Nội dung chi tiết môn học

- Chương 1: Đại cương về mạng máy tính
- Chương 2: Mô hình truyền thông
- Chương 3: Mạng cục bộ
- Chương 4: Internet
- Chương 5: Những vấn đề cơ bản của MMT

CHƯƠNG 1
KHÁI NIỆM VỀ MẠNG MÁY TÍNH

Chương 1: Khái niệm về mạng máy tính

I. Lịch sử ra đời và phát triển

II. Định nghĩa, các khái niệm

III. Mục tiêu kết nối mạng máy tính

IV. Các dịch vụ (services)

V. Giao thức mạng (protocol)

VI. Phương tiện, môi trường truyền (medium)

VII. Phân loại mạng

VIII. Các mô hình xử lý dữ liệu

IX. Kết luận chương

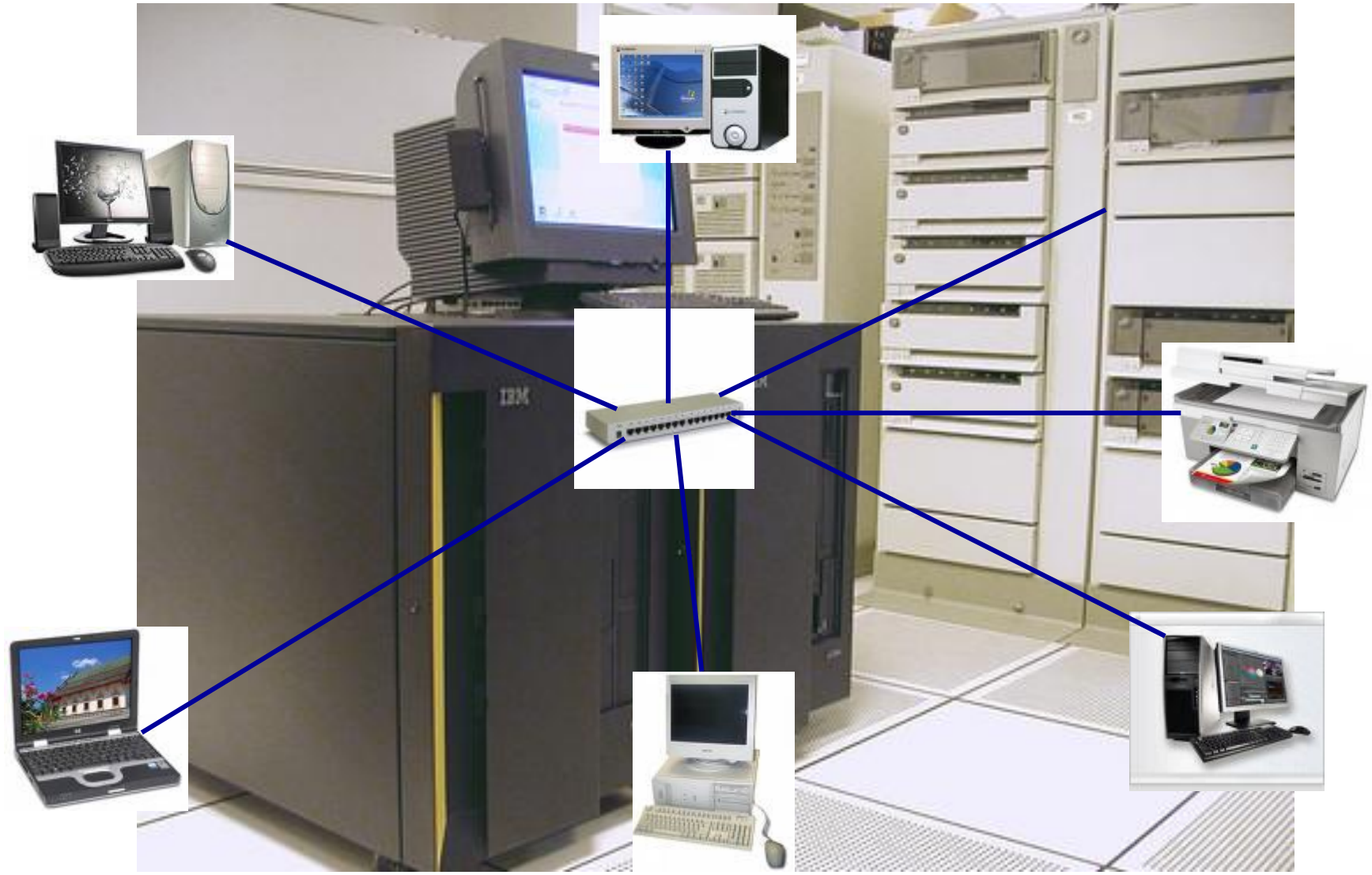
I. Lịch sử ra đời và phát triển của MMT

- Vào giữa những năm 50, thế hệ máy tính đầu tiên sử dụng bóng đèn điện tử, có kích thước rất cồng kềnh và tốn nhiều năng lượng. Nhập dữ liệu vào các máy tính được thông qua các tấm bìa mà người viết chương trình đã đục lỗ sẵn.
- 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.
- 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.

Sự hình thành mạng máy tính

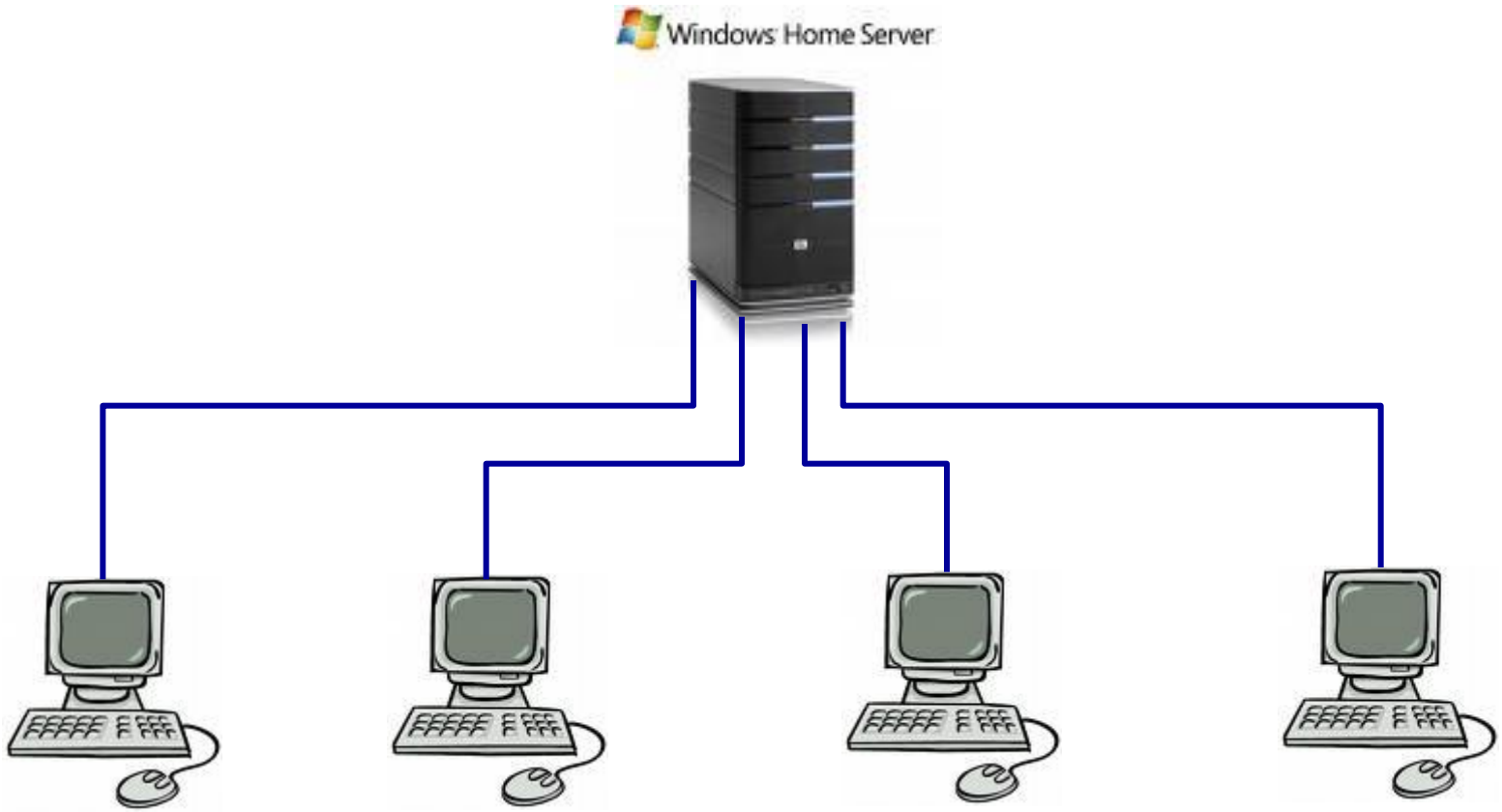
- Sự kết hợp giữa máy tính và các hệ thống truyền thông, đặc biệt là viễn thông đã tạo ra bước chuyển mới trong vấn đề khai thác và sử dụng các hệ thống máy tính.
- Các máy tính riêng lẻ được nối với nhau tạo nên môi trường làm việc mới, trong đó những người sử dụng phân tán trên các vị trí địa lý khác nhau có thể cùng khai thác tài nguyên của hệ thống.
- Tài nguyên hệ thống bao gồm: Hardware + Software + Database.
- 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...

Sự hình thành mạng máy tính



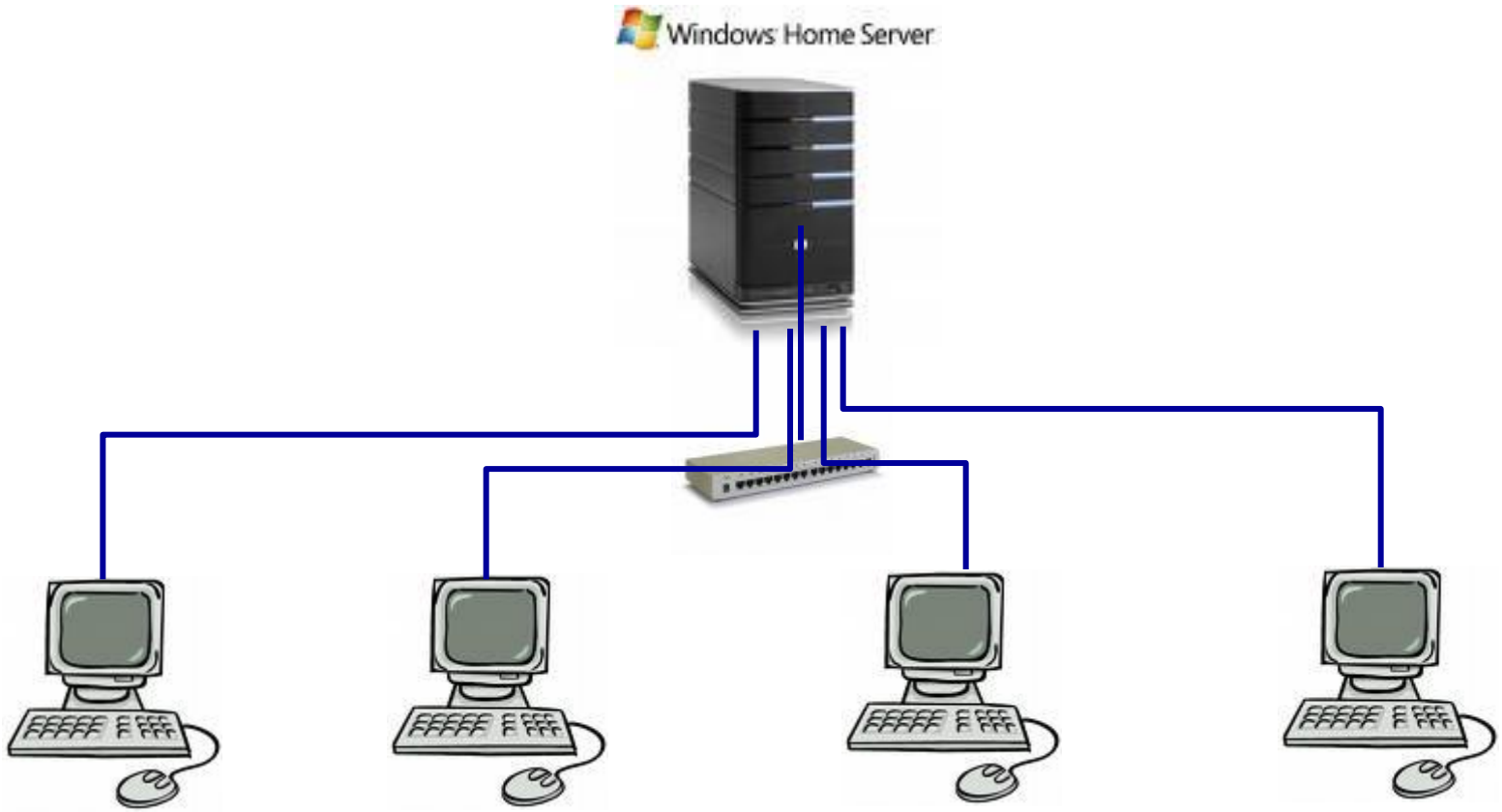
Các giai đoạn hình thành MMT (1)

- Giai đoạn các thiết bị đầu cuối (terminal) nối trực tiếp với máy tính trung tâm.



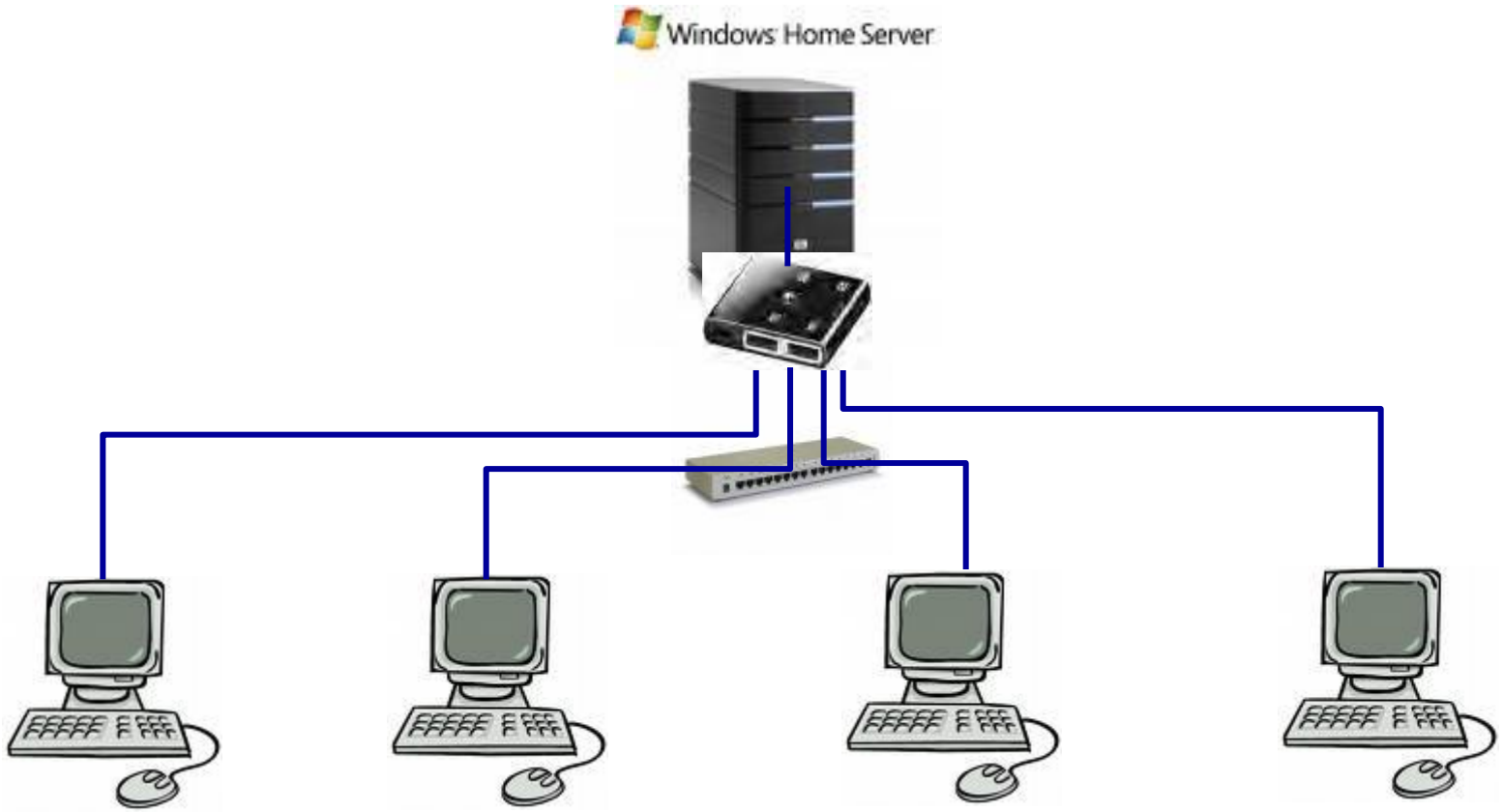
Các giai đoạn hình thành MMT (2)

- Giai đoạn sử dụng các thiết bị tập trung (hub/switch).



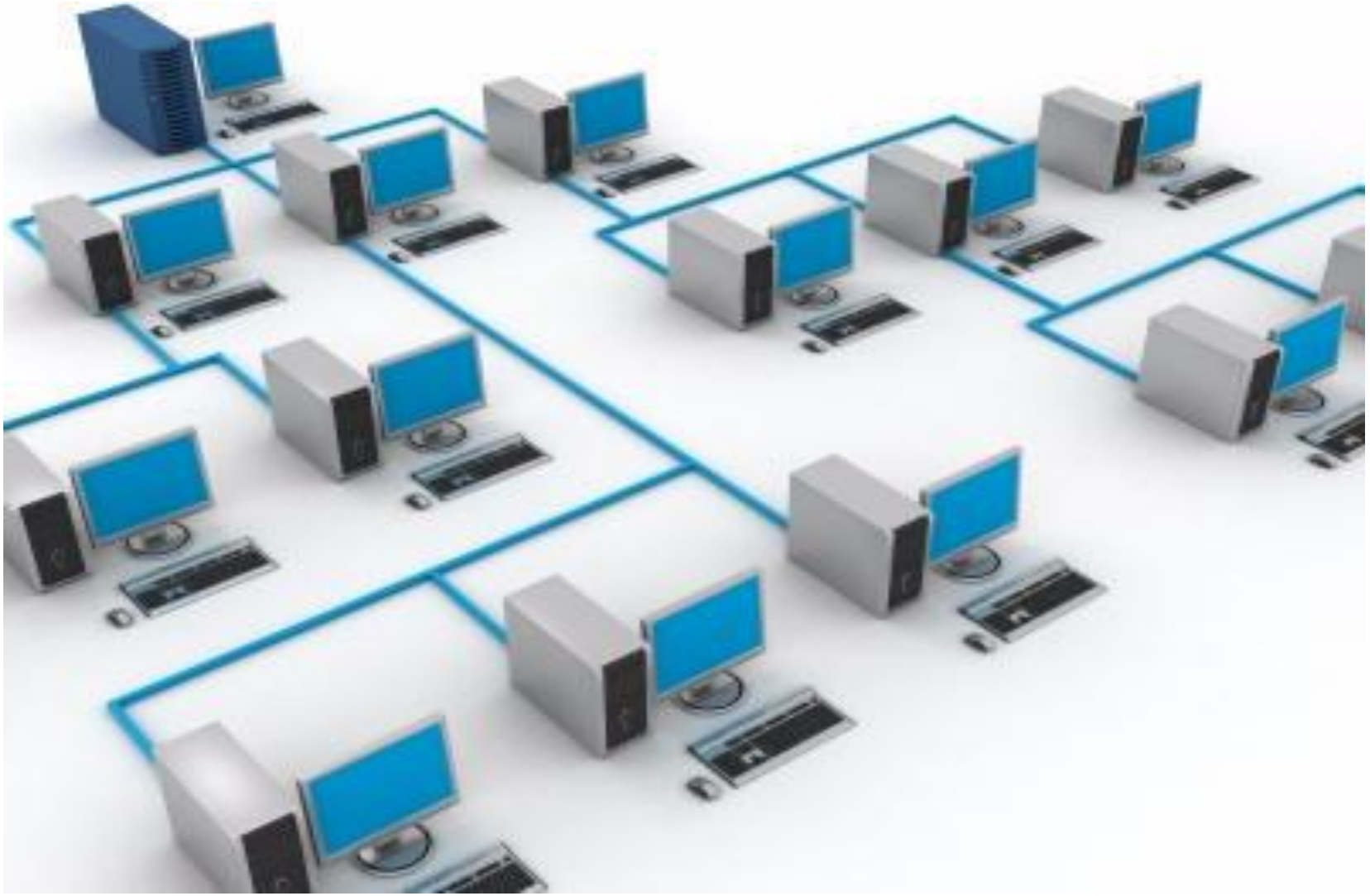
Các giai đoạn hình thành MMT (3)

- Giai đoạn kết hợp bộ tiền xử lý (pre-process).



Các giai đoạn hình thành MMT (3)

- Giai đoạn hình thành mạng máy tính



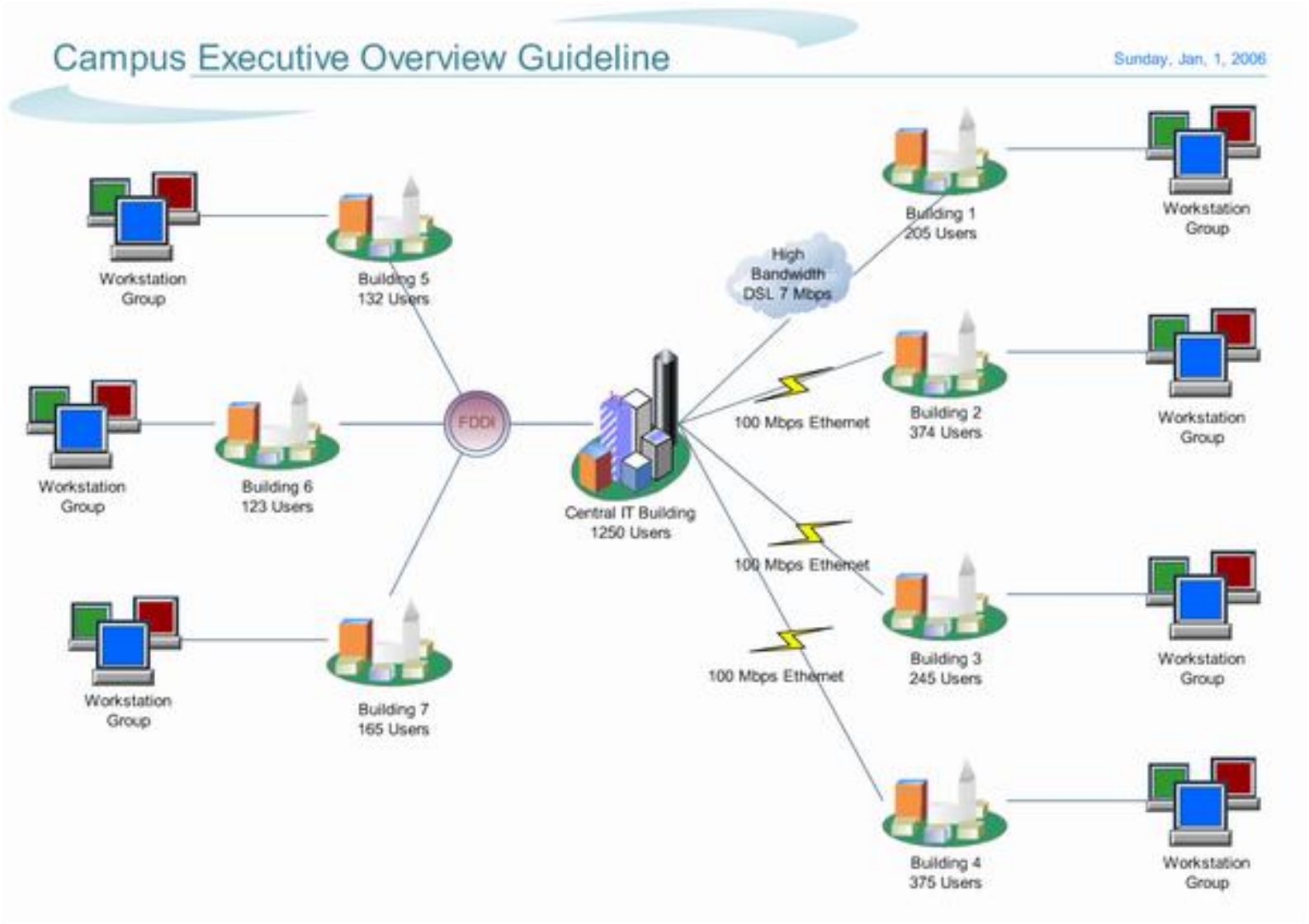
II. Mạng máy tính

- Về cơ bản, một mạng máy tính là một số các trạm máy tính, các thiết bị đầu cuối và các thiết bị khác (máy in, thiết bị lưu trữ,...) được nối kết với nhau theo một cách nào đó.
- Khác với các trạm truyền hình chỉ gửi thông tin đi, các mạng máy tính truyền trên cả hai chiều, khi máy tính A gửi thông tin tới máy tính B thì B có thể trả lời lại cho A.
- *Vì vậy, mạng (network) là một tập hợp các hệ thống máy tính và các thiết bị mạng, được kết nối với nhau thông qua một môi trường truyền, tuân theo tập các quy tắc truyền thông nhằm chia sẻ tài nguyên cho nhau.*

Cấu trúc của mạng máy tính

- Phần ngoại biên (network edge) gồm các chương trình ứng dụng, các máy tính nối vào mạng (host).
- Phần lõi của mạng (network core) bao gồm các bộ tìm đường (router) và kết nối liên mạng (mạng của các mạng).
- Các mạng truy cập (Access networks), các phương tiện kết nối vật lý (physical media) và các kết nối viễn thông (communication links)

Cấu trúc của mạng máy tính



Network Edge

- Các hệ thống đầu cuối (end systems – hosts):
  - Chạy các chương trình ứng dụng.
  - Ví dụ: WWW, email.
  - Nằm ở vòng ngoài cùng, chỉ thực hiện kết nối vào mạng.
- Mô hình làm việc khách/chủ (Client/Server model)
  - Các máy tính khách gửi yêu cầu truy cập dịch vụ đến các máy chủ và nhận lại các dịch vụ theo yêu cầu.
  - Ví dụ: WWW client (browser)/server; email client/server
- Mô hình làm việc ngang cấp (Peer-to-peer model)
  - Các máy tính trong mạng có vai trò ngang nhau
  - Ví dụ: hội thảo truyền hình (teleconferencing)

Network Core

- Mạng lưới gồm nhiều thiết bị tìm đường (router) kết nối liên thông.
- Phục vụ việc chuyển dữ liệu từ máy này sang máy khác trên mạng.
- Dữ liệu truyền trên mạng bằng phương pháp nào.

Access Network and Physical Media

Làm thế nào để nối một hệ thống ngoại biên vào mạng?

- Bằng cách nối thông qua các mạng truy cập tại vùng cư trú.
- Qua các mạng tại các trường học, cơ quan, công ty.
- Truy cập qua mạng di động.
- Vấn đề: băng thông đáp ứng của các kết nối này ở mức nào? kết nối theo phương pháp nào?

III. Mục tiêu kết nối mạng

- Cùng chia sẻ các tài nguyên chung, bất kỳ người sử dụng nào cũng có quyền khai thác, sử dụng tài nguyên của mạng mà không phụ thuộc vào vị trí địa lý của nó.
- Nâng cao độ tin cậy của hệ thống nhờ khả năng thay thế khi một số thành phần của mạng xảy ra sự cố kỹ thuật thì vẫn duy trì sự hoạt động bình thường của hệ thống.
- Tạo môi trường giao tiếp giữa người với người. Chinh phục được khoảng cách, con người có thể trao đổi, thảo luận với nhau cách xa nhau hàng nghìn km.

Ưu điểm của mạng máy tính

Từ nhiều máy tính riêng rẽ, độc lập với nhau, nếu ta kết nối chúng lại thành mạng máy tính thì chúng có thêm những ưu điểm sau:

- Nhiều người có thể dùng chung một phần mềm tiện ích.
- Một nhóm người cùng thực hiện một đề án nếu nối mạng họ sẽ dùng chung dữ liệu của đề án, dùng chung tệp tin chính (*master file*) của đề án, họ trao đổi thông tin với nhau dễ dàng.
- Dữ liệu được quản lý tập trung nên an toàn hơn, trao đổi giữa những người sử dụng thuận lợi hơn, nhanh chóng hơn.
- Có thể dùng chung thiết bị ngoại vi hiếm, đắt tiền (máy in, máy vẽ,...).

Ưu điểm của mạng máy tính

- Người sử dụng trao đổi với nhau thư tín dễ dàng (E-Mail) và có thể 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,...
- Một số người sử dụng không cần phải trang bị máy tính đắt tiền (chi phí thấp mà chức năng lại mạnh).
- 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.
- Rất an toàn cho dữ liệu và phần mềm vì phần mềm mạng sẽ khoá các tệp tin (files) khi có những người không đủ quyền hạn truy xuất các tệp tin và thư mục đó.

IV. Các dịch vụ mạng

- Các xu hướng phát triển dịch vụ mạng máy tính
  - Cung cấp các dịch vụ truy nhập vào các nguồn thông tin ở xa để khai thác và xử lý thông tin. Cung cấp các dịch vụ mua bán, giao dịch qua mạng...
  - Phát triển các dịch vụ tương tác giữa người với người trên phạm vi diện rộng. Đáp ứng nhu cầu trao đổi thông tin đa dịch vụ, đa phương tiện. Tạo các khả năng làm việc theo nhóm bằng các dịch vụ thư điện tử, video hội nghị, chữa bệnh từ xa ...
  - Xu hướng phát triển các dịch vụ giải trí trực tuyến (Online) hiện đại. Các hình thức dịch vụ truyền hình, nghe nhạc, chơi game trực tuyến qua mạng...

Các dịch vụ mạng

- Các dịch vụ phổ biến trên mạng máy tính
  - Dịch vụ tệp (File services) cho phép chia sẻ tài nguyên thông tin chung, chuyển giao các tệp dữ liệu từ máy này sang máy khác.
  - Dịch vụ thư điện tử Email (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.
  - 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.

VI. Giao thức mạng máy tính (Protocol)

1. Khái niệm về giao thức

- Các thực thể của mạng muốn trao đổi thông tin với nhau phải bắt tay, đàm phán về một số thủ tục, quy tắc... Cùng phải "nói chung một ngôn ngữ". Tập quy tắc hội thoại được gọi là giao thức mạng (Protocols). Các thành phần chính của một giao thức bao gồm:
  - Cú pháp: định dạng dữ liệu, phương thức mã hoá và các mức tín hiệu.
  - Ngữ nghĩa: thông tin điều khiển, điều khiển lưu lượng và xử lý lỗi..
- Trao đổi thông tin giữa hai thực thể có thể là trực tiếp hoặc gián tiếp. Trong hai hệ thống kết nối điểm - điểm, các thực thể có thể trao đổi thông tin trực tiếp không có sự can thiệp của các thực thể trung gian. Trong cấu trúc quảng bá, hai thực thể trao đổi dữ liệu với nhau phải thông qua các thực thể trung gian. Phức tạp hơn khi các thực thể không chia sẻ trên cùng một mạng chuyển mạch, kết nối gián tiếp phải qua nhiều mạng con.

VI. Giao thức mạng máy tính (Protocol)

2. Chức năng giao thức

- Đóng gói
- Phân đoạn và hợp lại
- Điều khiển liên kết
- Giám sát
- Điều khiển lưu lượng
- Điều khiển lỗi
- Đồng bộ hoá
- Địa chỉ hóa

VII. Phương tiện, môi trường truyền

Phương tiện (môi trường-medium) truyền vật lý là vật truyền tải các tín hiệu điện tử giữa các thành phần mạng với nhau, bao gồm các loại cáp và các phương tiện vô tuyến.

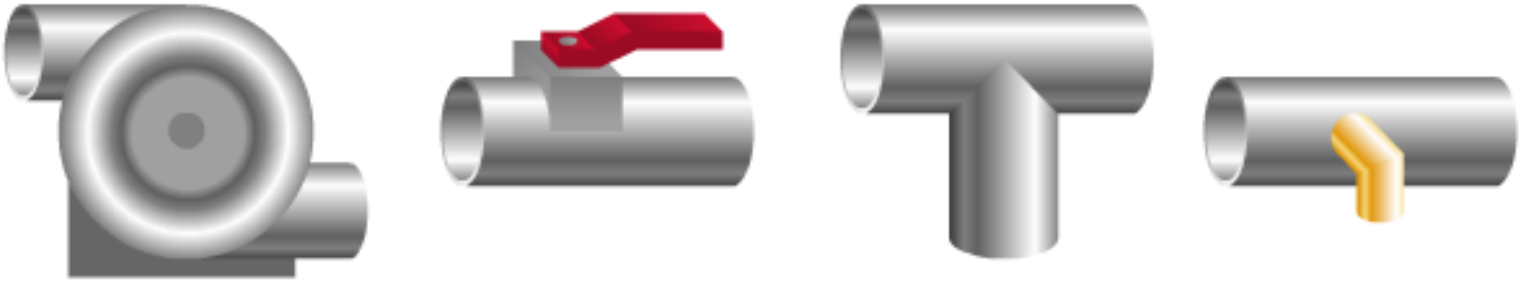
1. Đặc trưng cơ bản của đường truyền

- Băng thông (Bandwidth): Băng thông của một đường truyền là miền tần số giới hạn thấp và tần số giới hạn cao, tức là miền tần số mà đường truyền đó có thể đáp ứng được.
- Thông lượng (Throughput) Thông lượng của đường truyền là số lượng các bit (chuỗi bit) được truyền đi trong một giây. Hay nói cách khác là tốc độ của đường truyền dẫn. Ký hiệu là bit/s hoặc bps. Tốc độ của đường truyền phụ thuộc vào băng thông và độ dài của nó. Một mạng LAN Ethernet tốc độ truyền 10 Mbps và có băng thông là 10 Mbps.
- Suy hao (Attenuation): Là độ đo sự suy yếu của các tín hiệu trên đường truyền. Suy hao phụ thuộc vào độ dài của cáp, cáp càng dài thì suy hao càng cao. Khi thiết kế cáp cũng rất cần quan tâm đến giới hạn chiều dài cho phép của từng loại cáp.

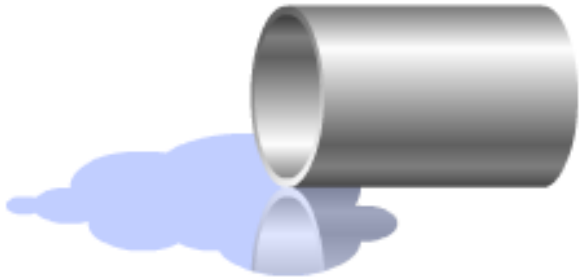
So sánh băng thông và lưu lượng ống nước

Bandwidth is like pipewidth.

Network devices are like pumps, valves, fittings, and taps.



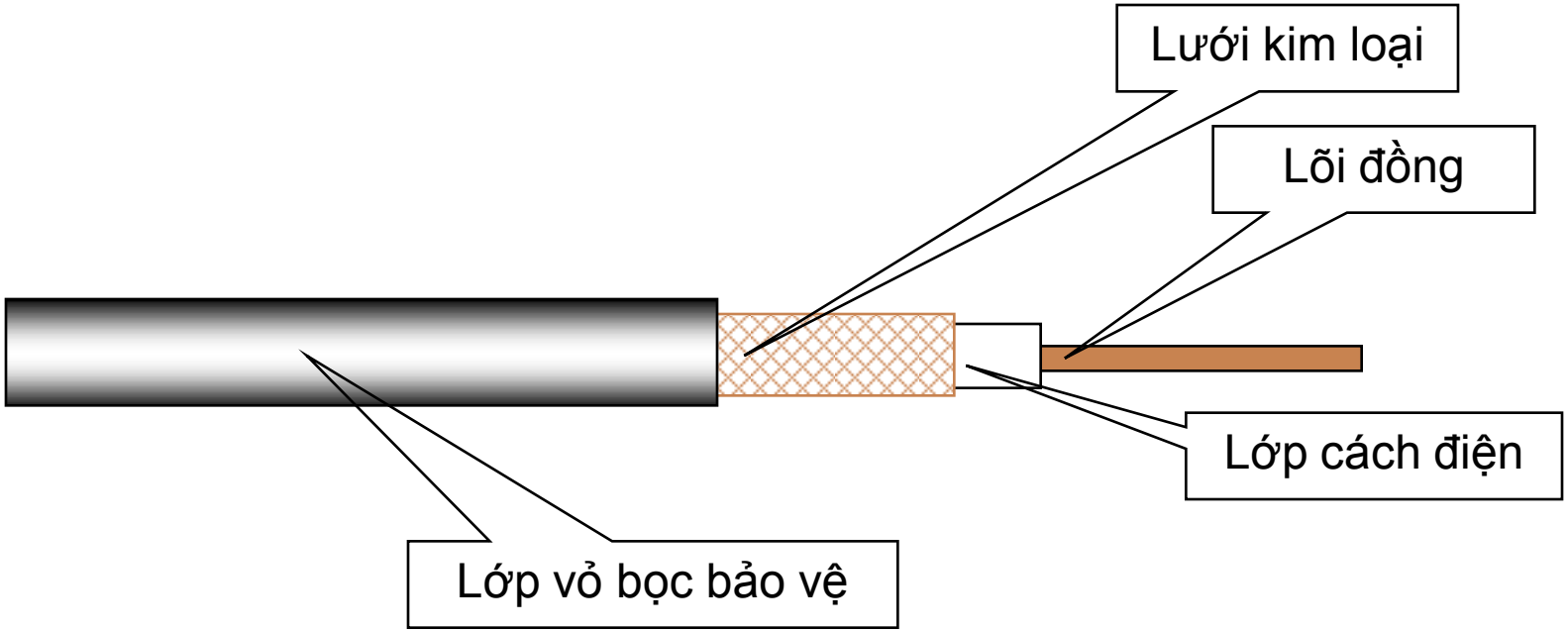
Packets are like water.

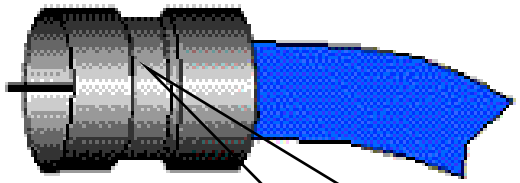


2. Phương tiện truyền hữu tuyến (cáp)

- Cáp đồng trục (Coaxial cable)
  - Cáp đồng trục dày (Thick cable)
  - Cáp đồng trục mỏng (Thin cable)
- Cáp xoắn đôi (Twisted Pair cable)
  - Cáp có màng chắn (STP - Shielded Twisted Pair)
  - Cáp không có vỏ bọc (UTP - Unshielded Twisted Pair)
- Cáp sợi quang (Fiber Optic Cable)
  - Cáp quang đơn chế độ (Single-Mode)
  - Cáp quang đa chế độ (Multi-Mode)
    - Step index
    - Graded index

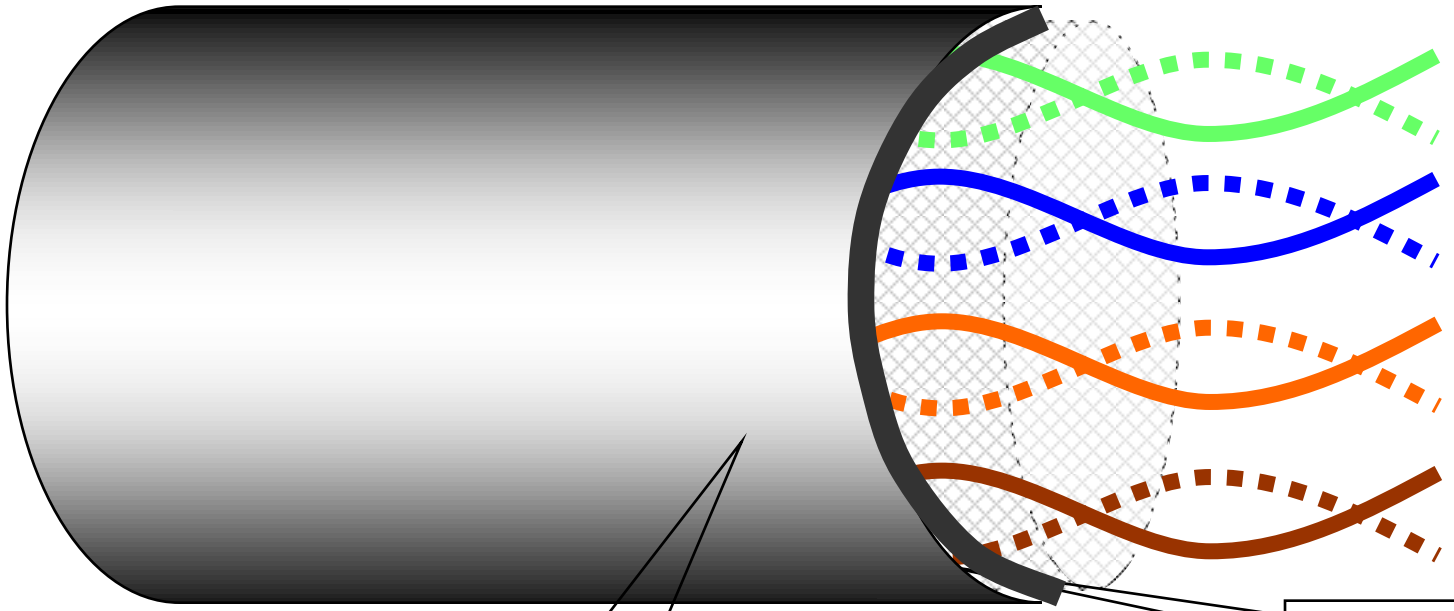
2.a. Cáp đồng trục (Coaxial cable)

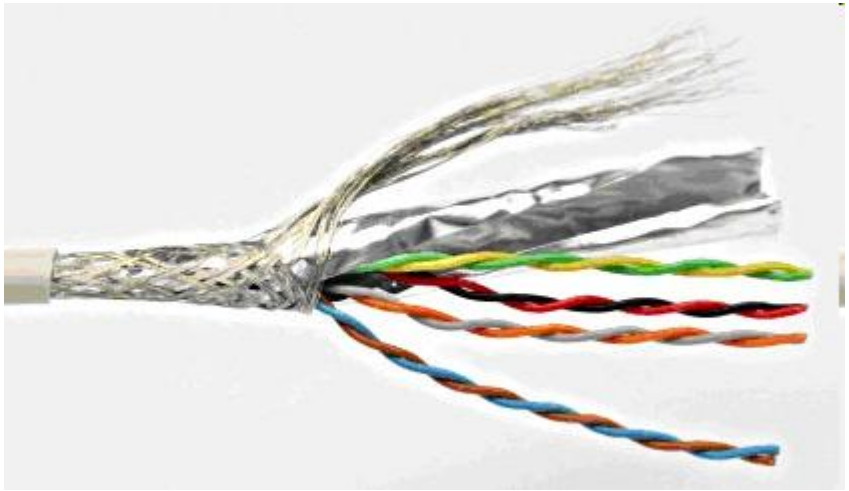




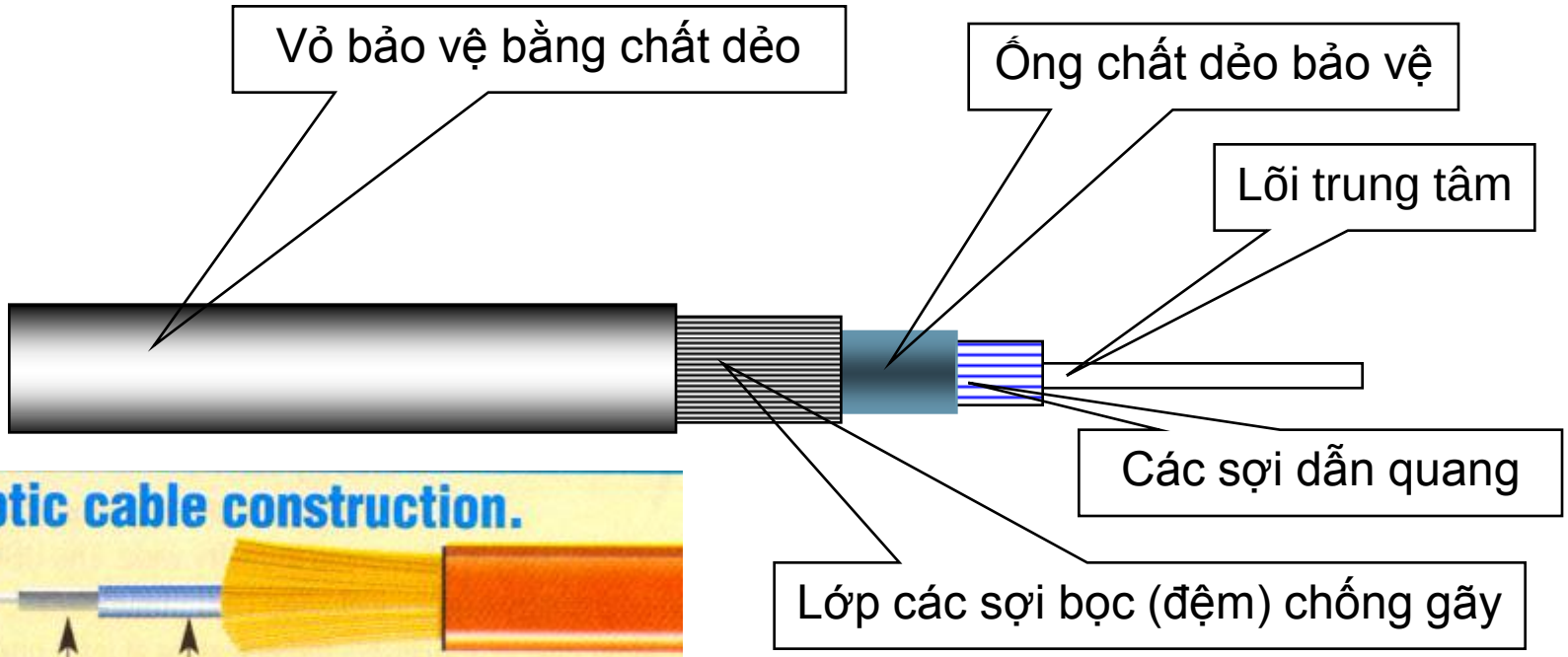
Đầu nối BNC

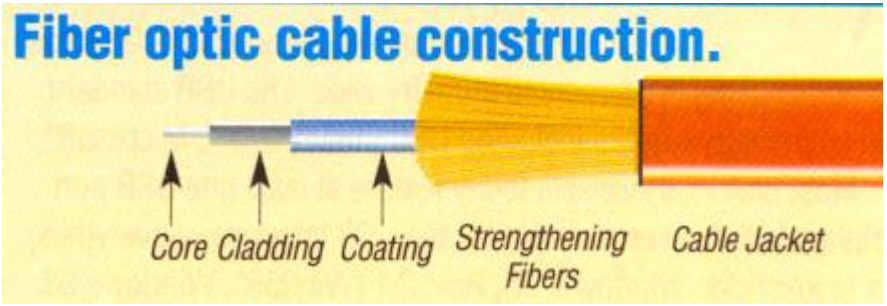
2.b. Cáp xoắn đôi (Twisted Pair cable)

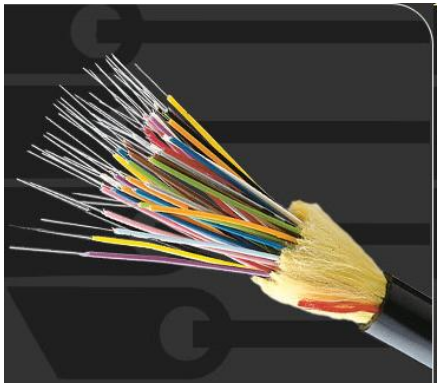




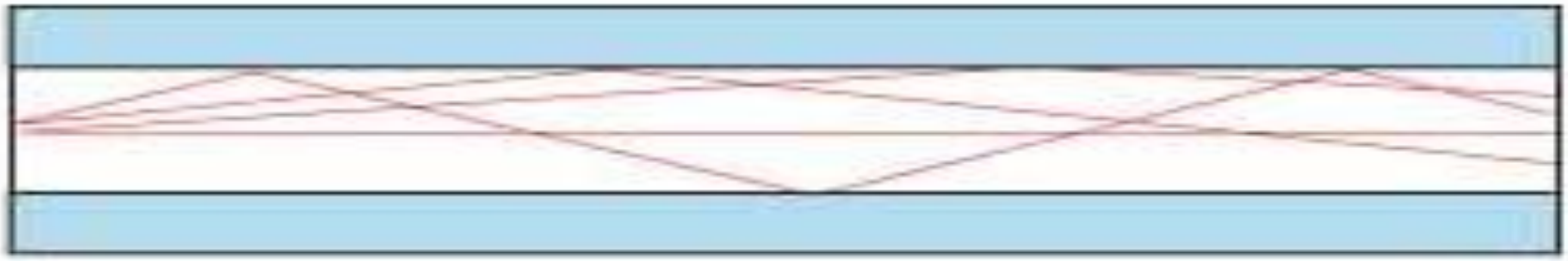
2.c. Cáp quang (Fiber Optic cable)



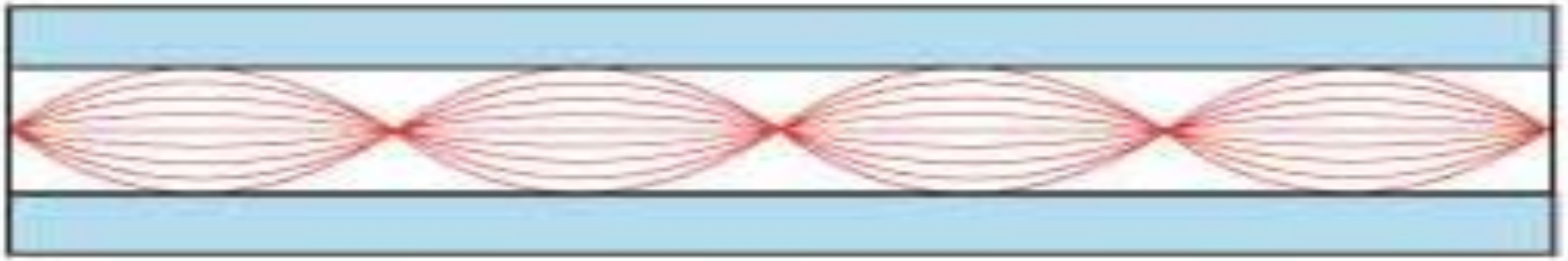




2.c. Cáp quang (Fiber Optic cable)



Multimode, Step-index



Multimode, Graded Index

Singlemode

3. Phương tiện truyền vô tuyến

- Radio: Quang phổ của điện từ nằm trong khoảng 10 KHz đến 1GHz. Có nhiều giải tần: Sóng ngắn (Short Wave), VHF (VeryHightFrequency) -Tivi&Radio FM và UHF (Ultra Hight Frequency) -Tivi
- Viba: Truyền thông viba có hai dạng: Viba mặt đất và vệ tinh. Viba mặt đất sử dụng các trạm thu và phát. Kỹ thuật truyền thông vệ tinh sử dụng các trạm thu mặt đất (các đĩa vệ tinh) và các vệ tinh.
- Tia hồng ngoại (Infrared system): Có 2 phương thức kết nối mạng Point-to-Point và Multi Point.
- WIFI: Sử dụng sóng vô tuyến, truyền và phát tín hiệu ở tần số 2.5 GHz hoặc 5GHz

Mạng máy tính sử dụng WIFI

VIII. Phân loại mạng

1. Theo phạm vi địa lý
   - PAN, LAN, MAN, WAN, GAN, Internet
2. Theo kỹ thuật chuyển mạch
   - Circuit Switched, Message Switched, Packet Switched
3. Theo cách khai thác dữ liệu
   - Peer to Peer, Client/Server

Các loại mạng dữ liệu

Distance Between CPUs	Location of CPUs	Name
0.1 m	Printed circuit board Personal data asst.	Motherboard Personal Area Network (PAN)
1.0 m	Millimeter Mainframe	Computer Systems Network
10 m	Room	Local Area Network (LAN) Your classroom
100 m	Building	Local Area Network (LAN) Your school
1000 m = 1 km	Campus	Local Area Network (LAN) Stanford University
100,000 m = 100 km	Country	Wide Area Network (WAN) Cisco Systems, Inc.
1,000,000 m = 1,000 km	Continent	Wide Area Network (WAN) Africa
10,000,000 m = 10,000 km	Planet	Wide Area Network (WAN) The Internet
100,000,000 m = 100,000 km	Earth-moon system	Wide Area Network (WAN) Earth and artificial satellites

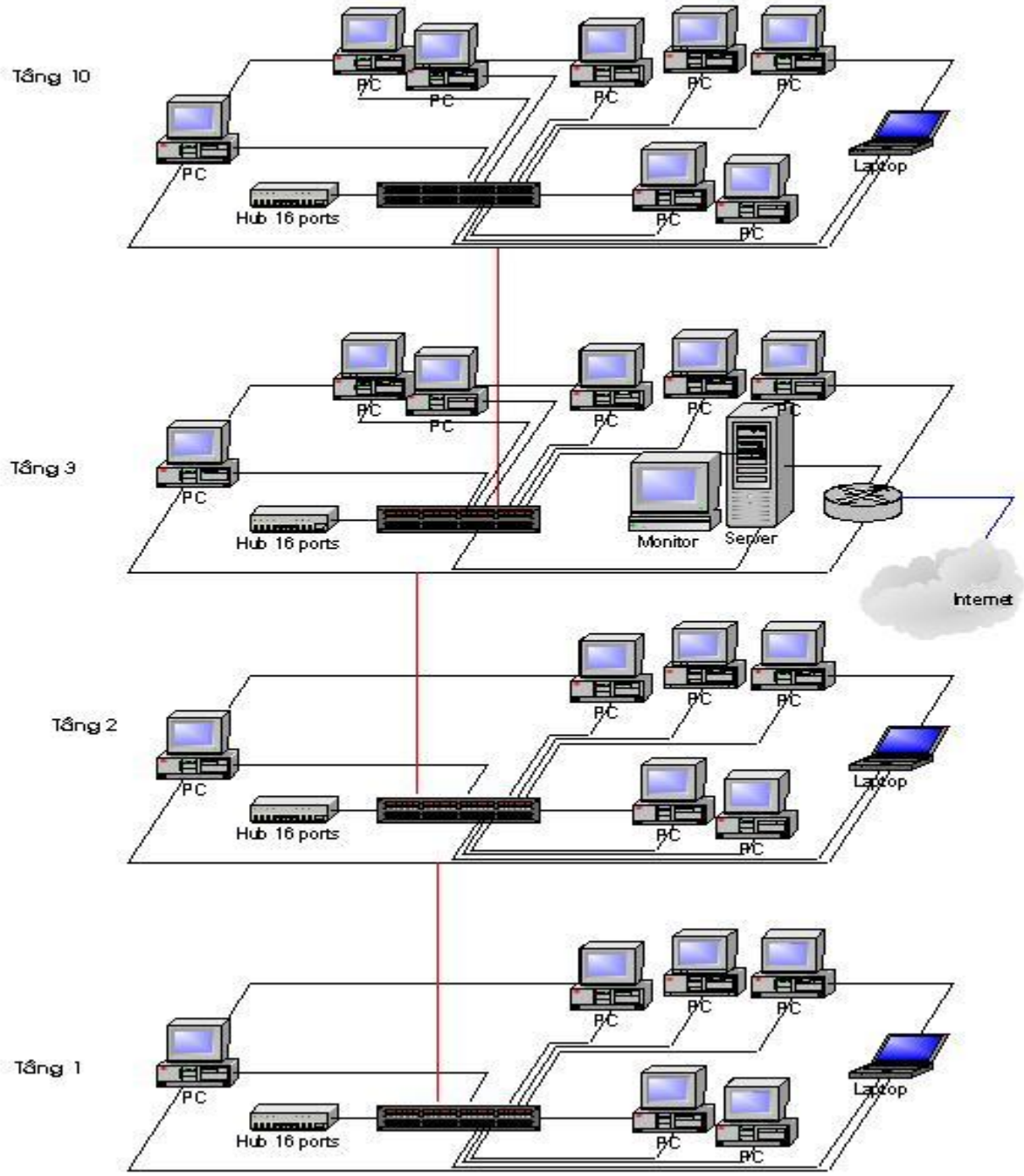
1.a. Mạng cục bộ LAN (Local Area Networks)

Mạng cục bộ LAN: kết nối các máy tính đơn lẻ thành mạng nội bộ, tạo khả năng trao đổi thông tin và chia sẻ tài nguyên trong cơ quan, xí nghiệp... Có hai loại mạng LAN khác nhau: LAN nối dây (sử dụng các loại cáp) và LAN không dây (sử dụng sóng cao tần hay tia hồng ngoại). Đặc trưng cơ bản của mạng cục bộ:

- Quy mô của mạng nhỏ, phạm vi hoạt động khoảng vài km
- Công nghệ truyền dẫn sử dụng trong mạng LAN thường là quảng bá (Broadcast)
- Hình trạng của mạng đa dạng

Băng thông một số môi trường trong LAN

Some Typical Media	Bandwidth	Max. Physical Distance
50-Ohm Coaxial Cable (Ethernet 10BASE2, ThinNet)	10-100 Mbps	185m
50-Ohm Coaxial Cable (Ethernet 10BASE5, ThickNet)	10-100 Mbps	500m
Category 5 Unshielded Twisted Pair (UTP) (Ethernet 10BASE-T)	10 Mbps	100m
Category 5 Unshielded Twisted Pair (UTP) (Ethernet 100BASE-TX)(Fast Ethernet)	100 Mbps	100m
Multimode (62.5/125μm) Optical Fiber 100BASE-FX	100 Mbps	2000m
Singlemode (9/125μm core) Optical Fiber 1000BASE-LX	1000 Mbps (1.000 Gbps)	3000m
Wireless	11 Mbps	a few 100meters


Tầng 10
PC
PC
PC
PC
PC
PC
Hub 16 ports
PC
PC
Laptop
Tầng 3
PC
PC
PC
PC
PC
Hub 16 ports
Monitor
Server
Internet
Tầng 2
PC
PC
PC
PC
Hub 16 ports
PC
PC
Laptop
Tầng 1
PC
PC
PC
PC
Hub 16 ports
PC
PC
Laptop

1.b. Mạng diện rộng WAN (Wide Area Network)

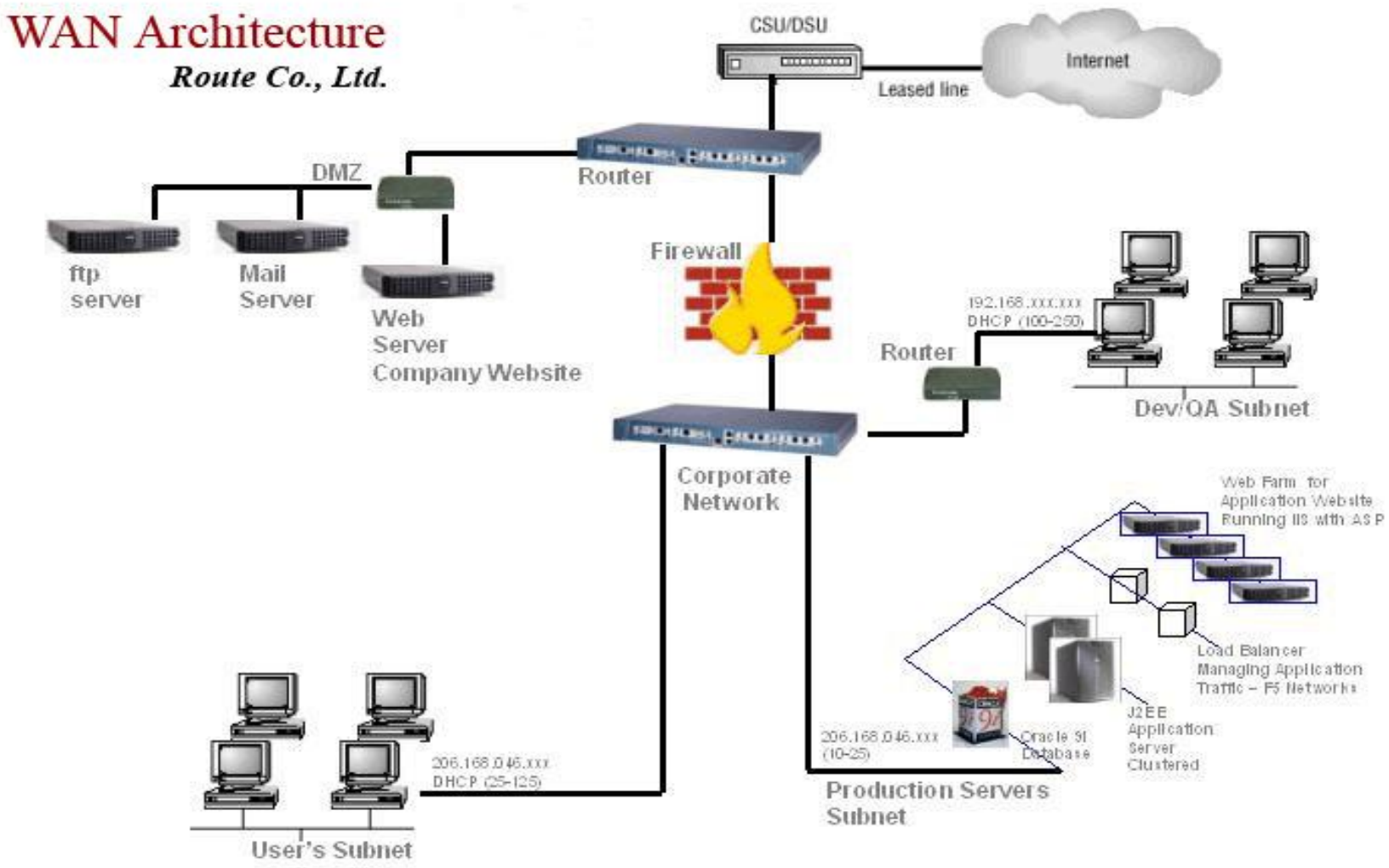
Đặc trưng cơ bản của một mạng WAN:

- Hoạt động trên phạm vi một quốc gia hoặc trên toàn cầu.
- Tốc độ truyền dữ liệu thấp so với mạng cục bộ.
- Lỗi truyền cao.

Một số mạng diện rộng điển hình

- Mạng tích số hợp đa dịch vụ ISDN (Integrated Services Digital Network)
- Mạng X25 và chuyển mạch khung Frame Relay
- Phương thức truyền không đồng bộ ATM (Asynchronous Transfer Mode)
- Mạng hội tụ - mạng thế hệ sau NGN (Next Generation Network)

1.b. Mạng diện rộng WAN (tt)



1.c. Liên mạng (inter-network)

- Nhu cầu trao đổi thông tin và chia sẻ tài nguyên chung đòi hỏi các hoạt động truyền thông cần thiết phải kết nối nhiều mạng thành một mạng lớn, gọi là liên mạng.
- Liên mạng (internet) là mạng của các mạng con, là một tập các mạng LAN, WAN, MAN độc lập được kết nối lại với nhau. Kết nối liên mạng có một số lợi ích sau:
  - Giảm lưu thông trên mạng.
  - Tối ưu hoá hiệu năng.
  - Đơn giản hoá việc quản trị mạng.
  - Hiệu quả hơn so với việc sử dụng các mạng đơn lẻ.
- Liên mạng được bổ sung thêm tài nguyên và các dịch vụ trở thành mạng Internet.

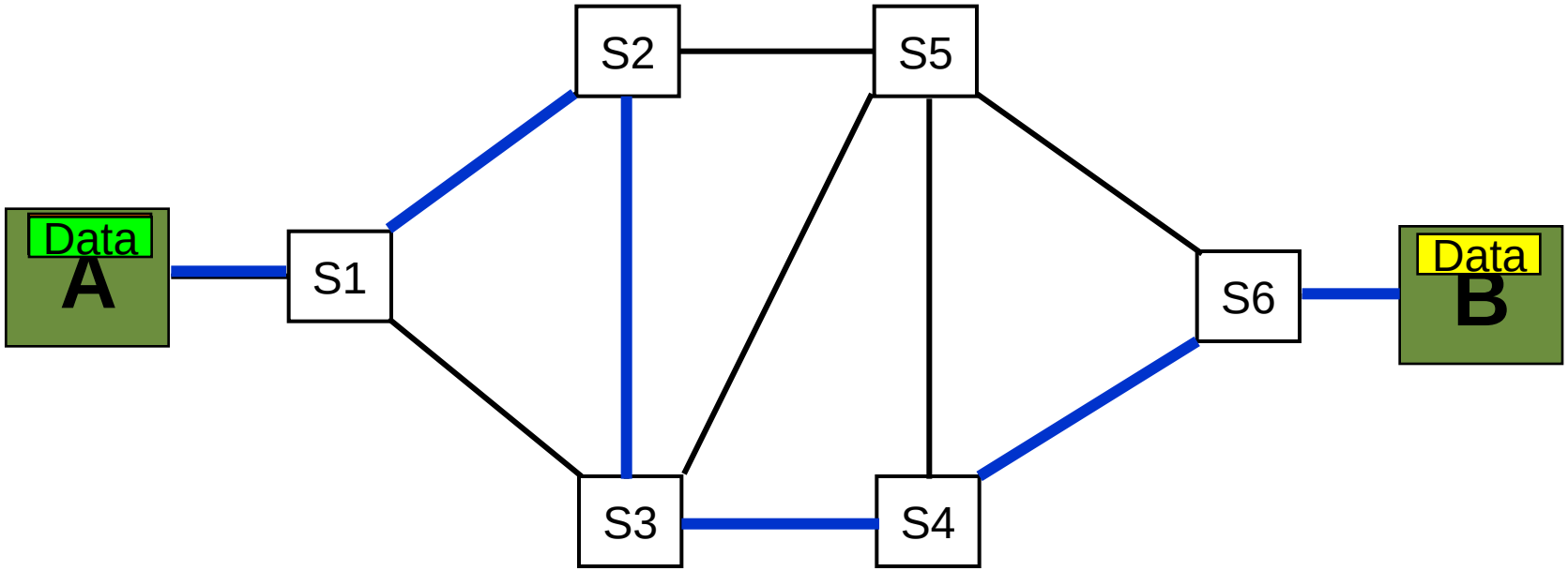
1.c. Liên mạng (tt)

2.a. Mạng chuyển mạch kênh

- Trước khi trao đổi thông tin, hệ thống sẽ thiết lập kết nối giữa 2 thực thể bằng một đường truyền vật lý. Thực thể đích nếu bận, kết nối này sẽ bị huỷ bỏ.
- Duy trì kết nối trong suốt quá trình 2 thực thể trao đổi thông tin.
- Giải phóng kết nối: Sau khi truyền xong dữ liệu, kết nối sẽ được huỷ bỏ, giải phóng các tài nguyên đã bị chiếm dụng để sẵn sàng phục vụ cho các yêu cầu kết nối khác.
- Nhược điểm là cần nhiều thời gian để thiết lập kênh truyền, vì vậy thời gian thiết lập kênh chậm và xác suất kết nối không thành công cao. Khi cả hai không còn thông tin để truyền, kênh bị bỏ không trong khi các thực thể khác có nhu cầu.

2.a. Mạng chuyển mạch kênh (tt)

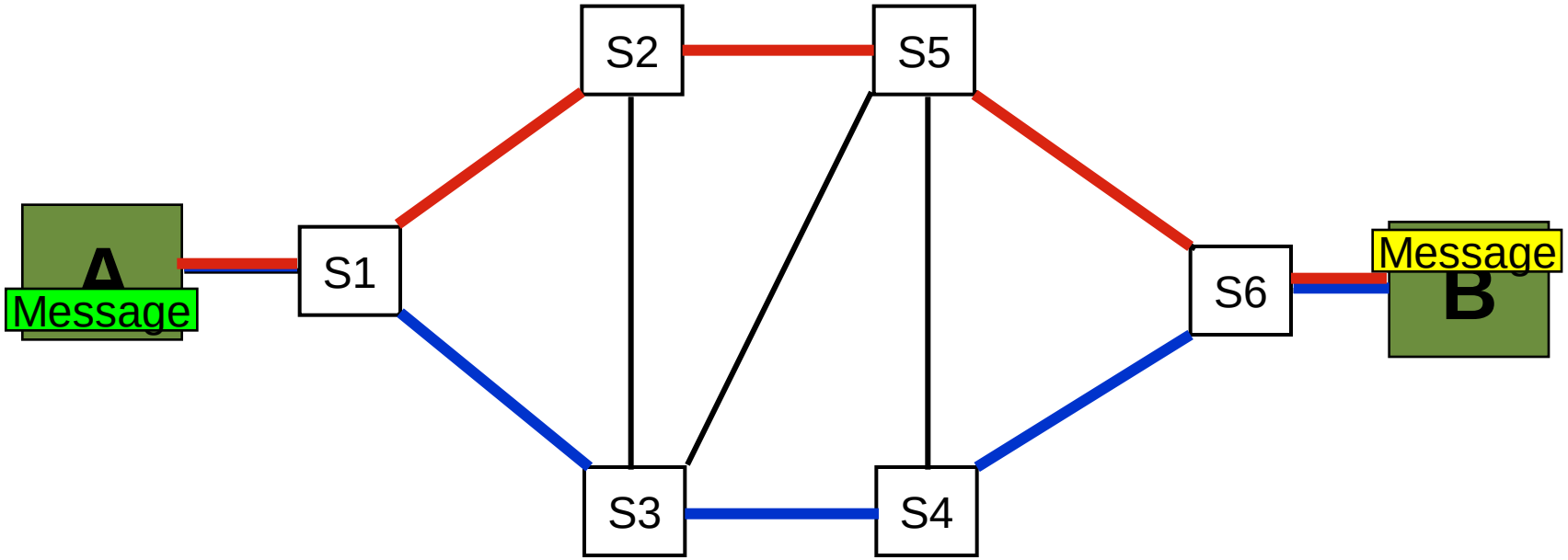
Giai đoạn 2: Thiết lập kết nối



2.b. Mạng chuyển mạch thông báo

- Các nút của mạng căn cứ vào địa chỉ đích của “thông báo” để chọn nút kế tiếp trên đường dẫn tới đích. Như vậy các nút cần lưu trữ tạm thời và đọc tin nhận được, quản lý việc chuyển tiếp thông báo đi. Tùy thuộc vào điều kiện mạng mà các thông báo khác nhau có thể được gửi trên các con đường khác nhau.
- 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 có thể lưu trữ thông báo cho tới khi kênh truyền rỗi mới chuyển thông báo đi, do đó giảm tình trạng tắc nghẽn trên mạng.
- Có thể điều khiển truyền tin bằng cách sắp xếp mức độ ưu tiên của các thông báo. Trong mạng chuyển mạch thông báo ta có thể làm tăng hiệu suất sử dụng băng thông của mạng bằng cách gán địa chỉ quảng bá cho các thông báo để gửi nó đồng thời đến nhiều đích khác nhau.
- Nhược điểm chủ yếu là trong trường hợp một thông báo dài bị lỗi, phải truyền thông báo này lại nên hiệu suất không cao. Phương pháp này thích hợp với phương pháp truyền thư tín điện tử (*Electronic mail*).

2.b. Mạng chuyển mạch thông báo (tt)

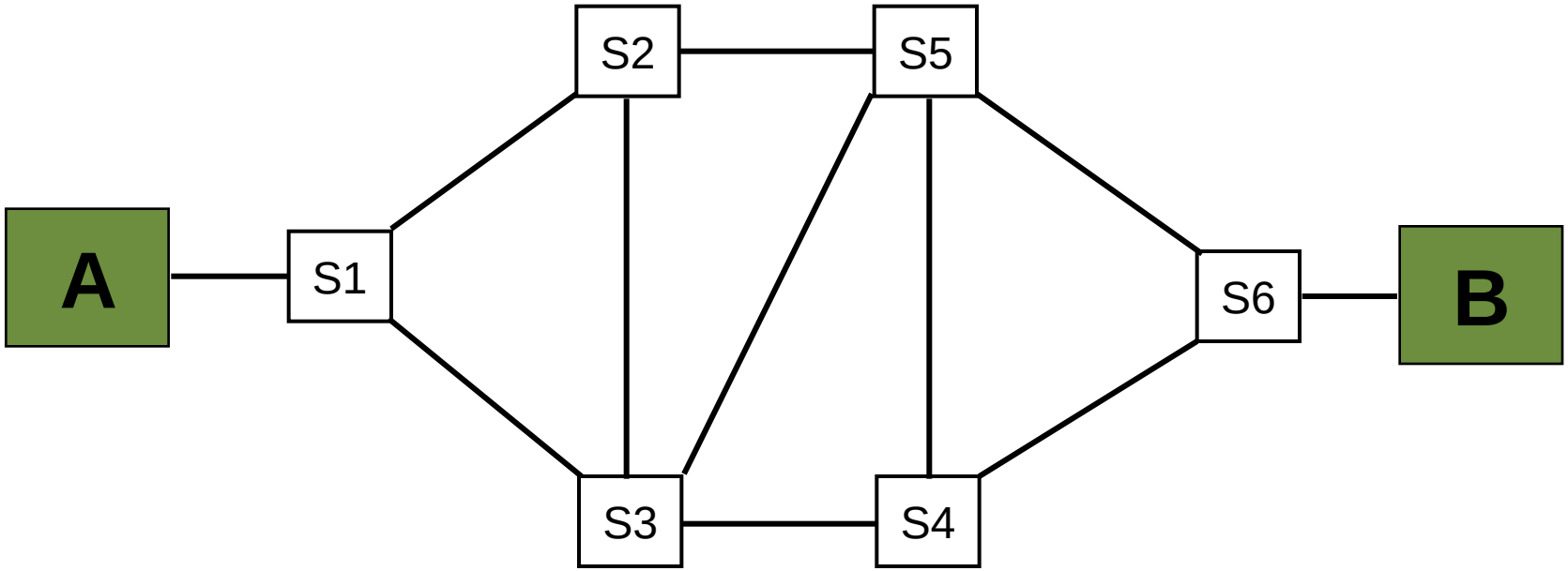


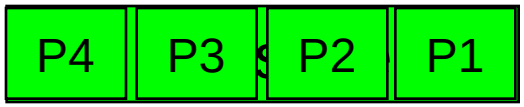
2.c. Mạng chuyển mạch gói

- Trong trường hợp này một thông báo có thể chia ra thành nhiều gói tin (Packet) khác nhau, độ dài khoảng 256 byte, có khuôn dạng quy định. Các gói tin chứa thông tin điều khiển, trong đó có địa chỉ nguồn và địa chỉ đích. Các gói tin của một thông báo có thể gửi đi bằng nhiều đường khác nhau.
- Mạng chuyển mạch gói có hiệu suất cao hơn mạng chuyển mạch thông báo vì kích thước của gói tin là hạn chế sao cho các nút mạng có thể xử lý toàn bộ gói tin trong bộ nhớ mà không cần lưu trữ tạm thời trên đĩa, do đó mạng chuyển các gói tin nhanh hơn.
- Mỗi đường truyền chiếm thời gian rất ngắn vì có thể dùng bất kỳ đường nào để đi đến đích và khả năng đồng bộ bit rất cao.
- Nhược điểm: thời gian truyền tin rất ngắn nên nếu thời gian chuyển mạch lớn thì tốc độ truyền không cao.
- Việc tập hợp các gói tin để tạo lại để thông báo là khó khăn, đặc biệt là trong trường hợp các gói được truyền đi theo nhiều đường khác nhau.

2.c. Mạng chuyển mạch gói (tt)

Giai đoạn 2: Thực hiện truyền các gói tin, thêm thông tin vào đầu các gói





Message

IX. Các mô hình xử lý dữ liệu

1. Mô hình ngang hàng (Peer-to-Peer)

- Trong mô hình ngang hàng tất cả các máy đều là máy chủ đồng thời cũng là máy khách.
- Các máy trên mạng chia sẻ tài nguyên không phụ thuộc vào nhau. Mạng ngang hàng thường được tổ chức thành các nhóm làm việc Workgroup. Mô hình này không có quá trình đăng nhập tập trung, nếu đã đăng nhập vào mạng có thể sử dụng tất cả tài nguyên trên mạng. Truy cập vào các tài nguyên phụ thuộc vào người đã chia sẻ các tài nguyên đó, vì vậy có thể phải biết mật khẩu để có thể truy nhập được tới các tài nguyên được chia sẻ.

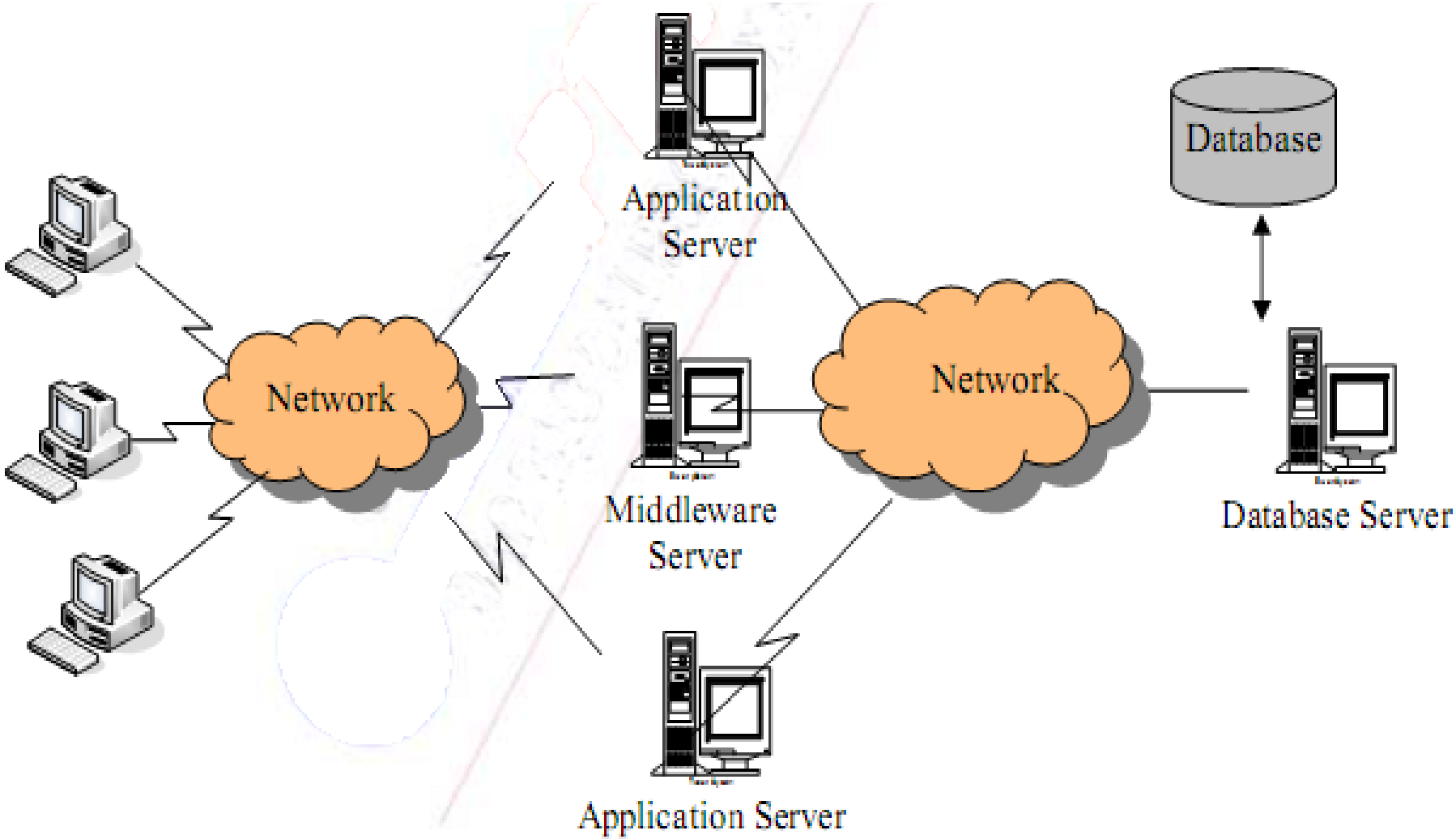
1. Mô hình mạng ngang hàng

IX. Các mô hình xử lý dữ liệu

2. Mô hình khách/phục vụ (client/server)

- Mô hình Client/Server mô tả các dịch vụ mạng và các ứng dụng được sử dụng để truy nhập các dịch vụ. Là mô hình phân chia các thao tác thành hai phần: phía Client cung cấp cho người sử dụng một giao diện để yêu cầu dịch vụ từ mạng, phía Server tiếp nhận các yêu cầu từ phía Client và cung cấp các dịch vụ một cách thông suốt cho người sử dụng.
- Chương trình Server được khởi động trên một máy chủ và ở trạng thái sẵn sàng nhận các yêu cầu từ phía Client. Chương trình Client cũng được khởi động một cách độc lập với chương trình Server. Yêu cầu dịch vụ được chương trình Client gửi đến máy chủ cung cấp dịch vụ và chương trình Server trên máy chủ sẽ đáp ứng hoặc từ chối các yêu cầu của Client. Sau khi thực hiện các yêu cầu từ phía Client, Server sẽ trở về trạng thái chờ các yêu cầu khác.

2. Mô hình mạng khách/phục vụ



X. Kết thúc chương 1

- Lịch sử ra đời, hình thành, mục tiêu và ứng dụng của mạng máy tính.
- Các lợi ích khi nối máy tính thành mạng.
- Khái niệm MMT. Chức năng các thành phần chủ yếu của MMT.
- Các đặc trưng cơ bản của đường truyền: Băng thông (bandwidth), thông lượng (throughput) và suy hao (attenuation).
- Các phương tiện (môi trương) truyền: Cáp đồng trục (Coaxial cable), cáp xoắn đôi (Twisted pair cable), cáp sợi quang (Fiber optic cable).
- Các kỹ thuật chuyển mạch. Vai trò của địa chỉ trong chuyển mạch kênh.
- Những khác biệt cơ bản giữa kiểu điểm - điểm và quảng bá.
- Khái niệm giao thức, vai trò của giao thức trong truyền thông.
- Trình bày các chức năng của giao thức.
- Mạng LAN, WAN và các đặc trưng cơ bản của chúng.

CHƯƠNG 2
KIẾN TRÚC PHÂN TẦNG VÀ MÔ HÌNH OSI

NỘI DUNG

I. Các tổ chức chuẩn hóa mạng

II. Mô hình kiến trúc và các quy tắc phân tầng

III. Mô hình kết nối các hệ thống mở OSI

IV. Một số mô hình kiến trúc chuẩn khác

I. Các tổ chức chuẩn hóa mạng

2. Các tổ chức tiêu chuẩn

- ISO (International Standards Organization)
- CCITT (International Telegraphand Telephone Consultative Commintte), nay là ITU (International Telecommunication Union)

2. Các tổ chức tiêu chuẩn

- Sự khác biệt về kiến trúc mạng đã gây trở ngại cho người sử dụng khi kết nối liên mạng.
- Cần xây dựng mô hình chuẩn làm cơ sở cho các nhà nghiên cứu và thiết kế mạng tạo ra các sản phẩm mở về mạng và tạo điều kiện cho việc phát triển và sử dụng mạng.
- Các tổ chức tiêu chuẩn quốc tế đã ra đời. Các nhà sản xuất đã thống nhất các sản phẩm, khi xuất xưởng phải tuân theo các chuẩn, các khuyến nghị quy định thiết kế và sản xuất các sản phẩm mạng.

3. Kiến trúc phân tầng

II. Mô hình kiến trúc phân tầng

- Để mạng đạt khả năng tối đa, các tiêu chuẩn được chọn phải cho phép mở rộng mạng để có thể phục vụ những ứng dụng. Tuy nhiên quan điểm này cho phép mạng làm việc với những thiết bị được sản xuất từ nhiều hãng khác nhau.
- Các tầng được chồng lên nhau, số lượng và chức năng phải các tầng phụ thuộc vào các nhà sản xuất và thiết kế. Tuy nhiên quan điểm chung là trong mỗi tầng có nhiều thiết bị để (các tiến trình) thực hiện một số chức năng nhằm cung cấp một số dịch vụ, thủ tục cho các thực thể tầng trên hoạt động.
- Các mạng máy tính được thiết kế và cài đặt theo quan điểm có cấu trúc đa tầng (layers). Mỗi một thành phần của mạng được xem như một hệ thống gồm nhiều tầng và mỗi một tầng bao gồm một số chức năng truyền thông.
- ISO đã đưa ra mô hình 7 tầng (gọi là lớp hay mức) cho mạng, gọi là kiểu hệ thống kết nối mở hoặc mô hình **OSI** (*Open System Interconnection*).

II.1. Quy tắc phân tầng

ISO quy định các quy tắc phân tầng như sau:

- Không định nghĩa quá nhiều tầng, số tầng ít nhất là như nhau, không quá phức tạp khi xác định và ghép nối các tầng. Chức năng các tầng độc lập với nhau và có tính mở.
- Dữ liệu không được truyền trực tiếp từ tầng thứ i của hệ thống phát sang tầng thứ i của hệ thống nhận (trừ tầng thấp nhất - tầng vật lý) mà được chuyển từ tầng cao xuống tầng thấp nhất bên hệ thống phát và qua đường truyền vật lý, dữ liệu lại được chuyển ngược lên các tầng trên. Giữa các đồng tầng xác định liên kết logic, giữa các tầng vật lý có liên kết vật lý.

Xác định mối quan hệ giữa các tầng, gồm:
- Trong mỗi hệ thống, cần xác định rõ mối quan hệ giữa các tầng kề nhau, mối quan hệ này gọi là giao diện tầng (Interface). Mối quan hệ này quy định những thao tác và dịch vụ cơ bản mà tầng kề dưới cung cấp cho tầng kề trên và sự tương tác qua lại giữa hai tầng kề nhau đó.

Và chức năng của các tầng trong một hệ thống mạng là những gì mà mỗi tầng phải thực hiện để truyền thông, mối quan hệ đó là tập các quy tắc và các thoả thuận trong hội thoại giữa các hệ thống, mối quan hệ này gọi là giao thức tầng.

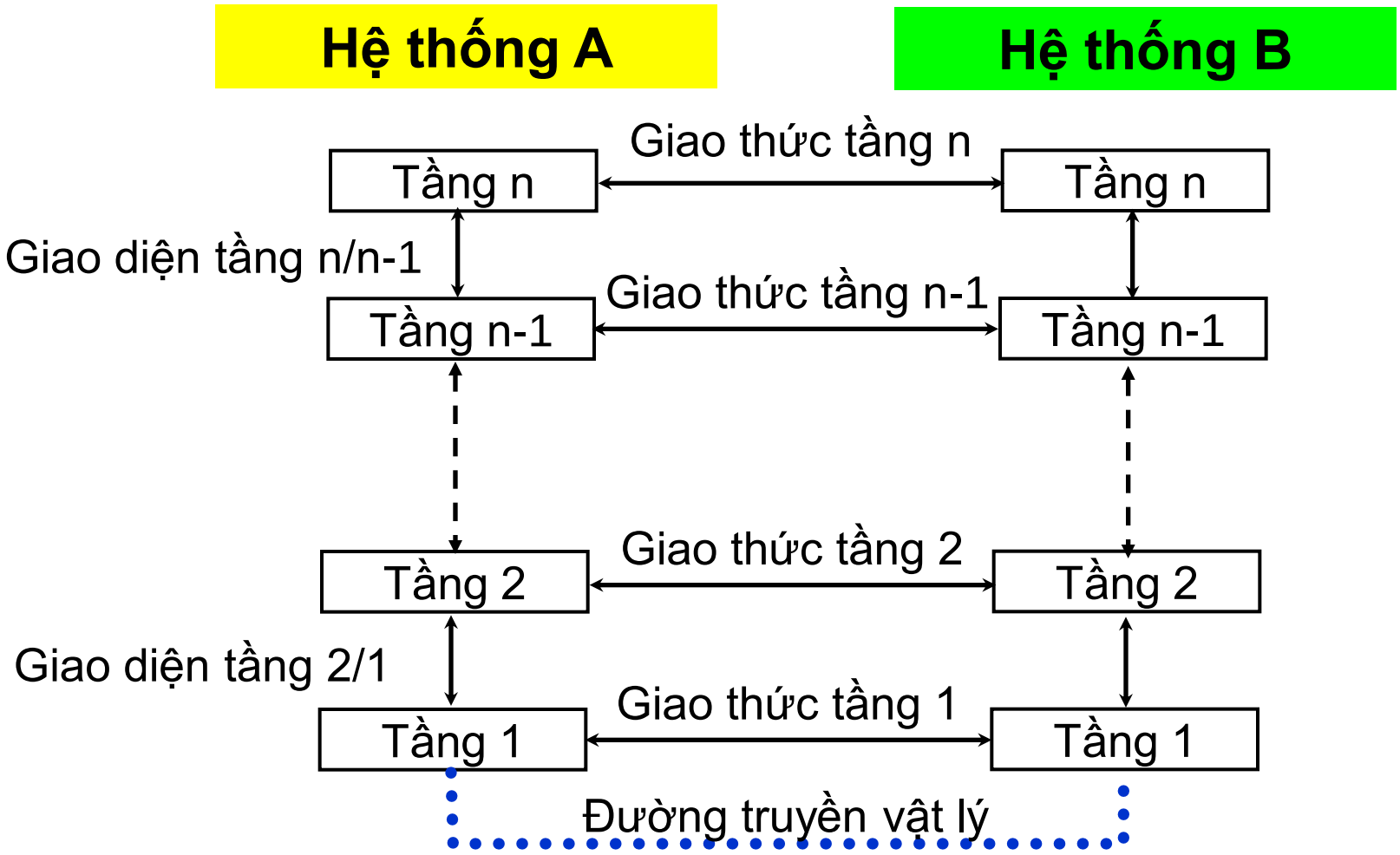
Kết hợp giữa các tầng đồng đẳng, gồm:
- Về các phương thức hoạt động trong quá trình truyền thông giữa các tầng đồng đẳng.

II.2. Quan hệ giữa các tầng

Như vậy mỗi một tầng có hai quan hệ: quan hệ theo chiều ngang và quan hệ theo chiều dọc. Số lượng các tầng và các giao thức tầng được gọi là kiến trúc mạng (Network Architecture).

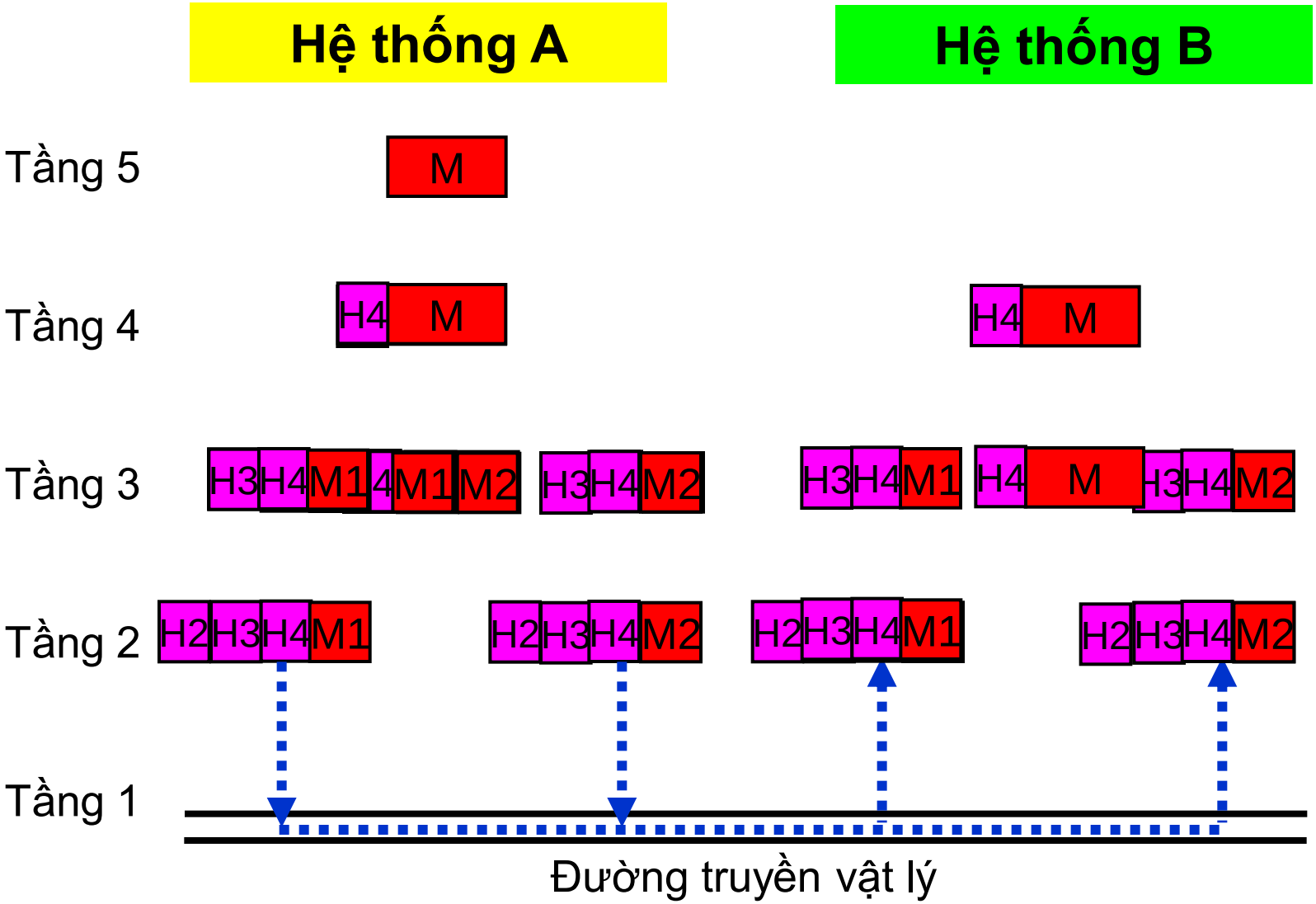
- **Quan hệ theo chiều dọc** là mối quan hệ giữa các tầng liền nhau trong cùng một hệ thống. Giữa chúng tồn tại giao diện xác định các phần tử dịch vụ mà tầng dưới cung cấp cho tầng trên. Đặc trưng của giao diện là **giao diện** bằng các tham số trao đổi (thông tin điều khiển, địa chỉ, độ dài dữ liệu, ...), được gọi là **giao thức** tầng.

Mô hình kiến trúc phân tầng

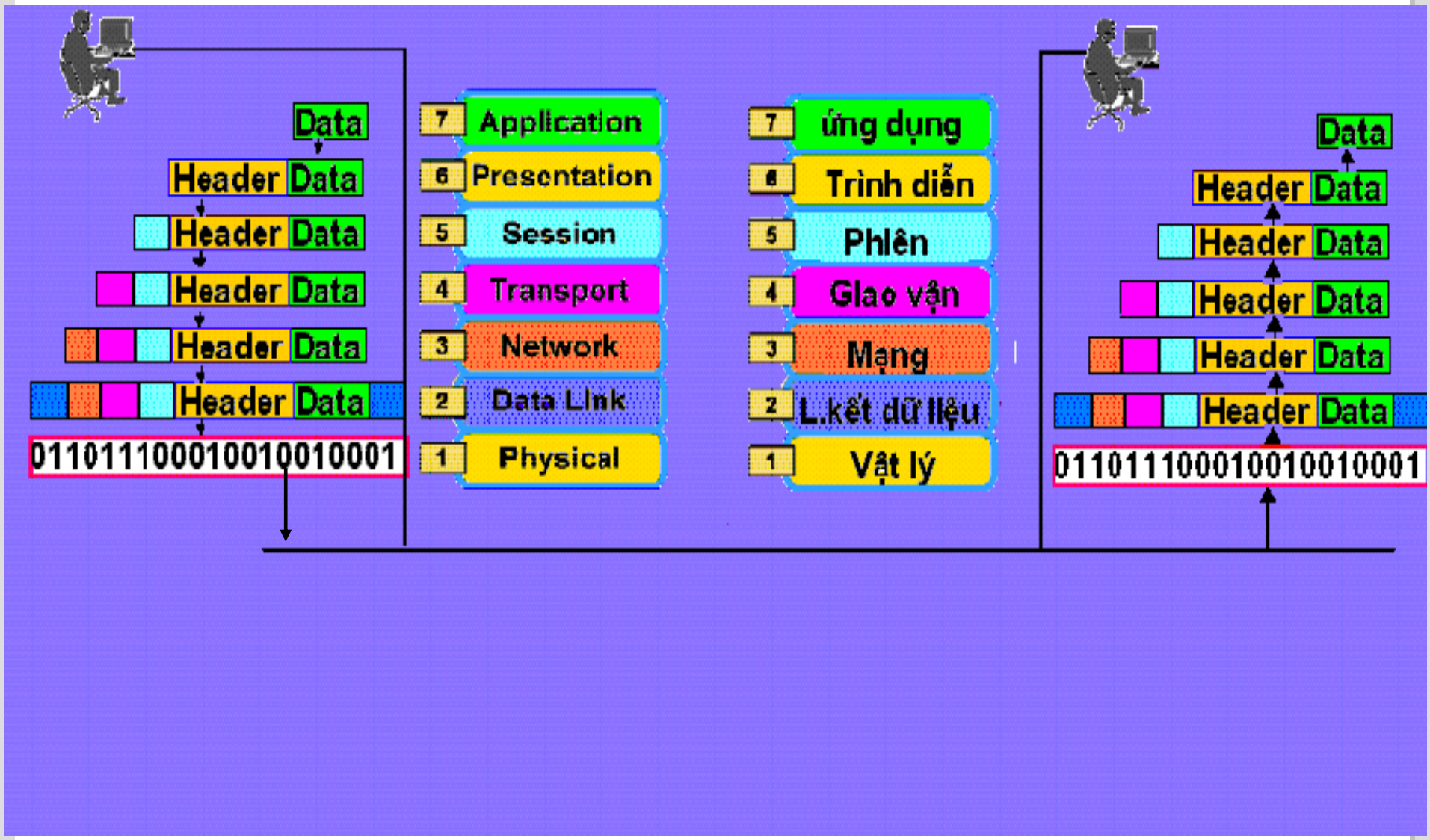


II.3. Truyền/nhận thông tin trong kiến trúc phân tầng

- Ví dụ truyền nhận trong mô hình hệ thống A và B với n=5



II.3. Truyền/nhận thông tin trong kiến trúc phân tầng



II.4. Nguyên tắc truyền thông đồng tầng

- Để truyền thông đồng tầng, gói tin khi truyền xuống các tầng sẽ được bổ sung thêm vào phần đầu bằng thông tin điều khiển của tầng.
  - Thông tin điều khiển giao thức PCI (Protocol Control Information): là thông tin được thêm vào đầu các gói tin trong quá trình hoạt động truyền thông của các thực thể. Ký hiệu N_PCI là thông tin điều khiển tầng N.
- Việc thêm Header vào đầu các gói tin khi đi qua mỗi tầng trong quá trình truyền dữ liệu được gọi là quá trình đóng gói (Encapsulation).
  - Đơn vị dữ liệu dịch vụ SDU (Service Data Unit): Là đơn vị dữ liệu truyền thông giữa các tầng kề nhau. Ký hiệu N_SDU là đơn vị dữ liệu truyền từ tầng (N+1) xuống tầng N, chưa có thông tin điều khiển.
- Quá trình bên nhận sẽ diễn ra theo chiều ngược lại, khi đi qua các tầng, gói tin sẽ tách thông tin điều khiển thuộc nó trước khi chuyển dữ liệu lên tầng trên.
  - Đơn vị dữ liệu giao thức PDU (Protocol Data Unit): Đơn vị dữ liệu giao thức tầng. Ký hiệu PDU = PCI + SDU, nghĩa là đơn vị dữ liệu giao thức bao gồm thông tin điều khiển PCI được thêm vào đầu đơn vị dữ liệu dịch vụ SDU.

II.5. Dịch vụ và chất lượng dịch vụ

- Tầng N sẽ phải biết sử dụng dịch vụ nào của tầng N-1 và cung cấp những dịch vụ gì cho tầng N+1.

- Quá trình cung cấp dịch vụ thông qua các điểm truy nhập dịch vụ (SAP) trên các giao diện tầng N/N+1.

- Có hai loại dịch vụ khác nhau:

  - Dịch vụ hướng liên kết (Connection Oriented) và

  - Dịch vụ không liên kết (Connectionless).

Dịch vụ hướng liên kết (Connection Oriented):

Các dịch vụ và giao thức trong các mô hình hệ thống mở thực hiện truyền thông 3 giai đoạn theo thứ tự thời gian như sau:

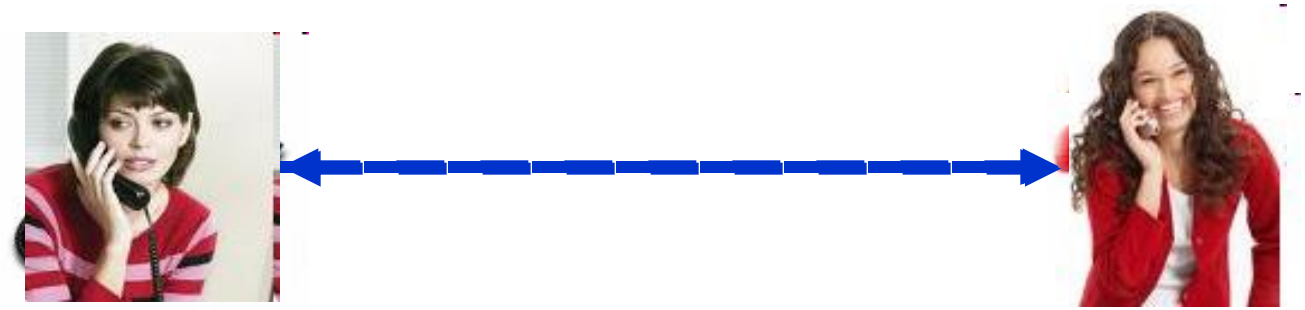
- Thiết lập liên kết
- Truyền dữ liệu
- Giải phóng liên kết

Truyền hướng liên kết trong các dịch vụ thoại.

Bên gọi

Bên nhận

Giai đoạn Thiết lập liên kết



Dịch vụ không liên kết (Connectionless)

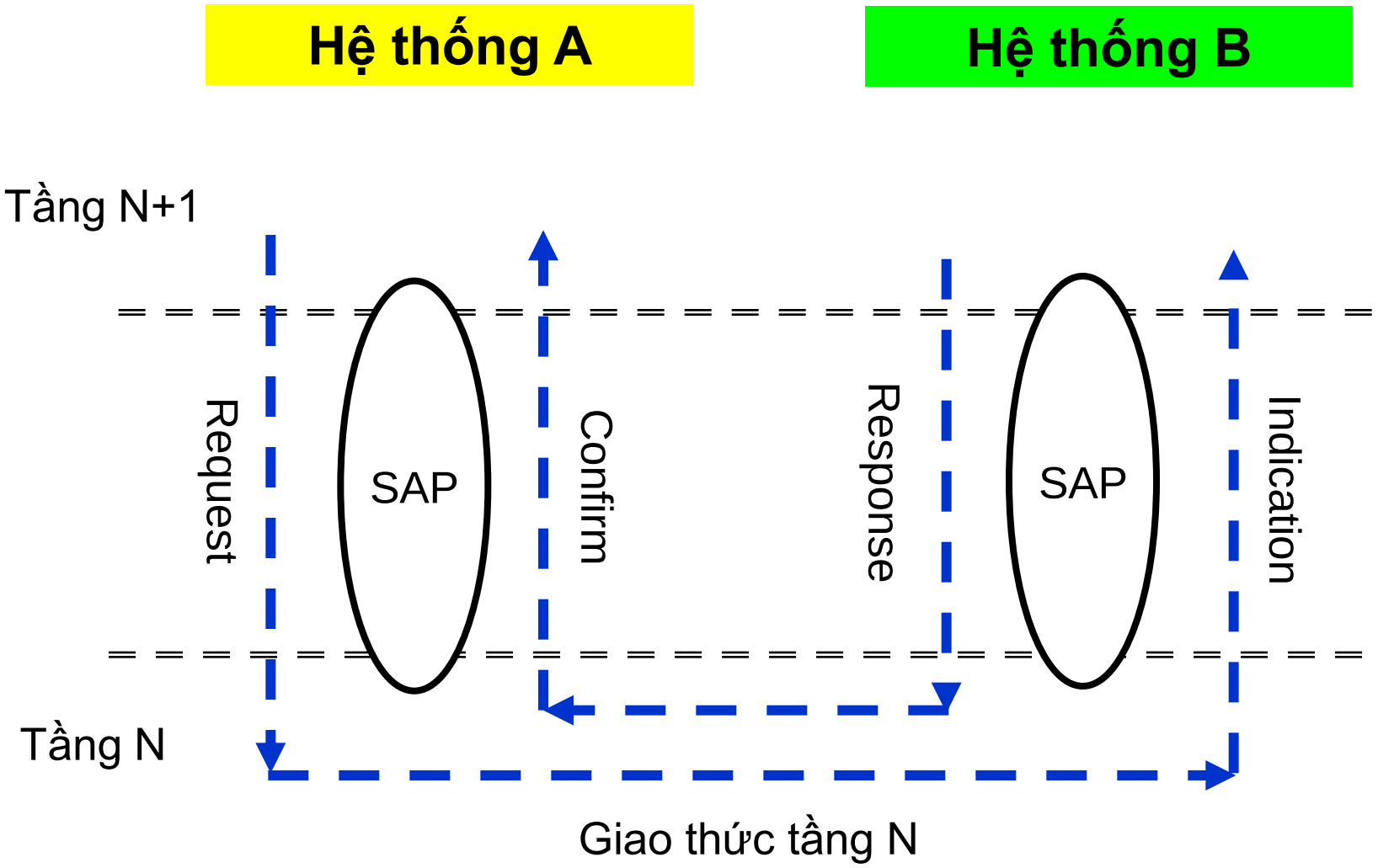
- Dịch vụ không liên kết không cần tiêu tốn thời gian để thiết lập liên kết và giải phóng liên kết giữa các thực thể đồng tầng.
  - Không yêu cầu kiểm soát luồng dữ liệu, dữ liệu được truyền với tốc độ cao độ nhưng độ tin cậy thấp.
  - Không truyền lại trong trường hợp xẩy ra lỗi đường truyền. Các dịch vụ không liên kết phù hợp với các yêu cầu truyền dung lượng không lớn, các cuộc trao đổi thông tin rải rác và độc lập.

II.6. Các hàm dịch vụ nguyên thuỷ (Primitive)

Việc cung cấp và nhận các dịch vụ giữa các thực thể trong các tầng kề nhau thông qua việc gọi các hàm dịch vụ nguyên thủy. Có bốn kiểu hàm dịch vụ nguyên thủy cơ bản:

1. Request (Yêu cầu): Được một thực thể sử dụng để gọi một chức năng, yêu cầu các phương tiện cung cấp dịch vụ mạng.
2. Indication (Chỉ báo): Được một thực thể chỉ báo yêu cầu cung cấp dịch vụ. Chỉ báo yêu cầu bằng cách:
   - Gọi một chức năng nào đó.
   - Chỉ báo một chức năng đã được gọi tại một điểm SAP.
3. Response (Trả lời): Được một thực thể sử dụng để hoàn tất một chức năng đã được gọi bởi hàm Indication tại điểm truy nhập dịch vụ.
4. Confirm (Xác nhận): Được thực thể cung cấp dịch vụ sử dụng để xác nhận hoàn tất các thủ tục đã được yêu cầu từ trước bởi hàm dịch vụ nguyên thủy Request.

Nguyên lý hoạt động của các hàm dịch vụ nguyên thuỷ

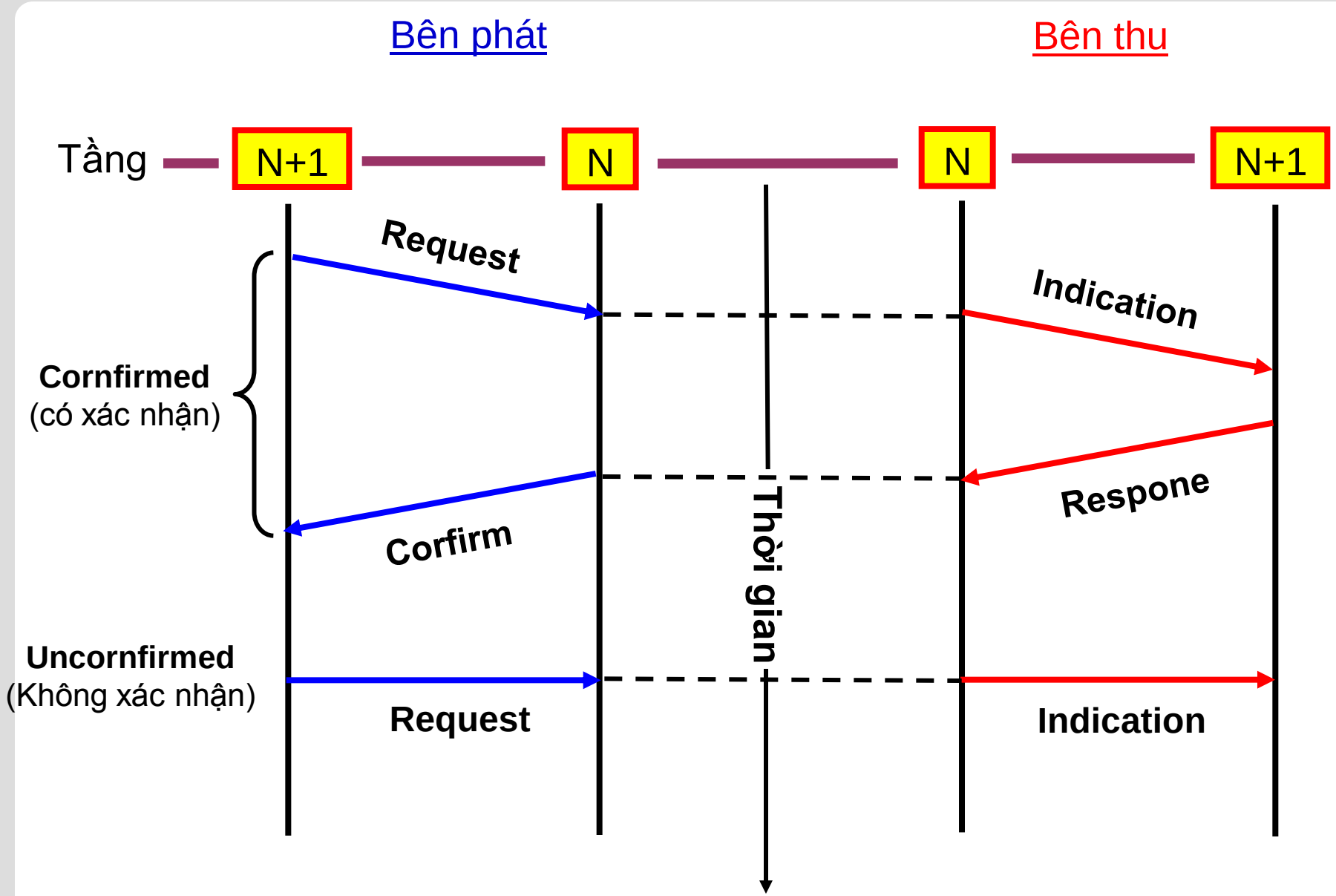


II.7. Quan hệ giữa dịch vụ và giao thức

Dịch vụ **giao thức** có hai đặc trưng: đặc trưng dịch vụ và đặc trưng giao thức.

- Một dịch vụ là một tập các các thao tác của các thực thể (thủ tục) của tầng cung cấp dịch vụ cho các hoạt động các thực thể của tầng trên kề nó. Dịch vụ tầng được định nghĩa ***trong suốt*** đối với đối tượng sử dụng dịch vụ.
- Đặc trưng dịch vụ là các tham số dịch vụ trong các hàm nguyên thủy. Thông qua các tham số dịch vụ mà các tầng ở trên có thể giao tiếp với đồng tầng trong hệ thống khác.
- Ngược lại, một giao thức là một tập các quy tắc, quy ước về kết nối, ngữ nghĩa, định dạng, ý nghĩa của khung, gói hoặc bản tin… được các thực thể đồng tầng đàm phán, thương lượng với nhau. Các thực thể sử dụng giao thức để thực hiện sự xác định các dịch vụ.
- Đặc trưng giao thức bao gồm: Khuôn dạng PDU, các tham số dịch vụ sử dụng cho mỗi một loại PDU và phương thức hoạt động của thực thể giao thức.

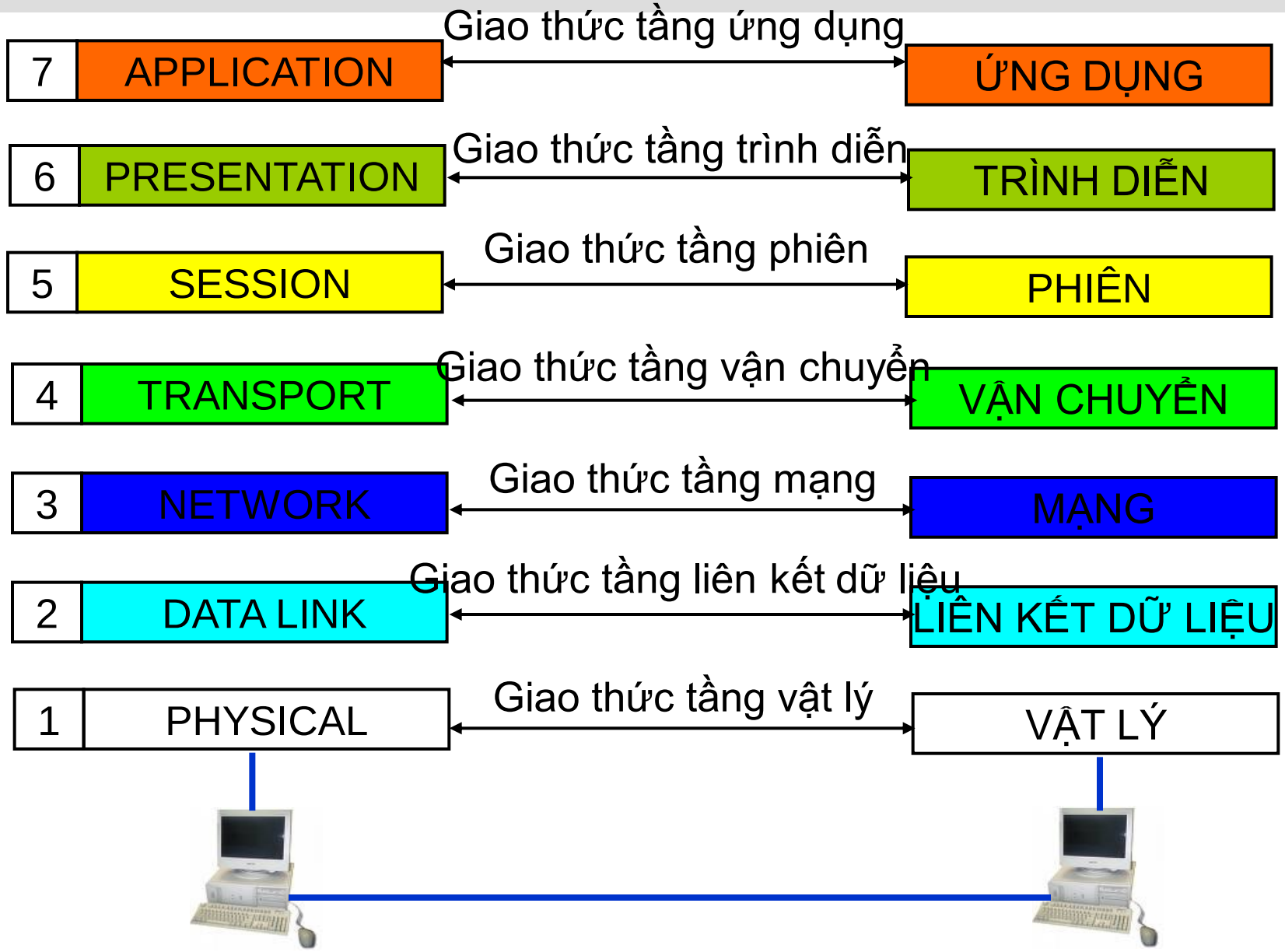
Biểu diễn thời gian các hàm dịch vụ nguyên thủy



III. Mô hình kết nối các hệ thống mở OSI

- Mô hình kết nối các hệ thống mở OSI là mô hình căn bản về các tiến trình truyền thông, thiết lập các tiêu chuẩn kiến trúc mạng ở mức Quốc tế.
- Là cơ sở chung để các hệ thống khác nhau có thể liên kết và truyền thông được với nhau.
- Mô hình OSI tổ chức các giao thức truyền thông thành 7 tầng, mỗi một tầng giải quyết một phần hẹp của tiến trình truyền thông, chia tiến trình truyền thông thành nhiều tầng và trong mỗi tầng có thể có nhiều giao thức khác nhau thực hiện các nhu cầu truyền thông cụ thể.

III.1. Các tầng hệ thống mở



III.2. Nguyên tắc định nghĩa các tầng trong OSI

Mô hình OSI tuân theo các nguyên tắc phân tầng như sau:

- Mô hình gồm N =7 tầng. OSI là hệ thống mở, phải có khả năng kết nối với các hệ thống khác nhau, tương thích với các chuẩn OSI.
- Quá trình xử lý các ứng dụng được thực hiện trong các hệ thống mở, trong khi vẫn duy trì được các hoạt động kết nối giữa các hệ thống.
- Thiết lập kênh logic nhằm thực hiện việc trao đổi thông tin giữa các thực thể.

III.3. Các giao thức trong mô hình OSI

Trong mô hình OSI có hai loại giao thức được sử dụng: giao thức hướng liên kết (Connection - Oriented) và giao thức không liên kết (Connectionless).

- **Giao thức không liên kết** Dữ liệu được truyền độc lập trên các tuyến khác nhau. Với các giao thức không liên kết thì trong giai đoạn đầu tiên ***thiết lập một liên kết logic***.

- Trước khi truyền dữ liệu, các thực thể đồng tầng trong hai hệ thống cần phải

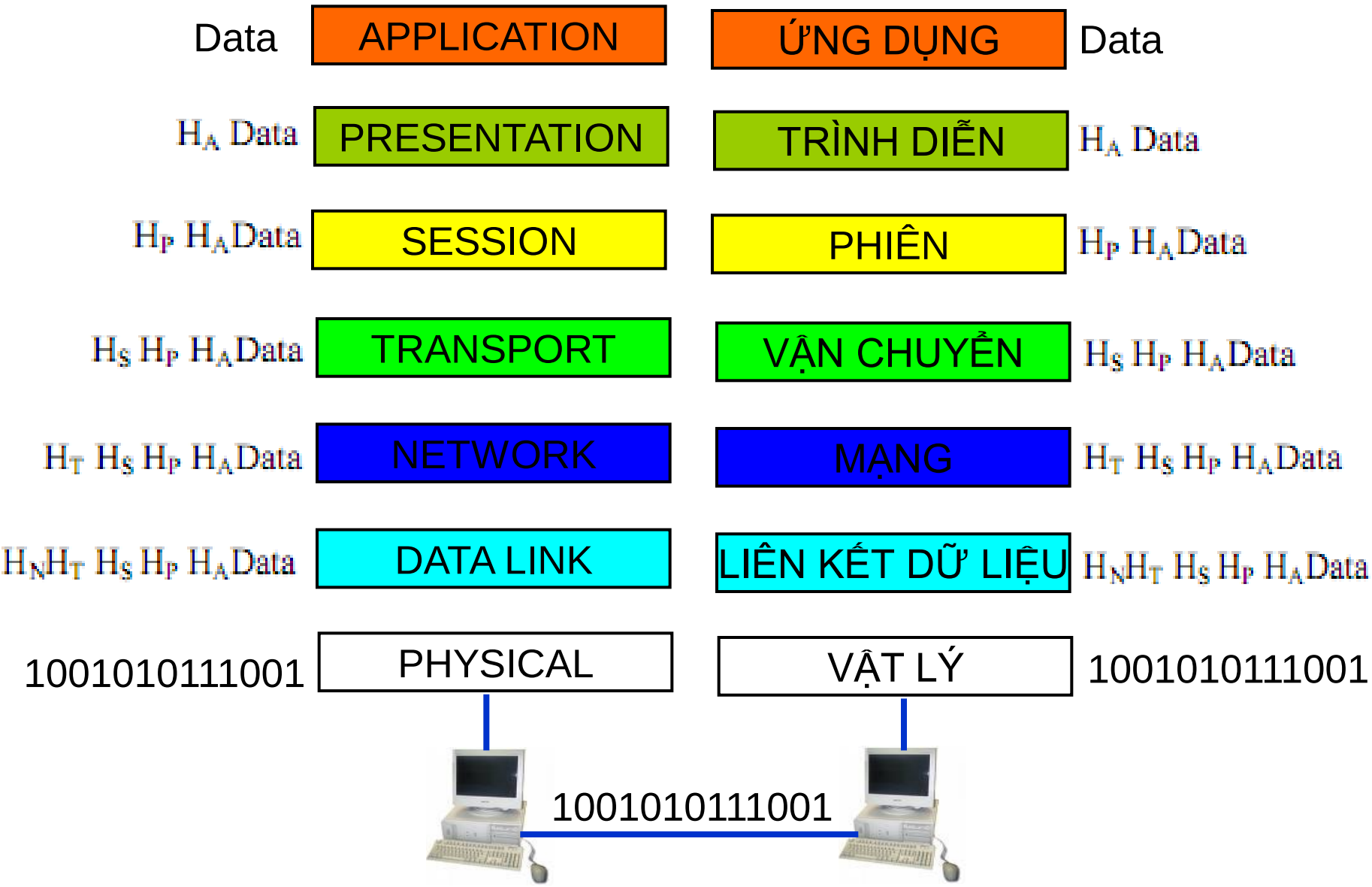
- Chúng thương lượng với nhau về tập các tham số sẽ sử dụng trong giai đoạn truyền dữ liệu.

- Dữ liệu được truyền với các cơ chế ***kiểm soát lỗi, kiểm soát luồng dữ liệu, cắt/hợp dữ liệu***, nhằm nâng cao độ tin cậy và hiệu quả của quá trình truyền dữ liệu.

- Sau khi trao đổi dữ liệu, liên kết sẽ được hủy bỏ.

Thiết lập liên kết logic sẽ ***nâng cao độ tin cậy và an toàn*** trong quá trình trao đổi dữ liệu.

III.4. Truyền dữ liệu trong mô hình OSI



III.4. Truyền dữ liệu trong mô hình OSI (tt)

Tầng	Header	Tên dữ liệu
Application	Ha	**Message** & Packet
Presentation	Hp	**Packet**
Session	Hs	**Packet**
Transport	Ht	Datagram,Segment & **Packet**
Network	Hn	**Datagram** & Packet
Data Link	Hd	**Frame** & Packet
Physical	Physical	**Bit**

III.5. Vai trò và chức năng chủ yếu các tầng

Tầng	Chức năng chủ yếu	Giao thức
7- Application	Giao tiếp người và môi trường mạng	Ứng dụng
6-Presentation	Chuyển đổi cú pháp dữ liệu để đáp ứng yêu cầu truyền thông của các ứng dụng.	Giao thức Biến đổi mã
5-Sesion	Quản lý các cuộc liên lạc giữa các thực thể bằng cách thiết lập, duy trì, đồng bộ hoá và huỷ bỏ các phiên truyền thông giữa các ứng dụng	Giao thức phiên
4-Transport	Vận chuyển thông tin giữa các máy chủ (End to End). Kiểm soát lỗi và luồng dữ liệu.	Giao thức Vận chuyển
3-Network	Thực hiện chọn đường và đảm bảo trao đổi thông tin trong liên mạng với công nghệ chuyển mạch thích hợp.	Giao thức Mạng
2-Data Link	Tạo/gỡ bỏ khung thông tin (Frames), kiểm soát luồng và kiểm soát lỗi.	Thủ tục kiểm soát
1-Physical	Đảm bảo các yêu cầu truyền/nhận các chuỗi bít qua các phương tiện vật lý.	Giao diện DTE - DCE

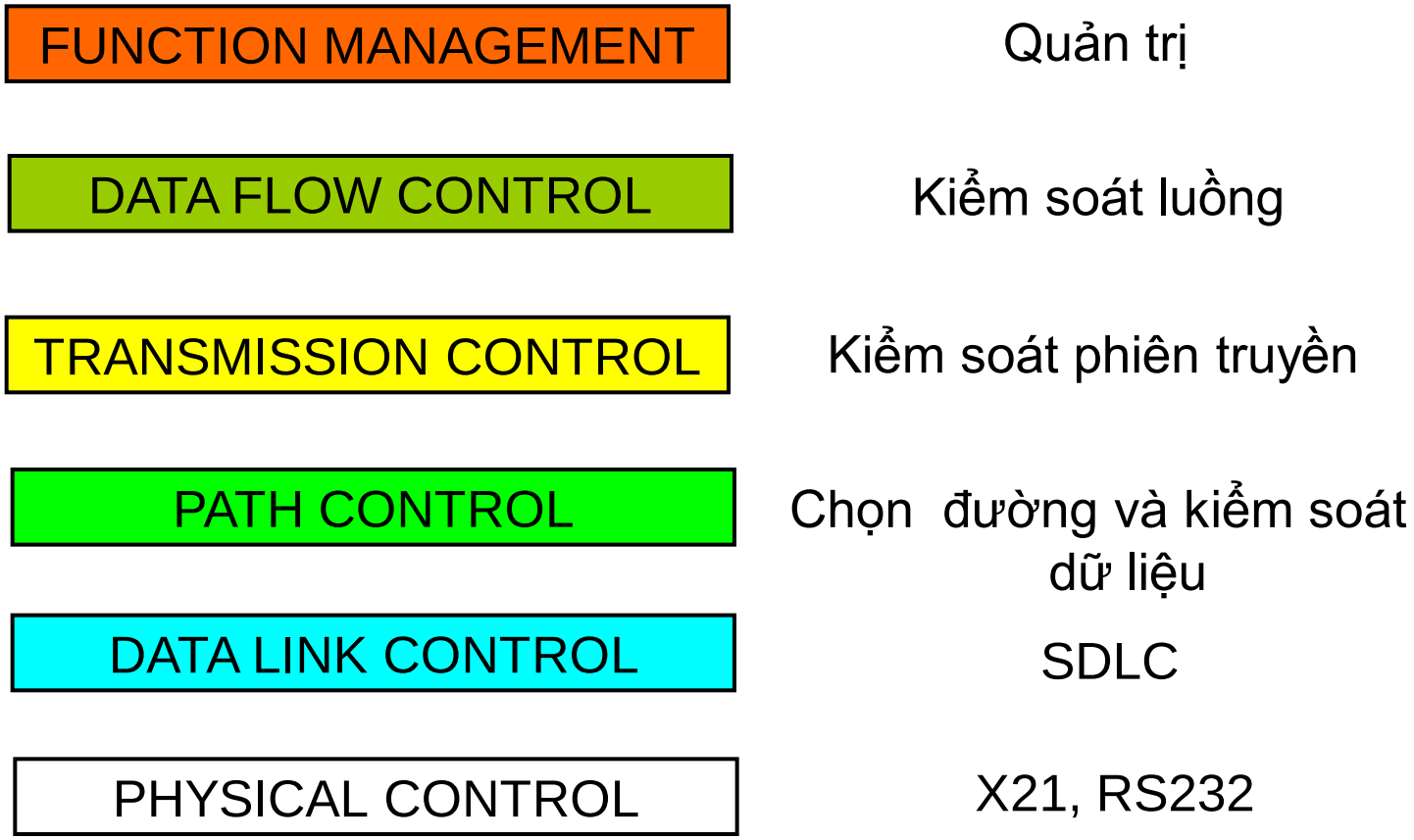
IV. Một số kiến trúc khác

1. Systems Nework Architecture (SNA)
2. Internetwork Packet Exchange/Sequenced (IPX/SPX – Sự trao đổi, sự nối tiếp)
3. AppleTalk
4. Digital Network Architecture (DNA)
5. Họ IEEE 802 (Institute of Electrical and Electronic Engineer)
6. TCP/IP (Transmission Control Protocol/Internet Protocol)
7. FDDI

IV.1. Systems Nework Architecture (SNA)

- Kiến trúc mạng SNA được công ty IBM thiết kế, đặc tả kiến trúc mạng xử lý dữ liệu phân tán.
- Chức năng của các node trong mạng: Node loại 5- kiểm soát tài nguyên mạng và các dịch vụ mạng, gọi là node Host. Node loại 4 định tuyến và điều khiển luồng dữ liệu. Node loại 2.0 và 2.1 là các loại node ngoại vi được nối với node loại 4 hoặc loại 5. Đây là node điều khiển cụm và là bộ xử lý phân tán.
- Giao thức định nghĩa các quy tắc, các tiến trình tương tác giữa các thành phần trong mạng như máy tính, terminal và phần mềm.
- Kiến trúc mạng các hệ thống đã phát triển khi các trạm cuối là những thiết bị bình thường được dùng để tương tác với các máy tính tập trung.
- Các mạng trạm cuối SNA được tổ chức theo hệ phân cấp và khi xuất hiện vào năm 1974, SNA chỉ hỗ trợ các mạng phân cấp.
- Hệ phân cấp gồm một điểm điều khiển trung tâm (máy chủ), các hệ điều khiển (trung tâm và cụm), các trạm cuối.

IV.1. Systems Nework Architecture (SNA)



IV.1. Systems Nework Architecture (SNA)

- Các giao thức SNA chính:
  - Token Ring
  - Synchronous Data Link Control (SDLC-Điều khiển liên kết DL đồng bộ)
  - Network Control Program (NCP-Chương trình điều khiển mạng)
  - Virtual Telecommunications Access Methol (VTAM-Phương thức truy cập viễn thông ảo)
  - Advanced Peer-to-Peer Networking (APPN-Mạng ngang hàng cao cấp)
  - Customer Information Control System (CICS-Hệ điều khiển thông tin khách hàng)
  - Information Management System (IMS-hệ thống quản trị thông tin)
  - Advanced Program-to-Program Communication (APPC-Truyền thông liên chương trình cao cấp)
  - Distributed Data Management (DDM- Quản trị dữ liệu phân tán)
  - SNA Distributed Services (SNADS-Các dịch vụ phân tán SNA)
  - Document Interchange Architecture (DIA-Kiến trúc hoán đổi tài liệu)
- SAA (Systems Application Architecture-kiến trúc ứng dụng các hệ thống) là một đợt chỉnh lý tiếp theo của SNA, được công bố vào năm 1987 và là đại diện cho hướng chiến lược của IBM.

IV.2. IPX/SPX

IPX/SPX: Internetwork Packet Exchange/Sequenced Packet Exchange

- Giao thức IPX/SPX được công ty Novell thiết kế sử dụng cho các sản phẩm mạng của chính hãng.
- IPX hoạt động ở tầng 3 trong mô hình OSI, là giao thức định tuyến, có chức năng tương tự như giao thức IP. Nó có thể sử dụng một trong hai giao thức định tuyến kết hợp với nó là RIP hoặc NLSP. Nếu không có yêu cầu đặc biệt thì nên sử dụng NLSP. Giao thức định tuyến NLSP là giao thức định tuyến trạng thái liên kết được phát triển bởi Novell. Nó sử dụng thuật toán Dijkstra để tính đường đi ngắn nhất. Nó có thể thiết lập các liên kết tuyến thông minh và chỉ trao đổi thông tin định tuyến khi có thay đổi trong mạng. Nó cũng hỗ trợ cân bằng tải và dự phòng. Routing Information Protocol (RIP) là giao thức định tuyến vector khoảng cách, sử dụng số bước nhảy (hop count) làm thước đo để tính toán đường đi. NetWare Link Services Protocol (NLSP) để trao đổi thông tin định tuyến với các bộ định tuyến lân cận.

IV.3. AppleTalk

- AppleTalk là một giao thức mạng được hãng Apple Computer ...

- Địa chỉ động dựa trên các giao thức truy nhập : Phase 1: Node ID; Phase 2: Network+Node ID; Phase 1&2: LocalTalk , Phase 1: Ethernet; Phase 2: IEEE 802.2, IEEE 802.5.

... chỉ được xác định bởi tổ hợp mạng và ID nút. Ngoài ra nó ...

... hoá trong các card mạng Ethernet và Token Ring.

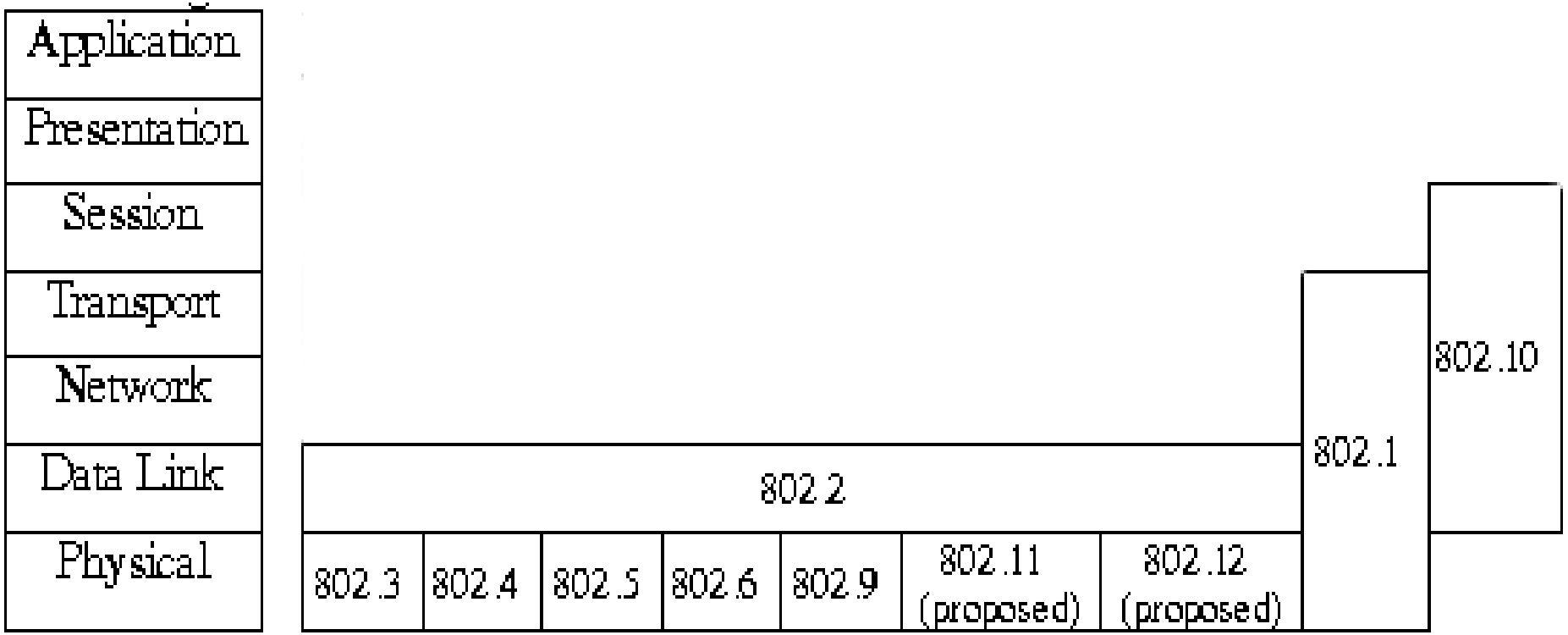
- Ban đầu, AppleTalk hỗ trợ các mạng có phạm vi nhỏ. Tuy nhiên, chuẩn AppleTalk Phase 2 phát hành năm 1989 đã mở rộng phạm vi hoạt động của AppleTalk ra các mạng xí nghiệp. Chuẩn Phase 2 còn cho phép AppleTalk cùng tồn tại trên các mạng có các bộ giao thức khác nhau.

IV.4. Digital Network Architecture (DNA)

- Trước thời DNA Phase V, DNA phần lớn là sản phẩm của hãng Digital Equipment Corporation. Bộ giao thức riêng của Digital bên trên tầng mạng (Network layer) là Ngăn xếp phát triển của Digital và các giao thức khác, vẫn được hỗ trợ để tương thích về trước. Các giao thức trước Phase V khác cũng được hỗ trợ tại cấp mạng thấp hơn.
- Kiến trúc mạng số hoá DNA đã được cải tiến nhiều đợt.
- DNA Phase V cũng đã đưa ra một ngăn giao thức thay thế dựa trên các chuẩn ISO.
- Thế hệ hiện nay của DNA Phase V, DECnet là họ sản phẩm thực thi kiến trúc DNA. Với đà phát triển của DNA, hãng Digital đã cổ vũ việc sử dụng các giao thức gốc các chuẩn và việc tuân thủ chặt chẽ mô hình OSI. Nhiều chuẩn OSI đã được kết hợp với bộ giao thức DNA.

IV.5. Họ IEEE 802

Là chuẩn cho kiến trúc các mạng LAN, WAN và MAN:

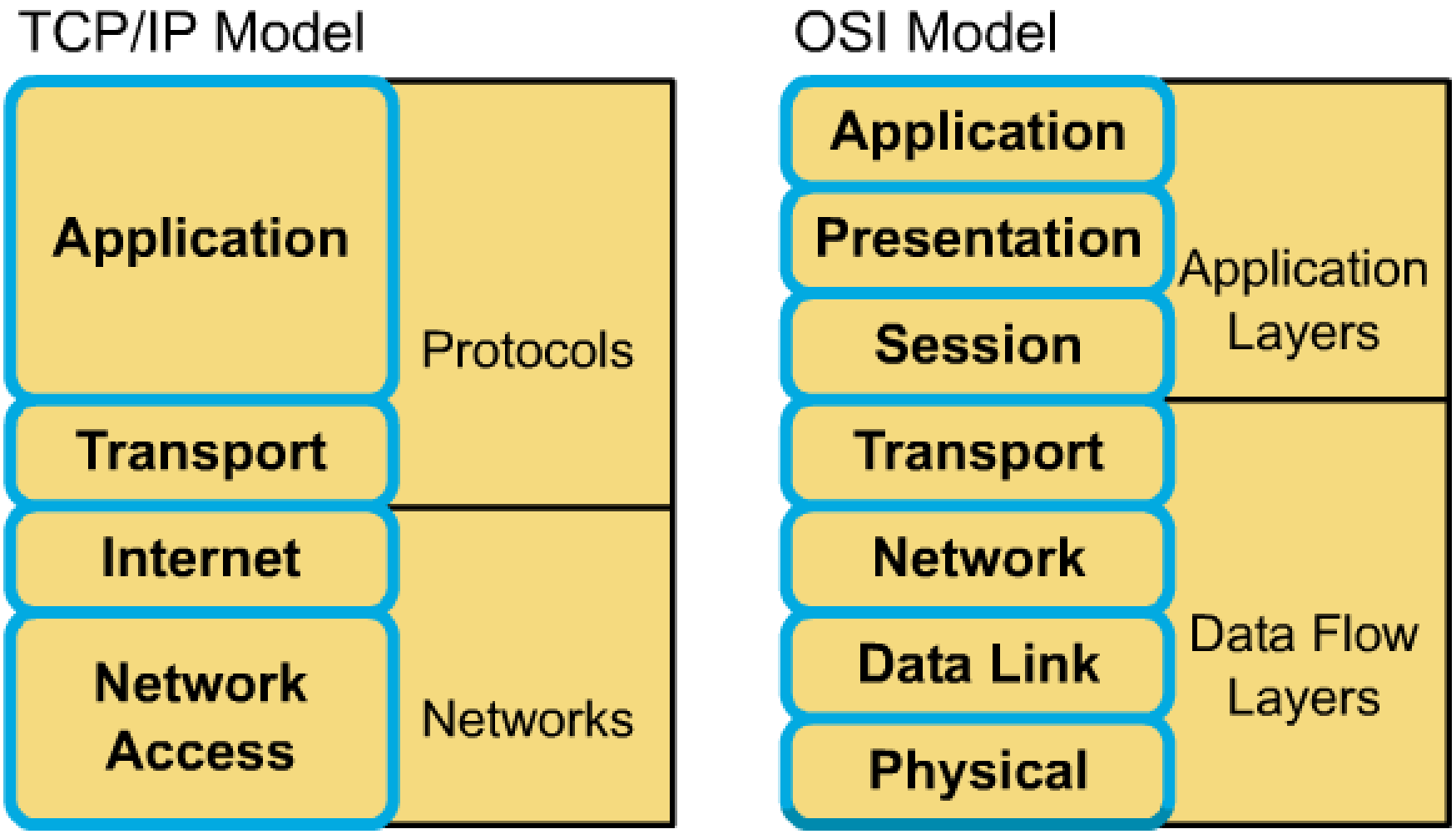


III.6. TCP/IP

- Là họ các giao thức cùng làm việc với nhau để cung cấp phương tiện truyền thông liên mạng.
- Vì lịch sử của TCP/IP gắn liền với Bộ quốc phòng Mỹ, nên việc phân lớp giao thức TCP/IP được gọi là mô hình DOD (Department of Defense).
- Đây là họ các giao thức được sử dụng phổ biến trên mạng Internet, mạng tính mở nhất , phổ dụng nhất và được hỗ trợ của nhiều hãng kinh doanh.
- TCP/IP được cài đặt sẵn trong phần thực thi UNIX BSD (Berkely Standard Distribution).

Mô hình DOD gồm 4 tầng:
- Network Access Layer (truy nhập mạng) tương ứng Physical Layer & Data Link Layer trong OSI.
- Internetwork Layer: Định tuyến gói dữ liệu giữa các máy chủ.
- Host to Host Layer: Kết nối các thành phần mạng.
- Application Layer: Hỗ trợ các ứng dụng.

III.6. TCP/IP


TCP/IP Model
Application
Transport
Internet
Network Access
Protocols
Networks
OSI Model
Application
Presentation
Session
Transport
Network
Data Link
Physical
Application Layers
Data Flow Layers

III.7. FDDI

- FDDI bao gồm tầng vật lý và tầng MAC của mô hình OSI. Thông thường, chuẩn IEEE 802.2 được dùng cho tầng con LLC.
- FDDI là một mạng LAN (Local Area Network) tương tự Token Ring và dựa trên cơ chế điều khiển truy cập truyền thẻ bài (token passing) và một topo hình vòng.
- Đầu tiên, được phát triển cho cáp sợi quang, chuẩn này đã được mở rộng để có thể sử dụng với cáp UTP. Dùng cáp quang cho phép FDDI hỗ trợ các mạng vật lý lớn.
- Giao tiếp dữ liệu phân tán sử dụng sợi quang (Fiber Distributed Data Interface-FDDI) là một chuẩn dành cho các mạng sợi quang, được phát triển bởi Ủy ban X3T9.5 của ANSI (American National Standards Institute-Viện các tiêu chuẩn quốc gia Mỹ).
- ISO đã chấp thuận FDDI như là chuẩn. FDDI được phát triển cho các WAN, nhưng nó cũng được dùng trong các MAN và LAN.

V. Kết luận chương

1. Khái niệm kiến trúc đa tầng và các quy tắc phân tầng
2. Quan hệ ngang và quan hệ dọc trong kiến trúc N tầng.
3. Các nguyên tắc truyền thông đồng tầng
4. Giao diện tầng, quan hệ các tầng kề nhau và dịch vụ
5. Dịch vụ và chất lượng dịch vụ
6. Khái niệm dịch vụ và dịch vụ liên kết, dịch vụ không liên kết
7. Các kiểu hàm dịch vụ nguyên thủy cơ bản.
8. Quá trình yêu cầu thiết lập liên kết của các thực thể đồng
9. Quan hệ giữa dịch vụ và giao thức
10. Các tham số dịch vụ và tương tác giữa các tầng
11. Trạng thái hoạt động các hàm dịch vụ trong mô hình OSI
12. Vai trò và chức năng chủ yếu các tầng phiên (Session Layer)
13. Vai trò & chức năng tầng vận chuyển (Transport Layer)
14. Vai trò & chức năng tầng mạng (Network Layer)
15. Vai trò & chức năng tầng liên kết dữ liệu (Data link Layer)
16. Hiểu thế nào là thực thể tầng vật lý và dịch vụ tầng vật lý.
17. Giao thức tầng vật lý khác với giao thức các tầng khác như thế nào?

Thanksss

Chương 3

MẠNG CỤC BỘ VÀ MẠNG DIỆN RỘNG

Nội dung chương 3

I. Mạng cục bộ
   1. Giới thiệu chung
   2. Các hình trạng và mô hình mạng cục bộ
   3. Các phương thức truyền tín hiệu và truy nhập đường truyền
   4. Các loại mạng cục bộ và các hệ điều hành mạng
   5. Thiết bị mạng

II. Mạng diện rộng
   1. Khái niệm
   2. Đặc trưng mạng diện rộng
   3. Các lợi ích và chi phí khi kết nối WAN
   4. Một số công nghệ kết nối WAN cơ bản

Mạng cục bộ

1.1. Giới thiệu chung

- **Khái niệm LAN:** **LAN** (Local Area Network) là một hệ thống mạng dùng để kết nối các máy tính trong một phạm vi nhỏ (nhà ở, phòng làm việc, trường học, công ty...)
- Mở rộng của LAN là **WAN** (Wide Area Network). Có nghĩa là mạng diện rộng. Dùng để nối các LAN lại với nhau (thông qua router). Một hình thức khác nữa của mạng LAN, mới xuất hiện trong những năm gần đây là **WLAN** (Wireless LAN).
- **Đặc điểm:** Một mạng LAN thường cần có máy chủ (*server*-máy phục vụ), các thiết bị ghép nối (*Repeater*, *Hub*, *Switch*, *Bridge*), máy tính con (*client*-máy khách), card mạng (*Network Interface Card–NIC*), phương tiện truyền (môi trường) để kết nối các máy tính lại với nhau và tài nguyên dùng chung.
- Tốc độ mạng LAN: có thể lên đến 10 Mbps, 100 Mbps hay thậm chí là 1 Gbps (phụ thuộc vào băng thông và kỹ thuật của thiết bị mạng).
- Các máy tính trong mạng LAN có thể chia sẻ tài nguyên với nhau.
- Thường thuộc sở hữu của một tổ chức.

1.2. Các hình trạng mạng (Topology)

- Hình trạng của mạng cục bộ thể hiện qua cấu trúc hay hình dáng hình học của 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.
- Có 2 phương thức kết nối mạng chính (topo mạng): point to point (điểm-điểm), point to multipoint (điểm-đa điểm) hay broadcast (quảng bá).
- Tùy theo cấu trúc của mỗi mạng mà 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.

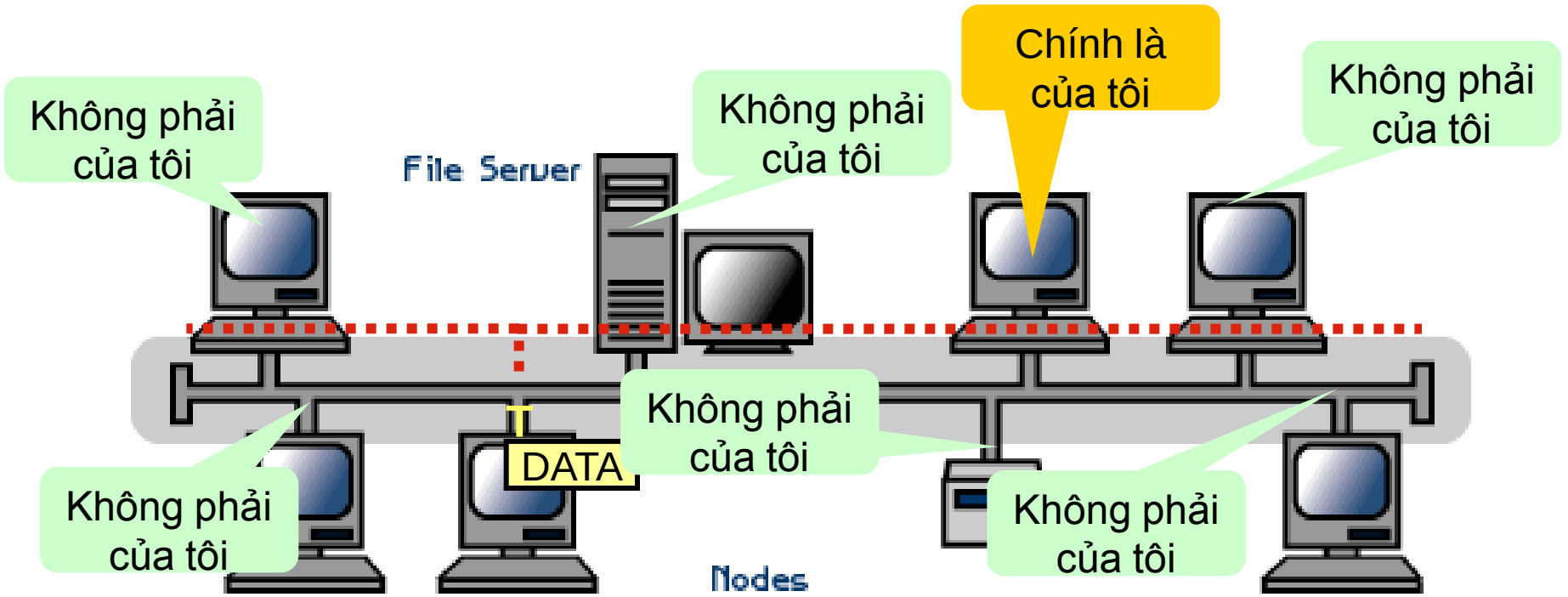
Có 3 loại hình trạng mạng cơ bản

- Dạng đường thẳng (Bus)
- Dạng vòng tròn (Ring)
- Dạng hình sao (star)

1.2.1. Dạng đường thẳng (Bus)

- Các máy tính đều được nối vào một đường truyền chính.
- Giới hạn hai đầu bởi một loại đầu nối đặc biệt gọi là *terminator.*
- Mỗi trạm được nối vào bus qua một đầu nối chữ T (T_connector) hoặc một bộ thu phát (transceiver).
- Tín hiệu được truyền trên cả hai chiều của đường truyền theo từng gói một, mỗi gói đều phải mang địa chỉ trạm đích.

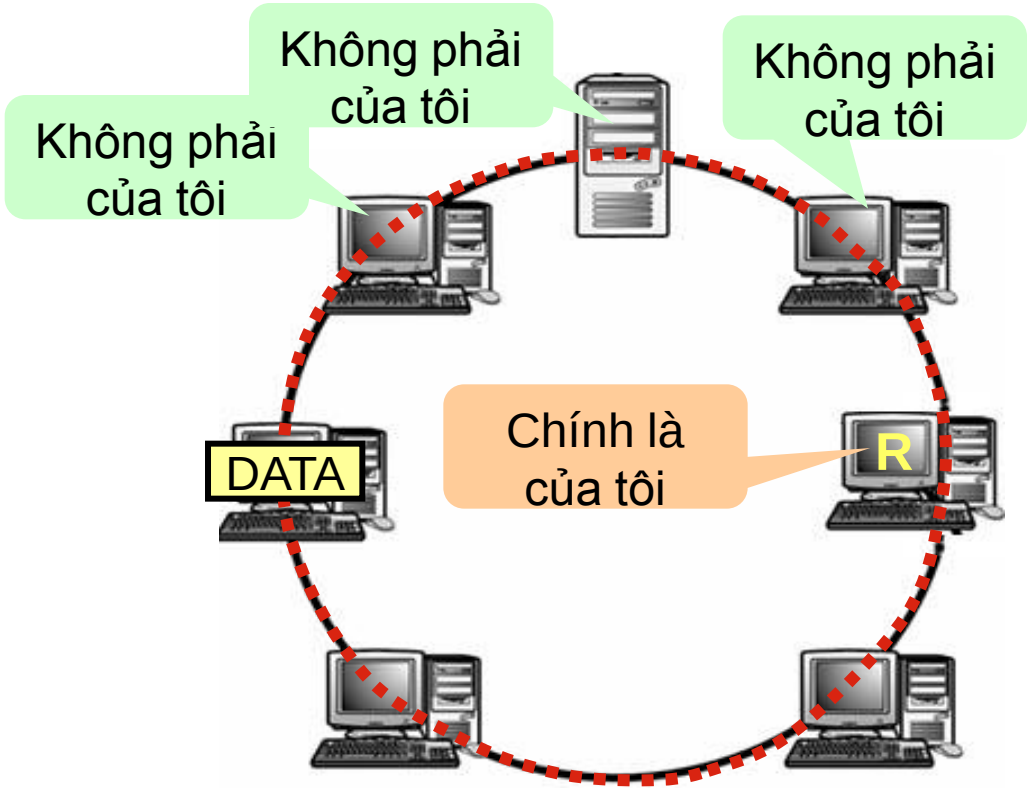
Mô tả quá trình truyền dữ liệu trên Bus



1.2.2. Dạng vòng tròn (Ring)

- Các máy tính được liên kết với nhau thành một vòng tròn theo phương thức "điểm - điểm“.
- Mỗi trạm của mạng được nối với vòng qua một bộ chuyển tiếp (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.
- Mỗi 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 sẽ 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.

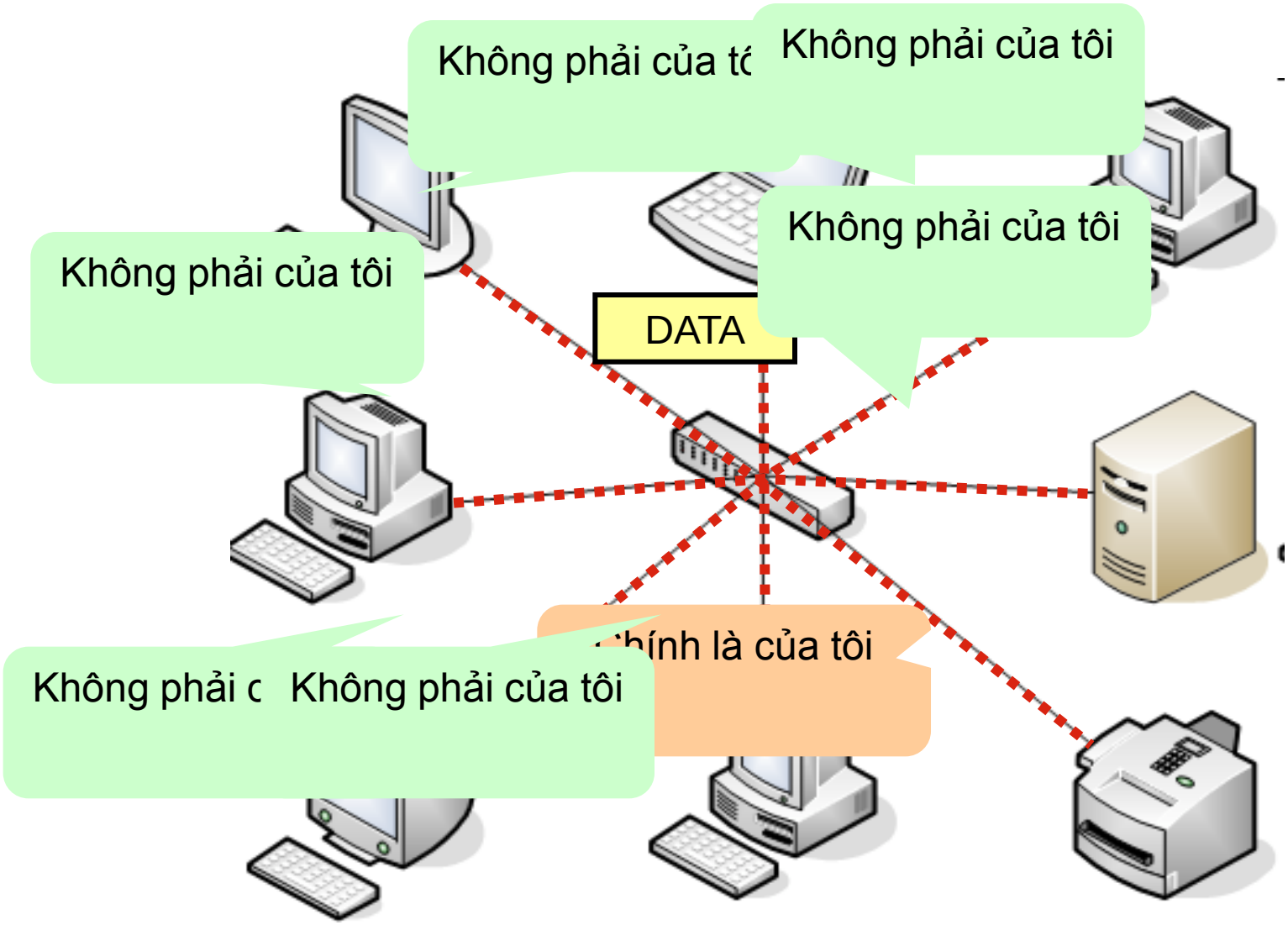
Mô tả quá trình truyền dữ liệu trên Ring



1.2.3. Dạng hình sao (star)

- Tất cả các trạm được nối vào một thiết bị trung tâm (Hub, Switch, Router).
- 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 "điểm - điểm".
- Ưu điểm là không đụng độ hay tắc nghẽn đường truyền, lắp đặt đơn giản, dễ dàng thêm, bớt trạm. Nếu có trục trặc trên một trạm thì cũng không gây ảnh hưởng đến toàn mạng, dễ kiểm soát và khắc phục sự cố.
- Độ dài cáp nối một trạm với thiết bị trung tâm bị hạn chế (< 100m) tốn nhiều dây cáp, tốc độ truyền dữ liệu không cao.

Mô tả quá trình truyền dữ liệu trên Star



1.3. Mô hình mạng cục bộ

Mạng cục bộ có 2 mô hình:

- ✓Mạng ngang hàng (Peer to Peer)
- ✓Mạng khách/phục vụ (Client/Server)

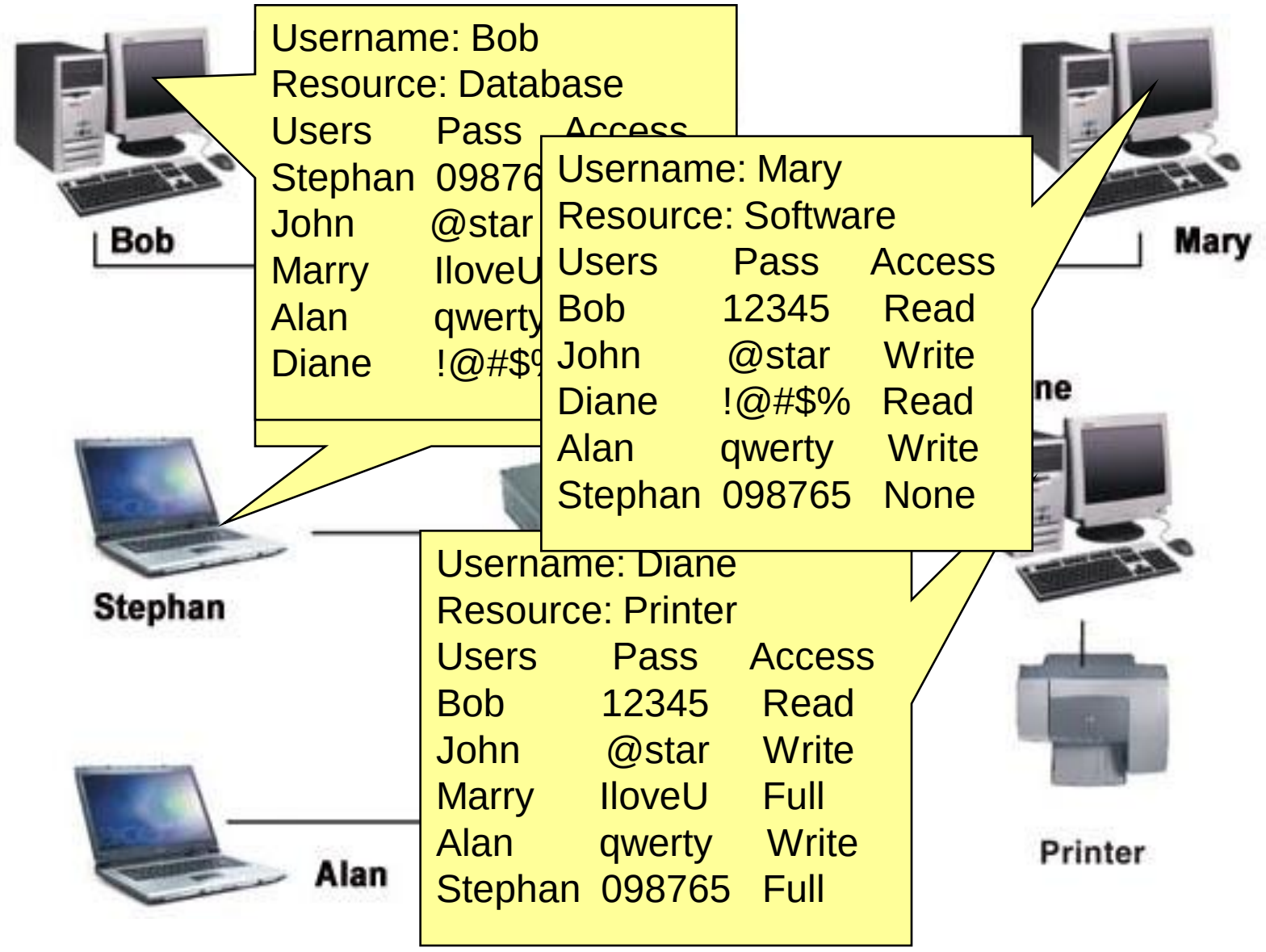
1.3.1. Mạng ngang hàng (Peer to Peer)

- **Các vấn đề quan tâm**
  - Người dùng cần được đào tạo.
  - Người dùng tự quản lý máy tính của mình.
  - Được xây dựng trên nhiều hệ điều hành.
  - Người dùng có thể chia sẻ tài nguyên như tập tin, máy in.
  - Chi phí thấp (phần mềm, phần cứng, đào tạo).

Người dùng cần được đào tạo.
Người dùng tự quản lý máy tính của mình.
Được xây dựng trên nhiều hệ điều hành.
Người dùng có thể chia sẻ tài nguyên như tập tin, máy in.
Chi phí thấp (phần mềm, phần cứng, đào tạo).

- Người dùng cần được đào tạo.
- Người dùng tự quản lý máy tính của mình.
- Được xây dựng trên nhiều hệ điều hành.
- Người dùng có thể chia sẻ tài nguyên như tập tin, máy in.
- Chi phí thấp (phần mềm, phần cứng, đào tạo).

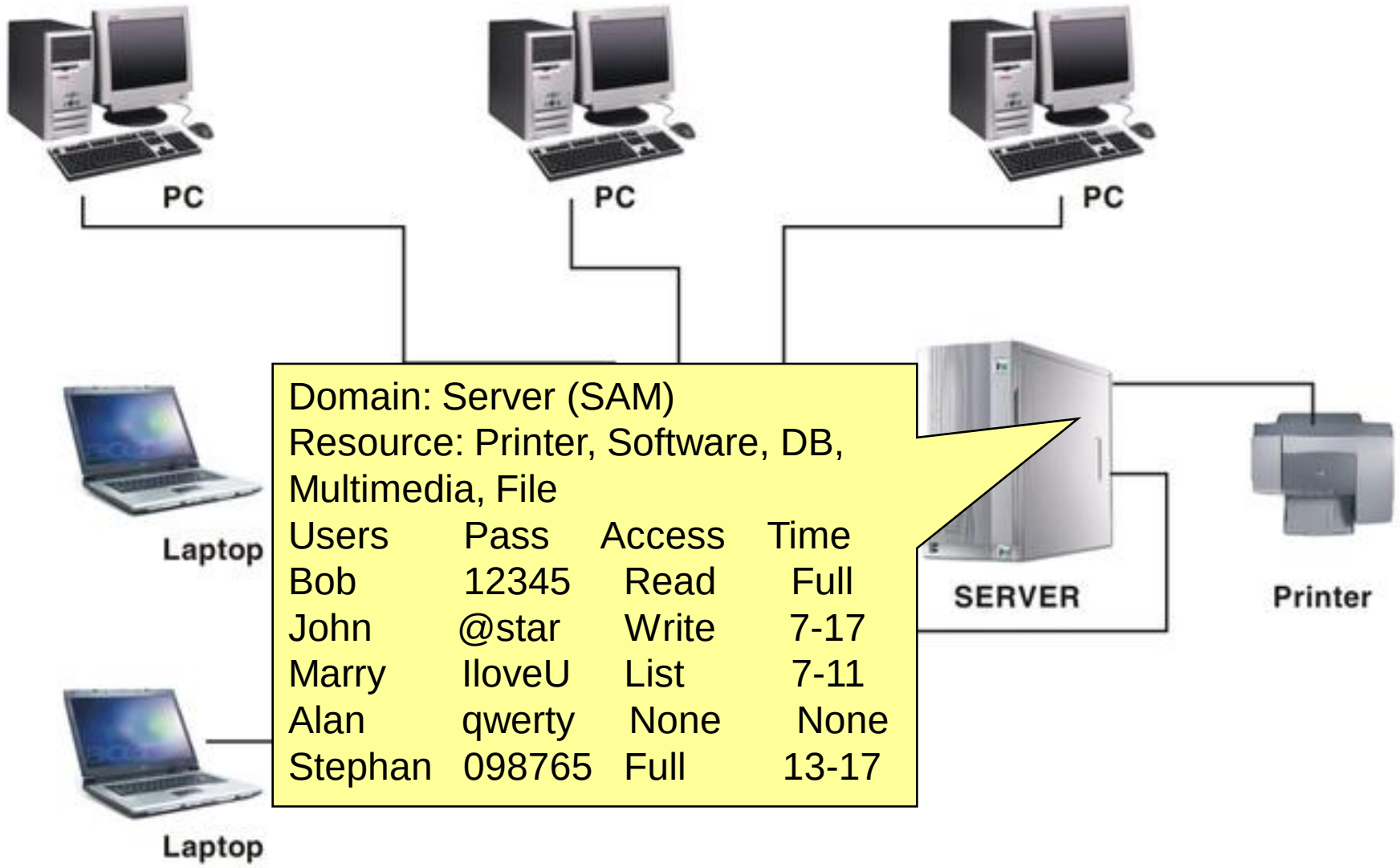
Minh họa mạng ngang hàng



1.3.2. Mạng khách/phục vụ (Client/Server)

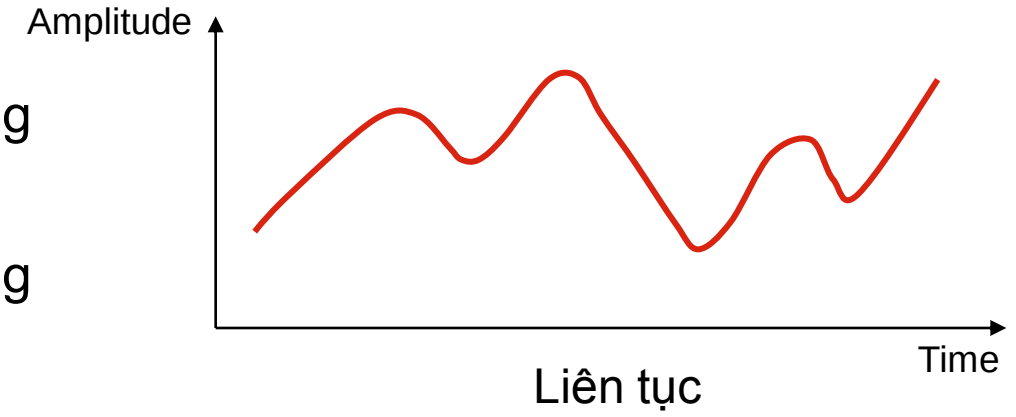
- **Các thuật ngữ liên quan đến máy chủ**
  - Tập trung.
  - Hệ thống mạng được tổ chức chặt chẽ, tuân theo chuẩn quy tắc nhất định.
  - Giới hạn mạng chủ yếu do cơ sở hạ tầng mạng.
  - Chi phí cao (Thiết bị, phần mềm, nhân sự).
  - Tập trung kinh nghiệm của người quản trị mạng: an toàn mạng, sao lưu, dự phòng, …
  - Có khả năng mở rộng của các hệ thống máy chủ.
  - Application Server
  - Mail Server
  - Database Server

Minh họa mạng khách/phục vụ

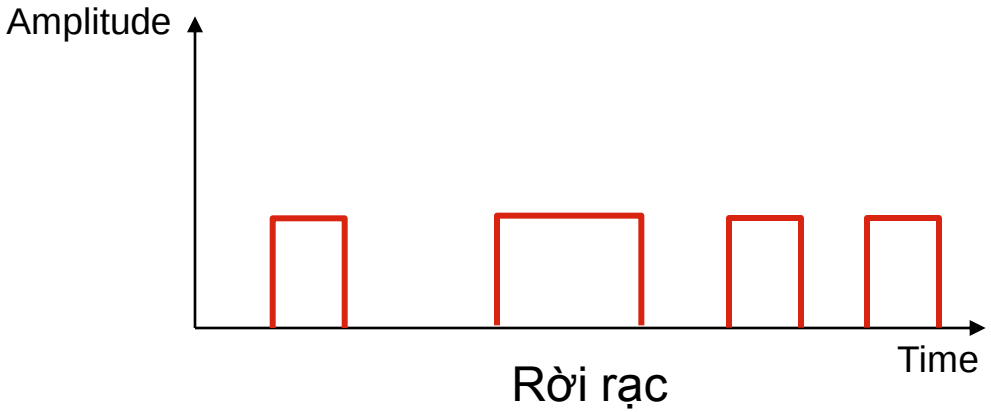


1.4. Các kỹ thuật truyền tín hiệu

- **Kỹ thuật truyền tương tự**
  - Mã hóa các bit như dạng sóng
  - Sử dụng trong hệ thống telephone/modem
  - Radio (wireless LAN)
  - Kênh vệ tinh



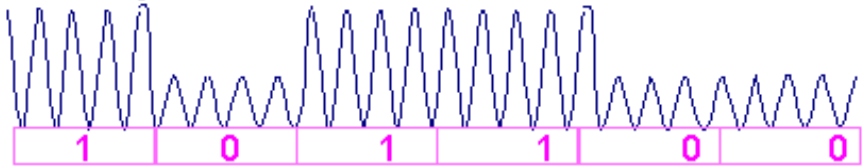
- **Kỹ thuật truyền số**
  - Mã hóa các bit như dạng xung



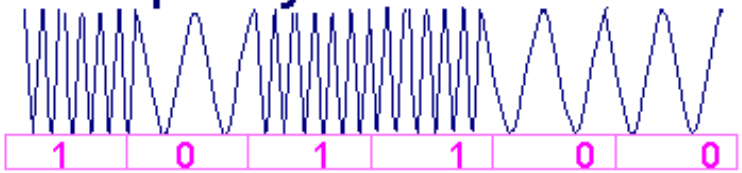
1.4.1. Kỹ thuật truyền tương tự

Analog Transmission

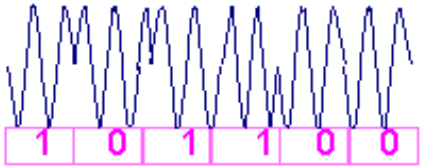
- Key considerations: noise + clock synchronization
- Amplitude modulation: encode bits in amplitude



- Frequency modulation: encode bits in frequency



- Phase modulation: encode bits in phase changes



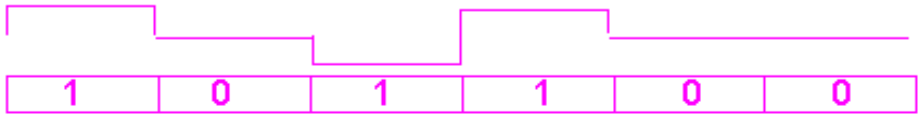
1.4.2. Kỹ thuật truyền số

Digital Transmission

- **NRZ-L (non-return-to-zero-level)**

1 = high (positive) level
0 = low (negative) level

- **Bipolar-AMI (alternate mark inversion)**



1 = alternate positive/negative
0 = zero level (no signal)

- **Manchester**

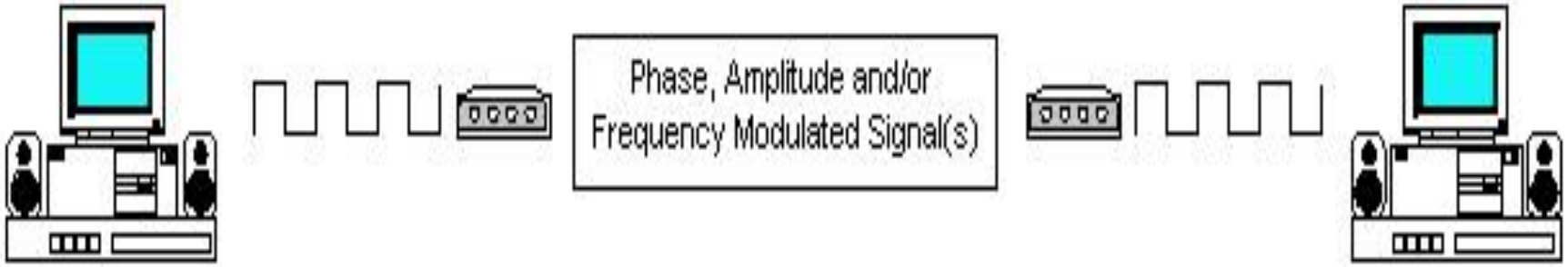
1 = low ->high transition
0 = high ->low transition

- **Differential Manchester**

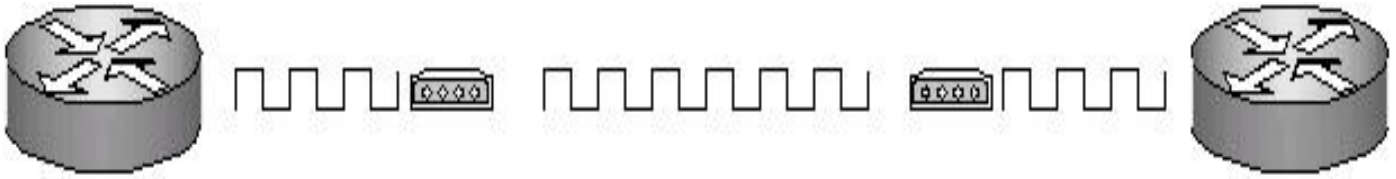
Transition in every interval
1 =no transition at interval beginning
0 =transition at interval begining

Chuyển đổi tín hiệu

- **MODEM (MO**dulate and **DEM**odulate**)**



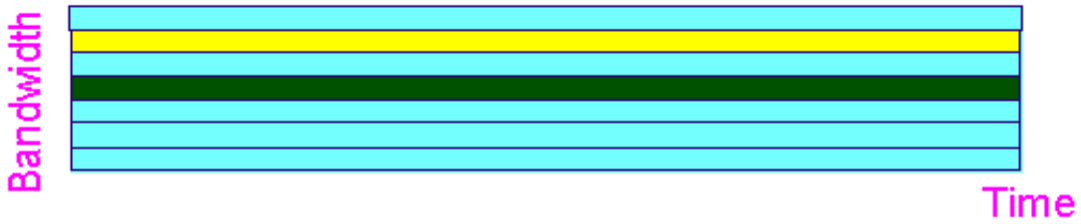
- **CSU/DSU(C**hannel **S**ervice **U**nit**/D**ata **S**ervice **U**nit**)**



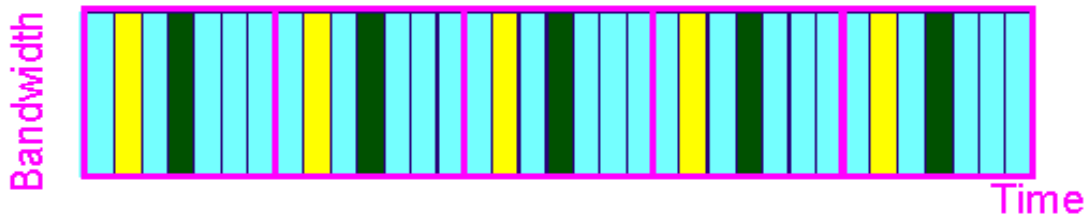
Chia sẻ môi trường truyền

How To Share A Transmission Medium

- **Frequency Division Multiple Access (FDMA)**
  - Non-adaptive, deterministic
  - Useful for constant traffic; How about bursty one?
  - Examples: radio, TV, CATV...
  - All optical networks: wave-length division multiplexing (WDM)



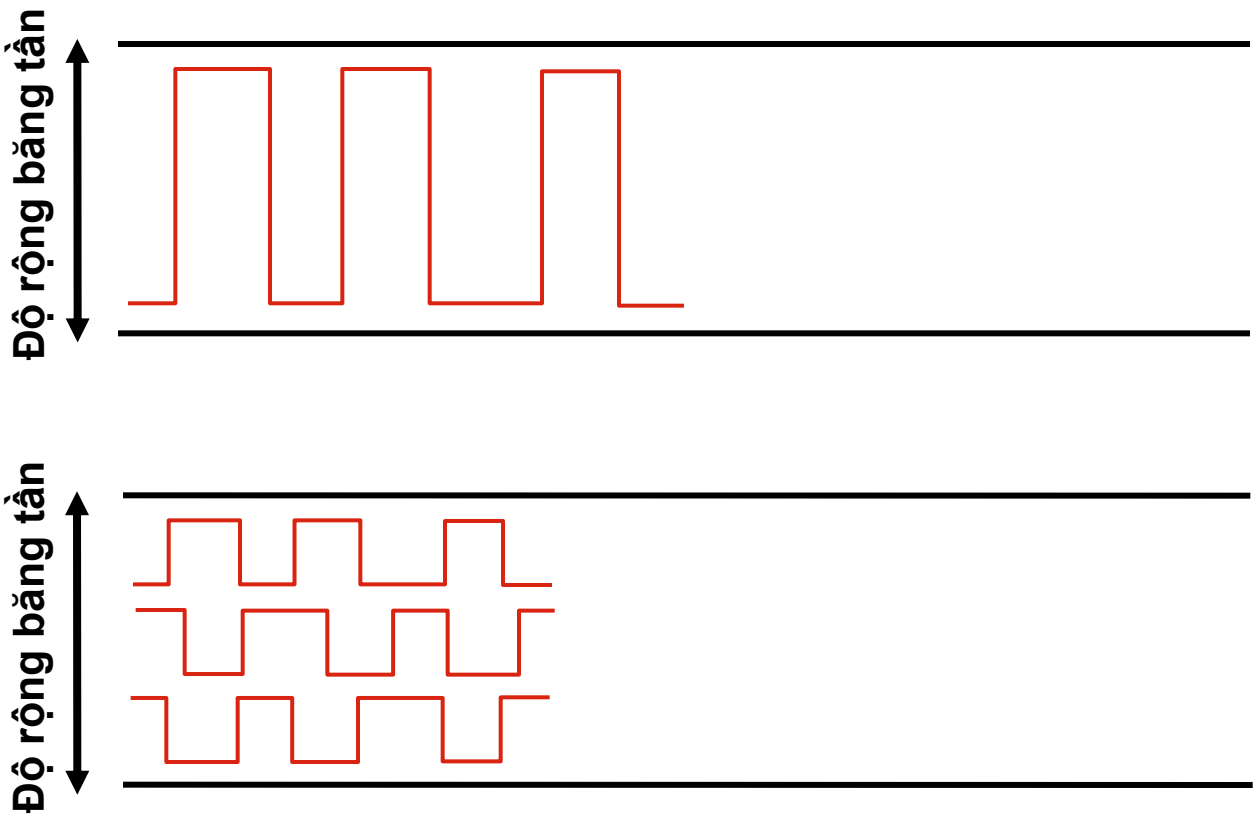
- **Time Division Multiple Access (TDMA)**
  - Examples: TDM bus, telecommunication links



1.5. Các phương thức truyền tín hiệu

- Có hai phương thức truyền tín hiệu trong mạng cục bộ là dùng băng tần cơ sở (baseband) và băng tần rộng (broadband).
  - Băng tầng cơ sở chỉ chấp nhận một kênh dữ liệu duy nhất.
  - Băng rộng có thể chấp nhận đồng thời hai hoặc nhiều kênh truyền thông cùng phân chia giải thông của đường truyền.
- Phương thức truyền trên băng tần cơ sở truyền tín hiệu đi dưới cả hai dạng: tương tự (analog) hoặc số (digital).
- Phương thức truyền trên 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.

Băng tần cơ sở và băng tần rộng

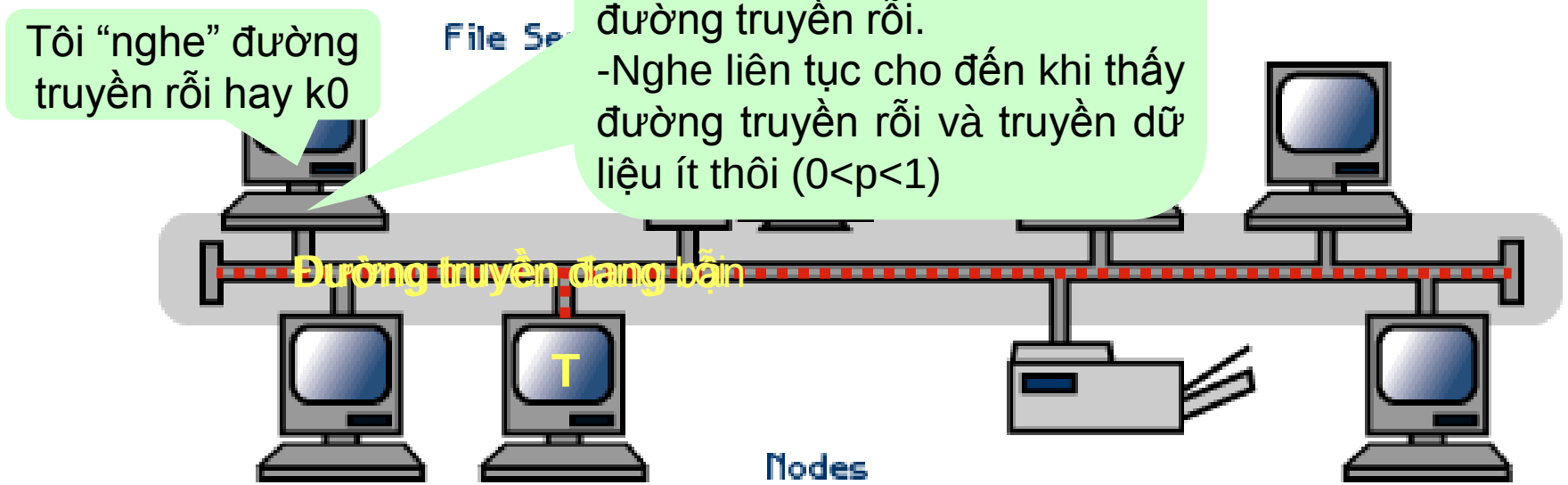


1.6. Phương thức truy nhập đường truyền

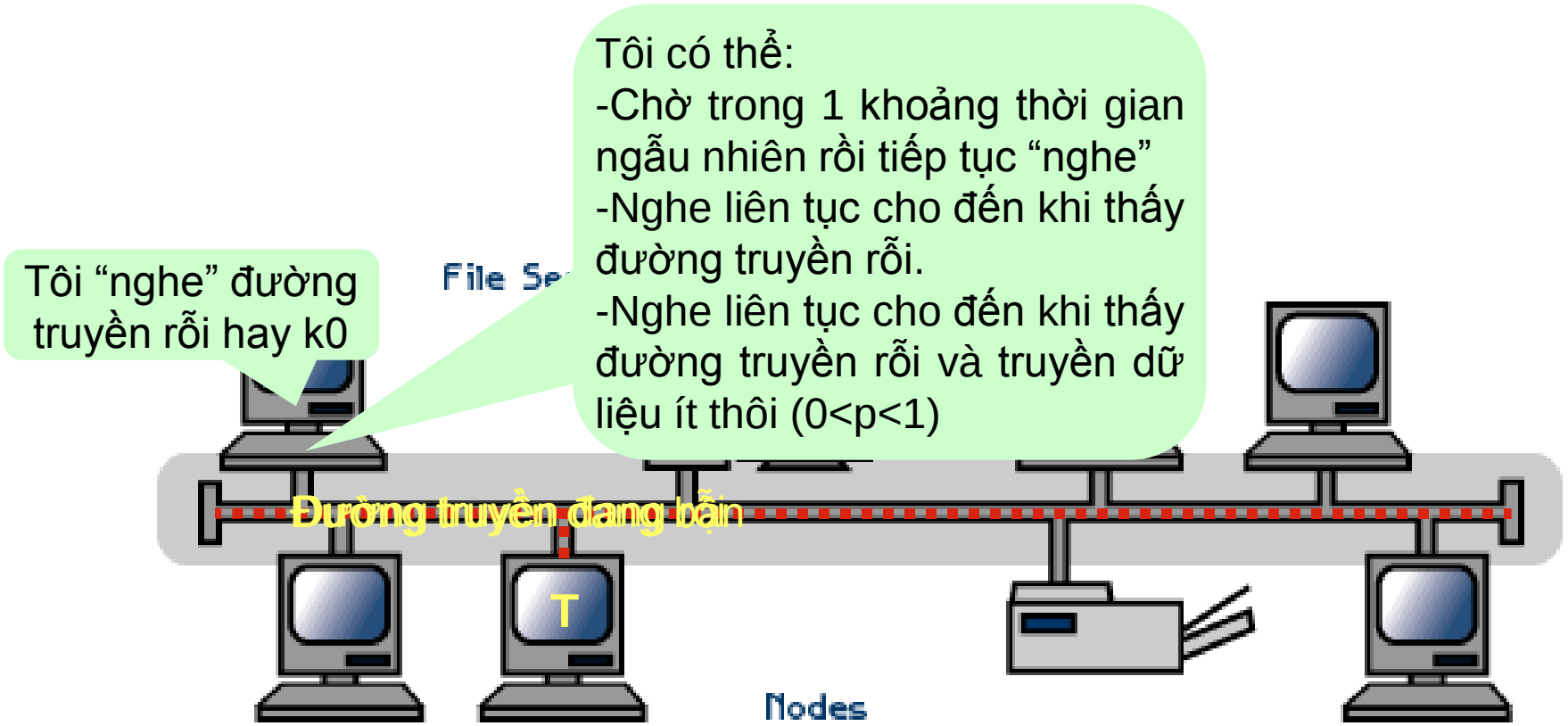
- Có nhiều giao thức khác nhau để truy nhập đường truyền vật lý, nhưng chủ yếu phân thành hai loại:
  - **Phương thức truy nhập có điều khiển:**
    - ✓ Token Bus
    - ✓ Token Ring
  - **Phương thức truy nhập ngẫu nhiên:**
    - ✓ Phương thức đa truy nhập sử dụng sóng mang CSMA (Carrier Sense Multiple Access – hay còn gọi là phương thức "nghe trước khi nói" – listen before talk)
    - ✓ Phương thức đa truy nhập sử dụng sóng mang có phát hiện xung đột CSMA/CD (Carrier Sense Multiple Access with Collision Detection)

Phương thức CSMA/CD

- Đây là phương pháp truy nhập ngẫu nhiên sử dụng cho mạng có cấu trúc dạng hình Bus. Tất cả các node truy nhập ngẫu nhiên vào trường truyền chung. Vì vậy cần có cơ chế tránh xung đột và nghẽn thông tin. CSMA/CD là phương pháp cải tiến của p e trước khi nói - Listen before talk).



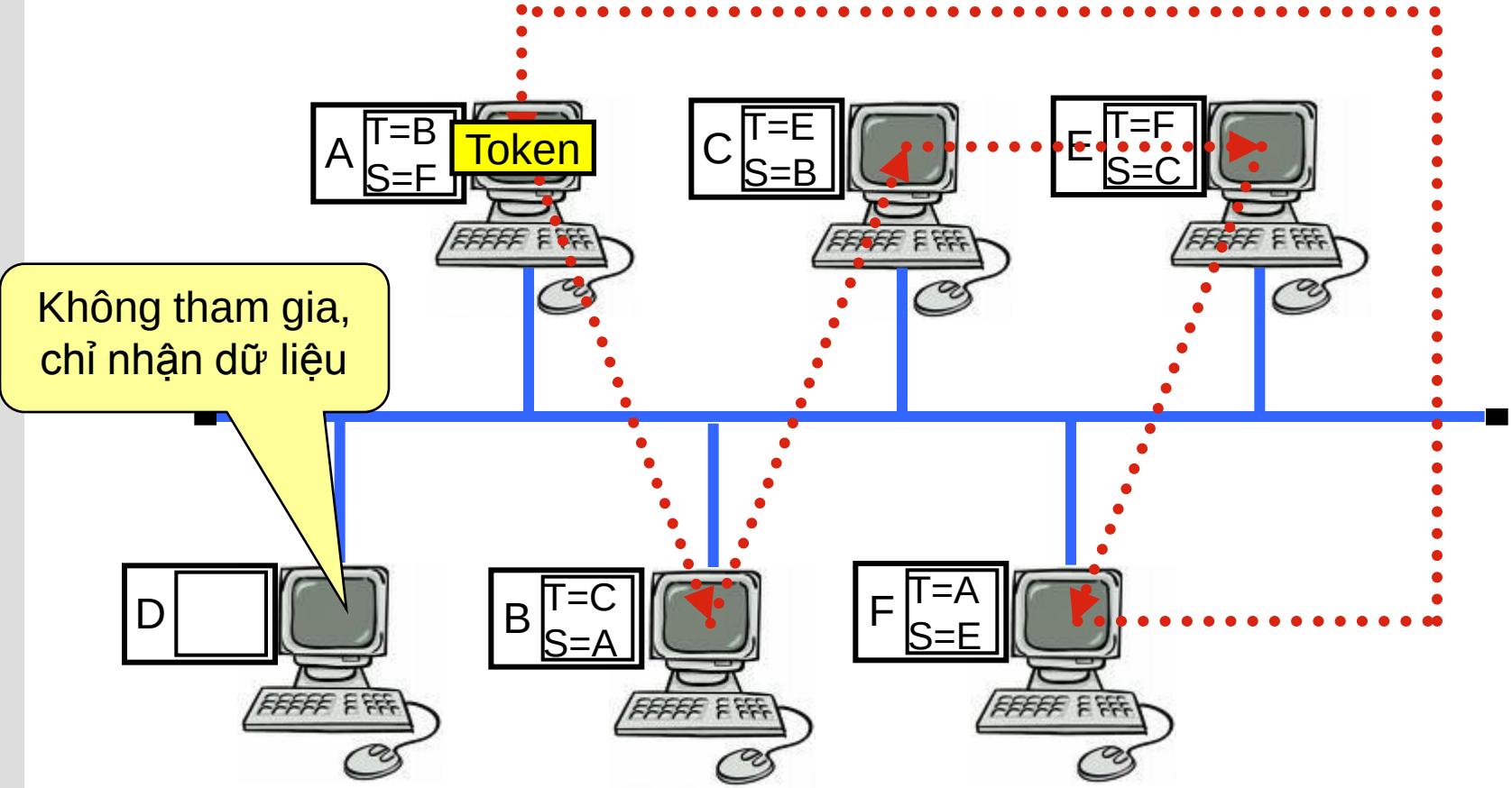
Minh họa


Tôi có thể:
-Chờ trong 1 khoảng thời gian ngẫu nhiên rồi tiếp tục “nghe”
-Nghe liên tục cho đến khi thấy đường truyền rỗi.
-Nghe liên tục cho đến khi thấy đường truyền rỗi và truyền dữ liệu ít thôi (0<p<1)
Tôi “nghe” đường truyền rỗi hay k0
File Se
Đường truyền đang bận
T
Nodes

Phương thức Token Bus

- Sử dụng một **thẻ bài** (token) để cấp phát quyền truy nhập đường truyền cho một trạm cần truyền dữ liệu.
- Thẻ bài 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 phương pháp.
- Thẻ bài được lưu chuyển trên một **vòng logic** nối các trạm có nhu cầu truyền dữ liệu lại với nhau.
- Khi một trạm nhận được thẻ bài nó có quyền truy nhập đường truyền trong một thời gian xác định và có thể truyền một hoặc nhiều đơn vị dữ liệu.
- Khi đã hết dữ liệu hoặc hết thời gian cho phép, nó chuyển thẻ bài cho trạm tiếp theo trên vòng logic.

Minh họa phương thức Token Bus



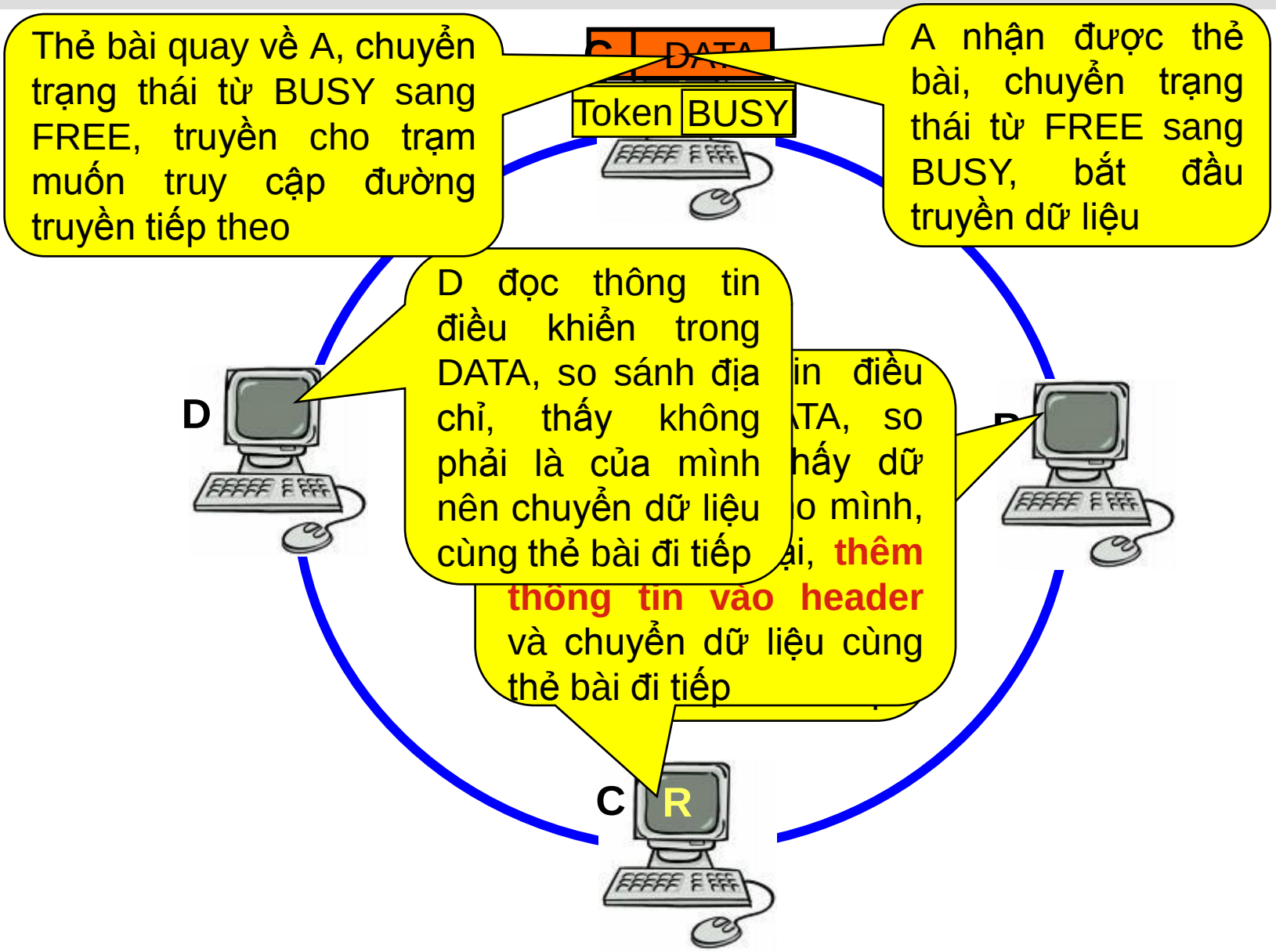
Duy trì trạng thái thực tế của mạng

- Bổ sung định kỳ các trạm nằm ngoài vòng logic nếu có nhu cầu truyền dữ liệu.
- Loại bỏ một trạm không còn nhu cầu truyền dữ liệu ra khỏi vòng logic.
- Quản lý lỗi: giám sát sự cố “đứt vòng” hoặc trùng địa chỉ.
- Khởi tạo vòng logic: Khi cài đặt mạng hoặc đứt vòng cần phải khởi tạo lại vòng. Việc khởi tạo vòng logic được thực hiện khi một hoặc nhiều trạm phát hiện Bus hoạt động vượt qua giá trị ngưỡng thời gian (Time-out) hoặc thẻ bài bị mất. Có nhiều nguyên nhân, chẳng hạn mạng mất nguồn hoặc trạm giữ thẻ bài hỏng. Lúc đó, trạm phát hiện sẽ gửi thông báo “yêu cầu thẻ bài” tới một trạm được chỉ định trước có trách nhiệm sinh thẻ bài mới và chuyển đi theo vòng logic.

Phương thức Token Ring

- Dùng thẻ bài lưu chuyển trên **vòng** vật lý để cấp phát quyền truy nhập đường truyền.
- Một trạm muốn truyền dữ liệu thì phải đợi đến khi nhận được một thẻ bài "rỗi" (free). Khi đó trạm sẽ đổi bit trạng thái của thẻ bài sang trạng thái "bận" (busy) và truyền một đơn vị dữ liệu cùng với thẻ bài đi theo chiều của vòng. Các trạm khác muốn truyền dữ liệu phải đợi thẻ bài "rỗi".
- Dữ liệu đến trạm đích phải được sao chép lại, sau đó cùng với thẻ bài đi tiếp cho đến khi quay về trạm nguồn.
- Trạm nguồn sẽ xoá bỏ dữ liệu và đổi bit thẻ bài thành "rỗi" và cho lưu chuyển tiếp trên vòng để các trạm khác có thể nhận được quyền truyền dữ liệu.

Phương thức Token Ring



Ý nghĩa của việc quay vòng thẻ bài

- Sự quay về lại trạm nguồn của dữ liệu và thẻ bài nhằm tạo ra cơ chế 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:

  (1) trạm đích không tồn tại hoặc không hoạt động;

  (2) trạm đích tồn tại nhưng dữ liệu không được sao chép;

  (3) dữ liệu đã được tiếp nhận;

  (4) có lỗi.

Các vấn đề liên quan

- Có hai vấn đề có thể dẫn đến phá vỡ hệ thống cần giải quyết, đó là:
  - Vấn đề mất thẻ bài.
  - Vấn đề thẻ bài "bận" lưu chuyển không dừng trên vòng.
- **Đối với vấn đề mất thẻ bài:** Có thể quy định vòng không thay đổi (Ví dụ khi gặp một thẻ bài chết đi qua trạm Monitor thì thẻ bài đó sẽ được tái tạo lại). Tuy nhiên, cần chọn một giải thuật để chọn trạm thay thế cho trạm Monitor khi bị hỏng.

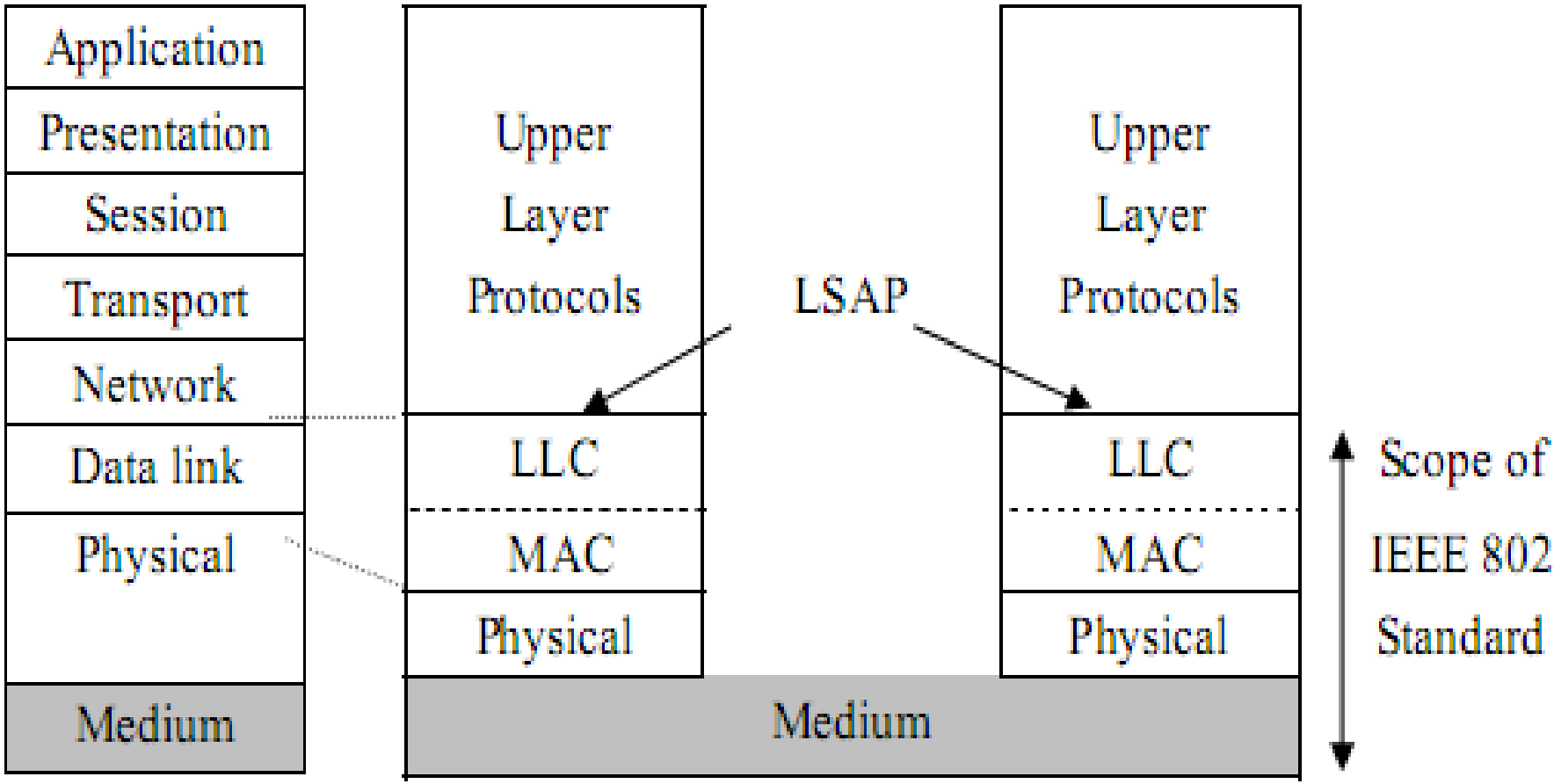
1.7. Các loại mạng cục bộ

- Ethernet và chuẩn IEEE 802
- Mạng cục bộ Token Ring
- Giao diện số liệu phân bố sử dụng cáp quang FDDI (Fiber Distributed Data Interface)
- Mạng LAN ATM

1.7.1. Ethernet và chuẩn IEEE 802

- **Ethernet**
  - Là công nghệ của mạng LAN cho phép truyền tín hiệu giữa các máy tính với tốc độ 10Mbps đến 10 Gbps. Trong các kiểu Ethernet thì kiểu sử dụng cáp xoắn đôi là thông dụng nhất. Hiện nay có khoảng 85% mạng LAN sử dụng công nghệ Ethernet.
  - Năm 1980, Xerox, tập đoàn Intel và tập đoàn Digital Equipment đưa ra tiêu chuẩn Ethernet 10 Mbps (Tiêu chuẩn DIX).
  - Năm 1985, IEEE đưa ra tiêu chuẩn về Ethernet đầu tiên với tên gọi "IEEE 802.3 Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications“.

Quan hệ IEEE 802 với OSI



Thành phần mạng Ethernet

- Data terminal Equipment (DTE): Các thiết bị truyền và nhận dữ liệu DTEs thường là PC, Workstation, File Server, Print Server ...
- Data Communication Equipment (DCE): Là các thiết bị kết nối mạng cho phép nhận và chuyển khung trên mạng. DCE có thể là các thiết bị độc lập như Repeter, Switch, Router hoặc các khối giao tiếp thông tin như Card mạng, Modem ..
- Interconnecting Media: Cáp xoắn đôi, cáp đồng (mỏng/dày), cáp quang.

Những đặc điểm cơ bản của Ethernet

- Cấu hình truyền thống: Bus/Star
- Cấu hình khác Star/Bus
- Kỹ thuật truyền: Base band
- Phương pháp truy nhập: CSMA/CD.
- Quy cách kỹ thuật: IEEE 802.3.
- Vận tốc truyền 10Mbps, 100Mbps ... 10Gbps
- Loại cáp: Cáp đồng trục mảnh, cáp đồng trục dày, cáp xoắn đôi, cáp quang ...

Các loại cáp Ethernet

- 10BASE-F: Dùng cáp quang, tốc độ 10 Mb/s, phạm vi cáp 4km. Chuẩn này có 3 dạng con: 10BASE-FL, 10BASE-FB và 10BASE-FP.
- 10BASE-T: Sử dụng một dải tần rộng hỗ trợ cho các tốc độ tín hiệu 10Mb/s. Dùng cáp UTP, với mạng hình sao.
- 100BASE-X: Gọi là Fast Ethernet, mạng hình sao tương tự 10BASE-T, tốc độ 100Mb/s. Chuẩn này gồm 100 BASE-TX dùng cho cáp UTP hoặc STP 2 đôI, 100 BASE-FX dùng cho cáp quang đa mode, 100 BASE-T4 dùng cho cáp UTP 4 đôi (Four Twisted Pairs).
- 10BROAD36: Dùng Broadband, tốc độ 10Mb/s, cáp đồng trục 75 Ohm, phạm vi cáp 1800 m (lên tới 3600m trong cấu hình cáp đôi), sử dụng topo dạng BUS.
- 10BASE-2 Dùng cáp đồng trục mỏng (thin cable) 50 □, T-connector, BNC connector. Khoảng cách tối thiểu giữa hai trạm là 0.5 m. Khoảng cách tối đa giữa hai trạm là 185m.
- 10BASE-5 Dùng cáp đồng trục dày (thick cable) 50 □, còn gọi là cáp vàng, AUI connector (Attachment Unit Interface). Khoảng cách tối thiểu giữa hai AUI là 2,5 m, khoảng cách tối đa là 500m.

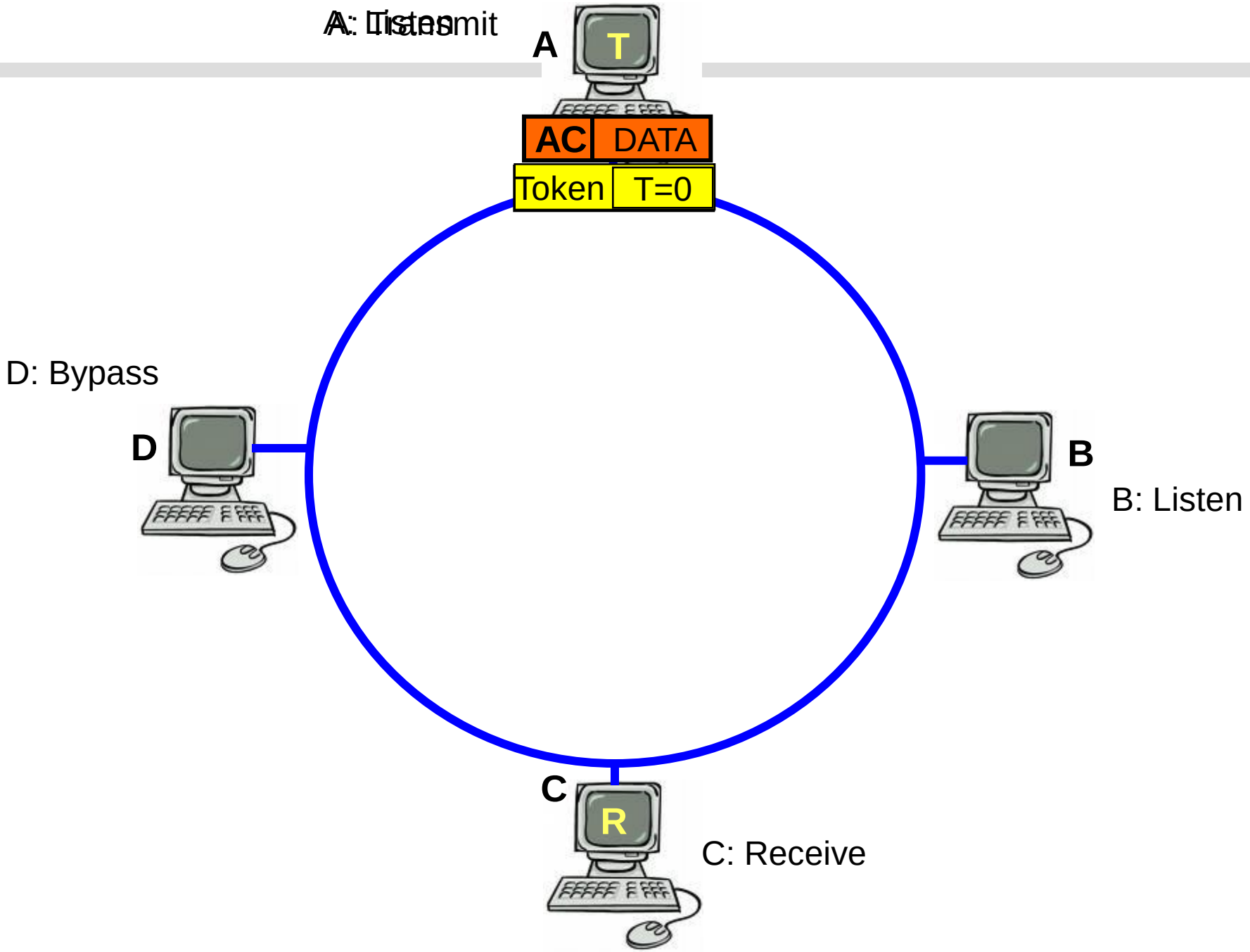
Gigabit Ethernet

- Sự ra đời của Gigabit Ethernet đã mở ra một kỷ nguyên mới Ethernet tốc độ cao. Nó được thiết lập dựa trên các nguyên lý cơ bản của 10BASE-T, Fast Ethernet và chuyển mạch Ethernet. Các chuẩn Gigabit Ethernet:
  - IEEE 802.32: Mạng Gigabit Ethernet trên cáp quang chuẩn hóa năm 1998. Phương tiện truyền dẫn cơ bản là sợi quang đơn mode.
  - IEEE 802.3ab: Gigabit Ehernet trên cáp đồng, đặc trưng bởi 1000Base-T. Sử dụng cả 4 đôi dây cáp UTP Cat 5 (hoặc Cat-6, Cat-7) với khoảng cách tối đa 100m.
  - IEEE 802.3ae: 10 Gigabit Ethernet (GbE). Tốc độ Ethernet lên đến 10Gbps, cho phép Ethernet có thể tích hợp với những công nghệ tốc độ cao trên mạng đường trục WAN với tốc độ xấp xỉ 9,5 Gbps.

Nguyên tắc cơ bản khi xây dựng các mạng chuyển mạch tốc độ cao là kết hợp nhiều đoạn mạng tốc độ thấp lại với nhau. Khi mật độ và số lượng các đoạn có tốc độ 100Mbps trong mạng tăng lên thì 1000BASE-X và 1000BASE-T trở thành công nghệ truyền dẫn ở mức cao hơn được sử dụng trên các lõi mạng.

1.7.2. Mạng cục bộ Token Ring

- Mỗi trạm hoạt động như là một bộ chuyển tiếp (repeater) hỗ trợ cho sự khuyếch đại tín hiệu suy hao.
- Có thể sử dụng các loại cáp đồng trục, cáp sợi quang, cáp xoắn đôi. Sử dụng phương thức truy nhập đường truyền Token Ring.
- Các trạm của mạng cục bộ Token Ring hoạt động theo 4 chế độ sau:
  - Chế độ truyền.
  - Chế độ lắng nghe.
  - Chế độ bỏ qua.
  - Chế độ nhận.


A: Transmit
A
T
AC
DATA
Token
T=0
D: Bypass
D
B
B: Listen
C
R
C: Receive

1.7.3. Mạng FDDI

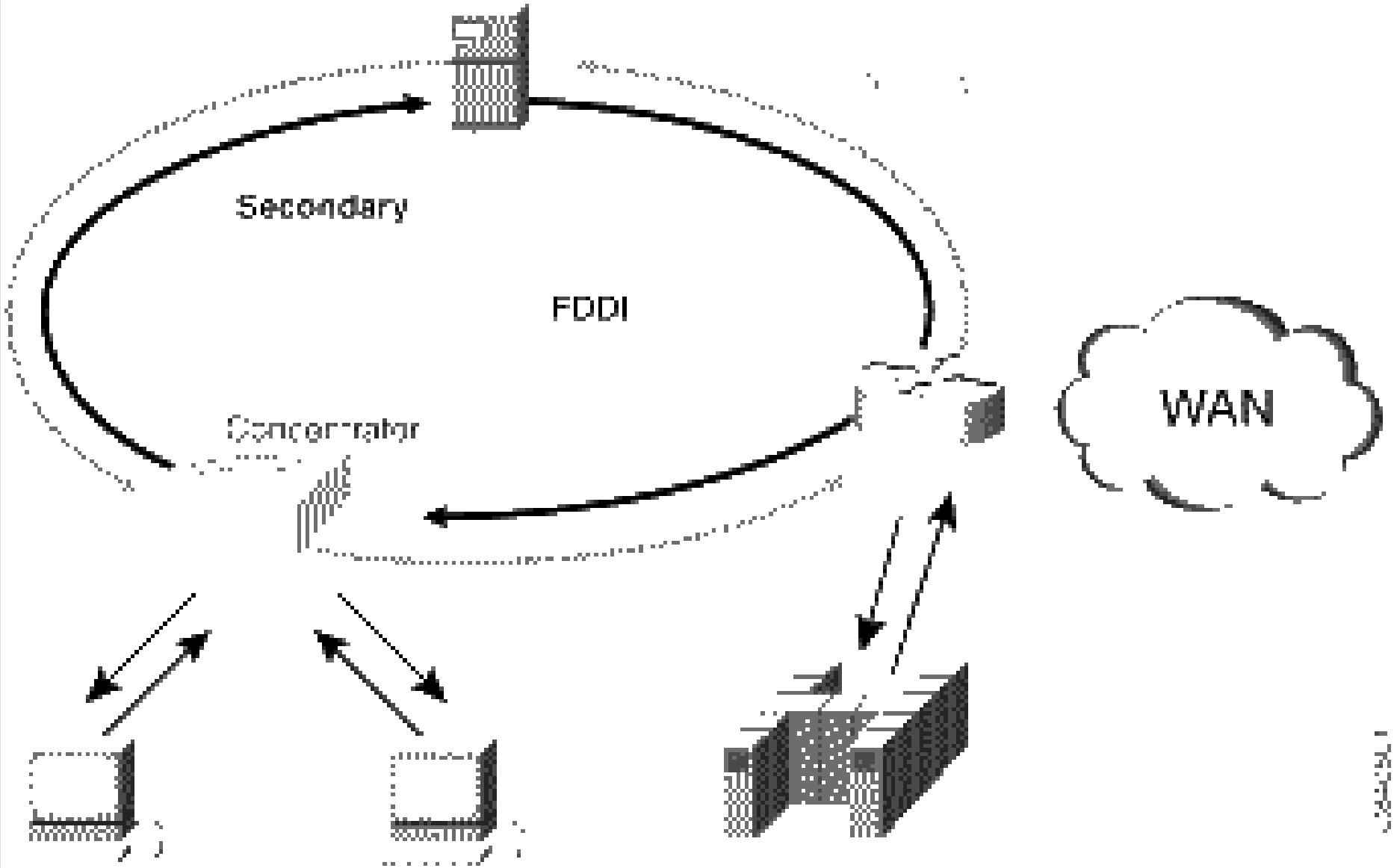
- FDDI là tập các giao thức ANSI truyền DL qua cáp quang.
- Các mạng FDDI sử dụng phương thức truy nhập Token Passing, tốc độ có thể đạt đến 100 Mbps.
- FDDI được sử dụng làm Backbone cho các mạng diện rộng MAN, WAN.
- Một trong các ứng dụng là để kết nối các máy chủ tốc độ cao. Khi đóng vai trò là một mạng xương sống, FDDI liên kết các thiết bị mạng khác nhau như Router, Switch, Brigde, các bộ tập trung... để tạo thành một mạng lớn hơn từ các mạng con.
- Tuy nhiên FDDI không được dùng cho các mạng diện rộng (WAN) có bán kính lớn hơn 100 km.

Ưu điểm của FDDI

Có 2 ưu điểm nổi bật:

- FDDI có thể được cấu hình như hai vòng Ring song song. Trong trường hợp có sự cố đứt cáp hoặc hỏng một trạm, vòng Ring thứ hai sẽ được kích hoạt (Thông thường vòng Ring thứ hai này không hoạt động), tạo thành một Ring đơn khác để thay thế. Khi đó, FDDI sẽ tự động cô lập phần bị hỏng và tiếp tục hoạt động bình thường. Phần bị hỏng có thể được sửa chữa hoặc thay thế mà không làm gián đoạn hoạt động của mạng. Nếu cần thiết, hai vòng Ring có thể được kết hợp lại thành một Ring đơn để tăng tốc độ truyền dữ liệu. Điều này cho phép FDDI có khả năng chịu lỗi cao và đảm bảo tính liên tục của mạng.
- Khả năng tự phục hồi bằng kỹ thuật Ring ngược: Khi phát hiện ra sự cố đứt cáp hoặc hỏng một trạm, FDDI sẽ tự động nối vòng hai Ring với nhau thành một Ring đơn.

Minh họa FDDI



1.7.4. Mạng LAN ATM

- Mạng LAN được xây dựng đựa trên kỹ thuật ATM - Asynchronous Transfer Mode gọi là Local LAN (LATM).
- Bộ điều khiển mạng đặt trong tổng đài ATM, tổng đài định lộ trình các thông báo và kiểm soát truy nhập trong trường hợp nghẽn mạch. Ngược với kỹ thuật LAN truyền thống, việc điều khiển được cài đặt trong các bộ giao tiếp mạng.
- Thông lượng rộng, dễ mở rộng bằng cách thêm nhiều node chuyển mạch tốc độ cao (hay thấp) cho các thiết bị nối vào.
- Là phương tiện liên kết mạng giữa kỹ thuật LAN và WAN.
- ATM có thể đáp ứng các yêu cầu nhờ các đường dẫn ảo và các kênh ảo, rất dễ tích hợp các lớp đa dịch vụ.
- Các gói tin là tế bào có độ dài cố định, vì vậy việc dùng ATM trong một mạng đầu cuối cho phép xoá dần ranh giới giữa LAN và WAN.

1.8. Các hệ điều hành mạng

- Cần phải có một hệ điều hành trên phạm vi toàn mạng có chức năng **quản lý dữ liệu**, **tính toán và xử lý** một cách thống nhất.
- HĐH mạng được thiết kế theo một hướng tối ưu khác với HĐH đơn. Mục đích của HĐH đơn là cung cấp cách thức thực hiện công việc tốt nhất cho người sử dụng trên máy đơn. Ngược lại, mục đích của HĐH mạng là tạo ra một sự điều phối tốt nhất có thể cho tất cả những người sử dụng đang truy cập vào máy chủ (server) chứ không phải nhằm tạo ra một sự ưu tiên cho bất kỳ trường hợp nào.
- HĐH mạng (Network Operating System-NOS) là phần mềm **điều hành** một hệ thống mạng máy tính kết nối với nhau, cho phép người sử dụng **chia sẻ** chương trình, dữ liệu, tài nguyên và **truy cập** vào máy phục vụ.

Phương pháp tạo ra phần mềm phục vụ:

- Giữ nguyên các HĐH cục bộ, HĐH mạng được cài đặt như một tập các chương trình tiện ích.
- Bỏ qua tất cả các HĐH trên các máy đơn và cài đặt một HĐH thống nhất trên toàn mạng. Chúng được gọi là các **HĐH phân tán** (distributed operating system).

Mỗi cách tiếp cận có ưu và nhược điểm riêng của chúng.

Các dịch vụ phổ biến trên HĐH mạng

Thường có thể phân thành các loại sau:

- Truy cập ứng dụng: các client yêu cầu các ứng dụng thực hiện trên server.
- Truy cập cơ sở dữ liệu: các client yêu cầu truy cập cơ sở dữ liệu trên server, thường là ngôn ngữ SQL.
- Dịch vụ in ấn.
- Truyền thông qua mạng: sử dụng các phần mềm thực hiện các giao thức IPX/SPX, TCP/IP.

Một số hệ điều hành mạng

HĐH mạng *NetWare* của Novell:

- Là HĐH phổ biến, 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.
- HĐH do các nhà khoa học xây dựng và được dùng rất phổ biến trong các phòng thí nghiệm, các trường ĐH.
- HĐH mạng UNIX là HĐH đa nhiệm, đa người sử dụng, phục vụ cho truyền thông tốt.
- Nhược điểm: hiện nay có nhiều *Version* khác nhau, không thống nhất gây khó khăn cho người sử dụng. Ngoài ra HĐH này khá phức tạp, đòi hỏi cấu hình máy mạnh.

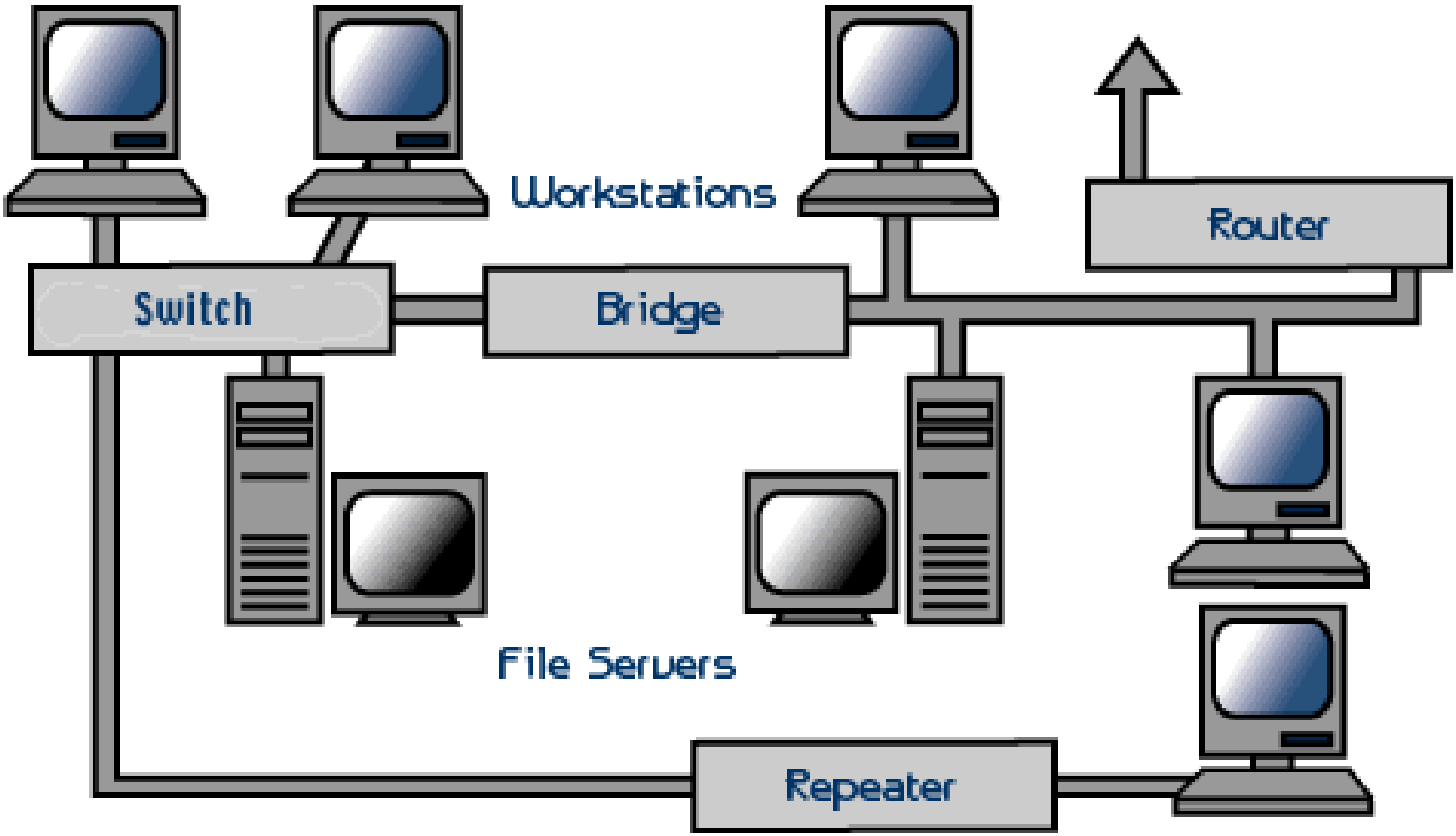
HĐH mạng *Windows NT* của MS:

- HĐH mạng của hãng Microsoft, cũng là HĐH đa nhiệm, đa người sử dụng.
- Đặc điểm nổi bật của *Windows NT* là một HĐH có giao diện đồ họa, thân thiện với người dùng, dễ cài đặt, dễ quản trị, tương thích với nhiều loại máy tính khác nhau.
- Tuy nhiên, để chạy có hiệu quả, *Windows NT* cũng đòi hỏi cấu hình máy tương đối mạnh. HĐH mạng *Windows for Workgroup* là HĐH 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 (hiện nay rất ít sử dụng). Đã có *Windows 2000 Server&Pro, Windows Server 2003, Windows Server 2008*.

HĐH mạng *BSD UNIX*:

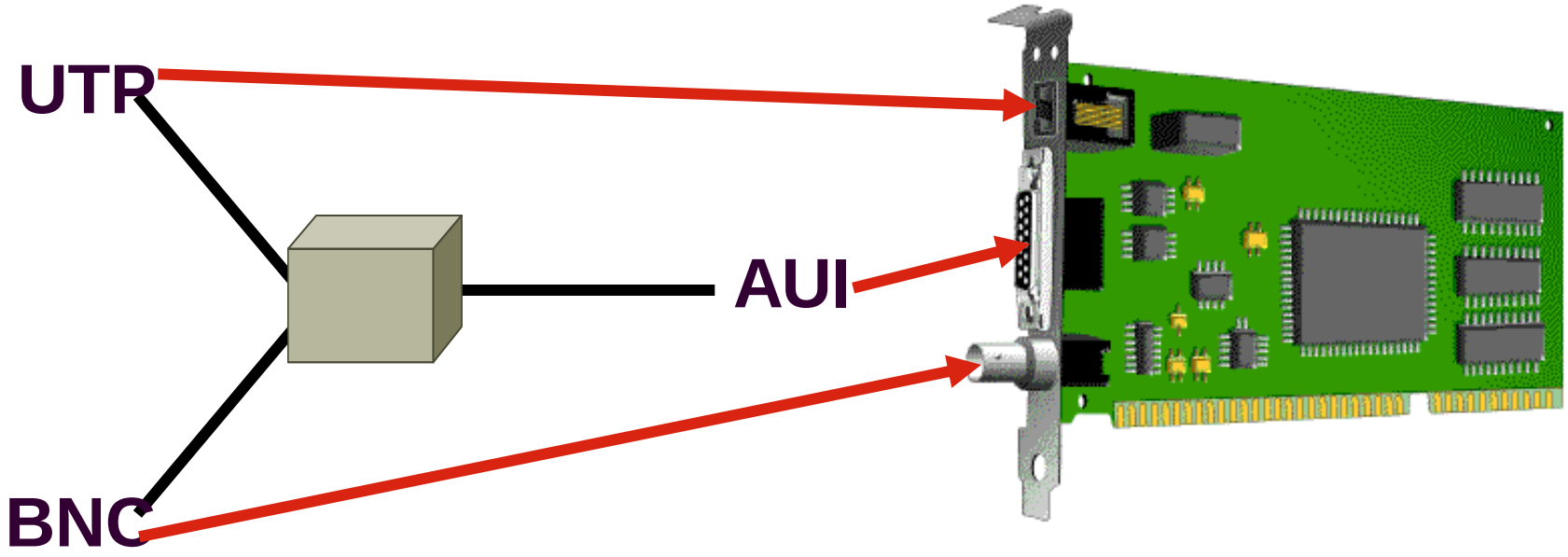
- Berkeley Software Distribution) là một HĐH mạng được phát triển dựa trên UNIX và có thể chạy trên máy tính Apple Macintosh.

1.9. Thiết bị mạng



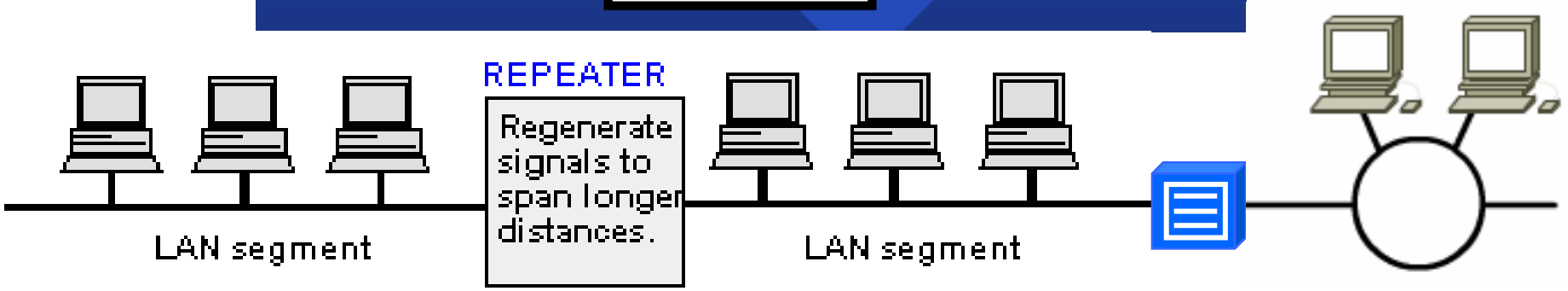
1.9.1. Thiết bị thu phát (Transceive)

- Kết nối các phương tiện truyền khác nhau với NIC
- Được tích hợp trên NIC
- Là thiết bị hoạt động ở tầng 1 của mô hình OSI

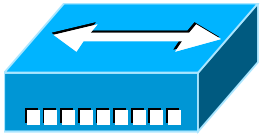


1.9.2. Thiết bị lặp tín hiệu (Repeater)

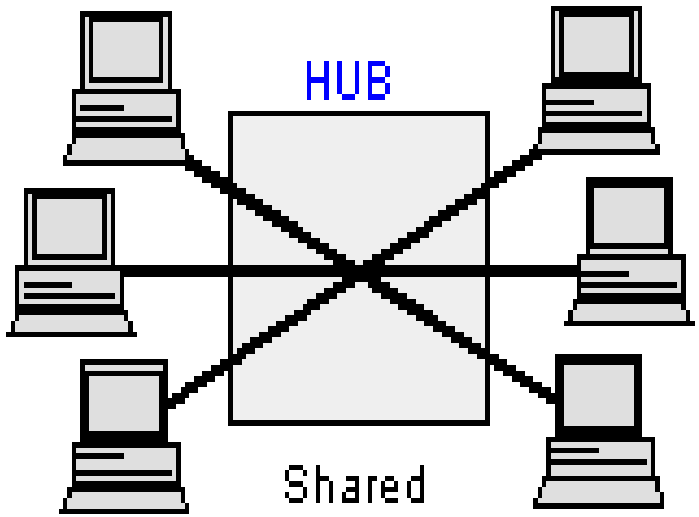
- Phục hồi tín hiệu, khuếch đại tín hiệu.
- Cho phép mở rộng mạng vượt xa chiều dài giới hạn của một môi trường truyền.
- Được hiện thực bằng phần cứng. Tích hợp trên card Token Ring
- Là thiết bị hoạt động ở tầng 1 của mô hình OSI

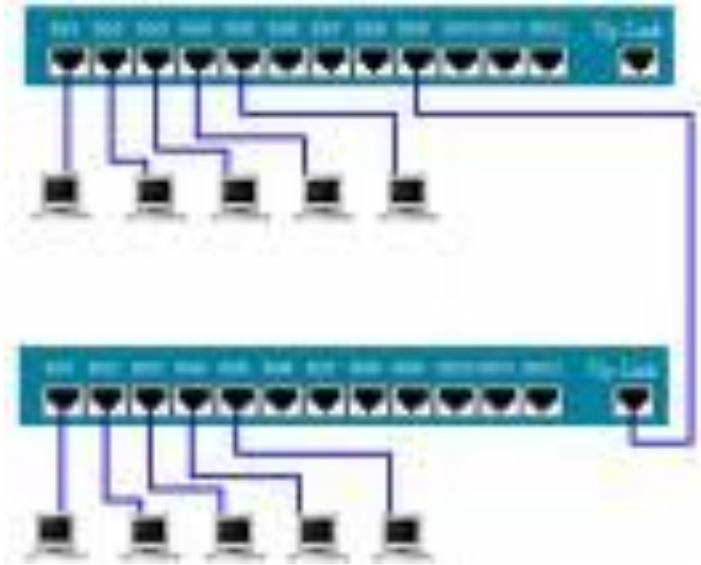


1.9.3. Thiết bị tập trung dây (Hub)



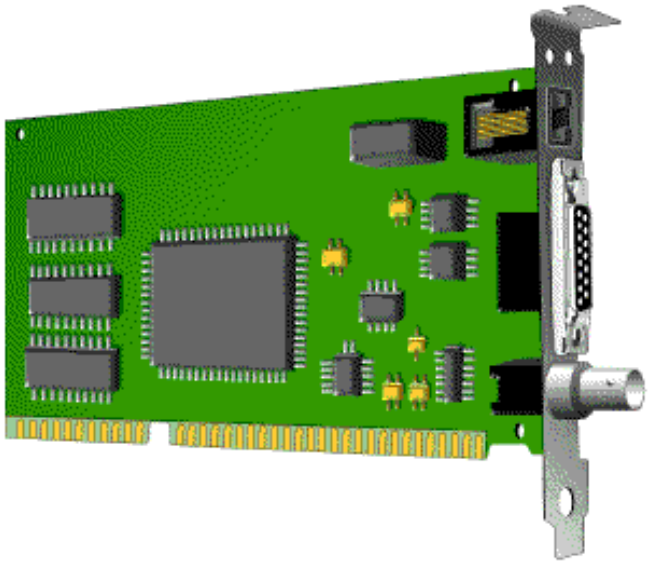
- Thực hiện chức năng như Repeater (nên còn có tên là bộ lặp đa cổng) tuy nhiên có mở rộng.
- Tạo ra điểm kết nối tập trung (nên có tên bộ tập trung dây).
- Tín hiệu được phân phối đến tất cả các thiết bị kết nối (nên có tên là bộ chia tín hiệu).
- Một số chức năng quản lý cũng được tích hợp.
- Là thiết bị hoạt động ở tầng 1 của mô hình OSI

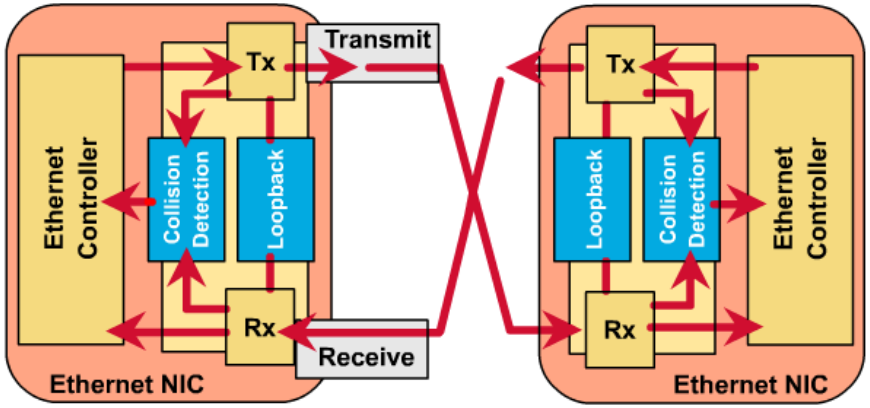




1.9.4. Card giao tiếp mạng (NIC)

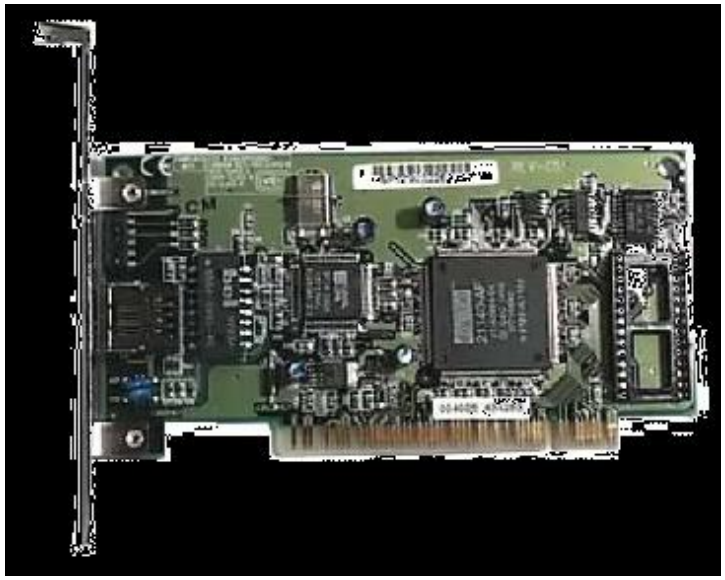
- Chuẩn mạng cục bộ sử dụng
  - Ethernet, Fast Ethernet, Gigabit Ethernet.
  - Tốc độ truyền dữ liệu.
- Môi trường truyền thông
  - Twisted-pair, coaxial hay fiber-optic.
  - Wireless.
- Slot cắm
  - ISA, PCI, PCI-X
  - PCMCIA
- Là thiết bị hoạt động ở tầng 1, 2 của mô hình OSI





MAC Address

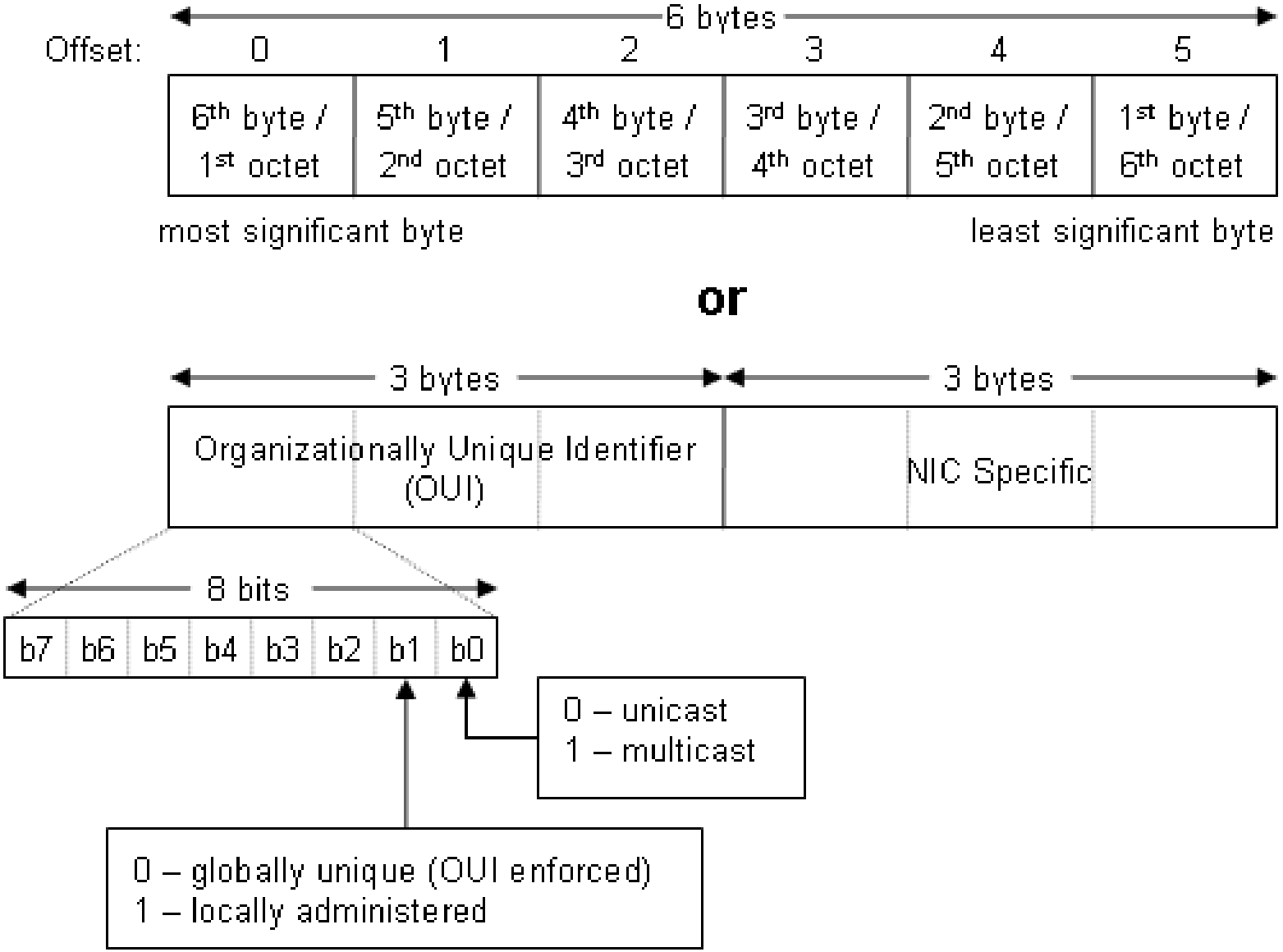
- Còn gọi là Ethernet address.
- Mỗi máy tính dùng địa chỉ MAC (địa chỉ vật lý) để xác định chính nó.
- Địa chỉ MAC được ghi lên trên NIC (card mạng) lúc xuất xưởng và không thay đổi được.



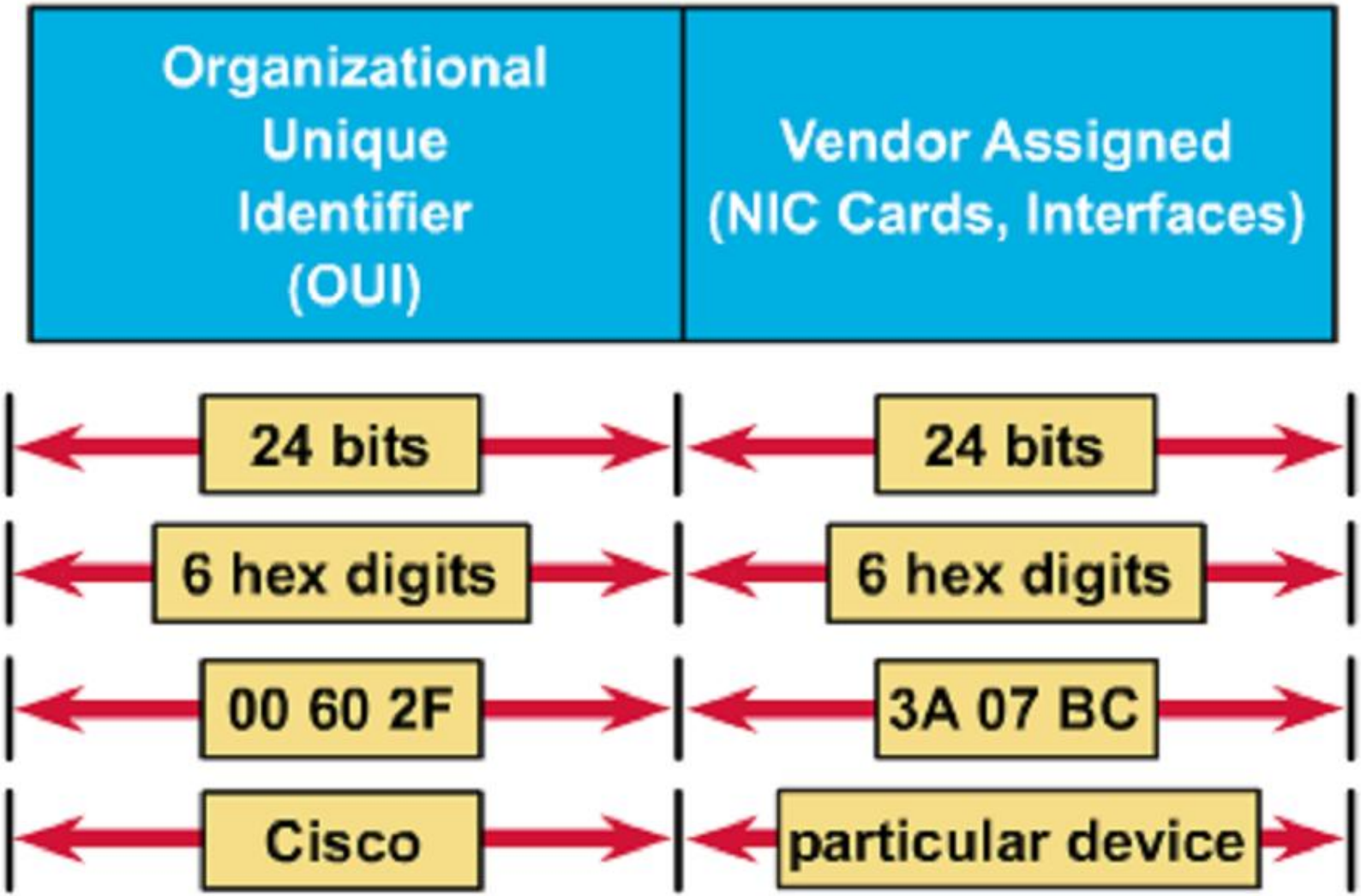
- Địa chỉ MAC không có cấu trúc.
- Địa chỉ MAC được ghi vào ROM và được chép vào RAM khi NIC khởi động
- Biểu diễn bởi 6 bytes (octet):

0000.0c12.3456 hay 00-00-0c-12-34-56.

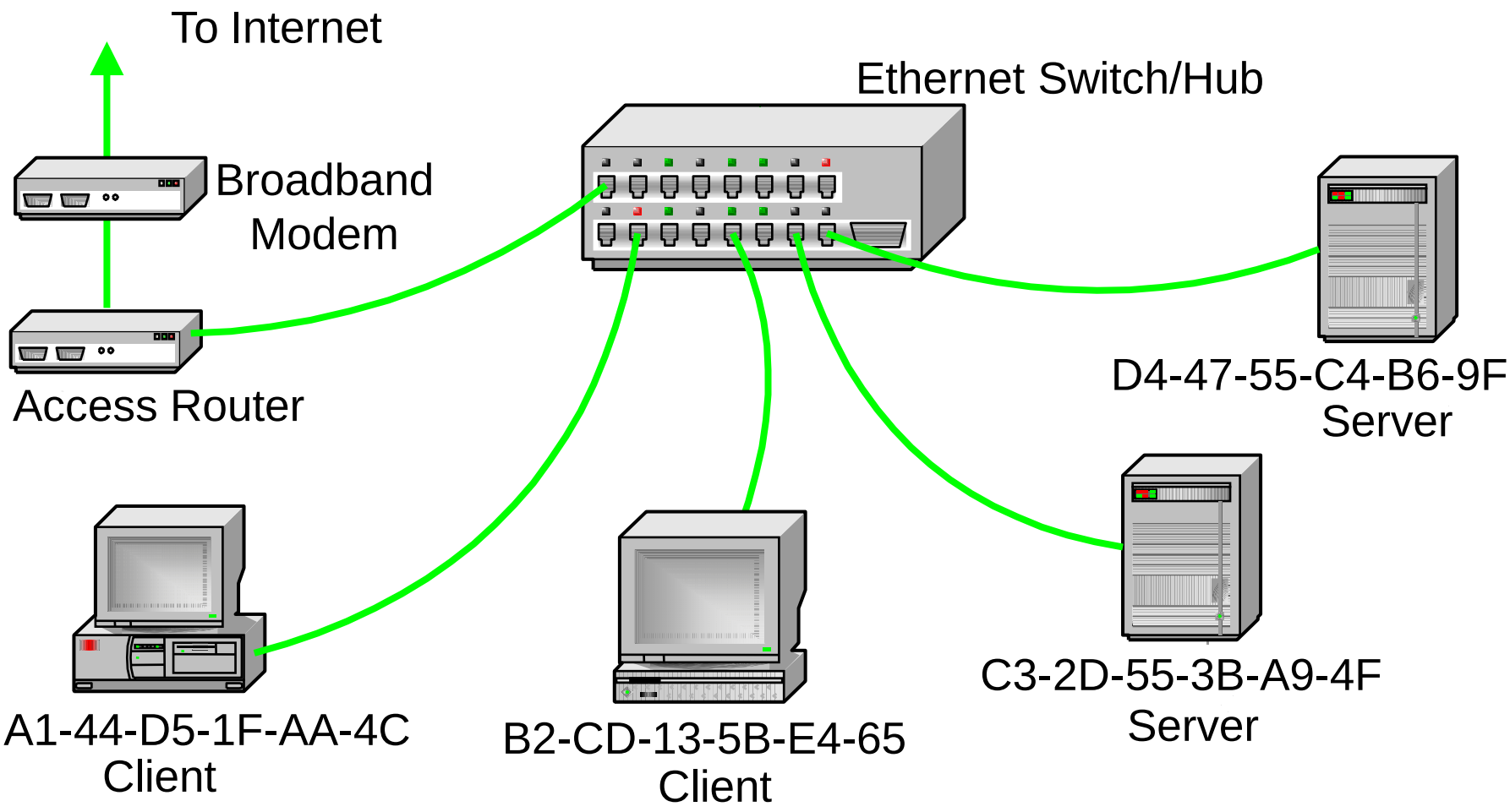
Định dạng địa chỉ mạng



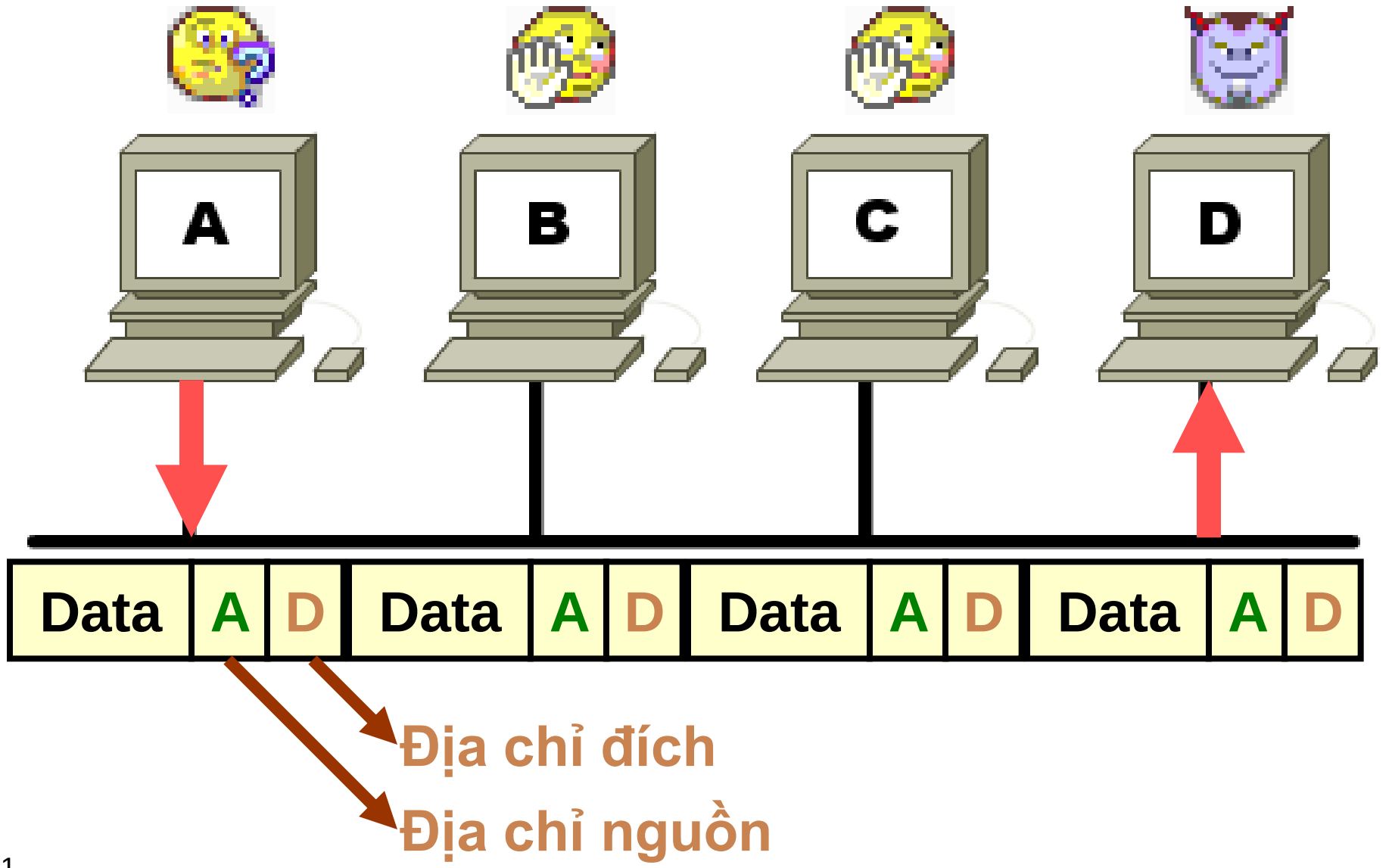
Định dạng địa chỉ mạng



Minh họa địa chỉ MAC



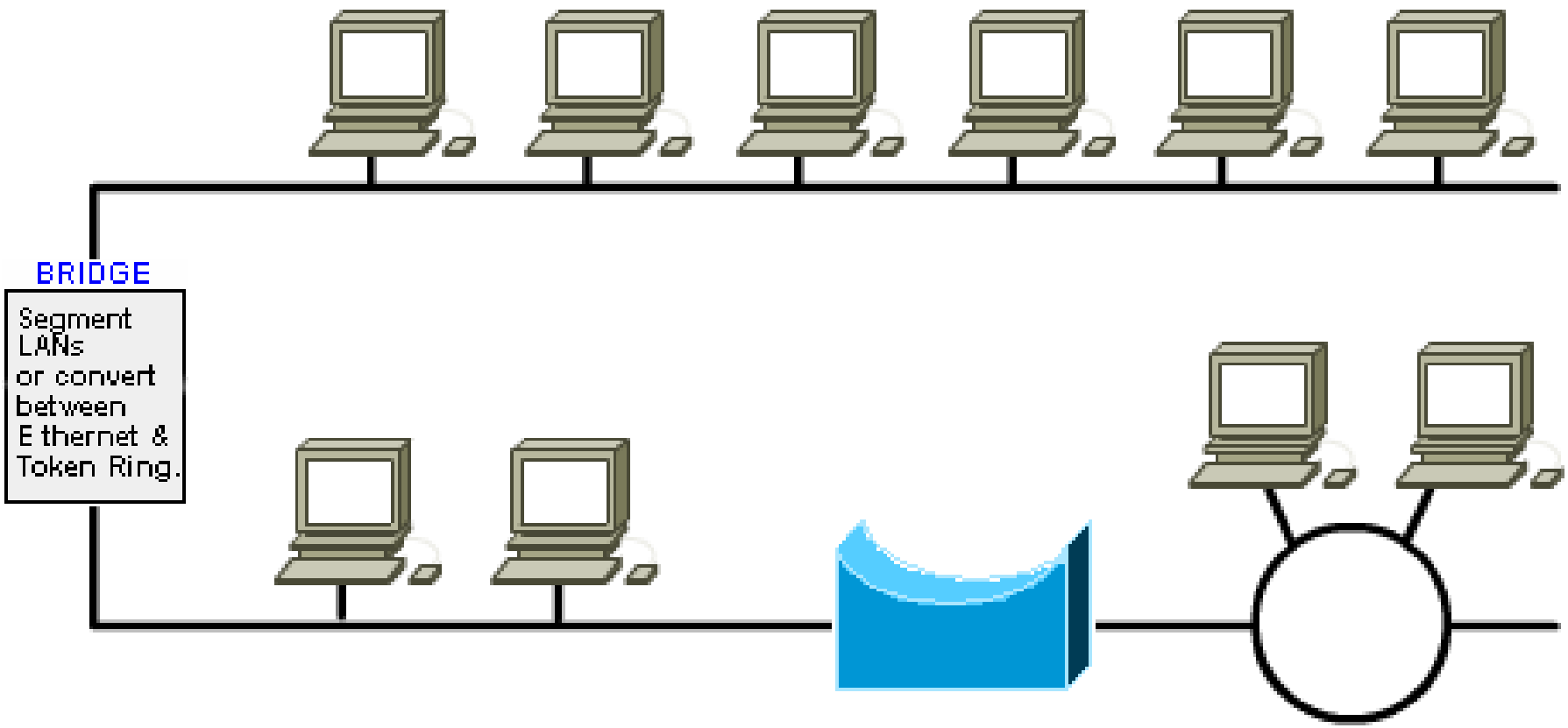
Sử dụng địa chỉ MAC



1.9.5. Thiết bị cầu nối (Bridge)

- Là cầu nối hai hoặc nhiều đoạn (segment) của một mạng.
- Thông minh hơn trong việc quyết định có chuyển tín hiệu qua đoạn mạng kia hay không, lọc những gói dữ liệu để gửi đi (hay không gửi) cho đoạn nối, hoặc gửi trả lại nơi xuất phát.
- Tăng hiệu suất mạng bởi loại trừ lưu lượng mạng không cần thiết và giảm sự đụng độ. Các bridge cũng thường được dùng để phân chia một mạng lớn thành hai mạng nhỏ nhằm làm tăng tốc độ.
- Chia mạng thành các đoạn mạng và lọc lưu lượng dựa trên địa chỉ MAC. Chuyển các gói tin có đích ở phần mạng bên kia dựa vào địa chỉ vật lý
- Chuyển frame giữa các đoạn mạng có giao thức tầng 2 khác nhau. Mặc dầu ít chức năng hơn router, nhưng bridge cũng được dùng phổ biến.
- Theo mô hình OSI thì Bridge thuộc tầng 2.

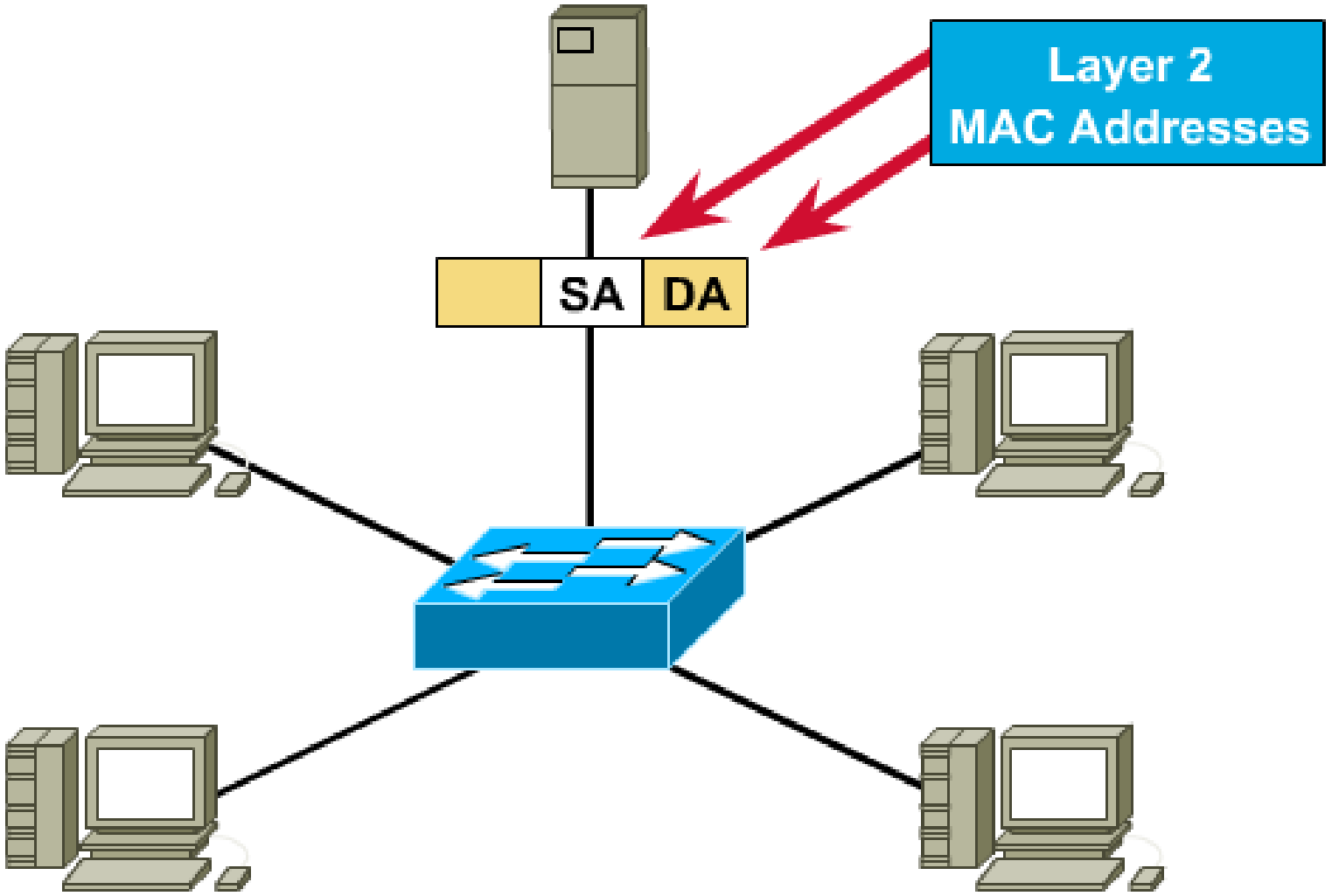
Ví dụ


BRIDGE
Segment LANs or convert between Ethernet & Token Ring.

1.9.6. Thiết bị 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 (nên còn gọi là cầu nối đa cổng). Tốc độ cao hơn Bridge, thay thế Hub với hệ thống dây giữ nguyên, sử dụng bảng địa chỉ MAC để xác định đoạn mạng frame cần truyền.
- Bộ chuyển mạch kết nối một số LAN riêng biệt và cung cấp khả năng lọc gói dữ liệu giữa chúng.
- Các Switch là loại thiết bị mạng mới, nhiều người cho rằng, nó sẽ trở nên phổ biến nhất vì nó là bước đầu tiên trên con đường chuyển sang chế độ truyền không đồng bộ ATM. Hỗ trợ các tính năng mới như VLAN (LAN ảo).
- Theo mô hình OSI thì Switch thuộc tầng 2.

Ví dụ thiết bị chuyển mạch

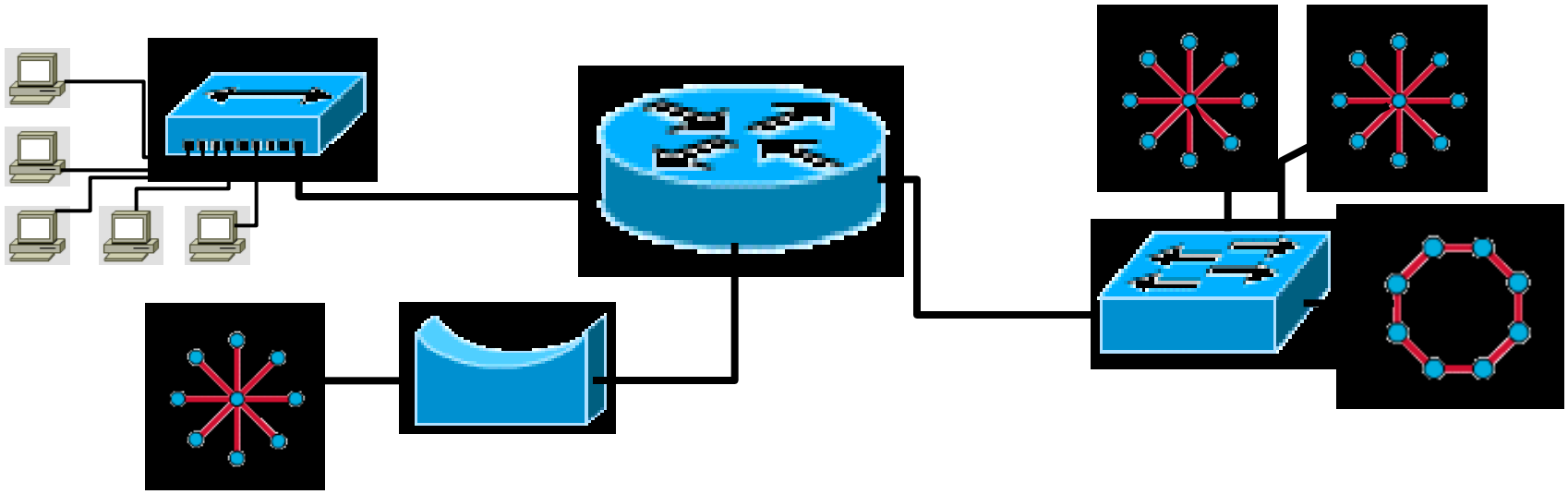


1.9.7. Bộ định tuyến (Router)

- Chức năng cơ bản của router là gửi đi các gói dữ liệu dựa trên địa chỉ phân lớp của mạng và cung cấp các dịch vụ như bảo mật, quản lý lưu thông...
- Giống như bridge, router là một thiết bị thông minh đối với các mạng thực sự lớn. Router biết địa chỉ của tất cả các máy tính ở từng phía và có thể chuyển các thông điệp cho phù hợp. Chúng còn phân đường-định tuyến để gửi từng thông điệp có hiệu quả.
- Theo mô hình OSI thì chức năng của router thuộc tầng 3, cung cấp thiết bị với thông tin chứa trong các header của giao thức, giúp cho việc xử lý các gói dữ liệu thông minh.
- Dựa trên những giao thức, router cung cấp dịch vụ mà trong đó mỗi packet dữ liệu được đọc và chuyển đến đích một cách độc lập.
- Khi số kết nối tăng thêm, mạng theo dạng router trở nên kém hiệu quả và cần suy nghĩ đến sự thay đổi.

Chức năng bộ định tuyến

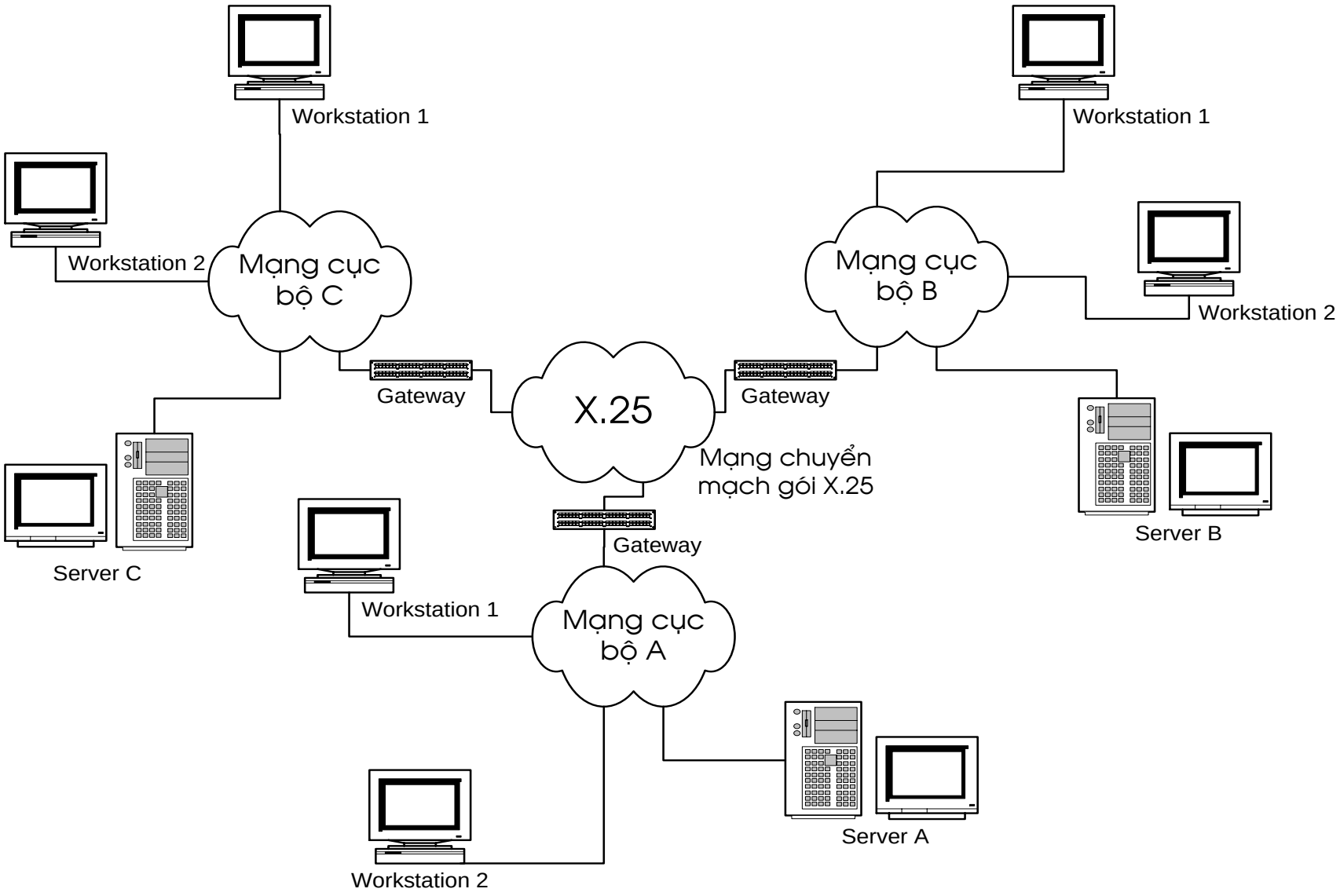
- **Tìm đường**
  - Quá trình tính toán dựa trên địa chỉ IP đích để quyết định sẽ gửi gói tin ra cổng nào.
- **Chuyển gói tin**
  - Đóng gói gói tin lại theo giao thức ở cổng ra và chuyển gói tin ra cổng đó.



1.9.8. Gateway

- Ban đầu thuật ngữ Gateway được dùng trong bộ giao thức Internet để chỉ bộ định tuyến (Router). Ngày nay, Gateway thường được sử dụng để ám chỉ một hệ thống hoạt động tại 3 tầng trên cùng của mô hình OSI (Session, Presentation, Applycation), cho phép truyền thông giữa các hệ giao thức khác nhau của các tầng trên.
- Gateway là một tổ hợp phần cứng và phần mềm để kết nối những máy tính không giống nhau (cả phần cứng và hệ điều hành) và những mạng khác nhau, sử dụng những thủ tục và giao thức khác nhau. Gateway có thể chuyển đổi địa chỉ mạng từ một kiểu mạng này thành một kiểu mạng khác. Kỹ thuật của Gateway phức tạp hơn Bridge và Router.
- Những hệ thống hợp thành mạng Internet được kết nối bởi những mini computer hoạt động như những Gateway, những Gateway này kết nối những vị trí riêng biệt một cách rộng rãi thành kết nối mạng qua một mạng chuyển mạch gói (packet switching) như Telenet hay Tymenet.
- Gateway không chỉ sử dụng cho những kết nối có khoảng cách xa. Nếu ta muốn kết nối hai loại LAN khác nhau (như một mạng Macintosh và một mạng Unix) có thể dùng Gateway để chuyển địa chỉ và dữ liệu. Gateway cũng được dùng để kết nối một Microcomputer và một Mainframe, và những loại Mainframe khác lại với nhau.

Ví dụ Gateway



Liên mạng

2.1. Khái niệm về liên mạng (Internetworking)

- Thuật ngữ "internetworking" là một tập các sử dụng để tạo mối liên kết các thiết bị mạng trung gian, có chức năng như là một mạng đơn
- Một cách chung nhất, internet là một tập hợp các mạng khác nhau
- Các mạng thành phần tạo nên liên mạng được gọi là mạng con (Subnetworks)
- Thuật ngữ "Internet" (chữ I hoa) là đề cập đến mạng Internet toàn cầu, hiện nay là một liên mạng trên phạm vi thế giới kết nối (Enhanced) hoạt động theo chuẩn TCP/IP, tích hợp các dịch vụ đa dạng
- Những thiết bị nối các mạng con lại với nhau được gọi là các thiết bị liên kết liên mạng (Intermediate nodes)

2.1. Khái niệm về liên mạng (Internetworking)

Liên mạng có thể được liên kết bởi LAN to LAN, LAN to WAN và WAN to WAN. Có ba phương pháp liên kết liên mạng phổ biến tương ứng với 3 tầng cuối của mô hình OSI.

1. Phương pháp liên kết tại tầng vật lý

- Các LAN phải cùng cấu trúc và **phương thức trao đổi thông tin**
- Bộ lặp (Repeater) hoặc bộ tập trung (Hub) tầng vật lý được dùng để mở rộng một mạng LAN.

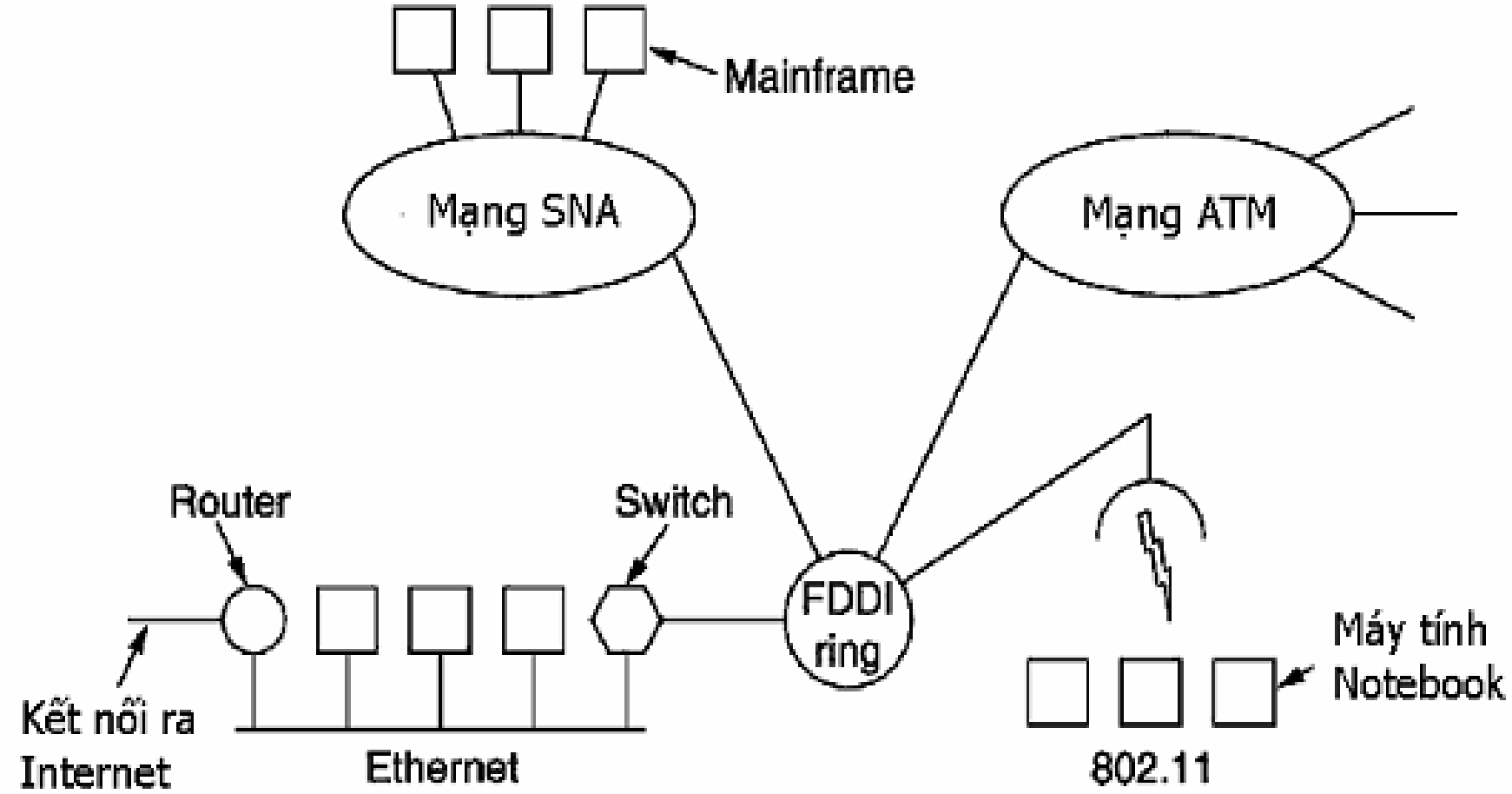
2. Phương pháp liên kết tại tầng liên kết dữ liệu

- Các LAN có cấu trúc khác nhau và **phương thức trao đổi thông tin** khác nhau
- Cầu nối (Bridge) hoặc các bộ chuyển mạch (Switches) ở tầng 2 được sử dụng tại tầng liên kết dữ liệu.
- Những thiết bị này hỗ trợ cho các giao thức tầng vật lý khác nhau và có thể liên kết giữa các mạng LAN có cấu trúc khác nhau

3. Phương pháp liên kết tại tầng mạng (Network Layer) hoặc tầng Internet (Internet Layer)

- Có thể sử dụng tầng mạng (Network Layer) hay tầng Internet (Internet Layer) cho các mạng khác nhau về phần cứng, khác nhau về phần mềm, khác nhau về giao thức và thường cung cấp những chức năng và ứng dụng khác nhau
- Thiết bị liên kết liên mạng trợ giúp cho các giao thức mạng như IP, IPX, Apple Talk

Minh họa liên mạng



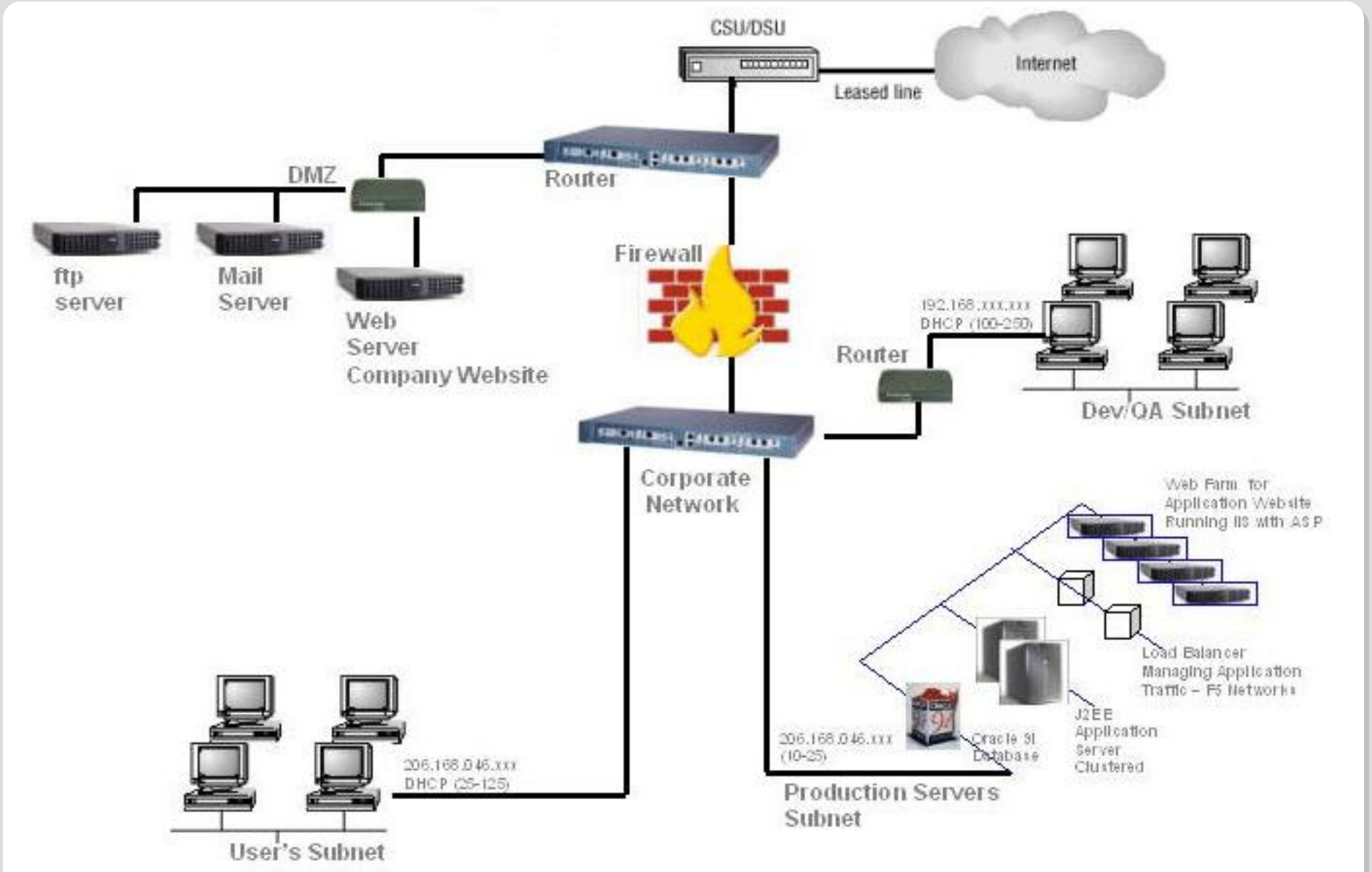
2.2. Mạng diện rộng (WAN)

- Mạng WAN được thiết lập để liên kết các máy tính của hai hay nhiều khu vực khác nhau, ở khoảng cách xa về mặt địa lý, như giữa các quận trong một thành phố, hay giữa các thành phố hay các miền trong nước
- Mạng WAN bao phủ vùng địa lý rộng lớn có thể là một quốc gia, một lục địa hay toàn cầu
- Mạng WAN thường là kết nối các công ty đa quốc gia hay toàn cầu
- WAN là tập hợp các LAN, MAN nối lại với nhau bằng các phương tiện như: vệ tinh (satellites), sóng viba (microwave), cáp quang, cáp điện thoại...

2.3. Đặc trưng của WAN

- WAN có thể kết nối thiết bị LAN, MAN lại với nhau, chúng có thể phức tạp và kết nối qua nhiều hạ tầng mạng của các tổ chức khác nhau
- WAN có thể cung cấp băng thông từ thấp đến cao tùy theo nhu cầu của người sử dụng
- WAN có thể kết nối thiết bị LAN, MAN lại với nhau trên một khoảng cách rất lớn từ hàng trăm đến hàng ngàn km
- WAN thường hoạt động ở tốc độ thấp hơn so với mạng LAN do tốc độ truyền dẫn trên đường truyền
- WAN có thể hoạt động ở tốc độ thấp hoặc cao tùy theo nhu cầu của người sử dụng
- WAN thường hoạt động ở tốc độ thấp hơn so với mạng LAN do tốc độ truyền dẫn trên đường truyền
- Một số công nghệ WAN hiện nay có thể hoạt động ở tốc độ rất lớn từ 56Kbps đến T1 với 1.544 Mbps hay E1 với 2.048 Mbps,....và đến Gigabit-Gbps
- Phần lớn các WAN hiện nay được phát triển cho việc truyền tải dữ liệu trên một cáp quang hay hạ tầng truyền dẫn khác nhau như: video, tiếng nói, dữ liệu...nhằm làm giảm chi phí dịch vụ

Minh họa kết nối WAN



2.4. Các lợi ích và chi phí khi kết nối WAN

- Khi đó, mạng của các chi nhánh sẽ là hệ thống trao đổi thông tin chính của cơ quan hay tổ chức
- Nó giúp tăng cường và thay đổi về chất công tác quản lý và trao đổi thông tin, tiến bước vững chắc tới một nền thương mại điện tử (e-commerce), chính phủ điện tử (e-goverment) trong tương lai không xa

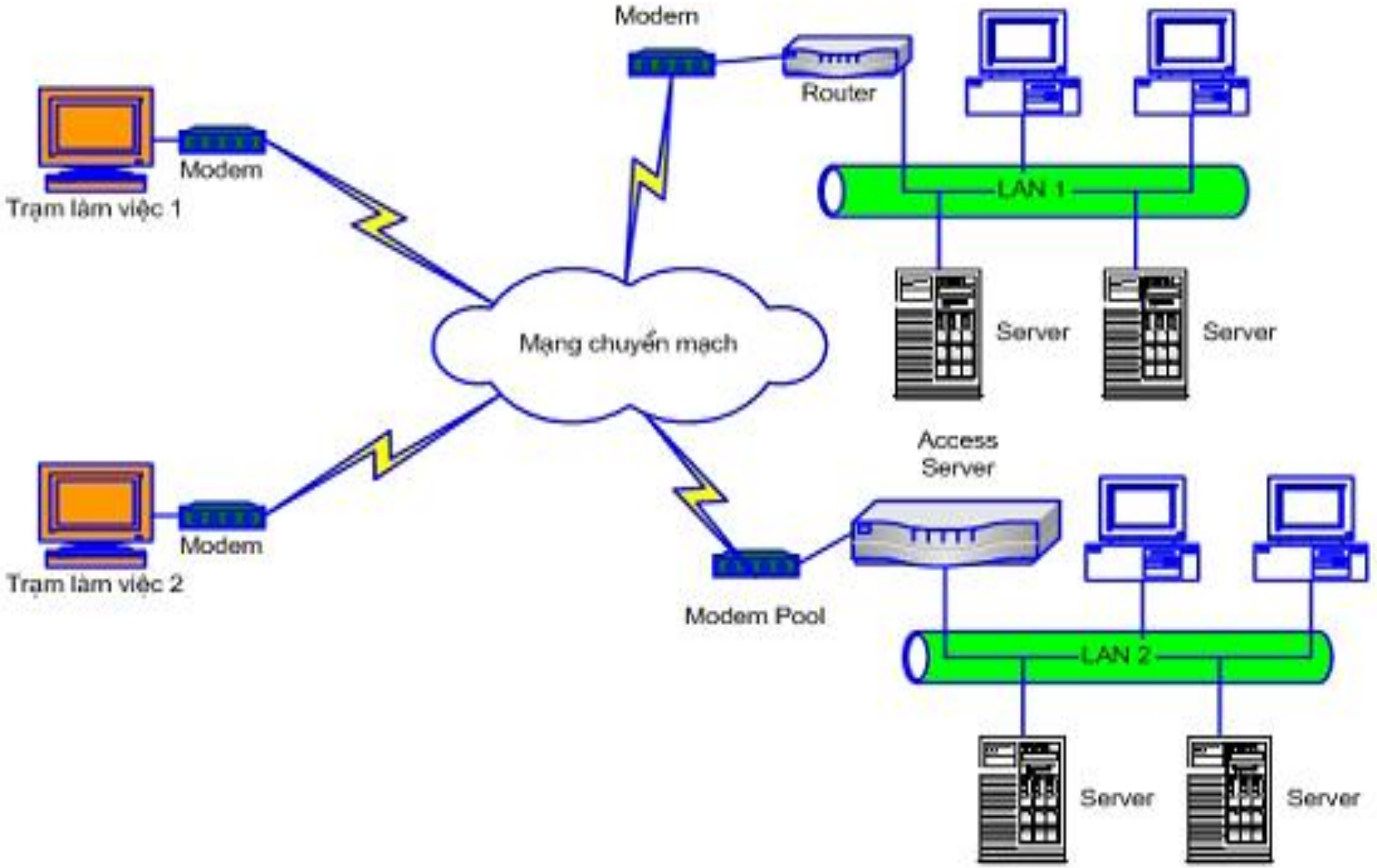
2.5. Một số công nghệ kết nối WAN cơ bản

- Mạng chuyển mạch kênh (Circuit Swiching Network)
- Mạng chuyển gói (Packet Switching Network)
- Kết nối WAN dùng mạng riêng ảo (Virtual Personal Network)
- Các thiết bị dùng cho WAN

2.5.1. Mạng chuyển mạch kênh

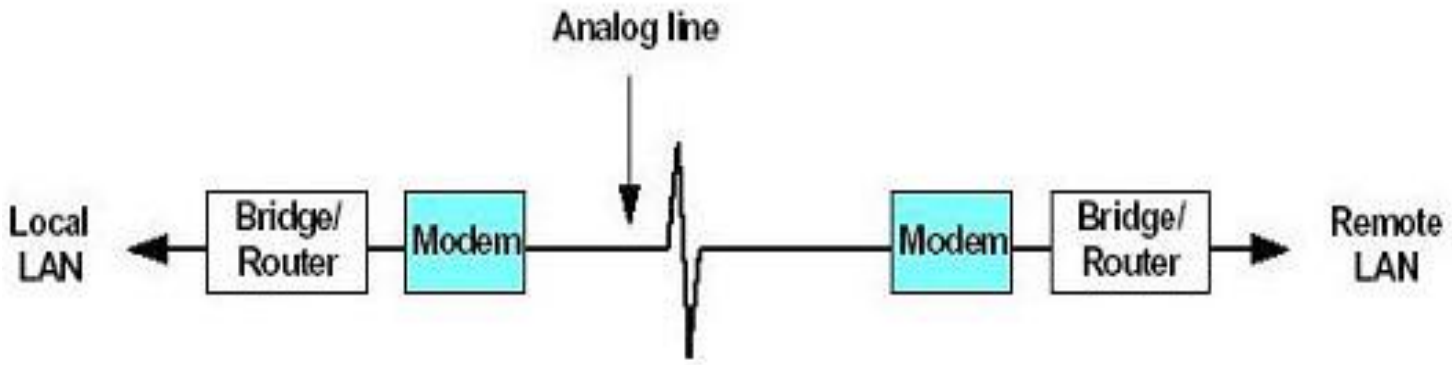
- Kết nối này được thực hiện bằng cách thiết lập một liên kết vật lý giữa hai điểm
- Liên kết này tồn tại trong suốt phiên làm việc của hai điểm
- Liên kết này được gọi là liên kết tạm thời hay liên kết riêng
- Để thực hiện một phiên làm việc cần có các thủ tục điều khiển cuộc gọi
- Trong mô hình này trước khi truyền dữ liệu cần thiết lập một đường liên kết tạm thời giữa hai thiết bị cung cấp thông báo cho mạng biết địa chỉ của nút gửi và nút nhận
- Với mô hình này mọi nút mạng có thể kết nối với bất kỳ một nút khác
- Hiện nay có 2 loại mạng chuyển mạch kênh
  - chuyển mạch tương tự (analog)
  - chuyển mạch số (digital)
- Thông qua những đường nối và các thiết bị chuyên dùng người ta có thể tạo ra một liên kết tạm thời từ nơi gửi tới nơi nhận

Mô hình kết nối WAN dùng mạng chuyển mạch kênh



a. Chuyển mạch tương tự (Analog)

- Việc chuyển dữ liệu qua mạng chuyển mạch tương tự được thực hiện qua mạng điện thoại
- Các trạm trên mạng sử dụng modem, thiết bị này sẽ chuyển các tín hiệu số từ máy tính sang tín hiệu tương tự có thể truyền dữ liệu đi trên các kênh điện thoại và ngược lại biến tín hiệu dạng tương tự thành tín hiệu số
- Một minh họa kết nối dùng mạng chuyển mạch qua mạng điện thoại PSTN, hay còn gọi là kết nối quay số (dial-up).

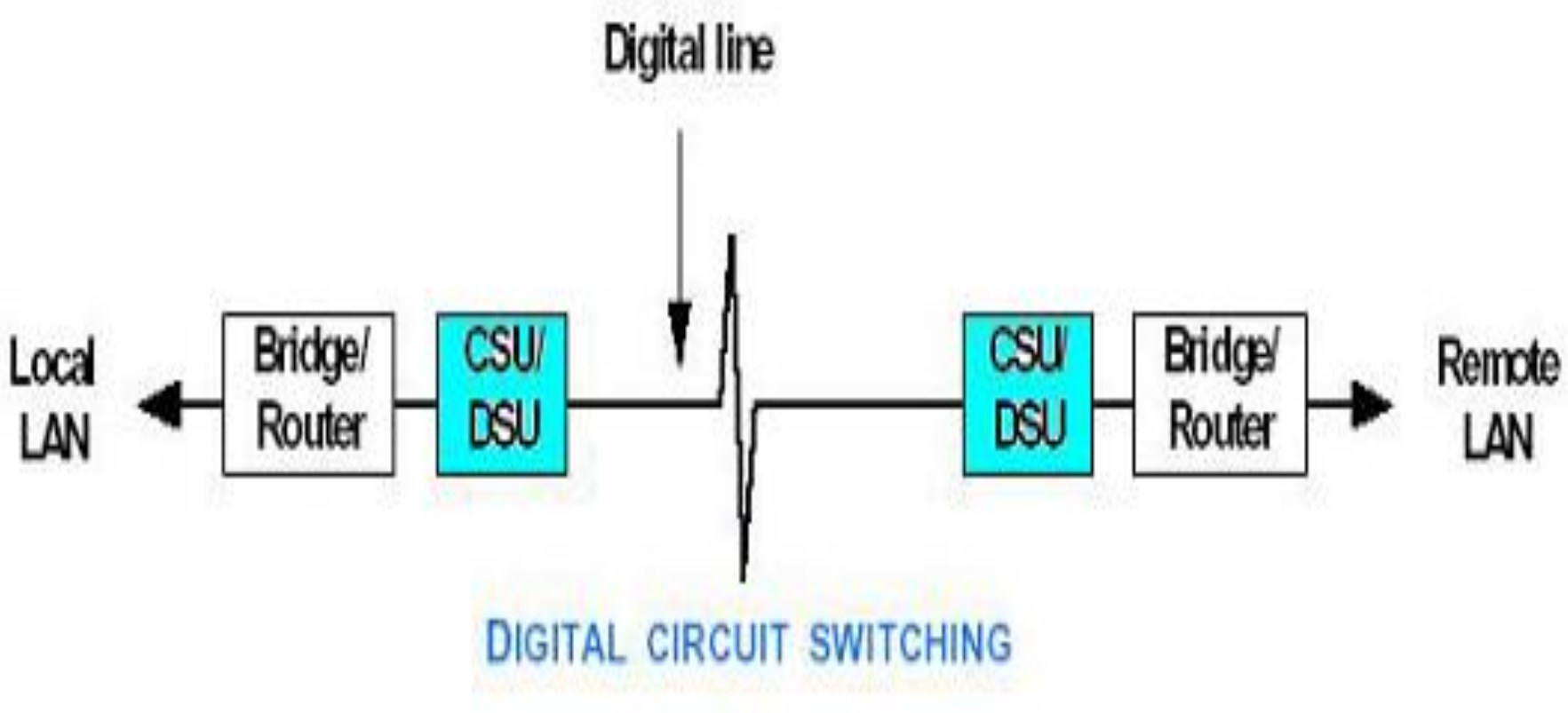


ANALOG CIRCUIT-SWITCHING

b. Mạng chuyển mạch số (Digital)

- ISDN - Integrated Service Digital Network: hệ thống viễn thông số tích hợp đa dịch vụ (PSTN)
- Kết nối tốc độ cao: Digital Network: hầm một loại hệ thống viễn thông số tích hợp đa dịch vụ điện thoại thường
- Tốc độ truy cập mạng WAN có thể lên đến 128 Kbps nếu sử dụng 2 kênh và tương thích với ISDN là giải pháp cho phép truyền thoại, dữ liệu và hình ảnh tốc độ cao
- Với cơ sở hạ tầng hiện có, ISDN là giải pháp sử dụng đường dây điện thoại thông thường
- Người dùng cùng một lúc có thể truy cập WAN và gọi điện thoại, fax mà chỉ cần một đường dây điện thoại duy nhất, thay vì 3 đường nếu dùng theo kiểu thông thường

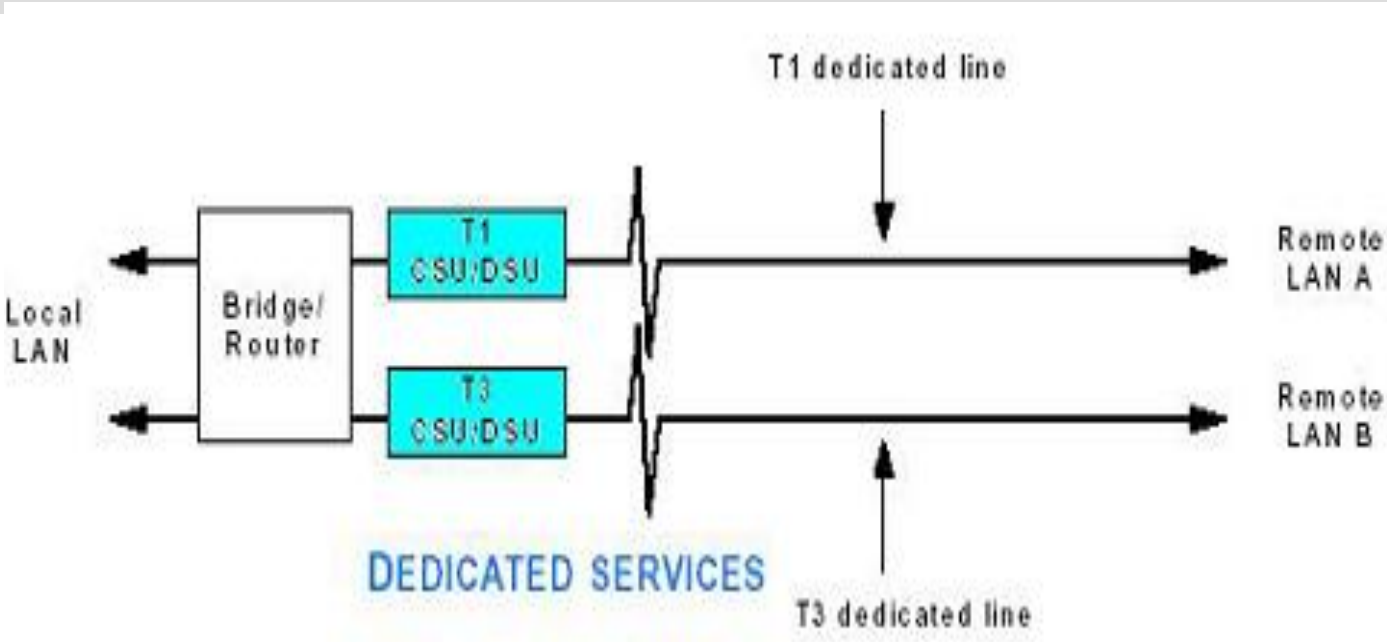
Mạng chuyển mạch số (Digital)



c. Mạng kênh thuê riêng (Leased lines Network)

- Cách kết nối phổ biến nhất hiện nay giữa hai điểm có khoảng cách lớn vẫn là Leased Line (thuê bao riêng)
- 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
- Vì vậy: khi số lượng các trạm sử dụng tăng cao ta 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
  - Phương thức ghép kênh theo tần số (Frequence Division Multiplexing - FDM)
  - Phương thức ghép kênh theo thời gian (Time Division Multiplexing - TDM)

Mạng kênh thuê riêng



Loại kênh	Thông lượng	Ghép kênh
T0	56 Kbps	1 đường thoại
T1	1.544 Mbps	24 đường T0
T2	6.312 Mbps	4 đường T1
T3	44.736 Mbps	28 đường T1
T4	274.176 Mbps	168 đường T1

Các công nghệ xDSL

- xDSL (Asymmetric Digital Subscriber Line) là công nghệ cho phép việc kết nối Internet được thực hiện dễ dàng thông qua đường dây điện thoại thông thường. Trên đường dây điện thoại, tín hiệu thoại chỉ dùng tần số rất nhỏ từ 0KHz đến 20KHz để truyền dữ liệu âm thanh (điện thoại)
- Việc kết nối Internet tốc độ cao thông qua đường dây điện thoại thông thường đã được thực hiện từ lâu bằng modem kỹ thuật số không đối xứng là một công nghệ mới nhất cung cấp kết nối tới các thuê bao qua đường cáp điện thoại với tốc độ cao cho phép người sử dụng kết nối Internet 24/24 mà không ảnh hưởng đến việc sử dụng điện thoại và fax
- Để vượt qua ngưỡng tốc độ người ta chuyển sang dùng kỹ thuật số xDSL (Digital Subscriber Line)
- Công nghệ này tận dụng hạ tầng cáp đồng điện thoại hiện có để cung cấp kết nối truyền dữ liệu số tốc độ cao
- ADSL là một chuẩn được Viện tiêu chuẩn quốc gia Hoa Kỳ thông qua năm 1993 và gần đây đã được Liên minh viễn thông quốc tế ITU công nhận và phát triển
- Công nghệ DSL tận dụng đặc điểm này để truyền dữ liệu trên cùng đường dây, nhưng ở tần số 25.875 KHz đến 1.104 MHz

2.5.2. Mạng chuyển gói (Packet Switching Network)

- Mạng chuyển mạch gói hoạt động theo nguyên tắc: Khi một trạm cần gửi dữ liệu nó 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 vậy: khi một trạm không gửi tin thì mọi tài nguyên của mạng sẽ dành cho các trạm khác, nên mạng tiết kiệm được tài nguyên và có thể sử dụng chúng một cách tốt nhất
- Có 2 phương thức chuyển mạch gói:
  - Phương thức chuyển mạch gói theo sơ đồ rời rạc
  - Phương thức chuyển mạch gói theo đường đi xác định

a. 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 nơi gửi và nơi nhận
- Mỗi nút trong mạng khi tiếp nhận gói tin sẽ quyết định xem 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

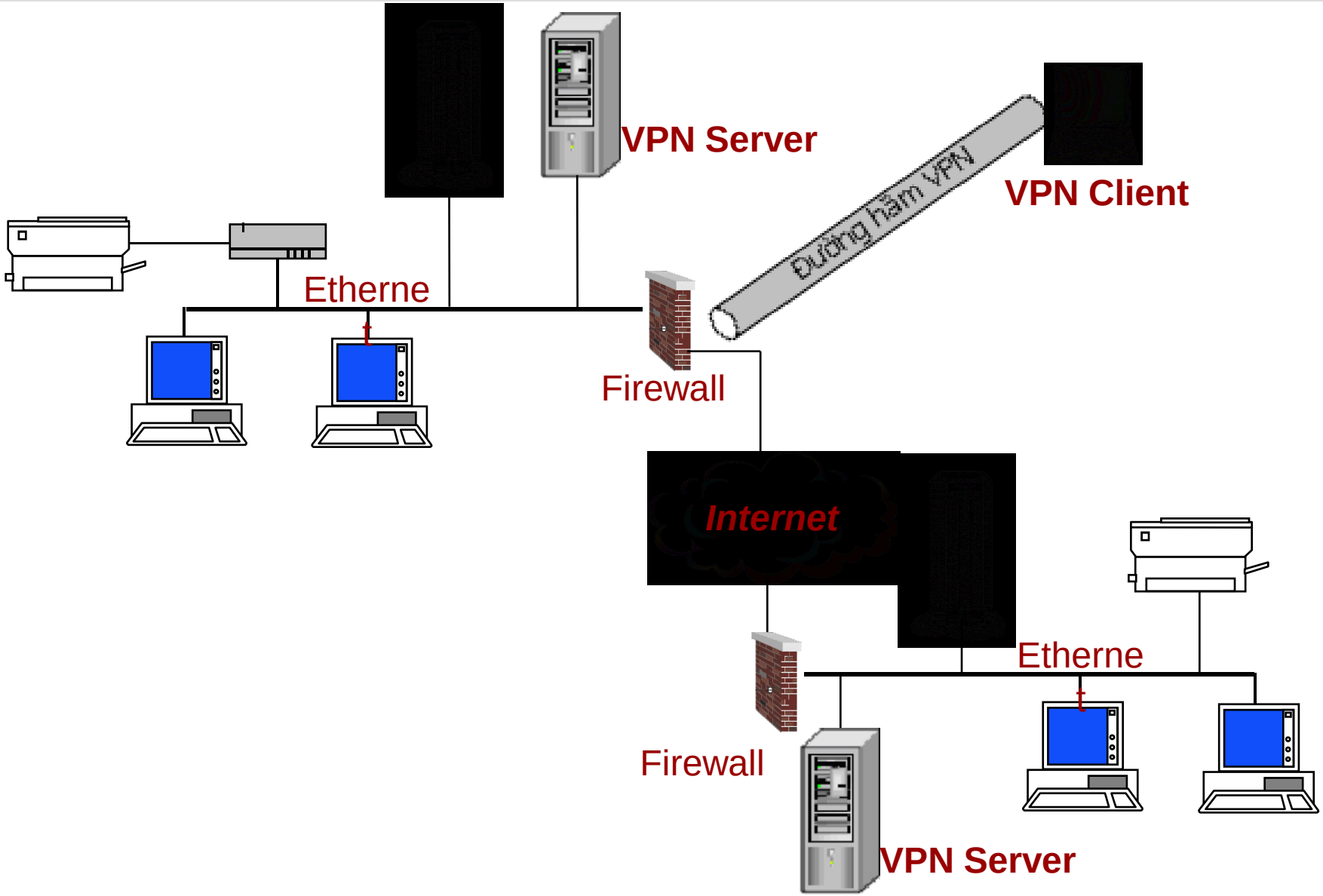
b. Phương thức chuyển mạch gói theo đường đi xác định

- 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 của 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

2.5.3. Kết nối WAN dùng mạng riêng ảo (VPN)

- VPN (Virtual Personal Network) là một mạng riêng được xây dựng trên nền tảng hạ tầng mạng công cộng (như là mạng Internet)
- Mạng IP riêng (VPN) là một dịch vụ mạng có thể dùng cho các ứng dụng khác nhau, cho phép việc trao đổi thông tin một cách an toàn với nhiều lựa chọn kết nối
- Giải pháp VPN cho phép người sử dụng làm việc tại nhà hoặc đang đi công tác ở xa có thể thực hiện một kết nối tới trụ sở chính của mình, bằng việc sử dụng hạ tầng mạng thông qua việc tạo lập một kết nối nội hạt tới một ISP. Khi đó, một kết nối VPN sẽ được thiết lập giữa người dùng với mạng trung tâm của họ

Một mạng riêng ảo



2.5.4. Các thiết bị dùng cho kết nối WAN

- Router (Bộ định tuyến)
- WAN Switch (Chuyển mạch WAN)
- Access Server
- Modem
- CSU/DSU (Channel Service Unit/Data Service Unit)
- ISDN Terminal Adaptor:

Thiết bị chuyển mạch WAN (WAN switch) là thiết bị nhiều cổng liên mạng (multiport internetworking device) dùng trong các

Là thiết bị phần cứng tại các điểm đầu cuối của các kênh thuê riêng. Nó làm nhiệm vụ chuyển dữ liệu trên đường truyền thuê bao số đến thiết bị LAN hay ngược lại. Thường dùng để kết nối WAN khi dùng các kênh thuê riêng

Là thiết bị đầu cuối để kết nối máy tới mạng ISDN

2.6. Đánh giá công nghệ dùng cho kết nối WAN

- Hiện nay việc làm sao có được một hệ thống mạng chạy thật tốt, thật an toàn với chi phí hợp lý, và mang lại lợi ích kinh tế cao, đang rất được quan tâm
- Một vấn đề đặt ra có rất nhiều giải pháp về công nghệ, mỗi 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

2.6. Đánh giá công nghệ dùng cho kết nối WAN

- Trong thiết kế WAN thì công nghệ kết nối là vấn đề cơ bản nhất cần được xem xét, đánh giá và lựa chọn hợp lý
- Kết nối PSTN (mạng điện thoại công cộng): Kết nối WAN qua mạng điện thoại công cộng có ưu điểm là đơn giản, dễ thực hiện, nhưng nhược điểm lớn nhất là hạn chế về tốc độ, và độ tin cậy thấp. Chỉ dùng hiệu quả cho các thuê bao có thời gian kết nối dưới 4 giờ/ngày
- Kết nối ISDN (mạng dịch vụ tổng hợp): Kết nối WAN qua mạng đa dịch vụ số ISDN có ưu điểm là ổn định hơn qua mạng điện thoại công cộng, nhưng lại chịu chi phí cao hơn, và là loại kết nối không phổ biến. Chỉ thực hiện được tại các địa phương mà tổng đài hỗ trợ dịch vụ ISDN

2.6. Đánh giá công nghệ dùng cho kết nối WAN

- Kết nối FRAME RELAY: Để sử dụng Frame Relay là chất lượng mạng truyền dẫn phải cao
- Tuy nhiên, ở những nơi đã triển khai công nghệ Frame Relay thì việc xem xét chọn giải pháp kết nối WAN dùng Frame Relay là hoàn toàn chấp nhận được, cần được xem xét và triển khai
- Kết nối sử dụng công nghệ xDSL: Như phần lớn công nghệ khác, tiềm năng trên lý thuyết của công nghệ DSL có sự khác biệt đáng kể đối với tốc độ kết nối WAN cho các tổ chức và giới doanh nghiệp hiện nay

2.6. Đánh giá công nghệ dùng cho kết nối WAN

- Các chuyên gia công nghệ cho biết đã có những hoàn thiện đáng kể trong chất lượng đường truyền theo công nghệ xDSL
- Vì thế lượng khách hàng thuê bao sử dụng dịch vụ xDSL vẫn không ngừng tăng lên
- Việc kết nối sử dụng xDSL ở những doanh nghiệp từ khoảng 1999 là bước hậu thuẫn cho việc sử dụng công nghệ ADSL hiện nay (công nghệ DSL không đối xứng) với tốc độ truy cập từ 512 Kbps đến 8 Mbps

Kết luận chương 3

- Khái niệm, đặc điểm, tốc độ của mạng LAN.
- Các hình trạng và mô hình mạng cục bộ. Ưu, nhược điểm của từng mô hình.
- Các kỹ thuật, phương thức truyền tín hiệu.
- Phương thức đa truy nhập sử dụng sóng mang có phát hiện xung đột CSMA/CD. Ưu, nhược điểm của từng giải thuật trong CSMA/CD.
- Token Bus: Thiết lập vòng logic, duy trì trạng thái thực tế của mạng và khởi tạo vòng logic khi cài đặt mạng hoặc đứt vòng.
- Token ring, nguyên tắc của phương pháp. Cần giải quyết hai vấn đề có thể dẫn đến phá vỡ hệ thống.

Kết luận chương 3

- So sánh CSMA/CD với các phương pháp dùng thẻ bài.
- So sánh phương thức Token Bus và Token Ring.
- Ethernet và chuẩn IEEE 802
- Giới thiệu chung về Ethernet. Thành phần mạng Ethernet, những đặc điểm cơ bản của mạng Ethernet.
- Ethernet 100 Mbps và Gigabit Ethernet.
- Mạng cục bộ Token Ring. Chuẩn Token Ring.
- Giao diện số liệu phân bố sử dụng quang FDDI.
- Mạng LAN ATM.
- Đặc điểm HĐH mạng, các loại HĐH mạng.
- Thiết bị kết nối LAN.

Kết luận chương 3

- Khái niệm liên mạng, Internet.
- Khái niệm, đặc trưng WAN.
- Các lợi ích và chi phí khi kết nối WAN.
- Có những kỹ thuật chuyển mạch nào, so sánh kỹ thuật chuyển mạch trong WAN.
- Kết nối WAN dùng VPN.
- Các thiết bị dùng cho kết nối WAN.

Thanksss

CHƯƠNG 4
TCP/IP

Nội dung

I. Giới thiệu mô hình kiến trúc TCP/IP.

II. Một số giao thức cơ bản của bộ giao thức TCP/IP

III. Một số hạn chế của giao thức IPv4 và nguyên nhân ra đời IPv6

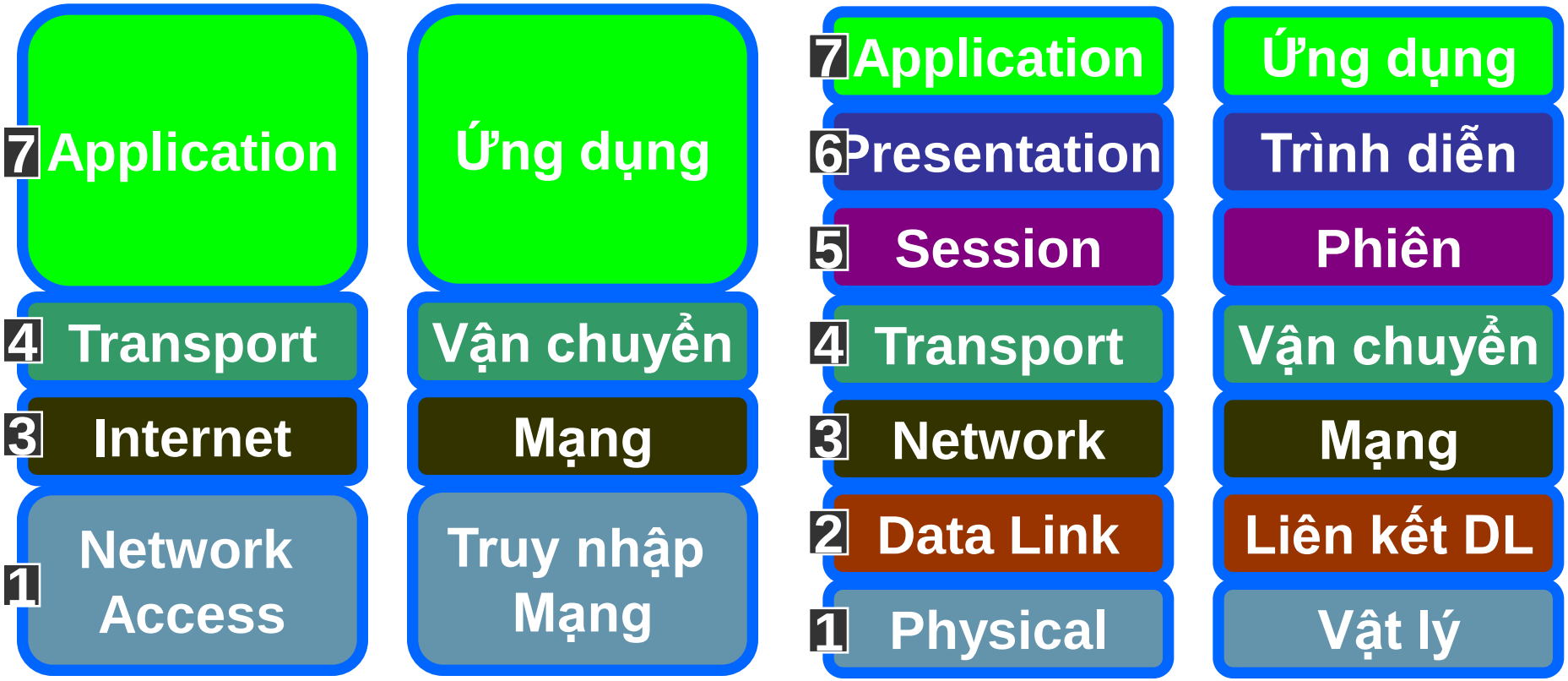
IV. Các lớp địa chỉ IPv6

V. Kết luận chương

I. Mô hình kiến trúc TCP/IP

- Năm 1981, TCP/IP phiên bản 4 (IPv4) được hoàn thành và chính thức trở thành phương tiện truyền thông liên mạng
- Sau này, trở thành một trong những giao thức cơ bản của Internet
- Năm 1983, TCP/IP được tích hợp vào hệ điều hành UNIX 4.2 BSD
- Năm 1990, ARPA giải thể, Internet trở thành mạng máy tính toàn cầu
- Năm 1991, TCP/IP phiên bản 4 (IPv4) được hoàn thành và chính thức trở thành phương tiện truyền thông liên mạng
- Sau này, trở thành một trong những giao thức cơ bản của Internet
- Năm 1993, DARPA đã phát triển TCP/IP để kết nối các mạng máy tính thuộc bộ quốc phòng Mỹ
- Năm 1994, một phiên bản mới IPv6 được hình thành trên cơ sở tiếp nhận những thành tựu của IPv4
- Internet là mạng máy tính toàn cầu sử dụng TCP/IP kết nối các mạng trên thế giới+cung cấp các dịch vụ

I.1. Mô hình kiến trúc TCP/IP



I.2. Vai trò và chức năng các tầng:

A. Tầng Ứng dụng (Application)

- Kết hợp chức năng của ba tầng phiên, trình bày, ứng dụng trong mô hình OSI.
- Tầng ứng dụng hỗ trợ các ứng dụng cho các giao thức tầng Host to Host.
- Các giao thức ứng dụng gồm:
  - FTP, HTTP, SMTP, SNMP, DNS, TELNET ...
  - Định dạng dữ liệu, cấu trúc dữ liệu, mã hoá …
  - Điều khiển đối thoại …

I.2. Vai trò và chức năng các tầng:

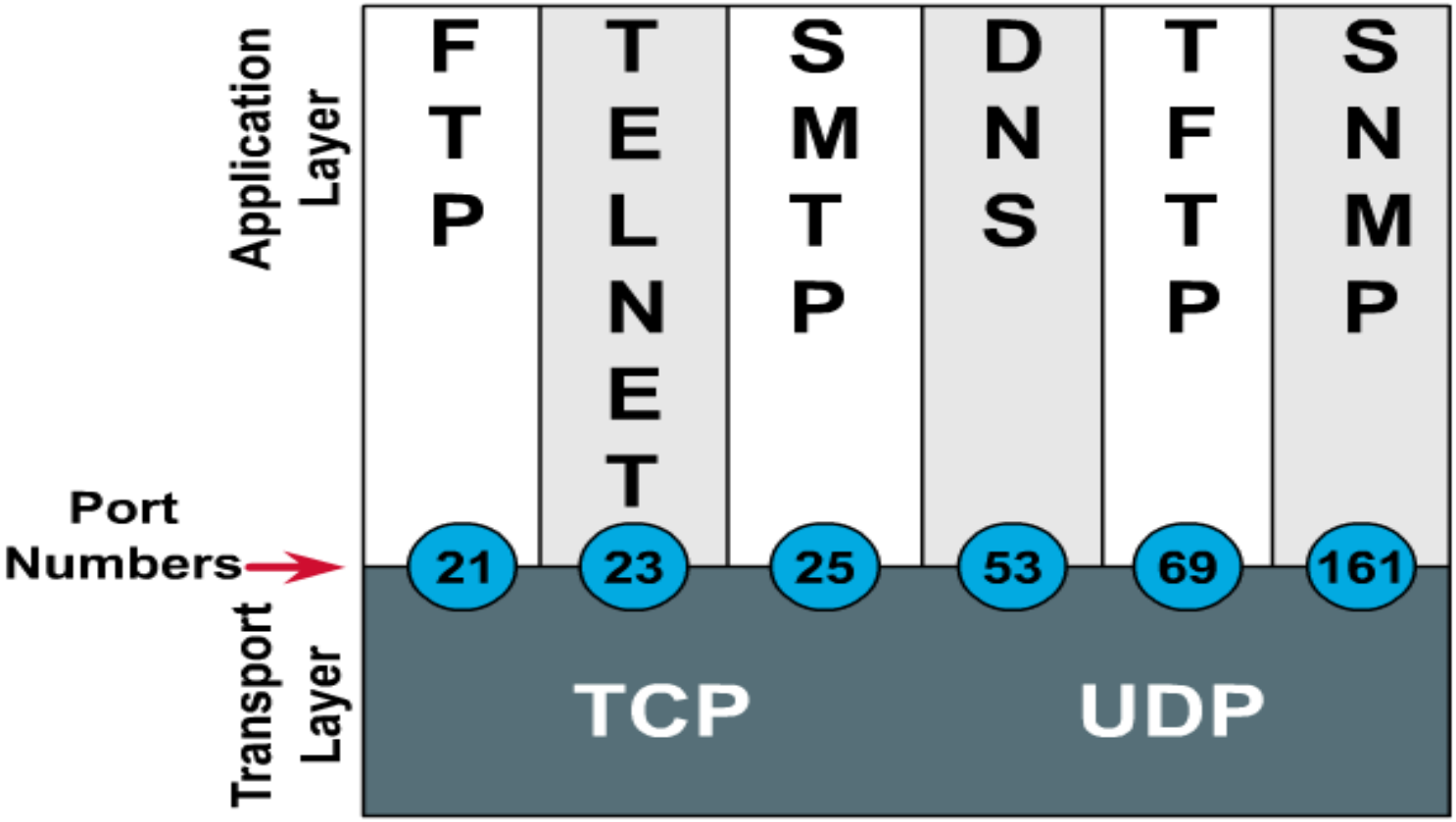
B. Tầng Vận chuyển (Transport)

- Tầng vận chuyển liên quan đến chất lượng dịch vụ như độ tin cậy, điều khiển lưu lượng và sửa lỗi (tương tự tầng vận chuyển mô hình OSI).
- Thực hiện những kết nối giữa hai máy chủ trên mạng bằng 2 giao thức:
  - Giao thức điều khiển trao đổi dữ liệu TCP (Transmission Control Protocol): là giao thức kết nối hướng liên kết (Connection - Oriented) chịu trách nhiệm đảm bảo tính chính xác và độ tin cậy cao trong việc trao đổi dữ liệu giữa các thành phần của mạng. Giao thức TCP cũng hỗ trợ những kết nối đồng thời, phân đoạn, dòng dữ liệu, điều khiển luồng, phát hiện và sửa lỗi.
  - Giao thức gam dữ liệu người sử dụng UDP (User Datagram Protocol): được sử dụng cho những ứng dụng không đòi hỏi độ tin cậy cao.

I.2. Vai trò và chức năng các tầng:

Các cổng (ports)

- TCP và UDP sử dụng số hiệu cổng (hoặc socket) để truyền dữ liệu lên giao thức lớp trên



I.2. Vai trò và chức năng các tầng:

c. Tầng Internet

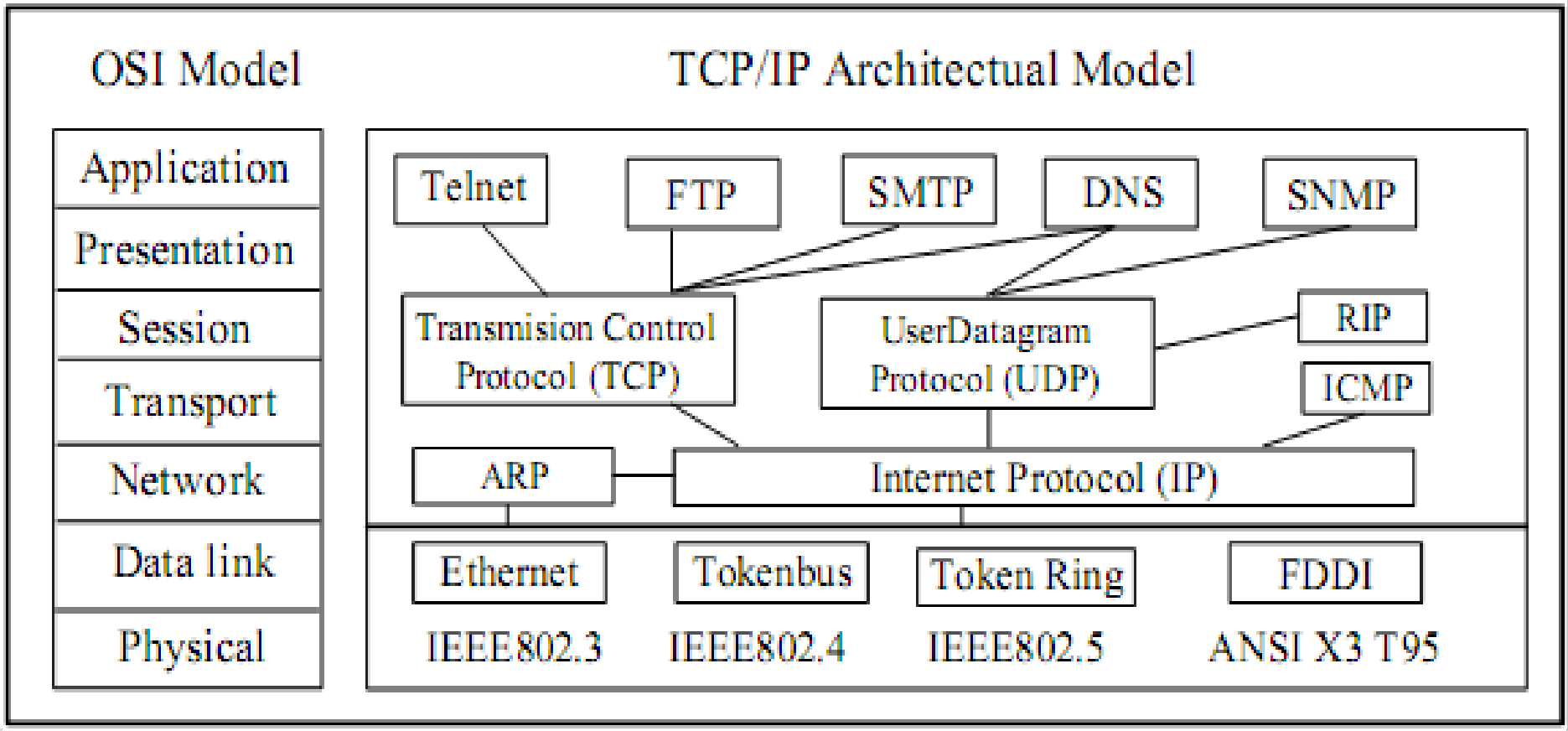
- Gửi dữ liệu đến đích qua các mạng con (tương tự tầng mạng mô hình OSI).
  - Chia nhỏ dữ liệu thành các gói
  - Sử dụng mạch ảo trong kết nối
  - Tìm đường, bảng tìm đường, giao thức tìm đường
  - Cung cấp địa chỉ logic cho giao diện vật lý mạng
  - Sự phân đoạn mạng
  - Giao thức Internet (IP) kết nối không liên kết (Connectionless).
  - Hỗ trợ các ánh xạ giữa địa chỉ vật lý (MAC) do tầng Network Access Layer cung cấp với địa chỉ logic bằng các giao thức phân giải địa chỉ ARP (Address Resolution Protocol) và phân giải địa chỉ đảo RARP (Reverse Address Resolution Protocol).

I.2. Vai trò và chức năng các tầng:

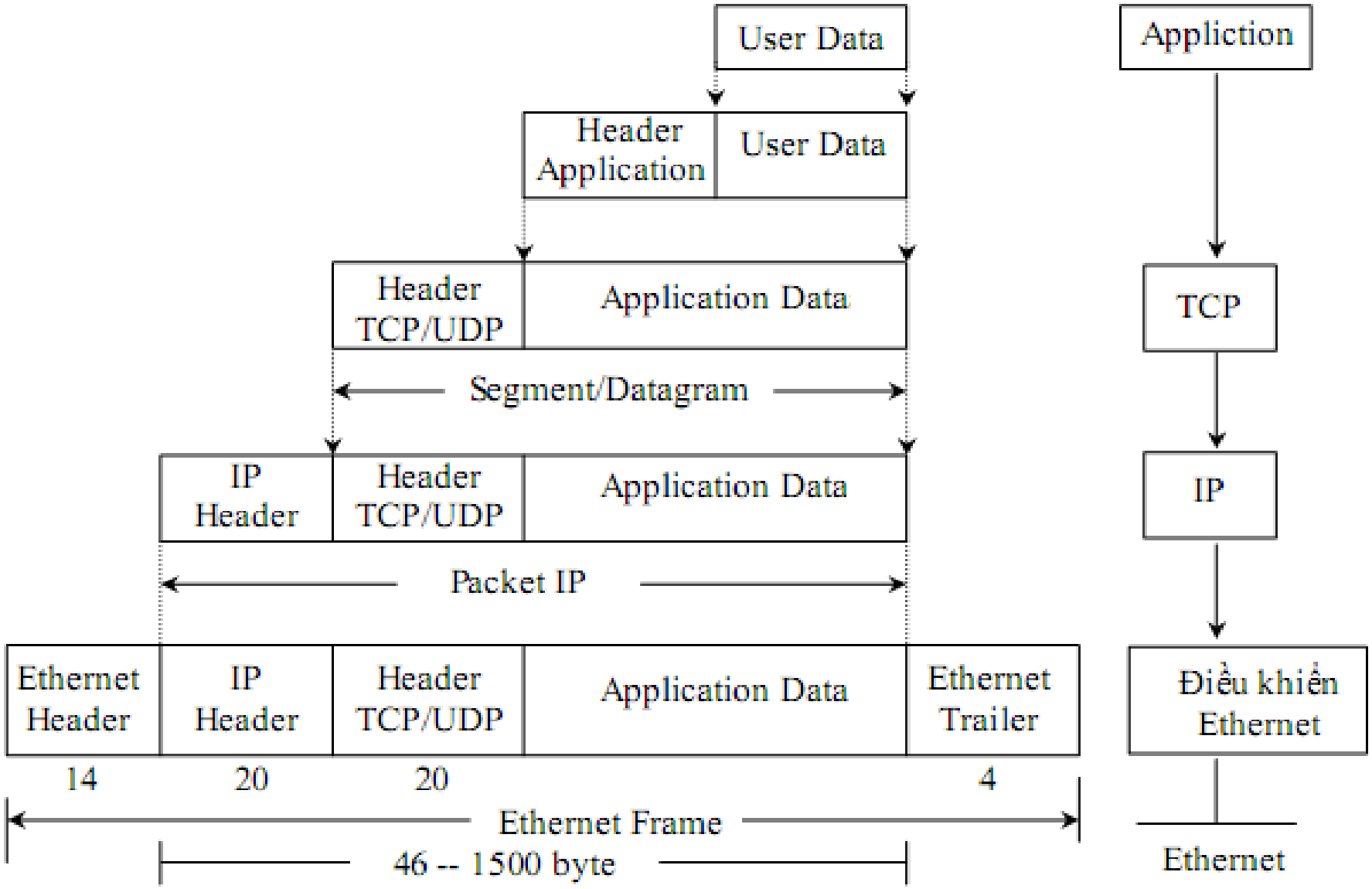
D. Tầng Truy nhập mạng (Network Access)

- Kết hợp chức năng hai tầng vật lý và liên kết dữ liệu mô hình OSI, bao gồm:
  - Cung cấp các chức năng, thủ tục, cơ chế, phân đoạn dữ liệu thành các khung.
  - Tốc độ truyền vật lý, khoảng cách.
  - Địa chỉ vật lý
  - Cung cấp các phương tiện kết nối vật lý: cáp, bộ chuyển đổi (Transceiver), Card mạng.
  - Quy định các giao thức kết nối, giao thức truy nhập đường truyền (CSMA/CD, Token Ring, Token Bus…).
  - Điều khiển lỗi, điều khiển lưu lượng.

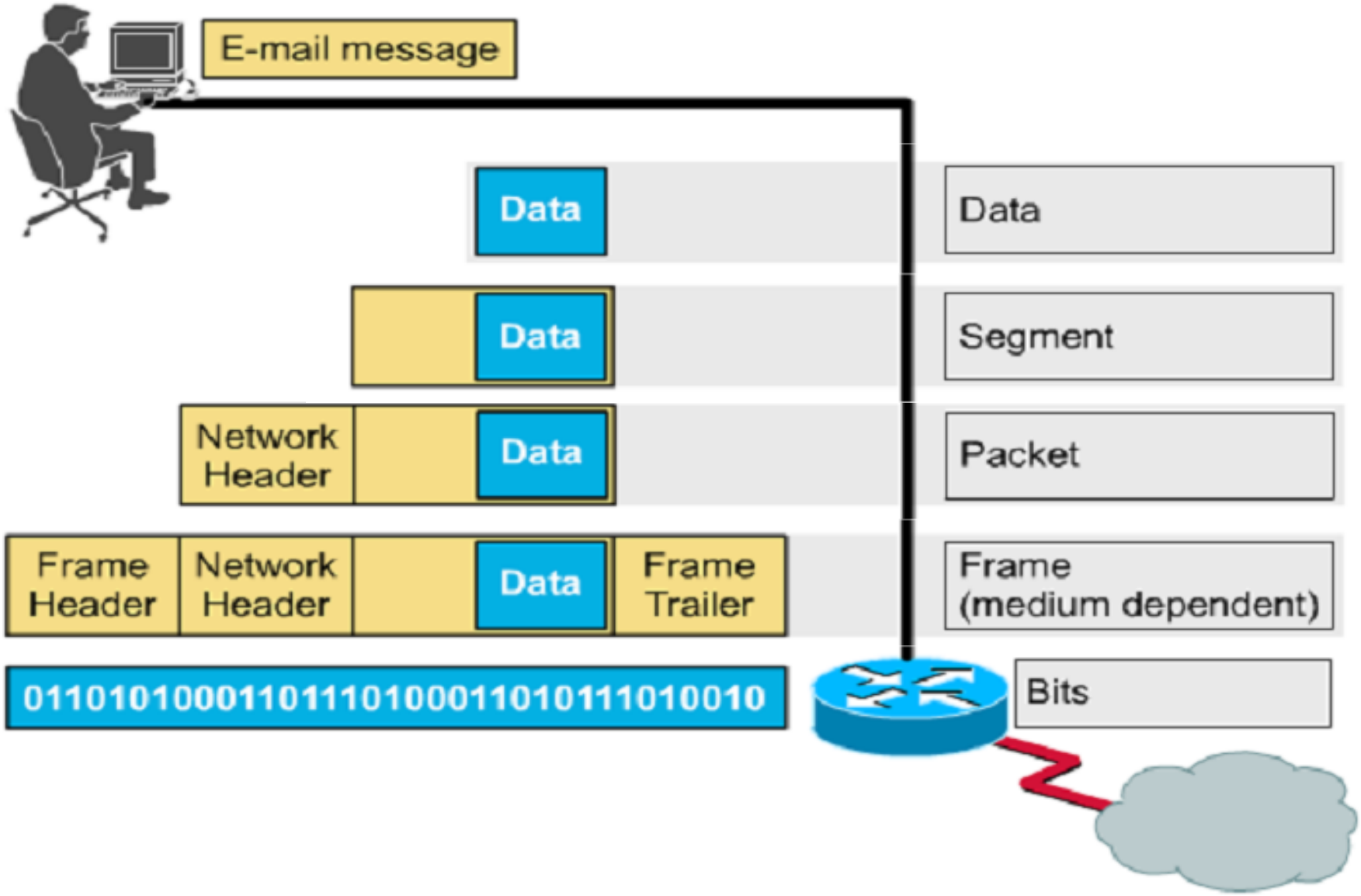
I.3. So sánh TCP/IP và OSI



I.4. Quá trình đóng gói dữ liệu (Encapsulation)



I.4. Quá trình đóng gói dữ liệu (Encapsulation)



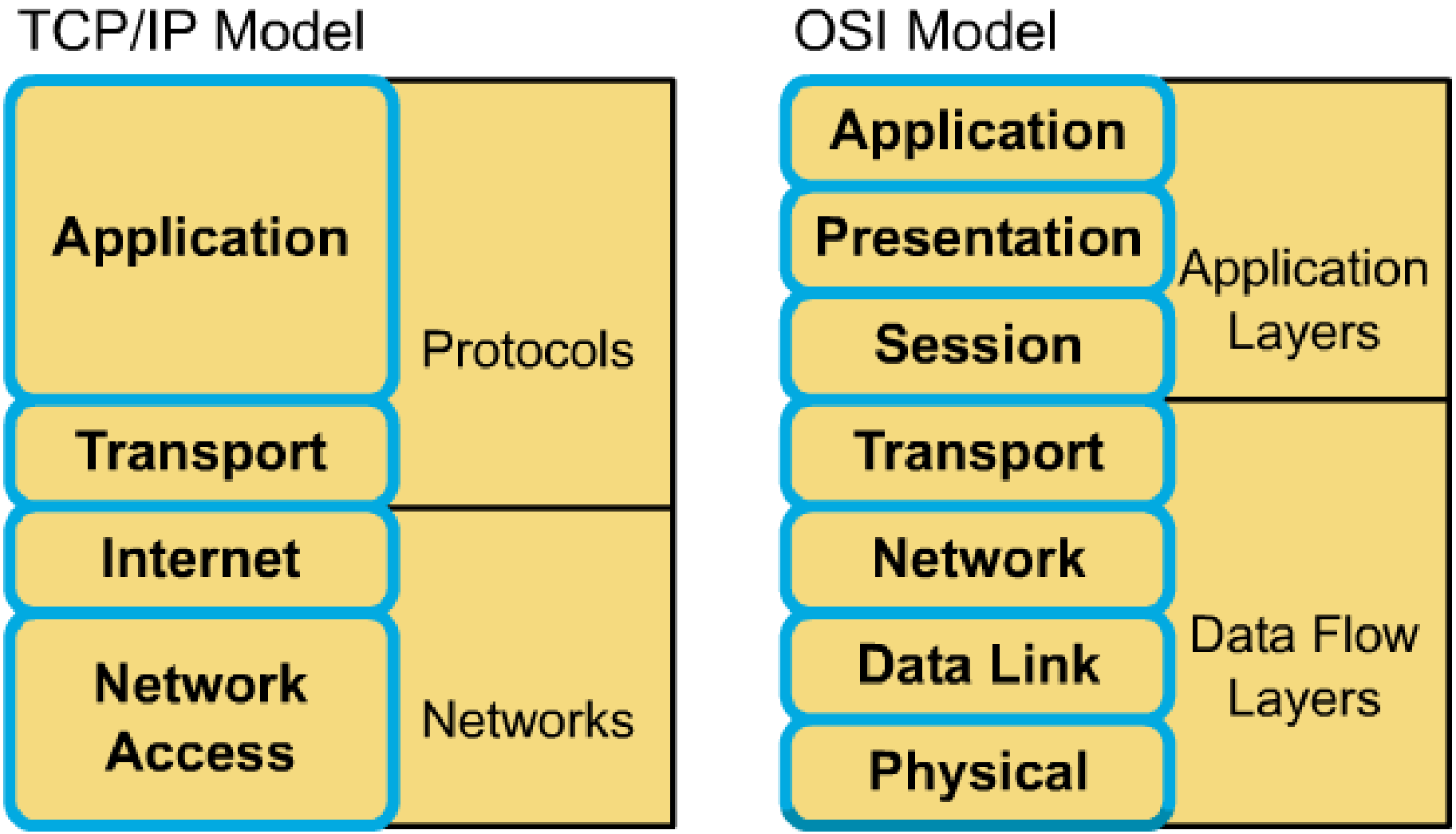
I.5. Quá trình phân mảnh dữ liệu (Fragment)

- Dữ liệu có thể được truyền qua nhiều mạng khác nhau
- Kích thước dữ liệu cho phép cũng khác nhau
- Kích thước lớn nhất của gói dữ liệu trong mạng gọi là đơn vị truyền cực đại MTU (Maximum Transmission Unit)
- Quá trình phân mảnh làm tăng thời gian xử lý, làm giảm tính năng của mạng và ảnh hưởng đến tốc độ trao đổi dữ liệu trong mạng. Hậu quả của nó là các gói bị phân mảnh sẽ đến đích chậm hơn so với các gói không bị phân mảnh.
- Mặt khác, vì IP là một giao thức không liên kết, độ tin cậy không cao, khi một gói dữ liệu bị phân mảnh và bị mất 1 mảnh thì tất cả các mảnh sẽ phải truyền lại. Vì vậy phần lớn các ứng dụng tránh không sử dụng kỹ thuật phân mảnh và gửi các gói dữ liệu lớn nhất mà không bị phân mảnh, giá trị này là Path MTU.

Nếu một thiết bị nhận được một gói dữ liệu có kích thước gói dữ liệu mà nó nhận lớn hơn MTU của nó, dữ liệu sẽ được phân mảnh ra thành gói nhỏ hơn để chuyển tiếp. Quá trình này gọi là quá trình phân mảnh dữ liệu.

Trong quá trình đóng gói, nếu kích thước của một gói lớn hơn kích thước mà mạng cho phép, nó sẽ tự động chia thành nhiều gói nhỏ và thêm thông tin điều khiển vào mỗi gói.

I.6. So sánh TCP/IP và OSI



I.6. So sánh TCP/IP và OSI

- Giống nhau:
  - Đều phân lớp.
  - Đều có lớp ứng dụng.
  - Đều có lớp mạng và lớp vận chuyển
  - TCP/IP đơn giản hơn vì ít lớp hơn
  - Kỹ thuật chuyển mạch gói.
  - Bộ giao thức TCP/IP là chuẩn trên Internet.
  - Các chuyên gia mạng phải nắm rõ cả hai.
- Khác nhau:
  - TCP/IP kết hợp lớp trình bày và phiên vào lớp ứng dụng.
  - TCP/IP kết hợp lớp liên kết dữ liệu và lớp vật lý thành một lớp truy cập mạng.

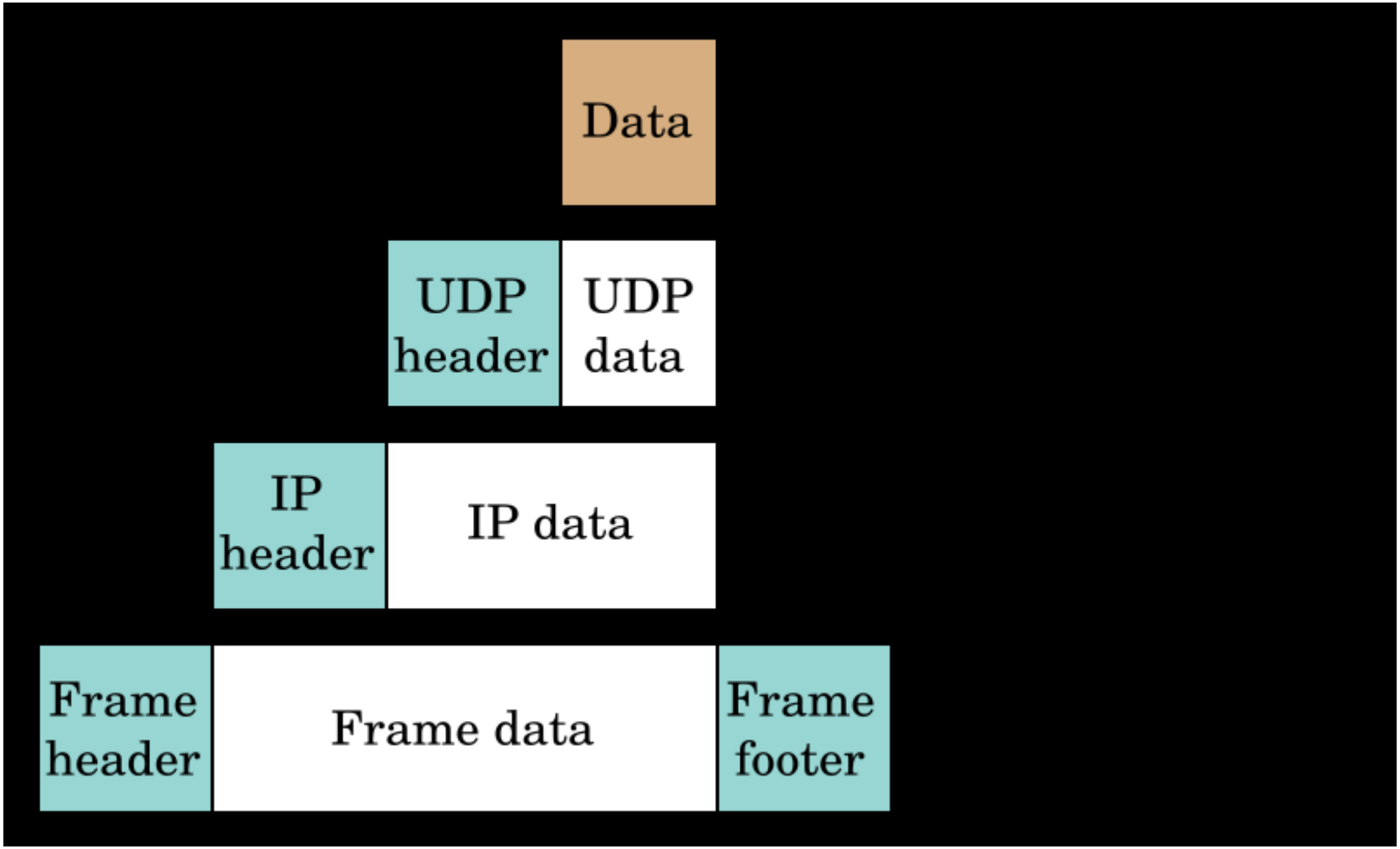
II. Một số giao thức cơ bản của TCP/IP

1. Giao thức gói tin người sử dụng UDP (User Datagram Protocol)
2. Giao thức điều khiển truyền TCP (Transmission Control Protocol)
3. Giao thức mạng IP (Internet Protocol)
4. Giao thức thông báo điều khiển mạng ICMP(Internet Control Message Protocol)
5. Giao thức phân giải địa chỉ ARP (Address Resolution Protocol)
6. Giao thức phân giải địa chỉ ngược RARP (Reverse Address Resolution Protocol)

II.1. Giao thức gói tin người sử dụng UDP

- UDP là giao thức không liên kết (Connectionless).
- UDP sử dụng cho các tiến trình không yêu cầu về độ tin cậy cao, không có cơ chế xác nhận ACK, không đảm bảo chuyển giao các gói dữ liệu đến đích và theo đúng thứ tự và không thực hiện loại bỏ các gói tin trùng lặp, không hợp dữ liệu tại nơi nhận.
- UDP thường sử dụng kết hợp với các giao thức khác, phù hợp cho các ứng dụng yêu cầu xử lý nhanh như các giao thưc SNMP và VoIP.
  - Giao thức SNMP (Simple Network Management Protocol) là giao thức quản lý mạng phổ biến, khả năng tương thích cao. SNMP cung cấp thông tin quản trị MIB (Management Information Base) và hỗ trợ quản lý và giám sát Agent.
  - VoIP ứng dụng UDP: Kỹ thuật VoIP (Voice over IP) được thừa kế kỹ thuật giao vận IP.

Đóng gói dữ liệu UDP trong gói IP



II.2. Giao thức điều khiển truyền TCP

- TCP là một giao thức hướng liên kết (Connection Oriented), tức là trước khi truyền dữ liệu, thực thể TCP phát và thực thể TCP thu thương lượng để thiết lập một kết nối logic tạm thời, tồn tại trong quá trình truyền số liệu.
- TCP nhận thông tin từ tầng trên, chia dữ liệu thành nhiều gói theo độ dài quy định và chuyển giao các gói tin xuống cho các giao thức tầng mạng (Tầng IP) để định tuyến.
- Bộ xử lý TCP xác nhận từng gói, nếu không có xác nhận gói dữ liệu sẽ được truyền lại. Thực thể TCP bên nhận sẽ khôi phục lại thông tin ban đầu dựa trên thứ tự gói và chuyển dữ liệu lên tầng trên.
- TCP cung cấp khả năng truyền dữ liệu một cách an toàn giữa các thành viên trong liên mạng. Cung cấp các chức năng kiểm tra tính chính xác của dữ liệu khi đến đích và truyền lại dữ liệu khi có lỗi xảy ra.

II.2. Giao thức điều khiển truyền TCP

- TCP cung cấp các chức năng chính sau:
  - Thiết lập, duy trì, giải phóng liên kết giữa hai thực thể TCP.
  - Phân phát gói tin một cách tin cậy.
  - Tạo số thứ tự (Sequencing) các gói dữ liệu.
  - Điều khiển lỗi.
  - Cung cấp khả năng đa kết nối cho các quá trình khác nhau giữa thực thể nguồn và thực thể đích thông qua việc sử dụng số hiệu cổng.
  - Truyền dữ liệu theo chế độ song công (Full-Duplex).

II.2. Giao thức điều khiển truyền TCP

- TCP có những đặc điểm sau:
  - Hai thực thể liên kết với nhau phải trao đổi, đàm phán với nhau về các thông tin liên kết.
  - Hội thoại, đàm phán nhằm ngăn chặn sự tràn lụt và mất dữ liệu khi truyền.
  - Hệ thống nhận phải gửi xác nhận cho hệ thống phát biết rằng nó đã nhận gói dữ liệu.
  - Các Datagram IP có thể đến đích không đúng theo thứ tự , TCP nhận sắp xếp lại.
  - Hệ thống chỉ phát lại gói tin bị lỗi, không loại bỏ toàn bộ dòng dữ liệu.

II.3. Giao thức mạng IP

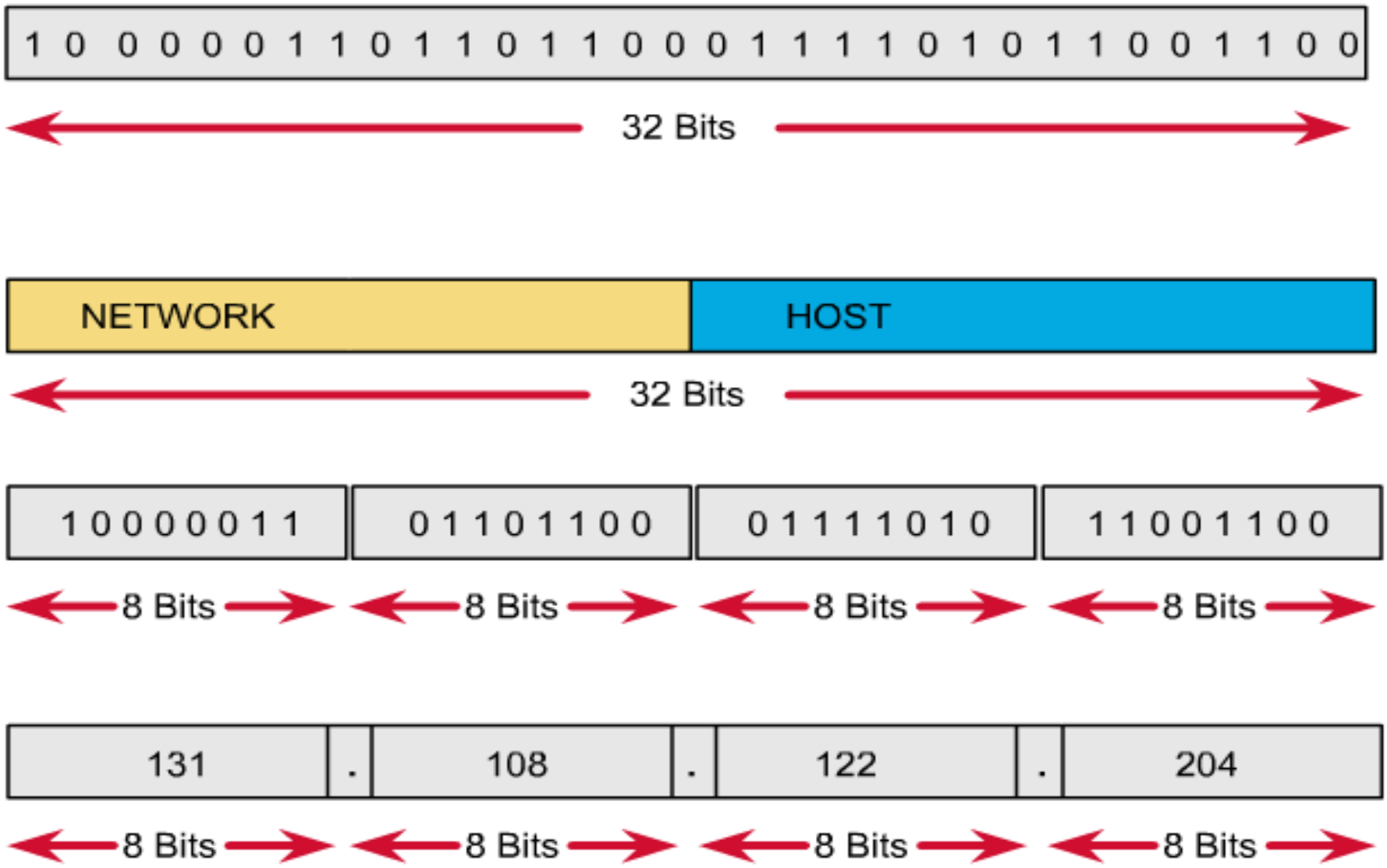
- IP (Internet Protocol) là giao thức liên mạng (định tuyến) cho phép các máy tính trên mạng kết nối với nhau.
- Chức năng chủ yếu của IP là cung cấp các dịch vụ Datagram và các khả năng kết nối các mạng con thành liên mạng để truyền dữ liệu với phương thức chuyển mạch gói IP Datagram, thực hiện tiến trình định địa chỉ và chọn đường.
- IP thực hiện việc tách và hợp các gói tin theo yêu cầu kích thước được định nghĩa cho các tầng vật lý và liên kết dữ liệu thực hiện.
- IP Header được thêm vào đầu các gói tin và được giao thức tầng thấp truyền theo dạng khung dữ liệu (Frame).
- IP kiểm tra lỗi thông tin điều khiển, phần đầu IP bằng giá trị tổng CheckSum.

- Định tuyến là thao tác chính của IP bằng cách sử dụng các bảng định tuyến động tham chiếu tại mỗi bước nhảy. Xác định tuyến được tiến hành bằng cách tham khảo thông tin thiết bị mạng vật lý và logic như ARP giao thức phân giải địa chỉ.

II.3.a. Địa chỉ IP

- Mỗi một trạm (Host) được gán một địa chỉ duy nhất gọi là địa chỉ IP.
- Mỗi địa chỉ IP có độ dài 32 bit được tách thành 4 vùng (mỗi vùng 1 byte), có thể được biểu diễn dưới dạng thập phân, bát phân, thập lục phân hoặc nhị phân. Cách viết phổ biến nhất là dưới dạng thập phân có dấu chấm để tách giữa các vùng.
- Địa chỉ IP được chia thành 5 lớp ký hiệu là A, B, C, D, E với cấu trúc mỗi lớp được xác định.
- 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

II.3.b. Dạng thức địa chỉ IP



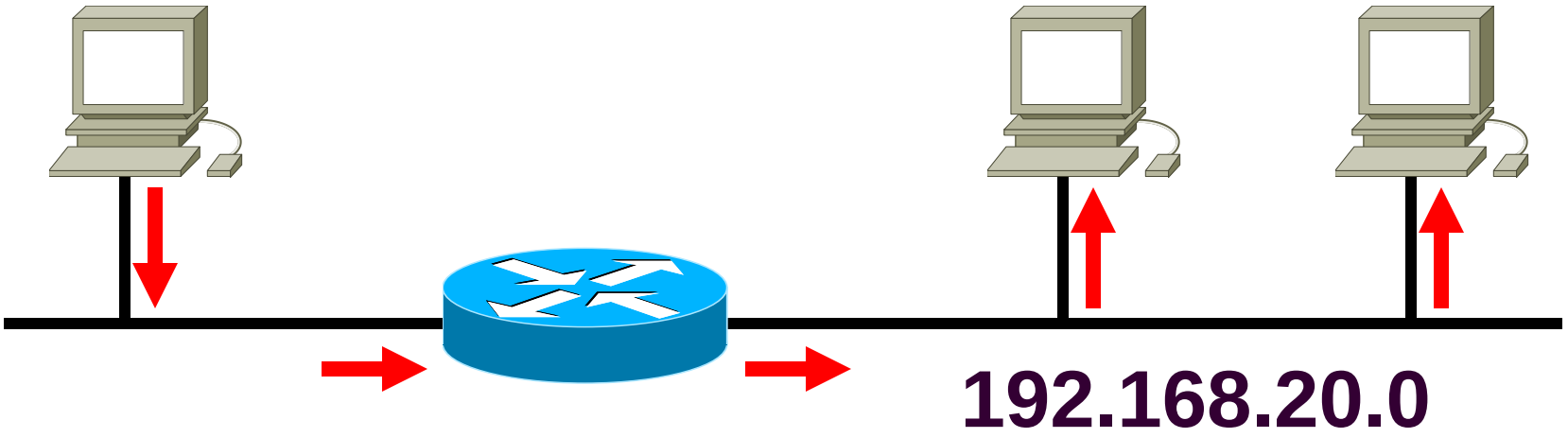
II.3.b. Dạng thức địa chỉ IP

- **Các bit phần mạng (NetworkID)**
  - Xác định phần địa chỉ mạng
  - Xác định lớp địa chỉ IP
  - Các bit phần mạng không được phép đồng thời là 0
- **Các bit phần máy (HostID)**
  - Xác định phần địa chỉ máy
  - Các bit đồng thời là 0: dành riêng cho địa chỉ mạng
  - Các bit đồng thời là 1: dành riêng cho địa chỉ quảng bá (broadcast)

II.3.b. Dạng thức địa chỉ IP

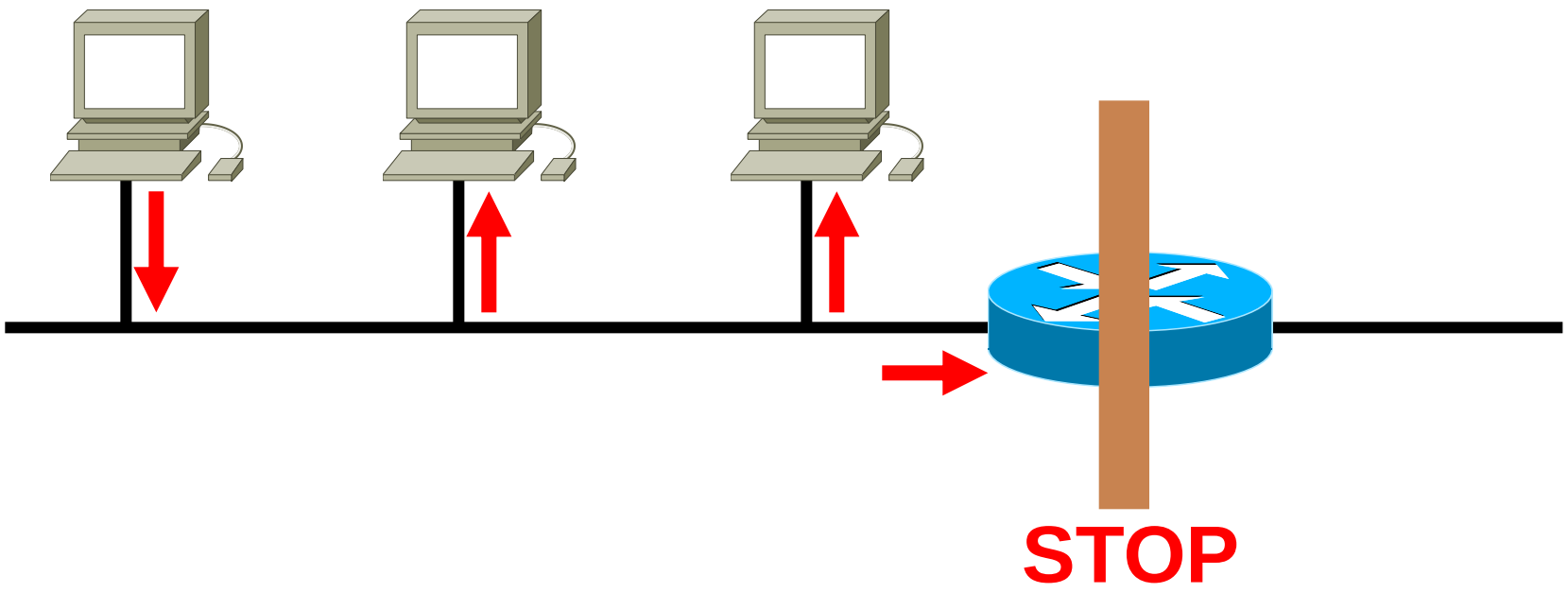
- Địa chỉ quảng bá (broadcast)
  - Muốn gởi dữ liệu đến tất cả các máy trong một mạng?
  - Địa chỉ mạng là địa chỉ của mạng hoặc một thiết bị nào đó thuộc về
  - Địa chỉ quảng bá được sử dụng để gởi dữ liệu đến tất cả các máy trong cùng một mạng
  - Địa chỉ mạng là địa chỉ mà các bit phần máy đồng thời là 0
  - Địa chỉ quảng bá trực tiếp: các bit phần máy đồng thời là 1
  - Các máy có cùng địa chỉ mạng có thể giao tiếp trực tiếp với nhau mà không cần thông qua thiết bị trung gian nào
  - Địa chỉ quảng bá nội bộ: tất cả các bit là 1 (255.255.255.255)
  - Các máy có thể chia sẻ đường truyền chung nhưng nếu chúng có địa chỉ mạng khác nhau thì không thể giao tiếp với nhau trực tiếp được mà phải thông qua một thiết bị trung gian (thường là router)

Địa chỉ quảng bá trực tiếp



192.168.20.255

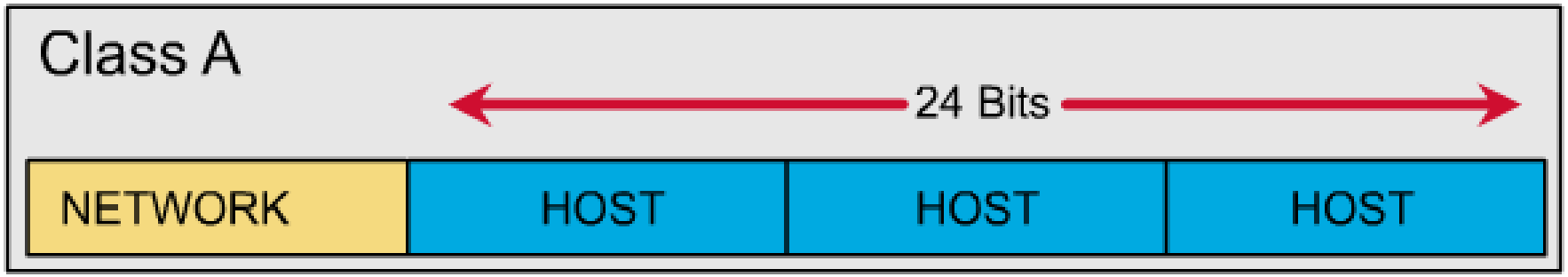
Địa chỉ quảng bá nội bộ

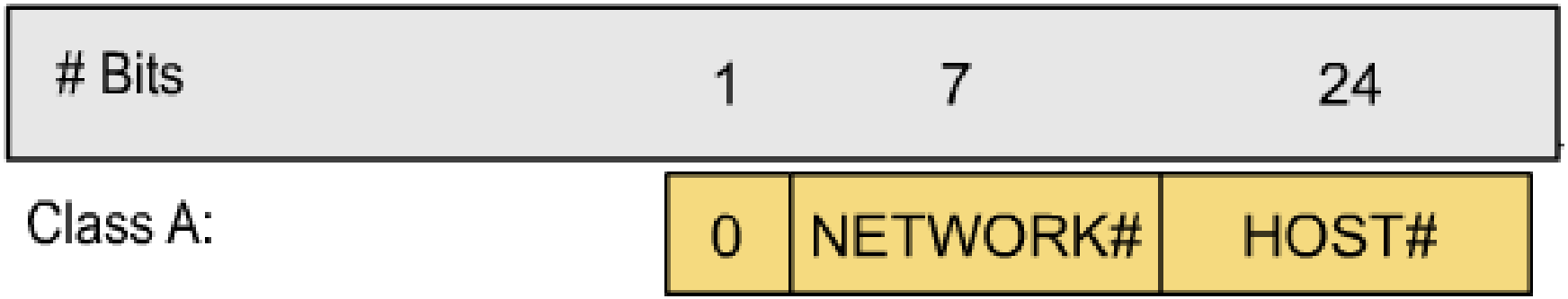


255.255.255.255

II.3.d. Phân lớp địa chỉ IP

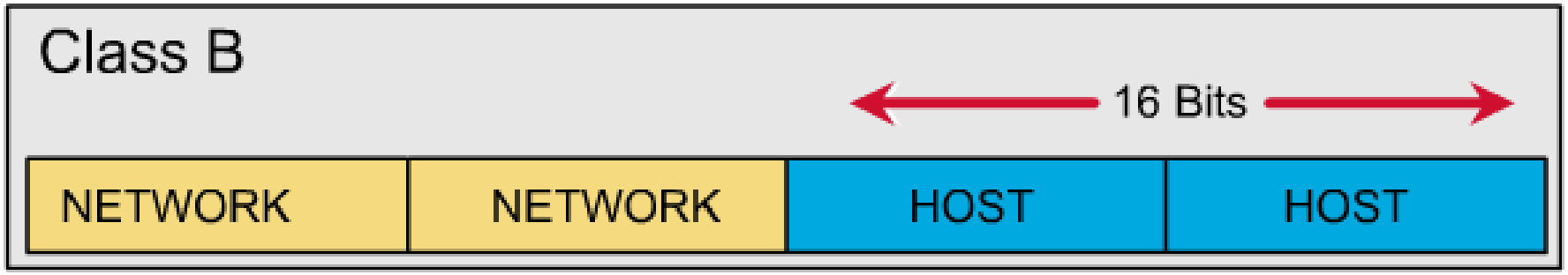
- Lớp A cho phép định danh tối đa 126 mạng (byte đầu tiên), với tối đa 16 triệu Host (3 byte còn lại) cho mỗi mạng. Lớp này được dùng cho các mạng có số trạm cực lớn.

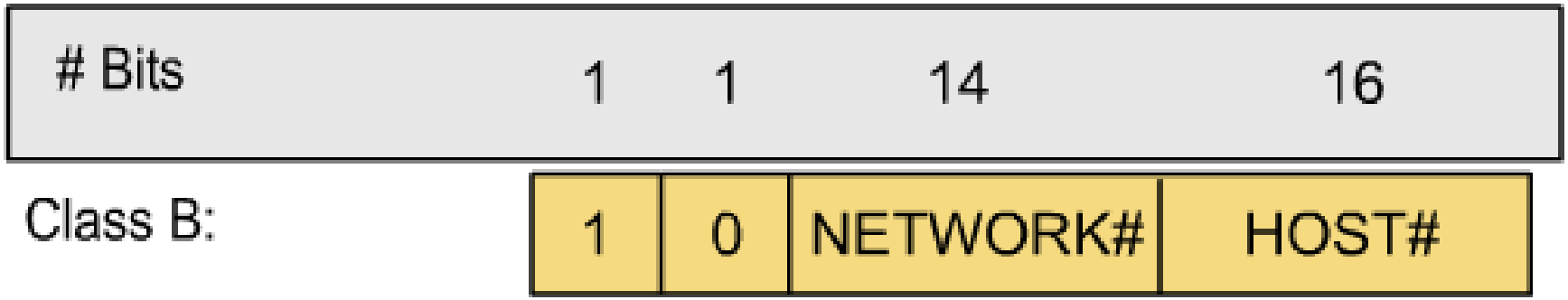




II.3.d. Phân lớp địa chỉ IP

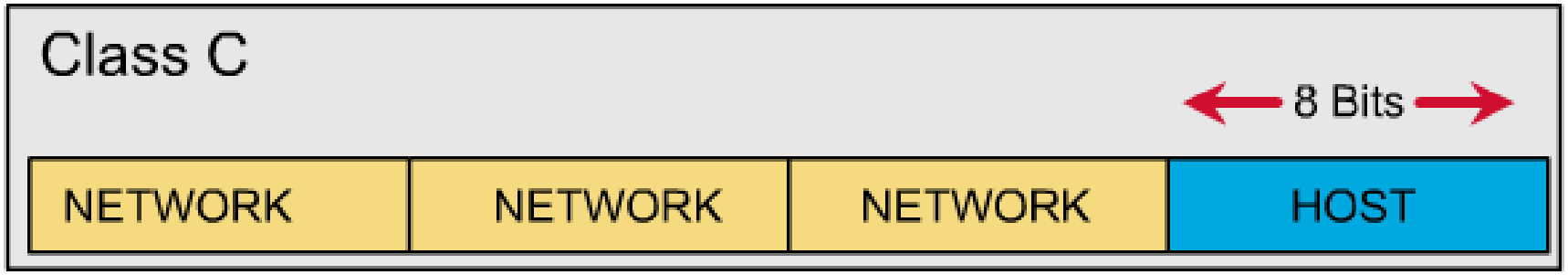
- Lớp B cho phép định danh tới 16384 mạng con, với tối đa 65535 Host trên mỗi mạng.

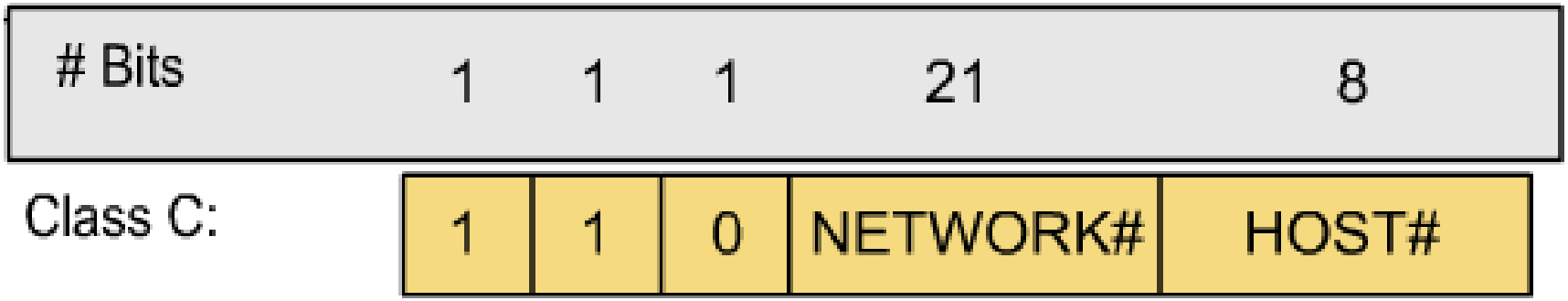




II.3.d. Phân lớp địa chỉ IP

- Lớp C cho phép định danh tới 2.097.150 mạng và tối đa 254 Host cho mỗi mạng.





II.3.d. Phân lớp địa chỉ IP

- 1.0.0.0 - 126.255.255.255: các mạng lớp A
- 127.0.0.0 : địa chỉ quay lui (loopback)
- 128.0.0.0 - 191.255.255.255: các mạng lớp B
- 192.0.0.0 - 223.255.255.255: các mạng lớp C
- 224.0.0.0 < 240.255.255.255: các mạng lớp D (multicast)
- >= 240.0.0.0 : các mạng lớp E (dành riêng)
- 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.

II.3.d. Phân lớp địa chỉ IP

Lớp	Bit đặc trưng	Số lượng Mạng	Số lượng Host	Biểu diễn bằng số Thập phân
A	0	127	16.777.214	0.1.0.0 —126.255.255.255
B	10	16.383	65.534	128.1.0.0 —191.255.255.255
C	110	2.097.151	234	192.1.0.0 —223.255.255.255
D	1110			223.0.0.0 —239.255.255.255
E	11110			240.0.0.0 —247.255.255.255

II.3.e. Địa chỉ IP trên Internet và địa chỉ máy

- Địa chỉ mạng Internet
  - Được cấp bởi INIC (*Internet Network Information Center*)
  - VNNIC chịu trách nhiệm cấp tên miền và địa chỉ IP cho Việt Nam
  - Xác định mạng mà một thiết bị nằm trong đó, hoặc một máy đơn kết nối dial-up
- Địa chỉ máy
  - Được cấp bởi người quản trị mạng hoặc cấp phát tự động (DHCP)
  - Xác định thiết bị trong mạng cục bộ

II.3.f. Ví dụ địa chỉ IP

- 172.16.20.200 là địa chỉ lớp B
- Phần mạng: 172.16
- Phần máy: 20.200
- Địa chỉ mạng: 172.16.0.0
- Địa chỉ quảng bá: 172.16.255.255
- Địa chỉ có thể dùng được cho các máy trong mạng
  - 172.16.0.1 - 172.16.255.254

II.3.f. Ví dụ địa chỉ IP

- 192.168.255.255 là địa chỉ lớp C
- Phần mạng: 192.168.255
- Phần máy: 255
- Địa chỉ mạng: 192.168.255.0
- Địa chỉ quảng bá: 192.168.255.255
- Địa chỉ dùng được cho máy trong mạng
  - 192.168.255.1 - 192.168.255.254

II.3.g. Các địa chỉ dành riêng

- Được mô tả trong RFC-1918. (Request For Command.)
- Class A: range from 10.0.0.0 to 10.255.255.255;
- Class B: range from 172.16.0.0 to 172.31.255.255;
- Class C: range from 192.168.0.0 to 192.168.255.255;
- Các lớp địa chỉ này dành riêng để đặt cho các máy trong nội bộ một tổ chức
- Cần có một NATserver (network address translation: dịch địa chỉ mạng) hoặc proxy server để cung cấp kết nối Internet cho các máy có địa chỉ dành riêng (thường thì trong router hiện nay có tích hợp các thành phần này)

II.4. Giao thức thông báo điều khiển mạng ICMP

- Giao thức IP không có cơ chế kiểm soát lỗi và kiểm soát luồng dữ liệu. Các nút mạng cần biết tình trạng các nút khác, các gói dữ liệu phát đi có tới đích hay không…

- Các chức năng chính:

  - ICMP là giao thức điều khiển (Redirection): Một Router gửi một thông điệp ICMP cho một trạm, thông báo nó sử dụng Router khác. Thường được dùng khi trạm nguồn ở trên cùng một mạng với hai thiết bị định tuyến.
  - Điều khiển lưu lượng (Flow Control): Khi các gói dữ liệu đến quá nhanh, thiết bị đích hoặc thiết bị định tuyến sẽ gửi một thông điệp ICMP để trạm nguồn tạm thời ngừng việc gửi dữ liệu.
  - Kiểm tra trạng thái hoạt động của thiết bị: Một thiết bị có thể gửi một thông điệp ICMP đến một thiết bị khác để kiểm tra trạng thái hoạt động của thiết bị đó.

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

II.5. Giao thức phân giải địa chỉ ARP

- TCP/IP sử dụng ARP để tìm địa chỉ vật lý của trạm đích.
- Các máy nhận đọc, phân tích và so sánh địa chỉ IP của nó với địa chỉ IP của gói.
- Ví dụ khi cần gửi một gói dữ liệu IP cho một hệ thống khác trên cùng một mạng vật lý Ethernet, hệ thống gửi cần biết địa chỉ Ethernet của hệ thống đích để tạo liên kết dữ liệu xây dựng khung gói dữ liệu.
- Trước khi trao đổi thông tin với nhau, node nguồn cần phải xác định địa chỉ vật lý MAC của node đích bằng cách tìm kiếm trong bảng địa chỉ IP.
- Nếu không tìm thấy, node nguồn gửi quảng bá(Broadcast) một gói yêu cầu ARP (ARP Request) có chứa địa chỉ IP nguồn, địa chỉ IP đích cho tất cả các máy trên mạng.
  - Nếu cùng địa chỉ IP, máy đích sẽ gửi trả lời (ARP Reply) có chứa địa chỉ MAC của nó và trả lời bằng một gói ARP Reply có chứa địa chỉ MAC cho node nguồn.
  - Nếu không cùng địa chỉ IP, nó chuyển tiếp gói yêu cầu nhận được dưới dạng quảng bá cho tất cả các trạm trên mạng.

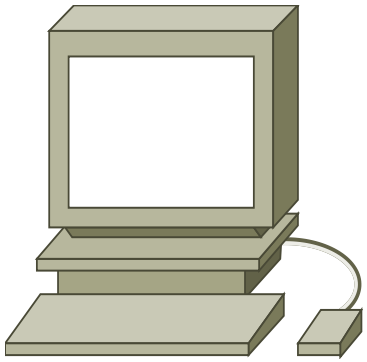
Tiến trình của ARP

- IP yêu cầu địa chỉ MAC.
- Tìm kiếm trong bảng ARP.
- Nếu tìm thấy sẽ trả lại địa chỉ MAC.
- Nếu không tìm thấy, tạo gói ARP yêu cầu và gửi tới tất cả các trạm.
- Tuỳ theo gói tin trả lời, ARP cập nhật vào bảng ARP và gửi địa chỉ MAC cho IP.

II.6. Giao thức phân giải địa chỉ ngược RARP

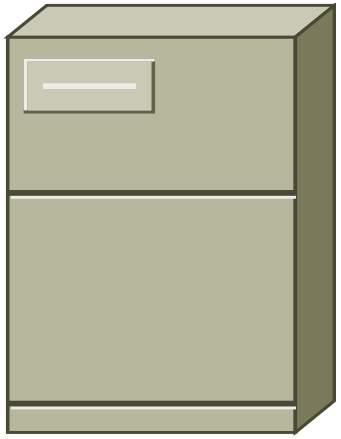
- RARP là giao thức phân giải địa chỉ ngược. Quá trình này ngược lại với quá trình ARP ở trên, nghĩa là cho trước địa chỉ mức liên kết, tìm địa chỉ IP tương ứng.
- Như vậy RARP được sử dụng để phát hiện địa chỉ IP, khi biết địa chỉ vật lý MAC.
- Nguyên tắc hoạt động của RARP ngược với ARP, nghĩa là máy đã biết trước địa chỉ vật lý MAC, tìm địa chỉ IP tương ứng của nó.
- Máy A cần biết địa IP của nó, nó gửi gói tin RARP Request chứa địa chỉ MAC cho tất cả các máy trong mạng LAN.
- Mọi máy trong mạng đều có thể nhận gói tin này nhưng chỉ có Server mới trả lại RARP Reply chứa địa chỉ IP của nó.

Nguyên tắc hoạt động của RARP



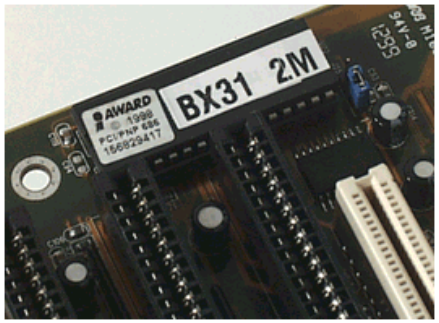
RARP Request

RARP Reply



RARP server

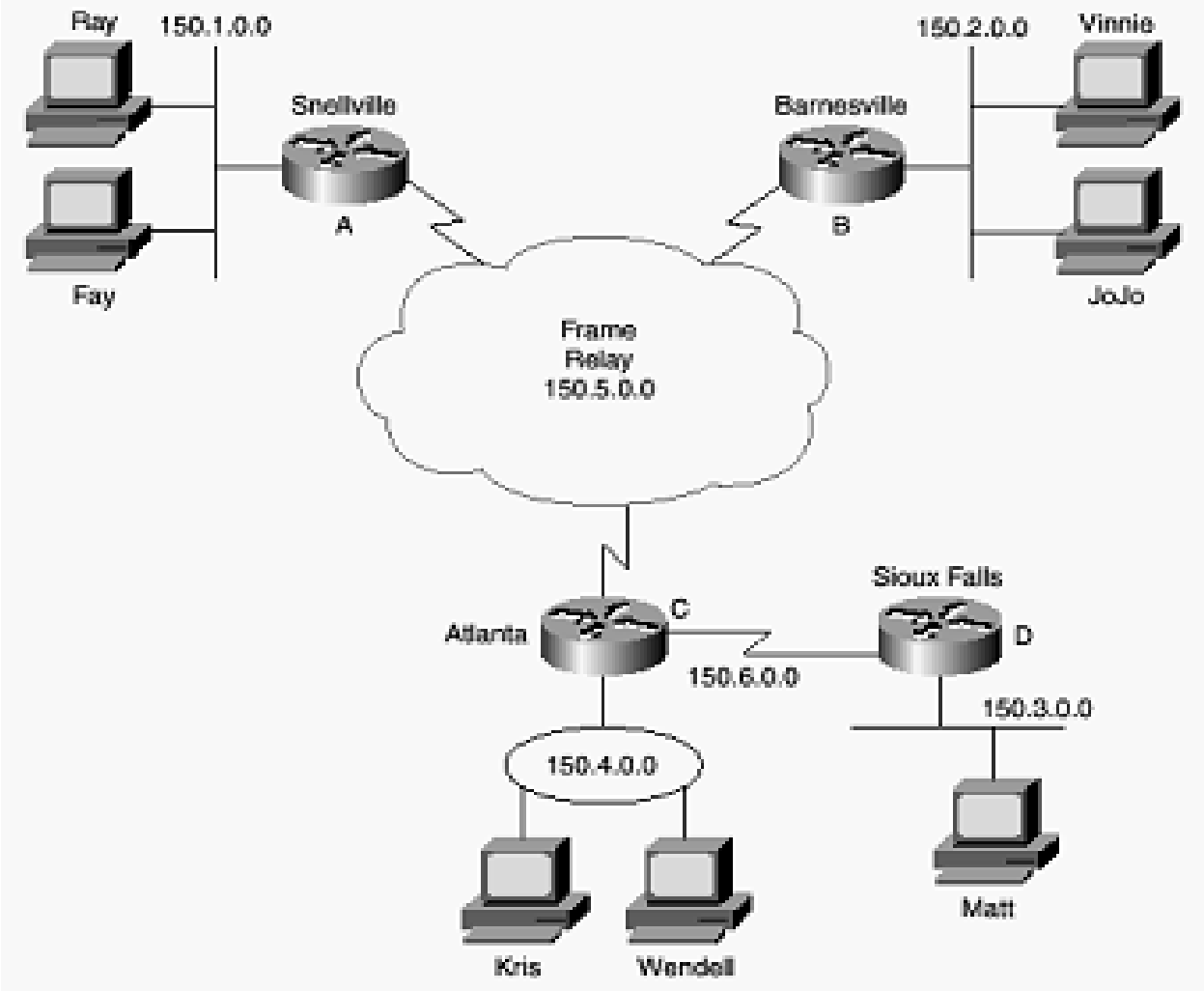
MAC: Known
IP: Unknown



MAC HEADER	IP HEADER	RARP REQUEST MESSAGE
Destination 08-00-02-89-90-8 Source 02-60-8C-01-02-03	Destination 11111111 Source ????????	What is my IP address?

II.7. Chia mạng con (subnetting)

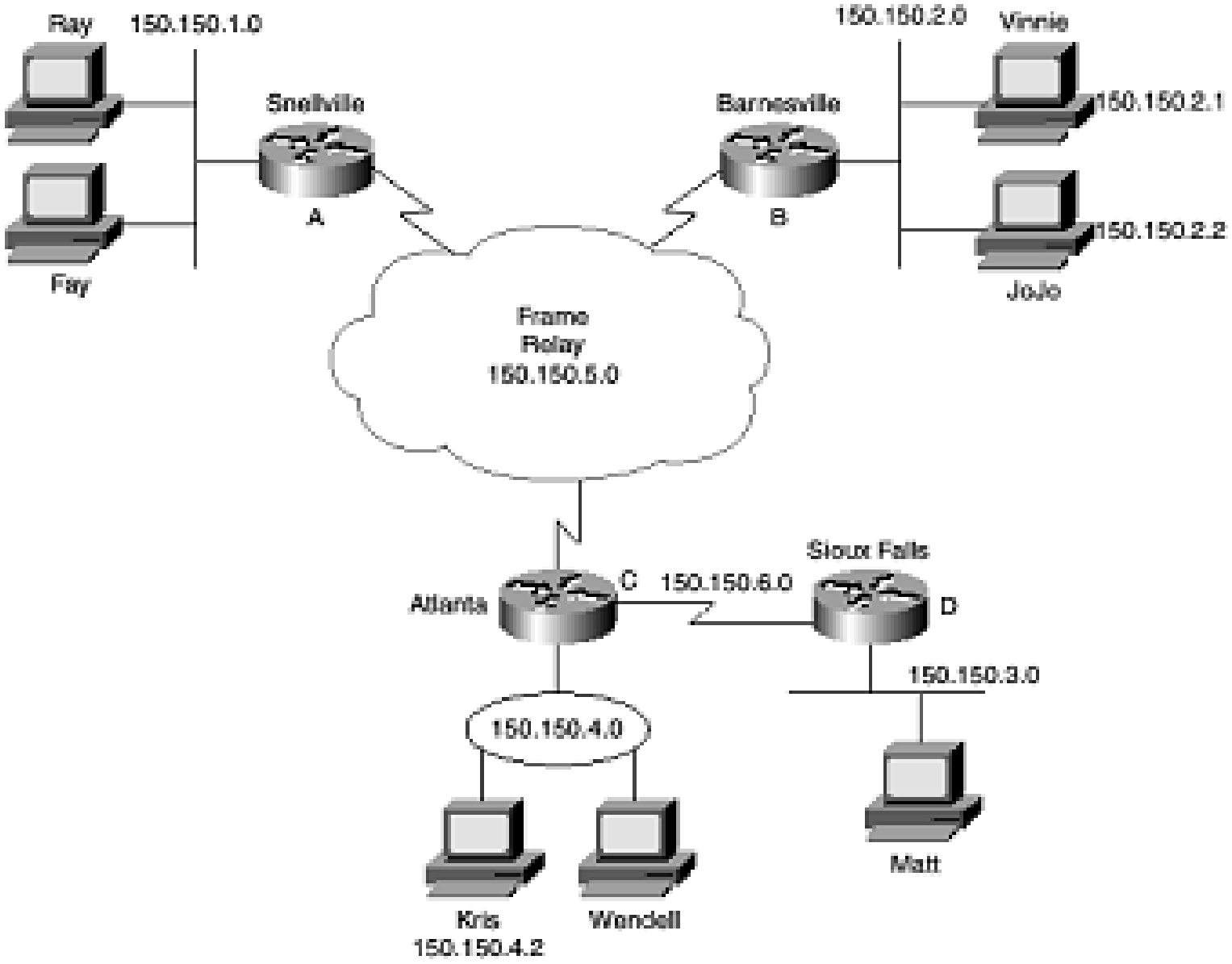
- Giả sử ta phải tiến hành đặt địa chỉ IP cho hệ thống có cấu trúc như sau:



II.7. Chia mạng con (subnetting)

- Theo hình trên, ta bắt buộc phải dùng đến tất cả là sáu đường mạng riêng biệt để đặt cho hệ thống mạng của mình, mặc dù trong mỗi mạng chỉ dùng đến vài địa chỉ trong tổng số 65534 địa chỉ hợp lệ, đó là một sự phí phạm to lớn.
- Thay vì vậy, khi sử dụng kỹ thuật chia mạng con, ta chỉ cần sử dụng một đường mạng (Ví dụ: 150.150.0.0) và chia đường mạng này thành sáu mạng con
- Rõ ràng khi tiến hành cấp phát địa chỉ cho các hệ thống mạng lớn, người ta phải sử dụng kỹ thuật chia mạng con trong tình hình địa chỉ IP ngày càng khan hiếm.
- Ví dụ trong hình trên hoàn toàn chưa phải là chiến lược chia mạng con tối ưu. Thật sự người ta còn có thể chia mạng con nhỏ hơn nữa, đến một mức độ không bỏ phí một địa chỉ IP nào khác.

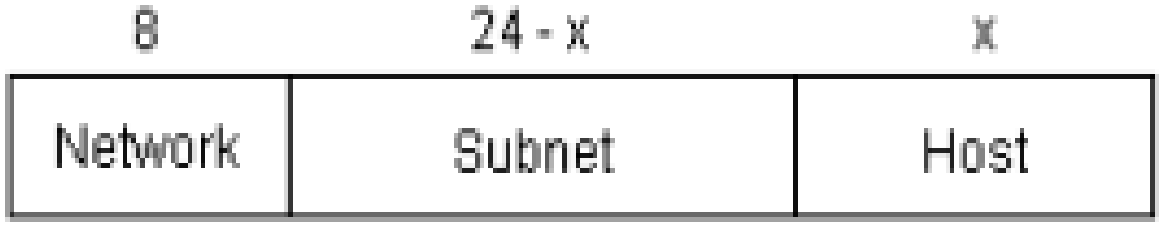
II.7. Chia mạng con (subnetting)



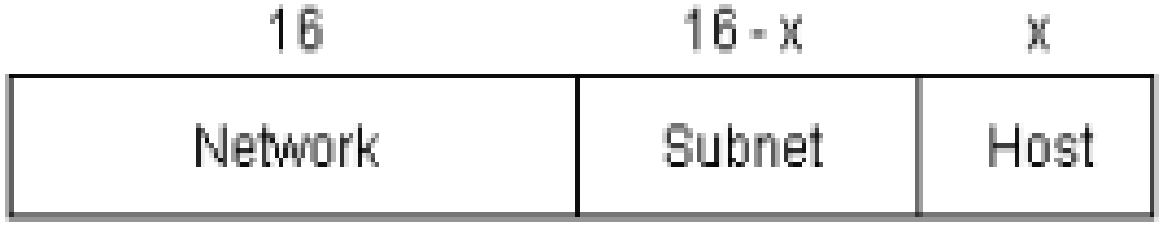
II.7. Chia mạng con (subnetting)

- Xét về khía cạnh kỹ thuật, chia mạng con chính là việc mượn một số bit trong phần host_id ban đầu để đặt cho các mạng c

Ví dụ:



- Lúc n
networ
subnet
con củ
hoặc n



- Tuy nh
host_ic
làm ho

Một số khái niệm mới:

- Địa chỉ mạng con (địa chỉ đường mạng): bao gồm cả phần network_id và subnet_id, phần host_id chỉ chứa các bit 0. Theo hình bên trên thì ta có các địa chỉ mạng con sau: 150.150.1.0, 150.150.2.0, …
- Địa chỉ broadcast trong một mạng con: Giữ nguyên các bit dùng làm địa chỉ mạng con, đồng thời bật tất cả các bit trong phần host_id lên 1.
- Ví dụ địa chỉ broadcast của mạng con 150.150.1.0 là 150.150.1.255.
- Mặt nạ mạng con (subnet mask): giúp máy tính xác định được địa chỉ mạng con của một địa chỉ host.

Một số khái niệm mới:

- Để xây dựng mặt nạ mạng con cho một hệ thống địa chỉ, ta bật các bit trong phần network_id và subnet_id lên 1, tắt các bit trong phần host_id thành 0.
- Ví dụ mặt nạ mạng con dùng cho hệ thống mạng trong hình trên là 255.255.255.0.
- Vấn đề đặt ra là khi xác định được một địa chỉ IP (ví dụ 172.29.8.230) ta không thể biết được host này nằm trong mạng nào (không thể biết mạng này có chia mạng con hay không, và nếu có chia thì dùng bao nhiêu bit để chia).

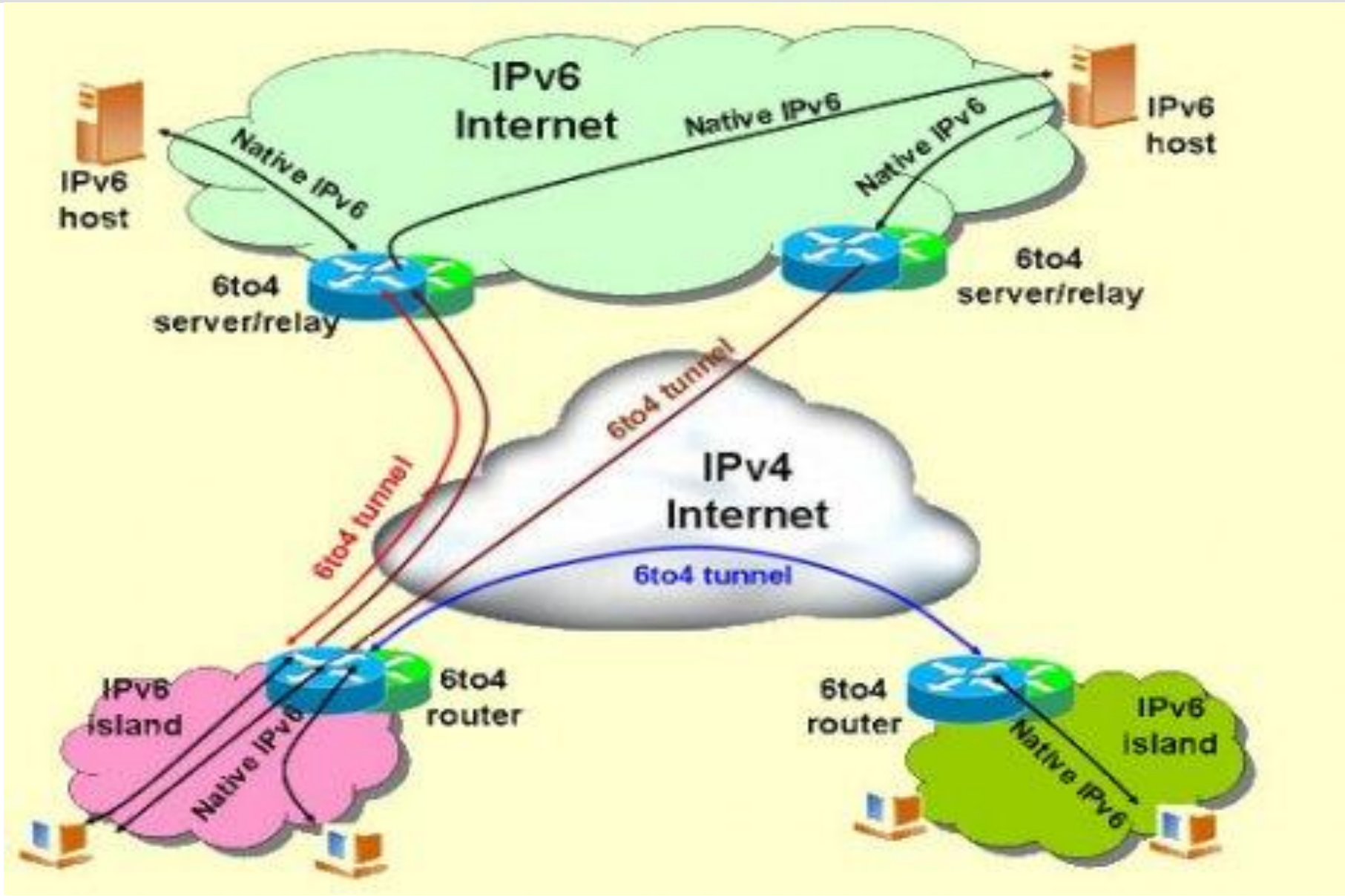
Một số khái niệm mới:

- Chính vì vậy khi ghi nhận địa chỉ IP của một host, ta cũng phải cho biết subnet mask là bao nhiêu (subnet mask có thể là giá trị thập phân, cũng có thể là số bit dùng làm subnet mask).
  - Ví dụ địa chỉ IP ghi theo giá trị thập phân của subnet mask là 172.29.8.230/255.255.255.0
  - Hoặc địa chỉ IP ghi theo số bit dùng làm subnet mask là 172.29.8.230/24.

III. Giao thức IPv6

- Giao thức IPng (Next General Internet Protocol) là phiên bản mới của giao thức IP được IETF (Internet Engineering Task Force) đề xướng và năm 1994.
- IESG (Internet Engineering Steering Group) phê chuẩn với tên chính thức là IPv6. IPv6 là phiên bản kế thừa phát triển từ IPv4.

III. Giao thức IPv6



III.1. Nguyên nhân ra đời của IPv6

- Internet phát triển mạnh, IPv4 đã sử dụng hết số IP và không đáp ứng được nhu cầu thêm địa chỉ.
- Trong quá trình hoạt động, IPv4 còn bộc lộ nhiều hạn chế về bảo mật và QoS.
- Việc phát triển quá nhanh của mạng Internet dẫn đến không gian địa chỉ ngày càng bị thu hẹp và tình trạng thiếu hụt địa chỉ tất yếu sẽ xảy ra.
- Khi kết nối thành mạng Intranet cần nhiều địa chỉ khác nhau và truyền thông qua môi trường công cộng. Vì vậy đòi hỏi phải có các dịch vụ bảo mật để bảo vệ dữ liệu ở mức IP.
- Việc phát triển quá nhanh của mạng Internet dẫn đến kích thước các bảng định tuyến trên mạng ngày càng lớn.
- Việc cần thiết phải thay thế giao thức IPv4 là tất yếu. Thiết kế IPv6 nhằm mục đích tối thiểu hóa ảnh hưởng qua lại giữa các giao thức lớp trên và lớp dưới bằng cách tránh việc bổ sung một cách ngẫu nhiên các chức năng mới.
- Cài đặt IPv4 bằng thủ công hoặc bằng giao thức cấu hình địa chỉ IP động DHCP (Dynamic Host Configuration Protocol).
- Chính vì vậy, khi mà nhiều máy tính và các thiết bị kết nối vào mạng thì cần thiết phải có một phương thức cấu hình địa chỉ tự động và đơn giản hơn.

III.2. Các đặc trưng của IPv6

- IPv6 được chọn thay thế cho giao thức IPv4 không chỉ do IPv4 không còn phù hợp với yêu cầu phát triển hiện tại của mạng Internet mà còn vì những ưu điểm của giao thức IPv6:
  - Khả năng định tuyến và chọn đường linh hoạt:

    Một số trường trong Header của IPv6 bị bỏ đi để giảm thời gian xử lý của gói tin. Có khả năng tự động trong việc đánh địa chỉ. Mở rộng khả năng chọn đường bằng cách thêm trường “Scop” vào địa chỉ quảng bá (Multicast).
  - Không gian địa chỉ lớn:

    Độ dài địa chỉ IPv6 là 128 bit, gấp 4 lần độ dài địa chỉ IPv4. Không gian địa chỉ IPv6 không bị thiếu hụt trong tương lai.
  - Tự động cấu hình địa chỉ:

    Khả năng tự cấu hình của IPv6 được gọi là khả năng cắm và chạy (Plug and Play). Cho phép tự cấu hình địa chỉ cho giao diện mà không cần sử dụng các giao thức DHCP.

III.2. Các đặc trưng của IPv6

- Khả năng bảo mật: IPsec bảo vệ và xác nhận các gói tin IP:
  - Mã hóa dữ liệu: Phía gửi sẽ tiến hành mã hóa gói tin trước khi gửi.
  - Toàn vẹn dữ liệu: Phía nhận có thể xác nhận gói tin nhận được để đảm bảo rằng dữ liệu không bị thay đổi trong quá trình truyền.
  - Xác nhận nguồn gốc dữ liệu: Phía nhận có thể biết được phía gửi gói tin. Dịch vụ này phụ thuộc vào dịch vụ toàn vẹn dữ liệu.
  - Antireplay: Phía nhận có thể phát hiện và từ chối gói tin gửi lại.
- Chất lượng dịch vụ QoS (Quanlity Of Service): Chất lượng dịch vụ QoS trong IPv4 không cao.Trong Header IPv4 chứa địa chỉ nguồn và địa chỉ đích, truyền có độ tin cậy không cao. IPv6 Header có thêm một số trường mới để xử lý và xác định lưu lượng trên mạng. Do cơ chế xác nhận gói tin ngay trong Header nên việc hỗ trợ QoS có thể thực hiện được ngay cả khi gói tin được mã hóa qua IPsec.

III.2. Các đặc trưng của IPv6

- Giao thức phát hiện lân cận NDP (Neighbor Discovery Protocol) của IPv6 là một dãy các thông báo ICMPv6 cho phép quản lý tương tác giữa các node lân cận, thay thế ARP trong IPv4. Các thông báo ICMPv4 Router Discovery và ICMPv4 Redirect được thay bởi các thông báo Multicast, Unicast Neighbor Discovery.
- Khả năng mở rộng: Thêm vào trường Header mở rộng tiếp ngay sau Header, IPv6 có thể được mở rộng thêm các tính năng mới một cách dễ dàng.
- Tính di động: IPv4 không hỗ trợ cho tính di động, IPv6 cho phép nhiều thiết bị di động kết nối vào Internet theo chuẩn của PCMCIA (Personal Computer Memory Card International Association) qua mạng công cộng nhờ sóng vô tuyến.

III.3. So sánh IPv4 và IPv6

IPv4	IPv6
Độ dài địa chỉ là 32 bit (4 byte)	Độ dài địa chỉ là 128 bit (16 byte)
IPsec chỉ là tùy chọn	IPsec được gắn liền với IPv6.
Header của địa chỉ IPv4 không có trường xác định luồng dữ liệu của gói tin cho các Router để xử lý QoS.	Trường Flow Label cho phép xác định luồng gói tin để các Router có thể đảm bảo chất lượng dịch vụ QoS
Việc phân đoạn được thực hiện bởi cả Router và máy chủ gửi gói tin	Việc phân đoạn chỉ được thực hiện bởi máy chủ phía gửi mà không có sự tham gia của Router
Header có chứa trường Checksum	Không có trường Checksum trong IPv6 Header
Header có chứa nhiều tùy chọn	Tất cả các tùy chọn có trong Header mở rộng
Giao thức ARP sử dụng ARP Request quảng bá để xác định địa chỉ vật lý.	Khung ARP Request được thay thế bởi các thông báo Multicast Neighbor Solicitation.

III.3. So sánh IPv4 và IPv6

IPv4	IPv6
Sử dụng giao thức IGMP để quản lý thành viên các nhóm mạng con cục bộ	Giao thức IGMP được thay thế bởi các thông báo MLD (Multicast Listener Discovery)
Sử dụng ICMP Router Discovery để xác định địa chỉ cổng Gateway mặc định phù hợp nhất, là tùy chọn.	Sử dụng thông báo quảng cáo Router (Router Advertisement) và ICMP Router Solicitation thay cho ICMP Router Discovery, là bắt buộc.
Địa chỉ quảng bá truyền thông tin đến tất cả các node trong một mạng con	Trong IPv6 không tồn tại địa chỉ quảng bá, thay vào đó là địa chỉ Multicast
Thiết lập cấu hình bằng thủ công hoặc sử dụng DHCP	Cho phép cấu hình tự động, không sử dụng nhân công hay cấu hình qua DHCP
Địa chỉ máy chủ được lưu trong DNS với mục đích ánh xạ sang địa chỉ IPv4	Địa chỉ máy chủ được lưu trong DNS với mục đích ánh xạ sang địa chỉ IPv6
Con trỏ địa chỉ được lưu trong IN – ADDR ARPA DNS để ánh xạ địa chỉ IPv4 sang tên máy chủ	Con trỏ địa chỉ được lưu trong Ipv6 – INT DNS để ánh xạ địa chỉ từ IPv4 sang tên máy chủ
Hỗ trợ gói tin kích thước 576 bytes (có thể phân đoạn)	Hỗ trợ gói tin kích thước 1280 bytes (không cần phân đoạn)

IV. Các lớp địa chỉ IPv6

IV.1. Phương pháp biểu diễn địa chỉ IPv6

IV.2. Phân loại địa chỉ IPv6

- Địa chỉ IPv6 được biểu diễn bằng chuỗi số Hexa được chia thành các nhóm 16 bit tương ứng với bốn chữ số Hexa, ngăn cách nhau bởi dấu “:”
- Ví dụ một địa chỉ IPv6 :

  4021 : 0000 : 240E : 0000 : 0000 : 0AC0 : 3428 : 121C
- Có thể thu gọn bằng cách thay các nhóm 0 liên tiếp bằng kí hiệu “::”

  Vis dụ: 4021 :: 240E : :: : :: : 0AC0 : 3428 : 121C.
- Địa chỉ Unicast (tương đương Loopback): Là địa chỉ của một giao diện. Một gói tin được chuyển đến địa chỉ Unicast sẽ chỉ được định tuyến đến giao diện gắn với địa chỉ đó
- Địa chỉ Anycast (tương đương với Broadcast): Là địa chỉ của một tập giao diện thuộc của nhiều node khác nhau. Mỗi gói tin tới địa chỉ Anycast được chuyển tới chỉ một trong tập giao diện gắn với địa chỉ đó (là giao diện gần node gửi nhất và có Metrics nhỏ nhất).
- Địa chỉ Multicast (tương đương với lớp D): Địa chỉ của tập các giao diện thuộc về nhiều node khác nhau. Một gói tin gửi tới địa chỉ Multicast sẽ được gửi tất cả các giao diện trong nhóm.

CHƯƠNG 5
BẢO ĐẢM AN TOÀN MẠNG

Nội dung

I. Tổng quan về an ninh mạng.

II. Một số phương thức tấn công mạng phổ biến.

III. Biện pháp đảm bảo an ninh mạng.

IV. Mạng riêng ảo VPN (Virtual Private Networks).

V.1. Tổng quan về an ninh mạng

1. Khái niệm an ninh mạng
2. Các đặc trưng kỹ thuật của an toàn mạng
3. Các lỗ hổng và điểm yếu của mạng
4. Các biện pháp phát hiện hệ thống bị tấn công

V.1.1. Khái niệm 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 sử dụng chung tài nguyên, trao đổi thông tin với nhau.
- Do đặc điểm nhiều người sử dụng lại phân tán về mặt vật lý nên việc bảo vệ các tài nguyên thông tin trên mạng, tránh sự mất mát, xâm phạm là cần thiết và cấp bách.
- An ninh mạng có thể hiểu là cách **bảo vệ, đảm bảo an toàn** cho tất cả các thành phần mạng bao gồm dữ liệu, thiết bị, cơ sở hạ tầng mạng và đảm bảo mọi tài nguyên mạng được sử dụng tương ứng với một chính sách hoạt động được ấn định với những người có thẩm quyền tương ứng.

An ninh mạng bao gồm:

- Xác định chính xác các khả năng, nguy cơ xâm phạm mạng, các sự cố rủi ro đối với thiết bị, dữ liệu trên mạng để có các giải pháp phù hợp đảm bảo an toàn mạng.
- Đánh giá nguy cơ tấn công của Hacker đến mạng, sự phát tán virus...
- Phải nhận thấy an toàn mạng là một trong những vấn đề cực kỳ quan trọng trong các hoạt động, giao dịch điện tử và trong việc khai thác sử dụng các tài nguyên mạng.

Khó khăn của việc bảo đảm an ninh mạng

- Một thách thức đối với an toàn mạng là xác định chính xác cấp độ an toàn cần thiết cho việc điều khiển hệ thống và các thành phần mạng.
- Đánh giá các nguy cơ, các lỗ hổng khiến mạng có thể bị xâm phạm thông qua cách tiếp cận có cấu trúc.
- Xác định những nguy cơ ăn cắp, phá hoại máy tính, thiết bị, nguy cơ virus, bọ gián điệp.., nguy cơ xoá, phá hoại CSDL, ăn cắp mật khẩu,... nguy cơ đối với sự hoạt động của hệ thống như nghẽn mạng, nhiễu điện tử...
- Đánh giá được hết những nguy cơ ảnh hưởng tới an ninh mạng thì mới có thể có được những biện pháp tốt nhất.

Hình thức tấn công an ninh

- Về bản chất có thể phân loại các vi phạm thành hai loại vi phạm thụ động và vi phạm chủ động.
- Thụ động và chủ động được hiểu theo nghĩa có can thiệp vào nội dung và luồng thông tin có bị tráo đổi hay không.
- Vi phạm thụ động chỉ nhằm mục đích nắm bắt được thông tin.
- Vi phạm chủ động là thực hiện sự biến đổi, xoá bỏ hoặc thêm thông tin ngoại lai để làm sai lệch thông tin gốc nhằm mục đích phá hoại.
- Các hành động vi phạm thụ động thường khó có thể phát hiện nhưng có thể ngăn chặn hiệu quả. Trái lại vi phạm chủ động rất dễ phát hiện nhưng lại khó ngăn chặn.

V.1.2. Các đặc trưng kỹ thuật của an toàn mạng

a. Tính xác thực (Authentification)

b. Tính khả dụng (Availability)

c. Tính bảo mật (Confidentialy)

d. Tính toàn vẹn (Integrity)

e. Tính khống chế (Accountlability)

f. Tính không thể chối cãi (Nonreputation)

a. Tính xác thực (Authentification)

- Kiểm tra tính xác thực của một thực thể giao tiếp trên mạng. Một thực thể có thể là một người sử dụng, một chương trình máy tính, hoặc một thiết bị phần cứng.
- Các hoạt động kiểm tra tính xác thực được đánh giá là quan trọng nhất trong các hoạt động của một phương thức bảo mật.
- Một hệ thống thường phải thực hiện kiểm tra tính xác thực của mỗi thực thể trước khi thực thể đó thực hiện kết nối với hệ thống.
- Có thể phân loại bảo mật trên VPN theo các cách sau: mật khẩu truyền thống hay mật khẩu một lần; xác thực thông qua các giao thức (PAP, CHAP, RADIUS…) hay phần cứng (các loại thẻ card: smart card, token card, PC card), nhận diện sinh trắc học (dấu vân tay, giọng nói, quét võng mạc)

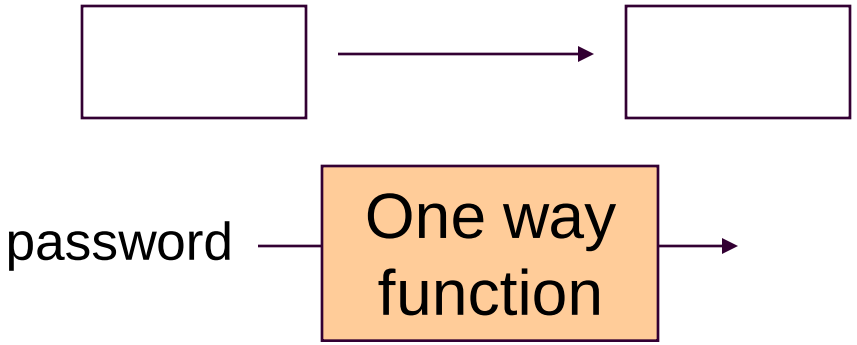
Kiểm tra tính xác thực của một thực thể giao tiếp trên mạng dựa vào 3 mô hình chính sau:

- Đối tượng kiểm tra cần phải có những thông tin trước, ví dụ như Password, hoặc mã số thông số cá nhân PIN (Personal Information Number).
- Kiểm tra dựa vào mô hình những thông tin đã có đối tượng kiểm tra cần phải thể hiện những thông tin mà chúng sở hữu, ví dụ như Private Key, hoặc số thẻ tín dụng.
- Kiểm tra dựa vào mô hình những thông tin xác định tính duy nhất đối tượng kiểm tra cần phải có những thông tin để định danh tính duy nhất của mình ví dụ như thông qua giọng nói, dấu vân tay, chữ ký…

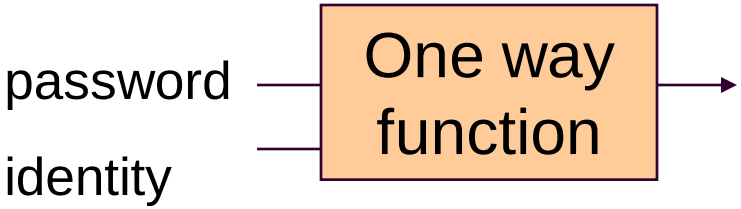
Một số mức xác thực

password

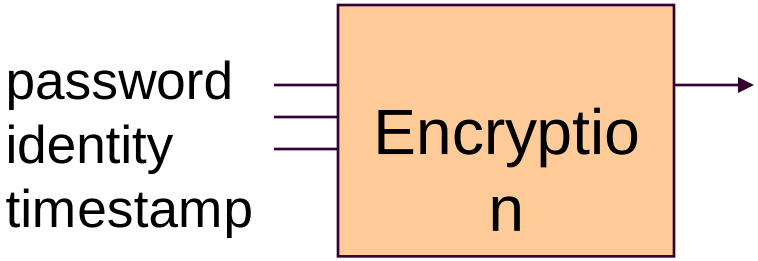
Level 0



Level 1



Level 2



Level 3

One way functions

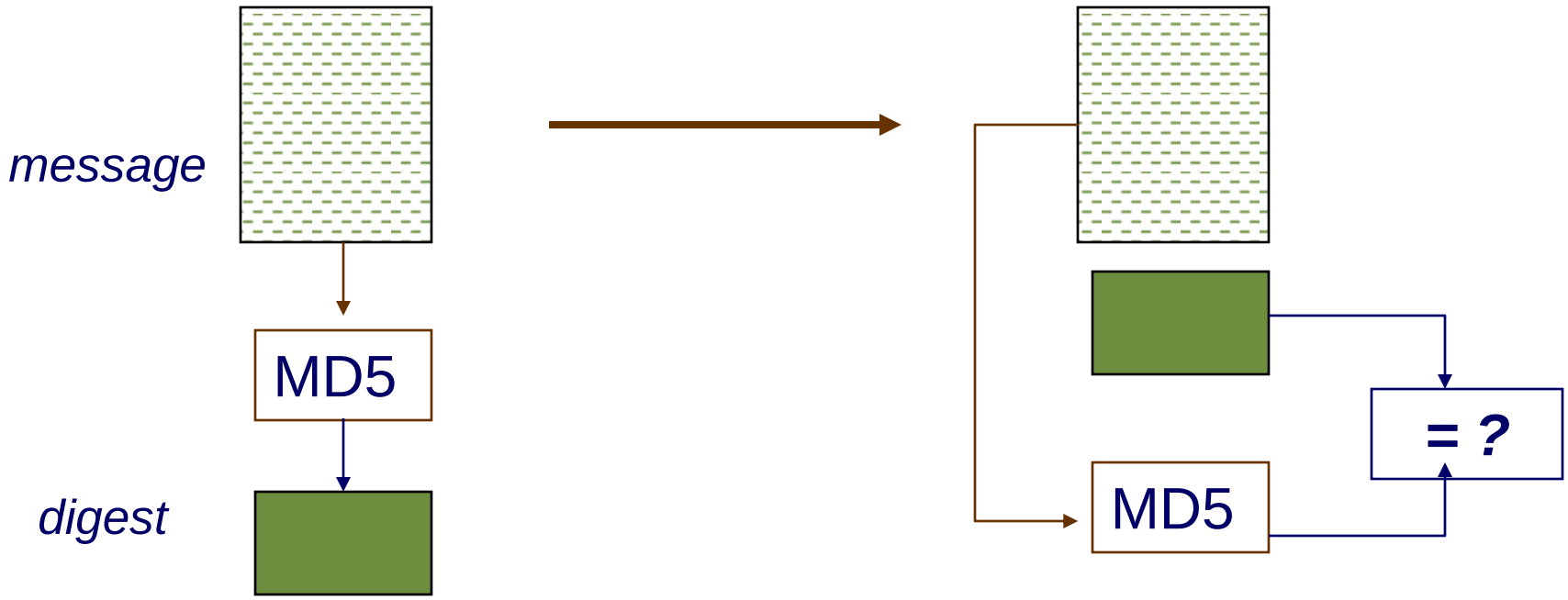
- Các hàm này được đưa ra nhằm mục đích “xáo trộn” thông tin đầu vào sao cho thông tin đầu ra không thể được phục hồi thành thông tin ban đầu.
- Hàm exclusive-OR (XOR):

$$C = b_1\ b_2\ b_3\ \ldots\ldots\ b_n$$

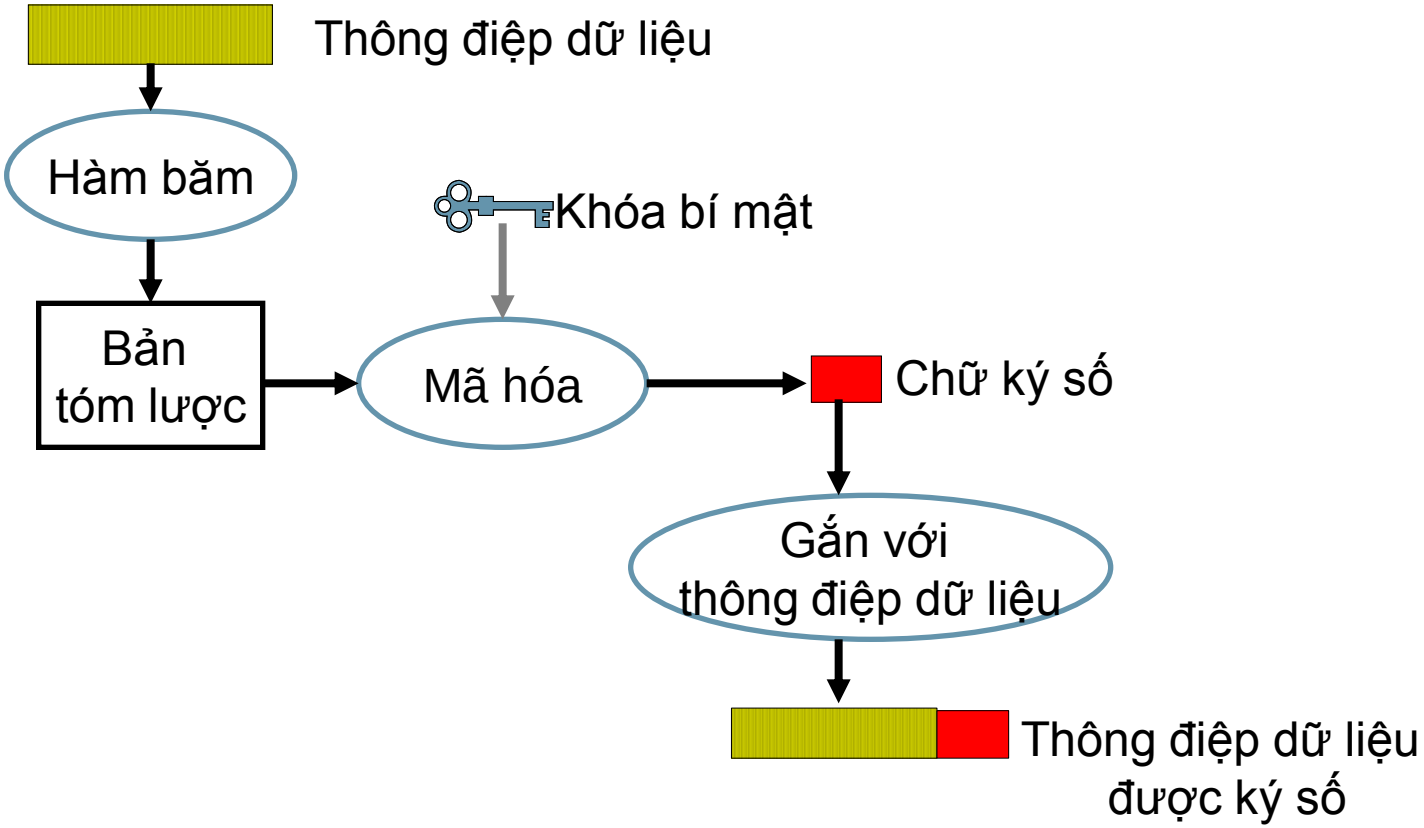
- Tuy nhiên hàm XOR có thể bị bẻ khóa dễ dàng.

Thuật toán “Tiêu hoá” MD5

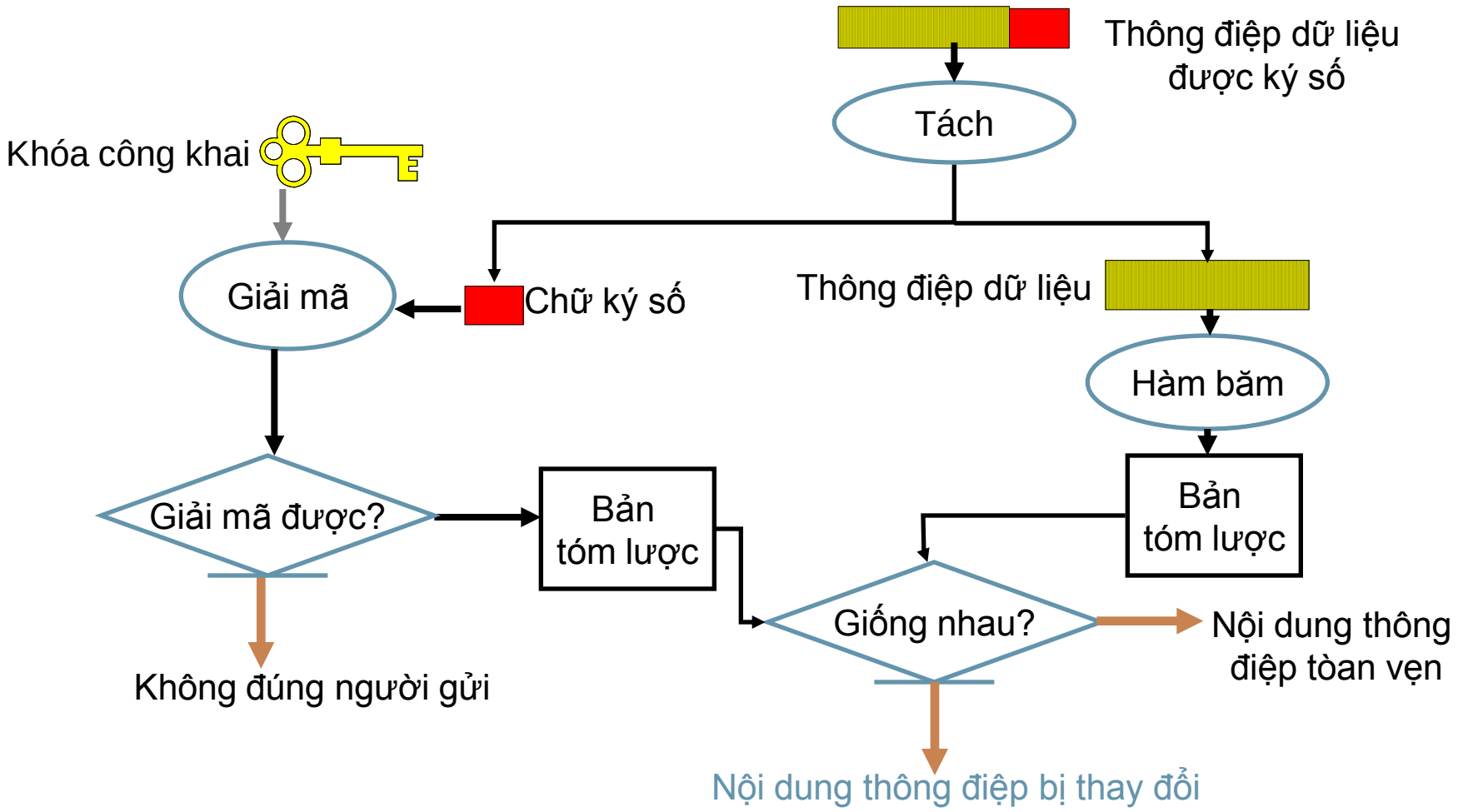
- Dùng cho chứng nhận thông tin đòi hỏi tính bảo mật cao.
- Làm thế nào chúng ta biết được thông tin gửi đến không bị thay đổi?



Xác thực mức cao - tạo chữ ký số



Thẩm định chữ ký số



b. Tính khả dụng (Availability)

- Tính khả dụng là đặc tính mà thông tin trên mạng được các thực thể hợp pháp tiếp cận và sử dụng theo yêu cầu, khi cần thiết bất cứ lúc nào, trong hoàn cảnh nào.
- Tính khả dụng sử dụng tỷ lệ giữa thời gian hệ thống được sử dụng bình thường với thời gian quá trình hoạt động.
- Tính khả dụng cần đáp ứng những yêu cầu sau:
  - Nhận biết và phân biệt thực thể
  - Khống chế tiếp cận (bao gồm cả việc khống chế tự tiếp cận và khống chế tiếp cận cưỡng bức)
  - Khống chế lưu lượng (chống tắc nghẽn..)
  - Khống chế chọn đường (cho phép chọn đường nhánh, mạch nối ổn định, tin cậy)
  - Giám sát tung tích (tất cả các sự kiện phát sinh trong hệ thống được lưu giữ để phân tích nguyên nhân, kịp thời dùng các biện pháp tương ứng).

c. Tính bảo mật (Confidentialy)

- Tính bảo mật là đặc tính tin tức không bị tiết lộ cho các thực thể hay quá trình không được uỷ quyền biết hoặc không để cho các đối tượng đó lợi dụng.
- Thông tin chỉ cho phép thực thể được uỷ quyền sử dụng.
- Kỹ thuật bảo mật thường là phòng ngừa dò la thu thập (làm cho đối thủ không thể dò la thu thập được thông tin), phòng ngừa bức xạ (phòng ngừa những tin tức bị bức xạ ra ngoài bằng nhiều đường khác nhau, tăng cường bảo mật thông tin (dưới sự khống chế của khoá mật mã), bảo mật vật lý (sử dụng các phương pháp vật lý để đảm bảo tin tức không bị tiết lộ).

c. Tính bảo mật bao gồm:

- Giữ bí mật
  - “Nếu chúng ta không nói cho ai biết các số điện thoại truy cập thì sẽ không có các xâm nhập qua các số điện thoại này”
  - “Chúng tôi thiết lập các cơ chế lọc gói tin ngay tại các gateway không cho phép các truy cập telnet hay ftp”
  - Nhân viên trong cơ quan đều biết các số điện thoại này. Nếu có một modem trong cơ quan cho phép kết nối từ bên ngoài thì sao?
  - Cơ chế lọc tin có đảm bảo cho tất cả các trường hợp không?
  - Nếu khoá mật mã bị mất ở đâu đó thì sao?
  - Giải mã sẽ mất nhiều thời gian và công sức, gây khó khăn nhất định cho công việc chung.
- Thiết lập cơ chế kiểm tra và lọc tin
- Mã hóa
  - “Chúng tôi mã hoá thư trước khi gửi”
  - Nếu thông tin là có giá trị thì việc sử dụng hệ thống máy tính mạnh, đặt tiền đề bẻ khóa là hoàn toàn có thể xảy ra.

d. Tính toàn vẹn (Integrity)

- Là đặc tính khi thông tin trên mạng chỉ được ủy quyền thì không thể tiến hành biến đổi được.
- Nghĩa là: thông tin trên mạng khi đang lưu giữ hoặc trong quá trình truyền dẫn đảm bảo không bị xoá bỏ, sửa đổi, giả mạo làm rối loạn trật tự, phát lại, xen vào một cách ngẫu nhiên hoặc cố ý và những sự phá hoại khác.
- Những nhân tố chủ yếu ảnh hưởng tới sự toàn vẹn thông tin trên mạng gồm: sự cố thiết bị, sai mã, bị tác động của con người, virus máy tính…
  - Yêu cầu cơ quan quản lý hoặc trung gian chứng minh tính chân thực của thông tin.

Một số phương pháp bảo đảm tính toàn vẹn thông tin:

- Giao thức an toàn có thể kiểm tra thông tin bị sao chép, sửa đổi. Nếu phát hiện thì thông tin đó sẽ bị vô hiệu hoá.
- Phương pháp phát hiện sai và sửa sai. Phương pháp sửa sai mã hoá đơn giản nhất và thường dùng là phép kiểm tra chẵn - lẻ.
- Biện pháp kiểm tra mật mã ngăn ngừa hành vi xuyên tạc và gian lận truyền tin.
- Chữ ký điện tử: bảo đảm tính xác thực của thông tin.

e. Tính khống chế (Accountlability)

- Là đặc tính về năng lực khống chế truyền bá và nội dung vốn có của tin tức trên mạng.

f. Tính không thể chối cãi (Nonreputation)

Trong quá trình giao lưu tin tức trên mạng, xác nhận tính chân thực đồng nhất của những thực thể tham gia, tức là tất cả các thực thể tham gia không thể chối bỏ hoặc phủ nhận những thao tác và cam kết đã được thực hiện.

V.1.3. Các lỗ hổng và điểm yếu của mạng

Các loại lỗ hổng bảo mật được chia như sau:

- Lỗ hổng loại C: Các lỗ hổng bảo mật hệ thống là các điểm yếu có thể tạo ra sự ngừng trệ của dịch vụ, thêm quyền đối với người sử dụng hoặc cho phép các truy nhập không hợp pháp vào hệ thống.
- Lỗ hổng loại B: Các lỗ hổng cho phép người sử dụng có thêm các quyền trên hệ thống mà không cần thực hiện kiểm tra tính hợp lệ. Mức độ nguy hiểm trung bình, những lỗ hổng này thường có trong các ứng dụng trên hệ thống, có thể dẫn đến hoặc lộ thông tin yêu cầu bảo mật.
- Lỗ hổng loại A: Các lỗ hổng này cho phép người sử dụng ở ngoài cho thể truy nhập vào hệ thống bất hợp pháp. Lỗ hổng rất nguy hiểm, có thể làm phá hủy toàn bộ hệ thống.

a. Khái niệm:

Cho phép thực hiện các phương thức tấn công theo kiểu từ chối dịch vụ DoS (Dinal of Services). Mức nguy hiểm thấp, chỉ ảnh hưởng chất lượng dịch vụ, có thể làm ngừng trệ, gián đoạn hệ thống, không phá hỏng dữ liệu hoặc chiếm quyền truy nhập.

Các lỗ hổng cho phép người sử dụng có thêm các quyền trên hệ thống mà không cần thực hiện kiểm tra tính hợp lệ. Mức độ nguy hiểm trung bình, những lỗ hổng này thường có trong các ứng dụng trên hệ thống, có thể dẫn đến hoặc lộ thông tin yêu cầu bảo mật.

Các lỗ hổng cho phép người sử dụng có thêm các quyền trên hệ thống mà không cần thực hiện kiểm tra tính hợp lệ. Mức độ nguy hiểm trung bình, những lỗ hổng này thường có trong các ứng dụng trên hệ thống, có thể dẫn đến hoặc lộ thông tin yêu cầu bảo mật.

b. Các phương thức tấn công mạng:

- Kẻ phá hoại có thể lợi dụng những lỗ hổng trên để tạo ra những lỗ hổng khác tạo thành một chuỗi những lỗ hổng mới.
- Để xâm nhập vào hệ thống, kẻ phá hoại sẽ tìm ra các lỗ hổng trên hệ thống, hoặc từ các chính sách bảo mật, hoặc sử dụng các công cụ dò xét (như SATAN, ISS) để đạt được quyền truy nhập.
- Sau khi xâm nhập, kẻ phá hoại có thể tiếp tục tìm hiểu các dịch vụ trên hệ thống, nắm bắt được các điểm yếu và thực hiện các hành động phá hoại tinh vi hơn.

V.1.4. Các biện pháp phát hiện hệ thống bị tấn công

- Không có một hệ thống nào đảm bảo an toàn tuyệt đối, mỗi một dịch vụ đều có những lỗ hổng bảo mật tiềm tàng.
- Người quản trị hệ thống không những phải nghiên cứu, xác định các lỗ hổng bảo mật mà còn phải thực hiện các biện pháp kiểm tra hệ thống có dấu hiệu tấn công hay không.
- Một số biện pháp cụ thể:

a. Kiểm tra các dấu hiệu hệ thống bị tấn công:

b. Kiểm tra các tài khoản người dùng mới lạ:

c. Kiểm tra sự xuất hiện các tập tin lạ:

- Hệ thống thường bị treo hoặc bị Crash bằng những thông báo lỗi không rõ ràng.
- Dấu hiệu khả nghi khác không bằng không.
- Khó xác định nguyên nhân do thiếu thông tin liên quan.

Người quản trị hệ thống nên có thói quen đặt tên tập tin theo nguyên tắc nhất định để dễ dàng phát hiện tập tin lạ.

Trước tiên xác định các nguyên nhân có phải nhân cứng hay không, nếu không phải hãy nghĩ đến khả năng máy bị tấn công.

Các biện pháp:

d. Kiểm tra thời gian thay đổi hệ thống của Account:

Đặc biệt là các chương trình Login, Shell hoặc các Scripts khởi động ...

Thường thường để phòng trường hợp các Account này bị truy nhập trái phép và thay đổi quyền hạn mà người sử dụng hợp pháp không kiểm soát được.

b. Kiểm tra hiệu năng của hệ thống:

e. Kiểm tra các file liên quan đến cấu hình mạng và d.vụ:

Sử dụng các tiện ích theo dõi tài nguyên và các tiến trình đang hoạt động trên hệ thống.

Bỏ các dịch vụ không cần thiết: đối với những dịch vụ không cần thiết chạy dưới quyền Root/Admin thì không chạy bằng các quyền yếu hơn.

c. Kiểm tra hoạt động của các dịch vụ hệ thống cung cấp:

f. Tham gia các nhóm tin về bảo mật:

Một trong các mục đích tấn công là làm cho tê liệt hệ thống (hình thức tấn công DoS). Sử dụng các lệnh, các tiện ích về mạng để phát hiện nguyên nhân trên hệ thống.

Các biện pháp này kết hợp với nhau tạo nên một chính sách về bảo mật đối với hệ thống.

V.II. Một số phương thức tấn công mạng:

1. Scanner
2. Bẻ khoá (Password Cracker)
3. Trojans
4. Sniffer

V.2.1. Scanner

- Kẻ phá hoại sử dụng chương trình Scanner tự động có thể tìm ra những điểm yếu trên hệ thống.
- Chương trình Scanner có thể hoạt động được trong môi trường TCP/IP, hệ điều hành UNIX, và các máy tính tương thích IBM, hoặc dòng máy Macintosh.
- Các chương trình Scanner cung cấp thông tin về khả năng bảo mật yếu kém của một hệ thống mạng.
- Các chương trình Scanner có thể rà soát và phát hiện các sơ hở trong (Ports) là thế mạnh và cần thiết đối với tầng vận chuyển và phát hiện những dịch vụ sử dụng trên hệ thống đó.
- Nó ghi lại những đáp ứng (Response) của hệ thống ở xa tương ứng với các dịch vụ mà nó phát hiện ra.

Dựa vào những thông tin này, những kẻ tấn công có thể tìm ra những điểm yếu trên hệ thống.

Chương trình Scanner có thể hoạt động được trong môi trường TCP/IP, hệ điều hành UNIX, và các máy tính tương thích IBM, hoặc dòng máy Macintosh.

Scanner là một chương trình trên một trạm làm việc tại cục bộ hoặc trên một trạm ở xa.

Các chương trình Scanner cung cấp thông tin về khả năng bảo mật yếu kém của một hệ thống mạng.

Các chương trình Scanner có thể rà soát và phát hiện các sơ hở trong (Ports) là thế mạnh và cần thiết đối với tầng vận chuyển và phát hiện những dịch vụ sử dụng trên hệ thống đó.

Nó ghi lại những đáp ứng (Response) của hệ thống ở xa tương ứng với các dịch vụ mà nó phát hiện ra.

Đối với người quản trị mạng, nhưng hết sức nguy hiểm khi những kẻ phá hoại có thông tin này.

V.2.2. Bẻ khoá (Password Cracker)

- Chương trình bẻ khoá sẽ so sánh với mật khẩu (Password) đã mã hoá cần phá. Nếu không trùng hợp, quá trình lại quay lại.
- Chương trình bẻ khoá (Password Cracker) là chương trình có khả năng giải mã một mật khẩu đã được mã hoá hoặc có thể vô hiệu hoá chức năng bảo vệ mật khẩu của một hệ thống.
- Phương thức bẻ khoá này gọi là Bruce-Force.
- Hầu hết việc mã hoá các mật khẩu được tạo ra từ một phương thức mã hoá.
- Phương pháp này tuy không chuẩn tắc nhưng thực hiện nhanh vì dựa vào nguyên tắc khi đặt mật khẩu người sử dụng cũng thường tuân theo một số qui tắc để thuận tiện khi sử dụng.
- Các chương trình mã hoá sử dụng các thuật toán mã hoá để mã hoá mật khẩu.
- Thông thường các chương trình phá khoá thường kết hợp một số thông tin khác trong quá trình đó mật khẩu như: giản đồ sử dụng tập ký tự/ký số và SAM từ điển và sử dụng các từ lặp các từ liệt kê tuần tự, chuyển đổi cách phát âm của một từ…
- Có thể thay thế phá khoá trên một hệ thống phân tán đơn giản hơn so với tập phá khoá trên một Server cục bộ.
- Một danh sách các từ được tạo ra và thực hiện mã hoá từng từ.
- Biện pháp khắc phục là cần xây dựng một chính sách bảo vệ mật khẩu đúng đắn.

V.2.3. Trojans

- Một chương trình Trojan chạy không hợp lệ trên một hệ thống với vai trò như một chương trình hợp pháp.
- Nó thể hiện các chức năng không hợp pháp.
- Thông thường, Trojans có thể chạy được là do các chương trình hợp pháp đã bị thay đổi mã bằng những mã bất hợp pháp.
- Trojan có thể lây lan trên nhiều môi trường hệ điều hành khác nhau. Đặc biệt thường lây lan qua một số dịch vụ phổ biến như Mail, FTP... hoặc qua các tiện ích, chương trình miễn phí trên mạng Internet.
- Khi chương trình hoạt động thì Server đang sẵn sàng là nhiễm một số chức năng mà người sử dụng không biết.

- Trojan có nhiều loại khác nhau:
  - Có thể là chương trình thực hiện chức năng ẩn dấu
  - Có thể là một tiện ích tạo ra một thư mục ẩn trong thư mục tạo.
  - Một đoạn mã phá khoá
  - Có thể là một chương trình xử lý văn bản hoặc một tiện ích nào đó...
- Virus là một loại biến nhiễm của các chương trình Trojans, vì các chương trình virus chèn đầu các đoạn mã trong những chương trình sử dụng hợp pháp.
- Khi nhiễm một số loại Trojan sẽ tự động tắt các chương trình phòng chống virus, tường lửa và những phiên bản cũ, có nguy cơ tiềm tàng lây lan Trojans.

V.2.4. Sniffer

- Sniffer theo nghĩa đen là "đánh hơi" hay "ngửi". Sniffer có thể "ngửi" các giao thức TCP, UDP, IPX .. ở tầng mạng.
- Là các công cụ (có thể là phần cứng hoặc phần mềm) "tóm bắt" các thông tin lưu chuyển trên mạng để đánh hơi những thông tin có giá trị trao đổi trên mạng.
- Mặt khác, giao thức ở tầng IP được định nghĩa tường minh và cấu trúc các trường Header rõ ràng, nên việc giải mã các gói tin không khó khăn lắm.
- Mục đích của các chương trình Sniffer là thiết lập chế độ dùng chung (Promiscuous) trên các Card mạng Ethernet, nơi các gói tin trao đổi và tìm bắt các gói tin tại đây.

Sniffer theo nghĩa đen là "đánh hơi" hay "ngửi". Sniffer có thể "ngửi" các giao thức TCP, UDP, IPX .. ở tầng mạng.
Là các công cụ (có thể là phần cứng hoặc phần mềm) "tóm bắt" các thông tin lưu chuyển trên mạng để đánh hơi những thông tin có giá trị trao đổi trên mạng.
Mặt khác, giao thức ở tầng IP được định nghĩa tường minh và cấu trúc các trường Header rõ ràng, nên việc giải mã các gói tin không khó khăn lắm.
Mục đích của các chương trình Sniffer là thiết lập chế độ dùng chung (Promiscuous) trên các Card mạng Ethernet, nơi các gói tin trao đổi và tìm bắt các gói tin tại đây.
Vì vậy, nó có thể tóm bắt các gói tin IP Datagram và Ethernet Packet.
Hoạt động của Sniffer cũng giống như các chương trình "tóm bắt" các thông tin gõ từ bàn phím (Key Capture).
Tuy nhiên các tiện ích Key Capture chỉ thực hiện trên một trạm làm việc cụ thể. Sniffer có thể bắt được các thông tin trao đổi giữa nhiều trạm làm việc với nhau.

V.3. Biện pháp đảm bảo an ninh mạng

- Thực tế không có biện pháp hữu hiệu nào đảm bảo an toàn tuyệt đối cho mạng.
- Hệ thống bảo vệ dù có chắc chắn đến đâu thì cũng có lúc bị vô hiệu hoá bởi những kẻ phá hoại điêu luyện.
- Có nhiều biện pháp đảm bảo an ninh mạng.

V.3.1. Bảo vệ thông tin bằng mật mã (Cryptography)

- Mật mã là quá trình chuyển đổi thông tin gốc sang dạng mã hóa (Encryption).
- Có hai cách tiếp cận để bảo vệ thông tin bằng mật mã:
  - Theo đường truyền (Link Oriented Security)
  - Từ mút-đến-mút (End-to-End).
- Cách thứ nhất:
- Cách thứ hai:

- Đặc điểm: thông tin được mã hoá để bảo vệ trên đường truyền giữa 2 nút không quan tâm đến nguồn và đích của thông tin đó.
- Ưu điểm: là có thể bí mật được luồng thông tin giữa nguồn và đích và có thể ngăn chặn được toàn bộ các vi phạm nhằm phân tích thông tin trên mạng.
- Nhược điểm: là vì thông tin chỉ được mã hoá trên đường truyền nên đòi hỏi các nút phải được bảo vệ tốt.

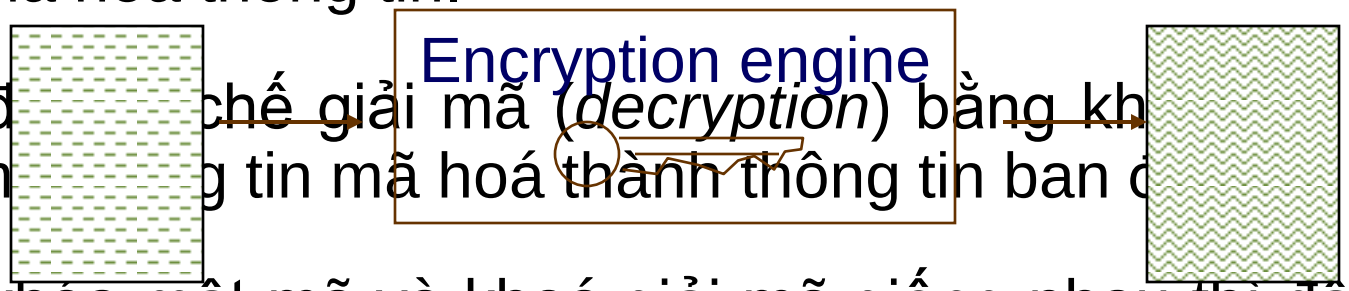
Đặc điểm: thông tin được bảo vệ trên toàn đường đi từ nguồn tới đích. Thông tin được mã hoá ngay khi mới được tạo ra và chỉ được giải mã khi đến đích.

Ưu điểm: là người sử dụng có thể dùng nó mà không ảnh hưởng gì đến người sử dụng khác.

Nhược điểm: là chỉ có dữ liệu người sử dụng được mã hoá, còn thông tin điều khiển phải giữ nguyên để có thể xử lý tại các node.

Quá trình mã hóa

- Thông tin ban đầu (*plaintext*) cần được thay đổi (*mật mã hoá - encryption*) thành thông tin được mã hoá (*cyphertext*).
- Một cơ chế mật mã bằng khóa mật mã được sử dụng để mật mã hoá thông tin.
- Sau đ chế giải mã (*decryption*) bằng kh mã sẽ giải m g tin mã hoá thành thông tin ban đ
- Nếu khóa mật mã và khoá giải mã giống nhau thì đây là hệ thống mật mã dùng khoá đối xứng (*symmetric key*). Ngoài ra còn có hệ thống mật mã dùng khóa không đối xứng (*asymmetric key*)

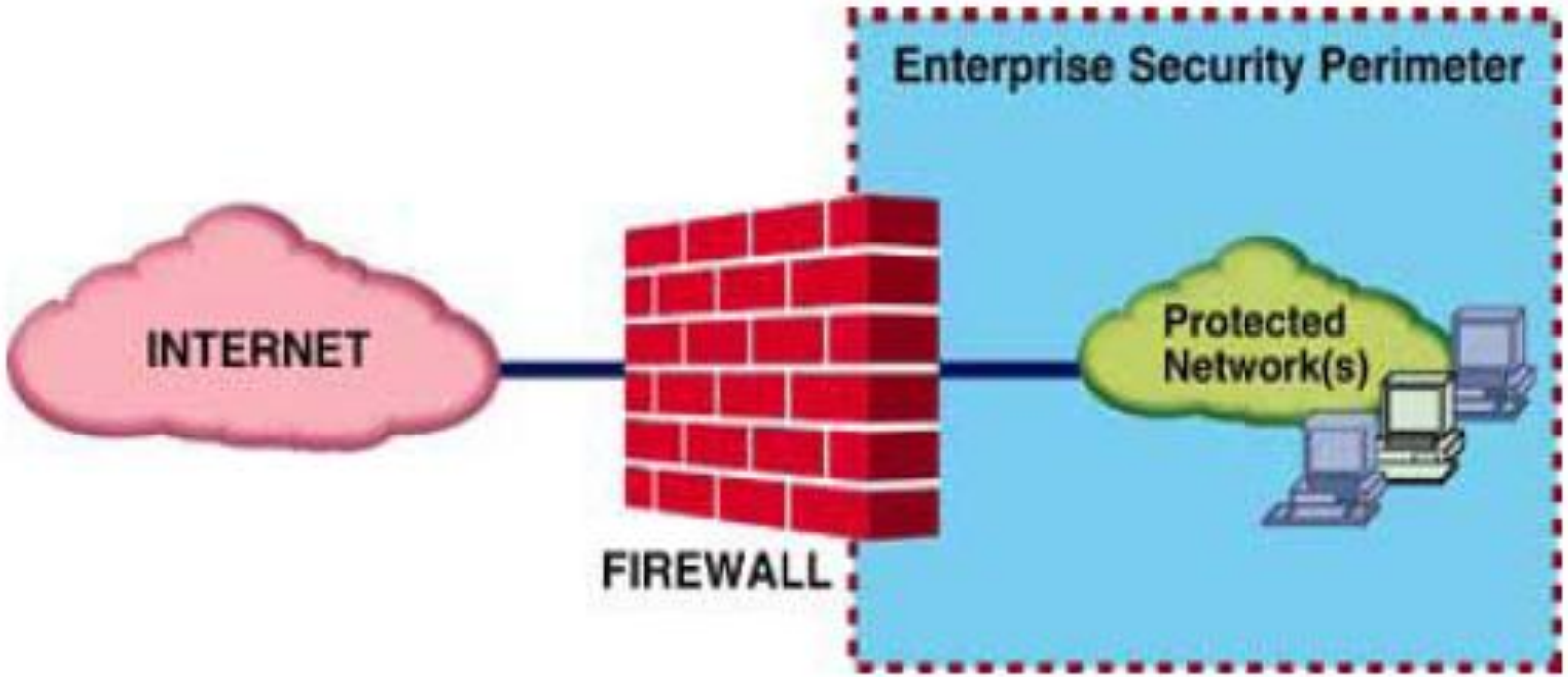


Một số giải thuật mật mã kinh điển

- Giải thuật DES (Dataencryption Standard)
- Khoá công khai (Public key):
  - Các phương pháp mật mã chỉ dùng một khoá cho cả mã hoá lẫn giải mã đòi hỏi người gửi và người nhận phải biết khoá và giữ bí mật.
  - Tồn tại chính của các phương pháp này là làm thế nào để phân phối khoá một cách an toàn, đặc biệt trong một môi trường nhiều người sử dụng.
  - Để khắc phục, người ta thường sử dụng phương pháp mã hoá 2 khoá, một khoá công khai để mã hoá và một khoá bí mật để giải mã.
- Giải thuật RSA
  - Khoá công khai 64 bits trong đó 56 bits được dùng mã hoá và 8 bits còn lại được dùng để kiểm soát lỗi.
  - Một khối dữ liệu cần mã hoá sẽ được xử lý như một số nhị phân lớn.
  - Mã hoá từng khối 64 bits của văn bản gốc thành 64 bits văn bản mật bằng một khoá.
  - Giải thuật RSA dựa trên nhận xét sau: phân tích ra thừa số của tích của 2 số nguyên tố rất lớn cực kỳ khó khăn.
  - Trong giải thuật RSA mỗi tram lựa chọn ngẫu nhiên 2 số nguyên tố lớn p và q và nhân chúng với nhau để có tích n=pq (p và q được giữ bí mật).

V.3.2. Bức tường lửa (Firewall)

- Firewall là một hệ thống dùng để tăng cường khống chế



- Tiến hành đồ thị giám sát và cảnh báo sự tấn công đối với mạng lưới.

Ưu điểm, nhược điểm của bức tường lửa

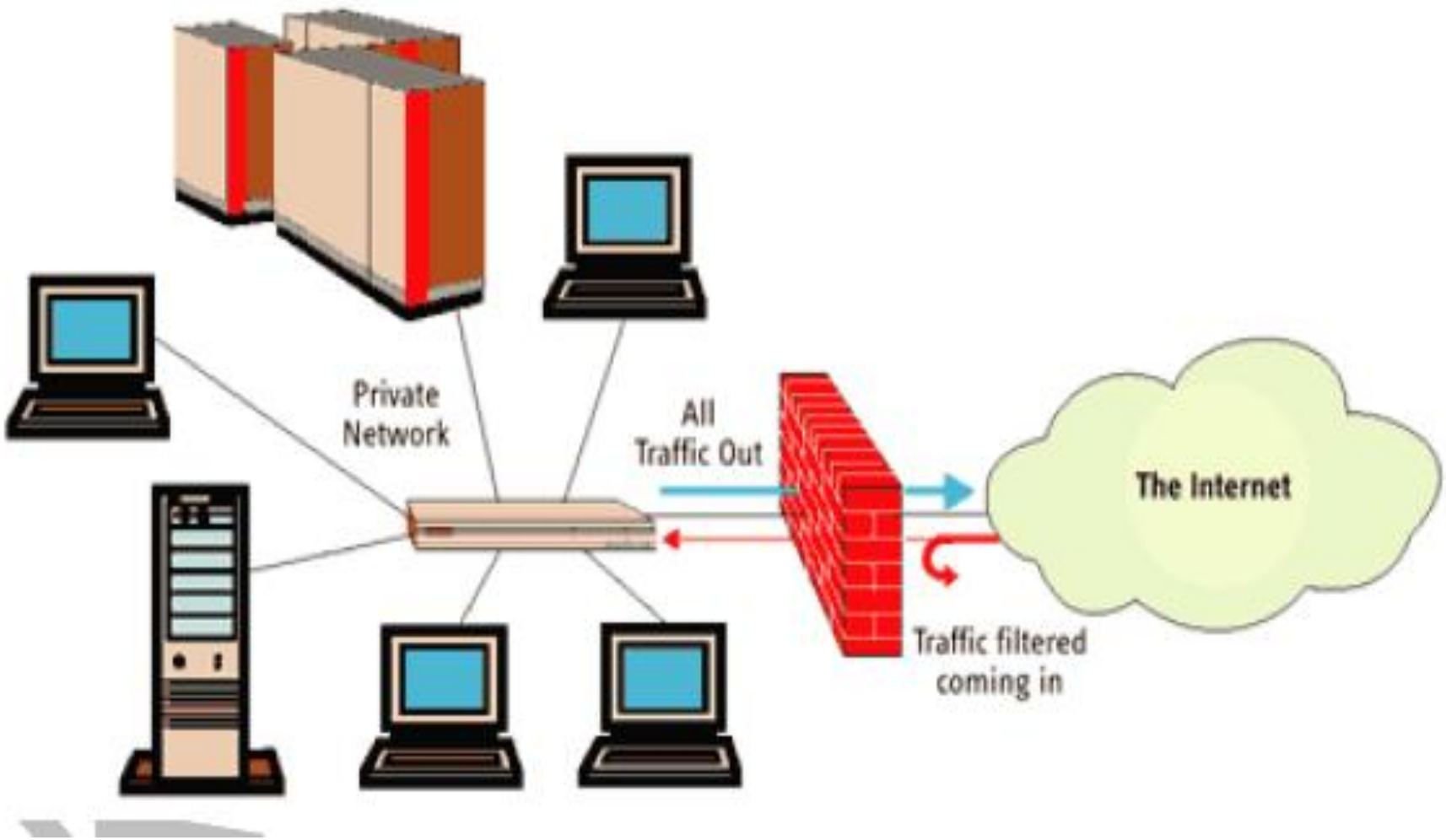
a. Ưu điểm:

- Bảo vệ mạng nội bộ. Cho phép người quản trị mạng xác định một điểm khống chế ngăn chặn để phòng ngừa tin tặc, kẻ phá hoại, xâm nhập mạng nội bộ.
- Cấm không cho các loại dịch vụ kém an toàn ra vào mạng, đồng thời chống trả sự công kích đến từ các đường khác.
- Tính an toàn tập trung, tính an toàn mạng được củng cố trên hệ thống Firewall mà không phải phân bố trên tất cả mấy chủ của mạng.
- Bảo vệ những dịch vụ yếu kém trong mạng. Firewall dễ dàng giám sát tính an toàn mạng và phát ra cảnh báo.
- Firewall có thể giấu đi thông tin hệ thống mạng như: Tất cả các máy trong mạng có thể dùng một địa chỉ IP của Firewall khi truy cập Internet, che dấu cấu trúc của mạng nội bộ.
- Tăng cường tính bảo mật, nhấn mạnh quyền sở hữu.
- Firewall được sử dụng để quản lý lưu lượng từ mạng ra ngoài, xây dựng phương án chống nghẽn.

b. Nhược điểm

- Hạn chế dịch vụ có ích, vì để nâng cao tính an toàn mạng, người quản trị hạn chế hoặc đóng nhiều dịch vụ có ích của mạng.
- Không phòng hộ được sự tấn công của kẻ phá hoại trong mạng nội bộ.
- Không thể ngăn chặn sự tấn công thông qua những con đường khác ngoài bức tường lửa.
- Firewall Internet không thể hoàn toàn phòng ngừa được sự phá của phần mềm có hại tải về từ Internet và virus.

Lọc gói tin tại firewall



V.3.3. Các loại Firewall

- Firewall lọc gói:
- Firewall cổng mạng hai ngăn:
- Firewall che chắn
- Firewall che chắn mạng con

- Thường là một bộ định tuyến có lọc.
- Là loại Firewall cơ bản nhất, nó thường được cài đặt trên một bộ định tuyến.
- Khi nhận một gói dữ liệu, nó quyết định cho phép qua hoặc chặn lại dựa trên một số tiêu chuẩn đã được thiết lập trước.
- Ví dụ một cửa hỏi tới một mạng bên ngoài, không tin tưởng vào một máy chủ bên trong, hoặc chặn các gói tin đến từ một địa chỉ IP cụ thể.
- Đặc điểm lớn nhất Firewall loại này là gói tin IP bị chặn lại hoàn toàn mà không có thông báo.

- Hệ thống Firewall che chắn mạng sử dụng hai bộ định tuyến lọc gói và một máy chủ kiên cố, cho phép thiết lập chính sách an ninh ở hai mức: mạng và ứng dụng.
- Hệ thống Firewall an toàn nhất vì nó đảm bảo chức năng an toàn tầng mạng và tầng ứng dụng.

- Hệ thống Firewall có cấp an toàn cao hơn so với hệ thống Firewall lọc gói thông thường vì nó đảm bảo an toàn tầng mạng (lọc gói) và tầng ứng dụng (dịch vụ đại lý).

V.3.4. Kỹ thuật Firewall

- Lọc khung (Frame Filtering):
  - Hoạt động trong tầng 2 của mô hình OSI, có thể lọc, kiểm tra được ở mức bit và nội dung của khung tin (Ethernet 802.3, Token Ring 802.5, FDDI, ...)
  - Trong tầng này các khung dữ liệu không tin cậy sẽ bị từ chối ngay trước khi vào mạng.
  - Nó kiểm tra toàn bộ đoạn dữ liệu để quyết định xem đoạn dữ liệu đó có thoả mãn một trong số các quy định của lọc Packet hay không.
  - Các quy tắc lọc Packet dựa vào các thông tin trong Packet Header.
- Lọc gói (Packet Filtering):
  - Một số Firewall chuyên dụng có tích hợp chức năng lọc gói tin ở tầng mạng của mô hình OSI.
  - Lọc gói cho phép hay từ chối gói tin mà nó nhận được.
  - Nó sử dụng địa chỉ IP nguồn làm chỉ thị, nếu một gói tin mang địa chỉ nguồn là địa chỉ giả thì nó sẽ chiếm được quyền truy nhập vào hệ thống.
- Tuy nhiên có nhiều biện pháp kỹ thuật có thể được áp dụng cho việc lọc gói tin nhằm khắc phục nhược điểm trên, ngoài trường địa chỉ IP được kiểm tra, còn có các thông tin khác được kiểm tra với các quy tắc được tạo ra trên Firewall, các thông tin này có thể là thời gian truy nhập, giao thức sử dụng, cổng ...

III.5. Kỹ thuật Proxy

- Là hệ thống Firewall trung gian cho các kết nối trực tiếp từ máy khách yêu cầu.
- Proxy hoạt động dựa trên phần mềm. Khi một người sử dụng nào đó đến mạng sử dụng Proxy thì kết nối đó sẽ bị chặn lại, sau đó Proxy sẽ kiểm tra các trường có liên quan đến yêu cầu kết nối.
- Nếu việc kiểm tra thành công, có nghĩa là các trường thông tin đáp ứng được các quy tắc đã đặt ra, nó sẽ tạo một cầu kết nối giữa máy khách với Firewall.

Ưu điểm của Firewall loại này là khả năng có thể cản lọc chuyển tiếp các gói tin IP và có thể điều khiển một cách chi tiết hơn các kết nối thông qua Firewall. Cung cấp nhiều công cụ cho phép ghi lại các quá trình kết nối. Các gói tin chuyển qua Firewall đều được kiểm tra kỹ lưỡng với các quy tắc trên Firewall, điều này phải trả giá cho tốc độ xử lý.

Khi một máy chủ nhận các gói tin từ mạng ngoài rồi chuyển chúng vào mạng trong, sẽ tạo ra một lỗ hổng cho các kẻ phá hoại (Hacker) xâm nhập từ mạng ngoài vào mạng trong.

Nhược điểm của kiểu Firewall này là hoạt động dựa trên trình ứng dụng uỷ quyền (Proxy).

V.4. Mạng riêng ảo (VPN-Virtual Private Network)

1. Khái niệm
2. Kiến trúc của mạng riêng ảo
3. Những ưu điểm của mạng VPN
4. Giao thức PPTP (Point to Point Tunnelling Protocol)
5. Giao thức L2F (Layer Two Forwarding Protocol)
6. Giao thức L2TP (Layer Two Tunnelling Protocol)
7. Giao thức IPSEC

V.4.1. Khái niệm mạng riêng ảo

- Mạng máy tính ban đầu được triển khai với 2 kỹ thuật chính: đường thuê riêng (Leased Line) cho các kết nối cố định và đường quay số (Dial-up) cho các kết nối không thường xuyên.
- Các mạng này có tính bảo mật cao, nhưng khi lưu lượng thay đổi và đòi hỏi tốc độ cao nên đã thúc đẩy hình thành một kiểu mạng dữ liệu mới, mạng riêng ảo.
- Mạng riêng ảo được xây dựng trên các kênh logic có tính "ảo". Xu hướng hội tụ của các mạng trên nền NGN tạo điều kiện cho sự xuất hiện nhiều dịch vụ mới, trong đó có dịch vụ mạng riêng ảo.
- Mạng riêng ảo là một mạng máy tính, trong đó các điểm của khách hàng được kết nối với nhau trên một cơ sở hạ tầng chia sẻ với cùng một chính sách truy nhập và bảo mật như trong mạng riêng.

V.4.1. Khái niệm mạng riêng ảo

- Có 2 dạng chính mạng riêng ảo VPN là:
  - Remote Access VPN: cho phép thực hiện các kết nối truy nhập từ xa đối với người sử dụng di động (máy tính cá nhân hoặc các Personal Digital Assistant) với mạng chính (LAN hoặc WAN) qua đường quay số, ISDN, đường thuê bao số DSL.
  - Site- to - Site VPN: dùng để kết nối các mạng tại các vị trí khác nhau thông qua kết nối VPN.
- Có thể chia thành 2 loại khác:
  - Intranet VPN kết nối các văn phòng ở xa với trụ sở chính thường là các mạng LAN với nhau.
  - Extranet VPN là khi Intranet VPN của một khách hàng mở rộng kết nối với một Intranet VPN khác.

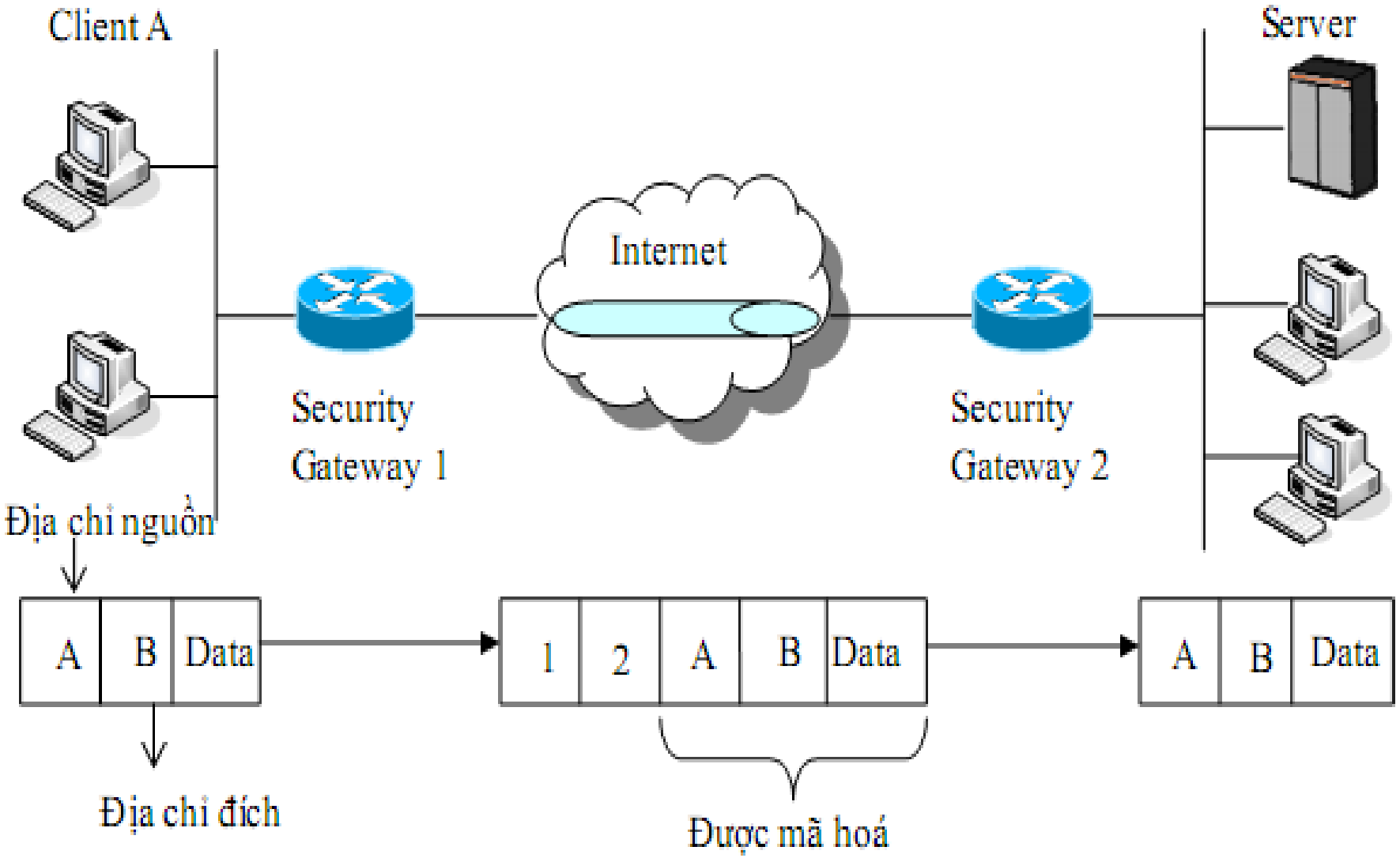
V.4.1. Khái niệm mạng riêng ảo

- Bảo mật là một yếu tố quan trọng bảo đảm cho VPN hoạt động an toàn và hiệu quả. Kết hợp với các thủ tục xác thực người dùng, dữ liệu được bảo mật thông qua các kết nối đường hầm (Tunnel) được tạo ra trước khi truyền dữ liệu.
- Tunnel là kết nối ảo điểm - điểm (Point to Point) và làm cho mạng VPN hoạt động như một mạng riêng.
- Dữ liệu truyền trên VPN có thể được mã hoá theo nhiều thuật toán khác nhau với các độ bảo mật khác nhau.
- Người quản trị mạng có thể lựa chọn tuỳ theo yêu cầu bảo mật và tốc độ truyền dẫn.
- Giải pháp VPN được thiết kế phù hợp cho những tổ chức có xu hướng tăng khả năng thông tin từ xa, các hoạt động phân bố trên phạm vi địa lý rộng và có các cơ sở dữ liệu, kho dữ liệu, hệ thống thông tin dùng riêng với yêu cầu đảm bảo an ninh cao.

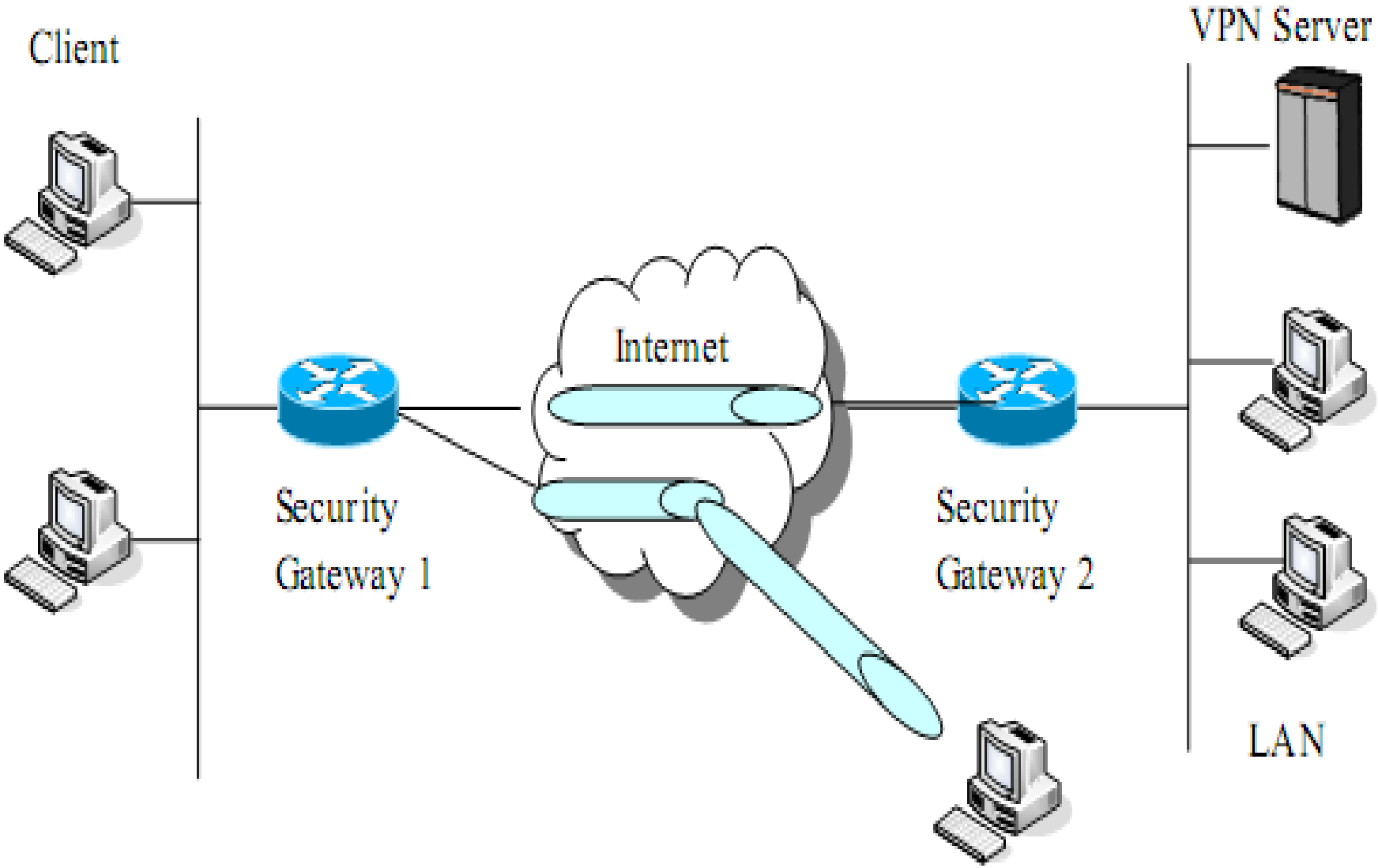
V.4.2. Kiến trúc của mạng riêng ảo

- Hai thành phần cơ bản của Internet tạo nên mạng riêng ảo VPN, đó là:
  - Đường hầm (Tunnelling) cho phép làm "ảo" một mạng riêng.
  - Các dịch vụ bảo mật đa dạng cho phép dữ liệu mang tính riêng tư.
- Đường hầm:
  - Là kết nối giữa 2 điểm cuối khi cần thiết.
  - Khi kết nối này sẽ được giải phóng khi không truyền dữ liệu dành băng thông cho các kết nối khác.
  - Kết nối này mang tính logic "ảo" không phụ thuộc vào cấu trúc vật lý của mạng.
  - Nó che giấu các các thiết bị như bộ định tuyến, chuyển mạch và trong suốt đối với người dùng.

Cấu trúc một đường hầm



Đường hầm trong các cấu trúc LAN và Client



Cách thức tạo đường hầm

- Đường hầm được tạo ra bằng cách đóng gói các gói tin (Encapsulate) để truyền qua Internet. Đóng gói có thể mã hoá gói gốc và thêm vào tiêu đề IP mới cho gói. Tại điểm cuối, dạng gói tin tạo đường hầm: IP Header, AH, ESP, Tiêu đề và dữ liệu.
- Đường hầm có 2 loại: Thường trực (Permanent) và tạm thời (Temporary hay Dynamic).
- Thông thường các mạng riêng ảo VPN sử dụng dạng đường hầm động. Đường hầm động rất hiệu quả cho VPN, vì khi không có nhu cầu trao đổi thông tin thì được huỷ bỏ.
- Đường hầm có thể kết nối 2 điểm cuối theo kiểu LAN- to - LAN tại các cổng bảo mật (Security Gateway), khi đó người dùng trên các LAN có thể sự dụng đường hầm này. Còn đối với trường hợp Client- to - LAN, thì Client phải khởi tạo việc xây dựng đường hầm trên máy người dùng để thông tin với cổng bảo mật để đến mạng LAN đích.

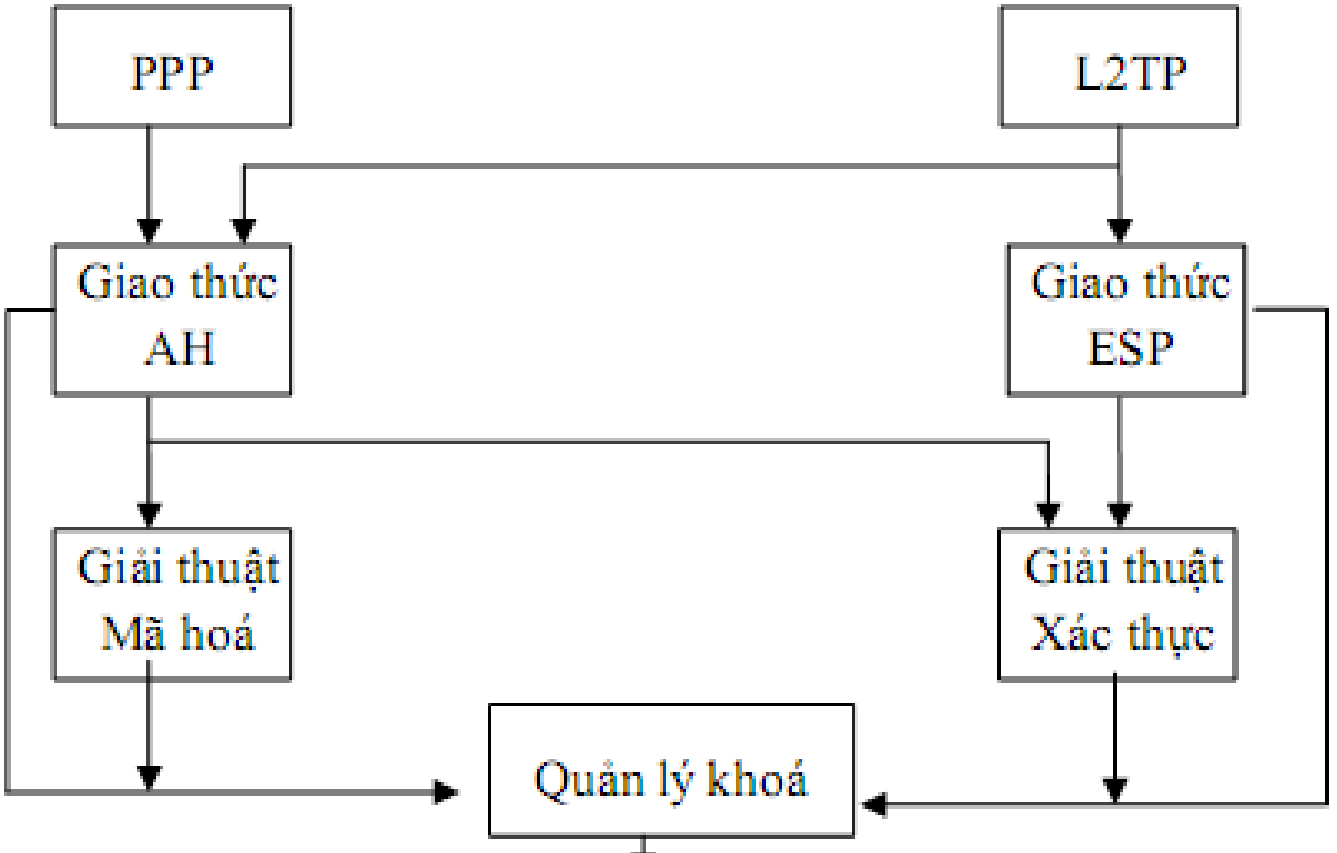
V.4.3. Những ưu điểm của mạng VPN

- **Chi phí**:
  - Công nghệ VPN cho phép tiết kiệm đáng kể chi phí thuê kênh riêng hoặc các cuộc gọi đường dài bằng chi phí cuộc gọi nội hạt.
  - Hơn nữa, sử dụng kết nối đến ISP còn cho phép vừa sử dụng VPN vừa truy nhập Internet.
  - Công nghệ VPN cho phép sử dụng băng thông đạt hiệu quả cao nhất. Giảm nhiều chi phí quản lý, bảo trì hệ thống.
- **Truy nhập dễ dàng**:
  - Người sử dụng trên VPN, ngoài việc sử dụng các tài nguyên trên VPN còn được sử dụng các dịch vụ khác của Internet mà không cần quan tâm đến phần phức tạp ở tầng dưới.

V.4.4. Giao thức PPTP (Point to Point Tunnelling Protocol)

- PPP là giao thức tầng 2-Data link, truy nhập mạng WAN như HDLC, SDLC, X.25, Frame Relay, Dial on Demand.
- PPP có thể sử dụng cho nhiều giao thức lớp trên như TCP/IP, Novell/IPX, Apple Talk nhờ sử dụng NCP - Network Control Protocol.
- PPP sử dụng Link Control Protocol để thiết lập và điều khiển các kết nối. PPP sử dụng giao thức xác thực PAP hoặc CHAP.
- PPTP dựa trên PPP để thực thi các chức năng sau:
  - Thiết lập và kết thúc kết nối vật lý.
  - Xác thực người dùng
  - Tạo gói dữ liệu PPP.

V.4.5. Giao thức L2F (Layer Two Forwarding Protocol)



thức không phải là IP, ví dụ như là IPX và NETBEUI.

V.4.7. Giao thức IPSEC

- IPSec bảo đảm tính tin cậy, tính toàn vẹn và tính xác thực truyền dữ liệu qua mạng IP công cộng. IPSec định nghĩa 2 loại tiêu đề cho gói IP điều khiển quá trình xác thực và mã hóa:
- Một là xác thực tiêu đề Authentication Header (AH), hai là đóng gói bảo mật tải Encapsulating Security Payload (ESP).
- Xác thực tiêu đề AH đảm bảo tính toàn vẹn cho tiêu đề gói và dữ liệu.
- Đóng gói bảo mật tải ESP thực hiện mã hóa và đảm bảo tính toàn vẹn cho gói dữ liệu nhưng không bảo vệ tiêu đề cho gói IP như AH.
- IPsec sử dụng giao thức Internet Key Exchange IKE để thỏa thuận liên kết bảo mật SA giữa hai thực thể và trao đổi các thông tin khóa. IKE cần được sử dụng phần lớn các ứng dụng thực tế để đem lại thông tin liên lạc an toàn trên diện rộng.

Thanksss

Tổng quan về mạng máy tính

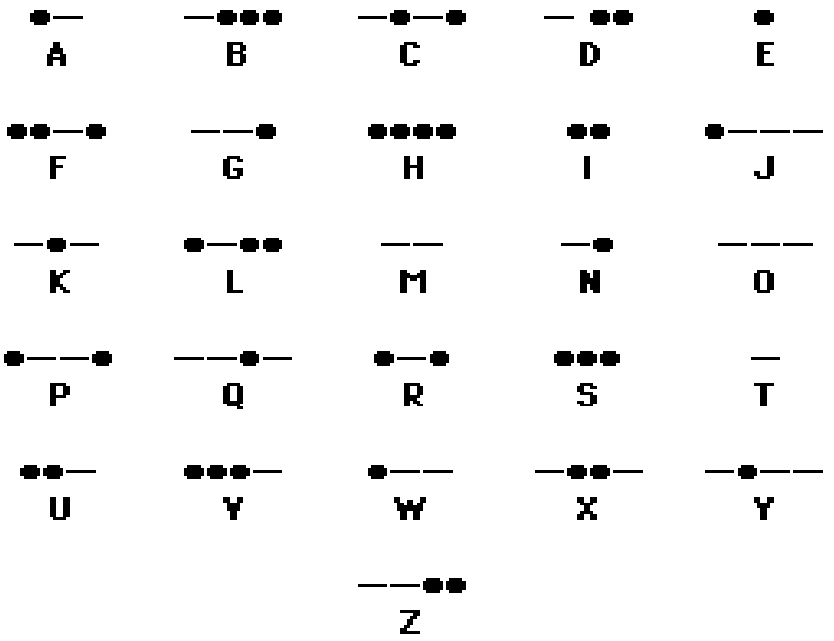
Trình bày: Ngô Bá Hùng
Khoa Công Nghệ Thông Tin&TT
Đại Học Cần Thơ

Tổng quan về mạng máy tính

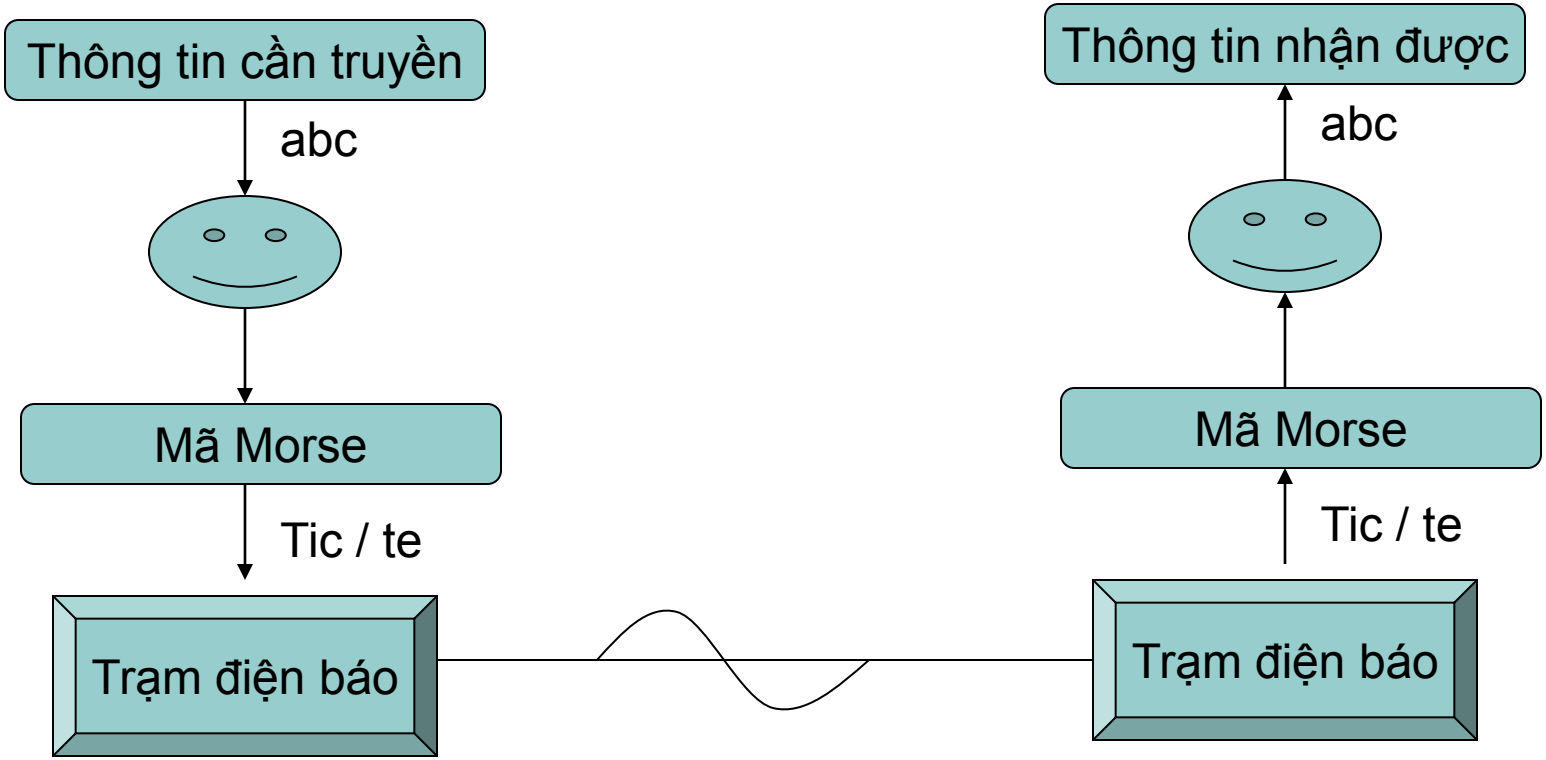
- Các mạng truyền dữ liệu
- Cấu trúc mạng máy tính
- Các phương pháp truyền tải thông tin
- Lợi ích mạng máy tính

Mạng điện báo

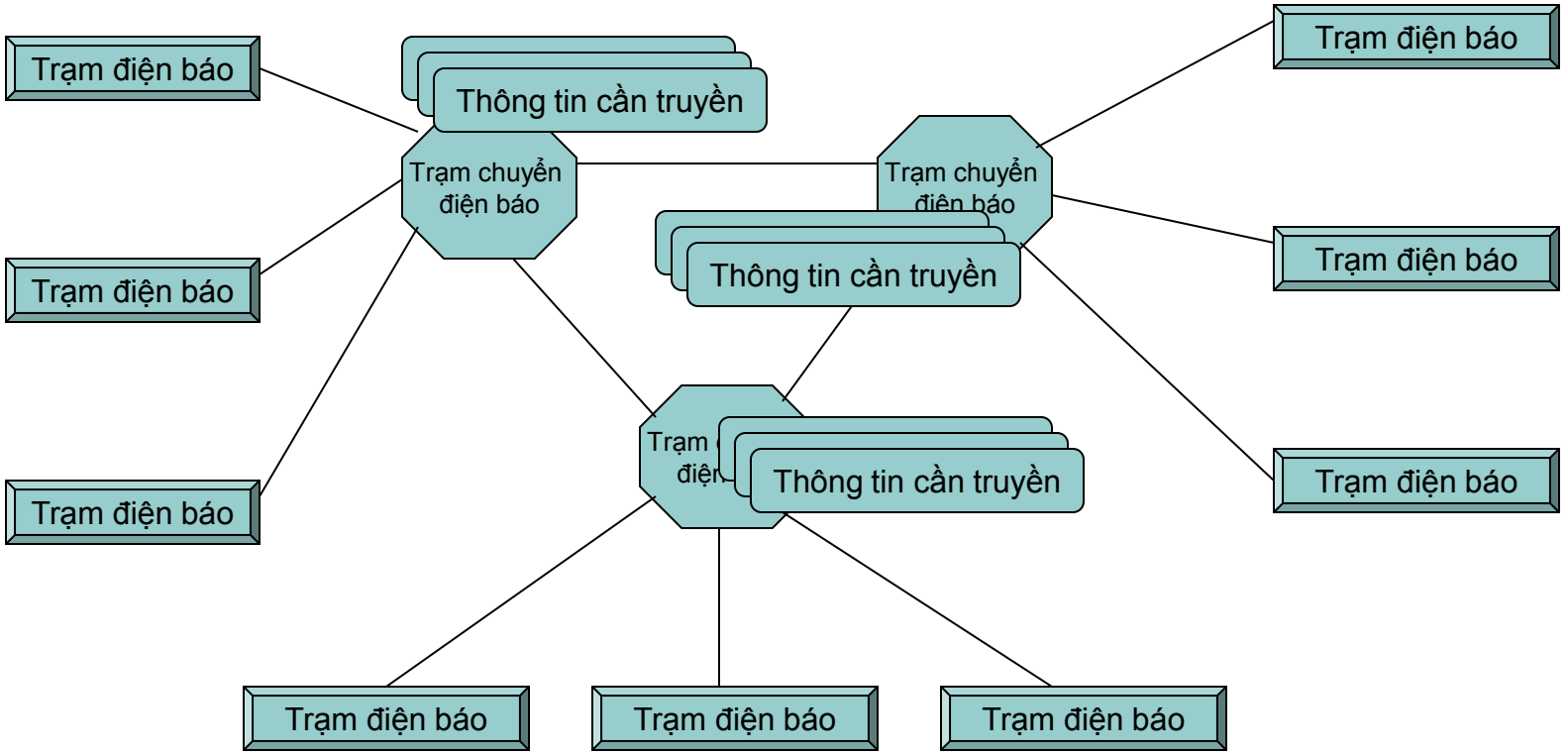
- Sử dụng mã Morse để mã hóa dữ liệu truyền đi



Mạng điện báo

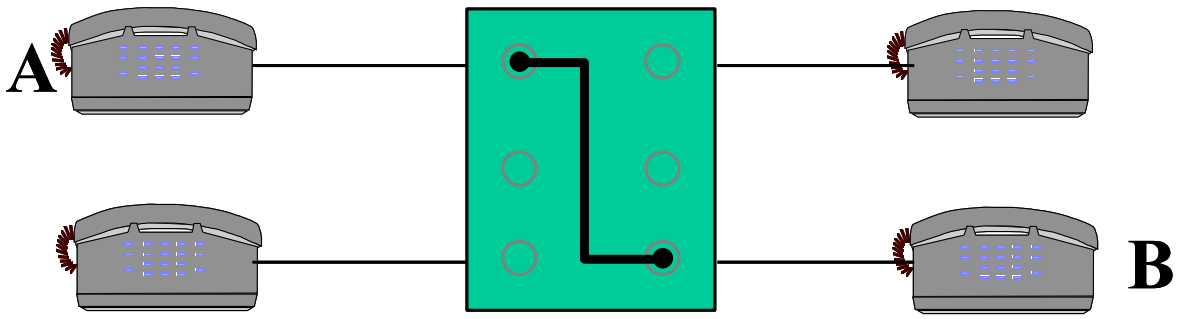


Mạng điện báo



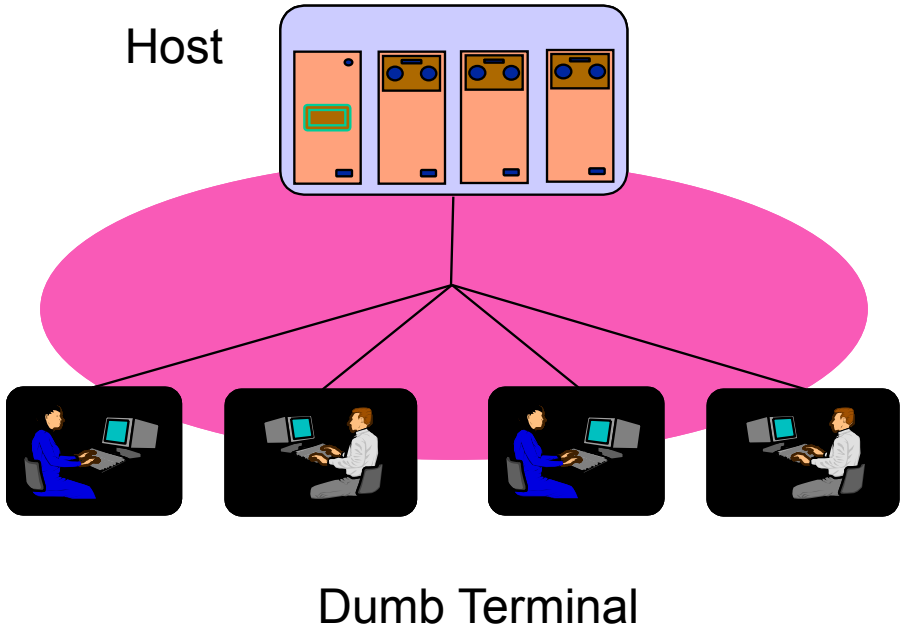
Mạng điện thoại

- Mạng chuyển mạch định hướng nối kết
- Thiết lập nối kết tận hiến giữa hai bên truyền nhận



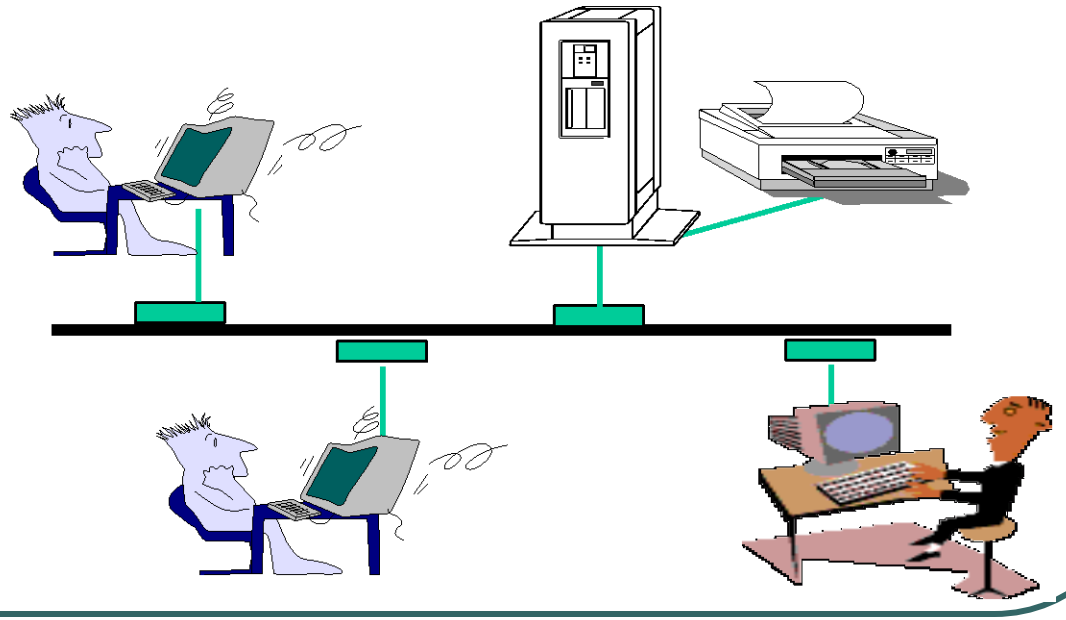
Mạng hướng đầu cuối

- Mạng của các máy tính lớn (Main Frame)



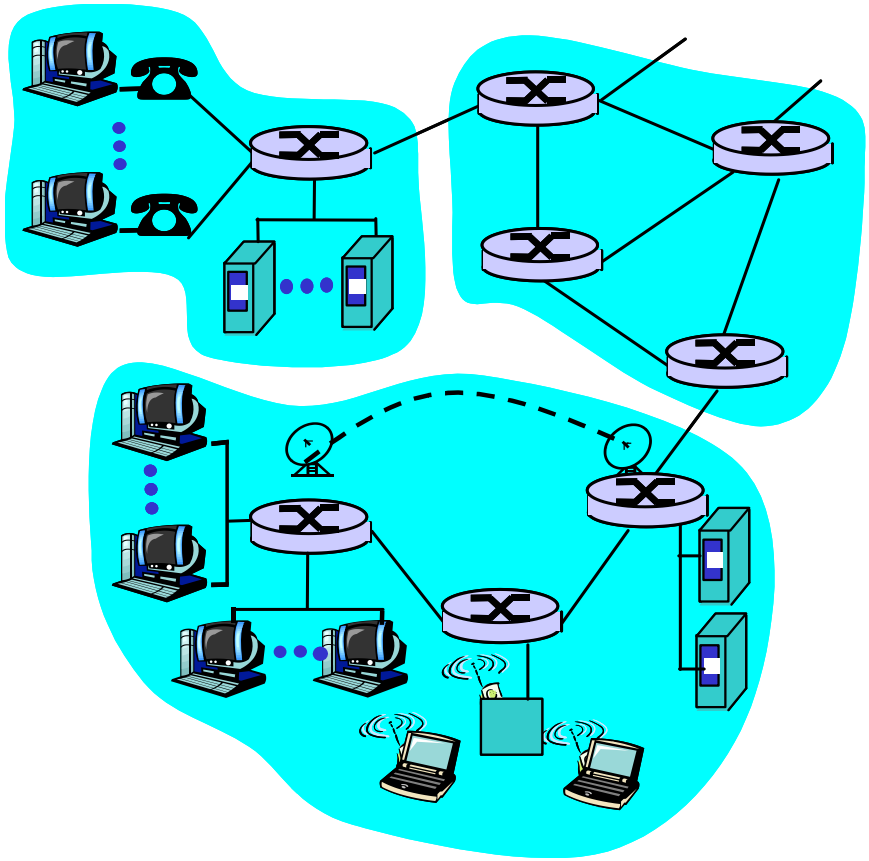
Mạng máy tính

- Mạng của hai hay nhiều máy tính được nối lại với nhau bằng một đường truyền vật lý theo một kiến trúc nào đó.



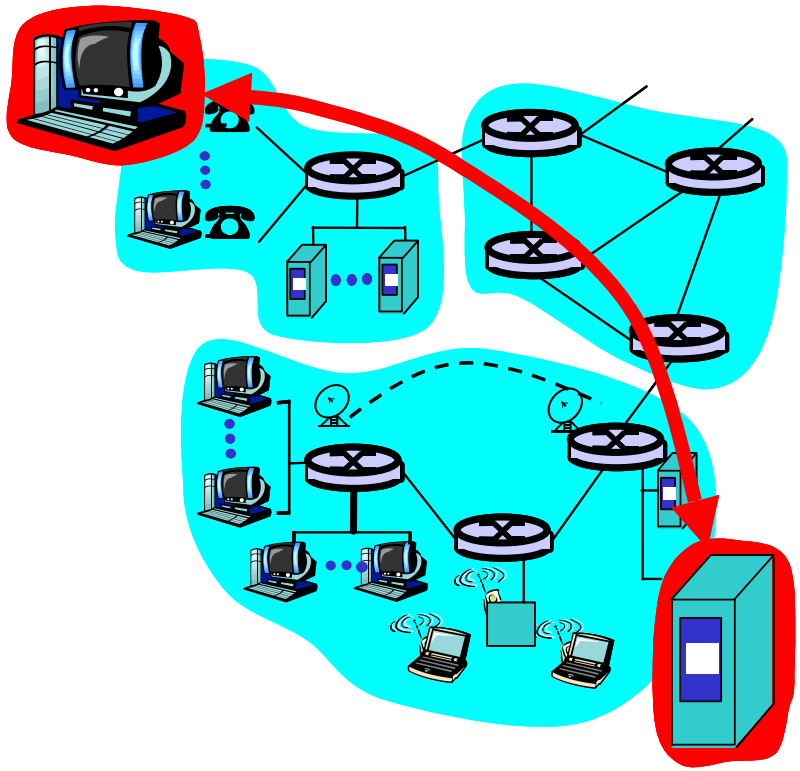
Mạng máy tính

- Mạng đầy đủ gồm 3 thành phần:
  - Đường biên mạng
  - Mạng đường trục
  - Mạng truy cập

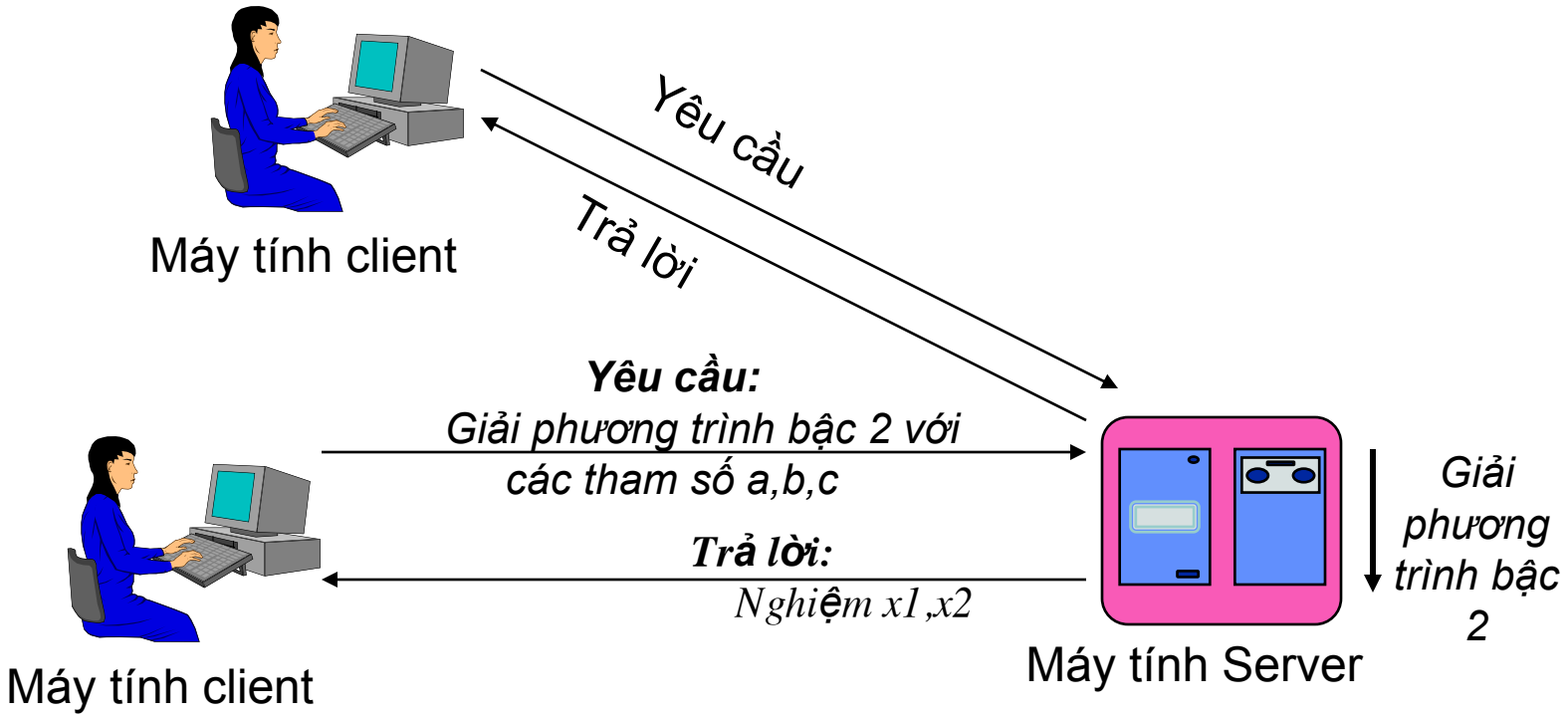


Đường biên mạng (Network edge)

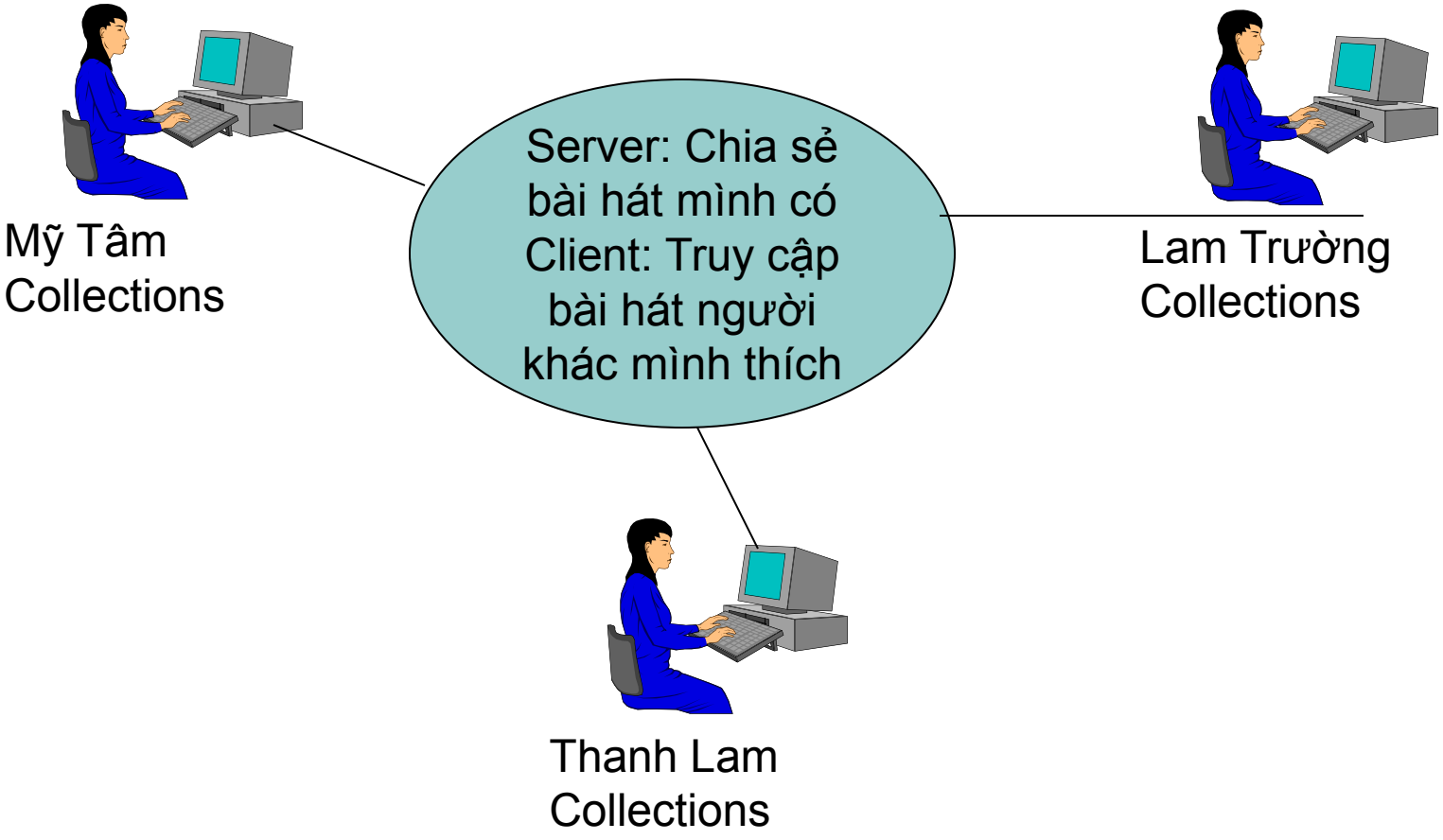
- Host & Application
- End Systems
- Tổ chức theo mô hình Client-Server hoặc Peer2Peer



Mô hình client/server

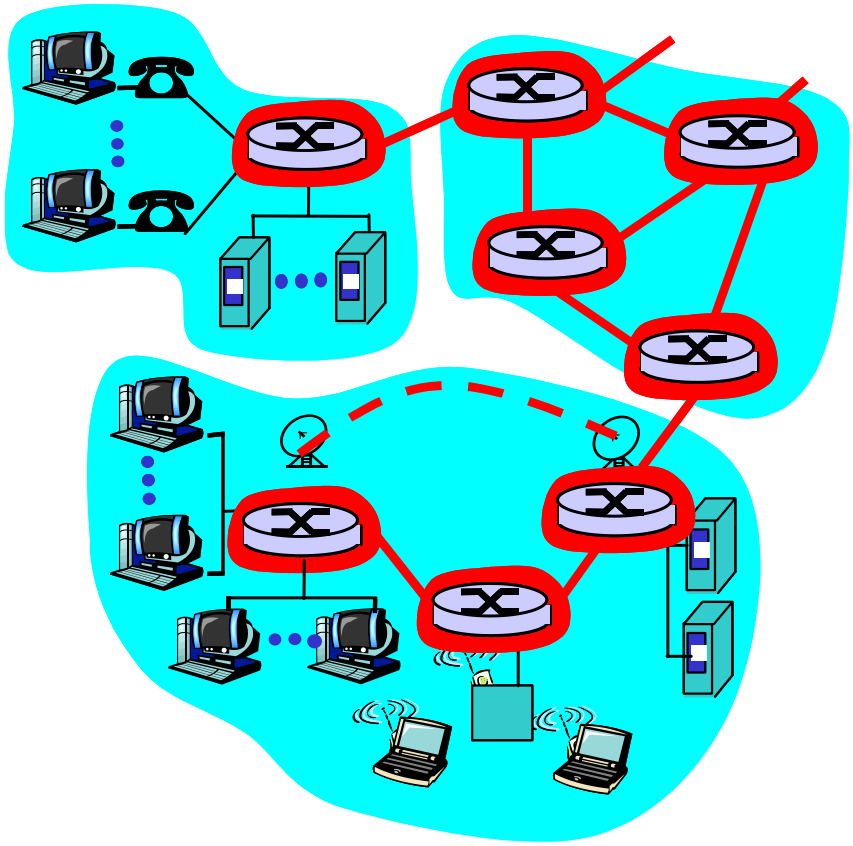


Mô hình Peer2Peer



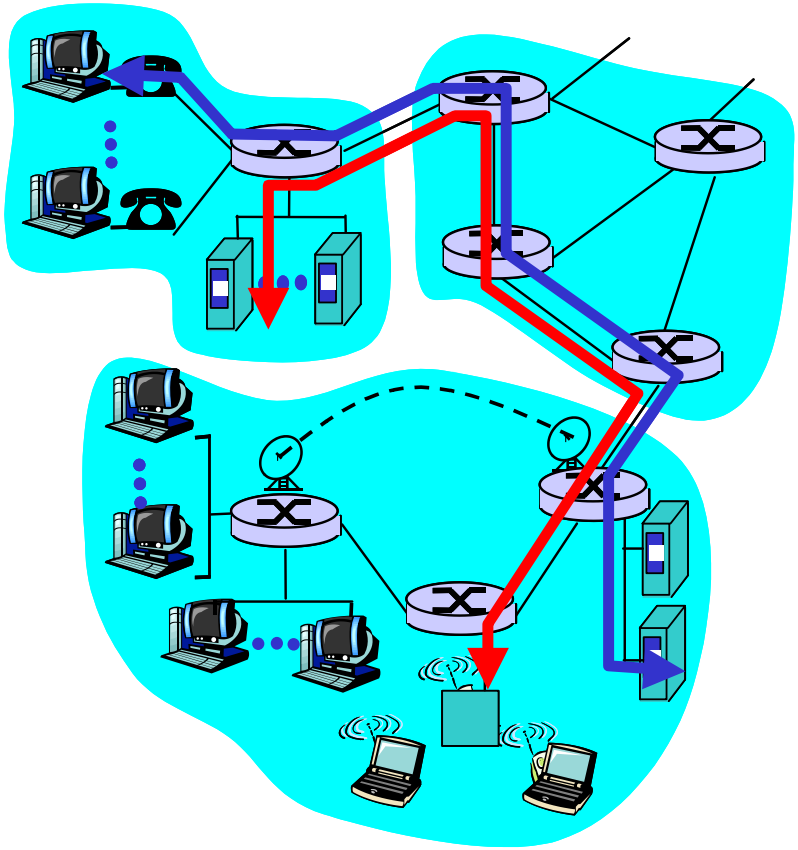
Mạng đường trục (Network core)

- Mạng của các router
- Đảm bảo thông tin thông suốt giữa hai máy tính cách xa nhau
- Hai chế độ truyền tin:
  - Chuyển mạch
  - Chuyển gói



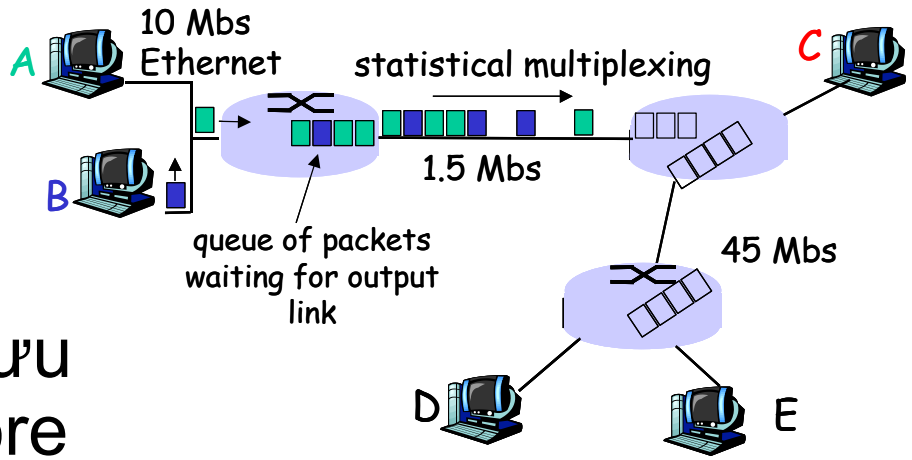
Mạng chuyển mạch (Circuit switching network)

- Thiết lập kênh truyền tận hiến giữa hai bên truyền nhận
- Hai phương pháp thực hiện:
  - Phân chia theo tần số (FDMA-Frequency Division Multi Access)
  - Phân chia theo thời gian (TDMA- Time Division Multi Access)



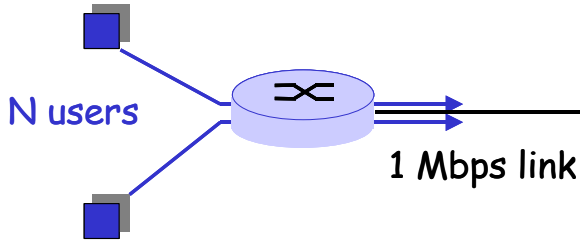
Mạng chuyển gói (Packet Passing Network)

- Thông tin truyền đi trong những đơn vị là gói tin (packet)



- Sử dụng kỹ thuật lưu và chuyển tiếp (store and forward)

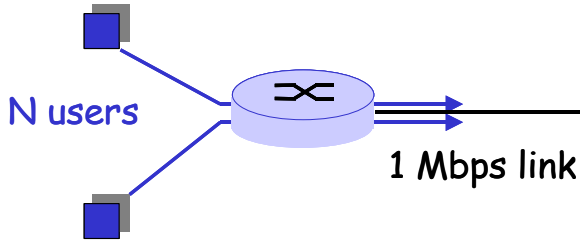
So sánh giữa mạng chuyển mạch và mạng chuyển gói



- Một đường truyền 1 Mbit
- Mỗi người dùng được cấp 100Kbps khi truy cập "active"
- Thời gian active chiếm 10% tổng thời gian.

- Khi đó:
  - circuit-switching: cho phép tối đa 10 users
  - packet switching: cho phép 35 users, (xác suất có hơn 10 "active" đồng thời là nhỏ hơn 0.004)

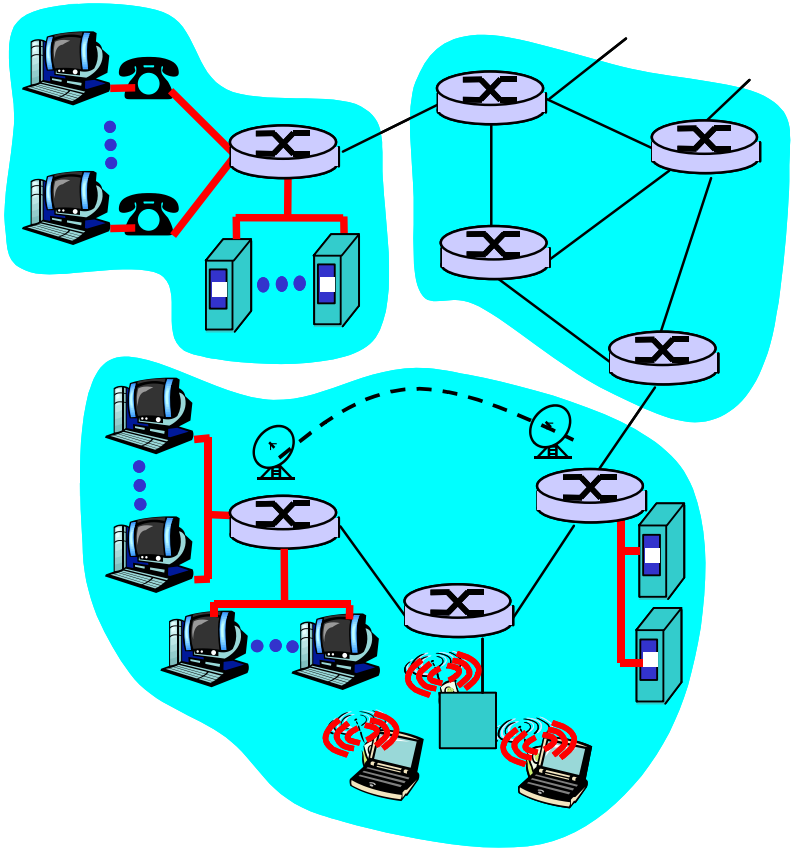
So sánh giữa mạng chuyển mạch và mạng chuyển gói



- Mạng 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

Mạng truy cập (Access Network)

- Nối máy tính vào các router ngoài bìa
- Ví dụ:
  - Dial qua đường điện thoại hay đường ADSL.
  - Mạng cục bộ cho các công ty, xí nghiệp.
  - Mạng không dây



Lợi ích của mạng

- Chia sẻ tài nguyên phần cứng, phần mềm, dữ liệu
- Nâng cao độ tin cậy của hệ thống
- Giúp nâng cao hiệu suất công việc
- Giảm chi phí đầu tư
- Tăng cường tính bảo mật thông tin
- Nhiều ứng dụng mới ra đời: làm việc từ xa, làm việc nhóm, văn phòng ảo ...

Các thành phần của mạng máy tính

Trình bày: Ngô Bá Hùng
Khoa Công Nghệ Thông Tin
Đại Học Cần Thơ

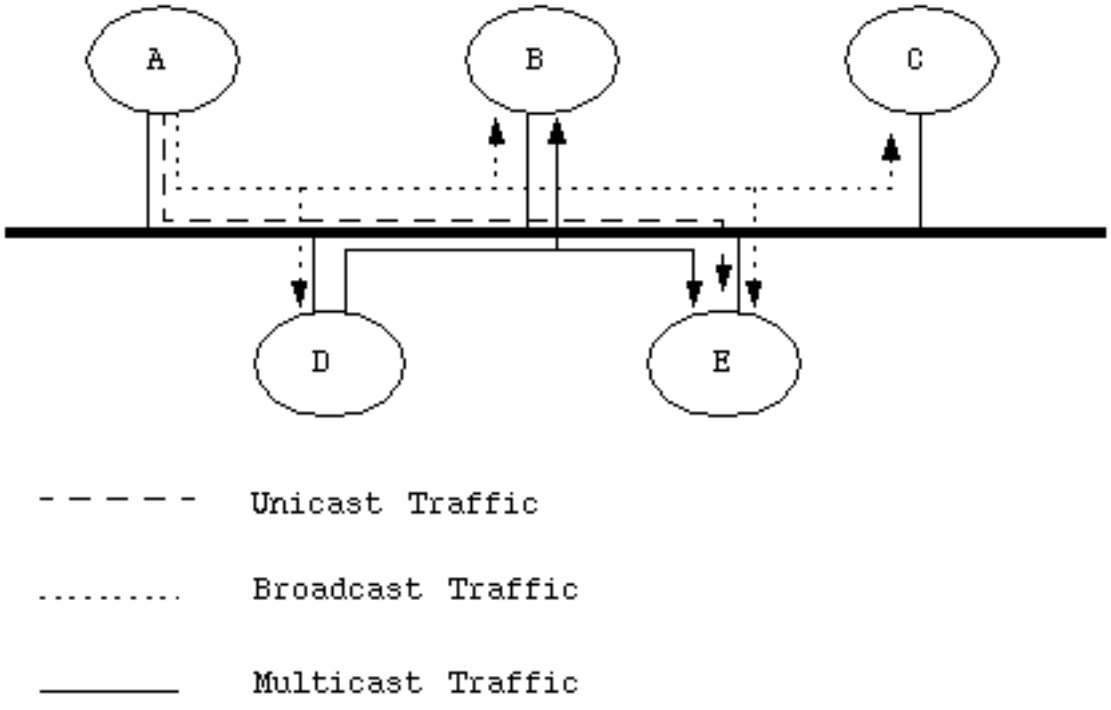
Các thành phần của mạng máy tính

- Phân loại mạng máy tính
- Kiến trúc phần mềm mạng máy tính
- Kiến trúc thứ bậc của mạng máy tính
- Mô hình tham khảo OSI

Phân loại mạng

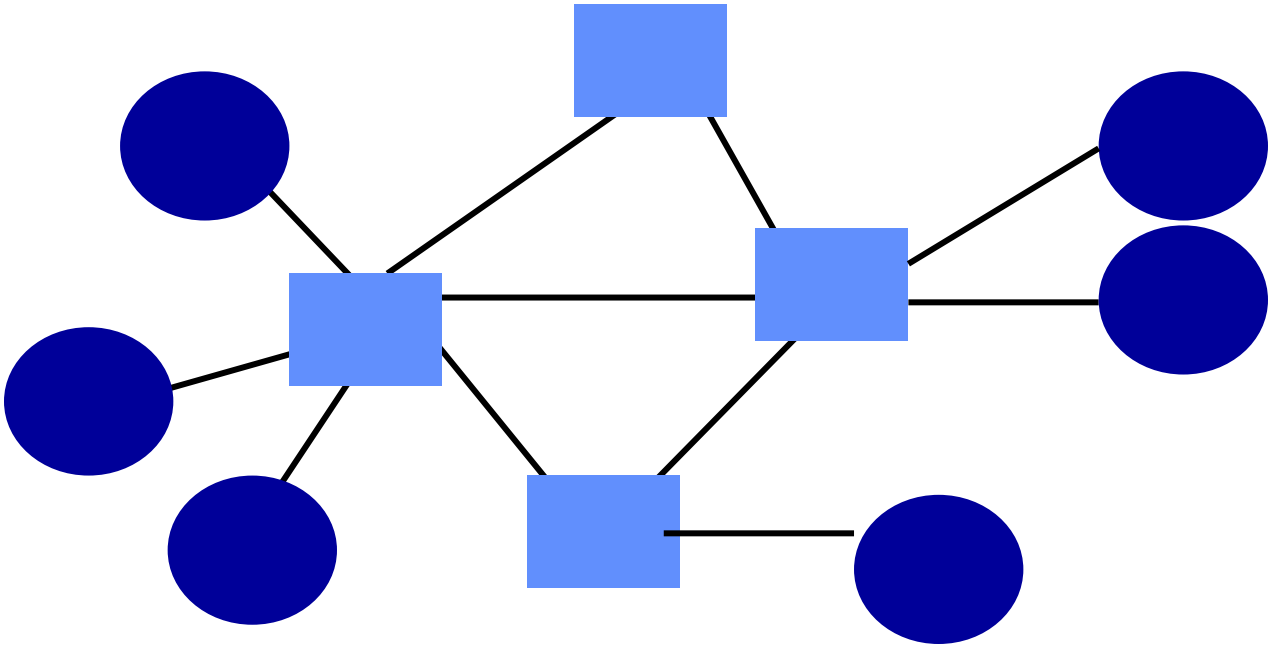
Phân loại mạng máy tính
Theo kỹ thuật truyền tin

- Mạng quảng bá (Broadcast)



Phân loại mạng máy tính
Theo thuật truyền tin

- Mạng chuyển mạch (Switched Network)

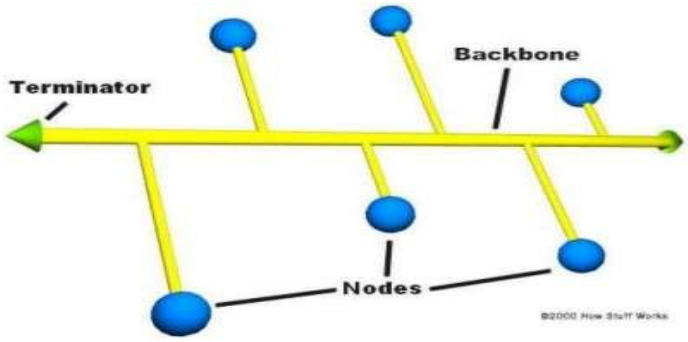


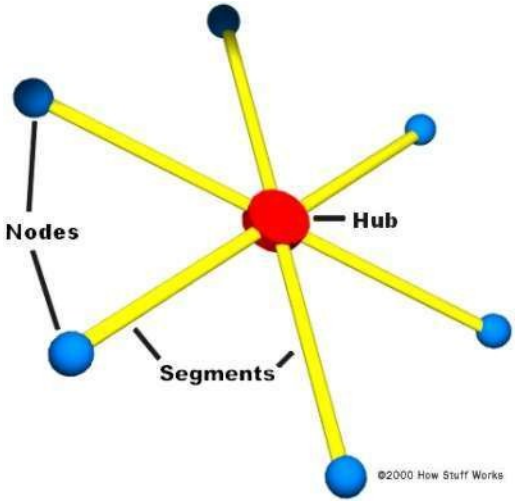
Phân loại mạng máy tính
Theo khoảng cách địa lý

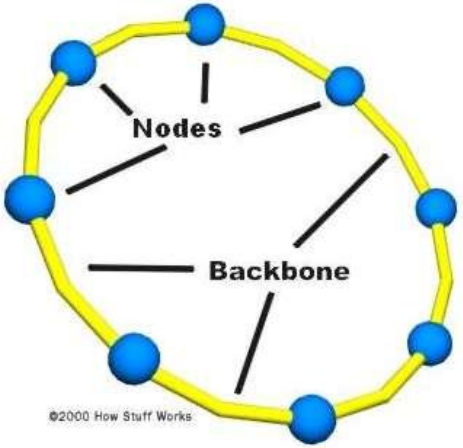
Đường kính mạng	Vị trí của các máy tính	Loại mạng
1 m	Trong một mét vuông	Mạng khu vực cá nhân
10 m	Trong 1 phòng	Mạng cục bộ, gọi tắt là mạng LAN (Local Area Network)
100 m	Trong 1 tòa nhà	
1 km	Trong một khu vực	
10 km	Trong một thành phố	Mạng thành phố, gọi tắt là mạng MAN (Metropolitan Area Network)
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	

Mạng cục bộ (LAN-Local Area Network)

- Mạng quảng bá
- Đường truyền băng thông rộng
- Topology: Bus, Star, Ring

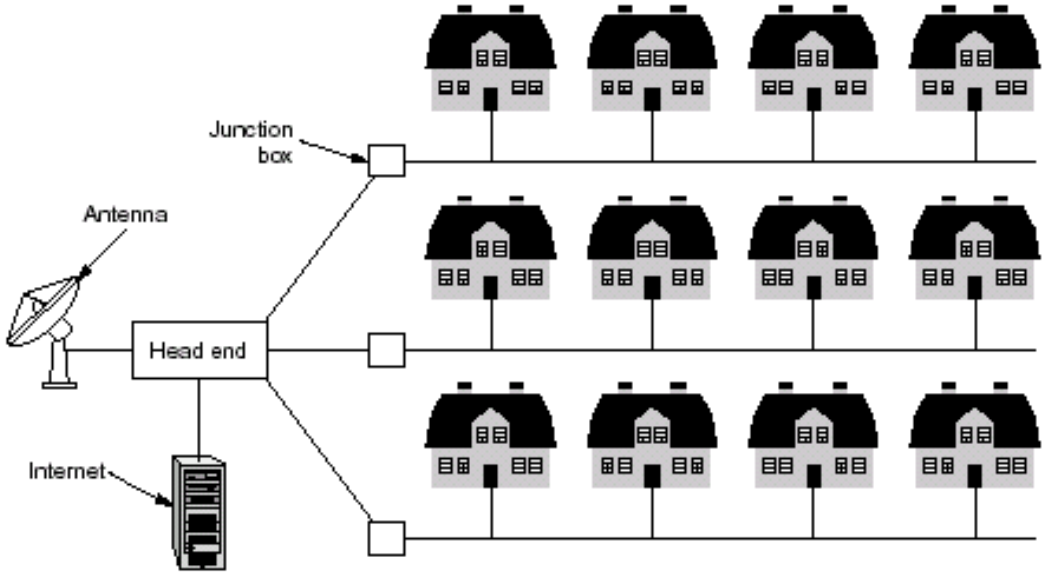






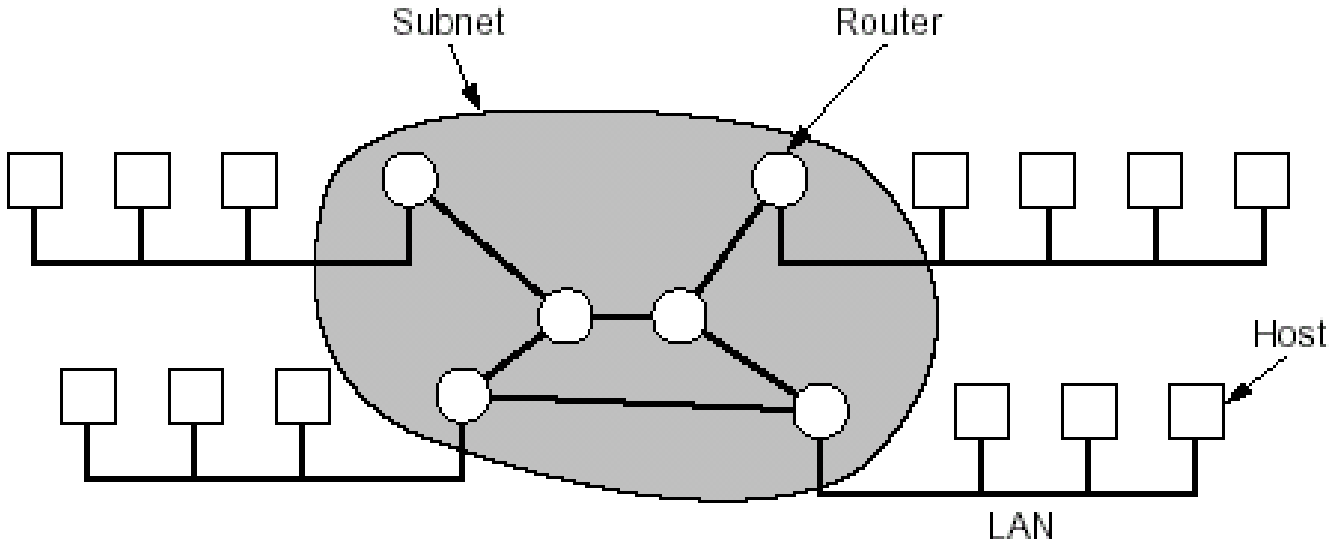
Mạng đô thị (MAN-Metropolitan Area Network)

- Phạm vi thành phố: Mạng truyền hình cáp



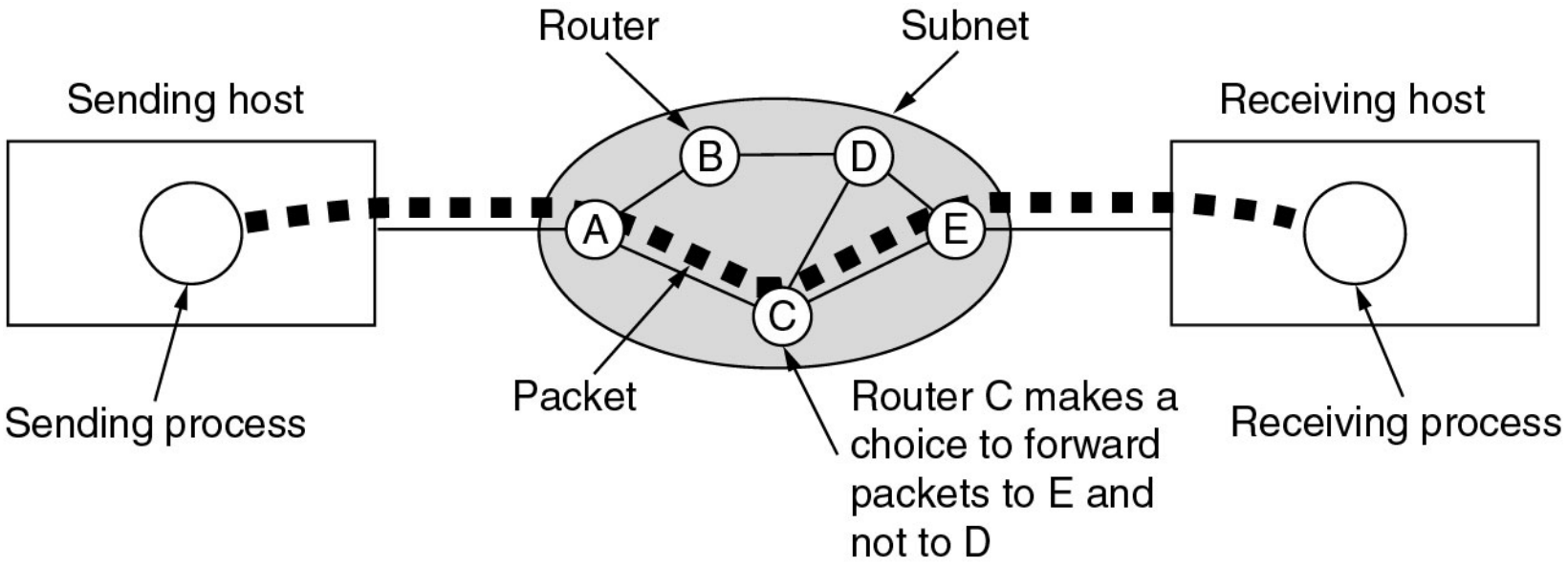
Mạng diện rộng (WAN – Wide Area Network)

- Mở rộng khoảng cách mạng
- Tăng số lượng máy tính trong mạng



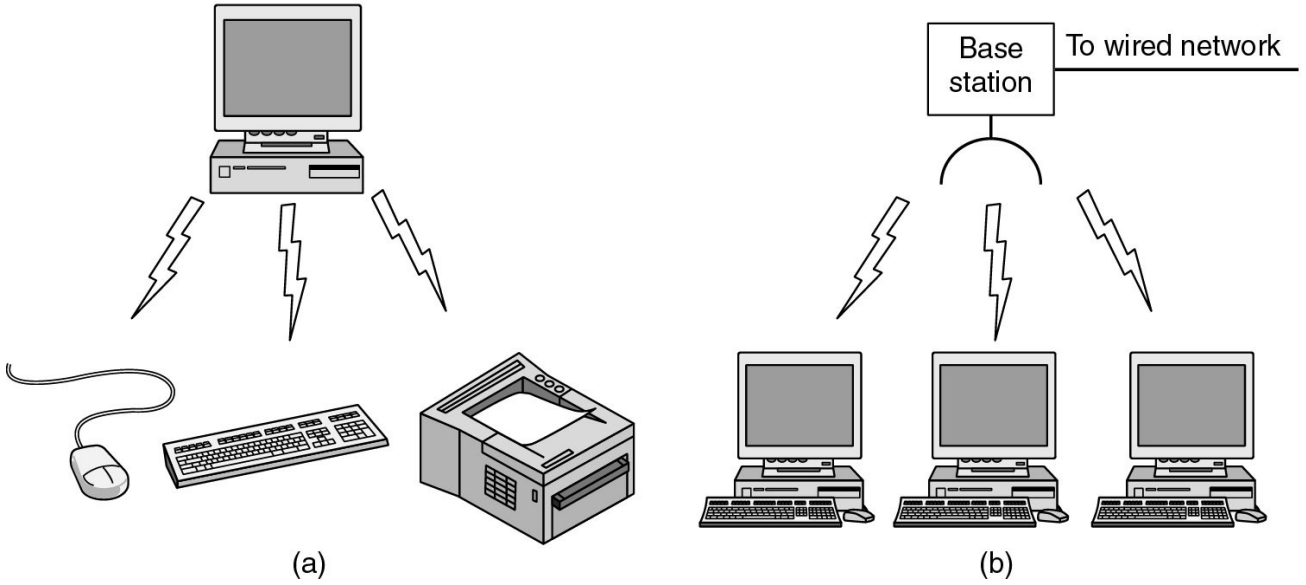
Mạng diện rộng (WAN – Wide Area Network)

- Sử dụng kỹ thuật Lưu và chuyển tiếp (Store and Forward)



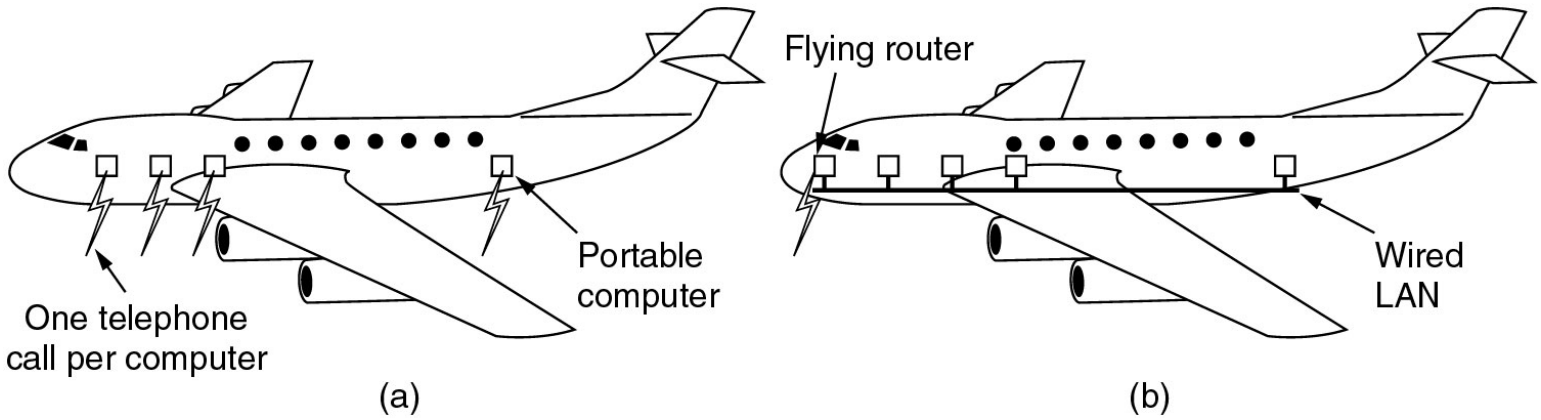
Phân loại mạng
Mạng không dây (wireless Network)

- (a) Thiết bị không dây
- (b) Wireless LAN



Phân loại mạng
Mạng không dây (wireless Network)

- Wireless WAN



Phân loại mạng
Liên mạng (Internetwork)

- Mạng hình thành từ việc nối kết nhiều mạng không đồng nhất về phần cứng và phần mềm lại với nhau
  - LAN = LAN + LAN
  - WAN = LAN + LAN
  - WAN = WAN + WAN

Kiến trúc phần mềm mạng

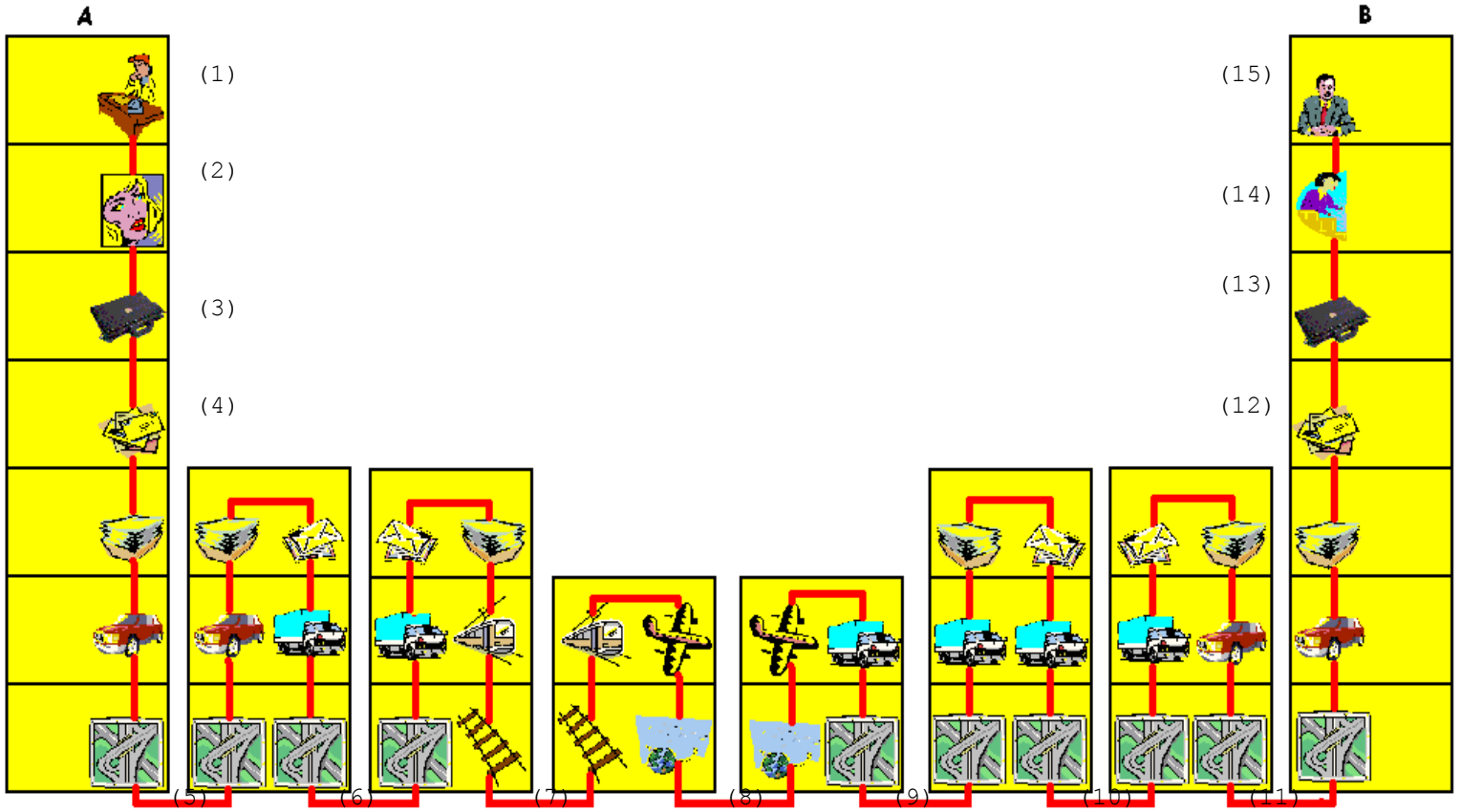
Các thành phần phần mềm mạng

- 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

Kiến trúc thứ bậc của giao thức

- Các dịch vụ mạng được nhóm vào những tầng khác nhau
- Tầng trên sử dụng dịch vụ của tầng dưới
- Hai tầng ngang cấp giao tiếp nhau theo một giao thức đã định nghĩa trước
- Giao thức qui định qui tắc trao đổi thông tin: Khuôn dạng dữ liệu, nghi thức bắt tay, phương thức phát hiện và xử lý lỗi, …

Hệ thống thư tín quốc tế



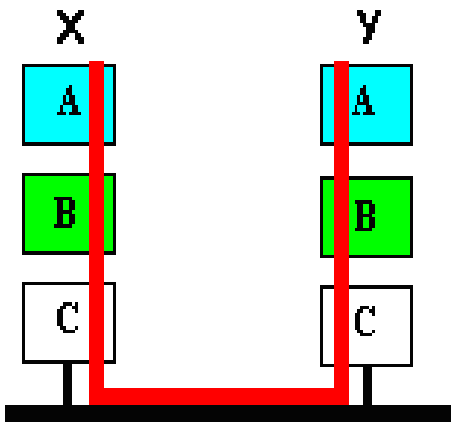
H2.10 Mô hình gởi nhận thư tín thế giới

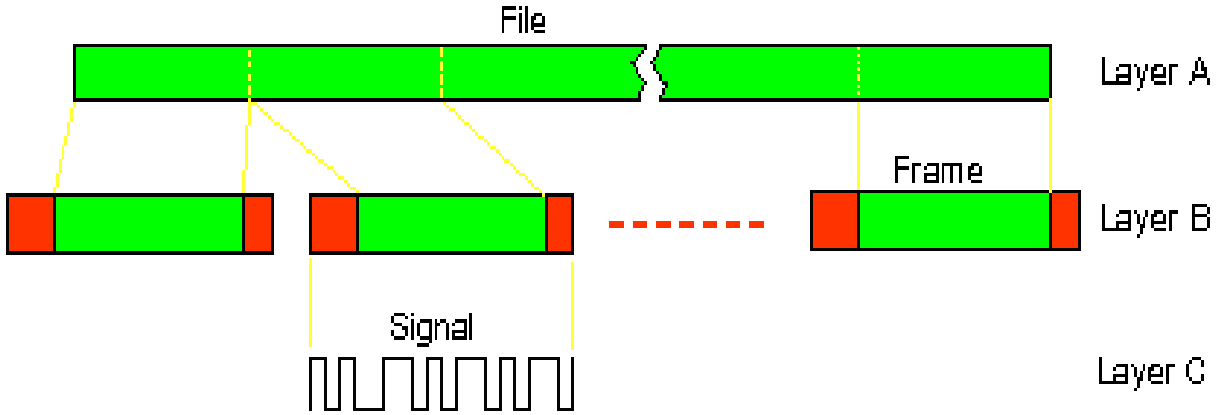
Mô hình truyền tải tập tin 3 tầng

A : Tầng ứng dụng

B : Tầng quản lý thông điệp

C : Tầng vật lý





Dịch vụ mạng

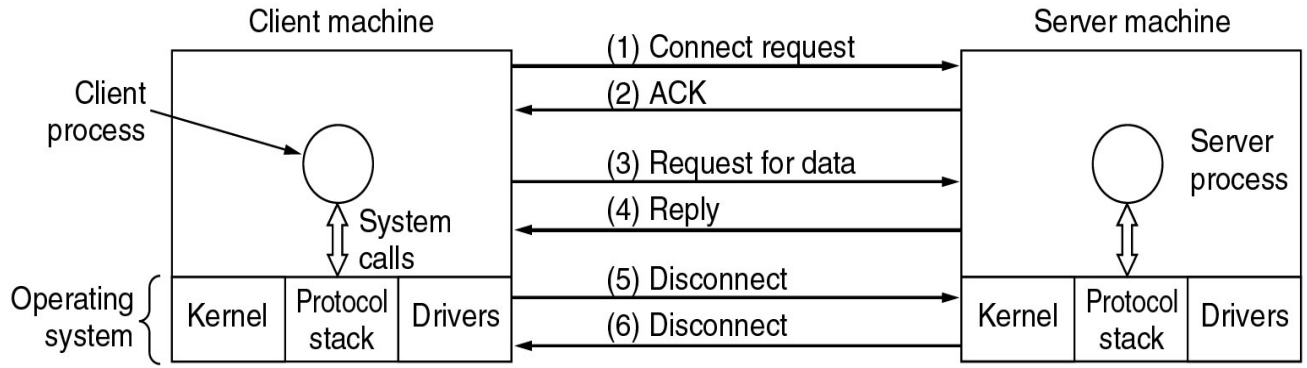
- Dịch vụ định hướng nối kết (Connection-oriented):
  - Mô hình của hệ thống điện thoại
  - Có thiết lập và xóa nối kết
- Dịch vụ không nối kết (Connectionless):
  - Mô hình kiểu thư tín.
  - Dữ liệu truyền đi trong những gói (Packet)
  - Gói tin có thông tin về địa chỉ người gởi và địa chỉ người nhận.

Các phép toán của dịch vụ

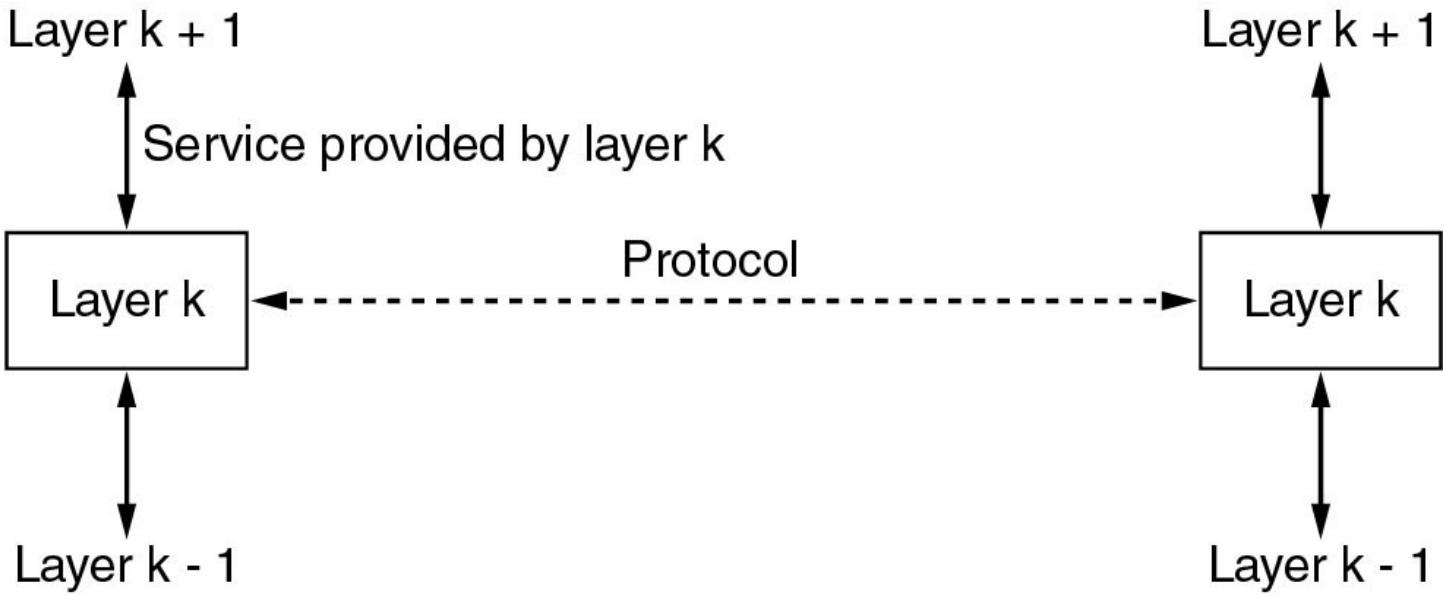
Hàm cơ bản	**Chức năng**
LISTEN	Nghẽn để chờ một yêu cầu nối kết gởi đến
CONNECT	Yêu cầu thiết lập nối kết với bên muốn giao tiếp
RECEIVE	Nghẽn để chờ nhận các thông điệp gởi đến
SEND	Gởi thông điệp sang bên kia
DISCONNECT	Kết thúc một nối kết

Dịch vụ định hướng nối kết

Server	Client
LISTEN	
	CONNECT
RECEIVE	SEND
SEND	RECIEVE
DISCONNECT	DISCONNECT



Dịch vụ & Giao thức



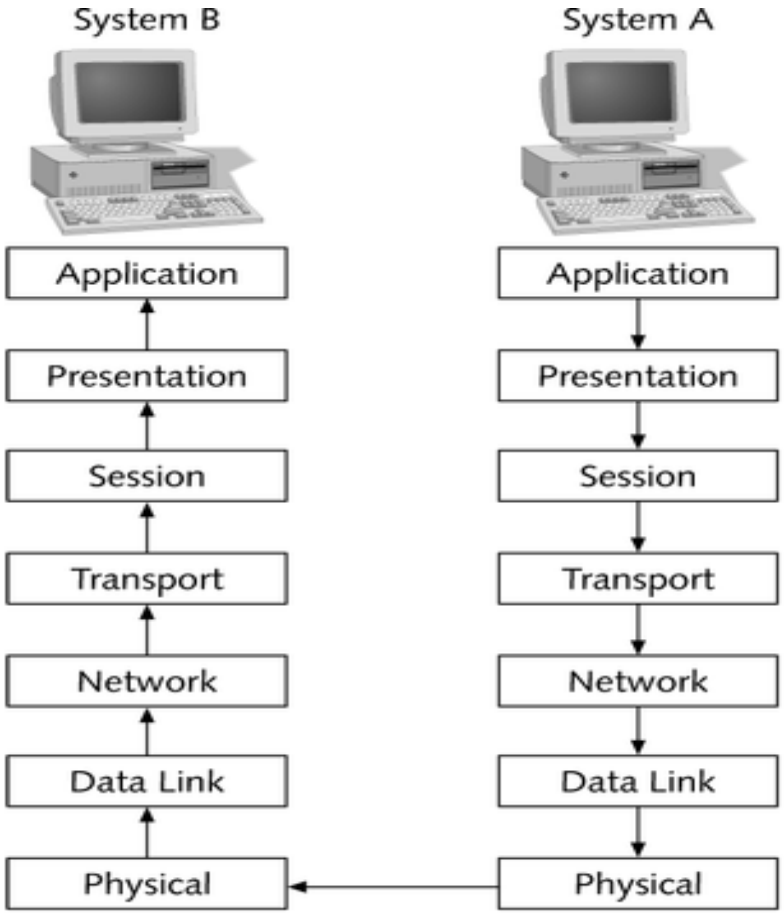
MÔ HÌNH THAM KHẢO OSI

Trình bày: Ngô Bá Hùng
Khoa Công Nghệ Thông Tin
Đại Học Cần Thơ

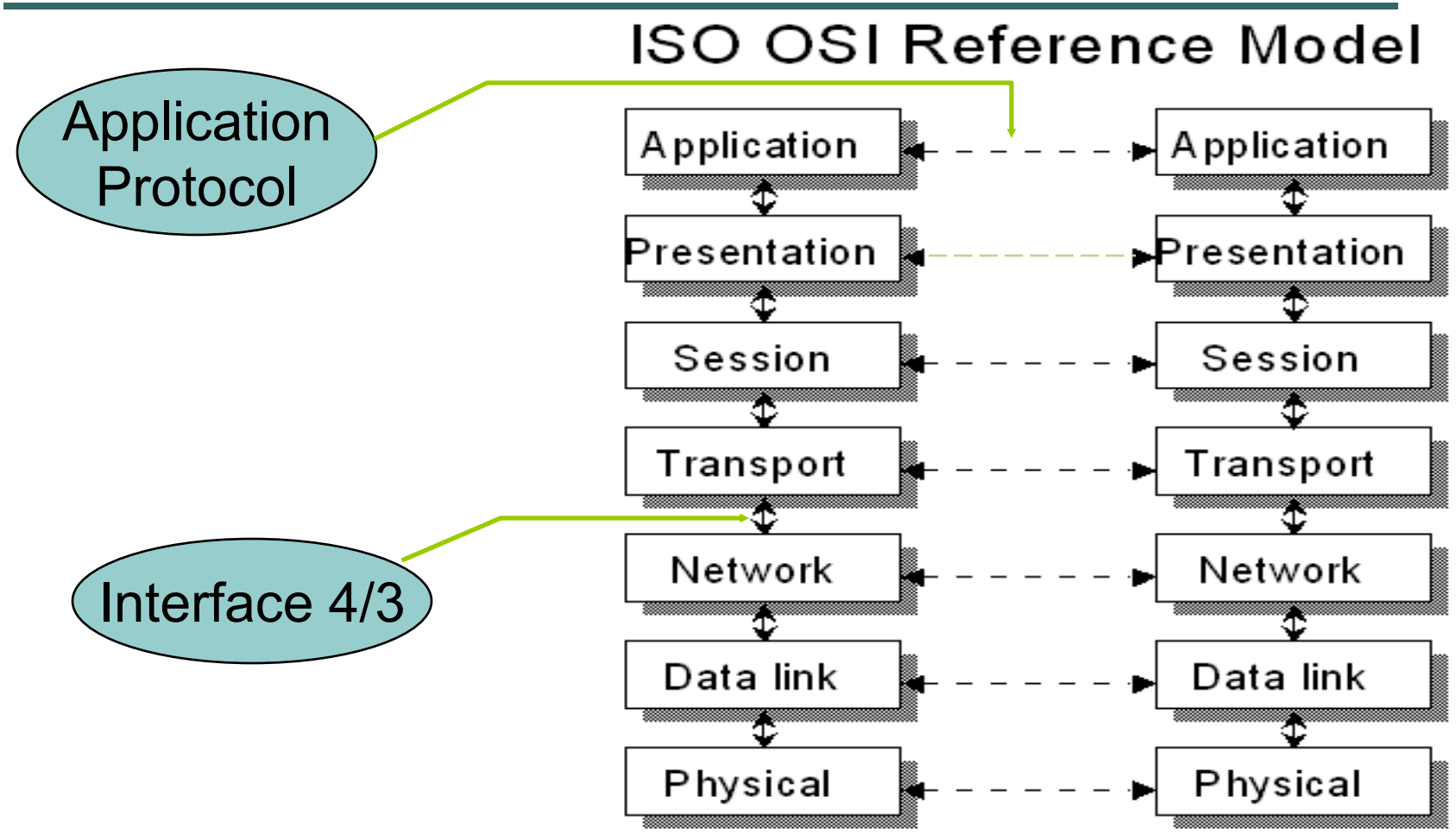
Mô hình tham khảo OSI (Open System Interconnection Model)

- Đợc phát triển bởi tổ chức tiêu chuẩn thế giới ISO (International Standard Organization)
- Gồm có 7 tầng:
  - Tầng vật lý (Physical layer)
  - Tầng liên kết dữ liệu (Data link layer)
  - Tầng mạng (Network layer)
  - Tầng vận chuyển (Transport layer)
  - Tầng giao dịch (Session layer)
  - Tầng trình bày (Presentation)
  - Tầng ứng dụng (Application layer)

Mô hình tham khảo OSI



Mô hình tham khảo OSI



Mô hình tham khảo OSI

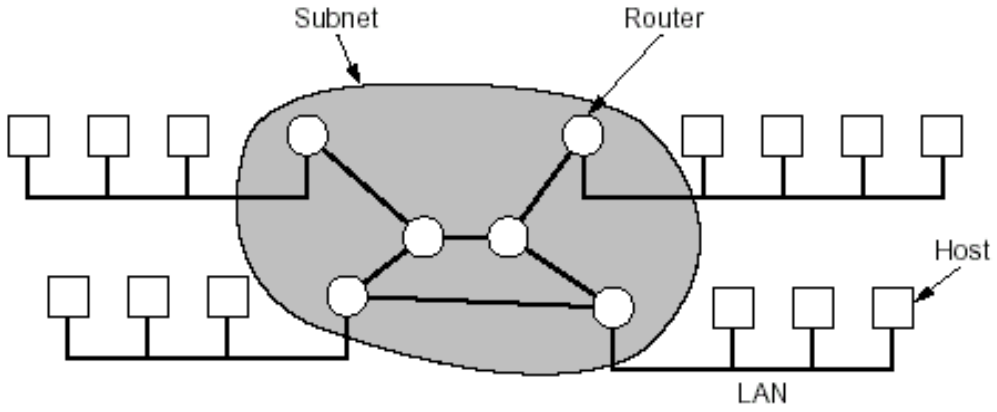
- Tầng vật lý (Physical layer)
  - Truyền tải các bit thô (raw bit) trên một kênh truyền vật lý
  - Định các chuẩn thiết kế:
    - ✓ Cách nối kết các máy
    - ✓ Mức điện thế, . ..
    - ✓ Cấu trúc các đầu nối,...
    - ✓ Phơng pháp truyền tải

Mô hình tham khảo OSI

- Tầng liên kết dữ liệu (Data link layer)
  - Đơn vị truyền nhận dữ liệu là khung (Frame)
  - Thiết lập cơ chế phát hiện và xử lý lỗi
  - Điều khiển dòng (Flow control)
  - Giải quyết tranh chấp đờng truyền
  - Kênh truyền nối ***trực tiếp*** hai máy tính
  - 01001 => 01001
  - 01001 => 01011

Mô hình tham khảo OSI

- Tầng mạng (Network layer)
  - Đơn vị truyền nhận dữ liệu là Gói tin (Packet)
  - Vạch đờng (Routing) và chuyển tiếp (Forwarding) các gói tin
  - Kiểm tra, khắc phục tình trạng tắt nghẽn đờng truyền
  - Cung cấp cơ chế tính tiền thông tin vận



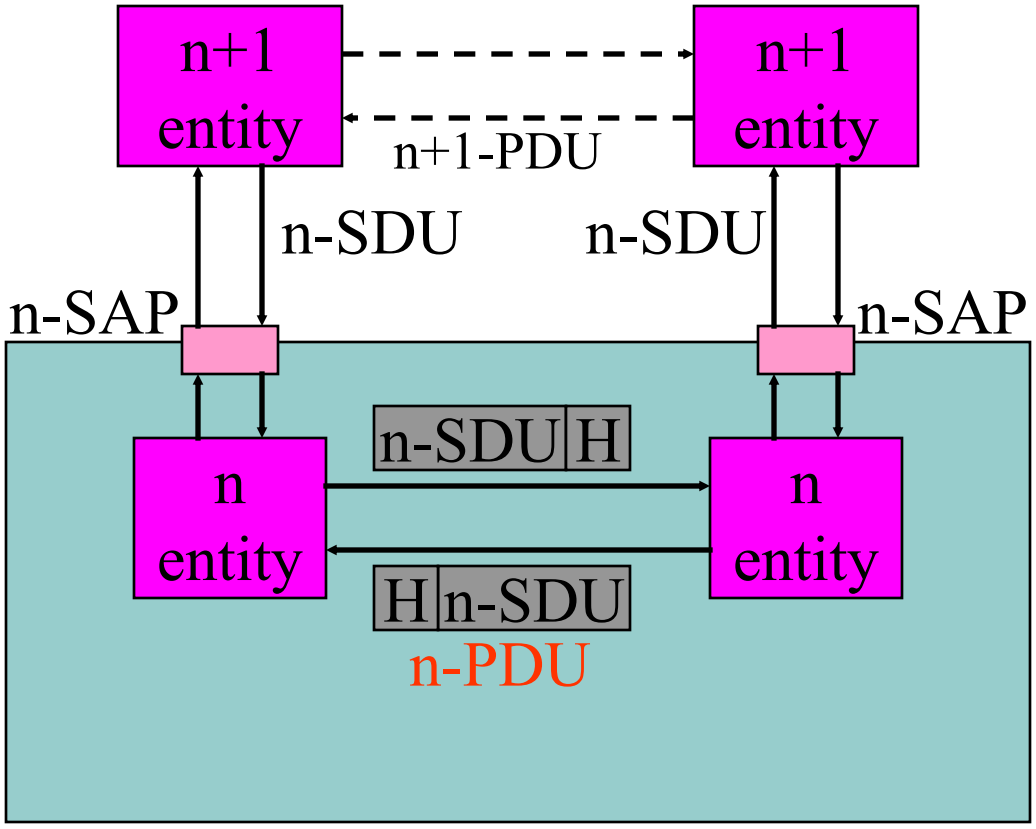
Mô hình tham khảo OSI

- Tầng vận chuyển (Transport layer)
  - Truyền dữ liệu điểm nối điểm (end-to-end)
  - Kiểm tra các gói tin truyền nhận: mất, trùng lắp
  - Đa hợp / Phân Hợp
- Tầng giao dịch (Session layer)
  - Quản lý các giao dịch
  - Đồng bộ hóa dữ liệu truyền, nhận

Mô hình tham khảo OSI

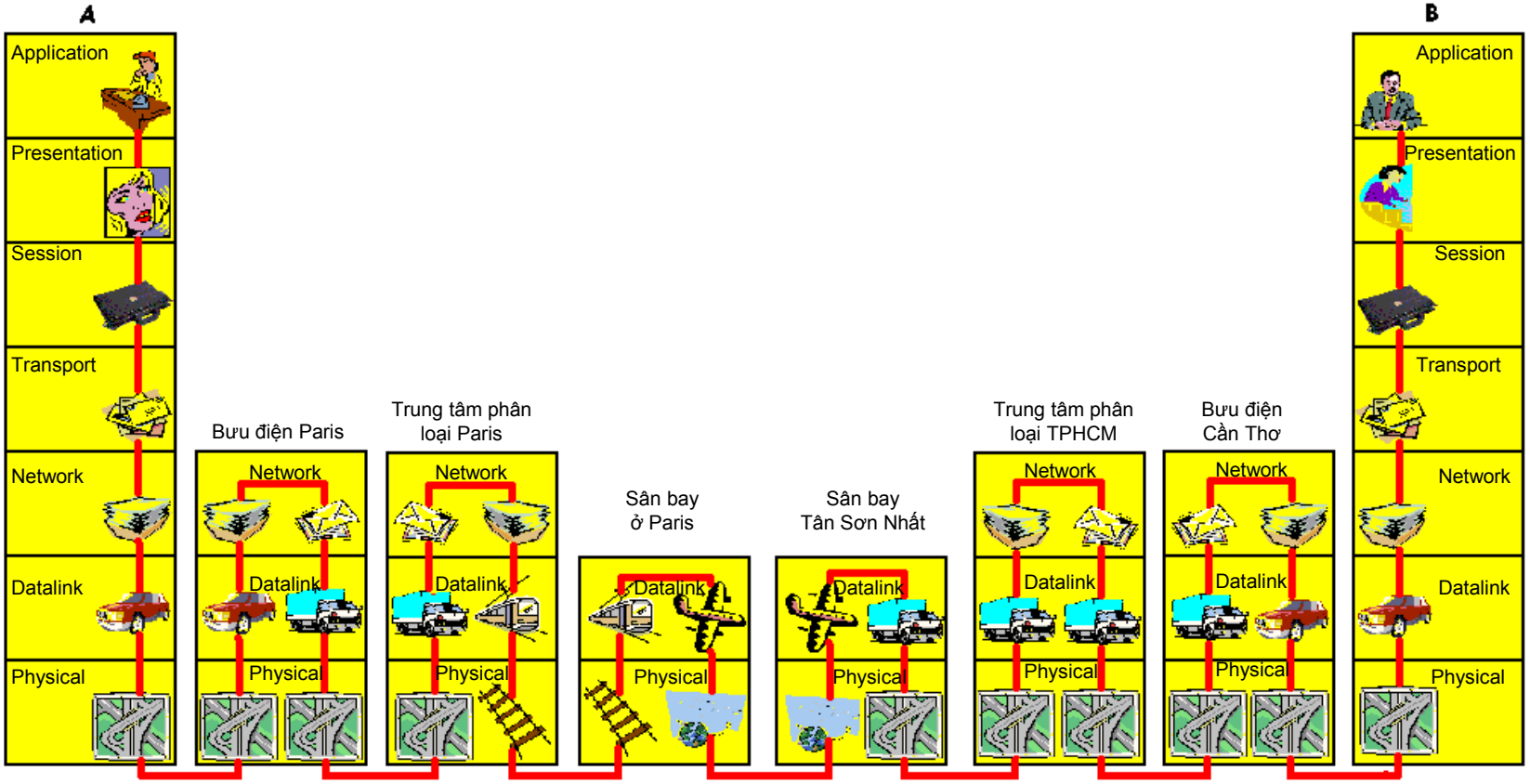
- Tầng trình bày (Presentation layer)
  - Chuẩn hóa dữ liệu trao đổi giữa các hệ thống khác nhau: Little India với Big India, . .
  - Nén, mã hóa thông tin
- Tâng ứng dụng (Application layer)
  - Các phần mềm, dịch vụ: Email, Web, FTP, . . .
  - Cho phép ngời phát triển định nghĩa các protocol của ứng dụng: HTTP, SMTP, POP,IMAP...

Mô hình tham khảo OSI



- n Entity (thực thể) một quá trình ở lớp n
- SAP = Service Access Point
- SDU = Service Data Unit
- PDU = Protocol Data Unit
- H=Header

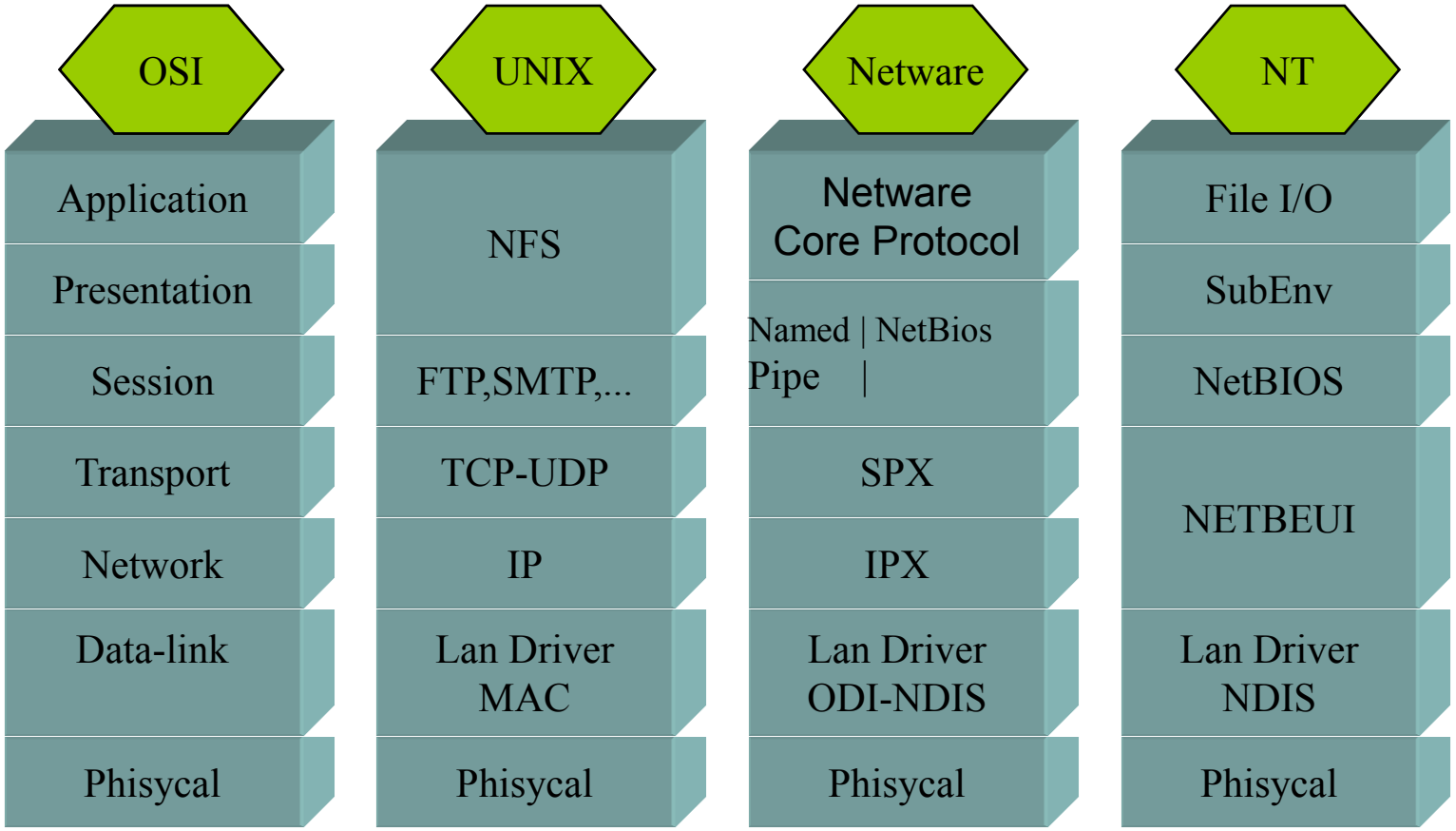
Ví dụ về phân tầng



Ví dụ về phân tầng

- Tầng ứng dụng: viết/đọc lá thư.
- Tầng trình bày: phiên dịch, bỏ thư gởi vào phong bì, mở phong bì các thư nhận được
- Tầng giao dịch: tập hợp/phân phát thư của các văn phòng.
- Tầng vận chuyển: vai trò của bộ phận văn thư.
- Tầng mạng: vai trò của bưu điện hay của trung tâm phân loại thư.
- Tầng vận chuyển: Chuyển thư giữa hai nút kế cận nhau.
- Tầng vật lý: Các phương tiện giao thông (đường bộ, đường sắt, đường ô tô).

Hệ điều hành mạng



Tầng vật lý
(Physical Layer)

Trình bày: Ngô Bá Hùng
Khoa Công Nghệ Thông Tin
Đại Học Cần Thơ

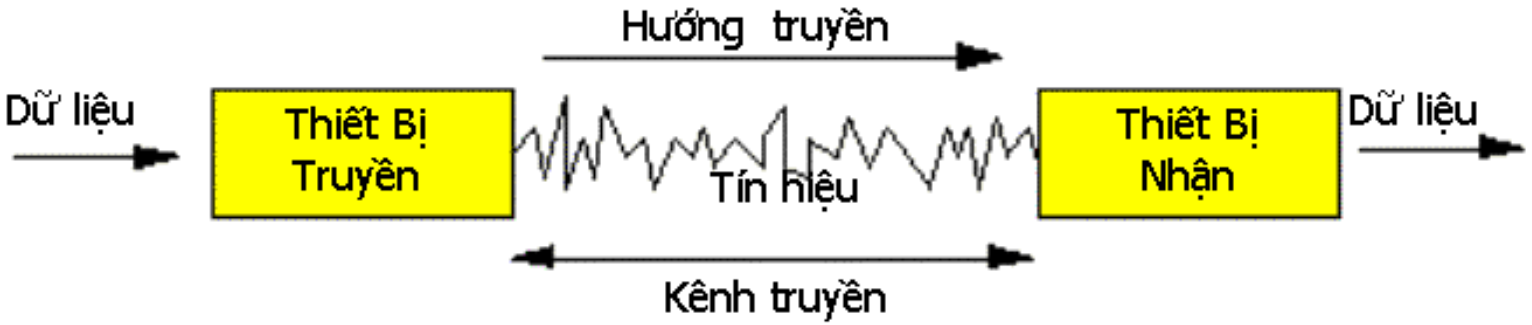
Mục đích

- 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.

Mô hình truyền dữ liệu cơ bản



- Các vấn đề phải quan tâm:
  - 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 bits từ thiết bị truyền sang thiết bị nhận.

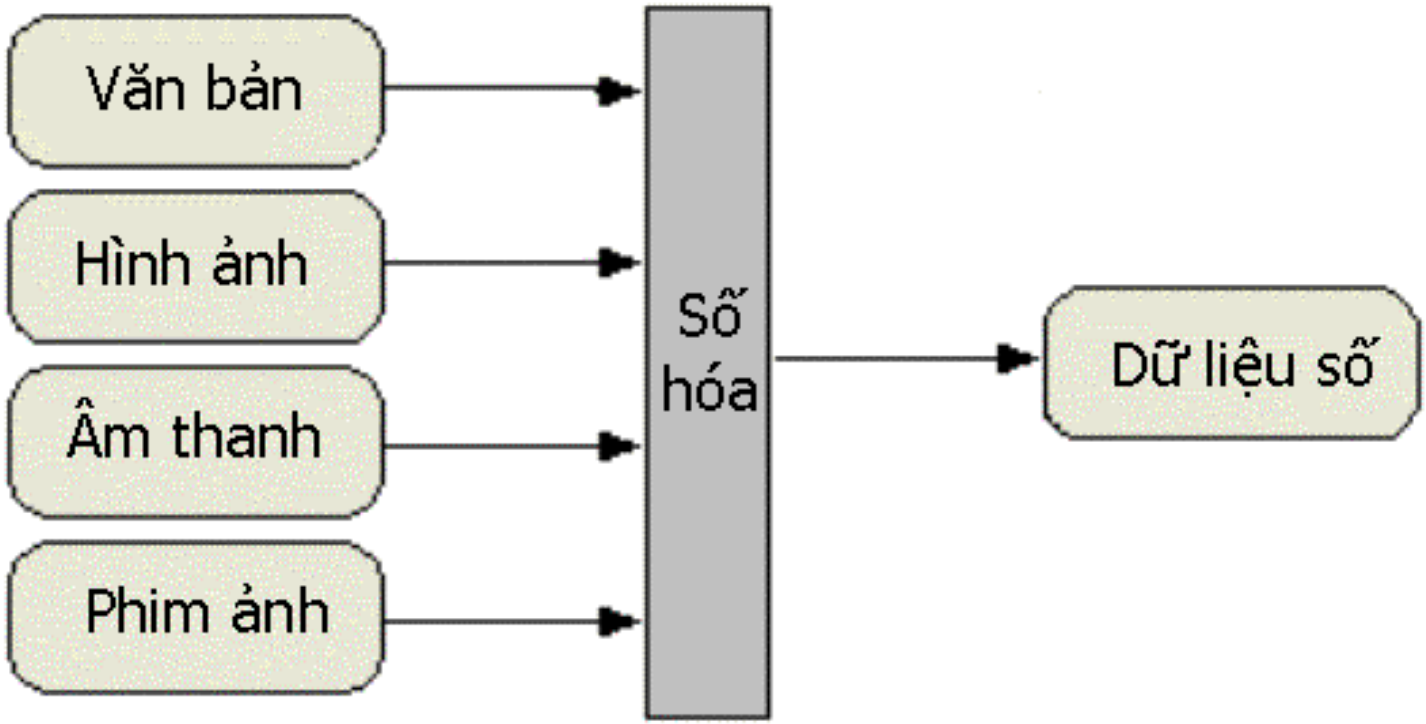
Số hóa dữ liệu

Trình bày: Nguyễn Phú Trường
Khoa Công Nghệ Thông Tin
Đại Học Cần Thơ

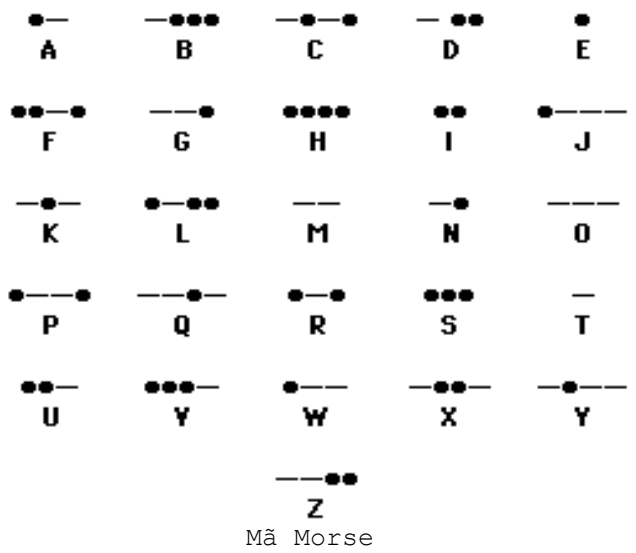
Vấn đề số hóa dữ liệu

Lời nói : Hệ thống : điện thoại Bộ mã hóa : micro Bộ giải mã : Loa Truyền tải : tín hiệu tuần tự hay 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.
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.	***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.

Mô hình số hóa dữ liệu



Số hóa văn bản



Mã Morse

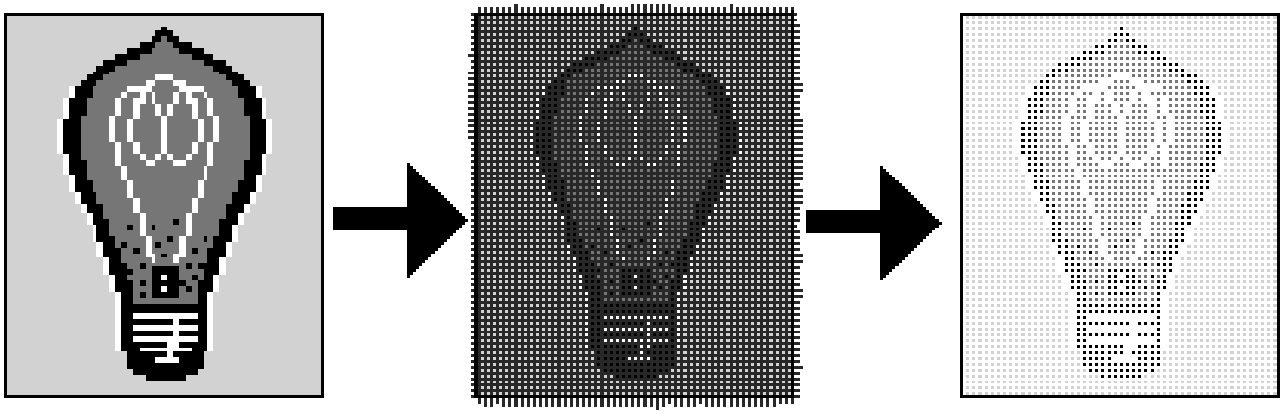
poids forts

poids faibles	000	001	010	011	100	101	110	111
0000	NUL	DLE	SP	0	@	P	\	p
0001	SOH	DC1	!	1	A	Q	a	q
0010	STX	DC2	"	2	B	R	b	r
0011	ETX	DC3	#	3	C	S	c	s
0100	EOT	DC4	$	4	D	T	d	t
0101	ENQ	NAK	%	5	E	U	e	u
0110	ACK	SYN	&	6	F	V	f	v
0111	BEL	ETB	'	7	G	W	g	w
1000	BS	CAN	(	8	H	X	h	x
1001	HT	EM	)	9	I	Y	i	y
1010	LF	SUB	*	:	J	Z	j	z
1011	VT	ESC	+	;	K	[	k	{
1100	FF	FS	,	<	L	Ç	l	ù
1101	CR	GS	-	=	M	]	m	}
1110	SO	RS	.	>	N	↑	n	≈
1111	SI	US	/	?	O	<--	o	DEL

code ASCII

- Bảng mã 8 bits:
  - Mã ASCII (American Standard Code for Informatics Interchange) mở rộng
  - Mã EBCDIC (Extended Binary-Coded Decimal Interchange Code)
- Mã 16 bits : Mã Unicode

Số hóa hình ảnh tĩnh

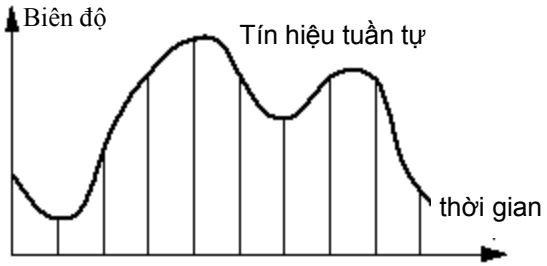


Ảnh gốc | Ảnh 1 độ phân giải | Ảnh đã số hóa

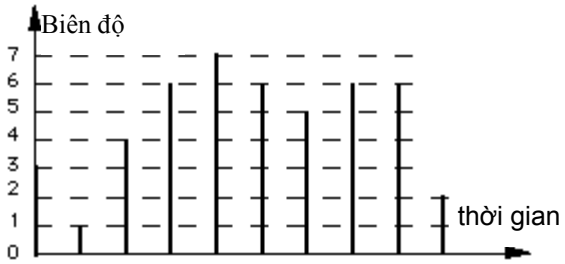
- Ảnh đen trắng : 0: đen, 1: trắng
- Ảnh 256 mức xám: 8 bits / điểm ảnh
- Ảnh màu: 1 điểm ảnh = aR + bG +cB

Số hóa âm thanh & phim ảnh

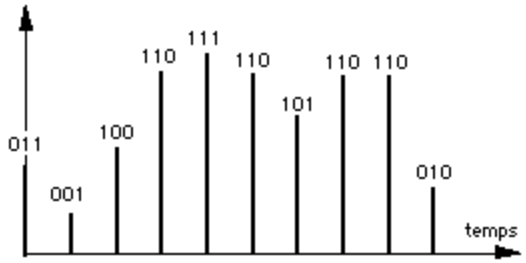
1.Lấy mẫu



2.Lượng hóa



3.Số 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).

Số hóa văn bản

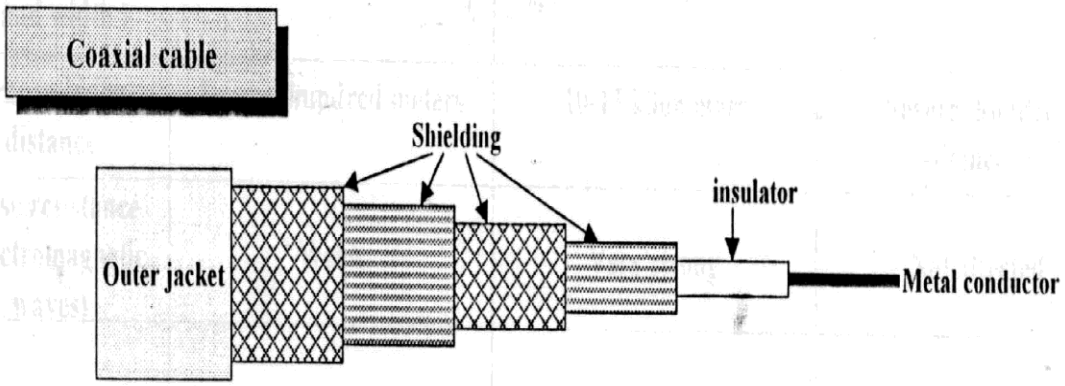
- Bảng mã 8 bits:
  - Mã ASCII (American Standard Code for Informatics Interchange) mở rộng
  - Mã EBCDIC
- Mã 16 bits : Mã Unicode

Kênh truyền

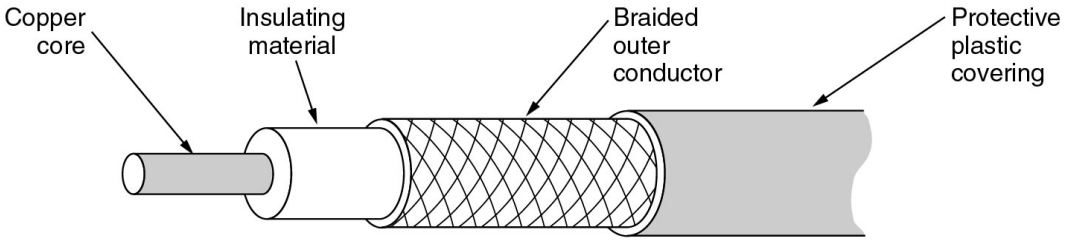
Kênh truyền hữu tuyến

- Sử dụng 3 loại cáp phổ biến:
  - Cáp xoắn đôi (twisted pair)
  - Cáp đồng trục (coax)
  - Cáp quang (fiber optic).
- Các yếu tố chọn lựa:
  - Giá thành
  - Khoảng cách
  - Số lượng máy tính
  - Tốc độ yêu cầu
  - Băng thông

Cáp đồng trục (Coaxial Cable)

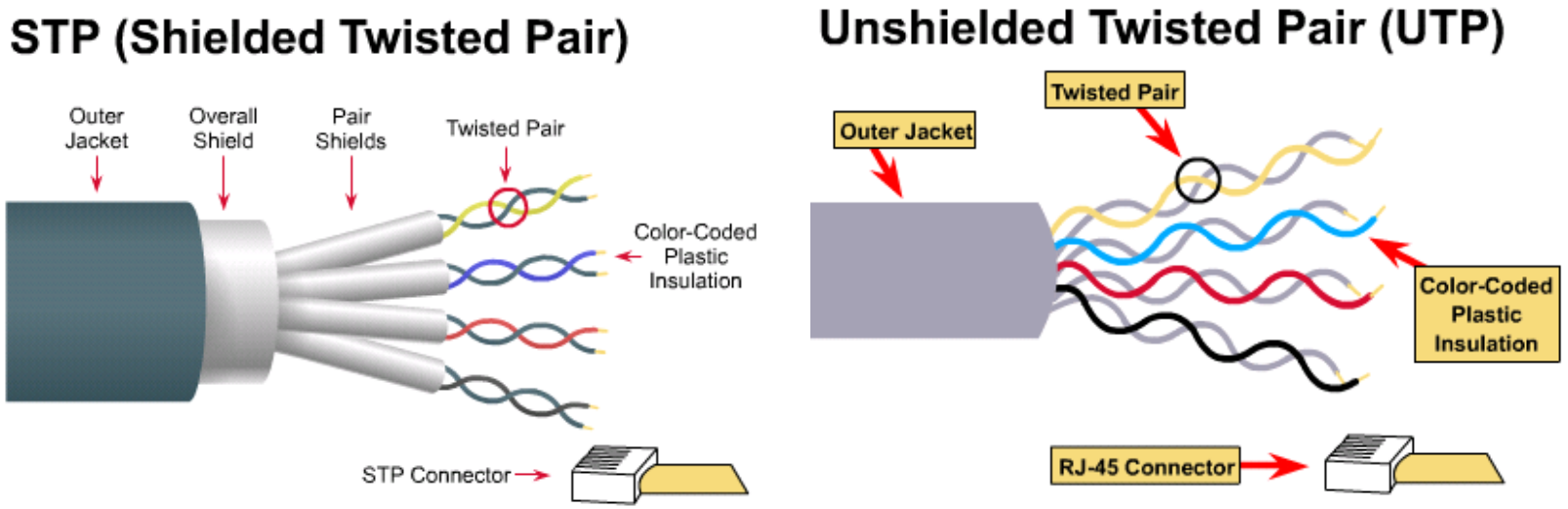


Thick coaxial cable (RG11)



Thin coaxial cable (RG58)

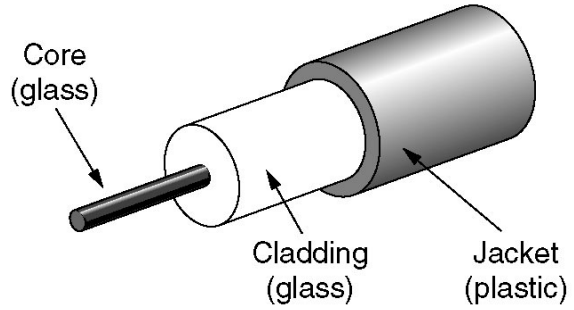
Cáp xoắn đôi (Twisted – paire cable)



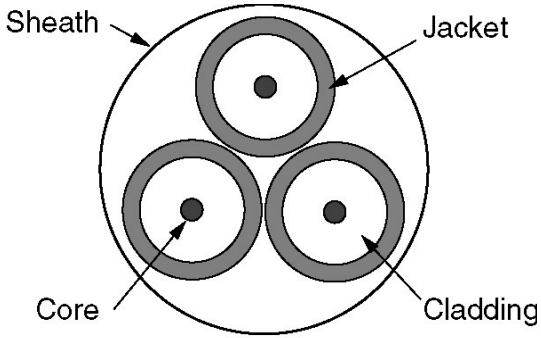
Cáp xoắn đôi (Twisted – paire cable)

- CAT 1, 2: 1Mbps (Telephone)
- CAT 3: 10Mbps (10BaseT)
- CAT 5: 100MBps (100BaseT)
- CAT 5E,6: 1000MBps (1000 BaseT)

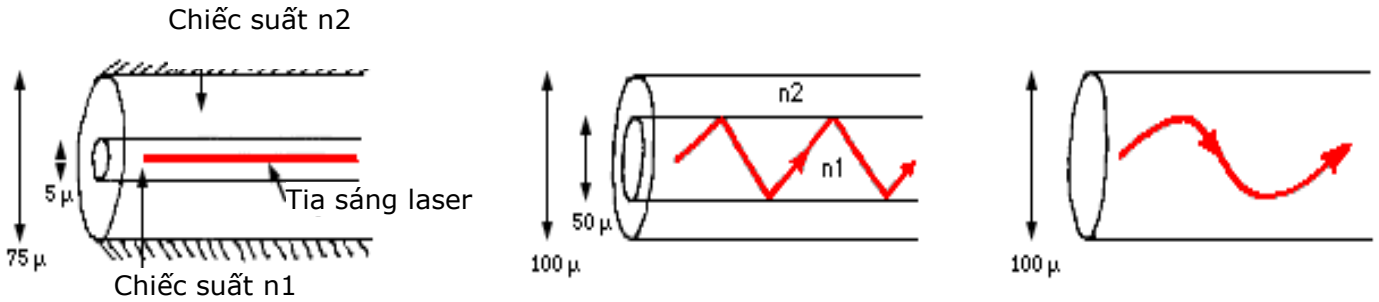
Cáp quang (Fiber optic cable)



(a)



(b)

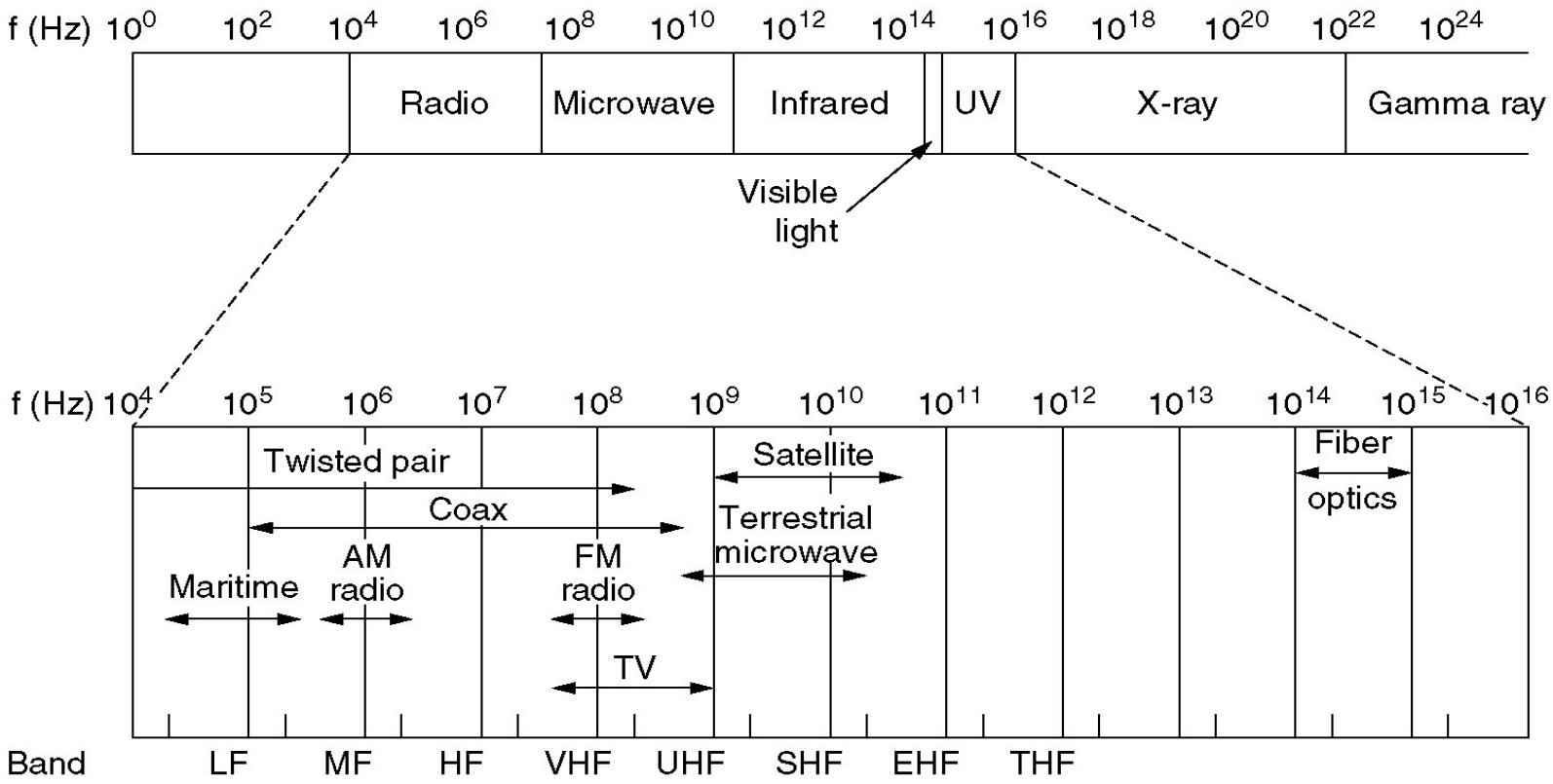


1. Cáp quang chế độ đơn – 2. chế độ đa không thẩm thấu – 3. chế độ đa thẩm thấu

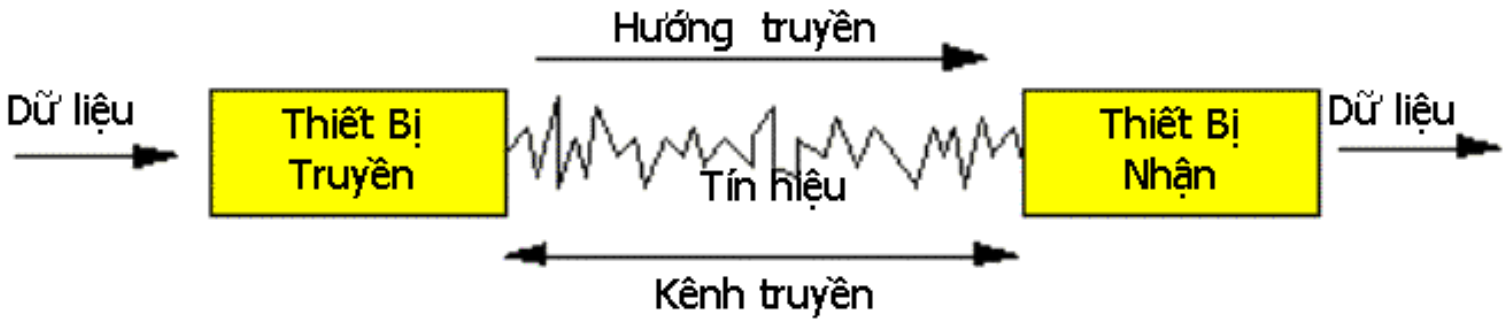
Kênh truyền vô tuyến

- c là tốc độ ánh sáng,
- f là tần số của tín hiệu sóng
- λ là độ dài sóng. Khi đó ta có
- $c = \lambda f$

Kênh truyền vô tuyến

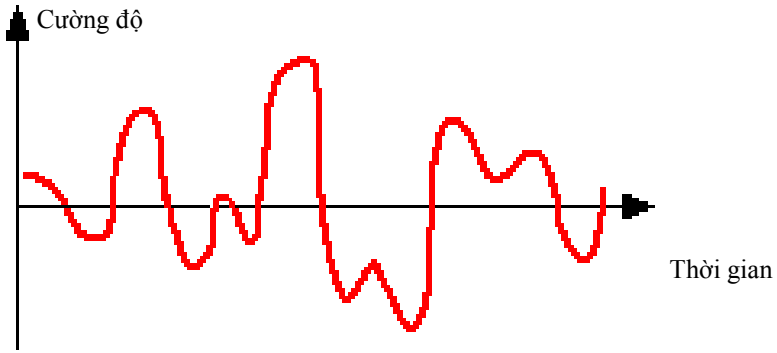


Tín hiệu tuần tự & Tín hiệu số

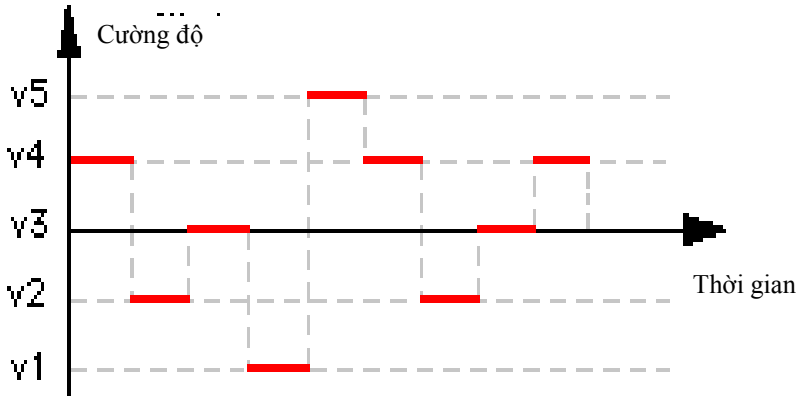


- Dữ liệu (các bits 0, 1) được truyền từ thiết bị truyền sang thiết bị nhận bằng các tín hiệu tuần tự hay tín hiệu số

Tín hiệu tuần tự & Tín hiệu số



Tín hiệu tuần tự



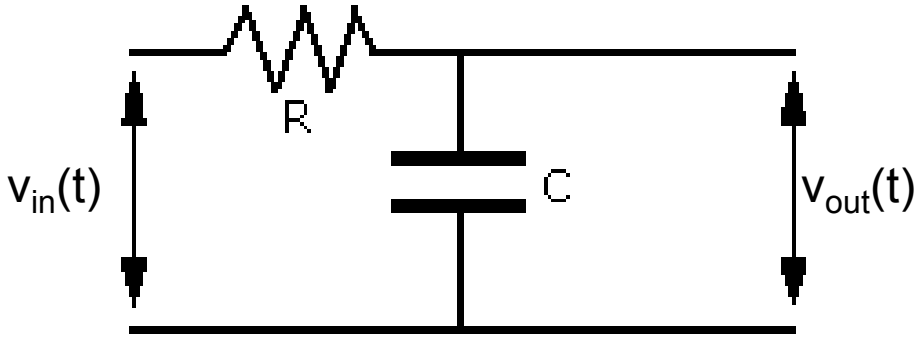
Tín hiệu số

Tín hiệu dạng sóng 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.
- **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.

Đặc điểm kênh truyền

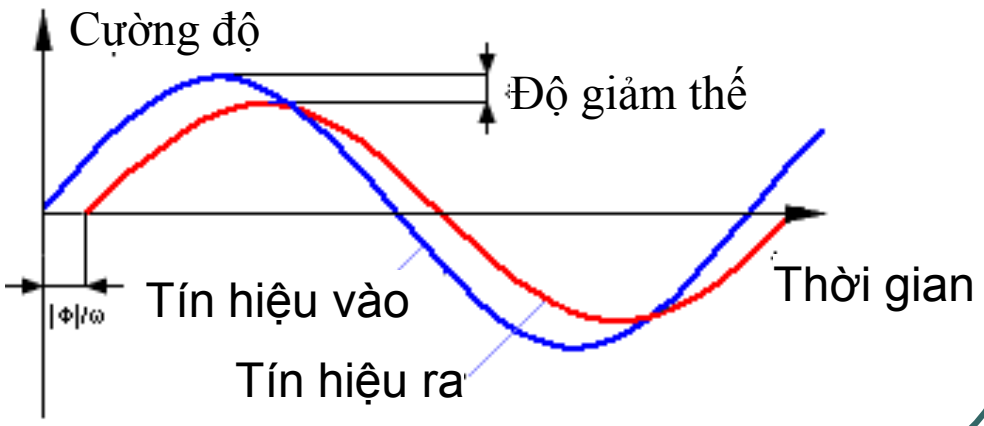
- Mô hình hóa một kênh truyền



- $v_{in}(t) = \mathbf{V}_{in} \sin wt$
  - $\mathbf{V}_{in}$: là hiệu điện thế cực đại ngỏ vào
  - w : nhịp ; f = w/2pi : là **tần số**;
  - T = 2pi/w = 1/f : là **chu kỳ**.
- $v_{out}(t) = V_{out} \sin (wt + F)$
  - $\mathbf{V}_{out}$: là hiệu điện thế cực đại ngỏ ra
  - F : là độ trễ pha.

Đặc điểm kênh truyền

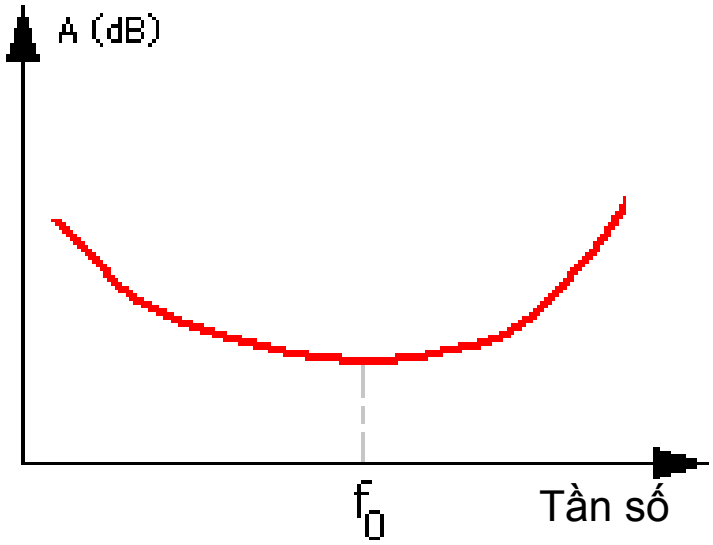
- Các luật trường điện tử chứng minh rằng trong trường hợp đơn giản nhất ta có:
  - $V_{out}/V_{in} = (1 + R^2C^2w^2)^{-1/2}$
  - $F = \text{atan}(-RC\ w)$



Đặc điểm kênh truyền

- Độ suy giảm trên kênh truyền = P_{in}/P_{out}
- Biểu diễn bằng đơn vị decibel:
  - A(w) = 10 log10(Pin/Pout)

Độ suy giảm càng nhỏ khi tần số của sóng càng gần f_0

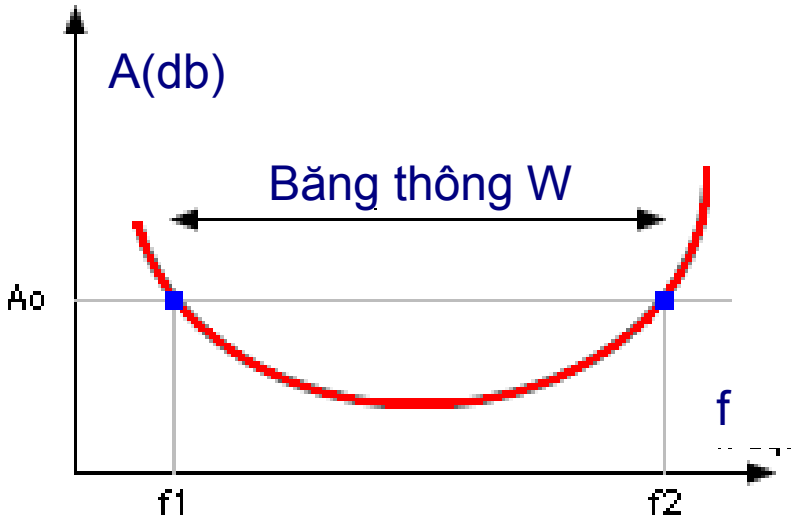


Truyền tín hiệu bất kỳ

- 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.

Băng thông kênh truyền (Bandwidth)

- A_0,: ngưỡng còn "nghe" được A_0,
  - Tất cả các tín hiệu hình sin có **tần số** nhỏ hơn f1 được xem như bị mất.
  - Tất cả 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. Khoảng **tần số** này được gọi là băng thông của một kênh truyền.

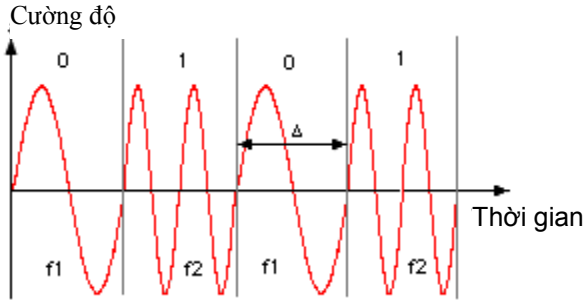


Ví dụ: Băng thông kênh truyền điện thoại là 3100 Hz vì các tín hiệu âm thanh có thể nghe được nằm ở khoảng **tần số** từ 300 Hz đến 3400 Hz

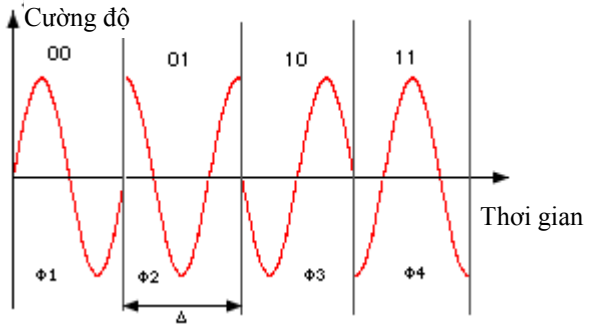
Tần số biến điệu và tốc độ dữ liệu (Baund rate and bit rate)

- Tần số biến điệu:
  - Nhịp đặt các tín hiệu lên kênh truyền
  - R = 1/t (đơn vị là bauds),
  - t: độ dài thời gian của tín hiệu
- 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.

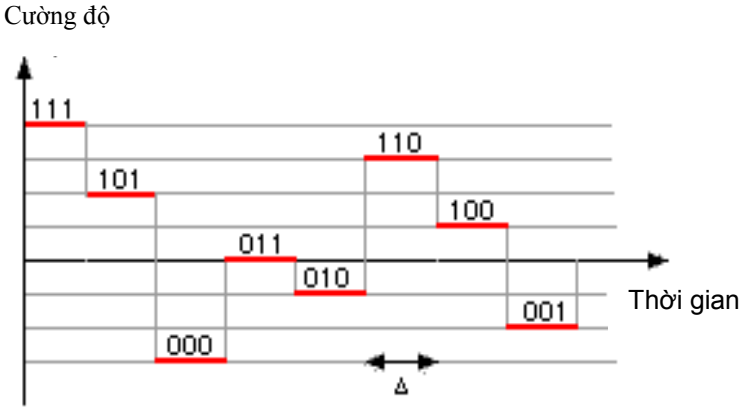
Một số ví dụ về tần số biến điệu và tốc độ dữ liệu



R = 1/Δ D = R



R = 1/ Δ D = 2R



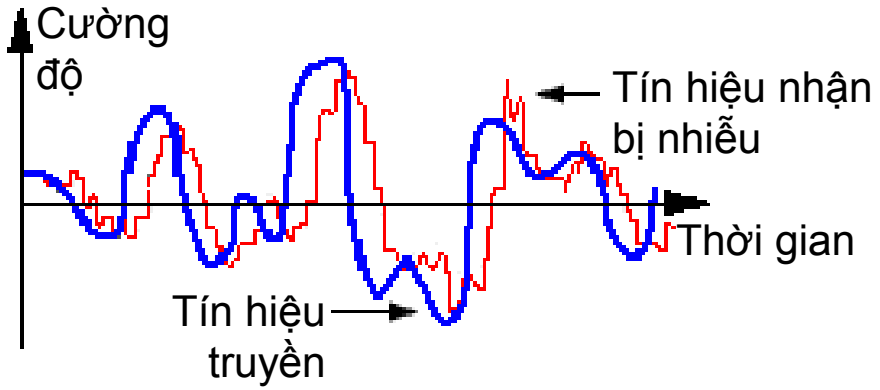
R = 1/ Δ D =3 R

Tăng tốc độ truyền dữ liệu

- Vì D = n R
- Để tăng D:
  - Hoặc tăng n (số bit truyền tải bởi một tín hiệu), tuy nhiên nhiễu là một rào cản quan trọng.
  - Hoặc R(tần số biến điệu), tuy nhiên chúng ta cũng không thể vượt qua tần số biến điệu cực đại Rmax
- Nyquist (1928):
  - Lý thuyết: Rmax = 2 W,
  - Thực tế thì Rmax = 1,25 W

Nhiễu và khả năng kênh truyền

- Có 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 và khả năng kênh truyền

- Tỷ lệ giữa công suất tín hiệu và công suất nhiễu tính theo đơn vị décibels :
  - $S/B = 10\log_{10}(P_S(Watt)/P_B(Watt))$
- Định lý Shannon (1948) xác định số bit tối đa có thể chuyên chở bởi một tín hiệu:

$$n_{max} = \log_2 \sqrt{1 + \frac{P_S}{P_B}}$$

Khả năng của kênh truyền

- Kết hợp giữa Nyquist và Shannon:

$$C = D_{max} = R_{max} n_{max} = 2W \log_2 \sqrt{1 + \frac{P_S}{P_B}} = W \log_2 [1 + \frac{P_S}{P_B}]$$

- 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

Khả năng của kênh truyền

- *Ví dụ* : Kênh truyền điện thoại có
  - Độ rộng băng thông là W = 3100 Hz
  - Tỷ lệ S/B = 20 dB.
  - Hãy tính được khả năng của kênh truyền điện thoại C = ?
- Ta có:

$$C = D_{max} = R_{max} n_{max} = 2W \log_2 \sqrt{1+\frac{P_S}{P_B}} = W \log_2 [1+\frac{P_S}{P_B}]$$

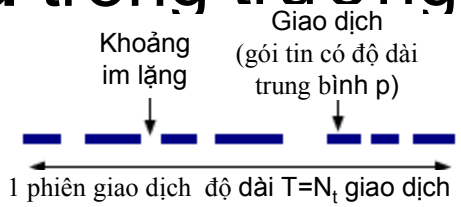
  - Từ $S/B = 10\log_{10}(P_S/P_B)$
  - => $P_S/P_B = 10^{((S/B)/10)} = 10^{((20)/10)} = 10^2$
  - => $C = W \log_2(1+P_S/P_B) = 3100 * \log_2(1+100) = 20600$ b/s

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.
- Một cuộc giao tiếp là một **phiên giao dịch** (session) với độ dài trung bình là T (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 :
  - E = T Nc / 3600
  - Đo mức độ sử dụng kênh truyền trong một giây

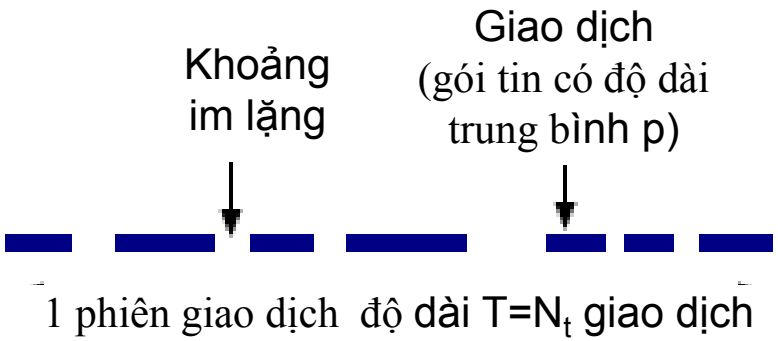
Giao thông (Traffic)

- 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.
- Gọi **D** là tốc độ bit của kênh truyền, tốc độ bit thật sự **d** trong trường hợp này là:



$$d = \frac{N_t p}{T}$$

Giao thông (Traffic)



- Gọi **D** là tốc độ bit của kênh truyền, tốc độ bit thật sự **d** trong trường hợp này là:

$$d = \frac{N_t p}{T}$$

- Tần suất sử dụng kênh truyền được định nghĩa bởi tỷ số:

$$\theta = \frac{d}{D}$$

Giao thông (Traffic)

- 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
    - Tần suất sử dụng kênh truyền θ = 0.05

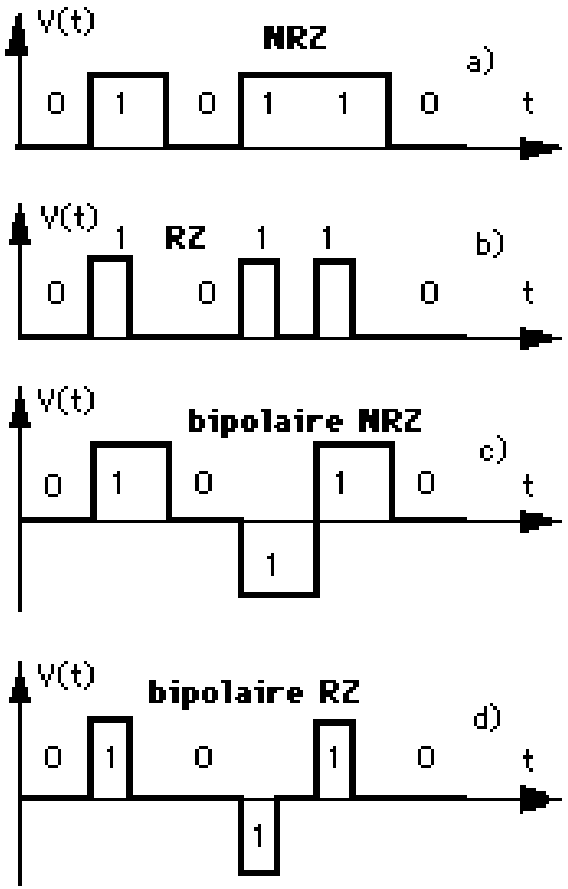
Mã hóa đường truyền (Line Coding)

Khái niệm

- 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).

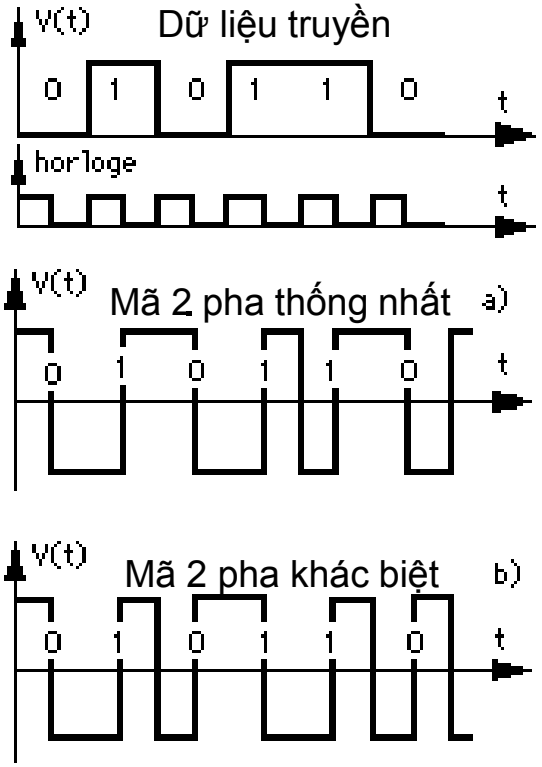
Mã hóa đường truyền bằng tín hiệu số

- 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.
- 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



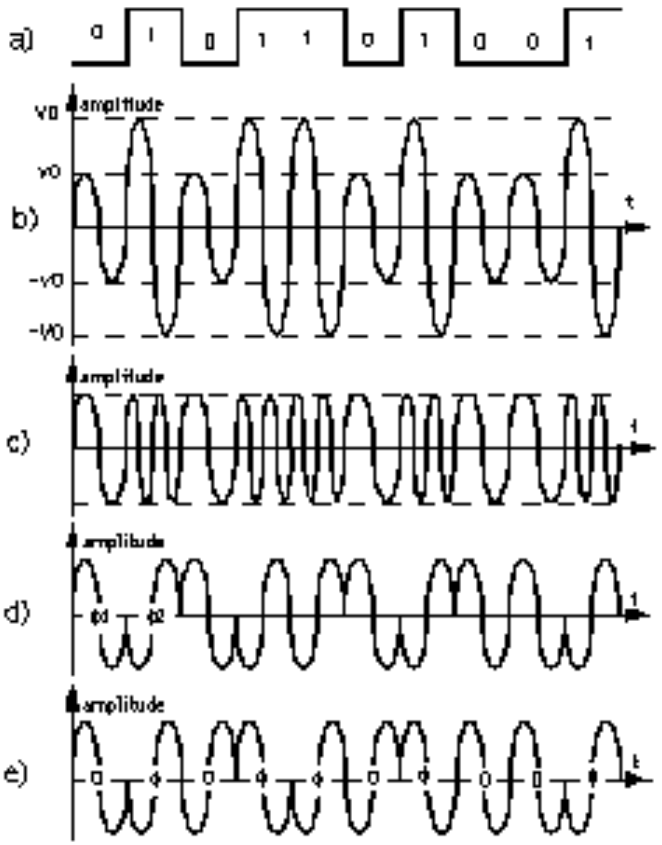
Mã hóa đường truyền bằng tín hiệu số

- Mã hóa hai pha (biphase):
  - 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.
  - 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 hóa đường truyền bằng tín hiệu tuần tự

- 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



Tầng Liên Kết Dữ Liệu (Data Link Layer)

Trình bày: Ngô Bá Hùng
Khoa CNTT&TT
Đại Học Cần Thơ

Mục đích

- Chương này nhằm giới thiệu những nội dung cơ bản 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.

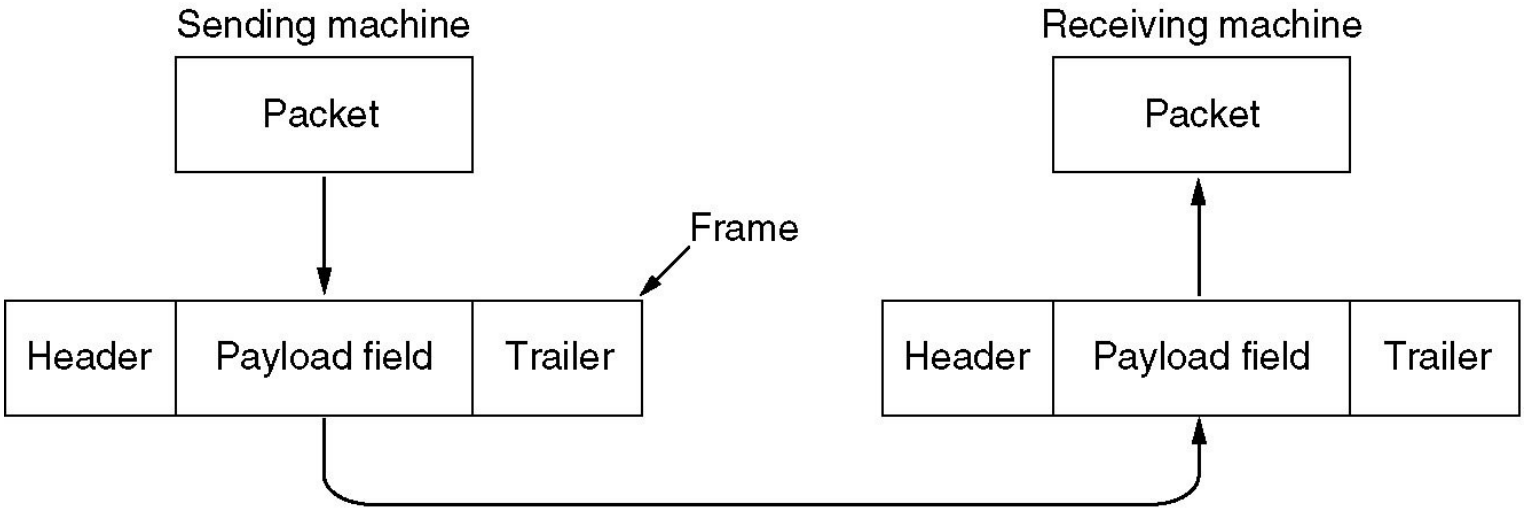
Yêu cầu

- Sau khi học xong chương này, người học phải có được những 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 đặc 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

Chức năng của tầng liên kết dữ liệu

- 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

Chức năng của tầng liên kết dữ liệu



- Cung cấp các dịch vụ cho tầng mạng
- Truyền tải dữ liệu nhận được từ tầng mạng trên máy gởi đến tầng mạng trên máy nhận

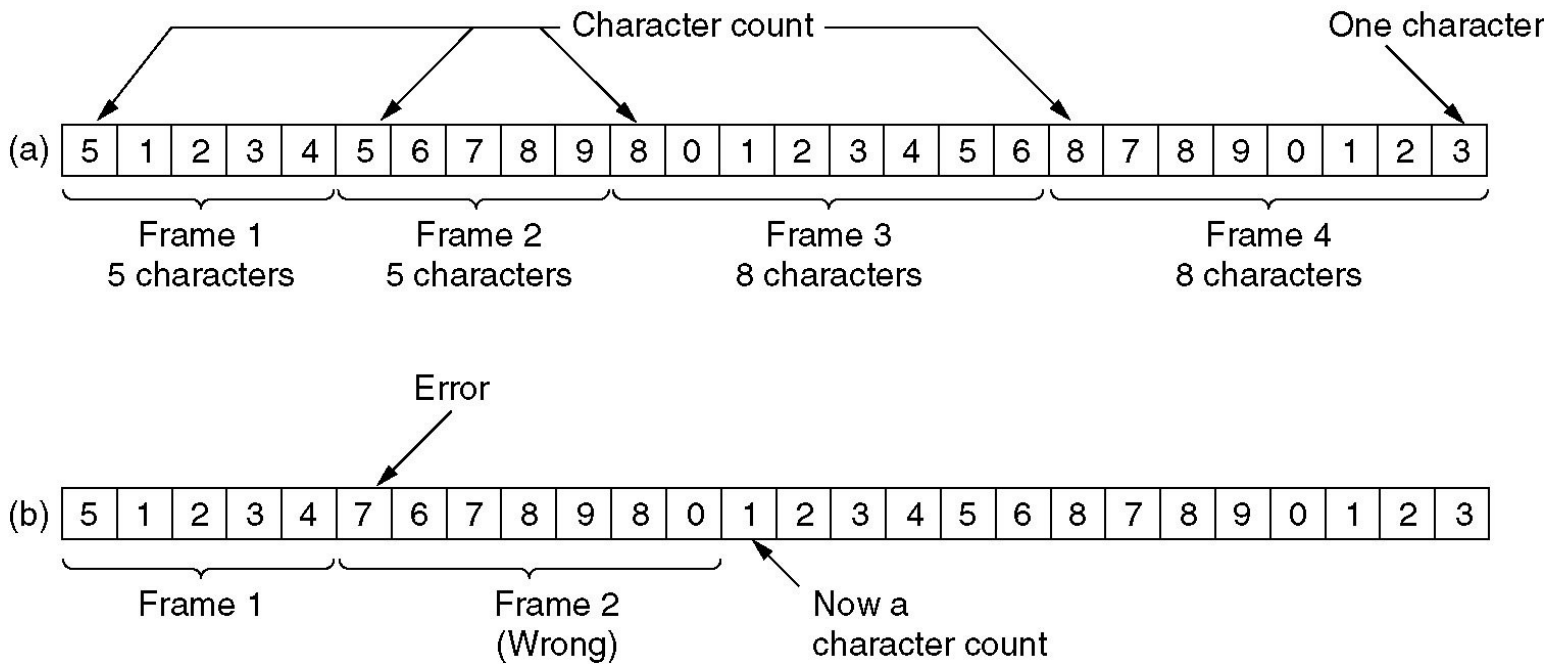
Chức năng của tầng liên kết dữ liệu
Các dịch vụ cơ bản

- 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.

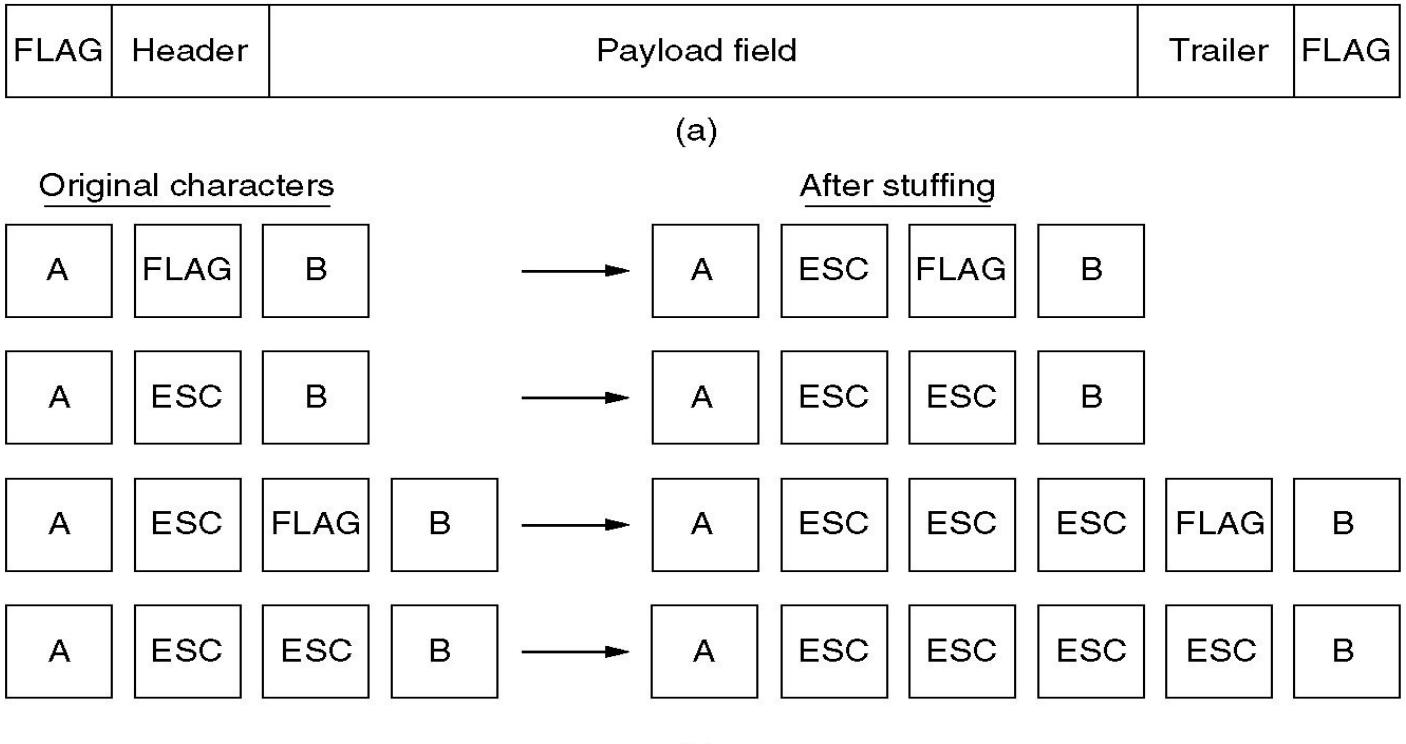
Chức năng của tầng liên kết dữ liệu
Định khung

- Qui định khuôn dạng của khung được sử dụng ở tầng Liên kết dữ liệu
- 3 phương pháp định khung phổ biến:
  - Đếm ký tự (Charater count)
  - Sử dụng các bytes làm cờ hiệu và các bytes độn (Flag byte with byte stuffing)
  - Sử dụng cờ bắt đầu và kết thúc khung cùng với các bit độn (Starting and ending flags with bit stuffing)

Phương pháp đếm ký tự (Character Count)



Phương pháp sử dụng byte làm cờ và các byte độn (Flag byte with byte stuffing)

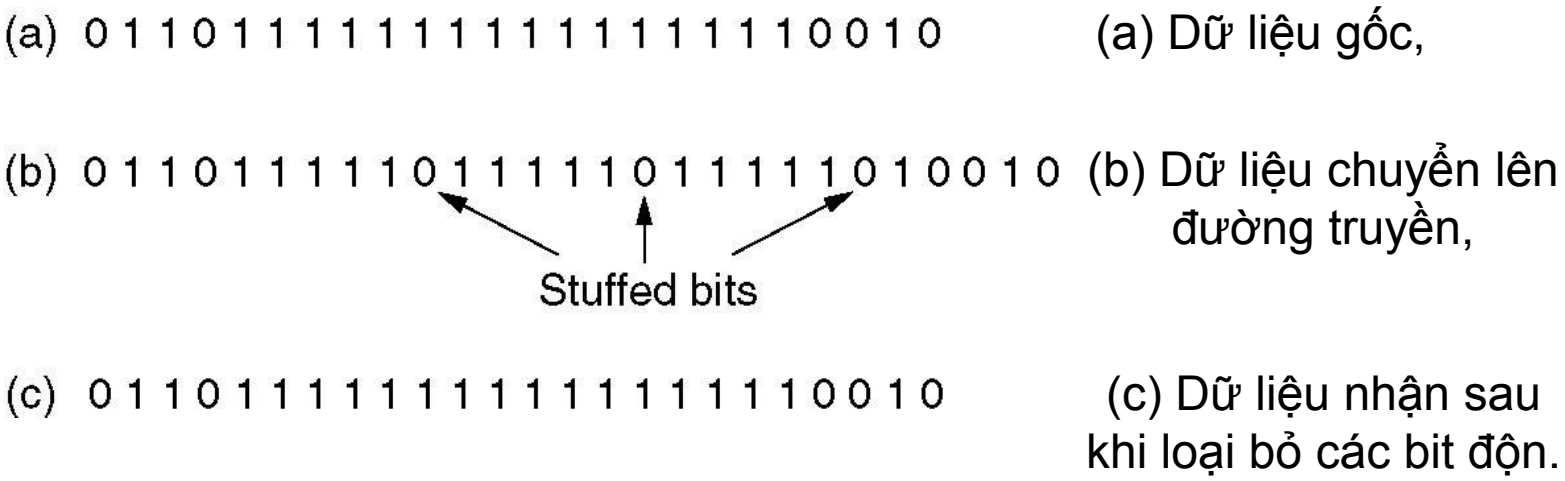


(a) Khung được đánh dấu bởi cờ hiệu,

(b) Dữ liệu có chứa cờ hiệu và byte ESC.

Phương pháp sử dụng cờ bắt đầu và kết thúc khung cùng với các bit độn (Starting and ending flags with bit stuffing)

- Sử dụng mẫu bit đặc biệt, 01111110, để làm cờ đánh dấu điểm bắt đầu và kết thúc khung



Chức năng của tầng liên kết dữ liệu
Điều khiển lỗi (Error Control)

- 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 ?
  - Người nhận báo về tình trạng nhận khung:
    - Sử dụng khung báo nhận (acknowledgement)
  - Tránh chờ vĩnh viễn:
    - Sử dụng bộ đếm thời gian (timer) + time-out
  - Trùng lắp gói tin nhận:
    - Gán số thứ tự cho khung

Chức năng của tầng liên kết dữ liệu
Điều khiển luồng (Flow Control)

- Giải quyết sự khác biệt về tốc độ truyền / nhận dữ liệu của bên truyền và bên nhận
- Hai tiếp cận:
  - 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

Vấn đề xử lý lỗi

Vấn đề xử lý lỗi

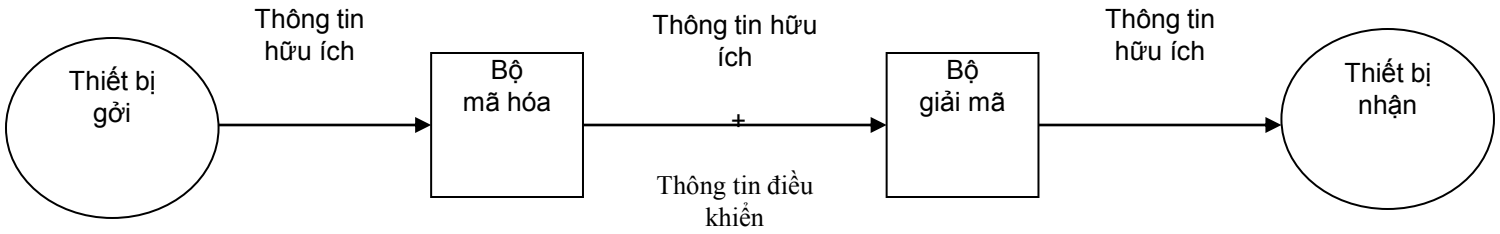
- Bộ mã phát hiện lỗi là gì ?
- Những bộ mã phát hiện lỗi
  - Kiểm tra chẵn lẽ (Parity checks)
  - Kiểm tra thêm theo chiều dọc (Longitudinal reduncy check)
  - Kiểm tra phần dư tuần hoàn (Cyclic redundancy check)

Lỗi trên đường truyền

- Bit 1 thành bit 0 và ngược lại
- Tỷ lệ lỗi
  - τ = Số bít bị lỗi / Tổng số bít được truyền
  - τ : 10^{-5} đến 10^{-8}
  - 88% : sai lệch một bit
  - 10% : sai lệch 2 bit kề nhau

Bộ 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 lỗl.



Bộ mã phát hiện lỗi

- Bộ mã sửa lỗi (Error-correcting codes):
  - Cho phép bên nhận có thể tính toán và suy ra được các thông tin bị lỗi (sửa dữ liệu bị lỗi)
- Bộ mã phát hiện lỗi (Error-detecting codes):
  - 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
- Các hệ thống mạng ngày nay có xu hướng chọn bộ mã phát hiện lỗi.

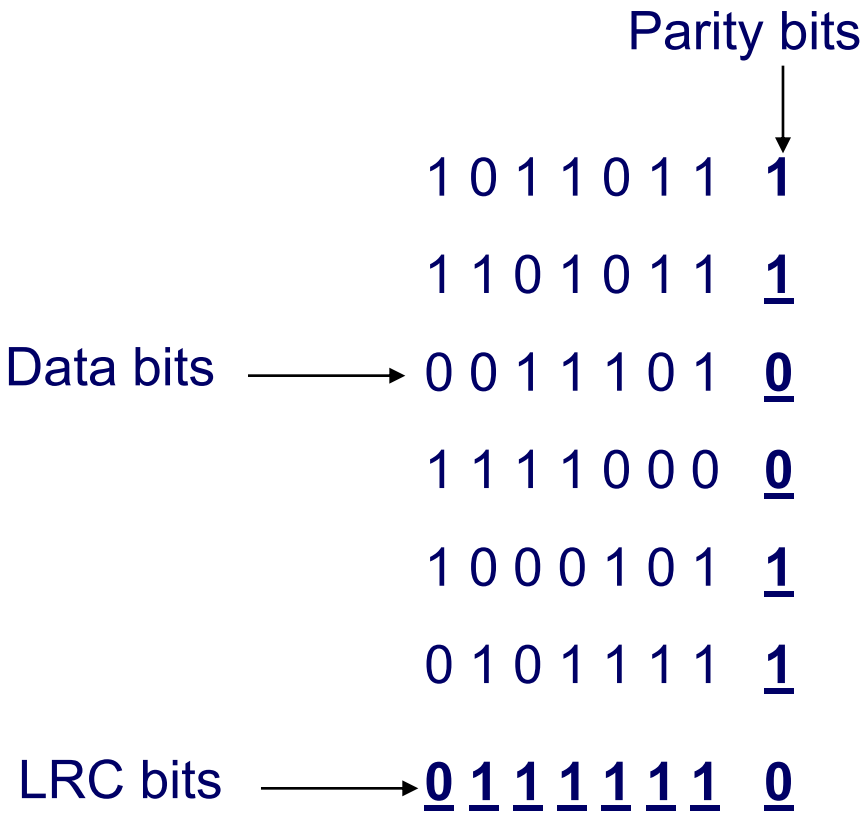
Phương pháp Kiểm tra chẵn lẽ (Parity Check)

- xxxxxxx: chuỗi bits dữ liệu cần truyền
- Thêm vào 1 bit chẵn-lẽ p
- Chuỗi bit truyền là: xxxxxxxp
- p được tính để đảm bảo:
  - Phương pháp kiểm tra chẵn: xxxxxxxp có một số chẵn các bit 1
  - Phương pháp kiểm tra lẽ: xxxxxxxp có một số lẽ các bit 1
- Bên nhận nhận được chuỗi xxxxxxxp:
  - Phương pháp kiểm tra chẵn:
    - Nếu có 1 số chẵn các bit 1: Dữ liệu xxxxxxx không có lỗi
    - Ngược lại là có lỗi
  - Phương pháp kiểm tra lẽ:
    - Nếu có 1 số lẽ các bit 1: Dữ liệu xxxxxxx không có lỗi
    - Ngược lại là có lỗi

Phương pháp Kiểm tra chẵn lẽ (Parity Check)

- Ví dụ: Cần truyền ký tự G = 1110001
- Sử dụng phương pháp kiểm tra chẵn:
  - p=0
  - Chuỗi truyền đi là: 1110001**0**
- Bên nhận nhận được chuỗi:
  - 11100010: 4 bit 1=> không có lỗi
  - 11000010: 3 bit 1=> dữ liệu có lỗi
  - 11000110: 4 bit 1=> không có lỗi ???

Kiểm tra thêm theo chiều dọc (Longitudinal Redundancy Check or Checksum)



Kiểm tra phần dư tuần hoàn (Cyclic Redundancy Check)

- Một số phương pháp cài đặt khác nhau như:
  - Modulo 2,
  - Đa thức,
  - Thanh ghi dịch với các cổng Exclusive-or

Kiểm tra phần dư tuần hoàn Modulo 2

- Giả sử ta có:
  - M: Thông điệp k bit cần gởi sang bên nhận.
  - 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.
  - 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:
  - Nối r bit 0 vào cuối M, hay thực hiện phép nhân M với 2^r
  - Dùng phép chia modulo 2 chia chuỗi bit $M*2^r$ cho P.
  - Phần dư của phép chia sẽ được cộng với $M*2^r$ tạo thành khung T truyền đi.
  - Trong đó P được chọn dài hơn F một bit, và cả hai bit cao nhất và thấp nhất phải là 1
- Bên nhận thực hiện phép chia T cho P:
  - Chia hết: T không có lỗi, Dữ liệu M từ T – k bits trọng số cao
  - Chia không hết: T có lỗi

Kiểm tra phần dư tuần hoàn Modulo 2

- Giả sử ta có:
  - M = 1010001101 (10 bit)
  - P = 110101 (6 bit)
  - FCS cần phải tính toán (5 bit)
- Lần lượt thực hiện các bước sau:
  - Tính $M*2^5$ = 1010001101**00000**.
  - Thực hiện phép chia modulo $M*2^5$ cho P ta được phần dư F = **01110**
  - Tạo khung gởi đi là $T = M*2^r + F$ = 1010001101**01110**

```
                          1 1 0 1 0 1 0 1 1 0     ( Q : Kết quả phép chia)
(P) 1 1 0 1 0 1 | 1 0 1 0 0 0 1 1 0 1 0 0 0 0 0   ( M*2^r)
                  1 1 0 1 0 1
                  -----------
                    1 1 1 0 1 1
                    1 1 0 1 0 1
                    -----------
                      0 1 1 1 0 1
                      0 0 0 0 0 0
                      -----------
                        1 1 1 0 1 0
                        1 1 0 1 0 1
                        -----------
                          0 1 1 1 1 1
                          0 0 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 |
                                  +-----------+
```

Kiểm tra phần dư tuần hoàn
Phương pháp đa thức

- Giả sử ta có M=110011và P = 11001, khi đó M và P được biểu diễn lại bằng 2 đa thức sau:
  - M(x) = x5 + x4 + x + 1
  - P(x) = x4 + x3 + 1
- Quá trình tính CRC được mô tả dưới dạng các biểu thức sau:

$$\frac{X^n\ M(X)}{P(X)} = Q(X) + \frac{R(X)}{P(X)}$$

$$T(X) = X^n\ M(X) + R(X)$$

Kiểm tra phần dư tuần hoàn
Phương pháp đa thức

Các version thường được sử dụng của P là :

$$\text{CRC-12} = X^{12} + X^{11} + X^3 + X^2 + X + 1$$

$$\text{CRC-16} = X^{16} + X^{15} + X^2 + 1$$

$$\text{CRC-CCITT} = X^{16} + X^{12} + X^5 + 1$$

$$\text{CRC-32} = X^{32} + X^{26} + X^{23} + X^{22} + X^{16} + X^{12} + X^{11} + X^{10} + X^8 + X^7 + X^5 + X^4 + X^2 + X + 1$$

Kiểm tra phần dư tuần hoàn
Phương pháp đa thức

Ví dụ:

- Cho: M=1010001101, P=110101
- Ta có: r=5

$$M(x)= x^9+x^7+x^3+x^2+1$$

$$x^5M(x)= x^{14}+x^{12}+x^8+x^7+x^5$$

$$P(x) = x^5+x^4+x^2+1$$

- Thực hiện phép toán:

$$\frac{x^rM(x)}{P(x)} = Q(x) + \frac{F(x)}{P(x)}$$

$$\Rightarrow \quad Q(x)= x^9+ x^8+ x^6+x^4+x^2 +x^1$$

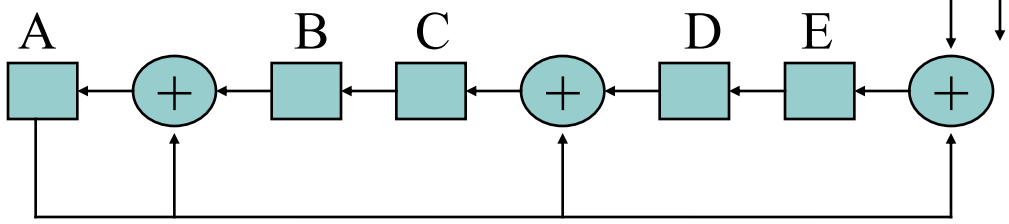
$$F(x)= x^3+ x^2+ x^1 <> \mathbf{01110}$$

⇨ Khung cần truyền đi là T= 1010001101**01110**

Tính FCS sử dụng thanh ghi dịch và cổng XOR

Thí dụ: M=1010001101, P=110101

1010001101**00000**



Thanh ghi dịch bit

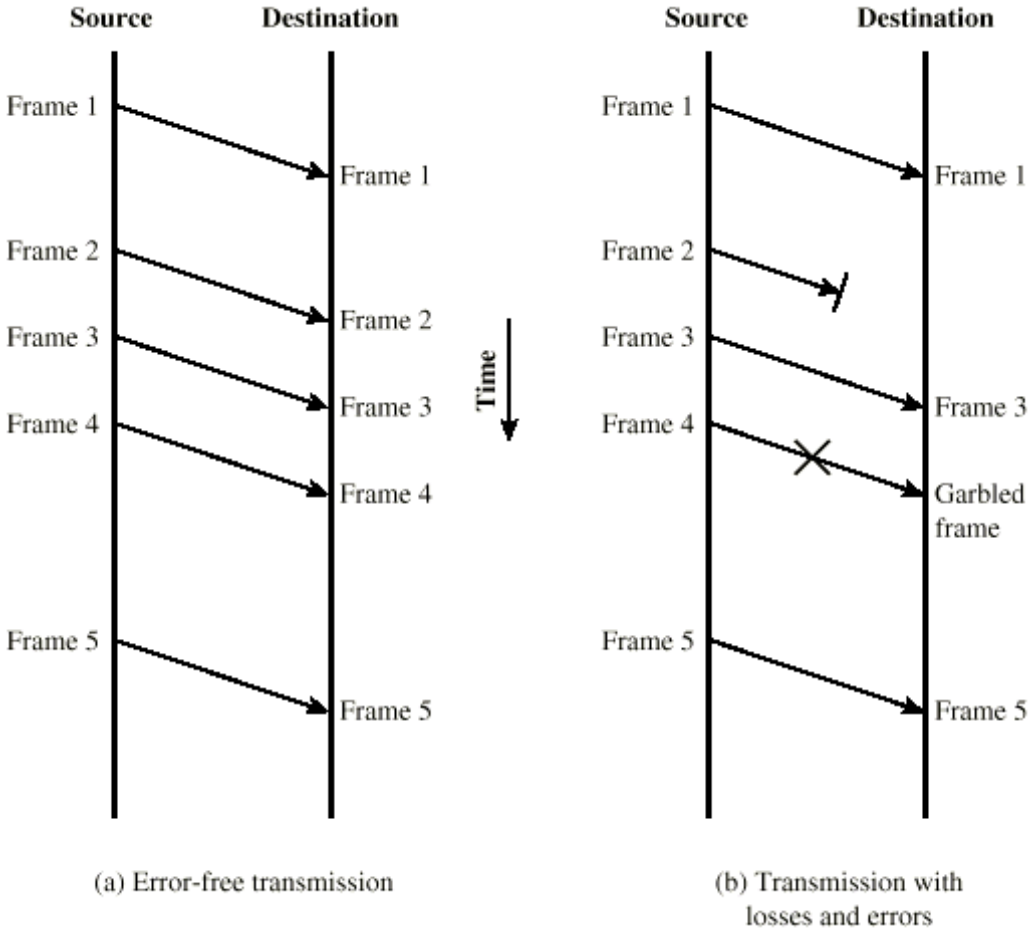
Mạch XOR

Step	A	B	C	D	E	Input
0	0	0	0	0	0	
1	0	0	0	0	1	1
2	0	0	0	1	0	0
3	0	0	1	0	1	1
4	0	1	0	1	0	0
5	1	0	1	0	0	0
6	1	1	1	0	1	0

Step	A	B	C	D	E	Input
7	0	1	1	1	0	1
8	1	1	1	0	1	1
9	0	1	1	1	1	0
10	1	1	1	1	1	1
11	0	1	0	1	1	0
12	1	0	1	1	0	0
13	1	1	0	0	1	0
14	0	0	1	1	1	0
15	0	1	1	1	0	0

VẤN ĐỀ ĐIỀU KHIỂN LỖI (Error Control)

Điều khiển lỗi

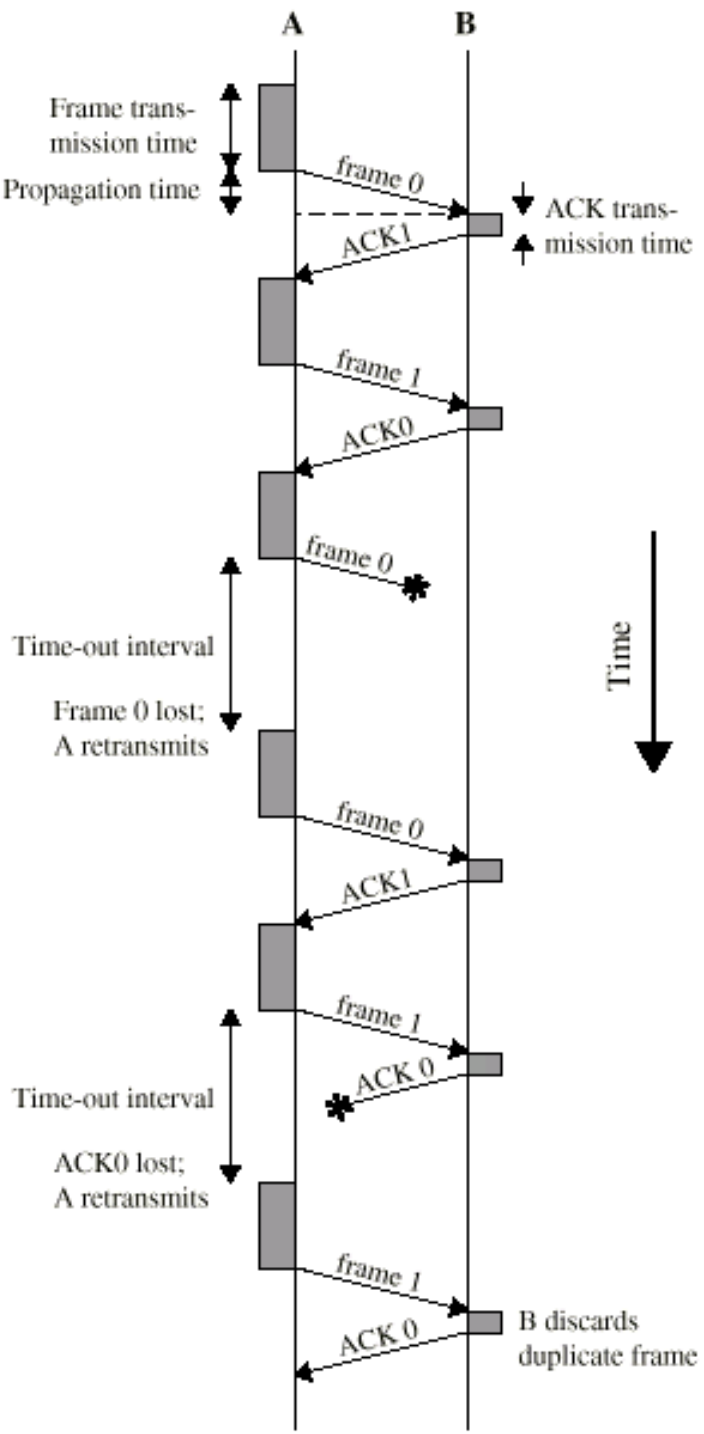


(a) Error-free transmission

(b) Transmission with losses and errors

Stop and Wait - Diagram

- Người gởi không biết được khung có đến nơi nhận tốt hay không.
  - Giải pháp: Khung báo nhận.
- Các khung báo nhận có thể bị mất.
  - Giải pháp:
    - Timer.
    - Time-out
    - Gởi lại
- Bên nhận không phân biệt được cá khung trùng lắp do bên gởi gởi lại.
  - Giải pháp: Mỗi khung sẽ có một số thứ tự



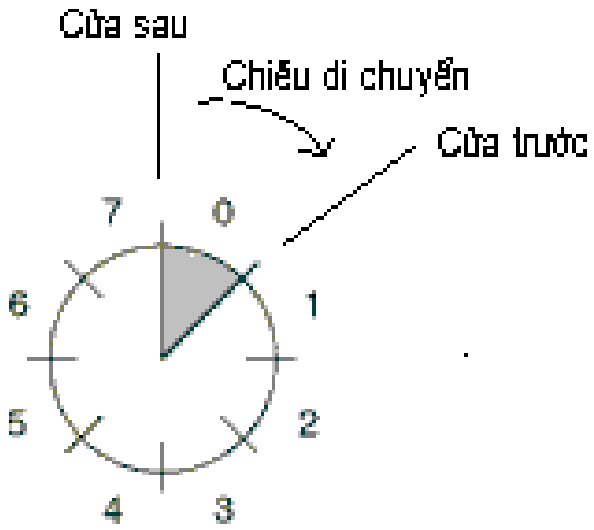
Vấn đề truyền tải thông tin theo hai chiều (Duplex)

- Stop and Wait: truyền đơn công (Simplex)
- Mong muốn việc truyền tải thông tin theo chế độ song công (Duplex) để khai thác tối đa năng lực kênh truyền. Nguyên tắc thực hiện như sau:
  - Vẫn thực hiện việc truyền tải khung,
  - Phân loại khung: DATA, ACK, NACK
  - Sử dụng kỹ thuật **piggyback**.

Giao thức cửa sổ trượt (Sliding windows)

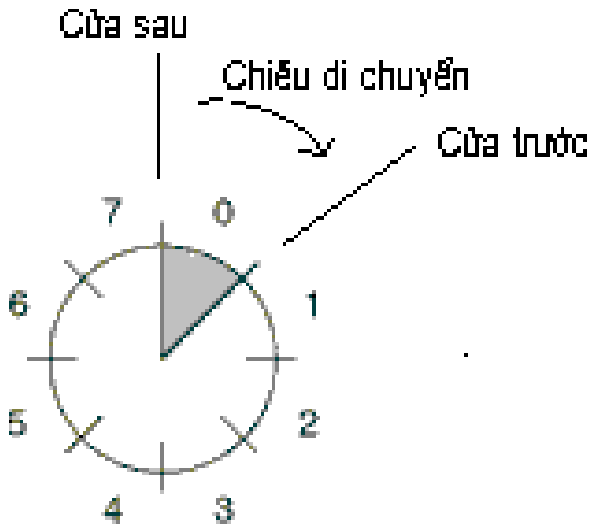
- Thay vì chỉ truyền đi một khung tại một thời điểm (simplex), giao thức cửa sổ trượt cho phép bên gởi có thể gởi đi nhiều khung.
- Cửa sổ gởi (Sending Windows): Bên gởi theo dõi các khung mà nó được phép gởi đi và các khung mà nó đang chờ báo nhận
- Cửa sổ nhận (Receiving Windows): Bên nhận theo dõi các khung mà nó được phép nhận

Cửa sổ trượt (Sliding Windows)



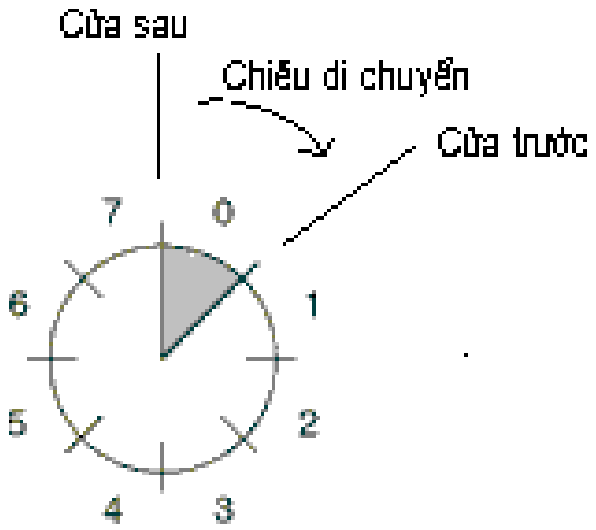
- Cửa sổ gồm có **cửa trước** và **cửa sau** cùng di chuyển theo một chiều.
- Kích thước của cửa sổ là chiều của cung giới hạn từ cửa sau đến cửa trước.
- Kích thước của cửa sổ có thể thay đổi:
  - Khi cửa trước di chuyển, cửa sổ được mở rộng ra.
  - Khi cửa sau di chuyển, kích thước của cửa sổ bị thu hẹp lại và nó làm cho cửa sổ thay đổi vị trí, trượt / quay quanh một tâm của vòng

Cửa sổ trượt (Sliding Windows)



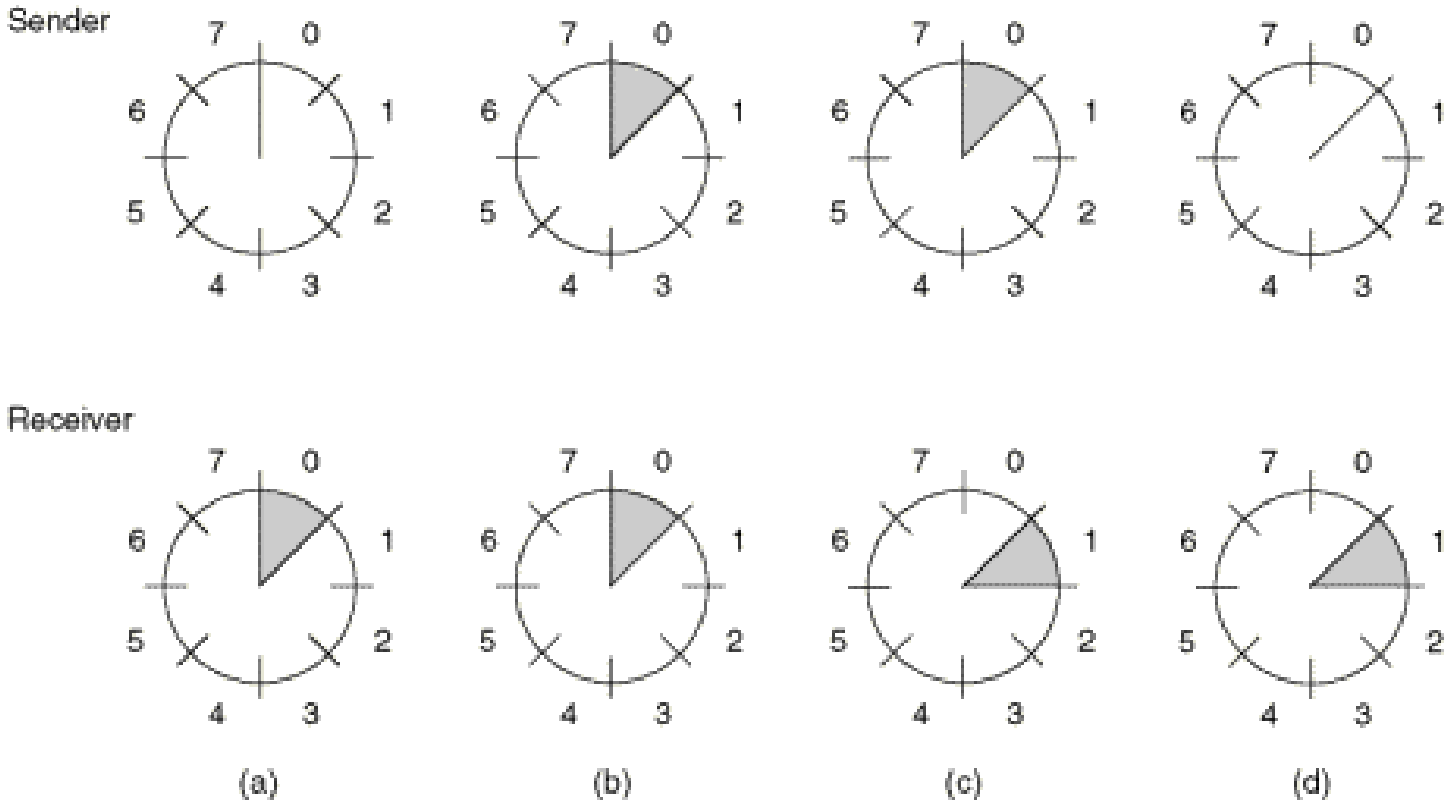
- Kích thước nhỏ nhất của cửa số là 0
- Kích thước tối đa của cửa sổ là n-1
- k bit để đánh số thứ tự khung [0- (2^k-1)] => Khi đó cửa sổ trượt sẽ được chia thành 2^k vị trí tương ứng với 2^k khung.
- Đối với cửa sổ gởi, các vị trí nằm trong cửa sổ trượt biểu hiện số thứ tự của các khung mà bên gởi đang 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.

Cửa sổ trượt (Sliding Windows)

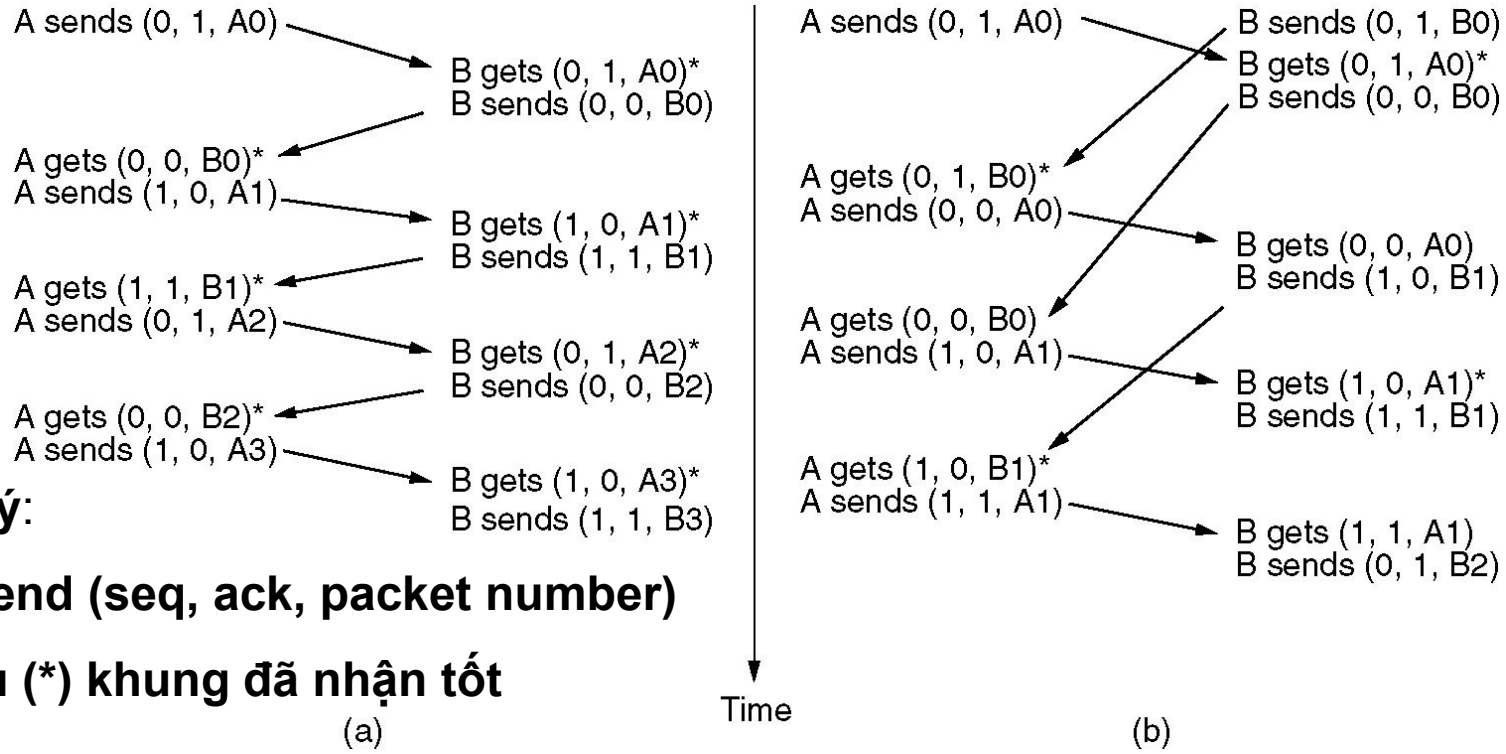


- Đối với bên nhận, các vị trí nằm trong cửa sổ biểu hiện số thứ tự các khung mà nó đang sẵn sàng chờ nhận.
- Kích thước tối đa của cửa sổ biểu thị dung lượng bộ nhớ đệm của bên nhận có thể lưu tạm thời các gói tin nhận được trước khi xử lý chúng.
- Giả sử bên nhận có một vùng bộ nhớ đệm có khả năng lưu trữ 4 khung nhận được. Khi đó, kích thước tối đa của cửa sổ sẽ là 4

Hoạt động cửa sổ trượt



Ví dụ giao thức cửa sổ trượt với kích thước là 1



Chú ý:

- **A send (seq, ack, packet number)**
- **Dấu (*) khung đã nhận tốt**

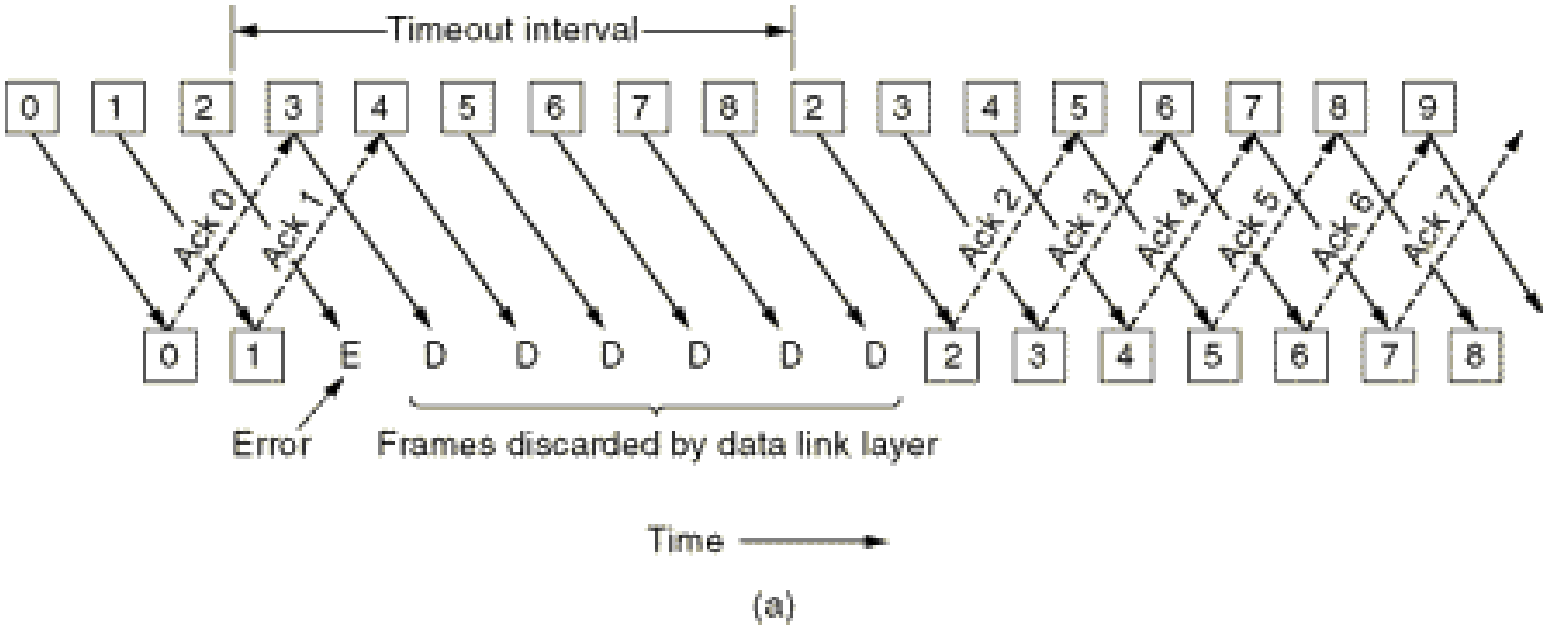
(a): Việc gởi nhận diễn ra bình thường theo đúng tuần tự

(b): Việc gởi nhận diễn ra theo một trình tự bất kỳ

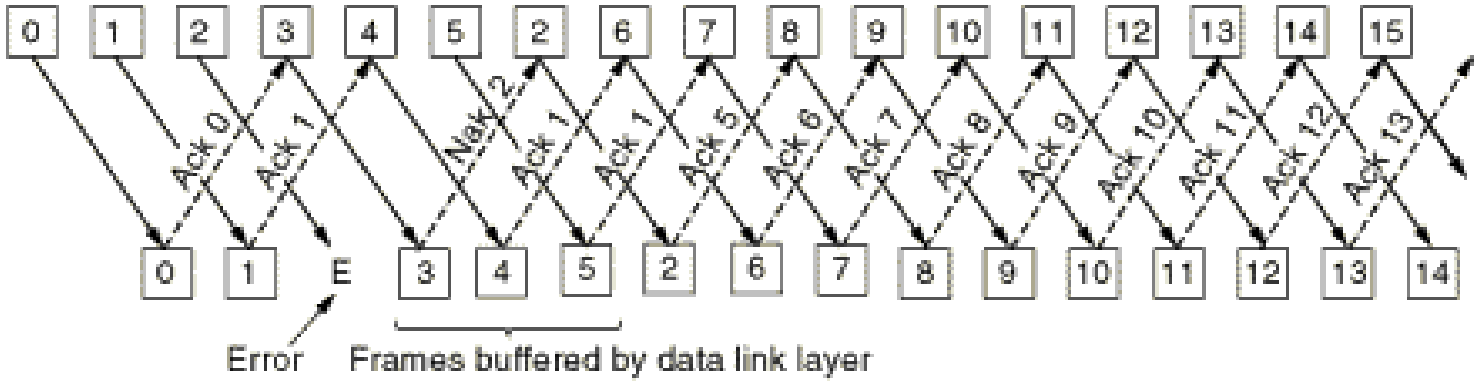
Giao thức Go-Back-N

- 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 khung bị lỗi và toàn bộ các khung phía sau nó.

Giao thức Go-Back-N



Giao thức Selective Repeat

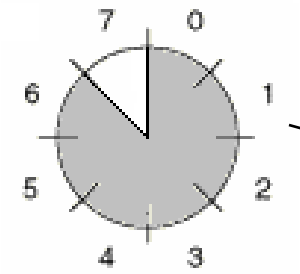


(b)

Xác định kích thước cửa sổ trượt

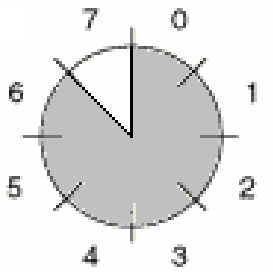
- Xét cửa sổ trượt sử dụng 3 bits để đánh chỉ số khung => Kích thước cửa sổ là 7

Sender



Đã gởi và chờ bào nhận các khung 0,1,2,3,4,5,6

Receiver

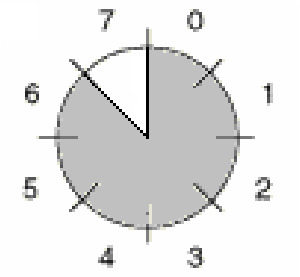


Đang sẵn sàng chờ nhận các khung 0,1,2,3,4,5,6

Xác định kích thước cửa sổ trượt

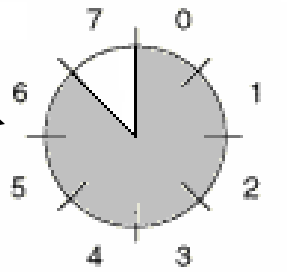
- Xét cửa sổ trượt sử dụng 3 bits để đánh chỉ số khung => Kích thước cửa sổ là 7

Sender



Đã gởi và chờ bào nhận các khung 0,1,2,3,4,5,6

Receiver

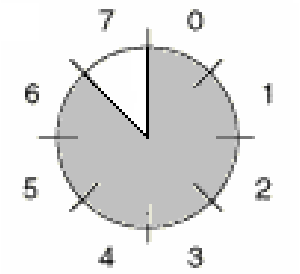


Nhận các 0,1,2,3,4,5,6, Kiểm tra lỗi

Xác định kích thước cửa sổ trượt

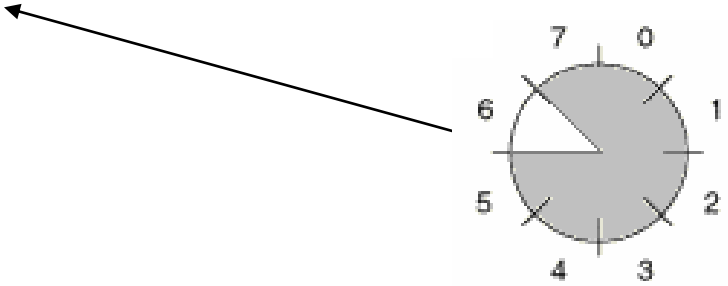
- Xét cửa sổ trượt sử dụng 3 bits để đánh chỉ số khung => Kích thước cửa sổ là 7

Sender



Đã gởi và chờ báo nhận các khung 0,1,2,3,4,5,6

Receiver

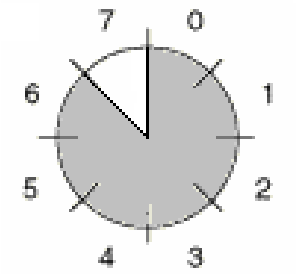


Khung 0,1,2,3,4,5,6 không có lỗi,
Gởi báo nhận cho các khung 0,1,2,3,4,5,6
Sẵn sàng chờ nhận các khung 7,0,1,2,3,4,5

Xác định kích thước cửa sổ trượt

- Xét cửa sổ trượt sử dụng 3 bits để đánh chỉ số khung => Kích thước cửa sổ là 7

Sender

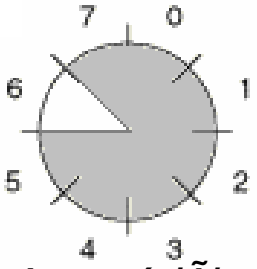


Đã gởi và chờ bào nhận các khung 0,1,2,3,4,5,6

Đường truyền bị lỗi
Khung báo nhận không đến nơi

X

Receiver

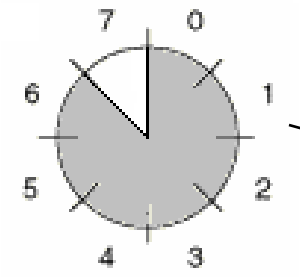


Khung 0,1,2,3,4,5,6 không có lỗi,
Gởi báo nhận cho các khung 0,1,2,3,4,5,6
Sẵn sàng chờ nhận các khung 7,0,1,2,3,4,5

Xác định kích thước cửa sổ trượt

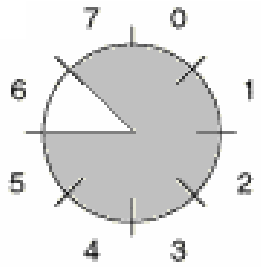
- Xét cửa sổ trượt sử dụng 3 bits để đánh chỉ số khung => Kích thước cửa sổ là 7

Sender



Quá thời hạn
Gởi lại khung 0
Chờ báo nhận
các khung 0,1,2,3,4,5,6

Receiver

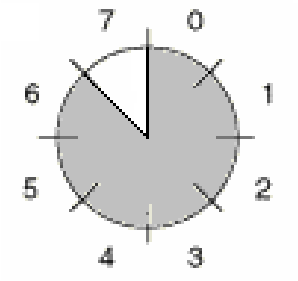


Đang sẵn sàng chờ nhận
các khung 7,0,1,2,3,4,5

Xác định kích thước cửa sổ trượt

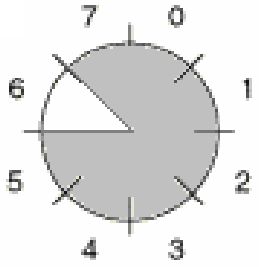
- Xét cửa sổ trượt sử dụng 3 bits để đánh chỉ số khung => Kích thước cửa sổ là 7

Sender



Quá thời hạn
Gởi lại khung 0
Chờ báo nhận
các khung 0,1,2,3,4,5,6

Receiver

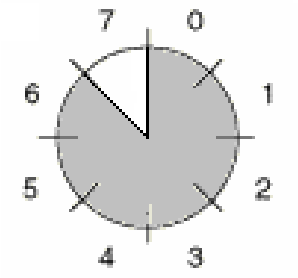


Khung 0 đến nơi, điều gì xảy ra tại bên nhận?

Xác định kích thước cửa sổ trượt

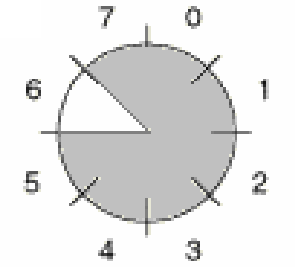
- Xét cửa sổ trượt sử dụng 3 bits để đánh chỉ số khung => Kích thước cửa sổ là 7

Sender



Quá thời hạn
Gởi lại khung 0
Chờ báo nhận
các khung 0,1,2,3,4,5,6

Receiver

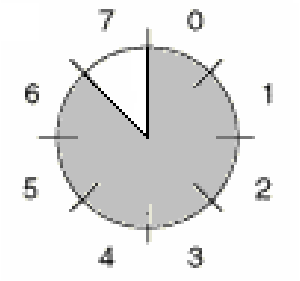


Khung 0 đến nơi,
Nếu giao thức xử lý lỗi Go-Back-N
Sẽ báo lỗi vì khung đang chờ để nhận
theo thứ tự là khung số 7, rồi mới đến 0

Xác định kích thước cửa sổ trượt

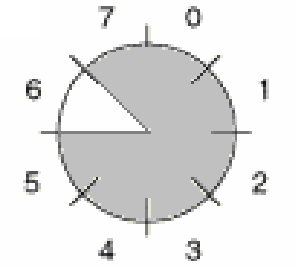
- Xét cửa sổ trượt sử dụng 3 bits để đánh chỉ số khung => Kích thước cửa sổ là 7

Sender



Quá thời hạn
Gởi lại khung 0
Chờ bào nhận
các khung 0,1,2,3,4,5,6

Receiver



Khung 0 đến nơi,
Nếu giao thức xử lý lỗi Selective-Repeat
Khung 0 là khung đang chờ để nhận,
=> chuyển lên tầng mạng, nhận khung 0 hai lần!!

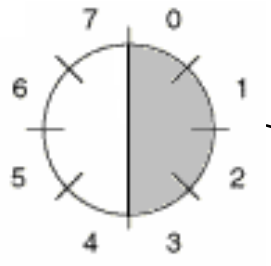
Xác định kích thước cửa sổ trượt

- Trong Go-Back-N:
  - Kích thước cửa sổ trượt tối đa 2^k-1
- Trong Selective-Repeat
  - Phải đảm bảo rằng cửa sổ nhận mới không đè chồng lên cửa sổ trước đó.
  - Kích thước tối đa của của sổ nhận bằng một nửa khoảng đánh số thứ tự của khung: 2^{k-1}
  - 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.
    - Nếu dùng 4 bit để đánh số thứ tự khung từ 0 đến 15 thì kích thước tối đa cửa sổ nhận là (15-0+1)/2 =8.

Xác định kích thước cửa sổ trượt

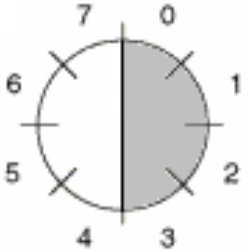
- Xét cửa sổ trượt sử dụng 3 bits để đánh chỉ số khung, cơ chế xử lý lỗi là Selective-Repeat => Kích thước cửa sổ là 4

Sender



Đã gởi và chờ báo nhận các khung 0,1,2,3,

Receiver

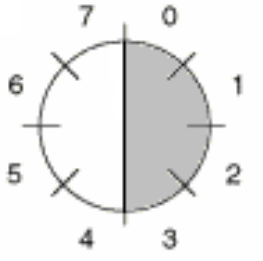


Đang sẵn sàng chờ nhận các khung 0,1,2,3

Xác định kích thước cửa sổ trượt

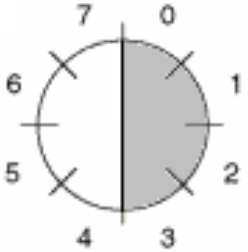
- Xét cửa sổ trượt sử dụng 3 bits để đánh chỉ số khung => Kích thước cửa sổ là 4

Sender



Đã gởi và chờ báo nhận các khung 0,1,2,3

Receiver

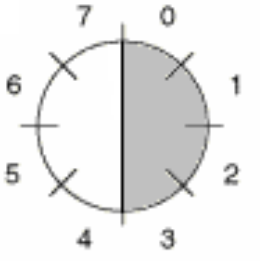


Nhận các 0,1,2,3
Kiểm tra lỗi

Xác định kích thước cửa sổ trượt

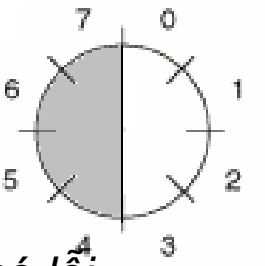
- Xét cửa sổ trượt sử dụng 3 bits để đánh chỉ số khung => Kích thước cửa sổ là 4

Sender



Đã gởi và chờ báo nhận các khung 0,1,2,3

Receiver

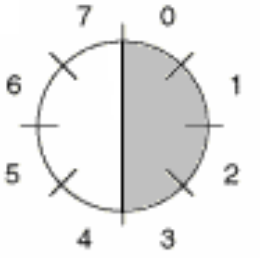


Khung 0,1,2,3 không có lỗi,
Gởi báo nhận cho các khung 0,1,2,3
Sẵn sàng chờ nhận các khung 4,5,6,7

Xác định kích thước cửa sổ trượt

- Xét cửa sổ trượt sử dụng 3 bits để đánh chỉ số khung => Kích thước cửa sổ là 4

Sender

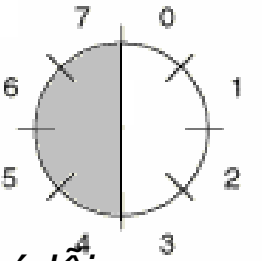


Đã gởi và chờ báo nhận các khung 0,1,2,3

Đường truyền bị lỗi
Khung báo nhận không đến nơi

X

Receiver

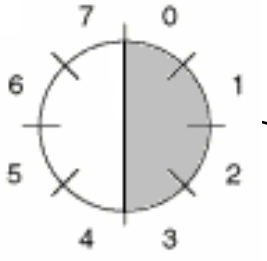


Khung 0,1,2,3 không có lỗi,
Gởi báo nhận cho các khung 0,1,2,3
Sẵn sàng chờ nhận các khung 4,5,6,7

Xác định kích thước cửa sổ trượt

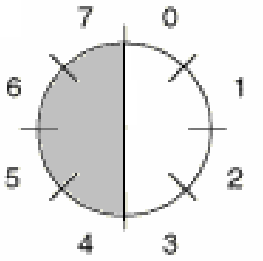
- Xét cửa sổ trượt sử dụng 3 bits để đánh chỉ số khung => Kích thước cửa sổ là 4

Sender



Quá thời hạn
Gởi lại khung 0
Chờ bào nhận
các khung 0,1,2,3

Receiver

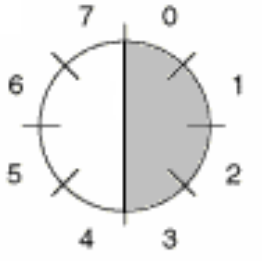


Đang sẵn sàng chờ nhận
các khung 4,5,6,7

Xác định kích thước cửa sổ trượt

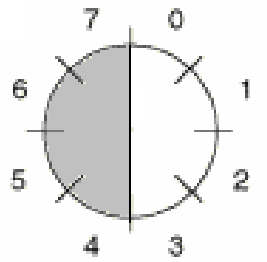
- Xét cửa sổ trượt sử dụng 3 bits để đánh chỉ số khung => Kích thước cửa sổ là 4

Sender



Quá thời hạn
Gởi lại khung 0
Chờ bào nhận
các khung 0,1,2,3

Receiver



Khung 0 đến nơi, Là khung đã nhận
*=> **không đưa lên tầng mạng***

Kích thước vùng đệm dữ liệu (buffer)

- 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.

Thời điểm gởi báo nhận

- Piggy-back: Gói báo nhận vào khung dữ liệu của bên nhận
- Bên nhận không còn dữ liệu để gởi đi?
  - Mỗi lần khung đến khởi động một timer
  - Time – out mà bên nhận không có dữ liệu để gởi => Gởi một khung báo nhận riêng

GIAO THỨC HDLC
(High Level Data Link Control)

Các loại trạm (HDLC Station Types)

- Primary station
  - Điều khiển đường nối kết
  - Khung gởi đi là các lệnh
  - Duy trì nhiều nối kết luận lý đến các secondary station
- Secondary station
  - Chịu sự điều khiển của primary station
  - Các khung gởi đi là các trả lời
- Combined station
  - Có đặc tính của cả Primary station và Secondary station
  - Có thể gởi lệnh và trả lời

Các cấu hình đường nối kết (HDLC Link Configurations)

- Không cân bằng (Unbalanced)
  - Một Primary station và một hoặc nhiều secondary stations
  - Hỗ trợ full duplex và half duplex
- Cân bằng (Balanced)
  - Gồm hai combined stations
  - Hỗ trợ full duplex và half duplex

Các chế độ truyền tải (HDLC Transfer Modes)

- Normal Response Mode (NRM)
- Asynchronous Balanced Mode (ABM)
- Asynchronous Response Mode (ARM)

Các chế độ truyền tải (HDLC Transfer Modes)

- Normal Response Mode (NRM)
  - Cấu hình không cân bằng
  - Primary khởi động cuộc truyền tải tới secondary
  - Secondary chỉ có thể truyền dữ liệu dưới dạng các trả lời cho các yêu cầu của primary
  - Được sử dụng trên các loại cáp nhiều sợi
  - Máy tính đóng vai trò primary
  - Terminals đóng vai trò secondary

Các chế độ truyền tải (HDLC Transfer Modes)

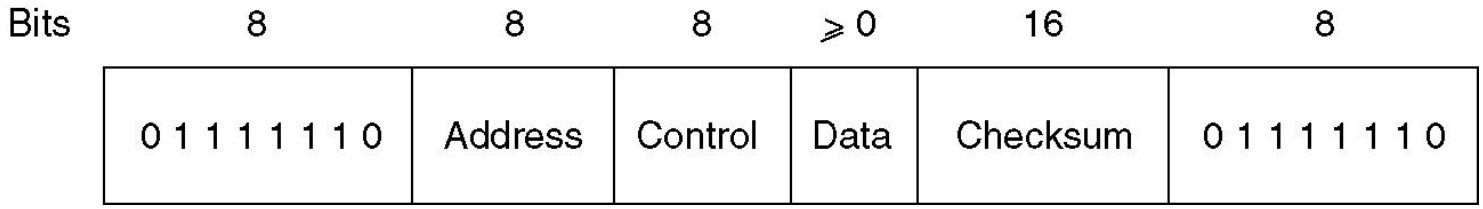
- Asynchronous Balanced Mode (ABM)
  - Cấu hình cân bằng
  - Các trạm đều có thể khởi động một cuộc truyền tải mà không cần có phép
  - Được sử dụng rộng rãi

HDLC Transfer Modes (3)

- Asynchronous Response Mode (ARM)
  - Cấu hình không cân bằng
  - Secondary có thể khởi động một cuộc truyền tải mà không cần xin phép từ primary
  - Primary đảm bảo về đường truyền
  - Ít được dùng

Cấu trúc khung

- Truyền tải đồng bộ (Synchronous transmission)
- Tất cả các cuộc truyền tải đều sử dụng khung
- Một dạng khung cho tất cả các loại dữ liệu và điều khiển

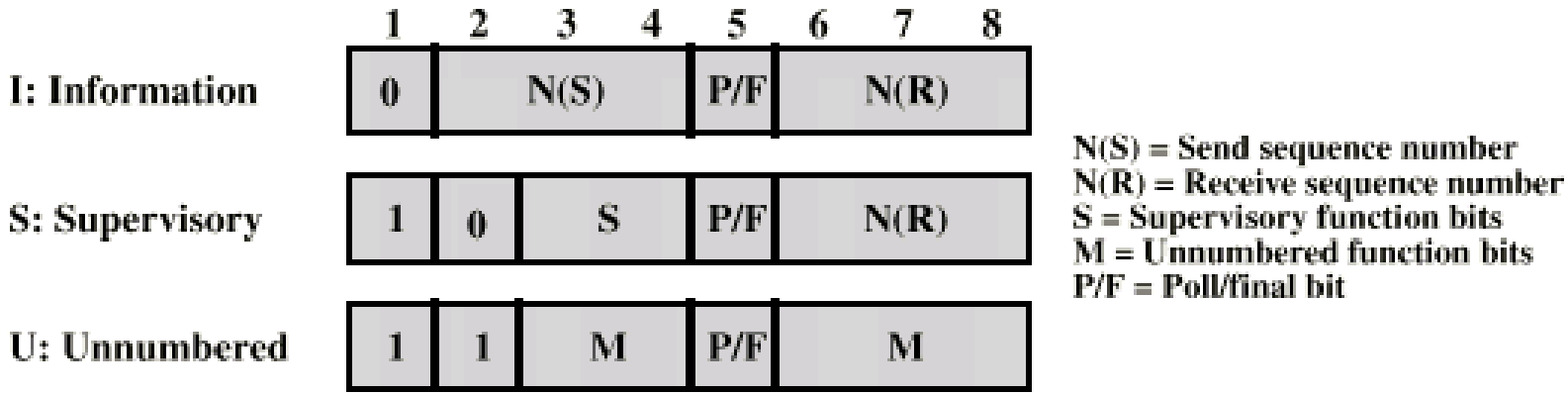


Cấu trúc khung

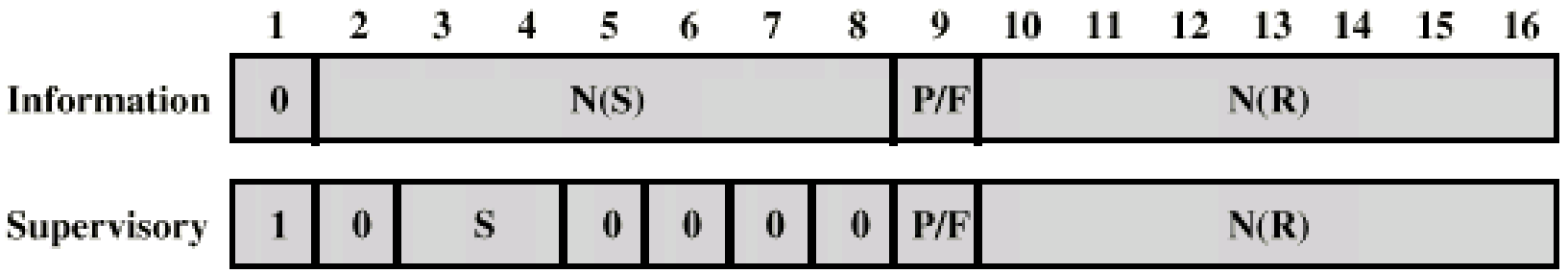
- **Flag (8 bit):** 01111110 , Sử dụng kỹ thuật bít độn
- **Address (8 bit):** Vùng ghi địa chỉ để xác định máy phụ được phép truyền hay nhận khung.
- **Control (8bit):** Được dùng để xác định loại khung:
  - Thông tin (Information),
  - Điều khiển (Supervisory)
  - Không đánh số (Unnumbered).
- **Information(128-1024 bytes):** Vùng chứa dữ liệu cần truyền.
- **FCS (Frame Check Sequence- 8 bit)**
  - CRC-CCITT = X16 + X12 + X5 +1

Control Field

- Khác nhau tùy thuộc vào kiểu khung
  - Information :
    - Khung chứa dữ liệu được truyền đi
    - Đồng thời chứa thông tin báo nhận (piggy-back)
  - Supervisory: Khung báo nhận khi không còn dữ liệu để gởi ngược lại
  - Unnumbered: Dùng để điều khiển nối kết



(c) 8-bit control field format



(d) 16-bit control field format

Poll/Final Bit

- Được sử dụng tùy thuộc vào ngữ cảnh
- Nếu là khung lệnh
  - Có ý nghĩa là Poll
  - Giá trị 1 để yêu cầu bên kia trả lời
- Nếu là khung trả lời
  - Có ý nghĩa là Final
  - Giá trị 1 để biểu thị rằng nó kết thúc việc gởi

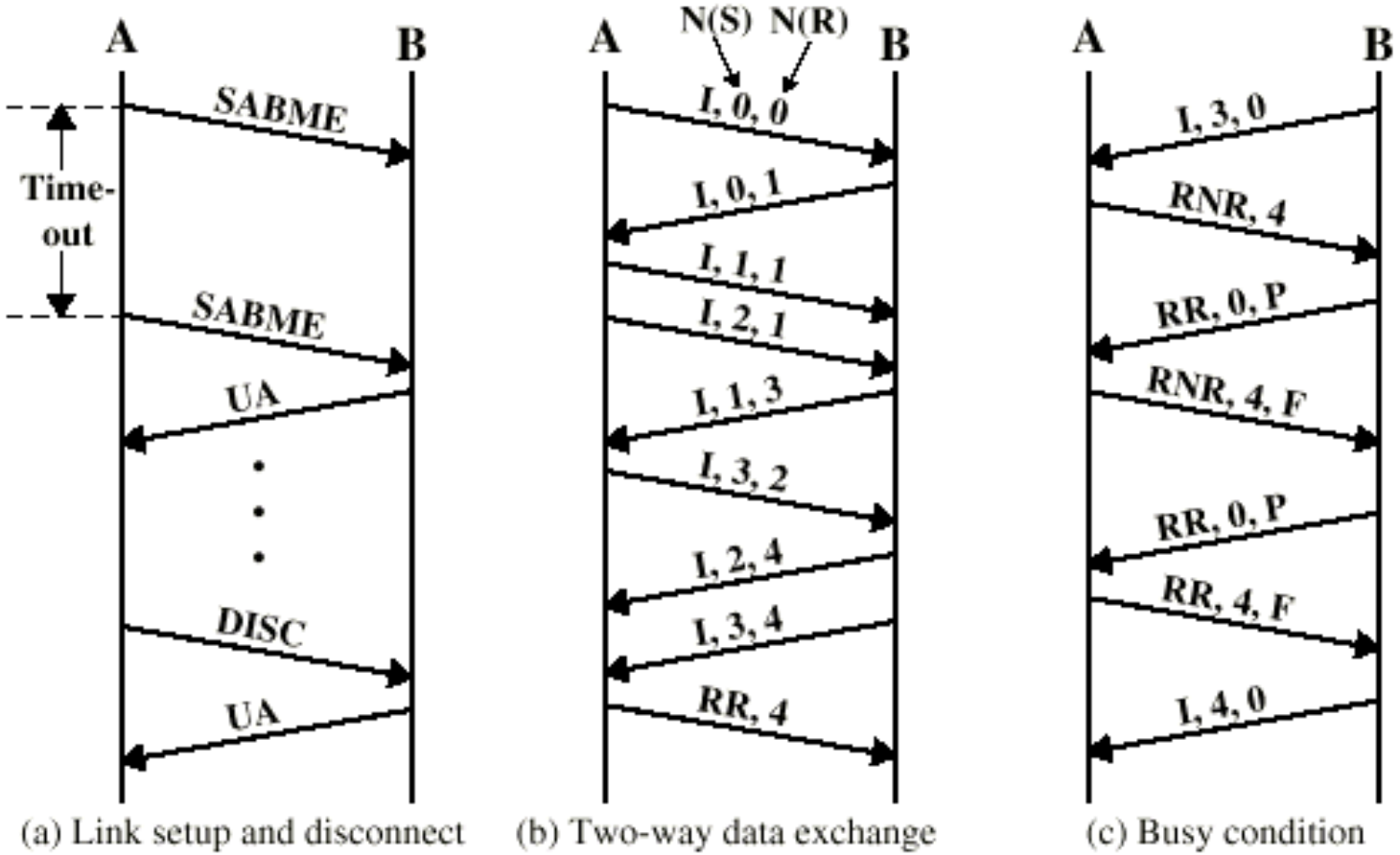
Supervisory function bits

SS=00	RR (Receive Ready), là khung báo nhận, thông báo sẵn sàng 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 (piggyback)
SS=01	REJ (Reject): đây là một khung báo không nhận (negative acknowledge), yêu cầu gởi lại các khung, từ khung Next.
SS=10	RNR (Receive Not Ready): thông báo không sẵn sàng nhận tin, đã nhận đến đến khung thứ Next-1, chưa sẵn sàng nhận khung Next
SS=11	SREJ (Selective Reject): yêu cầu gởi lại một khung có số thức tự là Next

Unumbered Function Bits

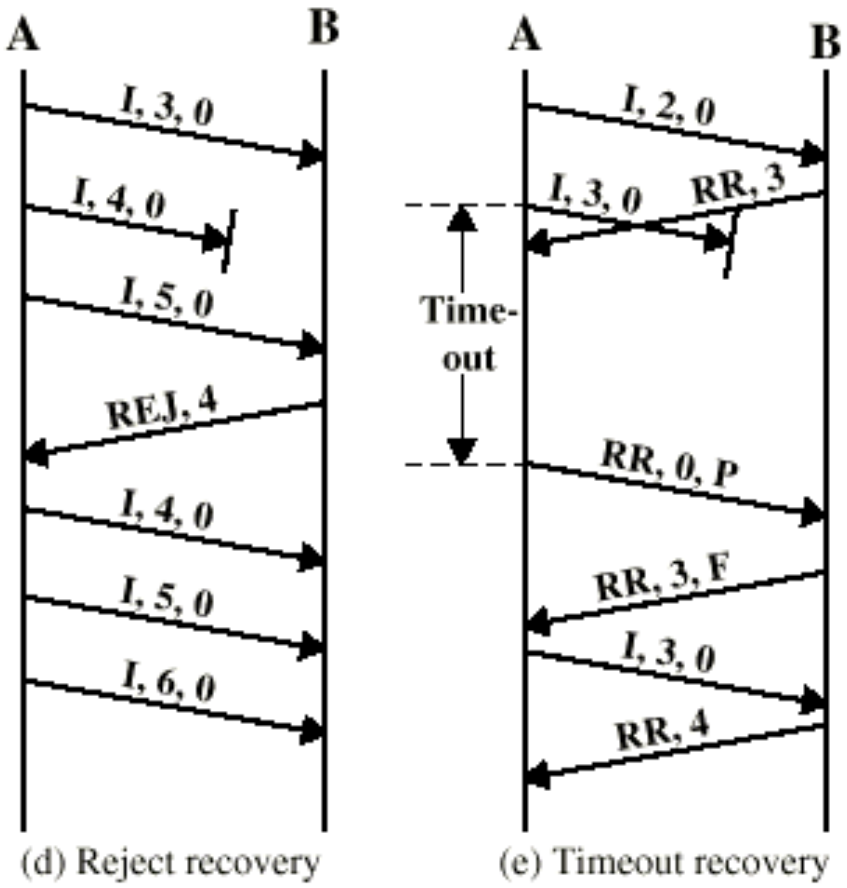
1111P100	Lệnh này dùng để thiết lập chế độ truyền tải SABM (Set Asynchronous Balanced Mode).
1100P001	Lệnh này dùng để thiết lập chế độ truyền tải SNRM (Set Normal Response Mode).
1111P000	Lệnh này dùng để thiết lập chế độ truyền tải SARM (Set Asynchronous Response Mode).
1100P010	Lệnh này để yêu cầu xóa nối kết DISC (Disconnect).
1100F110	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.
1100F001	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.

Một số kịch bản



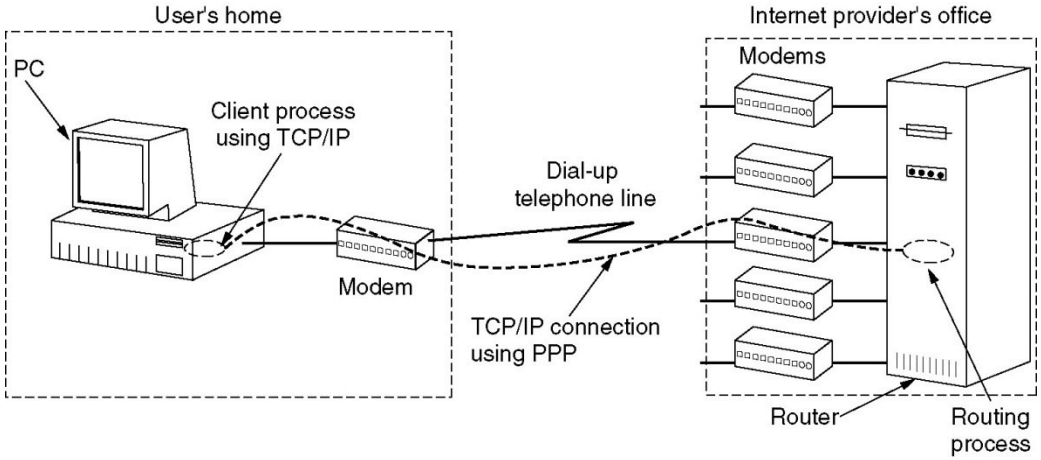
(a) Link setup and disconnect (b) Two-way data exchange (c) Busy condition

Một số kịch bản



(d) Reject recovery (e) Timeout recovery

Giao thức Điểm nối điểm (PPP- Point-to-Point Protocol)



- 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)
- Giao thức điều khiển đường truyền LCP (Link Control Protocol).
- Giao thức thương lượng về các tùy chọn tầng mạng NCP (Network Control Protocol)

LAN & MAC

Trình bày: Ngô Bá Hùng
Khoa CNTT&TT
Đại Học Cần Thơ

Mục đích

- Chương này nhằm giới thiệu những nội dung cơ bản 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
    - Các phương pháp phân lượt truy cập đường truyền.
  - Giới thiệu chi tiết về nguyên tắc hoạt động của các chuẩn mạng cục bộ thuộc mạng Ethernet

Yêu cầu

- Sau khi học xong chương này, người học phải có được những 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

Giới thiệu mạng cục bộ

Phân loại mạng máy tính
Theo khoảng cách địa lý

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 đô thị, 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 một châu lục	
10000 km	Cả hành tinh	

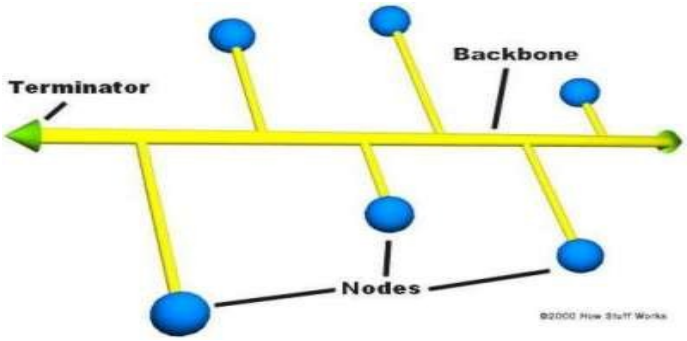
Các đặc tính quan trọng về mặt kỹ thuật

- Tất cả các host trong mạng LAN cùng chia sẻ đường truyền chung.
- Hoạt động dựa trên kiểu quảng bá (broadcast).
- Không yêu cầu phải có hệ thống trung chuyển (routing/switching) trong một LAN đơn.

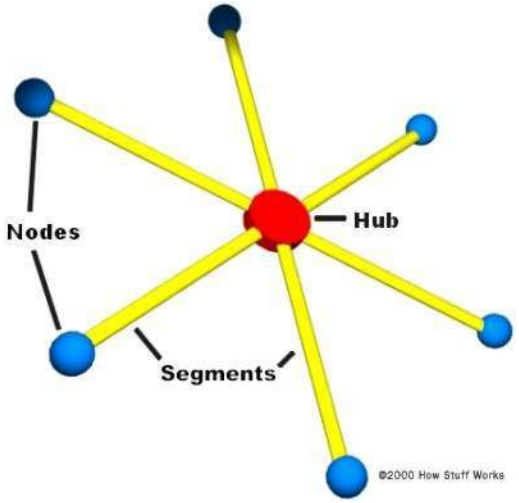
Các thông số định định nghĩa mạng LAN

- Hình trạng (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.
- 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.

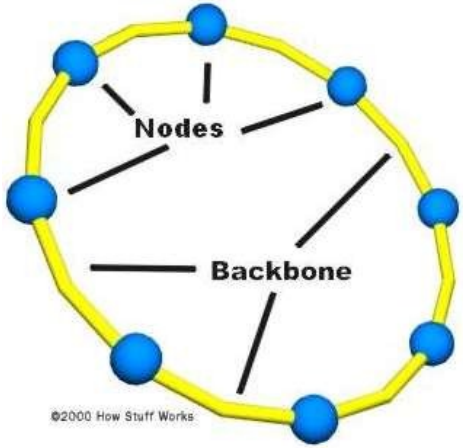
LAN Topologies



BUS



STAR

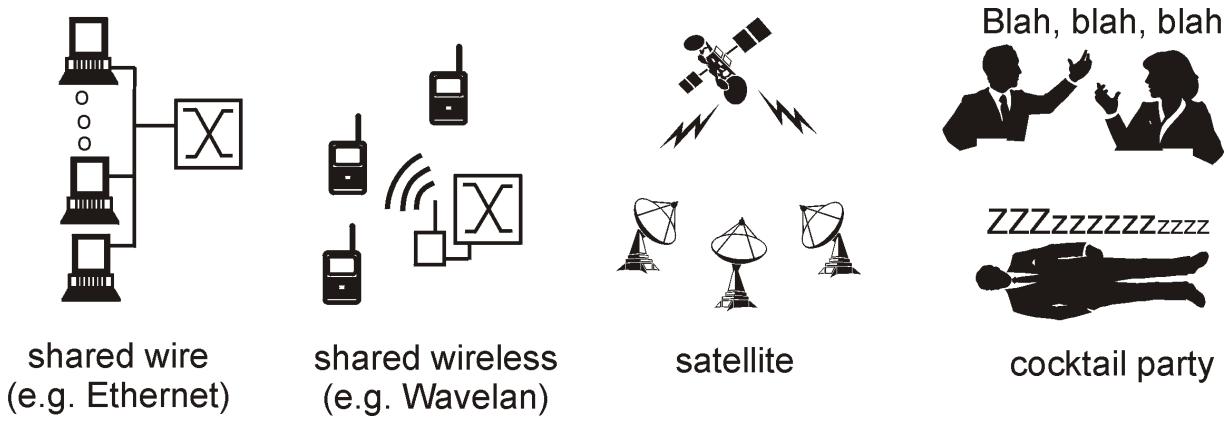


RING

MAC Layer

Kênh truyền đa truy cập (Multiple Access Links)

- Có 3 loại đường truyền:
  - Point – to – point (single wire, e.g. PPP, SLIP)
  - Broadcast (shared wire or medium; e.g, Ethernet, Wavelan, etc)

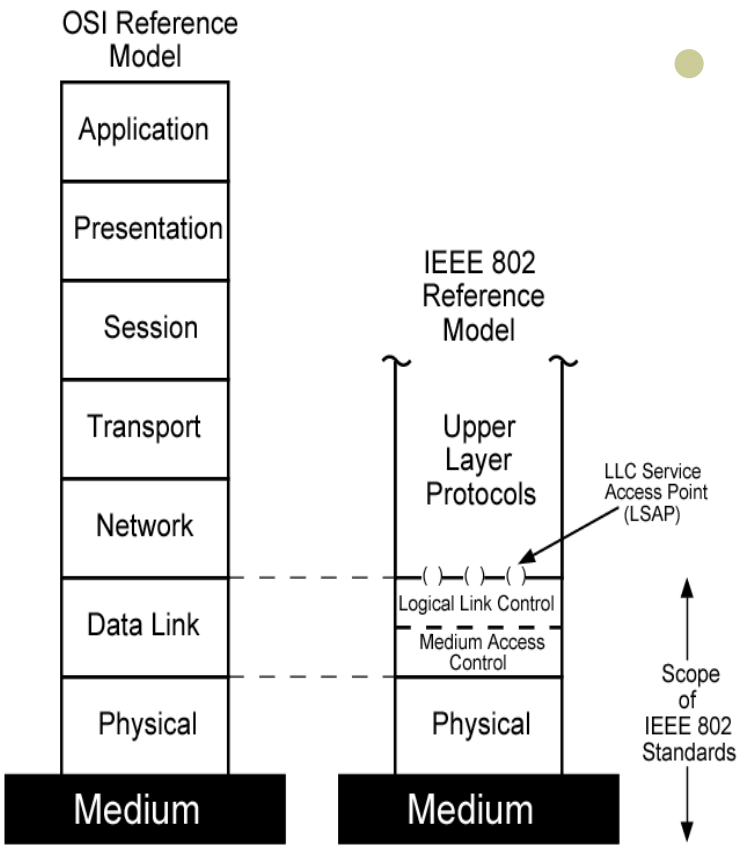


  - Switched (switched Ethernet, ATM)

Giao thức điều khiển truy cập đường truyền (Media Access Control Protocols)

- Vấn đề đa truy cập trong mạng LAN:
  - Một kênh giao tiếp được chia sẻ
  - Hai hay nhiều nút cùng truyền tin đồng thời sẽ dẫn đến giao thoa tín hiệu => tạo ra trạng thái lỗi
    - ➲ Chỉ cho phép một trạm truyền tin thành công tại một thời điểm
    - ➲ Cần có giao thức chia sẻ đường truyền chung giữa các nút trong mạng, gọi là giao thức điều khiển truy cập đường truyền (MAC Protocol)

MAC Protocol trong mô hình OSI



- Tầng liên kết dữ liệu được chia thành hai tầng con:
  - Tầng điều khiển kênh truyền luận lý (Logical Link Control Layer)
  - Tầng điều khiển truy cập đường truyền (Medium Access Control Layer)

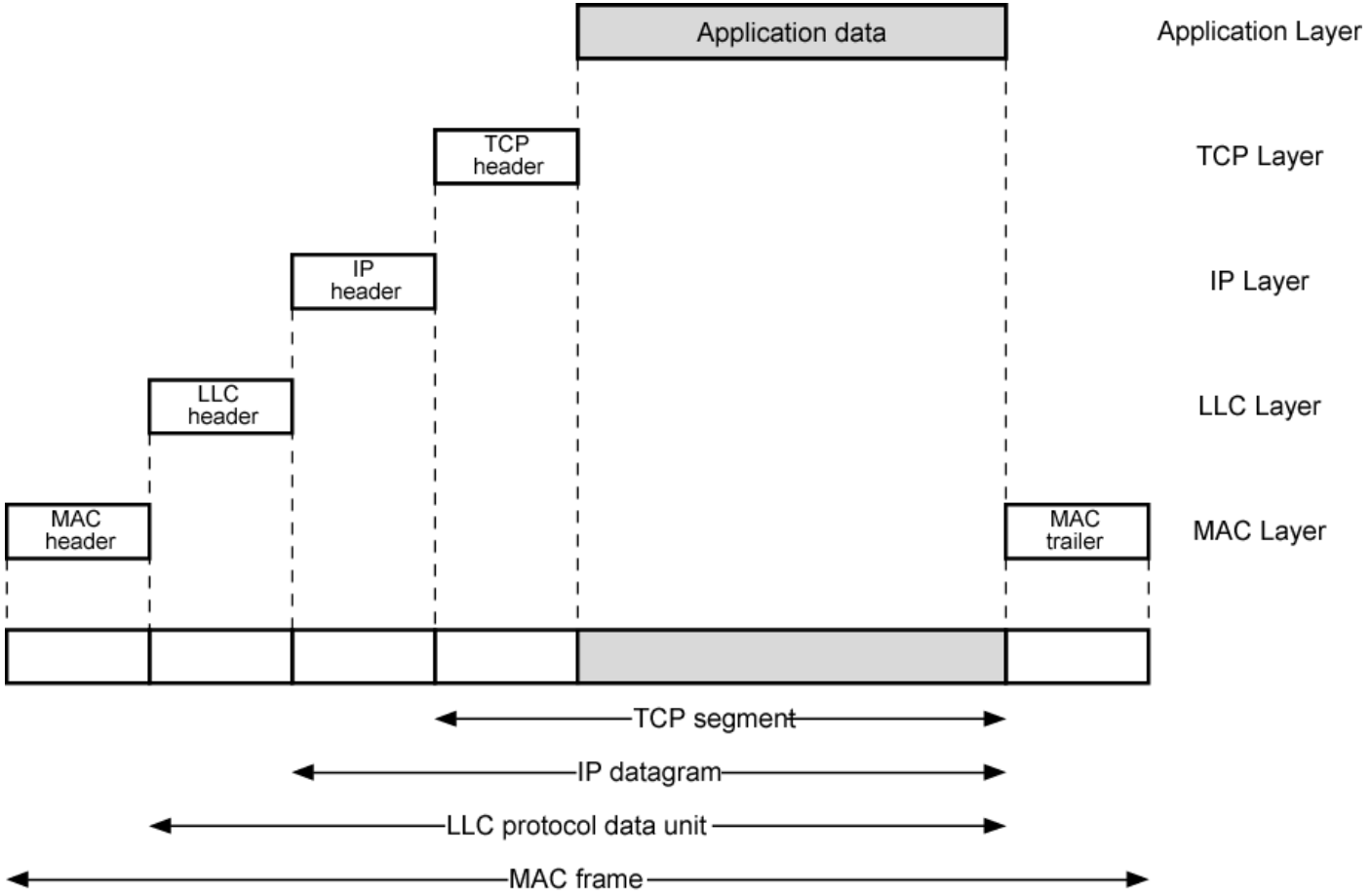
LLC layer

- Giao tiếp với tầng mạng
- Điều khiển lỗi và điều khiển luồng
- Dựa trên giao thức HDLC
- Cung cấp các loại dịch vụ:
  - Unacknowledged connectionless service
  - Connection mode service
  - Acknowledged connectionless service

MAC layer

- Tập hợp dữ liệu thành khung cùng với trường địa chỉ nhận/gởi, chuỗi kiểm tra khung
- Phân tách dữ liệu khung nhận được với trường địa chỉ và thực hiện kiểm tra lỗi
- Điều khiển việc truy cập đường truyền
  - Việc điều khiển này không có trong tầng liên kết dữ liệu truyền thống
- Cùng một tầng LLC có thể có nhiều tùy chọn cho tầng MAC

Các giao thức mạng LAN trong ngữ cảnh chung



Giao thức điều khiển truy cập đường truyền

- Phương pháp chia kênh (Channel Partitioning)
  - Phân chia kênh truyền thành nhiều phần nhỏ (time slots, frequency, code)
  - Cấp phát những phần nhỏ này cho các nút sử dụng một cách loại trừ nhau
- Phương pháp truy cập ngẫu nhiên (Random Access)
  - Cho phép đụng độ
  - Phục hồi lại từ đụng độ
- Phương pháp phân lượt (Taking turns)
  - Hợp tác chặt chẽ trong việc truy cập kênh truyền được chia sẻ để tránh đụng độ

Phương pháp chia kênh

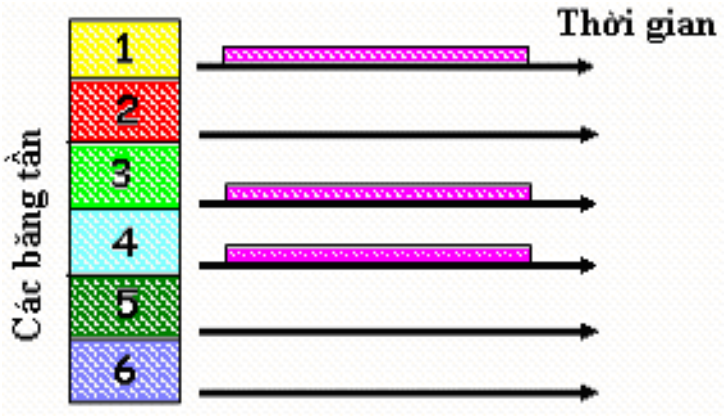
- Đường truyền sẽ được chia thành nhiều kênh truyền
- Mỗi kênh truyền sẽ được cấp phát riêng cho một trạm.
- Có ba phương pháp chia kênh chính:
  - FDMA (Frequency Division Multiple Access)
  - TDMA (Time Division Multiple Access)
  - CDMA (Code Division Multiple Access)

Phương pháp 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).

Phương pháp chia tần số FDMA

- 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.



Phương pháp chia tần số FDMA

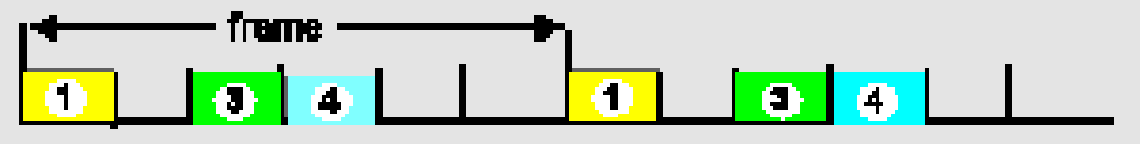
- Ưu điểm:
  - Không có sự đụng độ xảy ra.
  - Hiệu quả trong hệ thống có số lượng người dùng nhỏ và ổn định, mỗi người dùng cần giao tiếp
- Nhược điểm:
  - Lãng phí nếu ít người sử dụng hơn số phần đã chia
  - Người dùng bị từ chối nếu số lượng vượt quá số phần đã chia
  - Không tận dụng được kênh truyền một cách tối đa

Phương pháp chia thời gian (TDMA)

- Các trạm sẽ xoay vòng (round) để truy cập đường truyền.
- Qui tắc xoay vòng:
  - 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).

Phương pháp chia thời gian (TDMA)

- Ví dụ:
  - Các trạm 1, 3, 4 có dữ liệu cần truyền.
  - Các trạm 2, 5, 6 nhàn rỗi.
- Nếu người dùng không sử dụng khe thời gian được cấp để truyền dữ liệu thì thời gian sẽ bị lãng phí



Phân chia mã (CDMA)

- 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 chỉ ra rằng nhiều tín hiệu đồng 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 …).

Phân chia mã (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
- Nhiều người dùng đều chia sẻ chung một băng tần,
- 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.

Phân chia mã (CDMA)

- Ví dụ:
  - Cho dãy chip: (11110011).
    - Để gởi bit **1**, người dùng sẽ gởi đi dãy chip của mình: 11110011
    - Để gởi đi bit **0**, người dùng sẽ gởi đi phần bù của dãy chip của mình: 00001100

Phân chia mã (CDMA)

- Sử dụng ký hiệu lưỡng cực :
  - bit 0 được ký hiệu là -1,
  - bit 1 được ký hiệu là +1.
- Tích trong (inner product) 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:

$$S \bullet T = \frac{1}{m} \sum_{i=1}^{m} S_i T_i$$

- Ví dụ:

$$S = +1+1+1-1-1+1+1-1$$

$$T = +1+1+1+1-1-1+1-1$$

$$S \bullet T = \frac{+1+1+1+(-1)+1+(-1)+1+1}{8} = \frac{1}{2}$$

Phân chia mã (CDMA)

- Hai mã S và T có cùng chiều dài m bits được gọi là trực giao khi: S•T = 0.
- Ví dụ:

$$S = +1+1-1-1-1-1-1+1$$

$$T = -1-1+1-1-1-1+1+1$$

$$S \bullet T = \frac{(-1)+(-1)+(-1)+1+1+1+(-1)+1}{8} = 0$$

- 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

Phân chia mã (CDMA)

- Mã hóa và giải mã tín hiệu:
  - 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
  - *Tín hiệu được mã của người dùng i:*
    - Zi = Di x Ci
  - *Tín hiệu tổng hợp được gởi trên đường truyền:*

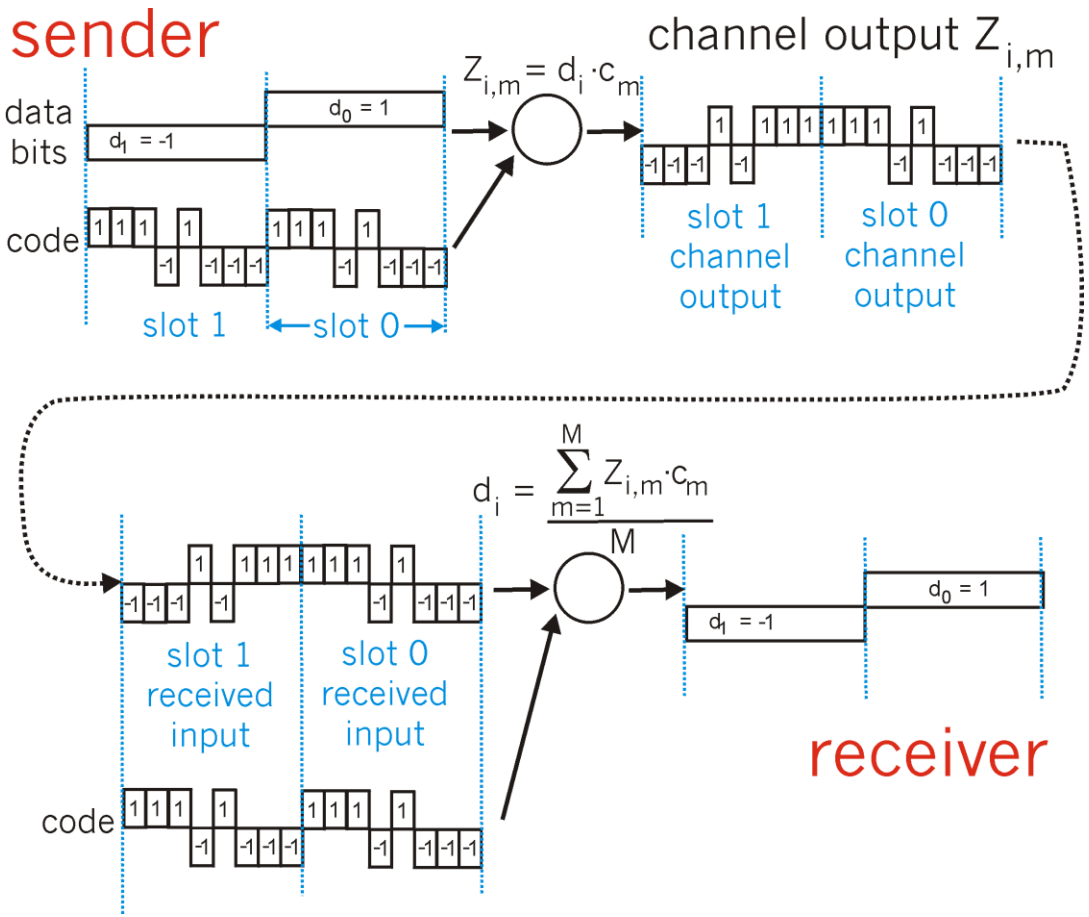
$$Z = \sum_{i=1}^{n} Z_i$$

    - 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:

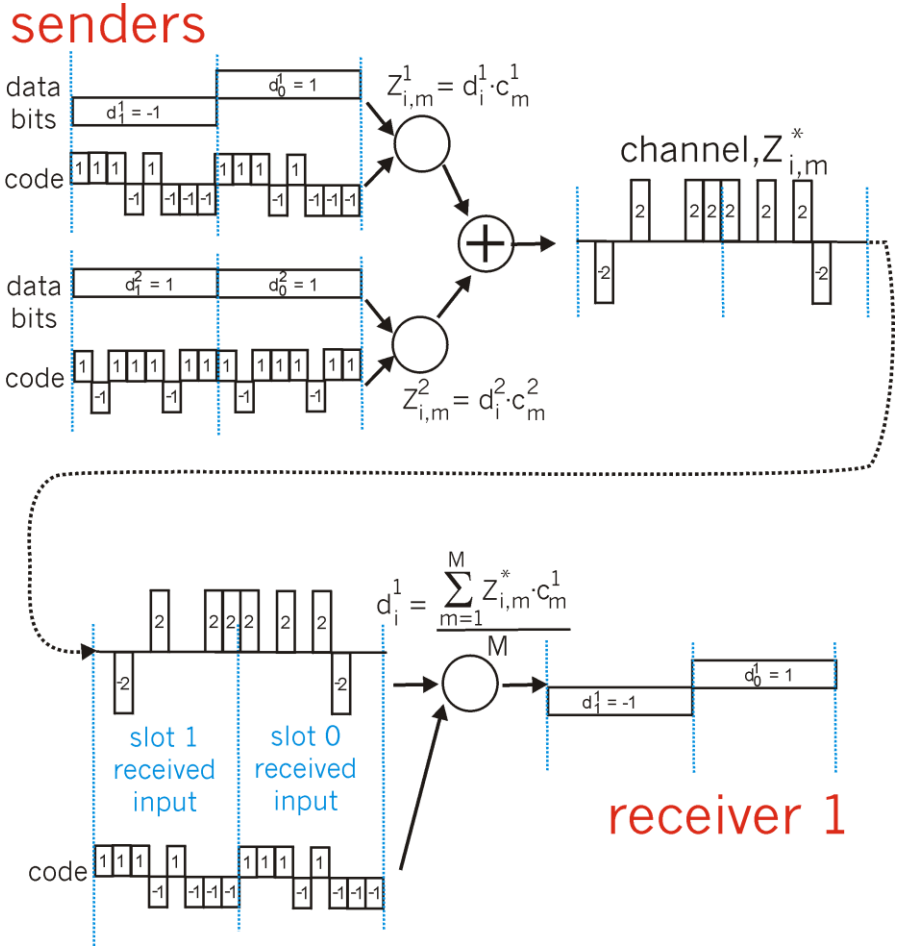
$$D_i = Z \bullet C_i$$

    - Nếu Di > "ngưỡng", coi nó là 1, ngược lại coi nó là -1

Phân chia mã (CDMA)



Phân chia mã (CDMA)



Phân chia mã (CDMA)

- Hệ thống có 4 người dùng A, B, C, D. Các mã số tương ứng của họ như sau:

  A: 0 0 0 1 1 0 1 1
  B: 0 0 1 0 1 1 1 0
  C: 0 1 0 1 1 1 0 0
  D: 0 1 0 0 0 0 1 0

- Nếu ký hiệu theo kiểu lưỡng cực thì:

  A: (–1 –1 –1 +1 +1 –1 +1 +1)
  B: (–1 –1 +1 –1 +1 +1 +1 –1)
  C: (–1 +1 –1 +1 +1 +1 –1 –1)
  D: (–1 +1 –1 –1 –1 –1 +1 –1)

- Để ý các mã số A, B, C, D là trực giao!

Phân chia mã (CDMA)

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

1) – – 1 –	C	Z = (–1 +1 –1 +1 +1 +1 –1 –1)
2) – 1 1 –	B + C	Z = (–2 0 0 0 +2 +2 0 –2)
3) 1 0 – –	A + $\overline{B}$	Z = (0 0 –2 +2 0 –2 0 +2)
4) 1 0 1 –	A + $\overline{B}$ + C	Z = (–1 +1 –3 +3 +1 –1 –1 +1)
5) 1 1 1 1	A + B + C + D	Z = (–4 0 –2 0 +2 0 +2 –2)
6) 1 1 0 1	A + B + $\overline{C}$ + D	Z = (–2 –2 0 –2 0 –2 +4 0)

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 :

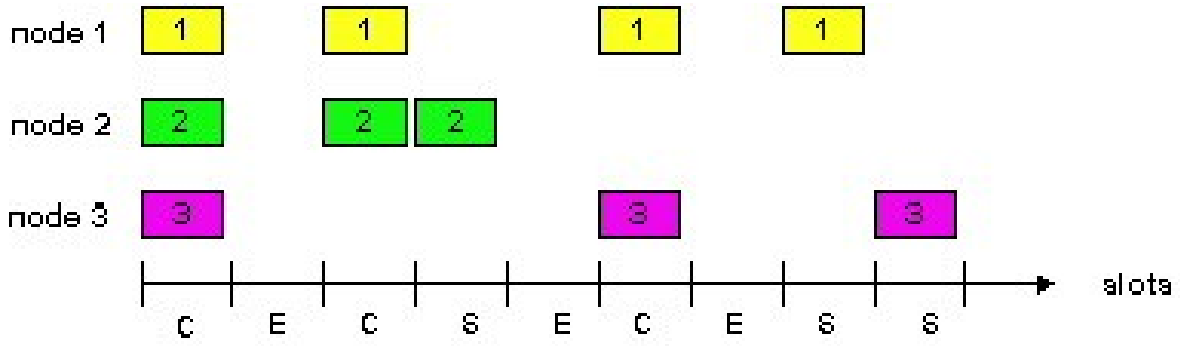
1) $Z \bullet C = (1 +1 +1 +1 +1 +1 +1 +1)/8 = 1$
2) $Z \bullet C = (2 +0 +0 +0 +2 +2 +0 +2)/8 = 1$
3) $Z \bullet C = (0 +0 +2 +2 +0 -2 +0 -2)/8 = 0$
4) $Z \bullet C = (1 +1 +3 +3 +1 -1 +1 -1)/8 = 1$
5) $Z \bullet C = (4 +0 +2 +0 +2 +0 -2 +2)/8 = 1$
6) $Z \bullet C = (2 -2 +0 -2 +0 -2 -4 +0)/8 = -1$

Phương pháp truy cập đường truyền ngẫu nhiên (Random Access)

- Nếu một trạm cần gởi một khung,
  - Nó sẽ gởi khung đó trên toàn bộ dãy thông của kênh truyền.
  - 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 xác định:
  - Cách để phát hiện đụng độ.
  - Cách để phục hồi sau đụng độ.
- Ví dụ về các giao thức truy cập ngẫu nhiên:
  - Slotted ALOHA
  - Pure ALOHA,
  - CSMA và CSMA/CD

Slotted Aloha

- Thời gian được chia thành nhiều khe (slot) bằng nhau (bằng thời gian truyền một khung)
- Một nút có khung cần truyền sẽ truyền khung vào lúc bắt đầu của khe kế tiếp
- Nếu đụng độ: truyền lại khung ở các khe thời gian tiếp theo với xác suất là p cho đến khi thành công.



Success (S), Collision (C), Empty (E) slots

Hiệu suất của giải thuật Slotted Aloha

Câu hỏi: Tỷ lệ các khe thời gian truyền thành công cực đại là bao nhiêu?

Trả lời: Giả sử có N trạm có khung cần gởi

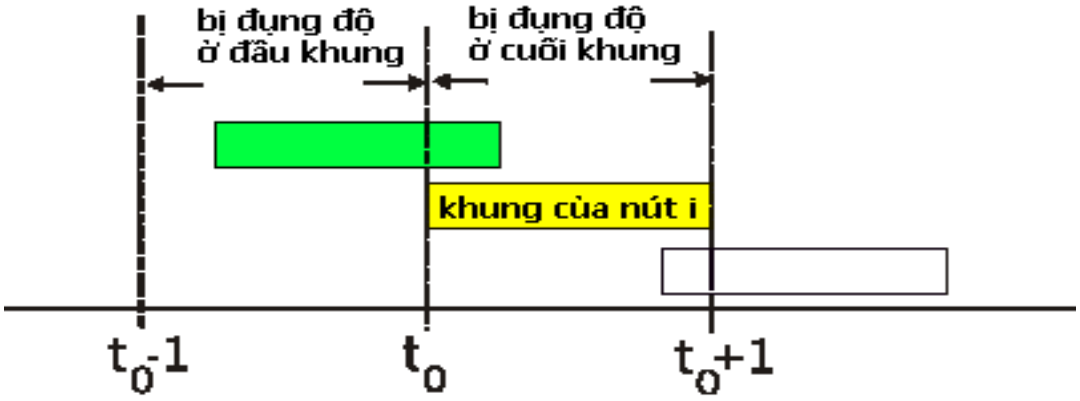
- Mỗi trạm trong khe thời gian của mình với xác suất *p*
- Khả năng truyền thành công của một trạm là *S* :

$$S = Np(1-p)^{(N-1)}$$

Khi $p = 1/N$, S(p) đạt giá trị cực đại : $(1-1/N)^{N-1}$

Pure (unslotted) ALOHA

- Đơn giản, không đồng bộ hóa
- Khi muốn truyền khung:
  - Gởi ngay không chờ đến đầu của khe thời gian
- Tỷ lệ đụng độ tăng lên
  - Khung gởi ở thời điểm t_0 sẽ đụng độ với các khung gởi trong khoản $[t_0-1, t_0+1]$



Pure (unslotted) ALOHA

- Gọi P là xác suất 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 [t0-1,t0]) * 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) = $Np(1-p)^{N-1}(1-p)^{N-1}$

CSMA: Carrier Sense Multiple Access)

- Lắng nghe kênh truyền:
  - Nếu thấy kênh truyền rỗi thì bắt đầu truyền khung
  - Nếu thấy đường truyền bận thì trì hoãn lại việc gởi khung.
    - Non-persistent CSMA: Nếu đường truyền bận, đợi trong một khoảng thời gian ngẫu nhiên rồi tiếp tục nghe lại đường truyền.
    - Persistent CSMA: Nếu đường truyền bận, tiếp tục nghe đến khi đường truyền rỗi rồi thì truyền gói tin với xác suất bằng 1.
    - 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

CSMA collisions

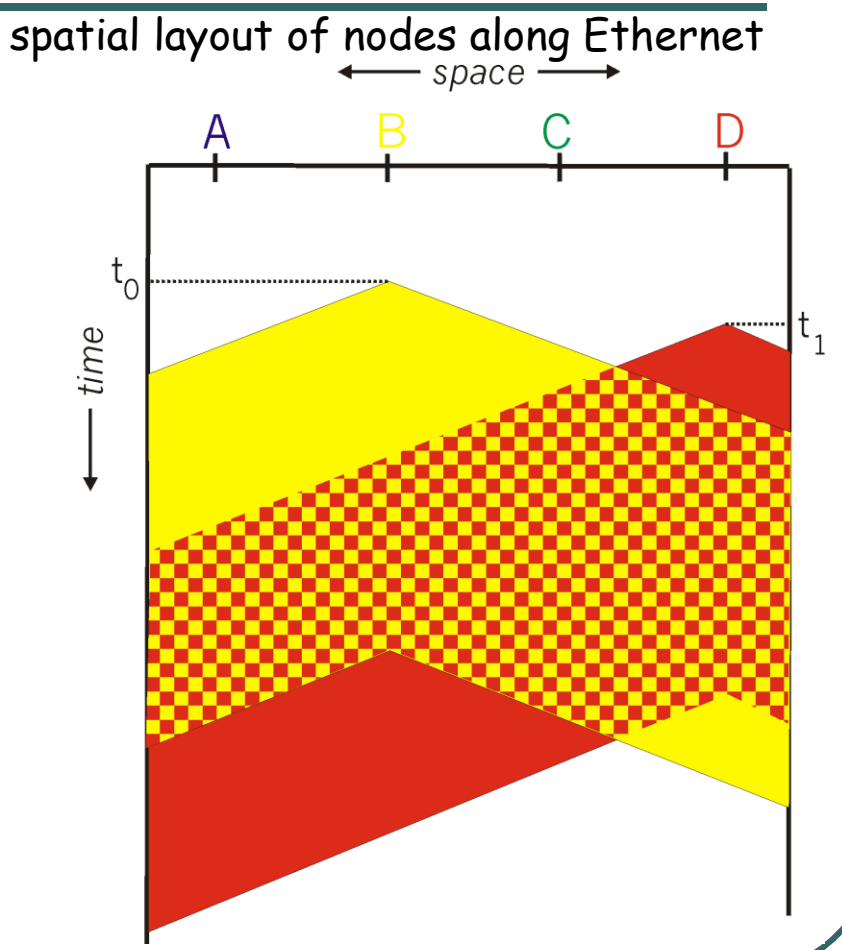
Đụng độ vẫn có thể xảy ra do sự trì hõan trong lan truyền tín hiệu: hai nút không nghe thấy sự truyền tải của nhau

Khi đụng độ:

Toàn bộ khung bị bỏ đi

Lưu ý:

Vai trò của khoảng cách và sự trì hoãn trong lan truyền sẽ xác định tỷ lệ đụng độ

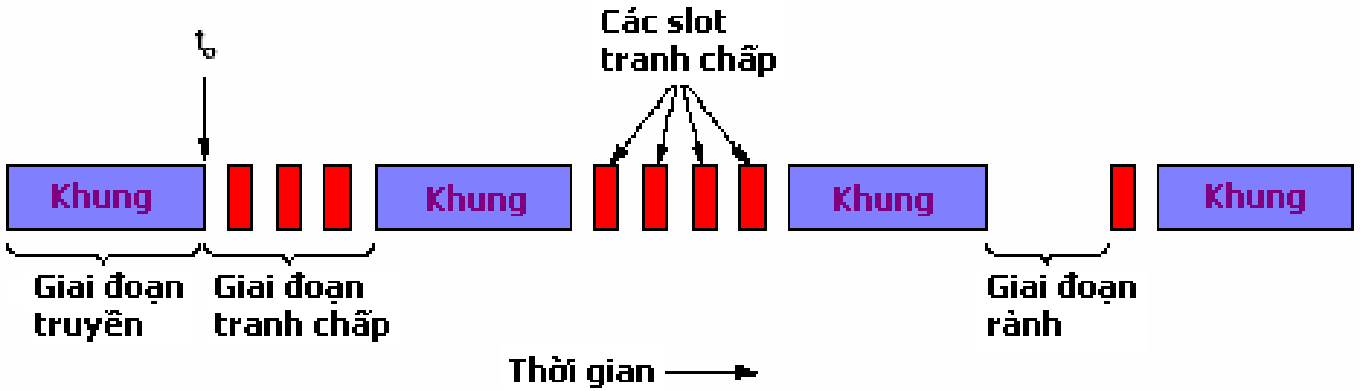


CSMA/CD (Collision Detection)

- Giống như CSMA: Lắng nghe trước khi truyền.
- Có hai cải tiến quan trọng là:
  - Phát hiện đụng độ
  - Làm lại sau đụng độ.

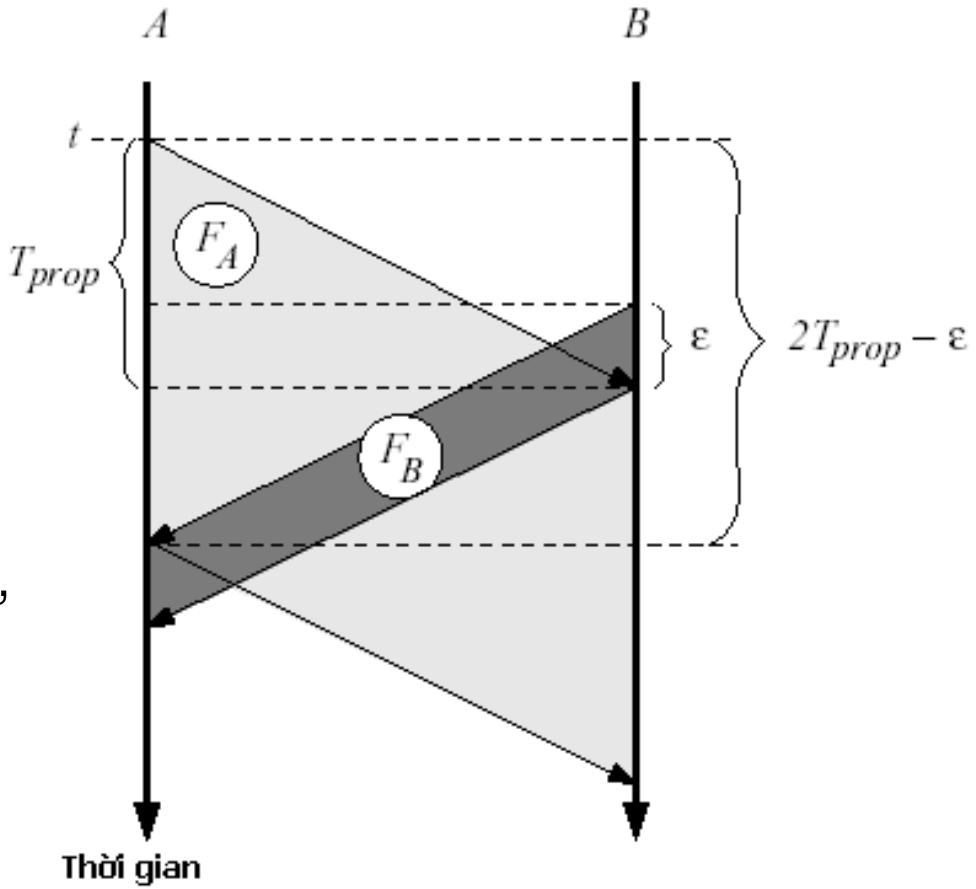
Phát hiện đụng độ

- 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 và bắt đầu làm lại sau đụng độ.



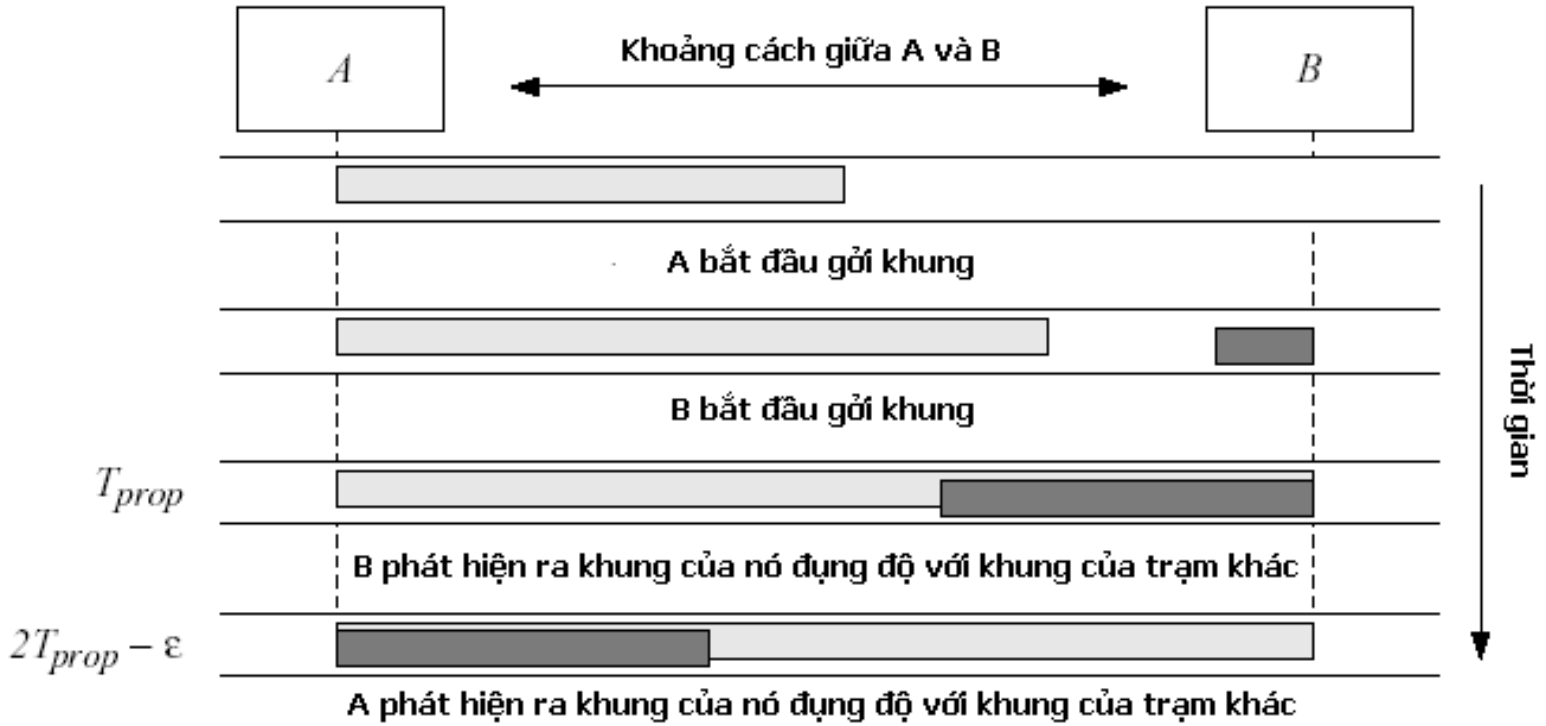
Thời gian truyền khung

- 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.

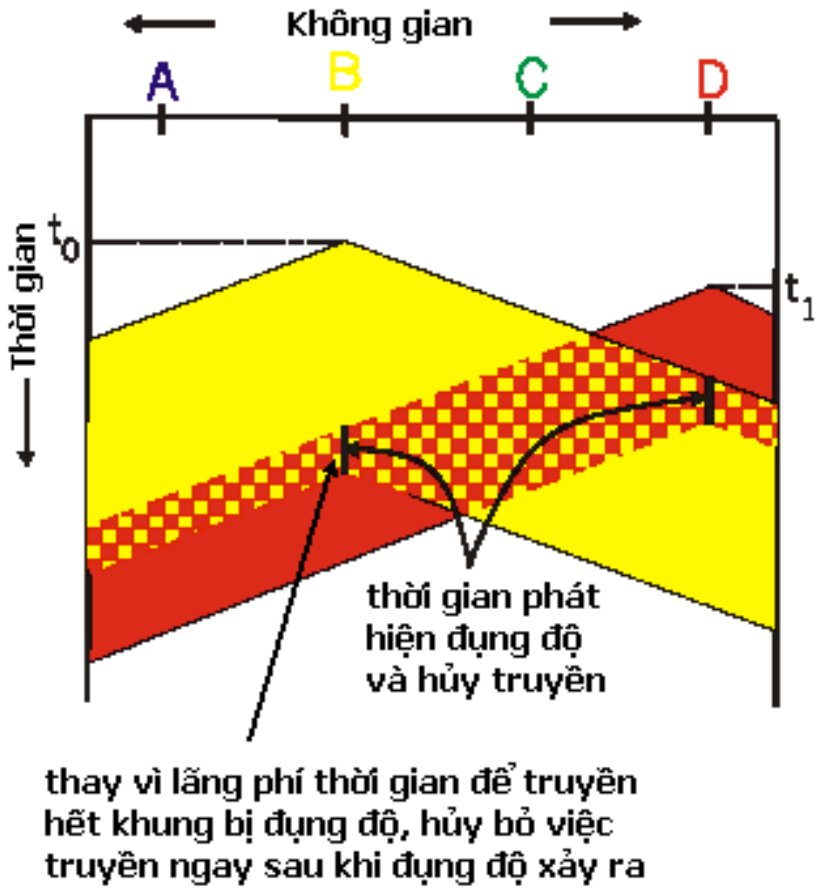


Thời gian truyền khung

- Tw = 2Tprop



Thời điểm hủy bỏ khung khi đụng độ



Làm lại sau khi đụng độ

- Sau khi bị đụng độ, trạm sẽ chạy thuật toán back-off:
  - 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 thoả: $0 \le M \le 2^k$
    - $k = \min(n, 10)$
    - 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 : M*Tw.
  - Khi mà n đạt đến giá trị 16 thì hủy bỏ việc truyền khung.

Phương pháp phân lượt truy cập đường truyền

Giới thiệu phương pháp phân lượt truy cập đường truyền

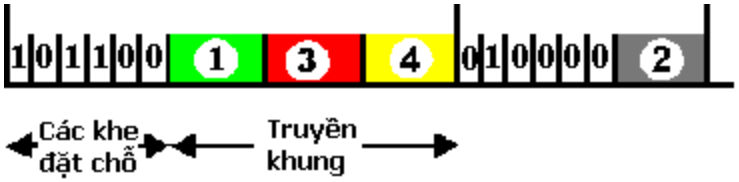
- Các giao thức dạng chia kênh:
  - Kênh truyền được phân chia một cách hiệu quả và công bằng khi tải trọng đường truyền là lớn.
  - Không hiệu quả khi tải trọng của đường truyền là nhỏ
- Các giao thức dạng truy cập ngẫu nhiên:
  - Hoạt động hiệu quả khi tải trọng của đường truyền thấp
  - Khi tải trọng đường truyền cao thì phải tốn nhiều chi phí cho việc xử lý đụng độ.
- Các giao thức dạng "phân lượt":
  - Để ý đến việc tận dụng những mặt mạnh của hai dạng nói trên.
  - Ý tưởng chính là không để cho đụng độ xảy ra bằng cách cho các trạm truy cập đường truyền một cách tuần tự.

Giới thiệu phương pháp phân lượt truy cập đường truyền

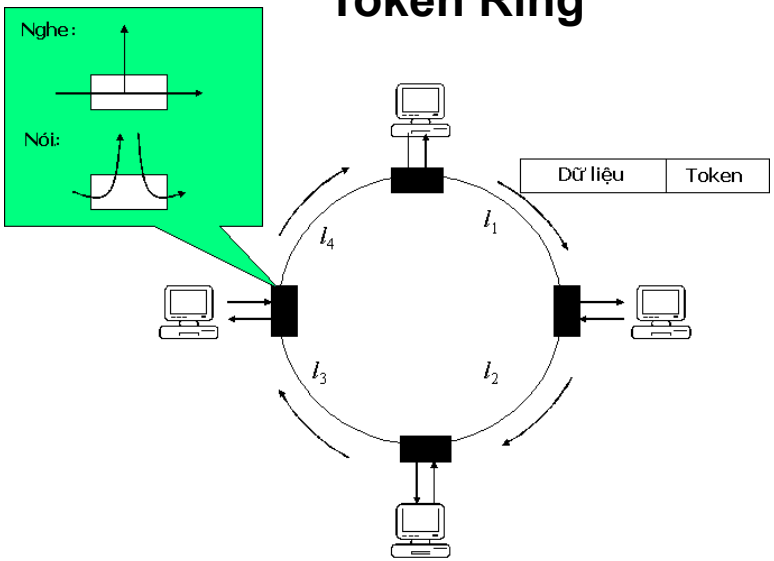
- **Thăm dò (polling)**:
  - Trạm chủ (master) sẽ mời các trạm tớ (slave) truyền khi đến lượt. Trạm chủ dành phần cho trạm tớ hoặc trạm tớ yêu cầu và được trạm chủ đáp ứng.
  - Vấn đề cần quan tâm: chi phí cho việc thăm dò, độ trễ do phải chờ được phân lượt truyền, hệ thống rối loạn khi trạm chủ gặp sự cố.
- **Chuyển 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 chuyển thẻ bài qua trạm kế tiếp.
  - 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.

Ví dụ về phương pháp phân lượt đường truyền

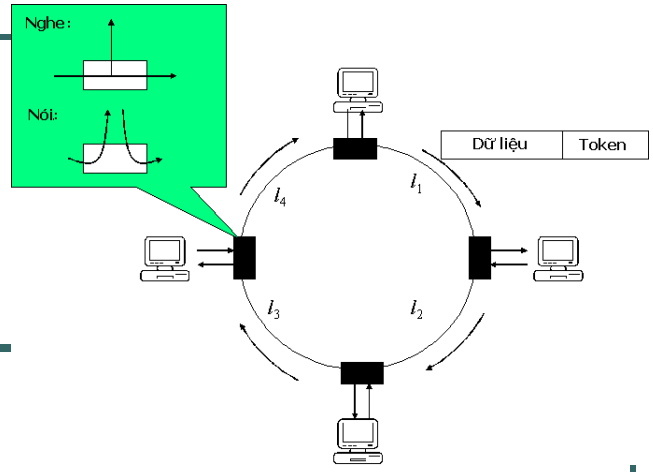
Thăm dò phân tán (Distributed Polling)



Token Ring

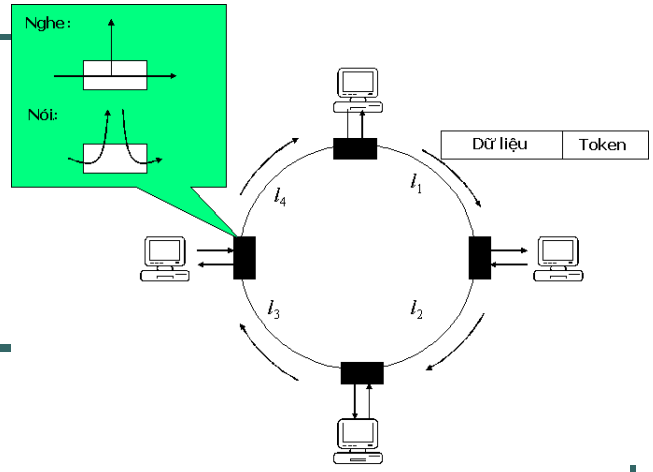


Token Ring



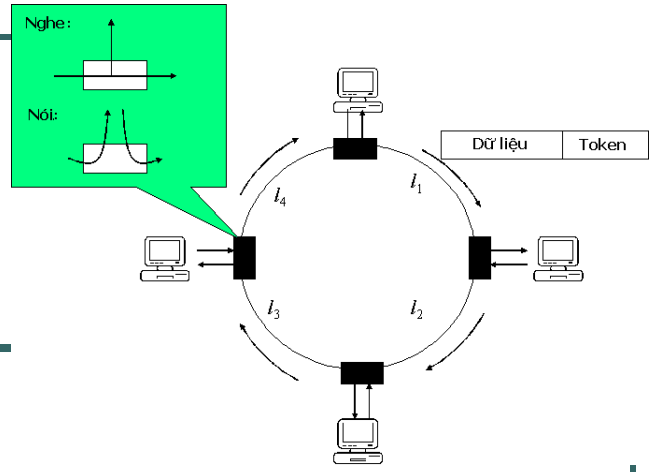
- Cách thức hoạt động:
  - Tồn tại một thẻ bài duy nhất trong mạng: là một dãy bit.
  - Thẻ bài sẽ chạy vòng quanh vòng
  - Mỗi nút sẽ nhận thẻ bài rồi lại chuyển tiếp thẻ bài này đi.
  - Khi một trạm có khung cần truyền và đúng lúc nó thấy có thẻ bài tới, nó liền lấy thẻ bài này ra khỏi vòng và sẽ truyền 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.

Token Ring

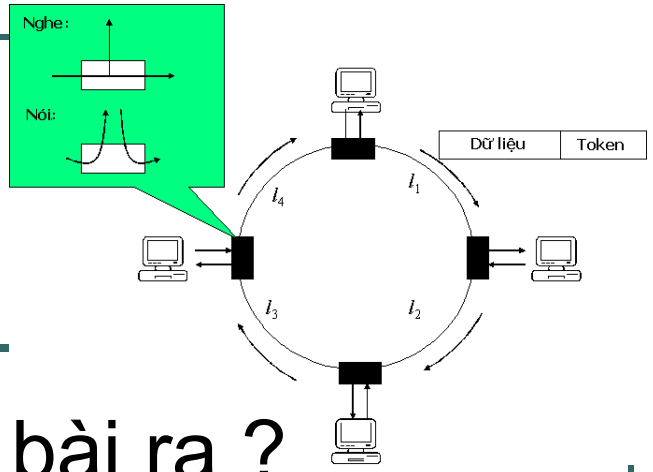


- Card mạng gồm: một bộ nhận, một bộ phát và một bộ đệm dùng chứa dữ liệu.
- Khi không có trạm nào trong vòng có dữ liệu để truyền, thẻ bài sẽ lưu chuyển vòng quanh. Nếu một trạm có dữ liệu cần truyền và có thẻ bài, nó có quyền truyền một hoặc nhiều khung dữ liệu tùy theo qui định của hệ thống.
- Khung thông tin chạy qua mỗi trạm trong vòng, trạm này sẽ nhìn vào địa chỉ đích trong khung 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 - không được xóa khung ra khỏi vòng.

Token Ring

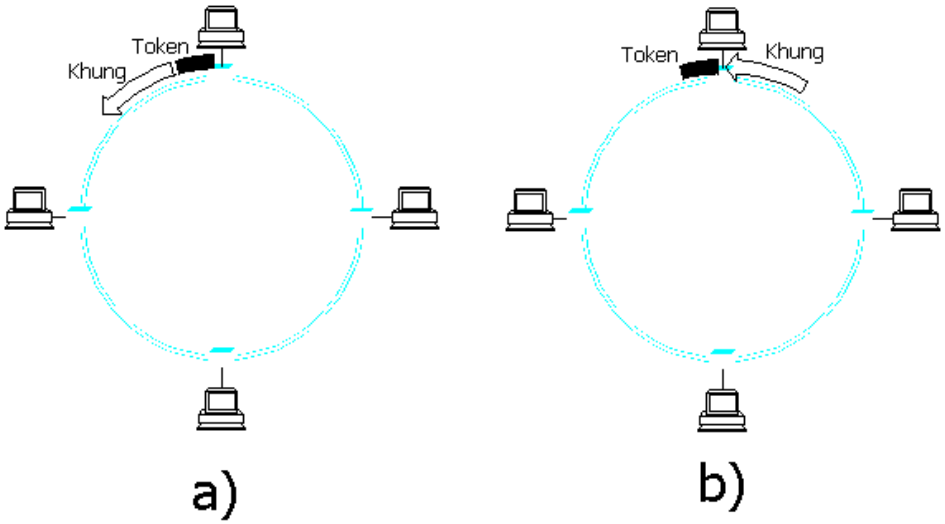


- Thời gian giữ thẻ bài (Token Holding Time)
- Thời gian xoay vòng của thẻ bài(Token rotation time)
- TRT ≤ Số nút hoạt động × THT
  + Độ trễ của vòng
  - Độ trễ của vòng: là tổng thời gian để thẻ bài đi hết một vòng khi trong vòng không có trạm nào cần truyền dữ liệu,
  - Số nút hoạt động: ám chỉ số trạm có dữ liệu cần truyền.



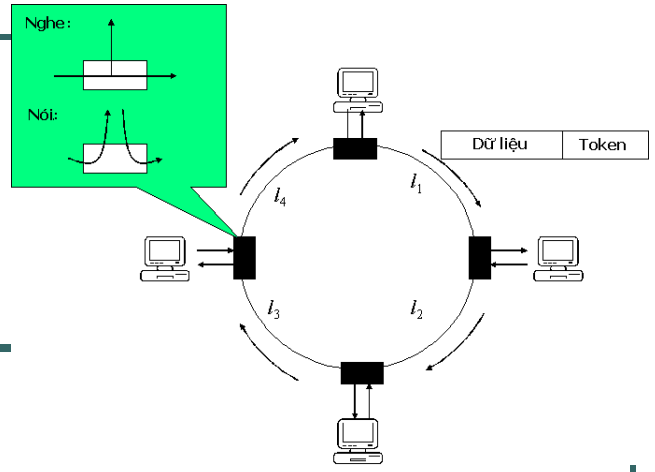
Token Ring

- Khi nào thì trạm sẽ nhả thẻ bài ra ?

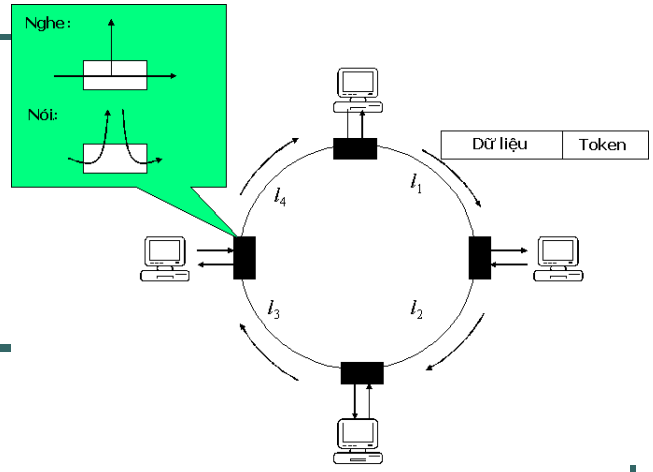


a) Nhả thẻ bài ra ngay sau khi trạm vừa truyền khung xong (RAT).
b) Nhả thẻ bài ra ngay sau khi trạm nhận lại khung vừa phát ra (RAR).

Token Ring

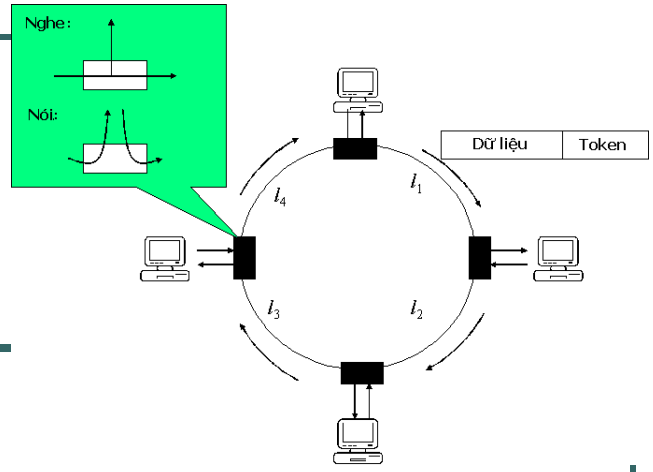


- Quản lý hoạt động của mạng:
  - Đề cử ra một trạm làm nhiệm vụ quản lý mạng token ring gọi là monitor.
  - Monitor đảm bảo hoạt động cho toàn bộ vòng.
  - Bất kỳ trạm nào cũng có thể trở thành monitor.
  - Thủ tục bầu chọn monitor diễn ra khi vòng vừa được tạo ra hoặc khi monitor của vòng bị sự cố.
  - Một monitor 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



Token Ring

- Quản lý hoạt động của mạng:
  - 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.
  - 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”.

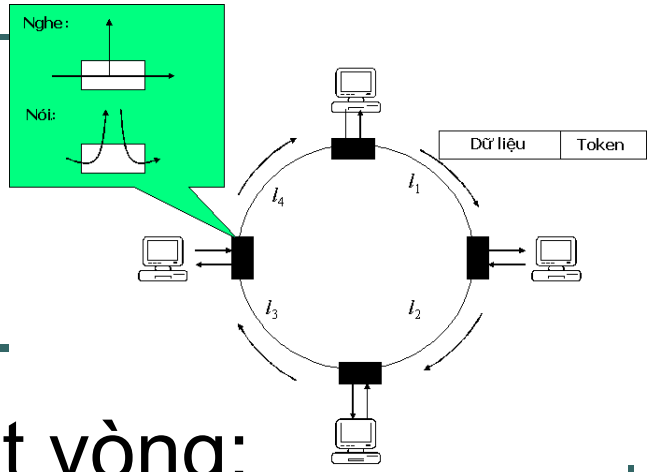


Token Ring

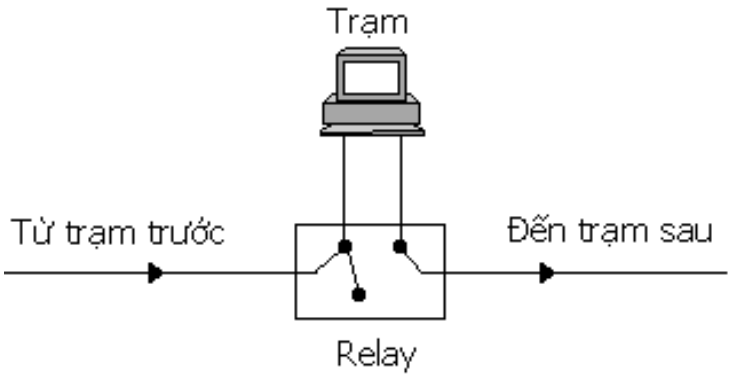
- Nhiệm vụ của monitor:
  - Phải đảm bảo rằng luôn luôn có sự hiện diện của thẻ bài ở đâu đó trên vòng,
  - Khi thẻ bài chạy ngang qua monitor, nó sẽ bật một bộ đếm thời gian để tính giờ. Bộ đếm này có giá trị tối đa là:

    Số lượng trạm $\times$ THT + Độ trễ của vòng
  - Monitor cũng phải kiểm tra xem có khung nào bị hỏng hoặc vô thừa nhận hay không.

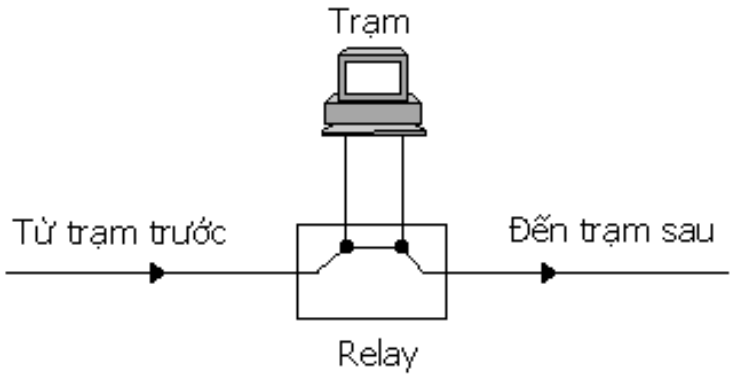
Token Ring



- Sử dụng relay để chống đứt vòng:



(a) Relay mở

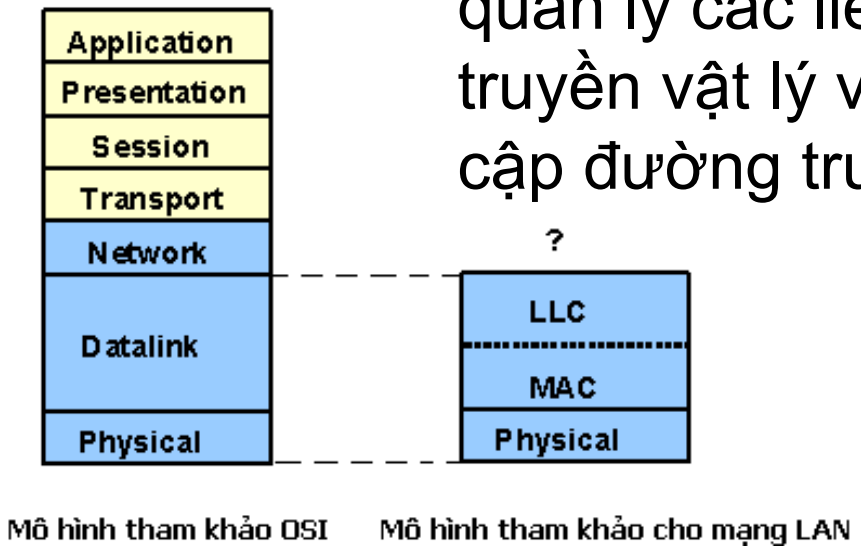


(b) Relay đóng

Một số chuẩn mạng cục bộ

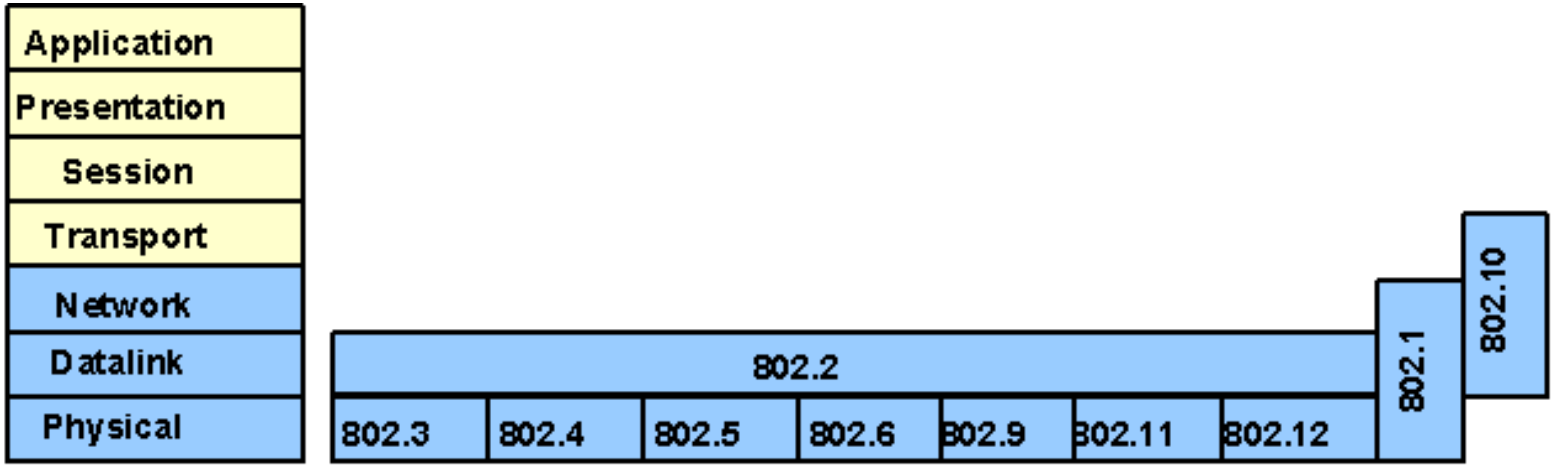
Chuẩn hóa mạng cục bộ

- MAC quản lý việc truy cập đường truyền
- 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.



Chuẩn hóa mạng cục bộ

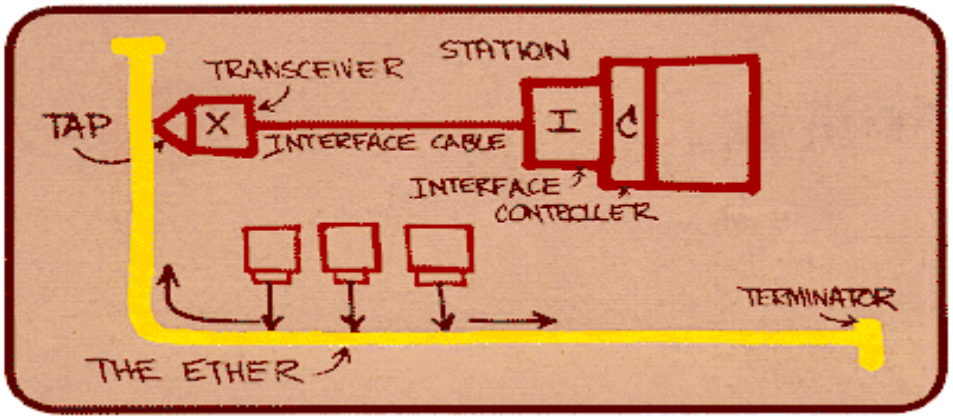
- IEEE (Institute of Electrical and Electronic Engineers)
  - Tổ chức đi tiên phong trong lĩnh vực chuẩn hóa mạng cục bộ
  - Dự án IEEE 802 định nghĩa hàng loạt chuẩn thuộc họ IEEE 802.x



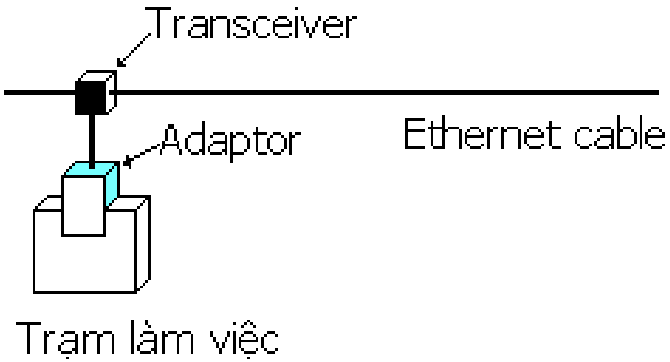
Chuẩn hóa mạng cục bộ IEEE 802.x

- IEEE 802.1 : High Level Interface
- IEEE 802.2 : Logical Link Control (LLC)
- IEEE 802.3: CSMA/CD
- 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

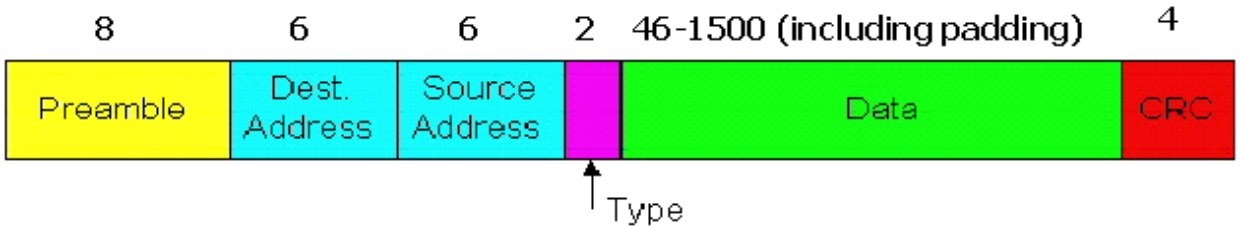
Chuẩn mạng Ethernet (802.3)



Bức phác họa Ethernet của Bob Metcalfe, người sáng lập ra Ethernet (Xerox PARC - 1972)



Chuẩn mạng Ethernet (802.3)

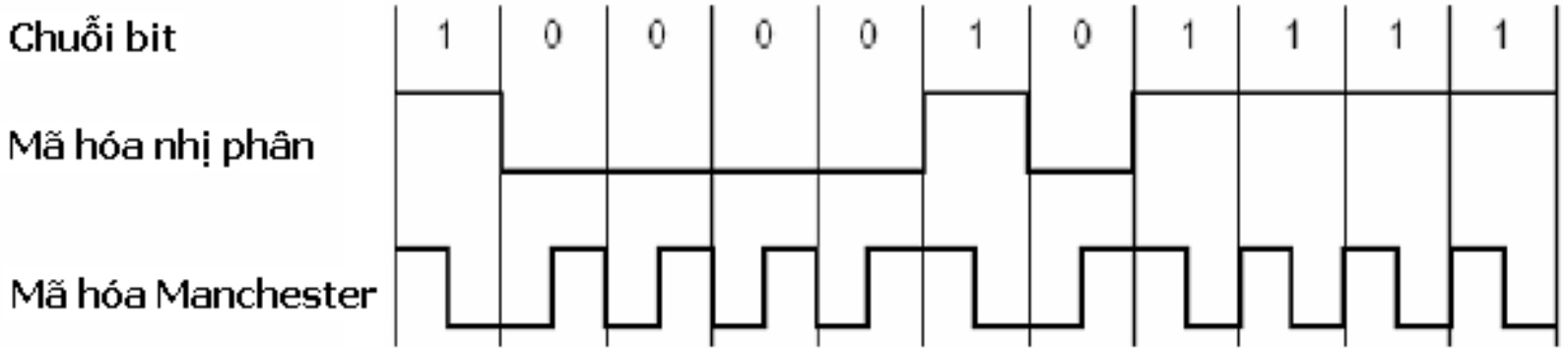


- Preamble: dài 7 bytes với mẫu 10101010 theo sau bởi 1 byte với mẫu 10101011, được sử dụng để đồng bộ hóa tốc độ đồng hồ giữa bên gởi và bên nhận.
- Source and dest. addresses: Địa chỉ nguồn và đích, gồm 6 bytes. Khung được nhận bởi tất cả các trạm trong LAN. Khung bị xóa nếu dest. address không trùng với địa chỉ MAC của bất kỳ trạm nào hoặc không phải thuộc dạng multicast.

  8:0:2b:e4:b1:2
  00001000 00000000 00101011 11100100 10110001 00000010
- 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.

Chuẩn mạng Ethernet (802.3)

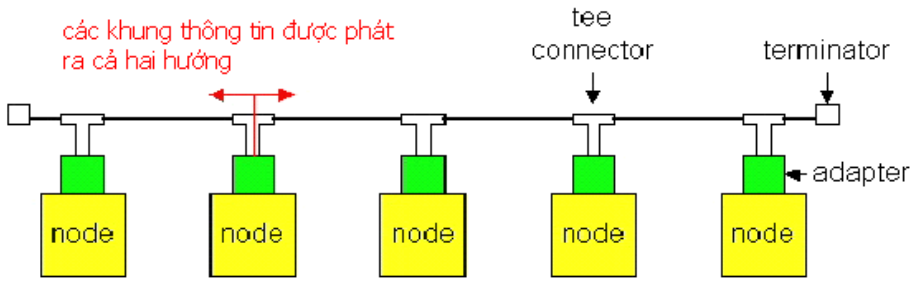
Sử dụng phương pháp mã hóa đường truyền Manchester



Chuẩn mạng Ethernet (802.3)

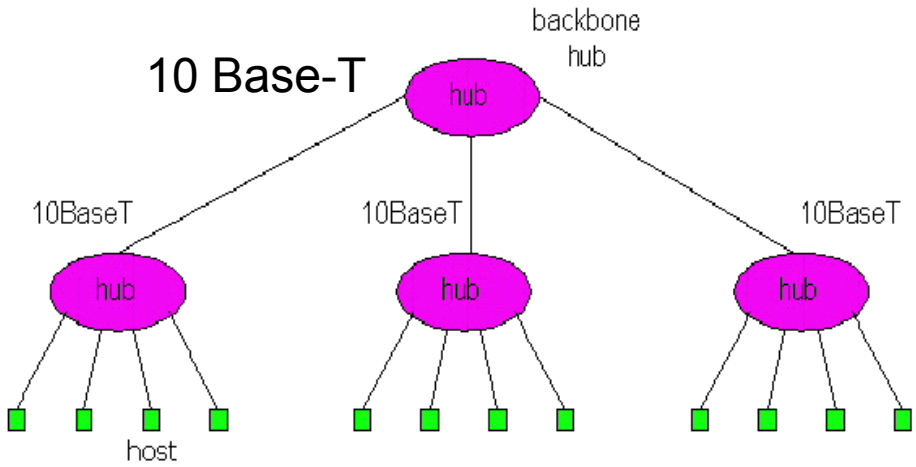
- MAC Protocol: CSMA/CD+Exponential backoff
- Nhận một gói tin từ tầng cao hơn;
  - K := 0; n :=0; // K: thời gian chờ đợi ngẫu nhiên; n: số vụ đụng độ đã gặp phải
  - repeat:
  - chờ trong khoảng thời gian K*512 bit-time;
  - while (đường truyền bận) wait;
  - chờ tiếp 96 bit-time sau khi nhận thấy 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;
  - }

Chuẩn mạng Ethernet (802.3)



10 Base-2

10 Base-T



100 Base-T

Tầng mạng
(Network Layer)

Trình bày: Ngô Bá Hùng
Khoa CNTT&TT
Đại Học Cần Thơ

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 học 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

Yêu cầu

- Sau khi học xong chương này, người đọc phải có được những khả năng sau:
  - 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

Một số hạn chế của tầng liên kết dữ liệu

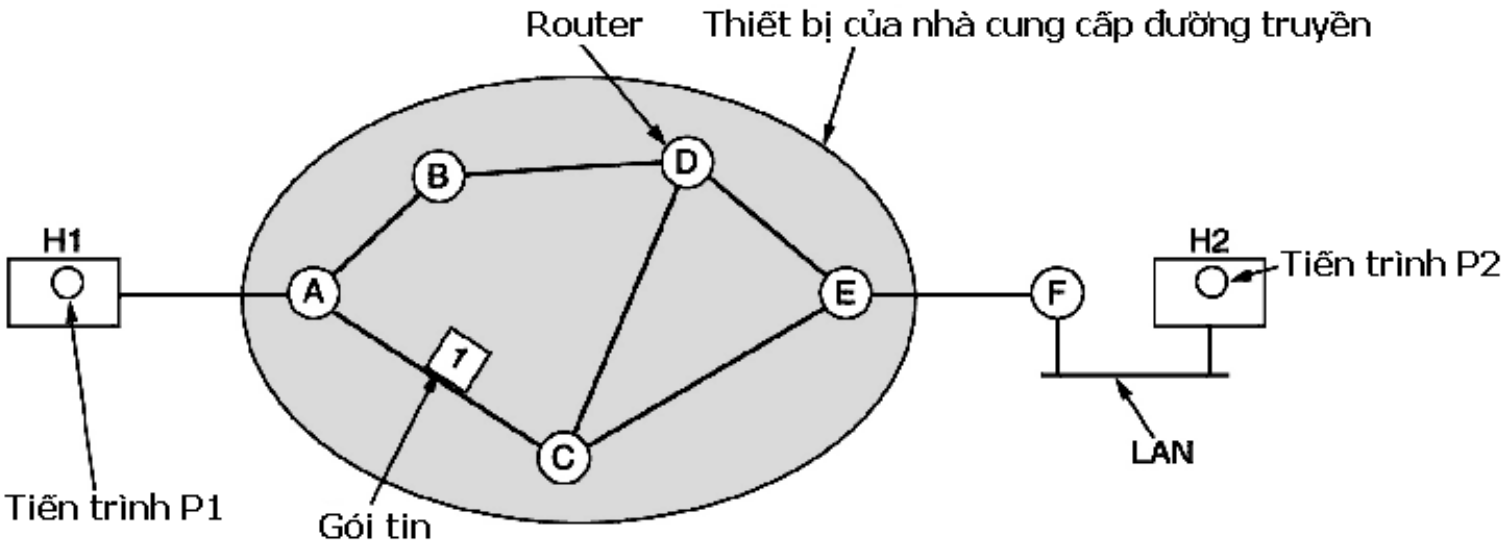
- Chỉ đảm bảo truyền tải thông tin giữa các máy tính có đường truyền trực tiếp
- Bị giới hạn về số lượng máy tính và kích thước mạng
- Khó khăn trong việc nối kết các mạng sử dụng kỹ thuật chia sẻ đường truyền khác nhau – mạng không đồng nhất

Vai trò của tầng mạng

- Cung cấp cho người dùng một dịch vụ nối kết host-host trên một hệ thống mạng diện rộng, không đồng nhất một cách dễ dàng
- Đưa các gói tin từ máy gởi qua các chặn đường để đến được máy nhận
- Chọn đường đi cho gói tin để tránh được tình trạng tắc nghẽn

Các vấn đề liên quan đến việc thiết kế tầng mạng

- Kỹ thuật hoán chuyển lưu và chuyển tiếp (Store-and-Forward Switching)



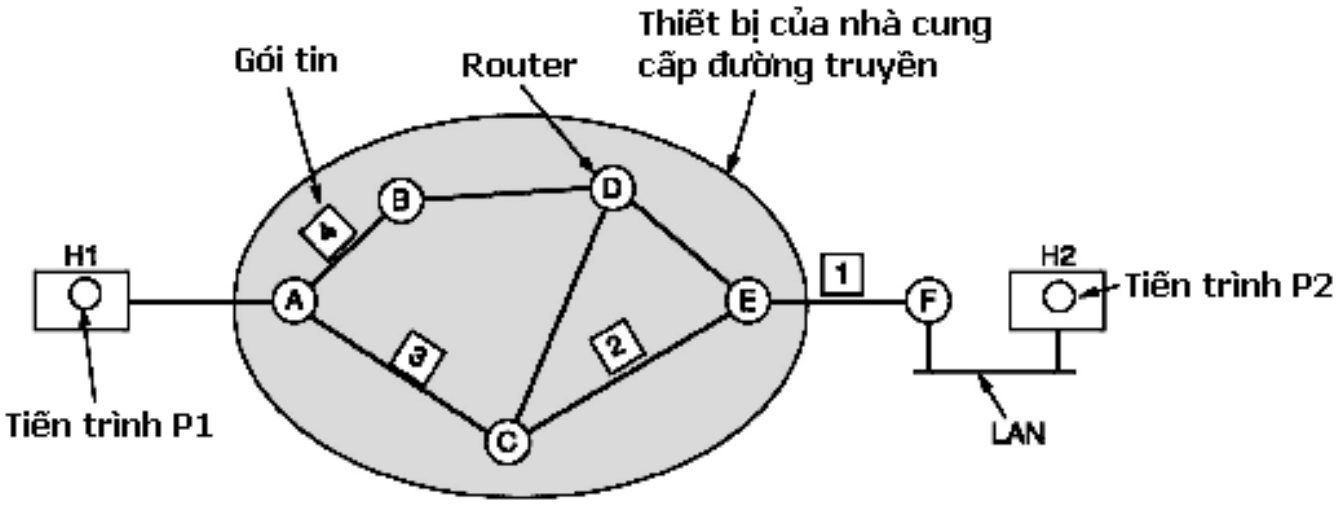
Các vấn đề liên quan đến việc thiết kế tầng mạng

- Các dịch vụ cung cấp cho tầng vận chuyển
  - Mục tiêu thiết kế: Các dịch vụ cần độc lập với kỹ thuật của các router.
    - Tầng vận chuyển cần được độc lập với số lượng, kiểu và hình trạng của các router hiện hành.
    - Địa chỉ mạng cung cấp cho tầng vận chuyển phải có sơ đồ đánh số nhất quán cho dù chúng là LAN hay WAN
  - Hai dịch vụ cơ bản:
    - Dịch vụ không nối kết (Connectionless Service)
    - Dịch vụ định hướng nối kết (Connection – Oriented Service)

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 được gọi là thư tín (Datagram) và subnet được gọi là Datagram Subnet.

Cài đặt dịch vụ không nối kết (Implementation of Connectionless Service)



Bảng vạch đường của nút A

lúc đầu		lúc sau	
A	–	A	–
B	B	B	B
C	C	C	C
D	B	D	B
E	C	E	B
F	C	F	B

Nút C

A	A
B	A
C	–
D	D
E	E
F	E

Nút E

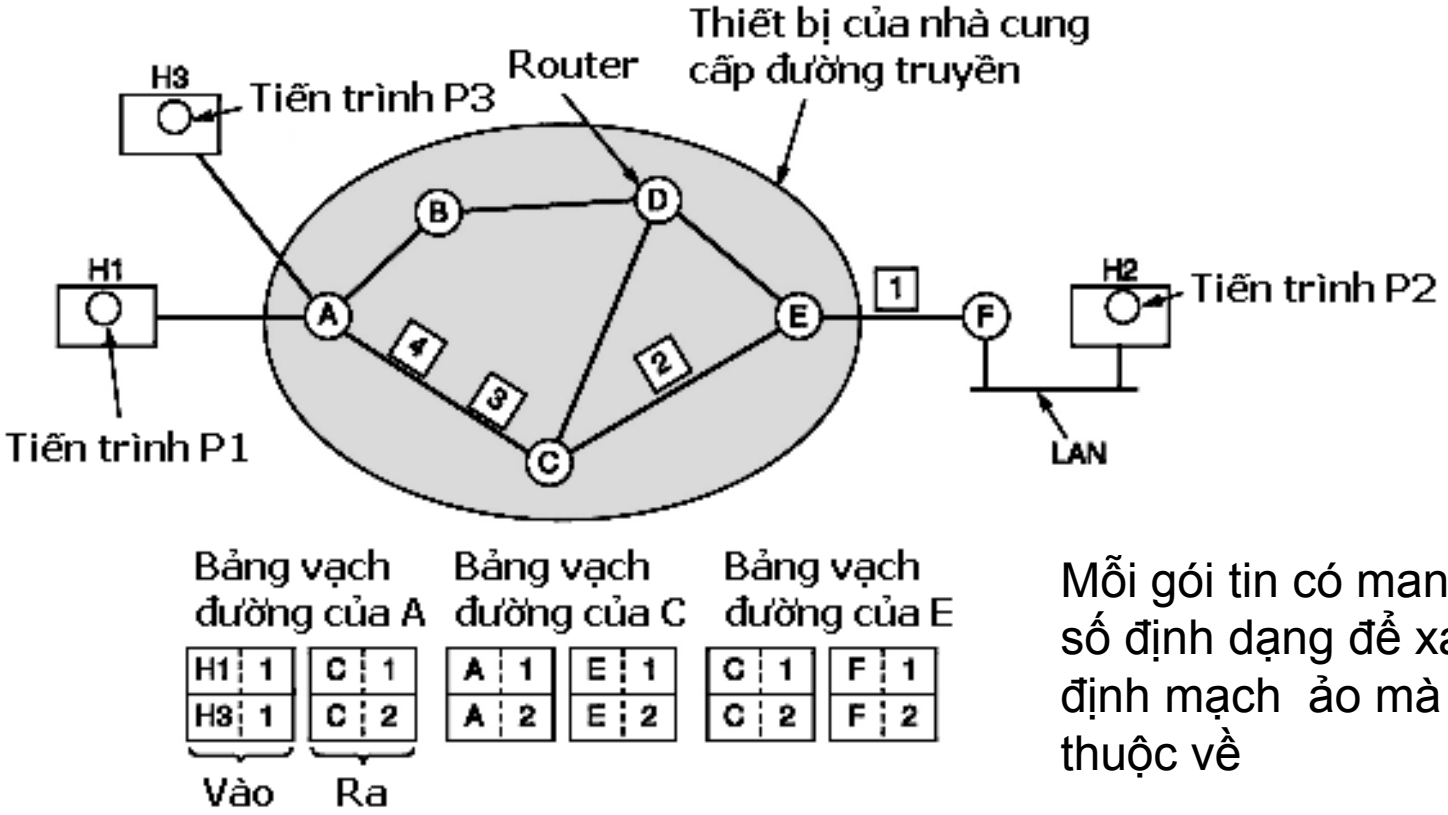
A	C
B	D
C	C
D	D
E	–
F	F

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).

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.

Cài đặt dịch vụ có nối kết (Implementation of Connection Service)



Mỗi gói tin có mang một số định dạng để xác định mạch ảo mà nó thuộc về

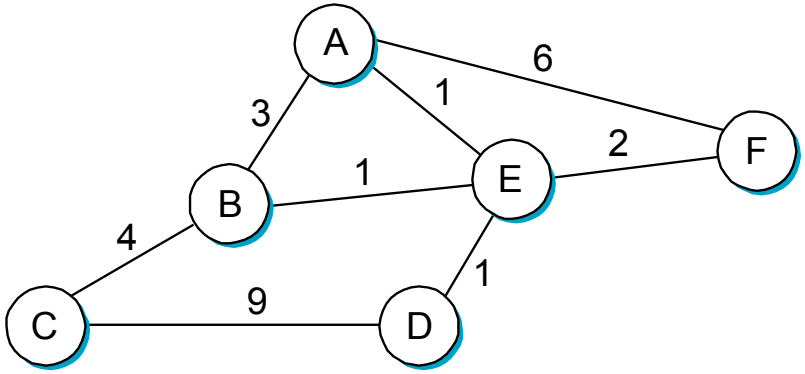
So sánh giữa Datagram subnet và Virtual-Circuit subnet

Vấn đề	Datagram Subnet	Circuit Subnet
Thiết lập nối kết	Không cần	Cần thiết
Đánh địa chỉ	Mỗi gói tin chứa đầy đủ địa chỉ gởi và nhận	Mỗi gói tin chỉ chứa số nhận dạng nối kết có kích thước nhỏ.
Thông tin trạng thái	Router không cần phải lưu giữ thông tin trạng thái của các nối kết	Mỗi nối kết phải được lưu lại trong bảng chọn đường của router.
Chọn đường	Mỗi gói tin có đường đi khác nhau	Đường đi được chọn khi mạch ảo được thiết lập, sau đó tất cả các gói tin đều đi trên đường này.
Ảnh hưởng khi router bị hỏng	Không bị ảnh hưởng, ngoại trừ gói tin đang trên đường truyền bị hỏng	Tất cả các mạch ảo đi qua router bị hỏng đều bị kết thúc
Chất lượng dịch vụ	Khó đảm bảo	Có thể thực hiện dễ dàng nếu có đủ tài nguyên gán trước cho từng nối kết
Điều khiển tắc nghẽn	Khó điều khiển	Có thể thực hiện dễ dàng nếu có đủ tài nguyên gán trước cho từng nối kết

Giải thuật chọn đường

Chọn đường (Routing)

- Mục tiêu: là xác định một đường đi tốt (chuỗi các router) xuyên trên mạng từ máy gởi đến máy nhận thông tin
- Cần đồ thị hóa hệ thống mạng cho các giải thuật chọn đường:
  - Nút là các host, switch, router hoặc là các mạng con.
  - 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



•Chọn đường là tìm ra đường đi có chi phí thấp nhất giữa hai nút bất kỳ

•Chi phí của đường đi là tổng chi phí khi đi qua tất cả các cạnh làm thành đường đi đó.

•Nếu không có một đường đi giữa hai nút; chi phí là vô cùng.

Mục tiêu của giải thuật chọn đường

- Xác định hướng 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

Phân loại giải thuật chọn đường

- 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): 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): Các router không thể tự cập nhật thông tin về đường đi khi hình trạng mạng thay đổi. Thông thường nhà quản trị mạng sẽ là người cập nhật thông tin về đường đi cho router.
- Chọn đường động (Dynamic routing): Các router sẽ tự động cập nhật lại thông tin về đường đi khi hình trạng mạng bị thay đổi.

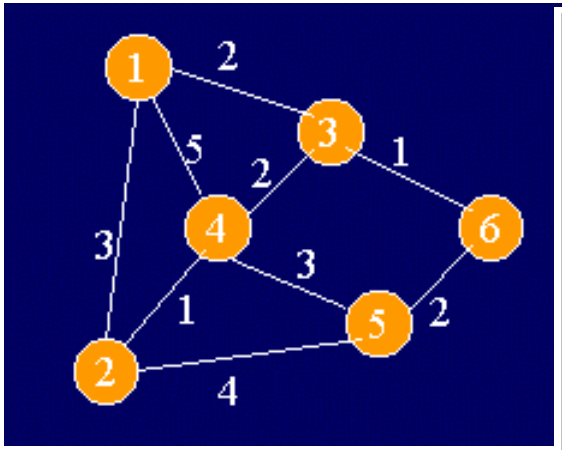
Giải thuật tìm đường đi ngắn nhất Dijkstra

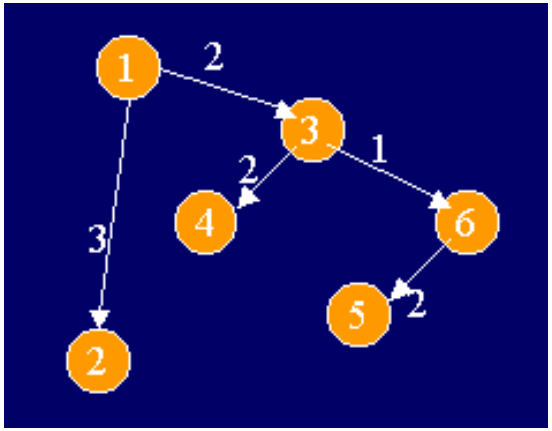
- Mục đích là để tìm đường đi ngắn nhất từ một nút cho trước trên đồ thị đến các nút còn lại trên mạng
- Thuộc loại giải thuật tìm đường đi tối ưu tập trung
- Gọi
  - S: là nút nguồn cho trước
  - N: là tập hợp tất cả các nút đã xác định được đường đi ngắn nhất từ S.
  - Di: là độ dài đường đi ngắn nhất từ nút nguồn S đến nút i.
  - 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.
  - Pj là nút cha của của nút j.

Giải thuật tìm đường đi ngắn nhất Dijkstra

- Bước 1: Khởi tạo
  - N={S}; D_s=0;
  - Với $\forall i \neq S$: $D_i = l_{si}$, P_i=S
- Bước 2: Tìm nút gần nhất kế tiếp
  - Tìm nút **i** $\notin$ N thoả D_i= min (D_j) với j $\notin$ N
  - Thêm nút **i** vào N.
  - Nếu N chứa tất cả các nút của đồ thị thì dừng. Ngược lại sang Bước 3
  - Bước 3: Tính lại giá đường đi nhỏ nhất
    - Với mỗi nút j $\notin$ N: Tính lại D_j= min{ D_j, D_i+ l_{ij}} ; P_j=i;
    - Trở lại Bước 2

Giải thuật tìm đường đi ngắn nhất Dijkstra – ví dụ





Lần lặp	N	D_2	D_3	D_4	D_5	D_6	P_2	P_3	P_4	P_5	P_6
Khởi tạo	{1}	3	2	5	∞	∞	1	1	1	1	1
1	{1,3}	3	**2**	4	∞	3	1	1	3	1	3
2	{1,3,2}	**3**		4	7	3	1		3	2	3
3	{1,3,2,6}			4	5	**3**			3	6	3
4	{1,3,2,6,4}			**4**	5				3	6	
5	{1,3,2,6,4,5}				**5**					6	

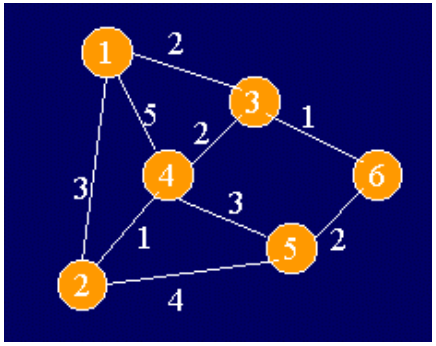
Giải thuật chọn đường tối ưu Ford-Fulkerson

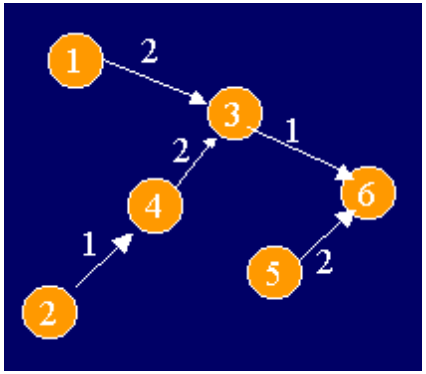
- Mục đích của giải thuật này là để tìm đường đi ngắn nhất từ tất cả các nút đến một nút đích cho trước trên mạng
- Thuộc loại giải thuật tìm đường đi tối ưu – phân tán
- Gọi
  - d là nút đích cho trước
  - D_i là chiều dài đường đi ngắn nhất từ nút i đến nút d.
  - C_i là nút con của nút i

Giải thuật chọn đường tối ưu Ford-Fulkerson

- Bước 1: Khởi tạo:
  - Gán $D_d = 0$;
  - Với $\forall i \neq d$: gán $D_i = \infty$; $C_i = -1$;
- Bước 2: Cập nhật giá đường đi ngắn nhất từ nút i đến nút d
  - $D_i = \min\{ l_{ij} + D_j\}$ với $\forall j \neq i \Rightarrow C_i = j$;
  - Lặp lại cho đến khi không còn D_i nào bị thay đổi giá trị

Giải thuật chọn đường tối ưu Ford-Fulkerson – ví dụ



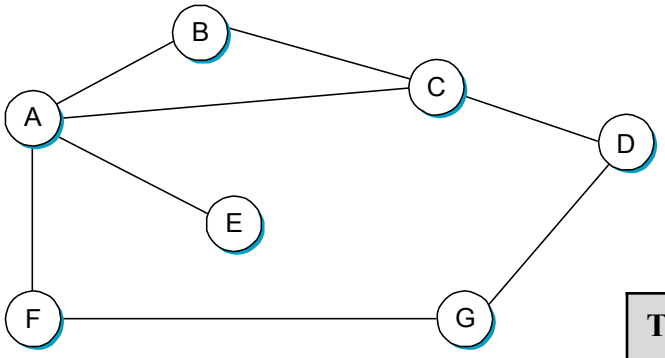


Lần lặp	D_1	D_2	D_3	D_4	D_5	C_1	C_2	C_3	C_4	C_5
Khởi tạo	∞	∞	∞	∞	∞	-1	-1	-1	-1	-1
1	∞	∞	**1**	**3**	**2**	-1	-1	**6**	**3**	**6**
2	**3**	**4**	1	3	2	**3**	**4**	6	3	6
3	3	4	1	3	2	3	4	6	3	6

Giải pháp vạch đường Vector Khoảng cách (Distance Vector)

- 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
  - Mỗi nút phải biết được chi phí của các đường nối từ nó đến tất cả các nút láng giềng
  - Một nối kết bị đứt (down) sẽ được gán cho chi phí có giá trị vô cùng.

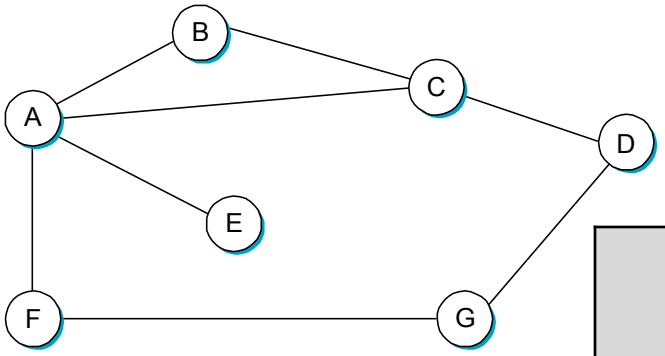
Giải pháp vạch đường Vector Khoảng cách (Distance Vector)



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

Thông tin được lưu tại các nút	Khoảng cách đến nút						
	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

Giải pháp vạch đường Vector Khoảng cách (Distance Vector)



Bảng vạch đường khởi đầu tại nút A

Đích (Destination)	Chi phí (Cost)	Nút kế tiếp (Next Hop)
B	1	B
C	1	C
D	∞	-
E	1	E
F	1	F
G	∞	-

Giải pháp vạch đường Vector Khoảng cách (Distance Vector)

Thông tin được lưu tại các nút	Khoảng cách đến nút						
	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

Mỗi nút sẽ gởi một thông điệp đến các láng giềng liền kề nó, chứa danh sách các khoảng cách mà cá nhân nút tính được

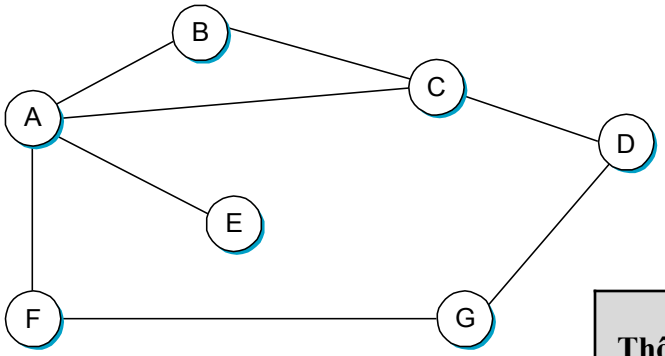
Đích	Chi phí	Nút kế tiếp
B	1	B
C	1	C
D	∞	-
E	1	E
F	1	F
G	∞	-

→

Đích	Chi phí	Nút kế tiếp
B	1	B
C	1	C
D	2	C
E	1	E
F	1	F
G	2	F

Bảng vạch đường tại nút A

Giải pháp vạch đường Vector Khoảng cách (Distance Vector)



Các khoảng cách cuối cùng được lưu tại mỗi nút

Thông tin được lưu tại các nút	Khoảng cách đến nút						
	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	2	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

Giải pháp vạch đường Vector Khoảng cách (Distance Vector)

- Một số vấn đề:
  - Thời điểm gởi thông tin vạch đường của mình cho các nút láng giềng:
    - Cập nhật theo chu kỳ
    - Cập nhật do bị kích hoạt khi có sự thay đổi thông tin trong bảng vạch đường của nút
  - Kiểm tra sự hiện diện của láng giềng
    - Gởi thông điệp hỏi thăm sức khỏe định kỳ
    - Không thấy bảng chọn đường của láng giềng gởi sang
  - Khi phát hiện đường truyền bị sự cố:
    - Router sẽ cập nhật đường đi tương ứng với giá trị vô cùng và gởi bảng chọn đường mới sang láng giềng
  - Vấn đề vòng quẩn

Giải pháp chọn đường "Trạng thái nối kết" (Link State)

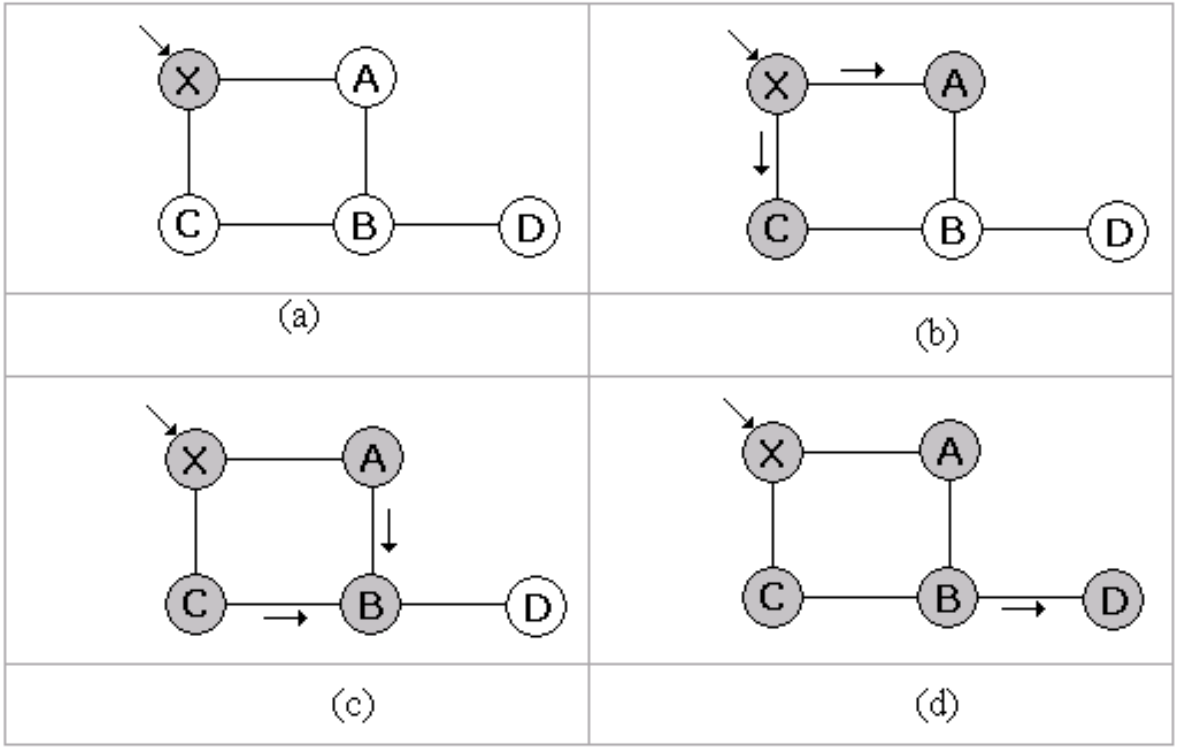
- Mỗi nút được giả định có khả năng tìm ra trạng thái của đường nối nó đến các nút láng giềng và chi phí trên mỗi đường nối đó
- Mọi nút đều biết đường đi đến các nút láng giềng kề bên chúng và nếu chúng ta đảm bảo rằng tổng các kiến thức này được phân phối cho mọi nút thì mỗi nút sẽ có đủ hiểu biết về mạng để dựng lên một bản đồ hoàn chỉnh của mạng
- Mỗi nút sẽ chạy các giải thuật tìm đường đi trên hình trạng của toàn mạng để tìm đường đi

Giải pháp chọn đường "Trạng thái nối kết" (Link State)

- Làm ngập một cách tin cậy (Reliable Flooding)
  - Đảm bảo 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
  - 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
  - Mỗi nút tạo ra gói tin cập nhật, còn được gọi là gói tin trạng thái nối kết (link-state packet – LSP), chứa :
    - 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

Giải pháp chọn đường "Trạng thái nối kết" (Link State)

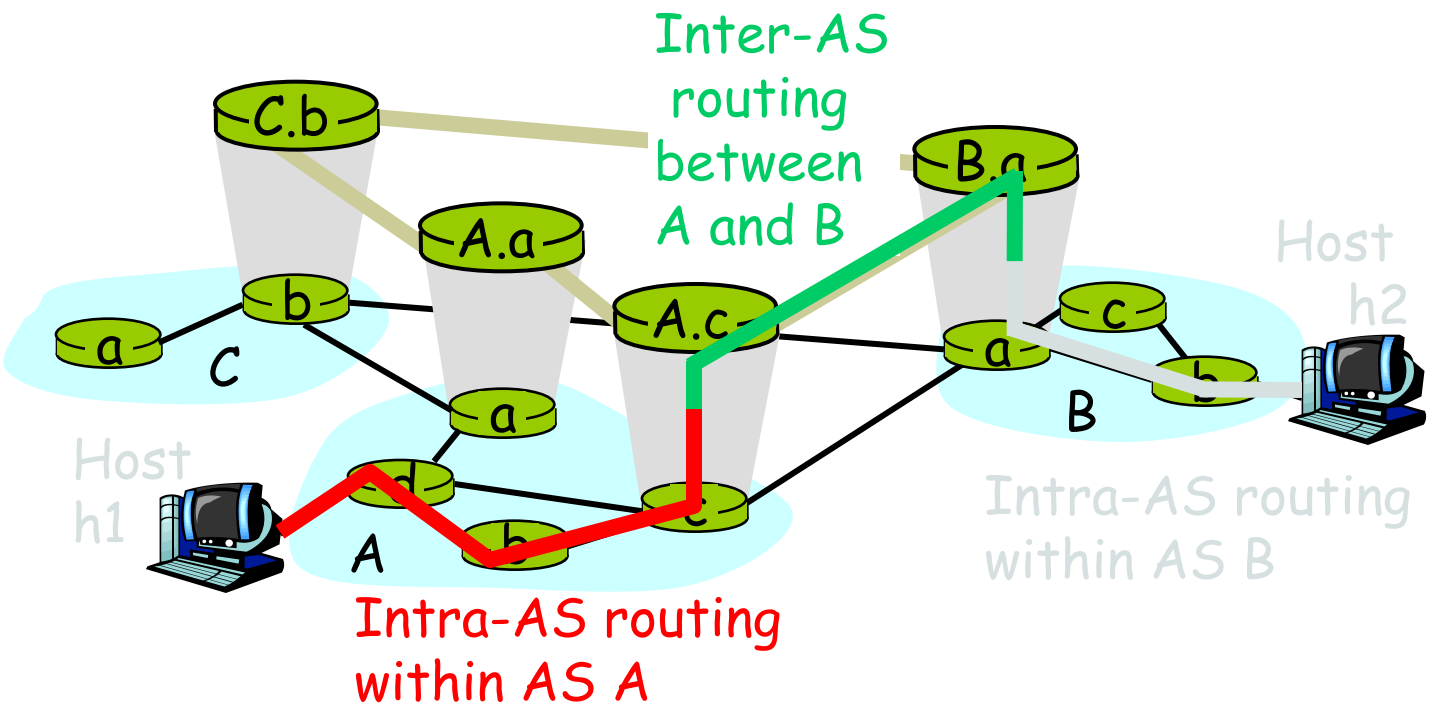
- Làm ngập một cách tin cậy (Reliable Flooding)



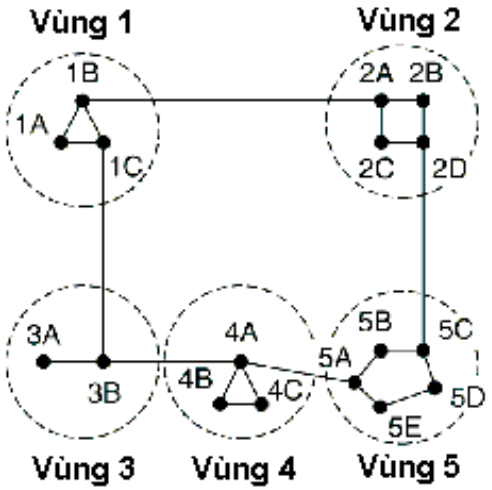
Vạch đường phân cấp (Hierarchical Routing)

- Khi mạng tăng kích thước:
  - Tăng kích thước bảng vạch đường của các router
  - Tăng kích thước bộ nhớ
  - Tăng thời gian tìm kiếm đường đi
  - Cần thực hiện vạch đường phân cấp
- Trong vạch đường phân cấp:
  - Các router được chia thành những vùng (domain).
  - Router biết cách vạch đường bên trong vùng, nhưng không biết gì về cấu trúc bên trong của các vùng khác.

Vạch đường phân cấp (Hierarchical Routing)



Vạch đường phân cấp (Hierarchical Routing)



(a)

Bảng vạch đường đầy đủ của nút 1A

Đích	Lối ra	Chi phí
1A	–	–
1B	1B	1
1C	1C	1
2A	1B	2
2B	1B	3
2C	1B	3
2D	1B	4
3A	1C	3
3B	1C	2
4A	1C	3
4B	1C	4
4C	1C	4
5A	1C	4
5B	1C	5
5C	1B	5
5D	1C	6
5E	1C	5

(b)

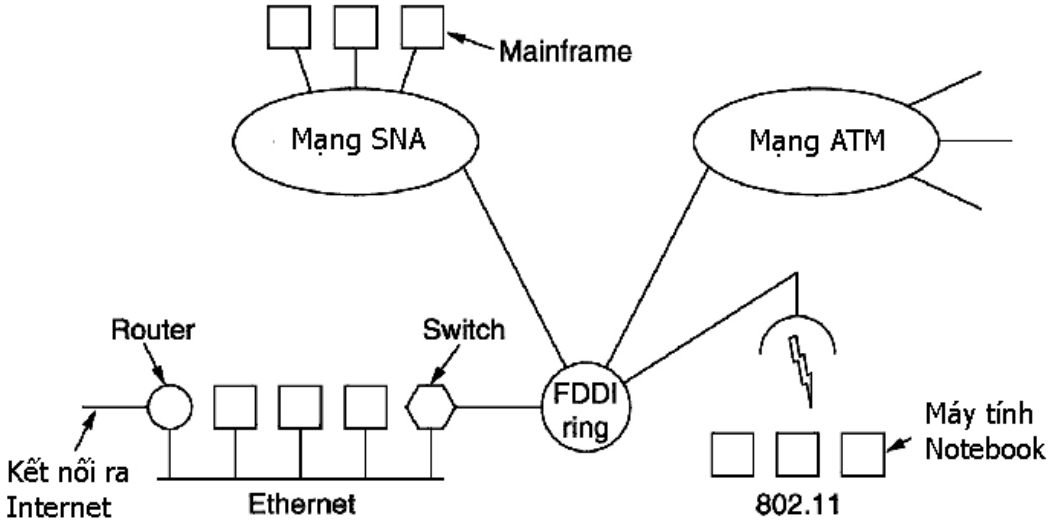
Bảng vạch đường phân cấp của host 1A

Đích	Lối ra	Chi phí
1A	–	–
1B	1B	1
1C	1C	1
2	1B	2
3	1C	2
4	1C	3
5	1C	4

(c)

Liên mạng và bộ giao thức IP

Liên mạng (Internetwork)



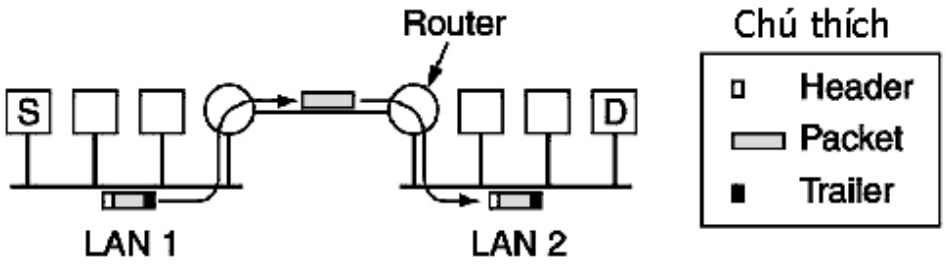
- Liên mạng: Mạng được hình thành từ việc liên nối kết nhiều mạng lại với nhau

- Các mạng thành phần là không đồng nhất (homogeneous): khác nhau về phần cứng, phần mềm, giao thức
- Mục tiêu của việc xây dựng liên mạng là cho phép người dùng trên một mạng con có thể liên lạc được với người dùng trên các mạng con khác

Các hình thức xây dựng liên mạng

- 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 tâng 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

Liên mạng ở tầng mạng



- Hai router được nối với nhau bằng đường nối điểm-điểm,
- Máy S muốn gởi cho máy D một gói tin,
- S 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, tìm ra địa chỉ mạng (IP) của máy đích, địa chỉ này sẽ được tham khảo trong bảng vạch đường của router LAN1 để tìm đường đi đến LAN 2
  - router LAN1 quyết định chuyển gói sang router LAN2 bằng cách đóng thành khung gởi cho router LAN2.

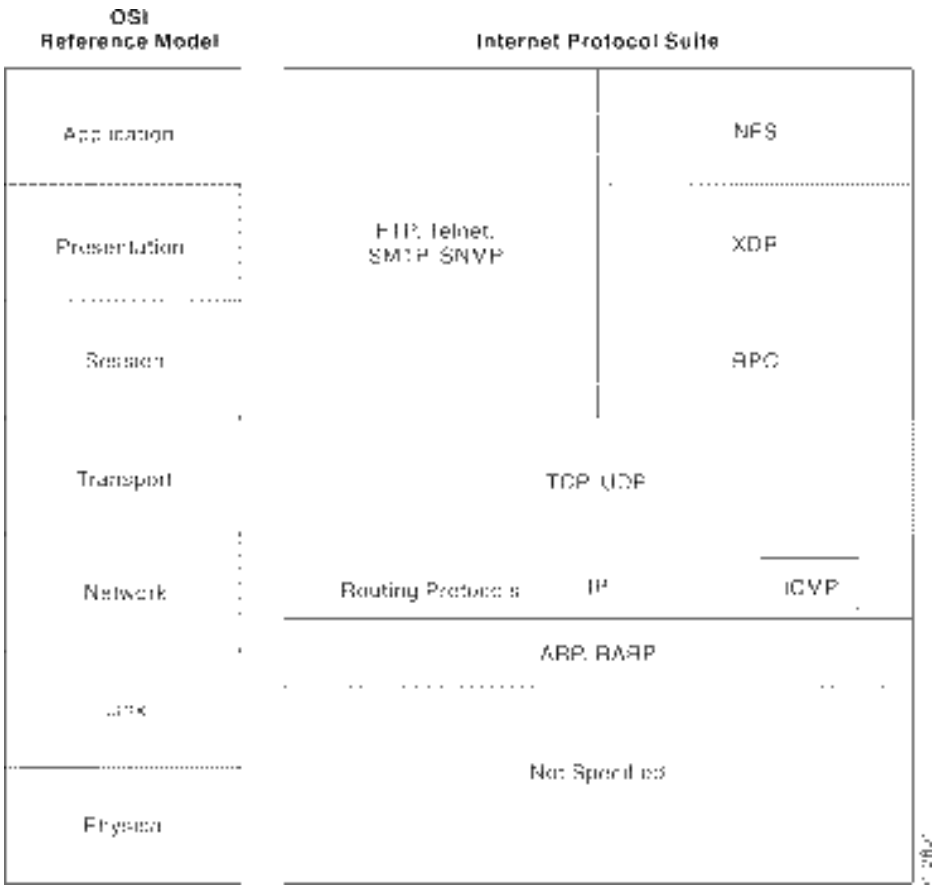
Bộ giao thức liên mạng (IPs - Internet Protocols)

- Bộ giao thức liên mạng lần đầu tiên được phát triển vào giữa những năm của thập niên 70 bởi môt dự án của Văn phòng các dự án nghiên cứu chuyên sâu của bộ quốc phòng Mỹ (DARPA-Defense Advanced Research Projects Agency)
- Mục đích: xây dựng một mạng chuyển mạch gói (packet-switched 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.

Bộ giao thức liên mạng (IPs - Internet Protocols)

- Là bộ giao thức liên mạng cho các hệ thống mở nổi tiếng nhất trên thế giới
- 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.
- Bao gồm một bộ các giao thức truyền thông:
  - Tầng 4 :
    - TCP (Transmission Control Protocol)
    - UDP (User Datagram Protocol)
  - Tầng 3: IP (Internet Protocol)
  - Tầng ứng dụng: SMTP, FTP, TELNET,HTTP, ...
  - Và các giao thức khác: ARP, RARP, ICMP, …

Bộ giao thức liên mạng (IPs - Internet Protocols)

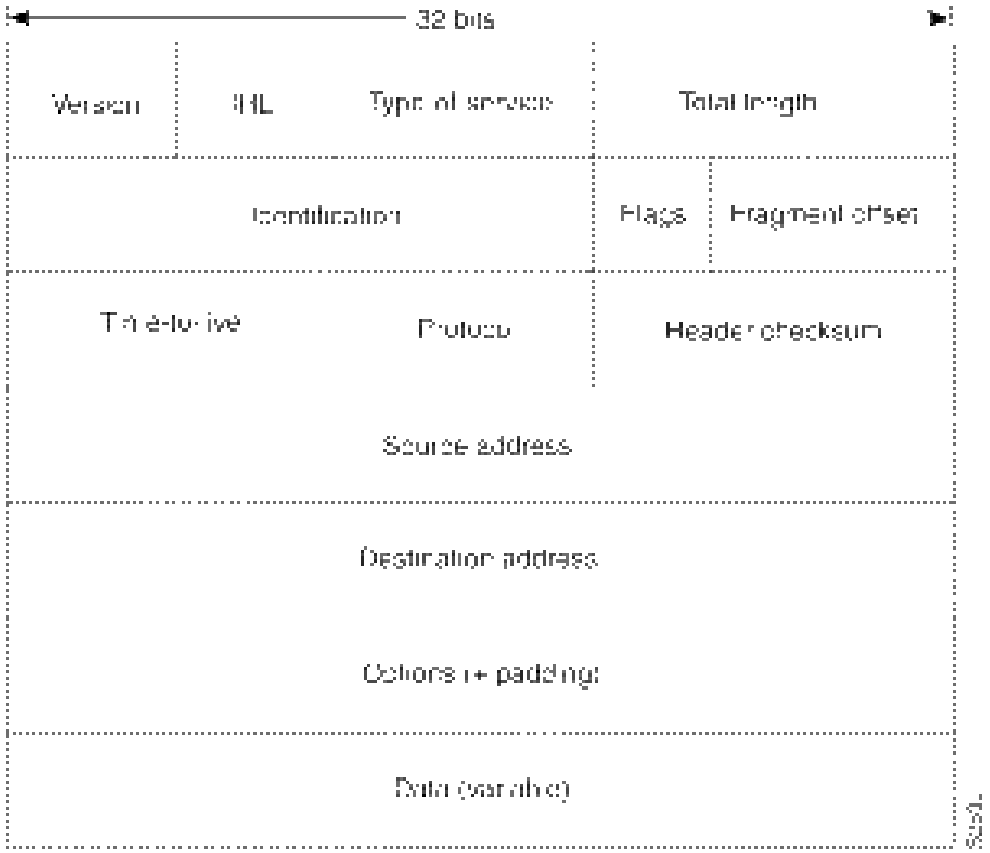


- TCP/IP được tích hợp vào hệ điều hành UNIX phiên bản BSD (Berkeley Software Distribution)
- Trở thành nền tảng cho mạng Internet và dịch vụ WWW (World Wide Web)

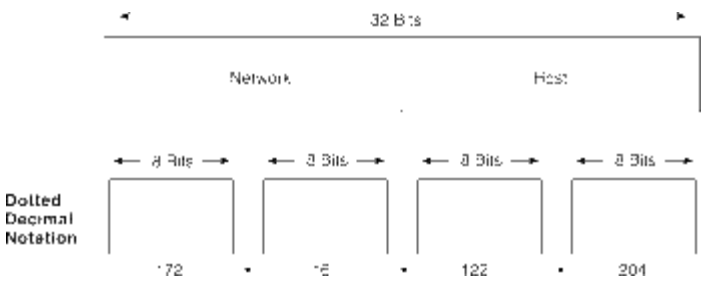
Giao thức IP (Internet protocol)

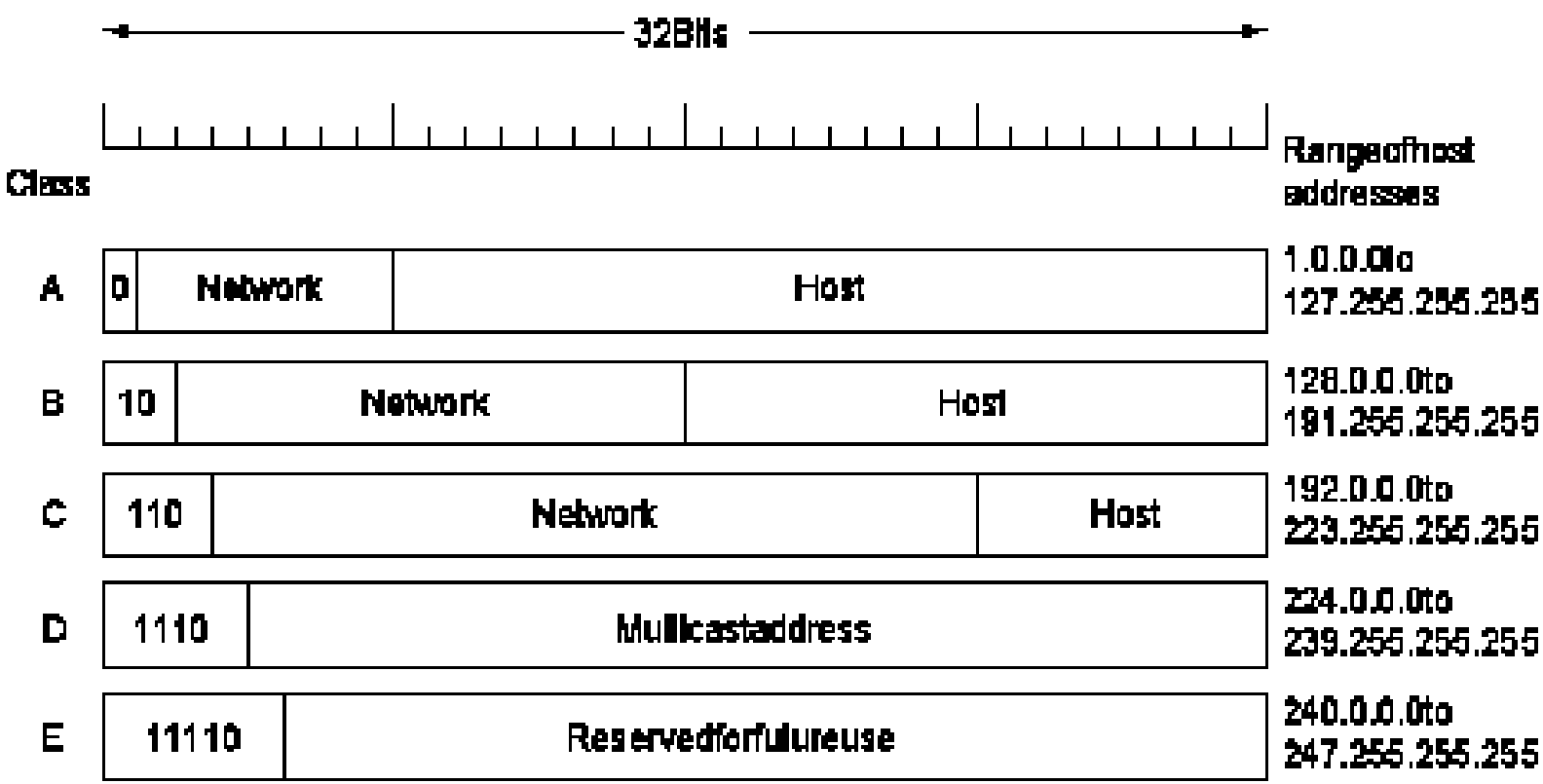
- Hoạt động ở tầng 3 của mô hình OSI
- Qui định cách thức định địa chỉ các máy tính và cách thức chuyển tải các gói tin qua một liên mạng.
- Được đặc tả trong RFC 791
- Cùng với giao thức TCP, IP trở thành trái tim của Bộ giao thức Internet.
- Hai chức năng chính
  - Cung cấp dịch vụ truyền tải dạng không nối kết để chuyển tải các gói tin qua một liên mạng
  - 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.

Cấu trúc gói tin của giao thức IP – V4



Cấu trúc địa chỉ IP





Lớp	Dạng	Mục đích	Các bits cao nhất	Khoản địa chỉ	Số bít phần nhận dạng mạng / Số bít phần nhận dạng máy tính	Tổng số máy tính trong một mạng
A	N.H.H.H	Cho một số ít các tổ chức lớn	0	1.0.0.0 đến 126.0.0.0	7/24	16.777. 214 (2^{24} - 2)
B	N.N.H.H	Cho các tổ chức có kích thước trung bình	10	128.1.0.0 đến 191.254.0.0	14/16	65. 543 (2^{16} - 2)
C	N.N.N.H	Cho các tổ chức có kích thước nhỏ	110	192.0.1.0 đến 223.255.254.0	21/8	254 (2^{8} - 2)
D		Truyền nhóm	1110	224.0.0.0 đến 239.255.255.255		
E		Dành cho thí nghiệm	1111	240.0.0.0 đến 254.255.255.255		

Chi tiết về các lớp của địa chỉ IP

Một 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.
  - 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
  - Không được dùng để đặt địa chỉ cho các máy tính
- 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)

Một số địa chỉ IP đặc biệt

- Địa chỉ mạng 127.0.0.0 là địa chỉ được dành riêng để đặt cho từng 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 :
  - 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

- Network Address = IP Address & Netmask

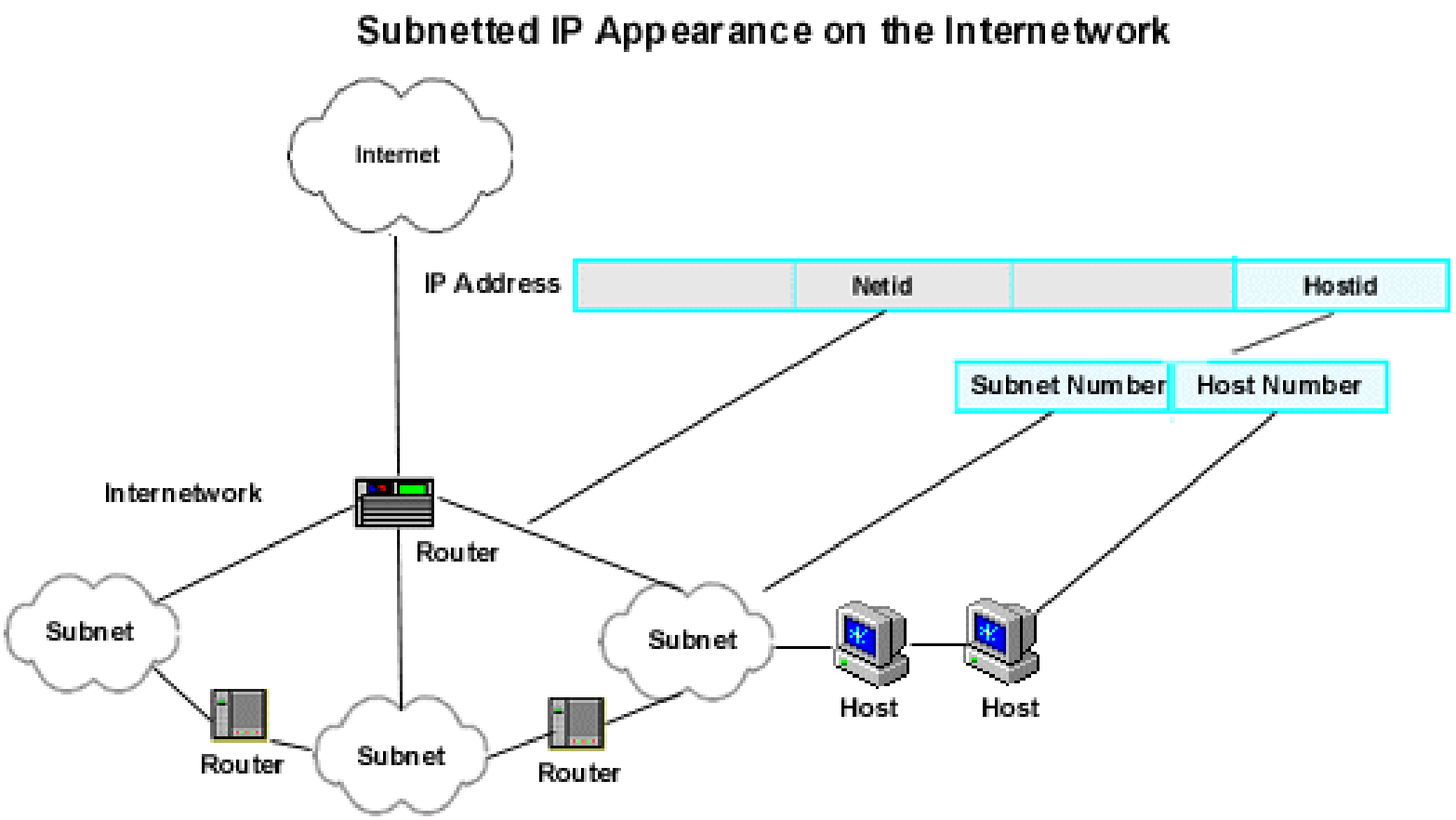
	Biểu diễn thập phân	Biểu diễn nhị phân
IP Address	198.53.147.45	11000110 00110101 10010011 00101101
Netmask	255.255.255.0	11111111 11111111 11111111 00000000
Network Address	198.53.147.0	11000110 00110101 10010011 00000000

Phân mạng con (Subnetting)

Phân mạng con là gì ?

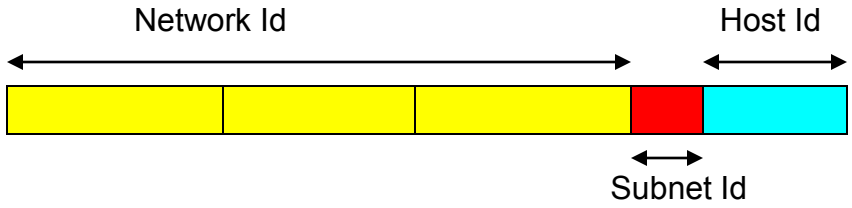
- Phân mạng con là một kỹ thuật cho phép nhà quản trị mạng chia một mạng thành những mạng con nhỏ, nhờ đó có được các tiện lợi sau :
  - Đơn giản hóa việc quản trị : Với sự trợ giúp của các router, các mạng có thể được chia ra thành nhiều mạng con (subnet) mà chúng có thể được quản lý như những mạng độc lập và hiệu quả hơn.
  - Có thể thay đổi cấu trúc bên trong của mạng mà không làm ảnh hưởng 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.

Phân mạng con là gì ?



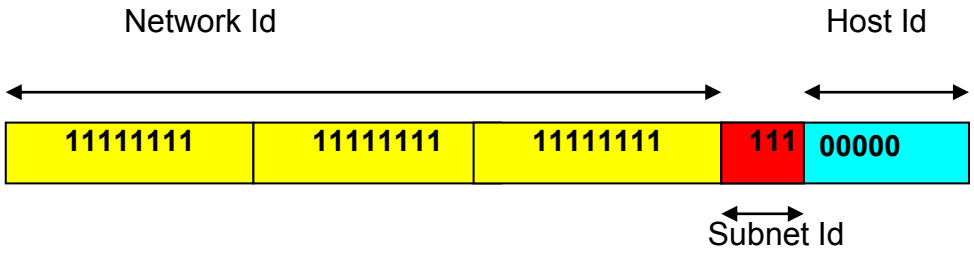
Phương pháp phân mạng con

- Nguyên tắc chung:
  - 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)
    - Phần nhận dạng máy tính trong mạng con (Host Id).



Phương pháp 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 con (Subnet Id) đều là 1 trong khi giá trị của các bits ở Phần nhận dạng máy tính (Host Id) đều là 0.
- Subnetwork Address = IP & Subnetmask



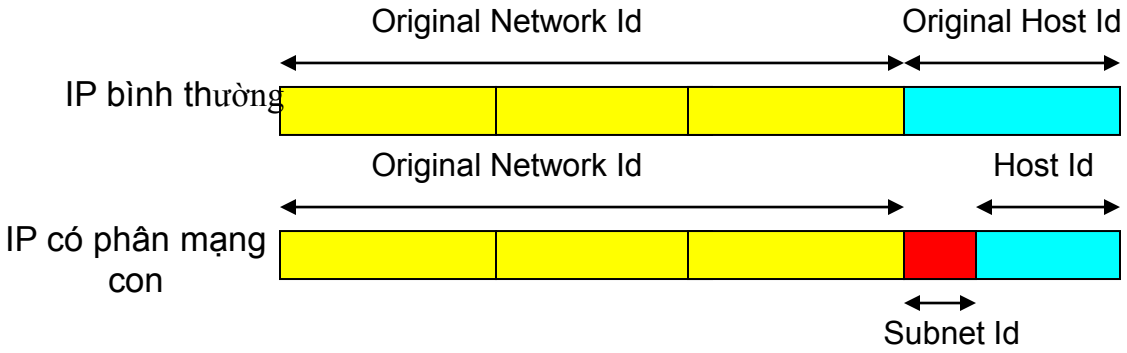
Mặt nạ mạng con khi phân mạng con lớp C

Phương pháp phân mạng con

- Có hai chuẩn để thực hiện phân mạng con là :
  - Chuẩn phân lớp hoàn toàn (Classfull standard)
  - Chuẩn Vạch đường liên miền không phân lớp CIDR (Classless Inter-Domain Routing).
- 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.

Phương pháp phân lớp hoàn toàn (Classfull Standard)

- 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
  - Phần nhận dạng máy tính trong mạng con (Host Id) bao gồm các bit còn lại



Phương pháp phân lớp hoàn toàn (Classfull Standard)

- Số lượng bits thuộc phần nhận dạng mạng con xác định số lượng mạng con.
  - 4 bits, ta có 2^4=16 mạng con.
  - 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.

Phương pháp phân lớp hoàn toàn (Classfull Standard)

- Ví dụ :
  - Cho địa chỉ mạng lớp C : 192.168.1.0 / 255.255.255.0.
  - Sử dụng 2 bits để làm phần nhận dạng mạng con.
  - Mặt nạ mạng con trong trường hợp này là 255.255.255.192.
  - Khi đó ta có các địa chỉ mạng con như sau :

Địa chỉ IP	Biểu diễn dạng thập phân	Biểu diễn dạng nhị phân			
Mạng ban đầu	192.168.1.0	1100 0000	1010 1000	0000 0001	0000 0000
Subnetmask	255.255.255.192	1111 1111	1111 1111	1111 1111	**11**00 0000
Mạng con 1	192.168.1.0	1100 0000	1010 1000	0000 0001	**00**00 0000
Mạng con 2	192.168.1.64	1100 0000	1010 1000	0010 0001	**01**00 0000
Mạng con 3	192.168.1.128	1100 0000	1010 1000	0000 0001	**10**00 0000
Mạng con 4	192.168.1.192	1100 0000	1010 1000	0000 0001	**11**00 0000

Phương pháp phân lớp hoàn toàn (Classfull Standard)

- 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

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.
- Cấu trúc địa chỉ CIDR:
  - Không sử dụng cơ chế phân lớp A,B,C,E,D
  - Phần nhận dạng mạng: từ 13 đến 27 bits
  - Một địa chỉ theo cấu trúc 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 : 206.13.01.48/25

Phương pháp Vạch đường liên miền không phân lớp CIDR (Classless Inter-Domain Routing)

Số bits nhận dạng mạng trong địa chỉ CIDR	Lớp tương ứng trong chuẩn phân lớp hoàn toàn	Số lượng máy tính trong mạng
/27	1/8 lớp C	32
/26	¼ lớp C	64
/25	1/2 lớp C	128
/24	1 lớp C	256
/23	2 lớp C	512
/22	4 lớp C	1.024
/21	8 lớp C	2.048
/20	16 lớp C	4.096
/19	32 lớp C	8.192
/18	64 lớp C	16.384
/17	128 lớp C	32.768
/16	256 lớp C (= 1 lớp B)	65.536
/15	512 lớp C	131.072
/14	1,024 lớp C	262.144
/13	2,048 lớp C	524.288

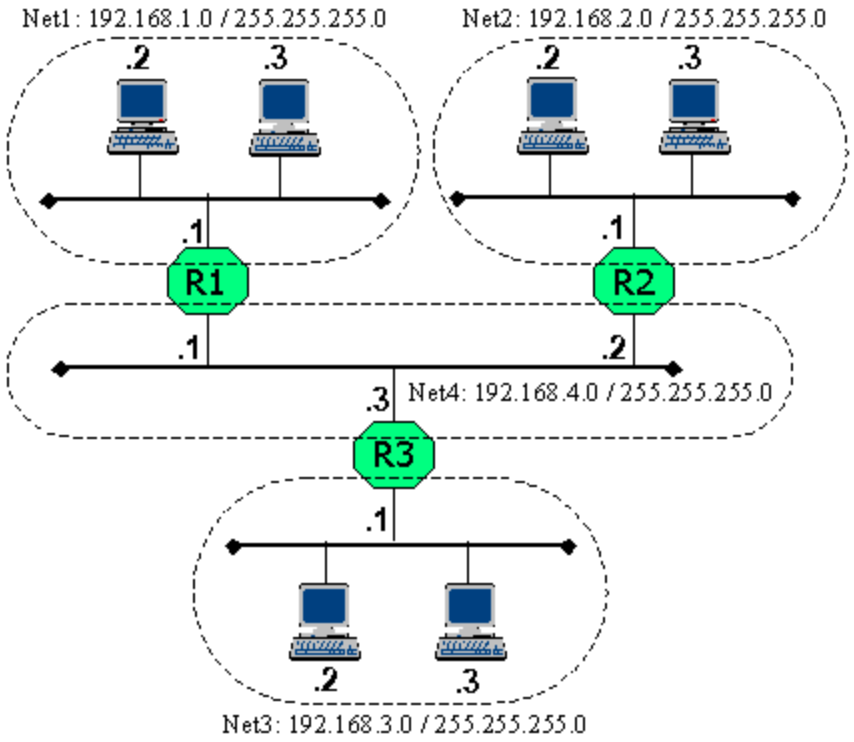
Kết hợp việc chọn đường có cấu trúc để giảm tối đa số lượng các mục từ trong bảng chọn đường

- CIDR cho phép kết hợp các đường đi
  - 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.
- Tương tự kiến trúc phân cấp của mạng điện thoại
  - 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 không lồ các số điện thoại riêng lẽ chứ không phải là một số điện thoại cụ thể.

Kết hợp việc chọn đường có cấu trúc để giảm tối đa số lượng các mục từ trong bảng chọn đường

- 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

Vạch đường trong giao thức IP



192.168.3.3 - Routing table

Network/Netmask	NextHop	Interface
192.168.3.0/255.255.255.0	local	local
default	192.168.3.1	local

R1-Routing table

Network/Netmask	NextHop	Interface
192.168.1.0/255.255.255.0	local	local
192.168.2.0/255.255.255.0	192.168.4.2	192.168.4.1
192.168.3.0/255.255.255.0	192.168.4.3	192.168.4.1
192.168.4.0/255.255.255.0	local	local

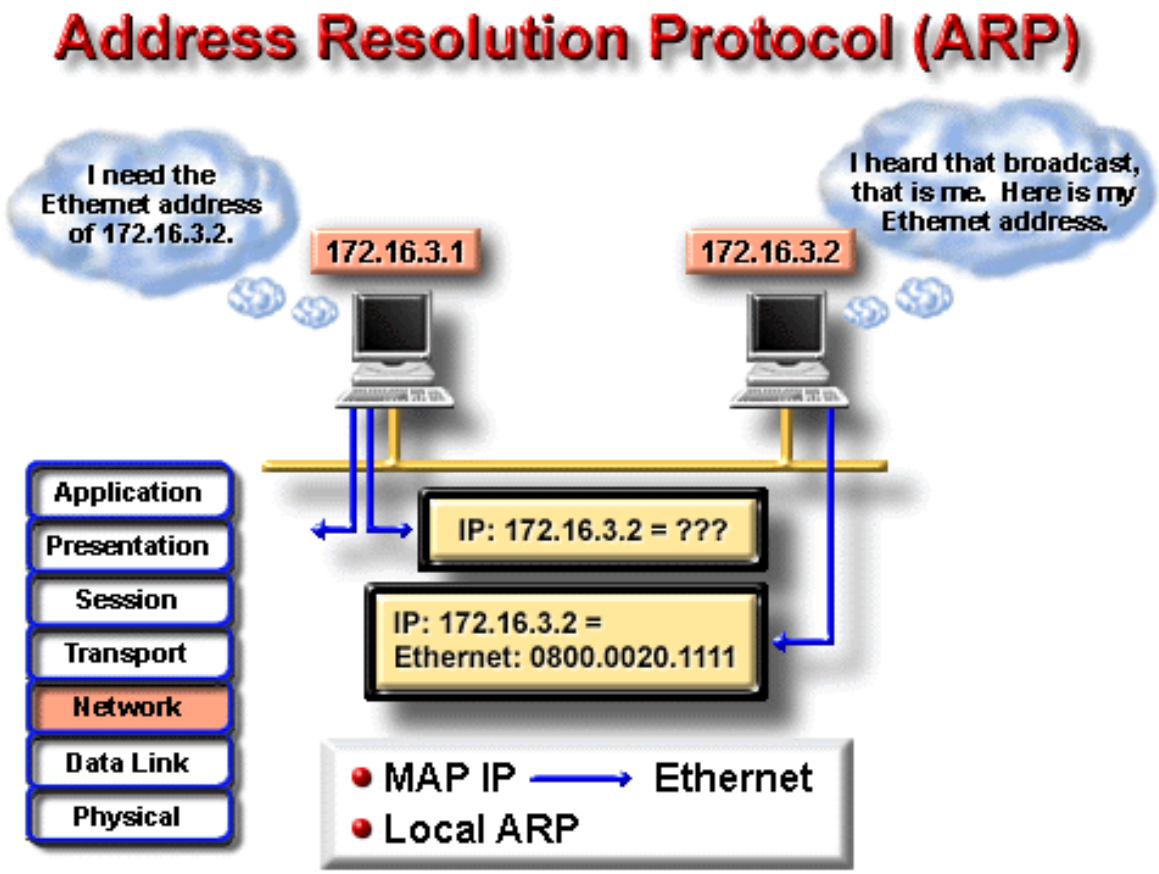
R2-Routing table

Network/Netmask	NextHop	Interface
192.168.1.0/255.255.255.0	192.168.4.1	192.168.4.2
192.168.2.0/255.255.255.0	local	local
192.168.3.0/255.255.255.0	192.168.4.3	192.168.4.2
192.168.4.0/255.255.255.0	local	local

R3-Routing table

Network/Netmask	NextHop	Interface
192.168.1.0/255.255.255.0	192.168.4.1	192.168.4.3
192.168.2.0/255.255.255.0	192.168.4.2	192.168.4.3
192.168.3.0/255.255.255.0	local	local
192.168.4.0/255.255.255.0	local	local

Giao thức phân giải địa chỉ (ARP - Address Resolution Protocol)



Giao thức phân giải địa chỉ (ARP - Address Resolution Protocol)

Tổng quát	Các trường	Kích thước (byte)	Các giá trị
Ethernet Header	Ethernet Destination Address	6	Địa chỉ máy nhận, trong trường hợp này là một địa chỉ quảng bá
	Ethernet Source Address	6	Địa chỉ của máy gởi thông điệp
	Frame Type	2	Kiểu khung, có giá trị là 0x0806 khi ARP yêu cầu và 0x8035 khi ARP trả lời
ARP request/ reply	Hardware Type	2	Giá trị là 1 cho mạng Ethernet
	Protocol Type	2	Có giá trị là 0x0800 cho địa chỉ IP
	Hardware Address Size in bytes	1	Chiều dài của địa chỉ vật lý, có giá trị là 6 cho mạng Ethernet
	Protocol Address Size in bytes	1	Chiều dài địa chỉ của giao thức, có giá trị là 4 cho giao thức IP
	Operation	2	Là 1 nếu là khung yêu cầu, là 2 nếu là khung trả lời
	Sender Ethernet Address	6	-
	Sender IP Address	4	-
	Destination Ethernet Address	6	Không sử dụng đến trong yêu cầu của ARP
	Destination IP Address	4	-

Giao thức phân giải địa chỉ ngược RARP (RARP - Reverse Address Resolution Protocol)

- Giao thức RARP được dùng để ánh xạ địa chỉ một địa chỉ MAC về một địa chỉ IP
- Dùng tron các hệ thống trạm làm việc không đĩa cứng (Diskless workstation)
- Các máy trạm cần có một địa chỉ IP để giao tiếo với server.
- 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

Giao thức thông điệp điều khiển Internet ICMP (Internet Control Message Protocol)

- 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
- 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)
  - ....

TẦNG VẬN CHUYỂN
(Computer Network)

Trình bày: Ngô Bá Hùng
Khoa CNTT&TT
Đại Học Cần Thơ

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

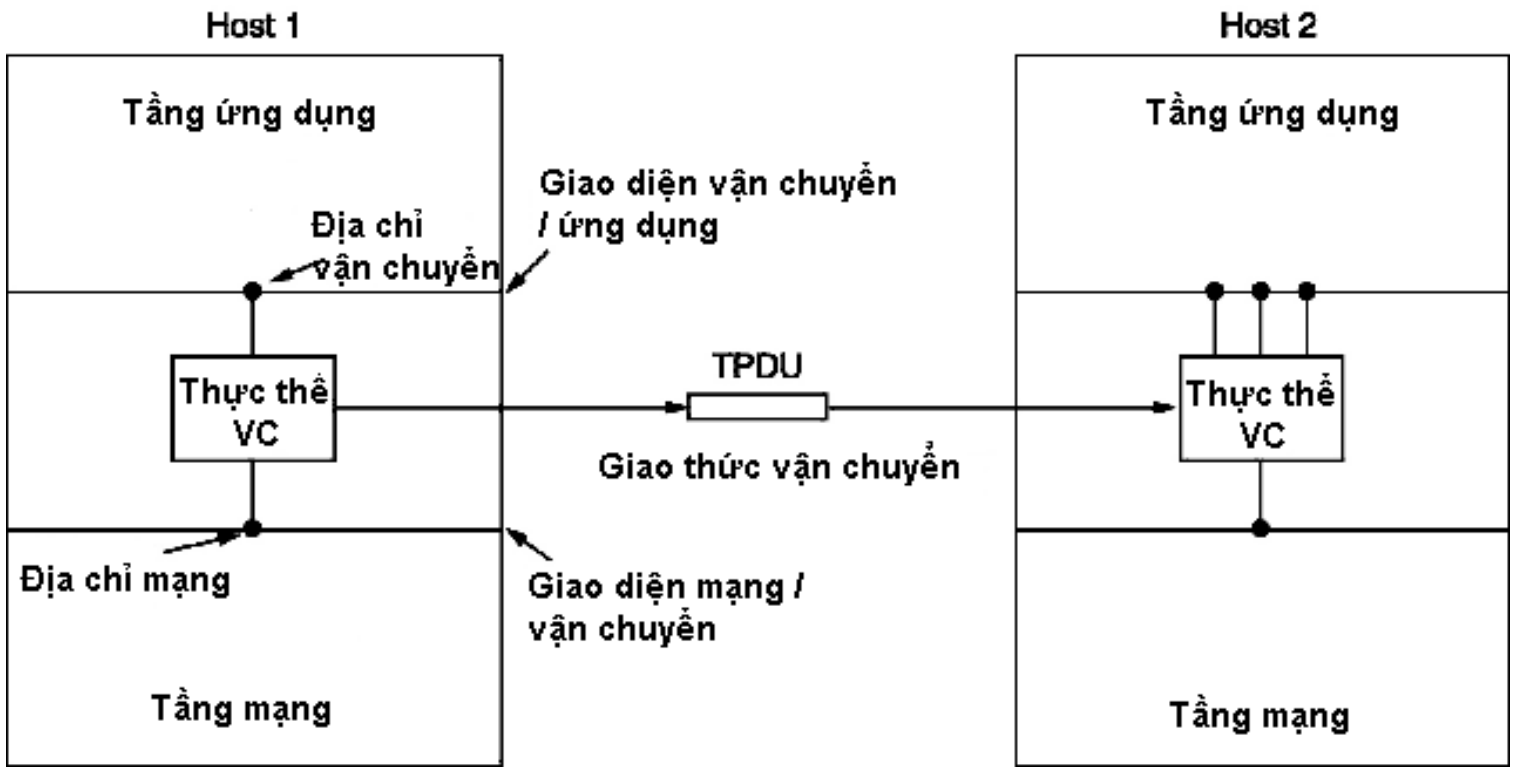
Yêu cầu

- 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

Nhiệm vụ của tầng vận chuyển

- Tầng mạng đảm bảo truyền tải kiểu Host -to- Host
- Tầng vận chuyển đảm bảo truyền tải kiểu End point –to- End point
- End point là các chương trình ứng dụng
- Cấp dịch vụ vận chuyển gói tin hiệu quả, tin cậy và tiết kiệm chi phi cho người dùng

Vị trí của tầng vận chuyển



Dịch vụ cung cấp bởi tầng vận chuyển

- Hai kiểu dịch vụ
  - Có nối kết :
    - Thiết lập nối kết,
    - Truyền dữ liệu
    - Hủy nối kết
  - Không nối kết
- 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

Các hàm dịch vụ cơ sở - Có nối kết

Hàm	Gói tin gởi đi	Ý nghĩa
LISTEN	Không có	Nghẽn cho đến khi tiến trình nào đó nối kết tới
CONNECT	Yêu cầu kết nối (Connection Request)	Chủ động yêu cầu thiết lập nối kết đến tiến trình khác
SEND	Dữ liệu (Data)	Gởi thông tin đi
RECEIVE	Không có	Nghẽn cho đến khi một gói tin đến và nhận nó
DISCONNECT	Yêu cầu hủy kết nối (Disconnection Request)	Muốn hủy kết nối với bên đối tác

Các hàm dịch vụ cơ sở - Không nối kết

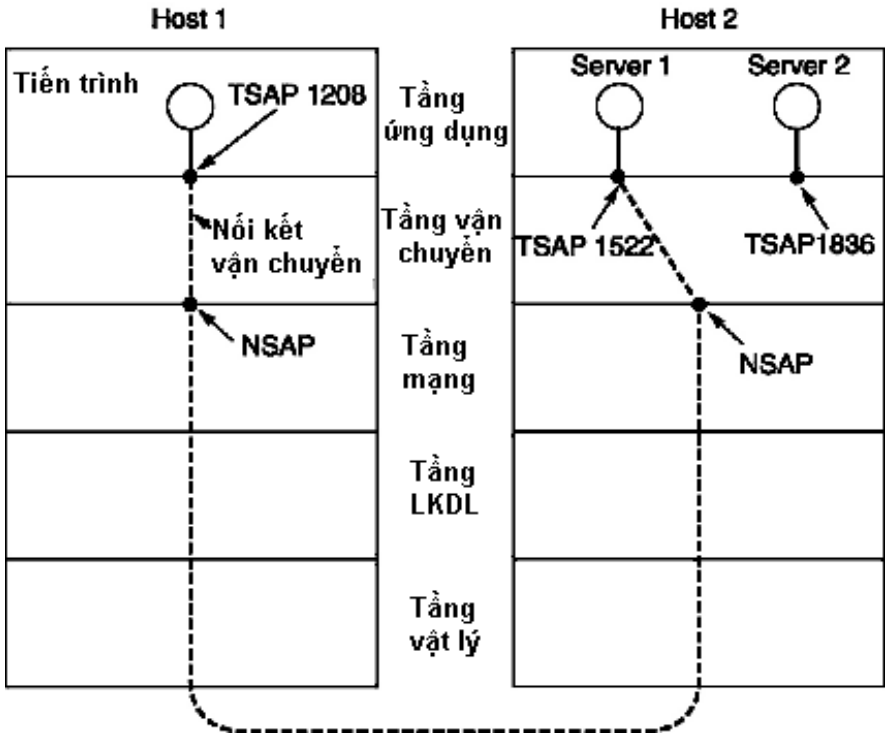
Hàm	**Gói tin gởi đi**	**Ý nghĩa**
SEND	Dữ liệu (Data)	Gởi thông tin đi
RECEIVE	Không có	Nghẽn cho đến khi một gói tin đến và nhận nó

Các yếu tố cấu thành giao thức vận chuyển

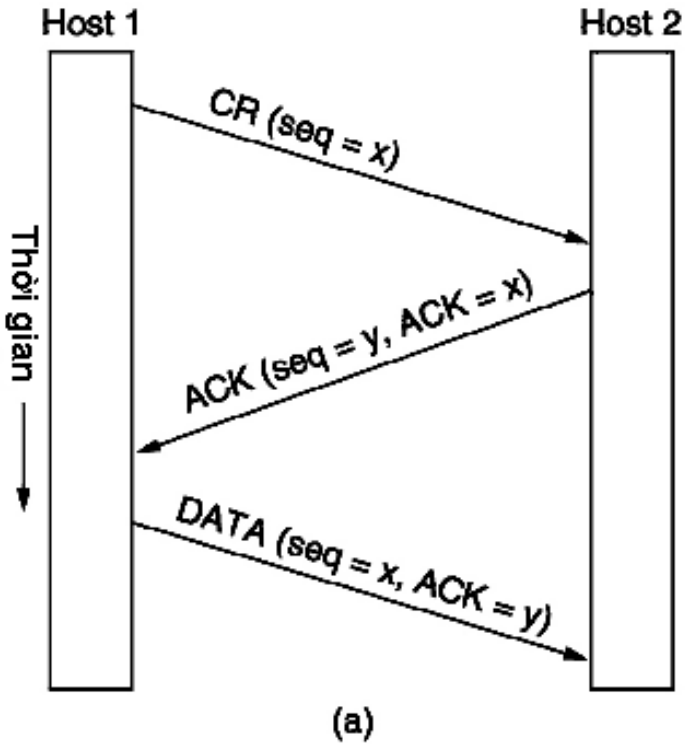
- Điều khiển lỗi, đánh số thứ tự gói tin và điều khiển luồng dữ liệu.
- Môi trường giao tiếp qua một tập các mạng trung gian
- Những vấn đề cần quan tâm:
  - Định địa chỉ các tiến trình trên các host
  - Xử lý những trường hợp mất gói tin, gói tin đi chậm dẫn đến mãn kỳ và gởi thêm một gói tin bị trùng lắp,
  - Đồng bộ hóa hai tiến trình đang trao đổi dữ liệu khi mà chúng đang ở rất xa nhau

Định địa chỉ

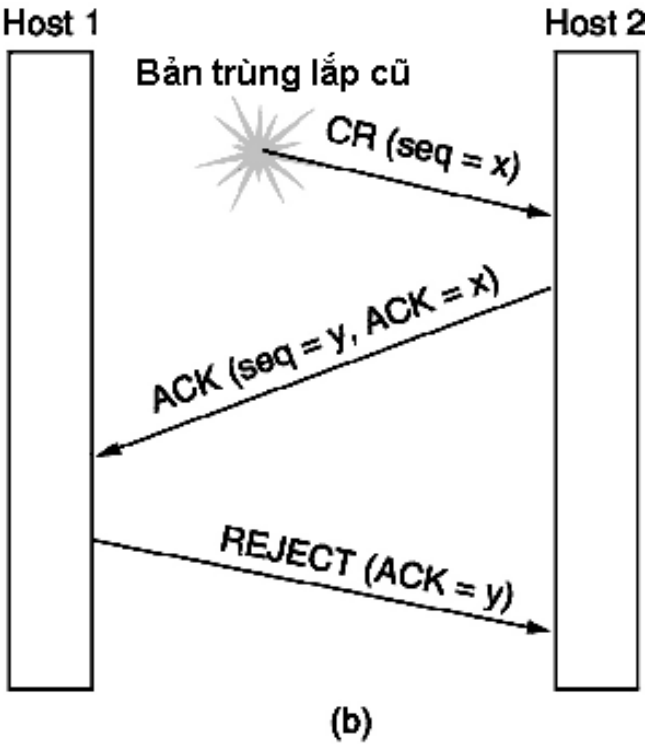
- Địa chỉ tiến trình là TSAP (Transport Service Access Point).
  - Mạng Internet là dùng số hiệu cổng (port),
  - Mạng ATM là AAL-SAP.
- Tầng mạng được gọi là NSAP



Thiết lập nối kết

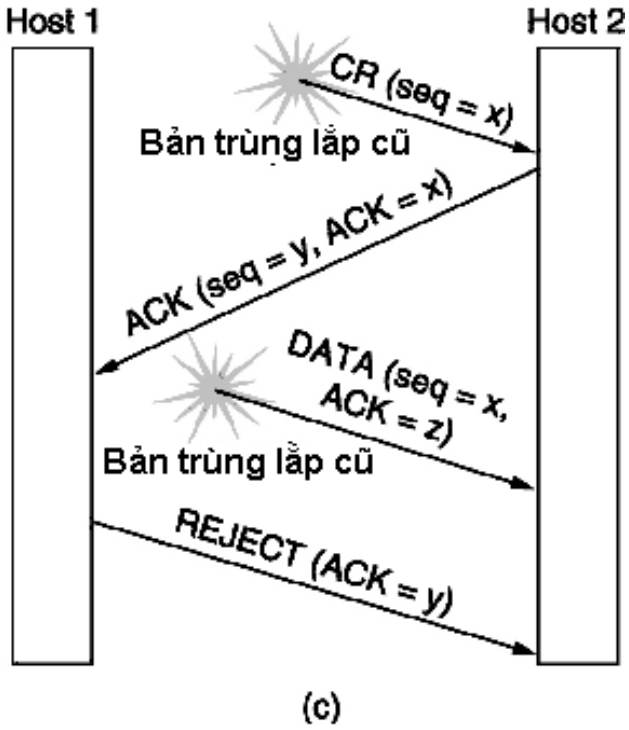


Three-way hand-shake
Hoạt động bình thường.



Bản CR bị trùng lắp

Thiết lập nối kết

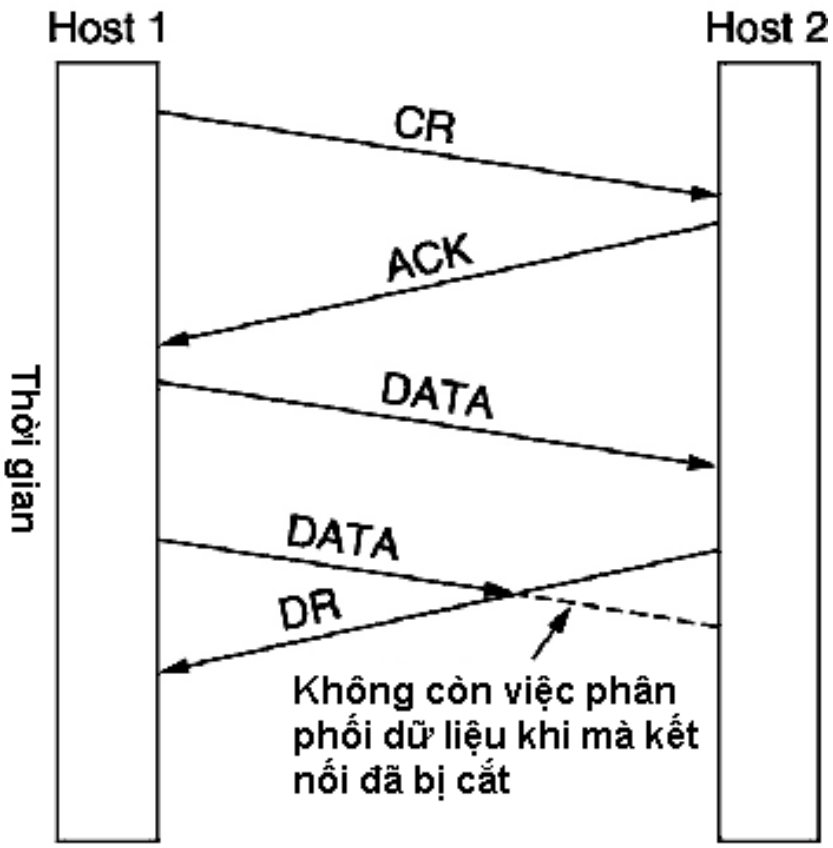


Cả CR và ACK đều bị trùng lắp

Giải phóng nối kết

- Hai kiểu giải phóng nối kết:
  - 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

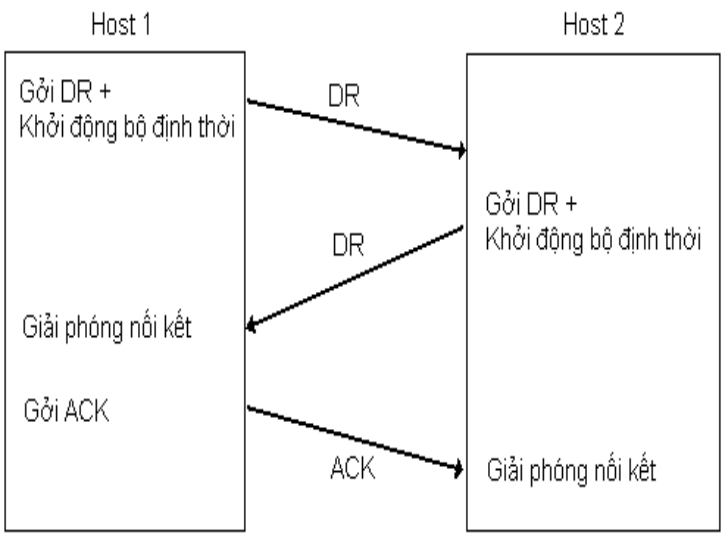
Giải phóng nối kết dị bộ



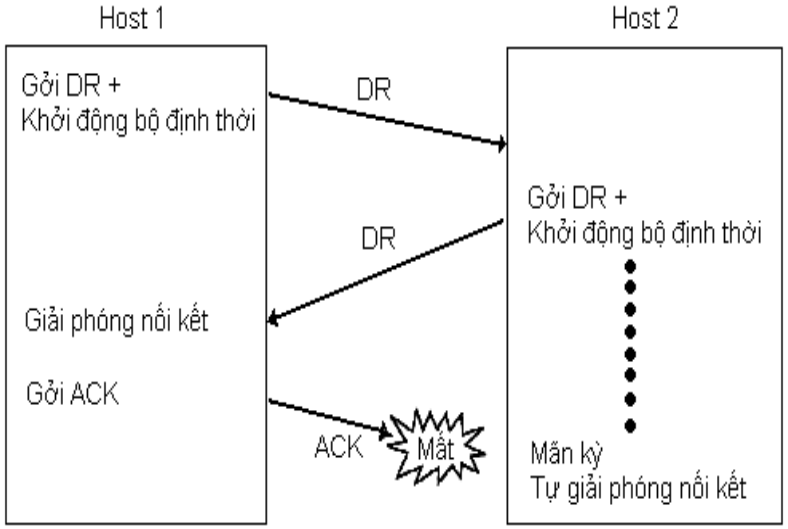
Giải phóng nối kết đồng bộ

- Một nút phải tiếp tục nhận dữ liệu sau khi đã gởi đi yêu cầu giải phóng nối kết (DISCONNECT REQUEST – CR), cho đến khi nhận được chấp thuận hủy bỏ nối kết của bên đối tác đó
- Sử dụng phương pháp hủy nối kết ba chiều cùng với bộ định thời

Giải phóng nối kết đồng bộ

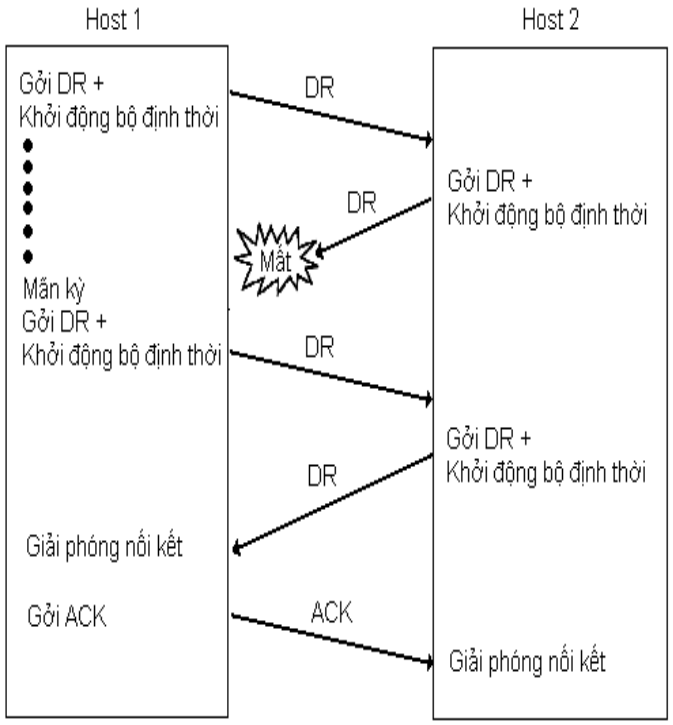


Bình thường

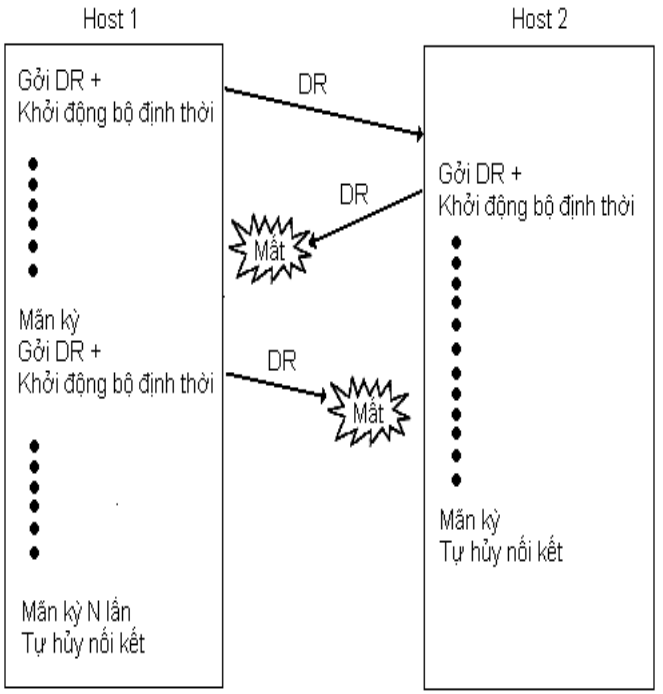


Khung ACK cuối cùng bị mất

Giải phóng nối kết đồng bộ



Trả lời bị mất



Trả lời mất và các gói tin DR theo sau cũng bị mất

Điều khiển thông lượng

- Sử dụng giao thức cửa sổ trượt với kích thước cửa sổ của bên gởi và bên nhận là khác nhau
- 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

Điều khiển thông lượng

	A	Thông điệp	B	Giải thích
1	→	<yêu cầu 8 buffers>	→	A muốn B cung cấp 8 buffers
2	← →	<ack = 0, buf = 4>	← →	B chỉ cấp cho A 4 buffers thôi
3	→	<seq = 0, data = m0>	→	A còn lại 3 buffers
4	→	<seq = 1, data = m1>		A còn lại 2 buffers
5	← →	<seq = 2, data = m2>	← → ...	Thông điệp bị mất, nhưng A nghĩ nó còn 1 buffer
6	→ →	<ack = 1, buf = 3>	→ →	B báo nhận cho thông điệp 0 và 1, còn 3 buffers
7	←	<seq = 3, data = m3>	←	A còn lại 1 buffer

Điều khiển thông lượng

8		<seq = 4, data = m4>		A không còn buffer nào và phải dừng
9		<seq = 2, data = m2>		Thông điệp thứ 2 của A mất kỳ và được truyền lại
10		<ack = 4, buf = 0>		Mọi thứ đã được báo nhận, nhưng A vẫn nghẽn
11	←	<ack = 4, buf = 1>	←	A có thể gởi 1 gói tin thứ 5
12	← →	<ack = 4, buf = 2>	← →	B có thêm 1 buffer nữa
13	→	<seq = 5, data = m5>	→	A còn lại 1 buffer
14	←	<seq = 6, data = m6>	← ←	A nghẽn một lần nữa
15		<ack = 6, buf = 0>		A vẫn còn nghẽn
16	...	<ack = 6, buf = 4>		Khả năng dẫn đến deadlock

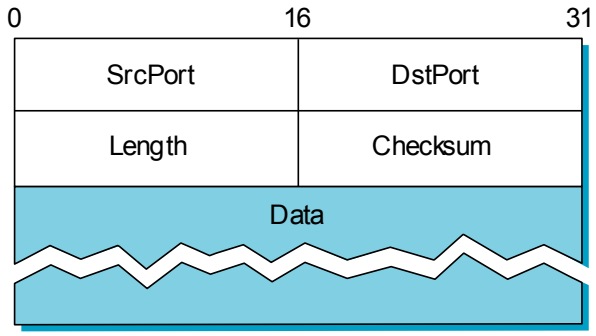
Tầng vận chuyển trong mạng Internet

- Nhiệm vụ
  - 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
- Hỗ trợ hai phương thức hoạt động
  - Không nối kết (UDP)
  - Có nối kết (TCP)

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,
- 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.

Giao thức UDP (User Datagram Protocol)



- Checksum:Là 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.

Giao thức UDP (User Datagram Protocol)

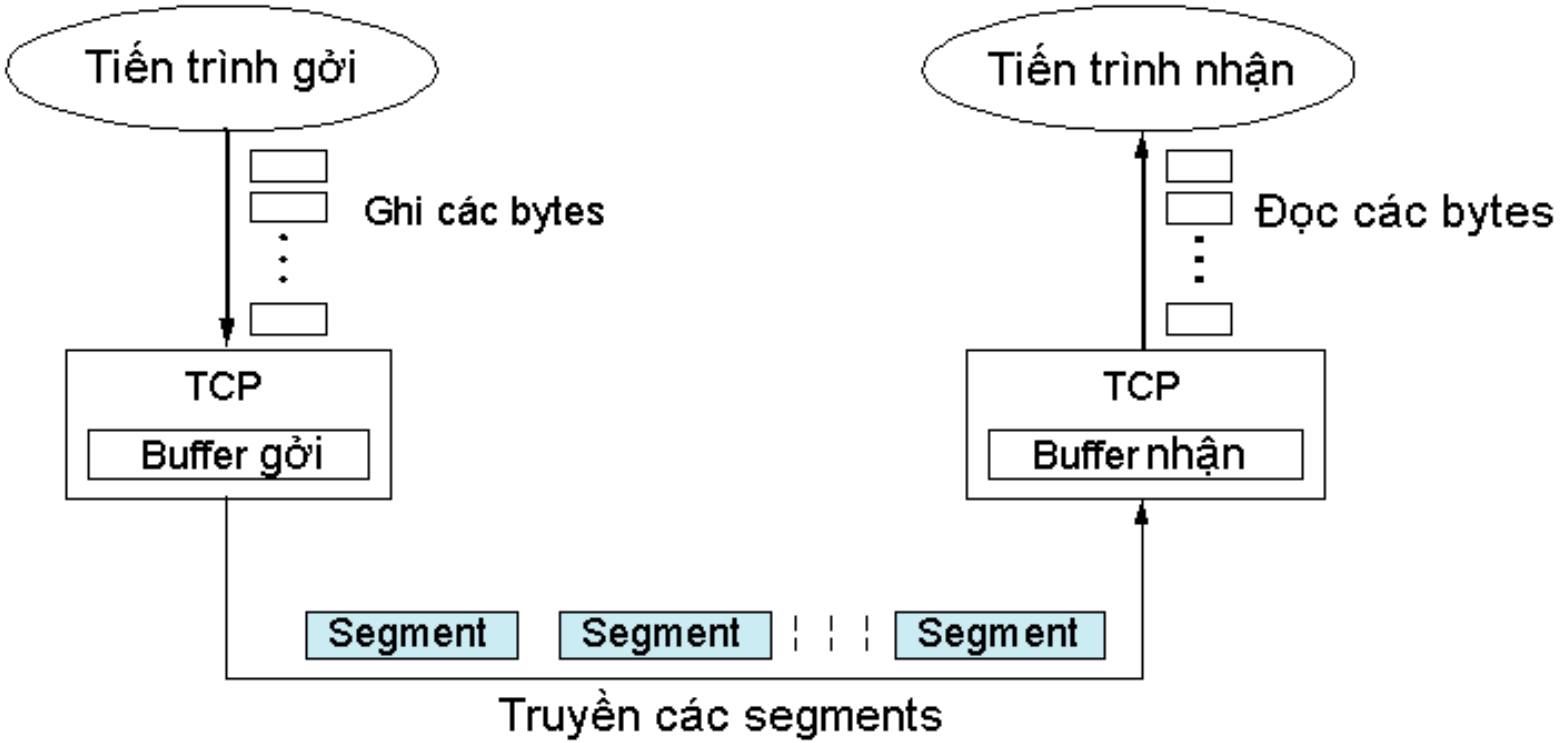
- Phương pháp kiểm tra lỗi

```
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);
}
```

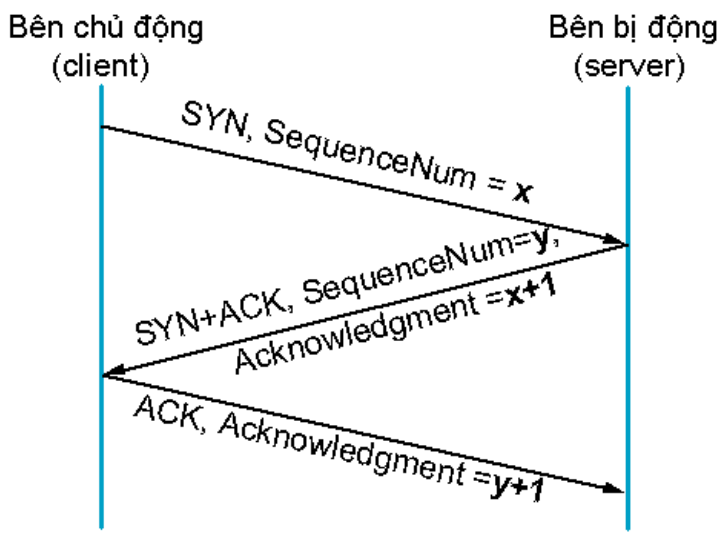
Giao thức TCP (Transmission Control Protocol)

- TCP là giao thức 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 song công, hỗ trợ cơ chế đa hợp
- TCP là giao thức hướng bytes

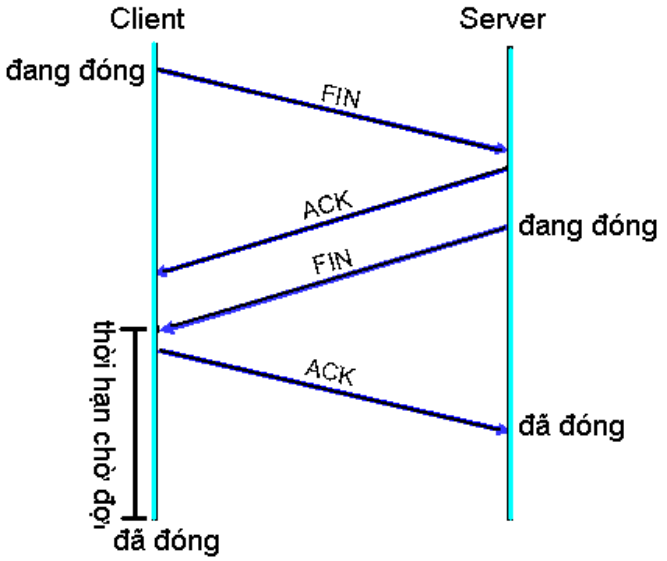
Giao thức TCP (Transmission Control Protocol)



Giao thức TCP (Transmission Control Protocol)



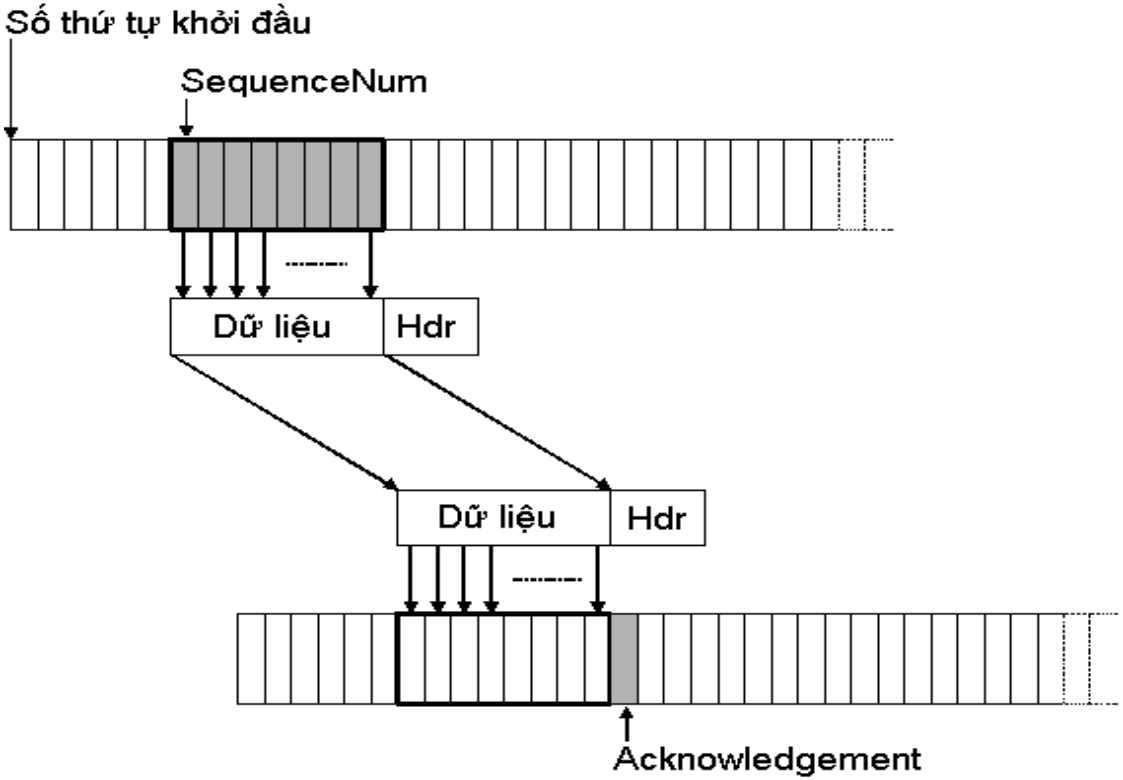
Bắt tay trong TCP



Hủy bắt tay trong TCP

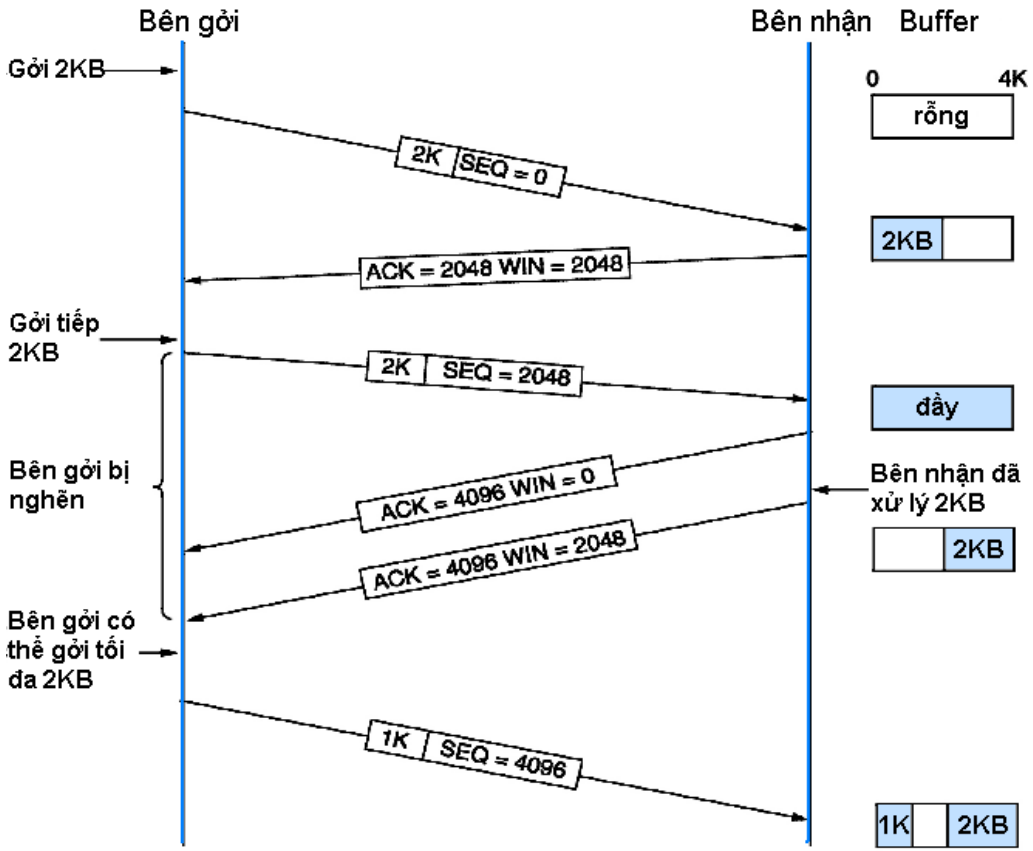
Điều khiển thông lượng trong TCP

- Là giao thức truyền hướng bytes
- Mỗi lần truyền đi một Segment

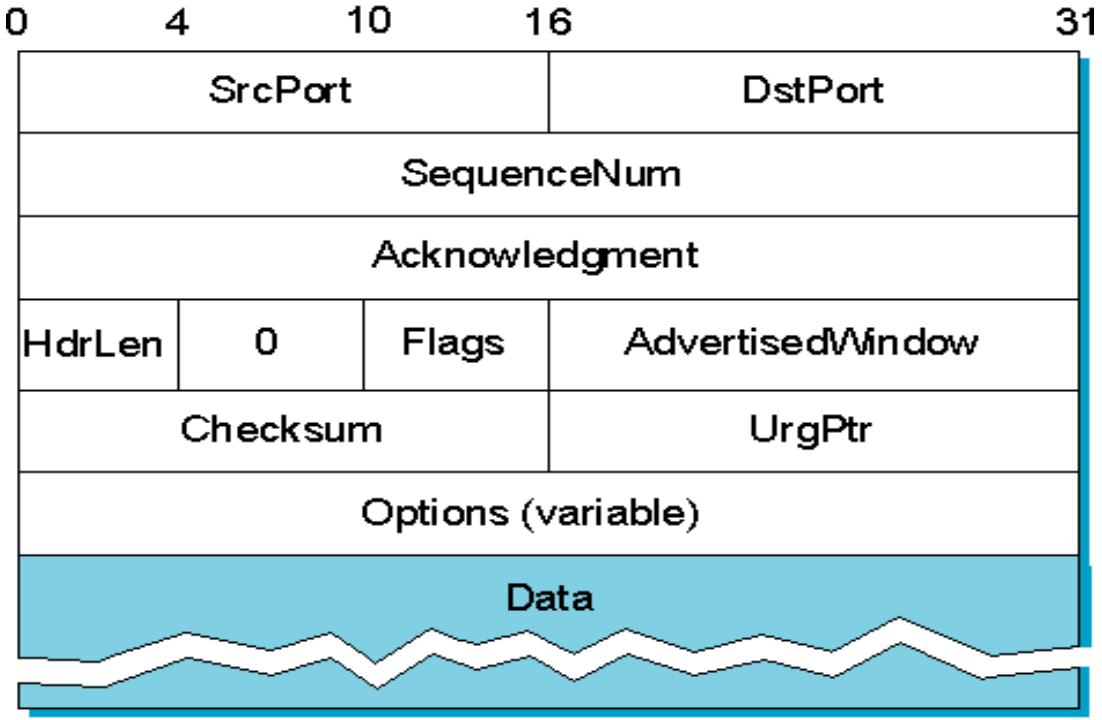


Điều khiển thông lượng trong TCP

- Sử dụng giao thức cửa sổ trượt



Giao thức TCP (Transmission Control Protocol)



Flags = [SYN, FIN, RESET, PUSH, URG, ACK]