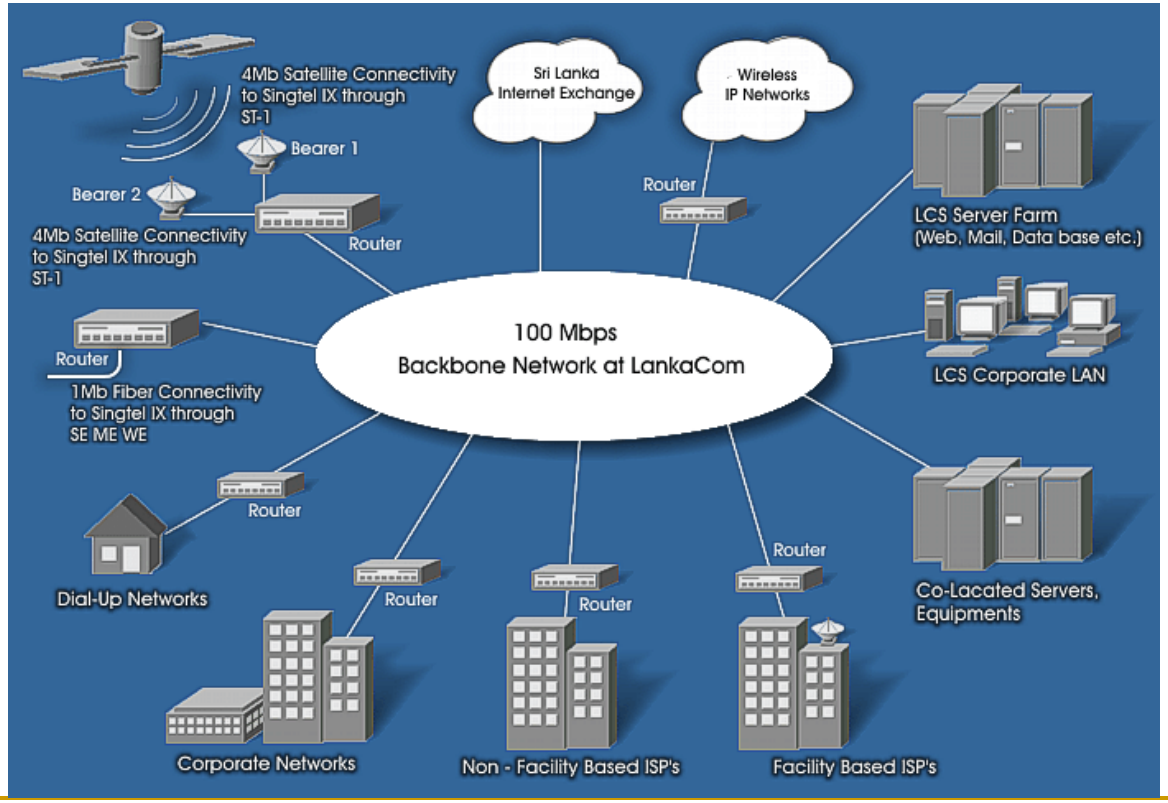
- Là mạng được thiết lập để liên kết các máy tính của hai hay nhiều khu vực khác nhau như giữa các thành phố hay các tỉnh, quốc gia, châu lục.



# Mạng GAN

- Phạm vi hoạt động toàn cầu
- Ai cũng có thể tham gia vào sử dụng mạng này
- Không có tổ chức nào điều hành, chịu trách nhiệm về mạng này



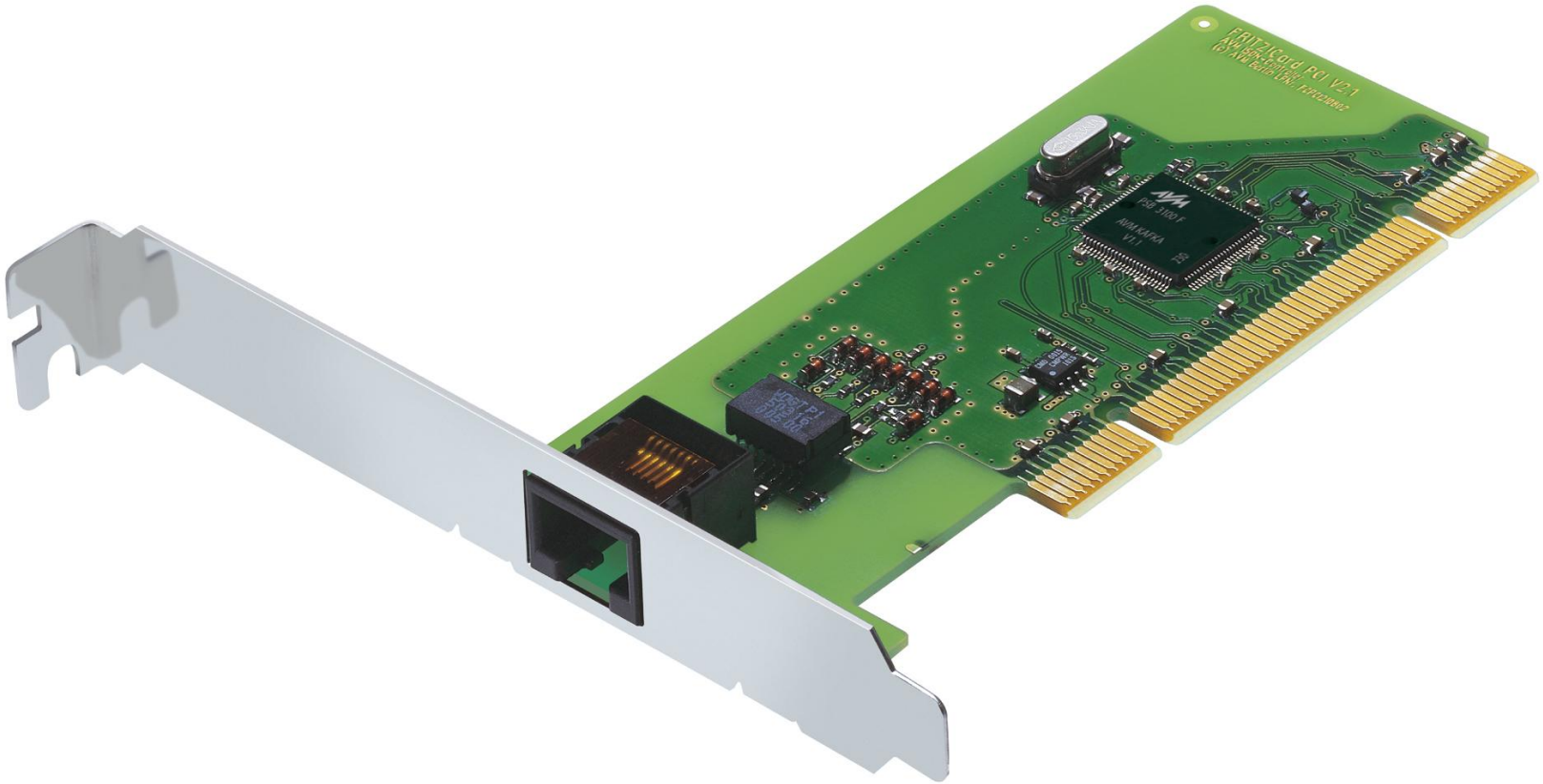
# Phân loại mạng máy tính theo kiến trúc mạng (tôpô).

- Star Topology
- Ring Topology
- Bus Topology
- Tree Topology
- Mesh Topology

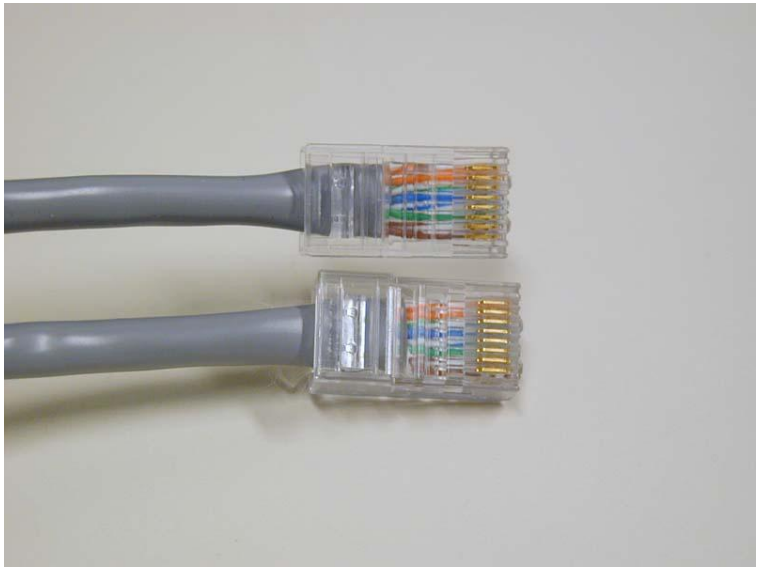
# Phần cứng/Phần mềm mạng

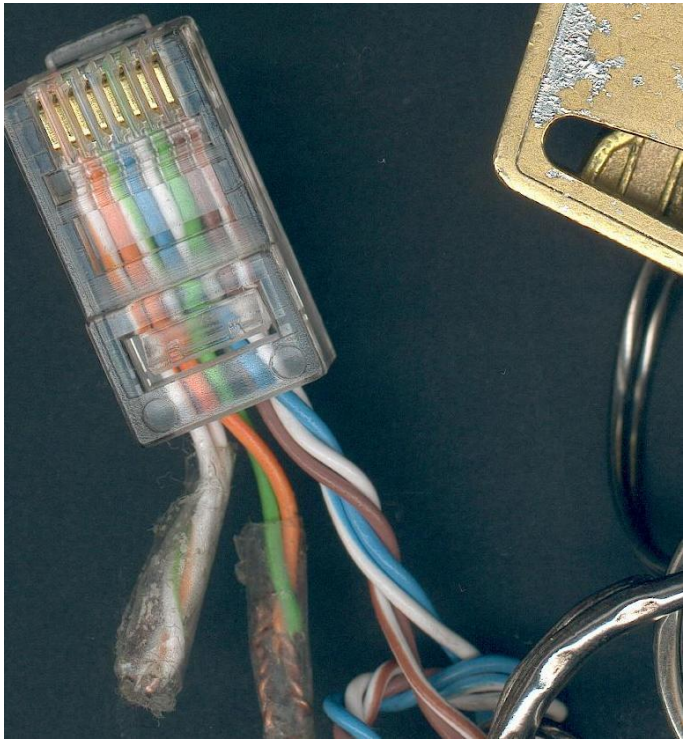
- Để thiết lập mạng cần phải có nhiều thiết bị phần cứng và phần mềm mạng.
- Phần cứng:
  - Card mạng
  - Cáp + đầu nối
  - HUB (mạng có trên 2 máy)

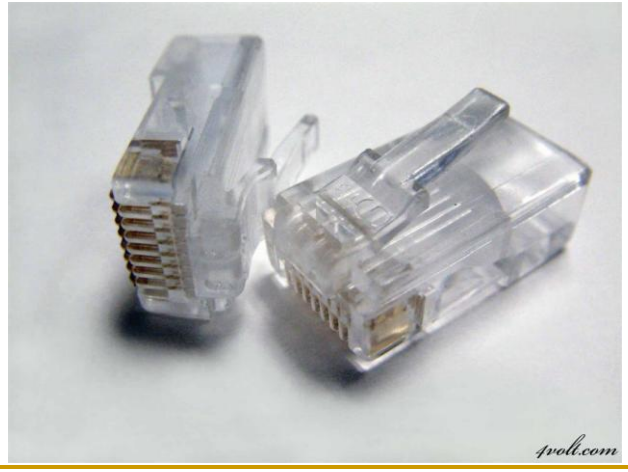
# Card mạng



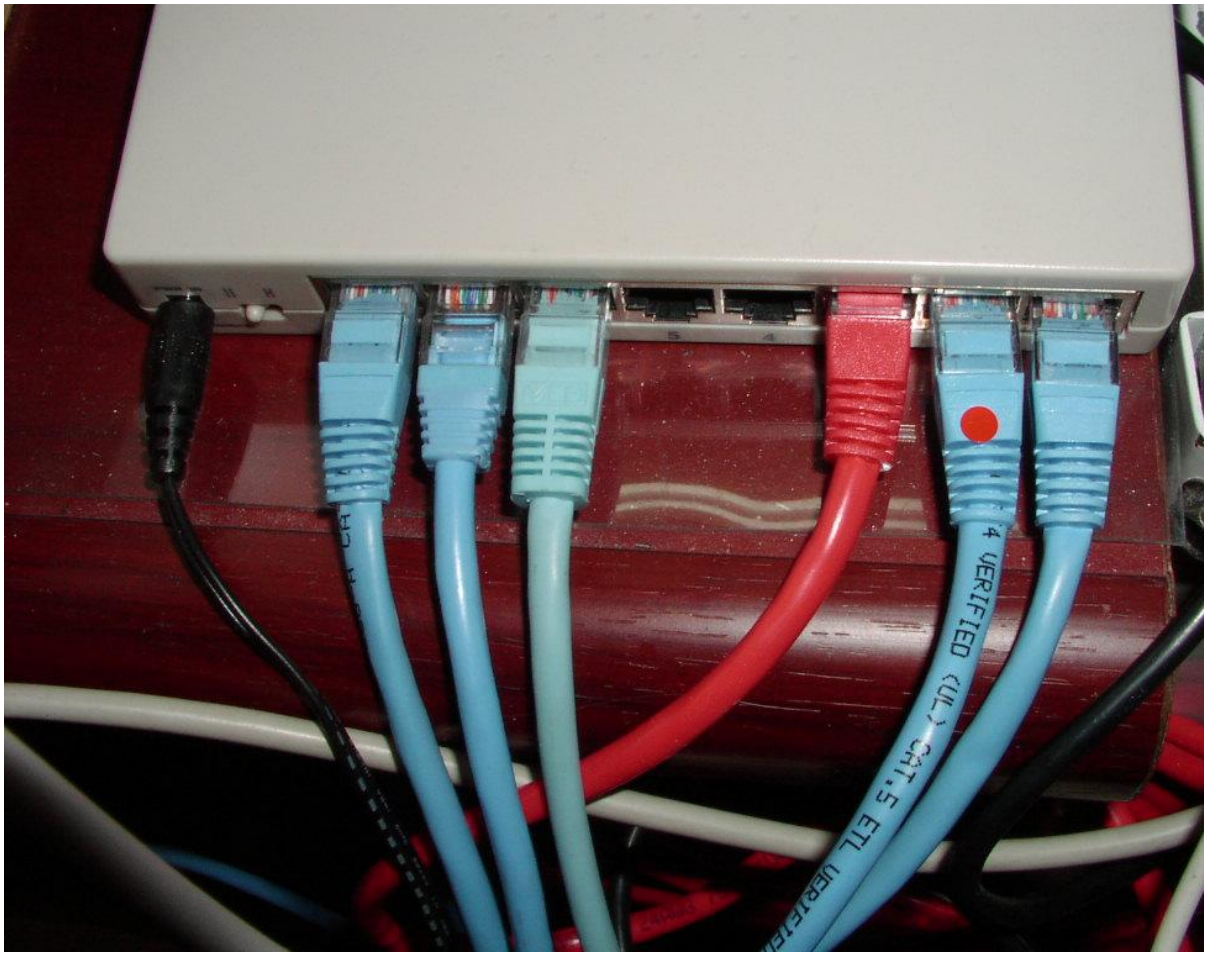
# Cáp và đầu nối







# HUB



# Phần cứng/Phần mềm mạng

- Phần mềm mạng
  - Phần mềm server
  - Phần mềm client
  - Phần mềm ứng dụng mạng
- Phần mềm mạng được cài đặt thông qua Hệ điều hành mạng
- Các loại hệ điều hành mạng:
  - Mạng server
    - Unix/Linux
    - Novel Netware
    - Win NT/2000/2003
  - Mạng peer-to-peer
    - Win 98/XP

# Mạng máy tính

## Các phương tiện truyền thông

# Nội dung

- Các loại phương tiện truyền thông
- Phương tiện hữu  tuyến
  - Cáp đồng
  - Cáp quang
- Phương tiên vô tuyến
  - Sóng vô tuyến radio
  - Viba
  - Tia hồng ngoại
  - Bluetooth

# Phương tiện truyền thông

- Phương tiện truyền thông là cách thức nối các máy tính lại với nhau.
- Có 2 loại phương tiện:
  - Hữu tuyến: dùng cáp để truyền dữ liệu giữa các máy tính
  - Vô tuyến: dùng sóng để truyền dữ liệu giữa các máy tính (không dây-wireless)

# Phương tiện hữu tuyến - Cáp đồng

- Dùng dây đồng để truyền tín hiệu dòng điện để biểu diễn thông tin truyền
- Vi dụ: Quy định
  - bit 1 → +5V
  - bit 0 → 0V
- Nhiễu: Tín hiệu dễ bị nhiễu
- Phải thiết kế loại cáp để có thể hạn chế nhiễu tối đa
- Có 2 loại cáp thông dụng
  - Cáp đồng trục (coorial cable)
  - Cáp xoắn đôi (twist-pair cable)

# Cáp đồng – Cáp đồng trục

- Tín hiệu được truyền qua lõi đồng
- Các lớp ngoài bảo vệ chống nhiễu
- Có 2 loại: dày (thick), mõng (thin)
  - Tính hiệu truyền xa tối đa 500m đối với cáp dày
  - Tính hiệu truyền xa tối đa 185m đối với cáp mõng, nhưng chi phí rẽ hơn, dễ di chuyển
- Muốn truyền xa hơn cần dùng thiết bị repeater để khuếch đại tính hiệu
- Tốc độ truyền tối đa 10Mb/s (10 triệu bit/1s)

# Cáp đồng trục

# Cáp đồng – Cáp xoắn đôi

- Dùng 2 hoặc 4 cặp dây xoắn đôi
- Có 2 loại:
  - STP (Shield twisted pair): có lớp vỏ bọc bên ngoài chống nhiễu tốt hơn
  - UTP (Unshield twisted pair): dùng trong môi trường bình thường

STP

UTP

# Cáp xoắn đôi - UTP

- Phân loại cáp UTP theo catelogy (CAT)
  - CAT1: không truyền data, chỉ truyền âm thanh
  - CAT2: truyền data, tốc độ 4Mbp/s
  - CAT3: truyền data, tốc độ 10Mbp/s
  - CAT4: truyền data, tốc độ 16Mbp/s
  - CAT5: truyền data, tốc độ 100Mbp/s
- Hiện nay, cáp UTP CAT5 được dùng phổ biến nhất
- Tín hiệu truyền tối đa 100m

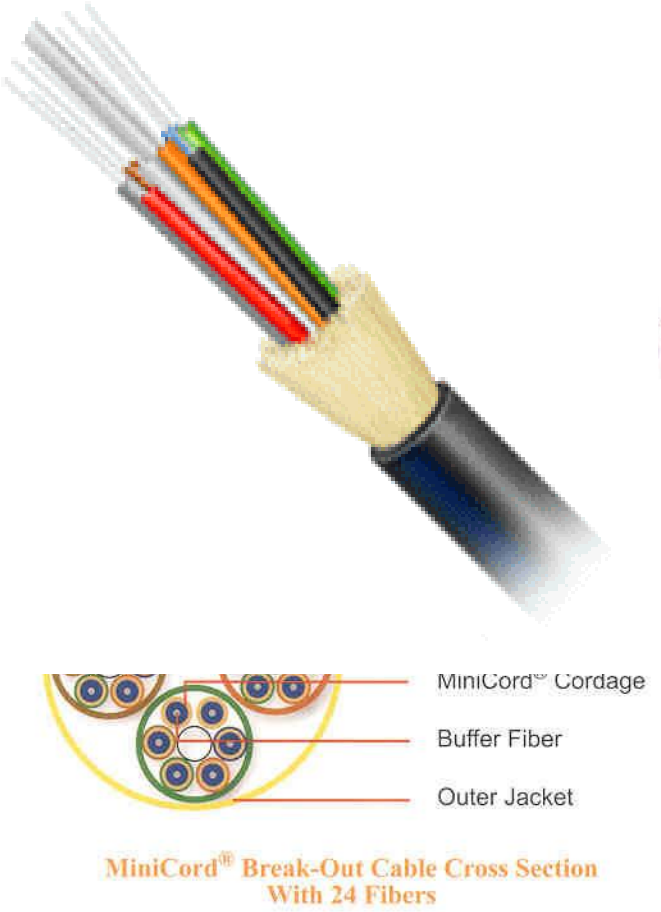
Nhận xét:

Cáp đồng trục truyền xa hơn, chống nhiễu tốt hơn nhưng cặp xoắn đôi lại truyền nhanh hơn

# Cáp quang-Fiber Optic Cable

- Người ta dung các sợi thủy tinh để chế tạo ra cáp quang
- Dùng ánh sáng để truyền dữ liệu
- Cáp quang dùng 2 sợi, 1 sợi truyền, 1 sợi nhận
- Cáp quang được nối vào một thiết bị gọi là ODF thiết bị này nối vào thiết bị "Media comverter" để chuyển tính hiệu điện thành quang và ngược lại
- Ưu điểm:
  - Không bị nhiễu
  - Tính hiệu truyền xa hơn (vài km →100Km)
  - Tốc độ nhanh hơn (1GBps = 1024MBps)
  - Khó gắn thiết bị nghe trộm
- Khuyết điểm
  - Chi phí cao
  - Khó cài đặt, đi cáp ( chỉ thích hợp làm mạng trục chính)

# Cáp quang-Fiber Optic Cable




MiniCord® Break-Out Cable Cross Section
With 24 Fibers

# Phương tiện vô tuyến

- Dùng sóng để truyền dữ liệu
  - Sóng radio (Mhz)
  - Sóng viba (Ghz)
  - Tia hồng ngoại (Thz)

# Sóng radio

- Card vô tuyến radio = angten + bộ thu phát sóng
- Sóng radio được phát theo mọi hướng
- Công suất: Chất lượng sóng mạng hay yếu
- Tần suất: Tần số sóng
  - Cao: tốc độ nhanh hơn, khoảng cách gần hơn
  - Thấp: tốc độ chậm hơn, khoảng cách xa hơn
- Ưu điểm: Không cần nối cáp
- Khuyết điểm:
  - Dể bị nhiễu
  - Tốc độ chậm hơn (tối đa khoảng 16Mbps)

# Sóng viba – Tia hồng ngoại

- Sóng vi ba có tần số cao hơn radio
- Viba chỉ phát theo 1 hướng → Không vượt qua được vật cản
- Tia hồng ngoại (infrared) dùng trong các remote
  - Được phát theo 1 hướng, nguồn phát phải thẳng hướng nơi nhận → không qua được vật cản
  - Chỉ hoạt động trong 1 phạm vi hẹp (phòng)
  - Ưu điểm: Không cần angten nên thường được ứng dụng trong các thiết bị di động (laptop, điện thoại di động)

# Mạng máy tính

## Truyền thông giữa 2 máy nối trực tiếp

# Nội dung

- Truyền thông khoảng cách gần
  - Chuẩn truyền thông RS-232
  - Cáp link COM
  - Tốc độ truyền – Band width
  - Các t/c của hệ truyền thông
- Truyền thông khoảng cách xa
  - Sóng mang
  - Modem
- Kỹ thuật truyền Baseband/Broadband
  - Truyền thông Baseband
  - Truyền thông Broadband
- Khung
- Kiểm soát lỗi
  - Mã dò lỗi
  - Mã sửa lỗi

# Truyền thông khoảng cách gần

- Chuẩn truyền thông RS-232
- Cáp link COM
- Tốc độ truyền – Band width
- Các tính chất của hệ truyền thông

# Chuẩn truyền thông RS-232

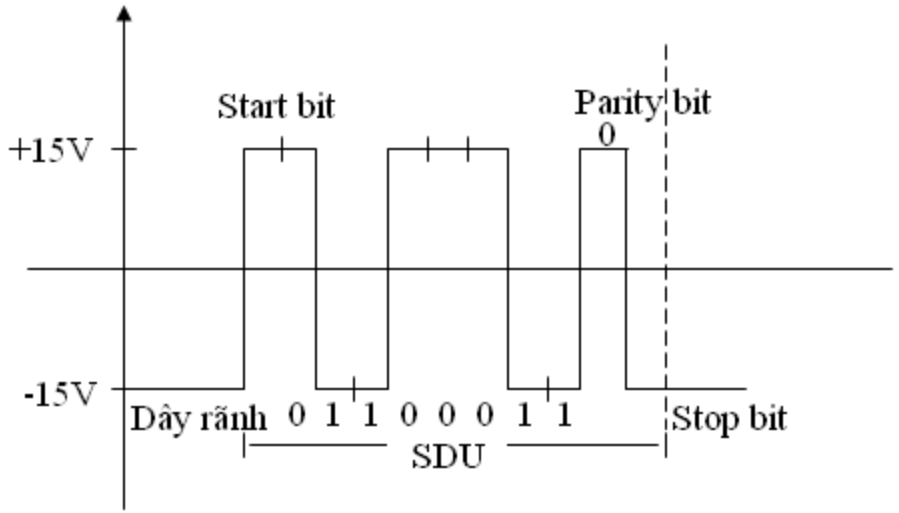
- Nối qua cổng truyền tin nối tiếp com1/com2 cho phép truyền thông giữa PC/PC, PC/Cân vàng điện tử, PC/máy in…
- Truyền thông nối tiếp bất đồng bộ
- Khoảng cách tối đa 50 feet
- Dùng dòng điện truyền dữ liệu qua cáp link COM, chỉ sử dụng 2 mức điện thế +/- 15V
  - +15V biểu diễn bit 0
  - -15V biểu diễn bit 1
  - Khi dây rãnh vẫn giữ mức điện thế -15V
- Một ký tự được truyền qua đơn vị truyền SDU (Serial data unit)
- Cấu trúc SDU gồm:
  - 1 start bit,8 bit data, 1 parity bit, 1 stop bit
  - khởi đầu (+15V),biểu diễn mã ký tự, kiểm lỗi, kết thúc(-15V)

# Chuẩn truyền thông RS-232

- parity bit: bit kiểm tra chẵn lẻ, dùng để kiểm lỗi ký tự truyền có chính xác hay bị lỗi
  - Kiểm tra chẵn (even)
    - parity bit = 0: tổng số bit 1 của ký tự là số chẵn
    - parity bit = 1: tổng số bit 1 của ký tự là số lẻ
  - Kiểm tra lẻ (odd): ngược lại
- Kiểm lỗi: bên nhận tính lại parity bit (dựa vào 8 bit data) so sánh với parity bit bên gởi
  - Nếu không khớp: ký tự truyền bị lỗi
  - Nếu khớp: xem như không bị lỗi

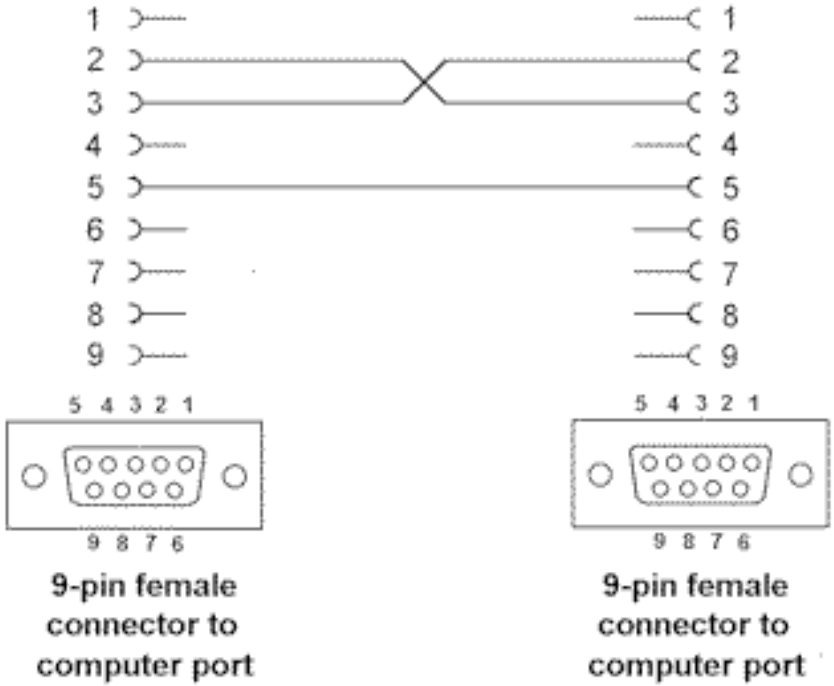
# Chuẩn truyền thông RS-232

- Thí dụ: Truyền ký tự "c" tại SDU và vẽ sơ đồ dòng điện tương ứng. Giả sử dùng phép kiểm chẵn
- Giải:
  - Tại SDU biểu diễn "c" = 99 = 63 Hex = 01100011
  - 1 parity bit = 0 (vì có 4 bit 1)
  - SDU: 1 start bit, 01100011, 0, 1 stop bit
- Vẽ sơ đồ dòng điện




- Nhận xét: parity chỉ kiểm được các lỗi đơn giản

# Cáp link COM




- Đầu D9 dùng 9 chân
  - TxD: chân truyền data
  - RxD: chân nhận data
  - Gnd: chân đất (ground)
  - DTR, DSR, RTS, CTS, CD, RI dùng để xác định các tính hiệu điều khiển
  - Chỉ cần 3 chân chính TxD,RxD,Gnd

- Có thể dùng phần mềm NC để kết nối 2 máy tính qua cổng COM theo chuẩn RS-232

# Tốc độ truyền – Band width

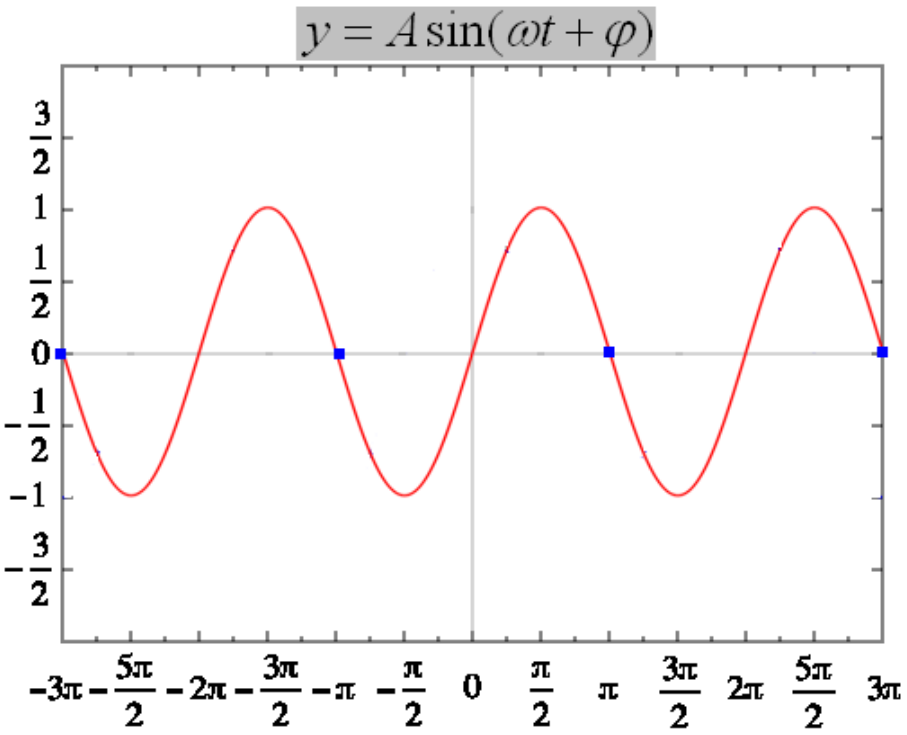
- Tốc độ truyền đo theo đơn vị bps (bit per second) xác định tần số bit truyền trên 1 giây
  - 1 kbps = 1000 bps
  - 1 Mbps = 1000 kbps
  - 1 Gbps = 1000 mbps
- Band width (băng thông/dải tần) xác định tốc độ tối đa mà phần cứng truyền thông cho phép.
- Mỗi hệ truyền thông có 1 band width xác định.
- Trong thực tế tốc độ truyền thông thực sự luôn thấp hơn band width nhiều lần.
- Chuẩn RS-232 qua cổng COM tốc độ tối đa 128 kbps

# Các tính chất của hệ truyền thông

- Simplex (đơn công)
  - Hệ truyền thông 1 chiều
  - Chỉ có thể truyền hoặc chỉ có thể nhận
  - Thí dụ: Television broastcast
- Half duplex (bán song công)
  - Hệ truyền thông 2 chiều
  - Có thể truyền và nhận không đồng thời
  - Thí dụ: khi dùng cáp đồng trục
- Full duplex (toàn song công)
  - Hệ truyền thông 2 chiều
  - Có thể truyền và nhận 1 cách đồng thời
  - Thí dụ: khi dùng cáp COM chuẩn RS-232 là full duplex

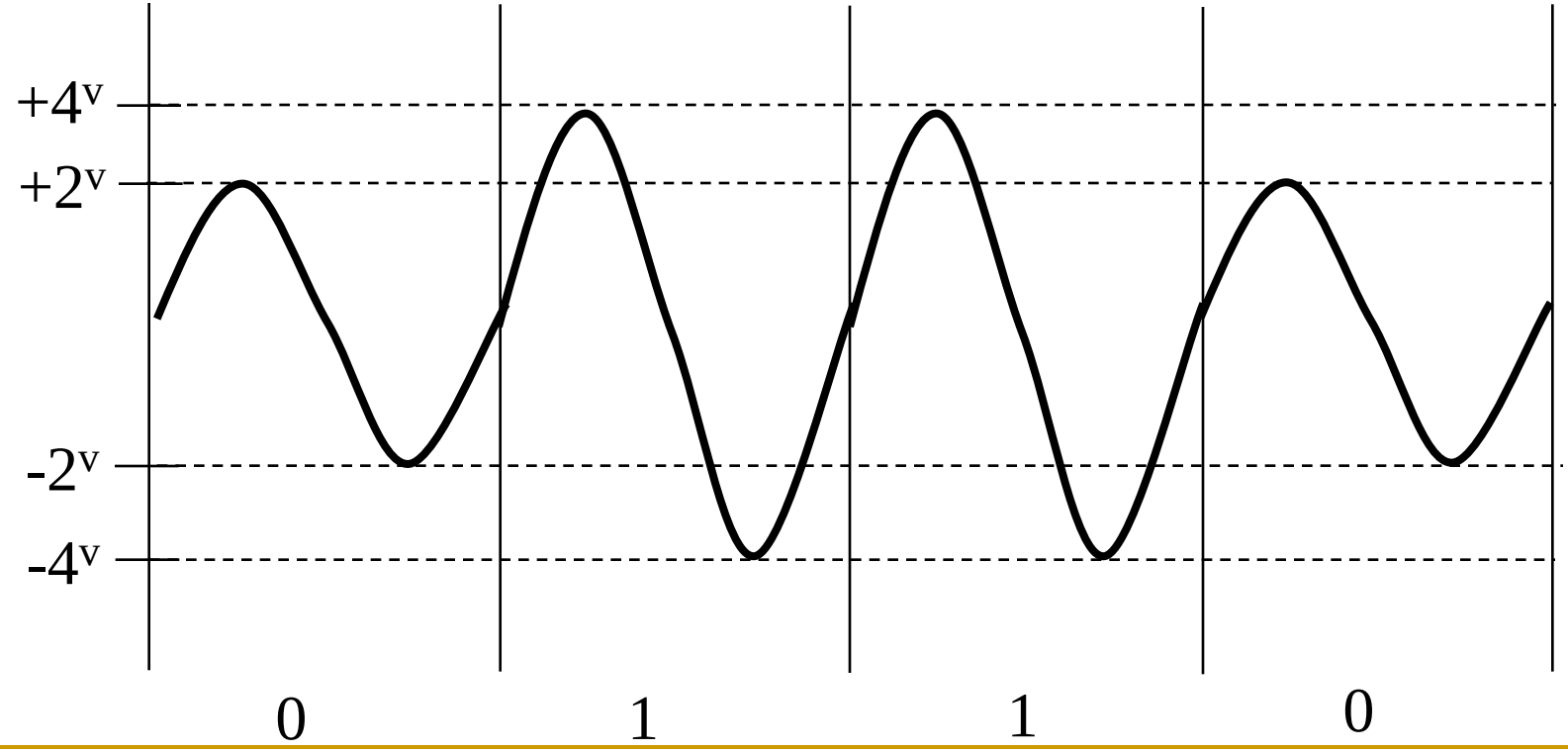
# Truyền thông k/c xa – sóng mang

- Truyền thông khoảng cách xa sử dụng tín hiệu dao động tuần hoàn liên tục hình Sin gọi là sóng mang (carrier)
- Để gởi data qua sóng mang ta phải điều chế sóng mang (modulation)
- Có 3 phương pháp điều chế
  - Điều biên
  - Điều tần
  - Điều pha



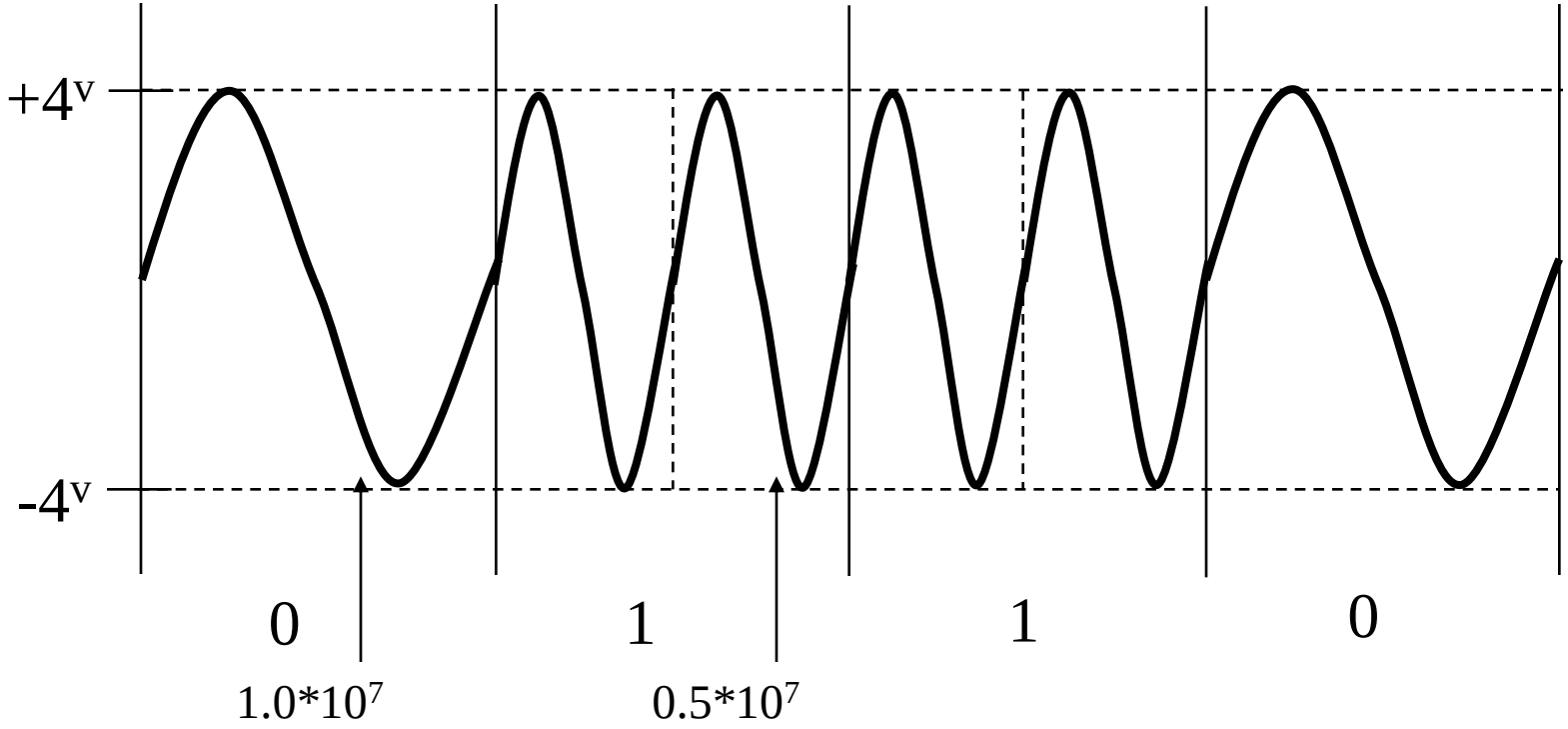
# Sóng mang – điều biên

- Thay đổi biên độ để điều chế sóng
- Thí dụ: Quy định
  - Biên độ 2 biểu diễn bit 0
  - Biên độ 4 biểu diễn bit 1



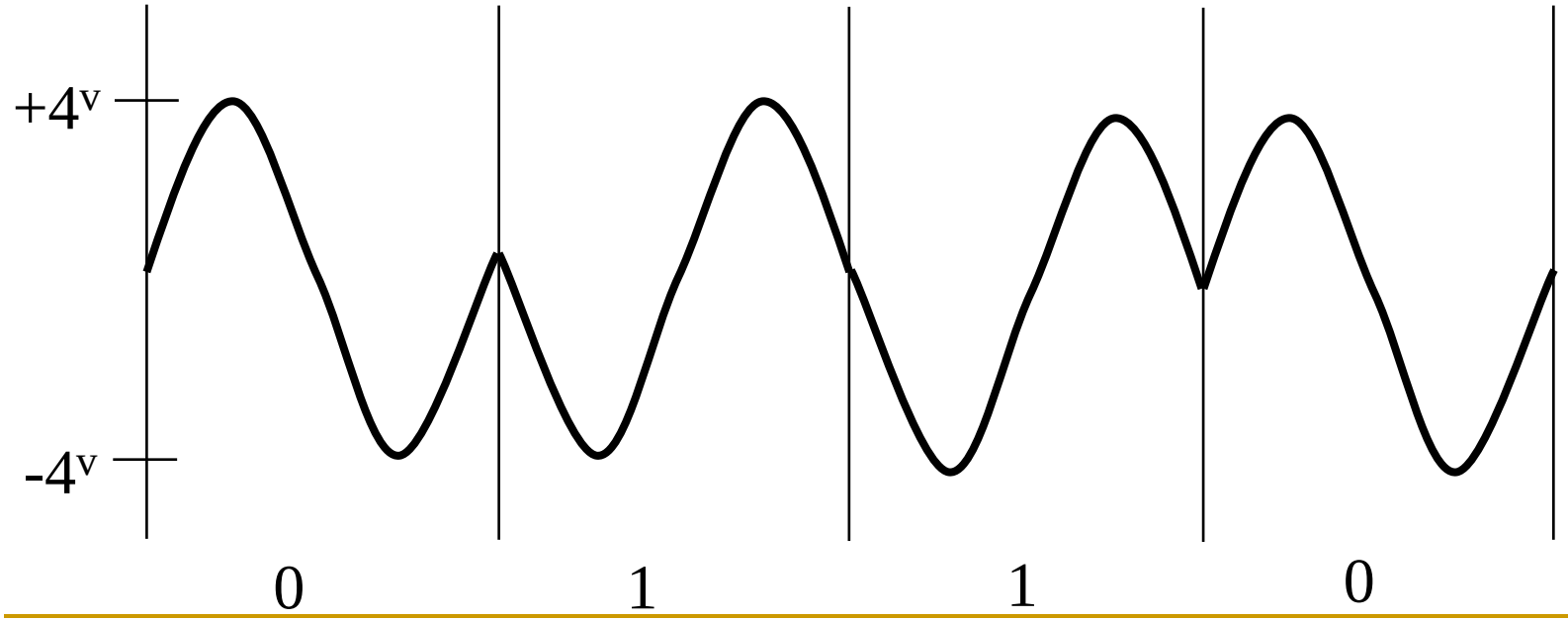
# Sóng mang – Điều tần

- Thay đổi tần số để điều chế sóng mang
- Thí dụ:
  - Tần số $1.0*10^7$ biểu diễn bit 0
  - Tần số $0.5*10^7$ biểu diễn bit 1



# Sóng mang – Điều pha

- Thay đổi pha để điều chế sóng mang
- Sự thay đổi pha gọi là lệch pha, mạng máy tính thường dùng pp lệch pha
- Thí dụ:
  - Lệch pha $\pi/2$ biểu diễn bit 0
  - Lệch pha $\pi$ biểu diễn bit 1



# Modem (Modulator)

- Modem là phần cứng cơ bản để truyền thông khoảng cách xa
- Modem có 2 loại chính:
  - Mạch điều chế (modulator) chuyển đổi tín hiệu dòng điện sang sóng mang tương ứng.
  - Mạch giải điều chế (demodulator) chuyển đổi tín hiệu sóng mang về dòng điện tương ứng.
- Có nhiều loại modem:
  - Modem quang: nối qua cáp quang
  - Modem vô tuyến: truyền bằng vô tuyến
  - Modem quay số: truyền qua hệ thống điện thoại (phổ biến nhất)

# Hoạt động của modem quay số

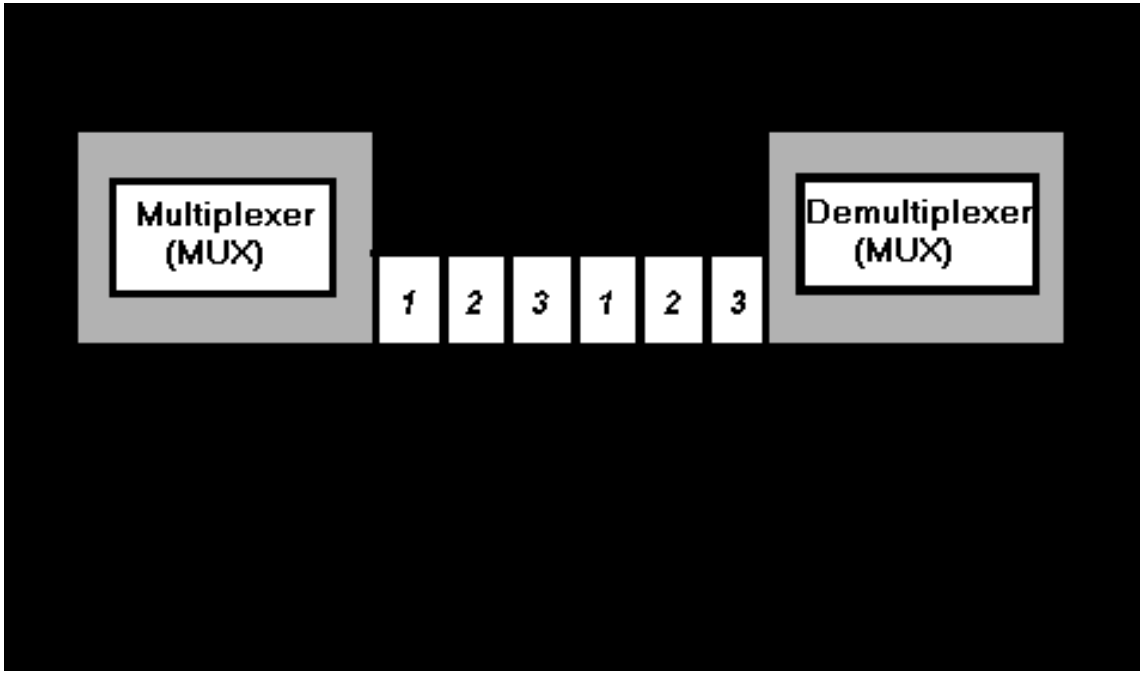
- Modem quay số có thêm mạch giả lập điện thoại thực hiện các thao tác sau bằng lệnh:
  - Nhấc ống nghe
  - Quay số
  - Gác máy
- Modem bắt đầu ở chế độ gọi: ra lệnh nhấc ống nghe, nghe tín hiệu điện thoại  và quay số
- Modem nhận ở chế độ đáp, trả lời cuộc gọi; 2 modem bắt đầu kết nối với nhau
- 2 modem trao đổi thông tin qua sóng mang
- Để kết thúc truyền thông, modem ra lệnh gác máy

# Kỹ thuật truyền Baseband/Broadband

- Truyền thông baseband (dải cơ sở)
  - 1 tín hiệu dữ liệu dùng toàn bộ băng thông đường truyền
  - Tại mỗi thời điểm chỉ có 1 máy truyền, các máy khác phải đợi
- Truyền thông broadband
  - Băng thông đường truyền được chia thành nhiều kênh.
  - Mỗi kênh có thể truyền 1 tín hiệu khác nhau.
  - Kỹ thuật này cho phép nhiều tín hiệu có thể truyền đồng thời qua đường truyền.
  - Thí dụ: Băng thông đường truyền 640kbps có thể chia thành 10 kênh truyền, mỗi kênh tốc độ 64kbps
- Phần cứng có thể truyền thông broad cast là thiết bị Multiplexor (bộ điều kênh) và Demultiplexor (bộ tách kênh)

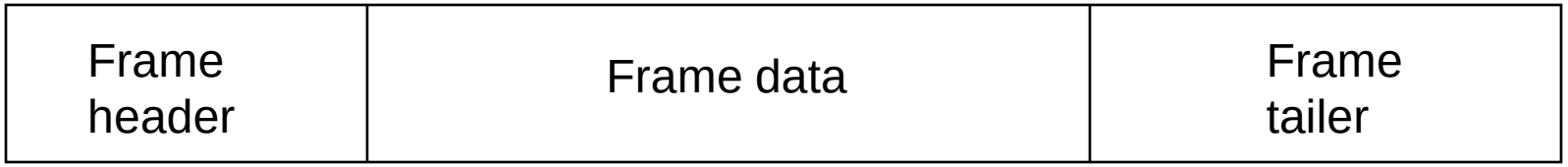
# Kỹ thuật truyền Baseband/Broadband

- Phương pháp dồn kênh chia tần (FDM): các tín hiệu với tần số khác nhau có thể dồn lại thành 1 tín hiệu
- Phương pháp dồn kênh chia thời (TDM): chia trục thời gian thành các khe thời gian, mỗi khe tạo thành một kênh truyền.



# Khung (frame)

- Mạng máy tính thường cung cấp giao diện truyền dữ liệu theo khung
- Một khung chứa nhiều byte dữ liệu




- Phần header/tailer chứa thông tin điều khiển
- Phần data: chứa dữ liệu cần truyền
- Thời gian truyền khung: $t = t_{startup} + t_{tranfer}$

  $t_{starup}$: t/g tạo khung và chuẩn bị truyền kích cỡ khung tối đa bao nhiêu

# Khung

- Khung nhỏ:
  - Khung chứa ít byte data
  - 1 lần truyền được ít byte
  - Tốn thời gian $t_{starup}$ và thời gian truyền header/tailer → không hiệu quả
- Khung quá lớn:
  - 1 lần truyền được nhiều byte → khung truyền rất lâu
  - Đối với mạng dùng chung đường truyền: 1 máy truyền các máy khác phải đợi.
  - Nếu khung truyền bị lỗi (dù sai 1 bit) phải truyền lại cả khung.
- Nên chọn khung có kích cỡ trung bình khoảng vài Kilobyte

# Khung

- Thí dụ: Truyền tập tin có dung lượng 123.500 byte trên hệ truyền thông tốc độ 64kbps. Tính thời gian truyền nếu sử dụng khung kích cỡ tối đa 1520byte (1500 byte data, 20byte header)
- Chia tập tin thành các khung, lấy 123.500/1500 = 82,33...
  - Chia thành 82 khung đủ 1500 byte
  - Chia thành 1 khung đủ 500byte
- 1s truyền được 64000bit = 8000 byte
- Thời gian truyền tập tin
  - $t = 82(t_{starup} + 1520/8000) + 1(t_{startup} + 520/8000)$
- Mỗi công nghệ mạng có thể sử dụng các dạng khung khác nhau
- Hai máy muốn truyền thông phải thống nhất chung dạng khung

# Khung

- Thí dụ: 1 dạng khung đơn giản là khung soh/eot dùng 2 ký tự đặc biệt
  - soh: ký tự bắt đầu khung
  - eot: ký tự kết thúc khung

- Ưu điểm: có thể kiểm được một số lỗi đơn giản như lỗi khung (ví dụ không nhận được ký tự eot)
- Khuyết: nếu ký tự soh/eot xuất hiện trong data thì không phân biệt được
- Người ta dùng thêm 1 ký tự đặc biệt gọi là esc.
  - Bên gởi thay các ký tự trong data: soh →esc x, eot →esc y, esc →esc z
  - Bên nhận thay thế ngược lại: esc x → soh, esc y → eot, esc z → esc

# Kiểm soát lỗi

- Lỗi truyền thông là hiện tượng khó tránh trên thực tế do nhiều nguyên nhân: thời tiết, tiếng ồn,… là cho data bị truyền sai
- Mạng máy tính phải có chức năng kiểm soát lỗi, nếu phát hiện lỗi, phải yêu cầu bên gởi truyền lại.
- Phương pháp chung là: dùng mã kiểm lỗi
  - Bên gởi: thêm vào khung truyền 1 mã đặc biệt được tính theo 1 công thức nào đó dựa vào vùng data gọi là mã kiểm lỗi
  - Bên nhận: kiểm lỗi bằng cách tính lại mã so sánh với mã bên gởi
    - Không khớp: khung truyền bi lỗi
    - Khớp: xem như không lỗi
  - Có 2 loại mã kiểm lỗi:
    - Mã dò lỗi
    - Mã sửa lỗi

# Mã dò lỗi (error detecting code)

- Phát hiện được lỗi nhưng không xác định được vị trí lỗi
- Parity: phép kiểm tra chẵn lẻ (dùng trong chuẩn RS-232) hiệu quả chưa cao chỉ kiểm được lỗi 1 bit hay số bit lẻ.
- Check sum ( kiểm tổng)
  - Dữ liệu truyền gồm 1 dãy các byte $d_1,d_2,\ldots d_n$
  - Check sum = $\sum_{i=1}^{n} di$
  - Thí dụ: xét dữ liệu gồm 5 ký tự A,B,C,D,E
    - Check sum = 41 + 42 + 43 + 44 + 45 = 014F (Hex)
    - Tạo khung soh | 4142434445 | eot | 014F
    - Bên nhận kiểm lại checksum so với checksum bên gởi xem có bị lỗi không
  - Nhận xét: checksum không kiểm được tất cả các lỗi
  - Thí dụ bên nhận soh | 4142434544 | eot | 014F
  - Tính lại Checksum = 014F, khớp nhưng thực chất truyền sai

# CRC (cyclic redundancy check)

- Kiểm kiểu dư vòng
- Dùng đa thức bậc n: $a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x^1 + a_0$
- Đa thức nhị phân là đa thức có hệ số 0 hay 1. Có tương ứng 1-1 giữa đa thức nhị phân và dãy số nhị phân
- Thí dụ: $x^5 + x^3 + x + 1 \rightarrow 101011$
- Thuật toán tính CRC của dãy m_bit
  - Dãy m_bit ~ đa thức nhị phân M(x)
  - Chọn 1 đa thức nhị phân G(x) bậc m gọi là đa thức sinh
  - Thêm n bit 0 vào sau dãy m_bit tạo dãy (m+n) bit ~ đa thức N(x)
  - Chia đa thức N(x)/G(x) theo module 2 dùng phép toán xóa bit
  - Phần dư là mã CRC n_bit

# Thí dụ tính CRC

- Cho dãy m_bit 10010110110111 và đa thức $G(x)=x^4 + x + 1$
- Ta có m=14, n=4, G(x) ~ 10011
- Thêm n=4 bit 0 vào m_bit 10010110110111 0000 ~ N(x)
- Lấy N(x)/G(x) ~ 10010110110111 0000/10011 ~ 001010
- CRC = 1010
- Kiểm lỗi CRC
  - Bên gởi: truyền dãy m_bit + CRC
  - Bên nhận: kiểm lỗi
    - Gọi M(x) ~ dãy m_bit + CRC bên gởi
    - T(x) ~ dãy m_bit + CRC bên nhận
    - T(x) = M(x) + E(x)
    - Nếu E(x) = 0: không có lỗi

| A | B | X-OR |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

# Kiểm lỗi CRC

- Nhận xét:
  - M(x)/G(x) chẵn → T(x)/G(x) = M(x)/G(x) +E(x)/G(x)
  - T(x)/G(x)
    - Chẵn: không lỗi
    - Lẻ: có lỗi → E(x)/G(x) khác 0 → E(x) khác 0 → có lỗi
  - Ta phải chọn G(x) sao cho thỏa E(x)/G(x) = 0 → E(x) =0
- Hệ quả:
  - CRC phục thuộc vào cách chọn đa thức sinh
  - Nếu chọn G(x) bậc 32 → phép kiểm lỗi 32 bit kiểm được 99%
- Các CRC thường được cài đặt bằng phần cứng

# Mã sửa lỗi (Error connecting code)

- Cho phép phát hiện và xác định vị trí lỗi
- Có thể sửa được lỗi → bên gởi không cần truyền lại
- Mã hamming: Cho phép sửa lỗi sai 1 bit
  - Cho dãy m_bit, mã hamming là thêm vào r_bit kiểu parity tạo thành dãy (m+r) bit
  - Các bit được đánh số bắt đầu từ 1 → m+r
  - Các bit mã hamming đặt ở các vị trí 1,2,4,8,...,$2^{r-1}$
  - Điều kiện r được chọn $m + r \leq 2^r - 1$

# Thí dụ tính mã Hamming

- Xét dãy m_bit với m=16
  - 1011010110110101
  - Tính mã Hamming?
- Giải:
  - Với m=16, theo điều kiện $m + r \leq 2^r - 1$ → r > 4. Xét r = 5 thỏa
  - Ta dùng 5 bit parity ở các vị trí 1,2,4,8,16
- Quy định:
  - bit 1: kiểu parity các bit {1/3/5/7/9/11/13/15/17/19/21}
  - bit 2: ---------- {2 3/6 7/10 11/14 15/18 19/}
  - bit 4: ---------- {4 5 6 7/12 13 14 15/20 21}
  - bit 8: ---------- {8 9 10 11 12 13 14 15}
  - bit 16: ---------- {16 17 18 19 20 21}

# Thí dụ tính mã Hamming

- Giả sử dùng phép kiểm parity chẵn
- Biểu diễn dãy (m + r) bit, r bit kiểu parity (0/1 ở vị trí chẵn/lẻ)

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 1 |

  - bit 1 = 1: vì có 7 số 1
  - bit 2 = 0: vì có 6 số 1
  - bit 4 = 0: vì có 6 số 1
  - bit 8 = 0: vì có 4 số 1
  - bit 16 = 1: vì có 3 số 1
- Mã Hamming sẽ gởi kèm m_bit là: 10001
- Để kiểm lỗi, bên nhận phải tính lại mã Hamming

# Thí dụ tính mã Hamming và sửa lỗi

- Giả sử bên nhận nhận được dãy m_bit 10110100101101O1 và mã Hamming là 10001. Hãy kiểm và sửa lỗi.
- Giải:
  - Tương tự thí dụ trước ta lý luận và sắp sếp (m+r) bit như sau

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 1 | | 0 | 1 | 1 | | 0 | 1 | 0 | 0 | 1 | 0 | 1 | | 1 | 0 | 1 | 0 | 1 |

  - Tính mã Hamming theo quy định (ở slide 28) và kiểm chẫn ta được:

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 1 |

  - Suy ra mã hamming mà bên nhận nhận được là: 10111
  - Tính lại : 10111 $\neq$ 10001. Suy ra sai tại bit 4,8

# Bên nhận kiểm và sửa lỗi

- bit 4 sai → A = {4,5,6,7/12,13,14,15/20,21} tập bit có thể sai
- bit 8 sai → B = {8,9,10,11,12,13,14,15} tập bit có thể sai
- Giao A và B → C= {12,13,14,15} tập các bit có thể sai
- bit 1 đúng → D = {1,3,5,7,9,11,13,15,17,19,21} đúng
- bit 2 đúng → E = {2,3,6,7,10,11,14,15,18,19} đúng
- bit 16 đúng → F = {16,17,18,19,20,21} đúng
- Từ tập D,E,F → {13,14,15} đúng
- Kết luận: bit 12 sai
- Sửa bit 12 từ 0 → 1
- Dãy m_bit đúng: 1011010110110101

# Bài tập

- Bài 1: Giả sử hệ truyền thông có tốc độ là 64Kbps và sử dụng cấu trúc khung kích cở 1520byte trong đó gồm 20 byte header và 1500 byte data. Cho tập tin A dài 16000 byte. Xác định thời gian truyền tập tin biết $t_{startup}$=15ms (milisecond)

- Bài 2: Cho khung dữ liệu truyền 16 bit dùng mã sửa lỗi hamming 5bit. Giả sử máy nhận được dãy bit như sau:

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 0 |

  - Trong đó 5 bit 1,2,4,8,16 là mã hamming
  - Cho biết khung dữ liệu nhận có bị lỗi hay không? Nếu bị lỗi hãy sửa lỗi

# Mạng máy tính

## Mạng LAN

# Nội dung

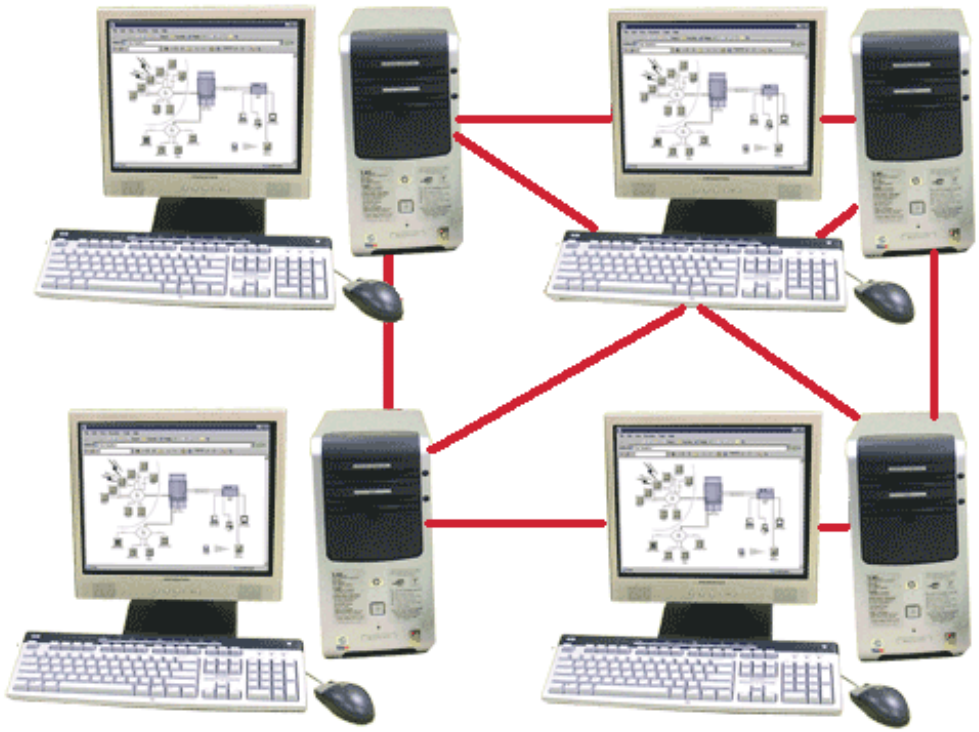
- Truyền thông giữa nhiều máy
  - Mạng điểm – điểm (point – to – point)
  - Mạng chia sẻ dùng chung đường truyền
- Các mô hình mạng LAN
  - Mô hình BUS
  - Mô hình STAR
  - Mô hình RING
  - Các mô hình kết hợp: BUS – BUS, BUS – STAR, STAR – STAR.
- Hoạt động của mạng LAN
  - LAN card
  - Địa chỉ trạm trên LAN
  - Hoạt động của LAN

# Nội dung

- Phương pháp truy cập trên LAN
  - Phương pháp CSMA/CD
  - Phương pháp truy cập token passing
- Các công nghệ mạng LAN
  - Mạng Ethernet
    - Đặc điểm
    - Các cấu hình Ethernet 10 Base
    - Mã hóa tính hiệu truyền
    - Cấu trúc khung Ethernet
    - Fast Ethernet 100 Base
  - Mạng Token Ring

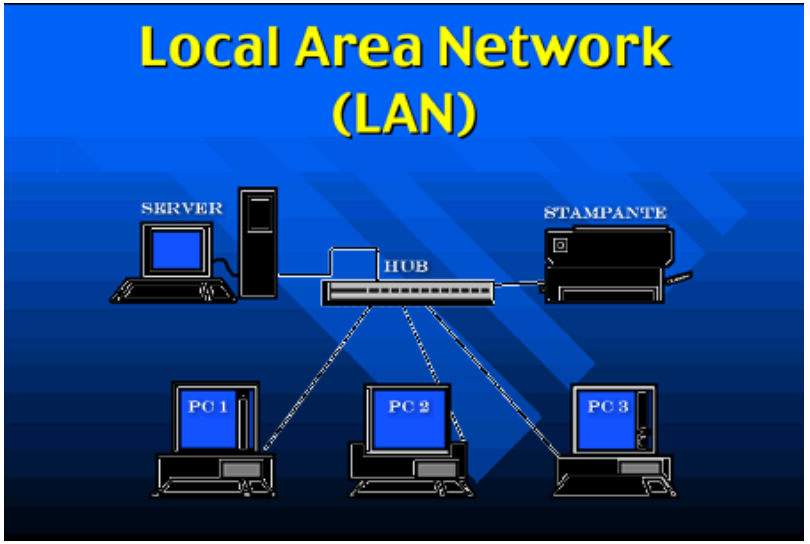
# Mạng điểm – điểm (point – to – point)

- Mỗi cặp máy sử dụng 1 kết nối khác nhau
- 3 máy → 3 kết nối
- 4 máy → 6 kết nối
- N máy → N(N-1)/2 kết nối
- Nhận xét: Mạng điểm - điểm chỉ thích hợp khi N nhỏ



# Mạng chia sẻ dùng chung đường truyền

- Các máy tính trên mạng có thể chia sẻ dùng chung các kết nối → tiết kiệm được số kết nối
- Mạng cục bộ LAN là mạng chia sẻ dùng chung đường truyền sao cho các máy có thể truy cập thông tin với nhau trên mạng
- Phạm vi hoạt động LAN: vài km, thích hợp với các văn phòng, công ty, trường học,...

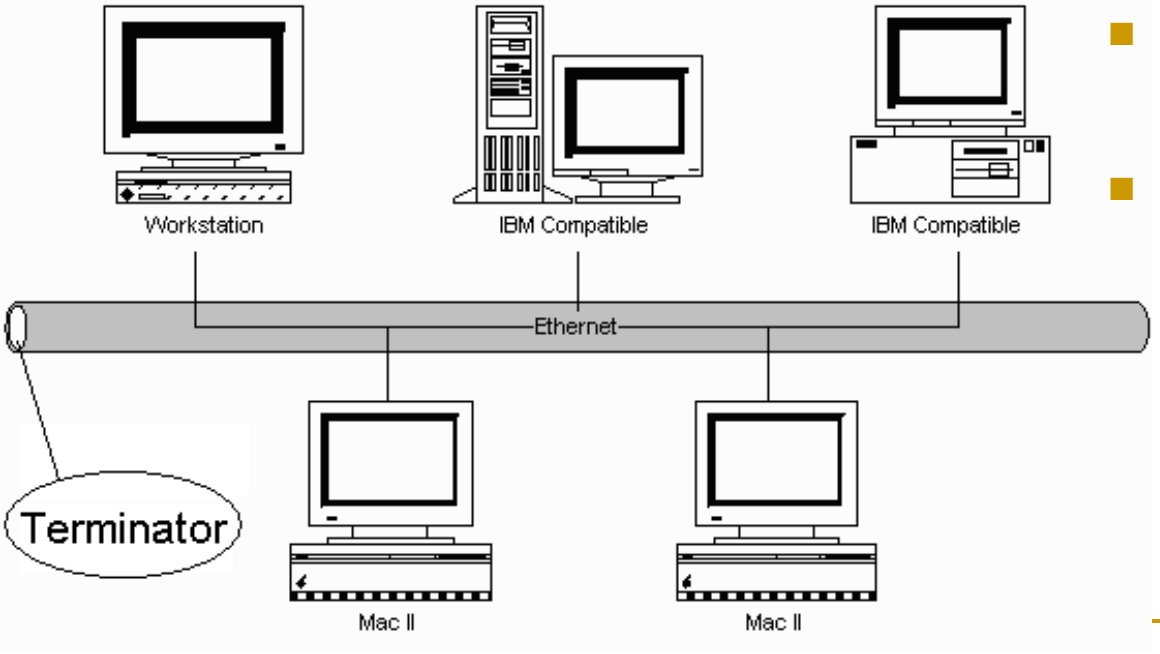


# Các mô hình LAN

- Mô hình LAN xác định cách thức các máy tính kết nối lại với nhau như thế nào
- Có nhiều mô hình:
  - BUS
  - STAR
  - RING
  - Mesh
  - Tree (ít dùng)

# Mô hình BUS

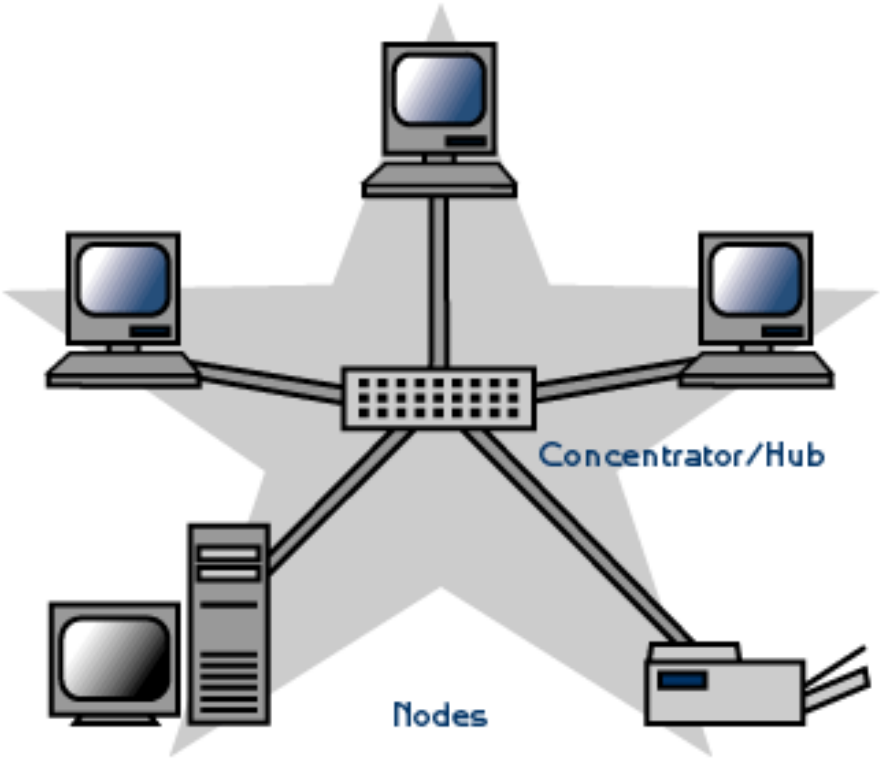
- Các máy được nối với nhau vào 1 đường truyền chung gọi là BUS
- Tín hiệu được truyền theo 2 hướng của bus → tất cả các máy đều nhận được tín hiệu.
- Tín hiệu đến 2 đầu bus có thể bị dội lại → gây nhiễu.
- Terminator dùng để hấp thu tín hiệu không cho dội lại




- Ưu: dễ lắp đặt, đơn giản, ít tốn cáp.
- Khuyết:
  - Bus đứt → toàn bộ mạng tê liệt
  - Khó thêm máy mới
  - Khó bảo trì cáp
  - Hiệu suất mạng giảm đáng kể nếu nhiều máy sử dụng mạng

# Mô hình STAR

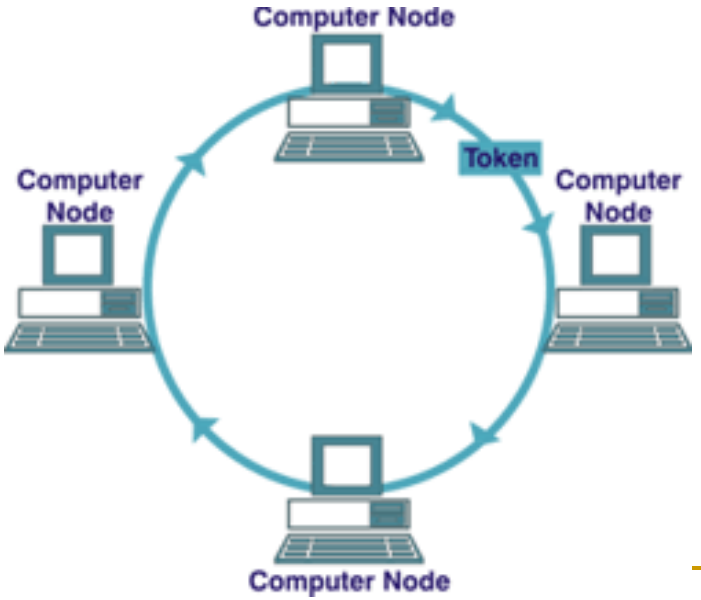
- Các máy được nối vào 1 hộp mốc trung tâm gọi là HUB
- HUB nhận tín hiệu từ 1 máy gởi đến truyền tín hiệu đến tất cả các máy khác
- Switch (HUB thông minh): nhận tín hiệu gởi đến, chỉ truyền tín hiệu đến máy cần nhận

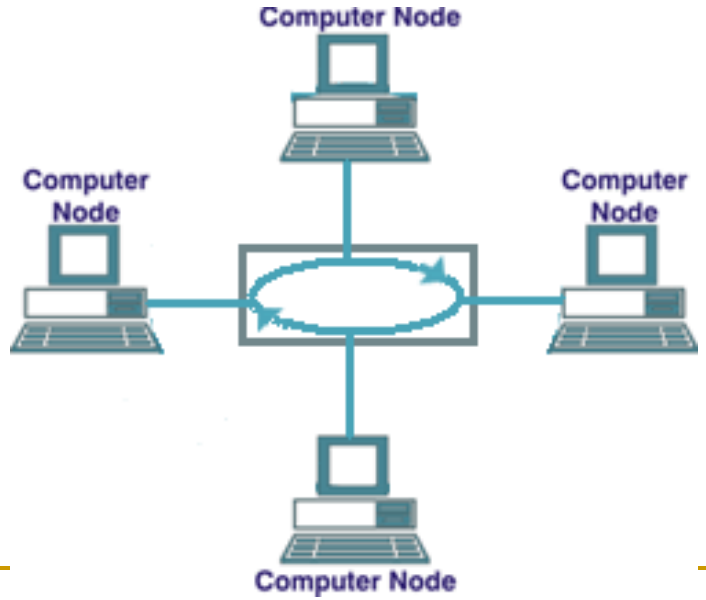



- Ưu:
  - Dễ thêm/bớt máy vào mạng
  - Dễ bảo trì cáp, khi 1 sợi cáp đứt chỉ một máy nối với cáp không sử dụng được mạng, các máy khác vẫn vào mạng bình thường
  - Nếu dùng Switch hiệu suất mạng vẫn đảm bảo nếu nhiều máy sử dụng mạng
- Khuyết:
  - HUB hư → mạng tê liệt
  - Chi phí cao hơn (chi phí cho HUB, nhiều cáp hơn)

# Mô hình RING

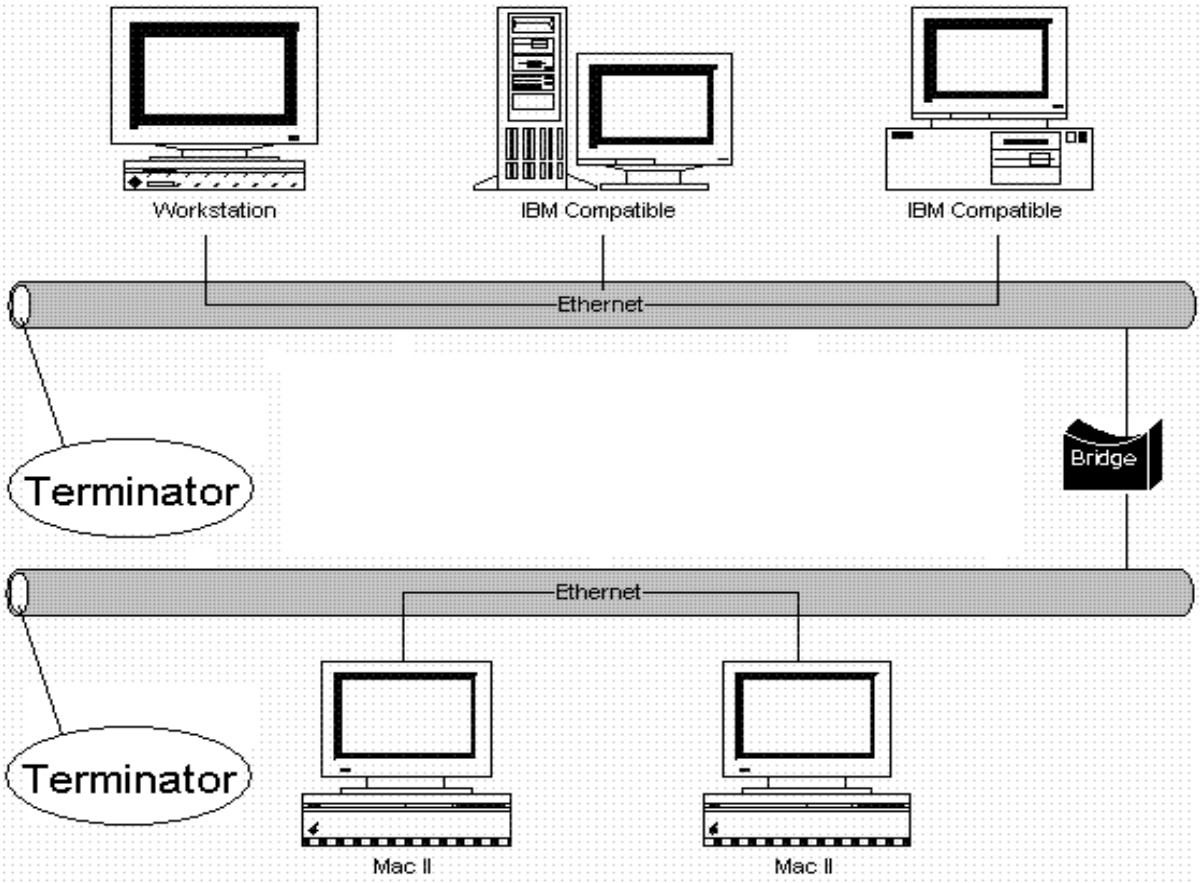
- Các máy nối trực tiếp vào 1 vòng tròn
- Tín hiệu được truyền theo 1 chiều trên vòng
- Có 2 loại vòng:
  - Trực tiếp
  - Qua HUB vòng
- Vòng đứt → mạng tê liệt



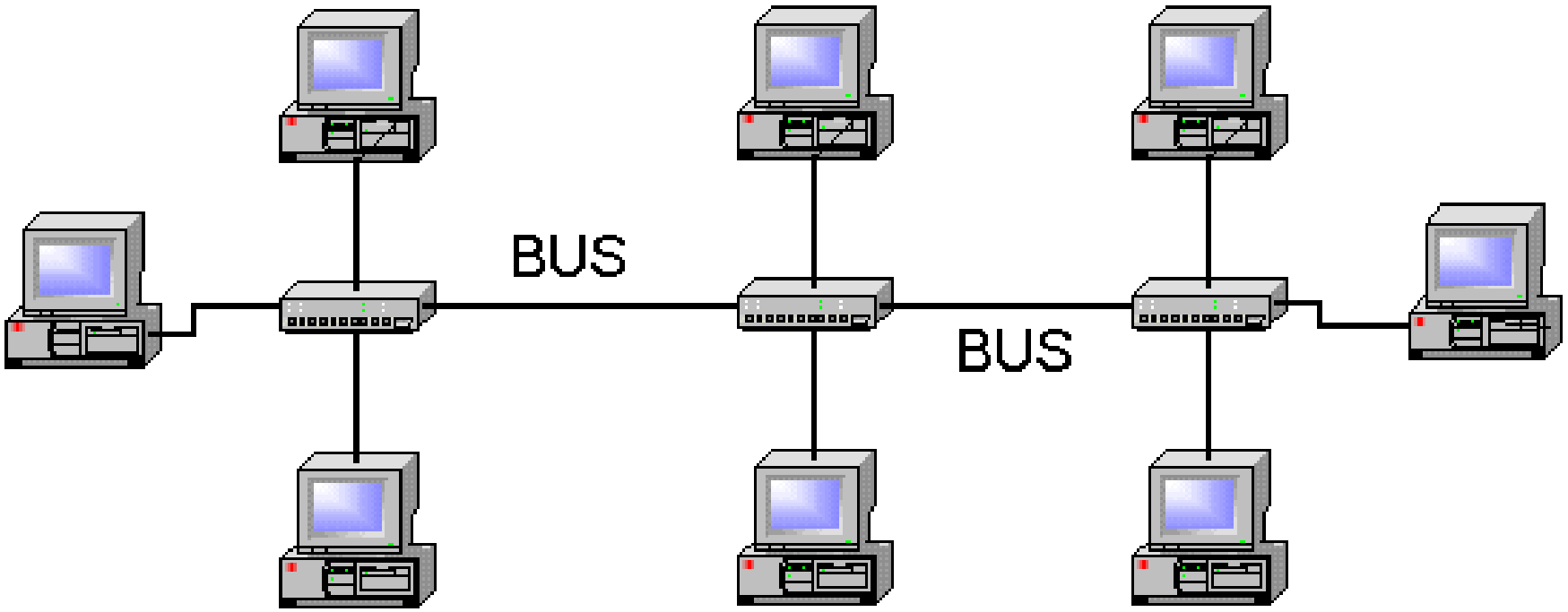
# Các mô hình kết hợp

- BUS – BUS: Các bus nối với nhau qua thiết bị cầu nối bridge → giảm tải trên BUS nếu BUS quá nhiều máy



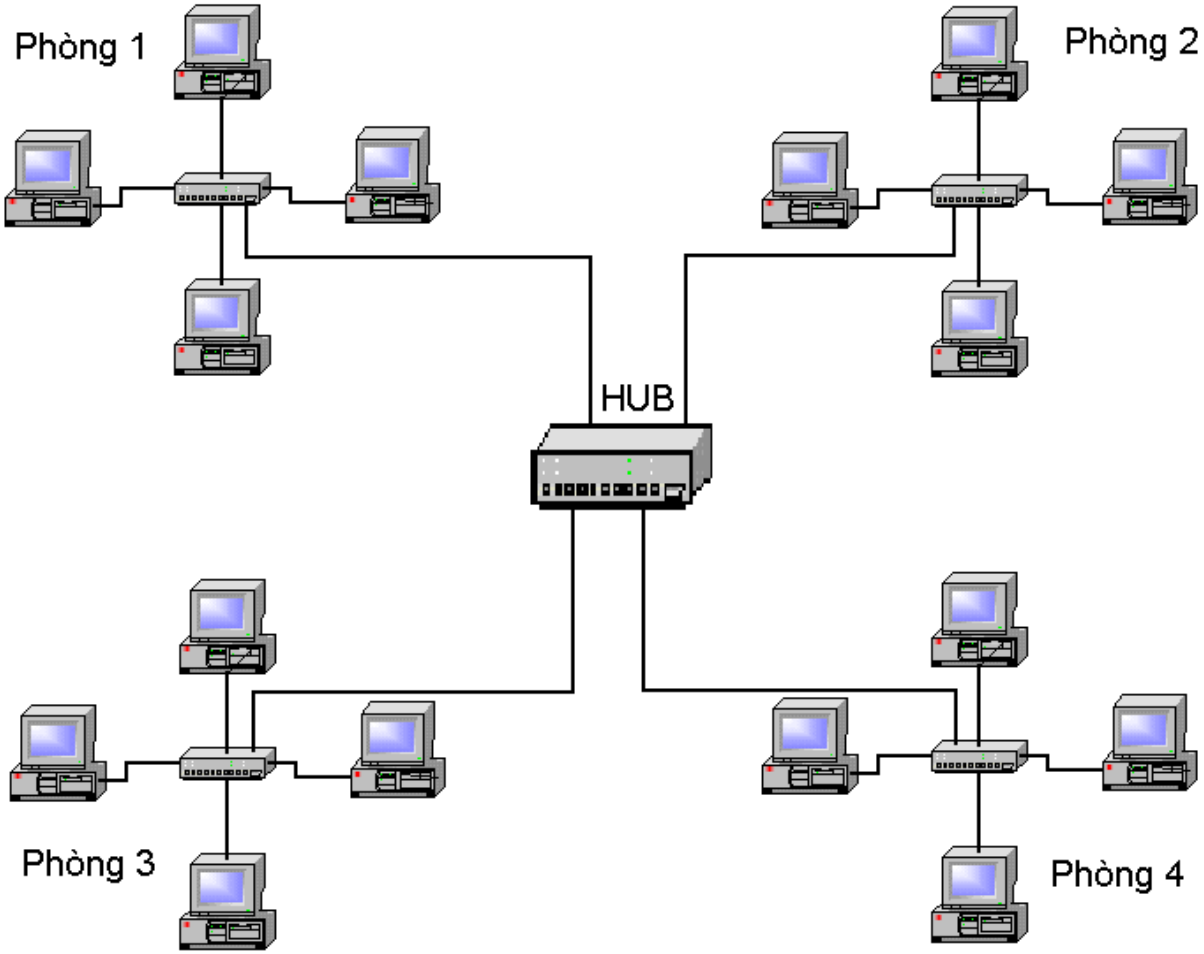
# Các mô hình kết hợp

- BUS-STAR



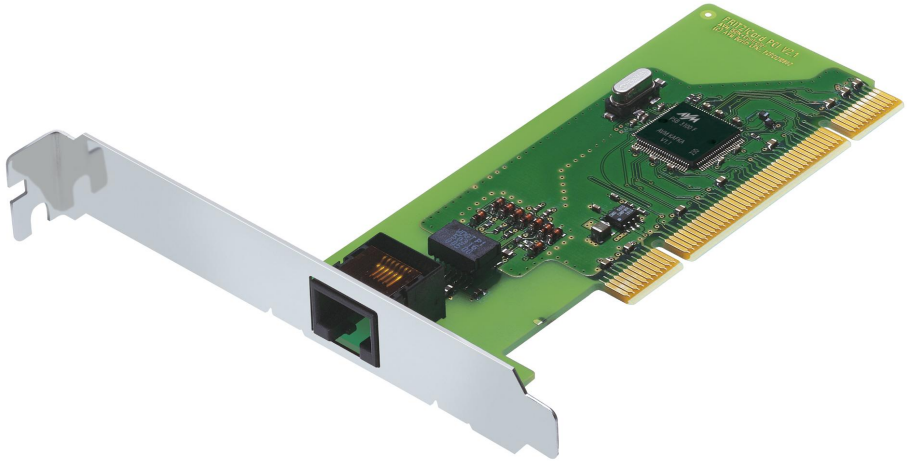
# Các mô hình kết hợp

- STAR-STAR



# Hoạt động của LAN – Card mạng

- Thiết bị cơ bản để nối mạng LAN là card mạng (LAN card)
- LAN card có chức năng truyền/nhận dữ liệu theo khung
- Cấu trúc LAN card:
  - Chip điều khiển: điều khiển các hoạt động trên LAN card
  - Bộ thu phát
  - Vùng đệm: bộ nhớ nằm trong Card
  - Đầu nối cáp
  - Boot ROM (option)
- Cài đặt LAN card: cấu hình
  - Đường IRQ (0→15): đường liên lạc với CPU
  - I/O port



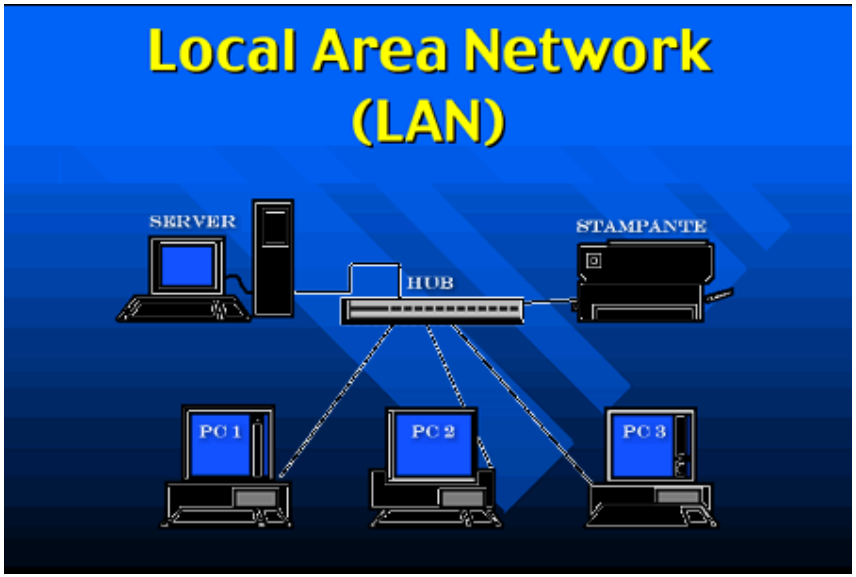
# Địa chỉ trạm trên LAN

- Để phân biệt các máy tính trên LAN, mỗi máy được quy định 1 địa chỉ duy nhất gọi là địa chỉ trạm
- Địa chỉ trạm trên LAN được quy định bởi phần cứng LAN Card (địa chỉ vật lý – MAC (Medium Access Control))
- Có 3 cách quy định địa chỉ:
  - Địa chỉ tĩnh: mỗi LAN Card khi sản xuất được gán 1 địa chỉ duy nhất trong phần cứng LAN Card
  - Địa chỉ khả cấu hình: một số LAN Card cho phép người dùng tự quy định được địa chỉ LAN Card bằng phần mềm.
  - Địa chỉ động: gán địa chỉ 1 cách tự động khi khởi động.
  - Thông thường thì dùng phương pháp gán địa chỉ tĩnh
  - Người ta dùng 48 bit để biểu diễn địa chỉ LAN Card
  - Có dạng XX XX XX XX XX XX ví dụ: 00-0B-5D-55-B5-DB
    Mã nhà SX Mã LAN Card

# Hoạt động của LAN

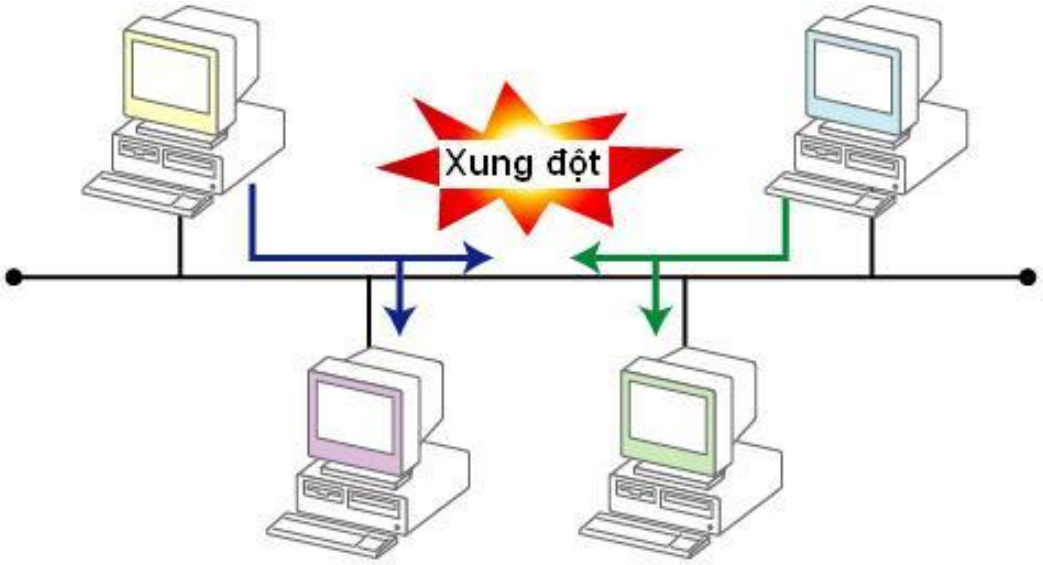
- Một máy muốn truyền khung sẽ kèm theo địa chỉ đích
- Khung được truyền lên mạng, tất cả các máy đều có thể nhận khung. Tuy nhiên chỉ máy có địa chỉ trạm trùng với địa chỉ trạm đích mới nhận khung, các máy khác bỏ qua khung.
- Nếu muốn truyền nhiều máy phải thêm 1 địa chỉ LAN Card đặc biệt gọi là địa chỉ **broad cast** **có** dạng

  FF FF FF FF FF FF cho phép khung gởi đến tất cả các máy trên LAN



# Phương pháp truy cập trên LAN

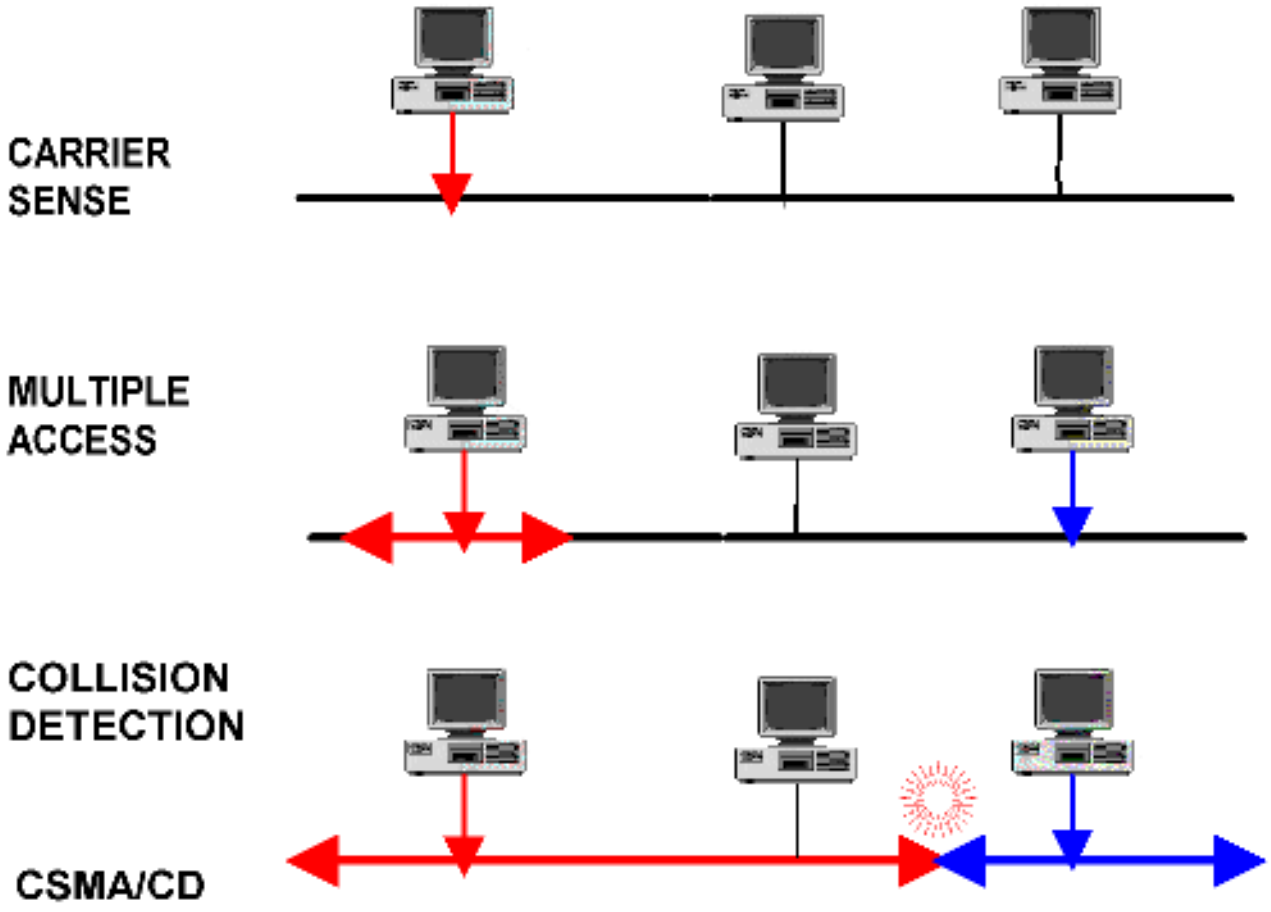
- Mạng LAN sử dụng đường truyền chia sẻ dùng chung → phải có 1 phương pháp truy cập đường truyền chung để các máy không bị xung đột
- Có nhiều phương pháp truy cập:
  - CSMA/CD
  - CSMA/CA
  - Token passing
  - Token bus
  - .....



# Phương pháp truy cập CSMA/CD

- CSMA/CD (Carrier Sense Multiple Access with Collision Detection): phương pháp đường dây đa truy cập với phát hiện sự xung đột
- Một máy muốn truyền, trước tiên phải kiểm tra đường truyền, nếu máy rãnh thì truyền. Ngược lại, máy tiếp tục thử cho tới khi rãnh và truyền.
- Có khả năng xảy ra trường hợp: Nếu 2 máy cùng kiểm tra đường truyền, cùng thấy rãnh và cùng truyền → 2 tín hiệu sẽ va chạm → gây ra xung đột
- Để giải quyết xung đột: 1 máy khi truyền vẫn tiếp tục kiểm tra đường truyền nếu phát hiện xung đột thì ngưng truyền và đợi 1 khoảng thời gian ngẫu nhiên < d, rồi tiếp tục thử lại.

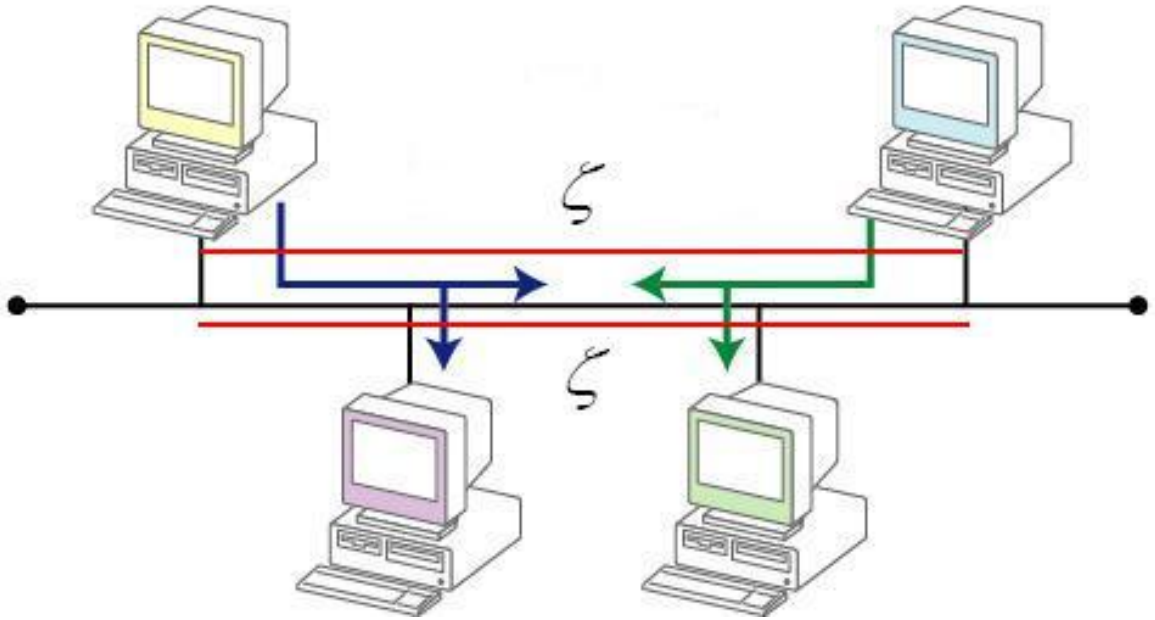
# Phương pháp truy cập CSMA/CD



# Phương pháp truy cập CSMA/CD

- Có thể xảy ra đa xung đột. Để giải quyết đa xung đột
  - Xung đột lần đầu: số ngẫu nhiên < d (khoảng thời gian đợi)
  - Xung đột lần 2: số ngẫu nhiên < 2d
  - Xung đột lần k: số ngẫu nhiên < kd
- Phạm vi số ngẫu nhiên càng lớn → xác suất trùng càng thấp, quy định tối đa 16 lần xung đột. Nếu sau 16 lần vẫn xung đột → bỏ qua khung → thông báo lỗi "truyền bị lỗi".
- Cách Chọn d:
  - Gọi $\zeta$ là tín hiệu lan truyền hết đường kính mạng
  - Chọn d = $2\zeta$ là khoảng thời gia tối đa phát hiện được xung đột

# Phương pháp truy cập CSMA/CD

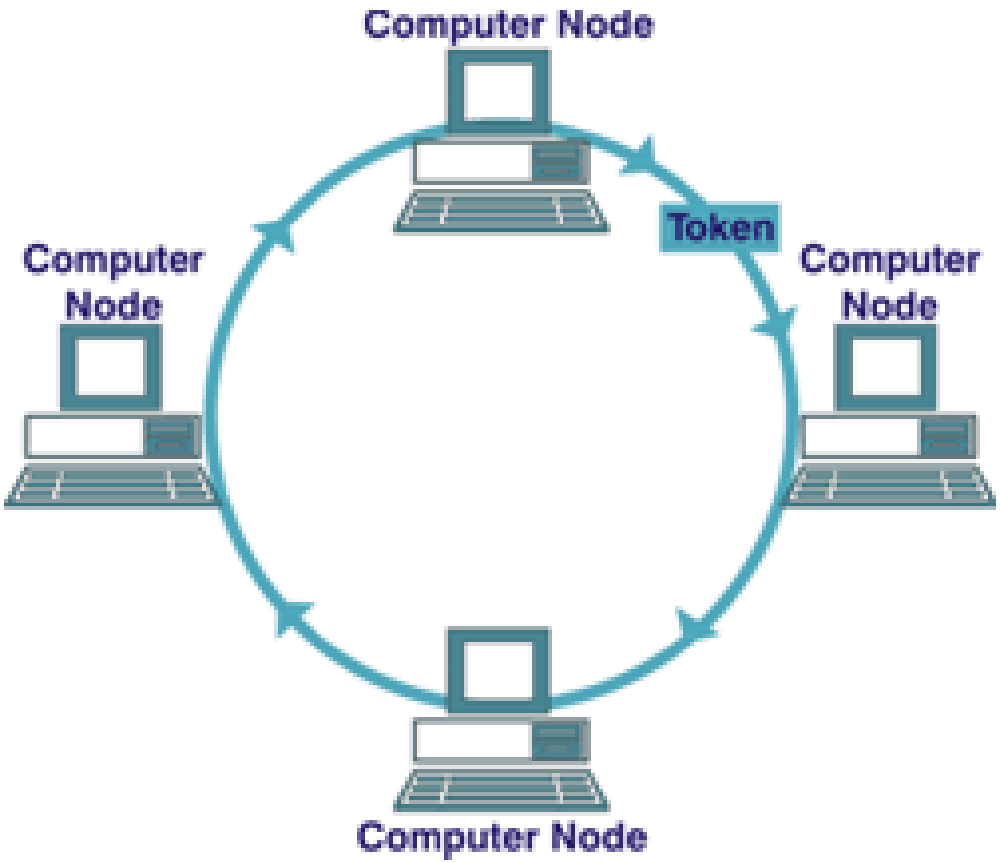


- Nhận xét
  - Phương pháp CSMA/CD phụ thuộc vào tải mạng (số máy sử dụng mạng)
  - Tải nhỏ: rất hiệu quả → nhanh do ít xung đột
  - Tải nặng: hiệu quả bị giảm đáng kể do các máy dễ bị xung đột hơn

# PP truy cập token passing (chuyển thẻ bài)

- Phương pháp này chỉ dùng trên mô hình vòng (ring).
- Một thể bài (token) được di chuyển liên tục quanh vòng.
- Một máy muốn truyền phải đợi token đến, giữ token và truyền khung dữ liệu
- Khung dữ liệu đến máy đích, máy sẽ sao chép khung vào máy và chuyển khung trở về lại máy gởi ban đầu
- Máy gởi bỏ khung và trả token đến máy kế trên vòng
- Quá trình tiếp tục

# PP truy cập token passing




- Nhận xét:
  - Phương pháp này không bị xung đột
  - So với phương pháp CSMA/CD:
    - Tải năng: hiệu quả hơn
    - Tải nhẹ: không hiệu quả

# Các công nghệ mạng LAN

- Có nhiều công nghệ mạng LAN
  - ArcNet (xưa nhất)
  - Ethernet (phổ biến nhất)
  - Token Ring
  - FDDI
  - Apple talk
  - 100 Base – any LAN
  - ATM (mới nhất)

# Mạng Ethernet

- Mạng Ethernet được hãng Xerox nghiên cứu vào những năm 1970. Về sau các hãng Intel và Digital Equipment và Xerox kết hợp đưa ra chuẩn Ethernet 10 Base
- Đặc điểm:
  - Sử dụng mô hình: BUS/STAR kết hợp
  - Cáp: xoắn đôi, đồng trục, quang
  - Kỹ thuật truyền: Baseband
  - Tốc độ: 10Mbps
  - Dùng phương pháp truy cập CSMA/CD
- Các cấu hình Ethernet 10 Base
  - Cấu hình 10 Base 5
  - Cấu hình 10 Base 2
  - Cấu hình 10 Base T
  - Cấu hình 10 Base F

# Cấu hình 10 Base 5

- Mô hình BUS với cáp đồng trục dày (thick)
- Mạng cho phép tối đa 5 đoạn BUS. Các đoạn nối với nhau qua bridge
- Mỗi đoạn dài tối đa 500m, nối tối đa 100 máy → dài tối đa 2500m, nối tối đa 500 máy
- Các thiết bị nối mạng
  - LAN car đầu AUI (D-15)
  - Bộ thu phát trên BUS gọi la transceiver
  - Terminator
  - Cáp nối AUI
  - Cấu hình này không phổ biến → do chi phí cao

# Cấu hình 10 Base 2

- Mô hình BUS với cáp đồng trục mãnh (thin)
- Mạng cho phép tối đa 5 đoạn BUS, các đoạn được nối với nhau qua bridge
- Mỗi đoạn dài tối đa 185m, nối tối đa 30 máy → mạng dài tối đa 925m, nối tối đa 150 máy
- Các thiết bị nối mạng:
  - LAN Card đầu BNC
  - Terminator
  - Đầu nối BNC và T_Connector
- 1 thời gian được dùng rất phổ biến do chi phí rẻ, dễ cài đặt

# Cấu hình 10 Base T

- Mô hình STAR với cáp xoắn đôi
- Khoảng cách tối đa máy → HUB là 100m
- Các HUB có thể kết hợp lại: BUS-STAR, STAR-STAR
- Tối đa 1020 máy
- Các thiết bị nối mạng:
  - LAN Card đầu RJ_45
  - HUB/Switch
  - Đầu nối RJ_45

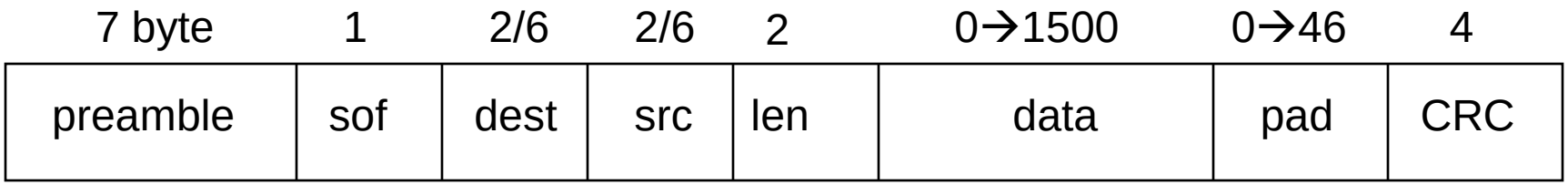
# Cấu hình 10 Base F

- Mô hình BUS với cáp quang
- Cấu hình này chủ yếu chỉ dùng làm trục chính (backbone) để nối các mạng ở xa với nhau, dài tối đa 2km

# Mã hóa tín hiệu truyền

- Dùng mã manchester
- Hiệu điện thế:
  - 0V biểu diễn bit 1
  - -1,5V biểu diễn bit 0

# Cấu trúc khung Ethernet




- Trường preamble (7 byte) có dạng
  - 1 0 1 0 1 0 1 0 … 1 0 1 0
  - Dùng làm tín hiệu đồng hồ (clock) để đồng bộ giữa máy gởi và máy nhận
- sof (start of frame) có giá trị 10101011 byte bắt đầu khung
- dest (2 hay 6 byte): xác định địa chỉ trạm đích (máy nhận)
- src (2 hay 6 byte): xác định địa chỉ nguồn (máy gởi)
- len (2 byte): xác định chiều dài data tính theo byte
- data: xác định vùng dữ liệu cần truyền

# Cấu trúc khung Ethernet

- Pad: vùng dữ liệu giả
  - Theo quy định 1 khung phải chứa ít nhất là 46 byte data (để có thể phát hiện xung đột)
  - Nếu dữ liệu không đủ thì ta phải thêm dữ liệu giả 0 cho đủ 46 byte
- CRC: Mã kiểm lỗi CRC 32 bit dùng đa thức sinh

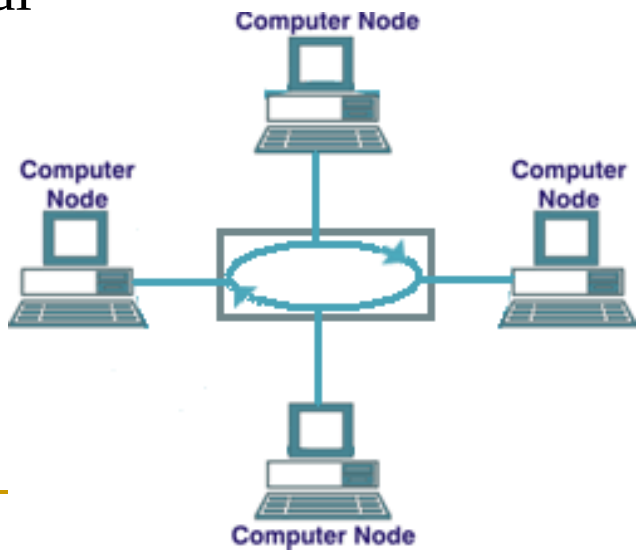
$$G(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$$

# Fast Ethernet 100 Base

- Cải tiến từ Ethernet 10 Base → Fast Ethernet 100 Base với tốc độ 100Mbps.
- Cấu hình Fast Ethernet 100 Base như sau:
  - 100 Base T4: cấu hình STAR với cáp UTP CAT 5, dùng 4 cặp xoắn đôi (Ethernet 10 Base chỉ dùng 2 cặp xoắn đôi) → không tương thích với Ethernet 10 Base
  - 100 Base TX: cấu hình STAR với cáp UTP CAT 5 chỉ dùng 2 cặp xoắn đôi → tương thích với Ethernet 10 Base. Đây là cấu hình dùng phổ biến nhất hiện nay
  - 100 Base FX: dùng cáp quang.

# Mạng Token Ring

- Được hãng IBM giới thiệu vào năm 1984
- Dùng mô hình Ring với HUB vòng
- Cáp xoắn đôi
- Tốc độ 4Mbps, về sau cải tiến lên 16Mbps
- Kỹ thuật truyền baseband
- Sử dụng phương pháp truy cập token passing
- Mã hóa tín hiệu: dùng mã Manchester vi sai
  - Bit đầu
    - bit 1
    - bit 0
  - Các bit kế:
    - Tín hiệu đảo chiều → bit 1
    - Tín hiệu không đảo chiều → bit 0



# Mạng Token Ring

- Cấu trúc khung token ring phức tạp hơn Ethernet
- Có 3 loại:
  - Token: bắt đầu 2 token
  - Dữ liệu: chứa dữ liệu truyền
  - Lệnh: chứa các lệnh token ring
- Token (3 byte):

| SD | AC | ED |
|---|---|---|

- Khung dữ liệu / lệnh

| SD | AC | FC | dest | src | data | Command | CRC | ED | FS |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 2/6 | 2/6 | | | 4 | 1 | 2 |

# Mạng Token Ring

- SD: byte bắt đầu khung
- ED: byte kết thúc khung
- AC (Access Control): cho biết token hay khung
- Dest: địa chỉ đích
- Src: địa chỉ nguồn
- Data/command: chứa dữ liệu cần truyền hay lệnh
- FS (Frame Status): cho biết trạng thái frame được thành công hay lỗi
- FC: xác định khung dữ liệu hay khung lệnh

# Mạng máy tính

## Mô hình phân tầng OSI

# Nội dung

- Protocol (giao thức)
  - Giao thức là gì?
  - Bộ giao thức (protocol stack)
- Mô hình phân tầng
  - Khái niệm
  - Truyền thông giữa 2 máy theo mô hình phân tầng
- Mô hình OSI (Open Systems Interconnection)
  - Tầng Physical
  - Tầng Data link
  - Tầng Network
  - Tầng Transport
  - Tầng Session
  - Tầng Presentation
  - Tầng Application

# Giao thức là gì?

- Là các quy tắc, quy ước hay các thủ tục để các máy có thể giao tiếp và truyền thông với nhau trên mạng
- 2 máy muốn truyền thông phải sử dụng cùng giao thức
- Ví dụ: giao thức quy định
  - Mã hóa tín hiệu
  - Dạng khung
  - Phương pháp truy cập
  - Các thủ tục truyền/nhận

# Bộ giao thức (protocol stack)

- Với bài toán truyền thông lớn, thường giao thức rất phức tạp.
- Để đơn giản, bài toán truyền thông lớn được phân thành các phần nhỏ và người ta thiết kế giao thức trên từng phần.
- Tất cả các giao thức trên từng tầng tạo thành bộ giao thức

# Các bộ giao thức thông dụng

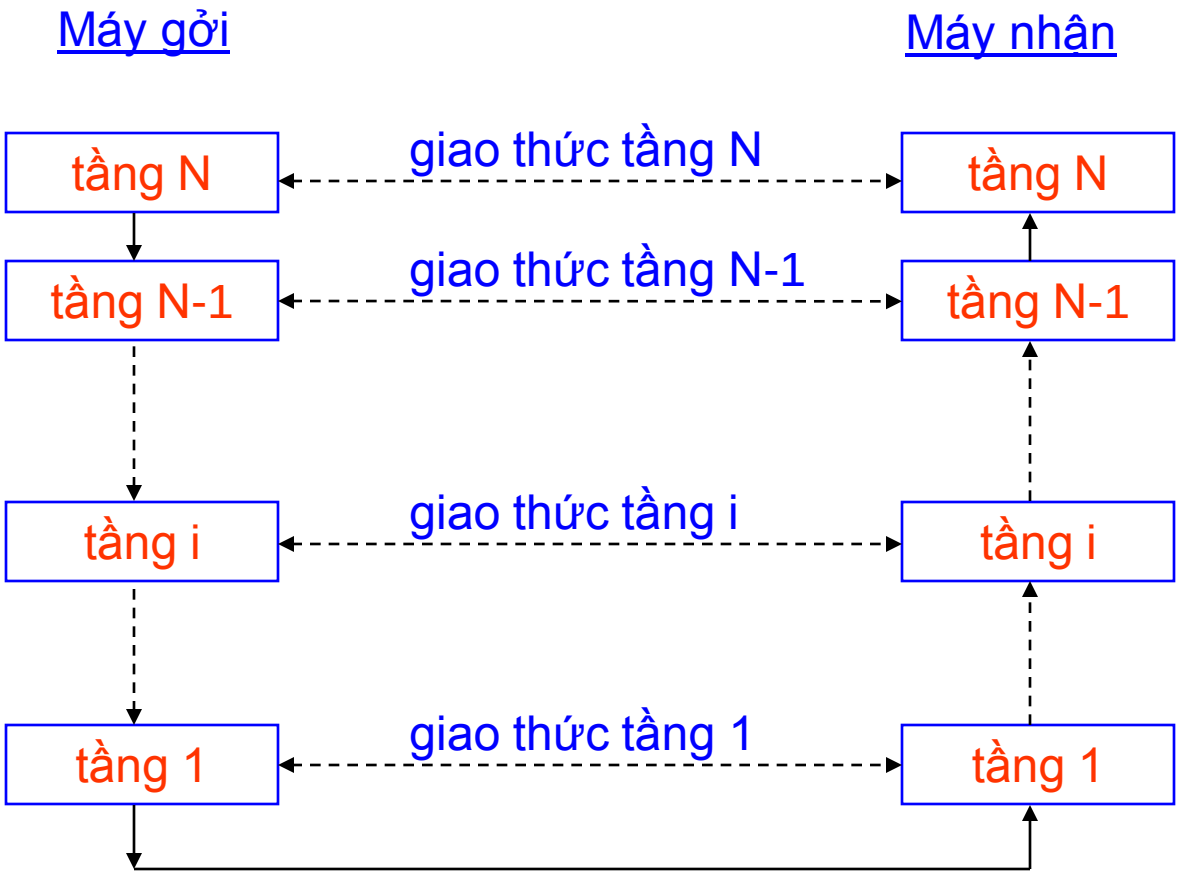
- Bộ giao thức IPX/SPX của hãng Novell trên mạng Novell Netware
- Bộ giao thức NetBEUI của hãng Microsoft trên mạng Microsoft Network
- Bộ giao thức TCP/IP được sử dụng trên liên mạng Internet (trên hệ điều hành Linux)
- Hệ điều hành Window hỗ trợ cả 3 bộ giao thức trên
- Một máy có thể cài đặt và sử dụng nhiều bộ giao thức đồng thời

# Mô hình phân tầng

- Là mô hình mô tả cách thức phân chia bài toán truyền thông lớn thành các thành phần nhỏ, mỗi phần là 1 tầng
- Mạng được tổ chức theo cấu trúc đa tầng. Tầng trên được xác định dựa vào các tầng dưới → tầng dưới sẽ cung cấp các dịch vụ cho tầng trên
- Thiết kế giao thức trên từng tầng
- Bộ giao thức mạng gồm các giao thức trên từng tầng
- Bài toán truyền thông mạng được đưa về bài toán truyền thông trên từng tầng

# Mô hình phân tầng

- Giả sử mạng gồm N tầng, xét hoạt động truyền thông giữa 2 máy theo mô hình phân tầng

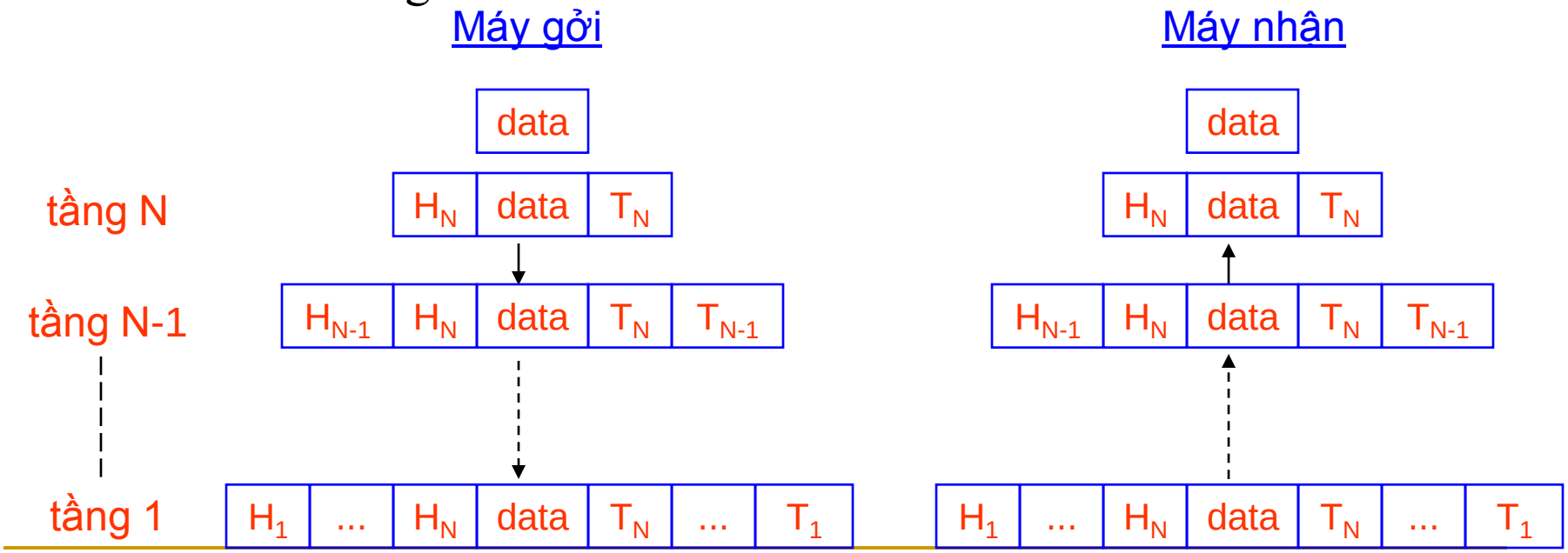


# Mô hình phân tầng

- Tại mỗi tầng có 2 mối quan hệ theo chiều ngang và dọc
  - Quan hệ chiều ngang: biểu diễn giao tiếp giữa 2 tầng giống nhau trên 2 máy theo giao thức tầng tương ứng
  - Quan hệ chiều dọc: biểu diễn giao tiếp giữa 2 tầng kề nhau trên 1 máy
- Tầng thấp nhất là tầng 1 mới có liên kết vật lý, dữ liệu được truyền từng bit trực tiếp qua đường truyền vật lý
- Tại tầng N: dữ liệu không truyền trực tiếp, dữ liệu lần lượt được đưa xuống các tầng thấp hơn cho đến tầng 1 và truyền qua đường truyền vật lý. Bên nhận sẽ nhận dữ liệu ở tầng 1, dữ liệu sẽ được đưa lên các tầng trên cho đến tầng N

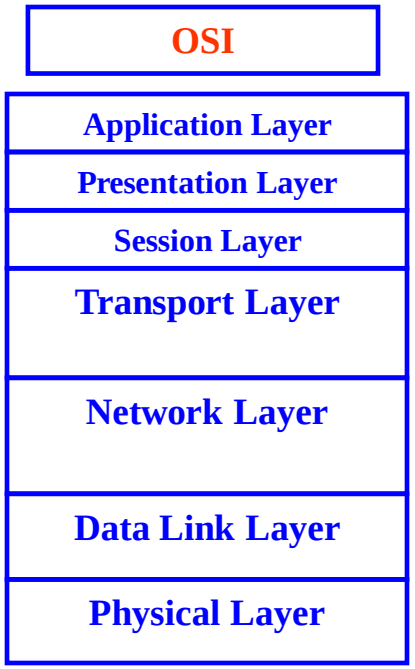
# Mô hình phân tầng

- Biểu diễn thông tin ở mỗi tầng giao thức
  - Bên gởi: tại mỗi tầng, sẽ đặt thêm thông tin điều khiển header/tailer vào khung dữ liệu để biểu diễn tầng giao thức tương ứng trước khi đưa xuống tầng dưới
  - Bên nhận: ngược lại, mỗi tầng sẽ cắt bỏ thông tin header/tailer trước khi đưa lên tầng trên



# Mô hình kết nối các hệ thống mở (OSI)

- Các mạng có mô hình phân tầng khác nhau → rất khó truyền thông với nhau → phải chuẩn hóa mô hình phân tầng
- Năm 1974, các tổ chức như tổ chức tiêu chuẩn quốc tế (ISO) CCITT,… đã tiêu chuẩn hóa mô hình phân tầng gọi là OSI.
- Mô hình này gồm 7 tầng:
  - Tầng 7: application – ứng dụng
  - Tầng 6: presentation – trình diễn
  - Tầng 5: session – phiên (giao dịch)
  - Tầng 4: transport – vận chuyển
  - Tầng 3: network – mạng
  - Tầng 2: data link – liên kết dữ liệu
  - Tầng 1: physical – vật lý

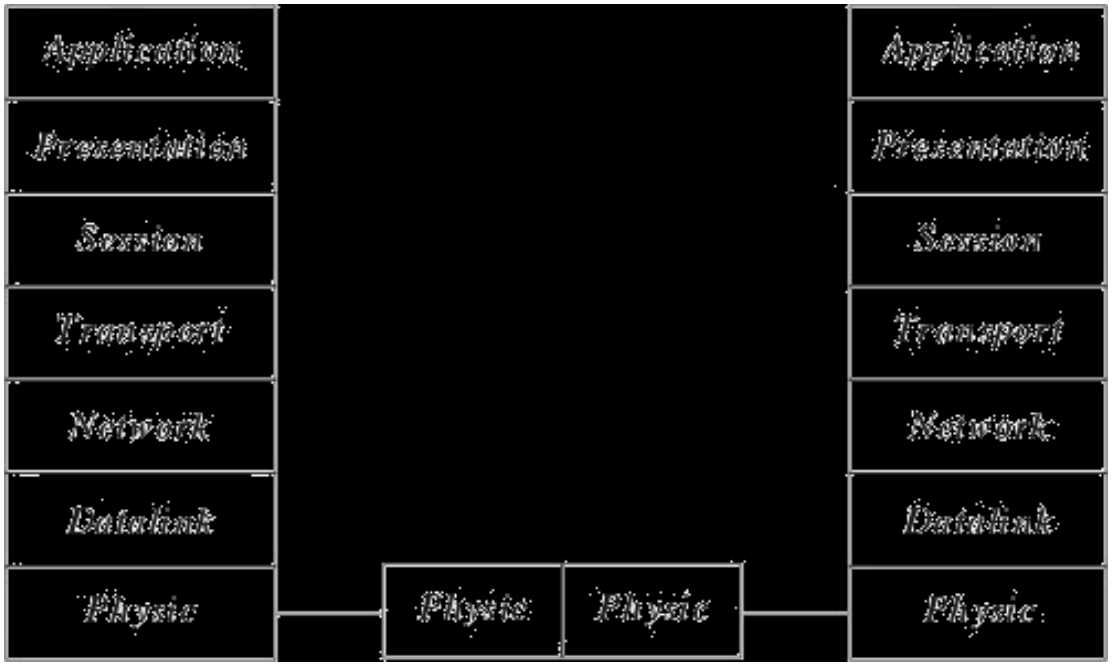


# Tầng vật lý (physical)

- Cung cấp giao thức truyền thông từng bit qua đường truyền vật lý
- Mã hóa tín hiệu bit và định thời giao truyền
  - Ví dụ mạng ethernet dùng mã Manchester
- Loại phương tiện truyền thông
- Mô hình vật lý của mạng (BUS/STAR/RING)
- Các thiết bị hoạt động ở tầng vật lý: Repeater, HUB, Brigde Multiplexor, transceiver,…

# Thiết bị hoạt động ở tầng vật lý

*Mô hình liên kết mạng của Repeater (bộ tiếp sức)*




Hoạt động của bộ tiếp sức trong mô hình OSI

# Tầng liên kết dữ liệu (data link)

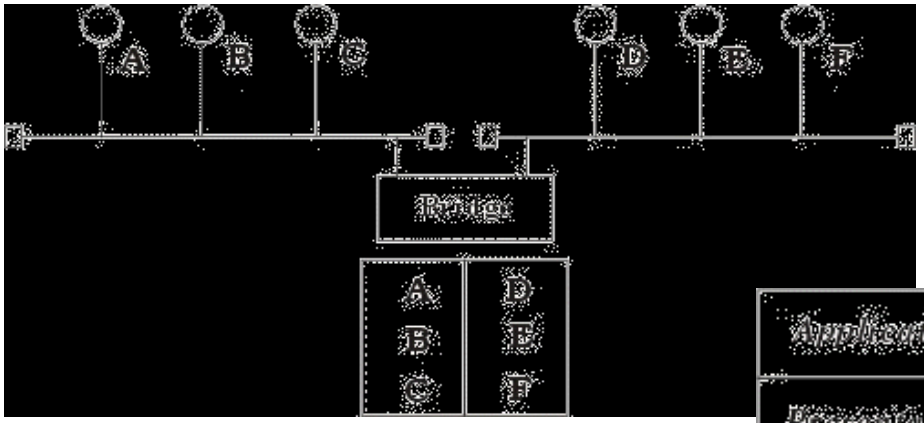
- Cung cấp giao thức truyền thông theo khung trong cùng 1 mạng
- Mô tả cấu trúc khung (ví dụ khung ethernet)
- Định nghĩa địa chỉ trạm của 1 máy trên mạng
- Phương pháp truy cập mạng.
  - Ví dụ mạng ethernet dùng phương pháp truy cập CSMA/CD
  - Mạng token ring dùng token passing
- Kiểm soát lỗi, luồng dữ liệu (ví dụ dùng mã dò lỗi CRC)

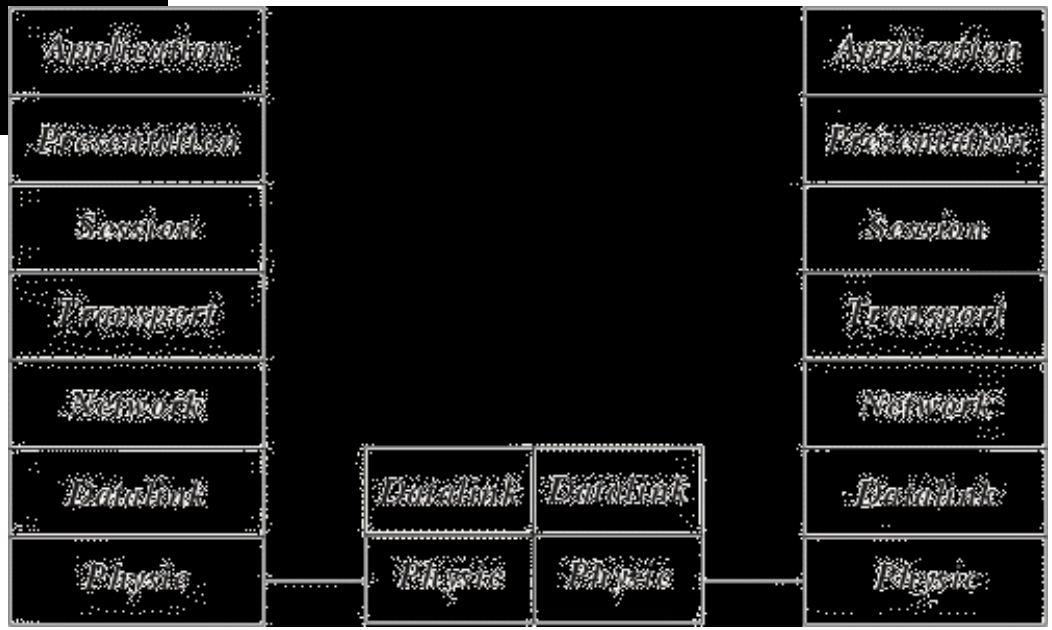
# Tầng liên kết dữ liệu (data link)

- Tầng data link cung cấp các dịch vụ truyền thông
  - Dịch vụ phi liên kết: 2 bên không cần thiết lập kết nối. Dịch vụ này nhanh, chi phí thấp nhưng không đảm bảo tin cậy (do không kiểm soát lỗi và luồng nên dữ liệu có thể bị mất) (như nhắn tin)
  - Dịch vụ hướng liên kết: 2 bên phải thiết lập kết nối. Dịch vụ này chi phí rất cao vì có kiểm soát lỗi và luồng → đảm bảo tin cậy, dữ liệu không bị mất
  - Dịch vụ phi liên kết có báo nhận
- Các thiết bị hoạt động ở tầng data link: LAN card, switch, bridge

# Thiết bị hoạt động ở tầng liên kết dữ liệu

*Hoạt động của Bridge*



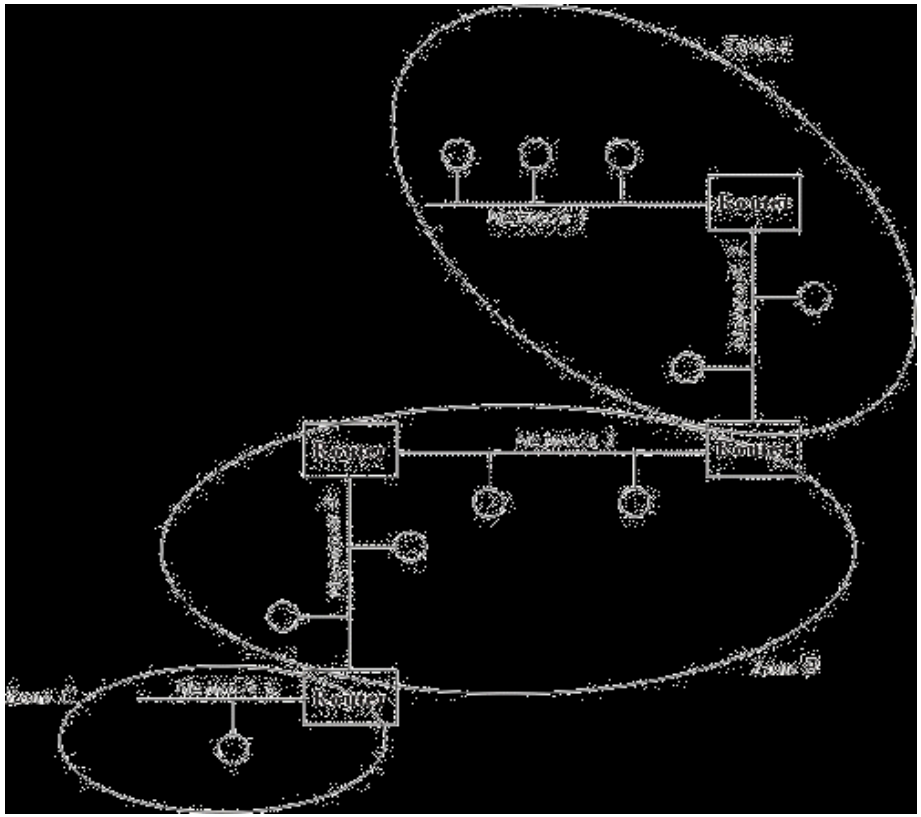
*Hoạt động của Bridge trong mô hình OSI*

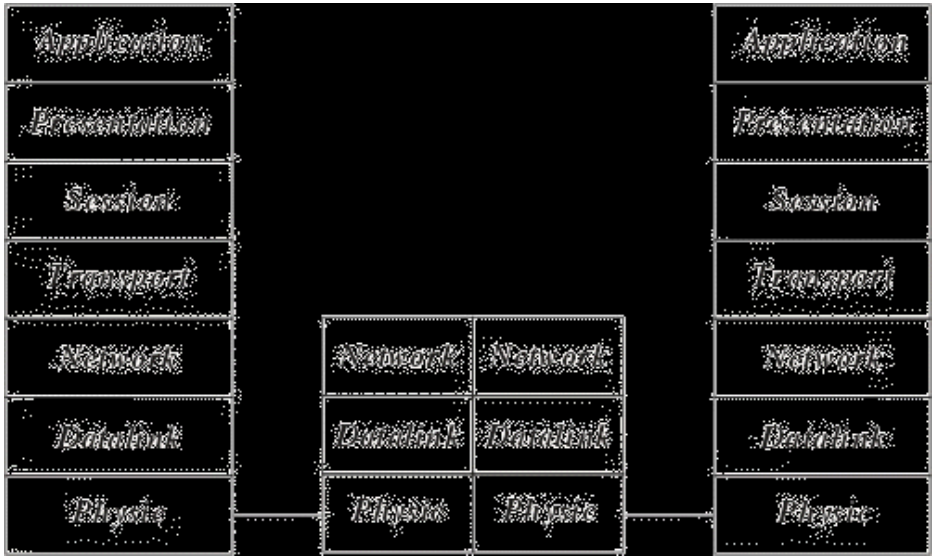
# Tầng Network

- Cung cấp giao thức truyền thông theo gói giữa 2 máy bất kỳ trên liên mạng (các máy kết nối lại với nhau tạo thành 1 mạng lớn hơn)
- Định nghĩa địa chỉ mạng của 1 mạng vật lý
- 2 chức năng chính của tầng Network là tìm đường (routing) và chuyển chặng.
- Các giao thức tìm đường đi ngắn nhất
  - RIP (Routing Information Protocol ): dùng thuật toán vector – tính khoảng cách
  - SPF (shactest path first): dùng thuật toán đô thị tìm đường đi ngắn nhất của Dijkstra
- Thiết bị hoạt động ở tầng Network là bộ định tuyến Router (thiết bị để kết nối liên mạng và có chức năng tìm đường đi)

# Thiết bị hoạt động ở tầng mạng

*Hoạt động của Router*





*Hoạt động của Router trong mô hình OSI*

# Tầng vận chuyển

- Tầng vận chuyển cung cấp các chức năng cần thiết giữa tầng mạng và các tầng trên.
- Là tầng cao nhất có liên quan đến các giao thức trao đổi dữ liệu giữa các hệ thống mở.
- Tầng vận chuyển là tầng cơ sở mà ở đó một máy tính của mạng chia sẻ thông tin với một máy khác.
- Tầng vận chuyển đồng nhất mỗi trạm bằng một địa chỉ duy nhất và quản lý sự kết nối giữa các trạm.
- Tầng vận chuyển cũng chia các gói tin lớn thành các gói tin nhỏ hơn trước khi gửi đi. Thông thường tầng vận chuyển đánh số các gói tin và đảm bảo chúng chuyển theo đúng thứ tự.

# Tầng giao dịch

- Tầng giao dịch (session layer) thiết lập "các giao dịch" giữa các trạm trên mạng
- Một giao dịch phải được thiết lập trước khi dữ liệu được truyền trên mạng
- Tầng giao dịch đảm bảo cho các giao dịch được thiết lập và duy trì theo đúng qui định
- Tầng giao dịch cung cấp cho người sử dụng các chức năng cần thiết để quản trị các giao dịch trong ứng dụng của họ:
  - Điều phối việc trao đổi dữ liệu giữa các ứng dụng bằng cách thiết lập và giải phóng các phiên giao dịch
  - Cung cấp các điểm đồng bộ để kiểm soát việc trao đổi dữ liệu.
  - Áp đặt các qui tắc cho các tương tác giữa các ứng dụng của người sử dụng.
  - Cung cấp cơ chế "lấy lượt" (nắm quyền) trong quá trình trao đổi dữ liệu.

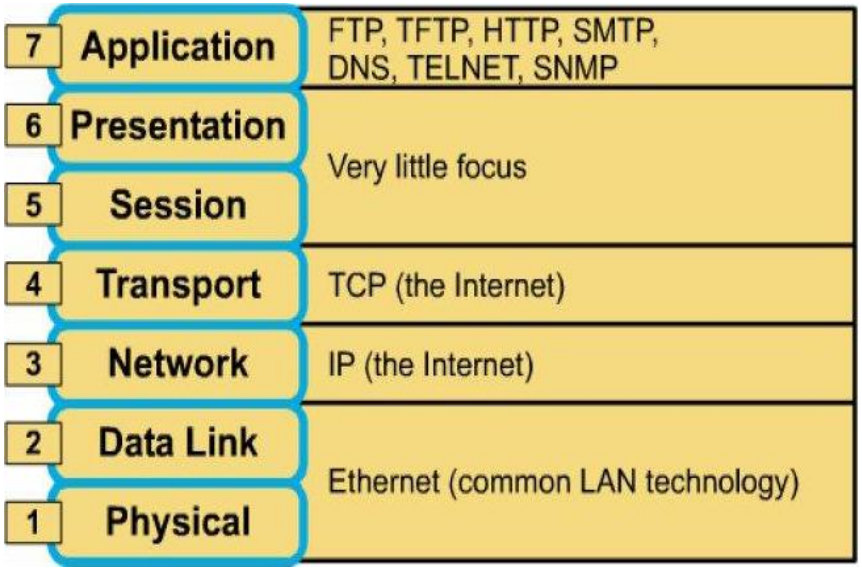
# Tầng trình diễn

- Cung cấp các giao thức biểu diễn và chuyển đổi dữ liệu giữa các máy trên mạng
  - Nén dữ liệu → dữ liệu nhỏ hơn → truyền nhanh hơn
    - Bên gởi: nén
    - Bên nhận: giải nén
  - Mã hóa dữ liệu → bảo mật thông tin
    - Bên gởi: mã hóa
    - Bên nhận giải mã → dữ liệu ban đầu
    - Ví dụ người ta dùng áp dụng cơ chế mã hóa SSL ở tầng trình diễn trong giao thức HTTP → HTTPs
  - Chuyển đổi dữ liệu: trên mạng có thể gồm nhiều máy tính có thể có cấu trúc khác nhau → có thể sử dụng các dạng dữ liệu khác nhau → phải chuyển đổi dữ liệu giữa các máy

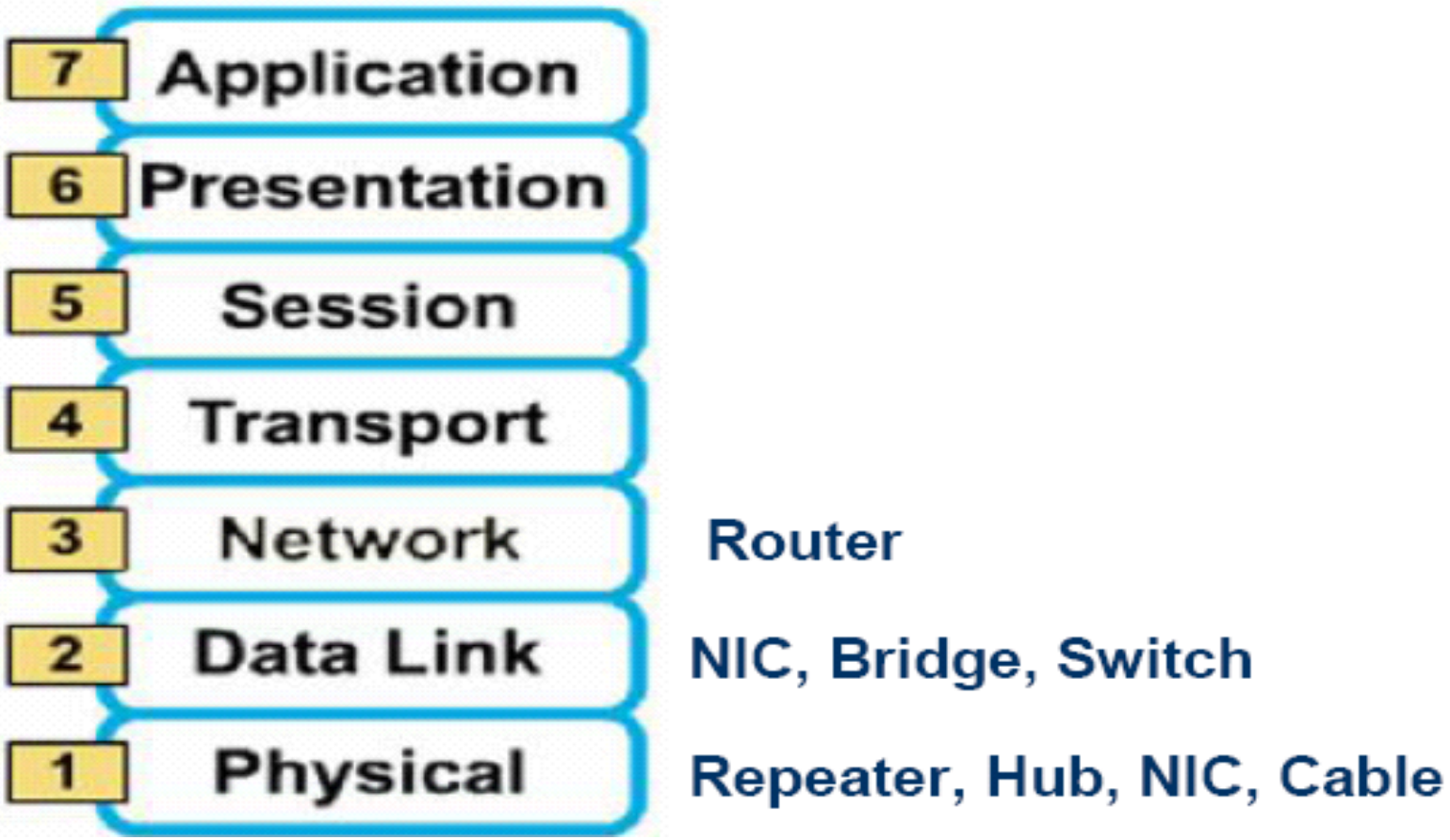
# Tầng ứng dụng

- Tầng ứng dụng là tầng cao nhất của mô hình OSI, nó xác định giao diện giữa người sử dụng và môi trường OSI
- Cung cấp giao thức cho các dịch vụ và các ứng dụng của người dùng trên mạng
- Ví dụ:
  - Dịch vụ web: sử dụng giao thức HTTP để truyền nội dung trang web
  - Dịch vụ FTP: sử dụng giao thức FTP để truyền tập tin
  - Dịch vụ mail sử dụng giao thức:
    - SMTP: giao thức gởi mail
    - POP3: giao thức nhận mail

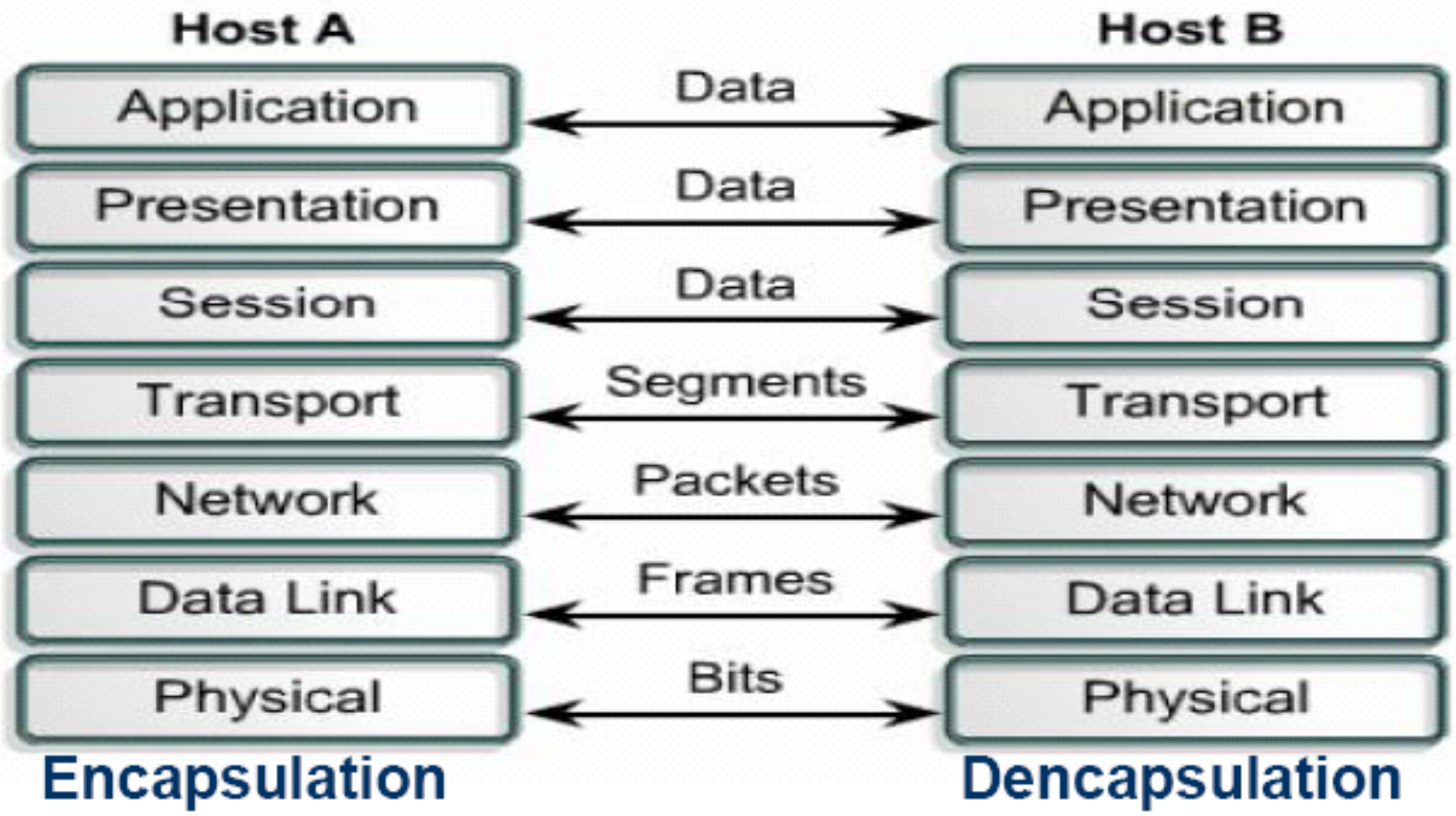
# Các giao thức làm việc tương ứng



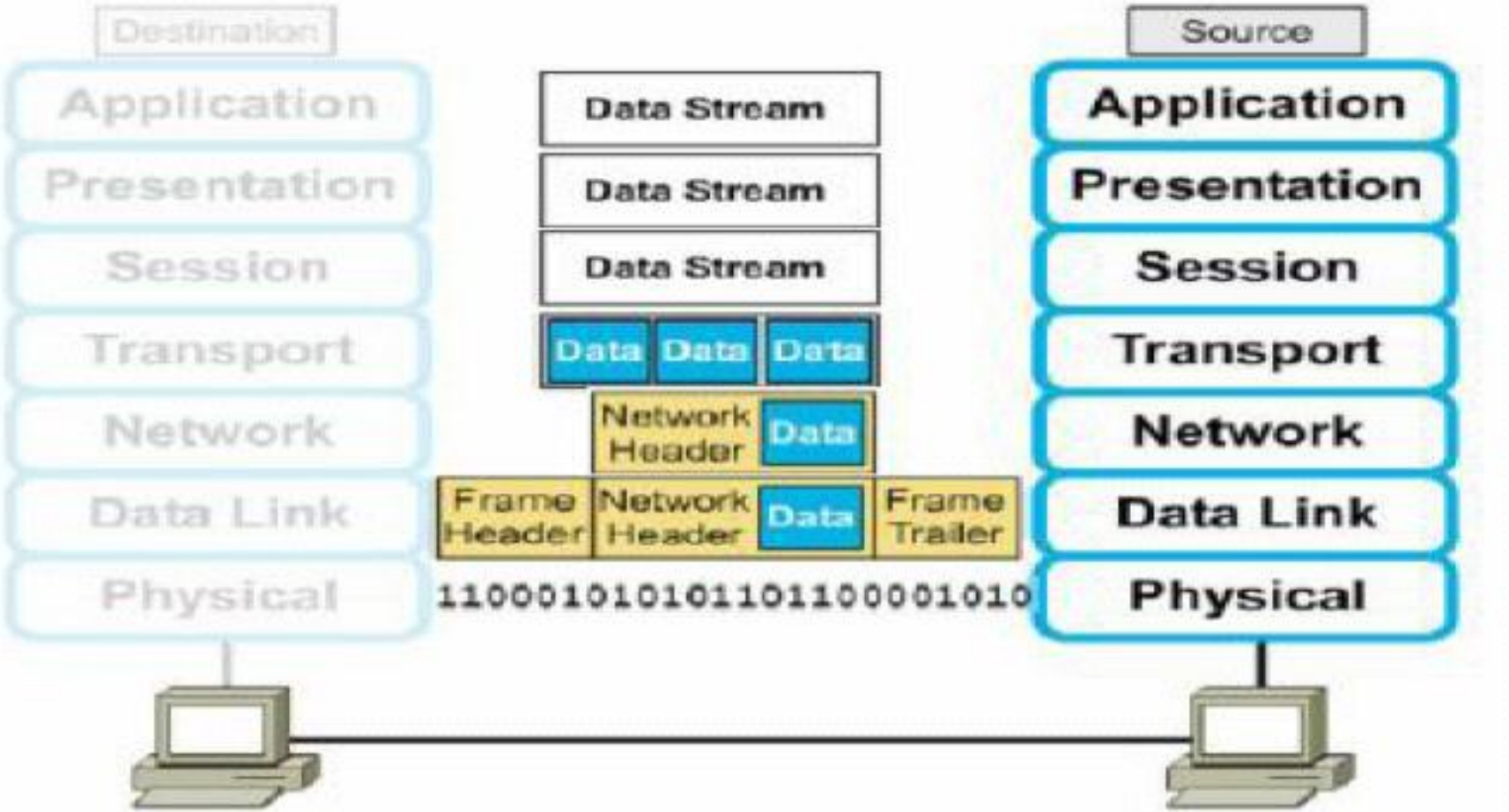
# Các thiết bị hoạt động tương ứng



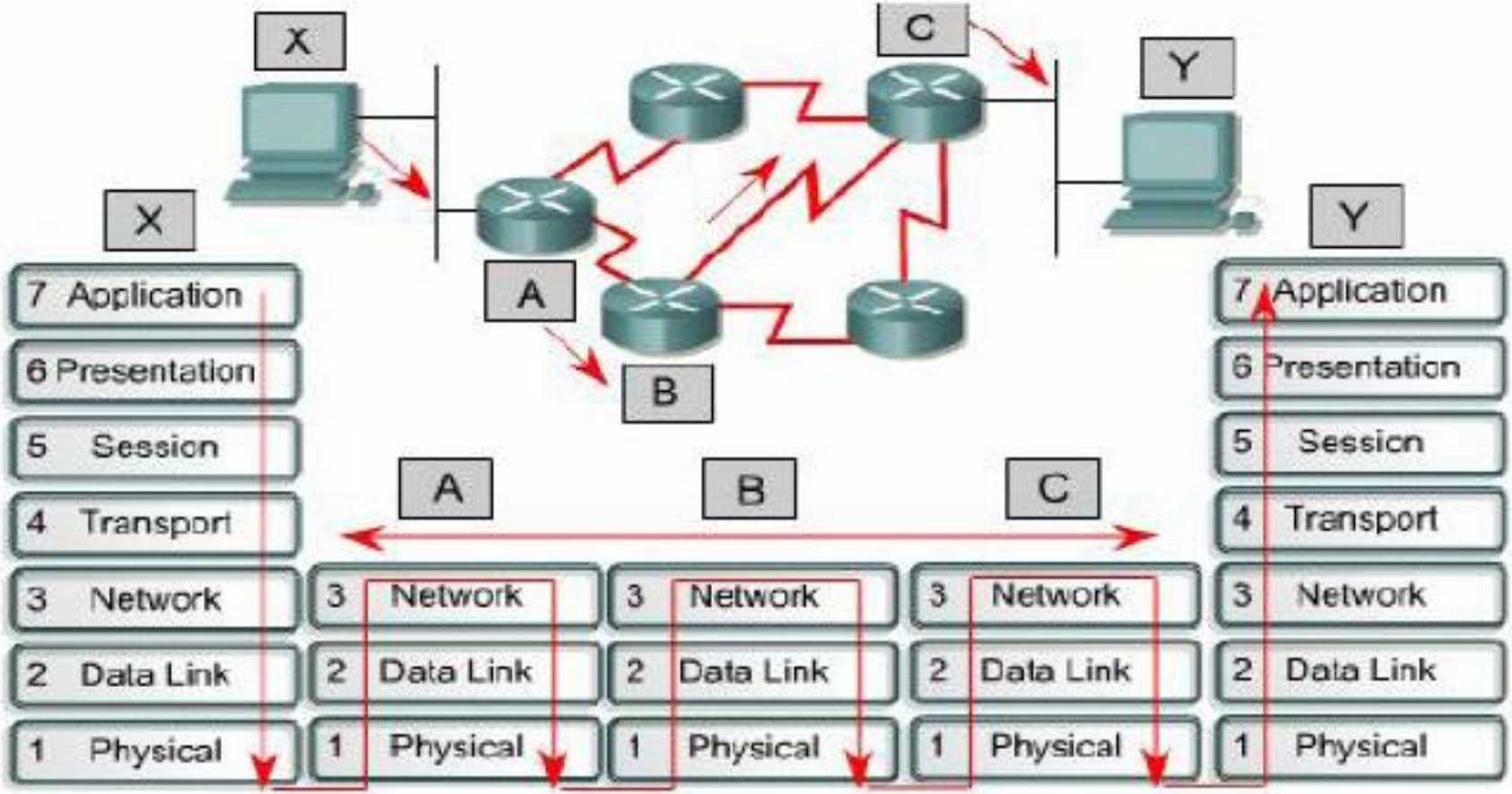
# Luồng dữ liệu qua các tầng



# Giới dữ liệu qua các tầng



# Giới dữ liệu đi qua các tầng



# Mạng máy tính

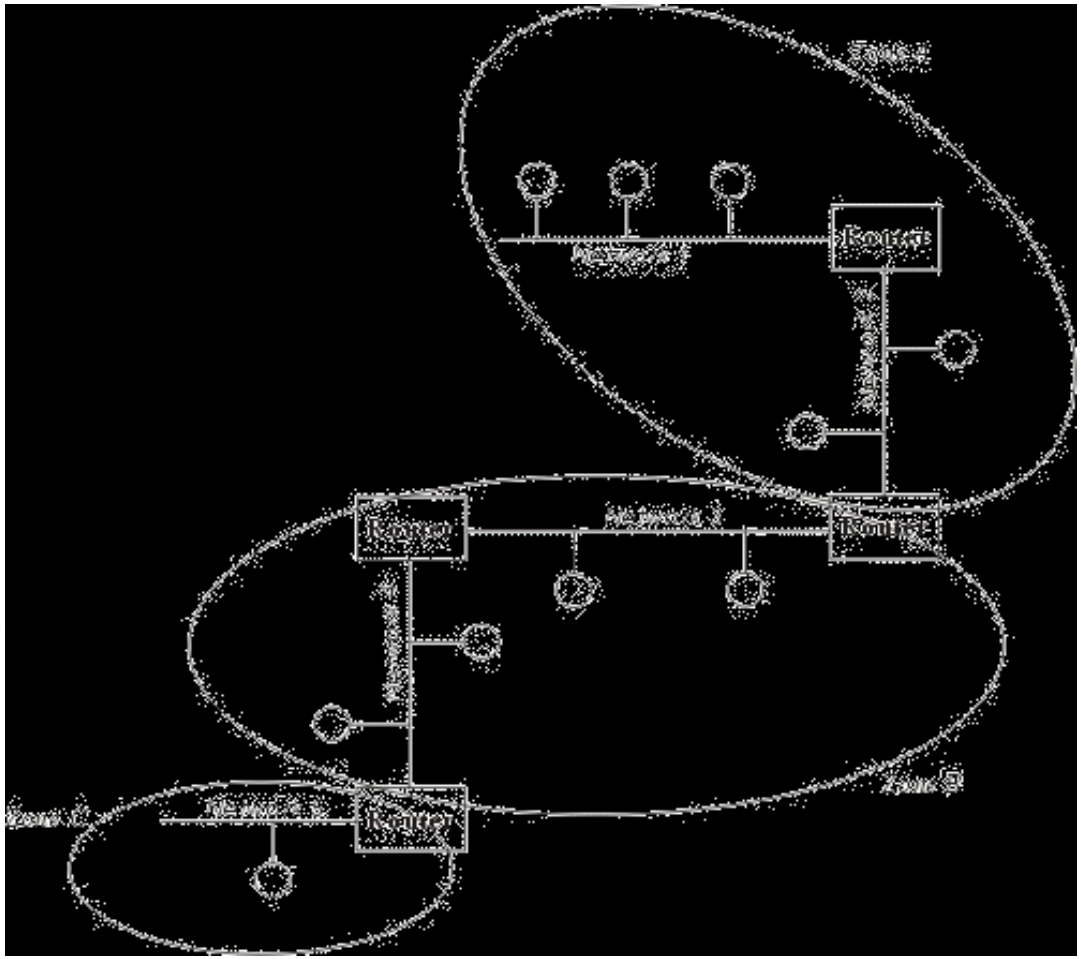
## MẠNG TOÀN CẦU Và Mô hình TCP/IP

# Nội dung

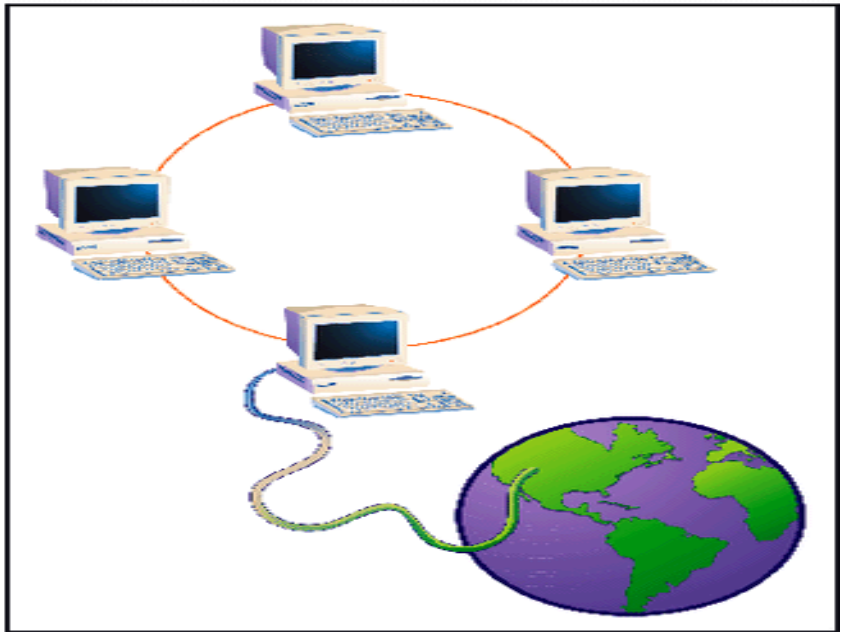
- Liên mạng – Mạng toàn cầu GAN
  - Liên mạng
  - GAN
- MÔ HÌNH TCP/IP
- Giao thức IP
  - Địa chỉ IP
  - Phân lớp địa chỉ IP
  - Cách biểu diễn địa chỉ IP
  - Các địa chỉ IP đặc biệt: đ/c mạng, đ/c broadcast, đ/c loopback
  - Bảng định tuyến
- Mạng con (subnet)

# Liên mạng (Internet working)

- Gồm các mạng vật lý được kết nối với nhau sao cho chúng có thể truyền thông với nhau
- Phần cứng cơ bản để kết nối liên mạng là thiết bị định tuyến Router
- Mỗi mạng vật lý phải được quy định 1 địa chỉ mạng duy nhất
- Ví dụ: liên mạng gồm 5 mạng nối qua 4 Router



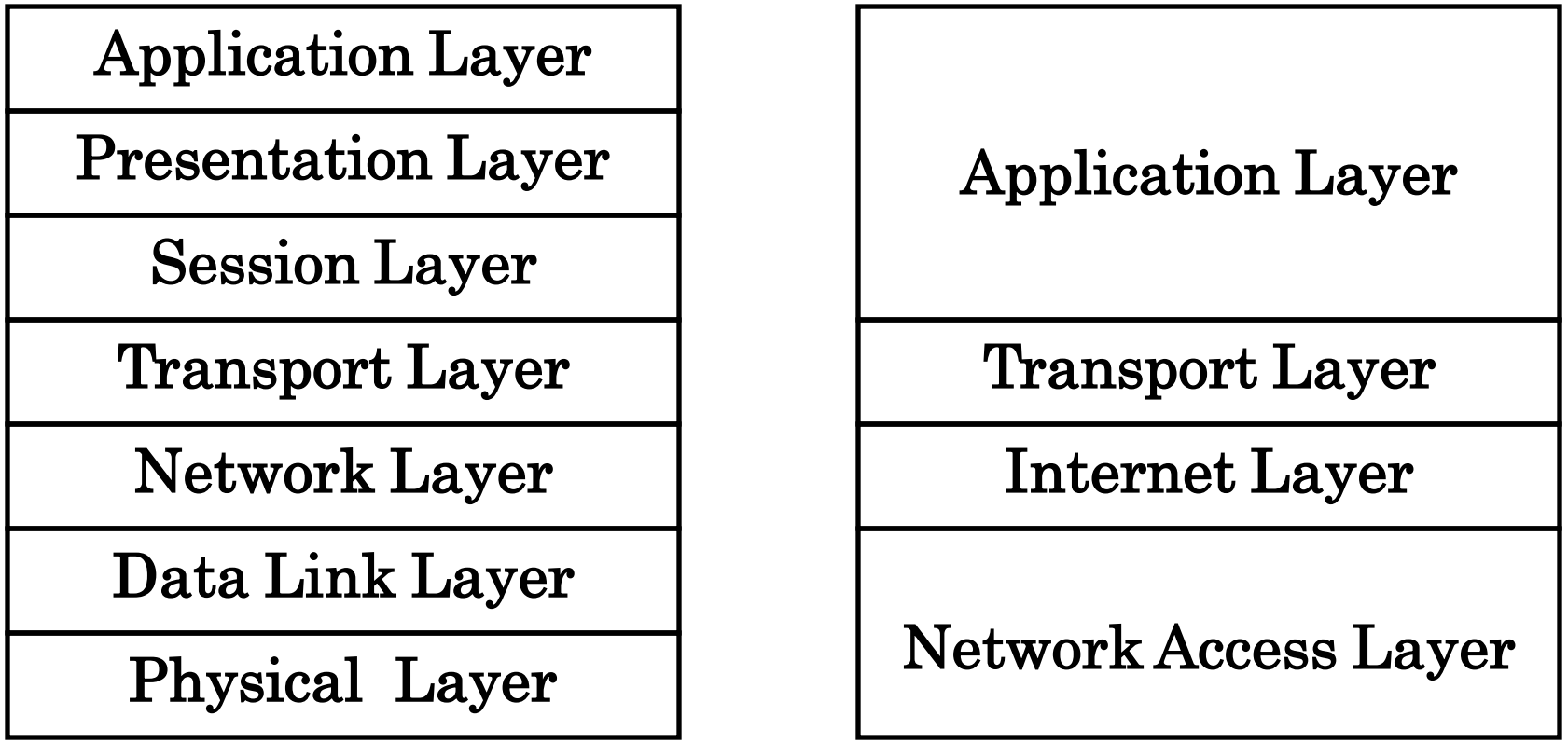
# GAN(Internet)



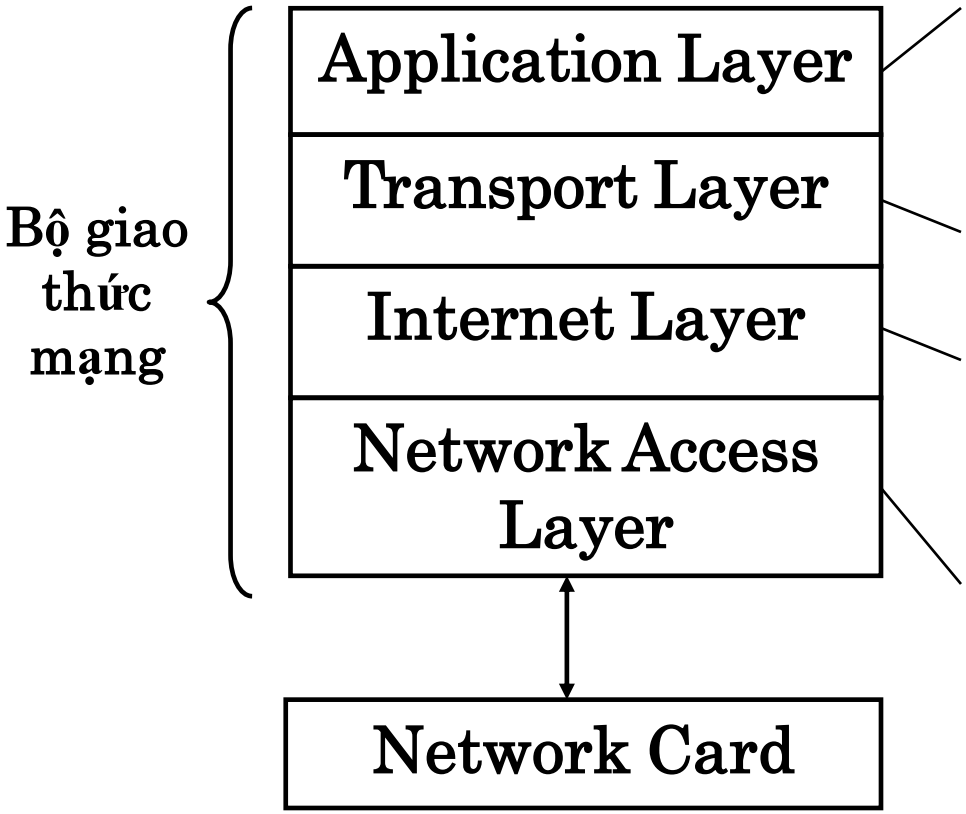
- Kết nối tất cả các mạng và liên mạng trên toàn cầu tạo thành mạng Internet
- Một mạng vật lý muốn tham gia vào Internet phải được cấp 1 địa chỉ mạng trên Internet
- Trung tâm điều hành Internet có chức năng cấp địa chỉ
- Tại mỗi quốc gia, có các công ty viễn thông (ISP – Internet Service Provider) cung cấp các dịch vụ kết nối internet
- Việt nam có các ISP như: VNN, FPT, Viettel,...

# MÔ HÌNH TCP/IP

- TCP/IP là bộ giao thức chính để kết nối liên mạng và Internet



# Cấu trúc TCP/IP

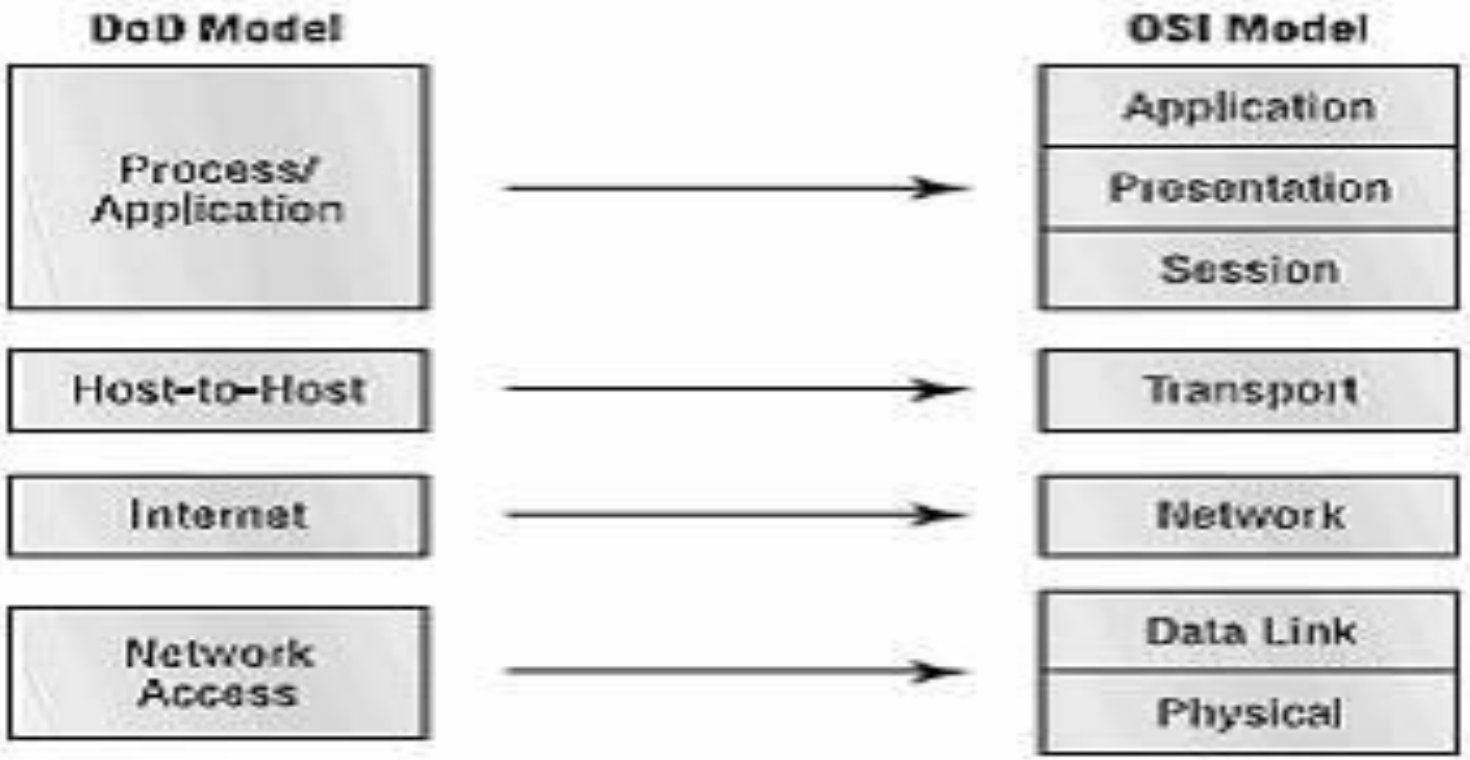



- Network Interface for Applications
- Flow/error control
- Logical Addressing & Routing
- Interface with the NIC
- (Network Interface Card)

# Mô hình TCP/IP

- TCP/IP có cấu trúc tương tự như mô hình OSI, tuy nhiên để đảm bảo tính tương thích giữa các mạng và sự tin cậy của việc truyền thông tin trên mạng, bộ giao thức TCP/IP được chia thành 2 phần riêng biệt: giao thức IP sử dụng cho việc kết nối mạng và giao thức TCP để đảm bảo việc truyền dữ liệu một cách tin cậy.

# So sánh giữa OSI và TCP/IP




Hình 1.3 The DoD and OSI models

# Lớp ứng dụng:

- Lớp ứng dụng: Tại mức cao nhất này, người sử dụng thực hiện các chương trình ứng dụng truy xuất đến các dịch vụ hiện hữu trên TCP/IP Internet. Một ứng dụng tương tác với một trong những protocol ở mức giao vận (transport) để gửi hoặc nhận dữ liệu. Mỗi chương trình ứng dụng chọn một kiểu giao vận mà nó cần, có thể là một dãy tuần tự từng thông điệp hoặc một chuỗi các byte liên tục. Chương trình ứng dụng sẽ gửi dữ liệu đi dưới dạng nào đó mà nó yêu cầu đến lớp giao vận.

# Lớp giao vận:

- Lớp giao vận: Nhiệm vụ cơ bản của lớp giao vận là cung cấp phưng tiện liên lạc từ một chương trình ứng dụng này đến một chưng trình ứng dụng khác. Việc thông tin liên lạc đó thường được gọi là end-to-end. Mức chuyên trở có thể điều khiển luông thông tin. Nó cũng có thể cung cấp sự giao vận có độ tin cậy, bảo đảm dữ liệu đến nơi mà không có lỗi và theo đúng thứ tự.

# Lớp giao vận:

- Để làm được điều đó, phần mềm protocol lớp giao vận cung cấp giao thức TCP, trong quá trình trao đổi thông tin nơi nhận sẽ gửi ngược trở lại một xác nhận (ACK) và nơi gửi sẽ truyền lại những gói dữ liệu bị mất. Tuy nhiên trong những môi trường truyền dẫn tốt như cáp quang chẳng hạn thì việc xy ra lỗi là rất nhỏ. Lớp giao vận có cung cấp một giao thức khác đó là UDP.

# Lớp Internet:

- Lớp Internet: Nhiệm vụ cơ bản của lớp này là xử lý việc liên lạc của các thiết bị trên mạng. Nó nhận được một yêu cầu để gửi gói dữ liệu từ lớp cùng với một định danh của máy mà gói dữ liệu phi được gửi đến. Nó đóng segment vào trong một packet, điền vào phần đầu của packet, sau đó sử dụng các giao thức định tuyến để chuyển gói tin đến được đích của nó hoặc trạm kế tiếp.

# Lớp Internet:

- Khi đó tại nơi nhận sẽ kiểm tra tính hợp lệ của chúng, và sử dụng tiếp các giao thức định tuyến để xử lý gói tin. Đối với những packet được xác định thuộc cùng mạng cục bộ, phần mềm Internet sẽ cắt bỏ phần đầu của packet, và chọn một trong các giao thức lớp chuyên trở thích hợp để xử lý chúng. Cuối cùng, lớp Internet gửi và nhận các thông điệp kiểm soát và sử lý lỗi ICMP.

# Lớp giao tiếp mạng:

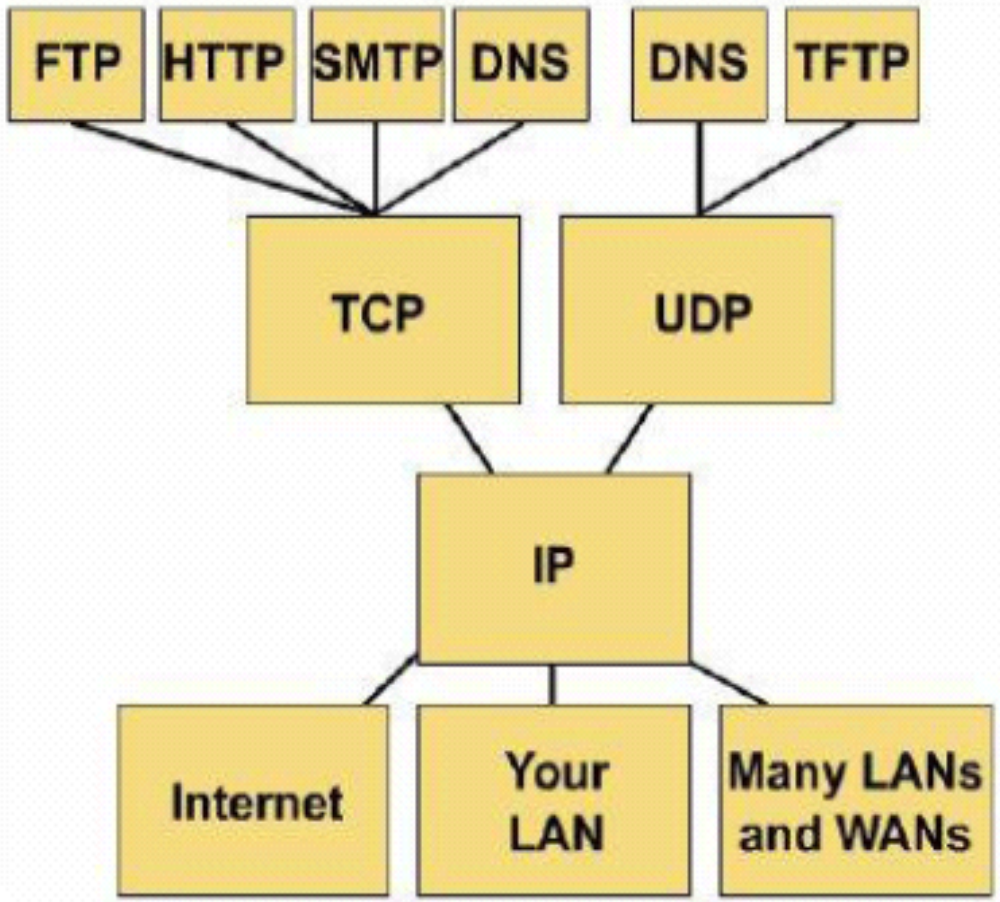
- Lớp giao tiếp mạng: Lớp thấp nhất của mô hình TCP/IP chính là lớp giao tiếp mạng, có trách nhiệm nhận các IP datagram và truyền chúng trên một mạng nhất định. Người ta lại chia lớp giao tiếp mạng thành 2 lớp con là:

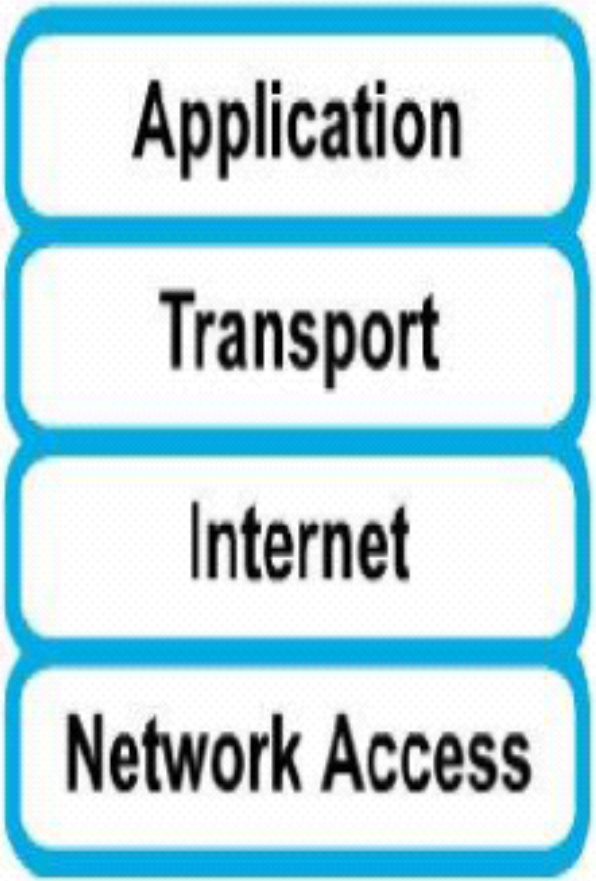
# Lớp giao tiếp mạng:

- +Lớp vật lý: Lớp vật lý làm việc với các thiết bị vật lý, truyền tới dòng bit 0, 1 từ ni gửi đến nơi nhận.

  +Lớp liên kết dữ liệu: Tại đây dữ liệu được tổ chức thành các khung (frame). Phần đầu khung chứa địa chỉ và thông tin điều khiển, phần cuối khung dành cho viêc phát hiện lỗi.

# Mô hình TCP/IP và Protocol



# The Process/Application Layer Protocols

- Dịch vụ đăng nhập từ xaTELNET
- Dịch vụ truyền file FTP
- Trivial File Transfer Protocol (TFTP)
- Network File System (NFS)
- Simple Mail Transfer Protocol (SMTP)

# The Process/Application Layer Protocols

- Simple Network Management Protocol (SNMP)
- Domain Name Service (DNS)
- Dynamic Host Configuration Protocol (DHCP)/BootP (Bootstrap Protocol)

# The Internet Layer Protocols

- Internet Protocol (IP)
  + Định dạng IP
  + Định tuyến
  + Điểu khiển và xử lý lỗi
- Giao thức bản tin điểu khiển liên mạng (ICMP)
- ARP và RARP

# Internet Protocol (IP)

Trong hệ thống địa chỉ IP được chia ra 2 loại địa chỉ:

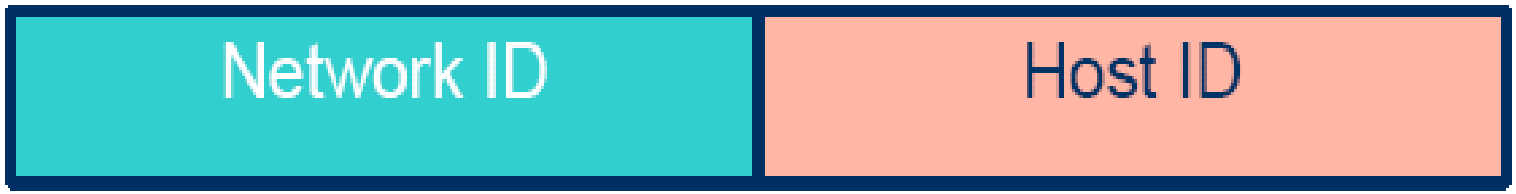
- Địa chỉ IPv4
- Địa chỉ IPv6

  Trên thực tế nguồn tài nguyên địa chỉ IPv4 đang dần cạn kiệt, địa chỉ IPv6 là một giải pháp nhằm dần thay thế cho địa chỉ IPv4.

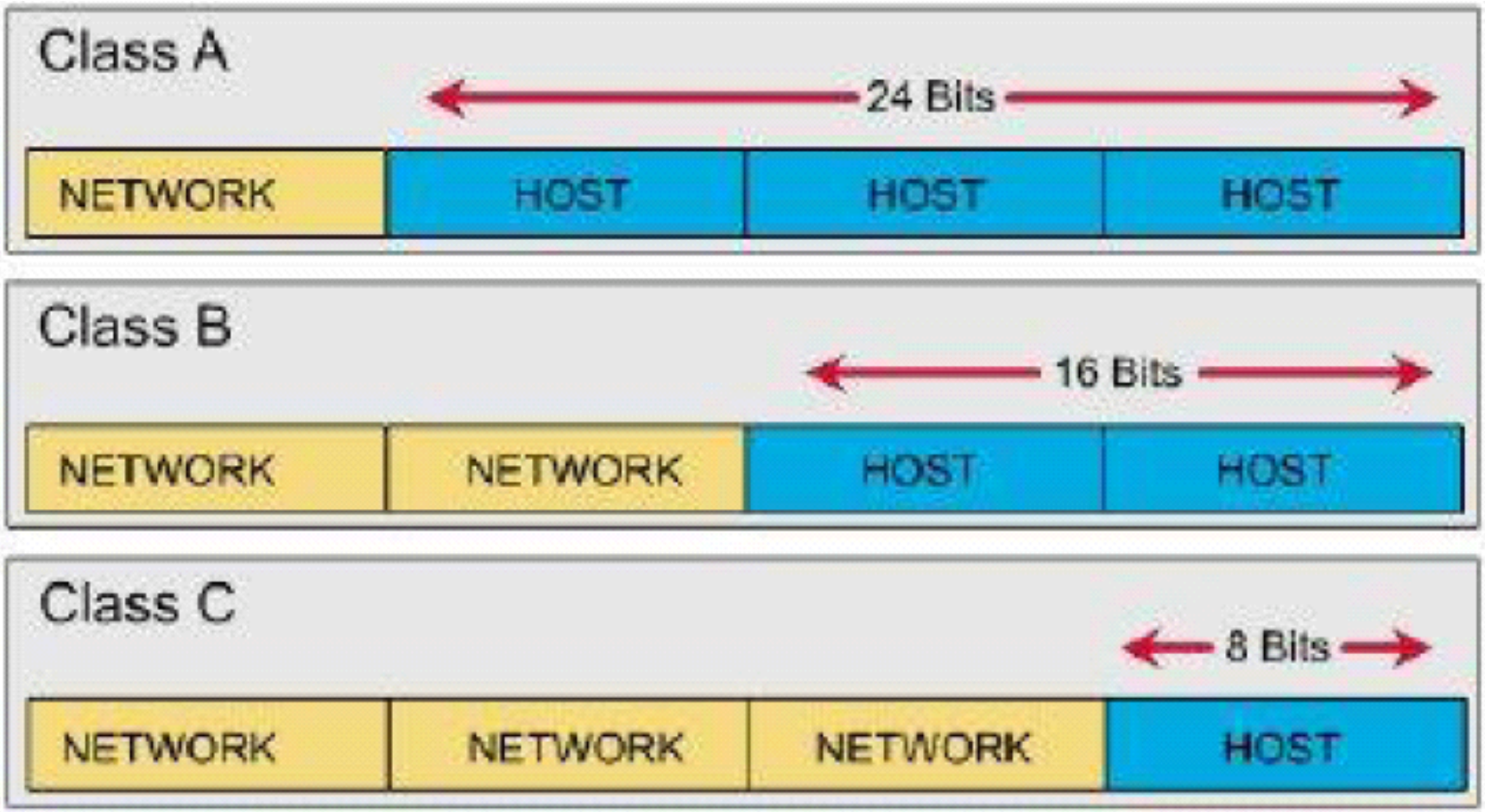
  Tại Việt Nam chúng ta vẫn sử dụng loại địa chỉ IPv4 với lý do chúng ta con quá nhiều máy tính không hỗ trợ cho địa chỉ IPv6.

# Cấu trúc địa chỉ IP

- Địa chỉ IPv4 được cấu tạo bởi 32 bit và chia làm 4 octet, mỗi octet chiếm 8 bit.
- Địa chỉ IP được cấu tạo bởi 2 phần chính là:
  - Network ID (Địa chỉ mạng)
  - Host ID (Địa chỉ host)



# Các lớp địa chỉ



# Các lớp địa chỉ

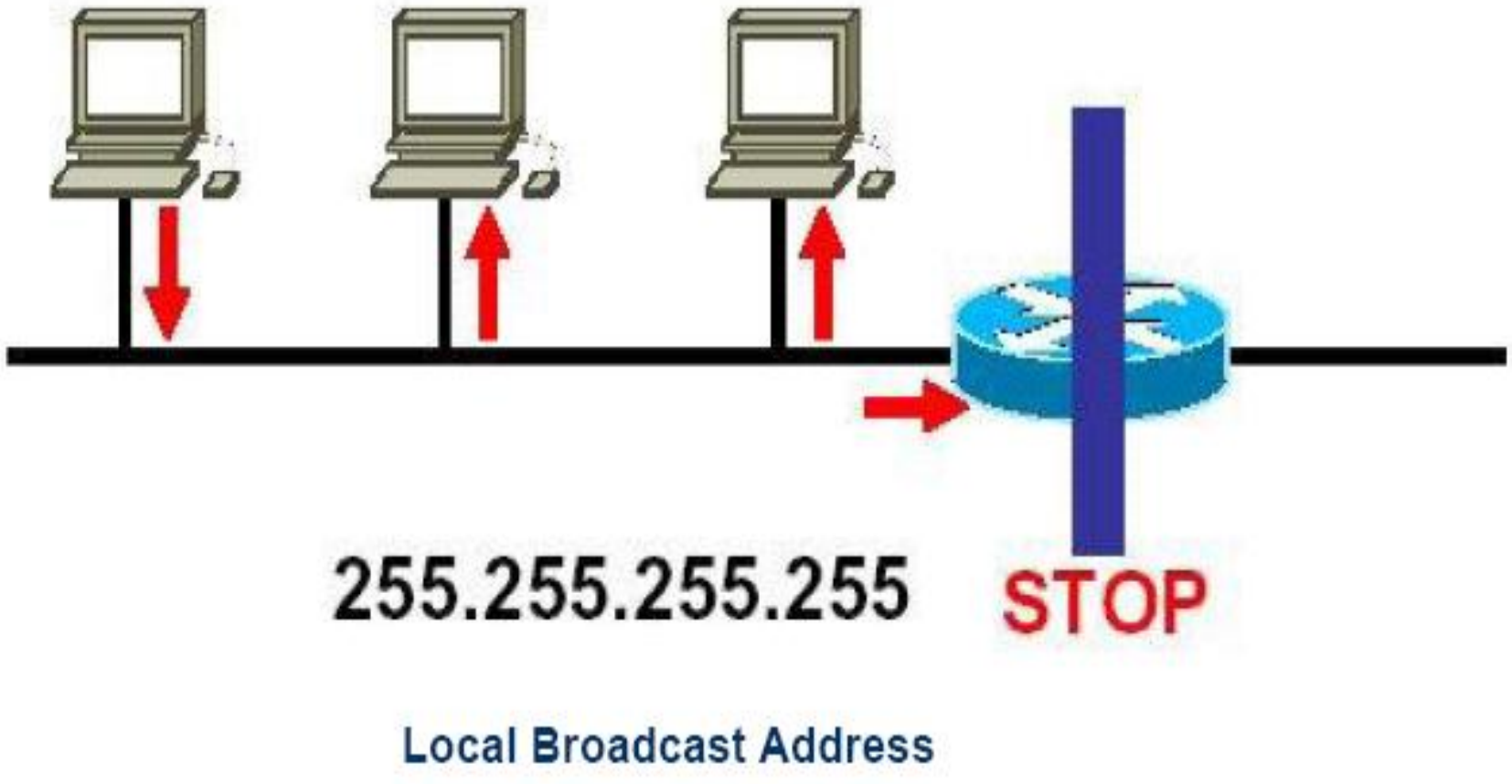
| Address Class | Number of Networks | Number of Host per Network |
|---|---|---|
| A | 126 * | 16,777,216 |
| B | 16, 384 | 65,535 |
| C | 2,097,152 | 254 |
| D (Multicast) | N/A | N/A |

| IP Address Class | High Order Bits | First Octet Address Range | Number of Bits in the Network Address |
|---|---|---|---|
| Class A | 0 | 0 - 127 * | 8 |
| Class B | 10 | 128 - 191 | 16 |
| Class C | 110 | 192 - 223 | 24 |
| Class D | 1110 | 224 - 239 | 28 |

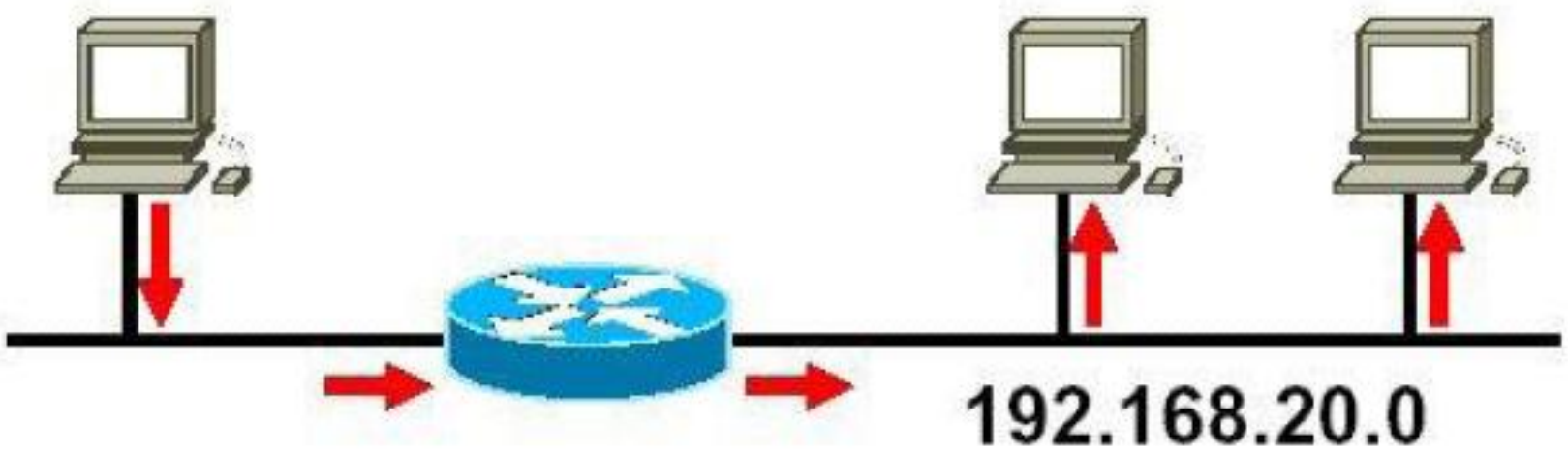
# Địa chỉ Broadcast

- Địa chỉ Broadcast có 2 loại:
- **Địa chỉ Broadcast Direct:** là địa chỉ IP mà tại phần Host ID có chứa toàn bộ các bit nhị phân là số 1 (VD: 192.168.20.255)
- **Địa chỉ Broadcast Directed:** là địa chỉ mà tại phần NetID và Host ID có chứa toàn bộ bit nhị phân 1. (VD: 255.255.255.255)

# Địa chỉ Broadcast



# Địa chỉ Broadcast




**192.168.20.255**

**Directed Broadcast Address**

# Ví dụ

- 172.16.20.200 là địa chỉ IP thuộc lớp B
- Net ID : **172.16**
- Host ID : **20.200**
- Network Add : **172.16.0.0**
- Broadcast Add : **172.16.255.255**

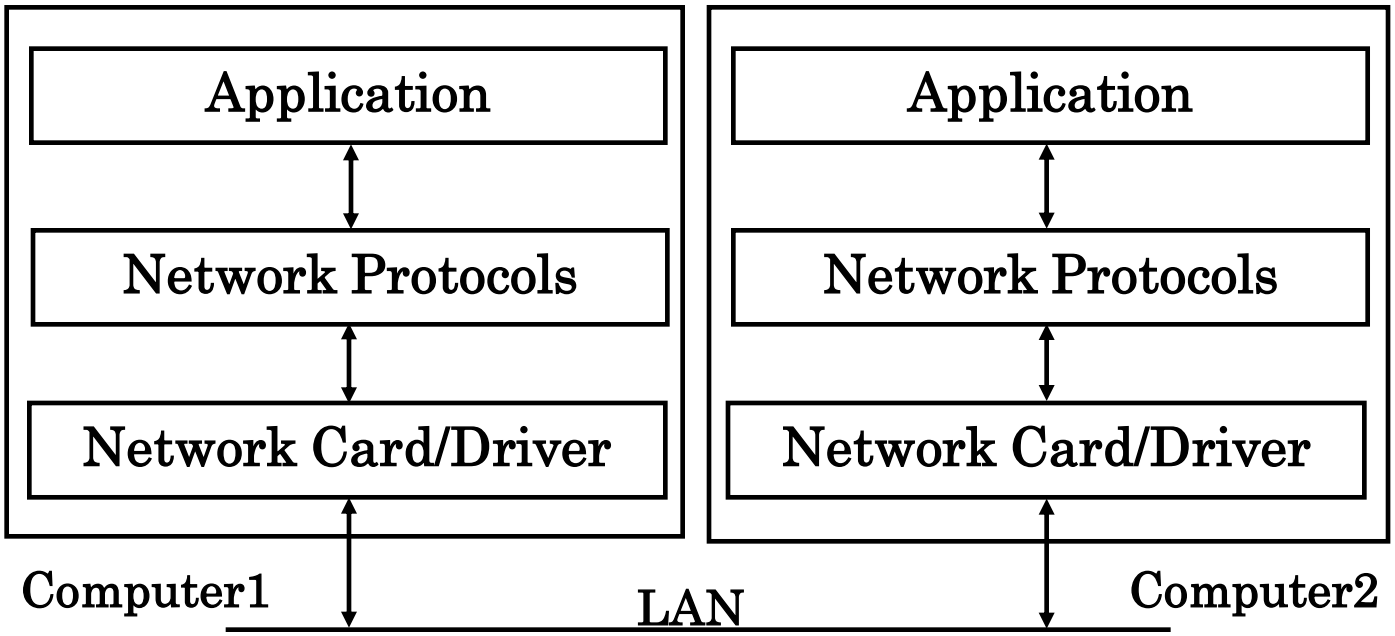
# Địa chỉ dùng trong mạng LAN

- Địa chỉ mạng riêng (private IP address) là địa chỉ có thể sử dụng địa chỉ riêng cho mỗi máy trong mạng cục bộ (LAN).
- Chuẩn RFC 1918 quy định 3 dãy địa chỉ IP cho mạng riêng:
  - Class A: **10.0.0.0**
  - Class B: **172.16.0.0 → 172.31.0.0**
  - Class C: **192.168.0.0 → 192.168.255.0**

# The Host-to-Host Layer Protocols

- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)

# 2 máy truyền thông dựa trên TCP/IP



# HỆ ĐIỀU HÀNH MẠNG

## GIỚI THIỆU WINDOWS và LINUX

# Mục tiêu của chương

**1. Giới thiệu chung về Windows và Linux.**

**2. So sánh Windows và Linux.**

- 1, Yêu cầu phần cứng.
- 2, Cài đặt và sử dụng.
- 3, Giao diện đồ họa.
- 4, Hiệu suất hoạt động.
- 5, Độ tin cậy.
- 6, Vấn đề bảo mật.
- 7, Vấn đề virus và khắc phục lỗi.
- 8, Tương thích phần cứng.
- 9, Hỗ trợ người sử dụng.

**3. Kết Luận.**

# I, Giới thiệu chung về Windows và Linux

## 1.1.Windows:

- Lần đầu tiên Microsoft giới thiệu một môi trường điều hành mang tên Windows (cửa sổ) là vào tháng 11 năm 1985 với những tín năng thêm vào MS-DOS giao diện hình tượng (Graphical User Interfaces, GUI)
- Windows khởi đầu được phát triển cho những máy tính tương thích với IBM (dựa vào kiến trúc x86 của Intel), và ngày nay hầu hết mọi phiên bản của Windows đều được tạo ra cho kiến trúc này
- Từ đó đến nay Microsofts Windows dần dần chiếm ưu thế trong thị trường máy tính cá nhân trên tòan thế giới với số lượng được cài đặt khoảng 90% vào năm 2004. Windows là phần_mềm nguồn đóng có bản quyền do công ty Microsoft giữ và kiểm soát việc phân phối. Vì lý do này, Microsoft đang có một vị trí độc quyền trong lĩnh vực máy tính cá nhân. Tất cả các phiên bản hệ điều hành gần đây củaWindows đều dựa trên sự phát triển từ phiên bản đầu tiên.

# I, Giới thiệu chung về Windows và Linux

## 1.2. Linux:

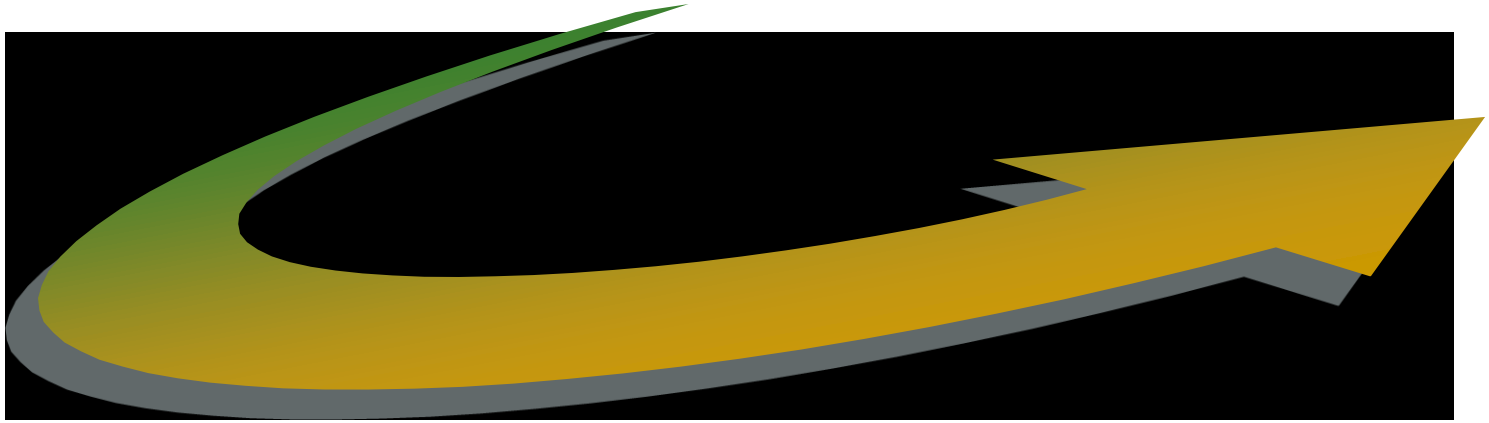
• Linux là tên gọi của một hệ điều hành máy tính v
cũng là tên hạt nhân của hệ điều hành. Nó có lẽ
một ví dụ nổi tiếng nhất của phần mềm tự do và cử
việc phát triển mã nguồn mở.

• Phiên bản Linux đầu tiên do Linus Torvalds viết vào năm 1991, lúc ông còn là một sinh viên của Đại_học Helsinki tại Phần Lan. Ông làm việc một cách hăng say trong vòng 3 năm liên tục và cho ra đời phiên bản Linux 1.0 vào năm 1994. Bộ phận chủ yếu này được phát triển và tung ra trên thị trường dưới bản quyền GNU General Public License.
Do đó mà bất cứ ai cũng có thể tải và xem mã nguồn của Linux.

• Khởi đầu, Linux được phát triển cho dòng vi xử lý 386, hiện tại hệ điều hành này hỗ trợ một số lượng lớn các kiến trúc vi xử lý, và được sử dụng trong nhiều ứng dụng khác nhau từ máy tính cá nhân cho tới các siêu_máy tính và các thiết bị nhúng như là các máy điện_thoại di động.

# II. So sánh giữa Windows và Linux

> = < ?



# 1. Yêu cầu phần cứng:

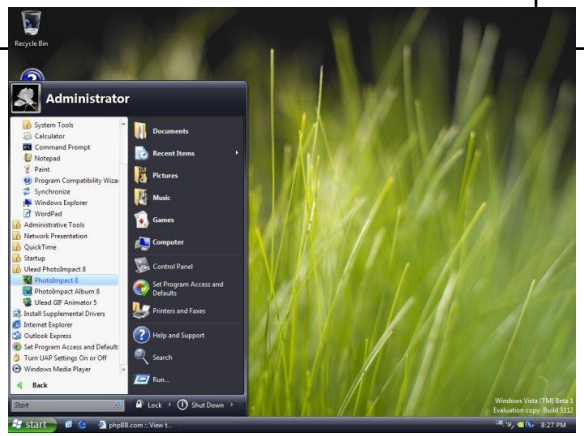
| Windows | Linus |
|---|---|
| • Windows đòi hỏi cấu hình khá cao. Windows NT4.0 cần tới 12Mb RAM, 70Mb ổ cứng. Windows XP đòi hỏi tối thiểu 64 Mb Ram, windows 2003 yêu cầu tới 128 Mb. Windows Vista Capable là phiên bản mới nhất, nó đòi hỏi cấu hình máy rất cao: partition tối thiểu là 15Gb, CPU tối thiểu là 800Mb, khả năng xử lí đồ họa DirectX9, dung lượng bộ cài lên tới 2Gb, ( chứa trong đĩa DVD), yêu cầu máy phải có ổ đĩa DVD. | • Linus tỏ ra rất dễ tính, nó có thể chạy trên nhiều nền tảng phần cứng khác nhau, chấp nhận cả những máy 386, 486. Linux phiên bản 1.x chỉ đòi hỏi 2Mb Ram và 6Mb graphich.<br>• Linux có thể chạy tốt trên những bộ vi xử lí nhỏ tích hợp trong các thiết bị điện tử dân dụng như điện thoại di động. Hiện nay, để kéo dài tuổi thọ của một số máy tính cũ, người ta chuyển từ dung windows sang dùn linux. |

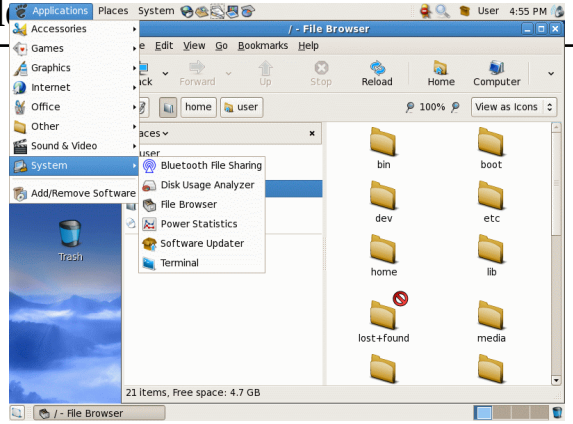
# 2. Cài đặt và khởi động:

| Windows | Linus |
|---|---|
| • Giao diện cài đặt thân thiện, chuyên nghiệp.<br>• Quá trình cài đặt khá nhanh.<br>• Cấu hình được lựa chọn trước bởi Microsoft nên người dùng không cần quan tâm nhiều về quá trình cài đặt<br>• Trợ giúp và hướng dẫn trong quá trình cài đặt chi tiết, chu đáo.<br>• Hình ảnh và âm thanh trong lần khởi động đầu tiên ấn tượng, có chương trình giới thiệu về windows.<br>• Quá trình khởi động:<br>▪ Chương trình mồi của BIOS tìm đến boot sector của master boot record.<br>▪ NTLDR đọc và chạy theo cấu hình trong boot.ini. NTDETECT kiểm tra và phát hiện phần cứng.<br>▪ NTLDR nạp NTOSKRNT.exe và HAL.ddl.<br>▪ Chương trình quản lý dịch vụ SMSS.exe được nạp. SCREG và LSASS được nạp cùng winlogon.<br>▪ Windows sẵn sàng. | • Cài đặt lên nhiều thư mục và phân vùng khác nhau. Các phân vùng có thể được thiết lập trên mạng.<br>• Các lựa chọn trong cài đặt rất phong phú. Có thể thêm hoặc loại bỏ bất kỳ một thành phần nào nên quá trình cài đặt có thể nhanh hay chậm.<br>• Có thể cài đặt từ xa.<br>• Có thể cài một hệ thống máy tính mà các thành phần chính dùng chung, giúp cho việc nâng cấp dễ dàng.<br>• Quá trình khởi động:<br>▪ Chương trình mồi của BIOS tìm đến boot sector của mater boot record sau đó nạp đoạn chương trình chứa trong đó lên bộ nhớ.<br>▪ Đoạn chương trình nạp file /etc/lib/lilo/conf, và biết là cần nạp nhân từ đâu.<br>▪ Khởi động chương trình init.<br>▪ Đọc file /etc/inittab và chạy theo các cấu hình đã thiết lập trong file.<br>▪ Người dùng có thể đăng nhập vào hệ thống. |

# 3, Giao diện đồ họa

| Windows | Linus |
| --- | --- |
| • Microsoft đã làm nên một cuộc cách mạng thực sự với sản phẩm windows 9x và windows XP. Giao diện đồ họa GUI đối với Linus là tùy chọn thì với Windows thì đó là một phần thiết yếu. | • Linux cung cấp hai chế độ đồ họa là GUI và chế độ dòng lệnh, mỗi giao diện có thể lựa chọn nhiều kiểu thể hiện khác nhau. Bản chất độc lập của Linux khiến cho việc điều khiển từ xa và quản trị từ xa một hệ thống Linux dễ dàng hơn so với windo |



# 4, Hiệu suất hoạt động:

| Windows | Linus |
| --- | --- |
| • Windows là một hệ điều hành khá tốt trong các ứng dụng của máy tính để bàn, máy xách tay. Tuy nhiên với các mạng lớn thì nó tỏ ra khó khăn hoặc không thể làm việc được. Sử dụng windows trong các hệ thống mạng, nhiều khi người ta gặp báo lỗi mà không biết nguyên nhân. | • Linux hoạt động tốt với nhiều ứng dụng, tuy nhiên không được tốt lắm với việc tải dữ liệu lớn trên mạng. So với FreeBSD thì hiệu suất mạng của Linux chỉ khoảng 20-30% trên cùng một phần cứng. Linux là phần mềm mã nguồn mở nên hiệu suất của nó sẽ được cải thiện nhanh chóng. |

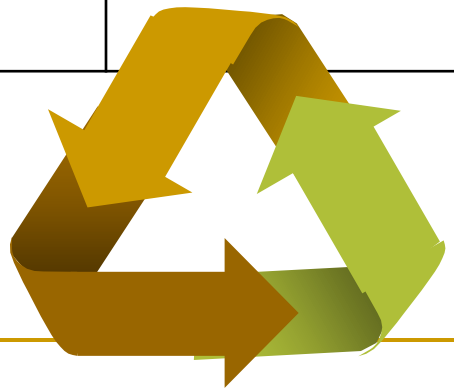
1 0 1010 01 01 01

1 0 1010 01 01 01

1 0 1010 01 01 01

# 5, Độ tin cậy:

| Windows | Linus |
| --- | --- |
| •Độ tin cậy kém là một trong những hạn chế lớn nhất của hệ điều hành này, nó gây ra rất nhiều khó khăn cho người sử dụng. Hầu như tất cả những người dùng máy tính đều đã từng ít nhất một lần gặp phải " Blue Screen of Death"-màn hình xanh tử thần. Hệ điều hành này sử dụng rất nhiều tài nguyên hệ thống khiến cho việc duy trì sự ổn định lâu dài là rất khó khăn. So với Linux thì windows tỏ ra ưu việt hơn trong việc tải dữ liệu. | •Linux nổi tiếng về độ tin cậy cao của nó. Những sever chạy trên nền Linux thì rất ổn định, có thể hoạt động tốt trong những khoảng thời gian lâu dài. Tuy nhiên khả năng truy xuất các loại đĩa vật lý của Linux là không đồng bộ và có thể gây hư hỏng những file hệ thống nếu như xuất hiện sự cố. Tuy vậy, với người dùng phổ thông thì Linux là một sự lựa chọn đáng tin cậy. |



# 6, Vấn đề bảo mật:

| Windows | Linus |
| --- | --- |
| •Windows cung cấp các tùy chọn bảo mật rất phong phú, ngoài ra nó có chương trình ghi nhận, thống kê các tác vụ bất hợp lệ. Firewall của Microsoft cũng là một "tấm là chắn" khá tin cậy so với các phần mềm trên thị trường.<br>•Microsoft thường cho rằng sản phẩm của họ an toàn về vấn đề bảo mật nhưng họ không đưa ra một sự đảm bảo nào. Windows là phần mềm mã nguồn đóng, người dùng không thể xem xét mã nguồn của windows, do đó không có cách nào để người sử dụng có thể tự khắc phục những lỗ hổng bảo mật của nó. Chỉ có một nhóm chuyên gia của Microsoft có thể làm công việc lấp đầy những lỗ hổng bảo mật của windows. | •Tính bảo mật của Linux được kiểm tra và xác nhận bởi hàng triệu người dùng và chuyên gia trên toàn thế giới. Bởi vậy, các lỗ hổng bảo mật của Linux nếu có thì cũng sẽ nhanh chóng được khắc phục.<br>•Việc phân quyền chặt chẽ khiến cho việc xóa hay ghi mà không được phép trở lên khó khăn hơn rất nhiều so với Windows.<br>•Firewall của Linus là một thành phần của hệ thống, nó nổi tiếng là tin cậy.<br>•Tuy nhiên, Linus chưa có các chương trình thống kê, ghi nhận và phát hiện các tác vụ không hợp lệ một cách chuyên nghiệp. |

# 7, Vấn đề Virus và Khắc phục l

| Windows | Linux |
|---|---|
| •Windows là hệ điều hành phổ biến nhất thế giới, do đó nó là mục tiêu của hầu như mọi loại hình tấn công trên mạng. Mỗi phiên bản hệ điều hành ra đời đều hầu như ngay lập tức có các virus phá hoại, mà việc khắc phục thì vô cùng khó khăn.<br>•Microsoft Windows được phát triển bởi những nhân viên lập trình ẩn danh, và những lỗi của họ được che khuất khỏi con mắt của thế giới do mã nguồn của Windows không được công bố rộng rãi, họ cho rằng đó là bí mật thương mại mang tính chiến lược.<br>•Việc khắc phục lỗi:<br>▪Khi gặp lỗi, người sử dụng có thể tìm xem có bản sửa lỗi thì download về, có thể gửi thông báo cho Microsoft, mà không thể tự sửa lấy.<br>▪Các lỗi được khắc phục thường lâu và có khi phải trả tiền.<br>▪Không thể đổi hãng cung cấp vì chỉ có Microsoft.<br>▪Microsoft thông báo rằng họ có tỉ lệ người lập trình/người kiểm tra là 1/1. | •Virus là một phần mềm do con người viết lên, do đó nếu nói rằng Linus là hệ điều hành "miễn nhiễm" virus thì hơi quá, nhưng Linus thực sự có ưu thế hơn Windows vì ít bị virus và hacker tấn công. Số lượng sâu( worm) và Trojan ở Linus ít hơn nhiều và gây tác hại không đáng kể so với windows.<br>•Linus được phát triển bởi hàng ngàn lập trình viên, họ công bố mã nguồn một cách rộng rãi, do đó bất kì một ai quan tâm cũng có thể xem xét, bất kì một lỗi gì cũng có thể nhanh chóng được khắc phục.<br>•Việc khắc phục lỗi:<br>▪Khi gặp lỗi người sử dụng có thể tìm xem có bản sửa lỗi thì tải về, có thể đề nghị sửa lỗi với tác giả, nếu không mang lại kết quả thì có thể tự sửa lấy.<br>▪Các lỗi được khắc phục rất nhanh, có khi chỉ trong vòng vài phút sau khi được thông báo.<br>▪Có thể đổi hãng cung cấp Linus nếu muốn.<br>▪Một bản Linus thường được rất nhiều chuyên gia kiểm tra trước khi tung ra thị trường. |

# 8, Tương thích với phần cứng:

| Windows | Linus |
|---|---|
| •Microsoft có mối quan hệ rất tốt với các nhà sản xuất phần cứng, do đó các hệ điều hành Windows của họ đã được tích hợp sẵn một số trình điều khiển thiết bị phần cứng, người sử dụng có thể mua về và sử dụng ngay một số thiết bị mà không cần cài đặt.<br>•Mặc dù vẫn có nhiều xung đột trong việc sử dụng các driver với các phiên bản khác nhau của Windows, nhưng nói chung, hầu hết người sử dụng có thể truy cập tốt các trình điều khiển thiết bị.<br>•Quá trình cài đặt các driver đơn giản và nhanh chóng. Các nhà cung cấp phần cứng thường xuyên nâng cấp các phiên bản driver của họ. | •Linus không có nhà phần phối duy nhất, do đó các bản Linus có nhiều sự khác nhau, đôi khi xung đột với nhau. Điều này gây khó khăn cho những nhà sản xuất thiết bị phần cứng vì họ phải cung cấp mã nguồn driver cho các nhà phát triển Linus, mà các nhà sản xuất thì không sẵn lòng làm như vậy do vấn đề bản quyền công nghệ.<br>•Trình điều khiển của một số thiết bị mới có thể không có hoặc muộn hơn so với Windows.<br>•Có một số thiết bị không thể hoạt động với Linux.<br>•Chưa hỗ trợ hoàn toàn các thiết bị flash, USB. |

# 9, Hỗ trợ người sử dụng:

| Windows | Linus |
| --- | --- |
| Microsoft đưa ra những dịch vụ hỗ trợ cho sản phẩm của mình, tuy nhiên những sự hỗ trợ đó mang tính chủ quan và thường không kịp thời. | Những nhà cung cấp Linus đưa ra nhiều dịch vụ hỗ trợ khách hàng, và thường miễn phí. Xuất hiện nhiều diễn đàn của cộng đồng người dùng Linus, đó cũng là một sự hỗ trợ lớn cho những người dùng Linus. |

# III. Kết Luận:

- Qua những so sánh trên ta thấy được sự vươn lên mạnh mẽ của một hệ điều hành mới thuộc họ UNIX. Có thể thấy những ưu điểm nổi bật nhất của Linus là tính bảo mật, độ tin cậy, miễn phí, và hỗ trợ người sử dụng rất tốt. Linus nhanh chóng khắc phục được những hạn chế của mình và đang trở thành đối thủ lớn của Windows.
- Song song với việc đó, Windows, mà đứng đằng sau là tập đoàn Microsoft mạnh nhất thế giới cũng có rất nhiều cải tiến nhằm tối ưu hóa hệ điều hành của mình. Ưu điểm lớn nhất của Windows là sự thống nhất mang tính toàn cầu và tương thích giữa hệ điều hành với các thiết bị phần cứng rất tốt.
- Sẽ còn là quá sớm để cho rằng Linus có thể thay thế được cho Windows trong một tương lai gần. Microsoft có những lý do để Windows của họ vẫn là hệ điều hành thông dụng nhất.
- Cuộc cạnh tranh phát triển hệ điều hành sẽ còn tiếp tục trong thời gian sắp tới, và "biết đâu, đến một lúc nào đó sẽ có sự gặp gỡ thân mật giữa Windows và Linus?"

# Operating Systems Network

| Properties / OS | Com-mand | GUI | Multi-user | Multi-tasking | Multi-processing | Net-work | Server | Real-time |
|---|---|---|---|---|---|---|---|---|
| MS-DOS | X | | | | | | | |
| Windows 9x | X | X | | X | | X | | |
| Windows NT/2000/XP | X | X | X | X | X | X | | |
| Windows NT/2000 Server | X | X | X | X | X | X | X | |
| Unix | X | X | X | X | X | X | X | |
| Linux | X | X | X | X | X | X | X | |
| Sun Solaris | X | X | X | X | X | X | X | |
| Mac OS | X | X | X | X | X | X | | |
| Real-Time OS | | | | | | | | X |

# HỆ ĐIỀU HÀNH MẠNG

## Cài đặt Windows XP và thiết lập mạng ngang hàng

# Mục đích:

- Mục đích của chương này nhằm giới thiệu chi tiết các bước cài đặt hệ điều hành Microsoft Windows 2000 Professional từ các máy tính có phiên bản thấp hơn và mới từ CDROM, thiết lập cấu hình mạng TCP/IP rồi kiểm tra mạng ở mức tầng vật lý. Từ đây ta xây dựng mạng con. Thiết lập, quản lý tài khoản người dùng và nhóm người dùng; rồi quản lý chia sẻ tài nguyên trên mạng như: tập tin, thư mục, máy in, …

# Yêu cầu về hệ thống

| | |
|---|---|
| **CPU** | **- Pentium 133MHz hoặc bộ vi xử lý cao hơn (hay tương đương).**<br>**- Windows XP hỗ trợ trên 2 bộ vi xừ lý.** |
| **Bộ nhớ (Memory)** | **- Tối thiểu 64 MB**<br>**- Tối đa 4 GB.** |
| **Màn hình hiển thị** | **- Màn hình có độ phân giải VGA (Video graphics array) hoặc cao hơn.** |
| **Thiết bị phụ trợ** | **- Bàn phím và chuột hay các thiết bị trỏ khác.** |
| **Nếu cài đặt bằng ổ CD-ROM** | **- Ổ CD-ROM từ 12x trở lên.** |
| **Nếu có cài đặt mạng** | **- Một hoặc nhiều card mạng, driver của card mạng tương ứng và các dây cable có liên quan.** |

# Yêu cầu phân vùng (partition)

- NTFS là hệ thống tập tin được đề nghị sử dụng cho Windows 2000 và XP. Sử dụng NTFS có các ưu điểm sau đây:
- - Bảo vệ tập tin và thư mục: NTFS cho phép kiểm soát và truy cập những tập tin và thư mục.
- - Nén dữ liệu: NTFS tự động nén dữ liệu để tạo khoảng trống cho việc lưu trữ.
- - Quản lý hạn ngạch ổ đĩa: NTFS cho phép kiểm soát việc sử dụng đĩa của từng người dùng (user). - Mã hoá dữ liệu: NTFS cho phép mã hoá dữ liệu.
- - FAT và FAT 32 cũng có thể được sử dụng trong Windows 2000 nhưng FAT không hỗ trợ partition có kích thước lớn hơn 2GB và chúng không bằng so với hệ thống NTFS. Tuy nhiên nên dùng FAT và FAT 32 nếu cần cấu hình hệ thống khởi động có chọn lựa giữa hệ thống Win9x và Win2000.

# Yêu cầu thực hành

- **Thực hành sử dụng chức năng My Network Places để duyệt các máy tính trong mạng.**
- **Thực hành cấu hình mạng ngang hàng**

- Xây dựng mạng con
- Mục tiêu của việc xây dựng mạng con
- Kiểm tra thông mạng qua các lệnh cơ bản: ping, ipconfig

- **Thiết lập và quản lý tài khoản người dùng và nhóm cục bộ**

**Giới thiệu**

- *Chế độ bảo mật trong Windows dựa trên khái niệm tài khoản người dùng (user account). Tài khoản người dùng gồm một cặp: username (tên truy cập), và password (mật khẩu) là giấy chứng nhận hợp pháp của riêng người dùng, cho phép người này có thể truy nhập tài nguyên cục bộ (local) hoặc tài nguyên vùng (domain).*

# Các loại tài khoản người dùng

| Tài khoản | Mô tả |
|---|---|
| *1.Tài khoản do người sử dụng tạo* | Cho phép người sử dụng đăng nhập máy tính cục bộ hoặc đăng nhập vùng với quyền truy cập cho phép. |
| *2. Guest* | Được dùng để cung cấp khả năng đăng nhập và truy cập tài nguyên trên máy tính cục bộ cho những người dùng không thường xuyên. |
| 3.Administrators | Được dùng để quản lý tài nguyên và cấu hình toàn thể của máy tính và của vùng. Tài khoản Administrator được dùng khi thi hành những tác vụ quản trị. |

# Các loại tài khoản người dùng

| Tuỳ chọn | Mô tả |
|---|---|
| User Must Change Password at Next Logon (Mặc định được chọn) | Cho phép user thay đổi mật mã của mình vào lần đăng nhập vào mạng đầu tiên. Điều này đảm bảo user là người duy nhất biết mật khẩu của mình. |
| User Cannot Change Password | User không thể thay đổi mật mã này. Ví dụ có một user dùng chung cho nhiều người. |
| Password Never Expires | Mật khẩu không bao giờ thay đổi. Khi chọn tùy chọn này thì tùy chọn User Must Change Password at Next Logon mờ đi |
| Account Disables | Tạm ngưng quyền sử dụng của user. |

# Các loại tài khoản người dùng

| | |
|---|---|
| Administrators | Là nhóm có quyền lực lớn nhất. Bởi vì, nhóm Administrators có đầy đủ quyền điều khiển trên toàn môi trường Windows, cho nên bạn cần phải thận trọng khi thêm vào những user trong group này. **Trong những trường hợp sau, thật là cần thiết để sử dụng nhóm Administrators:**<br>• Tạo ra những user quản trị khác.<br>• Chỉnh sửa hay hủy user.<br>• Quản lý những thành viên trong những group xây dựng sẵn. Khóa những máy trạm, không quan tâm đến người khoá chúng.<br>• Format đĩa cứng.<br>• Nâng cấp hệ điều hành.<br>• Backup và phục hồi những tệp và thư mục.<br>• Thay đổi những chính sách an toàn.<br>• Kết nối để quản trị tài nguyên đã chia sẻ. |
| Users | Mặc định, những user mới tạo sẽ là thành viên của group này. **Users có thể thi hành những tác vụ sau:**<br>•Chạy những ứng dụng.<br>•Quản lý những tệp và thư mục của mình (nhưng không chia sẻ chúng).<br>•Sử dụng máy in (nhưng không chia sẻ chúng).<br>•Kết nối đến những thư mục và máy in của những máy tính khác |

# Các loại tài khoản người dùng

| | |
|---|---|
| Guests | Thi hành những tác vụ họ đã được cấp quyền thi hành, và truy cập những tài nguyên họ đã được cấp phép truy cập. Thành viên của nhóm Guests không thể thực những thay đổi vĩnh viễn cho môi trường cục bộ của họ. Mặc định, tài khoản Guest cục bộ là thành viên của nhóm Guests. |
| Backup Operators | Mục đích duy nhất là backup file, thư mục và phục hồi lại chúng sau đó. Không có thành viên mặc định. |
| Replicator | Nhóm đặc biệt này được sử dụng bởi dịch vụ Directory Replication. |
| Print operators | Có nhiệm vụ tạo, quản lý và hủy những tài nguyên về in ấn. |
| Server Operators | Dùng để quản trị primary và backup domain controller. Những user trong nhóm này có thể logon vào và shutdown server, khóa và mở khóa server, thay đổi thời gian hệ thống, backup và phục hồi file, và quản lý những tài nguyên chia sẻ trên mạng. |
| Account Operators | Những thành viên trong nhóm này có khả năng tạo, hủy và chỉnh sửa users ngoại trừ nhóm Server Operators và Administrators. |

# Thực hành chia sẻ tài nguyên

**Chia sẻ tài nguyên trong mạng Workgroup**

**Chia sẻ máy in (print).**

**Truyền thông điệp (message)**

**Hội thảo (Meeting)**

# HỆ ĐIỀU HÀNH MẠNG

Quản trị Windows XP

# Windows XP

- **1. Cách thức làm việc của Registry**
- **1. Giới thiệu:** Registry là một database (cơ sở dữ liệu) dùng để lưu trữ thông số kỹ thuật của Windows mà nó cho phép bạn làm 3 chức năng cơ bản là: thêm/xóa/sửa. Và những thao tác đó đều ảnh hưởng đến windows. Trong Windows 2k, nó được lưu vào thư mục **C:\Windows\System32\Config**

# Windows XP

- **2 Cấu trúc của Registry:**
  Registry có cấu trúc kiểu cây thư mục với 5 nhánh chính (thông thường là 5) và nhiều nhánh con (hay còn gọi là key) chứa các thông tin khác nhau tùy vào từng nhánh. Các nhánh chính gồm
  **HKEY_CLASSES_ROOT**: Lưu những thông tin dùng chung cho toàn bộ hệ thống.
  **HKEY_CURRENT_USER**: Lưu những thông tin cho người dùng đang Logon
  **HKEY_LOCAL_MACHINE**: Lưu những thông tin về hệ thống, phần cứng, phần mềm.
  **HKEY_USERS**: Lưu những thông tin của tất cả các User, mỗi user là một nhánh với tên là số ID của user đó
  **HKEY_CURRENT_CONFIG**: Lưu thông tin về phần cứng hiện tại đang dùng.

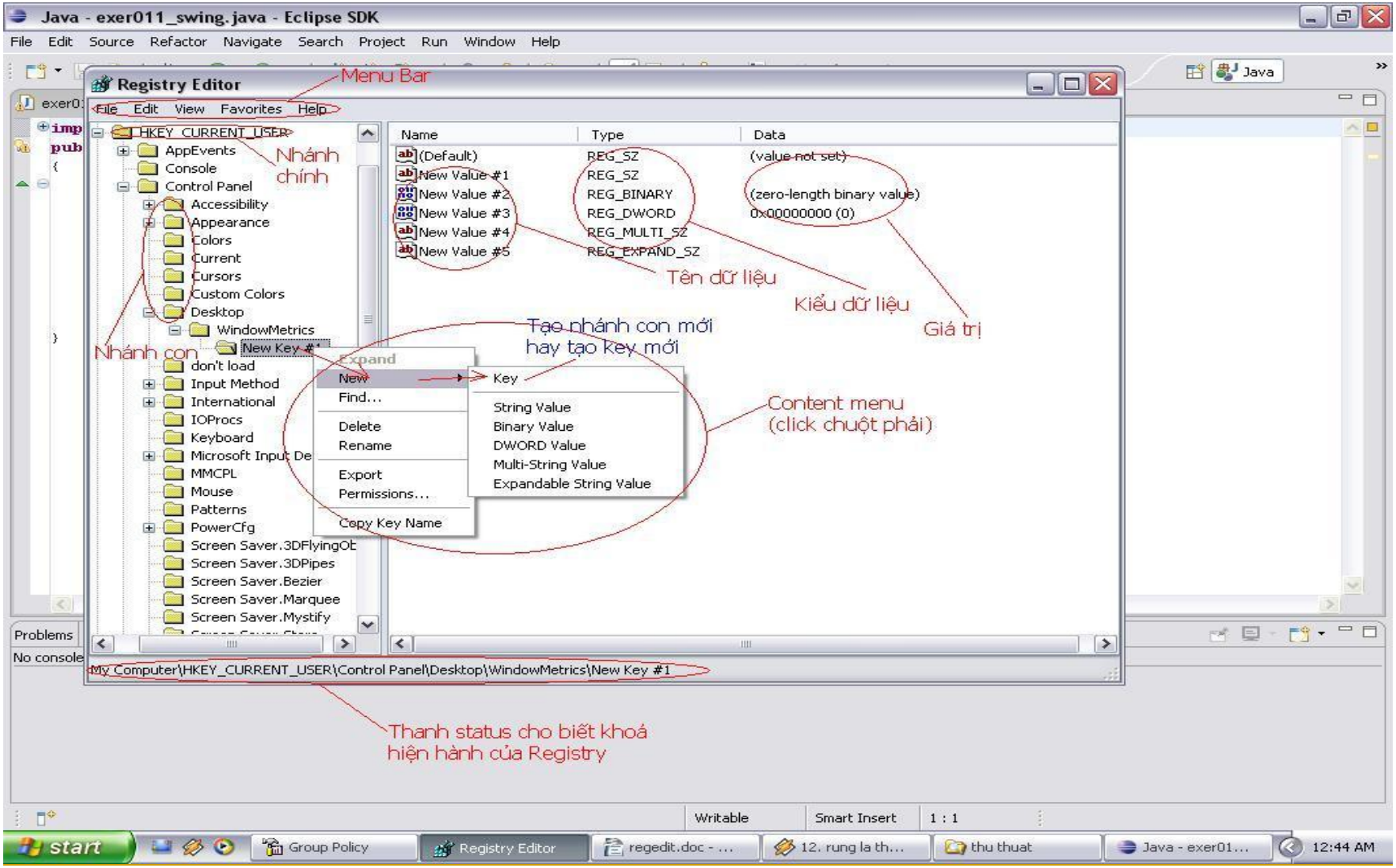
# Windows XP

- **3. Các kiểu dữ liệu :**
  -**REG_BINARY**: Kiểu nhị phân
  -**REG_DWORD**: Kiểu Double Word
  -**REG_EXPAND_SZ**: Kiểu chuỗi mở rộng đặc biệt. VD: “%SystemRoot%”
  -**REG_MULTI_SZ**: Kiểu chuỗi đặc biệt
  -**REG_SZ**: Kiểu chuỗi chuẩn

# Windows XP

- **4.Làm việc với Registry:**
  a.Giao diện Registry:
  b.Các chức năng chính: (trên thanh menu bar) ở đây chỉ giới thiệu với các bạn các chức năng thường xuyên sd
  -**File –> Import** : dùng để import 1 khoá hay 1 nhóm các khóa registry với dạng file có đuôi mở rộng xxx.reg. Ứng dụng trong trường hợp này là thực thi 1 file registry đc viết sẵn thay vì đánh trực tiếp vào (sẽ nói ở phần tiếp theo) hay backup lại registry
  -**File –> Export** : dùng để xuất ra 1 khoá hay 1 nhóm các khoá thường với 2 định dạng xxx.reg hoặc xxx.txt. Ứng dụng trong trường hợp này là để sao lưu Registry khi cần thiết có thể backup trở lại
  **EX:** Để sao lưu 1 nhánh Registry hoặc cả registry

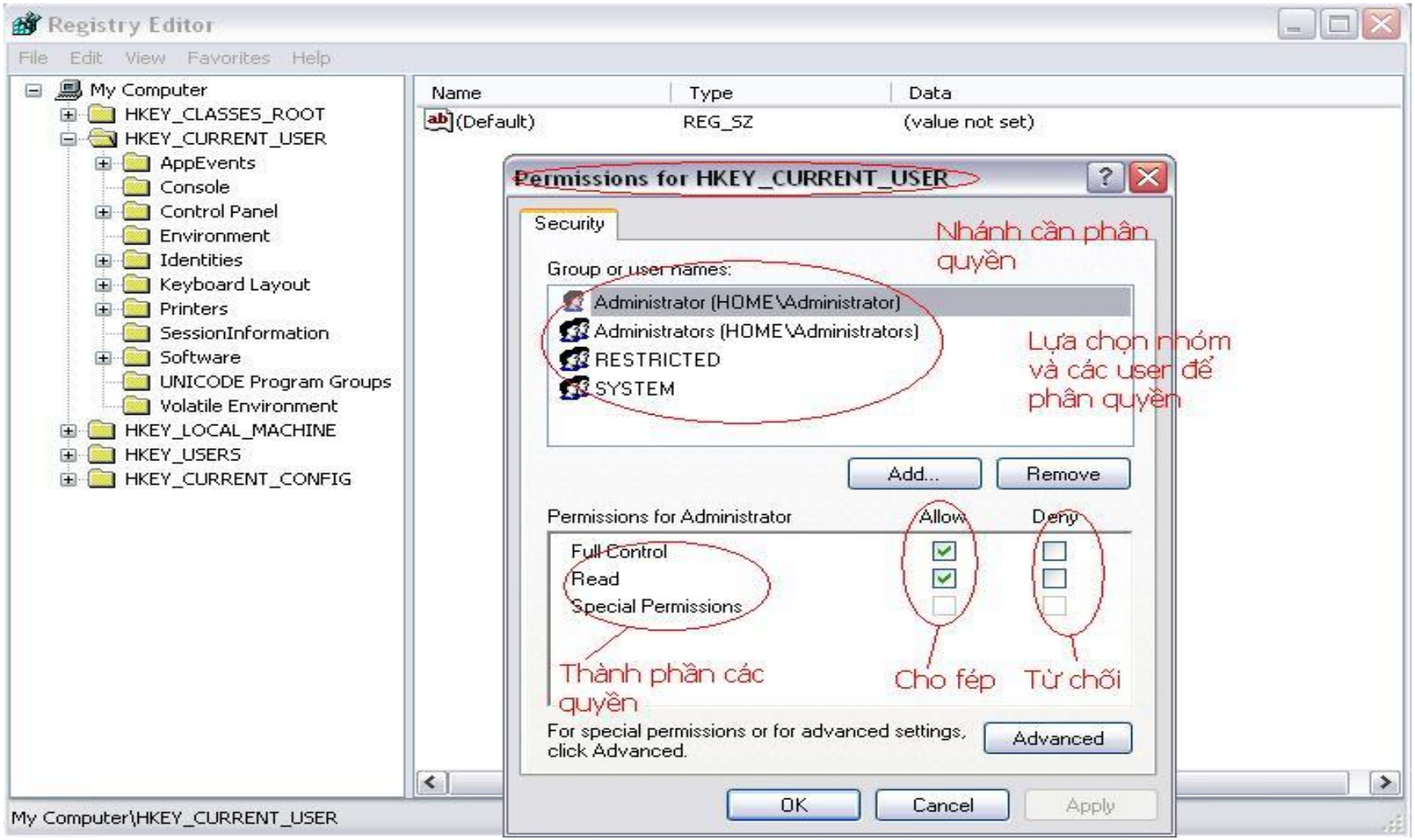
# Windows XP


Java - exer011_swing.java - Eclipse SDK
File Edit Source Refactor Navigate Search Project Run Window Help
Registry Editor
Menu Bar
File Edit View Favorites Help
HKEY_CURRENT_USER
AppEvents
Console
Control Panel
Accessibility
Appearance
Colors
Current
Cursors
Custom Colors
Desktop
WindowMetrics
New Key #1
don't load
Input Method
International
IOProcs
Keyboard
Microsoft Input De
MMCPL
Mouse
Patterns
PowerCfg
Screen Saver.3DFlyingOb
Screen Saver.3DPipes
Screen Saver.Bezier
Screen Saver.Marquee
Screen Saver.Mystify
Nhánh chính
Nhánh con
Name
Type
Data
(Default)
REG_SZ
(value not set)
New Value #1
REG_SZ
New Value #2
REG_BINARY
(zero-length binary value)
New Value #3
REG_DWORD
0x00000000 (0)
New Value #4
REG_MULTI_SZ
New Value #5
REG_EXPAND_SZ
Tên dữ liệu
Kiểu dữ liệu
Giá trị
Tạo nhánh con mới
hay tạo key mới
Expand
New
Find...
Delete
Rename
Export
Permissions...
Copy Key Name
Key
String Value
Binary Value
DWORD Value
Multi-String Value
Expandable String Value
Content menu
(click chuột phải)
My Computer\HKEY_CURRENT_USER\Control Panel\Desktop\WindowMetrics\New Key #1
Thanh status cho biết khoá
hiện hành của Registry
Problems
No console
Writable
Smart Insert
1 : 1
start
Group Policy
Registry Editor
regedit.doc - ...
12. rung la th...
thu thuat
Java - exer01...
12:44 AM

# Windows XP

- Các chức năng chính: (trên thanh menu bar) ở đây chỉ giới thiệu với các bạn các chức năng thường xuyên sử dụng
  -**File –> Import** : dùng để import 1 khoá hay 1 nhóm các khóa registry với dạng file có đuôi mở rộng xxx.reg. Ứng dụng trong trường hợp này là thực thi 1 file registry đc viết sẵn thay vì đánh trực tiếp vào (sẽ nói ở phần tiếp theo) hay backup lại registry
  -**File –> Export** : dùng để xuất ra 1 khoá hay 1 nhóm các khoá thường với 2 định dạng xxx.reg hoặc xxx.txt. Ứng dụng trong trường hợp này là để sao lưu Registry khi cần thiết có thể backup trở lại
  **EX:** Để sao lưu 1 nhánh Registry hoặc cả registry
- -**Edit –> Find**: cái này thì chắc bạn nào cũng biết nên mình sẽ bỏ wa
  -**Edit –> Permissions**, cho fép phân quyền theo nhóm hoặc user, bạn có thể làm theo hình sau:

# Windows XP


Registry Editor
File Edit View Favorites Help
My Computer
HKEY_CLASSES_ROOT
HKEY_CURRENT_USER
AppEvents
Console
Control Panel
Environment
Identities
Keyboard Layout
Printers
SessionInformation
Software
UNICODE Program Groups
Volatile Environment
HKEY_LOCAL_MACHINE
HKEY_USERS
HKEY_CURRENT_CONFIG
Name
Type
Data
(Default)
REG_SZ
(value not set)
Permissions for HKEY_CURRENT_USER
Security
Nhánh cần phân quyền
Group or user names:
Administrator (HOME\Administrator)
Administrators (HOME\Administrators)
RESTRICTED
SYSTEM
Lựa chọn nhóm và các user để phân quyền
Add...
Remove
Permissions for Administrator
Allow
Deny
Full Control
Read
Special Permissions
Thành phần các quyền
Cho fép
Từ chối
For special permissions or for advanced settings, click Advanced.
Advanced
OK
Cancel
Apply
My Computer\HKEY_CURRENT_USER

# Windows XP

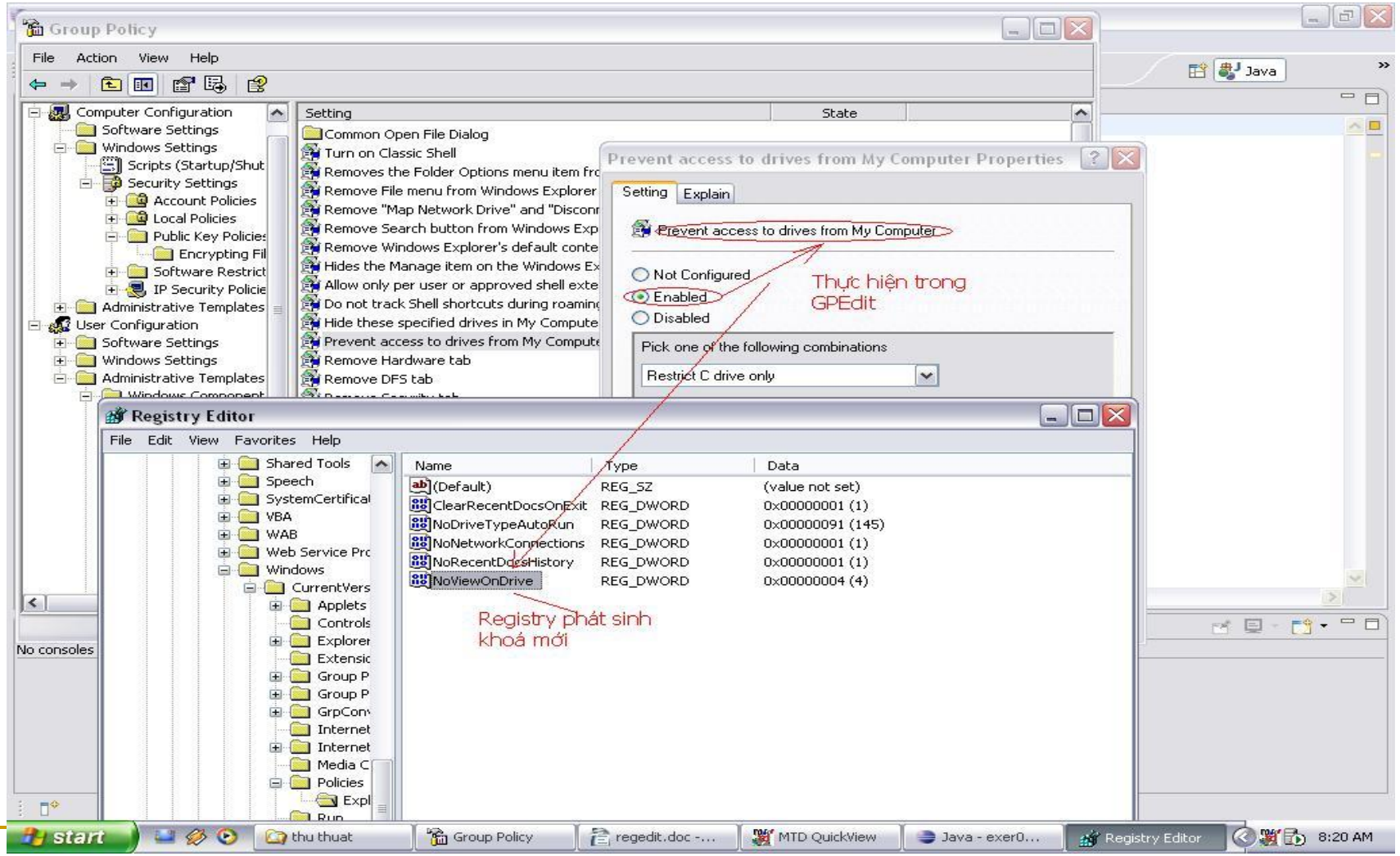
**Dùng Group policy trong Windows để quản lý Registry:**

- Như vậy trong phần 1 bạn có thể biết cách làm việc của 1 registry rồi phải ko? Tuy nhiên, trong ứng dụng thực tế, việc nhớ hết tất cả các từ khoá đó thì ko thể nào nhớ nổi. Ví dụ, bạn muốn tắt 1 cái nút search trong start menu để cấm người lạ tìm kiếm tài liệu của bạn hay muốn cấm truy xuất đến 1 ổ đĩa nhạy cảm mà bạn muốn sử dụng riêng hoặc là bạn tắt đi registry để tránh mọi người vào phá máy bạn thì để nhớ hết các khoá đó đúng là hết sức khó khăn. Rất may là có nhiều soft đã tạo sẵn và bạn có thể làm đều này chỉ với 1 cái click chuột (có rất nhiều trên Net). Trong bài viết này mình xin giới thiệu về Group Policy Edit có sẵn trong Windows để làm các công việc đó. Nội dung:
  **-Cách thức làm việc của Group Policy**
  **-Một số ứng dụng cụ thể**

# Windows XP

- **Cách thức làm việc của Group Policy :** -Khởi động Group Policy Edit : bạn có thể khởi động từ run và gỏ: gpedit.msc. Tuy nhiên, riêng với Win XP Home sẽ ko có file này, do đó bạn cần phải chép từ máy khác qua. Đường dẫn chứa file gpedit.msc trong các windows khác là : C:\windows\system32\gpedit.msc
  -***Giao diện***: tương tự như registry, giao diện của nó thuộc dạng cây thư mục bao gồm 2 nhánh chính và các nhánh con. Mỗi nhánh con khi được enable là đồng nghĩa với 1 khoá trong registry thực thi.
  EX : Khi bạn muốn cấm truy xuất 1 partition thì khi bạn làm trong gpedit thì registry sẽ phát sinh 1 khoá mới thực thi hành động bạn làm. Xem hình ảnh minh hoạ

# Windows XP


Group Policy
File Action View Help
Computer Configuration
Software Settings
Windows Settings
Security Settings
Account Policies
Local Policies
Public Key Policies
Software Restrict
IP Security Policie
Administrative Templates
User Configuration
Software Settings
Windows Settings
Administrative Templates
Setting
State
Common Open File Dialog
Turn on Classic Shell
Remove File menu from Windows Explorer
Remove "Map Network Drive" and "Disconn
Remove Search button from Windows Exp
Remove Windows Explorer's default conte
Hides the Manage item on the Windows Ex
Allow only per user or approved shell exte
Do not track Shell shortcuts during roaming
Hide these specified drives in My Compute
Prevent access to drives from My Compute
Remove Hardware tab
Remove DFS tab
Prevent access to drives from My Computer Properties
Setting
Explain
Prevent access to drives from My Computer
Not Configured
Enabled
Disabled
Thực hiện trong GPEdit
Pick one of the following combinations
Restrict C drive only
Registry Editor
File Edit View Favorites Help
Shared Tools
Speech
VBA
WAB
Windows
CurrentVers
Applets
Controls
Explorer
Internet
Media C
Policies
Run
Name
Type
Data
(Default)
REG_SZ
(value not set)
ClearRecentDocsOnExit
REG_DWORD
0x00000001 (1)
NoDriveTypeAutoRun
REG_DWORD
0x00000091 (145)
NoNetworkConnections
REG_DWORD
0x00000001 (1)
NoRecentDocsHistory
REG_DWORD
0x00000001 (1)
NoViewOnDrive
REG_DWORD
0x00000004 (4)
Registry phát sinh khoá mới
No consoles
Java
start
thu thuat
Group Policy
regedit.doc -...
MTD QuickView
Java - exer0...
Registry Editor
8:20 AM

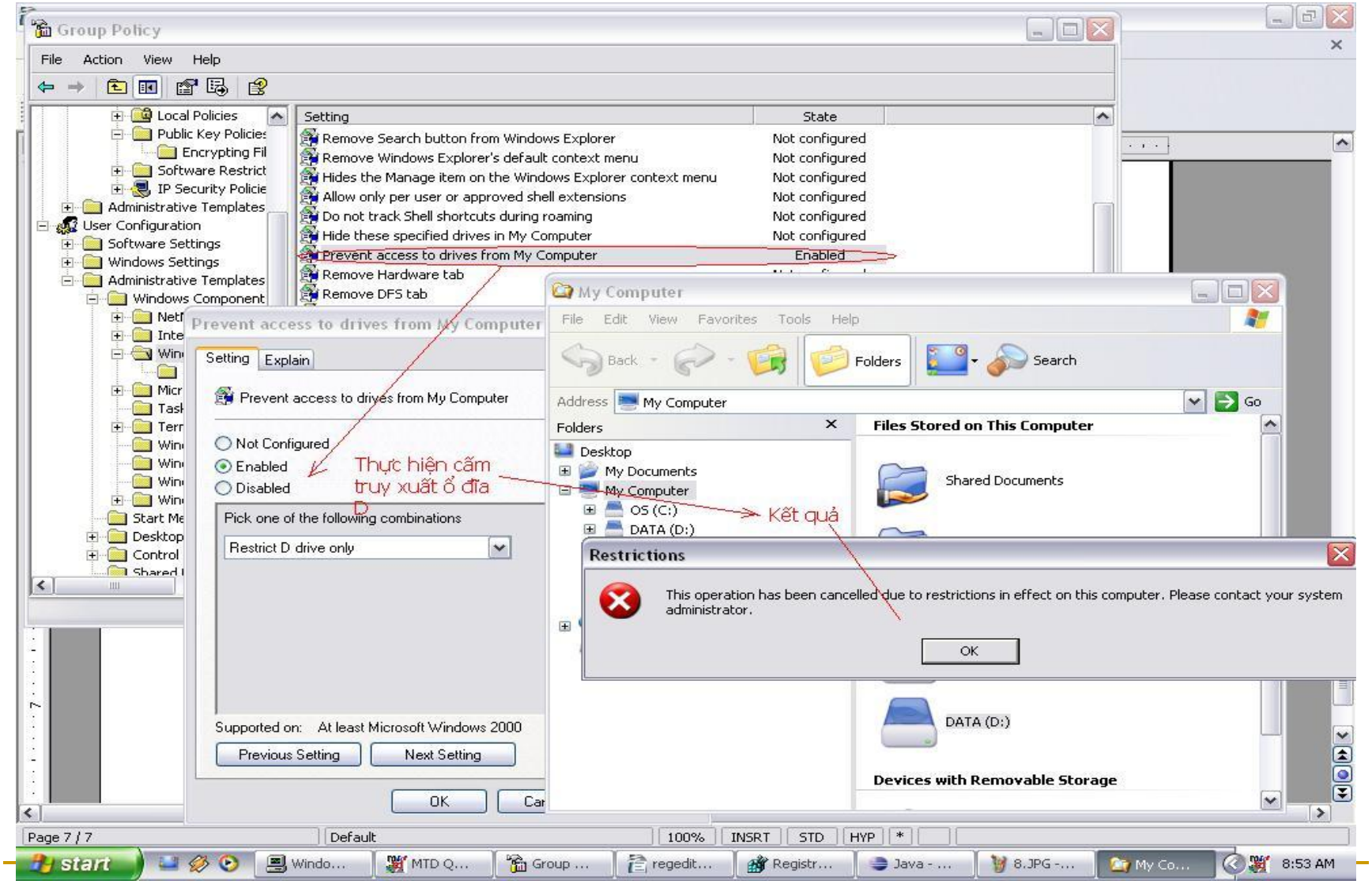
# Windows XP

- ***Cách thức thực hiện***: ở ví dụ trên, giả sử khi bạn cấm truy xuất đến ổ C thì bạn click chuột vào nó đưa bạn đến của sổ thành phần của hành động đó. Ở đây, có 3 từ khoá quan trong mà mình muốn nhắc đến là: Not Config, Enable và Disable
  +*Not Config*: Khi bạn chọn Not config là Registry sẽ giữ nguyên trạng thái ban đầu của nó
  +*Enable*: Thực thi hành động trong gpedit và Registry sẽ phát sinh 1 khoá mới để thực thi
  +*Disable*: Cấm ko cho phép thực thi hành động đó. Mới nhìn thì bạn thấy rất giống Not Config nhưng thực ra bạn cần phân biệt sự nhau giữ nhau giữa chúng. Đó là khi bạn Not Config thì hành động trước đó vẫn còn, và khi Disable thì nó sẽ mất hẳn luôn hành động trước.
  EX: Ban đầu bạn cấm truy xuất ổ đĩa C trong registry. Nếu bạn chọn Not Config thì việc cấm truy xuất đó vẫn thực hiện, còn nếu bạn chọn Disable là nó sẽ mất đi hành động

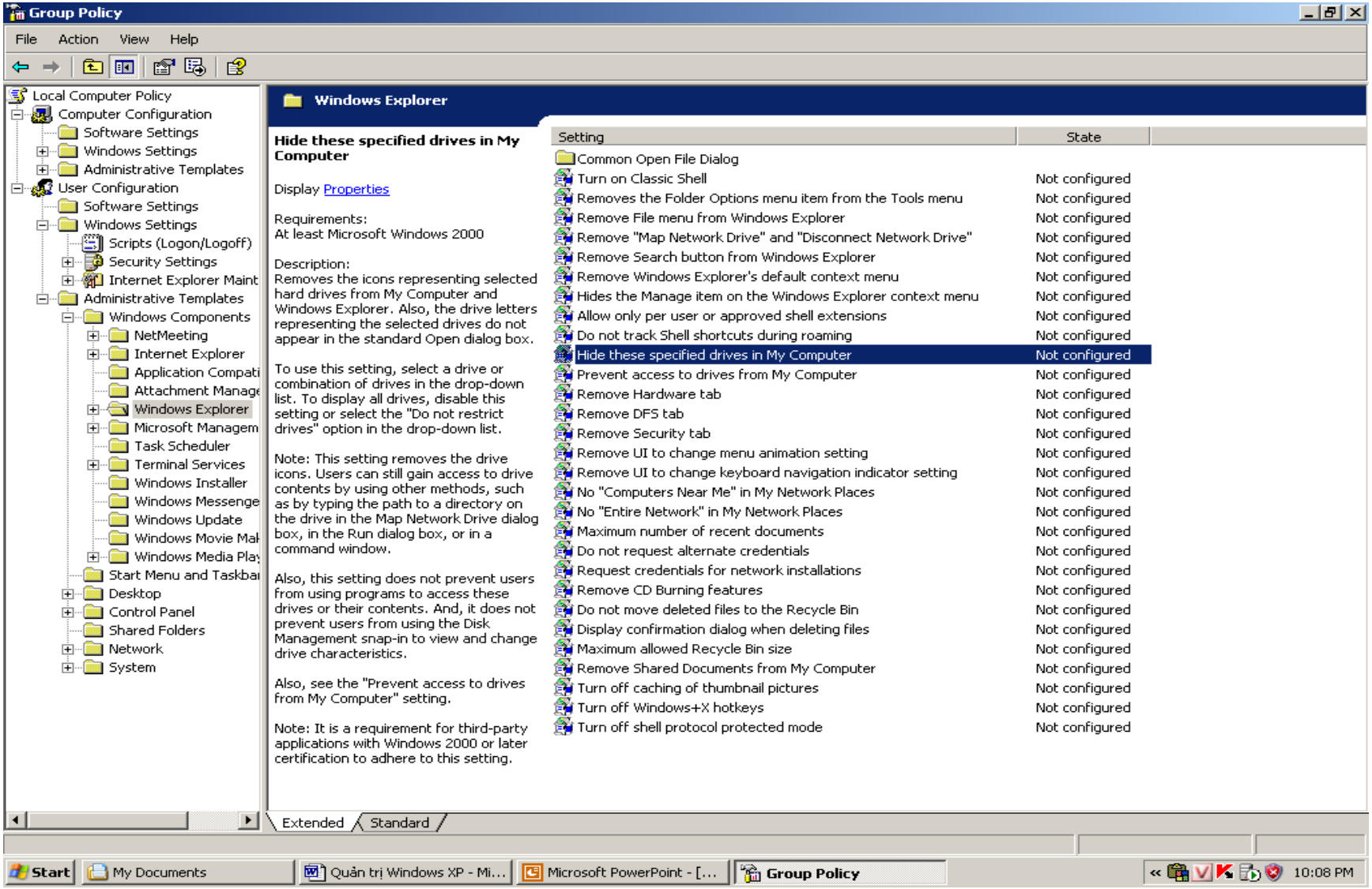
# Windows XP

- **Một số ứng dụng cụ thể** : Ở đây có rất nhiều hành động để bạn chọn, mình chỉ lấy ví dụ điển hình để các bạn có thể lấy mẫu để làm cho những cái khác
  Ex1: **Xử lý các component trong windows**. Có rất nhiều các hành động ở đây chỉ lấy 1 Ex về việc cấm truy xuất ổ đĩa D (hoặc các ổ đĩa khác tùy bạn chọn)

# Windows XP


Group Policy
File Action View Help
Setting State
Remove Search button from Windows Explorer Not configured
Remove Windows Explorer's default context menu Not configured
Hides the Manage item on the Windows Explorer context menu Not configured
Allow only per user or approved shell extensions Not configured
Do not track Shell shortcuts during roaming Not configured
Hide these specified drives in My Computer Not configured
Prevent access to drives from My Computer Enabled
Remove Hardware tab
Remove DFS tab
Prevent access to drives from My Computer
Setting Explain
Prevent access to drives from My Computer
Not Configured
Enabled
Disabled
Pick one of the following combinations
Restrict D drive only
Supported on: At least Microsoft Windows 2000
Previous Setting Next Setting
OK
Thực hiện cấm truy xuất ổ đĩa D
My Computer
File Edit View Favorites Tools Help
Back Folders Search
Address My Computer Go
Folders
Desktop
My Documents
My Computer
OS (C:)
DATA (D:)
Kết quả
Files Stored on This Computer
Shared Documents
Restrictions
This operation has been cancelled due to restrictions in effect on this computer. Please contact your system administrator.
OK
DATA (D:)
Devices with Removable Storage
Page 7 / 7
Default
100%
INSRT
STD
HYP
start
8:53 AM

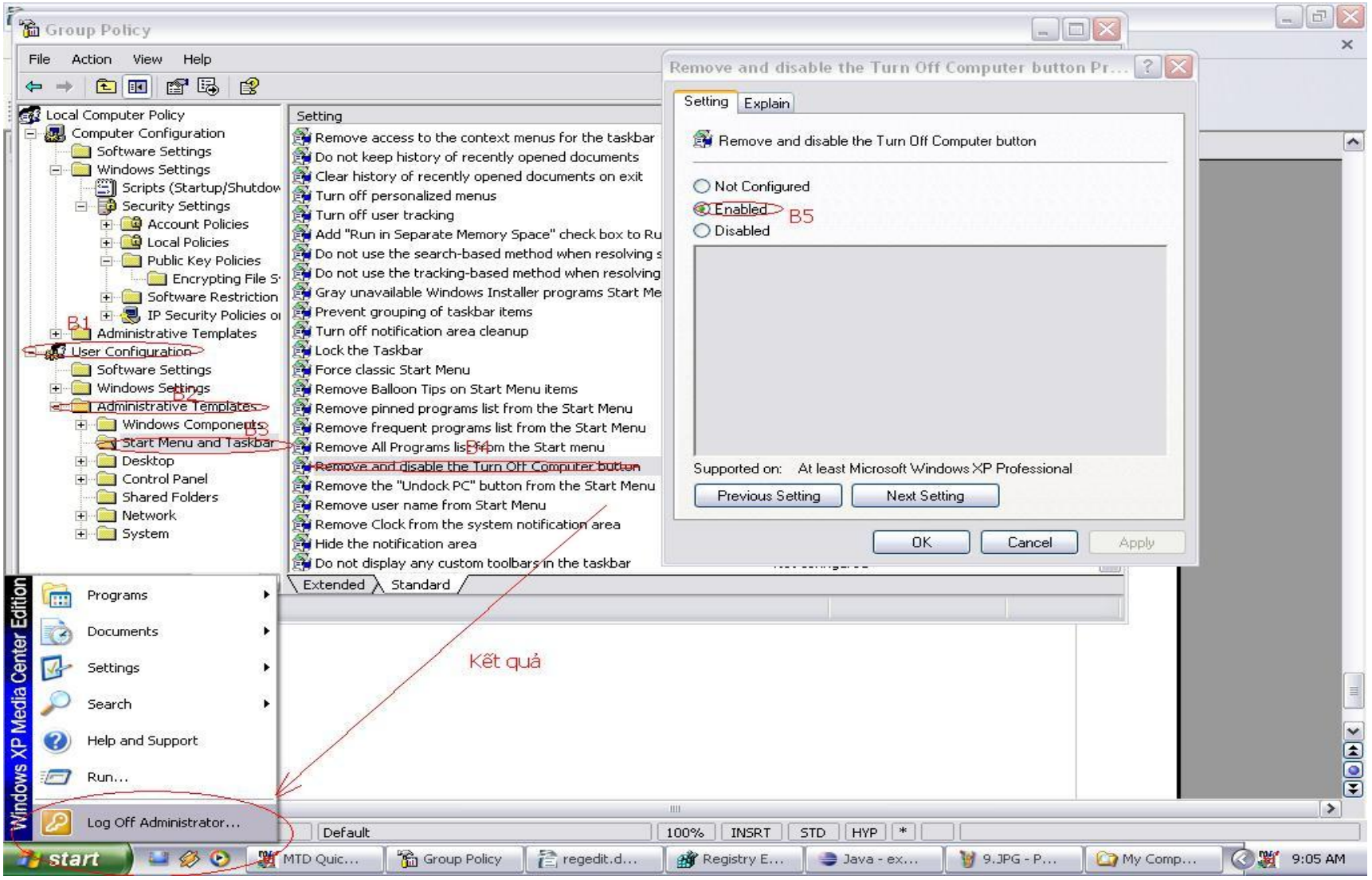
# Windows XP


Group Policy
File Action View Help
Local Computer Policy
Computer Configuration
Software Settings
Windows Settings
Administrative Templates
User Configuration
Software Settings
Windows Settings
Scripts (Logon/Logoff)
Security Settings
Internet Explorer Maint
Administrative Templates
Windows Components
NetMeeting
Internet Explorer
Application Compati
Attachment Manage
Windows Explorer
Microsoft Managem
Task Scheduler
Terminal Services
Windows Installer
Windows Messenge
Windows Update
Windows Movie Mak
Windows Media Play
Start Menu and Taskbar
Desktop
Control Panel
Shared Folders
Network
System
Windows Explorer
Hide these specified drives in My Computer
Display Properties
Requirements:
At least Microsoft Windows 2000
Description:
Removes the icons representing selected hard drives from My Computer and Windows Explorer. Also, the drive letters representing the selected drives do not appear in the standard Open dialog box.
To use this setting, select a drive or combination of drives in the drop-down list. To display all drives, disable this setting or select the "Do not restrict drives" option in the drop-down list.
Note: This setting removes the drive icons. Users can still gain access to drive contents by using other methods, such as by typing the path to a directory on the drive in the Map Network Drive dialog box, in the Run dialog box, or in a command window.
Also, this setting does not prevent users from using programs to access these drives or their contents. And, it does not prevent users from using the Disk Management snap-in to view and change drive characteristics.
Also, see the "Prevent access to drives from My Computer" setting.
Note: It is a requirement for third-party applications with Windows 2000 or later certification to adhere to this setting.
Setting
State
Common Open File Dialog
Turn on Classic Shell Not configured
Removes the Folder Options menu item from the Tools menu Not configured
Remove File menu from Windows Explorer Not configured
Remove "Map Network Drive" and "Disconnect Network Drive" Not configured
Remove Search button from Windows Explorer Not configured
Remove Windows Explorer's default context menu Not configured
Hides the Manage item on the Windows Explorer context menu Not configured
Allow only per user or approved shell extensions Not configured
Do not track Shell shortcuts during roaming Not configured
Hide these specified drives in My Computer Not configured
Prevent access to drives from My Computer Not configured
Remove Hardware tab Not configured
Remove DFS tab Not configured
Remove Security tab Not configured
Remove UI to change menu animation setting Not configured
Remove UI to change keyboard navigation indicator setting Not configured
No "Computers Near Me" in My Network Places Not configured
No "Entire Network" in My Network Places Not configured
Maximum number of recent documents Not configured
Do not request alternate credentials Not configured
Request credentials for network installations Not configured
Remove CD Burning features Not configured
Do not move deleted files to the Recycle Bin Not configured
Display confirmation dialog when deleting files Not configured
Maximum allowed Recycle Bin size Not configured
Remove Shared Documents from My Computer Not configured
Turn off caching of thumbnail pictures Not configured
Turn off Windows+X hotkeys Not configured
Turn off shell protocol protected mode Not configured
Extended Standard
Start
My Documents
Quản trị Windows XP - Mi...
Microsoft PowerPoint - [...
Group Policy
10:08 PM

# Windows XP

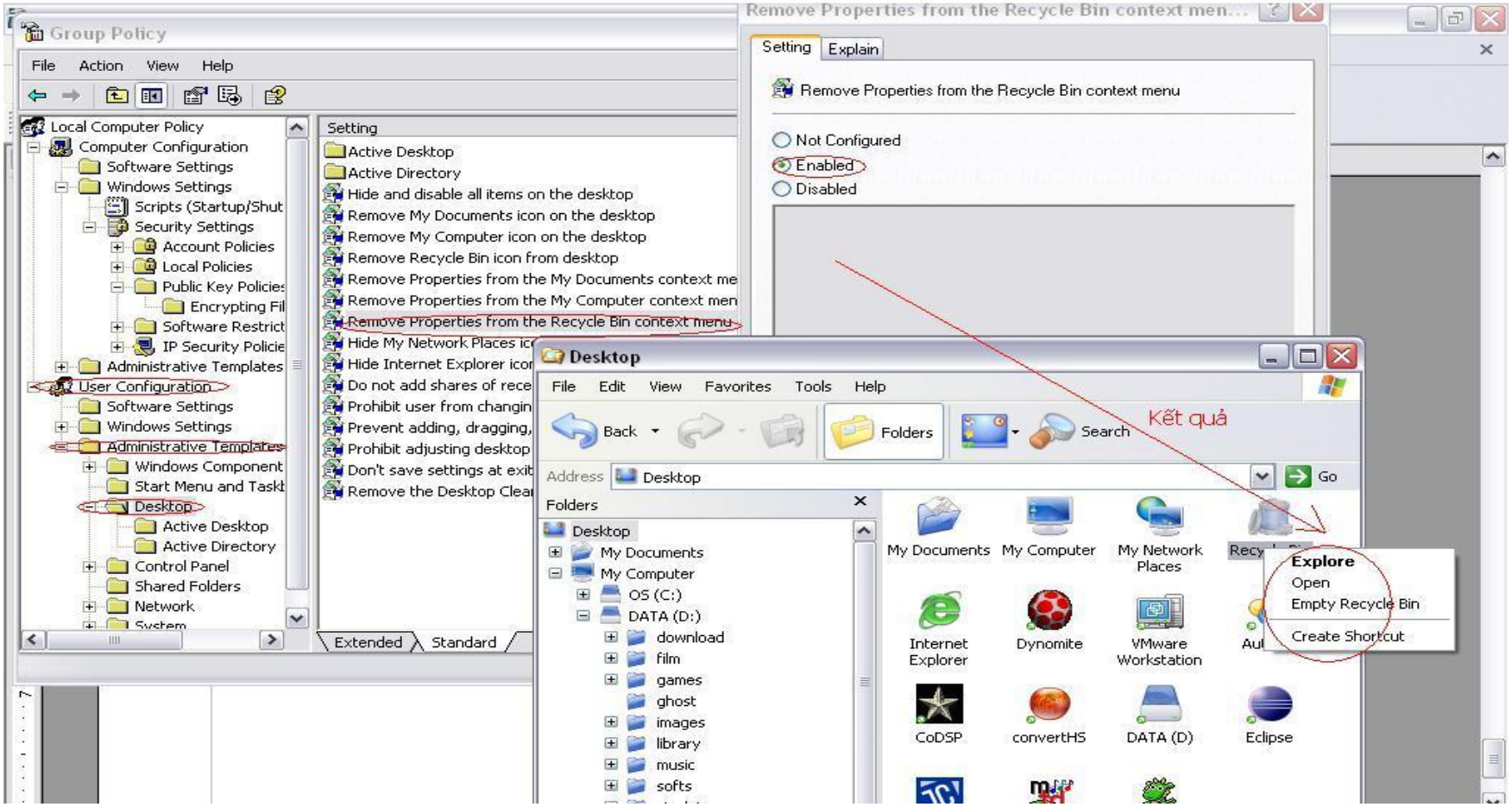
- Ex2: **Xử lý trong Start Menu và taskbar**. Một ngày buồn nào đó bạn chán muốn bỏ luôn cái nút Turn off chết tiệt thì có thể làm như sau:

# Windows XP


Group Policy
File Action View Help
Local Computer Policy
Computer Configuration
Software Settings
Windows Settings
Scripts (Startup/Shutdow
Security Settings
Account Policies
Local Policies
Public Key Policies
Encrypting File S
Software Restriction
IP Security Policies o
Administrative Templates
User Configuration
Software Settings
Windows Settings
Administrative Templates
Windows Components
Start Menu and Taskbar
Desktop
Control Panel
Shared Folders
Network
System
B1
B2
B3
B4
Setting
Remove access to the context menus for the taskbar
Do not keep history of recently opened documents
Clear history of recently opened documents on exit
Turn off personalized menus
Turn off user tracking
Add "Run in Separate Memory Space" check box to Ru
Do not use the search-based method when resolving s
Do not use the tracking-based method when resolving
Gray unavailable Windows Installer programs Start Me
Prevent grouping of taskbar items
Turn off notification area cleanup
Lock the Taskbar
Force classic Start Menu
Remove Balloon Tips on Start Menu items
Remove pinned programs list from the Start Menu
Remove frequent programs list from the Start Menu
Remove All Programs list from the Start menu
Remove and disable the Turn Off Computer button
Remove the "Undock PC" button from the Start Menu
Remove user name from Start Menu
Remove Clock from the system notification area
Hide the notification area
Do not display any custom toolbars in the taskbar
Extended Standard
Remove and disable the Turn Off Computer button Pr...
Setting Explain
Remove and disable the Turn Off Computer button
Not Configured
Enabled
Disabled
B5
Supported on: At least Microsoft Windows XP Professional
Previous Setting
Next Setting
OK
Cancel
Apply
Kết quả
Windows XP Media Center Edition
Programs
Documents
Settings
Search
Help and Support
Run...
Log Off Administrator...
Default
100%
INSRT
STD
HYP
start
MTD Quic...
Group Policy
regedit.d...
Registry E...
Java - ex...
9.JPG - P...
My Comp...
9:05 AM

# Windows XP

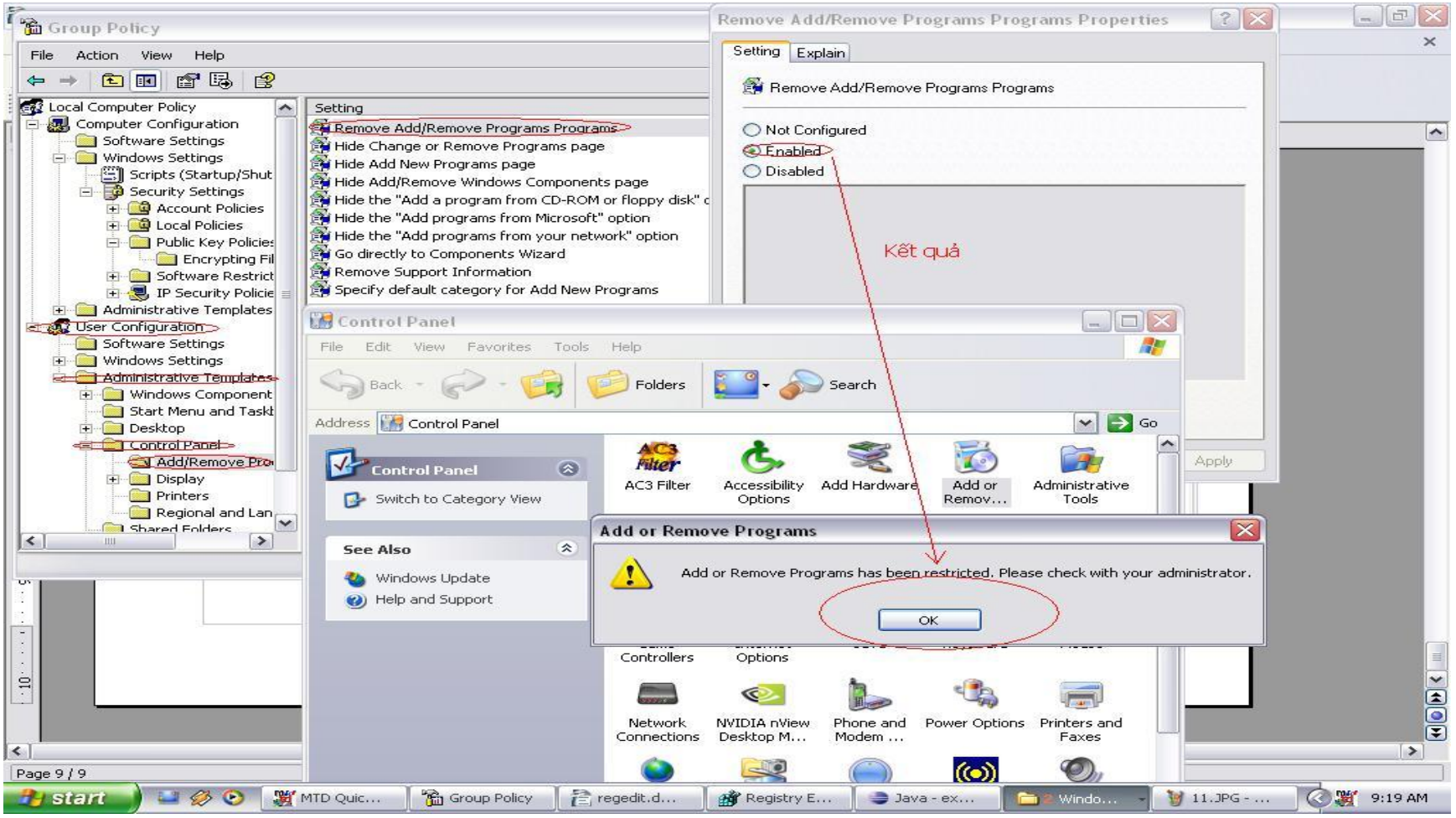
- Ex3: **Xử lý trong Desktop**. Loại bỏ property của Recycle Bin


Group Policy
File Action View Help
Local Computer Policy
Computer Configuration
Software Settings
Windows Settings
Scripts (Startup/Shut
Security Settings
Account Policies
Local Policies
Public Key Policies
Encrypting Fil
Software Restrict
IP Security Policie
Administrative Templates
User Configuration
Software Settings
Windows Settings
Administrative Templates
Windows Component
Start Menu and Taskb
Desktop
Active Desktop
Active Directory
Control Panel
Shared Folders
Network
System
Setting
Active Desktop
Active Directory
Hide and disable all items on the desktop
Remove My Documents icon on the desktop
Remove My Computer icon on the desktop
Remove Recycle Bin icon from desktop
Remove Properties from the My Documents context me
Remove Properties from the My Computer context men
Remove Properties from the Recycle Bin context menu
Hide My Network Places ic
Hide Internet Explorer icon
Do not add shares of rece
Prohibit user from changin
Prevent adding, dragging,
Prohibit adjusting desktop
Don't save settings at exit
Remove the Desktop Clear
Extended Standard
Remove Properties from the Recycle Bin context men...
Setting Explain
Remove Properties from the Recycle Bin context menu
Not Configured
Enabled
Disabled
Desktop
File Edit View Favorites Tools Help
Back Folders Search
Kết quả
Address Desktop
Go
Folders
Desktop
My Documents
My Computer
OS (C:)
DATA (D:)
download
film
games
ghost
images
library
music
softs
My Documents
My Computer
My Network Places
Internet Explorer
Dynomite
VMware Workstation
CoDSP
convertHS
DATA (D)
Eclipse
Explore
Open
Empty Recycle Bin
Create Shortcut

# Windows XP

- Ex4: **Xử lý Control Pannel**. Cấm truy xuất add/remove program

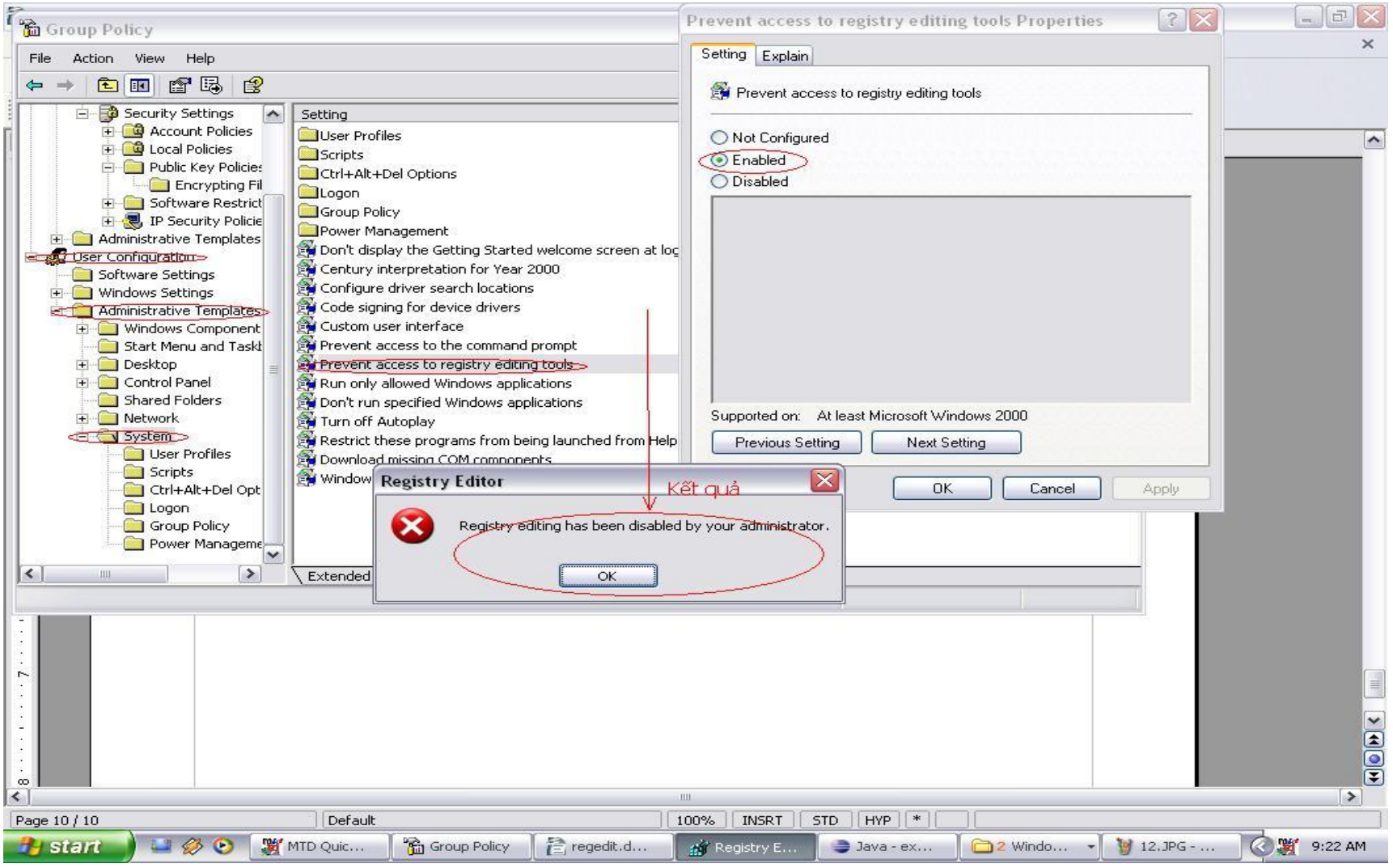
# Windows XP


Group Policy
File Action View Help
Local Computer Policy
Computer Configuration
Software Settings
Windows Settings
Administrative Templates
User Configuration
Software Settings
Windows Settings
Administrative Templates
Control Panel
Setting
Remove Add/Remove Programs Programs
Hide Change or Remove Programs page
Hide Add New Programs page
Hide Add/Remove Windows Components page
Hide the "Add programs from Microsoft" option
Hide the "Add programs from your network" option
Go directly to Components Wizard
Remove Support Information
Specify default category for Add New Programs
Remove Add/Remove Programs Programs Properties
Setting
Explain
Remove Add/Remove Programs Programs
Not Configured
Enabled
Disabled
Kết quả
Apply
Control Panel
File Edit View Favorites Tools Help
Back
Folders
Search
Address Control Panel
Go
Control Panel
Switch to Category View
See Also
Windows Update
Help and Support
AC3 Filter
Accessibility Options
Add Hardware
Add or Remov...
Administrative Tools
Add or Remove Programs
Add or Remove Programs has been restricted. Please check with your administrator.
OK
Controllers
Options
Network Connections
NVIDIA nView Desktop M...
Phone and Modem ...
Power Options
Printers and Faxes
Page 9 / 9
start
MTD Quic...
Group Policy
regedit.d...
Registry E...
Java - ex...
Windo...
11.JPG - ...
9:19 AM

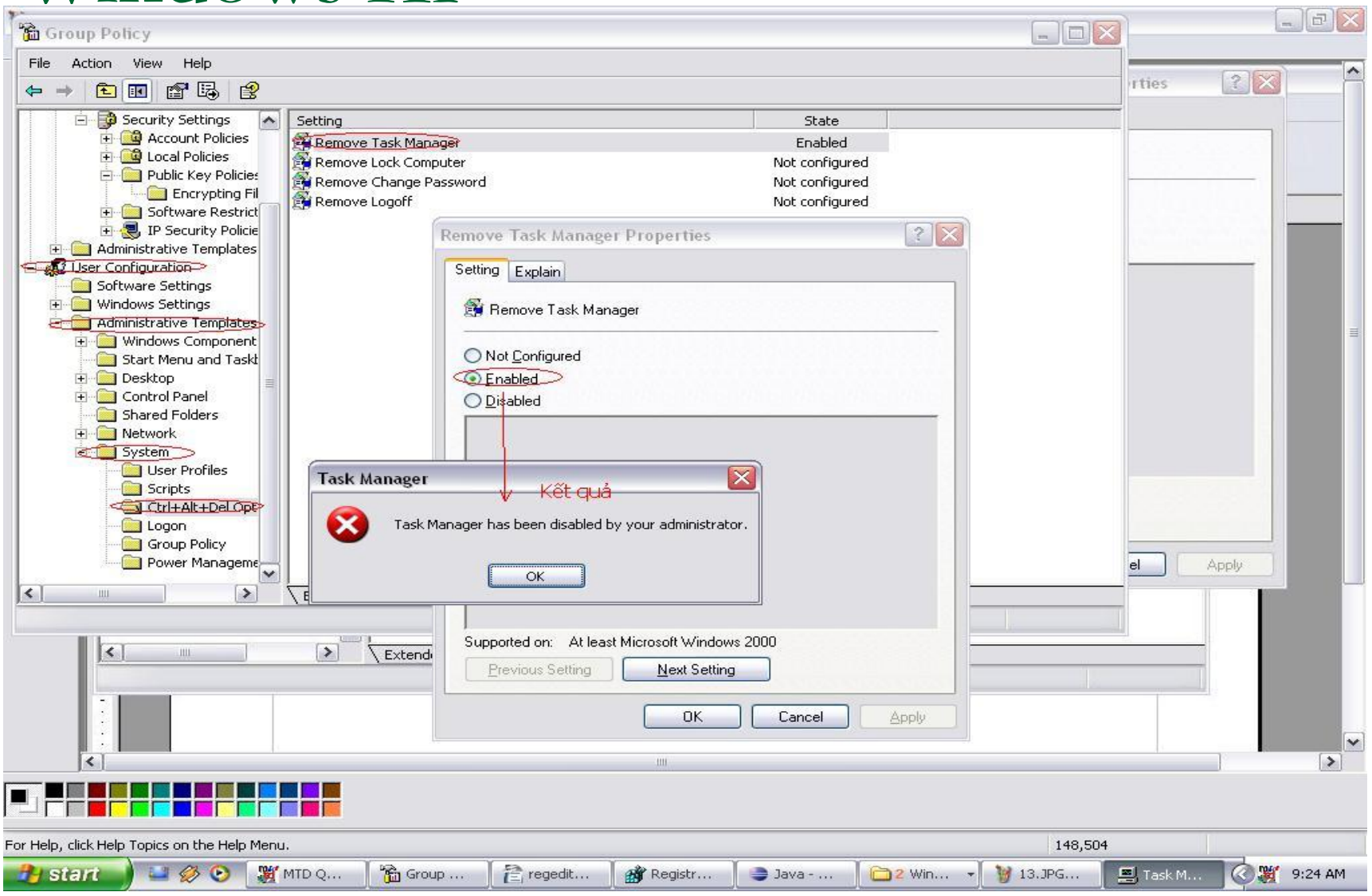
# Windows XP

- Ex5: **Xử lý trong system**. Lock registry, lock task manager, Lock registry

# Windows XP


Group Policy
File Action View Help
Security Settings
Account Policies
Local Policies
Public Key Policies
Encrypting Fil
Software Restrict
IP Security Policie
Administrative Templates
User Configuration
Software Settings
Windows Settings
Administrative Templates
Windows Component
Start Menu and Taskb
Desktop
Control Panel
Shared Folders
Network
System
User Profiles
Scripts
Ctrl+Alt+Del Opt
Logon
Group Policy
Power Manageme
Setting
User Profiles
Scripts
Ctrl+Alt+Del Options
Logon
Group Policy
Power Management
Don't display the Getting Started welcome screen at log
Century interpretation for Year 2000
Configure driver search locations
Code signing for device drivers
Custom user interface
Prevent access to the command prompt
Prevent access to registry editing tools
Run only allowed Windows applications
Don't run specified Windows applications
Turn off Autoplay
Restrict these programs from being launched from Help
Download missing COM components
Extended
Prevent access to registry editing tools Properties
Setting
Explain
Prevent access to registry editing tools
Not Configured
Enabled
Disabled
Supported on: At least Microsoft Windows 2000
Previous Setting
Next Setting
OK
Cancel
Apply
Registry Editor
Kết quả
Registry editing has been disabled by your administrator.
OK
Page 10 / 10
Default
100%
INSRT
STD
HYP
start
MTD Quic...
Group Policy
regedit.d...
Registry E...
Java - ex...
2 Windo...
12.JPG - ...
9:22 AM

# Windows XP


Group Policy
File Action View Help
Security Settings
Account Policies
Local Policies
Public Key Policies
Encrypting Fil
Software Restrict
IP Security Policie
Administrative Templates
User Configuration
Software Settings
Windows Settings
Administrative Templates
Windows Component
Start Menu and Taskb
Desktop
Control Panel
Shared Folders
Network
System
User Profiles
Scripts
Ctrl+Alt+Del Ope
Logon
Group Policy
Power Manageme
Setting
State
Remove Task Manager
Enabled
Remove Lock Computer
Not configured
Remove Change Password
Not configured
Remove Logoff
Not configured
Remove Task Manager Properties
Setting
Explain
Remove Task Manager
Not Configured
Enabled
Disabled
Supported on: At least Microsoft Windows 2000
Previous Setting
Next Setting
OK
Cancel
Apply
Task Manager
Kết quả
Task Manager has been disabled by your administrator.
OK
For Help, click Help Topics on the Help Menu.
148,504
start
MTD Q...
Group ...
regedit...
Registr...
Java - ...
2 Win...
13.JPG...
Task M...
9:24 AM

# HỆ ĐIỀU HÀNH MẠNG

## Cài đặt HĐH Windows Server 2003 & DHCP

# Windows Server 2003

- Hướng dẫn chi tiết cài đặt mới Windows 2003 Server cũng như nâng cấp lên từ các phiên bản cũ hơn. Cũng trong chương này bạn sẽ thực hành cài đặt cấu hình TCP/IP và các lệnh cơ bản để kiểm tra mạng. Cuối cùng hướng dẫn bạn thực hành duyệt qua các máy trong mạng sử dụng My Network Places.

# Windows Server 2003

- Trong mô hình mạng bạn có thể chọn cài đặt HĐH Windows 2000 Server hoặc Windows Server 2003 cho máy chủ và Windows 2000 hoặc Windows XP cho máy khách. Việc quyết định chọn HĐH nào để cài đặt tuỳ theo điều kiện thực tế của bạn, còn các bước thực hiện thì về cơ bản không khác nhau nhiều lắm.

# Windows Server 2003

- **CHUẨN BỊ**
  Trong mô hình này tôi chọn cài đặt HĐH Windows Server 2003 và Windows XP. Trước khi bắt tay vào việc bạn cần chuẩn bị :
- 2 máy tính có cấu hình phù hợp, một làm máy chủ và một làm máy trạm có nối mạng với nhau.
- 02 bộ đĩa cài đặt cho 02 HĐH này. Bạn có thể liên hệ với văn phòng Microsoft Việt Nam để được cung cấp phiên bản chính thức.

# Windows Server 2003

- **TRÌNH TỰ THỰC HIỆN**
  Trong mô hình này, chúng tôi chọn cài đặt HĐH Windows Server 2003 cho máy chủ và Windows XP cho máy khách. Trước khi bắt tay vào việc bạn cần chuẩn bị:
- 2 máy tính có cấu hình phù hợp (đã nêu trong Phần 1), một làm máy chủ và một làm máy trạm có nối mạng với nhau.
- 02 bộ đĩa cài đặt cho 02 HĐH này. Bạn liên hệ với văn phòng Microsoft Việt Nam hoặc các nhà phân phối ủy quyền để mua bản quyền.

- Trình tự thực hiện cài đặt mạng như sau:
- **Máy chủ**
  • Cài đặt HĐH Windows Server 2003
  • Cài đặt dịch vụ DHCP
- Máy trạm
  • Cài đặt HĐH Windows XP
  • Cài đặt các ứng dụng (tuỳ theo nhu cầu sử dụng của bạn)

# Windows Server 2003

- **Các yêu cầu chuẩn bị trước khi cài đặt**
- Yêu cầu cho máy cài đặt Windows2000 Server dùng cho mục đích thực tập thì chỉ cần là máy Pentium III, tốc độ 1.2 GHz, RAM 256, ổ cứng còn trống khoảng 2 GB là đủ. Trong thực tế sử dụng cần những máy tính chuyên nghiệp có thể hoạt động 24/24 giờ mỗi ngày, có khả năng thay ổ đĩa cúng khi đang hoạt động và đầy đủ tiện ích sao chép dự phòng dữ liệu.

# Windows Server 2003

- Định dạng hệ thống
- Nếu bạn cài đặt Win2kServer lên một phần chưa định dạng của ổ đĩa, bạn sẽ được yêu cầu chọn loại hệ thống định dạng. Windows 2000 hỗ trợ các loại định dạng hệ thống bao gồm NTFS và FAT .
- NTFS
- NTFS là loại định dạng hệ thống được hỗ trợ bởi Windows2000 và WindowsNT. Nó có tất cả các tính năng của FAT, cộng thêm các tính năng khác như security, compression và khả năng mở rộng partition. Version mới nhất của NTFS là NTFS 5.0 được cung cấp kèm với các CD cài đặt Windows 2000.

# Windows Server 2003

- FAT16 and FAT32
- FAT16 và FAT32 là loại định dạng hệ thống trên Windows 9x. Nó không có những tính năng mà NTFS hỗ trợ, tuy nhiên nếu bạn muốn partition của bạn được nhìn thấy bởi các hệ điều hành khác ngoài Windows2000 và WindowsNT thì bạn phải định dạng ổ đĩa theo FAT.
- Một vài điểm lưu ý
- Bạn có thể sử dụng một partition đã tồn tại hay khởi tạo một partition mới khi cài đặt hệ điều hành.
- Bạn có thể chuyển một partition định dạng FAT sang NTFS, nhưng không thể chuyển ngược lại.

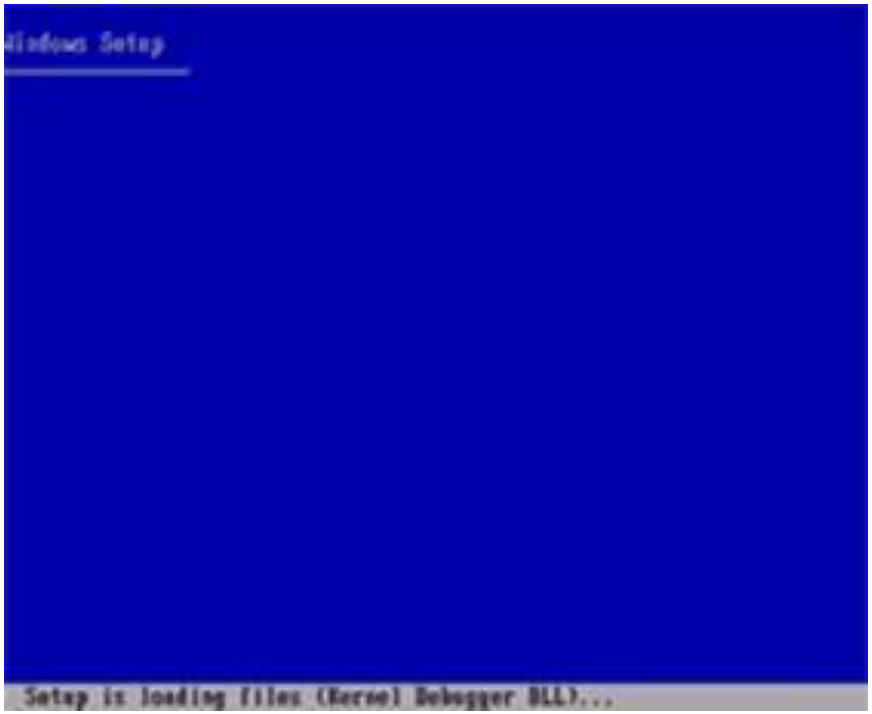
# Windows Server 2003

- Bạn có thể định dạng lại cho một partition đang tồn tại theo dạng FAT hay NTFS, nhưng tất cả các thông tin trên đó sẽ mất.
- Bạn nên chọn FAT nếu bạn muốn có cài đặt hệ điều hành kép gồm Windows 2000 và  Window9x trên cùng một máy tính.
- Bạn nên chọn NTFS nếu bạn cài đặt Windows 2000 Server để sử dụng các điểm ưu việt của NTFS.

# 1. Cài HĐH Windows Sever 2003

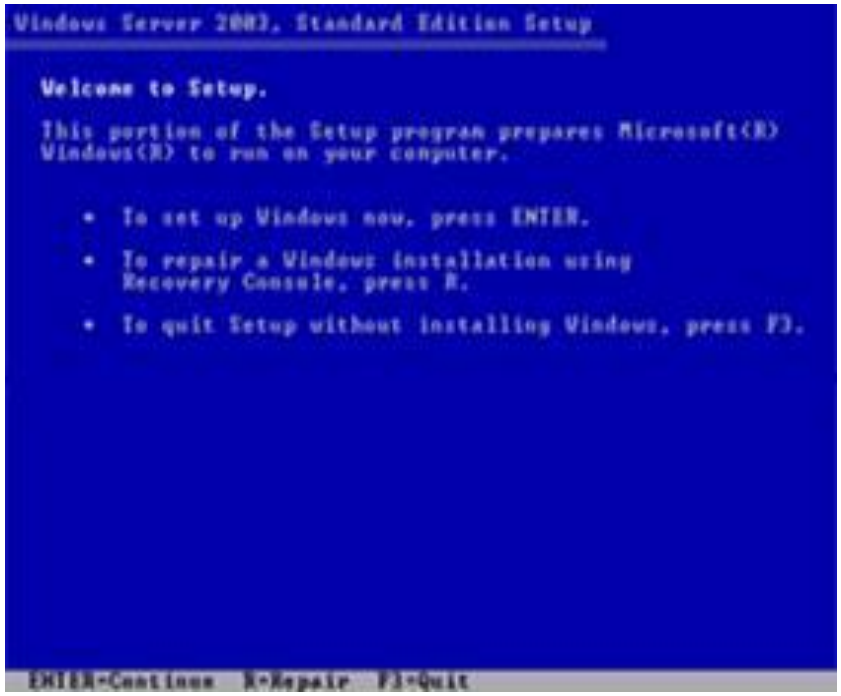
- Thiết lập trong BIOS Setup để máy tính khởi động đầu tiên từ CDROM. Đưa đĩa cài đặt Windows Servrer 2003 vào ổ CDROM, cho máy tính khởi động lại, máy tính sẽ tự động khởi động chương trình cài đặt từ đĩa cài đặt trong ổ CDROM.
- **Giai đoạn 01**:
  Chương trình cài đặt kiểm tra cấu hình máy tính và bắt đầu cài đặt HĐH ở chế độ tex (tex mode):

# § Giai đoạn 01:




- Chương trình cài đặt lần lượt nạp chương trình thực thi, các phần mềm hỗ trợ, các trình điều khiển thiết bị, các tập tin chương trình cài đặt.

# § Giai đoạn 01:

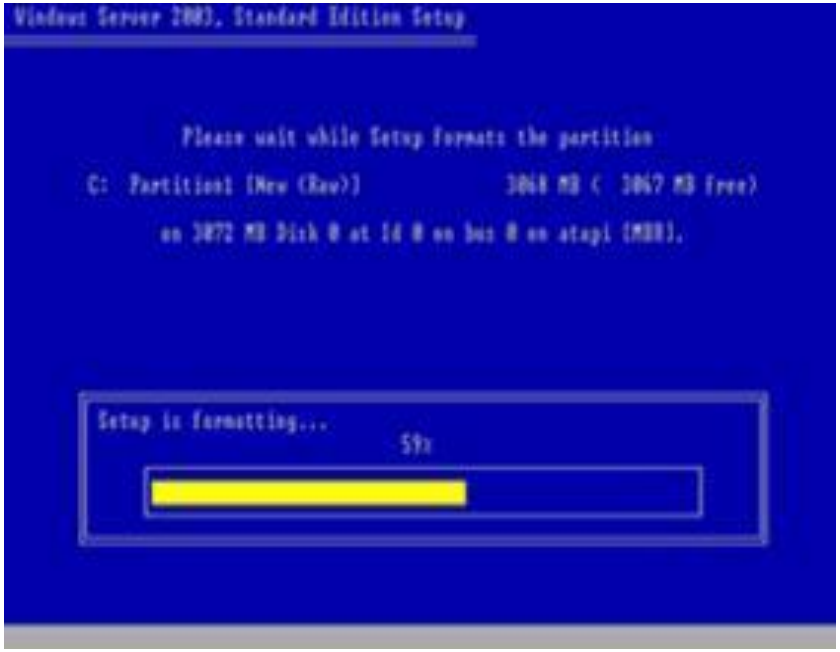



- Cửa sổ lựa chọn cài đặt: Nhấn Enter để cài đặt Windows, R để sửa chữa phiên bản đã cài đặt, F3 để hủy bỏ việc cài đặt.

# § Giai đoạn 01:

- Chọn không gian đĩa cài đặt: Tại hộp sáng, nhấn Enter để chọn toàn bộ vùng đĩa hoặc nhấn C để chia vùng đĩa này thành nhiều phân vùng nhỏ hơn.

# § Giai đoạn 01:




- Chương trình cài đặt đang định dạng

# § Giai đoạn 01:

- Một phân vùng mới đã được tạo và đòi hỏi phải được định dạng. Chọn mục thứ 3 để định dạng sử dụng hệ thống file NTFS

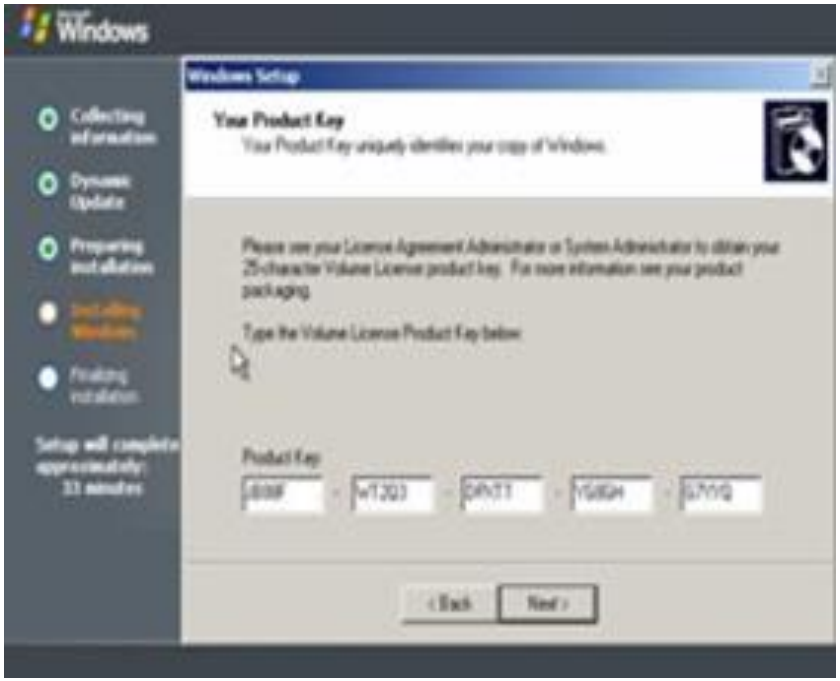
# § Giai đoạn 01:

- Sau khi định dạng xong, chương trình kiểm tra lỗi vật lý ổ cứng và chép các tập tin cần thiết vào ổ cứng

# 1. Cài HĐH Windows Sever 2003

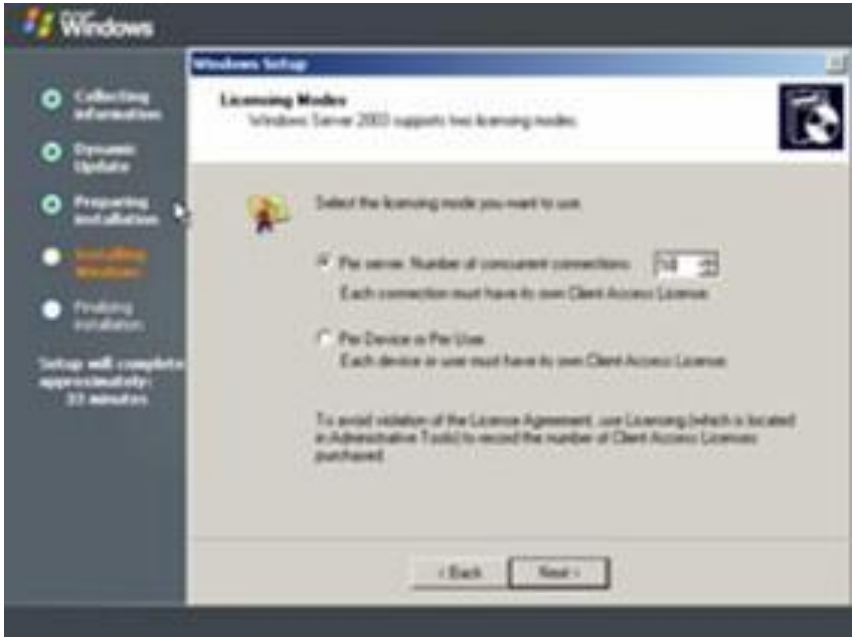
- **Giai đoạn 02**: Chương trình sẽ bắt đầu tiến trình cài đặt dưới giao diện đồ họa, ở giai đoạn này ta lần lượt đi theo các bước hướng dẫn và cung cấp thêm vài thông tin cần thiết cho trình cài đặt

# § Giai đoạn 02:



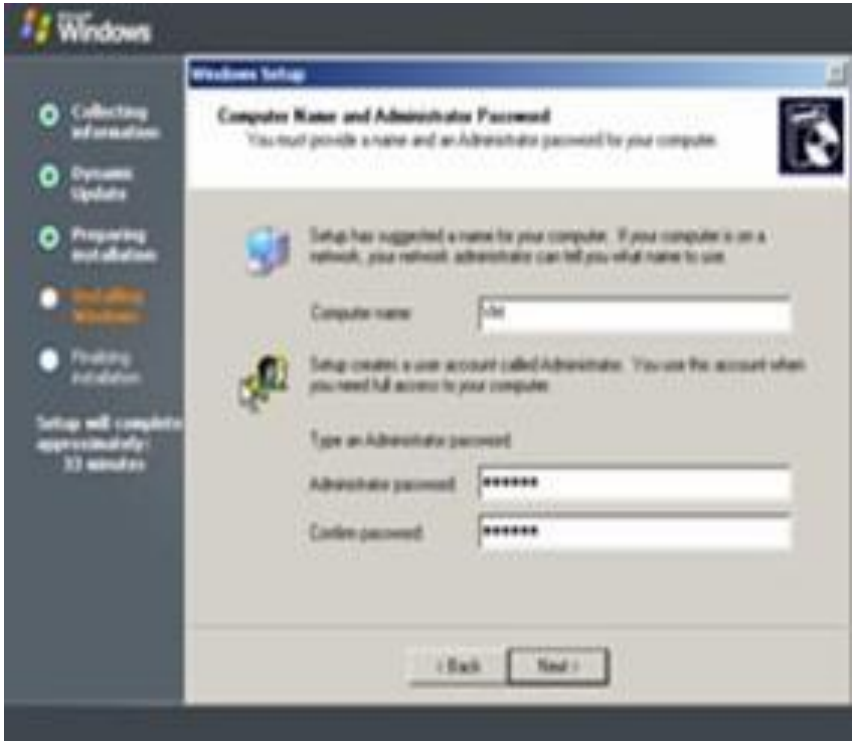

- Bạn cần phải mua bản quyền để được cấp một dãy số riêng và nhập vào các ô trong mục Product Key.

# § Giai đoạn 02:



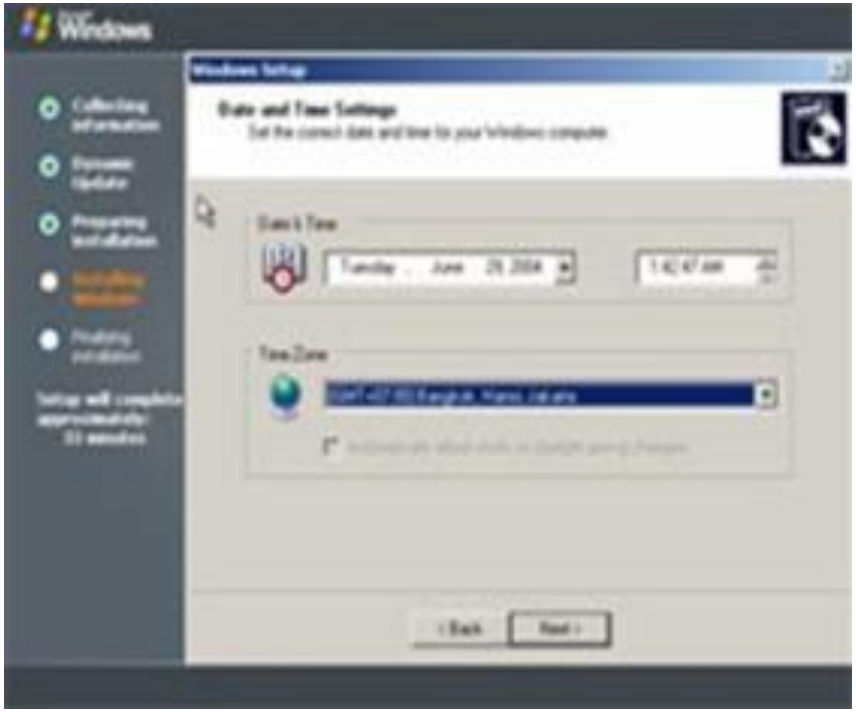

- Tuỳ theo bản quyền bạn mua ở chế độ nào mà bạn khai báo ở mục Per server hay Per Device or Per User tương ứng

# § Giai đoạn 02:




- Đặt tên cho máy tính và khai báomật khẩu cho tài khoản quản trị cao nhất Administrator

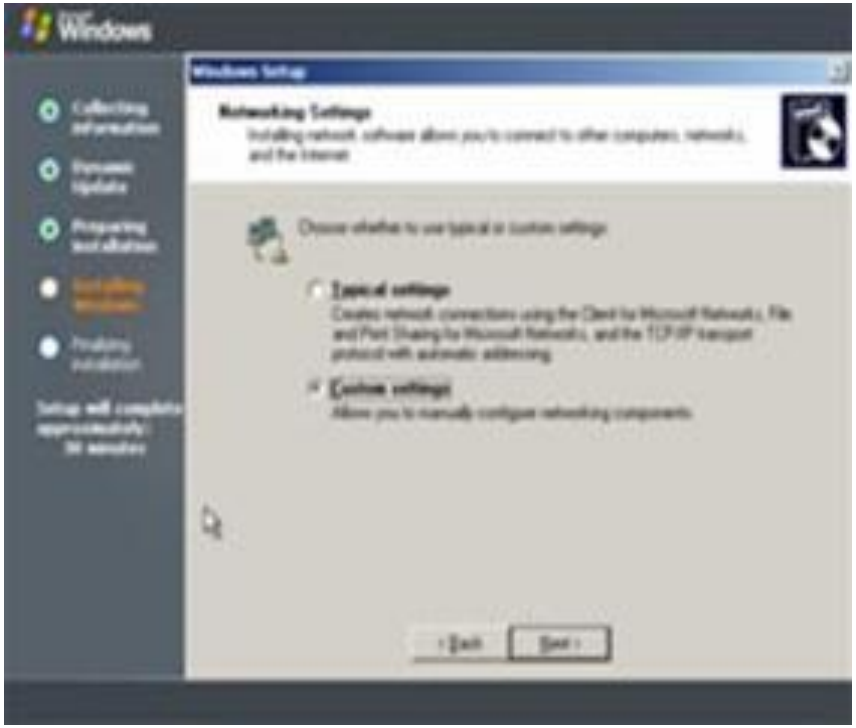
# § Giai đoạn 02:



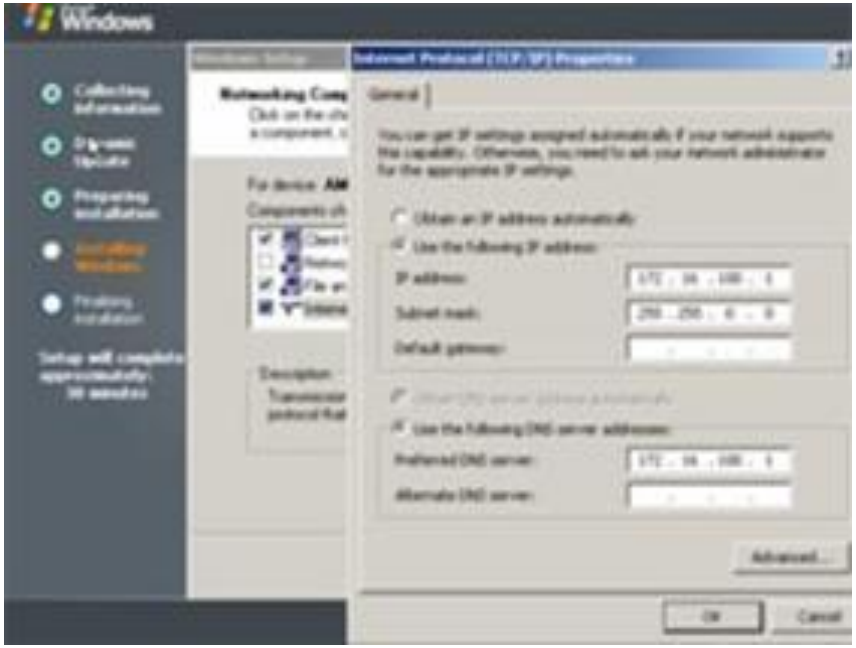

- Khai báo thời gian và lựa chọn múi giờ chính xác

# § Giai đoạn 02:

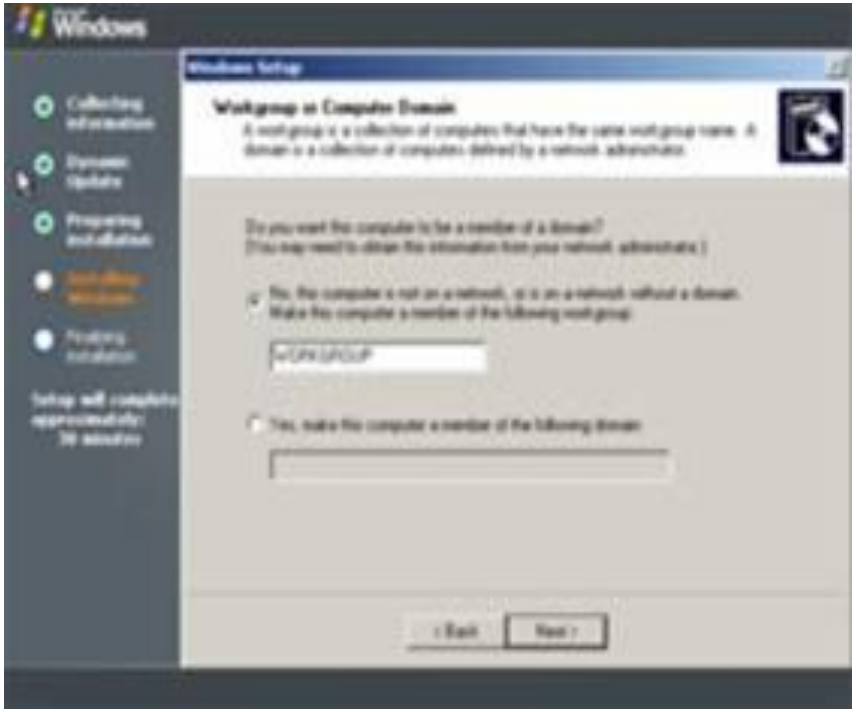
- Cài đặt các thành phần mạng




- Chọn kiểu thiết lập cấu hình bằng tay



- Khai báo địa chỉ IP cho card mạng




- Mặc định xem máy tính này như một thành viên của workgroup có tên là WORKGROUP

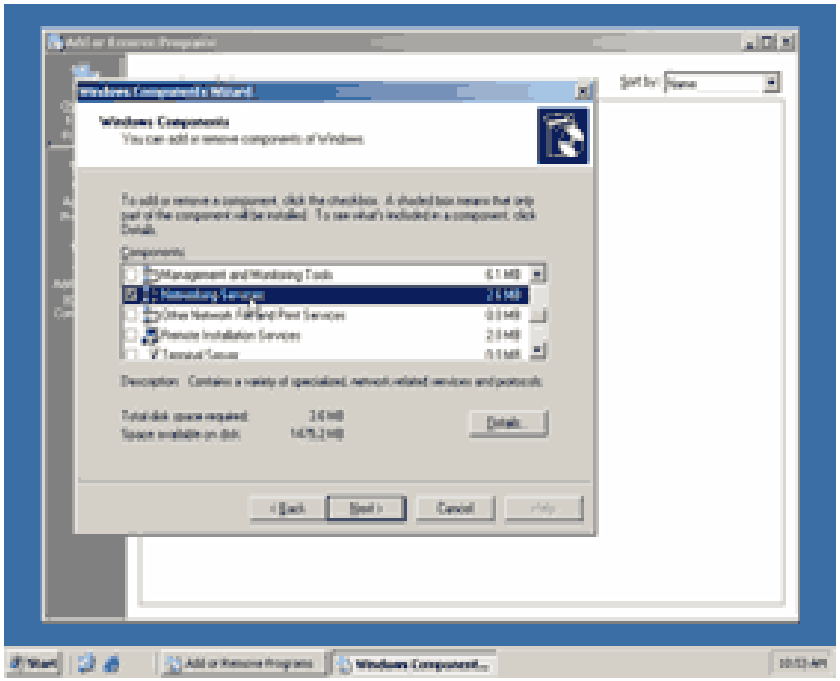
- Cài đặt các dịch vụ Web

- Hoàn tất quá trình cài đặt và khởi động máy

# 2. Cài đặt và cấu hình dịch vụ DHCP

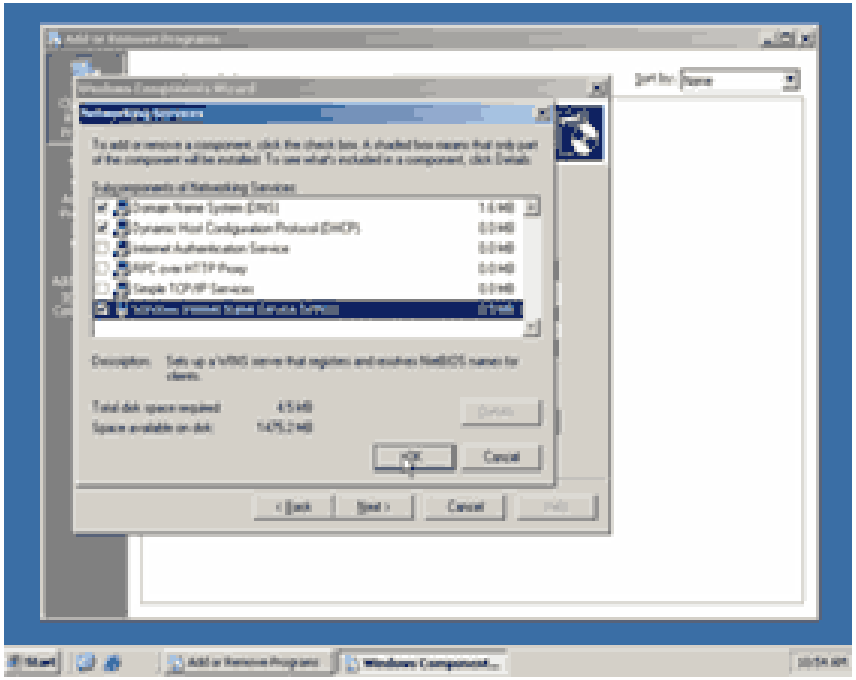
***Cài đặt***: Các máy khách sẽ nhận địa chỉ IP một cách tự động từ dịch vụ cấp phát địa chỉ động DHCP. Dịch vụ này được cài đặt trên máy chủ như sau:

# DHCP




- Trong Contral Panel, nhấn đúp biểu tượng Add or Remove Programs. Trong cửa sổ vừa mở, chọn mục Add/Remove Windows Components. Cửa sổ Windows Components Wizard xuất hiện.

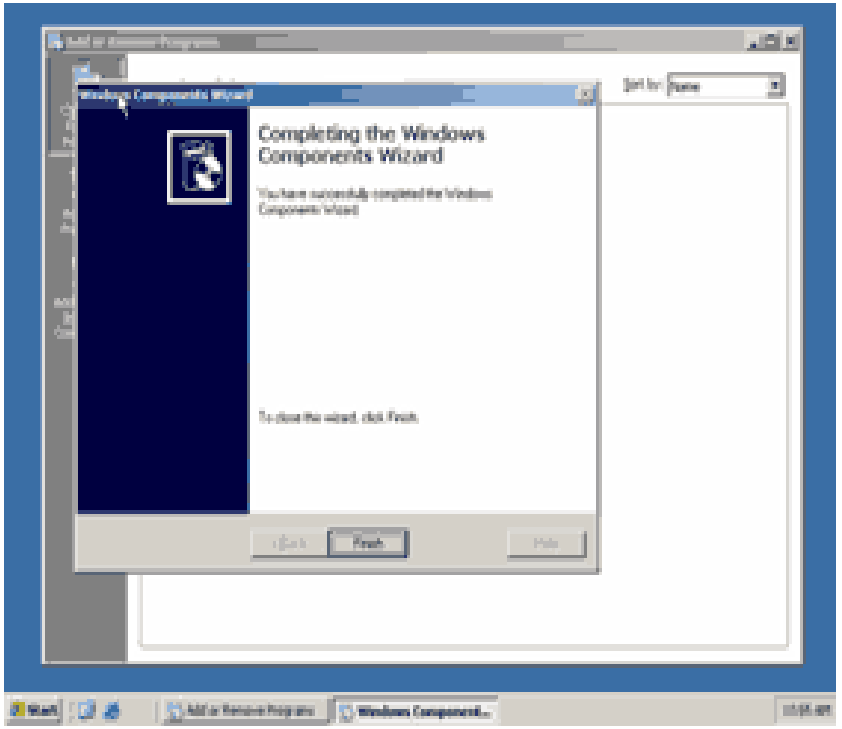
# DHCP



- Đưa hộp sáng đến mục Network Services và nhấn nút Details để làm xuất hiện cửa sổ Network Services. Trong cửa sổ này đánh dấu chọn vào mục Dynamic Host Configuration Protocol (DHCP) và nhấn OK.

# . DHCP

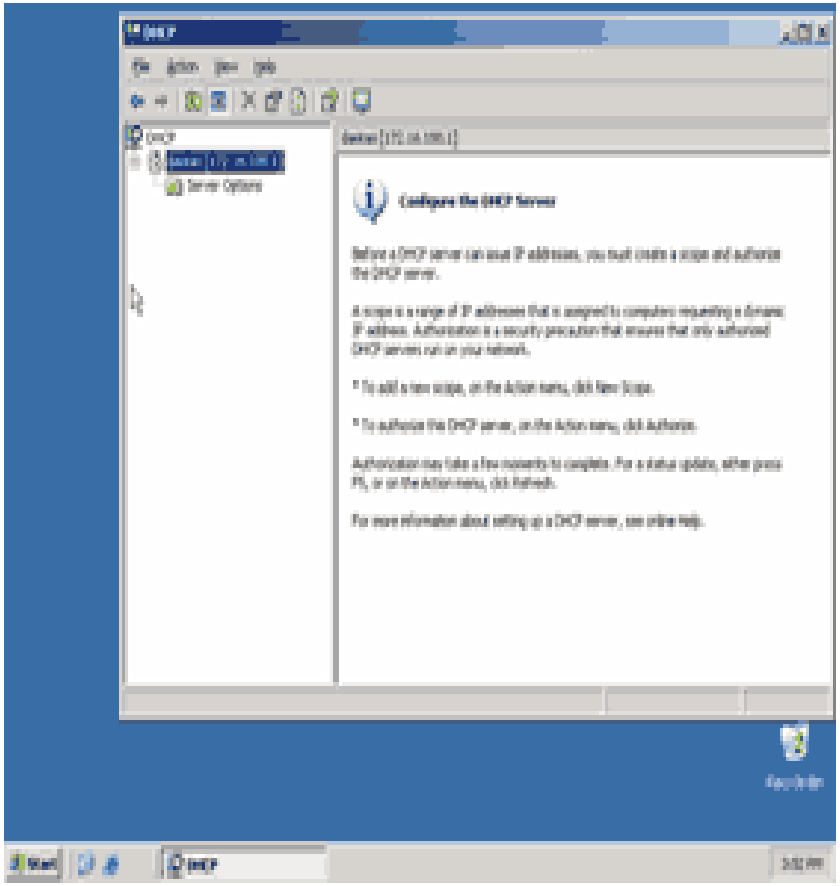
- Tiến trình cài đặt sẽ diễn ra cho đến khi bạn nhấn Finish để hoàn tất



# DHCP

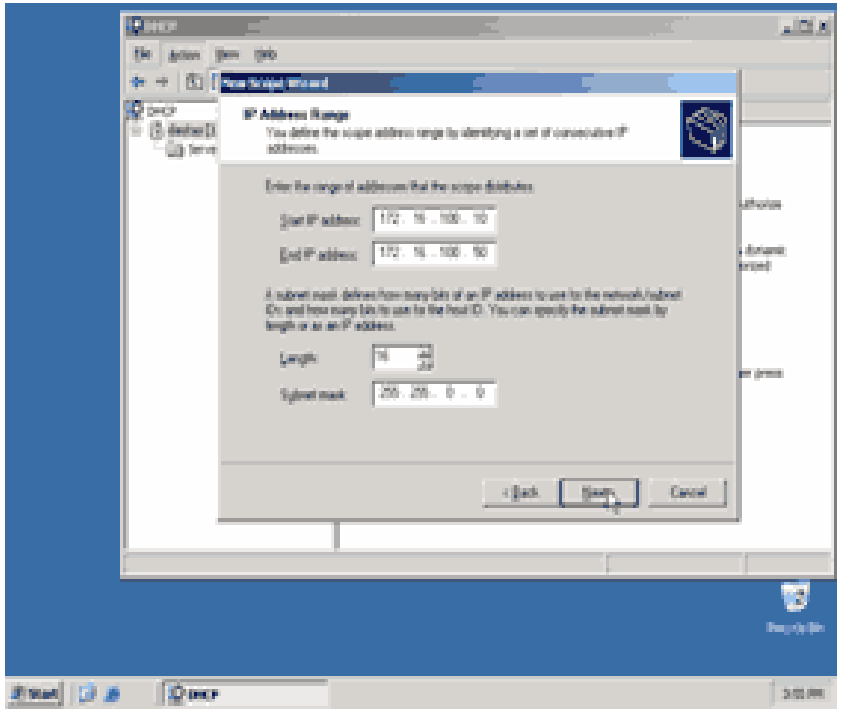
- ***Cấu hình***: Để dịch vụ DHCP có thể cấp phát được địa chỉ IP chúng ta cần cấu hình và kích hoạt dịch vụ này.

# DHCP



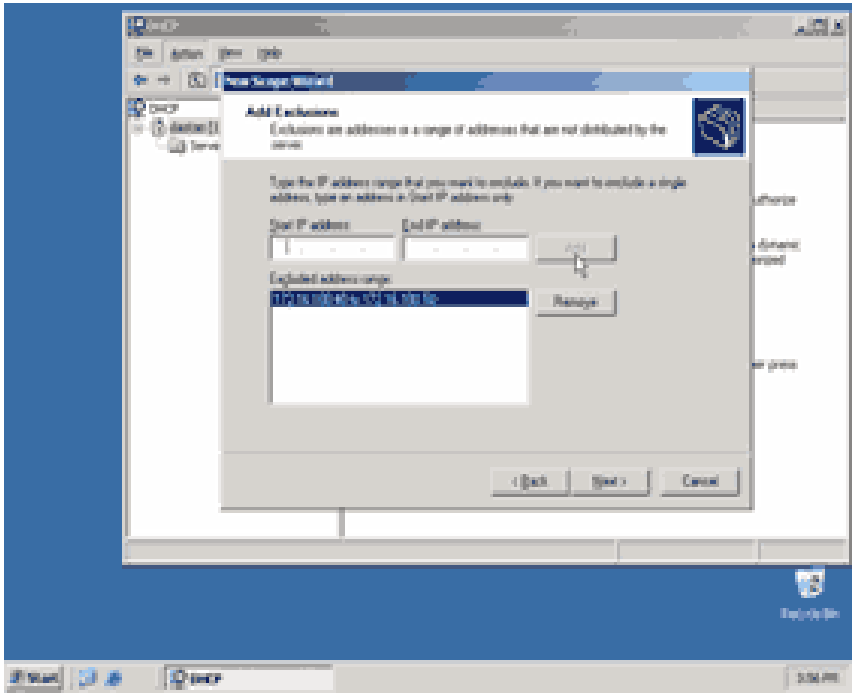
- Đầu tiên cần tạo ra một dãy địa chỉ cần cấp phát (scope): Chọn tên máy (daotao [172.16.100.1]), sau đó mở menu Action và chọn New Scope.

# DHCP



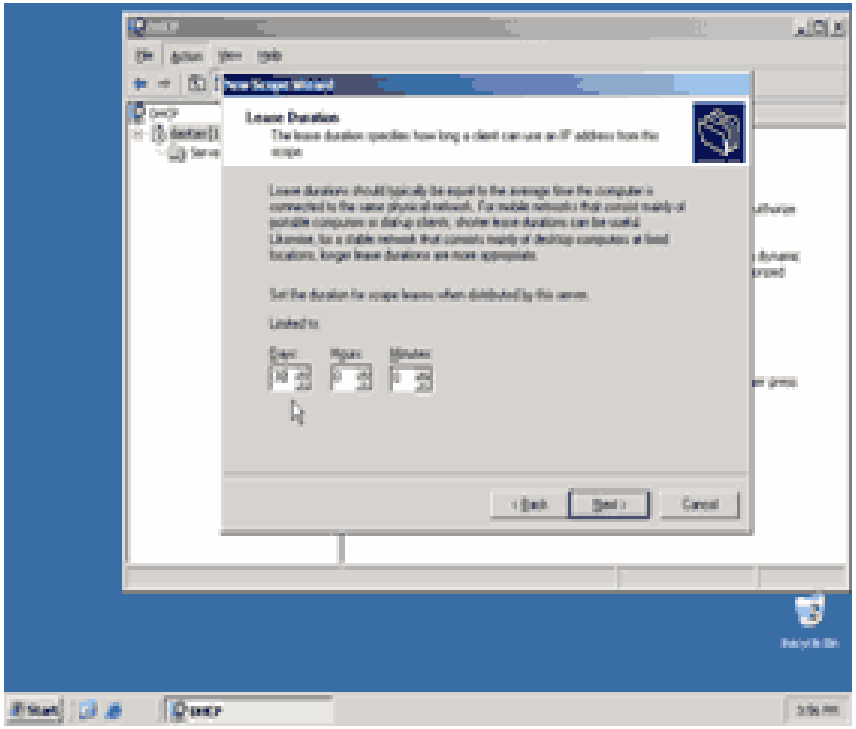

- Xác định địa chỉ IP bắt đầu (Start IP adress: 172.16.100.10) và kết thúc (End IP adress: 172.16.100.50) của scope

# DHCP



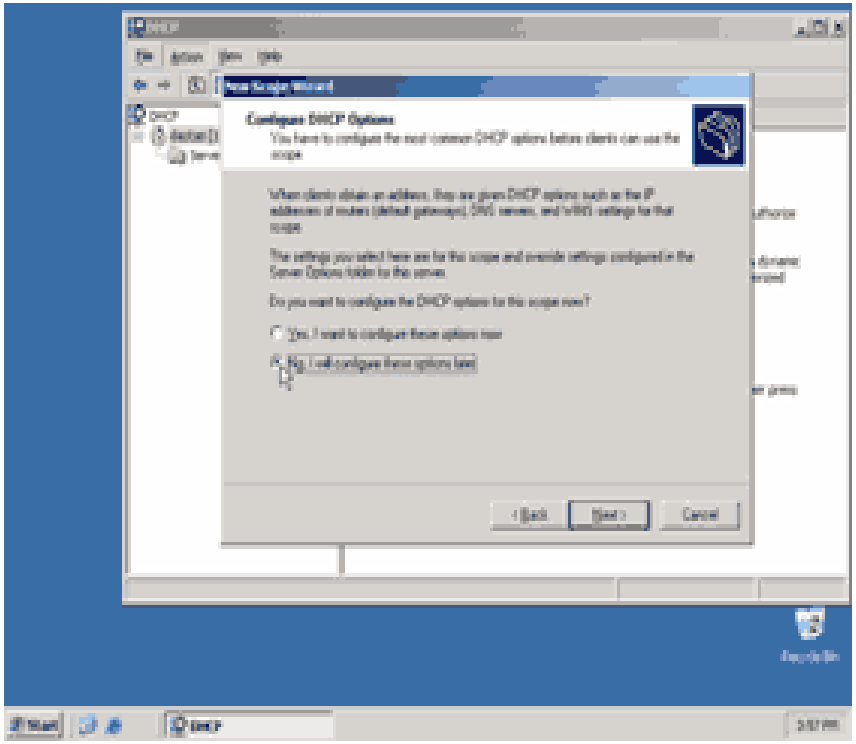
- Loại trừ ra một vùng địa chỉ IP không cấp phát.

# DHCP



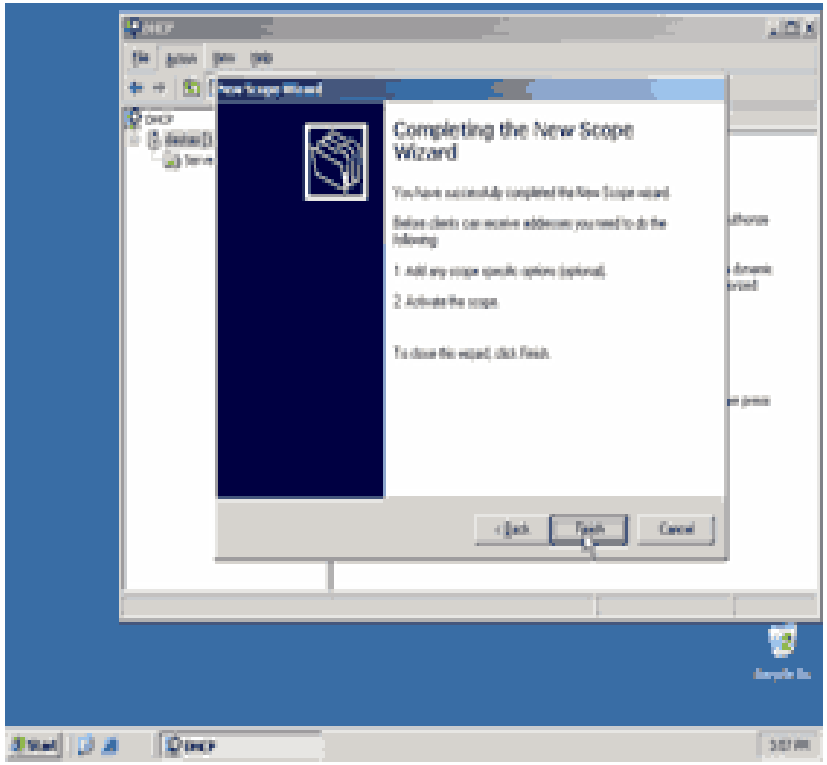

- Xác định thời hạn sử dụng địa chỉ IP mà máy khách nhận từ dich vụ DHCP

# DHCP



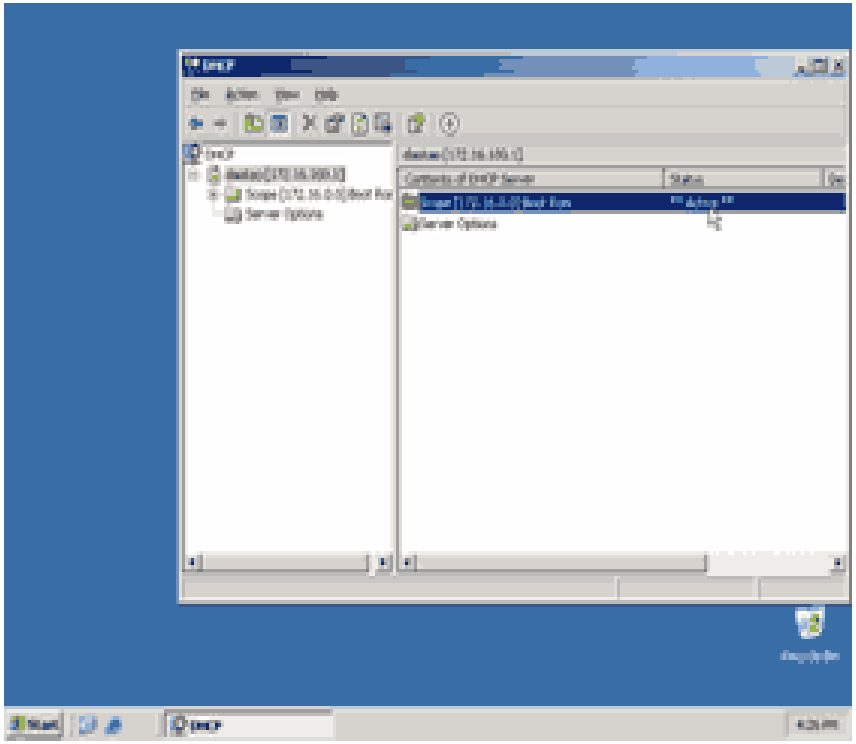

- Tại đây bạn có thể cấu hình thêm các thông số để cấp phát cho máy khách cùng với địa chỉ IP; hoặc chọn No để cấu hình sau.

# DHCP




- Cuối cùng, cửa sổ thông báo hoàn thành xuất hiện, nhắc nhở bạn cần phải kích hoạt scope vừa tạo. Nhấn Finish

# DHCP



- Để kích hoạt scope vừa tạo, chọn vào mục có tên scope đó (Scope [172.16.0.0] Boot Rom). Sau đó mở menu Action và chọn Active.

# HỆ ĐIỀU HÀNH MẠNG

Cài đặt và quản trị WINDOWS 2003 Domain Controller

# Domain Controller

- Mục đích của chương này nhằm giới thiệu về DNS (Domain Name System) dịch vụ tổ chức các máy tính thành vùng có cấu trúc phân cấp và AD (Active Directory) dịch vụ thư mục cho phép quản lý tài nguyên mạng hiệu quả.

# Dịch vụ tên miền DNS

- **Giới thiệu DNS**
- **DNS** (**Domain Name System**) là giải pháp dùng tên thay cho địa chỉ IP khó nhớ khi sử dụng các dịch vụ trên mạng. Ví dụ tên miền www.cisco.com với **www** là tên định danh cho máy tính, **cisco** là tên định danh cho tổ chức, còn **com** là tên định danh cho vùng cấp cao nhất còn gọi là vùng gốc (root domain).

# DNS

- Đối với Internet, vùng gốc có các tên định danh như com, edu, gov, net, ... được sử dụng trong các tên miền cấp phát tại Mỹ, còn ở các nước khác vùng gốc có tên định danh được tạo bởi hai chữ cái viết tắt của tên nước như VN (cho Việt Nam), JP (cho Nhật Bản). Trong mạng nội bộ không buộc phải tuân thủ theo cấu trúc tên miền quốc tế nên vùng gốc có thể lấy ngay tên định danh là com, edu, gov, net,...

# DNS

- **Cài đặt máy phục vụ DNS**
- Có thể lập cấu hình máy phục vụ Microsoft Windows 2000 bất kỳ làm máy phục vụ DNS. Bốn loại máy phục vụ DNS khả dụng gồm:
- Máy phục vụ chính tích hợp Active Directory: Máy phục vụ chính được tích hợp hoàn toàn với Active Directory. Toàn bộ dữ liệu DNS được lưu trực tiếp vào Active Directory.
- Máy phục vụ chính: Máy phục vụ DNS chính dành cho vùng, được tích hợp một phần với Active Directory.

# DNS

- Máy phục vụ dự phòng: Máy phục vụ DNS cung cấp dịch vụ sao lưu cho vùng. Máy này lưu giữ bản sao của mẫu tin DNS thu được từ máy phục vụ chính và cập nhật dựa vào đặc tính chuyển khu vực.
- Máy phục vụ chỉ chuyển tiếp: Máy phục vụ lưu tạm thông tin DNS sau khi dò thấy và luôn chuyển tiếp yêu cầu đến máy phục vụ khác. Những máy này lưu giữ thông tin DNS cho đến khi thông tin được cập nhật hay hết hạn dùng, hoặc đến lúc máy phục vụ tái khởi động.

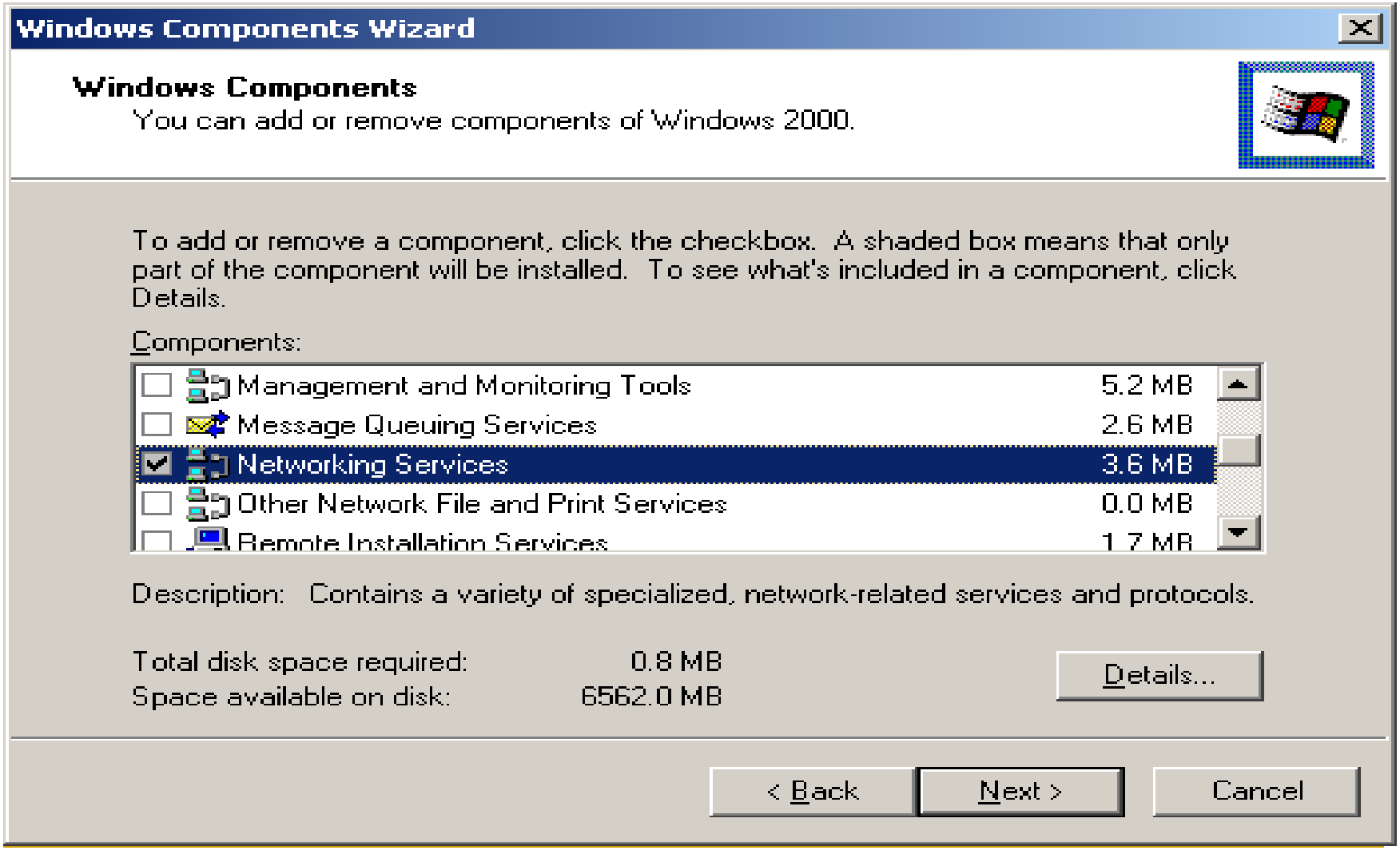
# DNS

- Trường hợp bạn đang làm việc với máy phục vụ thành viên thay vì máy điều khiển vùng, hay là bạn chưa cài DNS, hãy thực hiện theo các bước sau để cài DNS:

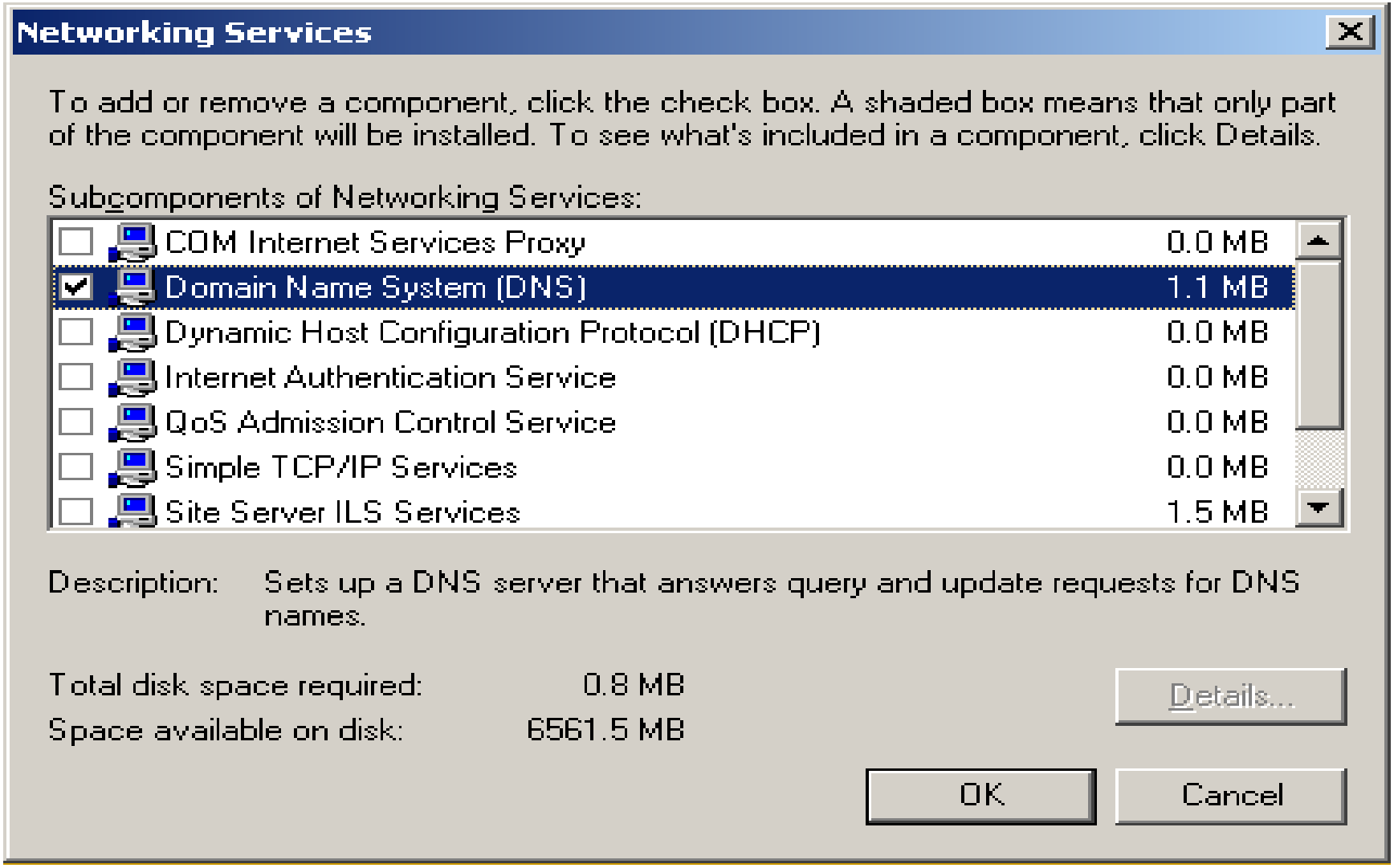
# DNS

- Nhấp *Start* chọn *Setting*→*Control Panel*.
- Trong *Control Panel*, nhấn đúp *Add/Remove Program*. Nhấn tiếp *Add/Remove Windows Components*.
- Nhấp *Components* khởi động *Windows Components Wizard*, nhấp *Next*.
- Dưới *Components*, nhấp *Networking Services*, nhấp tiếp *Details*.

# DNS


Windows Components Wizard
Windows Components
You can add or remove components of Windows 2000.
To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Components:
Management and Monitoring Tools 5.2 MB
Message Queuing Services 2.6 MB
Networking Services 3.6 MB
Other Network File and Print Services 0.0 MB
Remote Installation Services 1.7 MB
Description: Contains a variety of specialized, network-related services and protocols.
Total disk space required: 0.8 MB
Space available on disk: 6562.0 MB
Details...
< Back
Next >
Cancel

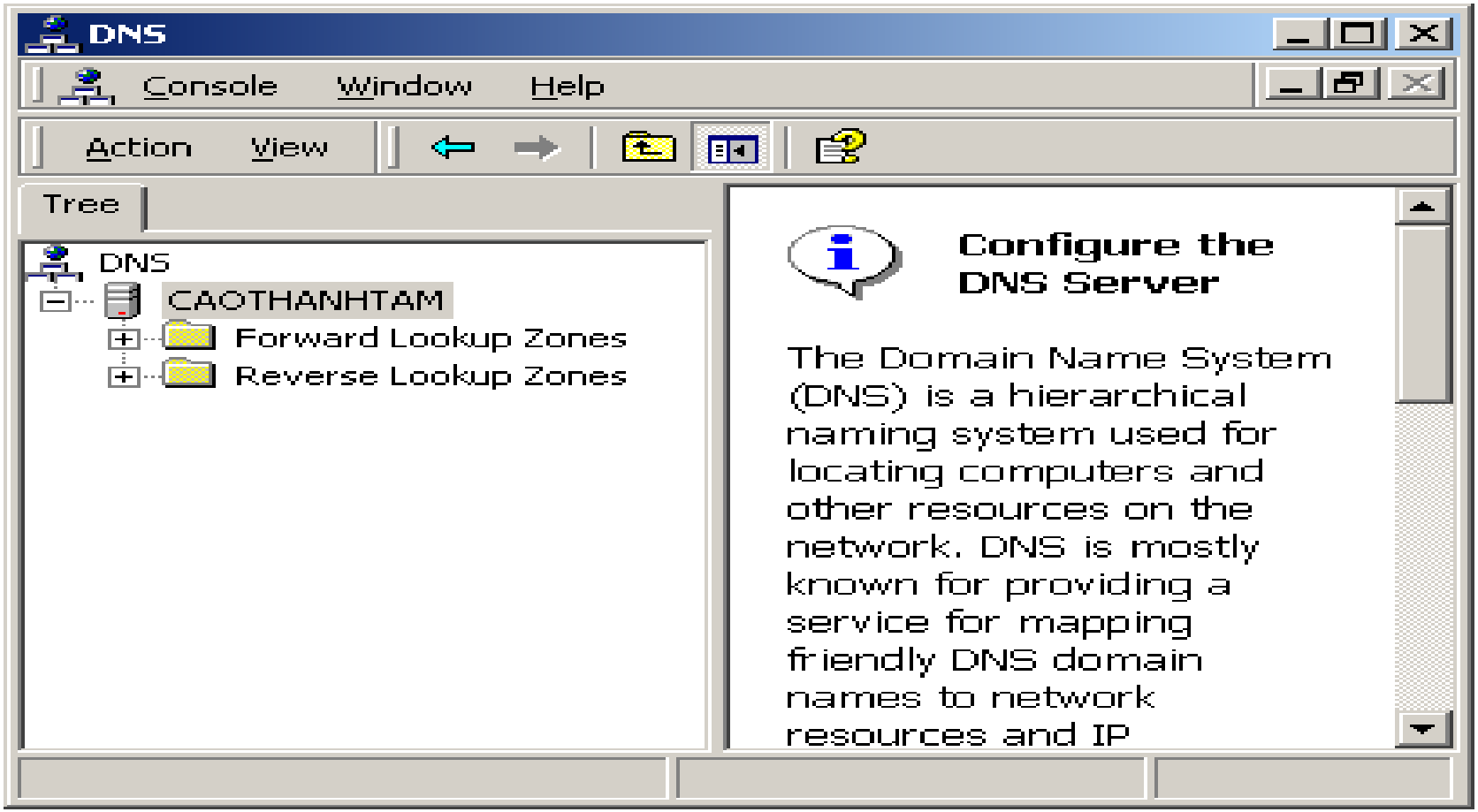
# DNS


Networking Services
To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Subcomponents of Networking Services:
COM Internet Services Proxy 0.0 MB
Domain Name System (DNS) 1.1 MB
Dynamic Host Configuration Protocol (DHCP) 0.0 MB
Internet Authentication Service 0.0 MB
QoS Admission Control Service 0.0 MB
Simple TCP/IP Services 0.0 MB
Site Server ILS Services 1.5 MB
Description: Sets up a DNS server that answers query and update requests for DNS names.
Total disk space required: 0.8 MB
Space available on disk: 6561.5 MB
Details...
OK
Cancel

# Cấu hình dịch vụ DNS

- Vùng nào cũng phải có máy phục vụ DNS chính, có thể tích hợp với Active Directory hay vận hành như máy phục vụ chính thông thường. Máy phục vụ chính phải có khu vực dò xuôi và khu vực dò ngược thích hợp. Khu vực dò xuôi (forward lookup zone) giúp phân giải tên vùng thành địa chỉ IP. Khu vực dò ngược (reserve lo*OK*up zone) rất cần thiết với tác vụ phê chuẩn các yêu cầu DNS bằng cách phân giải địa chỉ IP thành tên vùng hay tên máy chủ. Khi đã cài đặt DNS server trên máy phục vụ, bạn có thể lập cấu hình máy phục vụ chính theo tiến trình sau:

# Bước 1: Mở *Console*: Nhấp *Start→Programs→Adminitratives Tools→DNS*



# DNS

- Bước 2: Giả sử máy phục vụ cần lập cấu hình không có tên trong danh sách ở khung bên trái, bạn phải nối kết với nó. Nhấp nút phải chuột vào DNS bên khung trái, chọn *Conect to Computer*. Thực hiện một trong hai việc dưới đây:
- Nếu đang nối kết với máy phục vụ cục bộ, chọn *This computer* rồi nhấp *OK.*
- Trường hợp cố nối kết với máy phục vụ ở xa, chọn *The Following Computer* rồi gõ tên hay địa chỉ *IP* của máy phục vụ, nhấp *OK*.

# DNS

- Bước 3: Máy phục vụ DNS giờ đã có trong khung danh sách của *Console* DNS. Nhấp nút phải chuột vào mục nhập mới, chọn *New Zone* từ menu tắt để khởi động *New Zone Wizard*, nhấp *Next*.

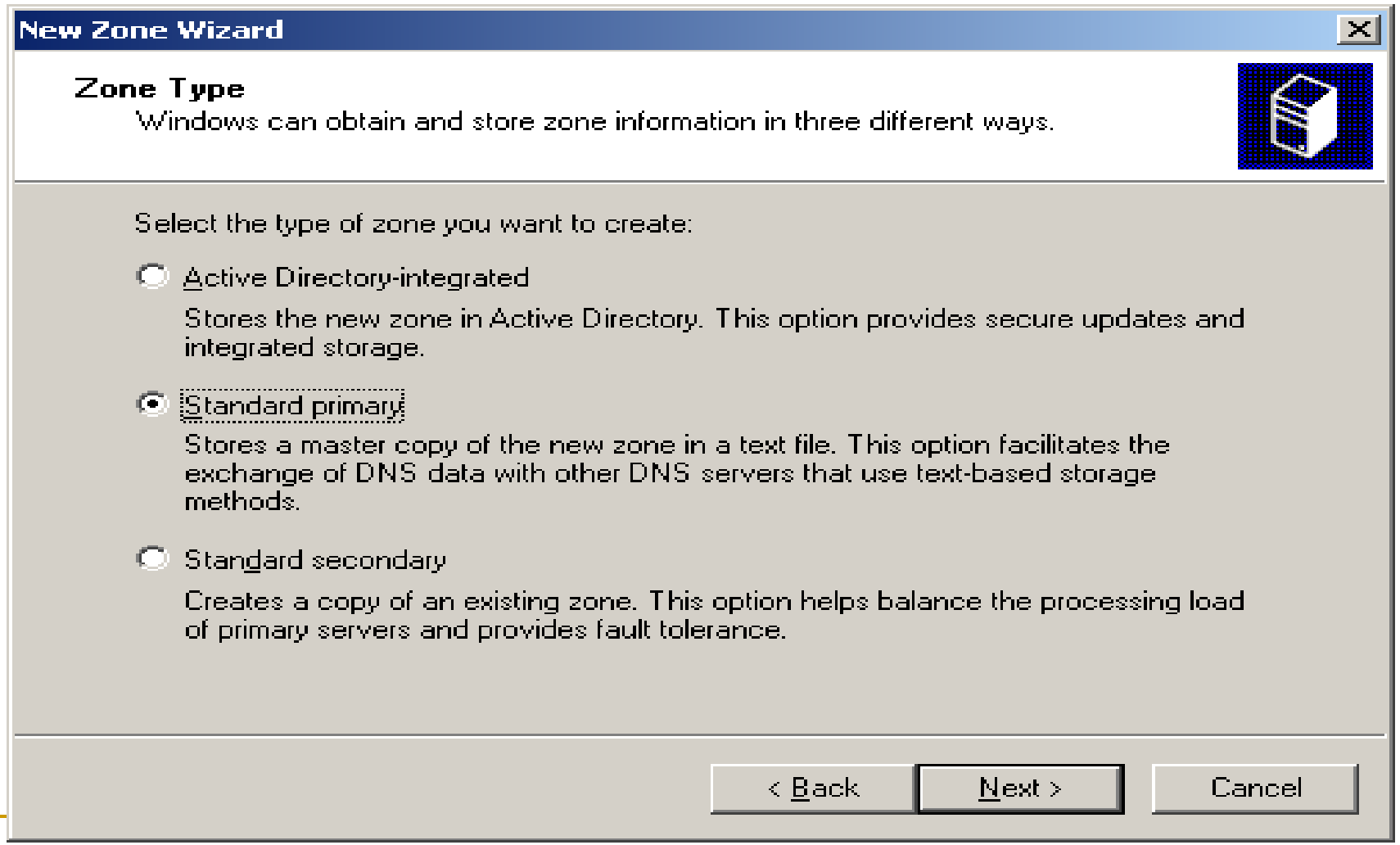
# DNS

New Zone Wizard
Welcome to the New Zone Wizard
This wizard helps you create a new zone for your DNS server.
A zone is a database that links DNS names and related data, such as IP addresses or network services.
To continue, click Next.
< Back
Next >
Cancel

# DNS

- Bước 4: Trong *New Zone Wizard*, chọn *Active Directory Intergrated*, nếu không chọn *Standard Primary* và nhấp *Next*

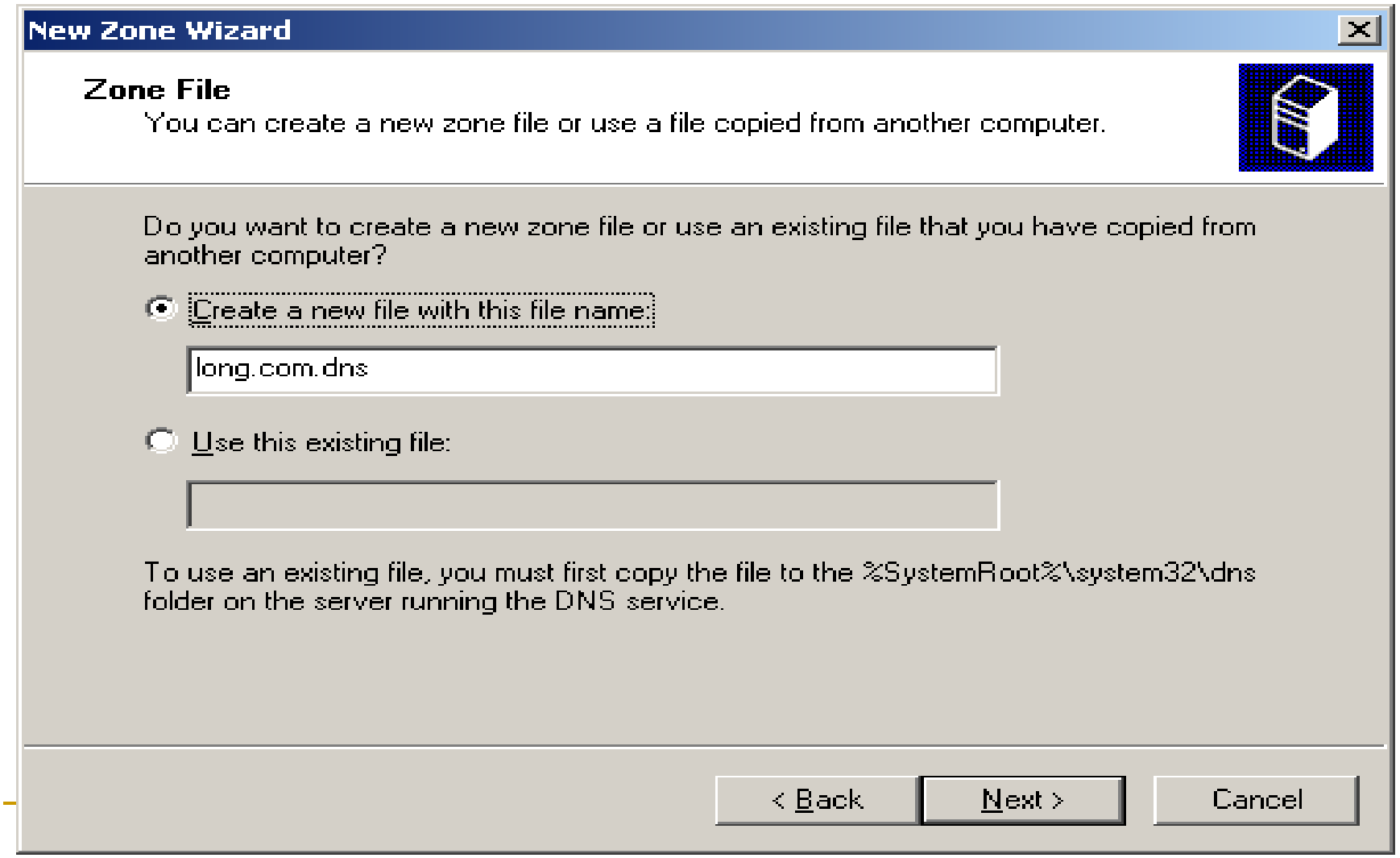
# DNS


New Zone Wizard
Zone Type
Windows can obtain and store zone information in three different ways.
Select the type of zone you want to create:
Active Directory-integrated
Stores the new zone in Active Directory. This option provides secure updates and integrated storage.
Standard primary
Stores a master copy of the new zone in a text file. This option facilitates the exchange of DNS data with other DNS servers that use text-based storage methods.
Standard secondary
Creates a copy of an existing zone. This option helps balance the processing load of primary servers and provides fault tolerance.
< Back
Next >
Cancel

# DNS

- Bước 5: Chọn *Forward Lookup Zone*, nhấp *Next*.
- Bước 6: Gõ tên *DNS* hoàn chỉnh cho khu vực, tên khu vực giúp xác định máy phục vụ hay khu vực trong cấu trúc vùng *Active Drectory*. Lấy ví dụ trường hợp đang thiết lập máy phục vụ chính cho trong cấu trúc vùng cisco.com, bạn phải gõ tên vùng là cisco.com.

# DNS


New Zone Wizard
Zone File
You can create a new zone file or use a file copied from another computer.
Do you want to create a new zone file or use an existing file that you have copied from another computer?
Create a new file with this file name:
long.com.dns
Use this existing file:
To use an existing file, you must first copy the file to the %SystemRoot%\system32\dns folder on the server running the DNS service.
< Back
Next >
Cancel

# DNS

- Bước 7: Nhấp *Next*, và cuối cùng nhấp *Finish* hoàn tất tiến trình, khu vực mới được bổ sung vào máy phục vụ  và các mẩu tin DNS sẽ tự động được tạo thành. Một máy phục vụ DNS sẽ có khả năng cung cấp dịch vụ cho nhiều vùng.

# Thiết lập máy DNS dự phòng

- Máy phục vụ dự phòng cung cấp dịch vụ DNS dự phòng trên mạng.Vì máy phục vụ dự phòng cung cấp khu vực dò xuôi cho hầu hết các loại, nên khu vực dò ngược có khi không cần thiết. Nhưng khu vực dò ngược lại vô cùng quan trọng cho máy phục vụ chính bởi vậy nhất thiết phải thiết lập chúng để cơ chế phân giải tên vùng vận hành thích hợp. Muốn thiết lập cơ chế  dự phòng sao lưu và cân bằng tải, ta thực hiện các bước như sau:

# DNS

+ Bước 1: Mở *Console DNS* và nối kết với máy phục vụ cần lập cấu hình .
+ Bước 2: Nhấp nút phải chuột vào mục nhập ứng với máy phục vụ, chọn *New Zone* khởi động *New Zone Wizard*, nhấp *Next*.
+ Bước 3: Trong hộp thoại *Zone Type*. Chọn *Standard Secondary*, nhấp *Next*

- + Bước 4: Máy phục vụ dự phòng có thể sử dụng tập tin khu vực cả dò xuôi lẫn dò ngược. Do đó sẽ thiết lập khu vực dò xuôi trước, chọn *Forward LoOKup Zone*, nhấp *Next*.
- + Bước 5: Gõ tên cho tập tin khu vực, nhấp *Next*.
- + Bước 6: Máy phục vụ dự phòng sẽ phải sao chép tập tin khu vực từ máy phục vụ chính. Gõ địa chỉ IP của máy phục vụ chính trong khu vực, nhấp *Next*, cuối cùng nhấp *Finish*.

# Thiết lập máy phục vụ khu vực dò ngược

- Khu vực dò xuôi (*Forward Lookup Zone*) dùng để phân giải tên vùng thành địa chỉ IP. Khu vực dò ngược (*Reverse Lookup Zone*) dùng để phân giải địa chỉ IP thành tên vùng. Mỗi mạng phải có một khu vực dò ngược ví dụ như ta chia mạng thành 3 mạng con 192.168.10.0, 192.168.11.0 và 192.168.12.0 nhất thiết phải có cả ba khu vực dò ngược. Cách thiết lập khu vực dò ngược:

# DNS

+ Bước 1: Mở *Console DNS* và nối kết với máy phục vụ cần lập cấu hình.
+ Bước 2: Nhấp nút phải chuột vào mục cần lập cấu hình ứng với máy phục vụ, chọn *New Zone* khởi động *New Zone Wizard*, nhấp *Next*.
+ Bước 3: Chọn *Active Drectory-Intergrated*, *Standard Primary* hay *Secondary* dựa trên loại máy phục vụ đang làm việc.
+ Bước 4: Chọn Reverse Lookup Zone, nhấp Next
+ Bước 5: Gõ số nhận diện mạng (*Net ID*) và mặt nạ mạng con (*subnet mask*) cho khu vực dò ngược. Các giá trị vừa gõ vào sẽ hình thành tên mặc định cho khu vực dò ngược.

# DNS

- + Bước 6: Nếu đang lập cấu hình máy phục vụ chính hay máy phục vụ dự phòng thông thường (Standard), bạn phải định rõ tên tập tin cơ sở dữ liệu DNS của khu vực. Tên mặc định cho tập tin cơ sở dữ liệu DNS của khu vực sẽ được tự động điền phát sinh, khi đó có thể sử dụng ngay hoặc sửa đổi.
- + Bước 7: Trường hợp đang lập cấu hình máy phục vụ dự phòng, hãy cung cấp địa chỉ IP của máy phục vụ chính trong khu vực rồi nhấp *Add*.
- + Bước 8:  Nhấp *Next*, cuối cùng nhấp *Finish*.

# Active Directory

- **Giới thiệu**
- **AD (Active Directory)** là dịch vụ thư mục chứa các thông tin về các tài nguyên trên mạng, có thể mở rộng và có khả năng tự điều chỉnh cho phép bạn quản lý tài nguyên mạng hiệu quả. Để có thể làm việc tốt với Active Directory, chúng ta sẽ tìm hiểu khái quát về Active Directory, sau đó khảo sát các thành phần của dịch vụ này.

# Active Directory

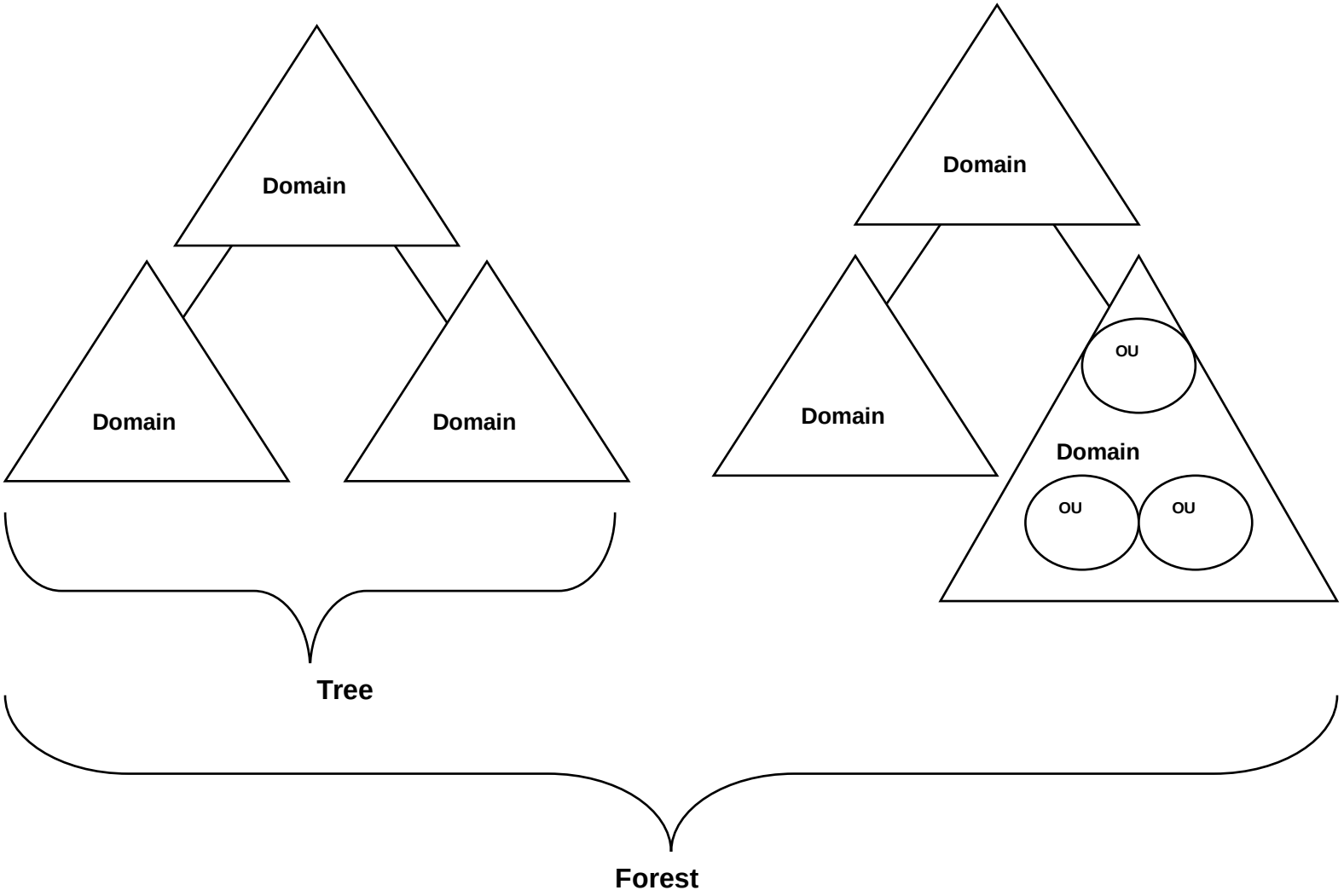
- Các đối tượng AD bao gồm dữ liệu của người dùng (user data), máy in(printers), máy chủ (servers), cơ sở dữ liệu (databases), các nhóm người dùng (groups), các máy tính (computers), và các chính sách bảo mật (security policies).

# Active Directory

- Ngoài ra một khái niệm mới được sử dụng là *container* (tạm dịch là tập đối tượng). Ví dụ Domain là một tập đối tượng chứa thông tin người dùng, thông tin các máy trên mạng, và chứa các đối tượng khác.

# Các thành phần của AD:

- Cấu trúc AD logic gồm các thành phần: domains (vùng), organization units (đơn vị tổ chức), trees (hệ vùng phân cấp ) và  forests (tập hợp hệ vùng phân cấp) .


Domain
Domain
Domain
Tree
Domain
Domain
OU
Domain
OU
OU
Forest

# Active Directory

- Vùng (Domain): là đơn vị cốt lõi của AD logic.
- Tất cả các đối tượng AD đều thuộc một vùng nhất định. Mỗi vùng có thể chứa đến hàng triệu đối tượng.
- Vùng là đường biên an toàn cho mạng. Người quản trị vùng chỉ được quyền quản lý các đối tượng trong vùng đó mà thôi. Danh sách kiểm soát truy nhập (Access Control Lists -ACLs) được lập riêng cho mỗi vùng và không có tác dụng đối với các vùng khác.

# Active Directory

- Đơn vị tổ chức (Organization Unit):
- OU là những tập đối tượng dùng để tổ chức các đối tượng trong một  vùng thành những nhóm quản trị lôgic nhỏ hơn.
- Một OU có thể chứa các đối tượng khác nhau như: các tài khoản người dùng, các nhóm, các máy tính, các máy in, các trình ứng dụng, các tệp sử dụng chung và các đơn vị tổ chức khác nằm trên cùng một vùng.
- Hệ vùng phân cấp (domain tree): Một hay nhiều vùng dùng chung không gian liên tục.
- Tập hợp hệ vùng phân cấp (doain forest): Một hay nhiều hệ vùng phân cấp dùng chung không gian thư mục.

# Active Directory

- Cấu trúc AD vật lý gồm: sites và domain controllers.
- Địa bàn (site): là tập hợp của một hay nhiều mạng con kết nối bằng đường truyền tốc độ cao.
- Điều khiển vùng (domain controllers): là máy tính chạy Windows2000 Server chứa bản sao dữ liệu vùng. Một vùng có thể có một hay nhiều điều khiển vùng. Mỗi sự thay đổi dữ liệu trên một điều khiển vùng sẽ được tự động cập nhật lên các điều khiển khác của vùng.

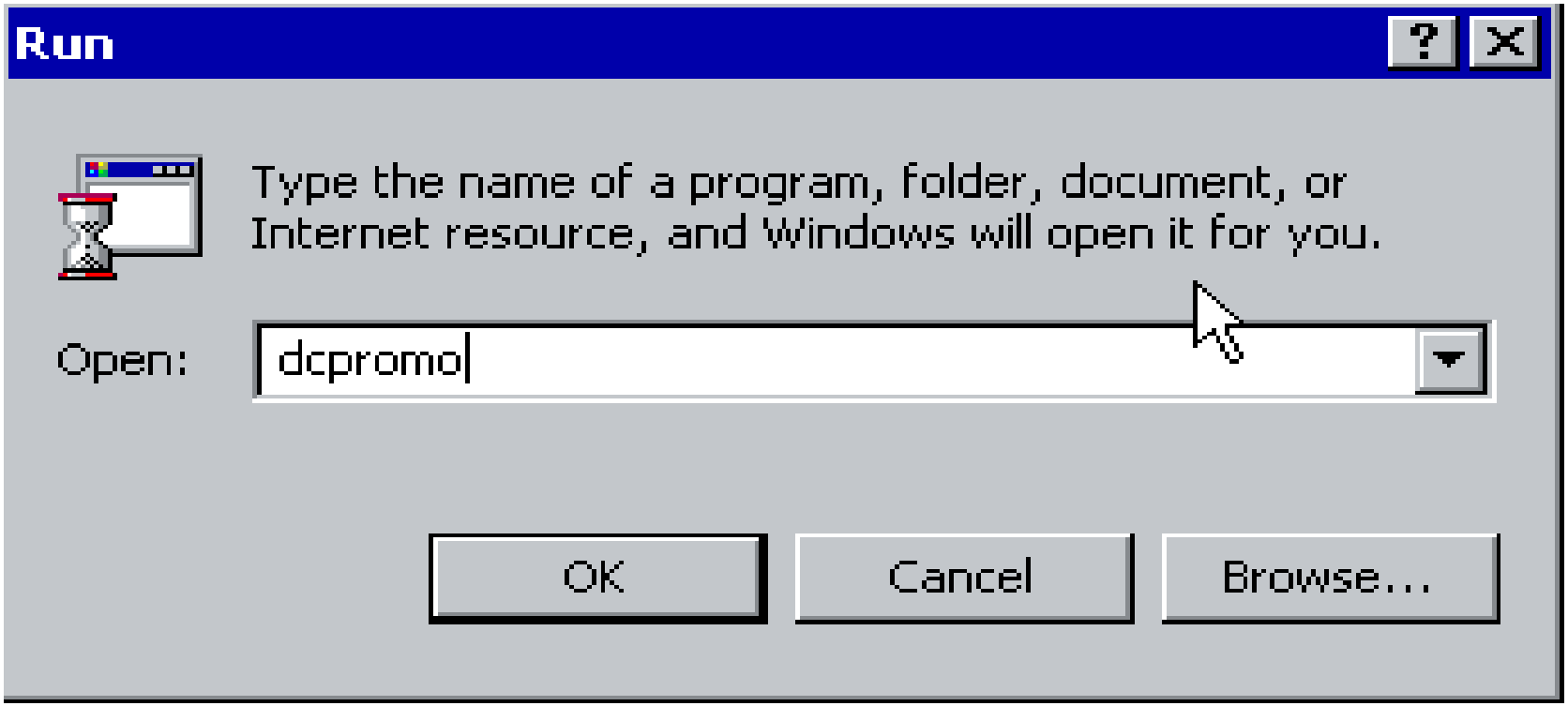
# Active Directory

- Cấu trúc logic giúp tổ chức các đối tượng thư mục, quản lý tài khoản mạng và tài nguyên dùng chung. Cấu trúc logic bao gồm nhiêu hệ vùng phân cấp, đơn vị tổ chức. Site và mạng con là  cấu trúc vật lý, tạo điều kiện truyền thông qua mạng dễ dàng ấn định ranh giới vật lý xung quanh các tài nguyên mạng. Vùng AD thực ra là nhóm máy tính dùng chung cơ sở dữ liệu thư mục.

# Cài đặt và cấu hình máy Windows 2000 điều khiển vùng (Domain Controller)

- **Cài đặt Active Directory**
- Để cài AD bạn phải cấu hình và có địa chỉ IP tĩnh cũng như bạn phải cấu hình và cài DNS trước.
- Bạn theo các bước sau để cài AD:
- Vào *Start->Run* gõ lệnh *dcpromo* để cài Active Directory

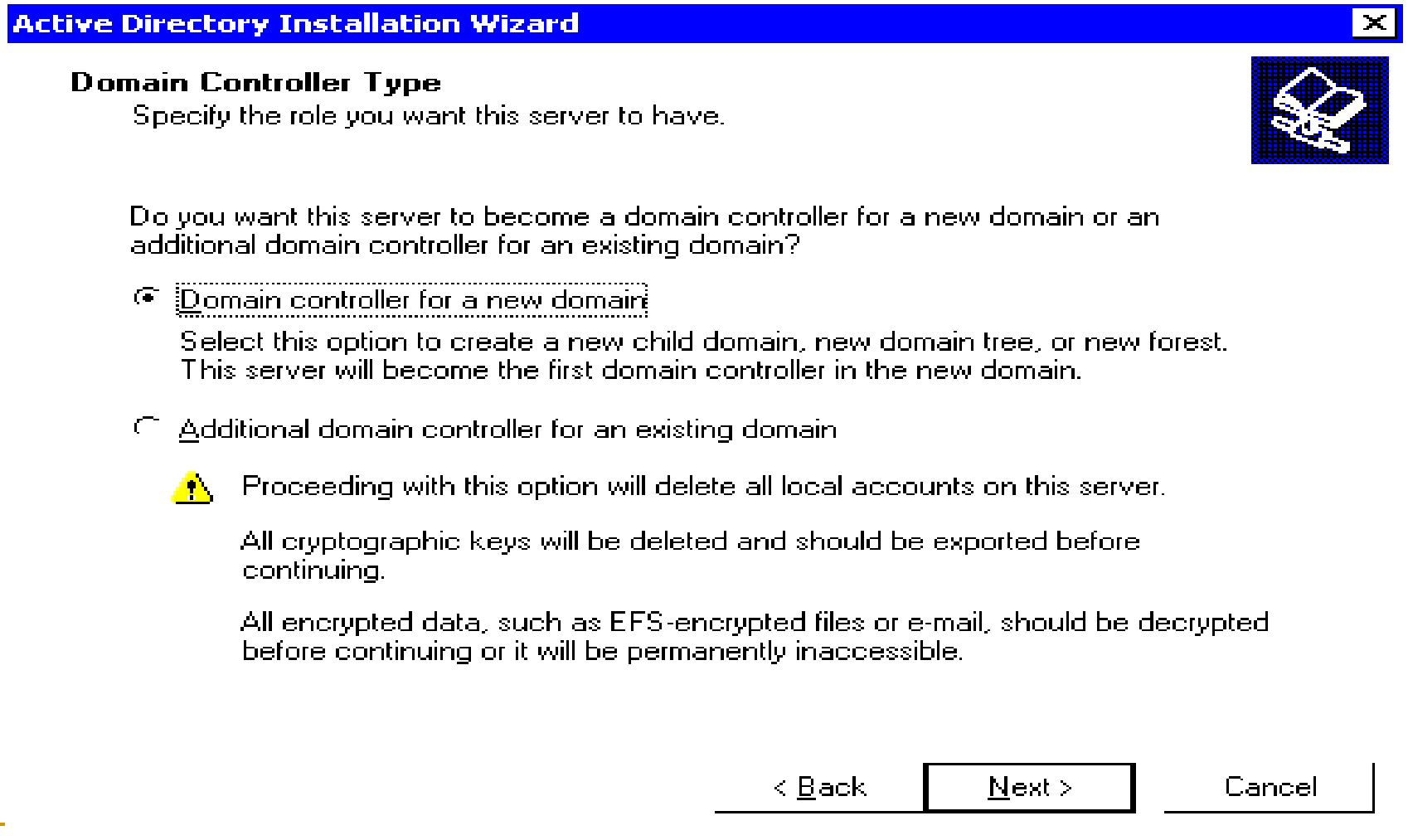
# Cài đặt Domain controller



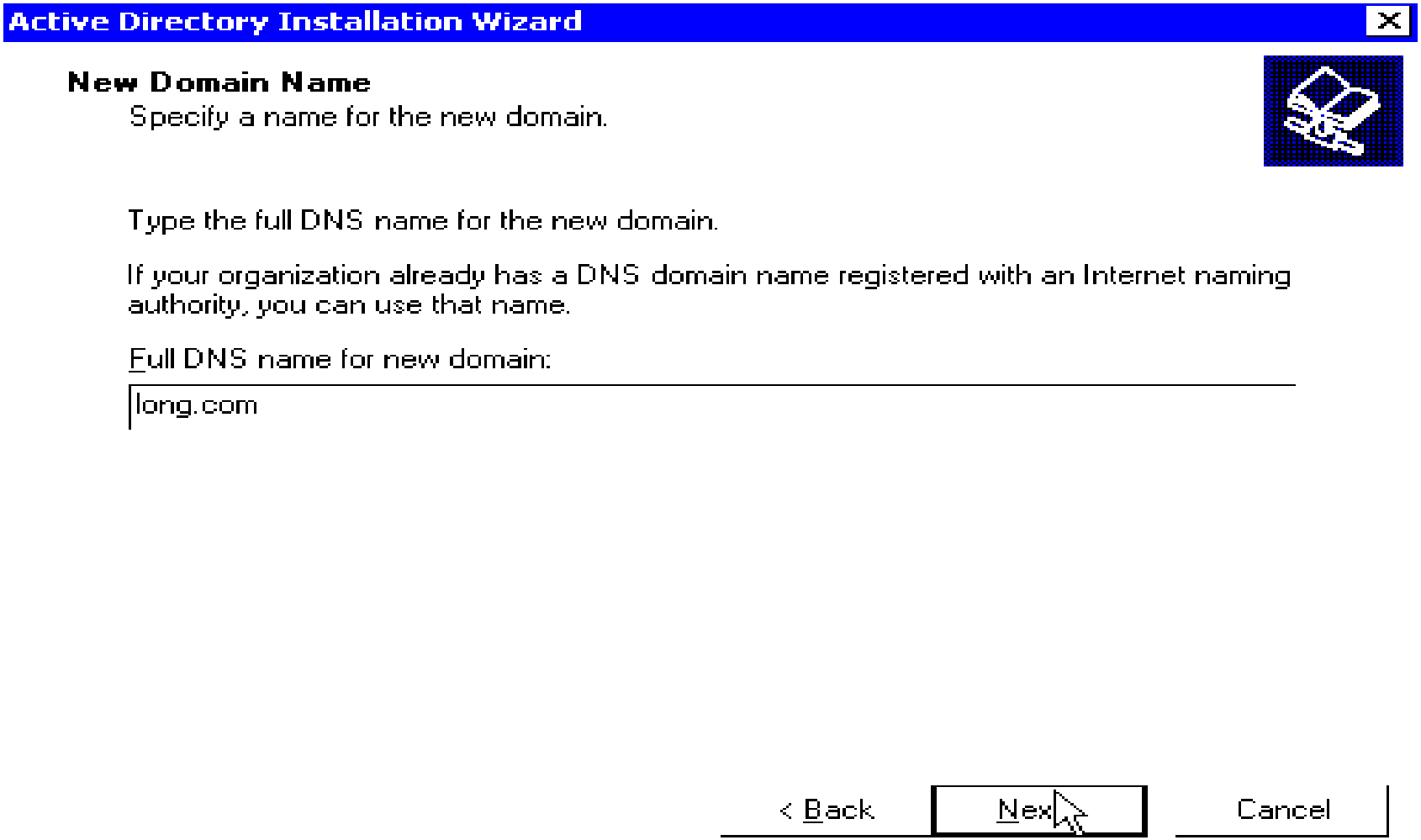
# Cài đặt Domain controller

- Khi *Active Direcrory Installation Wizard* xuất hiện chọn *Next*, dưới *Domain Controller Type* chọn *Domain controller for a new domain* nếu là domain mới. Xác định tên mới ở *New Domain Name*

# Cài đặt Domain controller



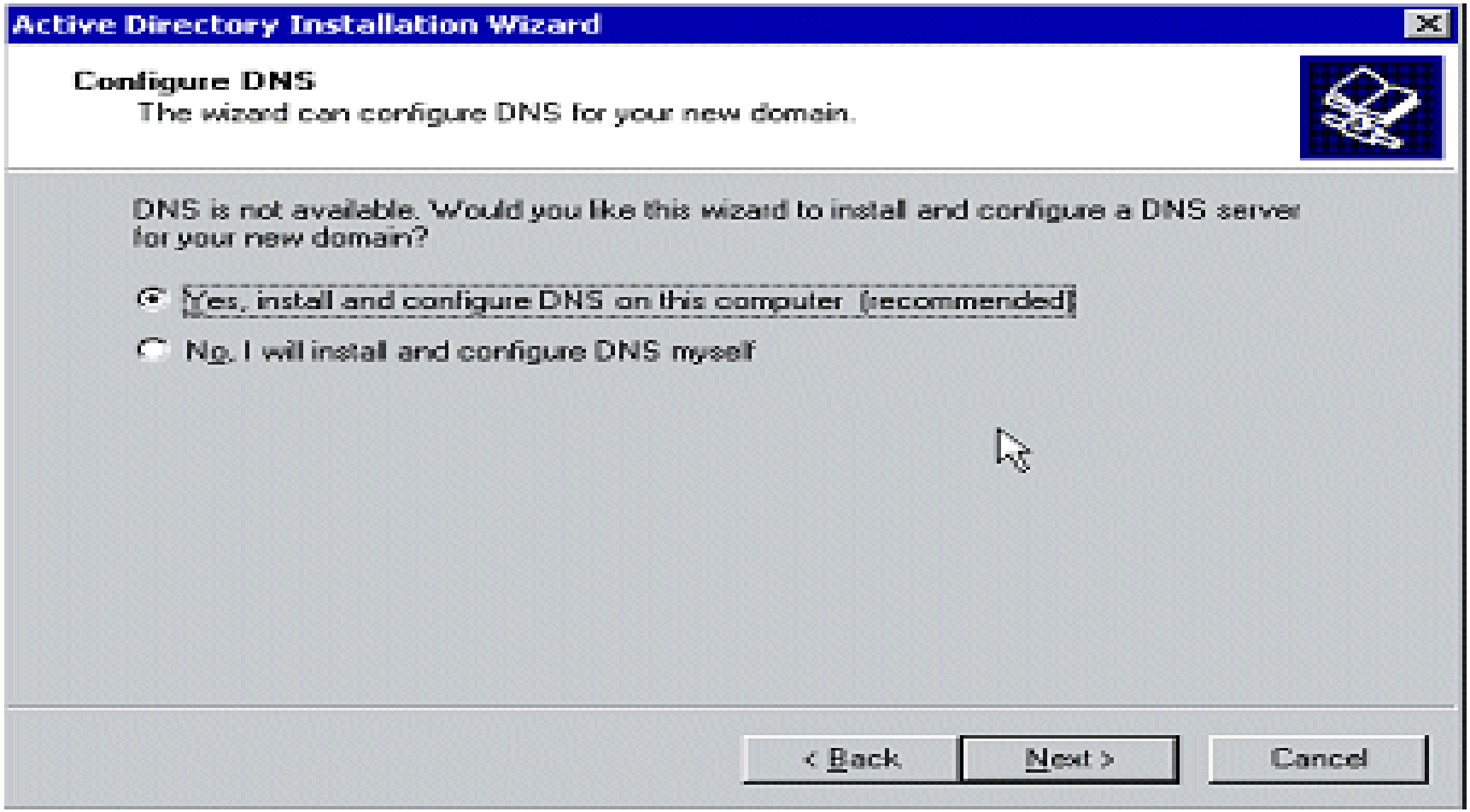
# Cài đặt Domain controller



# Cài đặt Domain controller

- Xác định tên *NestBIOS*, vị trí chứa cơ sở dữ liệu, mặc định sẽ chọn thư mục tên *SYSVOL* trong ổ đĩa chứa *WINNT*, bạn phải lưu ý là thư mục *SYSVOL* phải là thư mục đã được định dạng là *NTFS V5.0* trở lên, trong *Configures DNS* bạn chọn tự cấu hình hay cấu hình mặc định,

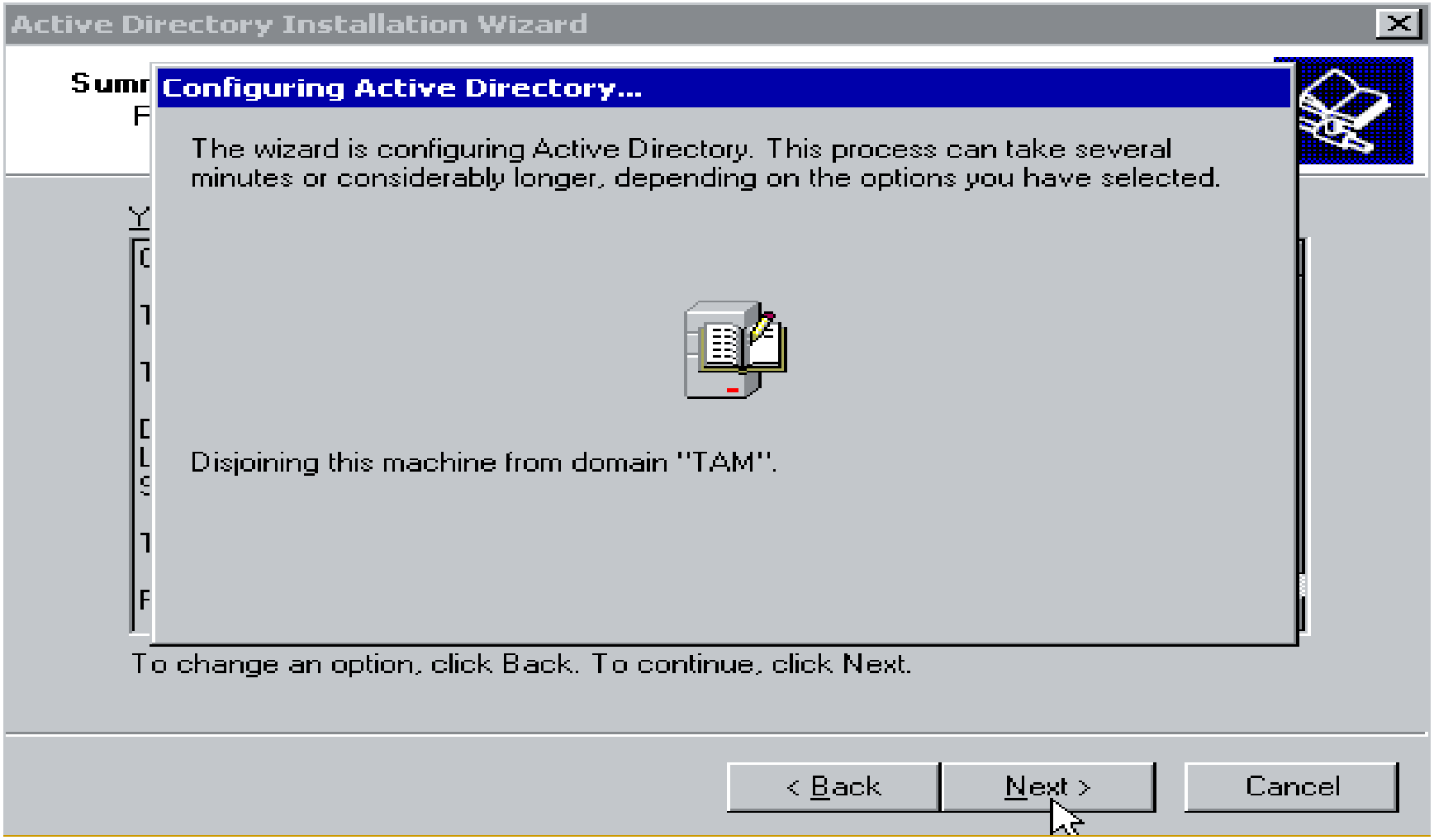
# Cài đặt Domain controller



# Cài đặt Domain controller

- Bạn chọn để AD  hỗ trợ hay không hỗ trợ các hệ điều hành trước Windows 2000 trong *Permission*, chọn *Password* và nhấp *Next* Trong phần *Summary*, sau đó Active Drectory được cài

# Cài đặt Domain controller



# The End.

# GIÁO TRÌNH
# MẠNG MÁY TÍNH

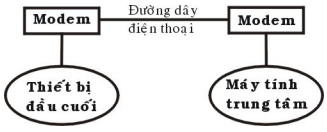
**Hà nội 11-2000**

**Chương 1**

# Sơ lược lịch sử phát triển của mạng máy tính

Vào giữa những năm 50 khi những thế hệ máy tính đầu tiên được đưa vào hoạt động thực tế với những bóng đèn điện tử thì chúng có kích thước rất cồng kềnh và tốn nhiều năng lượng. Hồi đó việc nhập dữ liệu vào các máy tính được thông qua các tấm bìa mà người viết chương trình đã đục lỗ sẵn. Mỗi tấm bìa tương đương với một dòng lệnh mà mỗi một cột của nó có chứa tất cả các ký tự cần thiết mà người viết chương trình phải đục lỗ vào ký tự mình lựa chọn. Các tấm bìa được đưa vào một "thiết bị" gọi là thiết bị đọc bìa mà qua đó các thông tin được đưa vào máy tính (hay còn gọi là trung tâm xử lý) và sau khi tính toán kết quả sẽ được đưa ra máy in. Như vậy các thiết bị đọc bìa và máy in được thể hiện như các thiết bị vào ra (I/O) đối với máy tính. Sau một thời gian các thế hệ máy mới được đưa vào hoạt động trong đó một máy tính trung tâm có thể được nối với nhiều thiết bị vào ra (I/O) mà qua đó nó có thể thực hiện liên tục hết chương trình này đến chương trình khác.

Cùng với sự phát triển của những ứng dụng trên máy tính các phương pháp nâng cao khả năng giao tiếp với máy tính trung tâm cũng đã được đầu tư nghiên cứu rất nhiều. Vào giữa những năm 60 một số nhà chế tạo máy tính đã nghiên cứu thành công những thiết bị truy cập từ xa tới máy tính của họ. Một trong những phương pháp thâm nhập từ xa được thực hiện bằng việc cài đặt một thiết bị đầu cuối ở một vị trí cách xa trung tâm tính toán, thiết bị đầu cuối này được liên kết với trung tâm bằng việc sử dụng đường dây điện thoại và với hai thiết bị xử lý tín hiệu (thường gọi là Modem) gắn ở hai đầu và tín hiệu được truyền thay vì trực tiếp thì thông qua dây điện thoại.




*Hình 1.1. Mô hình truyền dữ liệu từ xa đầu tiên*

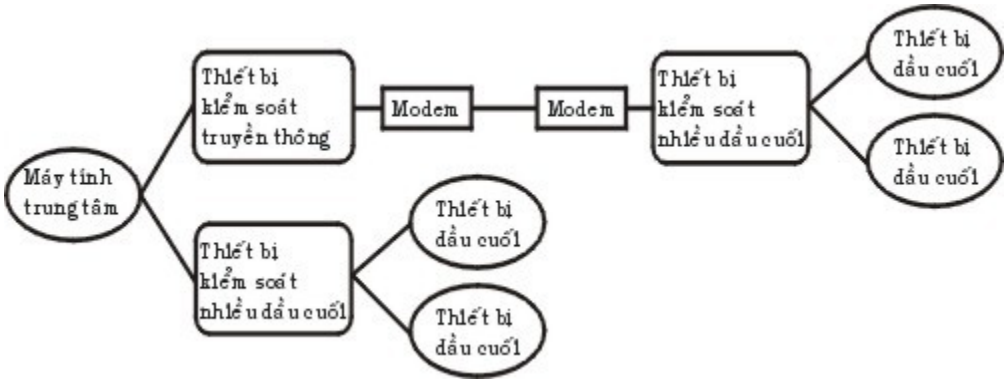
Những dạng đầu tiên của thiết bị đầu cuối bao gồm máy đọc bìa, máy in, thiết bị xử lý tín hiệu, các thiết bị cảm nhận. Việc liên kết từ xa đó có thể thực hiên thông qua những vùng khác nhau và đó là những dạng đầu tiên của hệ thống mạng.

Trong lúc đưa ra giới thiệu những thiết bị đầu cuối từ xa, các nhà khoa học đã triển khai một loạt những thiết bị điều khiển, những thiết bị đầu cuối đặc biệt cho phép người sử dụng nâng cao được khả năng tương tác với máy tính. Một trong những sản phẩm quan trọng đó là hệ thống thiết bị đầu cuối 3270 của IBM. Hệ thống đó bao gồm các màn hình, các hệ thống điều khiển, các thiết bị truyền thông được liên kết với các trung tâm tính toán. Hệ thống 3270 được giới thiệu vào năm 1971 và được sử dụng dùng để mở rộng khả năng tính toán của trung tâm máy tính tới các vùng xa. Để làm giảm nhiệm vụ truyền thông của máy tính trung tâm và số lượng các liên kết giữa

máy tính trung tâm với các thiết bị đầu cuối, IBM và các công ty máy tính khác đã sản xuất một số các thiết bị sau:

- **Thiết bị kiểm soát truyền thông**: có nhiệm vụ nhận các bit tín hiệu từ các kênh truyền thông, gom chúng lại thành các byte dữ liệu và chuyển nhóm các byte đó tới máy tính trung tâm để xử lý, thiết bị này cũng thực hiện công việc ngược lại để chuyển tín hiệu trả lời của máy tính trung tâm tới các trạm ở xa. Thiết bị trên cho phép giảm bớt được thời gian xử lý trên máy tính trung tâm và xây dựng các thiết bị logic đặc trưng.

- **Thiết bị kiểm soát nhiều đầu cuối**: cho phép cùng một lúc kiểm soát nhiều thiết bị đầu cuối. Máy tính trung tâm chỉ cần liên kết với một thiết bị như vậy là có thể phục vụ cho tất cả các thiết bị đầu cuối đang được gắn với thiết bị kiểm soát trên. Điều này đặc biệt có ý nghĩa khi thiết bị kiểm soát nằm ở cách xa máy tính vì chỉ cần sử dụng một đường điện thoại là có thể phục vụ cho nhiều thiết bị đầu cuối.




*Hình 1.2: Mô hình trao đổi mạng của hệ thống 3270*

Vào giữa những năm 1970, các thiết bị đầu cuối sử dụng những phương pháp liên kết qua đường cáp nằm trong một khu vực đã được ra đời. Với những ưu điểm từ nâng cao tốc độ truyền dữ liệu và qua đó kết hợp được khả năng tính toán của các máy tính lại với nhau. Để thực hiện việc nâng cao khả năng tính toán với nhiều máy tính các nhà sản xuất bắt đầu xây dựng các mạng phức tạp. Vào những năm 1980 các hệ thống đường truyền tốc độ cao đã được thiết lập ở Bắc Mỹ và Châu Âu và từ đó cũng xuất hiện các nhà cung cấp các dịnh vụ truyền thông với những đường truyền có tốc độ cao hơn nhiều lần so với đường dây điện thoại. Với những chi phí thuê bao chấp nhận được, người ta có thể sử dụng được các đường truyền này để liên kết máy tính lại với nhau và bắt đầu hình thành các mạng một cách rộng khắp. Ở đây các nhà cung cấp dịch vụ đã xây dựng những đường truyền dữ liệu liên kết giữa các thành phố và khu vực với nhau và sau đó cung cấp các dịch vụ truyền dữ liệu cho những người xây dựng mạng. Người xây dựng mạng lúc này sẽ không cần xây dựng lại đường truyền của mình mà chỉ cần sử dụng một phần các năng lực truyền thông của các nhà cung cấp.

Vào năm 1974 công ty IBM đã giới thiệu một loạt các thiết bị đầu cuối được chế tạo cho lĩnh vực ngân hàng và thương mại, thông qua các dây cáp mạng các thiết bị đầu cuối có thể truy cập cùng một lúc vào một máy tính dùng chung. Với việc liên kết các máy tính nằm ở trong một khu vực nhỏ như một tòa nhà hay là một khu nhà thì tiền chi phí cho các thiết bị và phần mềm là thấp. Từ đó việc nghiên cứu khả năng sử dụng chung môi trường truyền thông và các tài nguyên của các máy tính nhanh chóng được đầu tư.

Vào năm 1977, công ty Datapoint Corporation đã bắt đầu bán hệ điều hành mạng của mình là "Attached Resource Computer Network" (hay gọi tắt là Arcnet) ra thị trường. Mạng Arcnet cho phép liên kết các máy tính và các trạm đầu cuối lại bằng dây cáp mạng, qua đó đã trở thành là hệ điều hành mạng cục bộ đầu tiên.

Từ đó đến nay đã có rất nhiều công ty đưa ra các sản phẩm của mình, đặc biệt khi các máy tính cá nhân được sử dụng một cánh rộng rãi. Khi số lượng máy vi tính trong một văn phòng hay cơ quan được tăng lên nhanh chóng thì việc kết nối chúng trở nên vô cùng cần thiết và sẽ mang lại nhiều hiệu quả cho người sử dụng.

Ngày nay với một lượng lớn về thông tin, nhu cầu xử lý thông tin ngày càng cao. Mạng máy tính hiện nay trở nên quá quen thuộc đối với chúng ta, trong mọi lĩnh vực như khoa học, quân sự, quốc phòng, thương mại, dịch vụ, giáo dục... Hiện nay ở nhiều nơi mạng đã trở thành một nhu cầu không thể thiếu được. Người ta thấy được việc kết nối các máy tính thành mạng cho chúng ta những khả năng mới to lớn như:

- **Sử dụng chung tài nguyên:** Những tài nguyên của mạng (như thiết bị, chương trình, dữ liệu) khi được trở thành các tài nguyên chung thì mọi thành viên của mạng đều có thể tiếp cận được mà không quan tâm tới những tài nguyên đó ở đâu.

- **Tăng độ tin cậy của hệ thống**: Người ta có thể dễ dàng bảo trì máy móc và lưu trữ (backup) các dữ liệu chung và khi có trục trặc trong hệ thống thì chúng có thể được khôi phục nhanh chóng. Trong trường hợp có trục trặc trên một trạm làm việc thì người ta cũng có thể sử dụng những trạm khác thay thế.

- **Nâng cao chất lượng và hiệu quả khai thác thông tin:** Khi thông tin có thể được sữ dụng chung thì nó mang lại cho người sử dụng khả năng tổ chức lại các công việc với những thay đổi về chất như:

  - Đáp ứng những nhu cầu của hệ thống ứng dụng kinh doanh hiện đại.
  - Cung cấp sự thống nhất giữa các dữ liệu.
  - Tăng cường năng lực xử lý nhờ kết hợp các bộ phận phân tán.
  - Tăng cường truy nhập tới các dịch vụ mạng khác nhau đang được cung cấp trên thế giới.

Với nhu cầu đòi hỏi ngày càng cao của xã hội nên vấn đề kỹ thuật trong mạng là mối quan tâm hàng đầu của các nhà tin học. Ví dụ như làm thế nào để truy xuất thông tin một cách nhanh chóng và tối ưu nhất, trong khi việc xử lý thông tin trên mạng quá nhiều đôi khi có thể làm tắc nghẽn trên mạng và gây ra mất thông tin một cách đáng tiếc.

Hiện nay việc làm sao có được một hệ thống mạng chạy thật tốt, thật an toàn với lợi ích kinh tế cao đang rất được quan tâm. Một vấn đề đặt ra có rất nhiều giải pháp về công nghệ, một giải pháp có rất nhiều yếu tố cấu thành, trong mỗi yếu tố có nhiều cách lựa chọn. Như vậy để đưa ra một giải pháp hoàn chỉnh, phù hợp thì phải trải qua một quá trình chọn lọc dựa trên những ưu điểm của từng yếu tố, từng chi tiết rất nhỏ.

Để giải quyết một vấn đề phải dựa trên những yêu cầu đặt ra và dựa trên công nghệ để giải quyết. Nhưng công nghệ cao nhất chưa chắc là công nghệ tốt nhất, mà công nghệ tốt nhất là công nghệ phù hợp nhất.

Chương 2

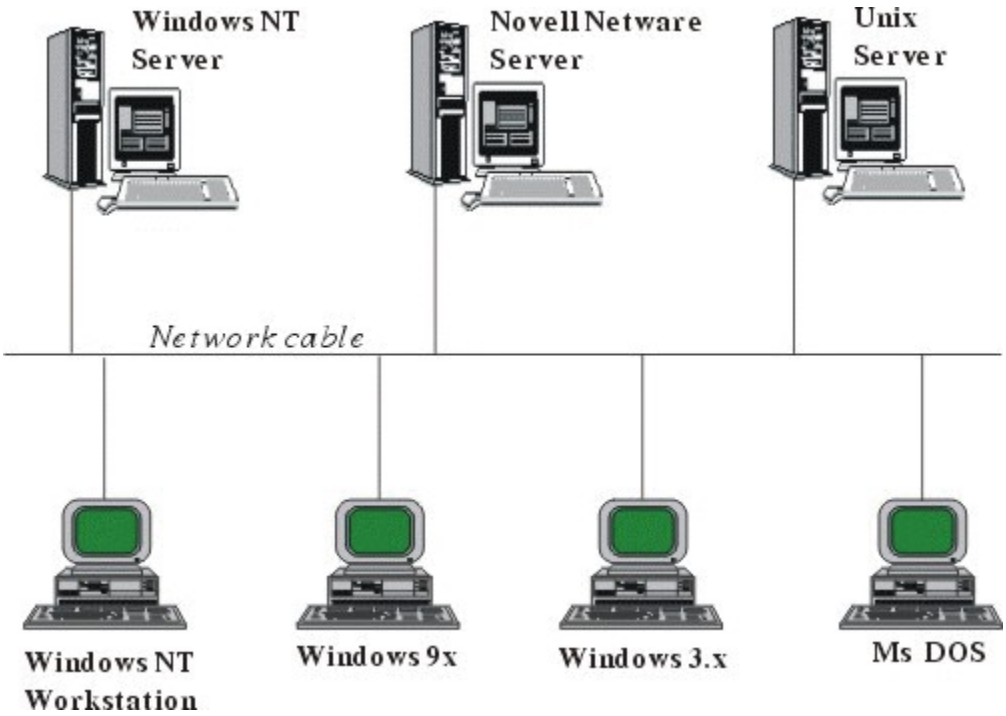
# Những khái niệm cơ bản của mạng máy tính

Với sự phát triển của khoa học và kỹ thuật, hiện nay các mạng máy tính đã phát triển một cách nhanh chóng và đa dạng cả về quy mô, hệ điều hành và ứng dụng. Do vậy việc nghiên cứu chúng ngày càng trở nên phức tạp. Tuy nhiên các mạng máy tính cũng có cùng các điểm chung thông qua đó chúng ta có thể đánh giá và phân loại chúng.

## I. Định nghĩa mạng máy tính

> *Mạng máy tính là một tập hợp các máy tính được nối với nhau bởi đường truyền theo một cấu trúc nào đó và thông qua đó các máy tính trao đổi thông tin qua lại cho nhau.*

Đường truyền là hệ thống các thiết bị truyền dẫn có dây hay không dây dùng để chuyển các tín hiệu điện tử từ máy tính này đến máy tính khác. Các tín hiệu điện tử đó biểu thị các giá trị dữ liệu dưới dạng các xung nhị phân (on - off). Tất cả các tín hiệu được truyền giữa các máy tính đều thuộc một dạng sóng điện từ. Tùy theo tần số của sóng điện từ có thể dùng các đường truyền vật lý khác nhau để truyền các tín hiệu. Ở đây đường truyền được kết nối có thể là dây cáp đồng trục, cáp xoắn, cáp quang, dây điện thoại, sóng vô tuyến ... Các đường truyền dữ liệu tạo nên cấu trúc của mạng. Hai khái niệm đường truyền và cấu trúc là những đặc trưng cơ bản của mạng máy tính.




*Hình 2.1: Một mô hình liên kết các máy tính trong mạng*

Với sự trao đổi qua lại giữa máy tính này với máy tính khác đã phân biệt mạng máy tính với các hệ thống thu phát một chiều như truyền hình, phát thông tin từ vệ tinh xuống các trạm thu thụ động... vì tại đây chỉ có thông tin một chiều từ nơi phát đến nơi thu mà không quan tâm đến có bao nhiêu nơi thu, có thu tốt hay không.

Đặc trưng cơ bản của đường truyền vật lý là giải thông. Giải thông của một đường chuyền chính là độ đo phạm vi tần số mà nó có thể đáp ứng được. Tốc độ truyền dữ liệu trên đường truyền còn được gọi là thông lượng của đường truyền - thường được tính bằng số lượng bit được truyền đi trong một giây (Bps). Thông lượng còn được đo bằng đơn vị khác là Baud (lấy từ tên nhà bác học - Emile Baudot). Baud biểu thị số lượng thay đổi tín hiệu trong một giây.

Ở đây Baud và Bps không phải bao giờ cũng đồng nhất. Ví dụ: nếu trên đường dây có 8 mức tín hiệu khác nhau thì mỗi mức tín hiệu tương ứng với 3 bit hay là 1 Baud tương ứng với 3 bit. Chỉ khi có 2 mức tín hiệu trong đó mỗi mức tín hiệu tương ứng với 1 bit thì 1 Baud mới tương ứng với 1 bit.

## II. Phân loại mạng máy tính

Do hiện nay mạng máy tính được phát triển khắp nơi với những ứng dụng ngày càng đa dạng cho nên việc phân loại mạng máy tính là một việc rất phức tạp. Người ta có thể chia các mạng máy tính theo khoảng cách địa lý ra làm hai loại: Mạng diện rộng và Mạng cục bộ.

- **Mạng cục bộ (Local Area Networks - LAN)** là mạng được thiết lập để liên kết các máy tính trong một khu vực như trong một toà nhà, một khu nhà.

- **Mạng diện rộng (Wide Area Networks - WAN)** là mạng được thiết lập để liên kết các máy tính của hai hay nhiều khu vực khác nhau như giữa các thành phố hay các tỉnh.

Sự phân biệt trên chỉ có tính chất ước lệ, các phân biệt trên càng trở nên khó xác định với việc phát triển của khoa học và kỹ thuật cũng như các phương tiện truyền dẫn. Tuy nhiên với sự phân biệt trên phương diện địa lý đã đưa tới việc phân biệt trong nhiều đặc tính khác nhau của hai loại mạng trên, việc nghiên cứu các phân biệt đó cho ta hiểu rõ hơn về các loại mạng.

## III. Sự phân biệt giữa mạng cục bộ và mạng diện rộng

Mạng cục bộ và mạng diện rộng có thể được phân biệt bởi: địa phương hoạt động, tốc độ đường truyền và tỷ lệ lỗi trên đường truyền, chủ quản của mạng, đường đi của thông tin trên mạng, dạng chuyển giao thông tin.

***Địa phương hoạt động*:** Liên quan đến khu vực địa lý thì mạng cục bộ sẽ là mạng liên kết các máy tính nằm ở trong một khu vực nhỏ. Khu vực có thể bao gồm một tòa nhà hay là một khu nhà... Điều đó hạn chế bởi khoảng cách đường dây cáp

được dùng để liên kết các máy tính của mạng cục bộ (Hạn chế đó còn là hạn chế của khả năng kỹ thuật của đường truyền dữ liệu). Ngược lại mạng diện rộng là mạng có khả năng liên kết các máy tính trong một vùng rộng lớn như là một thành phố, một miền, một đất nước, mạng diện rộng được xây dựng để nối hai hoặc nhiều khu vực địa lý riêng biệt.

***Tốc độ đường truyền và tỷ lệ lỗi trên đường truyền*:** Do các đường cáp của mạng cục bộ được xây dựng trong một khu vực nhỏ cho nên nó ít bị ảnh hưởng bởi tác động của thiên nhiên (như là sấm chớp, ánh sáng...). Điều đó cho phép mạng cục bộ có thể truyền dữ liệu với tốc độ cao mà chỉ chịu một tỷ lệ lỗi nhỏ. Ngược lại với mạng diện rộng do phải truyền ở những khoảng cách khá xa với những đường truyền dẫn dài có khi lên tới hàng ngàn km. Do vậy mạng diện rộng không thể truyền với tốc độ quá cao vì khi đó tỉ lệ lỗi sẽ trở nên khó chấp nhận được.

Mạng cục bộ thường có tốc độ truyền dữ liệu từ 4 đến 16 Mbps và đạt tới 100 Mbps nếu dùng cáp quang. Còn phần lớn các mạng diện rộng cung cấp đường truyền có tốc độ thấp hơn nhiều như T1 với 1.544 Mbps hay E1 với 2.048 Mbps.

(Ở đây bps (Bit Per Second) là một đơn vị trong truyền thông tương đương với 1 bit được truyền trong một giây, ví dụ như tốc độ đường truyền là 1 Mbps tức là có thể truyền tối đa 1 Megabit trong 1 giây trên đường truyền đó).

Thông thường trong mạng cục bộ tỷ lệ lỗi trong truyền dữ liệu vào khoảng $1/10^7$-$10^8$ còn trong mạng diện rộng thì tỷ lệ đó vào khoảng $1/10^6$ - $10^7$

***Chủ quản và điều hành của mạng:*** Do sự phức tạp trong việc xây dựng, quản lý, duy trì các đường truyền dẫn nên khi xây dựng mạng diện rộng người ta thường sử dụng các đường truyền được thuê từ các công ty viễn thông hay các nhà cung cấp dịch vụ truyền số liệu. Tùy theo cấu trúc của mạng những đường truyền đó thuộc cơ quan quản lý khác nhau như các nhà cung cấp đường truyền nội hạt, liên tỉnh, liên quốc gia. Các đường truyền đó phải tuân thủ các quy định của chính phủ các khu vực có đường dây đi qua như: tốc độ, việc mã hóa.

Còn đối với mạng cục bộ thì công việc đơn giản hơn nhiều, khi một cơ quan cài đặt mạng cục bộ thì toàn bộ mạng sẽ thuộc quyền quản lý của cơ quan đó.

***Đường đi của thông tin trên mạng:*** Trong mạng cục bộ thông tin được đi theo con đường xác định bởi cấu trúc của mạng. Khi người ta xác định cấu trúc của mạng thì thông tin sẽ luôn luôn đi theo cấu trúc đã xác định đó. Còn với mạng diện rộng dữ liệu cấu trúc có thể phức tạp hơn nhiều do việc sử dụng các dịch vụ truyền dữ liệu. Trong quá trình hoạt động các điểm nút có thể thay đổi đường đi của các thông tin khi phát hiện ra có trục trặc trên đường truyền hay khi phát hiện có quá nhiều thông tin cần truyền giữa hai điểm nút nào đó. Trên mạng diện rộng thông tin có thể có các con đường đi khác nhau, điều đó cho phép có thể sử dụng tối đa các năng lực của đường truyền hay nâng cao điều kiện an toàn trong truyền dữ liệu.

***Dạng chuyển giao thông tin:*** Phần lớn các mạng diện rộng hiện nay được phát triển cho việc truyền đồng thời trên đường truyền nhiều dạng thông tin khác nhau như: video, tiếng nói, dữ liệu... Trong khi đó các mạng cục bộ chủ yếu phát triển trong việc truyền dữ liệu thông thường. Điều này có thể giải thích do việc truyền các dạng thông tin như video, tiếng nói trong một khu vực nhỏ ít được quan tâm hơn như khi truyền qua những khoảng cách lớn.

Các hệ thống mạng hiện nay ngày càng phức tạp về chất lượng, đa dạng về chủng loại và phát triển rất nhanh về chất. Trong sự phát triển đó số lượng những nhà sản xuất từ phần mềm, phần cứng máy tính, các sản phẩm viễn thông cũng tăng nhanh với nhiều sản phẩm đa dạng. Chính vì vậy vai trò chuẩn hóa cũng mang những ý nghĩa quan trọng. Tại các nước các cơ quan chuẩn quốc gia đã đưa ra các những chuẩn về phần cứng và các quy định về giao tiếp nhằm giúp cho các nhà sản xuất có thể làm ra các sản phẩm có thể kết nối với các sản phẩm do hãng khác sản xuất.

Chương 3

# Mô hình truyền thông

## I. Sự cần thiết phải có mô hình truyền thông

Để một mạng máy tính trở một môi trường truyền dữ liệu thì nó cần phải có những yếu tố sau:

- Mỗi máy tính cần phải có một địa chỉ phân biệt trên mạng.
- Việc chuyển dữ liệu từ máy tính này đến máy tính khác do mạng thực hiện thông qua những quy định thống nhất gọi là giao thức của mạng.

Khi các máy tính trao đổi dữ liệu với nhau thì một quá trình truyền giao dữ liệu đã được thực hiện hoàn chỉnh. Ví dụ như để thực hiện việc truyền một file giữa một máy tính với một máy tính khác cùng được gắn trên một mạng các công việc sau đây phải được thực hiện:

- Máy tính cần truyền cần biết địa chỉ của máy nhận.
- Máy tính cần truyền phải xác định được máy tính nhận đã saün sàng nhận thông tin
- Chương trình gửi file trên máy truyền cần xác định được rằng chương trình nhận file trên máy nhận đã saün sàng tiếp nhận file.
- Nếu cấu trúc file trên hai máy không giống nhau thì một máy phải làm nhiệm vụ chuyển đổi file từ dạng này sang dạng kia.
- Khi truyền file máy tính truyền cần thông báo cho mạng biết địa chỉ của máy nhận để các thông tin được mạng đưa tới đích.

Điều trên đó cho thấy giữa hai máy tính đã có một sự phối hợp hoạt động ở mức độ cao. Bây giờ thay vì chúng ta xét cả quá trình trên như là một quá trình chung thì chúng ta sẽ chia quá trình trên ra thành một số công đoạn và mỗi công đoạn con hoạt động một cách độc lập với nhau. Ở đây chương trình truyền nhận file của mỗi máy tính được chia thành ba module là: Module truyền và nhận File, Module truyền thông và Module tiếp cận mạng. Hai module tương ứng sẽ thực hiện việc trao đổi với nhau trong đó:

- *Module truyền và nhận file* cần được thực hiện tất cả các nhiệm vụ trong các ứng dụng truyền nhận file. Ví dụ: truyền nhận thông số về file, truyền nhận

các mẫu tin của file, thực hiện chuyển đổi file sang các dạng khác nhau nếu cần. Module truyền và nhận file không cần thiết phải trực tiếp quan tâm tới việc truyền dữ liệu trên mạng như thế nào mà nhiệm vụ đó được giao cho Module truyền thông.

- *Module truyền thông* quan tâm tới việc các máy tính đang hoạt động và saün sàng trao đổi thông tin với nhau. Nó còn kiểm soát các dữ liệu sao cho những dữ liệu này có thể trao đổi một cách chính xác và an toàn giữa hai máy tính. Điều đó có nghĩa là phải truyền file trên nguyên tắc đảm bảo an toàn cho dữ liệu, tuy nhiên ở đây có thể có một vài mức độ an toàn khác nhau được dành cho từng ứng dụng. Ở đây việc trao đổi dữ liệu giữa hai máy tính không phụ thuộc vào bản chất của mạng đang liên kết chúng. Những yêu cầu liên quan đến mạng đã được thực hiện ở module thứ ba là module tiếp cận mạng và nếu mạng thay đổi thì chỉ có module tiếp cận mạng bị ảnh hưởng.

- *Module tiếp cận mạng* được xây dựng liên quan đến các quy cách giao tiếp với mạng và phụ thuộc vào bản chất của mạng. Nó đảm bảo việc truyền dữ liệu từ máy tính này đến máy tính khác trong mạng.

Như vậy thay vì xét cả quá trình truyền file với nhiều yêu cầu khác nhau như một tiến trình phức tạp thì chúng ta có thể xét quá trình đó với nhiều tiến trình con phân biệt dựa trên việc trao đổi giữa các Module tương ứng trong chương trình truyền file. Cách này cho phép chúng ta phân tích kỹ quá trình file và dễ dàng trong việc viết chương trình.

Việc xét các module một cách độc lập với nhau như vậy cho phép giảm độ phức tạp cho việc thiết kế và cài đặt. Phương pháp này được sử dụng rộng rãi trong việc xây dựng mạng và các chương trình truyền thông và được gọi là phương pháp phân tầng (layer).

Nguyên tắc của phương pháp phân tầng là:

- Mỗi hệ thống thành phần trong mạng được xây dựng như một cấu trúc nhiều tầng và đều có cấu trúc giống nhau như: số lượng tầng và chức năng của mỗi tầng.

- Các tầng nằm chồng lên nhau, dữ liệu được chỉ trao đổi trực tiếp giữa hai tầng kề nhau từ tầng trên xuống tầng dưới và ngược lại.

- Cùng với việc xác định chức năng của mỗi tầng chúng ta phải xác định mối quan hệ giữa hai tầng kề nhau. Dữ liệu được truyền đi từ tầng cao nhất của hệ thống truyền lần lượt đến tầng thấp nhất sau đó truyền qua đường nối vật lý dưới dạng các bit tới tầng thấp nhất của hệ thống nhận, sau đó dữ liệu được truyền ngược lên lần lượt đến tầng cao nhất của hệ thống nhận.

- Chỉ có hai tầng thấp nhất có liên kết vật lý với nhau còn các tầng trên cùng thứ tư chỉ có các liên kết logic với nhau. Liên kết logic của một tầng được thực hiện thông qua các tầng dưới và phải tuân theo những quy định chặt chẽ, các quy định đó được gọi giao thức của tầng.

*Hình 3.1: Mô hình phân tầng gồm N tầng*

## II. Mô hình truyền thông đơn giản 3 tầng

Nói chung trong truyền thông có sự tham gia của các thành phần: các chương trình ứng dụng, các chương trình truyền thông, các máy tính và các mạng. Các chương trình ứng dụng là các chương trình của người sử dụng được thực hiện trên máy tính và có thể tham gia vào quá trình trao đổi thông tin giữa hai máy tính. Trên một máy tính với hệ điều hành đa nhiệm (như Windows, UNIX) thường được thực hiện đồng thời nhiều ứng dụng trong đó có những ứng dụng liên quan đến mạng và các ứng dụng khác. Các máy tính được nối với mạng và các dữ liệu được trao đổi thông qua mạng từ máy tính này đến máy tính khác.

Việc gửi dữ liệu được thực hiện giữa một ứng dụng với một ứng dụng khác trên hai máy tính khác nhau thông qua mạng được thực hiện như sau: Ứng dụng gửi chuyển dữ liệu cho chương trình truyền thông trên máy tính của nó, chương trình truyền thông sẽ gửi chúng tới máy tính nhận. Chương trình truyền thông trên máy nhận sẽ tiếp nhận dữ liệu, kiểm tra nó trước khi chuyển giao cho ứng dụng đang chờ dữ liệu.

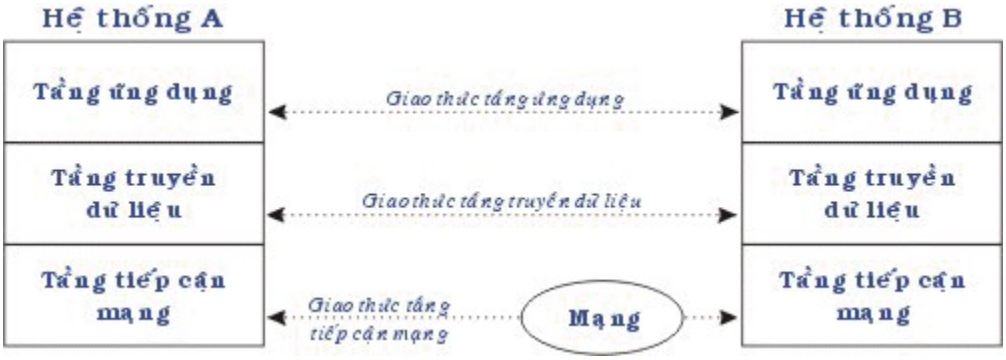
Với mô hình truyền thông đơn giản người ta chia chương trình truyền thông thành ba tầng không phụ thuộc vào nhau là: tầng ứng dụng, tầng chuyển vận và tầng tiếp cận mạng.

- ***Tầng tiếp cận mạng*** liên quan tới việc trao đổi dữ liệu giữa máy tính và mạng mà nó được nối vào. Để dữ liệu đến được đích máy tính gửi cần phải chuyển địa chỉ của máy tính nhận cho mạng và qua đó mạng sẽ chuyển các thông tin tới đích. Ngoài ra máy gửi có thể sử dụng một số phục vụ khác nhau mà mạng cung cấp như gửi ưu tiên, tốc độ cao. Trong tầng này có thể có nhiều

phần mềm khác nhau được sử dụng phụ thuộc vào các loại của mạng ví dụ như mạng chuyển mạch, mạng chuyển mạch gói, mạng cục bộ.

- ***Tầng truyền dữ liệu*** thực hiện quá trình truyền thông không liên quan tới mạng và nằm ở trên tầng tiếp cận mạng. Tầng truyền dữ liệu không quan tâm tới bản chất các ứng dụng đang trao đổi dữ liệu mà quan tâm tới làm sao cho các dữ liệu được trao đổi một cách an toàn. Tầng truyền dữ liệu đảm bảo các dữ liệu đến được đích và đến theo đúng thứ tự mà chúng được xử lý. Trong tầng truyền dữ liệu người ta phải có những cơ chế nhằm đảm bảo sự chính xác đó và rõ ràng các cơ chế này không phụ thuộc vào bản chất của từng ứng dụng và chúng sẽ phục vụ cho tất cả các ứng dụng.

- ***Tầng ứng dụng*** sẽ chứa các module phục vụ cho tất cả những ứng dụng của người sử dụng. Với các loại ứng dụng khác nhau (như là truyền file, truyền thư mục) cần các module khác nhau.




*Hình 3.2 Mô hình truyền thông 3 tầng*

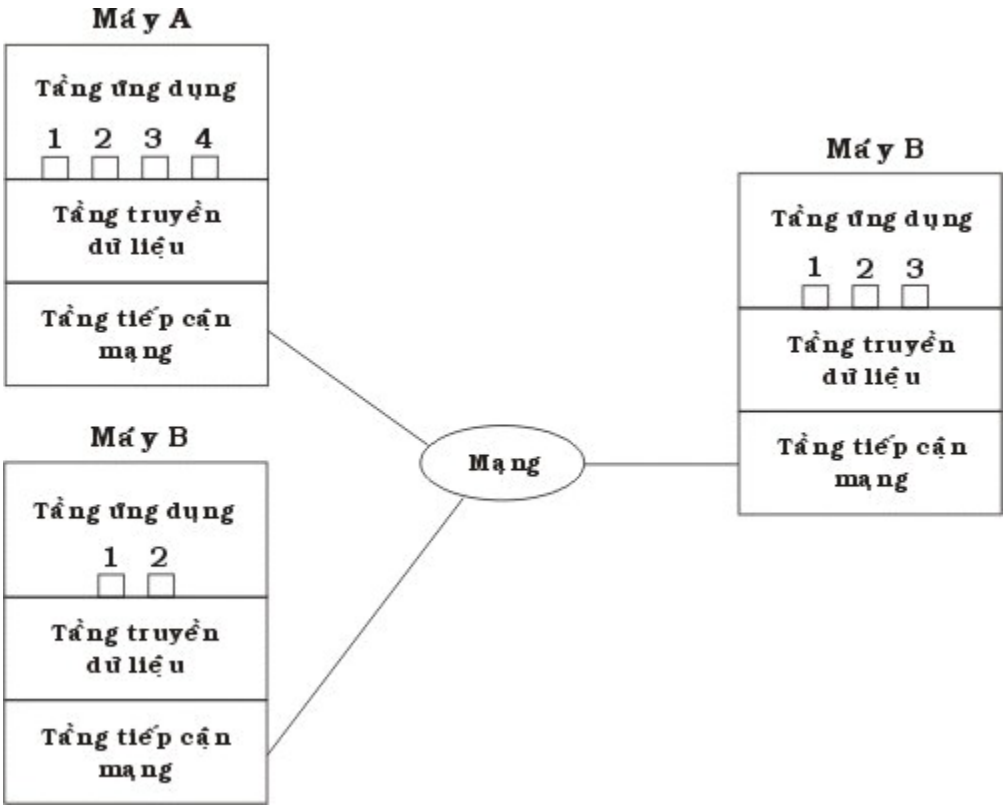
Trong một mạng với nhiều máy tính, mỗi máy tính một hay nhiều ứng dụng thực hiện đồng thời (Tại đây ta xét trên một máy tính trong một thời điểm có thể chạy nhiều ứng dụng và các ứng dụng đó có thể thực hiện đồng thời việc truyền dữ liệu qua mạng). Một ứng dụng khi cần truyền dữ liệu qua mạng cho một ứng dụng khác cần phải gọi 1 module tầng ứng dụng của chương trình truyền thông trên máy của mình, đồng thời ứng dụng kia cũng sẽ gọi 1 module tầng ứng dụng trên máy của nó. Hai module ứng dụng sẽ liên kết với nhau nhằm thực hiện các yêu cầu của các chương trình ứng dụng.

Các ứng dụng đó sẽ trao đổi với nhau thông qua mạng, tuy nhiên trong 1 thời điểm trên một máy có thể có nhiều ứng dụng cùng hoạt động và để việc truyền thông được chính xác thì các ứng dụng trên một máy cần phải có một địa chỉ riêng biệt. Rõ ràng cần có hai lớp địa chỉ:

- Mỗi máy tính trên mạng cần có một địa chỉ mạng của mình, hai máy tính trong cùng một mạng không thể có cùng địa chỉ, điều đó cho phép mạng có thể truyền thông tin đến từng máy tính một cách chính xác.

- Mỗi một ứng dụng trên một máy tính cần phải có địa chỉ phân biệt trong máy tính đo. Nó cho phép tầng truyền dữ liệu giao dữ liệu cho đúng ứng dụng đang cần. Địa chỉ đó được gọi là điểm tiếp cận giao dịch. Điều đó cho thấy mỗi một ứng dụng sẽ tiếp cận các phục vụ của tầng truyền dữ liệu một cách độc lập.

- Các module cùng một tầng trên hai máy tính khác nhau sẽ trao đổi với nhau một cách chặt chẽ theo các qui tắc xác định trước được gọi là giao thức. Một giao thức được thể hiện một cách chi tiết bởi các chức năng cần phải thực hiện như các giá trị kiểm tra lỗi, việc định dạng các dữ liệu, các quy trình cần phải thực hiện để trao đổi thông tin.




*Hình 3.3 Ví dụ mô hình truyền thông đơn giản*

Chúng ta hãy xét trong ví dụ (như hình vẽ trên): giả sử có ứng dụng có điểm tiếp cận giao dịch 1 trên máy tính A muốn gửi thông tin cho một ứng dụng khác trên máy tính B có điểm tiếp cận giao dịch 2. Ứng dụng trên máy tính A chuyển các thông tin xuống tầng truyền dữ liệu của A với yêu cầu gửi chúng cho điểm tiếp cận giao dịch 2 trên máy tính B. Tầng truyền dữ liệu máy A sẽ chuyển các thông tin xuống tầng tiếp cận mạng máy A với yêu cầu chuyển chúng cho máy tính B (Chú ý rằng mạng không cần biết địa chỉ của điểm tiếp cận giao dịch mà chỉ cần biết địa chỉ của máy tính B). Để thực hiện quá trình này, các thông tin kiểm soát cũng sẽ được truyền cùng với dữ liệu.

Đầu tiên khi ứng dụng 1 trên máy A cần gửi một khối dữ liệu nó chuyển khối đó cho tầng vận chuyển. Tầng vận chuyển có thể chia khối đó ra thành nhiều khối nhỏ phụ

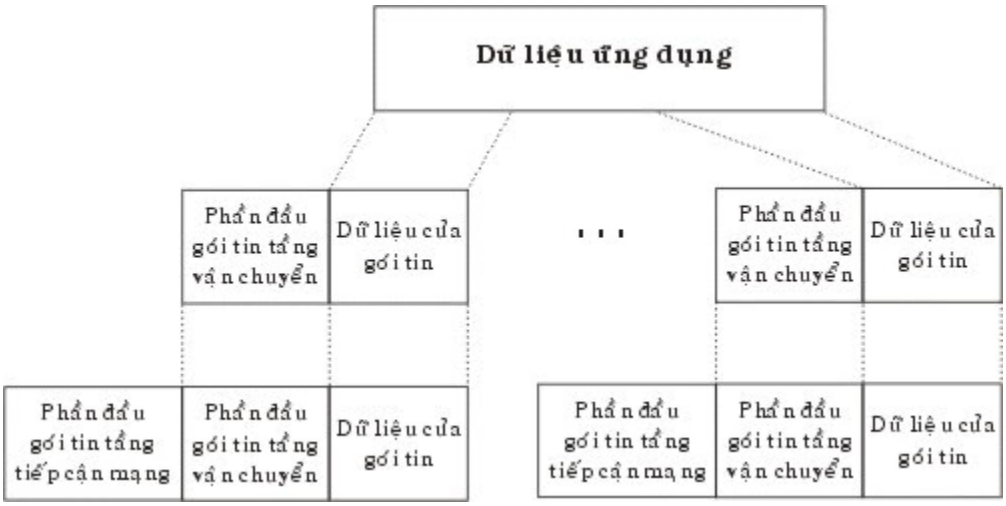
thuộc vào yêu cầu của giao thức của tầng và đóng gói chúng thành các gói tin (packet). Mỗi một gói tin sẽ được bổ sung thêm các thông tin kiểm soát của giao thức và được gọi là phần đầu (Header) của gói tin. Thông thường phần đầu của gói tin cần có:

- ***Địa chỉ của điểm tiếp cận giao dịch nơi đến* (Ở đây là 3):** khi tầng vận chuyển của máy B nhận được gói tin thì nó biết được ứng dụng nào mà nó cần giao.

- ***Số thứ tự*** của gói tin, khi tầng vận chuyển chia một khối dữ liệu ra thành nhiều gói tin thì nó cần phải đánh số thứ tự các gói tin đó. Nếu chúng đi đến đích nếu sai thứ tự thì tầng vận chuyển của máy nhận có thể phát hiện và chỉnh lại thứ tự. Ngoài ra nếu có lỗi trên đường truyền thì tầng vận chuyển của máy nhận sẽ phát hiện ra và yêu cầu gửi lại một cách chính xác.

- ***Mã sửa lỗi*:** để đảm bảo các dữ liệu được nhận một cách chính xác thì trên cơ sở các dữ liệu của gói tin tầng vận chuyển sẽ tính ra một giá trị theo một công thức có sãn và gửi nó đi trong phần đầu của gói tin. Tầng vận chuyển nơi nhận thông qua giá trị đó xác định được gói tin đó có bị lỗi trên đường truyền hay không.

Bước tiếp theo tầng vận chuyển máy A sẽ chuyển từng gói tin và địa chỉ của máy tính đích (ở đây là B) xuống tầng tiếp cận mạng với yêu cầu chuyển chúng đi. Để thực hiện được yêu cầu này tầng tiếp cận mạng cũng tạo các gói tin của mình trước khi truyền qua mạng. Tại đây giao thức của tầng tiếp cận mạng sẽ thêm các thông tin điều khiển vào phần đầu của gói tin mạng.




*Hình 3.4: Mô hình thiết lập gói tin*

Trong phần đầu gói tin mạng sẽ bao gồm địa chỉ của máy tính nhận, dựa trên địa chỉ này mạng truyền gói tin tới đích. Ngoài ra có thể có những thông số như là mức độ ưu tiên.

Như vậy thông qua mô hình truyền thông đơn giản chúng ta cũng có thể thấy được phương thức hoạt động của các máy tính trên mạng, có thể xây dựng và thay đổi các giao thức trong cùng một tầng.

## III. Các nhu cầu về chuẩn hóa đối với mạng

Trong phần trên chúng ta đã xem xét một mô hình truyền thông đơn giản, trong thực tế việc phân chia các tầng như trong mô hình trên thực sự chưa đủ. Trên thế giới hiện có một số cơ quan định chuẩn, họ đưa ra hàng loạt chuẩn về mạng tuy các chuẩn đó có tính chất khuyến nghị chứ không bắt buộc nhưng chúng rất được các cơ quan chuẩn quốc gia coi trọng.

Hai trong số các cơ quan chuẩn quốc tế là:

- **ISO (The International Standards Organization)** - Là tổ chức tiêu chuẩn quốc tế hoạt động dưới sự bảo trợ của Liên hợp Quốc với thành viên là các cơ quan chuẩn quốc gia với số lượng khoảng hơn 100 thành viên với mục đích hỗ trợ sự phát triển các chuẩn trên phạm vi toàn thế giới. Một trong những thành tựu của ISO trong lãnh vực truyền thông là mô hình hệ thống mở (Open Systems Interconnection - gọi tắt là OSI).

- **CCITT (Commité Consultatif International pour le Telegraphe et la Téléphone)** - Tổ chức tư vấn quốc tế về điện tín và điện thoại làm việc dưới sự bảo trợ của Liên Hiệp Quốc có trụ sở chính tại Geneva - Thụy sỹ. Các thành viên chủ yếu là các cơ quan bưu chính viễn thông các quốc gia. Tổ chức này có vai trò phát triển các khuyến nghị trong các lãnh vực viễn thông.

## IV. Một số mô hình chuẩn hóa

### 1. Mô hình OSI (Open Systems Interconnection)

Mô hình OSI là một cơ sở dành cho việc chuẩn hoá các hệ thống truyền thông, nó được nghiên cứu và xây dựng bởi ISO. Việc nghiên cứu về mô hình OSI được bắt đầu tại ISO vào năm 1971 với mục tiêu nhằm tới việc nối kết các sản phẩm của các hãng sản xuất khác nhau và phối hợp các hoạt động chuẩn hoá trong các lĩnh vực viễn thông và hệ thống thông tin. Theo mô hình OSI chương trình truyền thông được chia ra thành 7 tầng với những chức năng phân biệt cho từng tầng. Hai tầng đồng mức khi liên kết với nhau phải sử dụng một giao thức chung. Trong mô hình OSI có hai loại giao thức chính được áp dụng: giao thức có liên kết (connection - oriented) và giao thức không liên kết (connectionless)

- ***Giao thức có liên kết*:** trước khi truyền dữ liệu hai tầng đồng mức cần thiết lập một liên kết logic và các gói tin được trao đổi thông qua liên kết náy, việc có liên kết logic sẽ nâng cao độ an toàn trong truyền dữ liệu.

- ***Giao thức không liên kết*:** trước khi truyền dữ liệu không thiết lập liên kết logic và mỗi gói tin được truyền độc lập với các gói tin trước hoặc sau nó.

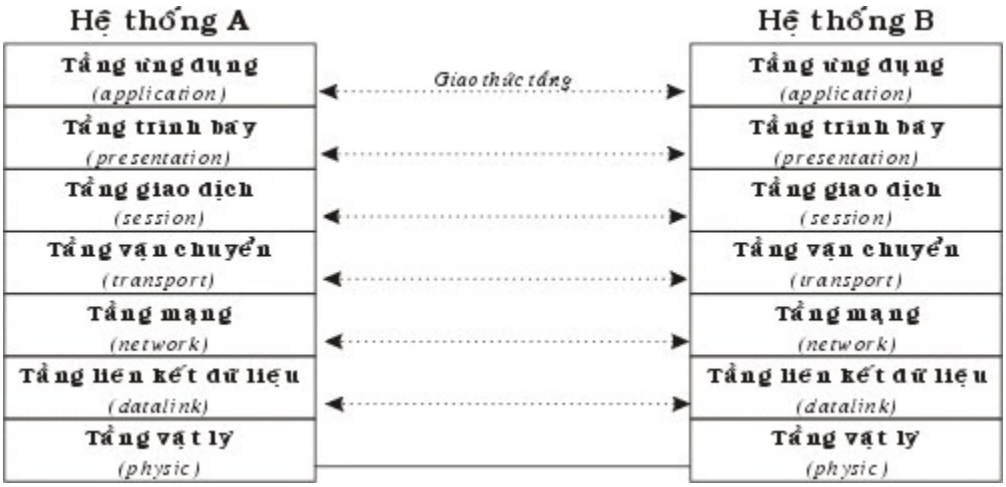
Nhiệm vụ của các tầng trong mô hình OSI:

- **Tầng ứng dụng (Application layer)**: tầng ứng dụng quy định giao diện giữa người sử dụng và môi trường OSI, nó cung cấp các phương tiện cho người sử dụng truy cập vả sử dụng các dịch vụ củ mô hình OSI.

- **Tầng trình bày (Presentation layer)**: tầng trình bày chuyển đổi các thông tin từ cú pháp người sử dụng sang cú pháp để truyền dữ liệu, ngoài ra nó có thể nén dữ liệu truyền và mã hóa chúng trước khi truyền để bảo mật.

- **Tầng giao dịch (Session layer)**: tầng giao dịch quy định một giao diện ứng dụng cho tầng vận chuyển sử dụng. Nó xác lập ánh xa giữa các tên đặt địa chỉ, tạo ra các tiếp xúc ban đầu giữa các máy tính khác nhau trên cơ sở các giao dịch truyền thông. Nó đặt tên nhất quán cho mọi thành phần muốn đối thoại riêng với nhau.

- **Tầng vận chuyển (Transport layer)**: tầng vận chuyển xác định địa chỉ trên mạng, cách thức chuyển giao gói tin trên cơ sở trực tiếp giữa hai đầu mút (end-to-end). Để bảo đảm được việc truyền ổn định trên mạng tầng vận chuyển thường đánh số các gói tin và đảm bảo chúng chuyển theo thứ tự.




*Hình 3.5: Mô hình 7 tầng OSI*

- **Tầng mạng (Network layer)**: tầng mạng có nhiệm vụ xác định việc chuyển hướng, vạch đường các gói tin trong mạng, các gói tin này có thể phải đi qua nhiều chặng trước khi đến được đích cuối cùng.

- **Tầng liên kết dữ liệu (Data link layer):** tầng liên kết dữ liệu có nhiệm vụ xác định cơ chế truy nhập thông tin trên mạng, các dạng thức chung trong các gói tin, đóng các gói tin...

- **Tầng vật lý (Phisical layer)**: tầng vật lý cung cấp phương thức truy cập vào đường truyền vật lý để truyền các dòng Bit không cấu trúc, ngoài ra nó cung cấp các chuẩn về điện, dây cáp, đầu nối, kỹ thuật nối mạch điện, điện áp, tốc độ cáp truyền dẫn, giao diện nối kết và các mức nối kết..

### 2. Mô hình SNA (Systems Netword Architecture)

Tháng 9/1973, Hãng IBM giới thiệu một kiến trúc mạng máy tính SNA (System Network Architecture). Đến năm 1977 đã có 300 trạm SNA được cài đặt. Cuối năm 1978, số lượng đã tăng lên đến 1250, rồi cứ theo đà đó cho đến nayđã có 20.000 trạm SNA đang được hoạt động. Qua con số này chúng ta có thể hình dung được mức độ quan trọng và tầm ảnh hưởng của SNA trên toàn thế giới.

Cần lưu ý rằng SNA không là một chuẩn quốc tế chính thức như OSI nhưng do vai trò to lớn của hãng IBM trên thị trường CNTT nên SNA trở thành một loại chuẩn thực tế và khá phổ biến. SNA là một đặc tả gồm rất nhiều tài liệu mô tả kiến trúc của mạng xử lý dữ liệu phân tán. Nó định nghĩa các quy tắc và các giao thức cho sự tương tác giữa các thành phần (máy tính, trạm cuối, phần mềm) trong mạng.

SNA được tổ chức xung quanh khái niệm miền (domain). Một SNA domain là một điểm điều khiển các dịch vụ hệ thống (Systems Services control point - SSCP) và nó sẽ điều khiển tất cả các tài nguyên đó, Các tài nguyên ở đây có thể là các đơn vị vật lý, các đơn vị logic, các liên kết dữ liệu và các thiết bị. Có thể ví SSCP như là "trái tim và khối óc" của SNA. Nó điều khiển SNA domain bằng cách gói các lệnh tới một đơn vị vật lý, đơn vị vật lý này sau khi nhận được lệnh sẽ quản lý tất cả các tài nguyên trực tiếp với nó. đơn vị vật lý thực sự là một "đối tác" của SSCP và chứa một tập con các khả năng của SSCP. Các Đơn vị vật lý đảm nhiệm việc quản lý của mỗi nút SNA.

SNA phân biệt giữa các nút miền con (Subarea node) và các nút ngoại vi (peripheral node).

- Một nút miền con có thể dẫn đường cho dữ liệu của người sử dụng qua toàn bộ mạng. Nó dùng địa chỉ mạng và một số hiệu đường (router suember) để xác định đường truyền đi tới nút kế tiếp trong mạng.

- Một nút ngoại vi có tính cục bộ hơn. Nó không dẫn đường giữa các nút miền con. Các nút được nối và điều khiển theo giao thức SDLC (Synchronous Data Link Control). Mỗi nút ngoại vi chỉ liên lạc được với nút miền con mà nó nối vào.

Mạng SNA dựa trên cơ chế phân tầng, trước đây thì 2 hệ thống ngang hàng không được trao đổi trực tiếp. Sau này phát triển thành SNA mở rộng: Lúc này hai tầng ngang hàng nhau có thể trao đổi trực tiếp. Với 6 tầng có tên gọi và chức năng tất như sau:

**Tầng quản trị chức năng SNA (SNA Function Manegement)** Tầng này thật ra có thể chia tầng này làm hai tầng như sau:

**Tầng dịch vụ giao tác (Transaction)** cung cấp các dịch vụ ứng dụng đến người dùng một mạng SNA. Những dịch vụ đó như : DIA cung cấp các tài liệu phân bố giữa các hệ thống văn phòng, SNA DS (văn phòng dịch vụ phân phối) cho việc truyền thông bất đồng bộ giữa các ứng dụng phân tán và hệ thống văn phòng. Tầng dịch vụ giao tác cũng cung cấp các dịch vụ và cấu hình, các dịch vụ quản lý để điều khiển các hoạt động mạng.

**Tầng dịch vụ trình diễn (Presentation Services):** tầng này thì liên quan với sự hiển thị các ứng dụng, người sử dụng đầu cuối và các dữ liệu hệ thống. Tầng này cũng định nghĩa các giao thức cho việc truyền thông giữa các chương trình và điều khiển truyền thông ở mức hội thoại.

**Tầng kiểm soát luồng dữ liệu (Data flow control)** tầng này cung cấp các dịch vụ điều khiểnluồng lưu thông cho các phiên từ logic này đến đơn vị logic khác (LU - LU). Nó thực hiện điều này bằng cách gán các số trình tự, các yêu cầu và đáp ứng, thực hiện các giao thức yêu cầu về đáp ứng giao dịch và hợp tác giữa các giao dịch gởi và nhận. Nói chung nó yểm trợ phương thức khai thác hai chiều đồng thời (Full duplex).

**Tầng kiểm soát truyền (Transmission control):** Tầng này cung cấp các điều khiển cơ bản của các phần tài nguyên truyền trong mạng, bằng cách xác định số trình tự nhận được, và quản lý việc theo dõi mức phiên. Tầng này cũng hỗ trợ cho việc mã hóa dữ liệu và cung cấp hệ thống hỗ trợ cho các nút ngoại vi.

**Tầng kiểm soát đường dẫn (Path control):** Tầng này cung cấp các giao thức để tìm đường cho một gói tin qua mạng SNA và để kết nối với các mạng SNA khác, đồng thời nó cũng kiểm soát các đường truyền này.

**Tầng kiểm soát liên kết dữ liệu (Data Link Control):** Tầng này cung cấp các giao thức cho việc truyền các gói tin thông qua đường truyền vật lý giữa hai node và cũng cung cấp các điều khiển lưu thông và phục hồi lỗi, các hỗ trợ cho tầng này là các giao thức SDLC, System/370, X25, IEEE 802.2 và 802.5.

**Tầng kiểm soát vật lý (Physical control):** Tầng này cung cấp một giao diện vật lý cho bất cứ môi trường truyền thông nào mà gắn với nó. Tầng nào định nghĩa các đặc trưng của tín hiệu cần để thiết lập, duy trì và kết thúc các đường nối vật lý cho việc hỗ trợ kết nối.

| SNA | | OSI |
|---|---|---|
| Tầng quản trị chức năng SNA (SNA Function Management) | (Transaction) | Tầng ứng dụng (application) |
| | (Presentation Services) | Tầng trình bày (presentation) |
| Tầng kiểm soát luồng dữ liệu (Data flow control) | | Tầng giao dịch (session) |
| Tầng kiểm soát truyền (Transmission control) | | Tầng vận chuyển (transport) |
| Tầng kiểm soát đường dẫn (Path control) | | Tầng mạng (network) |
| Tầng kiểm soát liên kết dữ liệu (Data Link Control) | | Tầng liên kết dữ liệu (datalink) |
| Tầng kiểm soát vật lý (Physical control) | | Tầng vật lý (physic) |

*Hình 3.6: Tương ứng các tầng các kiến trúc SNI và OSI*

**Chương 4**

# Mô hình kết nối các hệ thống mở

# Open Systems Interconection

Việc nghiên cứu về OSI được bắt đầu tại ISO vào năm 1971 với các mục tiêu nhằm nối kết các sản phẩm của các hãng sản xuất khác. Ưu điểm chính của OSI là ở chỗ nó hứa hẹn giải pháp cho vấn đề truyền thông giữa các máy tính không giống nhau. Hai hệ thống, dù có khác nhau đều có thể truyền thông với nhau một các hiệu quả nếu chúng đảm bảo những điều kiện chung sau đây:

Chúng cài đặt cùng một tập các chức năng truyền thông.

Các chức năng đó được tổ chức thành cùng một tập các tầng. các tầng đồng mức phải cung cấp các chức năng như nhau.

Các tầng đồng mức khi trao đổi với nhau sử dụng chung một giao thức

Mô hình OSI tách các mặt khác nhau của một mạng máy tính thành bảy tầng theo mô hình phân tầng. Mô hình OSI là một khung mà các tiêu chuẩn lập mạng khác nhau có thể khớp vào. Mô hình OSI định rõ các mặt nào của hoạt động của mạng có thể nhằm đến bởi các tiêu chuẩn mạng khác nhau. Vì vậy, theo một nghĩa nào đó, mô hình OSI là một loại tiêu chuẩn của các chuẩn.

## I. Nguyên tắc sử dụng khi định nghĩa các tầng hệ thống mở:

Sau đây là các nguyên tắc mà ISO quy định dùng trong quá trình xây dựng mô hình OSI

- Không định nghĩa quá nhiều tầng để việc xác định và ghép nối các tầng không quá phức tạp.
- Tạo các ranh giới các tầng sao cho việc giải thích các phục vụ và số các tương tác qua lại hai tầng là nhỏ nhất.
- Tạo các tầng riêng biệt cho các chức năng khác biệt nhau hoàn toàn về kỹ thuật sử dụng hoặc quá trình thực hiên.
- Các chức năng giống nhau được đặt trong cùng một tầng.
- Lựa chọn ranh giới các tầng tại các điểm mà những thử nghiệm trong quá khứ thành công.

- Các chức năng được xác định sao cho chúng có thể dễ dàng xác định lại, và các nghi thức của chúng có thể thay đổi trên mọi hướng.

- Tạo ranh giới các tầng mà ở đó cần có những mức độ trừu tượng khác nhau trong việc sử dụng số liệu.

- Cho phép thay đổi các chức năng hoặc giao thức trong tầng không ảnh hưởng đến các tầng khác.

- Tạo các ranh giới giữa mỗi tầng với tầng trên và dưới nó.

**II. Các giao thức trong mô hình OSI**

Trong mô hình OSI có hai loại giao thức chính được áp dụng: giao thức có liên kết (connection - oriented) và giao thức không liên kết (connectionless).

- *Giao thức có liên kết*: trước khi truyền dữ liệu hai tầng đồng mức cần thiết lập một liên kết logic và các gói tin được trao đổi thông qua liên kết náy, việc có liên kết logic sẽ nâng cao độ an toàn trong truyền dữ liệu.

- *Giao thức không liên kết*: trước khi truyền dữ liệu không thiết lập liên kết logic và mỗi gói tin được truyền độc lập với các gói tin trước hoặc sau nó.

Như vậy với giao thức có liên kết, quá trình truyền thông phải gồm 3 giai đoạn phân biệt:

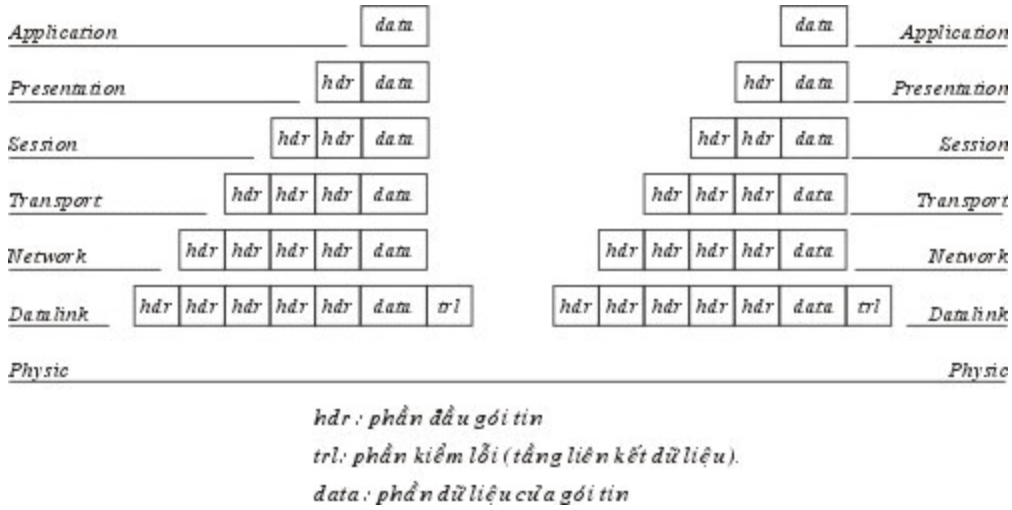
- *Thiết lập liên kết (logic):* hai thực thể đồng mức ở hai hệ thống thương lượng với nhau về tập các tham số sẽ sử dụng trong giai đoạn sau (truyền dữ liệu).

- *Truyền dữ liệu*: dữ liệu được truyền với các cơ chế kiểm soát và quản lý kèm theo (như kiểm soát lỗi, kiểm soát luồng dữ liệu, cắt/hợp dữ liệu...) để tăng cường độ tin cậy và hiệu quả của việc truyền dữ liệu.

- *Hủy bỏ liên kết (logic):* giải phóng tài nguyên hệ thống đã được cấp phát cho liên kết để dùng cho liên kết khác.

Đối với giao thức không liên kết thì chỉ có duy nhất một giai đoạn truyền dữ liệu mà thôi.

Gói tin của giao thức: Gói tin (Packet) được hiểu như là một đơn vị thông tin dùng trong việc liên lạc, chuyển giao dữ liệu trong mạng máy tính. Những thông điệp (message) trao đổi giữa các máy tính trong mạng, được tạo dạng thành các gói tin ở máy nguồn. Và những gói tin này khi đích sẽ được kết hợp lại thành thông điệp ban đầu. Một gói tin có thể chứa đựng các yêu cầu phục vụ, các thông tin điều khiển và dữ liệu.




*Hình 4.1: Phương thức xác lập các gói tin trong mô hình OSI*

Trên quan điểm mô hình mạng phân tầng tầng mỗi tầng chỉ thực hiện một chức năng là nhận dữ liệu từ tầng bên trên để chuyển giao xuống cho tầng bên dưới và ngược lại. Chức năng này thực chất là gắn thêm và gỡ bỏ phần đầu (header) đối với các gói tin trước khi chuyển nó đi. Nói cách khác, từng gói tin bao gồm phần đầu (header) và phần dữ liệu. Khi đi đến một tầng mới gói tin sẽ được đóng thêm một phần đầu đề khác và được xem như là gói tin của tầng mới, công việc trên tiếp diễn cho tới khi gói tin được truyền lên đường dây mạng để đến bên nhận.

Tại bên nhận các gói tin được gỡ bỏ phần đầu trên từng tầng tương ứng và đây cũng là nguyên lý của bất cứ mô hình phân tầng nào.

***Chú ý:*** Trong mô hình OSI phần kiểm lỗi của gói tin tầng liên kết dữ liệu đặt ở cuối gói tin

## III. Các chức năng chủ yếu của các tầng của mô hình OSI.

### Tầng 1: Vật lý (Physical)

Tầng vật lý (Physical layer) là tầng dưới cùng của mô hình OSI là. Nó mô tả các đặc trưng vật lý của mạng: Các loại cáp được dùng để nối các thiết bị, các loại đầu nối được dùng , các dây cáp có thể dài bao nhiêu v.v... Mặt khác các tầng vật lý cung cấp các đặc trưng điện của các tín hiệu được dùng để khi chuyển dữ liệu trên cáp từ một máy này đến một máy khác của mạng, kỹ thuật nối mạch điện, tốc độ cáp truyền dẫn.

Tầng vật lý không qui định một ý nghĩa nào cho các tín hiệu đó ngoài các giá trị nhị phân 0 và 1. Ở các tầng cao hơn của mô hình OSI ý nghĩa của các bit được truyền ở tầng vật lý sẽ được xác định.

***Ví dụ:*** Tiêu chuẩn Ethernet cho cáp xoắn đôi 10 baseT định rõ các đặc trưng điện của cáp xoắn đôi, kích thước và dạng của các đầu nối, độ dài tối đa của cáp.

Khác với các tầng khác, tầng vật lý là không có gói tin riêng và do vậy không có phần đầu (header) chứa thông tin điều khiển, dữ liệu được truyền đi theo dòng bit. Một giao thức tầng vật lý tồn tại giữa các tầng vật lý để quy định về phương thức truyền (đồng bộ, phi đồng bộ), tốc độ truyền.

Các giao thức được xây dựng cho tầng vật lý được phân chia thành phân chia thành hai loại giao thức sử dụng phương thức truyền thông dị bộ (asynchronous) và phương thức truyền thông đồng bộ (synchronous).

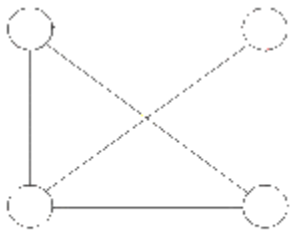
- *Phương thức truyền dị bộ*: không có một tín hiệu quy định cho sự đồng bộ giữa các bit giữa máy gửi và máy nhận, trong quá trình gửi tín hiệu máy gửi sử dụng các bit đặc biệt START và STOP được dùng để tách các xâu bit biểu diễn các ký tự trong dòng dữ liệu cần truyền đi. Nó cho phép một ký tự được truyền đi bất kỳ lúc nào mà không cần quan tâm đến các tín hiệu đồng bộ trước đó.

- *Phương thức truyền đồng bộ*: sử dụng phương thức truyền cần có đồng bộ giữa máy gửi và máy nhận, nó chèn các ký tự đặc biệt như SYN (Synchronization), EOT (End Of Transmission) hay đơn giản hơn, một cái "cờ " (flag) giữa các dữ liệu của máy gửi để báo hiệu cho máy nhận biết được dữ liệu đang đến hoặc đã đến.

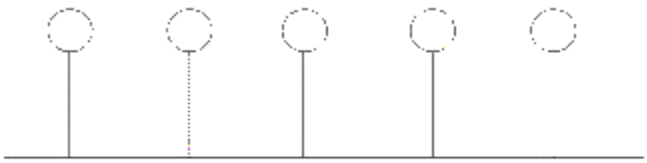
### Tầng 2: Liên kết dữ liệu (Data link)

Tầng liên kết dữ liệu (data link layer) là tầng mà ở đó ý nghĩa được gán cho các bít được truyền trên mạng. Tầng liên kết dữ liệu phải quy định được các dạng thức, kích thước, địa chỉ máy gửi và nhận của mỗi gói tin được gửi đi. Nó phải xác định cơ chế truy nhập thông tin trên mạng và phương tiện gửi mỗi gói tin sao cho nó được đưa đến cho người nhận đã định.

Tầng liên kết dữ liệu có hai phương thức liên kết dựa trên cách kết nối các máy tính, đó là phương thức "một điểm - một điểm" và phương thức "một điểm - nhiều điểm". Với phương thức "một điểm - một điểm" các đường truyền riêng biệt được thiết lập để nối các cặp máy tính lại với nhau. Phương thức "một điểm - nhiều điểm " tất cả các máy phân chia chung một đường truyền vật lý.



*một điểm - một điểm*



*một điểm - nhiều điểm*

*Hình 4.2: Các đường truyền kết nối kiểu "một điểm - một điểm" và "một điểm - nhiều điểm".*

Tầng liên kết dữ liệu cũng cung cấp cách phát hiện và sửa lỗi cơ bản để đảm bảo cho dữ liệu nhận được giống hoàn toàn với dữ liệu gửi đi. Nếu một gói tin có lỗi không sửa được, tầng liên kết dữ liệu phải chỉ ra được cách thông báo cho nơi gửi biết gói tin đó có lỗi để nó gửi lại.

Các giao thức tầng liên kết dữ liệu chia làm 2 loại chính là các giao thức hướng ký tư và các giao thức hướng bit. Các giao thức hướng ký tự được xây dựng dựa trên các ký tự đặc biệt của một bộ mã chuẩn nào đó (như ASCII hay EBCDIC), trong khi đó các giao thức hướng bit lại dùng các cấu trúc nhị phân (xâu bit) để xây dựng các phần tử của giao thức (đơn vị dữ liệu, các thủ tục.) và khi nhận, dữ liệu sẽ được tiếp nhận lần lượt từng bit một.

### Tầng 3: Mạng (Network)

Tầng mạng (network layer) nhắm đến việc kết nối các mạng với nhau bằng cách tìm đường (routing) cho các gói tin từ một mạng này đến một mạng khác. Nó xác định việc chuyển hướng, vạch đường các gói tin trong mạng, các gói này có thể phải đi qua nhiều chặng trước khi đến được đích cuối cùng. Nó luôn tìm các tuyến truyền thông không tắc nghẽn để đưa các gói tin đến đích.

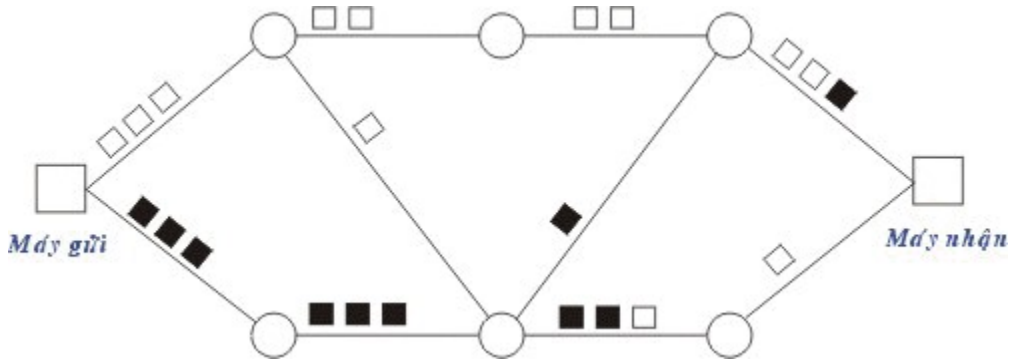
Tầng mạng cung các các phương tiện để truyền các gói tin qua mạng, thậm chí qua một mạng của mạng (network of network). Bởi vậy nó cần phải đáp ứng với nhiều kiểu mạng và nhiều kiểu dịch vụ cung cấp bởi các mạng khác nhau. hai chức năng chủ yếu của tầng mạng là chọn đường (routing) và chuyển tiếp (relaying). Tầng mạng là quan trọng nhất khi liên kết hai loại mạng khác nhau như mạng Ethernet với mạng Token Ring khi đó phải dùng một bộ tìm đường (quy định bởi tầng mạng) để chuyển các gói tin từ mạng này sang mạng khác và ngược lại.

Đối với một mạng chuyển mạch gói (packet - switched network) - gồm tập hợp các nút chuyển mạch gói nối với nhau bởi các liên kết dữ liệu. Các gói dữ liệu được truyền từ một hệ thống mở tới một hệ thống mở khác trên mạng phải được chuyển qua một chuỗi các nút. Mỗi nút nhận gói dữ liệu từ một đường vào (incoming link) rồi chuyển tiếp nó tới một đường ra (outgoing link) hướng đến đích của dữ liệu. Như vậy ở mỗi nút trung gian nó phải thực hiện các chức năng chọn đường và chuyển tiếp.

Việc chọn đường là sự lựa chọn một con đường để truyền một đơn vị dữ liệu (một gói tin chẳng hạn) từ trạm nguồn tới trạm đích của nó. Một kỹ thuật chọn đường phải thực hiện hai chức năng chính sau đây:

- Quyết định chọn đường tối ưu dựa trên các thông tin đã có về mạng tại thời điểm đó thông qua những tiêu chuẩn tối ưu nhất định.

- Cập nhật các thông tin về mạng, tức là thông tin dùng cho việc chọn đường, trên mạng luôn có sự thay đổi thường xuyên nên việc cập nhật là việc cần thiết.




*Hình 4. 3: Mô hình chuyển vận các gói tin trong mạng chuyển mạch gói*

Người ta có hai phương thức đáp ứng cho việc chọn đường là phương thức xử lý tập trung và xử lý tại chỗ.

- *Phương thức chọn đường xử lý tập trung* được đặc trưng bởi sự tồn tại của một (hoặc vài) trung tâm điều khiển mạng, chúng thực hiện việc lập ra các bảng đường đi tại từng thời điểm cho các nút và sau đó gửi các bảng chọn đường tới từng nút dọc theo con đường đã được chọn đó. Thông tin tổng thể của mạng cần dùng cho việc chọn đường chỉ cần cập nhập và được cất giữ tại trung tâm điều khiển mạng.

- *Phương thức chọn đường xử lý tại chỗ* được đặc trưng bởi việc chọn đường được thực hiện tại mỗi nút của mạng. Trong từng thời điểm, mỗi nút phải duy trì các thông tin của mạng và tự xây dựng bảng chọn đường cho mình. Như vậy các thông tin tổng thể của mạng cần dùng cho việc chọn đường cần cập nhập và được cất giữ tại mỗi nút.

Thông thường các thông tin được đo lường và sử dụng cho việc chọn đường bao gồm:

- Trạng thái của đường truyền.

- Thời gian trễ khi truyền trên mỗi đường dẫn.

- Mức độ lưu thông trên mỗi đường.

- Các tài nguyên khả dụng của mạng.

Khi có sự thay đổi trên mạng (ví dụ thay đổi về cấu trúc của mạng do sự cố tại một vài nút, phục hồi của một nút mạng, nối thêm một nút mới... hoặc thay đổi về mức độ lưu thông) các thông tin trên cần được cập nhật vào các cơ sở dữ liệu về trạng thái của mạng.

Hiện nay khi nhu cầu truyền thông đa phương tiện (tích hợp dữ liệu văn bản, đồ hoạ, hình ảnh, âm thanh) ngày càng phát triển đòi hỏi các công nghệ truyền dẫn tốc độ cao nên việc phát triển các hệ thống chọn đường tốc độ cao đang rất được quan tâm.

### Tầng 4: Vận chuyển (Transport)

Tầng vận chuyển cung cấp các chức năng cần thiết giữa tầng mạng và các tầng trên. nó là tầng cao nhất có liên quan đến các giao thức trao đổi dữ liệu giữa các hệ thống mở. Nó cùng các tầng dưới cung cấp cho người sử dụng các phục vụ vận chuyển.

Tầng vận chuyển (transport layer) là tầng cơ sở mà ở đó một máy tính của mạng chia sẻ thông tin với một máy khác. Tầng vận chuyển đồng nhất mỗi trạm bằng một địa chỉ duy nhất và quản lý sự kết nối giữa các trạm. Tầng vận chuyển cũng chia các gói tin lớn thành các gói tin nhỏ hơn trước khi gửi đi. Thông thường tầng vận chuyển đánh số các gói tin và đảm bảo chúng chuyển theo đúng thứ tự.

Tầng vận chuyển là tầng cuối cùng chịu trách nhiệm về mức độ an toàn trong truyền dữ liệu nên giao thức tầng vận chuyển phụ thuộc rất nhiều vào bản chất của tầng mạng. Người ta chia giao thức tầng mạng thành các loại sau:

- Mạng loại A: Có tỷ suất lỗi và sự cố có báo hiệu chấp nhận được (tức là chất lượng chấp nhận được). Các gói tin được giả thiết là không bị mất. Tầng vận chuyển không cần cung cấp các dịch vụ phục hồi hoặc sắp xếp thứ tự lại.

- Mạng loại B: Có tỷ suất lỗi chấp nhận được nhưng tỷ suất sự cố có báo hiệu lại không chấp nhận được. Tầng giao vận phải có khả năng phục hồi lại khi xẩy ra sự cố.

- Mạng loại C: Có tỷ suất lỗi không chấp nhận được (không tin cậy) hay là giao thức không liên kết. Tầng giao vận phải có khả năng phục hồi lại khi xảy ra lỗi và sắp xếp lại thứ tự các gói tin.

Trên cơ sở loại giao thức tầng mạng chúng ta có 5 lớp giao thức tầng vận chuyển đó là:

- *Giao thức lớp 0 (Simple Class - lớp đơn giản)*: cung cấp các khả năng rất đơn giản để thiết lập liên kết, truyền dữ liệu và hủy bỏ liên kết trên mạng "có liên kết" loại A. Nó có khả năng phát hiện và báo hiệu các lỗi nhưng không có khả năng phục hồi.

- *Giao thức lớp 1 (Basic Error Recovery Class - Lớp phục hồi lỗi cơ bản)* dùng với các loại mạng B, ở đây các gói tin (TPDU) được đánh số. Ngoài ra giao thức còn có khả năng báo nhận cho nơi gửi và truyền dữ liệu khẩn. So với giao thức lớp 0 giao thức lớp 1 có thêm khả năng phục hồi lỗi.

- *Giao thức lớp 2 (Multiplexing Class - lớp dồn kênh)* là một cải tiến của lớp 0 cho phép dồn một số liên kết chuyển vận vào một liên kết mạng duy nhất, đồng thời có thể kiểm soát luồng dữ liệu để tránh tắc nghẽn. Giao thức lớp 2 không có khả năng phát hiện và phục hồi lỗi. Do vậy nó cần đặt trên một tầng mạng loại A.

- *Giao thức lớp 3 (Error Recovery and Multiplexing Class - lớp phục hồi lỗi cơ bản và dồn kênh)* là sự mở rộng giao thức lớp 2 với khả năng phát hiện và phục hồi lỗi, nó cần đặt trên một tầng mạng loại B.

- *Giao thức lớp 4 (Error Detection and Recovery Class - Lớp phát hiện và phục hồi lỗi)* là lớp có hầu hết các chức năng của các lớp trước và còn bổ sung thêm một số khả năng khác để kiểm soát việc truyền dữ liệu.

### Tầng 5: Giao dịch (Session)

Tầng giao dịch (session layer) thiết lập "các giao dịch" giữa các trạm trên mạng, nó đặt tên nhất quán cho mọi thành phần muốn đối thoại với nhau và lập ánh xa giữa các tên với địa chỉ của chúng. Một giao dịch phải được thiết lập trước khi dữ liệu được truyền trên mạng, tầng giao dịch đảm bảo cho các giao dịch được thiết lập và duy trì theo đúng qui định.

Tầng giao dịch còn cung cấp cho người sử dụng các chức năng cần thiết để quản trị các giao dịnh ứng dụng của họ, cụ thể là:

- Điều phối việc trao đổi dữ liệu giữa các ứng dụng bằng cách thiết lập và giải phóng (một cách lôgic) các phiên (hay còn gọi là các hội thoại - dialogues)

- Cung cấp các điểm đồng bộ để kiểm soát việc trao đổi dữ liệu.

- Áp đặt các qui tắc cho các tương tác giữa các ứng dụng của người sử dụng.

- Cung cấp cơ chế "lấy lượt" (nắm quyền) trong quá trình trao đổi dữ liệu.

Trong trường hợp mạng là hai chiều luân phiên thì nẩy sinh vấn đề: hai người sử dụng luân phiên phải "lấy lượt" để truyền dữ liệu. Tầng giao dịch duy trì tương tác luân phiên bằng cách báo cho mỗi người sử dụng khi đến lượt họ được truyền dữ liệu. Vấn đề đồng bộ hóa trong tầng giao dịch cũng được thực hiện như cơ chế kiểm tra/phục hồi, dịch vụ này cho phép người sử dụng xác định các điểm đồng bộ hóa trong dòng dữ liệu đang chuyển vận và khi cần thiết có thể khôi phục việc hội thoại bắt đầu từ một trong các điểm đó

Ở một thời điểm chỉ có một người sử dụng đó quyền đặc biệt được gọi các dịch vụ nhất định của tầng giao dịch, việc phân bổ các quyền này thông qua trao đổi thẻ bài (token). Ví dụ: Ai có được token sẽ có quyền truyền dữ liệu, và khi người giữ token trao token cho người khác thi cũng có nghĩa trao quyền truyền dữ liệu cho người đó.

Tầng giao dịch có các hàm cơ bản sau:

- *Give Token* cho phép người sử dụng chuyển một token cho một người sử dụng khác của một liên kết giao dịch.
- *Please Token* cho phép một người sử dụng chưa có token có thể yêu cầu token đó.
- *Give Control* dùng để chuyển tất cả các token từ một người sử dụng sang một người sử dụng khác.

### Tầng 6: Trình bày (Presentation)

Trong giao tiếp giữa các ứng dụng thông qua mạng với cùng một dữ liệu có thể có nhiều cách biểu diễn khác nhau. Thông thường dạng biểu diễn dùng bởi ứng dụng nguồn và dạng biểu diễn dùng bởi ứng dụng đích có thể khác nhau do các ứng dụng được chạy trên các hệ thống hoàn toàn khác nhau (như hệ máy Intel và hệ máy Motorola). Tầng trình bày (Presentation layer) phải chịu trách nhiệm chuyển đổi dữ liệu gửi đi trên mạng từ một loại biểu diễn này sang một loại khác. Để đạt được điều đó nó cung cấp một dạng biểu diễn chung dùng để truyền thông và cho phép chuyển đổi từ dạng biểu diễn cục bộ sang biểu diễn chung và ngược lại.

Tầng trình bày cũng có thể được dùng kĩ thuật mã hóa để xáo trộn các dữ liệu trước khi được truyền đi và giải mã ở đầu đến để bảo mật. Ngoài ra tầng biểu diễn cũng có thể dùng các kĩ thuật nén sao cho chỉ cần một ít byte dữ liệu để thể hiện thông tin khi nó được truyền ở trên mạng, ở đầu nhận, tầng trình bày bung trở lại để được dữ liệu ban đầu.

### Tầng 7: Ứng dụng (Application)

Tầng ứng dụng (Application layer) là tầng cao nhất của mô hình OSI, nó xác định giao diện giữa người sử dụng và môi trường OSI và giải quyết các kỹ thuật mà các chương trình ứng dụng dùng để giao tiếp với mạng.

Để cung cấp phương tiện truy nhập môi trường OSI cho các tiến trình ứng dụng, Người ta thiết lập các thực thể ứng dụng (AE), các thực thể ứng dụng sẽ gọi đến các phần tử dịch vụ ứng dụng (Application Service Element - viết tắt là ASE) của chúng. Mỗi thực thể ứng dụng có thể gồm một hoặc nhiều các phần tử dịch vụ ứng dụng. Các phần tử dịch vụ ứng dụng được phối hợp trong môi trường của thực thể ứng dụng thông qua các liên kết (association) gọi là đối tượng liên kết đơn (Single Association Object - viết tắt là SAO). SAO điều khiển việc truyền thông trong suốt vòng đời của liên kết đó cho phép tuần tự hóa các sự kiện đến từ các ASE thành tố của nó.

**Chương 5**

# Các đặc tính kỹ thuật của mạng cục bộ

Trên thực tế mạng cục bộ là một hệ thống truyền dữ liệu giữa các máy tính với một khoảng cách tương đối hẹp, điều đó cho phép có những lựa chọn đa dạng về thiết bị . Tuy nhiên những lựa chọn đa dạng này lại bị hạn chế bởi các đặc tính kỹ thuật của mạng cục bộ, đó làø tập hợp các quy tắc chuẩn đã được quy ước mà tất cả các thực thể tham gia truyền thông trên mạng phải tuân theo để đảm bảo cho mạng hoạt động tốt. Các đặc tính chính của mạng cục bộ mà chúng ta nói tới sau đây là:

- Cấu trúc của mạng (hay topology của mạng mà qua đó thể hiện cách nối các mạng máy tính với nhau ra sao).
- Các nghi thức truyền dữ liệu trên mạng (các thủ tục hướng dẫn trạm làm việc làm thế nào và lúc nào có thể thâm nhập vào đường dây cáp để gửi các gói thông tin ).
- Các loại đường truyền và các chuẩn của chúng .
- Các phương thức tín hiệu

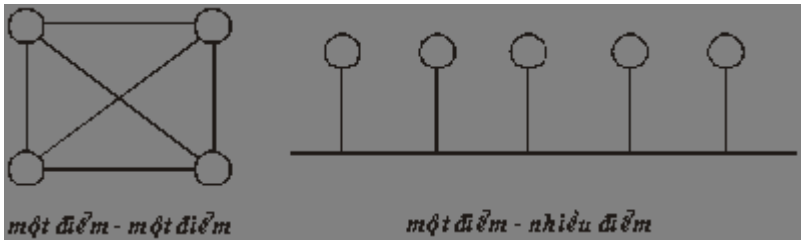
## I. Cấu trúc của mạng (Topology)

Hình trạng của mạng cục bộ thể hiện qua cấu trúc hay hình dáng hình học cuả các đường dây cáp mạng dùng để liên kết các máy tính thuộc mạng với nhau. Các mạng cục bộ thường hoạt động dựa trên cấu trúc đã định saün liên kết các máy tính và các thiết bị có liên quan.

Trước hết chúng ta xem xét hai phương thức nối mạng chủ yếu được sử dụng trong việc liên kết các máy tính là "một điểm - một điểm" và "một điểm - nhiều điểm ".

Với phương thức "một điểm - một điểm" các đường truyền riêng biệt được thiết lập để nối các cặp máy tính lại với nhau. Mỗi máy tính có thể truyền và nhận trực tiếp dữ liệu hoặc có thể làm trung gian như lưu trữ những dữ liệu mà nó nhận được rồi sau đó chuyển tiếp dữ liệu đi cho một máy khác để dữ liệu đó đạt tới đích.

Theo phương thức "một điểm - nhiều điểm " tất cả các trạm phân chia chung một đường truyền vật lý. Dữ liệu được gửi đi từ một máy tính sẽ có thể được tiếp nhận bởi tất cả các máy tính còn lại, bởi vậy cần chỉ ra địa chỉ đích của dữ liệu để mỗi máy tính căn cứ vào đó kiểm tra xem dữ liệu có phải dành cho mình không nếu đúng thì nhận còn nếu không thì bỏ qua.




*Hình 5.1: Các phương thức liên kết mạng*

Tùy theo cấu trúc của mỗi mạng chúng sẽ thuộc vào một trong hai phương thức nối mạng và mỗi phương thức nối mạng sẽ có những yêu cầu khác nhau về phần cứng và phần mềm.

## II. Những cấu trúc chính của mạng cục bộ

### 1. Dạng đường thẳng (Bus)

Trong dạng đường thẳng các máy tính đều được nối vào một đường dây truyền chính (bus). Đường truyền chính này được giới hạn hai đầu bởi một loại đầu nối đặc biệt gọi là *terminator* (dùng để nhận biết là đầu cuối để kết thúc đường truyền tại đây). Mỗi trạm được nối vào bus qua một đầu nối chữ T (T_connector) hoặc một bộ thu phát (transceiver). Khi một trạm truyền dữ liệu, tín hiệu được truyền trên cả hai chiều của đường truyền theo từng gói một, mỗi gói đều phải mang địa chỉ trạm đích. Các trạm khi thấy dữ liệu đi qua nhận lấy, kiểm tra, nếu đúng với địa chỉ của mình thì nó nhận lấy còn nếu không phải thì bỏ qua.

Sau đây là vài thông số kỹ thuật của topology bus. Theo chuẩn IEEE 802.3 (cho mạng cục bộ) với cách đặt tên qui ước theo thông số: tốc độ truyền tính hiệu (1,10 hoặc 100 Mb/s); BASE (nếu là Baseband) hoặc BROAD (nếu là Broadband).

- 10BASE5: Dùng cáp đồng trục đường kính lớn (10mm) với trở kháng 50 Ohm, tốc độ 10 Mb/s, phạm vi tín hiệu 500m/segment, có tối đa 100 trạm, khoảng cách giữa 2 tranceiver tối thiểu 2,5m (Phương án này còn gọi là Thick Ethernet hay Thicknet)

- 10BASE2: tương tự như Thicknet nhưng dùng cáp đồng trục nhỏ (RG 58A), có thể chạy với khoảng cách 185m, số trạm tối đa trong 1 segment là 30, khoảng cách giữa hai máy tối thiểu là 0,5m.

Dạng kết nối này có ưu điểm là ít tốn dây cáp, tốc độ truyền dữ liệu cao tuy nhiên nếu lưu lượng truyền tăng cao thì dễ gây ách tắc và nếu có trục trặc trên hành lang chính thì khó phát hiện ra.

Hiện nay các mạng sử dụng hình dạng đường thẳng là mạng Ethernet và G-net.

### 2. Dạng vòng tròn (Ring)

Các máy tính được liên kết với nhau thành một vòng tròn theo phương thức "một điểm - một điểm ", qua đó mỗi một trạm có thể nhận và truyền dữ liệu theo vòng một chiều và dữ liệu được truyền theo từng gói một. Mỗi gói dữ liệu đều có mang địa chỉ trạm đích, mỗi trạm khi nhận được một gói dữ liệu nó kiểm tra nếu đúng với địa chỉ của mình thì nó nhận lấy còn nếu không phải thì nó sẽ phát lại cho trạm kế tiếp, cứ như vậy gói dữ liệu đi được đến đích. Với dạng kết nối này có ưu điểm là không tốn nhiều dây cáp, tốc độ truyền dữ liệu cao, không gây ách tắc tuy nhiên các giao thức để truyền dữ liệu phức tạp và nếu có trục trặc trên một trạm thì cũng ảnh hưởng đến toàn mạng.

Hiện nay các mạng sử dụng hình dạng vòng tròn là mạng Tocken ring của IBM.

### 3. Dạng hình sao (Star)

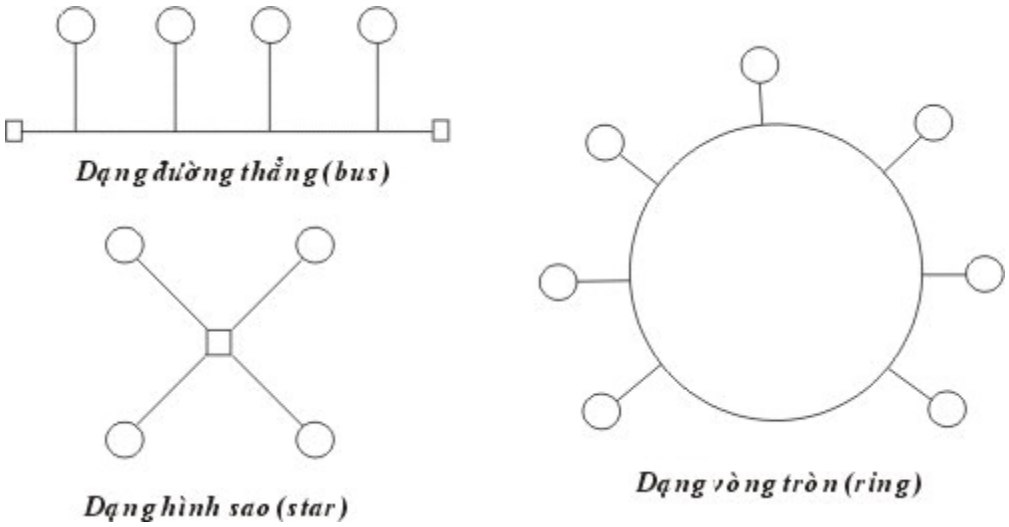
Ở dạng hình sao, tất cả các trạm được nối vào một thiết bị trung tâm có nhiệm vụ nhận tín hiệu từ các trạm và chuyển tín hiệu đến trạm đích với phương thức kết nối là phương thức "một điểm - một điểm ". Thiết bị trung tâm hoạt động giống như một tổng đài cho phép thực hiện việc nhận và truyền dữ liệu từ trạm này tới các trạm khác. Tùy theo yêu cầu truyền thông trong mạng , thiết bị trung tâm có thể là một bộ chuyển mạch (switch), một bộ chọn đường (router) hoặc đơn giản là một bộ phân kênh (Hub). Có nhiều cổng ra và mỗi cổng nối với một máy. Theo chuẩn IEEE 802.3 mô hình dạng Star thường dùng:

- 10BASE-T: dùng cáp UTP, tốc độ 10 Mb/s, khoảng cách từ thiết bị trung tâm tới trạm tối đa là 100m.
- 100BASE-T tương tự như 10BASE-T nhưng tốc độ cao hơn 100 Mb/s.

***Ưu và khuyết điểm***

- *Ưu điểm:* Với dạng kết nối này có ưu điểm là không đụng độ hay ách tắc trên đường truyền, lắp đặt đơn giản, dễ dàng cấu hình lại (thêm, bớt trạm). Nếu có trục trặc trên một trạm thì cũng không gây ảnh hưởng đến toàn mạng qua đó dễ dàng kiểm soát và khắc phục sự cố.
- *Nhược điểm:* Độ dài đường truyền nối một trạm với thiết bị trung tâm bị hạn chế (trong vòng 100 m với công nghệ hiện đại) tốn đường dây cáp nhiều, tốc độ truyền dữ liệu không cao.

Hiện nay các mạng sử dụng hình dạng hình sao là mạng STARLAN của AT&T và S-NET của Novell.




*Hình 5.2 : Các loại cấu trúc chính của mạng cục bộ.*

| | **Đường thẳng** | **Vòng Tròn** | **Hình sao** |
|---|---|---|---|
| Ứng dụng | Tốt cho trường hợp mạng nhỏ và mạng có giao thông thấp và lưu lượng dữ liệu thấp | Tốt cho trường hợp mạng có số trạm ít hoạt động với tốc độ cao,không cách nhau xa lắm hoặc mạng có lưu lượng dữ liệu phân bố không đều. | hiên nay mạng sao là cách tốt nhất cho trường hợp phải tích hợp dữ liệu và tín hiệutiếng.Các mạng đện thoại công cộng có cấu trúc này |
| Độ phức tạp | Tương đối không phức tạp | Đòi hỏi thiết bị tương đối phức tạp .Mặt khác việc đưa thông điệp đi trên tuyến là đơn giản, vì chỉ có 1 con đường, trạm phát chỉ cần biết địa chỉ của trạm nhận , các thông tin để dẫn đường khác thì không cần thiết | Mạng sao được xem là khá phức tạp . Các trạm được nối với thiết bị trung tâm và lần lượt hoạt động như thiết bị trung tâm hoặc nối được tới các dây dẫn truyền từ xa |
| Hiệu suất | Rất tốt dưới tải thấp có thể giảm hiệu suất rất mau khi tải tăng | Có hiệu quả trong trường hợp lượng lưu thông cao và khá ổn định nhờ sự tăng chậm thời gian trễ và sự xuống cấp so với các mạng khác | Tốt cho trường hợp tải vừa tuy nhiên kích thước và khả năng , suy ra hiệu suất của mạng phụ thuộc trực tiếp vào sức mạnh của thiết bị trung tâm. |
| Tổng phí | Tương đối thấp đặc biệt do nhiều thiết bị đã phát triển hòa chỉnh và bán sảm phẩm ở thị trường .Sự dư | Phải dự trù gấp đôi nguồn lực hoặc phải có 1 phương thức thay thế khi 1 nút không hoạt động nếu vẫn muốn mạng hoạt động bình thường | Tổng phí rất cao khi làm nhiêm vụ của thiết bị trung tâm, thiết bị trung tâm ï không được dùng vào việc khác .Số lượng dây riêng cũng nhiều. |

| | | | |
|---|---|---|---|
| | thừa kênh truyền được khuyến để giảm bớt nguy cơ xuất hiện sự cố trên mạng | | |
| Nguy cơ | Một trạm bị hỏng không ảnh hưởng đến cả mạng. Tuy nhiên mạng sẽ có nguy cơ bị tổn hại khi sự cố trên đường dây dẫn chính hoặc có vấn đề với tuyến. Vấn đề trên rất khó xác định được lại rất dễ sửa chữa | Mơt trạm bị hỏng có thể ảnh hưởng đến cả hệ thống vì các trạm phục thuộc vào nhau. Tìm 1 repeater hỏng rất khó ,vả lại việc sửa chữa thẳng hay dùng mưu mẹo xác định điểm hỏng trên mạng có địa bàn rôäng rất khó | Độ tin cậy của hệ thống phụ thuộc vào thiết bị trung tâm, .nếu bị hỏng thì mạng ngưng hoạt động Sự ngưng hoạt động tại thiết bị trung tâm thường không ảnh hươdng đến toàn bộ hệ thống . |
| Khả năng mở rộng | Việc thêm và định hình lại mạng này rất dễ.Tuy nhiên việc kết nối giữa các máy tính và thiết bị của các hãng khác nhau khó có thể vì chúng phải có thể nhận cùng địa chỉ và dữ liệu | Tương đối dễ thêm và bớt các trạm làm việc mà không phải nối kết nhiều cho mỗi thay đổi Giá thành cho việc thay đổi tương đối thấp | Khả năng mở rộâng hạn chế, đa số các thiết bị trung tâm chỉ chịu đựng nổi 1 số nhất định liên kết. Sự hạn chế về tốc độ truyền dữ liệu và băng tần thường được đòi hỏi ở mỗi người sử dụng. Các hạn chế này giúp cho các chức năng xử lý trung tâm không bị quá tải bởi tốc độ thu nạp tại tại cổng truyền và giá thành mỗi cổng truyền của thiết bị trung tâm thấp . |

*Hình 6.4 : Bảng so sánh tính năng giữa các cấu trúc của mạng LAN*

## III. Phương thức truyền tín hiệu

Thông thường có hai phương thức truyền tín hiệu trong mạng cục bộ là dùng băng tần cơ sở (baseband) và băng tần rộng (broadband). Sự khác nhau chủ yếu giữa hai phương thức truyền tín hiệu này là băng tầng cơ sở chỉ chấp nhận một kênh dữ liệu duy nhất trong khi băng rộng có thể chấp nhận đồng thời hai hoặc nhiều kênh truyền thông cùng phân chia giải thông của đường truyền.

Hầu hết các mạng cục bộ sử dụng phương thức băng tần cơ sở. Với phương thức truyền tín hiệu này này tín hiệu có thể được truyền đi dưới cả hai dạng: tương tự (analog) hoặc số (digital). Phương thức truyền băng tần rộng chia giải thông (tần số)

của đường truyền thành nhiều giải tần con trong đó mỗi dải tần con đó cung cấp một kênh truyền dữ liệu tách biệt nhờ sử dụng một cặp modem đặc biệt gọi là bộ giải / Điều biến RF cai quản việc biến đổi các tín hiệu số thành tín hiệu tương tự có tần số vô tuyến (RF) bằng kỹ thuật ghép kênh.

## IV. Các giao thức truy cập đường truyền trên mạng LAN

Để truyền được dữ liệu trên mạng người ta phải có các thủ tục nhằm hướng dẫn các máy tính của mạng làm thế nào và lúc nào có thể thâm nhập vào đường dây cáp để gửi các gói dữ kiện. Ví dụ như đối với các dạng bus và ring thì chỉ có một đường truyền duy nhất nối các trạm với nhau, cho nên cần phải có các quy tắc chung cho tất cả các trạm nối vào mạng để đảm bảo rằng đường truyền được truy nhập và sử dụng một cách hợp lý.

Có nhiều giao thức khác nhau để truy nhập đường truyền vật lý nhưng phân thành hai loại: các giao thức truy nhập ngẫu nhiên và các giao thức truy nhập có điều khiển.

### 1. Giao thức chuyển mạch (yêu cầu và chấp nhận)

Giao thức chuyển mạch là loại giao thức hoạt động theo cách thức sau: một máy tính của mạng khi cần có thể phát tín hiệu thâm nhập vào mạng, nếu vào lúc này đường cáp không bận thì mạch điều khiển sẽ cho trạm này thâm nhập vào đường cáp còn nếu đường cáp đang bận, nghĩa là đang có giao lưu giữa các trạm khác, thì việc thâm nhập sẽ bị từ chối.

### 2. Giao thức đường dây đa truy cập với cảm nhận va chạm (Carrier Sense Multiple Access with Collision Detection hay CSMA/CD )

Giao thức đường dây đa truy cập cho phép nhiều trạm thâm nhập cùng một lúc vào mạng, giao thức này thường dùng trong sơ đồ mạng dạng đường thẳng. Mọi trạm đều có thể được truy nhập vào đường dây chung một cách ngẫu nhiên và do vậy có thể dẫn đến xung đột (hai hoặc nhiều trạm đồng thời cùng truyền dữ liệu). Các trạm phải kiểm tra đường truyền gói dữ liệu đi qua có phải của nó hay không. Khi một trạm muốn truyền dữ liệu nó phải kiểm tra đường truyền xem có rảnh hay không để gửi gói dữ liệu của, nếu đường truyền đang bận trạm phải chờ đợi chỉ được truyền khi thấy đường truyền rảnh. Nếu cùng một lúc có hai trạm cùng sử dụng đường truyền thì giao thức phải phát hiện điều này và các trạm phải ngưng thâm nhập, chờ đợi lần sau các thời gian ngẫu nhiên khác nhau.

Khi đường cáp đang bận trạm phải chờ đợi theo một trong ba phương thức sau:

- Trạm tạm chờ đợi một thời gian ngẫu nhiên nào đó rồi lại bắt đầu kiểm tra đường truyền.

- Trạm tiếp tục kiểm tra đường truyền đến khi đường truyền rảnh thì truyền dữ liệu đi.

- Trạm tiếp tục kiểm tra đường truyềnđến khi đường truyền rảnh thì truyền dữ liệu đi với xác suất p xác định trước (0 < p < 1).

Tại đây phương thức 1 có hiệu quả trong việc tránh xung đột vì hai trạm cần truyền khi thấy đường truyền bận sẽ cùng rút lui và chờ đợi trong các thời gian ngẫu nhiên khác nhau. Ngược lại phương thức 2 cố gắng giảm thời gian trống của đường truyền bằng các cho phép trạm có thể truyền ngay sau khi một cuộc truyền kết thúc song nếu lúc đó có thêm một trạm khác đang đợi thì khả năng xẩy ra xung đột là rất cao. Phương thức 3 với giá trị p phải lựa chọn hợp lý có thể tối thiểu hóa được khả năng xung đột lẫn thời gian trống của đường truyền.

Khi lưu lượng các gói dữ liệu cần di chuyển trên mạng quá cao, thì việc đụng độ có thể xẩy ra với sồ lượng lớn có gây tắc nghẽn đường truyền dẫn đến làm chậm tốc độ truyền tin của hệ thống.

### 3. Giao thức dùng thẻ bài vòng (Token ring)

Đây là giao thức truy nhập có điều khiển chủ yếu dùng kỹ thuật chuyển thẻ bài (token) để cấp phát quyền truy nhập đường truyền tức là quyền được truyền dữ liệu đi. Thẻ bài ở đay là một đơn vị dữ liệu đặc biệt, có kích thước và nội dung (gồm các thông tin điều khiển) được quy định riêng cho mỗi giao thức. Theo giao thức dùng thẻ bài vòng trong đường cáp liên tục có một thẻ bài chạy quanh trong mạng Thẻ bài là một đơn vị dữ liệu đặc biệt trong đó có một bit biểu diễn trạng thái sử dụng của nó (bận hoặc rỗi). Một trạm muốn truyền dữ liệu thì phải đợi đến khi nhận được một thẻ bài rảnh. Khi đó trạm sẽ đổi bit trạng thái của thẻ bài thành bận, nép gói dữ liệu có kèm theo địa chỉ nơi nhận vào thẻ bài và truyền đi theo chiều của vòng.

Vì thẻ bài chạy vòng quang trong mạng kín và chỉ có một thẻ nên việc đụng độ dữ liệu không thể xẩy ra, do vậy hiệu suất truyền dữ liệu của mạng không thay đổi.

Trong các giao thức này cần giải quyết hai vấn đề có thể dẫn đến phá vỡ hệ thống. Một là việc mất thẻ bài làm cho trên vòng không còn thẻ bài lưu chuyển nữa. Hai là một thẻ bài bận lưu chuyển không dừng trên vòng.

### 4. Giao thức dung thẻ bài cho dạng đường thẳng (Token bus)

Đây là giao thức truy nhập có điều khiển trong để cấp phát quyền truy nhập đường truyền cho các trạm đang có nhu cầu truyền dữ liệu, một thẻ bài được lưu chuyển trên một vòng logic thiết lập bởi các trạm đó. Khi một trạm có thẻ bài thì nó có quyền sử dụng đường truyền trong một thời gian xác định trước. Khi đã hết dữ liệu hoặc hết thời đoạn cho phép, trạm chuyển thẻ bài đến trạm tiếp theo trong vòng logic.

Như vậy trong mạng phải thiết lập được vòng logic (hay còn gọi là vòng ảo) bao gồm các trạm đang hoạt động nối trong mạng được xác định vị trí theo một chuỗi thứ tự mà trạm cuối cùng của chuỗi sẽ tiếp liền sau bởi trạm đầu tiên. Mỗi trạm được biết địa chỉ của các trạm kề trước và sau nó trong đó thứ tự của các trạm trên vòng logic có thể

độc lập với thứ tự vật lý. Cùng với việc thiết lập vòng thì giao thức phải luôn luôn theo dõi sự thay đổi theo trạng thái thực tế của mạng.

## V. Đường cáp truyền mạng

Đường cáp truyền mạng là cơ sở hạ tầng của một hệ thống mạng, nên nó rất quan trọng và ảnh hưởng rất nhiều đến khả năng hoạt động của mạng. Hiện nay người ta thường dùng 3 loại dây cáp là cáp xoắn cặp, cáp đồng trục và cáp quang.

### 1. Cáp xoắn cặp

Đây là loại cáp gồm hai đường dây dẫn đồng được xoắn vào nhau nhằm làm giảm nhiễu điện từ gây ra bởi môi trường xung quanh và giữa chúng với nhau.

Hiện nay có hai loại cáp xoắn là cáp có bọc kim loại ( STP - Shield Twisted Pair) và cáp không bọc kim loại (UTP -Unshield Twisted Pair).

- Cáp có bọc kim loại (STP): Lớp bọc bên ngoài có tác dụng chống nhiễu điện từ, có loại có một đôi giây xoắn vào nhau và có loại có nhiều đôi giây xoắn với nhau.

- Cáp không bọc kim loại (UTP): Tính tương tự như STP nhưng kém hơn về khả năng chống nhiễu và suy hao vì không có vỏ bọc.

STP và UTP có các loại (Category - Cat) thường dùng:

- Loại 1 & 2 (Cat 1 & Cat 2): Thường dùng cho truyền thoại và những đường truyền tốc độ thấp (nhỏ hơn 4Mb/s).

- Loại 3 (Cat 3): tốc độ truyền dữ liệu khoảng 16 Mb/s , nó là chuẩn cho hầu hết các mạng điện thoại.

- Loại 4 (Cat 4): Thích hợp cho đường truyền 20Mb/s.

- Loại 5 (Cat 5): Thích hợp cho đường truyền 100Mb/s.

- Loại 6 (Cat 6): Thích hợp cho đường truyền 300Mb/s.

Đây là loại cáp rẻ, dễ cài đặt tuy nhiên nó dễ bị ảnh hưởng của môi trường.

### 2. Cáp đồng trục

Cáp đồng trục có hai đường dây dẫn và chúng có cùng một trục chung, một dây dẫn trung tâm (thường là dây đồng cứng) đường dây còn lại tạo thành đường ống bao xung quanh dây dẫn trung tâm (dây dẫn này có thể là dây bện kim loại và vì nó có chức năng

chống nhiễu nên còn gọi là lớp bọc kim). Giữa hai dây dẫn trên có một lớp cách ly, và bên ngoài cùng là lớp vỏ plastic để bảo vệ cáp.

| *Các loại cáp* | *Dây xoắn cặp* | *Cáp đồng trục mỏng* | *Cáp đồng trục dày* | *Cáp quang* |
|---|---|---|---|---|
| ***Chi tiết*** | Bằng đồng, có 4 và 25 cặp dây (loại 3, 4, 5) | Bằng đồng, 2 dây, đường kính 5mm | Bằng đồng, 2 dây, đường kính 10mm | Thủy tinh, 2 sợi |
| ***Loại kết nối*** | RJ-25 hoặc 50-pin telco | BNC | N-series | ST |
| ***Chiều dài đoạn tối đa*** | 100m | 185m | 500m | 1000m |
| ***Số đầu nối tối đa trên 1 đoạn*** | 2 | 30 | 100 | 2 |
| ***Chạy 10 Mbit/s*** | Được | Được | Được | Được |
| ***Chạy 100 Mbit/s*** | Được | Không | Không | Được |
| ***Chống nhiễu*** | Tốt | Tốt | Rất tốt | Hoàn toàn |
| ***Bảo mật*** | Trung bình | Trung bình | Trung bình | Hoàn toàn |
| ***Độ tin cậy*** | Tốt | Trung bình | Tốt | Tốt |
| ***Lắp đặt*** | Dễ dàng | Trung bình | Khó | Khó |
| ***Khắc phục lỗi*** | Tốt | Dở | Dở | Tốt |
| ***Quản lý*** | Dễ dàng | Khó | Khó | Trung bình |
| ***Chi phí cho 1 trạm*** | Rất thấp | Thấp | Trung bình | Cao |
| ***Ứng dụng tốt nhất*** | Hệ thống Workgroup | Đường backbone | Đường backbone trong tủ mạng | Đường backbone dài trong tủ mạng hoặc các tòa nhà |

*Hình 5.3: Tính năng kỹ thuật của một số loại cáp mạng*

Cáp đồng trục có độ suy hao ít hơn so với các loại cáp đồng khác (ví dụ như cáp xoắn đôi) do ít bị ảnh hưởng của môi trường. Các mạng cục bộ sử dụng cáp đồng trục có thể có kích thước trong phạm vi vài ngàn mét, cáp đồng trục được sử dụng nhiều trong các mạng dạng đường thẳng. Hai loại cáp thường được sử dụng là cáp đồng trục mỏng và cáp đồng trục dày trong đường kính cáp đồng trục mỏng là 0,25 inch, cáp đồng trục dày là 0,5 inch. Cả hai loại cáp đều làm việc ở cùng tốc độ nhưng cáp đồng trục mỏng có độ hao suy tín hiệu lớn hơn

Hiện nay có cáp đồng trục sau:

- RG -58,50 ohm: dùng cho mạng Thin Ethernet
- RG -59,75 ohm: dùng cho truyền hình cáp
- RG -62,93 ohm: dùng cho mạng ARCnet

Các mạng cục bộ thường sử dụng cáp đồng trục có dải thông từ 2,5 - 10 Mb/s, cáp đồng trục có độ suy hao ít hơn so với các loại cáp đồng khác vì nó có lớp vỏ bọc bên ngoài, độ dài thông thường của một đoạn cáp nối trong mạng là 200m, thường sử dụng cho dạng Bus.

### 3. Cáp sợi quang (Fiber - Optic Cable)

Cáp sợi quang bao gồm một dây dẫn trung tâm (là một hoặc một bó sợi thủy tinh có thể truyền dẫn tín hiệu quang) được bọc một lớp vỏ bọc có tác dụng phản xạ các tín hiệu trở lại để giảm sự mất mát tín hiệu. Bên ngoài cùng là lớp vỏ plastic để bảo vệ cáp. Như vậy cáp sợi quang không truyền dẫn các tín hiệu điện mà chỉ truyền các tín hiệu quang (các tín hiệu dữ liệu phải được chuyển đổi thành các tín hiệu quang và khi nhận chúng sẽ lại được chuyển đổi trở lại thành tín hiệu điện).

Cáp quang có đường kính từ 8.3 - 100 micron, Do đường kính lõi sợi thuỷ tinh có kích thước rất nhỏ nên rất khó khăn cho việc đấu nối, nó cần công nghệ đặc biệt với kỹ thuật cao đòi hỏi chi phí cao.

Dải thông của cáp quang có thể lên tới hàng Gbps và cho phép khoảng cách đi cáp khá xa do độ suy hao tín hiệu trên cáp rất thấp. Ngoài ra, vì cáp sợi quang không dùng tín hiệu điện từ để truyền dữ liệu nên nó hoàn toàn không bị ảnh hưởng của nhiễu điện từ và tín hiệu truyền không thể bị phát hiện và thu trộm bởi các thiết bị điện tử của người khác.

Chỉ trừ nhược điểm khó lắp đặt và giá thành còn cao , nhìn chung cáp quang thích hợp cho mọi mạng hiện nay và sau này.

### 4. Các yêu cầu cho một hệ thống cáp

- An toàn, thẩm mỹ: tất cả các dây mạng phải được bao bọc cẩn thận, cách xa các nguồn điện, các máy có khả năng phát sóng để tránh trường hợp bị nhiễu. Các đầu nối phải đảm bảo chất lượng, tránh tình trạng hệ thống mạng bị chập chờn.

- Đúng chuẩn: hệ thống cáp phải thực hiện đúng chuẩn, đảm bảo cho khả năng nâng cấp sau này cũng như dễ dàng cho việc kết nối các thiết bị khác nhau của các nhà sản xuất khác nhau. Tiêu chuẩn quốc tế dùng cho các hệ thống mạng hiện nay là EIA/ TIA 568B.

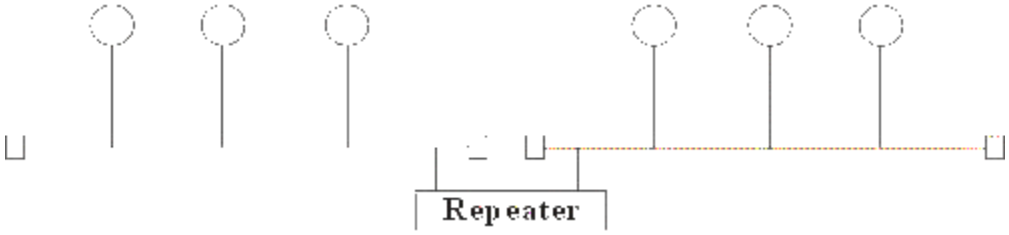
- Tiết kiệm và "linh hoạt" (flexible): hệ thống cáp phải được thiết kế sao cho kinh tế nhất, dễ dàng trong việc di chuyển các trạm làm việc và có khả năng mở rộng sau này.

**Chương 6**

# Các thiết bị liên kết mạng

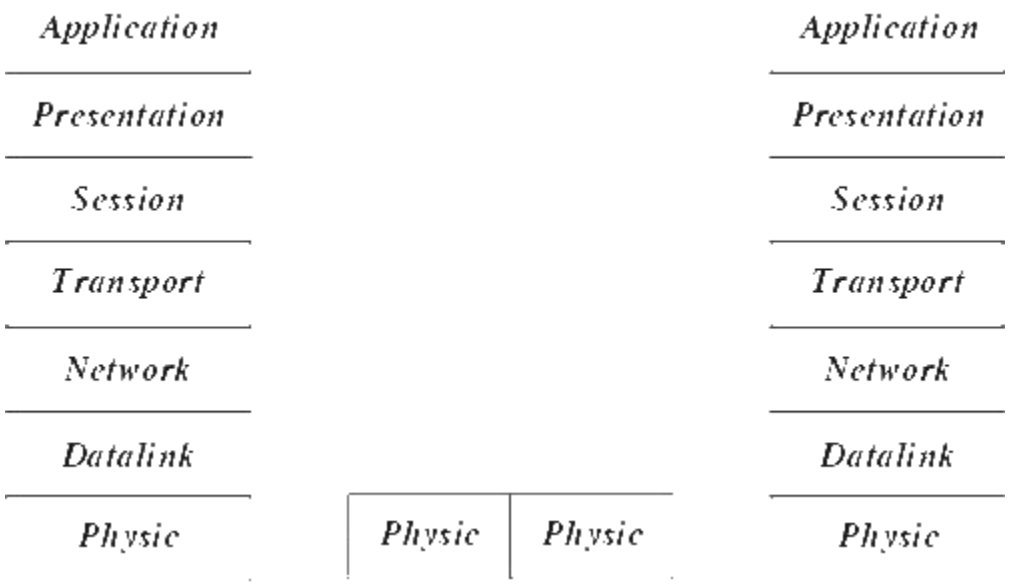
## I. Repeater (Bộ tiếp sức)

Repeater là loại thiết bị phần cứng đơn giản nhất trong các thiết bị liên kết mạng, nó được hoạt động trong tầng vật lý của mô hình hệ thống mở OSI. Repeater dùng để nối 2 mạng giống nhau hoặc các phần một mạng cùng có một nghi thức và một cấu hình. Khi Repeater nhận được một tín hiệu từ một phía của mạng thì nó sẽ phát tiếp vào phía kia của mạng.




*Hình 6.1: Mô hình liên kết mạng của Repeater.*

Repeater không có xử lý tín hiệu mà nó chỉ loại bỏ các tín hiệu méo, nhiễu, khuếch đại tín hiệu đã bị suy hao (vì đã được phát với khoảng cách xa) và khôi phục lại tín hiệu ban đầu. Việc sử dụng Repeater đã làm tăng thêm chiều dài của mạng.




*Hình 6.2: Hoạt động của bộ tiếp sức trong mô hình OSI*

Hiện nay có hai loại Repeater đang được sử dụng là Repeater điện và Repeater điện quang.

- ***Repeater điện*** nối với đường dây điện ở cả hai phía của nó, nó nhận tín hiệu điện từ một phía và phát lại về phía kia. Khi một mạng sử dụng Repeater điện để nối các phần của mạng lại thì có thể làm tăng khoảng cách của mạng, nhưng khoảng cách đó luôn bị hạn chế bởi một khoảng cách tối đa do độ trễ của tín hiệu. Ví dụ với mạng sử dụng cáp đồng trục 50 thì khoảng cách tối đa là 2.8 km, khoảng cách đó không thể kéo thêm cho dù sử dụng thêm Repeater.

- ***Repeater điện quang*** liên kết với một đầu cáp quang và một đầu là cáp điện, nó chuyển một tín hiệu điện từ cáp điện ra tín hiệu quang để phát trên cáp quang và ngược lại. Việc sử dụng Repeater điện quang cũng làm tăng thêm chiều dài của mạng.

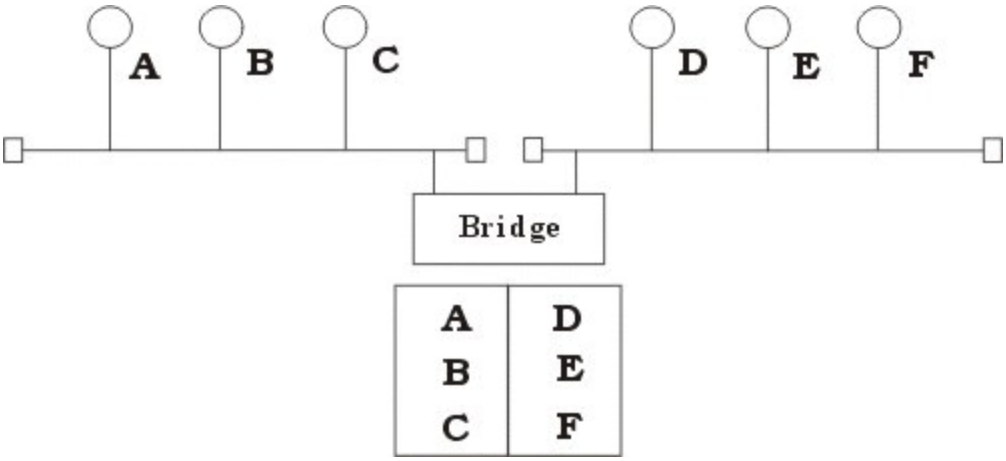
Việc sử dụng Repeater không thay đổi nội dung các tín hiện đi qua nên nó chỉ được dùng để nối hai mạng có cùng giao thức truyền thông (như hai mạng Ethernet hay hai mạng Token ring) nhưng không thể nối hai mạng có giao thức truyền thông khác nhau (như một mạng Ethernet và một mạng Token ring). Thêm nữa Repeater không làm thay đổi khối lượng chuyển vận trên mạng nên việc sử dụng không tính toán nó trên mạng lớn sẽ hạn chế hiệu năng của mạng. Khi lựa chọn sử dụng Repeater cần chú ý lựa chọn loại có tốc độ chuyển vận phù hợp với tốc độ của mạng.

**II. Bridge (Cầu nối)**

Bridge là một thiết bị có xử lý dùng để nối hai mạng giống nhau hoặc khác nhau, nó có thể được dùng với các mạng có các giao thức khác nhau. Cầu nối hoạt động trên tầng liên kết dữ liệu nên không như bộ tiếp sức phải phát lại tất cả những gì nó nhận được thì cầu nối đọc được các gói tin của tầng liên kết dữ liệu trong mô hình OSI và xử lý chúng trước khi quyết định có chuyển đi hay không.

Khi nhận được các gói tin Bridge chọn lọc và chỉ chuyển những gói tin mà nó thấy cần thiết. Điều này làm cho Bridge trở nên có ích khi nối một vài mạng với nhau và cho phép nó hoạt động một cách mềm dẻo.

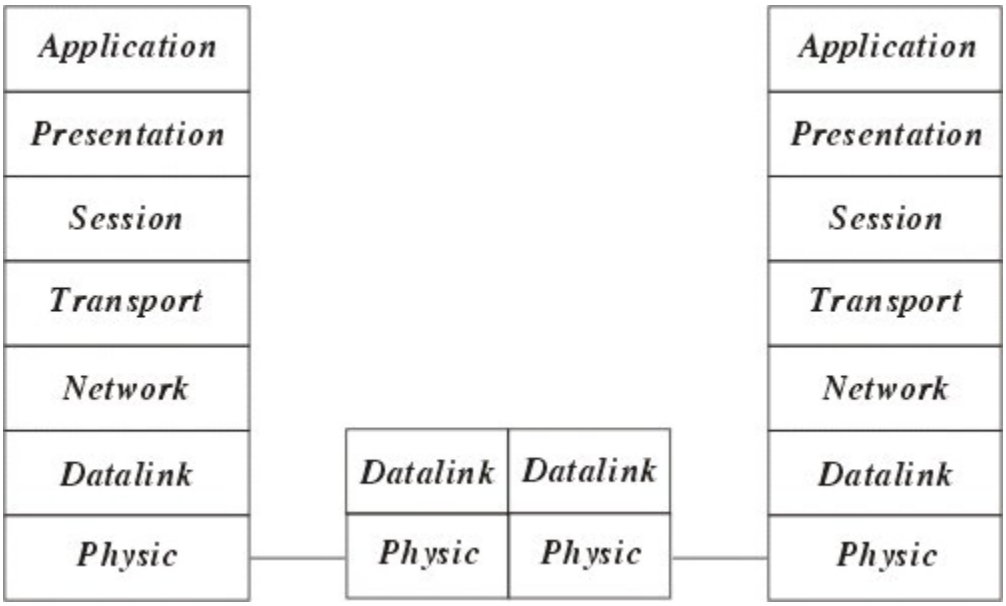
Để thực hiện được điều này trong Bridge ở mỗi đầu kết nối có một bảng các địa chỉ các trạm được kết nối vào phía đó, khi hoạt động cầu nối xem xét mỗi gói tin nó nhận được bằng cách đọc địa chỉ của nơi gửi và nhận và dựa trên bảng địa chỉ phía nhận được gói tin nó quyết định gửi gói tin hay không và bổ xung bảng địa chỉ.




*Hình 6.3: Hoạt động của Bridge*

Khi đọc địa chỉ nơi gửi Bridge kiểm tra xem trong bảng địa chỉ của phần mạng nhận được gói tin có địa chỉ đó hay không, nếu không có thì Bridge tự động bổ xung bảng địa chỉ (cơ chế đó được gọi là tự học của cầu nối).

Khi đọc địa chỉ nơi nhận Bridge kiểm tra xem trong bảng địa chỉ của phần mạng nhận được gói tin có địa chỉ đó hay không, nếu có thì Bridge sẽ cho rằng đó là gói tin nội bộ thuộc phần mạng mà gói tin đến nên không chuyển gói tin đó đi, nếu ngược lại thì Bridge mới chuyển sang phía bên kia. Ở đây chúng ta thấy một trạm không cần thiết chuyển thông tin trên toàn mạng mà chỉ trên phần mạng có trạm nhận mà thôi.




*Hình 6.4: Hoạt động của Bridge trong mô hình OSI*

Để đánh giá một Bridge người ta đưa ra hai khái niệm : Lọc và chuyển vận. Quá trình xử lý mỗi gói tin được gọi là quá trình lọc trong đó tốc độ lọc thể hiện trực tiếp khả

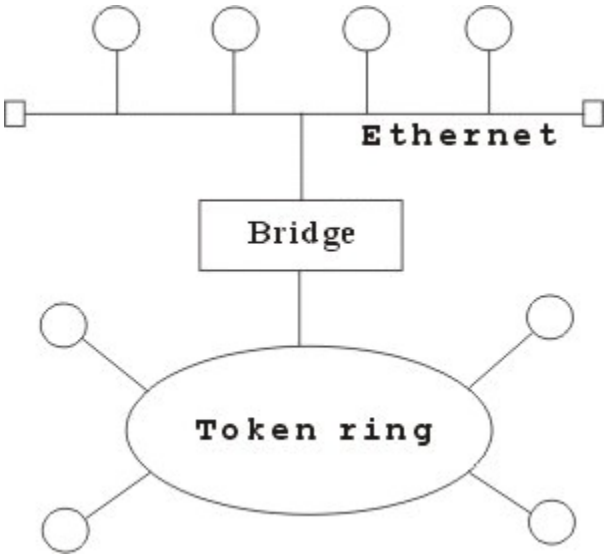
năng hoạt động của Bridge. Tốc độ chuyển vận được thể hiện số gói tin/giây trong đó thể hiện khả năng của Bridge chuyển các gói tin từ mạng này sang mạng khác.

Hiện nay có hai loại Bridge đang được sử dụng là Bridge vận chuyển và Bridge biên dịch. Bridge *vận chuyển* dùng để nối hai mạng cục bộ cùng sử dụng một giao thức truyền thông của tầng liên kết dữ liệu, tuy nhiên mỗi mạng có thể sử dụng loại dây nối khác nhau. Bridge vận chuyển không có khả năng thay đổi cấu trúc các gói tin mà nó nhận được mà chỉ quan tâm tới việc xem xét và chuyển vận gói tin đó đi.

Bridge biên dịch dùng để nối hai mạng cục bộ có giao thức khác nhau nó có khả năng chuyển một gói tin thuộc mạng này sang gói tin thuộc mạng kia trước khi chuyển qua

***Ví dụ :*** Bridge biên dịch nối một mạng Ethernet và một mạng Token ring. Khi đó Cầu nối thực hiện như một nút token ring trên mạng Token ring và một nút Enthernet trên mạng Ethernet. Cầu nối có thể chuyển một gói tin theo chuẩn đang sử dụng trên mạng Enthernet sang chuẩn đang sử dụng trên mạng Token ring.

Tuy nhiên chú ý ở đây cầu nối không thể chia một gói tin ra làm nhiều gói tin cho nên phải hạn chế kích thước tối đa các gói tin phù hợp với cả hai mạng. Ví dụ như kích thước tối đa của gói tin trên mạng Ethernet là 1500 bytes và trên mạng Token ring là 6000 bytes do vậy nếu một trạm trên mạng token ring gửi một gói tin cho trạm trên mạng Ethernet với kích thước lớn hơn 1500 bytes thì khi qua cầu nối số lượng byte dư sẽ bị chặt bỏ.




*Hình 6.5: Ví dụ về Bridge biên dịch*

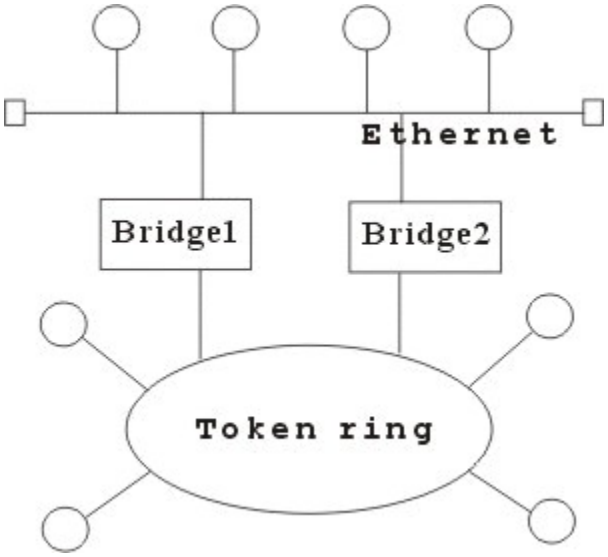
Người ta sử dụng Bridge trong các trường hợp sau :

- Mở rộng mạng hiện tại khi đã đạt tới khoảng cách tối đa do Bridge sau khi sử lý gói tin đã phát lại gói tin trên phần mạng còn lại nên tín hiệu tốt hơn bộ tiếp sức.

- Giảm bớt tắc nghẽn mạng khi có quá nhiều trạm bằng cách sử dụng Bridge, khi đó chúng ta chia mạng ra thành nhiều phần bằng các Bridge, các gói tin trong nội bộ tùng phần mạng sẽ không được phép qua phần mạng khác.

- Để nối các mạng có giao thức khác nhau.

Một vài Bridge còn có khả năng lựa chọn đối tượng vận chuyển. Nó có thể chỉ chuyển vận những gói tin của những địa chỉ xác định. Ví dụ : cho phép gói tin của máy A, B qua Bridge 1, gói tin của máy C, D qua Bridge 2.

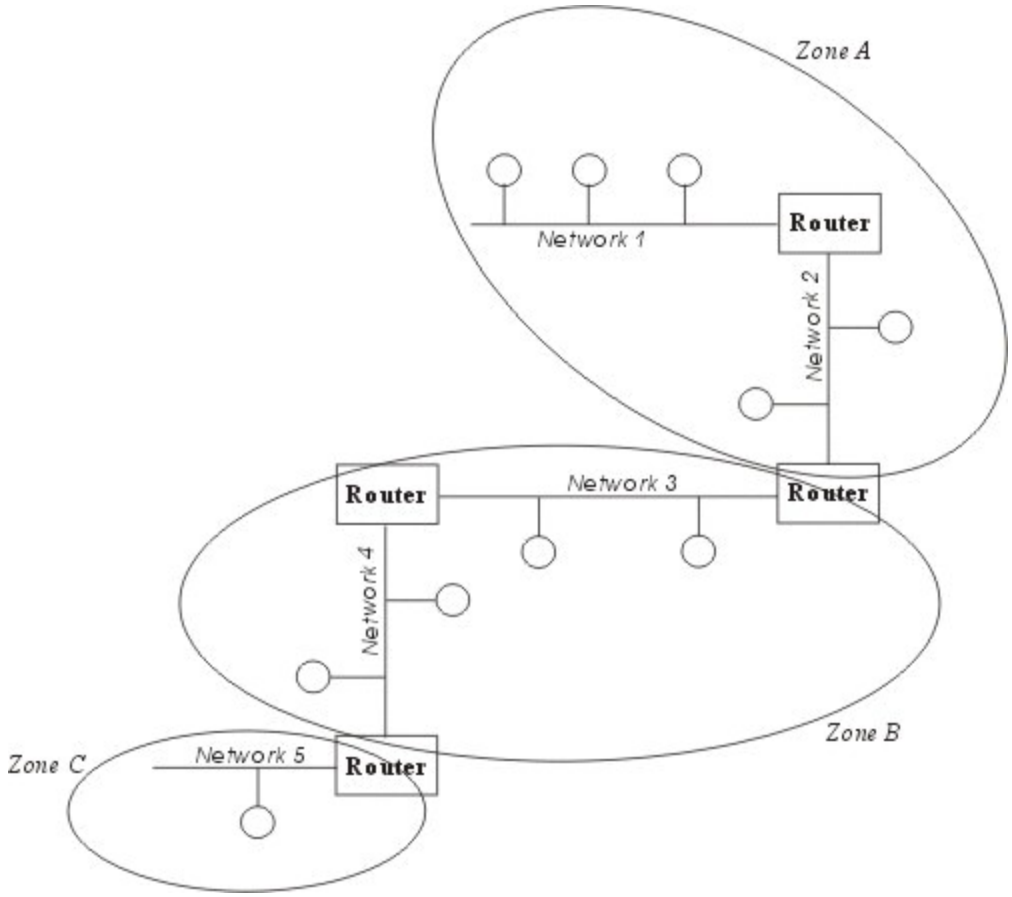



*Hình 6.6 : Liên kết mạng với 2 Bridge*

Một số Bridge được chế tạo thành một bộ riêng biệt, chỉ cần nối dây và bật. Các Bridge khác chế tạo như card chuyên dùng cắïm vào máy tính, khi đó trên máy tính sẽ sử dụng phần mềm Bridge. Việc kết hợp phần mềm với phần cứng cho phép uyển chuyển hơn trong hoạt động của Bridge.

### III. Router (Bộ tìm đường)

Router là một thiết bị hoạt động trên tầng mạng, nó có thể tìm được đường đi tốt nhất cho các gói tin qua nhiều kết nối để đi từ trạm gửi thuộc mạng đầu đến trạm nhận thuộc mạng cuối. Router có thể được sử dụng trong việc nối nhiều mạng với nhau và cho phép các gói tin có thể đi theo nhiều đường khác nhau để tới đích.




*Hình 6.7: Hoạt động của Router.*

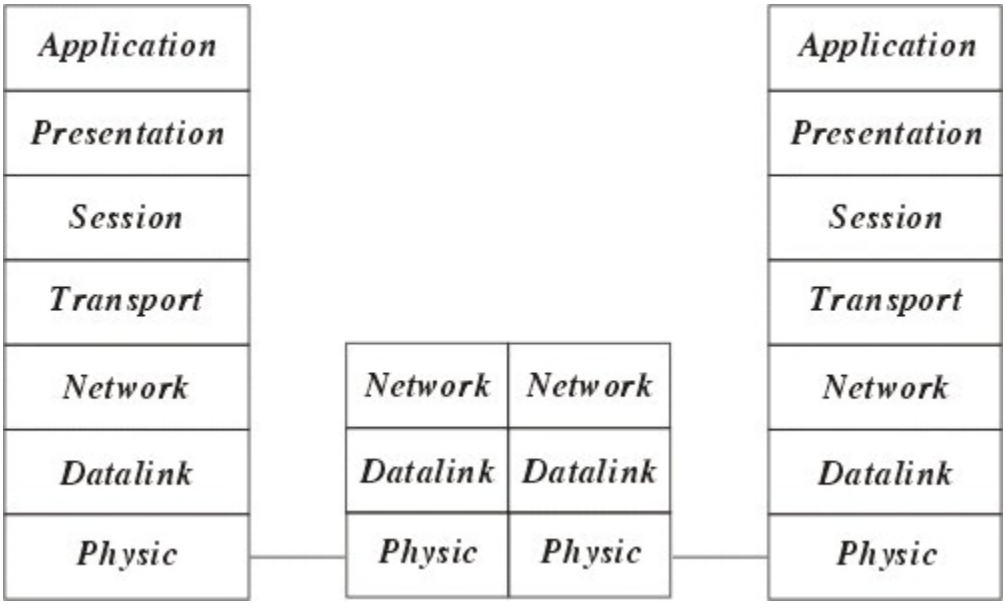
Khác với Bridge hoạt động trên tầng liên kết dữ liệu nên Bridge phải xử lý mọi gói tin trên đường truyền thì Router có địa chỉ riêng biệt và nó chỉ tiếp nhận và xử lý các gói tin gửi đến nó mà thôi. Khi một trạm muốn gửi gói tin qua Router thì nó phải gửi gói tin với địa chỉ trực tiếp của Router (Trong gói tin đó phải chứa các thông tin khác về đích đến) và khi gói tin đến Router thì Router mới xử lý và gửi tiếp.

Khi xử lý một gói tin Router phải tìm được đường đi của gói tin qua mạng. Để làm được điều đó Router phải tìm được đường đi tốt nhất trong mạng dựa trên các thông tin nó có về mạng, thông thường trên mỗi Router có một bảng chỉ đường (Router table). Dựa trên dữ liệu về Router gần đó và các mạng trong liên mạng, Router tính được bảng chỉ đường (Router table) tối ưu dựa trên một thuật toán xác định trước.

Người ta phân chia Router thành hai loại là Router có phụ thuộc giao thức (The protocol dependent routers) và Router không phụ thuộc vào giao thức (The protocol independent router) dựa vào phương thức xử lý các gói tin khi qua Router.

- *Router có phụ thuộc giao thức:* Chỉ thực hiện việc tìm đường và truyền gói tin từ mạng này sang mạng khác chứ không chuyển đổi phương cách đóng gói của gói tin cho nên cả hai mạng phải dùng chung một giao thức truyền thông.

- *Router không phụ thuộc vào giao thức*: có thể liên kết các mạng dùng giao thức truyền thông khác nhau và có thể chuyển đôiø gói tin của giao thức này sang gói tin của giao thức kia, Router cũng ù chấp nhận kích thức các gói tin khác nhau (Router có thể chia nhỏ một gói tin lớn thành nhiều gói tin nhỏ trước truyền trên mạng).




*Hình 6.8: Hoạt động của Router trong mô hình OSI*

Để ngăn chặn việc mất mát số liệu Router còn nhận biết được đường nào có thể chuyển vận và ngừng chuyển vận khi đường bị tắc.

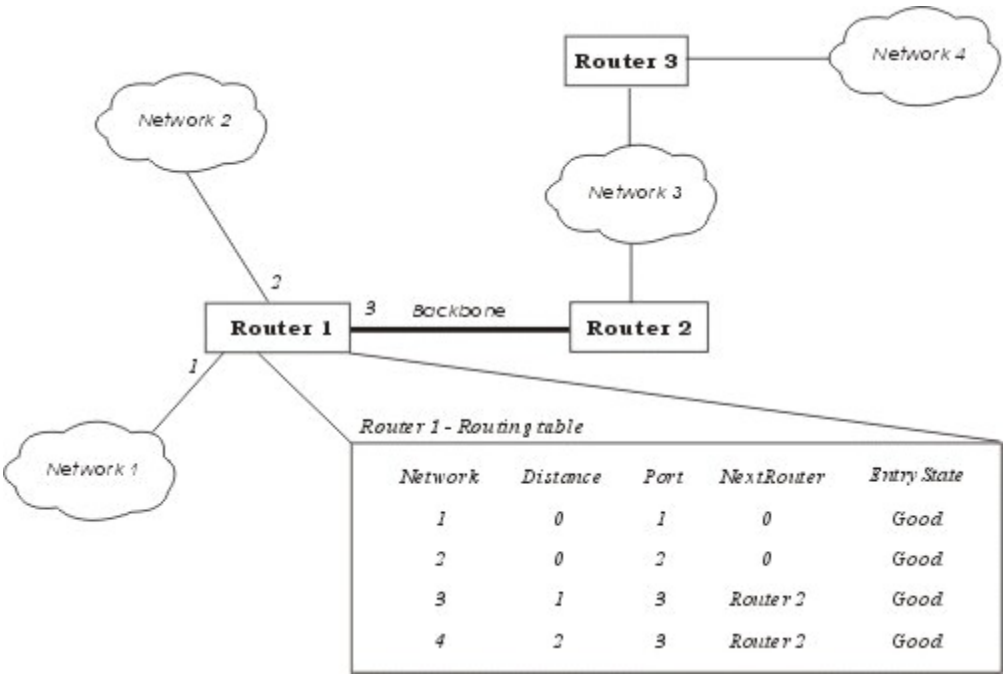
Các lý do sử dụng Router :

- Router có các phần mềm lọc ưu việt hơn là Bridge do các gói tin muốn đi qua Router cần phải gửi trực tiếp đến nó nên giảm được số lượng gói tin qua nó. Router thường được sử dụng trong khi nối các mạng thông qua các đường dây thuê bao đắt tiền do nó không truyền dư lên đường truyền.

- Router có thể dùng trong một liên mạng có nhiều vùng, mỗi vùng có giao thức riêng biệt.

- Router có thể xác định được đường đi an toàn và tốt nhất trong mạng nên độ an toàn của thông tin được đảm bảo hơn.

- Trong một mạng phức hợp khi các gói tin luân chuyển các đường có thể gây nên tình trạng tắc nghẽn của mạng thì các Router có thể được cài đặt các phương thức nhằm tránh được tắc nghẽn.




| Network | Distance | Port | NextRouter | Entry State |
|---|---|---|---|---|
| 1 | 0 | 1 | 0 | Good |
| 2 | 0 | 2 | 0 | Good |
| 3 | 1 | 3 | Router 2 | Good |
| 4 | 2 | 3 | Router 2 | Good |

*Hình 6.9: Ví dụ về bảng chỉ đường (Routing table) của Router.*

## Các phương thức hoạt động của Router

Đó là phương thức mà một Router có thể nối với các Router khác để qua đó chia sẻ thông tin về mạng hiện co. Các chương trình chạy trên Router luôn xây dựng bảng chỉ đường qua việc trao đổi các thông tin với các Router khác.

- Phương thức véc tơ khoảng cách : mỗi Router luôn luôn truyền đi thông tin về bảng chỉ đường của mình trên mạng, thông qua đó các Router khác sẽ cập nhật lên bảng chỉ đường của mình.

- Phương thức trạng thái tĩnh : Router chỉ truyền các thông báo khi có phát hiện có sự thay đổi trong mạng vàchỉ khi đó các Routerkhác ù cập nhật lại bảng chỉ đường, thông tin truyền đi khi đó thường là thông tin về đường truyền.

## Một số giao thức hoạt động chính của Router

- *RIP(Routing Information Protocol)* được phát triển bởi Xerox Network system và sử dụng SPX/IPX và TCP/IP. RIP hoạt động theo phương thức véc tơ khoảng cách.

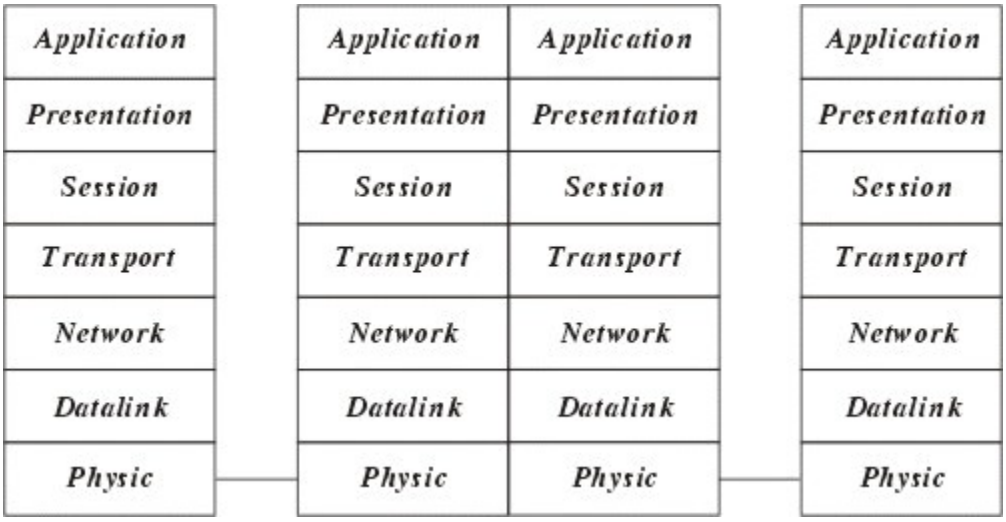
- *NLSP (Netware Link Service Protocol)* được phát triển bởi Novell dùng để thay thế RIP hoạt động theo phương thức véctơ khoảng cách, mỗi Router được biết cấu trúc của mạng và việc truyền các bảng chỉ đường giảm đi..

- *OSPF (Open Shortest Path First)* là một phần của TCP/IP với phương thức trạng thái tĩnh, trong đó có xét tới ưu tiên, giá đường truyền, mật độ truyền thông...

- *OSPF-IS (Open System Interconnection Intermediate System to Intermediate System)* là một phần của TCP/IP với phương thức trạng thái tĩnh, trong đó có xét tới ưu tiên, giá đường truyền, mật độ truyền thông...

## IV. Gateway (cổng nối)

Gateway dùng để kết nối các mạng không thuần nhất chẳng hạn như các mạng cục bộ và các mạng máy tính lớn (Mainframe), do các mạng hoàn toàn không thuần nhất nên việc chuyển đổi thực hiện trên cả 7 tầng của hệ thống mở OSI. Thường được sử dụng nối các mạng LAN vào máy tính lớn. Gateway có các giao thức xác định trước thường là nhiều giao thức, một Gateway đa giao thức thường được chế tạo như các Card có chứa các bộ xử lý riêng và cài đặt trên các máy tính hoặc thiết bị chuyên biệt.




*Hình 6.10: Hoạt động của Gateway trong mô hình OSI*

Hoạt động của Gateway thông thường phức tạp hơn là Router nên thông suất của nó thường chậm hơn và thường không dùng nối mạng LAN -LAN.

## V. Hub (Bộ tập trung)

Hub thường được dùng để nối mạng, thông qua những đầu cắm của nó người ta liên kết với các máy tính dưới dạng hình sao.

Người ta phân biệt các Hub thành 3 loại như sau sau :

- ***Hub bị động (Passive Hub) :*** Hub bị động không chứa các linh kiện điện tử và cũng không xử lý các tín hiệu dữ liệu, nó có chức năng duy nhất là tổ hợp các tín hiệu từ một số đoạn cáp mạng. Khoảng cách giữa một máy tính và Hub

không thể lớn hơn một nửa khoảng cách tối đa cho phép giữa 2 máy tính trên mạng (ví dụ khoảng cách tối đa cho phép giữa 2 máy tính của mạng là 200m thì khoảng cách tối đa giữa một máy tính và hub là 100m). Các mạng ARCnet thường dùng Hub bị động.

- ***Hub chủ động (Active Hub) :*** Hub chủ động có các linh kiện điện tử có thể khuyếch đại và xử lý các tín hiệu điện tử truyền giữa các thiết bị của mạng. Qúa trình xử lý tín hiệu được gọi là tái sinh tín hiệu, nó làm cho tín hiệu trở nên tốt hơn, ít nhạy cảm với lỗi do vậy khoảng cách giữa các thiết bị có thể tăng lên. Tuy nhiên những ưu điểm đó cũng kéo theo giá thành của Hub chủ động cao hơn nhiều so với Hub bị động. Các mạng Token ring có xu hướng dùng Hub chủ động.

- ***Hub thông minh (Intelligent Hub):*** cũng là Hub chủ động nhưng có thêm các chức năng mới so với loại trước, nó có thể có bộ vi xử lý của mình và bộ nhớ mà qua đó nó không chỉ cho phép điều khiển hoạt động thông qua các chương trình quản trị mạng mà nó có thể hoạt động như bộ tìm đường hay một cầu nối. Nó có thể cho phép tìm đường cho gói tin rất nhanh trên các cổng của nó, thay vì phát lại gói tin trên mọi cổng thì nó có thể chuyển mạch để phát trên một cổng có thể nối tới trạm đích.

**Chương 7**

# Giao thức TCP/IP

Giao thức TCP/IP được phát triển từ mạng ARPANET và Internet và được dùng như giao thức mạng và vận chuyển trên mạng Internet. TCP (Transmission Control Protocol) là giao thức thuộc tầng vận chuyển và IP (Internet Protocol) là giao thức thuộc tầng mạng của mô hình OSI. Họ giao thức TCP/IP hiện nay là giao thức được sử dụng rộng rãi nhất để liên kết các máy tính và các mạng.

Hiện nay các máy tính của hầu hết các mạng có thể sử dụng giao thức TCP/IP để liên kết với nhau thông qua nhiều hệ thống mạng với kỹ thuật khác nhau. Giao thức TCP/IP thực chất là một họ giao thức cho phép các hệ thống mạng cùng làm việc với nhau thông qua việc cung cấp phương tiện truyền thông liên mạng.

## I. Giao thức IP

### 1. Tổng quát

Nhiệm vụ chính của giao thức IP là cung cấp khả năng kết nối các mạng con thành liên kết mạng để truyền dữ liệu, vai trò của IP là vai trò của giao thức tầng mạng trong mô hình OSI. Giao thức IP là một giao thức kiểu không liên kết (connectionlees) có nghĩa là không cần có giai đoạn thiết lập liên kết trước khi truyền dữ liệu.

Sơ đồ địa chỉ hóa để định danh các trạm (host) trong liên mạng được gọi là địa chỉ IP 32 bits (32 bit IP address). Mỗi giao diện trong 1 máy có hỗ trợ giao thức IP đều phải được gán 1 địa chỉ IP (một máy tính có thể gắn với nhiều mạng do vậy có thể có nhiều địa chỉ IP). Địa chỉ IP gồm 2 phần: địa chỉ mạng (netid) và địa chỉ máy (hostid). Mỗi địa chỉ IP có độ dài 32 bits được tách thành 4 vùng (mỗi vùng 1 byte), có thể biểu thị dưới dạng thập phân, bát phân, thập lục phân hay nhị phân. Cách viết phổ biến nhất là dùng ký pháp thập phân có dấu chấm (dotted decimal notation) để tách các vùng. Mục đích của địa chỉ IP là để định danh duy nhất cho một máy tính bất kỳ trên liên mạng.

Do tổ chức và độ lớn của các mạng con (subnet) của liên mạng có thể khác nhau, người ta chia các địa chỉ IP thành 5 lớp, ký hiệu là A, B, C, D và E. Trong lớp A, B, C chứa địa chỉ có thể gán được. Lớp D dành riêng cho lớp kỹ thuật multicasting. Lớp E được dành những ứng dụng trong tương lai.

Netid trong địa chỉ mạng dùng để nhận dạng từng mạng riêng biệt. Các mạng liên kết phải có địa chỉ mạng (netid) riêng cho mỗi mạng. Ở đây các bit đầu tiên của byte đầu tiên được dùng để định danh lớp địa chỉ (0 - lớp A, 10 - lớp B, 110 - lớp C, 1110 - lớp D và 11110 - lớp E).

Ơû đây ta xét cấu trúc của các lớp địa chỉ có thể gán được là lớp A, lớp B, lớp C

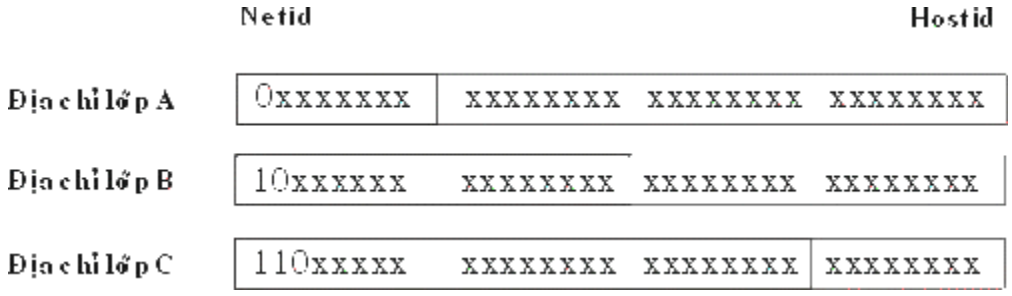
Cấu trúc của các địa chỉ IP như sau:

- Mạng lớp A: địa chỉ mạng (netid) là 1 Byte và địa chỉ host (hostid) là 3 byte.
- Mạng lớp B: địa chỉ mạng (netid) là 2 Byte và địa chỉ host (hostid) là 2 byte.
- Mạng lớp C: địa chỉ mạng (netid) là 3 Byte và địa chỉ host (hostid) là 1 byte.

Lớp A cho phép định danh tới 126 mạng, với tối đa 16 triệu host trên mỗi mạng. Lớp này được dùng cho các mạng có số trạm cực lớn.

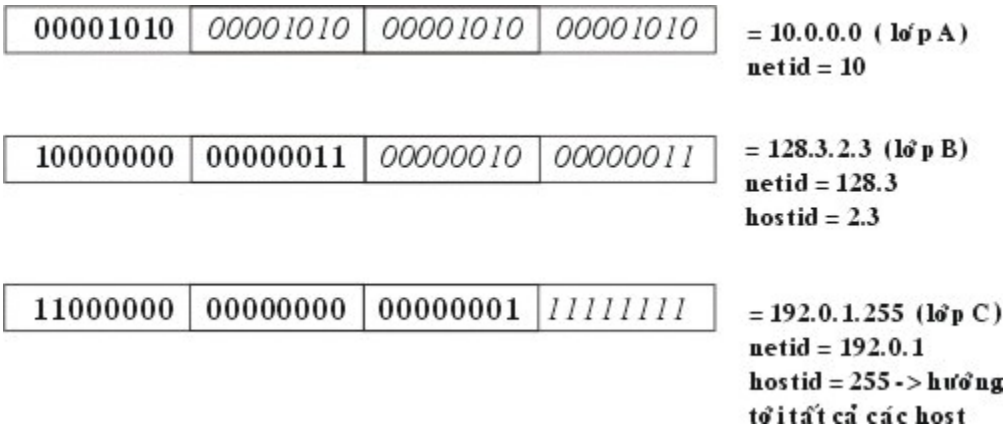
Lớp B cho phép định danh tới 16384 mạng, với tối đa 65534 host trên mỗi mạng.

Lớp C cho phép định danh tới 2 triệu mạng, với tối đa 254 host trên mỗi mạng. Lớp này được dùng cho các mạng có ít trạm.




*Hình 7.1: Cấu trúc các lớp địa chỉ IP*

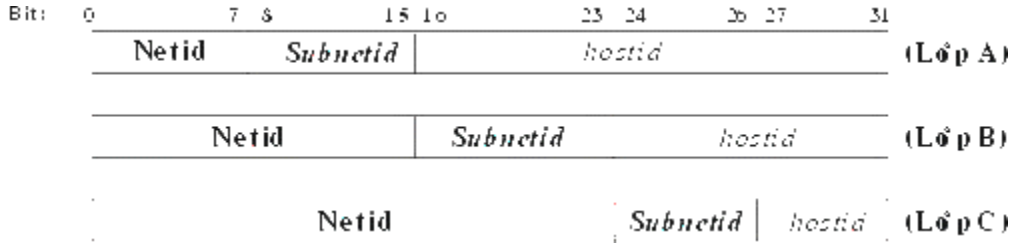
*Một số địa chỉ có tính chất đặc biệt*: Một địa chỉ có hostid = 0 được dùng để hướng tới mạng định danh bởi vùng netid. Ngược lại, một địa chỉ có vùng hostid gồm toàn số 1 được dùng để hướng tới tất cả các host nối vào mạng netid, và nếu vùng netid cũng gồm toàn số 1 thì nó hướng tới tất cả các host trong liên mạng




*Hình 7.2: Ví dụ cấu trúc các lớp địa chỉ IP*

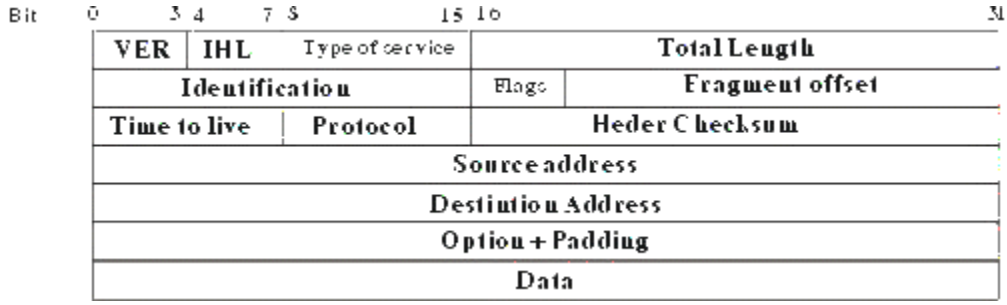
Cần lưu ý rằng các địa chỉ IP được dùng để định danh các host và mạng ở tầng mạng của mô hình OSI, và chúng không phải là các địa chỉ vật lý (hay địa chỉ MAC) của các trạm trên đó một mạng cục bộ (Ethernet, Token Ring.).

Trong nhiều trường hợp, một mạng có thể được chia thành nhiều mạng con (subnet), lúc đó có thể đưa thêm các vùng subnetid để định danh các mạng con. Vùng subnetid được lấy từ vùng hostid, cụ thể đối với lớp A, B, C như ví dụ sau:




*Hình 7.3: Ví dụ địa chỉ khi bổ sung vùng subnetid*

Đơn vị dữ liệu dùng trong IP được gọi là gói tin (datagram), có khuôn dạng



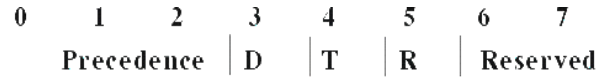

*Hình 7.4: Dạng thức của gói tin IP*

Ý nghĩa của thông số như sau:

- *VER* (4 bits): chỉ version hiện hành của giao thức IP hiện được cài đặt, Việc có chỉ số version cho phép có các trao đổi giữa các hệ thống sử dụng version cũ và hệ thống sử dụng version mới.

- *IHL* (4 bits): chỉ độ dài phần đầu (Internet header Length) của gói tin datagram, tính theo đơn vị từ ( 32 bits). Trường này bắt buột phải có vì phần đầu IP có thể có độ dài thay đổi tùy ý. Độ dài tối thiểu là 5 từ (20 bytes), độ dài tối đa là 15 từ hay là 60 bytes.

- *Type of service* (8 bits): đặc tả các tham số về dịch vụ nhằm thông báo cho mạng biết dịch vụ nào mà gói tin muốn được sử dụng, chẳng hạn ưu tiên, thời hạn chậm trễ, năng suất truyền và độ tin cậy. Hình sau cho biết ý nghĩ của trường 8 bits này.




- Precedence (3 bit): chỉ thị về quyền ưu tiên gửi datagram, nó có giá trị từ 0 (gói tin bình thường) đến 7 (gói tin kiểm soát mạng).

- D (Delay) (1 bit): chỉ độ trễ yêu cầu trong đó
  - D = 0 gói tin có độ trễ bình thường
  - D = 1 gói tin độ trễ thấp

- T (Throughput) (1 bit): chỉ độ thông lượng yêu cầu sử dụng để truyền gói tin với lựa chọn truyền trên đường thông suất thấp hay đường thông suất cao.
  - T = 0 thông lượng bình thường và
  - T = 1 thông lượng cao

- R (Reliability) (1 bit): chỉ độ tin cậy yêu cầu
  - R = 0 độ tin cậy bình thường
  - R = 1 độ tin cậy cao

- *Total Length* (16 bits): chỉ độ dài toàn bộ gói tin, kể cả phần đầu tính theo đơn vị byte với chiều dài tối đa là 65535 bytes. Hiện nay giới hạn trên là rất lớn nhưng trong tương lai với những mạng Gigabit thì các gói tin có kích thước lớn là cần thiết.

- *Identification* (16 bits): cùng với các tham số khác (như Source Address và Destination Address) tham số này dùng để định danh duy nhất cho một datagram trong khoảng thời gian nó vẫn còn trên liên mạng.

- *Flags (3 bits):* liên quan đến sự phân đoạn (fragment) các datagram, Các gói tin khi đi trên đường đi có thể bị phân thành nhiều gói tin nhỏ, trong trường hợp bị phân đoạn thì trường Flags được dùng điều khiển phân đoạn và tái lắp ghép bó dữ liệu. Tùy theo giá trị của Flags sẽ có ý nghĩa là gói tin sẽ không phân đoạn, có thể phân đoạn hay là gói tin phân đoạn cuối cùng. Trường ***Fragment Offset*** cho biết vị trí dữ liệu thuộc phân đoạn tương ứng với đoạn bắt đầu của gói dữ liệu gốc. Ý nghĩa cụ thể của trường Flags là:

  - bit 0: reserved - chưa sử dụng, luôn lấy giá trị 0.

- bit 1: (DF) = 0 (May Fragment) = 1 (Don't Fragment)
- bit 2: (MF) = 0 (Last Fragment) = 1 (More Fragments)

- *Fragment Offset (13 bits)*: chỉ vị trí của đoạn (fragment) ở trong datagram tính theo đơn vị 8 bytes, có nghĩa là phần dữ liệu mỗi gói tin (trừ gói tin cuối cùng) phải chứa một vùng dữ liệu có độ dài là bội số của 8 bytes. Điều này có ý nghĩa là phải nhân giá trị của Fragment offset với 8 để tính ra độ lệch byte.

- *Time to Live (8 bits)*: qui định thời gian tồn tại (tính bằng giây) của gói tin trong mạng để tránh tình trạng một gói tin bị quẩn trên mạng. Thời gian này được cho bởi trạm gửi và được giảm đi (thường qui ước là 1 đơn vị) khi datagram đi qua mỗi router của liên mạng. Thời lượng này giảm xuống tại mỗi router với mục đích giới hạn thời gian tồn tại của các gói tin và kết thúc những lần lặp lại vô hạn trên mạng. Sau đây là 1 số điều cần lưu ý về trường ***Time To Live***:
  - Nút trung gian của mạng không được gởi 1 gói tin mà trường này có giá trị= 0.
  - Một giao thức có thể ấn định ***Time To Live*** để thực hiện cuộc ra tìm tài nguyên trên mạng trong phạm vi mở rộng.
  - Một giá trị cố định tối thiểu phải đủ lớn cho mạng hoạt động tốt.

- *Protocol (8 bits):* chỉ giao thức tầng trên kế tiếp sẽ nhận vùng dữ liệu ở trạm đích (hiện tại thường là TCP hoặc UDP được cài đặt trên IP). Ví dụ: **TCP** có giá trị trường **Protocol** là 6, **UDP** có giá trị trường **Protocol** là 17

- *Header Checksum (16 bits)*: Mã kiểm soát lỗi của header gói tin IP.

- *Source Address (32 bits)*: Địa chỉ của máy nguồn.

- *Destination Address (32 bits)*: địa chỉ của máy đích

- *Options (độ dài thay đổi)*: khai báo các lựa chọn do người gửi yêu cầu (tuỳ theo từng chương trình).

- *Padding (độ dài thay đổi)*: Vùng đệm, được dùng để đảm bảo cho phần header luôn kết thúc ở một mốc 32 bits.

- *Data (độ dài thay đổi)*: Trên một mạng cục bộ như vậy, hai trạm chỉ có thể liên lạc với nhau nếu chúng biết địa chỉ vật lý của nhau. Như vậy vấn đề đặt ra là phải thực hiện ánh xạ giữa địa chỉ IP (32 bits) và địa chỉ vật lý (48 bits) của một trạm.

### 2. Các giao thức trong mạng IP

Để mạng với giao thức IP hoạt động được tốt người ta cần một số giao thức bổ sung, các giao thức này đều không phải là bộ phận của giao thức IP và giao thức IP sẽ dùng đến chúng khi cần.

- *Giao thức ARP (Address Resolution Protocol):* Ở đây cần lưu ý rằng các địa chỉ IP được dùng để định danh các host và mạng ở tầng mạng của mô hình OSI, và chúng không phải là các địa chỉ vật lý (hay địa chỉ MAC) của các trạm trên đó một mạng cục bộ (Ethernet, Token Ring.). Trên một mạng cục bộ hai trạm chỉ có thể liên lạc với nhau nếu chúng biết địa chỉ vật lý của nhau. Như vậy vấn đề đặt ra là phải tìm được ánh xạ giữa địa chỉ IP (32 bits) và địa chỉ vật lý của một trạm. *Giao thức ARP* đã được xây dựng để tìm địa chỉ vật lý từ địa chỉ IP khi cần thiết.

- *Giao thức RARP (Reverse Address Resolution Protocol)*: Là giao thức ngược với *giao thức ARP*. Giao thức RARP được dùng để tìm địa chỉ IP từ địa chỉ vật lý.

- *Giao thức ICMP (Internet Control Message Protocol):* Giao thức này thực hiện truyền các thông báo điều khiển (báo cáo về các tình trạng các lỗi trên mạng.) giữa các gateway hoặc một nút của liên mạng. Tình trạng lỗi có thể là: một gói tin IP không thể tới đích của nó, hoặc một router không đủ bộ nhớ đệm để lưu và chuyển một gói tin IP, Một thông báo ICMP được tạo và chuyển cho IP. IP sẽ "bọc" (encapsulate) thông báo đó với một IP header và truyền đến cho router hoặc trạm đích.

### 3. Các bước hoạt động của giao thức IP

Khi giao thức IP được khởi động nó trở thành một thực thể tồn tại trong máy tính và bắt đầu thực hiện những chức năng của mình, lúc đó thực thể IP là cấu thành của tầng mạng, nhận yêu cầu từ các tầng trên nó và gửi yêu cầu xuống các tầng dưới nó.

Đối với thực thể IP ở máy nguồn, khi nhận được một yêu cầu gửi từ tầng trên, nó thực hiện các bước sau đây:

- Tạo một IP datagram dựa trên tham số nhận được.

- Tính checksum và ghép vào header của gói tin.

- Ra quyết định chọn đường: hoặc là trạm đích nằm trên cùng mạng hoặc một gateway sẽ được chọn cho chặng tiếp theo.

- Chuyển gói tin xuống tầng dưới để truyền qua mạng.

Đối với router, khi nhận được một gói tin đi qua, nó thực hiện các động tác sau:

1) Tính chesksum, nếu sai thì loại bỏ gói tin.

2) Giảm giá trị tham số Time - to Live. nếu thời gian đã hết thì loại bỏ gói tin.

3) Ra quyết định chọn đường.

4) Phân đoạn gói tin, nếu cần.

5) Kiến tạo lại IP header, bao gồm giá trị mới của các vùng Time - to -Live, Fragmentation và Checksum.

6) Chuyển datagram xuống tầng dưới để chuyển qua mạng.

Cuối cùng khi một datagram nhận bởi một thực thể IP ở trạm đích, nó sẽ thực hiện bởi các công việc sau:

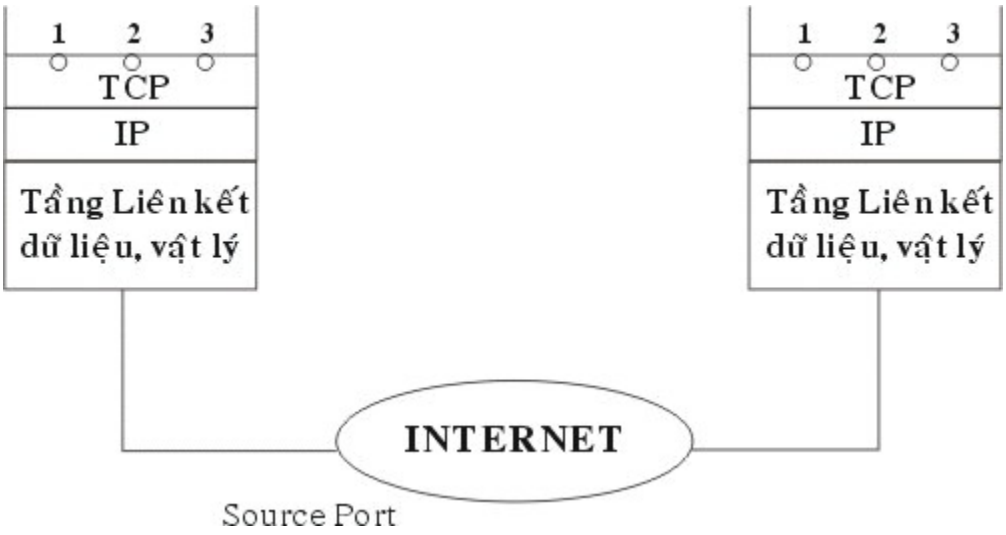
1) Tính checksum. Nếu sai thì loại bỏ gói tin.

2) Tập hợp các đoạn của gói tin (nếu có phân đoạn)

3) Chuyển dữ liệu và các tham số điều khiển lên tầng trên.

## II. Giao thức điều khiển truyền dữ liệu TCP

TCP là một giao thức "có liên kết" (connection - oriented), nghĩa là cần phải thiết lập liên kết giữa hai thực thể TCP trước khi chúng trao đổi dữ liệu với nhau. Một tiến trình ứng dụng trong một máy tính truy nhập vào các dịch vụ của giao thức TCP thông qua một cổng (port) của TCP. Số hiệu cổng TCP được thể hiện bởi 2 bytes.




*Hình 7.5: Cổng truy nhập dịch vụ TCP*

Một cổng TCP kết hợp với địa chỉ IP tạo thành một đầu nối TCP/IP (socket) duy nhất trong liên mạng. Dịch vụ TCP được cung cấp nhờ một liên kết logic giữa một cặp đầu nối TCP/IP. Một đầu nối TCP/IP có thể tham gia nhiều liên kết với các đầu nối TCP/IP ở xa khác nhau. Trước khi truyền dữ liệu giữa 2 trạm cần phải thiết lập một liên kết TCP giữa chúng và khi không còn nhu cầu truyền dữ liệu thì liên kết đó sẽ được giải phóng.

Các thực thể của tầng trên sử dụng giao thức TCP thông qua các hàm gọi (function calls) trong đó có các hàm yêu cầu để yêu cầu, để trả lời. Trong mỗi hàm còn có các tham số dành cho việc trao đổi dữ liệu.

*Các bước thực hiện để thiết lập một liên kết TCP/IP*: Thiết lập một liên kết mới có thể được mở theo một trong 2 phương thức: chủ động (active) hoặc bị động (passive).

- Phương thức bị động, người sử dụng yêu cầu TCP chờ đợi một yêu cầu liên kết gửi đến từ xa thông qua một đầu nối TCP/IP (tại chỗ). Người sử dụng dùng hàm passive Open có khai báo cổng TCP và các thông số khác (mức ưu tiên, mức an toàn)

- Với phương thức chủ động, người sử dụng yêu cầu TCP mở một liên kết với một một đầu nối TCP/IP ở xa. Liên kết sẽ được xác lập nếu có một hàm Passive Open tương ứng đã được thực hiện tại đầu nối TCP/IP ở xa đó.

**Bảng liệt kê một vài cổng TCP phổ biến.**

| Số hiệu cổng | Mô tả |
|---|---|
| 0 | Reserved |
| 5 | Remote job entry |
| 7 | Echo |
| 9 | Discard |
| 11 | Systat |
| 13 | Daytime |
| 15 | Nestat |
| 17 | Quotd (quote odd day |

| | |
|---|---|
| 20 | ftp-data |
| 21 | ftp (control) |
| 23 | Telnet |
| 25 | SMTP |
| 37 | Time |
| 53 | Name Server |
| 102 | ISO - TSAP |
| 103 | X.400 |
| 104 | X.400 Sending |
| 111 | Sun RPC |
| 139 | Net BIOS Session source |
| 160 - 223 | Reserved |

Khi người sử dụng gửi đi một yêu cầu mở liên kết sẽ được nhận hai thông số trả lời từ TCP.

- Thông số Open ID được TCP trả lời ngay lập tức để gán cho một liên kết cục bộ (local connection name) cho liên kết được yêu cầu. Thông số này về sau được dùng để tham chiếu tới liên kết đó. (Trong trường hợp nếu TCP không thể thiết lập được liên kết yêu cầu thì nó phải gửi tham số Open Failure để thông báo.)

- Khi TCP thiết lập được liên kết yêu cầu nó gửi tham số Open Sucsess được dùng để thông báo liên kết đã được thiết lập thành công. Thông báo này dược chuyển đến trong cả hai trường hợp bị động và chủ động. Sau khi một liên kết được mở, việc truyền dữ liệu trên liên kết có thể được thực hiện.

*Các bước thực hiện khi truyền và nhận dữ liệu:* Sau khi xác lập được liên kết người sữ dụng gửi và nhận dữ liệu. Việc gửi và nhận dữ liệu thông qua các hàm Send và receive.

- *Hàm Send:* Dữ liệu được gửi xuống TCP theo các khối (block). Khi nhận được một khối dữ liệu, TCP sẽ lưu trữ trong bộ đệm (buffer). Nếu cờ PUSH được dựng thì toàn bộ dữ liệu trong bộ đệm được gửi, kể cả khối dữ liệu mới đến sẽ được gửi đi. Ngược lại cờ PUSH không

được dựng thì dữ liệu được giữ lại trong bộ đệm và sẽ gửi đi khi có cơ hội thích hợp (chẳng hạn chờ thêm dữ liệu nữa để gửi đi với hiệu quả hơn).

- *Hàm reveive*: Ở trạm đích dữ liệu sẽ được TCP lưu trong bộ đệm gắn với mỗi liên kết. Nếu dữ liệu được đánh dấu với một cờ PUSH thì toàn bộ dữ liệu trong bộ đệm (kể cả các dữ liệu được lưu từ trước) sẽ được chuyển lên cho người sữ dụng. Còn nếu dữ liệu đến không được đánh dấu với cờ PUSH thì TCP chờ tới khi thích hợp mới chuyển dữ liệu với mục tiêu tăng hiệu quả hệ thống.

Nói chung việc nhận và giao dữ liệu cho người sử dụng đích của TCP phụ thuộc vào việc cài đặt cụ thể. Trường hợp cần chuyển gấp dữ liệu cho người sử dụng thì có thể dùng cờ URGENT và đánh dấu dữ liệu bằng bit URG để báo cho người sử dụng cần phải sử lý khẩn cấp dữ liệu đó.

- *Các bước thực hiện khi đóng một liên kết:* Việc đóng một liên kết khi không cần thiết được thực hiên theo một trong hai cách: *dùng hàm Close* hoặc *dùng hàm Abort.*

  - *Hàm Close*: yêu cầu đóng liên kết một cách bình thường. Có nghĩa là việc truyền dữ liệu trên liên kết đó đã hoàn tất. Khi nhận được một *hàm Close* TCP sẽ truyền đi tất cả dữ liệu còn trong bộ đệm thông báo rằng nó đóng liên kết. Lưu ý rằng khi một người sử dụng đã gửi đi một *hàm Close* thì nó vẫn phải tiếp tục nhận dữ liệu đến trên liên kết đó cho đến khi TCP đã báo cho phía bên kia biết về việc đóng liên kết và chuyển giao hết tất cả dữ liệu cho người sử dụng của mình.

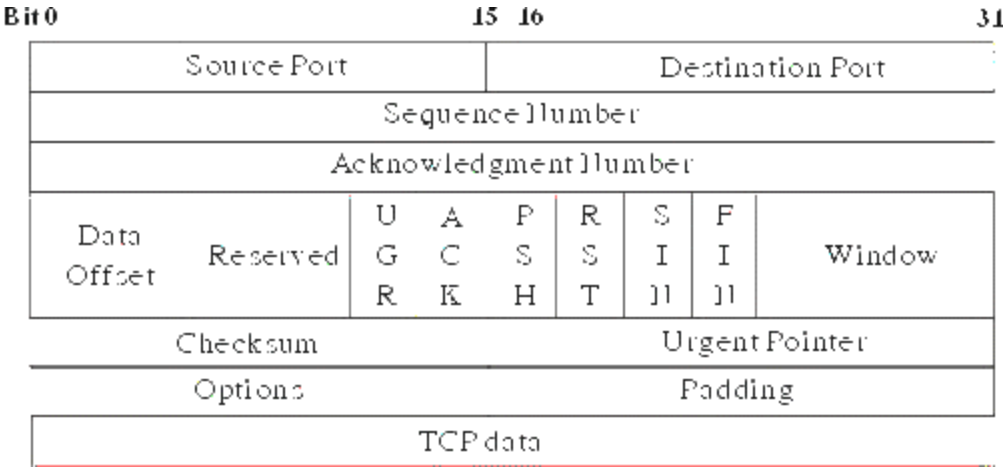
  - *Hàm Abort*: Người sử dụng có thể đóng một liên kết bất và sẽ không chấp nhận dữ liệu qua liên kết đó nữa. Do vậy dữ liệu có thể bị mất đi khi đang được truyền đi. TCP báo cho TCP ở xa biết rằng liên kết đã được hủy bỏ và TCP ở xa sẽ thông báo cho người sử dụng cũa mình.

- Một số hàm khác của TCP:

  - *Hàm Status*: cho phép người sử dụng yêu cầu cho biết trạng thái của một liên kết cụ thể, khi đó TCP cung cấp thông tin cho người sử dụng.

  - *Hàm Error*: thông báo cho người sử dụng TCP về các yêu cầu dịch vụ bất hợp lệ liên quan đến một liên kết có tên cho trước hoặc về các lỗi liên quan đến môi trường.

Đơn vị dữ liệu sử dụng trong TCP được gọi là segment (đoạn dữ liệu), có các tham số với ý nghĩa như sau:




*Hình 7.5: Dạng thức của segment TCP*

- Source Por (16 bits): Số hiệu cổng TCP của trạm nguồn.

- Destination Port (16 bit): Số hiệu cổng TCP của trạm đích.

- Sequence Number (32 bit): số hiệu của byte đầu tiên của segment trừ khi bit SYN được thiết lập. Nếy bit SYN được thiết lập thì Sequence Number là số hiệu tuần tự khởi đầu (ISN) và byte dữ liệu đầu tiên là ISN+1.

- Acknowledgment Number (32 bit): số hiệu của segment tiếp theo mà trạm nguồn đang chờ để nhận. Ngầm ý báo nhận tốt (các) segment mà trạm đích đã gửi cho trạm nguồn.

- Data offset (4 bit): số lượng bội của 32 bit (32 bit words) trong TCP header (tham số này chỉ ra vị trí bắt đầu của nguồn dữ liệu).

- Reserved (6 bit): dành để dùng trong tương lai

- Control bit (các bit điều khiển):

    - URG: Vùng con trỏ khẩn (Ucgent Poiter) có hiệu lực.

    - ACK: Vùng báo nhận (ACK number) có hiệu lực.

    - PSH: Chức năng PUSH.

    - RST: Khởi động lại (reset) liên kết.

    - SYN: Đồng bộ hóa số hiệu tuần tự (sequence number).

    - FIN: Không còn dữ liệu từ trạm nguồn.

- Window (16 bit): cấp phát credit để kiểm soát nguồn dữ liệu (cơ chế cửa sổ). Đây chính là số lượng các byte dữ liệu, bắt đầu từ byte được chỉ ra trong vùng ACK number, mà trạm nguồn đã saün sàng để nhận.

- Checksum (16 bit): mã kiểm soát lỗi cho toàn bộ segment (header + data)

- Urgemt Poiter (16 bit): con trỏ này trỏ tới số hiệu tuần tự của byte đi theo sau dữ liệu khẩn. Vùng này chỉ có hiệu lực khi bit URG được thiết lập.

- Options (độ dài thay đổi): khai báo các option của TCP, trong đó có độ dài tối đa của vùng TCP data trong một segment.

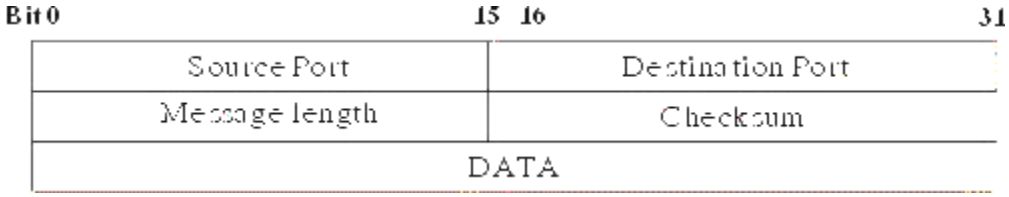
- Paddinh (độ dài thay đổi): phần chèn thêm vào header để đảm bảo phần header luôn kết thúc ở một mốc 32 bit. Phần thêm này gồm toàn số 0.

- TCP data (độ dài thay đổi): chứa dữ liệu của tầng trên, có độ dài tối đa ngầm định là 536 byte. Giá trị này có thể điều chỉnh bằng cách khai báo trong vùng options.

## III. Giao thức UDP (User Datagram Protocol)

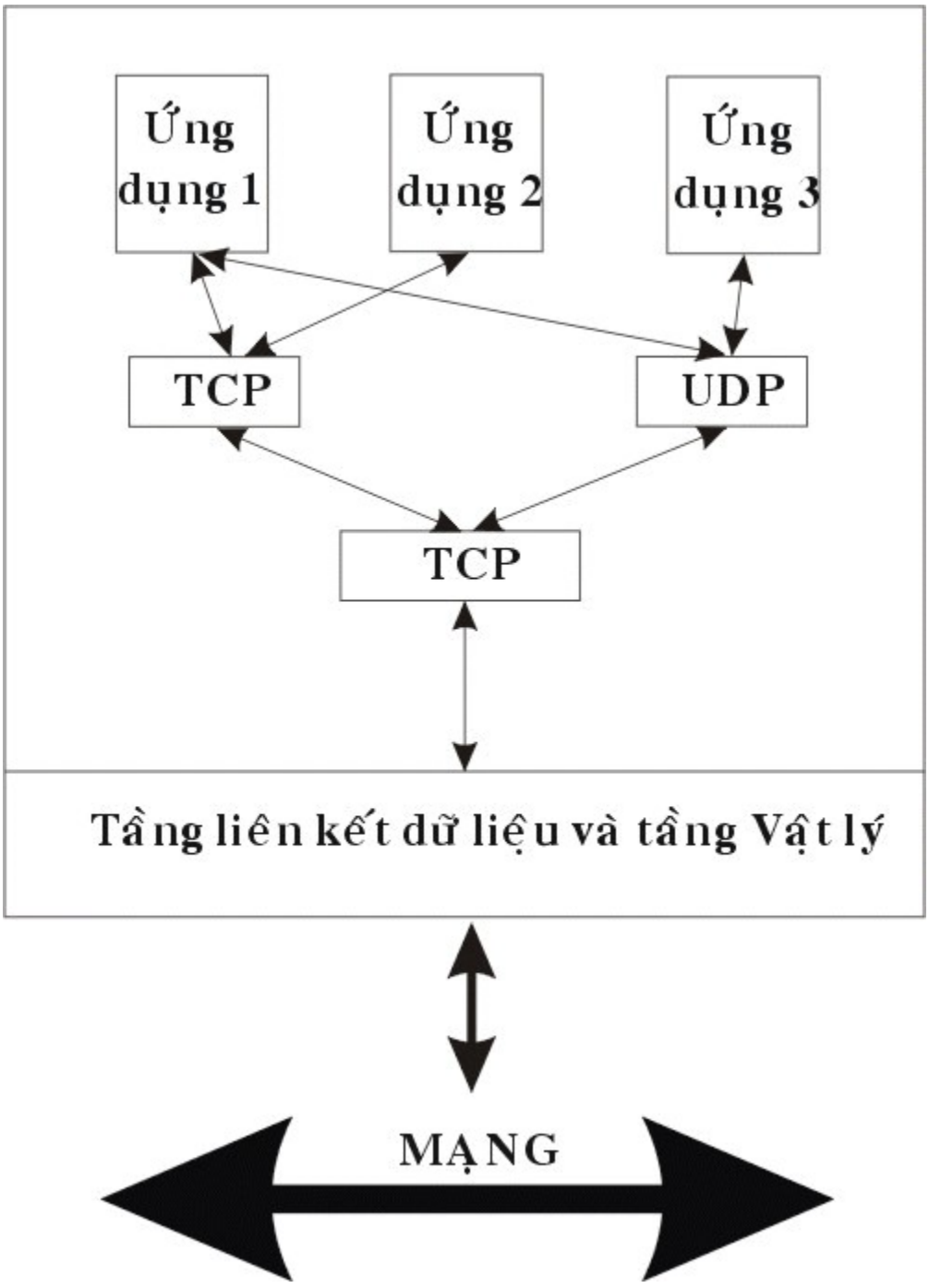
UDP (User Datagram Protocol) là giao thức theo phương thức không liên kết được sử dụng thay thế cho TCP ở trên IP theo yêu cầu của từng ứng dụng. Khác với TCP, UDP không có các chức năng thiết lập và kết thúc liên kết. Tương tự như IP, nó cũng không cung cấp cơ chế báo nhận (acknowledgment), không sắp xếp tuần tự các gói tin (datagram) đến và có thể dẫn đến tình trạng mất hoặc trùng dữ liệu mà không có cơ chế thông báo lỗi cho người gửi. Qua đó ta thấy UDP cung cấp các dịch vụ vận chuyển không tin cậy như trong TCP.

Khuôn dạng UDP datagram được mô tả với các vùng tham số đơn giản hơn nhiều so với TCP segment.




*Hình 7.7: Dạng thức của gói tin UDP*

UDP cũng cung cấp cơ chế gán và quản lý các số hiệu cổng (port number) để định danh duy nhất cho các ứng dụng chạy trên một trạm của mạng. Do ít chức năng phức tạp nên UDP thường có xu thế hoạt động nhanh hơn so với TCP. Nó thường được dùng cho các ứng không đòi hỏi độ tin cậy cao trong giao vận.




*Hình 7.8: Mô hình quan hệ họ giao thức TCP/IP*

**Chương 8**

# Các dịch vụ của mạng diện rộng (WAN)

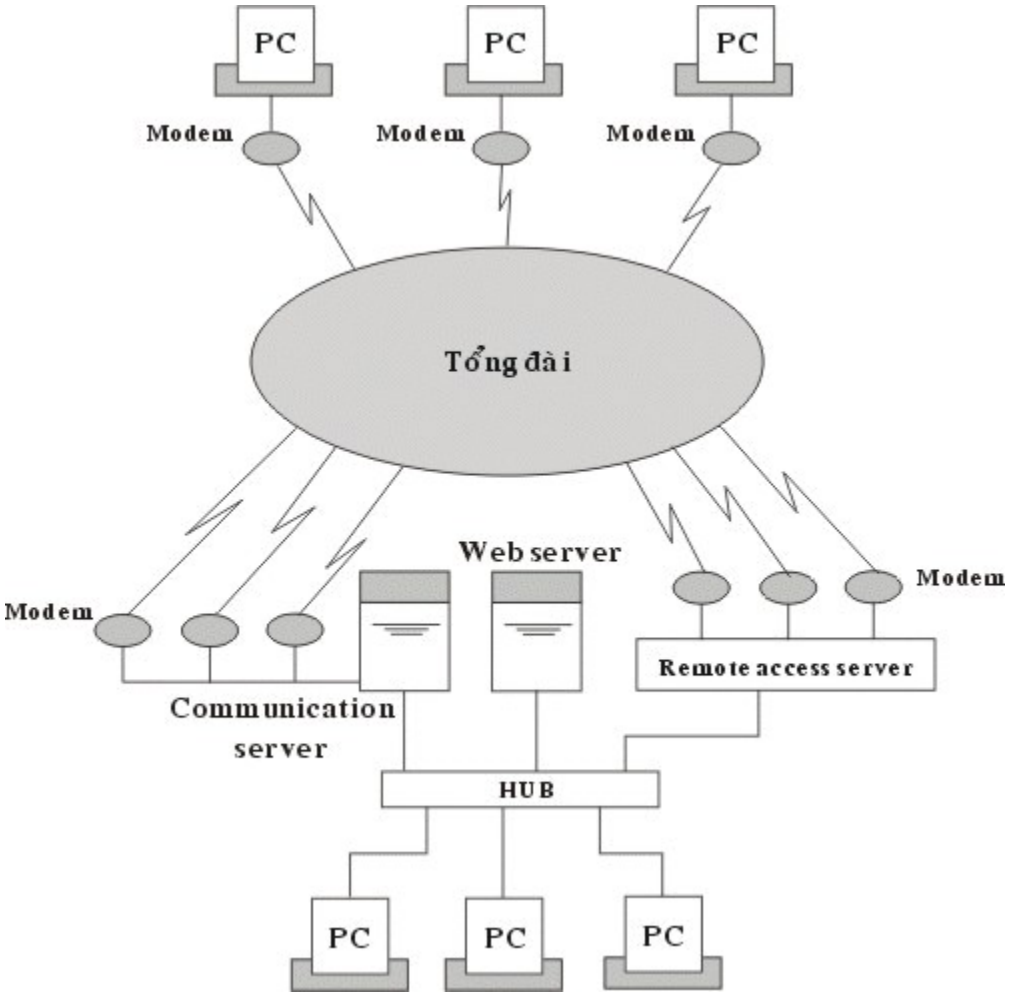
Hiện nay trên thế giới có nhiều dịch vụ dành cho việc chuyển thông tin từ khu vực này sang khu vực khác nhằm liên kết các mạng LAN của các khu vực khác nhau lại. Để có được những liên kết như vậy người ta thường sử dụng các dịch vụ của các mạng diện rộng. Hiện nay trong khi giao thức truyền thông cơ bản của LAN là Ethernet, Token Ring thì giao thức dùng để tương nối các LAN thông thường dựa trên chuẩn TCP/IP. Ngày nay khi các dạng kết nối có xu hướng ngày càng đa dạng và phân tán cho nên các mạng WAN đang thiên về truyền theo đơn vị tập tin thay vì truyền một lần xử lý.

Có nhiều cách phân loại mạng diện rộng, ở đây nếu phân loại theo phương pháp truyền thông tin thì có thể chia thành 3 loại mạng như sau:

- Mạng chuyển mạch (Circuit Swiching Network)
- Mạng thuê bao (Leased lines Network)
- Mạng chuyển gói tin (Packet Switching Network)

## I. Mạng chuyển mạch (Circuit Swiching Network)

Để thực hiện được việc liên kết giữa hai điểm nút, một đường nối giữa điểm nút này và điêm nút kia được thiết lập trong mạng thể hiện dưới dạng cuộc gọi thông qua các thiết bị chuyển mạch.




*Hình 8.1: Mô hình mạng chuyển mạch*

Một ví dụ của mạng chuyển mạch là hoạt động của mạng điện thoại, các thuê bao khi biết số của nhau có thể gọi cho nhau và có một đường nối vật lý tạm thời được thiết lập giữa hai thuê bao.

Với mô hình này mọi đường đều có thể một đường bất kỳ khác, thông qua những đường nối và các thiết bị chuyên dùng người ta có thể liên kết một đường tạm thời từ nơi gửi tới nơi nhận một đường nối vật lý, đường nối trên duy trì trong suốt phiên làm việc và chỉ giải phóng sau khi phiên làm việc kết thúc. Để thực hiện một phiên làm việc cần có các thủ tục đầy đủ cho việc thiết lập liên kết trong đó có việc thông báo cho mạng biết địa chỉ của nút nhận.

Hiện nay có 2 loại mạng chuyển mạch là chuyển mạch tương tự (analog) và chuyển mạch số (digital)

- *Chuyển mạch tương tự (Analog):* Việc chuyển dữ liệu qua mạng chuyển mạch tương tự được thực hiện qua mạng điện thoại. Các trạm sử dụng một

thiết bị có tên là modem, thiết bị này sẽ chuyển các tín hiệu số từ máy tính sao tín hiệu tuần tự có trể truyền đi trên mạng điện thoại và ngược lại.

*Hình 8.2: Mô hình chuyển mạch tương tự*

Khi sử dụng đường truyền điện thoại để truyền số liệu thì các chuẩn của modem và các tính chất của nó sẽ quyết định tốc độ của đường truyền. Cùng với các kỹ thuật chuyển đổi tín hiệu các tính năng mới như nén tín hiệu cho phép nâng tốc độ truyền dữ liệu lên rất cao.

| Loại | Tốc độ (bps)ä | Loại nén | Tốc độ thực tế (bps) |
|---|---|---|---|
| Bell 212A | 1200 | | |
| CCITT V22 | 1200 | | |
| CCITT V22 bis | 2400 | MNP Class 5 | 2400 - 3600 |
| CCITT V32 | 9600 | MNP Class 5, V42 bis | 9600 - 19200 |
| CCITT V32 bis | 14400 | MNP Class 5, V42 bis | 14400 - 33600 |

*Hình 8.3: Bảng kỹ thuật modem*

Các kỹ thuật nén thường dùng là MNP Class 5 và V42 bis, MNP Class 5 cho phép nén với tỷ lệ 1.5:1 và V42 bis nén với tỷ lệ 2:1. Tuy nhiên trên thực tế tỷ lệ nén có thể thay đổi dựa vào dạng dữ liệu được truyền.

- *Chuyển mạch số (Digital):* Đường truyền chuyển mạch số lần đầu tiên được AT&T thiệu vào cuối 1980 khi AT&T giới thiệu mạng chuyển mạch số Acnet với đường truyền 56 kbs. Việc sử dụng đường chuyển mạch số cũng đòi hỏi sử dụng thiết bị phục vụ truyền dữ liệu số (Data Service Unit - DSU) vào vị trí modem trong chuyển mạch tương tự. Thiết bị phục vụ truyền dữ liệu số có nhiệm vụ chuyển các tín hiệu số đơn chiều (unipolar) từ máy tính ra thành tín hiệu số hai chiều (bipolar) để truyền trên đường truyền.

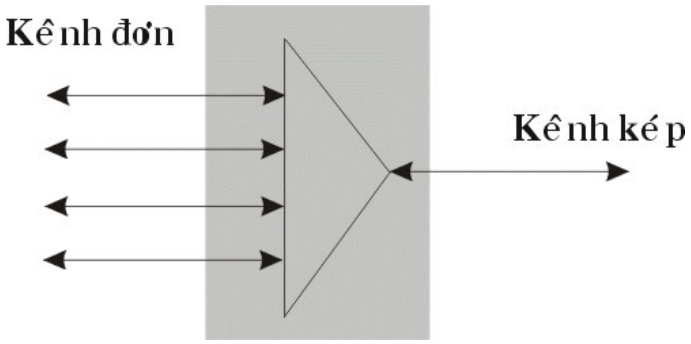
*Hình 8.3: Mô hình chuyển mạch số*

Mạng chuyển mạch số cho phép người sử dụng nâng cao tốc độ truyền (ở đây do khác biệt giữa kỹ thuật truyền số và kỹ thuật truyền tương tự nên hiệu năng của truyền mạch số cao hơn nhiều so với truyền tương tự cho dù cùng tốc độ), độ an toàn.

Vào năm 1991 AT&T giới thiệu mạng chuyển mạch số có tốc độ 384 Kbps. Người ta có thể dùng mạng chuyển mạch số để tạo các liên kết giữa các mạng LAN và làm các đường truyền dự phòng.

**II. Mạng thuê bao (Leased line Network)**

Với kỹ thuật chuyển mạch giữa các nút của mạng (tương tự hoặc số) có một số lượng lớn đường dây truyền dữ liệu, với mỗi đường dây trong một thời điểm chỉ có nhiều nhất một phiên giao dịch, khi số lượng các trạm sử dụng tăng cao người ta nhận thấy việc sử dụng mạng chuyển mạch trở nên không kinh tế. Để giảm bớt số lượng các đường dây kết nối giữa các nút mạng người ta đưa ra một kỹ thuật gọi là ghép kênh.




*Hình 8.4: Mô hình ghép kênh*

Mô hình đó được mô tả như sau: tại một nút người ta tập hợp các tín hiệu trên của nhiều người sử dụng ghép lại để truyền trên một kênh nối duy nhất đến các nút khác, tại nút cuối người ta phân kênh ghép ra thành các kênh riêng biệt và truyền tới các người nhận.

Có hai phương thức ghép kênh chính là ghép kênh theo tần số và ghép kênh theo thời gian, hai phương thức này tương ứng với mạng thuê bao tuần tự và mạng thuê bao kỹ thuật số. trong thời gian hiện nay mạng thuê bao kỹ thuật số sử dụng kỹ thuật ghép kênh theo thời gian với đường truyền T đang được sử dụng ngày một rộng rãi và dần dần thay thế mạng thuê bao tuần tự.

### 1. Phương thức ghép kênh theo tần số

Để sử dụng phương thức ghép kênh theo tần số giữa các nút của mạng được liên kết bởi đường truyền băng tần rộng. Băng tần này được chia thành nhiều kênh con được phân biệt bởi tần số khác nhau. Khi truyền dữ liệu, mỗi kênh truyền từ người sử dụng đến nút sẽ được chuyển thành một kênh con với tần số xác định và được truyền thông qua bộ ghép kênh đến nút cuối và tại đây nó được tách ra thành kênh riêng biệt để truyền tới người nhận. Theo các chuẩn của CCITT có các phương thức ghép kênh cho phép ghép 12, 60, 300 kênh đơn.

Người ta có thể dùng đường thuê bao tuần tự (Analog) nối giữa máy của người sử dụng tới nút mạng thuê bao gần nhất. Khi máy của người sử dụng gửi dữ liệu thì kênh dữ liệu được ghép với các kênh khác và truyền trên đường truyền tới nút đích và được phân ra thành kênh riêng biệt trước khi gửi tới máy của người sử dụng. Đường nối giữa máy trạm của người sử dụng tới nút mạng thuê bao cũng giống như mạng chuyển mạch tuần tự sử dụng đường dây điện thoại với các kỹ thuật chuyển đổi tín hiệu như V22, V22 bis, V32, V32 bis, các kỹ thuật nén V42 bis, MNP class 5.

### 2.Phương thức ghép kênh theo thời gian:

Khác với phương thức ghép kênh theo tần số, phương thức ghép kênh theo thời gian chia một chu kỳ thời gian hoạt động của đường truyền trục thành nhiều khoảng nhỏ và mỗi kênh tuyền dữ liệu được một khoảng. Sau khi ghép kênh lại thành một kênh chung dữ liệu được truyền đi tương tự như phương thức ghép kênh theo tần số. Người ta dùng đường thuê bao là đường truyền kỹ thuật số nối giữa máy của người sử dụng tới nút mạng thuê bao gần nhất.

Hiện nay người ta có các đường truyền thuê bao như sau :

Đường T1 với tốc độ 1.544 Mbps nó bao gồm 24 kênh vớp tốc độ 64 kbps và 8000 bits điều khiển trong 1 giây.

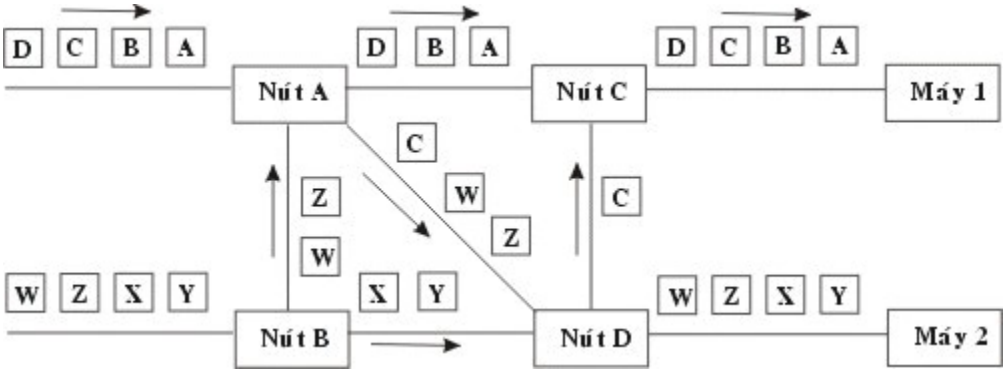
## III. Mạng chuyển gói tin (Packet Switching NetWork)

Mạng chuyển mạch gói hoạt động theo nguyên tắc sau : Khi một trạm trên mạng cần gửi dữ liệu nó cần phải đóng dữ liệu thành từng gói tin, các gói tin đó được đi trên mạng từ nút này tới nút khác tới khi đến được đích. Do việc sử dụng kỹ thuật trên nên khi một trạm không gửi tin thì mọi tài nguyên của mạng sẽ dành cho các trạm khác, do vậy mạng tiết kiệm được các tài nguyên và có thể sử dụng chúng một cách tốt nhất.

Người ta chia các phương thức chuyển mạch gói ra làm 2 phương thức:

- Phương thức chuyển mạch gói theo sơ đồ rời rạc.
- Phương thức chuyển mạch gói theo đường đi xác định.

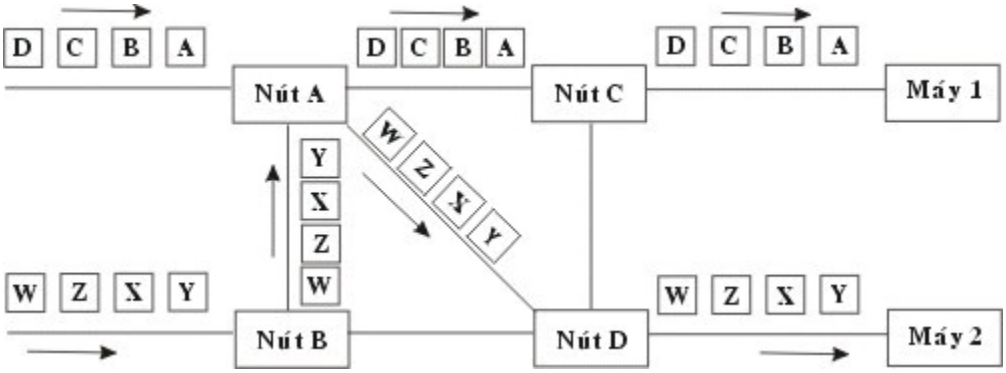
Với phương thức chuyển mạch gói theo sơ đồ rời rạc các gói tin được chuyển đi trên mạng một cách độc lập, mỗi gói tin đều có mang địa chỉ nơ i gửi và nơi nhận. Mỗi nút trong mạng khi tiếp nhận gói tin sẽ quyết định xenm đường đi của gói tin phụ thuộc vào thuật toán tìm đường tại nút và những thông tin về mạng mà nút đó có. Việc truyền theo phương thức này cho ta sự mềm dẻo nhất định do đường đi với mỗi gói tin trở nên mềm dẻo tuy nhiên điều này yêu cầu một số lượng tính toán rất lớn tại mỗi nút nên hiện nay phần lớn các mạng chuyển sang dùng phương chuyển mạch gói theo đường đi xác định.




*Hình 8.5: Ví dụ phương thức sơ đồ rời rạc.*

Phương thức chuyển mạch gói theo đường đi xác định:

Trước khi truyền dữ liệu một đường đi (hay còn gọi là đường đi ảo) được thiết lập giữa trạm gửi và trạm nhận thông qua các nút của mạng. Đường đi trên mang số hiệu phân biệt với các đường đi khác, sau đó các gói tin được gửi đi theo đường đã thiết lập để tới đích, các gói tin mang số hiệu củ đường ảo để có thể được nhận biết khi qua các nút. Điều này khiến cho việc tính toán đường đi cho phiên liên lạc chỉ cần thực hiện một lần.




*Hình 8.6: Ví dụ phương thức đường đi xác định*

## 1. Mạng X25

Được CCITT công bố lần đầu tiên vào 1970 lúc lĩnh vực viễn thông lần đầu tiên tham gia vào thế giới truyền dữ liệu với các đặc tính:

- X25 cung cấp quy trình kiểm soát luồng giữa các đầu cuối đem lại chất lương đường truyền cao cho dù chất lương đương dây truyền không cao.
- X25 được thiết kế cho cả truyền thông chuyển mạch lẫn truyền thông kiểu điểm nối điểm.
- Được quan tâm và tham gia nhanh chóng trên toàn cầu.

Trong X25 có chức năng dồn kênh (multiplexing) đối với liên kết logic (virtual circuits) chỉ làm nhiệm vụ kiểm soát lỗi cho các frame đi qua. Điều này làm tăng độ phức tạp trong việc phối hợp các thủ tục giữa hai tầng kề nhau, dẫn đến thông lượng bị hạn chế do tổng phí xử lý mỗi gói tin tăng lên. X25 kiểm tra lỗi tại mỗi nút trước khi truyền tiếp, điều này làm cho đường truyền chó chất lượng rất cao gần như phi lỗi. Tuy nhiên do vậy khối lượng tích toán tại mỗi nút khá lớn, đối với những đường truyền của những năm 1970 thì điều đó là cần thiết nhưng hiện nay khi kỹ thuật truyền dẫn đã đạt được những tiến bộ rất cao thì việc đó trở nên lãng phí

### 2. Mạng Frame Relay

Mỗi gói tin trong mạng gọi là Frame, do vậy mạng gọi là Frame relay. Đặc điểm khác biệt giữa mạng Frame Relay và mạng X25 mạng Frame Relay là chỉ kiểm tra lỗi tại hai trạm gửi và trạm nhận còn trong quá trình chuyển vận qua các nút trung gian gói tin sẽ không được kiểm lỗi nữa. Do vậy thời gian xử lý trên mỗi nút nhanh hơn, tuy nhiên khi có lỗi thì gói tin phải được phát lại từ trạm đầu. Với độ an toàn cao của đường truyền hiện nay thì chi phí việc phát lại đó chỉ chiếm một tỷ lệ nhỏ nếu so với khối lượng tính toán được giảm đi tại các nút nên mạng Frame Relay tiết kiệm được tài nguyên của mạng hơn so với mạng X25.

Frame relay không chỉ là một kỹ thuật mà còn là thể hiện một phương pháp tổ chức mới. Với nguyên lý là truyền mạch gói nhưng các thao tác kiểm soát giữa các đầu cuối giảm đáng kể Kỹ thuật Frame Relay cho phép thông lượng tối đa đạt tới 2Mbps và hiện nay nó đang cung cấp các giải pháp để tương nối các mạng cục bộ LAN trong một kiến trúc xương sống tạo nên môi trường cho ứng dụng multimedia.

### 3. Mạng ATM (Cell relay)

Hiện nay kỹ thuật Cell Relay dựa trên phương thức truyền thông không đồng bộ (ATM) có thể cho phép thông lương hàng trăm Mbps. Đơn vị dữ liệu dùng trong ATM được gọi là tế bào (cell). các tế bào trong ATM có độ dài cố định là 53 bytes, trong đó 5 bytes dành cho phần chứa thông tin điều khiển (cell header) và 48 bytes chứa dữ liệu của tầng trên.

Trong kỹ thuật ATM, các tế bào chứa các kiểu dữ liệu khác nhau được ghép kênh tới một đường dẫn chung được gọi là đường dẫn ảo (virtual path). Trong đường dẫn ảo đó có thể gồm nhiều kênh ảo (virtual chanell) khác nhau, mỗi kênh ảo được sử dụng bởi một ứng dung nào đó tại một thời điểm.

ATM đã kết hợp những đặc tính tốt nhất của dạng chuyển mạch liên tục và dạng chuyển mạch gói, nó có thể kết hợp dải thông linh hoạt và khả năng chuyển tiếp cao tốc và có khả năng quản lý đồng thời dữ liệu số, tiếng nói, hình ành và multimedia tương tác.

Mục tiêu của kỹ thuật ATM là nhằm cung cấp một mạng dồn kênh, và chuyển mạch tốc độ cao, độ trễ nhỏ dáp ứng cho các dạng truyền thông đa phương tiện (multimecdia)

Chuyển mạch cell cần thiết cho việc cung cấp các kết nối đòi hỏi băng thông cao, tình trạng tắt nghẽn thấp, hổ trợ cho lớp dịch vụ tích hợp lưu thông dữ liệu âm thanh hình ảnh. Đặc tính tốc độ cao là đặc tính nổi bật nhất của ATM.

ATM sử dụng cơ cấu chuyển mạch đặc biệt: ma trận nhị phân các thành tố chuyển mạch (a matrix of binary switching elements) để vận hành lưu thông. Khả năng vô hướng (scalability) là một đặc tính của cơ cấu chuyển mạch ATM. Đặc tính này tương phản trực tiếp với những gì diễn ra khi các trạm cuối được thêm vào một thiết bị liên mạng như router. Các router có năng suất tổng cố định được chia cho các trạm cuối có kết nối với chúng. Khi số lượng trạm cuối gia tăng, năng suất của router tương thích cho trạm cuối thu nhỏ lại. Khi cơ cấu ATM mở rộng, mỗi thiết bị thu trạm cuối, bằng con đường của chính nó đi qua bộ chuyển mạch bằng cách cho mỗi trạm cuối băng thông chỉ định. Băng thông rộng được chỉ định của ATM với đặc tính có thể xác nhận khiến nó trở thành một kỹ thuật tuyệt hảo dùng cho bất kỳ nơi nào trong mạng cục bộ của doanh nghiệp.

Như tên gọi của nó chỉ rõ, kỹ thuật ATM sử dụng phương pháp truyền không đồng bộ (asynchronouns) các tề bào từ nguồn tới đích của chúng. Trong khi đó, ở tầng vật lý người ta có thể sử dụng các kỹ thuật truyền thông đồng bộ như SDH (hoặc SONET).

Nhận thức được vị trí chưa thể thay thế được (ít nhất cho đến những năm đầu của thế kỷ 21) của kỹ thuật ATM, hầu hết các hãng khổng lồ về máy tính và truyền thông như IBM, ATT, Digital, Hewlett - Packard, Cisco Systems, Cabletron, Bay Network,... đều đang quan tâm đặc biệt đến dòng sản phẩm hướng đến ATM của mình để tung ra thị trường. Có thể kể ra đây một số sản phẩm đó như DEC 900 Multiwitch, IBM 8250 hub, Cisco 7000 rounter, Cablectron, ATM module for MMAC hub.

Nhìn chung thị trường ATM sôi động do nhu cầu thực sự của các ứng dụng đa phương tiện. Sự nhập cuộc ngày một đông của các hãng sản xuất đã làm giảm đáng kể giá bán của các sản phẩm loại này, từ đó càng mở rộng thêm thị trường. Ngay ở Việt Nam, các dự án lớn về mạng tin học đều đã được thiết kế với hạ tầng chấp nhận được với công nghệ ATM trong tương lai.

**Chương 9**

# Ví dụ một số mạng LAN và WAN

Hiện nay trên thế giới có rất nhiều mạng máy tính, chúng được sử dụng để phục vụ cho nhiều lĩnh vực khác nhau như nghiên cứu khoa học, truyền dữ liệu, kinh doanh. Vì vậy nên các mạng này cũng rất đa dạng về chủng loại. Trong phần này ta xem xét một số mạng LAN và WAN thông dụng.

## I. Mạng Novell NetWare

Được đưa ra bởi hãng Novell từ những năm 80 và đã được sử dụng nhiều trong các mạng cục bộ với số lượng ước tính hiện nay vào khoảng 50 -60%. Hệ điều hành mạng Novell NetWare là một hệ điều hành có độ an toàn cao đặc biệt là với các mạng có nhiều người sử dụng. Hệ điều hành mạng Netware khá phức tạp để lắp đặt và quản lý nhưng nó là một hệ điều hành mạng đang được dùng phổ biến nhất hiện nay. Hệ điều hành mạng Novell NetWare được thiết kế như một hệ thống mạng *client-server* trong đó các máy tính được chia thành hai loại:

- Những máy têêính cung cấp tài nguyên cho mạng gọi là *server* hay còn gọi là máy chủ mạng.
- Máy sử dụng tài nguyên mạng gọi là *clients* hay còn gọi là trạm làm việc.

Các server (File server) của Netware không chạy DOS mà bản thân Netware là một hệ điều hành cho server điều đó đã giải phóng Netware ra khỏi những hạn chế của DOS. Server của Netware dùng một cấu trúc hiệu quả hơn DOS để tổ chức các tập tin và thư mục, với Netware, chúng ta có thể chia mỗi ổ đĩa thành một hoặc nhiều tập đĩa (volumes), tương tự như các ổ đĩa logic của DOS. Các tập đĩa của Novell có tên chứ không phải là chữ cái. Tuy nhiên, để truy cập một tập đĩa của Netware từ một trạm làm việc chạy DOS, một chữ cái được gán cho tập đĩa.

Với các hệ điều hành Netware 3.x và 4.x các server phải được dành riêng, trong đó chúng ta không thể dùng một file server làm thêm việc cùa Workstation, tuy điều đó tốn kém hơn vì phải mua một máy tính để làm server nhưng nó có hiệu quả hơn vì máy tính server có thể tập trung để phục vụ mạng. Còn với Netware 2.x thì có thể lựa chọn trong đó một file server có thể làm việc như một Workstation như hai tiến trình Server và Workstation tách tời nhau hoàn toàn.

Các trạm làm việc trên một mạng Netware có thể là các máy tính DOS, chạy OS/2 hoặc các máy Macintosh. Nếu mạng vừa có máy PC và Macintosh thì Netware có thể là sự lựa chọn tốt.

Tất cả các phiên bản của Netware đều có đặc trưng được gọi là tính chịu đựng sai hỏng của hệ (System Fault Tolerance SFT) được thiết kế để giữ cho mạng vẫn chạy ngay cả khi phần cứng có sai hỏng.

NetWare là một hệ điều hành nhưng không phải là một hệ điều hành đa năng mà tập trung chủ yếu cho các ứng dụng truy xuất tài nguyên trên mạng, nó có một tập hợp xác định saün các dịch vụ dành cho người sử dụng. Tại đây Novell NetWare có một hệ thống các yêu cầu và trả lời mà Client và Server đều hiểu, nó bao gồm:

- Nhóm chương trình trên máy người dùng: Hệ điều hành trạm, các giao diện cho phép nhười sử dụng chi xuất các tài nguyên của mạng như là các tài nguyên của máy cục bộ, chương trình truyền số liệu qua mạng.

- Hệ điều hành trên máy máy chủ: Chương trình thực hiên từ DOS, Lưu các thông số của DOS, chuyển CPU của server qua chế độ protectied mode, quản lý việc sử dụng tài nguyên của mạng cho người sử dụng.

- Các tiện ích trên mạng: dành cho người sử dụng và người quản trị mạng.

- Novell NetWare hỗ trợ các giao thức cơ bản sau:

- Giao thức truy xuất (Access Protocol) (Ethernet, Token Ring, ARCnet, ProNET-10, FDDI)

- Giao thức trao đổi gói tin trên mạng (Internet Packet Exchange -IPX)

- Giao thức thông tin tìm đường (Routing Information Protocol - RIP)

- Giao thức thông báo dịch vụ (Sevice Advertising Protocol - SAP)

- Giao thức nhân NetWare (NetWare Core Protocol - NCP) cho phép người dùng truy xuất vào file server

Do nhu cầu cần thích nghi với nhiều kiểu mạng và để dễ dàng nâng cấp và quản lý, Novell NetWare cũng được chia thành nhiều tầng giao thức tương tự cấu trúc 7 tầng cuả hệ thống mở OSI.

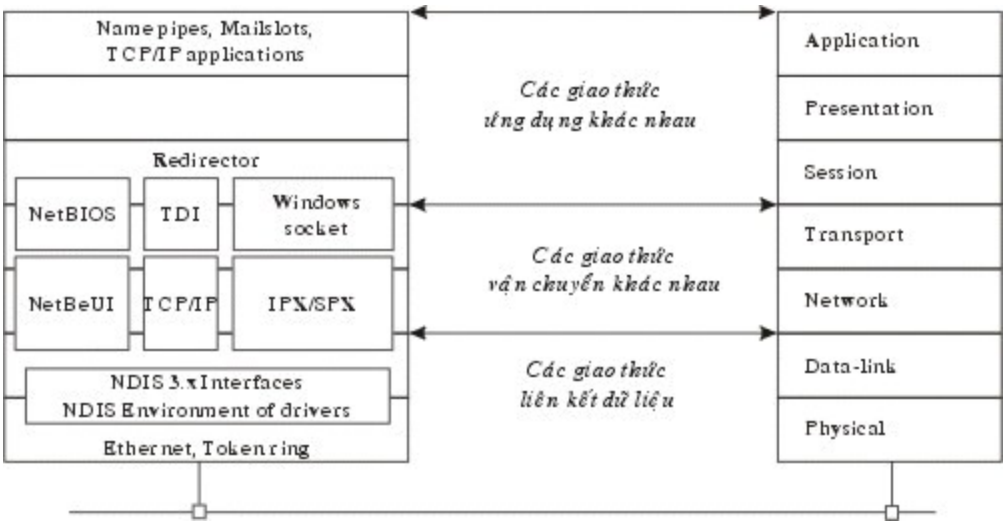
<table>
<tr><td>Tầng ứng dụng<br>(Application)</td><td rowspan="2">Giao thức<br>thông báo dịch vụ<br>(Service advertising<br>protocol - SAP)</td><td rowspan="2">Giao thức thông<br>tin tìm đường<br>(Routing Information<br>Protocol - RIP)</td><td rowspan="2">Giao thức<br>nhân NetWare<br>(NetWare core<br>protocol - NCP)</td></tr>
<tr><td>Tầng trình bày<br>(Presentation)</td></tr>
<tr><td>Tầng giao dịch<br>(Session)</td><td colspan="3">Hệ thống nhập xuất cơ bản trên mạng<br>(NetBIOS)</td></tr>
<tr><td>Tầng vận chuyển<br>(Transport)</td><td colspan="3">Trao đổi gói tin tuần tự<br>(Sequence Packet eXchange - SPX)</td></tr>
<tr><td>Tầng mạng<br>(Network)</td><td colspan="3">Trao đổi gói tin liên mạng<br>(Internet Packet Exchange - IPX)</td></tr>
<tr><td>Tầng liên kết dữ liệu<br>(Data link)</td><td colspan="3">Giao thức truy xuất và kỹ thuật mạng lưới<br>(Access protocol and wiring techniques)<br>(Chuẩn giao tiếp liên kết dữ liệu mở ODI)</td></tr>
<tr><td>Tầng vật lý<br>(Physical)</td><td colspan="3">Ethernet, Token Ring, ARCnet<br>cáp đồng trục, cáp trần xoắn cặp<br>(IEEE 802.X hoặc FDDI)</td></tr>
</table>

*Hình 9.1: Cấu trúc của Hệ điều hành Novell NetWare*

## II. Mạng Windows NT

Mạng dùng hệ điều hành **Windows NT** được đưa ra bởi hãng Microsoft với phiên bản mới nhất hiện nay là Windows NT 5.0, cụm từ windows NT được hiểu là công nghệ mạng trong môi trường Windows (Windows Network Technology). Hiện mạng Windows NT đang được đánh giá cao và được đua vào sử dụng ngày một nhiều. Windows NT là một hệ điều hành đa nhiệm, đa xử lý với địa chỉ 32 bit bộ nhớ. Ngoài việc yểm trơ các ứng dụng DOS, Windows 3.x, Win32 GUI và các ứng dụng dựa trên ký tự, Windows NT còn bao gồm các thành phần mạng, cơ chế an toàn, các công cụ quản trị có khả năng mạng diện rộng, các phần mềm truy cập từ xa. Windows NT cho phép kết nối với máy tính lớn, mini và máy Mac.

Hệ điều hành mạng Windows NT có thể chay trên máy có một CPU cũng như nhiều CPU. Hệ điều hành mạng còn có đưa vào kỹ thuật gương đĩa qua đó sử dụng tốt hệ thống nhiều đĩa nâng cao năng lực hoạt động. Hệ điều hành mạng Windows NT đảm bảo tránh được những người không được phép vào trong hệ thống hoặc thâm nhập vào các file và chương trình trên đĩa cứng. Hệ điều hành mạng Windows NT cung cấp các công cụ để thiết lập các lớp quyền dành cho nhiều nhiệm vụ khác nhau làm cho phép xây dựng hệ thống an toàn một cách mềm dẻo. Windows NT được thiết kế dành cho giải pháp nhóm (Workgroup) khi bạn muốn có kiểm soát nhiều hơn đối với mạng ngang hàng (như Windows For Workgroup, LANtastic hay Novell lite). Ngoài ra chức năng mới của Windows NT server là mô hình vùng (Domain) được thiết lập cho các mạng lớn với khả năng kết nối các mạng toàn xí nghiệp hay liên kết các kết nối mạng với các mạng khác và những công cụ cần thiết để điều hành.



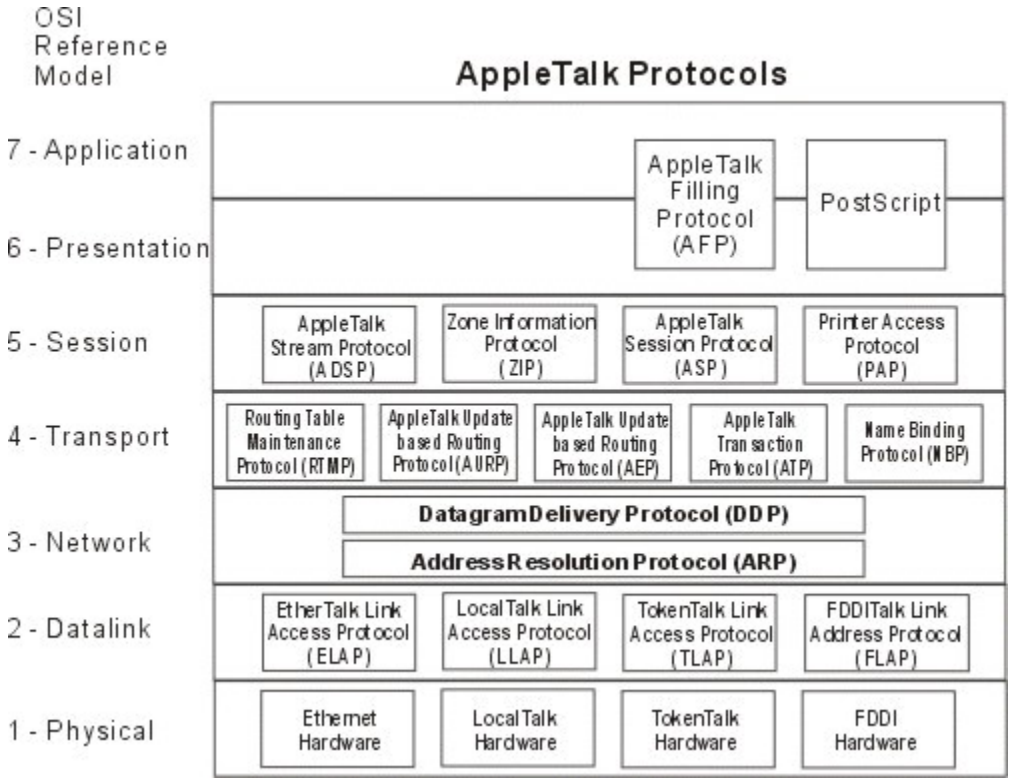

*Hình 9.2: Cấu trúc của Hệ điều hành Windows NT*

## III. Mạng Apple talk

Vào đầu những năm 1980, khi công ty máy tính Apple chuẩn bị giới thiệu máy tính Macintosh, các kỹ sư Apple đã thấy rằng mạng sẽ trở nên rất cần thiết. Họ muốn rằng mạng MAC cũng là một bước tiến mới trong cuộc cách mạng về giao diện thân thiện người dùng do Apple khởi xướng. Với ý định như vậy, Apple xây dựng một giao thức mạng cho họ máy Macintosh, và tích hợp giao thức trên vào máy tính để bàn. Cấu trúc mạng mới do Apple xây dựng được gọi là Apple Talk.

Mặc dù Apple Talk là giao thức mạng độc quyền của Apple, nhưng Apple cũng đã ấn hành nhiều tài liệu về Apple Talk trong cố gắng khuyến khích các nhà sản xuất phần mềm khác phát triển trên Apple Talk. Ngày nay đã có nhiều sản phẩm thương mại trên nền Apple Talk như của Novell, Microsoft.

Ban đầu **AppleTalk** chỉ cài đặt trên hệ thống cáp riêng của hãng là LocalTalk và có phạm vi ứng dụng rất hạn chế. Phiên bản đầu của Apple Talk được thiết kế cho nhóm người dùng cục bộ hay được gọi là *Apple Talk phase 1*. Sau khi tung ra thị trường 5 năm, số người dùng đã vượt quá 1,5 triệu người cài đặt, Apple nhận thấy những nhóm người dùng lớn đã vượt quá giới hạn của *Apple Talk phase 1*, nên họ đã nâng cấp giao thức. Giao thức đã được cải tiến được biết dưới cái tên *Apple Talk phase 2*, cải tiến khả năng tìm đường của Apple Talk và cho phép Apple Talk chạy trên những mạng lớn hơn.




*Hình 9.3: Cấu trúc của Hệ điều hành Appletalk*

Hãng Apple thiết kế Apple Talk độc lập với tầng liên kết dữ liệu. Apple hỗ trợ nhiều loại cài đặt của tầng liên kết dữ liệu, bao gồm *Ethernet, Token Ring, Fiber Distributed Data Interface* (FDDI), và *Local Talk*. Trên Apple Talk, Apple xem Ethernet như *ethertalk*, Token Ring như *tokentalk*, và FDDI như *fdditalk*.

**Các giao thức chính của mạng AppleTalk:**

- ***LLAP*** *(Local Talk Link Access)* là giao thức do Apple phát triển để hoạt động với cáp riêng của hãng (cũng được gọi là LocalTalk) dựa trên cáp xoắn đôi bọc kim (STP), thích hợp với các mạng nhỏ, hiệu năng thấp. Tốc độ tối đa là 230,4 Kb/s và khoảng cách các đoạn cáp có độ dài giới hạn là 300m, số lượng trạm tối đa là 32.

- ***ELAP*** *(Ethertalk Link Access)* và *TLAP (tokentalk Link Access)* là các giao thức cho phép sử dụng các mạng vật lý tương ứng là Ethernet và Token Ring.

- ***AARP*** *(AppleTalk Addresss Resolution Protocol)* là các giao thức cho phép ánh xạ giữa các địa chỉ vật lý của Ethernet và Token Ring, là giao diện giữa các tầng cao của AppleTalk với các tầng vật lý của Ethernet và Token Ring.

- ***DDP*** *(Datagram Delivery Protocol)* là giao thức tầng Mạng cung cấp dịch vụ theo phương thức không liên kết giữa 2 sockets (để chỉ 1 địa chỉ dịch vụ; một tổ hợp của địa chỉ thiết bị, địa chỉ mạng và socket sẽ định danh 1 cách duy nhất

cho môãi tiến trình). DDP thực hiện chức năng chọn đường (routing) dựa trên các bảng chọn đường cho RTMP bảo trì.

- ***RTMP*** *(Routing Table Maintenance protocol)* cung cấp cho DDP thông tin chọn đường trên phương pháp vector khoảng cách tương tự như RIP (Routing Information Protocol) dùng trong Netware IPX/SPX.

- ***NBP*** *(Naming Binding Protocol)*: cho phép định danh các thiết bị bởi các tên lôgic (ngoài địa chỉ của chúng). Các tên này ẩn dấu địa chỉ tầng thấp đối với người sử dụng và đối với các tầng cao hơn.

- ***ATP*** *(AppleTalk Transaction Protocol)* là giao thức thức tầng vận chuyển hoạt động với phương thức không liên kết. Dich vụ vận chuyển này được cung cấp thông qua một hệ thống các thông báo nhận và truyền lại. Độ tin cậy cũa ATP dựa trên các thao tác (transaction) (một thao tác bao gồm một cặp các thao tác hỏi-đáp).

- ***ASP*** *(AppleTalk Section Protocol)* là giao thức tầng giao dịch của AppleTalk, cho phép thiết lập, duy trì và hủy bỏ các phiên liên lạc giữa người yêu cầu dịch vụ và người cung cấp dịch vụ.

- ***ADSP*** *(AppleTalk Data Stream Protocol)* là một giao thức phủ cả tầng vận chuyển và tầng giao dịch, có thể thay cho nhóm giao thức dùng với ATP.

- ***ZIP*** *(Zone Information Protocol)* là giao thức có chức năng tổ chức các thiết bị thành các vùng (zone) để làm giảm độ phức tạp của 1 mạng bằng cách giới hạn sự tương tác của người sử dụng vào đúng các thiết bị mà anh ta cần.

- ***PAP*** *(Printer Access protocol)* cũng là 1 giao thức của tầng giao dịch tương tự như ASP. Nó không chỉ cung cấp các dịch vụ in như tên gọi mà còn yểm trợ các kiểu liên kết giữa người yêu cầu và người cung cấp dịch vụ.

- ***AFP*** *(AppleTalk Filling Protocol)* là giao thức cung cấp dịch vụ File và đảm nhận việc chuyển đổi cú pháp dữ liệu, bảo vệ an toàn dữ liệu (tương tự tầng trình bày trong mô hình OSI).

## IV. Mạng Arpanet

Đây là mạng được thiết lập tại Mỹ vào giữa những năm 60 khi bộ quốc phòng Mỹ muốn có một mạng dùng để ra lệnh và kiểm soát mà có khả năng sống còn cao trong trường hợp có chiến tranh hạt nhân. Những mạng sử dụng đường điện thoại thông thường vào lúc đó tỏ ra không đủ an toàn khi mà một đường dây hay một tổng đài bị phá hủy cũng có thể dẫn đến mọi cuộc nói chuyện hay liên lạc thông qua nó bị gián đoạn, việc đó còn đôi khi dẫn đến cắt rời liên lạc.

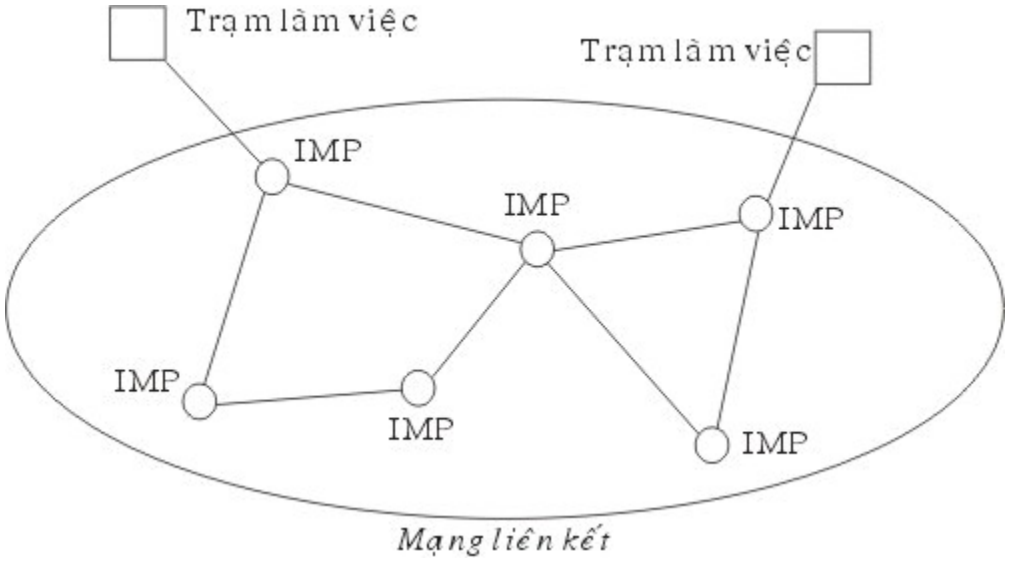
Để làm được điều này khi bộ quốc phòng Mỹ đưa ra chương trình ARPA (Advanced Research Projects Agency) với sự tham gia của nhiều trường đại học và công ty dưới sự quản lý của khi bộ quốc phòng Mỹ.

Vào đầu những năm 1960 những ý tưởng chủ yếu của chuyển mạch gói đã được Paul Baran công bố và sau khi tham khảo nhiều chuyên gia thì chương trình ARPA quyết định mạng tương lai của khi bộ quốc phòng Mỹ sẽ là mạng chuyển mạch gói và nó bao gồm một mạng liên kết và các trạm (host). Mạng liên kết bao gồm các máy tính dùng để liên kết các đường truyền dữ liệu được gọi là các điểm trung chuyển thôâng tin (IMP - Interface Message Processor).

Một IMP sẽ được liên kết với ít nhất là hai IMP khác với độ an toàn cao, các thông tin được chuyển trên mạng liên kết dưới dạng các gói dữ liệu tách rời, có nghĩa là khi có một số đường và nút bị phá hủy thì các gói tin tự động được chuyển theo những đường khác. Mỗi nút một máy tính của hệ thống bao gồm một trạm có được kết nối với một IMP trên mạng, nó gửi thông tin của mình đến IMP để rồi sau đó IMP sẽ phân gói, rồi lần lượt gửi các gói tin theo những đường mà nó lựa chọn để đến đích.

Tháng 10 năm 1968 ARPA quyết định lựa chọn hãng BBN một hãng tư vấn tại Cambridge, Massachsetts làm tổng thầu. Lúc đó BBN đã lựa chon máy DDP-316 làm IMP, các IMP được nối với đường thuê bao 56 Kbps từ các công ty điện thoại. Phần mềm được chia làm hai phần: phần liên kết mạng và phần cho nút, với phần mềm cho liên kết mạng bao gồm phần mềm tại các IMP đầu cuối và các IMP trung gian, các giao thức liên kết IMP với khả năng đảm bảo an toàn cao.

Phần mềm tại nút bao gồm phần mềm danh cho việc liên kết giữa nút với IMP, các giao thức giữa các nút với nhau trong quá trình truyền dữ liệu.




*Hình 9.4: Cấu trúc ban đầu của mạng ARPANET*

Vào tháng 10 năm 1969 mạng ARPANET bắt đầu được đưa vào hoạt động thử nghiệm với 4 nút là những trường đại học và trung tâm nghiên cứu tham gia chính vào dự án, mạng phát triển rất nhanh đến tháng 3 năm 1971 đã có 15 nút và tháng 9 năm 1972 đã có tới 35 nút. Các cải tiến tiếp theo cho phép nhiều trạm có thể liên kết với một IMP do vậy sẽ tiết kiệm tài nguyên và một trạm có thể liên kết với nhiều IMP nhằm tránh việc IMP hư hỏng làm gián đoạn liên lạc.

Cùng với việc phát triển các nút ARPA cũng dành ngân khoản cho phát triển các mạng truyền dữ liệu dùng kỹ thuật vệ tinh và dùng kỹ thuật radio. Điều đó cho phép thiết lập các nút tại những điểm các khoảng cách rất xa. Về các giao thức truyền thông thì sau khi thấy rằng các giao thức của mình không chạy được trên nhiều liên kết mạng vào năm 1974 ARPA đã đầu tư nghiên cứu hệ giao thức TCP/IP và dựa trên hợp đồng giữa BBN và Trường đại học tổng hợp Berkeley - California các nhà nghiên cứu của trường đại học đã viết rất nhiều phần mềm, chương trình quản trị trên cơ ở hệ điều hành UNIX. Dựa trên các phần mềm mới về truyền thông trên cơ sở TCP/IP đã cho phép dễ dành liên kết các mạng LAN vào mạng ARPANET. Vào năm 1983 khi mạng đã hoạt động ổn định thì phần quốc phòng của mạng (gồm khoảng 160 IMP với 110 IMP tại nước Mỹ và 50 IMP ở nước ngoài, hàng trăm nút) được tách ra thành mạng MILNETvà phần còn lại vẫn tiếp tục hoạt động như là một mạng nghiên cứu.

Trong những năm 1980 khi có nhiều mạng LAN được nối vào ARPANET để giảm việc tìm kiếm địa chỉ trên mạng người ta chia vùng các máy tính đưa tên các máy vào địa chỉ IP và xây dựng hệ quản trị cơ sở phân tán các tên các trạm của mạng Hệ cơ sở dữ liệu đó gọi là DNS (Domain Naming System) trong đó có chức mọi thông tin liên quan đến tên các trạm.

Vào năm 1990 với sự phát triển của nhiều mạng khác mà ARPANET là khởi xướng thì ARPANET đã kết thúc hoạt động của mình, tuy nhiên MILNET vẫn hoạt động cho đến ngày nay.

**V. Mạng NFSNET**

Vào cuối những năm 1970 khi Quỹ khoa học quốc gia Hoa kỳ (NFS - The U.S. National Science Foundation) thấy được sự thu hút của ARPANET trong nghiên cứu khoa học mà qua đó các nhà khoa học có thể chia sẻ thông tin hay cùng nhau nghiên cứu các đề án. Tuy nhiên việc sử dụng ARPANET cần thông qua bộ quốc phòng Mỹ với nhiều hạn chế và nhiều cơ sở nghiên cứu khoa học không có khả năng đó. Điều đó khiến NFS thiết lập một mạng ảo có tên là CSNET trong đó sử dụng các máy tính tại công ty BBN cho phép các nhà nghiên cứu có thể kết nối vào để tiếp tục nối với mạng ARPANET hay gửi thư điện tử cho nhau. Vào năm 1984 NFS bắt đầu nghiên cứu tới việc thiết lập một mạng tốc độ cao dành cho các nhóm nghiên cứu khoa học nhằm thay thế mạng ARPANET, bước đầu NFS quyết định xây dựng được đường trục truyền số liệu nối 6 máy tính lớn (Supercomputer) tại 6 trung tâm máy tính. Tại mỗi trung tâm máy tính lớn tại đây được nối với một máy mini loại LSI-11 và các máy mini được nối với nhau bằng đường thuê bao 56 Kbps tương tự như kỹ thuật đã sử dụng ở mạng ARPANET. Đồng thời NFS cũng cung cấp ngân khoản cho khoảng 20 mạng

vùng để liên kết với các máy tính lớn trên và qua đó tới các máy tính lớn khác. Toàn bộ mạng bao gồm mạng trục và các mạng vùng được gọi là NFSNET, mạng NFS có được kết nối với mạng ARPANET.

Mạng NFS được phát triển rất nhanh, sau một thời gian hoạt động đường trục chính được thay thế bằng đường cáp quang 448 Kbps và các máy IBM RS6000 được sử dụng làm công việc kết nối. Đến năm 1990 đường trục đã được nâng lên đến 1.5 Mbps.

Với việc phát triển rất nhanh và NFS thấy rằng chính quyền không có khả năng tiếp tục tài trợ nhưng do các công ty kinh doanh không thể sử dụng mạng NFSNET (do bin cấm theo luật) nên NFS yểm trợ các công ty MERIT, MCI, IBM thành lập một công ty không sinh lợi (nonprofit corporation) có tên là ANS (Advanced Networks and Services) nhằm phát triển việc kinh doanh hóa mạng. ASN tiếp nhận mạng NFSNET và bắt đầu nâng cấp đường trục lên từ 1.5 Mbps lên 45 Mbps để thành lập mạng ANSNET.

Vào năm 1995 khi các công ty cung cấp dịch vụ liên kết phát triển khắp nơi thì mạng trục ANSNET không còn cần thiết nữa và ANSNET được bán cho công ty America Online. Hiện nay các mạng vùng của NFS mua các dịch vụ truyền dữ liệu để liên kết với nhau, mạng NFS đang sử dụng dịch vụ của 4 mạng truyền dữ liệu là PacBell, Ameritech, MFS, Sprint mà qua đó các mạng vùng NFS có thể lựa chọn để kết nối với nhau.

**VI. Mạng Internet**

Cùng với sự phát triển của NFSNET và ARPANET nhất là khi giao thức TCP/IP đã trở thành giao thức chính thước duy nhất trên các mạng trên thì số lượng các mạng, nút muốn tham gia kết nối vào hai mạng trên đã tăng lên rất nhanh. Rất nhiều các mạng vùng được kết nối với nhau và còn liên kết với các mạng ở Canada, châu Aâu.

Vào khoảng giữa những năm 1980 người ta bắt đầu thấy được sự hình thành của một hệ thống liên mạng lớn mà sau này được gọi là Internet. Sự phát triển của Internet được tính theo cấp số nhân, nếu như năm 1990 có khoảng 200.000 máy tính với 3.000 mạng con thì năm 1992 đã có khoảng 1.000.000 máy tính được kết nối, đến năm 1995 đã có hàng trăm mạng cấp vùng, chục ngàn mạng con và nhiều triệu máy tính. Rất nhiều mạng lớn đang hoạt động cũng đã được kết nối vào Internet như các mạng SPAN, NASA network, HEPNET, BITNET, IBM network, EARN. Việc liên kết các mạng được thực hiện thông qua rất nhiều đường nối có tốc độ rất cao.

Hiện nay một máy tính được gọi là thành viên của Internet nếu máy tính đó có giao thức truyền dữ liệu TCP/IP, có một địa chỉ IP trên mạng và nó có thể gửi các gói tin IP đến tất cả các máy tính khác trên mạng Internet.

Tuy nhiên trong nhiều trường hợp thông qua một nhà cung cấp dịch vụ Internet người sử dụng kết nối máy của mình với máy chủ của nhà phục vụ và được cung cấp một địa chỉ tạm thời trước khi khai thác các tài nguyên của Internet. Máy tính của người đó

có thể gửi các gói tin cho các máy khác bằng địa chỉ tạm thời đó và địa chỉ đó sẽ trả lại cho nhà cung cấp khi kết thúc liên lạc. Vì máy tính của người đó sử dụng trong thời gian liên kết với Internet cũng có một địa chỉ IP nên người ta vẫn coi máy tính đó là thành viên của Internet.

Vào năm 1992 cộng đồng Internet đã ra đời nhằm thúc đẩy sự phát triển của Internet và điều hành nó. Hiện nay Internet có 5 dịch vụ chính:

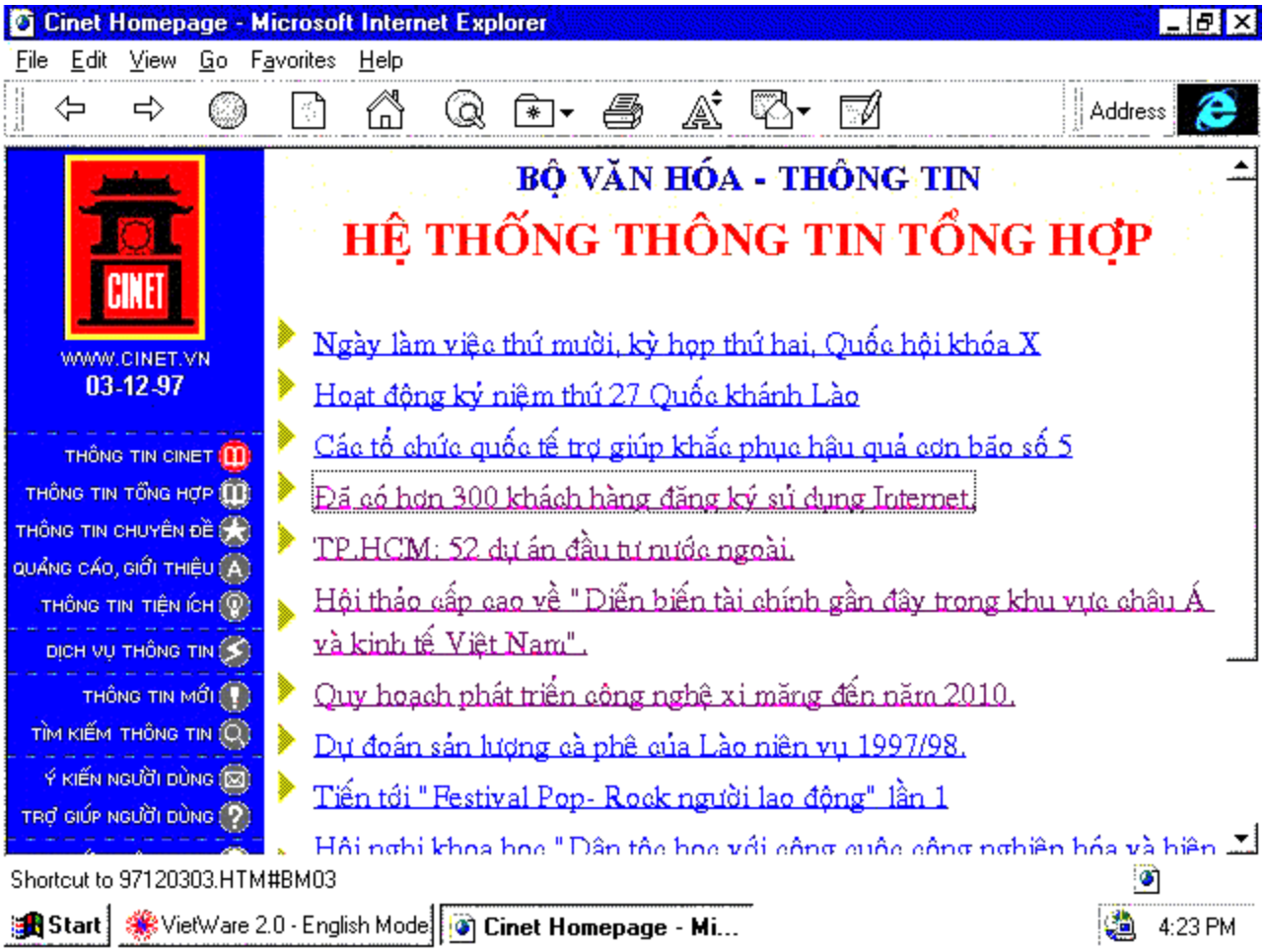
- **Thư điện tử** (Email): đây là dịch vụ đã có từ khi mạng ARPANET mới được thiết lập, nó cho phép gửi và nhận thư điến tử cho mọi thành viên khác trong mạng.

- **Thông tin mới** (News): Các vân đề thời sự được chuyển thành các diễn đàn cho phép mọi người quan tâm có thể trao đổi các thông tin cho nhau, hiện nay hiện nay có hàng nghìn diễ đàn về mọi mặt trên Internet.

- **Đăng nhập từ xa** (Remote Login): Bằng các chương trình như Telnet, Rlogin người sử dụng có thể từ một trạm của Internet đăng nhập (logon) vào một trạm khác nếu như người đó được đăng ký trên máy tính kia.

- **Chuyển file** (File transfer): Bằng chương trình FTP người sử dụng có thể chép các file từ một máy tính trên mạng Internet tới một máy tính khác. Người ta có thể chép nhiều phần mềm, cơ sở dữ liệu, bài báo bằng cách trên.

- **Dịch vụ WWW** (World Wide Web): WWW là một dịch vụ đặc biệt cung cấp thông tin từ xa trên mạng Internet. Các tập tin siêu văn bản được lưu trữ trên máy chủ sẽ cung cấp các thông tin và dẫn đường trên mạng cho phép người sử dụng dễ dàng Truy cập các tập tin văn bản, đồ họa, âm thanh.




*Hình 9.5: Ví dụ một trang Web cho phép dễ dàng khai thác các trang Web khác*

Người sử dụng nhận được thông tin dưới dạng các trang văn bản, một trang là một đơn thể nằm trong máy chu. Đây là dịch vụ đang mang lại sức thu hút to lớn cho mạng Internet, chúng ta có thể xây dựng các trang Web bằng ngôn ngữ HTML (Hypertext Markup Language) với nhiều dạng phong phú như văn bản, hình vẽ, video, tiếng nói và có thể có các kết nối với các trang Web khác. Khi các trang đó được đặt trên các máy chủ Web thì thông qua Internet người ta có thể xem được sự thể hiện của các trang Web trên và có thể xem các trang web khác mà nó chỉ đến.

Các phần mềm thông dụng được sử dụng hiện nay để xây dựng và duyệt các trang Web là Mosaic, Navigator của Netscape, Internet Explorer của Microsoft, Web Access của Novell.

**Chương 10 :**

# Giới thiệu về hệ điều hành mạng Windows NT

## I. Thế nào là một hệ điều hành mạng

Với việc ghép nối các máy tính thành mạng thì cần thiết phải có một hệ thống phần mềm có chức năng quản lý tài nguyên, tính toán và xử lý truy nhập một cách thống nhất trên mạng, hệ như vậy được gọi là hệ điều hành mạng. Mỗi tài nguyên của mạng như tệp, đĩa, thiết bị ngoại vi được quản lý bởi một tiến trình nhất định và hệ điều hành mạng điều khiển sự tương tác giữa các tiến trình và truy cập tới các tiến trình đó.

Căn cứ vào việc truy nhập tài nguyên trên mạng người ta chia các thực thể trong mạng thành hai loại chủ và khách, trong đó máy khách (Client) truy nhập được vào tài nguyên của mạng nhưng không chia sẻ tài nguyên của nó với mạng, còn máy chủ (Server) là máy tính nằm trên mạng và chia sẻ tài nguyên của nó với các người dùng mạng.

Hiện nay các hệ điều hành mạng thường được chia làm hai loại là hệ điều hành mạng ngang hàng (Peer-to-peer) và hệ điều hành mạng phân biệt (client/server).

Với hệ điều hành mạng ngang hàng mỗi máy tính trên mạng có thể vừa đóng vai trò chủ lẫn khách tức là chúng vừa có thể sử dụng tài nguyên của mạng lẫn chia sẻ tài nguyên của nó cho mạng, ví dụ: LANtastic của Artisoft, NetWare lite của Novell, Windows (for Workgroup, 95, NT Client) của Microsoft.

Với hệ điều hành mạng phân biệt các máy tính được phân biệt chủ và khách, trong đó máy chủ mạng (Server) giữ vai trò chủ và các máy cho người sử dụng giữ vai trò khách (các trạm). Khi có nhu cầu truy nhập tài nguyên trên mạng các trạm tạo ra các yêu cầu và gửi chúng tới máy chủ sau đó máy chủ thực hiện và gửi trả lời. Ví dụ các hệ điều hành mạng phân biệt: Novell Netware, LAN Manager của Microsoft, Windows NT Server của Microsoft, LAN Server của IBM, Vines của Banyan System với server dùng hệ điều hành Unix.

## II. Hệ điều hành mạng Windows NT

Windows NT là hệ điều hành mạng cao cấp của hãng Microsoft. Phiên bản đầu có tên là Windows NT 3.1 phát hành năm 1993, và phiên bản server là Windows NT Advanced Server (trước đó là LAN Manager for NT). Năm 1994 phiên bản Windows NT Server và Windows NT Workstation version 3.5 được phát hành. Tiếp theo đó ra đời các bản version 3.51. Các phiên bản workstation có sử dụng để thành lập mạng ngang hàng; còn các bản server dành cho quản lý file tập trung, in ấn và chia sẻ các ứng dụng.

Năm 1995, Windows NT Workstation và Windows NT Server version 4.0 ra đời đã kết hợp shell của người anh em Windows 95 nổi tiếng phát hành trước đó không lâu (trước

đây shell của Windows NT giống shell của Windows 3.1) đã kết hợp được giao diện quen thuộc, dễ sử dụng của Windows 95 và sự mạnh mẽ, an toàn, bảo mật cao của Windows NT.

Windows NT có hai bản mà nó đi đôi với hai cách tiếp cận mạng khác nhau. Hai bản này gọi là Windows NT Workstation và Windows NT server. Với hệ điều hành chuẩn của NT ta có thể xây dựng mạng ngang hàng, máy chủ mạng và mọi công cụ quản trị cần thiết cho một máy chủ mạng ngoài ra còn có thể có nhiều giải pháp về xây dựng mạng diện rộng. Cả hai bản Windows NT station và Windows NT server cùng được xây dựng trên cơ sở nhân NT chung và các giao diện và cả hai cùng có những đặc trưng an toàn theo tiêu chuẩn C2. Windows NT Wordstation được sử dụng để kết nối những nhóm người sử dụng nhỏ, thường cùng làm việc trong một văn phòng. Tuy nhiên với Windows NT server ta có được một khả năng chống hỏng hóc cao, những khả năng cung cấp dịch vụ mạng lớn và những lựa chon kết nối khác nhau, Windows NT Server không hạn chế về số người có thể thâm nhập vào mạng.

Với Windows NT ta cũng có những công cụ quản trị từ xa vào mạng mà có thể thực hiện được việc quản trị từ những máy tính ở xa. Nó thích hợp với tất cả các sơ đồ mạng BUS, STAR, RING và hỗn hợp.

Windows NT là hệ điều hành có sức mạnh công nghiệp đầu tiên cho số lượng khổng lồ các máy tính IBM compatible. Windows NT là một hệ điều hành thực sự dành cho người sử dụng, các cơ quan, các công ty xí nghiệp. Windows NT là một hệ điều hành đa nhiệm, đa xử lý với địa chỉ 32 bit bộ nhớ. Nó yểm trợ các ứng dụng DOS, Windows, Win32 GUI và các ứng dụng dựa trên ký tự. Windows NT server là một hệ điều hành mạng hoàn chỉnh, nó nhanh chóng được thừa nhận là một trong những hệ điều hành tốt nhất hiện nay vì:

- Là hệ điều hành mạng đáp ứng tất cả các giao thức truyền thông phổ dụng nhất. Ngoài ra nó vừa cho phép giao lưu giữa các máy trong mạng, vừa cho phép truy nhập từ xa, cho phép truyền file v.v... Windows NT là hệ điều hành vừa đáp ứng cho mạng cục bộ (LAN) vừa đáp ứng cho mạng diện rộng (WAN) như Intranet, Internet.

- Windows NT server hơn hẳn các hệ điều hành khác bởi tính mềm dẻo, đa dạng trong quản lý. Nó vừa cho phép quản lý mạng theo mô hình mạng phân biệt (Clien/Server), vừa cho phép quản lý theo mô hình mạng ngang hàng (peer to peer).

- Windows NT server đáp ứng tốt nhất các dịch vụ viễn thông, một dịch vụ được sử dụng rộng rãi trong tương lai.

- Windows NT server cài đặt đơn giản, nhẹ nhàng và điều quan trọng nhất là nó tương thích với hầu như tất cả các hệ mạng, nó không đòi hỏi người ta phải thay đổi những gì đã có.

- Cho phép dùng các dịch vụ truy cập từ xa (Remote access service - RAS), có khả năng phụp vụ đến 64 cổng truy nhập từ xa (trong đó Lan manager 16 cổng).

- Đáp ứng cho cả các máy trạm Macintosh nối với Windows NT server.

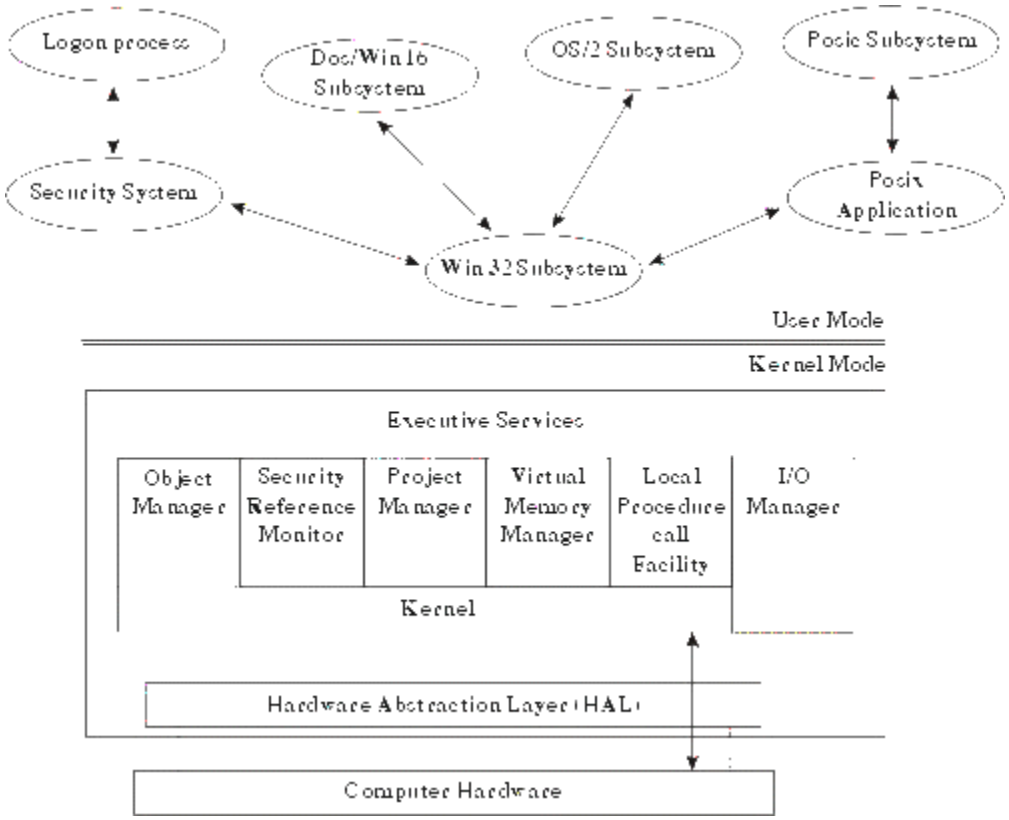
Windows NT yểm trợ mọi nghi thức mạng chuẩn như NetBUEI, IPX/SPX, TCP/IP và các nghi thức khác. Windows NT cũng tương thích với những mạng thông dụng hiên nay như Novell NetWare, Banyan VINES, và Microsoft LAN Manager. Đối với mạng lớn và khả năng thâm nhập từ xa sản phẩm Windows NT Server cũng cũng cấp các chức năng bổ xung nhu khả năng kết nối với máy tính lớn và máy MAC.

**III. Cấu trúc của hệ điều hành Windows NT**

Windows NT được thiết kế sử dụng cách tiếp cận theo đơn thể (modular). Các đơn thể khác nhau (còn được gọi là các bộ phận, thành phần) của Windows NT được trình bày trong hình 1 Các bộ phận của Windows NT có thể chạy dưới hai chế độ: User (người sử dụng) và Kernel (cốt lõi của hệ điều hành). Khi một thành phần của hệ điều hành chạy dưới cốt lõi của hệ điều hành (Kernel), nó truy cập đầy đủ các chỉ thị máy cho bộ xử lý đó và có thể truy cập tổng quát toàn bộ tài nguyên trên hệ thống máy tính.

Trong Windows NT: Executive Services, Kernel và HAL chạy dưới chế độ cốt lõi của hệ điều hành.

Hệ thống con (Subsystem) Win 32 và các hệ thống con về môi trường, chẳng hạn như DOS/Win 16.0S/2 và hệ thống con POSIX chạy dưới chế độ user. Bằng cách đặt các hệ thống con này trong chế độ user, các nhà thiết kế Windows NT có thể hiệu chỉnh chúng dễ dàng hơn mà không cần thay đổi các thành phần được thiết kế để chạy dưới chế độ Kernel.




*Hình 10.1: Cấu trúc Windows NT*

**Các lớp chính của hệ điều hành WINDOWS NT SERVER gồm:**

- ***Lớp phần cứng trừu tượng (Hardware Astraction Layer - HAL):*** Là phần cứng máy tính mà cốt lõi của hệ điều hành (Kernel) có thể được ghi vào giao diện phần cứng ảo, thay vì vào phần cứng máy tính thực sự. Phần lớn cốt lõi của hệ điều hành sử dụng HAL để truy cập các tài nguyên máy tính. Điều này có nghĩa là cốt lõi của hệ điều hành và tất cả các thành phần khác phụ thuộc vào cốt lõi có thể dễ dàng xuất (Ported) thông qua Microsoft đến các nền ( Platform ) phần cứng khác. Một thành phân nhỏ trong cốt lõi của hệ điều hành, cũng như bộ quản lý Nhập / Xuất truy cập phần cứng máy tính trực tiếp mà không cần bao gồm HAL.

- ***Lớp Kernel cốt lõi của hệ điều hành):*** Cung cấp các chức năng hệ điều hành cơ bản được sử dụng bởi các thành phần thực thi khác. Thành phần Kernel tương đối nhỏ và cung cấp các thành phần cốt yếu cho những chức năng của hệ điều hành. Kernel chủ yếu chịu trách nhiệm quản lý luồng, quản lý phần cứng và đồng bộ đa sử lý.

- **Các thành phần Executive:** Là các thành phần hệ điều hành ở chế độ Kernel thi hành các dịch vụ như :

  - Quản lý đối tượng (object manager)

- Bảo mật (security reference monitor)
- Quản lý tiến trình (process manager)
- Quản lý bộ nhớ ảo (virtual memory manager)
- Thủ tục cục bộ gọi tiện ích, và quản trị nhập/xuất (I/O Manager)

## IV.Cơ chế quản lý của Windows NT

### *1. Quản lý đối tượng* (Object Manager):

Tất cả tài nguyên của hệ điều hành được thực thi như các đối tượng. Một đối tượng là một đại diện trừu tượng của một tài nguyên. Nó mô tả trạng thái bên trong và các tham số của tài nguyên và tập hợp các phương thức (method) có thể được sử dụng để truy cập và điều khiển đối tượng.

Ví dụ một đối tượng tập tin sẽ có một tên tập tin, thông tin trạng thái trên file và danh sách các phương thức, như tạo, mở,đóng và xóa, đối tượng mô tả các thao tác có thể được thực hiện trên đối tượng file.

Bằng cách xử lý toàn bộ tài nguyên như đối tượng Windows NT có thể thực hiện các phương thức giống nhau như: tạo đối tượng, bảo vệ đối tượng, giám sát việc sử dụng đối tượng (Client object) giám sát những tài nguyên được sử dụng bởi một đối tượng.

Việc quản lý đối tượng (Object Manager) cung cấp một hệ thống đặt tên phân cấp cho tất cả các đối tượng trong hệ thống. Do đó, tên đối tượng tồn tại như một phần của không gian tên toàn cục và được sử dụng để theo dõi việc tạo và sử dụng đối tượng.

Sau đây là một số ví dụ của loại đối tượng Windows NT :

- Đối tượng Directory (thư mục).
- Đối tượng File (tập tin).
- Đối tượng kiểu object.
- Đối tượng Process (tiến trình).
- Đối tượng thread (luồng).
- Đối tượng Section and segment (mô tả bộ nhớ).
- Đối tượng Port (cổng).
- Đối tượng Semaphore và biến cố.

- Đối tượng liên kết Symbolic (ký hiệu).

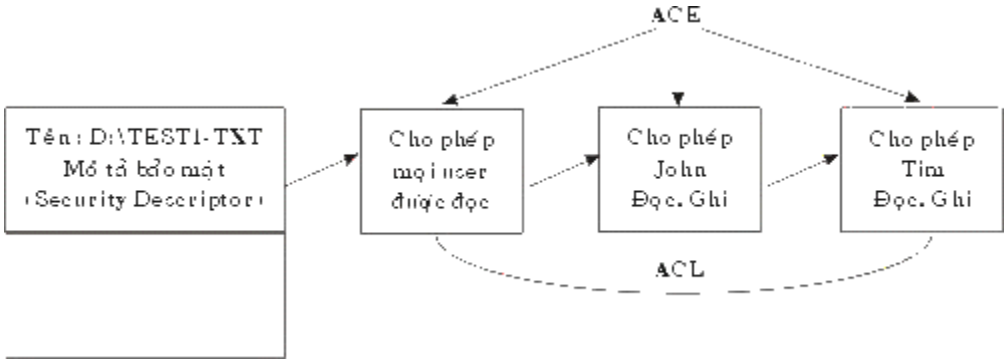
### *2. Cơ chế bảo mật* (SRM - Security Reference Monitor):

Được sử dụng để thực hiện vấn đề an ninh trong hệ thống Windows NT. Các yêu cầu tạo một đối tượng phải được chuyển qua SRM để quyết định việc truy cập tài nguyên được cho phép hay không. SRM làm việc với hệ thống con bảo mật trong chế độ user. Hệ thống con này được sử dụng để xác nhận user login vào hệ thống Windows NT.

Để kiểm soát việc truy cập, mỗi đối tượng Windows NT có một danh sách an toàn (Access Control List - ACL). Danh sách an toàn của mỗi đối tượng gồm những phần tử riêng biệt gọi là Access Control Entry (ACE). Mỗi ACE chứa một SecurityID (SID: số hiệu an toàn) của người sử dụng hoặc nhóm. Một SID là một số bên trong sử dụng với máy tính Windows NT mô tả một người sử dụng hoặc một nhóm duy nhất giữa các máy tính Windows NT.

Ngoài SID, ACE chứa một danh sách các hành động (action) được cho phép hoặc bị từ chối của một user hoặc một nhóm. Khi người sử dụng đăng nhập vào mạng Windows NT, sau khi việc nhận dạng thành công, một Security Access Token (SAT) được tạo cho người dùng đó. SAT chứa SID của người dùng và SID của tất cả các nhóm người dùng thuộc mạng Windows NT. Sau đó SAT hoạt động như một "passcard" (thẻ chuyển) cho phiên làm việc của người dùng đó và được sử dụng để kiểm tra tất cả hoạt động của người dùng.

Khi người dùng tham gia mạng truy cập một đối tượng, Security Reference Monitor kiểm tra bộ mô tả bảo mật của đối tượng xem SID liệt kê trong SAT có phù hợp với giá trị trong ACE không. Nếu phù hợp, các quyền về an ninh được liệt trong ACE áp dụng cho người dùng đó.




*Hình 10.2: Ví dụ về danh sách an toàn (Access Control List).*

### *3. Quản lý nhập / xuất (I/O Manager) :*

Chịu trách nhiệm cho toàn bộ các chức năng nhập / xuất trong hệ điều hành Windows NT. I/O Manager liên lạc với trình điều khiển của các thiết bị khác nhau.

**4. I/O *Manager:***

Ssử dụng một kiến trúc lớp cho các trình điều khiển. Mỗi bộ phận điều khiển trong lớp này thực hiện một chức năng được xác định rõ. Phương pháp tiếp cận này cho phép một thành phần điều khiển được thay thế dễ dàng mà không ảnh hưởng phần còn lại của các bộ phận điều khiển.

*Hình 10.3:Các trình điều khiển thiết bị theo lớp của I / O Manager*

## V. Các cơ chế bảo vệ dữ liệu trong Windows NT

Cơ chế bảo vệ dữ liệu của Windows NT gọi là fault tolerance, nó cho phép hệ thống khả năng tiếp tục làm việc và bảo toàn dữ liệu của hệ thống trong trường hợp một phần của hệ thống có sự cố hỏng hóc sai lệch. Trong Windows NT cơ chế fault tolerance bao gồm các biện pháp sau:

- Chống cúp điện bất thường.
- Cung cấp khả năng bảo vệ hệ thống đĩa (fault tolerance disk subsystem).
- Cung cấp khả năng sao chép dự phòng (backup) từ băng từ.

Khả năng bảo vệ hệ thống đĩa của Windows NT là RAID ø (viết tắt của Redundant Array of Inexpensiredisk). Thực chất RAID là một loạt các biện pháp để bảo vệ hệ thống đĩa. Các biện pháp trong RIAD được chia thành 6 mức sau:

- ***Mức 0*:** Đây là mức ứng với biện pháp chia nhỏ đĩa (disk striping). Thực chất nội dung của biện pháp này là phân chia dữ liệu thành khối và sau đó sắp xếp các khối dữ liệu theo thứ tự trong tất cả các đĩa thành 1 mảng.
- ***Mức 1*:** Mức này ứng với biện pháp disk Mirroring, biện pháp này cho phép tạo ra 2 đĩa giống nhau. Nếu trong quá trình vận hành mạng một đĩa có sự cố thì hệ thống sử dụng dữ liệu của đĩa kia.
- ***Mức 2*:** Mức này ứng với biện pháp phân chia nhỏ đĩa bằng cách phân chia các file thành các byte và sắp xếp các byte sang nhiều đĩa. Mức này sử dụng mã

sửa sai (error correcting code) trong quá trình phân chia đĩa. Nói chung biện pháp dùng ở mức này tốt hơn biện pháp dùng trong mức 1.

- ***Mức 3*:** Mức này sử dụng biện pháp giống mức 2. Tuy nhiên mã sửa sai (error correction code) chỉ sử dụng cho một đĩa. Không áp dụng cho nhiều đĩa như ở mức 2. Người ta thường dùng mức này để truy nhập vào một số ít file có dung tích lớn.

- ***Mức 4*:** Mức này sử dụng biện pháp giống ở mức 2 và 3 nhưng bằng phương pháp phân chia đĩa thành các khối lớn. Giống như mức 3 tất cả các mã sửa sai (error correction code) được hgi vào một đĩa và tách khỏi khối dữ liệu.

- ***Mức 5*:** Trong mức này người ta sử dụng biện pháp phân chia đĩa thành từng phần gọi là Striping with party. Biện pháp sử dụng ở mức này tương tự như ức 4, số liệu được phân nhỏ thành các khối lớn và sau đó ghi vào tất cả các đĩa. Các thông tin (party Infomation) được coi như các dữ liệu dùng tạm thời (data redundancy).

**Ngoài ra chúng ta còn có thể áp dụng các biện pháp bảo vệ dữ liệu trong Windows NT:**

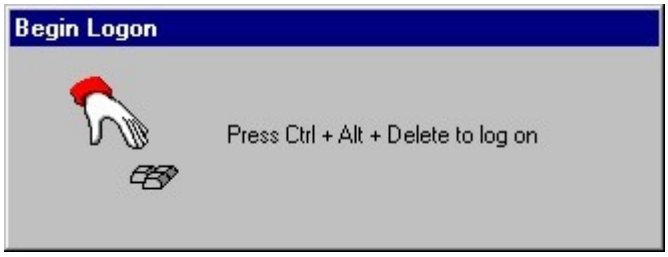
- ***Biện pháp Disk mirroring:*** Disk mirroring là cách sao tạm (redundant) lại đĩa hoặc partition. Biện pháp này bảo vệ dữ liệu tránh các sự cố bằng cách dưa ra chế độ thường xuyên backup đĩa hoặc partition. Hình dưới chỉ ra cách dùng biện pháp Mirroring:

- ***Disk Duplexing:*** Biện pháp dùng đĩa kép (Disk Duplexing) tường tự như disk mirroring chỉ khác là chúng dùng 2 disk controler. Diều này cho thên hả năng bảo vệ khi controler của một đĩa có sự cố. Trong khi đó biện pháp Mirror không thể khắc phục được tình huống này.

- ***Mirror Set:*** Các partition hoặc đĩa trong chế độ Mirror được tạo ra bằng cách lặp sao lại partition hoặc đĩa trên đĩa khác cùng một tên ổ đĩa được gán cho cả 2 partition. Ta có thể dùng establish Mirror trong menu Fault tolerance. Nếu đĩa hoặc partition trong chế độ Mirror bị lỗi thì chế độ Mirror cần phải ngắt để thực hiện chế độ sao chép dự phòng vào một đĩa riệng. Sau đó sao backup trở lại.

## VI. Giới thiệu về hoạt động của Windows NT Server

Khi chúng ta khởi động Windows NT Server hộp Begin logon sẽ hiện ra, server chờ đợi để chúng ta bấm Ctrl+Alt +Del để có thể tiếp tục hoạt động. Ở đậy có điểm khác với các hệ điều hành DOS, Windows 95 là tổ hợp Ctrl+Alt +Del không phải là khởi động lại máy. Trong trường hợp này Windows NT loại bỏ mọi chương trình Virus hay không có phép đang hoạt động trước khi bước vào làm việc.




*Hình 10.4: Thông báo gia nhập mạng*

Lúc này chúng ta sẽ thấy hộp Logon Information xuất hiện và yếu cầu chúng ta phải đánh đúng tên và mật khẩu thì mới được đăng nhập vào Server. Nếu là người dùng mới thì phải được người quản trị khai báo tên và mật khẩu trước khi đăng nhập..

*Hình 10.5: Màn hình gia nhập mạng*

Cũng giống như màn hình nền của hệ điều hành Windows 95 khi muốn thực hiện các trình, gọi các menu hệ thống chúng ta dùng nút Start ở cuối màn hình

*Hình 10.6: Điểm khởi đầu của Windows*

Trước muốn kết thúc chương trình và tắt máy chúng ta phải bấm phím Start rồi chọn ShutDown, màn hình kết thúc sẽ hiện ra cho chúng ta lựa chon công yêu cầu về tắt hay khởi động lại.

*Hình 10.7: Màn hình thoát khỏi Windows*

**Chương 11**

# Hệ thống quản lý của mạng Windows NT

Các mạng máy tính hiện nay được thiết kế rất đa dạng và đang thực hiện những ứng dụng trên nhiều lĩnh vực của đời sống xã hội. Điều đó có nghĩa là các thông tin lưu trữ trên mạng và các thông tin truyền giao trên mạng ngày càng mang nhiều giá trị có ý nghĩa sống còn. Do vậy những người quản trị mạng ngày càng phải quan tâm đến việc bảo vệ các tài nguyên của mình.

Việc bảo vệ an toàn là quá trình bảo vệ mạng khỏi bị xâm nhập hoặc mất mát, khi thiết kế các hệ điều hành mạng người ta phải xây dựng một hệ thống quản lý nhiều tầng và linh hoạt giúp cho người quản trị mạng có thể thực hiện những phương án về quản lý từ đơn giản mức độ thấp cho đến phức tạp mức độ cao trong những mạng có nhiều người tham gia. Thông qua những công cụ quản trị đã được xây dựng saün người quản trị có thể xây dựng những cơ chế về an toàn phù hợp với cơ quan của mình.

Thông thường hệ thống mạng có những mức quản lý chính sau:

- **Mức quản lý việc thâm nhập mạng (Login/Password):** Mức quản lý việc thâm nhập mạng (Login/Password) xác định những ai và lúc nào có thể vào mạng. Đối với người quản trị và người sử dụng mạng, mức an toàn này dường như khá đơn giản mà theo đó mỗi người sử dụng (người sử dụng) có một tên login và mật khẩu duy nhất.

- **Mức quản lý trong việc quản lý sử dụng các tài nguyên của mạng:** Kiểm soát những tài nguyên nào mà người sử dụng được phép truy cập, sử dụng và sử dụng như thế nào.

- **Mức quản lý với thư mục và file:** Mức an toàn của file kiểm soát những file và thư mục nào người sử dụng được dùng trên mạng và được sử dụng ở mức độ nào

- **Mức quản lý việc điều khiển File Server:** Mức an toàn trên máy chủ kiểm soát ai có thể được thực hiện các thao tác trên máy chủ như bật, tắt, chạy các chương trình khác. Người ta cần có cơ chế như mật khẩu để bảo vệ.

## I. Quản lý các tài nguyên trong mạng

Như chúng ta đã biết, mạng LAN cung cấp các dịch vụ theo hai cách: qua cách chia sẻ tài nguyên theo nguyên tắc ngang hàng và thông qua những máy chủ trung tâm. Dù bất cứ phương pháp nào được sử dụng, vấn đề cần phải giải quyết là là giúp người sử dụng xác định được các tài nguyên có saün ở đâu để có thể sử dụng.

Các kỹ thuật sau đây đã được sử dụng để tổ chức tài nguyên mạng máy tính:

- Quản lý đơn lẻ từng máy chủ (stand-alone services).
- Quản lý theo dịch vụ thư mục (directory services).
- Quản lý theo nhóm (workgroups).
- Quản lý theo domain (domains).

### 1. Quản lý đơn lẻ từng máy chủ (Stand-alone Services)

Với cách quản lý này trong mạng LAN thường chỉ có một vài máy chủ, mỗi máy chủ sẽ quản lý tài nguyên của mình, mỗi người sử dụng muốn thâm nhập những tài nguyên của máy chủ nào thì phải khai báo và chịu sự quản lý của máy chủ đó. Mô hình trên phù hợp với những mạng nhỏ với ít máy chủ và khi có trục trặc trên một máy chủ thì toàn mạng vẫn hoạt động. Cũng vì trong mạng LAN chỉ có ít máy chủ, do đó người sử dụng không mấy khó khăn để tìm các tập tin, máy in và các tài nguyên khác của mạng (plotter, CDRom, modem...).

Việc tổ chức như vậy không cần những dịch vụ quản lý tài nguyên phức tạp. Tuy nhiên khi trong mạng có từ hai máy chủ trở lên vấn đề trở nên phức tạp hơn vì mỗi máy chủ riêng lẻ giữ riêng bảng danh sách các người sử dụng và tài nguyên của mình. Khi đó mỗi người sử dụng phải tạo lập và bảo trì tài khoản của mình ở hai máy chủ khác nhau mới có thể đăng nhập (logon) và truy xuất đến các máy chủ này. Ngoài ra việc xác định vị trí của các tài nguyên trong mạng cũng rất khó khăn khi mạng có qui mô lớn.

### 2. Quản lý theo dịch vụ thư mục (Directory Services)

Hệ thống các dịch vụ thư mục cho phép làm việc với mạng như là một hệ thống thống nhất, tài nguyên mạng được nhóm lại một cách logic để dễ tìm hơn. Giải pháp này có thể được dùng cho những mạng lớn. Ở đây thay vì phải đăng nhập vào nhiều máy chủ, người sử dụng chỉ cần đăng nhập vào mạng và được các dịch vụ thư mục cấp quyền truy cập đến tài nguyên mạng, cho dù được cung cấp bởi bất kể máy chủ nào.

Người quản trị mạng chỉ cần thực hiện công việc của mình tại một trạm trên mạng mặc dù các điểm nút của nó có thể nằm trên cả thế giới. Hệ điều hành Netware 4.x cung cấp dịch vụ nổi tiếngi và đầy ưu thế cạnh tranh này với tên gọi ***Netware Directory Services (NDS).***

Giải pháp này thích hợp với những mạng lớn. Các thông tin của NDS được đặt trong một hệ thống cơ sở dữ liệu đồng bộ, rộng khắp được gọi là DIB (Data Information Base). Cơ sở dữ liệu trên quản lý các dữ liệu dưới dạng các đối tượng phân biệt trên toàn mạng. Các định nghĩa đối tượng sẽ được đặt trên các tập tin riêng của một số

máy chủ đặc biệt, mỗi đối tượng có các tính chất và giá trị của mỗi tính chất. Đối tượng bao hàm tất cả những gì có tên phân biệt như Người sử dụng, File server, Print server, group. Mỗi loại đối tượng có những tính chất khác nhau ví dụ như đối tượng Người sử dụng có tính chất về nhóm mà người sử dụng đó thuộc, còn nhóm có các tính chất về người sử dụng mà nhóm đó chứa.

Việc thiết lập các dịch vụ như vậy cần được lập kế hoạch, thiết kế rất cẩn thận, liên quan đến tất cả các đơn vị phòng ban có liên quan. Loại mạng này có khuyết điểm là việc thiết kế, thiết lập mạng rất phức tạp, mất nhiều thời gian nên không thích hợp cho các mạng nhỏ.

### 3. Quản lý theo nhóm (Workgroup)

Các nhóm làm việc làm việc theo ý tưởng ngược lại với các dịch vụ thư mục. Nhóm làm việc dựa trên nguyên tắc mạng ngang hàng (peer-to-peer network), các người sử dụng chia sẻ tài nguyên trên máy tính của mình với những người khác, máy nào cũng vừa là chủ (server) vừa là khách (client). Người sử dụngï có thể cho phép các người sử dụng khác sử dụng tập tin, máy in, modem... của mình, và đến lượt mình có thể sử dụng các tài nguyên được các người sử dụng khác chia sẻ trên mạng. Mỗi cá nhân người sử dụng quản lý việc chia sẻ tài nguyên trên máy của mình bằng cách xác định cái gì sẽ được chia sẻ và ai sẽ có quyền truy cập. Mạng này hoạt động đơn giản: sau khi logon vào, người sử dụng có thể duyệt (browse) để tìm các tài nguyên có saün trên mạng.

Workgroup là nhóm logic các máy tính và các tài nguyên của chúng nối với nhau trên mạng mà các máy tính trong cùng một nhóm có thể cung cấp tài nguyên cho nhau. Mỗi máy tính trong một workgroup duy trì chính sách bảo mật và CSDL quản lý tài khoản bảo mật SAM (Security Account Manager) riêng ở mỗi máy. Do đó quản trị workgroup bao gồm việc quản trị CSDL tài khoản bảo mật trên mỗi máy tính một cách riêng lẻ, mang tính cục bộ, phân tán. Điều này rõ ràng rất phiền phức và có thể không thể làm được đối với một mạng rất lớn.

Nhưng workgroup cũng có điểm là đơn giản, tiện lợi và chia sẽ tài nguyên hiệu quả, do đó thích hợp với các mạng nhỏ, gồm các nhóm người sử dụng tương tự nhau.

Tuy nhiên Workgroup dựa trên cơ sở mạng ngang hàng (peer-to-peer), nên có hai trở ngại đối với các mạng lớn như sau:

- Đối với mạng lớn, có quá nhiều tài nguyên có saün trên mạng làm cho các người sử dụng khó xác định chúng để khai thác.

- Người sử dụng muốn chia sẻ tài nguyên thường sử dụng một cách dễ hơn để chia sẻ tài nguyên chỉ với một số hạn chế người sử dụng khác.

Điển hình cho loại mạng này là Windws for Workgroups, LANtastic, LAN Manager... Window 95, Windows NT Workstation.

### 4. Quản lý theo vùng (Domain)

Domain mượn ý tưởng từ thư mục và nhóm làm việc. Giống như một workgroup, domain có thể được quản trị bằng hỗn hợp các biện pháp quản lý tập trung và địa phương. Domain là một tập hợp các máy tính dùng chung một nguyên tắc bảo mật và CSDL tài khoản người dùng (người sử dụng account). Những tài khoản người dùng và nguyên tắc an toàn có thể được nhìn thấy khi thuộc vào một CSDL chung và được tập trung.

Giống như một thư mục, một domain tổ chức tài nguyên của một vài máy chủ vào một cơ cấu quản trị. Người sử dụng được cấp quyền logon vào domain chứ không phải vào từng máy chủ riêng lẻ. Ngoài ra, vì domain điều khiển tài nguyên của một số máy chủ, nên việc quản lý các tài khoản của người sử dụng được tập trung và do đó trở nên dễ dàng hơn là phải quản lý một mạng với nhiều máy chủ độc lập.

Các máy chủ trong một domain cung cấp dịch vụ cho các người sử dụng. Một người sử dụng khi logon vào domain thì có thể truy cập đến tất cả tài nguyên thuộc domain mà họ được cấp quyền truy cập. Họ có thể dò tìm (browse) các tài nguyên của domain giống như trong một workgroup, nhưng nó an toàn, bảo mật hơn.

Để xây dựng mạng dựa trên domain, ta phải có ít nhất một máy Windows NT Server trên mạng. Một máy tính Windows NT có thể thuộc vào một workgroup hoặc một domain, nhưng không thể đồng thời thuộc cả hai. Mô hình domain được thiết lập cho các mạng lớn với khả năng kết nối các mạng toàn xí nghiệp hay liên kết các kết nối mạng với các mạng khác và những công cụ cần thiết để điều hành.

Việc nhóm những người sử dụng mạng và tài nguyên trên mạng thành domain có lợi ích sau:

- Mã số của người sử dụng được quản lý tập trung ở một nơi trong một cơ sở dữ liệu của máy chủ, do vậy quản lý chặt chẽ hơn.

- Các nguồn tài nguyên cục bộ được nhóm vào trong một domain nên dễ khai thác hơn.

*Quản lý theo Workgroup và domain là hai mô hình mà Windows NT lựa chọn. Sự khác nhau căn bản giữa Workgroup và domain là trong một domain phải có ít nhất một máy chủ (máy chủ) và tài nguyên người sử dụng phải được quản lý bởi máy chủ đó.*

## II. Hệ thống quản lý trên Hệ điều hành mạng Windows NT Server

Windows NT cung cấp những chức năng tuân theo chuẩn C2 (chuẩn về an toàn quốc tế) trong đó Windows NT đảm bảo tránh được những người không được phép vào trong hệ thống hoặc thâm nhập vào các file và chương trình trên đĩa cứng. Người ta không thể thâm nhập vào được nếu không có mật khẩu đúng. và qua đó đã bảo vệ

được các file. Windows NT cung cấp công cụ để xây dựng các lớp quyền dành cho nhiều nhiệm vụ khác nhau nhằm xây dựng hệ thống an toàn một cách mềm dẻo.

Nhiều người sử dụng có thể có quyền vào một máy chủ Windows NT. Một tài khoản của người sử dụng trên máy bao gồm tên, mật khẩu và nhiều tính chất được cho bởi người quản trị mạng. Người sử dụng có thể che các thư mục hay file của mình từ những người khác và cài đặt các thông số của File manager, Programe Manager, Control Panel một cách phù hợp.

Khi người dùng thâm nhập vào hệ thống thì tự động khởi động mọi thông số đã được lưu trữ từ trước. Nếu người sử dụng có quyền cao hơn thì họ có thể chia sẻ hoặc ngừng các tài nguyên đang dùng chung trên mạng như máy in hay file hoặc họ có thể thay đổi quyền của những người dùng mạng khác khi thâm nhập vào mạng.

### 1. Mô hình Workgroup (nhóm) của mạng Windows NT

Mỗi người truy cập vào mạng Windows NT tổ chức theo mô hình Workgroup cần phải đăng ký:

- Tên vào mạng
- Mật khẩu vào mạng

Dựa vào tên và mật khẩu đã cho, Windows NT cung cấp cho người một số gọi là mã số của người sử dụng (user account). Mã số này được lưu dữ trong cơ sở dữ liệu là hệ thống quản trị tài nguyên (SAM - Security Account Manager database). Hệ thống quản trị tài nguyên dùng để đảm bảo an toàn về tài nguyên trên mạng. Người vào mạng muốn truy nhập vào tài nguyên phải qua sự kiểm duyệt của hệ thống quản trị tài nguyên. Trong mô hình Workgroup mỗi máy trạm có một nguồn tài nguyên tương ứng với một hệ thống quản trị tài nguyên bảo vệ nó.

**Chú ý:** Mỗi người khai thác mạng phải nhớ nhiều mã số, vì ứng với mỗi máy trạm có một hệ thống quản trị tài nguyên riêng của nó.

### 2. Mô hình vùng (Domain)

Domain là một khái niệm rất cơ bản trong Windows NT server, nó là hạt nhân để tổ chức các mạng có quy mô lớn.

Mỗi người tham gia trong Domain cần phải đăng ký thông tin sau:

- Tên Domain
- Tên người sử dụng
- Mật khẩu

Các thông tin này được lưu ở máy chủ dưới dạng một mã số, gọi là tài khoản người sử dụng (user account) và các mã số cũa người sử dụng trong một domain được tổ chức thành một cơ sở dữ liệu trên máy chủ. Khi người sử dụng muốn truy nhập vào một Domain người đó phải chọn tên Domain trong hộp thoại trên máy trạm. Máy trạm sẽ chuyển các thông tin về hệ thống quản trị tài nguyên (SAM - Security Account Manager database) của Domain để kiểm tra. Khi đó hệ thống quản trị tài nguyên trên máy chủ sẽ kiểm tra các thông tin này, nếu kết quả kiểm tra là đúng, người khai thác mới được quyền truy nhập vào tài nguyên của Domain.

Một máy Windows NT mà không tham gia vào một Domain có nhược điểm sau:

- Máy trạm chỉ có thể cung cấp các mã số được tạo ra trên nó. Nếu máy này bị hư hỏng thì những người khai thác mạng không thể truy nhập bằng mã số của họ. Nếu máy này nằm trong một Domain nào đó thì các mã số này còn được lưu trong SAM của một Domain trên máy Máy chủ.

- Qua máy trạm không tham gia vào Domain, người khai thác mạng không thể truy nhập vào tài nguyên của Domain, mặc dù mã số của của người này có trong SAM của Domain

Trong một Domain thường có các loại máy thực hiện những công việc sau:

- Primary domain Controller (PDC), bao giờ cũng phải có để quản trị hệ thống các người sử dụng và các tài khoản trong Domain (hệ thống này gọi là cơ sở dữ liệu SAM - Security Account Manager của Domain). SAM trên máy chủ được thiết kế như hệ thống kiểm soát Domain. Trong một Domain chỉ có duy nhất một PDC.

- Ngoài ra hệ thống còn có một hay nhiều máy làm Backup Domain Controller (BDC). Các BDC có thể dùng thay thế cho máy PDC trong trường hợp cần thiết, chẳng hạn máy PDC bị hư

Người quản trị Domain chỉ cần tạo tài khoản người sử dụng (user account) chỉ một lần trên máy Primary Domain Controller, thông tin được tự động copy đến các máy Backup Domain Controller.

### 3. Mô hình quan hệ giữa các Domain trong mạng Windows NT

Trong một mạng có thể có nhiều Domain nhưng một máy tính Windows NT là thành viên của chỉ một domain tại mỗi thời điểm. Tuy nhiên, có một vài trường hợp đôi khi chúng ta cần truy cập tài nguyên trong những domain khác, để là được điều này hệ điều hành Windows NT server cho phép giữa các Domain có thể tồn tại một quan hệ gọi là quan hệ tin cậy (trust relationship). Chúng ta có thể sử dụng quan hệ tin cậy giữa các Domain cho phép người dùng trên một Domain truy cập tài nguyên trong Domain khác.

Hai Domain A, B gọi là quan hệ tin cậy (trust relationship) mà trong đó Domain A tin cậy Domain B nếu giữa chúng có một mối liên kết sao cho người khai thác mạng của Domain B có thể truy nhập vào Domain A từ một máy trạm trong Domain B.

Từ góc độ của người quản trị mạng mục đích của việc thiết lập quan hệ tin cậy giữa các Domain là làm cho việc quản lý mạng trở lên đơn giản hơn bằng cách kết hợp các Domain vào một đơn vị quản lý. Trong quan hệ tin cậy các Domain được chia ra như sau:

- Domain được tin cậy (trusted domain)
- Domain tin cậy (trusting domain)

Một Domain là loại này hoặc loại kia *thông thường* phụ thuộc vào nó chứa mã số của người sử dụng (người sử dụng account) hay chỉ chứa tài nguyên (resource)

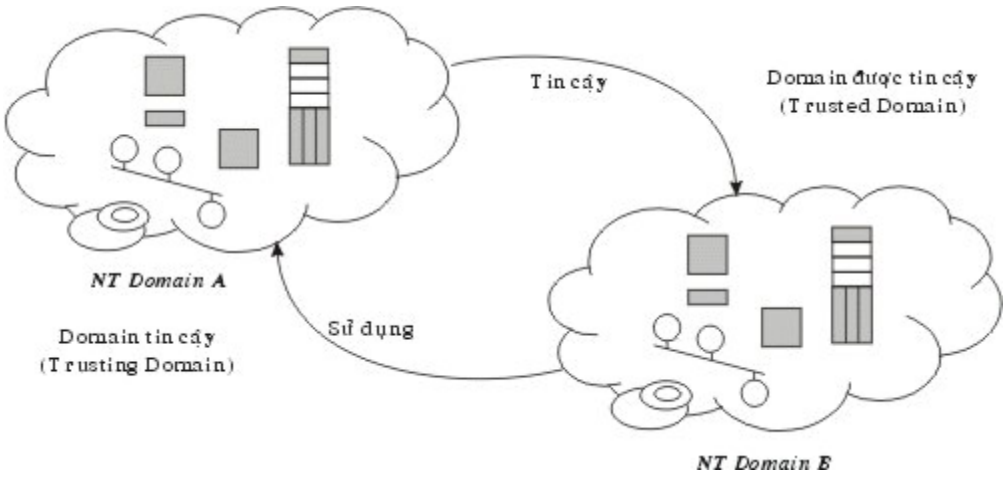
- Domain tin cậy (trusting domain) là Domain chứa tài nguyên.
- Domain được tin cậy (trusted domain) là Domain chứa mã số người sử dụng.

Khi người sử dụng truy nhập từ một máy trạm trong Domain tin cậy (trusting domain) vào Domain được tin cậy (trusted domain) thì quá trình kiểm soát diễn ra như sau:

- Người sử dụng phải cho mã số (mã số này ứng với tên, mật khẩu, tên domain cần truy nhập)
- Mã số được chuyển về máy chủ của Domain tin cậy.
- Máy chủ của Domain tin cậy chuyển mã số này sang Domain được tin cậy.
- Kết quả kiểm tra của máy chủ trong Domain được tin cậy diễn ra theo quá trình ngược lại.

**Ở đây chúng ta chú ý:**

- Việc liên kết giữa các Domain không có tính bắc cầu.
- Thông qua việc thiết lập mối quan hệ tin tưởng, chúng ta có thể sử dụng một tài khoản để truy xuất đến nhiều tài nguyên của nhiều Domain. Có thể quản trị nhiều Domain từ một vị trí tập trung.




*Hình 11.1: Mô hình tin cậy của các Domain trong mạng Windows NT*

### 4. Nhóm (group) trong Windows NT

Trong mạng Windows NT khái niệm nhóm (group) là một trong những khái niệm quan trọng đối với công việc quản lý, điều hành mạng Windows NT. Nhóm làm cho việc khai thác tài nguyên được dễ dàng thuận lợi và đơn giản hóa việc quản trị. Mỗi nhóm được đăng ký bởi một tài khoản (group account) và có các thành viên của nó. Các quyền đã được gán cho nhóm sẽ tự động gán cho các người sử dụng là thành viên của nhóm. Các tiện lợi của nhóm như sau:

- Quyền có thể được gán cho, hoặc hủy đi trên mọi thành viên của nhóm.
- Khi một người sử dụng bị loại ra khỏi nhóm, thì tự động bị mất các quyền đã được cấp khi còn trong nhóm.

Trong mạng Windows NT người ta phân biệt phân biệt hai loại nhóm là nhóm toàn cục (global group) và nhóm cục bộ (local group).

### 5. Nhóm toàn cục (global group)

Nhóm toàn cục còn được gọi là nhóm vùng (domain group). Thành viên của nhóm là các người dùng cấp vùng (domain user). Họ ngược lại với người dùng cục bộ (local user) là người có phạm vi giới hạn trong máy tính mà họ được xác định. Thành viên của nhóm toàn cục được phép chuyển ra ngoài (export) một Domain khác. Phạm vi của nhóm toàn cục là toàn bộ vùng trên đó user dược xác định, và thấy được từ bất kỳ máy tính NT nào trong vùng đó. Quyền có thể được gán cho nhóm toàn cục cho các tài nguyên trên một máy NT Server hay NT Workstation trong vùng.

Các tài khoản nhóm toàn cục được lưu ở PDC (Primary DomainController) của Domain, và được sao lưu đến các BDC (Backup Domain Controller) trong Domain đó.

Nhóm toàn cục có những đặc trưng sau:

- Thành viên của nhóm phải là các người sử dụng của domain (domain user account).
- Nhóm toàn cục có thể được gán quyền cho tài nguyên bất kỳ trong vùng mà chúng được xác định.
- Nhóm toàn cục có thể được gán quyền đến các tài nguyên trong vùng khác với vùng chúng được xác định khi quan hệ tin cậy (trust relationship) giữa các vùng có hiệu lực.
- Các thành viên của nhóm toàn cục có thể sử dụng nguồn tài nguyên trong vùng bất kỳ mà nhóm toàn cục có quyền.
- Nhóm toàn cục chỉ chứa mã số của người sử dụng trong Domain của nó. Nó không thể chứa các nhóm cục bộ và nhóm toàn cục khác.

### 6. Nhóm cục bộ (local group)

Nhóm cục bộ, trái lại, được gán quyền cho nguồn tài nguyên trên máy NT mà nó được xác định. Nếu máy NT là một phần của vùng, thì để tiện cho việc gán quyền, một nhóm cục bộ có thể chứa các tài khoản người dùng cấp vùng (domain user account) và các nhóm toàn cục trong Domain đó, nơi máy tính NT là thành viên, hoặc những người dùng từ Domain được tin cậy. Các người dùng cấp vùng (domain user) có thể được gán quyền truy cập đến tài nguyên bất kỳ trong Domain đó.

Nếu Windows NT computer không nối với mạng thì các thành viên trong local group có thể được gán quyền để truy xuất đến tài nguyên trên máy tính mà trong đó các thành viên được tạo ra còn nếu Windows NT computer nối vào mạng thì để tiện lợi cho việc phân quyền thì người quản trị mạng có thể đưa global group và domain user vào trong local group .

Có hai loại nhóm cục bộ: ***nhóm cục bộ trạm làm việc (workstation local group)*** và ***nhóm cục bộ vùng (domain local group).*** Một mạng làm việc theo cơ chế vùng bao gồm cả Windows NT Server và Windows NT Workstation việc hiểu rõ sự khác nhau giữa hai loại nhóm cục bộ là rất quan trọng.

#### *a. Nhóm cục bộ trạm làm việc (Workstation local group):*

Nhóm cục bộ trạm làm việc hiện diện trên Windows NT Workstation trên đó chúng được tạo ra. Chúng được chứa trong dữ liệu SAM lưu trữ trên Windows NT Workstation. Một người dùng cục bộ được tạo ra bằng công cụ *User Manager* của Windows NT Workstation (khác với công cụ *User Manager for Domains* trên Windows NT Server) có thể có quan hệ thành viên chỉ trong nhóm cục bộ của trạm làm việc đó.

Một nhóm cục bộ trong một trạm làm việc chỉ có thể được dùng trên máy tính trên đó nhóm được tạo ra, và không thể làm việc rên bất kỳ máy Windows NT nào khác.

Nhóm cục bộ trạm làm việc có thể chứa:

- Các tài khoản người dùng cục bộ từ trạm làm việc trên đó nó được xác định.
- Các tái khoản người dùng cấp vùng (domain user account) và các nhóm toàn cục từ vùng trong đó họ được xác định.
- Các tái khoản người dùng cấp vùng (domain user account) và các nhóm toàn cục từ các vùngï được ủy quyền.

### *b. Nhóm cục bộ vùng (Domain local group):*

**N**hóm cục bộ vùng hoạt động trên Windows NT Server ở mức vùng, và được tạo ra bằng *User Manager for Domains* (trên Windows NT Server). Các nhóm cục bộ vùng chỉ có thể hiện hữu trên máy Windows NT Server tạo ra nó. Do đó, các nhóm cục bộ vùng có thể dùng để truy cập nguồn tài nguyên trên máy tính Windows NT Server trong vùng đó, mà không dùng để truy cập nguồn tài nguyên trên máy tính Windows NT Workstation trong vùng này. Nhóm cục bộ vùng không thể được gán quyền trên bộ điều khiển không có cấp vùng, thậm chí cả các máy chủ.

## III. Các mô hình Domain trong mạng Windows NT

Windows NT máy chủ cung cấp 4 kiểu tổ chức domain gọi tắt là các mô hình domain (domain models). Dưới đây là 4 mô hình tổ chức của nó:

- Mô hình domain đơn (single domain)
- Mô hình domain chính (master domain)
- Mô hình multiple master domain
- Mô hình complete truts

### 1. Mô hình Domain đơn (single domain)

Mô hình domain đơn là mô hình trong mạng chỉ có một domain. Mô hình này thích hợp cho mạng ít người khai thác, cần quản lý tập trung. Mô hình đơn nói chung tương tự như mô hình workgroup, trong mô hình này người sử dụng có thể xem xét, khai thác tài nguyên theo cả mô hình workgroup và mô hình domain.

Loại mô hình này không có các quan hệ ủy quyền vì chỉ có một domain duy nhất, domain này cũng chứa CSDL SAM cho toàn bộ mạng và việc quản trị mạng có thể thực hiện từ một vị trí trung tâm.

Các tài khoản người dùng trong vùng (domain user account) và tài khoản nhóm trong vùng (domain group acconunt) có thể được xây dựng và có các quyền truy cập tài nguyên được gán trên các nhóm và người dùng riêng rẽ và có một phạm vi bao gồm tất cả các máy vi tính trong vùng.

Trong mô hình Domain đơn vấn đề an toàn dữ liệu, quản lý hệ thống được xem xét một cách tốt hơn so với Workgroup.

### 2. Mô hình Domain chính (Master domain)

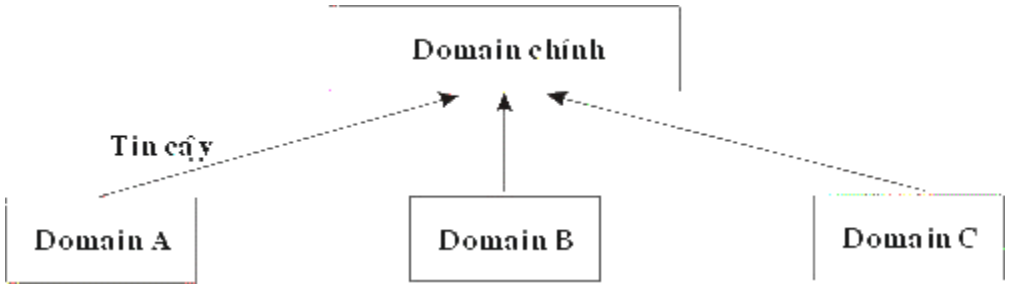
Mô hình Domain chính có thể được sử dụng cho các cơ quan khi họ muốn tổ chức mạng thành nhiều Domain tài nguyên (Resource domain) nhưng vẫn có những tiện lợi trong việc quản lý tập trung. Bằng cách phân chia tài nguyên mạng vào nhiều Domain, chúng ta sẽ tiện tổ chức và quản lý một lượng tài nguyên lớn. Một Domain chủ (master domain) được sử dụng để hổ trợ việc quản trị tập trung mà trong đó tất cả mã số của người sử dụng và mã số các nhóm toàn cục (global group) trên mạng được lưu giữ.

Đặc điểm của mô hình domain chính :

- Mô hình Master Domain là mô hình có nhiều Domain, trong đó có 1 Domain là Domain chính (premery domain). Mô hình này thích hợp cho mạng có số người dùng không quá lớn, nhưng cần phải phân chia thành các đơn vị nhỏ hơn nhưng việc quản lý được tiến hành tập trung.

- Trong mô hình này tất cả mã số của người khai thác mạng và mã số của các nhóm toàn cục (global group) đều chứa trên server trên Domain chính.

- Trong mô hình này tất cả các khác Domain đều tin cậy với Domain chính.




*Hình 11.2: Mô hình Domain chính*

Trong mô hình này mã số của người sử dụng quản lý tập trung và các nhóm toàn cục chỉ cần xác định một lần trong Domain chính. Tài nguyên được nhóm logic thành các đơn vị nhỏ hơn để có thể quản lý bởi từng Domain.

Mô hình Domain chính là mô hình quản lý tập trung vì vậy chiến lược phát triển mạng cần dựa vào các nhóm cục bộ và các nhóm toàn cục.

Mô hình này không những quản lý tập trung các mã số của người sử dụng mà còn cung cấp các dịch vụ như cài đặt phần mềm, sao chép backup cho tất cả các máy chủ trên mạng.

Tuy nhiên mô hình này có nhược điểm có thể gây ùn tắc nếu có quá nhiều nhóm và nhiều người dùng và các nhóm cục bộ cần phải xác định trong mỗi Domain mà chúng được sử dụng.

### 3. Mô hình nhiều Domain chính (muliple master domain)

Mô hình **nhiều Domain chính** (muliple master domain) có thể được sử dụng cho các tổ chức có nhiều khu vực và mỗi khu vực có nhiều bộ phận. Trong nhiều mạng kiểu như vậy, bộ phận điều hành riêng biệt cho mỗi khu vực muốn quản lý tập trung các tài nguyên mạng trong khu vực. Chúng ta xây dựng một Domain chủ (master domain) cho mỗi khu vực và chia các tài nguyên trong mỗi khu vực thành nhiều Domain tài nguyên (resoure domain) riêng biệt.

Trên mô hình này tồn tại các quan hệ sau:

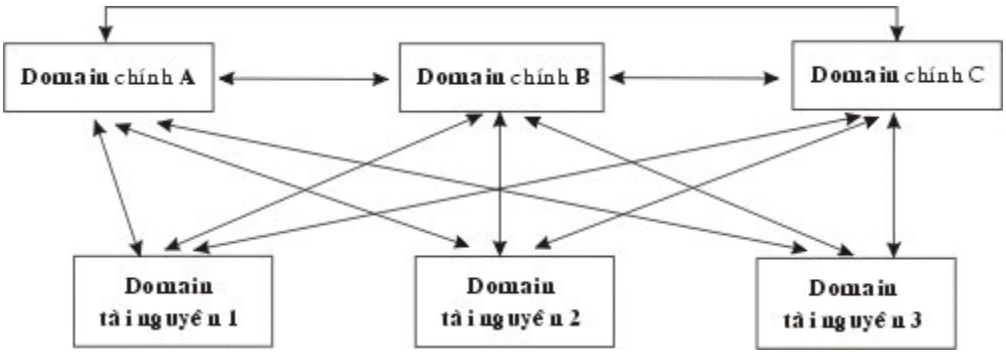
- Mỗi Domain chính quan hệ tin cậy hai chiều với các domain chính khác. Điều này cho phép mỗi Domain chính có thể quản lý các domain chính khác.

- Các Domain không phải là chính không có mã số của người sử dụng mà chỉ cung cấp tài nguyên trên mạng.

- Các Domain không phải là chính tin cậy đối với tất cả các Domain chính. Nhờ điều này mỗi mã số của người sử dụng sẽ được sử dụng trên tất cả các Domain chính và có được quyền truy nhập vào tài nguyên trong các tài nguyên trên các Domain khác của mạng.

Bằng cách phân chia tài nguyên mạng thành nhiều Domain, chúng ta có nhiều thuận lợi trong việc tổ chức quản lý một số lượng lớn các tài nguyên trong các đơn vị phù hợp.

Mô hình nhiều Domain chính có ưu điểm đối với mạng nhiều người dùng trong đó các tài nguyên được nhóm một cách logic theo công việc. Tuy nhiên các nhóm cục bộ và toàn cục phải xác định nhiều lần và mã số của người sử dụng phải chứa ở nhiều Domain chính .

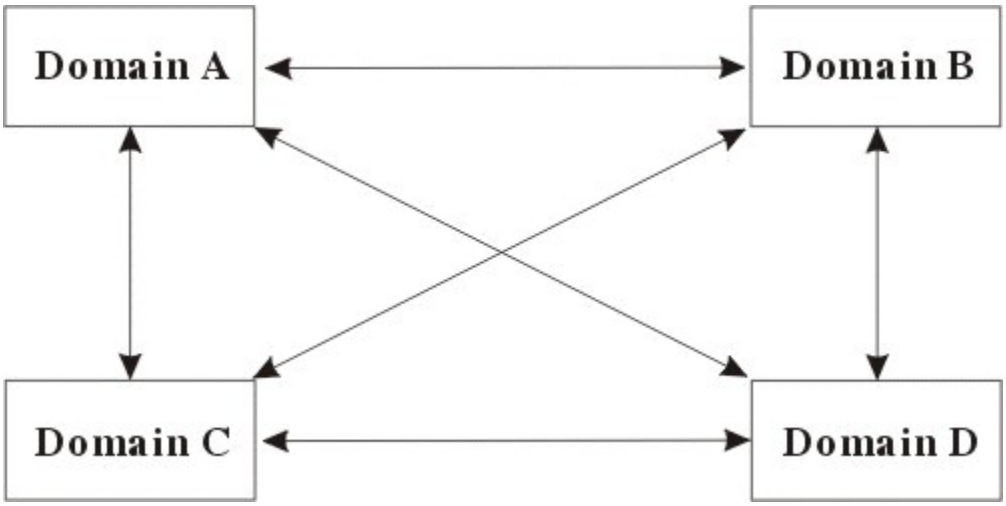



*Hình 11.3: Mô hình nhiều Domain chính*

### 4. Mô hình tin cậy hoàn toàn (complete trust)

Mô hình tin cậy hoàn toàn là mô hình mà trong đó mỗi Domain là quan hệ tin cậy 2 chiều với các Domain khác. Với mô hình này, người sử dụng có thể truy nhập vào bất kỳ Domain nào trên mạng từ một máy trạm nào đó.

Mô hình này có thể áp dụng với qui mô mạng tùy ý và phù hợp cho các cơ quan không có nhóm quản trị tập trung, nó cho phép không hạn chế số người khai thác mạng và số nhóm. Mỗi bộ phận trong đơn vị có thể kiểm soát được mã số của người sử dụng cũng như tài nguyên của bộ phận mình trong đó tài nguyên và mã số người sử dụng được nhóm thành một Domain.




*Hình 11.4: Mô hình nhiều Mô hình tin cậy hoàn toàn*

## IV. Các mặt hạn chế của những mô hình Domain

Mô hình vùng có một số kẽ hở về cấu trúc. Những hạn chế về domain được thảo luận ở đây nhằm mục đích giúp bạn thiết kế mạng chính xác và hoàn hảo.

- Domain NT đơn điệu theo nghĩa là không có cách nào diễn tả quan hệ phân cấp hoặc nhóm tài nguyên trong một vùng đơn. Người dùng có thể sử dụng những quyền được ủy thác thể hiện các quan hệ giữa những vùng, nhưng đây là quan hệ sử dụng và không thích hợp cho việc tổ chức mạng dựa trên phạm vi địa lý, tài nguyên sở hữu, logic hoặc nền tảng sơ đồ tổ chức.

- Mô hình vùng Domain chính duy nhất theo Microsoft thích hợp cho các mạng ít hơn 40.000 người dùng và nhóm. Khi số người dùng và nhóm tăng lên, số quan hệ ủy quyền và chi phí quản lý quan hệ cũng tăng. Nói cách khác chi phí quản lý mạng có thể tăng bất thình lình khi kích thước mạng tăng.

- Người dùng phải cẩn trọng về kẻ hở của quan hệ ủy quyền - đặc biệt quan hệ ủy quyền hai chiều. Nếu không cẩn thận trong việc gán các quan hệ ủy quyền và không có kế hoạch đúng đắn, người sử dụng có thể kết thúc bằng một mô hình ủy quyền trọn vẹn, với tất cả những hạn chế của mô hình đi kèm.

- Ngoài ra có một nguy cơ thực sự sẽ xảy ra là người cài đặt mạng có thể cài đặt một mạng hoạt động tốt trong thời gian ngắn còn khi mạng hoạt động dài hạn này sẽ ù nảy sinh vấn đề về mặt chính sách là ai ủy quyền cho ai.

**Chương 12**

# Cài đặt, quản trị, sử dụng mạng Windows NT

## I. Cài đặt hệ điều hành mạng Windows NT server

Trước khi cài đặt mạng Windows NT thì cũng giống như cài các hệ điều hành khác chúng ta phải cắm card mạng vào máy, thiết lập mạng và đảm bảo nó được hoạt động tốt. Khi cài chúng ta có thể sử dụng phần mềm trên đĩa CD ROM (nếu máy của chúng ta là PC thì chúng ta sử dụng thư mục I386) hoặc chúng ta chép thư mục I386 lên đĩa cứng trước khi cài đặt. Để cài đặt Windows NT ta và trong thư mục I386 và chạy lệnh "WINNT"

Chú ý trong trường hợp này chương trình sẽ yêu cầu chuẩn bị 3 đĩa mềm loại 1.44Mb để cài các chương trình khởi động cần thiết và trong quá trình cài đặt các đĩa mềm trên sẽ được sử dụng. Nếu ta không muốn thì thực hiện lệnh "WINNT /B" và phải chỉ đường dẫn của chương trình nguồn như d:\I386.

**Yêu cầu về phần cứng cho việc cài đặt windows NT**

| Thiết bị phần cứng | Yêu cầu |
|---|---|
| Processor | Intel 486, Pentium, Pentium Pro, những hệ thống chạy trên RISC (Ex: MIPS R4x00, DEC?s Alpha AXP). Windows NT hỗ trợ lên đến 4 CPU ở Mode Symmetriccal Multi-Processing |
| Display device | VGA hay những thiêt bị có độ phân giải cao hơn |
| Hard disk | Tối thiểu phải có 110 MB Hard Disk còn trống trong suốt quá trình cài đặt |
| Floppy disk | 31/2 inch hay 51/4 inch |
| CD-ROM | CD-ROM drive hay đĩa CD-ROM mà ta có thể truy xuất được thông qua đường mạng |
| Network adapter | Một hay nhiều card mạng, card mạng không có cũng được nhưng chức năng mạng sẽ không có |
| Memory | NT khuyến cáo ít nhất phải có 16 MB Ram cho cả hai hệ thống chạy trên Intel và RISC |

**Chương 13 :**

# Quản lý và khai thác File, thư mục trong mạng Windows NT

Trong số các tài nguyên của mạng chia sẻ cho người sử dụng thông tin lưu trữ trên đĩa cứng của các máy chủ là tài nguyên quan trọng nhất. Không phải ngẫu nhiên mà cái tên "File server" trở nên rất quen thuộc với những người dùng mạng giống như "Network server". Tuy nhiên để làm sao có thể sử dụng, quản lý các tài nguyên đó một cách tốt nhất Windows NT cung cấp cho chúng ta một cơ chế quản lý và phương thức khai thác. Thông thường chúng ta phải khai báo các tài nguyên trước khi chúng được người sử dụng khai thác. Ngoài ra người sử dụng cũng được cung cấp quyền sử dụng một cách phù hợp.

## I. Cơ chế an toàn của File và thư mục trong Windows NT

***Quá trình truy cập tập tin (File hoặc thư mục)* trong Windows NT:** Khi một người sử dụng muốn truy cập một tập tin thì tất cả các thông tin về phương thức phục hồi giao dịch và phục hồi giao dịch khi bị lỗi sẽ được đăng ký bởi Log File Server. Nếu giao dịch thành công, tập tin đó sẽ truy xuất được, ngược lại giao dịch sẽđược phục hồi. Nếu có lỗi trong quá trình giao dịch, tiến trình giao dịch sẽ kết thúc.

Việc truy xuất tập tin (File hoặc thư mục) được quản lý thông qua các quyền truy cập (right), quyền đó sẽ quyết định ai có thể truy xuất và truy xuất đến tập tin đó với mức độ giới hạn nào. Những Quyền đó là Read, Execute, Delete, Write, Set Permission, Take Ownership.

**Trong đó:**

- **Read (R):** Được đọc dữ liệu, các thuộc tính, chủ quyền của tập tin.
- **Execute (X):** Được chạy tập tin.
- **Write (W):** Được phép ghi hay thay đổi thuộc tính.
- **Delete (D):** Được phép xóa tập tin.
- **Set Permission (P):** Được phép thay đổi quyền hạn của tập tin.
- **Take Ownership (O):** Được đặt quyền chủ sở hữu của tập tin.

**Bảng tóm tắt các mức cho phép**

| Permission | R | X | W | D | P | O |
|---|---|---|---|---|---|---|
| No Access | | | | | | |
| Read | X | X | | | | |
| Change | X | X | X | X | | |
| Full Control | X | X | X | X | X | X |
| Special Access | ? | ? | ? | ? | ? | ? |

Để đảm bảo an toàn khi truy xuất đến tập tin (File và thư mục)ä, chúng ta có thể gán nhiều mức truy cập (permission) khác nhau đến các tập tin thông qua các quyền được gán trên tập tin. Có 5 mức truy cập được định nghĩa trước liên quan đến việc truy xuất tập tin (File và thư mục) là: No Access, Read, Change, FullControl, Special Access. Special Access được tạo bởi người quản trị cho bất cứ việc chọn đặt sự kết hợp của R, X, W, D, P, O. Những người có quyền hạn Full Control, P, O thì họ có quyền thay đổi việc gán các quyền hạn cho Special Access.

- Khi một người quản trị mạng định dạng một partition trong Windows NT, hệ thống sẽ mặc định có cấp cho quyền Full Control tới partition đó cho nhóm Everyone. Điều này có nghĩa không hạn chế truy xuất của tất cả người dùng.

- Tùy thuộc trên yêu cầu bảo mật cho các tập người quản lý sẽ cân nhắc việc xóa bỏ nhóm Everyone trong danh sách các quyền hạn sau khi định dạng hay hạn chế nhóm Everyone với quyền Read. Nếu sự hạn chế này là cần thiết, người quản trị nên cấp quyền hạn Full Control cho nhóm Administrators tới partition gốc.

Ở đây quyền truy cập được gán cho người sử dụng và nhóm người sử dụng do vậy quyền truy cập của một người sử dụng được tính bởi quyền hạn người đó và các nhóm mà người đó là thành viên. Khi người dùng đó truy xuất tài nguyên, các quyền hạn của người dùng được tính theo lối sau:

- Những quyền hạn của ngươì dùng và các nhóm trùng nhau.

- Nếu một trong những quyền là No Access thì quyền hạn chung là No Access.

- Nếu những quyền hạn đã yêu cầu được liệt kê không rõ ràng trong danh sách các quyền hạn, yêu cầu truy xuất này là không chấp nhận.

Một người sử dụng thuộc hai nhóm, nếu một nhóm quyền hạn của người dùng là No Access, nó luôn được liệt kê đầu tiên trong danh sách Access Control List.

**Quyền sở hữu của các tập tin:** Người tạo ra tập tin đó có thể cho các nhóm khác hay người dùng khác khả năng làm quyền sở hữu. Administrator luôn có khả năng làm quyền sở hữu của các tập tin.

Nếu thành viên của nhóm Administrator có quyền sở hữu một tập tin thì nhóm những Aministrator trở thành chủ nhân. Nếu người dùng không phải là thành viên của nhóm Administrator có quyền sở hữu thì chỉ người dùng đó là chủ nhân.

Những chủ nhân của tập tin có quyền điều khiển của tập tin đó và có thể luôn luôn thay đổi các quyền hạn. Trong File Manager, dưới Security Menu, sau khi xuất hiện hộp thoại Owner, chúng ta lựa chọn tập tin, chủ nhân hiện thời và nhấn nút Take Ownership, cho phép lập quyền sở hữu nếu được cấp quyền đó.

**Để có quyền sở hữu một tập tin chúng ta cần một trong những điều kiện sau:**

- Có quyền Full Control.
- Có những quyền Special Access bao gồm Take Ownership.
- Là thành viên của nhóm Administrator.

**II. Các thuộc tính của File và thư mục**

- **Archive:** Thuộc tính này được gán bởi hệ điều hành chỉ định rằng một File đã được sửa đổi từ khi nó được Backup. Các phần mềm Backup thường xóa thuộc tính lưu trữ đó. Thuộc tính lưu trữ này có thể chỉ định các File đã được thay đổi khi thực thi việc Backup.
- **Compress:** Chỉ định rằng các File hay các thư mục đã được nén hay nên được nén. Thông số này chỉ được sử dụng trên các partition loại NTFS.
- **Hidden:** Các File và các thư mục có thuộc tính này thường không xuất hiện trong các danh sách thư mục.
- **Read Only:** Các File và các thư mục có thuộc tính này sẽ không thể bị xóa hay sửa đổi.
- **System:** Các File thường được cho thuộc tính này bởi hệ điều hành hay bởi chương trình OS setup. Thuộc tính này ít khi được sửa đổi bởi người quản trị mạng hay bởi các User.
- Ngoài ra các File hệ thống và các thư mục còn có cả hai thuộc tính chỉ đọc và ẩn.

**Lưu ý:** Việc gán thuộc tính nén cho các File hay thư mục mà ta muốn Windows NT nén sẽ xảy ra trong chế độ ngầm (background). Việc nén này làm giảm vùng không

gian đĩa mà File chiếm chỗ. Có một vài thao tác chịu việc xử lý chậm vì các File nén phải được giải nén trước khi sử dụng. Tuy nhiên việc nén File thường xảy ra thường xuyên như là các File dữ liệu quá lớn mà có nhiều người dùng chia sẻ.

### III. Chia sẻ Thư mục trên mạng

Không có một người sử dụng nào có thể truy xuất các File hay thư mục trên mạng bằng cách đăng nhập vào mạng khi không có một thư mục nào được chia se.

Việc chia sẻ này sẽ làm việc với bảng FAT và NTFS file system. Để nâng cao khả năng an toàn cho việc chia sẻ, chúng ta cần phải gán các mức truy cập cho File và Thư mục.

Khi chúng ta chia sẻ một thư mục, thì chúng ta sẽ chia sẻ tất cả các File và các Thư mục con. Nếu cần thiết phải hạn chế việc truy xuất tới một phần của cây thư mục, chúng ta phải sử dụng việc cấp các quyền cho một user hay một nhóm đối với các Thư mục và các File đó.

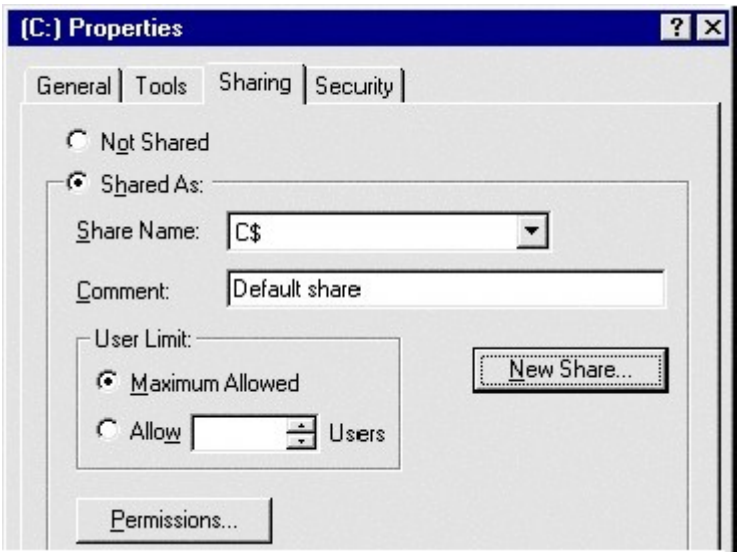
Để chia sẻ một Thư mục, ta phải Login như một thành viên của nhóm quản trị mạng hay nhóm điều hành server.

Tất cả các thủ tục chia sẻ thư mục được thực thi trong Windows NT Explorer.

**Để chia sẻ một thư mục ta phải thực hiện các bước sau:**

- **Right-click** lên Thư mục đó trong Windows NT Explorer. Hiện ra menu

- Click **Properties** trong Menu. Hiện ra hộp đối thoại sau:

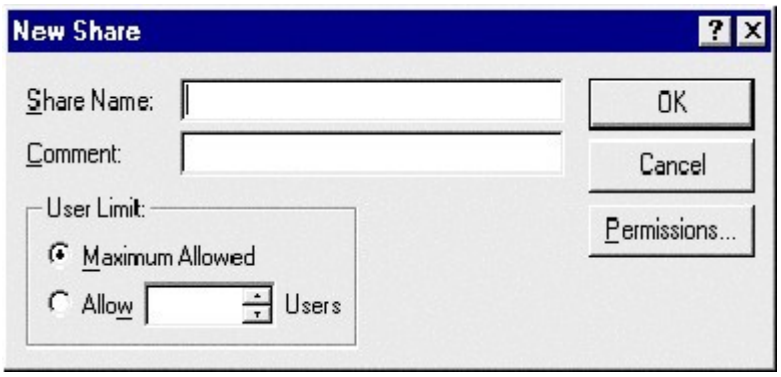



- Chọn **Sharing tab** hiện ra hộp đối thoại sau:
- Chọn **Shared As** để kích hoạt việc chia sẻ.
- Đưa một tên cần chia sẻ vào hộp **Share name**. Mặc nhiên tên Thư mục được chọn sẽ hiện ra. Đưa dòng ghi chú liên quan đến việc chia sẻ thư mục đó vào hộp **Comment**
- Thiết lập giới hạn số lượng các user bằng cách gỏ một con số vào hộp **Allow**
- Nếu muốn hạn chế việc truy xuất thì click **Permissions button.**
- **Click OK.**

Sau khi một thư mục được chia sẻ Icon cho thư mục đó có 1 bàn tay chỉ định rằng thư mục đó đã được chia sẻ.

Nếu chúng ta muốn thêm một chia sẻ mới với cùng một thư mục đã được chia sẻ (có thể với hai chia sẻ có hai quyền truy cập khác nhau), ta thực hiện các bước sau:

- **Right-click** vào thư mục đã được chia sẻ trong Windows NT Explorer.
- Click **Properties** trong **Menu** rút gọn, hiện ra hộp đối thoại **Properties**
- Click **Sharing tab.**
- Click button **New Share** để tạo một sự chia sẻ mới, hiện ra hộp đối thoại sau

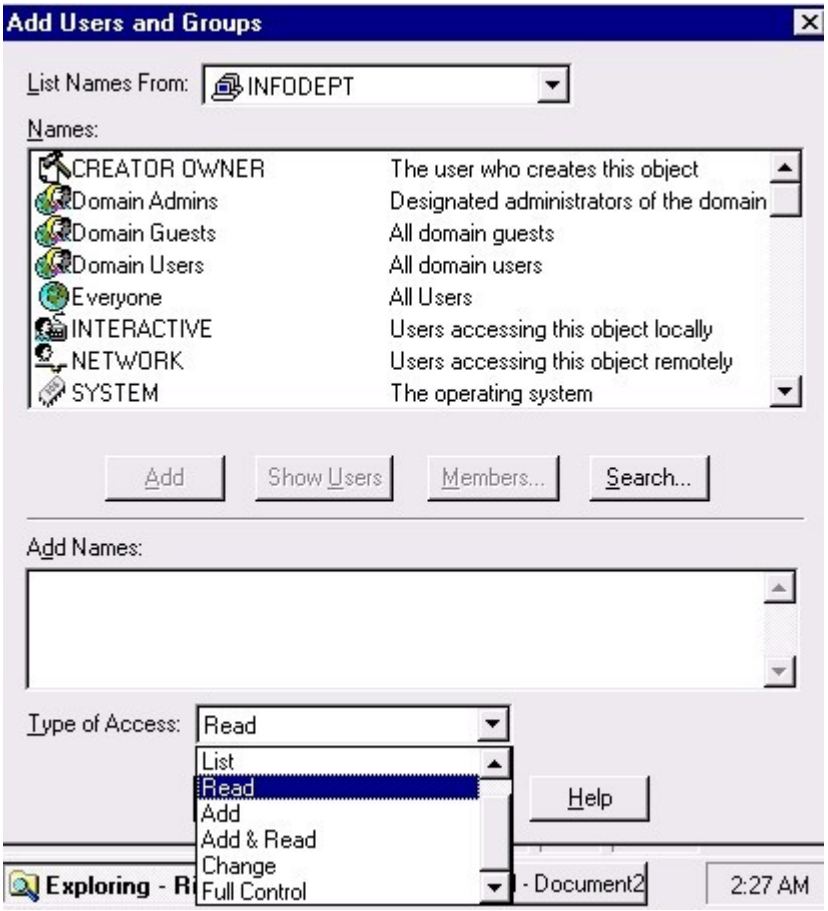



- Mỗi lần tạo một sự chia sẻ chúng ta phải đưa một tên mới cũng như những lời chú thích việc chia sẻ đó sẽ cho ai sử dụng.

## IV. Thiết lập quyền truy cập cho một người sử dụng hay một nhóm

Để thiết lập các quyền truy cập đối với một thư mục đã được chia sẻ cho một người sử dụng hay một nhóm ta thực hiện:

- **Right-click** lên thư mục đó trong Windows NT Explorer.
- Click **Properties** trong menu rút gọn**.**
- Chọn **Sharing** tab để hiện các tính chất của thư mục đó
- Click button **Permissions** trong **sharing tab** . Hiện ra Cửa sổ ***The Access Through Share Permissions.***
- Chọn button **Add**, hiện ra cửa sổ ***Add User and group.***




- Chọn một tên trong hộp ***Names*** và click button **Add.** Kết quả là tên đó được đưa vào hộp ***Add Names.***

- Chọn quyền truy xuất trong hộp ***Type of Access*** cho các tên đã chọn .

- Click button **OK.**

Khi chúng ta tạo một sự chia sẻ mới, quyền truy cập mặc nhiên cho nhóm **Everyone** là đầy đủ (**Full Control**). Giả sử rằng chúng ta sẽ gán giá trị mặc nhiên này cho quyền truy cập của thư mục và File. Khi cần thiết sẽ hạn chế việc truy xuất tới thư mục đó.

**Ở đây có một vài chú ý:**

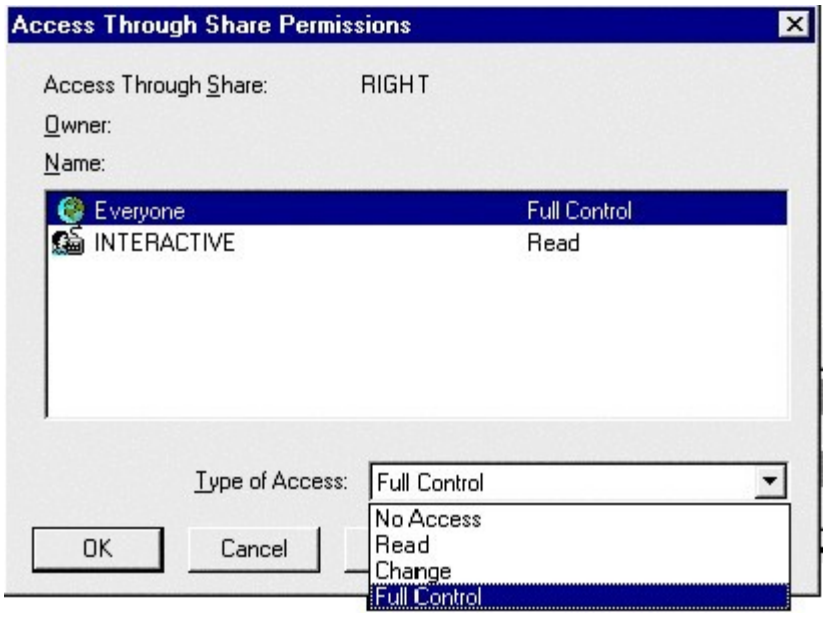
- Các người sử dụng thường chỉ cóù quyền đọc trong các thư mục chứa các chương trình ứng dụng vì họ không cần phải sửa đổi các File.

- Trong một vài trường hợp, các chương trình ứng dụng đòi hỏi các user chia sẻ một thư mục cho các File tạm thời. Nếu thư mục đó nằm trong cùng thư mục chứa trình ứng dụng, chúng ta có thể cho phép user tạo hay xóa các File trong thư mục đó bằng việc gán quyền **Change**.

- Thông thường các người sử dụng cần quyền **Change** trong bất kỳ thư mục nào chứa các Files dữ liệu và chỉ trong các thư mục cá nhân của ho là có đầy đủ các quyền truy cậpï.

**Để sửa đổi các quyền truy cập đối với một thư mục đã được chia sẻ ta thực hiện:**

- **Right-click** lên thư mục được chia sẻ trong Windows NT Explorer.
- Click **Properties**
- Click **Sharing** tab.
- Click button **Permissions** hiện ra cửa sổ ***Access Through Share Permissions*** sau:




- Chọn 1 tên trong hộp ***Name***
- Chọn một quyền khác trong hộp ***Type of Access*** mà ta muốn gán.
- Click **OK**.

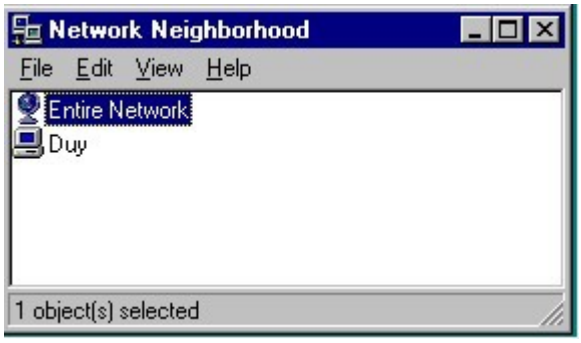
Thông qua việc chia sẻ một thư mục cho một user hay một nhóm cũng góp phần vào việc bảo đảm an toàn cho một thư mục không cho user khác hay nhóm khác truy xuất thư mục đó.

**V. Sử dụng các thư mục mạng**

Muốn sử dụng các thư mục mạng thì trước hết thư mục đó được cho phép chia sẻ, chúng ta phải liên kết thư mục mạng đó với tên một chữ cái tương ứng như một tên đĩa mạng (E,F ,G ,H I,...). Sau khi thư mục được chia sẻ đã kết nối với ký tự ổ đĩa mạng người dùng có thể truy cập thư mục được chia sẻ, các thư mục và file con của nó như là nó đang ở trên máy tính của mình .

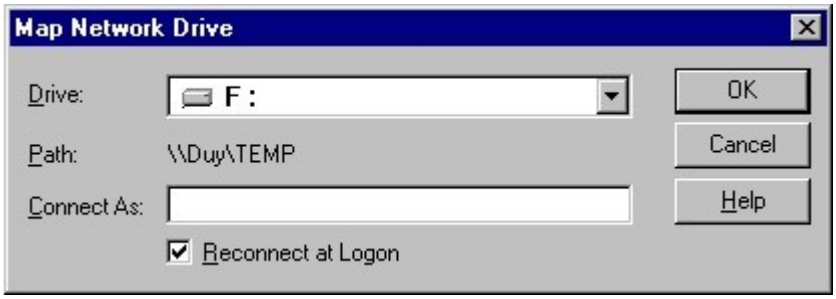
**Có thể dùng Network Neighborhood để thực hiện công việc trên như sau :**

- Click đúp trên **Network Neighborhood** để mở trình duyệt mạng.




- Duyệt qua **Network Neighborhood** để tìm nơi muốn liên kết.

- Click phải vào thư mục đã được chia sẻ mà chúng ta muốn truy cập và chọn **Map Network Drive** trong thực đơn **Options** ta thấy hộp **Map Network Drive** hiện ra




- Trong trường **Drive** của hộp thoại **Map Network Drive**, chọn ổ đĩa mạng chúng muốn liên kết với thư mục chia sẻ.

- Nếu thấy cần, chọn Path và gõ vào tên theo tổng quát UNC (Universal Naming Convention - xem cấu trúc ở phần dưới) để sửa lại đường dẫn tới tài nguyên được chia sẻ. (Việc này chỉ thực hiện khi sử dụng Network Neighborhood.)

- Nếu chúng ta không được quyền để truy cập vào tài nguyên chia sẻ trên nhưng trong cương vị người dùng khác thì chúng ta được quyền truy cập, trong trường hợp đó hãy gõ tên người dùng đó vào trường **Connect As**.

- Kích hoạt hộp kiểm tra **Reconnect at Logon** nếu muốn liên kết lâu dài, đó là loại kết nối được phục hồi mỗi lần chú ta đăng nhập vào mạng.

- Chọn **OK** để lưu các thông tin trên.

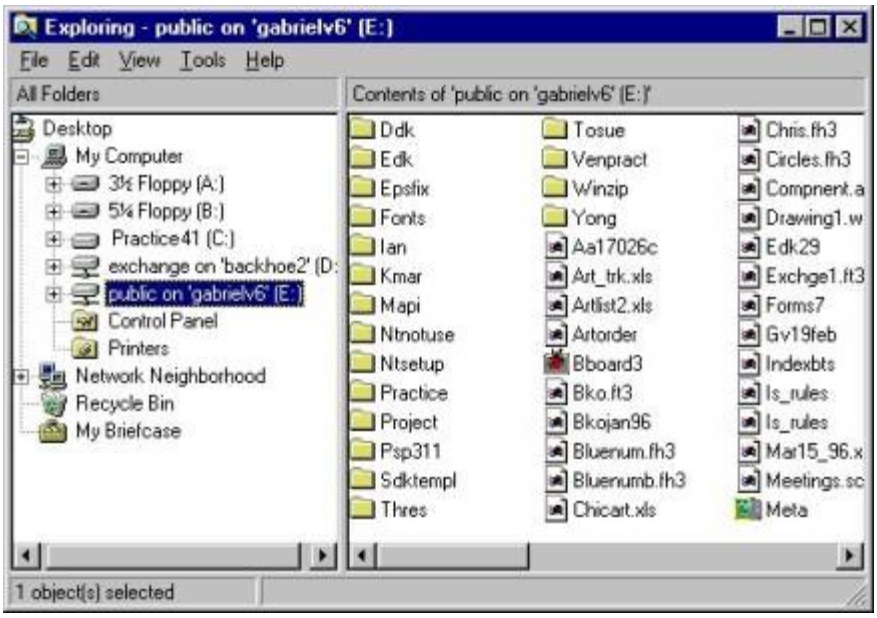
Ngoài ra ta có thể dùng lệnh **NET USE** để thực hiện các công việc trên.

Lệnh NET USE dùng Universal Naming Convention (UNC) để truy cập các tài nguyên dùng chung. Tên UNC bắt đầu bằng một dấu phân cách đặt biệt \\, dấu này chỉ sự bắt đầu của tên UNC (tên UNC có dạng "\\computer_name\share_name[\sub_directory]". NET USE đượcc dùng đểû truy cập một nguồn tài nguyên dùng chung. Lệnh NET USE dùng bộ hướng dẫn mạng (Network Redirector) trên máy tính NT để thiết lập sự nối kết dùng nguồn tài nguyên chung.

Chúng ta có thể xem ai dùng các file dùng chung khi ta đang xem trạng thái của một file dùng chung, File Manager sẽ cung cấp cho ta các thông tin bằng dùng chọn Properties trong thực đơn File

| Đề mục | Nội dung |
|---|---|
| Total Opens | Tổng số các user đang làm việc với file đó |
| Total Locks | Tổng số các khóa trên file |
| Open By | Tên của người dùng đã mở file |
| For | Loại truy xuất mà người dùng đã mở file |
| Locks | Một số khóa mà người dùng đặt trên file |
| File ID | Con số nhận diện của file |

Khi chúng ta dùng Windows Explorer để xem các tài nguyên chúng ta có thì các ổ đĩa mạng xuất hiện và cho chúng ta khai thác.


Exploring - public on 'gabrielv6' (E:)
File Edit View Tools Help
All Folders
Contents of 'public on 'gabrielv6' (E:)'
Desktop
My Computer
3½ Floppy (A:)
5¼ Floppy (B:)
Practice41 (C:)
exchange on 'backhoe2' (D:
public on 'gabrielv6' (E:)
Control Panel
Printers
Network Neighborhood
Recycle Bin
My Briefcase
Ddk
Edk
Epsfix
Fonts
Ian
Kmar
Mapi
Ntnotuse
Ntsetup
Practice
Project
Psp311
Sdktempl
Thres
Tosue
Venpract
Winzip
Yong
Aa17026c
Art_trk.xls
Artlist2.xls
Artorder
Bboard3
Bko.ft3
Bkojan96
Bluenum.fh3
Bluenumb.fh3
Chicart.xls
Chris.fh3
Circles.fh3
Compnent.a
Drawing1.w
Edk29
Exchge1.ft3
Forms7
Gv19feb
Indexbts
Is_rules
Is_rules
Mar15_96.x
Meetings.sc
Meta
1 object(s) selected

**Chương 14 :**

# Sử dụng máy in trong mạng Windows NT

Hiện nay máy in trên mạng cũng là một tài nguyên việc chia sẻ của mạng cho người sử dụng. Tuy các máy in đang ngày càng rẻ đi nhưng với nhu cầu về chất lượng đang ngày một cao thì việc chia sẻ các máy in đắt tiền trên mạng vẫn đang cần thiết. Windows NT là một hệ điều hành mạng mà bất kỳ máy tính Windows NT nào cũng có thể cung cấp các dịch vụ in ấn cho người sử dụng trong mạng.

Khi chia sẻ một máy in trên mạng (cho nhiều người có thể cùng sử dụng) chúng ta cần phải giải quyết những vấn đề sau :

- Máy in không làm được 2 việc một lúc, nếu phải nhận cùng một lúc thì sẽ có va chạm, do vậy mạng phải có cơ chế sắp xếp công việc sao cho máy in có thể thực hiện một cách lần lượt các công việc in.

- Các công việc in được thực hiện bởi những người sử dụng khác nhau có thể cần những mức độ ưu tiên khác nhau và hệ thống quan lý in cần có khả năng thực hiện điều này.

## I. Cơ chế in trong mạng Windows NT

Thông thường máy in mạng được quản lý thông qua một máy chủ mà trên đó thực hiện nhiệm vụ quản lý các công việc in, máy chủ đó thường được gọi là máy chủ in (Print server) và chạy chương trình quản lý in. Windows NT cho phép cài đặt máy in tại bất cứ đâu trên mạng, mỗi một máy có cài đặt Windows NT đều có thể thực hiện nhiệm vụ máy chủ in. Nó có thể quản lý máy in gắn trực tiếp vào nó hay một máy in gắn vào máy khác trên mạng.

Để giải quyết những vấn đề đặt ra với công việc in trên mạng Windows NT sử dụng kỹ thuật gọi là Spooling mà chủ yếu như sau:

- Khi người sử dụng quyết định thực hiện một công việc in thì công việc in đó không trực tiếp gửi ra máy in mà nó được đặt trong một file tại máy chủ in. Ở đây việc thực hiện giống như hàng đợi rạp hát, nó là một vùng lưu trữ các công việc in và có nhiệm vụ ngăn chặn xung đột khi các user chi xuất đồng thời ra máy in.

- Máy chủ in duy trì các hàng đợi để cất giữ các công việc in và đưa chúng tới máy in ngay khi có thể. Trong khi đó người sử dụng có thể làm tiếp công việc ngay khi công việc in được cất vào hàng đợi.

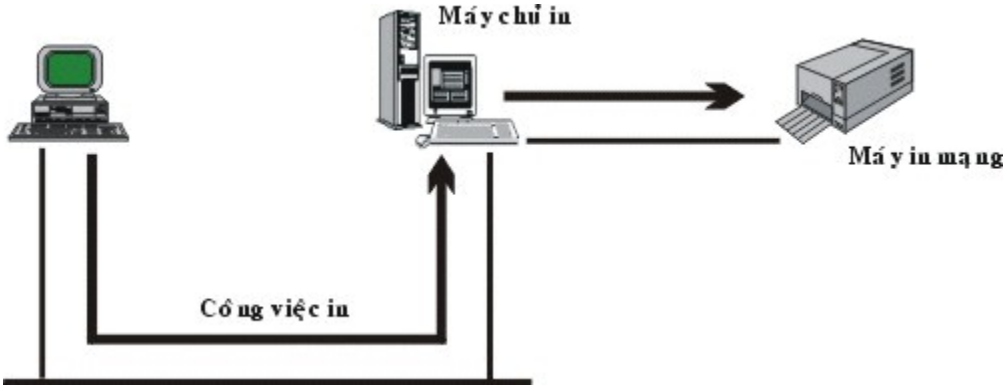
- Khi máy in rảnh máy chủ in sẽ chuyển lần lượt các công việc in đang đứng đợi trong hàng tới máy in. Tại đây máy chủ in phải có một khả năng lưu trữ dữ

liệu lớn để có thể lưu trữ nhiều công việc in một lúc và cần phải có khả năng đáp ứng những yêu cầu đa dạng của các công việc in.

Để giải quyết vấn đề nẩy sinh với máy in trong mạng Windows NT tiến hành phân biệt giữa máy in vật lý gọi là Printing device và một thực thể logic của máy in gọi là logic printer. Máy in logic được sử dụng để kiểm soát các tác vụ sau đây :

- Công việc in được gởi đi đâu.
- Công việc in ấn gởi đi khi nào.
- Thứ tự ưu tiên của các tác vụ in.

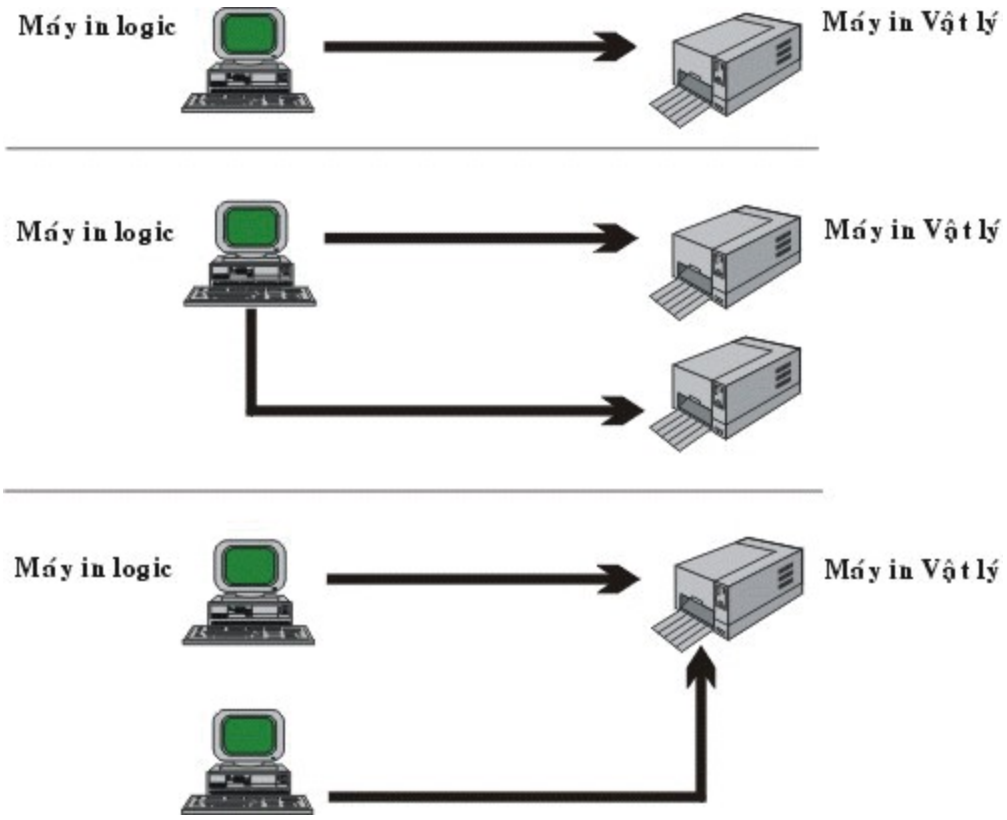
Người sử dụng in ra spool thông qua việc in ra máy in logic, họ sử dụng máy in logic như là máy in đang được gắn là máy của họ nhưng thực sự các dữ liệu được in ra máy in logic được chuyển cho mạng và qua đó đến máy chủ in trước khi được đưa ra máy in mạng.




*Hình 14.1: Máy chủ in và spool*

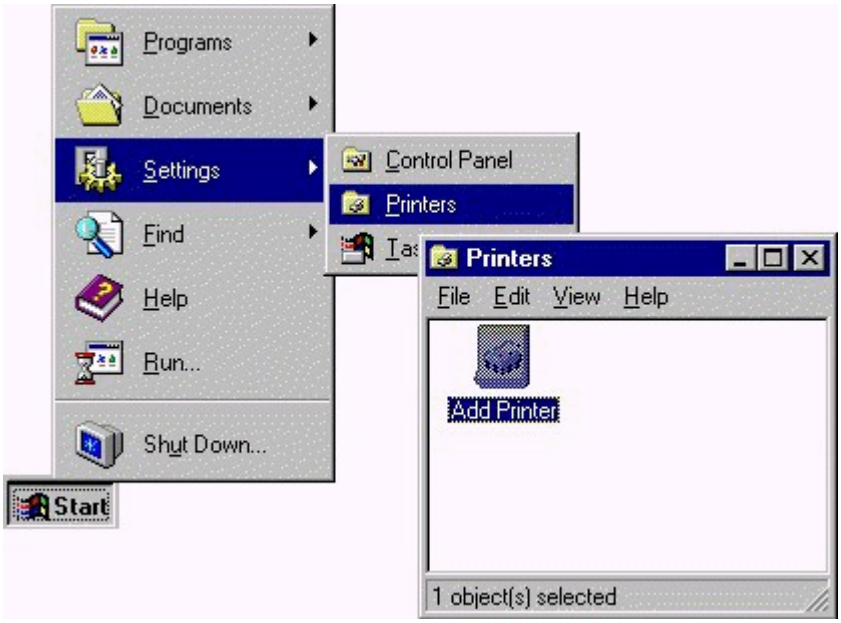
Máy chủ in sẽ liên kết các máy in logic với máy in vật lý, nó phải đảm bảo các công việc in phải được đưa đúng đến máy in vật lý. Tại đây có 3 trường hợp có thể đối với mối quan hệ giữa máy in logic và máy in vật lý

- Một máy in logic liên kết với một máy in vật lý.
- Nhiều máy in logic liên kết với một máy in vật lý.
- Một máy in logic liên kết với nhiều máy in vật lý.

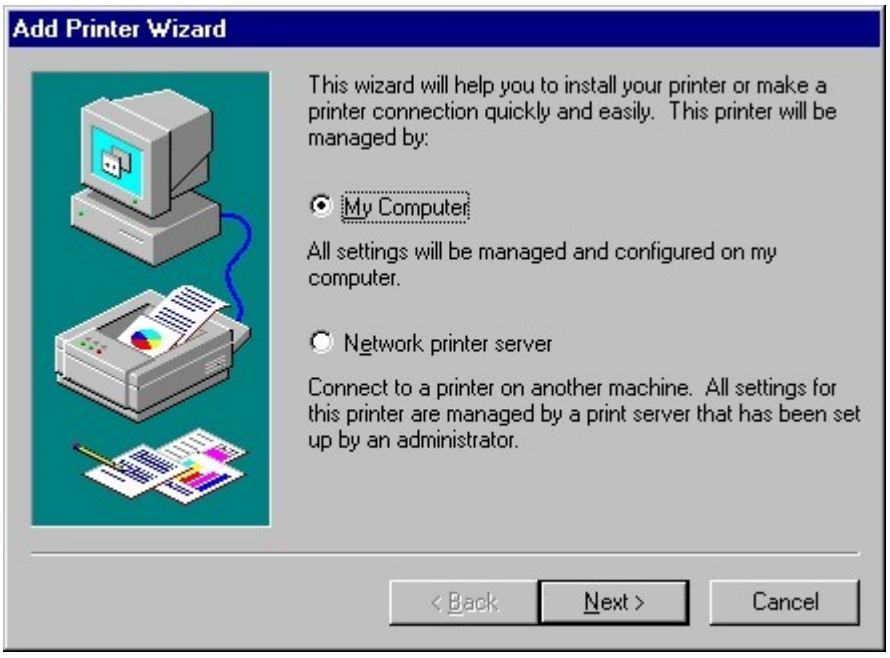



*Hình 14.2: Liên kết giữa máy in Logic và máy in vật lý*

Nếu Server chưa cài đặt máy in logic, ta phải cài đặt máy in logic tương ứng với một máy in thực tế cho Server. Vào menu **Start**, chọn **Settings**, chọn **Printers**, chọn **Add Printer** như:



Hộp sau đó hộp hội thoại **Add printer** winzar hiện ra

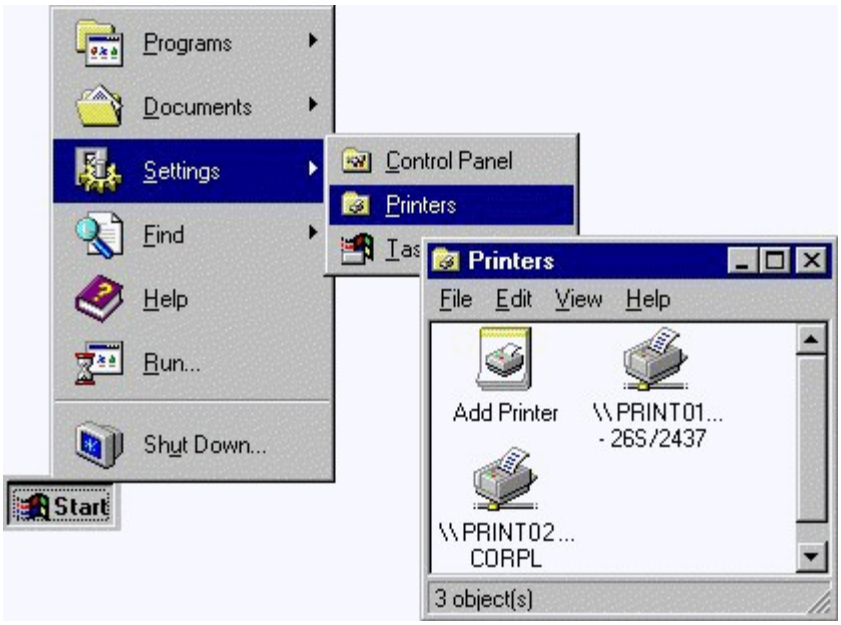



- Chọn My Computer nếu máy in của chúng ta không có card mạng và được nối trực tiếp vào Server.

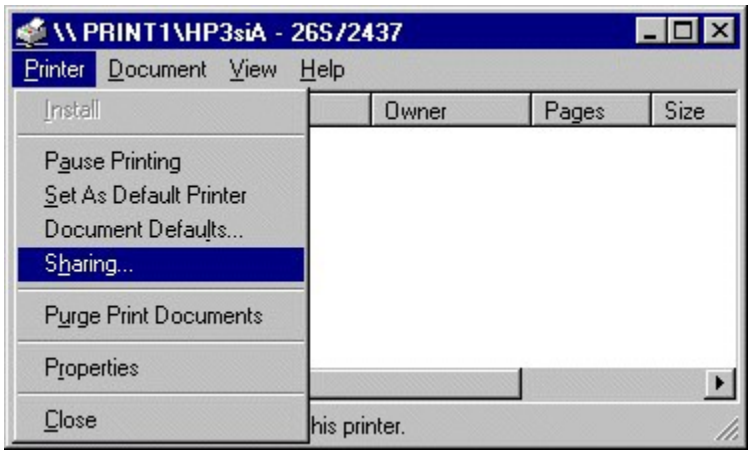
- Chọn Network printer server nếu máy in của chúng ta nối trực tiếp vào mạng.

- Chọn Next, chọn cổng nối với máy in (thường là LPT1). Chọn tên hãng sản xuất và loại máy in ta đang dùng, chọn Next, ta phải trả lời thêm vài câu hỏi phụ như ta có muốn in trang test không? Có muốn đặt máy in này là ngầm định không?

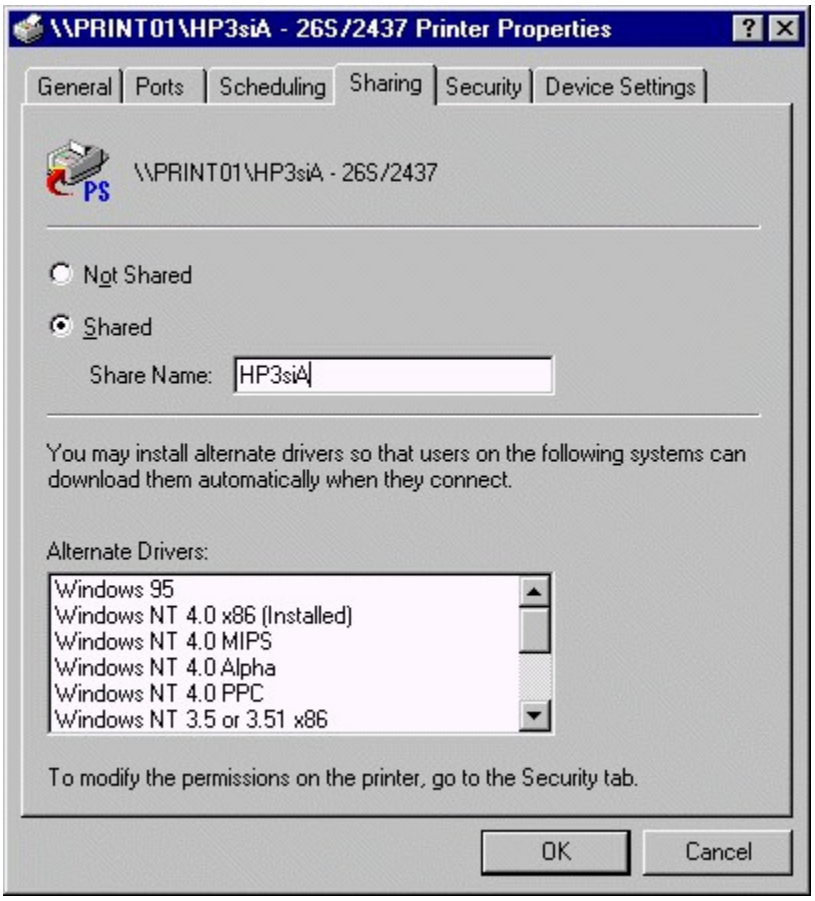
Sau khi cài đặt, chúng ta sẽ thấy xuất hiện thêm biểu tượng máy in mà vừa được cài đặt trong khung máy in. Chúng ta phải cho phép dùng chung máy in nàybằng cách lựa chọn máy in đó Trong khung Printers




- Ta nhắp chuột phải vào tên máy in đó, chọn **Sharing** như hình sau:




Khung **Printer properties** hiện ra cho chúng ta nhập các thông số như: tên máy in logic (Share namem), các tính chất khác như về an toàn. mà chúng ta muốn khi phục vụ mạng.




- Cuối cùng chọn **OK**, lúc này, ta sẽ thấy ở dưới biểu tượng máy in có bàn tay đỡ chứng tỏ máy in này đã được phép dùng chung. Nếu trên Server cài đặt nhiều loại máy in với nhiều chế độ khác nhau, ta có thể chọn máy in ngầm định bằng cách đánh dấu vào mục **Set As Default**.

- Để máy trạm có thể in được qua Server, nếu chưa cài đặt chúng ta phải cài máy in như sau: nhắp đúp vào tên Server có nối với máy in, khung **Shared Printers** sẽ hiện ra danh sách các máy in đã cài trên Server, chúng ta chọn tên máy in cần nối rồi bấm **OK**.

Quay trở lại khung màn hình **Print Manager** chúng ta nhìn thấy thông báo máy in này đã được phép sử dụng. Thoát ra khỏi **Print Manager** và chúng ta có thể in qua máy in mạng trên bất cứ một phần mềm nào trên Windows như Winword, Excel, v.v...

Bất kỳ máy tính Windows NT có thể được cấu hình như là một **print server**. Tuy nhiên chỉ có những người là thành viên của những nhóm sau đây mới có quyền tạo ra các máy in:

- Administrator (NT Worstation and Server).

- Server Operator (NT Server).

- Print Operator (NT Server).
- Power Users (NT Worstation).

## II. Bảo mật của máy in

### Windows NT có các mức độ bảo mật trong in ấn như sau:

- **Quyền sở hửu máy in (Ownership) :** người sử dụng tạo ra một máy in chính là người chủ sở hửu máy in đó và có toàn quyền trên tất cả các thuộc tính của máy in logic. Người chủ sở hửu máy in có thể gán quyền cho những người dùng khác quản lý tài liệu hay toàn quyền điều khiển việc in ấn. Một người sử dụng có toàn quyền thì họ toàn quyền sở hửu máy in logic đó.

- **Quản lý thuộc tính máy in (Permissions):** quyền quản lý máy in bao gồm 4 quyền sau:

  - **No access:** không được phép truy cập.
  - **Print:** in
  - **Manage document:** quản lý văn bản, có khả năng thực hiện các thao tác: Điều khiển khởi đặt tài liệu, Ngừng, phục hồi, khởi động lại,và xóa các tài liệu.
  - **Full control:** toàn quyền điều khiển, thực hiện các quyền quản lý tài liệu và các quyền sau đây:
    - Thay đổi trật tự in ấn tài liệu.
    - Ngừng, tổng hợp lại,che dấu các máy in logic.
    - Thay đổi thuộc tính của máy in logic.
    - Hủy các máy in logic.
    - Thay đổi quyền của máy in logic

Có thể xem tài liệu ở máy in logic và quản lý chúng theo nhiều cách. Người sử dụng luôn quản lý được tất cả các tài liệu mà họ tạo ra. Để quản lý được các tài liệu của các người sử dụng khác, phải là người chủ sở hửu của máy in logic hay là thành viên của các nhóm:

- Administrator.
- Server Operator

- Print operator.

Bất kỳ một máy in nào cũng có thể làm việc trong môi trường mạng nhưng điều quan trọng là xem xét **chu kỳ làm việc (duty cycle)** của máy in. Nghĩa là phải xem xét số lượng trang in tối đa mà máy in có thể in ra trong một khoảng thời gian nhất định.

Các máy in được thiết kế cho mạng thường có **chu kỳ làm việc (duty cycle)** cao. Các máy in có thể gắn vào bất cứ nơi đâu trên mạng. Công việc in không phù thuộc vào các thiết bị phần cứng hay các thiết bị kết nối mà do được quản lý bởi một **print server** và dữ liệu được chuyển vận trên mạng.

**Chương 15 :**

# Các dịch vụ mạng của Windows NT Server

Cũng như các hệ điều hành khác Windows NT cũng có những ưu, khuyết điểm của nó, tuy nhiên Windows NT hiện nay chinh phục được nhiều người dùng với những ưu điểm không thể chối cãi. Là hệ điều hành mạng cho phép tổ chức quản lý một cách chủ động theo nhiều mô hình khác nhau: peer-to-peer, clien/server. Nó thích hợp với tất cả các kiến trúc mạng hiện nay như: hình sao (start), đường thẳng (bus), vòng (ring) và phức hợp. Nó có một số đặc tính ưu việt bảo đảm thực hiện cùng lúc nhiều chương trình mà không bị lỗi. Bản thân Windows NT đáp ứng được hầu hết các giao thức phổ biến nhất trên mạng và cũng hỗ trợ được rất nhiều những dịch vụ truyền thông trên mạng. Nó vừa đáp ứng được cho mạng cục bộ (LAN) và cho cả mạng diện rộng (WAN).

Windows NT cho phép dùng giao thức Windows NT TCP/IP, vốn là một giao thức được sử dụng rất phổ biến trên hầu hết các mạng diện rộng và trên Internet. Giao thức TCP/IP dùng tốt cho nhiều dịch vụ mạng trên môi trường Windows NT.

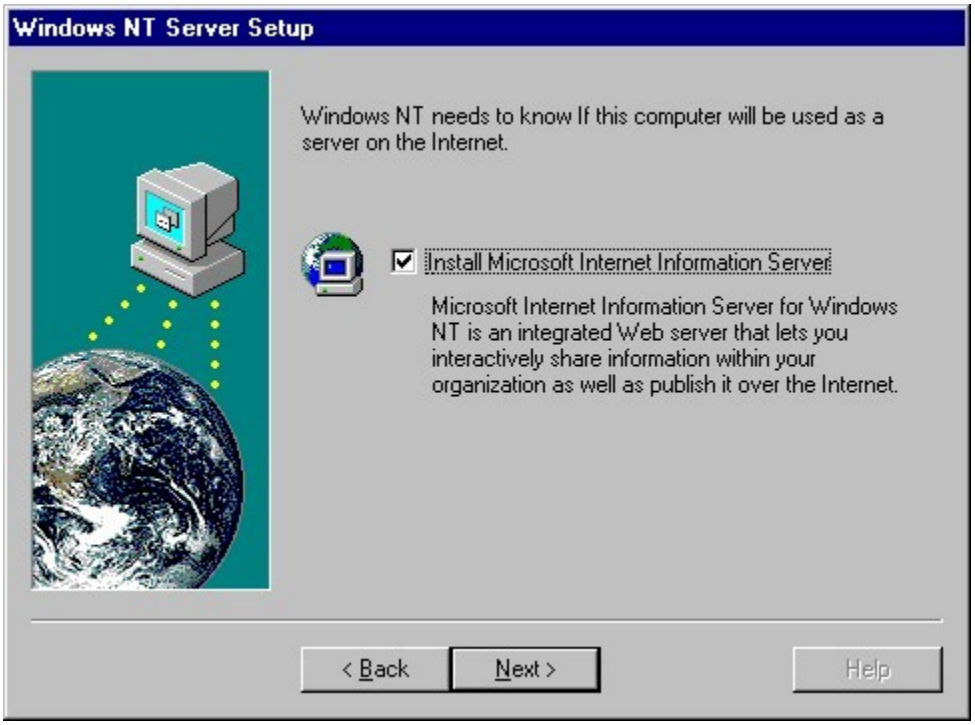
## I. Internet Information Server (IIS)

Internet Information Server là một ứng dụng chạy trên Windows NT, tích hợp chặt với Windows NT, khi cài đặt IIS, IIS có đưa thêm vào tiện ích màn hình kiểm soát (Performance monitor) một số mục như thống kê số lượng truy cập, số trang truy cập. Việc kiểm tra người dùng truy cập cũng dựa trên cơ chế quản lý người sử dụng của Windows NT. Sau khi cài đặt IIS, trong thư mục InetSrv sẽ có các thư mục gốc tương ứng cho từng dịch vụ chọn cài đặt.

IIS bao gồm 3 dịch vụ: World Wide Web (WWW), chuyển file (FTP - File Transfer Protocol) và Gopher. Cả 3 dịch vụ này đều sử dụng kết nối theo giao thức TCP/IP.

### 1. Cài đặt dịch vụ Internet Information Server

Khi cài đặt hệ điều hành Windows NT đến phần mạng Windows NT sẽ hỏi chúng ta xem có cài đặt dịch vụ Internet Information Server hay không với hộp hội thoại




*Hình 15.1: Màn hình cài đặt của IIS*

Để thực hiện việc cài đặt chúng ta Click vào phím Next và Hệ thống sẽ bắt đầu cài đặt các dịch vụ Internet Information Server.

## 2. Các dịch vụ trong IIS

### *a. WWW (World Wide Web) :*

Là một trong những dịch vụ chính trên Internet cho phép người sử dụng xem thông tin một cách dễ dàng, sinh động. Dữ liệu chuyển giữa Web Server và Web Client thông qua nghi thức HTTP (Hypertext Transfer Protocol).

Người quản trị có thể xem các thông tin như các người dùng đã truy cập, các trang được truy cập, các yêu cầu được chấp nhận, các yêu cầu bị từ chối. thông qua các file có thể được lưu dưới dạng cơ sở dữ liệu.

### *b. FTP (File Transfer Protocol)*

Sử dụng giao thức TCP để chuyển file giữa 2 máy và cũng hoạt động theo mô hình Client/Server, khi nhận được yêu cầu từ client, đầu tiên FTP Server sẽ kiểm tra tính hợp lệ của người dùng thông qua tên và mật mã. Nếu hợp lệ, FTP Server sẽ kiểm tra quyền người dùng trên tập tin hay thư mục được xác định trên FTP Server. Nếu hợp lệ và hệ thống file là NTFS thì sẽ có thêm kiểm tra ở mức thư mục, tập tin theo NTFS. Sau khi tất cả hợp lệ, người dùng sẽ được quyền tương ứng trên tập tin, thư mục đó.

**Để sử dụng FTP có nhiều cách:**

- Sử dụng Web Browser.
- Sử dụng Command line.
- Sử dụng từ <Run> command trong Windows.

***c. Gopher***

Là một dịch vụ sử dụng giao diện menu để Gopher Client tìm và chuyển bất kỳ thông tin nào mà Gopher Server đã được cấu hình. Gopher cũng sử dụng kết nối theo giao thức TCP/IP.

**II. Dynamic Host Configuration Protocol (DHCP) :**

Trong một mạng máy tính, việc cấp các địa chỉ IP tĩnh cố định cho các host sẽ dẫn đến tình trạng lãng phí địa chỉ IP, vì trong cùng một lúc không phải các host hoạt động đồng thời với nhau, do vậy sẽ có một số địa chỉ IP bị thừa. Để khắc phục tình trạng đó, dịch vụ DHCP đưa ra để cấp phát các địa chỉ IP động trong mạng.

Trong mạng máy tính NT khi một máy phát ra yêu cầu về các thông tin của TCPIP thì gọi là DHCP client, còn các máy cung cấp thông tin của TCPIP gọi là DHCP server. Các máy DHCP server bắt buộc phải là Windows NT server.

Cách cấp phát địa chỉ IP trong DHCP: Một user khi log on vào mạng, nó cần xin cấp 1 địa chỉ IP, theo 4 bước sau :

- Gởi thông báo đến tất cả các DHCP server để yêu cầu được cấp địa chỉ.
- Tất cả các DHCP server gởi trả lời địa chỉ sẽ cấp đến cho user đó.
- User chọn 1 địa chỉ trong số các địa chỉ, gởi thông báo đến server có địa chỉ được chọn.
- Server được chọn gởi thông báo khẳng định đến user mà nó cấp địa chỉ.

**Quản trị các địa chỉ IP của DHCP server:** Server quản trị địa chỉ thông qua thời gian thuê bao địa chỉ (lease duration). Có ba phương pháp gán địa chỉ IP cho các Worstation :

- Gán thủ công.
- Gán tự động.
- Gán động .

Trong phương pháp gán địa chỉ IP thủ công thì địa chỉ IP của DHCP client được gán thủ công bởi người quản lý mạng tại DHCP server và DHCP được sử dụng để chuyển tới DHCP client giá trị địa chỉ IP mà được định bởi người quản trị mạng

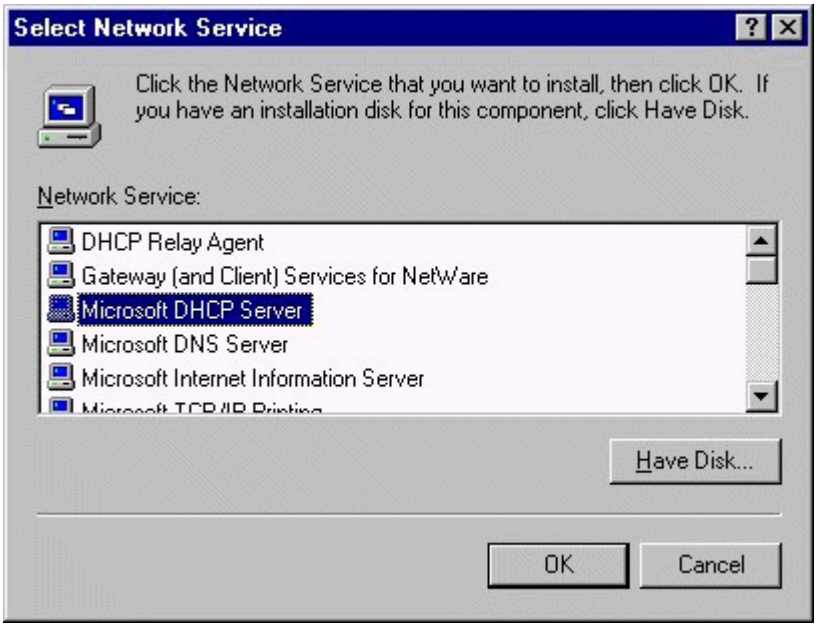
Trong phương pháp gán địa chỉ IP tự động DHCP client được gán địa chỉ IP khi lần đầu tiên nó nối vào mạng. Địa chỉ IP được gán bằng phương pháp này sẽ được gán vĩnh viễn cho DHCP client và địa chỉ này sẽ không bao giờ được sử dụng bởi một DHCP client khác

Trong phương pháp gán địa chỉ IP động thì DHCP server gán địa chỉ IP cho DHCP client tạm thời. Sau đó địa chỉ IP này sẽ được DHCP client sử dụng trong một thời gian đặc biệt. Đến khi thời gian này hết hạn thì địa chỉ IP này sẽ bị xóa mất. Sau đó nếu DHCP client cần nối kết vào mạng thì nó sẽ được cấp một địa chủ IP khác

Phương pháp gán địa chỉ IP động này đặc biệt hữu hiệu đối với những DHCP client chỉ cần địa chỉ IP tạm thời để kết nối vào mạng. Ví dụ một tình huống trên mạng có 300 users và sử dụng subnet là lớp C. Điều này cho phép trên mạng có 253 nodes trên mạng. Bởi vì mỗi computer nối kết vào mạng sử dụng TCP/IP cần có một địa chỉ IP duy nhất do đó tất cả 300 computer không thể đồng thời nối kết vào mạng. Vì vậy nếu ta sử dụng phương pháp này ta có thể sử dụng lại những IP mà đã được giải phóng từ các DHCP client khác.

Cài đặt DHCP chỉ có thể cài trên Windows NT server mà không thể cài trên Client. Các bước thực hiện như sau:

- Login vào Server với tên Administrator .
- Click hai lần vào icon **Network** . Ta sẽ thấy hộp hội thoại **Network dialog box**



*Hình 15.2: Màn hình cài đặt của DHCP*

- Chọn tab **service** và click vào nút **Add** .

- Ta sẽ thấy một loạt các service của Windows NT server nằm trong hộp hội thoại **Select Network Service**. Chọn **Microsoft DHCP server** từ danh sách các service được liệt kê ở phía dưới và nhấn **OK** và thực hiện các yêu cầu tiếp theo của Windows NT.

Để cập nhật và khai thác DHCP server chúng ta chọn mục DHCP manager trong Netwrok Administrator Tools.

### III. Dịch vụ Domain Name Service (DNS)

Hiện nay trong mạng Internet số lượng các nút (host) lên tới hàng triệu nên chúng ta không thể nhớ hết địa chỉ IP được, Mỗi host ngoài địa chỉ IP còn có một cái tên phân biệt, DNS là 1 cơ sở dữ liệu phân tán cung cấp ánh xạ từ tên host đếùn địa chỉ IP. Khi đưa ra 1 tên host, DNS server sẽ trả về địa chỉ IP hay 1 số thông tin của host đó. Điều này cho phép người quản lý mạng dễ dàng trong việc chọn tên cho host của mình

**DNS server được dùng trong các trường hợp sau :**

- Chúng ta muốn có 1 tên domain riêng trên Interner để có thể tạo, tách rời các domain con bên trong nó.

- Chúng ta cần 1 dịch vụ DNS để điều khiển cục bộ nhằm tăng tính linh hoạt cho domain cục bộ của bạn.

- Chúng ta cần một bức tường lửa để bảo vệ không cho người ngoài thâm nhập vào hệ thống mạng nội bộ của mình

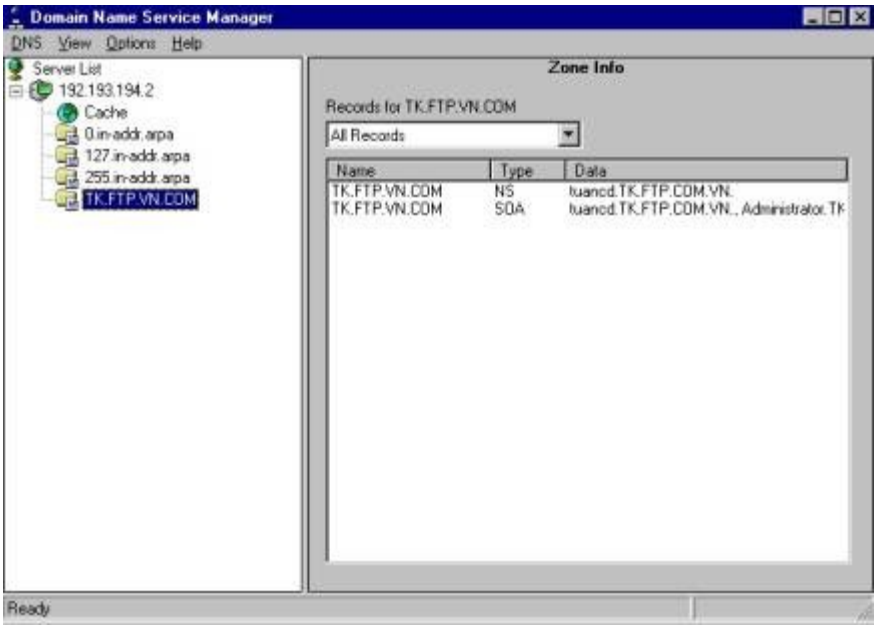
Có thể quản lý trực tiếp bằng các trình soạn thảo text để tạo và sửa đổi các file hoặc dùng DNS manager để tạo và quản lý các đối tượng của DNS như: Servers, Zone, Các mẫu tin, các Domains, Tích hợp với Win, .

Cài đặt DNS chỉ có thể cài trên Windows NT server mà không thể cài trên Client. Các bước thực hiện như sau:

- Login vào Server với tên **Administrator**.

- Click hai lần vào icon **Network**. Ta sẽ thấy hộp hội thoại **Network dialog box** tương tụ như trên và lựa chọn **Microsoft DNS Server**.

Để cập nhật và khai thác DNS server chúng ta chọn mục **DNS manager trong Netwrok Administrator Tools**. Hộp hội thoại sau đây sẽ hiện ra




*Hình 15.3: Màn hình DNS Manager*

Mỗi một tập hợp thông tin chứa trong **DNS database** được coi như là **Resourse record**. Những **Resourse record** cần thiết sẽ được liệt kê dưới đây:

| Tên Record | Mô tả |
|---|---|
| A (Address) | Dẫn đường một tên host computer hay tên của một thiết bị mạng khác trên mạng tới một địa chỉ IP trong DNS zone |
| CNAME () | Tạo một tên Alias cho tên một host computer trên mạng |
| MX () | Định nghĩa một sự trao đổi mail cho host computer đó |
| NS (name server) | Định nghĩa tên server DNS cho DNS domain |
| PTR (Pointer) | Dẫn đường một địa chỉ IP đến tên host trong DNS server zone |
| SOA (Start of authority) | Hiển thị rằng tên server DNS này thì chứa những thông tin tốt nhất |

## IV. Remote Access Service (RAS)

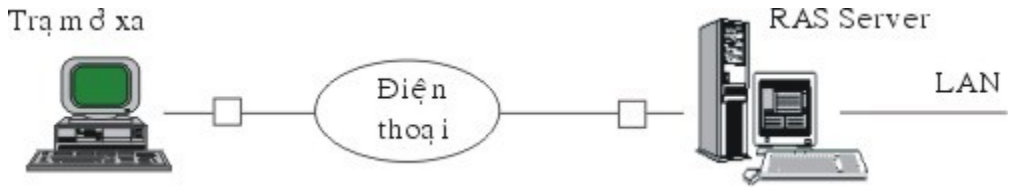
Ngoài những liên kết tại chỗ với mạng cục bộ (LAN) các nối kết từ xa vào mạng LAN hiện đang là những yêu cầu cần thiết của người sử dụng. Việc liên kết đó cho phép một máy từ xa như của một người sử dụng tại nhà có thể qua đường dây điện

thoại thâm nhập vào một mạng LAN và sử dụng tài nguyên của nó. Cách thông dụng nhất hiện nay là dùng modem để có thể truyền trên đường dây điện thoại.

Windows NT cung cấp Dịch vụ Remote access Service cho phép các máy trạm có thể nối với tài nguyên của Windows NT server thông qua đường dây điện thoại. RAS cho phép truyền nối với các server, điều hành các user và các server, thực hiện các chương trình khai thác số liệu, thiết lập sự an toàn trên mạng. .

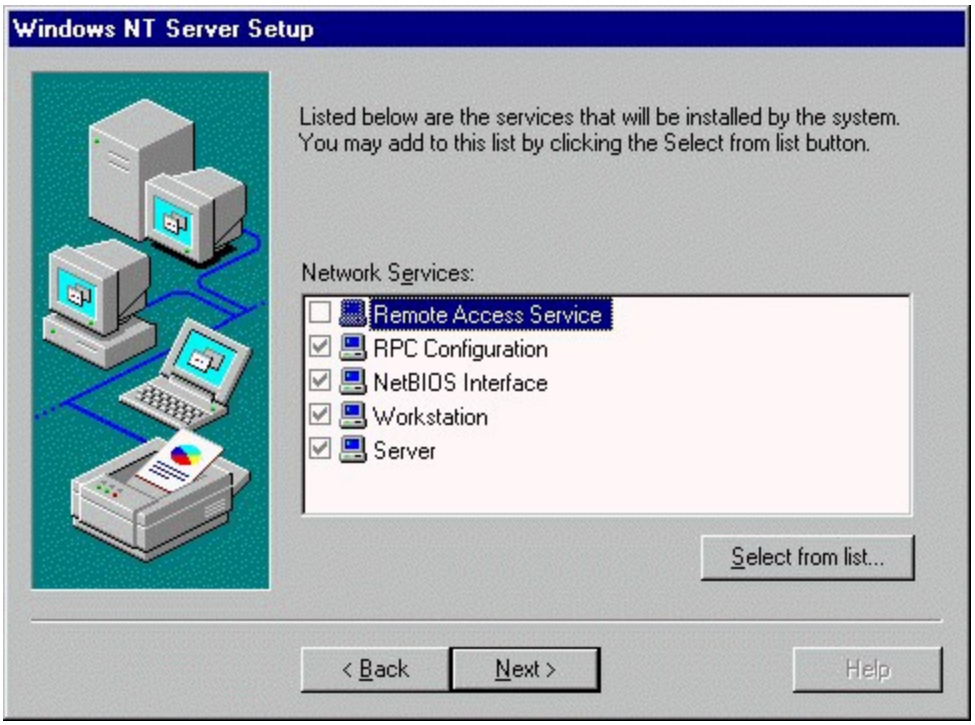
Máy trạm có thể được nối với server có dịch vụ RAS thông qua modem hoạc pull modem, cable null modem (RS232) hoặc X.25 network.

Khi đã cài đặt dịch vụ RAS, cần phải đảm bảo quyền truy nhập từ xa cho người sử dụng bằng tiện ích remote access amind để gán quyền hoặc có thể đăng ký người sử dụng ở remote access server. RAS cũng có cơ chế đảm bảo an toàn cho tài nguyên bằng cách kiểm soát các yếu tố sau: quyền sử dụng, kiểm tra mã số, xác nhận người sử dụng, đăng ký sử dụng tài nguyên và xác nhận quyền gọi lại.




*Hình 15.4: Mô hình truy cập từ xa bằng dịch vụ RAS*

Để cài đặt RAS chúng ta lựa chọn yêu cầu hộp Windows NT server setup hiện ra lúc cài đặt hệ điều hành Windows NT.




Với RAS tất cả các ứng dụng đều thực hiện trên máy từ xa, thay vì kết nối với mạng thông qua card mạng và đường dây mạng thì máy ở xa sẽ liên kết qua modem tới một RAS Server. Tất cả dữ liệu cần thiết được truyền qua đường điện thoại, mặc dù tốc độ truyền qua modem chậm hơn so với qua card mạng nhưng với những tác vụ của LAN không phải bao giờ dữ liệu cũng truyền nhiều.

Với những khả năng to lớn của mình trong các dịch vụ mạng, hệ điều hành Windows NT là một trong những hệ điều hành mạng tốt nhất hiện nay. Hệ điều hành Windows NT vừa cho phép giao lưu giữa các máy trong mạng, vừa cho phép truy nhập từ xa, cho phép truyền file, vừa đáp ứng cho mạng cục bộ (LAN) vừa đáp ứng cho mạng diện rộng (WAN) như Intranet, Internet. Với những khả năng như vậy hiện nay hệ điều hành Windows NT đã có những vị trí vững chắc trong việc cung cấp các giải pháp mạng trên thế giới.