**TRƯỜNG ĐẠI HỌC BÁCH KHOA ĐÀ NẴNG**
**KHOA CÔNG NGHỆ THÔNG TIN**

——— Â ———

GIÁO TRÌNH MÔN HỌC

# MẠNG MÁY TÍNH

**Ths. NGUYỄN TẤN KHÔI**

*(Lưu hành nội bộ)*
**Đà Nẵng – 2004**

# MỤC LỤC

*Chương 1 MỞ ĐẦU 1*

**1.1 Giới thiệu ..... 1**

**1.2 Phân loại mạng ..... 2**

1.2.1 Dựa theo khoảng cách địa lý ..... 2

1.2.2 Dựa theo cấu trúc mạng ..... 2

1.2.3 Theo phương pháp chuyển mạch ..... 3

**1.3 Kiến trúc phân tầng và chuẩn hoá mạng ..... 5**

1.3.1 Các tổ chức chuẩn hoá mạng ..... 5

1.3.2 Kiến trúc phân tầng ..... 6

**1.4 Mô hình OSI ..... 7**

1.4.1 Kiến trúc của mô hình OSI ..... 7

1.4.2 Sự ghép nối giữa các mức ..... 8

1.4.3 Chức năng của mỗi tầng ..... 9

1.4.4 Các giao thức chuẩn của OSI ..... 11

**1.5 Hệ điều hành mạng ..... 12**

**1.6 Mạng Internet ..... 13**

1.6.1 Lịch sử ra đời và phát triển ..... 13

1.6.2 Cấu trúc của mạng Internet ..... 14

1.6.3 Các kiến trúc khác ..... 15

*Chương 2 TẦNG VẬT LÝ 16*

**2.1 Môi trường truyền tin ..... 16**

2.1.1 Phương tiện truyền ..... 16

2.1.2 Các thông số cơ bản của môi trường truyền tin ..... 19

**2.2 Chuẩn giao diện ..... 19**

2.2.1 Modem ..... 19

2.2.2 DTE và DCE ..... 21

2.2.3 Chuẩn RS-232C ..... 21

*Chương 3 TẦNG LIÊN KẾT DỮ LIỆU 22*

**3.1 Chức năng ..... 22**

**3.2 Các vấn đề của tầng liên kết dữ liệu ..... 22**

3.2.1 Cung cấp dịch vụ cho tầng mạng ..... 22

3.2.2 Khung tin - Nhận biết gói tin ..... 23

3.2.3 Kiểm tra lỗi ..... 23

3.2.4 Điều khiển luồng dữ liệu ..... 23
3.2.5 Quản lý liên kết ..... 24
3.2.6 Nén dữ liệu khi truyền ..... 24
**3.3 Phát hiện và hiệu chỉnh lỗi ..... 24**
3.3.1 Phương pháp bit chẵn lẻ (Parity) ..... 25
3.3.2 Tính theo đa thức chuẩn ..... 25
3.3.3 Mã sửa sai ..... 26
**3.4 Thủ tục liên kết dữ liệu cơ bản ..... 27**
3.4.1 Giao thức đơn công với kênh có lỗi ..... 28
**3.5 Điều khiển dòng truyền ..... 28**
3.5.1 Cơ chế cửa sổ ..... 29
3.5.2 Trao đổi bản tin với cửa sổ 1 bit ..... 30
3.5.3 Vận chuyển liên tục ..... 31
**3.6 Các giao thức của tầng Liên kết dữ liệu ..... 33**
3.6.1 Giao thức BSC ..... 33
3.6.2 Giao thức HDLC ..... 34
***Chương 4 MẠNG CỤC BỘ 37***
**4.1 Các cấu hình của mạng LAN ..... 37**
4.1.1 Mạng dạng hình sao (Star Topology) ..... 37
4.1.2 Mạng hình tuyến (Bus Topology) ..... 38
4.1.3 Mạng dạng vòng (Ring Topology) ..... 38
4.1.4 Mạng dạng kết hợp ..... 39
**4.2 Các giao thức điều khiển truy nhập đường truyền ..... 39**
4.2.1 Phương pháp CSMA ..... 40
4.2.2 Phương pháp CSMA/CD ..... 41
4.2.3 Điều khiển truy nhập bus với thẻ bài ..... 41
4.2.4 Điều khiển truy nhập vòng với thẻ bài ..... 43
**4.3 Chuẩn hóa mạng cục bộ ..... 44**
4.3.1 Chuẩn Ethernet ..... 46
***Chương 5 TẦNG MẠNG 47***
**5.1 Các vấn đề của tầng mạng ..... 47**
5.1.1 Định địa chỉ cho tầng mạng ..... 47
5.1.2 Dịch vụ cung cấp cho tầng giao vận ..... 48
5.1.3 Tổ chức các kênh truyền tin trong tầng mạng ..... 49
5.1.4 Tìm đường đi trong mạng ..... 50
5.1.5 Tắc nghẽn trong mạng ..... 51

**5.2 Kết nối liên mạng ..... 51**
5.2.1 Các thiết bị dùng để kết nối liên mạng ..... 52
**5.3 Giao thức liên mạng IP ..... 58**
5.3.1 Cấu trúc khung tin IP ..... 59
5.3.2 Địa chỉ IP ..... 64
**5.4 Phân chia mạng con ..... 66**
**5.5 Hoạt động của giao thức IP ..... 67**
**5.6 Các giao thức liên quan đến IP ..... 68**
5.6.1 Giao thức phân giải địa chỉ ARP ..... 68
5.6.2 Giao thức RARP (Reverse Address Resolution Protocol) ..... 71
5.6.3 Giao thức ICMP ..... 71
**5.7 Phiên bản IPv6 ..... 76**
5.7.1 Khung tin IPng v6 ..... 77
**5.8 Định tuyến trên Internet ..... 77**
5.8.1 Bảng chọn đường ..... 77
5.8.2 Xây dựng bảng chọn đường cho các Router/Gateway ..... 78
**5.9 Mạng X.25 ..... 80**
5.9.1 Cơ sở kỹ thuật ..... 80
**5.10 Kỹ thuật FRAME RELAY ..... 82**
5.10.1 Khuôn dạng gói dữ liệu Frame-Relay ..... 82
***Chương 6 TẦNG GIAO VẬN 84***
**6.1 Các vấn đề của tầng giao vận ..... 84**
6.1.1 Cung cấp dịch vụ cho tầng phiên ..... 84
6.1.2 Chất lượng dịch vụ QoS ..... 86
6.1.3 Các lớp giao thức của tầng giao vận ..... 87
6.1.4 Thủ tục giao vận trên X. 25 ..... 90
***Chương 7 HỌ GIAO THỨC TCP/IP 91***
**7.1 Mô hình TCP/IP ..... 91**
**7.2 Giao thức TCP ..... 93**
7.2.1 Khuôn dạng gói tin TCP ..... 94
7.2.2 Quá trình nối-tách ..... 96
7.2.3 Quá trình trao đổi dữ liệu ..... 97
7.2.4 Thứ tự thực hiện ứng dụng TCP/IP ..... 97
**7.3 Giao thức UDP ..... 100**
**7.4 Cổng và Socket ..... 101**

7.4.1 Số hiệu cổng ..... 101
7.4.2 Socket ..... 101
**7.5 Mô hình giao tiếp Client/Server ..... 103**
7.5.1 Quá trình trao đổi dữ liệu dùng Stream Socket ..... 103
7.5.2 Quá trình trao đổi dữ liệu dùng Datagram Socket ..... 104
7.5.3 Ví dụ chương trình client/server ..... 105
***Chương 8 TẦNG PHIÊN 108***
**8.1 Dịch vụ OSI cho tầng Phiên ..... 108**
8.1.1 Cung cấp cho người sử dụng dịch vụ tầng phiên (SS-user) ..... 108
8.1.2 Điều khiển trao đổi dữ liệu ..... 109
8.1.3 Điều hành phiên làm việc ..... 110
8.1.4 Liên kết phiên ..... 111
**8.2 Giao thức chuẩn tầng phiên ..... 111**
8.2.1 Các loại SPDU, các tham số và chức năng ..... 112
***Chương 9 TẦNG TRÌNH DIỄN 114***
**9.1 Vai trò và chức năng ..... 114**
9.1.1 Phiên dịch dữ liệu ..... 116
**9.2 Dịch vụ OSI cho tầng trình diễn ..... 116**
**9.3 Giao thức chuẩn tầng trình diễn ..... 117**
9.3.1 Các chuẩn khác cho tầng trình diễn ..... 118
***Chương 10 TẦNG ỨNG DING 119***
**10.1 An toàn thông tin trên mạng ..... 119**
10.1.1 Các chiến lược an toàn hệ thống ..... 119
10.1.2 An toàn thông tin bằng mã hóa ..... 120
**10.2 CáC phương pháp mã hóa dữ liệu ..... 122**
10.2.1 Phương pháp hoán vị ..... 122
10.2.2 Phương pháp thay thế ..... 123
10.2.3 Phương pháp mã hóa chuẩn DES ..... 124
10.2.4 Phương pháp mã hoá khoá công khai ..... 128
**10.3 Cơ chế bảo vệ bằng firewall ..... 132**
10.3.1 Các loại firewall và cơ chế hoạt động ..... 134
**10.4 Hệ thống tên miền DNS (Domain Name System ) ..... 137**
10.4.1 Không gian tên miền DNS ..... 138
10.4.2 Máy chủ quản lý tên ..... 140
10.4.3 Chương trình phân giải tên ..... 140

**10.5 Hệ quản trị mạng ..... 140**
10.5.1 Hệ bị quản trị ..... 141
10.5.2 Cơ sở dữ liệu chứa thông tin quản trị mạng ..... 141
**10.6 Dịch vụ thư điện tử ..... 142**
10.6.1 Giao thức SMTP ..... 143
10.6.2 MIME ..... 147
10.6.3 Giao thức POP ..... 151
**10.7 Dịch vụ truy cập từ xa - TELNET ..... 154**
10.7.2 Dịch vụ truyền tập tin FTP ..... 156
10.7.3 UserNEWS ..... 162
10.7.4 WORLD-WIDE-WEB ..... 163

*Chương 1*

# MỞ ĐẦU

## 1.1 Giới thiệu

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

Mạng máy tính bao gồm phần cứng, các giao thức và các phần mềm mạng.

Khi nghiên cứu về mạng máy tính, các vấn đề quan trọng được xem xét là giao thức mạng, cấu hình kết nối của mạng, và các dịch vụ trên mạng.

Mạng máy tính có những công dụng như sau :

1. *Tập trung tài nguyên tại một số máy và chia sẻ cho nhiều máy khác*

- Nhiều người có thể dùng chung một phần mềm tiện ích.
- Dữ liệu được quản lý tập trung nên an toàn hơn, trao đổi giữa những người sử dụng thuận lợi hơn, nhanh chóng hơn.
- Mạng máy tính cho phép người lập trình ở một trung tâm máy tính này có thể sử dụng các chương trình tiện ích của một trung tâm máy tính khác đang rỗi, sẽ làm tăng hiệu quả kinh tế của hệ thống.

2. *Khắc phục sự trở ngại về khoảng cách địa lý.*
3. *Tăng chất lượng và hiệu quả khai thác thông tin.*
4. *Cho phép thực hiện những ứng dụng tin học phân tán*
5. *Độ an toàn tin cậy của hệ thống tăng lên nhờ khả năng thay thế khi có sự cố với máy có sự cố :* An toàn cho dữ liệu và phần mềm vì phần mềm mạng sẽ khoá các tập tin khi có những người không đủ quyền hạn truy xuất các tập tin và thư mục đó.
6. *Phát triển các công nghệ trên mạng:* Người sử dụng có thể trao đổi thông tin với nhau dễ dàng và sử dụng hệ mạng như là một công cụ để phổ biến tin tức, thông báo về một chính sách mới, về nội dung buổi họp, về các thông tin kinh tế khác như giá cả thị trường, tin rao vặt (muốn bán hoặc muốn mua một cái gì đó), hoặc sắp xếp thời khoá biểu của mình chen lẫn với thời khoá biểu của những người khác , . . .

## 1.2 Phân loại mạng

### 1.2.1 Dựa theo khoảng cách địa lý

Mạng máy tính có thể phân bổ trên một khu vực nhất định hoặc có thể trong một quốc gia hay toàn cầu. Dựa vào phạm vi phân bố, người ta có thể phân ra các loại mạng như sau:

a. LAN (Local Area Network - Mạng cục bộ) : LAN thường được sử dụng trong nội bộ một cơ quan/tổ chức..., kết nối các máy tính trong một khu vực bán kính khoảng 100m-10km. Kết nối được thực hiện thông qua các môi trường truyền thông tốc độ cao, ví dụ cáp đồng trục hay cáp quang.

b. MAN (Metropolitan Area Network - Mạng đô thị) : Kết nối các máy tính trong phạm vi một thành phố. Kết nối này được thực hiện thông qua các môi trường truyền thông tốc độ cao (50-100 Mbit/s).

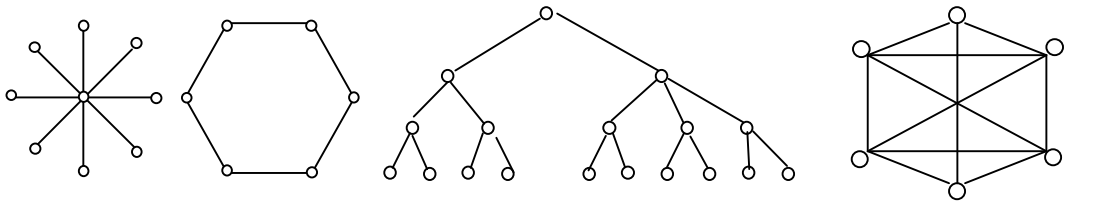
c. WAN (Wide Area Network) - Mạng diện rộng, kết nối máy tính trong nội bộ các quốc gia hay giữa các quốc gia trong cùng một châu lục. Thông thường kết nối này được thực hiện thông qua mạng viễn thông. Các WAN có thể được kết nối với nhau thành GAN hay tự nó đã là GAN.

d. GAN (Global Area Network) : Mạng toàn cầu, kết nối máy tính từ các châu lục khác nhau. Thông thường kết nối này được thực hiện thông qua mạng viễn thông và vệ tinh.

Trong các khái niệm nói trên, WAN và LAN là hai khái niệm hay được sử dụng nhất.

### 1.2.2 Dựa theo cấu trúc mạng

#### *1.2.2.1 Kiểu điểm - điểm (point - to - point)*



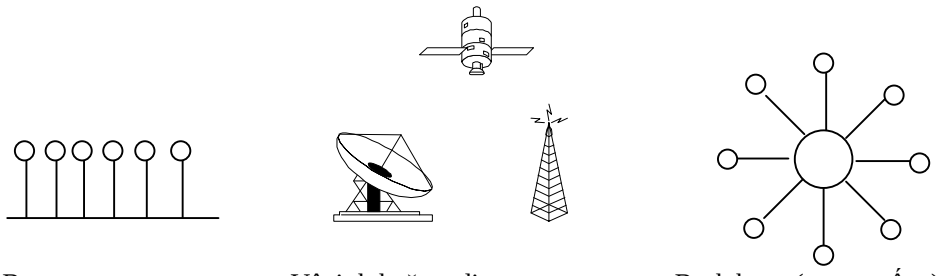
*H×nh sao* *Chu tr×nh* *H×nh c©y* *D¹ng ®Çy ®ñ*

Hình 1-1. Cấu trúc mạng kiểu điểm-điểm.

Đường truyền nối từng cặp nút mạng với nhau. Thông tin đi từ nút nguồn qua nút trung gian rồi gởi tiếp nếu đường truyền không bị bận. Do đó còn có tên là mạng lưu trữ và chuyển tiếp (*store and forward*).

#### *1.2.2.2 Kiểu khuyếch tán*

Bản tin được gởi đi từ một nút nào đó sẽ được tiếp nhận bởi các nút còn lại (còn gọi là broadcasting hay point to multipoint). Trong bản tin phải có vùng địa chỉ cho phép mỗi nút kiểm tra xem có phải tin của mình không và xử lý nếu đúng bản tin được gởi đến.




Hình 1-2. Sơ đồ kết nối theo kiểu khuyếch tán.

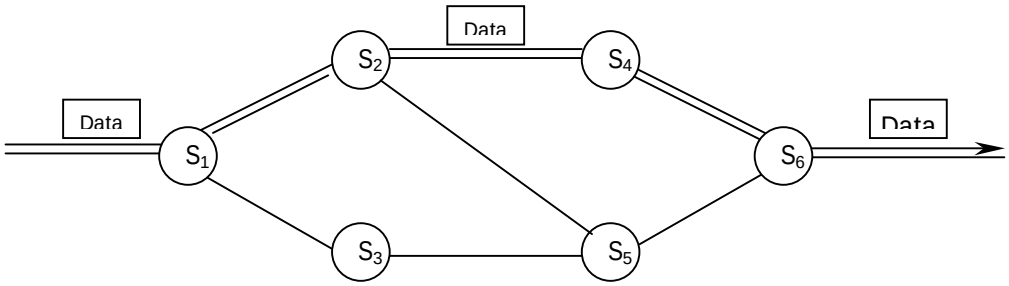
Trong cấu trúc dạng Bus và Vòng cần cơ chế "*trọng tài*" để giải quyết các xung đột (collision) xảy ra khi nhiều nút muốn truyền tin đồng thời. Trong cấu trúc vệ tinh hoặc radio, mỗi nút cần có ăng-ten thu và phát.

### 1.2.3 Theo phương pháp chuyển mạch

- Mạng chuyển mạch kênh (Line switching network), ví dụ như mạng điện thoại.
- Mạng chuyển mạch thông báo (Message switching network)
- Mạng chuyển mạch gói (Packet switching network)

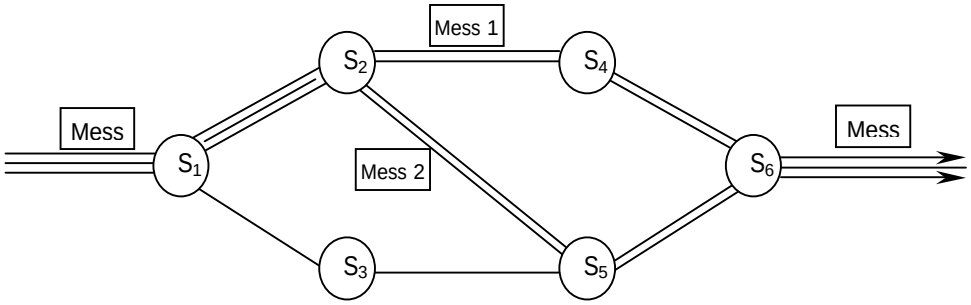
#### *1.2.3.1 Chuyển mạch kênh*

Chuyển mạch kênh (line switching) được dùng trong mạng điện thoại. Một kênh cố định được thiết lập giữa cặp thực thể cần liên lạc với nhau. Mạng này có hiệu suất không cao vì có lúc kênh bỏ không.




Hình 1-3. Mạng chuyển mạch kênh.

### *1.2.3.2 Mạng chuyển mạch bản tin*




Hình 1-4. Phương pháp chuyển mạch thông báo.

Các nút của mạng căn cứ vào địa chỉ đích của "bản tin" để chọn nút kế tiếp. Như vậy các nút cần lưu trữ và đọc tin nhận được, quản lý việc truyền tin. Trong trường hợp bản tin quá dài và nếu sai phải truyền lại thì hiệu suất không cao. Phương pháp này giống như cách gởi thư thông thường.

- Ưu điểm so với phương pháp chuyển mạch kênh:

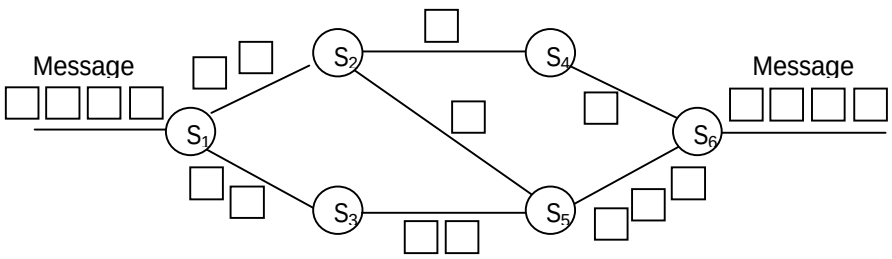
- Hiệu suất sử dụng đường truyền cao vì không bị chiếm dụng độc quyền mà được phân chia giữa nhiều thực thể.
- Mỗi nút mạng (hay nút chuyển mạch thông bao) có thể lưu trữ message cho tới khi kênh truyền rỗi mới gửi bản tin đi. Do đó giảm được tình trạng tắc nghẽn (congestion) trên mạng.
- Điều khiển việc truyền tin bằng cách sắp xếp độ ưu tiên cho các bản tin.
- Có thể tăng hiệu suất sử dụng giải thông của mạch bằng cách gán địa chỉ quảng bá (broadcast) để gởi bản tin đồng thời đến nhiều đích.

- Nhược điểm:

- Do không hạn chế kích thước của bản tin nên có thể dẫn đến phí tổn lưu trữ tạm thời cao và ảnh hưởng đến thời gian hồi đáp và chất lượng truyền đi.

Mạng chuyển mạch thông báo thích hợp với các dịch vụ thông tin kiểu thư điện tử (Email) hơn là đối với các ứng dụng có tính thời gian thực vì tồn tại độ trễ nhất định do lưu trữ và xử lý thông tin điều khiển tại mỗi nút.

### *1.2.3.3 Mạng chuyển mạch gói*




Hình 1-5. Mạng chuyển mạch gói.

Bản tin được chia thành nhiều gói tin (packet) độ dài 512 bytes, phần đầu là địa chỉ đích, mã để tập hợp các gói. Các gói của các bản tin khác nhau có thể được truyền độc lập trên cùng một đường truyền. Vấn đề phức tạp ở đây là tạo lại bản tin ban đầu, đặc biệt khi được truyền trên các con đường khác nhau.

Chuyển mạch gói mềm dẻo, hiệu suất cao. Xu hướng phát triển hiện nay là sử dụng hai kỹ thuật chuyển mạch kênh và chuyển mạch gói trong cùng một mạng thống nhất gọi là mạng ISDN (*Integrated Services Digital Network* - Mạng thông tin số đa dịch vụ).

## 1.3 Kiến trúc phân tầng và chuẩn hoá mạng

Tình trạng không tương thích giữa các mạng đặc biệt là các mạng trên thị trường gây trở ngại cho những người sử dụng khác nhau. Do đó cần phải xây dựng mô hình chuẩn làm cơ sở cho các nhà nghiên cứu thiết kế mạng để tạo ra các sản phẩm mới về mạng, dễ phổ cập, sản xuất, sử dụng. Các chuẩn có vai trò quan trọng trong công tác thiết kế và xây dựng các hệ thống kỹ thuật và công nghệ.

*Chuẩn hóa mạng máy tính là nêu ra các tiêu chuẩn cơ bản thống nhất về cấu trúc mạng giúp cho các mạng khác nhau có thể trao đổi thông tin được với nhau.*

Để mạng hoạt động đạt khả năng tối đa, các tiêu chuẩn được chọn phải cho phép mở rộng mạng để có thể phục vụ những ứng dụng không dự kiến trước trong tương lai tại lúc lắp đặt hệ thống và điều đó cũng cho phép mạng làm việc với những thiết bị được sản xuất từ nhiều hãng khác nhau.

### 1.3.1 Các tổ chức chuẩn hoá mạng

Hai tổ chức chính thực hiện chuẩn hóa mạng là ISO và CCTTT.

1. ISO (*International Standards Organization*) - Tổ chức chuẩn hóa quốc tế. ISO hoạt động dưới sự bảo trợ của LHQ. Thành viên của ISO là các cơ quan tiêu chuẩn hóa của các quốc gia và các Ban chuyên môn. Ban TC97 được chia ra thành các tiểu ban và các nhóm công tác.
2. IEEE (*Institute of Electrical and Electronic Engineers*) - Viện nghiên cứu các vấn đề về kỹ thuật điện và điện tử của Mỹ. IEEE chịu trách nhiệm về tầng Data Link và Physical. Phân ban các chuẩn này là phân ban 802 (thành lập tháng Hai năm 1980).
3. CCITT (*Commité Consultatif Internatinal pour Télégraphe et Téléphone*) - Tổ chức tư vấn quốc tế về điện báo và điện thoại hoạt động dưới sự bảo trợ của LHQ, chuyên nghiên cứu nhằm công bố các khuyến nghị thống nhất về mạng

máy tính. Bao gồm các khuyến nghị liên quan đến việc truyền dữ liệu trên mạng, mạng ISDN.

4. ANSI (*American National Standards Institute*) :Viện nghiên cứu các chuẩn quốc gia của Mỹ.
5. ECMA (*European Computer Manufactures Association*) : Hiệp hội máy tính châu âu
6. ATM Forum (*Asynchronous Transfers Mode*) - Thực hiện các giải pháp cho mạng ISDN.
7. IETF (*Internet Enggineering Task Force*) : Sản xuất các chuẩn liên quan đến Internet (SNMP, TCP/IP ...)

### 1.3.2 Kiến trúc phân tầng

Để giảm độ phức tạp thiết kế, kiến trúc mạng được tổ chức thành một cấu trúc đa tầng, mỗi tầng được xây trên tầng trước nó, tầng dưới sẽ cung cấp dịch vụ cho tầng cao hơn. Tầng N trên một máy thực hiện việc giao tiếp với tầng N trên một máy khác. Các qui tắc, luật lệ được sử dụng cho việc giao tiếp này được gọi là các giao thức của tầng N.

Các thực thể (entity) nằm trên các tầng tương ứng trên những máy khác nhau gọi là các tiến trình đồng mức. Các tiến trình đồng mức giao tiếp với nhau bằng cách sử dụng các giao thức trong tầng của nó.

Giữa 2 tầng kề nhau tồn tại một giao diện (*interface*) xác định các hàm nguyên thủy và các dịch vụ tầng dưới cung cấp cho tầng trên.

Tập hợp các tầng và các giao thức được gọi là kiến trúc mạng (*Network Architecture*).

Cấu trúc phân tầng của mạng máy tính có ý nghĩa đặc biệt như sau :

- Thuận tiện trong công tác thiết kế, xây dựng và cài đặt các mạng máy tính, trong đó mỗi hệ thống thành phần được xem như là một cấu trúc đa tầng.
- Mỗi tầng được xây dựng dựa trên cơ sở tầng kề liền trước đó. Như vậy tầng dưới sẽ cung cấp dịch vụ cho tầng trên.
- Số lượng, tên gọi và chức năng của mỗi tầng sẽ được người thiết kế mạng máy tính cụ thể quy định.
- Tập hợp các giao thức, các vấn đề kỹ thuật và công nghệ cho mỗi tầng có thể được khảo sát, nghiên cứu triển khai độc lập với nhau.

- Giao thức : Mỗi khi trao đổi thông tin như điện thoại, telex, viết . . . người ta phải tuân theo một số quy luật. Các quy luật này được nhóm lại và gọi là giao thức (*protocol*).

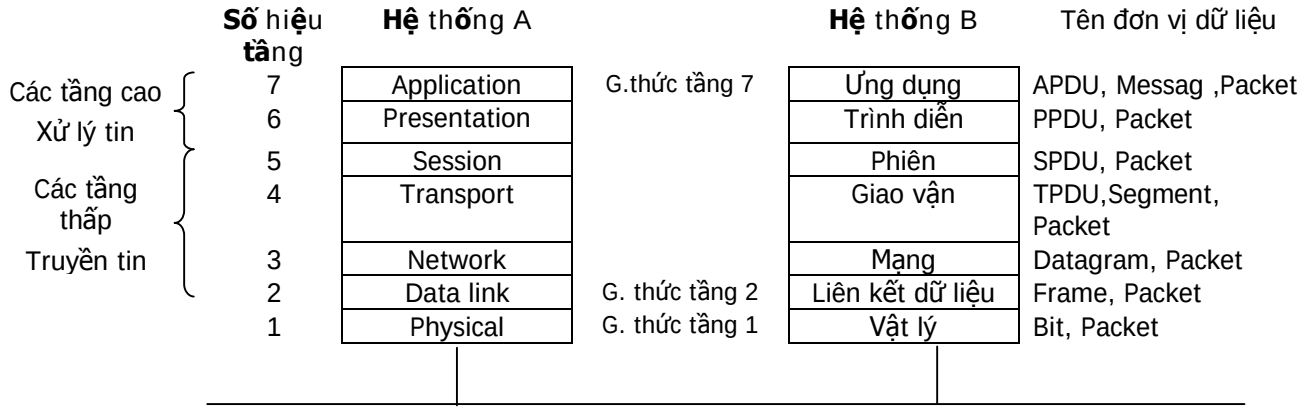
Giao thức có các chức năng chính như sau :

1. Định nghĩa cấu trúc khung một cách chính xác cho từng byte, các ký tự và bản tin.
2. Phát hiện và xử lý các lỗi, thông thường là gửi lại bản tin gốc sau khi phát hiện lần trước bị lỗi
3. Quản lý thứ tự các lệnh để đếm các bản tin, nhận dạng, tránh mất hoặc thu thừa bản tin.
4. Đảm bảo không nhầm lẫn giữa bản tin và lệnh
5. Chỉ ra các thuộc tính đường dây khi lập các đường nối đa điểm hoặc bán song công (cho biết ai đối thoại với ai).
6. Giải quyết vần đề xung đột thâm nhập (yêu cầu đồng thời), gửi khi chưa có số liệu, mất liên lạc, khởi động.

## 1.4 Mô hình OSI

### 1.4.1 Kiến trúc của mô hình OSI

Dựa trên kiến trúc phân tầng, ISO đã đưa ra mô hình 7 tầng (layer) cho mạng, gọi là mô hình kết nối hệ thống mở hoặc mô hình OSI (Open Systems Interconnection model), vào năm 1984.




Hình 1-6. Mô hình OSI 7 tầng.

Nhóm các tầng thấp (*physical, data link, network, transport*) liên quan đến các phương tiện cho phép truyền dữ liệu qua mạng. Các tầng thấp đảm nhiệm việc truyền dữ liệu, thực hiện quá trình đóng gói, dẫn đường, kiểm duyệt và truyền từng nhóm dữ liệu. Các tầng này không cần quan tâm đến loại dữ liệu mà nó nhận được từ hay gửi cho tầng ứng dụng, mà chỉ đơn thuần là gửi chúng đi.

Nhóm các tầng cao (*session, presentation, application*) liên quan chủ yếu đến việc đáp ứng các yêu cầu của người sử dụng để triển khai các ứng dụng của họ trên mạng thông qua các phương tiện truyền thông cung cấp bởi các nhóm tầng thấp.

Hệ thống kết nối mở OSI là hệ thống cho phép truyền thông tin với các hệ thống khác, trong đó các mạng khác nhau, sử dụng những giao thức khác nhau, có thể thông báo cho nhau thông qua chương trình để chuyển từ một giao thức này sang một giao thức khác.

Mô hình OSI đưa ra giải pháp cho vấn đề truyền thông giữa các máy tính không giống nhau. Hai hệ thống, dù khác nhau đều có thể truyền thông với nhau một cách hiệu quả nếu chúng đảm bảo những điều khiển chung sau đây :

1. Các hệ thống đều cài đặt cùng một tập hợp các chức năng truyền thông.
2. Các chức năng đó được tổ chức thành cũng một tập các tầng. Các tầng đồng mức phải cung cấp các chức năng như nhau, nhưng phương thức cung cấp không nhất thiết phải giống nhau.
3. Các tầng đồng mức phải sử dụng một giao thức chung.

Để đảm bảo những điều trên cần phải có các chuẩn xác định các chức năng và dịch vụ được cung cấp bởi một tầng (nhưng không cần chỉ ra chúng phải cài đặt như thế nào). Các chuẩn cũng phải xác định các giao thức giữa các tầng đồng mức. Mô hình OSI chính là cơ sở để xây dựng các chuẩn đó.

### 1.4.2 Sự ghép nối giữa các mức

Trong thực tế dữ liệu không truyền trực tiếp từ tầng i máy này sang tầng i máy kia (trừ tầng thấp nhất). tầng thấp nhất có đường truyền thông vật lý tới tầng thấp nhất của máy tương ứng từ đó dữ liệu và thông tin điều khiển lại được chuyển ngược lên tầng trên. Tầng trên chỉ xác định đường truyền thông lôgic (truyền thông ảo).

- Các Header của giao thức : Thông thường, thông tin điều khiển giao thức được gói thành một khối và được đặt trước dữ liệu nó đi kèm và được gọi là *Header* hay *Protocol Header*, được dùng để truyền thông tin giữa các tầng và giữa các máy tính với nhau. Các header của giao thức được phát triển theo các luật được cho trong tập tài liệu ASN.1 của ISẶ.
- Khi máy A gửi tin đi, các đơn vị dữ liệu đi từ tầng trên xuống dưới. Qua mỗi tầng nó được bổ sung thông tin điều khiển của tầng đó.
- Khi nhận tin, thông tin đi từ dưới lên. Qua mỗi tầng thông tin điều khiển được khử bỏ dần và cuối cùng máy B nhận được bản tin của A.

### 1.4.3 Chức năng của mỗi tầng

***1. Tầng Vật lý***

Cung cấp phương tiện truyền tin, thủ tục khởi động, duy trì huỷ bỏ các liên kết vật lý. Giữ nhiệm vụ chuyển tải các bit thông tin trên kênh truyền thông. Tầng Vật lý làm việc với các giao diện cơ, điện và giao diện thủ tục (chức năng) trên môi trường vật lý, không quan tâm đến nội dung biểu diễn của các bit.

Thực chất tầng này thực hiện nối liền các phần tử của mạng thành một hệ thống bằng các phương pháp vật lý, ở mức này sẽ có các thủ tục đảm bảo cho các yêu cầu về chuyển mạch hoạt động nhằm tạo ra các đường truyền thực cho các chuỗi bit thông tin.

***2. Tầng liên kết dữ liệu***

Thiết lập, duy trì, huỷ bỏ các liên kết dữ liệu kiểm soát luồng dữ liệu, phát hiện và khắc phục sai sót truyền tin

Tiến hành chuyển đổi thông tin dưới dạng chuỗi các bit ở mức mạng thành từng đoạn gọi là khung tin (frame). Sau đó đảm bảo truyền liên tiếp các khung tin tới tầng vật lý, đồng thời xử lý các thông báo từ trạm thu gửi trả lại. Bit thông tin trong khung tin đều mang những ý nghĩa riêng, bao gồm các *trường địa chỉ, trường kiểm tra, dữ liệu và kiểm tra lỗi* dùng cho các mục đích riêng.

Nhiệm vụ chính của mức 2 này là khởi tạo, tổ chức các khung tin và xử lý các thông tin liên quan tới khung tin.

***3. Tầng mạng***

Tầng mạng được xây dựng dựa trên kiểu nối kết *điểm - điểm* do tầng LKDL cung cấp, bảo đảm trao đổi thông tin giữa các mạng con trong một mạng lớn, mức này còn được gọi là mức thông tin giữa các mạng con với nhau.

Có nhiệm vụ gán địa chỉ cho các bản tin và chuyển đổi địa chỉ logic hay các tên thành các địa chỉ vật lý.

Thực hiện chọn đường truyền tin, cung cấp dịch vụ định tuyến (chọn đường) cho các gói dữ liệu trên mạng. Tầng này chỉ ra dữ liệu từ nguồn tới đích sẽ đi theo tuyến nào trên cơ sở các điều kiện của mạng, độ ưu tiên dịch vụ và các nhân tố khác.

Kiểm soát luồng dữ liệu, khắc phục sai sót, cắt/hợp dữ liệu, giúp loại trừ sự tắc nghẽn cũng như điều khiển luồng thông tin.

***4. Tầng Giao vận***

Tầng giao vận giúp đảm bảo độ tin cậy khi chuyển giao dữ liệu và tính toàn vẹn dữ liệu từ nơi gửi đến nơi nhận. Điều này được thực hiện dựa trên cơ chế kiểm tra lỗi do các tầng bên dưới cung cấp. Tầng giao vận còn chịu trách nhiệm tạo ra nhiều kết nối cục bộ trên cùng một kết nối mạng gọi là ghép kênh (multiplexing), phân chia thời gian xử lý (time sharing), cắt hợp dữ liệu.

Nhiệm vụ của mức này là xử lý các thông tin để chuyển tiếp các chức năng từ tầng phiên đến tầng mạng và ngược lại. Thực chất mức truyền này là để đảm bảo thông tin giữa các máy chủ với nhau. Mức này nhận các thông tin từ tầng phiên, phân chia thành các đơn vị dữ liệu nhỏ hơn và chuyển chúng tới mức mạng.

### *5. Tầng phiên*

Thiết lập, duy trì, đồng bộ hoá và huỷ bỏ các phiên truyền thông. Liên kết phiên phải được thiết lập thông qua đối thoại và trao đổi các thông số điều khiển.

Dùng tầng giao vận để cung cấp các dịch vụ nâng cao cho phiên làm việc như: kiểm soát các cuộc hội thoại, quản lý thẻ bài (*token*), quản lý hoạt động (*activity management*).

Nhận dạng tên và thủ tục cần thiết cũng như là các công việc bảo mật, để hai ứng dụng có thể giao tiếp với nhau trên mạng. Nhờ tầng phiên, những người sử dụng lập được các đường nối với nhau, khi cuộc hội thoại được thành lập thì mức này có thể quản lý cuộc hội thoại đó theo yêu cầu của người sử dụng. Một kết nối giữa hai máy cho phép người sử dụng được đăng ký vào một hệ thống phân chia thời gian từ xa hoặc chuyển tập tin giữa 2 máy.

### *6. Tầng trình diễn*

Quản lý cách thức biểu diễn thông tin theo cú pháp dữ liệu của người sử dụng, loại mã sử dụng (ASCII, QBCDIC, ...) và thực hiện các vấn đề nén dữ liệu.

Nhiệm vụ của mức này là lựa chọn cách tiếp nhận dữ liệu, biến đổi các ký tự, chữ số của mã ASCII hay các mã khác và các ký tự điều khiển thành một kiểu mã nhị phân thống nhất để các loại máy khác nhau đều có thể thâm nhập vào hệ thống mạng.

### *7. Tầng ứng dụng*

Tầng này là giao diện giữa người sử dụng và môi trường hệ thống mở.

Tầng này có nhiệm vụ phục vụ trực tiếp cho người sử dụng, cung cấp tất cả các yêu cầu phối ghép cần thiết cho người sử dụng, yêu cầu phục vụ chung như chuyển các File, sử dụng các Terminal của hệ thống,.... Mức sử dụng bảo đảm tự động hoá quá trình thông tin, giúp cho người sử dụng khai thác mạng tốt nhất.

### 1.4.4 Các giao thức chuẩn của OSI

#### *1.4.4.1 Các hàm nguyên thủy*

Mỗi thực thể truyền thông với các thực thể ở tầng trên và dưới nó qua một *giao diện* (interface). Giao diện này gồm một hoặc nhiều điểm truy cập dịch vụ (SAP - Service Access Point). Thực thể tầng N-1 cung cấp dịch vụ cho thực thể tầng N thông qua việc gọi các hàm dịch vụ nguyên thủy (primitive).

Hàm nguyên thuỷ chỉ rõ chức năng cần thực hiện và được dùng để chuyển dữ liệu và thông tin điều khiển. Bốn hàm nguyên thuỷ được sử dụng để định nghĩa tương tác giữa các tầng kề nhau như sau :

| | |
|---|---|
| request | *Ịêu cầu* |
| indication | *Chỉ báo* |
| response | *Trả lời* |
| confirm | *Xác nhận* |

*request* được gởi bởi người sử dụng dịch vụ ở tầng N+1 trong hệ thống A để gọi thủ tục của giao thức ở tầng N. Ịêu cầu này được cấu tạo dưới dạng một hoặc nhiều đơn vị dữ liệu giao thức (PDU - *Protocol Data Unit*) để gởi tới B.

Khi nhận được PDU, một thủ tục của giao thức ở tầng N của B sẽ thông báo yêu cầu đó lên tầng N+1 bằng hàm nguyên thủy *indication*. Sau đó *response* được gởi từ N + 1 của B xuống N gọi thủ tục giao thức tầng N để trả lời tới A.

Khi nhận được trả lời này một thủ tục giao thức tầng N sẽ gởi hàm *confirm* lên N+1 để hoàn tất chu trình yêu cầu thiết lập liên kết của người sử dụng ở tầng N+1 của A.

Các chu trình của người sử dụng khác nhau được phân biệt nhờ khái niệm điểm thâm nhập dịch vụ (SAP - *Service Access Point*) ở ranh giới của 2 tầng N + 1 và N.

#### *1.4.4.2 Các phương thức truyền thông*

Tại mỗi tầng trong mô hình OSI có 2 phương thức hoạt động chính được sử dụng : phương thức có liên kết (*connection oriented*) và phương thức không liên kết (*connectionless*).

Với các phương thức truyền không liên kết thì chỉ có một giai đoạn truyền dữ liệu. Các gói tin dữ liệu (còn được gọi là datagram) được truyền độc lập với nhau theo một con đường xác định dần bằng địa chỉ đích được đặt trong mỗi datagram. Có 3 giai đoạn phân biệt :

- *Thiết lập liên kết* : hai thực thể cùng tầng ở hai đầu của liên kết sẽ thương lượng với nhau về tập các tham số sử dụng trong giai đoạn truyền dữ liệu.
- *Truyền dữ liệu* : các cơ chế kiểm soát sai sót, luồng dữ liệu, ghép kênh, cắt hợp dữ liệu được thực hiện để tăng cường độ tin cậy và hiệu suất của việc truyền dữ liệu.
- *Kết thúc truyền* : giải phóng các tài nguyên hệ thống đã được cấp phát cho liên kết để dùng vào mục đích khác.

Tương ứng với 3 giai đoạn trao đổi trên, có 3 loại thủ tục cơ bản được sử dụng : CONNECT, DATA, DISCONNECT.

Ví dụ đối với giao thức tầng N ta có các thủ tục :

| | |
|---|---|
| N_CONNECT | Thiết lập liên kết |
| N_DATA | Truyền dữ liệu |
| N_DISCONNECT | Huỷ bỏ liên kết |

Ngoài ra có một số các thủ tục phụ được sử dụng tuỳ theo chức năng của mỗi tầng.

| | | |
|---|---|---|
| *Ví dụ:* | Thủ tục N_RESTART | Dùng để khởi động lại hệ thống ở tầng 3 |
| | Thủ tục T_EXPEDITED_DATA | Dùng cho việc truyền dữ liệu nhanh tầng 4 |
| | Thủ tục S_TOKEN_GIVE | Dùng để chuyển điều khiển ở tầng 5 |

Mỗi thủ tục trên sẽ dùng các hàm nguyên thuỷ (*request, indication, response, confirm*) để tạo thành các hàm cơ bản của mô hình OSI.

## 1.5 Hệ điều hành mạng

Việc lựa chọn hệ điều hành mạng (NOS - Network Operating System) làm nền tảng cho mạng tuỳ thuộc vào kích cỡ của mạng hiện tại và sự phát triển trong tương lai, ngoài ra còn tuỳ thuộc vào những ưu điểm và nhược điểm của từng hệ điều hành.

Một số hệ điều hành mạng phổ biến hiện nay:

- Hệ điều hành mạng UNIX: Đây là hệ điều hành do các nhà khoa học xây dựng và được dùng rất phổ biến trong giới khoa học, giáo dục. Hệ điều hành mạng UNIX là hệ điều hành đa nhiệm, đa người sử dụng, phục vụ cho truyền thông tốt. Nhược điểm của nó là hiện nay có nhiều Version khác nhau, không thống nhất gây khó khăn cho người sử dụng và là hệ điều hành này phức tạp.
- Hệ điều hành mạng Windows 2000: Đây là hệ điều hành của hãng Microsoft, cũng là hệ điều hành đa nhiệm, đa người sử dụng. Được xây dựng dựa trên công nghệ của hệ điều hành Windows NT. Đặc điểm của nó là tương đối dễ sử dụng, hỗ trợ mạnh cho các phần mềm WINDOWS. Windows 2000 có thể

liên kết tốt với máy chủ Novell Netware, Unix. Tuy nhiên, để chạy có hiệu quả, Windows 2000 Server đòi hỏi cấu hình máy tương đối mạnh.

- Hệ điều hành mạng NetWare của Novell: Đây là hệ điều hành phổ biến trên thế giới trong thời gian cuối, nó có thể dùng cho các mạng nhỏ (khoảng từ 5-25 máy tính) và cũng có thể dùng cho các mạng lớn gồm hàng trăm máy tính. Netware là một hệ điều hành LAN dùng cho các máy tính theo chuẩn của IBM hay các máy tính Apple Macintosh, chạy trên hệ điều hành MS-DOS hoặc OS/2.

## 1.6 Mạng Internet

### 1.6.1 Lịch sử ra đời và phát triển

Vào những năm 60, Bộ Quốc phòng Mỹ cho triển khai khẩn trương một mạng lưới thông tin với yêu cầu: Nếu như một trạm trung chuyển nào đó trong mạng bị phá huỷ, toàn bộ hệ thống thông tin vẫn phải làm việc bình thường... Cơ quan Nghiên cứu Dự án Cao cấp (ARPA - Advanced Research Projects Agency) thuộc Bộ Quốc phòng Mỹ được giao trách nhiệm thực hiện việc nghiên cứu kỹ thuật liên mạng (internet) nhằm đáp ứng yêu cầu trên. Đây là mạng chuyển mạch gói (packet switching) đầu tiên trên thế giới, lấy tên là ARPAnet. Ban đầu, ARPAnet chỉ gồm một vài mạng nhỏ được chọn lựa của các trung tâm nghiên cứu và phát triển khoa học. Giao thức truyền thông lúc bấy giờ là kiểu điểm - điểm, rất chậm và thường xuyên gây tắc nghẽn trên mạng. Để giải quyết vấn đề này, vào năm 1974 Vinton G. Cerf và Robert O. Kahn đưa ra ý tưởng thiết kế một bộ giao thức mạng mới thuận tiện hơn, đó chính là tiền thân của giao thức TCP/IP.

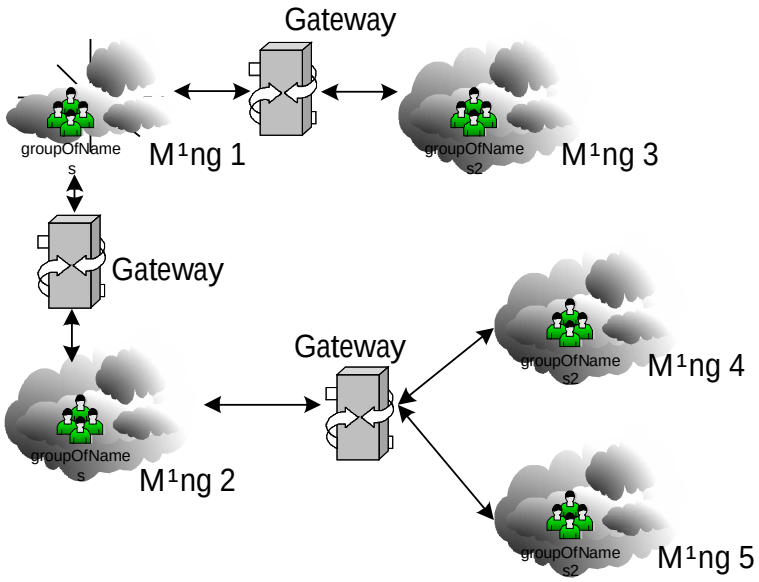
Tháng 09/1983, dưới sự tài trợ của Bộ Quốc phòng Mỹ, Berkeley Software Distribution đưa ra bản Berkeley UNIX 4.2BSD có kết hợp giao thức TCP/IP, biến TCP/IP thành phương tiện kết nối các hệ thống UNIX. Trên cơ sở đó, mạng ARPANỌT nhanh chóng lan rộng và chuyển từ mạng thực nghiệm sang hoạt động chính thức: nhiều trường đại học, viện nghiên cứu ghi tên gia nhập để trao đổi thông tin. Đến năm 1984, mạng ARPANỌT được chia thành hai nhóm mạng nhỏ hơn là MILNET, dành cho quốc phòng, và nhóm mạng thứ hai vẫn gọi là ARPANET, dành cho nghiên cứu và phát triển. Hai nhóm này vẫn có mối liên hệ trao đổi dữ liệu với nhau qua giao thức TCP/IP và được gọi chung là Enternet.

Mạng Internet đã và đang trở thành phương tiện trao đổi thông tin toàn cầu, là phương thức thông tin nhanh với lưu lượng truyền tải dữ liệu rất lớn. Thông qua Internet mà các nhà nghiên cứu khoa học kỹ thuật, các cơ quan giáo dục đào tạo, các nhà doanh nghiệp... có thể trao đổi thông tin với nhau, hoặc truy cập thông tin

của nhau về các công trình, các lĩnh vực nghiên cứu mới nhất; về các phương pháp, hình thức giáo dục và đào tạo, về các thông tin kinh tế, thị trường giá cả... một cách nhanh chóng, thuận tiện và dễ dàng.

### 1.6.2 Cấu trúc của mạng Internet

Mạng Internet không phải một mạng đơn mà là bao gồm nhiều mạng con (sub-network) được kết nối với nhau thông qua các cổng (gateway) như trên hình. Thuật ngữ mạng con ở đây mang nghĩa một *đơn vị mạng hoàn chỉnh* trong hệ thống mạng lớn. Mạng con hoàn toàn có thể là một mạng WAN với quy mô quốc gia, và có khả năng hoạt động độc lập với Internet. Do giao thức TCP/IP không phụ thuộc lớp vật lý, các mạng con có thể sử dụng những công nghệ ghép nối khác nhau (như Ọthernet, X.25,...) mà vẫn giao tiếp được với nhau.

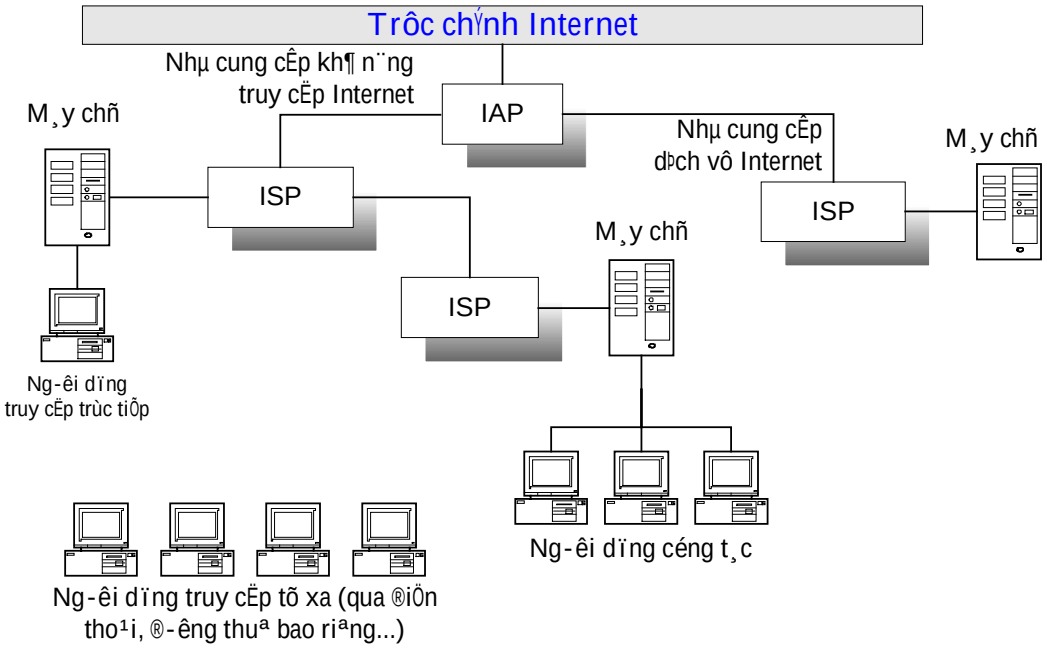



Hình 1-7. Cấu trúc của mạng Internet.

Các cổng được dùng để nối các mạng con tạo thành một mạng lớn.

Có 2 cách kết nối với Internet như sau :

- Máy con nối trong mạng LAN (hay WAN) và mạng này nối với Internet
- Máy con nối đến một trạm cung cấp dịch vụ Internet (Internet Service Provider), thông qua đó kết nối với Internet. Trong hình trên, ta có thể thấy các trạm ISP lại kết nối với Internet thông qua IAP (Internet Access Provider). Một IAP có thể làm luôn chức năng của ISP nhưng ngược lại thì không.




Hình 1-8. Sơ đồ kết nối của các trung tâm cung cấp dịch vụ (ISP)

### 1.6.3 Các kiến trúc khác

| Level | ISO | ARPANET | SNA | DECNET |
|---|---|---|---|---|
| 7 | Application | User | End User | Application |
| 6 | Presentation | Telnet, FTP | NAU Services | |
| 5 | Session | (none) | Data Flow Control | (none) |
| | | | Transmision Control | |
| 4 | Transport | Host - Host | | Network Services |
| | | SRC to DESI - IMP | Path Control | |
| 3 | Network | | | Transport |
| | | IMP - IMP | | |
| 2 | Datalink | | Data Link Control | Data Link Control |
| 1 | Physical | Physical | Physical | Physical |

ARPANET: Advanced Research Projects Agency
FTP: File Transfer Protocol
SNA: System Network Architecture cña IBM
IMP: Interface Message Procesor
NAU: Network Addressable Unit

*Chương 2*

# TẦNG VẬT LÝ

Nhiệm vụ của tầng vật lý là chuyển các bit tin từ máy này đến máy kia. Tốc độ truyền tin phụ thuộc vào môi trường truyền tin. Tín hiệu truyền có thể ở dạng tương tự (*analog*) hoặc ở dạng số (*digital*). Hướng phát triển hiện nay :

- Truyền tin bằng cáp quang, bằng vệ tinh.
- Hệ thống nối nhanh (Fast - Connect), hệ thống chuyển mạch gói
- Mạng thông tin số đa dịch vụ (Integrated Services Digital Network)

## 2.1 Môi trường truyền tin

### 2.1.1 Phương tiện truyền

Mục đích lắp đặt cáp là đảm bảo dung lượng (tốc độ) cần thiết cho các nhu cầu truyền thông trong mạng. Hệ thống cáp cần phải ổn định. Để đạt được mục tiêu này, người quản trị mạng phải cân đối bốn yếu tố sau:

- Tốc độ truyền lớn nhất của hệ thống cáp hiện hành, khả năng nâng cấp.
- Nhu cầu về tốc độ truyền thông trong vòng 5-10 năm tới là bao nhiêu.
- Chọn trong số những loại cáp đang có trên thị trường.
- Chi phí để lắp đặt thêm cáp dự phòng.

Việc kết nối vật lý một máy tính vào mạng được thực hiện bằng cách cắm một card giao tiếp mạng NIC (Network Interface Card) vào khe cắm của máy tính và nối với cáp mạng. Sau khi kết nối vật lý đã hoàn tất, quản lý việc truyền tin giữa các trạm trên mạng tuỳ thuộc vào phần mềm mạng.

NIC sẽ chuyển gói tín hiệu vào mạng LAN, gói tín hiệu được truyền đi như một dòng các bit dữ liệu thể hiện bằng các biến thiên tín hiệu điện. Khi nó chạy trong cáp dùng chung, mọi trạm gắn với cáp đều nhận được tín hiệu này, NIC ở mỗi trạm sẽ kiểm tra địa chỉ đích trong tín hiệu đầu của gói để xác định đúng địa chỉ đến, khi gói tín hiệu đi tới trạm có địa chỉ cần đến, đích ở trạm đó sẽ sao gói tín hiệu rồi lấy dữ liệu ra khỏi khung tin và đưa vào máy tính.

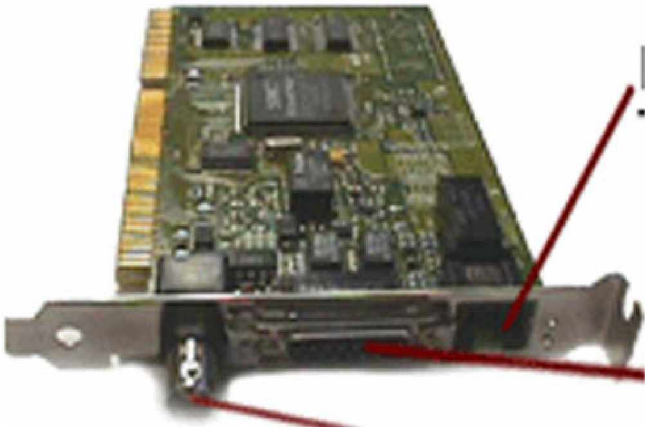
Có hai kỹ thuật truyền tín hiệu đã mã hóa lên mạng : Truyền ở dải tần gốc (baseband) và truyền ở dải tần rộng (broadband).

Đặc tính của cáp bao gồm sự nhạy cảm với nhiễu của điện, độ mềm dẻo, khả năng uốn nắn để lắp đặt, cự ly truyền dữ liệu, tốc độ truyền (Mbit/s). Hiện nay, tốc độ truyền dữ liệu trên các loại cáp biến động từ 10Mbit/s đến 100Mbit/s và hơn nữa.

Có 3 nhóm cáp chính được dùng để nối hầu hết các mạng :

- Cáp đồng trục (Coaxial)
- Cáp xoắn đôi (Twisted-Pair) : gồm có cáp xoắn đôi trần (Unshielded Twisted-Pair) và cáp xoắn đôi có bọc (Shielded Twisted-Pair).
- Cáp sợi quang (Fiber-Optic)

### *2.1.1.1 Card mạng*



Hình 2-1. Card mạng (NIC)

Card mạng còn được gọi là card giao tiếp mạng NIC (Network Interface Card) được lắp đặt trong mỗi máy tính trong mạng cục bộ, Card này có nhiệm vụ chuyển dữ liệu từ máy tính vào cáp mạng và ngược lại. Quá trình này chính là sự chuyển đổi từ tín hiệu số của máy tính thành các tín hiệu điện hay quang được truyền dẫn trên cáp mạng. Đồng thời nó cũng thực hiện chức năng tổ hợp dữ liệu thành các gói và xác định nguồn và đích của gói.

- Các loại đầu nối cho card mạng :

Một vài loại card mạng có nhiều đầu nối để nối với cáp mạng, để xác định đầu nào dùng ta có thể thay đổi các jump hay công tắc chuyển DIP ngay trên card mạng hoặc sử dụng phần mềm.

- Mạng thin Ethernet sử dụng các đầu nối cáp đồng trục BNC (British Naval Connector)
- Mạng thicknet dùng giắc nối AUI 15 chân để cắm vào đầu DB15 của card mạng.
- Mạng Ethernet twisted-pair (10 Base T) sử dụng đầu nối RJ45.

### *2.1.1.2 Cáp đồng trục*

Cáp đồng trục được chế tạo gồm một dây đồng ở giữa chất cách điện, chung quanh chất cách điện được quán bằng dây bện kim loại dùng làm dây đất. Giữa dây đồng dẫn điện và dây đất có một lớp cách ly, ngoài cùng là một vỏ bọc bảo vệ.

Cáp đồng trục có hai loại : loại nhỏ (Thin) và loại to (Thick). Dây cáp đồng trục loại nhỏ được thiết kế để truyền tin cho băng tần cơ bản (Base Band) hoặc băng tần rộng (broadband). Dây cáp loại to dùng cho đường xa, dây cáp nhỏ dùng cho đường gần, tốc độ truyền tin qua cáp đồng trục có thể đạt tới 35 Mbit/s.

#### *2.1.1.3 Cáp dây xoắn (Twisted Pair)*

Cáp xoắn gồm hai sợi dây đồng được xoắn cách điện với nhau. Nhiều đôi dây cáp xoắn gộp với nhau và được bọc chung bởi vỏ cáp hình thành cáp nhiều sợi. Cáp này có đặc tính dễ bị ảnh hưởng của nhiễu điện nên chỉ truyền dữ liệu ở cự ly khoảng 100m (khoảng 328 feet). Cáp xoắn đôi có hai loại: cáp xoắn đôi không bọc (UTP) và cáp xoắn đôi có bọc (STP).

Cáp xoắn thường được dùng trong hệ thống điện thoại để truyền tín hiệu tương tự (analog) cũng như tín hiệu số (digital). Trong khoảng cách vài km thì không cần bộ khuyếch đại và có tốc độ ở mức megabit/giây.

#### *2.1.1.4 Cáp quang (Fiber Optics)*

Khi các tín hiệu số được điều chế thành các tín hiệu xung ánh sánh thì được truyền tải qua cáp quang. Cáp sợi quang bao gồm một sợi thuỷ tinh cực mảnh gọi là lõi (core), được bao bọc bởi một lớp thuỷ tinh đồng tâm gọi là lớp vỏ bọc hay còn gọi là lớp phủ (cladding). Đôi khi các sợi được làm bằng chất dẻo. Chất dẻo dễ lắp đặt hơn nhưng không thể mang xung ánh sáng đi xa như thuỷ tinh.

Mỗi sợi thuỷ tinh chỉ truyền tín hiệu theo một hướng nhất định, do đó cáp có 2 sợi nằm trong vỏ bọc riêng biệt : một sợi truyền và một sợi nhận. Cáp sợi quang có thể truyền tín hiệu đi xa hơn với tốc độ cực nhanh (theo lý thuyết cáp quang có thể truyền tín hiệu với tốc độ tối đa 200.000Mbit/s).

Cáp quang có dải thông lớn hơn cáp đồng, ưu điểm mạnh của cáp quang là khoảng cách truyền dẫn lớn, giá rẻ, dung lượng truyền cao.

#### *2.1.1.5 Vệ tinh thông tin*

Vệ tinh truyền thông (communication satellites) nhận thông tin mặt đất, khuyếch đại tín hiệu thu được và phát lại xuống mặt đất ở tần số khác để tránh giao thoa (interference) với tín hiệu thu được. Các vệ tinh có vai trò như những trạm lặp tin giữa các trạm mặt đất với nhau. Một vệ tinh đều phủ sóng rất rộng và có thể có nhiều trạm mặt đất, thường hoạt động ở tần số 12 - 14Ghz. Truyền tin qua vệ tinh có dãi truyền rất rộng, do đó những khoảng cách xa (hàng trăm km) được bảo đảm chất lượng tin. Ngoài ra giá của truyền vệ tinh đang giảm nhanh.

Uỷ ban kỹ thuật điện tử (IEEE) đề nghị dùng các tên sau đây để chỉ 3 loại dây cáp dùng với mạng Ethernet chuẩn 802.3 :

1. Dây cáp đồng trục sợi to (thick coax) gọi là 10BASE5, có tốc độ 10 Mbps, tần số cơ sở, ≤ 500m.

2. Dây cáp đồng trục sợi nhỏ (thin coax) gọi là 10BASE2, có tốc độ 10 Mbps, tần số cơ sở, ≤ 200m.
3. Dây cáp đôi xoắn không vỏ bọc (twisted pair) gọi là 10BASET, có tốc độ 10 Mbps, tần số cơ sở, sử dụng cáp sợi xoắn.
4. Dây cáp quang (Fiber Optic Inter-Repeater Link) gọi là FOIRL .

### 2.1.2 Các thông số cơ bản của môi trường truyền tin

#### *2.1.2.1 Độ suy giảm*

Tín hiệu trên đường dây bị suy giảm trong quá trình truyền tin. Để khắc phục ta dùng các bộ khuyếch đại (amplifiers). Độ suy giảm được tính bằng đơn vị decibel. Nếu điện thế ban đầu là $V_1$ và sau đó giảm xuống $V_2$ thì số decibel của độ suy giảm được định nghĩa như sau:

$$\mathrm{S\,(decibel)} = 20\log_{10}\frac{V_1}{V_2}$$

#### *2.1.2.2 Độ nhiễu*

Điện từ trường trong môi trường truyền tin gây nhiễu cho các tín hiệu mang thông tin. Để khắc phục ta dùng các bộ lọc nhiễu (*filters*). Để đặc trưng độ nhiễu trên đường dây, ta dùng tỉ số tần số tín hiệu/tạp âm (Signal/Noise - S/N) :

$$SN(decibel) = 10\log_{10}\frac{S}{N} \quad (S: Signal;\ \ N: Noise)$$

#### *2.1.2.3 Tốc độ truyền*

$$C = B\log_2\left(1+\frac{S}{N}\right) bit/s$$

Trong đó B là độ rộng dải tần tính bằng Hz. C là tốc độ tính bằng bit/giây (b/s). Nếu mạng điện thoại có dải tần 3000Hz, tỉ số S/N = 20dB thì tốc độ truyền cực đại là :

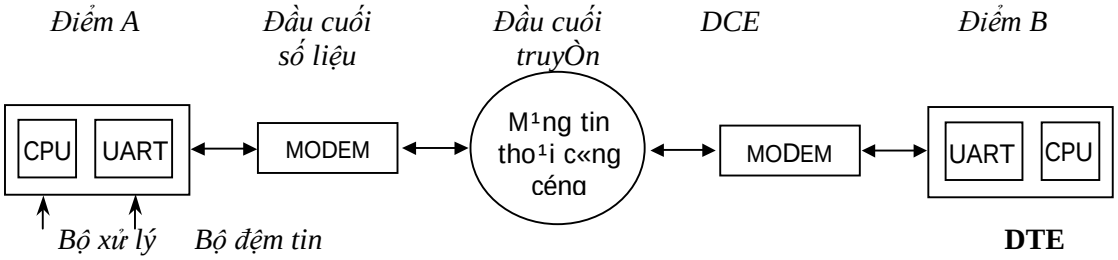
$$\frac{S}{N} = 10\log_{10}\frac{S}{N} = 20 \rightarrow \frac{S}{N} = 100 \qquad C = B\log_2\left(1+\frac{S}{N}\right) = 3000\times\log_2(1+100) = 19963b/s$$

Các tín hiệu trên kênh truyền có thể là tín hiệu tương tự hoặc tín hiệu số và tương ứng sẽ tạo thành kênh tương tự hoặc kênh số.

## 2.2 Chuẩn giao diện

### 2.2.1 Modem

Modem là bộ điều chế và giải điều chế biến đổi các tín hiệu số thành các tín hiệu tương tự và ngược lại trên mạng điện thoại.




Hình 2-2. Sơ đồ truyền tin giữa hai điểm A và B.

Tín hiệu số từ máy tính đến modem, được modem biến đổi thành tín hiệu tương tự để có thể đi qua mạng điện thoại. Tín hiệu này đến modem ở điểm B được biến đổi ngược lại thành tín hiệu số đưa vào máy tính ở B.

Các kỹ thuật điều chế cơ bản là điều chế biên độ AM, điều chế tần số FM, điều chế pha PM .

- Điều chế biên độ : Các tín hiệu 1 và 0 được phân biệt bởi biên độ, còn tần số của tín hiệu là giống nhau. Điều chế biên độ để thực hiện nhưng dễ bị nhiễu.
- Điều chế tần số : Các tín hiệu 1 và 0 được phân biệt bởi tần số, còn biên độ các tín hiệu giống nhau.

  Kỹ thuật điều tần phức tạp hơn nhưng tính chống nhiễu cao.
- Điều chế theo pha : Các tín hiệu 1 và 0 được phân biệt bởi các pha của dao động, còn biên độ và tần số của các tín hiệu giống nhau. Điều pha cũng phức tạp nhưng ít bị nhiễu.

Để tăng tốc độ truyền tin người ta kết hợp điều pha với điều biên gọi là điều pha biên.

Hiện nay có rất nhiều loại modem hiện đại từ loại thấp: 300, 600, 1200, 2400 bit/s, đến loại 9600 bit/s. Với tốc độ truyền tương đối cao trên đường truyền băng hẹp (băng thoại) nên đòi hỏi những phương pháp điều biên phức tạp.

Các *phương thức truyền dữ liệu* giữa hai điểm có thể là:

- Một chiều đơn (simplex)
- Hai chiều luân phiên (half - duplex)
- Hai chiều đầy đủ (duplex)

Truyền một chiều đơn chỉ cho phép truyền một hướng. Truyền hai chiều luân phiên cho phép truyền hai hướng, nhưng mỗi thời điểm chỉ có một hướng được truyền, sau đó phải thực hiện chuyển mạch để truyền ngược lại. Truyền hai chiều đầy đủ có thể nhận hoặc phát cùng một lúc. Các modem hiện nay đều có thể hoạt động ở hai chế độ bán song công và song công.

### 2.2.2 DTE và DCE

Trước khi nghiên cứu các chuẩn cho giao diện tầng Vật lý, chúng ta có hai khái niệm mới : đó là DTE và DCE.

- DTE (Data Terminal Equipment - Đầu cuối số liệu) : là khái niệm được sử dụng để chỉ các máy mà người sử dụng bình thường thao tác trực tiếp lên đó. Các máy này có thể là máy tính hay trạm cuối.
- DCE (Data Communication Equipment - Đầu cuối truyền) : là khái niệm chỉ các thiết bị cuối kênh dữ liệu có chức năng nối các DTE với các đường truyền vật lý và chuyển đổi dữ liệu. DCE có thể là các Modem, Tranducer, Multiplexer...

ISO qui định các chuẩn quy ước phương thức ghép nối giữa đầu cuối số liệu DTE và đầu cuối truyền DCE.

### 2.2.3 Chuẩn RS-232C

Đầu những năm 50, chuẩn RS-232(Recommended Standard 232C, của EIA) được phát triển để truyền tin giữa các thiết bị đầu cuối dữ liệu. Chuẩn này hiện nay đang được sử dụng, nó chính là các cổng COM1, COM2 trên các máy PC.

- *Phần cơ học :* là một bộ có 25 chân độ rộng tính ở giữa là 47,05mm ± 13 hàng trên đánh số 1 ÷ 13 (trái qua phải) hàng dưới 14 ÷ 25 (trái qua phải).
- *Phần điện :* gồm qui ước logic 1 <-3V và logic 0 >+ 3V.

Tốc độ truyền cho phép 20 *kbps* qua dây cáp 15m (thường là 9,6 *kbps*)

Từ năm 1987, RS-232-C đã được sửa đổi và đặt tên lại là EIA-232-D. Ngoài ra còn có một số chuẩn mở rộng khác như RS-422-A, RS-423-A RS-449, các khuyến nghị loại X của CCITT như X21. . .. Mặc dầu RS-232-C vẫn là chuẩn thông dụng nhất cho giao diện DTE/DCE nhưng các chuẩn mới nói trên được áp dụng phổ biến hiện nay.

Đối với các máy tính, thông thường người ta sử dụng hai cổng COM1, COM2 để *kết nối trực tiếp*. Cổng COM1 có địa chỉ vào/ra là 3F8_3FF hex và ngắt là IRQ4, cổng COM2 có địa chỉ vào/ra là 2F8_2FF hex và ngắt là IRQ3. Các chân cắm của hai cổng cũng được chuẩn hóa để tiện lợi hơn cho việc sử dụng.

*Chương 3*

# TẦNG LIÊN KẾT DỮ LIỆU

## 3.1 Chức năng

Tầng liên kết dữ liệu thực hiện các công việc chính như sau :

- Định danh các thiết bị trên mạng, cấu hình logic của mạng.
- Điều khiển luồng dữ liệu và việc truy nhập ở tầng vật lý.
- Phát hiện và chỉnh sửa các lỗi xuất hiện trong quá trình truyền dữ liệu.

Chức năng chính của tầng LKDL là tách rời các khung thành các bít để truyền đi và kiến tạo các khung (frames) từ các dòng bít nhận được.

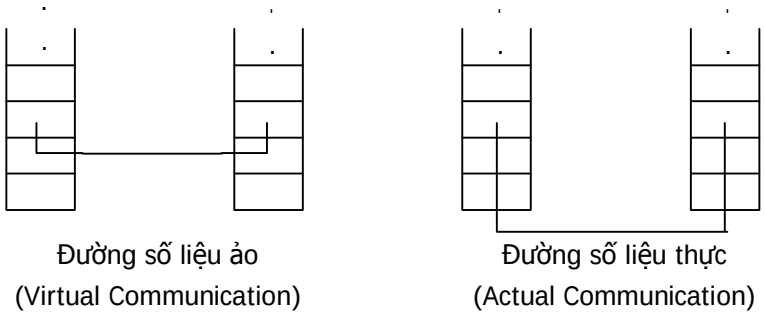
Tầng LKDL nghiên cứu các thuật toán thực hiện thông tin hiệu suất, tin cậy giữa hai máy cạnh nhau ở tầng 2. Đưa ra các thủ tục truyền tin có lưu ý đến lỗi có thể xẩy ra do nhiễu trên đường dây, sự trễ do lan truyền.

Thông thường, tầng LKDL có liên quan đến nhiễu của tín hiệu của phương tiện truyền vật lý, cho dù là truyền qua dây đồng, cáp quang hay truyền thông qua sóng ngắn. Nhiễu là một vấn đề rất thông thường và có thể do rất nhiều nguồn khác nhau, trong đó có cả nhiễu của các tia vũ trụ, nhiễu do tạp âm của khí quyển và từ các nguồn khác nhau.

## 3.2 Các vấn đề của tầng liên kết dữ liệu

### 3.2.1 Cung cấp dịch vụ cho tầng mạng

Tầng 2 chuyển dữ liệu từ mức 3 ở máy nguồn tới mức 3 ở máy nhận.




Hình 3-1. đường truyền dữ liệu trong tầng LKDL.

Các dịch vụ tầng 2 có thể là:

1. Dịch vụ không kết nối, không biên nhận (*Unacknowledged Connectionless Service*)
2. Dịch vụ không kết nối, có biên nhận (*Acknowledged Connectionless Service*)
3. Dịch vụ có kết nối (*Connection Oriented Service*)

Dịch vụ kết nối có hướng có 3 giai đoạn: *kết nối, truyền số liệu, tách bỏ liên kết* (kết thúc) : CONNECT, DATA, DISCONNECT. Truyền tin giữa 2 tầng kề nhau dùng các hàm dịch vụ nguyên thủy (request, indication, response và confirm).

Dịch vụ không kết nối được thể hiện bằng một bước duy nhất là truyền tin, không cần thiết lập liên kết logic. Các đơn vị dữ liệu truyền độc lập với nhau.

### 3.2.2 Khung tin - Nhận biết gói tin

Để cung cấp dịch vụ cho tầng mạng, tầng LKDL phải dùng dịch vụ được cung cấp từ tầng Vật lý. Tầng Vật lý tiếp nhận dòng bít và giao cho nơi nhận. Dòng bit này có thể có lỗi. Tầng LKDL sẽ kiểm tra và nếu cần sẽ sửa lỗi.

Tầng LKDL tách dòng bit thành các khung tin (frame) và tính thông số kiểm tra tổng (checksum) cho mỗi khung tin này, nếu kết quả tính được khác với checksum chứa trong khung tin, nghĩa là có lỗi và khi đó lỗi sẽ được thông báo cho nơi gửi.

Muốn tách các khung tin, có thể chèn các đoạn phân cách (timegaps) vào giữa các khung tin, giống như khoảng trống (*space*) giữa các từ trong văn bản. Nhưng điều này khó thực hiện nên người ta thường dùng các phương pháp sau :

- Đếm số ký tự : Hiện nay ít được dùng, vì từ đếm cũng bị lỗi khi truyền.
- Dùng ký tự bắt đầu (STX) và kết thúc (ETX) với ký tự đệm (DLE).
- Dùng các cờ (*flags*) đánh dấu bắt đầu và kết thúc với các bit đệm.

### 3.2.3 Kiểm tra lỗi

Các cách để kiểm tra lỗi trong quá trình truyền :

- Dùng thông số trả lời có biên nhận (ACK) hoặc không biên nhận (NAK) để biết đã nhận đúng bản tin hay phải phát lại.
- Dùng bộ định thời gian, nếu quá thời gian quy định không có trả lời nghĩa là bản tin chưa nhận được.
- Dùng phương pháp đánh số thứ tự các khung tin (frame) được gửi đi.

Quá trình kiểm tra lỗi đồng thời với quản lý thời gian và số thứ tự của các khung tin nhằm bảo đảm mỗi khung tin chỉ nhận được một lần duy nhất. Đây là chức năng quan trọng của tầng LKDL.

### 3.2.4 Điều khiển luồng dữ liệu

Trong quá trình truyền dữ liệu, nếu tốc độ bên phát nhanh hơn bên thu thì xảy ra hiện tượng mất tin do không nhận kịp. Vì vậy cần phải điều khiển luồng truyền

(*flow control* ) để quá trình thu phát được phối hợp nhịp nhàng và đồng bộ với nhau. Chức năng có tại một vài cấp giao thức, kể cả tầng con LLC.

Các giao thức phải chứa các quy tắc xác định rõ khi nào nơi gởi có thể phát các khung tin kế tiếp.

### 3.2.5 Quản lý liên kết

Một chức năng khác của tầng LKDL là quản lý các kết nối như tách, nối, đánh số khung tin, bắt đầu lại khi lỗi, quản lý các thiết bị đầu cuối thứ cấp hoặc sơ cấp bằng khung tin thăm dò (poll).

### 3.2.6 Nén dữ liệu khi truyền

Nén dữ liệu là một vấn đề quan trọng đơn vị việc truyền dữ liệu trên mạng. Về cơ bản, nén dữ liệu là ép chúng lại để đỡ tốn chỗ khi lưu trữ trên đĩa và đỡ tốn thời gian khi truyền trên đường dây. Thực tế, các dữ liệu số chứa nhiều đoạn lặp đi lặp lại, nén dữ liệu sẽ thay thế các thông tin lặp lại bằng một ký hiệu hoặc một đoạn mã để rút ngắn độ dài của tập tin. Các kỹ thuật nén dữ liệu cơ sở bao gồm :

- *Null compression* : Thay thế một dãy các dấu cách bằng một mã nén và một giá trị số lượng các dấu cách.
- *Run-length compression* : Mở rộng kỹ thuật trên bằng cách nén bất kỳ một dãy nào có từ 4 ký tự lặp. Các ký tự này được thay thế bằng một mã nén, là một trong các ký tự này, và một giá trị bằng đúng số lần lặp.
- *Keyword encoding* : Tạo ra một bảng mã cho các từ hoặc các cặp ký tự thường xuyên xuất hiện và thay thế.
- *Phương pháp thống kê Huffman* : Kỹ thuật nén này giả thiết rằng sự phân bố của các ký tự trong dữ liệu là không đồng nhất. Tức là một số ký tự xuất hiện nhiều hơn các ký tự khác. Ký tự nào càng xuất hiện nhiều thì càng ít tốn bit để mã hóa nó. Một bảng được tạo ra để ghi lại lược đồ mã hóa và bảng này có thể chuyển cho modem nhận để nó biến đổi trở lại các ký tự đã mã hóa.
- Ngoài ra còn một thuật toán nén nữa được gọi là nén ngẫu nhiên. Thuật toán này được sử dụng trong một chuẩn nén dữ liệu V.24bits

## 3.3 Phát hiện và hiệu chỉnh lỗi

Trong khi truyền đi một byte trong hệ thống máy tính thì khả năng xảy ra một lỗi do hỏng hóc ở phần nào đó hoặc do nhiễu gây nên là khá lớn. Các kênh vào-ra thường xẩy ra nhiều lỗi, đặc biệt là khi truyền số liệu. Phần lớn các hệ thống đều có các phương pháp phát hiện và sau đó sửa lỗi. Quá trình sửa lỗi thường khó hơn rất nhiều so với phát hiện lỗi. Có thể chia phương pháp xử lý lỗi ra làm hai nhóm:

- Phát hiện lỗi và thông báo cho bên phát biết để phát lại tin.
- Phát hiện lỗi và tự sửa.

### 3.3.1 Phương pháp bit chẵn lẻ (Parity)

Đây là phương pháp thường dùng nhất để phát hiện lỗi. Bằng cách thêm 1 bit (được gọi là bit chẵn lẻ) vào từ nhị phân phụ thuộc vào tổng số các bit 1 trong một từ là một số chẵn hay lẻ, và nhờ vào phép toán logic XOR, ta sẽ biết được bit thêm vào đó là bit chẵn hay bit lẻ.

Mạch kiểm tra sẽ xác định các số bit 1 có đúng tính chẵn lẻ hay không. Phương pháp tương đối đơn giản và có hai cách như sau :

- Kiểm tra ngang (VRC - Vertical Redundancy Checking) : Thêm một bit chẵn lẻ vào mỗi byte để phát hiện lỗi. Cách này làm mất đi khoảng 12,5% dung lượng bản tin. Để khắc phục ta có thể dùng phép kiểm tra tổng các byte.
- Kiểm tra dọc (LRC - Longitudinal Redundancy Checking) : lỗi được phát hiện trong các khối byte thay cho việc tìm lỗi trong từng byte. Trong phương pháp này người ta thêm mỗi khối *1 byte ở cuối*, byte này mang các thông tin về tính chất đặc thù của khối (Characteristic Redundancy Checking - CRC). Byte này đơn giản có thể tính bằng phép logic XOR của tất cả các byte trong khối hoặc tính theo đa thức chuẩn để được FCS.

  *Ví dụ :*

| Vị trí bit trong ký tự | Khối ký tự truyền đi | | | | | LRC |
|---|---|---|---|---|---|---|
| | A | S | C | I | I | |
| 0 | 1 | 1 | 1 | 1 | 1 | 1 |
| 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| 2 | 0 | 1 | 0 | 0 | 0 | 1 |
| 3 | 0 | 0 | 0 | 1 | 1 | 0 |
| 4 | 0 | 0 | 0 | 0 | 0 | 0 |
| 5 | 0 | 1 | 1 | 0 | 0 | 0 |
| 6 | 1 | 1 | 1 | 1 | 1 | 1 |
| VRC | 0 | 0 | 1 | 1 | 1 | 1 |

Kiểm soát lỗi 2 chiều : VRC-LRC.

Bên nhận sẽ kiểm tra parity theo cả hai chiều để phát hiện và định vị lỗi cho từng ký tự. ( $1 \oplus 1 = 0$ $0 \oplus 0 = 0$ $1 \oplus 0 = 0$ $0 \oplus 1 = 1$ )

### 3.3.2 Tính theo đa thức chuẩn

Cách tính check sum như sau :

- Giả sử ta nhận được bản tin M(x).

- Nếu đa thức chuẩn G(x) có bậc là r, ta bổ sung thêm r bit 0 vào cuối bản tin và được m+r bit tương ứng đa thức xrM(x).
- Chia xrM(x) theo module 2 cho G(x). Kết quả ta được số dư T(x) là checksum được phát đi.

Các đa thức chuẩn thường được dùng để tính biến kiểm tra tổng là :

CRC-12 = $x^{12} + x^{11} + x^3 + x^2 + x + 1$ (dùng cho ký tự 6 bit)

CRC-16 = $x^{16} + x^{15} + x^2 + 1$ (dùng cho ký tự 8 bit)

CRC-CCTTT= $x^{16} + x^{12} x^5 + 1$ (dùng cho ký tự 8 bit)

*Ví dụ* Khung tin ban đầu 1101011011, G(x) = $x^4 + x + 1$, vậy r = 4, chuỗi bit thêm : 10011. Ta có xrM(x) = 1101011011 0000. Chia xrM(x) theo module 2 cho G(x), ta được thông số kiểm tra tổng T(x) = 1110

```
   11010'1'1011 0'00'0'
⊕  10011
   01001 1
    10011
     0000010110
           10011
           0010100
              10011
               001110 → Số dư là 1110
```

Khung tin được truyền đi: 1101011011 1110

### 3.3.3 Mã sửa sai

Để sửa sai một bit, ta dùng tập mã Hamming dựa trên các "bit chẵn lẻ" được rải vào các bit số liệu trong từng byte theo nguyên lý cân bằng chẵn lẻ để chỉ ra các bit lỗi.

Nếu trong bản tin có k bit và số "bit chẵn lẻ" là r, thì số bit tin và "bit chẵn lẻ" phát đi sẽ là n=k+r. r bit kiểm tra luôn các vị trí 1, 2, 4, 8,..., 2r-1 và được tạo bởi cộng module 2 giá trị nhị phân của các vị trí có bit '1' của từ mã. Vì các bit kiểm tra chiếm vị trí $2^i$ với i = 0, 1, 2,..., r-1 nên độ dài cực đại của các từ mã Hamming là n $\leq 2^r - 1$ và từ dãy số cực đại của các bit tin được bảo vệ là : k $\leq (2^r - 1 - r)$. Từ đây ta xác định được r.

*Ví dụ:* Bản tin 11 bit (10101011001) được bảo vệ bởi mã Hamming.

Từ điều kiện 11 ≤ 2' - 1-r, ta cần 4 bit kiểm tra (r =4) để tạo mã Hamming (n=11+4=15)

| 1 | 0 | 1 | 0 | 1 | 0 | 1 | C | 1 | 0 | 0 | C | 1 | C | C |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |

Các bít kiểm tra C được tính như sau:

VÞ trÝ bit 1 Gi¸ trÞ nhÞ ph©n

| | |
|---|---|
| 15 | 1111 |
| 13 | 1101 |
| 11 | 1011 |
| 9 | 1001 |
| 7 | 0111 |
| | 1101 |

-> TËp m· c¸c bit kiÓm tra Hamming: 0100

Tõ m· Hamming: 10101010010011100

NÕu b¶n tin nhËn ®-îc lµ:

| 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 |

↑ bit error

| **Vị** trí bit 1 | Giá trị nhị phân |
|---|---|
| 15 | 1111 |
| 13 | 1101 |
| 9 | 1001 |
| 7 | 0111 |
| 4 | 0100 |
| 3 | 0011 |
| | 1011 (11) |

→ Vb trÝ sai ë bit 11

## 3.4 Thủ tục liên kết dữ liệu cơ bản

Để truyền tin có độ tin cậy cao ta dùng dịch vụ liên kết (Connection Oriented Service).

Ví dụ máy A gửi số liệu cho máy B, khi tầng 2 đã được nối, số liệu từ tầng 3 máy A chuyển xuống tầng 2 nhờ chương trình con “FromNetworkLayer”. Tầng 2 bổ sung phần đầu thông tin điều khiển và tính cờ kiểm tra tổng (FCS).

| Khung tin (Frame) = | Đầu tin (Header) | Thông tin (Information) | FCS |
|---|---|---|---|

Khung tin được phát sang tầng 2 máy B nhờ chương trình con ToPhysicalLayer.

Máy B đợi tin bằng chương trình con Procedure CallWait(Event). Khi khung tin tới bên nhận, máy B tính cờ kiểm tra tổng, nếu không đúng cờ sẽ báo event = CKsumErr, nếu khung tin đúng nó báo event=FrameArrival và thu nhận khung tin từ tầng Vật lý nhờ chương trình con FromPhysicalLayer.

Sau đó đầu tin chứa các thông tin điều khiển (*header*) sẽ được kiểm tra và nếu tất cả đều đúng cả, phần số liệu được chuyển lên tầng 3 nhờ chương trình con ToNetworkLayer.

- Giao thức đơn công với kênh không lỗi và không chờ : Trong giao thức này do tin chỉ truyền theo một hướng, đường kênh không có lỗi nên số liệu luôn sẵn sàng không phải chờ.
- Giao thức đơn công với kênh không lỗi và phải đợi : Bên thu bộ nhớ hạn chế và tốc độ vật lý hữu hạn, do đó bên phát phải chờ.

### 3.4.1 Giao thức đơn công với kênh có lỗi

- *Bên nhận*

Khi nào đường kênh có lỗi, bên nhận sẽ chỉ gửi tín hiệu biên nhận nếu gói tin nhận được là đúng, nếu gói tin nhận được là sai thì sẽ bị bỏ đi. Quá thời hạn qui định, bên phát sẽ gửi lại gói tin. Quá trình này lặp lại cho đến khi nhận được gói tin đúng. Trong trường hợp này, tầng 3 ở máy B không biết được gói tin bị mất hay nhận hai lần, tầng 2 phải nhận biết được điều này.

Có thể xảy ra các trường hợp :

- Tầng 3 ở máy A gửi gói tin X xuống tầng 2 của nó và phát đi.
- Máy B nhận được và trả lời bằng tín hiệu biên nhận ACK.
- Tín hiệu biên nhận bị mất trên đường đi.
- Quá thời gian qui định mà máy A không nhận được tín hiệu biên nhận, nó sẽ phát lại gói tin X. Dẫn đến máy B nhận được hai gói tin X

Để giải quyết vấn đề này người ta đánh dấu gói tin gửi đi và bên nhận gửi tín hiệu cho biết đã nhận gói tin số mấy.

- *Bên phát*

Bên phát sau khi phát gói tin, có 3 khả năng xảy ra: nhận được tín hiệu biên nhận đúng, tín hiệu biên nhận bị mất hoặc quá thời gian mà chưa nhận được trả lời. Nếu tín hiệu biên nhận đúng, máy A nhận tiếp gói tin từ tầng mạng đặt vào vùng đệm (*buffer*), xoá gói tin trước, tăng số thứ tự gói tin phát. Nếu tín hiệu biên nhận bị mất hoặc đã quá thời gian mà chưa nhận được thì phát lại gói tin với số thứ tự gói tin không thay đổi.

Bên nhận nếu nhận đúng gói tin thì tiếp nhận và chuyển đến tầng mạng và phát tín hiệu biên nhận. Nếu gói tin sai hoặc nhận 2 lần thì không được chuyển lên tầng mạng.

## 3.5 Điều khiển dòng truyền

Để tận dụng đường dây, các tín hiệu biên nhận (ACK ) được ghép cùng với gói tin. Khi gói tin đến, thay cho việc trả lời ngay tín hiệu biên nhận, bên thu nhận tiếp gói tin từ tầng mạng để ghép cùng cùng tín hiệu biên nhận và gửi trả lời. Kỹ thuật này được gọi là Piggybacking (ghép thêm).

Ưu điểm của phương pháp này là tận dụng đường kênh. Nếu quá thời gian (vài μs) mà không có gói tin mới thì bên thu cũng phải trả lời tín hiệu biên nhận để bên phát không phải phát lại gói tin cũ.

Để tận dụng đường kênh, bên phát và bên thu phải đồng bộ để bên thu kịp nhận các gói tin và bên phát cũng không lãng phí đường truyền, người ta dùng cơ chế cửa sổ trượt (sliding windows). Cửa sổ mở to thì số gói tin đưa lên đường kênh nhiều hơn(tốc độ nhanh), cửa sổ mở bé thì số gói tin đưa lên đường kênh ít lại (tốc độ chậm lại). Tương tự như cửa chắn đập nước.

### 3.5.1 Cơ chế cửa sổ

Người ta dùng số bit để đặc trưng cho độ rộng cực đại của cửa sổ. Trong thủ tục này, mỗi gói tin đi sẽ được đánh số từ 0 đến Max (Max là $2^n$ - 1) thông qua một dãy gồm các số 0, 1. Chẳng hạn cửa sổ 3 bit sẽ quản lý các gói tin có số từ 0 $\rightarrow$7. Ta có thể dùng *n* tuỳ ý.

Danh sách các gói tin gửi đi giữ trong cửa sổ phát. Danh sách các gói tin nhận được giữ trong cửa sổ nhận. Cửa sổ phát và nhận không bắt buộc phải có kích thước, giới hạn trên và dưới giống nhau.

Mặc dầu thủ tục này cho phép tầng liên kết dữ liệu linh hoạt hơn về thứ tự gởi, nhận gói tin nhưng nó yêu cầu phải đảm bảo tầng mạng đích ở bên nhận có cùng thứ tự với tầng mạng nguồn ở bên gửi.

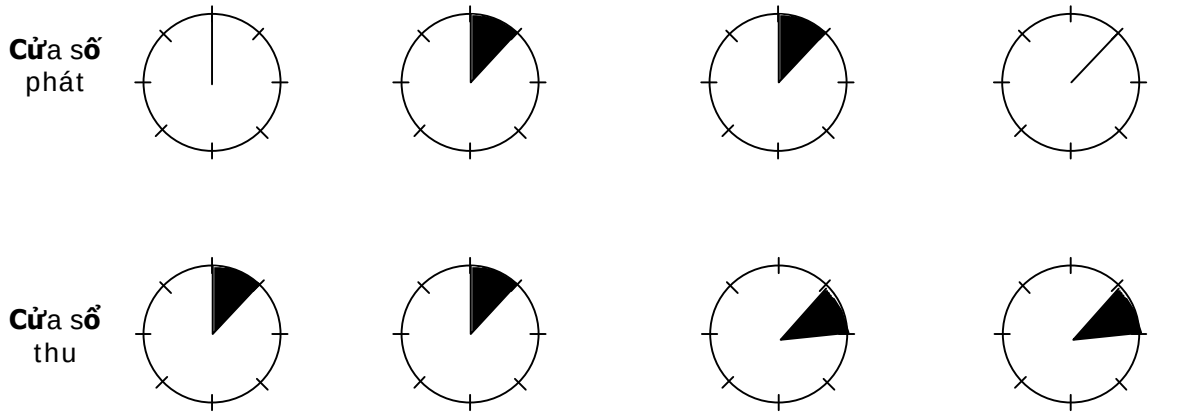
- *Cửa sổ bên phát*

Trong cửa sổ bên phát đặt các gói tin gửi đi nhưng chưa nhận được tín hiệu biên nhận. Khi nhận được gói tin mới đến từ tầng mạng để phát đi, biên trên cửa sổ tăng 1, và khi có tín hiệu biên nhận, biên dưới của cửa sổ tăng 1. Bên phát luôn giữ trong bộ nhớ các gói tin đã phát đi nhưng chưa nhận được tín hiệu biên nhận vì có thể phát lại. Như vậy nếu Max bằng n thì bên phát cần n vùng đệm để giữ các gói tin đã phát đi nhưng chưa nhận được trả lời. Nếu cửa sổ đã tới Max thì tầng liên kết dữ liệu bên phát ngừng nhận tin từ tầng 3 cho đến khi có bộ đệm tự do.

- *Cửa sổ bên nhận*

Cửa sổ bên nhận chứa các gói tin được chuyển đến. Khi gói tin có số thứ tự trùng với biên dưới của cửa sổ được nhận, cửa sổ chuyển tin lên tầng ba, phát tín hiệu biên nhận và quay một đơn vị. Không như cửa bên phát, cửa sổ bên nhận luôn duy trì cùng một kích thước. Khi kích thước cửa sổ = 1, tầng 2 nhận gói tin theo thứ tự. Nhưng nếu kích thước cửa sổ lớn hơn thì không phải như vậy.

Hoạt động của cửa sổ có kich thước là 3 bit với độ trượt 1 bit như sau :

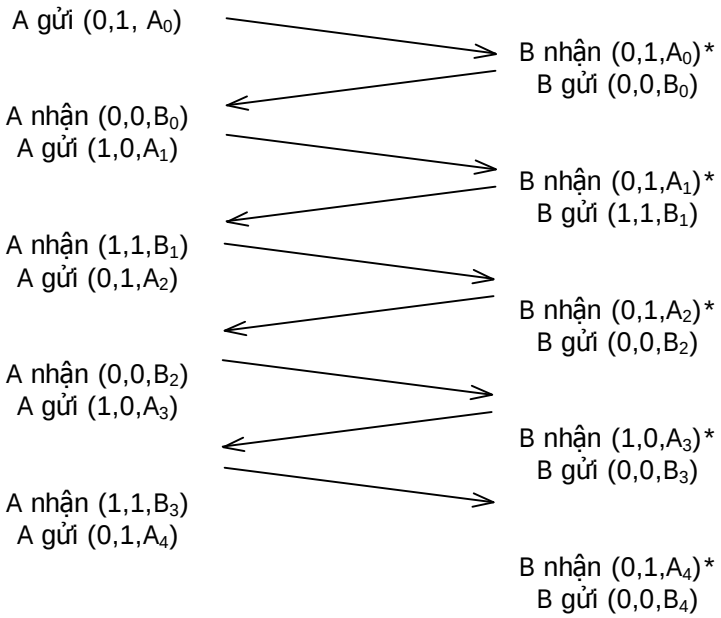



Hình 3-2. điều khiển dòng truyền theo cơ chế cửa sổ.

### 3.5.2 Trao đổi bản tin với cửa sổ 1 bit

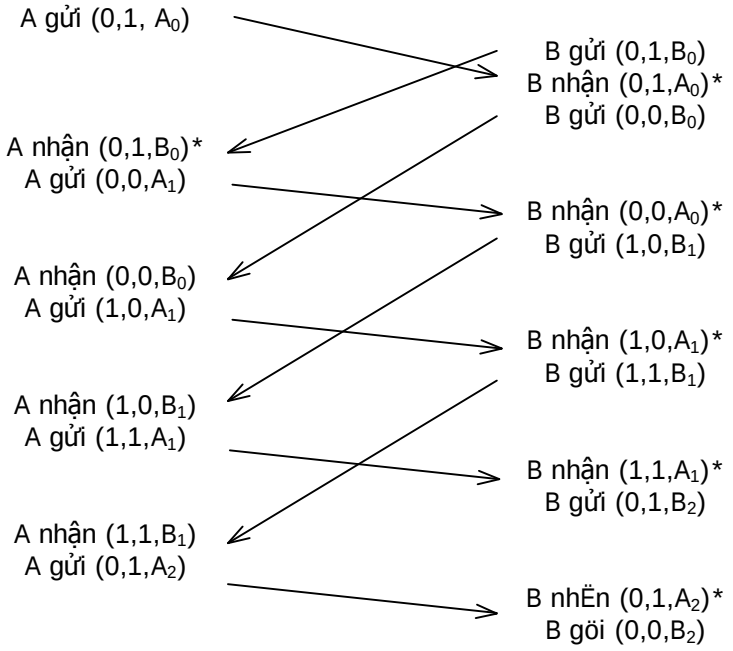
Bản tin gồn có gói tin với phần điều khiển (Header). Phần điều khiển gồm có số gói tin, số thứ tự phát *seq*, số gói tin, số thứ tự nhận là *ack*.

Trong trường hợp bình thường máy A gửi trước như sau :




Hình 3-3. Trao đổi bản tin với cửa sổ 1 bit bình thường.

Trong trường hợp bất thường máy A và B cùng gửi như sau :




Hình 3-4. Trao đổi bản tin với cửa sổ 1 bit bất thường.

Máy A ở tầng 2 nhận gói tin ở tầng 3, tạo bản tin và gửi đi. Khi bản tin này đến tầng 2 máy B, nó sẽ được kiểm tra xem có bị lặp lại không. Nếu đúng là bản tin đang mong đợi thì nó được chuyển lên tầng 3 và cửa sổ nhận dịch đi 1 nấc.

Vùng tín hiệu biên nhận chứa số bản tin cuối cùng đã được nhận mà không có lỗi. Nếu số này trùng với số bản tin vừa gửi. Bên phát sẽ lấy bản tin tiếp theo từ tầng mạng. Nếu số không đúng nó phải gửi lại bản tin cũ.

### 3.5.3 Vận chuyển liên tục

Thực tế cho ta thấy thời gian từ lúc phát gói tin đến lúc nhận trả lời biên nhận ACK là không đáng kể. Khi đó, nếu đường kênh vệ tinh có tốc độ 50Kbp/s với trễ lan truyền 500 ms, ta dùng thủ tục điều khiển dòng truyền gửi gói tin là 1000 bit qua vệ tinh. Thời gian phát gói tin là 20ms, vậy sau 520ms mới nhận được tín hiệu biên nhận trả lời. Như vậy bên phát phải chờ đến 96% thời gian (500/520), chỉ có 4% độ rộng băng được dùng đến.

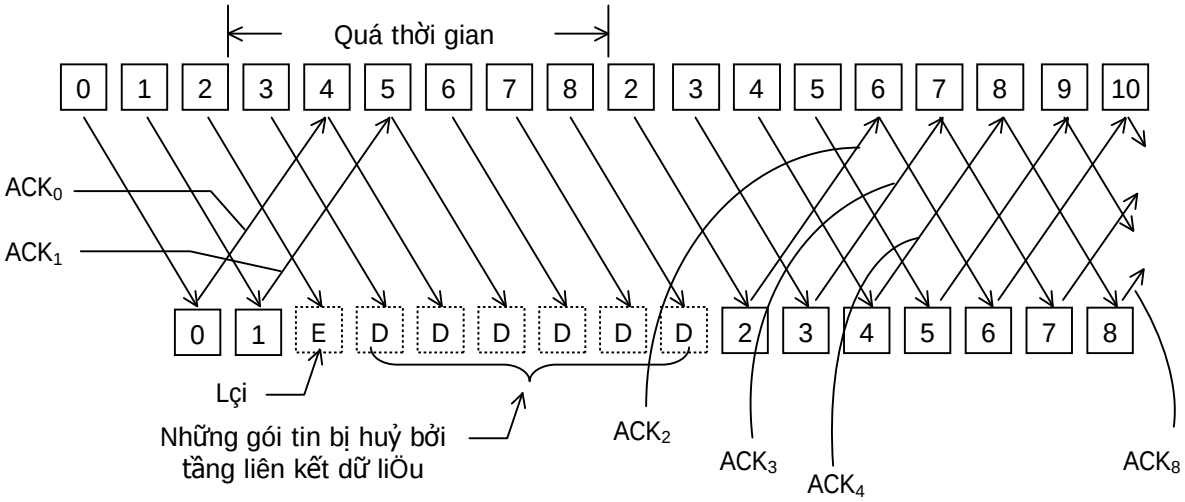
Để nâng cao hiệu suất đường truyền ta không chờ tín hiệu biên nhận mà cứ phát tiếp. Ví dụ, với thời gian phát 20ms cho một gói tin, ta sẽ gửi liên tục 26 gói tin. Như thế khi gửi hết 26 gói tin thì mất khoảng thời gian là 520 ms, đúng lúc tín hiệu biên nhận cho gói tin 0 cũng vừa đến. Kỹ thuật này gọi là Pipe-Lining (vận chuyển liên tục).

Khi có gói tin ở đoạn giữa bị hỏng thì làm thế nào ?, có bỏ những gói tin đúng đi tiếp sau nó không?. Có hai phương pháp như sau :

- Phát lại tất cả các gói tin kể từ gói tin hỏng (*go back n*)
- Phát lại chỉ riêng gói tin bị hỏng, còn gọi là phát có chọn lọc .
- Phát lại từ gói tin hỏng

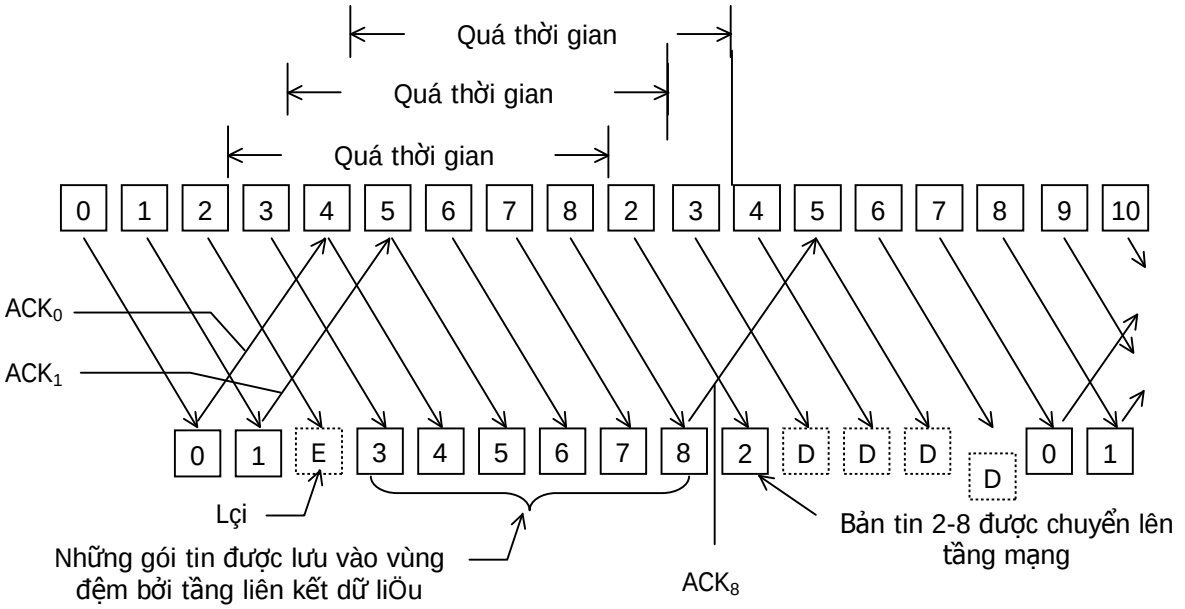
Trong trường hợp này, bên thu huỷ bỏ các gói tin tiếp theo gói tin bị hỏng. Bên phát phát lại tất cả các gói tin chưa được biên nhận bắt đầu từ gói tin bị hỏng.

Phương pháp này lãng phí đường truyền vì phải phát lại nhiều gói tin.




Hình 3-5. Cơ chế vận chuyển liên tục.

### *3.5.3.1 Phát lại có chọn läc*




Hình 3-6. Cơ chế phát bản tin có chọn lọc.

Trong phương pháp này, các gói tin nhận được có thể không theo thứ tự nhưng sẽ được sắp xếp lại để chuyển lên tầng mạng theo đúng thứ tự. Khi có gói tin bị lỗi, bên thu tiếp tục thu các gói tin đúng sau gói tin hỏng ở tầng 2. Bên phát chỉ phát lại

gói tin hỏng. Phương pháp này ứng với cửa sổ bên thu lớn hơn 1 và đòi hỏi bộ nhớ lớn để giữ các gói tin sau gói tin hỏng.

## 3.6 Các giao thức của tầng Liên kết dữ liệu

Tầng LKDL cung cấp các phương tiện để truyền thông tin qua liên kết vật lý đảm bảo tin cậy thông qua các cơ chế đồng bộ hóa, kiểm soát lỗi và kiểm soát luồng dữ liệu. Các giao thức được xây dựng cho tầng LKDL (DLP - Data Link Protocol) được phân thành hai loại :

1. Giao thức dị bộ (asynchronous DLP) : Cho phép một ký tự dữ liệu được truyền đi bất kỳ lúc nào mà không cần quan tâm đến các tính hiệu đồng bộ trước đó.
2. Giao thức đồng bộ (synchronous DLP) : Chèn các ký tự điều khiển hoặc các cờ giữa các dữ liệu của người sử dụng để báo cho bên nhận. Có hai nhóm giao thức đồng bộ :
    a. Đồng bộ hướng ký tự (character -oriented)
    b. Đồng bộ hướng bit (bit - oriented)

Các hệ thống truyền thông đòi hỏi hai mức đồng bộ hóa :

- Mức vật lý : để giữ đồng bộ giữa các đồng hồ người gửi và người nhận
- Mức LKDL : để phân biệt dữ liệu của người sử dụng với các 'cờ'và các vùng thông tin điều khiển khác

Sau đây ta xét hai loại giao thức đồng bộ là giao thức truyền tin đồng bộ nhị phân BSC (Binary Synchronous Control) và giao thức điều khiển liên kết dữ liệu mức cao HDLC (Highlevel Data Link Control).

### 3.6.1 Giao thức BSC

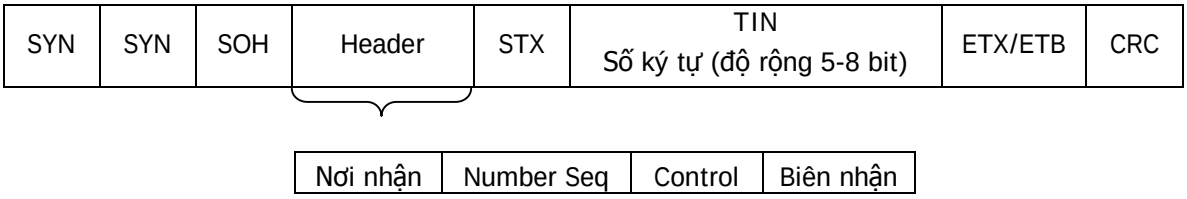
Đây là giao thức *hướng ký tự* (COP - Character Oriented Protocol) được xây dựng dựa trên các ký tự đặc biệt của một bộ mã chuẩn nào đó (như ASCII hoặc EBCDIC) hoạt động theo phương thức hai chiều luân phiên.

#### *3.6.1.1 Tập ký tự điều khiển*

ENQ (05): Enquire - Yêu cầu trả lời từ một trạm xa
ACK (06): Acknowledgement - Thông báo tiếp nhận tốt thông tin
NAK (15): Negative ACK - Thông báo tiếp nhận không tốt thông tin
STX (02): Start of text - Kết thúc phần Header và bắt đầu phần dữ liệu
ETX (03): End of text - Kết thúc phần dữ liệu
ETB (17): End of transmission block - Kết thúc đoạn tin (khối dữ liệu)

SOH (01): Start of heading - Bắt đầu phần header của bản tin
EOT (04): End of transmission - Kết thúc quá trình truyền tin và giải phóng liên kết
DLE (10): Data Link Escape - Để thay đổi ý nghĩa của các ký tự điều khiển truyền tin khác
SYN (16): Synchronous - Ký tự đồng bộ bản tin dùng để duy trì đồng bộ giữa 2 bên

### *3.6.1.2 Khuôn dạng tổng quát bản tin của giao thức BSC*

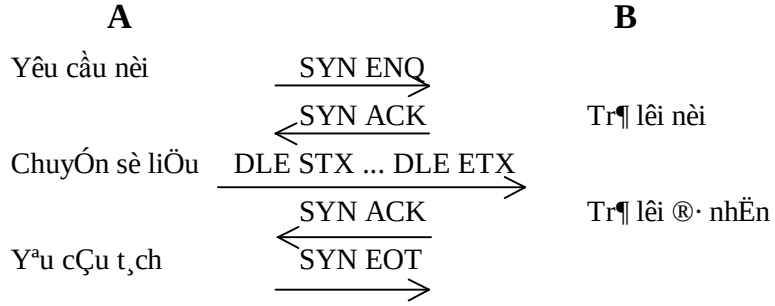



Để thông suốt bản tin, có thể dùng thêm các byte đệm :

| SYN | SYN | | DLE | DLE | | DLE | ETX/ETB | CRC |
|---|---|---|---|---|---|---|---|---|

Khi phát nếu ký tự phát trùng với DLE thì ta chèn thêm DLE. Khi thu, DLE chèn thêm sẽ được khử bỏ.

Ví dụ về thủ tục BCS




## 3.6.2 Giao thức HDLC

HDLC là giao thức hướng bit (Bit Oriented Protocol - BOP) có các phần tử của giao thức (đơn vị dữ liệu, thủ tục) được xây dựng từ các cấu trúc nhị phân (xâu bit) và khi nhận dữ liệu sẽ được tiếp nhận lần lượt từng bit một.

Đây là giao thức có vị trí quan trọng nhất, được ISO phát triển để sử dụng trong cả hai trường hợp : điểm - điểm và nhiều điểm, cho phép truyền thông hai chiều đồng thời.

### *3.6.2.1 Khuôn dạng tổng quát bản tin của giao thức HDLC*

<--- *Hướng truyền*

| | 8 bits | 8 bits | 128-1024 bytes | | |
|---|---|---|---|---|---|
| Flag | HEADER | | INFORMATION | FCS | Flag |
| 01111110 | Address | Control | Số các bit | (16 bit) | 01111110 |

*Trong đó :*

- *Flag* (01111110): là cờ dùng để nhận biết điểm bắt đầu và kết thúc bản tin.

Để tránh sự xuất hiện của mã cờ trong nội dung của bản tin, người ta cài đặt cơ chế '*cứng*' có các chức năng sau :

- Khi truyền tin cứ sau năm bit 1 liên tiếp thì thêm một bit 0 để không nhầm với Flag : 01101111111110010

  01101111011110010

  ↑ *bit chèn thêm (khi thu thì bit này sẽ được khử bỏ)*
- Khi nhận tin, nếu phát hiện có bit 0 sau 5 bit 1 liên tiếp thì tự động loại bỏ bít 0 đó đi.

- *Address* : vùng chứa địa chỉ trạm đích của khung tin.
- *Information* : vùng ghi thông tin truyền đi, có kích thước không xác định.
- *FCS (Frame Check Sequence)* : vùng để ghi mã kiểm soát lỗi (checksum) cho nội dung khung tin, dùng phương pháp CRC với đa thức sinh là CRC-CCITT = $x^{16} + x^{12} + x^5 + 1$
- *Control* : vùng định danh cho các loại khung tin khác nhau của HDLC, có ba dạng như sau :

  Dạng I : hiệu lực truyền tin tức - Information
  Dạng S : hiệu lực điều hành sự nối - Supervisor
  Dạng N : chức năng phụ của điều hành nối – Unnumbered

#### *3.6.2.2 Phương thức trao đổi thông tin*

Giao thức HDLC có 3 phương thức trao đổi thông tin chính, ứng với mỗi phướng thức có các giao thức khung tin tương ứng là SNRM, SARM hoặc SABM :

- *Phương thức trả lời chuẩn SNRM (Set Normal Response Mode):* Được sử dụng trong trường hợp cấu hình không cân bằng, có một trạm điều khiển chung (master), các trạm còn lại (slave) chỉ có thể truyền tin khi trạm chủ cho phép.
- *Phương thức trả lời dị bộ SARM (Set Asynchronous Response Mode):* Cũng được sử dụng trong trường hợp cấu hình không cân bằng như trường hợp trên, nhưng các trạm slave được phép truyền tin mà không cần sự cho phép của trạm master. Phương thức này được sử dụng trong trường hợp điểm-điểm với liên kết 2 chiều, cho phép trạm slave gửi các gói tin (frame) không đồng bộ với trạm master.

- *Phương thức trả lời dị bộ cân bằng SABM* (Set Asynchronous Balanced Mode) : Sử dụng trong trường hợp điểm-điểm, liên kết 2 chiều. Trong đó các trạm đều có vai trò tương đương.

#### *3.6.2.3 Các giao thức dẫn xuất của HDLC*

- LAP (Link Access Procedure) : tương ứng với phương thức trả lời dị bộ (ARM).
- LAPB (Link Access Protocol-Balanced) : tương ứng với phương thức trả lời dị bộ cân bằng (ABM), được dùng hầu hết trong các mạng truyền dữ liệu công cộng X25.
- LAP-D (Link Access Procedure, D Channel ) : Được xây dựng từ LAP-B và được dùng như giao thức liên kết dữ liệu cho các mạng ISDN
- SDLC, ADCCP

#### *3.6.2.4 So sánh BOP và COP*

- BOP nhận lần lượt từng bit một, do đó mềm dẻo, dễ dàng tương thích với các hệ khác nhau.
- BOP có overhead (phụ trội) ngắn, số bít bổ sung và số tín hiệu điều khiển ít do đó có tốc độ cao.
- Thủ tục điều khiển trên bit nhị phân đảm bảo không phụ thuộc mã dùng. Cách giải quyết này mềm dẻo và cho phép giải quyết vô số yêu cầu khác.
- Thủ tục HDLC được coi là chuẩn quốc tế và sẽ thông trị trong thời gian tới, nó thích ứng với các hệ thống phức tạp. Đối với các thiết bị ít phức tạp có thể dùng HDLC đơn giản hoá để đảm bảo sự tương thích với HDLC và sự phát triển mở rộng hệ thống sau này.

# BÀI TẬP

1. Tìm hiểu thêm về chuẩn giao tiếp RC232 và các chuẩn khác được phát tiển từ chuẩn này.
2. Tìm hiểu các chuẩn mở rộng của giao thức HDLC.

-

*Chương 4*

# MẠNG CỤC BỘ

Mạng cục bộ (LAN) là hệ truyền thông tốc độ cao được thiết kế để kết nối các máy tính và các thiết bị xử lý dữ liệu khác cùng hoạt động với nhau trong một khu vực địa lý nhỏ như ở một tầng của toà nhà, hoặc trong một toà nhà.... (100m đến vài km), có tốc độ truyền dữ liệu cao (có thể tới 100Mbps), tỷ lệ sai số dữ liệu nhỏ ($10^{-8}$ ->$10^{-11}$). Một số mạng LAN có thể kết nối lại với nhau trong một khu làm việc.

Mạng LAN thường bao gồm một hoặc một số máy chủ (file server, host), còn gọi là máy phục vụ) và một số máy tính khác gọi là trạm làm việc (Workstations, Client) hoặc còn gọi là nút mạng (Network Node) - một hoặc một số máy tính cùng nối vào một thiết bị nút.

## 4.1 Các cấu hình của mạng LAN

Cấu hình (topology) của mạng là cấu trúc hình học không gian mà thực chất là cách bố trí phần tử của mạng cũng như cách nối giữa chúng với nhau. Thông thường mạng có 3 dạng cấu trúc là: Mạng dạng hình sao (Star Topology), mạng dạng vòng (Ring Topology) và mạng dạng tuyến (Linear Bus Topology). Ngoài 3 dạng cấu hình kể trên còn có một số dạng khác biến tướng từ 3 dạng này như mạng dạng cây, mạng dạng hình sao - vòng, mạng hỗn hợp,v.v....

### 4.1.1 Mạng dạng hình sao (Star Topology)

Mạng dạng hình sao bao gồm một trung tâm và các nút thông tin. Các nút thông tin là các trạm đầu cuối, các máy tính và các thiết bị khác của mạng. Trung tâm của mạng điều phối mọi hoạt động trong mạng với các chức năng cơ bản là:

- Xác định cặp địa chỉ gửi và nhận được phép chiếm tuyến thông tin và liên lạc với nhau.
- Cho phép theo dõi và xử lý sai trong quá trình trao đổi thông tin.
- Thông báo các trạng thái của mạng...

Ưu điểm :

- Hoạt động theo nguyên lý nối song song nên nếu có một thiết bị nào đó ở một nút thông tin bị hỏng thì mạng vẫn hoạt động bình thường.
- Cấu trúc mạng đơn giản và các thuật toán điều khiển ổn định.
- Mạng có thể mở rộng hoặc thu hẹp tuỳ theo yêu cầu của người sử dụng.

Nhược điểm:

- Khả năng mở rộng mạng hoàn toàn phụ thuộc vào khả năng của trung tâm. Khi trung tâm có sự cố thì toàn mạng ngừng hoạt động.

- Mạng yêu cầu nối độc lập riêng rẽ từng thiết bị ở các nút thông tin đến trung tâm. Khoảng cách từ máy đến trung tâm rất hạn chế (100 m).

Nhìn chung, mạng dạng hình sao cho phép nối các máy tính vào một bộ tập trung (HUB) bằng cáp xoắn, giải pháp này cho phép nối trực tiếp máy tính với HUB không cần thông qua trục BUS, tránh được các yếu tố gây tắc nghẽn mạng. Gần đây, cùng với sự phát triển switching hub, mô hình này ngày càng trở nên phổ biến và chiếm đa số các mạng mới lắp.

### 4.1.2 Mạng hình tuyến (Bus Topology)

Theo cách bố trí hành lang các đường như hình vẽ thì máy chủ (host) cũng như tất cả các máy tính khác (workstation) hoặc các nút (node) đều được nối về với nhau trên một trục đường dây cáp chính để chuyển tải tín hiệu.

Tất cả các nút đều sử dụng chung đường dây cáp chính này. Phía hai đầu dây cáp được bịt bởi một thiết bị gọi là terminator. Các tín hiệu và gói dữ liệu (packet) khi di chuyển lên hoặc xuống trong dây cáp đều mang theo địa chỉ của nơi đến.

Loại hình mạng này dùng dây cáp ít nhất, dễ lắp đặt. Tuy vậy cũng có những bất lợi đó là sẽ có sự ùn tắc giao thông khi di chuyển dữ liệu với lưu lượng lớn và khi có sự hỏng hóc ở đoạn nào đó thì rất khó phát hiện, một sự ngừng trên đường dây để sửa chữa sẽ ngừng toàn bộ hệ thống.

### 4.1.3 Mạng dạng vòng (Ring Topology)

Mạng được bố trí theo dạng vòng tròn, đường dây cáp được thiết kế làm thành một vòng khép kín, tín hiệu chạy quanh theo một chiều nào đó. Các nút truyền tín hiệu cho nhau mỗi thời điểm chỉ được một nút mà thôi. Dữ liệu truyền đi phải có kèm theo địa chỉ cụ thể của mỗi trạm tiếp nhận.

Mạng Token Ring có thể chạy ở tốc độ 4Mbps hoặc 16Mbps. Phương pháp truy cập dùng trong mạng Token Ring gọi là Token passing. Token passing là phương pháp truy nhập xác định, trong đó các xung đột được ngăn ngừa bằng cách ở mỗi thời điểm chỉ một trạm có thể được truyền tín hiệu. Điều này được thực hiện bằng việc truyền một bó tín hiệu đặc biệt gọi là Token (mã thông báo) xoay vòng từ trạm này qua trạm khác. Một trạm chỉ có thể gửi đi bó dữ liệu khi nó nhận được Token, khi đó nó sẽ chiếm được quyền ưu tiên hoạt động trên mạng.

Mạng dạng vòng có thuận lợi là có thể nới rộng ra xa, tổng đường dây cần thiết ít hơn so với hai kiểu trên. Nhược điểm là đường dây phải khép kín, nếu bị ngắt ở một nơi nào đó thì toàn bộ hệ thống cũng bị ngừng.

### 4.1.4 Mạng dạng kết hợp

#### *4.1.4.1 Kết hợp hình sao và tuyến (star/Bus Topology)*

Cấu hình mạng dạng này có bộ phận tách tín hiệu (spitter) giữ vai trò thiết bị trung tâm, hệ thống dây cáp mạng có thể chọn hoặc Ring Topology hoặc Linear Bus Topology.

Ưu điểm của cấu hình này là mạng có thể gồm nhiều nhóm làm việc ở cách xa nhau, ARCNET là mạng dạng kết hợp Star/Bus Topology. Cấu hình dạng này đưa lại sự uyển chuyển trong việc bố trí đường dây tương thích dễ dàng đối với bất cứ toà nhà nào.

#### 4.1.4.2 Kết hợp hình Sao và Vòng (Star/Ring Topology)

Cấu hình dạng kết hợp Star/Ring Topology, có một "thẻ bài" (token) được chuyển vòng quanh một cái HUB trung tâm. Mỗi trạm làm việc được nối với HUB - là cầu nối giữa các trạm làm việc và để tăng khoảng cách cần thiết.

Một hub thông thường có nhiều cổng nối với người sử dụng để gắn máy tính và các thiết bị ngoại vi. Mỗi cổng hỗ trợ một bộ kết nối dùng cặp dây xoắn 10BASET từ mỗi trạm của mạng. Khi bó tín hiệu Ethernet được truyền từ một trạm tới hub, nó được lặp lại trên khắp các cổng khác của hub. Các hub thông minh có thể định dạng, kiểm tra, cho phép hoặc không cho phép bởi người điều hành mạng từ trung tâm quản lý hub. Có ba loại hub:

- Hub đơn (stand alone hub)
- Hub modun (modular hub) : Modular hub rất phổ biến cho các hệ thống mạng vì nó có thể dễ dàng mở rộng và luôn có chức năng quản lý, modular có từ 4 đến 14 khe cắm, có thể lắp thêm các modun Ethernet 10BASET.
- Hub phân tầng (stackable hub) : thuận tiện cho những cơ quan muốn đầu tư tối thiểu ban đầu nhưng lại có kế hoạch phát triển LAN sau này.

## 4.2 Các giao thức điều khiển truy nhập đường truyền

Giao thức dùng để đánh giá khả năng của một mạng được phân chia bởi các trạm như thế nào. Hệ số này được quyết định chủ yếu bởi hiệu quả sử dụng môi trường truy xuất (medium access) của giao thức.

Mọi kênh phương tiện chỉ có thể hỗ trợ một lần tín hiệu. Nếu hai máy tính truyền trên kênh cùng một lúc, các tín hiệu của chúng sẽ gây nhiễu cho nhau (ví dụ như hai người cùng nói một lúc). Có hai phương pháp điều khiển việc truy nhập phương tiện để không xảy ra sự cố gây nhiễu : truy nhập ngẫu nhiên và truy nhập có điều khiển.

- *Loại truy nhập ngẫu nhiên*

Trạm có thể truy nhập phương tiện truyền tuỳ theo ý muốn, bất kỳ ở thời điểm ngẫu nhiên nào.

a. Kỹ thuật truy cập ngẫu nhiên đối với dạng bus

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

b. Kỹ thuật truy cập ngẫu nhiên đối với dạng vòng

- Phương pháp chèn thanh ghi (Register insertion)
- Phương pháp vòng có ngăn (Slotted-ring)

- *Loại truy nhập có điều khiển*

Phương pháp điều khiển tranh chấp thường thích hợp với các mạng có sự trao đổi dữ liệu không liên tục và tương đối ít máy tính. Đây là dạng thông dụng trong cấu trúc mạng cục bộ.

- Kỹ thuật bus với thẻ bài (Token Bus) : dùng cho các mạng LAN
- Kỹ thuật vòng với thẻ bài (Token Ring) : dùng cho các mạng LAN
- Kỹ thuật tránh xung đột : dùng cho các mạng cục bộ tốc độ cao.

### 4.2.1 Phương pháp CSMA

Còn được gọi là phương pháp LBT (Listen Before Talk - Nghe trước khi nói). Một trạm có dữ liệu cần truyền trước hết phải 'nghe' xem phương tiện truyền rỗi hay bận. Nếu rỗi thì bắt đầu truyền tin, còn nếu bận thì thực hiện một trong ba giải thuật sau :

- Giải thuật '*non-persistent*' : Tram rút lui (không kiên trì) chờ đợi một thời gian ngẫu nhiên nào đó rồi lại bắt đầu 'nghe' đường truyền. Giải thuật này có hiểu quả tránh xung đột nhưng có thời gian chết.
- Giải thuật '*1-persistent*' : Trạm tiếp tục nghe đến khi phương tiện truyền rỗi thì tiến hành truyền dữ liệu đi (với xác xuất 1). Giải thuật này giảm thời gian chết, xong nếu có nhiều trạm cùng chờ và tiến hành phát dữ liệu cùng một lần thì sẽ xảy ra xung đột.
- Giải thuật '*p-persistent*' : trạm tiếp tục nghe, đến khi phương tiện truyền rỗi thì tiến hành phát tin với một xác xuất nhất định nào đó (mỗi trạm có gắn một hệ số ưu tiên). Ngược lại trạm 'rút lui' trong một thời gian cố định rồi

truyền với xác suất p hoặc tiếp tục chờ đợi với xác xuất 1-p. Giải thuật này phức tạp nhưng giảm được tối đa xung đột và thời gian chết.

Phương pháp CSMA chỉ 'nghe trước khi nói', không có khả năng phát hiện xung đột trong quá trình truyền, dẫn đến lãng phí đường truyền.

### 4.2.2 Phương pháp CSMA/CD

Phương pháp CSMA/CD có nguồn gốc từ hệ thống radio đã phát triển ở trường đại học Hawai vào khoảng năm 1970, gọi là ALOHANET, còn được gọi là phương pháp LWT (Listen While Talk - Nghe cả trong khi nói). Các va chạm luôn xảy ra tại một cấp nào đó trên các mạng, với số lượng gia tăng theo tỉ lệ thuận khi các phiên truyền gia tăng.

Phương pháp CSMA/CD ngoài các chức năng của CSMA còn bổ sung các quy tắc sau :

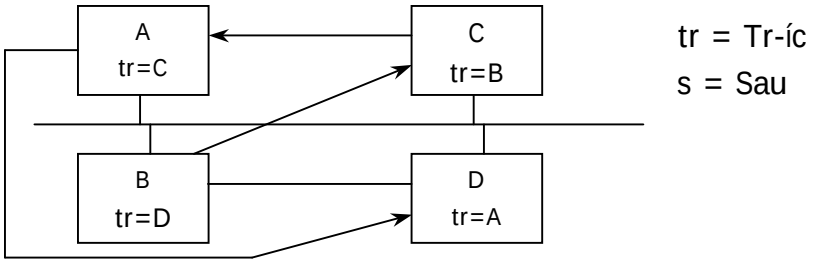
1. Khi đang truyền vẫn tiếp tục nghe đường dây.
2. Nếu phát hiện có xung đột thì *ngừng truyền* và *tiếp tục gởi sóng mang* thêm một thời gian nữa để bảo đảm các trạm đều có thể nghe được sự kiện xung đột.
3. Sau khi chờ đợi một thời gian ngẫu nhiên thì trạm thử truyền lại bằng cách sử dụng các phương pháp của CSMA.

Với phương pháp CSMA/CD thời gian chiếm dụng vô ích đường truyền giảm xuống bằng thời gian dùng để phát hiện một đụng độ. CSMA/CD sử dụng ba giải thuật 'persistent' ở trên. Trong đó giải thuật '*1-persistent*' được sử dụng trong mạng Ethernet, Mitrenet và được chọn cả trong chuẩn IEEE.802. Ngoài ra mỗi chuẩn LAN còn có thêm các cơ chế bổ sung.

### 4.2.3 Điều khiển truy nhập bus với thẻ bài

Các trạm trên bus tạo nên một vòng logic, được xác định vị trí theo một dãy thứ tự, trong đó trạm cuối sẽ tiếp liền ngay sau trạm đầu tiên. Mỗi trạm được biết địa chỉ của các trạm kề sau và kề trước nó.

Thẻ bài dùng cấp phát quyền truy nhập, được lưu chuyển trong vòng logic. Khi trạm nhận được thẻ bài thì được trao quyền sử dụng phương tiện trong một thời gian xác định để truyền dữ liệu. Khi truyền xong hoặc hết thời hạn, trạm sẽ chuyển thẻ bài đến trạm kế tiếp trong vòng logic. Các trạm không sử dụng thẻ bài vẫn có mặt trên bus nhưng chúng chỉ có thể trả lời cho yêu cầu xác nhận (nếu chúng là đích của gói tin nào đó). Thứ tự vật lý của trạm trên bus là không quan trọng, độc lập với thứ tự logic.




Hình 4-1. Điều khiển truy nhập bus với thẻ bài.

*Các chức năng :*

- Khởi tạo vòng logic : khi thiết lập mạng hoặc khi vòng logic bị gãy.
- Bổ sung trạm vào vòng logic (xem xét định kỳ) bằng cách mời nút đứng sau nhập vòng. Loại bỏ một trạm ra khỏi vòng logic bằng cách nối trạm trước và sau nó với nhau
- Quản lý sai sót : trùng địa chỉ, gãy vòng (các trạm bị treo, rơi vào trạng thái chờ lẫn nhau), bởi nút giữ Token.
- Khi đang giữ thẻ mà có trạm khác nhận được gói tin thì chứng tỏ nút khác đã có thẻ, lúc đó nó sẽ bỏ thẻ bằng cách chuyển sang trạng thái 'nghe'.
- Khi nút đã hoàn thành công việc, nó gửi thẻ đến nút đứng sau, nếu nút tiếp sau hoạt động thì nó gởi thẻ chuyển sang trạng thái bị động. Nếu ngược lại, nó gửi thẻ cho nút kế tiếp lần nữa. Nếu hai lần gửi không được thì xem như nút kế tiếp hỏng và gửi đi gói tin "tìm nút kế tiếp" để tìm nút tiếp theo.
- Nếu không thành công thì nút bị xem là có sự cố. Nút ngừng hoạt động và 'nghe' trên bus.

- Dạng bản tin của mạng Token bus

| Bắt đầu tin | Điều khiển gói tin | Địa chỉ nguồn | Địa chỉ đích | TIN | FSC | Kết thúc tin |
|---|---|---|---|---|---|---|
| 1 byte | 1 byte | 2-6 bytes | 2 - 6 bytes | | 4 bytes | 1 byte |
| | Khung tin cực đại 8191 bytes | | | | Tốc độ có thể là 1; 5; 10Mbps | |

- So sánh CSMA/CD và Token Bus

- Token bus quản lý phức tạp hơn so với CSMA/CD. Trong trường hợp tải nhẹ thì không hiệu quả bằng CSMA/CD (do phải qua nhiều trạm)
- Tuy nhiên Token Bus có hiệu quả trong trường hợp tải nặng, dễ điều hoà lưu thông trên mạng Token Bus. Không quy định độ dài tối thiểu của gói tin, không cần nghe trước khi nói.

### 4.2.4 Điều khiển truy nhập vòng với thẻ bài

Đây là giao thức thông dụng được dùng trong các LAN có cấu trúc vòng (Ring). Phương pháp này sử dụng một khối tín hiệu đặc biệt gọi là Token di chuyển vòng quanh mạng theo một chiều xác định. Một trạm muốn truyền phải đợi cho đến khi nhận được thẻ bài. Khi một trạm đang chiếm Token thì nó có thể phát đi một gói dữ liệu. Khi đã phát hết gói dữ liệu cho phép hoặc không còn gì để phát nữa thì trạm đó chuyển khung thẻ bài đến cho trạm kế tiếp trên mạng. Trong token có chứa một địa chỉ đích và được luân chuyển tới các trạm theo một trật tự đã định trước. Đối với cấu hình mạng dạng xoay vòng thì trật tự của sự truyền token tương đương với trật tự vật lý của các trạm xung quanh vòng.

Các chuẩn mạng sử dụng phương pháp điều khiển truy nhập thẻ bài :

- Chuẩn IEEE 802.5, còn gọi là chuẩn Token Ring.
- FDDI là chuẩn sợi quang 100 Mps sử dụng phương pháp chuyển thẻ bài và vòng tròn.

Phương pháp chuyển thẻ bài thích hợp trong các điều kiện như sau :

- Khi mạng đang tải dữ liệu quan trọng về thời gian do phương pháp này cung cấp khả năng bàn giao.
- Khi mạng được sử dụng nhiều, do tránh được xung đột.
- Khi một vài trạm có mức ưu tiên cao hơn so với các trạm khác. Phương pháp chuyển thẻ bài có thể áp dụng các mức ưu tiên cho trạm để ngăn cấm một trạm bất kỳ không được độc quyền về mạng.
- Do thẻ bài luân chuyển quanh mạng nên mỗi trạm có thể truyền theo quãng thời gian tối thiểu.

Phương pháp chuyển thẻ bài đòi hỏi cơ chế điều khiển phức tạp và chi phí đầu tư phần cứng cao, nhưng được thiết kế với độ tin cậy cao. Tuy vậy hiện nay Ethernet vẫn là chuẩn LAN thông dụng, chứng tỏ được ưu điểm của phương pháp tranh chấp khi sử dụng trên các mạng LAN.

Giao thức truyền token có trật tự hơn nhưng cũng phức tạp hơn CSMA/CD, có ưu điểm là vẫn hoạt động tốt khi lưu lượng truyền thông lớn. Giao thức truyền token tuân thủ đúng sự phân chia của môi trường mạng, hoạt động dựa vào sự xoay vòng tới các trạm. Việc truyền token sẽ không thực hiện được nếu việc xoay vòng bị đứt đoạn. Giao thức phải chứa các thủ tục kiểm tra token để cho phép khôi phục lại token bị mất hoặc thay thế trạng thái của token và cung cấp các phương tiện để sửa đổi logic (thêm vào, bớt đi hoặc định lại trật tự của các trạm).

Khung tin cực đại là 16KB ở chế độ truyền 16Mbps và 4KB ở chế độ truyền 4Mps.

Dạng bản tin với mạng Token Ring :

| Bắt đầu tin | Điều khiển thâm nhập | Điều khiển gói tin | Địa chỉ nguồn | Địa chỉ đích | TIN | FSC | Kết thúc gói tin | Trạng thái gói tin |
|---|---|---|---|---|---|---|---|---|
| 1 byte | 1 byte | 2-6 bytes | 2 - 6 bytes | 2 - 6 bytes | | 4 bytes | 1 byte | 1 byte |

#### *4.2.4.1 Phương pháp điều khiển truy nhập dò báo*

Dò báo (*polling*) là một phương pháp điều khiển truy cập sử dụng một thiết bị trung tâm để điều khiển toàn bộ việc truy cập mạng. Đây là phương pháp được sử dụng phổ dụng nhất trên các mạng máy tính lớn.

Thiết bị trung tâm có tên là thiết bị chính sẽ yêu cầu dữ liệu từ các thiết bị khác trên mạng có tên là thiết bị thứ cập (*secondaries*). Sau khi được dò báo, thiết bị thứ cấp có thể truyền một lượng dữ liệu được xác định bởi các giao thức dùng trên mạng. Một thiết bị thứ cấp không thể truyền trừ phi nó được thiết bị chính dò báo.

Phương pháp dò báo có nhiều ưu điểm của phương pháp chuyển thẻ bài như :

- Dự đoán được các lần truy cập định sẵn.
- Gán được các mức ưu tiên, tránh được va chạm.

So sánh phương pháp dò báo và phương pháp chuyển thẻ bài : kỹ thuật dò báo tập trung hóa quyền điều khiển. Nhìn dưới góc độ quản lý thì đây là một ưu điểm, nhưng nếu cơ chế điều khiển trung tâm bị hỏng, mạng sẽ ngừng hoạt động. Phương pháp chuyển thẻ bài sử dụng các chức năng điều khiển phân phối hơn do đó ít bị hỏng tập trung tại một điểm. Bên cạnh đó, phương pháp dò báo đôi khi lãng phí các lượng băng thông lớn do phải dò báo từng thiết bị thứ cấp, cho dù các thiết bị không có gì để truyền.

## 4.3 Chuẩn hóa mạng cục bộ

Các chuẩn LAN là các tiêu chuẩn công nghệ cho Lan được phê chuẩn bởi các tổ chức chẩun hóa quốc tế, nhằm hướng dẫn các nhà sản xuất thiết bị mạng đi đến sự thống chung khả năng sử dụng chung các sản phẩm của họ, vì lợi ích của người sử dụng và tạo điều kiện thuận lợi cho các nghiên cứu phát triển.

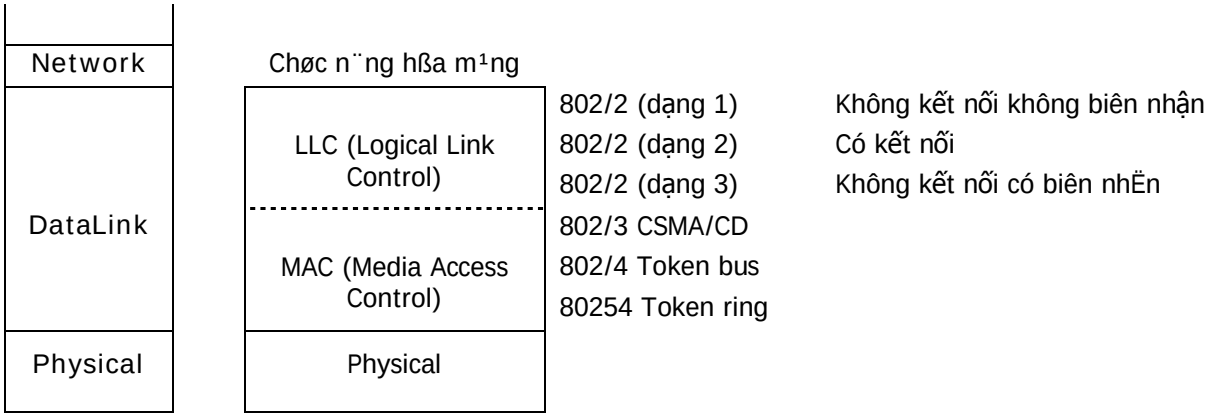
Các chuẩn này quy định môi trường truyền dẫn cũng như cách thức sử dụng chúng trong kết nối LAN; Các giao thức truyền thông ở các tầng vật lý và tầng liên kết dữ liệu của mạng theo mô hình OSI.

Các giao thức truyền thông ở các tầng trên của mô hình OSIhiện tại được xác định qua một số giao thức phổ biến như TCP/IP, IPX/SPX, NetBIOS,. . .

Uỷ ban IEEE phát triển tiêu chuẩn IEEE LAN và đề xuất phân chia hai tầng thấp nhất của mô hình OSI như dưới đây.

Theo chuẩn 802 thì tầng LKDL được chia thành 2 tầng con:

- Tầng con điều khiển logic LLC (Logical Link Control Sublayer) : giữ vai trò tổ chức dữ liệu, tổ chức thông tin để truyền và nhận. Thủ tục tầng LLC không bị ảnh hưởng khi sử dụng các đường truyền dẫn khác nhau, nhờ vậy mà linh hoạt hơn trong khai thác.
- Tầng con điều khiển xâm nhập mạng MAC (Media Access Control Sublayer). làm nhiệm vụ điều khiển việc xâm nhập mạng.




Hình 4-2. Các tầng con LLC và MAC.

Chuẩn 802.2 ở mức con LLC tương đương với chuẩn HDLC của ISO hoặc X.25 của CCITT.

Chuẩn 802.3 xác định phương pháp thâm nhập mạng tức thời có khả năng phát hiện lỗi chồng chéo thông tin CSMA/CD. Phương pháp CSMA/CD được đưa ra từ năm 1993 nhằm mục đích nâng cao hiệu quả mạng. Theo chuẩn này các mức được ghép nối với nhau thông qua các bộ ghép nối.

Chuẩn IEEE 802.3 dùng cho mạng Ethernet (sử dụng giao thức truy nhập CSMA/CD) bao gồm cả 2 phiên bản băng tần cơ bản và băng tần mở rộng.

Chuẩn IEEE 802.4 liên quan tới sự sắp xếp tuyến token, thực chất là phương pháp thâm nhập mạng theo kiểu phát tín hiệu thăm dò token qua các trạm và đường truyền bus.

Chuẩn IEEE 802.5 dùng cho mạng dạng vòng và trên cơ sở dùng tín hiệu thăm dò token. Mỗi trạm khi nhận được tín hiệu thăm dò token thì tiếp nhận token và bắt đầu quá trình truyền thông tin dưới dạng các frame. Các frame có cấu trúc tương tự như của chuẩn 802.4. Phương pháp xâm nhập mạng này quy định nhiều mức ưu tiên khác nhau cho toàn mạng và cho mỗi trạm, việc quy định này vừa cho người thiết kế vừa do người sử dụng tự quy định.

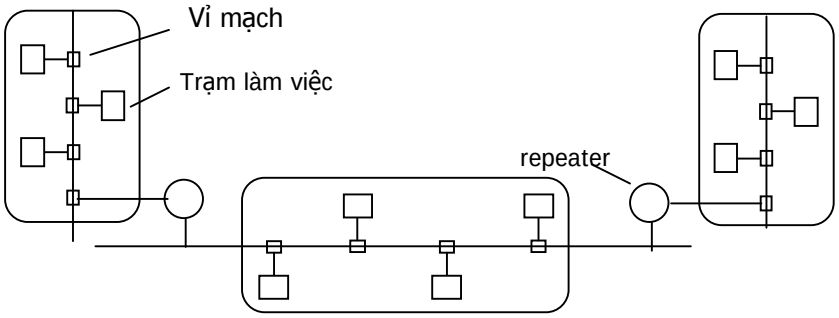
Chuẩn IEEE 802.11 dùng cho mạng không dây (Wireless).

### 4.3.1 Chuẩn Ethernet

Chuẩn Ethernet được sử dụng phổ biến nhất, đến mức đôi khi được hiểu đồng nghĩa với LAN. Tuy nhiên nó đã được xây dựng và phát triển qua các giai đoạn với các tên gọi là DIX standard Ethernet và IEE 802.3 standard. Chuẩn Ethernet do các công ty Xerox, Intel và Digital equipment xây dựng và phát triển. Ethernet LAN được xây dựng theo chuẩn 7 lớp trong cấu trúc mạng của ISO, mạng truyền số liệu Ethernet cho phép đưa vào mạng các loại máy tính khác nhau kể cả máy tính mini. Ethernet có các đặc tính kỹ thuật chủ yếu sau đây:

- Có cấu trúc dạng tuyến phân đoạn, đường truyền dùng cáp đồng trục, tín hiệu truyền trên mạng được mã hoá theo kiểu đồng bộ (Manchester), tốc độ truyền dữ liệu là 10 Mb/s.
- Chiều dài tối đa của một đoạn cáp tuyến là 500m, các đoạn tuyến này có thể được kết nối lại bằng cách dùng các bộ chuyển tiếp và khoảng cách lớn nhất cho phép giữa 2 nút là 2,8 km.
- Sử dụng tín hiệu băng tần cơ bản, truy xuất tuyến (bus access) hoặc tuyến token (token bus), giao thức là CSMA/CD, dữ liệu chuyển đi trong các gói. Gói tin dùng trong mạng có độ dài từ 64 đến 1518 byte.

- Cấu trúc của mạng Ethernet : Mạng Ethernet có cấu trúc dạng bus như sau :




Hình 4-3. Cấu trúc của mạng Ethernet.

Số trạm cực đại trong mạng là 1024, số lượng segment của mạng giới hạn nhỏ hơn 5 segment, khoảng cách tối đa giữa hai trạm là 2,5km. Mạng sử dụng cáp đồng trục tốc độ 10Mps. Cấu trúc khung tin Ethernet có khuôn dạng như sau :

| Cờ | Địa chỉ đích | Địa chỉ nguồn | Loại tin | TIN | CRC | Cờ |
|---|---|---|---|---|---|---|
| | 6 bytes | 6 bytes | 2 bytes | 46 – 1500 bytes | 4 bytes | |

*Chương 5*

# TẦNG MẠNG

Tầng mạng đảm bảo truyền tin thông suốt giữa hai nút đầu cuối trong mạng. Trên cơ sở cấu hình của mạng, tầng mạng sẽ kiểm tra sơ đồ kết nối (*topology*) của toàn mạng để quyết định đường đi tối ưu truyền gói dữ liệu, tránh quá tải trên một đường truyền trong khi một số đường truyền rỗi. Thực hiện cắt/ hợp dữ liệu khi qua mạng và liên kết mạng khi có nhiều mạng nối với nhau.

## 5.1 Các vấn đề của tầng mạng

### 5.1.1 Định địa chỉ cho tầng mạng

Tầng mạng sử dụng các kiểu địa chỉ bổ sung sau :

1. Địa chỉ mạng logic (Logical network addresses), định tuyến các gói tin theo các mạng cụ thể trên liên mạng. Dùng để định danh một mạng cụ thể trên liên mạng dưới dạng một nguồn hay đích của một gói tin.
2. Địa chỉ dịch vụ (Service addresses), định tuyến các gói tin theo các tiến trình cụ thể đang chạy trên thiết bị đích, dùng định danh một giao thức hay tiến trình trên máy tính là nguồn hay đích của một gói tin.
3. Địa chỉ mạng vật lý (MAC) định danh một thiết bị cụ thể dưới dạng một nguồn hay đích của một khung.

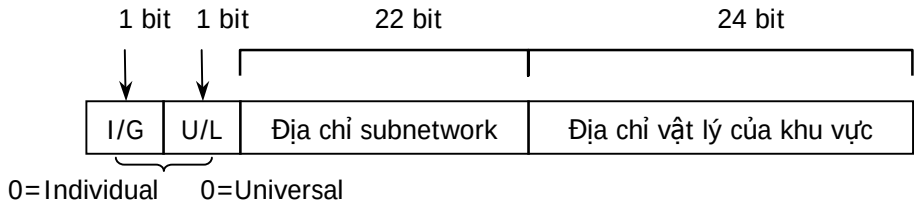
*Địa chỉ vật lý của máy trạm :*

Mỗi thiết bị trên một mạng có một địa chỉ vật lý duy nhất để giao tiếp với các thiết bị khác, còn gọi là địa chỉ phần cứng. Trên tất cả các mạng hiện nay, mỗi địa chỉ xuất hiện một lần duy nhất (nghĩa là mỗi thiết bị chỉ có một địa chỉ duy nhất). Đối với phần cứng, địa chỉ thường được mã hoá trong thiết bị card mạng (Network Interface Card), có thể được đặt bằng chuyển mạch hoặc bằng phần mềm. Trong mô hình OSI thì địa chỉ này được đặt ở lớp vật lý.

Độ dài của địa chỉ vật lý phụ thuộc vào từng mạng, chẳng hạn với mạng Ethernet và một số mạng khác thì dùng địa chỉ vật lý dài 48 bit. Để trao đổi thông tin thì cần có địa chỉ của nơi gởi, và địa chỉ của nơi nhận.

Hiện nay IEEE đang đảm nhiệm việc ấn định địa chỉ vật lý tổng thể (*universal physical address*) cho các subnetwork. Đối với mỗi subnetwork, IEEE ấn định một phần địa chỉ đồng nhất đối với tất cả các subnetwork gọi là OUI (Organization Unique Identifier) phần này có độ dài là 24 bit, cho phép IEEE ấn định phần địa chỉ 24 bit còn lại theo yêu cầu. (Trên thực tế, hai trong 24 bit địa chỉ OUI là các bit điều khiển, do đó 22 bit là để xác định subnetwork đó. Dó đó chỉ có khoảng $2^{22}$ địa chỉ

được dùng, nếu với tốc độ phát triển như hiện nay có thể sẽ thiếu địa chỉ trong tương lai). Sau đây là cấu tạo của địa chỉ OUI :




Hình 5-1. Cấu tạo của địa chỉ vật lý ĂUI.

### 5.1.2 Dịch vụ cung cấp cho tầng giao vận

- Các dịch vụ phải độc lập với công nghệ được dùng trong mạng.
- Tầng giao vận phải độc lập với công nghệ được dùng trong mạng.
- Các địa chỉ mạng phải thống nhất để tầng giao vận có thể dùng cả mạng LAN và WAN.

*Có 2 loại dịch vụ :*

- Dịch vụ truyền tin có liên kết (*Connection Ăriennted Service*)
- Dịch vụ truyền tin không liên kết (*Connectionless Service*)

Sự khác nhau giữa hai dịch vụ

| **Vấn đề** | **Dịch vụ có liên kết** | **Dịch vụ không liên kết** |
|---|---|---|
| Khởi động kênh | Cần thiết | Không |
| Địa chỉ đích | Chỉ cần lúc khởi động | Cần ở mọi gói tin |
| Thự tự gói tin | Được đảm bảo | Không đảm bảo |
| Kiểm soát lỗi | ở tầng mạng | ở tầng giao vận |
| Điều khiển thông lượng | ở tầng mạng | ở tầng giao vận |
| Thảo thuận tham số | Có | Không |
| Nhận dạng liên kết | Có | Không |

Các hàm cơ bản của dịch vụ liên kết tầng mạng :

N-CONNECT. Request (callce, caller, acks wanted, exp wanted, qos, user data)
N-CONNECT. Indication (callce, caller, acks wanted, exp wanted, qos, user data)
N-CONNECT. Response (response acks wanted, exp wanted, qos, user data)
N-CONNECT. Confirmation (response acks wanted, exp wanted, qos, user data)
N-DISCONNNECT. Request (originator, reason, user data, responding address)
N-DISCONNNECT. Indication (originator, reason, user data, responding address)
N-DATA. Request (user data)
N-DATA. Indication (user data)
N-DATA-ACKNOWLEDGED. Request ()
N-DATA-ACKNOWLEDGED. Indication ()
N-EXPEDITED-DATA. Request (user data)
N-EXPEDITED-DATA. Indication (user data)
N-RESET. Request (originator, reason)

N-RESET. Indication (originator, reason)
N-RESET. Response()
N-RESET. Confim()

Các hàm cơ bản của dịch vụ không liên kết tầng mạng

N-UNITDATA. Request (source address, destination address, qos, user_data)
N-UNITDATA. Indication (source address, destination address, qos, user_data)
N-FACILITY. Request (qos)
N-FACILITY. Indication (destination address, qos, reason)
N-FACILITY. Indication (destination address, qos, reason)

Hàm N_FACILITY.request cho phép NSD dịch vụ mạng biết tỷ lệ phần trăm gói tin đang được giao vận.

Hàm N_REPORT.indication cho phép tầng mạng thông báo lại cho NSD dịch vụ mạng.

### 5.1.3 Tổ chức các kênh truyền tin trong tầng mạng

Có hai loại kênh truyền tin hoạt động trong mạng :

#### *5.1.3.1 Kênh ảo (virtual circuit)*

Tương đương kênh điện thoại trong tầng vật lý sử dụng trong mạng có liên kết. Kênh ảo được thiết lập cho mỗi liên kết. Một khi đã được thiết lập thì các gói tin được chuyển đi tương tự trong mạng điện thoại cho đến khi liên kết bị hủy bỏ.

- Mỗi nút mạng chứa một kênh ảo, với cửa vào cho một kênh ảo
- Khi một liên kết được khởi động, một kênh ảo chưa dùng sẽ được chọn
- Nút chọn kênh ảo chứa đường dẫn đến trạm tiếp theo và có số thấp nhất

Khi gói tin khởi động đến nút đích, nút chọn kênh ảo có số thấp nhất thay thế số trong gói tin và chuyển vào trạm đích. Số kênh ảo nối với trạm đích có thể khác số kênh ảo mà trạm nguồn sử dụng.

#### *5.1.3.2 Mạng Datagram*

Tương đương với điện báo sử dụng trong mạng không liên kết. Trong mạng này, không có tuyến đường nào được thiết lập. Các gói tin có thể đi theo nhiều đường khác nhau mà không nhất thiết theo một trình tự xác định. Thông tin vào là địa chỉ đích, thông tin ra là nút mạng phải tới.

Mạng Datagram phức tạp về điều khiển nhưng nếu kênh hỏng thì dễ dàng đi theo kênh khác. Do đó có thể giải quyết được vấn đề tắc nghẽn dữ liệu.

- Các đặc trưng của mạng Datagram và mạng kênh ảo

| Vấn đề | Mạng datagram | Mạng kênh ảo |
|---|---|---|
| *Khởi động kênh* | Không | Cần thiết |
| *Địa chỉ (đ/c) hoá* | Gói tin phải có đ/c nguồn và đ/c đích | Gói tin chỉ cần số của kênh ảo |
| *Thông tin tìm đường* | Không cần bất cứ thông tin nào. | Mỗi kênh ảo cần một vùng trong bảng |
| *Tìm đường* | Mỗi gói tin tìm đường độc lập. Phải tìm đường mỗi khi có gói tin tới nút mạng. | Được thiết lập khi khởi động kênh ảo mới. Liên kết sẽ được duy trì cho cả phiên. |
| *Điều khiển* | Chỉ mất gói tin ở trong nút hỏng | Kênh ảo đi qua nút hỏng sẽ bị huỷ |
| *Hỏng nút* | Khó khắc phục | Dễ khắc phục hơn |
| *Độ phức tạp* | Trong tầng giao vận | Trong tầng mạng |
| *Thích hợp* | Các dịch vụ liên kết và không liên kết | Các dịch vụ liên kết |

### 5.1.4 Tìm đường đi trong mạng

Chức năng quan trọng nhất của tầng mạng là dẫn đường cho các gói tin từ trạm nguồn tới trạm đích. Thuật toán tìm đường là qui trình để quyết định chọn đường ra khỏi nút mạng nhằm gởi gói tin đi tiếp tới nút khác.

- Yêu cầu của thuật toán tìm đường

- Chính xác, ổn định, đơn giản và tối ưu.
- Thuật toán tìm đường phải có khả năng cập nhật lại cấu hình và đường vận chuyển để không phải khởi động lại mạng khi có một nút hỏng hoặc phải ngừng hoạt động của các máy ở trạm.

- Các thuật toán chia làm hai nhóm chính:

- Nhóm không thích nghi (*non adaptive*) : việc chọn đường không dựa vào việc đánh giá tình trạng giao thông và cấu hình trong thời gian thực.
- Nhóm thích nghi (*adaptive*) : việc tìm đường phải thích nghi với tình trạng giao thông hiện tại.

Sơ đồ mạng được biểu diễn dưới dạng đồ thị, mỗi nút của đồ thị là một nút mạng, cung của đồ thị biểu diễn đường truyền nối giữa hai nút. Việc chọn đường giữa hai nút mạng là tìm đường ngắn nhất giữa chúng.

Mỗi cung được gán một nhãn cho biết thời gian trung bình phải đợi và thời gian truyền một gói tin chuẩn. Thời gian này được thử mỗi giờ hay mỗi ngày một lần. Đường ngắn nhất là đường có ít bước chuyển tiếp qua nút nhất và có số đo độ dài nhỏ nhất, mất ít thời gian.

Có nhiều thuật toán để tìm đường ngắn nhất giữa 2 điểm, ví dụ như thuật toán Dijkstra (1959). Ta xây dựng đồ thị cho các nút mạng và tìm khoảng cách giữa các nút mạng.

### 5.1.5 Tắc nghẽn trong mạng

Khi có quá nhiều gói tin trong mạng hay một phần của mạng làm cho hiệu suất của mạng giảm đi vì các nút mạng không còn đủ khả năng lưu trữ, xử lý, gửi đi và chúng bắt đầu bị mất các gói tin. Hiện tượng này được gọi là sự tắc nghẽn (*congestion*) trong mạng.

Hàng đợi sẽ bị đầy (phải lưu tập tin, tạo các bảng chọn đường ...) nếu khả năng xử lý của nút yếu hoặc khi thông tin vào nhiều hơn khả năng của đường ra

*Điều khiển dòng dữ liệu* là xử lý giao thông giữa điểm với điểm, giữa trạm thu và phát. Trong khi đó điều khiển tránh tắc nghẽn là một vấn đề tổng quát hơn bao gồm việc tạo ra hoạt động hợp lý của các máy tính của các nút mạng, quá trình lưu trữ bên trong nút, điều khiển tất cả các yếu tố làm giảm khả năng vận chuyển của toàn mạng.

- Các biện pháp ngăn ngừa

- Bố trí khả năng vận chuyển, lưu trữ, xử lý của mạng dư so với yêu cầu.
- Huỷ bỏ các gói tin bị tắc nghẽn quá thời hạn.
- Hạn chế số gói tin vào mạng nhờ cơ chế cửa sổ (*flow control*).
- Chặn đường vào khi của các gói tin khi mạng quá tải.

## 5.2 Kết nối liên mạng

Nhu cầu trao đổi thông tin và phân chia các tài nguyên dùng chung đòi hỏi hoạt động truyền thông không chỉ ở phạm vi cục bộ mà ở cả khuôn khổ quốc gia và quốc tế. Từ đó dẫn đến sự nối kết các mạng viễn thông tin học được đặt ở các vị trí địa lý khác nhau và chịu sự quản lý của các tổ chức hoặc quốc gia khác nhau.

Sự nối kết mạng (*Networks Interconnection*) giống như ghép nối mạng đơn lẻ nhưng phức tạp hơn nhiều do tính chất không thuần nhất của các mạng con được kết nối. Chúng có thể có kiến trúc khác nhau bao gồm các máy tính nút mạng. Đường truyền khác nhau, chiến lược quản lý khác nhau.

Người ta thường xem xét các vấn đề sau để kết nối các mạng con lại với nhau :

- Xem mỗi nút của mạng con như là một hệ thống mở : mỗi nút mạng con có thể truyền thông trực tiếp với một nút của mạng con khác bất kỳ. Như thế yêu cầu phải xây dựng một chuẩn chung cho các mạng.
- Xem mỗi mạng như là một hệ thống mở : Hai nút thuộc hai mạng con không bắt tay trực tiếp với nhau mà phải thông qua một phần tử trung gian gọi là *giao diện kết nối (interconnection interface)* dat giữa hai mạng con đó.

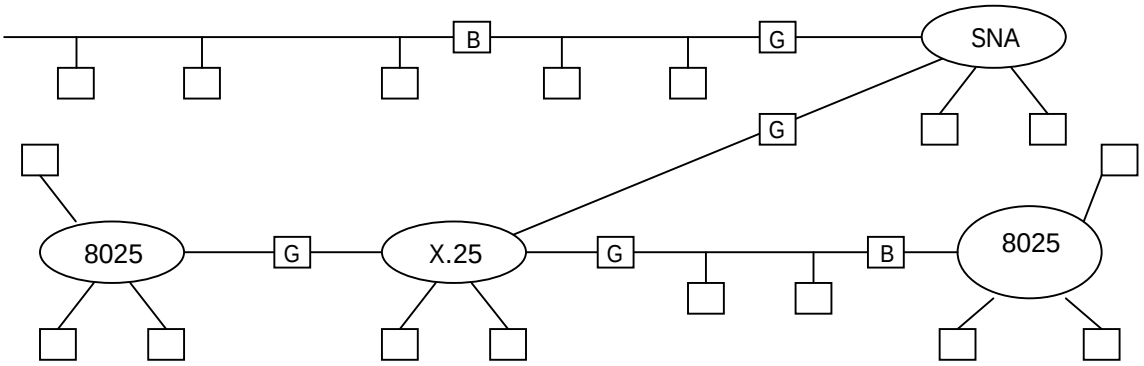
Chức năng của giao diện kết nối phụ thuộc vào sự khác biệt kiến trúc của mạng con : sự khác biệt càng lớn thì chức năng của giao diện càng phức tạp.

Có thể có các kết nối mạng như sau :

| | |
|---|---|
| LAN-LAN | : Nối các mạng cục bộ. |
| LAN-WAN | : Nối các mạng cục bộ với mạng đường dài. |
| WAN-WAN | : Nối các mạng đường dài |
| LAN-WAN- LAN | : Nối mạng đường dài với mạng cục bộ. |

Nếu máy nguồn và máy đích không ở cùng một mạng phải tìm đường từ mạng này sang mạng khác. Nếu trạm nguồn và đích không ở hai mạng liền kề thì giải quyết tìm đường qua nhiều trạm.

Các mạng khác nhau có các giao thức khác nhau, dẫn đến khác nhau về dạng khuôn của gói tin, đầu gói tin, điều khiển dòng dữ liệu và qui tắc xác nhận.



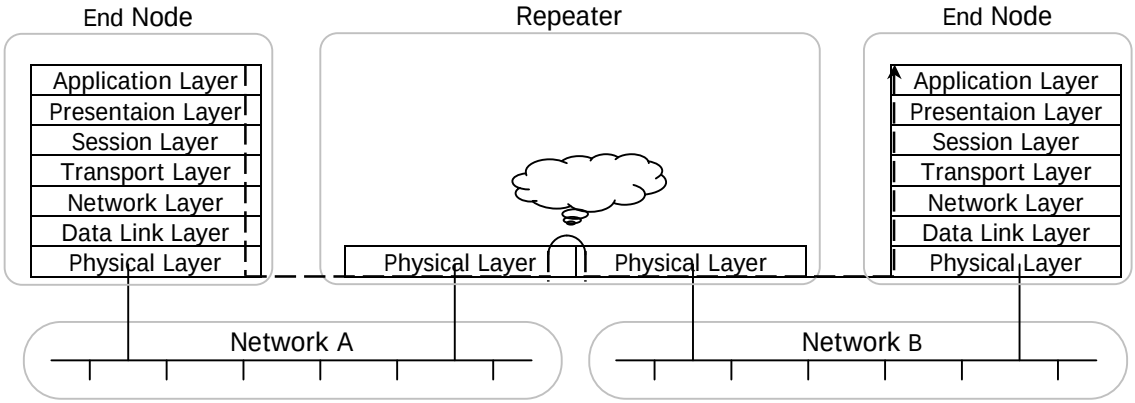

Hình 5-2. Kết nối liên mạng.

### 5.2.1 Các thiết bị dùng để kết nối liên mạng

Việc kết nối các LAN riêng lẻ thành một liên mạng chung gọi là Internetworking, sử dụng các thiết bị kết nối thông dụng như sau :

#### *5.2.1.1 Bộ lặp*

Bộ lặp (repeater) thực hiện chức năng ở tầng vật lý để khuyếch đại tín hiệu khi tín hiệu truyền đi xa. Bộ lặp được sử dụng để kết nối các đoạn mạng lại với nhau. Bộ lặp nhận tín hiệu từ một đoạn mạng, tái tạo và truyền tín hiệu này đến đoạn mạng khác. Nhờ có bộ lặp mà tín hiệu bị suy yếu do phải truyền qua một đoạn cáp dài có thể trở lại dạng ban đầu và truyền đi được xa hơn.




Hình 5-3. Sơ đồ kiến trúc của Repeater trong mô hình OSI.

Bộ lọc không có khả năng xử lý lưu lượng. Tất các tín hiệu điện, bao gồm cả nhiễu điện từ và các lỗi khác cũng được lặp và khuếch đại. Để bộ lặp hoạt động, cả hai đoạn mạng nối tới bộ lặp phải sử dụng cùng một phương thức truy nhập đường truyền. Ví dụ: bộ lặp không thể nối một đoạn mạng sử dụng phương thức CSMA/CD và một đoạn mạng sử dụng phương thức chuyển thẻ bài.

Bộ lặp có thể di chuyển gói dữ liệu từ phương tiện truyền dẫn này sang phương tiện truyền dẫn khác. Ví dụ có thể nhận gói dữ liệu từ một đoạn mạng dùng cáp đồng trục và chuyển gói đó sang đoạn mạng sử dụng cáp quang.

#### *5.2.1.2 Hub*

HUB là một thiết bị liên kết mạng được sử dụng rộng rãi. HUB còn là thành phần trung tâm trong cấu trúc mạng hình sao (Star). Mạng Star sử dụng sự phân chia tín hiệu trong HUB để đưa các tín hiệu ra các đường cáp khác nhau. Do vậy, có 3 loại HUB có thể sử dụng trong mạng là: HUB chủ động, HUB thụ động và HUB lai.

- ***HUB chủ động:*** Hầu hết các HUB đều là HUB chủ động, chúng tái tạo và truyền lại tín hiệu giống như bộ lặp. HUB thường có nhiều cổng nên thỉnh thoảng chúng còn được gọi là bộ lặp đa cổng. HUB chủ động đưa ra các tín hiệu mạnh hơn do đó cho phép đoạn cáp dài hơn.

Hình 5-4. Thiết bị kết nối mạng HUB.

- *HUB thụ động:* Các HUB thụ động hoạt động như các điểm kết nối, chúng không tái tạo hoặc khuếch đại tín hiệu.
- *HUB lai:* Các HUB thích ứng với nhiều loại cáp khác nhau được gọi là HUB lai.

#### *5.2.1.3 Cầu nối (Bridge)*

Cầu nối là một thiết bị hoạt động ở tầng liên kết dữ liệu. Dùng để nối hai hoặc nhiều đoạn (*segment*) của mạng LAN khác nhau.

Hình 5-5. Cầu nối.

- Chức năng của cầu nối :

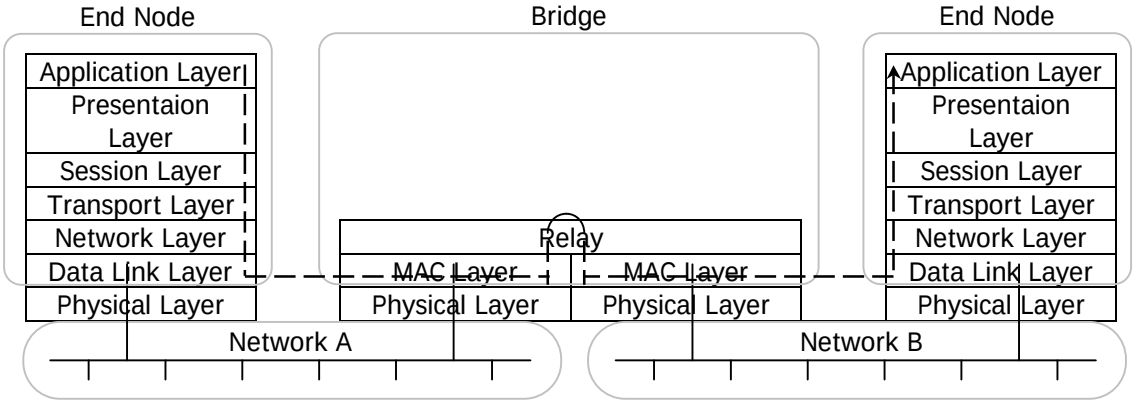
- Mở rộng khoảng cách của phân đoạn mạng, tăng số lượng máy tính trên mạng.
- Lọc những gói dữ liệu để gửi đi (hay không gửi) cho đoạn nối, hoặc gửi trả lại nơi xuất phát.
- Phân chia một mạng lớn thành hai mạng nhỏ nhằm cô lập lưu lượng, tăng tốc độ mạng. Nếu lưu lương từ một nhóm máy tính trở nên quá tải và làm giảm hiệu suất toàn mạng thì cầu nối có thể cô lập máy tính hoặc bộ phận này.
- Làm giảm hiện tượng tắc nghẽn do số lượng máy tính nối vào mạng qua lớn : Cầu nối có thể tiếp nhận một mạng quá tải và chia nó thành hai mạng riêng biệt, nhằm giảm bớt lưu lượng truyền trên mỗi đoạn mạng và do đó mỗi mạng sẽ hoạt động hiệu quả hơn.
- Kết nối các phương tiện truyền dẫn khác nhau, như cáp xoắn đôi và cáp quang.
- Kết nối các đoạn mạng sử dụng phương thức truy nhập đường truyền khác nhau, chẳng hạn CSMA/CD và chuyển thẻ bài.

- Nguyên lý hoạt dộng

- Cầu nối không phân biệt giữa giao thức này với giao thức khác, chỉ có nhiệm vụ chuyển lưu lượng của tất cả các giao thức dọc theo mạng. Vì giao thức nào cũng di chuyển ngang qua cầu nối, nên tuỳ thuộc vào từng máy tính quyết định chúng có thể nhận diện được giao thức nào.

- Cầu nối hoạt động trên nguyên tắc mỗi nút mạng có một địa chỉ riêng. Cầu nối chuyển gói dữ liệu dự trên địa chỉ của nút đích (địa chỉ MAC). Khi dữ liệu truyền qua cầu nối, thông tin địa chỉ của máy tính được lưu trong RAM của cầu nối dùng để xây dựng bảng địa chỉ dựa trên địa chỉ nguồn của gói tin.

Giao diện Bridge chỉ chứa tầng 1 và tầng con MAC, có chức năng chuyển đổi khuôn dạng của các đơn vị dữ liệu (frame) của các giao thức khác nhau và gửi chúng tới các mạng cục bộ đích có kèm theo phối hợp tốc độ.




Hình 5-6. Sơ đồ kiến trúc của Bridge trong mô hình OSI.

Ví dụ một Bridge nối giữa IEEE 820.3 và IEEE 820.5. Cầu nối này có hai card mạng: card Token Ring và card Ethermet để giao tiếp với hai mạng.

### *5.2.1.4 Bộ dẫn đường (router)*

Trong môi trường gồm nhiều đoạn mạng với giao thức và kiến trúc mạng khác nhau, cầu nối không thể đảm bảo truyền thông nhanh trong tất cả các đoạn mạng. Mạng có độ phức tạp như vậy cần một thiết bị không những biết địa chỉ của mỗi đoạn mạng, mà còn quyết định tuyến đường tốt nhất để truyền dữ liệu và lọc lưu lượng quảng bá trên các đoạn mạng cục bộ. Thiết bị như vậy được gọi là bộ định tuyến.

Hình 5-7. Bộ định tuyến.

- Chức năng của bộ định tuyến :

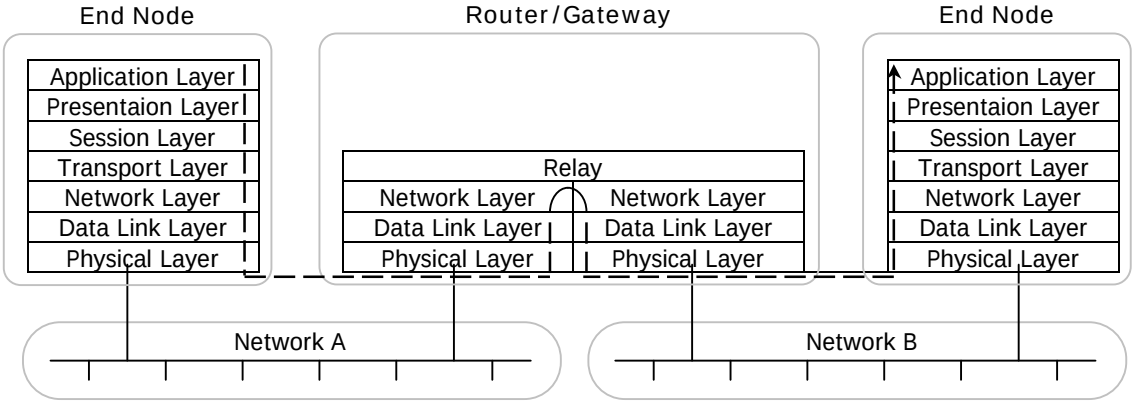
- Chuyển đổi và định tuyến gói dữ liệu qua nhiều mạng dựa trên địa chỉ phân lớp của mạng, cung cấp các dịch vụ như bảo mật, quản lý lưu thông...
- Phân chia một mạng lớn thành nhiều mạng nhỏ, và có thể kết nối nhiều đoạn mạng với nhau.
- Lọc gói tin và cô lập lưu lượng mạng : hoạt động như một rào cản an toàn giữa các đoạn mạng ( do có thể lọc dữ liệu).
- Ngăn chặn tình trạng quảng bá vì chúng không chuyển tiếp các gói tin quảng bá, cải thiện việc phân phát gói dữ liệu.
- Các bộ định tuyến có thể chia sẽ thông tin trạng thái và thông tin định tuyến với nhau và sử dụng thông tin này để bỏ qua các kết nối hỏng hoặc chậm.

- Nguyên lý hoạt động :

Trong bộ định tuyến có một bảng định tuyến chứa các địa chỉ mạng. Tuy nhiên, địa chỉ mạng có thể được lưu trữ tuỳ thuộc vào giao thức mạng đang chạy. Bộ định tuyến sử dụng bảng định tuyến để xác định địa chỉ đích cho dữ liệu nhận được. Bảng này liệt kê các thông tin sau:

- Địa chỉ mạng đã kết nối.
- Cách kết nối tới các mạng khác.
- Phí tổn truyền dữ liệu qua các lộ trình đó.

Khi bộ định tuyến nhận được một gói dữ liệu cần gởi đến mạng ở xa, nó kiểm tra bảng đinh tuyến và chọn đường đi tối ưu (theo một tiêu chuẩn nào đó) để gởi gói dữ liệu đến đích.




Hình 5-8. Sơ đồ kiến trúc của Router trong mô hình OSI.

- Truyền dữ liệu qua bộ định tuyến

Trong mọi trường hợp, khi một trạm xác định rằng nó phải gởi một gói dữ liệu tới một trạm trên một mạng khác. Công việc đầu tiên trạm này cần làm là lấy địa chỉ vật lý MAC của Router (địa chỉ cổng nối ngầm định). Sau đó nó điền thông tin trong trường địa chỉ vật lý đích của gói dữ liệu bằng địa chỉ vật lý MAC của Router, và trường thông tin địa chỉ đích ở tầng mạng (chẳng hạn địa chỉ IP nếu dùng giao thức TCP/IP) bằng địa chỉ của trạm đích.

Khi Router kiểm tra địa chỉ đích, nó xác định xem nó biết hay không biết cách chuyển tiếp gói dữ liệu đến bước nhảy tiếp theo (Router kế tiếp trên đường đi) bằng cách kiểm tra địa chỉ. Nếu địa chỉ mạng đích nằm trong gói dữ liệu không có bảng định tuyến, Router thường bỏ gói dữ liệu đi. Trong trường hợp địa chỉ mạng đích có bảng định tuyến, Router thay địa chỉ vật lý đích bằng địa chỉ vật lý của bước nhảy tiếp theo và truyền gói dữ liệu đến bước nhảy tiếp theo.

Như vậy, khi một gói tin được chuyển qua liên mạng, địa chỉ vật lý đích của nó thay đổi, nhưng địa chỉ của giao thức không đổi.

Bộ định tuyến được chia thành 2 loại, tuỳ theo cách sử dụng chúng. Bộ định tuyến cục bộ (Local Router) nối các đoạn mạng ở gần nhau. Hai bộ định tuyến ở xa nhau (Remote Router) nối hai đoạn mạng ở xa qua các kênh truyền thông.

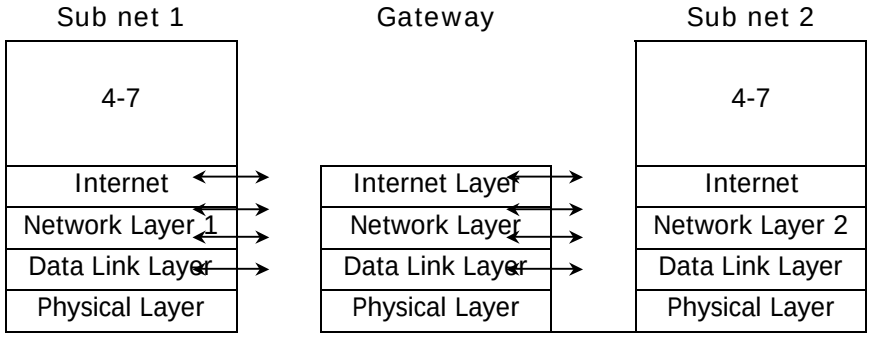
#### *5.2.1.5 Bộ chuyển mạch*

Chức năng chính của bô chuyển mạch (switch) là cùng một lúc duy trì nhiều cầu nối giữa các thiết bị mạng bằng cách dựa vào một loại đường truyền xương sống (backbone) nội tại tốc độ cao. Switch có nhiều cổng, mỗi cổng có thể hỗ trợ toàn bộ Ọthernet LAN hoặc Token Ring. Bộ chuyển mạch kết nối một số LAN riêng biệt và cung cấp khả năng lọc gói dữ liệu giữa chúng.

Các bộ chuyển mạch là loại thiết bị mạng mới, hiện đang được sử dụng rộng rãi vì Switch cho phép chuyển sang chế độ truyền không đồng bộ ATM.

#### *5.2.1.6 Gateway*

Hoạt động ở mức mạng, thực hiện ghép nối với WAN. Nguyên lý chung của nối kết này là tạo ra 1 tầng "*liên mạng*" (internet) chung trong tất cả các kiến trúc của mạng con tham gia nối kết. Tầng liên mạng thường là tầng con nằm ngay trên tầng 3 mô hình OSI.




Hình 5-9. Sơ đồ kiến trúc của gateway trong mô hình OSI.

Tầng con Internet được cài đặt trong tất cả các trạm cũng như trong các giao diện kết nối (gateway), Tầng này cung cấp dịch vụ truyền thông liên mạng với hai chức năng chính :

- Chuyển đổi các đơn vị dữ liệu của giao thức (Protocol Data Unit - PDU)
- Chọn đường đi cho các PDU này.

Các gói tin ở tầng con Internet lưu thông trong mạng theo phương pháp '*gói/bóc*' (encapsulation/decasulation). Khi một datagram được truyền từ mạng con này sang mạng con khác thông qua gateway thì nó được bổ sung thêm vào (hoặc tách ra) các phần thông tin điều khiển cần thiết tương ứng với các mạng con.

## 5.3 Giao thức liên mạng IP

Giao thức IP (Internet Protocol) hoạt động ở tầng mạng, cung cấp dịch vụ dữ liệu không liên kết (connectionless) cho nhiều giao thức liên kết dữ liệu khác. Đơn vị dữ liệu dùng trong giao thức IP được gọi là *datagram*, hay còn gọi là khung tin IP.

- Chức năng của giao thức IP :

- Định nghĩa gói tin Datagram là đơn vị dữ liệu cơ bản của việc truyền tin trên mạng Internet.
- Xác định mô hình đánh địa chỉ cho các khung tin và quản lý các quá trình trao đổi, xử lý các khung tin này.
- Chọn đường cho các datagram trên mạng
- Cung cấp cơ chế trên gói tin trên mạng hiệu quả nhất.
- Phân đoạn và tổng hợp các gói tin.

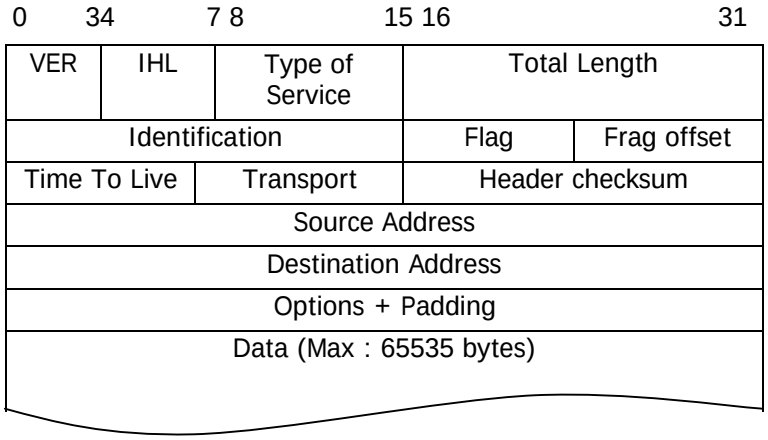
- Tính chất của giao thức IP :

- Hoạt động theo phương thức không kết nối : IP không chuyển các thông tin điều khiển trước khi truyền dữ liệu.

- Không tin cậy : giao thức IP không có khả năng phát hiện và khắc phục lỗi., không quan tâm đến vấn đề dữ liệu có được nhận một cách chính xác hay không. Do đó, các gói dữ liệu có thể bị thất lạc, bị trùng lặp, bị chuyển chậm hoặc đi không đúng thứ tự, mỗi gói dữ liệu được xử lý độc lập với nhau và có thể gửi theo những đường định tuyến khác nhau.

### 5.3.1 Cấu trúc khung tin IP

IP Header được gắn cho mỗi datagram, chứa các thông tin cần thiết cho sự hoạt động của gói tin trên mạng. Cấu trúc khung tin IP như hình sau :




Hình 5-10. Cấu trúc khung tin IP.

*VER (4 bit)*

Chứa phiên bản giao thức IP đang dùng. Phiên bản hiện nay là IPV4.

Một phần của giao thức IP quy định rằng phần mềm nhận dữ liệu trước tiên phải kiểm tra phiên bản của IP trong các khung tin đến, trước khi phân tích tiếp phần còn lại của Header và dữ liệu. Nếu như không đúng phiên bản thì lớp IP của máy nhận sẽ từ chối và bỏ qua toàn bộ nội dung của khung tin đến.

*IHL (Internet Header length) (4 bit)*

Chứa chiều dài của Header IP do máy gửi dữ liệu tạo nên, chiều dài này được tính theo các word có chiều dài 32 bit. Header ngắn nhất có chiều dài là 5 word (20 byte), nhưng do việc dùng các trường lựa chọn có thể làm tăng chiều dài của Header lên đến 6 word (24 byte). IHL dùng để giao thức IP được vị trí kết thúc của Header và bắt đầu phần dữ liệu của khung tin.

*Type of Service - Loại dịch vụ (8 bits)*

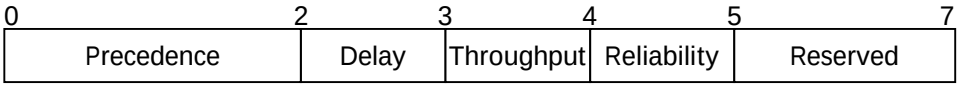
Trường này chứa các thông tin về quyền ưu tiên của việc truyền datagram và các ảnh hưởng có thể xảy ra trong quá trình truyền các datagram

đó. IP chuẩn không yêu chỉ ra các hành động cụ thể dựa trên giá trị của trường *Type of Service*. IP chỉ định sử dụng nó trong việc thiết lập các tuỳ chọn cho các mạng con và nó sẽ truyền qua trong bước nhảy tới.

Ví dụ, việc truy nhập vào mạng Token Ring cần thiết có các mức độ ưu tiên được xác định. IP có thể chuyển các mức độ ưu tiên của nó sang các mức độ ưu tiên tương ứng của mạng Token Ring.

Một số máy tính và bộ chọn đường (*router*) không quan tâm đến giá trị của trường này trong khi một số khác lại dựa vào đây để quyết định đường truyền.

Cấu trúc của trường như sau :




Cấu trúc của trường Type of Service

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

111 - Network Control (cao nhất) 011 - Flash
110 - Internetwork Control 10 - Immediate
101 - CRITIC/ECP 001 - Priority
100 - Flag Overrride 000 - Routime (thấp nhất)

D (Delay) - 1 bit : chỉ độ trễ yêu cầu
D = 0 độ trễ bình thường
D = 1 độ trễ thấp

T (Throughput) - 1 bit : chỉ thông lượng yêu cầu
T = 0 thông lượng bình thường
T = 1 thông lượng cao

R (Reliability) - 1 bít chỉ độ tin cậy yêu cầu
R = 0 độ tin cậy bình thường
R = 1 độ tin cậy cao

Ba bit đầu tiên của trường này là để chỉ ra quyền của khung tin đó, với các giá trị từ 0 (bình thường) đến 7 (Mạng điều khiển). Nếu giá trị của phần này càng cao thì khung tin đó càng quan trọng và trên lý thuyết thì khung tin này phải được chuyển đến đích nhanh hơn. Nhưng trên thực tế thì TCP/IP và các phần cứng dùng giao thức TCP/IP đều bỏ qua trường này và coi tất cả các khung tin có độ ưu tiên như nhau.

Ba bit tiếp theo là ba cờ 1-bit để điều khiển thời gian trễ, độ tin cậy, và thông lượng (throughput) của khung tin. Nếu tất cả các bit đều là 0 thì có nghĩa là đặt ở chế độ bình thường. Nếu bit thứ nhất là 1 thì có nghĩa là thời gian trễ thấp, truyền nhanh và độ tin cậy cao cho từng cờ. Còn hai bit còn lại của trường này không dùng. Phần lớn các bit của trường này đều bị bỏ qua khi thực hiện IP, và tất cả các khung tin đều được đặt thời gian trễ, thời gian truyền, và độ tin cậy như nhau.

Trong thực tế, hầu hết tất cả các bit của trường loại dịch vụ đều được đặt về giá trị 0 bởi vì sự khác nhau về quyền, thời gian trễ, thời gian truyền, độ tin cậy giữa các máy hầu như không tồn tại trừ khi một mạng mới được thành lập.

*Total Length (16 bits) - Chiều dài gói tin*

Trường này cho biết toàn bộ chiều dài của khung tin (datagram) bao gồm phần Header và phần dữ liệu, đơn vị tính bằng byte. Độ lớn của trường này là 16 bit do đó mà chiều dài của khung tin tối đa là 65535 byte.

*Indentification (16 bits) -Trường định danh*

Trường này chứa một giá trị đặc trưng do máy gửi khung tin tạo ra, cùng với các tham số khác (như Source Address và Destination Address), tham số này dùng để định danh duy nhất một khung tin trong khoảng thời gian nó tồn tại trên liên mạng.

Số trong trường này được cần đến khi sắp xếp các khung tin để đảm bảo rằng các khung tin không bị lẫn lộn với nhau. Khi lớp IP nhận được một đoạn dữ liệu từ các lớp cao hơn thì nó sẽ gán các số định danh này vào. Nếu như khung tin đã được tách (bằng kỹ thật tách thông tin) thì tất cả các khung tin sẽ mang cùng một số định danh như nhau.

*Flags (3 bits) - Các cờ*

Trường này có chiều dài 3 bit, liên quan đến sự phân đoạn các datagram.

Bit 0 : Dùng để dự trữ - chưa sử dụng, luôn có giá trị 0

Bit 1 : (DF) = 0 (May Fragment)

=1 (Don’t Fragment)

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

=1 (More Fragment)

Nếu như cờ DF có giá trị là 1 thì có nghĩa là khung tin không thể tách ra được trong bất cứ trường hợp nào. Nếu như mà phần mềm của lớp IP hiện tại không thể gửi khung tin đến nới nhận nếu như không tách ra, mà hiện tại bit cờ đang là 1 thì khi đó khung tin sẽ bị huỷ bỏ và một thông báo lỗi được gửi đến thiết bị phát.

Nếu router không thể truyền nguyên cả một datagram mà bit này được thiết lập bằng 1 thì datagram đó sẽ bị loại bỏ và nó sẽ có một thông báo lỗi gửi đến máy phát. Bất kì một người quản lý mạng nào cũng có thể sử dụng cách này để kiểm tra độ lớn của các datagram có thể được truyền trên các phần khác nhau trên mạng kết hợp.

Nếu như cờ MF là 1 có nghĩa là khung tin hiện tại vẫn đang còn các gói tin khác nữa đang đến, do đó mà phải cần đến việc sắp xếp lại để khôi phục lại message ban đầu. Khung tin cuối cùng đến sẽ lớn hơn các khung tin bình thường vì nó còn chứa thêm phần MF=0 để báo cho máy nhận biết là đã hết các khung tin cần thiết không cần phải đợi thêm nữa. Có thể là các khung tin đến không đúng với thứ tự chúng đã được phát đi, do đó cờ MF còn được dùng cùng với trường Fragment Off để chỉ cho máy nhận được thứ tự của toàn bộ message ban đầu.

*Fragment Offset (13 bits)*

Nếu mà cờ MF bằng 1 (tức là có sự tách thông tin từ một khung tin lớn), khi đó fragment offset chứa .vị trí của các message con trong message ban đầu trong khung tin hiện thời. Điều này cho phép IP sắp xếp lại các khung tin thành message ban đầu t theo đúng trật tự.

Offset thường được để ở đầu message. Trường này có chiều dài là 13 bit, do vậy offset được tính theo đơn vị 8 byte, tương ứng với gói lớn nhất là 65535 byte. Việc dùng số định danh để chỉ rằng khung tin đến là thuộc bản tin nào, lớp IP ở máy nhận có thể dùng fragment offset để sắp xếp lại message ban đầu.

*TTL (Time to Live - Thời gian sống)*

Trường này cho biết khoảng thời gian tính bằng giây mà một khung tin có thể tồn tại trên mạng trước khi nó bị huỷ bỏ. Giá trị này được nút gửi khung tin đi ấn định.

Các chuẩn của TCP/IP quy định rằng trường TTL phải được giảm đi ít nhất là 1 giây cho mỗi nút xử lý khung tin đó, thậm chí là thời gian xử lý có thể nhỏ hơn 1 giây. Khi một gateway nhận được một khung tin thì thời gian đến được đính vào khung tin do đó nếu như khung tin đó phải chờ để được xử lý. Bởi vậy nếu một gateway nào đó mà bị quá tải và không thể lấy khung tin về, khi đó bộ đếm thời gian của trường TTL sẽ tự động giảm đi trong quá trình chờ để được xử lý. Nếu trường TTL giảm về 0 thì khi đó khung tin đó phải được nút hiện thời hủy bỏ, sẽ có một thông báo gửi về máy gửi.

Hầu hết các TCP/IP cài đặt giá trị trường TTL khoảng 60 hoặc cao hơn, nghĩa là datagram có thể đi qau 60 router hay hop để đến đích. Trường TTL được thiết kế để tránh việc các gói dữ liệu cứ chuyển vòng quanh trên mạng mà không có đường ra.

*Giao thức giao vận (Transport Protocol)*

Trường này chứa số định danh của giao thức giao vận mà đã xử lý khung tin. Số định danh này do trung tâm thông tin mạng Internet NIC ấn định. Hiện nay đã có khoảng 50 giao thức giao vận được ấn định. Hai giao thức quan trọng nhất là : ICMP (Internet Control message Protocol) và TCP.

*Header checksum*

Dùng để tính checksum của trường Header để làm cho quá trình xử lý thông tin được nhanh hơn. Do trường TTL bị giảm đi 1 giây mỗi khi được xử lý, trường checksum cũng thay đổi tại các máy mà khung tin đi qua. Thuật toán checksum là một thuật toán nhanh và có hiệu quả, nhưng có một số trường hợp bị sai chẳng hạn mất hoàn toàn một từ 16 bit mà 16 bit này đều bằng 0. Tuy nhiên trường checksum do cả TCP và UDP để đóng gói, các lỗi này sẽ được phát hiện khi khung tin được tập hợp để truyền trên mạng.

*Source Address (32 bits) :* chứa địa chỉ IP 32 bit của máy gửi.

*Destination Address (32 bits) :* chứa địa chỉ IP 32 bit của máy nhận.

Hai trường trên được tạo ra cùng với khung tin và không bị thay đổi trong quá trình truyền.

*Options (32 bits) - Phần lựa chọn*

Phần lựa chọn được tạo ra từ một vài mã mà các mã này có độ dài có thể thay đổi được. Nếu như có nhiều lựa chọn trong khung tin, thì các lựa chọn đó được đặt liên tục nhau trong phần Header của IP. Tất cả các lựa chọn này được điều khiển bằng một byte có ba trường: ***Cờ copy*** có độ dài 1 bit, ***loại lựa chọn*** có độ dài 2 bit, và ***trường số lựa chọn*** có độ dài 5 bit. Trường cờ copy được dùng để quy định là lựa chọn sẽ được thực hiện như thế nào nếu ở một gateway nào đó cần đến kỹ thuật tách thông tin. Nếu như cờ này có giá trị là 0 thì có nghĩa là lựa chọn đó sẽ được copy vào khung tin thứ nhất mà không copy vào các khung tin tiếp theo sau. Nếu như cờ này có giá trị là 1 thì có nghĩa là lựa chọn đó sẽ được sao chép vào tất cả các khung tin.

Các lựa chọn quan trọng là Record route và Timestamp.

*Record route*

Trường Record Route (*Bản ghi chọn đường)* chứa danh sách dự trữ của các route mà datagram đã đi qua trên đường tìm tới đích. Mỗi lần đi qua một router thì trường này sẽ bổ sung một địa chỉ của router đó vào danh sách của nó. Độ dài của trường này do máy nguồn xác lập, do đó rất có thể là nó sẽ bị

đầy trước khi datagram tìm được đến đích. Trong trường hợp này thì các địa chỉ của các router sau sẽ không được thêm vào danh sách của nó.

*Timestamp :* Có 3 định danh cho trường Timestamp. Trường này có thể chứa:

- Danh sách của 32 bit Timestamp.
- Danh sách của địa chỉ IP và các cặp Timestamp tương ứng.

Danh sách của các địa chỉ cho trước bởi máy nguồn. Một nút bất kỳ được ghi vào trường này chỉ khi địa chỉ của nó là mục kế tiếp trong danh sách này. Trường này có thể bị đầy nếu rơi vào hai trường hợp đầu, trong trường hợp này sẽ có trường ghi tràn (overllow field) dùng để đếm số nút mà không thể ghi vào timestamp được.

*Padding (Độ dài thay đổi)*

Nội dung của phần **Padding** phụ thuộc vào phần **Options** như thế nào. Phần Padding thường được dùng để bảo đảm rằng chiều dài Header của khung tin luôn là một số nguyên bội số của 32.

*Data* : Vùng dữ liệu có độ dài thay đổi, nhưng luôn là bội số của 8 bits, và tối đa là 65535 bytes.

### 5.3.2 Địa chỉ IP

Mỗi thiết bị nối vào mạng TCP/IP được gán một địa chỉ IP duy nhất (mỗi card mạng sẽ có địa chỉ IP riêng). Khi sử dụng mạng cục bộ không kết nối với các mạng khác, người sử dụng có thể gán địa chỉ IP tuỳ ý cho các máy trạm. Tuy nhiên, đối với các site Internet thì địa chỉ IP phải được cung cấp từ trung tâm quản lý thông tin mạng trên thế giới (NIC - Network Information Center).

Địa chỉ của IP có độ dài 32 bit, được chia làm 4 phần, mỗi phần 1 byte, phân cách nhau bằng dấu chấm. Dạng tổng quát : ***x.y.z.t*** với $0 \leq x,y,z,t \leq 255$

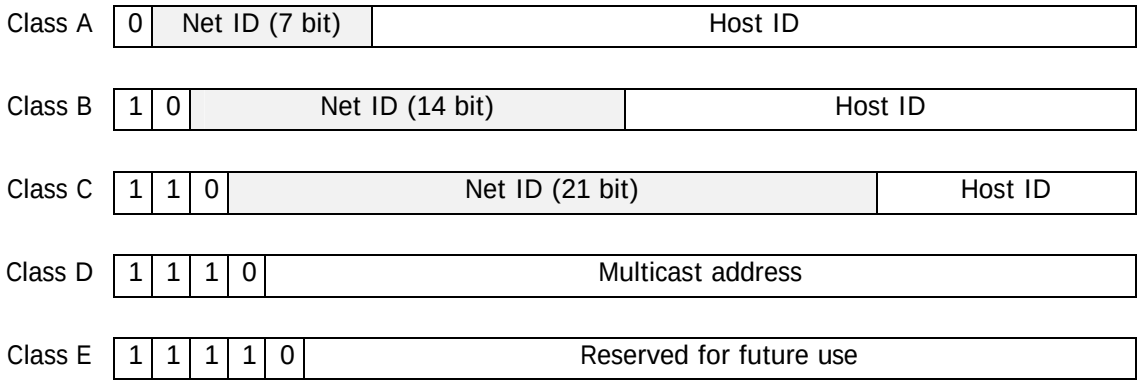
*Ví dụ:* 128.83.12.14 hoặc 0x80530C0E Hex.

Địa chỉ IP bao gồm hai phần thông tin: địa chỉ mạng (network address) và địa chỉ máy (host address): NetworkID.HostID

Khi đề nghị NIC cung cấp địa chỉ IP ta sẽ không nhận được địa chỉ tương ứng của máy trạm, thay vào đó là địa chỉ mạng và ta có quyền gán địa chỉ cho các máy trạm của mạng trong phạm vi địa chỉ được cung cấp.

#### *5.3.2.1 Các lớp địa chỉ IP*

Địa chỉ IP thuộc một trong E lớp địa chỉ, từ lớp A đến E. Các lớp địa chỉ nhằm để phân loại các mạng có quy mô khác nhau.




Hnh 5-11. Các lớp địa chỉ IP.

1. Lớp A (1≤ x ≤ 126) : NetworkID= x, HostID=y.z.t

- Cho phép định danh 126 mạng, với tối đa $2^{24}$ (= 167.772) máy trạm trên mỗi mạng, lớp A giới hạn số subnetwork trong Internet.
- Các mạng lớp A thuộc loại mạng diện rộng (very large), như mạng quốc gia

2. Lớp B (128≤ x ≤ 191) : NetworkID= x.y, HostID=z.t

- Cho phép định danh đến 16384 mạng, với tối đa $2^{16}$ (=65.536) host trên mỗi mạng.
- Mạng lớp B thuộc loại mạng trung bình như mạng University Campuses.

3. Lớp C (192 ≤ x ≤ 223) : NetworkID= x.y.z, HostID=t

- Giới hạn số trạm trong mạng lớn nhất là 256, có 21 bit cho địa chỉ mạng. Cho phép định danh đến 2 triệu mạng, với tối đa 254 host trên mỗi mạng.
- Mạng lớp C được sử dụng cho các loại LAN, như các mạng Enterprise-wide.

4. Lớp D (224≤ x ≤ 239)

- Địa chỉ lớp D dùng cho các giao thức đặc biệt (Internet Group management Protocol - IGMP) và các giao thức khác.

5. Lớp E (240≤ x ≤ 255) : Để dành cho sự phát triển về sau.

- Các máy trong cùng một mạng phải có địa chỉ mạng giống nhau.
- Các mạng khác nhau có địa chỉ mạng khác nhau.

#### *5.3.2.2 Các địa chỉ IP đặc biệt*

1. Địa chỉ quay vòng : 127.y.z.t

Tất cả các gói tin được gửi đến địa chỉ 127.0.0.0 sẽ được gửi ngược trở lại máy tính. Gói tin này được sao chép từ nơi truyền đến bộ đệm nơi nhận trên cùng một máy tính. Địa chỉ loopback có thể được sử dụng như một địa chỉ kiểm tra

nhanh xem phần mềm TCP/IP có được cấu hình thích hợp. Trên hệ điều hành Windows địa chỉ loopback là 127.0.0.1 còn Unix là 127.1.*.

2. Mặt nạ mạng (Netmask)

***Mặt nạ mạng*** của một địa chỉ IP là một giá trị 32 bits trong đó các bit tương ứng với phần địa chỉ mạng bằng 1, các bit của phần máy bằng 0.

Ví dụ : Địa chỉ IP lớp B có mặt nạ mạng là 255.255.255.0 sẽ cho địa chỉ mạng con là 180.10.15.0

3. Địa chỉ quảng bá (broadcast address)

Địa chỉ này có các bit của phần HostID bằng 1, được sử dụng khi muốn chuyển một gói tin đến mọi máy tính trong mạng con.

Ví dụ một mạng con có địa chỉ là 180.10.0.0 sẽ có địa chỉ quảng bá là 180.10.255.255. Tương tự, một mạng con có địa chỉ là 180.10.15.0 sẽ có địa chỉ quảng bá là 180.10.15.255.

Đặc biệt địa chỉ 255.255.255.255 quảng bá cục bộ (local broadcast) hay còn gọi là limited broadcast có thể sử dụng trong các LAN.

Địa chỉ 0.0.0.0 cũng được sử dụng trong bảng định tuyến để chỉ đến điểm vào mạng cho địa chỉ bộ định tuyến mặc định.

## 5.4 Phân chia mạng con

Để thuận tiện cho việc quản lý và định hướng dữ liệu trên mạng lớn, người ta thường tổ chức mạng IP theo cơ chế địa chỉ phân cấp : mỗi mạng được chia nhỏ thành nhiều mạng con, mỗi mạng con thực hiện các dvc về địa chỉ trong nội bộ mạng đó. Sự phân cấp này cho phép giảm khối lượng công việc chọn đường cho các gói tin trong toàn liên mạng.

Mỗi mạng con chịu trách nhiệm cho việc chọn đường cho các gói tin IP trong mạng của mình, các gói tin này được nhận ra nhờ phần địa chỉ mạng của nó. Trong các mạng loại A, B, C thì phần địa chỉ này có độ dài cố định. Tuy nhiên, để tạo sự linh hoạt trong việc phân chia mạng con thì địa chỉ mạng có thể mở rộng sang các bit của địa chỉ máy. Đó là kỹ thuật phân chia mạng con.

Ví dụ một mạng loại B có địa chỉ mạng là 203.160.9.0 và mặt nạ mạng là 255.255.255.0 (địa chỉ mạng dài 24 bit). Người ta cần chia mạng này thành 4 mạng cục bộ riêng, do đó sẽ lấy thêm 2 bit cho địa chỉ mạng (26 bit). Vậy ta có địa chỉ các mạng con này là :

Địa chỉ mạng 1 :

| 203 | 160 | 9 | 0 |
|---|---|---|---|
| 11001011 | 10100000 | 00001001 | 00000000 |

Địa chỉ mạng 2 :

| 203 | 160 | 9 | 64 |
|---|---|---|---|
| 11001011 | 10100000 | 00001001 | 01000000 |

Địa chỉ mạng 3 :

| 203 | 160 | 9 | 128 |
|---|---|---|---|
| 11001011 | 10100000 | 00001001 | 10000000 |

Địa chỉ mạng 4 :

| 203 | 160 | 9 | 192 |
|---|---|---|---|
| 11001011 | 10100000 | 00001001 | 11000000 |

Mặt nạ của các mạng con này là : 255.255.255.192

| 255 | 255 | 255 | 192 |
|---|---|---|---|
| 11111111 | 11111111 | 11111111 | 11000000 |

Việc phân chia mạng được tiến hành bởi người quản trị hệ thống và thường dựa trên ranh giới vật lý giữa các nhánh mạng. Khi có gói dữ liệu cần chuyển đi, bộ định tuyến sẽ dùng mặt nạ mạng để kiểm tra gói dữ liệu này thuộc mạng con nội bộ hay thuộc mạng ngoài. Sự phân chia mạng riêng thành các mạng con chỉ có ý nghĩa bên trong mạng đó.

Nếu kết nối Internet thông qua một mạng LAN, điều quan trọng là phải sử dụng đúng mặt nạ mạng. Cũng giống như địa chỉ IP, một mặt nạ mạng con có thể được gán một cách riêng lẻ hay có thể tự động thông qua DHCP (Dynamic Host Configuration Protocol).

## 5.5 Hoạt động của giao thức IP

Nếu địa chỉ đích của gói tin IP không nằm trên cùng mạng với máy chủ nguồn thì giao thức IP trong máy chủ hướng gói tin đến bộ định tuyến nội bộ. Nếu bộ định tuyến này không được nối đến mạng đích, gói tin sẽ được gởi đến một bộ định tuyến khác. Cứ thế cho đến khi tới trạm đích. Việc quy định truyền theo đường truyền nào của router dựa trên bảng đường truyền (*routing table*). Các bộ định tuyến có thể phát hiện :

- Một mạng mới đã được thêm vào liên mạng
- Đường dẫn đến trạm đích đã bị hỏng

Các bước thực hiện bởi một thực thể IP như sau :

- *Đối với thực thể IP ở trạm nguồn*

- Khi nhận được lệnh SEND từ tầng trên, nó thực hiện các bước như sau:
- Tạo một IP datagram dựa trên các tham số của lệnh SEND
- Tính checksum và ghép vàp phần đầu của datagram
- Ra quyết định chọn đường
- Chuyển datagram xuống tầng dưới

• *Đối với gateway*

- Khi nhận được datagram quá cảnh, nó thực hiện các tác động như sau :
- Tính checksum, nếu không đúng thì loại bỏ datagram
- Giảm giá trị tham số thời gian tồn tại. Nếu hết thời gian thì loại bỏ datagram
- Ra quyết định chọn đường
- Phân loại datagram nếu cần
- Kiến tạo lại phần đầu IP bao gồm giá trị mới của vùng TTL, checksum, Fragmentation.
- Chuyển datagram xuống tầng dưới để truyền qua mạng.

• *Tại trạm đích*

- Tính checksum, nếu không đúng thì loại bỏ datagram.
- Tập hợp các đoạn của datagram.
- Chuyển dữ liệu và các tham số điều khiển lên tầng trên.

Như vậy, do gói tin IP không sửa đổi, đơn giản nên hiệu suất đường truyền cao. Vì gói tin IP cung cấp dịch vụ giao nhận gói tin không tin cậy nên cần có giao thức ICMP để hỗ trợ, các bản tin ICMP được đóng gói và chuyển tải trong các gói tin IP. Tầng TCP đảm nhận việc bảo đảm các datagram được truyền đến đích một cách an toàn và đầy đủ.

## 5.6 Các giao thức liên quan đến IP

### 5.6.1 Giao thức phân giải địa chỉ ARP

Địa chỉ IP được dùng để *định danh các host và mạng ở tầng mạng* của mô hình OSI, và chúng không phải là các địa chỉ vật lý (hay địa chỉ MAC) của các trạm đó trên cùng một mạng cục bộ (Ethernet, Token Ring, ...). Trên một LAN như vậy, hai trạm chỉ có thể liên lạc với nhau nếu chúng biết địa chỉ vật lý của nhau.

Vấn đề đặt ra là phải thực hiện ánh xạ địa chỉ IP (32 bits) và địa chỉ vật lý (48 bits) của một trạm. Giao thức ARP (Address Resolution Protocol) đã được xây dựng để chuyển đổi từ địa chỉ IP sang địa chỉ vật lý khi cần thiết. Ngược lại, giao

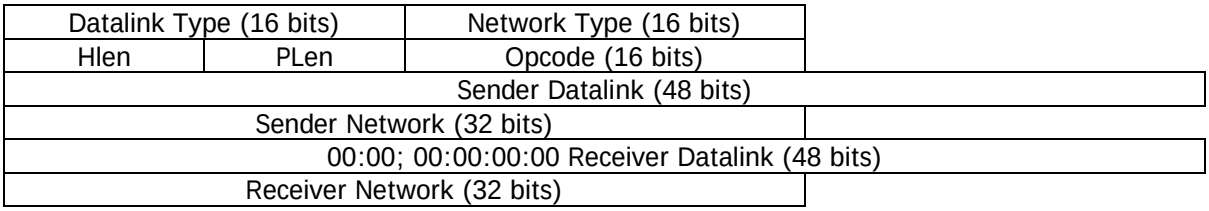
thức RARP (Reserse Address Resolution Protocol) được dùng để chuyển đổi từ địa chỉ vật lý sang địa chỉ IP.

Cả hai giao thức ARP và RARP đều không phải là bộ phận của IP, IP sẽ dùng đến chúng khi cần.

Mỗi ghép nối mạng có *địa chỉ giao thức mạng* (IP address) và *địa chỉ giao thức liên kết dữ liệu* (Datalink Protocol Address) riêng. Do đó cần có bảng ánh xạ giữa hai địa chỉ này ( địa chỉ ảo và địa chỉ vật lý ). Bảng địa chỉ này có thể làm bằng tay, nhưng do khối lượng địa chỉ lớn, tăng khá nhanh, nên người ta giải quyết thông qua thủ tục "*Tìm giải pháp cho địa chỉ*" (Address Resolution Protocol -ARP).

Các gói tin ARP được đóng gói trong khung dữ liệu liên kết (data link frame). Đối với mạng Ethernet, kiểu trường (type field) sẽ là 0x0806.

ARP ánh xạ địa chỉ IP sang địa chỉ liên kết dữ liệu (datalink address). Trạm tin sẽ gửi gói tin yêu cầu ARP (request packet) với khuôn dạng gói tin như hình sau.



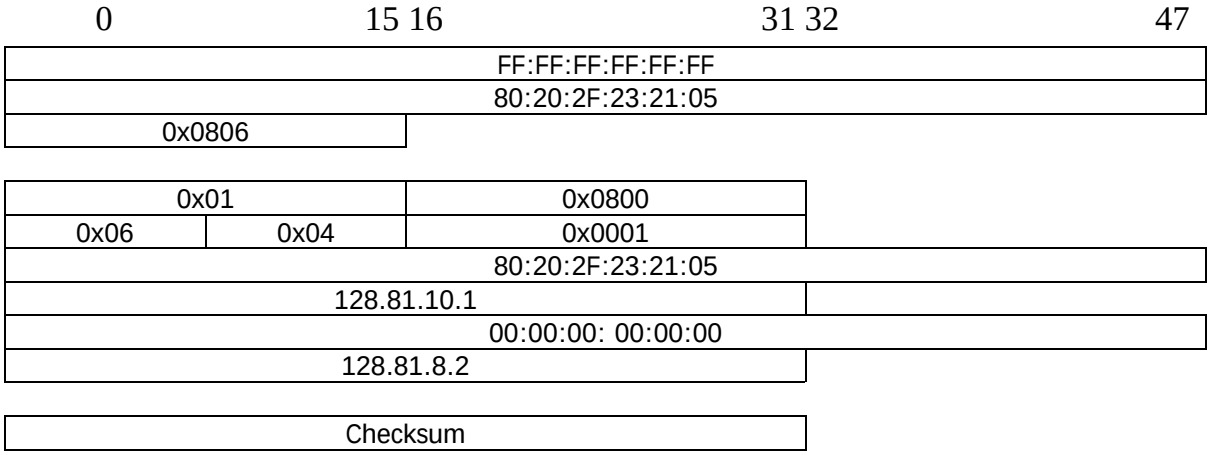

Hình 5-12. Khuôn dạng gói tin ARP.

- Data link type: Loại dữ liệu liên kết, với mạng Ethernet thì trường này có giá trị là 0x0001
- Network type : Loại địa chỉ mạng, Ethernet type used for IP (0x0800)
- Hlen : Độ rộng của phần địa chỉ dữ liệu liên kết, với mạng Ethernet độ rộng là 6 bytes
- Plen : Độ rộng của địa chỉ mạng, trong giao thức IP, phần này là 4 byte
- Opcode : Có giá trị là 0x0001 cho thủ tục yêu cầu ARP, 0x0002 cho ARP trả lời.
- Sender datalink and sender network : Địa chỉ vật lý và địa chỉ ảo (địa chỉ mạng) của người gửi
- Receive datalink and receive network : Địa chỉ vật lý và địa chỉ ảo (địa chỉ mạng) của người nhận

*Ví dụ:* Trạm A muốn gửi trạm B một gói tin IP. Cả hai máy A, B đều có cùng có địa chỉ mạng IP và cùng kết nối vào mạng Ethernet như hình sau :

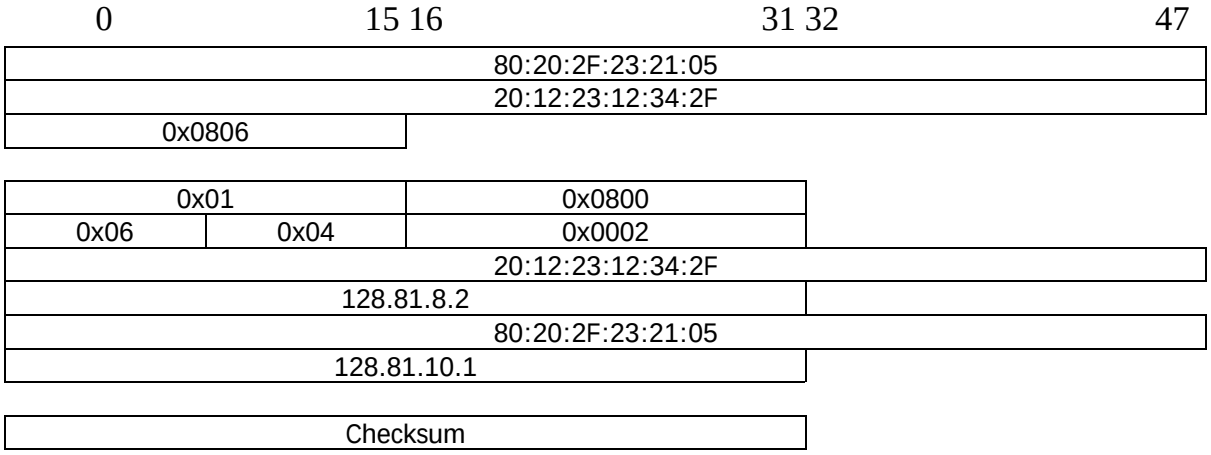
Trạm A biết được địa chỉ mạng của trạm B nhưng không biết địa chỉ vật lý của trạm B. Trạm A cần hỏi địa chỉ vật lý của trạm B để gửi tin. Khi đó trạm A phát đi một gói tin ARP yêu cầu (ARP request packet) đóng gói trong khung tin Ethernet.

- Quá trình gởi yêu cầu ARP




Hình 5-13. Khuôn dạng gói tin ARP yêu cầu.

Gói tin yêu cầu ARP (ARP request packet) được gửi tới các trạm, chỉ trạm B là đúng địa chỉ IP. Trạm B sẽ tạo ARP trả lời :




Hình 5-14. Khuôn dạng gói tin ARP trả lời.

Trạm B bổ sung IP_ to_Ethernet Address entry của host A và ARP cache của B

Trạm A bổ sung IP_to_Ethernet Address entry của host B và ARP cache của A

Như vậy bảng ánh xạ tự động bổ sung những đường dẫn (entry) mới mà nó biết, đồng thời cũng huỷ bỏ những đường dẫn (entry) mà nó không dùng đến.

### 5.6.2 Giao thức RARP (Reverse Address Resolution Protocol)

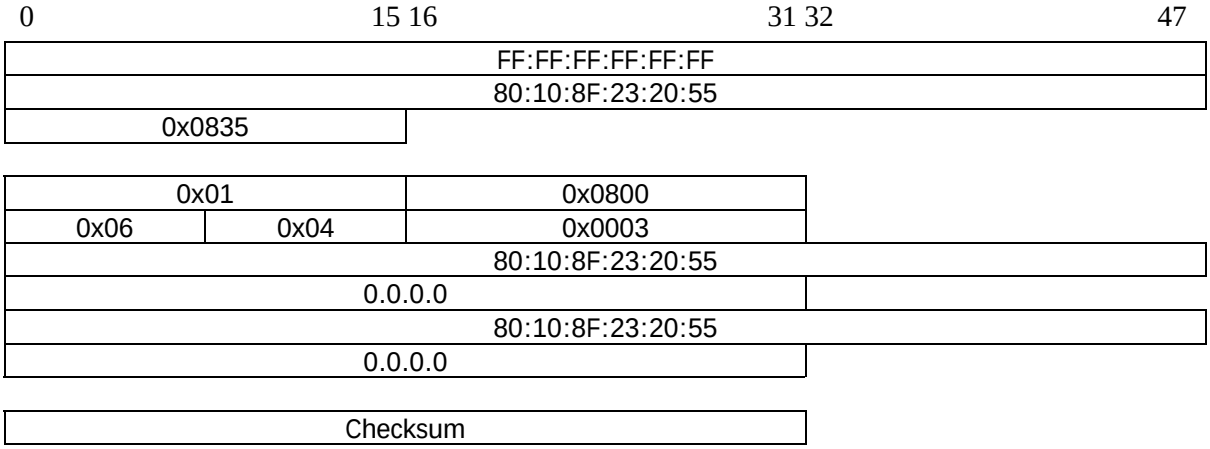
Đôi khi ta cần ánh xạ ngược lại.

Ví dụ một trạm không ổ đĩa, biết địa chỉ vật lý (datalink address) tức là địa chỉ card mạng giữ ở bộ nhớ ROM, nhưng không biết địa chỉ IP vì không có ổ đĩa. Khi này cần ánh xạ từ địa chỉ vật lý sang địa chỉ mạng.

Ta cũng làm như trên, nhưng thay kiểu trường từ 0x0806 bằng 0835.

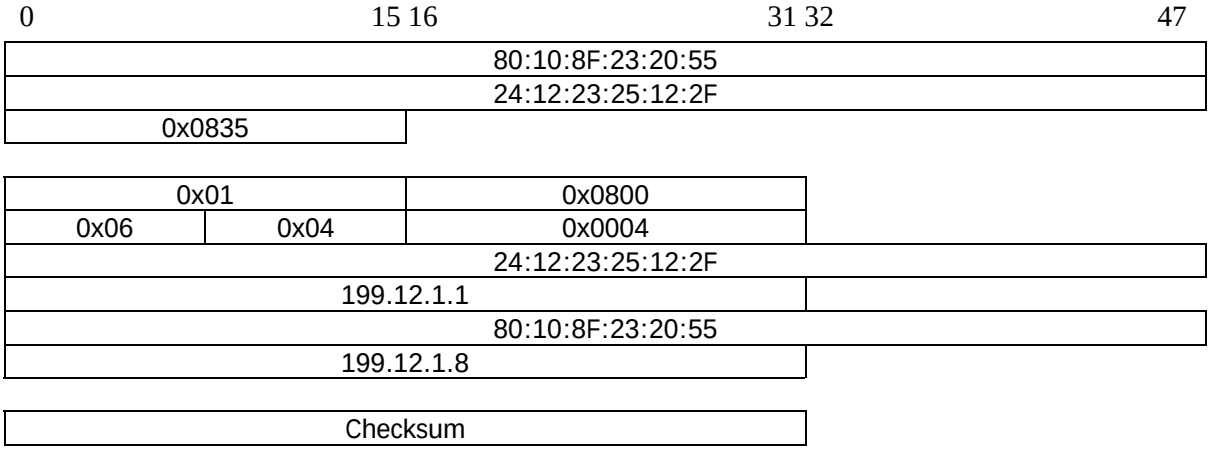
Yêu cầu chuyển đổi (reverse request) là 0x0003 và trả lời chuyển đổi (reverse reply) là 0x0004.

- Quá trình gởi yêu cầu RARP




Hình 5-15. Khuôn dạng gói tin RARP yêu cầu.

- Quá trình gởi trả lời RARP




Hình 5-16. Khuôn dạng gói tin trả lời RARP .

### 5.6.3 Giao thức ICMP

Giao thức ICMP (Internet Control Message Protocol) thực hiện truyền các thông tin điều khiển (các báo cáo về các tình trạng lỗi trên mạng, ...) giữa các

gateway hoặc các máy chủ trên liên mạng theo giao thức IP. Tình trạng lỗi có thể là: một datagram không thể đến được đích của nó, hoặc một router không đủ bộ nhớ đệm để lưu và chuyển một datagram, ... . Một thông báo ICMP được khởi tạo và chuyển cho IP. IP sẽ bọc (*encapsulate*) thông báo đó với một IP header và truyền đến cho router hoặc trạm đích.

#### *5.6.3.1 Ccác thành phần của thông báo ICMP hỗ trợ xác định lỗi và truy vấn*

Thông báo ICMP được chia làm 2 loại: thông báo lỗi ICMP và thông báo truy vấn ICMP.

Các thông báo ICMP khác nhau về định dạng tuỳ vào chức năng của từng loại, nhưng kiến trúc tổng quát bao gồm 2 phần: phần đầu (ICMP header) và phần dữ liệu (ICMP data).

Phần đầu của thông báo ICMP luôn bắt đầu bằng 3 trường:

a. TYPE: 8 bits, xác định loại thông báo ICMP.

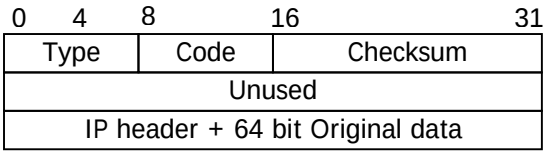
b. CODE: 8 bits, cung cấp thông tin chi tiết của từng loại thông báo ICMP.

c. CHECKSUM: 16 bits, xác định sự toàn vẹn dữ liệu trong quá trình truyền.

***1. Các thông báo lỗi ICMP***

Về mặt kỹ thuật, ICMP được thiết kế để cung cấp các thông tin về trạng thái không ổn định và thực hiện thông báo các trường hợp lỗi phát sinh của hệ thống phần cứng cũng như phần mềm làm ngăn chặn, huỷ bỏ quá trình gửi, nhận hoặc xử lý các datagram trên mạng Internet trước khi được chuyển đến đích cuối cùng.

Có 5 loại thông báo lỗi ICMP trong bảng I.1 và các thông báo có dạng chung như hình sau :




Hình 5-17. Dạng chung thông báo lỗi của ICMP

| Type | Thông báo lỗi ICMP |
|---|---|
| 3 | Destination Unreachable |
| 4 | Source Quench |
| 5 | Redirect |
| 11 | Time Exceeded |
| 12 | Parameter Problem |

***Bảng I.1***: Các loại thông báo lỗi của ICMP

Original IP header: 20-60 bytes chứa IP header của gói bị lỗi.

Original data: 8 bytes, chứa nội dung 64 bits đầu tiên của gói dữ liệu bị lỗi.

- *Destination Unreachable*

Các thông báo ICMP Destination Unreachable được tạo ra khi không thể chuyển đến 1 đích được xác định trong IP datagram. Bao gồm các loại lỗi sau:

| Code | Nội dung thông báo ICMP |
|---|---|
| 0 | Network Unreachable |
| 1 | Host Unreachable |
| 2 | Protocol Unreachable |
| 3 | Port Unreachable |
| 4 | Fragmentation needed and DF flag set |
| 5 | Source Route Fail |
| 6 | Destination Network unknown |
| 7 | Destination Host unknown |
| 8 | Source Host Isolated |
| 9 | Communication with Destination Network is Administratively Prohibited |
| 10 | Communication with Destination Host is Administratively Prohibited |

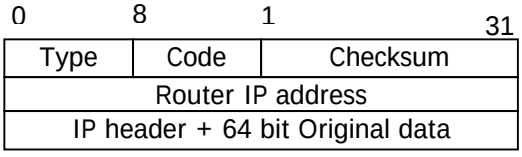
Bảng 5-1. Các lỗi của ICMP Destination Unreachable

- *Source Quench :* Khi vùng đệm của hệ thống nhận không đủ chỗ trống lưu trữ, hệ thống sẽ phát ra thông báo Source Quench. Trường CẶDQ của thông báo này luôn luôn nhận giá trị 0.
- *Redirect :* Một thông báo ICMP Redirect được tạo ra bởi 1 router trong trường hợp nó nhận thấy rằng một máy tính đang sử dụng con đường định tuyến không tối ưu.

Trường CẶDQ nhận 4 giá trị trong bảng và có định dạng như hình sau:

| Code | Nội dung |
|---|---|
| 0 | Redirect for the network (or subnet) |
| 1 | Redirect for the host |
| 2 | Redirect for the type of service and network |
| 3 | Redirect for the type of service and host |

Bảng 5-2. Các lỗi của ICMP Redirect




Hình 5-18. Dạng ICMP Redirect

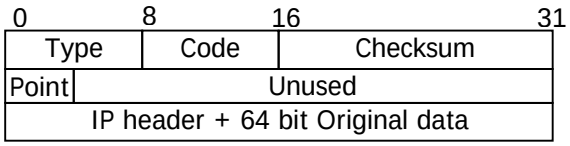
Router ip address là địa chỉ của bộ định tuyến mà máy nguồn sẽ dùng để trỏ máy đích.

- *Time Exceeded :* Router sẽ huỷ bỏ, không xử lý 1 datagram khi giá trị TTL của nó bằng 0 và phát ra một thông báo ICMP Time Exceeded. Có 2 loại ICMP Time Exceeded như sau:

| Code | Nội dung |
|---|---|
| 0 | Bộ đếm thời gian sống TTL của 1 datagram bằng 0 |
| 1 | Quá thời gian đợi để kết hợp các gói bị phân mảnh |

Bảng 5-3. Các lỗi của ICMP Time Qxceeded.

- *Parameter Problem :* Thông báo này được gửi đi khi có lỗi xuất hiện ở phần các tham số chọn lựa của datagram gửi đến. Trường CẶDỌ của thông báo này nhận 3 giá trị trong bảng và có định dạng như hình sau :




Hình 5-19. Dạng ICMP Parameter Problem

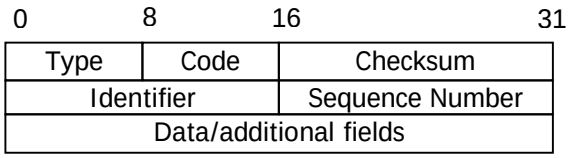
| Code | Giải thích |
|---|---|
| 0 | Có một lỗi đặc biệt trong lược đồ dữ liệu. |
| 1 | Phần option của IP header chưa định nghĩa. |
| 2 | Lỗi Header Length và (hoặc) Total Packet Length trong IP header. |

Bảng 5-4. Các lỗi của ICMP Parameter Problem

Pointer: xác định vị trí gây ra lỗi trong datagram.

***2. Các thông báo truy vấn ICMP***

ICMP được sử dụng trong việc khảo sát các đặc trưng chung của mạng với 2 loại thông báo request và reply. Có 8 loại thông báo truy vấn ICMP được liệt kê trong bảng và có định dạng như hình sau :



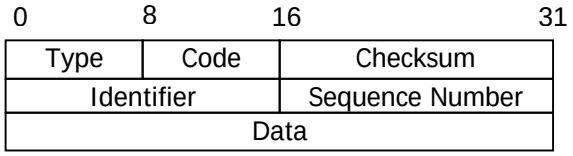

Hình 5-20. Dạng ICMP truy vấn.

| Type | Loại thông báo |
|---|---|
| 0 | Echo Reply |
| 8 | Echo Request |
| 13 | Timestamp Request |
| 14 | Timestamp Reply |
| 15 | Information Request |
| 16 | Information Reply |
| 17 | Address Mask Request |
| 18 | Address Mask Reply |

Bảng 5-5. Các loại thông báo truy vấn ICMP.

- Identifier được sử dụng để phân biệt các thông báo được gởi đến các host khác nhau.
- Sequence number được sử dụng để phân biệt các thông báo được gửi đến cùng một host.
- Data/additional fields được dùng theo từng loại thông báo truy vấn ICMP.

- *Echo Request vµ Echo Reply*



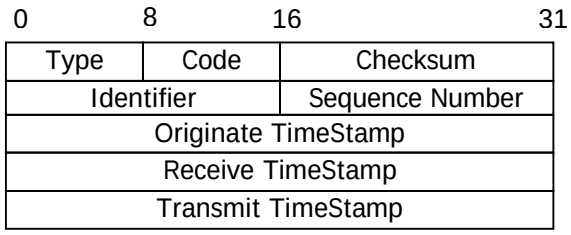

Hình 5-21. Dạng ICMP Echo Request & Reply.

Người ta sử dụng ICMP Echo để xác định xem một địa chỉ IP đích còn hoạt động hay không bằng cách gửi thông báo ICMP Echo Request đến hệ thống đích và chờ xem nếu nhận được thông báo ICMP Echo Reply thì sẽ xác định đích đấy vẫn còn hoạt động ngược lại thì đã bị down. Định dạng thông báo như trong hình sau :

Kích thước của DATA thay đổi tuỳ thuộc vào từng loại hệ điều hành. Trong hệ điều hành UNIX, kích thước của nó là 56 bytes, trong Microsoft Windows là 32 bytes,...

- *Timestamp Request và Timestamp Reply*

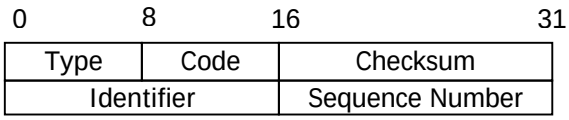
Mỗi máy đều có 1 đồng hồ riêng xác định thời gian vận hành của nó, quá trình hoạt động trong những hệ thống phần mềm phân tán thì sự khác biệt nhau lớn về thời gian giữa các máy tính sẽ gây ra nhiều vấn đề khó khăn. ICMP cung cấp một cơ chế cho phép lấy thời gian từ một máy khác và có định dạng như hình sau.




Hình 5-22. ICMP Timestamp Request & Reply

- Originate timestamp là thời gian máy nguồn thực hiện gửi báo.
- Receive timestamp là thời gian đầu tiên máy đích nhận được thông báo.
- Transmit timestamp là thời gian cuối bên đích xử lý thông báo và gửi đi.

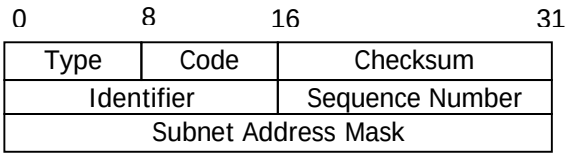
- *Information request và reply*




Hình 5-23. ICMP information request & reply

Được sử dụng nhằm hỗ trợ các hệ thống máy trạm không đĩa khi khởi động; cho phép các máy tính tìm ra địa chỉ Internet của chúng lúc khởi động hệ thống.

- *Address Mask Request và Reply*




H×nh 5-24. ICMP Ađress Mask Request & Reply

Để biết subnet mask, máy sẽ gửi một thông báo ICMP Address Mask Request đến 1 router và chờ nhận thông báo ICMP Address Mask Reply. Subnet Address Mask chứa địa chỉ của mặt nạ con của mạng.

Các bộ định tuyến phát bản tin ICMP để báo cho các trạm biết : gói tin không tới, hoặc tồn tại đường đi tốt hơn. Một số trường hợp có thể xảy ra là :

- *Destination unreachable* (không tới được đích): Bản tin không tới được đích do có lỗi hoặc không tìm được đường đi.
- *Routing redirect* (đổi đường đi): Thay đổi đường đi của bản tin do tồn tại đường đi tối ưu hơn (yêu cầu đổi đường đi).
- *Time expirect* (hết thời gian): Hết thời hạn khi TTL về 0 (timeout).
- *Echo request và cho echo reply* : Xuất hiện yêu cầu và trả lời.

  ICMP được dùng vào việc gỡ rối mạng cho biết tình trạng của mạng.

Lệnh Ping ***(Packet Internet Oroper)*** được dùng để hỏi (query) hệ thống (máy tính) khác để đảm bảo rằng một kết nối vẫn đang hoạt động (active). Lệnh Ping hoạt động bằng cách gửi ra một yêu cầu phản hồi (echo request) ICMP (Internet Control Message Protocol). Nếu như phần mềm IP của máy tính nhận được yêu cầu ICMP đó, nó đưa ra một trả lời phản hồi (echo reply) ngay lập tức. Máy gửi lại tiếp tục gửi một yêu cầu phản xạ cho đến khi lệnh ping được kết thúc bằng một tổ hợp phím thoát (Ctrl+C hoặc phím Delete trên UNIX).

## 5.7 Phiên bản IPv6

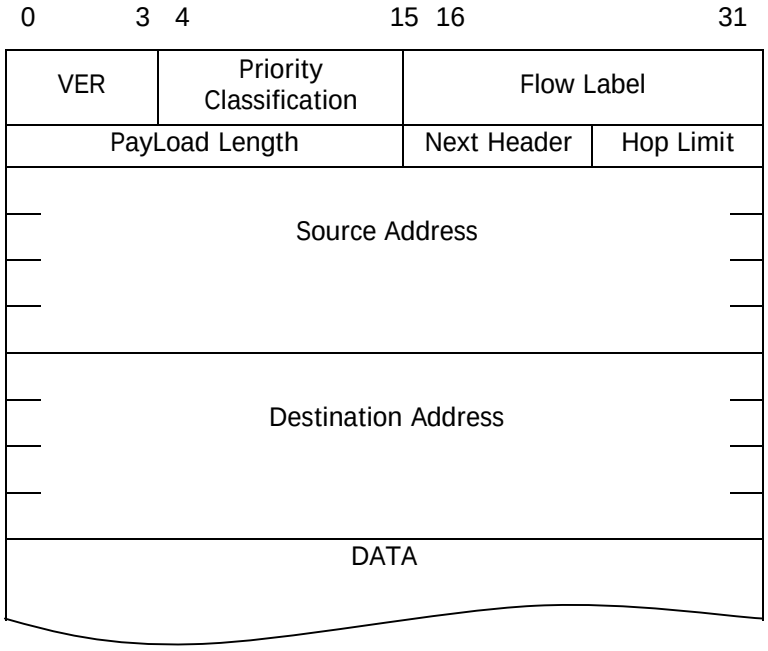
Với sự phát triển nhanh chóng của Internet thì địa chỉ IP 32 bit không thể đáp ứng được nhu cầu sử dụng Internet. Để khắc phục điều này phiên bản IP6 (IP Next Generation) đang được phát triển. Phiên bản IPv6 có các thay đổi như sau :

- Sử dụng 128 bit địa chỉ mạng thay cho 32 bit địa chỉ như phiên bản IPv4.
- Mở rộng phần Header cho ứng dụng và lựa chọn của khung tin.
- Hỗ trợ các loại dữ liệu audio và video.

- Có các giao thức mở rộng : cho phép bổ sung nhiều thông tin vào một datagram.

### 5.7.1 Khung tin IPng v6

Phần Header của các khung tin Ipng đã được thay đổi so với phiên bản 4. Phần lớn sự thay đổi của IPng là địa chỉ IP 128 bit và bỏ các trường không cần thiết. Cấu tạo của khung tin IPng như sau :




H×nh 5-25. CÊu t¹o cña gãi tin IPv6.

## 5.8 Định tuyến trên Internet

### 5.8.1 Bảng chọn đường

Một số phương thức thông thường xây dựng một bảng chọn đường (routing *table*) như sau :

- Bảng cố định được tạo ra dựa vào sơ đồ của mạng, bảng này liên tục được thay đổi và được cập nhật lại mỗi khi có sự thay đổi vật lý ở bất cứ nơi nào của mạng.
- Bảng động được dùng để ước lượng về đường truyền và các thông điệp từ các nút khác để điều chỉnh lại thông tin của bảng bên trong.
- Bảng dẫn đường cố định chính được tải về từ một trung tâm của các nút mạng trong một khoảng thời gian nhất định hoặc được tải về khi cần thiết.

Mỗi một phương thức đều có các ưu, nhược điểm của nó. Bảng động được đặt ở từng nút mạng hoặc được tải về trong những khoảng thời gian nhất định từ một

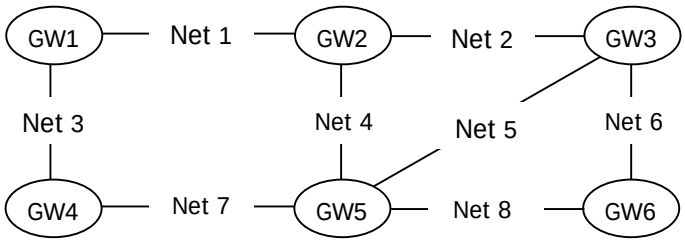
nơi chứa bảng cố định, nó không phức tạp và thích ứng với những thay đổi nhanh chóng trên mạng. Bảng chính thường là tốt hơn bảng cố định bởi vì quản lý một bảng ở trung tâm sẽ dễ dàng hơn quản lý từng bảng được đặt tại mỗi nút mạng.

### 5.8.2 Xây dựng bảng chọn đường cho các Router/Gateway

Trong liên mạng, tại mỗi cổng phải có một bảng chọn đường để chỉ ra muốn đến mạng đích nào thì phải đến cổng tiếp theo là cổng nào. Bảng chọn đường gồm hai phần : phần bên trái là mạng đích, nơi muốn đến, phần bên phải là khoảng cách tới đó và cổng tiếp theo.

Để xây dựng bảng chọn đường, từ cổng đang đứng ta xét các mạng cạnh đó, sau đó là các mạng ở cạnh các cổng tiếp theo và cứ thế cho đến hết các mạng trong liên mạng.

Ví dụ 1: Lập bảng chọn đường cho các router.gateway của liên mạng sau :




| GW1 | |
|---|---|
| Neti | D,G |
| 1 | 0,1 |
| 2 | 1,2 |
| 3 | 0,1 |
| 4 | 1,2 |
| 5 | 2,2(4) |
| 6 | 2,2 |
| 7 | 1,4 |
| 8 | 2,2(4) |

| GW2 | |
|---|---|
| Neti | D,G |
| 1 | 0,2 |
| 2 | 0,2 |
| 3 | 1,1 |
| 4 | 0,2 |
| 5 | 1,3(5) |
| 6 | 1,3 |
| 7 | 1,5 |
| 8 | 1,5 |

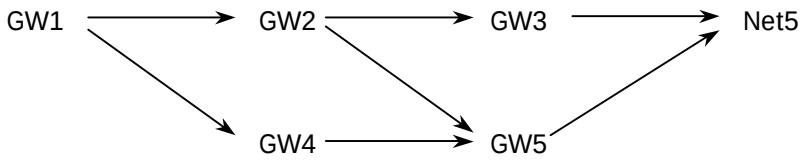
| GW3 | |
|---|---|
| Neti | D,G |
| 1 | 1,2 |
| 2 | 0,3 |
| 3 | 2,2 |
| 4 | 1,2(5) |
| 5 | 0,3 |
| 6 | 0,3 |
| 7 | 1,5 |
| 8 | 1,5(6) |

| GW4 | |
|---|---|
| Neti | D,G |
| 1 | 1,2 |
| 2 | 2,1(5) |
| 3 | 0,4 |
| 4 | 1,5 |
| 5 | 1,5 |
| 6 | 2,5 |
| 7 | 0,4 |
| 8 | 1,5 |

| GW5 | |
|---|---|
| Neti | D,G |
| 1 | 1,2 |
| 2 | 1,2 |
| 3 | 1,4 |
| 4 | 0,5 |
| 5 | 0,5 |
| 6 | 1,3(6) |
| 7 | 0,5 |
| 8 | 0,5 |

| GW6 | |
|---|---|
| Neti | D,G |
| 1 | 2,3(5) |
| 2 | 1,3 |
| 3 | 2,5 |
| 4 | 1,5 |
| 5 | 1,3(5) |
| 6 | 0,6 |
| 7 | 1,5 |
| 8 | 0,6 |

Dựa vào bảng chọn đường, tìm đường đi từ GW1 tới Net 5 như sau :




Đối với nhiều host, bảng dẫn đường tĩnh hoạt động như sau :

- Nếu đích nằm trong mạng cục bộ, dữ liệu được gởi đến máy đích
- Nếu đích nằm trên mạng ở xa, dữ liệu được chuyển tiếp đến gateway cục bộ.

Tuỳ thuộc vào kích cỡ của mạng mà các giao thức chọn đường khác nhau sẽ được sử dụng. Giao thức chọn đường trong một hệ thống nội bộ là RIP (Routing Information Protocol). Giao thức chọn đường giữa các hệ thống là EGP (External Gateway Protocol) và BGP (Border Gateway Protocol).

## 5.9 Mạng X.25

Vào những năm cuối thập niên 70, người ta phải cần đến một loạt các giao thức để cung cấp cho những người sử dụng mạng diện rộng WAN kết nối thông qua mạng dữ liệu công cộng (Public Data Networks - PDNs). Các loại hình PDNs như TELENET và TYMNET đã đạt được những thành công đáng ghi nhận, nhưng việc tiêu chuẩn hóa giao thức dường như còn ngoài tầm những người sử dụng mạng PDNs do việc đòi hỏi tính tương thích của thiết bị ngày một cao và đồng thời chi phí phải thấp. Kết quả của sự nỗ lực không ngừng này là sự ra đời của một loạt giao thức, trong đó X.25 được xem là giao thức phổ biến nhất.

Mạng X.25 và các giao thức liên quan do một tổ chức Quốc gia gọi là Hiệp hội Viễn thông Quốc tế (ITU) quản lý. Ban chịu trách nhiệm về các nghiệp vụ truyền tín hiệu âm thanh và dữ liệu của ITU gọi là ủy ban Tư vấn Quốc tế về Điện thoại và Điện báo (CCITT). Các thành viên của CCITT bao gồm FCC, PTTs Âu châu, các doanh nghiệp truyền thông và nhiều hãng máy tính, truyền dữ liệu khác. Do nhiều thành quả đóng góp trực tiếp có tính kế thừa, mạng X.25 thực sự được xem là mạng tiêu chuẩn có tính toàn cầu.

### 5.9.1 Cơ sở kỹ thuật

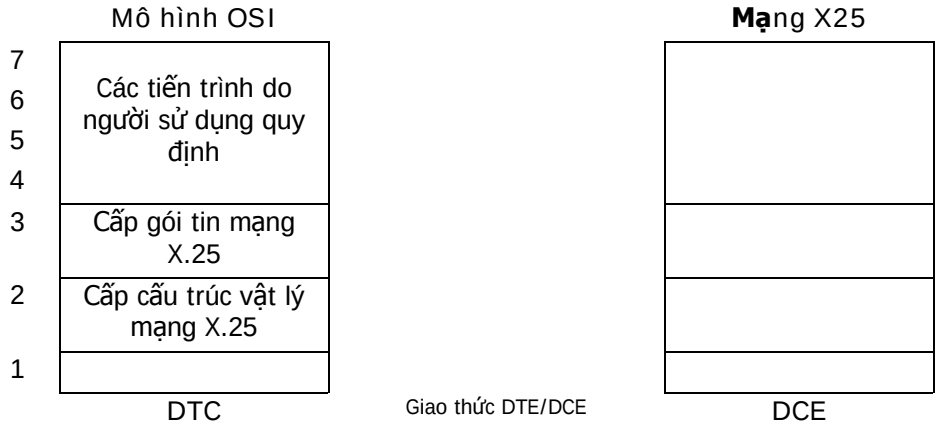
Mạng X.25 là một mạng điện thoại dùng để truyền dữ liệu. Để bắt đầu thực hiện quá trình giao tiếp, một máy tính cần phải liên kết với một máy khác để yêu cầu thực hiện giao tiếp. Máy được yêu cầu liên kết có thể chấp nhận hoặc từ chối việc giao tiếp. Nếu liên kết được chấp nhận, hai hệ thống có thể bắt đầu truyền tải thông tin qua lại hai chiều đồng thời với nhau. Cả hai bên đều có thể chấm dứt việc giao tiếp vào bất cứ thời điểm nào tùy ý.

Các đặc tính của mạng X.25 cho phép xác định quá trình tương tác từ nút-đến-nút (point-to-point) giữa các thiết bị truyền dữ liệu đầu cuối (Data Terminal Equipment - DTE) với các thiết bị kết cuối mạch truyền dữ liệu (Data Circuit-terminating Equipment - DCE). DTEs (bao gồm các trạm đầu cuối và máy chủ của người sử dụng mạng) kết nối với DCEs (bao gồm modem, các gói tin và các cổng truy cập PDN, thường đặt tại các trạm truyền thông), DCEs lại nối kết vào kênh chuyển mạch gói (Packet Switching Exchanges - PSEs) và các DCEs khác trong mạng PSNs và cuối cùng đến một DTE khác.

Một DTE có thể xem là một trạm đầu cuối nhưng không thực hiện đầy đủ các chức năng của mạng X.25. Các DTE được nối kết với DCE thông qua một thiết bị chuyển đổi gọi là thiết bị ghép/tách gói tin (Packet Assembler/Disassembler - PAD).

Quá trình hoạt động của mạch ghép nối từ trạm đầu cuối đến PAD, các dịch vụ do PAD cung cấp và các tương tác giữa PAD và các máy chủ do CCITT quy định.

Sơ đồ đặc tính của mạng X.25 kiểu phân tầng từ 1 tới 3 theo mô hình tham chiếu cho việc nối kết các hệ thống mở OSI. Tầng 3 của mạng X.25 mô tả các quy trình định dạng và chuyển mạch gói giữa các thành tố tầng 3 ngang cấp. Tầng 2 của mạng X.25 do các thủ tục truy cập liên kết cân bằng (Link Access Procedure Balance - LAPB) kiểm soát. LAPB xác lập các đơn vị gói tin (packet framing) cho các liên kết DTE/DCE. Tầng 1 của mạng X.25 xác lập các thủ tục về điện và cơ để kích hoạt và chấm dứt quá trình kết nối vật lý của DTE và DCE. Mối quan hệ này được minh họa theo hình vẽ dưới đây. Chú ý rằng tầng 2 và 3 cũng tham chiếu theo tiêu chuẩn ISO 7776 (LAPB) và ISO 8208 (các tầng gói tin mạng X.25).




Hình 5-26. Mối quan hệ giữa các tầng trong mạng X.25.

Quá trình giao tiếp từ nút-tới-nút (end-to-end) giữa các DTEs được thực hiện hoàn thiện thông qua một sự kết nối song phương gọi là liên kết truyền ảo (virtual circuit). Các liên kết ảo cho phép các hệ mạng khác nhau có thể giao tiếp được với nhau thông qua mọi nút liên kết trung gian mà không cần đến các bộ phận chuyên dụng để định rõ các liên kết vật lý. Các liên kết ảo hoặc có thể duy trì vĩnh viễn hoặc có thể tạm thời. Liên kết ảo vĩnh viễn được gọi là PVCs (Permanent Virtual Circuits), liên kết ảo tạm thời được gọi là SVCs (Switched Virtual Circuits). PVCs chủ yếu áp dụng cho phương thức truyền dữ liệu thường xuyên còn SVCs được áp dụng cho phương thức truyền dữ liệu không thường xuyên. Tầng 3 của mạng X.25 liên quan tới phương thức giao tiếp từ nút tới nút bao gồm cả hai liên kết ảo PVCs và SVCs.

Một khi đã thiết lập liên kết ảo, PTE có thể thực hiện truyền một gói tin đến một PTE khác bằng cách chuyển gói tin đến DCE thông qua một liên kết ảo thích hợp. Sau đó DCE sẽ tiến hành ền ưu tiên của liên kết ảo để định ra thức truyền gói tin lên mạng X.25. Các giao thức của tầng 3 mạng X.25 sẽ tiến hành chèn thông tin

vào giữa các DTE được kiểm soát bởi DCE của mạng phía nhận gói tin rồi sau đó được chuyển đến DTE đích.

## 5.10 Kỹ thuật FRAME RELAY

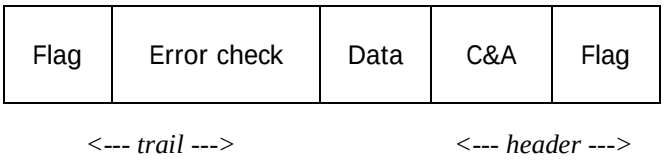
Bước sang thập kỷ 80 và đầu thập kỷ 90, công nghệ thông tin có những bước tiến đặc biệt là chế tạo và sử dụng cáp quang vào mạng truyền dẫn tạo nên chất lượng thông tin rất cao. Sử dụng giao thức X25 để truyền đa số liệu trên mạng cáp quang, dữ liệu nhận được có thể đánh giá là đạt yêu cầu. Tuy nhiên người ta nhận thấy rằng sử dụng giao thức này làm mất rất nhiều thời gian để truyền số liệu trên mạng cáp quang. Do đó công nghệ Frame Relay ra đời có thể chuyển nhận các khung lớn tới 4096 byte trong khi đó gói tiêu chuẩn của X25 khuyến cáo dùng là 128 byte, không cần thời gian cho việc hỏi đáp, phát hiện lỗi và sửa lỗi ở lớp 3 (*No protocol at Network Layer*) nên Frame Relay có khả năng chuyển tải nhanh hơn hàng chục lần so với X25 ở cùng tốc độ. Frame Relay rất thích hợp cho truyền số liệu tốc độ cao và cho kết nối LAN to LAN và cả cho âm thanh, nhưng điều kiện tiên quyết để sử dụng công nghệ Frame relay là chất lượng mạng truyền dẫn phải cao.

Frame-Relay bắt đầu được đưa ra như tiêu chuẩn của một trong những giao thức truyền số liệu từ năm 1984 trong hội nghị của ủy ban Tư vấn Quốc tế về Điệnthoại và Điện báo CCITT và cũng được Viện tiêu chuẩn quốc gia Mỹ ANSI đưa thành tiêu chuẩn của ANSI vào năm đó.

Mục tiêu chính của Frame-Relay cũng giống như của nhiều tiêu chuẩn khác, đó là tạo ra một giao diện chuẩn để kết nối thiết bị - của các nhà sản xuất thiết bị khác nhau - giữa người dùng và mạng UNI (*User to Network Interface*). Frame-Relay được thiết kế nhằm cung cấp dịch vụ chuyển khung nhanh cho các ứng dụng số liệu tương tự như X.25 hay ATM.

Mạng truyền số liệu theo công nghệ chuyển mạch gói X.25 chỉ có thể phục vụ cho các nhu cầu truyền số liệu tốc độ thấp (tối đa tới 128 Kbps) nhưng nó có tính an toàn cao, khắc phục được các yếu điểm của một mạng truyền dẫn chất lượng kém. Với các công nghệ truyền dẫn hiện nay, vấn đề nâng cấp chất lượng các đường truyền dẫn không còn quá phức tạp như trước kia. Vì vậy, chúng ta còn có thể chọn hướng phát triển là xây dựng mạng truyền số liệu theo công nghệ Frame-relay và tiến tới công nghệ ATM.

### 5.10.1 Khuôn dạng gói dữ liệu Frame-Relay




Hình 5-27. Khuôn dạng gói dữ liệu Frame-Relay.

- Flag: Cờ
- Error check: Trường kiểm tra lỗi
- Data: Trường dữ liệu
- C&A: Trường địa chỉ và điều khiển

Để thực hiện nhiệm vụ truyền số liệu, mạng Frame-Relay sẽ phải giải quyết vấn đề tắc nghẽn thông tin trên mạng, thực chất đây là vấn đề của tầng Mạng trong mô hình 7 tầng. Frame-Relay làm việc ở tầng Liên kết nhưng cũng phải giải quyết vấn đề này để đảm bảo khả năng lưu chuyển thông tin. Hầu hết các mạng truyền số liệu đều sử dụng kỹ thuật điều khiển luồng để giải quyết vấn đề tắc nghẽn. Có hai phương pháp được sử dụng khi xảy ra tắc nghẽn trong mạng: thông báo cho người dùng, router, chuyển mạch về sự cố tắc nghẽn xảy ra và thực hiện các công việc nhằm hiệu chỉnh luồng thông tin. Cả hai phương pháp này mạng Frame-Relay đều dùng đến các bit BECN (Backward Explicit Congestion Notification) và bit FECN (Forward Explicit Congestion Notification) trong trường điều khiển.

Bit FECN được thiết lập khi có tắc nghẽn để thông báo rằng thủ tục xử lý tắt nghẽn đã được khởi tạo, và tương ứng với lưu lượng bị nghẽn từ hướng của Frame có bit FECN tới. Ngược lại, bit BECN cũng được thiết lập khi có tắc nghẽn để thông báo rằng thủ tục xử lý nghẽn đã được khởi tạo, nhưng tương ứng với lưu l-ượng bị nghẽn từ hướng ngược với Frame có bit BECN tới. Khi các bit này được thiết lập thì mạng phải dùng đến một liên kết logic dự phòng để chuyển các thông tin để xử lý nghẽn, đó là liên kết với mã nhận dạng DLCI (Data Link Connection Identifier) số 1023. Các liên kết với mã nhận dạng nhỏ hơn được dùng để truyền số liệu của người dùng.

# BÀI TẬP

1. Viết sơ đồ mô tả thuật giải hoạt động chọn đường trên mạng.
2. Khảo sát cấu trúc và hoạt động của giao thức điều khiển ICMP
3. Tìm hiểu các lệnh của hệ điều hành Windows và Linux để xem và thay đổi các thông số bảng chọn đường.

*Chương 6*

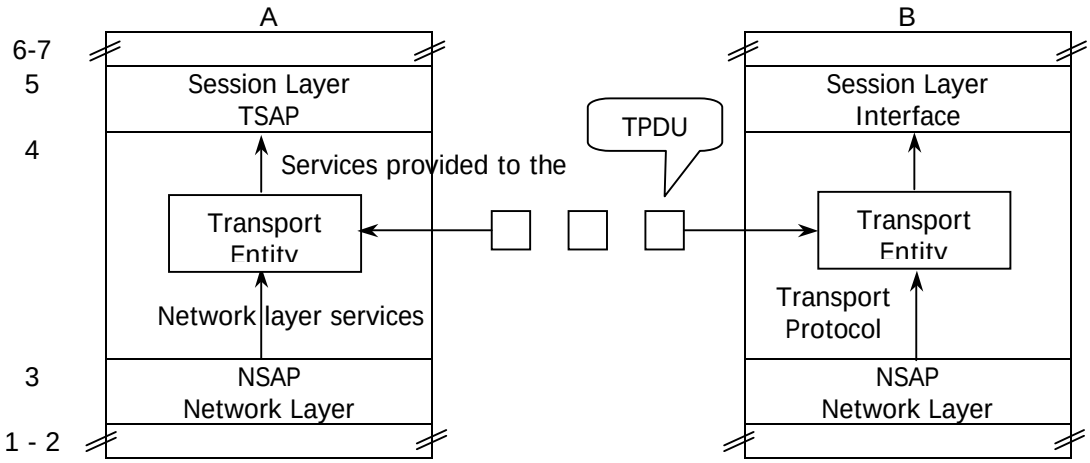
# TẦNG GIAO VẬN

Tầng giao vận làm nhiệm vụ thiết lập, duy trì và huỷ bỏ các cuộc giao tiếp giữa hai máy, đảm bảo việc dữ liệu truyền giống hoàn toàn dữ liệu nhận. Dữ liệu qua các mạng con có thể bị lỗi, tập tin tầng giao vận thực hiện cải thiện chất lượng dịch vụ, đảm bảo dữ liệu được truyền một cách chính xác và truyền lại nếu như phát hiện thấy lỗi. Tầng giao vận *quản lý dữ liệu gửi*, *xác định trật tự* của dữ liệu và *độ ưu tiên* của dữ liệu đó.

## 6.1 Các vấn đề của tầng giao vận

### 6.1.1 Cung cấp dịch vụ cho tầng phiên

Để thực hiện mục tiêu chuyển giao dữ liệu tin cậy, an toàn cho tầng 5, tầng 4 phải dùng các dịch vụ được cung cấp từ tầng 3 (network layer). Phần cứng và phần mền trong phần 4 để thực hiện công việc coi là thực thể giao vận (*transport entity*). Mối quan hệ giữa các lớp 3, 4, 5, được mô tả bởi hình sau:




Hình 6-1. Mối quan hệ giữa các thực thể trong tầng Phiên.

Có hai dịch vụ mạng nên cũng có hai dịch vụ giao vận: *dịch vụ có kết nối* và *không kết nối*.

Do dữ liệu qua các subnet có thể sai sót, người sử dụng không có được điều khiển trên subnet hoặc tăng cường quản lý lỗi ở tầng hai. Chỉ có khả năng đặt thêm một tầng trên lớp 3 để cải thiện chất lượng dịch vụ (QoS). Nếu giữa chúng một tầng giao vận được kết  nối mạng được kết thúc đột ngột và không biết được sự cố gì đã xảy ra, nó có thể thiết lập một kết nối mới ở lớp mạng tới tầng giao vận ở xa và gởi yêu cầu hỏi số liệu nào đến, số liệu nào không tự nó biết được sai sót xảy ra ở đâu. Tầng 4 có thể phát hiện mất gói tin, số liệu bị biến đổi, N-RESET ở lớp mạng. Tầng 1 -> 4 cung cấp dịch vụ giao vận. Tầng 5 ->7 sử dụng dịch vụ giao vận

- Các hàm dịch vụ của tầng giao vận có kết nối

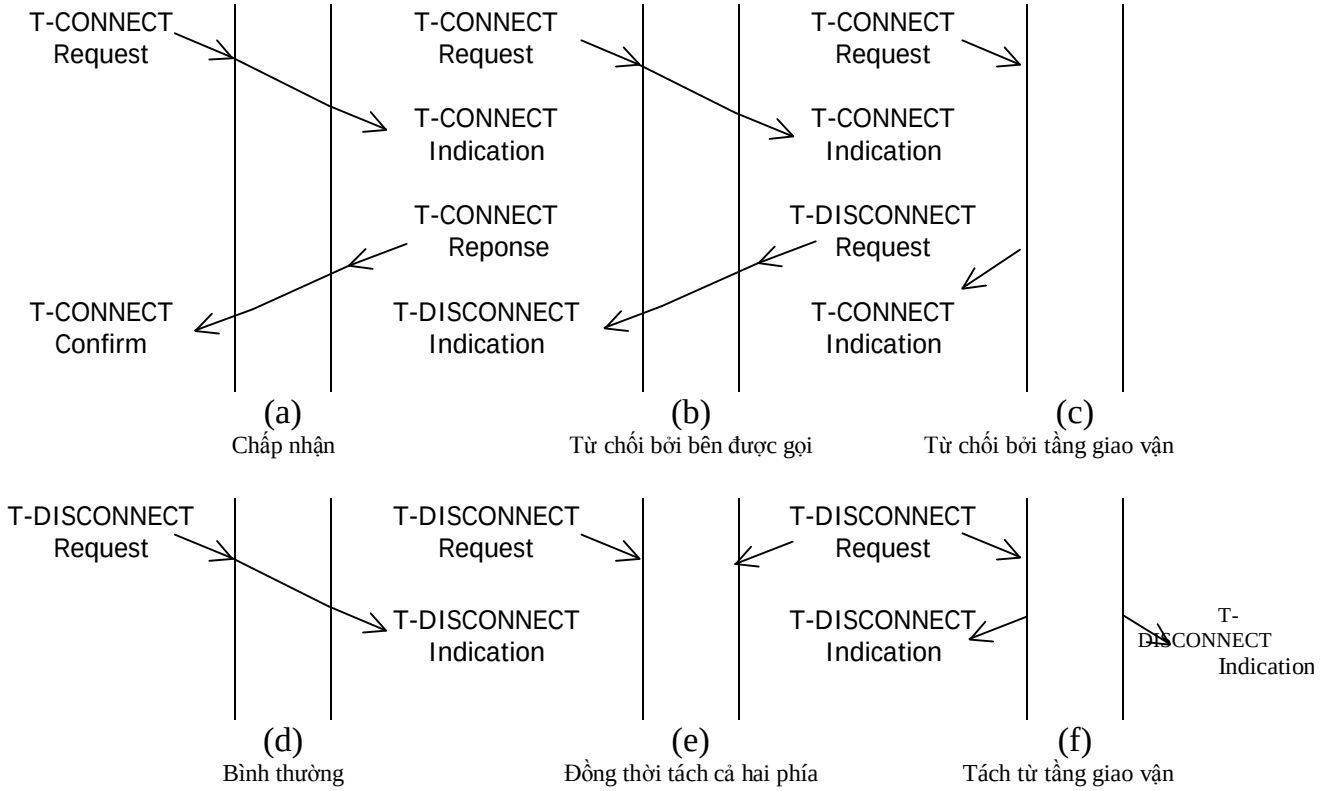
Ngoài phần giao thức chuẩn, ISO còn định nghĩa các dịch vụ mà tầng Giao vận cung cấp cho các thực thể ở tầng Phiên trong trường hợp có liên kết, dưới dạng một tập hợp các hàm dịch vụ nguyên thủy(services primitives) như sau :

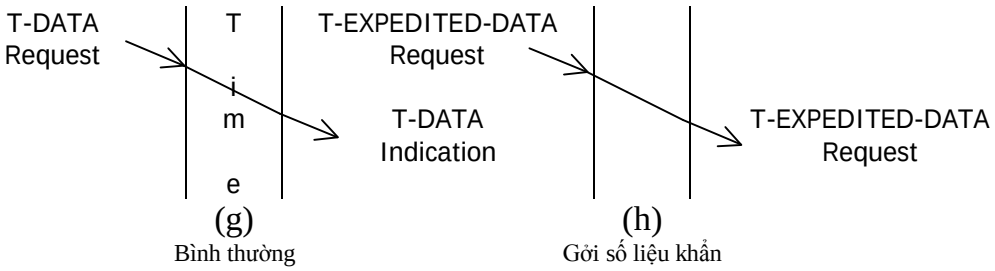
T-CONNECT request (callce, caller, exp wanted, qos, user data)
T-CONNECT indication (callce, caller, exp wanted, qos, user data)
T-CONNECT response (qos, responder, exp wanted, user data)
T-CONNECT confirm (qos, responder, exp wanted, user data)
T-DISCONNECT request (user data)
T-DISCONNECT indication (reason, user data)
T-DATA request (user data)
T-DATA indication (reason, user data)
T-EXPEDITED-DATA request (user data)
T-EXPEDITED-DATA indication (reason, user data)

- Các hàm dịch vụ của tầng giao vận không có kết nối : Chỉ có hai hàm dịch vụ được định nghĩa :

T-UNITDATA request (callce, caller, QoS, user data)
T-UNITDATA indication (callce, caller, QoS, user data)

- Quan hệ giữa các hàm OSI nguyên thủy : Quá trình nối, tách và trao đổi dữ liệu diễn ra như sau :






Hình 6-2. Quan hệ giữa các hàm OSI nguyên thủy.

Giải thích

(a) Quá trình nối được chấp nhận
(b) Quá trình nối bị từ chối bởi bên được gọi
(c) Quá trình nối bị từ chối bởi tầng Giao vận do lỗi của người sử dụng hoặc người chung cấp dịch vụ giao vận gây nên.
(d) Quá trình tách bình thường
(e) Quá trình tách đồng thời cả hai phía
(f) Quá trình tách từ tầng Giao vận
(g) Quá trình trao đổi dữ liệu bình thường
(h) Quá trình trao đổi dữ liệu khẩn

Trong hình (c) trên, việc từ chối có thể do lỗi của người sử dụng hoặc người cung cấp dịch vụ giao vận gây nên. Khi đó, không có gì được phát qua mạng vì vậy đầu kia không nghe được gì cả. Có những qui tắc cho người sử dụng các hàm dịch vụ giao vận. Ví dụ, không được dùng T-DISCONNECT.request khi tiếp nối chưa được thiết lập.

### 6.1.2 Chất lượng dịch vụ QoS

Chức năng cơ bản của tầng 4 là tăng cường chất lượng dịch vụ được cung cấp bởi tầng 3. Nếu lớp chất lượng chưa tốt, tầng Giao vận sẽ khắc phục khoảng ngăn cách giữa những gì mà người sử dụng tầng Giao vận muốn và những gì mà lớp mạng cung cấp. Các tham số của chất lượng dịch vụ QoS (Quality of Service) bao gồm :

- *Thời gian thiết lập liên kết* là thời gian từ khi gởi yêu cầu tới thời điểm nhận được xác nhận liên kết.
- *Xác nhận không thành công của thiết lập liên kết* - là tỷ lệ yêu cầu liên kết không được chấp nhận trong một thời hạn tối đa.
- *Lưu lượng của liên kết* do số byte hữu ích có thể truyền trong một giây, lưu lượng được tính *trong một cuộc trao đổi* hoặc dựa vào *khả năng của mạng theo 2 chiều.*

- *Thời gian trễ (*Độ trễ truyền dẫn - transmit delay) là khoảng thời gian giữa thời điểm mà người sử dụng dịch vụ của tầng Giao vận bên phát gởi thông báo tời thời điểm thực thể của tầng Giao vận bên thu nhận được. Đánh giá theo 2 chiều.
- *Tỷ lệ lỗi* là tỷ số giữa tin báo bị lỗi (hoặc mất) trên tổng số tin báo được truyền trong một chu kỳ định trước.
- *Xác nhận sự cố truyền:* tỷ số giữa thời gian có sự cố với thời gian cả chu kỳ quan sát.
- *Thời gian hủy liên kết* là thời gian từ khi một người sử dụng phát huy cầu huỷ liên kết đến khi liên kết được huỷ thật sự tại thiết bị đầu cuối từ xa.
- *Xác suất lỗi khi hủy liên kết* là tỷ lệ số yêu cầu hủy liên kết không được thực hiện trong thời gian lớn nhất.
- *Khả năng bảo vệ* là khả năng của người sử dụng cấm thiết bị đầu cuối bên ngoài truy nhập bất hợp pháp hay thay đổi dữ liệu truyền.
- *Thông số ưu tiên:* cho phép người sử dụng có quyền ưu tiên được phục vụ cao hơn đối với một liên kết.
- *Thông số hủy bỏ* cho phép tầng giao vận tự quyết định huỷ liên kết khi có tắc nghẽn hay các vấn đề bên trong mạng.

Người sử dụng khi yêu cầu liên kết sẽ gởi tất cả các thông số với các giá trị yêu cầu tới tầng giao vận và bắt đầu quá trình đàm thoại với các thông số đó.

So sánh các hàm cơ bản của dịch vụ giao vận và dịch vụ mạng, ta thấy các dịch vụ mạng và giao vận gần giống nhau. Sự khác nhau là dịch vụ mạng cho phép người sử dụng xử lý Acknowledgements và N-RQSQTS. Ngược lại, dịch vụ giao vận không quan tâm đến vì dịch vụ lớp giao vận là tin cậy, không có lỗi. Dịch vụ mạng được dùng bởi tầng giao vận.

### 6.1.3 Các lớp giao thức của tầng giao vận

Các dịch vụ tầng giao vận bảo đảm bằng các giao thức giữa 2 thực thể của tầng cũng tương tự như giao thức của tầng liên kết dữ liệu nó giải quyết vấn đề lỗi, điều khiển lưu lượng và bảo đảm trình tự mảng tin.

tầng liên kết dữ liệu, hai IMP truyền tin trực tiếp qua đường kênh vật lý. ở tầng giao vận, đường kênh vật lý này được thay bằng subnet. Sự khác nhau này kéo theo sự khác nhau về xây dựng các thủ tục. ở tầng giao vận phải xác định địa chỉ nơi nhận, ở tầng liên kết dữ liệu thì không cần vì chỉ có một đường truyền tin giữa hai điểm. Quá trình kết nối ở tầng giao vận cũng phức tạp hơn ở tầng liên kết giữ liệu.

Tầng giao vận đòi hỏi khả năng lưu trữ trong mạng (subnet) để giữ những gói tin bị sự cố và đòi hỏi thủ tục đặc biệt. tầng giao vận số các kết nối lớn hơn nên các vấn đề bộ đệm và điều khiển dòng phức tạp hơn.

Từ quan điểm thiết kế thủ tục giao vận, các dịch vụ được cho bởi mạng quan trọng hơn các tính chất thực tế của mạng, mặc dù cái sau bị ảnh hưởng mạnh bởi cái trước. Tuy vậy, trong một phạm vi nào đó, dịch vụ mức mạng có thể che những mặt ít được chú ý của mạng và cung cấp ghép nối tốt hơn. Để tiện lợi xem xét các thủ tục giao vận, ta chia các dịch vụ trên mạng thành 3 nhóm :

| Nhóm | Ý nghĩa |
|---|---|
| ***Nhóm A*** | - Hoàn thiện, tỷ lệ các gói tin bị mất, trùng lặp hoặc bị hỏng không đáng kể.<br>- Lệnh N-RESET có thể bỏ qua.<br>- Tầng giao vận đơn giản, không cần các dịch vụ phục hồi và sắp xếp lại thứ tự gói tin.<br>- Thường là mạng cục bộ. |
| ***Nhóm B*** | - Gói tin bị mất, nhưng kiểm soát được.<br>- Thỉnh thoảng tầng mạng gởi lệnh N-RESET do tắc nghẽn, hỏng phần cứng, vấn đề phần mềm.<br>- Thông thường là mạng đường dài<br>• Giao thức tầng Giao vận có nhiệm vụ:<br>- Thiết lập tại liên kết. Đồng bộ lại<br>- Theo dõi toàn bộ yêu cầu khởi động lại cho NSD. |
| ***Nhóm C*** | - Truyền tin không tin cậy, không liên kết<br>- Mạng đường dài, kết nối nhiều mạng con<br>- Giao thức của tầng giao vận phức tạp, phải có khả năng phục hồi lỗi khi xảy ra sự cố và sắp xếp lại thứ tự các gói tin. |

Bảng 6-1. Các nhóm dịch vụ của tầng Giao vận.

Dịch vụ mạng xấu thì giao thức của tầng giao vận sẽ phức tạp hơn. OSI đã nhận thức vấn đề này và chia giao thức của tầng giao vận thành 5 lớp ứng với các loại mạng như sau :

| Lớp | Ý nghĩa |
|---|---|
| *Lớp O*<br>*Mạng loại A* | - Lớp thủ tục đơn giản<br>- Kết nối mạng khi có yêu cầu giao vận không phải giải quyết lỗi<br>- Chủ yếu tạo ra trình tự, điều khiển dòng dữ liệu để tầng mạng hoạt động tốt.<br>- Bao gồm cơ cấu thiết lập và huỷ liên kết ở tầng giao diện. |
| *Lớp 1*<br>*Mạng loại B* | Có tính chất tương tự lớp 0, ngoài ra còn thêm:<br>- Khởi động lại mạng sau khi N-RESET. Giao thức có khả năng báo nhận (ACK) và truyền dữ liệu khẩn.<br>- Đồng bộ lại và sau đó nối lại liên lạc giữa các thực thể giao vận đã bị gián đoạn<br>- Lớp 1 không kiểm tra lỗi và kiểm soát dòng dữ liệu. |
| *Lớp 2*<br>*Mạng loại A* | Lớp 2 là phiên bản của lớp 0 và được xây dựng cho mạng tin cậy và có thêm một số chức năng như sau :<br>- Sự ghép kênh : Hai hay nhiều liên kết của tầng giao vận có thể dùng chung một kết nối ở tầng mạng.<br>- Sử dụng khi nhiều liên kết ở tầng giao vận được mở đồng thời, nối liên kết có lưu lượng nhỏ.<br>Ví dụ như hệ thống đặt vé máy bay cho phép tiết kiệm đường truyền. |
| *Lớp 3*<br>*Mạng loại B* | Là tổ hợp lớp 1 và lớp 2<br>- Cho phép dồn kênh<br>- Khởi động lại<br>- Điều khiển dòng dữ liệu. |
| *Lớp 4*<br>*Mạng loại C* | Lớp 4 có hầu hết các chức năng của lớp trước và bổ sung thêm một số khả năng kiểm soát luồng dữ liệu.<br>- Phải có biện pháp giải quyết vấn đề mất gói tin, gói tin bị hỏng<br>- Phải giải quyết yêu cầu khởi động lại<br>- Thủ tục Giao vận phức tạp nhất. |

Bảng 6-2. Các lớp dịch vụ của tầng Giao vận.

Dịch vụ không có kết nối đặt tất cả sự phức tạp và thủ tục Giao vận.

### 6.1.4 Thủ tục giao vận trên X. 25

Thủ tục X. 25 là thủ tục có nối và tin cậy, coi như lớp mạng loại A. Do đó thủ tục giao vận trên X.25 là thủ tục giao vận lớp 0 mô hình OSI. Thủ tục này được thể hiện qua các hàm dịch vụ cơ bản và quá trình nối, tách, trao đổi số liệu của thủ tục.

#### *6.1.4.1 Các hàm dịch vụ cơ bản*

Các hàm dịch vụ cơ bản được thực hiện bằng các chương trình con minh họa bằng ngôn ngữ Pascal

1. Hàm Connect thực hiện T-CONNECT .request

   connum = CONNECT(local, remote)

Hàm dịch vụ này để thiết lập kết nối tầng giao vận giữa 2 máy. Nếu kết nối thành công, hàm trả về một số dương, ngược lại hàm trả về số âm.

2. Hàm Listen thực hiện T-CONNECT.indication

   connum = LISTEN (local)

Hàm này dùng để thông báo tiếp nhận yêu cầu kết nối

3. Hàm Disconnect thực hiiện T-DISCONNECT.request

   status = DISCONNECT (commun)

Hàm này dùng để kết thúc kết nối, tham số commun cho biết kết nối nào sẽ bị ngắt, kết quả thực hiện sẽ được gán cho biến status với giá trị OK hoặc error

4. Hàm Send thực hiện T-DATA.request

   status = SEND (commun, buffer, bytes)

Hàm này để phát nội dung ở buffer với kích thước là bytes cho số kết nối đặt ở commun. Kết quả đặt ở status.

5. Hàm Receive thực hiện T-DATA.indication

   status = RECEIVE (commun buffer, bytes)

Hàm này để nhận tin vào buffer với kích thước là giá trị ở biến bytes. Kết quả thực hiện đặt vào status giá trị OK hoặc error.

*Chương 7*

# HỌ GIAO THỨC TCP/IP

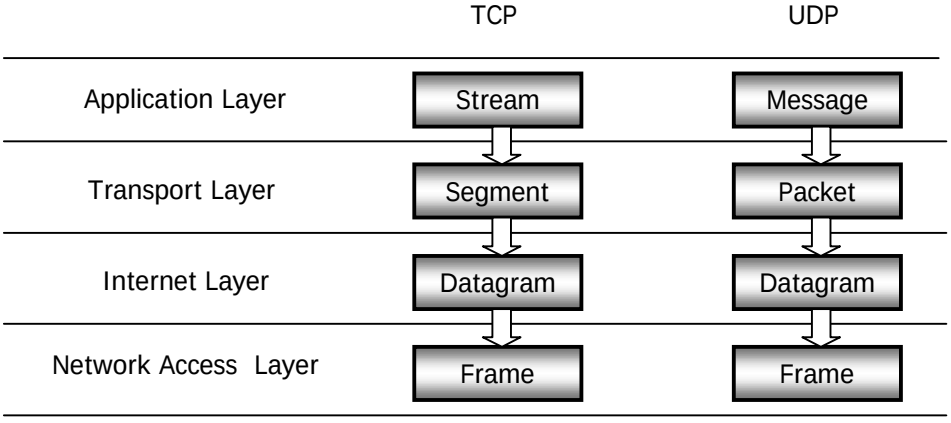
Do đặc tính của mô hình OSI là một mô hình tham chiếu, việc áp dụng mô hình OSI vào thực tế thường có hiệu suất kém do dữ liệu phải truyền qua tất cả các lớp của mô hình OSI ở cả hai máy, mô hình OSI là tiêu chuẩn để các nhà phát triển dựa vào mà phát triển các mô hình khác tối ưu hơn. Có rất nhiều mô hình khác nhau như NetBIOS, IPX/SPX, TCP/IP, tuy nhiên mô hình TCP/IP hiện nay đang được sử dụng phổ biến nhất.

TCP/IP thực chất là một họ giao thức cùng làm việc với nhau để cung cấp ptn truyền thông liên mạng. Mô hình TCP/IP có những tính chất chung như sau :

- TCP /IP độc lập với phần cứng mạng vật lý, điều này cho phép TCP/IP hoạt động trên nhiều mạng khác nhau như Ethernet, Token Ring, X25, dial up,...
- TCP/IP sử dụng sơ đồ đánh địa chỉ toàn cục duy nhất : mỗi máy tính trên mạng TCP/IP có một địa chỉ xác định duy nhất. Mỗi gói tin gởi trên mạng có một tiêu đề chứa địa chỉ nguồn và đích.
- Chuẩn giao thức mở : TCP/IP có thể thực hiện trên bất kỳ phần chứng hay hệ điều hành nào.
- Hoạt động theo mô hình Client/Server.
- Cung cấp các giao thức ứng dụng : cung cấp cho người lập trình phương thức truyền dữ liệu trên mạng giữa các ứng dụng mà còn cung cấp nhiều giao thức ở mức ứng dụng như giao thức truyền nhận mail, truyền file, . . .
- TCP/IP hỗ trợ cho liên mạng (internetworking) và định tuyến, các giao thức mức cao được chuẩn hoá thích hợp và cung cấp sẵn các dịch vụ người dùng.

## 7.1 Mô hình TCP/IP

Cấu trúc của bộ giao thức TCP/IP có bốn tầng, được mô tả như hình vẽ sau




Hình 7-1. Kiến trúc TCP/IP và các đơn vị dữ liệu.

Chức năng của các tầng như sau :

***1. Tầng truy cập mạng NAL (Network Access Layer)***

- Cung cấp cho hệ thống phương thức để truyền dữ liệu trên các thiết bị phần cứng vật lý khác nhau của mạng.
- Đóng gói các lược đồ dữ liệu IP (IP datagram) vào các *frame* truyền trên mạng và việc ánh xạ các địa chỉ IP thành các địa chỉ vật lý tương ứng dùng cho mạng trước khi truyền xuống kênh vật lý.
- Định nghĩa cách thức truyền các khối dữ liệu IP : Các giao thức ở lớp này phải biết chi tiết các phần cấu trúc vật lý mạng ở dưới nó để định dạng chính xác các dữ liệu sẽ được truyền phụ thuộc vào từng loại mạng vật lý cụ thể.

Lớp truy cập mạng NAL của mô hình kiến trúc TCP/IP tương đương với ba lớp thấp nhất của mô hình OSI là Network layer, Datalink layer, và Physical layer.

***2. Tầng mạng***

Tầng mạng chịu trách nhiệm định tuyến các thông báo (message) qua các mạng vật lý khác nhau, liên mạng, giao thức ở lớp này là IP là giao thức quan trọng nhất vì IP cung cấp dịch vụ giao nhận gói tin cơ bản trên các mạng TCP/IP, mọi giao thức ở các lớp trên và bên dưới tầng mạng đều sử dụng giao thức IP để thực hiện việc giao nhận dữ liệu. Hơn nữa IP bổ sung một hệ thống địa chỉ logic được gọi là địa chỉ IP, được sử dụng bởi lớp Internet và các lớp cao hơn để nhận diện các thiết bị và thực hiện định tuyến liên mạng.

***3. Tầng Giao vận (Host to Host Transport Layer)***

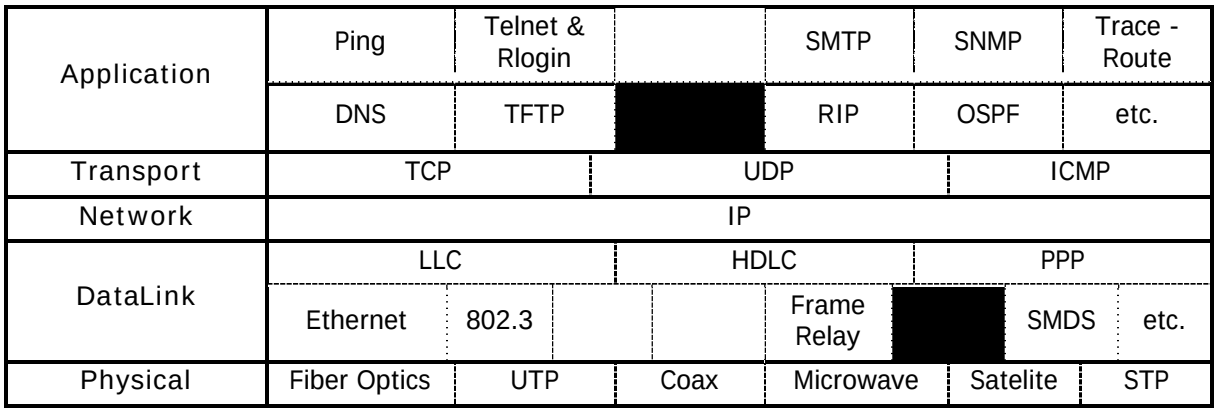
- Cung cấp phương tiện liên lạc từ một chương trình ứng dụng này đến chương trình ứng dụng khác, chịu trách nhiệm đảm bảo toàn vẹn dữ liệu đầu cuối.
- Trong lớp này có 2 giao thức quan trọng nhất:

- Transmission Control Protocol (TCP) : Về chức năng TCP tương đương với lớp giao thức đầy đủ nhất của giao thức chuẩn Transport của OSI. Tuy nhiên, khác với mô hình ISO, TCP sử dụng phương thức trao đổi các dòng dữ liệu (data stream ) giữa người sử dụng.
- User Datagram Protocol (UDP) : cung cấp dịch vụ giao nhận dữ liệu theo kiểu “không liên kết” (connectionless), không cần phải thực hiện thiết lập liên kết logic giữa một cặp thực thể UDP trước khi chúng trao đổi dữ liệu với nhau.

***4. Tầng ứng dụng (Application Layer)***

Bao gồm tất cả các tiến trình sử dụng các giao thức của lớp Transport để truyền dữ liệu. Có nhiều giao thức ứng dụng ở lớp này, phần lớn là nhằm cung cấp cho người dùng các dịch vụ ứng dụng, sử dụng 2 giao thức chính TCP và UDP.

Tầng ứng dụng cung cấp các dịch vụ trên Internet như thư điện tử (SMTP), truyền file (FTP), v.v.. Tầng dưới là phần mạng để định tuyến địa chỉ đến.




Hình 7-2. Họ giao thức TCP/IP.

| | | |
|---|---|---|
| Telnet | Tele Comunication | Dịch vụ truy cập từ xa. |
| FTP | File Transfer Protocol | Dịch vụ truyền File. |
| SMTP | Simple Mail Transfer Protocol | Dịch vụ truyền thư đơn giản. |
| DNS | Domain Name System | Hệ thống tên miền |
| SNMP | Simple Network Management Protocol | Giao thức quản lý mạng đơn giản |
| RPC | Remote Procedure Call | Thủ tục gọi từ xa |
| RIP | Routing Information Protocol | Giao thức định tuyến thông tin |
| TCP | Transmission Control Protocol | Giao thức TCP |
| UDP | User Datagram Protocol | Giao thức dữ liệu của người dùng. |
| IP | Internet Protocol | Giao thức IP |
| ICMP | Internet Control Message Protocol | G.thức kiểm soát message giữa các mạng. |
| FDDI | Fiber Distributed Data Multiplexing | |

## 7.2 Giao thức TCP

Tầng Giao vận sử dụng hai giao thức chính là TCP và UDP. Giao thức TCP (Transmission Control Protocol) đảm bảo độ tin cậy giữa nơi gởi và nơi nhận (end-to-end) trong điều kiện lớp mạng loại C không tin cậy. Dòng số liệu có chiều dài tuỳ ý được phân thành những đoạn không vượt quá 64KB, gửi đi đến đầu bên kia lại được gộp lại thành bản tin ban đầu.

- Chức năng của giao thức TCP :

| Chức năng | Giải thích |
|---|---|
| Phát hiện lỗi | Bằng cách sử dụng một trường checksum để kiểm tra lỗi bất cứ khi nào datagram được cắt ra trong quá trình truyền. |
| Truyền lại | TCP sẽ truyền lại các gói tin bị mất hoặc bị sai hỏng trong quá trình truyền. |
| Đánh số thứ tự | Cho phép bên gởi đã phát đi các gói tin theo một trật tự, bên nhận đã nhận và kết hợp các gói tin theo một trật tự đã định |
| Báo nhận và kiểm soát luồng | Bên TCP nhận sẽ gửi một đoạn báo nhận xác định một số chức năng trong quá trình truyền tin. |
| Phát gói tin đến đúng ứng dụng yêu cầu | Mỗi đoạn gói tin TCP có một số hiệu cổng nguồn và đích, là giá trị duy nhất để xác định một phiên làm việc. |

- Tính chất của giao thức TCP :

| Tính chất | Giải thích |
|---|---|
| Tin cậy | TCP cung cấp khả năng tin cậy bằng cách gởi lại dữ liệu đến khi bên nhận có một báo nhận hỏng. Đơn vị dữ liệu mà TCP truyền đi là segment và được giao thức IP phân ra thành các datagram. |
| Hướng kết nối | TCP thiết lập kết nối logic giữa các máy khi truyền dữ liệu, hoạt động theo cơ chế "bắt tay" (handshake), và có nhiệm vụ đồng bộ việc kết nối giữa hai máy. |
| Dòng dữ liệu | TCP xử lý dữ liệu dưới dạng một dòng nối tiếp các byte, theo cơ chế đánh số thứ tự gói tin. |

### 7.2.1 Khuôn dạng gói tin TCP

TCP là một giao thức có liên kết (*connection - oriented*) nghĩa là cần phải thiết lập liên kết logic giữa một cặp thực thể TCP trước khi chúng trao đổi dữ liệu với nhau, có 3 giai đoạn : ***thiết lập liên kết, truyền tải dữ liệu*** và ***hủy liên kết***. Đơn vị dữ liệu của TCP được gọi là **segment** (đoạn dữ liệu). Cấu trúc đơn vị dữ liệu của TCP được mô tả như hình sau :

*Source Port - Số hiệu cổng nguồn (16 bits)*

Xác định số hiệu cổng của trạm nguồn - User TCP cục bộ (thường là một chương trình ứng dụng trên lớp cao hơn).

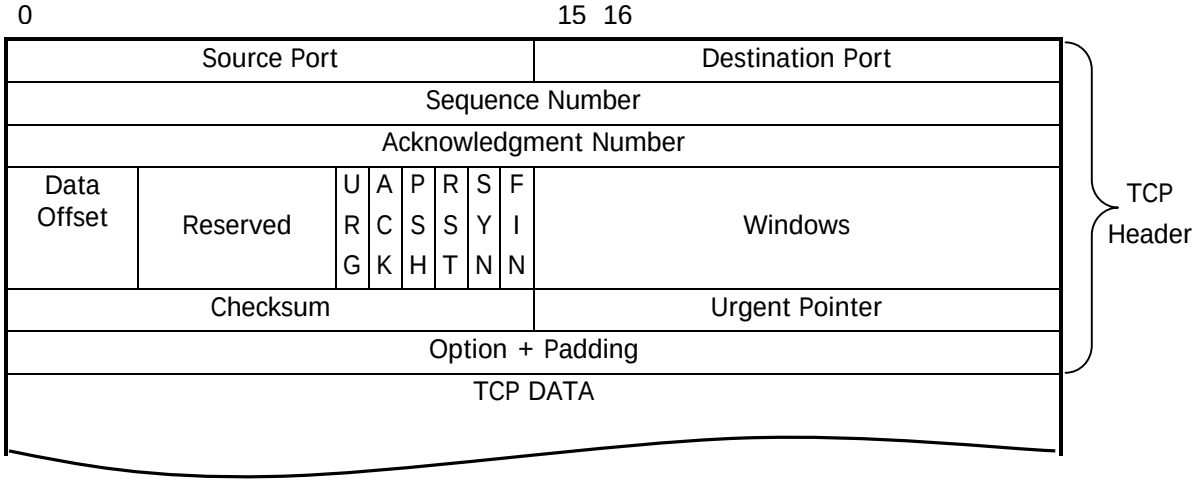
*Destination Port - Số hiệu cổng đích (16 bits)*

Xác định số hiệu cổng của trạm đích của máy ở xa. Dùng để nhận diện các tiến trình điểm đầu mút ở kênh ảo TCP.

*Sequence Number - Số thứ thự (32 bits)*

Trường này chứa một số chỉ vị trí hiện tại của khối tin trong Message. Số này cũng được các phiên bản khác nhau của TCP để cung cấp số thứ tự của khối tin ban đầu (ISN).

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




Hình 7-3. Cấu trúc của gói tin TCP.

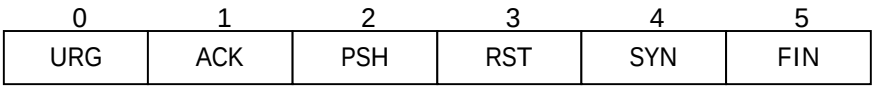
*Acknowledgment Number - Số phúc đáp (32 bits)*

Dùng để chỉ ra số hiệu của segment (khối tin) sắp được truyền tiếp theo mà trạm đích đang chờ để nhận. Dùng báo nhận tốt các Segment mà trạm nguồn đã gửi cho trạm đích. Ngoài ra nó cũng chỉ ra số thứ tự của khối tin nhận được sau cùng; nó chỉ ra số thứ tự của khối tin nhận được cộng thêm 1.

*Data offset (32 bits) :* Trường này dùng để chỉ ra vị trí bắt đầu của trường dữ liệu.

*Reserved (6 bits) :* Chưa dùng đến, dành sử dụng về sau. Các bit được đặt bằng 0.

*Control Bits* - Các bit điều khiển




Cờ URG : Nếu có giá trị là 1 thì thì trường urgent pointer rất quan trọng.
Cờ ACK : Nếu có giá trị là 1 thì trường Acknowledgment rất quan trọng.
Cờ PSH : Nếu thiết lập thì tức là chức năng PUSH sắp được thực hiện.
Cờ RST : Nếu được thiết lập thì kết nối hiện tại sắp được khởi tạo lại.
Cờ SYN : Chỉ ra số thứ tự của đoạn tin sẽ được đồng bộ hoá. Cờ này được dùng khi mà kết nối được thiết lập.
Cờ FIN : Nếu cờ này thiết lập, nó chỉ ra rằng phía gửi không còn dữ liệu để gửi nữa. Điều này tương đương với việc đánh dấu kết thúc quá trình truyền.

*Window - Cửa sổ (16 bits)*

Trường này cấp phát thẻ dùng để kiểm soát luồng dữ liệu theo cơ chế cửa sổ. Đây là số lượng các byte dữ liệu khối tin mà phía thu có thể chấp nhận được.

*Checksum (16 bits)*

Chứa mã kiểm soát lỗi (theo phương pháp CRC) cho toàn bộ segment.

*Urgent Pointer - Con trỏ khẩn (16 bits)*

Trường này được dùng khi mà cờ URG được thiết lập; con trỏ này trỏ tới số hiệu tuần tự của các byte đi theo sau dữ liệu khẩn, cho phép bên nhận biết được độ dài của dữ liệu khẩn.

*Options (có độ dài thay đổi)*

Trường này dùng để xác định các Option của TCP. Mỗi lựa chọn bao gồm một số (1 byte) để chỉ ra lựa chọn đó, một số chỉ giá trị của các byte trong trường Option, và các giá trị lựa chọn. Hiện nay với TCP mới có 3 Option được định nghĩa, như sau:

Số 0 : Cuối danh sách các lựa chọn
Số 1 : Không hoạt động (*No Operation*)
Số 2 : Kích cỡ lớn nhất của một Segment

Trường Options chỉ để xác định kích thước lớn nhất của bộ đệm mà TCP nhận có thể chấp nhận được. Bởi vì TCP dùng trường dữ liệu có chiều dài thay đổi được nên có thể có trường hợp là máy gửi sẽ tạo ra một đoạn tin mà phía nhận không thể chấp nhận được.

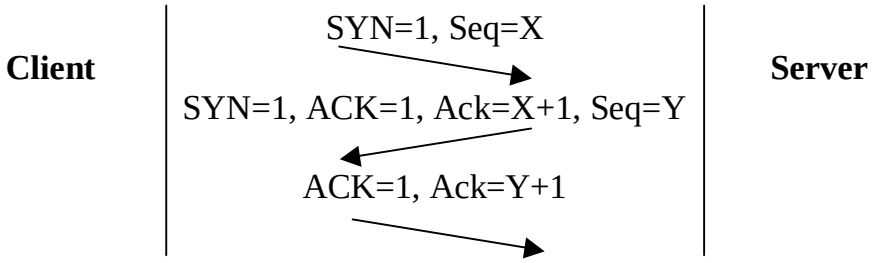
*Padding :*

Dùng để bổ sung vào Header để bảo đảm rằng phần Header luôn là bội số của 32 bit. Phần thêm vào bao gồm toàn số 0.

*TCP Data (Có độ dài thay đổi)*

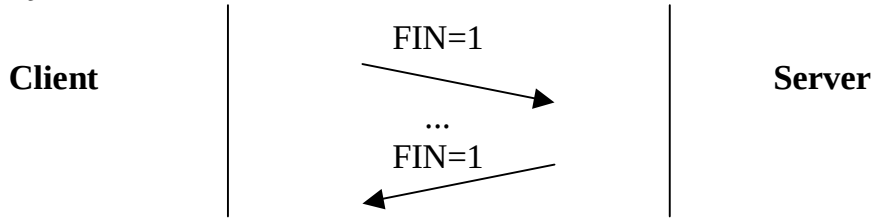
Chứa dữ liệu của tầng trên, độ dài tối đa ngầm định là 536 bytes. Giá trị có thể điều chỉnh bằng cách khai báo trong vùng Options.

### 7.2.2 Quá trình nối-tách



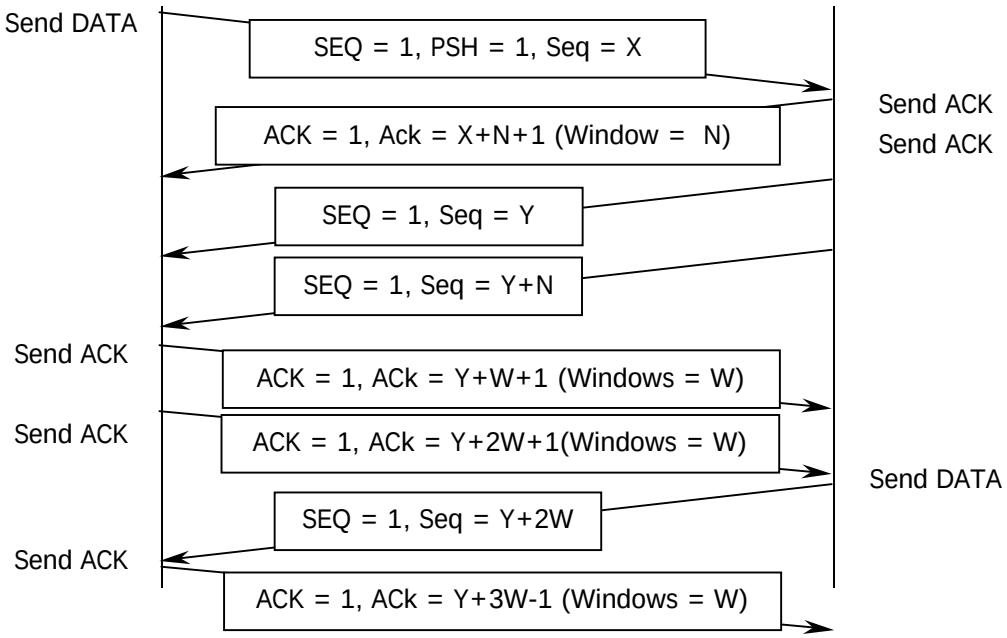
Quá trình thiết lập kết nối bằng thủ tục bắt tay 3 lần (three-way hand). Client gửi bản tin với SYN=1 (yêu cầu kết nối). Server nhận được, gửi bản tin với SYN=1 và ACK=1. Client lại đáp lại với bản tin ACK=1.

Kết thúc kết nối bằng thủ tục bắt tay hai lần (two-way hand). Bên kết thúc gởi số liệu, gởi bản tin với FIN=1, TCP cho phép nhận tiếp tục số liệu cho đến khi bên kia gửi bản tin FIN=1




Ngoài ra, thủ tục TCP/IP còn dùng để kết nối giữa LAN và WAN như một thủ tục cho mạng LAN.

### 7.2.3 Quá trình trao đổi dữ liệu




H×nh 7-4. S¬ ®å qu¸ tr×nh trao ®æi d÷ liÖu cña TCP.

W= maximun Segment size (W>N)

2W = Windows limit

### 7.2.4 Thứ tự thực hiện ứng dụng TCP/IP

Sự kết hợp của thủ tục TCP và IP thực sự là sự kết hợp giữa các mạng máy tính nối với nhau cho phép người dùng các mạng máy tính nối với nhau cho phép người dùng các mạng khác nhau liên lạc và làm việc được với nhau.

Thủ tục TCP là thủ tục tại đầu cuối, còn IP dùng để chạy trên mạng. Khi người sử dụng thủ tục TCP tạo được phân đoạn TCP và kết hợp vào IP để tạo thành IP datagram. Router căn cứ vào địa chỉ IP trong gói tin và thông tin chứa trong bảng định tuyến để chuyển gói này đi tới các router sau. Khi gói tin IP đến router cuối cùng, router này tìm và chuyển gói tin đến địa chỉ hệ thống đầu cuối.

Nếu IP datagram không chuyển tới đầu cuối được vì một lý do nào đó, nó sẽ bị hủy bỏ và giao thức IP không còn thông báo được điều này cho người sử dụng biết. Giao thức TCP cung cấp mối liên hệ tin cậy giữa các đầu cuối, đảm bảo dữ liệu phát đi đúng địa chỉ, không bị thiếu hay phát lặp nghĩa là tại điểm cuối cùng thủ tục TCP sẽ đọc số thứ tự trong phân đoạn TCP để biết gói tin bị thiếu hay gói đã nhận rồi và báo lại cho bên phát biết.

Gói tin IP không phụ thuộc vào các giao thức cụ thể của các mạng khác nhau mà nó đi qua (X.25 hay Frame relay v.v..). Với IP các mạng chỉ đơn thuần là đường dẫn các Router. Ta có thể hình dung IP datagram như một phong bì bình thường, người gửi thư không quan tâm đến bức thư đến được người nhận bằng ô tô, tàu hỏa hay máy bay.

Sự kết hợp giữa thủ tục TCP và IP giúp người dùng sử dụng được các dịch vụ trao đổi trên Internet thực hiện qua các bước chính sau đây:

**Bước 1:** Các dữ liệu ứng dụng kết hợp với số thứ tự để hình thành phân đoạn TCP.

Người sử dụng dùng dịch vụ trên mạng như thư điện tử, Telnet hay FTP v.v.. có nghĩa là đưa các dữ liệu của người dùng vào phần dữ liệu của gói tin TCP. Giao thức TCP sẽ đưa vào phần header của gói tin các thông tin sau:

- Số hiệu cổng quy định của Internet.
- Số thứ tự Segment gửi đi.
- Thông báo cho bên gửi biết đã nhận được Segment thứ mấy (ACK)
- Số byte cần phát.

**Bước 2:** Kiến tạo ra gói tin IP datagram

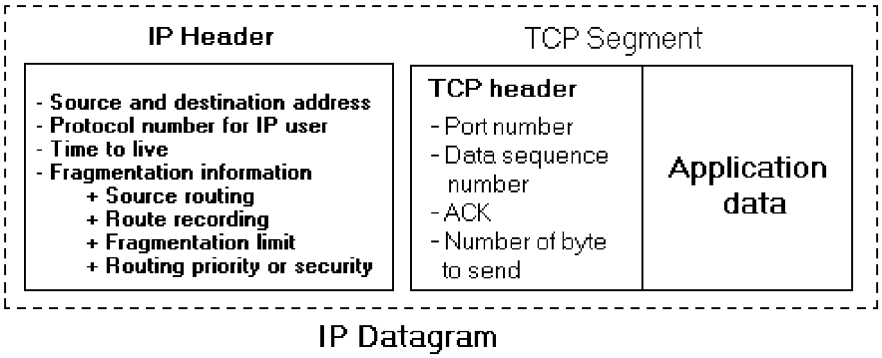
Trên cơ sở của gói tin TCP, IP thêm các thông tin sau đây vào để tạo thành IP Datagram.

- Địa chỉ phát và nhận : Router sử dụng địa chỉ này để định tuyến.
- Số thủ tục (Protocol number): định nghĩa thủ tục mà IP thực hiện.
- Thời gian tồn tại (Time to live): định nghĩa số Router bắt buộc Datagram phải đi qua trước khi nó bị hủy bỏ.
- Thông tin về các phân đoạn bị chia nhỏ trong quá trình chuyển đi trên mạng.

Kích thước gói tin thay đổi tùy thuộc vào mạng khác nhau, chẳng hạn như kích thước gói tin trong mạng Ethernet là 1500 bytes còn mạng X.25 chỉ có 128 bytes.

- Các thông tin tùy chọn

- Source Routing (Định tuyến bên phát): cung cấp danh sách các Router sử dụng.
- Route recording (Ghi lại tuyến đường đã đi qua): Thông tin sẽ yêu cầu mỗi Router ghi lại địa chỉ IP khi nó chuyển datagram qua, dùng để thống kê được số liệu của đường dẫn trong Internet.
- Fragmentation limit (Giới hạn phân mảnh): Định nghĩa cỡ lớn nhất (tính theo byte) của một datagram có thể chuyển đi mà không cần phải chia nhỏ.
- Routing priority or security (Ưu tiên hoặc bảo đảm an toàn cho Datagram): chỉ rõ tuyến nào dành ưu tiên hay tuyến nào bảo đảm được an toàn cho datagram.




Hình 7-5. Cấu trúc của IP Datagram.

Như vậy Datagram thực chất là hình thức một gói tin chứa dữ liệu thông tin được dùng trong internet.

**Bước 4:** Chuyển gói đến địa chỉ đích

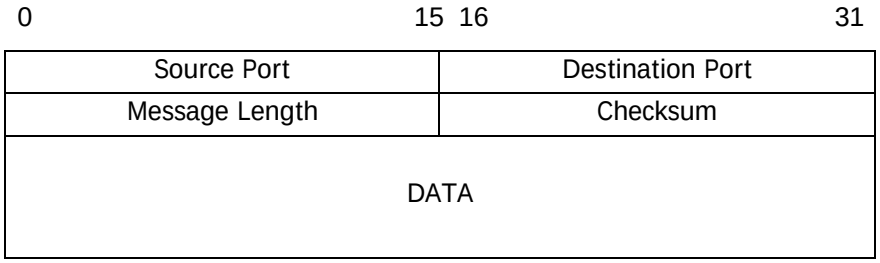
Các IP Datagram chuyển qua các lớp dưới đưa vào và định tuyến để tìm tới địa chỉ đến qua mạng căn cứ vào địa chỉ vật lý của mạng lưới ví dụ như địa chỉ mạng X.25, mạng Frame relay hoặc ngay bản thân của Internet. Tất cả các thông tin này đều nằm trong bảng định tuyến trong các Router. Các mạng X.25 hay Frame relay chỉ làm nhiệm vụ chuyển tải các Datagram.

Tại phía đầu cuối thu, TCP tách IP datagram để lấy phân đoạn TCP xử lý dữ liệu thông tin, đối chiếu số thứ tự, phát hiện những gói thiếu thiếu hay đã nhận được, đồng thời cũng nhận được thông báo (ACK) từ phía phát báo cho biết bên đấy đã nhận được gói thứ mấy do bên này phát đi.

Phía thu thông báo (ACK) cho bên phát biết số dữ liệu đã nhận được đồng thời cũng yêu cầu phát lại những gói tin thiếu nếu có.

## 7.3 Giao thức UDP

Giao thức UDP (User Datagram Protocol) cho phép người sử dụng gởi bản tin mà không cần thiết lập liên kết, do đó không bảo đảm việc giao nhận chính xác hoặc thứ tự bản tin. Giao thức UDP dùng cho dịch vụ không tin cậy 100%. Thực tế trong các mạng 99% bản tin UDP được giao nhận đúng đích. Do ít chức năng phức tạp nên UDP hoạt động nhanh hơn so với TCP.




Hình 7-6. Khuôn dạng của UDP Datagram.

Các trường có ý nghĩa như sau:

- *Source Port* - Số hiệu cổng nguồn (của máy gửi): Một trường có thể lựa chọn được với số hiệu cổng. Nếu một số hiệu cổng không xác định thì trường này có giá trị là 0.
- *Destination Port* - Số hiệu cổng trên máy nhận.
- *Message Length* - Chiều dài của dữ liệu trong đó cả phần Header và dũ liệu.
- *Trường Checksum*: là 16 bit bù một của phép tổng bù một của trường dữ liệu, có cả phần pseudoHeader giống như của TCP.

Trường checksum của UDP cũng có thể lựa chọn được, nhưng không được dùng. Không một checksum nào được dùng cho phần dữ liệu vì phần checksum của IP chỉ dùng cho phần Header IP mà thôi. Nếu phần checksum không được dùng thì các bit của trường này được thiết lập là 0.

Giao thức UDP được sử dụng trong một số tình huống đặc biệt :

- Khi truyền một dữ liệu nhỏ thì dùng UDP có hiệu quả hơn so với việc kết nối và hủy kết nối khi sử dụng TCP.
- Các ứng dụng hỏi đáp, mong muốn trả lời trong một thời gian ngắn sau khi người sử dụng gởi đi yêu cầu. Trả lời cũng là một cơ chế báo nhận. Người ta sử dụng giao thức UDP như trong các dịch vụ ứng dụng không yêu cầu độ chính xác cao như thông báo giờ hay các dịch vụ gởi nhắn tin, tỷ giá .. .

- Một số mô hình nén để truyền các thông tin audio, video, có thể chấp nhận được một vài gói dữ liệu bị hỏng hay thất lạc.
- Một vài ứng dụng có đô tin cậy riêng trong khi truyền dữ liệu thì nên dùng UDP hơn là TCP.

## 7.4 Cổng và Socket

### 7.4.1 Số hiệu cổng

Khi một máy khách kết nối vào máy chủ thì có thể yêu cầu nhiều dịch vụ khác nhau trên máy chủ. Mỗi dịch vụ đều có cách gởi và nhận dữ liệu theo quy ước riêng. TCP và UDP chỉ chịu trách nhiệm đưa dữ liệu từ một máy tính náy đến một máy tính khác, còn dữ liệu đó được gởi đến dịch vụ theo cách nào thì phải thông qua cổng của dịch vụ.

Cổng được đặc trưng bởi một số có giá trị từ 0 đến 65535. Các cổng chuẩn từ 0 - 1023 là cổng được dùng cho các dịch vụ phổ biến như FTP, eMAIL, POP3, HTTP, ... Không thể có hai tiến trình cùng sử dụng chung một số hiệu cổng.

Các số hiệu cổng (Port Numbers) được dùng thông dụng trong thực tế :

| UDP Port | | TCP Port | |
|---|---|---|---|
| 0 | Reversed | 0 | Reversed |
| 7 | Echo | 1 | TCP Multiplexor |
| 37 | Time | 20 | FTP_ Data Connection |
| 42 | Name Server | 21 | FTP_ Command Connection |
| 53 | Domain Name Server | 23 | TELNET |
| 69 | Trivial File Transfer Program ( TFTP ) | 25 | SMTP |
| 514 | System Log | 42 | Name Server |
| . . . . . | | 53 | Domain Name Server |
| | | 79 | Finger_ find a active user |
| | | 80 | HTTP |

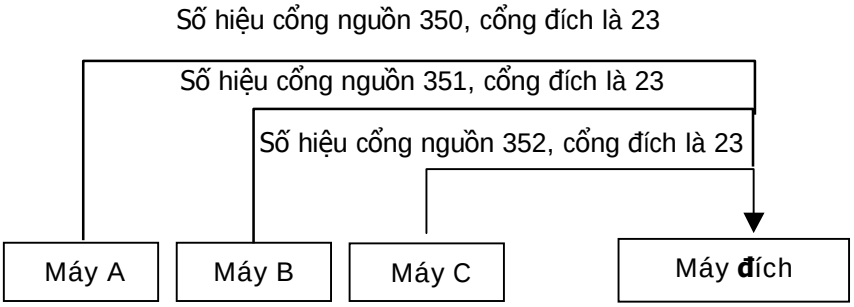
### 7.4.2 Socket

Mỗi socket xác định một điểm cuối trong liên kết truyền thông hai chiều giữa các tiến trình giao tiếp trên mạng, là đối tượng mà qua đó các dịch vụ ứng dụng truyền hoặc nhận các gói dữ liệu trên mạng. Khi cần gởi dữ liệu đi, các tiến trình ghi dữ liệu vào socket, khi có dữ liệu đến, các tiến trình sẽ đọc socket để lấy dữ liệu.

Trong những năm 80, do nhu cầu cần có một giao diện lập trình ứng dụng API (Application Programming Interface) để phát triển các trình ứng dụng trên mạng TCP/IP, giao diện socket đã được xây dựng lần đầu tiên trên hệ điều hành UNIX. Loại Berkelay Socket (Berkeley Software Distribution - BSD, tại Trường Đại học

- Loại socket : Stream socket hoặc Datagram socket.

Một liên kết giữa hai máy trên với nhau được xác định bởi một cặp socket : Socket (Host1, Port1) và Socket (Host2, Port2). Số **Socket** là duy nhất cho phép một tiến trình có thể giao tiếp với một tiến trình khác trên mạng.




Hình 7-7. Nhiều máy nguồn nối với một máy đích.

Một liên kết có thể được thiết lập theo một trong hai cách : chủ động (active) hoặc bị động. Các thực thể tầng trên sử dụng TCP thông qua bằng cách gọi các hàm dịch vụ nguyên thủy. Dịch vụ TCP được thiết lập nhờ một liên kết logic giữa một cặp Socket. Một Socket có thể tham gia nhiều liên kết với các Socket ở xa khác nhau. Vì các khung tin được đưa qua cổng đều có đầy đủ các thông tin về socket (với địa chỉ IP), cho nên không có xung đột dữ liệu xảy ra.

## 7.5 Mô hình giao tiếp Client/Server

TCP/IP phụ thuộc vào khái niệm máy khách (Client) và máy chủ (Server). Thuật ngữ Server dùng để chỉ những chương trình cung cấp các dịch vụ thông qua mạng. Các Server nhận đảm nhiệm chức năng đáp ứng các yêu cầu của máy khách, thực hiện việc phục vụ và trả lại kết quả. Thuật ngữ Client dùng để chỉ các chương trình ứng dụng gởi các yêu cầu đến Server và chờ kết quả trả về.

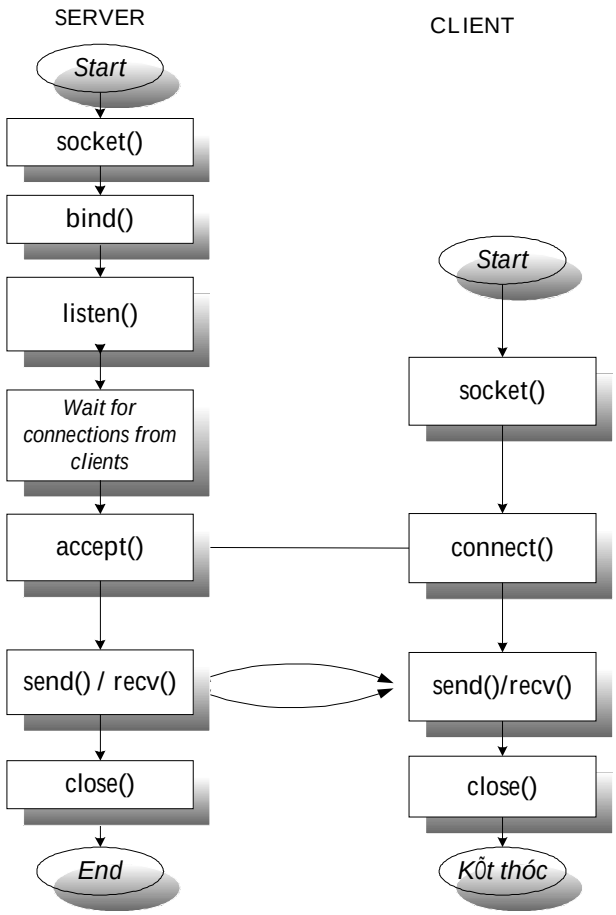
Các chương trình Client và Server thường thực thi trên các máy khác nhau. Mỗi chương trình Server có thể cùng đáp ứng cho nhiều chương trình Client trên nhiều máy tính khác nhau cùng một lúc.

### 7.5.1 Quá trình trao đổi dữ liệu dùng Stream Socket

Stream socket dựa trên nền giao thức TCP đòi hỏi phải tạo một kết nối trước khi hai bên có thể truyền hoặc nhận dữ liệu cho nhau. Stream Socket cung cấp một dòng các byte dữ liệu không có phân cách có thể truyền hai chiều. Các dòng dữ liệu có thể tin cậy được phân phát tuần tự, dữ liệu không trùng lắp, nghĩa là các gói dữ liệu được phân phát theo thứ tự được phát, và mỗi lần chỉ có một gói riêng biệt được truyền.

Dạng socket này rất thích hợp với mô hình Client/Server. Server sẽ tạo một socket, gán cho nó một tên (cung cấp một địa IP của máy và một port để giao tiếp), và đợi client nối kết đến socket. Bên client cũng tạo một socket và nối kết đến tên socket trên server. Khi server phát hiện có yêu cầu kết nối từ client, nó sẽ tạo một socket mới và sử dụng socket mới đó để giao tiếp với client. Socket cũ tiếp tục đợi kết nối từ các client khác.

Sơ đồ trao đổi dữ liệu giữa Client/Server bằng cách dùng Socket được biểu diễn như sau :



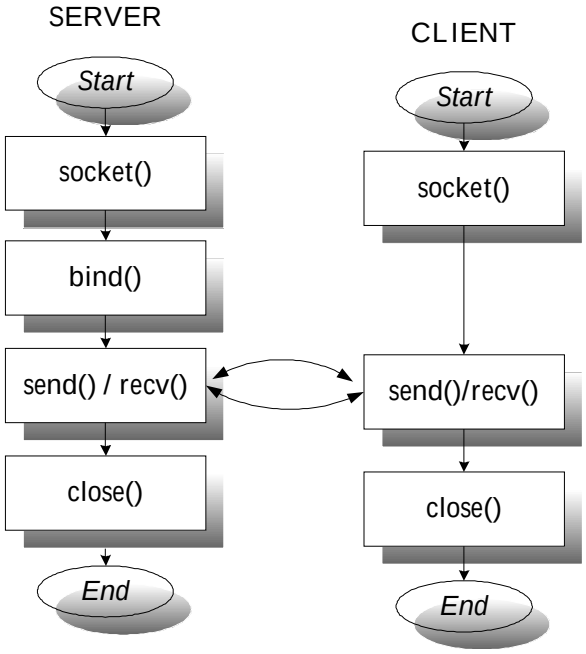

Hình 7-8. Sơ đồ trao đổi dữ liệu giữa Client/Server bằng StreamSocket.

### 7.5.2 Quá trình trao đổi dữ liệu dùng Datagram Socket

Datagram Socket dựa trên giao thức UDP không đòi hỏi phải thiết lập một kết nối trước khi truyền và nhận dữ liệu. Dữ liệu chỉ là một gói đơn, vì vậy dạng socket này thường dùng để truyền các mẫu tin, không cần nhiều các header lớp ứng dụng. Dạng socket này cung cấp luồng dữ liệu không bảo đảm theo thứ tự hoặc không bị trùng lắp, không bảo đảm dữ liệu sẽ đến được nơi nhận. Dữ liệu có thể đến không theo thứ tự được phát và có khả năng bị trùng lặp. Nhưng sự phân cách giữa các

mẫu tin thì được duy trì. Trong mạng LAN datagram có khả năng tin cậy tương đối tốt, nhưng trong mạng WAN, như mạng Internet thì không được đảm bảo.

§ Lưu đồ client/server sử dụng giao thức UDP




Hình 7-9. Sơ đồ trao đổi dữ liệu giữa Client/Server bằng DatagramSocket.

### 7.5.3 Ví dụ chương trình client/server

Trong ví dụ dưới đây chương trình server thực hiện các bước thiết lập cho việc chờ đợi một kết nối từ chương trình client. Sau khi thiết lập kết nối với client, cả hai thực hiện một số thao tác truyền và nhận thông tin rồi kết thúc chương trình.

#### *7.5.3.1 Mã lệnh chương trình Server*

- Tạo ra một socket với hàm *socket()*.
- Ràng buộc socket với một địa chỉ bằng hàm *bind ()*.
- Dùng hàm *listen()* để chờ đợi một kết nối.
- Nhận bất kỳ thông tin nào yêu cầu kết nối bằng hàm *accept()*.
- Nhận các thông báo gửi đến bằng hàm *read()* và gửi thông báo đến client bằng hàm *write()*.
-

```
/* mksock.c make and bind to a socket - userver*/
#include<stdio.h>
#include<sys/socket.h>
#include<sys/un.h>
#include<unistd.h>

void die(char * message);
void copyData(int from, int to);
```

```
int main(void) {
  struct sockaddr_un address;
  int sock,conn;
  size_t addrLength;
  if ((sock=socket(PF_UNIX,SOCK_STREAM,0))<0)
   die("socket");
/*unlik("./sample_socket");*/
  address.sun_family=AF_UNIX;
  strcpy(address.sun_path,"./sample_socket");

addrLength=sizeof(address.sun_family)+strlen(address.sun_path);
if(bind(sock,(struct sockaddr *)&address,addrLength))
  die("bind");
if(listen(sock,5))
  die("listen");
while((conn=accept(sock,(struct sockaddr*)&address,&addrLength))>=0) {
  printf("---getting data\n");
  copyData(conn,1);
  printf("---done\n");
  close(conn);
}
if (conn<0) die("accept");
close(sock);
return 0;
}
void die(char * message){
  perror(message);
  exit(1);
}
void copyData(int from,int to){
  char buf[1024];
  int amount;
  while ((amount=read(from,buf,sizeof(buf)))>0){
          if(write(to,buf,amount)!=amount){
                  die ("write");
                  return;
  }
}
if (amount<0) die("read");
}
```

### *7.5.3.2 Mã lệnh chương trình client*

Từ chương trình client , để thực hiện được một kết nối đến server và truyền nhận thông tin chỉ cần thực hiện 2 bước cơ bản như sau:

- Tạo một *socket()* tương ứng với chương trình *server* cụ thể .
- Yêu cầu đến server thực hiện kết nối bằng cách gọi hàm *connect()*.

Nếu một kết nối được tạo ra, client có thể gửi yêu cầu bằng hàm *write()* và nhận các đáp ứng phản hồi bằng hàm *read()*.

```
/* sockconn.c - connect to a socket - uclient*/
#include<sys/socket.h>
#include<sys/un.h>
#include<unistd.h>

void die (char * message);
```

```
void copyData(int from, int to);

int main(void){
  struct sockaddr_un address;
  int sock;
  size_t addrLength;

  if ((sock=socket(PF_UNIX,SOCK_STREAM,0))<0)        die("socket");
  address.sun_family=AF_UNIX;
  strcpy(address.sun_path,"./sample_socket");

  addrLength=sizeof (address.sun_family) + strlen(address.sun_path);
  if(connect(sock,(struct sockaddr *)& address,addrLength))   die("connect");
  copyData(0,sock);
  close(sock);
  return 0;
}
void die(char * message){
  perror(message);
  exit(1);
}
void copyData(int from, int to){
  char buf[1024];
  int amount;
  while ((amount=read(from,buf,sizeof(buf)))>0){
    if(write(to,buf,amount)!=amount) {
                    die("write");
                    return;
    }
  }
if (amount<0)      die("read");
}
```

---

# BÀI TẬP

1. Tìm hiểu các mô tả Socket và cấu trúc dữ liệu của socket mà hệ điều hành cấp phát để lưu trữ các thông tin cần thiết cho kết nối mạng.
2. Tìm hiểu các thư viện lập trình WinSock trên hệ điều hành Windows.
3. Viết các chương trình giao tiếp Client/Server theo mô hình giao tiếp TCP/IP hoặc UDP/IP.

*Chương 8*

# TẦNG PHIÊN

Tầng phiên (Session Layer) làm nhiệm vụ tổ chức và đồng bộ sự chuyển đổi dữ liệu giữa các tiến trình ứng dụng khác nhau. Tầng Phiên làm việc với tầng ứng dụng để cung cấp các tập dữ liệu, được gọi là các điểm đồng bộ, các điểm này cho phép một ứng dụng biết quá trình truyền và nhận dữ liệu được thực hiện như thế nào.

Tầng phiên chịu trách nhiệm thiết lập và duy trì một phiên truyền thông giữa hai trạm hoặc nút mạng. Một phiên truyền thông qua một mạng hoạt động có phần giống với một cuộc gọi qua các đường dây điện thoại. Tầng Phiên cố gắng thiết lập một phiên truyền thông giữa hai nút trên một mạng. Cả hai nút đều thừa nhận phiên truyền thông này thường sẽ được gán một số hiệu nhận diện. Mỗi nút có thể ngắt phiên truyền thông giữa hai nút trên một mạng được gọi là *một cổng luận lý* (Socket). Khi một phiên truyền thông được thiết lập, một cổng luận lý sẽ được mở ra. Một phiên truyền thông được kết thúc được gọi là *một cổng luận lý bị đóng* (Close Socket).

Mục tiêu của tầng phiên là có khả năng cung cấp cho người sử dụng các chức năng cần thiết để quản lý các phiên ứng dụng cụ thể như:

- Điều phối việc trao đổi dữ liệu giữa các ứng dụng bằng cách thiết lập và giải phóng (một cách ***logic***) các phiên (hay gọi là các hội thoại ***dialogues***).
- Cung cấp các điểm đồng bộ hóa để kiểm soát việc trao đổi dữ liệu.
- áp đặt các qui tắc cho các tương tác giữa các ứng dụng của người sử dụng.
- Cung cấp cơ chế lấy lượt (nắm quyền) trong các quá trình trao đổi dữ liệu.

Trong tầng phiên thì vấn đề đồng bộ hóa được thực hiện tương tự như một cơ chế kiểm tra / phục hồi (*check point/reset*).Trong một hệ quản trị tập tin, dịch vụ này cho phép người sử dụng xác định các điểm đồng bộ hóa trong dòng dữ liệu và có thể khôi phục lại việc hội thoại bắt đầu từ một trong các điểm đó.

## 8.1 Dịch vụ OSI cho tầng Phiên

Tầng phiên làm việc quản lý các cuộc thoại giữa hai máy tính bằng cách thiết lặp, quản lý, và kết thúc các phiên truyền thông.

### 8.1.1 Cung cấp cho người sử dụng dịch vụ tầng phiên (SS-user)

- Thiết lập một liên kết với một người sử dụng dịch vụ tầng phiên khác, trao đổi dữ liệu với người sử dụng đó một cách đồng bộ và hủy bỏ liên kết một cách có trật tự khi không dùng đến nữa.

- Thương lượng về việc dùng các thẻ bài (TOKEN) để trao đổi dữ liệu,đồng bộ hóa và hủy bỏ liên kết ,sắp xếp phương thức trao đổi dữ liệu (half-duplex hoặc full-duplex).
- Thiết lập các điểm đồng bộ hóa trong các hội thoại và khi xảy ra sự cố thì có thể khôi phục lại việc hội thoại bắt đầu từ một điểm đồng bộ hóa đã thỏa thuận.
- Ngắt hội thoại và khôi phục lại hội thoại sau đó từ một điểm xác định trước.

Các dịch vụ xác định điểm đồng bộ hóa là nhằm vào hai mục đích :

1) Các điểm đồng bộ hóa có thể phân tách các phần của một hội thoại.
2) Các điểm đồng bộ hóa có thể dùng để phục hồi lỗi.

*Các điểm đồng bộ hóa chính* dùng để cấu trúc quá trình trao đổi dữ liệu thành một chuỗi các đơn vị hội thoại (dialogue), mỗi điểm này phải được xác nhận và người sử dụng sẽ bị hạn chế trong một số dịch vụ nhất định cho tới khi nhận được một sự xác nhận mới. Một điểm đồng bộ hóa chính được dùng để tách biệt các hai đơn vị hội thoại liên tiếp.

*Các điểm đồng bộ hóa phụ* được dùng để cấu trúc quá trình trao đổi dữ liệu ở trong một đơn vị hội thoại, và các điểm này không cần phải được xác định trước.Việc dùng các điểm đồng hóa phụ trong quá trình truyền tập nó sẽ ngăn chặn việc truyền lại dữ liệu với một khối lượng lớn

*Một đơn vị hội thoại* là một Activity (hành động) nguyên tử trong đó mọi hành động truyền thông không có liên quan gì đến bất kỳ một hoạt động truyền thông nào trước và sau đó. Một hành động bao gồm nhiều đơn vị hội thoại, và đây cũng chính là một tập hợp logic các nhiệm vụ liên quan với nhau; ở một thời điểm thì chỉ có một activity trên một liên kết phiên nhưng một activity thì có thể diễn ra trên nhiều liên kết phiên, nó có thể bị ngắt và sau đó có thể khôi phục lại trong một liên kết phiên khác, một vòng đời của một liên kết phiên thì có thể có nhiều Activity liên tiếp.

### 8.1.2 Điều khiển trao đổi dữ liệu

Việc trao đổi dữ liệu xảy như sau để thực hiện một trong ba phương thức như sau : hai chiều đồng thời (*full-duplex*), hai chiều luân phiên (*haft -duplex*), một chiều (*simplex*).

#### *8.1.2.1 Trao đổi dữ liệu một chiều*

Liên quan đến các đợt chuyển giao dữ liệu một chiều. Báo cháy là một ví dụ, nó gửi một thông điệp báo động đến trạm chống cháy, nhưng không thể (và không cần) nhận các thông điệp từ trạm chống cháy.

Với phương thức một chiều thì ít xảy ra: chẳng hạn như dữ liệu được gửi đến một đối tượng tạm thời không làm việc, thì chỉ có một chương trình nhận với một nhiệm vụ duy nhất là tiếp nhận dữ liệu đến và giữ lại.

#### *8.1.2.2 Trao đổi dữ liệu hai chiều luân phiên*

Liên quan đến các đợt chuyển giao dữ liệu hai chiều, ở đó các luồng dữ liệu mỗi lần đi theo mỗi hướng. Khi một thiết bị hoàn tất một phiên truyền, nó phải " trả lại " vật tải cho thiết bị kia để đến phiên thiết bị đó được truyền.

Với phương thức luân phiên hai chiều thì nảy sinh các vấn đề như sau :

- Các đối tượng sử dụng phiên phải “lấy lượt” để truyền dữ liệu (điển hình của phương thức này là dùng cho các ứng dụng hỏi đáp).
- Thực thể tầng phiên *(session entity)* duy trì tương tác luân phiên bằng cách báo cho các đối tượng khi đến lược họ sẽ truyền dữ liệu.

#### *8.1.2.3 Trao đổi dữ liệu hai chiều đồng thời.*

Cho phép tiến hành các đợt chuyển giao dữ liệu hai chiều đồng thời bằng cách cung cấp cho mỗi thiết bị một kênh truyền thông riêng biệt. Điện thoại tiếng là những thiết bị song công đầy đủ, và một trong hai bên của một cuộc đàm thoại có thể nói bất kỳ lúc nào. Hầu hết các môđem máy tính đều có thể hoạt động theo chế độ song công đầy đủ.

Chế độ truyền thông bán song công có thể dẫn đến tình trạng băng thông bị lãng phí trong quãng thời gian mà đợt truyền thông đang quay trả. Trong khi đó, chế độ truyền thông song công đầy đủ thường yêu cầu một ban thông lớn hơn so với chế độ truyền thông bán song công

Với phương thức hai chiều đồng thời thì cả hai bên cùng đồng thời gửi dữ liệu cùng một lúc, một khi phương thức này đã được thỏa thuận thì không đòi hỏi phải có nhiệm vụ quản trị tương tác đặt biệt đây cũng là một phương thức phổ biến nhất.

### 8.1.3 Điều hành phiên làm việc

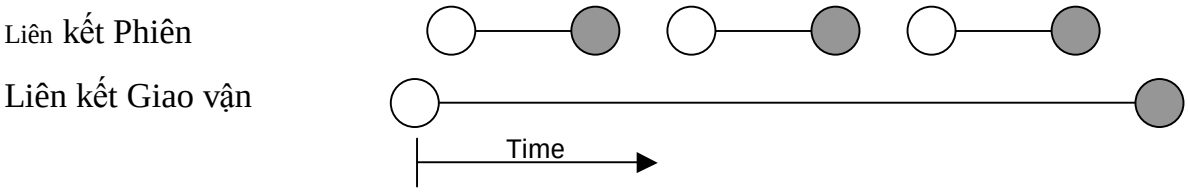
Phiên làm việc (session) là một cuộc thoại chính thức giữa một bên yêu cầu dich vụ và một bên cung cấp dịch vụ. Các phiên bản làm việc thường có ít nhất ba giai đoạn :

- *Thiết lập tuyến liên kết :* Bên yêu cầu dịch vụ sẽ yêu cầu khởi phát một dịch vụ. Trong quá trình xác lập, phiên truyền thông được thiết lập và các quy tắc được thoả thuận.
- *Chuyển giao dữ liệu* : Do các quy tắc được thoả thuận trong khi xác lập, nên mỗi bên của cuộc thoại sẽ biết nội dung mong đợi. Phiên truyền thông sẽ hữu hiệu và các lỗi cũng dễ phát hiện.
- *Giải phóng các kết nối* : Khi hoàn tất phiên làm việc, cuộc thoại kết thúc trong trật tự.

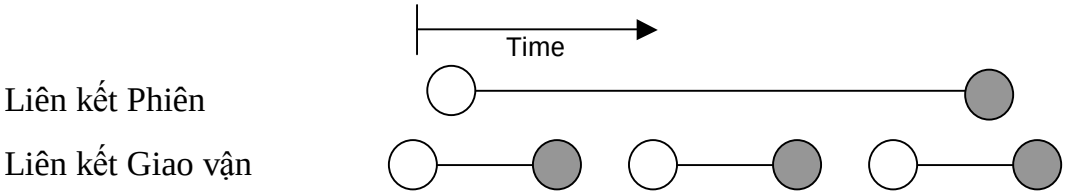
### 8.1.4 Liên kết phiên

Tầng Phiên thực hiện đặt tương ứng liên kết phiên với các liên kết giao vận. Trong một quá trình liên kết có thể xảy ra 2 trường hợp :

1. Một liên kết giao vận thiết lập với nhiều liên kết phiên liên tiếp :




2. Nhiều liên kết giao vận sử dụng cùng một liên kết phi[a]n:




Ký hiệu : : Thiết lập liên kết

: Giải phóng liên kết

## 8.2 Giao thức chuẩn tầng phiên

Giao thức chuẩn tầng phiên sử dụng tới 34 loại đơn vị dữ liệu (SPDU) khác nhau,và có khuôn dạng tổng quát như sau :


Trong đó :

- SI: Định danh của loại SPDU (một trong 34 loại)

- LI(length indicator): Chỉ độ dài của vùng tham số(parameters)
- PARAMETERS: vùng khai báo các tham số SPDU, mỗi loại SPDU có danh sách tham số riêng. Mỗi tham số được khai báo dưới dạng tổng quát gồm 3 vùng con : parameter identifier, length indecation, parameter value và chúng được gọi theo đơn vị pi hoặc PGI (mỗi đơn vị PGI gồm có 3 vùng con: PGI, LENGTH INDICATION, PARAMETER VALUE).
- User data: chứa dữ liệu của người sử dụng.

### 8.2.1 Các loại SPDU, các tham số và chức năng

| SPDU | PARAMENTERS | FUNCTION |
|---|---|---|
| CONNECT | Connection ID, Protocol Options, Version Number, Serial Number, Token setting, Maximum TSDU size, Requirements, Calling SSAP, Called SSAP, User Data. | Initiate session Connection |
| ACCEPT | Same as CONNECT SPDU. | Etablist SESSION CONNECTION |
| REFUSE | Connection ID, Transport disconnect, Requirements, Version number, Season. | Reject connection request |
| FINISH | Transport Disconnect, User Data. | Initiate Orderly Release |
| DISC0NNECT | User Data. | Acknowledge orderly Release |
| NOT FINISHED | User Data. | Reject Orderly Release |
| ABORT | Transport disconnect, Protocol Error Code, User Data. | Abnormal connection Release |
| ABORT ACCEPT | Transport disconnect, Protocol Error Code, User Data. | Acknowledge Abort |
| DATA TRANSFER | Enclosure item,User Data. | Transfer normal Data |
| EXPEDITED | User data. | Transfer typed data |
| CAPABILITY DATA ACK | User Data. | Acknowledge Capability data |
| GIVE TOKENS | Tokens. | Transfer tokens |
| PLEASE TOKENS | Tokens , User Data. | Request token Assignment |
| GIVE TOKENS CONFIRM | - | Transfer all tokens |
| GIVE TOKENS ACK | - | Acknowledge all tokens |
| MONOR SYNC POINT | Confirm required flag, Serial number, User data. | Define minor sync point |
| MINOR SYNC ACK | Serial number, User Data. | Acknowledge minor sync point |
| MAJOR SYNC POINT | End of activity flag, Serial number, User Data. | Define major sync point |
| MAJOR SYNC ACK | Serial number,User data. | Acknowledge major sync point |
| RESYNCHRONIZED | Tokens sittings, resync type, serial number, user data. | Resynchorize |
| RESYNCHRONIZED ACK | Tokens settings, Serial number, User Data. | Acknowledge resynchronize |

| | | |
|---|---|---|
| PREPERE | Type. | Notify type SPDU is coming |
| EXCEPTION REDORT | SPDU bit pattem. | Protocol Error detected |
| EXCEPTION DATA | Reason, User Data. | Put protocol in Error state |
| ACTIVITY START | Activity ID, User data. | Signal beginning of activity |
| ACTIVITY RESUME | Connect ID, Old activity ID, New Activity ID, User data. | Signal resumption of activity |
| ACTIVITY INTERRUPT | Reason. | Interrupt activity |
| ACTIVITY INTERRUPT ACK | - | Acknowledge interrupt |
| ACTIVITY DISCARD | Reason. | Cancel activity |
| ACTIVITY DISCARD ACK | - | Acknowledge cancellation |
| ACTIVITY END | Serial number/User data. | Signal activity end |
| ACTIVITY END ACK | Serial number/User data. | Acknowledge activity end |

Tầng Phiên đóng một vai trò quan trọng trong việc trao đổi thông tin giữa các máy Client với máy Server. Nhưng thông tin mà chúng ta cần truyền tải thì được chia nhỏ ra thành các khung (hay gói) trước khi chúng được truyền tải qua một mạng. Mỗi tầng của mô hình 7 tầng OSI đều có thể bổ sung thêm các thông tin vào đoạn đầu và đoạn cuối của một khung dữ liệu vvà sau đó các thông tin này sẽ được đọc bởi tầng tương đương ở máy trạm tiếp nhận. Và một số tầng khác có thể bổ sung thêm phần đầu(header) và cả một phần đuôi(trailer) vào khung dữ liệu có sẵn. Sau đó, khung dữ liệu này truyền chuyển tới tầng tương đương trên trạm tiếp nhận.

*Chương 9*

# TẦNG TRÌNH DIỄN

Tầng Trình diễn có nhiệm vụ phân cách giữa các tầng cao hơn và các tầng thấp hơn từ định dạng dữ liệu của tầng ứng dụng, chuyển đổi định dạng dữ liệu từ định dạng của tầng ứng dụng thành định dạng thông thường, gọi là "trình diễn hợp với quy tắc". Tầng Trình diễn xử lý dữ liệu không phụ thuộc vào máy tính từ tầng ứng dụng thành dữ liệu có định dạng phụ thuộc vào máy tính để chuyển cho các tầng thấp hơn.

Tầng trình diễn xử lý cú pháp, hoặc các quy tắc văn phạm, cần thiết cho phiên truyền thông giữa hai máy tính, bảo đảm cho các hệ thống cuối truyền th6ng có kết quả khi chúng sử dụng các dạng biểu diễn dữ liệu khác nhau. Tầng này trình bày một dạng thức dữ liệu đồng dạng cho tầng ứng dụng.

## 9.1 Vai trò và chức năng

Mục đích của tầng trình diễn là đảm bảo cho các hệ thống cuối có thể truyền thông có kết quả ngay cả khi chúng sử dụng các biểu diễn dữ liệu khác nhau .Để đạt được điều đó nó cung cấp một biểu diễn chung để dùng trong truyền thông và cho phép chuyển đổi từ biểu diễn cục bộ sang biểu diễn chung đó.

Tồn tại 3 dạng cú pháp thông tin được trao đổi giữa các thực thể ứng dụng :

- Cú pháp dùng bởi thực thể ứng dụng nguồn.
- Cú pháp dùng bởi thực thể ứng dụng đích.
- Cú pháp dùng bởi giữa các thực thể trình diễn ,loại cú pháp này gọi là cú pháp truyền (transfer syntax).

Tầng trình diễn đảm nhận việc chuyển đổi biểu diễn thông tin giữa cú pháp truyền và mỗi một cú pháp kia khi có yêu cầu

Chú ý rằng không tồn tại một cú pháp truyền xác định trước duy nhất cho mọi hoạt động trao đổi dữ liệu. Cú pháp truyền được duy nhất cho mọi hoạt động trao đổi dữ liệu. Cú pháp truyền được sử dụng trên một liên kết cụ thể của tầng trình diễn phải được thương lượng giữa các thực thể trình diễn tương ứng. Mỗi bên lựa chọn một cú pháp truyền sao cho có thể sẵn sàng được chuyển đổi sang cú pháp người sử dụng và ngược lại. Ngoài ra cú pháp truyền được chọn phải phản ánh các yêu cầu dịch vụ khác chẳng hạn nhu cầu nén dữ liệu .việc thương lượng cú pháp truyền sử dụng có thể được thay đổi trong vòng đời liên kết đó .Tầng trình diễn chỉ liên quan đến cú pháp truyền vì thế trong giao thức sẽ không quan tâm đến các cú pháp sử dụng bởi thực thể ứng dụng. Tuy nhiên mỗi thực thể trình diễn phải chịu trách nhiệm chuyển đổi giữa cú pháp người sử dụng và cú pháp truyền.

Các khái niệm liên quan đến bối cảnh của tầng trình diễn : Khi qua ranh giới giữa hai tầng trình diễn và tầng phiên có một sự thay đổi quan trọng trong cách nhìn dữ liệu. Đối với tầng phiên trở xuống tham số User Data trong các service primitives được đặc tả dưới dạng nhị phân (một chuỗi các byte). Giá trị này có thể được đưa vào trực tiếp trong các SDU (Service Data Unit) để chuyển giữa các tầng trong một hệ thống và trong các PDU (Protocol Data Unit) để chuyển giữa các tầng đồng mức ở hệ thống kết nối với nhau. Tuy nhiên tầng ứng dụng lại liên quan chặt chẽ với cách nhìn dữ liệu của người sử dụng nói chung cách nhìn đó là một tập thông tin có cấu trúc nào đó như là văn bản (text) trong một tài liệu một tệp về nhân sự hoặc một cơ sở dữ liệu .... Người sử dụng chỉ quan tâm đến ngữ nghĩa (semantics) của dữ liệu. Do đó tầng trình diễn ở giữa chỉ có nhiệm vụ cung cấp phương thức biểu diễn dữ liệu và chuyển đổi thành các giá trị nhị phân dùng cho các tầng dưới nghĩa là tất cả những gì liên quan đến cú pháp của dữ liệu

Tuy nhiên trong thực tế không thể tách bạch hoàn toàn giữa cú pháp và ngữ nghĩa và ngữ nghĩa dữ liệu. Nếu tầng ứng dụng không biết gì về cú pháp thì tầng trình diễn không biết gì về nhữ nghĩa thì không thể nào hoàn tất được việc kết hợp ngữ nghĩa với cú pháp dùng để tạo ra một biểu diễn cụ thể các giá trị dữ liệu cho dịch vụ phiên.

ở tầng ứng dụng thông tin được biểu diễn dưới dạng cú pháp trừu tượng (abstract syntax) liên quan đến các kiểu dữ liệu (data values) cú pháp trừu tượng này đặc tả một cách nhìn hình thức dữ liệu độc lập với mọi biểu diễn cụ thể.

Do vậy một cú pháp trừu tượng có nhiều đặc điểm giống kiểu dữ liệu như các ngôn ngữ lập trình Pascal, C .... Các ngữ nghĩa như là BNF. Các giao thức tầng ứng dụng mô tả các PDU của chúng bằng một cú pháp trừu tượng. Tầng trình diễn tương tác với tầng ứng dụng cũng dựa trên cú pháp trừu tượng này, tầng trình diễn có nhiệm vụ dịch thuật cú pháp trừu tượng của tầng ứng dụng và cú pháp truyền (transfer syntax) mô tả các giá trị dữ liệu dưới dạng nhị phân thích hợp cho việc tương tác với dịch vụ phiên việc dịch thuật này được thực hiện nhờ qui tắc mã hoá chỉ rõ biểu diễn của mỗi giá trị dữ liệu thuộc một kiểu nào đó .

Trước khi sử dụng liên kết của một tầng trình diễn để trao đổi dữ liệu thì hai thực thể trình diễn ở hai đầu phải thoả thuận về cú pháp truyền được xem như là bối cảnh trình diễn (presentation context) được dùng để trao đổi dữ liệu

Cú pháp truyền phải yểm trợ cú pháp trừu tượng tương ứng. Ngoài ra cú pháp truyền có thể có các thuộc tính khác không liên quan gì đến cú pháp trừu tượng mà nó yểm trợ ví dụ một cú pháp trừu tượng có thể yểm trợ bởi bất kì một cú pháp truyền về cơ bản thì giống nhau chỉ khác nhau ở chỗ một cung cấp khả năng mật mã, một chỗ cung cấp cả hai và một không cung cấp khả năng nào.

### 9.1.1 Phiên dịch dữ liệu

Một mục tiêu quan trọng cần giải quyết khi thiết kế các mạng đó là cho phép kiểu máy tính khác nhau trao đổi dữ liệu. Tuy mục tiêu này ít khi được giải quyết toàn vẹn, nhưng việc vận dụng hiệu quả các kỹ thuật phiên dịch dữ liệu có thể giúp nhiều kiểu máy tính truyền thông với nhau. Có bốn dạng phiên dịch dữ liệu, thứ tự bít, thứ tự byte, mã ký tự, và cú pháp tập tin như sau :

- Thứ tự bit : Khi số nhị phân được truyền qua một mạng, chúng gởi đi theo từng bit, thứ tự byte, mã ký tự, và cú pháp tập tin.
- Phiên dịch thứ tự Byte : Các giá trị phức tạp thường phải được biểu thị bằng nhiều byte, nhưng các máy tính khác nhau thường dùng quy ước khác nhau về việc sẽ truyền byte nào trước. Các bộ vi xử lý Intel bắt đầu bằng byte ít quan trọng nhất. Do chúng bắt đầu tại đầu nhỏ, nên được gọi là kết đầu nhỏ. Các bộ vi xử lý Motorola bắt đầu bằng byte quan trọng nhất. Để hoà hợp những khác biệt này, ta cần phải có tính năng phiên dịch thứ tự byte.
- Phiên dịch mã ký tự : Hầu hết các máy tính đều dùng một trong các bảng mã đánh số nhị phân dưới đây để biểu thị các bộ ký tự : Bảng mã ASCII được dùng để biểu thị các ký tự tiếng Anh trên tất cả máy tính và hầu hết các máy tính mini. EBCDIC (Extended Binary Coded Decimal Interchange Code = Mã hoán đổi thập phân mã hoá nhị phân mở rộng) được dùng để biểu thị cho các ký tự tiếng Anh trên máy tính lớn nhất.
- Phiên dịch cú pháp tập tin : Khi các dạng thức tập tin khác nhau giữa các máy tính, các dạng đó đòi hỏi phải phiên dịch.

## 9.2 Dịch vụ OSI cho tầng trình diễn

Dịch vụ OSI cho tầng trình diễn có 2 loại : một loại bao gồm các dịch vụ liên quan đến biểu diễn của dữ liệu người sử dụng để đảm bảo cho hai thực thể ứng dụng có thể trao đổi dữ liệu thành công ngay khi chúng dùng các biểu diễn cục bộ khác nhau cho dữ liệu đó, loại thứ hai bao gồm các dịch vụ cho phép các thực thể ứng dụng có thể sử dụng các dịch vụ tầng phiên để quản lý hội thoại.

Để cung cấp loại dịch vụ thứ nhất tầng trình diễn thực hiện hai nhiệm vụ sau :

- Thương lượng về cú pháp truyền : với mỗi kiểu dữ liệu người sử dụng cho trước một cú pháp truyền được thương lượng.
- Chuyển đổi : dữ liệu cung cấp bởi người sử dụng được chuyển đổi thành biểu diễn theo cú pháp truyền để truyền đi , ngược lại dữ liệu nhận được để giao cho người sử dụng sẽ chuyển đổi từ biểu diễn theo cú pháp truyền sang biểu diễn của người sử dụng.

ở thời điểm bất kì trong vòng đời của một liên kết trình diễn dịch vụ trình diễn dịch vụ trình diễn có liên quan đến một hoặc nhiều bối cảnh trình diễn (presentation context). Mối bối cảnh chỉ rõ cú pháp trừu tượng của dữ liệu đó. Có hai loại bối cảnh được sử dụng :

- Defined context set : bao gồm các bối cảnh đã được xác định thông qua sự thoả thuận giữa người sử dụng dịch vụ trình diễn (presentation service user) vaf người cung cấp dịch vụ trình diễn (presentation service provider).
- Default context : là một bối cảnh trình diễn mà người cung cấp dịch vụ trình diễn luôn luôn biết rõ và người sử dụng khi vắng mặt

Ở tầng phiên do kiến trúc phân tầng của ISO các thực thể ứng dụng không thể truy cập trực tiếp tới các dịch vụ tầng phiên, do vậy các yêu cầu dịch vụ liên quan đến tầng phiên phải được chuyển qua tầng trình diễn đến các dịch vụ tầng phiên.

## 9.3 Giao thức chuẩn tầng trình diễn

Giao thức chuẩn của ISO/CCITT cho tầng Trình diễn đặc tả những nội dung chính sau đây:

- Cấu trúc và mã hoá các đơn vị dữ liệu của giao thức trình diễn (PPDU) dùng để truyền dữ liệu và thông tin điều khiển .
- Các thủ tục để truyền dữ liệu và thông tin điều khiển giữa các thực thể trình diễn của hai hệ thống mở.
- Liên kết giữa giao thức trình diễn với dịch vụ trình diễn và với dịch vụ phiên .

Cũng như các PDU ở các tầng khác ,các PPDU cũng có khuôn dạng tổng quát bao gồm một phần đầu (header ) chứa các thông tin điều khiển và có thể thêm mmột phần chứa dữ liệu được truyền từ trên xuống hoặc được truyền lên cho tầng trên. Giao thức trình diễn sử dụng 14 PPDU được liệt kê trong bảng 2-17 cùng với các tham số của chúng .

Qua bảng trên ta thấy số lượng PPDU không nhiều như số lượng SPDU (ở tầng Phiên) và nhiều tham số (có đánh dấu *) là giống với các tham số của các SPDU. Như vậy cả về phương diện dịch vụ và giao thức, tầng trình diễn và tầng Phiên có một mối liên kết rất chặt chẽ .

Qua xem xét các tầng dưới từ tầng phiên trở xuống, chúng ta thấy có 2 nguyên lý sau đây luôn được tuân thủ :

- Mỗi dịch vụ tầng n được cài đặt nhờ trao đổi các nPDU;
- Mỗi nPDU trở thành User data và được “nhét” vào trong một (n-1) PDU;

Tuy nhiên ở tầng trình diễn (và cả ở tầng ứng dụng mà ta sẽ thấy), các nguyên lý đó không còn luôn luôn được áp dụng .Thực tế là không phải mọi dịch vụ trình diến đều yêu cầu các PPDU và một số tham số của một số PPDU không được chuyển thành User data trong một SPDU. Để giải thích động cơ củ a sự khác biệt đó, ta xem xét hai dịch vụ trình diễn : thiết lập liên kết (connection etablishment) và chuyển thẻ bài (token passing).

Khi phát triển các giao thức cho 3 tầng cao của Mô hình óI,người ta thấy rõ ràng nên thương lượng và thiết lập đồng thời các liên kết Phiên ,trình diễn và ứng dụng,mặc dù điều đó đòi hỏi một quan hệ 1-1 chặt chẽ (không có dồn kênh) với cùng vòng đời cho cả ba loại liên kết .Quá trình thiết lập đồng thời các liên kết đó được gọi là quá trình nhúng (embeding), vì các PDU CONNECT.request và CONNECT.response cho cả ba tầng cao đó ,cái này được nhúng vào trong cái kia.

Khuôn dạng của các PDDU header được đặc tả theo cú pháp trừu tượng chuẩn.

### 9.3.1 Các chuẩn khác cho tầng trình diễn

Ngoài các chuẩn về dịch vụ và giao thức cho tầng Trình diễn như đã trình bày ở trên, ISO và CCITT đã phát triển các chuẩn liên quan đến cú pháp trừu tượng (Abstract Syntas) và quy tắc mã hoá (Encoding Rules) mà chúng ta đã nói đến khi trình bày vai trò và chức năng của tầng Trình diễn

Các chuẩn của ISO gồm có :

- ISO 8824:Abstract Syntax Notation One(viết tắt là ASNI.1)
- ISO 8825:Báic Encoding Rules(Viết tắt là BER)
- Tương ứng CCITT có các khuyến nghị X208 (ANSI.1) và X.209 (BER).

Khái niệm cú pháp trừu tượng mà ISO và CCITT định nghĩa được dựa trên khái niệm kiểu dữ liệu (data type) mà chúng ta đã quen thuộc trong các ngôn ngữ lập trình phổ biến. Thông thường các ngôn ngữ này định nghĩa trước các kiểu dữ liệu đơn giản như integer và boolean, cùng với các phương thức tổ hợp các kiểu đơn giản đó để có các cấu trúc dữ liệu phức tạp hơn. Hơn nữa, các phương pháp tổ hợp có thể thực hiện một cách đệ quy cho phép tạo ra các kiểu phức tạp tuỳ ý.

*Chương 10*

# TẦNG ỨNG DING

Tầng ứng dụng giao tiếp trực tiếp với người sử dụng. Nhiệm vụ của tầng ứng dụng là hiển thị các thông tin nhận được và gửi các thông tin mới của người sử dụng cho các tầng thấp hơn.

Tầng ứng dụng liên quan đến tiến trình cung cấp các dịch vụ trên mạng, các dịch vụ này bao gồm : dịch vụ tập tin, dịch vụ in, dịch vụ cơ sở dữ liệu, và các dịch vụ khác.

Chúng ta sẽ xem xét các vấn đề trước khi bắt đầu với các ứng dụng. Đó là sự an toàn mạng, dịch vụ tên miền DNS dùng để điều khiển đặt tên trong Internet, giao thức hỗ trợ quản trị mạng, phần còn lại là các ứng dụng thực như thư điện tử, UserNet, FTP, Telnet, WWW ...

## 10.1 An toàn thông tin trên mạng

Việc kết nối mạng máy tính nhằm sử dụng và chia sẻ tài nguyên của các đối tượng trong hệ thống mạng cho dù họ có thể cách xa nhau về mặt địa lý. Tài nguyên hệ thống ở đây chủ yếu là là thông tin. Tuy nhiên đây là loại tài nguyên dễ bị xâm phạm, bị đánh cắp, bị tráo đổi nhất, đặc biệt là nó đang được trong lưu giữ trong môi trường mạng đầy phức tạp và phải chia xẻ cho nhiều người dùng khác nhau ở những vị trí khác nhau.

Vấn đề an toàn thông tin trên mạng đòi hỏi phải sử dụng nhiều biện pháp khác nhau từ cơ bản đến phức tạp, tuỳ theo lượng thông tin cần bảo vệ và khả năng cho phép của từng hệ thống cụ thể.

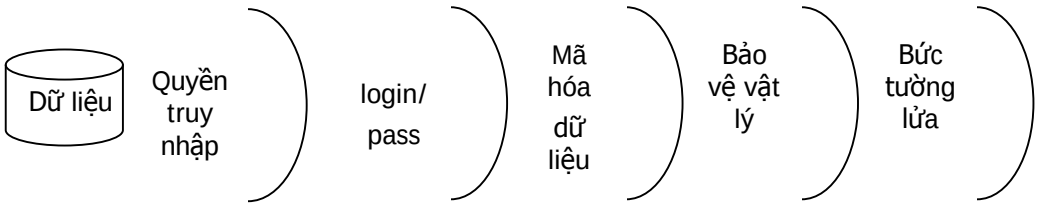
### 10.1.1 Các chiến lược an toàn hệ thống

1. Quyền hạn tối thiểu : Đây là chiến lược nền tảng nhất. Theo nguyên tắc này bất kì đối tượng nào cũng chỉ có những quyền hạn nhất định đối với những tài nguyên mạng nhất định khi thâm nhập vào mạng.
2. Bảo vệ theo chiều sâu : Tạo nhiều cơ chế an toàn cho hệ thống để chúng hỗ trợ cho nhau.
3. Cơ chế nút thắt : Tạo ra một “cửa khẩu” hẹp và chỉ cho phép thông tin đi vào hệ thông của mình bằng duy nhất con đường này. Đồng thời phải tổ chức một cơ chế kiểm soát và điều khiển các luồng thông tin đi qua cửa khẩu này.
4. Tính toàn cục : Các hệ thống an toàn đòi hỏi phải có tính toàn cục của các hệ thống cục bộ. Nếu có kẻ nào đó có thể bẻ gãy một cơ chế an toàn thì chúng có thể thành công bằng cách tấn công hệ thống nội bộ từ bên trong.

5. Tính đa dạng của việc bảo vệ : Cần phải sử dụng nhiều biện pháp khác nhau cho những hệ thống khác nhau. Nếu không, kẻ nào đó tấn công được hệ thống này thì cũng có thể tấn công vào hệ thống khác.

- Các mức bảo vệ thông tin trên mạng:

Vì không có một giải pháp bảo vệ nào an toàn tuyệt đối nên người ta thường sử dụng nhiều mức bảo vệ khác nhau tạo thành nhiều lớp rào chắn cho hệ thống. Mô hình như sau :




Hình 10-1. Các mức bảo vệ thông tin trên mạng.

### 10.1.2 An toàn thông tin bằng mã hóa

Để bảo vệ thông tin trên đường truyền, người ta chuyển đổi nó từ dạng nhận thức được sang dạng không nhận thức được trước khi truyền đi trên mạng nhằm bảo đảm tính bí mật cần thiết. Quá trình này diễn ra ở trạm phát được gọi là mã hoá thông tin (encrypting), ở trạm nhận phải thực hiện quá trình ngược lại, tức là biến đổi thông tin từ dạng không nhận thức được (đã mã hoá) sang dạng nhận thức được (dạng gốc), quá trình này gọi là giải mã (decrypting). Đây là một lớp bảo vệ thông tin rất quan trọng và được ứng dụng trong hầu hết các hệ thống mạng.

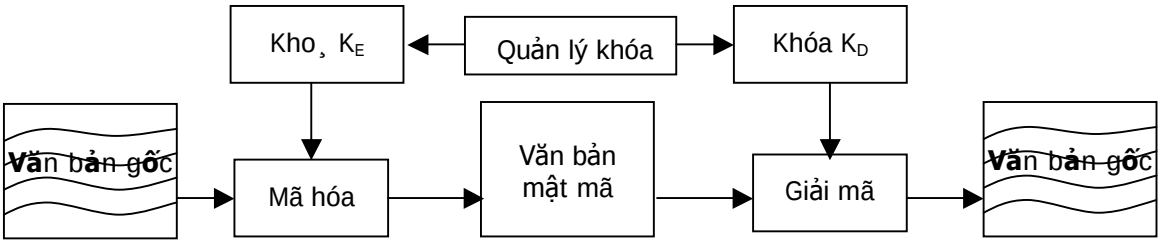
Để bảo vệ thông tin bằng mật mã, người ta thường tiếp cận theo hai hướng:

- Từ nút đến nút (end_to_end )
- Theo đường truyền (link_oriented security)

Theo cách thứ nhất, thông tin được mã hoá để bảo vệ trên đường truyền giữa hai nút mà không quan tâm đến nguồn và đích của thông tin đó. Ớ đây ta chú ý rằng thông tin chỉ được bảo vệ trên đường truyền, tức là ở mỗi nút đều có quá trình giải mã để sau đó thông tin được chuyển đi tiếp, do đó các nút cần được bảo vệ tốt.

Ngược lại theo cách thứ hai, thông tin trên mạng được bảo vệ trên toàn đường truyền từ nguồn đến đích. Thông tin sẽ được mã hoá ngay sau khi mới tạo ra và chỉ được giải mã khi đã về đến đích. Cách này có nhược điểm là chỉ có dữ kiệu người dùng mới được mã hoá còn các thông tin điều khiển thì phải giữ nguyên để có thể xử lí tại các nút.

Quá trình mã hoá và giải mã được mô tả như sau :




Hình 10-2. Sơ đồ quá trình mã hóa.

+ Văn bản gốc (plaintext) là văn bản chưa được mã hoá.

+ Khoá (key) : gồm một số hữu hạn các bit thường được biểu thị dưới dạng các xâu kí tự chữ số, số thập phân hoặc thập lục phân. Trong thực tế thường dùng các khoá có 8 kí tự.

Nếu gọi : M là văn bản gốc

C là văn bản mật mã (Ciphertext)

E là hàm mã hoá (Encryption Function )

D là hàm giải mã (Descryption Function)

Ta có hàm biểu diễn sự phụ thuộc giữa văn bản gốc và văn bản mã như sau:

$C = E(M)$

$M = D(C) = D(E(M))$

Khoá KE được dùng để mã hoá, khoá KD được dùng để giải mã .

Có rất nhiều phương pháp mã hoá nhưng tất cả đều qui về 2 phương pháp chung tuỳ theo việc sử dụng cặp khoá KD và KE:

- Khoá KD trùng với khoá KE : phương pháp này gọi là mã hoá khoá đối xứng, với phương pháp này yêu cầu khoá phải được giữ bí mật tuyệt đối, vì khoá dùng để mã hoá cũng được dùng giải mã.
- Khoá KD khác với khoá KE : phương pháp này gọi là mã hoá khoá công khai. Trong đó, có thể chuyển đổi vai trò giữa 2 khoá và rất khó để suy ra khoá này từ khoá kia. Khoá mã hoá (KE) có thể đưa ra công khai nhưng khoá dùng giải mã (KD) phải được giữ bí mật tuyệt đối.

Người ta còn phân biệt 2 loại khóa:

- Các khoá dùng trong thời gian dài gọi là khoá chính (primary) hay khoá mã hoá (key encryption).
- Các khoá được dùng trong khuôn khổ một cuộc truyền thông gọi là khoá làm việc (working) hay khoá mã hoá dữ liệu (data encryption).

## 10.2 CáC phương pháp mã hóa dữ liệu

### 10.2.1 Phương pháp hoán vị

Phương pháp này sắp xếp lại các kí tự trong văn bản gốc để tạo ra văn bản mật mã. Phương pháp này có một số kỹ thuật sau :

*1. Đảo ngược toàn bộ văn bản gốc*

Từ văn bản gốc, ta mã hoá bằng cách viết theo thứ tự ngược lại. Ví dụ DHKTDN được mã hoá thành NDTKHD. Đây là một trong những phương pháp mã hoá đơn giản nhất và chỉ mang tính tham khảo vì không an toàn.

2. *Mã hoá theo mẫu hình học*

Sắp xếp lại văn bản gốc theo mẫu hình học nào đó (thường là ma trận 2 chiều) để tạo văn bản mật mã.

Ví dụ : ĐAIHOCĐANANG được viết thành ma trận 3 x 4:

| | | | |
|---|---|---|---|
| Đ | A | I | H |
| O | C | Đ | A |
| N | A | N | G |

Nếu ta lấy các kí tự ra theo thứ tự các hàng là 3,1,2 ta sẽ có văn bản mật mã là N A N G O C Đ A Đ A I H. Phương pháp cũng kém an toàn, có thể dựa vào tần số xuất hiện của các kí tự trong bản mã để suy ra văn bản gốc.

3. *Đổi chổ cột*

Sắp xếp lại văn bản gốc thành dạng hình chữ nhật theo các cột, sau đó các cột được sắp xếp lại và lấy các kí tự theo chiều ngang.

Ví dụ : văn bản TRUONGDAIHOCKYTHUATDANANG được viết thành ma trận 5 x 5 :

| Cột | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| Văn bản | T | R | U | O | N |
| | G | D | A | I | H |
| | O | C | K | I | T |
| | H | U | A | T | D |
| | A | N | A | N | G |

Vì có 5 cột nên có thể sắp xếp lại theo 5!= 120 cách khác nhau. Nếu ta chuyển vị các cột theo thứ tự 2,3,4,1,5 rồi lấy các kí tự theo hàng ta sẽ có văn bản mã như sau: RUOTN DAIGH CKYOT UATHD NANAG.

Ta thấy rằng, với một văn bản càng lớn (nhiều kí tự) số cách sắp xếp có thể sẽ rất lớn làm tăng khả năng an toàn. Hạn chế của phương pháp này là toàn bộ ma trận kí tự phải được sinh để mã hoá và giải mã và cũng dễ nhầm lẫn trong việc giải mã.

*4. Hoán vị các kí tự của văn bản gốc theo chu kì cố định T*

Cho hàm f là hoán vị của một khối gồm T kí tự thì khoá mã hoá được biểu diễn bởi hàm K(T,f). Do vậy, văn bản gốc :

$M = m_1\ m_2\ md\ md_{+1} \ldots m_{2d}$

Trong đó $m_i$ là các kí tự riêng lẻ sẽ được mã hoá thành :

$Ek(M) = mf_{(1)}\ mf_{(2)} \ldots mf_{(d)}\ md_{+f(1)} \ldots md_{+f(d)}$

Với $mf_{(1)}\ mf_{(2)} \ldots mf_{(d)}$ là một hoán vị của $m_1\ m_2 \ldots md$

Ví dụ : giả sử T=7 và f hoán vị dãy i = 12345 thành f(i)=23415, chẳng hạn từ gốc STUDY được biểu diễn như sau :

| *Vị trí đầu* | *Vị trí hoán vị* | *từ* | *Mã hoá* |
|---|---|---|---|
| 1 | 2 | S | T |
| 2 | 3 | T | U |
| 3 | 4 | U | D |
| 4 | 1 | D | S |
| 5 | 5 | Y | Y |

Bằng cách đó văn bản gốc TRUONGDAIHOCKYTHUATDANANG được mã hoá thành RUOTN DAIGH CKYOT UATHD NANAG

### 10.2.2 Phương pháp thay thế

Phương pháp này mã hoá văn bản bằng cách thay thế mỗi kí tự trongvăn bản bằng một kí tự khác nào đó (có thể là chữ cái, chữ số hoặc kí hiệu), có thể dùng một trong các phương pháp thay thế sau :

*1. Thay thế đơn giản*

Mỗi kí tự trong văn bản gốc được thay thế bằng một kí tự tương ứng trong văn bản mật mã. Một ánh xạ 1 – 1 được dùng để mã hoá và giải mã thông điệp.

*2. Thay thế đồng âm*

Mỗi kí tự trong văn bản gốc được mã hoá với một số kí tự của văn bản mật mã (ánh xạ 1 - n). Ngoài ra còn một số phương pháp thay thế khác như thay thế đa mẫu tự, thay thế theo sơ đồ...

Một trong những mật mã thay thế đơn giản được biết đến nhiều nhất là mã Morse, trong đó các chữ cái được thay thế bằng các kí tự gạch và chấm. Bảng mã ASCII ta thường dùng cũng là một dạng mật mã thay thế đơn giản. Trong đó, chữ A

được biểu diễn bằng chuỗi số nhị phân 1000001 hoặc số thập phân 65, chữ B được biểu diễn bởi 1000010 hoặc 66,v.v...

Một dạng mật mã khác cũng được biết đến nhiều đó là bảng chữ cái dịch chuyển. ở đây, các chữ cái trong bảng được dịch chuyển sang phải k vị trí, k gọi là khoá. Ta có hàm dịch chuyển : f(a) = ( a + k ) mod n với a là một chữ cái trong bảng mã, n là số chữ cái (n=26 nếu là bảng chữ tiếng Anh chuẩn).

Ví dụ : với k = 5 ta có :

Bảng chữ gốc : A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Bảng chữ mật mã : F G H I J K LMN O P Q R S T U V W X Y Z A B C D E

Để giải mã, người nhận phải biết khoá k và phục hồi lại văn bản gốc bằng cách biến đổi ngược.

Như vậy nếu văn bản gốc là TRUONG DAI HOC KY THUAT DA NANG thì văn bản mã sẽ là YWZTSL IFN MTH PN YMZFY IF SFSL. Phương pháp này kém an toàn vì chỉ cần thử lần lượt 26 khả năng là ta đã giải mã được.

Một phương pháp thay thế khác tốt hơn là dùng từ khoá theo sơ đồ Vignère. Theo sơ đồ này, từ khoá được cộng vào liên tiếp theo từng kí tự một cho văn bản gốc, mỗi kí tự được biểu diễn bởi một vị trí của nó trong bảng kí tự và phép cộng được thực hiện theo môđun 26. Ví dụ, giả sử ta có bằng :

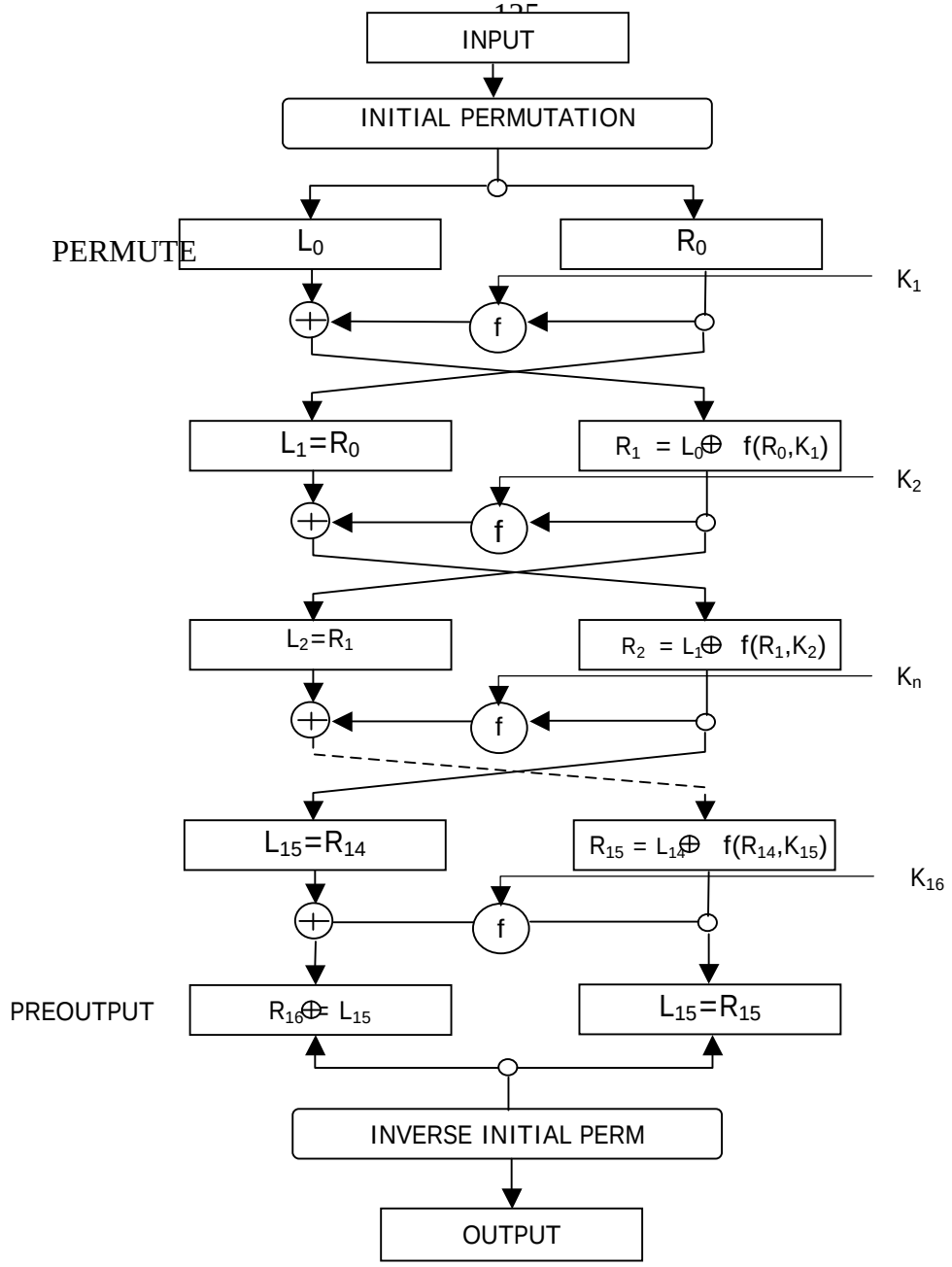
| ***Vị trí*** | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ***Ký tự*** | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S |

| 19 | 20 | 21 | 22 | 23 | 24 | 25 |
|---|---|---|---|---|---|---|
| T | U | V | W | X | Y | Z |

Cho từ khoá là ABCDEF, văn bản DAIHOC được mã hoá thành DBKKSH. Lưu ý rằng ở trên các từ được viết tách ra cho dễ đọc, trên thực tế dữ liệu được truyền thành từng dòng liên tục để sau đó bí mật tính chu kì.

### 10.2.3 Phương pháp mã hóa chuẩn DES

Những thuật toán hiện đại hơn dùng kết hợp cả hai kỹ thuật thay thế và đổi chỗ. Trong đó phương pháp được biết đến nhiều nhất là chuẩn mã hoá dữ liệu DES (Data Encryption Standard) được Mỹ và hãng IBM phát triển trong những năm 70. Lưu đồ mã hoá DES được mô tả như hình sau.

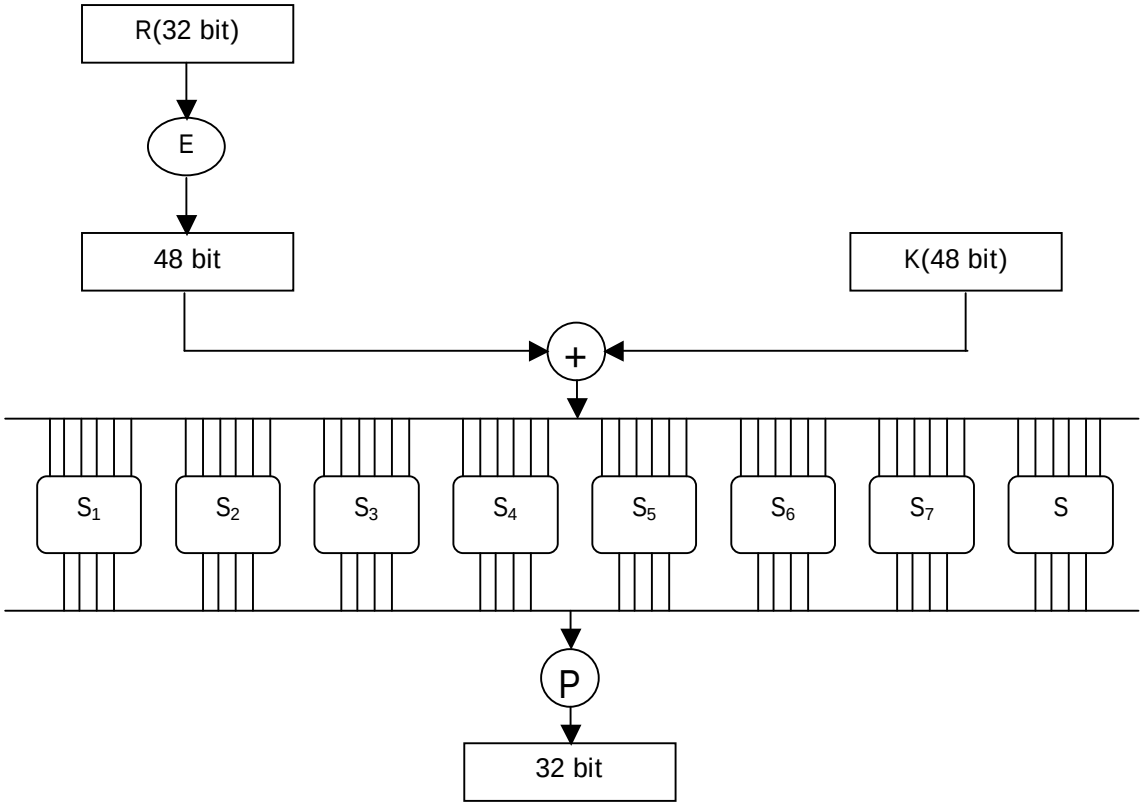



Hình 10-3. Sơ đồ mã hoá DES.

Đầu vào là một dãy 64 bit biểu diễn một khối các kí tự trong văn bản gốc và đầu ra là một dãy 64 bit biểu diễn văn bản mã. Quá trình mã hoá được chia làm 3 giai đoạn :

Đầu tiên văn bản gốc được chuyển qua bộ hoán vị khởi đầu (initial permutation-IP) để tạo ra 64 bit đã hoán vị . Sau đó thực hiện 16 phép lặp của một hàm chữ số (cipher function), kí hiệu là f(R,K) là tổ hợp cả kĩ thuật hoán vị lẫn kĩ thuật thay thế. Trong đó R là dãy con phải (32 bit) của văn bản gốc, khoá K có độ dài 56 bit. 64 bit đầu ra được làm đầu vào cho hoán vị ngược với hoán vị khởi đầu $IP^{-1}$ để tạo ra 64 bit văn bản gốc.

Chi tiết của hàm f(R,K) được mô tả như sau :




Hình 10-4. Hàm f(R,K).

Phép toán của f(R,K) :

Giả sử, bit đầu tiên trong kết quả hoán vị là bit 58 trong dãy ban đầu, bit thứ 2 trong kết quả là bit thứ 50 trong dãy ban đầu,v.v... Dãy hoán vị được chia làm 2 dãy con 32 bit : dãy con trái, kí hiệu là $L_0$ trong sơ đồ, và dãy con phải kí hiệu là $R_0$. Hàm f(R,K) dùng các phép toán thay thế và một khoá $K_1$ để chuyển $R_0$ thành một dãy 32 bit mới, kí hiệu $f(R_0,K_1)$. Dãy bit này được cộng vào $L_0$ từng bit một theo mođun 2(phép toán cộng loại trừ) để tạo ra dãy con phải ở giai đoạn tiếp theo. Dãy $R_0$ ban đầu trở thành dãy con trái $L_1$.

Phép hoán vị ban đầu IP được cho như bảng dưới đây :

| IP | | | | | | | |
|---|---|---|---|---|---|---|---|
| 58 | 50 | 42 | 34 | 26 | 18 | 10 | 2 |
| 60 | 52 | 44 | 36 | 28 | 20 | 12 | 4 |
| 62 | 54 | 46 | 38 | 30 | 22 | 14 | 6 |
| 64 | 56 | 48 | 40 | 32 | 24 | 16 | 8 |
| 57 | 49 | 41 | 33 | 25 | 17 | 9 | 1 |
| 59 | 51 | 43 | 35 | 27 | 19 | 11 | 3 |
| 61 | 53 | 45 | 37 | 29 | 21 | 13 | 5 |
| 63 | 55 | 47 | 39 | 31 | 23 | 15 | 7 |

Chuỗi các phép toán được thực hiện 16 lần với 16 khoá khác nhau $K_1$, $K_2$,..., $K_{16}$, ngoại trừ một điều là không có "phép chuyển qua" ở giai đoạn cuối cùng. Những phép toán này tạo ra dãy 64 bit $R_{16}L_{16}$, được đánh dấu PREOUTPUT trong sơ đồ. Phép toán ngược $IP^{-1}$ của phép hoán vị IP được dùng để biến đổi dãy PREOUTPUT để tạo ra bản mã cuối cùng.

| $IP^{-1}$ | | | | | | | |
|---|---|---|---|---|---|---|---|
| 40 | 8 | 48 | 16 | 56 | 24 | 64 | 32 |
| 39 | 7 | 47 | 15 | 55 | 23 | 63 | 31 |
| 38 | 6 | 46 | 14 | 54 | 22 | 62 | 30 |
| 37 | 5 | 45 | 13 | 53 | 21 | 61 | 29 |
| 36 | 4 | 44 | 12 | 52 | 20 | 60 | 28 |
| 35 | 3 | 43 | 11 | 51 | 19 | 59 | 27 |
| 34 | 2 | 42 | 10 | 50 | 18 | 58 | 26 |
| 33 | 1 | 41 | 9 | 49 | 17 | 57 | 25 |

Dãy con phải được kí hiệu bởi R trước hết được mở rộng thành một dãy số 48 bit dùng bảng chọn bit E sau đây :

| E | | | | | |
|---|---|---|---|---|---|
| 32 | 1 | 2 | 3 | 4 | 5 |
| 4 | 5 | 6 | 7 | 8 | 9 |
| 8 | 9 | 10 | 11 | 12 | 13 |
| 12 | 13 | 14 | 15 | 16 | 17 |
| 16 | 17 | 18 | 19 | 20 | 21 |
| 20 | 21 | 22 | 23 | 24 | 25 |
| 24 | 25 | 26 | 27 | 28 | 29 |
| 28 | 29 | 30 | 31 | 32 | 1 |

Như vậy, khối 6 bit đầu tiên gồm các bit 32,1,2,3,4,5 của R; khối thứ hai gồm các bit 4,5,6,7,8,9, ... Sau đó một phép toán thay thế được áp dụng cho dãy 48 bit này bằng cách cộng nó (theo phép cộng loại trừ) với khoá 48 bit. Một phép thay thế khác được sử dụng cho các khối 6 bit để tạo ra các khối 4 bit để kết quả cuối cùng là dãy 32 bit. Ví dụ bảng thay thế cho $S_1$ là :

| $S_1$ | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Số** hàng | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| 0 | 14 | 5 | 13 | 1 | 2 | 15 | 11 | 8 | 3 | 10 | 6 | 12 | 5 | 9 | 0 | 7 |
| 1 | 0 | 15 | 7 | 4 | 14 | 2 | 13 | 1 | 10 | 6 | 12 | 11 | 9 | 5 | 3 | 8 |
| 2 | 4 | 1 | 14 | 8 | 13 | 6 | 12 | 11 | 15 | 12 | 9 | 7 | 3 | 10 | 5 | 0 |
| 3 | 15 | 12 | 8 | 2 | 14 | 9 | 1 | 7 | 5 | 11 | 3 | 14 | 10 | 0 | 6 | 13 |

Để minh hoạ cách sử dụng, giả sử rằng khối 6 bit đầu tiên là 101000. Số nhị phân 10 tạo bởi bit đầu tiên và bit cuối cùng xác định một hàng trong bảng, cụ thể là hàng 2, 4 bit giữa 0100 xác định cột trong bảng, cụ thể là cột 4. Biểu diễn nhị phân 4 bit 1101 của phần tử 13 ở hàng 2 cột 4 trong bảng là giá trị thay thế cho 6 bit này. các phép toán tương tự $S_2$, $S_3$,..., $S_8$ được dùng để chuyển đổi cho các khối 6 bit khác.

Phép hoán vị cuối cùng P được áp dụng cho dãy 32 bit để tạo ra f(R,K):

| P | | | |
|---|---|---|---|
| 16 | 7 | 20 | 21 |
| 29 | 12 | 28 | 17 |
| 1 | 15 | 23 | 26 |
| 5 | 18 | 31 | 10 |
| 2 | 8 | 24 | 14 |
| 32 | 27 | 3 | 9 |
| 19 | 13 | 30 | 6 |
| 22 | 11 | 4 | 25 |

Mười sáu khoá khác nhau dùng trong DES được lấy ra theo một qui định chặt chẽ từ một khoá 64 bit duy nhất. Như vậy người dùng chỉ cần giữ một khoá để mã hoá và giải mã hơn là giữ 16 khoá khác nhau. Thuật toán giải mã cũng tương tự như khi mã hoá, chỉ khác một diều là 16 khoá được dùng theo thứ tự ngược lại.

Việc giải mã được thực hiện ngược lại với 64 bit văn bản mã làm đầu vào cho hoán vị ngược với hoán vị khởi đầu $IP^{-1}$ để tạo ra 64 bit văn bản gốc.

Phương pháp DES được Uỷ ban tiêu chuẩn quốc gia (National Bureau of Standards) Hoa Kỳ đề nghị như là một sơ đồ mã hoá “chuẩn “. Tuy nhiên, người ta còn đang tranh luận liệu khoá 48 bit có đủ dài hay chưa và các phép toán thay thế có đủ độ bảo mật cần thiết hay chưa.

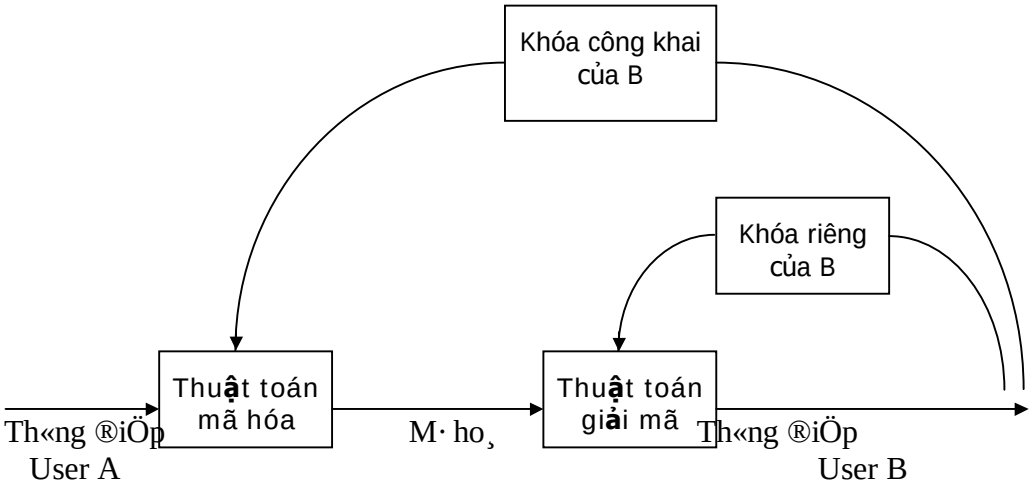
### 10.2.4 Phương pháp mã hoá khoá công khai

#### *10.2.4.1 Nguyên lí mã hóa công khai*

Trong khi thuật toán mã hoá cổ điển dùng một khoá chung cho mã hoá và giải mã thì phương pháp mã hoá bằng khoá công khai sử dụng hai khoá có quan hệ với nhau trong thuật toán để ứng dụng trong mã hoá/giải mã. Các thuật toán này có đặc trưng quan trọng là khó có thể tính toán bằng máy để tìm ra được khoá giải mã nếu chỉ biết được khoá mã hoá và phương pháp mã hoá.

Một số các thuật toán mã hóa công khai (như RSA chẳng hạn) còn có một đặc trưng nữa là khả năng hoán đổi vai trò giữa cặp khoá. Có nghĩa là khi khoá này dùng để mã hoá thì khoá kia dùng để giải mã và ngược lại.

Hình sau mô tả nguyên lí quá trình mã hoá/giải mã bằng khoá công khai :




Hình 10-5. Quá trình mã hoá/giải mã bằng khoá công khai.

Quá trình mã hoá/giải mã như sau:

b. Mỗi hệ thống cuối trong một mạng tạo ra một cặp khoá dùng để mã hoá và giải mã thông tin khi nhận được chúng.

c. Mỗi hệ thống phải có 2 khóa, khóa công khai và khóa bí mật, khoá công khai được công bố lên mạng tại nơi cho phép đăng kí công cộng hoặc đưa vào file. Khoá còn lại phải được giữ bí mật tuyệt đối.

d. Nếu A muốn gửi thông điệp cho B, A sẽ dùng khoá công khai của B trên mạng để mã hoá nó rồi gởi.

e. Khi B nhận được thông điệp của A, B sẽ dùng khoá riêng của mình để giải mã thông điệp nhận được. Không ai có thể giải mã thông điệp được vì chỉ có một mình B biết khoá giải mã.

Thông tin về khoá phải được giữ an toàn tuyệt đối và có thể cập nhật hoặc thay đổi lại khoá cũ. Việc tạo ra các hệ thống bảo vệ và quản lí khoá cũng cần hết sức chặt chẽ.

#### *10.2.4.2 Phương pháp mã hóa RSA*

Bản thuyết trình đầu tiên của Diffe và Hellman đưa ra năm 1976 tại hội nghị MIT và gần như ngay lập tức, sự thách thức về vấn đề mã hoá đã tìm được câu trả lời bởi hệ thống mã hoá công khai. Một trong những câu trả lời đầu tiên đưa ra vào năm 1977 bởi Ron Rivest, Adi Shamir và Len Adltôian được công bố vào năm 1978

(gọi tắt là rsa). ý tưởng RSA trở thành gần như độc tôn và được sử dụng rộng rãi trong phương pháp mã hoá bằng khoá công khai.

Giả sử ta có :

Văn bản gốc : $M = M_1 M_2 ... Mk$

Văn bản mã hóa : $C = C_1 C_2 ... Ck$ , trong đó $Ci = M_i^E \bmod n$, n là tích 2 số nguyên tố bất kì p và q.

Thuật toán RSA dùng thuyết số để phát triển phương pháp phát sinh một cặp các số nguyên tố - các khoá, thuật toán dựa trên nhận xét: *Có thể dễ dàng sinh ra 2 số nguyên tố lớn và khi nhân chúng với nhau thì rất khó khi muốn phân tích tích của chúng thành thừa số và khó có thể tìm được số còn lại từ số kia*.

Theo một hệ quả của định lí Euler đưa ra: *Cho 2 số nguyên tố p và q và hai số nguyên n và m để n=p.q và 0<m<n, tồn tại một số nguyên duy nhất k sao cho:*

$$(mk^{\phi(n)+1} = mk^{(p-1)(q-1)+1}) \bmod m = n$$

trong đó $\phi(n)$ là hàm Euler với giá trị số nhỏ hơn n và có quan hệ nguyên tố với n, $\phi(n)=(p-1)(q-1)$.

Do đó ta có thể đạt được kết quả mong muốn nếu: $ED = k\phi(n) + 1$

Điều này tương đương với: $ED \bmod \phi(n) = 1$.

Thuật toán RSA được mô tả như sau:

1. Chọn 2 số nguyên tố p, q.
2. Tính tích n = p*q
3. Tính $\phi(n) = (p-1)(q-1)$
4. Chọn E thỏa $USCLN(\phi(n), E) = 1$ ; *với* $1 < E < \phi(n)$
5. Tìm D thỏa $DE \bmod \phi(n) = 1$.

Khoá công khai là KE = {E,n}, khoá riêng là KD = {D,n} hoặc ngược lại.

Giả sử rằng user A công bố khoá công khai KE lên mạng và user B muốn gửi thông điệp cho user A :

- B sẽ dùng khóa công khai của user A để mã hoá thông điệp của mình bằng công thức $C = ME \bmod n$, rồi gởi nó đi.
- User A sẽ nhận được thông điệp đã mã hoá và giải mã nó bằng khoá riêng của mình bằng công thức $M = CD \bmod n$

Ví dụ: Chọn p =7, q =17

Tính n = p*q = 7*17 = 119

$\phi(n) = (p-1)*(q-1) = 96$

Chọn E thỏa : USCLN(E, 96) = 1. Ta chọn E = 5.

Tìm D thỏa : D*E mod 96 = 1 và D < 96 , suy ra D =77.

Ta được KE = {5,119} , KD = {77,119}.

Giả sử M = 19. Quá trình mã hoá: $C = 19^5 \bmod 119 = 66$.

Quá trình giải mã: $M = 66^{77} \bmod 119 = 19$.

#### *10.2.4.3 Các vấn đề nảy sinh trong thuật toán*

1. Vấn đề phức tạp trong tính toán.

Trong quá trình mã hoá và giải mã, thuật toán RSA phát sinh ra các số nguyên rất lớn, cho dù có phép chia modulo n. Rivest, Shamir và Adltôian đề nghị rằng các số p và q phải có độ dài trên 100 chữ số để đảm bảo an toàn gần như tuyệt đối. Như vậy sự luỹ thừa quá lớn và sau đó cho dù có chia modulo n thì kết quả trung gian cũng sẽ khổng lồ và rất dễ dẫn đến tràn số. Ta có thể ứng dụng tính chất của phép chia modulo sau:

((a mod n) * (b mod n)) mod n = (a * b) mod n

Do đó, chúng ta có thể làm giảm kết quả trung gian trong phép chia này đi. Điều này làm cho các phép toán trở nên khả thi hơn.

2. Vấn đề bẻ khoá

Với thuật toán thay thế và hoán vị, về mặt lí thuyết khi độ dài của khoá càng lớn thì mức độ an toàn càng cao, nhưng những người giải mã giàu kinh nghiệm vẫn có thể phân tích tần số xuất hiện của một số kí tự xác định hay tổ hợp của chúng để từ đó suy ra khoá và thực hiện giải mã. Trong thuật toán RSA khoá KE(E,n) là khoá công khai nên ta không cần giữ bí mật, ta chỉ giữ bí mật cho khoá riêng KD(D,n). Vì vậy, để bẻ khóa phải xác định được D từ các giá trị E và n. Theo như cách chọn các số E và D, điều này có thể làm được nếu có thể phân tích n thành tích của hai số nguyên tố. Như vậy tính an toàn của thuật toán RSA phụ thuộc vào sự khó khăn của việc xác định các thừa số nguyên tố của một số nguyên tố lớn. Hiện nay nếu sử dụng thuật toán phân tích thừa số nhanh nhất của Schroeppel thì cũng cần đến : $S = \exp[(\ln n)\ln(\ln n)]^{1/2}$ bước tính toán để phân tích n thành p và q.

Bảng dưới đây hiển thị các thời gian dự đoán của các nhà phân tích, giả sử rằng mỗi phép toán được thực hiện trong 1 micro giây :

| Độ dài của khóa | Thời gian |
|---|---|
| 50 | 4 giờ |

| | |
|---|---|
| 75 | 104 ngày |
| 100 | 74 năm |
| 200 | 4.000.000 năm |
| 300 | $5 \times 10^{15}$ năm |
| 500 | $4 \times 10^{25}$ năm |

Phương pháp mã hoá với khoá công khai xem như được bảo đảm vì hiện nay vẫn chưa tìm ra một thuật toán phân tích thừa số nguyên tố có hiệu quả.

#### *10.2.4.4 ứng dụng của mã hoá dữ liệu*

Mã hoá dữ liệu có các ưu điểm là an toàn vì ít phụ thuộc vào cấu trúc hệ thống mạng. Ngoài ra mã hoá dữ liệu có tính bảo mật do dữ liệu được mã hoá rồi thì chỉ có những người có quyền mới có thể giải mã để nhận lại được dữ liệu ban đầu. Các phương pháp mã hoá trên có thể áp dụng trong những tình huống sau :

- Phương pháp mã hoá thay thế kết hợp với phương pháp mã hoá hoán vị dùng tạo ra phương pháp mã hoá DES.
- Các dịch vụ e-mail trên mạng Internet hay các mạng cục bộ có thể sử dụng thuật toán RSA để tạo ra một mặt nạ nhận dạng (authentication mask) các thông điệp giữa các cá nhân với nhau. Có nghĩa là chỉ những người nhận được thư gởi cho mình bằng khoá mã hoá của mình thì mới giải mã được thông điệp đó và hoàn toàn không thể (nói theo nguyên tắc) đọc được các thư không phải gởi cho mình.
- Kỹ thuật mã hoá chữ kí số (digital signature) có thể dùng để tạo ra một chữ kí mã hoá dùng để xác định, nhận dạng một đối tượng trong các dịch vụ thương mại, ví dụ như các thẻ tín dụng hoặc các loại visa, cardphone chẳng hạn....
- Thư điện tử e-mail cũng có thể kết hợp thuật toán này với các thuật toán mã hoá khác như DES theo mô hình có thể là:

- Nội dung thư được mã hoá bằng phương pháp DES
- Tạo một chữ ký số và mã hoá bằng khoá RSA
- Khoá DES dùng để giải mã có thể được mã hoá bằng RSA và gửi kèm trong thư luôn mà không cần phải bí mật. Người nhận sẽ dùng khóa riêng của mình để giải mã khoá DES, sau đó giải mã thư nhận được.

## 10.3 Cơ chế bảo vệ bằng firewall

Vấn đề quan trọng trong việc quản lý các tài nguyên thông tin là cơ chế bảo vệ chống việc truy cập bất hợp pháp trong khi vẫn cho phép người được ủy nhiệm sử dụng những nguồn thông tin mà họ được cấp quyền, và phương pháp chống thất

thoát thông tin được truyền tải trên các mạng truyền dữ liệu công cộng (Public Data Communication Network). Đó chính là yêu cầu của một giải pháp hoặc hệ thống an ninh cho hệ thống mạng hay còn gọi là hệ thống an ninh dữ liệu (Data Security System).

Nhu cầu an ninh hệ thống ngày càng trở nên quan trọng vì nhiều nguyên nhân như các đối thủ luôn tìm cách để nắm được mọi thông tin liên quan, ngày càng nhiều hacker truy cập thông tin từ các mạng nội bộ theo nhiều mục đích khác nhau.

Một giải pháp an ninh cho hệ thống mạng được ứng dụng nhiều đó là bức tường lửa (firewall). Thuật ngữ firewall có nguồn gốc từ một kỹ thuật thiết kế trong xây dựng để ngăn chặn, hạn chế hỏa hoạn. Trong công nghệ mạng thông tin, firewall là một kỹ thuật được tích hợp vào hệ thống mạng để chống lại việc truy cập trái phép nhằm bảo vệ các nguồn thông tin nội bộ cũng như hạn chế sự xâm nhập vào hệ thống của một số thông tin khác không mong muốn.

***Về mặt chức năng hệ thống***, firewall là một thành phần được đặt giữa hai mạng để kiểm soát tất cả các việc lưu thông và truy cập giữa chúng với nhau, bao gồm:

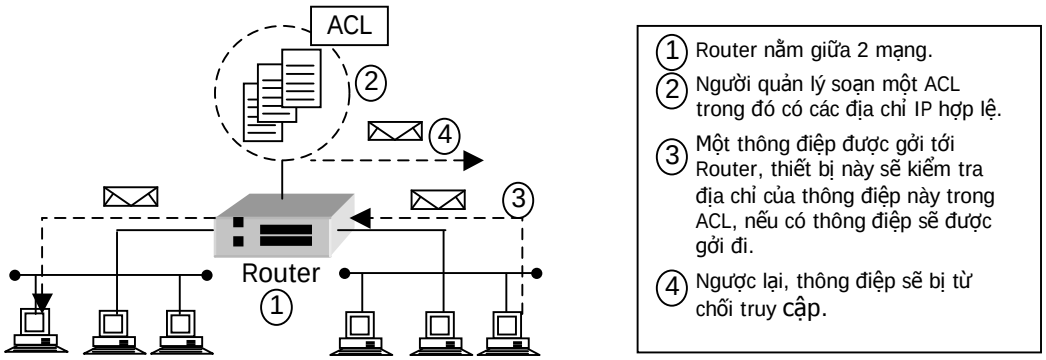
1. Tất cả các trao đổi dữ liệu từ trong ra ngoài và ngược lại phải thực hiện thông qua firewall.
2. Chỉ có những trao đổi nào được phép bởi chế độ an ninh của hệ thống mạng nội bộ (trusted network) mới được quyền lưu thông qua firewall.

***Về mặt vật lý***, firewall bao gồm:

1. Một hoặc nhiều hệ thống máy chủ kết nối với các bộ định tuyến (router) hoặc có chức năng router.
2. Các phần mềm quản lý an ninh chạy trên các hệ thống máy chủ. Thông thường là các hệ quản trị xác thực (Authentication), cấp quyền (Authorization) và kế toán (Accounting).

Firewall bao gồm phần cứng và/hoặc phần mềm nằm giữa 2 mạng (như mạng nội bộ và mạng Internet), bảo vệ mạng nội bộ bằng cách cấm các người sử dụng truy cập trái phép đến và đồng thời ngăn chặn những thông điệp không được phép gửi đi cho người nhận bên ngoài mạng. Firewall có thể nằm trên bộ dẫn đường hay trên Server. Cơ chế làm việc của Firewall dựa trên việc kiểm tra các gói dữ liệu IP lưu chuyển giữa hai mạng tùy thuộc vào các qui tắc mà người quản trị hệ thống đã xác lập.

Khái quát phương thức làm việc của Firewall như trong hình vẽ sau:




Hình 10-6. Cơ chế hoạt động của Firewall.

### 10.3.1 Các loại firewall và cơ chế hoạt động

Khi nói đến việc lưu thông dữ liệu giữa các mạng với nhau thông qua firewall thì điều đó có nghĩa rằng firewall hoạt động kết hợp chặt chẽ với giao thức TCP/IP. Vì giao thức này làm việc theo thuật toán chia nhỏ các dữ liệu nhận được từ các ứng dụng trên mạng, hay chính xác hơn là các dịch vụ chạy trên các giao thức (Telnet, SMTP, DSN, SMNP, NFS,...) thành các gói dữ liệu rồi gán cho các gói này những địa chỉ để có thể nhận dạng tái lập lại ở đích cần gửi đến. Do đó các loại firewall cũng liên quan rất nhiều đến các packet và các địa chỉ của chúng.

#### *10.3.1.1 Bộ lọc packet (Packet filtering)*

Loại firewall này thực hiện việc kiểm tra số nhận dạng địa chỉ của các packet để cho phép chúng có thể lưu thông qua lại hay không. Các thông số có thể lọc được của một packet như sau:

1. Địa chỉ IP nơi xuất phát (source IP address).
2. Địa chỉ IP nơi nhận (destination IP address).
3. Cổng TCP nơi xuất phát (TCP source port).
4. Cổng TCP nơi nhận (TCP destination port).

Nhờ đó firewall có thể ngăn cản được các kết nối vào những máy chủ hoặc mạng nào đó được xác định, hoặc khóa việc truy cập vào hệ thống nội bộ từ những địa chỉ không cho phép.

Hơn nữa việc kiểm soát các cổng làm cho firewall có khả năng chỉ cho phép một số loại kết nối nhất định vào máy chủ nào đó, hoặc chỉ có những dịch vụ nào đó (Telnet, SMTP, FTP,...) được phép mới chạy được trên hệ thống mạng nội bộ.

#### *10.3.1.2 Cổng ứng dụng (Application gateway)*

Đây là một loại firewall được thiết kế để tăng cường chức năng kiểm soát các loại dịch vụ, giao thức được cho phép truy cập vào hệ thống mạng. Cơ chế hoạt

động của nó dựa trên cách thức gọi là Proxy Service (dịch vụ đại diện): một ứng dụng nào đó được quy chiếu đến (hay đại diện bởi) một Proxy Service trong khi các Proxy Service chạy trên các hệ thống máy chủ thì được quy chiếu đến application gateway của firewall. Cơ chế lọc của packet filtering phối hợp kiểm soát với cơ chế "đại diện" của application gateway cung cấp một khả năng an toàn và uyển chuyển hơn.

Ví dụ một hệ thống mạng có chức năng lọc các gói tin ngăn các kết nối bằng Telnet vào hệ thống chỉ trừ một chủ duy nhất -Telnet application gateway là được phép. Một người sử dụng dịch vụ Telnet muốn kết nối vào hệ thống phải thực hiện các bước sau :

1. Thực hiện dịch vụ TELNET đến Telnet application gateway rồi cho biết tên của máy chủ bên trong cần truy cập.
2. Gateway kiểm tra địa chỉ IP nơi xuất phát của người truy cập rồi cho phép hoặc từ chối tùy theo chế độ an ninh của hệ thống.
3. Người truy cập phải vượt qua được hệ thống kiểm tra xác thực.
4. Proxy Service tạo một kết nối Telnet giữa gateway và máy chủ cần truy cập.
5. Proxy Service liên kết lưu thông giữa người truy cập và máy chủ.

Cơ chế hoạt động này có ý nghĩa quan trọng trong việc thiết kế an ninh hệ thống ví dụ như:

1. Che giấu các thông tin: người dùng chỉ có thể nhìn thấy trực tiếp các gateway được phép.
2. Tăng cường kiểm tra truy cập bằng các dịch vụ xác thực (Authentication).
3. Giảm đáng kể giá thành cho việc phát triển các hệ quản trị xác thực vì các hệ thống này được thiết kế chỉ quy chiếu đến application gateway.
4. Giảm thiểu các quy tắc kiểm soát của bộ lọc (Packet filtering). Điều này làm tăng tốc độ hoạt động của firewall.

#### *10.3.1.3 Bộ lọc session thông minh (Smart session filtering)*

Cơ chế hoạt động phối hợp giữa bộ lọc packet và cổng ứng dụng như trên cung cấp một chế độ an ninh cao tuy nhiên nó cũng bị vài hạn chế. Vấn đề chính hiện nay là làm sao để cung cấp đủ Proxy Service cho rất nhiều ứng dụng khác nhau đang phát triển ồ ạt. Điều này có nghĩa là nguy cơ, áp lực đối với việc đánh lừa firewall gia tăng lên rất lớn nếu các proxy không kịp đáp ứng.

Trong khi giám sát các packet ở những mức phía trên, nếu như lớp network đòi hỏi nhiều công sức hơn đối với việc lọc các packet đơn giản, thì việc giám sát

các giao dịch lưu thông ở mức mạng (Session) đòi hỏi ít công việc hơn. Cách này cũng loại bỏ được các dịch vụ đặc thù cho từng loại ứng dụng khác nhau.

Nếu kết hợp khả năng ghi nhận thông tin về các session và sử dụng nó để tạo các quy tắc cho bộ lọc thì sẽ có được một bộ lọc thông minh hơn. Đó chính là cơ chế hoạt động của bộ lọc session thông minh.

Vì một session ở mức network được tạo bởi 2 packet lưu thông theo 2 chiều, cho nên nếu thiết kế 2 quy tắc lọc cho 2 chiều này: một để kiểm soát các packet lưu thông từ host phát sinh ra nó đến máy chủ cần tới, một để kiểm soát packet trở về từ máy chủ phát sinh. Một bộ lọc thông minh sẽ nhận biết được rằng packet trở về theo chiều ngược lại nên quy tắc thứ 2 là không cần thiết. Do vậy, cách để tiếp nhận các packet không mong muốn sinh ra từ bên ngoài firewall sẽ khác biệt rất rõ với cách tiếp cận cho các packet do những kết nối được phép (ra bên ngoài). Và như vậy dễ dàng nhận dạng các packet "bất hợp pháp".

#### *10.3.1.4 Firewall hỗn hợp (Hybrid firewall)*

Trong thực tế các firewall được sử dụng là sự kết hợp của nhiều kỹ thuật để tạo ra hiệu quả an ninh tối đa. Ví dụ việc để lọt lưới tại các kiểm soát của bộ lọc packet có thể được thực hiện tại bộ lọc session thông minh ở mức ứng dụng. Các giám sát của bộ lọc lại được bọc lót chặt chẽ bởi các dịch vụ proxy của application gateway.

#### *10.3.1.5 Một vài ứng dụng của Firewall*

Từ các chế độ hoạt động trên, firewall được ứng dụng nhiều vào hệ thống an ninh dữ liệu. Có 3 yêu cầu chính cho vấn đề an ninh hệ thống theo tiêu chuẩn ISO cho mô hình mạng OSI :

- Quản lý xác thực (Authentication)
- Quản lý cấp quyền (Authorization)
- Quản lý kế toán (Accounting management)
-

### *f. Ưu điểm của Firewall*

Firewall là điểm kiểm tra các kết nối giữa mạng nội bộ và mạng Internet bên ngoài, mọi kết nối đều phải đi qua cửa khẩu này. Đây chính là một bộ lọc an toàn bởi vì có rất nhiều dịch vụ đang hoạt động trên Internet, nếu chúng ta không có một cơ chế kiểm soát chặt chẽ thì các dịch vụ này sẽ tự do mang thông tin tràn vào mạng của chúng ta và ngược lại.

Firewall có thể được sử dụng để ghi nhận lại các hoạt động kết nối với Internet. Bởi vì, mọi hoạt động như vậy đều phải thông qua Firewall nên nó có thể cung cấp thêm chức năng thu thập mọi thông tin về các kết nối xảy ra giữa mạng nội bộ và mạng Internet bên ngoài.

Ta cũng có thể sử dụng Firewall để bảo vệ một máy đơn của người sử dụng.

***g. Hạn chế của Firewall***

Bên cạnh những mặt tích cực của Firewall kể trên, nó còn có những hạn chế và những việc mà nó không thể thực hiện được như sau:

1. Bên cạnh việc ngăn chặn các người dùng trong mạng nội bộ kết nối ra ngoài khi không được phép thì nó cũng ngăn cản các việc làm tốt của họ.
2. Firewall không thể chống lại các mối nguy hiểm mới, bởi vì chúng nằm ngoài sự kiểm soát của Firewall.
3. Do không kiểm tra trên nội dung của các gói tin, nên Firewall không sử dụng để ngăn ngừa các thông tin xấu trên một dịch vụ đã được cho phép và cũng không thể nhận biết các đoạm mã virus trong các tập tin truyền đi.

## 10.4 Hệ thống tên miền DNS (Domain Name System )

Địa chỉ Internet 32 bit thỏa mãn yêu cầu kỹ thuật, nhưng phức tạp và khó nhớ đối với người dùng. Giải pháp đưa ra ở đây là dùng những tên gợi nhớ thay cho địa chỉ số là tự nhiên và dễ nhớ đối với người sử dụng. Hơn nữa, dùng tên tin cậy hơn địa chỉ số vì địa chỉ số có thể thay đổi những tên luôn luôn dùng lại được. Do đó nảy sinh vấn đề cách đặt tên và ánh xạ địa chỉ IP với tên.

Trước đây trung tâm thông tin Internet NIC chịu trách nhiệm cấp phát và quản lý tên. Người ta dùng một file có tên host.txt trên Windows hoặc /etc/hosts trên Unix, tập tin này chứa tên của tất cả các mạng, router, host và địa chỉ IP tương ứng với chúng. Các tên được cấp phát không có mối liên hệ gì với nhau. Khi Internet phát triển, giải pháp này trở nên phức tạp không chấp nhận được về mặt quản lý.

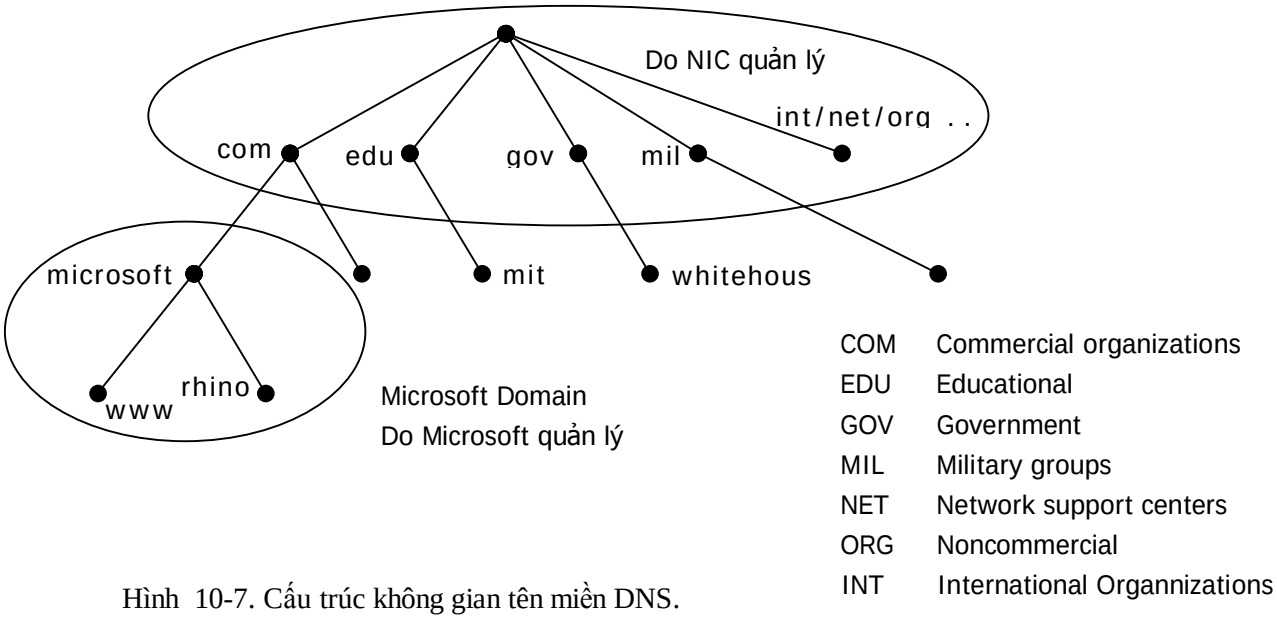
Theo Paul Mockepetris, người thiết kế chính DNS, mục tiêu thiết kế bắt đầu của DNS là để thay thế các tập tin host phức tạp bằng một cơ sở dữ liệu phân tán nhẹ hơn có khả năng cung cấp một *không gian tên thứ bậc, sự quản lý phân tán, có bộ đệm cục bộ (caching), các kiểu dữ liệu mở rộng, kích thước cơ sở dữ liệu không giới hạn và có hiệu năng.*

DNS tương ứng với tầng 7 của mô hình OSI và dùng giao thức UDP hay TCP ở tầng dưới. Việc truy cập DNS thực hiện theo mô hình Client/Server. Hầu hết các hệ thống kết nối Internet đều hỗ trợ DNS. Các đặc tả chính của DNS được định

nghĩa trong các tài liệu RFC 974, 1034, 1035. Dịch vụ cài đặt giao thức DNS phổ biến nhất là BIND (Berkeley Internet Name Domain), được phát triển đầu tiên tại Berkeyley cho hệ điều hành Unix.

DNS gồm 3 thành phần : ***Namespace, các NameServer và Resolver.***

### 10.4.1 Không gian tên miền DNS




Hình 10-7. Cấu trúc không gian tên miền DNS.

DNS tổ chức không gian tên miền theo cấu trúc cây, trên cùng là gốc, rồi đến các nút cha, nút con... và cuối cùng là các nút lá.

Một máy tính trong mạng sẽ ứng với một nút của cây. Như ở cây trên, máy ở lá www sẽ có địa chỉ hoàn chỉnh là www.microsoft.com. Mỗi nút trên cây biểu diễn một miền (domain) trong hệ thống DNS; mỗi miền lại có một hay nhiều miền con. Tại mỗi miền này đều phải có máy chủ DNS tương ứng quản lý hệ thống tên trong miền đó.

*Nút trên cây :* Mỗi nút có một tên tương ứng dài từ - đến 63 ký tự dưới 128 trong bảng mã ASCII. Các nút kề nhau không được có cùng tên. Mỗi nút có một tập (có thể rỗng) các *bản ghi tài nguyên* (Resource Record - RR) chứa thông tin đi kèm nút đó. Nhãn rỗng dành riêng cho nút gốc, ký hiệu bằng dấu chấm (.).

*Miền con :* Được tạo thành từ mỗi nút của không gian tên và các nút bên dưới có thể đi đến được các nút đó.

*Vùng :* là một phần cây con của cây DNS được quản lý như một thực thể riêng. Vùng có thể bao gồm một miền hay một miền với một số miền con. Các miền con mức thấp hơn của một vùng lại có thể chia thành các vùng rời nhau.

*Tên miền của một nút* : là dãy các nhãn từ một nút trên cây đến gốc của cây. Các nhãn trong tên miền cách nhau bằng dấu chấm (.). *Tên miền tuyệt đối* kết thúc bằng dấu chấm. Ví dụ "poneria.ISI.EDU.". *Tên miền tương đối* không kết thúc bằng dấu chấm và sẽ được phần mềm cục bộ ghép đầy đủ khi xử lý. Để đơn giản việc cài đặt, độ dài tên miền được giới hạn dưới 255. Một miền là miền con của miền khác nếu tên miền đó chứa tên miền kia. Ví dụ A.B.C.D là miền con của các miền con của các miền B.C.D, C.D, D và miền gốc.

*Tên miền đầy đủ* là tên các nút từ gốc đến lá của cây nối với nhau và phân cách bằng dấu chấm. Ví dụ : mrp2.widgets.mfg.universal.co.uk

*Các miền mức đỉnh* : Miền gốc và các miền mức đỉnh của cây DNS do NIC quản lý. Các tên miền mức đỉnh có thể chia ba loại :

- Các miền tổ chức (tên 3 ký tự) : com, edu, gov, . . .
- Các miền địa lý (các mã quốc gia, 2 ký tự) : uk, vn, ca, fr, . . .
- Miền in-addr-arpa : miền đặc biệt dùng để ánh xạ địa chỉ thành tên.

Trách nhiệm quản lý không gian tên DNS dưới mức đỉnh được NIC ủy nhiệm cho các tổ chức khác. Các tổ chức này lại chia không gian tên phía dưới và uỷ nhiệm xuống. Mô hình quản lý phân tán này cho phép DNS được quản lý tự trị bởi các tổ chức tham gia. Cách đặt tên như vậy có tác dụng phân cấp quản lý vùng tên. Các tổ chức có thể tự tạo và quản lý không gian tên riêng của mình trong mạng, không phụ thuộc vào sự cho phép của NIC.

Vấn đề tên và vùng còn được nhiều hãng lớn bổ sung và làm phong phú thêm bằng những giải pháp của riêng họ. Ví dụ Microsoft có WINS - Windows Internet Naming Service, IBM có DDNS - Dynamic Domain Name System.

#### *10.4.1.1 Cú pháp tên miền*

Cú pháp cho tên miền sau đây cho phép phù hợp với nhiều ứng dụng như mail, telnet, . . .

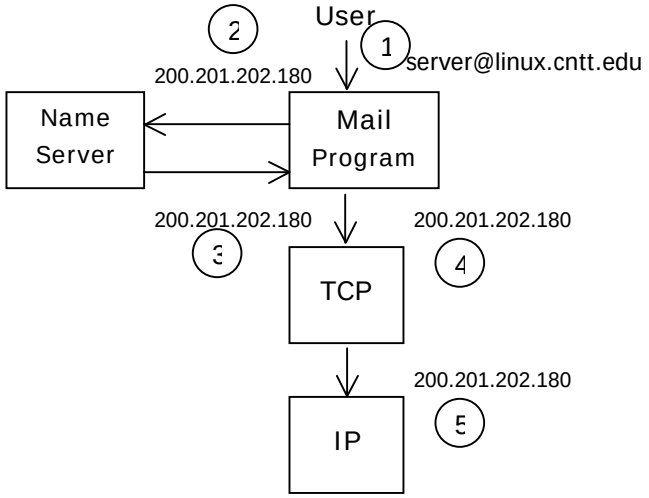
<domain>::=<subdomain>| " "
<subdomain>::=<label>|<subdomain> "." <label>
<label>::=<letter>[[<ldh-str>]<let-dig>]
<ldh-str>::=<let-dig-hyp>|<let-hyp><ldh-str>
<let-dig-hyp>::=<let-dig>| "-"
<let-dig>::=<letter>|<digit>
<letter>::= ký tự từ A-Z, a-z
<digit>::= chữ số 0-9

### 10.4.2 Máy chủ quản lý tên

Máy chủ quản lý tên (Name Server) là hệ thống chương trình quản lý cấu trúc cây của miền và các tập thông tin đi kèm. Máy chủ tên có thông tin đầy đủ về một số tập con gọi là vùng của không gian tên và các con trỏ đến các nameserver khác để lấy tin về một miền bất kỳ của cây miền. Các máy chủ tên có thông tin đầy đủ về một số phần của cây miền được gọi là có thẩm quyền (authoritative) về các phần đó. Một *vùng* (zone) là một đơn vị thông tin có thẩm quyền của cơ sở dữ liệu DNS. Trong thực tế, các máy chủ tên thường lưu tạm thời trong bộ đệm cấu trúc và thông tin các vùng và thông tin về các vùng khác để tăng hiệu năng. Các máy chủ quản lý tên trong vùng trao đổi thông tin với nhau bằng Zone Transfer Protocol.

### 10.4.3 Chương trình phân giải tên

Chương trình phân giải tên (Resolver) là các thường trình hệ thống lấy thông tin từ namserver để trả lời yêu cầu của những ứng dụng khách (client). Resolver phải có khả năng truy cập đến ít nhất một nameserver và dùng thông tin từ nameserver đó để trực tiếp trả lời câu hỏi hay để hỏi tiếp đến các nameserver khác. Chương trình người sử dụng có thể truy cập trực tiếp đến resolver, do đó không cần có một giao thức giữa resolver và chương trình người dïng.




Hình 10-8. Quá trình phân giải tên trong thực tế .

## 10.5 Hệ quản trị mạng

Hệ thống quản trị mạng (Network Management) còn gọi là mô hình Manager/Agent bao gồm các thành phần như sau :

- Hệ quản trị - Manager
- Hệ bị quản trị - Managed system
- Một cơ sở dữ liệu chứa thông tin quản trị và giao thức quản trị mạng.
- Hệ quản trị - Manager

Thực hiện cung cấp giao diện giữa người quản trị mạng và các thiết bị mạng được quản trị, bao gồm các thông tin thể hiện dưới dạng đồ họa, đồ thị, số liệu thống kê, báo cáo. Ví dụ như hiển thị dạng đồ họa bản đồ về topology liên mạng thể hiện các vị trí của các LAN segments, từ đó có thể chọn xem trạng thái hoạt động hiện hành của nó.

### 10.5.1 Hệ bị quản trị

- Bao gồm tiến trình Agent và các đối thượng quản trị (manager objects).
- Tiến trình Agent thực hiện các thao tác quản trị mạng như đặt các tham số cấu hình và các thống kê hoạt động hiện hành của các router trên một segments cho trước.
- Các đối tượng quản trị bao gồm các trạm làm việc, máy server, hub, kênh truyền.

### 10.5.2 Cơ sở dữ liệu chứa thông tin quản trị mạng

Được gọi là *cơ sở thông tin quản trị* (Management Information Base - MIB) được lưu trữ tại Server và Client. MIB được tổ chức thành một cấu trúc cây, gọi là SMI (Structure of Management Information). SMI bắt đầu từ gốc root, tiếp theo là các nhánh chứa các đối tượng quản trị được phân loại lôgic.

Kiến trúc quản trị mạng ISO như sau :

1. Quản trị sự cố (Fault Management) : phát hiện, cô lập và khắc phục sự cố.
2. Quản trị kế toán (Accounting Management) : kiểm soát va 2đánh giá việc sử dụng tài nguyên trong mạng
3. Quản trị cấu hình (Configuration Management)
4. Quản trị hiệu năng (Performance Management)
5. Quản trị an toàn (Security Management)

Simple Network Management Protocol (SNMP) được tạo ra ban đầu với mục đích cung cấp phương tiện để điều khiển các router trên mạng. SNMP, mặc dù là một phần trong gia đình giao thức TCP/IP, không phụ thuộc vào IP. SMNP được thiết kế độc lập với giao thức truyền, tuy nhiên phần lớn các hãng đều sản xuất SNMP chạy trên IP.

SNMP thực chất là gồm 3 giao thức cấu tạo thành, tất cả đều được thiết kế để làm việc với mục đích điều hành:

- Management Information Base (MIB): Một cơ sở dữ liệu chứa các thông tin trạng thái.

- Structure and Identification of Management Information (SMI): Một tiêu chuẩn định nghĩa các đầu mục của một MIB.
- Simple Network Management Protocol (SNMP): Phương thức trao đổi thông tin giữa các thiết bị và Server.

## 10.6 Dịch vụ thư điện tử

Electronic Mail (viết gọn là e-Mail, thư điện tử) là một trong những dịch vụ thông tin phổ biến nhất trên Internet. Dịch vụ e-Mail giúp mọi người có thể trao đổi thông tin với nhau trên mạng Internet. Liên lạc bằng thư điện tử nhanh hơn, thuận tiện hơn và chi phí thấp hơn rất nhiều so với trao đổi thư từ qua đường bưu điện bình thường. Ngoài ra còn cho phép họ gửi cho nhau cả các loại tài liệu như: các văn bản, các báo cáo, các chương trình máy tính, . .. và nhiều thông tin khác nữa.

Mỗi người sử dụng đều có một thư mục lưu trữ thư trên máy Server gọi là Mailbox. Tất cả các địa chỉ mail bao gồm hai phần được ngăn cách nhau bằng 1 ký tự @ (ampersand). Ví dụ : . Tên miền có thể được chia nhiều phần cách nhau bởi dấu chấm (.). Một địa chỉ mail tiêu biểu có các thành phần như sau :

*Username @ ServerName. Type of Organization . Country*

Cấu trúc của một E-Mail bao gồm các phần như sau :

- ***Phần tiêu đề thư***

Phần này do các MTA (Message Transfer Agent) tạo ra và sử dụng, nó chứa các thông tin để chuyển nhận e-Mail như địa chỉ của nơi nhận, địa chỉ của nơi gửi. Các hệ thống e-Mail cần những thông tin này để chuyển dữ liệu từ máy tính này sang máy tính khác. Cấu tạo phần này gồm nhiều trường (field), mỗi trường là một dòng văn bản ASCII chuẩn 7 bit như sau: <tên trường >: <nội dung của trường>.

Sau đây là một số trường thông tin thông dông:

| Trường | Chức năng |
|---|---|
| DATE | Chỉ ngày giờ nhận mail. |
| FROM | Chỉ địa chỉ người gởi. |
| TO | Chỉ địa chỉ người nhận. |
| CC | Chỉ địa chỉ những người nhận bản copy của mail. Các người nhận thấy được địa chỉ của những người cùng nhận trong nhóm. |
| BCC | Chỉ địa chỉ những người nhận bản sao chép của bức mail, nhưng từng người không biết những người nào sẽ nhận bức thư này. |
| REPLY-TO | Chứa các thông tin để người nhận có thể trả lời lại, thường nó chính là địa chỉ người gởi. |
| MESSAGE-ID | Định danh duy nhất, được sử dụng bởi hệ điều hành. |
| SUBJECT | Chủ đề của nội dung thư. |

Các trường trên là các trường chuẩn do giao thức SMTP quy định, ngoài ra trong phần header cũng có thể có thêm một số trường khác do chương trình e-Mail tạo ra nhằm quản lý các e-Mail riêng. Các trường này được bắt đầu bằng ký tự X- và thông tin theo sau là cũng giống như ta thấy trên một trường chuẩn.

- ***Phần nội dung***

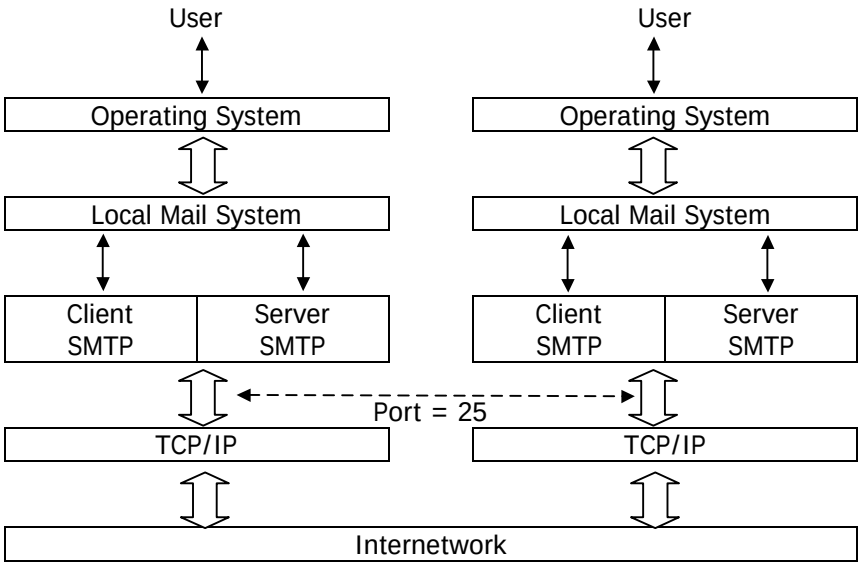
Để phân biệt phần tiêu đề và phần nội dung của e-Mail, người ta qui ước đặt ranh giới là một dòng trắng (chuỗi ký tự "\r\n"). Kết thúc của phần nội dung là chuỗi ký tự "\r\n.\r\n".

Như vậy nội dung bức thư nằm trong khoảng giữa dòng trắng đầu tiên và ký tự kết thúc thư, và trong phần nội dung của bức thư không được phép tồn tại chuỗi ký tự kết thúc thư. Mặt khác do môi trường truyền thông là mạng Internet nên các ký tự cấu thành phần thân của bức thư phải là các ký tự ASCII chuẩn.

### 10.6.1 Giao thức SMTP

SMTP (Simple Mail Transfer Protocol) là giao thức qui định việc truyền mail chủ yếu dùng trong mạng Internet.

Mối quan hệ giữa SMTP và hệ thống Mail cục bộ như sau:




Hình 10-9. Quan hệ giữa SMTP và hệ thống Mail cục bộ.

Client liên quan đến thư đi, Server liên quan đến nhận thư. Hệ thống thư cục bộ hộp thư (mailbox) cho mỗi user. Mail box có 2 phần: phần cục bộ và phần toàn cục.

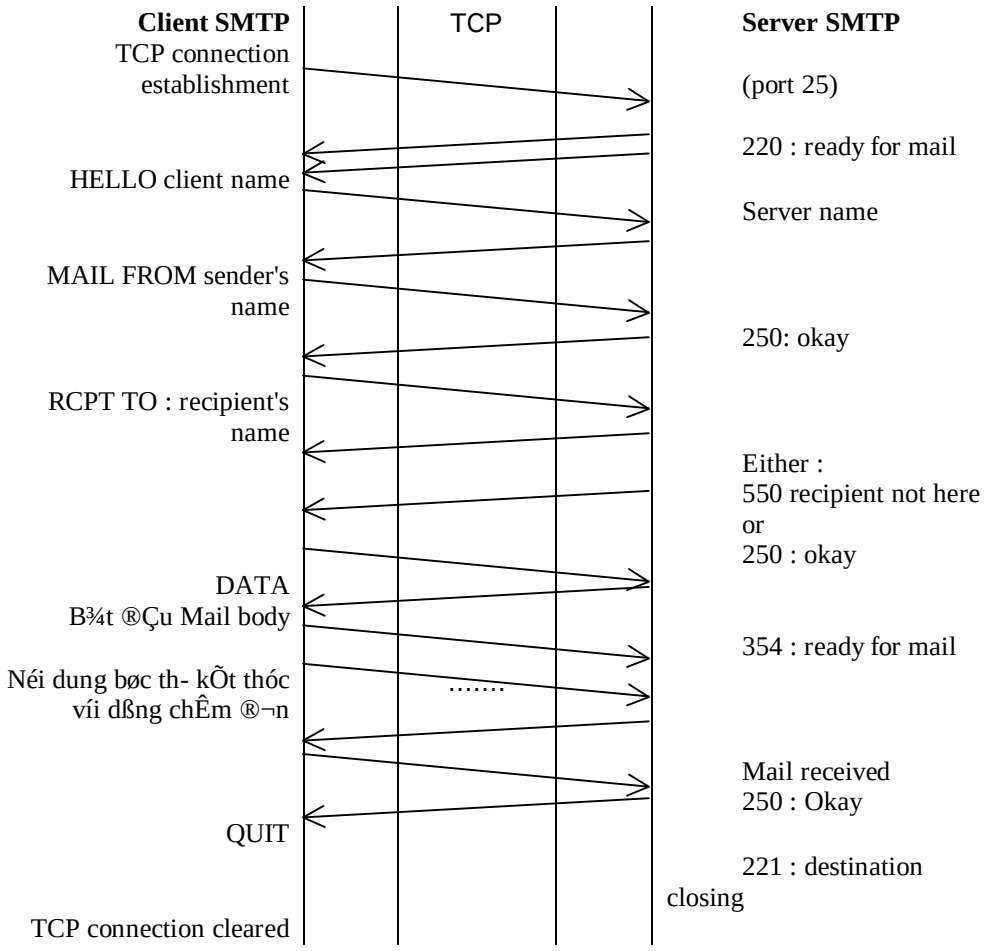
Sau khi tháo bức thư trong khuôn dạng chuẩn, hệ thống mail cục bộ xác định tên người nhận ở hộp thư cục bộ hay phải gửi ra ngoài. để gửi bức thư Client SMTP

phải biết địa chỉ IP của nơi nhận qua DNS và gửi qua cổng địa chỉ SMTP (25) để bắt đầu thiết lập kết nối server SMTP nơi nhận. Khi mối nối đã được thiết lập, Client bắt đầu chuyển bức thư đến Server bởi các lệnh của SMTP. SMTP dùng từ khóa như các lệnh để thực hiện thao tác chuyển giao mail. Một số lệnh chính của SMTP trong phiên làm việc giữa Client MTA và Server MTA như sau :

| Lệnh | Tác dụng |
|---|---|
| HELLO | Xưng danh với SMTP bên nhận, báo cho bên nhận biết bên gởi là ai. SMTP bên gởi gửi lệnh này đầu tiên cho SMTP bên nhận. |
| MAIL | Khởi động một cuộc giao dịch mail mà mục đích cuối cùng là chuyển giao các mail tới một hay nhiều Mailbox (nơi chứa Mail nhận được) khác nhau. |
| RCPT | Nói rõ người nhận mail là ai. |
| DATA | Các dòng sau lệnh DATA là dữ liệu của Mail. Đối với SMTP, chuỗi ký tự "CRLF.CRLF" báo nhận biết kết thúc nội dung bức Mail. |
| RSET | Bỏ (Reset) cuộc giao dịch hiện tại. |
| NOOP | Yêu cầu SMTP bên nhận không làm gì ngoài việc trả về câu trả lời OK (dùng để kiểm tra). |
| QUIT | Yêu cầu SMTP nhận trả lời OK và kết thúc phiên giao dịch hiện tại. |
| VRFY | Yêu cầu SMTP bên nhận kiểm tra người nhận là đúng, xác nhận các tham số gởi theo dòng lệnh. |
| SEND | Khởi động một cuộc giao dịch mà mail sẽ được gởi tới một hay nhiều thiết bị đầu cuối chứ không phải mailbox. |
| SOML | Khởi động một cuộc giao dịch mà mail sẽ được gởi tới một hay nhiều thiết bị đầu cuối hay mailbox. |
| SAML | Khởi động một cuộc giao dịch mà mail sẽ được gởi tới một hay nhiều thiết bị đầu cuối và mailbox. |
| HELP | Yêu cầu SMTP bên nhận gửi thông tin giúp đỡ cho SMTP bên phát. |
| EXPN | Yêu cầu SMTP bên nhận gởi về danh sách những người nhận Mail để có thể mở rộng việc chuyển mail cho các user khác. |
| TURN | Yêu cầu SMTP bên nhận gưi OK và đổi vai trò trở tránh SMTP gởi. |

Bảng 10-1. Các lệnh của giao thức SMTP.

SMTP (trong RFC 821) ban đầu được thiết kế để cho phép các mail server chuyển đổi các mail message. Cơ chế chính được dùng để chuyển đổi các mail là phân đường các message quanh Internet. SMTP hoạt động trên mô hình lưu và truyền trong đó client nắm các message cần để truyền đến server và gửi các lệnh đến server để báo cho server cách xử lí các message. Mail client có thể là một mail server khác, nó có một hay nhiều message phải truyền đến một server khác. Hầu hết các Internet mail client sử dụng SMTP để gửi các message.




Hình 10-10. Cơ chế trao đổi SMTP.

#### *10.6.1.1 Quy tắc làm việc với SMTP*

1. Mỗi câu lệnh phân cách tham số theo sau bằng khoảng trắng và kết thúc bằng ký tự CRLF. Mail đi từ SMTP gởi đến một SMTP nhận và đến lượt SMTP nhận trở thành SMTP gởi để gửi mail đi tiếp cho đến khi chúng được giao vào Mailbox của người nhận.
2. Các lệnh SMTP phải diễn ra một cách tuần tự.
3. Việc đánh địa chỉ phải theo cách đánh địa chỉ Internet.

Giao thức SMTP qui định các Server MTA (ở đây là SMTP bên nhận) phải gởi tín hiệu phản hồi ACK sau mỗi lệnh mà nó nhận được từ Client MTA. Mỗi câu trả lời của bên nhận đều mở đầu với một mã số theo sau mới là thông tin dạng text. Mỗi số mở đầu trong mã số có một ý nghĩa khác nhau, nó chỉ ra rằng kết quả thực hiện thao tác là tốt (số 2), thất bại (số 5) hay chưa hoàn thành (số 3).

#### *10.6.1.2 Một số mã phản hồi thông dụng của SMTP*

220 Dịch vụ đã sẵn sàng.

221 Đóng kết nối đã được thiết lập.

250 Thao tác do Client MTA yêu cầu đã được hoàn thành.

354 Sẵn sàng nhận nội dung của mail.

550 Thao tác yêu cầu không thực hiện được do không có mailbox trên máy.

.v.v...

#### *10.6.1.3 Phiên giao dịch SMTP*

Để hiểu cách dùng một số lệnh chúng ta xem xét qua ví dụ sau: Bên gởi tên Thuận ở máy Sample1 muốn gởi cho Tín , Thức ở máy Sample2, giả sử Thức không có Mailbox tại Sample2.

Bên gởi thực hiện một kết nối đến SMTP Server.

RECEIVER : 220 sample2 Simple Mail Transfer Service Ready
Khi được kết nối qua giao thức TCP/IP, máy nhận trả lời với mã 220
để báo cho máy gởi biết dịch vụ SMTP đã sẵn sàng.
SENDER : HELO sample1
Bên nhận đã sẵn sàng, bên gởi gởi HELLO và xưng tên người gởi.
RECEIVER : 250 sample2
Trả với mã 250 báo cho biết bên nhận đã sẵn sàng.
SENDER : MAIL FROM: <>
Bên gởi dùng lệnh MAIL để khởi động phiên giao dịch. Cú pháp trên cho bên nhận biết
địa chỉ bên gởi (mailbox của bên gởi) để bên nhận gởi thông báo lỗi nếu có về bên gởi.
RECEIVER : 250 OK
Trả lời với mã 250 cho biết đã chấp nhận.
SENDER: RCPT TO: <>
Bên gởi cho biết e-Mail đích
RECEIVER: 250 OK
Trả lời với mã 250 cho biết đã chấp nhận
SENDER : RCPT TO: <>
Muốn gởi cho bao nhiêu người dùng bấy nhiêu lệnh RCPT kèm theo địa chỉ nhận,
bên nhận nếu đúng sẽ trả về mã 250 kèm theo OK.
RECEIVER : 550 No such user here
Báo kèm theo mã 550 cho biết không có mailbox trên địa chỉ trên đối với nơi nhận.
SENDER : DATA
Báo cho bên nhận biết dữ liệu bắt đầu từ sau từ DATA.
RECEIVER : 354 Start mail input; end with <CRLF>.<CRLF>
Mã 354 báo cho biết đã sẵn sàng nhận mail, kết thúc mail với ký tự "CRLF.CRLF".
SENDER : Bắt đầu thân của mail
SENDER : . . .
SENDER : (đến khi kết thúc gởi CRLF.CRLF)
RECEIVER : 250 OK
E-Mail đã được chấp nhận.

SENDER : QUIT

Phát lệnh báo kết thúc phiên giao dịch.

RECEIVER : 221 sample2 Service closing transmission channel

Mã 221 đóng kết nối đã thiết lập

#### *10.6.1.4 Giao thức mở rộng ESMTP*

SMTP có một hạn chế gây khó khăn lớn trong việc truyền nhận mail là giới hạn tối đa kích thước nội dung một bức mail chỉ là 128KB. Do vậy người ta đã cải tiến chuẩn SMTP thành một chuẩn mở rộng mới gọi là ESMTP, cho phép tăng giới hạn kích thước của mail lên trên 1MB.

Để biết xem Server MTA có theo chuẩn ESMTP hay không, thay vì dùng lệnh HELO ở đầu một cuộc giao dịch, Client MTA dùng lệnh mới EHLO, nếu Server MTA có trang bị, nó sẽ trả về mã thành công là 250. Ngày nay chuẩn ESMTP đã thay thế chuẩn SMTP ở đa số các hệ thống.

Chẳng hạn để khởi động cuộc giao dịch với kích thước mail lên tới 1MB, sử dụng dòng lệnh sau:

MAIL FROM :<thuan@sample1> SIZE=1000000

### 10.6.2 MIME

Từ khi MIME (Multipurpose Internet Mail Extention) được đưa ra, kiểu dữ liệu mà user có thể gửi thông qua e-Mail được mở rộng. Ban đầu dữ liệu chỉ ở dạng text. Ngày nay, ta có thể gửi các tài liệu (file *.doc), các file ảnh hay các file âm thanh.

Để có thể phân phát các kiểu dữ liệu này, khuôn dạng các message trên Internet nên được mở rộng. MIME được phát triển cho mục đích này.

#### *10.6.2.1 Cấu trúc message của MIME*

MIME không phải cho các ứng dụng e-Mail mới, nhưng cho phép mở rộng khả năng e-Mail trên Internet trong khi vẫn giữ các ứng dụng giao vận và nền tảng hiện tại. Khuôn dạng MIME duy trì các cấu trúc message cơ bản với các phần Header và phần body (tham khảo RFC 822). Ví dụ về khuôn dạng của một tài liệu MIME như sau :

{Dòng này xác định MIME message}

MIME-Version: 1.0

To:

Subject: Book CD

{Dòng này xác định đây là một kiểu messsage hỗn hợp và các phần được phân tách nhau bởi dấu biên}

Content-Type: multipart/mixed; boundary="--------6B9767D111AE"

X-Mozilla-Status: 0001

{Kết thúc phần header}
{Biên đầu tiên, thể hiện phần đầu của message}

--------6B9767D111AE
{Đây là đoạn text, thể hiện các kí tự dạng US-ASCII}
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
{Kết thúc phần header}

Davis,
I am .....
Thanhs,
Davis
{Phần sau là phần đánh dấu biên}

--------6B9767D111AE
{Phần tiếp sau là một file nhị phân}
Content-Type: application/octet-stream
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="Sublic2.doc"
{Phần dưới đây là nội dung file}

0M8.....
{Phần sau đây là biên kết thúc file}

--------6B9767D111AE

### *10.6.2.2 MIME version header*

MIME version header định danh một message như một message MIME, và xác định version của MIME chuẩn để dịch message. Nếu không tìm thấy header, client sẽ đối xử với message theo khuôn dạng chuẩn trong RFC. Phiên bản hiện tại của MIME là 1.0. Cú pháp của MIME header version như sau:

MIME-Version: 1.0

*1. Content Type header*

Content Type header xác định khuôn dạng file được gán vào trong một đối tượng. Header báo cho MIME cách hiển thị hay thao tác trên thân của message. Content Type Header bao gồm tên của header, theo sau bởi kiểu MIME. Kiểu MIME theo sau hai tên và được cách biệt nhau bởi kí tự slash (/). Tên đầu tiên là tên kiểu và tên thứ hai là một tên phụ. Sau đây là các ví dụ của Content type header:

Content-Type: image/jpeg
Content-Type: image/gif
Content-Type: image/bmp
Content-Type: image/mpeg

Content-Type: application/octet-stream

Ba ví dụ đầu tiên trong phần này, đối tượng là kiểu ảnh (cũng là kiểu nhị phân), kiểu con của nó là jpeg, gif, và bmp. Các file ảnh này được nhúng vào trong các message. Dòng thứ tư trong các ví dụ này đó là một file chương trình.

Các kiểu và kiểu con có thể được thiết lập bởi các tham số. Mỗi tham số bao gồm một tên tham số, theo sau bởi dấu bằng (=) và tiếp theo là giá trị tham số. Các tham số này được tách biệt giữa kiểu và kiểu con, cũng như các tham số khác và được tách biệt nhau bởi dấu chấm phẩy. Ví dụ sau đây thể hiện một tập các tham số:

Content-Type: text/plain; charset=us-ascii

Kiểu đối tượng này báo cho người đọc message rằng các phần theo sau là dạng text và sử dụng các kí tự theo kiểu text.

Header này có thể hoàn toàn tuỳ chọn. Nếu nó không được cung cấp thì message được đối xử như một chuỗi các kí tự ASCII.

2. *Content Transfer Encoding Header*

Content Transfer Encoding Header xác định mô hình mã hoá được sử dụng để nhúng đối tượng vào trong thân của message. Để nhúng một đối tượng nhị phân vào trong một thư điện tử, cần phải chuyển nó sang kiểu dạng ASCII, do vậy nó được biên dịch theo khuôn dạng RFC 822. Ví dụ một cú pháp header dùng để mã hoá nội dung khi truyền là Content-Transfer-Encoding Base64.

Tài liệu MIME định nghĩa 5 kiểu mã hoá, nhưng 3 kiểu mã hoá thể hiện đối tượng không được mã hoá. Mã hoá 7 bit thường được dùng cho các vùng text theo khuôn dạng MIME. Hai kiểu kia mã hoá theo kiểu 8 bit và nhị phân, chỉ được sử dụng khi chuyển thư không phải SMTP, do SMTP chỉ cho phép các kí tự ASCII theo kiểu mã hoá 7 bit. Hai mô hình mã hoá còn lại đó là quoted-printable và base64 để chuyển các các đối tượng từ dạng nhị phân sang kiểu ASCII.

### *10.6.2.3 Cấu trúc message MIME đa phần*

Một trong số các khả năng phổ biến của MIME đó là có một message đa phần. Bằng cách sử dụng message đa phần, ta có thể nhúng cả hình ảnh và âm thanh vào các message text hay xây dựng một ứng dụng về một đối tượng hoạt hình, nó bao gồm một số file cần thiết để chạy ứng dụng.

Cấu trúc message đa phần bao gồm nhiều message kết hợp vào trong thân của một message, mỗi message với thông tin header của nó thể hiện kiểu nội dung mà mô hình mã hoá. Các phần này được tách biệt bởi các dấu biên mà message chính định ra. Để hiểu chi tiết về cấu trúc của một message đa phần, xem RFC 1521.

#### *10.6.2.4 Mã hóa BASE64*

Thuật toán mã hoá Base64 được thiết kế để mô tả một chuỗi tuỳ ý các giá trị 8bit mà con người không có khả năng đọc được thành các kí tự ASCII. Thuật toán mã hoá và giải mã đơn giản nhưng dữ liệu mã hoá sẽ lớn hơn dữ liệu nguồn 33%.

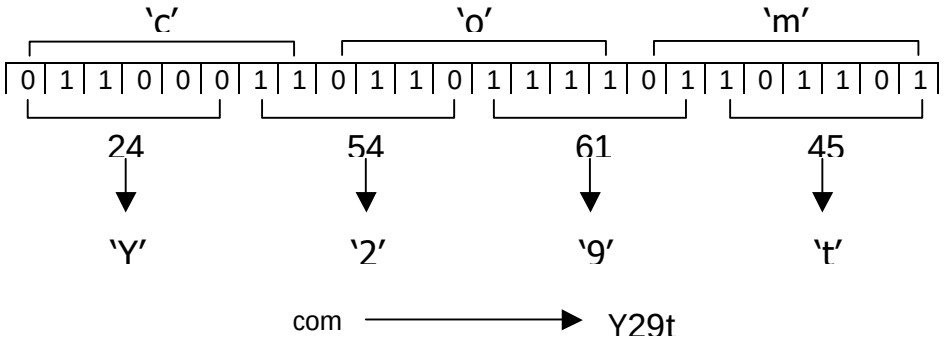
Một tập 65 kí tự US-ASCII được dùng, cho phép 6bits biểu diễn cho các kí tự có thể in được. (Kí tự thứ 65, "=", là một kí tự xử lý đặc biệt)

Tiến trình mã hoá biểu diễn nhóm 24 bits dữ liệu nhập thành 4 kí tự mã hoá ở đầu ra. Tiến trình thực hiện từ trái sang phải, một nhóm 24 bit nhập được kết hợp từ nhóm 3 kí tự 8bits. 24 bits đó được chia làm 4 nhóm kí tự 6bits, mỗi nhóm được dịch thành một kí tự đơn dựa vào bảng mã Base64.

**Bảng mã Base64**

| Value | Encoding | Value | Encoding | Value | Encoding | Value | Encoding |
|---|---|---|---|---|---|---|---|
| 0 | A | 17 | R | 34 | i | 51 | z |
| 1 | B | 18 | S | 35 | j | 52 | 0 |
| 2 | C | 19 | T | 36 | k | 53 | 1 |
| 3 | D | 20 | U | 37 | l | 54 | 2 |
| 4 | E | 21 | V | 38 | m | 55 | 3 |
| 5 | F | 22 | W | 39 | n | 56 | 4 |
| 6 | G | 23 | X | 40 | o | 57 | 5 |
| 7 | H | 24 | Y | 41 | p | 58 | 6 |
| 8 | I | 25 | Z | 42 | q | 59 | 7 |
| 9 | J | 26 | a | 43 | r | 60 | 8 |
| 10 | K | 27 | b | 44 | s | 61 | 9 |
| 11 | L | 28 | c | 45 | t | 62 | + |
| 12 | M | 29 | d | 46 | u | 63 | / |
| 13 | N | 30 | e | 47 | v | | |
| 14 | O | 31 | f | 48 | w | (pad) | = |
| 15 | P | 32 | g | 49 | x | | |
| 16 | Q | 33 | h | 50 | y | | |

Ví dụ sau mô tả tiến trình mã hoá 3 kí tự nhập là "com":




Luồng dữ liệu được mã hoá đầu ra phải được biểu diễn bằng các dòng có độ dài không lớn hơn 76 kí tự. Tất cả các kí tự xuống dòng hay các kí tự khác không có trong bảng mã Base64 đều được phần mềm giải mã bỏ qua.

Khi nhóm bit dòng nhập ít hơn 24 bits (nghĩa là đến cuối của dữ liệu cần mã hoá) thì cần có xử lý đặc biệt. Khi có ít hơn 24 bits dòng nhập thì các bits 0 được thêm vào phía bên phải nhóm bit để được đủ số 24 bits. Khi dòng nhập đã đủ 24bits thì có các khả năng có thể xảy ra:

1. Phần cuối cùng của dữ liệu cần mã hoá là 24 bits thì dữ liệu đầu ra cuối cùng sẽ là 4 kí tự đã mã hoá mà không có kí tự đệm "=".
2. Phần cuối cùng của dữ liệu cần mã hoá chính xác là 8 bits thì dữ liệu đầu ra cuối cùng sẽ là 2 kí tự đã mã hoá kèm theo với 2 kí tự đệm “=” ở cuối.

- Nếu phần cuối cùng của dữ liệu cần mã hoá chính xác là 16 bits thì dữ liệu đầu ra cuối cùng sẽ gồm 3 kí tự đã mã hoá kèm theo với 1 kí tự đệm “=” ở cuối.

Bởi vì các kí tự đệm chỉ được thêm vào cuối của dữ liệu nên khi gặp bất kì một kí tự “=” nào thì hiển nhiên là đã đến vị trí kết thúc của dữ liệu.

### 10.6.3 Giao thức POP

Người sử dụng có thể gửi thư bằng cách sử dụng SMTP, và có thể nhúng bất kỳ đối tượng nào vào trong message thông qua việc sử dụng khuôn dạng MIME. Tuy nhiên, với SMTP, server để nhận được các message thư phải nối đến client và gửi tất cả các message được phân phát cho client. Do đó, người sử dụng  phải đăng ký tên máy dưới dạng tên địa chỉ Internet của người nhận.

SMTP được thiết kế trong trường hợp nhiều user sử dụng tất cả thời gian của họ kết nối đến một vài host và chạy một phiên đầu cuối. Giao thức không được thiết kế cho các tình huống thông dụng hiện nay, trong đó, hầu hết tất cả các user sử dụng e-mail kết nối hạn chế đến mail server đang giữ hộp thư. Người sử dụng phải duy trì các message thư trên server và chuyển nó đến cho client khi client yêu cầu. Đây là một mục đích trong thiết kế của POP.

POP (Post office Protocol) được thiết kế để bù đắp cho SMTP trong phần nhận các message. Những người thiết kế POP không gộp các chức năng gửi message và cho rằng SMTP tiếp tục được sử dụng để thực hiện các chức năng đó. Với giao thức POP, máy tính  nhận khởi tạo kết nối. Máy nhận kết nối đến mail server, login và nhận bất kỳ một message nào đang chờ. Do vậy mà máy gửi không cần biết gì về máy nhận trừ khi nó sử dụng login và password để đăng nhập. Ngày nay, hầu hết tất cả các mail client trên Internet mà bạn có thể sử dụng để kết hợp cả SMTP và POP.

#### *10.6.3.1 Mô hình thông tin POP*

Trong mô hình lưu và phát, server mail cục bộ lưu các message đến khi các client nhận nó. POP client kết nối với server trên cổng 110 của TCP. Để đăng nhập vào server, user sử dụng định danh (ID) và password. Sau khi đăng nhập thành công vào server, client có thể yêu cầu server về các message mới đang sẵn sàng, lấy bất kỳ message nào mà server đang gửi hay xoá đi một message nào đó trên server.

Mô hình thông tin POP sử dụng 3 trạng thái giao tác để cung cấp chức năng này đến POP client:

- Trạng thái đặc quyền : Server kiểm tra quyền truy nhập của client (ID và password).
- Trạng thái giao tác : Client có thể nhận hay xoá các message.
- Trạng thái cập nhật : Trạng thái này được chuyển đến ngay sau khi client tạo ra lệnh QUIT.

Trạng thái cập nhật là trạng thái cho phép thao tác trên các message. Khi client đang ở trên trạng thái giao tác, bạn có thể tạo ra lệnh reset để huỷ bỏ tất cả các thao tác xóa trước đó (undo).

#### *10.6.3.2 Chuẩn POP3*

Giao thức POP3 được cải tiến từ giao thức POP. Nhiệm vụ của giao thức POP3 là lấy mail từ mailbox về khi nào người nhận muốn.

Đặc điểm của hệ thống dùng POP là cho phép người sử dụng login vào POP Server và nhận các mail từ mailbox của mình mà không cần phải login vào mạng mặc dù các mailbox thường nằm ở các Mail Server nằm trong mạng ( thông thường muốn thâm nhập mạng ta phải có một account trên mạng và phải cung cấp Password khi đăng nhập vào mạng ). Người sử dụng có thể truy xuất POP Server từ bất cứ một hệ thống nào trên mạng Internet, từ bất cứ UA nào dùng giao thức POP.

POP3 định nghĩa 3 giai đoạn tạo thành POP Session : Giai đoạn 1 là giai đoạn xác định tính hợp pháp của người nhận mail (Authorization); giai đoạn 2 là giai đoạn giao dịch giữa PC và POP Server (Transaction) và giai đoạn 3 là giai đoạn cập nhật thông tin (Update).

Sau khi thiết lập kết nối với Server, giai đoạn đầu Client sẽ cho Server biết nó là ai. Nếu Client hợp pháp POP Server sẽ mở Mailbox và bắt đầu chuyển sang giai đoạn giao dịch. Giai đoạn giao dịch, chương trình Client sẽ yêu cầu POP3 Server cung cấp các thông tin như danh sách mail..v..v..hay yêu cầu gởi về cho nó một bức mail xác định nào đó. Giai đoạn cuối cùng sẽ cập nhật và đóng kết hiện hành.

Các lệnh thông dụng của giao thức POP3 :

| Lệnh | ý nghĩa |
|---|---|
| **User** | Cho biết tên của user cho POP Server |
| **Pass** | Yêu cầu một Password cho người sử dụng trên Server |
| **Quit** | Đóng kết nối TCT đã được thiết lập trước đó |
| **Stat** | POP Server trả về số lượng Mail có trong mailbox của người sử dụng cùng kích thước chúng |
| **List** | Trả về các ID và size của các Message |
| **Retr** | Nhận một Message từ Mailbox (yêu cầu tham số là ID của mail cần nhận) |
| **Dele** | Đánh dấu một Message để xóa (yêu cầu tham số là ID của mail cần xóa) |
| **Noop** | POP Server trả về +OK nhưng không làm gì cả |
| **Last** | Yêu cầu POP Server trả về số Message đã truy nhập |
| **Top** | Liệt kê Header của Mail |
| **Rset** | Hủy đánh dấu trên Message bị đánh dấu để xóa |

POP3 chỉ định nghĩa 2 loại trả lời cho mỗi câu lệnh là : +OK để chỉ thao tác hoàn thành tốt và - ERR để báo có lỗi. Ví dụ cách dùng một số lệnh của POP3 như sau (các hàng sau dấu chấm phẩy để chú thích lệnh).

Giai đoạn 1 : Nhận dạng user

```
CLIENT : USER user01     ; cho biết tên user là user01
SERVER : +OK             ; báo thành công
CLIENT : PASS abc        ; cho biết password là abc
SERVER : +OK user01's    ; maildrop has 2 messages ( 520 octets)
```

Giai đoạn 2 : Trao đổi

```
CLIENT : STAT            ; số mail có trong mailbox
SERVER : +OK 2 520       ; Có 2 mail với tổng kích thước là 520
CLIENT : LIST            ; Liệt kê các ID và kích thước các mail
SERVER : +OK 2 message ( 520 octets )
SERVER : 1 110           ; mail thứ 1 kích thước 110
SERVER : 2 410           ; mail thứ 2 kích thước 410
CLIENT : LIST 1  ; Cho thông tin về mail có ID là 1
SERVER : +OK 1 110
CLIENT : LIST 4
SERVER : -ERR            no such message, only 2 message in maildrop
. . .v. . .v . . .
```

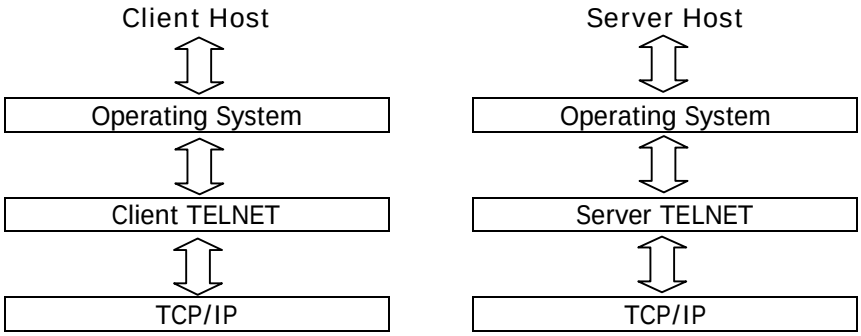
Giai đoạn 3 : Kết thúc

```
CLIENT : QUIT ; đóng kết nối TCP hiện hành
SERVER : +OK dhbk POP3 server signing off
```

Chú ý rằng các message bị đánh dấu để xóa bằng lệnh DELE thực sự chưa bị xóa ngay để nếu sau đó ta có thể dùng lệnh phục hồi không xóa bằng lệnh RSET,

chúng chỉ thực sự bị xóa bỏ khỏi maildrop khi bước vào giai đoạn Update (khi gởi lệnh QUIT).

## 10.7 Dịch vụ truy cập từ xa - TELNET




Hình 10-11. Phương thức truy nhập từ xa Telnet.

Chương trình Telnet (TELecommunication NETwork) cho phép truy cập từ xa hoặc có các thiết bị ảo thông qua mạng (điều này có nghĩa là bình thường thì bạn không thể có được thiết bị này nhưng nay nhờ có dịch vụ Telnet, bạn có thể truy cập và dùng được các thiết bị đầu cuối do đó gọi là các thiết bị đầu cuối ảo). Nói cách khác, một user A có thể truy cập vào một máy B ở bất cứ nơi nào trong mạng và làm việc với máy đó giống như đang ngồi trước máy đó. Dịch vụ Telnet được cung cấp qua cổng số 23 của TCP/IP. Khái niệm Telnet để chỉ cả *dịch vụ và giao thức* cung cấp các dịch vụ truy cập từ xa này.

Giao thức Telnet dùng một khái niệm Network ***Virtual Terminal*** (NVT), để định nghĩa kết nối Telnet cho cả hai phía. Mỗi đầu của kết nối (mỗi NVT) có một bàn phím và một máy in logic. Máy in logic có thể hiển thị các kí tự và bàn phím logic có thể tạo các kí tự. Máy in logic thường là một màn hình của thiết bị đầu cuối, trong khi đó bàn phím logic thường là bàn phím của người dùng

Khi một kết nối Telnet được thiết lập, Telnetd (hay bất kỳ một chương trình nào khác mà làm việc như là Telnet server) bắt đầu quá trình chạy một số các ứng dụng. Mỗi phím được ấn sẽ phải qua Telnet, Telnetd, và các ứng dụng được dùng trong quá trình thực hiện một phiên làm việc của kết nối Telnet.

Người sử dụng đưa vào lệnh và số liệu, chương trình Telnet ở máy khách (client Telnet) sẽ chuyển lệnh và số liệu đến chương trình Telnet trên máy chủ (server telnet) tương ứng. Server telnet xử lý và gửi kết quả trở lại cho Client Telnet.

### *10.7.1.1 Các lệnh của Telnet*

Hai hệ thống Telnet Client/Server liên lạc với nhau bằng những lệnh gồm những *kí tự đơn* hay một *chuỗi kí tự*, nó được mã hoá trong dạng chuẩn NVT (Network Virtual Terminal - Mạng đầu cuối ảo).

Khi một kết nối Telnet được thiết lập, một số dịch vụ có thể sẵn sàng để lựa chọn. Giá trị của chúng có thể thay đổi trong một phiên làm việc Telnet (*Telnet Session*) nếu cả hai phía của kết nối đồng ý sự thay đổi đó. (Có thể xảy ra trường hợp một đầu của kết nối Telnet không thể cho phép hay không cho phép một dịch vụ trong quá trình kết nối Telnet diễn ra do sự cho quyền của nhà quản lý hoặc các thiết lập nguồn (Source settings)). Có bốn giao thức Telnet được dùng để Để nghị (offer), Từ chối (refuse), Yêu cầu (request) và Ngăn chặn (prevent) các dịch vụ, đó là các động từ: WILL, WON'T, DO và DON'T. Các động từ trên được thiết kế đi với nhau theo từng cặp ( WILL/WON'T và DO/DON'T).

| **Lệnh** | **Mã thập phân** | **ý nghĩa** |
|---|---|---|
| IAC | 255 | Nhận biết byte tiếp theo là lệnh |
| NOP | 241 | Không điều khiển |
| EC | 247 | Xóa ký tự (Erase character) |
| EL | 248 | Xóa dòng (Erase line) |
| GA | 249 | Về đầu (Go ahead) |
| AYT | 246 | Are you there |
| IP | 244 | Quá trình ngắt (Interrupt process) |
| AO | 245 | Xóa bỏ đầu ra (Abort output) |
| BRK | 243 | Dừng (break output) |
| DMARK | 242 | Phục hồi đầu ra (Resume output) |
| SB | 250 | Bắt đầu trao đổi (Start potion request) |
| SE | 240 | Kết thúc (End) |
| WILL | 251 | Thỏa thuận/Yêu cầu (Agreement/request option) |
| WONT | 252 | Từ chối (Refuse option request) |
| DO | 253 | Tiếp nhận yêu cầu (Accept request option) |
| DON'T | 254 | Từ chối tiếp nhận yêu cầu |

- Các hàm chức năng khác :

| **Tên** | **Mã** | **ý nghĩa** |
|---|---|---|
| Transmit binary | 0 | Yêu cầu/T.nhận trao đổi số nhị phân 8 bit |
| Echo | 1 | Ký tự phản hồi (Echo character receiving back to sender) |
| Status | 5 | Trạng thái (Request/reply status of receiving TELNET) |
| Timing mark | 6 | Đánh dấu thời gian. |
| Terminal type | 24 | Loại yêu cầu/trả lời của thiết bị đầu cuối. |
| Line mode | 34 | Gửi dòng ký tự |

Ví dụ các dòng lệnh tiêu biểu như sau :

IAC, SB, WILL, 'O', SE : Yêu cầu bên nhận nhận số nhị phân 8 bit
IAC, SB, DO, 'O', SE : Hệ truy nhập từ xa nhận trả lời tiếp nhận
IAC, SB, DON'T, 'O', SE : Hoặc từ chối
IAC, SB, DO, 'O', SE : Bên nhận yêu cầu
IAC, SB, WILL, 'O', SE : Bên gửi thỏa thuận
IAC, SB, WON'T, 'O', SE : Hoặc từ chối

- Làm việc với Telnet

- Truy nhập vào mạng TCP/IP từ máy trạm
- Gõ lệnh : telnet <ĐịachỉIP hoặc tênmáyServer>
- Thao tác trên màn hình Telnet.

### 10.7.2 Dịch vụ truyền tập tin FTP

Giao thức truyền tập tin FTP (File Transfer Protocol) cho phép truyền các tập tin giữa hai máy tính, quản lý các thư mục và truy cập vào thư tín điện tử. FTP không được thiết kế để truy cập vào một máy khác và chạy các chương trình ở máy đó. FTP giúp người sử dụng truy cập file và thư mục trên một máy chủ ở xa và thực hiện những thao tác trên thư mục như sau :

- Liệt kê các file trên một thư mục cục bộ hay ở xa.
- Đổi tên và xóa tập tin (nếu có quyền).
- Truyền file đi hay về từ trạm và máy ở xa (download/upload).

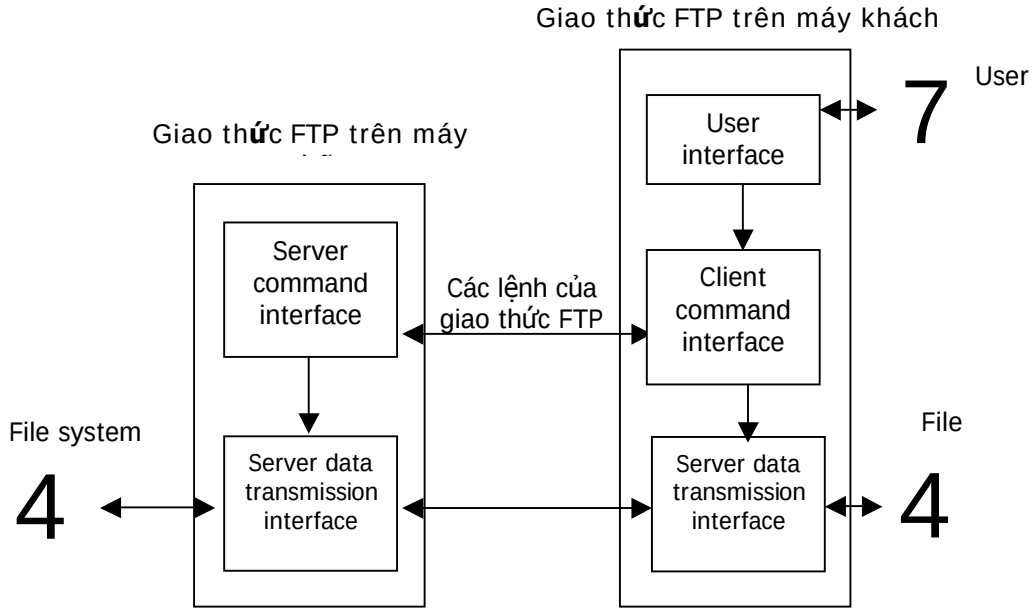
FTP dùng hai kênh TCP, với số hiệu cổng 20 là ***kênh dữ liệu***, và số hiệu cổng 21 là ***kênh lệnh*** (*command channel*). FTP khác các ứng dụng khác của TCP/IP ở là FTP quản lý tất cả việc truyền các tập tin bằng foreground thay vì background. Nói cách khác, FTP không dùng các hàng đợi hay các tiến trình kiểu ống (spooler) do đó bạn có thể quan sát quá trình truyền tập tin trong thời gian thực. Bằng cách dùng TCP, FTP loại trừ được việc quản lý kết nối và độ tin cậy, bởi vì FTP có thể dựa trên TCP để thực hiện các chức năng này một cách chính xác.

Kết nối đầu tiên, kênh lệnh, được khởi tạo thông qua FTP client. Client kết nối với server dựa trên cổng 21 của TCP, cung cấp cho server tên (login) và password và sau đó tiến đến các phiên FTP. Nếu client tạo ra một lệnh yêu cầu một dòng trả lời từ server, kênh lệnh sẽ truyền trả lời này.

Khi client gởi một yêu cầu có nhiều hơn một trả lời để gửi hay nhận dữ liệu, kênh thứ hai được đặt vào hoạt động. Để thiết lập kết nối thứ hai, bạn có 3 tuỳ chọn. Mặc định, server khởi tạo kết nối thứ 2 thông qua cổng 20 của TCP và kết nối đến một socket thứ hai trên client, sử dụng cùng một địa chỉ và cổng như trong kết nối thứ nhất trên client. Tuy nhiên, client có thể chỉ định một địa chỉ khác hay một cổng khác để truyền dữ liệu, trong trường hợp này, server cố gắng kết nối đến client

thông qua việc sử dụng một địa chỉ mới. Tuỳ chọn thứ 3 là client khởi tạo một kết nối truyền dữ liệu là báo cho server chuyển sang chế độ thụ động, server trả lời một địa chỉ và số hiệu cổng để truyền dữ liệu.

Ngay sau khi truyền dữ liệu kết thúc, kết nối để truyền dữ liệu được đóng lại. Kết nối này được mở lại khi client tạo ra một lệnh yêu cầu truyền dữ liÖu.




Hình 10-12. Mô hình giao tiếp FTP.

- FTP hoạt động theo mô hình Client/Server bao gồm thành phần chính :

  + Đơn vị trao đổi dữ liệu (Data Transmission interface)/

  + Đơn vị nhận biết lệnh (Command interface)

### *10.7.2.1 Chế độ truyền dẫn*

Có 3 chế độ được dùng để truyền dữ liệu giữa hai hệ thống. Chế độ đầu tiên là ngầm định nhưng 2 chế độ kia truyền hiệu quả hơn và có thể phục hồi.

- ***Truyền theo dòng:*** đây là chế độ truyền ngầm định, gửi một file dưới dạng một chuỗi các byte; FTP server và client không định dạng file đó. File nguồn không có cách gì để báo hết nội dung truyền, do vậy vấn đề kết thúc file được qui định bằng đóng kết nối dữ liệu.
- ***Truyền theo khối:*** chia file thành các khối, và mỗi khối có thêm các byte điều khiển (header). Trong header có một trường xác định số lượng byte trong khối, trường mô tả mã, nó có thể định đó là khối đặc biệt, kết thúc trong quá trình truyền. Chế độ truyền này cho phép phục hồi khi bị ngắt trong quá trình truyền file thông qua việc báo truyền lại một khối chỉ định trong trường count của header.

- ***Chế độ truyền nén:*** nén file để truyền thông qua việc sử dụng thuật toán mã hoá mã run-length. Thuật toán nhằm làm giảm các byte lặp lại vào trong hai byte kế tiếp. Byte đầu tiên cho biết byte theo sau là nén và số lần nó được lặp lại. Để thể hiện nén, bit đầu tiên của byte điều khiển được thiết lập 1. Nếu bit này là 0, nó cho biết byte theo sau không phải là byte nén. Phần còn lại của byte điều khiển xác định số lượng các byte không nén theo sau. Do vậy, hiệu quả khi nén các kí tự lặp lại đó là không làm mất đi các kí tự không nén.

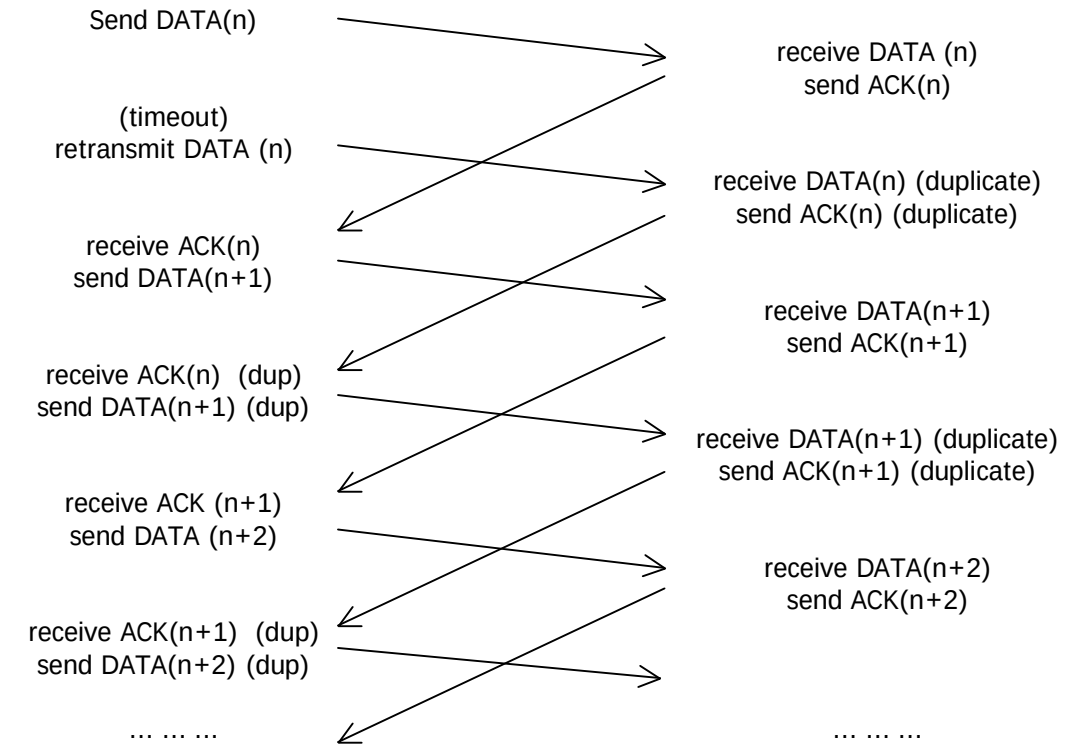
Để bắt đầu, client gửi yêu cầu **read** hay **write**. Gói tin trao đổi có độ dài đến 512 bytes. Mỗi block số liệu có đánh số và phải được biên nhận để gửi tiếp hay phát lại. Để tránh phát trùng lặp khi hết thời hạn, phát lại bản tin vừa phát và khi nhận ACK (n) trùng lặp thì không phát gì .

### *10.7.2.2 Dạng bản tin FTP*

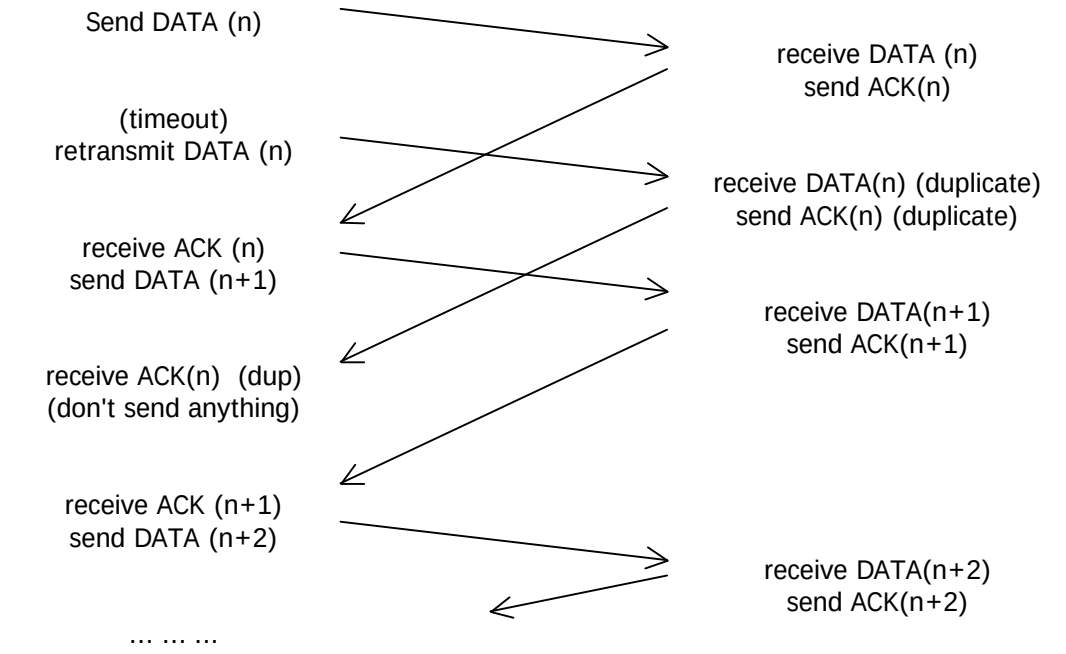
| | | | | | |
|---|---|---|---|---|---|
| Read request (RRQ) | opcode | String | EOs | String | EOs |
| | 01 | File name | 0 | mode | 0 |
| | 2 bytes | n bytes | 1 byte | n bytes | 1 byte |
| Write request (WRQ) | opcode | String | EOs | String | EOs |
| | 02 | File name | 0 | mode | 0 |
| | 2 bytes | n bytes | 1 byte | n bytes | 1 byte |
| DATA | opcode | Block# | Data | | |
| | 03 | | | | |
| | 2 bytes | 2 bytes | n bytes, 0≤n≤512 | | |
| Acknowled-gement (ACK) | opcode | Block# | | | |
| | 04 | | | | |
| | 2 bytes | 2 bytes | | | |
| Read request (RRQ) | opcode | | String | EOs | |
| | 05 | Errorcode | Err String | 0 | (EOs : End of String) |
| | 2 bytes | 2 bytes | n bytes | 1 byte | |

Hình 10-13. Khuôn dạng bản tin FTP.

*Ví dụ:* Quá trình phát lặp :




+ Tr¸nh ph¸t lÆp




Hình 10-14. Quá trình phát lặp bản tin FTP.

### *10.7.2.3 Quá trình làm việc FTP*

1. Truy nhập vào mạng TCP/IP từ máy trạm.
2. Gõ lệnh : ftp <Địa_chỉ_máy_Server>.
3. Làm việc với FTP.

Khi một kết nối FTP được thiết lập, thực hiện các bước như sau:

- Duyệt tên và mật khẩu (ID) của người dùng.
- Xác định thư mục bắt đầu làm việc.
- Định nghĩa chế độ truyền tập tin.
- Cho phép các lệnh của người dùng.
- Huỷ kết nối.

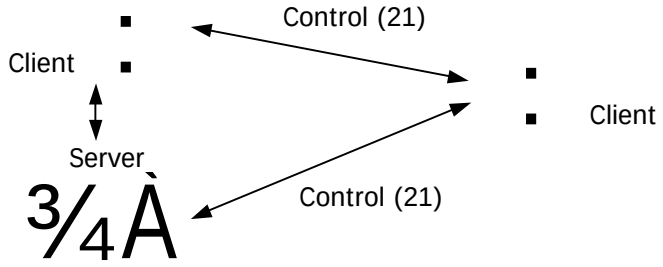
| **Lệnh FTP** | **Mô tả** |
|---|---|
| ascii | Chuyển sang chế độ truyền ascii |
| bell | âm thanh của chương trình sau khi truyền mỗi tập tin |
| binary | Chuyển sang chế độ truyền nhị phân |
| cd *directory* | Chuyển đổi thư mục hiện hành trên server |
| cdup | Lùi thư mục hiện hành về một cấp trước đó |
| close | Huỷ kết nối |
| delete *filename* | Xoá một tập tin trên server |
| dir *directory* | Hiển thị thư mục *directory* của server |
| get *filename* | Truyền tập tin trên server về máy cục bộ |
| hash | Hiển thị/làm mất dấu # cho mỗi khối các ký tự đã truyền được |
| help | Hiển thị các trợ giúp |
| lcd *directory* | Chuyển đổi thư mục hiện hành trên máy cục bộ |
| ls *directory* | Xem danh sách các tập tin trong thư mục directory trên Server |
| mdelete *files* | Xóa nhiều tập tin trên máy Server |
| mdir *directories* | Liệt kê các tập tin trong nhiều thư mục trên máy Server |
| mget *files* | Lấy một số file trên Server về thư mục hiện hành của máy cục bộ |
| mkdir *directory* | Tạo thư mục directory trên máy Server |
| mput *files* | Gửi một số tập tin từ máy cục bộ lên máy Server |
| open *host* | Kết nối với Server host từ xa |
| put *filename* | Truyền tập tin từ máy cục bộ lên máy Server |
| pwd | Hiển thị thư mục hiện thời của server |
| status | Hiển thị trạng thái của ftp |
| rename *file1 file2* | Đổi tên *file1* trên máy Server thành *file2* |
| quote | Cung cấp một lệnh FTP một cách trực tiếp |
| quit | Chấm dứt kết nối và thoát khỏi ftp |
| ? | Hiển thị danh sách lệnh |

Đề truyền một tập tin từ *thư mục hiện hành* trên máy Client đến máy Server bạn dùng lệnh *put*, ngược lại, muốn tải tập tin từ máy Server về máy Client, bạn dùng lệnh *get*. Cú pháp như sau :

```
ftp>put   local_file   remote_file
ftp>get   remote_file   local_file
```

Khi truy cập vào hệ thống, nếu chưa có account, người sử dụng có thể sử dụng một login name đặc biệt là *anonymous* để truy cập vào hệ thống. Acount này không có mật khẩu.

FTP cho phép truyền các tập tin thông qua máy thứ 3, máy này nằm giữa client và server. Thủ tục này được gọi là truyền tay ba điều này cần thiết để có được có được sự cho phép chính xác để truy cập vào máy ở xa. Hình sau mô tả sơ đồ của thủ tục này :




Hình 10-15. Truyền các tập tin thông qua máy thứ 3.

#### *10.7.2.4 Khuôn dạng dữ liệu*

Khi truyền dữ liệu giữa hai hệ thống, có thể sử dụng 4 kiểu dữ liệu để truyền. Trong số các kiểu dữ liệu này thì có 2 kiểu dữ liệu hay được sử dụng nhất hiện nay, hai kiểu khác vẫn được hỗ trợ nhưng ít được sử dụng. Các hệ thống ở cả hai đầu trong quá trình đàm thoại FTP phải hỗ trợ tất cả các kiểu dữ liệu sau đây:

- Kiểu ASCII, đây là kiểu mặc định được dùng trong các phiên FTP. Nó được dùng để truyền các file text. Nếu bạn cố truyền các file nhị phân mà bạn không thay đổi mode thì bạn cũng nhận được kết quả ở dạng text, do vậy nội dung của file đã bị thay đổi.
- EBCDIC được sử dụng để truyền các file giữa giữa các host, sử dụng EBCDIC như một tập các kí tự bên trong của nó. Về mặt kỹ thuật thì kiểu dữ liệu ASCII và EBCDIC là giống nhau, chỉ khác một điều là tập các kí tự mà nó sử dụng
- Kiểu nhị phân là kiểu được sử dụng để truyền các file nhị phân như các file ảnh và các file chương trình (các file ZIP và các file DOC). Việc truyền các file này dưới dạng một chuỗi các byte, kiểu dữ liệu này không quan tâm đến môi trường của máy đích và cấu trúc từ. Tất cả các cài đặt FTP nên hỗ trợ kiểu truyền dữ liệu này cũng như kiểu ASCII.
- Kiểu dữ liệu cục bộ. Kiểu dữ liệu này dựa trên byte, xác định cho các host cục bộ. Khuôn dạng phải khả dụng với các hệ thống khác để cấu trúc lại dữ liệu dựa vào dựa trên khuôn dạng ban đầu.

Kiểu dữ liệu ASCII và EBCDIC có thể có tham số tuỳ chọn thứ hai để xác định các ràng buộc dữ liệu. Khi được sử dụng, tham số này là một tuỳ chọn được thêm vào để xác định kiểu dữ liệu. Các ràng buộc định dạng phụ thuộc vào việc sử dụng của file được truyền. Liệu một file có thể được in, xem, hay được xử lí như một đầu vào. Việc định dạng một file có thể khác nhau ở mỗi đích. Các khuôn dạng dữ liệu sau được ít sử dụng hơn kiển dữ liệu ngầm định:

- Khuôn dạng không in: là kiểu dữ liệu ngầm định ASCII và EBCDIC. Khuôn dạng file này không có thông tin định dạng. Chú ý rằng, định dạng sử các dạng chuẩn cho kí tự cách và phân lề.
- Định dạng Telnet được sử dụng cho các file một thiết bị đầu cuối dùng để hiển thị. Định dạng này gồm các kí tự điều khiển, kí tự xuống dòng, tab.
- Kiểm soát di chuyển bao gồm các kí tự điều khiển định dạng in. Theo khuôn dạng này, kí tự đầu tiên của mỗi dòng không được in ra. Thay vào đó, kí tự này xác định sự di chuyển theo trục đứng so với mép giấy trước khi một bản ghi hay một dòng nào đó được in ra.

#### *10.7.2.5 Các cấu trúc dữ liệu*

Giao thức FTP cho phép truyền các file có cấu trúc với 3 cấu trúc file khác nhau. Các cấu trúc tập tin này chủ yếu dùng để truyền các tập tin giữa các hệ thống có cấu trúc lưu trữ khác nhau. Có các dạng như sau :

- Cấu trúc theo kiểu file, xem file một chuỗi các byte dữ liệu nối tiếp nhau mà không được cấu trúc bên trong.
- Cấu trúc bản ghi được sử dụng để truyền các file là một chuỗi các bản ghi. Cấu trúc này được sử dụng cho các Host IBM nhưng hiện nay ít sử dụng.
- Cấu trúc trang được sử dụng cho các file được chia thành các đối tượng với kích thước khác nhau, có thể có các thông tin khác được thêm vào trong đó. Cấu trúc trang có một cấu trúc header để định nghĩa kích thước của trang, theo sau là nội dung của trang. Header của mỗi trang còn chứa số hiệu trang logic của các trang dữ liệu nhưng số hiệu trang đó không cần thiết khi truyền.

### 10.7.3 UserNEWS

| Biểu tượng | Ý nghĩa | Biểu tượng | Ý nghĩa |
|---|---|---|---|
| :-) | Tôi hạnh phúc | =):=) | ABC Lincol |
| :-( | Tôi buồn/ tức giận | =):=) | Bác Sorn |
| :-\| | Tôi thờ ơ | *<:-) | ông già Noel |
| ;-) | Tôi nháy mắt | <:-( | Người tối dạ |
| ;-(0) | Tôi kêu la | (-: | Người Uực |
| :-(*) | Người nôn (mửa) | :-)x | Man with bowtic |
| :+) | Cằm chẻ | # -) | Tóc mướt |
| :-)) | Cằm chẻ | 8 -) | Mang kính |
| :-{) | Ria | C:-) | Mão lớn |

Khi mà có nhiều người thuê bao USENET, nhu cầu về những newsgroup mới, chuyên biệt hơn luôn được đòi hỏi. Kết quả là một thủ tục để tạo ra newsgroup mới, chuyên biệt hơn luôn được đòi hỏi. Kết quả là một thủ tục để tạo ra những

Newsgroup mới được. Trên Newsgroup, người ta có thể thảo luận, bầu cử, trao đổi với nhau.

### 10.7.4 WORLD-WIDE-WEB

World Wide Web (WWW) là một hệ thống quản lý thông tin phi cấu trúc. Bao gồm các Server cung cấp thông tin theo định dạng siêu văn bản (Hypertext) và các client (Browser, trình duyệt) nhận thông tin từ người sử dụng và đồng thời hiển thị thông tin mà các Server cung cấp theo định dạng được chỉ định bởi người sử dụng.

Thông tin trên WWW được biểu diễn trong các trang Web. Mỗi trang Web có thể là một chỉ mục hoặc một tài liệu chứa văn bản, hình ảnh, âm thanh, các liên kết... Người sử dụng có thể truy cập thông tin cần thiết trên WWW thông qua các đối tượng đã được đánh dấu trong tài liệu.

Các lệnh được dùng với WWW đã được định nghĩa trong giao thức HTTP (HyperText Transfer Protocol). Đây là giao thức chuẩn để liên lạc giữa Client và Server. Yêu cầu được gửi tới Server thông qua Client. Server xử lý các yêu cầu và gửi kết quả về cho Client  yêu cầu. Kết quả sẽ được trình bày dưới dạng thích hợp cho người sử dụng.

- Phía máy chủ

Mỗi web Site có một máy chủ đảm nhận việc “lắng nghe” TCP tại cổng 80 cho những kết nối đến từ các máy khách (thường là các trình duyệt). Sau khi một kết nối được thiết lập, máy khách gửi yêu cầu và máy chủ trả lời đáp lại, kết nối chấm dứt. Giao thức HTTP định nghĩa cho các yêu cầu và trả lời hợp lệ.

Ví dụ người dùng kích lên một mẫu văn bản hoặc có thể là biểu tượng trỏ đến trang có tên (tức là URL hay địa chỉ tới máy trạm Internet). Một URL có 3 phần sau: tên của giao thức (http), tên của máy nơi có chứa trang web, và tên của tập tin chứa trang đó (hypetext/WWW/TheProject.html). Từ khi người dùng nhấp chuột cho đến khi trang web được hiện ra trên màn hình đã xảy ra các sự kiện sau :

1. Trình duyệt kiểm tra URL (xem xét đối tượng được chọn là gì).
2. Trình duyệt hỏi DNS về địa chỉ IP của URL.
3. DNS trả lời là 18.23.0.23
4. Trình duyệt tạo một kết nối TCP đến cổng 80 trên địa chỉ 18.23.0.23
5. Trình duyệt gửi lệnh GET /hypetext/WWW/TheProject.html.
6. Máy chủ  gửi đến tập tin TheProject.html
7. Giải phóng kết nối TCP.

8. Trình duyệt hiển thị tất cả các văn bản trong tập tin TheProject.html.
9. Trình duyệt tiếp tục lấy về và hiển thị tất cả các hình ảnh có trong TheProject.html.

#### *10.7.4.1 Ngôn ngữ HTML*

HTML (HyperText Markup Laguage) là một ngôn ngữ HTML là một ngôn ngữ có cấu trúc, nó bao gồm các thẻ (TAGS) và các thực thể (ENTITY), dùng để cung cấp các chỉ thị định dạng để phục vụ cho việc trình bày văn bản trên Web.

Một tập tin HTML là một tập tin văn bản trong đó một số xâu ký tự được coi là các thẻ đánh dấu các vùng tài liệu và ấn định các ý nghĩa đặc biệt cho chúng. Các thẻ là các xâu ký tự được bắt đầu là dấu nhỏ hơn (<) và kết thúc bằng dấu lớn hơn (>). Các thẻ có thể được phân làm nhiều loại tùy theo nội dung, chức năng, kiểu tác động của chúng như: Thẻ mô tả định dạng, thẻ mô tả cấu trúc, thẻ rỗng, thẻ chứa...

Cấu trúc tổng quát của một tài liệu HTML như sau :

<HTML> *Thông báo cho trình duyệt đây là một văn bản tài liệu HTML*
<HEAD> *Thông báo bắt đầu phần đầu của tài liệu*
<TITLE> *Tiêu đề của tài liệu* </TITLE>
Phần đầu của tài liệu đặt tại đây
</HEAD> *Kết thúc phần đầu*
<BODY> *Thông báo bắt đầu phần thân tài liệu*
.....
Nội dung tài liệu HTML được đặt tại đây
</BODY> *Kết thúc phần thân tài liệu*
</HTML> *Kết thúc tài liệu HTML*

Phần đầu đề của tài liệu HTML thường chứa tiêu đề của tài liệu, tên tác giả, lời chú thích, tóm tắt... Đây là phần giúp ích cho việc tìm kiếm thông tin trên WEB hoặc cho các dịch vụ tìm kiếm có thể đánh chỉ mục, tiến hành tìm kiếm một cách dễ dàng. Một số các thẻ phục vụ trong phần đầu như: Title, Meta, Isindex...

Phần thân là phần chính của tài liệu HTML, nằm giữa cặp thẻ <BODY> và </BODY>, nó định nghĩa, hiển thị toàn bộ nội dung bên trong của tài liệu. Trong phần thân ta có thể sử dụng các thẻ để định dạng văn bản, chèn các hình ảnh, bảng biểu, liên kết...

Người sử dụng có thể tạo một tài liệu HTML bằng cách sử dụng các trình soạn thảo Web chuyên dụng như Microsoft Front Page 2000, hoặc Microsoft Word, Notepad ...

Một số thẻ HTML quan trọng :

### 1. *Thẻ <!-- (chú thích) -->:*

Dùng để thêm những dòng chú thích trong file HTML, người ta dùng thẻ nầy. Nội dung văn bản nằm giữa <!-- và --> sẽ được chương trình Browse bỏ qua. Cho phép có khoảnh trắng giữa -- và >, nhưng không được có khoảng trắng giữa <! và -- .

Thí dụ:

<HEAD> <TITLE>The HTML Reference</TITLE>

<!-- Created by Nguyen Tan Khoi, April 1996 --> </HEAD>

### 2. *Thẻ <A>*

Dùng để tạo các siêu liên kết (HyperLink). WWW cho phép kết nối và giao tiếp giữa các tài nguyên một cách dễ dàng nhờ định nghĩa các loại liên kết sau:

1. Liên kết giữa các thành phần khác nhau trong một tài liệu HTML.
2. Liên kết giữa các tài liệu HTML khác nhau.
3. Liên kết với các dạng tài liệu Multimedia.
4. Truy cập tới các dịch vụ thông tin khác trên mạng Intranet/Internet

Các thuộc tính của thẻ <A> như sau:

*a. Liên kết đến điểm neo trong trang HTML*

- NAME: Thuộc tính NAME xác định một vị trí để những thành phần khác trong tài liệu hoặc trong tài liệu khác có thể tham trỏ đến (gọi là điểm neo trong tài liệu HTML). Thí dụ :

  <A NAME="coffee"> Coffee</A>

  Các tài liệu khác có thể liên kết với tài liệu này ngay tại vị trí xác định.

*b. Liên kết đến một trang HTML*

<A HREF = "URL_HTML[#Name_Anchor]"> *Nội dung thông báo* </A>

Trong đó URL_HTML là địa chỉ để tham chiếu tới tài liệu HTML.

Nếu chỉ ra Name_Anchor thì có nghĩa ta định nghĩa một điểm neo dùng để chuyển đến một vị trí được quy định sẵn trong tài liệu HTML này. Thí dụ:

The <A HREF="document.html#glossary"> GLOSSARY </A>

Trong thí dụ trên, nếu kích vào "GLOSSARY" sẽ được chuyển đến tài liệu document.html, ngay tại vị trí điểm neo có tên glossary trong tài liệu này.

c. *Liên kết với các kiểu dữ liệu khác nhau*

Để liên kết giữa tài liệu hiện thời với các kiểu dữ liệu khác nhau như: hình ảnh, âm thanh, video...

<A HREF ="URL_DATA"> ...</A>

Trong đó URL_DATA là địa chỉ tới kiểu dữ liệu cần liên kết. Ví dụ:

<A HREF ="car.jpg">

<IMG SRC ="carla.gif" WIDTH=87 HEIGHT=60> </A>

d. *Liên kết với các dịch vụ thông tin khác trên mạng*

<A HREF = "URL_Service" > ... </A>

Trong đó URL_Service là một địa chỉ đến các dịch vụ trên internet.

<A HREF="http://..."> Liên kết với 1 Web Site.

<A HREF="ftp://..."> Với 1 Ftp Site.

<A HREF="gopher://..."> Với 1 Gopher server.

<A HREF="news:..."> Liên kết với 1 nhóm Tin.

<A HREF="mailto:..."> liên kết tới 1 địa chỉ gởi Mail. Liên kết nầy sẽ kích hoạt chương trình Mail và tự động điền địa chỉ vào mục To dùm bạn. Bạn có thể khai báo luôn cả chủ đề thư (?subject).

Thí dụ: <A HREF="mailto:cmlehunt@swan.ac.uk?

subject=The HTMLib is fantastic">link text</A>

- TARGET: Chương trình Browser có thể nạp đối tượng liên kết vào 1 cửa sổ chỉ định bằng thẻ nầy. Nếu cửa sổ nầy cha có, trình Browse sẽ mở 1 cửa sổ mới. Chủ yếu thẻ nầy dùng cho frames.

  Dạng chung:

  <A HREF="url.html" TARGET="window_name">Link text</A>

  Trong đó window_name là tên đặt cho Frame.

  Khi kích chuột vào dòng "Link text", trang "url.html" sẽ được nạp vào frame có tên chỉ định.

Ngoài ra ta còn có thể chèn thêm các Script sau vào thẻ <A> dựa vào các phương thức như sau :

| Phương thức | Giải thích |
|---|---|
| OnMouseOver | Khi bạn di chuyển Mouse đến liên kết, sẽ có 1 dòng văn bản mô tả xuất hiện trong thanh trạng thái của trình Browse. Thí dụ:<br><A HREF="index.html"<br>OnMouseOver="self.status=('Back to the main page')">Link text</A><br>Dòng chữ "Back to the main page" sẽ hiện trong thanh trạng thái khi dời Mouse đến chữ "Link text". |
| OnMouseOut | Tương tự như trên nhưng dòng chữ nầy lại xuất hiện khi kéo Mouse ra khỏi liên kết. Thí dụ:<br><A HREF="index.html"<br>OnMouseOut="alert('Oh please go to this document')">Link text</A> |
| OnClick | Khi bấm Mouse lên liên kết, sẽ xuất hiện hộp thoại yêu cầu xác nhận. Thí dụ:<br><A HREF="http://www.netscape.com/"<br>OnClick="confirm('Are you want to go to the Netscape site?')">Link text</A> |

### 3. *Thẻ <INPUT>*

Dùng để tạo một field để nhận tác động của người sử dụng.

<INPUT TYPE = "*Kiểu*" NAMQ = "*TênĐT*"
SIZQ = "*KíchThước*"
VALUQ = "*Giatri*" MAXLQNGTH = "n" . . . >

Các thuộc tính:

| Thuộc tính | Giải thích |
|---|---|
| ALIGN | So hàng cho field. |
| CHECKED | Kiểm tra người dùng đã đánh dấu cho checkbox hay radio button chưa. |
| MAXLENGTH | Chỉ định độ dài ký tự có thể nhập vào text field, độ dài nầy có thể lớn hơn kích thước Text field. Mặc định là không giới hạn. |

| | |
|---|---|
| NAME | Tên của Field. |
| SIZE | Khai báo kích thước hay số lượng ký tự cho field. |

- TYPE: Chỉ định kiểu của Field:

| Giá trị | Giải thích |
|---|---|
| BUTTON | Chèn một nút bấm vào tài liệu. Giá trị VALUE dùng chỉ định Text sẽ hiện trong nút nầy. Thí dụ:<br><input type="button" value="hello" name="btnhello"> |
| HIDDEN | Với thuộc tính nầy, field sẽ không hiển thị ra nhưng nội dung của field vẫn có giá trị. Dùng trao đổi thông tin ngầm giữa Client/Server. |
| PASSWORD | Giống như Text, nhưng ký tự nhập vào sẽ không hiển thị ra. |
| CHECKBOX | Chèn 1 chechbox vào tài liệu. Thí dụ :<br> So thich<br><input type="checkbox" name="C1" value="ĂN">The thao<br><input type="checkbox" name="C2" value="ĂN">Xem phim |
| RADIO | Chèn 1 field có dạng nút Radio. Ví dụ :<br> Gioi tinh<br><input type="radio" checked value="V1" name="R1">Nam<br><input type="radio" name="R2" value="V2">Nu |
| RESET | Chèn 1 nút bấm dùng phục hồi lại tình trạng cũ cho các field. Đặt tên của nút nầy qua thuộc tính Values. |
| SUBMIT | Một dạng nút bấm giống RỌSỌT. Có tác dụng giống nh xác nhận đồng ý. Thí dụ:<br> <input type="submit" value="Submit" name="B1"><br><input type="reset" value="Reset" name="B2"> <br>Chèn 1 nút có tên "SUBMIT" và sẽ hiển thị thông báo "Xin chao các bạn" khi người sử dụng Mouse vào nút nầy :<br><INPUT TYPE="SUBMIT" OnClick="Xin chao các bạn'"> |
| TEXT | Nhập 1 dòng text vào fields. Dùng thuộc tính SIZỌ và MAXLENGTH để quy định kích thước. Trong trường hợp cần nhập |

| | |
|---|---|
| | nhiều dòng, phải dùng thẻ <TEXTAREA>. |
| VALUE | Chỉ định Text sẽ hiển thị trên các nút bấm. |
| IMAGE | Chèn field chứa hình ảnh để người dùng bấm Mouse khi chọn.<br><INPUT TYPE="IMAGE" SRC="../ iexplore.gif" ALIGN="middle"> |

### 4. *Thẻ TEXTAREA*

Cho phép nhập nhiều dòng văn bản vào một hộp Text.

Thí dụ:

```
<TEXTAREA
NAME="descr"
COLS="30"          ROWS="3"
OnBlur="count_char(document.egForm.descr.value)">Enter a short description here
 </TEXTAREA>
```

Ví dụ : <textarea name="Ghichu" rows="2" cols="20"></textarea>

### 5. *Thẻ FORM*

Forms là một thiết lập nhỏ trong HTML, nó cho phép người sử dụng đưa vào các thông tin. Giao diện Forms tạo nên sự thuận lợi trong việc tương tác giữa người sử dụng và các dịch vụ. Trên Form ta có thể tạo các thành phần như các nút lệnh, các trường văn bản (Text) hay các danh sách lựa chọn ... Khi forms được hoàn thành bởi người sử dụng, Client sẽ gửi thông tin đến Server, Server sẽ thực thi các chương trình kết hợp với form và các tham số là các thông tin nhận từ Form.

Thông thường các Form sử dụng cho hai mục đích chính:

- Dùng để thu thập thông tin từ người sử dụng.
- Là trung gian để tương tác qua lại giữa người sử dụng và hệ thống.

Cú pháp : <Form ACTION = “Action” METHOD="PhuongThuc">

**Action**: là một URL hoặc một Script mà khi nút ***Submit*** được nhấn nó sẽ thực thi.

**Method=**GET/POST : Xác định kiểu yêu cầu mà trình duyệt gởi đến cho Server.

- METHOD = GET: trình duyệt sẽ bổ sung dữ liệu đầu vào dưới dạng một biến môi trường là CGI_QueryString.
- METHOD=POST: Forrn dữ liệu đầu vào sẽ đợi từ các thiết bị nhập của Server cùng với một số dữ liệu được lưu trữ trong biến môi trường CGI_ContentLength.

**EncType:** cung cấp kiểu Mime của tập được dùng như đầu vào trong các biểu mẫu.

Ví dụ : <Form ACTION = METHOD="GET">

### 6. *Thẻ TABLE*

- Dùng để tạo ra một bảng. Bảng được tạo thành từ các hàng, trên mỗi hàng có các ô (cell).

```
<TABLE>
        <TABLE   BORDER = “n” . . . >
        <TR>
                <TD>  . . . </TD> <TD>  . . . </TD> <TD>  . . . </TD>
        </TR>
        . . . .
        <TR>
                <TD>  . . . </TD> <TD>  . . . </TD> <TD>  . . . </TD>
        </TR>
</TABLE>
```

### 7. *Thẻ SELECT*

- Hiển thị hộp ComboBox cho phép chọn lựa một trong nhiều giá trị :

```
<SELECT  NAME =”TenĐT”>
        <OPTION SELECTED VALUE =”Gia trị 1”> Nội dung 1
        <OPTION SELECT VALUE =”Gia trị 2”> Nội dung 2
                . . .
</SELECT>
```

*Ví dụ :*

```
<p>Que quan <select size="1" name="cboQuequan">
        <option selected>Da Nang</option>
        <option>Hue</option>
        <option>Ha Noi</option>
        </select></p>
```

### 8. *Thẻ <APPLET>*

Dùng để chèn Applet Java vào trang Web. Có dạng tổng quát sau:

```
<APPLET
    [CODEBASE = URL] [CODE = appletFile]
    [NAME = appletInstanceName]:
    [ARCHIVE = compressed file] [ALT = alternateText]
    [WIDTH = pixels]  [HEIGHT = pixels]  [ALIGN = alignment]
    [VSPACE = pixels] [HSPACE = pixels]
    [ARCHIVE = URL to archive]
 </APPLET>
```

Trong đó :

| Tham số | Giải thích |
|---|---|
| CODEBASE=URL | Chỉ định địa chỉ tuyệt đối của Applet. |
| CODE=appletFile | Chỉ định địa chỉ tương đối của Applet. |
| ALT=alternateText | Chỉ định dòng text sẽ hiển thị trong trường hợp trình Browse không hiểu Applet. |
| NAME = appletInstanceName | Đặt tên cho Applet để phục vụ cho việc tìm kiếm. |
| WIDTH=pixels HEIGHT=pixels | Chỉ định kích thước cho Applet. |
| ALIGN=alignment | Dùng canh lề, có các giá trị sau: LEFT, RIGHT, TOP, TEXTTOP, MIDDLE, ABSMIDDLE, BASELINE, BOTTOM, ABSBOTTOM. |
| VSPACE=pixels HSPACE=pixels | Chỉ định khoảng trống bao chung quanh Applet. |
| ARCHIVE=compressed file | Khai báo các file nén cần thiết của Applet để trình Browse tải về máy cá nhân, phục vụ cho việc đọc lại sau nầy. |

Ví dụ:

```
<APPLET CODEBASE=http://200.201.202.180/applets/ NervousText
CODE="NervousText.class"
WIDTH=400      HEIGHT=75
ALIGN=CENTER>
<PARAM NAME="text" VALUE="This is the Applet Viewer.">
</APPLET>
```

Chỉ thị cho trình Browse nạp Applet ở địa chỉ htttp://java.sun.com/JDK-prebeta1/applets/NervousText/NervousText.class". Chỉ định kích thước là 400x75 pixels và canh giữa dòng. Nếu trình Browse hiểu Applet, dòng "This is the Applet Viewer." sẽ hiển thị và Applet tạo hiệu ứng cho dòng chữ nầy. Nếu trình Browse không hiểu Applet, nó sẽ bỏ qua nội dung của <APPLET> cũng như <PARAM> và chỉ hiển thị nội dung của <BLOCKQUOTE>

9. ***Thẻ <IMG>***

Dùng để chèn 1 file hình vào tài liệu HTML

Các thuộc tính :

- ALIGN="left/right/top/texttop/middle/absmiddle/baseline/bottom/absbotto": So hàng hình ảnh với Text.
- ALT="Alternative Text": Cho hiển thị 1 dòng text thay thế cho file hình trong trường hợp trình Browse đang ở trong chế độ không hiển thị hình ảnh. Dòng Text nầy cũng hiển thị theo dạng ToolTip khi dời chuột đến hình.

Ví dụ: <IMG SRC="triangle.gif" ALT="Warning:"> Read these instructions.

- SRC="URL of image": Chỉ định đia chỉ file hình chèn vào trang Web.

Ví dụ : <IMG SRC="warning.gif">Be sure to read these instructions.

- WIDTH=value/ HEIGHT=value: Chỉ định khoảng cách dành sẳn cho hình trong khi trình Browse nạp toàn bộ hình.
- BORDER=value: Chỉ định cho hiển thị đường viền bao quanh hình ảnh. Ta có thể chọn "0" để hiển thị đường viền màu xanh khi có liên kết.
- VSPACE=value HSPACE=value: Quy định khoảng trống giữa hình và Text. VSPACE cho trên và dới hình, HSPACE cho trái và phải hình. Value tính theo pixel.
- LOWSRC: Thuộc tính nầy cho phép hiển thị 2 hình lần lượt trong cùng 1 vị trí. Thường dùng để nạp một hình nhỏ trong khi chờ đợi nạp hình chính có dung luợng file lớn hơn:

Ví dụ: <IMG SRC="hiquality.gif" LOWSRC="lowquality.gif">

Đầu tiên trình Browse sẽ hiển thị file hình "lowquality.gif". Sau khi nạp hoàn tất cả trang, trình duyệt sẽ nạp file hình chính thức vào thay thế.

### *10.7.4.2 Chỉ định tài nguyên trong URL*

Để chỉ định vị trí của tài nguyên HTTP dùng URL (Uniform Resouce Locators) đó là tên quy ước để nhận diện một cách duy nhất vị trí của một thư mục

hoặc một tập tin trên Intranet/Internet. Trong URL cũng chỉ định giao thức kết nối như HTTP, GOPHER... cần thiết cho việc tìm kiếm và lấy tài nguyên. Nếu ta biết URL của một tài nguyên ta có thể truy xuất nó một cách trực tiếp hoặc thông qua các siêu liên kết trong các tài liệu.

URL sử dụng một dòng đơn các ký tự ASCII. Sơ đồ này bao gồm các giao thức trên Intranet/Internet như FTP, Gopher, http... URL là một trong những công cụ cơ sở của WWW và được dùng trong các tài liệu HTML để tham chiếu đến các tài nguyên trên mạng.

Một URL gồm các thông tin sau :

a. Tên các giao thức khi truy cập Server (như HTTP, Gopher, Wais...).

b. Tên miền của Server thực thi, theo bất cứ thông tin về user và password của site trên Intranet/Internet.

c. Số cổng mà server sử dụng. Nếu điều này không được chỉ rõ trình duyệt sẽ dùng số cổng mặc định trong giao thức (cổng 80).

d. Định vị của tài nguyên trong kiến trúc phân cấp của Server.

#### *10.7.4.3 Giao thức HTTP*

Giao thức HTTP (Hyper Text Transfer Protocol - Giao thức truyền siêu văn bản) sử dụng cho các dịch vụ truyền thông đa phương tiện WWW, dựa trên mô hình Client/Server. Dịch vụ WWW cho phép NSD kết hợp văn bản, âm thanh, hình ảnh, hoạt hình tạo nên nguồn thông tin tư liệu. Đặc biệt ở đây là thông tin tư liệu trong WWW có dạng HyperText - là dạng tư liệu chuẩn trong WWW. Giao thức cho phép lấy và đọc nhanh các tư liệu đó. HTTP là giao thức truyền thông nhưng có thêm ưu điểm là thông tin tư liệu cần truy cập lại có chứa các liên kết tới cá tư liệu khác nằm khắp nơi trên mạng Internet.

Phần mềm cho WWW Server là một chương trình điều khiển sự thu nhập các tư liệu WWW trên một máy chủ. Để truy cập WWW, cần thiết phải chạy hệ thống ứng dụng WWW là một trình duyệt (browser) trên máy của WWW Client.

HTTP là một giao thức Internet Client/Server, được thiết kế để truyền các dạng dữ liệu  siêu văn bản. HTTP là một giao thức không trạng thái, nghĩa là khi Server đáp ứng dữ liệu được yêu cầu bởi Client xong thì server huỷ bỏ kết nối đó không tốn bộ nhớ cho sự kiện. Không trạng thái là yếu tố làm cho tốc độ truyền dẫn giữa HTTP Server và HTTP Client rất nhanh.

Các giao tiếp HTTP truyền dữ liệu dưới dạng các ký tự 8 bit hay một octet. Điều này đảm bảo truyền dẫn an toàn mọi dạng dữ liệu bao gồm hình ảnh, âm thanh, các tài liệu HTML hay các chương trình khả thi.

### 1. *Các giai đoạn kết nối của HTTP*

Một HTTP Server kết nối thông qua 4 giai đoạn:

- ***Mở kết nối:*** Client tiếp xúc với Server tại địa chỉ internet và số cổng chỉ định trong URL (cổng mặc định là 80)
- ***Tạo yêu cầu :*** Client gửi một thông điệp tới Server yêu cầu dịch vụ. Yêu cầu bao gồm các tiêu đề HTTP, nó định nghĩa phương thức được yêu cầu cho tác vụ và cung cấp thông tin về khả năng của Client (được theo sau dữ liệu gửi tới Server). Các phương thức HTTP điển hình là GET để nhận các đối tượng từ Server hoặc POST để chuyển dữ liệu cho đối tượng (ví dụ như các chương trình GateWay) trên Server.
- ***Gửi đáp ứng :*** Server trả lời cho Client bao gồm các tiêu đề để trả lời trạng mô tả trạng thái của tác vụ (ví dụ thành công, không thành công...) theo sau dữ liệu thật sự.
- ***Đóng kết nối:*** Kết nối được đóng, Server không giữ lại dấu vết của tác vụ đã hoàn thành. Thủ tục này có nghĩa là mỗi kết nối chỉ xử lý một tác vụ và do đó chỉ có thể tải xuống Client chỉ một tệp dữ liệu. Tính chất không trạng thái của tác vụ cũng có nghĩa là mỗi kết nối không hề biết về các kết nối trước đó.

### 2. *Các phương thức của giao thức HTTP*

| Phương thức | Giải thích |
|---|---|
| GET | Lấy dữ liệu hiển thị trong URL. Dữ liệu cũng có thể gửi trong URL thông qua một chuỗi truy vấn. Đây cũng là nơi dữ liệu gửi từ ISINDEX hoặc Form với thuộc tính METHOD="GET" |
| HEAD | Lấy thông tin của HTTP, Header chỉ định trong URL. |
| POST | Gửi dữ liệu đến cho URL nếu URL là tồn tại. Phương thức này được dùng bởi những thành phần của Form trong HTML với giá trị thuộc tính METHOD="POST". |
| PUT | Là nơi mà dữ liệu gửi bởi Client biểu thị trong URL, nó sẽ thay thế nội dung của URL đã có. |
| DELETE | Xóa tài nguyên cục bộ tại nơi được chỉ định bởi URL. |
| LINK | Liên kết một đối tượng đã tồn tại với một đối tượng khác. |
| UNLINK | Huỷ bỏ một liên kết đã được tạo bởi phương thức LINK. |

# BÀI TẬP

1. Những nguyên tắc cơ bản giám sát và quản trị hệ thống mạng máy tính
2. Khảo sát cấu trúc và hoạt động dịch vụ DNS
3. Khảo sát cấu trúc và hoạt động của giao thức SNMP
4. Khảo sát cấu trúc và hoạt động của giao thức HTTP
5. Tìm hiểu giao thức DHCP.

- - - - - - - - - - - - - - - - - - - - - - - - -

# TÀI LIỆU THAM KHẢO

**Tiếng Việt**

[1] Nguyễn Thúc Hải, ***Mạng máy tính và các hệ thống mở*** , NXB Giáo dục, 1997

[2] Lê Văn Sơn, ***Giáo trình mạng máy tính***, Trường ĐH Bách Khoa Đà Nẵng, 1998

[3] Nguyễn Hồng Sơn, ***Giáo trình hệ thống mạng máy tính CCNA,*** Nhà XB Lao động, 2002

**Tiếng Anh**

[4] Douglas E.Comer, ***Computer Networks and Internets***, Prentice Hall, 1997

[5] Ed Taylor, ***TCP/IP complete***, McGraw-Hill, 1998

[6] Microsoft Press, ***Networking Essentials***

[7] Stallings W., ***Data and Computer Communications***, Macmillan Publishing, 1995

[8] Tanenbaum Andrew S., ***Computer*** **Networks,** Prentice Hall, 1997

[9] Pujolle, ***Les rĐseaux***, EYROLLES, 2003

***@2004, Nguyễn Tấn Khôi***

**Khoa Công Nghệ Thông Tin - Trường Đại học Bách Khoa Đà Nẵng**

----------o & o----------

**TRƯỜNG ĐẠI HỌC ĐÀ LẠT**
**KHOA CÔNG NGHỆ THÔNG TIN**

**TRẦN NGÔ NHƯ KHÁNH**

**BÀI GIẢNG TÓM TẮT**

# MẠNG MÁY TÍNH

**Dành cho sinh viên ngành Công nghệ Thông tin**

**(Lưu hành nội bộ)**

**Đà Lạt 2008**

# Mục Lục

**Chương I. Những khái niệm căn bản về mạng ..... 4**
I.1. Khái niệm và phân loại mạng ..... 4
I.2. Dịch vụ mạng ..... 8
I.3. Giao thức mạng ..... 8
I.4. Các mô hình tham chiếu(reference models) ..... 10
I.5. Hệ điều hành trong môi trường mạng ..... 15
I.6. Mạng Internet ..... 16
**Chương II. Tầng vật lý ..... 18**
II.1. Chức năng ..... 18
II.2. Môi trường truyền tin ..... 18
II.3. Đặc tả các loại cáp mạng ..... 20
II.4. Chuẩn giao diện ..... 22
**Chương III. Giao thức tầng liên kết dữ liệu ..... 24**
III.1. Chức năng và dịch vụ ..... 24
III.2. Cơ chế phát hiện và sửa lỗi ..... 30
III.3. Các giao thức đa truy cập ..... 33
III.4. Khái niệm mạng LAN ..... 38
III.5. Địa chỉ vật lý (MAC address) ..... 47
III.6. Một số công nghệ tầng liên kết dữ liệu khác ..... 47
**Chương IV. Giao thức tầng mạng ..... 53**
IV.1. Chức năng của tầng mạng ..... 53
IV.2. Bộ định tuyến và các thiết bị kết nối mạng khác: ..... 56
IV.3. Giao thức IP (IP Protocol) ..... 61
IV.4. Các giao thức liên quan đến IP ..... 69
IV.5. Giao thức định tuyến ..... 70
IV.6. Định tuyến trên Internet ..... 77
**Chương V. Giao thức tầng giao vận ..... 79**
V.1. Dịch vụ tầng vận chuyển ..... 79

V.2. Giao thức không kết nối UDP ..... 80
V.3. Giao thức hướng kết nối TCP ..... 81
V.4. So sánh TCP và UDP ..... 87
**Chương VI. Giao thức tầng ứng dụng ..... 89**
VI.1. Chức năng: ..... 89
VI.2. World Wide Web - HTTP ..... 89
VI.3. Giao thức truyền File-FTP ..... 92
VI.4. Giao thức SMTP ..... 93
VI.5. Các giao thức nhận mail: ..... 102
VI.6. Dịch vụ phân giải tên miền (DNS Services-Domain Name System Services) ..... 105

# Mở đầu

Cùng với sự phát triển mạnh mẽ của công nghệ thông tin ngày nay, mạng máy tính đóng một vai trò quan trọng, cung cấp những dịch vụ tiện ích cho nhiều lĩnh vực đời sống xã hội khác nhau.

Giáo trình này nhằm cung cấp cho sinh viên ngành Công nghệ Thông tin những kiến thức căn bản về mạng máy tính, cách thức hoạt động và tổ chức của một hệ thống mạng. Các khái niệm về kiến trúc phân tầng, các giao thức mạng trong các tầng khác nhau. Tài liệu cũng trình bày về mô hình TCP/IP, các công nghệ mạng phổ biến, các thiết bị cần thiết để triển khai một hạ tầng mạng, khái niệm địa chỉ IP, định tuyến,…

Tuy đã có nhiều cố gắng trong quá trình biên soạn nhưng vẫn còn nhiều thiếu sót, chúng tôi mong nhận được các ý kiến đóng góp của các thầy cô, đồng nghiệp và các bạn sinh viên để chúng tôi có thể hoàn thiện giáo trình này hơn.

# Chương I. Những khái niệm căn bản về mạng

## I.1. Khái niệm và phân loại mạng

### I.1.1. Khái niệm

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

Mạng máy tính bao gồm phần cứng, các giao thức và các phần mềm mạng.

Khi nghiên cứu về mạng máy tính, các vấn đề quan trọng được xem xét là giao thức mạng, cấu hình kết nối mạng và các đích vụ trên mạng.

Mạng máy tính có những công dụng như sau:

1. Tập trung tài nguyên tại môt số máy và chia sẽ cho nhiều máy khác
   - Nhiều người có thể dùng chung một tiện ích.
   - Dữ liệu đực quản lý tập trung nên an toàn hơn, trao đổi giữa người sử dụng thuận lợi hơn, nhanh chóng hơn.
   - Mạng máy tính cho phép người lập trình ở một trung tâm máy tính này có thể sử dụng các chương trình tiện ích của một trung tâm máy tính khác đang rỗi, sẽ làm tăng hiệu quả kinh tế của hệ thống.
2. Khắc phục trở ngại về khoảng cách địa lý.
3. Tăng chất lượng và hiệu quả khai thác thông tin.
4. Cho phép thực hiện những ứng dụng tin học phân tán.
5. Độ an toàn, tin cậy của hệ thống tăng lên nhờ khả năng thay thế máy có sự cố khi có sự cố*:* An toàn cho dữ liệu của phần mềm vì phần mềm mạng sẽ khóa các tập tin khi có người không đủ quyền hạn truy xuất các tập tin và các thư mục đó.
6. Phát triển các công nghệ trên mạng: Người sử dụng có thể trao đổi thông tin với nhau dễ dàng và sử dụng các hệ mạng như là một công cụ để phổ biến tin tức, thông báo về một chính sách mới, về nội dung buổi họp, về các thông tin kinh tế như giá cả thị trương, tin rao vặt (muốn bán hoặc mua một cái gì đó), hoặc sắp xếp thời khóa biểu của mình chen lẫn với thời khóa biểu của những người khác …

### I.1.2. Phân loại mạng

- **Dựa theo khoảng cách địa lý**

Mạng máy tính có thể phân bổ trên một khu vực nhất định trong phạm vị quốc gia hay toàn cầu. Dựa vào phạm vi phân bố, người ta có thể phân ra các loại mạng như sau:

a. LAN ( Local Area Netwowk – mạng cục bộ): LAN thường được sử dụng trong nội bộ một cơ quan tổ chức… kết nối các máy tính trong một khu vực bán kính khoảng 100m đến 100km. Kết nối được thực hiện thông qua các môi trường truyền thông tốc độ cao, ví dụ cáp đồng trục hay cáp quang.

b. MAN (Metropolitan Area Network – mạng đô thị) : Kết nối các máy tính trong phạm vi một thành phố. Kết nối này được thực hiện qua các môi trường truyền thông tốc độ cao ( 50 – 100 Mbit/s)

c. WAN (Wide Area Network – mạng diện rộng) : Kết nối các máy tính trong nội bộ các quốc gia hay các quốc gia trong cùng một châu lục. Thông thường kết nối này được thực hiện thông qua mạng viễn thông. Các WAN có thể được kết nối với nhau thành GAN hay tự nó đã là GAN.

d. GAN (Global Area Network - Mạng toàn cầu) : Kết nối máy tính từ các châu lục khác nhau. Thông thường kết nối này được thực hiện thông qua mạng viễn thông và vệ tinh.

Trong các khái niệm nói trên, WAN và LAN là hai khái niệm hay được sử dụng nhất.

- **Dựa theo cấu trúc mạng**

1. ***Kiểu điểm - điểm (point – to – point)***

Đường truyền nối từng cặp nút mạng với nhau. Thông tin đi từ nút nguồn qua nút trung gian rồi gởi tiếp nếu đường truyền không bị bận. Do đó còn có tên là mạng lưu trữ và chuyển tiếp (*store and forward).*

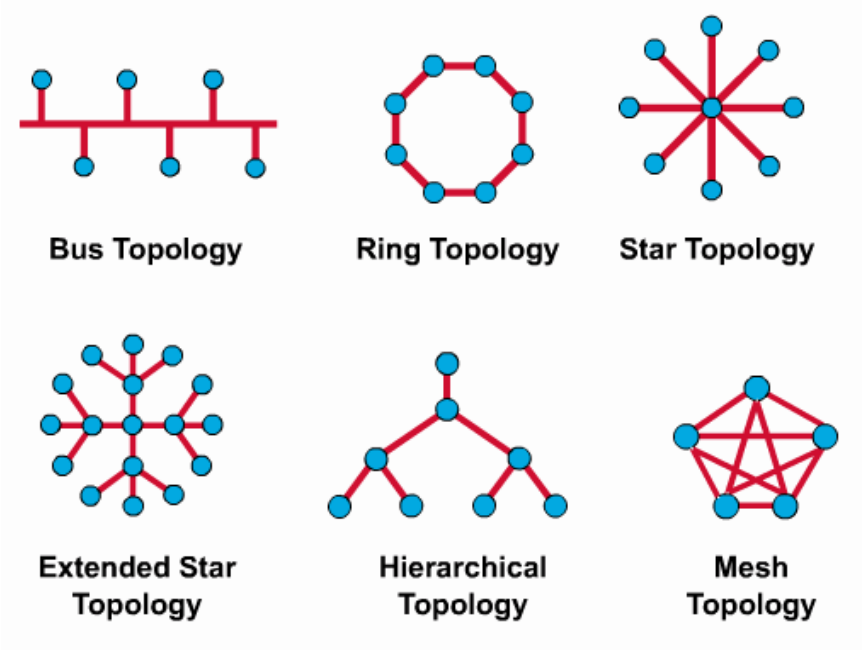
Ví dụ: mạng hình sao(star), dạng vòng (ring), dạng cấp bậc (hierarchical)

***2. Kiểu quảng bá (broadcast)***

Bản tin được gửi đi từ một nút nào đó sẽ được tiếp nhận bởi các nút còn lại (còn gọi là broadcasting hay point-to-multipoint). Trong bản tin phải có vùng địa chỉ cho phép mỗi nút kiểm tra xem có phải bản tin của mình không và xử lý nếu đúng bản tin được gởi đến.

Ví dụ: mạng bus.

Trong cấu trúc dạng Bus và Vòng cơ chế "*Trọng tài"* dùng để giải quyết các xung đột *(collision)* xảy ra khi nhiều nút muốn truyền tin đồng thời. Trong cấu trúc vệ tinh hoặc radio, mỗi nút cần có ăng ten thu và phát.

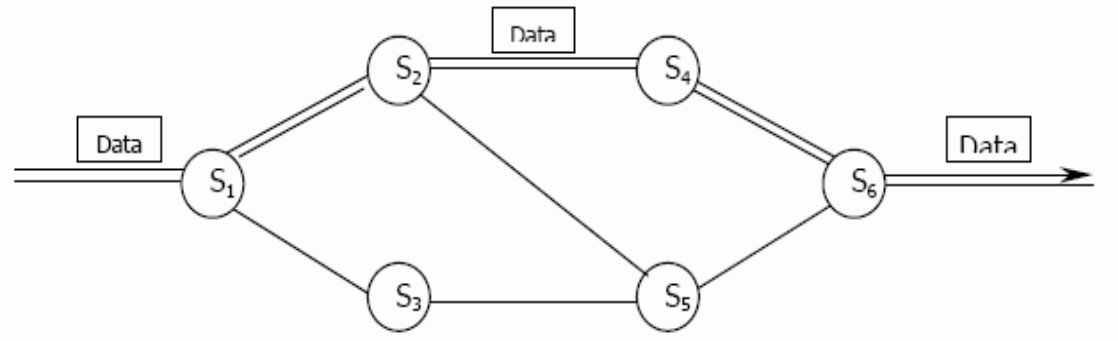



Hìng I-1. Một số dạng cấu trúc mạng

- **Dựa theo phương pháp chuyển mạch**
  - Mạng chuyển kênh (Line switching network), ví dụ như mạng điện thoại.
  - Mạng chuyển mạch thông báo (Message switching network)
  - Mạng chuyển mạch gói (Packet switching network)

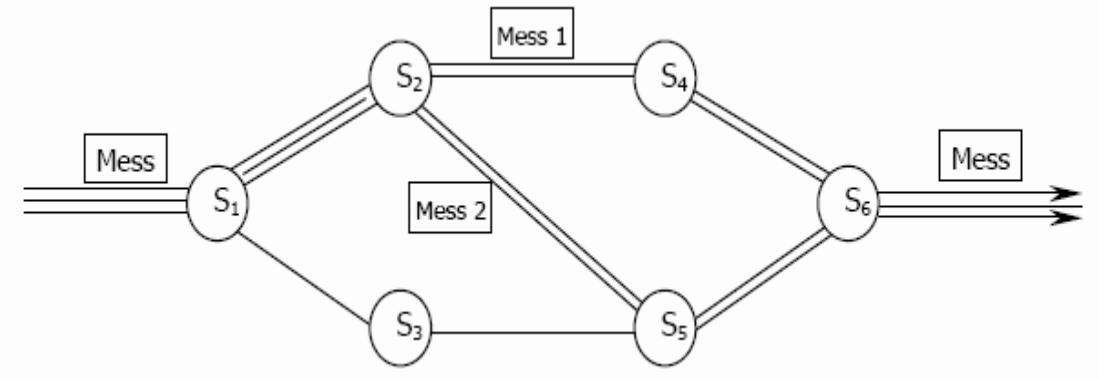
### *1. Mạng chuyển mạch kênh*

Chuyển mạch kênh (line switching) được dùng trong mạng điện thoại. Một kênh cố định được thiết lập các cặp thực thể cần liên lạc với nhau. Mạng này có hiệu suất không cao vì có lúc kênh bỏ không.




Hình I-2. Mạng chuyển mạch kênh.

### *2. Mạng chuyển mạch bản tin*




Hình I-3. Phương pháp chuyển mạch thông báo

Các nút của mạng căn cứ vào địa chỉ đích của "bản tin" để chọn nút kết tiếp. Như vậy các nút cần lưu trữ và đọc tin nhận được, quản lý việc truyền tin. Trong trường hợp bản tin quá dài và nếu sai phải truyền lại thì hiệu suất không cao. Phương pháp này giống như cách gởi thư thông thường.

Ưu điểm so với phương pháp chuyển mạch kênh:

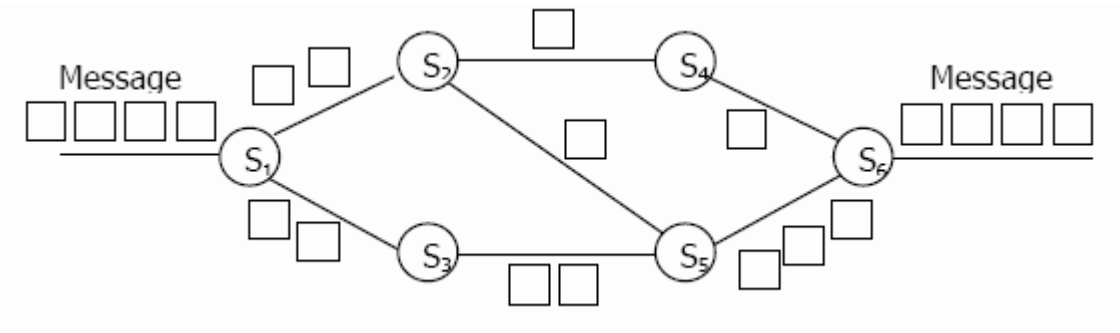
- Hiệu suất sử dụng đường truyền cao vì không bị chiếm dụng độc quyền mà được chia cho nhiều thực thể.
- Mỗi nút mạng (hay nút chuyển mạch thông báo) có thể lưu trữ bản tin cho tới khi kênh truyền mới gởi bản tin lại. Do đó giảm được tình trạng tắc nghẽn (congestion) trên mạng.
- Điều khiển việc truyền tin bằng cách sắp xếp độ ưu tiên của các bản tin.
- Có thể tăng hiệu suất sử dụng giải thông của mạch bằng cách gán địa chỉ quảng bá (broadcast) để gởi bản tin đồng thời đến nhiều đích.

Nhược điểm

- Do không hạn chế kích thước của bản tin nên có thể dẫn đến phí tổn lưu trữ tạm thời cao và ảnh hưởng đến thời gian hồi đáp và chất lượng truyền đi.
- Mạng chuyển mạch thông báo thích hợp với các dịch vụ thông tin kiểu thư điện tử (Email) hơn là đối với các ứng dụng có tính thời gian thực vì tồn tại độ trễ nhất định do lưu trữ và xử lý thông tin điều khiển tại mỗi nút.

### *3. Mạng chuyển mạch gói*

Bản tin được chia thành nhiều gói tin (packet) với độ dài 512 bytes, phần đầu là địa chỉ đích, mã để tập hợp các gói. Các gói của các bản tin khác nhau có thể được truyền độc lập trên cùng một đường truyền. Vấn đề phức tạp ở đây là tạo lại bản tin ban đầu, đặc biệt khi được truyền trên nhiều con đường khác nhau.




Hình I-4. Mạng chuyển mạch gói

Chuyển mạch gói mềm dẻo, hiệu suất cao. Xu hướng phát triển hiện nay là sử dụng hai kỹ thuật chuyển mạch kênh và chuyển mạch gói cùng một mạng thống nhất gọi là ISDN (*Interated Services Digital Network* – Mạng thông số đa dịch vụ).

## I.2. Dịch vụ mạng

Một số dịch vụ mạng phổ biến:

- Dịch vụ tập tin (File Services): Cho phép các máy tính trên mạng chia sẻ tập tin với nhau.
- Dịch vụ in ấn (Print Service): Nhiều máy trên mạng sử dụng chung một máy in. Giúp giảm chi phí và tăng độ linh hoạt
- Dịch vụ thư tính (Message Service): Là dịch vụ cho phép gửi/nhận thư điện tử. Thư có thể kèm phim ảnh, âm thanh,…
- Dịch vụ thư mục (Directory Service): Cho phép quản lý tất cả thông tin các đối tượng trên mạng, nhờ đó quá trình quản lý và chia sẻ tài nguyên hiệu quả hơn.
- Dịch vụ ứng dụng (Application Service): Dịch vụ cung cấp kết quả cho các chương trình ở client bằng cách thực hiện các chương trình phù hợp ở server.

## I.3. Giao thức mạng

Giao thức (protocol) là tập hợp các quy tắc giao tiếp giữa các hệ máy tính. Giao thức có các chức năng chính sau:

1. Định nghĩa cấu trúc khung một cách chính xác cho từng byte, các kí tự và bản tin.
2. Phát hiện và xử lý lỗi, thông thường là gửi lại bản tin gốc sau khi phát hiện lần trước bị lỗi.

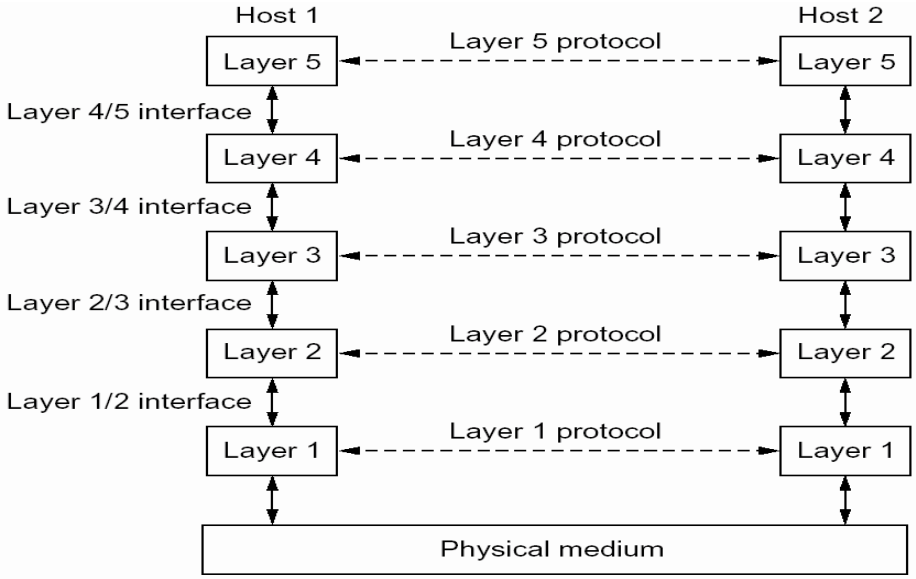
3. Quản lý thứ tự các lệnh để đếm bản tin, nhận dạng, tránh mất hoặc nhận thừa bản tin.
4. Đảm bảo không nhầm lẫn bản tin và lệnh.
5. Chỉ ra các thuộc tính đường dây khi lập các đường nối đa điểm hoặc bán song công (cho biết ai đang trao đổi thông tin với ai).
6. Giải quyến vấn đề xung đột truy cập (yêu cầu đồng thời), gửi khi chưa có số liệu, mất liên lạc, khởi động.

Để giảm độ phức tạp thiết kế, giao thức mạng hiện nay được thiết kế theo kiến trúc đa tầng, mỗi tầng được xây dựng trên tầng trước nó, tầng bên dưới sẽ cung cấp dịch vụ cho tầng bên trên. Tầng N trên một máy sẽ thực hiện việc giao tiếp với tầng N trên máy khác. Các nguyên tắc, luật lệ sử dụng cho việc giao tiếp này gọi là các giao thức của tầng N.

Các thực thể (entity) nằm trên tầng tương ứng ở những máy khác nhau gọi là các tiến trình đồng mức. Các tiến trình đồng mức giao tiếp với nhau bằng các giao thức của tầng đó. Giữa hai tầng kề nhau tồn tại một giao diện (interface) xác định các hàm nguyên thủy và các dịch vụ tầng dưới cung cấp cho tầng bên trên.

Tập hợp các tầng và các giao thức hình thành kiến trúc mạng (Network Architecture). Cấu trúc phân tầng của máy tính có ý nghĩa đặc biệt như sau:

- Thuận tiện trong việc thiết kế, xây dựng và cài đặt các mạng máy tính, trong đó mỗi hệ thống được xem là cấu trúc đa tầng.
- Mỗi tầng được xây dựng trên cơ sở tầng trước đó, tầng dưới cung cấp dịch vụ cho tầng bên trên.
- Tập hợp các giao thức, các vấn đề kĩ thuật và công nghệ có thể được khảo sát, nghiên cứu, triển khai độc lập với nhau.




Hình I-5. Mô hình trao đổi dữ liệu giữa các tầng

## I.4. Các mô hình tham chiếu(reference models)

### I.4.1. Mô hình OSI

Mô hình OSI (Open System Interconnection) là một cơ sở dành cho việc chuẩn hoá các hệ thống truyền thông, nó được nghiên cứu và xây dựng bởi ISO. Việc nghiên cứu về mô hình OSI được bắt đầu tại ISO vào năm 1971 với mục tiêu nhằm tới việc nối kết các sản phẩm của các hãng sản xuất khác nhau và phối hợp các hoạt động chuẩn hoá trong các lĩnh vực viễn thông và hệ thống thông tin. Theo mô hình OSI, chương trình truyền thông được chia ra thành 7 tầng với những chức năng phân biệt cho từng tầng. Hai tầng đồng mức khi liên kết với nhau phải sử dụng một giao thức chung. Trong mô hình OSI có hai loại giao thức chính được áp dụng: giao thức hướng liên kết (connection - oriented) và giao thức không liên kết (connectionless)

- **Giao thức hướng liên kết**: trước khi truyền dữ liệu hai tầng đồng mức cần thiết lập một liên kết logic và các gói tin được trao đổi thông qua liên kết này, việc có liên kết logic sẽ nâng cao độ an toàn trong truyền dữ liệu.
- **Giao thức không liên kết:** trước khi truyền dữ liệu không thiết lập liên kết logic và mỗi gói tin được truyền độc lập với các gói tin trước hoặc sau nó.

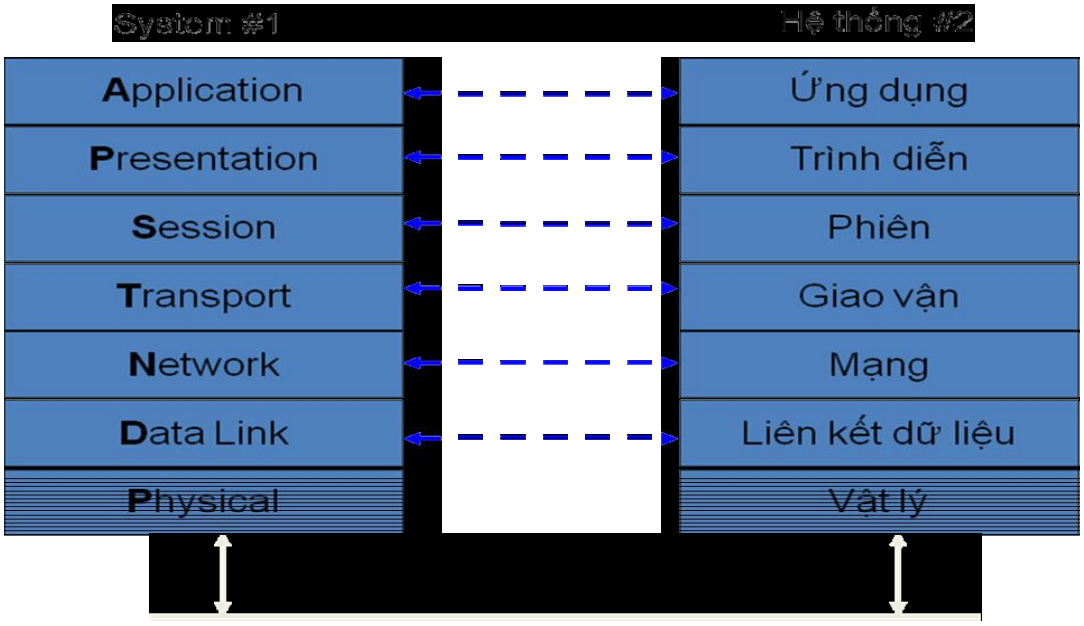
Như vậy với giao thức có liên kết, quá trình truyền thông phải gồm 3 giai đoạn phân biệt:

• Thiết lập liên kết (logic): hai thực thể đồng mức ở hai hệ thống thương lượng với nhau về tập các tham số sẽ sử dụng trong giai đoạn sau (truyền dữ liệu).

• Truyền dữ liệu: dữ liệu được truyền với các cơ chế kiểm soát và quản lý kèm theo (như kiểm soát lỗi, kiểm soát luồng dữ liệu, cắt/hợp dữ liệu...) để tăng cường độ tin cậy và hiệu quả của việc truyền dữ liệu.

• Hủy bỏ liên kết (logic): giải phóng tài nguyên hệ thống đã được cấp phát cho liên kết để dùng cho liên kết khác.

Đối với giao thức không liên kết thì chỉ có duy nhất một giai đoạn truyền dữ liệu.




Hình I-6. Mô hình OSI

Chức năng các tầng trong mô hình OSI:

- **Tầng ứng dụng (Application layer)**: tầng ứng dụng quy định giao diện giữa người sử dụng và môi trường OSI, nó cung cấp các phương tiện cho người sử dụng truy cập vả sử dụng các dịch vụ của mô hình OSI.
- **Tầng trình bày (Presentation layer)**: tầng trình bày chuyển đổi các thông tin từ cú pháp người sử dụng sang cú pháp để truyền dữ liệu, ngoài ra nó có thể nén dữ liệu truyền và mã hóa chúng trước khi truyền để bảo mật.
- **Tầng phiên (Session layer)**: tầng phiên quy định một giao diện ứng dụng cho tầng vận chuyển sử dụng. Nó xác lập ánh xạ giữa các tên, đặt địa chỉ, tạo ra các tiếp xúc ban đầu giữa các máy tính khác nhau trên cơ sở các giao dịch truyền thông. Nó đặt tên nhất quán cho mọi thành phần muốn đối thoại riêng với nhau.
- **Tầng vận chuyển (Transport layer)**: tầng vận chuyển xác định địa chỉ trên mạng, cách thức chuyển giao gói tin trên cơ sở trực tiếp giữa hai đầu mút (end-to-end). Để bảo đảm được việc truyền ổn định trên mạng tầng vận chuyển thường đánh số các gói tin và đảm bảo chúng chuyển theo thứ tự.
- **Tầng mạng (Network layer)**: tầng mạng có nhiệm vụ xác định việc chuyển hướng, vạch đường các gói tin trong mạng, các gói tin này có thể phải đi qua nhiều chặng trước khi đến được đích cuối cùng.

- **Tầng liên kết dữ liệu (Data link layer):** tầng liên kết dữ liệu có nhiệm vụ xác định cơ chế truy nhập thông tin trên mạng, các dạng thức chung trong các gói tin, đóng các gói tin...
- **Tầng vật lý (Physical layer)**: tầng vật lý cung cấp phương thức truy cập vào đường truyền vật lý để truyền các dòng bit không cấu trúc, ngoài ra nó cung cấp các chuẩn về điện, dây cáp, đầu nối, kỹ thuật nối mạch điện, điện áp, tốc độ cáp truyền dẫn, giao diện nối kết và các mức nối kết..

### I.4.2. Mô hình TCP/IP

Mô hình OSI chỉ mang tính chất lý thuyết, phục vụ nghiên cứu và học tập. Có nhiều mô hình khác nhau như NetBIOS, IPX/SPX,..nhưng mô hình được sử dụng rộng rãi cho Internet là TCP/IP. Về lịch sử phát triển, vào cuối những năm 1960 và đầu 1970, bộ quốc phòng Mỹ (Department of Defense - DoD) được giao trách nhiệm phát triển mạng ARPANET. Mạng ARPANET bao gồm mạng của những tổ chức quân đội, các trường đại học và các tổ chức nghiên cứu kết nối bằng đường điện thoại, được dùng để hỗ trợ cho những dự án nghiên cứu khoa học và quân đội. Khi vệ tinh và mạng vô tuyến được sử dụng để trao đổi thông tin, các giao thức cũ không còn đủ đáp ứng dẫn đến yêu cầu có một kiến trúc tham chiếu mới. Vì vậy khả năng kết nối linh động nhiều mạng khác nhau được đặt lên hàng đầu. Kiến trúc này sau đó được biết đến với tên gọi mô hình tham chiếu TCP/IP, dựa trên hai giao thức chính của kiến trúc.

Mô hình kiến trúc TCP/IP được chia làm 4 tầng:

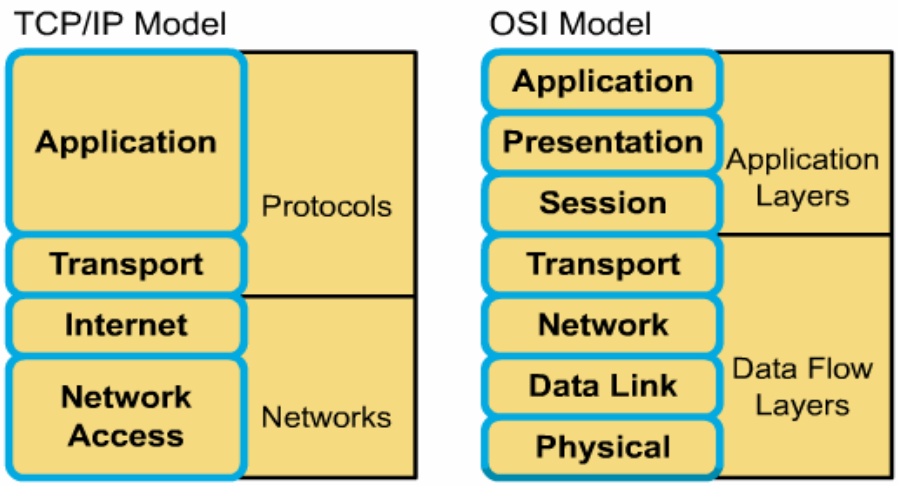
1. **Tầng truy cập mạng (Network Access)**

Cung cấp cho hệ thống phương thức để truyền dữ liệu trên các thiết bị phần cứng vật lý khác nhau của mạng. Đồng thời đóng gói các lược đồ dữ liệu IP (IP datagram) thành các khung (frame) truyền trên mạng và ánh xạ địa chỉ IP thành các địa chỉ vật lý tương ứng.

Tầng này còn định nghĩa cách thức truyền các khối dữ liệu IP, các giao thức của tầng này phải biết chi tiết cấu trúc vật lý mạng ở dưới để định dạng chính xác dữ liệu sẽ được truyền.

2. **Tầng mạng**

Tầng mạng chịu trách nhiệm định tuyến các bản tin (message) qua các mạng vật lý khác nhau, liên mạng. Giao thức chính của tầng này là IP, cung cấp dịch vụ giao nhận gói tin cơ bản trên các mạng TCP/IP. Giao thức IP bổ sung một địa chỉ logic là gọi là địa chỉ IP được sử dụng để nhận diện thiết bị và định tuyến liên mạng.




Hình I-7. Các lớp tương ứng giữa TCP/IP và OSI

### 3. Tầng giao vận

Tầng giao vận còn được gọi là tầng truyền Trạm-tới-Trạm (Host-to-Host) chịu trách nhiệm cung cấp cho tầng ứng dụng các dịch vụ tạo lập phiên và truyền dữ liệu. Các giao thức chính của tầng Giao vận là TCP (Transmision Control Protocol) và UDP (User Datagram Protocol).

- TCP cung cấp các dịch vụ truyền thông tin cậy một-một (one-to-one), hướng liên kết (connection-oriented). TCP chịu trách nhiệm thiết lập các kết nối TCP, gửi các gói tin có sắp xếp, thông báo, và các gói tin phục hồi dữ liệu bị mất trong quá trình truyền.
- UDP cung cấp các dịch vụ truyền tin một-một, một-nhiều, không liên kết và không tin cậy. UDP được sử dụng khi lượng dữ liệu cần truyền nhỏ (ví dụ dữ liệu không điền hết một gói tin), khi việc thiết lập liên kết TCP là không cần thiết, hoặc khi các ứng dụng hoặc các giao thức tầng trên cung cấp dịch vụ đảm bảo trong khi truyền.

Tầng Giao vận chịu trách nhiệm tầng Giao vận trong mô hình OSI và một số nhiệm vụ của tầng Phiên (Session) của OSI.

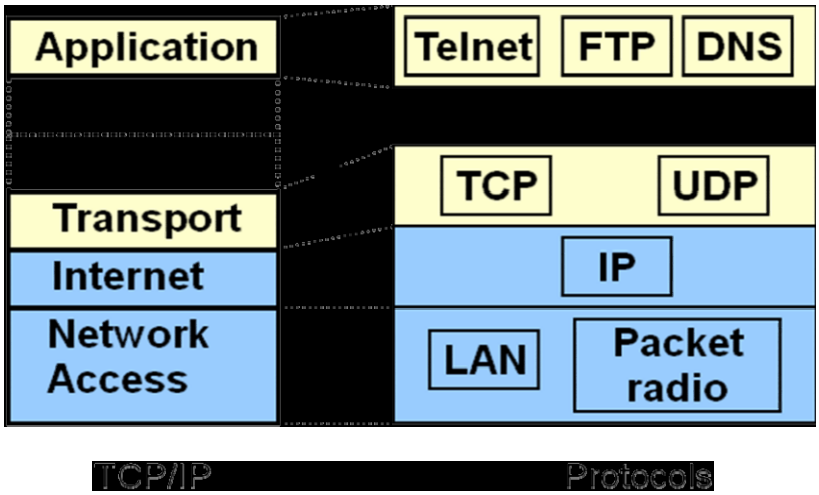
### 4. Tầng ứng dụng:

Tầng ứng dụng cung cấp các ứng dụng với khả năng truy cập các dịch vụ của các tầng khác và định nghĩa các giao thức mà các ứng dụng sử dụng để trao đổi dữ liệu. Có nhiều giao thức tầng ứng dụng và các giao thức mới luôn luôn được phát triển.

Các giao thức được ứng dụng rộng rãi nhất của tầng ứng dụng được sử dụng để trao đổi thông tin của người sử dụng là:

- Giao thức truyền tin siêu văn bản HTTP (HyperText Transfer Protocol) được sử dụng để truyền các tệp tạo nên trang web của World Wide Web.

- Giao thức FTP - File Transfer Protocol đươợc sử dụng để thực hiện truyền file.
- Giao thức SMTP - Simple Mail Transfer Protocol đươợc sử dụng để truyền các thông điệp thư và các tệp đính kèm.
- Telnet, một giao thức mô phỏng trạm đầu cuối, được sử dụng để đăng nhập từ xa vào các máy trạm trên mạng.




Hình I-8 Các giao thức của TCP/IP

**Chuẩn mạng máy tính(network standards)**

Tình trạng không tương thích gữa các mạng đặc biệt là các mạng trên thị trường gây trở ngại cho những người sử dụng khác nhau. Do đó cần phải xây dựng mô hình chuẩn làm cơ sở cho các nhà nghiên cứu, thiết kế mạng để tạo ra các sản phẩm mới về mạng, dễ phổ cập, sản xuất, sử dụng. Các chuẩn có vai trò quan trọng trong công tác thiết kế và xây dựng các hệ thống kỹ thuật và công nghệ.

*Chuẩn hóa mạng máy tính là nêu ra các tiêu chuẩn cơ bản thống nhất về cấu trúc mạng giúp cho các mạng khác nhau có thể trap đổi thông tin được với nhau.*

Để mạng hoạt động đạt khả năng tối đa, các tiêu chuẩn được chọn phải cho phép mở rộng mạng để có thể phục vụ những ứng dụng không dự kiến trước trong tương lai tại lúc lắp đặt hệ thống và điều đó cũng cho phép mạng làm việc với những thiết bị được sản xuất từ nhiều hãng khác nhau.

Một số tổ chức thực hiện chuẩn hóa mạng:

1. ISO (*International Standards Organization* – Tổ chức chuẩn hóa quốc tế) hoạt động dưới sự bảo trợ của LHQ. Thành viên của ISO là các cơ quan tiêu chuẩn hóa của các quốc gia và các ban chuyên môn. Ban TC97 được chia ra thành các tiểu ban và các nhóm công tác.

2. IEEE (*Institute of Electrical and Electronic Engineers* - Viện nghiên cứu các vấn đề về kỹ thuật điện và điện tử Mỹ) chịu trách nhiệm về tầng Data Link và physical. Phân ban các chuẩn này là phân ban 802 ( thành lập tháng 2 năm 1980)
3. CCITT (*Commite Consultatof Intẻnational pour Télégraphe et Téléphone*- Tổ chức tư vấn quốc tế về điện báo và điện thoại) hoạt động dưới sự bảo trợ của LHQ, chuyên nghiên cứu nhằm công bố các khuyến nghị thống nhất về mạng máy tính. Bao gồm các khuyến nghị liên quan đến việc truyền dữ liệu trên mạng, mạng ISDN.
4. ANSI (*American National Standards Institute)* – Viện nghiên cứu các chuẩn quốc gia Mỹ).
5. ECMA (*European Computer Manufactures Association)* – Hiệp hội máy tính Châu Âu.
6. ATM Forum (*Asynchronous Transfers Mode)* - Thực hiện các giải pháp cho mạng ISDN.
7. IETF (*Internet Enggineering Task Force)* - Sản xuất các chuẩn liên quan đến Internet (SNMP, TCP/IP…)

## I.5. Hệ điều hành trong môi trường mạng

Việc lựa chọn hệ điều hành mạng (NOS – Network Operating System) làm nền tảng cho mạng phụ thuộc vào kính cỡ của mạng hiện tại và sự phát triển trong tương lai, ngoài ra còn tùy thuộc vào những ưu điểm và nhược điểm của từng hệ điều hành.

Một số hệ điều hành mạng phổ biến hiện nay:

- Hệ điều hành UNIX: là hệ điều hành do các nhà khoa học xây dựng và được dùng phổ biến trong giới khoa học, giáo dục. Hệ điều hạnh mạng UNIX là hệ điều hành đa nhiệm, đa người sử dụng, phục vụ cho truyền thông tốt. Nhược điểm của nó là hiện nay có nhiều version khác nhau, không thống nhất gây khó khăn cho người sử dụng và hệ điều hành này phức tạp.
- Hệ điều hành mạng Windows 2000: là hệ điều hành của hãng Microsoft, cũng là hệ điều hành đa nhiệm, đa người sử dụng. Được xây dựng dựa trên công nghệ của hệ điều hành Windows NT. Đặc điểm của nó tương đối dễ sử dụng , hỗ trợ mạnh cho phần mềm WINDOWS. Windows 2000 có thể liên kết tốt với máy chủ Novell Netware, Unix. Tuy nhiên, để chạy có hiệu quả, Windows 2000 Server đòi hỏi cấu hình máy tương đối mạnh. Phiên bản tiếp theo là hệ điều hành Windows Server 2003.
- Hệ điều hành mạng NetWare: là hệ điều hành của hãng Novell, nó có thể dùng cho các mạng nhỏ (khoảng từ 5 – 25 máy tính) và cũng có thể dùng cho các mạng lớn gồm hàng trăm máy tính. Netware là hệ điều hành LAN

dùng cho các máy tính theo chuẩn IBM hay các máy Apple Macintosh, chạy trên hệ điều hành MS-DOS hoặc OS/2.

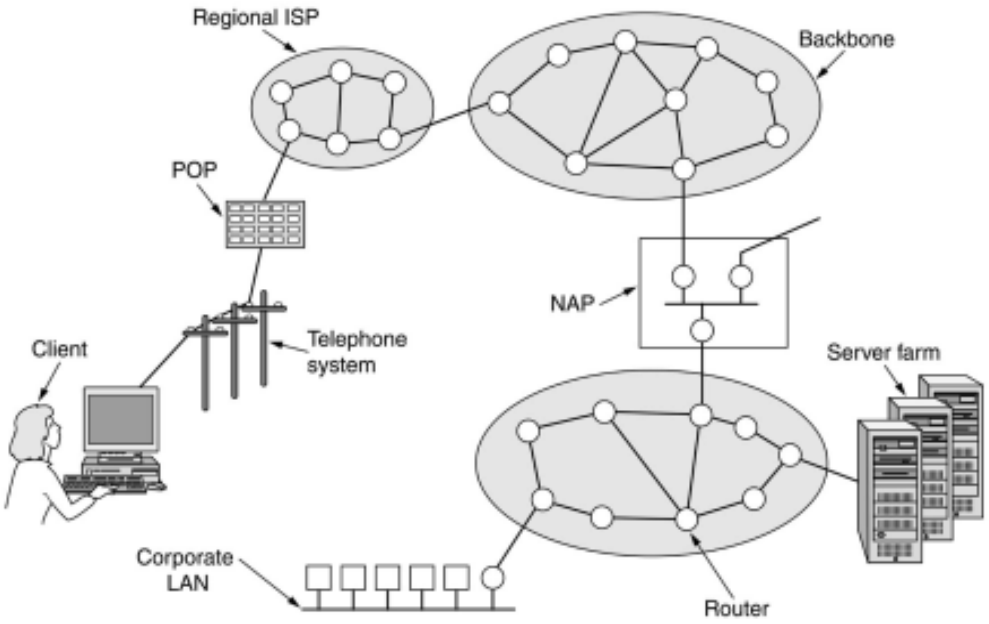
## I.6. Mạng Internet

Vào những năm 60 thế kỷ 20, Bộ Quốc phòng Mỹ cho triển khai một mạng lưới thông tin với yêu cầu: nếu như một trạm trung chuyển nào đó trong mạng bị phá hủy, toàn bộ hệ thống thông tin vẫn hoạt động bình thường… Cơ quan Nghiên cứu Dự án Cao cấp (ARPA – Advanced Research Projects Agency) thuộc Bộ Quốc phòng Mỹ được giao trách nhiệm thực hiện việc nghiên cứu kỹ thuật liên mạng(internet) nhằm đáp ứng yêu cầu trên. Đây là mạng chuyển mạch gói (paket switching) đầu tiên trên thế giới, lấy tên là ARPAnet. Ban đầu, ARPAnet chỉ gồm một vài mạng nhỏ được chọn lựa của các trung tâm nghiên cứu và phát triển khoa học. Giao thức truyền thông lúc bấy giờ là kiểu *điểm- điểm*, rất chậm và thường xuyên gây tắc nghẽn trên mạng. Để giải quyết vấn đề này, vào năm 1974 Vinton G. Cerf và Robert O. Kahn đưa ra ý tưởng thiết kế một bộ giao thức mạng mới thuận tiện hơn, đó chính là tiền thân của giao thức TCP/IP.

Tháng 09/1983, dưới sự tài trợ của Bộ Quốc phòng Mỹ, Berkeley Software Distribution đưa ra bản Berkeley UNIX 4.2BSD có kết hợp giao thức TCP/IP. biến TCP/IP thành phương tiện kết nối các hệ thống UNIX. Trên cơ sở đó , mạng ARPANET nhanh chóng lan rộng và chuyển từ mạng thực nghiệm sang hoạt động chính thức: nhiều trường đại học, viện nghiên cứu ghi tên gia nhập để trao đổi thông tin. Đến năm 1984, mạng ARPANET được chia thành hai nhóm là MILNET, dành cho Quốc phòng và nhóm mạng thứ hai vẫn gọi là ARPANET, dành cho nghiên cứu và phát triển. Hai nhóm này vẫn có mối liên hệ trao đổi dữ liệu với nhau qua giao thức TCP/IP và được gọi chung là Internet.

Mạng Internet đã và đang trở thành phương tiện trao đổi thông tin toàn cầu, là phương thức thông tin nhanh với lưu lượng truyền tải dữ liệu rất lớn. Thông qua Internet mà các nhà nghiên cứu khoa học kỹ thuật, các cơ quan giáo dục đào tạo, các nhà doanh nghiệp,… có thể trao đổi thông tin với nhau, hoặc truy cập thông tin của nhau về các công trình, các lĩnh vực nghiên cứu mới nhất; về các phương pháp, hình thức giáo dục và đào tạo, về các thông tin kinh tế, thị trường giá cả,… một cách nhanh chóng, thuận tiện và dễ dàng.

Mạng Internet không phải là một mạng đơn mà là bao gồm nhiều mạng con (sub-network) được kết nối với nhau thông qua các cổng (gateway). Thuật ngữ mạng con ở đây mang nghĩa một *đơn vị mạng hoàn chỉnh* trong hệ thống mạng lớn. Mạng con hoàn toàn có thể là một mạng WAN với quy mô quốc gia và có khả năng hoạt động độc lập với Internet. Do giao thức TCP/IP không phụ thuộc lớp vật lý, các mạng con có thể sử dụng những công nghệ ghép nối khác nhau (như Ethernet, X.25,...) mà vẫn giao tiếp được với nhau.




Hình I-9.Mô hình mạng Internet

Các cổng được dùng để nối các mạng con tạo thành mạng lớn.

Có hai cách kết nối mạng như sau:

- Máy con nối trong mạng LAN( hay WAN) và mạng này nối với Internet
- Máy con nối đến một trạm cung cấp dịch vụ Internet (Internet Service Provider), thông qua đó kết nối vơi Internet. Các trạm ISP lại kết nối với Internet thông qua IAP (Internet Access Provider). Một IAP có thể làm luôn chức năng của ISP nhưng ngược lại thì không.

# Chương II. Tầng vật lý

## II.1. Chức năng

Tầng vật lý cung cấp phương thức truy cập vào đường truyền vật lý để truyền các dòng bit không cấu trúc, ngoài ra nó cung cấp các chuẩn về điện, dây cáp, đầu nối, kỹ thuật nối mạch điện, điện áp, tốc độ cáp truyền dẫn, giao diện nối kết và các mức nối kết..

## II.2. Môi trường truyền tin

Mục đích lắp đặt cáp là đảm bảo dung lượng (tốc độ) cần thiết cho các nhu cầu truyền thông trên mạng. Để hệ thống cáp hoạt động ổn định, người quản trị mạng cần cân đối các yếu tố sau:

- Tốc độ truyền lớn nhất của hệ thống cáp hiện hành, khả năng nâng cấp.
- Nhu cầu về tốc độ truyền thông trong những năm tới (5-10 năm) là bao nhiêu.
- Chọn những loại cáp nào có trên thị trường.
- Chi phí để lắp đặt cáp dự phòng.

Việc kết nối vật lý một máy tính vào mạng được thực hiện bằng cách cắm một card giao tiếp mạng NIC (Network Interface Card) vào khe cắm của máy tính và nối với cáp mạng. Sau khi kết nối vật lý hoàn tất, việc quản lý truyền tin giữa các trạm trên mạng phục thuộc vào phần mềm mạng.

NIC sẽ chuyển gói dữ liệu vào mạng LAN, gói tin được truyền đi như một dòng các bit dữ liệu thể hiện bằng các biến thiên tín hiệu điện. Khi nó chạy trong cáp dùng chung, mọi trạm gắn với cáp đều nhận tín hiệu này. NIC ở mỗi trạm sẽ kiểm tra địa chỉ đích trong tín hiệu đầu của gói để xác định đúng địa chỉ cần đến, đích ở trạm đó sẽ sao chép gói tín hiệu rồi lấy dữ liệu ra khỏi khung tin và đưa vào máy tính.

Đặc tính của cáp bao gồm sự nhạy cảm với nhiễu của điện, độ mềm dẻo và khả năng uốn nắn để lắp đặt, cự ly truyền dữ liệu và tốc độ truyền (Mbps).

Có ba nhóm cáp chính được sử dụng để nối hầu hết các mạng

- Cáp đồng trục (Coaxial)
- Cáp xoắn đôi (Twisted-pair)
- Cáp quang (Fiber Optic)

### II.2.1. Card mạng

Card mạng, còn được gọi là card giao tiếp mạng-NIC, được lắp đặt tại mỗi máy trong mạng cục bộ. Card này có nhiệm vụ chuyển dữ liệu từ máy tính vào cáp mạng và ngược lại. Quá trình này chính là sự chuyển đổi từ tín hiệu số của máy tính thành tính hiệu điện hay quang được truyền trên cáp mạng. Đồng thời card mạng cũng thực hiện chức năng tổ hợp dữ liệu thành các gói và xác định nguồn đích của gói.

Hình II-1 Card giao tiếp mạng

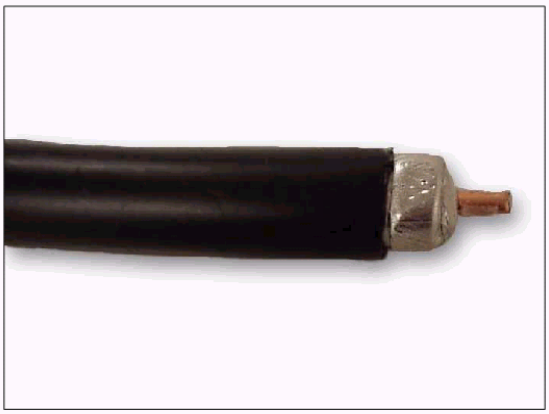
Các loại đầu nối cho cáp mạng:

- Mạng Thin Enthernet sử dụng các đầu cáp đồng trục BNC.
- Mạng Thick Net sử dụng jack nối AUI 15 chân để cắm vào đầu DB 15 của card mạng.
- Mạng Ethernet Twisted-pair sử dụng đầu nối RJ45.

### II.2.2. Cáp đồng trục:

Cáp đồng trục được chế tạo gồm một dây đồng ở giữa chất cách điện, xung quanh chất cách điện được quấn bằng dây bên kim loại làm dây đất. Giữa dây đồng dẫn điện và dây đất có một lớp cách ly, ngoài cùng là vỏ bọc bảo vệ.

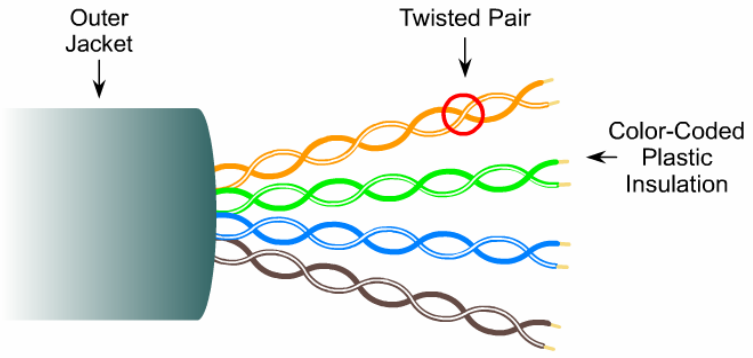
Cáp đồng trục có hai loại : loại nhỏ (Thin) và loại to (Thick).



Hình II-2 Cáp đồng trục

### II.2.3. Cáp xoắn cặp:

Cáp xoắn gồm hai sợi dây đồng được xoắn cách điện với nhau. Nhiều đôi dây cáp xoắn gộp với nhau và được bọc chung bởi vỏ cáp hình thành cáp nhiều sợi. Loại cáp này có đặc tính là dễ bị ảnh hưởng của nhiễu điện nên chỉ truyền được dữ liệu ở cự ly khoảng 100m. Cáp xoắn đôi có hai loại là cáp xoắn đôi không có vỏ bọc(UTP) và cáp xoắn đôi có vỏ bọc(STP).




Hình II-3 Cáp xoắn đôi UTP

### II.2.4. Cáp quang:

Khi tín hiệu số được điều chế thành các tín hiệu xung ánh sáng thì được truyền tải qua cáp quang. Cáp quang bao gồm một sợi thủy tinh cực mảnh gọi là lõi (core), được bao phủ bởi lớp thủy tinh đồng tâm gọi là lớp vỏ bọc hay lớp phủ (cladding). Đôi khi các sợi được làm bằng chất dẻo. Chất dẻo dễ lắp đặt hơn nhưng không thể mang xung ánh sáng đi xa như thủy tinh.

Mỗi sợi thủy tinh chỉ truyền được tín hiệu theo một hướng nhất định, do đó cáp thường có 2 sợi nằm trong vỏ bọc riêng biệt: một sợi truyền và một sợi nhận. Cáp quang có thể truyền tín hiệu đi xa với tốc độ cực nhanh (theo lý thuyết cáp quang có thể truyền tín hiệu với tốc độ tối đa 200.000 Mbps).

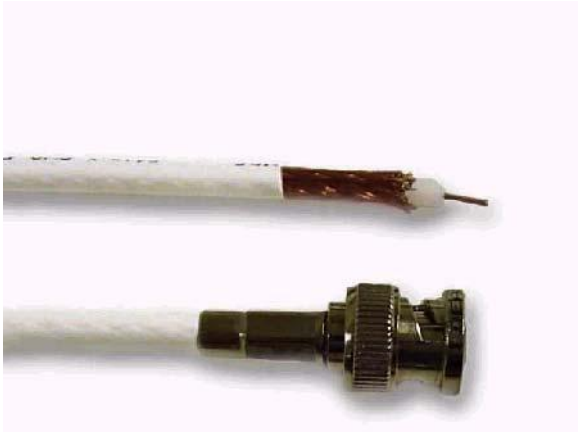
## II.3. Đặc tả các loại cáp mạng

Thông thường đặc điểm kĩ thuật của cáp mạng gồm có:

- Tốc độ truyền dữ liệu tối đa. Đây là đặc điểm quan trọng và ảnh hưởng bởi vật liệu chế tạo cáp.
- Loại dữ liệu truyền. Có hai kĩ thuật truyền tín hiệu mã hóa lên mạng là truyền ở dải tầng gốc (baseband) và truyền ở dải tầng rộng (boardband).
- Tín hiệu có thể truyền bao xa trên loại cáp cụ thể trước khi bị suy giảm

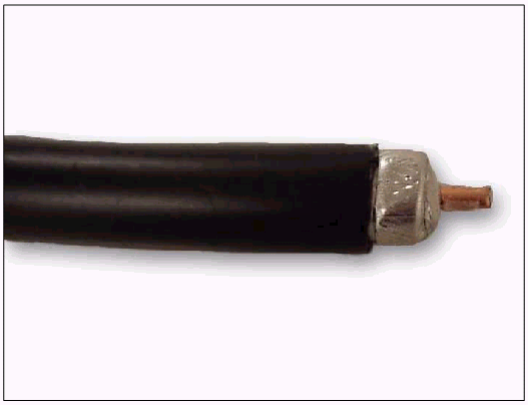
Một số ví dụ:

- 10BASE2
  - Tốc độ truyền dẫn 10 Mbps
  - Loại dữ liệu truyền là dải tầng gốc (kĩ thuật số)
  - Khoảng cách tối đa giữa hai nút là 200 m, còn gọi là cáp Thinnet



Hình II-4 Cáp ThinNet

- 10BASE5
  - Tốc độ truyền dẫn 10 Mbps
  - Loại dữ liệu truyền là dải tầng gốc (kĩ thuật số)
  - Khoảng cách tối đa giữa hai nút là 500 m, còn gọi là cáp Thicknet



Hình II-5 Cáp ThickNet

- 100BASET
  - Tốc độ truyền dẫn 100 Mbps
  - Loại dữ liệu truyền là dải tầng gốc (kĩ thuật số)
  - Là cáp xoắn đôi.

Hình II-6 Cáp xoắn đôi

## II.4. Chuẩn giao diện

### II.4.1. Modem:

Modem là bộ điều chế và giải điều chế, biến đổi các tín hiệu số thành tín hiệu tương tự và ngược lại trên mạng điện thoại.

Tín hiệu số từ máy tính đến modem, được modem biến đổi thành tín hiệu tương tự để có thể đi qua mạng điện thoại. Tín hiệu này đến modem ở máy tính đầu kia, được biến đổi thành tín hiệu số đưa vào máy tính này.

Các kỹ thuật điều chế cơ bản:

- Điều chế biên độ AM: Các tín hiệu 0 và 1 được phân biệt bằng biên độ, còn tầng số của tín hiệu giống nhau. Điều chế biên độ dễ thực hiện nhưng dễ bị nhiễu.
- Điều chế tần số FM: Các tín hiệu 0 và 1 được phân biệt bởi tần số, còn biên độ tín hiệu giống nhau. Kỹ thuật này phức tạp hơn nhưng tính chống nhiễu cao.
- Điều chế theo pha PM: Các tín hiệu 0 và 1 được phân biệt theo pha của dao động, còn biên độ và tần số của các tín hiệu giống nhau. Điều pha cũng phức tạp nhưng tính chống nhiễu cao.

Để tăng tốc độ truyền tin người ta kết hợp điều pha và điều biên gọi là điều pha biên.

Hiện nay có nhiều loại modem từ loại thấp 300, 600, 1200, 2400 bit/s đến loại 9600 bit/s.

Các phương thức truyền dữ liệu giữa hai điểm có thể là:

- Một chiều đơn (simplex).

- Hai chiều luân phiên (half-duplex).
- Hai chiều đầy đủ (duplex)

### II.4.2. DTE và DCE:

DTE (Data Terminal Equipment-Đầu cuối số liệu): là các khái niệm được sử dụng để chỉ các máy mà người sử dụng bình thường thao tác trực tiếp lên đó. Các máy này có thể là máy tính hay trạm cuối.

DCE (Data Communication Equipment-Đầu cuối truyền): là khái niệm chỉ các thiết bị cuối kênh dữ liệu có chức năng nối các DTE với các đường truyền vật lý và chuyển đổi dữ liệu. DCE có thể là các modem, multiplexer,..

# Chương III. Giao thức tầng liên kết dữ liệu

## III.1. Chức năng và dịch vụ

### III.1.1. Chức năng

Tầng liên kết dữ liệu (Data link) thực hiện các công việc chính như sau:

- Định danh các thiết bị trên mạng, cấu hình logic của mạng.
- Điều khiển luồng dữ liệu và việc truy nhập ở tầng vật lý
- Phát hiện và chỉnh sửa các lỗi xuất hiện trong quá trình truyền dữ liệu.

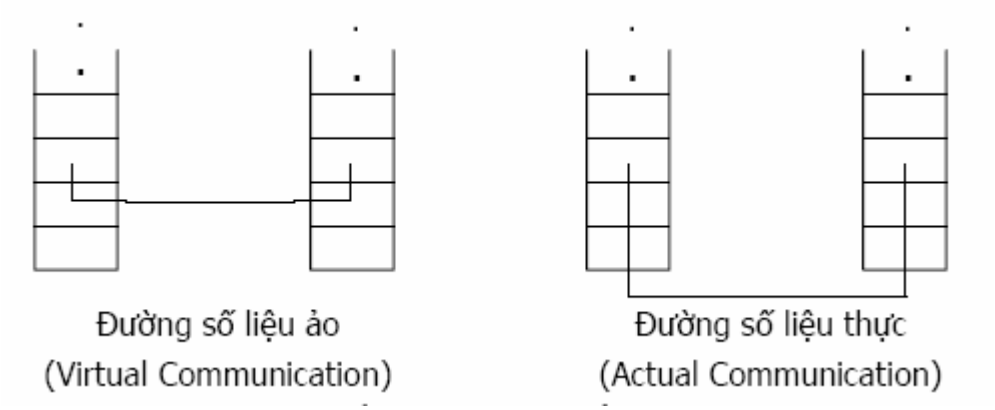
Chức năng chính của tầng LKDL là tách rời các khung thành các bit để truyền đi và kiến tạo các khung (frames) từ các dòng bit nhận được.

Tầng LKDL nghiên cứu các thuật toán thực hiện thông tin hiệu suất, tin cậy giữa hai máy cạnh nhau ở tầng 2. Đưa ra các thủ tục truyền tin có lưu ý đến lỗi có thể xảy ra do nhiễu trên đường dây, sự trễ do lan truyền.

Thông thường, tầng LKDL có liên quan đến nhiễu của tín hiệu của phương tiện truyền vật lý, cho dù là truyền qua dây đồng, cáp quang hay truyền thông qua sóng ngắn. Nhiễu là một vấn đề rất thông thường và có thể do rất nhiều nguồn khác nhau, trong đó có cả nhiễu của các tia vũ trụ, nhiễu do tạp âm của khí quyển và từ các nguồn khác nhau.

### III.1.2. Cung cấp dịch vụ cho tầng mạng

Tầng 2 chuyển dữ liệu từ mức 3 ở máy nguồn tới mức 3 của máy nhận.




Hình III-1. Đường truyền dữ liệu trong tầng LKDL.

Các dịch vụ tầng 2 có thể là:

1. Dịch vụ không kết nối, không hồi báo (*Unacknowledged Connectionless Service)*
2. Dịch vụ không kết nối, có hồi báo (*Acknowledged Connectionless Service)*
3. Dịch vụ có kết nối *(Connection Oriented Service)*

Dịch vụ kết nối có hường gồm 3 giai đoạn: *kết nối, truyền số liệu, tách bỏ liên kết* (kết thúc): CONECT, DATA, DISCONNECT. Dịch vụ không kết nối được thể hiện bằng một bước duy nhất là truyền tin, không cần thiết lập liên kết logic. Các đơn vị dữ liệu truyền độc lập với nhau.

### III.1.3. Khung tin - Nhận biết gói tin

Để cung cấp dịch vụ cho tầng mạng, tầng LKDL phải dùng dịch vụ được cung cấp từ tầng vật lý. Tầng vật lý tiếp nhận dòng bit và giao cho nơi nhận. Dòng bit này có thể có lỗi. Tầng LKDL sẽ kiểm tra và nếu cần sẽ sửa lỗi.

Tầng LKDL tách dòng bit thành các khung (flame) và tính thông số kiểm tra (checksum) cho mỗi khung tin này, nếu kết quả tính được khác với checksum chứa trong khung tin, nghĩa là có lỗi và khi đó lỗi sẽ được thông báo cho nơi gởi.

Muốn tách các khung tin, có thể chèn các đoạn phân tách (timegaps) vào giữa các khung tin, giống như khoảng trống (space) giữa các từ trong văn bản. Nhưng điều này khó thực hiện nên người ta thường dùng các phương pháp sau:

- Đếm số ký tự: hiện nay ít được dùng vì từ đếm cũng bị lỗi khi truyền.
- Dùng ký tự bắt đầu (STX) và kết thúc (ETX) với ký tự đệm (DLE).
- Dùng các cờ (*flags)* đánh dấu bắt đầu và kết thúc với các bít đệm.

### III.1.4. Điều khiển dòng truyền

Để tận dụng đường dây, các tín hiệu biên nhận (ACK) được ghép cùng với gói tin. Khi gói tin đến, thay cho việc trả lời ngay tín hiệu bên nhận, bên thu nhận tiếp gói tin từ mạng để ghép cùng tín hiệu biên nhận và gởi trả lời. Kỹ thuật này được gọi là Piggybacking (ghép thêm).

Ưu điểm của phương pháp này là tận dụng đường kênh. Nếu quá thời gian (vài μs) mà không có gói tín hiệu mới thì bên thu phải trả lời tín hiệu biên nhận để bên phát lại không phát lại gói tin cũ.

Để tận dụng đường kênh, bên phát và bên thu phải đồng bộ để bên thu kịp nhận các gói tin và bên phát cũng không lãng phí đường truyền, người ta dùng cơ chế cửa sổ trượt (sliding windows). Cửa sổ mở to thì số gói tin đưa lên đường kênh nhiều hơn (tốc độ nhanh), cửa sổ mở bé thì số gói kênh đưa lên đường kênh ít lại (tốc độ chậm lại). Tương tự như cửa chắn đập nước.

## *1. Cơ chế cửa sổ*

Người ta dùng số bit để đặc trưng cho độ rộng cực đại của cửa sổ. Trong thủ tục này, mỗi gói tin đi sẽ được đánh số từ 0 đến Max (Max là $2^n - 1$) thông qua một dãy gồm các số 0, 1. Chẳng hạn cửa sổ 3 bit sẽ quản lý các gói tin có số từ 0Ặ 7. Ta có thể dùng n tùy ý.

Danh sách các gói tin gởi đi trong cửa sổ phát. Danh sách các gói tin nhận được gởi trong cửa sổ nhận, cửa sổ phát và nhận không bắt buộc phải có kích thước, giới hạn trên và dưới giống nhau.

Mặc dù thủ tục này cho phép tầng liên kết dữ liệu linh hoạt hơn về thứ tự gởi, nhận gói tin nhưng nó yêu cầu phải đảm bảo tầng mạng đích ở bên nhận có cùng thứ tự với tầng mạng nguồn ở bên gửi.

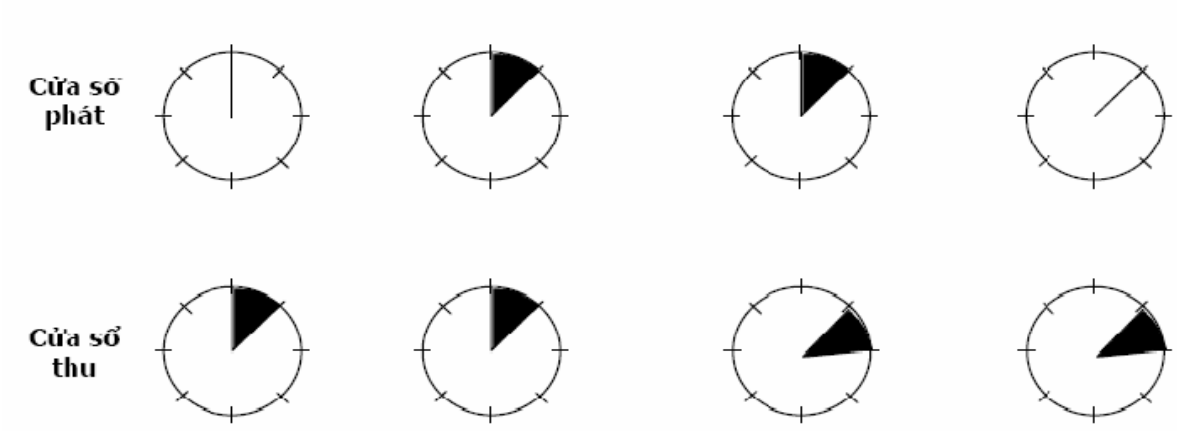
- ***Cửa sổ bên phát***

Trong cửa sổ bên phát đặt các gói tin gởi đi nhưng chưa nhận được tín hiệu biên nhận. Khi nhận được gói tin mới đến từ tầng mạng để phát đi, biên trên cửa sổ tăng 1 và khi có tín hiệu biên nhận biên dưới của cửa sổ tăng 1. Bên phát luôn giữ trong bộ nhớ các gói tin đã phát đi nhưng chưa nhận được tín hiệu biên nhận vì có thể phát lại. Như vậy nếu Max bằng n thì bên phát cần n vùng đệm để các gói tin đã phát đi nhưng chưa nhận được trả lời. Nếu cửa sổ đã tới Max thì tầng liên kết giữ liệu bên phát ngừng nhận tin từ tầng 3 cho đến khi có bộ đệm tự do.

- ***Cửa sổ bên nhận***

Cửa sổ bên nhận chứa các gói tin được chuyển đến. Khi gói tin có số thứ tự trùng biên dưới của cửa sổ được nhận, cửa sổ chuyển tin lên tầng ba, phát tín hiệu biên nhận và quay một đơn vị. Không như cửa bên phát, cửa sổ bên nhận luôn duy trì một kích thước. Khi kích thước cửa sổ bằng 1, tầng 2 nhận gói tin theo thứ tự. Nhưng nếu kích thước cửa sổ lớn hơn thì không phải như vậy.

Hoạt động của cửa số có kích thước là 3 bit với độ trượt một bit như sau:

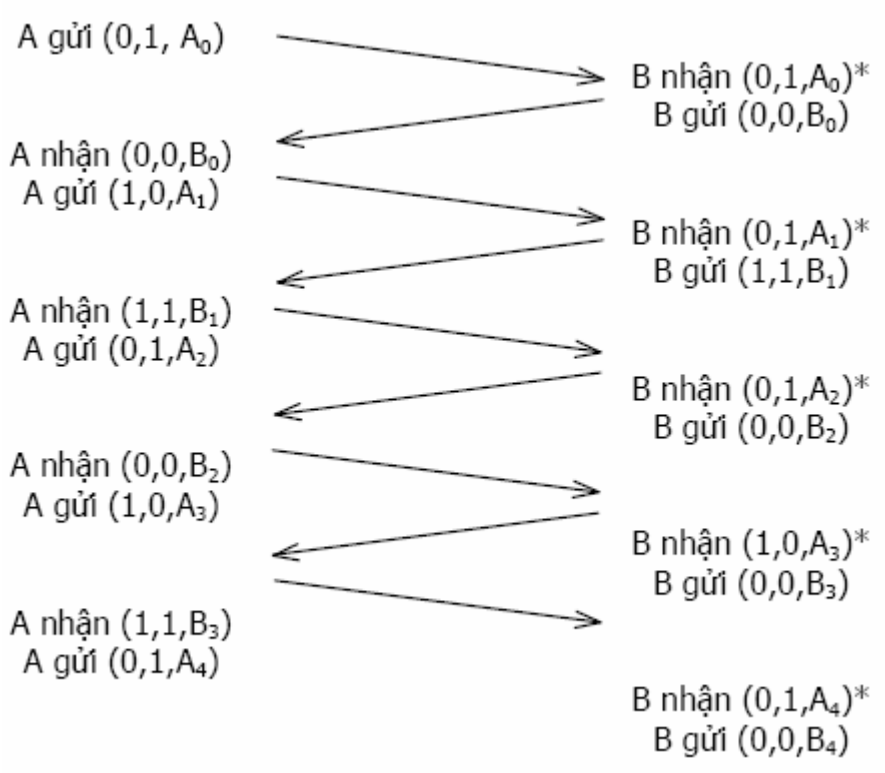



Hình III-2. Điều khiển dòng truyền theo cơ chế cửa sổ (Bắt đầu-Gửi gói tin đầu tiên-Nhận tin và trả lời ACK-Nhận ACK)

### *2. Trao đổi bản tin với cửa sổ 1 bit*

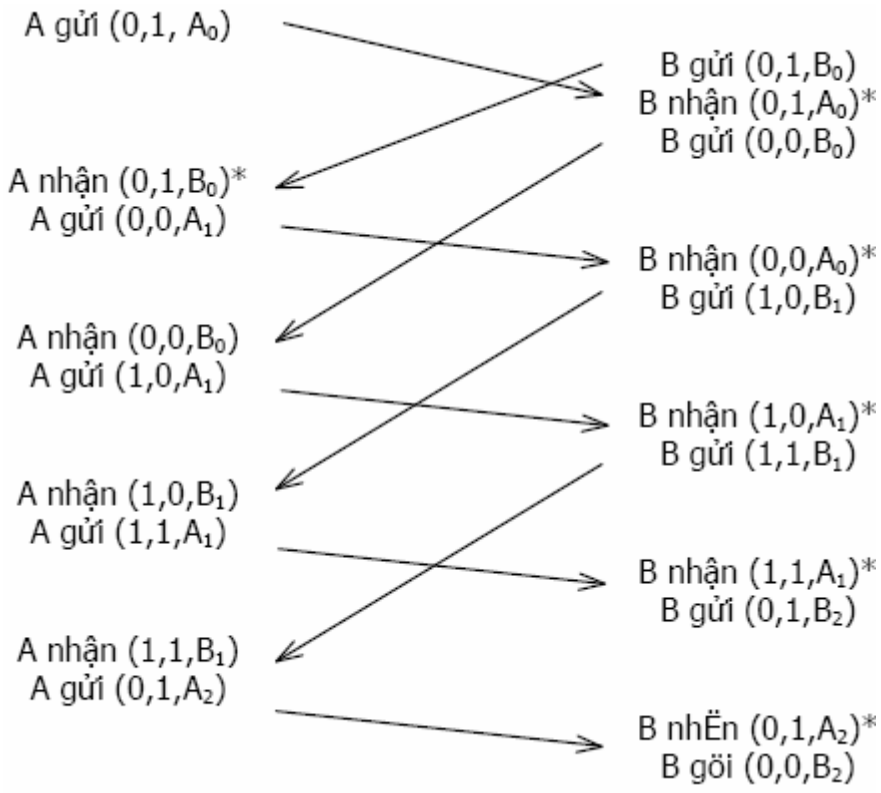
Bản tin gồm có gói tin với phần điều khiển (Header). Phần điều khiển gồm có số thứ tự phát *seg*, số thứ tự nhận của *ack*, số gói tin.

Trong trường hợp bình thường máy A gủi trước như sau:




Hình III-3. Trao đổi bản tin với cửa sổ 1 bit bình thường.

Trong truòng hợp bất thường máy A và B cùng gởi như sau:




Hình III-4. Trao đổi bản tin với cửa sổ 1 bit bất thường.

Máy A ở tầng 2 nhận gói tin ở tầng 3, tạo bản tin và gởi đi. Khi bản tin này đến tầng 2 máy B, nó sẽ được kiểm tra có bị lặp lại hay không. Nếu đúng là bản tin đang mong đợi thì nó được chuyển lên tầng 3 và cửa sổ nhận dịch đi một nấc.

Vùng tín hiệu biên nhận chứa số bản tin cuối cùng đã được nhận mà không có lỗi, nếu số này trùng với số bản tin vừa gởi, bên phát sẽ lấy bản tin tiếp theo từ tầng mạng. Nếu số không đúng nó phải gởi lại bản tin cũ.

### *3. Vận chuyển liên tục*

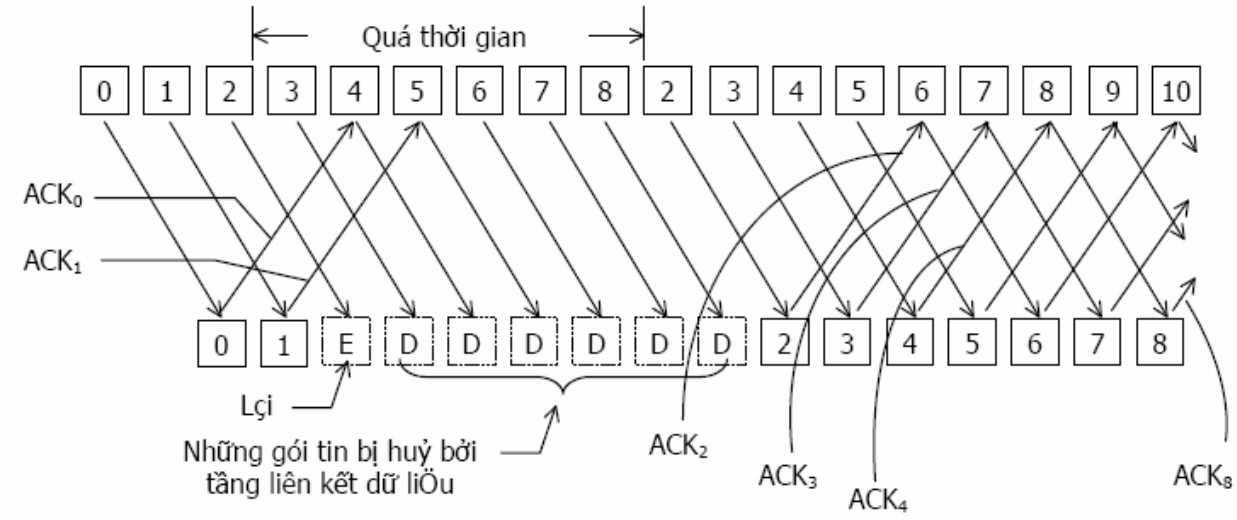
Thực tế cho thấy thời gian từ lúc phát gói tin đến khi nhận trả lời biên nhận ACK là không đáng kể. Khi đó, nếu đường kênh vệ tinh có tốc độ 50Kbp/s với trễ lan truyền 500 ms, ta dùng thủ tục điều chỉnh dòng truyền gởi gói tin là 1000 bit qua vệ tinh. Thời gian phát gói tin 20 ms, vậy sau 520 ms mới nhận được tín hiệu biên nhận cho gói tin 0 cũng vừa đến. Kỹ thuật này gọi là Pipe-Lining (vận chuyển liên tục).

Khi có gói tin ở đoạn giữa bị hỏng thì làm thế nào? Có bỏ những gói tin đúng đi tiếp sau nó không? Có hai phương pháp như sau:

- Phát lại các gói tin kể từ gói tin hỏng (*go back n)*
- Phát lại chỉ riêng gói tin bị hỏng, còn gọi phát tin có chọn lọc.
- Phát lại từ gói tin hỏng.

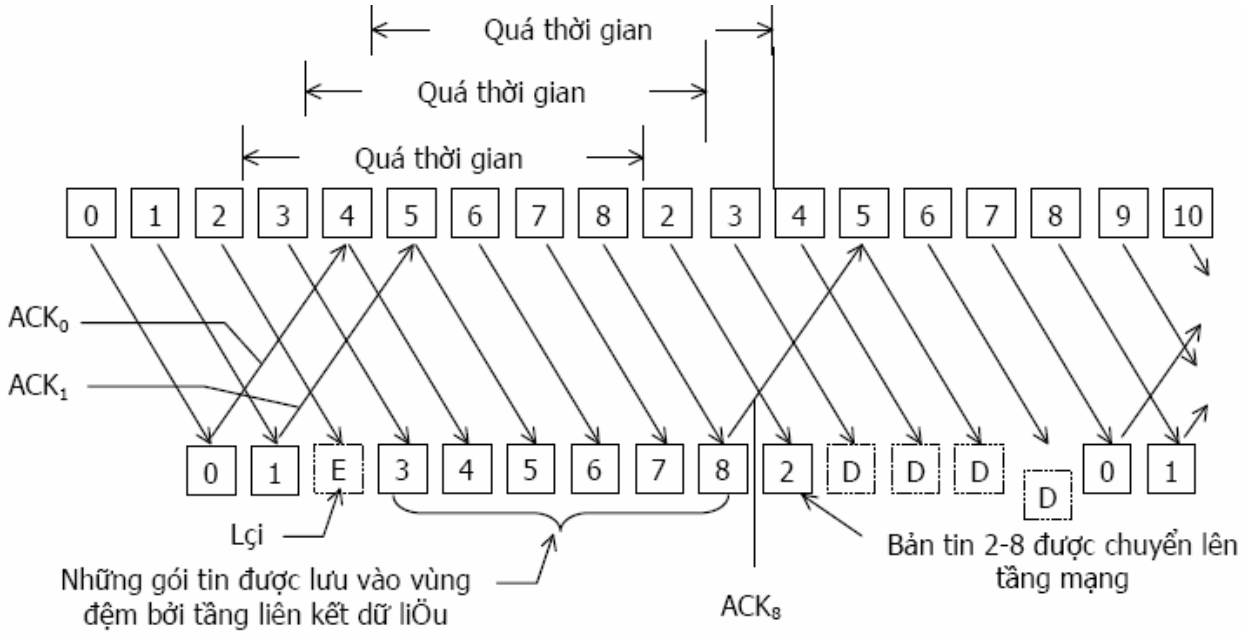
Trong trường hợp này, bên thu hủy bỏ các gói tin tiếp theo gói tin bị hỏng. Bên phát phát lại các gói tin chưa được biên nhận bắt đầu từ gói tin bị hỏng.

Phương pháp này lãng phí đường truyền vì phải phát lại nhiều gói tin.




Hình III-5. Cơ chế vận chuyển liên tục

* ***Phát lại có chọn lọc***




Hình III-6. Cơ chế phát bản tin có chọn lọc.

Trong phương pháp này, các gói tin nhận được có thể không theo thứ tự nhưng sẽ được sắp xếp lại để chuyển lên tầng mạng theo đúng thứ tự. Khi có gói tin bị lỗi, bên thu tiếp tục thu các gói tin đứng sau gói tin hỏng ở tầng 2. Bên phát chỉ phát lại gói tin hỏng. Phương pháp này ứng với cửa sổ bên thu lớn hơn 1 và đòi hỏi bộ nhớ lớn để các gói tin sau gói tin hỏng.

## III.2. Cơ chế phát hiện và sửa lỗi

Lỗi bit thường xảy ra trong frame. Mặc dù lỗi rất ít khi xảy ra, đặc biệt là trên cáp quang, tuy nhiên cần có những kỹ thuật để phát hiện lỗi khi lỗi xảy ra. Một kỹ thuật được biết trong việc phát hiện lỗi khi truyền là phương pháp kiểm tra CRC (cyclic redundancy check). Nó được sử dụng hầu hết trong các giao thức Byte-Oriented, Bit-Oriented, CSMA/CD và FDDI.

Hai phương pháp đơn giản được sử dụng rộng rãi là: two-demensional parity và checksum. Two-demensional parity được sử dụng trong giao thức BISYNC lúc nó truyền các ký tự ASCII. Checksum được sử dụng bởi một vài giao thức Internet.

Ý tưởng cơ bản của CRC là thêm các thông tin dư vào frame, thông tin này được sử dụng để phát hiện lỗi. Ví dụ chúng ta có thể truyền hai bản sao của dữ liệu, nếu hai bản sao giống nhau ở máy nhận, có thể là trong trường hợp này là cả hai đều đúng. Ngược lại, nếu hai bản sao này khác nhau thì một trong hai bản sao bị sai, do đó phải thực hiện truyền lại.

Nhược điểm của các tiếp cận trên:

- Thêm n bit dư cho một thông điệp n bit
- Không phát hiện sai nếu lỗi sai xảy ra ở cùng một vị trí.

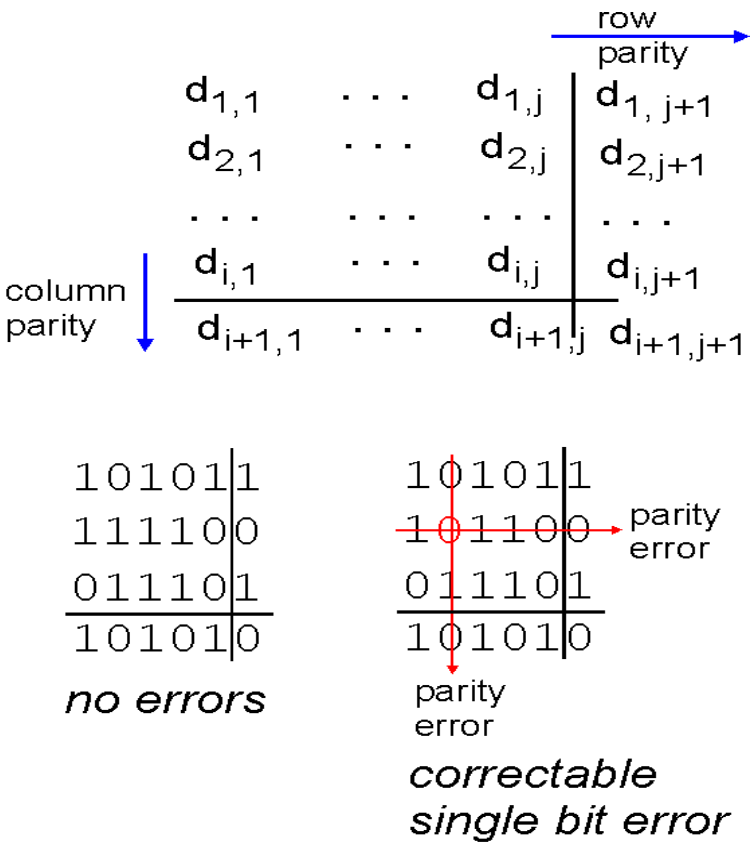
Chúng ta có thể hoàn toàn cung cấp một khả năng phát hiện lỗi tốt với việc gửi k bit dư cho một thông điệp n bit (k<<n). Ví dụ trên Ethernet, mỗi khung mang 12000 bit (1500byte) dữ liệu chỉ yêu cầu mã 32 bit CRC.

Việc thêm các bit không có nghĩa là thêm thông tin mới vào thông điệp. Thay vào đó, chúng có thể sử dụng một vài thuật toán tối ưu tác động trực tiếp vào thông điệp nguồn. Cả hai máy gửi và máy nhận biết chính xác thuật toán làm gì. Máy gửi tác động thuật toán đến thông điệp để tạo ra bit dư, sao đó nó truyền cả thông điệp và các bit dư. Máy nhận tác động cùng thuật toán vào thông điệp nhận, nếu phát hiện sai nó yêu cầu truyền lại hay sữa sai nếu có thể.

Phát hiện lỗi chỉ là một phần của vấn đề, vấn đề tiếp theo là xử lý lỗi khi lỗi được phát hiện. Có hai cách phương pháp được sử dụng lúc phát hiện một thông điệp bị lỗi.

- Thông báo cho máy gửi thông điệp bị lỗi và máy gửi sẽ truyền lại.
- Nếu lỗi chỉ xảy ra tại một số bit nào đó, một số thuật toán sẽ phát hiện lỗi và cho phép tạo lại một thông điệp đúng như ban đầu thậm chí sau khi thông điệp đã bị hỏng.

### a. Two-Dimension Parity




Hình III-7. Phương pháp Two-dimesion parity

**b. Internet Checksum**

Thuật toán này không sử dụng ở mức liên kết tuy nhiên nó cung cấp cùng chức năng với CRC và parity.

Ý tưởng: ta cộng tất cả các từ mà nó được truyền, sau đó truyền dữ liệu cùng với kết quả của phép cọng đó. Kết quả được gọi là checksum. Máy nhận thực hiện tính toán tương tự trên dữ liệu nhận và so sánh kết quả với kết quả cheksum. Nếu kết quả sai, máy nhận biết có lỗi xuất hiện. Thông thường người ta xem dữ liệu bị checksum là các số nguyên 16 bit, cộng tất cả các số nguyên này lại và ta được được kết quả là một số 16 bit. Đó chính là checksum.

Ưu điểm: chỉ thêm vào 16 bit nhưng có thể kiểm tra dữ liệu chiều dài bất kỳ.

Nhược điểm: nếu một cặp bit sai ở cùng một vị trí thì chúng không thể bị phát hiện.

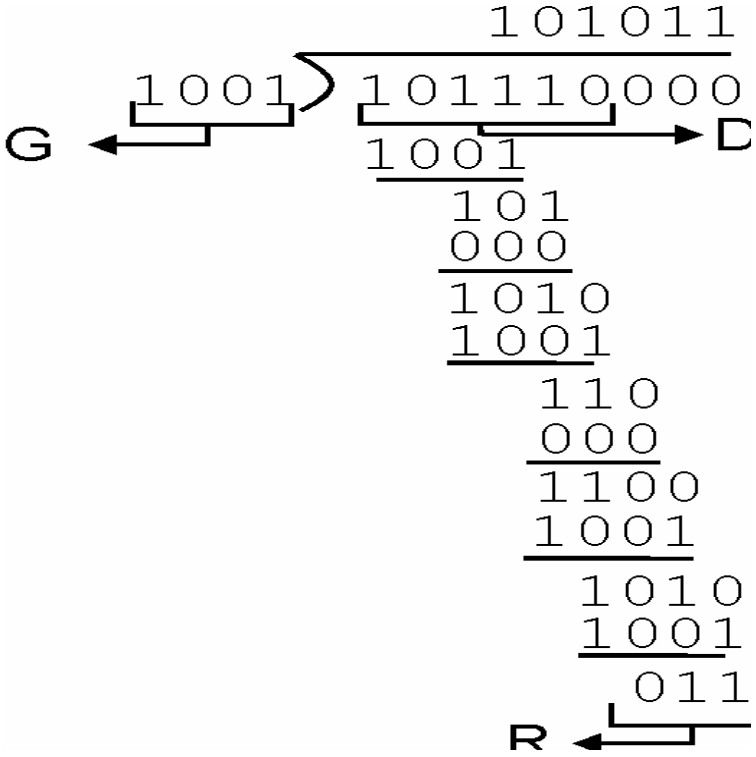
Lý do sử dụng một thuật toán này:

- Nó rất dễ cài đặt trong phần mềm. Kinh nghiệm trong APPANET thì sử dụng thuật toán checksum như thế là đầy đủ.

- Thuật toán này được bảo vệ bởi một giao thức end-to-end. Các lỗi chính hầu hết đã được phát hiện bởi các thuật toán phát hiện lỗi mạnh mẽ như là CRC tại mức liên kết.

**c. CRC**

CRC là phương pháp phát hiện lỗi thoả mãn việc sử dụng một số ít nhất các bit thêm vào nhưng có thể phát hiện tất cả các lỗi khi truyền. Ví dụ chỉ sử dụng 32 bit CRC có thể dùng để kiểm tra dữ liệu dài hàng ngàn byte.




Hình III-8. Ví dụ minh họa phương pháp CRC

**Ý tưởng:**

Một thông điệp n+1 bit có thể được biểu diễn bởi một đa thức bậc n. Đa thức sử dụng giá trị của mỗi bit trong thông điệp làm hệ số của đa thức.

Để hổ trợ cho việc tính CRC, máy gửi và máy nhận cùng sử dụng một đa thức chia. Có một nhóm các đa thức chia mà chúng là những chọn lựa rất tốt trên các các môi trường khác nhau và sự chọn lựa thường phụ thuộc vào việc thiết kế giao thức. Ví dụ Ethenet sử dụng CRC 32.

Lúc máy gửi muốn chuyển một thông điệp M(x) mà nó dài (n+1)bit, điều gì thật sự xảy ra với một thông điệp n+1 bit và k bit thêm vào.

- Gọi P(x) là đa thức gồm thông điệp truyền và bit dư.
- Nếu P(x) được truyền qua liên kết và không có lỗi xuất hiện trong quá trình truyền, thì thiết bị nhận có thể chia P(x) cho C(x) với phần

dư là 0. Ngược lại, nếu phần dư khác không thì máy nhận biết rằng có lỗi xuất hiện trong khi truyền.

Nhận xét đa thức:

- Các bậc của đa thức chỉ là 0 hoặc 1.
- B(x) có thể chia cho C(x) nếu bậc của nó cao hơn C(x).
- B(x) chỉ có thể chia một lần cho C(x) nếu mũ của chúng bằng nhau.
- Phần dư của B(x) chia cho C(x) có thể lấy từ kết quả của việc lấy B(x)-C(x).
- B(x) trừ C(x) thực chất là thực hiện phép XOR từng cặp hệ số.

**Thuật toán:**

Cộng k bit zero vào cuối thông điệp ta được thông điệp T(x).

Chia T(x) cho C(x) và tìm phần dư.

Trừ T(x) cho phần dư.

Mạng Ethernet và 802.5 sử dụng CRC 32, HDLC sử dụng CRC_CCITT. ATM sử dụng CRC-8, 10, 12.

Phương pháp kiểm tra lỗi này dễ dàng thi hành tại phần cứng, đơn giản chỉ là sử dụng thanh ghi và cổng XOR. Bảng 2.3 đưa ra một số đa thức sử dụng trong CRC.

| CRC | C(x) |
|---|---|
| CRC-8 | $x^8 + x^2 + x^1 + 1$ |
| CRC-10 | $x^{10} + x^9 + x^5 + x^4 + x^1 + 1$ |
| CRC-12 | $x^{12} + x^{11} + x^3 + x^2 + 1$ |
| CRC-16 | $x^{16} + x^{15} + x^2 + 1$ |
| CRC-CCITT | $x^{16} + x^{12} + x^5 + 1$ |
| CRC-32 | $x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$ |

## III.3. Các giao thức đa truy cập

Giao thức dùng để đánh giá khả năng của một mạng được phân chia bởi các trạm như thế nào. Hệ số này được quyết định chủ yếu bởi hiệu quả sử dụng môi trường truy xuất (medium access) của giao thức.

Mọi kênh phương tiện chỉ có thể hỗ trợ một lần tín hiệu. Nếu hai máy tính truyền trên kênh cùng một lúc, các tín hiệu của chúng sẽ gây nhiễu cho nhau (ví dụ như hai người cùng nói một lúc). Có hai phương pháp điều khiển việc truy nhập

phương tiện để không xảy ra sự cố gây nhiễu: truy cập ngẫu nhiên và truy cập có điều khiển.

*a. Loại truy cập ngẫu nhiên*

Trạm có thể truy nhập phương tiện truyền tùy theo ý muốn, bất kỳ ở thời điểm ngẫu nhiên nào.

- Kỹ thuật cập ngẫu nhiên đối với dạng bus
  - Phương pháp đa truy nhập sử dụng sóng mang (CSMA – Carrier Sense Multiple Access).
  - Phương pháp đa truy nhập sử dụng sóng mang với phát hiện xung đột ( CSMA/CD – With Collision Detection)
- Kỹ thuật cập ngẫu nhiên đối với dạng vòng
  - Phương pháp chèn thanh ghi (Registeer insertion)
  - Phương pháp vòng có ngăn (Slotted-ring)

b. *Loại truy nhập có điều khiển*

Phương pháp điều khiển tranh chấp thường thích hợp với các mạng có sự trao đổi dữ liệu không liên tục và tương đối ít máy tính. Đây là đạng thông dụng trong cấu trúc mạng cục bộ.

- Kỹ thuật bus với thẻ bài (Tocken Bus): dùng cho các mạng LAN.
- Kỹ thuật vòng với thẻ bài ( Tocken Ring): dùng cho các mạng LAN
- Kỹ thuật tránh xung đột: dùng cho các mạng cục bộ tốc độ cao

### III.3.1. Phương pháp CSMA

Còn được gọi là phương pháp LBT (Listen Before Talk – Nghe trước khi nói). Một trạm có dữ liệu cần truyền trước hết phải "nghe" xem phương tiện truyền rỗi hay bận. Nếu rỗi thì bắt đầu truyền tin, còn nếu bận thì thực hiện một trong ba giải thuật sau:

- Giải thuật '*non-persistent' :* Trạm rút lui (không kiên trì) chờ đợi một thời gian ngẫu nhiên nào đó rồi bắt đầu 'nghe' đường truyền. Giải thuật này có hiệu quả tránh xung đột nhưng có thời gian chết.
- Giải thuật '*l-persistent':* trạm tiếp tục nghe đến khi phương tiện truyền rỗi thì tiến hành truyền dữ liệu đi (với xác xuất 1). Giải thuật này giảm thời gian chết, xong nếu có nhiều trạm cùng chờ và tiến hành phát dữ liệu cùng một lần thì sẽ xảy ra xung đột.
- Giải thuật '*p-persistent':* Trạm tiếp tục nghe, đến khi phương tiện truyền rỗi thì tiến hành phát tin với một xác suất nhất định nào đo (mỗi trạm có gắn một hệ số ưu tiên). Ngược lại trạm 'rút lui' trong

một thời gian cố định rồi truyền với sác xuất p hoặc tiếp tục chờ đợi với sác xuất 1-n. Giải thuật này phức tạp nhưng giảm được tối đa xung đột và thời gian chết.

Phương pháp CSMA chỉ 'nghe trước khi nói', không có khả năng phát hiện xung đột trong quá trình truyền, dẫn đến lãng phí đường truyền.

### III.3.2. Phương pháp CSMA/CD

Phương pháp CSMA/CD có nguồn gốc từ hệ thống radio đã phát triển ở trường đại học Hawai vào khoảng năm 1970, gọi là ALOHANET, còn được gọi là phương pháp LWT ( Listen While Talk – Nghe trong khi nói). Các va chạm luôn xảy ra tại một cấp nào đó trên các mạng, với số lượng tham gia tăng theo tỉ lệ thuận khi các phiên truyền gia tăng.

Phương pháp CSMA/CD ngoài các chức năng của CSMA còn bổ xung các quy tắc sau:

- Khi đang truyền vẫn tiếp tục nghe đường dây.
- Nếu phát hiện có xung đột thì *ngừng truyền và tiếp tục gởi sóng mang* thêm một thời gian nữa để đảm bảo các trạm đều có thể nghe được sự kiện xung đột.
- Sau khi chờ đợi một thời gian ngẫu nhiên thì trạm thử truyền lại bằng cách sử dụng các phương pháp của CSMA.

Với phương pháp CSMA/CD, thời gian chiếm dụng vô ích đường truyền giảm xuống bằng thời gian dùng để phát hiện một đụng độ. CSMA/CD sử dụng ba giải thuật 'persistent' ở trên. Trong đó giải thuật '*l-persistent'* được sử dụng trong mạng Ethernet, Mitrenet và được chọn cả trong chuẩn IEEE.802. Ngoài ra mỗi chuẩn LAN còn có thêm các cơ chế bổ sung.

### III.3.3. Điều khiển truy nhập bus với thẻ bài

Các trạm trên bus tạo nên một vòng logic, được xác định vị trí theo một dãy thứ tự, trong đó trạm cuối sẽ tiếp liền ngay sau trạm đầu. Mỗi trạm được biết địa chỉ của các trạm kề sau và kề trước nó.

Thẻ bài dùng cấp phát quyền truy nhập, được lưu chuyển trong vòng logic. Khi trạm nhận được thẻ bài thì được trao quyền sử dụng phương tiện trong một thời gian xác định để truyền dữ liệu. Khi truyền xong hoặc hết thời hạn, trạm sẽ chuyển thẻ bài đến trạm kế tiếp trong vòng logic. Các trạm không sử dụng thẻ bài vẫn có mặt trên bus nhưng chúng chỉ có thể trả lời cho yêu cầu xác nhận (nếu chúng là đích của gói tin nào đó). Thứ tự vật lý của trạm trên bus là không quan trọng, độc lập với thứ tự logic.

***Các chức năng:***

- Khởi tạo vòng logic: khi thiết lập mạng hoặc khi vòng logíc bị gãy.

- Bổ sung trạm vào vòng logic (xem xét định kỳ) bằng cách mời nút đứng sau nhập vòng. Loại bỏ một trạm ra khỏi vòng logic bằng cách nối trạm trước và sau nó với nhau.
- Quản lý sai sót: trùng địa chỉ, gãy vòng (các trạm bị treo, rơi vào trạng thái chờ lẫn nhau) bởi nút giữ Token.
- Khi giữ thẻ mà không có trạm khác nhận được gói tin thì chứng tỏ nút khác đã có thẻ, lúc đó nó sẽ bỏ thẻ bằng cách chuyển sang trạng thái "nghe".
- Khi nút hoàn thành công việc, nó gởi thẻ đến nút đứng sau, nếu nút tiếp sau hoạt động thì nó gởi thể chuyển sang trạng thái bị động. Nếu ngược lại, nó gởi thẻ cho nút kế tiếp lần nữa. Nếu hai lần gởi không được thì xem như nút kế tiếp hỏng và gởi đi gói tin "tìm nút kế tiếp" để tìm nút tiếp theo.
- Nếu không thành công thì nút bị xem là có sự cố. Nút ngừng hoạt động và "nghe" trên bus.

 Định dạng khung bản tin mạng mạng Token bus

| Bắt đầu tin | Điều khiển gói tin | Địa chỉ nguồn | Địa chỉ đích | TIN | FSC | Kết thúc tin |
|---|---|---|---|---|---|---|
| 1 byte | 1 byte | 2-6 bytes | 2 - 6 bytes | | 4 bytes | 1 byte |
| | Khung tin cực đại 8191 bytes | | | Tốc độ có thể là 1; 5; 10Mbps | | |

 So sánh CSMA/CD và Token bus

- Token bus quản lý phức tạp hơn so với CSMA/CD. Trong trường hợp tải nhẹ thì không hiệu quả bằng CMSA/CD (do phải qua nhiều trạm).

- Tuy nhiên Token Bus có hiệu quả trong trường hợp tải nặng, dễ điều hòa lưu thông trên mạng Token bus. Không quy định độ dài tối thiểu của gói tin, không cần nghe trước khi nói.

### III.3.4. Điều khiển truy cập vòng với thẻ bài

Đây là giao thức thông dụng được dùng trong các LAN có cấu trúc vòng (Ring). Phương pháp này sử dụng một khối tín hiệu đặc biệt gọi là Token di chuyển vòng quanh mạng theo một chiều xác định. Một trạm muốn truyền phải đợi cho đến khi nhận được thẻ bài. Khi một trạm đang chiếm token thì nó có thể phát đi một gói dữ liệu. Khi đã phát hết gói dữ liệu cho phép hoặc không còn gì để phát nữa thì trạm đó chuyển sang khung thẻ bài đến cho trạm kế tiếp trên mạng. Trong Token có chứa một địa chỉ đích và được luân chuyển tới các trạm theo một trật tự đã định trước. Đối với cấu hình dạng xoay vòng thì trất tự của sư truyền Token tương đương với trật tự vật lý của các trạm xung quanh vòng.

Các chuẩn mạng sử dụng phương pháp điều khiển truy nhập thẻ bài:

- Chuẩn IEEE 802.5 còn gọi là chuẩn Token Ring.
- FDDI là chuẩn sợi quang 100Mpb sử dụng phương pháp chuyển thẻ bài và vòng tròn.

Phương pháp chuyển thẻ bài thích hợp trong các điều kiện như sau:

- Khi mạng đang tải dữ liệu quan trọng về thời gian do phương pháp này cung cấp khả năng bàn giao.
- Khi mạng được sử dụng nhiều, do tránh được xung đột.
- Khi một vài trạm có mức ưu tiên cao hơn so với các trạm khác. Phương pháp chuyển thẻ bài có thể áp dụng các mức ưu tiên cho trạm để ngăn cấm một trạm bất kỳ không được độc quyền về mạng.
- Do thẻ bài luân chuyển quanh mạng nên mỗi mạng có thể truyền theo quãng thời gian tối thiểu.

Phương pháp chuyển thẻ bài đòi hỏi cơ chế điều khiển phức tạp và chi phí đầu tư phần cứng cao, nhưng được thiết kế với độ tin cậy cao. Tuy vậy hiện nay Ethernet vẫn là chuẩn LAN thông dụng, chứng tỏ được ưu điểm của phương pháp tranh chấp khi sử dụng trên các mạng LAN.

Giao thức truyền Token có trật tự hơn nhưng cũng phức tạp hơn CSMA/CD, có ưu điểm là vẫn hoạt động tốt khi lưu lượng truyền thông lớn. Giao thức truyền Token tuân thủ đúng sự phân chia của môi trường mạng, hoạt động dựa vào việc xoay vòng bị đứt đoạn. Giao thức phải chứa thủ tục kiểm tra Token để cho phép khôi phục lại oken bị mất hoặc thay thế trạng thái của Token và cung cấp các phương tiện để sửa đổi logic (thêm vào, bớt đi hoặc định lại trật tựu của các trạm)

Khung tin cực đại 16KB ở chế độ truyền 16Mps và 4KB ở chế độ truyền 4Mps.

Dạng bản tin mạng Token Ring:

| Bắt đầu tin | Điều khiển thâm nhập | Điều khiển gói tin | Địa chỉ nguồn | Địa chỉ đích | TIN | FSC | Kết thúc gói tin | Trạng thái gói tin |
|---|---|---|---|---|---|---|---|---|
| 1 byte | 1 byte | 2-6 bytes | 2 - 6 bytes | 2 - 6 bytes | | 4 bytes | 1 byte | 1 byte |

**Phương pháp điều khiển truy nhập dò báo**

Dò báo (polling) là một phương pháp điều khiển truy cập sử dụng một thiết bị trung tâm điều khiển toàn bộ việc truy nhập mạng. Đây là phương pháp được sử dụng phổ dụng nhất trên các mạng máy tính lớn.

Thiết bị trung tâm có tên là thiết bị chính sẽ yêu cầu dữ liệu từ các thiết bị khác trên mạng có tên là thiết bị thứ cấp (secondary). Sau khi được dò báo thiết bị thứ cấp có thể truyền một dữ liệu được xác định bởi các giao thức dùng trên mạng. Một thiết bị thứ cấp không thể truyền trừ khi nó được thiết bị chính dò báo.

Phương pháp dò báo có nhiều ưu điểm của phương pháp chuyển thẻ bài như:

- Dự đoán được các lần truy cập định sẵn.
- Gán được các mức ưu tiên, tránh được va chạm.

So sánh phương pháp dò báo và phương pháp chuyển thẻ bài : kỹ thuật dò báo tập trung hóa quyền điều khiển. Nhìn dưới góc độ quản lý thì đây là một ưu điểm, nhưng nếu cơ chế điều khiển trung tâm bị hỏng, mạng sẽ ngừng hoạt động. Phương pháp chuyển thẻ bài sử dụng các chức năng điều khiển phân phối hơn do đó ít bị hỏng tập trung tại một điểm. Bên cạnh đó, phương pháp dò báo đôi khi lãng phí các lượng băng thông lớn do phải dò báo từng thiết bị thứ cấp, cho dù các thiết bị không có gì để truyền.

## III.4. Khái niệm mạng LAN

### III.4.1. Các cấu trúc của mạng LAN

Cấu trúc (topology) của mạng là cấu trúc hình học không gian, thực chất là cách bố trí phần tử của mạng cũng như cách thức nối giữa chúng với nhau. Thông thường có 3 dạng cấu trúc là: mạng dạng hình sao (Star topology), mạng dạng vòng (Ring topology) và mạng dạng tuyến (Bus topology). Ngoài ra còn có một số dạng biến thể khác như mạng dạng cây, mạng hỗn hợp, sao mở rộng,…

**1. Mạng dạng hình sao (Star topology)**

Mạng dạng hình sao bao gồm một trung tâm và các nút thông tin. Các nút thông tin là các trạm đầu cuối, các máy tính và các thiết bị khác của mạng. Trung tâm của mạng điều phối mọi hoạt động trong mạng với chức năng cơ bản là:

- Xác định cặp địa chỉ gửi và nhận được phép chiếm tuyến thông tin và liên lạc với nhau.
- Cho phép theo dõi và xử lý sai trong quá trình trao đổi thông tin.
- Thông báo các trạng thái của mạng.

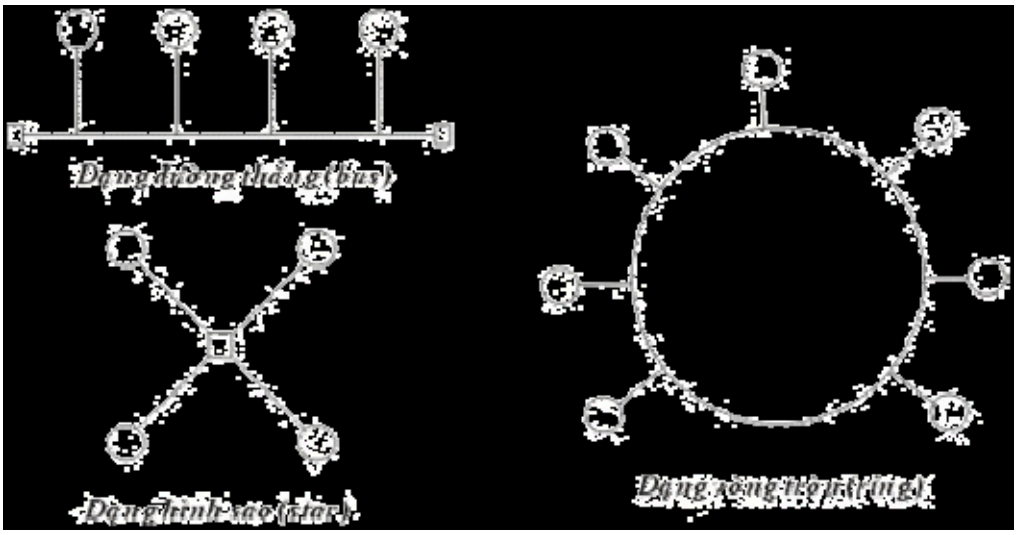
Ưu điểm:

- Hoạt động theo nguyên lý nối song song nên nếu có một thiết bị nào đó ở một nút thông tin bị hỏng thì mạng vẫn hoạt động bình thường.
- Cấu trúc mạng đơn giản và các thuật toán điều khiển ổn định.
- Mạng có thể mở rộng hoặc thu hẹp tùy theo yêu cầu người sử dụng.

Nhược điểm:

- Khả năng mở rộng mạng phụ thuộc hoàn toàn vào khả năng của trung tâm. Khi trung tâm có sự cố thì mạng ngừng hoạt động.
- Mạng yêu cầu kết nối độc lập riêng lẻ từng thiết bị ở các nút thông tin đến trung tâm. Khoảng cách từ máy đến trung tâm hạn chế (thường 100 m).

Thông thường, mạng hình sao cho phép nối các máy tính vào một bộ tập trung (HUB) bằng cắp xoắn, giải pháp này cho phép nối trực tiếp nhiều máy tính với HUB không cần qua trục BUS, tránh được các yếu tố gây nghẽn mạng. Cùng với sự phát triển của Switch, mà hình này ngày càng trở nên phổ biến.



Hình III-9. Một số cấu trúc chính của mạng LAN

## 2. Mạng dạng tuyến (Bus topology)

Trong mạng hình bus, các máy tính và nút mạng sẽ đều được nối về với nhau trên một trục đường dây cáp chính để chuyển tải tín hiệu.Tất cả các nút đều sử dụng chung đường dây cáp chính này. Phía hai đầu dây cáp được bịt bởi một thiết bị gọi là terminator. Các tín hiệu và dữ liệu khi di chuyển lên và xuống trong dây cáp đều mang theo địa chỉ nơi đến.

Loại mạng này dùng ít dây cáp nhất, dễ lắp đặt. Tuy vậy cũng có những bất lợi khi sẽ có sự ùn tắc khi dữ liệu di chuyển với lưu lượng lớn và khi có sự hỉng hóc ở đoạn nào đó thì rất khó phát hiện. Hư hỏng trên đường dây chính sẽ ngừng toàn bộ hệ thống.

## 3. Mạng dạng vòng (Ring topology)

Mạng được bố trí theo dạng vòng tròn, đường dây cáp được thiết kế làm thành một vòng khép kín, tín hiệu chạy quanh theo một chiều nào đó. Các nút

truyền tín hiệu cho nhau mỗi thời điểm chỉ được một nút mà thôi. Dữ liệu truyền đi phải kèm theo địa chỉ cụ thể của trạm tiếp nhận.

Mạng Token Ring có thể chạy ở tốc độ 4Mbps hoặc 16 Mbps. Phương pháp truy cập dùng trong mạng Token Ring gọi là Toking passing.Token passing là phương pháp truy cập xác định, trong đó các xung đột được ngăn ngừa bằng cách ở mỗi thời điểm chỉ có một trạm có thể truyền dữ liệu. Điều này được thực hiện bằng việc truyền một tín hiệu đặc biệt gọi là Token xoay vòng từ trạm này qua trạm khác. Mỗi trạm chỉ có thể gửi dữ liệu khi nó nhận được Token.

Mạng dạng vòng có thuận lợi là có thể nới rộng ra xa, tổng đường dây cần thiết ít hơn so với hai kiểu trên. Nhược điểm điểm là đường dây phải khép kín, nếu bị ngắt ở một nơi nào đó thì toàn bộ hệ thống cũng bị ngừng.

### III.4.2. Các chuẩn mạng LAN

Các chuẩn LAN là các tiêu chuẩn công nghệ cho LAN được phê chuẩn bởi các tổ chức chuẩn hóa quốc tế, nhằm hướng dẫn các nhà sản xuất thiết bị mạng đi đến sự thống nhất chung khả năng sử dụng chung các sản phẩm của họ, vì lợi ích của người sử dụng và tạo điều kiện thuận lợi cho các nghiên cứu phát triển.

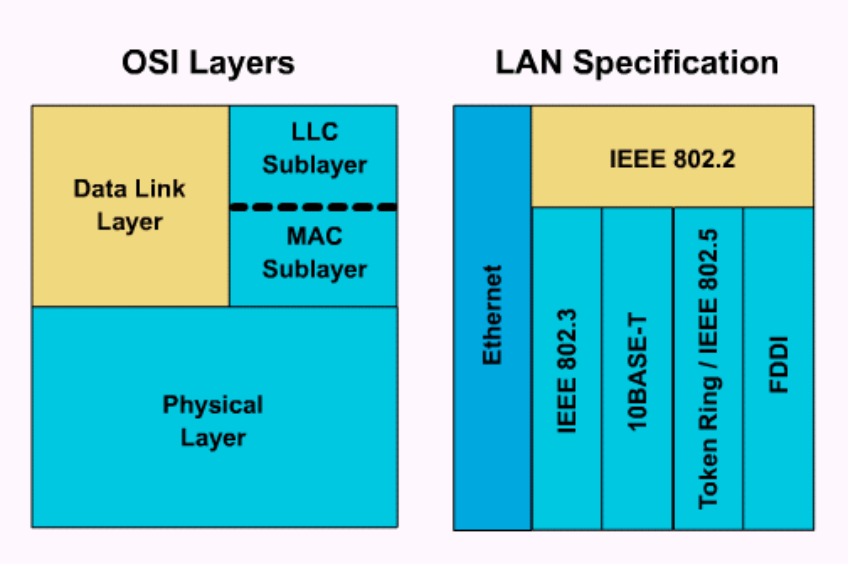
Các chuẩn quy định môi trường truyền dẫn cũng như cách thức sử dụng chúng trong kết nối LAN: các giao thức truyền thông ở các tầng vật lý và tầng liên kết dữ liệu của mạng theo mô hình OSI.

Các giao thức truyền thông ở các tầng trên mô hình OSI hiện tại được xác định qua một số giao thức phổ biến như TCP/IP, IPX/SPX, NetBIOS…

Ủy ban IEEE phát triển tiêu chuẩn IEEE LAN và đề xuất phân chia hai tầng thấp nhất của mô hình OSI như dưới đây:

Theo chuẩn 802 thì tầng LKDL được chia thành hai tần:

- Tầng con điều chỉnh logic LLC(Logical Link Control Sub-layer) : giữ vai trò tổ chức dữ liệu, tổ chức thông tin để truyền và nhận. Thủ tục tầng LLC không bị ảnh hưởng khi sử dụng các đường truyền dẫn khác nhau, nhờ vậy mà linh hoạt hơn trong khai thác.
- Tầng con điều khiển xâm nhập mạng MAC (Media Access Control Sub-layer), làm nhiệm vụ điều khiển truy cập mạng.




Hình III-10. Các tầng LLC và MAC.

Chuẩn 802.2 ở mức con LLC tương đương với chuẩn HDLC của ISO hoặc X.25 của CCITT.

Chuẩn 802.3 xác định phương pháp truy cập mạng tức thời có khả năng phát hiện lỗi chồng chéo thông tin CSMA/CD. Phương pháp CSMA/CD được đưa ra từ năm 1993 nhằm mục đích nâng cao hiệu quả mạng. Theo chuẩn này các mức được ghép nối với nhau thông qua các bộ ghép nối.

Chuẩn IEEE 802.3 dùng cho mạng Ethernet ( sử dụng giao thức truy nhập CSMA/CD) bao gồm cả hai phiên bản băng tần cơ bản và băng tần mở rộng.

Chuẩn IEEE 802.4 liên quan đến sự sắp xếp tuyến token, thực chất là phương pháp truy cập mạng theo kiểu phát tín hiệu thăm dò token qua các trạm và đường truyền bus.

Chuẩn IEEE 802.5 dùng cho mạng dạng vòng và trên cơ sở dùng tín hiệu thăm dò token. Mỗi trạm khi nhận được tín hiệu thăm dò token thì tiếp nhận token và bắt đầu quá trình truyền thông tin dưới dạng các frame. Các frame có cấu trúc tương tự như của chuẩn 802.4. Phương pháp truy cập mạng này quy định nhiều mức ưu tiên khác nhau cho toàn mạng và cho mỗi trạm, việc quy định này vừa do người thiết kế vừa do người sử dụng quy định.

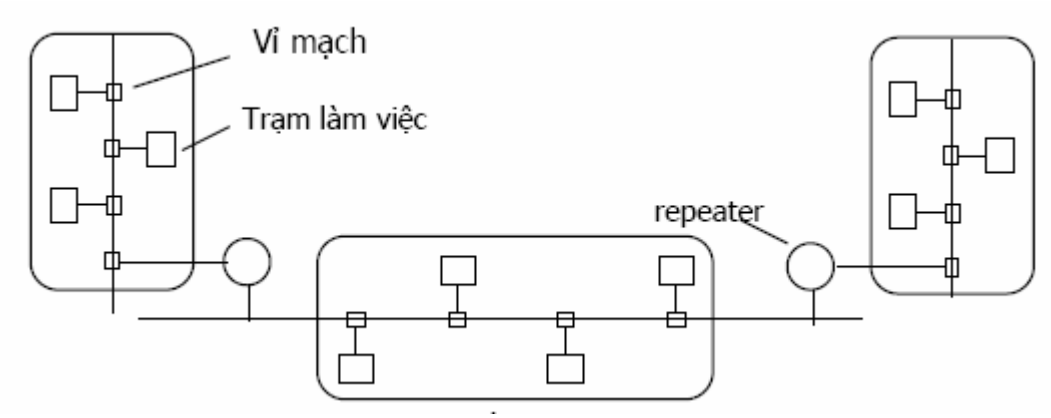
Chuẩn IEEE 802.11 dùng cho mạng không dây (Wireless)

## 1. Chuẩn Ethernet

Đây là kỹ thuật mạng cục bộ thành công nhất những năm gần đây và sử dụng công nghệ CSMA/CD(Carrier Sence, Multiple Access With Collision Detect)

Ethernet là một mạng đa truy xuất, các nút gửi và nhận khung qua một liên kết chia sẻ.Digital Equipment Corporation và Intel Corporation kết hợp với Xerox định nghĩa  chuẩn Ethernet vào năm 1978. Chuẩn này sau đó được xây dựng thành

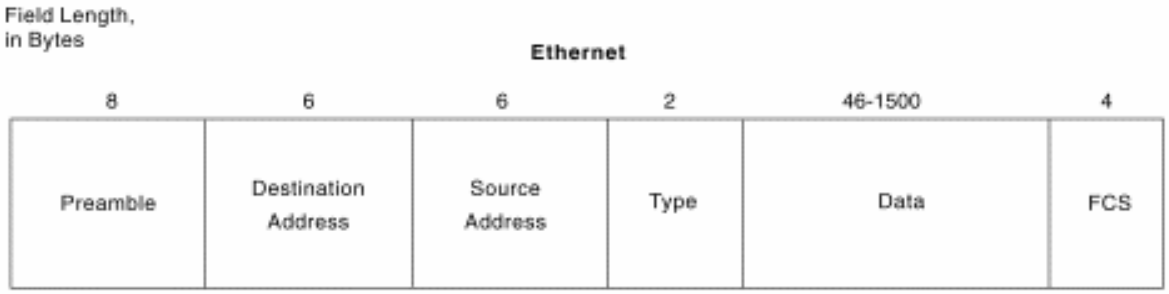
chuẩn 802.3 IEEE(chuẩn năm 1978 là con của chuẩn này). 802.3 xây dựng thêm nhiều chức năng mới. Gần đây, nó đã có phiên bản 100 Mbps được gọi là Fast Ethernet và 1000 Mbps gọi là Giagabit Ethernet.




Hình III-11. Cấu trúc Ethernet dạng bus.

Thuật toán kiểm soát truy xuất đường truyền chia sẻ trong Ethernet gọi là Ethernet's Media Accsess Control. Nó đặc thù được thi hành trên phần cứng của card mạng.

**Định dạng khung cơ bản:**




Hình III-12. Định dạng khung Ethernet

- 64 bit Preamble (một chuỗi thay đổi giữa 0 và 1) cho phép máy nhận đồng bộ tín hiệu với máy gửi.
- Cả máy nguồn và máy đích đều có 48 bit địa chỉ.
- Trường Type chứa khoá để thực hiện phân kênh(ở các giao thức mức cao).
- Mỗi khung chứa tối đa 1500 byte và tối thiểu 46 byte dữ liệu (nếu thiếu các host phải đệm dữ liệu thêm vào trước khi truyền, lý do là khung phải đủ lớn để giúp phát hiện xung đột).
- FCS-Frame Check Sequence**:** Sử dụng 32 bit CRC kiểm tra lỗi.
- Các khung trong Ethernet truyền theo kiểu Bit-Oriented.

- Ethernet có 14 byte header.
- Card mạng tại các máy gửi sẽ gắn Preamble, CRC trước khi truyền và ngược lại, nó sẽ được loại bỏ tại card mạng của máy nhận.

**Thuật toán truyền**

Ý tưởng:

Lúc một card giao tiếp mạng có một khung để gởi và liên kết rãnh, nó truyền khung ngay lập tức, không có sự điều đình với các card giao tiếp mạng khác. Giới hạn kích thước 1500 byte có nghĩa rằng card giao tiếp mạng chỉ có thể chiếm giữ đường dây trong một khoảng thời gian cố định.

Lúc một card giao tiếp mạng có một khung để gởi và liên kết bận, nó đợi cho tới khi đường dây rãnh và truyền ngay lập tức khi liên kết trở nên rảnh. Chúng được gọi là giao thức 1-persistent vì một card giao tiếp mạng với 1 khung để gửi sẽ truyền với xác suất 1 bất kỳ lúc nào đường dây trở nên rãnh.

Tổng quát, thuật toán truyền p-persistent với xác suất 0 <= p <=1 sau khi đường dây rãnh và khả năng trì hoãn với xác suất q = 1-p, lý do chọn p < 1 là do có thể nhiều adapter đợi đường dây rãnh và chúng ta không muốn tất cả chúng cùng truyền một lúc. Nếu một adaptor truyền ngay với một xác suất 33%(giả sử) tức là 3 adapter đợi để truyền. Mặc dù với lý do trên, trong thực tế một adapter luôn truyền ngay lập tức sau khi liên kết rãnh và thật sự rất hiệu quả khi thực hiện cách này.

Nếu cả hai cùng truyền một lúc thì gọi là hiện tượng xung đột. Vì Ethernet hổ trợ phát hiện xung đột, nên mỗi máy gửi đều có thể phát hiện xung đột trong quá trình truyền của mình, khi phát hiện xung đột nó đầu tiên truyền 32 bit jamming tuần tự và dừng việc truyền. Thật sự nó là 64 bit, 32 bit premble + 32 bit jamming

## 2. Token Ring

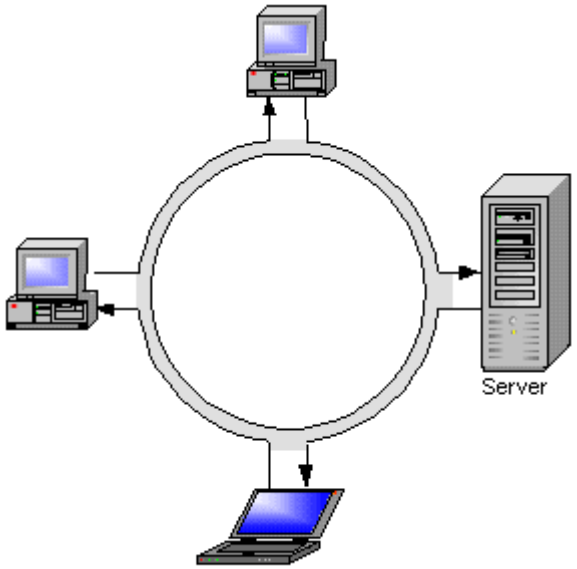
Cùng với Ethernet, Token Ring là một lớp quan trọng khác của mạng chia xẻ liên kết. Tuy nhiên, có nhiều vấn đề khó khăn trong Token Ring hơn là trong Ethernet.

Trước đây Token Ring định nghĩa bởi chuẩn IBM's Token Ring. Gần đây 802.5 là chuẩn định nghĩa bởi IEEE. Nhưng hầu hết các nguyên tắc tổng quát của Token Ring đều tương tự nhau giữa IBM và 802.5. Tuy nhiên chuẩn FDDI (Fiber Distributed Data Interface) là chuẩn mới nhất và nhanh nhất hiện nay.

Mạng Token Ring bao gồm một tập các nút nối trong một vòng. Dữ liệu luôn truyền theo hướng xác định vòng quanh vòng, mỗi nút nhận khung từ hàng xóm trên của nó và gửi chúng xuống hàng xóm bên dưới nó. Sơ đồ nối kết của Ring hoàn toàn trái ngược với sơ đồ nối kết Ethernet. Các nút tham gia nối kết trong mạng Token Ring chia sẽ chung một đường truyền vật lý.

Token Ring chia sẽ hai đặc trưng của Ethernet:

- Yêu cầu một thuật toán phân phối để điều khiển lúc một nút được phép truyền.
- Tất cả các nút trên vòng đều nhìn thấy các khung, mỗi nút xem xét địa chỉ trong header của khung và lưu lại một bảng sao của các khung khi các khung này đi qua nó.




Hình III-13.Mạng Token Ring

"Token" dùng để chỉ phương pháp truy xuất chia sẻ đường truyền. Nó thật sự chỉ là một chuỗi các bit đặc biệt, đi vòng quanh vòng. Mỗi nút trên vòng nhận và chuyển token. Khi một nút có dữ liệu cần truyền nhìn thấy token, nó chộp lấy token và chèn một khung vào trong vòng. Các nút còn lại trên vòng đơn giản chỉ chuyển khung này. Trước khi truyền dữ liệu các nút sẽ lưu trữ một bảng sao của khung sẽ truyền và sau đó sẽ chuyển khung này đến nút kế tiếp trong vòng. Lúc khung quay lại máy gửi, nút này nhận lại khung đó và trả lại token cho vòng.

**Giao thức điều khiển truy xuất đường truyền(MAC protocol)**

Card mạng cho một nút trong Token Ring chứa một receiver, một tranceiver, buffer.

Khi không có trạm nào truyền dữ liệu token đi vòng quanh vòng. Do đó, mỗi nút trên vòng phải có khả năng lưu trữ toàn bộ Token. Ví dụ token của 802.5 là 24 bit chiều dài.

Khi một token đi vòng quanh vòng, bất kỳ trạm nào có dữ liệu đều có thể chộp lấy token, giữ nó lại và bắt đầu gởi dữ liệu. Trong mạng 802.5, sự chộp lấy bằng cách chỉ thay đổi một bit trong byte thứ hai của token, 2 byte đầu tiên của

token được thay đổi bây giờ trở thành gói mang "lời chào hỏi". Khi một trạm có token nó có thể thực hiện gởi một hay nhiều gói.

Mỗi gói được truyền chứa địa chỉ của máy nhận. Mỗi nút cũng có thể truyền gói theo multicast hay broadcast. Khi mỗi gói đi qua mỗi nút, mỗi nút xem xét địa chỉ bên trong gói. Nếu là gói truyền đến nó, trạm này sẽ chép một bản sao vào trong buffer của nó khi gói đi qua card mạng, nhưng không di chuyển gói này ra khỏi vòng. Máy gửi có nhiệm vụ di chuyển gói ra khỏi vòng.

Một vấn đề cần giải quyết là bao nhiêu dữ liệu mà một nút được cho phép truyền mỗi lần nó có token, thời gian này được gọi là THT(token holding time). Nếu chúng ta cho rằng hầu hết các nút không có dữ liệu thì không hợp lý. THT được đặt cố định, nhưng thật vô lý trong trường hợp một nút bị giới hạn gửi chỉ một thông điệp và bắt buột phải đợi cho tới khi token đi quanh một vòng trước khi có cơ hội truyền tiếp.

Cách dễ dàng là một nút có thể gửi nhiều byte mỗi lần lúc nó token, điều này rất tốt khi nhận biết được trên vòng chỉ có một nút cần gửi dữ liệu, nhưng khả năng này không làm việc tốt lúc nhiều nút có dữ liệu gửi. Trong mạng 802.5 THT quy định là 10ms. Do đó các nút phải khéo léo khi sử dụng THT, trước khi đặt mỗi gói vào trong vòng, mỗi trạm phải kiểm tra khoảng thời gian dùng để truyền gói sẽ không vượt quá THT.

802.5 cung cấp một các thức thức truyền tin cậy, sử dụng 2 bit cuối gói, bit A và C được khởi tạo là 0. Lúc một trạm thấy một khung mà nó muốn nhận nó set bit A trong khung. Khi nó chép khung vào trong adaptor, nó set bit C, nếu máy gửi nhìn thấy khung quay trở lại với bit A vẫn là 0 thì nó sẽ biết không có máy nhận. Nếu bit A được đặt nhưng bit C thì không lý do là máy nhận không chấp nhận khung

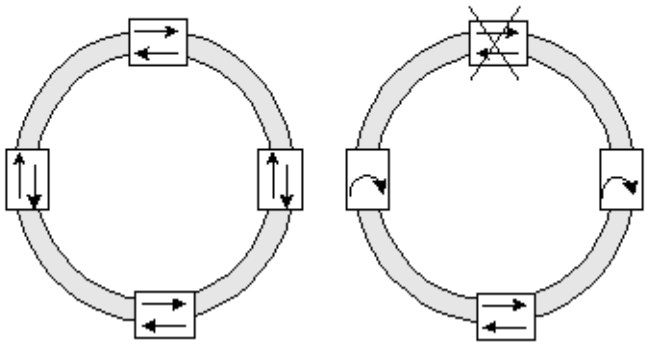
## 3. FDDI

FDDI (Fiber Distributed Data Interface) thì tương tự IBM và 802.5, tuy nhiên nó có một số điểm khác nhau bởi vì nó chạy trên cáp quang và nó thực hiện một số cách tân.

**Đặc điểm vật lý**

Nó bao gồm một vòng đôi, hai vòng truyền dữ liệu theo hai hướng ngược nhau, vòng thứ hai sẽ không được sử dụng nhưng nó sẽ trở nên hoạt động nếu vòng sơ cấp bị hỏng. Mạng FDDI vẫn hoạt động khi một đường cáp hay một trạm bị hỏng.

Bởi vì sự phí tổn của cấu hình vòng đôi. FDDI cho phép nút gắn vào mạng chỉ bởi một cáp đơn. Nó được gọi single attachment stations(SAS), kết nối đôi được gọi là Dual Attachment Stations.



Hình III-14. Mô hình mạng FDDI

Một thiết bị tập trung được sử dụng để gắn SAS vào vòng(sử dụng hai đường cáp đơn).

FDDI là một mạng 100 Mbps.

Giới hạn chuẩn 500 station.

Giới hạn chuẩn khoảng các là 2km giữa bất kỳ 2 trạm nào.

Toàn bộ mạng giới hạn 200 km của cáp quang, do vòng đôi nên nó tổng cộng chiếu dài chỉ là 100km.

Nó có thể chạy qua các môi trường vật lý khác nhau như cáp đồng trục hay cáp xoắn đôi.

FDDI sử dụng mã hoá 4B/5B.

**Thuật toán Time-Token**

THT của mỗi nút được xác định trước và gán ở một giá trị cố định. Thêm vào đó, để đảm bảo mỗi nút có cơ hội truyền trong một khoảng thời gian nào đó, ta đặt giới hạn trên của TRT(token ratation time) cho tất cả nút, gọi là target TRT và tất cả các nút đều chấp nhận thời gian TTRT này. Mỗi nút đo thời gian bởi sự di chuyển thành công của token. Ta goị là "Measured TRT".

If mesured-TRT > TTRT: token đến trễ và nút không truyền dữ liệu.

If mesured-TRT < TTRT: token đến sớm và nút được cho phép giữ token để truyền.

Có hai lớp truyền: đồng bộ và không đồng bộ. Lúc một nút có token nó được phép gởi dữ liệu đồng bộ, không cần quan tâm token đến sớm hay trễ (gởi âm thanh hay video). Ngược lại nó chỉ có thể gửi khi token đến sớm (các ứng dụng file). Nó sử dụng một bit để phân biệt đồng bộ và không đồng bộ.

## III.5. Địa chỉ vật lý (MAC address)

Mỗi host trên một Ethernet chỉ có một địa chỉ duy nhất có chiều dài 48 bit. Địa chỉ này được lưu trữ trên card mạng và có thể đọc tuần tự 6 số phân cách nhau bởi dấu ":"Để đảm bảo mỗi host có một địa chỉ duy nhất mỗi nhà sản xuất thiết bị Ethernet bị bắt buộc gán một mã trên các card mạng mà họ sản xuất.

Mỗi khung truyền trên Ethernet được nhận bởi tất cả các adapter nối đến Ethernet đó (kiểm tra địa chỉ để nhận hay không nhận).

Ngoài địa chỉ unicast, một địa chỉ bao gồm tất cả các bit 1 được xem là địa chỉ broadcast. Địa chỉ có bit đầu tiên là 1 nhưng không phải là broadcast thì được xem là multicast (một host có thể được lập trình trên adapter đó để có thể chấp nhận một vài địa chỉ multicast).

Tóm lại, một card giao tiếp mạng nhận tất cả khung và chỉ chấp nhận khung khi trên header của khung đó chứa địa chỉ của nó, địa chỉ multicast, địa chỉ broadcast, hay một khung vô tình.

## III.6. Một số công nghệ tầng liên kết dữ liệu khác

### III.6.1. Mạng không dây(Wireless Network)

Mạng không dây là một kỹ thuật gần đây phát triển mạnh. Các máy tính bên trong một toà nhà có thể sử dụng tia hồng ngoại để liên lạc với nhau hay người ta còn sử dụng sóng viba để xây dựng một mạng rộng lớn từ một lưới điều khiển của một số vệ tinh quỹ đạo thấp. 802.11 được thiết kế để sử dụng trong một khu vực địa lí giới hạn.

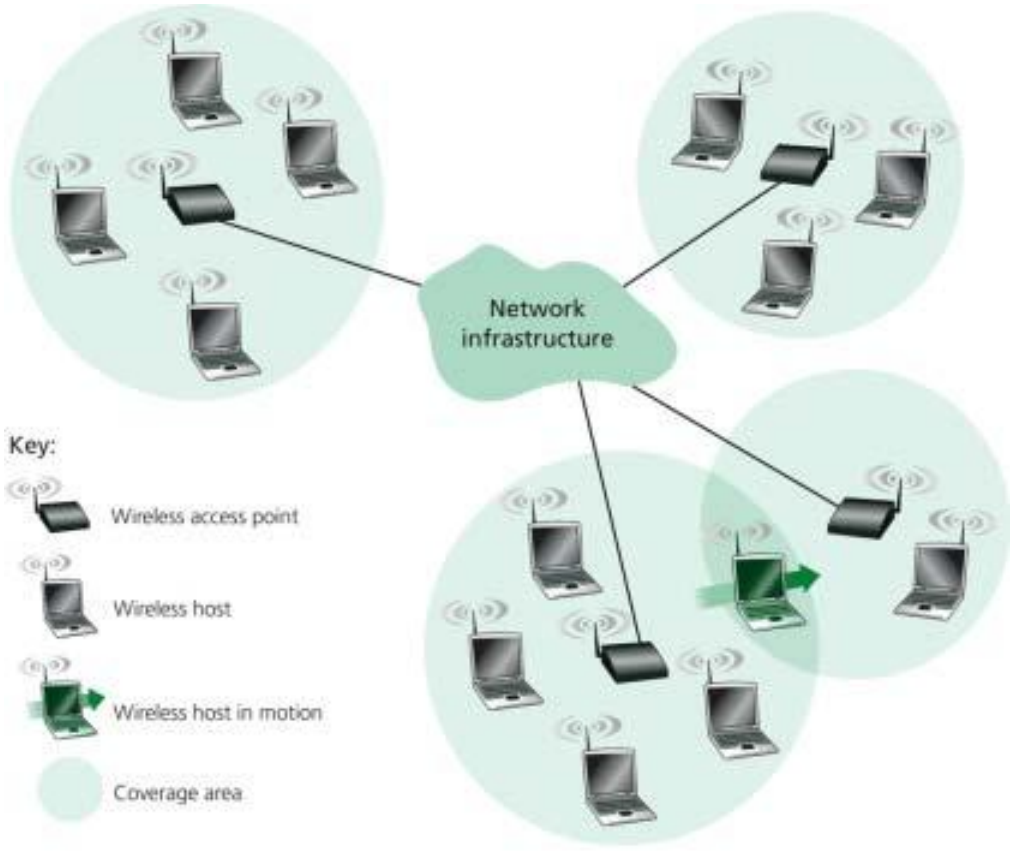
802.11 sử dụng 3 dạng đường truyền vật lý khác nhau:

- Sử dụng sóng vô tuyến
- Sử dụng sóng viba
- Sử dụng tia hồng ngoại.

Sóng vô tuyến được lan truyền qua một tần số rộng hơn bình thường, nhằm giảm tối thiểu tác động ảnh hưởng từ các thiết bị khác. **Frequency hopping** là một kỹ thuật sóng vô tuyến thực hiện truyền tín hiệu qua một dãy các tần số ngẫu nhiên, đầu tiên nó truyền ở tần số 1, rồi 2, rồi 3, nhưng dãy các tần số này thì không thật sự ngẫu nhiên, nó dùng thuật toán tạo ra số ngẫu nhiên giả. Các máy nhận sử dụng cùng thuật toán như là máy gửi và vì vậy hai máy có thể đồng bộ và truyền dữ liệu với nhau.

**Lan truyền trực tiếp (direct sequence):** mỗi bit trong khung truyền được thể hiện bởi nhiều bit trong tín hiệu truyền. Với mỗi bit muốn truyền máy gửi thực hiện phép XOR chuỗi bit đó với một chuỗi bit ngẫu nhiên.

Kỹ thuật truyền tia hồng ngoại truyền dựa trên sự khuyếch tán. Và thường nằm trong cự ly khoảng 10m và giới hạn bên trong một toà nhà.




Hình III-15. Ví dụ mạng không dây

**Quản lý xung đột**

Cách thức truyền của mạng không dây tương tự cách thức truyền của Ethernet. Một nút sẽ đợi cho đến khi liên kết rãnh trước khi truyền và nếu hai nút cùng truyền một lúc xung đột sẽ xuất hiện. Vấn đề xung đột trong mạng không dây phức tạp bởi vì không phải tất cả các nút luôn luôn ở trong phạm vi truyền của các nút khác.

**Thuật toán Multiple Access with Collision Avoidance (MACA)**

Máy gửi và máy nhận trao đổi các khung điều khiển với nhau trước khi máy gửi thực hiện truyền dữ liệu. Máy gửi truyền một khung Request to Send (RTS) đến máy nhận, khung RTS bao gồm một trường chỉ ra thời gian nó muốn chiếm giữ đường truyền (chiều dài của khung được truyền). Máy nhận đáp lại với khung Clear to Send(CTS), khung này đáp lại trường chiều dài của máy gửi, bất kỳ nút mà nó nhận thấy khung CTS thì nó biết nó không thể liên lạc với máy nhận, vì vậy nó không thể truyền trong khoảng thời gian này. Bất kỳ nút mà nó nhìn thấy khung, nhưng không thấy khung CTS thì nó có thể tự do liên lạc với máy nhận.

Hai vấn đề quan trọng trong mạng không dây

- Máy nhận gởi một ACK đến máy gửi thông báo thành công sau khi nhận khung, tất cả các nút phải đợi ACK trước khi truyền tiếp.
- Có hai hay nhiều nút nhận thấy liên kết trống và vì vậy sẽ truyền khung ở cùng một lúc, do đó các khung sẽ xung đột với nhau, 802.11 không hỗ trợ phát hiện xung đột nhưng nó sẽ phát hiện xung đột khi nó không nhận được khung CTS sau một khoảng thời gian nào đó. Trong trường hợp này chúng sẽ đợi một khoảng thời gian ngẫu nhiên trước khi truyền lại nó.

**Hệ thống phân phối (Distribution System)**

802.11 là một hệ thống phù hợp cho một mạng có cấu hình các nút đặc biệt, một nút trong mạng có thể bị giới hạn thông tin với một hay tất cả các nút khác trên mạng. Hơn nữa sự thuận lợi của mạng không dây là các nút tự do di chuyển, chúng không bị ràng buộc bởi dây dẫn, một tập các nút có thể thay đổi bất kỳ thời gian nào.

Các nút trong mạng không dây bên cạnh việc trao đổi thông tin tự do với các máy khác trong cùng một cấu trúc nó còn có thể trao đổi với các máy khác thông qua một thiết bị khác gọi là AP(Access Point). Thiết bị này sử dụng cáp để nối trực tiếp với một thiết bị gọi là distribution system. Các nút trong mạng có thể tự chọn riêng cho mình một AP.

Kỹ thuật chọn 1 AP được gọi là scanning thực hiện qua 4 bước:

- Gởi một khung thăm dò.
- Tất cả các AP trong phạm vi của máy gửi đáp lại với một khung trả lời khung thăm dò.
- Nút chọn một AP và gởi một khung giao thiệp.
- AP đáp lại với một khung trả lời giao thiệp.
- Các nút thực hiện cách này bất cứ lúc nào nó tham gia mạng, cũng như nó cảm thấy không cảm thấy "hạnh phúc" với AP hiện tại.
- AP có thể gởi một khung thông báo khả năng truy xuất của mình (tỉ lệ truyền hổ trợ bởi AP).

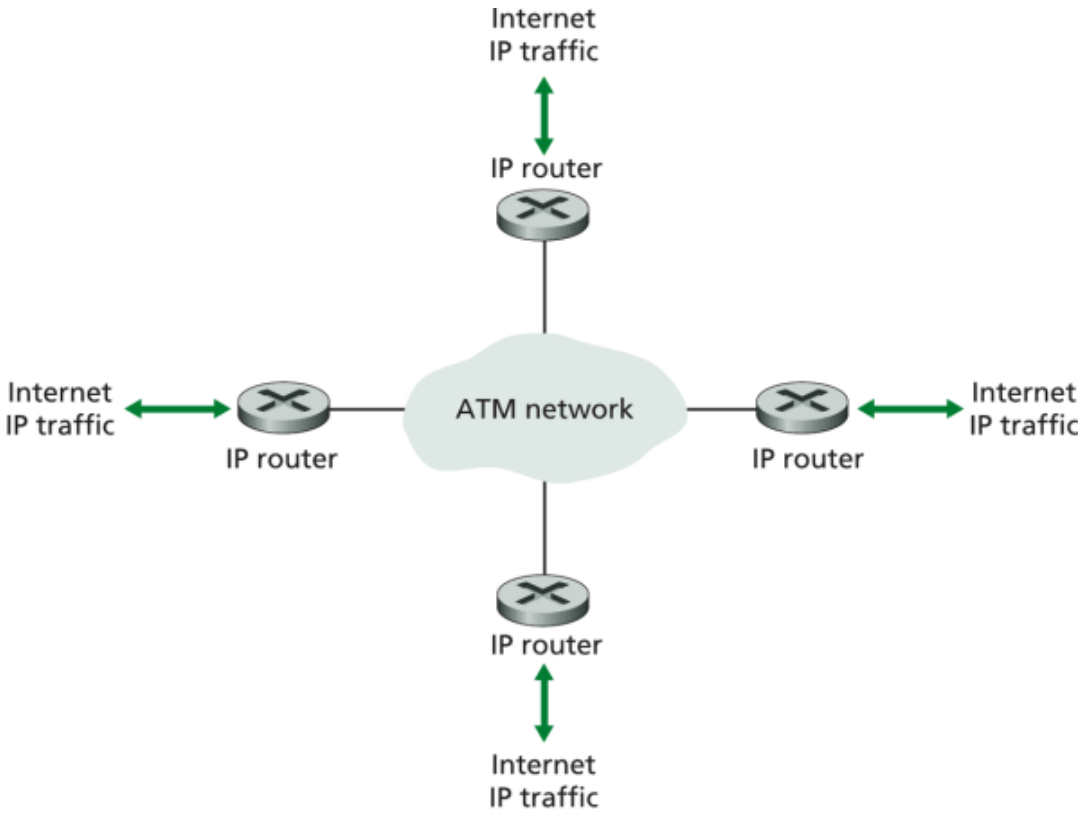
### III.6.2. ATM

Một công nghệ được quan tâm gần đây là ATM (Asychronous Tranfer Model). ATM là một công nghệ quan trọng trong những năm 1980 và đầu những năm 1990. ATM là tiếp cận theo dạng connection-oriented. Trong ATM giai đoạn thiết lập nối kết được gọi là signalling. Giao thức chính của ATM signalling là Q.2931. Ngoài khả năng tìm ra một đường đi xác định qua một mạng ATM, Q.2931 còn có nhiệm vụ cấp phát tài nguyên tại các chuyển mạch dọc kênh. Nó

đảm bảo một chất lượng phục vụ của kênh. Thật vậy, khả năng QoS cuả ATM là một trong nhữnh khả năng mạnh mẽ nhất.

Lúc một kênh ảo được thiết lập, nó cần thiết đặt địa chỉ nguồn trong thông điệp signalling. Trong ATM, địa chỉ có thể có ở một vài dạng, nhưng dạng chung nhất được sử dụng là E.164 và NSAP (Network Service Access Point), nó khác địa chỉ MAC sử dụng trong LAN.

Một điều mà làm ATM thật sự khác thường là các gói trong một mạng ATM có chiều dài cố định. Chiều dài của chúng là 53 byte bao gồm 5 byte header và 48 byte trọng tải, để phân biệt giữa các gói có chiều dài thay đổi và cố định người ta đưa ra một tên đặc biệt goị là tế bào (cell). ATM là một ví dụ chuẩn của mạng tế bào.




Hình III-16. Mạng ATM

**Cell**

Tất cả các công nghệ mạng mà chúng ta đã xem xét trước đây đều sử dụng các gói có chiều dài thay đổi. Gói có chiều dài thay đổi thì trói buột bên trong một vài giới hạn:

- Giới hạn thấp nhất: số lượng thông tin nhỏ nhất mà một gói có thể chứa mà một header không được tuỳ ý mở rộng.

- Giới hạn cao nhất: được đặt bởi nhiều yếu tố, ví dụ kích thước gói lớn nhất trong mạng FDDI xác định bao lâu mỗi trạm cho phép truyền mà không trả lại token và thật vậy nó xác định bao lâu mỗi trạm phải đợi cho token đến.

Cell, ngược lại giới hạn trên và dưới là cố định.

**Kích thước cell**

Gói có chiều dài thay đổi có một vài đặc trưng quan trọng:

- Nếu ta chỉ có một byte gửi, ta đặt nó trong gói có kích thước nhỏ nhất.
- Nếu chúng ta có một file lớn để gửi ta phân nó ra thành nhiều gói có kích thước lớn nhất để gửi.

Ta không cần thêm bất cứ thông tin gì trong trường hợp đầu, trong trường hợp thứ hai nó gia tăng hiệu quả băng truyền. Chúng ta cũng có thể giảm tối thiểu tổng số gói gửi bằng cách giảm tổng cộng hoạt động xử lý trên gói, điều này rất quan trọng trong một mạng có thông lượng cao bởi vì nhiều thiết bị mạng không giới hạn bao nhiêu bit trên 1 giây mà chúng có thể xử lý hơn là giới hạn số gói trên một giây mà chúng có thể xử lý.

Vậy tại sao phải sử dụng cell. Một lý do chính là nó thuận tiện được thi hành của phần cứng mạng. Bởi vì trong mạng điện thoại mỗi mạng điện thoại thường phục vụ 10.000 khách hàng, chiều dài cố định thì rất hữu ích nếu chúng ta muốn xây dựng các mạng nhanh, có tính khả mở. Có hai lý do:

- Xây dựng phần cứng là một nhiệm vụ dễ dàng, và nhiệm vụ xử lý mỗi gói thì dễ dàng khi biết chiều dài thật sự của chúng.
- Nếu tất cả các gói có cùng chiều dài, ta có thể có nhiều chuyển mạch. Tất cả chúng cùng làm một nhiệm vụ(xử lý song song).

Một đặc điểm quan trọng của truyền tế bào liên quan đến tổ chức hàng đợi. Khi ta lấy một gói từ hàng đợi và bắt đầu truyền nó, ta tiếp tục thực hiện thao tác này cho đến khi toàn bộ gói được truyền. Ví dụ, một mạng với một gói thay đổi, kích thước gói lớn nhất là 4KB và tốc độ truyền là 100Mbps, thời gian để truyền gói có kích thước lớn nhất là 327.69 micro giây, thật vậy một gói ưu tiên cao đến chỉ sau khi gói có kích thước lớn nhất được truyền sẽ ngồi đợi 327.68 micro giây để truy xuất liên kết, ngược lại nếu chuyển một cell 53 byte thời gian lâu nhất nó đợi là 4.24s điều này dường như không đáng kể nhưng nó dẫn đến tình trạng "bồn chồn" cho một số ứng dụng.

### III.6.3. X25

Được CCITT công bố lần đầu tiên vào 1970 lúc lĩnh vực viễn thông lần đầu tiên tham gia vào thế giới truyền dữ liệu với các đặc tính:

- X25 cung cấp quy trình kiểm soát luồng giữa các đầu cuối đem lại chất lương đường truyền cao cho dù chất lương đương dây truyền không cao.
- X25 được thiết kế cho cả truyền thông chuyển mạch lẫn truyền thông kiểu điểm nối điểm.
- Được quan tâm và tham gia nhanh chóng trên toàn cầu.

Trong X25 có chức năng dồn kênh (multiplexing) đối với liên kết logic (virtual circuits) chỉ làm nhiệm vụ kiểm soát lỗi cho các frame đi qua. Điều này làm tăng độ phức tạp trong việc phối hợp các thủ tục giữa hai tầng kề nhau, dẫn đến thông lượng bị hạn chế do tổng phí xử lý mỗi gói tin tăng lên. X25 kiểm tra lỗi tại mỗi nút trước khi truyền tiếp, điều này làm cho đường truyền có chất lượng rất cao gần như phi lỗi. Tuy nhiên do vậy khối lượng tích toán tại mỗi nút khá lớn, đối với những đường truyền của những năm 1970 thì điều đó là cần thiết nhưng hiện nay khi kỹ thuật truyền dẫn đã đạt được những tiến bộ rất cao thì việc đó trở nên lãng phí.

### III.6.4. Frame Relay

Mỗi gói tin trong mạng gọi là Frame, do vậy mạng gọi là Frame relay. Đặc điểm khác biệt giữa mạng Frame Relay và mạng X25 mạng Frame Relay là chỉ kiểm tra lỗi tại hai trạm gửi và trạm nhận còn trong quá trình chuyển vận qua các nút trung gian gói tin sẽ không được kiểm lỗi nữa. Do vậy thời gian xử lý trên mỗi nút nhanh hơn, tuy nhiên khi có lỗi thì gói tin phải được phát lại từ trạm đầu. Với độ an toàn cao của đường truyền hiện nay thì chi phí việc phát lại đó chỉ chiếm một tỷ lệ nhỏ nếu so với khối lượng tính toán được giảm đi tại các nút nên mạng Frame Relay tiết kiệm được tài nguyên của mạng hơn so với mạng X25.

Frame relay không chỉ là một kỹ thuật mà còn là thể hiện một phương pháp tổ chức mới. Với nguyên lý là truyền mạch gói nhưng các thao tác kiểm soát giữa các đầu cuối giảm đáng kể. Kỹ thuật Frame Relay cho phép thông lượng tối đa đạt tới 2Mbps và hiện nay nó đang cung cấp các giải pháp để tương nối các mạng cục bộ LAN trong một kiến trúc xương sống tạo nên môi trường cho ứng dụng multimedia.

# Chương IV. Giao thức tầng mạng

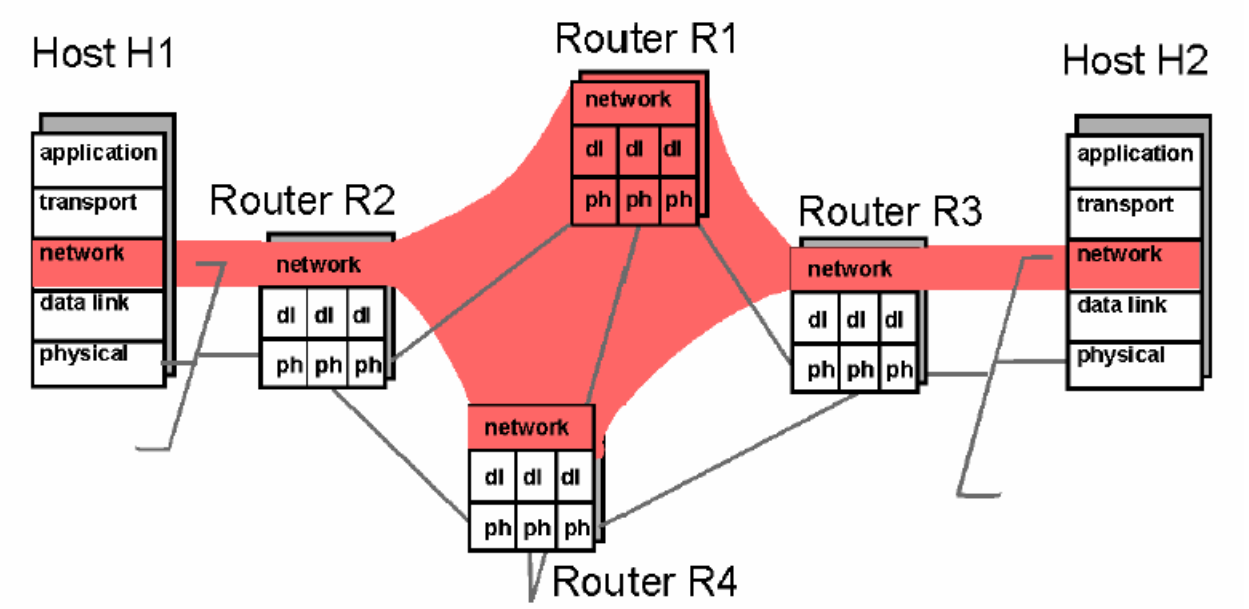
## IV.1. Chức năng của tầng mạng

### IV.1.1. Chức năng

Tầng mạng (Network layer) đảm bảo truyền tin thông suốt giữa hai nút đầu cuối trong mạng. Truyền các gói tin (packets) từ nơi gửi (sending host) tới nơi nhận (receiving host). Tầng mạng được cài đặt tại router và cả end system.

Chức năng chính:

- Chọn đường (path selection): có nhiều đường đi, gói tin sẽ đi theo đường nào?
- Chuyển mạch (switching, forwarding): chuyển gói tin từ cổng vào tới cổng ra của router một cách thích hợp.
- Thiết lập liên kết (call setup): một số kiến trúc mạng cần thiết lập kênh truyền trước khi truyền.




Hình IV-1. Tầng mạng

### IV.1.2. Dịch vụ cung cấp cho tầng giao vận

- Các dịch vụ phải độc lập với công nghệ được dùng trong mạng.
- Tầng giao vận phải độc lập với công nghệ được dùng trong mạng.

- Các địa chỉ mạng phải thống nhất để tầng iao vận có thể dùng cả mạng LAN và WAN

  *Có hai loại dịch vụ:*

  - Dịch vụ truyền tin liên kết (Connection Oriented Service)
  - Dich vụ truyền tin không liên kết (Connectionless Service)

  Sự khác nhau giữa hai dịch vụ:

| **Vấn đề** | **Dịch vụ có liên kết** | **Dịch vụ không liên kết** |
|---|---|---|
| Khởi động kênh | Cần thiết | Không |
| Địa chỉ đích | Chỉ cần lúc khởi động | Cần ở mọi gói tin |
| Thứ tự gói tin | Được đảm bảo | Không đảm bảo |
| Kiểm soát lỗi | Ở tầng mạng | Ở tầng giao vận |
| Điều khiển thông lượng | Ở tầng mạng | Ở tầng giao vận |
| Thỏa thuận tham số | Có | Không |
| Nhận dạng liên kết | Có | Không |

### IV.1.3. Tổ chức các kênh truyền tin trong mạng

#### 1. Kênh ảo (Virtual Circuit):

Tương đương kênh điện thoại trong tầng vật lý sử dụng trong mạng có liên kêt. Kênh ảo được thiết lập cho mỗi liên kết. Một khi đã được thiết lập thì các gói tin được chuyển đi tương tự trong mạng điện thoại cho đến khi liên kết bị hủy bỏ.

- Mỗi nút mạng chứa một kênh ảo.
- Khi một liên kết được khởi động một kênh ảo chưa dùng sẽ được chọn.
- Nút chọn kênh ảo chứa đường dẫn đến trạm tiếp theo và có số thấp nhất.

Khi gói tin khởi động đến nút đích, nút chọn kênh ảo có số thấp nhất thay thế số trong gói tin và chuyển vào trạm đích. Số kênh ảo nối với trạm đích có thể khác số kênh ảo mà trạm nguồn sử dụng.

#### 2. Mạng Datagram:

Tương đương với điện báo sử dụng trong mạng không liên kết. Trong mạng này không có tuyến đường nào được thiết lập. Các gói tin có thể đi theo nhiều đường khác nhau mà không nhất thiết theo một trình tự xác định. Thông tin vào là địa chỉ đích, thông tin ra là nút mạng phải tới.

Mạng Datagram phức tạp về điều khiển nhưng nếu kênh hỏng thì dễ dàng chuyển sang kênh mới.

Một số đặc trưng của mạng kênh ảo và datagram:

| Vấn đề | Mạng kênh ảo | Mạng datagram |
|---|---|---|
| Khởi động kênh | Cần thiết | Không |
| Địa chỉ hóa | Gói tin chỉ cần số kênh ảo | Gói tin phải có địa chỉ nguồn và địa chỉ đích |
| Thông tin tìm đường | Mỗi kênh ảo cần một vùng trong bảng | Không cần bất cứ thông tin nào |
| Tìm đường | Được thiết lập khi khởi động kênh ảo mới. Liên kết sẽ được duy trì cho cả phiên | Mỗi gói tin tìm đường độc lập.Phải tìm đường mỗi khi có gói tin đến nút mạng |
| Điều khiển | Kênh ảo qua nút hỏng sẽ bị hủy | Chỉ mất gói tin trong nút hỏng |
| Hỏng nút | Dễ khắc phục | Khó khắc phục |
| Độ phức tạp | Trong tầng mạng | Trong tầng giao vận |
| Thích hợp | Các dịch vụ liên kết | Các dịch vụ liên kết và không liên kết |

### IV.1.4. Tìm đường đi (định tuyến) trong mạng

Chức năng quan trọng nhất của tầng mạng là dẫn đường cho các gói tin từ trạm nguồn đến trạm đích. Thuật toán tìm đường là quy trình để quyết định chọn đường ra khỏi nút mạng nhằm gửi gói tin đi tiếp đến nút khác.

Yêu cầu của thuật toán tìm đường:

- Chính xác, ổn định, đơn giản và tối ưu.
- Thuật toán tìm đường phải có khả năng cập nhật lại cấu hình và đường vận chuyển để không phải khởi động lại mạng khi có một nút hỏng hoặc phải ngừng hoạt động của các máy trạm.

Các thuật toán chia làm hai nhóm:

- Nhóm không thích nghi (non adaptive): việc chọn đường không dựa vào việc đánh gia tình trạng mạng và cấu hình trong thời gian thực.
- Nhóm thích nghi (adaptive): việc tìm đường phải thích nghi với tình trạng mạng hiện tại.

### IV.1.5. Tắc nghẽn trong mạng

Khi có quá nhiều gói tin trong mạng hoặc một phần của mạng làm cho hiệu suất của mạng giảm đi vì các nút mạng không đủ khả năng lưu trữ, xử lý, gửi đi và

chúng bắt đầu bị mất các gói tin. Hiện tượng này gọi là sự tắc nghẽn (congestion) trong mạng.

Hàng đợi sẽ bị đầy (phải lưu tập tin, các bảng định tuyến,...) nếu khả năng xử lý của nút yếu hay thông tin vào nhiều hơn khả năng của đường ra.

Các biện pháp ngăn ngừa:

- Bố trí khả năng vận chuyển, lưu trữ, xử lý của mạng dư so với yêu cầu.
- Hủy bỏ các gói tin bị tắc nghẽn quá thời hạn.
- Hạn chế số gói tin vào mạng nhờ cơ chế cửa sổ (flow control).
- Chặn đường vào của các gói tin khi mạng quá tải.

## IV.2. Bộ định tuyến và các thiết bị kết nối mạng khác:

### IV.2.1. Bộ định tuyến (Router)

Trong môi trường gồm nhiều mạng gắn kết với nhau bằng nhiều giao thức và kiến trúc mạng khác nhau, bộ chuyển mạch (cầu nối) không thể truyền thông nhanh trong tất cả các đoạn mạng. Mạng có độ phức tạp như vậy cần một thiết bị không những biết địa chỉ mạng mỗi đoạn mạng mà còn quyết định tuyến đường tốt nhất để truyền dữ liệu và lọc các lưu lượng quảng bá trên các đoạn mạng cục bộ. Thiết bị như vậy gọi là bộ định tuyến (Router).

Hình IV-2. Router

Chức năng bộ định tuyến:

- Chuyển và định tuyến gói dữ liệu qua nhiều mạng dựa trên địa chỉ phân lớp mạng.
- Phân chia mạng lớn thành nhiều mạng nhỏ và kết nối các đoạn mạng với nhau.
- Lọc gói tin và giới hạn lưu lượng mạng, hoạt động như một rào cản an toàn giữa các đoạn mạng.
- Ngăn chặn tình trạng quảng bá vì router không chuyển tiếp gói tin dạng quảng bá.

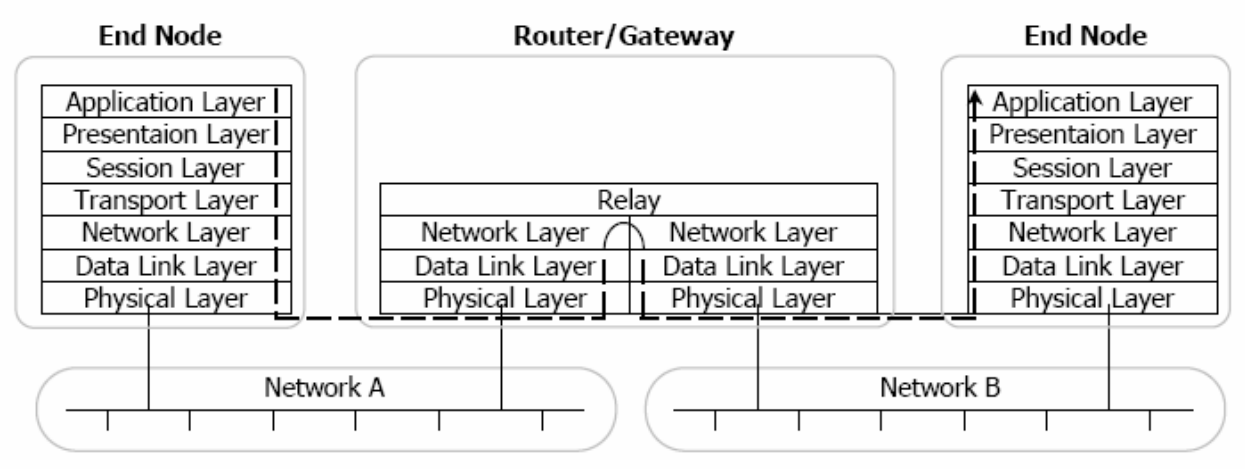
- Các bộ định tuyến có thể chia sẻ thông tin trạng thái và thông tin định tuyến với nhau, sử dụng thông tin này để bỏ qua các kết nối hỏng hoặc chậm.

**Nguyên lý hoạt động:**

Trong bộ định tuyến có một bảng định tuyến chứa các địa chỉ mạng. Tuy nhiên địa chỉ mạng có thể được lưu trữ tùy vào giao thức mạng đang chạy. Bộ định tuyến dùng bảng định tuyến để xác định địa chỉ đích cho dữ liệu nhận được. Bảng này liệt kê các thông tin sau:

- Địa chỉ mạng đã kết nối trực tiếp.
- Cách kết nối tới những mạng khác.
- Chi phí truyền dữ liệu qua các lộ trình đó.

Khi router nhận được gói dữ liệu truyền tới mạng ở xa, nó kiểm tra bảng định tuyến và chọn đường đi tối ưu (có chi phí thấp nhất) để gửi gói dữ liệu đến đích.




Hình IV-3. Kiến trúc Router trong mô hình OSI

**Truyền dữ liệu qua bộ định tuyến:**

Khi một trạm xác định cần gửi một gói dữ liệu tới một trạm trên một mạng khác. Công việc đầu tiên của trạm này là lấy địa chỉ vật lý của router (địa chỉ cổng kết nối ngầm định). Sau đó nó điền thông tin trong trường địa chỉ vật lý của gói dữ liệu bằng địa chỉ vậy lý của router và trường thông tin địa chỉ đích của tầng mạng (là địa chỉ IP nếu dùng TCP/IP) bằng địa chỉ của trạm đích.

Khi router kiểm tra địa chỉ đích, nó xác định xem nó có biết cách hay không chuyển tiếp gói tin đến chặng tiếp theo (next hop) là router kế tiếp trên đường đi, bằng cách kiểm tra địa chỉ. Nếu địa chỉ mạng đích nằm trong gói dữ liệu không có trong bảng định tuyến, router sẽ bỏ gói dữ liệu trừ khi nó được cấu hình đường đi mặc định. Ngược lại nếu địa chỉ mạng đích có trong bảng định tuyến, router thay

địa chỉ vật lý đích bằng địa chỉ vật lý của chặng tiếp theo và truyền gói dữ liệu đến đó.

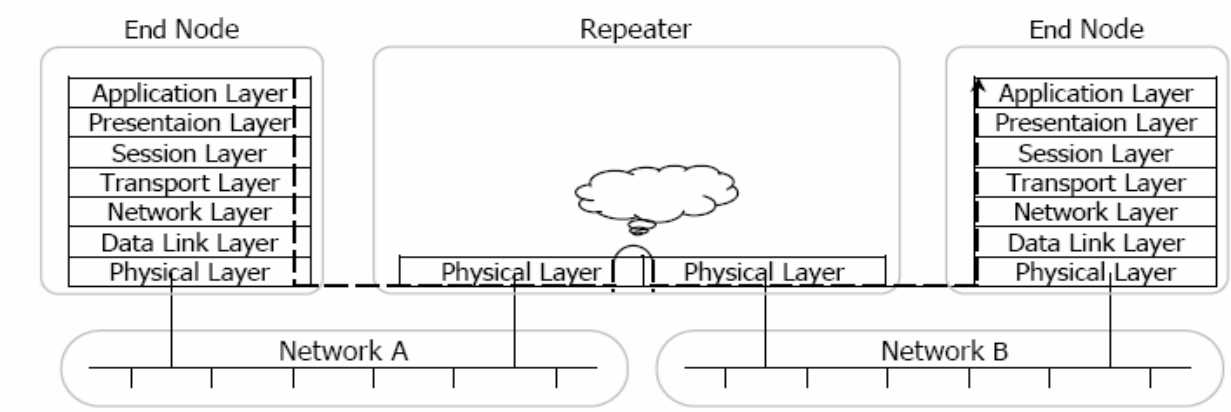
Như vậy, khi một gói tin truyền qua liên mạng, địa chỉ vật lý thay đổi nhưng địa chỉ của giao thức không đổi.

### IV.2.2. Bộ lặp (Repeater)

Bộ lặp thực hiện chức năng ở tầng vật lý dùng để khuyếch đại tín hiệu khi tín hiệu đi xa. Bộ lặp được sử dụng để kết nối các đoạn mạng lại với nhau. Bộ lặp nhận tín hiệu từ một đoạn mạng, tái tạo lại và truyền tín hiệu này đến đoạn mạng khác. Nhờ có bộ lặp mà tín hiệu bị suy yếu do phải truyền qua một đoạn cáp dài có thể trở lại dạng ban đầu và truyền đi được xa hơn.

Hình IV-4.Bộ lặp.

Tất cả các tín hiệu điện, bao gồm nhiễu điện từ và các lỗi khác cũng được lặp và khuyếch đại. Để bộ lặp hoat động, cả hai đoạn mạng nối với bộ lặp phải sử dụng cùng một phương pháp truy cập đường truyền.




Hình IV-5. Repeater trong mô hình OSI

### IV.2.3. Hub

Hub là thiết bị liên kết mạng được sử dụng làm trung tâm trong cấu trúc mạng có dạng hình sao (star). Mạng sao dùng sự phân chia tín hiệu trong Hub để đưa các tín hiệu ra các đường cáp khác nhau. Có 3 loại Hub thường sử dụng trong mạng là

- Hub chủ động: tái tạo và truyền tín hiệu giống như bộ lặp. Hub có nhiều cổng nên được gọi là bộ lặp đa cổng. Hub chủ động đưa các các tín hiệu mạnh hơn do đó cho phép đoạn cáp dài hơn. Đa phần các Hub là Hub chủ động.
- Hub thụ đông: hoặc động như các điểm kết nối, không tái tạo hay khuyếch đại tín hiệu.
- Hub lai: thích ứng với nhiều loại cáp khác nhau

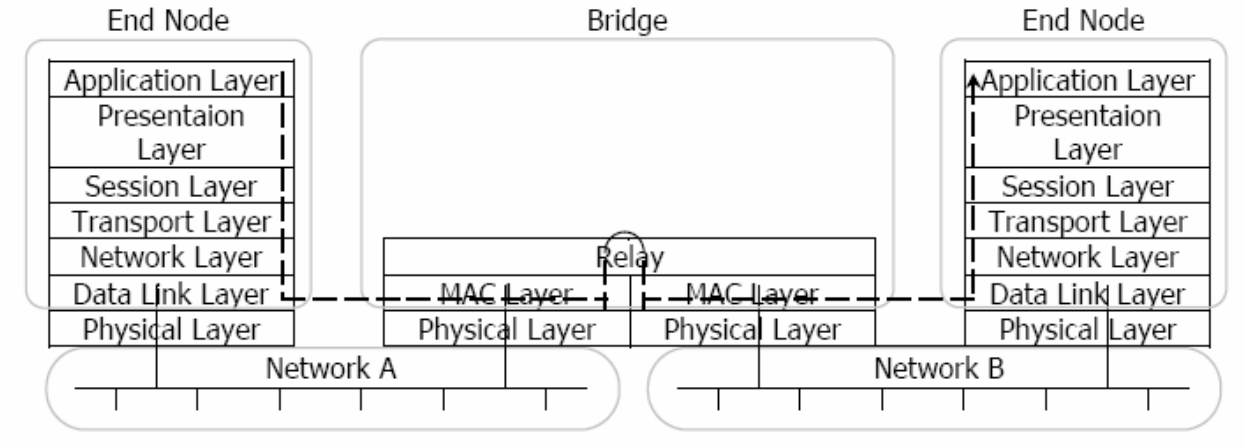
Hình IV-6.Hub

### IV.2.4. Cầu nối (Bridge)

Cầu nối là thiết bị hoạt động ở tầng liên kết dữ liệu, dùng để nối hai hay nhiều đoạn mạng (segment) của mạng LAN khác nhau.

Chức năng của cầu nối:

- Mở rộng khoảng cách phân đoạn mạng, tăng số lượng máy tính trên mạng.
- Lọc những gói dữ liệu để gửi đi hay không gửi đi cho đoạn nối, hoặc gửi trả lại nơi xuất phát.
- Phân chia mạng lớn thành nhiều mạng nhỏ nhằm cô lập lưu lượng, tăng tốc độ mạng. Nếu lưu lượng từ một nhóm máy tính trở nên quá tải và giảm hiệu xuất mạng thì cầu nối có thể cô lập máy tính hay bộ phận này.
- Kết nối các phương tiện truyền dẫn khác nhau.
- Kết nối các đoạn mạng sử dụng phương pháp truy cập khác nhau.




Hình IV-7.Bridge trong mô hình OSI

Nguyên lý hoạt động:

- Cầu nối không phân biệt giao thức này với giao thức khác, chỉ có nhiệm vụ lưu chuyển tất cả các giao thức trên mạng. Vì các giao thức đều có thể di chuyển qua cầu nối nên tùy thuộc vào từng máy quyết định chúng có thể nhận diện giao thức
- Cầu nối hoạt động trên nguyên tắc mỗi nút mạng có một địa chỉ riêng. Cầu nối chuyển gói dữ liệu dựa trên địa chỉ vật lý (MAC address) của nút đích. Khi dữ liệu truyền qua cầu nối, thông tin địa chỉ này sẽ được lưu trong RAM của cầu nối dùng để xây dựng bản địa chỉ dựa trên địa chỉ nguồn của gói tin.

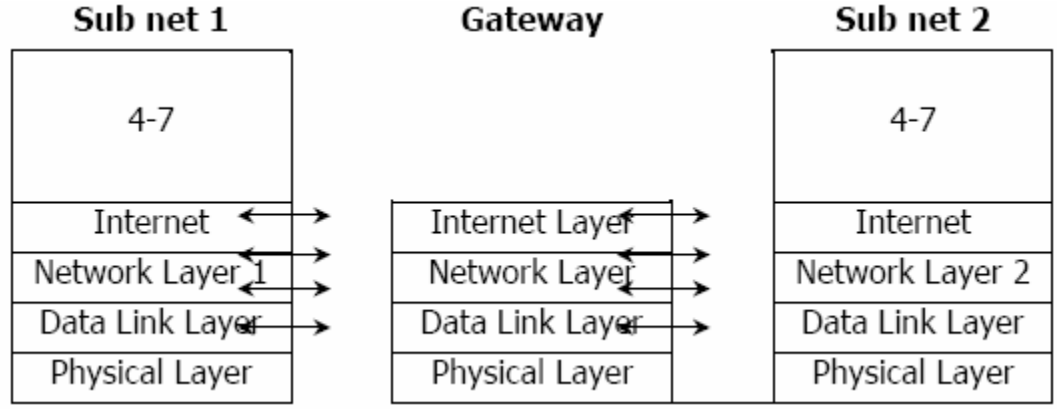
### IV.2.5. Bộ chuyển mạch (Switch)

Bộ chuyển mạch có chức năng giống cầu nối nhưng có nhiều port. Bộ chuyển mạch có thể kết nối một số mạng LAN riêng biệt và cung cấp khả năng lọc gói dữ liệu giữa chúng. Hiện nay, bộ chuyển mạch được sử dụng rộng rãi thay thế cho Hub.

Hình IV-8. Switch

### IV.2.6. Gateway

Gateway (cổng nối) hoạt động ở mức mạng, thực hiện việc ghép nối với WAN. Nguyên lý chung của nối kết này là tạo ra một tầng "liên mạng" (internet) trong tất cả các kiến trúc của mạng con tham gia nối kết. Tầng liên mạng thường là tầng con nằm ngay trên tầng 3 trong mô hình OSI.




Hình IV-9. Sơ đồ kiến trúc của gateway trong mô hình OSI.

Tầng con Internet được cài đặt trong tất cả các trạm cũng như trong các giao diện kết nối (gateway). Tầng này cung cấp dịch vụ truyền thông liên mạng với hai chức năng chính:

- Chuyển đổi các đơn vị dữ liệu của giao thức (Protocol Data Unit-PDU).
- Chọn đường đi cho các PDU này.

Các gói tin ở tầng con Internet lưu thông trong mạng theo phương pháp "đóng gói/tách gói". Khi một datagram được truyền từ mạng con này qua mạng con khác thông qua gateway thì nó được bổ sung vào hoặt tách ra các phần thông tin điều khiển cần thiết cho mạng con. Gateway có các giao thức xác định trước thường là nhiều giao thức, một gateway đa giao thức thường được chế tạo như các card có chứa các bộ xử lý riêng và cài đặt trên các máy tính hoặc thiết bị chuyên biệt.

## IV.3. Giao thức IP (IP Protocol)

Giao thức IP (Internet Protocol) hoạt động ở tầng mạng, cung cấp dịch vụ dữ liệu không liên kết (connectionless) cho nhiều giao thức liên kết dữ liệu khác. Đơn vị dữ liệu dùng trong IP là *datagram*, hay còn gọi là gói tin.

Chức năng chính của IP:

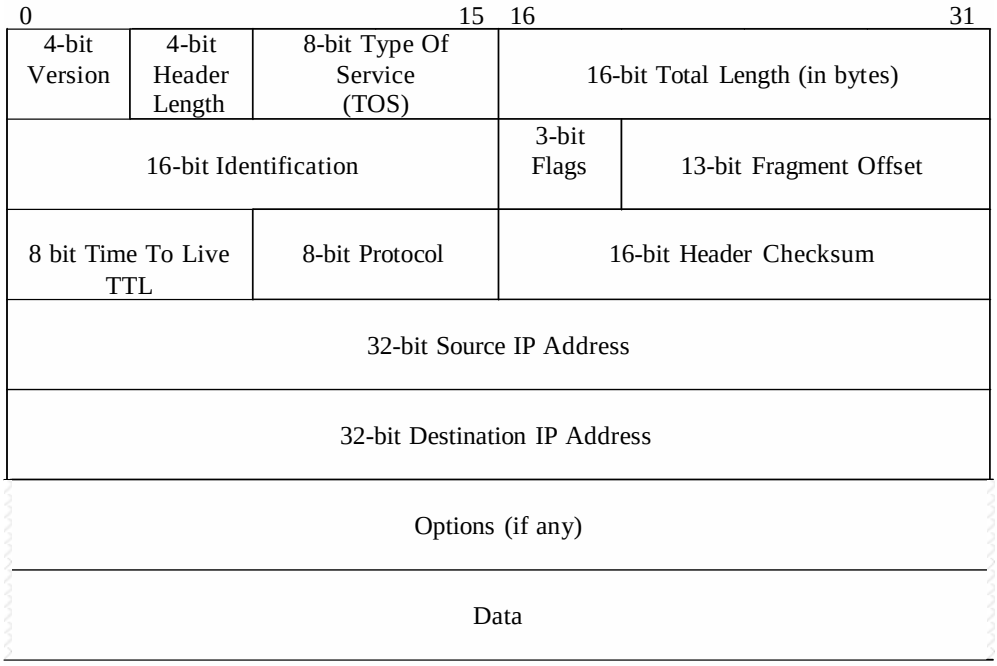
- Định nghĩa gói tin datagram là đơn vị dữ liệu cơ bản của việc truyền tin trên Internet.

- Xác định mô hình gán địa chỉ cho các gói tin và quản lý các quá trình trao đổi, xử lý các gói tin này.
- Chọn đường cho các datagram trên mạng.
- Phân đoạn và sắp xếp lại các gói tin.

Tính chất của giao thức IP

- Là giao thức hoạt động theo phương thức không nối kết.
- Không tin cậy: giao thức IP không có khả năng phát hiện và khắc phục lỗi, không quan tâm đến vấn đề dữ liệu có được nhận một cách chính xác không. Các gói dữ liệu có thể bị thất lạc, trùng lập, bị chậm hoặc không đúng thứ tự. Mỗi gói dữ liệu được xử lý độc lập và có thể gửi theo những đường định tuyến khác nhau.

### IV.3.1. Định dạng khung gói tin IP




Hình IV-10. Định dạng khung gói tin IP

Ý nghĩa các trường dữ liệu:

- *VER* (4 bits): chỉ version hiện hành của giao thức IP hiện được cài đặt, việc có chỉ số version cho phép có các trao đổi giữa các hệ thống sử dụng version cũ và hệ thống sử dụng version mới.
- *IHL* (4 bits): chỉ độ dài phần đầu (Internet header Length) của gói tin datagram, tính theo đơn vị từ ( 32 bits). Trường này bắt buột phải có

vì phần đầu IP có thể có độ dài thay đổi tùy ý. Độ dài tối thiểu là 5 từ (20 bytes), độ dài tối đa là 15 từ hay là 60 bytes.

- *Type of service* (8 bits): đặc tả các tham số về dịch vụ nhằm thông báo cho mạng biết dịch vụ nào mà gói tin muốn được sử dụng, chẳng hạn ưu tiên, thời hạn chậm trễ, năng suất truyền và độ tin cậy. Hình sau cho biết ý nghĩ của trường 8 bits này.


  - Precedence (3 bit): chỉ thị về quyền ưu tiên gửi datagram, nó có giá trị từ 0 (gói tin bình thường) đến 7 (gói tin kiểm soát mạng).
  - D (Delay) (1 bit): chỉ độ trễ yêu cầu trong đó (D = 0 gói tin có độ trễ bình thường, D = 1 gói tin độ trễ thấp)
  - T (Throughput) (1 bit): chỉ độ thông lượng yêu cầu sử dụng để truyền gói tin với lựa chọn truyền trên đường thông suất thấp hay đường thông suất cao.
    - T = 0 thông lượng bình thường và
    - T = 1 thông lượng cao
  - R (Reliability) (1 bit): chỉ độ tin cậy yêu cầu (R = 0 độ tin cậy bình thường, R = 1 độ tin cậy cao)
- *Total Length* (16 bits): chỉ độ dài toàn bộ gói tin, kể cả phần đầu tính theo đơn vị byte với chiều dài tối đa là 65535 bytes. Hiện nay giới hạn trên là rất lớn nhưng trong tương lai với những mạng Gigabit thì các gói tin có kích thước lớn là cần thiết.
- *Identification* (16 bits): cùng với các tham số khác (như Source Address và Destination Address) tham số này dùng để định danh duy nhất cho một datagram trong khoảng thời gian nó vẫn còn trên liên mạng.
- *Flags (3 bits):* liên quan đến sự phân đoạn (fragment) các datagram, Các gói tin khi đi trên đường đi có thể bị phân thành nhiều gói tin nhỏ, trong trường hợp bị phân đoạn thì trường Flags được dùng điều khiển phân đoạn và tái lắp ghép bó dữ liệu. Tùy theo giá trị của Flags sẽ có ý nghĩa là gói tin sẽ không phân đoạn, có thể phân đoạn hay là gói tin phân đoạn cuối cùng. Trường ***Fragment Offset*** cho biết vị trí dữ liệu thuộc phân đoạn tương ứng với đoạn bắt đầu của gói dữ liệu gốc. Ý nghĩa cụ thể của trường Flags là:

  - bit 0: reserved - chưa sử dụng, luôn lấy giá trị 0.
  - bit 1: (DF) = 0 (May Fragment) = 1 (Don't Fragment)
  - bit 2: (MF) = 0 (Last Fragment) = 1 (More Fragments)

- Fragment Offset (13 bits): chỉ vị trí của đoạn (fragment) ở trong datagram tính theo đơn vị 8 bytes, có nghĩa là phần dữ liệu mỗi gói tin (trừ gói tin cuối cùng) phải chứa một vùng dữ liệu có độ dài là bội số của 8 bytes. Điều này có ý nghĩa là phải nhân giá trị của Fragment offset với 8 để tính ra độ lệch byte.
- *Time to Live (8 bits)*: qui định thời gian tồn tại của gói tin trong mạng để tránh tình trạng một gói tin bị quẩn trên mạng. Thời gian này được cho bởi trạm gửi và được giảm đi (thường qui ước là 1 đơn vị) khi datagram đi qua mỗi router của liên mạng. Thời lượng này giảm xuống tại mỗi router với mục đích giới hạn thời gian tồn tại của các gói tin và kết thúc những lần lặp lại vô hạn trên mạng. Sau đây là 1 số điều cần lưu ý về trường ***Time To Live***:
  - Nút trung gian của mạng không được gởi 1 gói tin mà trường này có giá trị= 0.
  - Một giao thức có thể ấn định **Time To Live** để thực hiện cuộc ra tìm tài nguyên trên mạng trong phạm vi mở rộng.
  - Một giá trị cố định tối thiểu phải đủ lớn cho mạng hoạt động tốt.
- *Protocol (8 bits): chỉ giao thức tầng trên kế tiếp sẽ nhận vùng dữ liệu ở* trạm đích (hiện tại thường là TCP hoặc UDP được cài đặt trên IP). Ví dụ: **TCP** có giá trị trường **Protocol** là 6, **UDP** có giá trị trường **Protocol** là 17.
- Header Checksum (16 bits): Mã kiểm soát lỗi của header gói tin IP.
- Source Address (32 bits): Địa chỉ IP của máy nguồn.
- Destination Address (32 bits): Địa chỉ IP của máy đích.
- Options (độ dài thay đổi): Khai báo các lựa chọn do người gửi yêu cầu (tuỳ theo từng chương trình).
- Padding (độ dài thay đổi): Vùng đệm, được dùng để đảm bảo cho phần header luôn kết thúc ở một mốc 32 bits.
- *Data (độ dài thay đổi)*: Trên một mạng cục bộ như vậy, hai trạm chỉ có thể liên lạc với nhau nếu chúng biết địa chỉ vật lý của nhau. Như vậy vấn đề đặt ra là phải thực hiện ánh xạ giữa địa chỉ IP (32 bits) và địa chỉ vật lý (48 bits) của một trạm.

### IV.3.2. Phân mảnh và sắp xếp lại

Mỗi mạng đều có một maximum transmission unit (MTU), đây là kích thước lớn nhất mà một IP datagram có thể mang trong một khung. Chú ý rằng giá trị này thì nhỏ hơn kích thước gói lớn nhất trên mạng bởi vì IP datagram cần điều chỉnh cho phù hợp với khung trong tầng liên kết.

Lúc một gói gửi một IP datagram nó có thể chọn bất cứ kích thước nào mà nó muốn. Thông thường nó chọn bằng MTU của mạng mà host được nối kết trực tiếp. Sự phân mảnh sẽ được thực hiện nếu đường dẫn nguồn đi qua một mạng có MTU nhỏ hơn. Các giao thức vận chuyển ở trên IP sẽ truyền một gói có kích thước lớn hơn MTU cục bộ và host nguồn phải phân mảnh nó.

Sự phân mảnh thường xuất hiện ở các router lúc nó nhận một datagram và datagram này phải truyền qua một mạng có MTU nhỏ hơn kích thước của datagram nó nhận. Và sự sắp xếp xảy ra tại host đích nơi nó nhận datagram(các gói phải có cùng Id trong trường Ident), trường này được chọn bởi host gửi và nó định danh duy nhất trong số tất cả các datagram đến đích qua một khoảng thời gian nào đó (IP không cố gắng tìm lại khi sự phân mảnh bị lỗi).

Ví dụ một gói tin 4000 bytes và MTU là 1500:

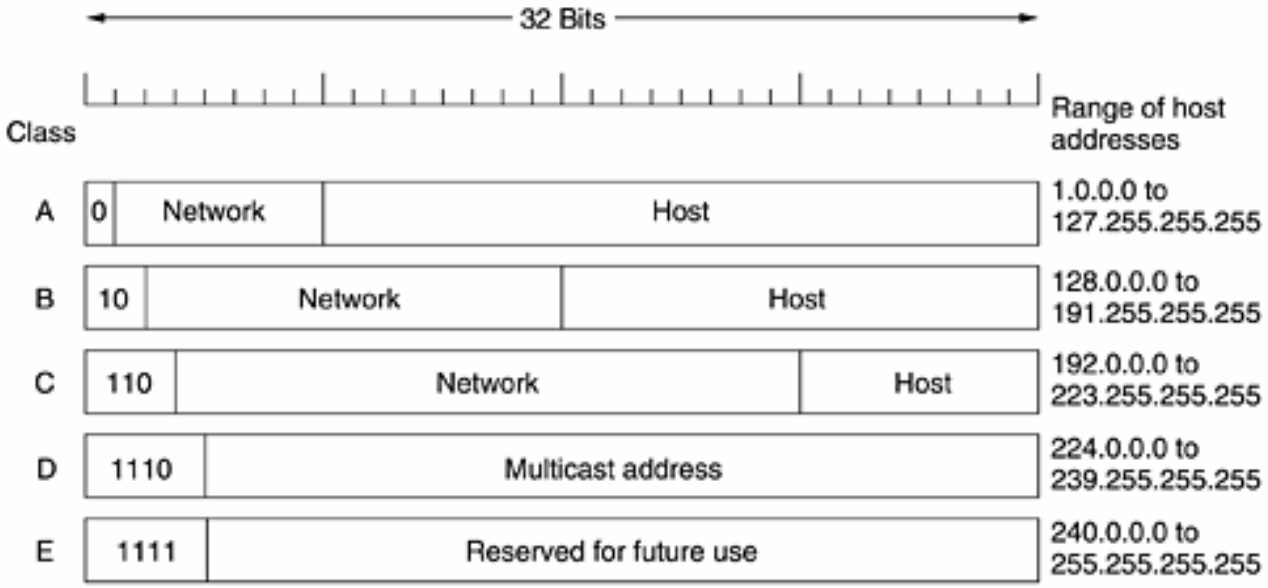

### IV.3.3. Địa chỉ IP

Sơ đồ địa chỉ hóa để định danh các trạm (host) trong liên mạng được gọi là địa chỉ IP 32 bits (32 bit IP address). Mỗi giao diện trong 1 máy có hỗ trợ giao thức IP đều phải được gán 1 địa chỉ IP (một máy tính có thể gắn với nhiều mạng do vậy có thể có nhiều địa chỉ IP). Địa chỉ IP gồm 2 phần: địa chỉ mạng (netid) và địa chỉ máy (hostid). Mỗi địa chỉ IP có độ dài 32 bits được tách thành 4 vùng (mỗi vùng 1 byte), có thể biểu thị dưới dạng thập phân, bát phân, thập lục phân hay nhị

phân. Cách viết phổ biến nhất là dùng ký pháp thập phân có dấu chấm (dotted decimal notation) để tách các vùng. Mục đích của địa chỉ IP là để định danh duy nhất cho một máy tính bất kỳ trên liên mạng.

Do tổ chức và độ lớn của các mạng con (subnet) của liên mạng có thể khác nhau, người ta chia các địa chỉ IP thành 5 lớp, ký hiệu là A, B, C, D và E. Trong lớp A, B, C chứa địa chỉ có thể gán được. Lớp D dành riêng cho lớp kỹ thuật multicasting. Lớp E được dành những ứng dụng trong tương lai.

Netid trong địa chỉ mạng dùng để nhận dạng từng mạng riêng biệt. Các mạng liên kết phải có địa chỉ mạng (netid) riêng cho mỗi mạng. Ở đây các bit đầu tiên của byte đầu tiên được dùng để định danh lớp địa chỉ (0 - lớp A, 10 - lớp B, 110 - lớp C, 1110 - lớp D và 11110 - lớp E).




Hình IV-11. Phân lớp địa chỉ IP

Khi sử dụng mạng cục bộ, không liên kết với mạng khác người sử dụng có thể gán tùy ý địa chỉ IP cho các trạm. Tuy nhiên với các site Internet thì địa chỉ IP phải được cung cấp bởi trung tâm quản lý thông tin mạng (NIC-Network Information Center).

Một số địa chỉ IP đặc biệt:

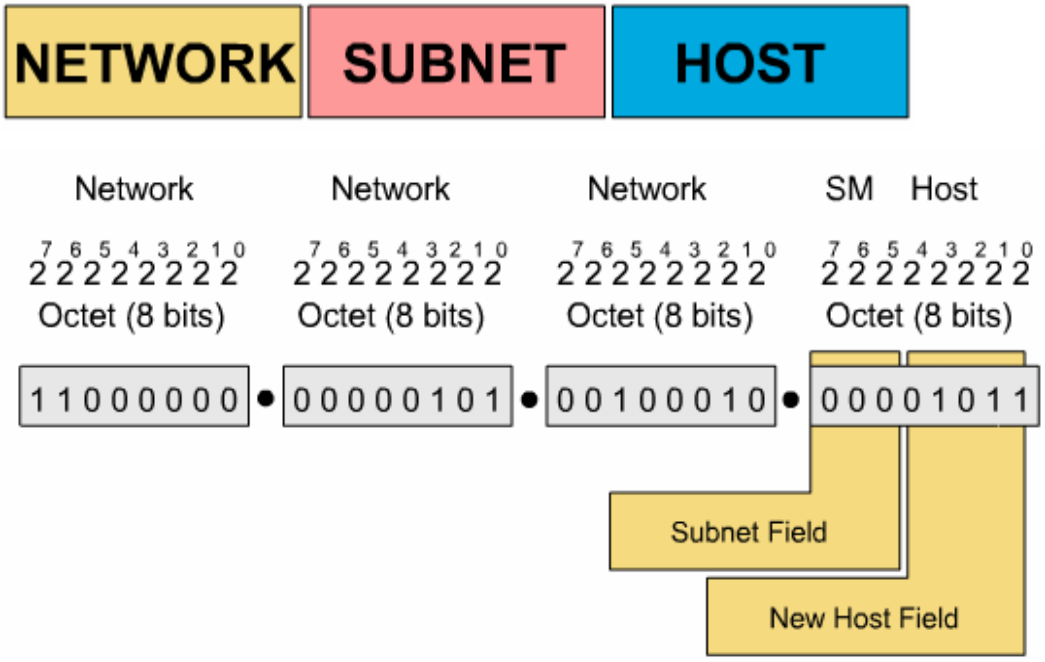
- Địa chỉ Loopback (127.x.x.x): tất cả các gói tin được gửi đến địa chỉ 127.0.0.0 đều được gửi trở lại máy tính.Địa chỉ loopback có thể được dùng như một địa chỉ kiểm tra nhanh xem phần mền TCP/IP có được cấu hình thích hợp. Trên hệ điều hành Windows thường dùng 127.0.0.1, Unix 127.0.0.*
- Địa chỉ quảng bá (broadcast address): địa chỉ này có các bit của phần hostID đều mang giá trị 1, được sử dụng khi muốn gửi gói tin đến tất cả

các máy của mạng con. Ví dụ địa chỉ 192.168.1.0 có địa chỉ quảng bá là 192.168.1.255.

**Mặt nạ mạng con(sunet mask):** là một số 32 bit bao gồm các bit cao = 1 và các bit thấp = 0. Các bit 1 quy định subnet, các bit 0 quy định địa chỉ host.từ subnet mask có thể xác định ranh giới giữa địa chỉ mạng và địa chỉ của interface (host). Thực hiện phép toán AND giữa địa chỉ IP và sunet mask sẽ cho địa chỉ mạng.

Ví dụ: địa chỉ IP lớp B 172.16.1.1, có mặt nạ 255.255.0.0 sẽ cho địa chỉ mạng là 172.16.0.0

**Mạng con (subnet):** để thuận lợi cho việc định tuyến dữ liệu trên mạng lớn, người ta thường tổ chức mạng IP theo cơ chế địa chỉ phân cấp, mỗi mạng được chia nhỏ thành nhiều mạng con. Mỗi mạng con chịu trách nhiệm cho việc chọn đường cho các gói tin IP trong mạng của mình, các gói tin này được nhận ra nhờ phần địa chỉ mạng. Trong các lớp mạng A, B, C thì phần địa chỉ mạng cố định. Tuy nhiên, để tạo sự linh hoạt khi phân chia mạng con thì địa chỉ mạng có thể mở rộng sang các bit của phần host, đó là kĩ thuật phân chia mạng con




Hình IV-12. Chia mạng con

### IV.3.4. Các bước hoạt động của giao thức IP

Khi giao thức IP được khởi động nó trở thành một thực thể tồn tại trong máy tính và bắt đầu thực hiện những chức năng của mình, lúc đó thực thể IP là cấu thành của tầng mạng, nhận yêu cầu từ các tầng trên nó và gửi yêu cầu xuống các tầng dưới nó.

Đối với thực thể IP ở máy nguồn, khi nhận được một yêu cầu gửi từ tầng trên, nó thực hiện các bước sau đây:

- Tạo một IP datagram dựa trên tham số nhận được.
- Tính checksum và ghép vào header của gói tin.
- Ra quyết định chọn đường: hoặc là trạm đích nằm trên cùng mạng hoặc một gateway sẽ được chọn cho chặng tiếp theo.
- Chuyển gói tin xuống tầng dưới để truyền qua mạng.

Đối với router, khi nhận được một gói tin đi qua, nó thực hiện các động tác sau:

1. Tính chesksum, nếu sai thì loại bỏ gói tin.
2. Giảm giá trị tham số Time-to-Live. nếu thời gian đã hết thì loại bỏ gói tin.
3. Ra quyết định chọn đường.
4. Phân đoạn gói tin, nếu cần.
5. Kiến tạo lại IP header, bao gồm giá trị mới của các vùng Time - to - Live, Fragmentation và Checksum.
6. Chuyển datagram xuống tầng dưới để chuyển qua mạng.

Cuối cùng khi một datagram nhận bởi một thực thể IP ở trạm đích, nó sẽ thực hiện bởi các công việc sau:

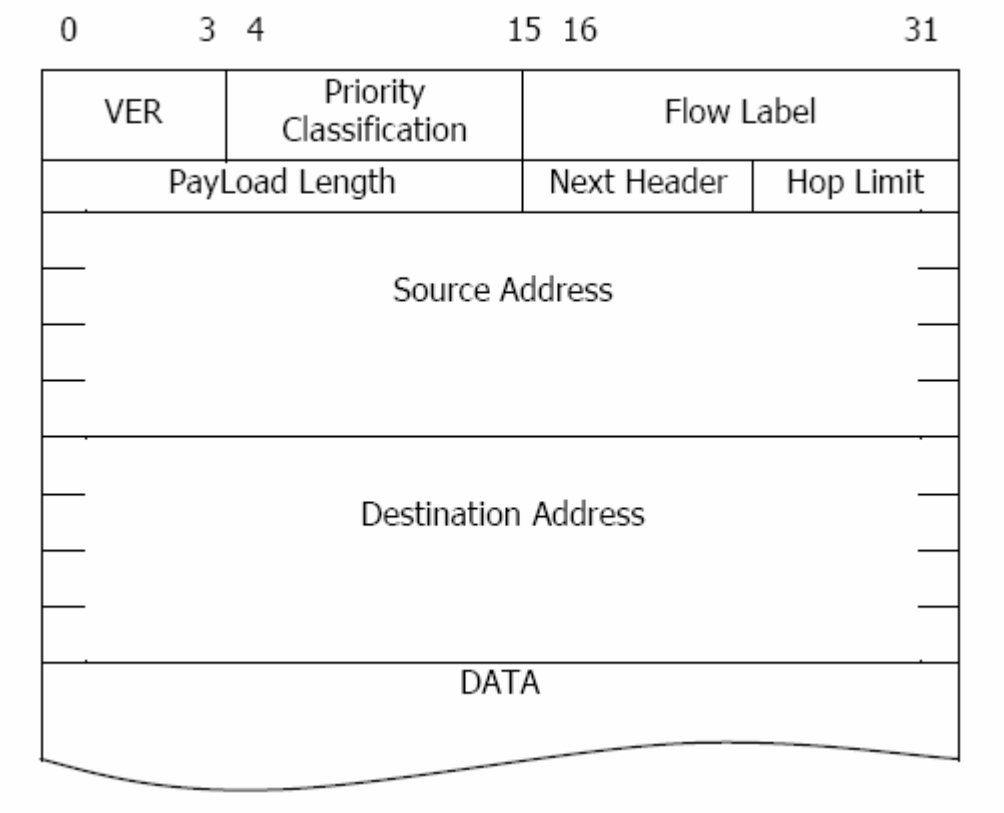
1. Tính checksum. Nếu sai thì loại bỏ gói tin.
2. Tập hợp các đoạn của gói tin (nếu có phân đoạn)
3. Chuyển dữ liệu và các tham số điều khiển lên tầng trên.

### IV.3.5. IPv6

Với sự phát triển nhanh chóng của Internet thì địa chỉ IP 32 bit không còn đáp ứng đủ cho nhu cầu sử dụng Internet. Để khắc phục điều này, phiên bản IPv6 (IP Next Generation) đang được phát triển. Phiên bản IPv6 có các thay đổi sau:

- Sử dụng 128 bit địa chỉ mạng thay vì 32 bit địa chỉ như phiên bản IPv4.
- Mở rộng phần Header cho ứng dụng và lựa chọn của khung tin.
- Hỗ trợ các loại dữ liệu video và audio.
- Có các giao thức mở rộng: cho phép bổ sung nhiều thông tin vào một datagram.

Định dạng khung header của IPv6:




Hình IV-13. Định dạng khung IPv6

## IV.4. Các giao thức liên quan đến IP

Để mạng với giao thức IP hoạt động được tốt người ta cần một số giao thức bổ sung, các giao thức này đều không phải là bộ phận của giao thức IP và giao thức IP sẽ dùng đến chúng khi cần.

- **Giao thức ARP (Address Resolution Protocol):** Ở đây cần lưu ý rằng các địa chỉ IP được dùng để định danh các host và mạng ở tầng mạng của mô hình OSI, và chúng không phải là các địa chỉ vật lý (hay địa chỉ MAC) của các trạm trên đó một mạng cục bộ (Ethernet, Token Ring.). Trên một mạng cục bộ hai trạm chỉ có thể liên lạc với nhau nếu chúng biết địa chỉ vật lý của nhau. Như vậy vấn đề đặt ra là phải tìm được ánh xạ giữa địa chỉ IP (32 bits) và địa chỉ vật lý của một trạm. *Giao thức ARP* đã được xây dựng để tìm địa chỉ vật lý từ địa chỉ IP khi cần thiết.
- **Giao thức RARP (Reverse Address Resolution Protocol):** Là giao thức ngược với *giao thức ARP*. Giao thức RARP được dùng để tìm địa chỉ IP từ địa chỉ vật lý.
- **Giao thức ICMP (Internet Control Message Protocol):** Giao thức này thực hiện truyền các thông báo điều khiển (báo cáo về các tình trạng các

lỗi trên mạng.) giữa các gateway hoặc một nút của liên mạng. Tình trạng lỗi có thể là: một gói tin IP không thể tới đích của nó, hoặc một router không đủ bộ nhớ đệm để lưu và chuyển một gói tin IP. Một thông báo ICMP được tạo và chuyển cho IP, IP sẽ "bọc" (encapsulate) thông báo đó với một IP header và truyền đến cho router hoặc trạm đích.

## IV.5. Giao thức định tuyến

Chúng ta cho rằng cả chuyển mạch và router không đủ thông tin về topology mạng để chúng có thể quyết định chọn đúng cổng cho các gói được output. Trong trường hợp chuyển mạch kênh, định tuyến là vấn đề chỉ cho các gói yêu cầu nối kết, còn tất cả các gói theo sau thì đi cùng đường dẫn như gói yêu cầu.

Trong mạng datagram(mạng IP), định tuyến là vấn đề của tất cả các gói. Một chuyển mạch hay một router cần phải xem xét các địa chỉ đích trong mỗi gói và rồi quyết định cổng tốt nhất mà gói có thể truyền. Chuyển mạch thực hiện quyết định dựa trên các thông tin trong bảng chuyển tiếp. Vấn đề cơ bản của quá trình chuyển tiếp là các chuyển mạch hay router lấy được thông tin trong các bảng này.

- Quá trình chuyển tiếp bao gồm lấy một gói, xem địa chỉ nguồn, tham khảo bảng và gửi gói đó theo hướng được xác định bởi dữ liệu trong bảng đó.
- Định tuyến là một quá trình xây dựng bảng.

Xem bảng sau, trong trường hợp bảng định tuyến có nghĩa là mạng số 10 có thể đến bởi router chặng tiếp theo có địa chỉ 171.69.245.10, trong khi bảng forwarding chứa thông tin chính xác như thế nào để chuyển gói chặng tiếp theo, gửi gói ra ngoài qua giao tiếp 0 với địa chỉ 8:0:2b:e4:b:1:2.

| NetworkNum | NextHop |
|---|---|
| 10 | 171.69.245.10 |

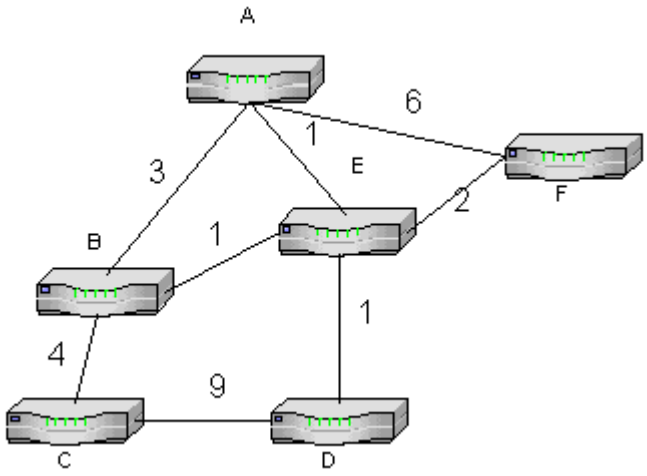
a)Bảng định tuyến

| NetworkNum | Interface | MAC address |
|---|---|---|
| 10 | If0 | 8:0:2b:e4:b:1:2 |

b)Bảng forwarding

### 1. Mạng là đồ thị:

Định tuyến là một bài toán của đồ thị, hình trên là một đồ thị thể hiện một mạng, một nút của đồ thị là các nhãn từ A đến F, các nhãn có thể là host, chuyển mạch, router hay một mạng. Trong trường hợp này chúng ta chỉ quan tâm các nút là router. Các cạnh của đồ thị tương ứng với một liên kết mạng. Mỗi cạnh được gán một trọng số(chi phí).




Hình IV-14.Mạng thể hiện như đồ thị

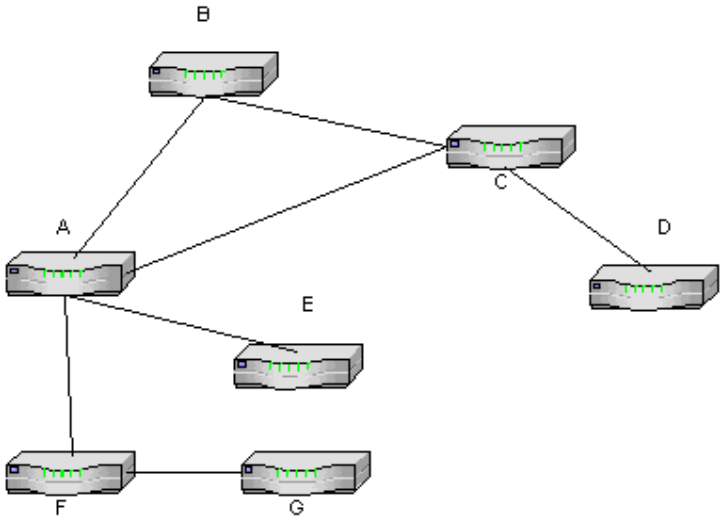
Vấn đề cơ bản của định tuyến là tìm được một đường đi có chi phí thấp nhất giữa hai nút(chi phí của đường đi bằng tổng chi phí của tất cả các cạnh trên đường đi).

Có 2 cách xây dựng định tuyến cho các nút:

- Tính tất cả các đường đi ngắn nhất và lưu trữ chúng trên mỗi nút.
- Thực hiện giao thức định tuyến tương ứng giữa tất cả các nút.

Chúng ta giả sử chi phí mỗi cạnh trong mạng có thể biết được, chúng ta xem xét hai lớp giao thức routing chính được sử dụng trong mạng: distance vector và link state.

**2. Định tuyến theo vector khoảng cách-Distance Vector(RIP):**




Hình IV-15. Ví dụ về định tuyến Distance Vector

**Ý tưởng:**

Mỗi nút xây dựng một mảng một chiều(vector) chứa khoảng cách(chi phí) đến tất cả các nút và phân phối vector đó với người hàng xóm của chúng. Để bắt đầu xây dựng, mỗi nút phải biết chi phí của các liên kết trực tiếp với người hàng xóm của chúng. Sau đó nó mới gán một chi phí xác định.

| Thoâng tin löu trõõ ôû Nuùt | Khoaûng caùch ñeán caùc nuùt | | | | | | |
|---|---|---|---|---|---|---|---|
| | A | B | C | D | E | F | G |
| A | 0 | 1 | 1 | ∞ | 1 | 1 | ∞ |
| B | 1 | 0 | 1 | ∞ | ∞ | ∞ | ∞ |
| C | 1 | 1 | 0 | 1 | ∞ | ∞ | ∞ |
| D | ∞ | ∞ | 1 | 0 | ∞ | ∞ | 1 |
| E | 1 | ∞ | ∞ | ∞ | 0 | ∞ | ∞ |
| F | 1 | ∞ | ∞ | ∞ | ∞ | 0 | 1 |
| G | ∞ | ∞ | ∞ | 1 | ∞ | 1 | 0 |

Bảng IV-1.Khởi tạo khoảng cách tại mỗi nút

Bảng trên trình bày thông tin khởi tạo về khoảng cách của từng nút đến tất cả các nút còn lại trong mạng.

Mỗi hàng trong bảng là một danh sách khoảng cách từ một nút đến tất cả các nút khác. Khởi tạo, mỗi nút đặt một chi phí là 1 cho tất cả các người hàng xóm của chúng và cho tất cả các nút khác. Thật vậy, lúc khởi tạo A có thể tin rằng nó có thể đi 1 bước tới B, nhưng không thể đến D. Bảng định tuyến lưu trữ ở A như sau:

| Destination | Cost | NextHop |
|---|---|---|
| B | 1 | B |
| C | 1 | C |
| D | ∞ | - |
| E | 1 | E |
| F | 1 | F |
| G | ∞ | - |

Bảng IV-2.Khởi tạo bảng định tuyến ở nút A

Tiếp theo mỗi nút gửi một thông điệp chứa danh sách khoảng cách cá nhân của nó trực tiếp đến các nút hàng xóm. Ví dụ nút F nói với nút A là nó có thể đến G với chi phí là 1; A biết nó có thể đến F với chi phí 1, nó cộng chi phí này với chi phí đến G từ F. Tổng chi phí là 2. Vậy A có thể đến G với chi phí là 2 qua F. Tương tự A có thể học từ C và biết rằng nó có thể đến D với chi phí là 2 qua C.

Lúc này A có thể cấp nhật bảng định tuyến với chi phí và chặng tiếp theo (nexthop) cho tất cả các nút trên mạng. Kết quả trong bảng sau:

| Destination | Cost | NextHop |
|---|---|---|
| B | 1 | B |
| C | 1 | C |
| D | 2 | C |
| E | 1 | E |
| F | 1 | F |
| G | 2 | F |

Bảng IV-3.Bảng định tuyến hoàn chỉnh ở nút A

Có hai tình huống khác nhau lúc một nút quyết định gửi bảng cập nhật routing đến hàng xóm của nó.

Cập nhật định kỳ: mỗi nút tự động gửi cập nhật sau một khoảng thời gian dù không có sự thay đổi, nó nhằm thông báo cho các nút khác là nó vẫn còn chạy, nó cũng đảm bảo rằng nó muốn lấy thông tin khác nếu người hàng xóm của nó bị hỏng.

Cập nhật phản ứng (triggered): xảy ra bất cứ lúc nào một nút nhận một cập nhật từ một người hàng xóm mà nó có sự thay đổi trong bảng routing.

Giả sử nút F phát hiện ra nút G sai. Đầu tiên F đặt khoảng cách mới tới G là không xác định và nó gởi thông tin này tới A, bởi vì A biết rằng nó có thể đi tới G 2 bước qua F , A cũng sẽ đặt khoảng cách tới G là không xác định, Tuy nhiên, với việc cập nhật kế tiếp từ , A sẽ học là C có thể đi 2 bước đến G. Thật vậy, A sẽ biết đến G với 3 bước qua C, nó sẽ cập nhật giá trị này vào bảng, lúc nó quảng cáo đến Khung, nút F sẽ học đến G 4 bước qua A. Để ngăn ngừa trường hợp này, ví dụ lúc liên kết từ A đến E bị hỏng, trong lần cập nhật tiếp theo, A quảng cáo một khoảng cách không xác định đến Ethernet, nhưng B và C quảng cáo 2 bước tới E. Dựa vào một khoảng thời gian, vấn đề có thể xảy ra, nút B nghe rằng nó có thể đến E hai bước từ C, vậy nó có thể đến Ethernet 3 bước và quảng cáo với A, nút kết luận rằng nó có thể đến E 4 bước và quảng cáo tới C ….vòng lặp này chỉ kết thúc khi khoảng cách tăng đến một số đủ lớn. Nghĩa là, không có nút nào thật sự biết E là nút không thể đến. Có một vài cách để giải quyết vấn đề này:

- Sử dụng một số nhỏ nhất để xác định khoảng cách, ví dụ chúng ta có thể quyết định số chặng lớn nhất qua một mạng nào đó sẽ không bao giờ lớn hơn 16.
- Split hozizon: lúc một nút gửi một routing cập nhật đến hàng xóm của nó, nó không gởi router mà nó học từ mỗi hàng xóm trở lại router đó. Ví dụ, nếu B có router(E,2,A) trong bảng của nó, và nó biết rằng nó học cái này từ router A, và vì vậy bất cứ lúc nào B gửi router cập nhật đến A, nó sẽ không gửi router(E,2). B thật sự gửi router đó về A, nhưng nó đặt một thông tin phủ nhận để đảm bảo rằng A không thể đến E từ B, ví dụ B gửi router(E, ) đến A.

| Thoâng tin löu trõõ ôû Nuùt | Khoaûng caùch ñeán caùc nuùt | | | | | | |
|---|---|---|---|---|---|---|---|
| | A | B | C | D | E | F | G |
| A | 0 | 1 | 1 | 2 | 1 | 1 | 2 |
| B | 1 | 0 | 1 | 2 | 2 | 2 | 3 |
| C | 1 | 1 | 0 | 1 | 2 | 2 | 2 |
| D | 2 | 3 | 1 | 0 | 3 | 2 | 1 |
| E | 1 | 2 | 2 | 3 | 0 | 2 | 3 |
| F | 1 | 2 | 2 | 2 | 2 | 0 | 1 |
| G | 2 | 3 | 2 | 1 | 3 | 1 | 0 |

Bảng IV-4.Khoảng cách hoàn chỉnh ở tất cả các nút

### 3. Định tuyến theo trạng thái kết nối-Link state(OSPF):

Thông đường theo trạng thái liên kết là một lớp thứ hai quan trọng của giao thức lộ trình. Mỗi nút cho rằng nó có khả năng tìm ra trạng thái liên kết với người hàng xóm của nó và chi phí của mỗi liên kết(chúng ta muốn cung cấp cho mỗi nút đầy đủ thông tin để có thể nó tìm ra một đường đi có chi phí nhỏ nhất đến bất cứ địa chỉ nào).

**Ý tưởng:**

Mỗi nút biết như thế nào để nối kết trực tiếp với hàng xóm của nó, và nếu chúng ta đảm bảo rằng toàn bộ những hiểu biết này được phổ biến đến tất cả các nút và rồi mỗi nút đủ kiến thức để xây dựng một sơ đồ mạng hoàn chỉnh. Đây rõ ràng là một điều kiện lý tưởng cho việc tìm đường đi ngắn nhất cho bất kỳ điểm nào trong mạng. Giao thức thông đường trạng thái liên kết dựa vào hai kỹ thuật chính:

- Đảm bảo sự phổ biến thông tin trạng thái liên kết.
- Tính toán đường đi từ tổng hợp tất cả các trạng thái liên kết mà nó biết.

**Reliable Flooding**

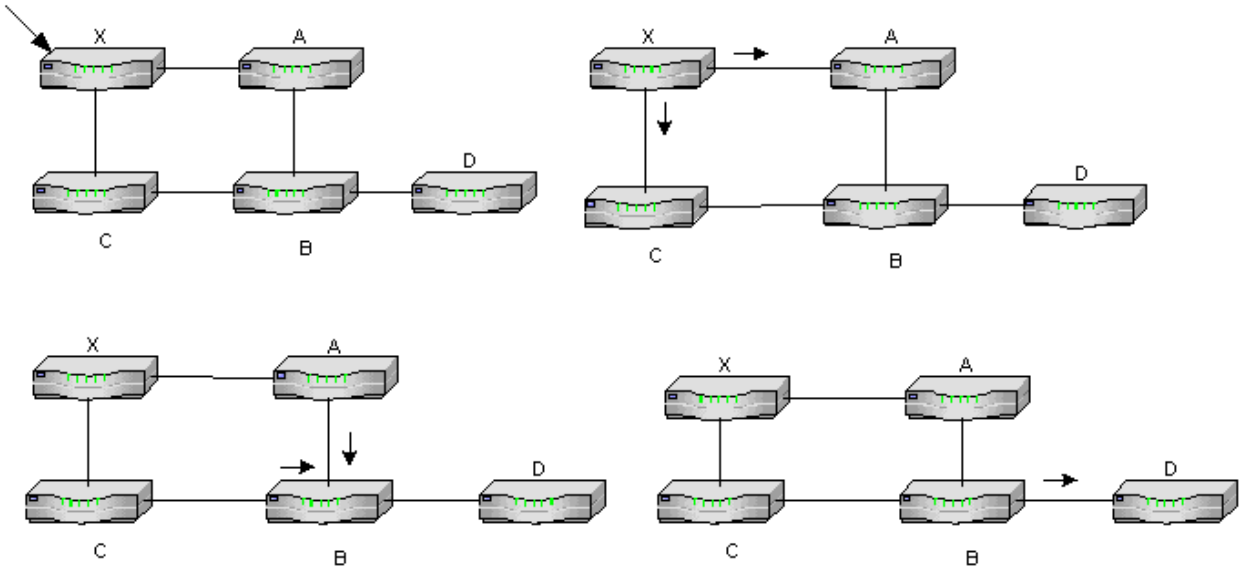
Đây là một quá trình nhằm đảm bảo tất cả các nút tham gia liên kết có một bản sao thông tin trạng thái liên kết từ tất cả các nút khác. "Flooding" có nghĩa rằng một nút gửi thông tin trạng thái liên kết ra tất cả các hàng xóm nối kết trực tiếp đến nó và mỗi nút nhận thông tin này tiếp tục chuyển ra tất cả các nút khác. Quá trình này tiếp tục cho tới khi chúng truyền thông tin đến toàn bộ mạng. Chính xác hơn, mỗi nút tạo một gói (LSP) chứa các thông tin sau:

- ID của nút tạo ra LSP
- Danh sách chi phí từ nó đến các hàng xóm nối kết trực tiếp.
- Một số thứ tự.

- Thời gian sống của gói.

Flooding làm việc theo cách sau:

Đầu tiên thực hiện truyền một LSP giữa các router nằm sát nhau(nó đảm bảo truyền bằng cách sử dụng cách thức truyền và hồi báo), tuy nhiên có nhiều bước cần đảm bảo flooding một LSP đến tất cả các nút trong mạng. Xem xét một nút X mà nó nhận bản sao của LSP từ host Y. X kiểm tra xem nó đã thật sự lưu trữ một bản sao LSP từ Y hay chưa, nếu chưa thì lưu trữ nó, ngược lại nó so sánh số thứ tự, nếu nó cho rằng bảng mới nhất thì nó thay thế cái củ, tiếp theo X gửi một bản sao LSP đó đến tất cả người hàng xóm ngoại trừ Y , và sau đó thông tin này sẽ đến tất cả các nút.




Hình IV-16. Flooding gói qua trạng thái liên kết.

Hình trên là một ví dụ chỉ ra một LSP bị flooding trong một mạng nhỏ.

Mỗi nút có thể sinh ra LSP theo hai cách:

- Theo một khoảng thời gian định sẳn,
- Thay đổi sơ đồ nối kết có thể là nguyên nhân một nút tạo ra một LSP mới(chỉ thực hiện khi có một nút mới tham gia nối kết hay một liên kết bị hỏng). Nó có thể phát hiện sự hỏng hóc bằng cách gửi một thông điệp thăm dò, nếu sau một khoảng thời gian không nhận được hồi báo nó xem như hàng xóm bị hỏng và tạo ra một LSP mới.

Một trong những mục tiêu thiết kế quan trọng của giao thức flooding là các thông tin mới nhất phải được flood đến tất cả các nút nhanh chóng, trong khi các thông tin cũ phải được di chuyển từ mạng và không cho phép lưu thông. Thêm vào đó nó giảm tổng phí giao thông trên mạng.

Một cách để làm giảm sự quá tải trên mạng là bằng cách tránh tạo ra LSP trừ khi thật sự cần thiết. Nó được thực hiện bằng cách gán một thời gian dài, thường là một vài giờ cho việc tạo ra một LSP mới.

Để đảm bảo rằng thông tin củ được thay thế bởi thông tin mới hơn, LSP mang một số thứ tự. Mỗi lần sinh ra một LSP mới, nó tăng số thứ tự lên 1, trường này tới 64 bit. Nếu một nút bị hỏng và nối kết lại nó gán số thứ tự này bằng 0. Nếu nút đó bị hỏng trong một thời gian dài, tất cả các LSP của nút sẽ bị xoá, ngược lại nếu nó nhận một bảng sao của chính nó với số thứ tự cao hơn, nó có thể gia tăng và sau đó sử dụng số thứ tự này.

LSP cũng mang một thời gian sống(time-to-live), nó dùng để đảm bảo rằng thông tin liên kết củ phải được di chuyển khỏi mạng. Một nút luôn luôn giảm TTL của một LSP mới nhận trước khi gửi nó cho tất cả các người hàng xóm.

**Tính toán đường đi**

Khi một nút có một bản sao của LSP từ các nút khác, nó có thể tạo ra một sơ đồ hoàn chỉnh của mạng và từ bảng đồ này nó có thể quyết định đường đi tốt nhất đến đích. Dựa vào thuật tóan Dijkstra, tưởng tượng rằng một nút lấy tất cả LSP mà nó nhận và xây dựng một đồ thị thể hiện đường đi trên mạng.

**Thuật toán:**

- N tập tất cả các nút trong đồ thị.
- l(i,j) chi phí cho cạnh(i,j)
- s chỉ nút hiện tại.
- C(n) chi phí đường đi từ s đến n
- M chỉ tập các nút
- Thuật toán tìm đường đi ngắn nhất:
  - M={s}
  - For each n in N-{s}

    C(n) = l(s,n)
  - While (N!=M)
    - M = M U {w} mà C(w) là giá trị nhỏ nhất trong tất cả w in (N-M)
    - For each n in (N-M)

      C(n) = MIN(C(n), C(w) + l(w,n))

Trong thực tế, mỗi chuyển mạch tính bảng table routing của nó từ các LSP, nó sử dụng thuật toán forward search. Mỗi chuyển mạch chứa hai danh sách

Tentative và Confirmed. Mỗi danh sách này chứa một tập các entry dạng <Destination, Cost, NextHop>. Thuật toán làm việc như sau:

1. Khởi tạo danh sách confirmed với một entry cho chính nó, với chi phí là 1.
2. Cho nút vừa thêm đến danh sách confirmed trong bước trước, gọi nút Next.
3. Cho mỗi hàng xóm của Next tính cost(chi phí) đến các hàng xóm này(bằng tổng chi phí từ chính nó đến Next và từ Next đến hàng xóm).
4. If hàng xóm hiện tại không có trong confirmed và tentative, thêm (Neighbor, Cost, NextHop) tới danh sách tentative
5. If hàng xóm hiện tại trên danh sách tentative, và chi phí hiện tại thấp hơn chi phí hiện tại, thay thế entry với (Neighbor, Cost, Nexthop).
6. If tentative rỗng, thì dừng lại, ngược lại lấy từ danh sách Tentative một entry chi phí thấp nhất và đặt nó vào danh sách Confirmed và chạy lại bước 2.

## IV.6. Định tuyến trên Internet

Do qui mô của mạng Intern là rất lớn, một nút không thể chứa tất cả các bản ghi cho mọi đích và việc cập nhật bảng dẫn đường tốn kém. Vì vậy mạng Internet được thành các hệ tự trị AS-Autonomous System, mỗi AS chứa nhiều mạng. Người quản trị mạng chịu trách nhiệm chọn giao thức định tuyến cho một AS bằng các giao thức định tuyến intra-AS (intra-AS routing protocol). Tiếp đó các gói dữ liệu được định tuyến giữa các AS khác nhau bằng giao thức định tuyến inter-AS (intra-AS routing protocol)

### 1. Intra-Autonomous System Routing protocol

Các giao thức tuyến intra-AS được dùng để cấu hình và duy trì các bảng định tuyến trong một hệ tự trị AS. Một khi có các bảng định tuyến này, các gói tin có thể tìm đường trong một hệ AS. Các giao thức này còn có tên gọi Interior Gateway Protocols (IGP).

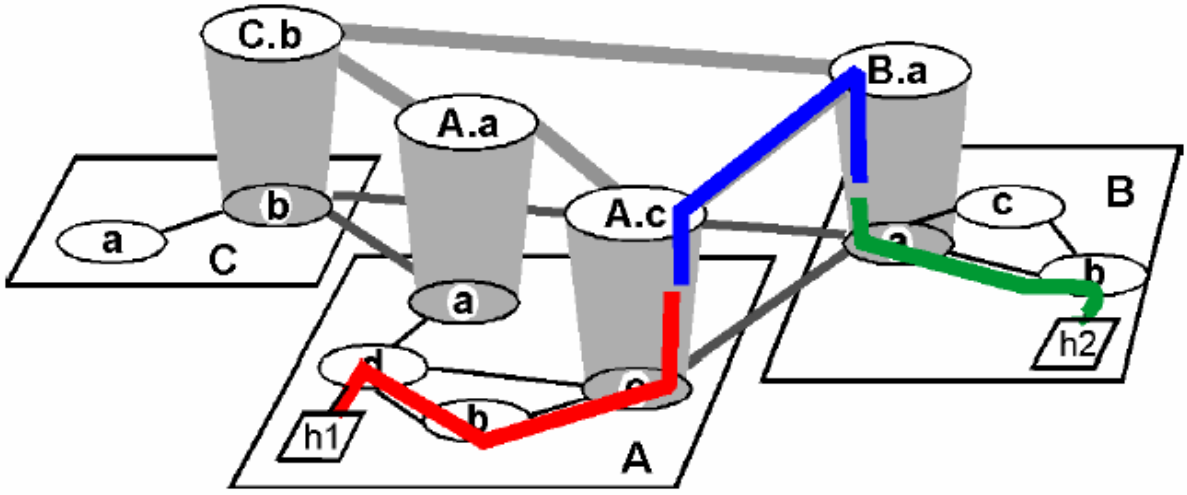
Một số giao thức định tuyến intra-AS:

- RIP: Routing Information Protocol
- OSPF: Open Shortest Path First
- IGRP: Interior Gateway Routing Protocol (của Cisco)

### 2. Inter-Autonomous System Routing protocol

Trong mỗi hệ tự trị, có các router đặc biệt gọi là **gateway router**.Các router này sử dụng intra-routing protocol với các router khác trong cùng AS và sử dụng inter-routing protocol với các gateway router của các AS khác. Một giao thức chuẩn phổ biến để định tuyến giữa các AS khác nhau là **Border Gateway Protocol-BGP**.

Mặc dù BGP trong các router có cách hoặc động tương tự theo kiểu giao thức giao thức định tuyến distance vector, nó có những đặc điểm như một giao thức vector chỉ đường (path vector protocol). Nguyên nhân là do BGP không thực hiệm việc quảng bá các thông tin về chi phí (như hop count,…) mà thực hiện quảng bá các thông tin về đường đi, ví dụ như tuần tự đường đi từ một AS này đến AS khác.

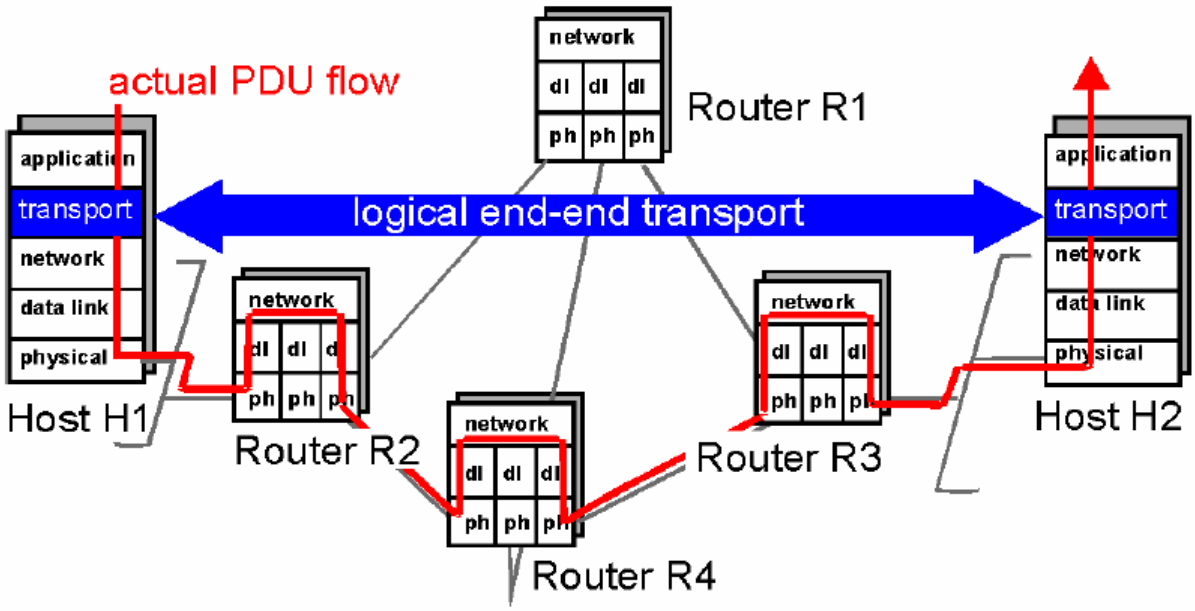



Hình IV-17. Định tuyến giữa các Autonomous System

# Chương V.Giao thức tầng giao vận

## V.1. Dịch vụ tầng vận chuyển

Tầng vận chuyển đóng vai trò quan trọng trong việc cung cấp các dịch vụ truyền thông trực tiếp đến các tiến trình ứng dụng tại các máy khác nhau. Các giao thức tầng ứng dụng cung cấp sự truyền thông logic (logical communication) giữa các tiến trình ứng dụng chạy ở các máy khác nhau. Truyền thông mức độ logic giữa các tiến trình ứng dụng có nghĩa là không kết nối về mặt vật lý (tại những vị trí khác nhau, kết nối thông qua nhiều router và các loại kết nối diện rộng khác,..). Các tiến trình sử dụng truyền thông logic được cung cấp bởi tầng vận chuyển để gửi thông điệp mà không cần quan tâm chi tiết đến hạ tầng vật lý bên dưới.




Hình V-1. Tầng vận chuyển cung cấp sự truyền thông logic

Các giao thức tầng vận chuyển được thực thi tại các trạm cuối (end system), không có tại các router. Tại phía gửi, tầng vận chuyển nhận thông điệp từ tầng ứng dụng, chia nhỏ và thêm vào các thông tin (header) của tầng mình và chuyển xuống tầng mạng bên dưới, nơi dữ liệu sẽ được đóng gói thành các gói tin. Tại nơi nhận, tầng vận chuyển nhận gói tin từ tầng mạng, loại bỏ các thông tin tầng vận chuyển (transport header), sắp xếp lại các thông điệp và chuyển cho các tiến trình ứng dụng bên trên.

Mô hình TCP/IP cung cấp hai giao thức tầng vận chuyển là UDP (User Datagram Protocol) và TCP (Transmission Control Protocol)

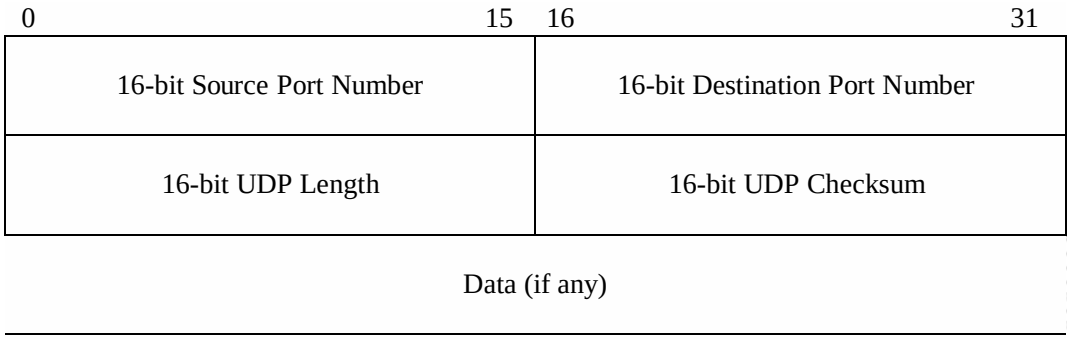
- UDP là giao thức không kết nối (connectionless) và không tin cậy (unreliable)
- TCP là giao thức hướng kết nối (connection-oriented) và tin cậy (reliable).

Khi thiết kế ứng dụng mạng, các nhà phát triển ứng dụng phải xác định rõ sử dụng UDP hay TCP.

## V.2. Giao thức không kết nối UDP

UDP-User Datagram Protocol cung cấp dịch vụ phi nối kết và không yêu cầu máy nhận thông báo rằng nó đã sẵn sàng cho việc nhận các thông điệp. Nó có thể mang dữ liệu ngay trong gói đầu tiên. Các ứng dụng sử dụng UDP thường quan tâm nhiều về tốc độ hơn là độ chính xác của dữ liệu.

**Port và Header**

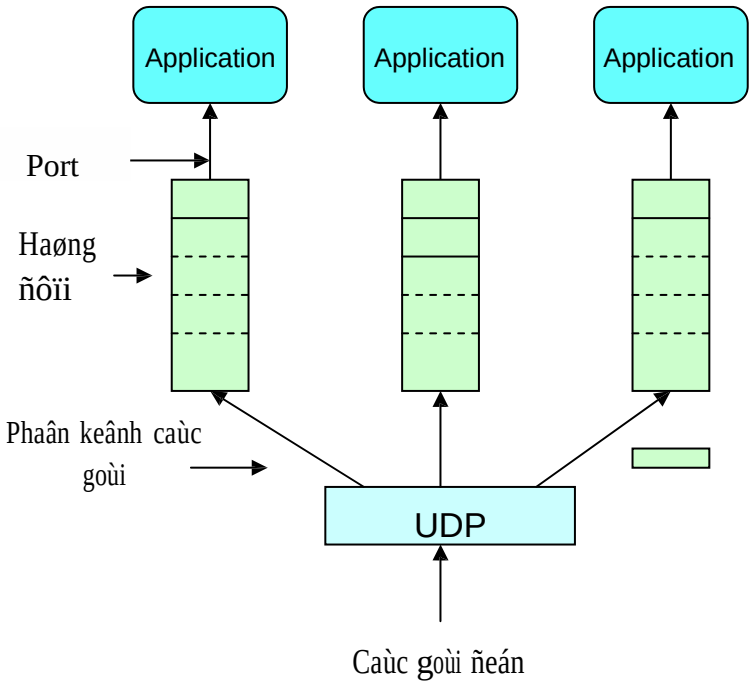



Hình V-2. Định dạng khung UDP

Một cách tiếp cận thông thường nhất(UDP) để trao đổi thông tin giữa các tiến trình ứng dụng là tiến trình xác định gián tiếp(không phải do OS gán) một ví trí ảo giữa hai tiến trình trên hai máy khác nhau để trao đổi thông tin, nó thường được gọi là port. Ý tưởng là máy gửi gửi thông tin qua một port và máy nhận nhận thông tin qua một port.

Để thực hiện chức năng phân kênh, mỗi header trong gói thông điệp của UDP chứa một định danh (port) của máy gửi và máy nhận. Trong hình minh hoạt định dạng khung UDP ở trên, mỗi port có giá trị 16 bit.

Vấn đề tiếp theo là như thế nào một tiến trình biết port mà nó muốn gửi 1 thông điệp. Một tiến trình client khởi tạo trao đổi thông tin với một tiến trình server, một khi liên lạc được với server, server có thể biết port của client và có thể đáp lại. Một số server nhận thông điệp ở một cổng cố định. Trong Internet, DNS(Domain Name Server)nhận thông điệp port 53 ở trên mỗi host.




Hình V-3. Hàng đợi thông điệp UDP

Minh họa trong hình trên, lúc một thông điệp được truyền đến, thông điệp được ở cuối hàng đợi. Nên khi hàng đợi đầy thông điệp sẽ bị loại bỏ. Không có kỹ thuật điều khiển luồn được sử dụng tại đây. Lúc một tiến trình ứng dụng muốn nhận một thông điệp nó lấy từ hàng đợi. Nếu hàng đợi rỗng tiến trình sẽ đợi cho đến khi thông điệp đến hàng đợi.

Mặc dù UDP không thực thi điều khiển luồn, đảm bảo phân phối, trật tự gói, nhưng nó cũng thực hiện kiểm tra lỗi khi truyền bằng cách sử dụng thuật toán checksum.

## V.3. Giao thức hướng kết nối TCP

Ngược lại với UDP, TCP-Transmission Control Protocol là một giao thức vận chuyển cung cấp dịch vụ tin cậy, connection-oriented, byte-stream.

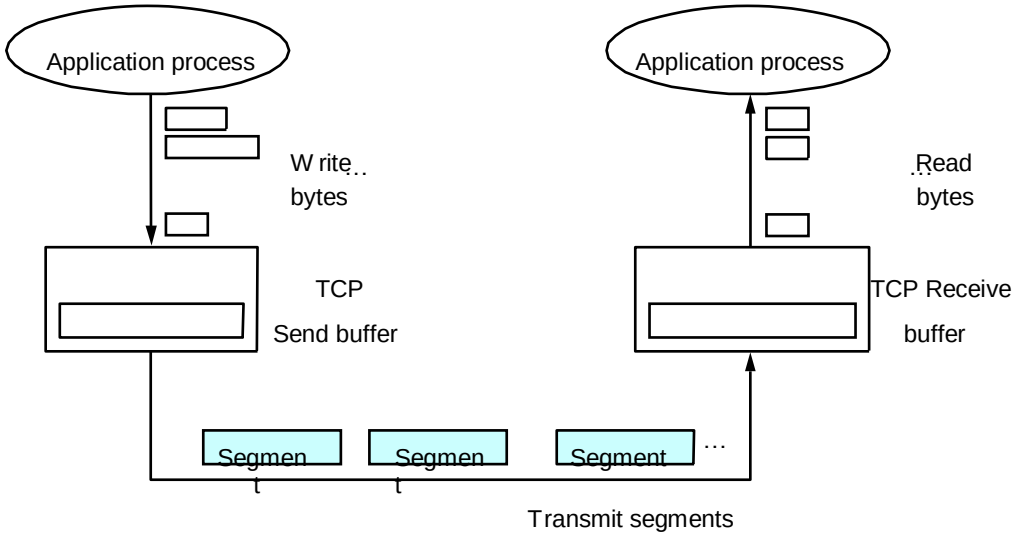
Dịch vụ này nâng cao hiệu quả của các ứng dụng bởi vì ứng dụng không cần lo lắng về lỗi hay thứ tự dữ liệu khi truyền. TCP có thể là một giao thức thỏa mãn tất cả những yêu cầu này.

- TCP là một giao thức full-duplex(có thể trao đổi thông tin hai chiều).
- TCP cũng gồm một kỹ thuật điều khiển luồn cho mỗi byte-stream mà nó cho phép máy nhận giới hạn dữ liệu máy gửi gửi trong một khoảng thời gian nào đó.

- TCP hỗ trợ kỹ thuật phân kênh mà nó cho phép nhiều chương trình ứng dụng trên bất kỳ máy có thể đồng thời trao đổi thông tin với các chương trình trên máy khác.
- TCP cũng thực hiện kỹ thuật điều khiển xung đột(không làm máy gửi quá tải máy nhận).

**1. Định dạng khung:**

TCP là một giao thức byte-oriented, điều này có nghĩa rằng máy gửi ghi các byte vào trong một nối kết TCP và máy nhận nhận được byte này từ nối kết TCP. Mặc dù "byte stream" được xem là dịch vụ TCP cung cấp cho các tiến trình ứng dụng. TCP không phải chính nó truyền các byte riêng biệt qua Internet, máy nguồn nhận các byte từ các tiến trình rồi tạo thành các gói có kích thước hợp lý, sau đó nó gửi các gói này đến đích. TCP của máy đích nhận các gói vào trong một buffer và tiến trình nới máy đích đọc các gói này lúc rảnh rỗi.



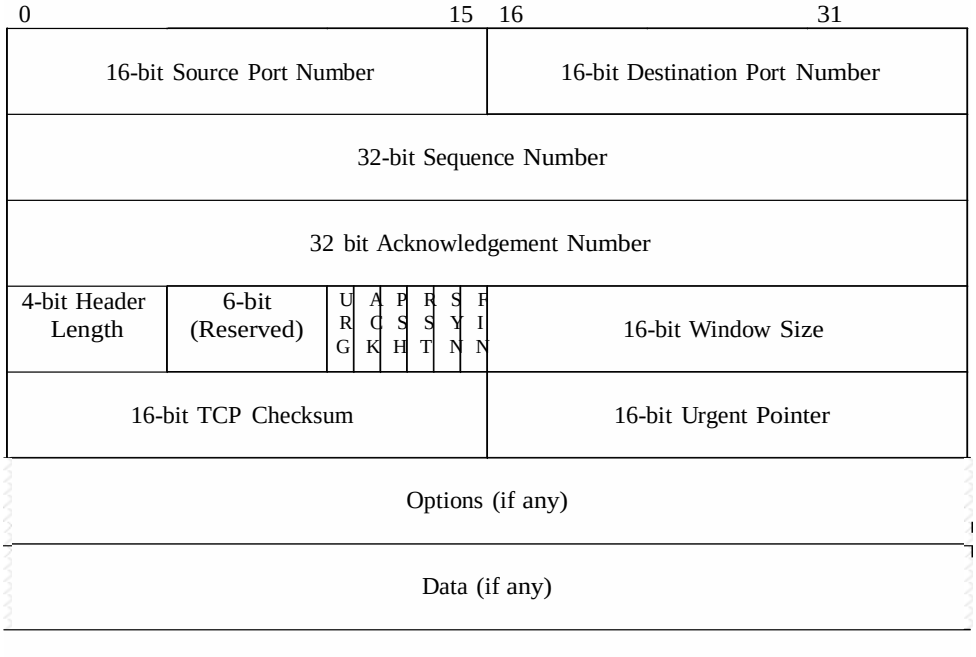

H

ình V-4. TCP quản lý một bit stream

Các gói được trao đổi giữa hai TCP được gọi là các đoạn, bởi vì mỗi đoạn mang một nhóm các byte. Câu hỏi đặt ra là như thế nào TCP quyết định đủ số byte để gửi vào trong một đoạn. TCP có 3 kỹ thuật để xây dựng truyền một đoạn:

- TCP chứa một biến maximum segment size(MSS) và nó gửi ngay một đoạn khi nó nhận đủ số byte từ các tiến trình.
- Các tiến trình yêu cầu thực hiện gửi.
- Sau một khoảng thời gian, nó sẽ gửi bất cứ đoạn đang có trong buffer.

Mỗi đoạn TCP chứa một header mô tả trong hình sau:



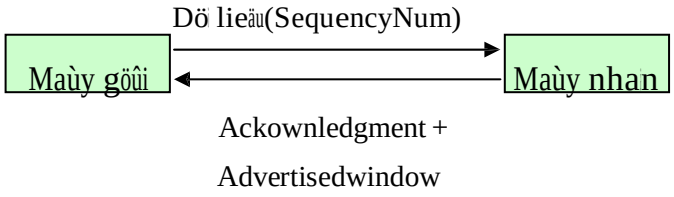

Hình V-5. Định dạng khung TCP

SrcPort và DstPort xác định port nguồn và port đích.

<SrcPort, SrcIPAddr, DstPort, DstIPAddr> xác định duy nhất cho một nối kết TCP.

Bởi vì TCP là một nối kết đến và đi, nó cho phép một nối kết giữa hai port được thiết lập, sử dụng để gửi và nhận dữ liệu và sau đó đóng lại và rồi một khoảng thời gian nào đó hai port như vậy khẩn cầu một nối kết thứ hai.

SequenceNum, Acknownledgment, AdvertiseWindow được sử dụng trong thuật toán cửa sổ trượt. Bởi vì TCP là một giao thức byte-oriented nên mỗi byte dữ liệu có một số thứ tự. Trường SequenceNum chứa số thứ tự của byte dữ liệu đầu tiên mang đoạn. Acknownledgment, AdvertiseWindow mang thông tin về dòng dữ liệu đi theo các hướng khác nhau.




Hình V-6. Minh họa đơn giản một tiến trình TCP

6 bit Flag thường được sử dụng để sắp đặt thông tin tin điều khiển giữa hai TCP. Nó bao gồm SYN, FIN, RESET, PUSH, URG, ACK.

- SYN và FIN dùng để thiết lập và kết thúc một nối kết.

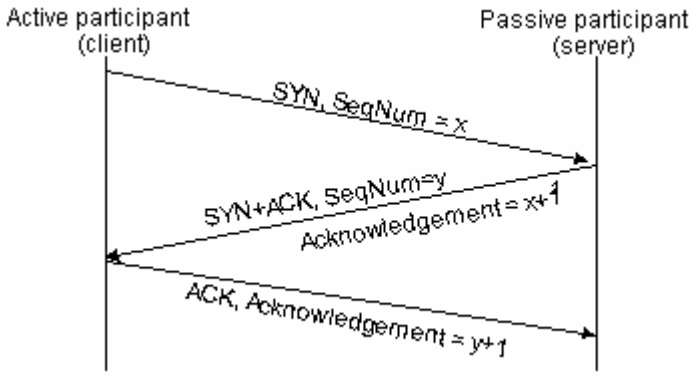
- ACK thiết lập để chỉ sự hồi báo.
- URG để chỉ đoạn chứa dữ liệu khẩn cấp.
- PUSH thiết bị gửi mong muốn một hoạt động push, nó muốn TCP máy nhận thông báo đến các tiến trình sự kiện này.
- RESET thiết bị nhận bị nhầm lẫn, ví dụ nó nhận một đoạn không mong đợi.
- CheckSum dùng để kiểm tra lỗi.

**2. Quá trình thiết lập và kết thúc kết nối:**

Một nối kết bắt đầu với một client thực hiện một hoạt động mở đến server. Cho rằng server chủ động mở nối kết trước, hai phía hứa hẹn với một thông điệp trao đổi để thiết lập nối kết. Chỉ sau khi giai đoạn thiết lập nối kết, hai phía mới bắt đầu gởi dữ liệu. Ngược lại, một khi không muốn trao đổi, nó đóng nối kết. Mỗi phía tự động đóng nối kết của mình.

**Thuật toán 3 cách bắt tay**

Thuật toán này bao gồm gửi 3 thông điệp giữa client và server. Minh họa trong hình sau:

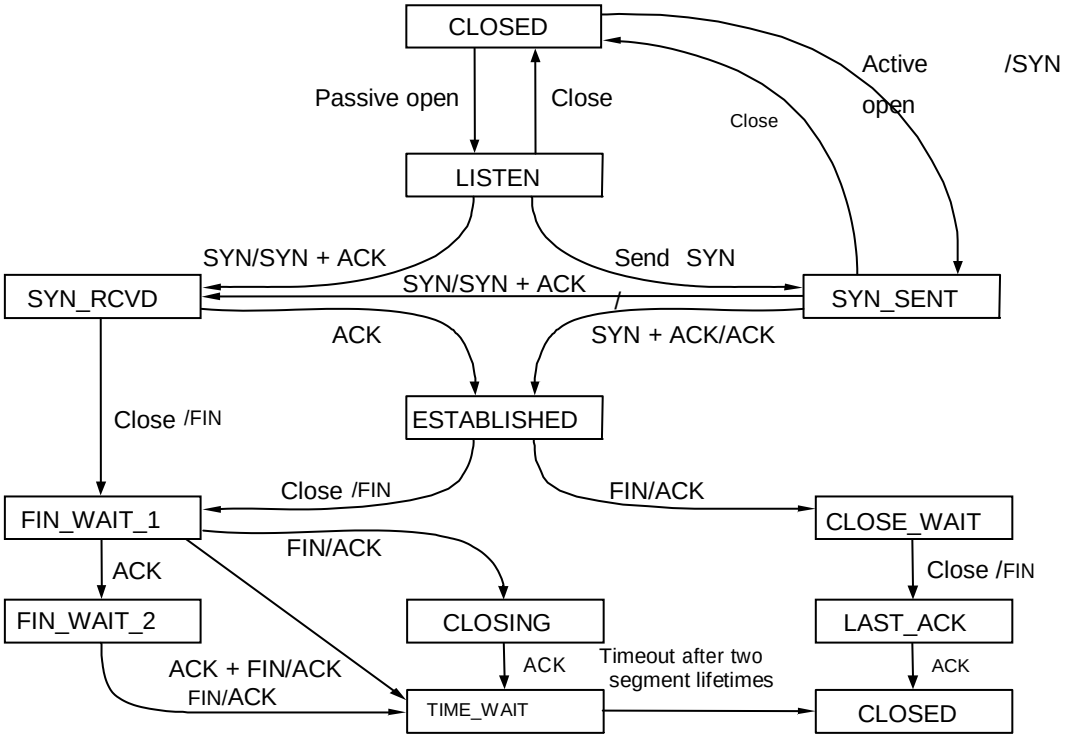



Hình V-7.Thuật toán ba cái bắt tay.

**Ý tưởng:**

Hai phía đồng ý nối kết trên một tập các thông số(tất cả các thông tin mà chúng muốn biết về nhau). Trong trường hợp mở nối kết, đầu tiên client gửi một thông điệp đến server với (flag = SYN, SequenceNum = x). Server đáp lại với một đoạn chứahồi báo(flag = ACK, ACK = x + 1) và trạng thái bắt đầu (flag = SYN, SequenceNum = y), Kết thúc client hồi báo với thông điệp (flag = ACK, ACK = y+1).

Lược đồ trạng thái chuyển tiếp:




Hình V-8. Hình lược đồ trạng thái chuyển tiếp.

Lược đồ này chỉ ra trạng thái yêu cầu để mở một nối kết và đóng một nối kết.

Có hai loại sự kiện gây ra trạng thái chuyển tiếp:

- Một đoạn đến từ TCP ngang hàng.
- Tiến trình ứng dụng cục bộ yêu cầu một hoạt động trên TCP.

Chú ý: Nếu một ACK từ client đến server bị mất(tương ứng với bước thứ ba của 3 cách bắt tay), nối kết vẫn thực hiện đúng. Bởi vì phía client đã thật sự ở trạng thái ESTABLISHED, vì vậy các tiến trình ứng dụng cục bộ có thể bắt đầu gởi dữ liệu. Mỗi đoạn dữ liệu này đặt cờ ACK, vì vậy server sẽ chuyển đến trạng thái ESTABLISHED lúc gói đầu tiên được nhận.

Tiến trình ứng dụng trên cả hai phía của nối kết phải tự đóng nữa nối kết. Nếu chỉ một phía đóng nối kết (có nghĩa là nó không còn dữ liệu để gửi) nhưng nó vẫn còn nhận dữ liệu từ phía kia.

Có ba khả năng xảy ra khi một phía đóng kết nối:

- Nó đóng trước phía kia:

  ESTABLISHED -> FIN_WAIT_1 -> FIN_WAIT_2 -> TIME_WAIT -> CLOSED

- Nó đóng sau phía kia:

ESTABLISHED ->CLOSE_WAIT -> LAST_ACK -> CLOSED.

- Hai phía cùng đóng

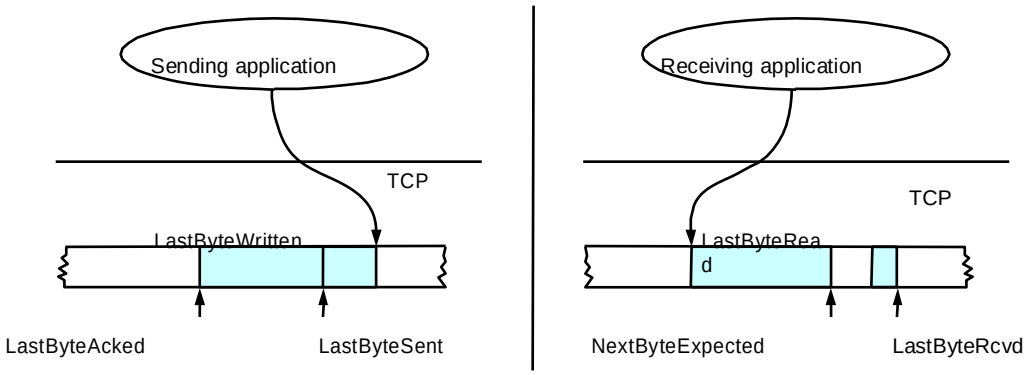
ESTABLISHED -> FIN_WAIT_1 -> CLOSING -> TIME_WAIT -> CLOSED.

**3. Điều khiển dòng truyền (Cửa sổ trượt):**

Mục đích của cửa sổ trượt:

- Đảm bảo phân phối dữ liệu tin cậy.
- Dữ liệu phân phối theo đúng trật tự
- Sử dụng điều khiển dòng giữa máy gửi và máy nhận.

Để có được kích thước cửa sổ thanh trượt cố định, máy nhận quảng cáo kích thước cửa sổ đến máy gửi. Nó được thực hiện bởi sử dụng trường AdvertiseWindow trong header TCP.




Hình V-9. Quan hệ giữa buffer gửi và buffer nhận.

**a) Phân phối tin cậy và thứ tự**

TCP bên phía gửi duy trì một buffer gửi. Buffer này được sử dụng lưu các dữ liệu đã gửi nhưng chưa có hồi báo, cũng như các dữ liệu được ghi bởi các ứng dụng nhưng chưa truyền. Bên phía nhận TCP duy trì một buffer nhận, buffer này lưu trữ dữ liệu đến thứ tự hay không thứ tự  mà các tiến trình ứng dụng chưa có cơ hội để đọc.

**b) Điều khiển luồng**

Trong giao thức cửa sổ trượt, kích thước của cửa sổ thiết lập dung lượng dữ liệu mà chúng có thể gửi mà không cần đợi hồi báo từ máy nhận. Thật vậy máy nhận có thể bóp nghẹt máy nhận bởi nó quảng cáo một cửa sổ mà nó lớn hơn dung lượng dữ liệu lưu trữ của buffer. Do đó kích thước cửa sổ trên máy nhận phải thỏa:

**LastByteRcvd - LastByteRead <= MaxRcvBuffer**

Để tránh quá tải trong buffer, nó phải quảng cáo kích thước cửa sổ:

**AdvertiseWindow = MaxRcvBuffer -( LastByteRcvd - LastByteRead)**

Nó thể hiện số không gian còn trống còn lại trong buffer.

TCP trên máy gửi lấy thông tin quảng cáo từ máy nhận. Nó phải đảm bảo rằng:

**LastByteSent - LastByteAcked <= AdvertisedWindow**

Máy gửi tính kích thước cửa sổ giới hạn dữ liệu gửi, phải đảm bảo:

**EffectiveWindow = AdvertisedWindow - (LastByteSent - LastByteAcked)**

Rõ ràng, EffectiveWindow phải lớn hơn không trước khi nguồn có thể gửi dữ liệu. Có khả năng, một đoạn đến hồi báo x byte, do đó cho phép máy gửi gia tăng LastByteAcked thêm x, nhưng bởi vì tiến trình tại các máy nhận không đọc bất kỳ dữ liệu, cửa sổ quảng cáo bây giờ giảm x byte so với thời gian trước. Trong trường hợp này, máy gửi có thể giải phóng buffer nhưng không tiếp tục gửi dữ liệu.

Máy gửi cũng đảm bảo rằng các tiến trình ứng dụng cục bộ không quá tải buffer gửi bằng cách giới hạn:

**LastByteWriten - LastByteAcked <= MaxSendBuffer.**

Nếu tiến trình gửi cố gắng viết y byte đến TCP nhưng

**LastByteWriten - LastByteAcked + y > MaxSendBuffer**

TCP sẽ khoá tiến trình gửi và không cho phép tạo ra dữ liệu.

## V.4. So sánh TCP và UDP

TCP là giao thức có liên kết, quản lý trạng thái liên kết và tin cậy. Tuy nhiên tốc độ truyền của TCP chậm hơn UDP vì phải có thời gian thiết lập, quản lý liên kết. Tùy vào yêu cầu cụ thể của ứng dụng mà sử dụng TCP hay UDP.

Một số các ứng dụng thực tế:

| **Ứng dụng** | **Giao thức ứng dụng** | **Giao thức vận chuyển** |
|---|---|---|
| Thư điện tử | SMTP | TCP |
| Truy cập từ xa | Telnet | TCP |
| Web | HTTP | TCP |
| Truyền File | FTP | TCP |
| Phân giải tên | DNS | thông thường là UDP |
| Giao thức định tuyến | RIP | thông thường là UDP |

# Chương VI. Giao thức tầng ứng dụng

## VI.1. Chức năng:

Chương trình ứng dụng (Applicationa) chạy trên các máy tính, trao đổi thông điệp (message) với các ứng dụng khác nhằm thực thi vai trò của ứng dụng. Khác với ứng dụng, **giao thức tầng ứng dụng (application-layer protocols)** là một thành phần của chương trình ứng dụng mạng, dùng để định nghĩa các quy tắc trao đổi thông điệp và giao tiếp với các dịch vụ được cung cấp bởi tầng dưới (chẳng hạn TCP hay UDP). Ví dụ như Web là một ứng dụng mạng cho phép người dùng lấy những "tài liệu" từ Web server theo yêu cầu. Ứng dụng Web gồm nhiều thành phần, bao gồm các chuẩn định dạng tài liệu (HTML,..), trình duyệt Web (Internet Explorer, Firefox,..), Web server (IIS, Apache,..) và một giao thức ứng dụng. Giao thức ứng dụng của web là HTTP (Hyper Text Transfer Protocol), định nghĩa thông điệp được truyền giữa Web server và trình duyệt như thế nào. Vì vậy HTTP chỉ là một thành phần của ứng dụng Web.

Giao thức tầng ứng dụng định nghĩa làm cách thức các tiến trình của ứng dụng trao đổi thông điệp với nhau.Cụ thể giao thức tầng ứng dụng định nghĩa:

- Các loại thông điệp cần trao đổi khác nhau, ví dụ như thông điệp yêu cầu (request message), thông điệp phản hồi (response message),…
- Cú pháp của các loại thông điệp, chẳng hạn các trường của thông điệp.
- Ý nghĩa của các trường.
- Các nguyên tắc quyến định lúc và cách thức gửi thông điệp yêu cầu hay phản hồi.

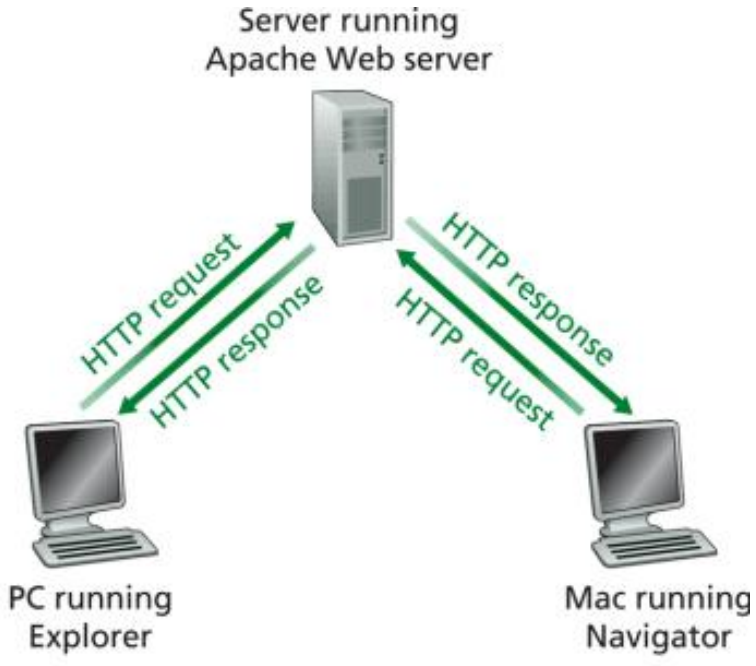
Các giao thức ứng dụng thường được đặc tả trong RFC và phổ biến rộng rãi. Tuy nhiên cũng có một số giao thức có bản quyền.

## VI.2. World Wide Web - HTTP

Hyper Text Transfer Protocol-Giao thức truyền siêu văn bản, sử dụng cho các dịch vụ truyền thông đa phương tiện WWW, dựa trên mô hình Client/Server. Dịch vụ WWW cho phép người sử dụng kết hợp văn bản, âm thanh, hình ảnh, hoạt hình tạo nên nguồn thông tin tư liệu. Đặc biệt ở đây là thông tin tư liệu trong WWW có dạng chủ yếu là HyperText-là dạng tư liệu chuẩn trong WWW. Về cơ bản đây là các file HTML-Hyper Text Markup Language.HTML sử dụng các thẻ (tag) để mô tả đối tượng chứa trong nó.Giao thức HTTP cho phép lấy và đọc nhanh các tài liệu này.

HTTP là giao thức truyền thông nhưng có thêm ưu điểm là thông tin tư liệu cần truy cập lại có chứa các liên kết với các đối tượng khác nằm khắp nơi trên mạng Internet. Phần mền cho Web server là chương trình điều khiển cho sự thu thập các tư liệu WWW trên một máy chủ. Để truy cập WWW cần phải có một trình duyệt (browser) chạy trên WWW client.

HTTP là giao thức Client/Server, được thiết kế để truyền các dạng dữ liệu siêu văn bản.Client yêu cầu truy cập web thông qua URL (URL request) và Server Gửi các đối tượng tới client thông quan phản hồi (response). HTTP là một giao thức không trạng thái, nghĩa là khi Server đáp ứng được yêu cầu dữ liệu của Client xong thì Server hủy bỏ kết nối đó để không tốn bộ nhớ cho sự kiện. Không trạng thái là yếu tố làm cho tốt độ truyền dẫn giữa Client và Server rất nhanh.

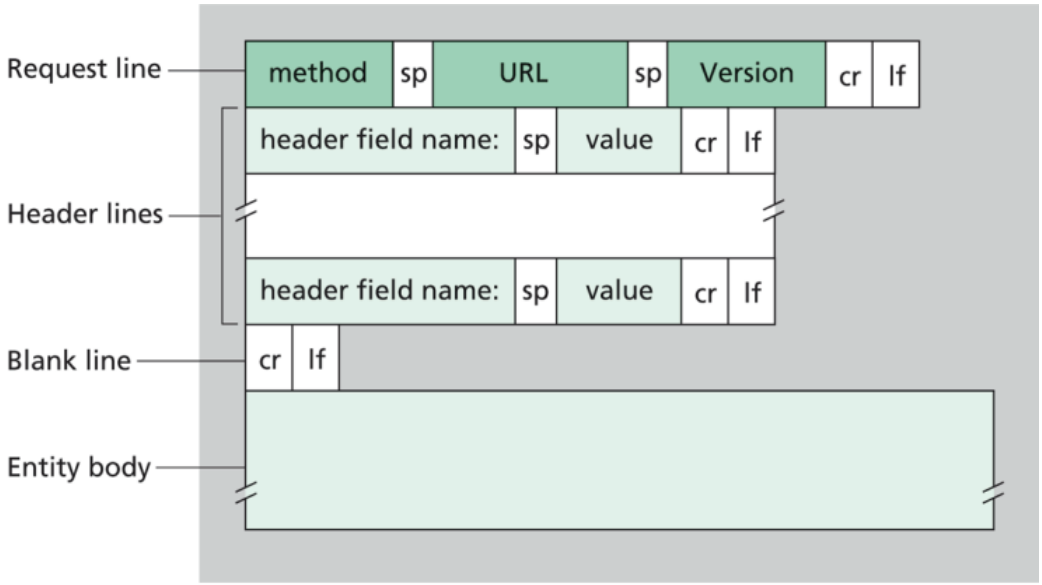



Hình VI-1. Mô hình hoạt động giao thức HTTP

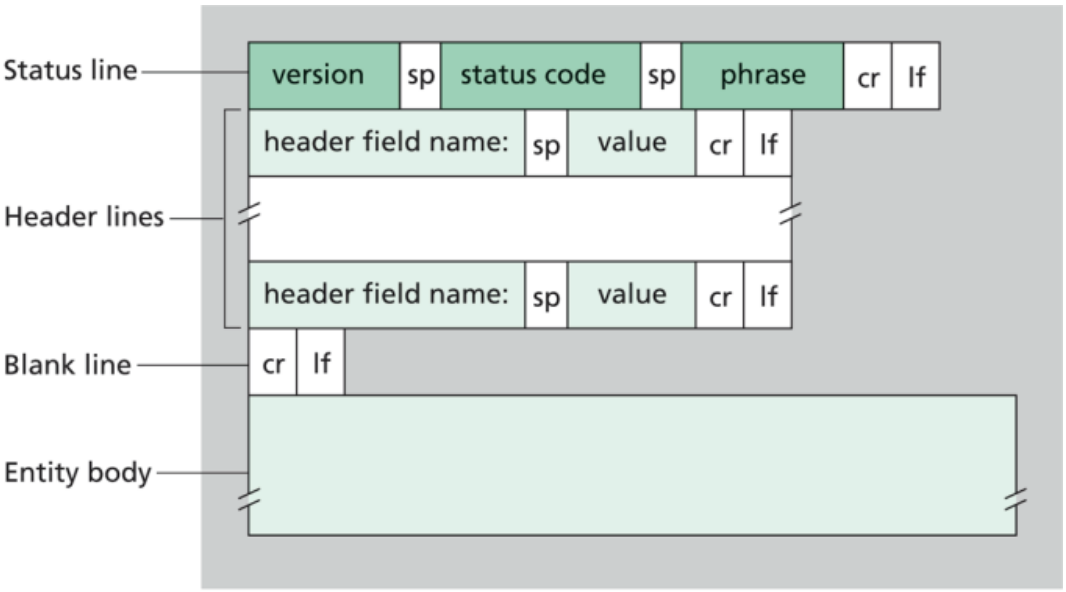
Các giai đoạn kết nối của HTTP:

- Mở kết nối: Client (browser) thiết lập liên kết tới web server (TCP connection) qua cổng 80 (mặc định). Server đồng ý kết nối (accept).
- Tạo yêu cầu: Client gửi thông điệp tới Server yêu cầu dịch vụ. Yêu cầu bao gồm các tiêu đề của HTTP, nó định nghĩa các phương thức được yêu cầu cho tác vụ và cung cấp thông tin về khả năng của Client (được theo sau dữ liệu gửi tới Server). Các phương thức HTTP điển hình là GET để nhận các đối tượng từ Server và POST để truyền dữ liệu cho đối tượng trên Server.

- Gửi đáp ứng: Server trả lời cho Client bao gồm các tiêu đề để trả lời mô tả trạng thái của các tác vụ (ví dụ thành công hay không thành công,..) theo sau dữ liệu thật sự.
- Ngắt kết nối.




Hình VI-2. Thông điệp HTTP Request




Hình VI-3. Thông điệp HTTP Response

Có hai kết nối HTTP:

- **Non-persistent HTTP**: Nhiều nhất là một đối tượng được truyền qua liên kết TCP (HTTP 1.0).

- **Persistent HTTP**: Cho phép nhiều đối tượng được truyền trên cùng một liên kết. Client phân tích, tìm ra và gửi yêu cầu tới tất cả các đối tượng ngay sau khi nhận được trang HTML ban đầu (base HTML).HTTP 1.1 sử dụng liên kết loại này ở chế độ mặc định.

## VI.3. Giao thức truyền File-FTP

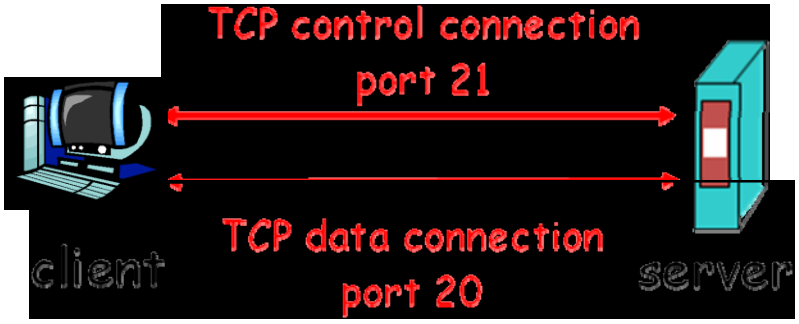
File Transfer Protocol-Giao thức truyền tập tin cho phép truyền tập tin giữa hai máy tính, quản lý các thư mục. FTP không được thiết kế để truy cập vào máy khác và chạy các chương trình ở máy đó. FTP giúp người sử dụng truy cập file và thư mục trên một máy chủ ở xa và thực hiện thao tác trên các thư mục như sau:

- Liệt kệ các file trên một thư mục cục bộ hay ở xa.
- Đổi tên và xóa tập tin (nếu có quyền).
- Tải các file về máy trạm hay truyền file đến máy ở xa (download/ upload).

FTP sử dụng đồng thời 2 liên kết TCP tại 2 cổng:

- TCP control connection, port 21: trao đổi các thông điệp điều khiển (commands, responses…).
- TCP data connection, port 20: truyền tải tệp.

Ngoài ra FTP lưu giữ trạng thái client trong phiên làm việc.




Hình VI-4. Mô hình hoạt động của FTP.

Quá trình trao đổi truyền tải:

- FTP server nghe tại cổng 21.
- FTP client yêu cầu kết nối với FTP server qua TCP tại cổng 21. Gửi user & password để đăng nhập.
- FTP server chấp nhận, liên kết điều khiển (control connection) được thiết lập. Quá trình trao đổi có thể bắt đầu.

- Khi server nhận được lệnh truyền tệp, nó mở liên kết dữ liệu (data connection) tới client, tệp được truyền qua liên kết này.
- Sau khi truyền xong một tệp, server ngắt liên kết dữ liệu (mỗi liên kết chỉ sử dụng để truyền một tệp).

## VI.4. Giao thức SMTP

Electronic Mail (viết tắt là e-Mail, thư điện tử) là một trong những dịch vụ thông tin phổ biến nhất trên Internet. Dịch vụ e-Mail giúp mọi người có thể trao đổi thông tin với nhau trên mạng Internet. Liên lạc bằng thư điện tử nhanh hơn, thuận tiện hơn và chi phí thấp hơn rất nhiều so với trao đổi thư từ qua đường bưu điện bình thường. Ngoài ra còn cho phép họ gởi cho nhau cả các loại tài liệu như : các văn bản, các báo cáo, các chương trình máy tính,… và nhiều thông tin khác.

Mỗi người sử dụng đều có một thư mục lưu trữ như trên máy server gọi là Mailbox. Tất cả các địa chỉ mail bao gồm hai phần được ngăn cách nhau bằng ký tự @ (ampersand). Tên miền có thể chia nhiều phần cách nhau bởi dấu chấm (.). Một địa chỉ Mail tiêu biểu có các phần như sau:

*Uername@ServerName.Type of Organization.Country*

Cấu trúc của một e-mail bao gồm các phần như sau:

- **Phần tiêu đề thư**

Phần này do các MTA (Messagn Transfer Agent) tạo ra và sử dụng, nó chứa các thông tin để chuyển nhận e-mail như địa chỉ của nơi nhận, địa chỉ của nơi gởi. Các hệ thống e-Mail cần những thông tin này để chuyển dữ liệu từ máy tính này sang máy tính khác. Cấu tạo phần này gồm nhiều trường (field), mỗi trường là một dòng văn bản ASCII chuẩn 7 bit như sau :<tên trường>:<nội dung của trường>.

Sau đây là một số trường thông tin thông dụng:

| Trường chức năng | Chức năng |
|---|---|
| DATE | Chỉ ngày giờ nhận mail |
| PROM | Chỉ địa chỉ người gởi |
| TO | Chỉ địa chỉ người nhận |
| CC | Chỉ địa chỉ những người nhận bản copy mail. Các người nhận thấy được địa chỉ của những người cùng nhận trong nhóm |
| BCC | Chỉ địa chỉ những người nhận bản sao chép của bức mail, nhưng từng người không biết những người nào sẽ nhận bức thư này. |

| | |
|---|---|
| REPLY-TO | Chứa cá thông tin để người nhận có thể nhận lại, thường nó chính là địa chỉ người gởi. |
| MESSAGE-ID | Định danh duy nhất, được sử dụng bởi hệ điều hành |
| SUBJECT | Chủ đề của nội dung thư |

Các trường trên là các trường chuẩn do giao thức SMTP quy định, ngoài ra trong phần header cũng có thể có thêm một số trường khác do chương trình e-Mail tạo ra nhằm quản lý các e-Mail riêng. Các trường này được bắt đầu ký tự X- và thông tin theo sau là cũng giống như ta thấy trên một trường chuẩn.

- **Phần nội dung**

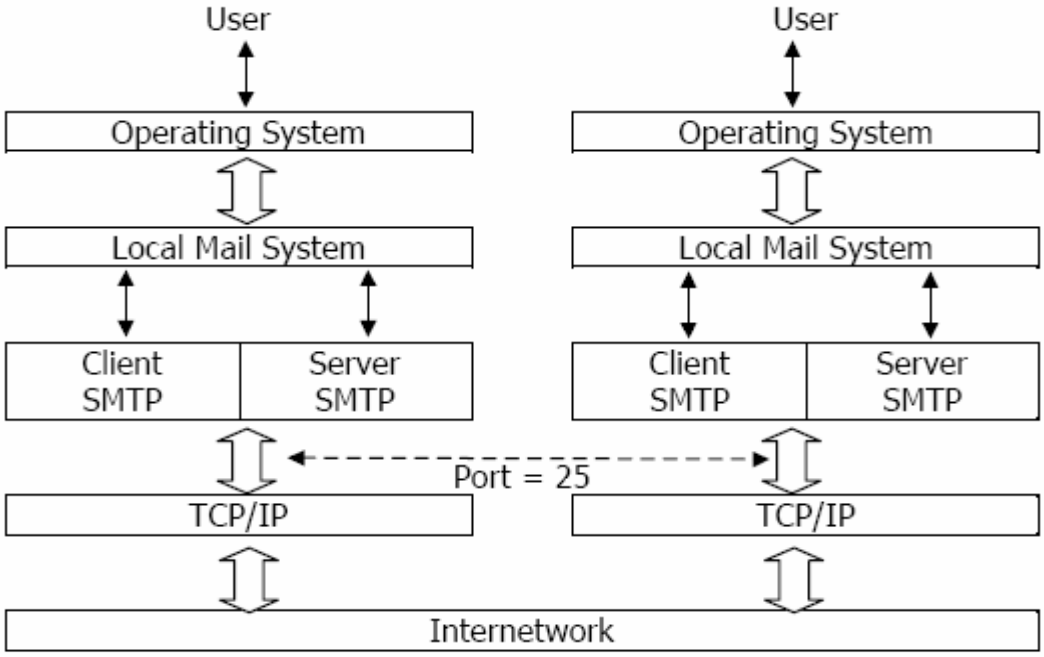
Để phân biệt phần tiêu đề và phần nội dung của e-mail, người ta quy ước ranh giới là một dòng trắng (chuỗi ký tự '\r\n'). kết thúc của dòng nội dung là chuỗi ký tự "\r\n.\r\n" .

Như vậy nội dung bức thư nằm trong khoảng giữa dòng trắng đầu tiên và ký tự kết thúc thư, và trong phần nội dung của bức thư không được phép tồn tại chuỗi ký tự kết thúc thư. Mặt khác do môi trường truyền thông là mạng Internet nên cá ký tự cấu thành phần thân của bức thư phải là các ký tự ASCII chuẩn.

### VI.4.1. Giao thức SMTP

SMTP (Simple Mail Transfer Protocol) là giao thức quy định về việc truyền mail chủ yếu dùng trong mạng Internet.

Mối quan hệ giữa SMTP và hệ thống Mail cục bộ như sau:




Hình VI-5. Quan hệ giữa SMTP và hệ thống Mail cục bộ.

Client liên quan đến thư đi, Server liên quan đến nhận thư. Hệ thống thư cục bộ hộp thư (mailbox) cho mỗi user. Mailbox có 2 phần: phần cục bộ và phần toàn cục.

Sau khi tháo bức thư trong khuôn dạng chuẩn, hệ thống mail cục bộ xác định tên người nhận ở hộp thư cục bộ hay phải gởi ra ngoài, để gởi bức thư Client SMTP phải biết địa chỉ IP của nơi nhận qua DNS và gởi qua cổng địa chỉ SMTP (25) để bắt đầu nối kết server SMTP nơi nhận. Khi mối nối đã được thiết lập, client bắt đầu chuyển thư đến Server bởi các lệnh của SMTP. SMTP dùng từ khóa như các lệnh để thực hiện thao tác chuyển giao mail. Một số lệnh chính của SMTP trong phiên việc giữa Client MTA và Server MTA như sau:

| **Lệnh** | **Tác dụng** |
|---|---|
| HELLO | Xưng danh với SMTP bên nhận, báo cho bện nhận biết bên gởi là ai. SMTP bên gởi gởi lệnh này đầu tiên cho SMTP bên nhận |
| MAIL | Khởi động một cuộc giao dịch mail mà mục đích cuối cùng là chuyển giao các mail tới một hay nhiều mailbox (nơi chứa mai nhận được) khác nhau. |
| RCPT | Nói rõ người nhận là ai |
| DATA | Các dòng lệnh DATA là dữ liệu của Mail. Đối với SMTP, chuỗi ký tự "CRLF.CRLF" báo nhận biết kết thúc nội dung bức mail. |
| RSET | Bỏ (Reset) cuộc giao dịch hiện tại. |
| NOOP | Yêu cấu SMTP bên nhận không làm gì ngoài việc trả về câu trả lời OK (dùng để kiểm tra). |
| QUIT | Yêu cầu SMTP nhận trả lời Ok và kết thúc phiên giao dịch hiện tại,=. |
| VRFY | Yêu cầu SMTP bên nhận kiểm tra người nhận là đúng, xác nhận các tham số gởi theo dòng kênh |
| SEND | Khởi động một cuộc giao dịch mà mail sẽ được gởi tới một hay nhiều thiết bị đầu cuối chứ không phải mailbox. |
| SOML | Khởi động một cuộc giao dịch mà mail sẽ được gởi tới một hay nhiều thiết bị đầu cuối hay mailbox. |
| SAML | Khởi động một cuộc giao dịch mà mail sẽ được gởi tới một hay nhiều thiết bị đầu cuối và mailbox |
| HELP | Yêu cầu SMTP bên nhận gởi thông tin giúp đỡ cho SMTP bên phát. |

| | |
|---|---|
| EXPN | Yêu cầu SMTP bên nhận gởi về danh sách những người nhận mail để có thể mở rộng việc chuyển mail cho các user khác. |
| TURN | Yêu cầu SMTP bên nhận gởi OK và đổi vai trò trở thành SMTP gởi. |

SMTP (trong RFC 821) ban đầu được thiết kế để cho phép các mail server chuyển đổi các mail message. Cơ chế chính được dùng để chuyển đổi các mail là phân đường các message quanh Internet. SMTP hoạt động trên mô hình lưu và truyền trong đó Client nắm các message cần để truyền đến server và gởi các lệnh đến server để báo cho server cách sử lý các message. Mail Client có thể là một mail server khác, nó có một hay nhiều các message phải truyền đến một server khác. Hầu hết các Internet Mail Client sử dụng SMTP để gởi message.

### *1. Quy tắc làm việc với SMTP*

1. Mỗi lệnh câu phân cách tham số theo sau bằng khoảng trắng và kết thúc bằng ký tựu CRLF. Mail đi từ SMTP gởi đến SMTP nhận và đến lượt SMTP nhận trở thành SMTP gởi để gởi mai đi tiếp cho đến khi chúng được giao vào Mailbox của người nhận.
2. Các lệnh SMTP phải diễn ra một cách tuần tự.
3. Việc đánh địa chỉ phải theo cách đánh địa chỉ của Internet

Giao thức SMTP quy định các Server MTA (ở đây SMTP bên phải) phải gởi tín hiệu phản hồi ACK sau mỗi lệnh mà nó nhận được từ Client MTA. Mỗi câu trả lời bên nhận đều mở đầu với một mã số theo sau mới là thông tin dạng text. Mỗi số mở đầu trong mã số có ý nghĩa khác nhau, nó chỉ ra rằng kết quả thực hiện thao tác là tốt (số 2) , thất bại (số 5), hay chưa hoàn thành (số 3).

### *2. Một số mã phản hồi thông dụng của SMTP*

220 Dịch vụ đã sẵn sàng

221 Đóng kết nối đã được sẵn sàng

250 Thao tác do Client MTA yêu cầu đã được hoàn thành.

234 Sẵn sàng nhận nội dung của mail

555 Thao tác yêu cầu không thực hiện được do không có Mailbox trên máy….

### *3. Phiên giao dịch SMTP*

Để hiểu cách dùng một số lệnh chúng ta xem xét qua ví dụ sau: bên gởi tên aa ở máy Samplel muốn gởi cho bb, cc ở máy Sample2, giả sử cc không có Mailbox tại Simple 2.

Bên gởi thực hiện một kết nối SMTP Server.

RECEIVER: 220 sample2 Simple mail Transfer Server ready

Khi được kết nối qua giao thức TCP/IP, máy nhận trả lời với mã 220 để báo cho máy gởi biết dịch vụ SMTP đã sẵn sàng.

SENDER: HELO sample1

Bên nhận đã sẵn sàng, bên gởi gởi HELLO và xưng tân người gởi.

RECEIVER: 250 sample2

trả với mã 250 báo cho biết bên nhận đã sẵn sàng.

SENDER: MAIL FROM:<>

Bên gởi dung lệnh MAIL để khởi động phiên giao dịch. Cú pháp trên cho bên nhận biết địa chỉ bên gởi (mailbox của bên gởi) để bên nhận thông báo lỗi nếu có về bên gởi.

RECEIVER: 250 OK

Trả lời với mã 250 cho biết đã chấp nhận.

SENDER: RCPT TO:<>

Bên gởi cho biết e-Mail đích.

RECEIVER: 250 OK

Trả lời với mã 250 cho biết đã chấp nhận.

SENDER: RCPT TO:<>

Muốn gởi bao nhiêu người dùng bấy nhiêu lệnh RCPT kèm theo địa chỉ nhận, nếu đúng sẽ trả lời về về mã 250 kèm theo OK

RECEIVER: 550 No such user here

Báo kèm theo mã 550 cho biết không có mailbox trên địa chỉ trên đối với người nhận.

SENDER: DATA

Báo cho bên nhận biết dữ liệu bắt đầu từ sau từ DATA.

RECEIVER: 354 Start mail input;end with <CRLF>,<CRLF>

Mã 354 báo cho biết đã sẵn sàng nhận mail, kết thúc mail với ký tự “CRLF,CRLF”

SENDER: bắt đầu thân của mail

SENDER: …

SENDER: (đến khi kết thúc gởi CRLF,CRLF)

RECEIVER: 250 OK

E-mail đã được chấp nhận.

SENDER: QUIT

Phát lệnh báo kết thúc phiên giao dịch

RECEIVER: 221 sample2 Server closing transmission chênnl

Mã 221 đóng kết nối đã thiết lập.

### *4. Giao thức mở rộng ESMTP*

SMTP có một hạn chế gây khó khăn trong việc truyền nhận mail là giới hạn tối đa kích thước nội dung một bức mail chỉ là 128KB. Do đó người ta đã cải tiến chuẩn SMTP thành một chuẩn mở rộng mới gọi là ESMTP, cho phép tăng giới hạn kích thước của mail lên 1MB.

Để xem xét Server MTA có theo chuẩn ESMTP hay không, thay vì dùng lệnh HELO ở đầu một cuộc giao dịch, Client MTA dùng lệnh mới EHLO, nếu Server thay thế chuẩn SMTP ở đa số các hệ thống

Chẳng hạnh để khởi động cuộc giao dịch với kích thước mail lên tới 1MB, sử dụng dòng lệnh sau:

MAIL FROM:<aa@sample1>SIZE=1000000

### VI.4.2. MIME

Từ khi MIME (Multipurpose Internet Mail Extention) được đưa ra, kiểu dữ liệu mà người dùng có thể gởi thông qua e-Mail được mở rộng. Ban đầu dữ liệu chỉ ở dạng text. Ngày nay, ta có thể gởi các tài liệu (file *.doc), cá file ảnh hay file âm thanh.

Để có thể phân phát các kiểu dữ liệu này, khuôn dạng các message trên Internet nên được mở rộng . MIME được phát triển cho mục đích này.

#### 1. *Cấu trúc message của MIME*

MIME không phải cho các ứng dung e-Mail mới, nhưng cho phép mở rộng khả năng e-Mail trên Internet trong khi vẫn dữ các ứng dụng giao vận và nền tảng hiện tại. Khuôn dạng MIME duy trì các cấu trúc message cơ bản với các phần Header và phần body (tham khảo RFC 822). Ví dụ về khuôn dạng của một tài liệu MIME như sau:

{Dòng này xác định MIME message}

MINE-Version:1.0

To:

Subject:Book CD

{Dòng này xác định đây là kiểu message hỗn hợp và các phần được phân tách nhau bởi đầu biên}

Content-Type: multipart/mixed;boundary=”---------6B9767D111AE”

X-Mozilla-Status: 0001

{Kết thúc phần header}

{Biên đầu tiên, thể hiện phần đầu của message}

----6B9767D111AE

{Đây là đoạn text, thể hiện các ký tự dạng US-ASCII}

Content-Type: text/plain;charset=us-ascii

Content-Transfer-Encoding:7bit

{Kết thúc phần header}

Davis,

I am----------

Thanks,

Davis

{phần sau là phần đánh dấu biên}

----------6B767D111AE

Content-Type: application/octet-stream

Content-Transfer –Encoding:base64

Content-Disposision:attachment;filename=”Sublic2.doc”

{Phần dưới đây là nội dung file}

0M8……

{Phần sau đây là biên kết thúc file}

--------6B767D111AE

### 2. *MIME version header*

MIME version header định dạng một message như một message MIME, và xác định server của MIME chuẩn để dịch message. Nếu không tìm thấy header, client sẽ đối xử với message theo khuôn dạng chuẩn trong RFC. Phiên bản hiện tại của MINM là 1.0. cú pháp MIME header version như sau:

MIME-Version: 1.0

- **Content Type header**

Content Type header xác định khuôn dạng file được gắn vào một đối tượng. Header báo cho MIME cách hiển thị hay thao tác trên thân của message. Content Type Header bao gồm tên của header, theo sau bởi MIME. Kiểu MIME theo sau hai tên và được cách biệt nhau bởi ký tự slash (/). Tên đầu tiên là tên kiểu và tên thứ 2 là tên phụ. Sau đây là các ví dụ của Content type header;

Content-Type: image/jpeg

Content-Type: image/gif

Content-Type: image/bup

Content-Type: image/mpeg

Content-Type: applicatipn/octet-stream

Ba ví dụ đầu tiên trong phần này, đối tượng là kiểu ảnh (cũng là kiểu nhị phân), kiểu con của nó là jpeg, gif, và bmp. Các file ảnh này được nhúng vào trong các message. Dòng thứ tư trong các ví dụ này đó là một file chương trình.

Các kiểu và kiểu con có thể được thiết lập bởi các tham số. Mỗi tham số bao gồm một tên tham số, theo sau bởi dấu bằng (=) và tiếp theo là giá trị tham số. Các tham số được tách biệt giữa kiểu và kiểu con, cũng như các tham số khác và được tách biệt nhau bằng dấu chấm phẩy. Ví dụ sau đây thể hiện một tập các tham số:

Content-Type: text/plain;charset=us-ascii

Kiểu đối tượng này báo cho người đọc message rằng các phần đi sau là dạng text và sử dụng các ký tự theo kiểu text.

Header này có thể hoàn toàn tùy chon. Nếu nó không được cung cấp thì message được đối xử như một chuỗi các ký tự ASCII.

- **Content Transfer Encoding Header**

Content transfer Encoding Header xác định mô hình mã hóa được sử dụng để nhúng đối tượng vào trong thân của message. Để nhúng một đối tượng nhị phân vào trong một thư điện tử, cần phải chuyển nó sang dạng ASCII, do vậy nó được biên dịch theo khuôn dạng RFC 822. Ví dụ một cú pháp header để mã hóa nội dung khi chuyển là Content-Transfer-Encoding Base64.

Tài liệu MIME định nghĩa 5 kiểu mã hóa, nhưng 3 kiểu mã hóa thể hiện đối tượng không được mã hóa. Mã hóa 7 bit thường được dùng cho các vùng text theo khuôn dạng MIME. Hai kiểu kia mã hóa theo kiểu 8 bit và nhị phân, chỉ được sử dụng khi chuyển thư không phải SMTP, do SMTP chỉ cho phép các ký tự ASCII theo kiểu mã hóa 7 bit. Hai mô hình mã hóa còn lại đó là quoted-printable và base65 để chuyển các đối tượng từ dạng nhị phân sang kiểu ASCII.

### 3. *Cấu trúc message MIME đa phần*

Một số các khả năng phổ biến của MINE đó là có một message đa phần. Bằng cách sử dụng message đa phần, ta có thể nhúng cả hình ảnh và âm thanh vào các message text hay xay dựng một ứng dụng về một đối tượng hoạt hình, nó bao gồm một số file cần thiết để chạy ứng dụng.

Cấu trúc message đa phần gồm nhiều message kết hợp vào trong thân của một message, mỗi message với thông tin header của nó thể hiện kiểu nội dung mà mô hình mã hóa. Các phần này được tách biệt bởi các dấu biên mà message chính định ra. Để hiểu chi tiết về cấu trúc của một message đa phần, xem RFC 1521.

### 4. *Mã hóa BASE64*

Thuật toán mã hóa Base64 được thiết kế để mô tả một chuỗi tùy ý các giá trị 8 bit mà con người không có khả năng đọc được thành các ký tự ASCII. Thuật toán mã hóa và giải mã đơn giản nhưng dữ liệu mã hóa sẽ lớn hơn dữ liệu nguồn 33%.

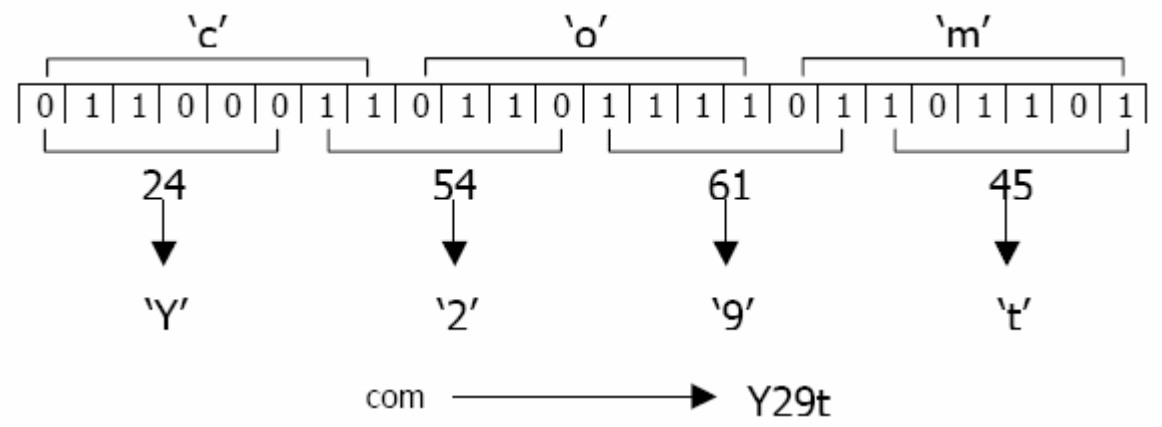
Một tập 65 ký tự AS-ASCII được dùng,cho phép 6 bit biểu diễn cho các ký tự có thể in được. (Ký tự 65, "=", là một ký tự sử lsy đặc biệt)

Tiến trình mã hóa biểu diễn nhóm 24 bít dữ liệu thành 4 ký tự mã hóa ở đầu ra. Tiến trình thực hiện từ trái sang phải, một nhóm 24 bit nhập được kết hợp từ nhóm 3 ký tự 8 bit. 24 bit đó được chia thành 4 ký tự 6 bit, mỗi nhóm được dịch thành một ký tự đơn dựa vào bảng mã Base64.

**Bảng mã Base64**

| Value | Encoding | Value | Encoding | Value | Encoding | Value | Encoding |
|---|---|---|---|---|---|---|---|
| 0 | A | 17 | R | 34 | i | 51 | Z |
| 1 | B | 18 | S | 35 | j | 52 | 0 |
| 2 | C | 19 | T | 36 | k | 53 | 1 |
| 3 | D | 20 | U | 37 | l | 54 | 2 |
| 4 | E | 21 | V | 38 | m | 55 | 3 |
| 5 | F | 22 | W | 39 | n | 56 | 4 |
| 6 | G | 23 | X | 40 | o | 57 | 5 |
| 7 | H | 24 | Y | 41 | p | 58 | 6 |
| 8 | I | 25 | Z | 42 | q | 59 | 7 |
| 9 | J | 26 | a | 43 | r | 60 | 8 |
| 10 | K | 27 | b | 44 | s | 61 | 9 |
| 11 | L | 28 | c | 45 | t | 62 | + |
| 12 | M | 29 | d | 46 | u | 63 | / |
| 13 | N | 30 | e | 47 | v | | |
| 14 | O | 31 | f | 48 | w | | |
| 15 | P | 32 | g | 49 | x | | |
| 16 | Q | 33 | h | 50 | y | | |

Ví dụ mô tả tiến trình mã hóa 3 ký tự nhập là "com":




Luồng dữ liệu được mã hóa đầu ra phải được biểu diễn bằng cá dòng có độ dài không lớn hơn 76 ký tự. Tất cả các ký tự xuống dòng hay các ký tự khác không có trong bảng mã Base64 đều được phần mềm giải mã bỏ qua.

Khi nhóm bit dòng nhập ít hơn 24 bít ( nghĩa là đến cuối của dữ liệu cần mã hóa) thì cần có xử lý đặc biệt. Khi có ít hơn 24bít dòng nhập thì các bits 0 được thêm vào phía bên phải nhóm bit để được đủ số 42 bít. Khi dòng nhập đã dủ 24 bít thì có các khả năng có thể xảy ra:

1. Phần cuối cùng của dữ liệu cần được mã hóa là 23 bít thì dữ liệu đầu ra cuối cùng sẽ là 4 ký tự đã mã hóa mà không có ký tự đệm"=".
2. Phần cuối cũng của dữ liệu cần mã hóa chính xác là 8 bít thì dữ liệu đầu ra cuối cùng sẽ là 2 ký tự đã mã hóa kèm theo 2 ký tự đệm "=" ở cuối.

Nếu phần cuối cùng của dữ liệu cần mã hóa chính xác là 16bít thì dữ liệu đầu ra cuối cùng sẽ gồm 3 ký tự đã mã hóa kèn theo với một ký tự đệm "=" ở cuối.

Bởi vì các ký tự đệm chỉ được thêm vào cuối của dữ liệu nên khi gặp bất kỳ một ký tự "=" nào thì hiển nhiên đã đến vị trí kết thúc của dữ liệu.

## VI.5. Các giao thức nhận mail:

### VI.5.1. Giao thức POP:

Người sử dụng có thể gởi thư bằng cách sử dụng SMTP, và có thể nhúng bất kỳ đối tượng nào vào trong message thông qua việc sử dụng khuôn mạng dạng MINE. Tuy nhiên, với SMTP, server để nhận được các message thư phải nối đến client và gởi tất cả các measage được phân phát cho client. Do đó, người sử dụng phải đăng ký tên máy dưới dạng tên địa chỉ Internet của người nhận.

SMTP được thiết kế trong trường hợp nhiều user sử dụng tất cả thời gian của họ kết nối đến một vài host và chạy một phiên đầu cuối. Giao thức không được thiết kế cho các tình huống thông dụng hiện nay, trong đó, hầu hết tất cả các user sử dụng e-mail kết nối hạn chế đến mail server đang giữ hộp thư. Người sử dụng

phải duy trì các message thư trên server và chuyển nó đến cho client khi client yêu cầu. Đây là mục đích trong thiết kế của POP.

POP (Post Office Protocol) được thiết kế bù đắp cho SMTP trong phần nhận các message. Những người thiết kế POP không gộp các chức năng gởi message và cho rằng SMTP tiếp tục được sử dụng để thực hiện các chức năng đó. Với giao thức POP, máy tính nhận được khởi tạo kết nối. Máy nhận kết nối đến mail server, login và nhận bất kỳ một mesage nào đang chờ. Do vậy máy gởi không cần biết gì về máy nhận trừ khi nó sử dụng login và password để dăng nhập. Ngày nay, hầu hết tất cả các mail client trên Internet mà bạn có thể sử dụng để kết hợp cả SMTP và POP.

### *1. Mô hình thông tin POP*

Trong mô hình lưu và phát, server mail cục bộ lưu các message đến khi các client nhận nó. POP client kết nối với server 110 của TCP. Để đăc nhập vào server, user sử dụng định danh (ID) và password. Sau khi đăng nhập thành công vào server, client có thể yêu server về các message mới đang sẵn sàng, lấy bất kỳ message nào mà server đang gởi hay đang xóa đi một message nào đó trên server.

Mô hình thông tin POP sử dụng 3 trạng thái giao tác để cung cấp chức năng này đến POP client:

- Trạng thái đặc quyền: Server kiểm tra quyền truy nhập của client (ID và password).
- Trạng thái giao tác: Client có thể nhận hay xóa message.
- Trạng thái cập nhập : Trạng thái này được chuyển đến ngay sau khi client tạo ra lệnh quit.

Trạng thái cập nhật là trạng thái cho pháp thao tác trên message. Khi client đang ở trên trạng thái giao tác, bạn có thể tạo ra lệnh reset để hủy bỏ tất cả các thao tác xóa trước đó (undo).

### *2. Chuẩn POP3*

Giao thức POP3 được cải biên từ giao thức POP. Nhiệm vụ của giao thức POP3 là lấy từ mailbox về khi nào người nhận muốn

Đặc điểm của hệ thống dùng POP là cho phép người sử dụng login vào POP server và nhận các mailbox của mình mà không cần phải login vào mạng mặc dù các mailbox thường nằm ở các Mail Server nằm trong mạng (thông thường muốn thâm nhập mạng ta phải có một account trên mạng và phải cung cấp password khi đăng nhập vào mạng). Người sử dụng có thể truy nhập POP Server bất cứ hệ thống nào trên mạng Interrnet, từ bất cứ UA nào dùng giao thức POP.

POP3 định nghĩa 3 giai đoạn tạo thành POP Session: Giai đoạn 1 là giai đoạn xác định tính hợp pháp của người nhận mail (Authorization); giai đoạn 2 là giai đoạn giao dịch giữa PC và POP Server (Transaction) và giai đoạn 3 là giai đoạn cập nhập thông tin (Update).

Sau khi thiết lập kết nối với Server, giai đoạn đầu Client sẽ cho Server biết nó là ai. nếu Client hợp pháp POP Server sẽ mở Mailbox và bắt đầu chuyển sang giai đoạn giao dịch. Giai đoạn giao dịch, chương trình sẽ yêu cầu POP3 Server cung cấp các thông tin như danh sách mail … hay yêu cầu gởi về cho nó một bức mail xác định nào đó. Giai đoạn cuối cũng sẽ cập nhập và đóng kết hiện hành.

Các lệnh thông dụng của giao thức POP3:

| **Lệnh** | **Ý nghĩa** |
|---|---|
| User | Cho biết tên của user cho POP Server |
| Pass | Yêu cầu một password cho người sử dụng trên Server |
| Quit | Đóng kết nối đã được thiết lập trước đó |
| Stat | POP Server trả về số lượng Mail có trong mailbox của người sử dụng cùng kích thước chúng |
| List | Trả về các ID và size của các message |
| Retr | Nhận một message từ mailbox (yêu cầu tham số là ID của mail cần nhận) |
| Dele | Đánh dấu một message để xóa ( yêu cầu tham số là ID của mail cần xóa) |
| Noop | POP Server trả về +OK nhưng không làm gì cả |
| Last | Yêu cầu POP Server trả về số Message đã truy nhập |
| Top | Liệt kê header của Mail |
| Rset | Hủy đánh dấu trên Message bị đánh dấu để xóa |

POP3 chỉ định nghĩa hai loại trả lời cho mỗi câu lệnh là : +OK để chỉ thao tác hoàn thành tốt và –ERR để báo có lỗi. Ví dụ cách dùng một số lệnh của POP3 như sau (các hàng sau dấu chấm phẩy để chú thích lệnh)

**Giai đoạnn 1: Nhận dạng user**

```
CLIENT: USER user01      ; cho biết tên user là user01
SERVER: +OK              ; báo thành công
CLIENT: PAS abc          ;cho biêt Password là abc
```

SERVER: +OK user01's ; maildrop là 2 message (520octets)

**Giai đoạn 2: Trao đổi**

CLIENT: STAR ; số mail trong mailbox

SERVER: +OK 2 500 ; có 2 mail với tổng kích thước là 520

CLIENT: LIST ; Liệt kê các ID và kích thước của các mail

SERVER: +OK 2message (520 octets)

SERVER: 1 110 ; mail thứ 1 kích thước 110

SERVER: 2 410 ; mail thứ 2 kích thước 410

CLIENT: List 1 ;Cho thông tin về mail có ID là 1

SERVER: +OK 1 110

CLIENT: LIST 4

SERVER: -ERR no such message, only 2 message in maildrop

……

**Giai đoạn 3: Kết thúc**

CLIENT: q\QUIT ; đóng kết nối TCP hiện hành

SERVER: +OK dhdl POP3 server signing off

Chú ý rằng các message bị đánh dấu để xóa bằng lệnh DELE thực sự chưa bị xóa ngay để nếu sau đó ta có thể dùng lệnh phục hồi không xóa băng lệnh RSET, chúng chỉ thực sự bị xóa bỏ khỏi maildrop khi bước vào giai đoạn Update (khi gởi lệnh QUIT).

### V.5.1. Giao thức IMAP:

Không giống như POP3, hoạt động với giả thiết người dùng sẽ download thư điện tử về máy tính và xóa trên server, IMAP (Internet Mail Access Protocol), là giao thức cho phép các thư điện tử lưu trữ không giới hạn về thời gian trên server. IMAP cung cấp các cơ chế để đọc và thậm chí chia nhỏ thư, một đặc tính có lợi khi sử dụng kết nối tốc độ chậm. Vì hoạt động theo hướng thư điện tử sẽ không chuyển về lưu trữ trên máy tính người dùng, IMAP cho phép tạo, xóa và quản lý nhiều mail-box trên server.

## VI.6. Dịch vụ phân giải tên miền (DNS Services-Domain Name System Services)

Địa chỉ Internet 32 bit thỏa mãn yêu cầu kỹ thuật, nhưng phức tạp và khó nhớ đối với người dùng. Giải pháp đưa ra ở đây là dùng những tên gợi nhớ thay chổ địa chỉ số là tự nhiên và dễ nhớ đối với người sử dụng. Hơn nữa, dùng tin tin cậy hơn địa chỉ số vì địa chỉ số có thể thay đổi những tên luôn luôn dùng lại được. Do đó nảy sinh vấn đề cách đặt tên và ánh xạ địa chỉ IP với tên.

Trước đây trung tâm thông tin Internet NIC chịu trách nhiệm cấp phát và quản lý tên. Người ta dùng một file có tên host.txt trên Windows hoặc/etc/hosts trên Unix, tập tin này chứa tên của tất cả các mạng, router, host và địa chỉ IP tương ứng với chúng. Các tên được cấp phát không có mối liên hệ gì với nhau. Khi Internet phát triển, giải pháp này trở nên phức tạp không chấp nhận được về mặt quản lý.

Theo Paul Mockipetris, người thiết kế chính DNS, mục tiêu thiết kế bắt đầu của DNS là để thay thế các tập tin host phức tạp bằng một cơ sở dữ liệu phân tán nhẹ hơn có khả năng cung cấp một *không gian tên thứ bậc, sự quản lý phân tán, có bộ đệm cục bộ (caching), các kiểu mở rộng, kích thước cơ sở dữ liệu không giới hạn và có hiệu năng.*

DNS tương ứng với tầng 7 của mô hình OSI và dùng giao thức UDP hay TCP ở tầng dưới. Việc truy cập DNS thực hiện theo mô hình Client/Server. Hầu hết các hệ thống kết nối Internet đầu hỗ trợ DNS. Các địa chỉ DNS được định nghĩa trong tài liệu RFC 974, 1034, 1035. Dịch vụ cài đặt giao thức DNS phổ biến nhất BIND (Berkeley Internet Name Domain), được phát triển đầu tiên tại Berkeleycho hệ diều hành Unix.

DNS gồm 3 thành phần : **Namespace, các NameServer và Resover**

### V.5.2. Không gian tên miền

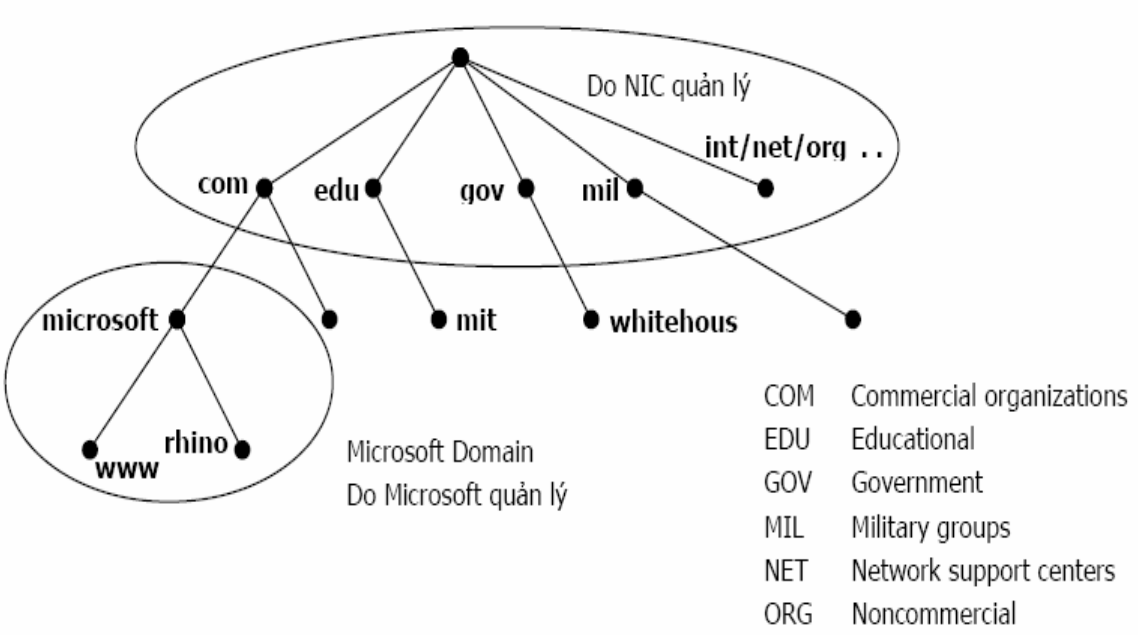
DNS tổ chức không gian tiên miền theo cấu trúc cây, trên cùng là gốc, rồi đến các nút cha, nút con… và cuối cùng là các nút lá.

Một máy tính trong mạng sẽ ứng với một nút của cây. Như ở trên, máy ở lá www sẽ có địa chỉ hoàn chỉnh www.microsoft.com. Mỗi nút trên cây biểu diễn một miền (domain) trong hệ thống DNS; mỗi miền lại có một hay nhiều miền con. Tại mỗi miền này đều phải có máy chủ DNS tương ứng quản lý hệ thống tên trong miền đo.

*Nút trên cây*: Mỗi nút có một tên tương ứng dài từ - đến 63 ký tự dưới 128 trong bảng mã ASCII. Các nút kề nhau không được có cùng tên. Mỗi nút có một tập (có thể rỗng) các *bản ghi tài nguyên* (Resource Record –RR) chứa thông tin đi kèm nút đó. Nhãn rỗng dành riêng cho nút gốc, ký hiệu bằng dấu chấm (.).

*Miền con*: Được tạo thành từ mỗi nút của không gian tên và các nút bên dưới có thể đi đến được các nút đó.

*Vùng:* Là một phần cây con của cây DNS được quản lý như một thực thể riêng. Vùng có thể bao gồm một miền hay một miền với một số miền con. Các miền con mức thấp hơn của một vùng lại có thể chia thành các vùng rời nhau.




Hình VI-6. Cấu trúc không gian tên miền DNS

*Tên miền của một nút:* là dãy các nhãn từ một nút trên cây đến gốc của cây. Các nhãn trong tên miền cách nhau bằng dấu chấm (.). *Tên miền tuyệt đối* kết thúc bằng dấu chấm và sẽ được phần mềm cục bộ ghép đầy đủ khi xử lý. Để đơn giản việc cài đặt, độ dài tên miền được giới hạn 255. Một miền là miền con của miền khác nếu tên miền đó chứa tên miền kia. Ví dụ A,B,C,D là miền con của các miền B,C,D,C,D,D, và miền gốc.

*Tên miền đầy đủ*: là tên các nút từ gốc lá của cây nối với nhau và phân cách bằng dấu chấm. Ví dụ mrp2.widgets.mfg.universal.co.uk

*Các miền mức định*: Miền gốc và các miền mức định của cây DNS do NIC quản lý. Các tên miền mứ định có thể chia ba loại.

- Các miền tổ chức (tên 3 ký tự): com, edu, gov…
- Các miền địa lý (các mã quốc gia, 2 ký tự): uk, vn, ca, fr…
- Miền in-addr-arpa: miền đặc biệt để ánh xạ địa chỉ thành tên.

Trách nhiệm quản lý không gian tên DNS dưới mức đỉnh được NIC ủy nhiệm cho các tổ chức khác. Các tổ chức này lại chia không gian tên phía dưới và ủy nhiệm xuống. Mô hình quản lý phân tầng cho phép DNS được quản lý tự trị bởi các tổ chức tham gia. Các đặt tên như vậy có tác dụng phân cấp quản lý vùng tên. Các tổ chức có thể tự tạo không gian tên riêng của mình trong mạng không phụ thuộc vào sự cho phép của NIC.

Vấn đề tên và vùng con được nhiều hãng lớn bổ sung và làm phong phú thêm bằng những phương pháp của riêng họ. Ví dụ Microsoft có WINS-Windows Internet Naming Service, IBM, có DDNS – Dynamic Domain Nam System.

- **Cú pháp tên miền**

Cú pháp cho tên miền sau đây cho phép phù hợp với nhiều ứng dung nhưmail, telnet,…

<domain>::<subdomain>|” ”

<subdomain>::=<label>|<subdomain>”.”<label>

<label>::=<letter>[[<ldh-str>]<let-dig>]

<ldh-str>::=<let-dig-hyp>|<let-hyp><ldh-str>

<let-dig-hyp>::=<let-dig>|” ”

<let-dig>:=<letter>|<digit>

<leter>::=ký tự từ A-Z, a-z

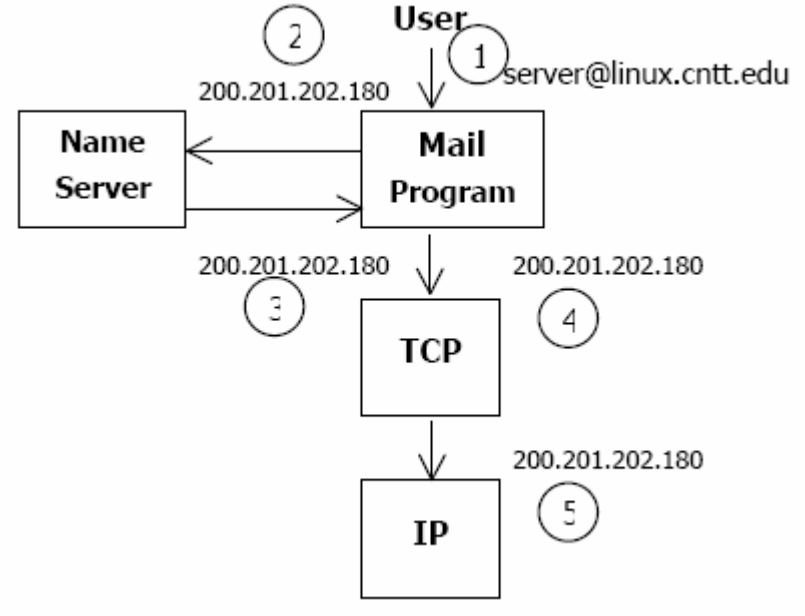
<digit>::=chữ số 0-9

### V.5.3. Máy chủ quản lý tên miền

Máy chủ quản lý tên (Name Server) quản lý cấu trúc cây của miền và các tập thông tin đi kèm. Máy chủ tên có thông tin đầy đủ về một số tập con gọi là vùng của không gian tên và các con trỏ đến các name server khác để lấy tin về một miền bất kỳ của cây miền. Các máy chủ tên có thông tin đầy đủ về một số phần của cây miền được gọi là có thẩm quyền (authoritative) về các phần đo. Một *vùng* (zone) là một đơn vị thông tin có thẩm quyền của cơ sở dữ liệu DNS. Trong thực tế, các máy chủ thường lưu tạm thời trong bộ đếm cấu trúc và thông tin các vùng về các vùng khác để tăng hiệu năng. Các máy chủ quản lý tên trong vùng trao đổi thông tin với nhau bằng Zone Transfer Protocol.

### V.5.4. Chương trình phân giải tên miền

Chương trình phân giải tên (resolver) là các chương trình hệ thống lấy thông tin từ nameserver để trả lời yêu cầu của những ứng dụng khách (client). Resolver phải có khả năng truy cập đến ít nhất một nameserver và dùng thông tin của nameserver đó trả lời trực tiếp câu hỏi hay để hỏi tiếp các nameserver khác. Chương trình người sử dụng có thể truy cập trực tiếp đến resolver, do đó không cần có một giao thức giữa resolver và chương trình người dùng.




Hình VI-7. Quá trình phân giải tên miền trong thực tế

# Tài liệu tham khảo

[1] Andrew S. Tanenbaum, **Computer Network**, Fourth Edition, Prentice Hill, 2003.

[2] James F. Kurose, Keith W.Ross, **A top-down approach featuring the Internet**, Addison Wesley, Third Edition, 2000.

[3] Nguyễn Tấn Khôi**, Giáo trình Mạng máy tính**, Đại học Bách khoa Đà Nẵng, 2004.

# Giáo trình mạng máy tính

Trang

**GIỚI THIỆU .....5**

**CHƯƠNG 1 - GIỚI THIỆU VỀ MẠNG MÁY TÍNH .....6**

*1.1 Lịch sử mạng máy tính .....6*
*1.2 Một số khái niệm cơ bản .....7*
*1.3 Mạng ngang hàng (Peer to Peer) và mạng có máy chủ (Server based) .....10*
*1.4 Các hệ điều hành mạng.....11*
*1.5 Các dịch vụ mạng .....12*
*1.6 Làm thế nào để trở thành một chuyên nghiệp viên về mạng máy tính?.....13*

**CHƯƠNG 2 - MÔ H Ì NH OSI.....17**

*2.1 Kiến trúc phân tầng và mô hình OSI (Open System Interconnect).....17*
*2.2 Ý nghĩa và chức năng của các tầng trong mô hình OSI .....19*
*2.3 Áp dụng mô hình OSI.....23*
*2.4 Mô tả các thành phần của khuôn dữ liệu (Frame) .....25*

**CHƯƠNG 3 - ĐƯỜNG TRUYỀN VẬT LÝ ..... 30**

*3.1 Truyền dữ liệu: tín hiệu tương tự (analogue) và tín hiệu số hoá (digital) ..... 30*

*3.2 Các đặc tính của đường truyền mạng ..... 31*

*3.3 Các mạng LAN: Baseband và Broadband ..... 32*

*3.4 Các loại cáp mạng ..... 33*

**CHƯƠNG 4 - CÁC GIAO THỨC MẠNG (PROTOCOLS) ..... 40**

*4.1 Giao thức (protocol) mạng là gì? ..... 40*

*4.2 Bộ giao thức TCP/IP (Transmission Control Protocol / Internet Protocol) ..... 41*

*4.3 Bộ giao thức IPX/SPX (Internetwork Packet Exchange / Sequenced Packet Exchange ) 44*

*4.4 Bộ giao thức Microsoft Network ( NETBIOS, NETBEUI, SMB) ..... 45*

*4.5 Một số Protocols khác ..... 47*

**CHƯƠNG 5 - CÁC HÌNH TRẠNG (TOPOLOGIES) CỦA MẠNG CỤC BỘ (LAN) ..... 49**

*5.1 Các đặc trưng cơ bản của mạng cục bộ (LAN) ..... 49*

*5.2 Các hình trạng LAN đơn giản ..... 51*

*5.3 Các hình trạng LAN hỗn hợp ..... 54*

*5.4 Các hệ thống giao vận mạng ..... 56*

*5.5 Kiến trúc Ethernet ..... 59*

*5.6 Mạng Token Ring ..... 64*

**CHƯƠNG 6 – GIỚI THIỆU WINDOWS 2000 ..... 70**

*6.1 Các phiên bản của Windows 2000 ..... 70*

*6.2 Một số đặc điểm mới của Windows 2000 ..... 71*

*6.3 Mô hình workgroup và mô hình domain trong Windows 2000 ..... 76*

**CHƯƠNG 7 – CÀI ĐẶT WINDOWS 2000 SEVER ..... 80**

*7.1 Cài đặt Windows 2000 Server ..... 80*

*7.2 Đăng nhập tới một Domain ..... 88*

*7.3 Các công cụ quản trị ..... 90*

*7.4 Hộp thoại bảo mật Windows 2000 ..... 90*

**CHƯƠNG 8 - QUẢN TRỊ TÀI KHOẢN NGƯỜI DÙNG ..... 93**

*8.1 Các loại tài khoản người dùng (user) ..... 93*

*8.2 Lập kế hoạch tài khoản người dùng ..... 94*

*8.3 Tạo tài khoản người dùng cục bộ và tài khoản người dùng miền ..... 97*

*8.4 Thiết lập hồ sơ người dùng (User Profile) ..... 106*

**CHƯƠNG 9 - QUẢN TRỊ TÀI KHOẢN NHÓM ..... 113**

*9.1. Các loại nhóm trong Windows 2000 ..... 113*
*9.2. Lập kế hoạch nhóm Local Domain và nhóm Global ..... 114*
*9.3. Tạo và xoá các nhóm ..... 114*
*9.4. Thêm các thành viên vào nhóm ..... 116*

**TÀI LIỆU THAM KHẢO ..... 121**

# GIỚI THIỆU

Yêu cầu có các tài liệu tham khảo cho sinh viên của khoa Công nghệ Thông tin - Trường Cao đẳng Công nghiệp 4 ngày càng trở nên cấp thiết. Việc biên soạn tài liệu này nằm trong kế hoạch xây dựng hệ thống giáo trình các môn học của Khoa.

Đề cương của giáo trình đã được thông qua Hội đồng Khoa học của Khoa và Trường. Mục tiêu của giáo trình nhằm cung cấp cho sinh viên một tài liệu tham khảo chính về môn học Mạng máy tính, trong đó giới thiệu những khái niệm căn bản nhất về hệ thống mạng máy tính, đồng thời trang bị những kiến thức và một số kỹ năng chủ yếu cho việc bảo trì và quản trị một hệ thống mạng. Đây có thể coi là những kiến thức ban đầu và nền tảng cho các kỹ thuật viên, quản trị viên về hệ thống mạng.

Tài liệu này có thể tạm chia làm 2 phần:

- Phần 1: từ chương 1 đến chương 5
- Phần 2: từ chương 6 đến chương 9

Phần 1, bao gồm những khái niệm cơ bản về hệ thống mạng (chương 1), nội dung chính của mô hình tham chiếu các hệ thống mở - OSI (chương 2), những kiến thức về đường truyền vật lý (chương 3), khái niệm và nội dung cơ bản của một số giao thức mạng thường dùng (chương 4) và cuối cùng là giới thiệu về các hình trạng mạng cục bộ (chương 5)

Phần 2, trình bày một trong những hệ điều hành mạng thông thường nhất hiện đang dùng trong thực tế: hệ điều hành mạng Windows 2000 Server. Ngoài phần giới thiệu chung, tài liệu còn hướng dẫn cách thức cài đặt và một số kiến thức liên quan đến việc quản trị tài quản người dùng.

Tham gia biên soạn giáo trình có:

- Giảng viên Nguyễn Văn Bình biên soạn chính các chương 1, 2, 5
- Giảng viên Tạ Duy Công Chiến biên soạn chính các chương 3, 4, 9
- Giảng viên Nguyễn Chí Hiếu biên soạn các chương 6, 7, 8.

Mặc dù đã có những cố gắng để hoàn thành giáo trình theo kế hoạch, nhưng do hạn chế về thời gian và kinh nghiệm soạn thảo giáo trình, nên tài liệu chắc chắn còn những khiếm khuyết. Rất mong nhận được sự đóng góp ý kiến của các thầy cô trong Khoa cũng như các bạn sinh viên và những ai sử dụng tài liệu này. Các góp ý xin gửi về Tổ Hệ thống máy tính – Khoa Công nghệ thông tin - Trường Cao đẳng Công nghiệp 4. Xin chân thành cảm ơn trước.

**Nhóm biên soạn**

Tháng 08/2004

# CHƯƠNG 1 - GIỚI THIỆU VỀ MẠNG MÁY TÍNH

## MỤC TIÊU CỦA CHƯƠNG

*Kết thúc chương này, sinh viên sẽ có thể:*

- Nắm sơ lược về lịch sử phát triển của mạng máy tính
- Hiểu được khái niệm mạng máy tính cũng như hai yếu tố cơ bản của nó là kiến trúc và môi trường truyền. Nắm được ba tiêu chí cơ bản để phân loại mạng máy tính và hình trạng tổng quan của mạng LAN.
- Nắm được hai mô hình mạng: *ngang hàng* (peer-to-peer) và *client/server*.
- Biết được một số hệ điều hành mạng thông dụng.
- Nắm được một số dịch vụ cơ bản có trên mạng.
- Những yêu cầu cần có để trở thành một chuyên nghiệp viên về mạng máy tính.

## 1.1 Lịch sử mạng máy tính

*Từ đầu những năm 60* đã xuất hiện các *mạng xử lý* trong đó các *trạm cuối* (terminal) thụ động được nối vào một máy xử lý trung tâm. Vì máy xử lý trung tâm làm tất cả mọi việc: quản lý các thủ tục truyền dữ liệu, quản lý sự đồng bộ của các trạm cuối v.v…, trong khi đó các trạm cuối chỉ thực hiện chức năng nhập xuất dữ liệu mà không thực hiện bất kỳ chức năng xử lý nào nên hệ thống này vẫn chưa được coi là *mạng máy tính.*

*Giữa năm 1968*, Cục các dự án nghiên cứu tiên tiến (ARPA – Advanced Research Projects Agency) của Bộ Quốc phòng Mỹ đã xây dựng dự án nối kết các máy tính của các trung tâm nghiên cứu lớn trong toàn liên bang, mở đầu là Viện nghiên cứu Standford và 3 trường đại học (Đại học California ở Los Angeless, Đại học California ở Santa Barbara và Đại học Utah). Mùa thu năm 1969, 4 trạm đầu tiên được kết nối thành công, đánh dấu sự ra đời của ARPANET. Giao thức truyền thông dùng trong ARPANET lúc đó đặt tên là NCP (Network Control Protocol).

*Giữa những năm 1970*, họ giao thức TCP/IP được Vint Cerf và Robert Kahn phát triển cùng tồn tại với NCP, đến năm 1983 thì hoàn toàn thay thế NCP trong ARPANET.

*Trong những năm 70*, số lượng các mạng máy tính thuộc các quốc gia khác nhau đã tăng lên, với các kiến trúc mạng khác nhau (bao gồm cả phần cứng lẫn giao thức truyền thông), từ đó dẫn đến tình trạng không tương thích giữa các mạng, gây khó khăn cho người sử dụng. Trước tình hình đó, vào *năm 1984* Tổ chức tiêu chuẩn hoá quốc tế ISO đã cho ra đời *Mô hình tham chiếu cho việc kết nối các hệ thống mở* (Reference Model for Open Systems Interconnection - gọi tắt là mô hình OSI). Với sự ra đời của OSI và sự xuất hiện của máy tính cá nhân, số lượng mạng máy tính tính trên toàn thế giới đã tăng lên nhanh chóng. Đã xuất hiện những khái niệm về các loại mạng LAN, MAN.

*Tới tháng 11/1986* đã có tới 5089 máy tính được nối vào ARPANET, và đã xuất hiện thuật ngữ "Internet".

*Năm 1987*, mạng xương sống (backborne) NSFnet (National Science Foundation network) ra đời với tốc độ đường truyền nhanh hơn (1,5 Mb/s thay vì 56Kb/s trong ARPANET) đã thúc đẩy sự tăng trưởng của Internet. Mạng Internet dựa trên NSFnet đã vượt qua biên giới của Mỹ.

*Đến năm 1990*, quá trình chuyển đổi sang Internet - dựa trên NSFnet kết thúc. NSFnet giờ đây cũng chỉ còn là một mạng xương sống thành viên của mạng Internet toàn cầu. Như vậy có thể nói lịch sử phát triển của Internet cũng chính là lịch sử phát triển của mạng máy tính.

## 1.2 Một số khái niệm cơ bản

### 1.2.1. Mạng máy tính là gì?

Ta có thể định nghĩa: mạng máy tính là một tập hợp các máy tính được nối kết với nhau bởi các *đường truyền vật lý* theo một *kiến trúc* nào đó.

Một cách cụ thể hơn ta có thể hiểu mạng máy tính bao gồm sự kết nối từ hai máy tính trở nên. Các máy tính này có thể giao tiếp với nhau, chia xẻ tài nguyên (các đĩa cứng, các máy in và các ổ đĩa CD-ROM v.v…), mỗi máy có thể truy xuất các máy ở xa hoặc các mạng khác để trao đổi các file, dữ liệu và thông tin hoặc cho phép các giao tiếp điện tử.

### 1.2.2. Các yếu tố của mạng máy tính.

Như đã định nghĩa ở trên, hai yếu tố căn bản của mạng máy tính là: *đường truyền vật lý* và *kiến trúc* mạng. Kiến trúc mạng bao gồm: *hình trạng* (topology) của mạng và *giao thức* (protocol) truyền thông. Đường truyền mạng (medium) bao gồm: loại có dây (wire): các loại cáp kim loại, cáp sợi quang, và loại không dây (wireless): tia hồng ngoại, sóng điện từ tần số radio v.v…. Chi tiết về các nội dung này sẽ được trình bày ở các chương sau.

### 1.2.3. Các tiêu chí phân loại mạng máy tính.

Dựa vào các tiêu chí khác nhau, người ta phân chia mạng máy tính thành các loại khác nhau. Sau đây là ba tiêu chí cơ bản.

a) Phân loại mạng dựa trên *khoảng cách địa lý,* có ba loại mạng:

- *Mạng cục bộ* (Local Area Network – LAN): là mạng được cài đặt trong một phạm vi tương đối nhỏ (trong một phòng, một toà nhà, hoặc phạm vi của một trường học v.v…) với khoảng cách lớn nhất giữa hai máy tính nút mạng chỉ trong khoảng vài chục km trở lại. Tổng quát có hai loại mạng LAN: *mạng ngang hàng* (peer to peer) và *mạng có máy chủ* (server based). Mạng server based còn được gọi là mạng "*Client / Server*" (Khách / Chủ).
- *Mạng đô thị* (Metropolitan Area Network – MAN): là mạng được cài đặt trong phạm vi một đô thị hoặc một trung tâm kinh tế - xã hội có bán kính khoảng 100 km trở lại.
- *Mạng diện rộng* (Wide Area network – WAN): phạm vi của mạng có thể vượt qua biên giới quốc gia và thậm chí cả lục địa. Cáp truyền qua đại dương và vệ tinh được dùng cho việc truyền dữ liệu trong mạng WAN.

- *Mạng toàn cầu* (Global Area Network – GAN): phạm vi của mạng trải rộng toàn Trái đất.

b) Phân loại mạng dựa trên *kỹ thuật chuyển mạch*, cũng có ba loại mạng:

- *Mạng chuyển mạch kênh* (circuit – switched networks): khi có hai thực thể cần trao đổi thông tin với nhau thì giữa chúng sẽ được thiết lập một "kênh" cố định và được duy trì cho đến khi một trong hai bên ngắt kết nối. Các dữ liệu chỉ được truyền theo con đường cố định này. Kỹ thuật chuyển mạch kênh được sử dụng trong các kết nối ATM (Asynchronous Transfer Mode) và dial-up ISDN (Integrated Services Digital Networks). Ví dụ về mạng chuyển mạch kênh là mạng điện thoại.

  Phương pháp chuyển mạch kênh có hai nhược điểm chính:

  - Phải tốn thời gian để thiết lập đường truyền cố định giữa hai thực thể.
  - Hiệu suất sử dụng đường truyền không cao, vì có lúc trên kênh không có dữ liệu truyền của hai thực thể kết nối, nhưng các thực thể khác không được sử dụng kênh truyền này.

- *Mạng chuyển mạch thông báo* (message – switched networks):

  *Thông báo* (message) là một đơn vị thông tin của người sử dụng có khuôn dạng được qui định trước. Mỗi thông báo có chứa vùng thông tin điều khiển trong đó có phần địa chỉ đích của thông báo.

  Trong mạng chuyển mạch thông báo, giữa hai thực thể truyền thông tồn tại nhiều đường truyền khác nhau. Căn cứ vào địa chỉ đích, các thông báo khác nhau có thể đến đích theo những con đường khác nhau.

  Phương pháp chuyển mạch thông báo có một số ưu điểm:

  - Hiệu suất sử dụng đường truyền cao, vì có thể phân chia giữa nhiều thực thể.
  - Mỗi nút mạng có thể lưu trữ thông báo cho đến khi kênh truyền rảnh mới gửi thông báo đi, do đó giảm được trình trạng tắc nghẽn mạng. v.v…

  Nhược điểm chính của phương pháp chuyển mạch thông báo là không hạn chế kích thước của các thông báo, do đó có thể dẫn đến phí tổn lưu trữ tạm thời cao. Kỹ thuật chuyển mạch thông báo thích hợp với các dịch vụ thông tin kiểu thư điện tử (Electronic Mail)

- *Mạng chuyển mạch gói* (packet - switched networks): mỗi thông báo được chia thành nhiều phần nhỏ hơn gọi là các *gói tin* (packet) có khuôn dạng qui định trước. Mỗi gói tin cũng có phần thông tin điều khiển chứa địa chỉ nguồn (sender) và địa chỉ đích (receiver) của gói tin. Các gói tin thuộc về một thông báo có thể truyền tới đích theo những con đường khác nhau.

  Kỹ thuật chuyển mạch gói về cơ bản giống kỹ thuật chuyển mạch thông báo, nhưng có hiệu quả hơn là phí tổn lưu trữ tạm thời tại mỗi nút giảm đi vì kích thước tối đa của các gói tin được giới hạn.

  Những khó khăn của kỹ thuật chuyển mạch gói cần giải quyết là: tập hợp các gói tin tại nơi nhận để tạo lại thông báo ban đầu cũng như xử lý việc mất gói.

Do có nhiều ưu điểm nên hiện nay mạng chuyển mạch gói được dùng phổ biến hơn các mạng chuyển mạch thông báo. Việc tích hợp cả hai kỹ thuật chuyển mạch kênh và thông báo trong một mạng thống nhất gọi là *mạng dịch vụ tích hợp số hoá* (Integrated Services Digital Networks – ISDN) đang là một trong những xu hướng phát triển của mạng ngày nay.

c) Phân loại mạng dựa trên *kiến trúc mạng* (topology và protocol). Ví dụ như mạng System Network Architecture (SNA) của IBM, mạng ISO (theo kiến trúc chuẩn quốc tế), mạng TCP/IP v.v….

### 1.2.4. Tổng quan về hình trạng mạng (topology) LAN

Hình trạng mạng chủ yếu thể hiện trong các mạng LAN. Mỗi chuẩn về LAN có các quy tắc riêng cho việc nối dây. Các quy tắc này định nghĩa việc kết nối đường truyền, những yêu cầu về phần cứng và cách thức sắp xếp các thành phần khác nhau. Có ba yếu tố xác định bản chất của một mạng LAN:

- Hình trạng mạng.
- Đường truyền.
- Kỹ thuật truy xuất đường truyền.

a) Hình trạng mạng (Topology)

Cách sắp đặt hình học (hoặc vật lý) sơ đồ nối dây mạng máy tính gọi là *hình trạng mạng* (topology). Có hai loại hình trạng:

- *Hình trạng vật lý* của một mạng mô tả con đường các cáp mạng được định tuyến. Nó không xác định kiểu của các thiết bị, phương pháp kết nối hoặc các địa chỉ trên mạng.
- *Hình trạng luận lý* của một mạng mô tả con đường mà mạng hoạt động trong khi truyền thông tin giữa các thiết bị khác nhau.

b) Hình trạng vật lý (Physical topology).

Cấu trúc vật lý đầy đủ của đường truyền mạng được gọi là *hình trạng vật lý*.

Hình trạng vật lý của một mạng được phân thành ba loại hình dạng hình học cơ bản: *bus, ring* hoặc *star*. Ba hình trạng này có thể kết hợp để tạo thành các hình trạng *hỗn hợp* (hybrid) như: *star-wired ring, star-wired bus* và *daisy chains* (Chi tiết về các hình trạng này sẽ được khảo sát ở chương 3 - "Topology").

Khi chọn một topology mạng vật lý, ta nên tập trung vào các đặc tính sau:

- Tính dễ dàng sắp đặt.
- Tính thuận tiện cho việc cấu hình lại.
- Việc chẩn đoán và sửa chữa các sự cố tương đối dễ dàng.
- Chi phí, hiệu suất, độ tin cậy, khả năng mở rộng mạng trong tương lai, kiểu và chiều dài của cáp mạng.

c) Hình trạng luận lý (Logical topology)

Hình trạng luận lý của mạng xác định các đặc tính truyền dữ liệu của nó, chẳng hạn như mô hình giao vận mạng. Đối với các mạng LAN, hai hình trạng luận lý thông thường nhất là *Ethernet* và *Token Ring*.

## 1.3 Mạng ngang hàng (Peer to Peer) và mạng có máy chủ (Server based)

### 1.3.1 Mạng ngang hàng (peer-to-peer network)

Các mạng peer-to-peer là một ví dụ rất đơn giản của các mạng LAN. Chúng cho phép mọi nút mạng vừa đóng vai trò là thực thể *yêu cầu* các dịch vụ mạng, vừa là các thực thể *cung cấp* các dịch vụ mạng. Phần mềm mạng peer-to-peer được thiết kế sao cho các thực thể ngang hàng thực hiện cùng các chức năng tương tự nhau.

Các đặc điểm của mạng peer-to-peer:

- Các mạng peer-to-peer còn được biết đến như các mạng **workgroup** (nhóm làm việc) và được sử dụng cho các mạng có 10 người sử dụng (user) làm việc trên mạng đó.
- Mạng peer-to-peer không đòi hỏi phải có người quản trị mạng (administrtor). Trong mạng peer-to-peer mỗi user làm việc như người quản trị cho trạm làm việc riêng của họ và chọn tài nguyên hoặc dữ liệu nào mà họ sẽ cho phép chia xẻ trên mạng cũng như quyết định ai có thể truy xuất đến tài nguyên và dữ liệu đó.

Các ưu điểm của mạng peer-to-peer:

- Đơn giản cho việc cài đặt.
- Chi phí tương đối rẻ.

Những nhược điểm của mạng peer-to-peer:

- Không quản trị tập trung, đặc biệt trong trường hợp có nhiều tài khoản cho một người sử dụng (user) truy xuất vào các trạm làm việc khác nhau.
- Việc bảo mật mạng có thể bị vi phạm với các user có chung username, password truy xuất tới cùng tài nguyên.
- Không thể sao chép dự phòng (backup) dữ liệu tập trung. Dữ liệu được lưu trữ rải rác trên từng trạm.

### 1.3.2 Mạng có máy chủ (Server based network / Client-Server network)

Mạng *server based* liên quan đến việc xác định vai trò của các thực thể truyền thông trong mạng. Mạng này xác định thực thể nào có thể tạo ra các *yêu cầu* dịch vụ và thực thể nào có thể *phục vụ* các yêu cầu đó (còn gọi là các thực thể *đáp ứng* yêu cầu dịch vụ). Các máy tính được gọi là các **file server** thực hiện việc xử lý dữ liệu và giao tiếp giữa các máy tính khác trong mạng. Các máy tính khác đó được gọi là các **workstation** (máy tính trạm).

Các mạng *server based* thường được sử dụng cho các mạng có 10 người sử dụng và thực hiện các công việc chuyên biệt sau:

- *File* và *Print Servers* - quản lý truy xuất của user tới các file và các máy in.
- *Application Servers* – máy chủ có nhiệm vụ cung cấp các ứng dụng, các phần mềm cho các máy trạm trong môi trường client/server.
- *Database Server* - máy chủ có cài đặt các hệ thống Cơ sở dữ liệu (DBMS) như SQL SERVER, Oracle, DB2 phục vụ cho các nhu cầu ứng dụng truy xuất dữ liệu trên mạng.
- *Communication Server* - máy chủ phục vụ cho công tác truyền thông, giao tiếp trên mạng như Web (Web Server), mail (mail Server), truyền nhận file (FTP server)…
- *Mail Servers* - hoạt động như một server ứng dụng, trong đó có các ứng dụng server và ứng dụng client, với dữ liệu được tải xuống từ server tới client.

Đặc điểm của mạng *server based*:

- Khó khăn trong việc cài đặt, cấu hình và quản trị hơn so với mạng peer-to-peer
- Cung cấp sự bảo mật tốt hơn cho các tài nguyên mạng.
- Dễ dàng hơn trong việc quản trị sao chép dự phòng dữ liệu (backup). Thậm chí có thể lập lịch cho công việc này thực hiện tự động.

## 1.4 Các hệ điều hành mạng

Cùng với việc ghép nối các máy tính thành mạng, cần thiết phải có các hệ điều hành được cài đặt trên từng máy tính có trong mạng. Trong đó có các hệ điều hành trên phạm vi toàn mạng có chức năng quản lý dữ liệu và tính toán, xử lý một cách thống nhất.

Những hệ điều hành dùng cho mạng máy tính cá nhân peer-to-peer bao gồm:

- Microsoft Windows for Workgroups 3.11
- Microsoft Windows 9X, ME
- Microsoft Windows NT Workstation
- Microsoft Windows 2000 Professional
- Microsoft Windows XP Professional
- Novell Netware Lite
- Linux for Workstation

Những hệ điều hành mạng máy tính cá nhân phổ biến nhất cho mạng server based bao gồm:

- Windows NT Server
- Windows 2000 Server và Advanced Server
- Unix (bao gồm cả Linux)
- Novell Netware

## 1.5 Các dịch vụ mạng

Các mạng kết nối hai hoặc nhiều hơn các máy tính với nhau để cung cấp một số phương pháp cho việc chia xẻ và truyền dữ liệu. Nhiều đặc điểm mà một mạng cung cấp được xem như các *dịch vụ* (services). Các dịch vụ thông thường nhất trên một mạng là: *thư điện tử* (email)*, in ấn, chia xẻ file, truy xuất Internet, quay số từ xa* (remote dial-in)*, giao tiếp*(communication) và *dịch vụ quản trị* (management service). Các mạng lớn có thể có những máy chủ (server) riêng, mỗi máy này thực hiện một trong các dịch vụ mạng. Với các mạng nhỏ hơn, tất cả các dịch vụ mạng được cung cấp bởi một hoặc vài máy chủ. (Một máy chủ có thể cung cấp nhiều dịch vụ mạng).

### 1.5.1 Các dịch vụ file và in ấn

Các dịch vụ file của một mạng có thể được sử dụng để chia xẻ các *phần mềm ứng dụng* như các chương trình xử lý văn bản, các cơ sở dữ liệu, các bảng tính hoặc các chương trình email. Các chương trình này được chạy trên một máy chủ trung tâm, có nghĩa là chúng không phải cài đặt cục bộ trên mọi máy tính. Chính điều này giảm bớt thời gian và chi phí cài đặt, cập nhật các file trên từng máy tính, vì mọi thứ được lưu trữ trong một vị trí trung tâm.

Các dịch vụ file cho phép các user chia xẻ dữ liệu và các tài nguyên khác nhanh và tiết kiệm. Email được gửi trong vài giây. Các file đa truyền thông (multimedia file) với kích thước lớn dễ dàng truyền qua mạng. Các web site có thể giúp chúng ta cập nhật thông tin mới nhất. Các tài nguyên quí hiếm như CD-ROM, fax modem, scanner v.v… có thể chia xẻ để dùng chung trên mạng.

Các máy in có thể dùng chung trên mạng nhờ các *dịch vụ in mạng*. Người quản trị mạng có thể cài đặt, quản trị, chẩn đoán và sửa các lỗi xảy ra trên các máy in mạng dễ dàng hơn do số lượng các máy in trong mạng giảm đi và công việc quản trị máy in mạng có thể được thực hiện trên chính máy tính mà người quản trị đang đăng nhập mà không cần trực tiếp đến từng máy in.

### 1.5.2 Sự bảo mật và quản trị được tập trung

Các file và chương trình trên một máy tính có thể được bảo vệ với các quyền chỉ cho các user nào được phép truy xuất và truy xuất ở mức nào. Các user chỉ cần đăng nhập với một tài khoản user hợp lệ sẽ cho phép họ truy xuất dữ liệu và tài nguyên mạng trong giới hạn quyền (permission) đã được cấp. Những tài nguyên mà một user có thể thấy trên mạng có thể bị ẩn đi đối với các user khác.

Các mạng cho phép các user truy xuất dữ liệu của họ từ bất kỳ máy tính nào trong mạng. Vì dữ liệu của họ được lưu trữ trên một máy tính chủ.

Việc sao chép dự phòng dữ liệu (backup) cũng trở nên dễ dàng hơn vì người quản trị chỉ cần backup một máy tính (máy chủ server). Chính việc lưu trữ các dữ liệu quan trọng trên một vị trí tập trung cho phép điều khiển và quản trị dữ liệu chặt chẽ hơn, tiết kiệm thời gian hơn so với việc lưu trữ dữ liệu trên mọi máy tính riêng lẻ.

### 1.5.3 Các dịch vụ thư điện tử (e-mail)

Việc chuyển e-mail giữa các user trên một mạng LAN hoặc giữa các user trên một mạng LAN và Internet được quản lý bởi các *dịch vụ thư tín* (mail service) mạng. Điều kiện để mọi người có thể giao tiếp trên mạng bằng e-mail là mỗi người phải có một địa chỉ e-mail.

### 1.5.4 Các dịch vụ giao tiếp (Communication services)

Các *dịch vụ giao tiếp* mạng cho phép các user bên ngoài kết nối tới mạng từ xa thông qua một đường dây điện thoại và một modem. Các dịch vụ này cũng cho phép các user trên mạng kết nối tới các máy hoặc mạng khác bên ngoài mạng LAN. Đa số các hệ điều hành mạng (Network Operating System – NOS) có các dịch vụ này bên trong, chẳng hạn:

- Windows NT 4.0 có Remote Access Server (RAS)
- Windows 2000 Server có Routing and Remote Access Server (RRAS)
- Netware có Network Access Server (NAS)

Các máy tính đang chạy các dịch vụ giao tiếp được gọi là các *máy chủ giao tiếp* (communication server) và chịu trách nhiệm quản lý các giao tiếp. Một khi user đã đăng nhập vào mạng từ xa và được xác nhận là hợp lệ thông qua máy chủ giao tiếp họ sẽ có các quyền truy xuất mà họ mong muốn giống như đang ngồi ở một máy tính trạm được kết nối vật lý trực tiếp với mạng đó (trừ trường hợp người quản trị hạn chế việc truy xuất khi đăng nhập từ xa).

### 1.5.5 Các dịch vụ Internet

Các *dịch vụ Internet* bao gồm các máy chủ World Wide Web (WWW) và các trình duyệt (browser), khả năng truyền file, sơ đồ định địa chỉ Internet, các bộ lọc bảo vệ. Các dịch vụ này là cần thiết đối với các mạng hiện nay để cho phép giao tiếp và chuyển đổi dữ liệu toàn cầu.

### 1.5.6 Các dịch vụ quản trị (Management services)

Các công việc quản trị mạng trở thành phức tạp hơn đối với các mạng có kích thước lớn, đặc biệt khi nó mở rộng qua các châu lục khác nhau (Các mạng WAN).

Các *dịch vụ quản trị* cho phép những người quản trị mạng quản trị tập trung các mạng lớn và phức tạp. Các công việc quản trị này bao gồm: *theo dõi và điều khiển lưu thông, cân bằng tải, chẩn đoán và cảnh báo các lỗi, quản trị tài nguyên, điều khiển và theo dõi sự cho phép, kiểm tra tính bảo mật, phân bố phần mềm, quản trị địa chỉ, backup và phục hồi dữ liệu.*

## 1.6 Làm thế nào để trở thành một chuyên nghiệp viên về mạng máy tính?

Có nhiều cách để trở thành một người chuyên nghiệp về mạng máy tính. Hoặc được học tập ở các trường đại học, cao đẳng hoặc lấy các bằng cấp thông qua việc học các khoá của các công ty và tham dự các kỳ thi. Một số văn bằng của các công ty bao

gồm: Microsoft Certified Systems Engineer, Novell Network Engineer hoặc các văn bằng của Cisco và Intel.

Một số lĩnh vực chuyên nghành về mạng máy tính là:

- Bảo mật mạng.
- Thiết kế Internet và Intranet.
- Quản trị mạng.
- Tích hợp dữ liệu và tiếng nói.
- Tính toán di dộng và từ xa.
- Tích hợp dữ liệu và cơ chế chống lỗi.
- Kiến thức sâu về các sản phẩm mạng của Microsoft cũng như của Netware.
- Kiến thức sâu về việc cấu hình và quản trị các thiết bị tìm đường (router)

Ngoài những kiến thức kỹ thuật sâu sắc (kỹ năng "cứng"), một người chuyên nghiệp về mạng máy tính cũng cần phải có các kỹ năng "mềm" tốt. Các kỹ năng này bao gồm:

- Kỹ năng quan hệ với khách hàng.
- Kỹ năng giao tiếp bằng lời và bằng văn bản.
- Vừa có khả năng làm việc độc lập vừa có khả năng làm việc tập thể.
- Có khả năng quản lý và lãnh đạo.
- Tính tin cậy cao.

# Câu hỏi ôn tập chương 1

1. Một số các máy tính phân bố trên một vùng địa lý rộng và được kết nối với nhau bằng các cáp và các thiết bị không dây là một ……

a. LAN b. MAN
c. WAN d. Virtual network.

2. Các thành phần cơ bản của kiến trúc mạng là ……(chọn 2)

a. Topology b. Form of the network
c. Protocols d. Physical Media

3. **Hai** mô hình mạng là …….

a. Wire b. Peer to peer
c. Wireless d. Server Based Network

4. Có **hai** loại hình trạng :

a. Physical topology
b. Simple topology
c. Complex topology
d. Logical topology

5. **Một** trong những đặc điểm của mạng LAN:

a. Khoảng cách xa nhất giữa hai trạm lớn hơn 100 km
b. Khoảng cách xa nhất giữa hai trạm vào khoảng vài chục km
c. Cả hai câu trên đều đúng.

6. Lịch sử mạng máy tính cũng chính là lịch sử của Internet

a. Đúng b. Sai

7. Những nhược điểm của mạng server-based là: (chọn 2)

a. Cài đặt phức tạp
b. Bảo mật kém
c. Không có cơ chế sao chép dữ liệu tập trung
d. Chi phí đắt hơn so với mạng peer-to-peer

8. Những nhược điểm của mạng peer to peer là: (chọn 2)

a. Cài đặt phức tạp
b. Bảo mật kém
c. Quản trị phức tạp
d. Không có cơ chế sao chép dữ liệu tập trung

9. Trong mạng peer-to-peer không tồn tại bất kỳ máy server nào.

a. Đúng b. Sai

10. Những dịch vụ thông thường nhất trên mạng là: (chọn 3 )

a. Dịch vụ File b. Dịch vụ Email
c. Dịch vụ thư mục d. Dịch vụ in
e. Dịch vụ chia xẻ

# CHƯƠNG 2 - MÔ HÌNH OSI

## MỤC TIÊU CỦA CHƯƠNG

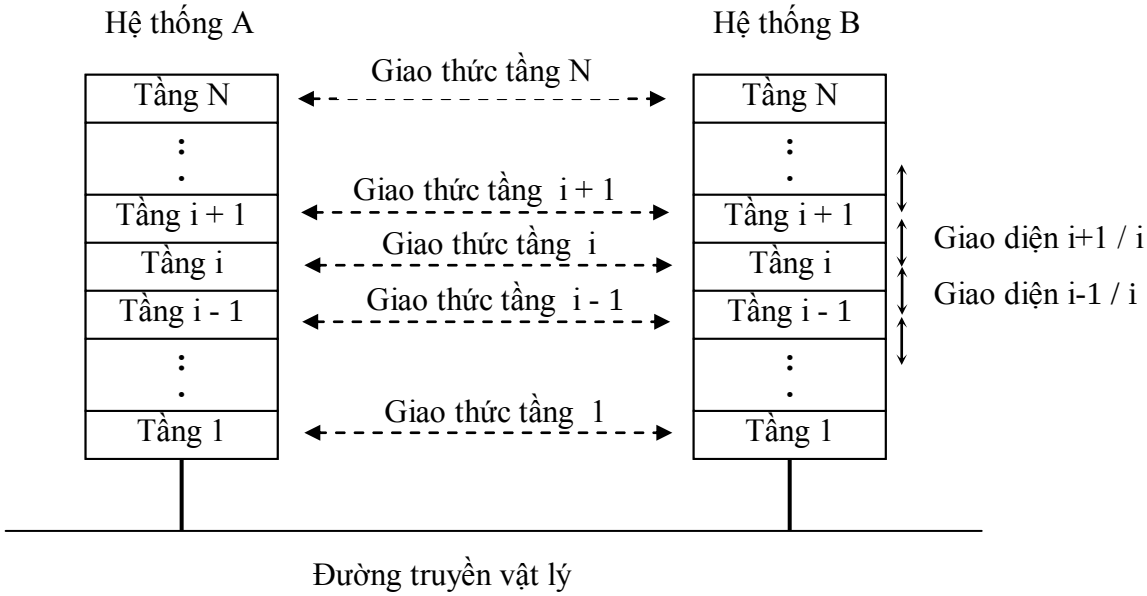
*Kết thúc chương này, sinh viên sẽ có thể:*

- Hiểu một cách khái quát về kiến trúc phân tầng mạng máy tính.
- Nắm được tổng quan về mô hình OSI
- Hiểu và nắm được ý nghĩa cũng như chức năng của các tầng trong mô hình OSI
- Áp dụng mô hình OSI trong việc phân tích một quá trình trong mạng máy tính.
- Hiểu được các thành phần của một khuôn dạng (frame) dữ liệu.

## 2.1 Kiến trúc phân tầng và mô hình OSI (Open System Interconnect)

### 2.1.1 Kiến trúc phân tầng

Để giảm độ phức tạp của việc thiết kế và cài đặt mạng, hầu hết các mạng máy tính hiện có đều được phân tích thiết kế theo quan điểm phân tầng (layering). Mỗi hệ thống thành phần của mạng được xem như một cấu trúc đa tầng, trong đó mỗi tầng được xây trên tầng trước nó. Số lượng các tầng cũng như tên và chức năng của mỗi tầng là tuỳ thuộc vào các nhà thiết kế. Tuy nhiên, trong hầu hết các mạng, mục đích của mỗi tầng là cung cấp một số *dịch vụ* nhất định cho tầng cao hơn. Hình 2.1 là một kiến trúc phân tầng tổng quát, với giả thiết A và B là hai hệ thống máy tính thành phần của mạng được nối với nhau.




*Hình 2.1* Minh hoạ kiến trúc phân tầng tổng quát

*Nguyên tắc của kiến trúc phân tầng là:*

- Mỗi hệ thống trong một mạng đều có cùng cấu trúc tầng (số lượng tầng, chức năng của mỗi tầng là như nhau).
- Sau khi xác định cấu trúc tầng, công việc kế tiếp là định nghĩa mối quan hệ (giao diện) giữa hai tầng kề nhau và mối quan hệ giữa hai tầng đồng mức ở hai hệ thống nối kết với nhau. Nếu một hệ thống mạng có N tầng thì tổng số các quan hệ (giao diện) cần phải xây dựng là 2*N –1.
- Trong thực tế, dữ liệu không được truyền trực tiếp từ tầng thứ i của hệ thống này sang tầng thứ i của hệ thống khác (trừ trường hợp tầng thấp nhất trực tiếp sử dụng đường truyền vật lý để truyền các chuỗi bít (0,1) từ hệ thống này sang hệ thống khác). Qui ước dữ liệu ở bên *hệ thống gửi* (sender) được truyền từ tầng trên xuống tầng dưới và truyền sang *hệ thống nhận* (receiver) bằng đường truyền vật lý và cứ thế đi ngược lên các tầng trên.

### 2.1.2 Tổng quan về mô hình OSI

Khi thiết kế mạng máy tính, các nhà thiết kế tự do lựa chọn kiến trúc riêng của mình. Từ đó dẫn đến tình trạng không tương thích giữa các mạng: phương pháp truy nhập đường truyền khác nhau, sử dụng họ giao thức khác nhau v.v… Sự không tương thích đó làm trở ngại cho sự tương tác của người sử dụng các mạng khác nhau. Nhu cầu trao đổi thông tin càng cao thì trở ngại đó càng lớn, đến mức không thể chấp nhận được đối với người sử dụng. Tình hình đó làm cho các nhà sản xuất và các nhà nghiên cứu, thông qua các tổ chức chuẩn hoá quốc gia và quốc tế cần phải xây dựng được một khung chuẩn về kiến trúc mạng để làm căn cứ cho các nhà thiết kế và chế tạo các sản phẩm về mạng.

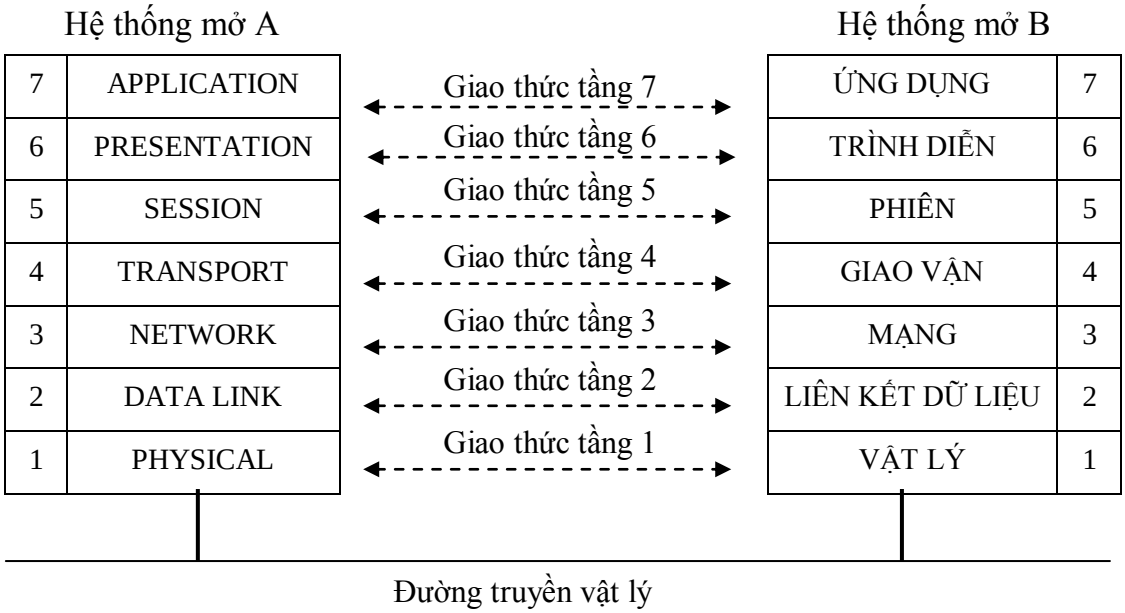
Vì lý do đó, Tổ chức tiêu chuẩn hoá quốc tế (International Organization for Standardization – ISO) đã lập ra một tiểu ban nhằm phát triển một khung chuẩn về kiến trúc mạng. Kết quả là vào năm 1984, mô hình tham chiếu OSI (Open System Interconnection Reference Model) ra đời.

Mô hình OSI là một tập các mô tả chuẩn cho phép các máy tính khác nhau giao tiếp với nhau theo cách *mở*. Từ "mở" ở đây nói lên khả năng 2 hệ thống khác nhau có thể kết nối để trao đổi thông tin với nhau nếu chúng tuân thủ mô hình tham chiếu và các chuẩn liên quan. Mô hình OSI phân chia kiến trúc mạng máy tính thành 7 tầng – tầng *Vật lý* (**Physical**), tầng *Liên kết Dữ liệu* (**Data Link**), tầng *Mạng* (**Network**), tầng *Giao vận* (**Transport**), tầng *Phiên* (**Session**), tầng *Trình diễn* (**Presentation**) và tầng *Ứng dụng* (**Application**). Mỗi tầng khác nhau có tập các chức năng riêng và chỉ giao tiếp với các tầng kề cận trên và dưới và giao tiếp với tầng đối diện (đồng mức) trên các máy tính khác. (Hình 2.2)

Từ khi có mô hình OSI, nhiều nhà sản xuất máy tính đã thay đổi kiến trúc mạng phân tầng của họ để tuân thủ các tầng của mô hình OSI. Ví dụ, các chức năng giao tiếp được phân chia thành một tập các tầng. Mỗi tầng thực hiện các chức năng cần thiết để giao tiếp với các hệ thống khác. Mỗi tầng dựa trên tầng kế tiếp bên dưới để thực hiện nhiều hơn các chức năng nguyên thuỷ (primitive function). Bản thân mỗi

tầng cũng cung cấp các dịch vụ cho tầng kế tiếp phía trên nó. Nói một cách khác tầng *N* sử dụng các dịch vụ của tầng *N-1* và cung cấp các dịch vụ cho tầng *N+1*.

Một cách lý tưởng, các tầng nên được định nghĩa sao cho những thay đổi trong một tầng không đòi hỏi những thay đổi trong các tầng khác. Nói một cách khác, ý tưởng của việc phân tầng là chia một vấn đề lớn thành một số các vấn đề nhỏ có thể quản lý được.




*Hình 2.2* Mô hình OSI 7 tầng

## 2.2 Ý nghĩa và chức năng của các tầng trong mô hình OSI

### 2.2.1 Tầng vật lý (Physical Layer)

Tầng *vật lý* là tầng thấp nhất trong mô hình OSI. Tầng này liên quan đến các qui tắc truyền dòng bit không có cấu trúc qua đường truyền vật lý. Tầng này định nghĩa:

- Cấu trúc mạng vật lý.
- Những mô tả về mặt cơ và điện cho việc sử dụng đường truyền.
- Các qui tắc mã hoá việc truyền các bit và các qui tắc định thời.

Tầng vật lý không bao gồm việc mô tả đường truyền và không cung cấp bất kỳ cơ chế kiểm soát lỗi nào.

Phần cứng kết nối mạng được coi là thuộc về tầng vật lý bao gồm:

- Các bộ giao tiếp mạng (Network Interface Card – NIC, Adapter, v.v…)
- Các bộ tập trung (Concentrator, Hub), các bộ chuyển tiếp (Repeater) dùng để tái sinh các tín hiệu điện.
- Các đầu nối (connector) cung cấp giao tiếp cơ để kết nối các thiết bị với đường truyền (các cáp, các đầu nối BNC – BayoNette Connector)

- Các bộ điều chế và giải điều chế (MODEM – MOdulation-DEModulation) thực hiện việc chuyển đổi giữa tín hiệu *số hoá* (digital) và tín hiệu *tương tự* (analog).

### 2.2.2 Tầng liên kết dữ liệu (Data Link Layer)

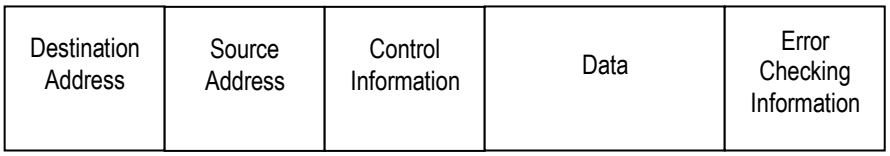
Tầng *liên kết dữ liệu* chịu trách nhiệm điều khiển tất cả các giao tiếp giữa tầng mạng bên trên nó và tầng vật lý bên dưới nó. Dữ liệu nhận được từ tầng mạng được phân chia thành các khối riêng biệt (khuôn dạng - *frame*), sau đó chúng được đưa tới tầng vật lý và cuối cùng truyền ra mạng. Mục đích chính của việc thực thi giao thức tầng liên kết dữ liệu là:

- Tổ chức các bit thuộc tầng vật lý thành các nhóm thông tin được gọi là các *khuôn dạng* (frame - giống như một byte, một frame là một dãy liên tục các bit được nhóm lại với nhau như một đơn vị dữ liệu)
- Phát hiện và sửa sai lỗi.
- Kiểm soát luồng dữ liệu.
- Định danh các máy tính trên mạng .

Tầng liên kết dữ liệu bổ sung thông tin điều khiển riêng của nó vào phía trước gói dữ liệu. Thông tin này bao gồm:

- Địa chỉ (vật lý) của máy nguồn và máy đích (Source address, Destination address) .
- Thông tin về chiều dài của frame.

Một khi dữ liệu được truyền trên mạng, tầng liên kết dữ liệu chờ thông tin phản hồi (Acknowledge –ACK) từ máy tính nhận, báo cho biết là nó đã nhận được tất cả các gói. Trái lại, các gói còn thiếu sẽ được truyền lại. Tầng liên kết dữ liệu không liên quan đến việc tại sao một gói không đến được đích, tầng này chỉ quan tâm đến sự kiện là, nếu một gói nào đó không đến đích thì nó phải được truyền lại. Như vậy tầng liên kết dữ liệu cung cấp các phương tiện đảm bảo sự tin cậy cho việc truyền thông tin.




*Hình 2.3* Một frame dữ liệu được đơn giản hoá

Các thiết bị kết nối mạng được xem như thuộc về tầng liên kết dữ liệu bao gồm:

- Bridges (Các cầu nối)
- Intelligent hubs (các hub thông minh)

Các chức năng của tầng liên kết dữ liệu bình thường được phân tách thành hai tầng con (sub-layer):

1. *Điều khiển truy xuất đường truyền* (Media Access Control - **MAC**)

   Tầng con ***MAC*** là lớp con phía dưới của tầng liên kết dữ liệu. Nó chịu trách nhiệm bổ sung địa chỉ vật lý của máy tính đích vào frame dữ liệu.

2. *Điều khiển liên kết lôgíc* (Logical Link Control – **LLC**)

   Tầng con ***LLC*** là lớp con phía trên của tầng liên kết dữ liệu và chịu trách nhiệm cung cấp một giao tiếp chung cũng như cung cấp tính tin cậy và các dịch vụ kiểm soát luồng dữ liệu. Nó thiết lập và duy trì liên kết cho việc truyền các frame dữ liệu từ thiết bị này tới thiết bị khác.

### 2.2.3 Tầng mạng (Network Layer)

Tầng mạng là tầng thứ ba của mô hình OSI. Mục tiêu chính của nó là *di chuyển dữ liệu tới các vị trí mạng xác định*. Để làm điều này, nó dịch các địa chỉ lôgíc thành địa chỉ vật lý tương ứng và sau đó quyết định con đường tốt nhất cho việc truyền dữ liệu từ máy gửi tới máy nhận. Điều này tương tự như công việc mà tầng liên kết dữ liệu thực hiện thông qua việc định địa chỉ thiết bị vật lý. Tuy nhiên, việc định địa chỉ của tầng liên kết dữ liệu chỉ hoạt động trên một *mạng đơn*. Tầng mạng mô tả các phương pháp di chuyển thông tin giữa *nhiều mạng độc lập* (và thường là không giống nhau) – được gọi là *liên mạng* (internetwork)

Ví dụ, các mạng cục bộ (LAN) Token Ring hoặc Ethernet có các kiểu địa chỉ khác nhau. Để kết nối hai mạng này, ta cần một cơ chế định địa chỉ giống nhau mà có thể được hiểu bởi cả hai loại mạng đó. Khả năng này được cung cấp bởi giao thức *chuyển đổi gói Internet* (Internet Packet Exchange – IPX) – một giao thức tầng mạng trong hệ điều hành Novell Netware.

Việc định địa chỉ của tầng liên kết dữ liệu để chuyển dữ liệu tới tất cả các thiết bị được gắn tới một mạng đơn và nhờ vào các thiết bị nhận để xác định xem dữ liệu có được truyền tới nó hay không. Trái lại, tầng mạng chọn một con đường xác định qua một liên mạng và tránh gửi dữ liệu tới các mạng không liên quan. Mạng thực hiện điều này bằng việc *chuyển mạch* (switching), *định địa chỉ* và các *giải thuật tìm đường*. Tầng mạng cũng chịu trách nhiệm đảm bảo ***định tuyến*** (routing) dữ liệu đúng qua một liên mạng bao gồm các mạng không giống nhau.

Một vấn đề có thể nảy sinh khi việc định tuyến dữ liệu qua một liên mạng không đồng dạng là sự khác nhau của kích thước gói dữ liệu mà mỗi mạng có thể chấp nhận. Một mạng không thể gửi dữ liệu trong các gói có kích thước lớn hơn kích thước của gói dữ liệu mà một mạng khác có thể nhận được. Để giải quyết vấn đề này, tầng mạng thực hiện một công việc được gọi là ***sự phân đoạn*** (segmentation). Với sự phân đoạn, một gói dữ liệu được phân tách thành các *gói* nhỏ hơn mà mạng khác có thể hiểu được - gọi là các ***packet***. Khi các gói nhỏ này đến mạng khác, chúng được ***hợp nhất*** (reassemble) thành gói có kích thước và dạng ban đầu. Toàn bộ sự *phân đoạn* và *hợp nhất* này xảy ra ở tầng mạng của mô hình OSI.

### 2.2.4 Tầng giao vận (Transport Layer)

Tầng giao vận nâng cấp các dịch vụ của tầng mạng. Công việc chính của tầng này là đảm bảo dữ liệu được gửi từ máy nguồn phải *tin cậy, đúng trình tự* và *không có*

*lỗi* khi tới máy đích. Để đảm bảo truyền dữ liệu *tin cậy*, tầng giao vận dựa trên cơ chế *kiểm soát lỗi* được cung cấp bởi các tầng bên dưới. Tầng này là cơ hội cuối cùng để sửa lỗi. Dữ liệu cùng với thông tin điều khiển mà tầng giao vận quản lý gọi là các *phân đoạn* (segment)

Tầng giao vận cũng chịu trách nhiệm *kiểm soát luồng dữ liệu.* Tốc độ truyền dữ liệu được xác định dựa trên khả năng mà máy đích có thể nhận các gói dữ liệu được gửi đến nó như thế nào. Dữ liệu ở máy gửi được phân chia thành các gói có kích thước tối đa mà loại mạng đó có thể quản lý. Chẳng hạn, một mạng Ethernet không thể điều khiển các gói có kích thước lớn hơn 1500 byte, vì thế tầng giao vận nhận dữ liệu và chia nó thành các gói 1500 byte. Mỗi gói con này được gắn một số trình tự, dùng để hợp nhất nó ở vị trí đúng bởi tầng giao vận của máy nhận. Công việc này được gọi là ***sắp xếp theo trình tự*** (sequencing).

Khi gói dữ liệu đến máy nhận, nó được hợp nhất theo đúng trình tự như lúc gửi. Sau đó một thông tin *báo nhận* (acknowledgement - ACK) được gửi quay trở lại máy gửi để báo cho nó biết rằng gói dữ liệu đã đến chính xác. Nếu có lỗi trong gói dữ liệu thì một yêu cầu truyền lại gói đó được gửi quay trở lại thay thế cho ACK. Nếu máy gửi ban đầu không nhận được thông tin ACK (hoặc yêu cầu truyền lại) trong một khoảng thời gian định trước, gói dữ liệu gửi được xem như bị thất lạc hoặc bị hư, khi đó nó sẽ được gửi lại.

Trong mạng TCP/IP, các chức năng TCP (Transmission Control Protocol) thuộc về tầng giao vận. Trong mạng Novell Netware sử dụng IPX/SPX thì giao thức SPX (Sequence Packet Exchange) hoạt động ở tầng giao vận.

### 2.2.5 Tầng phiên (hay Tầng giao dịch - Session Layer)

Tầng phiên quản lý các liên kết của user trên mạng để cung cấp các dịch vụ cho user đó. Ví dụ một người sử dụng đăng nhập vào một máy tính mạng để lấy file thì một phiên (hay một giao dịch / một liên kết) được thiết lập cho mục đích truyền file.

Tầng phiên tạo điều kiện thuận lợi cho việc giao tiếp giữa các hệ thống *yêu cầu* dịch vụ và các hệ thống *cung cấp* dịch vụ. các phiên giao tiếp được kiểm soát thông qua cơ chế *thiết lập, duy trì, đồng bộ hoá* và *quản lý* các phiên (hay còn gọi là cuộc hội thoại – dialogue) giữa các thực thể truyền thông. Tầng này cũng trợ giúp các tầng trên định danh và kết nối tới các dịch vụ có thể sử dụng trên mạng. Nếu một phiên giao tiếp bị ngắt, tầng phiên xác định vị trí để khởi tạo lại việc truyền phát một khi phiên giao tiếp đó được tái kết nối. Tầng phiên cũng chịu trách nhiệm xác định thời hạn của phiên giao tiếp. Nó xác định máy tính hoặc nút nào có thể truyền đầu tiên và truyền trong bao lâu.

Tầng phiên sử dụng thông tin địa chỉ lôgíc được cung cấp bởi các tầng bên dưới để định danh tên và địa chỉ của các máy chủ mà các tầng trên đòi hỏi.

### 2.2.6 Tầng trình diễn (Presentation Layer)

Tầng trình diễn quản lý cách thức dữ liệu được biểu diễn. Nó là trình dịch giữa ứng dụng và mạng. Có nhiều cách để biểu diễn dữ liệu, chẳng hạn như các bảng mã ASCII và EDBCDIC cho các file văn bản. Tầng trình diễn biến đổi dữ liệu sang một

định dạng mà mạng có thể hiểu được. Nó cũng chịu trách nhiệm *mã hoá* (encrypt) và *giải mã* (decrypt) dữ liệu - chẳng hạn như dữ liệu được mã hoá dữ liệu nó được gửi tới ngân hàng, nếu ta giao dịch trực tuyến với ngân hàng qua Internet.

### 2.2.7 Tầng ứng dụng (Application Layer)

Tầng ứng dụng chứa các giao thức và chức năng đòi hỏi bởi ứng dụng của người sử dụng để thực hiện các công việc truyền thông. Nó không liên quan đến các ứng dụng thực sự đang hoạt động như Microsoft Word hoặc Adobe Photoshop.

Các chức năng chung bao gồm:

- Các giao thức cung cấp các dịch vụ file từ xa, như các dịch vụ mở file, đóng file, đọc file, ghi file và chia xẻ truy xuất tới file.
- Các dịch vụ truyền file và truy xuất cơ sở dữ liệu từ xa.
- Các dịch vụ quản lý thông báo cho các ứng dụng thư điện tử.
- Các dịch vụ thư mục toàn cục để định vị tài nguyên trên mạng.
- Một cách quản lý đồng nhất các chương trình giám sát hệ thống và các thiết bị.
- v.v….

Nhiều dịch vụ này được gọi là *các giao tiếp lập trình ứng dụng* (Application Programming Interface – API). Các API là những thư viện lập trình mà người phát triển ứng dụng có thể sử dụng để viết các ứng dụng mạng.

## 2.3 Áp dụng mô hình OSI

Bảng sau đây tổng kết các chức năng của mô hình OSI:

| Tầng | Chức năng |
|---|---|
| Ứng dụng | Chuyển thông tin từ chương trình này tới chương trình khác. |
| Trình diễn | Điều khiển định dạng văn bản và hiển thị chuyển đổi mã. |
| Phiên | Thiết lập, duy trì và kết hợp các phiên truyền thông. |
| Giao vận | Đảm bảo phân phát chính xác dữ liệu. |
| Mạng | Tìm đường và quản lý việc truyền thông báo. |
| Liên kết Dữ liệu | Mã hoá, định địa chỉ và truyền thông tin. |
| Vật lý | Quản lý kết nối phần cứng |

Cách dễ nhất để xem xét mô hình OSI và áp dụng nó trong hoạt động mạng là tìm hiểu một quá trình cụ thể diễn ra trong mạng. Một trong những công việc được thực hiện nhiều lần trong một ngày trên hầu hết các mạng là đọc một thư điện tử (E-mail).

Sau khi người sử dụng đăng nhập vào trong mạng và khởi tạo chương trình e-mail, quá trình kiểm tra thư mới bắt đầu.

Đầu tiên *tầng ứng dụng* xác nhận yêu cầu (request) về thư thông qua một API chuẩn được xây dựng trong ứng dụng. Tầng ứng dụng nhận yêu cầu này và chuyển nó thành một yêu cầu dữ liệu được đọc từ máy chủ e-mail. Yêu cầu được chuyển tới *tầng trình diễn*.

*Tầng trình diễn* nhận yêu cầu và xác định xem nó nên được định dạng như thế nào theo kiểu mạng riêng mà yêu cầu đang hoạt động trên đó. Tầng này cũng xác định xem có bất kỳ đòi hỏi nào về *mã hoá* hay không. Dữ liệu sau khi được định dạng (và có thể được mã hoá) được truyền tới *tầng phiên*.

*Tầng phiên* nhận yêu cầu và gán một thẻ (token) dữ liệu tới nó. Thẻ này là một đơn vị dữ liệu điều khiển đặc biệt mà nó báo cho phần còn lại của mạng là người sử dụng có quyền truyền dữ liệu. Dữ liệu và thẻ được truyền tới *tầng giao vận.*

Khi tới *tầng giao vận,* dữ liệu và các thông tin điều khiển được chia thành các khối có kích thước có thể quản lý được. Nếu dữ liệu quá lớn để thích hợp trong một frame ở *tầng liên kết dữ liệu, tầng giao vận* sẽ phân chia dữ liệu thành các khối nhỏ hơn và gán một *số trình tự* (sequence number) hay *định danh* (identifier) cho mỗi khối. Sau đó từng khối được truyền tới *tầng mạng.*

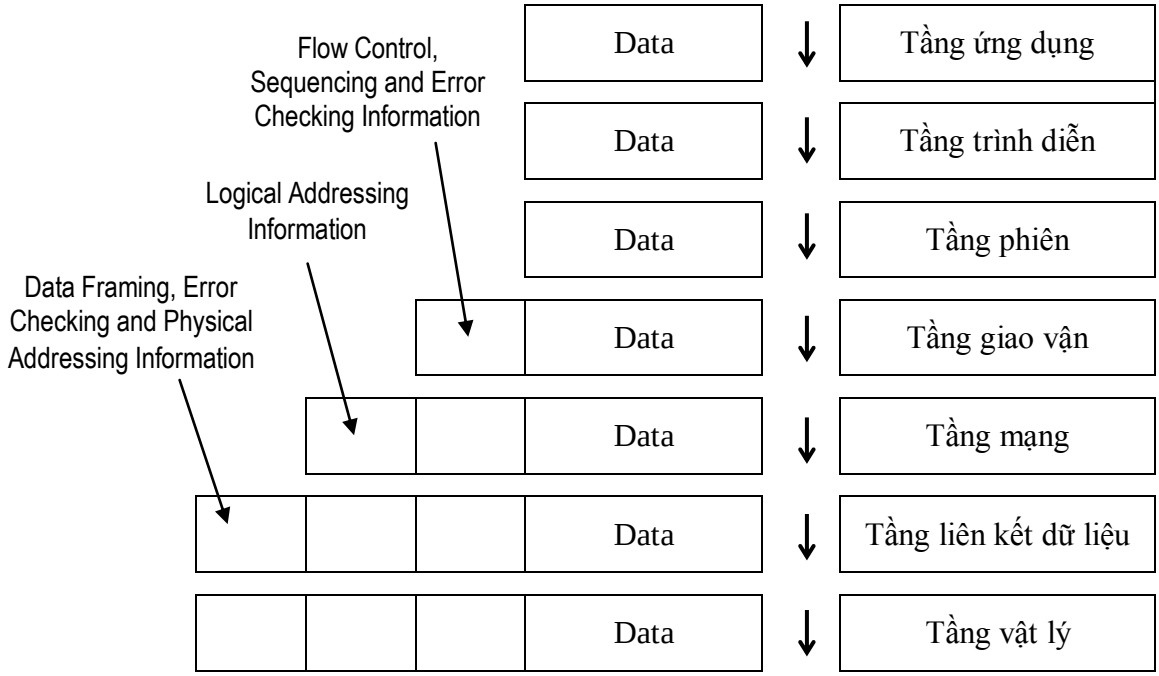
*Tầng mạng* bổ sung thông tin *địa chỉ lôgíc* tới dữ liệu mà nó nhận được từ *tầng giao vận* sao cho các tầng kế tiếp sẽ biết cả địa chỉ nguồn và đích của dữ liệu . Các khối dữ liệu tiếp theo được truyền cùng với thông tin định địa chỉ tới *tầng liên kết dữ liệu*.

Một khi dữ liệu đến được *tầng liên kết dữ liệu,* chúng được đóng gói thành các frame riêng rẽ. Mỗi frame này kèm theo giải thuật kiểm tra lỗi được biết như là **Frame Check Sequence (FCS) -** vùng để ghi mã kiểm soát lỗi – được chèn ở cuối mỗi frame. *Tầng liên kết dữ liệu* sau đó bổ sung thêm một header tới frame trước khi truyền nó tới *tầng vật lý*. Phần header này bao gồm *địa chỉ vật lý* của cả hai nút gửi và nút nhận.

Khi dữ liệu bắt đầu tới card giao tiếp mạng (NIC) ở *tầng vật lý,* nó được gửi ra mạng. *Tầng vật lý* không bổ sung bất kỳ thứ gì tới frame và tầng này cũng không quan tâm xem cái gì có trong frame. Nó đơn giản chỉ lấy dữ liệu (các bit) và truyền nó trên mạng.

Một khi các gói dữ liệu đến được nút nhận, chúng được lấy lại nhờ NIC của *tầng vật lý* bên hệ thống nhận và được truyền tiếp lên qua các tầng hệ thống đó. Mỗi một tầng dịch thông tin được bổ sung bởi các tầng tương ứng bên hệ thống gửi và sau đó truyền gói lên tầng bên trên cho tới khi cuối cùng gói đó được hợp nhất và *yêu cầu* được thực thi.

Nút nhận sau đó tạo ra một *đáp ứng* (response) và gửi nó quay trở lại nút gửi ban đầu đi theo trình tự chính xác như mô tả ở trên. Mỗi tầng kế tiếp của mô hình OSI bổ sung thông tin điều khiển, thông tin định dạng hay thông tin định địa chỉ tới dữ liệu mà nó điều khiển. Hệ thống nhận phiên dịch và sau đó sử dụng thông tin bổ sung khi nó đảo ngược tiến trình, truyền dữ liệu từ *tầng vật lý* lên tới *tầng ứng dụng.*




*Hình 2.4* Dữ liệu được truyền qua mô hình OSI

Bảng sau đây tổng kết đơn vị dữ liệu do các tâng quản lý:

| **Tầng** | **Đơn vị dữ liệu** |
|---|---|
| Tầng ứng dụng, trình diễn, phiên | Data |
| Tầng giao vận | Segment |
| Tầng mạng | Packet |
| Tầng liên kết dữ liệu | Frame |
| Tầng vật lý | Bit |

## 2.4 Mô tả các thành phần của khuôn dữ liệu (Frame)

Như ta đã thấy ở phần trên, dữ liệu khi truyền ngang qua mạng được phân tách thành những khối nhỏ, có kích thước phụ thuộc vào hình trạng lôgíc của mạng đó. Như đối với mạng Ethernet không thể sử dụng các khối dữ liệu lớn hơn 1500 byte. Các khối dữ liệu nhỏ này được gọi là các **frame** (khung hoặc khuôn dạng).

Có hai loại frame: **Ethernet** và **Token Ring** – tương ứng với tên hai loại mạng được sử dụng thông thường nhất.

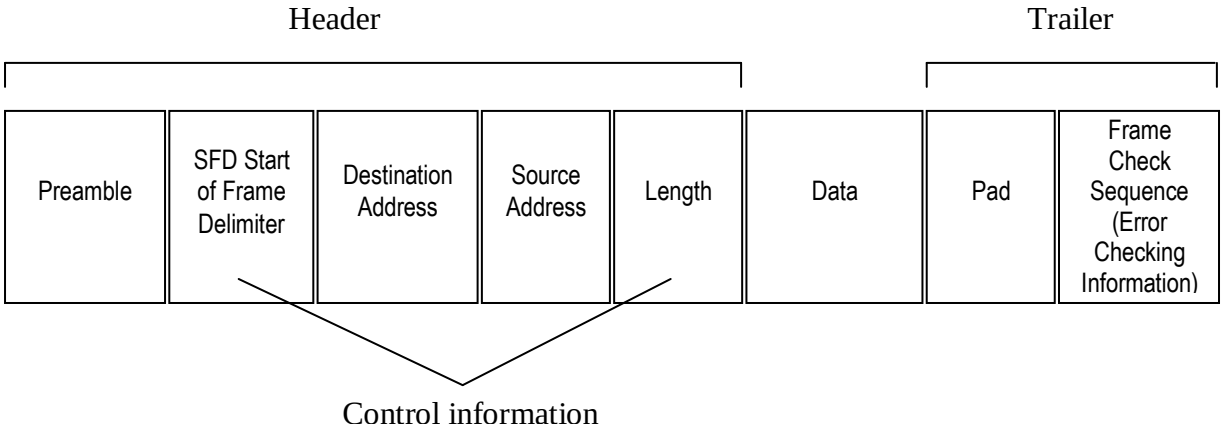
Công ty Xerox Corporation bắt đầu phát triển Ethernet vào năm 1970. Sau đó do liên kết giữa Xerox Corp. với DEC và Intel, Ethernet đã được cải tiến và hiện giờ có 4 công nghệ Ethernet chủ yếu đang được sử dụng – 10Base2, 10Base5, 10BaseT và 100BaseT.

Token Ring đã được phát triển bởi IBM vào năm 1980 và dựa trên liên kết giữa các nút với công nghệ vòng (ring): một thẻ bài (token) được truyền quanh các

nút. Một nút chỉ có thể truyền dữ liệu trên mạng sau khi nó nhận được thẻ bài. Cáp nối mạng hình thành một vòng (ring hoặc circle) và các tín hiệu dữ liệu được truyền chỉ theo một hướng quanh vòng.

Mặc dù về lý thuyết có thể truyền cả hai frame Ethernet và Token Ring trên cùng một mạng, nhưng điều này không thực hiện trong thực tế. Giao tiếp Ethernet không thể phiên dịch các frame Token Ring và trái lại. Một mạng luôn chỉ là Ethernet hoặc Token Ring chứ không thể đồng thời cả hai. Tuy nhiên có thể kết hợp các giao thức trên cùng trên một mạng. Chẳng hạn, có thể sử dụng cả hai bộ giao thức TCP/IP và IPX/SPX trên mạng mạng Ethernet, vì cả hai giao thức này cùng sử dụng một kiểu frame dữ liệu.

### 2.4.1 Một khuôn dữ liệu Ethernet điển hình



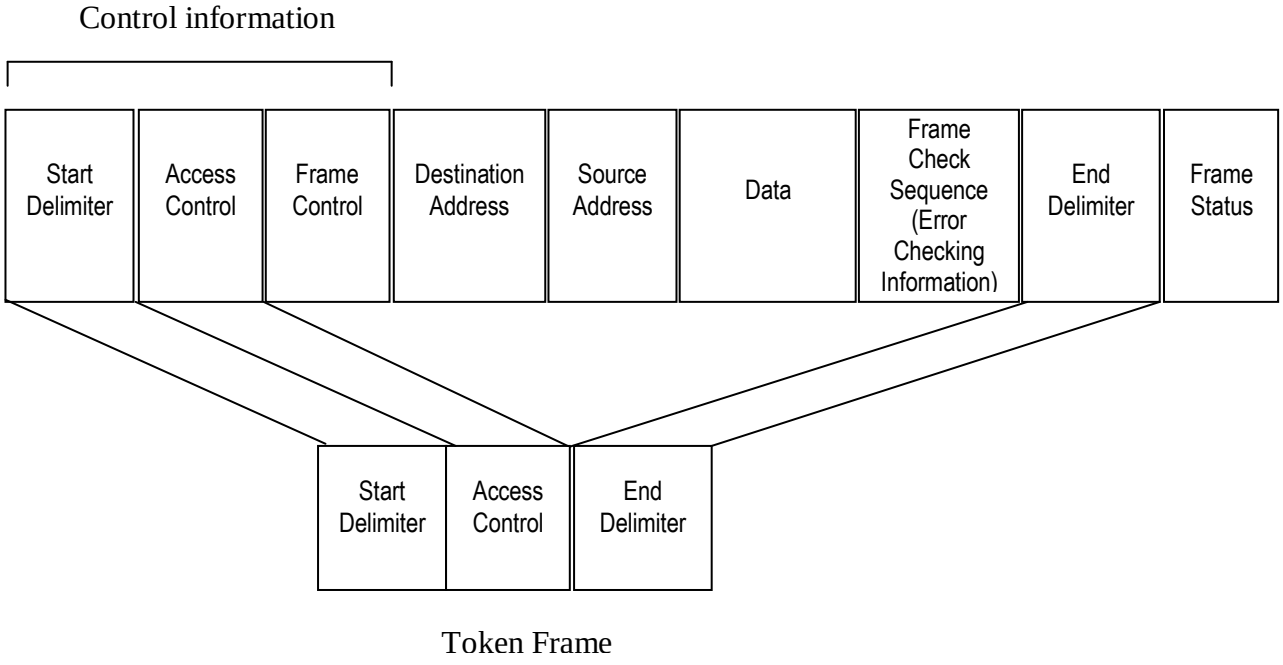

*Hình 2.5* Một khuôn dữ liệu Ethernet điển hình

Các thành phần của frame Ethernet 802.3 bao gồm:

- *Preamble* (Phần mở đầu)– Đánh dấu bắt đầu của toàn bộ frame, là tín hiệu thông báo tới mạng rằng dữ liệu đang truyền. (Vì trường này là một phần của quá trình giao tiếp, nên nó không được tính vào kích thước của frame)
- *Start of Frame Delimiter (SFD)* – Chứa thôngng tin khởi đầu của việc định địa chỉ frame.
- *Destination Address* – Chứa địa chỉ của nút đích.
- *Source Address* – Chứa địa chỉ của nút nguồn.
- *Length (LEN)* – Chứa chiều dài của gói.
- *Data* – Chứa dữ liệu được truyền từ nút nguồn.
- *Pad* – Được sử dụng để tăng kích thước của frame tới kích thước yêu cầu nhỏ nhất là 46 byte.

- *Frame Check Sequence (FCS)* – Cung cấp một giải thuật để xác định xem dữ liệu nhận được có chính xác hay không. Giải thuật được sử dụng thông thường nhất là **Cyclic Redundancy Check (CRC).**

### 2.4.2 Một khuôn dữ liệu Token Ring điển hình




*Hình 2.6* Một khuôn dữ liệu Token Ring điển hình

Các thành phần của frame Token ring 802.5 bao gồm:

- *Start Delimiter (SD)* – Báo hiệu bắt đầu gói. Nó là một trong ba trường tạo thành khuôn dạng Token Ring.
- *Access Control (AC)* – Chứa thông tin về độ ưu tiên của frame. Nó là trường thứ hai tạo thành khuôn dạng Token Ring.
- *Frame Control (FC)* – Định nghĩa kiểu của frame, được dùng trong Frame Check Sequence.
- *Destination Address* – Chứa địa chỉ của nút đích.
- *Source Address* – Chứa địa chỉ của nút nguồn.
- *Data* – Chứa dữ liệu được truyền từ nút nguồn, cũng có thể chứa thông tin quản lý và tìm đường.
- *Frame Check Sequence (FCS)* – Được sử dụng để kiểm tra tính toàn vẹn của frame.
- *End Delimiter (ED)* – Báo hiệu kết thúc frame. Nó là trường thứ ba của khuôn dạng Token Ring.

- *Frame Status (FS)* – Báo hiệu nút đích nhận dạng và sao chép đúng frame hay không.

### 2.4.3 Giới thiệu các chuẩn đặc tả mạng IEEE 802.x

Tổ chức tiêu chuẩn hoá Quốc tế (ISO) chịu trách nhiệm xây dựng mô hình OSI. Chính ISO cũng thông qua một tập các chuẩn được gọi là đề án "Project 802", được dùng để chuẩn hoá các thành phần vật lý của một mạng. Các chuẩn này do Viện Kỹ thuật Điện và Điện tử (Institute of Electrical and Electronic Engineers – IEEE) xây dựng, bao gồm các vấn đề liên quan đến khả năng kết nối, môi trường truyền mạng, các giải thuật kiểm tra lỗi, sự mã hoá và các công nghệ khác.

Bảng sau đây tổng quát hoá các chuẩn trong đề án "Project 802" :

| Chuẩn | Tên | Giải thích |
|---|---|---|
| 802.1 | Internetworking | Bao gồm việc định tuyến, tạo cầu nối, và các giao tiếp liên mạng. |
| 802.2 | Logical Link Control | Liên quan tới việc kiểm soát lỗi và kiểm soát luồng dữ liệu qua các frame. |
| 802.3 | Ethernet LAN | Bao gồm tất cả các dạng đường truyền và giao tiếp Ethernet |
| 802.4 | Token Bus LAN | Bao gồm tất cả các dạng đường truyền và giao tiếp Token Bus |
| 802.5 | Token Ring LAN | Bao gồm tất cả các dạng đường truyền và giao tiếp Token Ring |
| 802.6 | Metropolitan Area Network (MAN) | Bao gồm các công nghệ, định địa chỉ và các dịch vụ MAN |
| 802.7 | Broadband Technical Advisory Group | Bao gồm môi trường truyền, giao tiếp và các thiết bị khác cho mạng băng tần dải rộng. |
| 802.8 | Fibre-Optic Technical Advisory Group | Bao gồm đường truyền cáp quang và các công nghệ cho các loại mạng khác nhau. |
| 802.9 | Integrated Voice / Data Networks | Bao gồm sự tích hợp tiếng nói và dữ liệu qua một đường truyền mạng. |
| 802.10 | Network Security | Bao gồm các vấn đề về kiểm soát truy xuất mạng, sự mã hoá, xác nhận và các vấn đề bảo mật khác. |
| 802.11 | Wireless Networks | Các chuẩn cho mạng không dây. |
| 802.12 | High-Speed Networking | Bao gồm các công nghệ 100Mbs-plus, kể cả 100BaseVG-AnyLAN |

# Câu hỏi ôn tập chương 2

1. Mục tiêu của việc phân tích thiết kế các mạng máy tính theo quan điểm phân tầng là: (chọn 1)
   a. Để dễ dàng cho việc quản trị mạng
   b. Để giảm độ phức tạp của việc thiết kế và cài đặt mạng
   c. Đề nâng cấp hệ thống mạng dễ dàng hơn
   d. Không phải các lý do trên
2. Nếu một hệ thống mạng có 8 tầng thì tổng số các quan hệ (giao diện) cần phải xây dựng là …….
   a. 16 b. 24 c. 15 d. 22
3. Tầng …… của mô hình OSI có thể giao tiếp trực tiếp với tầng đối diện của hệ thống máy tính khác.
   a. Application b. Data link c. Network
   d. Physical. e. Transport
4. Những tầng nào của mô hình OSI cung cấp việc kiểm soát luồng dữ liệu?(chọn 3)
   a. Data-Link b. Transport c. Application
   d. Presentation e. Network
5. Một gói (packet) mạng bao gồm: (chọn 1)
   a. Một header, một body và một trailer
   b. Một địa chỉ của máy gửi và một thông báo
   c. Một chuỗi văn bản với thông tin định dạng
   d. Một URL tương ứng với một địa chỉ www.
6. Đơn vị dữ liệu do tầng Liên kết Dữ liệu quản lý là …….
   a. Bit b. Packet c. Frame d. Segment
7. Một Router làm việc ở tầng nào trong mô hình OSI?
   a. Data-Link b. Transport c. Application
   d. Presentation e. Network
8. Những vấn đề liên quan đến kiểm soát truy xuất mạng, mã hoá, xác nhận và bảo mật mạng thuộc chuẩn nào trong các chuẩn do IEEE 802.X xây dựng?
   a. 802.2 b. 802.3 c. 802.4
   d. 802.5 e. 802.10 f. 802.11
9. Tầng nào của mô hình OSI liên quan đến các dịch vụ hỗ trợ trực tiếp phần mềm truyền file, truy xuất cơ sở dữ liệu và e-mail.

a. Application b. Data link c. Network
d. Physical. e. Transport

10. Một cách tổng quát, dữ liệu có thể truyền trực tiếp từ một tầng của hệ thống gửi sang thẳng tầng đối diện (đồng mức) của hệ thống nhận trong mô hình OSI .
    a. Đúng b. Sai

# CHƯƠNG 3 - ĐƯỜNG TRUYỀN VẬT LÝ

## MỤC TIÊU CỦA CHƯƠNG

*Kết thúc chương này, sinh viên sẽ có thể:*

- Nắm được lý thuyết chung về các loại tín hiệu cũng như các đặc tính cơ bản của đường truyền mạng.
- Có những kiến thức và những thông số cơ bản về các loại cáp mạng.

## 3.1 Truyền dữ liệu: tín hiệu tương tự (analogue) và tín hiệu số hoá (digital)

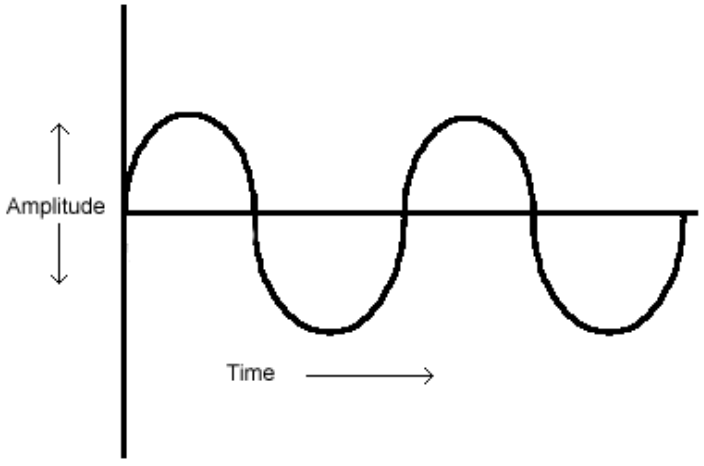
Tín hiệu truyền đi trên mạng hoặc là tương tự (analog), hoặc là số (digital)

### 3.1.1 Tín hiệu tương tự

Tín hiệu tương tự là tín hiệu bao gồm hàng loạt các sóng liên tục do sự biến đổi của điện áp. Nó cũng tương tự như quá trình truyền tín hiệu trên điện thoại. Tín hiệu tương tự không có khả năng loại bỏ nhiễu trên đường truyền trong quá trình truyền dữ liệu, và do đó nhiễu sẽ làm cho qua trình truyền dữ liệu không có tính chính xác cao.

Các đại lượng đặc trưng cho tín hiệu tương tự là: Biên độ và tần số. Đại lượng để đo tần số là Hz.

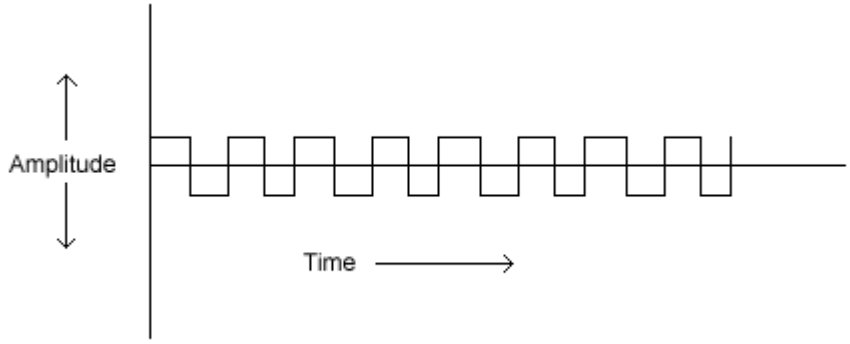
Một trong những vấn đề của tín hiệu tương tự đó là chúng bị *suy giảm*. Biên độ của tín hiệu sẽ tỷ lệ nghịch với khoảng cách mà tín hiệu truyền đi. Khi tín hiệu tương tự đi qua các thiết bị như HUB, hay Repeater thì biên độ của tín hiệu được khuyếch đại, nhưng nhiễu cũng vì vậy mà được khuyếch đại theo (Hình 3.1).




*Hình 3.1* Tín hiệu tương tự

### 3.1.2 Tín hiệu số

Tín hiệu số được tạo thành từ giá trị của các xung điện áp. Nhưng khi chúng đi qua các thiết bị như HUB hay Repeater thì chúng chỉ truyền hay lập lại các tín hiệu nguyên mẫu 1 hay 0 , quá trình này gọi là tái tạo lại. Tín hiệu số ít bị ảnh hưởng của nhiễu do đó có độ tin cậy cao hơn so với tín hiệu tương tự (Hình 3.2).



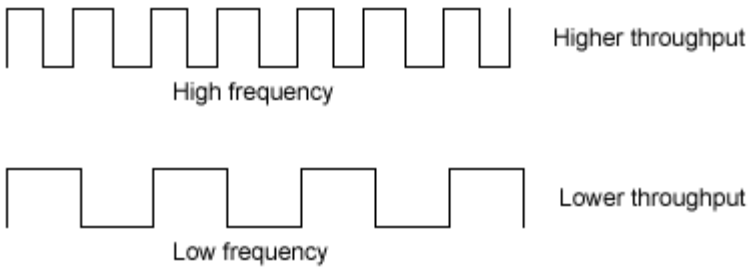

*Hình 3.2* Tín hiệu số

## 3.2 Các đặc tính của đường truyền mạng

Một số vấn đề cần quan tâm khi quyết định môi trường truyền thông trên mạng, bao gồm: dung lượng (throughput), băng thông (bandwidth), chi phí, kích thước, độ linh động, các thiết bị liên kết, và nhiễu.

*Dung lượng* (throughput hay capacity) là lượng dữ liệu đi qua đường truyền trong một đơn vị thời gian. Đơn vị là MegaBits/giây (Mbps). Dung lượng của mạng máy tính phụ thuộc vào khoảng cách địa lý và môi trường đang sử dụng.

*Băng thông* (bandwidth) là đại lượng dùng để đo sự sai biệt giữa tần số lớn nhất và tần số nhỏ nhất của môi trường truyền. Nó liên quan trực tiếp đến dung lượng của đường truyền, nếu một mạng máy tính đang hoạt động ở tần số 870MHz và 880Hz thì băng thông của nó là 10MHz. Thông thường băng thông là lượng dữ liệu thật sự đi qua đường truyền. Đơn vị đo là Hz.




So sánh tín hiệu số tần số cao và tần số thấp

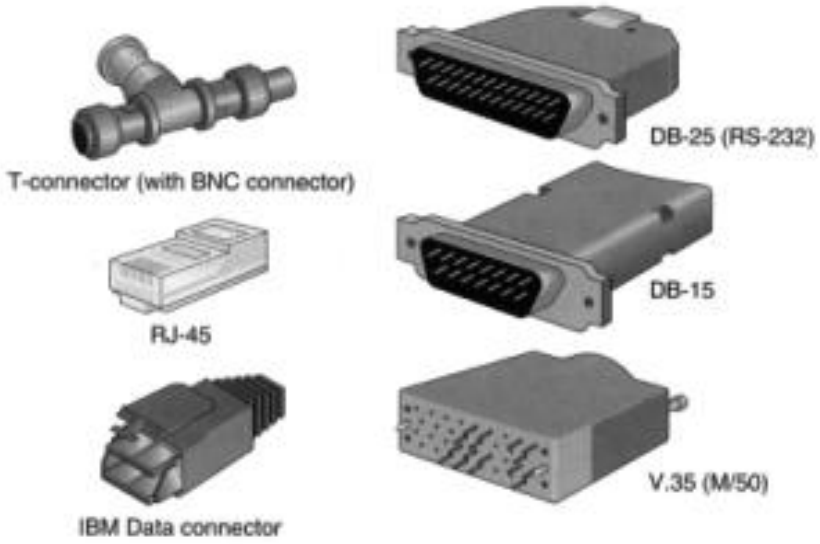
*Chi phí* là một trong các yếu tố quan trọng nó phụ thuộc vào một số các yếu tố như: chi phí cài đặt, chi phí cơ sở hạ tầng, chi phí bảo trì và hỗ trợ v.v...

*Kích thước* và quy mô của môi trường truyền thông mạng máy tính phụ thuộc vào số nút trên mỗi phân đoạn, số phân đoạn và chiều dài của mỗi phân đoạn. Việc chọn lựa cáp nào sẽ ảnh hưởng đến các yếu tố trên.

Số nút trên mỗi phân đoạn càng nhiều sẽ làm suy giảm tín hiệu trên đường truyền. Tín hiệu sau khi đi qua mỗi nút sẽ bị suy giảm và do đó dữ liệu nhận được ở nút sau có thể khác nút trước. Số nút trên mỗi phân đoạn và chiều dài tổng cộng của cả phân đoạn đều phụ thuộc vào dạng cáp đang dùng.

Một yếu tố khác cũng đáng quan tâm đó là *độ trễ* tín hiệu. Độ trễ là thời gian từ lúc tín hiệu được truyền đi cho đến khi nhận được tín hiệu. Ví dụ khi dùng MS Word để xử lý một văn bản được lấy trên server, khi người dùng nhấn Save trên thanh toolbar, thì độ trễ là thời gian được tính từ khi MS Word hiện ra thông báo đi qua mô hình OSI ra card mạng tới cáp, đi qua trường truyền dẫn , qua HUB/SWITCH/ROUTER tới card mạng trên server đi qua mô hình OSI và được chấp nhận bởi server. Lỗi trên đường truyền có thể xảy ra khi thời gian trễ là đủ lớn. Do đó mỗi dạng cáp thường hay qui định số phân đoạn và chiều dài tối đa cho một phân đoạn để tránh lỗi xảy ra.

*Thiết bị liên kết* (Connectors) là các thiết bị dùng để liên kết dây mạng với các nút trên mạng. Các nút này có thể là các trạm làm việc, các máy chủ, các máy in, HUB, Switchs, Routers. Có một số thiết bị như: BNC, T-Connector, RJ45. (Hình 3.3)




*Hình3.3* Một số thiết bị mạng

*Nhiễu điện từ*: bất kỳ hệ thống cáp nào cũng có nhiễu. Nhiễu càng nhiều thì càng ảnh hưởng đến chất lượng đường truyền. Có 2 nguyên nhân chính gây ra nhiễu đó là do điện và do tần số sóng âm thanh.

## 3.3 Các mạng LAN: Baseband và Broadband

Các mạng cục bộ chia làm hai loại: Mạng cục bộ băng thông cơ sở và mạng cục bộ băng thông rộng (Baseband và Broadband LAN).

a. *Mạng cục bộ băng thông cơ sở:* (Baseband LAN) là dạng mạng LAN chỉ cho phép truyền một dạng tín hiệu trên đường truyền hay nói khác đi chỉ có một kênh truyền ( tần số ) duy nhất hỗ trợ truyền số do đó nhanh hơn rất nhiều so với kỹ thuật truyền tín hiệu tương tự.


**Baseband Cable**

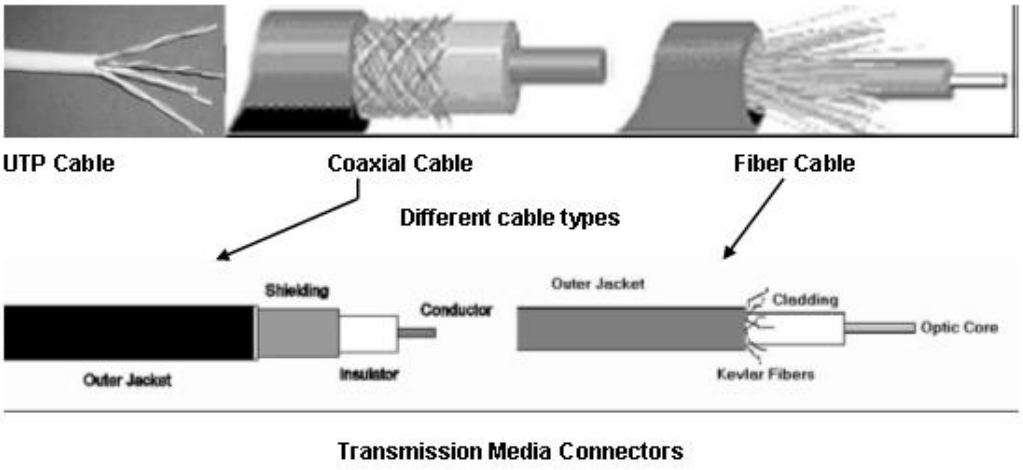
b. *Mạng cục bộ băng thông rộng*: (Broadband LAN) thông thường mạng cục bộ không thuộc loại này. Mạng cục bộ băng thông rộng thường sữ dụng cáp xoắn hay cáp cáp quang để tạo ra nhiều kênh truyền dữ liệu.


**Broadband Cable**

Ứng với mỗi kênh truyền sẽ có một tần số sóng khác nhau, nó sử dụng sóng âm thanh, tín hiệu truyền đi là tương tự do đó có thể xử lý các tín hiệu với các tần số khác nhau. Với băng thông rộng đường truyền được chia thành dãy tần số, mỗi tần số ứng với một loại dữ liệu , theo cách này thì các tính hiệu như âm thanh, hình ảnh. có thể truyền cùng một lúc. Mạng băng thông rộng thích hợp cho các bệnhviện và các viện đại học.

## 3.4 Các loại cáp mạng

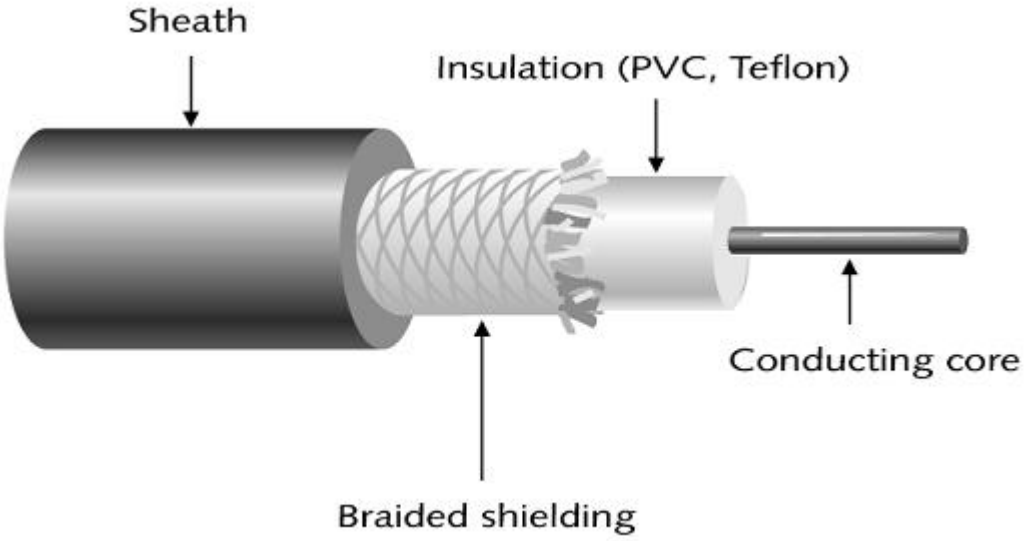
Các phương tiện nối mạng được chia làm hai nhóm: có quy định giới hạn và không quy định giới hạn . Phương tiên có quy định giới hạn thường là cáp, và các phương tiện không qui định là: sóng vô tuyến, laser, viba và tia hồng ngoại. Hệ thống cáp chia ra làm ba loại : *cáp đồng trục* (Coaxial), *cáp xoắn đôi* (twisted-pair) và *cáp sợi quang* (optical fiber)




**Transmission Media Connectors**

### 3.4.1 Cáp đồng trục (Coaxial cable)

Là loại cáp xuất hiện đầu tiên, gồm hai dây dẫn: một lõi bên trong và một lớp bọc ngoài. (Hình 3.4)




*Hình3.4* Cáp đồng trục

Cáp đồng trục chia ra làm hai loại

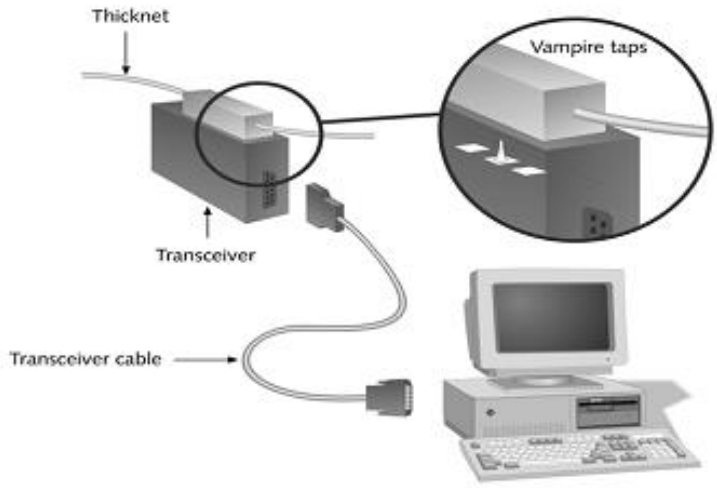
- Cáp đồng trục dày (Thick cable) - 10BASE-5
- Cáp đồng trục mảnh (Thin Cable) - 10BASE-2

Một số thông số kỹ thuật về 2 loại cáp này:

| **Cáp đồng trục mảnh (10BASE-2)** | **Giá trị** |
|---|---|
| Tốc độ truyền dữ liệu ( Max) | 10 Mbps |
| Số repeaters (Max) | 4 |
| Chiều dài tối đa cho 1 phân đoạn | 185 meters |
| Số trạm tối đa trên 1 phân đoạn | 30 |
| Số trạm tối đa | 90 |
| Khảng cách tối thiểu giữa hai trạm | 0.5m |

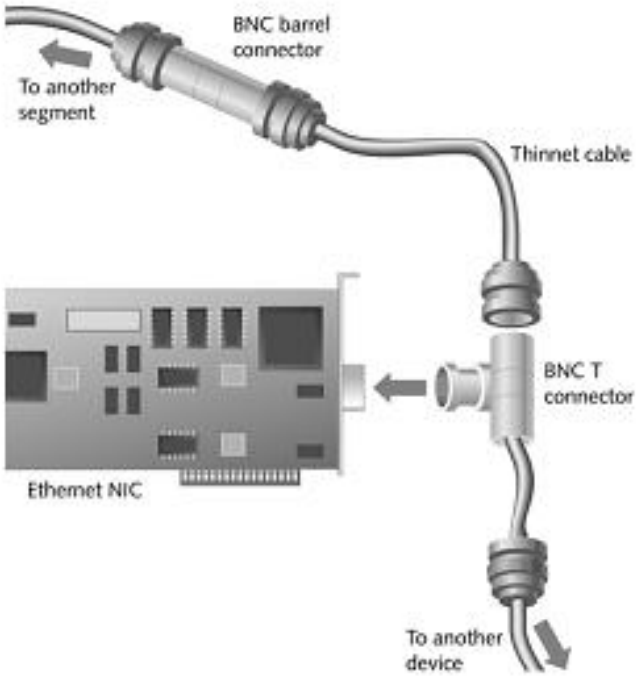
| **Cáp đồng trục dày ( 10BASE-5)** | **Giá trị** |
|---|---|
| Tốc độ truyền dữ liệu ( Max) | 10 Mbps |
| Số repeaters (Max) | 4 |
| Chiều dài tối đa cho 1 phân đoạn | 500 meters |
| Số trạm tối đa trên 1 phân đoạn | 50 |
| Số trạm tối đa | 300 |
| Khảng cách tối thiểu giữa hai trạm | Multiples of 2.5m |

Cáp đồng trục dày (RG-62) thường được dùng trong một mạng máy tính nó tạo thành các đường xương sống (backbone) trong hệ thống mạng (Hình 3.5)




*Hình 3.5* Sơ đồ mạng dùng cáp đồng trục dày

Cáp đồng trục mảnh (RG-58A/U) thường dùng để nối các trạm làm việc trên một mạng cục bộ (Hình 3.6).




*Hình 3.6* Sơ đồ mạng dùng cáp đồng trục mảnh

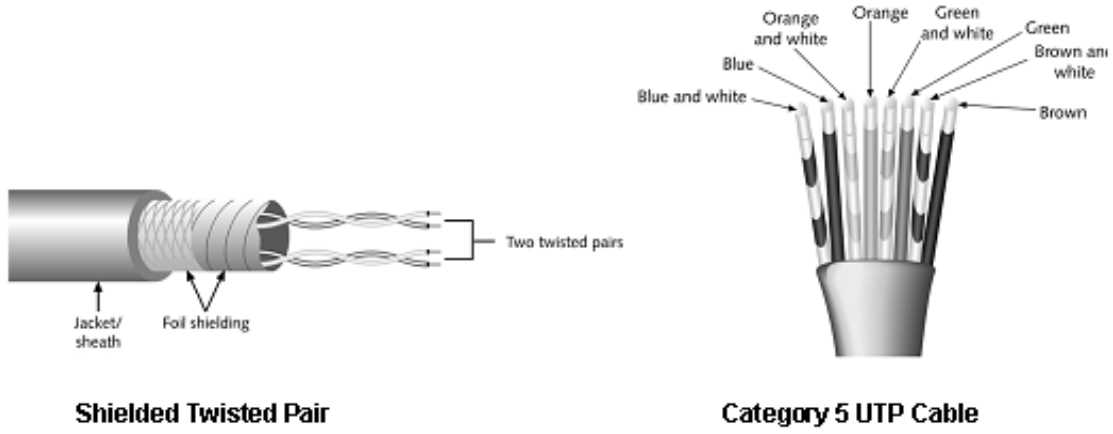
Cáp đồng trục **c**ó các tính chất sau:

- Bị ảnh hưởng của nhiễu bên ngoài và phải được bọc để làm giảm độ nhiễu ảnh hưởng đó.
- Khi khoảng cách mạng lớn, nó có thể thu lấy các nhiễu tạp âm và nhiễu từ xe cộ và các nguồn điện khác.
- Phát ra các tín hiệu khác.

### 3.4.2 Cáp xoắn đôi (Twisted Pair cable)

Có hai loại cáp xoắn đôi:

- Có bọc ngoài (Shielded Twisted Pair cable - STP)
- Không bọc ngoài (Unshielded Twisted Pair cable - STP). Riêng loại cáp dùng cho mạng Ethernet là loại cáp xoắn đôi không bọc ngoài hay còn gọi là cáp UTP (Hình 3.7).



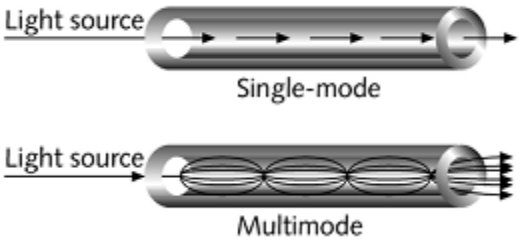

*Hình 3.7* Cáp xoắn đôi

Ngoài ra cáp UTP loại 5 còn gọi là cáp 10BASE-T

Cáp xoắn đôi có các tính chất sau

- Là hệ thống cáp kinh tế nhất
- Có thể dùng những đường cáp điện thoại có sẵn trong một số trường hợp
- Có chiều dài hạn chế
- Có thể bị ảnh hưởng bởi nhiễu bên ngoài

### 3.4.3 Cáp quang (Fibre-Optic cable)




Một số đặc điểm cơ bản của cáp sợi quang:

- Có nhiều kích cỡ khác nhau và chúng chuyển tải ánh sáng chớ không phải điện.
- Thường được dùng kết hợp với những loại cáp khác như là một đường nối kiểu xương sống giữa các server và các LAN

- Có ưu thế lớn về chiều dài cáp và tốc độ truyền nhanh hơn hẳn các loại cáp khác
- Không phát ra tín hiệu
- Không bị ảnh hưởng của nhiễu bên ngoài

Các thông số kỹ thuật của hệ thống cáp rất quan trọng, có thể kiểm tra theo 5 tính chất sau: Chiều dài - Hệ số suy giảm - Nhiễu chen ngang đầu cáp - Tạp nhiễu - Độ thất thoát

- **Việc nối cáp**

Việc chọn loại cáp là một điều quan trọng khi lắp đặt một mạng. Trong các loại cáp thì cáp quang là loại cáp an toàn nhất nhưng giá thành rất cao.

Bảng so sánh các tính năng của cáp

| Yếu tố so sánh | Cáp UTP | Cáp đồng trục | Cáp quang |
|---|---|---|---|
| Giá cả | Thấp | Trung bình | Cao |
| Băng Thông | Trung bình | Cao | Cực kỳ cao |
| Chiều dài | Hàng trăm feet | Hàng ngìn feet | Hàng dặm |
| Nhiễu | Khá nhiều | Thấp | Không có |
| Độ tin cậy | Cao | Cao | Rất cao |

- **Các thành phần của một mạng sử dụng cáp đồng trục 10BASE-2**

-Card giao tiếp 10BASE-2 : hầu hết tất cả đều hỗ trợ hệ thống cáp này. Card cho loại này phải có một đầu nối loại BNC để nối vào dường cáp chính . Trên đường cáp chính có gắn một đầu nối T-Connector để gắn vào một đầu nối BNC ở phía sau card . Nếu máy không có đĩa cứng thì phải gắn thêm một Boot ROM.

- Bộ tiếp sức (Repeater): là một thiết bị chọn thêm, dùng để nối 2 đoạn cáp chính và làm tăng tín hiệu truyền qua lại giữa chúng.
- Cáp: là loại cáp đồng trục có điện trở là 50 Ohm đường kính 0.2 inch
- Các đầu nối cáp kiểu BNC: được gắn vào hai đầu của khúc cáp
- Các đầu nối T-Connector kiểu BNC dùng để đưa tính hiệu vào và ra
- Các đầu nối thanh ngang kiểu BNC được dùng để nối hai khúc cáp lại với nhau
- Các Terminal gắn ở hai đầu cuối của đoạn mạng, có điện trở là 50 Ohm

Khi nối mạng bằng loại cáp này, phải tuân theo các quy tắc và hạn chế sau:

- Chiều dài của mỗi đoạn cáp chính tối đa là khoảng 185 mét
- Dùng các T-Connector để nối cáp với card mạng
- Chỉ dùng tối đa 4 repeater để nối kết 5 đoạn cáp mạng chính, trong đó chỉ có 3 đoạn là được dùng để nối với trạm làm việc, 2 đoạn còn lại chỉ dùng để nối đến những khoảng cách ở xa.
- Chiều dài tối đa của toàn mạng là 910 mét
- Tối đa có 30 nút trên mỗi đoạn mạng, các nút ở đây bào gồm: máy tính, server, repeater, router.

- **Các thành phần của một mạng khi dùng cáp xoắn đôi (10BASE-T hay là UTP)**

Các trạm làm việc được nối vào một HUB, có tác dụng làm khuyếch đại tín hiệu từ server tới và phát đi tiếp tới các máy khác trên mạng

** Các thành phần của một mạng dùng cáp UTP*

- Card giao tiếp mạng 10BASE-T
- Hub
- Cáp UTP

# Câu hỏi ôn tập chương 3

1. Công nghệ cáp đồng trục ..... hỗ trợ nhiều kênh, mỗi kênh chiếm khoảng 6 MHz.

a. Thick b. Baseband

c. Broadband d. Thin

2. Điều nào là không đúng khi nói về cáp sợi quang trong các điều sau?

a. It has a lower noise level

b. Light signals do not attenuate as quickly as electric signals

c. Light propagates more quickly through glass than electric signals

d. It is easy to wiretap

3. Việc tăng tốc độ truyền có thể tăng ảnh hưởng của nhiễu và vì vậy giá trị của tín hiệu.

a. Đúng b. Sai

3. Loại mội trường truyền nào trong các loại sau không phải là mội trường trường định hướng?

a. Twisted pair wire b. Coaxial cable

c. Fiber optic cable d. Microwave

4. Kỹ thuật chuyển từ dữ liệu số hoá sang tín hiệu tương tự gọi là .....

a. Manchester encoding b. Modulation

c. Multiplying d. Negotiation

5. Bạn chịu trách nhiệm bảo trì máy tính Microsoft Windows 2000 Server trên mạng công ty của mình. Card mạng trong server hiện thời được kết nối tới mạng. Bạn thấy có một đầu nối 15 chân ở phía sau của card giao tiếp mạng (NIC) đang nối tới một transceiver bên ngoài. Loại cáp nào được sử dụng cho kết nối mạng?

a. ThinNet coaxial (10Base2) b. ThickNet coaxial (10Base5)

c. Twisted-pair (10BaseT) cable d. Fiber-optic cable

6. Những loại cáp nào thuộc về công nghệ Ethernet 10 Mbps? (Chọn tất cả các câu trả lời đúng)

a. 10Base2 b. 10Base10 c. 10BaseTL

d. 10BaseUT e. 10BaseFL f. 10Base5

7. Hai loại cáp nào được sử dụng với đầu nối BNC connector và các thành phần terminator?

a. 10Base2 b. 10Base10

c. Thinnet d. 10BaseUT

# CHƯƠNG 4 - CÁC GIAO THỨC MẠNG (PROTOCOLS)

## MỤC TIÊU CỦA CHƯƠNG

*Kết thúc chương này, sinh viên sẽ có thể:*

- Hiểu được khái quát khái niệm giao thức mạng máy tính.
- Đặc điểm và nội dung các giao thức con của các bộ giao thức thông thường đang sử dụng: TCP/IP, IPX/SPX, MicroSoft Network. Có so sánh chúng với mô hình OSI.

## 4.1 Giao thức (protocol) mạng là gì?

*Tập hợp tất cả các quy tắc, quy ước để đảm bảo cho các máy tính trên mạng có thể giao tiếp với nhau gọi là giao thức*. Như vậy các máy trên mạng muốn giao tiếp với nhau thì phải có chung một giao thức.

Vai trò của giao thức là quan trọng, không thể thiếu.

Ví dụ một số giao thức như: TCP/IP, SPX/IPX, v.v...

Các dạng liên kết:

- Giao thức hướng kết nối và giao thức không kết nối (Connectionless & Connection- Oriented protocols)
- Giao thức có khả năng định tuyến và giao thức không có khả năng định tuyến (Routable & non - Routable protocols)

### 4.1.1 Giao thức hướng kết nối và giao thức không kết nối

- Đặc điểm của giao thức không kết nối:
  a. Không kiểm soát đường truyền
  b. Dữ liệu không bảo đảm đến được nơi nhận
  c. Dữ liệu thường dưới dạng datagrams

  Ví dụ: giao thức UDP của TCP/IP
- Đặc điểm của giao thức hướng kết nối:
  a. Ngược lại với giao thức không kết nối , kiểm soát được đường truyền
  b. Dữ liệu truyền đi tuần tự, nếu nhận thành công thì nơi nhận phải gởi tín hiệu ACK (ACKnowledge)

  Ví dụ: các giao thức TCP, SPX

### 4.1.2 Giao thức có khả năng định tuyến và giao thức không có khả năng định tuyến

- Giao thức có khả năng định tuyến

Là các giao thức cho phép đi qua các thiết bị liên mạng như Router để xây dựng các mạng lớn có qui mô lớn hơn

Ví dụ, các giao thức có khả năng định tuyến là: TCP/IP, SPX/IPX

- Giao thức không có khả năng định tuyến

Ngược với giao thức có khả năng định tuyến, các giao thức này không cho phép đi qua các thiết bị liên mạng như Router để xây dựng các mạng lớn.

Ví dụ về giao thức không có khả năng định tuyến là : NETBEUI

Hiện có 3 loại giao thức thường hay sử dụng:

- TCP/IP
- SPX/IPX (Novell Netware)
- Microsoft Network

## 4.2 Bộ giao thức TCP/IP (Transmission Control Protocol / Internet Protocol)

TCP/IP được thiết kế hoàn toàn độc lập với các phương pháp truy cập mạng, cấu trúc gói dữ liệu (data frame), môi trường truyền, do đó mà TCP/IP có thể dùng để liên kết các dạng mạng khác nhau như mạng LAN Ethernet, LAN Token Ring hay các dạng WAN như: Frame Relay, X.25

Hình 4.1 so sánh bộ giao thức TCP/IP với mô hình OSI.

TCP/IP là một lớp các giao thức ( protocol stack) bao gồm các giao thức sau:

### 4.2.1 FTP (File Transfer Protocol).

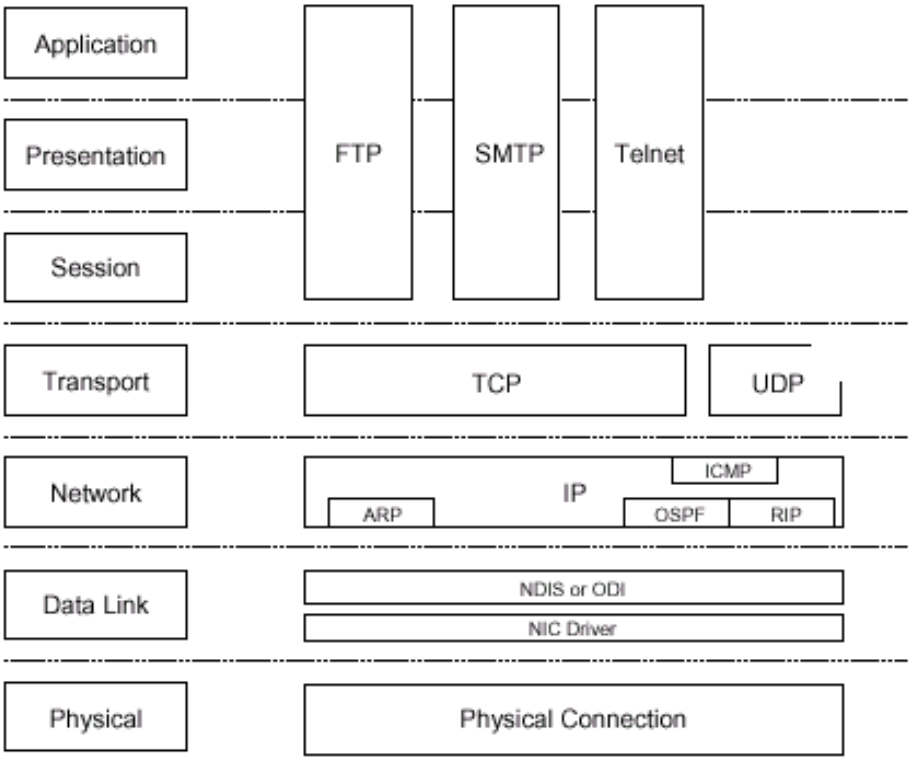
FTP cung cấp phương pháp truyền nhận file giữa các máy với nhau, nó cho phép người sử dụng có thể gởi một hay nhiều file từ máy mình lên hệ thống bất kỳ (upload) và nhận một hay nhiều file từ một hệ thống bất kỳ về máy mình (download)

### 4.2.2 Telnet

Với Telnet, người sử dụng có thể kết nối vào các hệ thống ở xa thông qua mạng Internet.

### 4.2.3 SMTP (Simple Mail Transfer protocol)

Là giao thức cho phép thực hiện dịch vụ truyền nhận mail trên mạng Internet.




*Hình 4.1* So sánh giao thức TCP/IP với mô hình OSI

### 4.2.4 TCP và UDP

Hai giao thức này đóng vai trò của tầng transport, có trách nhiệm tạo liên kết và dịch vụ kết nối dữ liệu (datagram communication service)

- TCP (Transmission Control Protocol) là giao thức chuyển giao chính trong TCP/IP. TCP cung cấp một đường truyền có độ tin cậy cao, là liên kết có định hướng (connection oriented protocol), khôi phục các gói dữ liệu bị mất trong qúa trình truyền. Quá trình truyền dữ liệu theo TCP là các byte, gói dữ liệu TCP bao gồm các thông tin sau

| **Thông tin** | **Chức năng** |
|---|---|
| Source Port | Thông tin về địa chỉ cổng (port) của máy gởi |
| Destination port | Thông tin về port của máy nhận |
| Chỉ số thứ tự | Chỉ số thứ tự tính từ byte đầu tiên trong dữ liệu TCP |
| ACK | Chỉ số byte mà người gởi nhận được từ người nhận |
| Window | Bộ đệm dữ liệu cho TCP |
| TCP Checksum | Xác định tính toàn vẹn dữ liệu trong TCP header và TCP data |

Một số port TCP thông dụng

| Số port | Dịch vụ |
|---|---|
| 20 | FTP ( Data) |
| 21 | FTP (Control) |
| 23 | Telnet |
| 80 | HTTP |
| 139 | NETBIOS |

- UDP (User Datagram protocol) là loại liên kết một một hay một nhiều, không định hướng (Connectionless), không có độ tin cậy cao, thường hay dùng khi dung lượng dữ liệu truyền tải trên mạng là nhỏ. Các thông tin trong UDP header bao gồm:

| Thông tin | Chức năng |
|---|---|
| Source Port | Thông tin về port của máy gởi |
| Destination port | Thông tin về port của máy nhận |
| TCP Checksum | Xác định tính toàn vẹn dữ liệu trong TCP header và TCP data |

Một số port UDP thông dụng:

| Số port | Dịch vụ |
|---|---|
| 53 | Domain name system |
| 137 | NETBIOS NAME |
| 138 | NETBIOS Datagram |
| 161 | SNMP |

### 4.2.5 Các giao thức IP, ARP, ICMP, RIP.

Đóng vai trò của tầng Internet có chức năng tìm đường (routing), nhận dạng địa chỉ (addressing), đóng gói (package)

- IP (Internet protocol) là dạng giao thức cho phép tìm đường (routable protocol), nhận dạng địa chỉ (addressing), phân tích và đóng gói. Một gói IP bao gồm IP header và IP payload, trong đó IP header bao gồm các thông tin sau:

| IP Header | Chức năng |
|---|---|
| Địa chỉ IP gởi | Thông tin về địa chỉ IP của máy gởi |
| Địa chỉ IP nhận | Thông tin về địa chỉ IP của máy nhận |
| Identification | Nhận dạng các mạng con nếu có trong địa chỉ IP |
| Checksum | Xác định tính toàn vẹn dữ liệu trong phần IP header |

- ARP (Address Resolution Protocol) có chức năng phân giải một địa chỉ IP thành một địa chỉ giao tiếp trên mạng.

- ICMP (Internet Control Message Protocol) có chức năng thông báo lại các lỗi xảy ra trong qua trình truyền dữ liệu.

### 4.2.6 NDIS (Network Driver Interface Specification) và ODI (Open Data Interface)

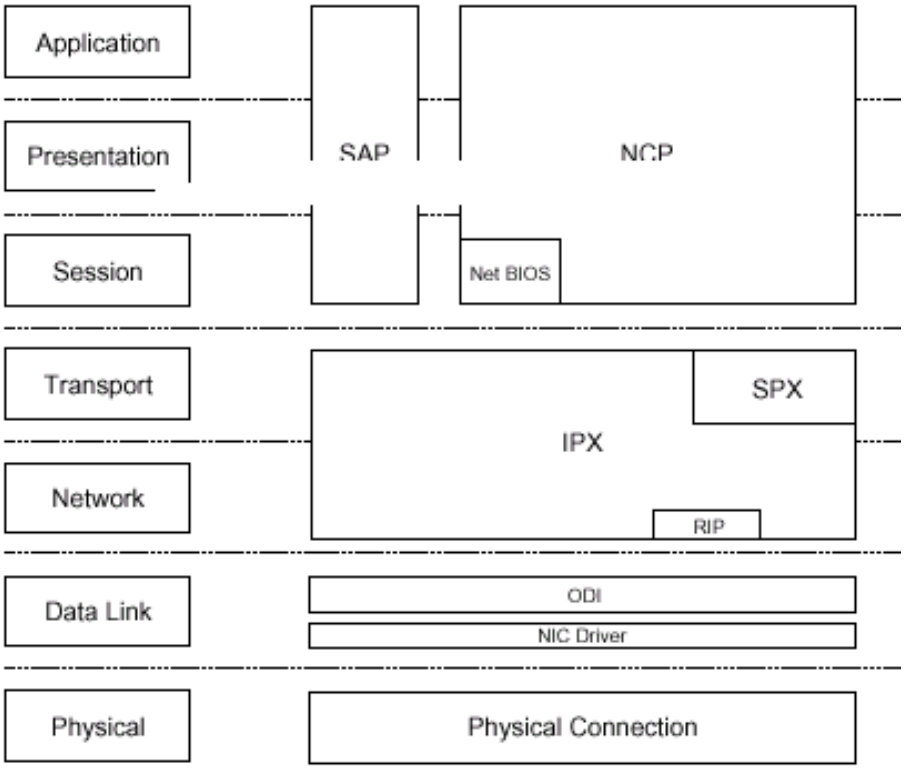
Hai giao thức này đóng vai trò của tầng DataLink, cho phép một card giao tiếp (interface card) có thể giao tiếp với nhiều giao thức khác nhau trên mạng.

- ODI được phát triển bởi Novell và Apple, ban đầu ODI driver được viết cho Novell và Macintosh

- NDIS được phát triển bởi Microsoft và 3 COM có các phiên bản như NDIS, NDIS2 và NDIS3. Các phiên bản cũ dùng cho Windows for workgroup, NT 3.5, còn các phiên bản mới dùng cho WinNT 4.0 hay Windows 2000.

## 4.3 Bộ giao thức IPX/SPX (Internetwork Packet Exchange / Sequenced Packet Exchange )

So sánh IPX/SPX với mô hình OSI (Hình 4.2)




*Hình 4.2* So sánh giao thức IPX/SPX với mô hình OSI

Cũng giống như TCP/IP, IPX/SPX là một lớp giao thức bao gồm các giao thức sau:

### 4.3.1 SAP (Service Advertising Protocol)

Là giao thức dùng để quảng cáo địa chỉ của server và các dịch vụ khác trên mạng như File servers và Print server dùng SAP.

### 4.3.2 NCP (Netware Core Protocol)

Xử lý quá trình tương tác giữa client và server, ví dụ như việc chia xẻ các tài nguyên trên mạng.

### 4.3.3 SPX (Sequenced Packet Exchange )

Cung cấp liên kết định hướng (connection oriented protocol) trên IPX.

### 4.3.4 RIP (Routing information Protocol)

Là giao thức tìm ra đường đi tốt nhất cho các gói dữ liệu.

### 4.3.5 IPX (Internetwork Packet Exchange)

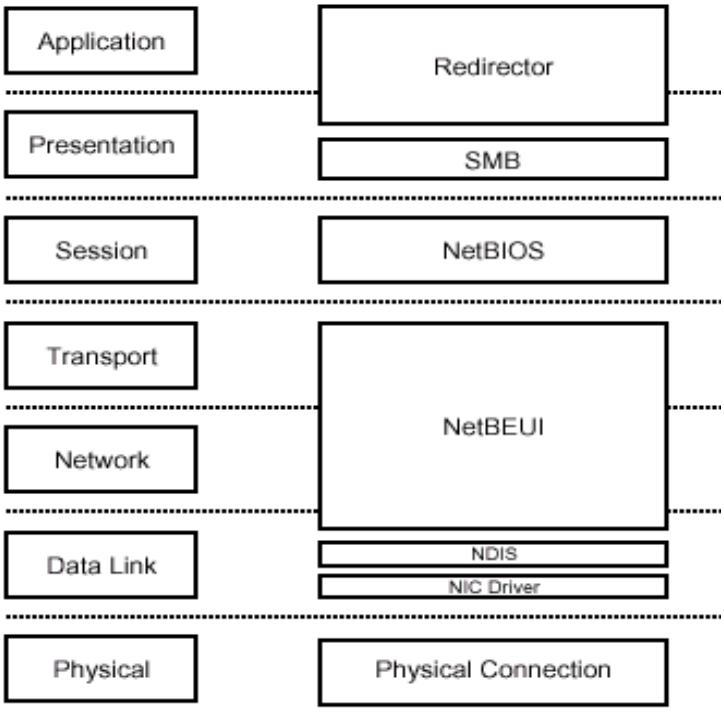
Là giao thức không định hướng, dùng để xác định địa chỉ mạng và tìm đường trên mạng IPX/SPX, IPX cung cấp dịch vụ về datagram.

### 4.3.6 ODI (Open Data Interface)

Giao thức này đóng vai trò của tầng DataLink, cho phép một card giao tiếp có thể giao tiếp với nhiều giao thức khác nhau trên mạng. ODI được phát triển bởi Novell và Apple, do đó ban đầu ODI driver được viết cho Novell và Macintosh

## 4.4 Bộ giao thức Microsoft Network ( NETBIOS, NETBEUI, SMB)

Microsoft Networking là sự kết hợp của IBM & Microsoft, nó là lớp các giao thức, so sánh với mô hình OSI ( Hình 4.3 )




*Hình 4.3* So sánh giao thức Microsoft Networking với mô hình OSI

NetBIOS : Network Basic Input Output System

NetBEUI : Network Extended User Interface

Microsoft Network bao gồm các giao thức sau:

### 4.4.1 Redirector

Giao thức này có tác dụng:

- Làm cho tài nguyên trên mạng trở thành cục bộ.
- Trực tiếp truy xuất tới tài nguyên trên các server tương ứng

### 4.4.2 SMB

Có chức năng tương tự như tầng biểu diễn, cung cấp liên kết ngang hàng giữa client và server, cho phép thành lập các mạng ngang hàng.

### 4.4.3 NetBIOS

Giao thức này dùng để thành lập phiên làm việc giữa các máy tính. Nó có các đặc điểm sau:

- Hoạt động tại tầng Session.
- Dùng tên có 15 ký tự để tự nhận dạng.
- Thành lập liên kết giữa 2 máy để truyền dữ liệu
- Cho phép liên kết không định hướng
- Dùng broadcast để định dạng các máy tính trên mạng.

Cơ chế hoạt động của NetBIOS bao gồm 4 phần :

- NetBIOS Interface
- NetBIOS Management
- NetBIOS Datagram
- NetBIOS Session

❖ NetBIOS Interface

Bao gồm các hàm API chuẩn cho phép các ứng dụng có thể gởi hay nhận thông tin từ server. NetBIOS Interface còn thực hiện chức năng NetBIOS trên TCP/IP.

❖ NetBIOS Management

Bao gồm những chức năng sau

. Đăng ký và hủy tên: cho phép các máy có thể đăng ký một tên nhận dạng trên mạng và sau đó xóa đi khi thoát khỏi mạng

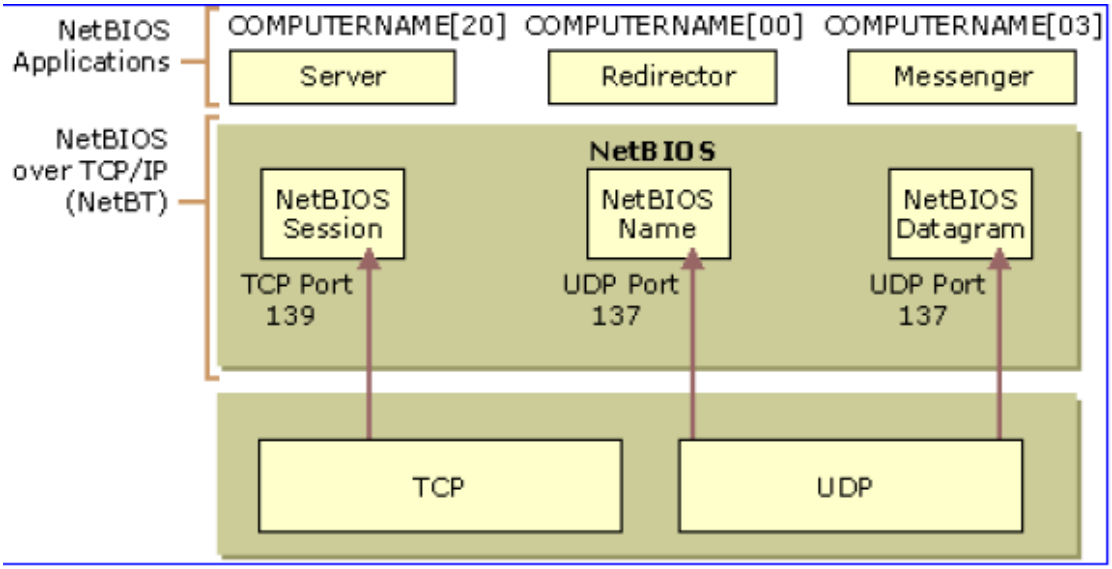
. Phân giải tên (Name Resolution): khi có một chương trình NetBIOS muốn giao tiếp với một chương trình NetBIOS khác, thì địa chỉ IP của chương trình này phải được phân giải thành NETBIOS name, NETBIOS trên TCP/IP sẽ thực hiện chức năng này.

❖ NetBIOS Datagram

Quản lý cách truyền các datagram theo liên kết không định hướng. Các datagram có thể truyền cho một người hay một nhóm người nào đó sử dụng cơ chế NetBIOS Name.

❖ NetBIOS Session

Quản lý cách truyền các datagram theo liên kết có định hướng và theo thứ tự có độ tin cậy cao. Nó sử dụng giao thức TCP để thành lập một liên kết và kết thúc khi cần thiết. Xem hình vẽ (Hình 4.4)




*Hình 4.4* Cơ chế NETBIOS

### 4.4.5 NetBEUI

- Là giao thức thích hợp cho các mạng LAN nhỏ từ 10 - 200 máy
- Nhanh, hiệu qủa, ít tốn vùng nhớ.

### 4.4.6 NDIS

Được phát triển bởi Microsoft và 3 COM có các phiên bản như NDIS, NDIS2 và NDIS3. Các phiên bản cũ dùng cho Windows for workgroup, NT 3.5, còn các phiên bản mới dùng cho WinNT 4.0 hay Windows 2000.

## 4.5 Một số Protocols khác

- DLC (Data Link Control): dùng để liên kết IBM mainframes và máy in của HP
- NFS ( Network File System) : là giao thức dùng trên UNIX
- SNA ( System Network Architecture) dùng trên máy IBM
- X-windows: tập các giao thức (MIT) dưới dạng Graphic để giao tiếp với người sử dụng trên Unix.

# Câu hỏi ôn tập chương 4

1. Mục nào trong các mục sau không phải là một thuộc tính TCP/IP trong một môi trường định tuyến?
   a. TCP/IP address b. Subnet mask
   c. Default gateway d. DNS server
2. Một mạng LAN, trong đó các máy tính được kết nối tới một HUB với cáp xoắn đôi, tốt nhất có thể được mô tả như:
   a. Một hình trạng star lôgíc
   b. Một hình trạng bus lôgíc và một hình trạng star vật lý.
   c. Một hình trạng ring hoặc loop.
   d. Một hình trạng bus vật lý.
3. Giao thức nào trong các giao thức sau không phải là một giao thức có thể định tuyến?
   a. FTP b. IP c. NetBEUI d. SMTP
4. Giao thức nào chuyển đổi datagrams mà không có thông tin ACK hoặc truyền đảm bảo?
   a. TCP b. ASP c. TCP/IP d. UDP
5. Một trong những khác nhau chính giữa NetBEUI và TCP/IP là:
   a. NetBEUI là định tuyến và TCP/IP là không định tuyến.
   b. NetBEUI là không định tuyến và TCP/IP là định tuyến.
   c. NetBEUI thì khó quản lý.
   d. TCP/IP cấu hình dễ dàng hơn so với NetBEUI.
6. Các yêu cầu tối thiểu cho việc định địa chỉ trong một mạng dựa trên giao thức TCP/IP?
   a. IP address, Subnet Mask, và default gateway.
   b. MAC address và subnet mask.
   c. IP address.
   d. IP address và subnet mask.
7. Những lợi ích mà TCP có so với UDP?
   a. TCP cho phép các gói lớn hơn được gửi qua mạng nhờ đó cải tiến hiệu suất ứng dụng.
   b. TCP có một cơ chế "gửi lại" để ngăn chặn việc mất gói dữ liệu.
   c. TCP sử dụng một header nhỏ hơn UDP.
   d. Không phải những điều ở trên.
8. Giao thức nào trong các giao thức giao vận sau được sử dụng cho việc chơi các trò chơi trên Internet?
   a. TCP b. IPX/SPX.
   b. NetBEUI d. UDP
9. Giao thức nào được sử dụng để gán các địa chỉ IP tĩnh?
   a. ARP b. Proxy ARP
   c. DHCP d. TCP/IP
10. Cái gì được sử dụng trong giao thức để tách host ID khỏi network ID?
    a. Network address b. Node address.
    c. Default gateway d. Subnet mask.

# CHƯƠNG 5 - CÁC HÌNH TRẠNG (TOPOLOGIES) CỦA MẠNG CỤC BỘ (LAN)

## MỤC TIÊU CỦA CHƯƠNG

*Kết thúc chương này, sinh viên sẽ có thể:*

- Nắm được các đặc trưng cơ bản của mạng cục bộ.
- Hiểu được các đặc điểm cũng như các ưu và nhược điểm của các hình trạng LAN đơn giản: *bus*, *star* và *ring*, cũng như đặc điểm của các hình trạng LAN hỗn hợp.
- Hiểu được ba kỹ thuật chuyển mạch: *kênh*, *thông báo* và *gói*; So sánh ba kỹ thuật chuyển mạch này.
- Nắm được nội dung cơ bản hai phương pháp truy xuất đường truyền: *CSMA/CD* và *Token Passing*.
- Nắm được các yếu tố (cả về lý thuyết và kỹ thuật cơ bản) tạo nên kiến trúc mạng Ethernet và mạng Token Ring

## 5.1 Các đặc trưng cơ bản của mạng cục bộ (LAN)

Trong mục 1.2.3 ở phần đầu tài liệu này, khi phân loại các mạng máy tính dựa trên yếu tố chính là khoảng cách địa lý, ta có các loại mạng như mạng cục bộ (LAN), mạng đô thị (MAN), mạng diện rộng (WAN) và mạng toàn cầu (GAN). Tuy nhiên khoảng cách địa lý giữa các trạm của mạng cũng chỉ là một trong các đặc trưng của mạng cục bộ. Còn có các đặc trưng khác (như tốc độ truyền, tỷ suất lỗi, …) cũng đóng vai trò quan trọng quyết định hiệu suất và sự phát triển của LAN.

Sau đây là một số đặc trưng cơ bản của LAN cho phép phân biệt LAN và các loại mạng khác, đặc biệt là với WAN.

### *5.1.1 Đặc trưng địa lý*

Cũng như đã được trình bày trong mục 1.2.3, mạng LAN là mạng được cài đặt trong một phạm vi tương đối nhỏ (trong một phòng, một toà nhà, hoặc phạm vi của một trường học v.v…) với khoảng cách lớn nhất giữa hai máy tính trạm chỉ trong khoảng vài chục ki-lô-met trở lại. Tuy nhiên giới hạn về khoảng cách này cũng chỉ có tính chất tương đối. Vì vậy, không thể chỉ lấy đặc trưng về địa lý để phân biệt LAN với các loại mạng khác.

### *5.1.2 Đặc trưng tốc độ truyền*

Mạng cục bộ có tốc độ truyền thường *cao hơn* so với mạng diện rộng (WAN). Hiện nay, tốc độ truyền của LAN có thể đạt tới 100 Mb/s.

### *5.1.3 Đặc trưng độ tin cậy*

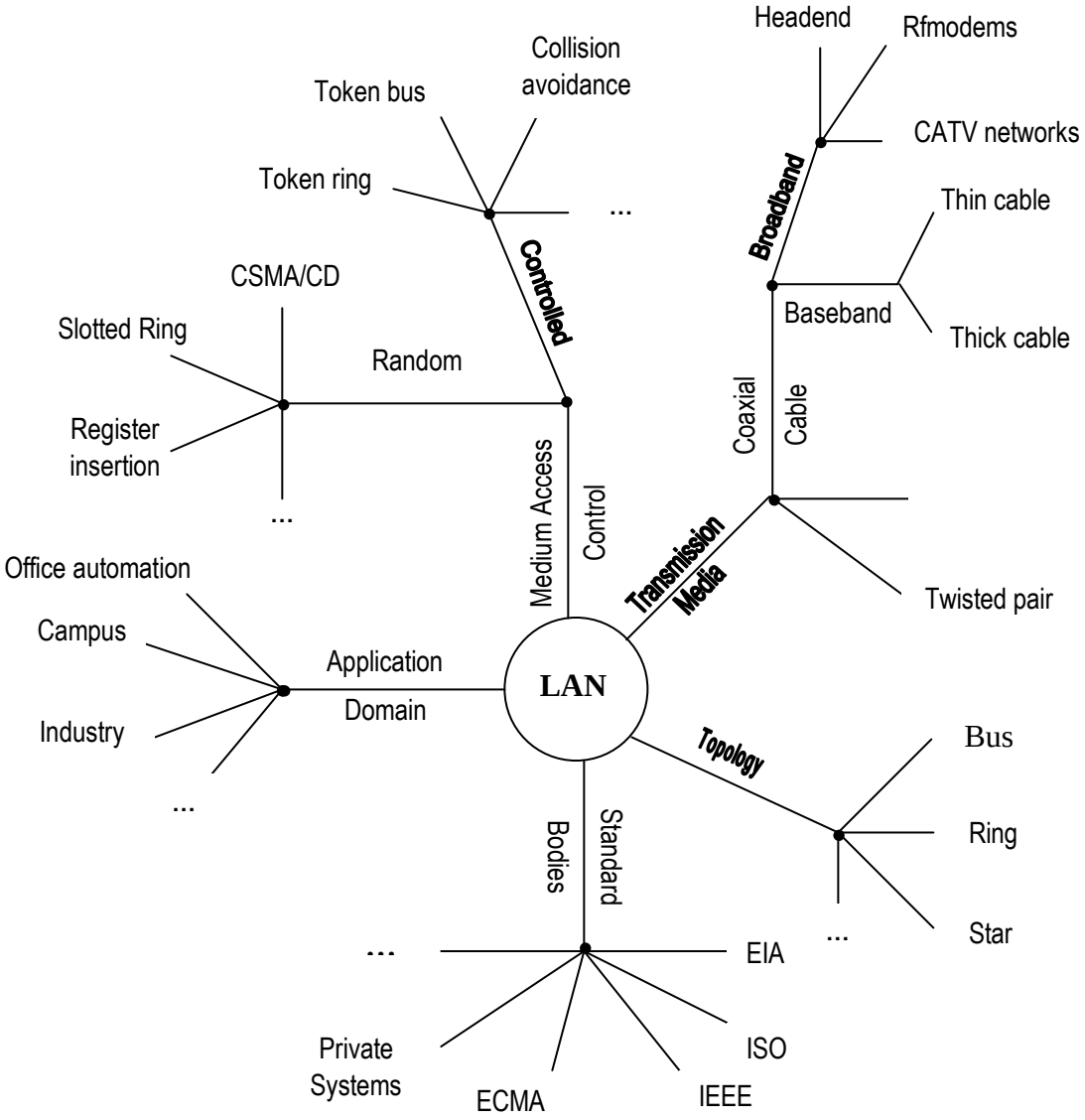
Tỷ suất lỗi (error rate) trên mạng LAN *thấp hơn* nhiều so với WAN: có thể đạt từ $10^{-8}$ đến $10^{-11}$.

### *5.1.4 Đặc trưng quản lý*

Mạng cục bộ thường là sở hữu riêng của một cá nhân hoặc tổ chức nào đó (trường học, doanh nghiệp, v.v…) do đó việc quản lý khai thác mạng hoàn toàn tập trung, thống nhất.

Tuy nhiên, với sự phát triển nhanh chóng của công nghệ mạng, các đặc trưng nói trên cũng chỉ có tính chất tương đối. Sự phân định giữa mạng cục bộ và mạng diện rộng sẽ ngày càng "mờ" hơn.

Hình 5.1 cho ta một sơ đồ tóm tắt các vấn đề cần xem xét khi tìm hiểu về mạng cục bộ.




*Hình 5.1* Sơ đồ tóm tắt những vấn đề liên quan đến mạng LAN

Những vấn đề liên quan đến đường truyền vật lý (Transmission media) đã được tìm hiểu ở chương 3. Chương này tập trung xem xét về hình trạng (topology) và kỹ thuật truy xuất đường truyền (Medium Access Control) LAN.

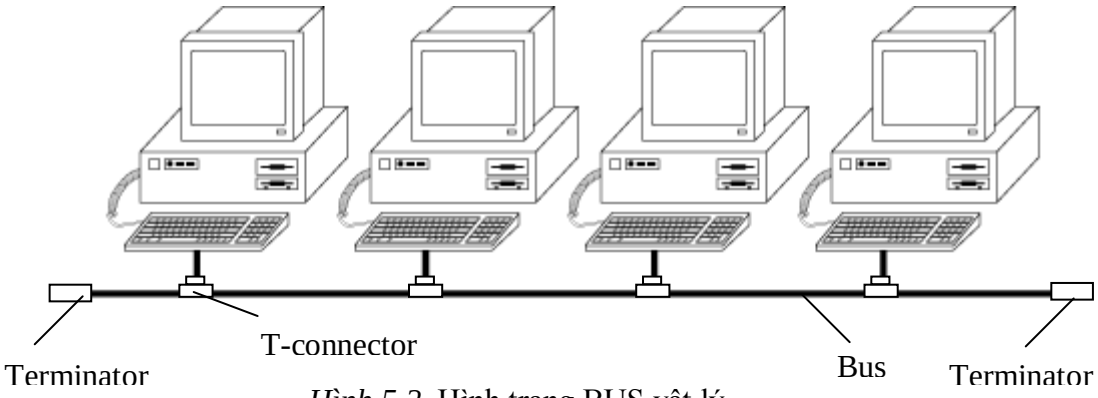
## 5.2 Các hình trạng LAN đơn giản

Như đã trình bày trong phần 1.2.4, mạng cục bộ có ba hình trạng đơn giản là *bus* (đường trục), *star* (hình sao), và *ring* (vòng). Sau đây ta sẽ lần lượt tìm hiểu các hình trạng này.

### 5.2.1 Hình trạng BUS

Một hình trạng *bus* vật lý (còn gọi là hình trạng *bus tuyến tính*) căn bản sử dụng một đường cáp chung dài gọi là đường *xương sống* (backborne hay bus). Đường cáp này còn được gọi là *đường truyền chính* (trunk line) hoặc *phân đoạn mạng* (network segment).

Có những đoạn cáp ngắn được gắn với đường xương sống bằng các *đầu nối* (tap) để kết nối với các thiết bị mạng (Các *tap* là những thiết bị cơ khí dùng để phân tách tín hiệu điện hoặc điện từ). Tuy nhiên các hình trạng bus hiện nay chủ yếu gắn các máy tính trực tiếp với đường truyền chính bằng đầu nối chữ T (T-connector). Đường truyền chính được kết thúc (terminate) ở hai đầu bằng các terminator để loại bỏ các tín hiệu trên dây sau khi nó truyền qua mọi thiết bị gắn với bus. Tất cả các nút (bao gồm máy chủ file, các máy trạm, và các thiết bị ngoại vi) được kết nối tới đường truyền chính đó (Hình 5.2).




*Hình 5.2* Hình trạng BUS vật lý

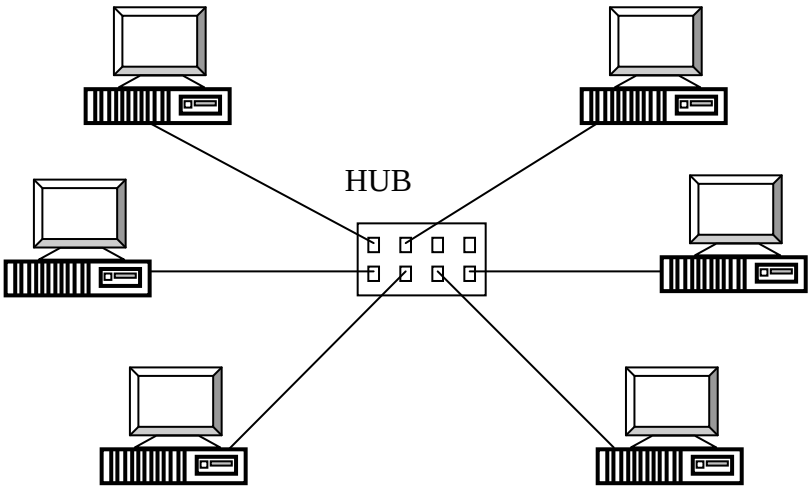
Đa số các hình trạng bus cho phép các tín hiệu điện hoặc điện từ lan truyền theo cả hai hướng

- *Ưu điểm của hình trạng* BUS*:*
  - Sử dụng các chuẩn đã được thiết lập, cài đặt tương đối dễ dàng.
  - Đòi hỏi đường truyền cáp ít hơn các hình trạng khác.
  - Cách bố trí dây rất đơn giản, dễ mở rộng và tin cậy.
- *Nhược điểm của hình trạng* BUS*:*

- Khó khăn trong việc cấu hình lại, đặc biệt khi khoảng cách và số các đầu nối vượt quá mức tối đa cho phép.
- Việc chẩn đoán và cô lập các lỗi khó khăn.
- Mạng sẽ không hoạ t động (down) khi có lỗi hoặc đứt cáp.

### 5.2.2 Hình trạng STAR

Mạng ở dạng hình sao có một *bộ xử lý trung tâm* (HUB) – còn gọi là bộ *chuyển tiếp nhiều cổng* (multiport repeater) hay *bộ tập trung* (concentrator) mà tất cả các nút (máy chủ file, các máy trạm, và các thiết bị ngoại vi) gắn với nó qua đường cáp (Hình 5.3). Các mạng hình sao có thể được lồng trong các mạng hình sao khác để tạo thành mạng hình cây hoặc mạng phân cấp




*Hình 5.3* Hình trạng STAR với HUB ở trung tâm

Dữ liệu trên mạng STAR truyền qua HUB trước khi tiếp tục tới đích. HUB quản lý và điều khiển tất cả các chức năng của mạng. HUB cũng hoạt động như một bộ chuyển tiếp luồng dữ liệu. Nó được sử dụng trong các mạng ARCnet, Token Ring, FDDI (Fiber Distributed Data Interface) và các mạng cục bộ 10BaseT với cáp xoắn đôi, cáp đồng trục hoặc cáp sợi quang. Những ví dụ điển hình của hình trạng STAR là các kiến trúc *mainframe* và *minicomputer*, trong đó máy chủ (host) là một bộ chuyển mạch (switch) tập trung. Trong mạng hình sao, nếu một cáp bị đứt, nó chỉ ảnh hưởng tới nút (máy trạm) nối tới HUB bằng cáp đó. Tuy nhiên nếu HUB bị hư thì toàn bộ phân đoạn mạng kết nối tới HUB đó sẽ ngừng hoạt động.

Đa số các mạng cục bộ Ethernet hiện nay đều sử dụng hình trạng STAR vì khả năng mở rộng và dễ dàng kết nối với các mạng khác. Chúng cũng dễ dàng cô lập các lỗi xảy ra với cáp mạng. Nhiều mạng bus và ring cũ cũng được nâng cấp để chuyển sang mạng hình sao.

❖ *Ưu điểm của hình trạng* STAR*:*

- Dễ cài đặt và cấu hình lại.

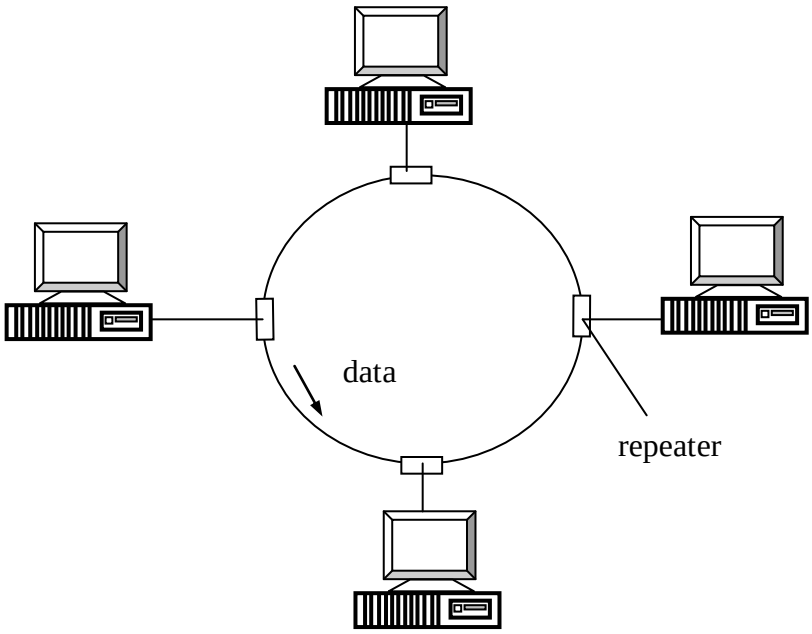
- Dễ giải quyết các sự cố.
- Lỗi đường truyền tự động cô lập phân đoạn mạng bị lỗi.
- Không cần phải ngắt mạng khi cần kết nối thêm hoặc tháo bỏ bớt các thiết bị mạng.

❖ *Nhược điểm của hình trạng* STAR*:*

- Đòi hỏi nhiều cáp hơn các hình trạng khác.
- Việc tồn tại một HUB tập trung (hoặc concentrator) đồng nghĩa với việc tồn tại khả năng ngừng hoạt động của toàn phân đoạn mạng khi HUB đó có sự cố.

### 5.2.3 Hình trạng RING

Một hình trạng RING vật lý là một hình trạng vòng (vòng kín liên kết điểm-điểm). Mỗi thiết bị kết nối trực tiếp tới vòng hoặc gián tiếp qua một thiết bị giao tiếp và cáp. Mỗi thiết bị hoạt động như một bộ chuyển tiếp (repeater), khuếch đại tín hiệu giữa các máy trạm.




*Hình 5.4* Hình trạng RING

Các tín hiệu điện hoặc điện từ được truyền từ thiết bị này tới thiết bị khác chỉ theo một hướng. Mỗi thiết bị kết hợp một thiết bị nhận ở cáp đến (receiver) và một thiết bị phát (transmitter) ở cáp đi. Các tín hiệu được lặp lại và tái sinh ở mỗi thiết bị sao cho sự suy hao là nhỏ nhất. Một ví dụ sử dụng hình trạng vòng là mạng cục bộ *Token Ring*. Loại mạng vòng này sử dụng việc *truyền thẻ bài* (token passing) để cho phép từng máy tính gửi dữ liệu trên mạng.

Một *thẻ bài* (token) là một gói dữ liệu nhỏ (3 byte) cho phép các nút truy xuất mạng. Nút (máy tính) gửi phải lấy thẻ bài và bổ sung thông tin địa chỉ, thông tin điều khiển riêng cùng với dữ liệu để hình thành một frame dữ liệu. Sau đó frame này được truyền trên mạng tới nút kế tiếp trong vòng. Nếu frame

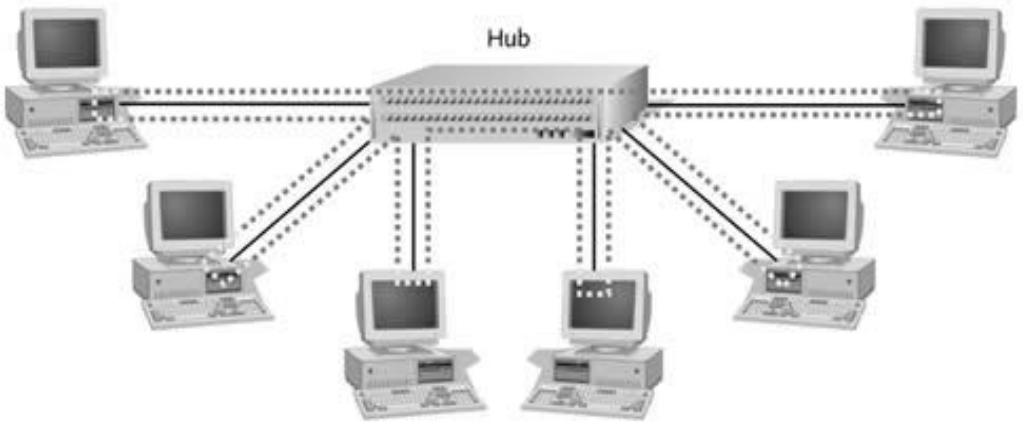
dữ liệu không phải dành cho nút kế tiếp thì nút này tái sinh lại tín hiệu và truyền tiếp nó trên mạng. Quá trình này tiếp tục cho đến khi nút nhận lấy được frame dữ liệu. Sau khi nhận được frame dữ liệu, nút nhận đáp lại nút gửi ban đầu bằng cách phát ra một đáp ứng truyền trên mạng cũng ở dạng một frame dữ liệu. Frame này di chuyển quanh mạng theo cùng hướng trước đây cho đến khi nó chạm tới nút gửi ban đầu. Khi đó frame này sẽ bị loại bỏ khỏi mạng, và một thẻ bài mới lại được sinh ra và truyền trên dây để cho một nút khác nhận nó, tạo frame dữ liệu và truyền tiếp v.v…. Quá trình này đảm bảo là ở bất kỳ thời điểm nào chỉ có thể có một nút truyền dữ liệu trên mạng .

- *Ưu điểm của hình trạng* RING*:*
  - Các lỗi về cáp xác định dễ dàng
  - Vòng đôi (Dual loop ring) có thể chống lỗi tốt.
- *Nhược điểm của hình trạng* RING*:*
  - Việc cài đặt, thay đổi và cấu hình lại khó khăn hơn hình trạng bus.
  - Lỗi về đường truyền trên các vòng đơn làm ngừng hoàn toàn hoạt động của mạng.
  - Các đầu nối khá đắt, đặc biệt là các đầu nối IBM (IBM connectors).

## 5.3 Các hình trạng LAN hỗn hợp

### 5.3.1 Star-Wired Ring

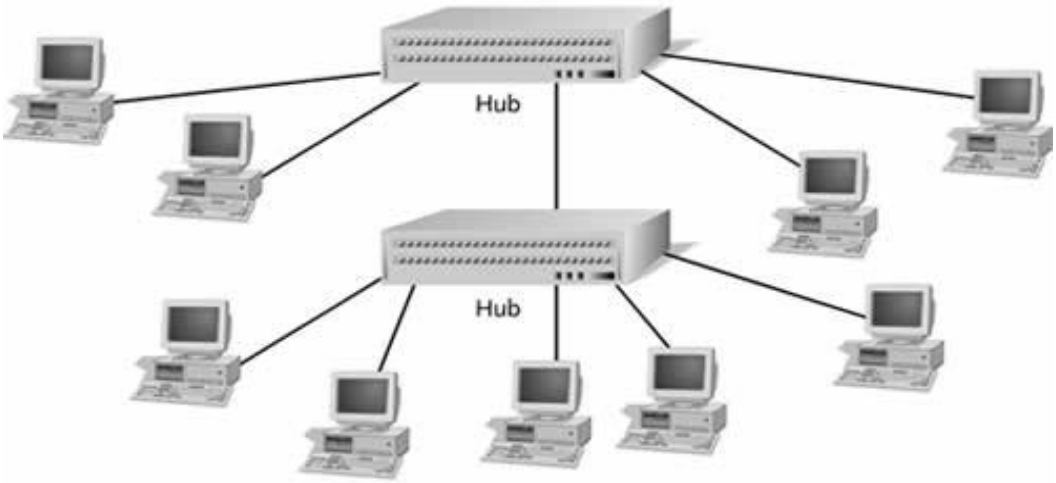
Một mạng hình trạng **star-wired ring** sử dụng cách sắp xếp vật lý của mạng *hình sao*, nhưng tích hợp phương pháp *truyền thẻ bài* (token passing). Dữ liệu được gửi quanh star theo một vòng khép kín. Điều này cho phép cơ chế chống lỗi tốt hơn mạng star và bổ sung thêm tính tin cậy của việc truyền thẻ bài. Những mạng vòng hiện nay thường sử dụng hình trạng hỗn hợp này. Trong hình 5.5 dưới đây, các đường nối liền nét đậm biểu diễn cáp vật lý kết nối hub và các trạm theo hình trạng STAR, trong khi các đường không liền nét biểu diễn vòng luận lý của hình trạng RING.




*Hình 5.5* Hình trạng mạng cục bộ Star-wired Ring

### 5.3.2 Star-Wired Bus

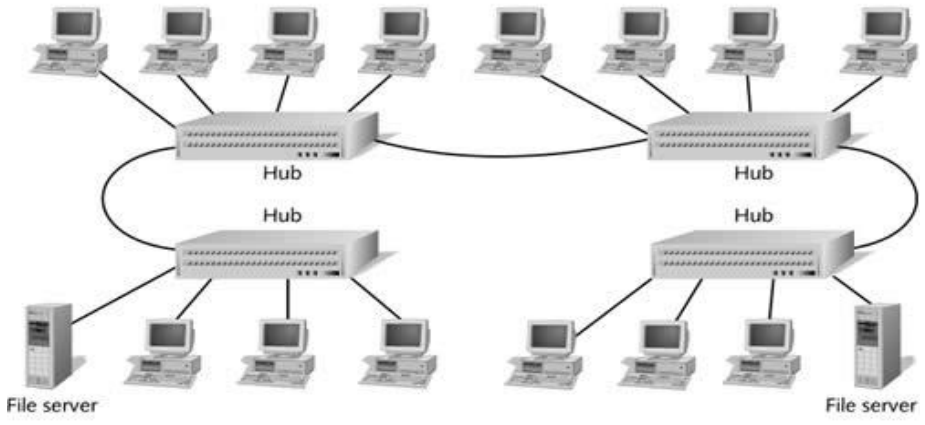
Một hình trạng **star-wired bus** là một dạng khác của hình trạng hỗn hợp. Các nhóm máy tính trạm được kết nối tới hub theo dạng *hình sao*, sau đó các hub được kết nối với nhau qua *đường trục đơn* (single bus). Điều này cho phép liên kết dễ dàng các phân đoạn mạng khác nhau và thường được sử dụng trong các mạng Ethernet và Fast Ethernet.




*Hình 5.6* Hình trạng mạng cục bộ Star-wired Bus

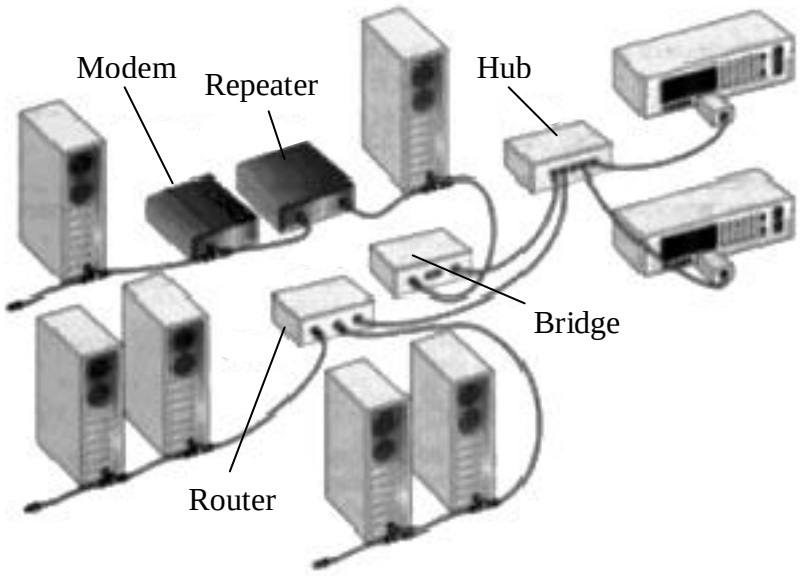
### 5.3.3 Daisy-Chained

Một mạng hình dạng *vòng hoa cúc* (daisy chain) thì tương tự như hình trạng star-wired bus. Các mạng sử dụng hình trạng star-wired bus hoặc star-wired ring có thể kết nối với nhau để hình thành một chuỗi vòng hoa phức tạp hơn. Đây là một kỹ thuật đơn giản mở rộng mạng LAN với chi phí bổ sung ít. Các quản trị mạng nên nhớ rằng, những hình trạng mạng đơn giản như Ethernet bị hạn chế về số phân đoạn có thể kết nối mà không bị mất tính toàn vẹn dữ liệu. Mặc dù về mặt vật lý rất dễ dàng mở rộng mạng, nhưng nếu chúng ta vượt quá số phân đoạn xác định, mạng của ta sẽ có lỗi.




*Hình 5.7* Một Daisy-chain có hai mạng cục bộ Star-wired Bus

## 5.4 Các hệ thống giao vận mạng




*Hình 5.8* Minh hoạ việc kết nối các thiết bị của mạng LAN (Hub, Repeater, Bridge, Router, Modem v.v….).

Hai hệ thống giao vận mạng phổ biến nhất là Ethernet và Token Ring. Những khái niệm cơ bản mà cả hai hình trạng lôgíc này sử dụng được trình bày ở phần dưới đây.

### 5.4.1 Kỹ thuật chuyển mạch (Switching)

Kỹ thuật chuyển mạch là một thành phần của hình trạng lôgíc mạng mà nó xác định cách thức các kết nối được tạo ra giữa các nút (hoặc trạm) trên mạng. Có ba kiểu chuyển mạch: *chuyển mạch kênh* (circuit switching); *chuyển mạch thông báo* (message switching); *và chuyển mạch gói* (packet switching). Mọi hệ thống giao vận mạng đều dựa trên một trong ba kiểu phương pháp chuyển mạch này. Nội dung về các kỹ thuật chuyển mạch này có thể xem lại ở mục 1.2.3. Phần tiếp theo chỉ trình bày những nét khái quát về các kỹ thuật này.

**1) Kỹ thuật chuyển mạch kênh (Circuit Switching)**

Trong kỹ thuật *chuyển mạch kênh*, một kết nối được thiết lập giữa hai nút mạng trước khi chúng khởi tạo việc truyền dữ liệu. Một tổng băng thông được dành riêng cho kết nối này và vẫn tiếp tục duy trì cho tới khi một trong hai thực thể kết thúc giao tiếp. Một khi kênh giao tiếp được thiết lập, toàn bộ dữ liệu sẽ tiếp tục đi theo cùng một con đường từ nút gửi tới nút nhận.

Kiểu chuyển mạch này không hiệu quả vì nó chiếm dụng băng thông cho trong suốt khoảng thời gian các nút kết nối.

**2) Kỹ thuật chuyển mạch thông báo (Message Switching)**

Kỹ thuật *chuyển mạch thông báo* và kỹ thuật *chuyển mạch kênh* có chung một đặc điểm là dữ liệu (toàn bộ thông báo) luôn luôn đi theo cùng một

đường. Tuy nhiên chuyển mạch thông báo *không duy trì một kết nối liên tục*. Khi một kết nối được tạo ra giữa hai thiết bị, dữ liệu được truyền tới thiết bị thứ hai, sau đó kết nối bị huỷ bỏ. Tiếp theo một kết nối được thiết lập giữa thiết bị thứ hai và thiết bị thứ ba. Một khi dữ liệu đã được truyền tới thiết bị thứ ba, kết nối đó được giải phóng. Quá trình cứ thế tiếp diễn cho đến khi dữ liệu tới đích cuối cùng. Kiểu chuyển mạch này sử dụng chương trình *lưu trữ* và *đẩy tới* (store and forward). Dữ liệu được đẩy đi từ một thiết bị này tới thiết bị kế tiếp, lưu trữ tại đó trước khi được đẩy tới thiết bị thứ ba. Kỹ thuật chuyển mạch thông báo đòi hỏi bộ nhớ lưu trữ tạm thời cao và những phí tổn xử lý tại các nút trung gian.

**3) Kỹ thuật chuyển mạch gói (Packet Switching)**

Như đã trình bày trong mục 1.2.3, kỹ thuật *chuyển mạch gói* ngắt dữ liệu thành những khối dữ liệu nhỏ, kích thước của nó có thể quản lý được - những khối này được gọi là các *gói* (packet) - trước khi chúng được truyền ngang qua mạng. Mỗi một gói có thể có con đường riêng qua mạng để tới đích cuối cùng của nó vì mỗi gói có cả hai địa chỉ nguồn và địa chỉ đích. Nói một cách khác, mỗi gói có thể tìm được kênh nhanh nhất tới đích ở bất kỳ thời điểm nào.

Nút đích trên mạng chuyển mạch gói nhận các gói và hợp nhất chúng lại theo đúng trình tự ban đầu dựa trên thông tin điều khiển bên trong gói. Kỹ thuật này tạo ra những phí tổn, mà nó không thích hợp cho việc truyền hình ảnh và âm thanh. Ưu điểm lớn nhất của kỹ thuật chuyển mạch gói là không tồn tại một con đường cố định trong khi dữ liệu được gửi từ một nút này tới nút kia và không đòi hỏi việc xử lý bởi các thiết bị trên đường truyền. Kỹ thuật chuyển mạch gói được sử dụng trong các mạng Ethernet, FDDI và Frame Relay.

### 5.4.2 Đa truy nhập có cảm nhận sóng mang / Phát hiện xung đột (Carrier Sense Multiple Access / Collision Detection - CSMA/CD)

Các hệ thống tranh chấp hoạt động dựa trên nguyên tắc: việc truy xuất đường truyền được thực hiện trên cơ sở thực thể nào chiếm dụng đường truyền đầu tiên sẽ được quyền truyền dữ liệu. Trước khi một trạm Ethernet truyền dữ liệu, nó lắng nghe kênh truyền có ở trạng thái tích cực hay không. Giao thức Ethernet thường được mô tả như giao thức "*lắng nghe trước khi truyền"* ("listen before talking"). Một kênh truyền được gọi là tích cực (activity), nếu như có bất kỳ tín hiệu đang được truyền bởi một trạm Ethernet nào đó. Sự xuất hiện của một tín hiệu truyền được gọi là *sóng mang* (carrier). Mỗi trạm có thể cảm nhận sự có mặt của một sóng mang.

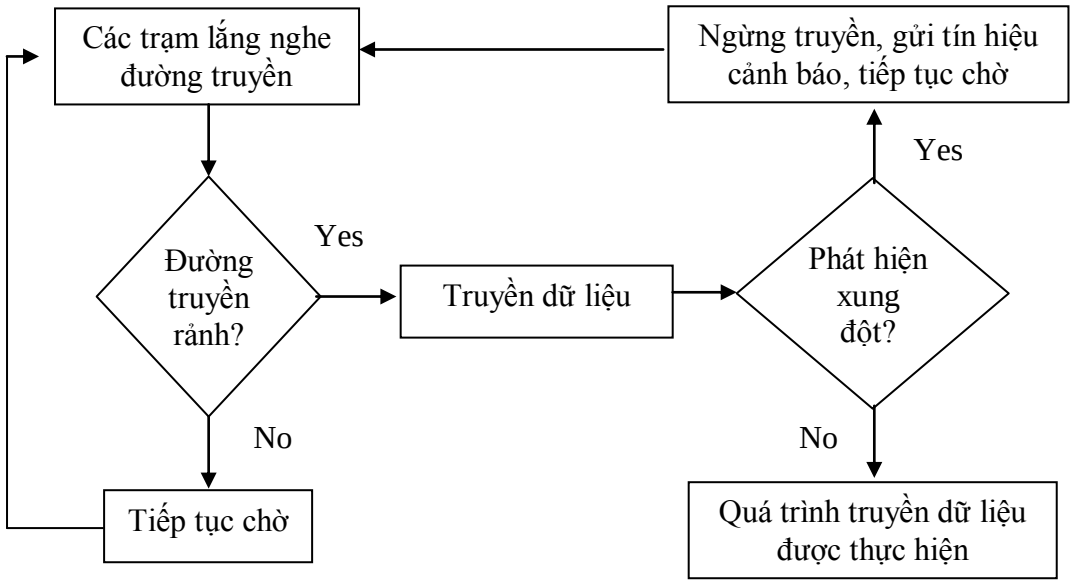
Nếu một trạm phát hiện kênh truyền đang ở trạng thái bận (trạng thái tích cực), trạm đó không thực hiện việc truyền dữ liệu. Sau khi bit cuối cùng của frame truyền qua, tầng *Ethernet Data Link* tiếp tục chờ tối thiểu 9,6 mili giây để tạo ra khoảng cách giữa các frame. Ở cuối thời điểm này, nếu một frame dữ liệu đang chờ để được truyền và nếu kênh truyền rảnh, quá trình truyền được khởi tạo. Nếu trạm không có dữ liệu để truyền, nó lại tiếp tục quá trình cảm nhận sóng mang ("Listen Before Talk" - LBT). Khoảng cách giữa các frame cung cấp thời gian hồi phục (recovery time) cho các trạm Ethernet khác.

Nếu một trạm vẫn cố truyền dữ liệu khi kênh truyền đang ở trạng thái bận, *sự đụng độ* (collision) xảy ra và kết quả là dữ liệu không đến được trạm đích hoặc nếu có đến thì cũng bị sai lệch. Nếu kênh truyền ở trạng thái rảnh (không một sóng mang nào được phát hiện), trạm đang lắng nghe có quyền truyền dữ liệu. Vì có nhiều trạm được kết nối tới kênh Ethernet sử dụng cơ chế cảm nhận sóng mang nên hệ thống này được gọi là *đa truy nhập có cảm nhận sóng mang* (Carrier Sense with Multiple Access - CSMA).

Một sự đụng độ cũng sẽ sẽ xảy ra nếu hai trạm quyết định truyền dữ liệu ở cùng một thời điểm mà kênh truyền không ở trạng thái tích cực. Những đụng độ xảy ra trong suốt quá trình hoạt động bình thường của mạng cục bộ Ethernet vì các trạm truyền dữ liệu chỉ dựa vào một sự kiện duy nhất: có tồn tại một sóng mang trên kênh truyền hay không.

Các trạm Ethernet giảm thiểu sự đụng độ bằng cách phát hiện những đụng độ khi chúng xảy ra. Vì thế thuật ngữ CSMA/CD mô tả cơ chế truy xuất đường truyền Ethernet, trong đó CD là viết tắt của Collision Detect (*phát hiện xung đột*). Cơ chế phát hiện xung đột này được gọi là "*nghe trong khi nói"* ("Listen While Talk" – LWT). Khi xảy ra xung đột các trạm (đang truyền dữ liệu ) ngừng việc truyền dữ liệu. Trạm đầu tiên phát hiện ra xung đột sẽ gửi một tín hiệu sóng mang đặc biệt tới tất cả các trạm kết nối tới mạng để cảnh báo sự kiện xung đột này. Sau khi một xung đột xảy ra, tất cả các trạm chờ đợi trong một thời đoạn ngẫu nhiên nào đó. Việc truyền chỉ xảy ra sau khi kết thúc thời đoạn này. Việc xử lý độ trễ truyền dẫn trước khi truyền có thể giảm đi những xung đột. Vì thế Ethernet không thích hợp cho các ứng dụng thời gian thực.

Giản đồ sau đây minh họa quá trình CSMA/CD.




*Hình 5.9* Quá trình CSMA/CD

## 5.5 Kiến trúc Ethernet

Sự mô tả về mạng Ethernet được xác định trong chuẩn IEEE 802.3. Về *giao thức,* mạng này sử dụng phương pháp CSMA/CD để truy xuất đường truyền. *Hình trạng* chính của Ethernet là đường trục bus tuyến tính, tuy nhiên mỗi thành phần của nó có thể là hình trạng star. (Star-wired bus)

### 5.5.1 Các loại cáp mạng Ethernet

Ethernet có thể hoạt động trên ba loại cáp khác nhau, mỗi loại có những hạn chế, yêu cầu và các thành phần riêng. Mạng Ethernet chủ yếu sử dụng cáp Ethernet chuẩn (Thicknet) và cáp Ethernet mảnh (Thinnet). Chi tiết về các loại cáp này xem lại phần *Coaxial cable* của chương 3.

Ngoài hai loại chính trên, hiện nay trong các mạng cục bộ Ethernet còn sử dụng loại cáp xoắn đôi không bọc kim loại (unshielded twisted-pair – UTP). Chi tiết về loại cáp này xem lại phần *Twisted Pair Cable* của chương 3.

Chuẩn Ethernet IEEE 802.3 mô tả ba loại cáp sử dụng trong mạng Ethernet là 10Base2, 10Base5 và 10Base-T (xem lại chương 3).

Mạng Ethernet là một lựa chọn tốt cho các mạng có lưu lượng đôi khi thay đổi mạnh. Mạng Ethernet không thích hợp cho các kiến trúc mạng cục bộ có yêu cầu tải ổn định.

Một ưu điểm của mạng Ethernet là khả năng sử dụng các giao thức khác, đặc biệt là giao thức TCP/IP (Transmission Control Protocol/Internet Protocol). Chính điều này làm cho mạng Ethernet dễ dàng cho việc truy xuất các minicomputer và các trạm công suất cao. Mạng Ethernet cũng là một chọn lựa tốt cho các mạng trong môi trường kỹ thuật, vì các nút trong môi trường này thường là các trạm cài đặt hệ điều hành UNIX sử dụng giao thức TCP/IP.

### 5.5.2 Phân đoạn mạng Ethernet

Một mạng Ethernet bao gồm các nút gắn tới đường trục bus của nó ở những cự ly khác nhau. Đường trục bus này thực sự là cáp chính dài của mạng Ethernet. Phần cáp chính này và các nút gắn tới nó được gọi là *phân đoạn mạng* Ethernet (Ethernet trunk segment).

Đa số các mạng Ethernet không thực thi một cáp dài. Thông thường cáp phân đoạn mạng được chia thành một dãy các cáp được kết nối qua các bộ chuyển tiếp(repater), cầu (bridge) và các bộ tìm đường (router).

Bảng ở phần 5.5.3 và 5.5.4 dưới đây là những mô tả chuẩn IEEE 802.3, trong đó cáp phân đoạn được giới hạn trong khoảng cách có thể truyền một tín hiệu. Cáp phân đoạn có chiều dài cực đại và bị hạn chế số nút có thể gắn tới nó. Phân đoạn mạng có thể được chia thành các đơn vị nhỏ hơn bằng việc sử dụng các đầu nối (connector). Phân đoạn mạng cáp đồng trục dày có chiều dài tối đa 500 mét (1640 feet) và có thể có tối đa 100 nút. Phân đoạn mạng cáp đồng trục mảnh có chiều dài tối đa 185 mét (607 feet) và có thể gắn tối đa 30 nút.

Một bộ chuyển tiếp (repeater) là một thiết bị dùng để mở rộng chiều dài của cáp phân đoạn mạng Ethernet. Các phân đoạn mạng bổ sung có thể mở rộng phân đoạn mạng Ethernet, tuy nhiên một phân đoạn mạng không thể được mở rộng vượt quá giới hạn xác định. Chú ý rằng mỗi nút cuối của một phân đoạn phải được gắn đầu nối terminator và một trong các nut phải được nối đất.

Mạng Ethernet không có một hub hoặc concentrator riêng như đối với hình trạng ring hoặc star. Mỗi cáp phân đoạn riêng rẽ đóng vai trò như một hub hoặc concentrator.

Một mạng Ethernet cũng có thể kết hợp các cáp Thinnet và Thicknet trong cùng một mạng. Tuy nhiên mỗi loại cáp có đặc tính kỹ thuật riêng và việc cài đặt mạng phải tuân theo các đặc tính của cả hai loại cáp này.

### 5.5.3 Các quy tắc nối cáp Ethernet mảnh (10Base2)

Các tham số cho cáp Ethernet mảnh (10Base2) được trình bày trong bảng dưới đây:

| **Các tham số cho cáp Ethernet mảnh (10Base2)** | **Giá trị** |
|---|---|
| Tốc độ cực đại của dữ liệu | 10 Mbps |
| Số repeater cực đại | 4 |
| Chiều dài cực đại cho phân đoạn cáp đồng trục | 185 mét |
| Số trạm cực đại / 1 phân đoạn | 30 |
| Tổng số trạm cực đại | 90 |
| Khoảng cách nhỏ nhất giữa các trạm | 0,5 mét |

### 5.5.4 Các quy tắc nối cáp Ethernet dày (10Base5)

Các tham số cho cáp Ethernet dày được trình bày trong bảng sau:

| **Các tham số cho cáp Ethernet dày (10base5)** | **Giá trị** |
|---|---|
| Tốc độ cực đại của dữ liệu | 10 Mbps |
| Số repeater cực đại | 4 |
| Chiều dài cực đại cho phân đoạn cáp đồng trục | 500 mét |
| Chiều dài cáp cực đại của transceiver | 50 mét |
| Chiều dài cực đại của phân đoạn mạng nối kết | 1500 mét |
| Số trạm cực đại / 1 phân đoạn | 100 |
| Tổng số trạm cực đại | 300 |
| Khoảng cách giữa các trạm | n*2,5 mét (n=1,2,3, …) |

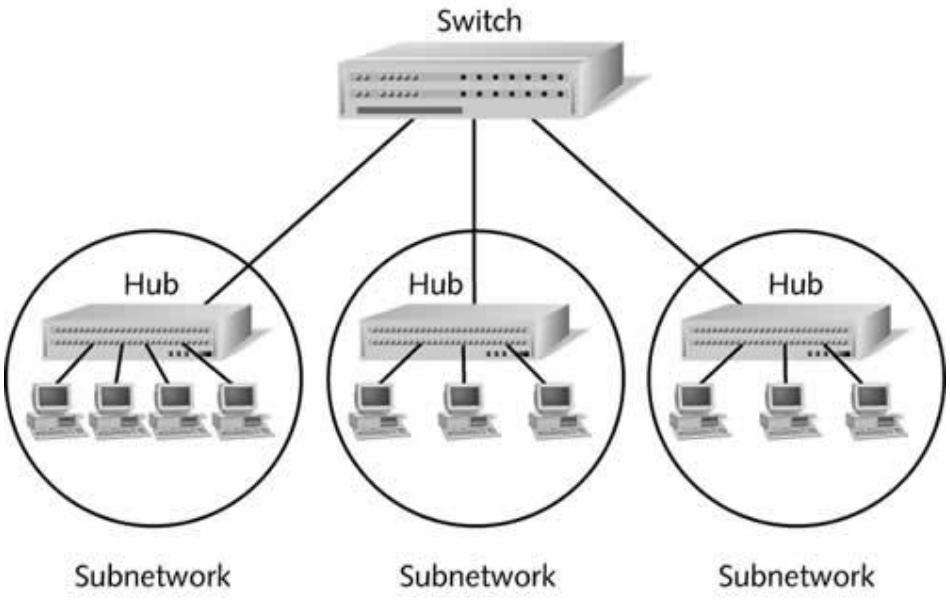
### 5.5.5 Mạng Ethernet dùng chung (Shared Ethernet)

Các mạng cục bộ Ethernet truyền thống gọi là mạng *Ethernet dùng chung*. Mạng này cung cấp tổng băng thông cố định được dùng chung giữa các thiết bị kết nối trên một phân đoạn. Hai nút mạng không thể gửi và nhận dữ liệu đồng thời, vì mạng Ethernet dùng chung này sử dụng một **hub** có chức năng nhận tín hiệu, sau đó khuếch đại và truyền lại tín hiệu đó tới mọi thiết bị.

### 5.5.6 Mạng Ethernet chuyển mạch (Switched Ethernet)

Mạng *Ethernet chuyển mạch* sử dụng một bộ chuyển mạch (**switch**) thay cho một hub. Switch này có thể phân tách một phân đoạn mạng thành các phân đoạn mạng độc lập nhỏ hơn. Mỗi phân đoạn nhỏ này có thể có lưu lượng riêng và cho phép nhiều nút truyền và nhận dữ liệu đồng thời. Như vậy, một mạng Ethernet chuyển mạch trở thành nhiều mạng *Ethernet dùng chung* độc lập, liên kết với nhau bởi switch. Điều này có nghĩa là băng thông được sử dụng hiệu quả hơn nhiều.

Mạng *Ethernet chuyển mạch* có những cải tiến đáng kể vì số các nút hoặc trạm đang tranh chấp đường truyền mạng ở bất kỳ khoảng thời gian nào được giảm đi rõ rệt. Chẳng hạn, nếu có 100 trạm trên mạng *Ethernet chuyển mạch,* mạng này có 100 máy tính đang cố giao tiếp cùng một lần. Vì mạng Ethernet sử dụng phương pháp CSMA/CD, khả năng xung đột là rất lớn. Tuy nhiên, nếu phân đoạn 100 trạm này được phân chia thành bốn phân đoạn độc lập (với số trạm ngang đều nhau) bằng việc sử dụng một switch, chỉ có 25 trạm tranh chấp đường truyền mạng. Điều này giảm thiểu khả năng xung đột một cách đáng kể.



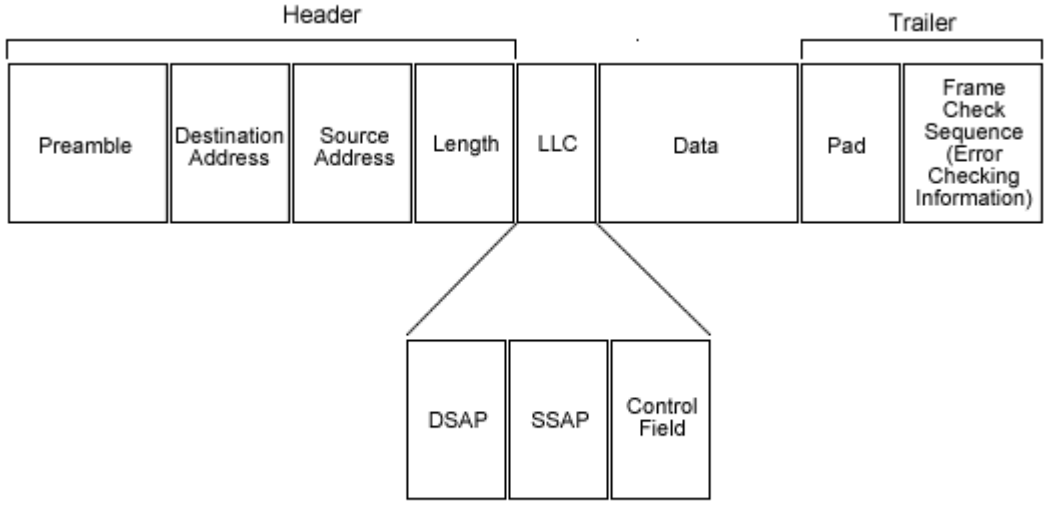

*Hình 5.10* Mạng Ethernet chuyển mạch

### 5.5.7 Các kiểu khuôn dạng Ethernet (Ethernet Frame Types)

Có bốn kiểu khuôn dạng dữ liệu khác nhau được sử dụng trong mạng Ethernet bao gồm **Ethernet 802.2**, **Ethernet 802.3**, **Ethernet II,** và **Ethernet SNAP** (Xem lại mục 2.3.1 giới thiệu về khuôn dạng Ethernet tổng quát) . Mỗi kiểu khuôn dạng có phần khác nhau và chúng đều có bốn trường chung: địa chỉ nguồn (*source addres),* địa chỉ đích (*destination address),* dữ liệu (*data)* và trường kiểm tra lỗi (*error-checking*). Các kiểu khuôn dạng Ethernet được sử dụng thông thường nhất là Ethernet 802.2 và Ethernet 802.3. Các khuôn dạng Ethernet có kích thước biến đổi từ tối thiểu 64 byte tới tối đa 1518 byte. (Mỗi khuôn dạng chứa thông tin *header* kích thước14 byte cộng với trường *Frame Check Sequence* chiều dài 4 byte. Phần *dữ liệu* của khuôn dạng có kích thước biến đổi từ 46 byte tới tối đa 1500 byte. Kích thước tổng cộng của frame được tính toán đơn giản bằng cách cộng kích thước của tất cả các trường – Nếu trường dữ liệu của frame nhỏ hơn 46 byte, frame sẽ được đệm thêm trường *pad* để kích thước tối thiểu của nó là 46 byte.

***a) 802.2***

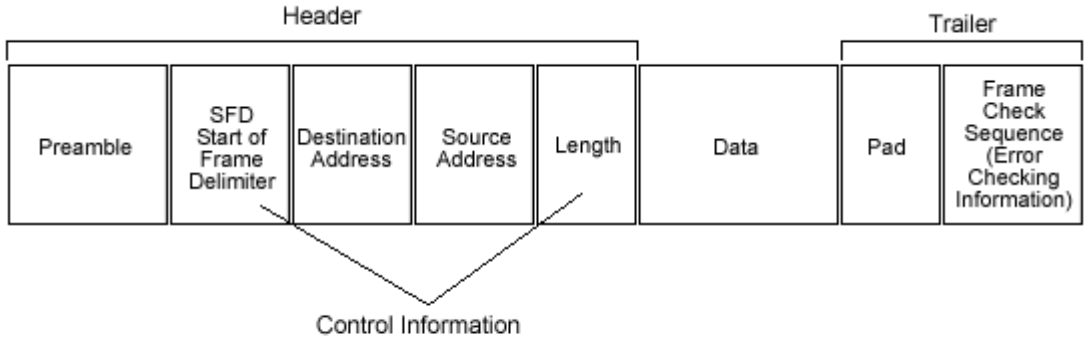
Khuôn dạng **Ethernet 802.2** là khuôn dạng mặc định được sử dụng cho mạng Novell Netware 4.x và hệ điều hành mạng cao hơn. Khuôn dạng này hỗ trợ giao thức IPX/SPX cũng như giao thức TCP/IP và là khuôn dạng Ethernet thông thường nhất được sử dụng ngày nay. Các khuôn dạng này chứa một *điểm truy nhập dịch vụ đích* (Destination Service Access Point - **DSAP)** và một *điểm truy nhập dịch vụ nguồn* (Source Service Access Point - **SSAP)**. Một *điểm truy nhập dịch vụ* (Service Access Point - SAP) định danh một nút hoặc quá trình bên trong, mà quá trình này sử dụng tầng con Logical Link Control của tầng Data Link. Mỗi quá trình xảy ra giữa nút nguồn và nút đích trên mạng có một SAP duy nhất.




*Hình 5.11* Một khuôn dạng Ethernet 802.2 điển hình

### *b) 802.3*

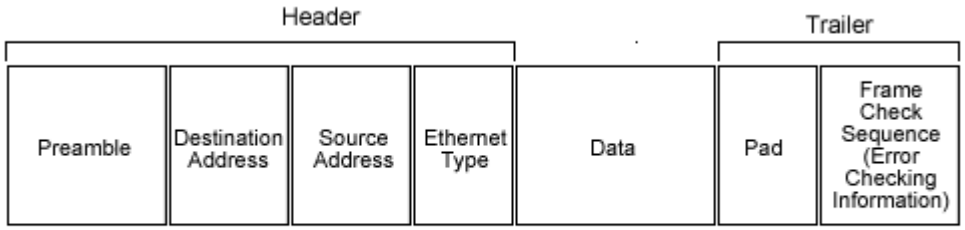
Kiểu khuôn dạng **Ethernet 802.3** là kiểu khuôn dạng Novell Netware ban đầu. Nó dùng cho các mạng đang sử dụng Novell Netware 3.12 và các phiên bản thấp hơn. Giống như Ethernet 802.2, kiểu khuôn dạng này cũng hỗ trợ giao thức IPX/SPX, nhưng nó không hỗ trợ các giao thức khác như TCP/IP. Không có các bit điều khiển (DSAP và SSAP) bên trong khuôn dạng 802.3.




*Hình 5.12* Một khuôn dạng Ethernet 802.3 điển hình

### *c) Ethernet II*

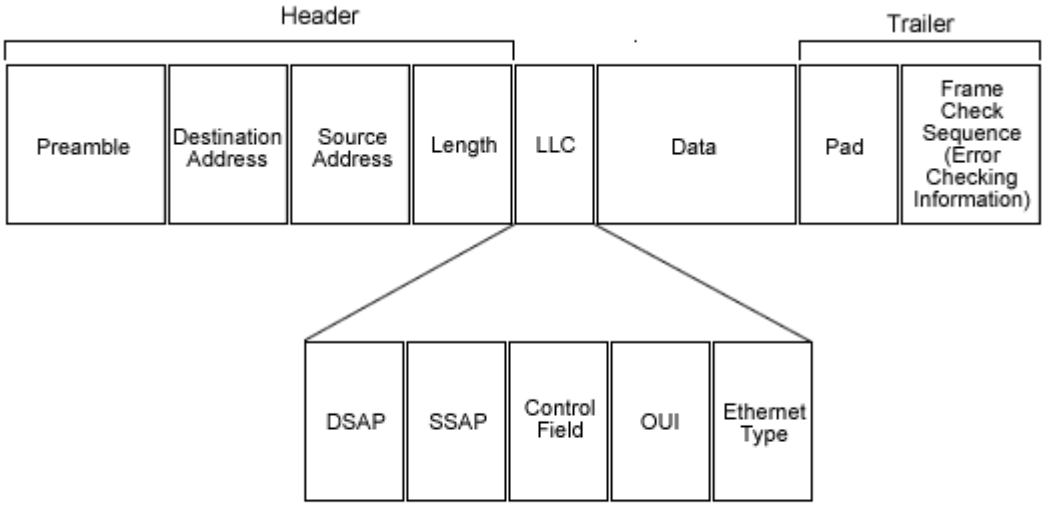
Ethernet II là kiểu khuôn dạng Ethernet đầu tiên được phát triển bởi DEC, Intel và Xerox. Nó được phát triển trước chuẩn IEEE 802. Nó tương tự khuôn dạng Ethernet 802.3, nhưng không chứa trường *length*. Thay thế, khuôn dạng Ethernet II chứa trường *Ethernet Type*, mà nó cho phép phân biệt việc sử dụng các giao thức IPX/SPX, TCP/IP và AppleTalk (Nội dung các giao thức này xem lại ở chương 4)




*Hình 5.13* Một khuôn dạng Ethernet II điển hình

### *d) Ethernet SNAP (Sub-Network Access Protocol)*

**Ethernet SNAP** là một sự điều chỉnh của khuôn dạng Ethernet 802.2 và Ethernet II. Kiểu khuôn dạng này sử dụng cùng các trường điều khiển như khuôn dạng 802.2 – *Destination Service Access Point (DSAP)* và *Source Service Access Point (SSAP)*. Nó cũng bổ sung trường *Ethernet Type* từ khuôn dạng Ethernet II cộng thêm một trường khác gọi là trường **Organisation ID (OUI)**. Trường này định danh kiểu mạng mà các khuôn dạng đó đang hoạt động. Ethernet SNAP thì thích hợp với các giao thức IPX/SPX, TCP/IP và AppleTalk, nhưng khuôn dạng này hiếm khi được sử dụng.




*Hình 5.13* Một khuôn dạng Ethernet SNAP điển hình

## 5.6 Mạng Token Ring

### 5.6.1 Kỹ thuật truyền thẻ bài (Token Passing)

Trong các hệ thống truyền thẻ bài, một frame dữ liệu nhỏ (token) được truyền lần lượt từ thiết bị này đến thiết bị khác. Một thẻ bài là một thông báo đặc biệt mà khi thiết bị nào lưu giữ nó, thiết bị đó tạm thời có quyền điều khiển đường truyền. Kỹ thuật truyền thẻ bài phân bố việc điều khiển truy xuất giữa các thiết bị mạng.

Mỗi thiết bị biết được thiết bị nào truyền thẻ bài tới nó cũng như thiết bị nào sẽ nhận thẻ bài do nó truyền đi (các thiết bị đứng trước và sau nó trong vòng lôgíc). Mỗi thiết bị định kỳ lấy quyền điều khiển thẻ bài, thực hiện nhiệm vụ của nó, và sau đó truyền thẻ bài cho thiết bị kế tiếp sử dụng. Các giao thức giới hạn mỗi thiết bị có thể kiểm soát thẻ bài trong bao lâu.

Tồn tại một số giao thức truyền thẻ bài. Hai chuẩn về mạng LAN truyền thẻ bài là *Token Bus* IEEE 802.4 và *Token Ring* 802.5. Mạng *Token Bus* sử dụng phương pháp điều khiển truy xuất bằng truyền thẻ bài và một hình trạng bus vật lý hoặc lôgíc, trong khi mạng *Token Ring* cũng sử dụng phương pháp điều khiển truy xuất bằng truyền thẻ bài nhưng hình trạng vật lý hoặc lôgíc là ring. Một chuẩn truyền thẻ bài khác (dùng cho các mạng LAN cáp sợi quang) được gọi là FDDI (Fibre-Distributed Data Interface).

Kỹ thuật truyền thẻ bài thì thích hợp cho các mạng có tải thay đổi mạnh theo thời gian chẳng hạn như các mạng truyền hình ảnh hoặc âm thanh số hoá hoặc các mạng có tải cao.

### 5.6.2 Kiến trúc Token Ring

Kiến trúc *Token Ring* tuân theo các chuẩn được tạo ra bởi IEEE 802.5 thuộc về một đề án có tên **Project 802.**

Hình trạng của *Token Ring* được sử dụng là star-wired ring, với ring được hình thành bởi hub. Các nút được gắn với ring (hoặc hub) tạo thành star. Mạng

*Token Ring* sử dụng phương pháp *xác định* (chứ không *ngẫu nhiên* như giao thức CSMA/CD) để truy xuất cáp. Thẻ bài – một khối bít xác định trước – cho phép một nút giao tiếp với cáp. Thẻ bài được truyền từ nút này tới nút kia cho tới khi một nút có yêu cầu truyền dữ liệu – quá trình này được gọi là *truyền thẻ bài* (**token passing**). Ta cần chú ý là phải tồn tại một vòng để thẻ bài di chuyển theo ở mọi thời điểm. Dữ liệu di chuyển trên vòng chỉ theo một hướng.

Mạng *Token Ring* có hai kiểu chính với tốc độ truyền dữ liệu là 4 và 16 Mbps, cả hai kiểu này đều dùng kỹ thuật truyền băng tần cơ sở. Cả hai kiểu mạng *Token Ring* đều có khả năng sử dụng cáp xoắn đôi không bọc kim loại, cung cấp khả năng tăng độ tin cậy cũng như mở rộng khoảng cách truyền tín hiệu.

### 5.6.3 Các thành phần của Token Ring

Có bốn thành phần cơ bản tạo nên mạng *Token Ring*: Token Ring NIC, Token Ring Multistation Access Unit (MAU), Cabling System, và Token Ring Network Connector.

**a) NIC của Token Ring**

Bảng mạch giao tiếp mạng (Network Interface Card - NIC) dùng cho *Token Ring* thì tương tự những NIC sử dụng với các loại mạng khác, chẳng hạn như Ethernet, nhưng được thiết kế đặc biệt cho phương pháp giao vận *Token Ring*. Ta không thể sử dụng NIC của một kiểu mạng này cho một kiểu mạng khác. Các NIC phải được kết nối qua một cáp tới *đơn vị truy xuất nhiều trạm (*Multistation Access Unit – MAU). MAU là một thiết bị tương đương với hub hoặc repeater của *Token Ring*. NIC của *Token Ring* có thông lượng là 4 Mbps hoặc 16 Mbps.

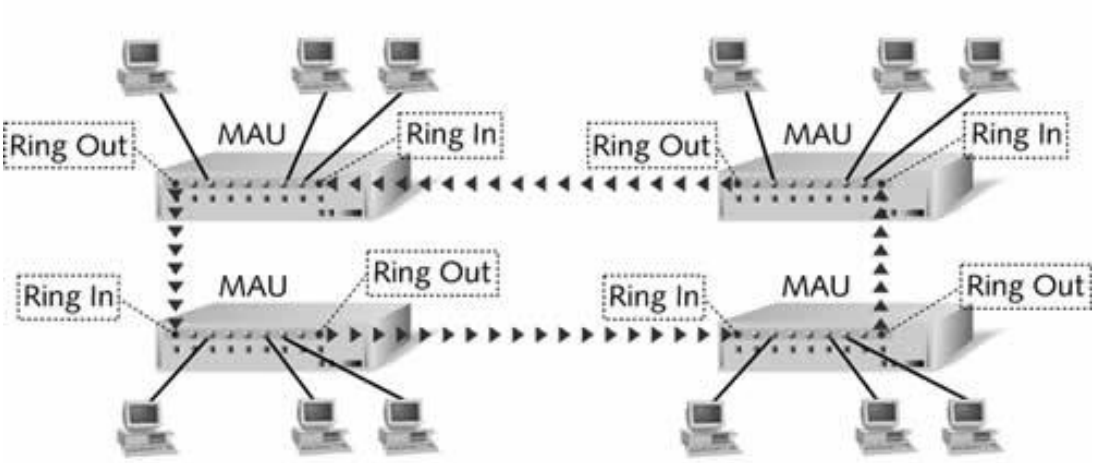
**b) MAU - Đơn vị truy xuất nhiều trạm của Token Ring**

*Đơn vị truy xuất nhiều trạm* được gọi là MAU (Multistation Access Unit ) hoặc là SMAU (Smart Multistation Access Unit). MAU cũng còn được tham chiếu như là một chuẩn 8228 (Đặc tả 8225 của IBM). MAU là một hub của mạng *Token Ring.*

Có 10 cổng trên một MAU 8228, tám cổng dùng cho kết nối các nút mạng, hai cổng còn lại được gọi là cổng *Ring-In* và cổng *Ring-Out*. Hai cổng này được sử dụng khi kết nối một dãy các MAU để duy trì tính toàn vẹn của vòng (Hình 5.14). *Ring-Out* là cổng xuất tín hiệu và *Ring-In* là cổng nhập tín hiệu. Nếu mạng chỉ có một MAU thì cổng *Ring-Out* và cổng *Ring-In* có thể được để nguyên (không kết nối). Nếu bất kỳ cổng nào trên MAU còn để trống, nó sẽ "*tự làm ngắn mạch*" để tạo nên một kết nối nhằm mục đích duy trì vòng.

Mỗi MAU có khả năng kết nối tối đa tám nút. Khi có nhiều hơn các nút được yêu cầu , nhiều MAU được kết nối bằng việc liên kết các cổng *Ring-In* và cổng *Ring-Out* của chúng. Các MAU được cài đặt trong một mạng có thể kết nối tối đa 72 nút khi sử dụng cáp xoắn đôi không bọc kim loại (Unshielded Twisted Pair - UTP) , hoặc tối đa 260 nút khi sử dụng cáp xoắn đội có bọc kim (Shielded Twisted Pair - STP).

Các MAU hoặc hub được nối với nhau để hình thành vòng. Các nút được kết nối tới MAU để tạo thành star của mạng.




*Hình 5.14* Nối kết các MAU Token Ring

**c) Hệ thống cáp**

Có rất nhiều đặc tả cáp Token Ring khác nhau, bao gồm: IBM loại 1, IBM loại 2, IBM loại 3, IBM loại 5, IBM loại 6 và IBM loại 9. Bảng sau đây cho thấy các đặc tính của mỗi loại cáp này.

| Loại cáp IBM | Mô tả |
|---|---|
| **Loại 1**  | ■ Hai cặp cáp xoắn với nhau, sau đó tất cả được bọc bên ngoài<br>■ Kích cỡ 22 AWG, được kiểm tra tới 16Mbps<br>■ Điện trở 150 Ohms ■ 0 % ở tần số 3-20Mhz<br>■ Độ suy hao 22dB / 1 km<br>■ Độ nhiễu (crosstalk) giữa các cặp phải nhỏ hơn 58dB<br>■ Sử dụng cho LAN : giữa các MAU và từ MAU tới vách tường |
| **Loại 2** | ■ Hai cặp xoắn với nhau và được bọc bên ngoài, sau đó hai cặp này được bọc cùng với bốn cặp dùng cho tiếng nói (cáp Unshielded Twisted Pair Category 3)<br>■ Kích cỡ 22 AWG, được kiểm tra tới 16Mbps<br>■ Điện trở 150 Ohms ■ 0 % ở tần số 3-20Mhz<br>■ Độ suy hao 22dB / 1 km<br>■ Độ nhiễu (crosstalk) giữa các cặp phải nhỏ hơn 58dB<br>■ Sử dụng cho LAN: đi xuyên qua các vách tường tới các trạm, mang tiếng nói, sử dụng cho mạng *token ring* và mạng Ethernet 10Base-T. |

| Loại cáp IBM | Mô tả |
|---|---|
| **Loại 3**  | ■ Các cặp cáp xoắn không bọc (Unshielded Twisted Pair )<br>■ Dây có kích cỡ 22 AWG hoặc 24 AWG<br>■ Ít nhất 2 lần xoắn / 1 foot<br>■ Điện trở 100 Ohms ở tần số 256Khz - 2.3Mhz<br>■ Sử dụng cho LAN: nối khắp mạng *Token Ring* |
| **Loại 5**  | ■ Hai cáp sợi quang *multimode*đường kính 62,5/125 micromet. (loại cáp đường kính 50/125 micromet và 100/140 micromet cũng được sử dụng)<br>■ Cáp đường kính 62,5/125 micromet là chuẩn thực tế cho FDDI<br>■ Độ suy hao: 3,75 dB/km khi sử dụng nguồn 850 nm<br>■ Độ suy hao: 1,5 dB/km khi sử dụng nguồn 1300 nm<br>■ Đường kính cáp 8,3/125 micromet cho cáp kiểu đơn<br>■ Các loại đầu nối: SMA, ST, và SC |
| **Loại 6**  | ■ Hai cặp cáp xoắn với nhau, sau đó bọc bên ngoài<br>■ Cáp được bện 26 AWG<br>■ Điện trở 150 Ohms ■ 0 % ở tần số 3-20Mhz<br>■ Sử dụng cho LAN: dùng cho việc nối từ vách tường tới NIC của mỗi trạm, độ dài tối đa 30 mét. |
| **Loại 9**  | ■ Hai cặp cáp xoắn với nhau, sau đó bọc bên ngoài<br>■ Cáp được bện hoặc liền khối 26 AWG<br>■ Điện trở 150 Ohms ■ 0 % ở tần số 3-20Mhz<br>■ Chấp nhận đầu nối RJ-45 (đường kính nhỏ hơn)<br>■ Sử dụng cho LAN: nối từ vách tường tới NIC của trạm |

Cáp bọc kim IBM loại 6 được sử dụng như cáp thích ứng (adapter) nối một trạm tới một MAU. Một đầu cáp có đầu nối tiếp 25 chân để kết nối tới NIC, và đầu cáp kia có một đầu nối dữ liệu IBM dùng để gắn tới hoặc một giá *faceplate* hoặc một MAU IBM 8228.

Cáp IBM loại 6 cũng có thể sử dụng làm cáp chắp nối (patch cable). Chiều dài của cáp loại 6 này biến đổi từ 2,5 mét đến 45 mét, với một đầu nối dữ liệu IBM ở mỗi đầu. Các cáp chắp nối này sau đó được nối với nhau để nối với cáp thích ứng hoặc tới MAU IBM 8228. Ví dụ, cáp chắp nối IBM loại 6 được sử dụng để gắn một nút tới một MAU. Cáp thích ứng chỉ dài 2,5 mét, nhưng khoảng cách tới MAU lớn hơn 2,5 mét. Một cáp chắp nối có thể được sử dụng để mở rộng khoảng cách, nó nối kết cáp thích ứng ở một đầu và MAU ở đầu kia. Cáp IBM loại 6 cũng được sử dụng để nối hai MAU.

Cáp IBM loại 9 được sử dụng chủ yếu khi cần phải đi dây trên trần nhà hoặc qua các khối bê tông. Nó có vỏ bọc bên ngoài đặc biệt và được sử dụng thay cho cáp IBM loại 1 và cáp IBM loại 2.

**d) Các đầu nối cáp Token Ring (Token Ring Connectors )**

Các đầu nối cáp mạng *Token Ring* về cơ bản có ba loại sau:

- Đầu nối dữ liệu cho cáp loại 1 và loại 2.
- Đầu nối điện thoại RJ-45 (8 chân) cho cáp loại 3
- Đầu nối điện thoại RJ-11 (4 chân) cho cáp loại 3

Chú ý rằng các đầu nối RJ thì chỉ dùng cho cáp loại 3. Trong đó RJ-45 được sử dụng rộng rãi hơn. Bổ sung thêm chú ý nữa, khi cáp IBM loại 3 được nối tới MAU, phải cần sử dụng một thiết bị lọc đường truyền loại 3. Thiết bị lọc này cũng cần cho cáp UTP.

### 5.6.4 Các quy tắc thiết kế việc nối cáp mạng Token Ring (IEEE 802.5)

Bảng sau đây tổng quát hoá các quy tắc thiết kế cho việc nối cáp mạng *Token Ring*:

| Các tham số *Token Ring* | Loại 1, 2 | Loại 3 |
|---|---|---|
| Số tối đa thiết bị / vòng | 260 | 96 |
| Tốc độ dữ liệu được kiểm tra | 16Mbps | 4Mbps |
| Khoảng cách tối đa từ trạm tới mạng cục bộ một MAU | 300m | 100m |
| Khoảng cách tối đa từ trạm tới mạng cục bộ nhiều MAU | 100m | 45m |
| Số tối đa các MAU / LAN | 12 | 2 |
| Khoảng cách tối đa từ MAU tới MAU | 200m | 120m |

### 5.6.5 Một số nguyên tắc cho việc đi cáp mạng Token Ring

Sau đây là những nguyên tắc chung cho việc nối cáp *Token Ring* :

1. Các trạm cách MAU 2,5 mét có thể được nối bằng cáp thích ứng 2,5 mét.
2. Các trạm cách MAU hơn 8 feet ( [redacted]50 mét) được nối bằng dây kéo dài.
3. Để tạo một vòng có nhiều MAU, nối một cáp chắp nối từ *Ring-Out* của MAU đầu tiên tới *Ring-In* của MAU thứ nhì. Tiếp tục như vậy cho tất cả các MAU cho tới MAU cuối cùng. Nối *Ring-Out* của MAU cuối cùng tới *Ring-In* của MAU đầu tiên.
4. Ta không thể nối các trạm tới các cổng *Ring-Out* và *Ring-In*. Các cổng *Ring-In* và *Ring-Out* chỉ được sử dụng cho việc nối kết giữa các MAU.
5. Các cáp chắp nối (cáp IBM loại 6) không nên ghép với nhau.
6. Cáp chắp nối (cáp IBM loại 6) không nên được sử dụng trong bất kỳ đường ống, trần nhà hoặc vùng thông khí nào. Có thể thay thế bằng cáp IBM loại 9, được xem như loại cáp rắn chắc.

# Câu hỏi ôn tập chương 5

1. Những phát biểu nào trong các phát biểu sau là đúng (chọn 1):
   a. Mạng LAN giống mạng Internet là không có chủ sở hữu và người quản trị.
   b. Mạng LAN có tốc độ truyền thường *cao hơn* so với mạng diện rộng (WAN)
   c. Mô hình OSI do ISO đưa ra chỉ có thể áp dụng cho mạng LAN.
   d. Mọi phát biểu trên đều đúng.
2. Các ưu điểm của các hình trạng STAR (choose 2):
   a. Dễ cài đặt và cấu hình b. Đòi hỏi ít cáp hơn các hình trạng khác
   c. Dễ phát hiện và sửa chữa các sự cố
3. Nhược điểm của hình trạng BUS (choose 2):
   a. Khó cài đặt và cấu hình hơn hình trạng STAR
   b. Đòi hỏi nhiều cáp hơn các hình trạng khác
   c. Khó mở rộng hơn các hình trạng khác
   d. Khó chẩn đoán và cô lập sự cố.
4. Ưu điểm của hình trạng RING (chọn 2):
   a. Các lỗi về cáp xác định dễ dàng
   b. Việc cài đặt, thay đổi và cấu hình lại dễ dàng hơn hình trạng bus.
   c. Vòng đôi (Dual loop ring) có thể chống lỗi tốt.
   d. Lỗi đường truyền trên vòng đơn không ngừng hoàn toàn hoạt động của mạng.
5. Đa số các mạng cục bộ Ethernet hiện nay đều sử dụng hình trạng …… vì khả năng mở rộng và dễ dàng kết nối với các mạng khác.
   a. STAR b. BUS c. RING
6. Mạng cục bộ Ethernet sử dụng (chọn 2)
   a. Hình trạng Star –wired – bus b. Hình trạng Star –wired – ring
   c. Giao thức truyền thẻ bài d. Giao thức CSMA/CD
7. CSMA/CD là một giao thức truy xuất đường truyền (chọn):
   a. Có điều khiển và xác định b. Ngẫu nhiên c. Cả hai
8. Dữ liệu (và cả thẻ bài ) trong các hình trạng RING di chuyển theo:
   a. Một chiều b. Cả hai chiều c. Quảng bá (broadcast)
9. Mỗi kiểu khuôn dạng (frame) Ethernet có các phần khác nhau nhưng chúng đều có **bốn** trường chung:
   a. Source addres b. Destination address c. Length
   d. Data e. Error-checking information
10. Phát biểu nào là đúng trong các phát biểu sau (chọn 1):
    a. Tổng số tối đa các trạm khi dùng cáp Ethernet dày (10Base5) là: 200 trạm
    b. Khoảng cách tối đa từ trạm tới LAN một MAU dùng cáp IBM loại 3 là 100 m
    c. Để mở rộng mạng *Token Ring* các cáp IBM loại 6 thường được ghép với nhau.

# CHƯƠNG 6 – GIỚI THIỆU WINDOWS 2000

## MỤC TIÊU CỦA CHƯƠNG

*Kết thúc chương này bạn có thể:*

- Biết được các phiên bản của Windows 2000
- Một số đặc điểm mới của Windows 2000
- Các mô hình làm việc trên Windows 2000

## 6.1 Các phiên bản của Windows 2000

Windows 2000 là hệ điều hành máy chủ được sử dụng phổ biến nhất hiện nay của Microsoft. Nó được xây dựng trên nền của kỹ thuật Windows NT, nhưng nó tin cậy, linh động, dễ phát triển, dễ quản lý và sử dụng hơn bất kỳ phiên bản nào trước kia của Windows. Gia đình Windows 2000 có bốn hệ điều hành: *Windows 2000 Professional, Windows 2000 Server*, *Windows 2000 Advanced Server* và *Windows 2000 Datacenter Server*. Chúng được tóm tắt trong bảng sau:

| Hệ điều hành | Mô tả |
|---|---|
| **Windows 2000 Professional** | Windows 2000 Professional thay thế cho Windows 95, Windows 98 và Windows NT 4.0 Workstation. Nó được thiết kế cho các loại máy tính cá nhân để bàn. |
| **Windows 2000 Server** | Windows 2000 Server có tất cả các đặc tính của Windows 2000 Professional, cộng thêm các dịch vụ quản lý mạng. Phiên bản này của Window 2000 rất lý tưởng đối với các dịch vụ file và máy in, dịch vụ Web và nhóm làm việc. |
| **Windows 2000 Advanced Server** | Windows 2000 Advanced Server có tất cả các đặc điểm của Windows 2000 Server, thêm các tính năng như có thể cho phép nhiều người dùng tài nguyên hệ thống cùng một lúc. Phiên bản này của Windows 2000 được thiết kế để quản lý cho các mạng xí nghiệp và các cơ sở dữ liệu chuyên dùng. |
| **Windows 2000 Datacenter Server** | Windows 2000 Datacenter Server có tất cả các đặc điểm của Windows 2000 Advanced Server, cộng thêm chức năng hỗ trợ nhiều bộ nhớ hơn và nhiều CPU trên một máy tính. Windows 2000 Datacenter Server là mạnh nhất trong gia Windows 2000. Nó được thiết kế để quản lý kho dữ liệu lớn, xử lý giao dịch trực tuyến và giả lặp mềm dẻo và các dự án hợp nhất máy chủ. |

## 6.2 Một số đặc điểm mới của Windows 2000

Mặc dù Windows 2000 được xây dựng trên nền tảng của Windows NT, nhưng nó có nhiều tính năng nổi bật hơn so với các phiên bản trước của Windows, bao gồm:

| Các đặc điểm | Mô tả |
|---|---|
| **Active Directory** | Active Directory là dịch vụ thư mục có thể phục vụ nhiều người dùng, được xây dựng từ cơ sở bằng cách sử dụng công nghệ chuẩn Internet, và tích hợp đầy đủ mức hệ điều hành. Active Directory đơn giản hoá việc quản trị và giúp cho người dùng dễ dàng tìm kiếm tài nguyên. Active Directory cung cấp nhiều đặc điểm và khả năng, bao gồm chính sách nhóm, nhiều người cùng làm việc mà không phức tạp, hỗ trợ nhiều giao thức thẩm định quyền, và sử dụng các chuẩn của Internet. |
| **Active Directory Service Interfaces (ADSI)** | ADSI là mô hình dịch vụ thư mục và là tập của các giao diện Component Object Service Model (COM). Nó cho phép các ứng dụng chạy trên các hệ điều hành Windows 95, Windows 98, Windows NT, và Windows 2000 truy xuất nhiều dịch vụ mạng trực tiếp, bao gồm Active Directory. Nó được cung cấp như một công cụ phát triển phần mềm (Software Development Kit - SDK). |
| **Asynchronous Transfer Mode (ATM)** | ATM là giao thức hướng nối kết và tốc độ cao, được thiết kế để truyền nhiều loại dữ liệu trên mạng. Nó thích hợp cho cả các mạng cục bộ (LAN) và các mạng diện rộng (WAN). Dùng ATM, có thể đồng thời truyền nhiều loại dữ liệu như: âm thanh, dữ liệu, hình ảnh, và video qua mạng. |
| **Certificate Services** | Sử dụng Certificate Services và các công cụ quản lý chứng nhận trong Windows 2000, bạn có thể triển khai các khoá công cộng của mình. Với khoá công cộng, bạn có thể hiện thực các kỹ thuật cơ bản chuẩn như khả năng đăng nhập thẻ thông minh, sự thẩm định quyền khách hàng (thông qua Secure Sockets Layer và Transport Layer Security), bảo mật thư điện tử, chữ ký điện tử và bảo mật kết nối (sử dụng Internet Protocol Security). |
| **Component Services** | Component Services là một tập hợp các dịch vụ cơ bản trên phần mở rộng của Component Object Model (COM) và trên Microsoft Transaction Server. Component Services cung cấp sự cải thiện luồng và bảo mật, quản lý giao dịch, đối tượng dùng chung, hàng đợi hợp thành, quản trị ứng dụng và đóng gói. |
| **Hỗ trợ hạn ngạch đĩa** | Bạn có thể dùng các hạn ngạch đĩa khi định dạng dung tích đĩa với hệ thống file NTFS, để giám sát và giới hạn khối lượng của không gian đĩa cho từng người dùng. Bạn có thể định nghĩa những đáp ứng khi người dùng sử dụng vượt qúa ngưỡng cho phép của họ. |

| Các đặc điểm | Mô tả |
|---|---|
| **Dynamic Host Configuration Protocol (DHCP) with Domain Name System (DNS) and Active Directory** | DHCP làm việc với DNS và Active Directory trên các mạng Internet Protocol (IP), giải phóng bạn khỏi việc gán và kiểm tra địa chỉ tĩnh. DHCP gán địa chỉ IP tự động đến các máy tính hoặc các nguồn tài nguyên khác kết nối tới mạng IP. |
| **Encrypting File System (EFS)** | EFS trong Windows 2000 bổ sung điều khiển truy xuất hiện có và thêm vào mức mới bảo vệ dữ liệu của bạn. Hệ thống mã hoá file thực thi như dịch vụ hệ thống tích hợp, làm nó dễ quản lý, khó bị thâm nhập và trong suốt với người sử dụng. |
| **Graphical Disk Management** | Disk Management là các công cụ đồ hoạ để quản lý đĩa cứng bao gồm nhiều đặc trưng mới, như hỗ trợ khối lượng động, quản lý đĩa trực tuyến, quản lý đĩa cục bộ và từ xa, Volume Mount Points. |
| **Group Policy (Một phần của Active Directory)** | Các chính sách có thể định nghĩa các hành động được phép và những cài đặt cho người sử dụng và máy tính. Trái với chính sách cục bộ, bạn có thể dùng chính sách nhóm để thiết lập các chính sách áp dụng cho các vị trí, miền hay tập tổ chức đã cho trong Active Directory. Quản lý dựa trên chính sách đơn giản hoá các thao tác nâng cấp hệ điều hành, cài đặt ứng dụng, hồ sơ người dùng, và khoá hệ thống màn hình. |
| **Indexing Service** | Chỉ mục dịch vụ cung cấp cách nhanh, dễ và bảo mật để người dùng tìm thông tin cục bộ hay trên mạng. Người dùng có thể dùng các câu truy vấn mạnh để tìm file trong các định dạng và ngôn ngữ khác nhau, qua lệnh Search của trình đơn Start hoặc qua các trang Hypertext Markup Language (HTML) mà chúng ta thấy trong các trình duyệt web. |
| **IntelliMirror** | IntelliMirror cung cấp các mức cao của việc điều khiển các hệ thống khách chạy trên hệ điều hành Windows 2000 Professional. Bạn có thể dùng IntelliMirror để định nghĩa các chính sách cơ bản tương ứng với công việc của người dùng, các thành viên nhóm và vị trí. Sử dụng các chính sách này nền màn hình Windows 2000 Professional được cấu hình tự động để làm quen với các yêu cầu của người dùng riêng biệt mỗi lần người dùng đăng nhập vào mạng, bất kể là người dùng đăng nhập từ đâu. |
| **Internet Authentication Service (IAS)** | IAS cung cấp một điểm tập trung để quản lý thẩm định quyền, quyền hạn, tài khoản và kiểm tra người dùng dial-up hoặc Virtual Private Network. IAS dùng giao thức Internet Engineering Task Force (IETF) gọi là Remote Authentication Dial-In User Service (RADIUS). |

| Các đặc điểm | Mô tả |
|---|---|
| **Internet Connection Sharing** | Với đặc điểm chia sẻ nối kết Internet của Network and Dial-Up Connections, bạn có thể sử dụng Windows 2000 để kết nối mạng gia đình của mình hoặc mạng văn phòng nhỏ tới Internet. Thí dụ, bạn phải có mạng gia đình để kết nối tới Internet bằng cách sử dụng kết nối dial-up. Bằng cách cho phép máy tính kết nối chia sẻ với Internet qua kết nối dial-up, bạn đang cung cấp cách thông dịch địa chỉ mạng, địa chỉ hoá, và các dịch vụ phân giải tên đối với tất cả các máy tính trên mạng của mình. |
| **Internet Information Services (IIS) 5.0** | Các đặc điểm mạnh trong Internet Information Services (IIS), như một phần của Microsoft Windows 2000 Server, làm nó dễ chia sẻ tài liệu và thông tin qua mạng intranet hoặc Internet. Dùng IIS, bạn có thể triển khai một cách linh hoạt và tin cậy các ứng dụng Web-based, và bạn có thể chuyển các dữ liệu và ứng dụng đang tồn tại tới Web. IIS bao gồm Active Server Pages và các đặc trưng khác. |
| **Hỗ trợ Internet Security (IPSec)** | Dùng IPSec để bảo mật giao tiếp bên trong mạng intranet và khởi tạo các giải pháp bảo mật Virtual Private Network trên Internet. IPSec được thiết kế bởi IETF và là chuẩn công nghiệp để mã hoá Transmission Control Protocol/Internet Protocol (TCP/IP). |
| **Hỗ trợ Kerberos V5 Protocol** | Kerberos V5 là giao thức thẩm định quyền mạng công nghiệp chuẩn. Với hỗ trợ Kerberos V5 việc sử lý đăng nhập nhanh và đơn giản cho người dùng truy xuất các nguồn tài nguyên của mạng, như các môi trường khác để hỗ trợ giao thức này. Sự hỗ trợ đối với Kerberos V5 bao gồm việc thêm các lợi ích như là thẩm định quyền lẫn nhau và uỷ nhiệm quyền thẩm định. |
| **Hỗ trợ Layer 2 Tunnelling Protocol (L2TP)** | L2TP là phiên bản bảo mật hơn Point-to-Point Tunnelling Protocol (PPTP) và được dùng để đường ống hoá, chỉ định địa chỉ và thẩm định quyền. |
| **Hỗ trợ Lightweight Directory Access Protocol (LDAP)** | LDAP là giao thức truy xuất chính Active Directory và là một chuẩn công nghiệp. Phiên bản LDAP 3 được thiết kế bởi IETF. |
| **Message queuing** | Tích hợp chức năng hàng đợi tin nhắn trong Windows 2000 giúp những người phát triển xây dựng và phát triển các ứng dụng làm nó chạy tin cậy hơn trên môi trường mạng. Các ứng dụng này có thể điều khiển các ứng dụng chạy trên các nền khác nhau như các hệ thống máy tính lớn và các hệ thống trên cơ sở UNIX. |
| **Microsoft Management Console (MMC)** | Dùng MMC để sắp xếp các công cụ quản lý và các quá trình bạn cần bên trong giao diện đơn. Bạn cũng có thể uỷ nhiệm các thao tác tới người dùng cụ thể bằng cách khởi tạo các màn hình điều khiển MMC cấu hình trước cho chúng. Màn hình điều khiển sẽ cung cấp các công cụ mà bạn lựa chọn cho người dùng. |

| Các đặc điểm | Mô tả |
|---|---|
| **Network Address Translation (NAT)** | NAT ẩn bên trong địa chỉ IP từ các mạng bên ngoài bằng cách truyền địa chỉ trong riêng tới địa chỉ ngoài chung. Điều này giảm thiểu chi phí việc đăng ký địa chỉ IP bằng cách cho phép bạn dùng địa chỉ IP bên trong chưa đăng ký, với việc truyền một số nhỏ của địa chỉ IP bên ngoài đã đăng ký. Nó cũng che dấu cấu trúc mạng bên trong, giảm sự rủi ro do những việc tấn công các hệ thống bên trong. |
| **Operating system migration, support, and integration** | Windows 2000 hợp nhất liền một khối với các hệ thống đang tồn tại và bao gồm sự hỗ trợ đối với các hệ điều hành Windows trước đây, như những đặc trưng mới để hỗ trợ các hệ điều hành chung khác. Windows 2000 cung cấp: thao tác giữa các phần với Windows NT Server 3.51 và 4.0; hỗ trợ cho các máy khách đang chạy nhiều loại hệ điều hành như Windows 3.x, Windows 95, Windows 98, và Windows NT Workstation 4.0; Máy tính lớn với khoảng cách kết nối trung bình, sử dụng các cổng giao dịch và hàng đợi S/390 và AS/400 qua Systems Network Architecture (SNA) Server; File Server cho máy Macintosh, cho phép máy khách Macintosh sử dụng giao thức TCP/IP (AppleTalk File Protocol (AFP) qua IP) để chia sẻ các file và truy cập chia sẻ trên máy chủ Windows 2000. |
| **Plug and Play** | Với Plug and Play, tổ hợp hỗ trợ của phần cứng và phần mềm, máy chủ có thể nhận biết và thích ứng với cấu hình phần cứng tự động thay đổi, không cần sự can thiệp và khởi động lại. |
| **Public key infrastructure (PKI) and smart card infrastructure** | Dùng Certificate Services và các công cụ quản lý chứng chỉ trong Windows 2000, bạn có thể triển khai cơ sở hạ tầng khoá công cộng. Với cơ sở hạ tầng khoá công cộng, bạn có thể hiện thực kỹ thuật cơ bản chuẩn như các khả năng đăng nhập thẻ thông minh, sự thẩm định quyền máy khách (qua Secure Sockets Layer và Transport Layer Security), bảo mật e-mail, chữ ký điện tử, và bảo mật kết nối (dùng Internet Protocol Security). Dùng Certificate Services, bạn có thể cài đặt và quản lý các chứng nhận quyền truy xuất mà nó cấp và thu hồi các chứng chỉ X.509V3. Cách thức này cho phép bạn không phụ thuộc vào các dịch vụ thẩm định quyền máy khách thương mại, mặc dù bạn có thể tích hợp việc thẩm định quyền máy khách thương mại bên trong cơ sở hạ tầng khoá công cộng của bạn nếu bạn chọn. |
| **Quality of Service (QoS)** | Dùng QoS, bạn có thể điều khiển các ứng dụng đã được phân phối trên băng thông mạng. Bạn có thể cho các ứng dụng quan trọng nhiều băng thông hơn, và các ứng dụng ít quan trọng ít băng thông hơn. Các dịch vụ tựa QoS và các giao thức cung cấp hệ thống phân phối thông tin trên mạng nhanh, bảo đảm, end-to-end. |

| Các đặc điểm | Mô tả |
|---|---|
| **Remote Installation Services (RIS)** | Với Remote Installation Services, bạn có thể cài đặt Windows 2000 Professional từ xa, mà không cần cài đặt trực tiếp trên mỗi máy khách. Các máy đích phải hoặc là hỗ trợ khởi động từ xa với Pre-Boot eXecution Environment (PXE) ROM, hoặc là phải được khởi động từ xa bằng đĩa mềm. Việc cài đặt cho nhiều máy khách trở nên đơn giản hơn nhiều. |
| **Removable Storage and Remote Storage** | Removable Storage làm nó dễ kiểm tra phương tiện lưu trữ có thể tháo dời và quản lý các thư viện phần cứng, như là các hộp ổ cứng nắp ngoài. Ổ cứng điều khiển từ xa dùng tiêu chuẩn mà bạn chỉ định để tự động việc sao chép các file ít sử dụng để di chuyển thiết bị truyền thông. Nếu không gian đĩa cứng bị giảm dưới mức xác định, Remote Storage xoá nội dung file chứa trên đĩa. Nếu file được dùng sau này thì nội dung của nó sẽ được tự động lấy lại từ nơi lưu trữ. Vì giá thành tính trên 1 MB của đĩa quang học và băng từ nhỏ hơn của ổ cứng, nên nó có thể giảm giá thành mạng của bạn. |
| **Routing and Remote Access service** | Routing and Remote Access service là dịch vụ tích hợp đơn mà các thiết bị đầu cuối kết nối từ các máy khách hoặc bằng dial-up hoặc bằng Virtual Private Network (VPN), hoặc thực hiện tìm đường (IP, IPX, and AppleTalk) hoặc cả hai. Với việc tìm đường và truy xuất từ xa, Windows 2000 server của bạn có thể hoạt động như dịch vụ truy xuất từ xa, máy chủ VPN , cổng vào hoặc tìm đường. |
| **Safe mode startup** | Với chế độ an toàn, bạn có thể khởi động Windows 2000 với tập tối thiểu các trình điều khiển và các dịch vụ, và do đó bạn sẽ thấy chuỗi các sự kiện lúc khởi động. Sử dụng chế độ an toàn, bạn có thể chuẩn đoán các vấn đề của các trình điều khiển và các thành phần khác mà bị ngăn cản bởi khởi động chuẩn. |
| **Cơ sở hạ tầng thẻ thông minh** | Dùng Certificate Services và các công cụ quản lý chứng chỉ trong Windows 2000, bạn có thể phát triển cơ sở hạ tầng khoá công cộng của bạn. Với chúng bạn có thể hiện thực các kỹ thuật chuẩn cơ sở như thẻ đăng nhập thông minh, thẩm định quyền máy khách (qua Secure Sockets Layer và Transport Layer Security), bảo mật thư điện tử, chữ ký điện tử, và bảo mật nối kết (dùng Internet Protocol Security). |
| **TAPI 3.0** | TAPI 3.0 hợp nhất IP và hệ thống điện thoại truyền thống để cho phép những nhà phát triển máy tính tạo thế hệ mới các ứng dụng hệ thống điện thoại máy tính để làm việc bằng Internet hay intranet trên hệ thống mạng điện thoại truyền thống. |

| Các đặc điểm | Mô tả |
|---|---|
| **Terminal Services** | Gia đình Windows 2000 Server chỉ cho phép những hệ điều hành máy chủ tích hợp các dịch vụ giả lặp đầu cuối. Dùng Terminal Services, người dùng có thể truy xuất các chương trình đang chạy trên các máy trạm từ nhiều thiết bị cũ hơn. Thí dụ, người dùng có thể truy xuất màn hình nền Windows 2000 Professional ảo và các ứng dụng trên nền Windows 32-bit từ phần cứng mà không thể chạy phần mềm cục bộ. Terminal Services cung cấp khả năng này cho cả các thiết bị của máy khách chạy hệ điều hành Windows và các hệ điều hành khác |
| **Mạng riêng ảo (Virtual Private Network - VPN)** | Bạn có thể cho phép người dùng sẵn sàng truy cập mạng ngay cả khi họ ở ngoài văn phòng và giảm giá truy xuất, bằng cách hiện thực VPN. Dùng VPN, người dùng có thể kết nối dễ dàng và bảo mật tới mạng công ty. Sự kết nối thông qua Internet Service Provider (ISP) cục bộ làm giảm thời gian kết nối. Với Windows 2000 Server, bạn có thể dùng các giao thức bảo mật hơn để tạo Virtual Private Networks, bao gồm: L2TP - một phiên bản bảo mật hơn của PPTP và IPSec - một giao thức cơ sở chuẩn để cung cấp các mức cao nhất việc bảo mật VPN. Dùng IPSec, mọi thứ trên lớp mạng có thể được mã hoá. |
| **Windows Media Services** | Dùng Windows Media Services, bạn có thể truyền đa phương tiện chất lượng cao cho người dùng Internet và intranet. |
| **Windows Script Host (WSH)** | Dùng WSH, bạn có thể tự động hoá các hành động như tạo nối tắt, kết nối và bỏ kết nối với máy chủ mạng. WSH phụ thuộc ngôn ngữ. Bạn có thể viết các kịch bản dưới những ngôn ngữ kịch bản thông thường như VBScript và JScript. |

## 6.3 Mô hình workgroup và mô hình domain trong Windows 2000

Sau khi kết nối máy tính của mình tới mạng, bạn có thể chia sẻ các file, các máy in, và thư điện tử với các máy tính khác. Có một vài khái niệm cơ bản cần biết để thiết kế cấu trúc file và cài đặt hệ thống của bạn.

**Workgroup hay Domain**

Khi cài đặt Windows 2000 Professional hoặc Server trong môi trường mạng, chúng có thể được cài đặt hoặc là **workgroup** hoặc là **domain.**

### a) Windows 2000 Workgroup

Windows 2000 *workgroup* là một nhóm máy tính mạng cùng chia sẻ tài nguyên như file dữ liệu, máy in. Nó là một nhóm lôgíc của các máy tính mà tất cả chúng có cùng tên nhóm. Có thể có nhiều nhóm làm việc (workgroups) khác nhau cùng kết nối trên một mạng cục bộ (LAN).

Workgroups cũng được coi là mạng peer-to-peer bởi vì tất cả các máy trong workgroup có quyền chia sẻ tài nguyên như nhau mà không cần sự chỉ định của Server. Mỗi máy tính trong nhóm tự bảo trì, bảo mật cơ sở dữ liệu cục bộ của nó. Điều này có nghĩa là, tất cả sự quản trị về tài khoản người dùng, bảo mật cho nguồn tài nguyên chia sẻ không được tập trung hoá. Bạn có thể kết nối tới một nhóm đã tồn tại hoặc khởi tạo một nhóm mới.

❖ *Ưu điểm của Windows 2000 Workgroup:*

- Workgroups không yêu cầu máy tính chạy trên hệ điều hành Windows 2000 Server để tập trung hoá thông tin bảo mật.
- Workgroups thiết kế và hiện thực đơn giản và không yêu cầu lập kế hoạch có phạm vi rộng và quản trị như domain yêu cầu.
- Workgroups thuận tiện đối với nhóm có số máy tính ít và gần nhau (<=10 máy).

❖ *Nhược điểm của Windows 2000 workgroup:*

- Mỗi người dùng phải có một tài khoản người dùng trên mỗi máy tính mà họ muốn đăng nhập.
- Bất kỳ sự thay đổi tài khoản người dùng, như là thay đổi password hoặc thêm tài khoản người dùng mới, phải được làm trên tất cả các máy tính trong workgroup. Nếu bạn quên bổ sung tài khoản người dùng mới tới một máy tính trong nhóm thì người dùng mới sẽ không thể đăng nhập vào máy tính đó và không thể truy xuất tới tài nguyên của máy tính đó.
- Việc chia xẻ thiết bị và file được xử lý bởi các máy tính riêng, và chỉ cho người dùng có tài khoản trên máy tính đó được được sử dụng.

### b) Windows 2000 Domain

Windows 2000 *domain* là một nhóm máy tính mạng cùng chia sẻ *cơ sở dữ liệu thư mục tập trung* (**central directory database**)**.** Thư mục dữ liệu chứa tài khoản người dùng và thông tin bảo mật cho toàn bộ Domain. Thư mục dữ liệu này được biết như là thư mục hiện hành (**Active Directory**).

Trong một Domain, thư mục chỉ tồn tại trên các máy tính được cấu hình như *máy điều khiển miền* (**domain controller**)**.** Một **domain controller là** một Server quản lý tất cả các khía cạnh bảo mật của Domain. Không giống như Windows 2000 workgroup, bảo mật và quản trị trong domain được tập trung hoá. Chỉ những máy tính đang chạy Windows 2000 Server mới có thể được thiết kế là các Domain controller.

Một domain không được xem như một vị trí đơn hoặc cấu hình mạng riêng biệt. Các máy tính trong cùng domain có thể ở trên một mạng LAN nhỏ hoặc có thể được đặt trong các nước khác nhau trên thế giới. Chúng có thể giao tiếp với nhau qua bất kỳ kết nối vật lý nào, như: dial-up, Integrated Services Digital Network (ISDN), fibre, Ethernet, Token Ring, Frame Relay, satellite, or leased lines.

❖ *Ưu điểm của Windows 2000 Domain:*

- Cho phép quản trị tập trung. Nếu người dùng thay đổi password của họ, thì sự thay sẽ được cập nhật tự động trên toàn Domain.
- Domain cung cấp quy trình đăng nhập đơn giản để người dùng truy xuất các tài nguyên mạng mà họ được phép truy cập.
- Domain cung cấp linh động để người quản trị có thể khởi tạo mạng rất rộng lớn.

Các miền Windows 2000 điển hình có thể chứa các kiểu máy tính sau :

| Kiểu máy tính | Mô tả |
|---|---|
| **Máy điều khiển miền (Domain controllers) – Windows 2000 Server** | Mỗi Domain controller cất trữ và bảo trì bản sao thư mục. Trong domain, tài khoản người dùng được tạo một lần, Windows 2000 ghi nó trong thư mục này. Khi người dùng đăng nhập tới máy tính trong domain, domain controller kiểm tra thư mục nhờ tên người sử dụng, mật khẩu và giới hạn đăng nhập. Khi có nhiều domain controllers, chúng định kỳ tái tạo thông tin thư mục của chúng. |
| **Các máy chủ thành viên (Member servers) – Windows 2000 Server** | Một *member server* là bất kỳ máy chủ nào mà không được cấu hình như là domain controller. Máy chủ không cất thông tin thư mục và không thể xác nhận domain người dùng. Các máy chủ cung cấp các tài nguyên chia sẻ như các thư mục dùng chung hay các máy in. |
| **Các máy tính trạm (Client computers) – Windows 2000 Professional** | Các máy tính trạm chạy một môi trường màn hình nền của người dùng và cho phép người dùng truy cập tới nguồn tài nguyên trong domain. |

Không giống như Workgroup, Domain phải tồn tại trước khi bạn tham gia vào nó. Việc tham gia vào Domain luôn yêu cầu người quản trị Domain cấp tài khoản cho máy tính của bạn tới domain đó. Tuy nhiên, nếu người quản trị cho bạn đúng đặc quyền, bạn có thể khởi tạo tài khoản máy tính của bạn trong quá trình cài đặt.

# Câu hỏi ôn tập chương 6

1. Chọn đúng **ba** hệ điều hành mạng theo liệt kê sau:
   a. DOS b. Win 2000 c. Win 9x
   d. Linux e. Novel NetWare
2. WINS được cấu hình ở đâu trong trạm làm việc khách? (chọn 1)
   a. Trong đặc tính của bộ điều hợp mạng.
   b. Trong sự thiết lập của modem.
   c. Trong các đặc tính của TCP/IP .
   d. Trong sự thiết lập máy khách của Microsoft.
3. Chọn lựa nào phù hợp nhất để dùng WINS?
   a. Windows 3.11 workstation
   b. Linux server
   c. Novel Server
   d. Windows 2000 workstation
4. WINS thuộc về tầng nào trong mô hình OSI?
   a. Application
   b. Presentation
   c. Session
   d. Transport
5. Windows 2000 Server được phát triển từ …….
   a. Windows NT 4.0 Enterprise Edition
   b. Windows NT 4.0 Server
   c. Windows NT 5.0 Server
   d. None of the others
6. Hệ điều hành nào trong các hệ điều điều hành sau được thiết kế để hỗ trợ nhiều bộ nhớ và CPU hơn trên một máy tính?
   a. Windows 2000 Professional
   b. Windows 2000 Server
   c. Windows 2000 Advanced Server
   d. Windows 2000 Data Center Server
7. Member server là Domain Controller?
   a. Đúng. b. Sai.
8. Ưu điểm của Windows 2000 Domain là không phải quản trị tập trung?
   a. Đúng. b. Sai.
9. Workgroups cũng được coi là mạng peer-to-peer ?
   a. Đúng. b. Sai.

# CHƯƠNG 7 – CÀI ĐẶT WINDOWS 2000 SEVER

## MỤC TIÊU CỦA CHƯƠNG

*Kết thúc chương này bạn có thể:*

- Nắm được lý thuyết chung của việc cài đặt Windows 2000 Server
- Nắm được yêu cầu phần cứng tối thiểu cho việc cài đặt Windows 2000 Server
- Nắm được các bước của quá trình cài đặt

## 7.1 Cài đặt Windows 2000 Server

### 7.1.1 Chuẩn bị cho việc cài đặt

Giống như cách cài đặt các phiên bản khác của Windows, Windows 2000 Server cũng hướng dẫn từng bước cho chúng ta cài đặt. Tuy nhiên trước khi cài đặt, cần phải xem xét trước một vài điểm về hệ thống, thể hiện trong bảng sau:

| **Hãy xem xét các điểm sau …** |
|---|
| Yêu cầu ổ cứng tối thiểu còn chưa sử dụng là: 2GB (Gigabytes). |
| Kiểm tra các phần cứng trong máy (network adapters, video drivers, sound cards, CD-ROM drives, PC cards v.v...) có tồn tại trong **Windows 2000 Hardware Compatibility List (HCL).** |
| Xác định phần ổ đĩa bạn sẽ cài Windows 2000 Server. |
| Chọn hệ thống file phù hợp với yêu cầu của bạn – **NTFS** hoặc **FAT16/FAT32.** Bạn nên chọn NTFS trừ khi bạn cần chạy nhiều hơn một hệ điều hành trên máy tính của bạn, hoặc máy tính của bạn cần sử dụng một vài phần mềm cũ (Xem xét nâng cấp phần mềm cũ sử dụng NTFS). |
| Lựa chọn kiểu per-seat hay per- server. Bạn có thể chuyển từ per-seat sang per-server, nhưng chiều ngược lại thi không được. |
| Chọn loại mạng bạn sẽ kết nối – Workgroup hay Domain. Nếu bạn đang kết nối domain, bạn cần thêm thông tin như là tên domain và tên tài khoản máy tính đã khởi tạo cho bạn. Với tài khoản quản trị và mật khẩu trong domain, bạn có thể khởi tạo tài khoản máy tính trong domain. |
| Chọn cài đặt mới hoặc nâng cấp từ Windows NT Server. Windows NT Workstation and Windows 9*x* không thể nâng cấp thành Windows 2000 Server. |
| Chọn phương pháp cài đặt: từ đĩa khởi động, CD-ROM hay mạng. |
| Chọn các thành phần bạn cần cài đặt, như Networking Services hay Microsoft Networking Service. |

### 7.1.2 Yêu cầu phần cứng tối thiểu

Máy tính của bạn phải phù hợp với yêu cầu phần cứng tối thiểu, trước khi bạn cài đặt Windows 2000 Server. Các yêu cầu được liệt kê theo bảng sau:

| Thành phần | Yêu cầu tối thiểu |
|---|---|
| Processor | 32-bit Pentium 133 MHz. |
| Không gian đĩa cứng còn trống | Ổ cứng tối thiểu còn trống là 671 MB (Đề nghị là 2 GB). |
| Bộ nhớ RAM | 64 MB đối với mạng có ít hơn 5 máy; 128 MB là yêu cầu tối thiểu với hầu hết các môi trường mạng. |
| Màn hình | Khả năng của màn hình VGA là 640 x 480 (đề nghị 1024 x 768). |
| Ổ đĩa CD-ROM | 12X hoặc đề nghị nhanh hơn; không yêu cầu khi cài đặt qua mạng. |
| Các ổ đĩa bổ sung | Đĩa mềm mật độ cao 3.5-inch, ngoại trừ máy bạn có thể khởi động từ CD-ROM. |
| Các thành phần tuỳ chọn | Chuột hay thiết bị trỏ khác. Đối với việc cài đặt qua mạng: một card mạng và hệ điều hành mạng dựa trên MS-DOS cho phép kết nối tới server chứa các file cài đặt Windows 2000. |

### 7.1.3 Các chương trình cài đặt Windows 2000 Server

Windows 2000 Server được cài đặt bằng cách sử dụng, hoặc là chương trình Winnt.exe hoặc Winnt32.exe, việc dùng chương trình cài đặt nào phụ thuộc vào hệ điều hành hiện tại đang sử dụng trên máy tính của bạn. Bạn cũng có thể sử dụng chương trình Setup.exe, nhưng thực sự nó thực hiện việc cài đặt trên Winnt.exe hoặc Winnt32.exe. Để cài đặt Windows 2000 Server trên máy tính đang chạy hệ điều hành MS-DOS hoặc Windows 3.x, bạn cần chạy file Winnt.exe từ thông số dòng lệnh của MS-DOS. Để cài trên các máy đang chạy hệ điều hành: Windows 95, Windows 98, Windows NT Workstation, Windows NT Server 3.51 hoặc Windows NT Server 4.0, bạn cho chạy file Winnt32.exe.

Windows 2000 Setup Program

Khi bạn thực thi chương trình Setup.exe, màn hình máy tính cho phép bạn cài đặt Windows 2000 Server, cài đặt các thành phần, các tùy chọn của đĩa CD, hoặc thoát khỏi chương trình cài đặt.

Nếu hệ thống của bạn cho phép chạy Autorun, Autorun gọi Setup.exe, chương trình này sẽ kiểm tra hệ thống của bạn. Nếu Setup xác định rằng máy tính của bạn đang chạy Windows NT Server 3.51, Windows NT Server 4.0, hoặc phiên bản trước Windows 2000 Server. Bạn cho phép máy hoặc nâng cấp hoặc cài đặt mới Windows 2000 Server. Nếu phiên bản trên hệ điều hành mới hơn Windows 2000 Server, Setup.exe sẽ không cho phép bạn cài đặt tiếp tục.

Winnt.exe Setup Program

Winnt.exe được sử dụng khi cài đặt từ máy đang chạy hệ điều hành MS-DOS hoặc Windows 3.x. Nó thường được sử dụng để cài đặt qua mạng cho máy trạm mạng MS-DOS. Winnt.exe thực hiện các bước sau:

- Khởi tạo thư mục tạm $WIN_NT$.~BT trên ổ đĩa và sao chép file khởi động cài đặt trên thư mục này.
- Khởi tạo thư mục tạm $WIN_NT$.~LS và sao chép các file Windows 2000 từ server vào thư mục này.
- Các dấu nhắc được sử dụng để khởi động lại hệ thống, trình đơn khởi động xuất hiện và quá trình cài đặt tiếp tục.

Winnt.exe cài đặt Windows 2000 Server và có thể được thực thi từ MS-DOS hoặc hệ điều hành Windows 16 bit từ thông số dòng lệnh. Có một số lựa chọn để thực thi chương trình Winnt.exe:

| Tuỳ chọn | Mô tả |
|---|---|
| /s[:*sourcepath*] | Định rõ vị trí nguồn của các file Windows 2000. Vị trí phải là đường dẫn đầy đủ. |
| /t[:*tempdrive*] | Chỉ thị việc cài đặt từ file tạm trên ổ đĩa định rõ và cài đặt Windows 2000 trên ổ đĩa đó. Nếu bạn không định rõ vị trí, việc cài đặt sẽ cố gắng thử định vị tới ổ cứng mặc định. |
| /u[:*answer file*] | Thực hiện cài đặt không giám sát. Việc trả lời file cung cấp trả lời tới một vài hoặc tất cả của lời nhắc trong suốt quá trình cài đặt. |
| /udf:id[,*UDF_file*] | Cho biết chỉ số nhận dạng mà quá trình cài đặt sử dụng để chỉ định làm thế nào sửa đổi Uniqueness Database File (UDF). Quá trình cài đặt nhắc bạn đưa đĩa chứa file $Unique$.udb. |
| /r[:*folder*] | Định rõ thư mục được cài đặt. Thư mục đó vẫn còn lại sau khi cài đặt xong. |
| /rx[:*folder*] | Định rõ thư mục lựa chọn để sao chép. Thư mục này bị xoá sau khi cài đặt xong. |
| /e | Định rõ lệnh thực thi tại lúc kết thúc cài đặt chế độ GUI. |
| /a | Cho phép lựa chọn khả năng truy xuất. |

Winnt32.exe Setup Program

Nếu máy tính của bạn sẽ cài Windows 2000 Server khi đang chạy các hệ điều hành: Windows 95, Windows 98, Windows NT Workstation, Windows NT Server 3.51 hoặc Windows NT Server 4.0, thì chương trình cài đặt Winnt32.exe sẽ được sử dụng để cài đặt. Bạn cũng có thể chạy Winnt32.exe từ thư mục gốc (chẳng hạn như \i386) trên đĩa

CD-ROM; hoặc thực thi Winnt32.exe từ thông số dòng lệnh từ Start Menu\run, khi hệ điều hành máy bạn đang chạy là Windows 95, Windows 98, hoặc Windows NT.

Nếu việc cài đặt Windows 2000 Server được cài đặt trên mạng, Winnt32.exe khởi tạo thư mục tạm $WIN_NT$.~LS và sao chép các file Windows 2000 Server từ server vào thư mục này. Thư mục tạm này được khởi tạo trên ổ đĩa đầu tiên mà nó đủ lớn, trừ khi bạn chọn /t. Việc này được gọi là *giai đoạn tiền sao chép* (Pre-Copy Phase) .

Các chọn lựa có thể được sử dụng với lệnh Winnt32.exe là:

| Tuỳ chọn | Mô tả |
|---|---|
| /s:*sourcepath* | Định rõ vị trí file nguồn Windows 2000. Để đồng thời sao chép file từ nhiều Server. Nếu bạn dùng nhiều /s, server đầu tiên phải sẵn sàng hoặc cài đặt sẽ thất bại. |
| /tempdrive:*drive_letter* | Điều khiển Setup đặt các file tạm trên phân hoạch xác định và cài đặt Windows 2000 trên ổ đó. |
| /Unattend or /u | Nâng cấp từ phiên bản trước của Windows 2000 trong chế độ cài đặt tự động. Tất cả các người dùng được lấy từ lần cài đặt trước, vì thế không có người dùng nào được thêm vào.<br>Dùng /unattend để tự động cài đặt xác nhận rằng bạn đang đọc và chấp nhận End-User License Agreement (EULA) cho Windows 2000. Trước khi dùng lựa chọn này để cài Windows 2000 với danh nghĩa là tổ chức khác hơn là bạn làm chủ, bạn phải xác nhận rằng người dùng cuối đã nhận, đọc và chấp nhận điều khoản của Windows 2000 EULA. OEMs có thể không định rõ khoá này trên máy nhượng lại từ những người dùng cuối. |
| /unattend[*num*][:*answer_file*] | Thực hiện làm tươi quá trình cài đặt trong chế độ cài đặt tự động. File trả lời cung cấp việc cài đặt với những mô tả tuỳ ý của bạn.. *Num* là số cộng thêm giữa thời gian cài đặt xong sao chép các file khi khởi động lại máy tính của bạn. Bạn có thể dùng số này trên bất kỳ máy tính đang chạy Windows NT hay Windows 2000. Trình lưu giữ *answer_file* là tên của file trả lời. |

| Tuỳ chọn | Mô tả |
|---|---|
| /copydir:*folder_name* | Khởi tạo và thêm danh mục bên trong danh mục mà các file Windows 2000 được cài đặt. Thí dụ, nếu danh mục nguồn chứa danh mục gọi là Private_drivers sửa đổi chỉ với vị trí (site) của bạn, bạn có thể gõ **/copydir:Private_drivers** để thực hiện việc sao chép danh mục tới danh mục Windows 2000 đã cài đặt của bạn. Do vậy vị trí danh mục mới sẽ là %systemroot%\Private_drivers. Bạn có thể dùng /copydir để tạo các thư mục bổ sung nếu bạn muốn. |
| /copysource:*folder_name* | Khởi tạo các thư mục tạm bên trong thư mục mà các file Windows 2000 được cài đặt. Thí dụ, nếu thư mục nguồn chứa thư mục gọi là Private_drivers sửa đổi chỉ với vị trí (site) của bạn, bạn có thể gõ **/copysource:Private_drivers** để thực hiện việc sao chép thư mục tới thư mục Windows 2000 đã cài đặt của bạn và sử dụng các file của nó trong suốt quá trình cài đặt. Do vậy vị trí thư mục mới sẽ là %systemroot%\Private_drivers. Khác với các thư mục được tạo bằng /copydir, các thư mục tạo bằng /copysource bị xoá sau khi quá trình cài đặt hoàn thành. |
| /cmd:*command_line* | Chỉ thị cài đặt tiến hành ra lệnh cụ thể trước giai đoạn kết thúc của quá trình cài đặt. Công việc này xuất hiện sau khi máy tính của bạn khởi động lại hai lần và sau khi cài đặt sưu tập thông tin cấu hình cần thiết, nhưng trước khi quá trình cài đặt hoàn thành. |
| /debug[*level*][:*filename*] | Tạo bản ghi gỡ rối mức danh nghĩa, thí dụ /debug4:C:\ Win2000.log. File mặc định là %systemroot%\Winnt32.log, với mức gỡ rối đặt là 2: Có các mức sau: 0-severe errors, 1-errors, 2-warnings, 3-information, và 4- chi tiết thông tin cho gỡ rối. Mỗi mức bao gồm các mức thấp hơn nó. |
| /udf:*id*[,*UDF_file*] | Biểu thị định danh mà quá trình cài đặt dùng để chỉ rõ việc sửa đổi và sự giải đáp file Uniqueness Database File (UDF) (see the /unattend entry). UDF ghi đè giá trị trong file giải đáp và xác định giá trị trong UDF được dùng. Thí dụ, /udf:RAS_user, Our_company.udb ghi đè việc cài đặt đã xác định cho định danh RAS_user trong file Our_company.udb. Nếu không có một UDF được xác định, Setup nhắc nhở người dùng đưa đĩa chứa file $Unique$.udb. |

| Tuỳ chọn | Mô tả |
|---|---|
| /syspart:*drive_letter* | Chỉ rõ rằng bạn có thể sao chép các fie bắt đầu cài đặt từ ổ cứng, đánh dấu đĩa hoạt động, và sau đó cài đặt đĩa trên máy tính khác. Khi bạn bắt đầu với máy tính đó, nó tự động khởi động với giai đoạn kế tiếp của quá trình cài đặt. Bạn phải luôn luôn sử dụng thông số /tempdrive với thông số /syspart.<br>Chọn /syspart khi chạy Winnt32.exe chỉ từ máy tính đang chạy Windows NT 3.51, Windows NT 4.0, hoặc Windows 2000. Nó không thể chạy từ Windows 9*x*. |
| /checkupgradeonly | Kiểm tra máy tính của bạn để nâng cấp tương thích với Windows 2000. Đối với Windows 9x, việc cài đặt tạo một báo cáo với tên là Upgrade.txt trong thư mục cài đặt Windows. Với việc nâng cấp từ Windows NT 3.51 hay 4.0, nó cất file báo cáo là Winnt32.log trong thư mục cài đặt. |
| /cmdcons | Thêm tùy trọn Recovery Console để hệ điều hành lựa chọn màn hình, sửa chữa lỗi cài đặt. |
| /m:*folder_name* | Định rõ rằng quá trình cài đặt sao chép các file thay thế từ vị trí luân phiên. Chỉ dẫn việc cài đặt xem vị trí luân phiên đầu tiên, và nếu các file có mặt, sử dụng chúng thay vì phải dùng các file từ vị trí mặc định. |
| /makelocalsource | Chỉ thị việc cài đặt sao chép tất cả các file nguồn cài đặt tới ổ cứng cục bộ của bạn. Sử dụng /makelocalsource khi cài đặt từ CD để cung cấp các file cài đặt. |
| /noreboot | Chỉ thị việc cài đặt không khởi động lại máy tính sau giai đoạn sao chép file của Winnt32 được hoàn thành để mà bạn có thể thực thi một lệnh khác. |

### 7.1.4 Các giai đoạn của quá trình cài đặt.

Có ba giai đoạn trong quá trình cài đặt Windows 2000 Server là: *Pre-Copy Phase*, *Text mode*, và *GUI mode*.

**a. Giai đoạn trước khi sao chép (Pre-Copy)**

Giai đoạn tiền sao chép của quá trình cài đặt là khi tất cả các file cần để cài đặt được sao chép vào thư mục tạm trên ổ cứng cục bộ. Khi Winnt.exe hoặc Winnt32.exe được dùng để cài Windows 2000 Server trên mạng, các file cài đặt được sao chép vào thư mục tạm $WIN_NT$.~LS trên ổ cứng. Quá trình cài đặt tiếp tục như là nó được thực hiện trên ổ cứng cục bộ.

Bạn có thể chọn không tạo đĩa mềm khởi động bằng cách chọn hộp chọn *Copy All Setup Files From The Setup CD To The Hard Drive*. Khi bạn lựa chọn tùy chọn này, thư mục $WIN_NT$.~BT được khởi tạo trên ổ cứng cục bộ. Thư mục này chứa các file mà có thể chứa trong 4 đĩa mềm.

**b. Chế độ văn bản (Text Mode)**

Sau quá trình Pre-Copy là phần Text mode. Bạn sẽ được nhắc các thông tin cần thiết để hoàn tất quá trình cài đặt. Sau khi bạn chấp nhận bản quyền, bạn chỉ định hay khởi tạo ổ đĩa cài đặt. Tất cả các file yêu cầu để cài đặt được sao chép từ thư mục tạm (hoặc CD-ROM).

- *Thỏa thuận bản quyền Windows 2000 Server*

Sự thoả thuận bản quyền Windows 2000 Server được trình bày trên nhiều trang. Bạn có thể dùng phím Page Down để xem hết văn bản, và nhấn phím F8 khi đọc hết để chấp nhận bản quyền này.

- *Cài đặt trên hệ điều hành đã tồn tại (Existing Installations)*

Nếu quá trình cài đặt nhận ra là đã tồn tại Windows 2000, nó sẽ hiển thị một danh sách cho phép bạn chọn sự cài đặt ( nhấn R để sửa chữa, hoặc Esc để cài đặt tiếp tục).

- *Partitions*

Quá trình cài đặt hiển thị tất cả các ổ cứng hiện hữu và phần ổ chưa sử dụng. Dùng phím Up, Down bạn có thể lựa chọn ổ cứng bạn muốn cài Windows 2000 Server. Tại thời điểm này bạn có thể xoá hoặc khởi tạo ổ đĩa.

- *File Systems*

Quá trình cài đặt cho phép bạn chọn để giữ file hệ thống như cũ hoặc cho phép bạn chuyển đổi nó thành NTFS. Nếu bạn không muốn thay đổi nó, chọn Leave Current File System Intact (default), nhấn Enter để tiếp tục.

Quá trình cài đặt khảo sát ổ cứng của bạn và sao chép các file cần cài đặt từ thư mục tạm tới thư mục cài đặt (mặc định là \WINNT).

**c. Chế độ giao diện đồ họa (GUI Mode)**

Ngay khi chế độ văn bản của quá trình cài đặt hoàn tất, máy tính khởi động lại và bắt đầu chế độ giao diện đồ hoạ. Phần này của quá trình cài đặt cho phép bạn chọn các thành phần để cài đặt. Nó cũng nhắc nhập mật khẩu của quản trị viên.

Có ba giai đoạn tạo thành GUI Mode

1. Lấy lại thông tin về máy tính của bạn
2. Cài đặt mạng Windows 2000 Server
3. Hoàn thành quá trình cài đặt.

❖ *Lấy lại thông tin về máy tính của bạn*

Giai đoạn đầu tiên này của GUI Mode bao gồm nhiều hộp thoại mà Windows 2000 Server dùng để thu thập thông tin cấu hình để cài đặt hệ thống. Trong suốt giai đoạn này, các đặc trưng bảo mật Windows 2000, các thiết bị và cấu hình được cài đặt. Bạn sẽ được nhắc các thông tin sau:

| Nội dung | Mô tả |
|---|---|
| **Regional Settings** | Windows 2000 hiển thị xác lập miền hiện hành. Bạn có thể thêm sự hỗ trợ ngôn ngữ, thay đổi vị trí xác lập của bạn đối với hệ thống, và cấu hình thiết lập mặc định tài khoản người dùng cũng được. |
| **Personalize Your Software** | Khi cấu hình hệ thống, bạn phải nhập tên mà Windows 2000 Server đã ghi nhớ. Ngoài ra bạn có thể thêm vào tên của tổ chức. Mặc dù đó chỉ là tuỳ chọn. |
| **Licensing Mode** | Bạn phải chọn phương pháp cấp phép Per Server hay Per Seat. Nếu bạn chọn Per Server, bạn phải nhập số cấp phép của Per Server. |
| **Computer Name and Administrator Password** | Bạn phải nhập vào tên máy tính (tên NetBIOS tối đa 15 ký tự) khi cài Windows 2000. Tên tự động tổng quát sẽ là 15 ký tự. Tên bạn nhập vào phải khác tên các máy tính khác, tên nhóm, tên miền đã nhập trên mạng. Tên máy tính mặc định được hiển thị. Bạn cũng có thể nhập mật khẩu quản trị đối với tài khoản người dùng quản trị cục bộ. Mật khẩu này có thể tới 127 ký tự. |
| **Optional Component Manager** | Optional Component Manager cho phép bạn thêm hoặc bỏ các thành phần bổ sung trong và sau quá trình cài đặt. |
| **Date and Time Settings** | Trong suốt quá trình cài đặt, nếu cần bạn phải chọn múi giờ tương ứng và điều chỉnh ngày và giờ,. |

❖ *Cài đặt mạng Windows 2000 Server*

Ngay sau quá trình thu thập thông tin, Setup sẽ trở lại màn hình cài đặt và bắt đầu khảo sát máy tính để tìm các card mạng đã cài đặt.

***** Cài đặt hoạt động mạng (Networking Settings)

Quá trình cài đặt mạng bắt đầu bằng việc hỏi bạn chọn kiểu cài đặt (Typical Settings), kiểu mặc định hay kiểu tuỳ thích (**Custom Settings**). Kiểu cài đặt mặc định cấu hình hệ thống những mặc định: *Client for Microsoft Networks, File and Print Sharing for Microsoft Networks,* và *Internet Protocol (TCP/IP) cấu hình như DHCP client.*

Các loại cài đặt tuỳ thích cho phép cấu hình theo ba mục sau:

| Cài đặt | Mô tả |
|---|---|
| **Clients** | Mặc định khách là **Client For Microsoft Networks**. Bạn có thể thêm **Gateway (and Client) Services for NetWare**. |
| **Services** | Mặc định dịch vụ là **File and Printer Sharing for Microsoft Networks**. Bạn có thể thêm **SAP Agent** và **QoS Packet Scheduler**. Bạn có thể sửa đổi cài đặt đối với File và Printer Sharing cho mạng Microsoft bằng chọn lấy dịch vụ và chọn Properties.<br>Điều này cho phép bạn tối ưu việc cài đặt dịch vụ tương thích với mạng LAN. |
| **Protocols** | Giao thức mặc định là **Transport Control Protocol/Internet Protocol (TCP/IP).** Bạn có thể thêm các giao thức, **NWLink IPX/SPX**, **NetBEUI**, **DLC**, **AppleTalk**, **Network Monitor Driver**, và các giao thức khác. Bạn có thể cũng sửa đổi việc cài đặt giao thức bằng cách chọn Properties. |

❖ *Hoàn thành quá trình cài đặt*

Phần cuối cùng của chế độ GUI là giai đoạn hoàn thành quá trình cài đặt, nó không yêu cầu bất kỳ sự tương tác người dùng nào. Nó thực hiện các thao tác sau:

| Công việc | Mô tả |
|---|---|
| Copying files | Thiết lập việc sao chép các file cần thiết tới thư mục cài đặt như các file phụ trợ và file hình ảnh. |
| Configuring the computer | Thiết lập việc khởi tạo trình đơn bắt đầu của bạn; các nhóm chương trình; cài đặt máy in, các dịch vụ, tài khoản quản trị, phông chữ, và đăng ký các thư viện động. |
| Saving the configuration | Thiết lập việc lưu trữ cấu hình, khởi tạo thư mục sửa chữa, đặt lại file Boot.ini. |
| Removing temporary files | Thiết lập việc dọn dẹp file và thư mục tạm đã khởi tạo và sử dụng trong quá trình cài đặt, như thư mục<br>$WIN_NT$.~LS. |

## 7.2 Đăng nhập tới một Domain

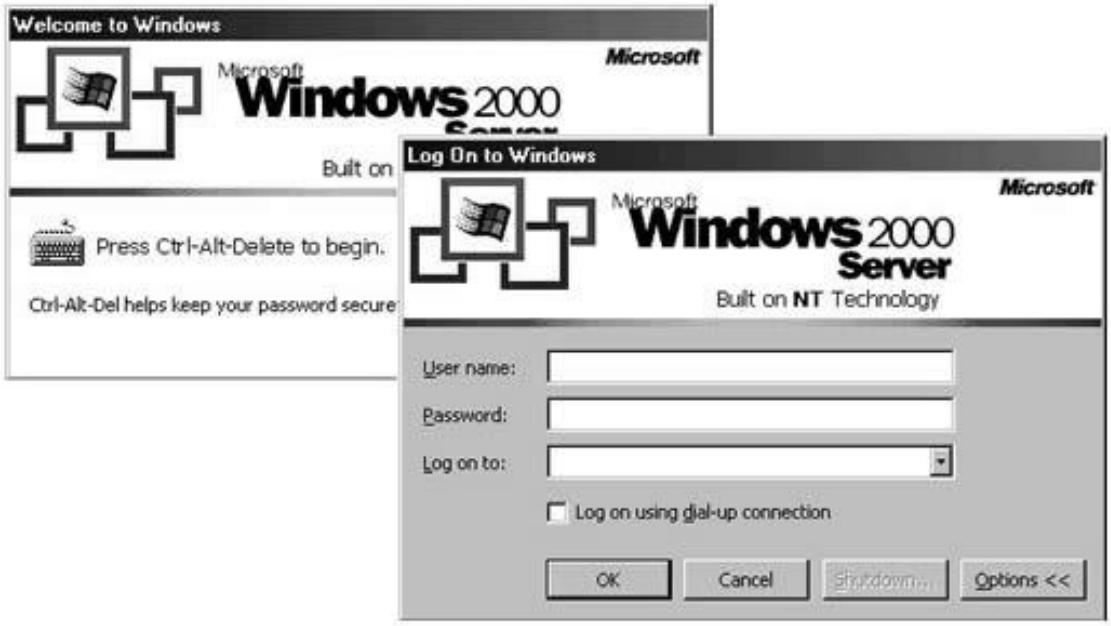
Bạn phải đăng nhập vào Windows 2000 để có thể truy xuất bất kỳ phần nào của hệ thống. Không giống như Windows 3.x hoặc Windows 9.x, bạn có thể truy xuất các file mà không cần đăng nhập tới mạng, bạn phải cung cấp thông tin đăng nhập đầu tiên trong Windows 2000.

Đăng nhập là quá trình nhận biết chính bạn tới máy tính bằng cách nhập tên và mật khẩu. Quá trình này nhận biết bạn như là người sử dụng hợp lệ và giúp duy trì sự bảo mật.

Để đăng nhập bạn phải cung cấp đúng tên và mật khẩu (user name and password), để kiểm tra định danh của bạn. Chỉ những người dùng hợp lệ mới có thể truy xuất tới nguồn tài nguyên và dữ liệu trên máy tính hoặc mạng.

Khi máy tính bắt đầu chạy Windows 2000 Server, nó sẽ hiển thị hộp thoại Welcome to Windows với lời nhắc nhấn **Ctrl+Alt+Delete** để đăng nhập.

Quá trình đăng nhập bắt đầu và đảm bảo rằng người dùng cung cấp đúng tên và mật khẩu tới hệ điều hành Windows khi bạn hoàn tất hộp thoại *Log On To Windows*.




Các lựa chọn trong hộp thoại Log on to Windows là:

| Tuỳ chọn | Mô tả |
|---|---|
| Hộp User Name | Mục này yêu cầu người dùng đăng nhập tên được cấp bởi người quản trị mạng. Để đăng nhập tới domain với tên người dùng, tài khoản người dùng phải lưu trữ tập trung trong thư mục hiện hành(Active Directory). |
| Hộp Password | Mật khẩu có phân biệt chữ hoa và chữ thường (case-sensitive). Các phần mật khẩu xuất hiện trên màn hình như là các dấu hoa thị (*) để đảm bảo bí mật. |
| Danh sách Log On To | Lựa chọn tên miền chứa tài khoản của bạn. Danh sách này chứa tất cả các miền trong cây miền. |
| Hộp kiểm tra Log On Using Dial-Up Connection | Cho phép người dùng kết nối tới miền máy chủ bằng cách dùng mạng dial-up, cho phép người dùng đăng nhập và thực hiện công việc từ vị trí ở xa. |

| | |
|---|---|
| Nút Shutdown | Đóng tất cả các file, lưu trữ tất cả dữ liệu của hệ điều hành, và chuẩn bị cho máy tính tắt an toàn. Trên các máy tính chạy hệ điều hành Windows 2000 Server, nút Shutdown không được đặt mặc định. |
| Nút Options | Dùng để đóng hoặc mở danh sách Log On To và hộp chọn Log On Using Dial-Up Connection. |

## 7.3 Các công cụ quản trị

Có một số công cụ quản trị sẵn có trên Windows 2000. Đa số các công cụ dùng wizard. Một số công cụ bao gồm: *Active Directory Users and Computers*; *Active Directory Domains and Trusts*; và snap-ins cho *DNS*, *DHCP* và *WINS*.

## 7.4 Hộp thoại bảo mật Windows 2000

Hộp thoại bảo mật Windows 2000 cung cấp một cách dễ dàng để truy xuất đến thông tin bảo mật. Nó hiển thị tài khoản người dùng đăng nhập hiện hành, miền hay máy tính mà người dùng được đăng nhập, ngày và thời gian người dùng đăng nhập. Thông tin này quan trọng đối với những người dùng có nhiều tài khoản. Thông qua nó ta xác định được ai có tài khoản chính, ai có tài khoản ưu tiên. Bạn truy cập vào hộp thoại bảo mật bằng cách nhấn **Ctrl+Alt+Delete** khi đăng nhập.

Bảng mô tả các nút nhấn trên hộp thoại Windows 2000 Security:

| Nút | Mô tả |
|---|---|
| **Lock Computer** | Cho phép người dùng bảo vệ máy tính không cần Log Off tất cả các chương trình đang chạy còn lại. Người dùng nên khoá máy tính của họ nếu không sử dụng. Người dùng có thể mở khoá lại bằng cách nhấn Ctrl+Alt+Delete và nhập đúng tên và mật khẩu. Người quản trị cũng có thể giải phóng khoá máy tính của người dùng hiện tại, tuy nhiên điều này là bắt ép đăng xuất (logoff) và dữ liệu có thể bị mất. |
| **Log Off** | Cho phép người dùng hiện tại đăng xuất và đóng tất cả các chương trình đang chạy. Hệ điều hành Windows 2000 vẫn đang chạy. |
| **Shut Down** | Cho phép người dùng đóng tất cả các file, cất tất cả dữ liệu hệ điều hành, và chuẩn bị cho máy tính có thể tắt máy một cách an toàn. |
| **Change Password** | Cho phép người dùng đổi mật khẩu tài khoản của họ. Họ phải biết mật khẩu cũ để khởi tạo mật khẩu mới. Đó là cách người dùng có thể thay đổi mật khẩu của họ. Các nhà quản trị nên yêu cầu những người dùng thay đổi mật khẩu chính của họ và nên tạo sự giới hạn mật khẩu như là phần của chính sách tài khoản. |

| Nút | Mô tả |
|---|---|
| **Task Manager** | Cung cấp danh sách những chương trình hiện tại đang chạy, xem xét hiệu suất sử dụng toàn bộ CPU và bộ nhớ, tổng quan mỗi chương trình, mỗi thành phần chương trình, hoặc hệ thống xử lý đang xử dụng CPU, bộ nhớ, trình quản lý tác vụ có thể được dùng để lựa chọn chương trình và dừng chương trình khi nó không đáp ứng. |
| **Cancel** | Đóng hộp thoại Windows Security. |

# Câu hỏi ôn tập chương 7

1. Khi cài đặt Windows 2000 Server ổ cứng yêu cầu còn trống tối thiểu là:
   a. 571 MB
   b. 671 MB
   c. 2 GB
2. Những hệ điều hành nào, trên đó khi cài đặt Windows 2000 Server phải sử dụng file Winnt32.exe ?
   a. Win 9X.
   b. Win NT 4.0 Workstation
   c. MS-DOS
   d. Win NT Server 4.0
   e. Windows 3.x
3. Thư mục nào sẽ được tạo mặc định khi bạn cài hệ điều hành Windows 2000 Server ?
   a. Windows
   b. WINNT
   c. None of the others
4. Chọn các quy tắc để đặt tên cho máy tính khi bạn cài hệ điều hành Windows 2000 Server .
   a. up to 15 characters
   b. different from all other computer, workgroup, or domain names.
   c. can contain asterisk characters.
5. Giao thức mặc định khi bạn cài đặt hệ điều hành Windows 2000 Server là …….
   a. IPX/SPX
   b. TCP/IP
   c. NetBEUI
   d. Apple Talk
6. Mật khẩu tối đa là bao nhiêu ký tự?
   a. 64
   b. 127
   c. 15
   d. 31

# CHƯƠNG 8 - QUẢN TRỊ TÀI KHOẢN NGƯỜI DÙNG

## MỤC TIÊU CỦA CHƯƠNG

*Kết thúc chương này bạn có thể:*

- Biết được các loại tài khoản người dùng
- Biết cách lập kế hoạch về tài khoản người dùng
- Tạo một số tài khoản người dùng và quản trị nó.

## 8.1 Các loại tài khoản người dùng (user)

Windows 2000 có một số loại tài khoản người dùng sau: *tài khoản cục bộ* ( local user accounts), *tài khoản miền* (domain user accounts), và *tài khoản cài đặt sẵn* (built-in user accounts). Với tài khoản cục bộ người dùng có thể đăng nhập vào máy tính riêng để truy xuất tài nguyên mạng trên máy tính đó. Với tài khoản miền, người dùng có thể đăng nhập tới miền để truy cập các nguồn tài nguyên mạng. Tài khoản cài đặt sẵn được dùng để thực hiện các tác vụ quản trị hoặc truy cập tới các nguồn tài nguyên mạng.

### 8.1.1 Tài khoản cục bộ

Tài khoản cục bộ được tạo trên những máy tính riêng biệt và cho phép người dùng đăng nhập vào máy tính và sử dụng tài nguyên chỉ trên máy tính đó. Tài khoản người dùng được khởi tạo trong những cơ sở dữ liệu bảo mật cục bộ và không tạo bản sao tới phần còn lại của miền. Trên các máy điều khiển miền (Domain Controller – DC) không có các tài khoản cục bộ, do vậy người dùng sẽ không được xác nhận trên miền và sẽ không được sử dụng tài nguyên miền. Các nhà quản trị miền không thể quản trị tài khoản cục bộ trừ khi họ kết nối riêng tới máy tính cục bộ để thực hiện các thao tác quản trị.

### 8.1.2 Tài khoản miền

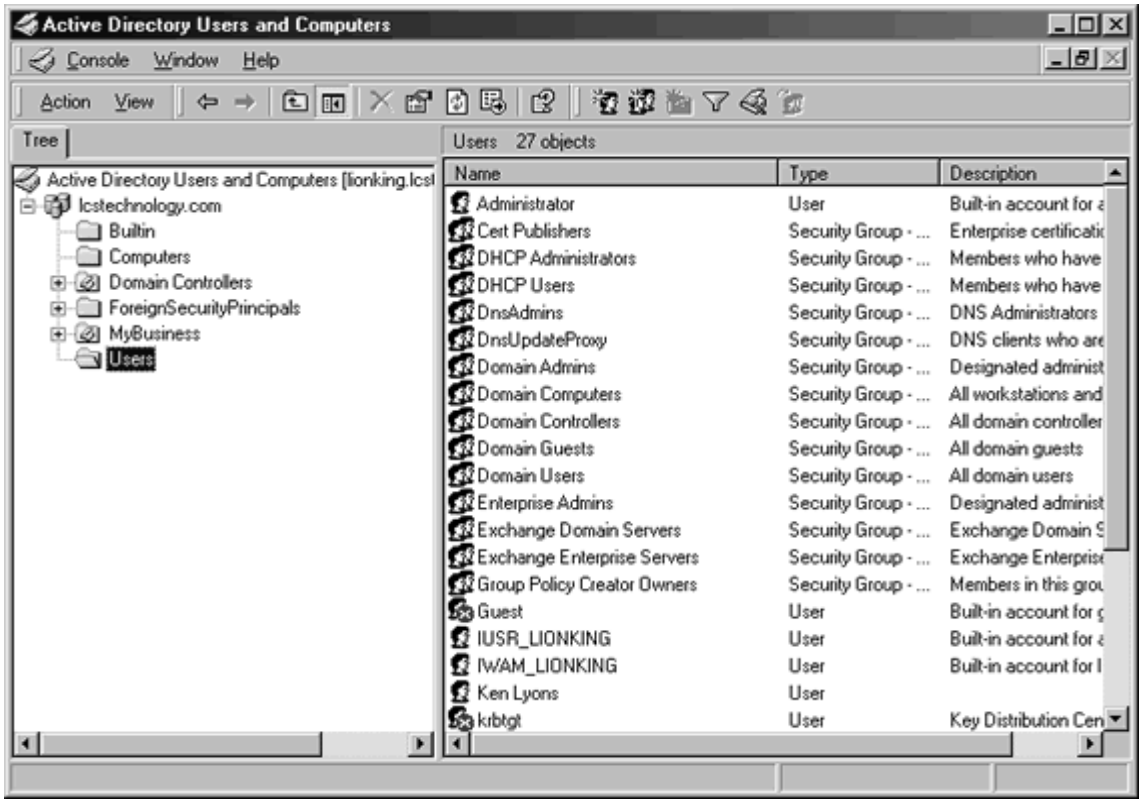
Tài khoản miền cho phép người dùng đăng nhập tới miền và truy xuất tới các tài nguyên ở bất kỳ đâu trên mạng. Người dùng cần nhập tên và mật khẩu của mình khi đăng nhập, việc kiểm tra tên và mật khẩu người dùng do DC đảm nhiệm. Khi một tài khoản được xác minh, Windows 2000 cấp một thẻ truy cập được dùng trong suốt phiên đăng nhập. Thẻ này chứa các thông tin về người dùng và tất cả các tài nguyên mà người dùng được phép truy cập.

Tài khoản miền được khởi tạo bên trong một container hoặc một đơn vị tổ chức (organizational unit – OU) trong bản sao của cơ sở dữ liệu Active Directory trên máy DC. Mỗi DC định kỳ tạo những bản sao về thông tin tài khoản người dùng mới tới tất cả các DC khác trong miền để xác nhận quyền truy cập của người dùng trên miền trong phiên đăng nhập.

### 8.1.3 Tài khoản cài đặt sẵn

Có một số tài khoản người dùng được tạo tự động khi Windows 2000 Server được cài đặt. Như tài khoản **Administrator** và **Guest**. Tài khoản Administrator được dùng để quản lý tất cả các máy tính và cấu hình miền cho các thao tác như là khởi tạo và sửa đổi

tài khoản người dùng và tài khoản nhóm, quản lý các chính sách bảo mật, khởi tạo máy in, và cấp phép và cấp quyền truy cập tài nguyên tới người dùng.




*Hình 8.1* Microsoft Management Console (MMC)
Active Directory Users and Computer

## 8.2 Lập kế hoạch tài khoản người dùng

Trước khi bạn cài đặt mạng, bạn cần phải lập kế hoạch người dùng, điều này rất quan trọng với mạng của bạn. Mọi thứ như là qui ước đặt tên người dùng phải hoàn tất trước khi tiến hành cài đặt.

### 8.2.1 Qui ước đặt tên

Qui ước đặt tên xác định mỗi user được nhận dạng duy nhất trong miền. Qui ước đặt tên nhất quán sẽ giúp bạn và người dùng nhớ nó khi đăng nhập.

Một vài điểm cần xem xét khi xác định qui ước đặt tên là:

| Consideration | Explanation |
|---|---|
| Các tài khoản người dùng cục bộ (Local user accounts) | Các tên tài khoản người dùng cục bộ phải duy nhất trên máy tính mà bạn tạo tài khoản cục bộ đó. |
| Các tài khoản người dùng miền (Domain user accounts) | Tên đăng nhập của người dùng phải duy nhất tới thư mục. Tên đầy đủ của người dùng cũng phải duy nhất trong Organisation Unit (OU) nơi bạn tạo tài khoản người dùng miền đó. |

| Consideration | Explanation |
|---|---|
| Nhiều nhất là 20 ký tự | Tên đăng nhập có thể dài tới 20 ký tự, bao gồm chữ hoa hoặc chữ thường. Dù trường dữ liệu có thể chấp nhận dài hơn, Windows 2000 chỉ lấy 20 ký tự đầu. |
| Các ký tự không hợp lệ | Bao gồm: " / \ [ ] : ; \| = , + * ? < > |
| Tên đăng nhập của người dùng không phân biệt ký tự hoa hay ký tự thường. | Bạn có thể dùng tổ hợp các ký tự kể cả ký tự đặc biệt để tạo tài khoản người dùng duy nhất. |
| Xét các nhân viên có cùng tên . | Nếu hai người dùng có cùng tên là John Smith, bạn có thể dùng tên của họ và thêm vào các ký tự hay ký số khác nhau để phân biệt. Thí dụ: Johns và Johnsm, hay Johns1 và Johns2. |
| Nhận dạng loại nhân viên. | Trong một số tổ chức có thể có nhiều loại nhân viên, ví dụ như nhân viên chính và nhân viên tạm tuyển. Để phân biệt nhân viên tạm, bạn có thể dùng ký tự T (Temp) làm tiếp đầu ngữ, ví dụ: T-Johns, cho John Smith. |
| Tính tương thích với hệ thống thư điện tử | Một số hệ thống thư điện tử có thể không chấp nhận một số ký tự như khoảng trắng hay dấu ngoặc ( "()" ) |

### 8.2.2 Những yêu cầu về mật khẩu (Password Requirements)

Mỗi tài khoản người dùng trên mạng Windows 2000 nên có mật khẩu để bảo vệ truy xuất tới domain hoặc máy tính cá nhân. Một vài quy tắc khi đặt mật khẩu là:

- Tài khoản quản trị phải có mật khẩu để ngăn sự đăng nhập bất hợp pháp.
- Quyết định xem nên để người quản trị hay người dùng điều khiển mật khẩu. Bạn có thể gán mật khẩu duy nhất đối với tài khoản người dùng và ngăn người dùng thay mật khẩu, hoặc bạn có thể cho phép người dùng nhập mật khẩu lần đầu họ đăng nhập. Người dùng nên điều khiển mật khẩu của bạn.
- Sử dụng mật khẩu phải khó đoán. Thí dụ, tránh sử dụng mật khẩu với những kết hợp rõ ràng, như tên thành viên gia đình.
- Mật khẩu có thể tới 14 ký tự, tối thiểu nên là 8 ký tự.
- Ba nhóm ký tự có thể dùng để đặt mật khẩu: Các ký tự hoa và ký tự thường, các ký số, và các ký tự khác.
- Tạo mật khẩu sau phải khác nhiều so với các mật khẩu trước.
- Chúng không được trùng với tên của người dùng hoặc chứa tên người dùng.

### 8.2.3 Hạn chế giờ đăng nhập và hạn chế trạm đăng nhập

Mặc định, mỗi tài khoản người dùng mới lúc khởi tạo không bị giới hạn giờ đăng nhập. Tạo ra các hạn chế này là do yêu cầu bảo mật của mạng. Nếu người dùng bao giờ cũng làm việc từ 9 giờ sáng đến 5 giờ chiều, từ thứ hai đến thứ sáu, thì việc truy cập ngoài giờ đó sẽ bị kiểm tra kỹ. Việc này sẽ giới hạn khả năng đối với những truy xuất không được phép. Cũng như vậy, nên xem xét việc giới hạn đăng nhập của user trên những máy tính xác định. Điều này giúp cho việc bảo mật mạng và giúp cho các nhà quản trị xác định chính xác người dùng có thể truy cập mạng ở đâu. Đối với tài khoản của các nhân viên tạm tuyển, thì nên có ngày kết thúc. Khi nhân viên đi khỏi công ty thì ngày sử dụng tài khoản của họ cũng nên hết hạn.

Các điểm cần nhớ khi xét đến giờ đăng nhập và giới hạn trạm làm việc:

- Giờ đăng nhập nên thiết lập cho người dùng chỉ yêu cầu truy cập tại thời gian cụ thể định trước, thí dụ chỉ cho phép các công nhân làm việc ca đêm truy cập mạng trong giờ làm của họ.
- Nên yêu cầu người dùng đăng nhập mạng từ máy tính của họ khi dữ liệu nhạy cảm được lưu giữ trên ổ cứng cục bộ của họ.

### 8.2.4 Bảng kế hoạch tài khoản người dùng

Để giúp cho công việc lập kế hoạch tài khoản người dùng dễ dàng, Microsoft đã phát triển phần mềm User Account Planning Worksheet. Để hoàn thiện công việc này bạn cần làm các bước sau:

- Ghi tên đầy đủ cho mỗi người dùng
- Định tên quy ước của bạn và ghi tên người dùng trên cơ sở này.
- Bao gồm cả tên công việc cho mỗi nhân viên
- Xác định mật khẩu cho mỗi người dùng (mật khẩu lúc khởi tạo)
- Ở cột vị trí Home Folder, ghi vị trí của nó là trên máy cục bộ hay máy chủ
- Ở cột giờ đăng nhập, điền giờ truy xuất cho mỗi người dùng
- Ghi dưới giới hạn trạm làm việc là yes nếu người dùng bị giới hạn và là no nếu không.

Bản kế hoạch hoàn thành sẽ có dạng như sau:

**User Accounts Planning Sheet**

**Qui ước đặt tên:** 3 ký tự đầu tiên của phần tên (first name), đi theo 3 ký tự đầu của phần họ (surname). Mật khẩu là ký tự đầu tiên của first name, theo sau là từ "password", cuối cùng là ký tự đầu của surname.

| Full Name | User Account | Description | Password Requirements | Home folder location | Logon hours | Workstation |
|---|---|---|---|---|---|---|
| John Smith | Johsmi | Vice President | Jpasswords | Server | 7.30 – 23.55 | N |
| Jim Jones | Jimjon | Temp | Jpasswordj | Server | 8.55 – | Y |

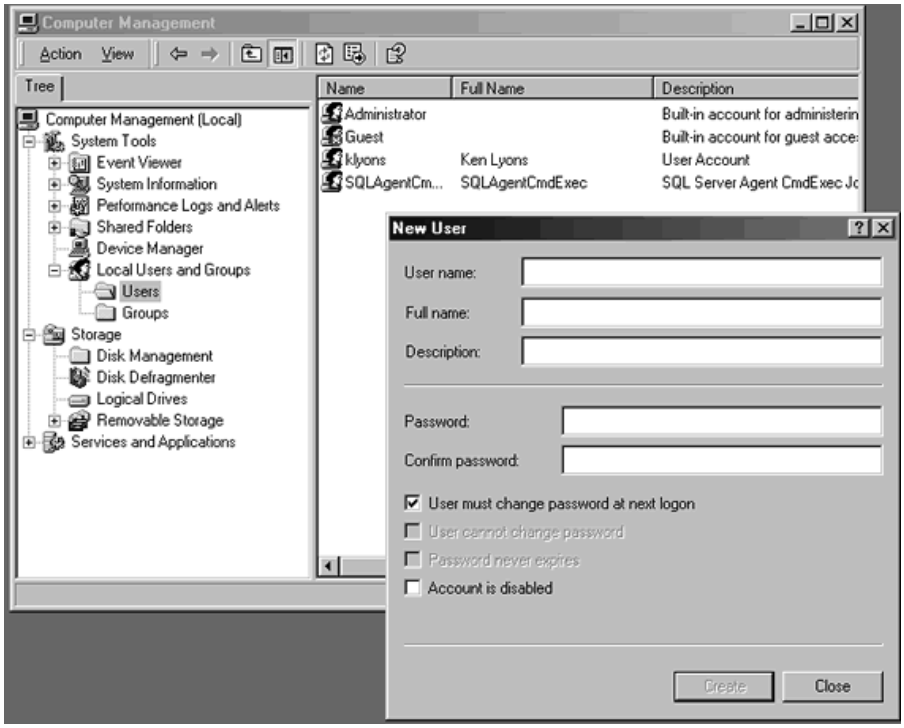
| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | 17.15 | |

## 8.3 Tạo tài khoản người dùng cục bộ và tài khoản người dùng miền

### 8.3.1 Tạo tài khoản người dùng cục bộ

Để tạo tài khoản người dùng, bạn sử dụng chương trình MMC *Local Users and Groups*. Bạn có thể tạo, xoá hoặc vô hiệu tài khoản người dùng trên máy cục bộ trong nhóm làm việc. Bạn không thể tạo tài khoản cục bộ trên domain controller.

1. Kích Start -> Programs -> Administrative Tools -> kích Computer Management.
2. Mở rộng mục Local Users and Groups, kích nút phải trên Users, và chọn New User.
3. Trong cửa sổ New User nhập các thông tin tài khoản user cục bộ như đã xác định trong giai đoạn lập kế hoạch.




Các mục chọn trong cửa sổ New User:

| Các tuỳ chọn | Mô tả |
|---|---|
| User Name | Tên phải duy nhất khi bạn nhập. Hộp thoại này là bắt buộc. |
| Full Name | Tên đầy đủ của người dùng. Hộp thoại này là tuỳ chọn. |
| Description | Các mô tả rất hữu ích để xác định người dùng, thí dụ như phòng ban hay nơi làm việc. Hộp thoại này là tuỳ chọn |
| User Must Change Password At Next Logon | Yêu cầu người dùng thay đổi mật khẩu của họ khi đăng nhập lần đầu. |

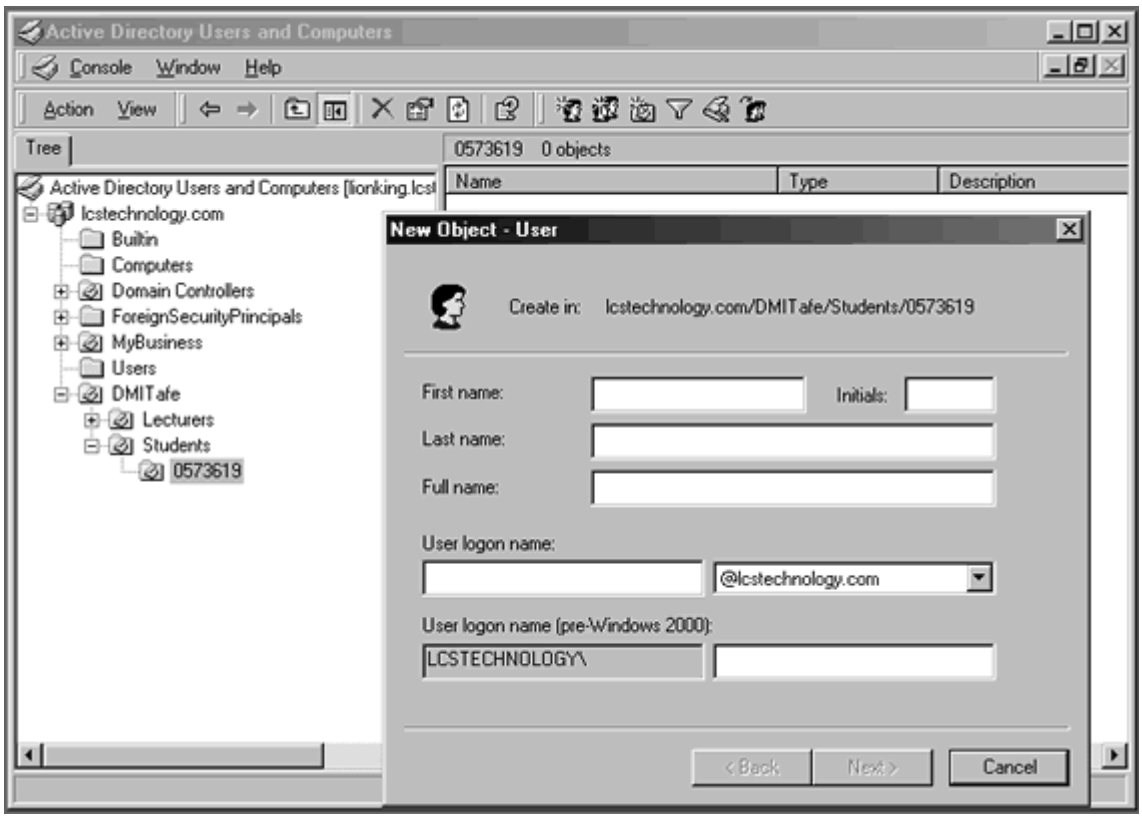
| Các tuỳ chọn | Mô tả |
|---|---|
| User Cannot Change Password | Chỉ cho phép nhà quản trị thay đổi mật khẩu. |
| Password Never Expires | Mật khẩu sẽ không bao giờ thay đổi. Người dùng phải thay đổi mật khẩu tại lần đăng nhập kế và ghi đè nên mục chọn mật khẩu không bao giờ đổi. |
| Account Is Disabled | Ngăn người dùng không cho dùng tài khoản của họ. |

### 8.3.2 Tạo tài khoản người dùng miền (Domain)

Để tạo tài khoản người dùng miền, bạn cần sử dụng chương trình *Active Directory Users and Computers*. Dùng chương trình này bạn có thể tạo, xoá hoặc vô hiệu tài khoản người dùng trên domain controller, hay tài khoản người dùng cục bộ trên bất kỳ máy tính nào trong miền.

Khi bạn tạo tài khoản người dùng miền, người dùng sẽ đăng nhập tới miền bằng tên mặc định. Tuy nhiên, bạn có thể lựa chọn bất kỳ miền nào để tạo tài khoản người dùng miền cho người dùng đó. Bạn phải chọn nơi cất trữ tài khoản mới đó. Bạn có thể tạo tài khoản người dùng miền trong nơi chứa người dùng mặc định hoặc ở nơi cất trữ miền. Thí dụ, nơi chứa (OU) gọi là DMITafe được khởi tạo. OU đó có thể chứa các OU khác, như Lecturers, Students, vân vân. Mỗi OU có thể có tài khoản người dùng đã được tạo.

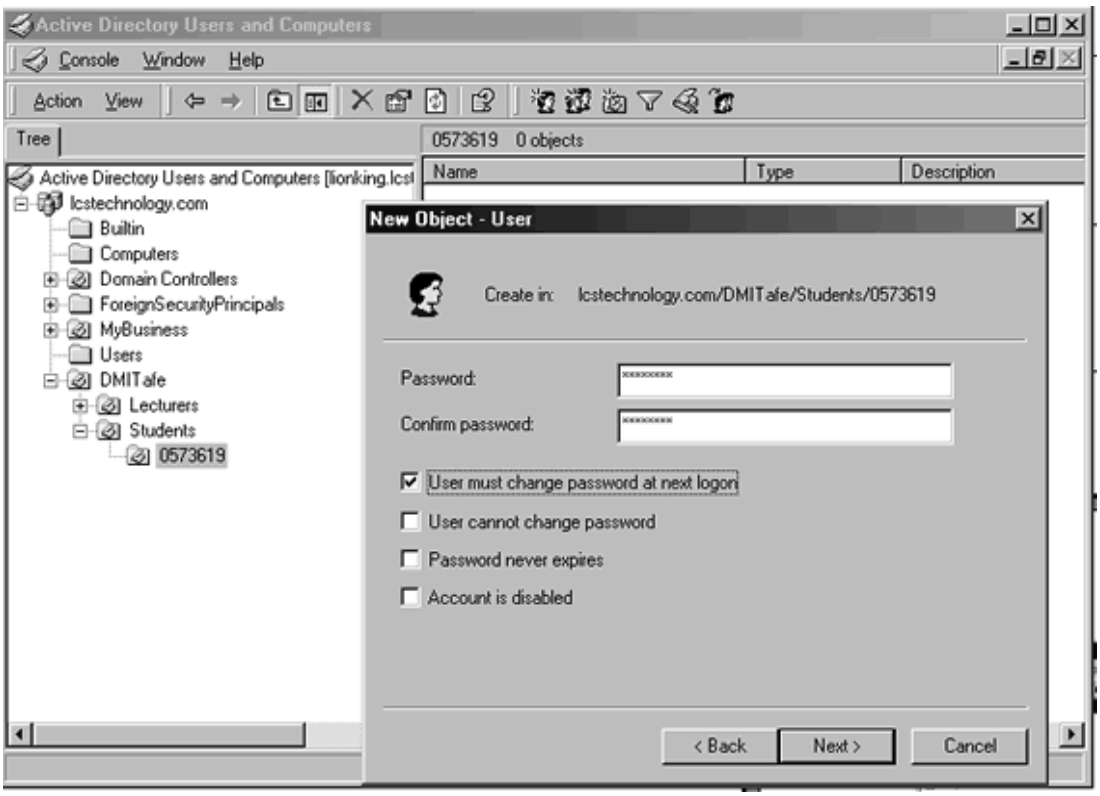
1. Kích Start -> Programs -> Administrative Tools -> Active Directory Users And Computers.
2. Chọn domain -> kích nút phải tại container Users -> New -> User
3. Trong cửa sổ *New Object – User* nhập các thông tin tài khoản user miền như đã xác định trong giai đoạn lập kế hoạch.



Các mục chọn trong hộp thoại New Object - User:

| Các tuỳ chọn | Mô tả |
|---|---|
| First Name | Tên người dùng hoặc họ tên, hộp thoại này yêu cầu bắt buộc phải nhập. |
| Initials | Tên viết tắt của người dùng, hộp thoại này bắt buộc. |
| Last Name | Họ của người sử dụng, hộp thoại này bắt buộc. |
| Full Name | Họ tên người dùng. Tên phải duy nhất trong nơi lưu giữ nó. Windows 2000 hoàn thiện mục chọn này nếu bạn nhập vào thông tin vào ba hộp thoại trên . Mục Create-In hiển thị tên này ở dạng đường dẫn tên phân biệt. |
| User Logon Name | Tên đăng nhập chứa trong hộp và danh sách xác định duy nhất người dùng trên mạng. Hộp thoại này bắt buộc và yêu cầu không được nhập trùng tên đã có trên miền. |
| User Logon Name (Pre-Windows 2000) | Dùng cho các phiên bản khác của Windows, như Windows NT 4.0 hay Windows NT 3.5.1. Hộp thoại này bắt buộc và yêu cầu không được nhập trùng tên đã có trên miền. |

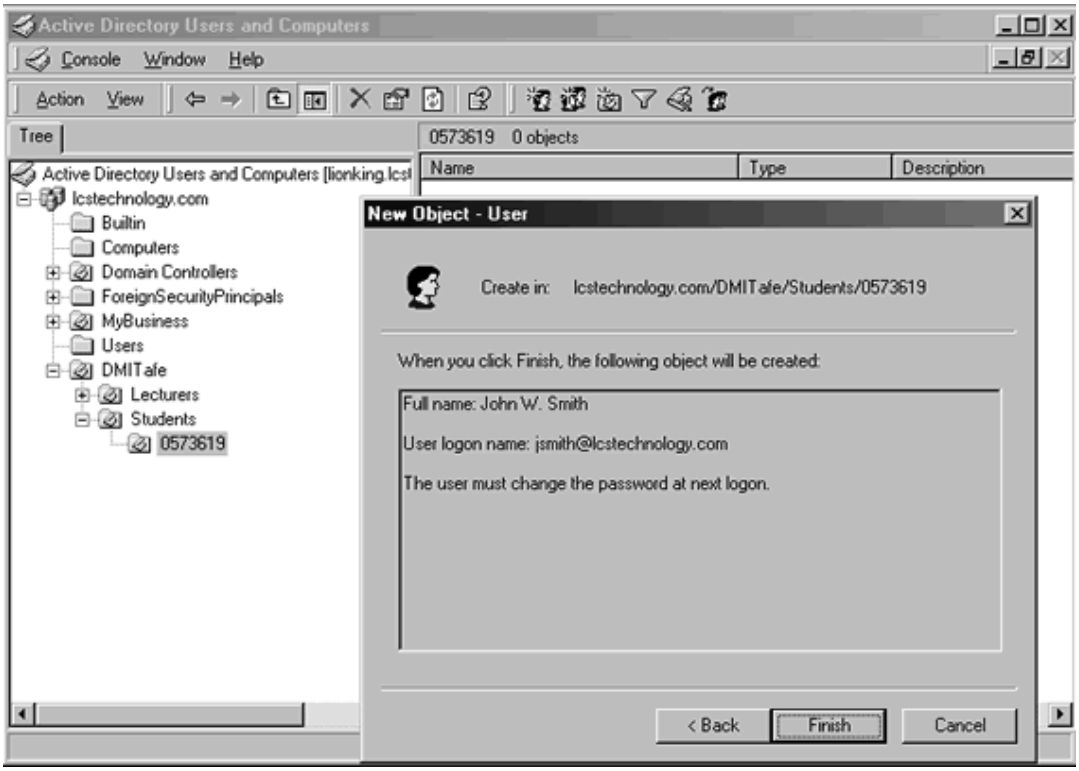
Khi những mục này đã hoàn thành, người quản trị nhấn vào nút Next, nó sẽ hiển thị tiếp hộp thoại Password Options.



Các mục chọn trong hộp thoại New Object – User Password Options :

| Các tuỳ chọn | Mô tả |
|---|---|
| Password | Mật khẩu được dùng để xác nhận quyền người dùng. Để bảo mật hơn bạn luôn gán mật khẩu. |
| Confirm Password | Xác nhận mật khẩu bằng cách nhập nó một lần nữa để đảm bảo rằng bạn đã gõ đúng mật khẩu. Hộp thoại này bắt buộc nếu bạn gán mật khẩu. |
| User Must Change Password At Next Logon | Yêu cầu người dùng thay đổi mật khẩu của họ lần đầu đăng nhập vào mạng. Điều này đảm bảo rằng chỉ người dùng mới biết mật khẩu của họ. |
| User Cannot Change Password | Chỉ những người quản trị mới được phép thay đổi mật khẩu. Chọn hộp kiểm này nếu bạn có nhiều hơn một người sử dụng cùng tài khoản miền hoặc để bảo trì điều khiển trên các mật khẩu tài khoản người dùng. |
| Password Never Expires | Mật khẩu sẽ không bao giờ thay đổi. Đối với tài khoản sử dụng miền bạn sẽ dùng chương trình hoặc dịch vụ Windows 2000. Mục User Must Change Password At Next Logon ghi đè nên mục Password Never Expires. |
| Account Is Disabled | Ngăn người dùng sử dụng tài khoản của họ. |

Sau khi điền vào hộp thoại Password Option, nhấn Next và sau đó là Finish để tạo tài khoản mới.



Mỗi tài khoản người dùng mới được tạo mặc định có thể thay đổi bằng cách nhắp đúp chuột vào người dùng mới trong trình đơn *Active Directory Users and Computers* và sau đó xác nhận các thuộc tính còn lại. Các thuộc tính này bao gồm các thuộc tính cá nhân và tài khoản, các mục chọn đăng nhập và thiết lập dial-in.

Các thuộc tính đó nên được điền đầy đủ thông tin.

Bảng sau mô tả các thuộc tính của người dùng:

| Tab | Mô tả |
|---|---|
| General | Chứa tên người dùng, hiển thị tên, mô tả, vị trí cơ quan, số điện thoại, địa chỉ e-mail, trang chủ và các trang Web bổ sung. |
| Address | Chứa địa chỉ đường phố , địa chỉ gửi thư đường bưu điện, mã vùng và mã nước. |
| Account | Chứa các thuộc tính tài khoản người dùng bao gồm: Tên đăng nhập, giờ đăng nhập, các máy được phép đăng nhập tới, các mục tài khoản, thời hạn kết thúc. |
| Profile | Thiết lập đường dẫn hồ sơ, đường dẫn kịch bản đăng nhập, thư mục gốc, thư mục tài liệu chia sẻ. |
| Telephones | Chứa số điện thoại bàn , điện thoại di động, số fax, giao thức Internet, và chỗ trống cho lời chú giải. |
| Organisation | Chứa các tiêu đề về người dùng như tên phòng ban, công ty, người quản lý, và các báo cáo trực tiếp. |
| Remote Control | Thiết lập điều khiển từ xa cho Terminal Services. |
| Terminal Services Profile | Cấu hình hồ sơ người dùng dịch vụ đầu cuối. |
| Member Of | Chứa các nhóm mà người sử dụng là thành viên. |
| Dial-In | Chứa các thuộc tính dial-in cho người dùng . |
| Environment | Cấu hình môi trường khởi động các dịch vụ đầu cuối. |
| Sessions | Thiết lập ngưỡng thời gian cho Terminal Services và các thiết lập lại kết nối. |

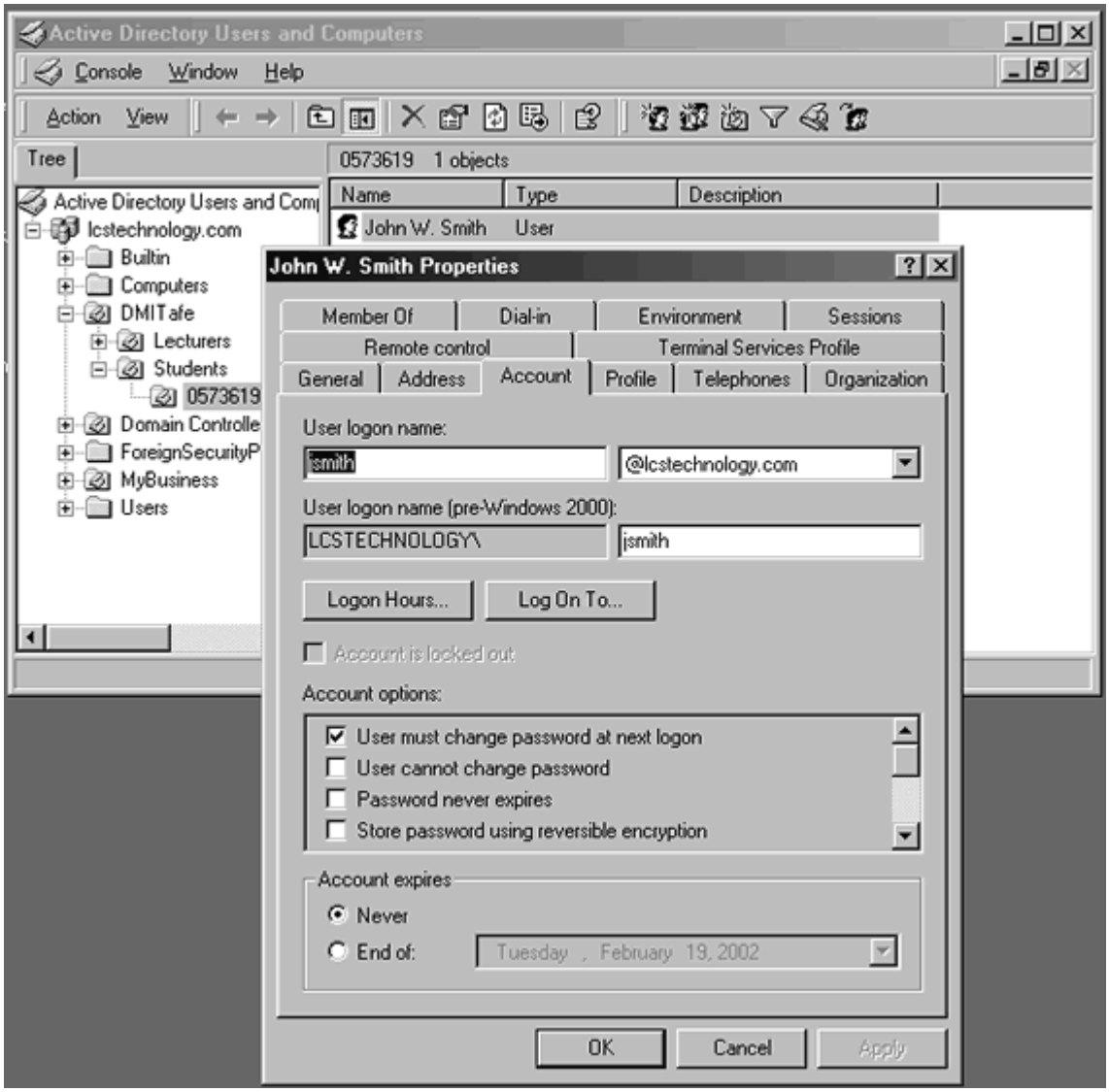
- Các thuộc tính cá nhân (Personal properties)

Bao gồm các trang (Tab) General, Address, Telephones, Organisation và cần được hoàn tất tương ứng với mỗi một tài khoản người dùng. Tương ứng với mỗi trường là một thuộc tính tìm kiếm.

- Các thuộc tính tài khoản (Account Properties)

Thuộc tính tài khoản người dùng được nhập qua trang Account. Một vài thuộc tính được tạo cùng thời gian với tài khoản người dùng miền. Tuy nhiên, các thuộc tính

thêm chỉ có hiệu lực khi bạn chọn lựa trang Account và hoàn tất các mục còn lại trong bảng.



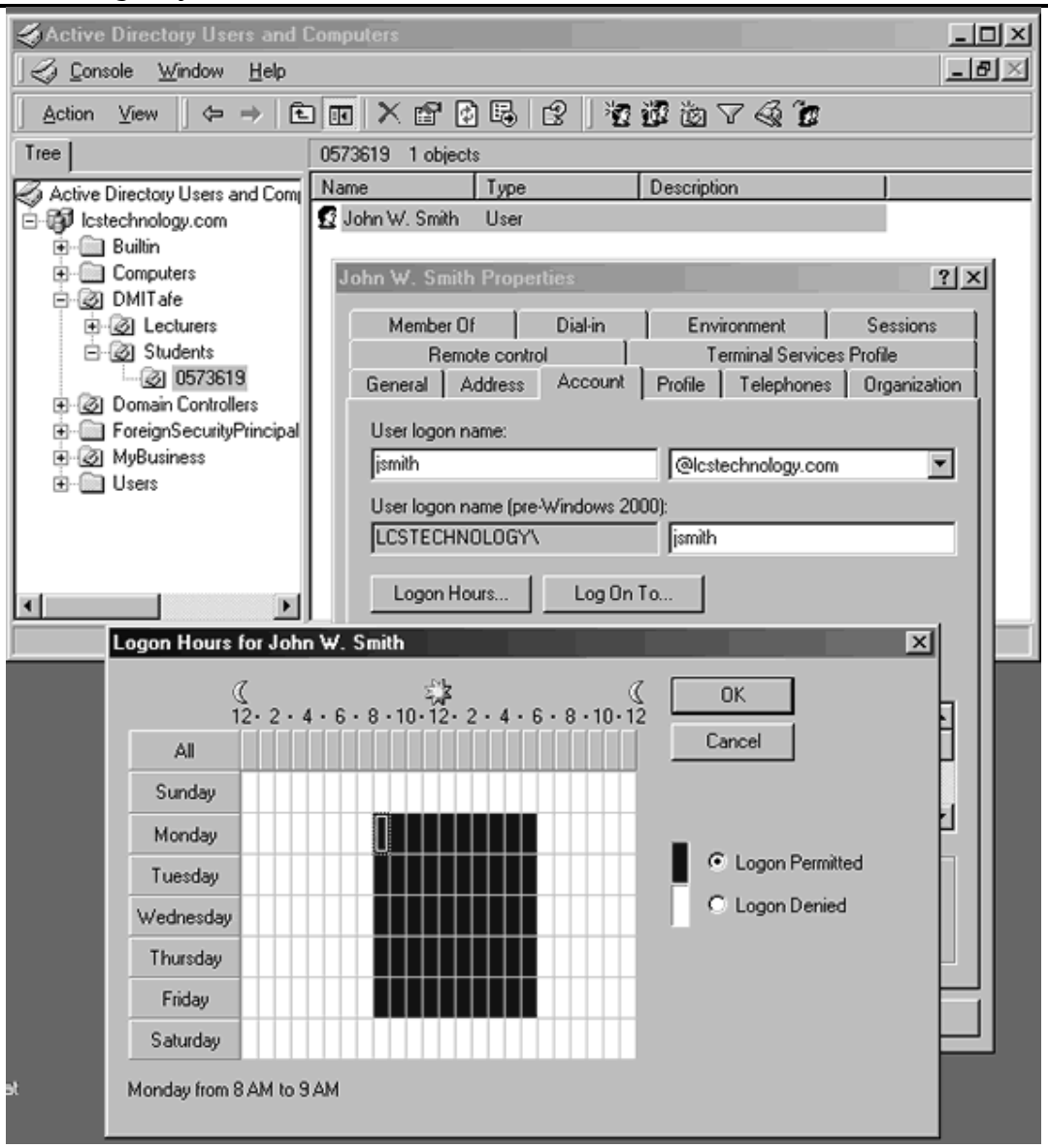

- Giờ đăng nhập( Logon Hours)

Thiết lập giờ đăng nhập trong hộp thoại Properties của bảng Account, nhấp chuột vào Logon Hours. Trên hộp thoại Logon Hours cho người dùng, hộp màu xanh chỉ định người dùng có thể đăng nhập, hộp màu trắng chỉ thị rằng người dùng không thể đăng nhập.

Để cho phép hay từ chối truy xuất cần làm những điều sau:

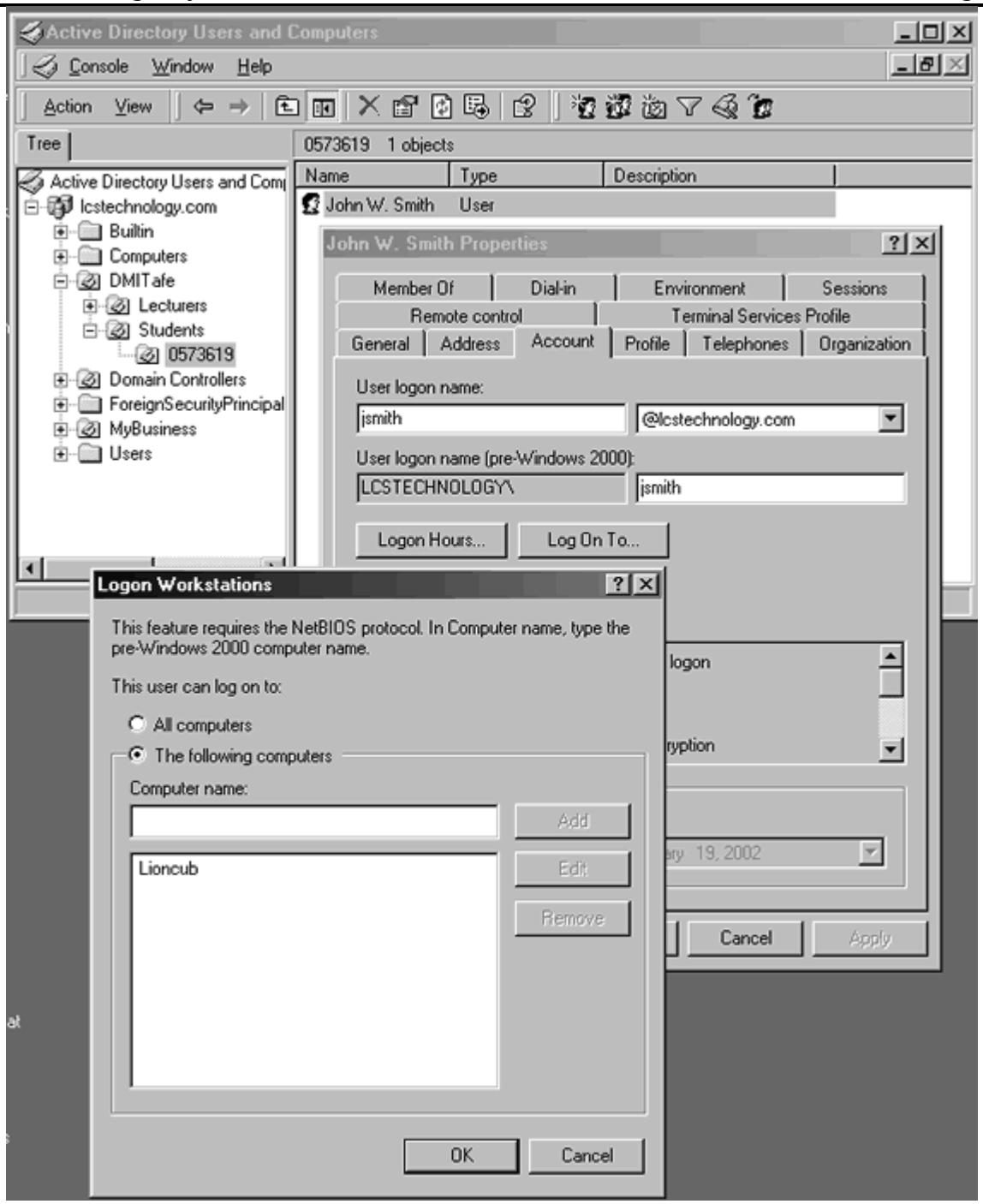
- Chọn các hình chữ nhật trên đó có các ngày và giờ bạn cho phép người dùng truy cập, chọn thời gian bắt đầu và thời gian kết thúc, và nhấp nút Logon Permitted.

- Chọn các hình chữ nhật trên đó có các ngày và giờ bạn không cho phép người dùng truy cập, chọn thời gian bắt đầu và thời gian kết thúc, và nhấp nút Logon Denied.



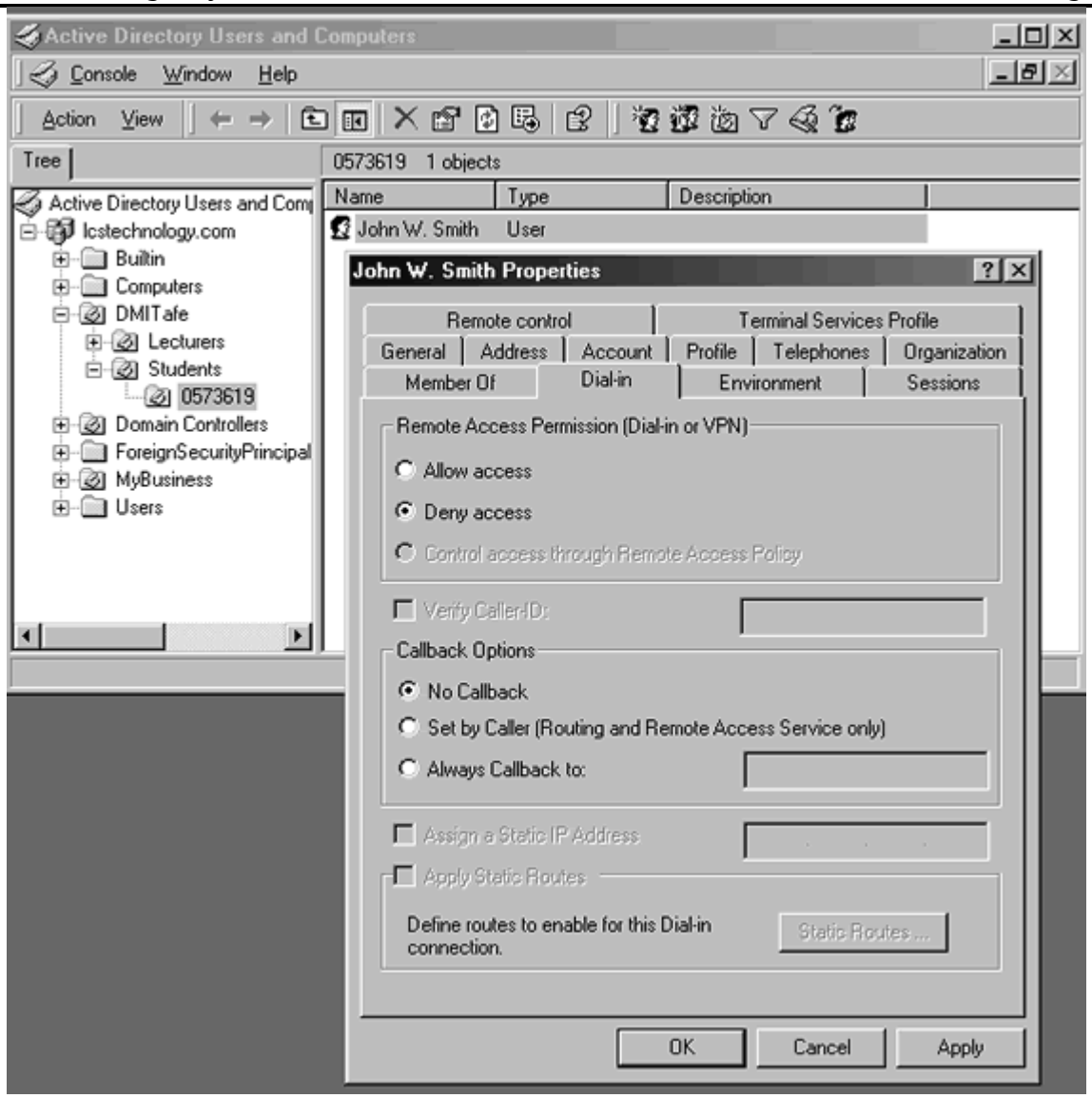

- Giới hạn các máy tính mà người dùng có thể đăng nhập tới

Cân nhắc xem người dùng có nên bị giới hạn đăng nhập tới các máy tính riêng hay không. Điều này rất cần cho việc bảo mật mạng và nó giúp người quản trị mạng biết chính xác người dùng truy cập mạng ở đâu. Để giới hạn người dùng truy cập tới máy tính khác ta chọn nút *Log On To…* trên trang Account và thêm tên các máy tính mà bạn cho phép người dùng đăng nhập tới.




- Xác nhận cho phép Dial-In

Các thiết lập xác nhận dial-in cho tài khoản người dùng được phép kết nối dial-in tới mạng từ xa. Để truy cập tới mạng, người dùng chạy chương trình Windows 2000 Remote Access Server (RAS). Người dùng được xác thực đồng thời là đang truy cập mạng nếu họ đã thực sự đăng nhập tới trạm đang kết nối tới mạng LAN.




Các mục chọn trong bảng Dial-In:

| **Các tuỳ chọn** | **Mô tả** |
|---|---|
| Allow Access | Quay số hoăc mạng ảo truy xuất từ xa cho người dùng. |
| Deny Access | Tắt dial-in hoặc truy xuất từ xa VPN cho người dùng. |
| Control Access Through Remote Access Policy | Cho phép người dùng truy cập từ xa. |
| Verify Caller-ID | Chỉ định số điện thoại mà người dùng phải quay vào. |

| Các tuỳ chọn | Mô tả |
|---|---|
| Callback Options | Các phương pháp gọi sau bao gồm:<br>*No Callback.* Dịch vụ RAS sẽ không gọi cho người dùng muốn gọi lại , mục này là mặc định.<br>*Set By Caller (Routing and Remote Access Service Only).* Người dùng cung cấp cho RAS số điện thoại để gọi lại. Công ty sẽ trả tiền cho mục này.<br>*Always Callback To.* Dịch vụ RAS dùng số điện thoại danh nghĩa cho người dùng gọi lại. Người dùng phải có số điện thoại danh nghĩa để kết nối với máy chủ. Dùng mục chọn này cho môi trường cần bảo mật cao. |
| Assign A Static IP Address | Định rõ những thiết lập cho hồ sơ dial-in nhóm ít quan tâm và gán địa chỉ TCP/IP tới người dùng này. |
| Apply Static Routes | Định rõ cấu hình tìm đường giới hạn trước để kết nối. |
| Static Routes | Cho phép xác định tìm đường tĩnh. |

## 8.4 Thiết lập hồ sơ người dùng (User Profile)

### 8.4.1 Khái niệm hồ sơ người dùng (User Profiles)

Hồ sơ người dùng bao gồm các thư mục và dữ liệu liên quan đến môi trường màn hình làm việc hiện tại của người dùng, những ứng dụng và dữ liệu cá nhân. Hồ sơ người dùng lưu tất cả các kết nối mạng được thiết lập khi người dùng đăng nhập tới máy tính, như là các mục trong trình Start và các ổ đĩa được ánh xạ tới các máy chủ mạng. Mỗi lần người dùng đăng nhập vào mạng, các thiết lập của họ sẽ giống như lần đăng nhập trước.

### 8.4.2 Ưu điểm của hồ sơ người dùng

- Cho phép nhiều người cùng sử dụng chung một máy tính, và mỗi người nhận được cài đặt màn hình riêng khi họ đăng nhập.
- Khi người dùng đăng nhập vào trạm làm việc của họ, họ sẽ nhận được màn hình như là khi họ đã thoát khỏi của phiên làm việc trước.
- Sự tuỳ biến của môi trường màn hình bởi một người sử dụng nào đấy sẽ không ảnh hưởng đến các thiết lập của người dùng khác.
- Các hồ sơ người dùng có thể được cất trên máy chủ để chúng có thể theo người dùng tới bất kỳ máy tính nào đang chạy Windows NT 4.0 hay Windows 2000 trên mạng. Hồ sơ này gọi là hồ sơ người dùng lang thang (*roaming user profiles).*
- Thiết lập ứng dụng được tiếp tục sử dụng, đó là các ứng dụng được xác nhận trên Windows 2000.
- Các nhà quản trị có thể khởi tạo hồ sơ người dùng mặc định, mà nó thích hợp với các công việc của người dùng đó.
- Bạn có thể thiết lập hồ sơ người dùng bắt buộc, hồ sơ đó không lưu giữ các thay đổi khi người dùng thiết lập màn hình. Người dùng có thể sửa đổi những thiết lập

màn hình của máy tính trong khi họ đăng nhập, nhưng không có thay đổi nào được lưu lại khi họ rời hệ thống. Hồ sơ bắt buộc được tải xuống từ máy tính cục bộ mỗi lần người dùng đăng nhập.

- Bạn có thể chỉ định người dùng mặc định bao gồm tất cả hồ sơ người dùng riêng biệt.

Có ba loại người dùng cá nhân: *hồ sơ người dùng cục bộ, hồ sơ người dùng lang thang* và *hồ sơ người dùng bắt buộc*.

### 8.4.3 Hồ sơ người dùng cục bộ

Hồ sơ người dùng cục bộ được tạo tự động lần đầu người dùng đăng nhập vào máy tính. Nó được cất trên ổ cứng cục bộ và bất kỳ sự thay đổi trên hồ sơ cục bộ sẽ được thể hiện trên máy tính đó. Hồ sơ người dùng cục bộ được cập nhật tự động bởi Windows 2000. Thí dụ, mỗi lần người dùng thay đổi trên màn hình, những thay đổi này được lưu giữ để lần đăng nhập tới sẽ được nạp nên giống như lần thoát trước.

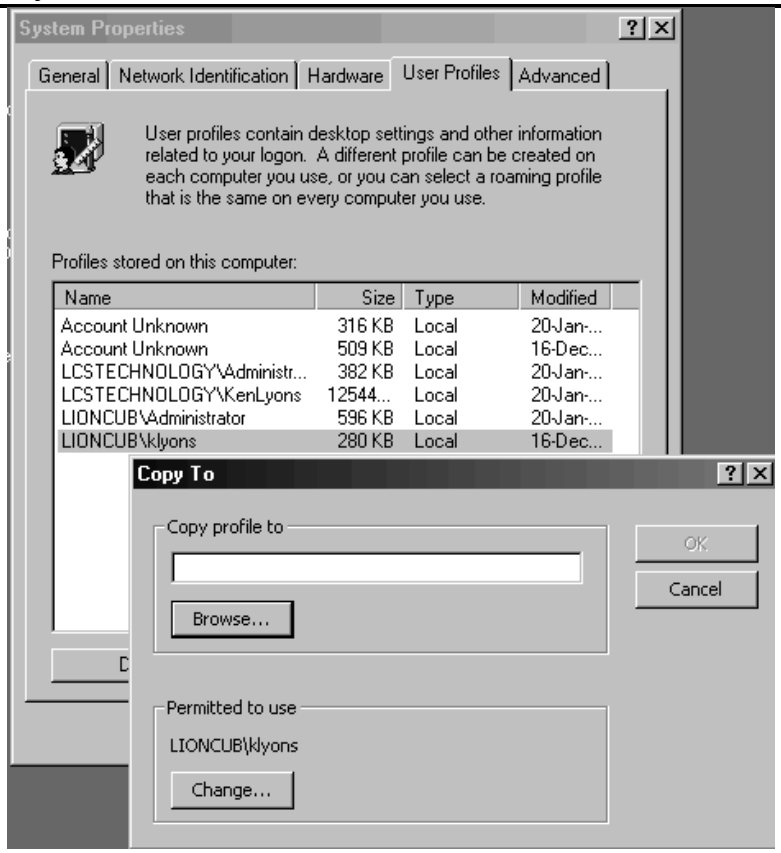
### 8.4.4 Hồ sơ người dùng lang thang (Roaming user profile)

Hồ sơ người dùng lang thang được tạo bởi người quản trị hệ thống và được cất trên máy chủ. Hồ sơ này có hiệu lực mỗi lần người dùng đăng nhập vào mạng ở bất kỳ máy tính nào. Mọi sự thay đổi trên màn hình của người dùng được cập nhật trên máy chủ và được bảo trì tự động. Sự khác nhau giữa hồ sơ cục bộ và lang thang chỉ là nơi lưu trữ. Hồ sơ lang thang được cất trên thư mục chia sẻ trong máy chủ để họ có thể truy cập từ bất kỳ máy nào trên mạng.

Lần đầu người dùng đăng nhập vào mạng, Windows 2000 sao chép tất cả các tài liệu của người dùng tới máy tính cục bộ. Từ thời gian này, khi người dùng đăng nhập tới máy tính, Windows 2000 sẽ so sánh với hồ sơ cất trữ cục bộ và hồ sơ lang thang. Nó chỉ chép lại những file có thay đổi. Việc này làm cho quá trình đăng nhập nhanh hơn.

- **Thiết lập hồ sơ người dùng lang thang**

1. Tạo mẫu hồ sơ người dùng với cấu hình thích hợp. Làm điều này bằng cách tạo tài khoản người dùng qua chương trình Active Directory Users and Computers, sau đó thoát ra và đăng nhập lại như người dùng mới. Cấu hình các thiết lập màn hình thích hợp và sau đó thoát ra khỏi tài khoản người dùng đó và đăng nhập lại như người quản trị.
2. Tạo thư mục dùng chung trên máy chủ, như : *\\server_name\profiles*.
3. Trong hộp thoại Properties của người dùng trên trang Profile, cung cấp đường dẫn tới thư mục dùng chung trong hộp Profile Path. (Sử dụng một đường dẫn Qui ước đặt tên chung (Universal Naming Convention - UNC) như là: *\\server_name\shared_folder_name\logon_name*).
   Bạn có thể gõ biến **%username%** thay vì tên đăng nhập. Khi người dùng sử dụng biến này, Windows 2000 tự động thay thế biến với tên tài khoản người dùng cho hồ sơ lang thang, nó hữu ích khi sao chép các tài khoản mẫu.
4. Sao chép mẫu hồ sơ người dùng tới thư mục dùng chung trên máy chủ và chỉ định những người dùng được phép sử dụng hồ sơ trong trang hồ sơ người dùng trong hộp thoại System Properties của Control Panel .




## 8.4.5 Hồ sơ người dùng bắt buộc (Mandatory user profile)

Hồ sơ người dùng bắt buộc là một loại hồ sơ lang thang đặc biệt chỉ đọc mà có thể thiết lập các chỉ định cá nhân đặc biệt hoặc gom nhóm người dùng. Chỉ những người quản trị hệ thống mới có thể thay đổi các hồ sơ bắt buộc. Hồ sơ bắt buộc được tải xuống máy người dùng mỗi lần người dùng đăng nhập vào mạng. Người dùng có thể thay đổi cấu hình màn hình của họ, nhưng khi thoát ra thì những thay đổi đó sẽ mất. Loại hồ sơ này không cập nhật.

Có một file ẩn trong hồ sơ này (*\\server_name\share\user_logon_name*) gọi là NTUSER.DAT, nó chứa các thiết lập hệ thống Windows 2000 áp dụng cho tài khoản người dùng cá nhân. File này cũng chứa các thiết lập môi trường người dùng. Bằng cách thay đổi tên của file NTUSER.DAT thành NTUSER.MAN, nó trở thành hồ sơ người dùng chỉ đọc.

## 8.4.5 Những thiết lập được lưu trữ trong hồ sơ người dùng

Bảng sau mô tả các thiết lập được lưu trữ trong hồ sơ người dùng. Các thiết lập này xác định môi trường màn hình của người dùng. Hồ sơ cục bộ được lưu trong thư mục *C:\Documents and Settings\user_logon_name*, ở đây C:\ là tên ổ cứng và *user_logon_name* là tên người dùng đăng ký khi đăng nhập vào hệ thống. Hồ sơ lang thang được lưu trên thư mục chia sẻ của máy chủ.

| Tham số | Nguồn |
|---|---|
| Toàn bộ những thiết lập được định nghĩa bởi user cho Windows Explorer | Windows Explorer |
| Các tài liệu do user lưu trữ | My Documents |
| Các file hình ảnh do user lưu giữ | My Pictures |

| Tham số | Nguồn |
|---|---|
| Các shortcuts cho các vị trí ưa thích trên Internet | Favourites |
| Bất kỳ một ổ đĩa mạng được ánh xạ do user tạo ra | Mapped network drive |
| Các liên kết tới các máy tính khác trên mạng | My Network Places |
| Các mục được lưu trữ trên màn hình Desktop và các Shortcut | Desktop contents |
| Toàn bộ các thiết lập font chữ và màu màn hình máy tính được định nghĩa bởi user. | Screen colours and fonts |
| Những thiết lập cấu hình được định nghĩa bởi user và dữ liệu của ứng dụng | Application data and registry hive |
| Những kết nối máy in mạng | Printer settings |
| Toàn bộ các thiết lập do user thực hiện trong Control Panel | Control Panel |
| Toàn bộ các thiết lập chương trình do user tạo ra ảnh hưởng đến môi trường Window của user, bao gồm Calculator, Clock, Notepad, và Paint | Accessories |
| Các thiết lập chương trình của mỗi user cho các chương trình được viết cho Windows 2000 và được thiết kế để theo dõi các cài đặt chương trình | Windows 2000-based programs |
| Bất kỳ bookmark nào được đặt trong hệ thống Help của Windows 2000 | Online user education bookmarks |

Bảng chứa nội dung của thư mục hồ sơ người dùng điển hình:

| Mục | Mô tả |
|---|---|
| Thư mục Application data * | Dữ liệu chương trình cụ thể, thí dụ từ điển tuỳ biến. Những người bán chương trình quyết định dữ liệu gì được cất trong thư mục hồ sơ người dùng. |
| Thư mục Cookies | Thông tin người dùng và các tham chiếu. |
| Thư mục Desktop | Các mục màn hình nền bao gồm các file, các shortcut, và các thư mục. |
| Thư mục Favourites | Các shortcut tới các vị trí ưa thích trên Internet. |
| Thư mục FrontPageTempDir | Thư mục tạm dùng bởi Microsoft Front Page. |
| Thư mục Local Settings * | Dữ liệu ứng dụng, lịch sử, các file tạm. Dữ liệu ứng dụng đi theo người dùng bằng hồ sơ người dùng lang thang. |
| Thư mục My Documents | Các tài liệu người dùng. |
| Thư mục My Pictures | Các mục ảnh người dùng. |
| Thư mục NetHood * | Shortcut tới các mục My Network Places. |

| Mục | Mô tả |
|---|---|
| Thư mục PrintHood * | Shortcut tới các thư mục máy in. |
| Thư mục Recent * | Shortcut tới các tài liệu và thư mục mới truy cập gần đây nhất. |
| Thư mục SendTo * | Shortcut tới các tài liệu xử lý hữu ích . |
| Thư mục Start Menu | Shortcut tới các mục chương trình. |
| Thư mục Templates | Các mục mẫu người dùng. |
| File NTUSER.DAT * | Lưu giữ những thiết lập đăng ký người dùng. |

### 8.4.6 Các thư mục đích (Home Folders)

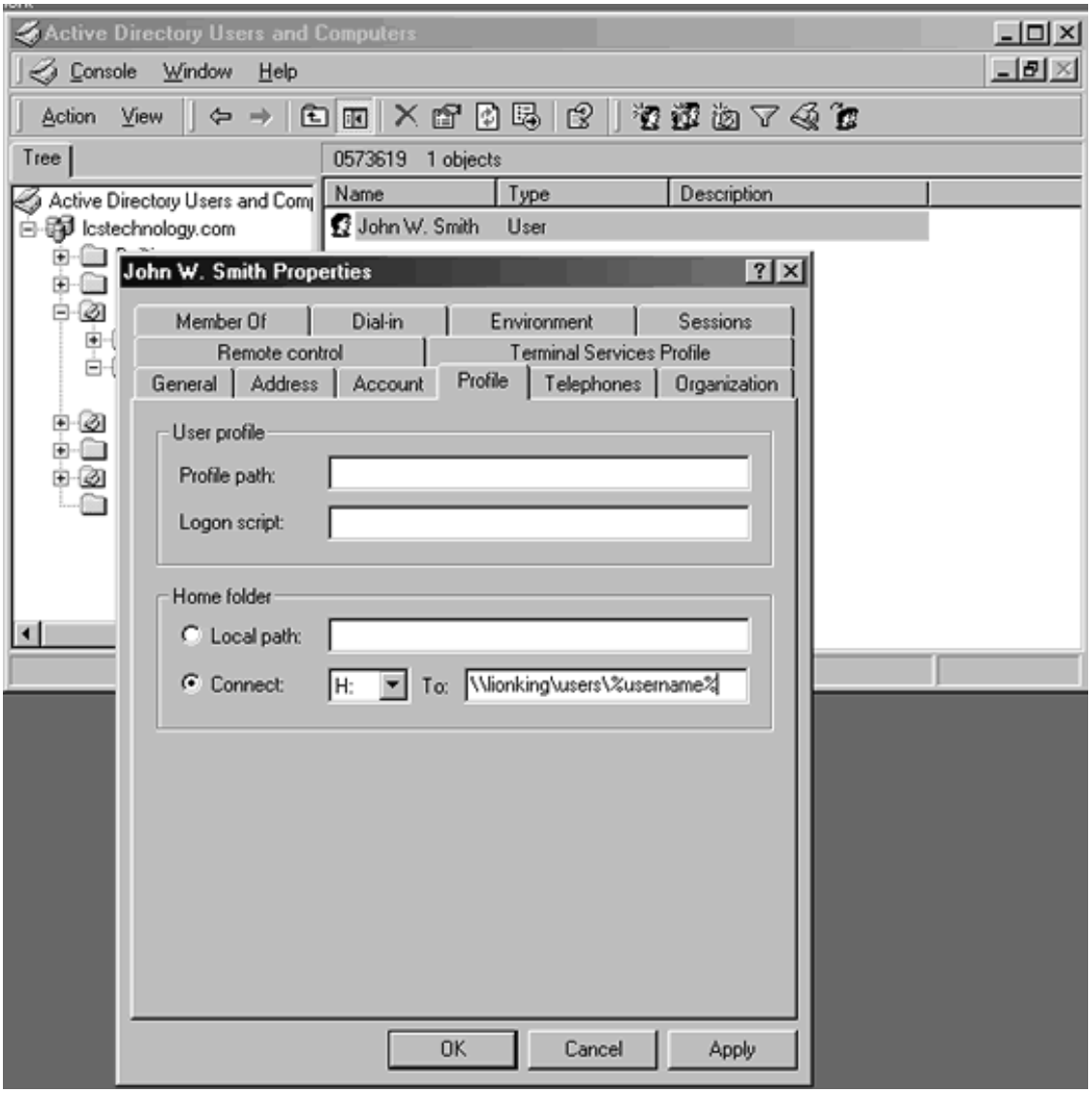
Thư mục đích (home) là thư mục để người dùng lưu giữ tài liệu. Bạn có thể lưu thư mục đích trên máy tính của bạn nhưng phổ biến hơn nó được lưu trên thư mục chia sẻ của máy chủ. Mặc dù các thư mục đích được hiện thực trên bảng Profile của hộp thoại Properties, chúng vẫn không được lưu như là một phần của hồ sơ lang thang. Cho nên, kích thước của thư mục đích không ảnh hưởng đến giao dịch trên mạng trong quá trình đăng nhập bởi vì nó không phải sao chép tới máy cục bộ. Đặt tất cả các thư mục đích trên một vị trí trung tâm của máy chủ làm cho các tác vụ quản trị như back up dữ liệu dễ dàng hơn.

- Ưu điểm của việc để các thư mục đích trên máy chủ
  - Người dùng có thể truy cập vào các thư mục đích từ bất kỳ máy trạm nào trên mạng.
  - Tập trung hoá việc back up và quản trị dữ liệu.
  - Các thư mục đích có thể được truy cập từ các máy chạy trên các hệ điều hành bất kỳ của Microsoft (bao gồm MS-DOS, Windows 95, Windows 98, và Windows 2000).
- Tạo các thư mục đích trên máy chủ

Để tạo thư mục đích cho tài khoản người dùng, bạn phải có quyền quản trị đối tượng mà tài khoản người dùng nhắm tới:

1. Tạo thư mục dùng chung để cất tất cả các thư mục trên máy chủ mạng. Các thư mục người dùng được lưu trên thư mục chia sẻ này.
2. Với thư mục chia sẻ, loại bỏ quyền mặc định Full Control từ nhóm Everyone, gán Full Control tới nhóm Users. (Việc này đảm bảo chỉ những người dùng xác thực với tài khoản người dùng miền mới có thể truy cập tới thư mục dùng chung).
3. Tại hộp thoại Properties của người dùng trong trình đơn Active Directories Users and Computers, chọn bảng Profile và sau đó tạo đường dẫn tới thư mục đích. Vì thư mục đích ở trên máy chủ, nhấn Connect định rõ ổ cứng để người dùng kết nối tới thư mục này. Trong hộp To, chỉ rõ tên UNC (địa chỉ đến một tập tin trong mạng cục bộ) cho thư mục, ví dụ, *\\server_name\shared_folder_ name\user_ logon_name*. Thay vì gõ

tên đăng nhập thực sự của người dùng, bạn gõ biến *%username%*. Hệ thống sẽ tự động tạo thư mục với tên đăng nhập của người dùng và gán các quyền cho người dùng. Thí dụ, gõ ***\\server_name\Users\%username%.***



# Câu hỏi ôn tập chương 8

1. Loại tài khoản nào cho phép người dùng đăng nhập vào Domain để truy cập các tài nguyên mạng?
   a. Local user accounts
   b. Default user accounts
   c. Domain user accounts
   d. Built-in user accounts
2. Loại tài khoản nào cho phép người dùng đăng nhập vào máy tính riêng biệt để truy xuất tài nguyên chỉ trên máy tính đó?
   a. Local user accounts
   b. Default user accounts
   c. Domain user accounts
   d. Built-in user accounts
3. Loại tài khoản nào cho phép người dùng thực hiện các tác vụ quản trị hoặc truy xuất các nguồn tài nguyên mạng ?
   a. Local user accounts
   b. Default user accounts
   c. Domain user accounts
   d. Built-in user accounts
4. Mỗi một Domain Controller định thời tái tạo bản sao tài khoản người dùng mới tới tất cả các Domain Controller khác trong toàn domain.
   a. Đúng
   b. Sai
5. Có hai loại Built-In User Accounts được tạo tự động khi cài đặt Windows 2000 Server là:
   a. Administrator account
   b. Guest account.
   c. User account
6. Trước khi tạo tài khoản người dùng cần xem xét những điều gì dưới đây:
   a. Naming Conventions
   b. Quantity user accounts
   c. Password Requirements
   d. Logon Hours and Workstation Restrictions
   e. User Account Planning Sheet
7. Người sử dụng không thể tự động thay đổi mật khẩu của mình. Chỉ những nhà quản trị mới có thể thay đổi được mật khẩu của người dùng.
   a. Đúng
   b. Sai
8. Người dùng có thể truy cập vào các thư mục đích từ bất kỳ máy trạm nào trên mạng.
   a. Đúng.
   b. Sai.
9. Chỉ những người quản trị hệ thống mới có thể thay đổi các hồ sơ bắt buộc.
   a. Đúng.
   b. Sai.
10. Một trong những ưu điểm của hồ sơ người dùng là cho phép nhiều người cùng sử dụng chung một máy tính, và khi họ đăng nhập vào mạng thì màn hình của họ được thiết lập giống như máy tính cá nhân của họ trong lần đăng nhập trước.
    a. Đúng
    b. Sai.

# CHƯƠNG 9 - QUẢN TRỊ TÀI KHOẢN NHÓM

## MỤC TIÊU CỦA CHƯƠNG

*Kết thúc chương này, sinh viên sẽ có thể:*

- Hiểu được cơ chế quản trị tài khoản user thông qua quản trị nhóm
- Nắm được các loại nhóm trong Windows 2000
- Biết cách lập kế hoạch tạo nhóm
- Nắm được các bước tạo, xoá và thêm các thành viên vào nhóm

## 9.1. Các loại nhóm trong Windows 2000

Nhóm bao gồm nhiều thành viên. Nhóm được dùng trong windows 2000 để đơn giản cho công việc quản trị mạng và dùng để gán quyền sử dụng cho một số tài nguyên trên mạng.

### 9.1.1 Các dạng nhóm (Type group)

Trong windows 2000, chia ra làm 2 dạng nhóm: *Nhóm Security* và *nhóm Distribution*. Cả hai dạng nhóm này đều được lưu trữ trên Active Directory nên chúng có thể truy cập từ bất kỳ nơi đâu trên hệ thống.

*Nhóm Security*: hệ thống windows 2000 chỉ sử dụng nhóm Security để cấp các quyền sử dụng tài nguyên trên hệ thống. Nhóm Security cũng có những đặc tính như nhóm Distribution.

*Nhóm Distribution*: dùng cho những mục đích không có tính bảo mật như gởi thông tin. Ta có thể đưa các thành viên vào trong một nhóm sau đó gởi thông tin đến nhóm này thì tất cả các thành viên đều nhận được thông tin .

### 9.1.2 Phạm vi của nhóm (Group Scopes)

Có 3 dạng: nhóm *Global* – nhóm *Domain Local* – nhóm *Universal*

*Nhóm Global*: chỉ bao gồm các thành viên trên một domain mà tạo ra nhóm này. Nó có thể truy cập vào bất kỳ tài nguyên nào trên các domain khác nhau thuộc cây domain hay rừng domain

*Nhóm Domain Local*: khác với nhóm Global, nhóm Domain Local có thể bao gồm nhiều thành viên trên các domain khác nhau, tuy nhiên chúng được tạo ra để truy cập vào các tài nguyên trên cùng domain nào mà tạo ra nhóm này.

*Nhóm Universal*: là sự kết hợp của nhóm Global và nhóm Domain Local, tuy nhiên chỉ hổ trợ cho những hệ thống mà chỉ toàn là Windows 2000 trở lên (Native mode)

### 9.1.3 Local Group

Nhóm Local được tạo trên các trạm làm việc sử dụng Windows 2000 hay trên các server thành viên của một mạng máy tính. Nhóm Local có đặc điểm sau:

- Chỉ chứa các tài khoản user trên máy tính trên đó nhóm Local được tạo ra.
- Không thể chứa các nhóm khác.

## 9.2. Lập kế hoạch nhóm Local Domain và nhóm Global

Một vấn đề quan trọng trong việc quản trị các nhóm là lập kế hoạch cho các nhóm trên. Sau đây là một số gợi ý.

- Gán tất cả các thành viên có chung một công việc vào Global group. Ví dụ tạo ra một nhóm có tên PGKETOAN và đưa tất cả các thành viên trong phòng này vào nhóm trên.

- Tạo Domain Local Group đối với các tài nguyên dùng chung trên hệ thống. Việc định dạng ra các tài nguyên dùng chung trên hệ thống để các thành viên có thể truy cập tới và tạo ra các Domain Local Group cho các tài nguyên này. Ví dụ như nếu công ty có một máy in màu, tạo ra domain local group có tên là PRINTCOLOR.

- Đưa tất cả các Global Group nào cần truy cập tài nguyên vào domain local group. Ví dụ đưa Global Group PGKETOAN vào trong domain local group PRINTCOLOR.

- Gán quyền truy cập tài nguyên vào domain local group. Ví dụ gán quyền truy cập máy in màu vào nhóm PRINTCOLOR để mọi thành viên có thể dùng máy in.

## 9.3. Tạo và xoá các nhóm

### 9.3.1 Tạo nhóm

Chọn Start → Programs → Administrative Tools → Active Directory users and computers (Hình 9.1)

Chọn tên domain → Users Container → new → Group (Hình 9.2)

Điền vào một số thông tin trong cửa sổ New Group như : tên nhóm, dạng nhóm, phạm vi của nhóm.

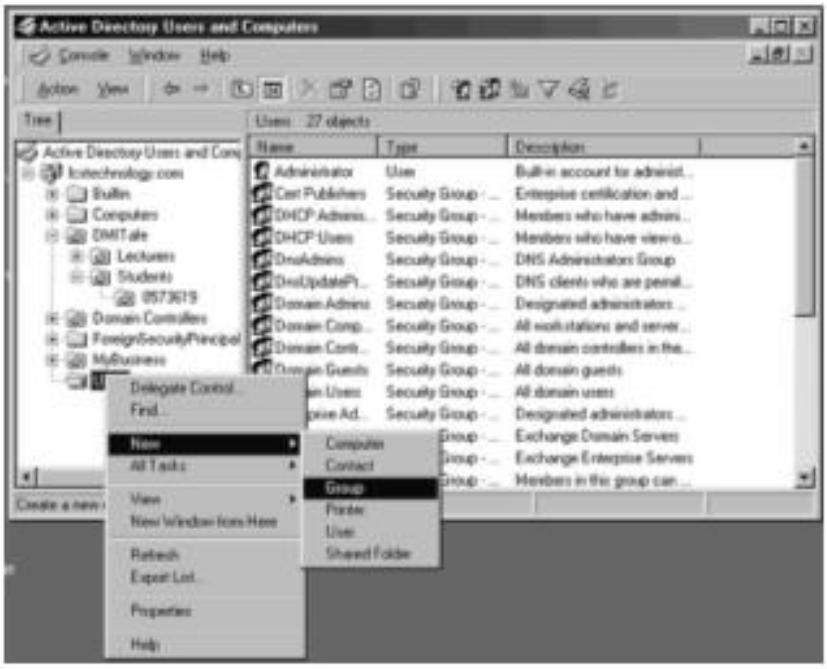
### 9.3.2 Xóa nhóm

Mỗi nhóm tạo ra đều có một SID (security Identifier), windows 2000 dùng SID để gán quyền cho các đối tượng.

Khi xóa nhóm thì các thành viên trong nhóm không bị xóa và tất cả các tài nguyên liên kết với nó cũng bị xóa theo

Để xóa nhóm, đơn giản chọn tên nhóm, nhấn chuột phải → delete

*Hình 9.1* Cách chọn Active Directory Service




*Hình 9.2* Cách chọn Group trong Active Directory

## 9.4. Thêm các thành viên vào nhóm

### 9.4.1 Built-in Group

Trong windows 2000 có một số các nhóm được tạo sẵn sau khi cài đặt xong. Đối với Windows NT 4.0 bao gồm các nhóm : Built-In Local, Built-in Global, System. Trong Windows 2000, các nhóm này được mở rộng và chia ra làm 4 nhóm: Predefine, Local, Global và Special Identifier .

- Nhóm định nghĩa trước (Predefined Group)

Nhóm này có phạm vi toàn cục, thường dùng để gom những tài khỏan người dùng có tính chất giống nhau. Theo mặc định Windows 2000 sẽ tự động đưa các thành viên vào một trong các nhóm thuộc Predefined Global. Người quản trị có thể đưa thêm một số thành viên vào Predefine Global, để thực hiện chế độ phân quyền cho các thành viên này.

Khi hệ thống là một domain, Windows 2000 sẽ tạo ra nhóm Predefined Global trong thư mục USERS trong Active Directory, các nhóm Predefined này không có quyền thừa kế, các nhóm này có quyền bằng cách đưa nhóm Global vào trong nhóm Domain Local hoặc có thể gán quyền trực tiếp trên chúng.

Sau đây là một số nhóm Prdefined Global

| **Predefined Global Group** | **Mô tả** |
|---|---|
| Domain Admins | Windows 2000 tự động đưa Domain Admins vào trong nhóm Domain Local có sẵn với tên là Administrators sao cho các thành viên trong Domain Admins có thể thực hiện công việc quản trị mạng trên hệ thống. Mặc định, người Administrator sẽ là thành viên thuộc nhóm này |
| Domain Guests | Windows 2000 tự động đưa Domain Guests vào nhóm Domain Local có sẵn với tên là Guests. Mặc định tài khoản Guest là thành viên thuộc nhóm này. |
| Domain Users | Windows 2000 tự động đưa Domain Users vào nhóm tự có Domain Local có tên Users. Mặc định, các tài khoản người dùng Administrator, Guest IUSR_*computername*, IWAM_ *computername*, Krbtgt, và TsInternet là những thành viên thuộc nhóm này. |
| Enterprise Admins | Người quản trị có thể đưa các thành viên vào nhóm Enterprise Admins để các thành viên này có quyền giám sát hệ thống. Sau đó đưa Enterprise Admins vào nhóm Domain Local có tên Administrators trong mỗi domain. Mặc định, người Administrator sẽ là thành viên thuộc nhóm này. |

- Các nhóm có sẵn (Built-in Groups)

Nếu như các nhóm Predefined có phạm vi toàn cục, thì các nhóm Built-in do Windows 2000 tạo ra có phạm vi cục bộ miền. Windows 2000 sẽ tạo ra nhóm Built-in Global trong thư mục BuiltIn trong Active Directory, các nhóm này có quyền trên toàn domain và trong Active Direcoty. Chúng có các quyền của nhóm Prdefined.

Sau đây là một số nhóm có sẵn (Built-in Groups)

| **Built-in Group** | **Mô tả** |
|---|---|
| Account Operators | Các thành viên có thể tạo, xóa, thay đổi các tài khỏan người dùng và các nhóm, tuy nhiên không thể thay đổi nhóm Administrators hay bất kỳ nhóm operators nào. |
| Administrators | Các thành viên có thể thực hiện tất cả các công việc quản trị trên tất cả Domain Controllers và chính trên domain đó. Mặc định, tài khoản Administrator và các nhóm toàn cục định nghĩa trước Domain Admins và Enterprise Admins là các thành viên. |
| Backup Operators | Các thành viên có thể thực hiện viêc lưu trữ (backup) và phục hồi trên Domain Controllers dùng Windows Backup. |
| Guests | Các thành viên chỉ có thể truy cập vào những tài nguyên cho phép; các thành viên không có quyền thay đổi các cài đặt về môi trường làm việc. Mặc định, các tài khoản user Guest, IUSR_*computername*, IWAM_*computername*, và TsInternet và nhóm toàn cục định nghĩa trước Domain Guests là các thành viên thuộc nhóm này. |
| Pre-Windows 2000 Compatible Access | Cho phép các thành viên có quyền đọc trong domain. Mặc định, chỉ có nhóm hệ thống Everyone pre-Windows 2000 là thành viên |
| Print Operators | Các thành viên có thể cài đặt và quản lý máy in trên mạng. |
| Replicator | Hổ trợ Chức năng nhân bản thư mục. |
| Server Operators | Các thành viên có thể chia xẻ các tài nguyên trên đĩa, lưu trữ, phục hồi các file trên một domain controller. |
| Users | Các thành viên có thể truy cập vào các tài nguyên của mình. Mặc định, các nhóm Authenticated Users và INTERACTIVE pre-Windows 2000 và nhóm toàn cục định nghĩa trước Domain Users là những thành viên của nhóm này. |

- Built-in Local Group

Trong tất cả các máy chạy Windows 2000 dù là server hay professional đều có nhóm Buitl-in Local. Chúng chỉ cho phép tất cả các thành viên trong nhóm này sử dụng tài nguyên trên chính máy đó, Các nhóm này được tạo trong thư mục Groups trong công cụ Local User Manager. Trên các máy domain controller không tồn tại nhóm Local và nhóm Built-in Local. Sau đây là các nhóm Built-in Local:

| Group | Mô tả |
|---|---|
| Administrators | Các thành viên có thể thực hiên công việc quản trị mạng trên máy tính này .Mặc định, Administrator là thành viên của nhóm. Khi có một server thành viên hoặc máy tính chạy Windows 2000 gia nhập vào một domain, Windows 2000 sẽ đưa nhóm toàn cục định nghĩa trước Domain Admins vào nhóm Administrators cục bộ. |
| Backup Operators | Các thành viên nhóm này có thể dùng Windows Backup để lưu trữ và phục hồi dữ liệu trên máy.. |
| Guests | Các thành viên chỉ có thể truy cập vào những tài nguyên cho phép; các thành viên không có quyền thay đổi các cài đặt về môi trường làm việc. Mặc định, Guest là thành viên. Khi có một server thành viên hoặc máy tính chạy Windows 2000 gia nhập vào một domain, Windows 2000 sẽ đưa nhóm toàn cục định nghĩa trước Domain Guests vào nhóm Guests cục bộ. |
| Power Users | Các thành viên có thể tạo và thay đổi các tài khoản user cục bộ trên máy tính cục bộ và chia xẻ các tài nguyên trên máy tính đó. |
| Replicator | Hổ trợ chức năng nhân bản thư mục. |
| Users | Các thành viên có thể truy cập vào các tài nguyên của mình. Mặc định, Windows 2000 sẽ đưa các tài khoản cục bộ được tạo ra trên máy vào trong nhóm Users . Khi có một server thành viên hoặc máy tính chạy Windows 2000 gia nhập vào một domain, Windows 2000 sẽ đưa nhóm nhóm toàn cục định nghĩa trước Domain Users vào nhóm Users cục bộ. |

- Nhóm định danh đặc biệt (Special Identifier Groups)

Mỗi máy tính chạy windows 2000 đều có các nhóm Special Identifier hay còn gọi các nhóm System.

Sau đây là các nhóm Special Identifier:

| Group | Mô tả |
|---|---|
| Anonymous Logon | Bao gồm bất kỳ tài khỏan người dùng mà Windows 2000 không xác nhận |
| Authenticated Users | Bao gồm tất cả tài khoản người dùng hợp lệ có tạo ra trong máy hay trong Active Directory. Dùng nhóm này để ngăn chặn quyền truy xuất bất hợp pháp của người dùng. |
| CREATOR OWNER | Bao gồm những người cho phép tạo ra các files hay thư mục. Nếu một thành viên thuộc nhóm Administrators tạo ra một tài nguyên nào đó thì tài nguyên đó thuộc quyền Administrators |
| Dialup | Bao gồm bất kỳ ai có thể kết nối vào mạng qua modem. |
| Everyone | Bao gồm tất cả mọi người đang truy cập vào máy tính. Theo mặc định nhóm này được gán quyền Full Control, do đó bất kỳ người nào cũng có toàn quyền trên bất kỳ tài nguyên nào của hệ thống. |
| Interactive | Bao gồm các tài khỏan cho phép người dùng có thể kết nối vào hệ thống. Các thành viên của nhóm này có thể truy cập vào bất kỳ máy nào tại bất kỳ nơi đâu. |
| Network | Bao gồm bất kỳ người nào có thể kết nối vào mạng để truy cập tài nguyên . |

# Câu hỏi ôn tập chương 9

1. Có ba phạm vi cho các nhóm được tạo ra trong domain là:

   a. Global groups b. Local groups
   c. Domain local groups d. Universal groups

2. Tên các nhóm có sẵn (built-in group) trong Windows 2000 là ..... (chọn 3)

   a. Users b. Administrators
   c. System d. Guests

3. Nhóm tài khoản nào mà Administrator có thể xoá trong các nhóm tài khoản sau:

   a. Users b. Guests
   c. Bult-in groups d. Created groups by the Administrator

4. Các nhóm nào trong các nhóm sau có thể chứa một số các tài khoản user từ một domain được nhóm lại với nhau.

   a. Global groups b. Local groups
   c. Domain local groups d. Universal groups

5. Những nhóm nào trong các nhóm sau đây được sử dụng để gán các quyền tới các tài nguyên.

   a. Global groups b. Local groups
   c. Domain local groups d. Universal groups

6. Những nhóm nào trong các nhóm sau đây được sử dụng để gán các quyền tới các tài nguyên liên quan trong nhiều domain.

   a. Global groups b. Local groups
   c. Domain local groups d. Universal group

# TÀI LIỆU THAM KHẢO

[1] DMIT – Network Maintenance Text Book, 2000
[2] MCSE Training Kit - Microsoft Windows 2000 Server / Microsoft Corporation. Microsoft Press, 2000.
[3] MCSE Training Kit – Networking Essentials Plus, 3rd ed. Microsoft press, 1999.
[4] Nguyễn Thúc Hải - Mạng máy tính và các hệ thống mở, Nhà xuất bản giáo dục, Hà nội, 1997.

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

- - - - - - - 🕮 - - - - - - -

SÁCH HƯỚNG DẪN HỌC TẬP

# MẠNG MÁY TÍNH

**Biên soạn : Ts. PHẠM THẾ QUẾ**

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
Km10 Đường Nguyễn Trãi, Hà Đông, Hà Tây
Tel: (04) 5541221, Fax: (04) 5540587
Website: http://www.ptit.edu.vn, e-mail: dhtx@ptit.edu.vn
CHƯƠNG TRÌNH PTIT ĐÀO TẠO ĐẠI HỌC TỪ XA

Lưu hành nội bộ

**HÀ NỘI - 2006**

# MỞ ĐẦU

Tài liệu này phục vụ cho sinh viên hệ đào đại học từ xa học tập và nghiên cứu về "Mạng máy tính".

Tài liệu gồm các nội dung chính sau:

Chương I: Giới thiệu tổng quan về mạng máy tính. Khái niệm cơ bản về kiến trúc và các giao thức mạng, các loại mạng máy tính và mục tiêu ứng dụng của nó.

Chương II: Nghiên cứu các nguyên tắc cơ bản để thiết kế một mô hình giao thức mạng máy tính theo quan điểm chia các tiến trình truyền thông thành cấu trúc nhiều tầng, được xếp chồng lên nhau để thực hiện một tiến trình truyền thông hoàn chỉnh. Giới thiệu mô hình OSI, được xem như là một mô hình chuẩn, một chiến lược phát triển các hệ thống mở và một khung khái niệm về giao thức và dịch vụ.

Chương III*:* Giới thiệu một số bộ giao thức mạng mang tính đặc trưng và được áp dụng phổ biến. Đặc biệt trong chương này tìm hiểu sâu hơn bộ giao thức TCP/IP đã trở thành chuẩn chung cho mạng máy tính toàn cầu, mạng Internet.

Chương IV: Chương này giới thiệu các công nghệ mạng cục bộ. Kiến trúc mạng cục bộ Ethrnet, Virtual LAN, Local ATM , LAN ARCnet..

Chương V: Giới thiệu về công nghệ và kỹ thuật mạng diện rộng WAN. Cụ thể xem xét công nghệ các mạng tích hợp số đa dịch vụ ISDN và băng rộng B-ISDN, Frame Relay và X25, dịch vụ SDMS và phương thức truyền dẫn không đồng bộ ATM.

Chương VI: Giới thiệu một số công nghệ mới như công nghệ đường dây thuê bao số DSL, các mạng chuyển mạch gói chuyển tải tiếng nói trên nền IP, ATM và Frame Raly. Các công nghệ chuyển mạch nhãn đa giao thức IP/MPLS, chuyển mạch mềm Softswitch sử dụng trong mạng hội tụ và mạng thế hệ sau NGN.

Chương VII: Đề cập đến một số vấn đề bảo vệ thông tin trên mạng. Chương này giới thiệu cách tiếp cận các hệ mật mã, các giao thức bảo mật, mạng riêng ảo VPN và các giải pháp an toàn mạng, xác thực điện tử, các giải pháp chữ ký điện tử, xác minh chữ ký và từ chối chữ ký giả mạo..

Tài liệu không chỉ đề cập đến những vấn đề cơ sở lý luận mà còn trình bày một số kỹ năng, kinh nghiệm cần thiết để thiết kế và cài đặt các mạng máy tính. Hy vọng sẽ có ích cho các bạn học sinh sinh viên và những người muốn xây dựng các hệ thống tin học ứng dụng phục vụ cho sản xuất, quản lý trong các doanh nghiệp. Có thể còn nhiều thiếu sót trong trình bày và biên soạn do khả năng, trình độ, nhưng người biên soạn mạnh dạn giới thiệu tài liệu này và mong nhận được sự góp ý của bạn đọc.

***TS Phạm Thế Quế***

# CHƯƠNG I: KHÁI NIỆM VỀ MẠNG MÁY TÍNH

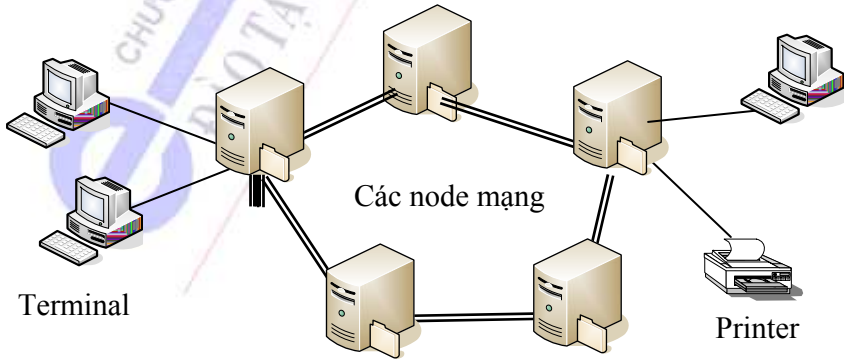
Nội dung của chương sẽ trình bày các khái niệm cơ bản của mạng máy tính, định nghĩa mạng máy tính, mục tiêu và ứng dụng của mạng, cấu trúc và các thành phần cơ bản của một mạng máy tính. Các thực thể trên mạng có thể tham gia truyền thông với nhau cần tuân theo tập các phần mềm điều khiển hoạt động của mạng, được gọi là chuẩn, hay còn gọi là tập các giao thức mạng (Protocols). Nội dung của chương bao gồm các phần sau:

- Định nghĩa mạng máy tính
- Mục tiêu mạng máy tính.
- Các dịch vụ mạng.
- Cấu trúc mạng (Topology)
- Khái niệm giao thức mạng máy tính (Protocols)
- Mạng LAN, MAN, WAN.
- Mạng chuyển mạch kênh (Circuit switched Networks)
- Mạng chuyển mạch gói (Packet Switched Networks).
- Các mô hình xử lý dữ liệu

## 1.1. Định nghĩa mạng máy tính

Mạng máy tính là tập hợp các máy tính đơn lẻ được kết nối với nhau bằng các phương tiện truyền vật lý (Transmission Medium) và theo một kiến trúc mạng xác định (Network Architecture).

Mạng viễn thông cũng là mạng máy tính. Các node chuyển mạch là hệ thống máy tính được kết nối với nhau bằng các đường truyền dẫn và hoạt động truyền thông tuân theo các chuẩn mô hình tham chiếu OSI. Hình 1.2 mô tả khái quát các thành phần của định nghĩa.




**Hình 1.1 Mạng máy tính**

*Kiến trúc mạng* gồm cấu trúc mạng (Topology) và giao thức mạng (Protocols). Topology là cấu trúc hình học của các thực thể mạng và giao thức mạng là tập các quy tắc chuẩn các thực thể hoạt động truyền thông phải tuân theo.

## 1.2. Mục tiêu mạng máy tính

### 1.2.1. Mục tiêu kết nối mạng máy tính

- 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.

### 1.2.2. Lợi ích kết nối mạng

- Có thể giảm số lượng máy in, đĩa cứng và các thiết bị khác. Kinh tế trong việc đầu tư xây dựng cho một hệ thống tin học của một cơ quan, xí nghiệp, doanh nghiệp...

- Dùng chung tài nguyên đắt tiền như máy in, phần mềm...Tránh dư thừa dữ liệu, tài nguyên mạng. Có khả năng tổ chức và triển khai các đề án lớn thuận lợi và dễ dàng.

- Bảo đảm các tiêu chuẩn thống nhất về tính bảo mật, an toàn dữ liệu khi nhiều người sử dụng tại các thiết bị đầu cuối khác nhau cùng làm việc trên các hệ cơ sở dữ liệu.

**Tóm lại,** mục tiêu kết nối các máy tính thành mạng là cung cấp các dịch vụ mạng đa dạng, chia sẻ tài nguyên chung và giảm bớt các chi phí về đầu tư trang thiết bị.

## 1.3. Các dịch vụ mạng

### 1.3.1. 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.....

### 1.3.2. 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. Tìm kiếm thông tin và điều khiển truy nhập. Dịch vụ thư điện tử E_Mail (Electronic mail) cung cấp cho người sử dụng phương tiện trao đổi, tranh luận bằng thư điện tử. Dịch vụ thư điện tử giá thành hạ, chuyển phát nhanh, an toàn và nội dung có thể tích hợp các loại dữ liệu.

- Dịch vụ in ấn: Có thể dùng chung các máy in đắt tiền trên mạng. Cung cấp khả năng đa truy nhập đến máy in, phục vụ đồng thời cho nhiều nhu cầu in khác nhau. Cung cấp các dịch vụ FAX và quản lý được các trang thiết bị in chuyên dụng.

- Các dịch vụ ứng dụng hướng đối tượng: Sử dụng các dịch vụ thông điệp (Message) làm trung gian tác động đến các đối tượng truyền thông. Đối tượng chỉ bàn giao dữ liệu cho tác nhân (Agent) và tác nhân sẽ bàn giao dữ liệu cho đối tượng đích.

- Các dịch vụ ứng dụng quản trị luồng công việc trong nhóm làm việc: Định tuyến các tài liệu điện tử giữa những người trong nhóm. Khi chữ ký điện tử được xác nhận trong các phiên giao dịch thì có thể thay thế được nhiều tiến trình mới hiệu quả và nhanh chóng hơn.

- Dịch vụ cơ sở dữ liệu là dịch vụ phổ biến về các dịch vụ ứng dụng, là các ứng dụng theo mô hình Client/Server. Dịch vụ xử lý phân tán lưu trữ dữ liệu phân tán trên mạng, người dùng trong suốt và dễ sử dụng, đáp ứng các nhu cầu truy nhập của người sử dụng.

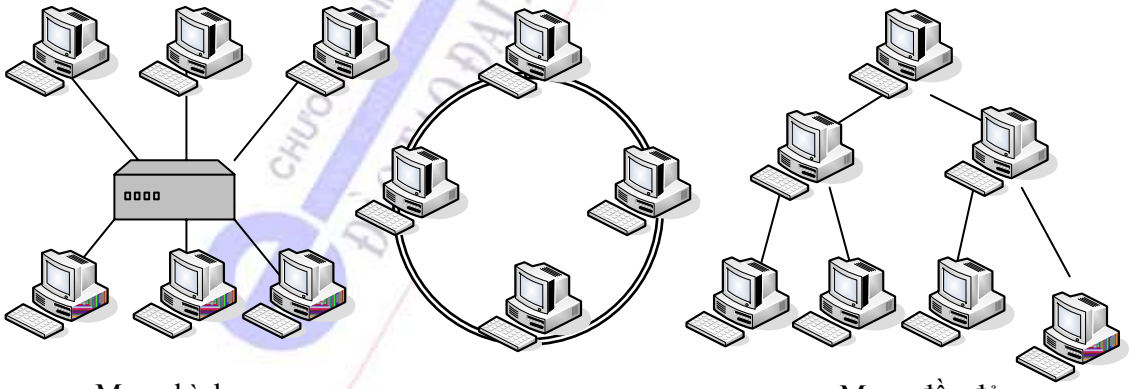
## 1.4. Cấu trúc mạng (Topology)

Topology là cấu trúc hình học không gian của mạng thực chất là cách bố trí vị trí vật lý các node và cách thức kết nối chúng lại với nhau. Có hai kiểu cấu trúc mạng: kiểu điểm - điểm (Point to Point) và kiểu quảng bá (Multi Point).

### 1.4.1. Kiểu điểm - điểm (Point to Point)

Đường truyền nối từng cặp node lại với nhau theo một hình học xác định. Một kênh truyền vật lý sẽ được thiết lập giữa 2 node có nhu cầu trao đổi thông tin. Chức năng các node trung gian: tiếp nhận, lưu trữ tạm thời và gửi tiếp thông tin sang node tiếp theo khi đường truyền rỗi. Cấu trúc điểm- điểm gọi là mạng lưu và gửi tiếp (Store - and - Forward).

Ưu điểm là ít khả năng đụng độ thông tin (Collision). Nhược điểm của nó là hiệu suất sử dụng đường truyền thấp. Chiếm dụng nhiều tài nguyên, độ trễ lớn, tiêu tốn nhiều thời gian để thiết lập đường truyền và xử lý tại các node. Vì vậy tốc độ trao đổi thông tin thấp.



Mạng hình sao (Star) | Mạng chu trình (Loop) | Mạng đầy đủ (Complete)

**Hình 1.2 Các mạng có cấu trúc điểm - điểm**

### 1.4.2. Kiểu đa điểm hay quảng bá (Point to Multipoint, Broadcasting)

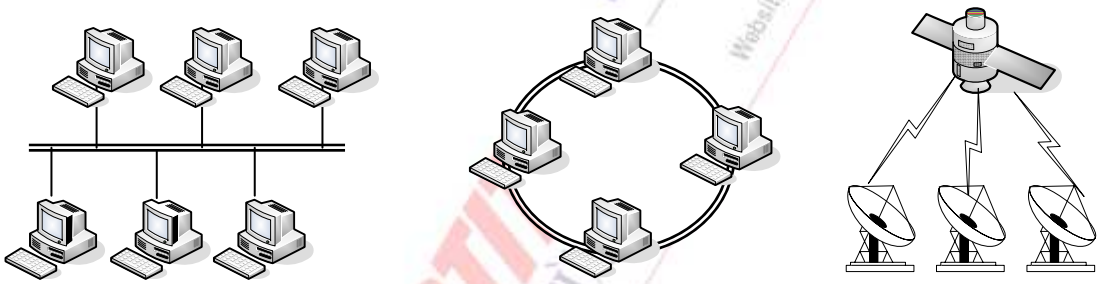
Tất cả các node cùng truy nhập chung trên một đường truyền vật lý. Một thông điệp được truyền đi từ một node nào đó sẽ được tất cả các node còn lại tiếp nhận và kiểm tra địa chỉ đích trong thông điệp có phải của nó hay không. Cần thiết phải có cơ chế để giải quyết vấn đề đụng độ thông tin (Collision) hay tắc nghẽn thông tin trên đường truyền trong các mạng hình BUS và hình RING.

Các mạng có cấu trúc quảng bá được phân chia thành hai loại: quảng bá tĩnh và quảng bá động phụ thuộc vào việc cấp phát đường truyền cho các node. Trong quảng bá động có quảng bá động tập trung và quảng bá động phân tán.

*Quảng bá tĩnh:* Chia thời gian thành nhiều khoảng rời rạc và dùng cơ chế quay vòng (Round Robin) để cấp phát đường truyền. Các node có quyền được truy nhập khi đến cửa thời gian của nó.

*Quảng bá động tập trung*: Một thiết bị trung gian có chức năng tiếp nhận yêu cầu liên lạc và cấp phát đường truyền cho các node. Kiểu cấp phát này giảm được tối đa thời gian chết của đường truyền, hiệu suất kênh truyền cao, nhưng thiết kế phức tạp và khó khăn.

*Quảng bá động phân tán*: Không có bộ trung gian, các node tự quyết định có nên hay không nên truy nhập đường truyền, phụ thuộc vào trạng thái của mạng.



Mạng hình BUS | Mạng hình vòng RING | Vệ tinh

**Hình 1.3 Các mạng có cấu trúc quảng bá**

## 1.5. Khái niệm giao thức mạng máy tính (Protocols)

### 1.5.1. 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.

### 1.5.2. Chức năng giao thức

*Đóng gói:* Trong quá trình trao đổi thông tin, các gói dữ liệu được thêm vào một số thông tin điều khiển, bao gồm địa chỉ nguồn và địa chỉ đích, mã phát hiện lỗi, điều khiển giao thức... Việc thêm thông tin điều khiển vào các gói dữ liệu được gọi là quá trình đóng gói (Encapsulation). Bên thu sẽ được thực hiện ngược lại, thông tin điều khiển sẽ được gỡ bỏ khi gói tin được chuyển từ tầng dưới lên tầng trên.

*Phân đoạn và hợp lại:* Mạng truyền thông chỉ chấp nhận kích thước các gói dữ liệu cố định. Các giao thức ở các tầng thấp cần phải cắt dữ liệu thành những gói có kích thước quy định. Quá trình này gọi là quá trình phân đoạn. Ngược với quá trình phân đoạn bên phát là quá trình hợp lại bên thu. Dữ liệu phân đoạn cần phải được hợp lại thành thông điệp thích hợp ở tầng ứng dụng (Application). Vì vậy vấn đề đảm bảo thứ tự các gói đến đích là rất quan trọng. Gói dữ liệu trao đổi giữa hai thực thể qua giao thức gọi là đơn vị giao thức dữ liệu PDU (Protocol Data Unit).

*Điều khiển liên kết:* Trao đổi thông tin giữa các thực thể có thể thực hiện theo hai phương thức: hướng liên kết (Connection - Oriented) và không liên kết (Connectionless). Truyền không liên kết không yêu cầu có độ tin cậy cao, không yêu cầu chất lượng dịch vụ và không yêu cầu xác nhận. Ngược lại, truyền theo phương thức hướng liên kết, yêu cầu có độ tin cậy cao, đảm bảo chất lượng dịch vụ và có xác nhận. Trước khi hai thực thể trao đổi thông tin với nhau, giữa chúng một kết nối được thiết lập và sau khi trao đổi xong, kết nối này sẽ được giải phóng.

G*iám sát*: Các gói tin PDU có thể lưu chuyển độc lập theo các con đường khác nhau, khi đến đích có thể không theo thứ tự như khi phát. Trong phương thức hướng liên kết, các gói tin phải được yêu cầu giám sát. Mỗi một PDU có một mã tập hợp duy nhất và được đăng ký theo tuần tự. Các thực thể nhận sẽ khôi phục thứ tự các gói tin như thứ tự bên phát.

*Điều khiển lưu lượng* liên quan đến khả năng tiếp nhận các gói tin của thực thể bên thu và số lượng hoặc tốc độ của dữ liệu được truyền bởi thực thể bên phát sao cho bên thu không bị tràn ngập, đảm bảo tốc độ cao nhất. Một dạng đơn giản của của điều khiển lưu lượng là thủ tục dừng và đợi (Stop-and Wait), trong đó mỗi PDU đã phát cần phải được xác nhận trước khi truyền gói tin tiếp theo. Có độ tin cậy cao khi truyền một số lượng nhất định dữ liệu mà không cần xác nhận. Kỹ thuật cửa sổ trượt là thí dụ cơ chế này. Điều khiển lưu lượng là một chức năng quan trọng cần phải được thực hiện trong một số giao thức.

*Điều khiển lỗ*i là kỹ thuật cần thiết nhằm bảo vệ dữ liệu không bị mất hoặc bị hỏng trong quá trình trao đổi thông tin. Phát hiện và sửa lỗi bao gồm việc phát hiện lỗi trên cơ sở kiểm tra khung và truyền lại các PDU khi có lỗi. Nếu một thực thể nhận xác nhận PDU lỗi, thông thường gói tin đó sẽ phải được phát lại.

*Đồng bộ hoá:* Các thực thể giao thức có các tham số về các biến trạng thái và định nghĩa trạng thái, đó là các tham số về kích thước cửa sổ, tham số liên kết và giá trị thời gian. Hai thực thể truyền thông trong giao thức cần phải đồng thời trong cùng một trạng thái xác định. Ví dụ cùng trạng thái khởi tạo, điểm kiểm tra và huỷ bỏ, được gọi là đồng bộ hoá. Đồng bộ hoá sẽ khó khăn nếu một thực thể chỉ xác định được trạng thái của thực thể khác khi nhận các gói tin. Các gói

tin không đến ngay mà phải mất một khoảng thời gian để lưu chuyển từ nguồn đến đích và các gói tin PDU cũng có thể bị thất lạc trong quá trình truyền.

*Địa chỉ hoá:* Hai thực thể có thể truyền thông được với nhau, cần phải nhận dạng được nhau. Trong mạng quảng bá, các thực thể phải nhận dạng định danh của nó trong gói tin. Trong các mạng chuyển mạch, mạng cần nhận biết thực thể đích để định tuyến dữ liệu trước khi thiết lập kết nối.

## 1.6. Cáp mạng - phương tiện truyền (Network Medium)

Phương tiện 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.

### 1.6.1. 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. Ví dụ băng thông của cáp thoại từ 400 đến 4000 Hz, có nghĩa là nó có thể truyền các tín hiệu với tần số từ 400 đến 4000 chu kỳ/giây. Băng thông của cáp phụ thuộc vào chiều dài của cáp. Cáp ngắn băng thông cao và ngược lại. Vì vậy khi thiết kế lắp đặt cáp, chiều dài cáp sao cho không vượt qua giới hạn cho phép, vì có thể xảy ra lỗi trong quá trình truyền.

*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.

### 1.6.2. Các loại cáp mạng

*Cáp đồng trục (Coaxial cable):* Là phương tiện truyền các tín hiệu có phổ rộng và tốc độ cao. Băng thông của cáp đồng trục từ 2,5 Mbps (ARCnet) đến 10 Mbps (Ethernet). Thường sử dụng để lắp đặt mạng hình BUS (các loại mạng LAN cục bộ Thick Ethernet, Thin Ethernet) và mạng hình sao (mạng ARCnet).

Cáp đồng trục gồm: một dây dẫn trung tâm, một dây dẫn ngoài, tạo nên đường ống bao quanh trục, tầng cách điện giữa 2 dây dẫn và cáp vỏ bọc ngoài.

Các loại cáp đồng trục .

- Cáp RC-8 và RCA-11, 50 Ohm dùng cho mạng Thick Ethernet.
- Cáp RC-58 , 50 Ohm dùng cho mạng Thin Ethernet.
- Cáp RG-59 , 75 Ohm dùng cho truyền hình cáp.
- Cáp RC-62, 93 Ohm dùng cho mạng ARCnet.

*Cáp xoắn đôi* (*Twisted Pair cable*): *C*áp xoắn đôi được sử dụng trong các mạng LAN cục bộ. Giá thành rẻ, dễ cài đặt, có vỏ bọc tránh nhiệt độ, độ ẩm và có loại có khả năng chống nhiễu

STP (Shield Twisted Pair). Cáp cơ bản có 2 dây đồng xoắn vào nhau, giảm độ nhạy của cáp với EMI, giảm bức xạ âm nhiễu tần số radio gây nhiễu. Các loại cáp xoắn:

- *Cáp có màng chắn (STP):* Loại cáp STP thường có tốc độ truyền vào khoảng 16 Mbps trong loại mạng Token Ring. Với chiều dài 100 m tốc độ đạt 155 Mbps (lý thuyết là 500 Mbps). Suy hao cho phép khoảng 100 m, đặc tính EMI cao. Giá thành cao hơn cáp Thin Ethernet, cáp xoắn trần, nhưng lại rẻ hơn giá thành loại cáp Thick Ethernet hay cáp sợi quang. Cài đặt đòi hỏi tay nghề và kỹ năng cao.

- *Loại cáp không có vỏ bọc UTP (Unshield Twisted Pair):* Cáp trần không có khả năng chống nhiễu, tốc độ truyền khoảng 100 Mbps. Đặc tính suy hao như cáp đồng, giới hạn độ dài tối đa 100m. Do thiếu màng chắn nên rất nhạy cảm với EMI, không phù hợp với môi trường các nhà máy. Được dùng phổ biến cho các loại mạng, giá thành hạ, dễ lắp đặt.

*Cáp sợi quang (Fiber Optic Cable)* rất lý tưởng cho việc truyền dữ liệu, băng thông có thể đạt 2 Gbps, tránh nhiễu tốt, tốc độ truyền 100 Mbps trên đoạn cáp dài vài km. Cáp sợi quang gồm một hoặc nhiều sợi quang trung tâm được bao bọc bởi một lớp vỏ nhựa phản xạ các tín hiệu trở lại, vì vậy hạn chế sự suy hao, mất mát tín hiệu. Cáp sợi quang chỉ truyền các tín hiệu quang. Các tín hiệu dữ liệu được biến đổi thành các tín hiệu quang trên đường truyền và khi nhận, các tín hiệu quang chuyển thành các tín hiệu dữ liệu. Cáp sợi quang hoạt động một trong hai chế độ: chế độ đơn (Single Mode) và đa chế độ (Multi Mode). Cài đặt cáp sợi quang đòi hỏi phải có kỹ năng cao, quy trình khó và phức tạp.

### 1.6.3. Các phương tiện 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

Đặc tính truyền: tần số đơn, công suất thấp không hỗ trợ tốc độ dữ liệu các mạng cục bộ LAN yêu cầu. Tần số đơn, công suất cao dễ cài đặt, băng thông cao từ 1 - 10 Mbps, suy hao chậm. Khả năng nhiễu từ thấp, bảo mật kém. Giá thành cao trung bình. Radio quang phổ trải (Spread spectrum) độ tin cậy cao, bảo mật dữ liệu. Băng thông cao, tốc độ truyền có thể đạt theo yêu cầu của các mạng cục bộ.

*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. Tín hiệu đến vệ tinh và từ vệ tinh đến trạm thu một lượt đi hoặc về 23.000 dặm. Thời gian truyền một tín hiệu độc lập với khoảng cách. Thời gian truyền tín hiệu từ vệ tinh đến các trạm nằm vòng tròn 1/3 chu vi quả đất là như nhau, gọi là trễ lan truyền (Propagation Delay). Thông thường là 0,5-5 giây.

*Tia hồng ngoại (Infrared system):* Có 2 phương thức kết nối mạng Point - to - Point và Multi Point. Point - to – Point tiếp sóng các tín hiệu hồng ngoại từ thiết bị này sang thiết bị khác.Giải tần từ 100 GHz đến 1000 THz, tốc độ truyền khoảng 100 Kbps-16 Mbps. Multi Point truyền đồng thời các tín hiệu hồng ngoại đến các thiết bị. Giải tần số từ 100 GHz đến 1000 THz, nhưng tốc độ truyền chỉ đạt tối đa 1 Mbps.

## 1.7. Phân loại mạng

### 1.7.1. Theo khoảng cách

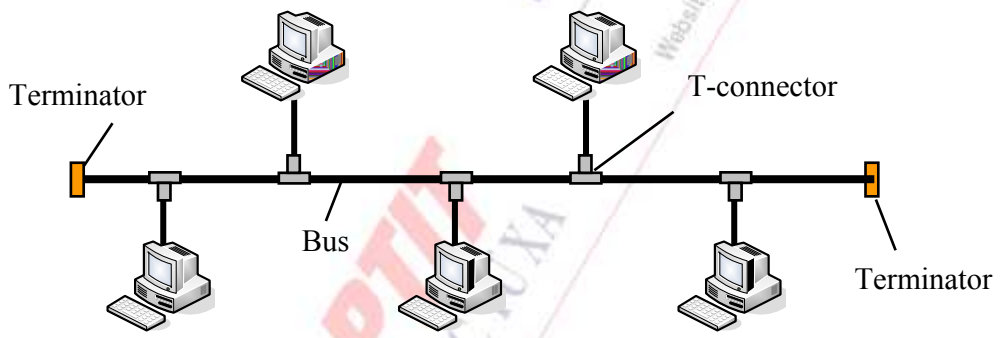
**a. Mạng cục bộ LAN (Local Area Networks):**

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 nhiệp... 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 vào khoảng vài km. Các máy trong một tòa nhà, một cơ quan hay xí nghiệp.. nối lại với nhau. Quản trị và bảo dưỡng mạng đơn giản.

*Công nghệ truyền dẫn* sử dụng trong mạng LAN thường là quảng bá (Broadcast), bao gồm một cáp đơn nối tất cả các máy. Tốc độ truyền dữ liệu cao, từ 10÷100 Mbps đến hàng trăm Gbps, thời gian trễ nhỏ (cỡ 10μs), độ tin cậy cao, tỷ số lỗi bit từ $10^{-8}$ đến $10^{-11}$.

*Cấu trúc tôpô của mạng* đa dạng. Ví dụ Mạng hình BUS, hình vòng (Ring), hình sao (Star) và các loại mạng kết hợp, lai ghép.....

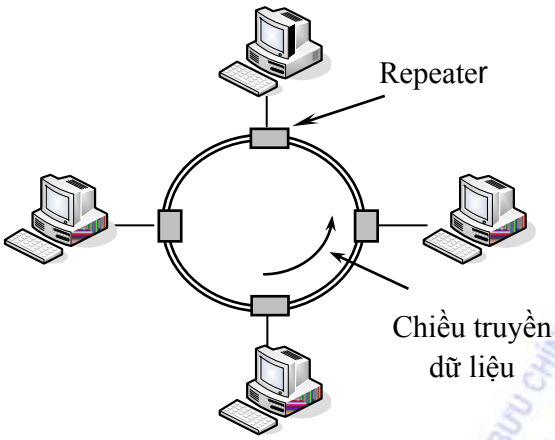



**Hình 1.4 Cấu trúc mạng hình BUS**

- *Mạng hình BUS* hoạt động theo kiểu quảng bá (Broadcast). Tất cả các node truy nhập chung trên một đường truyền vật lý có đầu và cuối (BUS). Chuẩn IEEE 802.3 được gọi là Ethernet, là một mạng hình BUS quảng bá với cơ chế điều khiển quảng bá động phân tán, trao đổi thông tin với tốc độ 10 Mbps hoặc 100 Mbps.

Phương thức truy nhập đường truyền được sử dụng trong mạng hình BUS hoặc TOKEN BUS, hoặc đa truy nhập sử dụng sóng mang với việc phát hiện xung đột thông tin trên đường truyền CSMA/CD (Carrier Sense Multiple Access with Collision Detection).

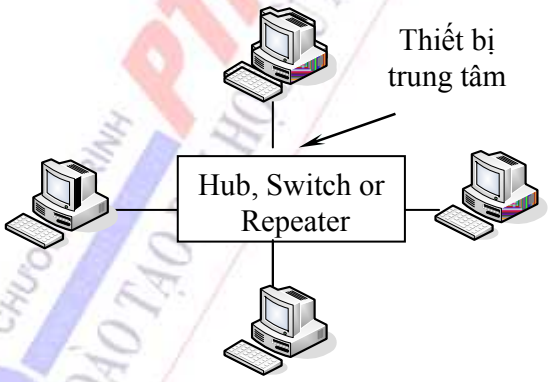
- *Mạng hình vòng (RING)* là mạng quảng bá (Broadcast), tất cả các node cùng truy nhập chung trên một đường truyền vật lý. Tín hiệu được lưu chuyển trên vòng theo một chiều duy nhất, theo liên kết điểm - điểm. Dữ liệu được chuyển một cách tuần tự từng bit quanh vòng, qua các bộ chuyển tiếp. Bộ chuyển tiếp có ba chức năng: chèn, nhận và hủy bỏ thông tin. Các bộ chuyển tiếp sẽ kiểm tra địa chỉ đích trong các gói dữ liệu khi đi qua nó.




**Hình 1.5 Cấu trúc mạng hình RING**

- *Mạng hình sao (Star)* các trạm kết nối với một thiết bị trung tâm có chức năng điều khiển toàn bộ hoạt động của mạng. Dữ liệu được truyền theo các liên kết điểm - điểm. Thiết bị trung tâm có thể là một bộ chuyển mạch, một bộ chọn đường hoặc đơn giản là một HUB.

- *Mạng LAN hồng ngoại (Infrared)* sử dụng sóng hồng ngoại để truyền dữ liệu. Phạm vi hoạt động của mạng bị hạn chế trong một phòng, vì tín hiệu hồng ngoại không đi xuyên qua t-ường. Có hai phương pháp kết nối điểm- điểm và kết nối quảng bá. Các mạng điểm - điểm hoạt động bằng cách chuyển tiếp các tín hiệu hồng ngoại từ một thiết bị tới thiết bị kế tiếp. Tốc độ dữ liệu đạt khoảng 100Kb/s đến 16Mb/s. Các mạng quảng bá hồng ngoại có tốc độ truyền dữ liệu thực tế chỉ đạt dưới 1Mb/s.



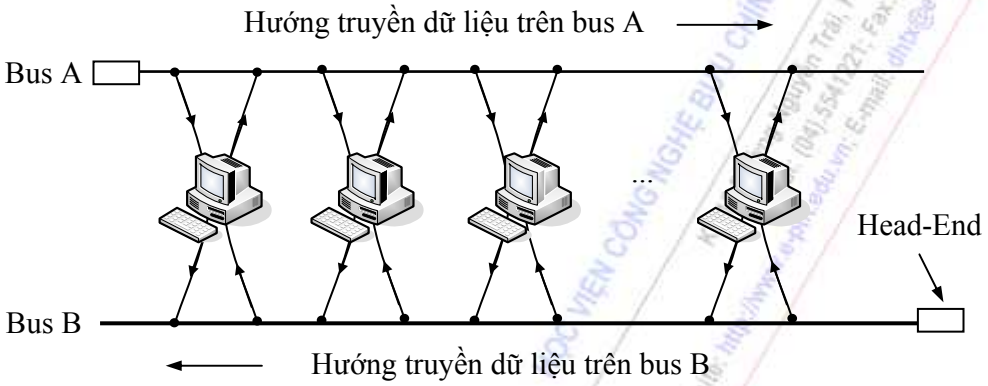

**Hình 1.6 Cấu trúc mạng hình sao**

- *Mạng LAN trải phổ (Spread spectrum)* Sử dụng kỹ thuật trải phổ, thường dùng trong công nghiệp và y tế.

- *Mạng LAN vi ba băng hẹp:* Hoạt động với tần số vi ba nhưng không trải phổ. Có hai dạng truyền thống: vi ba mặt đất và vệ tinh. Các hệ thống vi ba mặt đất thường hoạt động ở băng tần 4-6 GHz và 21- 23 GHz, tốc độ truyền dữ liệu khoảng vài chục Mbps.

**b. Mạng đô thị MAN (Metropolitan Area Networks)**

Mạng đô thị MAN hoạt động theo kiểu quảng bá, LAN to LAN. Mạng cung cấp các dịch vụ thoại và phi thoại và truyền hình cáp. Trong một mạng MAN, có thể sử dụng một hoặc hai đường truyền vật lý và không chứa thực thể chuyển mạch. Dựa trên tiêu chuẩn DQDB (Distributed Queue Dual Bus - IEEE 802.6) quy định 2 cáp đơn kết nối tất cả các máy tính lại với nhau, các máy bên trái liên lạc với các máy bên phải thông tin vận chuyển trên đường BUS trên. Các máy bên trái liên lạc với các máy bên phải, thông tin đi theo đường BUS dưới.

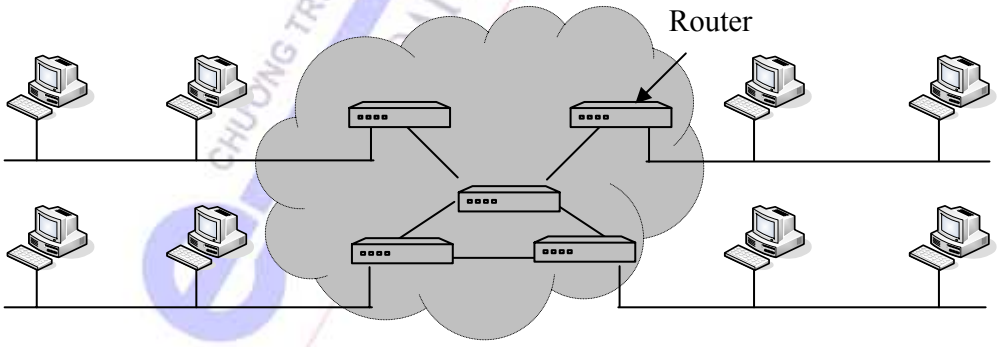



**Hình 1.7: Cấu trúc mạng đô thị MAN**

**c. Mạng diện rộng WAN (Wide Area Networks)**

*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.




**Hình 1.8: Cấu trúc một mạng diện rộng WAN**

*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)

**d. Kết nối liên mạng (Internet Connectivity)**

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*: Các gói tin thường được lưu chuyển trên các mạng con và các gói tin lưu thông trên liên mạng khi các mạng con liên lạc với nhau.

*Tối ưu hoá hiệu năng*: Giảm lưu thông trên mạng là tối ưu hiệu năng của mạng, tuy nhiên máy chủ (Server Load) sẽ phải tăng tải khi nó được sử dụng như một Router.

*Đơn giản hoá việc quản trị mạng*: Có thể xác định các sự cố kỹ thuật và cô lập dễ dàng hơn trong một mạng có quy mô nhỏ, thường là trong một mạng cục bộ chẳng hạn.

*Hiệu quả hơn so với mạng* WAN có phạm vi hoạt động lớn, chi phí giảm, hiệu năng liên mạng tăng và độ phức tạp của việc quản lý nhỏ hơn.

Một trong những chức năng chủ yếu của các thiết bị kết nối liên mạng là chức năng định tuyến (Routing). Có 3 phương thức kết nối liên mạng cơ bản:

- Kết nối các mạng LAN thuần nhất tại tầng vật lý tạo ra liên mạng có phạm vi hoạt động rộng và tăng số lượng các node trên mạng, giảm bớt lưu lượng trên mỗi mạng con, hạn chế tắc nghẽn và đụng độ thông tin. Các mạng con hoạt động hiệu quả hơn.

- Kết nối các mạng LAN không thuần nhất tại tầng 2 (Data Link) tạo ra một liên mạng bao gồm một số mạng LAN cục bộ kết nối với nhau bằng các bộ chuyển mạch đến các máy chủ cô lập với tốc độ cao.

- Kết nối các mạng LAN các kiểu khác nhau tại tầng 3 (Network Layer) tạo ra một mạng WAN đơn. Các node chuyển mạch kết nối với nhau theo một cấu trúc lưới. Mỗi một node chuyển mạch cung cấp dịch vụ cho tập hợp các thiết bị đầu cuối (DTE) của nó.

### 1.7.2. Mạng chuyển mạch kênh (Circuit Switched Networks)

- 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.

### 1.7.3. Mạng chuyển mạch gói (Packet Switched Networks)

*Nguyên lý chuyển mạch gói*: Thông điệp (Message) của người sử dụng được chia thành nhiều gói nhỏ (Packet) có độ dài quy định. Độ dài gói tin cực đại (Maximum Transfer Unit) MTU trong các mạng khác nhau là khác nhau. Các gói tin của một thông điệp có thể truyền độc lập trên nhiều tuyến hướng đích và các gói tin của nhiều thông điệp khác nhau có thể cùng truyền trên một tuyến liên mạng. Tại mỗi node, các gói tin được tiếp nhận, lưu trữ, xử lý tại bộ nhớ, không cần phải lưu trữ tạm thời trên bộ nhớ ngoài (như đĩa cứng) và được chuyển tiếp đến node kế tiếp. Định tuyến các gói tin qua mạng nhanh hơn và hiệu quả hơn.

*Kỹ thuật chuyển mạch gói có nhiều ưu điểm hơn so với chuyển mạch kênh:*

- Các gói tin lưu chuyển hướng đích độc lập, trên một đường có thể chia sẻ cho nhiều gói tin. Vì vậy hiệu suất đường truyền cao hơn.

- Các gói tin được xếp hàng và truyền qua tuyến kết nối.

- Hai thực thể có tốc độ dữ liệu khác nhau có thể trao đổi các gói với tốc độ phù hợp.

- Trong mạng chuyển mạch kênh, khi lưu lượng tăng thì mạng từ chối thêm các yêu cầu kết nối (do nghẽn) cho đến khi giảm xuống. Trong mạng chuyển mạch gói, các gói tin vẫn được chấp nhận, nhưng trễ phân phát gói tin có thể tăng lên.

*Các công nghệ chuyển mạch gói:* Nếu một thực thể gửi một gói dữ liệu qua mạng có độ dài lớn hơn kích thước gói cực đại MTU, nó sẽ được chia thành các gói nhỏ có độ dài quy định và gửi lên mạng. Có hai kỹ thuật được sử dụng trong các mạng chuyển mạch gói là kỹ thuật *datagram* trong mạng không liên kết (Connectionless) và kỹ thuật *kênh ảo* cho mạng hướng liên kết (Connection- Oriented).

- *Phương thức datagram sử dụng trong mạng không liên kết:* Mỗi một gói tin được lưu chuyển và xử lý độc lập, không cần tham chiếu đến các gói tin đã gửi trước. Mỗi một gói tin được xem như là một datagram.

Ưu, nhược điểm của phương thức datagram: Giai đoạn thiết lập và giải phóng kết nối sẽ được bỏ qua. Phù hợp với yêu cầu truyền khối lượng dữ liệu không lớn trong thời gian ngắn. Phương thức linh hoạt hơn so với phương thức kênh ảo. Nếu xẩy ra nghẽn thông tin, các datagram có thể được định tuyến ra khỏi vùng nghẽn. Và nếu có node bị hỏng, các gói tin tự tìm một tuyến khác để lưu chuyển hướng đích, việc phân phát các gói tin tin cậy hơn.

*Phương thức kênh ảo VC (Virtual Circuit) sử dụng trong mạng hướng liên kết*: Trước khi trao đổi thông tin, hai thực thể tham gia truyền thông đàm phán với nhau về các tham số truyền thông như kích thước tối đa của gói tin, các cửa sổ, đường truyền.... Một kênh ảo đã được hình thành thông qua liên mạng và tồn tại cho đến khi các thực thể ngừng trao đổi với nhau. Tại một thời điểm, có thể có nhiều kênh ảo đi và đến từ nhiều hướng khác nhau. Các gói tin vẫn được đệm tại mỗi node và được xếp hàng đầu ra trên một đường truyền, các gói tin của các thông điệp khác trên kênh ảo khác có thể chia sẻ sử dụng đường truyền này.

Ưu, nhược điểm của phương pháp kênh ảo: Mạng có thể cung cấp các dịch vụ kênh ảo, bao gồm việc điều khiển lỗi và thứ tự các gói tin. Tất cả các gói tin đi trên cùng một tuyến sẽ đến theo thứ tự ban đầu. Điều khiển lỗi đảm bảo không chỉ các gói đến đích theo đúng thứ tự mà cho tất cả các gói không bị lỗi. Một ưu điểm khác là các gói tin lưu chuyển trên mạng sẽ nhanh hơn vì không cần phải định tuyến tại các node. Tuy nhiên sẽ khó khăn hơn việc thích ứng với nghẽn. Nếu

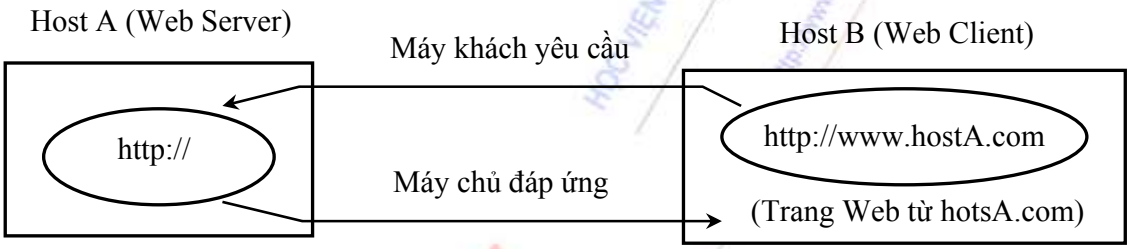
có node bị hỏng thì tất cả các kênh ảo qua node đó sẽ bị mất, việc phân phát datagram càng khó khăn hơn, độ tin cậy không cao.

## 1.8. Các mô hình xử lý dữ liệu

### 1.8.1. Mô hình 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 và phía Server tiếp nhận các yêu cầu từ phía Client và cung cấp các dịch vụ một cách thông suốt cho người sử dụng.

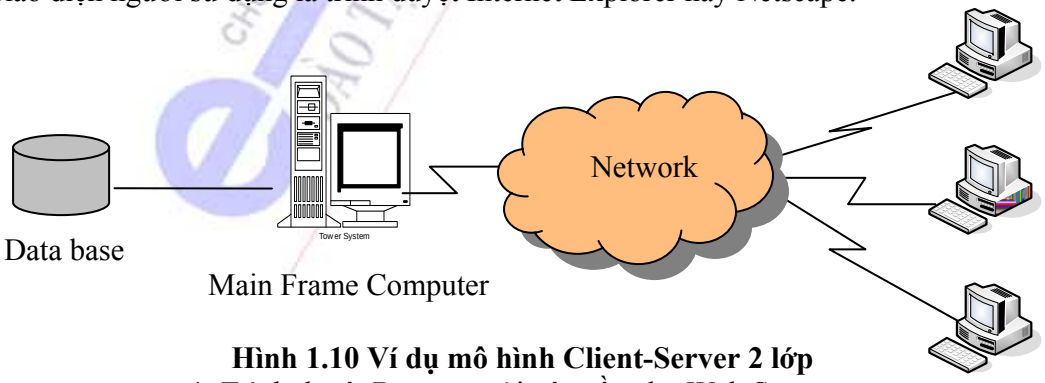
Chương trình Server được khởi động trên một máy chủ và ở trạng thái sẵn sàng nhận các yêu cầu từ phía Client. Chương trình Client cũng được khởi động một cách độc lập với chương trình Server. Yêu cầu dịch vụ được chương trình Client gửi đến máy chủ cung cấp dịch vụ và chương trình Server trên máy chủ sẽ đáp ứng 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.




**Hình 1.9: Mô hình chủ /khách (Client / Server)**

Trong mô hình Client/Server nhiều lớp, quá trình xử lý được phân tán trên 3 lớp khác nhau với các chức năng riêng biệt. Mô hình này thích hợp cho việc tổ chức hệ thống thông tin trên mạng Internet/ Intranet. Phát triển mô hình 3 lớp sẽ khắc phục được một số hạn chế của mô hình 2 lớp. Các hệ cơ sở dữ liệu được cài đặt trên các máy chủ Web Server và có thể được truy nhập không hạn chế các ứng dụng và số lượng người dùng.

*Lớp khách* (Clients) cung cấp dịch vụ trình bày (Presentation Services), giao tiếp người sử dụng với lớp giao dịch thông qua trình duyệt Browser hay trình ứng dụng để thao tác và xử lý dữ liệu. Giao diện người sử dụng là trình duyệt Internet Explorer hay Netscape.




**Hình 1.10 Ví dụ mô hình Client-Server 2 lớp**

1. Trình duyệt Browser gửi yêu cầu cho Web Server.
2. Web Server trả kết quả về cho trình duyệt

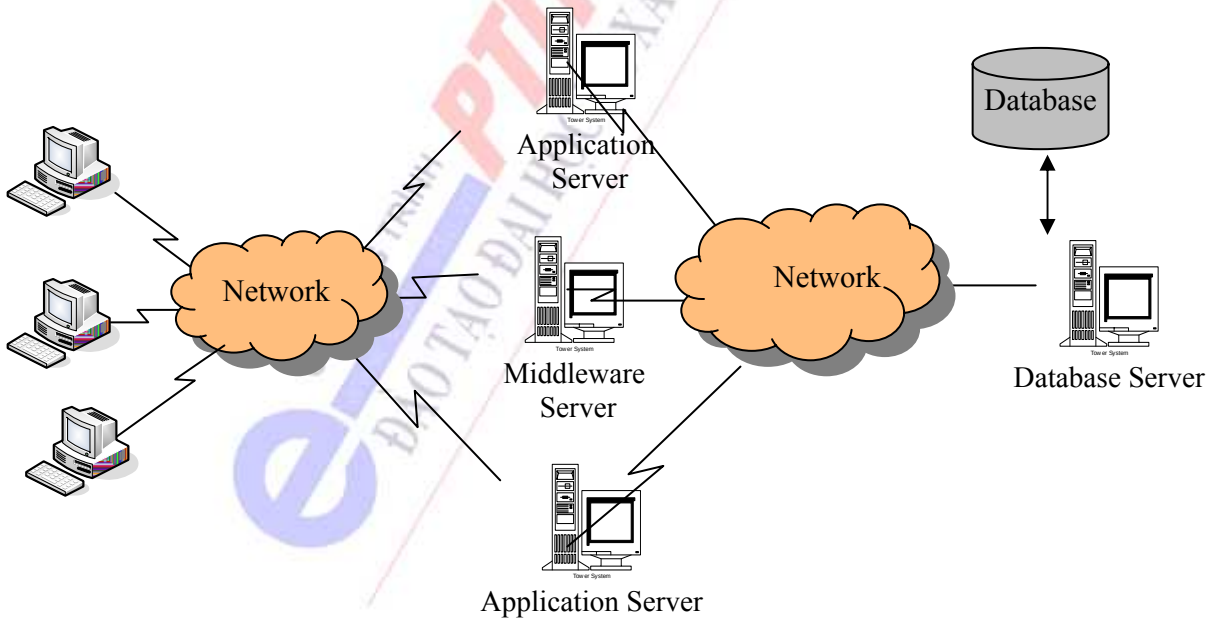
*Lớp giao dịch (Business)* cung cấp các dịch vụ quản trị, tổ chức và khai thác cơ sở dữ liệu. Các componenet trước đây được cài đặt trên lớp khách, nay được cài đặt trên lớp giao dịch. Ví dụ, một người sử dụng trên máy khách đặt mua hàng, lớp giao dịch kiểm tra mã mặt hàng để quyết định tiếp tục bán hay không bán. Thành phần của lớp giao dịch trong mô hình Internet là Web Server và COM+/MTS. Công nghệ của Microsoft với Web Server là IIS (Internet Information Services) sử dụng ASP để kết nối Client với COM. Web Server giao tiếp với COM+/MTS component qua COM. COM+/MTS component điều khiển tất cả giao tiếp với lớp dữ liệu nguồn thông qua ODBC hoặc OLE - DB.

*Lớp nguồn dữ liệu (Data Source)* cung cấp các dịch vụ tổ chức và lưu trữ các hệ cơ sở dữ liệu quan hệ. Sẵn sàng cung cấp dữ liệu cho lớp giao dịch. Đặc trưng của lớp này là ngôn ngữ tìm kiếm, truy vấn dữ liệu SQL.

### 1.8.2. 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.

*Mô hình lai (Hybrid)*: Sự kết hợp giữa Client-Server và Peer-to-Peer. Phần lớn các mạng máy tính trên thực tế thuộc mô hình này.




**Hình 1.11 Mô hình Client-Server nhiều lớp**

## Câu hỏi trắc nghiệm:

1. Hãy chọn câu đúng nhất về định nghĩa mạng máy tính:
   A. Tập các máy tính kết nối với nhau bằng đường truyền vật lý.
   B. Tập các máy tính kết nối với nhau và hoạt động tuân theo tập giao thức.
   C. Tập các máy tính kết nối với nhau bằng các đường truyền vật lý và hoạt động theo một kiến trúc mạng xác định
2. Mục tiêu kết nối mạng máy tính:
   A. Chia sẻ tài nguyên mạng, nâng cao độ tin cậy, chinh phục khoảng cách.
   B. Chia sẻ phần cứng, phần mềm, nâng cao độ tin cậy, chinh phục khoảng cách.
   C. Chia sẻ thông tin, nâng cao độ tin cậy, chinh phục khoảng cách.
   D. Cung cấp các dịch vụ mạng đa dạng, chia sẻ tài nguyên, nâng cao độ tin cậy, chinh phục khoảng cách và giảm bớt các chi phí về đầu tư .
3. Các xu hướng phát triển dịch vụ mạng máy tính:
   A. Cung cấp các dịch vụ truy nhập vào các nguồn thông tin ở xa
   B. Phát triển các dịch vụ tương tác giữa người với người trên phạm vi diện rộng.
   C. Xu hướng phát triển các dịch vụ giải trí trực tuyến (Online) hiện đại.
   D. Cả 3 câu trên.
4. Mạng có cấu trúc điểm- điểm (Point to Point) là:
   A. Mạng lưu và gửi tiếp (Store - and - Forward).
   B. Nối từng cặp node lại với nhau theo một hình học xác định.
   C. Các node trung gian: tiếp nhận, lưu trữ tạm thời và gửi tiếp thông tin
5. Nhược điểm của mạng có cấu trúc điểm- điểm (Point to Point) là:
   A. Khả năng đụng độ thông tin (Collision) thấp.
   B. Hiệu suất sử dụng đường truyền thấp. Chiếm dụng nhiều tài nguyên
   C. Độ trễ lớn, tốn nhiều thời gian để thiết lập đường truyền và xử lý tại các node.
   D. Tốc độ trao đổi thông tin thấp.
6. Đặc trưng của mạng quảng bá (Point to Multipoint, Broadcasting)
   A. Tất cả các node cùng truy nhập chung trên một đường truyền vật lý.
   B. Nối từng cặp node lại với nhau theo một hình học xác định.
   C. Các node trung gian: tiếp nhận, lưu trữ tạm thời và gửi tiếp thông tin
7. Chức năng giao thức:
   A. Đóng gói, phân đoạn và hợp lại
   B. Điều khiển liên kết và giám sát.
   C. Điều khiển lưu lượng và điều khiển lỗi.
   D. Đồng bộ hoá và địa chỉ hoá.

E. Tất cả các khẳng định trên.

8. Đặc trưng cơ bản của đường truyền
   A. Băng thông (Bandwidth).
   B. Thông lượng (Throughput)
   C. Suy hao (Attenuation)
   D. Tốc độ truyền dẫn.
9. Mạng cục bộ LAN (Local Area Networks):
   A. Quy mô của mạng nhỏ, phạm vi khoảng vài km.
   B. Công nghệ truyền dẫn sử dụng thường là quảng bá (Broadcast)
   C. Tốc độ truyền dữ liệu cao, từ 10÷100 Mbps đến hàng trăm Gbps,
   D. Thời gian trễ cỡ 10μs , độ tin cậy cao, tỷ số lỗi bit từ $10^{-8}$ đến $10^{-11}$.
   E. Cấu trúc tôpô của mạng đa dạng.
   F. Tất cả các khẳng định trên.
10. Đặc trưng cơ bản của một mạng WAN:
   A. Hoạt động trên phạm vi một quốc gia hoặc trên toàn cầu.
   B. Tốc độ truyền dữ liệu thấp so với mạng cục bộ.
   C. Lỗi truyền cao.
   D. Tất cả các khẳng định trên.
11. Lợi ích khi kết nối liên mạng:
   A. Giảm lưu thông trên mạng
   B. Tối ưu hoá hiệu năng
   C. Đơn giản hoá việc quản trị mạng
   D. Hiệu quả hơn so với mạng WAN có phạm vi hoạt động lớn.
12. Mạng chuyển mạch kênh (Circuit Switched Networks)
   A. Thiết lập kết nối vật lý giữa 2 thực thể, duy trì kết nối trong quá trình trao đổi thông tin và giải phóng kết nối khi truyền xong dữ liệu.
   B. Thiết lập kết nối logic giữa 2 thực thể , duy trì kết nối trong quá trình trao đổi thông tin và giải phóng kết nối khi truyền xong dữ liệu.
   C. Truyền dữ liệu giữa 2 thực thể.
13. Khẳng định đúng nhất trong mạng chuyển mạch gói (Packet Switched Networks):
   A. Gói tin lưu chuyển trên các kết nối logic.
   B. Gói tin lưu chuyển trên các kết nối vật lý.
   C. Gói tin lưu chuyển độc lập hướng đích.
   D. Các gói tin lưu chuyển hướng đích độc lập và trên một đường có thể chia sẻ cho nhiều gói tin.

14. Độ dài gói tin cực đại MTU (Maximum Transfer Unit)
    A. Trong các mạng khác nhau là khác nhau.
    B. Trong các mạng khác nhau là như nhau.
    C. Trong các mạng không quan tâm đến độ dài gói tin
15. Hãy chọn những khẳng định đúng sau:
    A. Kỹ thuật datagram sử dụng trong các mạng không liên kết (Connectionless)
    B. Kỹ thuật datagram sử dụng trong các mạng hướng liên kết (Connection- Oriented). Kỹ thuật datagram sử dụng trong các mạng chuyển mạch kênh.
    C. Kỹ thuật datagram sử dụng trong các mạng chuyển gói X25.
16. Hãy chọn những khẳng định đúng sau:
    A. Kỹ thuật kênh ảo VC (Virtual Circuit) sử dụng trong các mạng không liên kết
    B. Kỹ thuật kênh ảo VC sử dụng trong các mạng hướng liên kết
    C. Kỹ thuật kênh ảo VC sử dụng trong các mạng chuyển mạch kênh.
    D. Kỹ thuật kênh ảo VC sử dụng trong các mạng chuyển gói X25.

## Câu hỏi

1. Hãy trình bày mục tiêu và ứng dụng mạng máy tính.
2. Hãy phát biểu các lợi ích khi nối máy tính thành mạng.
3. Hãy trình bày tổng quát về xu hướng phát triển các dịch vụ mạng.
4. Hiểu thế nào là mạng máy tính. Hãy trình bày tóm tắt chức năng các thành phần chủ yếu của một mạng máy tính ?.
5. Hãy trình bày khái quát về các đặc trưng cơ bản của đường truyền: Băng thông (bandwidth), thông lượng (throughput) và suy hao (attenuation).
6. Khái quát các đặc trưng cơ bản của các phương tiện truyền: Cáp đồng trục (Coaxial cable), cáp xoắn đôi (Twisted pair cable), cáp sợi quang (Fiber optic cable).
7. Hãy trình bày cấu trúc kiểu điểm - điểm (Point to Point).
8. Trong kỹ thuật chuyển mạch kênh, vai trò địa chỉ như thế nào ?.
9. Hãy trình bày kiểu quảng bá (Point to Multipoint, Broadcast).
10. Trình bày ưu, nhược điểm các phương thức quảng bá tĩnh và động, Quảng bá động tập trung và phân tán ?.
11. Những khác biệt cơ bản giữa kiểu điểm - điểm và quảng bá ?.
12. Hiểu thế nào là giao thức, vai trò của giao thức trong truyền thông ?.
13. Trình bày các chức năng của giao thức.
14. Mạng cục bộ LAN (Local Area Networks) và các đặc trưng cơ bản của nó
15. Hãy trình bày cấu trúc mạng hình BUS, RING và STAR.
16. Sự khác nhau cơ bản giữa mạng hình BUS và mạng hình RING ?.

17. Hãy trình bày những đặc trưng cơ bản của các mạng LAN không dây ?.
18. Mạng đô thị MAN (Metropolitan Area Networks) và đặc trưng cơ bản của nó.
19. Mạng diện rộngWAN và những đặc trưng của mạng diện rộng.
20. Hiểu thế nào là liên mạng (Internetworking). Mạng WAN là một liên mạng ?.
21. Chức năng của các thiết bị kết nối liên mạng.
22. HUB là thiết bị kết nối liên mạng ?.
23. Chức năng của bộ định tuyến ROUTER. Có thể thay thế HUB trong kết nối liên mạng. Ví dụ minh họa ?.
24. Hiểu thế nào là dịch vụ hướng liên kết (Connection - Oriented) và không liên kết (Connectioless). Hãy cho thí dụ minh họa.
25. Nguyên tắc hoạt động của mạng chuyển mạch kênh (Circuit Switched Networks).
26. Trình bày ưu, nhược điểm của kỹ thuật chuyển mạch kênh.
27. Trình bày nguyên tắc hoạt động của mạng chuyển mạch gói (Packet Switched Networks).
28. Vì sao nói kỹ thuật chuyển mạch gói có hiệu suất kênh truyền cao, vì sao ?.
29. Ưu nhược điểm của kỹ thuật chuyển nạch gói ?.
30. Nói mạng chuyển mạch gói là mạng X25 ?.
31. Kỹ thuật chuyển mạch gói nhiều ưu điểm hơn kỹ thuật chuyển mạch kênh, vì sao ?.
32. Trình bày phương thức Datagram.
33. Trình bày phương thức kênh ảo VC (Virtual circuit)
34. So sánh ưu, nhược của phương pháp kênh ảo và Datagram.
35. Phương thức kênh ảo và chuyển mạch kênh khác nhau, giống nhau ?.
36. Vì sao mạng chuyển mạch gói có tốc độ trao đổi thông tin nhanh hơn tốc độ trao đổi thông tin trong mạch chuyển mạch tin báo.
37. Hiểu thế nào là cấu trúc mạng Client/Server, Peer to Peer ?

# CHƯƠNG II: KIẾN TRÚC MẠNG VÀ MÔ HÌNH KẾT NỐI CÁC HỆ THỐNG MỞ OSI

Nội dung của chương này sẽ trình bày các khái niệm về kiến trúc phân tầng và mô hình kết nối các hệ thống mở OSI (Open System Interconnection) với mục tiêu kết nối các sản phẩm của các hãng sản xuất khác nhau. Mô hình OSI là giải pháp cho các vấn đề truyền thông giữa các máy tính và được thiết kế theo quan điểm có cấu trúc đa tầng. Mỗi một tầng thực hiện một số chức năng truyền thông, các tầng được xếp chồng lên nhau, gọi là chồng giao thức, thực hiện các tiến trình truyền thông hoàn chỉnh. Giữa các tầng kề nhau được xác định bởi giao diện bằng các hàm dịch vụ nguyên thuỷ. Nội dung gồm các phần như sau:

- Các tổ chức chuẩn hóa mạng
- Mô hình kiến trúc đa tầng và các quy tắc phân tầng.
- Mô hình kết nối các hệ thống mở OSI .
- Những vấn đề cơ bản thiết kế mô hình kiến trúc.
- Đánh giá độ tin cậy của mạng.
- Một số mô hình kiến trúc chuẩn khác.

## 2.1. Các tổ chức tiêu chuẩn hóa mạng máy tính

### 2.1.1. Cơ sở xuất hiện kiến trúc đa tầng

Sự khác biệt về kiến trúc mạng đã gây trở ngại cho người sử dụng khi kết nối liên mạng, ảnh hưởng đến sức sản xuất và tiêu thụ các sản phẩm về 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. Vì vậy các tổ chức tiêu chuẩn quốc tế đã ra đời. Các nhà sản xuất đã có tiếng nói chung cho các sản phẩm của họ, đó là các chuẩn, các khuyến nghị quy định thiết kế và sản xuất các sản phẩm mạng.

### 2.1.2. Các tổ chức tiêu chuẩn

*ISO (International Standards Organization)*: Tổ chức tiêu chuẩn quốc tế hoạt động dưới sự bảo trợ của Liên Hiệp Quốc. Chia thành nhiều ban kỹ thuật- Technical Commitee- ký hiệu là TC, trong đó ban TC97 đảm nhận việc nghiên cứu chuẩn hoá xử lý thông tin. Các sản phẩm của nó gọi là các chuẩn- Standard - Mô hình OSI - Open Systems Interconnection là sản phẩm điển hình của tổ chức này.

*CCITT* (*International Telegraphand Telephone Consultative Committe*): Uỷ ban tư vấn điện tín & điện thoại quốc tế nay là Hiệp hội Viễn thông quốc tế ITU *(International Telecommunication Union).* Là tổ chức bao gồm các cơ quan Bưu chính Viễn thông của các nước. Các sản phẩm được gọi là các khuyến nghị (Recommendation):

- *Khuyến nghị loại V*: Tập các tiêu chuẩn về truyền dữ liệu bằng Modem: V21 tốc độ 300 bps, V32 tốc độ 9600 - 14.400 bps, V90, V92 cho tốc độ 56 Kbps.

- *Khuyến nghị loại X:* Tập các tiêu chuẩn liên quan đến mạng truyền số liệu. Quy định các thủ tục giao diện người sử dụng và giao diện mạng: X21, X25,...

- *Khuyến nghị loại* I: Các tiêu chuẩn liên quan đến mạng ISDN

- *IEEE (Institute of Electronical And Electronic Engineers)*: Viện các kỹ sư điện và điện tử. Tập các thủ tục tầng vật lý.

## 2.2. Mô hình kiến trúc đa tầng

Các mạng máy tính được thiết kế và cài đặt theo quan điểm có cấu trúc đa tầng. 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. Các tầng được chồng lên nhau, số lượng và chức năng của các tầng phụ thuộc vào các nhà sản xuất và thiết kế. Tuy nhiên quan điểm chung là trong mỗi tầng có nhiều thực thể (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.

### 2.2.1. Các quy tắc phân tầng

Tổ chức tiêu chuẩn quốc tế ISO quy định các quy tắc phân tầng như sau:

- Không định nghĩa quá nhiều tầng, số lượng tầng, vai trò và chức năng của các tầng trong mỗi hệ thống của mạng 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.

- 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 số các tương tác qua lại giữa hai tầng kề nhau là nhỏ nhất.

- Xác định mối quan hệ giữa các đồng tầng để thống nhất về các phương thức hoạt động trong quá trình truyền thông, mối quan hệ đó là tập các quy tắc và các thoả thuận trong hội thoại giữa các hệ thống, gọi là giao thức tầng.

- 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 là chuỗi bit không cấu trúc được truyền sang tầng thấp nhất của hệ thống nhận và từ đó dữ liệu 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.

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).

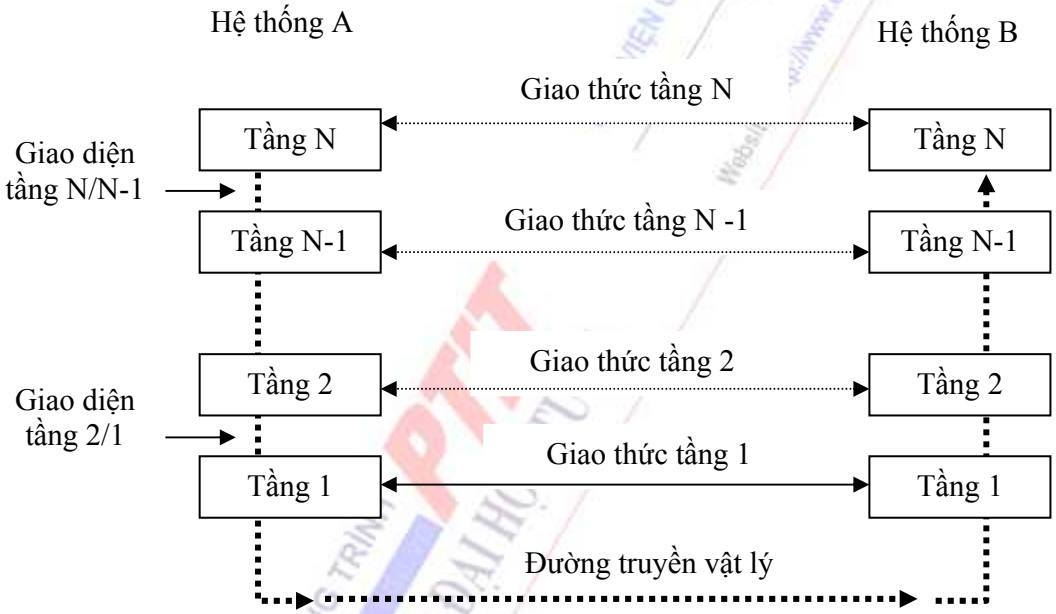
*Quan hệ theo chiều ngang* phản ánh sự hoạt động của các đồng tầng. Các đồng tầng trước khi trao đổi thông tin với nhau phải bắt tay, hội thoại và thỏa thuận với nhau bằng các tham số của các giao thức (hay là thủ tục), được gọi là giao thức tầng.

*Quan hệ theo chiều dọc* là quan hệ giữa các tầng kề nhau trong cùng một hệ thống. Giữa chúng tồn tại giao diện xác định các thao tác nguyên thủy và các dịch vụ tầng dưới cung cấp cho tầng trên. Được gọi là giao diện tầng.

Trong mỗi một tầng có một hoặc nhiều thực thể (Entity) hoạt động. Các thực thể có thể là một tiến trình (Process) trong một hệ đa xử lý, hoặc có thể là một chương trình con....Chúng thực hiện các chức năng của tầng N và giao thức truyền thông với các thực thể đồng tầng trong các hệ thống khác. Ký hiệu N_Entity là thực thể tầng N.

Các thực thể truyền thông với các thực thể tầng trên nó và các thực thể tầng dưới nó thông qua các điểm truy nhập dịch vụ trên các giao diện SAP (Service Access Point). Các thực thể phải biết nó cung cấp những dịch vụ gì cho các hoạt động tầng trên kề nó và các hoạt động truyền thông của nó được sử dụng những dịch vụ gì do tầng kề dưới nó cung cấp thông qua các lời gọi hàm qua các điểm truy nhập SAP trên giao diện các tầng.

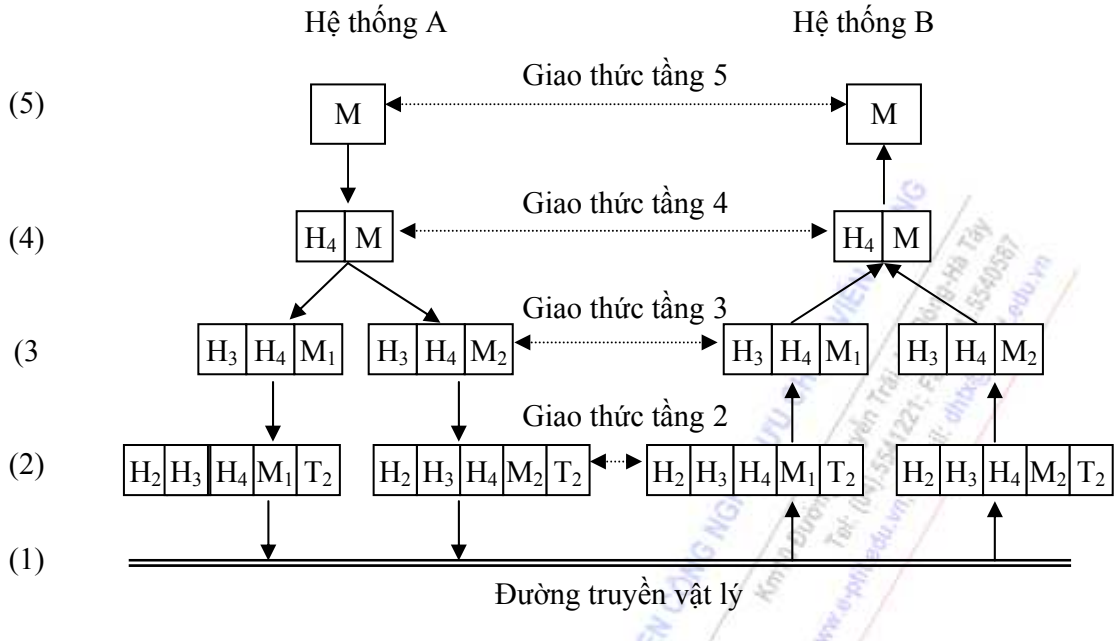
Khi mô tả hoạt động của bất kỳ giao thức nào trong mô hình OSI, cần phải phân biệt được các dịch vụ cung cấp bởi tầng kề dưới, hoạt động bên trong của tầng và các dịch vụ mà nó khai thác. Sự tách biệt giữa các tầng giúp cho việc bổ sung, sửa đổi chức năng của giao thức tầng mà không ảnh hưởng đến hoạt động của các tầng khác.




**Hình 2.1 Mô hình kiến trúc phân tầng**

### 2.2.2. Lưu chuyển thông tin trong kiến trúc đa tầng

Hình 2.2 là một ví dụ minh hoạ cho sự lưu chuyển thông tin trong mạng máy tính kết nối giữa 2 hệ thống A và B gồm N=5 tầng.




**Hinh 2.2 Ví dụ về lưu chuyển thông tin**

### 2.2.3. Nguyên tắc truyền thông đồng tầng

Để truyền thông đồng tầng, gói tin khi chuyển xuống qua các tầng sẽ được bổ sung thêm vào phần đầu bằng thông tin điều khiển của tầng. Việc thêm Header vào đầu các gói tin khi đi qua mỗi tầng trong quá trình truyền dữ liệu được gọi là quá trình *Encapsulation*. 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 được sử dụng trong các tầng bao gồm*

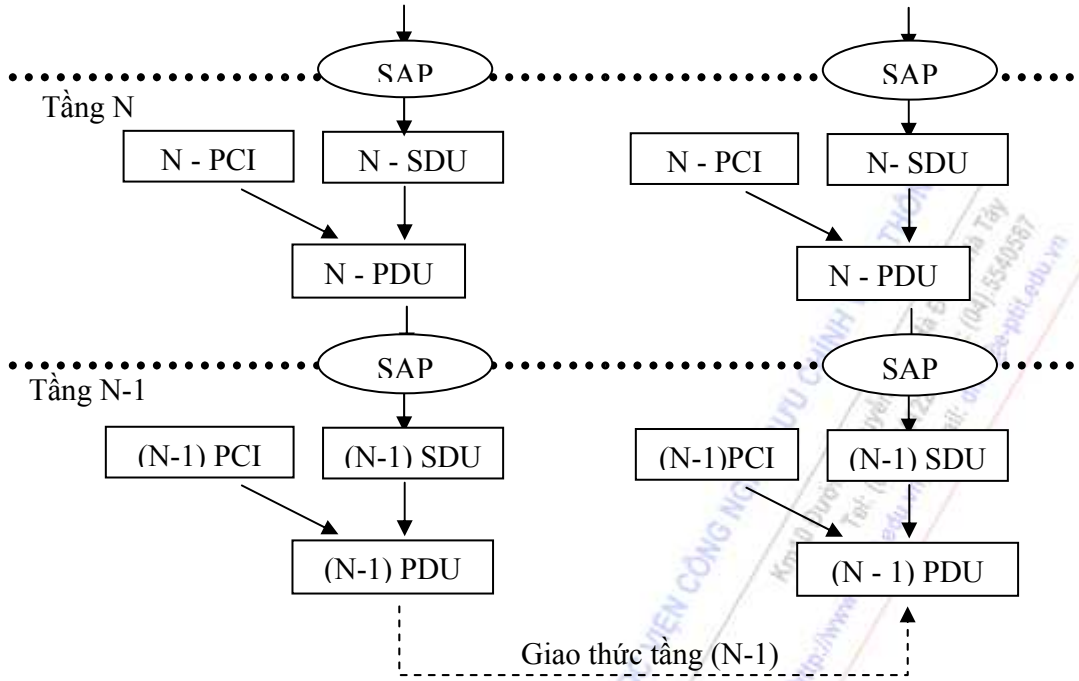
- *Thông tin điều khiển giao thức PCI (Protocol Control Information):* Thông tin được thêm vào đầu các gói tin trong quá trình hoạt động truyền thông của các thực thể. Ký hiệu N_PCI là thông tin điều khiển tầng N.

- *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 thêm thông tin điều khiển.

- *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.

### 2.2.4. Giao diện tầng, quan hệ các tầng kề nhau và dịch vụ

Chức năng của các tầng là cung cấp dịch vụ cho tầng trên kề nó. Trong mỗi tầng có một hay nhiều thực thể. Thực thể ở tầng N thực hiện các dịch vụ mà tầng N+1 yêu cầu sử dụng, Các thực thể trao đổi dịch vụ với nhau qua các điểm truy cập dịch vụ SAP (Service Access Points). Các thực thể tầng N cung cấp dịch vụ cho tầng N+1 qua các SAP trên giao diện N+1/N. Mỗi một SAP có một nhận dạng duy nhất.




**Hình 2.3 Khái niệm giao diện và dịch vụ trong môi trường các hệ thống mở**

Hai tầng trao đổi thông tin với nhau phải có những thoả thuận về thiết lập các quy tắc giao diện. Thực thể của tầng N+1 chuyển một PDU tới thực thể tầng N qua SAP. PDU bao gồm một đơn vị dữ liệu dịch vụ SDU và thông tin điều khiển PCI. SDU là thông tin gửi qua mạng tới thực thể đồng tầng và sau đó đưa lên tầng N+1. Nếu độ dài của SDU lớn hơn độ dài quy định, các thực thể tầng N chia SDU ra nhiều gói nhỏ có độ dài quy định và thêm Header PCI vào mỗi gói tin. Header của PDU được các thực thể đồng tầng nhận dạng PDU nào chứa dữ liệu và PDU nào chứa thông tin điều khiển.....

Hình 2.3 minh hoạ giao diện và dịch vụ trong các tầng kề nhau. Như đã biết, thực thể ở tầng N từ hệ thống A không thể truyền dữ liệu trực tiếp sang tầng N của hệ thống B mà phải chuyển tuần tự xuống các tầng dưới nó, cho tới tầng thấp nhất, tầng vật lý. Bằng phương tiện truyền vật lý, dữ liệu là những chuỗi bit 0 và 1 được truyền sang tầng vật lý của hệ thống B. Từ đây dữ liệu được chuyển lên các tầng trên.

### 2.2.5 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 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).

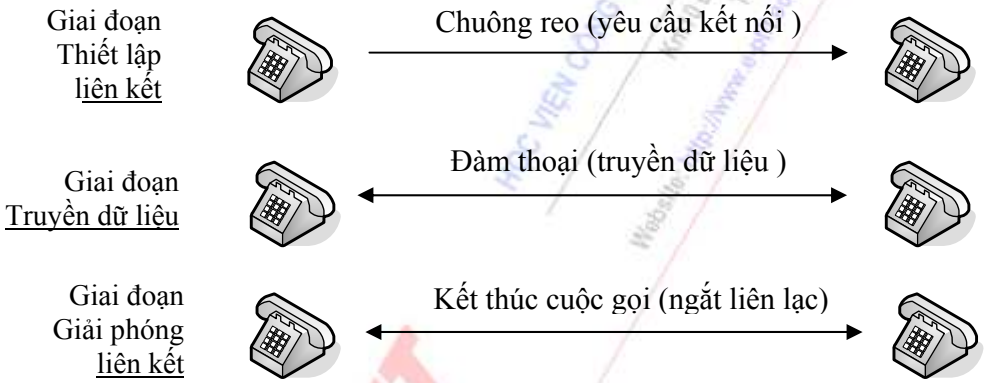
**a. Dịch vụ hướng liên kết (Connection Oriented):** Các dịch vụ và giao thức trong các mô hình hệ thống mở thực hiện truyền thông 3 giai đoạn theo thứ tự thời gian như sau:

*Thiết lập liên kết*: Một kênh logic được thiết lập giữa các thực thể đồng tầng của hai hệ thống khác nhau. Chúng sẽ đàm phán, thương lượng với nhau về tập các tham số và sử dụng các tham số này như thế nào trong quá trình truyền số liệu.

*Truyền dữ liệu*: Dữ liệu được truyền giữa hai tầng đồng tầng theo cơ chế kiểm soát và quản lý quá trình truyền dữ liệu, thực hiện việc ghép kênh, cắt hợp dữ liệu... bảo đảm được thứ tự truyền, phát hiện lỗi, kiểm soát luồng dữ liệu, phát hiện tắc nghẽn thông tin...nhằm tăng cường độ tin cậy cao và hiệu suất truyền.

*Giải phóng liên kết*: Sau khi kết thúc quá trình truyền dữ liệu, các tài nguyên của hệ thống được cấp phát cho quá trình thiết lập liên kết và truyền dữ liệu sẽ được giải phóng, sẵn sàng cấp phát cho liên kết tiếp theo.

Hình 2.4 minh họa phương thức truyền hướng liên kết trong các dịch vụ thoại.




**Hình 2.4 Ví dụ hoạt động kết nối liên kết**

**b. 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.

Mỗi dịch vụ được đặc trưng bởi chất lượng dịch vụ. Một số dịch vụ yêu cầu có độ tin cậy cao, bằng cách yêu cầu thực thể đích gửi xác nhận phản hồi sau khi nhận gói tin. Vì vậy máy thu luôn bảo đảm gói tin đã đến đúng và không để mất dữ liệu. Xử lý xác nhận phản hồi đòi hỏi phải chèn thêm vào gói tin một số thông tin điều khiển và làm tăng thời gian trễ. Một loại dịch vụ hướng liên kết tin cậy là dịch vụ truyền file với yêu cầu mọi bit gửi đến đều chính xác và đúng thứ tự như khi gửi đi. Một số loại dịch vụ chấp nhận có một số lỗi nhưng yêu cầu yêu cầu độ trễ nhỏ như thoại số, video. Với dịch vụ loại này thì không cần xác nhận có báo nhận, nhằm để giảm thời gian trễ tại các nút.

Ngoài dịch vụ hướng liên kết và không liên kết, còn có kiểu dịch vụ hỏi-đáp. Máy gửi sẽ gửi các thông tin chứa yêu cầu xác nhận trong các gói tin và yêu cầu máy nhận trả lời. Khi máy nhận nhận được gói tin, sẽ gửi các trả lời đến máy gửi. Dịch vụ hỏi-đáp được sử dụng truyền

thông trong mô hình khách-chủ (Client-Server). Máy khách (Client) gửi các yêu cầu cho máy chủ (Server) và máy chủ trả lời kết quả cho máy khách.

| | Dịch vụ | Ví dụ |
|---|---|---|
| Hướng liên kết | Truyền/nhận các gói tin, yêu cầu có xác nhận. | Gửi các trang sách theo đúng thứ tự. |
| | Truyền/nhận dòng byte, yêu cầu có xác nhận. | Truy nhập và khai thác từ xa. |
| | Kết nối không yêu cầu có xác nhận. | Các dịch vụ thoại số |
| Không liên kết | Datagram không xác nhận | Thư điện tử, nhắn tin |
| | Datagram có xác nhận | Thư có đăng ký, thư khẩn |
| | Hỏi-Đáp | Câu truy vấn trong cơ sở dữ liệu |

**Hình 2.5 Các loại dịch vụ khác nhau hướng liên kết và không liên kết**

### 2.2.6. 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*. Một dịch vụ được đặc tả hình thức bằng nhiều hàm dịch vụ nguyên thủy. Các hàm dịch vụ nguyên thủy sử dụng để định nghĩa sự tương tác giữa các tầng kề nhau, chỉ rõ chức năng cần thực hiện và sử dụng để chuyển dữ liệu và thông tin điều khiển. Cụ thể hơn, các hàm dịch vụ nguyên thủy là đặc tả các thao tác cần thực hiện một yêu cầu hay trả lời một yêu cầu của các thực thể đồng tầng.

*Có bốn kiểu hàm dịch vụ nguyên thủy cơ bản:*

1. Request (Yêu cầu): Được một thực thể sử dụng 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 thực thể yêu cầu sử dụng 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.

Hình 2.6 minh họa nguyên lý hoạt động của các hàm dịch vụ nguyên thuỷ.

*Trong hệ thống A:*

- Tầng (N+1) gửi hàm Request xuống tầng N qua SAP trên giao diện (N+1)/N.

- Tại tầng N, kiến tạo một đơn vị dữ liệu gửi yêu cầu sang tầng N của hệ thống B qua giao thức tầng N.

*Trong hệ thống B:*

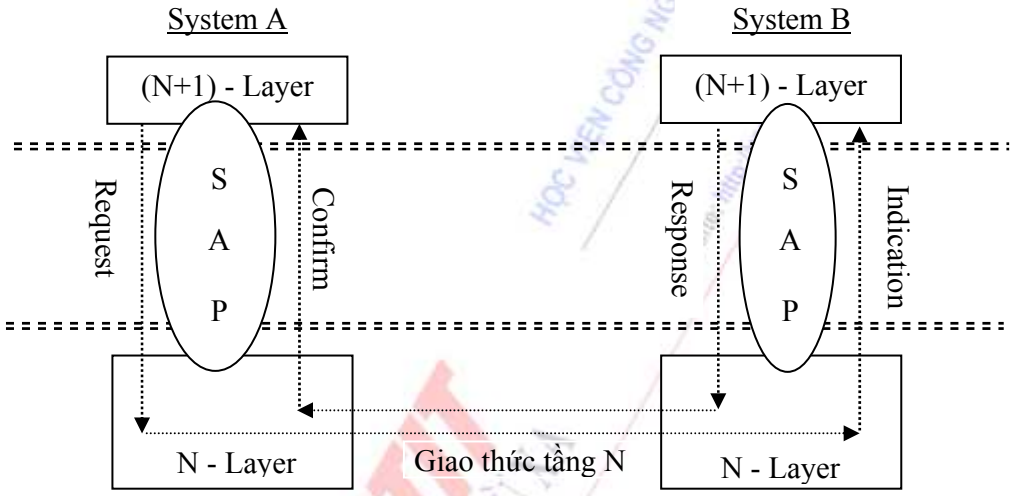
- Tầng N nhận được yêu cầu, chỉ báo- lên tầng (N+1) bằng hàm Indication qua SAP trên giao diện (N+1)/N .

- Tầng (N+1) trả lời tầng N bằng hàm Response qua SAP của giao diện 2 tầng.

- Tâng N, kiến tạo một đơn vị dữ liệu gửi trả lời sang tầng N của hệ thống A qua giao thức tầng N.

Nhận trả lời, tầng N của hệ thống A gửi xác nhận lên tâng (N+1) bằng hàm Confirm qua SAP trên giao diện. Kết thúc giao tác giữa 2 hệ thống.

Quá trình yêu cầu thiết lập liên kết giữa các thực thể đồng tầng có thể có xác nhận (Confirmed) hoặc không có xác nhận (Unconfirmed).

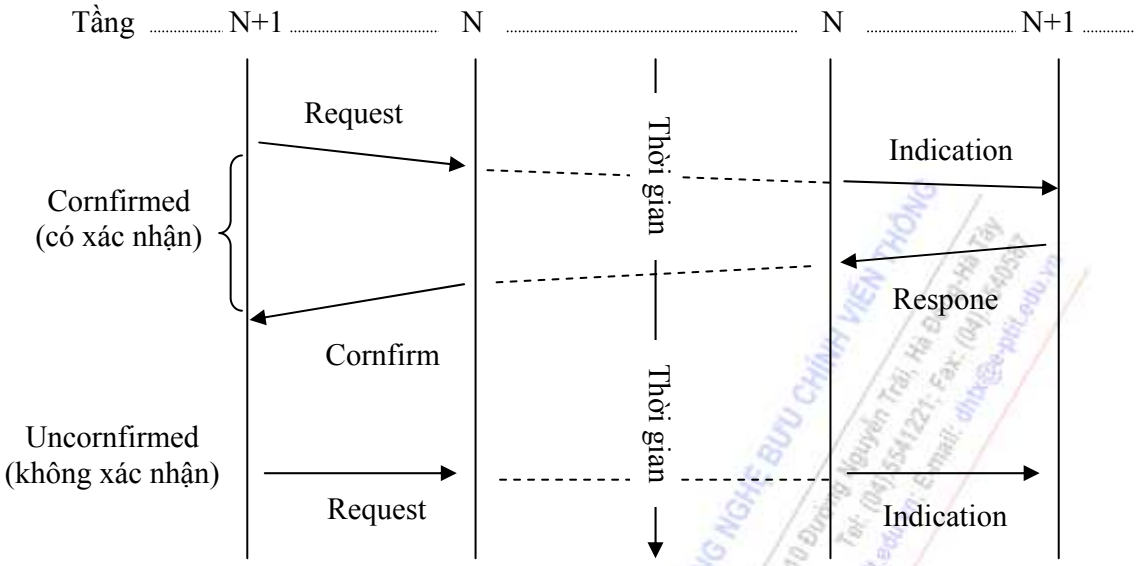



**Hình 2.6 Sơ đồ nguyên lý hoạt động của các hàm nguyên thuỷ**

### 2.2.7. Quan hệ giữa dịch vụ và giao thức

Mỗi một lớp giao thức có hai đặc trưng: đặc trưng dịch vụ và đặc trưng giao thức. 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. 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 của thực thể giao thức.

Dịch vụ và giao thức là những khái niệm khác nhau. 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. 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.

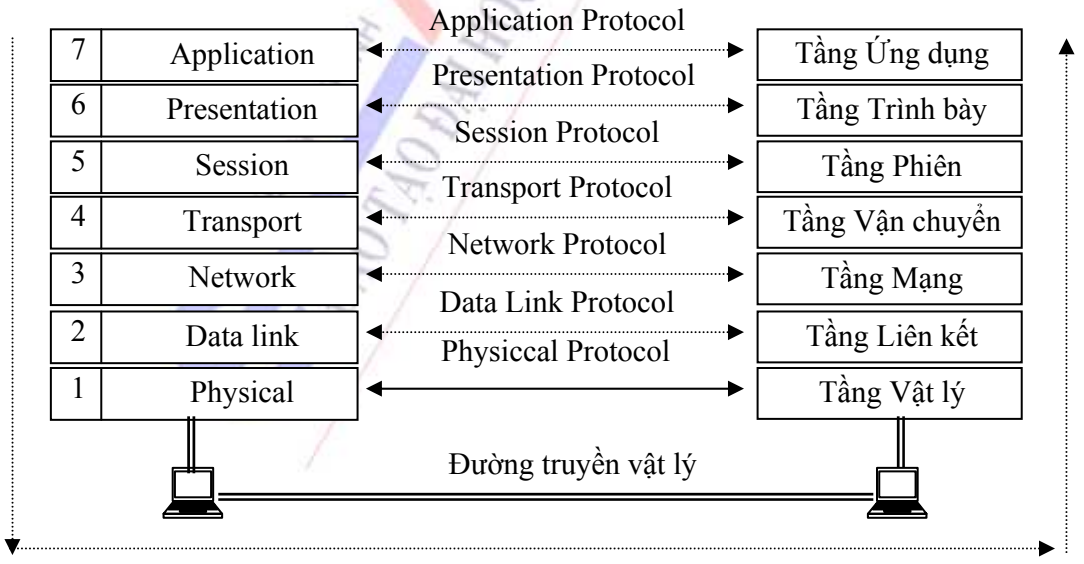



**Hình 2.7 Biểu diễn thời gian các hàm dịch vụ nguyên thủy**

## 2.3 Mô hình kết nối các hệ thống mở OSI (Open System Interconnection)

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.

### 2.3.1 Nguyên tắc định nghĩa các tầng hệ thống mở




**Hình 2.8 Mô hình kết nối các hệ thống mở 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.

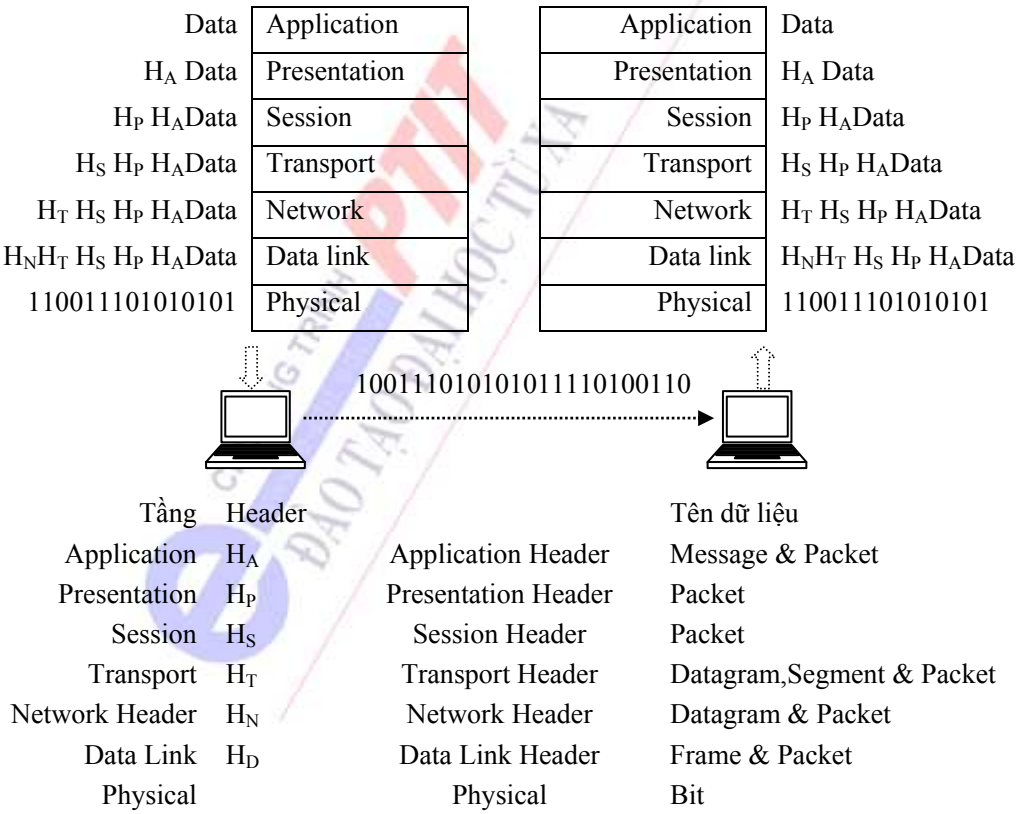
### 2.3.2. Các giao thức trong mô hình OSI

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 hướng liên kết*: Trước khi truyền dữ liệu, các thực thể đồng tầng trong hai hệ thống cần phải thiết lập một liên kết logic. 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.

*Giao thức không liên kết*: Dữ liệu được truyền độc lập trên các tuyến khác nhau. Với các giao thức không liên kết chỉ có giai đoạn duy nhất truyền dữ liệu.

### 2.3.3 Truyền dữ liệu trong mô hình OSI




| Tầng | Header | | Tên dữ liệu |
|---|---|---|---|
| Application | $H_A$ | Application Header | Message & Packet |
| Presentation | $H_P$ | Presentation Header | Packet |
| Session | $H_S$ | Session Header | Packet |
| Transport | $H_T$ | Transport Header | Datagram,Segment & Packet |
| Network Header | $H_N$ | Network Header | Datagram & Packet |
| Data Link | $H_D$ | Data Link Header | Frame & Packet |
| Physical | | Physical | Bit |

**Hình 2.9: Bổ sung phần đầu thông điệp & tên dữ liệu sử dụng**

### 2.3.4. Vai trò và chức năng chủ yếu các tầng

*Vai trò & chức năng tầng ứng dụng (Application Layer*) Xác định giao diện giữa người sử dụng và môi trường OSI. Bao gồm nhiều giao thức ứng dụng cung cấp các phương tiện cho người sử dụng truy cập vào môi trường mạng và cung cấp các dịch vụ phân tán. Khi các thực thể ứng dụng AE (Application Entity) được thiết lập, nó sẽ gọi đến các phần tử dịch vụ ứng dụng ASE (Application Service Element). Mỗi thực thể ứng dụng có thể gồm một hoặc nhiều các phần tử dịch vụ ứng dụng. Các phần tử dịch vụ ứng dụng được phối hợp trong môi trường của thực thể ứng dụng thông qua các liên kết gọi là đối tượng liên kết đơn SAO (Single Association Object). SAO điều khiển việc truyền thông và cho phép tuần tự hóa các sự kiện truyền thông.

*Vai trò & chức năng tầng trình bày (Presentation Layer*): Tầng trình bày giải quyết các vấn đề liên quan đến cú pháp và ngữ nghĩa của thông tin được truyền. Biểu diễn thông tin người sử dụng phù hợp với thông tin làm việc của mạng và ngược lại. Thông thường biểu diễn thông tin các ứng dụng nguồn và ứng dụng đích có thể khác nhau bởi các ứng dụng được chạy trên các hệ thống có thể khác nhau. Tầng trình bày phải chịu trách nhiệm chuyển đổi dữ liệu gửi đi trên mạng từ một loại biểu diễn này sang một loại khác. Để đạt được điều đó nó cung cấp một dạng biểu diễn truyền thông chung cho phép chuyển đổi từ dạng biểu diễn cục bộ sang biểu diễn chung và ngược lại.

*Vai trò & chức năng tầng phiên (Session Layer)***:** Tầng phiên cho phép người sử dụng trên các máy khác nhau thiết lập, duy trì, huỷ bỏ và đồng bộ phiên truyền thông giữa họ với nhau. Nói cách khác tầng phiên thiết lập "các giao dịch" giữa các thực thể đầu cuối.

Dịch vụ phiên cung cấp một liên kết giữa 2 đầu cuối sử dụng dịch vụ phiên sao cho trao đổi dữ liệu một cách đồng bộ và khi kết thúc thì giải phóng liên kết. Sử dụng thẻ bài (Token) để thực hiện truyền dữ liệu, đồng bộ hóa và hủy bỏ liên kết trong các phương thức truyền đồng thời hay luân phiên. Thiết lập các điểm đồng bộ hóa trong hội thoại. Khi xảy ra sự cố có thể khôi phục hội thoại bắt đầu từ một điểm đồng bộ hóa đã thỏa thuận.

*Vai trò & chức năng tầng vận chuyển (Transport Layer):* Là tầng cao nhất có liên quan đến các giao thức trao đổi dữ liệu giữa các hệ thống mở, kiểm soát việc truyền dữ liệu từ mút tới mút (End- to -End). Thủ tục trong 3 tầng dưới (vật lý, liên kết dữ liệu và mạng) chỉ phục vụ việc truyền dữ liệu giữa các tầng kề nhau trong từng hệ thống. Các thực thể đồng tầng hội thoại, thương lượng với nhau trong quá trình truyền dữ liệu.

Tầng vận chuyển thực hiện việc chia các gói tin lớn thành các gói tin nhỏ hơn trước khi gửi đi và đánh số các gói tin và đảm bảo chúng chuyển theo đúng thứ tự. Là tầng cuối cùng chịu trách nhiệm về mức độ an toàn trong truyền dữ liệu nên giao thức tầng vận chuyển phụ thuộc nhiều vào bản chất của tầng mạng. Tầng vận chuyển có thể thực hiện việc ghép kênh (multiplex) một vài liên kết vào cùng một liên kết nối để giảm giá thành.

*Vai trò & chức năng tầng mạng (Network Layer)*: Thực hiện các chức năng *chọn đường (Routing* đi cho các gói tin từ nguồn tới đích có thể trong cùng một mạng hoặc khác mạng nhau. Đường có thể được cố định, cũng có thể được định nghĩa khi bắt đầu hội thoại và có thể đường đi là động (Dynamic) có thể thay đổi với từng gói tin tuỳ theo trạng thái tải tức thời của mạng. Trong mạng kiểu quảng bá (Broadcast) routing rất đơn giản.

Một chức năng quan trọng khác của tầng mạng là chức năng *điều khiển tắc nghẽn (Congestion Control)*. Nếu có quá nhiều gói tin cùng lưu chuyển trên cùng một đường thì có thể xảy ra tình trạng tắc nghẽn. Thực hiện chức năng *giao tiếp giữa các mạng* khi các gói tin đi từ mạng này sang mạng khác để tới đích.

*Vai trò & chức năng tầng liên kết dữ liệu (Data link Layer):* Chức năng chủ yếu của tầng liên kết dữ liệu là thực hiện thiết lập các liên kết, duy trì và huỷ bỏ các liên kết dữ liệu. Kiểm soát lỗi và kiểm soát lưu lượng.

Chia thông tin thành các khung thông tin (Frame), truyền các khung tuần tự và xử lý các thông điệp xác nhận (Acknowledgement Frame) từ bên máy thu gửi về. Tháo gỡ các khung thành chuỗi bít không cấu trúc chuyển xuống tầng vật lý. Tầng 2 bên thu, tái tạo chuỗi bít thành các khung thông tin. Đường truyền vật lý có thể gây lỗi, nên tầng liên kết dữ liệu phải giải quyết vấn đề kiểm soát lỗi, kiểm soát luồng, kiểm soát lưu lượng, ngăn không để nút nguồn gây " ngập lụt" dữ liệu cho bên thu có tốc độ thấp hơn. Trong các mạng quảng bá, tầng con MAC (Medium Acces Sublayer) điều khiển việc truy nhập đường truyền.

*Vai trò & chức năng tầng Vật lý (Physical layer):* Tầng vật lý là tầng thấp nhất trong mô hình 7 lớp OSI. Các thực thể tầng giao tiếp với nhau qua một đường truyền vật lý. Tầng vật lý xác định các chức năng, thủ tục về điện, cơ, quang để kích hoạt, duy trì và giải phóng các kết nối vật lý giữa các hệ thống mạng. Cung cấp các cơ chế về điện, cơ hàm, thủ tục ...nhằm thực hiện việc kết nối các phần tử của mạng thành một hệ thống bằng các phương pháp vật lý. Đảm bảo cho các yêu cầu về chuyển mạch hoạt động nhằm tạo ra các đường truyền thực cho các chuỗi bit thông tin. Các chuẩn trong tầng vật lý là các chuẩn xác định giao diện người sử dụng và môi trường mạng. Các giao thức tầng vật lý có hai loại truyền dị bộ (Asynchronous) và truyền đồng bộ (Synchronous).

Tóm tắt chức năng các tầng như sau:

| 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 |

## 2.4. Một số kiến trúc khác

### 2.4.1. 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. Giao thức định nghĩa các quy tắc, các tiến trình cho sự tương tác giữa các thành phần trong mạng như máy tính, terminal và phần mềm.

- Mạng SNA sử dụng kiến trúc 6 tầng: tầng1- Physical Control (X21,RS-232), tầng 2-Data Link Control (SDLC) , tầng 3- Path Control (chọn đường và kiểm soát dữ liệu), tầng 4 - Transmission Control (kiểm soát truyền), tầng 5- Data Flow Control (kiểm soát luồng) và tầng 6 - Function Management (quản trị).

- 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.

### 2.4.2. Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX)

Giao thức IPX/SPX được công ty Novell thiết kế sử dụng cho các sản phẩm mạng của chính hãng. SPX hoạt động trên tầng Transport của OSI, có chức năng bảo đảm độ tin cậy của liên kết truyền thông từ mút đến mút. Nó đảm bảo chuyển giao các gói tin đúng trình tự, đúng đích nhưng không có vai trò trong định tuyến. IPX tuân theo chuẩn OSI, hoạt động tầng mạng, chịu trách nhiệm thiết lập địa chỉ cho các thiết bị mạng. Nó là giao thức định tuyến, kết hợp với các giao thức Routing Information Protocol (RIP) và Netware Link Services Protocol (NLSP) để trao đổi thông tin định tuyến với các bộ định tuyến lân cận.

### 2.4.3. AppleTalk

Là kiến trúc mạng do hãng Apple Computer phát triển cho họ các máy tính cá nhân Macintosh. Giao thức AppleTalk cũng được phát triển trên tầng vật lý của Ethernet và Token Ring.

- Các vùng tối đa trên một phân mạng: Phase 1 là 1; Phase 2 là 255 .

- Các node tối đa trên mỗi mạng: Phase 1: 254; Phase 2: khoảng 16 triệu.

- 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.

- Định tuyến Split-horizon: Phase 1: không; Phase 2: có.

### 2.4.4. Digital Network Architectur (DNA)

Kiến trúc mạng DNA là sản phẩm của hãng Digital Equipment Corporation. Đặc biệt Digital kết hợp với các hãng Intel và Xerox phát triển các phiên bản Ethernet, trong đó có Ethernet Version 2.

### 2.4.5. Họ IEEE 802 (Institute of Electrical and Electronic Engineer)

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

- Chuẩn IEEE 802.2 định nghĩa một tầng con LLC được giao thức tầng dưới sử dụng. Giao thức tầng mạng có thể thiết kế độc lập với tầng vật lý.

- Giao thức tầng dưới: 802.3 (1Base5, 10Base5, 10Base2, 10Basef, 10Broad36, 10BaseT, 10BaseX), 802.4 (TokenBus), 802.5 (Token Ring) , 802.6 , 802.9, 802.11, 802.12.

### 2.4.6. TCP/IP (Transmission Control Protocol/Internet Protocol)

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, mang 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 .

## Câu hỏi trắc nghiệm

1. Các phát biểu nào về nguyên tắc phân tầng là đúng
   A. Chức năng các tầng độc lập với nhau và có tính mở.
   B. Xác định mối quan hệ giữa các tầng kề nhau
   C. Xác định mối quan hệ giữa các đồng tầng
   D. Dữ liệu không truyền trực tiếp giữa các tầng đồng hệ thống (trừ tầng vật lý).
   E. Cả 4 phát biểu đều đúng.
2. Kiến trúc mạng (Network Architecture) là:
   A. Giao diện Interface giữa 2 tầng kề nhau.
   B. Giao thức tầng- quan hệ đồng tầng
   C. Số lượng tâng.
   D. Dịch vụ tầng.
   E. Tập các giao diện, số lượng tâng và giao thức tầng- quan hệ đồng tầng
3. Điểm truy nhập dịch vụ SAP (Service Access Point) là gì ?
   A. Nơi trao cung cấp dịch vụ các tầng kề nhau.
   B. Nơi hoạt động của các dịch vụ.
   C. Nơi cung cấp dịch vụ của tầng dưới cho các hoạt động tầng trên.
4. Những phát biểu nào đúng:

A. 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.
B. Các dịch vụ nguyên thuỷ là các thủ tục trao đổi thông tin.
C. Các hàm dịch vụ nguyên thủy tương tác giữa các tầng kề nhau.
D. Các hàm dịch vụ nguyên thủy đặc tả các thao tác thực hiện yêu cầu hay trả lời một yêu cầu của các thực thể đồng tầng.

5. Tầng nào xác định giao diện giữa người sử dụng và môi trường OSI.
   A. Tầng ứng dụng
   B. Tầng trình bày
   C. Tầng phiên
   D. Tầng vận chuyển
6. Tầng nào cung cấp một dạng biểu diễn truyền thông chung cho phép chuyển đổi từ dạng biểu diễn cục bộ sang biểu diễn chung và ngược lại.
   A. Tầng mạng
   B. Tầng trình bày
   C. Tầng phiên
   D. Tầng vật lý
7. Tầng nào thiết lập, duy trì, huỷ bỏ "các giao dịch" giữa các thực thể đầu cuối.
   A. Tầng mạng
   B. Tầng liên kết dữ liệu
   C. Tầng phiên
   D. Tầng vật lý
8. Tầng nào có liên quan đến các giao thức trao đổi dữ liệu
   A. Tầng mạng
   B. Tầng vận chuyển
   C. Tầng liên kết dữ liệu
   D. Tầng vật lý
9. Những thuật ngữ nào dùng để mô tả các đơn vị dữ liệu sử dụng trong tầng liên kết dữ liệu:
   A. Datagram.
   B. Packet.(*)
   C. Message
   D. Frame (*)
10. Tầng nào thay đổi, duy trì tuyến kết nối giữa các thiết bị truyền thông.
    A. Tầng vật lý.
    B. Tầng con MAC.
    C. Tầng con LLC(*)

D. Tầng mạng.

11. Phương pháp chuyển mạch nào sử dụng mạch ảo ?.
    A. Message.
    B. Packet(*).
    C. Bit
    D. Circuit Switching
12. Tầng nào thực hiện mã hoá dữ liệu?
    A. Tầng mạng
    B. Tầng vận chuyển.
    C. Tầng liên kết dữ liệu.
    D. Tầng phiên.
    E. Tầng ứng dụng
    F. Tầng trình bày.(*)
13. Tầng nào thực hiện bàn giao các thông điệp giữa các tiến trình trên các thiết bị?
    A. Tầng mạng.
    B. Tầng vận chuyển.(*).
    C. Tầng liên kết dữ liệu..
    D. Tầng phiên.
    E. Tầng ứng dụng.
14. Tầng nào thực hiện việc phân giải địa chỉ/tên?
    A. Tầng mạng.
    B. Tầng vận chuyển.(*).
    C. Tầng liên kết dữ liệu..
    D. Tầng ứng dụng
15. Khẳng định nào đúng:
    A. Băng thông mạng hiệu suất cao khi sử dụng kỹ thuật chọn đường DIJKTRA.
    B. Băng thông mạng hiệu suất cao khi sử dụng kỹ thuật chọn đường BellMan Ford (*).
    C. Cả hai kết hợp.
16. Hoạt động nào có liên quan đến ID giao kết
    A. Chuyển mạch gói.
    B. Định tuyến.
    C. Phát triển phân đoạn.(*)
    D. Điều khiển luồng
17. Khẳng định nào đúng:
    A. Tầng liên kết dữ liệu xử lý lưu thông giữa các thiết bị.(*).
    B. Tầng mạng xử lý lưu thông giữa các tiến trình của tầng trên..

C. Tầng lvận chuyển xử lý lưu thông giữa các thiết bị đầu cuối.(*)

D. Tất cả đều đúng.

18. Điều khiển cuộc liên lạc là chức năng của tầng:

A. Vật lý.

B. Tầng mạng.

C. Tầng phiên.(*)

D. Tầng trình bày.

19. Chức năng điều khiển phiên làm việc của một cuộc liên lạc là:

A. Thiết lập tuyến liên kết.(*).

B. Phát hiện lỗi bằng CheckSum.

C. Chuyển giao dữ liệu.(*)

D. Giải phóng các liên kết.(*)

20. Chức năng của việc thiết lập liên kết:

A. Bắt đầu khi phiên truyền thông bị gián đoạn.

B. Xác minh tên đăng nhập và mật khẩu.(*)

C. Xác định các dịch vụ cần thiết.(*).

D. Phát tín hiệu báo nhận dữ liệu.

21. Chức năng của tầng trình bày:

A. Mã hoá dữ liệu.(*).

B. Trình bày dữ liệu trên các thiết bị hiển thị.

C. Phiên dịch dữ liệu.(*)

D. Chuyển đổi dạng thức hiển thị.

22. Chức năng của tầng ứng dụng

A. Dịch vụ in mạng.(*).

B. Các ứng dụng của người sử dụng đầu cuối.

C. Hệ khách truy nhập các dịch vụ mạng.(*)

D. Quảng cáo các dịch vụ.(*).

23. Đúng hay sai khẳng định sau: Trong mạng LAN hình BUS, mỗi một máy trên BUS đều có địa chỉ riêng, nhiều máy có thể đồng thời gửi dữ liệu lên mạng mà vẫn đảm bảo được dữ liệu sẽ đến đích?

24. Mô hình tham khảo OSI chia hoạt động truyền thông thành..... tầng.

25. Mục đích của mỗi một tầng là cung cấp các dịch vụ cho tầng ..... và bảo vệ cho tầng ..... khỏi những chi tiết về cách thức dịch vụ được thực hiện. Trong mỗi tầng, các gói dữ liệu được bổ sung thêm thông tin điều khiển, đó là các thông tin về.....

26. Mỗi một tầng hoạt động giao tiếp với .....tầng.... ..

27. Tầng ..... quyết định đường đi của dữ liệu từ node nguồn đến node đích.

28. Tầng Data Link chịu trách nhiệm gửi..... từ tầng Network xuống tầng Physical.
29. Thông tin ..... trong khung dữ liệu (Frame) được sử dụng chỉ rõ loại khung, đường đi và thông tin về phân đoạn.
30. Tầng con ..... giao tiếp trực tiếp với Card mạng và chịu trách nhiệm chuyển giao dữ liệu không lỗi giữa hai máy tính trên mạng.
31. Dữ liệu được phân chia thành nhiều .... nhỏ để ..... xử lý dễ dàng.
32. Nhiều giao thức phối hợp cùng thực hiện hoạt động truyền thông, gọi là.....
33. Sự liên kết ..... sẽ cho biết ..... của tầng nào đang hoạt động.
34. Có ba kiểu giao thức ứng với mô hình OSI, đó là các loại giao thức....
35. Giao thức ứng dụng hoạt động trên tầng cao nhất và cung cấp trao đổi dữ liệu giữa các chương trình ứng dụng. ?
36. Khi gói dữ liệu được truyền giữa các bộ định tuyến với nhau, địa chỉ nguồn và đích của tầng Data Link bị loại bỏ và _____
    A. Sau đó được tạo lại.
    B. tiếp tục được gửi riêng để rồi sẽ được tái tạo tại node đích.
    C. Các gói tin được chuyển tiếp dựa trên độ dài tính bằng Byte
    D. Gói tin được truyền tiếp dựa trên mức độ ưu tiên.
37. Chuyển tiếp gói dữ liệu dựa trên địa chỉ tầng con MAC (Media Access Control_____
    A. Bộ chuyển tiếp
    B. Cổng giao tiếp
    C. SONET.
    D. SMDS
    E. Cầu nối (Bridge)
38. Tập hợp các giao thức mạng chuyển mạch gói_____
    A. Bộ chuyển tiếp
    B. Cổng giao tiếp
    C. SONET.
    D. X25
39. Liên kết nhiều mạng sử dụng các giao thức khác nhau_____
    A. Bộ chuyển tiếp
    B. Cổng giao tiếp
    C. SONET.
    D. Bộ định tuyến.

## Câu hỏi và bài tập

1. Hãy cho biết ý nghĩa của khuyến nghị loại V, khuyến nghị loại X và loại I.
2. Tổng quát về khái niệm kiến trúc đa tầng và các quy tắc phân tầng

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

CHƯƠNG TRÌNH ĐÀO TẠO ĐẠI HỌC TỪ XA PTIT

# CHƯƠNG 3: MẠNG INTERNET VÀ GIAO THỨC TCP/IPv4

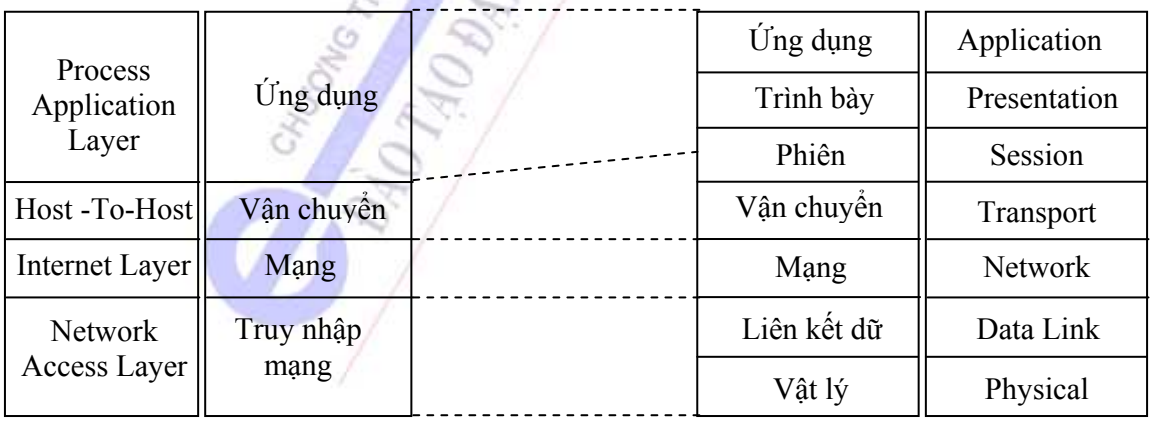
Nội dung của chương sẽ giới thiệu tổng quát về mạng Internet và kiến trúc mô hình TCP/IP. Bộ giao thức TCP/IP đã trở thành chuẩn chung cho mạng máy tính toàn cầu. Tìm hiểu về chồng giao thức TCP/IP sẽ cung cấp những kiến thức cơ bản về các thành phần giao thức khác nhau cần thiết cho các ứng dụng TCP/IP trên nền các hệ điều hành mạng. Phần cuối của chương sẽ trình bày những hạn chế của IPv4 và sự cần thiết ra đời giao thức IPv6. Nội dung của chương bao gồm:

- Giới thiệu mô hình kiến trúc TCP/IP.
- Một số giao thức cơ bản của bộ giao thức TCP/IP
- Một số hạn chế của giao thức IPv4 và nguyên nhân ra đời IPv6
- Các lớp địa chỉ IPv6

## 3.1. Mô hình TCP/IP

TCP/IP (Transmission Control Protocol/Internet Protocol) là chồng giao thức cùng hoạt động nhằm cung cấp các phương tiện truyền thông liên mạng. Năm 1981, TCP/IP phiên bản 4 (IPv4) được hoàn thành và sử dụng phổ biến trên máy tính sử dụng hệ điều hành UNIX, trở thành một trong những giao thức cơ bản của hệ điều hành Windows 9x. Năm 1994, một phiên bản mới IPv6 được hình thành trên cơ sở cải tiến những hạn chế của IPv4.

### 3.1.1. Mô hình kiến trúc TCP/IP



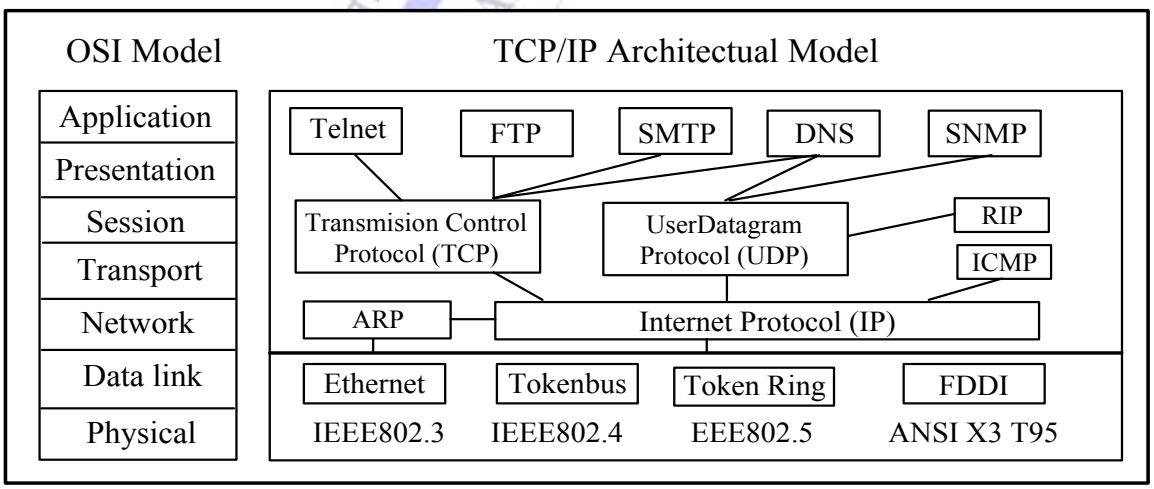

**Hình 3.1 Tương quan Mô hình OSI và mô hình TCP/IP**

### 3.1.2. Vai trò và chức năng các tầng trong mô hình TCP/IP

*Tầng ứng dụng (Process/Application Layer):* Ứng với các tầng Session, Presentation và Aplication trong mô hình OSI. Tầng ứmg dụng hỗ trợ các ứng dụng cho các giao thức tầng Host to Host. Cung cấp giao diện cho người sử dụng mô hình TCP/IP. Các giao thức ứng dụng gồm TELNET(truy nhập từ xa), FTP (truyền File), SMTP (thư điện tử),.....

*Tầng vận chuyển Host to Host:* Ứng với tầng vận chuyển (Transport Layer) trong mô hình OSI, tầng Host to Host 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) và giao thức dữ liệu người sử dụng UDP (User Datagram Protocol).Giao thức TCP 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, tính đồng thời và kết nối song công (Full Duplex). Khái niệm tin độ cậy cao nghĩa là TCP kiểm soát lỗi bằng cách truyền lại các gói tin bị lỗi. Giao thức TCP cũng hỗ trợ những kết nối đồng thời. Nhiều kết nối TCP có thể được thiết lập tại một máy chủ và dữ liệu có thể được truyền đi một cách đồng thời và độc lập với nhau trên các kết nối khác nhau. TCP cung cấp kết nối song công (Full Duplex), dữ liệu có thể được trao đổi trên một kết nối đơn theo 2 chiều. Giao thức UDP được sử dụng cho những ứng dụng không đòi hỏi độ tin cậy cao.

*Tầng mạng (Internet Layer):*Ứng với tầng mạng (Network Layer) trong mô hình OSI, tầng mạng cung cấp một địa chỉ logic cho giao diện vật lý mạng. Giao thức thực hiện của tầng mạng trong mô hình DOD là giao thức IP kết nối không liên kết (Connectionless), là hạt nhân hoạt động của Internet. Cùng với các giao thức định tuyến RIP, OSPF, BGP, tầng tầng mạng IP cho phép kết nối một cách mềm dẻo và linh hoạt các loại mạng "vật lý" khác nhau như: Ethernet, Token Ring, X.25... Ngoài ra tầng này còn 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). Các vấn đề có liên quan đến chuẩn đoán lỗi và các tình huống bất thường liên quan đến IP được giao thức ICMP (Internet Control Message Protocol) thống kê và báo cáo. Tầng trên sử dụng các dịch vụ do tầng Liên mạng cung cấp.

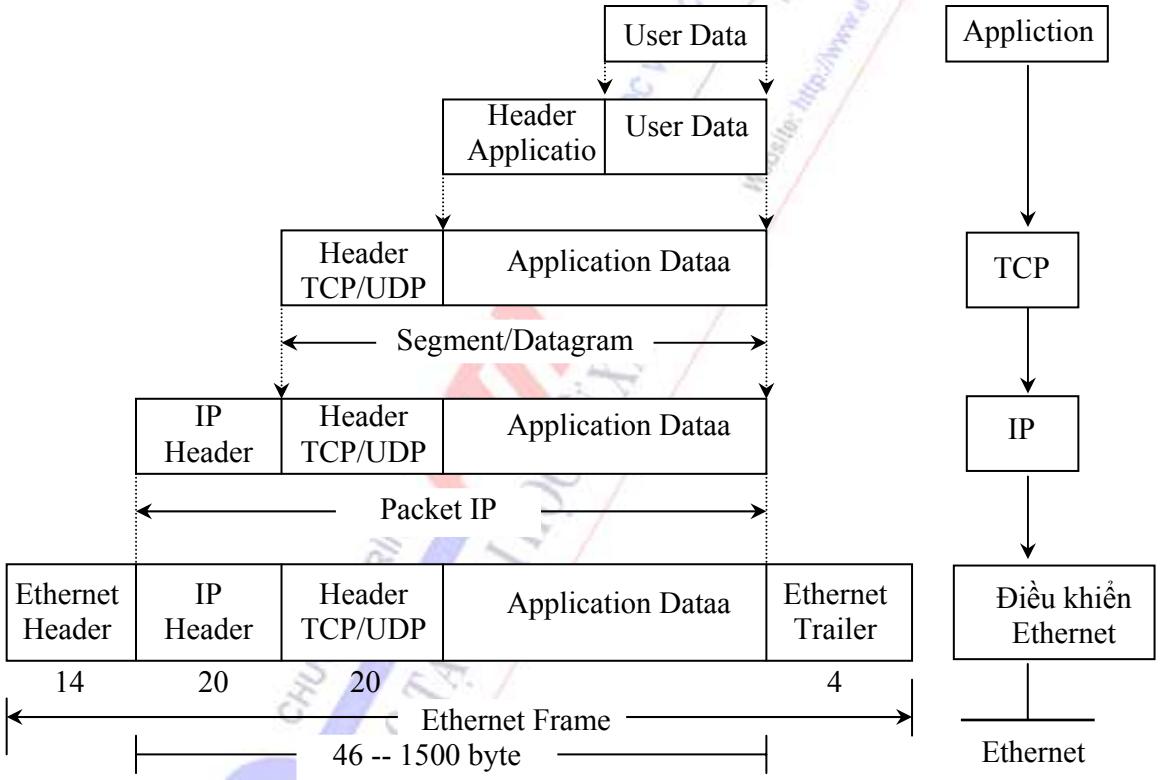



**Hình 3.2 Mô hình OSI và mô hình kiến trúc của TCP/IP**

*Tầng tầng truy nhập mạng (Network Access Layer):* Tương ứng với tầng Vật lý và Liên kết dữ liệu trong mô hình OSI, tầng truy nhập mạng cung cấp các phương tiện kết nối vật lý cáp, bộ chuyển đổi (Transceiver), Card mạng, giao thức kết nối, giao thức truy nhập đường truyền như CSMA/CD, Tolen Ring, Token Bus..). Cung cấp các dịch vụ cho tầng Internet phân đoạn dữ liệu thành các khung.

### 3.1.3. Quá trình đóng gói dữ liệu Encapsulation

Cũng như mô hình OSI, trong mô hình kiến trúc TCP/IP mỗi tầng có một cấu trúc dữ liệu riêng, độc lập với cấu trúc dữ liệu được dùng ở tầng trên hay tầng dưới kề nó. Khi dữ liệu được truyền từ tầng ứng dụng cho đến tầng vật lý, qua mỗi tầng được thêm phần thông tin điều khiển (Header) đặt trước phần dữ liệu được truyền, đảm bảo cho việc truyền dữ liệu chính xác. Việc thêm Header vào đầu các gói tin khi đi qua mỗi tầng trong quá trình truyền dữ liệu được gọi là *Encapsulation*. Quá trình nhận dữ liệu sẽ diễn ra theo chiều ngược lại, khi qua mỗi tầng, các gói tin sẽ tách thông tin điều khiển thuộc nó trước khi chuyển dữ liệu lên tầng trên.




**Hình 3.3 Đóng gói dữ liệu khi chuyển xuống tầng kề dưới**

- Process/Application Layer: Message (Thông điệp )
- Host - To- Host Layer: Segment/ Datagram (Đoạn/Bó dữ liệu)
- Internet Layer: Packet (Gói dữ liệu)
- Network Layer: Frame (Khung dữ liệu).

### 3.1.4. Quá trình phân mảnh dữ liệu Fragment

Dữ liệu có thể được truyền qua nhiều mạng khác nhau, kích thước 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). Trong quá trình đóng gói *Encapsulation,* nếu kích thước của một gói lớn hơn kích thước cho phép, tự động chia thành nhiều gói nhỏ và thêm thông tin điều khiển vào mỗi gói. Nếu một mạng nhận dữ liệu từ một mạng khác, kích thước gói dữ liệu 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 *Fragment*.

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 bị mất 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.

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

### 3.2.1. Giao thức gói tin người sử dụng UDP (User Datagram Protocol)

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. Nó cung cấp cơ chế gán và quản lý các số hiệu cổng để định danh duy nhất cho các ứng dụng chạy trên một Client của mạng và thực hiện việc ghép kênh. 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. Các mạng IP sử dụng hai loại giao thức định tuyến: định tuyến vectơ khoảng cách và định tuyến trạng thái liên kết. Hệ thống đảm bảo tính năng thời gian thực, tốc độ truyền cao, các gói thoại không có trễ quá mức và độ tin cậy cao.

### 3.2.2. Giao thức điều khiển truyền TCP (Transmission Control Protocol)

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 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. 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).

TCP có những đặc điểm sau:

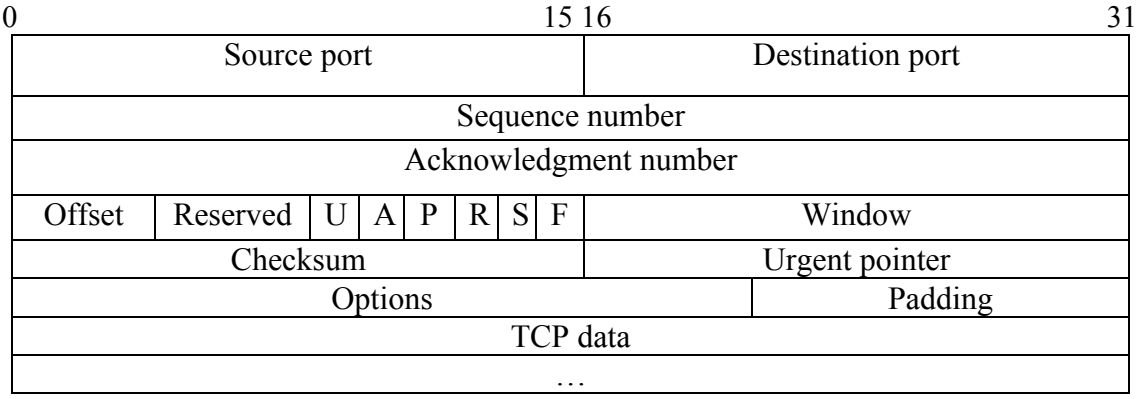
- Hai thực thể liên kết với nhau phải trao đổi, đàm phán với nhau về các thông tin liên kết. Hội thoại, đàm phán nhằm ngăn chặn sự tràn lụt và mất dữ liệu khi truyền.

- 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.

Cấu trúc gói tin TCP: Đơn vị dữ liệu sử dụng trong giao thức TCP được gọi là Segment. Khuôn dạng và nội dung của gói tin TCP được biểu diễn như sau




**Hình 3.4 Cấu trúc gói tin TCP (TCP Segment)**

- Cổng nguồn (Source Port): 16 bít, số hiệu cổng nguồn.

- Cổng đích (Destination Port): Độ dài 16 bít, chứa số hiệu cổng đích.

- Sequence Number: 32 bits, số thứ tự của gói số liệu khi phát.

- Acknowlegment Number (32 bits), Bên thu xác nhận thu được dữ liệu đúng.

- Offset (4 bits): Độ dài Header gói tin TCP.

- Reserved (6 bít) lưu lại: Lấp đầy bằng 0 để dành cho tương lai.

- Control bits: Các bits điều khiển

URG : Vùng con trỏ khẩn có hiệu lực.

ACK : Vùng báo nhận (ACK number) có hiệu lực .

PSH: Chức năng PUSH.

RST: Khởi động lại (reset) liên kết.

SYN : Đồng bộ các số liệu tuần tự (sequence number).

FIN : Không còn dữ liệu từ trạm nguồn .

- Window (16bits): Số lượng các Byte dữ liệu trong vùng cửa sổ bên phát.
- Checksum (16bits): Mã kiểm soát lỗi (theo phương pháp CRC).
- Urgent Pointer (16 bits): Số thứ tự của Byte dữ liệu khẩn, khi URG được thiết lập .
- Option (độ dài thay đổi): Khai báo độ dài tối đa của TCP Data trong một Segment .
- Padding (độ dài thay đổi): Phần chèn thêm vào Header.

Việc kết hợp địa chỉ IP của một máy trạm và số cổng được sử dụng tạo thành một Socket. Các máy gửi và nhận đều có Socket riêng. Số Socket là duy nhất trên mạng.

*Điều khiển lưu lượng và điều khiển tắc nghẽn*

Cơ chế cửa sổ động là một trong các phương pháp điều khiển thông tin trong mạng máy tính. Độ lớn của cửa sổ bằng số lượng các gói dữ liệu được gửi liên tục mà không cần chờ thông báo trả lời về kết quả nhận từng gói dữ liệu đó. Độ lớn cửa sổ quyết định hiệu suất trao đổi dữ liệu trong mạng. Nếu chọn độ lớn của sổ cao thì có thể gửi được nhiều dữ liệu trong cùng một đơn vị thời gian. Nếu truyền bị lỗi, dữ liệu phải gửi lại lớn thì hiệu quả sử dụng đường truyền thấp. Giao thức TCP cho phép thay đổi độ lớn của sổ một cách động, phụ thuộc vào độ lớn bộ đệm thu của thực thể TCP nhận.

Cơ chế phát lại thích nghi: Để đảm bảo kiểm tra và khắc phục lỗi trong việc trao đổi dữ liệu qua liên mạng, TCP phải có cơ chế đồng hồ kiểm tra phát (Time Out) và cơ chế phát lại (Retransmission) mềm dẻo, phụ thuộc vào thời gian trễ thực của môi trường truyền dẫn cụ thể. Thời gian trễ toàn phần RTT (Round Trip Time) được xác định bắt đầu từ thời điểm phát gói dữ liệu cho đến khi nhận được xác nhận của thực thể đối tác, là yếu tố quyết định giá trị của đồng hồ kiểm tra phát $T_{out}$. Như vậy $T_{out}$ phải lớn hơn hoặc bằng RTT.

Cơ chế điều khiển tắc nghẽn**:** Hiện tượng tắc nghẽn dữ liệu thể hiện ở việc gia tăng thời gian trễ của dữ liệu khi chuyển qua mạng. Để hạn chế khả năng dẫn đến tắc nghẽn dữ liệu trong mạng, điều khiển lưu lượng dựa trên việc thay đổi độ lớn của sổ phát.

*Thiết lập và huỷ bỏ liên kết:* TCP là một giao thức hướng liên kết, tức là cần phải thiết lập một liên kết giữa một cặp thực TCP trước khi truyền dữ liệu. Sau khi liên kết được thiết lập, những giá trị cổng (Port) hoạt động như một nhận dạng logic được sử dụng nhận dạng mạch ảo (Virtual Circuit).Trên kênh ảo dữ liệu được truyền song công (Full Duplex). Liên kết TCP được duy trì trong thời gian truyền dữ liệu. Kết thúc truyền, liên kết TCP được giải phóng, các tài nguyên như bộ nhớ, các bảng trạng thái.. cũng được giải phóng.

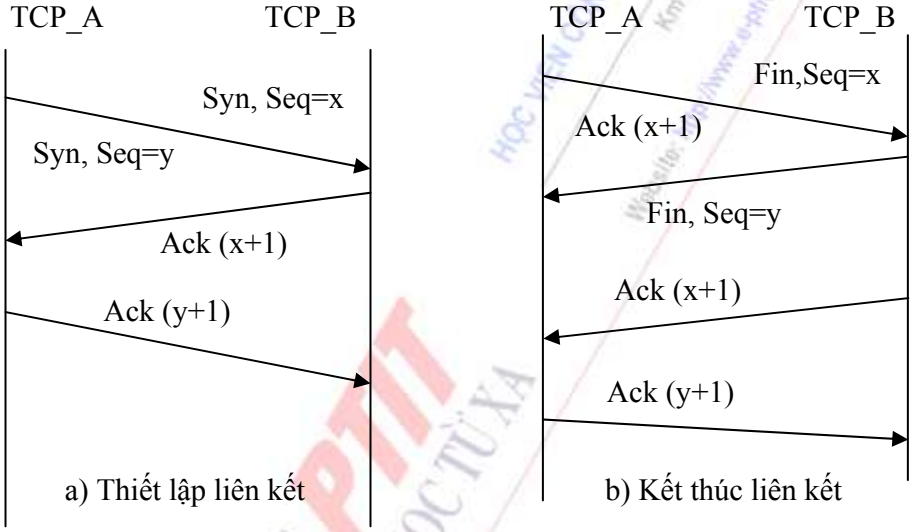
Thiết lập liên kết TCP: Được thực hiện trên cơ sở phương thức bắt tay ba bước (Tree - Way Handsake):

Bước 1: Như hình 3.7 yêu cầu liên kết luôn được trạm nguồn khởi tạo tiến trình bằng cách gửi một gói TCP với cờ SYN=1 và chứa giá trị khởi tạo số tuần tự ISN của Client. Giá trị ISN này là một số 4 byte không dấu và được tăng mỗi khi liên kết được yêu cầu (giá trị này quay về 0 khi nó tới giá trị 232). Trong thông điệp SYN này còn chứa số hiệu cổng TCP của phần mềm dịch vụ mà tiến trình trạm muốn liên kết.

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

Bước 2: Khi thực thể TCP của phần mềm dịch vụ nhận được thông điệp SYN, nó gửi lại gói SYN cùng giá trị ISN của nó và đặt cờ ACK=1 trong trường hợp sẵn sàng nhận liên kết . Thông điệp này còn chứa giá trị ISN của tiến trình trạm trong trường hợp số tuần tự nhận để báo rằng thực thể dịch vụ đã nhận được giá trị ISN của tiến trình trạm.

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




**Hình 3.5 Quá trình thiết lập và kết thuc liên kết TCP 3 bước**

*Kết thúc liên kết:* Khi có nhu cầu kết thúc liên kết TCP, ví dụ A gửi yêu cầu kết thúc liên kết với FIN=1. Vì liên kết TCP là song công (Full-Duplex) nên mặc dù nhận được yêu cầu kết thúc liên kết của A, thực thể B vẫn có thể tiếp tục truyền cho đến khi B không còn số liệu để gửi và thông báo cho A bằng yêu cầu kết thúc liên kết với FIN=1. Khi thực thể TCP đã nhận được thông điệp FIN và sau khi đã gửi thông điệp FIN của mình, liên kết TCP thực sụ kết thúc. Như vậy cả hai trạm phải đồng ý giải phóng liên kết TCP bằng cách gửi cờ FIN=1 trước khi chấm dứt liên kết xẩy ra, việc này bảo đảm dữ liệu không bị thất lạc do đơn phương đột ngột chấm dứt liên lạc.

*Truyền và nhận dữ liệu* Sau khi liên kết được thiết lập giữa một cặp thực thể TCP, các thực thể truyền dữ liệu. Liên kết TCP dữ liệu có thể được truyền theo hai hướng. Khi nhận một khối dữ liệu cần chuyển đi từ người sử dụng, TCP sẽ lưu trữ tại bộ đệm. Nếu cờ PUST được xác lập thì toàn bộ dữ liệu trong bộ đệm sẽ được gửi đi dưới dạng TCP Segment. Nếu PUST không được xác lập thì dữ liệu trong bộ đệm vẫn chờ gửi đi khi có cơ hội thích hợp.

Bên nhận, dữ liệu sẽ được gửi vào bộ đệm. Nếu dữ liệu trong đệm được đánh dấu bởi cờ PUST thì toàn bộ dữ liệu trong bộ đệm sẽ được gửi lên cho người sử dụng. Ngược lại, dữ liệu vẫn được lưu trong bộ đệm. Nếu dữ liệu khẩn cần phải chuyển gấp thì cờ URGENT được xác lập và đánh dấu dữ liệu bằng bit URG để báo dữ liệu khẩn cần được chuyển gấp.

### 3.2.3. Giao thức mạng IP (Internet Protocol)

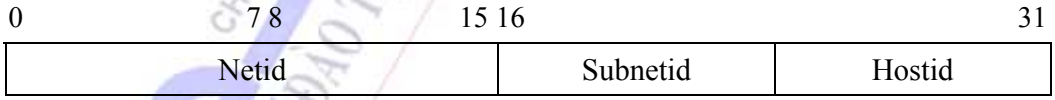
*Các chức năng chính của IP:* IP (Internet Protocol) là giao thức không liên kết. Chức năng chủ yếu của IP là cung cấp các dịch vụ Datagram và các khả năng kết nối các mạng con thành liên mạng để truyền dữ liệu với phương thức chuyển mạch gói IP Datagram, thực hiện tiến trình định địa chỉ và chọn đường.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

*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.

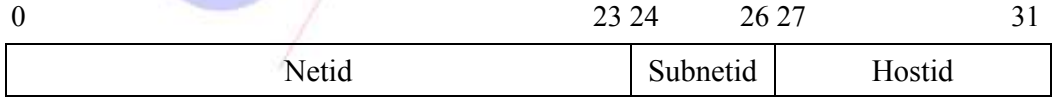
Địa chỉ IP được chia thành 5 lớp ký hiệu là A, B, C, D, E với cấu trúc mỗi lớp được xác định. Các bit đầu tiên của byte đầu tiên được dùng để định danh lớp địa chỉ (0-lớp A, 10 - lớp B, 110 - lớp C, 1110 - lớp D, 11110 - lớp E).

- 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.


- Lớp B cho phép định danh tới 16384 mạng con, với tối đa 65535 Host trên mỗi mạng. Dạng địa chỉ của lớp B: (Network number. Network number.Host.Host).




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




- 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.

| 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 |

**Hình 3.6: Cấu trúc các lớp địa chỉ IP**

*Cấu trúc gói dữ liệu IP:* Các gói dữ liệu IP được gọi là các Datagram. Mỗi Datagram có phần tiêu đề (Header) chứa các thông tin điều khiển. Nếu địa chỉ IP đích cùng mạng với trạm nguồn thì các gói dữ liệu sẽ được chuyển thẳng tới đích, nếu địa chỉ IP đích không cùng mạng IP với máy nguồn thì các gói dữ liệu sẽ được gửi đến một máy trung chuyển IP Gateway để chuyển tiếp. IP Gateway là một thiết bị mạng IP đảm nhận việc lưu chuyển các gói dữ liệu IP giữa hai mạng IP khác nhau. Hình 3.3 mô tả cấu trúc gói IP.

- VER (4 bits): Version hiện hành của IP được cài đặt.
- IHL(4 bits): Internet Header Length của Datagram, tính theo đơn vị word (32 bits).
- Type of service(8 bits): Thông tin về loại dịch vụ và mức ưu tiên của gói IP:
- Total Length (16 bits): Chỉ độ dài Datagram,
- Identification (16bits): Định danh cho một Datagram trong thời gian sống của nó.
- Flags(3 bits): Liên quan đến sự phân đoạn (Fragment) các Datagram:
- Fragment Offset (13 bits): Chỉ vị trí của Fragment trong Datagram.
- Time To Live (TTL-8 bits): Thời gian sống của một gói dữ liệu.
- Protocol (8 bits): Chỉ giao thức sử dụng TCP hay UDP.
- Header Checksum (16 bits): Mã kiểm soát lỗi CRC(Cycle Redundancy Check).
- Source Address (32 bits): địa chỉ của trạm nguồn.
- Destination Address (32 bits): Địa chỉ của trạm đích.
- Option (có độ dài thay đổi): Sử dụng trong trường hợp bảo mật, định tuyến đặc biệt.
- Padding (độ dài thay đổi): Vùng đệm cho phần Header luôn kết thúc ở 32 bits
- Data (độ dài thay đổi): Độ dài dữ liệu tối đa là 65.535 bytes, tối thiểu là 8 bytes.

| | | | | |
|---|---|---|---|---|
| VERS | IHL | Service type | Toltal length | |
| Identification | | | Flags | Fragment offset |
| Time to live | | Protocol | Header checksum | |
| Source IP address | | | | |
| Destination IP address | | | | |
| IP options(may be none) | | | | Padding |
| IP Datagram data(up to 65535 bytes) | | | | |

**Hình 3.7 Cấu trúc gói dữ liệu IP**

*Phân mảnh và hợp nhất các gói IP:* Các gói IP được nhúng trong khung dữ liệu ở tầng liên kết dữ liệu tương ứng trước khi chuyển tiếp trong mạng. Một gói dữ liệu IP có độ dài tối đa 65.536 byte, trong khi hầu hết các lớp liên kết dữ liệu chỉ hỗ trợ các khung dữ liệu nhỏ hơn độ lớn tối đa của gói dữ liệu IP nhiều lần (ví dụ độ dài lớn nhất của một khung dữ liệu Ethernet là 1500 byte). Vì vậy cần thiết phải có cơ chế phân mảnh khi phát và hợp nhất khi nhận đối với các gói dữ liệu IP.

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

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

### 3.2.4. Giao thức thông báo điều khiển mạng ICMP(Internet Control Message Protocol)

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 của tầng IP, sử dụng để trao đổi các thông tin điều khiển dòng dữ liệu, thông báo lỗi và các thông tin trạng thái khác của bộ giao thức TCP/IP.

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

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

- Định hướng lại các tuyến (Redirect Router): Một Router gửi một thông điệp ICMP cho một trạm thông báo nên sử dụng Router khác. Thông điệp này có thể chỉ được dùng khi trạm nguồn ở trên cùng một mạng với hai thiết bị định tuyến.

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

| Nhóm | Loại bản tin | Type |
|---|---|---|
| Thông điệp truy vấn (ICMP Queries) | Hỏi và phúc đáp Echo (Echo Request và Echo Reply) | 8/0 |
| | Hỏi và phúc đáp nhãn thời gian (Timestamp Request và Timestamp Reply) | 13/14 |
| | Yêu cầu và phúc đáp mặt nạ địa chỉ (Address mask Request và Address mask Reply) | 17/18 |
| | Yêu cầu và quảng bá bộ định tuyến (Router soliciation và Router advertisement) | 10/9 |
| Thông điệp thông báo lỗi (ICMP Error Reports) | Không thể đạt tới đích (Destination Unreachable) | 3 |
| | Yêu cầu ngừng hoặc giảm tốc độ phát (Source Quench) | 4 |
| | Định hướng lại (Redirection) | 5 |
| | Vượt ngưỡng thời gian (Time Exceeded) | 11 |

**Hình 3.8 Các loại thông điệp ICMP.**

*Các loại thông điệp ICMP:* Các thông điệp ICMP được chia thành hai nhóm: các thông điệp truy vấn và các thông điệp thông báo lỗi. Các thông điệp truy vấn giúp cho người quản trị mạng nhận các thông tin xác định từ một node mạng khác. Các thông điệp thông báo lỗi liên quan đến các vấn đề mà bộ định tuyến hay trạm phát hiện ra khi xử lý gói IP. ICMP sử dụng địa chỉ IP nguồn để gửi thông điệp thông báo lỗi cho node nguồn của gói IP.

### 3.2.5. Giao thức phân giải địa chỉ ARP (Address Resolution Protocol)

Giao thức TCP/IP sử dụng ARP để tìm địa chỉ vật lý của trạm đích. Ví dụ khi cần gửi một gói dữ liệu IP cho một hệ thống khác trên cùng một mạng vật lý Ethernet, hệ thống gửi cần biết địa chỉ Ethernet của hệ thống đích để tầng liên kết dữ liệu xây dựng khung gói dữ liệu. Thông thường, mỗi hệ thống lưu giữ và cập nhật bảng thích ứng địa chỉ IP-MAC tại chỗ (còn được gọi là bảng ARP Cache). Bảng thích ứng địa chỉ được cập nhật bởi người quản trị hệ thống hoặc tự động bởi giao thức ARP sau mỗi lần ánh xạ được một địa chỉ tương ứng mới.

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. Các máy nhận, đọc, phân tích và so sánh địa chỉ IP của nó với

địa chỉ IP của gói. Nếu cùng địa chỉ IP, nghĩa là node đích tìm trong bảng thích ứng địa chỉ IP-MAC của nó và trả lời bằng một gói ARP Rely 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.

Tóm lại tiến trình của ARP được mô tả như sau:

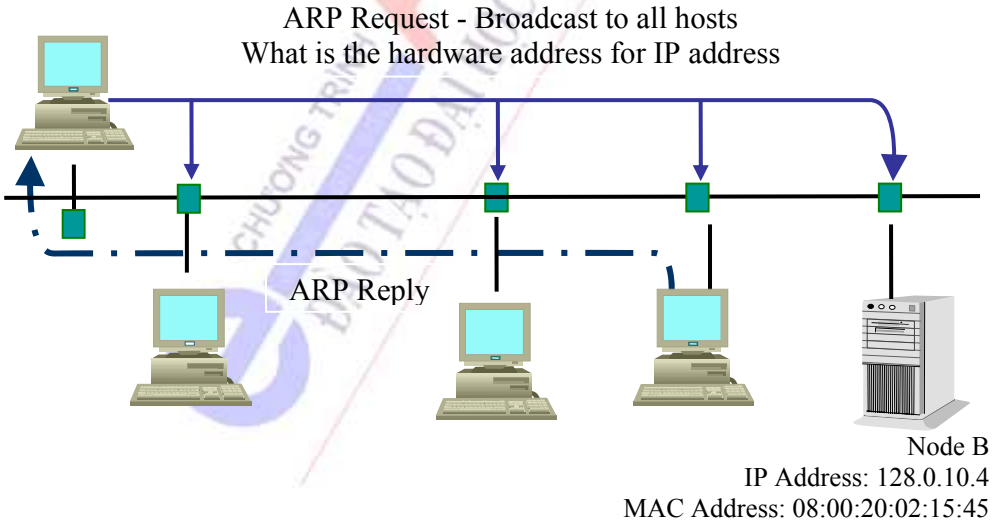
- IP yêu cầu địa chỉ MAC.
- Tìm kiếm trong bảng ARP.
- Nếu tìm thấy sẽ trả lại địa chỉ MAC.
- Nếu không tìm thấy, tạo gói ARP yêu cầu và gửi tới tất cả các trạm.
- Tuỳ theo gói tin trả lời, ARP cập nhật vào bảng ARP và gửi địa chỉ MAC cho IP.

### 3.2.6. Giao thức phân giải địa chỉ ngược RARP (Reverse Address Resolution Protocol)

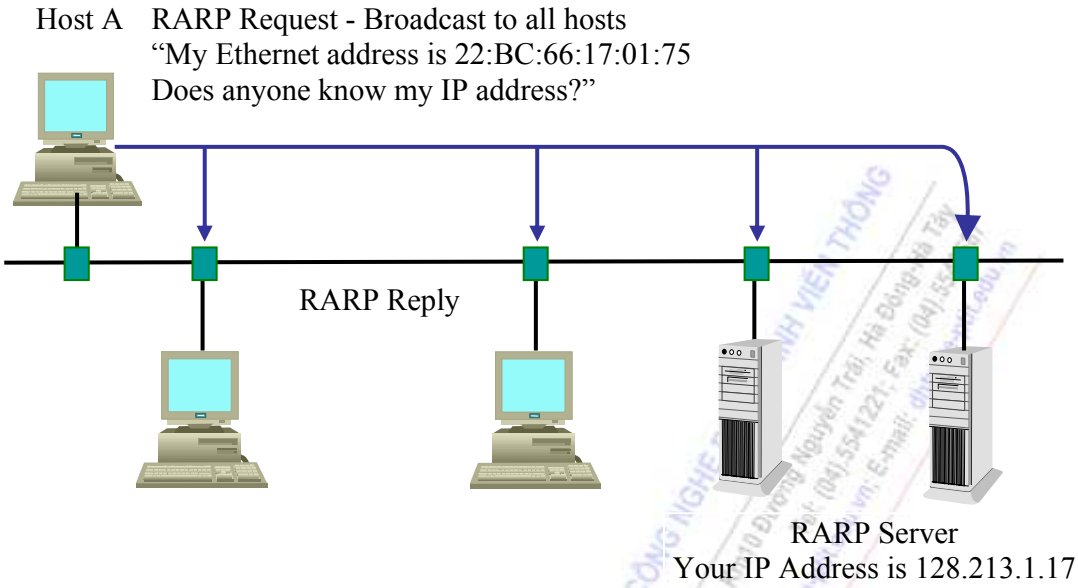
RARP là giao thức phân giải địa chỉ ngược. Quá trình này ngược lại với quá trình ARP ở trên, nghĩa là cho trước địa chỉ mức liên kết, tìm địa chỉ IP tương ứng. Như vậy RARP được sử dụng để phát hiện địa chỉ IP, khi biết địa chỉ vật lý MAC. Và cũng được sử dụng trong trường hợp trạm làm việc không có đĩa

Khuôn dạng gói tin RARP tương tự như khuôn dạng gói ARP đã trình bày, chỉ khác là trường Opcode có giá trị 0×0003 cho mã lệnh yêu cầu(RARP Request) và có giá trị 0×0004 cho mã lệnh trả lời(RARP Reply).

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. Hình 3.12 minh họa hoạt động của giao thức RARP. 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.




**Hình 3.9 Minh hoạ quá trình tìm địa chỉ MAC bằng ARP**




**Hình 3.10 Minh họa quá trình tìm địa chỉ IP bằng giao thức RARP.**

## 3.3. Giao thức IPv6 (Internet Protocol Version Number 6)

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.

### 3.3.1. Nguyên nhân ra đời của IPv6

- Internet phát triển mạnh, nhu cầu sử dụng địa chỉ IP tăng dẫn đến không gian địa chỉ ngày càng bị thu hẹp và tình trạng thiếu hụt địa chỉ tất yếu sẽ xảy ra trong vài năm tới.

- Việc phát triển quá nhanh của mạng Internet dẫn đến kích thước các bảng định tuyến trên mạng ngày càng lớn.

- Cài đăt IPv4 bằng thủ công hoặc bằng giao thức cấu hình địa chỉ trạng thái DHCP (Dynamic Host Configuration Protocol), 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.

- Trong quá trình hoạt động IPv4 đã phát sinh một số vấn đề về bảo mật và QoS. 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.

- Mặc dù có các chuẩn đảm bảo chất lượng dịch vụ QoS trong IPv4 trường IPv4 TOS (Type of Service), nhưng hạn chế về mặt chức năng, cần thiết hỗ trợ tốt hơn cho các ứng dụng thời gian thực.

Vì vậy 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.

### 3.3.2. 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:

- Đơn giản hoá Header: Một số trường trong Header của IPv4 bị bỏ hoặc chuyển thành các trường tuỳ chọn. Giảm thời gian xử lý và tăng thời gian truyền.

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

- Khả năng địa chỉ hoá và chọn đường linh hoạt: IPv6 cho phép nhiều lớp địa chỉ với số lượng các node. Cho phép các mạng đa mức và phân chia địa chỉ thành các mạng con riêng lẻ. 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).

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

- 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.

- 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.

### 3.3.3. 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. |
| 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) |

**Hình 3.11 So sánh IPv4 và IPv6**

## 3.4. Các lớp địa chỉ IPv6

### 3.4.1. Phương pháp biểu diễn 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.Ccó thể thu gọn bằng cách thay các nhóm 0 liên tiếp bằng kí hiệu "::". Ví dụ 12AB : 0000 : 0000 : CD30 : 0000 : 0000 : 0000 : 0000 /60 có thể viết là 12AB : 0 : 0 : CD30 : 0 : 0 : 0 : 0 /60 hoặc 12AB :: CD30 : 0 : 0 : 0 : 0 /60 hoặc 12AB : 0 : 0 : CD30 :: /60 . Không được viết 12AB :: CD30 /60 hay 12AB :: CD30 :: /60

### 3.4.2. Phân loại địa chỉ IPv6

- Địa chỉ Unicast: 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: 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: 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.

### 3.4.3. So sánh địa chỉ IPv4 và địa chỉ IPv6

Địa chỉ IPv6 và IPv4 có một số điểm chung như cùng sử dụng một số loại địa chỉ với một số chức năng tương tự, nhưng trong IPv6 có một số thay đổi thể hiện trong bảng sau:

**Bảng So sánh địa chỉ IPv4 và IPv6**

| **IPv4 Address** | **IPv6 Address** |
|---|---|
| Phân lớp địa chỉ (Lớp A, B, C và D) | Không phân lớp địa chỉ. Cấp phát theo tiền tố |
| Lớp D là Multicast (224.0.0.0/4) | Địa chỉ multicast có tiền tố FF00::/8 |
| Sử dụng địa chỉ Broadcast | Không có Broadcast, thay bằng Anycast |
| Địa chỉ unspecified là 0.0.0.0 | Địa chỉ Unspecified là :: |
| Địa chỉ Loopback 127.0.0.1 | Địa chỉ Loopback là ::1 |
| Sử dụng địa chỉ Public | Tương ứng là địa chỉ Unicast toàn cầu |
| Địa chỉ IP riêng (10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16) | Địa chỉ Site-lLcal (FEC0::/48) |
| Địa chỉ tự cấu hình (169.254.0.0/16) | Địa chỉ Link-Local (FE80::/64) |
| Dạng biểu diễn: chuỗi số thập phân cách nhau bởi dấu chấm | Dạng biểu diễn: chuỗi số Hexa cách nhau bởi dấu hai chấm; có thể nhóm chuỗi số 0 liền nhau vào một kí tự |
| Sử dụng mặt nạ mạng con | Chỉ sử dụng kí hiệu tiền tố để chỉ mạng |
| Phân giải tên miên DNS: bản ghi tài nguyên địa chỉ máy chủ IPv4 (A) | Phân giải tên miên DNS: bản ghi tài nguyên địa chỉ máy chủ IPv6 (AAAA) |
| Tên miền ngược: IN-ADDR.ARPA | Tên miền ngược: IP6.INT domain |

## Câu hỏi và bài tập

1. Hãy trình bày tổng quát mô hình kiến trúc TCP/IP
2. Vai trò và chức năng các tầng trong mô hình TCP/IP
3. Tầng ứng dụng (Process/Application Layer) và các giao thức ứng dụng.
4. Tầng vận chuyển Host to Host và các giao thức.
5. Tầng mạng (Internet Layer) và các giao thức tầng mạng.
6. Trình bày khái quát các giao thức định tuyến RIP, OSPF, BGP.
7. Quá trình đóng gói dữ liệu Encapsulation
8. Quá trình phân mảnh các gói dữ liệu Fragment
9. Khái niệm đơn vị truyền cực đại MTU (Maximum Transmission Unit).
10. Quá trình phân mảnh làm tăng thời gian xử lý, làm giảm tính năng của mạng.
11. Vai trò và chức năng, cấu trúc gói tin của UPP (User Datagram Protocol)
12. Vai trò và chức năng của TCP :
13. Trình bày các đặc điểm của TCP
14. Điều khiển lưu lượng và điều khiển tắc nghẽn
15. Trình bày các cơ chế cửa sổ động, phát lại thích nghi, điều khiển tắc nghẽn.
16. Thiết lập và huỷ bỏ liên kết:
17. Độ tin cậy và điều khiển luồng của TCP:
18. Các chức năng chính của IP:
19. Địa chỉ IP, cấu trúc gói dữ liệu IP.
20. Phân mảnh và hợp nhất các gói IP:
21. Trình bày chức năng giao thức thông báo điều khiển mạng ICMP.
22. Tiến trình của Giao thức phân giải địa chỉ ARP (Address Resolution Protocol)
23. Nguyên tắc hoạt động, khuôn dạng gói tin của giao thức RARP
24. Các đặc trưng của IPv6
25. Chất lượng dịch vụ và bảo mật trong IPv6
26. Cấu trúc khuôn dạng Datagram Ipv6
27. Header mở rộng
28. So sánh IPv4 header và IPv6 header
29. Lớp địa chỉ IPv6, biểu diễn, các loại địa chỉ IPv6
30. So sánh địa chỉ IPv4 và địa chỉ IPv6
31. Mô hình kiến trúc TCP/IP và so sánh với mô hình OSI.

# CHƯƠNG 4: KỸ THUẬT MẠNG CỤC BỘ

Nội dung của chương này sẽ trình bày các khái niệm cơ bản về kỹ thuật mạng cục bộ LAN, các phương pháp truy nhập ngẫu nhiên và có điều khiển được sử dụng trong các mạng quảng bá. Nội dung của chương gồm các phần sau:

- Các phương thức truy nhập đường truyền.
- Mạng Ethernet và họ chuẩn IEEE 802.
- Mạng cục bộ Token Ring.
- Giao diện số liệu phân bố sử dụng cáp sợi quang.
- Giới thiệu mạng LAN ATM.

## 4.1. Các phương thức truy nhập đường truyền

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

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 Bus chung. Vì vậy cần có cơ chế tránh xung đột và nghẽn thông tin. CSMA/CD là phương pháp cải tiến của phương pháp CSMA (Nghe trước khi nói - Listen before talk).

*Nguyên tắc hoạt động:* Khi một trạm truyền dữ liệu, trước hết nó sẽ phải "nghe" xem đường truyền "bận" hay "rỗi". Nếu "rỗi" nó sẽ truyền dữ liệu đi (theo khuôn dạng chuẩn), nếu đường truyền đang "bận" thì nó sẽ thực hiện 1 trong 3 giải thuật sau:

1. Trạm tạm "rút lui" chờ đợi trong một thời gian ngẫu nhiên, sau đó lại bắt đầu nghe đường truyền (Non persistent)
2. Trạm tiếp tục "nghe" đến khi đường truyền rỗi thì truyền dữ liệu đi với xác suất bằng 1 (persistent).
3. Trạm tiếp tục "nghe" đến khi đường truyền rỗi thì truyền dữ liệu đi với xác suất bằng $0<p<1$ xác định trước (p-persistent).

*Ưu, nhược điểm của từng giải thuật trên:* Giải thuật 1 có hiệu quả trong việc tránh xung đột. Tuy nhiên, có thể có thời gian "chết" của đường truyền vì cả hai cùng đợi. Giải thuật 2 ngược lại, cố gắng giảm được thời gian "chết" của đường truyền nhưng nếu có hơn một trạm cùng truyền thì khả năng xảy ra xung đột sẽ cao và giải thuật 3 với giá trị $p$ chọn một cách hợp lý có thể tối thiểu hoá được khả năng xung đột cũng như giảm được thời gian "chết" của đường truyền.

Tuy nhiên, xung đột xảy ra thường do độ trễ truyền dẫn. CSMA thực chất là các trạm chỉ "Nghe trước khi nói" mà không "nghe trong khi nói", nên thực tế có xung đột nhưng các trạm vẫn

không thể biết và tiếp tục truyền dữ liệu dẫn đến tắc nghẽn, xung đột thông tin trên đường truyền. Giải pháp CSMA/CD (hay còn gọi là LWT - Listen while talk) có thể phát hiện xung đột như sau:

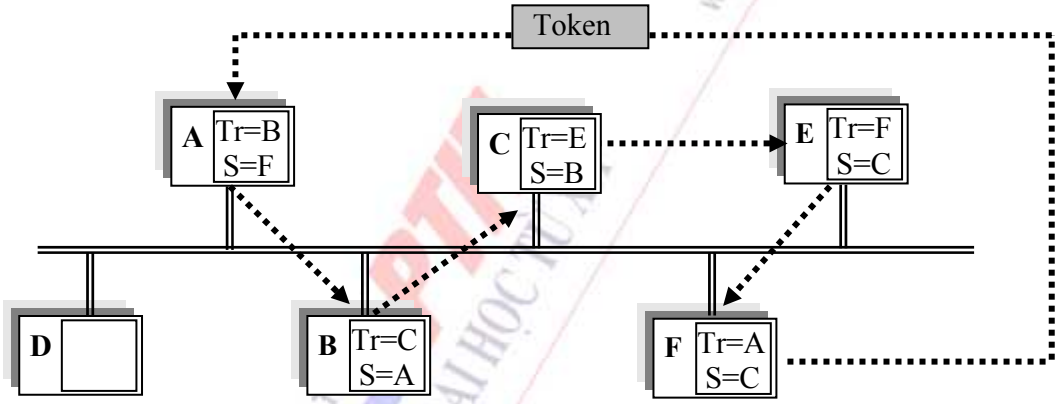
- Khi một trạm đang truyền, vẫn tiếp tục "nghe" đường truyền. Nếu phát hiện thấy xung đột, nó ngừng ngay việc truyền nhưng vẫn tiếp tục gửi sóng mang đi thêm một thời gian để đảm bảo rằng các trạm trên mạng đều có thể "nghe" được xung đột đó.

- Sau đó, trạm chờ đợi trong một thời đoạn ngẫu nhiên, nó tiếp tục thử truyền lại theo nguyên tắc các giải thuật của CSMA.

Với CSMA/CD, thời gian chiếm dụng vô ích đường truyền giảm xuống đúng bằng thời gian dùng để phát hiện một xung đột. CSMA/CD cũng sử dụng 3 giải thuật "kiên nhẫn" của CSMA, trong đó giải thuật (2) (1-persistent) là được dùng hơn cả.

### 4.1.2. Token Bus

Để cấp phát quyền truy nhập đường truyền cho một trạm cần truyền dữ liệu, một thẻ bài được lưu chuyển trên một vòng logic được thiết lập bởi các trạm có nhu cầu. 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. Thẻ bài (Token) 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.




**Hình 4.1 Token BUS**

*Thiết lập vòng logic*: Vòng logic giữa các trạm có nhu cầu truyền, được xác định theo một chuỗi có thứ tự mà trạm cuối cùng liền kề với trạm đầu tiên của vòng. Mỗi trạm được biết địa chỉ của trạm liền kề trước và sau nó. Thứ tự của các trạm trên vòng logic độc lập với thứ tự vật lý. Các trạm không hoặc chưa có nhu cầu truyền dữ liệu thì không đưa vào vòng logic và chúng chỉ có thể tiếp nhận dữ liệu.

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.

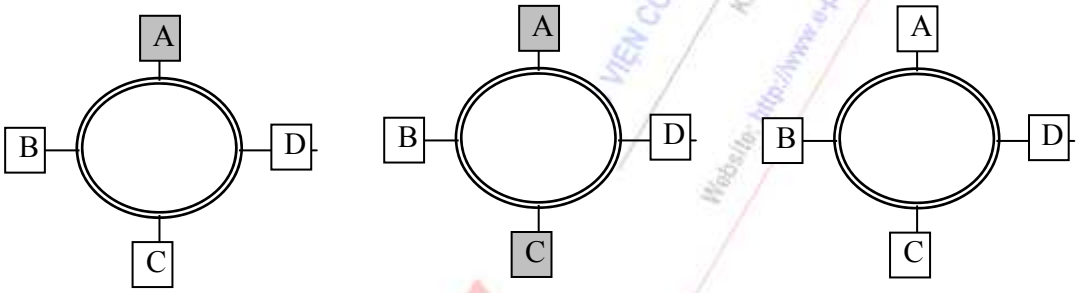
- Loại bỏ một trạm không còn nhu cầu truyền dữ liệu ra khỏi vòng logic.

- Quản lý lỗi: Lỗi: có thể "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.

### 4.1.3. Token ring

*Nguyên tắc của phương pháp:* Dùng thẻ bài lưu chuyển trên đường vật lý để cấp phát truy nhập đường truyền. Một trạm muốn truyền dữ liệu thì phải đợi đến khi nhận được một thẻ bài "rỗi". Khi đó trạm sẽ đổi bit trạng thái của thẻ bài sang trạng thái "bận" 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. Dữ liệu đến trạm đích phải được sao 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.




A có nhu cầu truyền dữ liệu đến C. Đợi Free Token,chuyển sang trạng thái Busy, gửi kèm Packet dữ liệu

Node B đọc, phân tích và so sánh địa chỉ đích với địa chỉ MAC. Node C sao chép dữ liệu

Khi Packet dữ liệu quay về, Node A chuyển trạng thái Token thành Free.

**Hình 4.2 Token Ring**

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*: Cần giải quyết hai vấn đề có thể dẫn đến phá vỡ hệ thống. Một là mất thẻ bài. Hai là một thẻ bài "bận" lưu chuyển không dừng trên vòng. Có thể có nhiều giải pháp khác nhau để khắc phục vấn đề này, sau đây là một giải pháp được khuyến nghị:

Đối với vấn đề mất thẻ bài: Có thể quy định trước một trạm điều khiển chủ động (Active Monitor), phát hiện mất thẻ bài bằng cách dùng cơ chế ngưỡng thời gian Time-out. Sau khoảng thời gian đó, nếu không nhận lại được thẻ bài, trạm sẽ phát hiện tình trạng phục hồi bằng cách phát lại thẻ bài mới.

Đối với vấn đề thẻ bài "bận"lưu chuyển trên vòng không dừng: trạm Monitor sử dụng một bit trên thẻ bài đánh dấu (M=1) khi gặp một thẻ bài bận đi qua nó. Nếu nó gặp lại một thẻ bài bận

với bit đã đánh dấu đó thì có nghĩa là trạm nguồn đã không nhận lại được đơn vị dữ liệu của mình và thẻ bài bận cứ quay vòng mãi. Lúc đó, trạm Monitor sẽ đổi bit trạng thái của thẻ bài thành "rỗi" và chuyển tiếp trên vòng. Tuy nhiên, cần chọn một giải thuật để chọn trạm thay thế cho trạm monitor khi bị hỏng.

### 4.1.4. So sánh CSMA/CD với các phương pháp dùng thẻ bài

Độ phức tạp của phương pháp dùng thẻ bài lớn hơn nhiều so với phương pháp truy nhập ngẫu nhiên CSMA/CD, xử lý đơn giản hơn.Trong điều kiện tải nhẹ phương pháp thẻ bài không cao do một trạm có thể đợi khá lâu mới đến lượt (có thẻ bài). Ngược lại,: trong điều kiện tải nặng, phương pháp dùng thẻ bài hiệu quả hơn so với CSMA/CD.

Ưu điểm lớn nhất của phương pháp dùng thẻ bài là khả năng điều hoà lưu thông trong mạng bằng cách cho phép các trạm truyền số lượng đơn vị dữ liệu khác nhau khi nhận được thẻ bài hoặc bằng cách lập chế độ ưu tiên cấp phát cho các trạm cho trước.

## 4.2. Ethernet và chuẩn IEEE 802

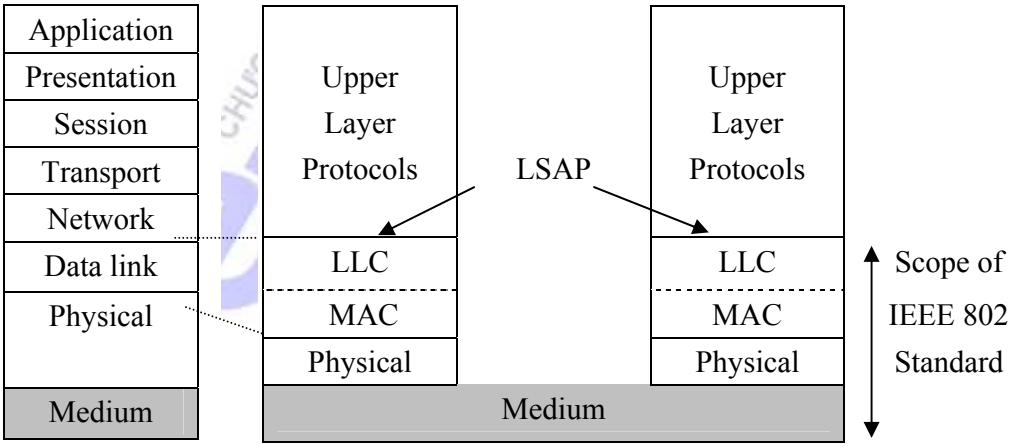
### 4.2.1. Giới thiệu chung về Ethernet

Ethernet là công nghệ của mạng LAN cho phép truyền tín hiệu giữa các máy tính với tốc độ 10Mb/s đến 10 Gigabit/s. Trong các kiểu Ethernet thì kiểu sử dụng cáp xoắn đôi là hay 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).

IEEE (Institute of Electrical and Electronics Engineers, Inc- Viện công nghệ điện và điện tử) đưa ra tiêu chuẩn về Ethernet đầu tiên vào năm 1985 với tên gọi "IEEE 802.3 Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications"

Gần đây, với các phương tiện truyền dẫn và công nghệ mới, công nghệ Ethernet đã ngày càng phát triển và đạt được tốc độ trao đổi số liệu đến 10 Gigabit trên giây.




**Hình 4.3 Quan hệ của các chuẩn IEEE 802 với mô hình tham chiếu OSI.**

*Thành phần mạng Ethernet bao gồm:*

- 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 đường thẳng/ 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 ...

### 4.2.2. Chức năng các tầng trong IEEE 802

Chuẩn IEEE 802 bao gồm chức năng tầng vật lý (Physical) và liên kết dữ liệu (Data Link) trong mô hình OSI. Điều này có nghĩa là Uỷ ban 802 của IEEE nhấn mạnh tới việc tiêu chuẩn hoá các công nghệ phần cứng sử dụng tại tầng vật lý và tầng liên kết dữ liệu.

Chuẩn IEEE chia tầng liên kết dữ liệu thành hai tầng con, tầng điều khiển truy nhập MAC (Media Access Control) và điều khiển liên kết logic LLC (Logical Link Control).

*Tầng LLC (Logical Link Control ):*Tất cả mạng LAN theo chuẩn IEEE có cùng lớp LLC được định nghĩa bởi 802.2. Dùng chung tầng con LLC, cơ chế các tầng trên như nhau bất kể loại phần cứng nào được sử dụng. Giao diện giữa tầng kề trên với LLC được định nghĩa bởi các điểm LSAP (Link Service Access Points ). LSAP là các địa chỉ liên kết logic. Địa chỉ Ethernet có nhiều địa chỉ LSAP, những địa chỉ này cho phép liên kết giữa các thực thể trên mạng. Địa chỉ MAC là duy nhất.

- Nếu thiết bị là DTE, nó quy định giao diện giữa giữa tầng MAC và tầng mạng. LLC quản lý liên kết dữ liệu và định nghĩa các điểm truy nhập dịch vụ (Service Access Point - SAP). LLC Sublayer được tiêu chuẩn hoá trong IEEE 802.2

- Nếu thiết bị DCE là Bridge. Brige cung cấp giao diện LAN-to-LAN sử dụng chung Protocol (Ethenet to Ethenet) hoặc giữa các LAN sử dụng khác Protocol (như Ethernet to Token Ring). Bridge được tiêu chuẩn hoá trong IEEE 802.1

- LLC Header:

| DSAP (1) | SSAP (1) | Cont (1) | Data (43 …) |
|---|---|---|---|

+ DSAP (Destination Service Access Point): Con trỏ thông báo cho NIC vị trí bộ đệm để lưu trữ thông tin nhận.

+ SSAP (Source Service Access Point) Vị trí bộ đệm lưu trữ thông tin đi.

+ DSAP and SSAP cho phép nhiều giao thức cùng sử dụng chung NIC Card.

+ Cont (Control). Kiểu của LLC.

+ Data: Dữ liệu được đưa xuống từ lớp Network, có chiều dài tối đa là 1497 bytes.

*Tầng con LLC cung cấp các dịch vụ sau:*

- Type 1: Dịch vụ Datagram không liên kết và không có cơ chế báo nhận biết (Unacknowledgement). Cung cấp kết nối Point to Point, Multipoint và Broadcast.

- Type 2: Dịch vụ mạch ảo, kiểu liên kết (Connection -Oriented ). Cung cấp các dịch vụ tuần tự, kiểm soát luồng, không lỗi giữa các LSAP.

- Type 3: Dịch vụ Datagram kiểu không liên kết và có cơ chế báo nhận biết (Acknowledgement).

*Tầng Ethernet Mac Sublayer:* Liên quan đến các phương pháp truy nhập và kiểm soát truy nhập đến đường truyền chung. Token RING và Ethernet thực hiện trong tầng MAC bằng các phương pháp khác nhau cùng chia sẻ đường truyền.

- Tạo Frame: Thêm các trường PRE, SFD, DE, SA, Length/Type, PAD, FCS và dữ liệu từ LLC đưa xuống tạo thành khung dữ liệu cung cấp cho tầng Vật lý.

- Nhận khung dữ liệu từ tầng Vật lý, kiểm tra lỗi và gữi dữ liệu cho tầng LLC.

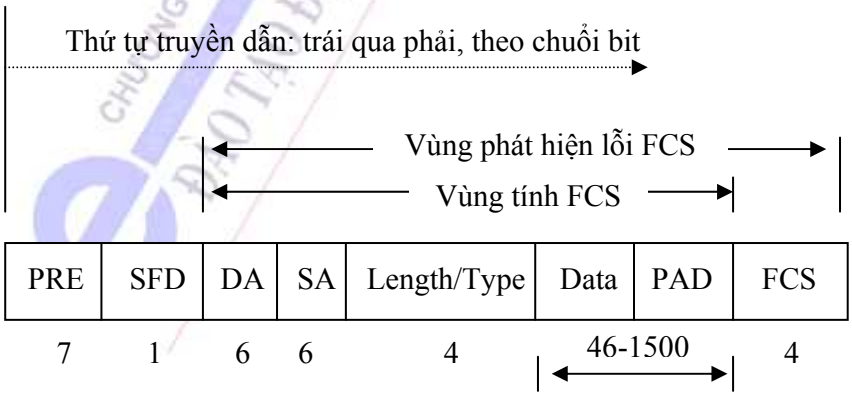
- Điều khiển truy nhập phương tiện truyền dẫn.

*Tầng Vật lý:* Xác định tốc độ truyền, phương pháp mã hoá và phương tiện truyền dẫn và cách thức kết nối vật lý. Tầng vật lý của IEEE 802.3 được phân chia là 2 phần:

- Phần độc lập với đường truyền đặc tả giao diện giữa tầng MAC và tầng vật lý.

- Phần phụ thuộc đường truyền và đặc tả giao diện với đường truyền của LAN và các tín hiệu trao đổi với đường truyền. Có nhiều tuỳ chọn khác nhau về kiểu đường truyền, phương thức truyền tín hiệu và tốc độ truyền, cách thức mã hoá.

### 4.2.3. Cấu trúc khung Ethernet:




**Hình 4.4 Token Ring**

- PRE (7bytes): Đánh dấu điểm đầu khung, đồng bộ.

- SFD (1byte): 10101011

- DA/SA (6 bytes): Địa chỉ đích, địa chỉ nguồn.

- Length/Type (2 bytes): Chiều dài dữ liệu nếu nhỏ hơn 1500.

- Data: Dữ liệu gửi từ LLC đưa xuống, gồm n byte (n<1501).

- PAD: Có thể có hay không. Nếu n<46 thì thêm 1 số byte (toàn 0) vào PAD để chiều dài tổng cộng của Data+Pad là 46 byte

- FCS (4 bytes) kiểm tra lỗi của các trường DA, SA, Length /Type và Data và PAD.

### 4.2.4. Họ IEEE 802

Bridge được tiêu chuẩn hoá trong IEEE 802.1, kiến trúc mạng, cung cấp giao diện LAN-to-LAN sử dụng chung Protocol LAN (ví dụ: Ethenet to Ethenet) hoặc giữa các LAN sử dụng khác Protocol (như Ethernet to Token Ring).

Logical Link Control (LLC) được tiêu chuẩn hoá trong IEEE 802.2, đặc tả chuẩn giao diện (Interface) giữa MAC và tầng mạng LLC quản lý liên kết dữ liệu và định nghĩa các điểm truy nhập dịch vụ (Service Access Point – SAP). IEEE 802.2 cung cấp 3 kiểu giao thức LLC:Type1, Type2, Type3. Các giao thức này theo phương thức cân bằng (Balanced Mode) của giao thức HDLC và có các khuôn dạng dữ liệu và chức năng tương tự.

EEE 802.3 đặc tả một mạng cục bộ dựa trên mạng Ethernet do Digital, Intel và Xerox hợp tác pháp triển từ năm 1980. IEEE 802.3 tương tự như DIX Ethernet, bao gồm cả tầng vật lý và tầng con MAC với các đặc tả sau:

- Đặc tả dịch vụ MAC (MAC ServicesSecification)

- Giao thức MAC (MAC Protocol).

- Đặc tả vật lý (Medium-Independent Physical Specification) độc lập với đường truyền

- Đặc tả vật lý phụ thuộc đường truyền (Medium - Dependent Physical Specification)

- Đặc tả dịch vụ MAC định nghĩa các dịch vụ IEEE 802.3 cung cấp cho tầng LLC hoặc người sử dụng ở tầng cao hơn.

Tầng MAC với giao thức truy nhập đường truyền CSMA/CD, làm giảm tình trạng xung đột và nghẽn thông tin bằng cách mỗi thiết bị trước khi truyền phải lắng nghe đường truyền và trong khi truyền vẫn tiếp tục nghe để xử lý khi có hiện tượng va chạm.

Tầng vật lý của IEEE 802.3 được chia làm hai phần. Phần độc lập với đường truyền, đặc tả giao diện giữa MAC và tầng vật lý. Phần phụ thuộc đường truyền là bắt buộc phải có và đặc tả giao diện với đường truyền của LAN và các tín hiệu trao đổi với đường truyền. Có các dạng sau cho tầng vật lý của IEEE 802.3:

- Tốc độ truyền tín hiệu (1 Mb /s hoặc 10Mb /s hoặc 100 Mb /s)

- BASE (nếu là Baseband) hoặc BROAD (nếu là Broadband)

- Chỉ định đặc trưng đường truyền.

*10BASE -F:* Dùng cáp quang, tốc độ 10 Mb/s, phạm vi cáp 4km Chuẩn này được phân thành 3 dạng con: 10BASE-FL, 10BASE-FB và 10BASE-FP.

10BASE-T: Sử dụng nột dải tần rộng hỗ trợ cho các tốc độ tín hiệu 10Mb/s. Dùng cáp UTP, trợ kháng 75 Ohm, với mạng hình sao.

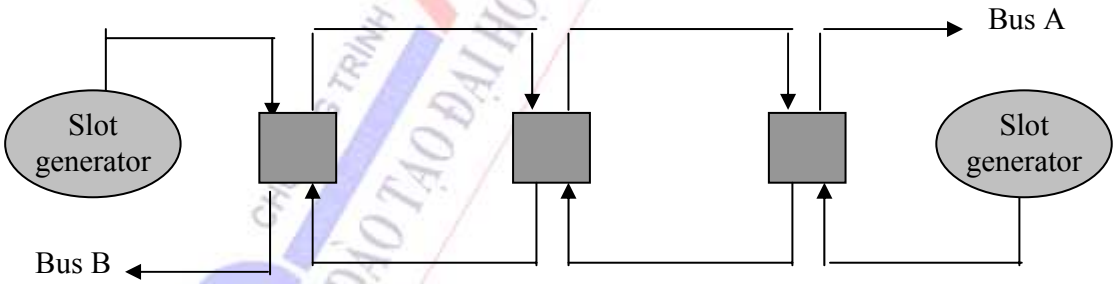
100 BASE-X: Gọi là Fast Ethernet, mạng hình sao tương tự 10BASE-, tốc độ 100Mb/s. Chuẩn này gồm 100 BASE-TX dùng cho cáp UTP hoặc STP 2 đôI, 100 BASE-FX dùng cho cáp quang, 100 BASE-T4 dùng cho cáp UTP 4 đôi (Four Twisted Pairs).

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.

IEEE 802.4: Mô tả một mạng cục bộ với cấu trúc dạng hình BUS và cơ chế điều khiển truy nhập đường truyền thẻ bài Token BUS. Mạng dùng cáp đồng trục 75 ohm với cả hai dạng Baseband và Broadband. IEEE 802.4 bao gồm tầng vật lý và tầng MAC. IEEE 802.4 sử dụng cáp đồng 75-ohm (tốc độ 1 Mbps, 5 Mbps và 10 Mbps) hoặc cáp quang (tốc độ 5 Mbps, 10 Mbps và 20 Mpbs). Nó được thiết kế để ứng dụng trong các văn phòng và trong các môi trường công nghiệp và quân sự.

Chuẩn IEEE 802.5: Là chuẩn đặc tả mạng cục bộ với mạng dạng vòng (RING) sử dụng thẻ bài Token RING để điều khiển truy nhập đường truyền. IEEE 802.5 bao gồm cả tầng vật lý và tầng con MAC.

IEEE 802.6: Mô tả một mạng tốc độ cao kết nối nhiều LAN thuộc các khu vực khác nhau của một đô thị (còn được gọi là MAN - Metropolitan Area Network). Mạng sử dụng cáp quang với mạng dạng Bus kép (Dual - BUS), vì thế còn được gọi là DQDB (Distributed Queue Dual Bus). Lưu thông trên mỗi Bus là một chiều và khi cả cặp Bus cùng hoạt động sẽ tạo thành một cấu hình bỏ qua được các lỗi (Fault - Tolerant). Phương pháp điều khiển truy nhập dựa trên một giải thuật xếp hàng phân tán có tên là QPDS (Queued - Packet, Distrubuted -Switch). DQDB là Bus quảng bá đa truy nhập, tương tự như CSMA/CD, nhưng phải dùng một phương pháp truy nhập theo "khe" (Slotted Access) để khắc phục các hạn chế về truy nhập của CSMA/CD. Để quảng bá dữ liệu cần phải cài đặt Bus dưới dạng cặp Bus một chiều tương tự như một dạng vòng (Ring). Vì hai Bus chuyển dữ liệu ngược chiều nhau nên việc quảng bá dữ liệu đòi hỏi phải truyền cả trên hai Bus.




**Hình 4.5: Sơ đồ nối bus của DQDB**

Đơn vị dữ liệu được dùng trong các mạng DQDB được thiết kế tương thích với thế hệ mới của các mạng diện rộng công cộng gọi là B-ISDN (Broadband Integrated Services Digital Networks). Các mạng này sử dụng kỹ thuật chuyển mạch gói nhanh (Fast Packet Switching) với công nghệ hứa hẹn nhất là ATM. Vì thế đơn vị dữ liệu dùng trong các mạng DQDB cũng được gọi là "tế bào" (Cell) với khuôn dạng tổng quát gồm 53 bytes, trong đó có bytes của phần Header cố định và 48 bytes dữ liệu.

Các mạng IEEE 802.6 cho phép truyền dữ liệu với tốc độ cao từ vài chục đến hàng trăm Mb/s. Đáp ứng các yêu cầu truyền dữ liệu đa phương diện.

- IEEE 802.9: Đặc tả một mạng tích hợp dữ liệu và tiếng nói bao gồm 1 kênh dị bộ 10 Mb/s cùng với 96 kênh 64 Kb/s (tổng cộng 6Mb/s). Giải thông tổng cộng là 16 Mb/s. Chuẩn này còn được gọi là Isochronous Ethernet (IsoEnet) và nó được thiết kế cho các môi trường có lượng lưu thông lớn và cấp bách.

- IEEE 802.10: Chuẩn đặc tả về an toàn và mã hoá thông tin trong các mạng cục bộ.

- IEEE802.11: lchuẩn đặc tả mạng cục bộ không dây (Wireless LAN), hiện đang tiếp tục phát triển với phương pháp truy nhập CSMA/CD.

- IEEE 802.12 là chuẩn đặc tả mạng cục bộ bởi AT&T, IBM và HP, gọi là 100 VG - AnyLAN hay 100BASE-VG. Mạng sử dụng dạng hình sao xếp tầng (Cascaded Star Topology) và phương pháp truy nhập đường truyền có điều khiển tranh chấp. Khi có nhu cầu truyền dữ liệu, một trạm sẽ gửi yêu cầu đến HUB và trạm chỉ có thể truyền dữ liệu khi HUB cho phép. Chuẩn cung cấp một mạng tốc độ trên 100 Mb/s, có thể hoạt động trong các môi trường hỗn hợp Ethernet và Token Ring. Vì thế nó chấp nhận cả hai dạng Frame.

- IEEE 802.14: Chuẩn cuối cùng hiện nay là 802.14. Chuẩn này dùng cho truyền dữ liệu qua đường cáp TV, nhằm nâng cao tốc độ truy nhập Internet tại gia đình.

### 4.2.5. Ethernet 100 Mbps

Mạng Ethernet 100 Mbps được gồm 2 chuẩn :

* Fast Ethernet (IEEE 802.3u): 100Base-TX, 100Base-T4 và 100Base-FX.

*Các loại cáp sử dụng*

- 100BASE-T4 sử dụng bốn đôi dây cân bằng cáp UTP Cat-3 hoặc Cat-5.
- 100BASE-TX sử dụng hai đôi UTP Cat-5 hoặc đôi dây STP.
- 100BASE-FX sử dụng đôi dây cáp quang đa mode.

*Mã hóa:*

- 100Base-TX và 100Base-FX sử dụng kỹ thuật mã hóa 4B/5B.
- 100Base-T4 sử dụng kỹ thuật mã hóa 8B/6T.

*Phương thức điều khiển truy nhập CSMA/CD*

- 100Base-T4 sử dụng phương thức hoạt động bán song công.
- 100Base-TX sử dụng phương thức hoạt động song công.
- 100Base-FX sử dụng cả phương thức hoạt động song công và bán song công.

* 100VG-AnyLAN là công nghệ cạnh tranh với Fast Ethernet, ít được sử dụng.

### 4.2.6. Gigabit Ethernet.

Sự ra đời của Gigabit Ethernet đã mở ra một kỷ nguyên mới Ethernet tốc độ cao. Gigabit Ethernet được thiết lập dựa trên các nguyên lý cơ bản của 10BASE-T, Fast Ethernet và chuyển mạch Ethernet. Có 2 chuẩn Gigabit Ethernet:

* IEEE 802.3z: Mạng Gigabit Ethernet trên cáp quang chuẩn hóa năm 1998. Phương tiện truyền dẫn cơ bản là sợi quang đơn mode (SMF) với đường kính lõi là 10 µm, hay sợi quang đa mode với đường kính lõi là 50 µm hoặc 62.5 µm. Tín hiệu được truyền dẫn chủ yếu trên hai bước sóng là 850nm (bước sóng ngắn) và 1310 nm (bước sóng dài). Nếu sử dụng cáp đồng thì đó là loại cáp bốn đôi Cat-5 UTP, với khoảng cách có thể lên tới 100m.

*Tại tầng vật lý: IEEE 802.3z :*

1000Base-SX : chuẩn cho cáp quang bước sóng ngắn.

- Với cáp quang đa mode 62.5 µm, khoảng cách tối đa 220-275 m
- Với cáp quang đa mode 50 µm, khoảng cách tối đa 500-550 m

1000Base-LX : chuẩn cho cáp quang bước sóng dài

- Với cáp quang đa mode 62.5/50 µm, khoảng cách tối đa 550 m
- Với cáp quang đơn mode 9 µm, khoảng cách tối đa 5000 m

1000Base-CX : chuẩn cho cáp đồng tuyến ngắn.

- Với cáp đồng trục, khoảng cách tối đa là 25 m

*Tại tầng liên kết dữ liệu:*

- Hoạt động ở chế độ song công và chuyển mạch.
- Điều khiển truy nhập: CSSMA/CD trong phương thức song công.
- Trong phương thức bán song công sử dụng CSMA/CD cải tiến.

*Gigabit Ehernet trên cáp đồng:* Chuẩn IEEE 802.3ab 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. Tín hiệu truyền dẫn song công trực tiếp 2 chiều trên cả 4 đôi với tốc độ 250 Mbps/ 1 đôi dây.

### 4.2.7. Gigabit Ethernet qua cáp sợi quang

10 Gigabit Ethernet (GbE) được trình bày trong dự thảo tiêu chuẩn IEEE 802.3ae. Tốc độ Ethernet đã tăng từ 1 Gbps lên 10 Gbps, 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. Ngoài ra, 10 GbE có thể tương thích với các hệ thống SONET/SDH, có thể hỗ trợ cho tất cả các dịch vụ tại các tầng 2 và 3. 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 100 Mbps 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.

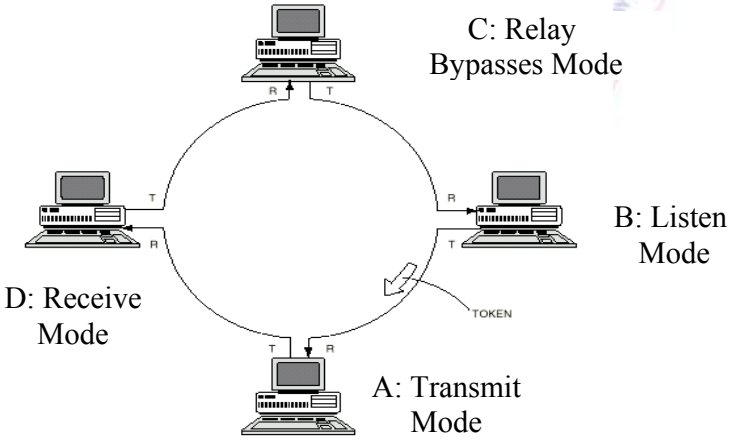
## 4.3. Mạng cục bộ Token Ring

Cấu trúc mạng hình vòng (Ring) là một chuỗi kết nối điểm - điểm các node lại với nhau tạo thành vòng tròn. Vì vậy Ring LAN không phải là mạng quảng bá như Ethernet, chúng được xem như mạng truyền tuần tự, điểm điểm. Công nghệ Ring LAN là số hoá, không giống như công nghệ mạng Ethernet trong đó cơ chế cảm nhận sóng mang là tín hiệu tương tự (Analog). Ring LAN thường sử dụng là IEEE 802.5

### 4.3.1. Hoạt động của Token Ring

Mỗi trạm hoạt động như là một bộ chuyển tiếp 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, gồm 24 bit. Nếu tốc độ trên vòng là 4 Mbps thì vòng phải có thời gian trì hoãn là 24/2 Mbps = 6 Micro giây.

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. và chế độ nhận. Hình 4.6 minh hoạ 4 trạm hoạt động: Giả sử A truyền dữ liệu đến D. Trạm A nhận Token, kiểm tra bit T. Nếu giá trị bằng 0, Token bận, nghĩa là đã có trạm trên mạng đang trong chế độ truyền. Nếu giá trị bit T bằng 1, đường truyền rỗi, trạm chuyển giá trị 1 bằng 0 sang trạng thái bận và A bước vào chế độ truyền (Transmit Mode). Vì A truyền đến D, nên địa chỉ đích sẽ là D, địa chỉ nguồn là A. Vì địa chỉ đích không phải là của B, nó bước vào chế độ lắng nghe (Listen Mode). Trạm C vì không cung cấp điện (giả sử bị mất điện chẳng hạn), do đó nó ở chế độ bỏ qua (Delay bypassesMode). Trạm đích D phát hiện ra rằng địa chỉ đích chính là của nó, nó bước vào chế độ nhận (Receive Mode). Khung dữ liệu được sao chép vào bộ nhớ của trạm.



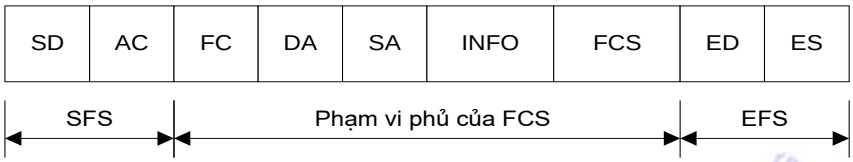

**Hình 4.6 Các chế độ làm việc của các trạm Token Ring**

Trong Frame có một số cờ kiểm soát quá trình truyền và nhận dữ liệu. Cờ Frame Status Flags nhận biết dựa vào phần cứng. Cờ Frame Status gồm các cờ nhận biết địa chỉ A (Address Recognized), cờ sao chép khung C (Frame Copied) và cờ lỗi E (Error).

### 4.3.2. Chuẩn Token Ring

Là chuẩn đặc tả mạng cục bộ với Topo dạng vòng (Ring) sử dụng thẻ bài để điều khiển truy nhập đường truyền tuân thủ chuẩn IEEE 802.5. Chuẩn IEEE 802.5 hoạt động trong tầng vật lý và tầng con MAC .

Giao thức MAC là phần cốt lõi của IEEE 802.5, sử dụng phương pháp Token Ring để điều khiển truy nhập đường truyền. Khuôn dạng của Frame dùng trong giao thức MAC của IEEE 802.5 được trình bày trong hình 4.8




**Hình 4.7 Khuôn dạng tổng quát của IEEE 802.5 Frame**

- SFS = Start Frame Sequence .
- SD = Starting Delimiter (1 byte): SD chỉ bắt đầu của một Frame hoặc Token.
- AC = Access Control (1 byte): Điều khiển truy nhập.
- FC=Frame Conrtol (1byte): Điều khiển Frame chứa LLC data hay là một MAC Control Frame.
- DA = Destination Address (2/6 byte): Địa chỉ đích của Frame.
- SA = Source Address (2/6 byte): Địa chỉ nguồn của Frame.
- INFO = Information (0 hoặc nhiều bytes).
- FCS = Frame Check Sequence (4 bytes): FCS: mã kiểm soát lỗi CRC 32 bit cho các vùng FC, DA, SA, và INFO.
- EFS = End - of - Frame Sequence
- ED = Ending Delimiter (1 byte): Các ký hiệu kết thúc Frame.
- FS = Frame Status (1 byte): Tình trạng Frame.

## 4.4. Giao diện số liệu phân bố sử dụng quang FDDI (Fiber Distributed Data Interface)

### 4.4.1. Giới thiệu FDDI

FDDI là một tập các giao thức ANSI truyền dữ liệu 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. Cấu hình Ring cáp quang, có thể kết nối trực tiếp các trạm đầu cuối và các máy chủ trong một nhóm làm việc hay liên kết các mạng trong phạm vi một tòa nhà, trong một khu vực hay trong một thành phố. Một trong các ứng dụng là để kết nối các máy chủ tốc độ cao. Khi đóng vai trò là một mạng xương sống (Backbone), 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.

Mặc dù bị thay thế bởi các công nghệ LAN khác, FDDI vẫn có những ưu điểm nhất định.

FDDI có thể được cấu hình như là hai mạng Ring ngược nhau độc lập. Điều này làm tăng tính ổn định hệ thống cao hơn. Nếu cấu hình (Topo) của mạng được thiết kế hai đường quang của cả hai mạng khác nhau về mặt vật lý thì sẽ đảm bảo cho hai mạng không bị phá hủy trong cùng một thời gian khi xảy ra các sự cố liên quan đến hệ thống cáp.

FDDI có đặc tính tự hồi phục bằng kỹ thuật Autowraping. Lỗi phát sinh ở Ring sơ cấp (Ring đang hoạt động) sẽ được khắc phục bằng cách nối vòng với Ring thứ cấp (Ring dự phòng), tạo thành một Ring đơn và cho phép mạng FDDI hoạt động ở tốc độ cao nhất. Phần cứng mạng có khả năng phát hiện ra sự cố của cáp giữa các điểm kết nối, do có hai đường cáp nên trạm phát hiện ra lỗi sẽ tự động nối vòng hai Ring với nhau thành một Ring đơn. Khung tin của FDDI có độ dài tới 4500 Byte, điều này làm tăng hiệu xuất mạng, giảm các thông tin Header giao thức.FDDI mã hóa dữ liệu khác biệt với các công nghệ khác để tăng hiệu quả truyền dẫn.

FDDI-2 là công nghệ mở rộng của FDDI, hỗ trợ truyền dẫn các tín hiệu tiếng nói, hình ảnh và dữ liệu. Một biến thể khác của FDDI là FFDT (FDDI Full Duplex Technology) sử dụng hạ tầng mạng như FDDI nhưng có thể tốc độ truyền số liệu lên đến 200 Mbps.

FDDI sử dụng cấu trúc vòng kép với lưu lượng truyền trên mỗi vòng Ring theo hướng ngược nhau. Vòng Ring kép bao gồm một Ring thứ cấp và một Ring sơ cấp. Trong quá trình hoạt động, Ring thứ cấp sử dụng để truyền số liệu còn Ring sơ cấp ở trạng thái rỗi. Mục đích của việc sử dụng vòng Ring kép là để đảm bảo tính bền vững và ổn định hơn.

### 4.4.2. So sánh những giữa FDDI và IEEE 802.5

| FDDI | IEEE 802.5 |
|---|---|
| - Dùng cáp quang .<br>- Tốc độ 100Mb/s<br>- Phương pháp mã hoá NRZI -4B/ 5B<br>- Đặc tả độ tin cậy tường minh<br>- Đồng bộ phân tán<br>- Quay vòng thẻ bài theo thời gian.<br>- Sinh thẻ bài mới sau khi truyền<br>- Chiếm thẻ bài bằng cách thu lại<br>- Khuôn dạng Frame FDDI<br>- Kích thước Frame tối đa 4500 Bytes<br>- Các địa chỉ 16 và / hoặc48 bits<br>- Chức năng phục hồi phân tán cho các trạm | - Dùng cáp đôi xoắn<br>- Tốc độ 1,4 và 16 Mb/s<br>- Phương pháp mã hoá Manchester vì sai<br>- Đặctả độ tin cậy không tường minh<br>- Đồng bộ tập trung<br>- Sử dụng các bit priority và reservation<br>- Sinh thẻ bài mới sau khi nhận<br>- Chiếm thẻ bài bằng cách đổi bit trạng thái<br>- Khuôn dạng Frame IEEE 802.5<br>- Không qui định kích thước Frame tối đa<br>- Các địa chỉ 16 hoặc 48 bits<br>- Trạm điều khiển (Active Monitor) đảm nhiệm chức năng phục hồi. |

**Bảng 4.8 Những điểm khác nhau giữa FDDI và IEEE 802.5**

### 4.4.3. Các kiểu kết nối đầu cuối FDDI

Một trong những đặc điểm đặc trưng của FDDI là việc hỗ trợ nhiều cách kết nối khác nhau giữa các thiết bị trên mạng FDDI. FDDI đưa ra bốn kiểu kết nối

- Trạm kết nối đơn SAS (Single Attachment Station) - được kết nối vào duy nhất một Ring qua một bộ tập trung.

- Trạm kết nối kép DAS (Dual Attachment Station). Mỗi DAS có hai port và được kết nối vào cả hai Ring.

- Bộ tập trung kết nối đơn SAC (Single Attachment Concentrator)

- Bộ tập trung kết nối kép DAC (Dual Attachment Concentrator

### 4.4.4. Khả năng chịu lỗi của FDDI

FDDI là một công nghệ mạng có đặc tính chịu lỗi cao vì mạng có cấu trúc Ring kép, sử dụng các chuyển mạch vòng quang, hỗ trợ kỹ thuật Dual Homing.

*Ring kép:* Ring kép có khả năng chịu lỗi cao. Nếu một trạm trên Ring bị lỗi hoặc một đường cáp bị đứt thì các thiết bị ở phần còn lại sẽ tự động khép lại thành một Ring đơn. Các hoạt động của mạng vẫn tiếp tục được duy trì trên các trạm còn lại của Ring.Tuy nhiên FDDI nếu hai hay nhiều lỗi xảy ra, Ring FDDI sẽ bị phân mảnh thành hai hoặc nhiều Ring con độc lập và các thiết bị trên mỗi Ring vẫn có khả năng trao đổi thông tin với nhau.

*Chuyển mạch vòng quang (Optical Bypass Switch):* Chuyển mạch vòng quang đảm bảo sự hoạt động của Ring kép một cách liên tục nếu một thiết bị nào đó trên Ring bị lỗi. Nó được sử dụng để ngăn chặn việc phân mảnh Ring cũng như loại bỏ các trạm có lỗi ra khỏi Ring. Chuyển mạch vòng quang bằng cách sử dụng các gương quang học để truyền trực tiếp các tia sáng từ Ring tới các thiết bị truy nhập kép DAS. Nếu một lỗi nào đó xảy ra trên thiết bị DAS, thì chuyển mạch quang này sẽ chuyển tia sáng qua chính nó bằng các gương nội tại, vì vậy vẫn duy trì được hoạt động của Ring . Lợi ích mang lại từ khả năng này là Ring sẽ không phải chuyển sang trạng thái Ring đơn khi thiết bị có lỗi. Hình 8 mô tả chức năng của một chuyển mạch vòng quang trong một mạng FDDI.

Các thiết bị quan trọng (Router,Mainframe) có thể sử dụng công nghệ Dual-homing để các kết nối dự phòng, nhằm đảm bảo cho thiết bị hoạt động một cách liên tục. Theo mô hình Dual-homing, các thiết bị quan trọng được gắn vào Ring qua hai bộ tập trung.

FDDI là một công nghệ mạng LAN/MAN sử dụng cáp quang, tốc độ 100 Mbps được thiết kế theo dạng Ring, được thiết kế để đáp ứng nhu cầu của người sử dụng mạng cần tốc độ truyền dẫn lớn hơn so với các mạng Ethernet/802.3 và token Ring hiện thời. Công nghệ này được thực hiện trước khi có sự phát triển của Fast Ethernet và Gigabit Ethernet.

Hiện nay, mạng FDDI không được dùng phổ biến vì chi phí thực hiện lớn, phức tạp (thiết bị quang đắt…) và bị cạnh tranh bởi các mạng Ethernet/802.3 có giá thành rẻ, dễ thực hiện, . Tuy nhiên, vẫn còn có những nghiên cứu với mục đích cải tiến để tận dụng khả năng cung cấp băng thông rất lớn cũng khả năng chống lỗi của nó.

## 4.5. Mạng LAN ATM

Mạng LAN được xây dựng đựa trên kỹ thuật ATM 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.

### 4.5.1. Đặc trưng của ATM LAN

- Hỗ trợ nhiều lớp dịch vụ tin cậy, ví dụ dịch vụ video trực tuyến có thể yêu cầu một cầu nối tin cậy có tốc độ 2Mbps để chất lượng dịch vụ có thể chấp nhận được.

- Thông lượng rộng, có khả năng mở rộng dung lượng trên từng Host (để cho phép các ứng dụng cần lượng dữ liệu xuất nhập lớn trên một host) và cả trên dung lượng phối hợp (để cho phép cài đặt và mở rộng từ vài host đến vài trăm host tốc độ cao).

- 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. Theo kiểu kết nối cố định hay chuyển mạch, ATM rất dễ mở rộng bằng cách thêm nhiều node chuyển mạch tốc độ cao (hay thấp) cho các thiết bị nối vào.

- 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.

### 4.5.2. Các loại ATM LAN

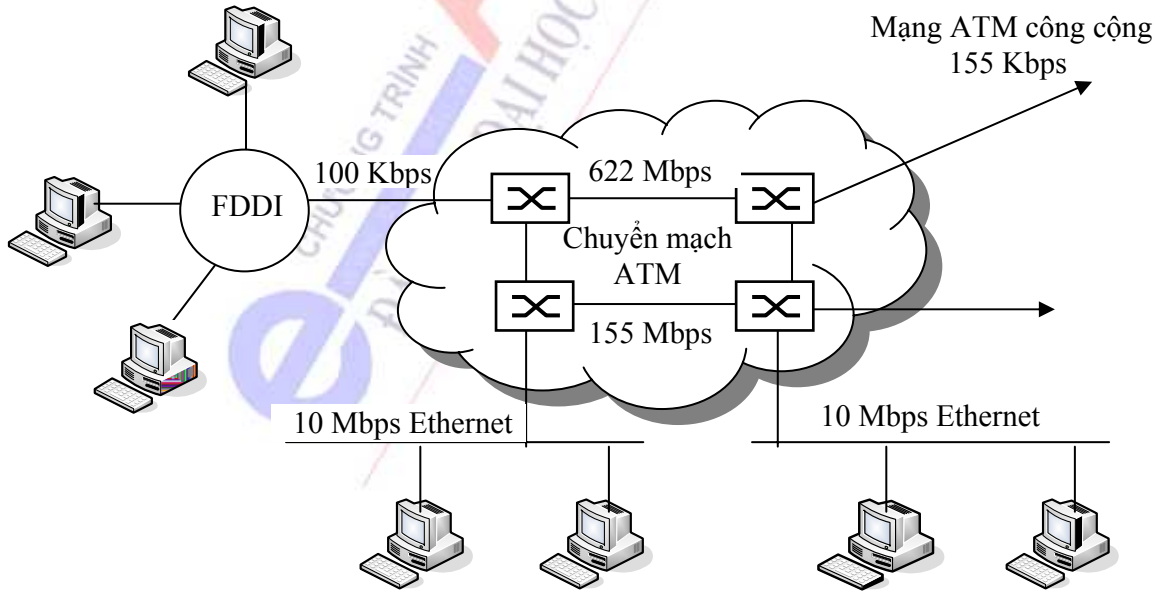
- Getway to ATM LAN: Là một chuyển mạch ATM đóng vai trò nh một Router và bộ tập trung tải để liên kết một mạng đầu cuối phức tạp vào ATM WAN.

- Backbone ATM Switch: Là chuyển mạch ATM hay một chuyển mạch ATM cục bộ liên kết các LAN khác nhau.

- Workgroup ATM: Là các máy trạm đa phương tiện chất lượng cao và các hệ thống đầu cuối được kết nối trực tiếp vào một chuyển mạch ATM .

Trên đây là 3 cấu hình thuần nhất. Trong thực tế một hỗn hợp của 2 hoặc 3 loại cũng có thể được sử dụng để tạo ra một mạng ATM LAN theo yêu cầu của doanh nghiệp.

Hình 4.9 minh hoạ một ví dụ mạng LAN ATM sử dụng bộ định tuyến chuyển mạch ATM và các giao tiếp ATM tại các trạm làm việc.




**Hình 4.9 Mạng LAN ATM**

### 4.5.3. Kỹ thuật chuyển mạch ATM LAN

Phải có khả năng chuyển đổi tốc độ từ bộ chuyển mạch ATM đến mạng LAN phải phù hợp với tốc độ dữ liệu của LAN. Đồng thời ATM có nhiệm vụ chuyển đổi giao thức từ MAC (điều khiển truy nhập đa phương tiện) sử dụng cho LAN thành dòng các tế bào ATM dùng trong mạng ATM. Vì vậy cần phải sử dụng thêm cầu nối (Bridge) và định tuyến.

Với chuyển mạch ATM Backbone, có thể thêm các bộ chuyển mạch ATM, nghĩa là tăng thêm dung lượng của trục sương sống, tốc độ dữ liệu của các trung kế giữa các chuyển mạch và LAN lúc này cũng tăng. Tuy nhiên số lượng chuyển mạch thêm vào có hạn và trục chính ATM đơn giản không thể đáp ứng mọi nhu cầu của LAN. Hệ thống đầu cuối bị hạn chế tốc độ dữ liệu, vì vậy cần sử dụng công nghệ ATM với HUB. Một HUB thường có nhiều cổng nối với nhiều thiết bị đầu cuối và các cổng hoạt động với tốc độ dữ liệu và giao thức khác nhau, gọi là ATM - LAN thuần tuý.

Quy ước sử dụng một tập các giao thức tầng vật lý trong các mạng LAN truyền thống khác với quy ước tập các giao thức trong tầng vật lý mạng WAN. Vì vậy khi liên kết các mạng LAN lại thành một mạng diện rộng cần thiết phải sử dụng các thiết bị như Gateway, Router.. để chuyển đổi các giao thức LAN, tốc độ dữ liệu và các tín hiệu giao thức sử dụng cho WAN. Hình 4.54 minh hoạ một mạng LAN/WAN được xây dựng đựa trên các bộ định tuyến ATM, như các mạng LAN/WAN truyền thống.

Trong kỹ thuật ATM, giao thức ATM có thể dùng cho cả mạng LAN và WAN. Điều này cho phép xây dựng một mạng LAN hoặc mạng WAN chỉ cần sử dụng các tổng đài ATM. Để kết nối một mạng Local ATM vào mạng WAN, chỉ cần sử dụng một cổng duy nhất trong tổng đài ATM để kết nối đến mạng của tổng đài TM.

## Câu hỏi trắc nghiệm

1. Phát biểu nào đúng:
    A. Dùng thể bài luân chuyển trên vòng logiic
    B. Trước khi truyền xác định đường truyền “bận” hay “rỗi”, nếu “bận” thì thực hiện 1 trong 3 giải thuật Non persistent, Persistent và P-persistent.
    C. Trong khi truyền phát hiện thấy xung đột, nó ngừng ngay truyền nhưng và thông báo cho các node khác biết. Sau đó chờ đợi với thời đoạn ngẫu nhiên, thực hiện giải thuật của CSMA.
2. Chức năng của Token Bus
    A. Bổ sung định kỳ các trạm nằm ngoài vòng logic nếu có nhu cầu truyền dữ liệu.
    B. Loại bỏ một trạm không còn nhu cầu truyền dữ liệu ra khỏi vòng logic.
    C. Quản lý lỗi.
    D. Khởi tạo vòng logic
    E. Khôi phục dữ liệu bị mất do gẫy vòng logic
3. Trong phương pháp Token ring cần giải quyết vấn đề phá vỡ hệ thống:
    A. Một là mất thẻ bài.
    B. Thẻ bài “bận” lưu chuyển không dừng trên vòng.

C. Khởi tạo vòng logic

D. Khôi phục dữ liệu bị mất do gẫy vòng logic

4. Phương pháp nào có cơ chế xác nhận ACK

A. CSMA/CD

B. TOKEN BUS

C. TOKEN RING

D. Cả 3 phương pháp.

5. Phương pháp nào có độ phức tạp hơn các phương pháp còn lại

A. CSMA/CD

B. TOKEN BUS

C. TOKEN RING

D. Cả 3 phương pháp.

6. Phương pháp nào xử lý hiệu quả hơn trong trường hợp tải nhẹ

A. CSMA/CD

B. TOKEN BUS

C. TOKEN RING

D. Cả 3 phương pháp.

7. Những đặc điểm kỹ thuật cơ bản của Ethernet

A. Cấu hình Bus / Star hoặc lai ghép Bus -Star

B. Quy cách kỹ thuật: IEEE 802.3.Phương pháp truy nhập: CSMA/CD.

C. Vận tốc truyền 10Mbps, 100Mbps ... 10Gbps

D. Loại cáp: Cáp đồng trục mảnh, cáp đồng trục dày, cáp xoắn đôi, cáp quang ...

E. Tất cả đều sai.

## Câu hỏi và bài tập

1. Phương thức đa truy nhập sử dụng sóng mang có phát hiện xung đột CSMA/CD
2. Ưu, nhược điểm của từng giải thuật trong CSMA/CD
3. Token Bus: Thiết lập vòng logi, duy trì trạng thái thực tế của mạng và khởi tạo vòng logic khi cài đặt mạng hoặc đứt vòng.
4. Token ring, nguyên tắc của phương pháp. Cần giải quyết hai vấn đề có thể dẫn đến phá vỡ hệ thống.
5. So sánh CSMA/CD với các phương pháp dùng thẻ bài
6. Token ring thế hệ thứ hai: Switched Token Ring, Token ring chuyên dụng (Dedicated Token ring), Full-duplex Token ring (Token ring song công (hai chiều), 100 Mbps Token ring (HSTR- high speed token ring).
7. Ethernet và chuẩn IEEE 802

8. Giới thiệu chung về Ethernet. Thành phần mạng Ethernet, những đặc điểm cơ bản của mạng Ethernet
9. Vai trò, chức năng các tầng trong IEEE 802
10. LLC Header:
11. Các dịch vụ tầng con LLC
12. Tầng Ethernet Mac sublayer:
13. Định dạng khung Ethernet:
14. Họ IEEE 802
15. Chuẩn IEEE 802.5:
16. IEEE 802.6 và các mạng IEEE 802.6
17. IEEE 802.9:
18. IEEE 802.10
19. IEEE802.11:
20. IEEE 802.12
21. IEEE 802.14:
22. Ethernet 100 Mbps.
23. Gigabit Ethernet.
24. Mạng cục bộ Token Ring
25. Chuẩn Token Ring
26. Giao diện số liệu phân bố sử dụng quang FDDI
27. Sự tương quan gữa FDDI và mô hình OSI
28. So sánh FDDI và IEEE 802.5
29. Các kiểu kết nối đầu cuối FDDI
30. Khả năng chịu lỗi của FDDI
31. Khuôn dạng tổng quát của FDDI Frame
32. Mạng LAN ATM, Đặc trưng và các loại ATM LAN
33. Kỹ thuật chuyển mạch ATM LAN
34. Kiến trúc giao thức ATM LAN
35. Tầng nào thay đổi, duy trì tuyến kết nối giữa các thiết bị truyền thông.

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
Km10 Đường Nguyễn Trãi, Hà Đông-Hà Tây
Tel: (04).5541221, Fax: (04).5540587
Website: http://www.e-ptit.edu.vn; E-mail: dhtx@e-ptit.edu.vn
ĐẠI HỌC TỪ XA

# CHƯƠNG 5: KỸ THUẬT MẠNG DIỆN RỘNG WAN

Nội dung của chương này sẽ trình bày tổng quát về mạng diện rộng WAN và các loại mạng diện rộng: mạng tích hợp đa dịch vụ số ISDN, B_ISDN, mạng chuyển mạch gói X25, chuyển mạch khung Frame Relay và các ưu nhược điểm của nó và phương thức truyền dẫn không đồng bộ ATM.

- Liên kết liên mạng.
- Mạng tích hợp đa dịch vụ số ISDN
- Băng rộng B_ISDN
- Mạng chuyển mạch gói và chuyển mạch khung Frame Relay.
- Dịch vụ chuyển mạch dữ liệu megabit
- Phương thức truyền dẫn không đồng bộ ATM

## 5.1. Khái niệm về liên mạng (Internetworking)

Liên mạng (internetworking) là một tập các mạng riêng lẻ được nối với nhau bởi các thiết bị mạng trung gian, có chức năng như là một mạng đơn. Các mạng thành phần tạo nên liên mạng được gọi là mạng con (Subnetworks), Các thiết bị được nối đến các mạng con được gọi là hệ thống đầu cuối (End nodes) và những thiết bị nối các mạng con lại với nhau được gọi là các thiết bị liên kết liên mạng (Intermediate nodes*)*

Thuật ngữ "internetworking" thường được sử dụng dưới dạng rút gọn là "internet". Một cách chung nhất, internet là một tập hợp các mạng được nối với nhau. Khi sủ dụng "I" hoa ở trước, thì thuật ngữ "Internet" là đề cập đến mạng internetwork toàn cầu, bao gồm hàng triệu mạng trên thế giới liên kết với nhau và hoạt động theo chuẩn TCP/IP.

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. Phương pháp liên kết tại tầng vật lý, cùng cấu trúc và phương thức trao đổi thông tin. Bộ lặp Repeater hoạt động tại tầng vật lý, là thiết bị được sử dụng để mở rộng chiều dài của một mạng LAN. Phương pháp liên kết tại tầng liên kết dữ liệu (Datalink), có cấu trúc khác nhau và phương thức trao đổi thông tin khác nhau. Cầu (Bridge) và các bộ chuyển mạch (Switched) tầng 2 hoạt động 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. Phương pháp liên kết sử dụng tầng mạng (Network Layer) hay tầng Internet (Inernet Layer) cho các mạng khác nhau về phần cứng, khác nhau về phần mền, 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. Việc nối kết được thực hiện bởi việc định dạng gói tin từ một mạng đến một mạng khác bởi thông tin điều khiển tầng mạng như địa chỉ nguồn, địa chỉ đích. Thực hiện chuyển đổi giao thức mạng (Network Protocol Translation). Một thiết bị cung cấp các liên kết tại tầng mạng được gọi là một bộ định tuyến (Router). Chức năng chủ yếu của một Router là liên kết các mạng khác nhau về vật

lý và chuyển đổi các gói tin từ một mạng này sang một mạng khác, quyết định đường đi của các gói tin đến node đích.

## 5.2. Mạng tích hợp đa dịch vụ số ISDN (Integrated Service Digital Network)

### 5.2.1. ISDN là gì

Khái niệm về mạng tích hợp đa dịch vụ số được CCITT định nghĩa là: "Một mạng viễn thông, dựa trên kỹ thuật chuyển kênh và chuyển mạch gói, cung cấp các đường truyền số, có khả năng phục vụ nhiều loại dịch vụ khác nhau, bao gồm dịch vụ thoại và phi thoại. Các thuê bao liên kết mạng phải tuân theo các chuẩn …"

Mạng ISDN có những đặc điểm sau:

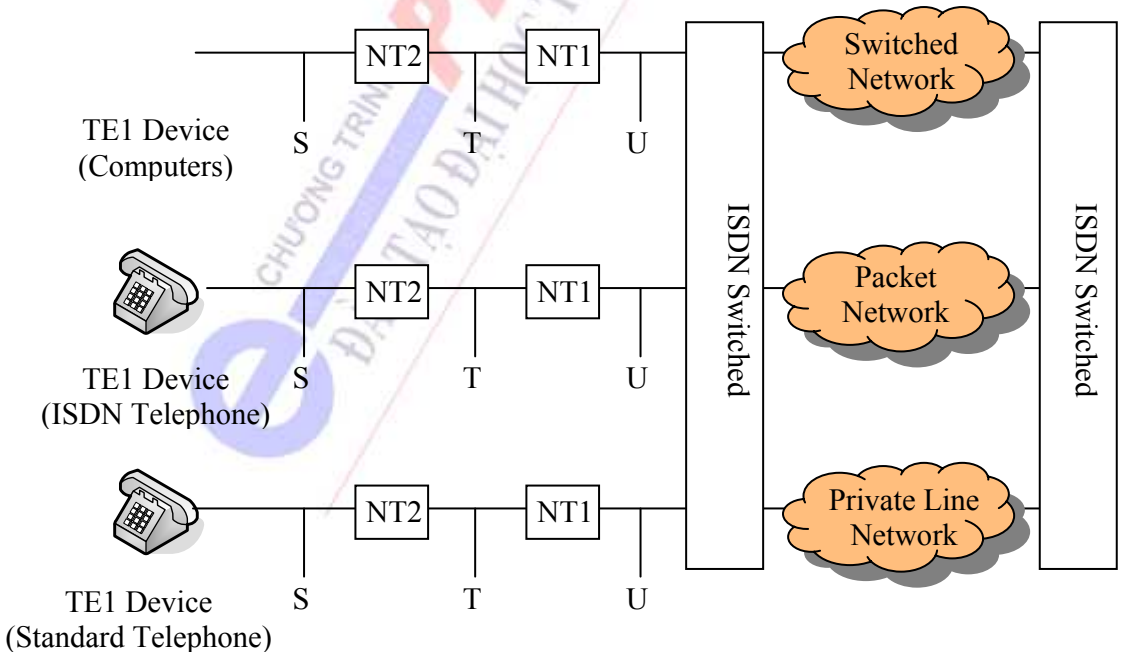
- Là một mạng đa dịch vụ, thay thế nhiều mạng viễn thông khác nhau đang cùng tồn tại bằng một mạng duy nhất có khả năng cung cấp tất cả các dịch vị hiện tại và các dịch vụ tương lai với một giao tiếp thuê bao duy nhất.

- ISDN có hệ thống báo hiệu số 7 và các node chuyển mạch thông minh.

- Kiến trúc ISDN tương thích với mô hình OSI. Các giao thức đã được phát triển có liên quan tới các ứng dụng của mô hình OSI có thể sử dụng được trong ISDN. Các giao thức có thể phát triển sử dụng một cách độc lập cho các tầng khác nhau, cho các chức năng riêng của từng tầng mà không ảnh hưởng đến các tầng kề nhau.

Mục tiêu chính của mạng là chuẩn hoá tất cả các thiết bị đầu cuối, cho phép các phương tiện như âm thanhi, hình ảnh, văn bản...được tích hợp chung vào một mạng duy nhất. Nhằm sử dụng có hiệu quả các tài nguyên của mạng.

Nguyên lý chung của ISDN là liên kết các thiết bị đầu cuối khác nhau lên cùng một đường dây thuê bao và có thể đồng thời truyền thông số giữa thuê bao và mạng. Cước phí được tính theo dung lượng thông tin truyền đi, không tính riêng cho mỗi loại dịch vụ sử dụng. Các dịch vụ khác nhau được hỗ trợ bởi hệ thống báo hiệu số 7 giữa mạng và báo hiệu DSS1 thuê bao.



### 5.2.2. Các phần tử cơ bản của mạng ISDN

- TE1 (Termination Equipment 1) là các thiết bị đầu cuối có các thuộc tính ISDN như: điện thoại số ISDN, các đầu cuối thoại, số liệu, digital fax,…

- TE2 (Termination Equipment 2) là các thiết bị đầu cuối không có tính năng ISDN, để có thể liên kết với ISDN phải có thêm các bộ phối ghép đầu cuối TA (Terminal Adapter).

- NT1 (Network Termination 1):Thực hiện các chức năng thuộc tầng vật lý của mô hình OSI, tức là các tính năng về điện, về giao tiếp giữa ISDN và người sử dụng, các chức năng kiểm soát chất lượng đường truyền, đấu vòng,…

- NT2 (Network Termination 2) là một thiết bị thông minh có khả năng đáp ứng các chức năng đến tầng mạng của mô hình OSI. NT2 có thể là tổng đài riêng PBAX, bộ điều khiển đầu cuối hoặc là mạng cục bộ LAN.

R, S, T, U : Các điểm chuẩn phân cách (R: rate, S: system, T: terminal, U: user)

### 5.2.3. Các loại kênh trong mạng ISDN

"Kênh" là đường truyền thông tin giữa người sử dụng và mạng, được gọi là kênh thuê bao. Trong ISDN kênh thuê bao chỉ truyền các tín hiệu số và được chia thành 3 loại kênh cơ bản: kênh D, kênh B và kênh H, được phân biệt với nhau về chức năng và tốc độ:

* Kênh D: Dùng để truyền báo hiệu giữa người sử dụng và mạng. Vì có thể không sử dụng hết băng tần của kênh, nên có thể dùng kênh D để truyền dữ liệu người sử dụng. Kênh D hoạt động với tốc độ 16 Kbps hoặc 64 Kbps, phụ thuộc vào giao diện người sử dụng.

* Kênh B: Dùng để truyền tín hiệu tiếng nói, âm thanh (Audio), số liệu và hình ảnh (Video) của người sử dụng. Kênh B luôn hoạt động ở tốc độ 64 Kbps. Ba loại liên kết có thể thiết lập qua kênh B :

- Chuyển mạch kênh (Circuit-switched): Quá trình thiết lập liên kết không thực hiện trên kênh B mà sử dụng hệ thống báo hiệu kênh chung.

- Chuyển mạch gói (Packet-switched): Thuê bao được nối tới một node chuyển mạch gói và số liệu sẽ được chuyển đổi nhờ chuẩn X25.

- Liên kết bán cố định (Semipermanent): loại liên kết này không đòi hỏi thủ tục thiết lập liên kết, tương tự như thuê bao kênh riêng (Leased line).

* *Kênh H* cung cấp các dịch vụ tốc độ cao và ghép các luồng thông tin ở tốc độ thấp hơn. có 4 loại kênh H :

- Kênh H0 : tương đương với 6 kênh B, có tốc độ 384 Kbps.

- Kênh H10 : tương đương với 23 kênh B, có tốc độ 1.472 Mbps.

- Kênh H11 : tương đương với 24 kênh B, có tốc độ 1.536 Mbps.

- Kênh H12 : tương đương với 30 kênh B, có tốc độ 1.920 Mbps.

### 5.2.4. Giao diện ISDN

- Giao diện BRI (Basic Rate Interface): Có cấu trúc kênh là 2B+D, trong đó kênh D hoạt động với tốc độ 16 Kbps. Tổng cộng tốc độ của giao diện này là 144 Kbps nhưng trong thực tế

cấu trúc của giao diện tốc độ cơ sở có thể lên tới 192 Kbps. Giao diện này dành cho các thuê bao nhỏ để cung cấp các dịch vụ truy nhập mạng bằng các thiết bị đầu cuối đa năng hoặc các thiết bị riêng lẻ.

- Giao diện PRI (Primary Rate Interface): Dùng cho thuê bao có dung lượng lớn như tổng đài PBAX hoặc các mạng cục bộ LAN. Do các tiêu chuẩn truyền dẫn khác nhau nên có 2 loại truy nhập là: 23B+D cho tiêu chuẩn Bắc Mỹ 1544 Kbps và 30B+D cho tiêu chuẩn Châu Âu 2048 Kbps (ở giao diện này kênh D luôn có tốc độ là 64 Kbps).

### 5.2.5. Chức năng các tầng trong kiến trúc ISDN

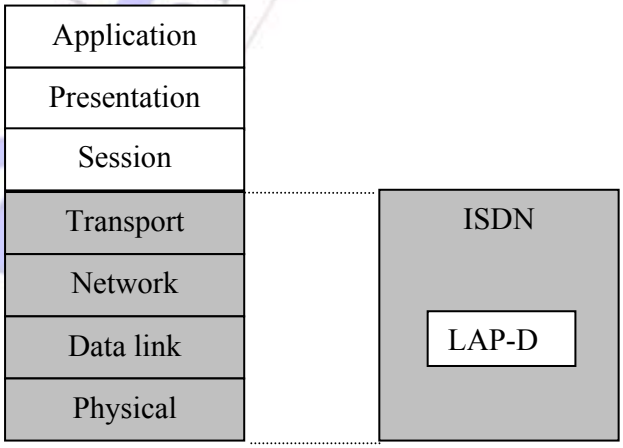
Mạng ISDN là sự tích hợp kỹ thuật chuyển mạch kênh và chuyển mạch gói, trên cơ sở số hoá toàn bộ mạng lưới. Vì vậy nó có ưu thế về dịch vụ mà chưa một mạng nào có được.

*** Tầng vật lý trong ISDN:** Cấu trúc trong tầng này phụ thuộc vào hướng liên kết từ thiết bị đầu cuối đến mạng hay từ mạng đến thiết bị đầu cuối. Giao diện của tầng gồm:

- NT Frame (Network to Terminal)
- TE Frame (Terminal to Network)

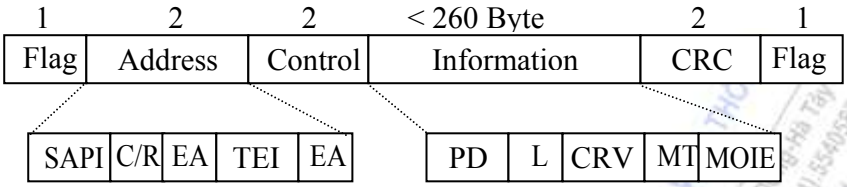
*** Tầng 2 trong ISDN:** Tương ứng với tầng liên kết dữ liệu (Data Link Layer) của mô hình OSI. Hoạt động trong tầng này có giao thức LAP-D (Link Access Protocol - D channel). LAP-D được dẫn xuất từ giao thức HDLC (High Level Data Link Control). LAP-D thực hiện các chức năng sau đây :

- Cung cấp dịch vụ thiết lập một hay nhiều liên kết Data Link trên cùng kênh D cho các hoạt động của các thực thể tầng 3
- Tạo khung (Frame).
- Kiểm soát đồng bộ.
- Phát hiện lỗi và tự động phát lại khung có lỗi.
- Ghi nhận các sai sót về thủ tục.
- Kiểm soát luồng.
- Các chức năng giám sát tầng 2.




**Hình 5.2: Kiến trúc ISDN và mô hình OSI**

Cấu trúc khung của LAP-D như sau.




**Hình 5.3: Cấu trúc khung và các trường của LAP-D**

Flag : biểu thị sự bắt đầu hay kết thúc của khung.

Address : Địa chỉ ISDN.

- SAPI (Service Access Point Identifier):Điểm truy nhập dịch vụ cho tầng 3 (6 bit).
- C/R (Command/ Response): Khung này là một lệnh hay một đáp ứng (1 bit).
- EA (Extended Address - Higher/Lower Order) bắt đầu hay kết thúc của trường địa chỉ (bằng 1 là byte cuối của địa chỉ) (2 bit).
- TEI (Terminal Endpoint Identifier) :địa chỉ đặc biệt hoặc ấn định ID cho mỗi thiết bị đầu cuối ISDN liên kết với mạng ISDN thông qua giao diện S/T (7 bit ).

Control : Trường điều khiển.

Information : Trường dữ liệu

- PD (Protocol Discriminator) (1 byte).
- L (Length) cho biết chiều dài của trường CRV (1 byte).
- CRV (Call Reference Value) thiết lập số hiệu cho mỗi cuộc gọi (1 hoặc 2 byte).
- MT (Message Type) Loại Message (1byte).
- MOIE (Mandatory/ Optional Information Elements)

CRC : Trường kiểm tra.

*** Tầng 3 trong ISDN:** Chức năng của tầng này là thiết lập, duy trì và giải phóng các liên kết. Các thực thể tầng 3 sẽ cung cấp các thông điệp (Message) để truyền trong các trường tầng 2. Các thông điệp thường có độ dài 8 bit và có nhiều loại thông điệp sử dụng trong các trường hợp khác nhau. Ví dụ như thông điệp SETUP (00000101) thiết lập cuộc gọi.

Mạng tích hợp đa dịch vụ số ISDN nếu được triển khai sẽ thực sự là một cuộc cách mạng trong công nghệ thông tin. Từ một mạng duy nhất nó có thể cung cấp các dịch vụ khác nhau mà hiện nay đang được cung cấp bởi các mạng viễn thông khác nhau. Việc triển khai ISDN không chỉ dừng lại ở việc nâng cấp các hệ thống viễn thông hiện có để có khả năng truyền tải được những dòng dữ liệu lớn với tốc độ nhanh mà còn phải tiến hành đồng bộ về phía người dùng và về phía các nhà cung cấp dịch vụ.

## 5.3. Mạng băng rộng B_ISDN (Broadband ISDN)

### 5.3.1. Tổng quan về sự ra đời của B-isdn

Giữa thập kỷ 80, CCITT đã triển khai nghiên cứu mô hình mạng viễn thông mới gọi là ISDN băng rộng (Broadband- ISDN). B-ISDN là mạng thông tin số đa dịch vụ, trợ giúp tất cả các ứng dụng đa dịch vụ trên cùng một hệ thống mạng. Nghĩa là mạng phải có khả năng cung cấp các dịch vụ truyền thông với tốc độ thay đổi từ một vài Kbps đến hàng trăm Gbps cho các loại kênh Analog và kênh Digital bao gồm những dịch vụ đang có và những dịch vụ sẽ có trong tương lai. Công nghệ truyền dẫn không đồng bộ ATM dựa trên nguyên lý truyền dẫn và chuyển mạch gói được CCITT chọn làm giải pháp cho B-ISDN. Đầu những năm 90 các khuyến nghị cho B-ISDN dựa trên công nghệ ATM đã được ban hành.

Giao tiếp B-ISDN ban đầu cung cấp tốc độ truyền 51 Mbps, 155 Mbps hoặc 622 Mbps trên đường cáp quang. Tầng vật lý hỗ trợ B-ISDN được cung cấp bởi SONET (Synchronous Optical Network) và ATM (Asynchronous Transfer Mode). Tầng Client có thể hỗ trợ Frame Relay, SMDS hoặc IEEE 802.2

B-ISDN có thể được xem như một mạng thông tin được phát triển từ mạng ISDN băng hẹp hiện đang được sử dụng.

<table>
<tr><td rowspan="2">B-ISDN</td><td>IEEE 802.2</td><td>SMDS</td><td>Frame Relay</td><td>Other Services</td></tr>
<tr><td>Adaptation Layer</td><td>Adaptation Layer</td><td>Adaptation Layer</td><td>Adaptation Layer</td></tr>
<tr><td colspan="5">ATM</td></tr>
<tr><td colspan="5">SONET/SDH, FDDI ...</td></tr>
</table>

**Hình 5.4: B-ISDN hỗ trợ cơ sở hạ tầng**

### 5.3.2. Đặc điểm của dịch vụ B-ISDN

Mục tiêu của B-ISDN là kết hợp tất cả các dịch vụ hiện có vào một mạng truyền thông duy nhất. Về cơ bản nó cung cấp các dịch vụ băng hẹp. Ngoài ra, nó có khả năng cung cấp nhiều dịch vụ băng rộng như điện thoại thấy hình, hội nghị từ xa, truyền số liệu tốc độ cao...

B-ISDN có khả năng cung cấp dịch vụ băng rộng tốc độ đến Mbit/s, còn các tần số mà nó sử dụng và phân bố thời gian sử dụng thì có phạm vi rất rộng.

Đặc tính phân bố khác của tín hiệu dịch vụ B-ISDN là các tín hiệu liên tục. Các tín hiệu tiếng nói và hình ảnh có thể cùng "sống chung" với các tín hiệu nhóm như số liệu đầu cuối. Tuy nhiên, các tín hiệu dữ liệu khác nhau có các tốc độ biến đổi rất rộng. Mặt khác, các tín hiệu hình ảnh và âm thanh đòi hỏi phải xử lý theo thời gian thực.

Kỹ thuật chuyển mạch gói lý tưởng đối với tốc độ thấp hoặc số liệu nhóm, trong khi đó, đối với tín hiệu thoại và hình ảnh thì chuyển mạch kênh là thích hợp. Ngoài ra với các tín hiệu thoại

cũng thích hợp chuyển mạch phân chia thời gian và với các tín hiệu video tốc độ cao thì thích hợp với chuyển mạch kênh phân chia theo không gian.

Vì vậy, tìm được một hệ thống truyền dẫn có khả năng trao đổi các tín hiệu tốc độ thấp/cao và các tín hiệu liên tục/ nhóm là cực kỳ khó khăn.

### 5.3.3. Cấu trúc chức năng của B_ISDN

Mô hình cấu trúc chức năng chung của ISDN băng rộng về cơ bản giống như ISDN băng hẹp. Có nghĩa là về mặt cấu hình tiêu chuẩn, nhóm chức năng và điểm gốc, cả hai cấu trúc đó là như nhau. Nó chỉ ra rằng B-ISDN được hình thành trên cơ sở khái niệm của ISDN. Cấu trúc của ISDN băng rộng bao gồm khả năng mức cao và khả năng mức thấp.

Khả năng mức cao là chức năng liên quan đến thiết bị đầu cuối (TE) và khả năng mức thấp bao gồm khả năng ISDN băng hẹp dựa trên khả năng băng rộng, 64 bit/s và khả năng báo hiệu liên tổng đài.

### 5.3.4. So sánh giữa ISDN và B_ISDN

B-ISDN là một mạng số liên kết đa dịch vụ như ISDN, nhưng việc thiết lập B-ISDN thực hiện khác với thiết lập ISDN. B_ISDN nó bảo đảm liên kết các tín hiệu băng rộng và có khả năng đồng thời xử lý các tín hiệu băng rộng băng hẹp. Mô hình cấu trúc cơ bản của B-ISDN và ISDN như nhau. Tuy nhiên, chúng chỉ tương tự nhau về mặt khái niệm mà không tương thích về mặt hoạt động. Các thiết bị B_ISDN không thể hoạt động nếu đấu nối vào mạng ISDN hoặc TE của ISDN không thể đấu nối tới NT của B-ISDN. Trong thực tế B-ISDN khác rất xa với ISDN, vì ISDN tích hợp kỹ thuật chuyển mạch kênh và kỹ thuật chuyển mạch gói, trong khi đó B-ISDN sử dụng công nghệ ATM hoàn toàn khác với các hệ thống của ISDN. Nghĩa là, trong khi ISDN chủ yếu điều khiển hệ thống thông tin chuyển mạch kênh thì B-ISDN chủ yếu sử dụng hệ thống thông tin chuyển mạch gói, đồng thời vẫn điều khiển hệ thống thông tin kênh. B-ISDN khác hẳn so với ISDN.

Sự phát triển của ISDN và B_ISDN là bước đệm cho sự ra đời các kỹ thuật mạng viễn thông mới với mục đích cung cấp đa dịch vụ trên cùng một mạng viễn thông duy nhất. Mạng thế hệ sau NGN đang được nghiên cứu và phát triển đáp ứng nhu cầu ngày càng cao của xã hội, đó là một bước tiến mới trong kỹ thuật mạng viễn thông? Một câu hỏi được giải đáp trong tương lai không xa.

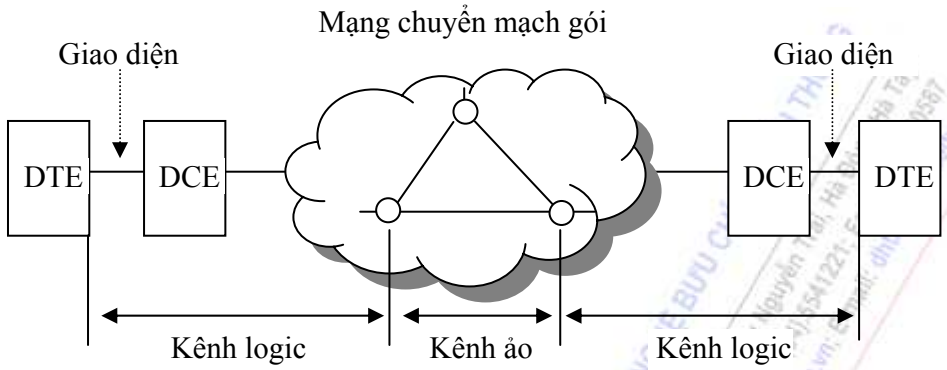
## 5.4. Mạng chuyển mạch gói X25

### 5.4.1. Khái quát kỹ thuật mạng X25

X25 định nghĩa chuẩn giao diện giữa các thiết bị đầu cuối số liệu của người sử dụng DTE (Data Terminal Equipment) với thiết bị kết cuối kênh dữ liệu DCE (Data Circuit Terminating). X25 có chức năng vừa điều khiển giao diện DTE/DCE vừa thực hiện chức năng truyền dữ liệu giữa DTE với node của mạng chuyển mạch gói. Các mạng X.25 cung cấp các lựa chọn cho chuyển mạch ảo hoặc cố định. X.25 cung cấp các dịch vụ tin cậy cũng như điều khiển luồng dữ liệu từ node tới node (End to End).

Các mạng X25 có tốc độ tối đa 64 Kbps. Tốc độ này thích hợp với các tiến trình truyền thông chuyển giao tệp và các thiết bị đầu cuối có lượng lưu thông lớn. Tuy nhiên với tốc độ như vậy không thích hợp với việc cung cấp các dịch vụ đòi hỏi từ 1 Mbps trở lên. Vì vậy các mạng

X25 không hấp dẫn khi cung cấp các dịch vụ ứng dụng LAN trong môi trường WAN. Năm 1976, CCITT công bố khuyến nghị loại X về giao thức X25 trong các mạng chuyển mạch gói công cộng (Public Packet Switched Networks).

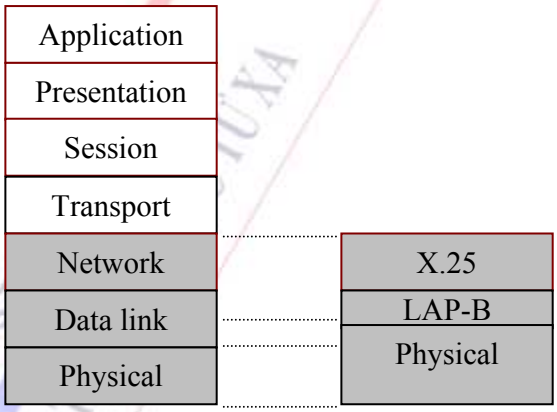



**Hình 5.5: Một ví dụ mạng X25 đơn giản**

### 5.4.2. Giao thức X.25

X25 hoạt động trên 3 tầng: tầng vật lý, tầng liên kết dữ liệu và tầng mạng.

*Tầng vật lý:* Tương ứng với tầng vật lý mô hình OSI, giao thức X25.1 xác định các vấn đề về điện, hàm, thủ tục và kiểu các bộ đấu chuyển được sử dụng. Bao gồm các chuẩn của CCITT X26/27 và EIA (USA Electronic Institue Association), RS :X.21, X.21 Bis, V.32...




**Hình 5.6: Mối quan hệ X.25 vơíi mô hình OSI**

*Tầng liên kết dữ liệu:* X.25.2 cung cấp các liên kết giữa hai thiết bị đầu cuối của một tuyến thông tin có độ tin cậy cao, kiểm soát luồng và kiểm soát lỗi. LAP-B (Link Access Procedure Balanced) là giao thức LLC tầng con của Liên kết dữ liệu, chuẩn hướng bit, hoạt động theo chế độ song công và đồng bộ.

*Tầng cấp mạng:* X.25.3 là giao thức giữa một DTE và một DCE. DTE có thể là một PAD còn DCE có thể là một thiết bị X.25. Giao thức X.25 cung cấp các khả năng chọn mạch ảo thường trực hay theo nhu cầu. X.25 yêu cầu cung cấp dịch vụ tin cậy và tính năng điều khiển luồng dữ

liệu End to End. Do các thiết bị trên mạng có thể hoạt động theo nhiều mạch ảo, nên X25 phải cung cấp tính năng điều khiển luồng cho mỗi mạch

Bảng sau tổng kết các chức năng của các tầng trong mô hình X25:

| | |
|---|---|
| Tầng 1: | Đồng bộ hoá liên kết |
| Tầng 2: | Phát hiện lỗi và phát lại.<br>Điều khiển luồng |
| Tầng 3: | Tạo số thứ tự gói tin.<br>Truyền dữ liệu theo phương thức Datagram<br>Thực hiện ghép kênh.<br>Thiết lập kết nối và giảI phóng kênh ảo.<br>Thực hiện báo hiệu |

### 5.4.3. Hoạt động của giao thức X25

X25 hoạt động dựa trên cơ sở kênh cố định PVC (Permanent Virtual Chanel) và kênh ảo chuyển mạch SCV (Switch Virtual Chanel). PCV thay thế chức năng cho kênh liên kết điểm-điểm cố định giữa các thiết bị đầu cuối. Sử dụng loại kênh này, giao diện có hiệu quả hơn nhờ sự liên kết được đảm bảo và không bị trễ cuộc gọi. SVC sử dụng tối đa sự mềm dẻo linh hoạt của chuyển mạch gói trong thực tế.

Hoạt động của X25 theo các giai đoạn: giai đoạn thiết lập kênh ảo, giai đoạn trao đổi thông tin và giai đoạn giải phóng kênh ảo. Ngay sau khi thiết lập kênh ảo, một thông báo tóm tắt của cấu trúc gói tin sẽ được node nguồn gửi đi đến node đích. Nếu chấp nhận, node đích sẽ hiển thị và thông báo lại cho node nguồn. Đường truyền song hướng được thiết lập. Giai đoạn trao đổi dữ liệu: Node nguồn gửi khung thông tin, node đích sẽ tiến hành kiểm tra tính hợp lý của khung thông qua các bit FCS. Nếu không hợp lý thì loại bỏ khung và gửi thông báo lại cho node nguồn biết, yêu cầu truyền lại. Nếu khung là hợp lý thì node này tiếp tục các thủ tục truyền gửi khung tới node tiếp theo trong mạng, đồng thời thông báo lại cho node nguồn biết là đã nhận được thông tin. Node nguồn sau khi đã nhận được thông báo âm từ node đích, tiếp tục gửi gói tin tiếp theo...Sau khi kết thúc, kênh ảo sẽ được giải phóng.

Như vậy hoạt động của X25 cho phép sử dụng một cách có hiệu quả kênh thông tin liên kết giữa người sử dụng và các node mạng. Các thủ tục của tầng mạng đảm bảo trao đổi thông tin có tỷ lệ lỗi bit thấp, với xác suất lớn các gói tin được gửi tới đích không có lỗi, đúng thứ tự, điều này rất cần thiết đối với các đường truyền có độ tin cậy không cao.

## 5.5. Mạng chuyển mạch khung Frame Relay

### 5.5.1. Giới thiệu chung

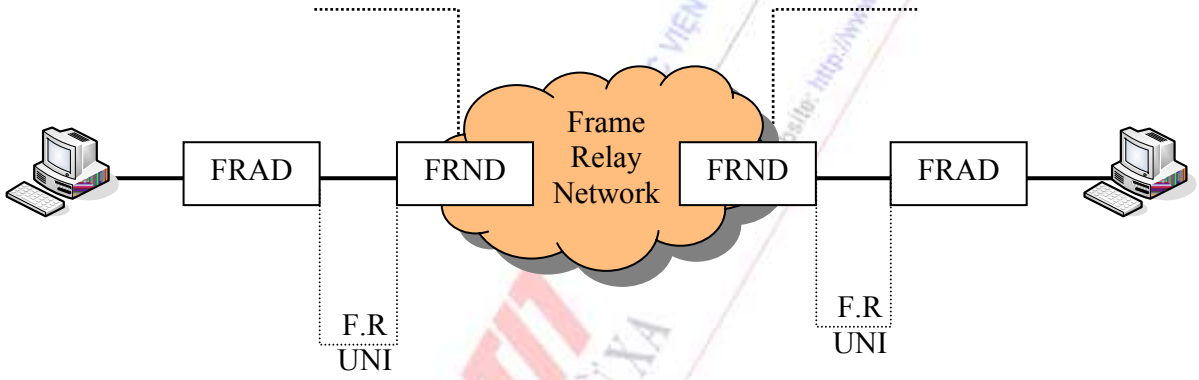
Những năm cuối của thế kỷ XX các hệ thống viễn thông sử dụng công nghệ cáp quang có độ tin cậy cao, đảm bảo tốc độ và chất lượng truyền dẫn, giảm thiểu tình trạng nghẽn mạch và tỉ lệ lỗi dữ liệu. Các giao thức trước đây cho mạng chuyển mạch gói đặc tả các thủ tục quản lý lưu

lượng, quản lý tắc nghẽn và xử lý lỗi, đảm bảo tính thống nhất, toàn vẹn thông tin trên đường truyền đã trở nên phức tạp, cồng kềnh, làm giảm thông lượng.

Frame Relay ra đời như là một công nghệ kế thừa những đặc điểm ưu việt của mạng chuyển mạch gói như tính tin cậy, mềm dẻo, khả năng chia sẻ tài nguyên. Đồng thời hạn chế tối đa thủ tục kiểm soát, hỏi đáp.. không cần thiết gây ra độ trễ lớn. Nó cho phép tận dụng các ưu thế về tốc độ truyền tải và tính ổn định của công nghệ truyền dẫn, thỏa mãn nhu cầu dịch vụ tốc độ cao, sử dụng nhiều thông lượng mạng diện rộng WAN trên đó truyền tải một lượng lớn dữ liệu với nhiều định dạng khác nhau.

Công nghệ Frame Relay tích hợp tính năng dồn kênh tĩnh và chia sẻ công nghệ X.25. Dữ liệu được tổ chức thành các khung có độ dài không cố định được đánh địa chỉ tương tự như X.25. Tuy nhiên, khác với X.25, Frame Relay loại bỏ hoàn toàn các thủ tục ở tầng 3 trong mô hình OSI. Chỉ một số chức năng chính ở tầng 2 được thực hiện. Vì vậy tốc độ truyền trong mạng Frame Relay cao hơn nhiều so với X.25 và mạng Frame Relay được gọi là mạng chuyển mạch gói tốc độ cao.

### 5.5.2. Cấu hình tổng quát mạng Frame Relay




**Hình 5.7 Cấu trúc mạng Frame Relay**

Hình 5.7 trình bày các thành phần chính của mạng Frame Relay. Các kênh riêng tạo ra liên kết vật lý giữa DTE và DCE. DTE còn được gọi là thiết bị truy nhập mạng FRAD (Frame Relay Access Device) thường là các Router, Bridge, ATM Switch... DCE còn được gọi là thiết bị mạng FRND (Frame Relay Network Device) là các thiết bị chuyển mạch Frame Relay Switch. FRAD và FRND chuyển đổi dữ liệu thông qua các quy định của giao tiếp UNI. Mạng trục của Frame Relay có thể là các mạng viễn thông IP, PSTN...

### 5.5.3. So sánh Frame Relay với X25

Sự khác biệt giữa căn bản giữa công nghệ Frame Relay và X.25 là Frame Relay không kế thừa công nghệ X.25 mà là một giao thức tiên tiến có nhiều điểm tương đồng với X.25. X.25 là một giao thức của công nghệ chuyển mạch gói, đặc tả giao tiếp giữa DTE và DCE.

Dữ liệu trong tầng 3 của X.25 sẽ được chia thành các gói (Packet), trong mỗi gói được bổ sung phần Network Header. Các gói này sẽ được chuyển xuống tầng 2, các hàm chức năng của LAP-B sẽ bổ sung Layer 2 Header và các Flag vào mỗi gói tạo thành các khung LAP-B. Các khung sẽ được chuyển xuống tầng vật lý và truyền đến đích.

Hoạt động của các thực thể chặt chẽ, các node mạng X25 phải luôn biết trạng thái của mạng trong mỗi liên kết logic. Các gói tin điều khiển và báo nhận, báo mất (ACK/NACK) thường xuyên được truyền trên cùng liên kết của gói tin dữ liệu không chỉ tại các giao tiếp DTE-DCE mà còn tại tất cả các node mạng. Tại các node mạng phải duy trì bảng trạng thái cho mỗi liên kết logic để quản lý liên kết và điều khiển lỗi và lưu lượng, đảm bảo gói tin đến đúng địa chỉ đích được lưu trong Network Header và số lượng gói tin gửi vào mạng không được vượt quá khả năng xử lý của mạng. Như vậy các giao thức tại tầng mạng là tuyệt đối cần thiết nhất là khi triển khai hệ thống mạng X.25 trên các đường truyền có độ tin cậy thấp, dễ bị nhiễu loạn, suy giảm tín hiệu...

Frame Relay được thiết kế để loại bỏ những hạn chế trong các mạng X.25 khi triển khai trên tuyến truyền dẫn tốc độ cao bằng cách:

- Các gói tin điều khiển và dữ liệu được truyền trên các liên kết logic riêng biệt. Vì vậy, tại các node không cần duy trì bảng trạng thái, không xử lý các gói tin điều khiển.

- Dồn kênh, chuyển mạch các liên kết logic được thực hiện ở tầng liên kết. Loại bỏ các quá trình trình xử lý ở tầng mạng.

- Không điều khiển lưu lượng và điều khiển lỗi theo từng đoạn mạng (Hop-by-Hop Control). Trong trường hợp cần thiết sẽ để các tầng cao hơn đảm trách.

Frame Relay chỉ sử dụng một phần các chức năng ở tầng 2 nên khung thông tin của Frame Relay sẽ có cấu trúc đơn giản hơn so với khung thông tin của X.25 nhưng vẫn duy trì đặc điểm của một khung thông tin quy định bởi giao thức điều khiển.

Khung Frame Relay không có Header của tầng mạng. Vì Frame Relay không sử dụng các thủ tục điều khiển lưu lượng, điều khiển lỗi của tầng mạng. Mặt khác, giao thức được sử dụng tại tầng liên kết chỉ là phần lõi của giao thức điều khiển (LAP-F Core) nên việc xử lý tại các node mạng sẽ ít hơn nhiều so với X.25. Kích thước phần dữ liệu (User Data) trong khung Frame Relay có thể tối đa 2048 byte trong khi phần dữ liệu trong khung X.25 chỉ có thể đạt tối đa 128 byte. DCE thực hiện ba chức năng chính:

- Kiểm tra các khung, loại bỏ các khung có lỗi.

- Căn cứ vào địa chỉ trong khung chọn đường.

- Kiểm tra có bị nghẽn hay không. Nếu có thì lập bit báo nghẽn hoặc loại bỏ khung tùy trường hợp cụ thể.

### 5.5.4. Frame Relay và mô hình OSI

*Tầng vật lý*: Các giao thức chuẩn định nghĩa giao tiếp vật lý giữa thiết bị truy nhập FRAD và thiết bị mạng FRND, giữa các node mạng theo chuẩn giao tiếp vật lý của ISDN. Frame Relay tương thích với nhiều giao diện vật lý khác nhau như V.35, X.21...

*Tầng liên kết:* Các thủ tục liên kết của Frame Relay được định nghĩa bằng giao thức truy cập LAP-D và LAP-F. Giao thức truy cập LAP-F được cải tiến từ LAP-D và được sử dụng phổ biến trong các mạng Frame Relay. Để quản lý liên kết và truyền dữ liệu LAP-F chia thành 2 tầng chức năng là Upper Function (LAP-F Upper) và Coreùunction (LAP-F Core).

- Core Function: có các chức năng kiểm soát độ dài khung, phát hiện lỗi đường truyền, điều khiển nghẽn qua trường báo hiệu trong cấu trúc khung.

- Upper Function: có chức năng điều khiển DLCI (Data Link Connection Identifier), xác định liên kết logic giữa FRAD và FRND.

*Tầng mạng (Network Layer):* Tầng mạng định nghĩa các khung dữ liệu lưu chuyển trong hệ thống, đảm bảo việc định tuyến trong một mạng hay giữa các mạng với nhau. Trong Frame Relay, các giao tiếp giữa DTE và DCE tầng 3 không có thủ tục nên tốc độ nhanh hơn nhiều so với X.25. Tuy nhiên, nếu một liên kết logic được thiết lập động (SVC), Frame Relay có thể sử dụng một phần của giao thức đặc tả chuẩn Q.931 của giao thức điều khiển ISDN (còn gọi là Q.933) để thiết lập liên kết.

Giao thức liên kết hai node mạng X.25 là X.75, còn để liên kết hai node mạng Frame Relay người ta sử dụng giao diện NNI (Network to Network Interface).

| Network | X25 PLP | Management | Q.933 Subnet Management | Full Q.933 Management |
|---|---|---|---|---|
| Data Link | LAP - B | LAP - F | LAP - F | LAP - F |
| Physical | X21,V35 (56/64 Kbps) | V35 (DS-0,DS-1..) | V35 (DS-0,DS-1..) | V35 (DS-0,DS-1..) |
| OSI - RM | X25 | PC only (With link Management) | Non ISDN SVC (With link | ISDN SVC (With link Management) |

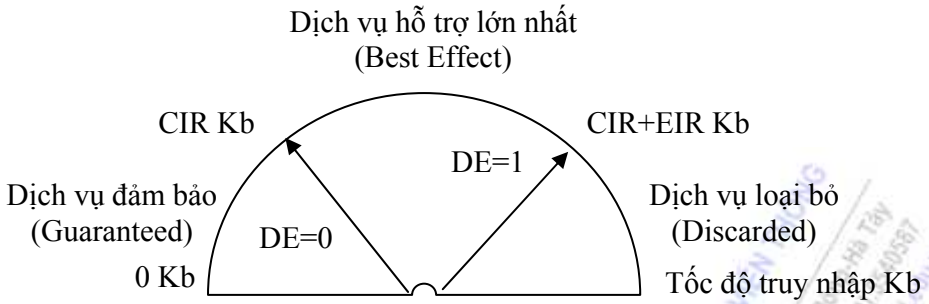
**Hình 5.8: So sánh mô hình OSI với X25 và Frame Relay**

### 5.5.5. Điều khiển quản lý lưu lượng

Hầu hết các nhà cung cấp dịch vụ Frame Relay đều sử dụng phương thức tốc độ cam kết CIR (Committed Information Rate) để giải thích chính xác thông tin nào được truyền đến một dịch vụ đảm bảo, thông tin nào nhận được dịch vụ hỗ trợ lớn nhất và thông tin nào bị loại bỏ ở cổng vào của Frame RelayH node nguồn.

Với lưu lượng trên kênh PVC có tốc độ trong khoảng giữa 0 Kbps và phụ thuộc người sử dụng. Khi đó chúng sẽ được truyền đi bình thường qua mạng mà không bị tổn hao đó là dịch vụ đảm bảo "Guaranteed". Đối với các khung thông tin vượt quá CIR một lượng tốc độ thông tin bùng nổ EIR (Excess Information Rate) thì có thể bị Frame Relay node tiếp theo hủy nếu xảy ra nghẽn. Đây chính là dịch vụ hỗ trợ lớn nhất. Khi dữ liệu vượt quá ngưỡng CIR + EIR thì các khung thông tin sẽ bị hủy ngay bởi Frame RelayH node nguồn cho đến khi tốc độ của người sử dụng giảm xuống dưới ngưỡng CIR + EIR.

Tốc độ EIR thường được các nhà khai thác mạng đặt bằng đúng tốc độ CIR.




DE: Discard Eligibility-Bit đánh dấu khung có khả năng bị loại bỏ
CIR: Committed Information Rate- Tốc độ cam kết.
EIR: Eccess Information Rate- Tốc độ thông tin bùng nổ

**Hình 5.9: Điều khiển quản lý lưu lượng mạng**

### 5.5.6. Các dịch vụ Frame Relay

Hiện nay, phần lớn các dịch vụ mạng Frame Relay được cung cấp dưới hai dạng:

- Mạng dịch vụ công cộng (Public Carrier-Provided Networks): Frame Relay và FRAD, FRND của nhà cung cấp, khách hàng được tính cước trên cơ sở thông số mạng đã thuê, việc bảo trì và quản trị do các nhà cung cấp thực hiện.

- Mạng riêng doanh nghiệp: Các doanh nghiệp có quy mô toàn cầu triển khai các mạng Frame Relay riêng. Toàn bộ thiết bị mạng là tài sản của doanh nghiệp. Công tác quản trị, vận hành và bảo dưỡng do chính doanh nghiệp đó thực hiện.

Hiện tại, ở Việt Nam phổ biến hình thức mạng dịch vụ công cộng do giá thành sử dụng rẻ hơn, không đòi hỏi doanh nghiệp duy trì đội ngũ nhân viên kỹ thuật chuyên trách. Ngân hàng Á Châu (ACB) là một trong số các đơn vị đang khai thác hiệu quả dịch vụ này.

Frame Relay là công nghệ được ưu tiên lựa chọn bởi ngày càng có nhiều người dùng đang tìm kiếm các giải pháp mạng diện rộng trên nền tảng hạ tầng viễn thông hiện đại. Mặt dù đã có nhiều công nghệ mới ra đời có tính năng hiện đại hơn nhưng với xu thế khách hàng đang ưa chuộng mạng trên nền IP, Frame Relay tiếp tục thể hiện tính ưu việt qua khả năng kết hợp mạng IP với các ưu điểm như quản lý dịch vụ dễ dàng, truyền dữ liệu tốc độ cao an toàn, chi phí liên kết thấp. Có thể khẳng định, công nghệ Frame Relay vẫn có thể được tiếp tục sử dụng hiệu quả trong thời gian dài.

## 5.6. SMDS (Switched Multimegabit Data Service)

### 5.6.1. Giới thiệu chung.

SMDS - Switched Multimegabit Data Service là một dịch vụ WAN được thiết kế cho các liên kết LAN-to-LAN. SMDS được Bellcore và Các công ty Regional Bell Operating (RBOCs) phát triển để thoả mãn nhu cầu khách hàng về liên kết LAN Multimegabit trong vùng mạng chính. SMDS được thiết kế là một dịch vụ chuyển mạch gói giá cả hợp lý, cung cấp các liên kết và mở rộng chất lượng cao.

Khác với sự thành công của SMDS ở châu Âu, ở Mỹ SMDS không phát triển. SMDS Interest Group, một tổ chức lớn nhất tài trợ SMDS đã ngừng hoạt động từ năm 1997. Hơn nữa, trong ngày kỷ niệm lần thứ 25 của Truyền thông số liệu - Data Communications (21/10/1997), SMDS được bình chọn là một trong 25 thất bại tiêu biểu nhất - Top 25.

### 5.6.2. SMDS là gì

SMDS là một dịch vụ mạng diện rộng được thiết kế dành cho liên kết từ mạng LAN với mạng LAN. Là một mạng MAN có đặc trưng: đơn vị dữ liệu là tế bào (Cell-based), không liên kết (Connectionless), tốc độ cao, chuyển mạch gói băng thông rộng. SMDS cũng là một dịch vụ dữ liệu, nghĩa là chỉ truyền dữ liệu (mặc dù nó có thể truyền cả âm thanh và hình ảnh). SMDS là một dịch vụ thật sự, không gắn với một công nghệ truyền số liệu nào.

### 5.6.3. Tổng quan về SMDS

Tế bào SMDS là đơn vị cơ bản có độ dài cố định. Tương tự như tế bào của ATM gồm 53 bytes - 44-byte dữ liệu, 7-byte Header và 2-byte dấu vết. Điều này tạo cho nó sự tương thích với các mạng diện rộng công cộng B-ISDN sử dụng công nghệ chuyển mạch gói nhanh và công nghệ ATM. Mỗi tế bào của SMDS chứa địa chỉ đích cho phép các thuê bao SMDS có thể truyền dữ liệu với nhau.Là một dịch vụ dữ liệu không liên kết, SMDS thiết lập một đường kênh ảo (Virtual Circuit) giữa thực thể nguồn và đích, các tế bào dữ liệu truyền đi một cách độc lập với nhau và không theo một thứ tự đặc biệt nào.

Mạng SMDS cung cấp băng thông theo yêu cầu cho các bùng nổ giao thông, một thuộc tính của các ứng dụng mạng LAN.Vì không cần phải định nghĩa trước đường truyền giữa các thiết bị, dữ liệu có thể đi qua những đường ít tắc nghẽn nhất trong mạng SMDS, vì vậy sẽ cung cấp một đường truyền nhanh hơn, tăng tính bảo mật và mềm dẻo hơn Khía cạnh băng rộng của SMDS là từ sự tương thích của nó với B-ISDN và tương thích với chuẩn IEEE 802.6 MAN.

### 5.6.4. Tổng quan về kỹ thuật SMDS

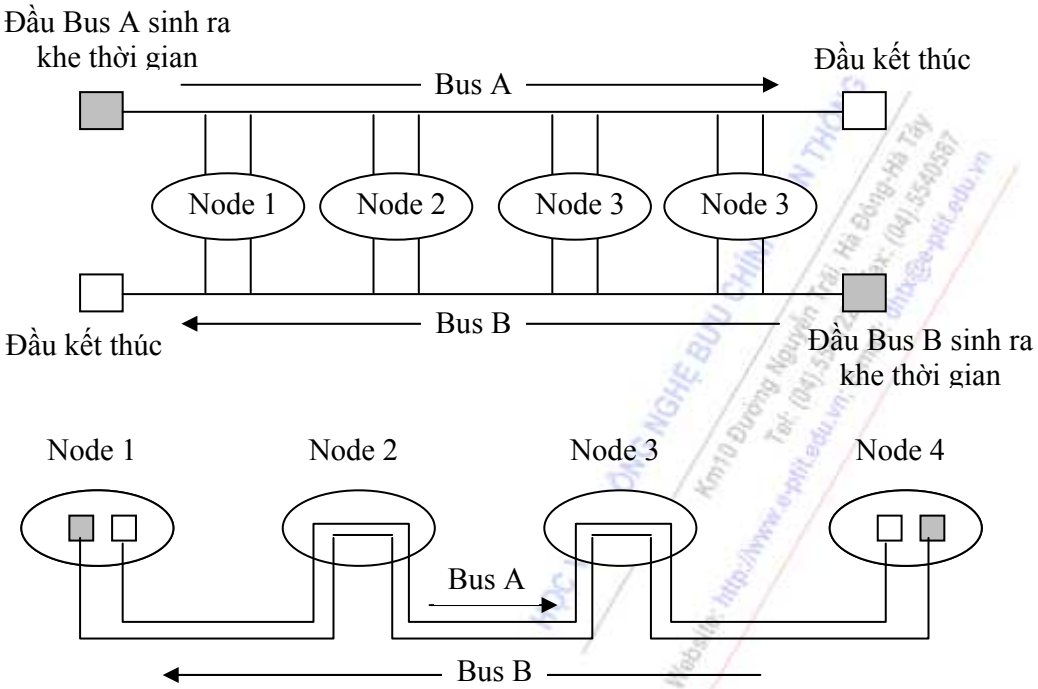
SMDS dựa trên một tập con của tầng vật lý của IEEE 802.6 và chuẩn tầng dưới của MAC (Media Access Control), vì vậy nó hoạt động tương tự như Token Ring tốc độ cao.

- Đặc điểm tầng vật lý: IEEE 802.6 có thể được thiết kế như một Bus hở hoặc một Bus vòng. Khi thiết kế Bus hở, các Bus khởi đầu và kết thúc tại các node khác nhau.Với Bus dạng vòng, các Bus khởi đầu và kết thúc tại cùng một node .

- Đặc điểm tầng liên kết dữ liệu - DQDB (Distributed Queue Dual Bus): Tại tầng liên kết dữ liệu, mạng SMDS được quản lý bởi giao thức DQDB bus quảng bá đa truy nhập. IEEE 802.6, chia nhỏ mỗi bus thành các khe để truyền dữ liệu. Trong mỗi bus có một bit bận và một bit yêu cầu. DQDB làm việc như sau:

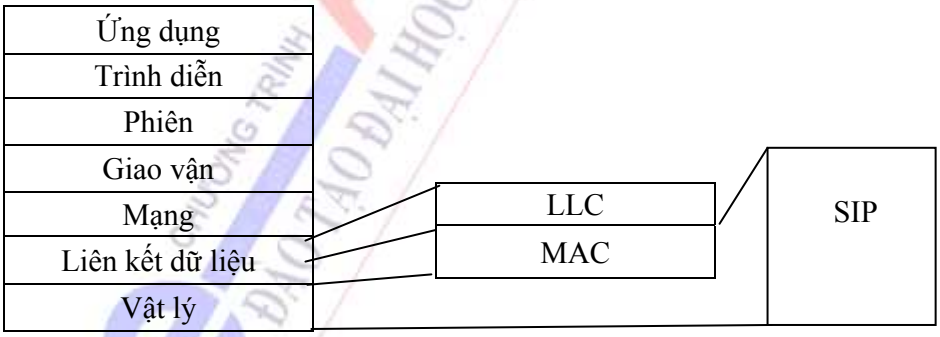
Ví dụ node 2 truyền dữ liệu cho node 3, trước khi truyền, đặt bit Req trên Bus B để thông báo cho các bus phía trên của Bus A biết rằng tại node đó đang có dữ liệu cần gửi. Sau khi yêu cầu một khe, node 2 quan sát cả hai bus và duy trì một số đếm các yêu cầu. Số đếm đó sẽ tăng 1 khi node 2 thấy một bit yêu cầu được thiết lập trên Bus B và giảm đi 1 cho mọi khe trống trên Bus A. Như vậy số đếm tại mỗi node cho biết chiều dài hàng các tế bào đang đợi để truyền bởi các node phía dưới. Khi số đếm bằng 0 nghĩa là không còn node dưới nào có dữ liệu cần gửi thì node đó bắt đầu gửi dữ liệu.

DQDB hỗ trợ dich vụ không liên kết và hướng liên kết và có khả năng truyền dữ liệu, tiếng nói và hình ảnh. Mặc dù là một tập con của IEEE 802.6, SMDS chỉ truyền dữ liệu.




**Hình 5.10: Cấu hình vật lý của mạng SMDS.**

Giao thức giao diện mạng SMDS (SMDS Interface Protocol - SIP): SIP được định nghĩa bởi Bellcore và cấu thành bởi ba mức giao thức: SIP mức 3, SIP mức 2, và SIP mức 1, hoạt động trong tầng Liên kết dữ liệu và tầng vật lý.




**Hình 5.11: Các tầng của SIP tương ứng với mô hình OSI**

### 5.6.5. SMDS so với các công nghệ ATM và Frame Relay.

- SMDS là một dich vụ, không phải một công nghệ; Frame Relay và ATM là công nghệ .

- SMDS dịch vụ chuyển mạch gói không liên kết (Connectionless), Frame Relay và ATM là hướng liên kết (Connection-Oriented).

- SMDS cung cấp nhiều cách quản lý mạng đặc trưng.

- SMDS bị cạnh tranh bởi ATM và Frame Relay ở nước Mỹ.

- DQDB cung cấp các công nghệ cân thiết cho sự truyền các ứng dụng thời gian thực.

- SDMS hỗ trợ tính bảo mật, cho phép dùng các mạng công cộng, chia sẻ một mạng riêng như mạng xương sồng. Khái niệm này đã bị che lấp bởi Internet và VPN.

Là một dich vụ, không phải là một công nghệ nên có thể triển khai trên cả Frame Relay và ATM. Không phụ thuộc về giao thức, nên có thể hỗ trợ nhiều giao thức mạng LAN hay mạng máy tính. Có băng thông từ 56/64 Kbps tới tốc độ SONET, phù hợp với giải thông cho mọi ứng dụng. Là dịch vụ không liên kết, không cần định nghĩa các PVC như Frame Relay. Tế bào 53 byte tương thích với ATM, có thể chuyển đổi thuận tiện sang mạng ATM.

Tuy nhiên một số điểm không thuận lợi đã làm cho SMDS bị ATM và Frame Relay che khuất như là được nhìn nhận là một dịch vụ đắt tiền, mặc đù có khả năng truyền được hình ảnh nhưng SMDS không hỗ trợ tính năng này...

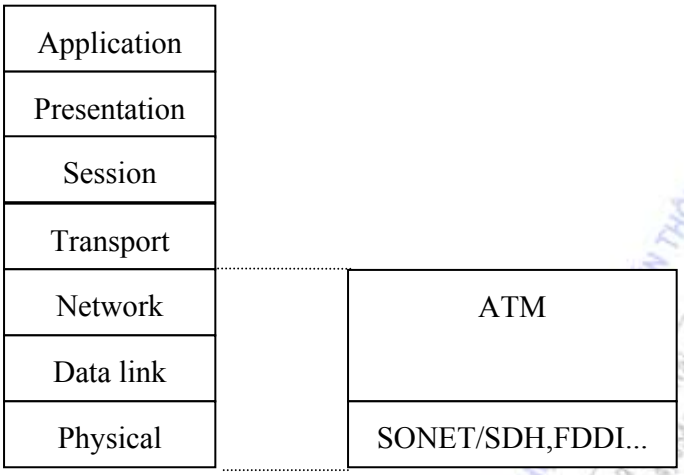
## 5.7. Phương thức truyền dẫn không đồng bộ ATM (Asynchronous Transfer Mode)

### 5.7.1. Giới thiệu chung

Công nghệ truyền dẫn không đồng bộ ATM (Asynchronous Transfer Mode) ra đời như là một nền tảng cho mạng tổ hợp đa dịch vụ số băng rộng B-ISDN. ATM cho phép truyền thông đa phương tiện, đáp ứng đầy đủ các loại hình dịch vụ và có khả năng cung cấp chất lượng dịch vụ theo yêu cầu. ATM có một số đặc trưng khác với các công nghệ chuyển mạch khác. Đơn vị dữ liệu dùng trong ATM gọi là tế bàol (Cel), có độ dài 53 byte (5 byte Header và 48 byte dữ liệu). Trong các công nghệ khác độ dài của khung dữ liệu thay đổi (từ 64 đến 1500 Byte). Những Cell này là đơn vị cơ sở cho truyền dữ liệu. Lưu lượng dữ liệu từ nhiều kênh được ghép với nhau tại mức Cell. Kích thước Cell cố định, nên các cơ chế chuyển mạch hoạt động truyền thông của mạng ATM hiệu quả cao, tốc độ cao. Một số mạng ATM có thể hoạt động tới tốc độ 622 Mbps, tốc độ chung 155 Mbps.

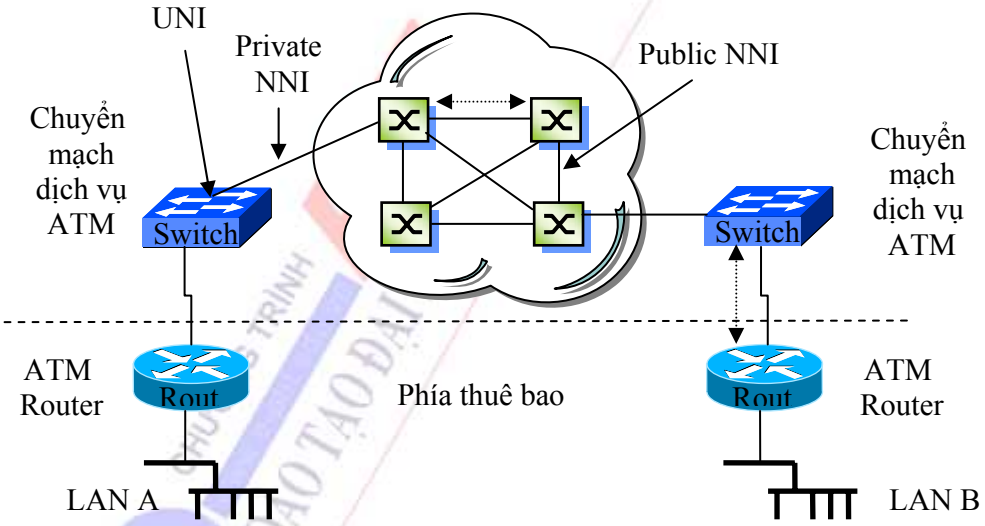
ATM hoạt động ở tầng 2 và 3 trong 3 tầng cuối của OSI. Tầng vật lý có các giao thức hỗ trợ như SONET, FDDI,... ATM hoạt động không phụ thuộc vào đường truyền vật lý. ATM được chia làm hai Channel có chứa các ô (Cell) hoạt động như tốc độ truyền bit cố định khi dữ liệu được truyền giữa các mạch (Circuit) có kích thước khác nhau.

Các thiết bị mạng ATM liên kết với nhau bằng các đường dẫn ảo VPI (Virtual Path Identifier). Trong mỗi đường ảo, có nhiều kênh ảo VCI (Virtual Circuit Identifier). Mặc dù ATM được phát triển như là công nghệ của mạng WAN nhưng ATM có nhiều chức năng hỗ trợ cho các mạng LAN hiệu năng cao. Đó là ATM cho phép sử dụng cùng một công nghệ cho cả mạng LAN và WAN.




**Hình 5.12 Mối quan hệ ATM vơí mô hình OSI**

Về cơ bản, mạng ATM giống như mạng Frame Relay, các tế bào được truyền từ nguồn tới đích qua các mạng con chuyển mạch ATM. Node mạng giao tiếp với thiết bị đầu cuối qua giao diện người sử dụng - mạng UNI (User Network Interface) và thiết bị chuyển mạch ATM giao tiếp với những thiết bị khác qua giao diện mạng-mạng NNI (Network Network Interface). Một mạng ATM đơn giản điển hình như sau:



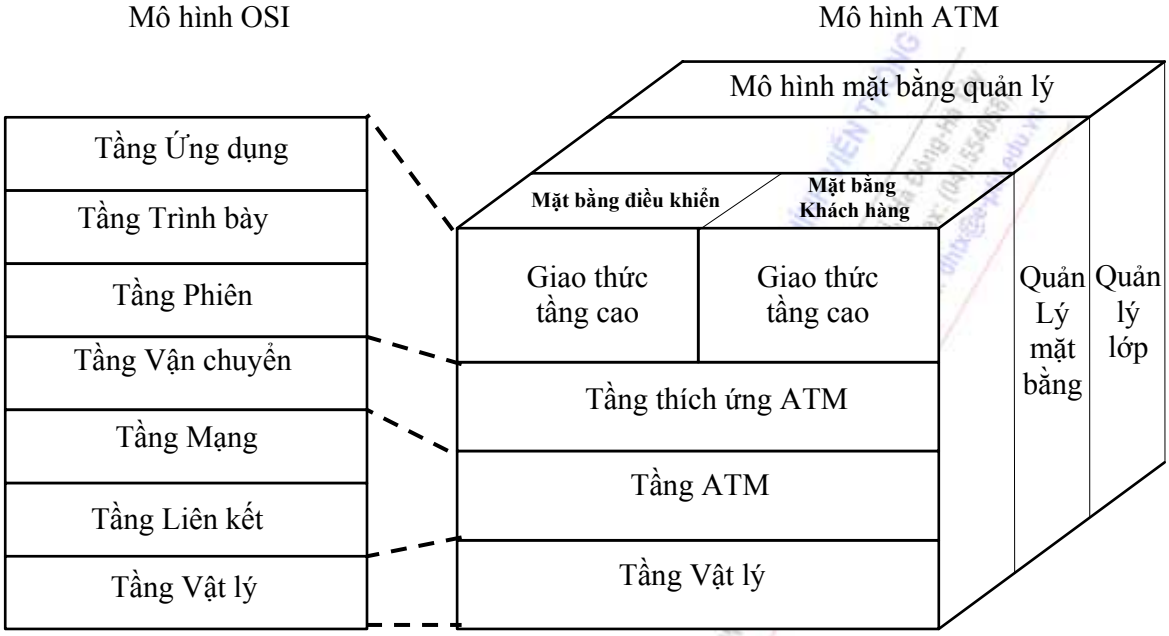

**Hình 5.13 Mối quan hệ ATM với mô hình OSI**

### 5.7.2. Kiến trúc phân tầng ATM

Kiến trúc ATM không có sự tương ứng hoàn toàn với các tầng của mô hình OSI. Mô hình kiến trúc ATM bao gồm các mặt bằng quản lý, mặt bằng điều khiển (kiểm tra) và mặt bằng người sử dụng. Mặt bằng quản lý gồm có quản lý mặt bằng và quản lý tầng.

**a. Các mặt bằng quản lý**

- Mặt bằng điều khiển: Cung cấp các chức năng thiết lập, giám sát và giải phóng liên kết. Mặt bằng này có nhiệm vụ khởi tạo và quản lý các yêu cầu báo hiệu.




**Hình 5.14 Kiến trúc phân tầng mô hình ATM**

- Mặt bằng khách hàng: Cung cấp chức năng điều khiển vận chuyển các luồng thông tin, điều khiển luồng và quản lý các luồng dữ liệu , sữa lỗi.

- Mặt bằng quản lý: Cung cấp chức năng giám sát mạng liên quan đến dữ liệu và thông tin điều khiển. Gồm các chức năng quản lý lớp và quản lý mặt bằng.

- Quản lý lớp: Thực hiện việc điều hành các tham số người sử dụng, các thông tin quản lý khai thác và bảo dưỡng.

- Quản lý mặt bằng: Điều khiển hệ thống bằng cách can thiệp vào giữa các mặt bằng.

**b. Vai trò và chức nằn các tầng ATM**

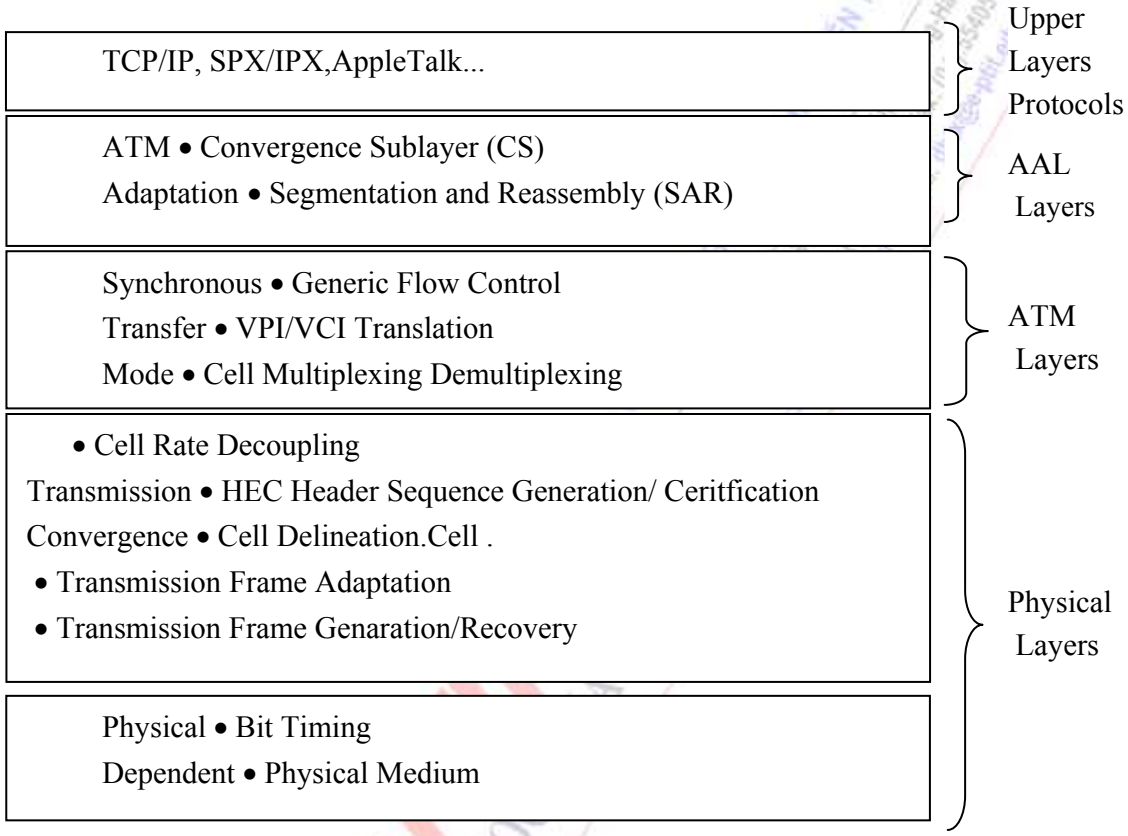
Ngoài ra giao thức của mặt bằng điều khiển và mặt bằng khách hàng được phân loại tiếp thành tầng giao thức mức cao, tầng thích ứng, tầng ATM và tầng vật lý như sau:

- *Tầng vật lý:* Tương tự như lớp vật lý của OSI, ATM quản lý môi trường truyền dẫn, bao gồm 02 tầng con: Tầng con môi trường vật lý PMD (Physical Medium-Dependent) và tầng con kết hợp truyền dẫn TC (Transmission Convergence).

- *Tầng ATM:* Tầng ATM kết hợp với tầng thích ứng ATM có chức năng tương tự như tầng liên kết dữ liệu trong mô hình tham chiếu OSI. Hỗ trợ cho việc tách/ghép tế bào, dịch VPI và VCI, phát sinh tế bào mào đầu, điều khiển luồng chung.

- *Lớp thích ứng ATM - AAL (ATM Adaption Layer):* Có nhiệm vụ giao tiếp với lớp bậc cao. Cung cấp các phương tiện hội tụ cho phép các dạng truyền thông khác nhau có thể tương thích với

các dịch vụ ATM. Lớp AAL chuẩn bị dữ liệu của người sử dụng và phân đoạn dữ liệu thành 48 byte trong tế bào ATM. Tầng AAL chia thành hai tầng con: Tầng con hội tụ CS (Convergence Sublayer) và tầng con phân chia và kết hợp SAR (Segmentation and Reassembly Sublayer), thực hiện việc cắt các đơn vị dữ liệu của người sử dụng thành các Cell ATM 48-byte để truyền và hợp các Cell ATM thành đơn vị dữ liệu của người sử dụng khi nhận.




**Hình 5.15 Các tầng trong ATM**

- *Giao thức các tầng trên (Upper Layers Protocols*) : Nằm trên lớp AAL, nó tập hợp các dữ liệu khách hàng được chấp nhận, sau đó tiến hành sắp xếp vào trong các gói, và liên kết với lớp AAL.

| Tầng | Phân tầng | Các chức năng |
|---|---|---|
| Tầng bậc cao | | Chức năng của tầng bậc cao |
| Tầng ATM thích ưng | Tầng con hội tụ | Chức năng kết hợp |
| | Chia và tập hợp lớp | Chức năng phân chia và kết hợp lại |
| Tầng ATM | | Điều khiển lưu lượng chung<br>Tạo và tách thông tin ghép đầu<br>Dịch các tế bào VPI/VCI<br>Ghép và tách tế bào |
| Tầng vật lý | Truyền dẫn hội tụ tầng con | Phân chia tốc độ tế bào<br>Tạo và xác định tín hiệu HEC<br>Nhận dạng biên của tế báo<br>Tạo và xác định khung truyền dẫn |
| | Môi trường vật lý | Chức năng thông tin thời gian bít<br>Chức năng tương ứng môi trường vật lý |

**Hình 5.16 Vai trò & chức năng các tầng trong ATM**

### 5.7.3. Liên kết ảo (Virtual Connections)

Liên kết ATM gồm hai loại liên kết ảo:

- Liên kết kênh ảo VCC (Virtual Channel Connection): Một kênh ảo cung cấp một liên kết logic giữa các thiết bị đầu cuối ATM. Kênh ảo có thể là kênh ảo cố định PVC (Permanent VC) hoặc kênh ảo chuyển mạch SVC (Switch VC).

- Liên kết đường dẫn ảo VPC (Virtual Path Connection): Một liên kết đường dẫn ảo cung cấp một tập hợp logic các kênh ảo mà có cùng điểm cuối.

Kênh ảo và đường dẫn ảo có thể nhận diện qua các trường VCI và VPI trong Header của ATM Cell. Trong một đường dẫn ảo có thể có nhiều kênh ảo và kênh ảo trong các đường dẫn ảo khác nhau có thể có cùng một VCI. Do đó một kênh ảo hoàn toàn có thể xác định bởi sự kết hợp giữa VPI và VCI.

Trong kỹ thuật ATM, các tế bào chứa các loại dữ liệu khác nhau được dồn kênh trên một đường dẫn ảo VPI, thường một đường trung kế tốc độ cao hoặc một liên kết sử dụng thiết bị ATM. Trong một đường dẫn ảo có thể có một số kênh ảo VCI (Virtual Channel Identiier) riêng biệt. Trong cấu trúc khung của một tế bào ATM, trường VPI là 1 byte, tiếp theo trường VCI 2 byte. Thiết bị chuyển mạch ATM có thể định tuyến ATM trên cơ sở byte đầu tiên. Khi Cell đến đích, VCI được dùng xác định sâu hơn vị trí chính xác để truyền Cell. Như vậy cặp VPI và VCI tạo một trường 3 byte, cho phép sử dụng tối đa 16 triệu kênh ảo trên một giao diện đơn.

VPI/VCI phải qua quá trình ánh xạ dựa trên bảng lộ trình lưu trữ tại các tổng đài chuyển mạch ATM. Khi một kênh ảo được thiết lập, bảng chọn đường tại các node chuyển mạch ATM

tìm kiếm và cung cấp địa chỉ đích của các Cell đến dựa trên địa chỉ Header của Cell. Bảng chọn đường thường xuyên được cập nhật các địa chỉ mới VPI/VCI khi được các bộ chuyển mạch ATM chấp nhận. Trong giai đạon thiết lập cuộc gọi, các Cell được truyền từ node này sang node khác, đường dẫn gọi là Virtual.


**Hình 5.17 Khái niệm kênh ảo và đường dẫn ảo**

Công nghệ truyền dẫn không đồng bộ ATM (Asynchronous Transfer Mode) ra đời như là một nền tảng cho mạng tổ hợp đa dịch vụ số băng rộng B-ISDN. ATM cho phép truyền

### 5.7.4. So sánh ATM với các dịch vụ và kỹ thuật khác

ATM so sánh với Frame Relay:

- ATM và Frame Relay là hai công nghệ chuyển mạch tốc độ nhanh . Có thể nói ATM tương tự với Frame Relay. Tuy nhiên, khung dữ liệu (Frame) trong Frame Relay có kích thước thay đổi, thì ATM sử dụng các gói tin cố định 53 bytes (được gọi là tế bào – Cell).

- Frame Relay cho phép vượt ngưỡng 64 Kb/s của X25, nhưng thông lượng tối đa chỉ đạt tới 2 Mb/s, trong khi thông lượng ATM có thể đạt 155 Mb/s hoặc 622 Mb/s.

- ATM có thể chèn các tế bào có độ trễ truyền dẫn nhạy cảm, điều này không thể được với Frame Relay, bởi vì Frame Relay có khung dữ liệu dài hơn, độ trễ lớn hơn và không thể dự đoán được độ trễ khi xử lý truyền thông tiếng nói và hình ảnh. Vì vậy Frame Relay không phù hợp cho các dịch vụ yêu cầu thời gian thực cao.

- Mặc dầu chưa đáp ứng được yêu cầu của truyền thông đa phương tiện, Frame Relay vẫn là một giải pháp quá độ được lựa chọn trong khi chờ đợi kỹ thuật ATM đưa vào ứng dụng rộng rãi.

ATM và SONET

- SONET đơn giản là một kỹ thuật truyền dẫn, có thể hỗ trợ cho nhiều loại topo thay đổi, bao gồm : điểm-điểm, hình sao, hình vòng.

- Khi phát triển ATM, thay vì phát triển một lớp vật lý mới, những nhà thiết kế của ATM đã sử dụng kỹ thuật liên kết dữ liệu của SONET và sử dụng nó cho chuyển mạch ATM. Hơn nữa, ATM Forum xác định tốc độ 622-Mbps ATM để chạy trên SONET. Tóm lại SONET là một dịch vụ vận chuyển bit từ nguồn tới đích và ATM là một kỹ thuật sử dụng SONET như là một dịch vụ vận chuyển của nó.

So Sánh ATM và Ethernet Gigabit

- Tốc độFast Ethernet và Ethernet Gigabit nhanh hơn tốc độ của ATM và ỗây dựng ATM khá đắt. Tuy nhiên ATM Forum đang phát triển ATM 2,5 Gbps cho LAN.

- Ethernet Gigabit có khả năng truyền dữ liệu và tiếng nói ở mức chấp nhận được, tuy nhiên nó vẫn chỉ là một kỹ thuật VBR (tốc độ bit thay đổi) và gặp phải khó khăn khi mạng tắc nghẽn hoặc đòi hỏi truyền hình độ phân giải cao (HDTV).

- Giao thức giữ trước nguồn tài nguyên RSVP (Resource Reservation Protocol) và giao thức truyền dẫn thời gian thực RTP (Realtime Transport Protocol) là phương thức lỗi chất lượng dịch vụ của Ethernet Gigabit. Cả hai giao thức cho phép các ứng dụng bảo tồn tổng số riêng biệt của giải thông truyền dữ liệu. So sánh Ethernet Gigabit với ATM:

Khung Ethernet 802.3 có sự phân chia tốc độ không phù hợp, vì chiều dài thay đổi từ 64 đến 1518 bytes. Trong khi tế bào ATM phân chia tốc độ ổn định và đảm bảo sự phân chia có thứ tự trong khung thời gian riêng biệt mà bit dữ liệu đến theo thứ tự đúng thời gian.

Trong Ethernet 802.3, khung được xếp hàng tại một node chuyển mạch trên cơ sở vào trước-ra trước (FI-FO). Hơn nữa trước khi chuyển mạch để truyền hàng khung 'n' thì toàn bộ dữ liệu chứa trong hàng khung 'n-1' phải được truyền. Theo đó một chuyển mạch phát hàng khung liên tục theo thứ tự chúng được đệm. Sự xử lý này ở trong ATM thì khác hẳn, tại node chuyển mạch ATM , hàng đợi khung không theo thứ tự chúng được đệm, mà chuyển mạch ATM dựa vào sự ưu tiên để truyền dẫn: khung có độ ưu tiên cao hơn sẽ được truyền dẫn trước và ngược lại. Do đó ATM có thể tạo ra đồng thời nhiều hàng dịch vụ độc lập nhau với sự ưu tiên truyền dẫn khác nhau dựa trên loại dịch vụ mà vẫn cung cấp một tốc độ phân chia không đổi. Đây chính là thế mạnh và sự "thông minh" của ATM. Do vậy mạng nhanh không phải là giải pháp cho nhiều vấn đề hội tụ.

Công nghệ ATM xuất hiện với mạng diện rộng, đa dịch vụ băng rộng. Phương thức truyền tải như là một "Mạng trong mạng", không đồng bộ, tích hợp chuyển mạch gói và chuyển mạch kênh. Thông tin được đặt trong các gói có độ dài cố định. ATM sử dụng kênh ảo và nhóm kênh ảo tạo thành một đường dẫn ảo Thích hợp với dịch vụ yêu cầu truyền thời gian thực, đa phương tiện.

## Câu hỏi trắc nghiệm:

1. Hãy chọn câu đúng nhất về phương pháp kết nối liên mạng:
    A. Phương pháp kết nối tại tầng vật lý, bộ lặp Repeater.
    B. Phương pháp kết nối tại tầng liên kết dữ liệu, thiết bị sử dụng cầu (Bridge) và các bộ chuyển mạch (Switched)
    C. Phương pháp kết nối tầng mạng. Thiết bị sử dụng bộ định tuyến (Router).
    D. Kết nối liên mạng sử dụng các thiết bị như Modem, cáp Modem, Router..
2. Mạng ISDN có những đặc điểm sau:
    A. Là một mạng đa dịch vụ.
    B. ISDN có hệ thống báo hiệu số 7 và các node chuyển mạch thông minh.
    C. Kiến trúc ISDN tương thích với mô hình OSI.
    D. Tất cả khẳng định trên.
3. Các phần tử cơ bản của mạng ISDN
    A. TE1 là các thiết bị đầu cuối có các thuộc tính ISDN.

B. TE2 là các thiết bị đầu cuối không có tính năng ISDN.

C. NT1 (Network Termination 1) thực hiện các chức năng thuộc tầng vật lý .

D. NT2 (Network Termination 2) là một thiết bị thông minh, thực hện các chức năng đến tầng mạng.

E. Tất cả đều đúng.

4. Các loại kênh trong mạng ISDN

A. Kênh D: Dùng để truyền báo hiệu giữa người sử dụng và mạng.

B. Kênh B: Dùng để truyền dữ liệu

C. Kênh H cung cấp các dịch vụ tốc độ cao và ghép các luồng thông tin ở tốc độ thấp hơn. có 4 loại kênh H.

D. Các loại đường ảo và kênh ảo

5. Giao diện ISDN

A. Giao diện BRI (Basic Rate Interface)

B. Giao diện PRI (Primary Rate Interface)

C. Giao diện giữa các tầng, cung cấp các điểm truy nhập dịch vụ.

6. Hoạt động trong tầng Datalink của ISDN:

D. Giao thức LAP-D

A. Giao thức HDLC

B. Giao thức LAP-B và LAP – F

C. Giao thức LAP-D và LAP – F

7. Đặc tính kỹ thuật mạng của X25

A. X25 định nghĩa chuẩn giao diện giữa DTE và DCE

B. Cung cấp các lựa chọn cho chuyển mạch ảo hoặc cố định. X.25

C. Cung cấp các dịch vụ cóp độ tin cậy cao từ node tới node (End to End).

D. Tốc độ tối đa 64 Kbps.

E. Tất cả đều đúng

8. Trên cáp sợi quang, các tốc độ điển hình của B-ISDN là:

A. 51 Mbps(*)

B. 155 Mbps(*)

C. 312 Mbps

D. 622 Mbps(*)

9. Mạng X25 không hấp dẫn, vì:

A. Tốc độ thấp, không thích hợp các dịch vụ yêu cầu tốc độ cao. Các dịch vụ LAN trong môi trường WAN.

B. Không phù hợp trong môi trường truyền dẫn quang.

C. Tất cả khẳng định trên đều đúng.

10. Hoạt động trong tầng Datalink của X25, có:
    A. Giao thức LAP-B
    B. Giao thức HDLC
    C. Giao thức LAP-B và LAP – F
    D. Giao thức LAP-D và LAP – F
11. Đặc trưng cơ bản của Frame Relay:
    A. Không cần duy trì bảng trạng thái, không xử lý các gói tin điều khiển.
    B. Loại bỏ các quá trình trình xử lý ở tầng mạng.
    C. Không điều khiển lưu lượng và điều khiển lỗi theo từng đoạn mạng (Hop-by-Hop Control).
    D. Khung dữ liệu (Frame) có kích thước thay đổi,
    E. Các trường hợp trên đều đúng.
12. Hoạt động trong tầng Datalink Frame Relay, có:
    A. Giao thức LAP- F
    B. Giao thức HDLC
    C. Giao thức LAP-B và LAP – F
    D. Giao thức LAP-D và LAP – F.
13. Đặc trưng cơ bản SMDS:
    A. SMDS là một dich vụ, không phải một công nghệ.
    B. SMDS dịch vụ chuyển mạch gói không liên kết
    C. SDMS hỗ trợ tính bảo mật, cho phép dùng các mạng công cộng, chia sẻ một mạng riêng như mạng xương sống.
    D. Tất cả phát biểu trên đều đúng.
14. Những khẳng định nào sau đây là đúng:
    A. Công nghệ ATM gần giống với công nghệ Frame Relay.
    B. Khung dữ liệu của Frame Relay có kích thước thay đổi, của ATM cố định.
    C. Tốc độ truyền tối đa 2 Mb/s trong Frame Relay, của ATM có thể đạt 155 Mb/s hoặc 622 Mb/s.
15. Những thực thể nào dưới đây là giao thức của WAN
    A. Frame Relay (*).
    B. SLIP
    C. IEEE 802.6
    D. X25(*)
16. Các giao thức nào thường được sử dụng với IEEE 802.2
    A. IEEE 802.3
    B. IEEE 802.5

C. IEEE 802.6

D. Tất cả đều đúng

17. Nêu đặc tính chủ yếu để phân biệt một tế bào và một gói tin.
    A. Các tế bào nhỏ hơn một gói tin.
    B. Các tế bào không có địa chỉ vật lý.
    C. Các tế bào có độ dài cố định (*).
    D. Các gói tin không thể truyền.
18. Giao thức nào được sử dụng trên cáp sợi quang.
    A. Frame Relay
    B. FDDI(*)
    C. SONET(*)
    D. X25
19. Các chuẩn nào sử dụng kỹ thuật truy nhập đường truyền bằng thẻ bài:
    A. IEEE 802.4(*)
    B. IEEE 802.6
    C. Frame Relay
    D. FDDI(*)
20. Giao thức nào phù hợp nhất cho việc giao vận dữ liệu quan trọng về mặt thời gian:
    A. X25.
    B. Frame Relay
    C. IEEE 802.5(*)
    D. ATM(*)

## Câu hỏi và bài tập

1. Mạng tích hợp đa dịch vụ số ISDN (Integrated Service Digital Network), Khái niệm. Nguyên lý chung của ISDN.
2. Các dịch vụ ISDN: Dịch vụ tải tin, dịch vụ viễn thông, các dịch vụ bổ sung.
3. Các phần tử cơ bản của mạng ISDN
4. Các loại kênh trong mạng ISDN: Kênh D, Kênh B, Kênh H.
5. Giao diện ISDN:
    - ✓ Giao diện BRI (Basic Rate Interface)
    - ✓ Giao diện PRI (Primary Rate Interface):
6. Địa chỉ của mạng ISDN và cấu trúc địa chỉ trong ISDN:
7. Chức năng các tầng trong kiến trúc ISDN: Tầng vật lý, Tầng 2 và tầng 3.
8. Mạng băng rộng B_ISDN ( Broadband ISDN)

9. Đặc điểm của dịch vụ B-ISDN
10. Nền tảng kỹ thuật của B-ISDN
11. Cấu trúc chức năng của B_ISDN
12. So sánh ISDN và B_ISDN
13. Mạng chuyển mạch gói X25
14. Giao thức X.25: Tầng vật lý, Tầng liên kết dữ liệu, Tầng mạng
15. Hoạt động của giao thức X25
16. Mạng chuyển mach khung Frame Relay
17. Cấu hình tổng quát mạng Frame Relay
18. So sánh Frame Relay với X25:
    - ✓ Tầng vật lý (Physical Layer),
    - ✓ Tầng liên kết (Link Access Layer),
    - ✓ Tầng mạng (Packet Layer)
19. Frame Relay được thiết kế loại bỏ những hạn chế trong các mạng X.25, vì sao?.
20. Vì sao thời gian xử lý tại các node trong Frame Relay ít hơn nhiều so với X.25 ?.
21. Frame Relay và mô hình OSI: Tầng vật lý, Tầng liên kết và Tầng mạng .
22. Trình bày giao thức LAP-F, LAP-D.
23. Điều khiển quản lý lưu lượng
24. Khái niệm CIR.
25. Các dịch vụ Frame Relay
26. SDMS (Switched Multimegabit Data Service )
27. SMDS so với các công nghệ ATM và Frame Relay.
28. Phương thức truyền dẫn không đồng bộ ATM (Asynchronous Transfer Mode)
29. Kiến trúc phân tầng ATM:
    - ✓ Các mặt bằng quản lý
    - ✓ Vai trò và chức nằn các tầng.
30. Khuôn dạng Cell ATM
31. UNI-Format Header : Khuôn dạng giao diện người sử dụng và mạng
32. NNI-Format Header: Khuôn dạng giao diện mạng và mạng.
33. Các loại tế bào
34. Liên kết ảo (Virtual Connections)
35. So sánh ATM với các dịch vụ và kỹ thuật khác
36. ATM so sánh với Frame Relay:
37. ATM và SONET
38. So Sánh ATM và Ethernet Gigabit

# CHƯƠNG 6: MẠNG TỐC ĐỘ CAO VÀ ỨNG DỤNG CÁC CÔNG NGHỆ MỚI

Nội dung của chương sẽ trình bày một cách tổng quát về các loại mạng tốc độ cao và các ứng dụng công nghệ mới bao gồm đường dây thuê bao số DSL, các mạng truyền tải voice chuyển mạch gói trên nền IP như Voice over Internet Protocol, Voice over ATM và Voice over Frame Relay. Công nghệ MPLS phù hợp với xu thế và nhu cầu truyền thông hiện tại và tương lai. MPLS được ứng dụng trong mạng lõi NGN và nền tảng cho dịch vụ VPN. Mạng thế hệ sau NGN (Next Generation Network) là một trong những mạng hội tụ tiên tiến đang phát triển và thay thế dần các mạng truyền thống. Hoạt động dựa trên các công nghệ chuyển mạch mềm Softswitch, điều khiển chuyển mạch không phụ thuộc vào phần cứng . Có khả năng lập trình độc lập và kiến tạo dịch vụ mềm dẻo. Nội dung của chương gồm:

- Đường dây thuê bao số DSL
- Truyền thoại qua mạng chuyển mạch gói VoPN
- Công nghệ chuyển mạch đa giao thức MPLS.
- Công nghệ chuyển mạch mềm Softwitch
- Mạng hội tu và mạng thế hệ sau NGN.

## 6.1. Đường dây thuê bao số DSL (Digital Subscribers Line)

### 6.1.1. *Mở đầu*

Công nghệ đường dây thuê bao số DSL cho phép tận dụng miền tần số cao truyền tín hiệu tốc độ cao trên đôi dây cáp đồng thông thường. Modem DSL biến đổi tín hiệu của người sử dụng như tín hiệu điện thoại, tín hiệu truyền hình, dữ liệu... thành các tín hiệu phù hợp với đường truyền DSL, có cấu trúc dữ liệu riêng, mã đường dây riêng và một số tín hiệu điều khiển nhất định của mạng. Đường dây thuê bao số được sử dụng đầu tiên với mạng số tích hợp đa dịch vụ ISDN (Integrated Services Digital Network) truyền số liệu giữa các đầu cuối. Nhiều phiên bản DSL sau này được thiết kế từ thực tế ISDN DSL. Các thế hệ DSL sau được cải thiện rất nhiều về công suất, cách thức hoạt động, khả năng cung cấp dịch vụ… Kỹ thuật DSL cho phép truyền chế độ song công đối xứng và bất đối xứng.

### 6.1.2. Tổng quan về họ công nghệ DSL

*IDSL (ISDN DSL):C*ông nghệ đường dây thuê bao số truy nhập mạng ISDN sử dụng các kênh đối xứng BRI (128 Kb/s hoặc 144 Kb/s) kết hợp thành một kênh truyền dữ liệu giữa bộ định tuyến và máy tính của khách hàng. DSL làm việc với tốc độ 160 Kb/s tương ứng với 2B+D (144 Kb/s). Để truyền dẫn song công, sử dụng kỹ thuật triệt tiếng vọng. Phần lớn các dạng IDSL làm việc với ISDN NT tiêu chuẩn ở đầu cuối khách hàng của đường dây. Do đó, IDSL chuyển mạch nội hạt ISDN được thay thế bởi bộ định tuyến gói. Cấu hình này được sử dụng cho truy nhập Internet.

*HDSL (High Data Rate DSL):* Có khả năng truyền tải hai hướng 1,544 Mbps hoặc 2,048 Mbps trên đường dây điện thoại. HDSL truyền dẫn tin cậy tỷ lệ lỗi bit từ $10^{-9}$ đến $10^{-10}$. Hệ thống HDSL DS-1 (1,544 Mbps) sử dụng hai đôi dây, mỗi đôi dây truyền 768 Kb/s trên mỗi hướng. HDSL E1 (2,048 Mbps) có thể lựa chọn sử dụng hai hoặc 3 đôi dây, mỗi đôi dây sử dụng hoàn toàn song công. HDSL 2,048 Mbps 3 đôi dây sử dụng bộ thu phát giống bộ thu phát hệ thống 1,544 Mbps. Mạch vòng HDSL 2,048 Mbps có thể có mạch rẽ nhưng không cân bằng. Tiêu chuẩn HDSL2 có tốc độ bit và độ dài mạch vòng như HDSL thế hệ thứ nhất chỉ khác là sử dụng 1 đôi dây thay vì 2 đôi dây. HDSL2 có kỹ thuật mã hoá cao và điều chế phức tạp hơn. Lựa chọn tần số phát và thu cho HDSL2 để chống xuyên âm. *SDSL (Single Pair DSL)*: Truyền đối xứng tốc độ 784 Kb/s trên một đôi dây, ghép kênh thoại và số liệu trên cùng một đường dây, sử dụng mã 2B1Q. Công nghệ này chưa có các tiêu chuẩn thống nhất nên không được phổ biến cho các dịch vụ tốc độ cao. SDSL mới chỉ ứng dụng truy cập trang Web, tải dữ liệu và thoại với tốc độ 128 Kb/s, khoảng cách nhỏ hơn 6,7 Km và tốc độ tối đa là 1024 Kb/s trong khoảng 3,5 Km.

*VDSL (Very High Data Rate DSL):* Sử dụng mạch vòng từ tổng đài trung tâm đến khách hàng và các bộ ghép kênh phân phối. Tiêu chuẩn kỹ thuật VDSL được phát triển từ nhóm T1E1.4 mô tả các tốc độ và khoảng cách từ đơn vị mạng quang ONU tới thuê bao. Cáp từ mạng cho tới các ONU có thể được nối trực tiếp đến ONU, theo hình tròn hoặc là bộ tách quang thụ động. Tính năng và ứng dụng của VDSLlà hỗ trợ đồng thời tất cả những ứng dụng thoại, dữ liệu và video. Đặc biệt VDSL hỗ trợ truyền hình có độ phân giải cao (HDTV) và các ứng dụng máy tính tiên tiến. Tính đối xứng của VDSL cung cấp tốc độ dữ liệu 2 chiều lên tới 26 Mbps cho các khu vực không có cáp quang nối tới.

| Công nghệ | Tốc độ | Khoảng cách Truyền dẫn | Số đôi dây đồng sử dụng |
|---|---|---|---|
| IDSL | 144 Kb/s đối xứng | 5km | 1 đôi |
| HDSL | 1,544Mb/s đối xứng<br>2,048Mb/s đối xứng | 3,6 km – 4,5 km | 2 đôi<br>3 đôi |
| HDSL2 | 1,544Mb/s đối xứng<br>2,048 Mb/s đối xứng | 3,6 km – 4,5 km | 1 đôi |
| SDSL | 768kb/s đối xứng<br>1,544Mb/s hoặc 2,048 Mb/s một chiều | 7 km<br>3 km | 1 đôi |
| ADSL | 1,5- 8 Mb/s đường xuống<br>1,544 Mb/s đường lên | ≤ 5km | 1 đôi |
| VDSL | 26 Mb/s đối xứng<br>13–52 Mb/s đường xuống<br>1,5-2,3 Mb/s đường lên | 300 m – 1,5 km<br>(tuỳ tốc độ) | 1 đôi |

**Hình 6.1: So sánh một số tính năng trong họ công nghệ xDSL**

*ADSL (Asymmetric Digital Subscriber Line):* ADSL là công nghệ đường dây thuê bao số bất đối xứng được phát triển cho nhu cầu truy nhập Internet tốc độ cao, các dịch vụ trực tuyến, video,... ADSL cung cấp tốc độ truyền tới 8 Mb/s đường xuống (Download) và 16 - 640 Kb/s đường lên (Upload). Ưu điểm nổi bật của ADSL là cho phép người sử dụng sử dụng đồng thời một đường dây thoại cho cả 2 dịch vụ thoại và số liệu, vì ADSL truyền ở miền tần số cao (4400 Hz÷1,1MHz) không ảnh hưởng tới tín hiệu thoại. Các bộ lọc được đặt ở hai đầu mạch vòng tách tín hiệu thoại và số liệu theo mỗi hướng. ADSL "Lite" hay ADSL không sử dụng bộ lọc chủ yếu cho ứng dụng truy cập Internet tốc độ cao. Kỹ thuật này không đòi hỏi bộ lọc phía thuê bao nên giá thành thiết bị và chi phí lắp đặt giảm đi tuy nhiên tốc độ đường xuống chỉ còn 1,5 Mb/s.

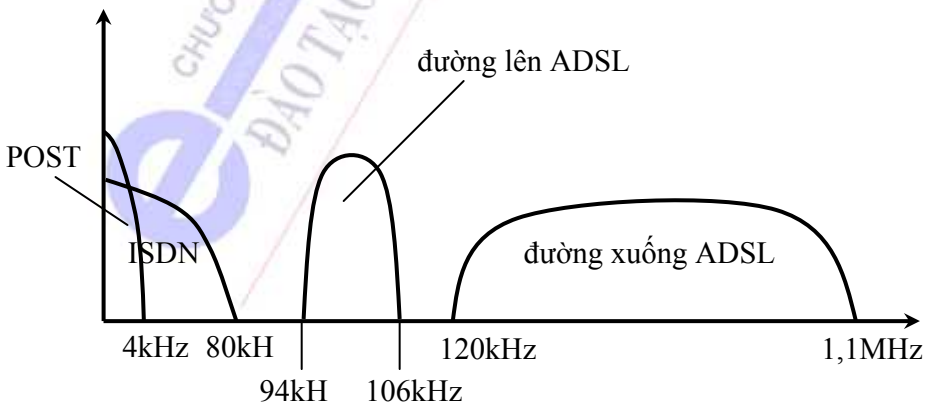
*ADSL2 và ADSL2$^{+}$:* ADSL2 được chuẩn hoá trong ITU G.992.3, G.992.4, ADSL2+ được chuẩn hóa trong ITU-T G.925.5 là thế hệ thứ ba của ADSL, phát triển dựa trên nền tảng ADSL và ADSL2 nên mang đầy đủ đặc trưng của ADSL và ADSL2. ADSL2 và ADSL2+ bổ sung nhiều tính năng mới cho các ứng dụng, dịch vụ và tiến trình triển khai mới so với ADSL chuẩn. Công nghệ ADSL2+ đáp ứng các yêu cầu tốc độ cao, băng thông rộng vì nó hỗ trợ được tốc độ truyền số liệu lên 1,2 Mbps và tốc độ xuống 24 Mbps.

### 6.1.3. Các vấn đề cơ bản công nghệ DSL trên mạng cáp đồng

Phân chia tần số: Phổ tần cáp đồng từ 0 đến 1,1 Mhz được chia thành các khoảng tấn số để sử dụng cho các dịch vụ như sau:

- Từ 0 kHz đến 4 kHz: dùng cho điện thoại và các dịch vụ dữ liệu băng tần thấp.
- Từ 0 kHz đến 80 kHz: khoảng tần số dùng cho ISDN.
- Từ 80 kHz đến 94 kHz: đảm bảo sự an toàn phổ tấn thoại và đường lên của ADSL.
- Từ 94 kHz đến 106 kHz: khoảng tần số dùng cho đường lên của ADSL.
- Từ 106 kHz đến 120 kHz: an toàn phổ tần đường lên và xuống của ADSL.
- Từ 120 kHz đến 1,1 MHz: khoảng tần số dùng cho đường xuống của ADSL.

Việc phân tách phổ tần giữa thoại và ADSL cũng như giữa đường xuống và đường lên của ADSL được thực hiện nhờ bộ lọc Spilitter (bộ lọc này ngăn cản cả dòng DC không cho vào modem ADSL).




**Hình 6.2 : Phân chia tần số**

### 6.1.4. Các phương pháp mã hóa đường truyền

Phương pháp mã hóa đường dây CAP và DMT sử dụng kỹ thuật điều chế biên độ cầu phương (QAM) là kỹ thuật điều chế kết hợp cả điều chế pha và điều chế biên độ. Một ký hiệu được biểu diễn bằng một điểm của chòm sao. Có các kiểu mã hóa QAM: 4-QAM, 16-QAM, 64-QAM... Số 4,16,64… là số trạng thái mã hóa. Số trạng thái càng nhiều trên mỗi ký hiệu QAM thì tín hiệu càng yếu đi, dẫn đến tỷ số tín hiệu trên tạp âm phải cao để Modem thu có thể phân biệt được tín hiệu từ tạp âm. Khi chòm sao QAM trở nên càng ngày càng lớn thì phải tăng công suất hay giảm nhiễu.

ADSL sử dụng mã đường truyền DMT vì nó được định nghĩa trong ANSI T1.413 và G.992.1. Tuy nhiên, CAP vẫn được một số hãng phát triển áp dụng cho ADSL. Việt Nam khuyến nghị sử dụng phương pháp điều chế DMT.

- Phương pháp điều chế biên độ và pha triệt sóng mang CAP dựa trên kỹ thuật điều chế biên độ cầu phương QAM. Ưu điểm của nó là không có kênh con nên thực thi đơn giản hơn DMT. CAP thích ứng được việc tốc độ khi thay đổi kích cỡ chòm sao mã hoá (4-CAP, 64-CAP, 512-CAP, ...) hoặc là khi tăng hoặc giảm phổ tần sử dụng. Nhược điểm của phương pháp này là không có sóng mang nên năng lượng suy giảm nhanh trên đường truyền và tín hiệu thu chỉ biết biên độ mà không biết đến pha, do đó đầu thu phải có bộ thực hiện chức năng quay nhằm xác định chính xác điểm tín hiệu.

- Phương pháp đa âm tần rời rạc DMT hỗ trợ kiến trúc ghép kênh phân chia theo tần số lẫn triệt tiếng vọng. Sử dụng các phổ tần chồng lấn để có được tốc độ dữ liệu cao hơn nhưng phức tạp và chi phí cũng cao hơn vì cần có bộ sai động để triệt tiếng vọng. Kỹ thuật DMT đã lợi dụng kỹ thuật xử lý tín hiệu số, căn cứ đặc tính mạch điện tự thích ứng điều chỉnh những tham số này, làm cho lỗi bit và xuyên âm nhỏ nhất và dung lượng thông tin ở bất cứ mạch nào cũng lớn nhất. Nguyên lý cơ bản của DMT là chia độ rộng băng tần có thể sử dụng (1104 KHz) thành các kênh con (Subcarrier) và căn cứ vào các đặc tính của kênh t, phân phối dữ liệu đầu vào cho mỗi kênh con. Nếu một kênh con không thể chịu tải số liệu sẽ đóng lại. Mỗi kênh con có thể truyền số liệu 1 đến 15 bit thông tin trong một đơn vị mã.

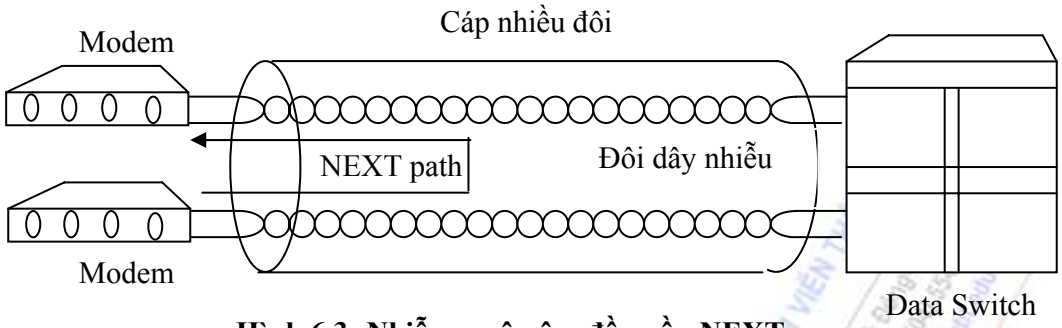
### 6.1.5. Phát hiện lỗi và sửa lỗi

ADSL sử dụng mã Reed Solomon và Trellis luôn làm việc trong chế độ sửa lỗi. ATM (mã HEC) sử dụng phương pháp sửa lỗi và sẽ chuyển sang phương thức phát hiện lỗi khi có lỗi xảy ra. Sự lựa chọn phương thức sửa lỗi hoặc phát hiện lỗi là thống nhất.

Một số cơ chế mã hoá có thể chuyển đổi từ phương thức phát hiện lỗi ngay khi các lỗi được phát hiện. Khối FEC có tác dụng giúp bên thu có thể thu đúng thông tin, thực hiện bằng cách thêm các byte kiểm tra FCS, công suất 3 dB với tỷ lệ lỗi bit là $10^{-7}$.

### 6.1.6. Nhiễu và chống xuyên nhiễu

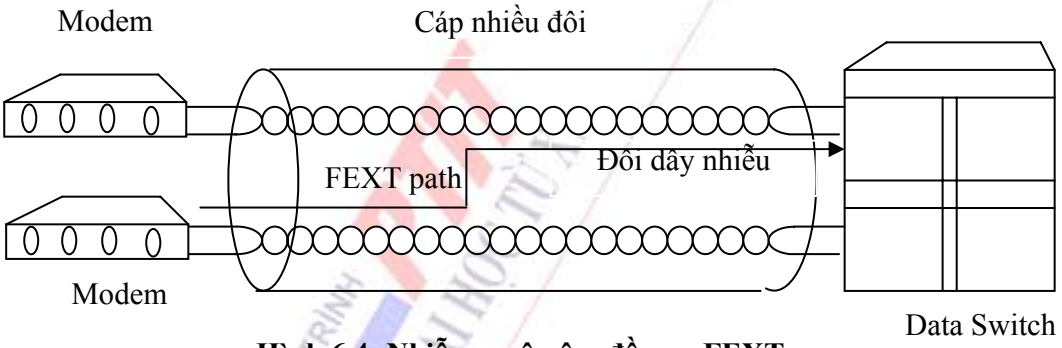
*Nhiễu xuyên âm đầu gần NEXT* (Near - end Crosstalk): Xuất hiện ở các bộ thu do nguồn nhiễu từ các bộ phát cùng đầu cáp với nó gây ra. Loại nhiễu này là đáng kể nhất. Nhiễu NEXT gây suy giảm cho hệ thống sử dụng cùng băng tần số cho truyền dẫn thu và phát.




**Hình 6.3: Nhiễu xuyên âm đầu gần NEXT**

Để tránh xuyên âm đầu gần NEXT, hệ thống truyền dẫn có thể sử dụng các dải tần số cho thu và phát khác nhau. Hệ thống ghép kênh theo tần số FDM loại bỏ được NEXT từ các hệ thống giống nhau. Xem xét một tín hiệu V truyền dọc theo một đôi dây, tại khoảng x1dọc theo đôi dây có nhiễu tác động do không cân bằng và truyền trở lại đầu thu như trong H.6.3

*Nhiễu xuyên âm đầu xa FEXT* (Far - end- Crosstalk): Xuất hiện ở bộ thu đặt ở đầu kia của cáp, khác với đầu phát ra nguồn nhiễu. FEXT thường nhỏ hơn nhiều so với nhiễu xuyên âm đầu gần NEXT vì tín hiệu từ đầu xa bị suy hao khi nó chạy trên mạch vòng thuê bao. FEXT thu được cũng sử dụng phương pháp tương tự như khi sử dụng phương pháp thu NEXT. Hình 6.4 trình bày một ví dụ của FEXT từ một điểm không cân bằng x1.



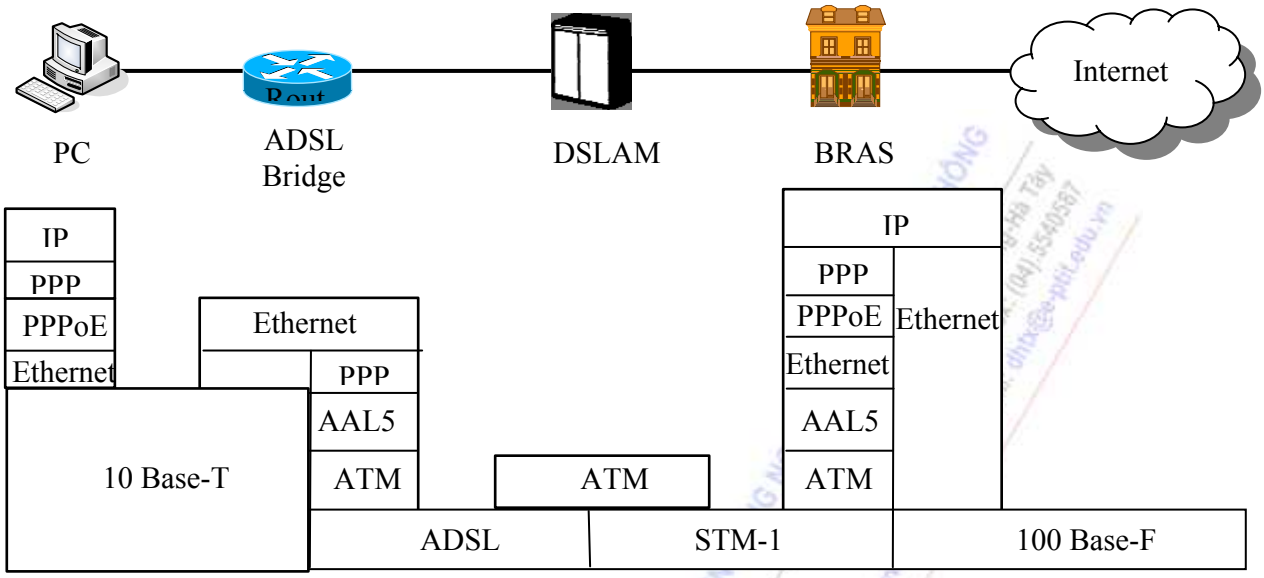

**Hình 6.4: Nhiễu xuyên âm đầu xa FEXT**

Nhiễu xuyên âm đầu gần cũng như đầu xa thì công suất của nhiễu phụ thuộc vào phổ của tín hiệu nhiễu. Thông thường người ta chỉ quan tâm đến công suất nhiễu xuyên âm mà không cần quan tâm đến mức điện áp của nhiễu xuyên âm. Vì theo thống kê thì hầu như đối với các mô hình của công suất nhiễu xuyên âm đã có thể cho phép xác định tỷ số tín hiệu trên tạp âm SNR trên đôi dây, còn đối với mô hình mức điện áp thì rất khó xác định.

*Chống xuyên nhiễu*: Năng lượng điện truyền trên mỗi đôi dây tạo ra một từ trường bao bọc quanh đôi dây gây ra tín hiệu điện, cảm ứng sang các đôi dây xung quanh, gọi là nhiễu xuyên âm. ADSL khắc phục bằng cách giảm tốc độ bit hướng lên, sử dụng dải tần số thấp hơn tần số nơi suy hao truyền dẫn nhỏ và nhiễu xuyên âm nhỏ nhất.

*Phương pháp triệt tiếng vọng* (EC): Tiếng vọng là sự phản xạ của tín hiệu phát vào bộ thu đầu gần. Tiếng vọng đáng ngại là vì các tín hiệu đi theo cả 2 hướng của truyền dẫn số và cùng tồn

*** Mô hình PPPoE (Point to Point over Ethernet) RFC 2516**



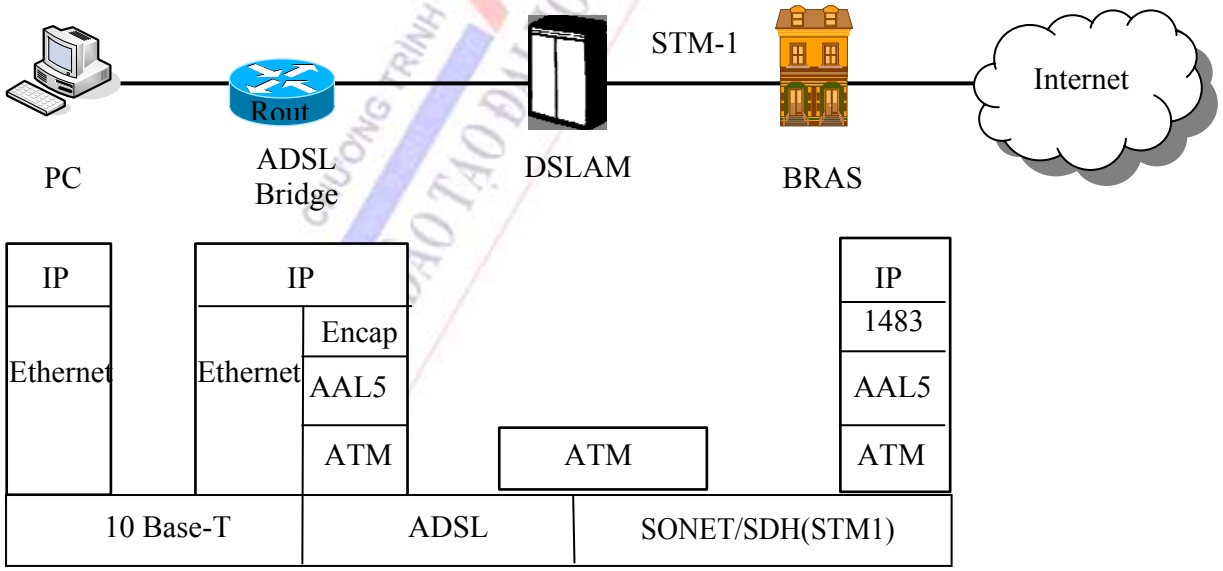

**Hình 6.6 PPPoE - Giao thức nối điểm qua Ethernet**

PPPoE yêu cầu hầu hết các giao thức đóng khung:

- PPP trên PC để bảo an kết nối tử PC đến bộ định tuyến của ISP.
- PPPoE kết nối từ PC đến modem.
- RFC 1483 kết nối từ modem đến bộ định tuyến của ISP.

*** Mô hình IP over ATM (RFC 1483R)**

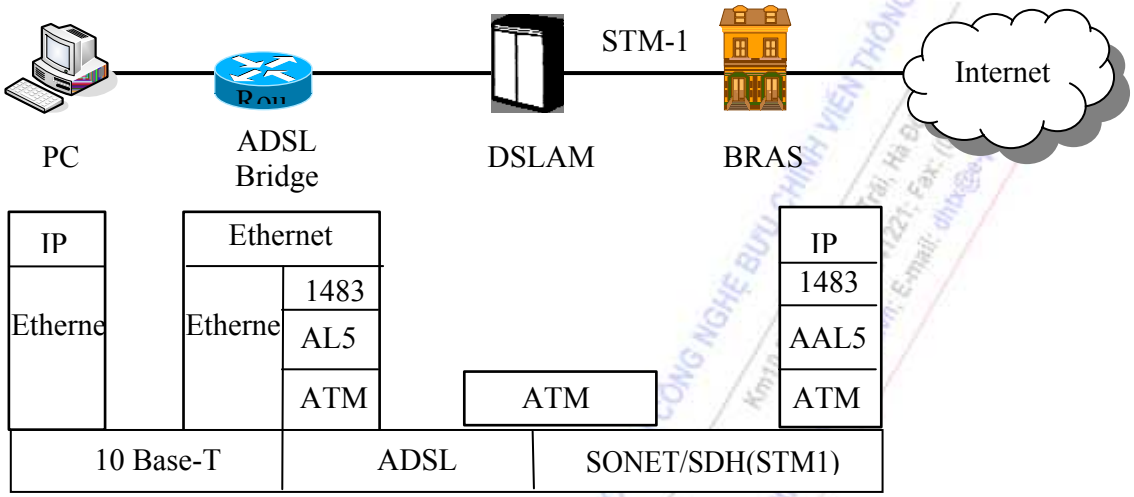
Được xác định trong RFC 1483R. Tiêu chuẩn này hỗ trợ giao thức định hướng (giống IP) và giao thức không định hướng (giống Ethernet). Nó cũng có kết hợp tùy chọn cho VC Multiplexing và LLC Multiplexing.




**Hình 6.7 Mô hình IP over ATM (RFC 1483R)**

*** Mô hình Ethernet over ATM (RFC 1483B)**

Tiêu chuẩn đa giao thức kết hợp mức đáp ứng AAL5. Tiêu chuẩn này hỗ trợ giao thức định hướng (giống IP) và giao thức không định hướng (giống Ethernet). Nó cũng có kết hợp tùy chọn cho VC Multiplexing và LLC Multiplexing.




**Hình 6.8 Mô hình IP over ATM (RFC 1483R)**

RFC 1483 (Bridged) sử dụng trong Modem ADSL ngoài với giao thức tạo khung RFC 1483. Hiện nay được triển khai trong các sản phẩm của SBC và Pac Bell .

### 6.1.8. Các ứng dụng của ADSL

Truy nhập Internet tốc độ cao: Với tốc độ truyền bất đối xứng nên ADSL là công nghệ lý tưởng cho truy nhập Internet tốc độ cao, bởi lẽ nhu cầu tải thông tin từ Internet về lớn hơn rất nhiều so với nhu cầu tải tin đi.

Truyền hình theo yêu cầu (VoD): Truyền hình theo yêu cầu sử dụng các phương pháp nén, số hóa tín hiệu âm thanh, hình ảnh để truyền đi qua mạng. Các nhà cung cấp dịch vụ VoD có thể cung cấp các kênh truyền hình theo yêu cầu với chất lượng khác nhau tùy theo yêu cầu sử dụng. Các kênh truyền hình chuẩn (SDTV) yêu cầu tốc độ truyền là 3-4Mbps. Các kênh truyền hình độ trung thực cao (HDTV) yêu cầu tốc độ truyền là 15-18 Mbps. Như vậy, dịch vụ ADSL với tốc độ hướng xuống tối đa 8 Mbps thì chỉ có thể hỗ trợ tối đa 2 kênh SDTV và không thể hỗ trợ được HDTV, ADSL2+ sẽ hỗ trợ được dịch vụ này.

Hội nghị từ xa: Cho phép nhiều người ở các địa điểm khác nhau có thể hội họp, trao đổi trực tiếp như đang trong cùng một phòng họp. Tăng hiệu quả công việc, tiết kiệm thời gian và chi phí do giảm thiểu việc di chuyển, cũng như công tác tổ chức hội họp.

Truyền hình và phát thanh qua mạng: Các kênh truyền hình và phát thanh từ đài truyền hình và đài phát thanh có thể được truyền hình trực tiếp trên mạng ADSL2+ đến người sử dụng. Vì tín hiệu Video và Audio chỉ chiếm một phần băng thông của đường dây, nên người sử dụng vừa xem video vừa có thể duyệt Web.

Một số các dịch vụ khác: Các dịch vụ có thể triển khai trên công nghệ ADSL như: Truyền số liệu tốc độ cao, học từ xa, game trực tuyến, khám bệnh từ xa, làm việc tại nhà, mua bán hàng qua mạng và các hoạt động giao dịch khác...

Hiện nay, công nghệ đường dây thuê bao số DSL đã được ứng dụng rộng rãI, đáp ứng mọi nhu cầu về các dịch vụ băng rộng trên mạng cáp đồng sẵn có. Với ưu điểm về phương thức truyền cũng như phương pháp mã hoá, sửa lỗi, ADSL rất phù hợp với các dịch vụ Internet tốc độ cao, đưa lại nhiều lợi ích cho người sử dụng cũng như nhà cung cấp dịch vụ.

## 6.2. Truyền thoại qua mạng chuyển mạch gói VoPN (Voice over Packet Network)

### 6.2.1. Khái niệm

Là mô hình truyền thoại thời gian thực không sử dụng hệ thống chuyển mạch kênh thông thường mà sử dụng các mạng chuyển mạch gói. Tín hiệu thoại tương tự sau khi được số hóa sẽ được truyền qua mạng chuyển mạch gói dưới dạng các gói dữ liệu.

VoPN đang trở thành một trong những công nghệ viễn thông hấp dẫn nhất hiện nay không chỉ đối với các nhà cung cấp dịch vụ mà với cả những người sử dụng dịch vụ. Sự phát triển của các mạng chuyển mạch gói và đặc biệt là mạng Internet với giao thức IP đã tạo ra nền tảng phát triển các giao thức cho phép truyền dữ liệu thoại qua các mạng số liệu khác nhau. Các mạng chuyển mạch gói thường được sử dụng để truyền thoại là mạng Frame Relay, mạng ATM và mạng IP.

### 6.2.2. Mô hình truyền thoại qua mạng chuyển mạch gói

Tại phía phát, tín hiệu thoại tương tự từ máy điện thoại hay micro sẽ được số hóa và chuyển đổi thành các gói dữ liệu thích hợp để truyền qua mạng, việc chuyển đổi sẽ được thực hiện thông qua các bộ mã hóa-giải mã CODEC (Coder-Decoder). Bộ xử lý tín hiệu số DSP (Digital Signal Processing) sẽ nén các gói dữ liệu này với tốc độ bit thích hợp để truyền qua mạng chuyển mạch gói.

Tại bên thu, các tiến trình diễn ra ngược lại, khi nhận được các gói tin đã được nén, các DSP sẽ giải nén các gói tin, sau đó giải mã (Decode) các gói tin thành tín hiệu âm thanh tương tự và phát ra điện thoại hoặc loa cho người nghe.

Trong một cuộc đàm thoại, các khoảng lặng chiếm tỉ lệ rất lớn (30% - 40%), khi truyền thoại qua mạng chuyển mạch gói người ta sử dụng kỹ thuật VAD (Voice Activity Detection) để loại bỏ các khoảng lặng nhằm giảm lượng gói tin truyền qua mạng. Tại phía thu các khoảng lặng lại được tái tạo để phát thông tin thoại cho người nghe.

### 6.2.3. Ưu điểm của truyền thoại qua mạng chuyển mạch gói

- Tiết kiệm chi phí đầu tư hạ tầng mạng và chi phí sử dụng dịch vụ: Việc tiết kiệm chi phí hạ tầng mạng ở đây được hiểu theo nghĩa sử dụng các mạng chuyển mạch gói đã có sẵn để truyền dữ liệu thoại. Thực tế việc đầu tư một hệ thống mạng chuyển mạch gói sử dụng các công nghệ tiên tiến như mạng ATM cũng rất tốn kém và thường chỉ sử dụng cho mạng đường trục. Do tận dụng được các mạng chuyển mạch gói có sẵn, đặc biệt là mạng Internet để thực hiện các cuộc gọi đường dài có thể tiết kiệm được rất nhiều chi phí cuộc gọi so với việc thực hiện cuộc gọi thông qua mạng chuyển mạch kênh thông thường.

- Sử dụng hiệu quả băng thông với chất lượng dịch vụ QoS chấp nhận được: Trong mạng chuyển mạch kênh, băng thông cấp cho một cuộc lien lạc là cố định (một kênh 64kbps) nhưng khi truyền thoại qua mạng chuyển mạch gói việc phân chia tài nguyên cho các cuộc gọi linh hoạt hơn nhiều. Khi một cuộc liên lạc diễn ra, nếu lưu lượng của mạng thấp, băng thông dành cho liên lạc sẽ cho chất lượng thoại tốt nhất có thể, nếu lưu lượng của mạng cao, mạng sẽ hạn chế băng thông của từng cuộc gọi ở mức chất lượng thoại QoS chấp nhận được nhằm phục vụ được nhiều người nhất.

- Kết hợp các dịch vụ thoại, số liệu, video trên một mạng duy nhất: cho phép sử dụng hạ tầng mạng gói đa dịch vụ duy nhất để truyền các loại lưu lượng khác nhau.

### 6.2.4. Các vấn đề về chất lượng dịch vụ QoS

Khác với mạng chuyển mạch kênh, trong mạng chuyển mạch gói có rất nhiều các gói tin thuộc các loại dữ liệu khác nhau được lưu chuyển hướng đích trên cùng một kênh truyền. Vì vậy cần phải có cơ chế ưu tiên đối với các dữ liệu thời gian thực như dữ liệu thoại. Ngoài ra mạng chuyển mạch gói sử dụng cơ chế lưu và chuyển tiếp (Store-and-Forward) để truyền thông tin nên gây trễ tại các nút chuyển mạch.

*** Trễ (Delay):** Trễ là một nhân tố ảnh hưởng đến chất lượng thoại. Mỗi hệ thống truyền thông chỉ cho phép một giới hạn trễ nhất định. Thời gian trễ có thể chấp nhận được trong khoảng từ 200ms đến 400ms. Chất lượng cuộc gọi tốt thì thời gian trễ yêu cầu không quá 200ms. Yêu cầu giảm trễ là rất cần thiết trong hệ thống VoPN để có thể nâng cao chất lượng dịch vụ. Nguyên nhân gây trễ khi truyền thoại qua mạng chuyển mạch gói có thể do:

- Trễ tích lũy hay trễ thuật toán: là trễ do chờ đủ khung dữ liệu để xử lý ở các bộ mã hóa.

- Trễ xử lý: thời gian mã hóa và đóng gói dữ liệu đã mã hóa để truyền qua mạng

- Trễ truyền qua mạng: trễ truyền dữ liệu qua mạng chuyển mạch gói hoặc do các bộ đệm chống Jitter ở phía thu.

Để giảm thiểu trễ, phải tăng tốc độ mạng, năng lực của các bộ xử lý, mã hóa, ngoài ra cần sử dụng các bộ triệt tiếng vọng Echo Canceller.

*** Trượt (Jitter):** Trượt là sự chênh lệch thời gian đến của các gói tin theo các đường khác nhau từ nguồn đến đích gây ra. Để có thể tái tạo tiếng nói một cách chính xác và trung thực bên thu cần phải loại bỏ Jitter bằng cách sử dụng bộ đệm (Buffer), các gói sau khi nhận sẽ được lưu trong bộ đệm và sẽ được xử lý lần lượt. Dùng bộ đệm sẽ tránh được những thời gian trễ lớn của các gói tin, nhưng làm tăng thời gian trễ trong hệ thống. Thời gian trượt càng lớn thì dung lượng của bộ đệm càng lớn. Bộ đệm càng lớn thì thời gian trễ gây ra càng tăng. Vì vậy việc tính toán dung lượng của bộ đệm thích hợp đối với từng hệ thống là rất cần thiết sao cho tránh được trượt mà thời gian trễ không làm giảm chất lượng của hệ thống.

*** Mất gói (Packet Loss):** Không thể đảm bảo tất cả các gói tin đều đến đích an toàn và đúng thứ tự, nhất là trong mạng IP. Các gói tin có thể bị mất khi mạng bị quá tải hay trong trường hợp nghẽn mạng hoặc do đường kết nối không đảm bảo. Yêu cầu chất lượng dịch vụ tỉ lệ mất gói là nhỏ hơn 10%. Do hạn chế của thời gian trễ nên các giao thức vận chuyển không liên kết giải quyết vấn đề này. Để duy trì chất lượng thoại ở mức chấp nhận được hoặc truyền lại các gói tin bị mất, hoặc thay thế các gói tin mất bằng các khoảng im lặng. Để nâng cao độ tin cậy của đường truyền cần tăng tốc độ kênh truyền, tăng dung lượng hệ thống thiết bị truyền dẫn (sử dụng các mạng tiên tiến như mạng Frame Relay, ATM).

### 6.2.5. Voice over Frame Relay - VoFR

Các chuẩn VoFR trong Frame Relay Forum FRF, năm 1998: FRF.11 định nghĩa định dạng các khung, FRF.12 định nghĩa quá trình phân mảnh các gói tin (tạo ra các gói tin nhỏ hơn để truyền dữ liệu thoại thời gian thực qua mạng). Các khung dữ liệu trong mạng Frame Relay có kích thước Header nhỏ 2 byte. VoFR thường được sử dụng trong các mạng riêng hoặc mạng riêng ảo VPN kết hợp thoại và số liệu. Việc sử dụng mạng Frame Relay để truyền thoại giúp giảm giá thành. Trong VoFR, các tổng đài PBX được kết nối với nhau thông qua các Permanent Virtual Circuit (PVCs). Trong đó tốc độ kết nối của các kênh trong mạng Frame Relay có thể dễ dàng thay đổi để thích ứng truyền thoại, fax hay số liệu. Khi truyền thoại trong mạng Frame Relay, các gói dữ liệu thoại sẽ được ưu tiên hơn so với các gói dữ liệu khác.

### 6.2.6. Voice over ATM - VoATM

Phương thức truyền không đồng bộ ATM (Asynchronous Transfer Mode) là công nghệ đa dịch vụ, có thể truyền đồng thời thoai, dữ liệu và video với tốc độ và độ tin cậy cao. Giá thành các hệ thống ATM đắt và chỉ được sử dụng ở một số mạng yêu cầu tốc độ, như mạng đường trục Backbone. Các chuẩn VoATM được định nghĩa bởi ATM Forum và ITU_T.

Giao thức dịch vụ tốc độ bit cố định CBR (Constant Bit Rate) của AAL1 là chuẩn truyền thoại qua ATM. Tuy nhiên giao thức này không hiệu quả đối với các ứng dụng thoại. Dịch vụ mô phỏng kênh CES (Circuit Emulation Service) có chất lượng dịch vụ cao nhất, cung cấp truyền một dòng liên tục các bit thông tin, cấp một lượng không đổi băng thông cho một kết nối trong thời gian truyền. Nhưng CES chiếm băng thông cho các ứng dụng khác. Ngoài ra, nhằm giảm trễ, CES gửi các ATM Cell trống không đợi thêm 6 ms để lấp đầy 47 byte dữ liệu thoại vào Cell. Điều này làm lãng phí băng thông khoảng 20 bytes trên một ATM Cell. Dịch vụ mô phỏng kênh băng thông động DBCES là một biến thể của CES, DBCES không gửi một dòng bit cố định các Cell mà chỉ truyền khi có cuộc thoại hoạt động (Off Hook). Cũng như CES, một phần của Cell rỗng. Do đó sử dụng AAL1 để truyền thoại qua ATM tăng phần tiêu đề dữ liệu thoại và lãng phí băng thông.

Dịch vụ tốc độ bit biến đổi VBR của AAL2 trong khuyến nghị I.363.2 của ITU_T, cho phép đóng gói các gói ngắn từ 1Byte đến 45-64 Bytes, gọi là các Minicells, thành một hoặc nhiều ATM Cell. Khác với AAL1, AAL2 cho phép các Cell có Payload khác thay đổi. AAL2 hỗ trợ nén thoại và nén khoảng lặng và cho phép nhiều kênh thoại có băng thông khác nhau trên một kết nối ATM đơn.

Trong mạng thuần ATM, việc nén thoại là không cần thiết, do băng thông rất lớn. Tuy nhiên trong các mạng ATM-Frame Relay, việc nén thoại là cần thiết vì Frame Relay có nén thoại. Khi truyền thoại qua mạng ATM, các Permanent Virtual Circuit được dùng để truyền thoại và báo hiệu. Các bản tin báo hiệu sẽ được truyền một cách trong suốt trên các Signaling PVCs. Việc kết hợp giữa các hệ thống cuối cho phép chọn ra một PVC để truyền thoại giữa các trạm kết cuối. Trong mô hình dịch báo hiệu VoATM, ATM dịch báo hiệu từ cả các thiết bị mạng ATM và Non-ATM

Do giá thành của một mạng ATM rất cao nên thường chỉ được dùng cho mạng Backbone hoặc nhà cung cấp dịch vụ

### 6.2.7. Voice over Internet Protocol - VoIP

VoIP là mô hình truyền thoại sử dụng giao thức IP Internet Protocol. VoIP là một công nghệ hấp dẫn nhất hiện nay. Các chuẩn giao thức của VoIP được đưa ra bởi ITU_T (International

Telecomunication Union), ITMC (International Multimedia Telecommunications Consortium) và IETF (Internet Engineering Task Force).

*** Các thành phần chủ yếu của VoIP gồm có:**

- Internet Protocol IP: Định danh địa chỉ các thiết bị và định tuyến các gói tin lưu chuyển mạng. Các gói IP có phần Header 20 Bytes.

- Các chuẩn nén tín hiệu thoại : Chuyển đổi tín hiệu Analog - Digital và nén tín hiệu.

- Chuẩn H.323 hoặc SIP: Thiết lập cuộc gọi

- Real Time Transport Protocol (RTP): Quản lý các kết nối End to End để giảm thiểu mất gói và trễ.

| | | |
|---|---|---|
| 7 | Application | Các ứng dụng |
| 6 | Presentation | CODECS |
| 5 | Session | H323 hoặc SIP |
| 4 | Transport | UDP, TCP, RTP |
| 3 | Network | IP |
| 2 | Data link | ATM,FR,PPP<br>Ethernet |
| 1 | Physical | |

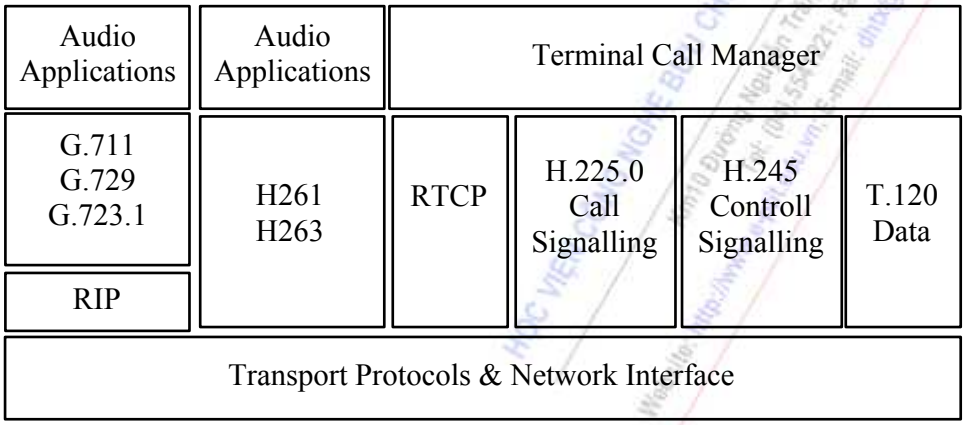
**Hình 6.9 Mô hình Voice over Internet Protocol**

Các phần tử H.323 bao gồm: Các Gateway, các bộ kiểm soát cổng Gatekeeper và các khối điều khiển đa điểm MCU (Multipoint Control Unit). Các thiết bị đầu cuối hỗ trợ cho hội nghị điểm-điểm và hội nghị đa điểm với nhiều thành phần audio, video, data phối hợp tham gia. Các Gateway liên kết mạng PSTN hoặc ISDN phục vụ cho các điểm cuối thuộc hai mạng làm việc với nhau. Các Gatekeeper cung cấp các dịch vụ như điều khiển tiếp nhận, thông dịch địa chỉ cho các đầu cuối hoặc cho Gateway. Các MCU cho phép các thiết bị đầu cuối hay các Gateway thiết lập hội nghị trên các phiên audio, video và data.

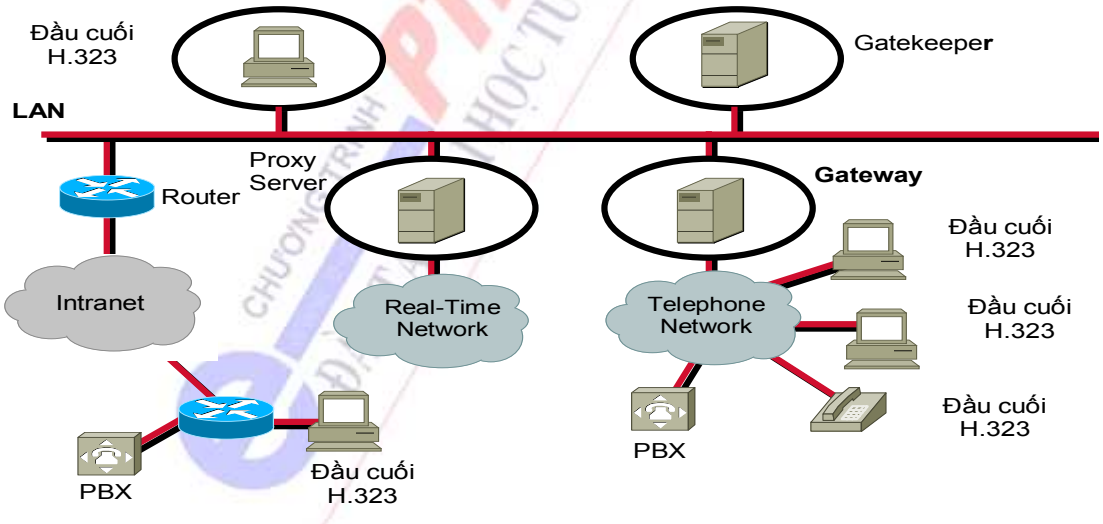
H.323 là một tập các giao thức và thủ tục cung cấp các dịch vụ truyền thông đa phương tiện - truyền thoại, hình ảnh và dữ liệu thời gian thực qua mạng chuyển mạch gói bao gồm mạng IP-based LAN, MAN, WAN… do Hiệp hội viễn thông quốc tế về tiêu chuẩn hoá ITU-T đưa ra. Chuẩn H.323 bao gồm các chức năng như báo hiệu và điều khiển cuộc gọi, vận chuyển và điều khiển đa truyền thông (Multimedia Transport and Control), điều khiển độ rộng băng tần cho hội nghị điểm-điểm và hội nghị đa điểm (Point-to-Point and Multipoint Conferences). Ngoài khuyến nghị H.323, các khuyến nghị thuộc nhóm H (H-Series) còn có: H.320 cho mạng tích hợp số đa dịch vụ ISDN, H.324 cho dịch vụ mạng thoại thông thường POTS (Plain Old Telephone Service) như là các kỹ thuật vận chuyển.

Chuẩn H.323 bao gồm các thành phần và giao thức sau :

| | |
|---|---|
| Báo hiệu cuộc gọi | H.225 |
| Điều khiển truyền thông | H.245 |
| Mã hoá và giải mã Audio | G.711, G.722, G.723, G.728, G.729 |
| Mã hoá và giải mã Video | H.271, H.263 |
| Chia sẻ dữ liệu | T.120 |
| Giao vận truyền thông | RTP/RTCP |




**Hình 6.10 Mô hình giao thức H.323**




**Hình 6.11 Mô hình mạng theo chuẩn H.323**

Giao thức SIP (Session Initial Protocol): Giao thức khởi tạo phiên SIP là giao thức điều khiển báo hiệu lớp ứng dụng, thiết lập, duy trì và kết thúc các phiên đa truyền thông bao gồm thoại Internet, các hội nghị và các ứng dụng audio, video và data .. SIP hỗ trợ các phiên điểm - điểm hoặc đa điểm. SIP là giao thức dựa trên kí tự văn bản (Text Based Protocol), kiến trúc đa truyền thông. Các chức năng của SIP độc lập với nhau, có thể giao tiếp, liên kết với các giao thức báo hiệu khác như giao thức H.323 .

Real-time Transport Protocol RTP là một giao thức End to End, thời gian thực như Audio và Video. RTP thực hiện việc quản lý về thời gian truyền, quản lý số hiệu tuần tự, kiểm tra truyền dữ liệu và nhận dạng kiểu dữ liệu được truyền. Nhưng RTP không cung cấp bất cứ một cơ chế nào bảo đảm thời gian truyền và cũng không cung cấp bất cứ một cơ chế nào giám sát chất lượng dịch vụ. Sự giám sát và bảo đảm về thời gian truyền dẫn cũng như chất lượng dịch vụ được thực hiện nhờ hai giao thức là RTCP và RSVP.

Real-time Transport Control Protocol RTCP: Mặc dù RTP là một giao thức độc lập nhưng thường được hỗ trợ bởi giao thức RTCP điều khiển cho phép gửi về các thông tin bên thu và tự thích nghi với bên phát như tự thích nghi kiểu nén tín hiệu và từ điều chỉnh lưu lượng dữ liệu cho phù hợp với bên phát.

Resource Reservation Protocol RSVP: Cung cấp một cơ chế đảm bảo băng thông cho các hoạt động của các ứng dụng. RSVP gửi tham số chất lượng dịch vụ QoS kết hợp với các dữ liệu thời gian thực được truyền trên mạng TCP/IP. Hỗ trợ giao thức RTP, giao thức RSVP có thể giải quyết các lỗi xảy ra trên đường truyền để đảm bảo các tham số chất lượng. Giao thức RTP chỉ hỗ trợ việc truyền thông điểm - điểm và không quản lý các tham số liên kết trên mạng. RSVP không những tác động ở máy phát, máy thu mà còn tác động trên cả các Router trong mạng. RSVP thiết lập và duy trì kết nối duy nhất cho một luồng dữ liệu, xác lập một hệ thống quản lý thứ tự các gói và tạo modun điều khiển để quản lý các nguồn tài nguyên của các nút mạng khác nhau. RSVP đưa ra một mô hình tối ưu để liên kết các dữ liệu từ mộ nguồn tới nhiều đích. RSVP đóng vai trò quản lý một cách độc lập các host đích để tự thích nghi các tham số chất lượng giữa khả năng cung cấp và nhu cầu đáp ứng.

Giao thức MGCP (Media Gateway Control Protocol) cho phép điều khiển các Gateway thông qua các thành phần điều khiển nằm bên ngoài mạng. MGCP sử dụng mô hình kết nối tương tự như SGCP dựa trên các kết nối cơ bản giữa thiết bị đầu cuối và gateway. Các kết nối có thể là kết nối điểm-điểm hoặc kết nối đa điểm. Ngoài các chức năng điều khiển như SGCP, MGCP còn cung cấp thêm các chức năng yêu cầu Gateway xác định kiểu mã hoá ở phía đường dây kết nối đến thiết bị đầu cuối, kiểm tra trạng thái và kết nối ở một thiết bị đầu cuối và thông báo với Call Agent khi nào các thiết bị đậu cuối ngừng sử dụng dịch vụ và khi nào quay lại sử dụng dịch vụ.

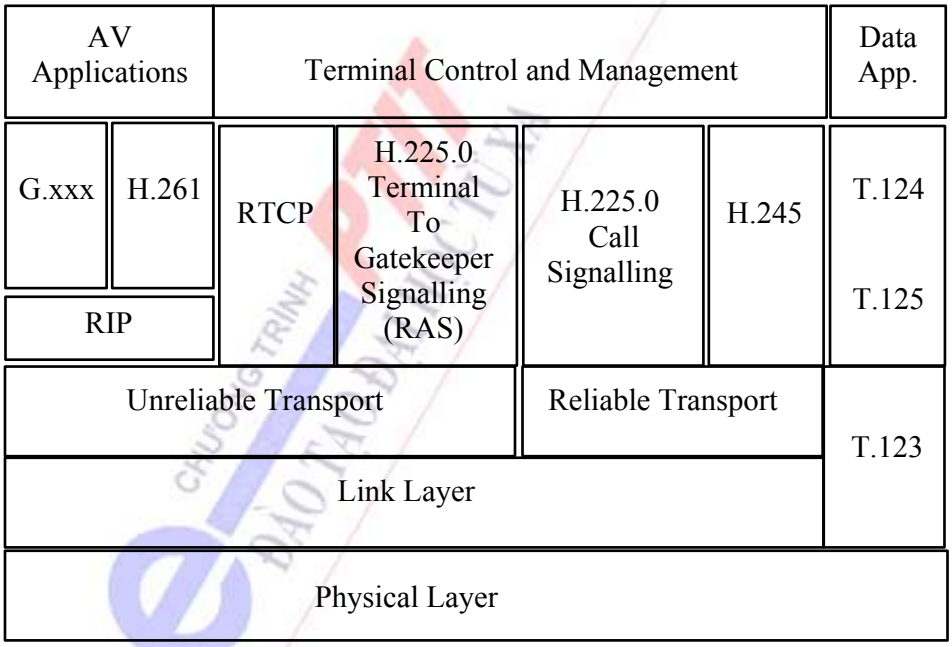
Giao thức Megaco/H.248: Kiến trúc chính của Megaco được thể hiện bao gồm hoạt động giữa các hệ thống MG, MGC. Megaco chia các thiết bị có chức năng khác nhau thành phần truyền thông và phần báo hiệu. Trong khi Media Gateway (Cổng giao tiếp truyền thông) điều khiển phần truyền thông thì Media Gateway Controller (Bộ điều khiển cổng giao tiếp truyền thông) hay Call Agents (Các tác nhân gọi) lại điều khiển các MGs để thiết lập các đường dẫn truyền thông thông qua mạng phân tán. Một MGC có thể điều khiển nhiều MGs . Nói một cách khác, một MG có thể đăng ký với nhiều MGCs. Việc trao đổi thông tin giữa hai thiết bị này (MG và MGC) được thực hiện nhờ giao

thức Megaco. Vì thế, Megaco là một giao thức chủ/tớ, các tác nhân cuộc gọi hoạt động như các bộ khởi tạo lệnh (máy chủ), còn các MGs hoạt động như các bộ đáp ứng lệnh (máy tớ).

Điều khiển và truyền tải thông tin H.245 mô tả chi tiết cấu trúc và định nghĩa các bản tin, tóm lược những thủ tục điều khiển, thiết lập và giám sát quá trình liên lạc đa phương tiện (dữ liệu và âm thanh) giữa hai điểm cuối. Các bản tin điều khiển H.245 kiểm soát hoạt động của các phần trong mạng H.323 bao gồm khả năng trao đổi, đóng mở kênh logic, yêu cầu chế độ ưu tiên, điều khiển luồng. Các bản tin được truyền trên kênh điều khiển H.245 tương ứng với kênh lôgic 0. Mỗi cuộc gọi chỉ có một kênh điều khiển H.245 được thiết lập chức năng điều khiển đến khi kênh logic 0 được giải phóng. Báo hiệu H.245 được thiết lập giữa hai điểm cuối, có thể là thiết bị đầu cuối, MC, Gateway hoặc Gatekeeper.

Báo hiệu điều khiển cuộc gọi H.225 mô tả phương thức tích hợp dữ liệu, phương thức mã hoá và đóng gói thông tin giữa hai thành phần của mạng H.323. H.225 cũng mô tả các giao thức và định dạng các bản tin cho Gateway H.323 có liên quan đến các thiết bị đầu cuối H.320, H.324 hoặc H.310, H.321 trên các mạng N-ISDN, B-ISDN. Ngoài ra, chuẩn H.225 còn mô tả các giao thức và định dạng các bản tin cho quá trình truyền thông giữa Gateway H.323 và Gateway H.322 cũng như các điểm cuối trong mạng H.322 với sự đảm bảo về chất lượng dịch vụ (QoS).

RTCP: H.225 còn được thiết kế để một Gateway H.323 có khả năng phối hợp hoạt động với các loại thiết bị đầu cuối H.320. Ngoài ra H.225 còn bảo đảm chất lượng dịch vụ của thiết bị đầu cuối H.320 có thể được thay đổi phù hợp với đặc tính và khả năng của Gateway H.323.




**Hình 6.12 Mối quan hệ các giao thức trong H323**

Báo hiệu đăng ký, chấp nhận và trạng thái RAS: Kênh RAS được sử dụng để truyền các bản tin phục vụ quá trình tìm kiếm Gatekeeper và đăng ký điểm cuối. Các bản tin RAS được truyền trên kênh không được đảm bảo độ tin cậy do đó tất cả các bản tin đều được quy định một khoảng

thời gian và một bộ đếm. Khi điểm cuối hoặc Gatekeeper không thể phúc đáp lại yêu cầu trong khoảng thời gian quy định thì có thể sử dụng bản tin RIP (Request in Progress) để chỉ thị rằng yêu cầu vẫn đang được xử lý. Điểm cuối hoặc Gatekeeper nhận được bản tin RIP sẽ đặt lại đồng hồ và bộ đếm.

RAS còn được sử dụng để truyền các bản tin về quá trình chấp nhận, thay đổi độ rộng băng tần, cung cấp thông tin trạng thái. Các bản tin này được trao đổi giữa Gatekeeper và điểm cuối để cung cấp các chức năng điều khiển truy nhập và quản lý băng tần. Điểm cuối gửi bản tin ARQ (Admission Request) đến Gatekeeper bao gồm cả các thông tin về độ rộng băng tần yêu cầu. Đó là tốc độ giới hạn trên cho các luồng tín hiệu phát và thu bao gồm cả kênh Audio kênh Video và các Header như RTP Header, RTCP Header... Gatekeeper có thể chấp nhận hoặc giảm các yêu cầu này.

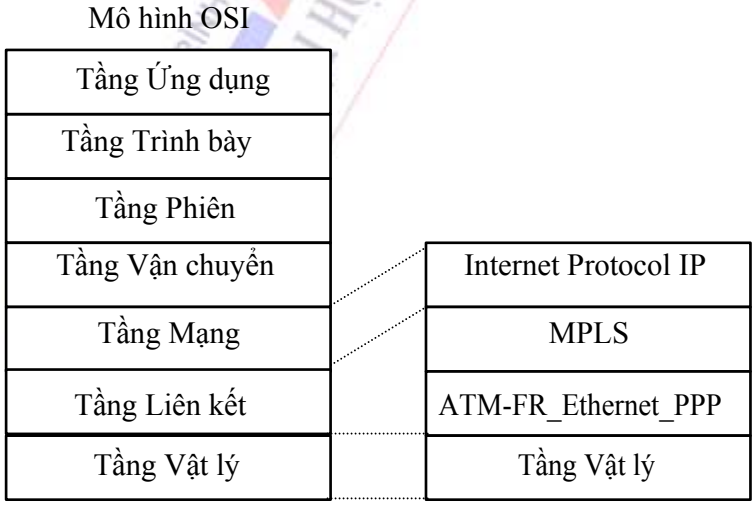
## 6.3. Công nghệ chuyển mạch nhãn đa giao thức MPLS (MultiProtocol Label Switching)

### 6.3.1. Mở đầu

Chuyển mạch nhãn đa giao thức MPLS là một kỹ thuật truyền dữ liệu trong công nghệ mạng truyền thông, được chuẩn hóa bởi tổ chức IETF trong khuyến nghị RFC 3031.Ý tưởng cơ bản của MPLS là cung cấp một dịch vụ truyền gói tin thống nhất cho chuyển mạch kênh và chuyển mạch gói dựa trên các thiết bị chuyển mạch tốc độ cao, có cấu trúc đơn giản. MPLS có khả năng hỗ trợ nhiều mô hình dịch vụ và quản lý được lưu lượng nên có thể được dùng để chuyển tải nhiều loại lưu lượng khác nhau như thoại, số liệu, video...

MPLS được xem là sự tích hợp giữa công nghệ chuyển mạch gói và chuyển mạch kênh, giữa chức năng định tuyến trên nền tảng IP và chức năng chuyển mạch trên nền tảng ATM.

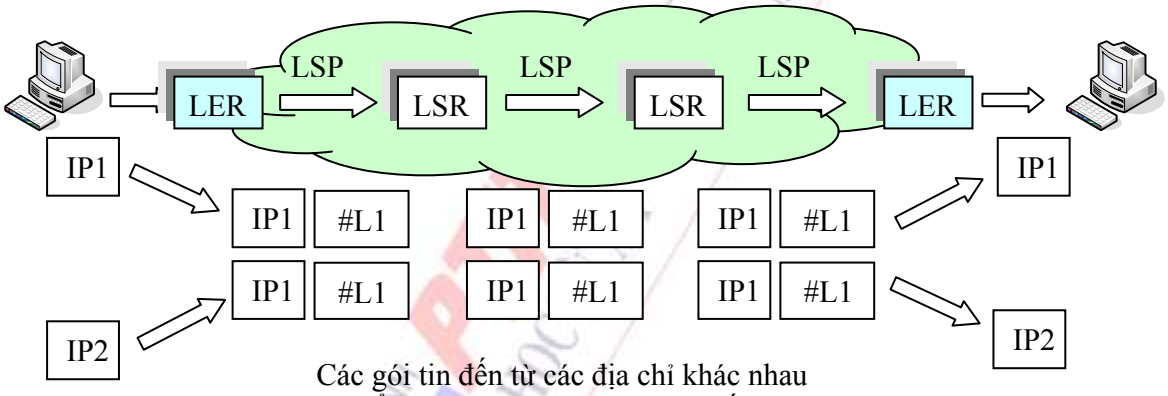
### 6.3.2. Kiến trúc và nguyên tắc hoạt động MPLS




**Hình 6.13 MPLS trong mô hình OSI**

Cấu trúc mạng MPLS: Một cách tổng quát, cấu trúc mạng MPLS gồm có 2 phần biên và lõi. Chức năng các thành phần trong mạng tách biệt. Chức năng chuyển mạch nhãn và chuyển gói có xu hướng tập trung ở phần lõi, chức năng xử lý gói và định tuyến được đẩy về thành phần biên. Bộ định tuyến biên LER (Label Edge Router) là phần tử biên của mạng MPLS thường được tích hợp các giao thức định tuyến MPLS và IP. Phần tử này còn được gọi là bộ định tuyến PE (Provider Edge). Tùy theo vị trí của LER đối với chiều đi của gói tin gọi LER là bộ định tuyến đầu vào (Ingress) hay đầu ra (Egress). Bộ định tuyến lõi LSR (Label Switch Router) là phần tử nằm trong mạng MPLS, thực hiện chức năng định tuyến dựa trên việc chuyển mạch nhãn. Phần tử này còn được gọi là bộ định tuyến P (Provider).

Nguyên tắc chuyển mạch nhãn MPLS: Gói tin chưa được gán nhãn MPLS được chuyển đến LER để chuyển qua mạng MPLS, LER sẽ xác định và phân loại gói tin vào các lớp gọi là lớp chuyển tiếp tương đương FEC (Forwarding Equivalence Class). Phần Header MPLS của gói tin sẽ được thêm bằng cách chèn thêm một hoặc nhiều nhãn trước gói tin. Sau đó, gói tin được chuyển đi trên tuyến logic gọi là hầm (Tunnel) để đến Router kế tiếp trên đường đến đích. Việc ấn định FEC dựa trên một phần hoặc toàn bộ địa chỉ lớp mạng đích. Các gói tin thuộc cùng một FEC sẽ được chuyển đi trên cùng một tuyến gọi là LSP (Label Switch Path). Cơ chế chuyển gói theo các LSP cho thấy tính định hướng kết nối của MPLS.




**Hình 6.13 Nguyên tắc hoạt động của MPLS**

Cơ chế phân phối nhãn nhằm mục đích trao đổi các thông tin liên kết nhãn trong mạng MPLS đảm bảo cho các bộ định tuyến liền kề có thể cập nhật, duy trì và thống nhất với nhau về giá trị nhãn cho các FEC (biểu thị bởi trường Destination) trong cơ sở dữ liệu nhãn. Cơ chế này có thể dựa trên giao thức định tuyến BGP, OSPF, RSVP-TUNNELS hoặc giao thức phân phối nhãn chuyên dụng LDP (Label Distribution Protocol). Việc trao đổi thông tin nhãn trong MPLS theo nguyên tắc ngang hàng. Có 4 loại bản tin trong LDP: Discovery, Session, Advertisement và Notification.

Cơ chế xử lý nhãn và chuyển gói tin: Khi một gói tin đã được gán nhãn MPLS được chuyển đến LSR, phần nhãn ngoài cùng sẽ được phân tích. Tùy theo nội dung của nhãn, một trong ba thao tác sau đây sẽ được thực hiện lên chồng nhãn: tráo đổi hay thay nhãn mới (Swap), lấy nhãn ra (Pop), thêm nhãn vào (Push).

Thao tác Push sẽ cộng thêm nhãn vào phía trước của phần nhãn đang có, nghĩa là đóng gói tin (Encapsulating) vào phân lớp khác trong MPLS. Quá trình này cho phép gói tin MPLS được định tuyến theo cơ chế phân cấp (Hierarchical Routing), đặc biệt là được sử dụng cho dịch vụ VPN.

Cơ chế điều khiển lưu lượng và chất lượng dịch vụ trong MPLS: MPLS hỗ trợ chức năng điều khiển lưu lượng nhờ quản trị mạng tạo ra LSP theo phương pháp định tuyến cưỡng bức để đảm bảo chất lượng dịch vụ hoặc giảm lưu lượng tải qua các nút chuyển tiếp tránh tắc nghẽn trong các tình huống đặc biệt. Với cơ chế định tuyến ràng buộc, người quản lý mạng lập trình các điều kiện ràng buộc và mạng MPLS sẽ tự động thực hiện việc định tuyến thỏa mãn các điều kiện trên. Cơ chế này được hỗ trợ bởi báo hiệu LDP để tạo ra các CR-LSP (Compulsory Routing - LSP). MPLS hỗ trợ chất lượng dịch vụ trên cơ sở phân loại các luồng lưu lượng theo độ trễ, băng tần..... Tại biên của mạng, luồng lưu lượng được nhận dạng thông qua việc phân tích một số trường trong Header của gói tin để phân loại chúng vào các FEC để chuyển đi trong các LSP có thuộc tính CoS hay QoS. Thông tin CoS có thể được truyền trong nhãn của mỗi gói hoặc được gán ngầm định cho LSP. Thông tin QoS được hỗ trợ trong trường hợp mạng MPLS chạy trên nền ATM. Vấn đề đặt ra trong MPLS là tiêu chí để phân loại gói tin thành các FEC. Điều này phụ thuộc nhiều vào công nghệ xử lý gói tải tin.

Đánh giá công nghệ chuyển mạch nhãn đa giao thức MPLS:

a. *Ưu điểm*: Công nghệ MPLS đơn giản, có thể giải quyết được vấn đề độ phức tạp và khả năng mở rộng mạng. Có thể thay thế công nghệ ra đời trước đó như Frame Relay, ATM. Có thể nói MPLS hội tụ những ưu điểm của cơ chế định tuyến gói IP và cơ chế hoán đổi nhãn của ATM, cho phép giảm thiểu thời gian xử lý gói tin mà không cần thay đổi các giao thức định tuyến IP. Nhãn MPLS đơn giản, kích thước nhỏ và linh hoạt. Có thể xếp nối tiếp nhãn để tạo thành chồng nhãn có độ phức tạp cao, rất tiện lợi cho việc đánh địa chỉ và truy tìm.

Nếu so sánh với ATM thì MPLS có ưu điểm là không cần đến các giao thức điều khiển báo hiệu hay chuyển mạch tế bào phức tạp như ATM. Kích thước gói MPLS lớn hơn nhiều so với tế bào ATM nên giảm đáng kể thông tin tiêu đề đóng gói tải tin. Mạng truyền thông hiện đại , công nghệ mạng quang với tốc độ cực lớn (10Gbit/s) không chỉ chuyển tải được các gói tin có độ dài 1518 byte (kích thước cực đại của gói Ethernet) mà còn chuyển tải được gói tin MPLS có kích thước tải tin bất kỳ. Tóm lại, MPLS cho phép nâng cao độ thông (thông lượng) mạng. Mặc khác, MPLS duy trì được chức năng kiểm soát lưu lượng và điều khiển ngoài băng như FR hay ATM. MPLS cũng có thể tận dụng cơ sở hạ tầng mạng ATM vì gói tin MPLS có thể chuyển vào kênh ảo ATM và ngược lại. So với giải pháp IP/ATM, IP/MPLS có topo (cấu trúc lên kết) và cấu hình mạng đơn giản hơn.

Ưu điểm của MPLS so với IP là khả năng điều khiển lưu lượng và hỗ trợ kiểm soát chất lượng dịch vụ (cao hơn DiffServ, thấp hơn ATM). MPLS tách bạch rõ ràng chức năng định tuyến với chức năng chuyển tiếp gói (Routing- Forwarding) mặc dù có thể sử dụng lại kiểu định tuyến IP nếu cần.

Nhìn chung, MPLS là công nghệ phù hợp và bắt kịp với xu thế và nhu cầu công nghệ truyền thông hiện tại và tương lai. MPLS hiện tại đang được ứng dụng trong mạng lõi NGN, trong kỹ thuật lưu lượng và nền tảng cho dịch vụ VPN.

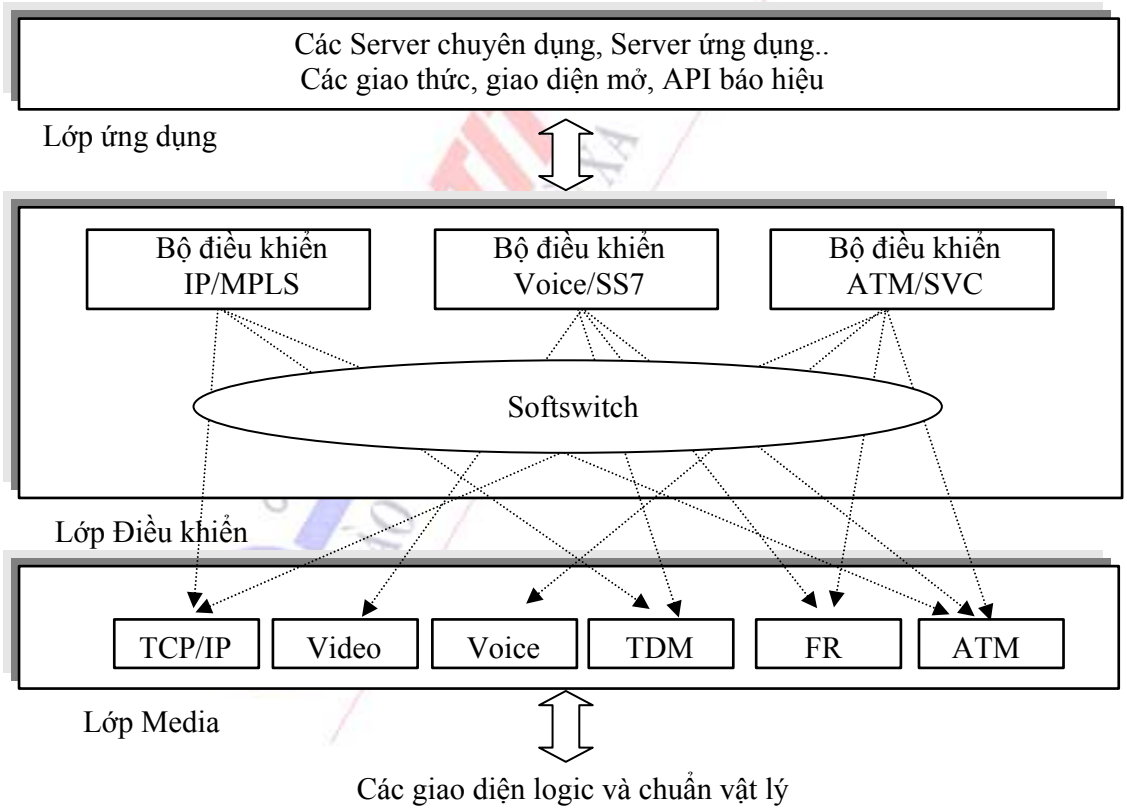
*b. Hạn chế của MPLS*: MPLS không cung cấp dịch vụ đầu cuối (End-Point) để có thể sử dụng trực tiếp như Ethernet. Về phương diện này, MPLS tương tự như giao thức PPP. MPLS có khả năng bị ảnh hưởng bởi lỗi đường truyền cao hơn các công nghệ khác nên phần nào làm giảm đi độ tin cậy. Đối thủ duy nhất hiện nay của MPLS là giao thức L2TPv3 trong lĩnh vực VPN đặc biệt là trong các mạng có lớp lõi thuần túy là IP.

Xu hướng phát triển: Hướng phát triển mới của MPLS là GMPLS, cung cấp mảng điều khiển chung dựa trên cơ sở IP cho tất cả các lớp. GMPLS sẽ sử dụng kết hợp các thiết bị chuyển mạch gói (bộ định tuyến...) và các thiết bị chuyển mạch kênh (SDH..)

## 6.4. Công nghệ chuyển mạch mềm (Softswitch)

### 6.4.1. Mở đầu

Hệ thống chuyển mạch mềm thực hiện chức năng xử lý cuộc gọi trong mạng NGN như định tuyến, báo hiệu, cung cấp dịch vụ cuộc gọi. Chuyển mạch mềm dựa trên ý tưởng tách riêng chức năng điều khiển cuộc gọi (phần mềm) khỏi chức năng chuyển mạch vật lý (phần cứng) và đặt nền tảng trên cơ sở chuyển mạch gói. Chuyển mạch mềm được thực thi bằng các module phần mềm và các giao diện chương trình ứng dụng API (Application Program Interface) chạy trên nền phần cứng là các hệ thống Server dung lượng lớn. Vị trí của chuyển mạch mềm thuộc lớp điều khiển trong mô hình phân lớp chức năng của NGN.




**Hình 6.14 Vị trí chuyển mạch mềm trong mô hình phân lớp NGN**

Các đặc trưng cơ bản của công nghệ chuyển mạch mềm như sau:

- Dựa trên công nghệ chuyển mạch gói.

- Thiết kế theo mô hình xử lý phân tán

- Giao diện mở API

- Phần mềm điều khiển chuyển mạch không phụ thuộc vào phần cứng chuyển mạch như ở các thiết bị chuyển mạch truyền thống. Có khả năng lập trình được độc lập.

- Tích hợp và liên kết các giao thức khác nhau trong mạng NGN và giữa NGN với mạng truyền thống (PSTN, ATM&IP…).

### 6.4.2. Cấu trúc và nguyên tắc chuyển mạch mềm

Chuyển mạch mềm hoạt động liên quan đến rất nhiều giao thức ứng dụng khác nhau. Việc liên kết các giao thức được thực hiện nhờ việc liên kết các khối chức năng trong chuyển mạch mềm với sự hỗ trợ đặc biệt của khối liên kết mạng IW-F. Mô hình giao thức sử dụng giải pháp chuyển mạch mềm tổng quát như sau:

BICC (Bearer Independent Call Control): Là giao thức điều khiển cuộc gọi độc lập với kênh truyền tải. Báo hiệu dựa trên ISUP theo chuẩn ITU-T. BICC hỗ trợ các dịch vụ ISDN băng hẹp. BICC thường được dùng cho báo hiệu giữa các chuyển mạch mềm.

MEGACO/H.248/MGCP: Đây là giao thức điều khiển điều khiển giữa Softswitch (MGC) và thiết bị cổng MG theo cơ chế Master/Slave. MGC quyết định chính trong quá trình liên lạc với MG, còn MG là thực thể thụ động thực hiện mọi lệnh do MGC yêu cầu. Các tương tác (transaction) trong MGCP gồm có lệnh và đáp ứng.

RTP/RTCP/RTSP: Real Time Protocol/ Real Time Control Protocol-Real Time Streaming Protocol: là các giao thức hoạt động ngay trên lớp UDP dùng để truyền các thông tin yêu cầu thời gian thực qua mạng gói. RTP được xem như giao thức lớp truyền tải. Bản thân RTP không đảm bảo chất lượng của thông tin cần truyền tải về thời gian thực. Nó chỉ đơn giản cung cấp đầy đủ thông tin lên lớp ứng dụng để xác định độ trễ gói và quyết định cách thức xử lý gói tin như hiệu chỉnh độ di pha. Các dịch vụ mà RTP cung cấp là loại thông tin chuyển tải trong gói, số thứ tự của gói truyền (sequence number), mốc thời gian và thời gian truyền tối đa của 1 gói (Timestamp). Các bản tin RTCP được dùng để trao đổi thông tin phản hồi về chất lượng của phiên RTP đối với tất cả các thành viên tham gia trong phiên truyền tin.

SCTP (Stream Control Transport Protocol) hay SIGTRAN (Signalling Transport): là một giao thức hướng liên kết truyền tải (Transport Protocol) được xây dựng để thay thế TCP (Transmission Control Protocol) trong việc chuyển tải thông tin báo hiệu SS7 trong mạng chuyển mạch vì lý do TCP là giao thức đảm bảo truyền dữ liệu tin cậy thông qua cơ chế xác nhận ACK và cơ chế tuần tự gây trễ gói tin. Các cơ chế này đã có trong giao thức SS7, hơn nữa SS7 yêu cầu thời gian thực nên việc dùng TCP cho SS7 là không hiệu quả.

SCTP chuyển tải theo định hướng bản ghi thay vì định hướng byte như TCP, đồng thời cho phép nhiều luồng dữ liệu logic được ghép kênh để truyền qua một kết nối. SCTP đảm bảo truyền tin cậy theo cơ chế khác với TCP bằng cách thiết lập nhiều kết nối.

SIP (Session Initiation Protocol)/H.323: Các bộ giao thức điều khiển cuộc gọi đa phương tiện (lớp ứng dụng), dùng để thiết lập, điều chỉnh và kết thúc phiên làm việc của thuê bao.

### 6.4.3. Giao diện ứng dụng API trong chuyển mạch mềm

Chuyển mạch mềm ứng dụng công nghệ phần mềm lập trình theo hướng đối tượng, công nghệ Agent và xử lý phân tán. API là tập hợp các thủ tục, giao thức và các công cụ phần mềm được chuẩn hóa nhằm cho phép liên kết các ứng dụng với nhau. Bằng cách xây dựng các khối chức năng theo API, có thể dễ dàng phát triển ứng dụng phần mềm. API cho phép chia sẻ dữ liệu giữa các ứng dụng trên cùng nền tảng.

**a. Các phương thức chia sẻ dữ liệu qua API:**

- Gọi thủ tục từ xa RPC (Remote Procedure Calls): Dùng cho các ứng dụng trao đổi thông tin với nhau bởi các thủ tục (Procedure/Task) trên cùng bộ đệm dữ liệu.

- Ngôn ngữ truy vấn chuẩn SQL (Standard Query Language) là ngôn ngữ dùng truy xuất dữ liệu không cần thủ tục, cho phép chia sẻ dữ liệu giữa các ứng dụng bằng cách truy nhập vào cơ sở dữ liệu chung.

- Chuyển file (File Transfer): Phương thức này cho phép chia sẻ số liệu bằng cách trao đổi file đã được định dạng giữa các ứng dụng.

- Phân phát bản tin (Message Delivery): Cho phép chia sẻ dữ liệu bằng cách trao đổi thông tin trực tiếp thông qua các bản tin định dạng có kích thước nhỏ giữa các ứng dụng có liên kết với nhau.

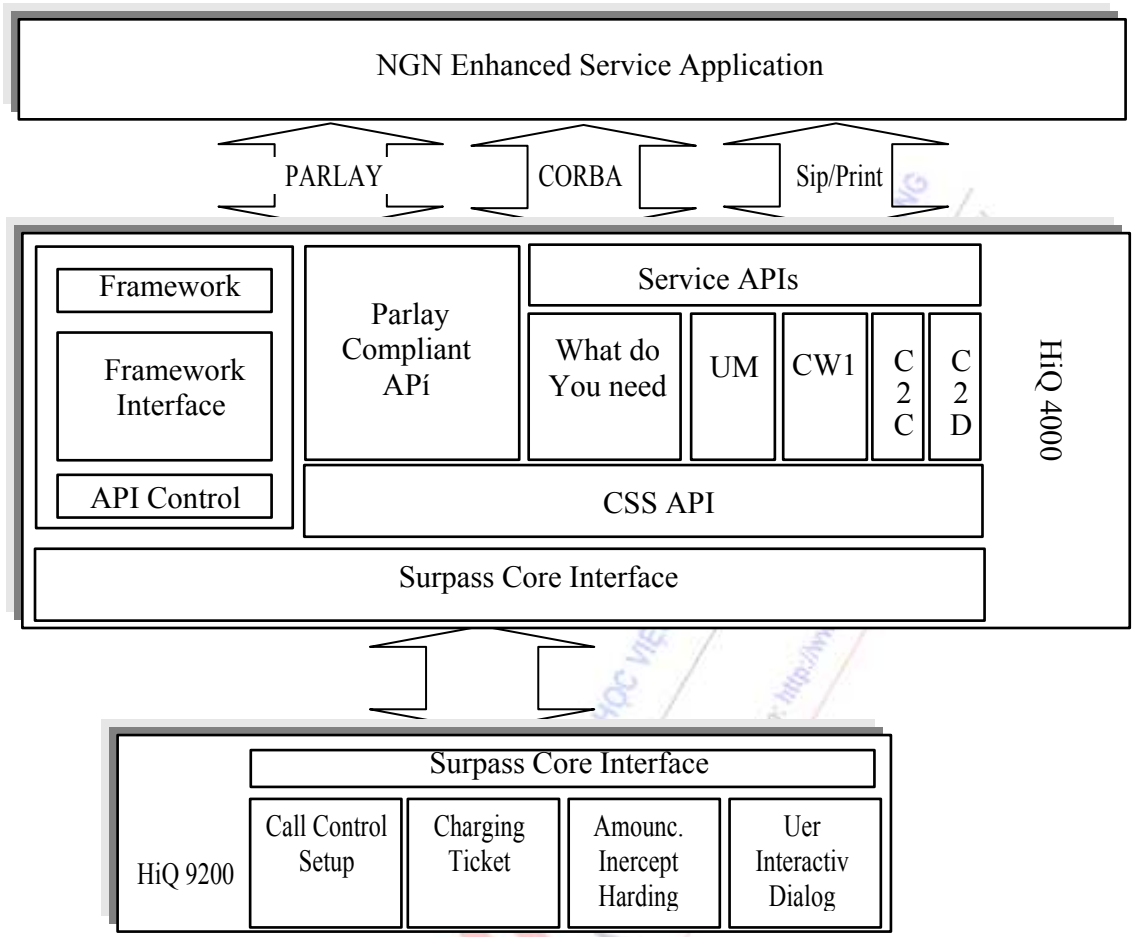
**b. Có thể phân lớp các API trong Softswitch thành 3 nhóm chính:**

- API liên kết các nguồn tài nguyên mạng (Resources API)

- API liên kết các module có năng lực xử lý trong mạng (Network Capability API)

- API liên kết NGN với môi trường ngoài như nhà cung cấp dịch vụ thứ 3 hay khách hàng có nhu cầu phát triển ứng dụng.

CHƯƠNG TRÌNH PTIT ĐÀO TẠO ĐẠI HỌC TỪ XA




**Hình 6.15 Mô hình API trong chuyển mạch mềm giải pháp của SIEMENS**

Hiện nay, API liên kết các nguồn tài nguyên mạng và API liên kết các module có năng lực xử lý trong mạng được phát triển nhiều trên cơ sở JAIN (Java API Intergrated Network). Nhóm thứ ba được phát triển theo nhiều hướng như JAIN, 3GPP (3th Generation Ship Project, PARLAY GROUP). Các chuẩn API hiện vẫn đang được phát triển và chuẩn hiện đang được dùng phổ biến là SQL API của ANSI.

### 6.4.4. Kế hoạch đánh số trong chuyển mạch mềm

Việc đánh địa chỉ cũng như số thuê bao và dịch vụ trong NGN là hoàn toàn linh hoạt bằng cách khai báo dữ liệu kho số vào cơ sở dữ liệu động của máy chủ quản lý địa chỉ. Cơ sở dữ liệu này có thể cập nhật, bổ sung hoặc thay đổi bởi nhà quản trị mạng, tuy nhiên phải dựa các tiêu chí chính như sau:

- Quy luật đánh địa chỉ tuân theo khuyến nghị của ITU-T (E164-E169).

- Quy hoạch địa chỉ cần kế thừa và giữ được thói quen quay số của người dùng.

- Quy hoạch địa chỉ tận dụng một số các mã đặc biệt dành riêng để phát triển về sau với nhiều mục đích khác nhau.

- Việc quy hoạch địa chỉ trong NGN phải đảm bảo không trùng lặp với các dải địa chỉ đang được sử dụng trong các mạng truyền thống kết nối đến mạng NGN.

### 6.4.5. Đánh giá công nghệ chuyển mạch mềm

**Bảng so sánh công nghệ Softwwitch và chuyển mạch kênh.**

| | **Softswitch** | **Tổng đài PSTN** |
|---|---|---|
| Phương pháp chuyển mạch | Phần mềm | Điện tử |
| Kiến trúc | Phân tán, theo các chuẩn mở | Riêng biệt của từng nhà sản xuất |
| Khả năng tích hợp với ứng dụng của nhà cung cấp khác | Dễ dàng | Khó khăn |
| Khả năng thay đổi mềm dẻo | có | Khó khăn |
| Giá thành | Rẻ, khoảng bằng một nửa tổng đài điện tử | Đắt |
| Khả năng nâng cấp | Rất cao | Rất tốt, tuy có hạn chế hơn |
| Giá thành của cấu hình cơ bản | Thấp, giá thành thay đổi gần như tuyến tính theo số lượng thuê bao. Cấu hình cơ bản có thể sử dụng cho mạng doanh nghiệp | Rất cao, tổng đài PSTN không thích hợp cho mạng doanh nghiệp. |
| Truyền thông đa phương tiện | Có | Rất hạn chế |
| Hội nghị truyền hình | Tốt hơn | Có |
| Lưu lượng | Thoại, fax, dữ liệu, video... | Chủ yếu là thoại và fax |
| Thiết kế cho độ dài cuộc gọi | Khụng hạn chế | Ngắn (chỉ vài phút) |

Công nghệ chuyển mạch mềm có những ưu điểm nổi bật so với các công nghệ truyền thông như sau:

- Cho phép đưa ra giải pháp phần mềm chung đối với việc xử lý cuộc gọi, có thể áp dụng trên nhiều loại mạng khác nhau.

- Đơn giản cấu trúc hệ thống và linh hoạt trong việc thay đổi tính năng, cấu hình, mở rộng phát triển và liên kết giữa các hãng cũng như giữa các nhà cung cấp dịch vụ.

- Cho phép tích hợp và phát triển các phần mềm thông minh của các nhà cung cấp dịch vụ, khai thác tiềm năng của mạng trong tương lai.

- Dễ dàng tích hợp dịch vụ mới từ nhà cung cấp thứ ba đồng thời cho phép người sử dụng có thể tự phát triển ứng dụng và dịch vụ.

## 6.5. Mạng hội tụ và mạng thế hệ sau NGN (Network Convergence and Next Generation Network )

### 6.5.1. Mở đầu

Xu hướng công nghệ truyền thông hiện nay đang xóa dần ranh giới giữa công nghệ thông tin và viễn thông. Thế giới đang bước vào kỷ nguyên của sự hội tụ. Các nhà sản xuất và cung cấp dịch vụ không chỉ quan tâm đến việc phát triển dịch vụ mà còn phải xây dựng và củng cố và tối ưu hóa hạ tầng mạng lưới trên cơ sở hội tụ mạng.

Mạng hội tụ là sự tích hợp một cách thông minh giữa các mạng truyền thông, tích hợp giữa cơ sở hạ tầng của mạng mới với mạng hiện có. Nói cụ thể, hội tụ mạng là sự hợp nhất hay tích hợp nhiều công nghệ, phương tiện truy nhập và truyền thông, giao thức, tài nguyên dữ liệu và ứng dụng khác nhau trên một cơ sở hạ tầng và quản lý chung nhằm tạo ra một mạng truyền thông mới, cung cấp đồng thời nhiều loại hình dịch vụ với chất lượng cao, đáp ứng được đồng thời các loại hình dịch vụ khác nhau, mọi nhu cầu của khách hàng.

Sự hội tụ thể hiện ở nhiều khía cạnh như đa công nghệ, đa giao thức, đa truy nhập, đa phương tiện truyền thông, đa dịch vụ …

Giao thức Internet (IP) được sử dụng phổ biến để liên kết các mạng khác nhau tạo nên mạng hội tụ với xu hướng trước mắt là hội tụ giữa mạng thoại và mạng số liệu.

Một trong những mạng hội tụ tiên tiến đang được ứng dụng là mạng thế hệ sau (Next Generation Network - NGN). Ý tưởng về mạng NGN đã được hình thành từ cuối những năm 90 của thế kỷ trước và cho đến nay NGN đã được triển khai rộng khắp ở các nước phát triển và đang phát triển, thay thế dần các mạng truyền thống thế hệ trước.

### 6.5.2. Tổng quan về mạng thế hệ sau sau - NGN (Next Generation Network )

**Mạng thế hệ sau NGN được xây dựng theo các nguyên tắc sau:**

- Có kiến trúc mở, phân lớp, linh hoạt, dễ dàng phát triển mở rộng
- Cơ sở hạ tầng dựa trên công nghệ truyền tải băng rộng, công nghệ chuyển mạch gói
- Có khả năng kiểm soát được chất lượng dịch vụ (QoS)
- Đáp ứng được đồng thời và đa dạng các loại hình dịch vụ, cho phép thuê bao truy nhập một cách linh hoạt đến nhiều nhà cung cấp dịch vụ khác nhau.
- Lớp (chức năng) cung cấp dịch vụ độc lập với lớp (công nghệ) truyền tải bên dưới.
- Tương thích và hỗ trợ các mạng và dịch vụ hiện có

**NGN hội tụ những ưu điểm của công nghệ chuyển mạch kênh và chuyển mạch gói:**

a. Ưu điểm từ chuyển mạch kênh:

- Đảm bảo thời gian thực
- Giảm hiện tượng thất thoát thông tin do nghẽn hay trễ
- Đảm bảo chất lượng dịch vụ

b. Ưu điểm từ chuyển mạch gói:

- Chia xẻ và tận dụng được tài nguyên mạng

- Linh hoạt trong việc định tuyến và điều khiển lưu lượng
- Kích thước tải tin có thể thay đổi

### 6.5.3. Sự bùng nổ và nhu cầu da dạng của các loại hình dịch vụ

- Dịch vụ băng hẹp (voice) - Dịch vụ băng rộng (video, truyền hình)
- Dịch vụ đơn phương tiện (fax) - Dịch vụ đa phương tiện (hội nghị truyền hình)
- Dịch vụ truyền thông theo thời gian thực (đàm thoại) - Dịch vụ phi thời gian thực (truyền số liệu)
- Dịch vụ truy cập ứng dụng của nhà cung cấp dịch vụ (MegaVNN) - Dịch vụ thuê cơ sở hạ tầng (MegaWAN)
- Dịch vụ đơn giản (giải đáp thông tin) - Dịch vụ thông minh (truy xuất cơ sở dữ liệu thông tin tự động)
- Dịch vụ tương tác 2 chiều (trò chơi) - Dịch vụ phân bố một chiều (quảng bá)
- Dịch vụ chất lượng thấp (VoIP giá rẻ 8Kb/s) - Dịch vụ chất lượng cao (VoIP 64kb/s)

Các dịch vụ băng rộng yêu cầu tốc độ và thời gian chiếm kênh lớn vượt quá khả năng của mạng hiện tại.

### 6.5.4. Mô hình phân lớp và chức năng các lớp NGN

NGN là xu hướng phát triển kỹ thuật mạng hiện đại. Các hãng cung cấp thiết bị khác nhau có các mô hình phân lớp khác nhau. Tuy nhiên, mô hình NGN chung phân chia lớp dịch vụ với lớp truyền tải, giúp cho các nhà cung cấp dịch vụ có thể đưa vào các dịch vụ mới mà không cần quan tâm đến việc kiến trúc lớp truyền tải. Nói cách khác, lớp dịch vụ là độc lập (trong suốt) đối với lớp truyền tải.

**Có thể phân lớp chức năng NGN như sau:**

1. Lớp truy nhập (Access): có chức năng kết nối giữa mạng NGN với thiết bị đầu cuối thuê bao hoặc các mạng truyền thống khác.

2. Lớp truyền tải (Transport): có chức năng định tuyến, chuyển mạch và chuyển tiếp gói tin giữa các phần tử mạng.

3. Lớp điều khiển (Control): có chức năng

- Điều khiển kết nối và báo hiệu cuộc gọi
- Điều khiển lưu lượng và chất lượng dịch vụ
- Điều khiển hoạt động của các phần tử thiết bị trong mạng NGN.

4. Lớp ứng dụng/dịch vụ (Application/Service): có chức năng điều phối và cung cấp các loại hình dịch vụ và ứng dụng trên mạng NGN, cung cấp môi trường kiến tạo dịch vụ mạng thông minh (Intelligent Network Service Creation Environment) và các giao diện mở cho các nhà phát triển dịch vụ thứ ba.

5. Lớp quản lý (Management): có chức năng quản lý mạng theo mô hình TMN:

- Quản lý kinh doanh, chăm sóc khách hàng
- Quản lý dịch vụ
- Quản lý kết nối, tính cước

- Quản lý tài nguyên và chất lượng mạng lưới
- Quản lý phần tử thiết bị

**Kiến trúc phân lớp mang lại cho NGN các ưu điểm sau:**

- Chức năng chuyển mạch vật lý phân tán sẽ giúp giải quyết vấn đề tắc nghẽn
- Chức năng điều phối cuộc gọi tập trung sẽ giúp cho việc quản lý thuận lợi
- Giao diện chuẩn cho phép sự lựa chọn linh hoạt các phần tử mạng của các nhà cung cấp khác nhau, phát huy điểm mạnh của từng nhà cung cấp
- Sự thay đổi hay nâng cấp công nghệ một lớp không ảnh hưởng đến toàn mạng.
- Các nhà cung cấp dịch vụ có thể tự do phát triển các dịch vụ mới mà không quá phụ thuộc vào các nhà khai thác mạng

### 6.5.5. Cấu trúc và các thành phần hệ thống NGN

Các hãng khác nhau đưa ra các giải pháp khác nhau về cấu trúc NGN. Tuy nhiên, nhìn chung các thành phần cơ bản của hệ thống bao gồm:

Các hệ thống ở lớp truy nhập gồm nhiều chủng loại thiết bị với công nghệ khác nhau như POTS, VOIP, IP, FR, X25, ATM, xDSL… cho phép kết nối tới các thiết bị đầu cuối của người dùng (Residential Gateway), kết nối tới mạng truy nhập (Access Gateway) và cung cấp giao diện kết nối và chuyển đổi dạng thông tin giữa NGN với mạng chuyển mạch kênh (Media gateway hay Trunk Gateway).

Các hệ thống ở lớp chuyển tải bao gồm bộ định tuyến, chuyển mạch IP/MPLS, thiết bị truyền dẫn quang dung lượng lớn DWDM/SONET/SDH.

Các hệ thống ở lớp điều khiển bao gồm chuyển mạch mềm (SoftSwitch) là phần tử điều khiển kết nối cuộc gọi (Call Agent) và điều khiển cổng đa phương tiện MGC (Media Gateway Controller), thiết bị cổng báo hiệu SG (Signalling Gateway) cung cấp giao diện kết nối báo hiệu với mạng truyền thống với các giao thức báo hiệu SS7, SMS, WAP...

Các hệ thống ở lớp dịch vụ và ứng dụng bao gồm các thiết bị máy chủ ứng dụng: Media Server (MS), Application Server (AS), Call Feature Server (FS), Man-machine Server, Subscriber Database Server.

Các hệ thống ở lớp quản lý bao gồm các thiết bị quản lý cước, giám sát sự cố, can thiệp lệnh, quản lý cấu hình, tài nguyên, quản lý chất lượng mạng.

### 6.5.6. Các công nghệ nền tảng trong NGN

Công nghệ truy nhập thuê bao số xDSL (Digital Subscriber Line): Là công nghệ điều chế cung cấp giải pháp truyền dữ liệu và thoại trên đường dây cáp đồng âm tần nhằm tận dụng được dải thông tần số của cáp đồng. Về bản chất, DSL là công nghệ thực hiện ở Modem DSL chuyển dữ liệu thành dạng tín hiệu số dung lượng lớn, tần số cao, phổ rộng. DSL bao gồm nhiều phiên bản khác nhau như ADSL có tốc độ hai chiều không đối xứng, HDSL, SHDSL, G.SHDSL (tốc độ hai chiều đối xứng) …

Công nghệ truyền dẫn quang tốc độ cao với ghép kênh phân chia bước sóng mật độ cao DWDM (Dense Wavelength Division Multiplexing) theo phân cấp đồng bộ SONET/SDH

(Synchronous Optical Network/Synchronous Digital Hierachy). WDM cho phép sử dụng độ rộng băng tần rất lớn của sợi quang bằng cách kết hợp một số các tín hiệu ghép kênh theo thời gian với bước sóng khác nhau đồng thời có thể tận# dụng được các cửa sổ không gian, thời gian và độ dài bước sóng. Công nghệ WDM cho phép nâng tốc độ các truyền dẫn lên 5 Gb/s, 10 Gb/s và 20 Gb/s.

Phương thức truyền thông không đồng bộ ATM (Asynchronous Transfer Mode): Thông tin của một ứng dụng không nhất thiết phải xuất hiện một cách tuần hoàn và đồng bộ. ATM sử dụng các tế bào có độ dài cố định 53 byte, không định vị theo xung đồng bộ và thay đổi theo nhu cầu truyền tin. ATM cho phép chuyển tải lưu lượng cho nhiều loại dịch vụ với tốc độ khác nhau. Hiện nay, xu hướng kết hợp công nghệ ATM với DSL mang lại một giải pháp hiệu quả cho dịch vụ truy nhập băng rộng.

Các đặc trưng chính của ATM như sau:

- Hỗ trợ đa dịch vụ, đa tốc độ
- Đảm bảo QoS
- Quản lý băng tần
- Kết nối hướng liên kết.
- Tốc độ chuyển gói cao, giảm trễ gói tin

Định tuyến và chuyển mạch gói tin IP (Internet Protocol): Có các đặc trưng cơ bản sau: Qui hoạch địa chỉ toàn cục: Mỗi một giao diện mạng được gán một địa chỉ duy nhất. Tận dụng năng lực truyền tối đa (Best Effort): IP cố gắng tối đa để chuyền các gói tin, tuy nhiên nó không có cam kết về chất lượng dịch vụ (QoS) như tỉ lệ thành công hay thời gian cần để đưa gói tin đến đích. Với phiên bản IPv6, một số tính năng mới được hỗ trợ như phương pháp đánh địa chỉ linh hoạt, không gian địa chỉ lớn. Cơ chế bảo mật cao. Hỗ trợ đa phương tiện. Hỗ trợ chất lượng dịch vụ QoS và có khả năng tự cấu hình

Chuyển mạch nhãn đa giao thức MPLS (Multiprotocol Label Switching) đã trở thành công nghệ nền tảng trong lớp chuyển tải của NGN.

Công nghệ chuyển mạch mềm (Softswitch):là công nghệ cốt lõi trong lớp điều khiển NGN. Phần tử hệ thống trung tâm sử dụng công nghệ này chính là MGC (Media Gateway Controller). Ngoài ra, công cụ lập trình theo module giao diện chương trình ứng dụng API (Application Program Interface) cũng được ứng dụng nhiều ở các lớp ứng dụng/dịch vụ và quản lý cũng như liên kết giữa chúng với lớp điều khiển trong NGN. Có thể xem API như một công nghệ phần mềm nền tảng trong Softswitch nói riêng và NGN nói chung.

Tóm lại xu hướng hiện nay của công nghệ nền tảng theo phân lớp NGN như sau:

- IP/ATM/DSL: công nghệ nền tảng trong lớp truy nhập
- IP/MPLS/SDH/WDM/Optical: công nghệ nền tảng trong lớp truyền tải
- IP/Ehernet (FE,GE) + Softswitch: công nghệ nền tảng trong lớp điều khiển
- IP/FE + API: công nghệ nền tảng trong lớp ứng dụng/dịch vụ và quản
- SCTP chuyển tải theo hướng bản ghi, không như TCP hướng byte, đồng thời cho phép nhiều luồng dữ liệu logic được ghép kênh để truyền qua một kết nối. SCTP đảm bảo truyền tin cậy theo cơ chế khác với TCP bằng cách thiết lập nhiều kết nối.

### 6.5.7. Mô hình NGN và các giải pháp thiết kế của một số hãng

Trên cơ sở mô hình chung NGN, các hãng viễn thông khác nhau có các giải pháp thiết kế theo nhiều chuẩn khác nhau. Trong đó, một số giải pháp thể hiện tính khả thi, rõ ràng, đáp ứng được mục tiêu đặt ra chung nhất của các mô hình, có nhiều ý tưởng mới và phù hợp với cơ sở hạ tầng mạng hiện tại, đồng thời đảm bảo xu hướng phát triển chung của công nghệ như: giải pháp SURPASS của SIEMENS, Alcatel 1000 SoftSwitch của ALCATEL, ENGINE của ERICSSON… Đặc biệt, mô hình của SIEMENS có nhiều điểm tương đồng với mô hình NGN của tổ chức MSF (MultiService Switching Forum).

* ALCATEL đưa ra giải pháp tổng thể gồm các bước phát triển từ mạng viễn thông hiện tại tiến tới mạng NGN như sau :

1. Duy trì mạng PSTN và hội tụ với mạng số liệu.
2. Phát triển thoại trên công nghệ gói đối với các dịch vụ đường dài.
3. Phát triển thoại trên công nghệ gói đối với các dịch vụ truy nhập nội hạt.
4. Phát triển các dịch vụ đa phương tiện
5. Phát triển mạng NGN hoàn chỉnh

* ERICSSON: Ericsson giới thiệu giải pháp mạng thế hệ mới có tên gọi là ENGINE. Cấu trúc ENGINE hướng tới các ứng dụng và hoạt động theo cơ chế Client/Server và Gateway/Server. Các ứng dụng gồm có hai phần: phần Client trên máy đầu cuối và phần Server chạy trên máy chủ. Hai phần giao tiếp với nhau qua các giao diện mở.

* NORTEL: Mục tiêu chính của Nortel là hoàn thiện mạng lõi, đảm bảo hợp nhất các mạng thoại và số liệu để có thể cung cấp các dịch vụ IP, ATM bằng cách đưa ra giải pháp mạng lõi IP/MPLS bao gồm bộ định tuyến và chuyển mạch MPLS có giao diện quang. Hệ thống chuyển mạch trên cơ sở kết hợp ATM và IP/MPLS có khả năng cung cấp đa dịch vụ cho thuê bao với dung lượng 40 Gbit/s và có khả năng mở rộng lên tới 19,2 Terabit/s.

* JUNIPER: Giới thiệu mô hình NGN gồm các thành phần: POS (Paket over Synchnonization Network). B-RAS (Broadband Remote access Server) và NAS (Narrow Access Server).

* CISCO: DS-1,T1: Digital Signal Level 1, CPE: Customer Premise Equipment, PBX: Private Exchange, SS7: Signalling system no.7, MGCP: Media Gateway Control Protocol.

* LUCENT: Lucent đưa ra giải pháp NGN tập trung chủ yếu vào hai lớp:

1. Lớp lõi ATM/IP và công nghệ truyền dẫn quang tiên tiến DWDM
2. Lớp phân phối dịch vụ

* NEC đưa ra giải pháp chuyển mạch tích hợp IP/ATM/STM với các cổng đa năng.

* SIEMENS đưa ra giải pháp khả thi và khá hoàn chỉnh về cấu trúc mạng NGN, đáp ứng được phần lớn các mục tiêu đặt ra ở mô hình NGN. Giải pháp NGN của SIEMENS có tên gọi là SURPASS. Theo quan điểm của SIEMENS, NGN có cấu trúc phân tán, vì vậy có khả năng điều khiển chuyển mạch NGN, cơ chế truy nhập, cơ chế truyền tải, cơ chế quản lý mạng, cơ chế điều khiển dựa trên hệ thống máy chủ tập trung, cơ chế truy nhập đa dịch vụ, cơ chế truyền tải trên IP/MPLS và giao diện quang, cơ chế điều khiển sử dụng giao thức SNMP (Simple Network Management Protocol) trên nền JAVA/CORBA, với giao diện HTTP để tạo giao diện WEB với người sử dụng.

**Nhận xét:**

- Qua các giải pháp thiết kế của các hãng, nhìn chung chức năng truyền dẫn và chuyển mạch được tích hợp chung trong lớp chuyển tải hay lớp lõi. Như vậy thiết bị truyền dẫn và chuyển mạch được xem như công cụ thực hiện chức năng chuyển tải lưu lượng. Một số hãng gộp chung lớp truy nhập với lớp chuyển tải.

- Các hãng chú ý đến chức năng điều khiển và quản lý. Tính phức hợp giao thức ở lớp này đòi hỏi khả năng tương thích cao giữa các chủng loại thiết bị.

- Chức năng quản lý có xu hướng tập trung cao và xuyên suốt qua các lớp khác nhau trong cấu trúc mạng lưới.

- Vai trò của các thiết bị điều khiển, thiết bị quang và thiết bị truy nhập và các giao thức chuyển gói như IP đóng vài trò quan trọng trong việc hình thành mạng NGN.

- NGN có thể xem như mạng thế hệ kế tiếp, không phải là mạng hoàn toàn mới, vì vậy các hãng đều cân nhắc đến khía cạnh tương thích với mạng và chủng loại thiết bị hiện có.

- Mỗi giải pháp đều có những ưu điểm và hạn chế nhất định. Việc lựa chọn giải pháp tối ưu cần phải căn cứ trên nhiều tiêu chí và cân nhắc về giữa các yêu cầu và mục tiêu có thể mâu thuẫn nhau.

### 6.5.8. Một số dịch vụ NGN

Dịch vụ thoại truyền thống sẽ chuyển dần sang VoIP và được tích hợp trong các dịch vụ mới khác. Các dịch vụ truyền số liệu sẽ được thay thế bởi các dịch vụ mạng riêng ảo VPN. Dịch vụ ISDN sẽ được thay thế bằng các dịch vụ MMA trên nền NGN. Dịch vụ truy cập Internet băng hẹp chuyển sang truy cập băng rộng DSL. Các dịch vụ trên nền WEB và dịch vụ thông minh sẽ được tăng cường phát triển trên cơ sở giao diện phần mềm mở, hướng đến nhà cung cấp dịch vụ thứ ba và khách hàng.

- Dịch vụ thẻ trả trước 1719cho phép sử dụng tài khoản thẻ thực hiện cuộc gọi nội hạt, liên vùng và quốc tê. Khách hàng cũng có thể gán một tài khoản trả trước cho một số điện thoại cố định. Ưu điểm nổi bật của dịch vụ 1719 là khả năng cung cấp dịch vụ với nhiều cấp chất lượng dịch vụ trên cùng một hạ tầng mạng. Khách hàng có thể lựa chọn chất lượng cao như PSTN 64kb/s hoặc giá rẻ như VoIP 8kb/s

- Dịch vụ gọi miễn cước 1800 (Freephone) cho phép thực hiện cuộc gọi miễn cước đến nhiều đích khác nhau thông qua một số truy nhập thống nhất. Khi thuê bao quay số Freephone, số Freephone sẽ được chuyển thành một số đích tương ứng tại chuyển mạch mềm và cuộc gọi sẽ được thiết lập đến đích tương ứng. Đích tương ứng được lựa chọn trên cơ sở vùng của thuê bao chủ gọi, mã số dịch vụ và thời điểm gọi trong ngày.

- Các dịch vụ đa phương tiện MMA là dịch vụ cho phép thực hiện cuộc gọi đa phương tiện tích hợp như thoại, số liệu, hình ảnh… đồng thời. Một số dịch vụ MMA đang được triển khai như: hội nghị truyền hình, đào tạo từ xa, y tế, truyền bản tin video tương tác..

- Các dịch vụ thông minh: Một số dịch vụ thông minh được phát triển trên nền NGN như: chuyển đổi ngôn ngữ, game trực tuyến, truy vấn cơ sở dữ liệu, video theo yêu cầu… Ví dụ 1900 là dịch vụ giải trí, tư vấn có nội dung phụ thuộc vào các phần mềm ứng dụng được xây dựng trên các máy chủ của nhà cung cấp dịch vụ.

- Dịch vụ WEB trên NGN có khả năng cung cấp nhiều loại hình dịch vụ WEBk hác nhau. Một trong các dịch vụ thông dụng đang được triển khai là WEB DIAL PAGE cho phép thực hiện cuộc gọi từ trang WEB, WEB CONFERENCE: điện thoại hội nghị qua WEB.

Dịch vụ truy nhập Internet tốc độ cao cung cấp kết nối Internet băng rộng với công nghệ truy nhập DSL, có các cam kết (SLA) như về tốc độ, băng thông … Dịch vụ này cho phép kết nối máy đơn hoặc mạng máy tính với phương thức cấp địa chỉ IP tĩnh hoặc động tùy theo nhu cầu.

- Dịch vụ mạng riêng ảo VPN cung cấp kết nối mạng LAN/WAN riêng cho khách hàng trên nền hạ tầng mạng công cộng NGN IP/MPLS, có hỗ trợ an ninh mạng và thỏa thuận về cấp độ dịch vụ SLA (Service Layer Agreement). Dịch vụ cung cấp cho khách hàng các tài nguyên mạng, các ứng dụng trong VPN là do khách hàng tự xây dựng.

VPN trên nền NGN có nhiều ưu điểm so với các mạng máy tính khác, có khả năng đảm bảo chất lượng dịch vụQoS, khả năng cung cấp các kết nối linh hoạt có thể thay đổi cấu hình dễ dàng, sử dụng tài nguyên mạng một cách hiệu quả., khả năng mở rộng dịch vụ toàn cầu và không hạn chế băng thông kết nối.

### 6.5.9. NGN trong mạng viễn thông Việt nam

NGN cũng đã được triển khai ở Việt Nam từ năm 2004 theo giải pháp kết hợp: SIEMENS cho lớp điều khiển, JUNIPER cho lớp chuyển tải, ALCATEL cho lớp truy nhập. Trong tương lai, NGN sẽ được phát triển mở rộng trên địa bàn cả nước. Tận dụng năng lực của mạng hiện có, việc chuyển từ mạng viễn thông hiện tại lên mạng thế hệ sau NGN phải trải qua nhiều giai đoạn. từng bước, vẫn phải duy trì hoạt động của các mạng truyền thống. Đồng thời mạng đường trục VNPT sẽ được đầu tư các công nghệ trong NGN. Các mạng truyền thống khác như di động và nội hạt sẽ kết nối với NGN qua thiết bị cổng chuyển đổi. Trong tương lai, các mạng này cũng sẽ được thay thế hoàn toàn bởi công nghệ NGN.

Chức năng các lớp NGN trong mạng viễn thông Việt Nam:

- Lớp quản lý: sẽ hình thành hệ thống quản lý mạng viễn thông tập trung theo mô hình TNM (Telecom Network Management).

- Lớp ứng dụng và dịch vụ mạng: trang bị các server dịch vụ tại hai điểm nút Hà Nội và TP Hồ Chí Minh, cung cấp các dịch vụ mới trên nền NGN như dịch vụ giải trí, truy nhập cơ sở dữ liệu thông tin tự động, điện thoại thẻ giá rẻ, điện thoại miễn cước đường dài, cuộc gọi hội nghị, các dịch vụ trên cơ sở WEB, truy nhập Internet băng rộng qua NGN, cho thuê cơ sở hạ tầng mạng dưới hình thức mạng riêng ảo (VPN) có thương hiệu là MegaWAN…

- Lớp điều khiển: Tổ chức 5 nút điều khiển (chuyển mạch mềm) ứng với 5 vùng lưu lượng theo mô hình hai mặt nghĩa là có dự phòng 1+1

- Lớp truyền tải: Lớp truyền tải NGN dựa trên công nghệ IP/MPLS/SDH/WDM/truyền dẫn quang. Lớp truyền tải được tổ chức thành hai cấp: cấp đường trục quốc gia và cấp vùng. Mạng truyền dẫn quang đường trục quốc gia đạt đến dung lượng 20Gb/s.

- Lớp truy nhập: Tại mỗi vùng đều được trang bị các thiết bị truy nhập cho lưu lượng VoiP qua hệ thống MG và lưu lượng truy nhập internet và mạng riêng ảo qua hệ thống DSLAM với công nghệ ADSL và SHDSL.

## Câu hỏi trắc nghiệm:

1. Hãy chọn câu đúng nhất về DSL:
    A. Công nghệ DSL cho phép tận dụng miền tần số cao truyền tín hiệu tốc độ cao trên đôi dây cáp đồng thông thường.
    B. Công nghệ DSL biến đổi tín hiệu của người sử dụng thành các tín hiệu phù hợp với đường truyền.
    C. Kỹ thuật DSL cho phép truyền chế độ song công đối xứng và bất đối xứng.
2. Họ công nghệ DSL gồm:
    A. IDSL
    B. HDSL
    C. VDSL
    D. ADSL
    E. ROUTER
3. Các phương pháp mã hóa đường truyền
    A. Phương pháp điều chế biên độ và pha triệt sóng mang CAP
    B. Phương pháp đa âm tần rời rạc DMT
    C. Cả hai phương pháp.
4. Nhiễu trong kỹ thuật DSL:
    D. Nhiễu xuyên âm đầu gần NEXT (Near - end Crosstalk)
    E. Nhiễu xuyên âm đầu xa FEXT (Far - end- Crosstalk)
    F. Cả hai phương pháp.
5. Các phương pháp chống nhiễu trong kỹ thuật DSL:
    A. Chống xuyên nhiễu
    B. Phương pháp triệt tiếng vọng (EC)
    C. Cả hai phương pháp.
6. Các mô hình kết nối ADSL
    A. Mô hình PPPoA (Point to Point over ATM)
    B. Mô hình PPPoE (Point to Point over Ethernet) RFC 2516
    C. Mô hình IP over ATM (RFC 1483R)
    D. Mô hình Ethernet over ATM (RFC 1483B)
7. Công nghệ truyền thoại qua mạng chuyển mạch gói:
    A. Tại phía phát, tín hiệu thoại được mã hóa bằng các bộ CODEC (Coder-Decoder). Bộ xử lý tín hiệu số DSP (Digital Signal Processing) sẽ nén các gói dữ liệu/. VAD (Voice Activity Detection) loại bỏ các khoảng lặng
    B. Tại bên thu, ngược lại, DSP sẽ giải nén các gói tin, CODEC giải mã các gói tin thành tín hiệu âm thanh tương tự. Các khoảng lặng được tái tạo để phát thông tin thoại cho người nghe.
    C. Cả hai phương pháp.

8. Các ưu điểm của truyền thoại qua mạng chuyển mạch gói
   A. Tiết kiệm chi phí đầu tư hạ tầng mạng và chi phí sử dụng dịch vụ
   B. Sử dụng hiệu quả băng thông với chất lượng dịch vụ QoS chấp nhận được.
   C. Kết hợp các dịch vụ thoại, số liệu, video trên một mạng duy nhất
9. Các vấn đề về chất lượng dịch vụ QoS
   A. Trễ (Delay)
   B. Trượt (Jitter)
   C. Mất gói (Packet Loss)
10. Các mô hình truyền thoại qua mạng chuyển mạch gói
   A. Voice over Frame Relay - VoFR
   B. Voice over ATM - VoATM
   C. Voice over Internet Protocol - VoIP
11. Cấu trúc mạng MPLS gồm :
   A. Bộ định tuyến biên LER gọi là bộ định tuyến PE
   B. Bộ định tuyến lõi LSR được gọi là bộ định tuyến P
   C. Cả hai phương pháp.
12. Ưu điểm của công nghệ MPLS:
   A. Công nghệ MPLS đơn giản, có thể giải quyết các vấn đề phức tạp và khả năng mở rộng mạng.
   B. Có thể thay thế công nghệ Frame Relay, ATM.
   C. MPLS hội tụ những ưu điểm của cơ chế định tuyến IP và cơ chế hoán đổi nhãn của ATM
   D. Giảm thiểu thời gian xử lý gói tin, không thay đổi các giao thức định tuyến IP.
   E. Nhãn MPLS đơn giản, kích thước nhỏ và linh hoạt. Có thể xếp nối tiếp nhãn thành chồng nhãn. Rất tiện lợi cho việc đánh địa chỉ và truy tìm.
13. Hạn chế của MPLS:
   A. MPLS không cung cấp dịch vụ đầu cuối (End-Point)
   B. MPLS bị lỗi đường truyền cao hơn các công nghệ khác, giảm đi độ tin cậy.
   C. Cả 2 khẳng định.
14. Các đặc trưng cơ bản của công nghệ chuyển mạch mềm như sau:
   A. Dựa trên công nghệ chuyển mạch gói, thiết kế theo mô hình xử lý phân tán
   B. Giao diện mở API
   C. Phần mềm không phụ thuộc vào phần cứng chuyển mạch
   D. Có khả năng lập trình được độc lập.
   E. Tích hợp và liên kết các giao thức khác nhau trong mạng NGN và giữa NGN với mạng truyền thống (PSTN, ATM&IP…).
15. API trong Softswitch gồm:
   A. API liên kết các nguồn tài nguyên mạng.
   B. API liên kết các module có năng lực xử lý trong mạng
   C. API liên kết NGN với môi trường ngoài

16. Công nghệ chuyển mạch mềm có những ưu điểm:
    A. Giải pháp phần mềm chung trên nhiều loại mạng khác nhau.
    B. Đơn giản cấu trúc hệ thống và linh hoạt khi thay đổi tính năng, cấu hình, mở rộng phát triển.
    C. Tích hợp và phát triển các phần mềm thông minh, khai thác tiềm năng của mạng trong tương lai.
    D. Dễ dàng tích hợp dịch vụ mới từ nhà cung cấp thứ ba đồng thời cho phép người sử dụng có thể tự phát triển ứng dụng và dịch vụ.

## Câu hỏi và bài tập

1. Tổng quan về IDSL (ISDN DSL):
2. Tổng quan về HDSL (High Data Rate DSL):
3. Tổng quan về VDSL (Very High Data Rate DSL):
4. Tổng quan về ADSL (Asymmetric Digital Subscriber Line)
5. Tổng quan về ADSL2 và ADSL2+
6. Các vấn đề cơ bản công nghệ DSL trên mạng cáp đồng
7. Các phương pháp mã hóa đường truyền
8. Kỹ thuật phát hiện lỗi và sửa lỗi
9. Nhiễu xuyên âm đầu xa FEXT (Far - end Crosstalk)
10. Nhiễu xuyên âm đầu gần
11. Chống xuyên nhiễu
12. Phương pháp triệt tiếng vọng (EC)
13. Mô hình PPPoA (Point to Point over ATM)
14. Mô hình PPPoE (Point to Point over Ethernet) RFC 2516
15. Mô hình IP over ATM (RFC 1483R)
16. Mô hình Ethernet over ATM (RFC 1483B)
17. Truyền thoại qua mạng chuyển mạch gói VoPN (Voice over Packet Network)
18. Mô hình truyền thoại qua mạng chuyển mạch gói
19. Ưu điểm của truyền thoại qua mạng chuyển mạch gói
20. Các vấn đề về chất lượng dịch vụ QoS: Trễ , Trượt và mất gói
21. Voice over Frame Relay VoFR
22. Voice over ATM - VoATM
23. Voice over Internet Protocol - VoIP
24. Các thành phần chủ yếu của VoIP: Internet Protocol IP: Các chuẩn nén tín hiệu thoại
25. H.320, H.324 và POTS (Plain Old Telephone Service)
26. Vai trò, chức năng và các thành phần giao thức H.323
27. Giao thức SIP (Session Initial Protocol)
28. Real-time Transport Protocol RTP

29. Real-time Transport Control Protocol RTCP:
30. Resource Reservation Protocol RSVP
31. Giao thức MGCP (Media Gateway Control Protocol)
32. Giao thức Megaco/H.248
33. Kiến trúc và nguyên tắc hoạt động MPLS
34. Cấu trúc mạng MPLS
35. Nguyên tắc chuyển mạch nhãn MPLS
36. Cơ chế phân phối nhãn. Cơ chế xử lý nhãn và chuyển gói tin
37. Cơ chế điều khiển lưu lượng và chất lượng dịch vụ trong MPLS
38. Đánh giá công nghệ chuyển mạch nhãn đa giao thức MPLS:
39. So sánh MPLS với ATM. So sánh MPLS so với IP
40. Hạn chế của MPLS:
41. Cấu trúc và nguyên tắc chuyển mạch mềm
42. MEGACO/H.248/MGCP
43. RTP/RTCP/RTSP: Real Time Protocol/ Real Time Control Protocol-Real Time Streaming Protocol:
44. SCTP (Stream Control Transport Protocol) hay SIGTRAN (Signalling Transport)
45. SIP (Session Initiation Protocol)/H.323
46. Giao diện ứng dụng API trong chuyển mạch mềm
47. Các phương thức chia sẻ dữ liệu qua API:
48. Phân lớp các API trong Softswitch
49. Kế hoạch đánh số trong chuyển mạch mềm
50. Đánh giá công nghệ chuyển mạch mềm
51. So sánh công nghệ Softwwitch và chuyển mạch kênh.
52. Công nghệ chuyển mạch mềm có những ưu điểm nổi bật so với các công nghệ truyền thông khác.
53. Mạng hội tụ và mạng thế hệ sau NGN
54. Các nguyên tắc xây dựng mạng thế hệ sau NGN
55. NGN hội tụ những ưu điểm của công nghệ chuyển mạch kênh và chuyển mạch gói
56. Mô hình phân lớp và chức năng các lớp NGN
57. Vai trò và chức năng Lớp truy nhập (Access)
58. Vai trò và chức năng Lớp truyền tải (Transport)
59. Vai trò và chức năng Lớp ứng dụng/dịch vụ (Application/Service)
60. Vai trò và chức năng Lớp quản lý (Management)
61. Dịch vụ thẻ trả trước 1719, Dịch vụ gọi miễn cước 1800 (Freephone), Các dịch vụ đa phương tiện MMA, Các dịch vụ thông minh, Dịch vụ WEB trên NGN, Dịch vụ truy nhập Internet tốc độ cao, Dịch vụ mạng riêng ảo VPN,
62. NGN trong mạng viễn thông Việt Nam

# CHƯƠNG 7: AN TOÀN MẠNG

Nội dung của chương này sẽ trình bày những vấn đề cơ bản về an toàn mạng bao gồm các đặc trưng kỹ thuật, các lỗ hổng và điểm yếu của mạng. Nghiên cứu các phương thức tấn công mạng phổ biến, các biện pháp an toàn mạng bằng kỹ thuật mật mã và Fire wall. Đặc biệt nội dung nghiên cứu mạng riêng ảo và vấn đề bảo mật trong mạng riêng ảo, các giao thức đặc trưng IPSEC, PPP, L2TP. Nội dung chương gồm các phần sau:

- Tổng quan về an ninh mạng.
- Một số kiểu tấn công mạng phổ biến.
- Biện pháp đảm bảo an ninh mạng
- Mạng riêng ảo

## 7.1. Tổng quan về an ninh mạng

### 7.1.1. An toàn mạng là gì?

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 toàn 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 và với chỉ những người có thẩm quyền tương ứng.

An toàn 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.

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...Khi đánh giá được hết những nguy cơ ảnh hưởng tới an ninh mạng thì mới có thể có được những biện pháp tốt nhất để đảm bảo an ninh mạng.

Sử dụng hiệu quả các công cụ bảo mật (ví dụ như Firewall ...) và những biện pháp, chính sách cụ thể chặt chẽ.

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.

### 7.1.2. Các đặc trưng kỹ thuật của an toàn mạng

**1. 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 thông thường phải thực hiện kiểm tra tính xác thực của một thực thể trước khi thực thể đó thực hiện kết nối với hệ thống. Cơ chế kiểm tra tính xác thực của các phương thức bảo mật dựa vào 3 mô hình chính sau:

- Đối tượng cần kiểm tra cần phải cung cấp 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 ...

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...).

**2. 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 khi nào, trong hoàn cảnh nào. Tính khả dụng nói chung dùng tỷ lệ giữa thời gian hệ thống được sử dụng bình thường với thời gian quá trình hoạt động để đánh giá. 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).

**3. 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).

**4. Tính toàn vẹn (Integrity):** Là đặc tính khi thông tin trên mạng chưa được uỷ quyền thì không thể tiến hành biến đổi được, tức 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…

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

- Giao thức an toàn có thể kiểm tra thông tin bị sao chép, sửa đổi hay sao chép. Nừu 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 cản trở truyền tin.
- Chữ ký điện tử: bảo đảm tính xác thực của thông tin.
- Yêu cầu cơ quan quản lý hoặc trung gian chứng minh tính chân thực của thông tin.

**5. Tính khống chế (Accountlability):** Là đặc tính về năng lực khống chế truyền bá và nội dung vốn có của tin tức trên mạng.

**6. 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.

### 7.1.3. Các lỗ hổng và điểm yếu của mạng

**1. Các lỗ hổng bảo mật hệ thống** là các điểm yếu có thể tạo ra sự ngưng trệ của dịch vụ, thêm quyền đối với người sử dụng hoặc cho phép các truy nhập không hợp pháp vào hệ thống. Các lỗ hổng tồn tại trong các dịch vụ như Sendmail, Web,Ftp ... và trong hệ điều hành mạng như trong Windows NT, Windows 95, UNIX; hoặc trong các ứng dụng. Các loại lỗ hổng bảo mật trên một hệ thống được chia như sau:

*Lỗ hổng loại C:* 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 ngưng trệ, gián đoạn hệ thống, không phá hỏng dữ liệu hoặc chiếm quyền truy nhập.

*Lổ hổng loại B*: 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.

**2. 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.

### 7.1.4. Các biện pháp phát hiện hệ thống bị tấn công

Không có một hệ thống nào có thể 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 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 cụ thể:

1. Kiểm tra các dấu hiệu hệ thống bị tấn công: Hệ thống thường bị treo hoặc bị Crash bằng những thông báo lỗi không rõ ràng. Khó xác định nguyên nhân do thiếu thông tin liên quan. Trước tiên, xác định các nguyên nhân có phải phần cứng hay không, nếu không phải hãy nghĩ đến khả năng máy bị tấn công.

2. Kiểm tra các tài khoản người dùng mới lạ, nhất là ID của tài khoản đó bằng không.

3. Kiểm tra sự xuất hiện các tập tin lạ. Người quản trị hệ thống nên có thói quen đặt tên tập theo mẫu nhất định để dễ dàng phát hiện tập tin lạ. Dùng các lệnh Ls-l để kiểm tra thuộc tính Setuid và Setgid đối với những tập tinh đáng chú ý, đặc biệt là các tập tin Scripts.

4. Kiểm tra thời gian thay đổi trên hệ thống, đặc biệt là các chương trình Login, Sh hoặc các Scripts khởi động ...

5. Kiểm tra hiệu năng của hệ thống: Sử dụng các tiện ích theo dõi tài nguyên và các tiến trình đang hoạt động trên hệ thống như Ps hoặc Top ...

6. Kiểm tra hoạt động của các dịch vụ hệ thống cung cấp: Một trong các mục đích tấn công là làm cho tê liệt hệ thống (hình thức tấn công DoS). Sử dụng các lệnh như Ps, Pstat, các tiện ích về mạng để phát hiện nguyên nhân trên hệ thống.

7. Kiểm tra truy nhập hệ thống bằng các Account thông thường, đề phòng trường hợp các Âccount này bị truy nhập trái phép và thay đổi quyền hạn mà người sử dụng hợp pháp không kiểm soát được.

9. Kiểm tra các file liên quan đến cấu hình mạng và dịch vụ như /etc/inetd.conf; bỏ các dịch vụ không cần thiết; đối với những dịch vụ không cần thiết chạy dưới quyền Root thì không chạy bằng các quyền yếu hơn; ví dụ Fingerd chỉ chạy với quyền Nobody.

10. Kiểm tra các phiên bản của Sendmail, /bin/mail, ftp, fingerd; tham gia các nhóm tin về bảo mật để có thông tin về lỗ hổng của dịch vụ sử dụng

Các biện pháp này kết hợp với nhau tạo nên một chính sách về bảo mật đối với hệ thống. Chi tiết về phương thức và kế hoạch xây dựng một chính sách bảo mật sẽ được trình bày trong phần ba - xây dựng chính sách bảo mật.

## 7.2. Một số phương thức tấn công mạng phổ biến

### 7.2.1. Scanner

Kẻ phá hoạt sử dụng chương trình Scanner tự động rà soát và có thể phát hiện ra những điểm yếu lỗ hổng về bảo mật trên một Server ở xa Scanner là một chương trình trên một trạm làm việc tại cục bộ hoặc trên một trạm ở xa.

Các chương trình Scanner có thể rà soát và phát hiện các số hiệu cổng (Port) sử dụng trong giao thức TCP/UDP của 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 tim 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. Những thông tin này là hết sức hữu ích và cần thiết đối với người quản trị mạng, nhưng hết sức nguy hiểm khi những kẻ phá hoại có thông tin này.

### 7.2.2. Bẻ khoá (Password Cracker)

Chương trinh bẻ khoá Password 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. Hầu hết việc mã hoá các mật khẩu được tạo ra từ một phương thức mã hoá. Các chương trình mã hoá sử dụng các thuật toán mã hoá để mã hoá mật khẩu.Có thể thay thế phá khoá trên một hệ thống phần tán, đơn giản hơn so với việc phá khoá trên một Server cục bộ.

Một danh sách các từ được tạo ra và thực hiện mã hoá từng từ. Sau mỗi lần mã hoá, sẽ so sánh với mật khẩu (Password) đã mã hoá cần phá. Nếu không trùng hợp, quá trình lại quay lại. Phương thức bẻ khoá này gọi là Bruce-Force. Phương pháp này tuy không chuẩn tắc nhưng thực hiện nhanh vì dựa vào nguyên tắc khi đặt mật khẩu người sử dụng cũng thương tuân theo một số qui tắc để thuận tiện khi sử dụng.

Thông thường các chương trình phá khoá thường kết hợp một số thông tin khác trong quá trình dò mật khẩu như: thông tin trong tập tin /etc/passwd, từ điển và sử dụng các từ lặp các từ liệt kê tuần tự, chuyển đổi cách phát âm của một từ ...

Biện pháp khắc phục là cần xây dựng một chính sách bảo vệ mật khẩu đúng đắn.

### 7.2.3. Trojans

Một chương trình Trojan chạy không hợp lệ trên một hệ thống với vai trò như một chương trình hợp pháp. Nó thực 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. Virus là một loại điển hình của các chương trình Trojans, vì các chương trình virus che dấu các đoạn mã trong những chương trình sử dụng hợp pháp. Khi chương trình hoạt động thì những đoạn mã ẩn sẽ thực hiện 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 chỉ mục cho file trong thưc mục, hoặc một đoạn mã phá khoá, hoặc cố thể là một chương trình xử lý văn bản hoặc một tiện ích mạng...

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. Hầu hết các chương trình FTP Server đang sử dụng là những phiên bản cũ, có nguy cơ tiềm tàng lây lan Trojans.

Đánh giá mức độ phá hoại của Trojans là hết sức khó khăn. Trong một số trường hợp, nó chỉ làm ảnh hương đến các truy nhập của ngwòi sử dụng. Nghiêm trọng hơn, nó là những kẻ tán công lỗ hổng bảo mật mạng. Khi kẻ tấn công chiếm được quyền Root trên hệ thống, nó có thể phá

huỷ toàn bộ hoặc một phần của hệ thống. Chúng sử dụng các quyền Root để thay đổi logfile, cài đặt các chương trình Trojans khác mà người quản trị không thể phát hiện được và người quản trị hệ thống đó chỉ còn cách là cài đặt lại toàn bộ hệ thống

### 7.2.4. Sniffer

Sniffer theo nghĩa đen là ”đánh hơi” hoặc ”ngửi”. 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. 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. Các chương trình Sniffer hoặc các thiết bị Sniffer có thể ”ngửi” các giao thức TCP, UDP, IPX .. ở tầng mạng. Vì vậy nó có thể tóm bắt các gói tin IP Datagram và Ethernet Packet. 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 "tóm bắt" các gói tin tại đây.

## 7.3. 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.

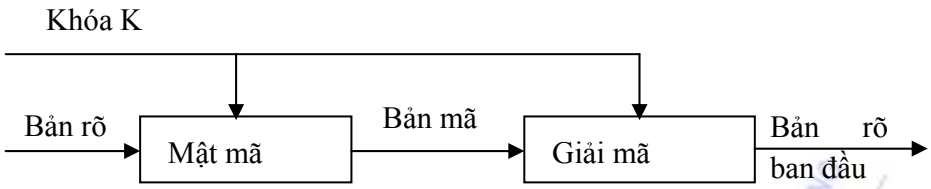
### 7.3.1. Tổng quan về bảo vệ thông tin bằng mật mã (Cryptography)

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) và từ mút-đến-mút (End-to-End).

Trong cách thứ nhất, 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 của cách này 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.

Ngược lại, trong cách thứ hai, 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 của tiếp cận này là người sử dụng có thể dùng nó mà không ảnh hưởng gì đến người sử dụng khác. Nhược điểm của phương pháp 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.

Giải thuật DES mã hoá các khối 64 bits của văn bản gốc thành 64 bits văn bản mật bằng một khoá. Khoá gồm 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 phải trải qua 3 quá trình xử lý: Hoán vị khởi đầu, tính toán phụ thuộc khoá và hoán vị đảo ngược hoán vị khởi đầu.




**Hình 7.1: Mô hình mật mã đối xứng**

Phương pháp sử dụng 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 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 mã bí mật để giải mã. Mặc dù hai khoá này thực hiện các thao tác ngược nhau nhưng không thể suy ra khoá bí mật từ khoá công khai và ngược lại nhờ các hàm toán học đặc biệt gọi là các hàm sập bẫy một chiều (trap door one-way functions). Đặc điểm các hàm này là phải biết được cách xây dựng hàm thì mới có thể suy ra được nghịch đảo của nó.

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. Vì vậy, tích của 2 số nguyên tố có thể công khai, còn 2 số nguyên tố lớn có thể dùng để tạo khoá giải mã mà không sợ bị mất an toàn. Trong giải thuật RSA mỗi trạm 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).


**Hình 7.2: Mô hình mật mã không đối xứng**

### 7.3.2. Firewall

Firewall là một hệ thống dùng để tăng cường khống chế truy xuất, phòng ngừa đột nhập bên ngoài vào hệ thống sử dụng tài nguyên của mạng một cách phi pháp. Tất cả thông tin đến và đi nhất thiết phải đi qua Firewall và chịu sự kiểm tra của bức tường lửa. Nói chung Firewall có 5 chức năng lớn sau:

1. Lọc gói dữ liệu đi vào/ra mạng lưới.
2. Quản lý hành vi khai thác đi vào/ra mạng lưới
3. Ngăn chặn một hành vi nào đó.

4. Ghi chép nội dung tin tức và hoạt động thông qua bức tường lửa.
5. Tiến hành đo thử giám sát và cảnh báo sự tấn công đối với mạng lưới.

Ưu điểm và nhược điểm của bức tường lửa:

**Ưu điểm** chủ yếu của việc sử dụng Firewall để 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 mạng được củng cố trên hệ thống Firewall mà không phải phân bố trên tất cả máy 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 bảo. Tính an toàn tập trung. Firewall có thể giảm đi vấn đề không gian địa chỉ và 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.

**Nhược điểm** là 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 chăn sự tấn công thông qua những con đường khác ngoài bức tường lửa. Firewall Internet không thể hoàn toàn phòng ngừa được sự phát tán phần mềm hoặc tệp đã nhiễm virus.

### 7.3.3. Các loại Firewall

Firewall lọc gói thường là một bộ định tuyến có lọc. Khi nhận một gói dữ liệu, nó quyết định cho phép qua hoặc từ chối bằng cách thẩm tra gói tin để xác định quy tắc lọc gói dựa vào các thông tin của Header để đảm bảo quá trình chuyển phát IP.

Firewall cổng mạng hai ngăn là loại Firewall có hai cửa nối đến mạng khác. Ví dụ một cửa nối tới một mạng bên ngoài không tín nhiệm còn một cửa nối tới một mạng nội bộ có thể tín nhiệm. Đặc điểm lớn nhất Firewall loại này là gói tin IP bị chặn lại.

Firewall che chắn (Screening) máy chủ bắt buộc có sự kết nối tới tất cả máy chủ bên ngoài với máy chủ kiên cố, không cho phép kết nối trực tiếp với máy chủ nội bộ. Firewall che chắn máy chủ là do bộ định tuyến lọc gói và máy chủ kiên cố hợp thành. 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).

Firewall che chắn mạng con: Hệ thống Firewall che chắn mạng con dùng hai bộ định tuyến lọc gói và một máy chủ kiên cố, cho phép thiết lập hệ thống Firewall an toàn nhất, vì nó đảm bảo chức năng an toàn tầng mạng và tầng ứng dụng.

### 7.3.4. Kỹ thuật Fire wall

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

Lọc gói (Packet Filtering): Kiểu Firewall chung nhất là kiểu dựa trên tầng mạng của mô hình OSI. Lọc gói cho phép hay từ chối gói tin mà nó nhận được. 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.

Nếu quy tắc lọc Packet được thoả mãn thì gói tin được chuyển qua Firewall. Nếu không sẽ bị bỏ đi. Như vậy Firewall có thể ngăn cản các kết nối vào hệ thống, hoặc khoá việc truy cập vào hệ thống mạng nội bộ từ những địa chỉ không cho phép.

Một số Firewall hoạt động ở tầng mạng (tương tự như một Router) thường cho phép tốc độ xử lý nhanh vì chỉ kiểm tra địa chỉ IP nguồn mà không thực hiện lệnh trên Router, không xác định địa chỉ sai hay bị cấm. 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 ...

Firewall kiểu Packet Filtering có 2 loại:

**a. Packet filtering Fire wall:** Hoạt động tại tầng mạng của mô hình OSI hay tầng IP trong mô hình TCP/IP. Kiểu Firewall này không quản lý được các giao dịch trên mạng.

**b. Circuit Level Gateway:** Hoạt động tại tầng phiên (Session) của mô hình OSI hay tầng TCP trong mô hình TCP/IP. Là loại Firewall xử lý bảo mật giao dịch giữa hệ thống và người dùng cuối (VD: kiểm tra ID, mật khẩu...) loại Firewall cho phép lưu vết trạng thái của người truy nhập.

### 7.3.5. Kỹ thuật Proxy

Là hệ thống Firewall thực hiện các kết nối thay cho các kết nối trực tiếp từ máy khách yêu cầu.Proxy hoạt động dựa trên phần mềm. Khi một kết nối từ 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 hai node với nhau. Ưu điểm của kiểu Firewall loại này là không có chức năng 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).

## 7.4. Mạng riêng ảo VPN (Virtual Private Networks)

### 7.4.1. 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 lôgích 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. Có 2 dạng chính mạng riêng ảo VPN là: Remote Access VPN , Site - to - Site VPN (Intranet VPN và Extranet VPN).

*Remote Access VPN (Client - to - LAN 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 loại này ra 2 loại khác: Intranet VPN và Extranet VPN. 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.

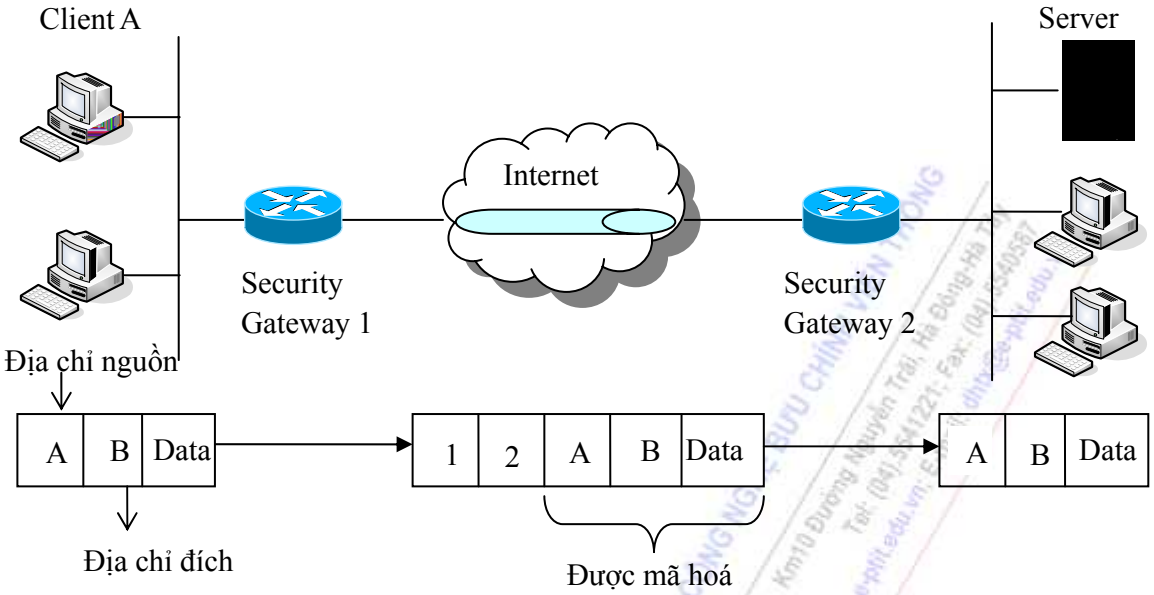
Bảo mật là một yếu tố quan trọng bảo đảm cho VPN hoạt động an toàn và hiệu quả. Kết hợp với các thủ tục xác thực người dùng, dữ liệu được bảo mật thông qua các kết nối đường hầm (Tunnel) được tạo ra trước khi truyền dữ liệu. Tunnel là kết nối ảo điểm - điểm (Point to Point) và làm cho mạng VPN hoạt động 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.

Chất lượng dịch vụ QoS, các thoả thuận (Service Level Agreement-SLA) với các ISP liên quan đến độ trễ trung bình của gói trên mạng, hoặc kèm theo chỉ định về giới hạn dưới của băng thông. Bảo đảm cho QoS là một việc cần được thống nhất về phương diện quản lý đối với các ISP. Tất cả các giao thức sử dụng trong mạng VPN, các gói dữ liệu IP được mã hoá (RSA RC-4 trong PPTP hoặc mã khóa công khai khác trong L2TP, IPSec) và sau đó đóng gói (ESP), thêm tiêu đề IP mới để tạo đường hầm trên mạng IP công cộng. Như vậy, khi gói tin MTU bị thất lạc trên mạng IP công cộng thì thông tin trong đó đã được mã hoá nên kẻ phá hoại khó có thể dò tìm thông tin thực sự chứa trong bản tin. Trong các giao thức PPTP và L2TP, mã hoá gói tin đã được thực hiện từ người dùng cho đến máy chủ của VPN. Việc mất mát gói tin dẫn đến việc phải truyền lại toàn bộ gói tin, điều này gây nên độ trễ chung đối với VPN và ảnh hưởng đến QoS của mạng VPN.

### 7.4.2. Kiến trúc của mạng riêng ảo

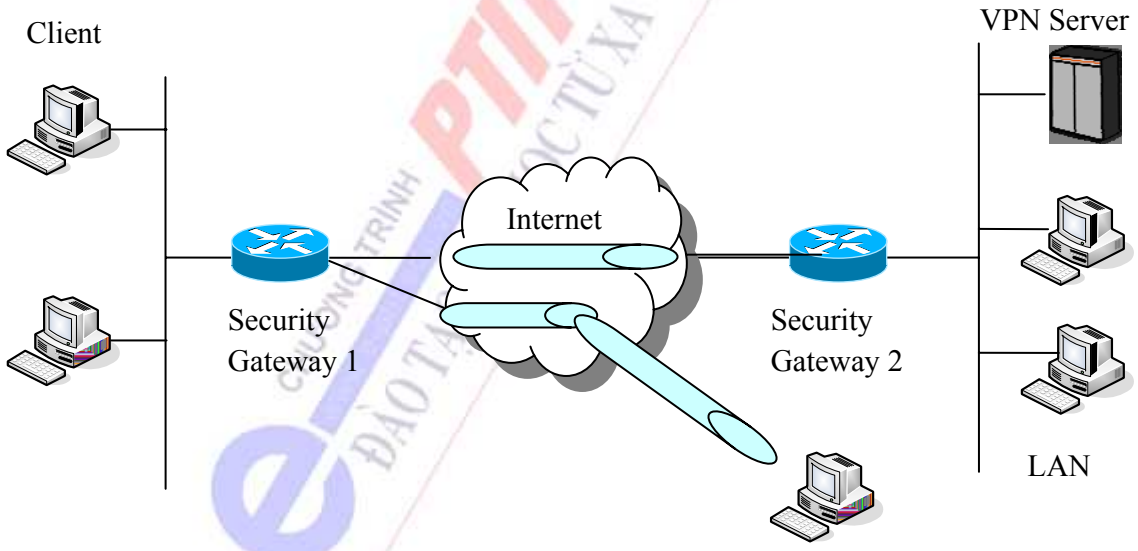
Hai thành phần cơ bản của Internet tạo nên mạng riêng ảo VPN, đó là:

- 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.




**Hình 7.3: Cấu trúc một đường hầm**

*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 lôgích "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.




**Hình 7.4: Đường hầm trong các cấu trúc LAN và Client.**

*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, cổng

Định 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.

### 7.4.3. 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.

*Tính bảo mật*: Trong VPN sử dụng cơ chế đường hầm (Tunnelling) và các giao thức tầng 2 và tầng 3, xác thực người dùng, kiểm soát truy nhập, bảo mật dữ liệu bằng mã hoá, vì vậy VPN có tính bảo mật cao, giảm thiểu khả năng tấn công, thất thoát dữ liệu.

*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.

### 7.4.4. 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.

### 7.4.5. Giao thức L2F (Layer Two Forwarding Protocol)

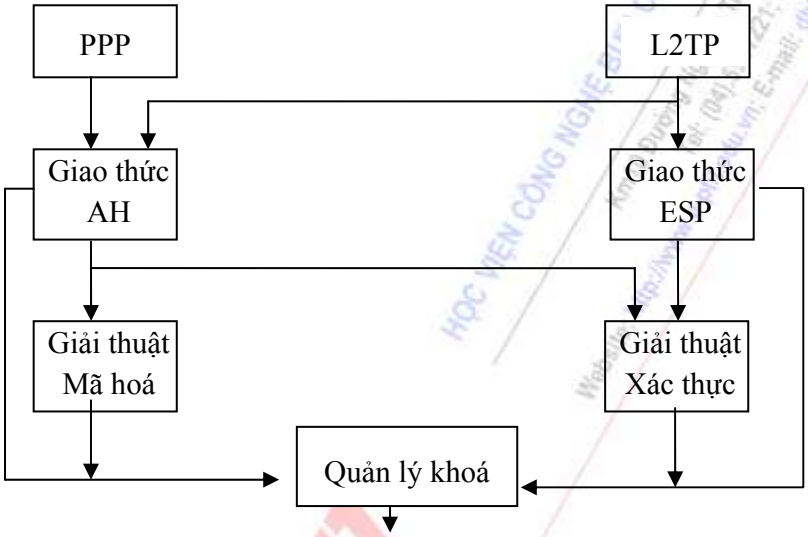
Giao thức L2FP do hãng Cisco phát triển, dùng để truyền các khung SLIP/PPP qua Internet. L2F hoạt động ở tầng 2 (Data Link) trong mô hình OSI. Cũng như PPTP, L2F được thiết kế như là một giao thức Tunnel, sử dụng các định nghĩa đóng gói dữ liệu riêng của nó để truyền các gói tin ở mức 2. Một sự khác nhau giữa PPTP và L2F là tạo Tunnel trong giao thức L2F không phụ thuộc vào IP và GRE, điều này cho phép nó làm việc với các môi trường vật lý khác nhau.

Cũng như PPTP, L2F sử dụng chức năng của PPP để cung cấp một kết nối truy cập từ xa và kết nối này có thể được đi qua một tunnel thông qua Internet để tới đích. Tuy nhiên L2TP định nghĩa giao thức tạo tunnel riêng của nó, dựa trên cơ cấu của L2F. Cơ cấu này tiếp tục định nghĩa việc truyền L2TP qua các mạng chuyển mạch gói như X25, Frame Relay và ATM. Mặc dù nhiều

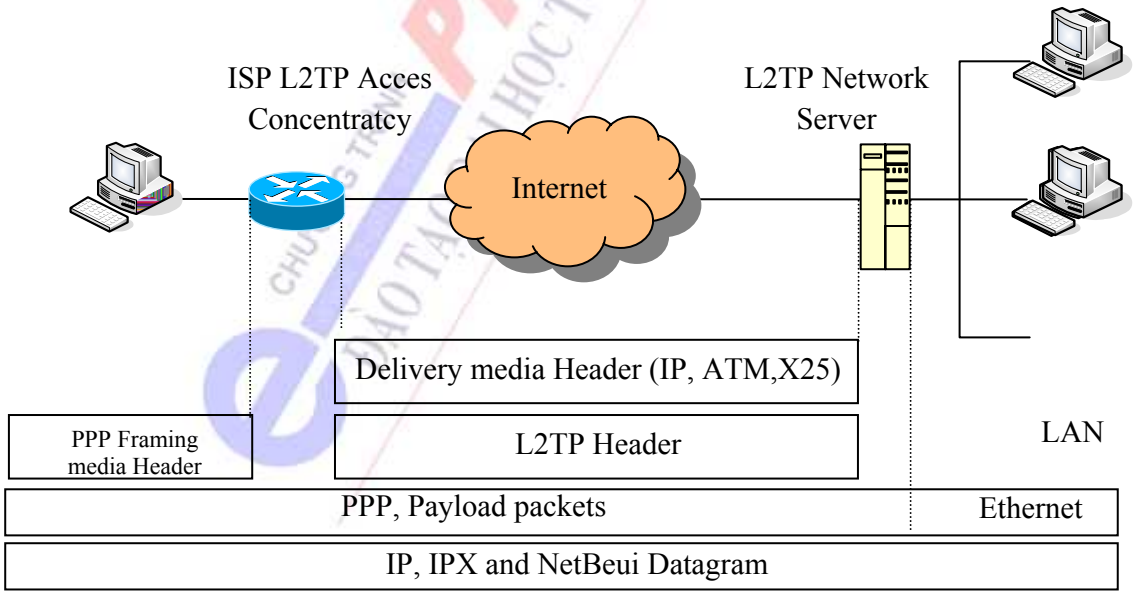
cách thực hiện L2TP tập trung vào việc sử dụng giao thức UDP trên mạng IP, ta vẫn có khả năng thiết lập một hệ thống L2TP không sử dụng IP. Một mạng sử dụng ATM hoặc Frame Relay cũng có thể được triển khai cho các tunnel L2TP.

### 7.4.6. Giao thức L2TP (Layer Two Tunnelling Protocol)

Giao thức L2TP được sử dụng để xác thực người sử dụng Dial-up và Tunnel các kết nối SLIP/PPP qua Internet. Vì L2TP là giao thức lớp 2, nên hỗ trợ cho người sử dụng các khả năng mềm dẻo như PPTP trong việc truyền tải các giao thức không phải là IP, ví dụ như là IPX và NETBEUI.




**Hình 7.5: Kiến trúc của L2TP.**




**Hình 7.6: Quá trình chuyển gói tin qua Tunnel L2TP**

*Bảo mật trong L2TP:* Việc xác thực người dùng trong 3 giai đoạn: Giai đoạn 1 tại ISP, giai đoạn 2 và giai đoạn 3 (tuỳ chọn) tại máy chủ mạng riêng. Trong giai đoạn 1, ISP có thể sử dụng số điện thoại của người dùng hoặc tên người dùng để xác định dịch vụ L2TP và khởi tạo kết nối đường hầm đến máy chủ của VPN. Khi đường hầm được thiết lập, LAC của ISP chỉ định một số nhận dạng cuộc gọi (Call ID) mới để định danh cho kết nối trong đường hầm và khởi tạo phiên làm việc bằng cách chuyển thông tin xác thực cho máy chủ VPN. Máy chủ VPN tiến hành tiếp bước 2 là quyết định chấp nhận hay từ chối cuộc gọi dựa vào các thông tin xác thực từ cuộc gọi của ISP chuyển đến. Thông tin đó có thể mang CHAP, PAP, EAP hay bất cứ thông tin xác thực nào. Sau khi cuộc gọi được chấp nhận, máy chủ VPN có thể khởi động giai đoạn 3 tại lớp PPP, bước náy tương tự như máy chủ xác thực một người dùng quay số truy nhập vào thăngr máy chủ.

Việc sử dụng các giao thức xác thực đơn giản nhưng không bảo mật cho các luồng dữ liệu điều khiển và thông báo dữ liệu tạo kẽ hở cho việc chèn gói dữ liệu để chiếm quyền điều khiển đường hầm, hay kết nối PPP, hoạc phá vỡ việc đàm phán PPP, lấy cắp mật khẩu người dùng. Mã hoá PPP không có xác thực địa chỉ, toàn vẹn dữ liệu, quản lý khoá nên bảo mật này yếu không an toàn trong kênh L2TP. Vì vậy, để có được xác thực như mong muốn, cần phải phân phối khoá và có giao thức quản lý khoá. Về mã hoá, sử dụng IPSec cung cấp bảo mật cao để bảo vệ gói mức IP, tối thiểu cũng phải được thực hiện cho L2TP trên IP. Việc quản lý khoá được thực hiện thông qua liên kết bảo mật - Security Association( SA). SA giúp 2 đối tượng truyền thông xác định phương thức mã hoá, nhưng việc chuyển giao khoá lại do IKE thực hiện. Nội dung này sẽ được nói rõ hơn trong giao thức IPSec.

### 7.4.7. 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. Trong khi đó 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.

*** Xác thực tiêu đề AH:** AH một trong những giao thức bảo mật IPsec đảm bảo tính toàn vẹn cho tiêu đề gói và dữ liệu cũng như việc chứng thực người sử dụng. Nó đảm bảo chống phát lại và chống xâm nhập trái phép như một tùy chọn. Trong những phiên bản đầu của IPsec đóng gói bảo mật tải ESP chỉ thực hiện mã hóa mà không có chứng thực nên AH và ESP được dùng kết hợp còn ở những phiên bản sau ESP đã có thêm khả năng chứng thực. Tuy nhiên AH vẫn được dùng do đảm bảo việc chứng thực cho toàn bộ tiêu đề và dữ liệu cũng như việc đơn giản hơn đối với truyền tải dữ liệu trên mạng IP chỉ yêu cầu chứng thực.

AH có hai chế độ: Transport và Tunnel. Chế độ Tunnel AH tạo ra tiêu đề IP cho mỗi gói còn ở chế độ Transport AH không tạo ra tiêu đề IP mới. Hai chế độ AH luôn đảm bảo tính toàn vẹn (Integrity), chứng thực (Authentication) cho toàn bộ gói.

*** Xử lý đảm bảo tính toàn vẹn:** IPsec dùng thuật toán mã chứng thực thông báo băm HMAC (Hash Message Authentication Code) thường là HMAC-MD5 hay HMAC-SHA-1. Nơi

phát giá trị băm được đưa vào gói và gửi cho nơi nhận. Nơi nhận sẽ tái tạo giá trị băm bằng khóa chia sẻ và kiểm tra sự trùng khớp giá trị băm qua đó đảm bảo tính toàn vẹn của gói dữ liệu. Tuy nhiên IPsec không bảo vệ tính toàn vẹn cho tất cả các trường trong tiêu đề của IP. Một số trường trong tiêu đề IP như TTL (Time to Live) và trường kiểm tra tiêu đề IP có thể thay đổi trong quá trình truyền. Nếu thực hiện tính giá trị băm cho tất cả các trường của tiêu đề IP thì những trường đã nêu ở trên sẽ bị thay đổi khi chuyển tiếp và tại nơi nhận giá trị băm sẽ bị sai khác. Để giải quyết vấn đề này giá trị băm sẽ không tính đến những trường của tiêu đề IP có thể thay đổi hợp pháp trong quá trình truyền.

*** ESP cũng có hai chế độ:** Transport và Tunnel. Chế độ Tunnel ESP tạo tiêu đề IP mới cho mỗi gói. Chế độ này có thể mã hóa và đảm bảo tính toàn vẹn của dữ liệu hay chỉ thực hiện mã hóa toàn bộ gói IP gốc. Việc mã hóa toàn bộ gói IP (gồm cả tiêu đề IP và tải IP) giúp che được địa chỉ cho gói IP gốc. Chế độ Transport ESP dùng lai tiêu đề của gói IP gốc chỉ mã hóa và đảm bảo tính toàn vẹn cho tải của gói IP gốc. Cả hai chế độ chứng thực để đảm bảo tính toàn vẹn được lưu ở trường ESP Auth.

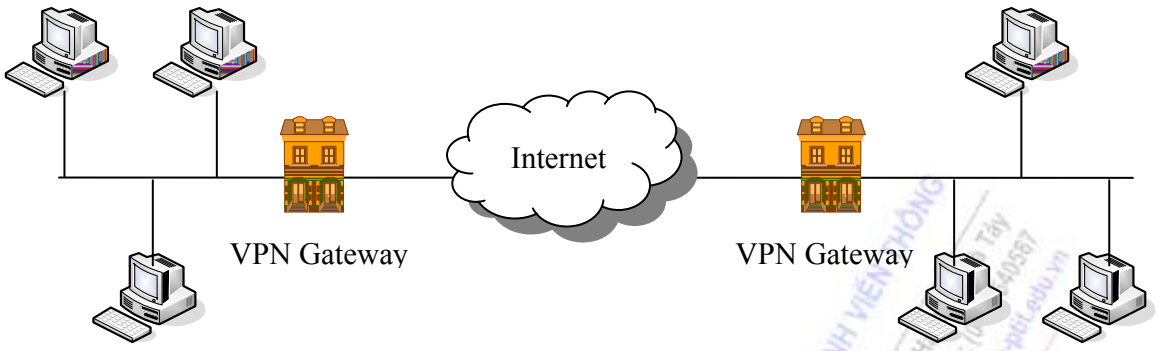
*** Xử lý mã hóa:** ESP dùng hệ mật đối xứng để mã hóa gói dữ liệu, nghĩa là thu và phát đều dùng cùng một loại khóa để mã hóa và giải mã dữ liệu. ESP thường dùng loại mã khối AES-CBC (AES-Cipher Block Chaining), AES-CTR (AES Counter Mode) và 3DES

*** Trao đổi khóa mã hóa IKE (Internet Key Exchange):** Trong truyền thông sử dụng giao thức IPsec phải có sự trao đổi khóa giữa hai điểm kết cuối, do đó đòi hỏi phải có cơ chế quản lý khóa. Có hai phương thức chuyển giao khóa đó là chuyển khóa bằng tay và chuyển khóa bằng giao thức IKE. Một hệ thống IPsec phụ thuộc phải hỗ trợ phương thức chuyển khóa băng tay. Phương thức chìa khóa trao tay chẳng hạn khóa thương mại ghi trên giấy. Phương thức này chỉ phù hợp với số lượng nhỏ các Site, đối với mạng lớn phải thực hiện phương thức quản lý khóa tự động. Trong IPsec người ta dùng giao thức quản lý chuyển khóa IKE (Internet Key Exchange). IKE có các khả năng sau :

- Cung cấp các phương tiện cho 2 bên sử dụng các giao thức, giải thuật và khóa.
- Đảm bảo ngay từ lúc bắt đầu chuyển khóa.
- Quản lý các khóa sau khi chúng được chấp nhận trong tiến trình thỏa thuận.
- Đảm bảo các khóa được chuyển một cách bảo mật.

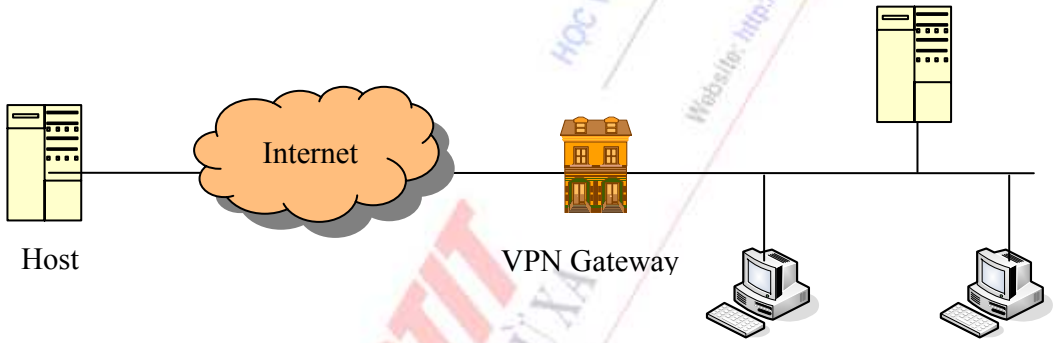
### 7.4.8. Ứng dụng ESP và AH trong cấu hình mạng

*** ESP trong cấu hình Gateway-to-Gateway:** Trong cấu hình này sẽ thiết lập kết nối có IPsec để mã hoá và đảm bảo tính toàn vẹn của dữ liệu giữa hai điểm A và B (điểm kết cuối A dùng Gateway A trên mạng A, điểm kết cuối B dùng Gateway B trên mạng B).




**Hình 7.7 Cấu hình Gateway -to-Gateway**

*** ESP và AH trong cấu hình Host-to-Host:** Trong cấu hình này sẽ thiết lập kết nối có IPsec để mã hoá và đảm bảo tính toàn vẹn của dữ liệu giữa hai điểm A và B. Tuỳ thuộc và nhu cầu bảo mật có thể dùng ESP hay AH.




**Hình 7.8 Cấu hình Host-to-Host**

### 7.4.9. So sánh các giao thức VPN

| Giao thức | Ưu điểm | Nhược điểm | Sử dụng trong mạng |
|---|---|---|---|
| IPSec | Chuẩn giao thức rãnh.<br>Hoạt động độc lập cho các ứng dụng mức caohơn.<br>Giấu địa chỉ mạng không sử dụng dịch địa chỉ mạng NAT.<br>Đáp ứng sự phát triển các kỹ thuật mã hoá . | Không quản lý NSD.<br>Không khả năng tương tác giữa các nhà cung cấp.<br>Không hỗ trợ giao diện.<br>( Desktop support) | Phần mềm tốt nhất cho các giải pháp độc quyền của nhà cung cấp đối với việc truy nhập từ xa bằng quay số. |

| | | | |
|---|---|---|---|
| PPTP | Chạy trên Wind NT, 95 ,98.<br>Cung cấp End to End và định hướng đường hầm kết nối node - to - node.<br>Các đặc điểm giá trị được thêm vào phổ biến cho truy cập từ xa.<br>Xác thực trên nền Windows.<br>Có khả năng đa giao thức.<br>Sử dụng mã hoá RSA RC-4. | Không cung cấp mã hoá dữ liệu từ những máy chủ truy cập từ xa.<br>Mang tính độc quyền, yêu cầu máy chủ chạy Win NT để kết thúc những đường hầm.<br>Chỉ sử dụng mã hoá RSA RC- 4. | Được dùng tại các máy chủ truy nhập từ xa định đường hầm proxy.<br>Có thể được dùng giữa các văn phòng ở xa có máy chủ Win NT để chạy máy chủ truy cập từ xa và định tuyến RRAS.<br>Có thể dùng cho những máy để bàn Win9x hay máy trạm dùng Win NT. |
| L2F | Cho phép định đường hầm đa giao thức.<br>Có nhiều nhà cung cấp. | Không có mã hoá<br>Xác thực NSD yếu.<br>Không điều khiển luồng cho đường hầm. | Dùng cho truy cập từ xa tại POP. |
| L2TP | Kết hợp PPTP và L2TP.<br>Chỉ cần một gói dựa trên mạng để chạy trên X.25 và Frame Relay.<br>Sử dụng IPSec iệc mã hoá. | Chưa được cung cấp trong nhiều sản phẩm.<br>Không bảo mật ở giai đoạn cuối. | Dùng cho truy nhập từ xa tại POP. |

## Câu hỏi và bài tập

1. Tổng quan về an ninh mạng
2. An toàn mạng là gì
3. Các đặc trưng kỹ thuật của an toàn mạng
4. Xác thực (Authentification), Tính khả dụng (Availability), Tính bảo mật (Confidentialy), Tính toàn vẹn (Integrity), Tính khống chế (Accountlability)
5. Các lỗ hổng và điểm yếu của mạng: Lỗ hổng loại C, Lổ hổng loại B, Lỗ hổng loại A
6. Các phương thức tấn tân công mạng
7. Các biện pháp phát hiện hệ thống bị tấn công
8. Một số phương thức tấn công mạng phổ biến: Scanner, Bẻ khoá (Password Cracker), Trojans, Sniffer
9. Tổng quan về bảo vệ thông tin bằng mật mã (Cryptography)
10. Firewall, ưu điểm và nhược điểm của Fire wall
11. Các loại Firewall
12. Kỹ thuật Fire wall

13. Kỹ thuật Proxy
14. Mạng riêng ảo VPN (Virtual Private Networks): khái niệm mạng riêng ảo và kiến trúc của mạng riêng áo
15. Các thành phần cơ bản của mạng riêng ảo VPN:
16. Những ưu điểm của mạng VPN
17. Giao thức PPTP (Point to Point Tunnelling Protocol)
18. Quá trình kết nối của PPTP: Tạo kết nối PPP, tạo kết nối điều khiển PPTP, Truyền dữ liệu qua Tunnel PPTP
19. Bảo mật trong PPTP
20. Giao thức L2F (Layer Two Forwarding Protocol)
21. Giao thức L2TP (Layer Two Tunnelling Protocol)
22. Bảo mật trong L2TP
23. Giao thức IPSEC
24. Ứng dụng ESP và AH trong cấu hình mạng
25. So sánh các giao thức VPN

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
CHƯƠNG TRÌNH ĐÀO TẠO ĐẠI HỌC TỪ XA PTIT

# CÁC TỪ VIẾT TẮT

| | |
|---|---|
| AAL | ATM Adaptation Layer |
| ANSI | American National Standard Institute |
| ABM | Asynchronous Balance Mode |
| ACK | Acknowledgement |
| ACSE | Association Control Service Element |
| ADCCP | Advanced Data Communication Control Procedures |
| AE | Application Element |
| AFI | Authority and Format Identifier. |
| AFP | AppleTalk Filing Protocol. |
| AIX | Advanced Interactive Executive |
| ALU | Aritmetic Unit |
| AM | Amplitude Modulation |
| ANSI | American National Standard Institute |
| APDU | Application Protocol Data Unit |
| API | Application Program Interface |
| APPC | Advanced Program to Program Communications |
| APPN | Advanced Peer to Peer Networking |
| ARCnet | Attached Resolution Protocol |
| ARP | Address Resolution Protocol. |
| ARPA | Advanced Research Projects Agency |
| ARQ | Automatic Repeat Request |
| ASCII | American Standard Code For Information Interchange |
| ASDU | Application Service Data Unit |
| ASE | Application Service Element |
| ASM | Address Space Manager |
| ASN.1 | Abstract Syntax Notion One |

| | |
|---|---|
| ASP | AppleShere Protocol. |
| AS | Autonomous System |
| ATM | Asynchronouse Transfer Mode |
| ATP | AppleTalk Transaction Protocol |
| BBS | Bulletin Broad System |
| BCC | Block Check Character |
| BCS | Basic Combined Subnet |
| BECN | Backward explicit Congestion Notification |
| BER | Basic Wncoding Rules |
| BERT | Bit Error Ratio Test |
| B-ISDN | Broadband Intergrated Services Digital Network. |
| BGP | Border Gateway Protocol |
| BRI | Basic Rate Interface. |
| CASE | Common Application Service Element |
| CATV | Community Antena Television |
| CCITT | International and Telephone Consultative Committe. |
| CCRSE | Commitment, Concurrency and Recovery Service Element |
| CD-ROM | Computer Disk Read Only Memory. |
| CEPT | Conference of European Postal and Telecommunications Administration |
| CICS | Customer Information Control System. |
| CLNP | Connectionless Network Servicess |
| CLNS | Connectionless Mode Network Service |
| CMIP | Common Management Information Protocol. |
| CMOT | CMIP Over TCP/IP. |
| CRC | Cyclic Redundancy Code. |
| CSMA/CA | Carrier Sense Multiple Access / Collision Avoidance |
| CSMA/CD | Carrier Sense Multiple Access / Collision Dectection |
| CSU/DSU | Channel Service Unit/Digital Service Unit |
| CSU/DSU | Channel Services Network/Digital Services Unit. |
| C/R | Command/ Request |

| | |
|---|---|
| DAP | Data Access Protocol. |
| DAS | Dual Attached Stations. |
| DCE | Data Circuit Terminating Equipment |
| DDCMP | Digital Data Communication Message Protocol |
| DDCMP | Digital Data Communications Protocol. |
| DDM | Distributed Data Management |
| DDM | Distributed Data Management. |
| DES | Dataencryption Standard. |
| DFC | Data Flow Control. |
| DHCP | Dynamic Host Configuable Protocol. |
| DIA | Document Interchange Architecture. |
| DIA | Document Interchange Architecture. |
| DIP | Dual In Line Packege |
| DIX | Digital Intel Xerox. |
| DLC | Data Link Control |
| DE | Discard Eligibility |
| DLE | Data Link Escape. |
| DMA | Direct Memory Mapping. |
| DNA | Digital Network Architecture. |
| DNS | Domain Name System. |
| DNS-MX | Mail Routing and the Domain System. |
| DOD | Derpartment Of Defense. |
| DQDB | Distributed Queue Dual Bus. |
| DS | Directory Services. |
| DSP | Domain Specific Part. |
| DTAM | Document Transfer, Access and Management. |
| DTE | Data Terminal Equipment. |
| DTP | Distributed Transaction Processing. |
| EA | Extend Address |
| EBCDIC | Extended Binary Coded Decimal Interchange Code. |

| | |
|---|---|
| EGP | Exterior Gateway Protocol |
| ECMA | European Computer Manufacturers Association. |
| EIA | Electronic Industries Association |
| FECN | Forward Explicit Congestion Notification |
| FCS | Frame Check Sequence. |
| FDDI | Fiber Distributed Data Interface. |
| FDM | Frequency Division Multipling. |
| FEA | Frame Relay Adaptor. |
| FM | Frequency Modulation. |
| FR | Frame Relay |
| FRAD | Frame Relay Access Device |
| FRND | Frame Relay Network Device |
| FR UNI | Frame Relay User to Network Interface |
| FTAM | File Transfer Access and Management. |
| FTP | File Transfer Protocol. |
| GGP | Gateway to gateway Protocol. |
| GOSIP | Goverment OSI Profil. |
| HDLC | High Level Data Link Control. |
| HIPPI | High Performance Parellet Interface. |
| HTML | Hyper Text Markup Language. |
| HTTP | Hyper Text Transfer Protocol. |
| IA5 | International Alphalbet Number 5. |
| IANA | Internet Assigned Numbers Authority |
| ICMP | Internet Control Message Protocol. |
| IDI | Initial Domain Identifier. |
| IDP | Initial Domain Part. |
| IEEE | Institute of Electrical and Electric Engineers. |
| IETF | Internet Engineering Task Force |
| IGP | Interior Gateway Protocol. |
| IMS | Information Management System. |

| | |
|---|---|
| INTERNIC | Internet Netwowrk Information Center. |
| IP | Internet Protocol. |
| IPL | Initial Program Load. |
| IPX | Internetwork Packet Exchange. |
| ISA | Industry Standard Architecture . |
| ISDN | Intergrated Services Digital Network |
| ISO | International Standard Organization. |
| ISP | Internet Service Provider |
| ITU | International Telecommunications Union. |
| JTM | Job Transfer and Management. |
| LAN | Local Area Network. |
| LAP-B | Link Access Procedure Balanced |
| LAP-D | Link Access Procedure Dchannel. |
| LED | Ligh Emiting Diode. |
| LLAP | LocalTalk Link Access Protocol. |
| LLC | Logical Link Control. |
| LPDU | Link Protocol Data Unit. |
| LSAP | Link SAP. |
| LSDU | Link Service Data Unit. |
| LSL | Link Support Layer. |
| LU | Logical Unit. |
| MAC | Media Access Control. |
| MAN | Metropolitan Area network. |
| MAP | Manufacturing Automation Protocol. |
| MAU | Multistation Access Unit. |
| MCA | Micro Channel Architecture. |
| MHS | Message Handling System. |
| MIB | Management Information Base. |
| MLID | Multiple Link Interface Driver. |
| MMS | Manufacturing Messaging Service. |

| | |
|---|---|
| MODEM | Mudulation Demodulation. |
| MUX | Multiplexer. |
| NAK | Negative Acknowledgment. |
| NAU | Network Addressable Unit. |
| NAU | Network Address Unit. |
| NBS | National Bureau of Standard. |
| NCP | Netware Core Protocol. |
| NDS | Network Operating System. |
| NFS | Network File System. |
| NFS | Network File System. |
| NIC | Network Interface Card. |
| NLM | Netware Loadable Modules. |
| NLSP | Network Link Services Protocol. |
| NMS | Network Management System. |
| NNI | Network to Network Interface |
| NPDU | Network Protocol Data unit. |
| NREN | National Research and Education Network. |
| NRM | Normal Response Mode |
| NRZ | Non Return to Zero. |
| NS | Network Services. |
| NSAP | Network SAP. |
| NSDU | Network Service Data Unit. |
| NSP | Network Services Protocol. |
| NAT | Network Address Translation |
| NFS | Network File System |
| NIS | Network Information System |
| NVTS | Network Virtual Terminal Service. |
| OC | Optical Carrier. |
| ODI | Open Data Link Interface. |
| ODIF | Office Document Interchane Format. |

| | |
|---|---|
| OPA | Office Document Architecture. |
| OS | Operating System. |
| OSF | Open Software Foundation. |
| OSI | Open Systems Interconnection.. |
| OSPF | Open Shortest Path First. |
| PA | Point of P Attachement. |
| PAD | Packet Assembler Disassembler. |
| PAP | Printer Access Protocol. |
| PBX | Pripheral Component Interconnection. |
| PDN | Public Data Network. |
| PDU | Protocol Data Unit. |
| PE | Presentation Entity. |
| POP | Post Office Protocol. |
| POSIX | Portable Operating System Interface Exchange. |
| PPDU | Presentation Protocol Data Unit. |
| PPP | Point to Point Protocol. |
| PPTP | Point to Point Tunneling Protocol |
| PPSDN | Public Packet Switched Data Network. |
| PRI | Primary Rate Interface. |
| PSAP | Presentation Service Access Point. |
| PSDN | Packet Switched Data Network.. |
| PSDU | Presentation Service Data Unit. |
| PSTN | Public Switched Telphone network. |
| PTT | Post, Telphone and Communications. |
| PU | Physical Unit. |
| PVC | Permanent Virtual Circuit. |
| QOS | Quality Of Service |
| RARP | Reverse Address Resolution Protocol |
| RAID | Redundant Array of Inexpensive Drives. |
| RARP | Reverse Address Resolution Protocol. |

| | |
|---|---|
| RAS | Remote Access Services. |
| RDA | Remote Database Access. |
| RFC | Request For Command. |
| RFNM | Ready For Next Message. |
| RIP | Routing Information Protocol. |
| RISC | Reduced Instruction Set Computer. |
| RNR | Receive Not Ready. |
| ROSE | Remote Operation Service Element. |
| RPC | Remote Procedure Call. |
| RR | Receive Ready. |
| RTMP | Routing Table Maintenance Protocol. |
| RTSE | Reliable Transfer Service Element. |
| SAP | Service Access Point. |
| SAP | Service Advertising Protocol. |
| SAPI | SAP Identifier. |
| SAS | Single Attached Stations. |
| SCSI | Small Computer Systems Interface. |
| SDH | Synchronouse Digital Hierarchy. |
| SDLC | Synchronouse Data Link Control. |
| SE | Session Entity. |
| SI | Subnet Identifier. |
| SLIP | Serial Line Internet Protocol. |
| SMDS | Switched Multimegabit Digital Service. |
| SMTP | Simple Mail Transfer Protocol. |
| SNA | System Network Architecture. |
| SNADS | SNA Distribute Service. |
| SNAP | Subnetwork Address Protocol. |
| SNMP | Simple Network Management Protocol. |
| SONET | Synchronouse Optical Network. |
| SPDU | Session PDU. |

| | |
|---|---|
| SPX | Sequenced Packet Exchange. |
| SQL | Structured Query Language. |
| SSAP | Session SAP. |
| SSL | Secure Sockets Layer |
| SSCP | System Services Control Point. |
| SSDU | Session Service Data Unit. |
| STP | Shield Twisted Pair. |
| SVC | Switch Virtual Circuit |
| TCP | Transmission Control Protocol. |
| TDM | Time Division Multiplexing. |
| TE | Transport Entity. |
| TELNET | Telnet Protocol. |
| TFTP | Trivial File Transfer protocol. |
| TPDU | Transport PDU. |
| TSAP | Transport SAP. |
| TSDU | Transport SDU. |
| UART | Universal Asynchronouse Receiver Transmitter. |
| UDP | User Datafram Protocol. |
| UNI | User to Network Interface. |
| UTP | Unshield Twisted Pair. |
| VC | Virtual Circuit. |
| VCI | Virtual Circuit Identifier. |
| VLAN | Virtaul Local Area Network. |
| VPI | Virtual Path Identifier. |
| VPN | Virtual Private Network. |
| VTAM | Virtual Telecommunication Access Method. |
| WAN | Wide Area network. |
| WWW | World Wide Web. |
| XNS | Xerox Network Service. |

# MỤC LỤC

**MỞ ĐẦU** ..... 3
**CHƯƠNG 1: KHÁI NIỆM VỀ MẠNG MÁY TÍNH** ..... 5
1.1. Định nghĩa mạng máy tính ..... 5
1.2. Mục tiêu mạng máy tính ..... 6
1.2.1. Mục tiêu kết nối mạng máy tính ..... 6
1.2.2. Lợi ích kết nối mạng ..... 6
1.3. Các dịch vụ mạng ..... 6
1.3.1. Các xu hướng phát triển dịch vụ mạng máy tính ..... 6
1.3.2 Các dịch vụ phổ biến trên mạng máy tính ..... 6
1.4 Cấu trúc mạng (Topology) ..... 7
1.4.1 Kiểu điểm - điểm (Point to Point) ..... 7
1.4.2. Kiểu đa điểm hay quảng bá (Point to Multipoint, Broadcasting) ..... 8
1.5. Khái niệm giao thức mạng máy tính (Protocols) ..... 8
1.5.1. Khái niệm về giao thức ..... 8
1.5.2. Chức năng giao thức ..... 9
1.6. Cáp mạng - phương tiện truyền (Network Medium) ..... 9
1.6.1. Đặc trưng cơ bản của đường truyền ..... 10
1.6.2. Các loại cáp mạng ..... 10
1.6.3. Các phương tiện vô tuyến ..... 11
1.7. Phân loại mạng ..... 12
1.7.1. Theo khoảng cách ..... 12
1.7.2. Mạng chuyển mạch kênh (Circuit Switched Networks) ..... 15
1.7.3. Mạng chuyển mạch gói (Packet Switched Networks) ..... 16
1.8. Các mô hình xử lý dữ liệu ..... 17
1.8.1. Mô hình Client-Server ..... 17
1.8.2. Mô hình ngang hàng (Peer-to-Peer) ..... 18
Câu hỏi trắc nghiệm: ..... 19
Câu hỏi ..... 21
**CHƯƠNG 2: KIẾN TRÚC MẠNG VÀ MÔ HÌNH KẾT NỐI CÁC HỆ THỐNG MỞ OSI** ..... 23
2.1. Các tổ chức tiêu chuẩn hóa mạng máy tính ..... 23
2.1.1. Cơ sở xuất hiện kiến trúc đa tầng ..... 23
2.1.2. Các tổ chức tiêu chuẩn ..... 23
2.2. Mô hình kiến trúc đa tầng ..... 24
2.2.1. Các quy tắc phân tầng ..... 24
2.2.2. Lưu chuyển thông tin trong kiến trúc đa tầng ..... 25
2.2.3. Nguyên tắc truyền thông đồng tầng ..... 26
2.2.4. Giao diện tầng, quan hệ các tầng kề nhau và dịch vụ ..... 26
2.2.5 Dịch vụ và chất lượng dịch vụ ..... 27
2.2.6. Các hàm dịch vụ nguyên thuỷ (Primitive) ..... 29
2.2.7. Quan hệ giữa dịch vụ và giao thức ..... 30
2.3 Mô hình kết nối các hệ thống mở OSI (Open System Interconnection) ..... 31
2.3.1 Nguyên tắc định nghĩa các tầng hệ thống mở ..... 31
2.3.2. Các giao thức trong mô hình OSI ..... 32
2.3.3 Truyền dữ liệu trong mô hình OSI ..... 32
2.3.4. Vai trò và chức năng chủ yếu các tầng ..... 33
2.4. Một số kiến trúc khác ..... 35
2.4.1. Systems Nework Architecture (SNA) ..... 35
2.4.2. Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX) ..... 35

2.4.3. AppleTalk ..... 36
2.4.4. Digital Network Architectur (DNA) ..... 36
2.4.5. Họ IEEE 802 (Institute of Electrical and Electronic Engineer) ..... 36
2.4.6. TCP/IP (Transmission Control Protocol/Internet Protocol) ..... 36
Câu hỏi trắc nghiệm ..... 37
Câu hỏi và bài tập ..... 41
**CHƯƠNG 3: MẠNG INTERNET VÀ GIAO THỨC TCP/IPV4** ..... 42
3.1. Mô hình TCP/IP ..... 42
3.1.1. Mô hình kiến trúc TCP/IP ..... 42
3.1.2. Vai trò và chức năng các tầng trong mô hình TCP/IP ..... 43
3.1.3. Quá trình đóng gói dữ liệu Encapsulation ..... 44
3.1.4. Quá trình phân mảnh dữ liệu Fragment ..... 45
3.2. Một số giao thức cơ bản của bộ giao thức TCP/IP ..... 45
3.2.1. Giao thức gói tin người sử dụng UDP (User Datagram Protocol) ..... 45
3.2.2. Giao thức điều khiển truyền TCP (Transmission Control Protocol) ..... 45
3.2.3. Giao thức mạng IP (Internet Protocol) ..... 49
3.2.4. Giao thức thông báo điều khiển mạng ICMP(Internet Control Message Protocol) ..... 51
3.2.5. Giao thức phân giải địa chỉ ARP (Address Resolution Protocol) ..... 52
3.2.6 Giao thức phân giải địa chỉ ngược RARP (Reverse Address Resolution Protocol) ..... 53
3.3 Giao thức IPv6 (Internet Protocol Version Number 6) ..... 54
3.3.1 Nguyên nhân ra đời của IPv6 ..... 54
3.3.2 Các đặc trưng của IPv6 ..... 55
3.3.3 So sánh IPv4 và IPv6 ..... 56
3.4 Các lớp địa chỉ IPv6 ..... 57
3.4.1 Phương pháp biểu diễn địa chỉ IPv6 ..... 57
3.4.2 Phân loại địa chỉ IPv6 ..... 57
3.4.3 So sánh địa chỉ IPv4 và địa chỉ IPv6 ..... 57
Câu hỏi và bài tập ..... 58
**CHƯƠNG 4: KỸ THUẬT MẠNG CỤC BỘ** ..... 59
4.1 Các phương thức truy nhập đường truyền ..... 59
4.1.1 Phương thức đa truy nhập sử dụng sóng mang có phát hiện xung đột CSMA/CD (Carrier Sense Multiple Access with Collision Detection) ..... 59
4.1.2 Token Bus ..... 60
4.1.3 Token ring ..... 61
4.1.4 So sánh CSMA/CD với các phương pháp dùng thẻ bài ..... 62
4.2 Ethernet và chuẩn IEEE 802 ..... 62
4.2.1 Giới thiệu chung về Ethernet ..... 62
4.2.2 Chức năng các tầng trong IEEE 802 ..... 63
4.2.3 Cấu trúc khung Ethernet: ..... 64
4.2.4 Họ IEEE 802 ..... 65
4.2.5 Ethernet 100 Mbps. ..... 67
4.2.6 Gigabit Ethernet. ..... 67
4.2.7 Gigabit Ethernet qua cáp sợi quang ..... 68
4.3 Mạng cục bộ Token Ring ..... 68
4.3.1 Hoạt động của Token Ring ..... 69
4.3.2 Chuẩn Token Ring ..... 69
4.4. Giao diện số liệu phân bố sử dụng quang FDDI (Fiber Distributed Data Interface) ..... 70
4.4.1 Giới thiệu FDDI ..... 70
4.4.2. So sánh những giữa FDDI và IEEE 802.5 ..... 71
4.4.3 Các kiểu kết nối đầu cuối FDDI ..... 71
4.4.4 Khả năng chịu lỗi của FDDI ..... 72
4.5 Mạng LAN ATM ..... 72
4.5.1 Đặc trưng của ATM LAN ..... 73
4.5.2 Các loại ATM LAN ..... 73
4.5.3 Kỹ thuật chuyển mạch ATM LAN ..... 74

Câu hỏi trắc nghiệm....74
Câu hỏi và bài tập....75
**CHƯƠNG 5: KỸ THUẬT MẠNG DIỆN RỘNG WAN....77**
5.1 Khái niệm về liên mạng (Internetworking)....77
5.2. Mạng tích hợp đa dịch vụ số ISDN (Integrated Service Digital Network)....78
5.2.1 ISDN là gì....78
5.2.2 Các phần tử cơ bản của mạng ISDN....79
5.2.3 Các loại kênh trong mạng ISDN....79
5.2.4 Giao diện ISDN....79
5.2.5 Chức năng các tầng trong kiến trúc ISDN....80
5.3 Mạng băng rộng B_ISDN ( Broadband ISDN)....82
5.3.1 Tổng quan về sự ra đời của B-isdn....82
5.3.2 Đặc điểm của dịch vụ B-ISDN....82
5.3.3 Cấu trúc chức năng của B_ISDN....83
5.3.4 So sánh giữa ISDN và B_ISDN....83
5.4 Mạng chuyển mạch gói X25....83
5.4.1 Khái quát kỹ thuật mạng X25....83
5.4.2 Giao thức X.25....84
5.4.3 Hoạt động của giao thức X25....85
5.5 Mạng chuyển mach khung Frame Relay....85
5.5.1 Giới thiệu chung....85
5.5.2 Cấu hình tổng quát mạng Frame Relay....86
5.5.3 So sánh Frame Relay với X25....86
5.5.4 Frame Relay và mô hình OSI....87
5.5.5 Điều khiển quản lý lưu lượng....88
5.5.6 Các dịch vụ Frame Relay....89
5.6 SMDS (Switched Multimegabit Data Service )....89
5.6.1 Giới thiệu chung.....89
5.6.2 SMDS là gì....90
5.6.3 Tổng quan về SMDS....90
5.6.4 Tổng quan về kỹ thuật SMDS....90
5.6.5 SMDS so với các công nghệ ATM và Frame Relay....91
5.7 Phương thức truyền dẫn không đồng bộ ATM (Asynchronous Transfer Mode)....92
5.7.1 Giới thiệu chung....92
5.7.2 Kiến trúc phân tầng ATM....93
5.7.3 Liên kết ảo (Virtual Connections)....96
5.7.4 So sánh ATM với các dịch vụ và kỹ thuật khác....97
Câu hỏi trắc nghiệm:....98
Câu hỏi và bài tập....101
**CHƯƠNG 6: MẠNG TỐC ĐỘ CAO VÀ ỨNG DỤNG CÁC CÔNG NGHỆ MỚI....103**
6.1 Đường dây thuê bao số DSL (Digital Subscribers Line)....103
6.1.1 *Mở đầu*....103
6.1.2 Tổng quan về họ công nghệ DSL....103
6.1.3 Các vấn đề cơ bản công nghệ DSL trên mạng cáp đồng....105
6.1.4 Các phương pháp mã hóa đường truyền....106
6.1.5 Phát hiện lỗi và sửa lỗi....106
6.1.6 Nhiễu và chống xuyên nhiễu....106
6.1.7 Các mô hình kết nối ADSL....108
6.1.8 Các ứng dụng của ADSL....110
6.2 Truyền thoại qua mạng chuyển mạch gói VoPN (Voice over Packet Network)....111
6.2.1 Khái niệm....111
6.2.2 Mô hình truyền thoại qua mạng chuyển mạch gói....111
6.2.3 Ưu điểm của truyền thoại qua mạng chuyển mạch gói....111
6.2.4 Các vấn đề về chất lượng dịch vụ QoS....112
6.2.5 Voice over Frame Relay - VoFR....113

6.2.6 Voice over ATM - VoATM....113
6.2.7 Voice over Internet Protocol – VoIP....113
6.3. Công nghệ chuyển mạch nhãn đa giao thức MPLS (MultiProtocol Label Switching)....118
6.3.1 Mở đầu....118
6.3.2 Kiến trúc và nguyên tắc hoạt động MPLS....118
6.4. Công nghệ chuyển mạch mềm (Softswitch)....121
6.4.1 *Mở đầu*....121
6.4.2 Cấu trúc và nguyên tắc chuyển mạch mềm....122
6.4.3 Giao diện ứng dụng API trong chuyển mạch mềm....123
6.4.4 Kế hoạch đánh số trong chuyển mạch mềm....124
6.4.5 Đánh giá công nghệ chuyển mạch mềm....125
6.5. Mạng hội tụ và mạng thế hệ sau NGN (Network Convergence and Next Generation Network)....126
6.5.1 Mở đầu....126
6.5.2 Tổng quan về mạng thế hệ sau sau - NGN (Next Generation Network)....126
6.5.3 Sự bùng nổ và nhu cầu da dạng của các loại hình dịch vụ....127
6.5.4 Mô hình phân lớp và chức năng các lớp NGN....127
6.5.5 Cấu trúc và các thành phần hệ thống NGN....128
6.5.6 Các công nghệ nền tảng trong NGN....128
6.5.7 Mô hình NGN và các giải pháp thiết kế của một số hãng....130
6.5.8 Một số dịch vụ NGN....131
6.5.9 NGN trong mạng viễn thông Việt nam....132
Câu hỏi trắc nghiệm:....133
Câu hỏi và bài tập....135
**CHƯƠNG 7: AN TOÀN MẠNG**....137
7.1 Tổng quan về an ninh mạng....137
7.1.1 An toàn mạng là gì....137
7.1.2 Các đặc trưng kỹ thuật của an toàn mạng....138
7.1.3 Các lỗ hổng và điểm yếu của mạng....139
7.1.4 Các biện pháp phát hiện hệ thống bị tấn công....140
7.2 Một số phương thức tấn công mạng phổ biến....140
7.2.1 *Scanner*....140
7.2.2 Bẻ khoá (Password Cracker)....141
7.2.3 Trojans....141
7.2.4 Sniffer....142
7.3 Biện pháp đảm bảo an ninh mạng....142
7.3.1 Tổng quan về bảo vệ thông tin bằng mật mã (Cryptography)....142
7.3.2 Firewall....143
7.3.3 Các loại Firewall....144
7.3.4 Kỹ thuật Fire wall....144
7.3.5 Kỹ thuật Proxy....145
7.4. Mạng riêng ảo VPN (Virtual Private Networks)....145
7.4.1. Khái niệm mạng riêng ảo....145
7.4.2 Kiến trúc của mạng riêng áo....146
7.4.3 Những ưu điểm của mạng VPN....148
7.4.4 Giao thức PPTP (Point to Point Tunnelling Protocol)....148
7.4.5 Giao thức L2F (Layer Two Forwarding Protocol)....148
7.4.6 Giao thức L2TP (Layer Two Tunnelling Protocol)....149
7.4.7 *Giao thức IPSEC*....150
7.4.8 Ứng dụng ESP và AH trong cấu hình mạng....151
7.4.9 So sánh các giao thức VPN....152
Câu hỏi và bài tập....153
**CÁC TỪ VIẾT TẮT**....155
**TÀI LIỆU THAM KHẢO**....164

# MẠNG MÁY TÍNH

**Mã số: 492MMT450**

**Chịu trách nhiệm bản thảo**

TRUNG TÂM ĐÀO TẠO BƯU CHÍNH VIỄN THÔNG 1

*(Tài liệu này được ban hành theo Quyết định số: 352/QĐ-TTĐT1 ngày 12/05/2006 của Giám đốc Học viện Công nghệ Bưu chính Viễn thông)*

In tại : *Công ty cổ phần In Bưu điện*
Số lượng : *2000 cuốn, khổ 19 x 26 cm*
Ngày hoàn thành : *01/06/2006.*

# GIÁO TRÌNH
# MẠNG MÁY TÍNH

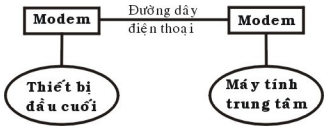
**Hà nội 11-2000**

**Chương 1**

# Sơ lược lịch sử phát triển của mạng máy tính

Vào giữa những năm 50 khi những thế hệ máy tính đầu tiên được đưa vào hoạt động thực tế với những bóng đèn điện tử thì chúng có kích thước rất cồng kềnh và tốn nhiều năng lượng. Hồi đó việc nhập dữ liệu vào các máy tính được thông qua các tấm bìa mà người viết chương trình đã đục lỗ sẵn. Mỗi tấm bìa tương đương với một dòng lệnh mà mỗi một cột của nó có chứa tất cả các ký tự cần thiết mà người viết chương trình phải đục lỗ vào ký tự mình lựa chọn. Các tấm bìa được đưa vào một "thiết bị" gọi là thiết bị đọc bìa mà qua đó các thông tin được đưa vào máy tính (hay còn gọi là trung tâm xử lý) và sau khi tính toán kết quả sẽ được đưa ra máy in. Như vậy các thiết bị đọc bìa và máy in được thể hiện như các thiết bị vào ra (I/O) đối với máy tính. Sau một thời gian các thế hệ máy mới được đưa vào hoạt động trong đó một máy tính trung tâm có thể được nối với nhiều thiết bị vào ra (I/O) mà qua đó nó có thể thực hiện liên tục hết chương trình này đến chương trình khác.

Cùng với sự phát triển của những ứng dụng trên máy tính các phương pháp nâng cao khả năng giao tiếp với máy tính trung tâm cũng đã được đầu tư nghiên cứu rất nhiều. Vào giữa những năm 60 một số nhà chế tạo máy tính đã nghiên cứu thành công những thiết bị truy cập từ xa tới máy tính của họ. Một trong những phương pháp thâm nhập từ xa được thực hiện bằng việc cài đặt một thiết bị đầu cuối ở một vị trí cách xa trung tâm tính toán, thiết bị đầu cuối này được liên kết với trung tâm bằng việc sử dụng đường dây điện thoại và với hai thiết bị xử lý tín hiệu (thường gọi là Modem) gắn ở hai đầu và tín hiệu được truyền thay vì trực tiếp thì thông qua dây điện thoại.




*Hình 1.1. Mô hình truyền dữ liệu từ xa đầu tiên*

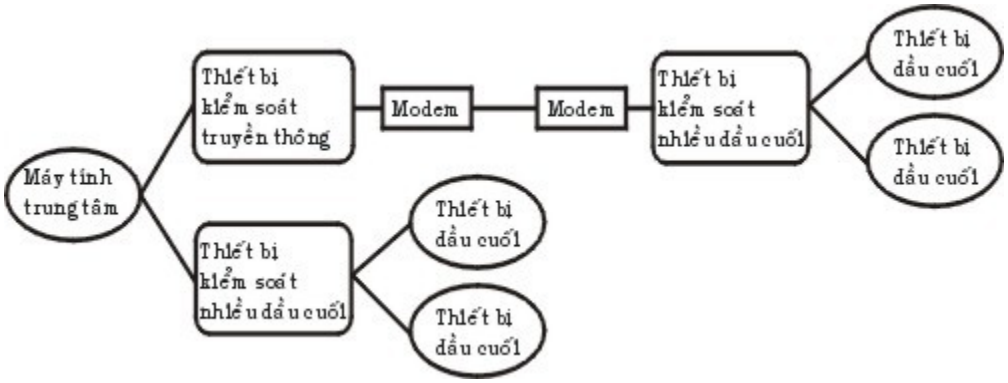
Những dạng đầu tiên của thiết bị đầu cuối bao gồm máy đọc bìa, máy in, thiết bị xử lý tín hiệu, các thiết bị cảm nhận. Việc liên kết từ xa đó có thể thực hiên thông qua những vùng khác nhau và đó là những dạng đầu tiên của hệ thống mạng.

Trong lúc đưa ra giới thiệu những thiết bị đầu cuối từ xa, các nhà khoa học đã triển khai một loạt những thiết bị điều khiển, những thiết bị đầu cuối đặc biệt cho phép người sử dụng nâng cao được khả năng tương tác với máy tính. Một trong những sản phẩm quan trọng đó là hệ thống thiết bị đầu cuối 3270 của IBM. Hệ thống đó bao gồm các màn hình, các hệ thống điều khiển, các thiết bị truyền thông được liên kết với các trung tâm tính toán. Hệ thống 3270 được giới thiệu vào năm 1971 và được sử dụng dùng để mở rộng khả năng tính toán của trung tâm máy tính tới các vùng xa. Để làm giảm nhiệm vụ truyền thông của máy tính trung tâm và số lượng các liên kết giữa

máy tính trung tâm với các thiết bị đầu cuối, IBM và các công ty máy tính khác đã sản xuất một số các thiết bị sau:

- **Thiết bị kiểm soát truyền thông**: có nhiệm vụ nhận các bit tín hiệu từ các kênh truyền thông, gom chúng lại thành các byte dữ liệu và chuyển nhóm các byte đó tới máy tính trung tâm để xử lý, thiết bị này cũng thực hiện công việc ngược lại để chuyển tín hiệu trả lời của máy tính trung tâm tới các trạm ở xa. Thiết bị trên cho phép giảm bớt được thời gian xử lý trên máy tính trung tâm và xây dựng các thiết bị logic đặc trưng.

- **Thiết bị kiểm soát nhiều đầu cuối**: cho phép cùng một lúc kiểm soát nhiều thiết bị đầu cuối. Máy tính trung tâm chỉ cần liên kết với một thiết bị như vậy là có thể phục vụ cho tất cả các thiết bị đầu cuối đang được gắn với thiết bị kiểm soát trên. Điều này đặc biệt có ý nghĩa khi thiết bị kiểm soát nằm ở cách xa máy tính vì chỉ cần sử dụng một đường điện thoại là có thể phục vụ cho nhiều thiết bị đầu cuối.




*Hình 1.2: Mô hình trao đổi mạng của hệ thống 3270*

Vào giữa những năm 1970, các thiết bị đầu cuối sử dụng những phương pháp liên kết qua đường cáp nằm trong một khu vực đã được ra đời. Với những ưu điểm từ nâng cao tốc độ truyền dữ liệu và qua đó kết hợp được khả năng tính toán của các máy tính lại với nhau. Để thực hiện việc nâng cao khả năng tính toán với nhiều máy tính các nhà sản xuất bắt đầu xây dựng các mạng phức tạp. Vào những năm 1980 các hệ thống đường truyền tốc độ cao đã được thiết lập ở Bắc Mỹ và Châu Âu và từ đó cũng xuất hiện các nhà cung cấp các dịnh vụ truyền thông với những đường truyền có tốc độ cao hơn nhiều lần so với đường dây điện thoại. Với những chi phí thuê bao chấp nhận được, người ta có thể sử dụng được các đường truyền này để liên kết máy tính lại với nhau và bắt đầu hình thành các mạng một cách rộng khắp. Ở đây các nhà cung cấp dịch vụ đã xây dựng những đường truyền dữ liệu liên kết giữa các thành phố và khu vực với nhau và sau đó cung cấp các dịch vụ truyền dữ liệu cho những người xây dựng mạng. Người xây dựng mạng lúc này sẽ không cần xây dựng lại đường truyền của mình mà chỉ cần sử dụng một phần các năng lực truyền thông của các nhà cung cấp.

Vào năm 1974 công ty IBM đã giới thiệu một loạt các thiết bị đầu cuối được chế tạo cho lĩnh vực ngân hàng và thương mại, thông qua các dây cáp mạng các thiết bị đầu cuối có thể truy cập cùng một lúc vào một máy tính dùng chung. Với việc liên kết các máy tính nằm ở trong một khu vực nhỏ như một tòa nhà hay là một khu nhà thì tiền chi phí cho các thiết bị và phần mềm là thấp. Từ đó việc nghiên cứu khả năng sử dụng chung môi trường truyền thông và các tài nguyên của các máy tính nhanh chóng được đầu tư.

Vào năm 1977, công ty Datapoint Corporation đã bắt đầu bán hệ điều hành mạng của mình là "Attached Resource Computer Network" (hay gọi tắt là Arcnet) ra thị trường. Mạng Arcnet cho phép liên kết các máy tính và các trạm đầu cuối lại bằng dây cáp mạng, qua đó đã trở thành là hệ điều hành mạng cục bộ đầu tiên.

Từ đó đến nay đã có rất nhiều công ty đưa ra các sản phẩm của mình, đặc biệt khi các máy tính cá nhân được sử dụng một cánh rộng rãi. Khi số lượng máy vi tính trong một văn phòng hay cơ quan được tăng lên nhanh chóng thì việc kết nối chúng trở nên vô cùng cần thiết và sẽ mang lại nhiều hiệu quả cho người sử dụng.

Ngày nay với một lượng lớn về thông tin, nhu cầu xử lý thông tin ngày càng cao. Mạng máy tính hiện nay trở nên quá quen thuộc đối với chúng ta, trong mọi lĩnh vực như khoa học, quân sự, quốc phòng, thương mại, dịch vụ, giáo dục... Hiện nay ở nhiều nơi mạng đã trở thành một nhu cầu không thể thiếu được. Người ta thấy được việc kết nối các máy tính thành mạng cho chúng ta những khả năng mới to lớn như:

- **Sử dụng chung tài nguyên:** Những tài nguyên của mạng (như thiết bị, chương trình, dữ liệu) khi được trở thành các tài nguyên chung thì mọi thành viên của mạng đều có thể tiếp cận được mà không quan tâm tới những tài nguyên đó ở đâu.

- **Tăng độ tin cậy của hệ thống**: Người ta có thể dễ dàng bảo trì máy móc và lưu trữ (backup) các dữ liệu chung và khi có trục trặc trong hệ thống thì chúng có thể được khôi phục nhanh chóng. Trong trường hợp có trục trặc trên một trạm làm việc thì người ta cũng có thể sử dụng những trạm khác thay thế.

- **Nâng cao chất lượng và hiệu quả khai thác thông tin:** Khi thông tin có thể được sữ dụng chung thì nó mang lại cho người sử dụng khả năng tổ chức lại các công việc với những thay đổi về chất như:

  - Đáp ứng những nhu cầu của hệ thống ứng dụng kinh doanh hiện đại.
  - Cung cấp sự thống nhất giữa các dữ liệu.
  - Tăng cường năng lực xử lý nhờ kết hợp các bộ phận phân tán.
  - Tăng cường truy nhập tới các dịch vụ mạng khác nhau đang được cung cấp trên thế giới.

Với nhu cầu đòi hỏi ngày càng cao của xã hội nên vấn đề kỹ thuật trong mạng là mối quan tâm hàng đầu của các nhà tin học. Ví dụ như làm thế nào để truy xuất thông tin một cách nhanh chóng và tối ưu nhất, trong khi việc xử lý thông tin trên mạng quá nhiều đôi khi có thể làm tắc nghẽn trên mạng và gây ra mất thông tin một cách đáng tiếc.

Hiện nay việc làm sao có được một hệ thống mạng chạy thật tốt, thật an toàn với lợi ích kinh tế cao đang rất được quan tâm. Một vấn đề đặt ra có rất nhiều giải pháp về công nghệ, một giải pháp có rất nhiều yếu tố cấu thành, trong mỗi yếu tố có nhiều cách lựa chọn. Như vậy để đưa ra một giải pháp hoàn chỉnh, phù hợp thì phải trải qua một quá trình chọn lọc dựa trên những ưu điểm của từng yếu tố, từng chi tiết rất nhỏ.

Để giải quyết một vấn đề phải dựa trên những yêu cầu đặt ra và dựa trên công nghệ để giải quyết. Nhưng công nghệ cao nhất chưa chắc là công nghệ tốt nhất, mà công nghệ tốt nhất là công nghệ phù hợp nhất.

Chương 2

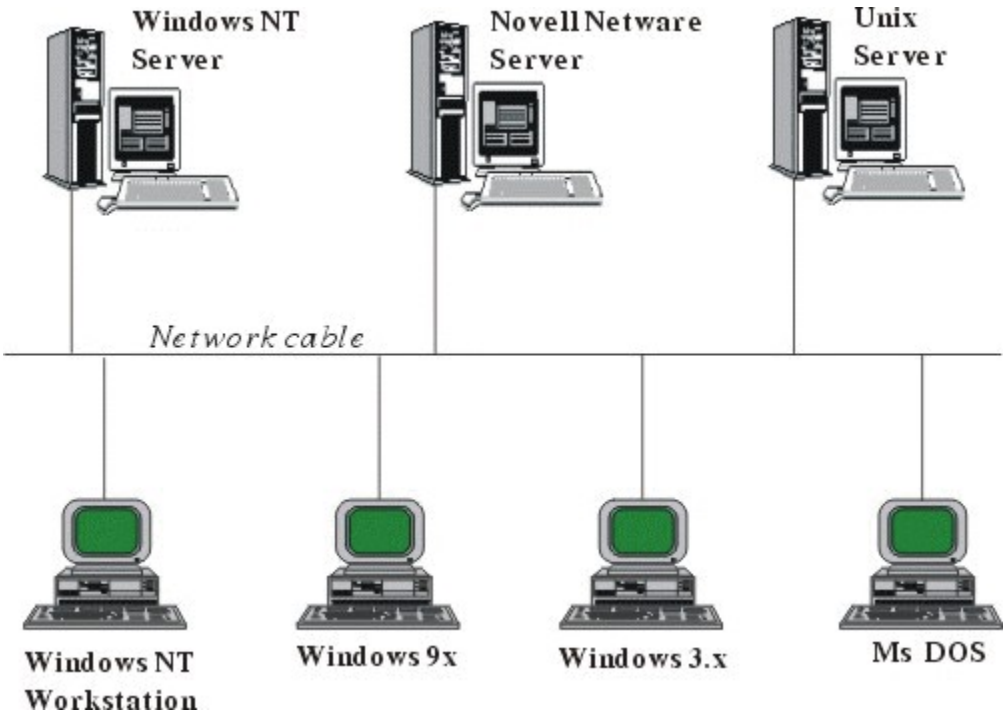
# Những khái niệm cơ bản của mạng máy tính

Với sự phát triển của khoa học và kỹ thuật, hiện nay các mạng máy tính đã phát triển một cách nhanh chóng và đa dạng cả về quy mô, hệ điều hành và ứng dụng. Do vậy việc nghiên cứu chúng ngày càng trở nên phức tạp. Tuy nhiên các mạng máy tính cũng có cùng các điểm chung thông qua đó chúng ta có thể đánh giá và phân loại chúng.

## I. Định nghĩa mạng máy tính

> *Mạng máy tính là một tập hợp các máy tính được nối với nhau bởi đường truyền theo một cấu trúc nào đó và thông qua đó các máy tính trao đổi thông tin qua lại cho nhau.*

Đường truyền là hệ thống các thiết bị truyền dẫn có dây hay không dây dùng để chuyển các tín hiệu điện tử từ máy tính này đến máy tính khác. Các tín hiệu điện tử đó biểu thị các giá trị dữ liệu dưới dạng các xung nhị phân (on - off). Tất cả các tín hiệu được truyền giữa các máy tính đều thuộc một dạng sóng điện từ. Tùy theo tần số của sóng điện từ có thể dùng các đường truyền vật lý khác nhau để truyền các tín hiệu. Ở đây đường truyền được kết nối có thể là dây cáp đồng trục, cáp xoắn, cáp quang, dây điện thoại, sóng vô tuyến ... Các đường truyền dữ liệu tạo nên cấu trúc của mạng. Hai khái niệm đường truyền và cấu trúc là những đặc trưng cơ bản của mạng máy tính.




*Hình 2.1: Một mô hình liên kết các máy tính trong mạng*

Với sự trao đổi qua lại giữa máy tính này với máy tính khác đã phân biệt mạng máy tính với các hệ thống thu phát một chiều như truyền hình, phát thông tin từ vệ tinh xuống các trạm thu thụ động... vì tại đây chỉ có thông tin một chiều từ nơi phát đến nơi thu mà không quan tâm đến có bao nhiêu nơi thu, có thu tốt hay không.

Đặc trưng cơ bản của đường truyền vật lý là giải thông. Giải thông của một đường chuyền chính là độ đo phạm vi tần số mà nó có thể đáp ứng được. Tốc độ truyền dữ liệu trên đường truyền còn được gọi là thông lượng của đường truyền - thường được tính bằng số lượng bit được truyền đi trong một giây (Bps). Thông lượng còn được đo bằng đơn vị khác là Baud (lấy từ tên nhà bác học - Emile Baudot). Baud biểu thị số lượng thay đổi tín hiệu trong một giây.

Ở đây Baud và Bps không phải bao giờ cũng đồng nhất. Ví dụ: nếu trên đường dây có 8 mức tín hiệu khác nhau thì mỗi mức tín hiệu tương ứng với 3 bit hay là 1 Baud tương ứng với 3 bit. Chỉ khi có 2 mức tín hiệu trong đó mỗi mức tín hiệu tương ứng với 1 bit thì 1 Baud mới tương ứng với 1 bit.

## II. Phân loại mạng máy tính

Do hiện nay mạng máy tính được phát triển khắp nơi với những ứng dụng ngày càng đa dạng cho nên việc phân loại mạng máy tính là một việc rất phức tạp. Người ta có thể chia các mạng máy tính theo khoảng cách địa lý ra làm hai loại: Mạng diện rộng và Mạng cục bộ.

- **Mạng cục bộ (Local Area Networks - LAN)** là mạng được thiết lập để liên kết các máy tính trong một khu vực như trong một toà nhà, một khu nhà.

- **Mạng diện rộng (Wide Area Networks - WAN)** là mạng được thiết lập để liên kết các máy tính của hai hay nhiều khu vực khác nhau như giữa các thành phố hay các tỉnh.

Sự phân biệt trên chỉ có tính chất ước lệ, các phân biệt trên càng trở nên khó xác định với việc phát triển của khoa học và kỹ thuật cũng như các phương tiện truyền dẫn. Tuy nhiên với sự phân biệt trên phương diện địa lý đã đưa tới việc phân biệt trong nhiều đặc tính khác nhau của hai loại mạng trên, việc nghiên cứu các phân biệt đó cho ta hiểu rõ hơn về các loại mạng.

## III. Sự phân biệt giữa mạng cục bộ và mạng diện rộng

Mạng cục bộ và mạng diện rộng có thể được phân biệt bởi: địa phương hoạt động, tốc độ đường truyền và tỷ lệ lỗi trên đường truyền, chủ quản của mạng, đường đi của thông tin trên mạng, dạng chuyển giao thông tin.

***Địa phương hoạt động*:** Liên quan đến khu vực địa lý thì mạng cục bộ sẽ là mạng liên kết các máy tính nằm ở trong một khu vực nhỏ. Khu vực có thể bao gồm một tòa nhà hay là một khu nhà... Điều đó hạn chế bởi khoảng cách đường dây cáp

được dùng để liên kết các máy tính của mạng cục bộ (Hạn chế đó còn là hạn chế của khả năng kỹ thuật của đường truyền dữ liệu). Ngược lại mạng diện rộng là mạng có khả năng liên kết các máy tính trong một vùng rộng lớn như là một thành phố, một miền, một đất nước, mạng diện rộng được xây dựng để nối hai hoặc nhiều khu vực địa lý riêng biệt.

***Tốc độ đường truyền và tỷ lệ lỗi trên đường truyền*:** Do các đường cáp của mạng cục bộ được xây dựng trong một khu vực nhỏ cho nên nó ít bị ảnh hưởng bởi tác động của thiên nhiên (như là sấm chớp, ánh sáng...). Điều đó cho phép mạng cục bộ có thể truyền dữ liệu với tốc độ cao mà chỉ chịu một tỷ lệ lỗi nhỏ. Ngược lại với mạng diện rộng do phải truyền ở những khoảng cách khá xa với những đường truyền dẫn dài có khi lên tới hàng ngàn km. Do vậy mạng diện rộng không thể truyền với tốc độ quá cao vì khi đó tỉ lệ lỗi sẽ trở nên khó chấp nhận được.

Mạng cục bộ thường có tốc độ truyền dữ liệu từ 4 đến 16 Mbps và đạt tới 100 Mbps nếu dùng cáp quang. Còn phần lớn các mạng diện rộng cung cấp đường truyền có tốc độ thấp hơn nhiều như T1 với 1.544 Mbps hay E1 với 2.048 Mbps.

(Ở đây bps (Bit Per Second) là một đơn vị trong truyền thông tương đương với 1 bit được truyền trong một giây, ví dụ như tốc độ đường truyền là 1 Mbps tức là có thể truyền tối đa 1 Megabit trong 1 giây trên đường truyền đó).

Thông thường trong mạng cục bộ tỷ lệ lỗi trong truyền dữ liệu vào khoảng $1/10^7$-$10^8$ còn trong mạng diện rộng thì tỷ lệ đó vào khoảng $1/10^6$ - $10^7$

***Chủ quản và điều hành của mạng:*** Do sự phức tạp trong việc xây dựng, quản lý, duy trì các đường truyền dẫn nên khi xây dựng mạng diện rộng người ta thường sử dụng các đường truyền được thuê từ các công ty viễn thông hay các nhà cung cấp dịch vụ truyền số liệu. Tùy theo cấu trúc của mạng những đường truyền đó thuộc cơ quan quản lý khác nhau như các nhà cung cấp đường truyền nội hạt, liên tỉnh, liên quốc gia. Các đường truyền đó phải tuân thủ các quy định của chính phủ các khu vực có đường dây đi qua như: tốc độ, việc mã hóa.

Còn đối với mạng cục bộ thì công việc đơn giản hơn nhiều, khi một cơ quan cài đặt mạng cục bộ thì toàn bộ mạng sẽ thuộc quyền quản lý của cơ quan đó.

***Đường đi của thông tin trên mạng:*** Trong mạng cục bộ thông tin được đi theo con đường xác định bởi cấu trúc của mạng. Khi người ta xác định cấu trúc của mạng thì thông tin sẽ luôn luôn đi theo cấu trúc đã xác định đó. Còn với mạng diện rộng dữ liệu cấu trúc có thể phức tạp hơn nhiều do việc sử dụng các dịch vụ truyền dữ liệu. Trong quá trình hoạt động các điểm nút có thể thay đổi đường đi của các thông tin khi phát hiện ra có trục trặc trên đường truyền hay khi phát hiện có quá nhiều thông tin cần truyền giữa hai điểm nút nào đó. Trên mạng diện rộng thông tin có thể có các con đường đi khác nhau, điều đó cho phép có thể sử dụng tối đa các năng lực của đường truyền hay nâng cao điều kiện an toàn trong truyền dữ liệu.

***Dạng chuyển giao thông tin:*** Phần lớn các mạng diện rộng hiện nay được phát triển cho việc truyền đồng thời trên đường truyền nhiều dạng thông tin khác nhau như: video, tiếng nói, dữ liệu... Trong khi đó các mạng cục bộ chủ yếu phát triển trong việc truyền dữ liệu thông thường. Điều này có thể giải thích do việc truyền các dạng thông tin như video, tiếng nói trong một khu vực nhỏ ít được quan tâm hơn như khi truyền qua những khoảng cách lớn.

Các hệ thống mạng hiện nay ngày càng phức tạp về chất lượng, đa dạng về chủng loại và phát triển rất nhanh về chất. Trong sự phát triển đó số lượng những nhà sản xuất từ phần mềm, phần cứng máy tính, các sản phẩm viễn thông cũng tăng nhanh với nhiều sản phẩm đa dạng. Chính vì vậy vai trò chuẩn hóa cũng mang những ý nghĩa quan trọng. Tại các nước các cơ quan chuẩn quốc gia đã đưa ra các những chuẩn về phần cứng và các quy định về giao tiếp nhằm giúp cho các nhà sản xuất có thể làm ra các sản phẩm có thể kết nối với các sản phẩm do hãng khác sản xuất.

Chương 3

# Mô hình truyền thông

## I. Sự cần thiết phải có mô hình truyền thông

Để một mạng máy tính trở một môi trường truyền dữ liệu thì nó cần phải có những yếu tố sau:

- Mỗi máy tính cần phải có một địa chỉ phân biệt trên mạng.
- Việc chuyển dữ liệu từ máy tính này đến máy tính khác do mạng thực hiện thông qua những quy định thống nhất gọi là giao thức của mạng.

Khi các máy tính trao đổi dữ liệu với nhau thì một quá trình truyền giao dữ liệu đã được thực hiện hoàn chỉnh. Ví dụ như để thực hiện việc truyền một file giữa một máy tính với một máy tính khác cùng được gắn trên một mạng các công việc sau đây phải được thực hiện:

- Máy tính cần truyền cần biết địa chỉ của máy nhận.
- Máy tính cần truyền phải xác định được máy tính nhận đã saün sàng nhận thông tin
- Chương trình gửi file trên máy truyền cần xác định được rằng chương trình nhận file trên máy nhận đã saün sàng tiếp nhận file.
- Nếu cấu trúc file trên hai máy không giống nhau thì một máy phải làm nhiệm vụ chuyển đổi file từ dạng này sang dạng kia.
- Khi truyền file máy tính truyền cần thông báo cho mạng biết địa chỉ của máy nhận để các thông tin được mạng đưa tới đích.

Điều trên đó cho thấy giữa hai máy tính đã có một sự phối hợp hoạt động ở mức độ cao. Bây giờ thay vì chúng ta xét cả quá trình trên như là một quá trình chung thì chúng ta sẽ chia quá trình trên ra thành một số công đoạn và mỗi công đoạn con hoạt động một cách độc lập với nhau. Ở đây chương trình truyền nhận file của mỗi máy tính được chia thành ba module là: Module truyền và nhận File, Module truyền thông và Module tiếp cận mạng. Hai module tương ứng sẽ thực hiện việc trao đổi với nhau trong đó:

- *Module truyền và nhận file* cần được thực hiện tất cả các nhiệm vụ trong các ứng dụng truyền nhận file. Ví dụ: truyền nhận thông số về file, truyền nhận

các mẫu tin của file, thực hiện chuyển đổi file sang các dạng khác nhau nếu cần. Module truyền và nhận file không cần thiết phải trực tiếp quan tâm tới việc truyền dữ liệu trên mạng như thế nào mà nhiệm vụ đó được giao cho Module truyền thông.

- *Module truyền thông* quan tâm tới việc các máy tính đang hoạt động và saün sàng trao đổi thông tin với nhau. Nó còn kiểm soát các dữ liệu sao cho những dữ liệu này có thể trao đổi một cách chính xác và an toàn giữa hai máy tính. Điều đó có nghĩa là phải truyền file trên nguyên tắc đảm bảo an toàn cho dữ liệu, tuy nhiên ở đây có thể có một vài mức độ an toàn khác nhau được dành cho từng ứng dụng. Ở đây việc trao đổi dữ liệu giữa hai máy tính không phụ thuộc vào bản chất của mạng đang liên kết chúng. Những yêu cầu liên quan đến mạng đã được thực hiện ở module thứ ba là module tiếp cận mạng và nếu mạng thay đổi thì chỉ có module tiếp cận mạng bị ảnh hưởng.

- *Module tiếp cận mạng* được xây dựng liên quan đến các quy cách giao tiếp với mạng và phụ thuộc vào bản chất của mạng. Nó đảm bảo việc truyền dữ liệu từ máy tính này đến máy tính khác trong mạng.

Như vậy thay vì xét cả quá trình truyền file với nhiều yêu cầu khác nhau như một tiến trình phức tạp thì chúng ta có thể xét quá trình đó với nhiều tiến trình con phân biệt dựa trên việc trao đổi giữa các Module tương ứng trong chương trình truyền file. Cách này cho phép chúng ta phân tích kỹ quá trình file và dễ dàng trong việc viết chương trình.

Việc xét các module một cách độc lập với nhau như vậy cho phép giảm độ phức tạp cho việc thiết kế và cài đặt. Phương pháp này được sử dụng rộng rãi trong việc xây dựng mạng và các chương trình truyền thông và được gọi là phương pháp phân tầng (layer).

Nguyên tắc của phương pháp phân tầng là:

- Mỗi hệ thống thành phần trong mạng được xây dựng như một cấu trúc nhiều tầng và đều có cấu trúc giống nhau như: số lượng tầng và chức năng của mỗi tầng.

- Các tầng nằm chồng lên nhau, dữ liệu được chỉ trao đổi trực tiếp giữa hai tầng kề nhau từ tầng trên xuống tầng dưới và ngược lại.

- Cùng với việc xác định chức năng của mỗi tầng chúng ta phải xác định mối quan hệ giữa hai tầng kề nhau. Dữ liệu được truyền đi từ tầng cao nhất của hệ thống truyền lần lượt đến tầng thấp nhất sau đó truyền qua đường nối vật lý dưới dạng các bit tới tầng thấp nhất của hệ thống nhận, sau đó dữ liệu được truyền ngược lên lần lượt đến tầng cao nhất của hệ thống nhận.

- Chỉ có hai tầng thấp nhất có liên kết vật lý với nhau còn các tầng trên cùng thứ tư chỉ có các liên kết logic với nhau. Liên kết logic của một tầng được thực hiện thông qua các tầng dưới và phải tuân theo những quy định chặt chẽ, các quy định đó được gọi giao thức của tầng.


*Hình 3.1: Mô hình phân tầng gồm N tầng*

## II. Mô hình truyền thông đơn giản 3 tầng

Nói chung trong truyền thông có sự tham gia của các thành phần: các chương trình ứng dụng, các chương trình truyền thông, các máy tính và các mạng. Các chương trình ứng dụng là các chương trình của người sử dụng được thực hiện trên máy tính và có thể tham gia vào quá trình trao đổi thông tin giữa hai máy tính. Trên một máy tính với hệ điều hành đa nhiệm (như Windows, UNIX) thường được thực hiện đồng thời nhiều ứng dụng trong đó có những ứng dụng liên quan đến mạng và các ứng dụng khác. Các máy tính được nối với mạng và các dữ liệu được trao đổi thông qua mạng từ máy tính này đến máy tính khác.

Việc gửi dữ liệu được thực hiện giữa một ứng dụng với một ứng dụng khác trên hai máy tính khác nhau thông qua mạng được thực hiện như sau: Ứng dụng gửi chuyển dữ liệu cho chương trình truyền thông trên máy tính của nó, chương trình truyền thông sẽ gửi chúng tới máy tính nhận. Chương trình truyền thông trên máy nhận sẽ tiếp nhận dữ liệu, kiểm tra nó trước khi chuyển giao cho ứng dụng đang chờ dữ liệu.

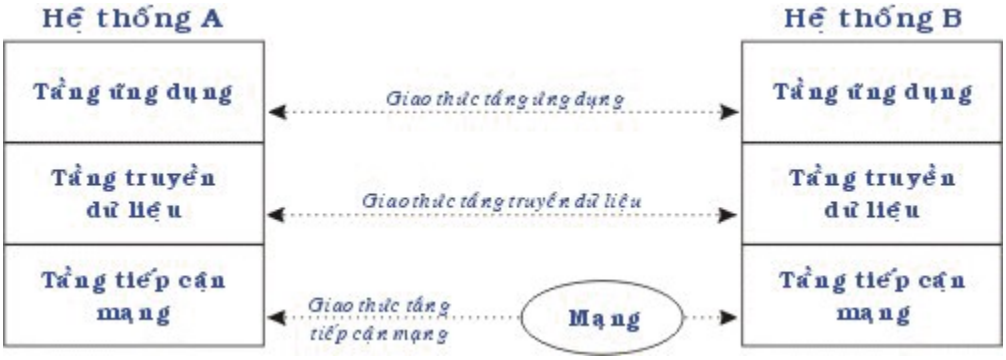
Với mô hình truyền thông đơn giản người ta chia chương trình truyền thông thành ba tầng không phụ thuộc vào nhau là: tầng ứng dụng, tầng chuyển vận và tầng tiếp cận mạng.

- ***Tầng tiếp cận mạng*** liên quan tới việc trao đổi dữ liệu giữa máy tính và mạng mà nó được nối vào. Để dữ liệu đến được đích máy tính gửi cần phải chuyển địa chỉ của máy tính nhận cho mạng và qua đó mạng sẽ chuyển các thông tin tới đích. Ngoài ra máy gửi có thể sử dụng một số phục vụ khác nhau mà mạng cung cấp như gửi ưu tiên, tốc độ cao. Trong tầng này có thể có nhiều

phần mềm khác nhau được sử dụng phụ thuộc vào các loại của mạng ví dụ như mạng chuyển mạch, mạng chuyển mạch gói, mạng cục bộ.

- ***Tầng truyền dữ liệu*** thực hiện quá trình truyền thông không liên quan tới mạng và nằm ở trên tầng tiếp cận mạng. Tầng truyền dữ liệu không quan tâm tới bản chất các ứng dụng đang trao đổi dữ liệu mà quan tâm tới làm sao cho các dữ liệu được trao đổi một cách an toàn. Tầng truyền dữ liệu đảm bảo các dữ liệu đến được đích và đến theo đúng thứ tự mà chúng được xử lý. Trong tầng truyền dữ liệu người ta phải có những cơ chế nhằm đảm bảo sự chính xác đó và rõ ràng các cơ chế này không phụ thuộc vào bản chất của từng ứng dụng và chúng sẽ phục vụ cho tất cả các ứng dụng.

- ***Tầng ứng dụng*** sẽ chứa các module phục vụ cho tất cả những ứng dụng của người sử dụng. Với các loại ứng dụng khác nhau (như là truyền file, truyền thư mục) cần các module khác nhau.




*Hình 3.2 Mô hình truyền thông 3 tầng*

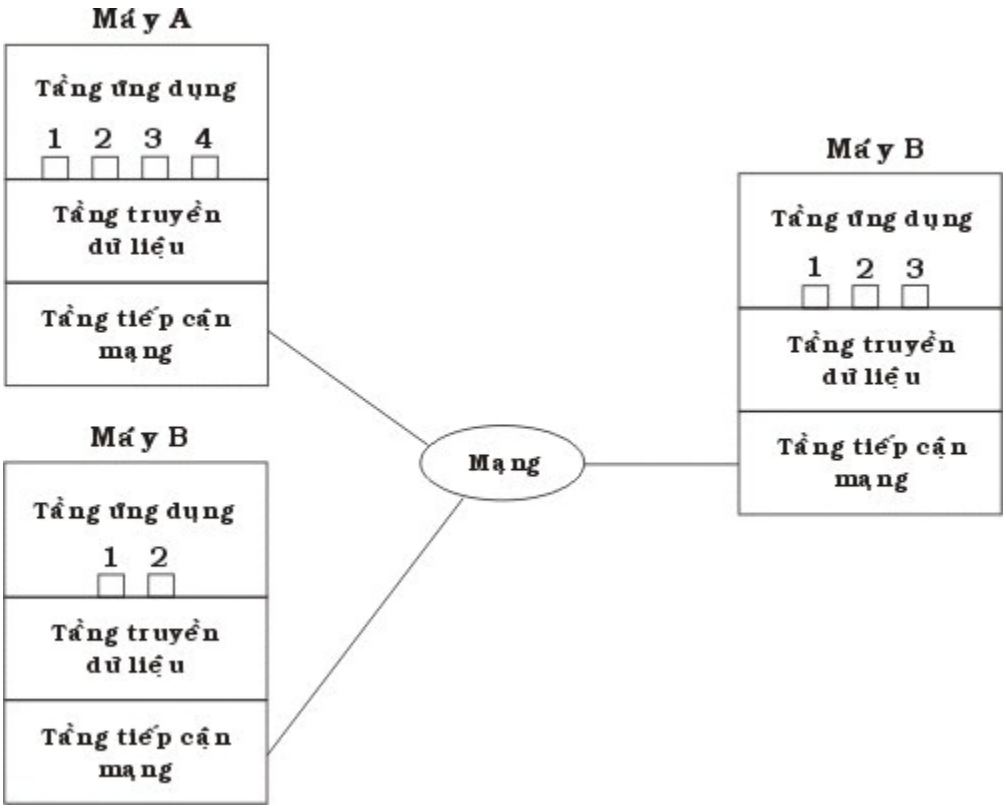
Trong một mạng với nhiều máy tính, mỗi máy tính một hay nhiều ứng dụng thực hiện đồng thời (Tại đây ta xét trên một máy tính trong một thời điểm có thể chạy nhiều ứng dụng và các ứng dụng đó có thể thực hiện đồng thời việc truyền dữ liệu qua mạng). Một ứng dụng khi cần truyền dữ liệu qua mạng cho một ứng dụng khác cần phải gọi 1 module tầng ứng dụng của chương trình truyền thông trên máy của mình, đồng thời ứng dụng kia cũng sẽ gọi 1 module tầng ứng dụng trên máy của nó. Hai module ứng dụng sẽ liên kết với nhau nhằm thực hiện các yêu cầu của các chương trình ứng dụng.

Các ứng dụng đó sẽ trao đổi với nhau thông qua mạng, tuy nhiên trong 1 thời điểm trên một máy có thể có nhiều ứng dụng cùng hoạt động và để việc truyền thông được chính xác thì các ứng dụng trên một máy cần phải có một địa chỉ riêng biệt. Rõ ràng cần có hai lớp địa chỉ:

- Mỗi máy tính trên mạng cần có một địa chỉ mạng của mình, hai máy tính trong cùng một mạng không thể có cùng địa chỉ, điều đó cho phép mạng có thể truyền thông tin đến từng máy tính một cách chính xác.

- Mỗi một ứng dụng trên một máy tính cần phải có địa chỉ phân biệt trong máy tính đo. Nó cho phép tầng truyền dữ liệu giao dữ liệu cho đúng ứng dụng đang cần. Địa chỉ đó được gọi là điểm tiếp cận giao dịch. Điều đó cho thấy mỗi một ứng dụng sẽ tiếp cận các phục vụ của tầng truyền dữ liệu một cách độc lập.

- Các module cùng một tầng trên hai máy tính khác nhau sẽ trao đổi với nhau một cách chặt chẽ theo các qui tắc xác định trước được gọi là giao thức. Một giao thức được thể hiện một cách chi tiết bởi các chức năng cần phải thực hiện như các giá trị kiểm tra lỗi, việc định dạng các dữ liệu, các quy trình cần phải thực hiện để trao đổi thông tin.




*Hình 3.3 Ví dụ mô hình truyền thông đơn giản*

Chúng ta hãy xét trong ví dụ (như hình vẽ trên): giả sử có ứng dụng có điểm tiếp cận giao dịch 1 trên máy tính A muốn gửi thông tin cho một ứng dụng khác trên máy tính B có điểm tiếp cận giao dịch 2. Ứng dụng trên máy tính A chuyển các thông tin xuống tầng truyền dữ liệu của A với yêu cầu gửi chúng cho điểm tiếp cận giao dịch 2 trên máy tính B. Tầng truyền dữ liệu máy A sẽ chuyển các thông tin xuống tầng tiếp cận mạng máy A với yêu cầu chuyển chúng cho máy tính B (Chú ý rằng mạng không cần biết địa chỉ của điểm tiếp cận giao dịch mà chỉ cần biết địa chỉ của máy tính B). Để thực hiện quá trình này, các thông tin kiểm soát cũng sẽ được truyền cùng với dữ liệu.

Đầu tiên khi ứng dụng 1 trên máy A cần gửi một khối dữ liệu nó chuyển khối đó cho tầng vận chuyển. Tầng vận chuyển có thể chia khối đó ra thành nhiều khối nhỏ phụ

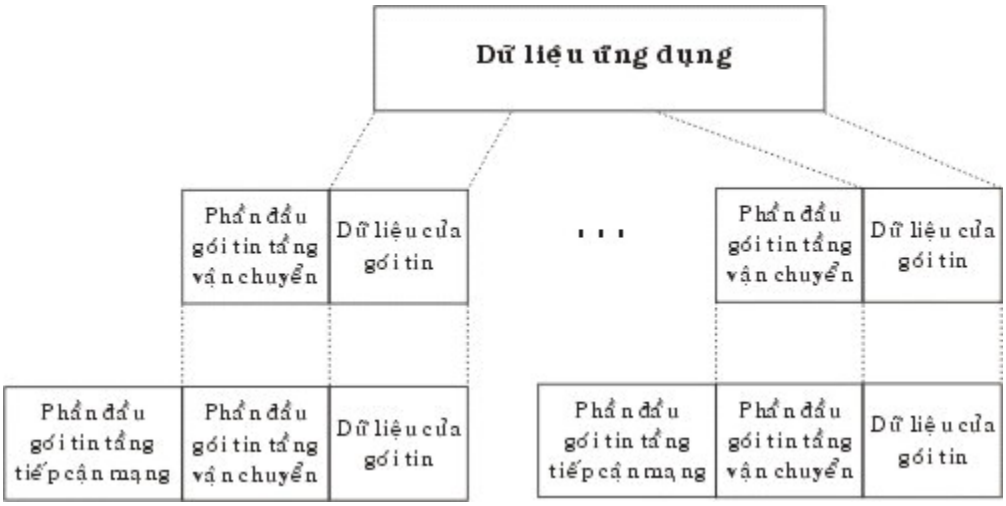
thuộc vào yêu cầu của giao thức của tầng và đóng gói chúng thành các gói tin (packet). Mỗi một gói tin sẽ được bổ sung thêm các thông tin kiểm soát của giao thức và được gọi là phần đầu (Header) của gói tin. Thông thường phần đầu của gói tin cần có:

- ***Địa chỉ của điểm tiếp cận giao dịch nơi đến* (Ở đây là 3):** khi tầng vận chuyển của máy B nhận được gói tin thì nó biết được ứng dụng nào mà nó cần giao.

- ***Số thứ tự*** của gói tin, khi tầng vận chuyển chia một khối dữ liệu ra thành nhiều gói tin thì nó cần phải đánh số thứ tự các gói tin đó. Nếu chúng đi đến đích nếu sai thứ tự thì tầng vận chuyển của máy nhận có thể phát hiện và chỉnh lại thứ tự. Ngoài ra nếu có lỗi trên đường truyền thì tầng vận chuyển của máy nhận sẽ phát hiện ra và yêu cầu gửi lại một cách chính xác.

- ***Mã sửa lỗi*:** để đảm bảo các dữ liệu được nhận một cách chính xác thì trên cơ sở các dữ liệu của gói tin tầng vận chuyển sẽ tính ra một giá trị theo một công thức có sãn và gửi nó đi trong phần đầu của gói tin. Tầng vận chuyển nơi nhận thông qua giá trị đó xác định được gói tin đó có bị lỗi trên đường truyền hay không.

Bước tiếp theo tầng vận chuyển máy A sẽ chuyển từng gói tin và địa chỉ của máy tính đích (ở đây là B) xuống tầng tiếp cận mạng với yêu cầu chuyển chúng đi. Để thực hiện được yêu cầu này tầng tiếp cận mạng cũng tạo các gói tin của mình trước khi truyền qua mạng. Tại đây giao thức của tầng tiếp cận mạng sẽ thêm các thông tin điều khiển vào phần đầu của gói tin mạng.




*Hình 3.4: Mô hình thiết lập gói tin*

Trong phần đầu gói tin mạng sẽ bao gồm địa chỉ của máy tính nhận, dựa trên địa chỉ này mạng truyền gói tin tới đích. Ngoài ra có thể có những thông số như là mức độ ưu tiên.

Như vậy thông qua mô hình truyền thông đơn giản chúng ta cũng có thể thấy được phương thức hoạt động của các máy tính trên mạng, có thể xây dựng và thay đổi các giao thức trong cùng một tầng.

## III. Các nhu cầu về chuẩn hóa đối với mạng

Trong phần trên chúng ta đã xem xét một mô hình truyền thông đơn giản, trong thực tế việc phân chia các tầng như trong mô hình trên thực sự chưa đủ. Trên thế giới hiện có một số cơ quan định chuẩn, họ đưa ra hàng loạt chuẩn về mạng tuy các chuẩn đó có tính chất khuyến nghị chứ không bắt buộc nhưng chúng rất được các cơ quan chuẩn quốc gia coi trọng.

Hai trong số các cơ quan chuẩn quốc tế là:

- **ISO (The International Standards Organization)** - Là tổ chức tiêu chuẩn quốc tế hoạt động dưới sự bảo trợ của Liên hợp Quốc với thành viên là các cơ quan chuẩn quốc gia với số lượng khoảng hơn 100 thành viên với mục đích hỗ trợ sự phát triển các chuẩn trên phạm vi toàn thế giới. Một trong những thành tựu của ISO trong lãnh vực truyền thông là mô hình hệ thống mở (Open Systems Interconnection - gọi tắt là OSI).

- **CCITT (Commité Consultatif International pour le Telegraphe et la Téléphone)** - Tổ chức tư vấn quốc tế về điện tín và điện thoại làm việc dưới sự bảo trợ của Liên Hiệp Quốc có trụ sở chính tại Geneva - Thụy sỹ. Các thành viên chủ yếu là các cơ quan bưu chính viễn thông các quốc gia. Tổ chức này có vai trò phát triển các khuyến nghị trong các lãnh vực viễn thông.

## IV. Một số mô hình chuẩn hóa

### 1. Mô hình OSI (Open Systems Interconnection)

Mô hình OSI là một cơ sở dành cho việc chuẩn hoá các hệ thống truyền thông, nó được nghiên cứu và xây dựng bởi ISO. Việc nghiên cứu về mô hình OSI được bắt đầu tại ISO vào năm 1971 với mục tiêu nhằm tới việc nối kết các sản phẩm của các hãng sản xuất khác nhau và phối hợp các hoạt động chuẩn hoá trong các lĩnh vực viễn thông và hệ thống thông tin. Theo mô hình OSI chương trình truyền thông được chia ra thành 7 tầng với những chức năng phân biệt cho từng tầng. Hai tầng đồng mức khi liên kết với nhau phải sử dụng một giao thức chung. Trong mô hình OSI có hai loại giao thức chính được áp dụng: giao thức có liên kết (connection - oriented) và giao thức không liên kết (connectionless)

- ***Giao thức có liên kết*:** trước khi truyền dữ liệu hai tầng đồng mức cần thiết lập một liên kết logic và các gói tin được trao đổi thông qua liên kết náy, việc có liên kết logic sẽ nâng cao độ an toàn trong truyền dữ liệu.

- ***Giao thức không liên kết*:** trước khi truyền dữ liệu không thiết lập liên kết logic và mỗi gói tin được truyền độc lập với các gói tin trước hoặc sau nó.

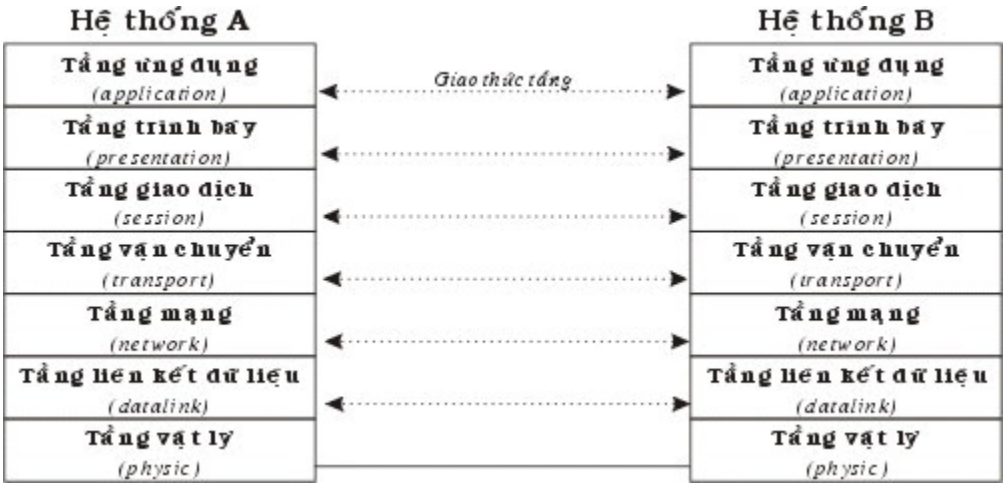
Nhiệm vụ của các tầng trong mô hình OSI:

- **Tầng ứng dụng (Application layer)**: tầng ứng dụng quy định giao diện giữa người sử dụng và môi trường OSI, nó cung cấp các phương tiện cho người sử dụng truy cập vả sử dụng các dịch vụ củ mô hình OSI.

- **Tầng trình bày (Presentation layer)**: tầng trình bày chuyển đổi các thông tin từ cú pháp người sử dụng sang cú pháp để truyền dữ liệu, ngoài ra nó có thể nén dữ liệu truyền và mã hóa chúng trước khi truyền để bảo mật.

- **Tầng giao dịch (Session layer)**: tầng giao dịch quy định một giao diện ứng dụng cho tầng vận chuyển sử dụng. Nó xác lập ánh xa giữa các tên đặt địa chỉ, tạo ra các tiếp xúc ban đầu giữa các máy tính khác nhau trên cơ sở các giao dịch truyền thông. Nó đặt tên nhất quán cho mọi thành phần muốn đối thoại riêng với nhau.

- **Tầng vận chuyển (Transport layer)**: tầng vận chuyển xác định địa chỉ trên mạng, cách thức chuyển giao gói tin trên cơ sở trực tiếp giữa hai đầu mút (end-to-end). Để bảo đảm được việc truyền ổn định trên mạng tầng vận chuyển thường đánh số các gói tin và đảm bảo chúng chuyển theo thứ tự.




*Hình 3.5: Mô hình 7 tầng OSI*

- **Tầng mạng (Network layer)**: tầng mạng có nhiệm vụ xác định việc chuyển hướng, vạch đường các gói tin trong mạng, các gói tin này có thể phải đi qua nhiều chặng trước khi đến được đích cuối cùng.

- **Tầng liên kết dữ liệu (Data link layer):** tầng liên kết dữ liệu có nhiệm vụ xác định cơ chế truy nhập thông tin trên mạng, các dạng thức chung trong các gói tin, đóng các gói tin...

- **Tầng vật lý (Phisical layer)**: tầng vật lý cung cấp phương thức truy cập vào đường truyền vật lý để truyền các dòng Bit không cấu trúc, ngoài ra nó cung cấp các chuẩn về điện, dây cáp, đầu nối, kỹ thuật nối mạch điện, điện áp, tốc độ cáp truyền dẫn, giao diện nối kết và các mức nối kết..

### 2. Mô hình SNA (Systems Netword Architecture)

Tháng 9/1973, Hãng IBM giới thiệu một kiến trúc mạng máy tính SNA (System Network Architecture). Đến năm 1977 đã có 300 trạm SNA được cài đặt. Cuối năm 1978, số lượng đã tăng lên đến 1250, rồi cứ theo đà đó cho đến nayđã có 20.000 trạm SNA đang được hoạt động. Qua con số này chúng ta có thể hình dung được mức độ quan trọng và tầm ảnh hưởng của SNA trên toàn thế giới.

Cần lưu ý rằng SNA không là một chuẩn quốc tế chính thức như OSI nhưng do vai trò to lớn của hãng IBM trên thị trường CNTT nên SNA trở thành một loại chuẩn thực tế và khá phổ biến. SNA là một đặc tả gồm rất nhiều tài liệu mô tả kiến trúc của mạng xử lý dữ liệu phân tán. Nó định nghĩa các quy tắc và các giao thức cho sự tương tác giữa các thành phần (máy tính, trạm cuối, phần mềm) trong mạng.

SNA được tổ chức xung quanh khái niệm miền (domain). Một SNA domain là một điểm điều khiển các dịch vụ hệ thống (Systems Services control point - SSCP) và nó sẽ điều khiển tất cả các tài nguyên đó, Các tài nguyên ở đây có thể là các đơn vị vật lý, các đơn vị logic, các liên kết dữ liệu và các thiết bị. Có thể ví SSCP như là "trái tim và khối óc" của SNA. Nó điều khiển SNA domain bằng cách gói các lệnh tới một đơn vị vật lý, đơn vị vật lý này sau khi nhận được lệnh sẽ quản lý tất cả các tài nguyên trực tiếp với nó. đơn vị vật lý thực sự là một "đối tác" của SSCP và chứa một tập con các khả năng của SSCP. Các Đơn vị vật lý đảm nhiệm việc quản lý của mỗi nút SNA.

SNA phân biệt giữa các nút miền con (Subarea node) và các nút ngoại vi (peripheral node).

- Một nút miền con có thể dẫn đường cho dữ liệu của người sử dụng qua toàn bộ mạng. Nó dùng địa chỉ mạng và một số hiệu đường (router suember) để xác định đường truyền đi tới nút kế tiếp trong mạng.

- Một nút ngoại vi có tính cục bộ hơn. Nó không dẫn đường giữa các nút miền con. Các nút được nối và điều khiển theo giao thức SDLC (Synchronous Data Link Control). Mỗi nút ngoại vi chỉ liên lạc được với nút miền con mà nó nối vào.

Mạng SNA dựa trên cơ chế phân tầng, trước đây thì 2 hệ thống ngang hàng không được trao đổi trực tiếp. Sau này phát triển thành SNA mở rộng: Lúc này hai tầng ngang hàng nhau có thể trao đổi trực tiếp. Với 6 tầng có tên gọi và chức năng tất như sau:

**Tầng quản trị chức năng SNA (SNA Function Manegement)** Tầng này thật ra có thể chia tầng này làm hai tầng như sau:

**Tầng dịch vụ giao tác (Transaction)** cung cấp các dịch vụ ứng dụng đến người dùng một mạng SNA. Những dịch vụ đó như : DIA cung cấp các tài liệu phân bố giữa các hệ thống văn phòng, SNA DS (văn phòng dịch vụ phân phối) cho việc truyền thông bất đồng bộ giữa các ứng dụng phân tán và hệ thống văn phòng. Tầng dịch vụ giao tác cũng cung cấp các dịch vụ và cấu hình, các dịch vụ quản lý để điều khiển các hoạt động mạng.

**Tầng dịch vụ trình diễn (Presentation Services):** tầng này thì liên quan với sự hiển thị các ứng dụng, người sử dụng đầu cuối và các dữ liệu hệ thống. Tầng này cũng định nghĩa các giao thức cho việc truyền thông giữa các chương trình và điều khiển truyền thông ở mức hội thoại.

**Tầng kiểm soát luồng dữ liệu (Data flow control)** tầng này cung cấp các dịch vụ điều khiểnluồng lưu thông cho các phiên từ logic này đến đơn vị logic khác (LU - LU). Nó thực hiện điều này bằng cách gán các số trình tự, các yêu cầu và đáp ứng, thực hiện các giao thức yêu cầu về đáp ứng giao dịch và hợp tác giữa các giao dịch gởi và nhận. Nói chung nó yểm trợ phương thức khai thác hai chiều đồng thời (Full duplex).

**Tầng kiểm soát truyền (Transmission control):** Tầng này cung cấp các điều khiển cơ bản của các phần tài nguyên truyền trong mạng, bằng cách xác định số trình tự nhận được, và quản lý việc theo dõi mức phiên. Tầng này cũng hỗ trợ cho việc mã hóa dữ liệu và cung cấp hệ thống hỗ trợ cho các nút ngoại vi.

**Tầng kiểm soát đường dẫn (Path control):** Tầng này cung cấp các giao thức để tìm đường cho một gói tin qua mạng SNA và để kết nối với các mạng SNA khác, đồng thời nó cũng kiểm soát các đường truyền này.

**Tầng kiểm soát liên kết dữ liệu (Data Link Control):** Tầng này cung cấp các giao thức cho việc truyền các gói tin thông qua đường truyền vật lý giữa hai node và cũng cung cấp các điều khiển lưu thông và phục hồi lỗi, các hỗ trợ cho tầng này là các giao thức SDLC, System/370, X25, IEEE 802.2 và 802.5.

**Tầng kiểm soát vật lý (Physical control):** Tầng này cung cấp một giao diện vật lý cho bất cứ môi trường truyền thông nào mà gắn với nó. Tầng nào định nghĩa các đặc trưng của tín hiệu cần để thiết lập, duy trì và kết thúc các đường nối vật lý cho việc hỗ trợ kết nối.

<table>
<tr><th colspan="2">SNA</th><th>OSI</th></tr>
<tr><td rowspan="2">Tầng quản trị chức năng SNA<br>(SNA Function Management)</td><td>(Transaction)</td><td>Tầng ứng dụng<br>(application)</td></tr>
<tr><td>(Presentation Services)</td><td>Tầng trình bày<br>(presentation)</td></tr>
<tr><td colspan="2">Tầng kiểm soát luồng dữ liệu<br>(Data flow control)</td><td>Tầng giao dịch<br>(session)</td></tr>
<tr><td colspan="2">Tầng kiểm soát truyền<br>(Transmission control)</td><td>Tầng vận chuyển<br>(transport)</td></tr>
<tr><td colspan="2">Tầng kiểm soát đường dẫn<br>(Path control)</td><td>Tầng mạng<br>(network)</td></tr>
<tr><td colspan="2">Tầng kiểm soát liên kết dữ liệu<br>(Data Link Control)</td><td>Tầng liên kết dữ liệu<br>(datalink)</td></tr>
<tr><td colspan="2">Tầng kiểm soát vật lý<br>(Physical control)</td><td>Tầng vật lý<br>(physic)</td></tr>
</table>

*Hình 3.6: Tương ứng các tầng các kiến trúc SNI và OSI*

**Chương 4**

# Mô hình kết nối các hệ thống mở

# Open Systems Interconection

Việc nghiên cứu về OSI được bắt đầu tại ISO vào năm 1971 với các mục tiêu nhằm nối kết các sản phẩm của các hãng sản xuất khác. Ưu điểm chính của OSI là ở chỗ nó hứa hẹn giải pháp cho vấn đề truyền thông giữa các máy tính không giống nhau. Hai hệ thống, dù có khác nhau đều có thể truyền thông với nhau một các hiệu quả nếu chúng đảm bảo những điều kiện chung sau đây:

Chúng cài đặt cùng một tập các chức năng truyền thông.

Các chức năng đó được tổ chức thành cùng một tập các tầng. các tầng đồng mức phải cung cấp các chức năng như nhau.

Các tầng đồng mức khi trao đổi với nhau sử dụng chung một giao thức

Mô hình OSI tách các mặt khác nhau của một mạng máy tính thành bảy tầng theo mô hình phân tầng. Mô hình OSI là một khung mà các tiêu chuẩn lập mạng khác nhau có thể khớp vào. Mô hình OSI định rõ các mặt nào của hoạt động của mạng có thể nhằm đến bởi các tiêu chuẩn mạng khác nhau. Vì vậy, theo một nghĩa nào đó, mô hình OSI là một loại tiêu chuẩn của các chuẩn.

## I. Nguyên tắc sử dụng khi định nghĩa các tầng hệ thống mở:

Sau đây là các nguyên tắc mà ISO quy định dùng trong quá trình xây dựng mô hình OSI

- Không định nghĩa quá nhiều tầng để việc xác định và ghép nối các tầng không quá phức tạp.
- Tạo các ranh giới các tầng sao cho việc giải thích các phục vụ và số các tương tác qua lại hai tầng là nhỏ nhất.
- Tạo các tầng riêng biệt cho các chức năng khác biệt nhau hoàn toàn về kỹ thuật sử dụng hoặc quá trình thực hiên.
- Các chức năng giống nhau được đặt trong cùng một tầng.
- Lựa chọn ranh giới các tầng tại các điểm mà những thử nghiệm trong quá khứ thành công.

- Các chức năng được xác định sao cho chúng có thể dễ dàng xác định lại, và các nghi thức của chúng có thể thay đổi trên mọi hướng.

- Tạo ranh giới các tầng mà ở đó cần có những mức độ trừu tượng khác nhau trong việc sử dụng số liệu.

- Cho phép thay đổi các chức năng hoặc giao thức trong tầng không ảnh hưởng đến các tầng khác.

- Tạo các ranh giới giữa mỗi tầng với tầng trên và dưới nó.

**II. Các giao thức trong mô hình OSI**

Trong mô hình OSI có hai loại giao thức chính được áp dụng: giao thức có liên kết (connection - oriented) và giao thức không liên kết (connectionless).

- *Giao thức có liên kết*: trước khi truyền dữ liệu hai tầng đồng mức cần thiết lập một liên kết logic và các gói tin được trao đổi thông qua liên kết náy, việc có liên kết logic sẽ nâng cao độ an toàn trong truyền dữ liệu.

- *Giao thức không liên kết*: trước khi truyền dữ liệu không thiết lập liên kết logic và mỗi gói tin được truyền độc lập với các gói tin trước hoặc sau nó.

Như vậy với giao thức có liên kết, quá trình truyền thông phải gồm 3 giai đoạn phân biệt:

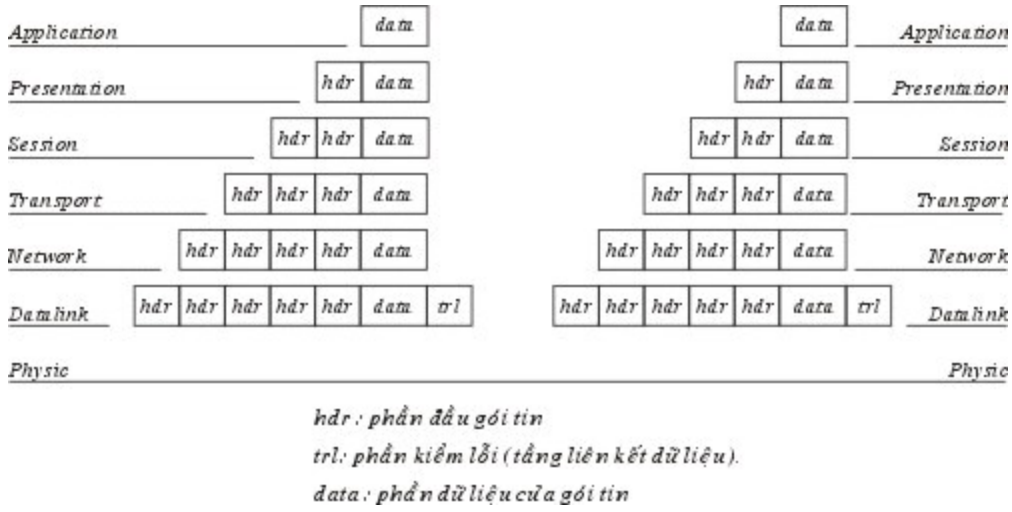
- *Thiết lập liên kết (logic):* hai thực thể đồng mức ở hai hệ thống thương lượng với nhau về tập các tham số sẽ sử dụng trong giai đoạn sau (truyền dữ liệu).

- *Truyền dữ liệu*: dữ liệu được truyền với các cơ chế kiểm soát và quản lý kèm theo (như kiểm soát lỗi, kiểm soát luồng dữ liệu, cắt/hợp dữ liệu...) để tăng cường độ tin cậy và hiệu quả của việc truyền dữ liệu.

- *Hủy bỏ liên kết (logic):* giải phóng tài nguyên hệ thống đã được cấp phát cho liên kết để dùng cho liên kết khác.

Đối với giao thức không liên kết thì chỉ có duy nhất một giai đoạn truyền dữ liệu mà thôi.

Gói tin của giao thức: Gói tin (Packet) được hiểu như là một đơn vị thông tin dùng trong việc liên lạc, chuyển giao dữ liệu trong mạng máy tính. Những thông điệp (message) trao đổi giữa các máy tính trong mạng, được tạo dạng thành các gói tin ở máy nguồn. Và những gói tin này khi đích sẽ được kết hợp lại thành thông điệp ban đầu. Một gói tin có thể chứa đựng các yêu cầu phục vụ, các thông tin điều khiển và dữ liệu.




*Hình 4.1: Phương thức xác lập các gói tin trong mô hình OSI*

Trên quan điểm mô hình mạng phân tầng tầng mỗi tầng chỉ thực hiện một chức năng là nhận dữ liệu từ tầng bên trên để chuyển giao xuống cho tầng bên dưới và ngược lại. Chức năng này thực chất là gắn thêm và gỡ bỏ phần đầu (header) đối với các gói tin trước khi chuyển nó đi. Nói cách khác, từng gói tin bao gồm phần đầu (header) và phần dữ liệu. Khi đi đến một tầng mới gói tin sẽ được đóng thêm một phần đầu đề khác và được xem như là gói tin của tầng mới, công việc trên tiếp diễn cho tới khi gói tin được truyền lên đường dây mạng để đến bên nhận.

Tại bên nhận các gói tin được gỡ bỏ phần đầu trên từng tầng tương ứng và đây cũng là nguyên lý của bất cứ mô hình phân tầng nào.

***Chú ý:*** Trong mô hình OSI phần kiểm lỗi của gói tin tầng liên kết dữ liệu đặt ở cuối gói tin

## III. Các chức năng chủ yếu của các tầng của mô hình OSI.

### Tầng 1: Vật lý (Physical)

Tầng vật lý (Physical layer) là tầng dưới cùng của mô hình OSI là. Nó mô tả các đặc trưng vật lý của mạng: Các loại cáp được dùng để nối các thiết bị, các loại đầu nối được dùng , các dây cáp có thể dài bao nhiêu v.v... Mặt khác các tầng vật lý cung cấp các đặc trưng điện của các tín hiệu được dùng để khi chuyển dữ liệu trên cáp từ một máy này đến một máy khác của mạng, kỹ thuật nối mạch điện, tốc độ cáp truyền dẫn.

Tầng vật lý không qui định một ý nghĩa nào cho các tín hiệu đó ngoài các giá trị nhị phân 0 và 1. Ở các tầng cao hơn của mô hình OSI ý nghĩa của các bit được truyền ở tầng vật lý sẽ được xác định.

***Ví dụ:*** Tiêu chuẩn Ethernet cho cáp xoắn đôi 10 baseT định rõ các đặc trưng điện của cáp xoắn đôi, kích thước và dạng của các đầu nối, độ dài tối đa của cáp.

Khác với các tầng khác, tầng vật lý là không có gói tin riêng và do vậy không có phần đầu (header) chứa thông tin điều khiển, dữ liệu được truyền đi theo dòng bit. Một giao thức tầng vật lý tồn tại giữa các tầng vật lý để quy định về phương thức truyền (đồng bộ, phi đồng bộ), tốc độ truyền.

Các giao thức được xây dựng cho tầng vật lý được phân chia thành phân chia thành hai loại giao thức sử dụng phương thức truyền thông dị bộ (asynchronous) và phương thức truyền thông đồng bộ (synchronous).

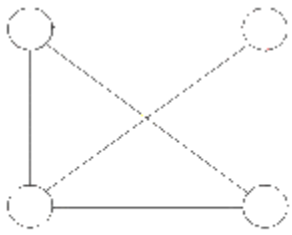
- *Phương thức truyền dị bộ*: không có một tín hiệu quy định cho sự đồng bộ giữa các bit giữa máy gửi và máy nhận, trong quá trình gửi tín hiệu máy gửi sử dụng các bit đặc biệt START và STOP được dùng để tách các xâu bit biểu diễn các ký tự trong dòng dữ liệu cần truyền đi. Nó cho phép một ký tự được truyền đi bất kỳ lúc nào mà không cần quan tâm đến các tín hiệu đồng bộ trước đó.

- *Phương thức truyền đồng bộ*: sử dụng phương thức truyền cần có đồng bộ giữa máy gửi và máy nhận, nó chèn các ký tự đặc biệt như SYN (Synchronization), EOT (End Of Transmission) hay đơn giản hơn, một cái "cờ " (flag) giữa các dữ liệu của máy gửi để báo hiệu cho máy nhận biết được dữ liệu đang đến hoặc đã đến.

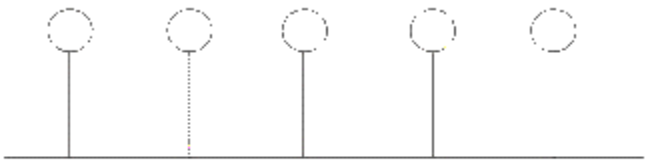
### Tầng 2: Liên kết dữ liệu (Data link)

Tầng liên kết dữ liệu (data link layer) là tầng mà ở đó ý nghĩa được gán cho các bít được truyền trên mạng. Tầng liên kết dữ liệu phải quy định được các dạng thức, kích thước, địa chỉ máy gửi và nhận của mỗi gói tin được gửi đi. Nó phải xác định cơ chế truy nhập thông tin trên mạng và phương tiện gửi mỗi gói tin sao cho nó được đưa đến cho người nhận đã định.

Tầng liên kết dữ liệu có hai phương thức liên kết dựa trên cách kết nối các máy tính, đó là phương thức "một điểm - một điểm" và phương thức "một điểm - nhiều điểm". Với phương thức "một điểm - một điểm" các đường truyền riêng biệt được thiết lập để nối các cặp máy tính lại với nhau. Phương thức "một điểm - nhiều điểm " tất cả các máy phân chia chung một đường truyền vật lý.



*một điểm - một điểm*



*một điểm - nhiều điểm*

*Hình 4.2: Các đường truyền kết nối kiểu "một điểm - một điểm" và "một điểm - nhiều điểm".*

Tầng liên kết dữ liệu cũng cung cấp cách phát hiện và sửa lỗi cơ bản để đảm bảo cho dữ liệu nhận được giống hoàn toàn với dữ liệu gửi đi. Nếu một gói tin có lỗi không sửa được, tầng liên kết dữ liệu phải chỉ ra được cách thông báo cho nơi gửi biết gói tin đó có lỗi để nó gửi lại.

Các giao thức tầng liên kết dữ liệu chia làm 2 loại chính là các giao thức hướng ký tư và các giao thức hướng bit. Các giao thức hướng ký tự được xây dựng dựa trên các ký tự đặc biệt của một bộ mã chuẩn nào đó (như ASCII hay EBCDIC), trong khi đó các giao thức hướng bit lại dùng các cấu trúc nhị phân (xâu bit) để xây dựng các phần tử của giao thức (đơn vị dữ liệu, các thủ tục.) và khi nhận, dữ liệu sẽ được tiếp nhận lần lượt từng bit một.

### Tầng 3: Mạng (Network)

Tầng mạng (network layer) nhắm đến việc kết nối các mạng với nhau bằng cách tìm đường (routing) cho các gói tin từ một mạng này đến một mạng khác. Nó xác định việc chuyển hướng, vạch đường các gói tin trong mạng, các gói này có thể phải đi qua nhiều chặng trước khi đến được đích cuối cùng. Nó luôn tìm các tuyến truyền thông không tắc nghẽn để đưa các gói tin đến đích.

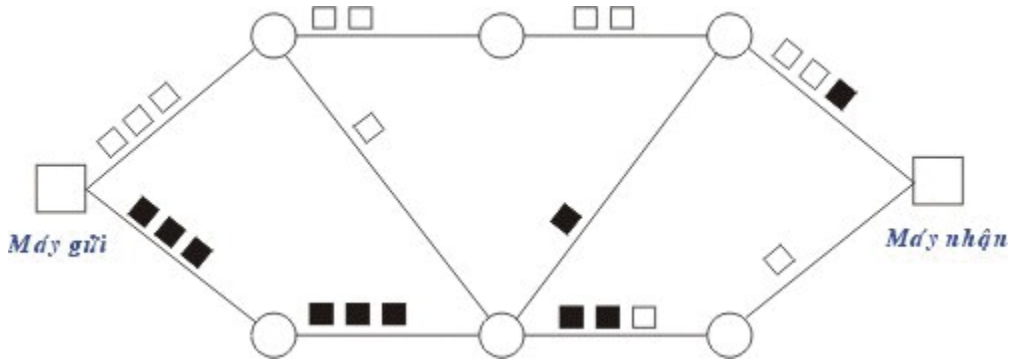
Tầng mạng cung các các phương tiện để truyền các gói tin qua mạng, thậm chí qua một mạng của mạng (network of network). Bởi vậy nó cần phải đáp ứng với nhiều kiểu mạng và nhiều kiểu dịch vụ cung cấp bởi các mạng khác nhau. hai chức năng chủ yếu của tầng mạng là chọn đường (routing) và chuyển tiếp (relaying). Tầng mạng là quan trọng nhất khi liên kết hai loại mạng khác nhau như mạng Ethernet với mạng Token Ring khi đó phải dùng một bộ tìm đường (quy định bởi tầng mạng) để chuyển các gói tin từ mạng này sang mạng khác và ngược lại.

Đối với một mạng chuyển mạch gói (packet - switched network) - gồm tập hợp các nút chuyển mạch gói nối với nhau bởi các liên kết dữ liệu. Các gói dữ liệu được truyền từ một hệ thống mở tới một hệ thống mở khác trên mạng phải được chuyển qua một chuỗi các nút. Mỗi nút nhận gói dữ liệu từ một đường vào (incoming link) rồi chuyển tiếp nó tới một đường ra (outgoing link) hướng đến đích của dữ liệu. Như vậy ở mỗi nút trung gian nó phải thực hiện các chức năng chọn đường và chuyển tiếp.

Việc chọn đường là sự lựa chọn một con đường để truyền một đơn vị dữ liệu (một gói tin chẳng hạn) từ trạm nguồn tới trạm đích của nó. Một kỹ thuật chọn đường phải thực hiện hai chức năng chính sau đây:

- Quyết định chọn đường tối ưu dựa trên các thông tin đã có về mạng tại thời điểm đó thông qua những tiêu chuẩn tối ưu nhất định.

- Cập nhật các thông tin về mạng, tức là thông tin dùng cho việc chọn đường, trên mạng luôn có sự thay đổi thường xuyên nên việc cập nhật là việc cần thiết.




*Hình 4. 3: Mô hình chuyển vận các gói tin trong mạng chuyển mạch gói*

Người ta có hai phương thức đáp ứng cho việc chọn đường là phương thức xử lý tập trung và xử lý tại chỗ.

- *Phương thức chọn đường xử lý tập trung* được đặc trưng bởi sự tồn tại của một (hoặc vài) trung tâm điều khiển mạng, chúng thực hiện việc lập ra các bảng đường đi tại từng thời điểm cho các nút và sau đó gửi các bảng chọn đường tới từng nút dọc theo con đường đã được chọn đó. Thông tin tổng thể của mạng cần dùng cho việc chọn đường chỉ cần cập nhập và được cất giữ tại trung tâm điều khiển mạng.

- *Phương thức chọn đường xử lý tại chỗ* được đặc trưng bởi việc chọn đường được thực hiện tại mỗi nút của mạng. Trong từng thời điểm, mỗi nút phải duy trì các thông tin của mạng và tự xây dựng bảng chọn đường cho mình. Như vậy các thông tin tổng thể của mạng cần dùng cho việc chọn đường cần cập nhập và được cất giữ tại mỗi nút.

Thông thường các thông tin được đo lường và sử dụng cho việc chọn đường bao gồm:

- Trạng thái của đường truyền.

- Thời gian trễ khi truyền trên mỗi đường dẫn.

- Mức độ lưu thông trên mỗi đường.

- Các tài nguyên khả dụng của mạng.

Khi có sự thay đổi trên mạng (ví dụ thay đổi về cấu trúc của mạng do sự cố tại một vài nút, phục hồi của một nút mạng, nối thêm một nút mới... hoặc thay đổi về mức độ lưu thông) các thông tin trên cần được cập nhật vào các cơ sở dữ liệu về trạng thái của mạng.

Hiện nay khi nhu cầu truyền thông đa phương tiện (tích hợp dữ liệu văn bản, đồ hoạ, hình ảnh, âm thanh) ngày càng phát triển đòi hỏi các công nghệ truyền dẫn tốc độ cao nên việc phát triển các hệ thống chọn đường tốc độ cao đang rất được quan tâm.

### Tầng 4: Vận chuyển (Transport)

Tầng vận chuyển cung cấp các chức năng cần thiết giữa tầng mạng và các tầng trên. nó là tầng cao nhất có liên quan đến các giao thức trao đổi dữ liệu giữa các hệ thống mở. Nó cùng các tầng dưới cung cấp cho người sử dụng các phục vụ vận chuyển.

Tầng vận chuyển (transport layer) là tầng cơ sở mà ở đó một máy tính của mạng chia sẻ thông tin với một máy khác. Tầng vận chuyển đồng nhất mỗi trạm bằng một địa chỉ duy nhất và quản lý sự kết nối giữa các trạm. Tầng vận chuyển cũng chia các gói tin lớn thành các gói tin nhỏ hơn trước khi gửi đi. Thông thường tầng vận chuyển đánh số các gói tin và đảm bảo chúng chuyển theo đúng thứ tự.

Tầng vận chuyển là tầng cuối cùng chịu trách nhiệm về mức độ an toàn trong truyền dữ liệu nên giao thức tầng vận chuyển phụ thuộc rất nhiều vào bản chất của tầng mạng. Người ta chia giao thức tầng mạng thành các loại sau:

- Mạng loại A: Có tỷ suất lỗi và sự cố có báo hiệu chấp nhận được (tức là chất lượng chấp nhận được). Các gói tin được giả thiết là không bị mất. Tầng vận chuyển không cần cung cấp các dịch vụ phục hồi hoặc sắp xếp thứ tự lại.

- Mạng loại B: Có tỷ suất lỗi chấp nhận được nhưng tỷ suất sự cố có báo hiệu lại không chấp nhận được. Tầng giao vận phải có khả năng phục hồi lại khi xẩy ra sự cố.

- Mạng loại C: Có tỷ suất lỗi không chấp nhận được (không tin cậy) hay là giao thức không liên kết. Tầng giao vận phải có khả năng phục hồi lại khi xảy ra lỗi và sắp xếp lại thứ tự các gói tin.

Trên cơ sở loại giao thức tầng mạng chúng ta có 5 lớp giao thức tầng vận chuyển đó là:

- *Giao thức lớp 0 (Simple Class - lớp đơn giản)*: cung cấp các khả năng rất đơn giản để thiết lập liên kết, truyền dữ liệu và hủy bỏ liên kết trên mạng "có liên kết" loại A. Nó có khả năng phát hiện và báo hiệu các lỗi nhưng không có khả năng phục hồi.

- *Giao thức lớp 1 (Basic Error Recovery Class - Lớp phục hồi lỗi cơ bản)* dùng với các loại mạng B, ở đây các gói tin (TPDU) được đánh số. Ngoài ra giao thức còn có khả năng báo nhận cho nơi gửi và truyền dữ liệu khẩn. So với giao thức lớp 0 giao thức lớp 1 có thêm khả năng phục hồi lỗi.

- *Giao thức lớp 2 (Multiplexing Class - lớp dồn kênh)* là một cải tiến của lớp 0 cho phép dồn một số liên kết chuyển vận vào một liên kết mạng duy nhất, đồng thời có thể kiểm soát luồng dữ liệu để tránh tắc nghẽn. Giao thức lớp 2 không có khả năng phát hiện và phục hồi lỗi. Do vậy nó cần đặt trên một tầng mạng loại A.

- *Giao thức lớp 3 (Error Recovery and Multiplexing Class - lớp phục hồi lỗi cơ bản và dồn kênh)* là sự mở rộng giao thức lớp 2 với khả năng phát hiện và phục hồi lỗi, nó cần đặt trên một tầng mạng loại B.

- *Giao thức lớp 4 (Error Detection and Recovery Class - Lớp phát hiện và phục hồi lỗi)* là lớp có hầu hết các chức năng của các lớp trước và còn bổ sung thêm một số khả năng khác để kiểm soát việc truyền dữ liệu.

### Tầng 5: Giao dịch (Session)

Tầng giao dịch (session layer) thiết lập "các giao dịch" giữa các trạm trên mạng, nó đặt tên nhất quán cho mọi thành phần muốn đối thoại với nhau và lập ánh xa giữa các tên với địa chỉ của chúng. Một giao dịch phải được thiết lập trước khi dữ liệu được truyền trên mạng, tầng giao dịch đảm bảo cho các giao dịch được thiết lập và duy trì theo đúng qui định.

Tầng giao dịch còn cung cấp cho người sử dụng các chức năng cần thiết để quản trị các giao dịnh ứng dụng của họ, cụ thể là:

- Điều phối việc trao đổi dữ liệu giữa các ứng dụng bằng cách thiết lập và giải phóng (một cách lôgic) các phiên (hay còn gọi là các hội thoại - dialogues)

- Cung cấp các điểm đồng bộ để kiểm soát việc trao đổi dữ liệu.

- Áp đặt các qui tắc cho các tương tác giữa các ứng dụng của người sử dụng.

- Cung cấp cơ chế "lấy lượt" (nắm quyền) trong quá trình trao đổi dữ liệu.

Trong trường hợp mạng là hai chiều luân phiên thì nẩy sinh vấn đề: hai người sử dụng luân phiên phải "lấy lượt" để truyền dữ liệu. Tầng giao dịch duy trì tương tác luân phiên bằng cách báo cho mỗi người sử dụng khi đến lượt họ được truyền dữ liệu. Vấn đề đồng bộ hóa trong tầng giao dịch cũng được thực hiện như cơ chế kiểm tra/phục hồi, dịch vụ này cho phép người sử dụng xác định các điểm đồng bộ hóa trong dòng dữ liệu đang chuyển vận và khi cần thiết có thể khôi phục việc hội thoại bắt đầu từ một trong các điểm đó

Ở một thời điểm chỉ có một người sử dụng đó quyền đặc biệt được gọi các dịch vụ nhất định của tầng giao dịch, việc phân bổ các quyền này thông qua trao đổi thẻ bài (token). Ví dụ: Ai có được token sẽ có quyền truyền dữ liệu, và khi người giữ token trao token cho người khác thi cũng có nghĩa trao quyền truyền dữ liệu cho người đó.

Tầng giao dịch có các hàm cơ bản sau:

- *Give Token* cho phép người sử dụng chuyển một token cho một người sử dụng khác của một liên kết giao dịch.
- *Please Token* cho phép một người sử dụng chưa có token có thể yêu cầu token đó.
- *Give Control* dùng để chuyển tất cả các token từ một người sử dụng sang một người sử dụng khác.

### Tầng 6: Trình bày (Presentation)

Trong giao tiếp giữa các ứng dụng thông qua mạng với cùng một dữ liệu có thể có nhiều cách biểu diễn khác nhau. Thông thường dạng biểu diễn dùng bởi ứng dụng nguồn và dạng biểu diễn dùng bởi ứng dụng đích có thể khác nhau do các ứng dụng được chạy trên các hệ thống hoàn toàn khác nhau (như hệ máy Intel và hệ máy Motorola). Tầng trình bày (Presentation layer) phải chịu trách nhiệm chuyển đổi dữ liệu gửi đi trên mạng từ một loại biểu diễn này sang một loại khác. Để đạt được điều đó nó cung cấp một dạng biểu diễn chung dùng để truyền thông và cho phép chuyển đổi từ dạng biểu diễn cục bộ sang biểu diễn chung và ngược lại.

Tầng trình bày cũng có thể được dùng kĩ thuật mã hóa để xáo trộn các dữ liệu trước khi được truyền đi và giải mã ở đầu đến để bảo mật. Ngoài ra tầng biểu diễn cũng có thể dùng các kĩ thuật nén sao cho chỉ cần một ít byte dữ liệu để thể hiện thông tin khi nó được truyền ở trên mạng, ở đầu nhận, tầng trình bày bung trở lại để được dữ liệu ban đầu.

### Tầng 7: Ứng dụng (Application)

Tầng ứng dụng (Application layer) là tầng cao nhất của mô hình OSI, nó xác định giao diện giữa người sử dụng và môi trường OSI và giải quyết các kỹ thuật mà các chương trình ứng dụng dùng để giao tiếp với mạng.

Để cung cấp phương tiện truy nhập môi trường OSI cho các tiến trình ứng dụng, Người ta thiết lập các thực thể ứng dụng (AE), các thực thể ứng dụng sẽ gọi đến các phần tử dịch vụ ứng dụng (Application Service Element - viết tắt là ASE) của chúng. Mỗi thực thể ứng dụng có thể gồm một hoặc nhiều các phần tử dịch vụ ứng dụng. Các phần tử dịch vụ ứng dụng được phối hợp trong môi trường của thực thể ứng dụng thông qua các liên kết (association) gọi là đối tượng liên kết đơn (Single Association Object - viết tắt là SAO). SAO điều khiển việc truyền thông trong suốt vòng đời của liên kết đó cho phép tuần tự hóa các sự kiện đến từ các ASE thành tố của nó.

**Chương 5**

# Các đặc tính kỹ thuật của mạng cục bộ

Trên thực tế mạng cục bộ là một hệ thống truyền dữ liệu giữa các máy tính với một khoảng cách tương đối hẹp, điều đó cho phép có những lựa chọn đa dạng về thiết bị . Tuy nhiên những lựa chọn đa dạng này lại bị hạn chế bởi các đặc tính kỹ thuật của mạng cục bộ, đó làø tập hợp các quy tắc chuẩn đã được quy ước mà tất cả các thực thể tham gia truyền thông trên mạng phải tuân theo để đảm bảo cho mạng hoạt động tốt. Các đặc tính chính của mạng cục bộ mà chúng ta nói tới sau đây là:

- Cấu trúc của mạng (hay topology của mạng mà qua đó thể hiện cách nối các mạng máy tính với nhau ra sao).
- Các nghi thức truyền dữ liệu trên mạng (các thủ tục hướng dẫn trạm làm việc làm thế nào và lúc nào có thể thâm nhập vào đường dây cáp để gửi các gói thông tin ).
- Các loại đường truyền và các chuẩn của chúng .
- Các phương thức tín hiệu

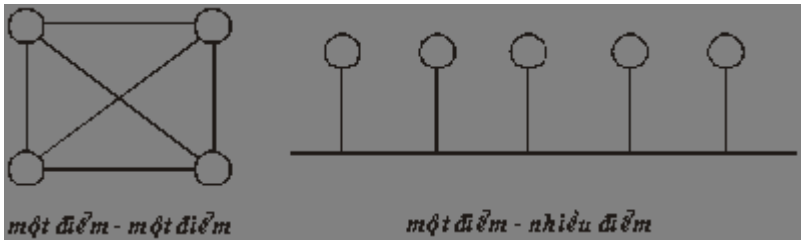
## I. Cấu trúc của mạng (Topology)

Hình trạng của mạng cục bộ thể hiện qua cấu trúc hay hình dáng hình học cuả các đường dây cáp mạng dùng để liên kết các máy tính thuộc mạng với nhau. Các mạng cục bộ thường hoạt động dựa trên cấu trúc đã định saün liên kết các máy tính và các thiết bị có liên quan.

Trước hết chúng ta xem xét hai phương thức nối mạng chủ yếu được sử dụng trong việc liên kết các máy tính là "một điểm - một điểm" và "một điểm - nhiều điểm ".

Với phương thức "một điểm - một điểm" các đường truyền riêng biệt được thiết lập để nối các cặp máy tính lại với nhau. Mỗi máy tính có thể truyền và nhận trực tiếp dữ liệu hoặc có thể làm trung gian như lưu trữ những dữ liệu mà nó nhận được rồi sau đó chuyển tiếp dữ liệu đi cho một máy khác để dữ liệu đó đạt tới đích.

Theo phương thức "một điểm - nhiều điểm " tất cả các trạm phân chia chung một đường truyền vật lý. Dữ liệu được gửi đi từ một máy tính sẽ có thể được tiếp nhận bởi tất cả các máy tính còn lại, bởi vậy cần chỉ ra địa chỉ đích của dữ liệu để mỗi máy tính căn cứ vào đó kiểm tra xem dữ liệu có phải dành cho mình không nếu đúng thì nhận còn nếu không thì bỏ qua.




*Hình 5.1: Các phương thức liên kết mạng*

Tùy theo cấu trúc của mỗi mạng chúng sẽ thuộc vào một trong hai phương thức nối mạng và mỗi phương thức nối mạng sẽ có những yêu cầu khác nhau về phần cứng và phần mềm.

## II. Những cấu trúc chính của mạng cục bộ

### 1. Dạng đường thẳng (Bus)

Trong dạng đường thẳng các máy tính đều được nối vào một đường dây truyền chính (bus). Đường truyền chính này được giới hạn hai đầu bởi một loại đầu nối đặc biệt gọi là *terminator* (dùng để nhận biết là đầu cuối để kết thúc đường truyền tại đây). Mỗi trạm được nối vào bus qua một đầu nối chữ T (T_connector) hoặc một bộ thu phát (transceiver). Khi một trạm truyền dữ liệu, tín hiệu được truyền trên cả hai chiều của đường truyền theo từng gói một, mỗi gói đều phải mang địa chỉ trạm đích. Các trạm khi thấy dữ liệu đi qua nhận lấy, kiểm tra, nếu đúng với địa chỉ của mình thì nó nhận lấy còn nếu không phải thì bỏ qua.

Sau đây là vài thông số kỹ thuật của topology bus. Theo chuẩn IEEE 802.3 (cho mạng cục bộ) với cách đặt tên qui ước theo thông số: tốc độ truyền tính hiệu (1,10 hoặc 100 Mb/s); BASE (nếu là Baseband) hoặc BROAD (nếu là Broadband).

- 10BASE5: Dùng cáp đồng trục đường kính lớn (10mm) với trở kháng 50 Ohm, tốc độ 10 Mb/s, phạm vi tín hiệu 500m/segment, có tối đa 100 trạm, khoảng cách giữa 2 tranceiver tối thiểu 2,5m (Phương án này còn gọi là Thick Ethernet hay Thicknet)

- 10BASE2: tương tự như Thicknet nhưng dùng cáp đồng trục nhỏ (RG 58A), có thể chạy với khoảng cách 185m, số trạm tối đa trong 1 segment là 30, khoảng cách giữa hai máy tối thiểu là 0,5m.

Dạng kết nối này có ưu điểm là ít tốn dây cáp, tốc độ truyền dữ liệu cao tuy nhiên nếu lưu lượng truyền tăng cao thì dễ gây ách tắc và nếu có trục trặc trên hành lang chính thì khó phát hiện ra.

Hiện nay các mạng sử dụng hình dạng đường thẳng là mạng Ethernet và G-net.

### 2. Dạng vòng tròn (Ring)

Các máy tính được liên kết với nhau thành một vòng tròn theo phương thức "một điểm - một điểm ", qua đó mỗi một trạm có thể nhận và truyền dữ liệu theo vòng một chiều và dữ liệu được truyền theo từng gói một. Mỗi gói dữ liệu đều có mang địa chỉ trạm đích, mỗi trạm khi nhận được một gói dữ liệu nó kiểm tra nếu đúng với địa chỉ của mình thì nó nhận lấy còn nếu không phải thì nó sẽ phát lại cho trạm kế tiếp, cứ như vậy gói dữ liệu đi được đến đích. Với dạng kết nối này có ưu điểm là không tốn nhiều dây cáp, tốc độ truyền dữ liệu cao, không gây ách tắc tuy nhiên các giao thức để truyền dữ liệu phức tạp và nếu có trục trặc trên một trạm thì cũng ảnh hưởng đến toàn mạng.

Hiện nay các mạng sử dụng hình dạng vòng tròn là mạng Tocken ring của IBM.

### 3. Dạng hình sao (Star)

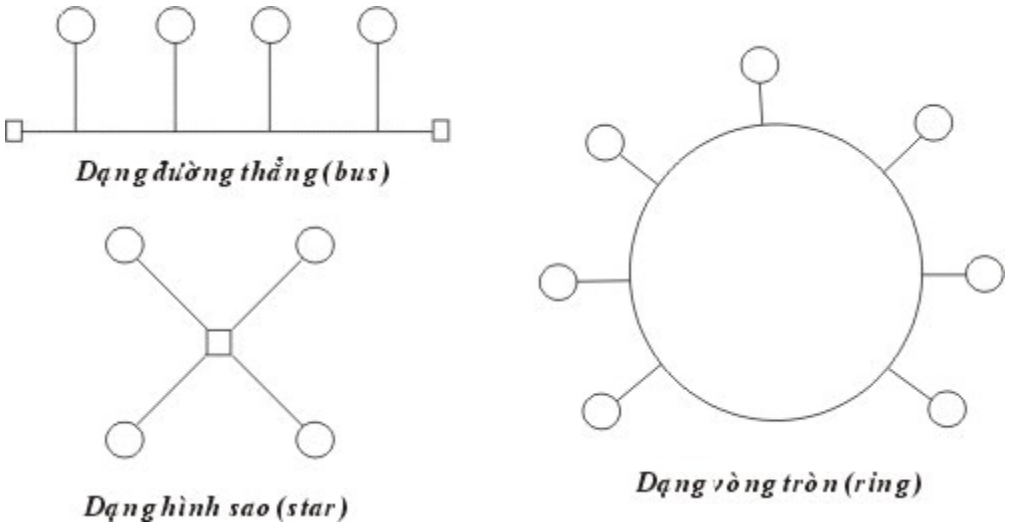
Ở dạng hình sao, tất cả các trạm được nối vào một thiết bị trung tâm có nhiệm vụ nhận tín hiệu từ các trạm và chuyển tín hiệu đến trạm đích với phương thức kết nối là phương thức "một điểm - một điểm ". Thiết bị trung tâm hoạt động giống như một tổng đài cho phép thực hiện việc nhận và truyền dữ liệu từ trạm này tới các trạm khác. Tùy theo yêu cầu truyền thông trong mạng , thiết bị trung tâm có thể là một bộ chuyển mạch (switch), một bộ chọn đường (router) hoặc đơn giản là một bộ phân kênh (Hub). Có nhiều cổng ra và mỗi cổng nối với một máy. Theo chuẩn IEEE 802.3 mô hình dạng Star thường dùng:

- 10BASE-T: dùng cáp UTP, tốc độ 10 Mb/s, khoảng cách từ thiết bị trung tâm tới trạm tối đa là 100m.
- 100BASE-T tương tự như 10BASE-T nhưng tốc độ cao hơn 100 Mb/s.

***Ưu và khuyết điểm***

- *Ưu điểm:* Với dạng kết nối này có ưu điểm là không đụng độ hay ách tắc trên đường truyền, lắp đặt đơn giản, dễ dàng cấu hình lại (thêm, bớt trạm). Nếu có trục trặc trên một trạm thì cũng không gây ảnh hưởng đến toàn mạng qua đó dễ dàng kiểm soát và khắc phục sự cố.
- *Nhược điểm:* Độ dài đường truyền nối một trạm với thiết bị trung tâm bị hạn chế (trong vòng 100 m với công nghệ hiện đại) tốn đường dây cáp nhiều, tốc độ truyền dữ liệu không cao.

Hiện nay các mạng sử dụng hình dạng hình sao là mạng STARLAN của AT&T và S-NET của Novell.




*Hình 5.2 : Các loại cấu trúc chính của mạng cục bộ.*

| | **Đường thẳng** | **Vòng Tròn** | **Hình sao** |
|---|---|---|---|
| Ứng dụng | Tốt cho trường hợp mạng nhỏ và mạng có giao thông thấp và lưu lượng dữ liệu thấp | Tốt cho trường hợp mạng có số trạm ít hoạt động với tốc độ cao,không cách nhau xa lắm hoặc mạng có lưu lượng dữ liệu phân bố không đều. | hiên nay mạng sao là cách tốt nhất cho trường hợp phải tích hợp dữ liệu và tín hiệutiếng.Các mạng đện thoại công cộng có cấu trúc này |
| Độ phức tạp | Tương đối không phức tạp | Đòi hỏi thiết bị tương đối phức tạp .Mặt khác việc đưa thông điệp đi trên tuyến là đơn giản, vì chỉ có 1 con đường, trạm phát chỉ cần biết địa chỉ của trạm nhận , các thông tin để dẫn đường khác thì không cần thiết | Mạng sao được xem là khá phức tạp . Các trạm được nối với thiết bị trung tâm và lần lượt hoạt động như thiết bị trung tâm hoặc nối được tới các dây dẫn truyền từ xa |
| Hiệu suất | Rất tốt dưới tải thấp có thể giảm hiệu suất rất mau khi tải tăng | Có hiệu quả trong trường hợp lượng lưu thông cao và khá ổn định nhờ sự tăng chậm thời gian trễ và sự xuống cấp so với các mạng khác | Tốt cho trường hợp tải vừa tuy nhiên kích thước và khả năng , suy ra hiệu suất của mạng phụ thuộc trực tiếp vào sức mạnh của thiết bị trung tâm. |
| Tổng phí | Tương đối thấp đặc biệt do nhiều thiết bị đã phát triển hòa chỉnh và bán sảm phẩm ở thị trường .Sự dư | Phải dự trù gấp đôi nguồn lực hoặc phải có 1 phương thức thay thế khi 1 nút không hoạt động nếu vẫn muốn mạng hoạt động bình thường | Tổng phí rất cao khi làm nhiêm vụ của thiết bị trung tâm, thiết bị trung tâm ï không được dùng vào việc khác .Số lượng dây riêng cũng nhiều. |

| | | | |
|---|---|---|---|
| | thừa kênh truyền được khuyến để giảm bớt nguy cơ xuất hiện sự cố trên mạng | | |
| Nguy cơ | Một trạm bị hỏng không ảnh hưởng đến cả mạng. Tuy nhiên mạng sẽ có nguy cơ bị tổn hại khi sự cố trên đường dây dẫn chính hoặc có vấn đề với tuyến. Vấn đề trên rất khó xác định được lại rất dễ sửa chữa | Mơt trạm bị hỏng có thể ảnh hưởng đến cả hệ thống vì các trạm phục thuộc vào nhau. Tìm 1 repeater hỏng rất khó ,vả lại việc sửa chữa thẳng hay dùng mưu mẹo xác định điểm hỏng trên mạng có địa bàn rôäng rất khó | Độ tin cậy của hệ thống phụ thuộc vào thiết bị trung tâm, .nếu bị hỏng thì mạng ngưng hoạt động Sự ngưng hoạt động tại thiết bị trung tâm thường không ảnh hươdng đến toàn bộ hệ thống . |
| Khả năng mở rộng | Việc thêm và định hình lại mạng này rất dễ.Tuy nhiên việc kết nối giữa các máy tính và thiết bị của các hãng khác nhau khó có thể vì chúng phải có thể nhận cùng địa chỉ và dữ liệu | Tương đối dễ thêm và bớt các trạm làm việc mà không phải nối kết nhiều cho mỗi thay đổi Giá thành cho việc thay đổi tương đối thấp | Khả năng mở rộâng hạn chế, đa số các thiết bị trung tâm chỉ chịu đựng nổi 1 số nhất định liên kết. Sự hạn chế về tốc độ truyền dữ liệu và băng tần thường được đòi hỏi ở mỗi người sử dụng. Các hạn chế này giúp cho các chức năng xử lý trung tâm không bị quá tải bởi tốc độ thu nạp tại tại cổng truyền và giá thành mỗi cổng truyền của thiết bị trung tâm thấp . |

*Hình 6.4 : Bảng so sánh tính năng giữa các cấu trúc của mạng LAN*

## III. Phương thức truyền tín hiệu

Thông thường có hai phương thức truyền tín hiệu trong mạng cục bộ là dùng băng tần cơ sở (baseband) và băng tần rộng (broadband). Sự khác nhau chủ yếu giữa hai phương thức truyền tín hiệu này là băng tầng cơ sở chỉ chấp nhận một kênh dữ liệu duy nhất trong khi băng rộng có thể chấp nhận đồng thời hai hoặc nhiều kênh truyền thông cùng phân chia giải thông của đường truyền.

Hầu hết các mạng cục bộ sử dụng phương thức băng tần cơ sở. Với phương thức truyền tín hiệu này này tín hiệu có thể được truyền đi dưới cả hai dạng: tương tự (analog) hoặc số (digital). Phương thức truyền băng tần rộng chia giải thông (tần số)

của đường truyền thành nhiều giải tần con trong đó mỗi dải tần con đó cung cấp một kênh truyền dữ liệu tách biệt nhờ sử dụng một cặp modem đặc biệt gọi là bộ giải / Điều biến RF cai quản việc biến đổi các tín hiệu số thành tín hiệu tương tự có tần số vô tuyến (RF) bằng kỹ thuật ghép kênh.

## IV. Các giao thức truy cập đường truyền trên mạng LAN

Để truyền được dữ liệu trên mạng người ta phải có các thủ tục nhằm hướng dẫn các máy tính của mạng làm thế nào và lúc nào có thể thâm nhập vào đường dây cáp để gửi các gói dữ kiện. Ví dụ như đối với các dạng bus và ring thì chỉ có một đường truyền duy nhất nối các trạm với nhau, cho nên cần phải có các quy tắc chung cho tất cả các trạm nối vào mạng để đảm bảo rằng đường truyền được truy nhập và sử dụng một cách hợp lý.

Có nhiều giao thức khác nhau để truy nhập đường truyền vật lý nhưng phân thành hai loại: các giao thức truy nhập ngẫu nhiên và các giao thức truy nhập có điều khiển.

### 1. Giao thức chuyển mạch (yêu cầu và chấp nhận)

Giao thức chuyển mạch là loại giao thức hoạt động theo cách thức sau: một máy tính của mạng khi cần có thể phát tín hiệu thâm nhập vào mạng, nếu vào lúc này đường cáp không bận thì mạch điều khiển sẽ cho trạm này thâm nhập vào đường cáp còn nếu đường cáp đang bận, nghĩa là đang có giao lưu giữa các trạm khác, thì việc thâm nhập sẽ bị từ chối.

### 2. Giao thức đường dây đa truy cập với cảm nhận va chạm (Carrier Sense Multiple Access with Collision Detection hay CSMA/CD )

Giao thức đường dây đa truy cập cho phép nhiều trạm thâm nhập cùng một lúc vào mạng, giao thức này thường dùng trong sơ đồ mạng dạng đường thẳng. Mọi trạm đều có thể được truy nhập vào đường dây chung một cách ngẫu nhiên và do vậy có thể dẫn đến xung đột (hai hoặc nhiều trạm đồng thời cùng truyền dữ liệu). Các trạm phải kiểm tra đường truyền gói dữ liệu đi qua có phải của nó hay không. Khi một trạm muốn truyền dữ liệu nó phải kiểm tra đường truyền xem có rảnh hay không để gửi gói dữ liệu của, nếu đường truyền đang bận trạm phải chờ đợi chỉ được truyền khi thấy đường truyền rảnh. Nếu cùng một lúc có hai trạm cùng sử dụng đường truyền thì giao thức phải phát hiện điều này và các trạm phải ngưng thâm nhập, chờ đợi lần sau các thời gian ngẫu nhiên khác nhau.

Khi đường cáp đang bận trạm phải chờ đợi theo một trong ba phương thức sau:

- Trạm tạm chờ đợi một thời gian ngẫu nhiên nào đó rồi lại bắt đầu kiểm tra đường truyền.
- Trạm tiếp tục kiểm tra đường truyền đến khi đường truyền rảnh thì truyền dữ liệu đi.

- Trạm tiếp tục kiểm tra đường truyềnđến khi đường truyền rảnh thì truyền dữ liệu đi với xác suất p xác định trước (0 < p < 1).

Tại đây phương thức 1 có hiệu quả trong việc tránh xung đột vì hai trạm cần truyền khi thấy đường truyền bận sẽ cùng rút lui và chờ đợi trong các thời gian ngẫu nhiên khác nhau. Ngược lại phương thức 2 cố gắng giảm thời gian trống của đường truyền bằng các cho phép trạm có thể truyền ngay sau khi một cuộc truyền kết thúc song nếu lúc đó có thêm một trạm khác đang đợi thì khả năng xẩy ra xung đột là rất cao. Phương thức 3 với giá trị p phải lựa chọn hợp lý có thể tối thiểu hóa được khả năng xung đột lẫn thời gian trống của đường truyền.

Khi lưu lượng các gói dữ liệu cần di chuyển trên mạng quá cao, thì việc đụng độ có thể xẩy ra với sồ lượng lớn có gây tắc nghẽn đường truyền dẫn đến làm chậm tốc độ truyền tin của hệ thống.

### 3. Giao thức dùng thẻ bài vòng (Token ring)

Đây là giao thức truy nhập có điều khiển chủ yếu dùng kỹ thuật chuyển thẻ bài (token) để cấp phát quyền truy nhập đường truyền tức là quyền được truyền dữ liệu đi. Thẻ bài ở đay là một đơn vị dữ liệu đặc biệt, có kích thước và nội dung (gồm các thông tin điều khiển) được quy định riêng cho mỗi giao thức. Theo giao thức dùng thẻ bài vòng trong đường cáp liên tục có một thẻ bài chạy quanh trong mạng Thẻ bài là một đơn vị dữ liệu đặc biệt trong đó có một bit biểu diễn trạng thái sử dụng của nó (bận hoặc rỗi). Một trạm muốn truyền dữ liệu thì phải đợi đến khi nhận được một thẻ bài rảnh. Khi đó trạm sẽ đổi bit trạng thái của thẻ bài thành bận, nép gói dữ liệu có kèm theo địa chỉ nơi nhận vào thẻ bài và truyền đi theo chiều của vòng.

Vì thẻ bài chạy vòng quang trong mạng kín và chỉ có một thẻ nên việc đụng độ dữ liệu không thể xẩy ra, do vậy hiệu suất truyền dữ liệu của mạng không thay đổi.

Trong các giao thức này cần giải quyết hai vấn đề có thể dẫn đến phá vỡ hệ thống. Một là việc mất thẻ bài làm cho trên vòng không còn thẻ bài lưu chuyển nữa. Hai là một thẻ bài bận lưu chuyển không dừng trên vòng.

### 4. Giao thức dung thẻ bài cho dạng đường thẳng (Token bus)

Đây là giao thức truy nhập có điều khiển trong để cấp phát quyền truy nhập đường truyền cho các trạm đang có nhu cầu truyền dữ liệu, một thẻ bài được lưu chuyển trên một vòng logic thiết lập bởi các trạm đó. Khi một trạm có thẻ bài thì nó có quyền sử dụng đường truyền trong một thời gian xác định trước. Khi đã hết dữ liệu hoặc hết thời đoạn cho phép, trạm chuyển thẻ bài đến trạm tiếp theo trong vòng logic.

Như vậy trong mạng phải thiết lập được vòng logic (hay còn gọi là vòng ảo) bao gồm các trạm đang hoạt động nối trong mạng được xác định vị trí theo một chuỗi thứ tự mà trạm cuối cùng của chuỗi sẽ tiếp liền sau bởi trạm đầu tiên. Mỗi trạm được biết địa chỉ của các trạm kề trước và sau nó trong đó thứ tự của các trạm trên vòng logic có thể

độc lập với thứ tự vật lý. Cùng với việc thiết lập vòng thì giao thức phải luôn luôn theo dõi sự thay đổi theo trạng thái thực tế của mạng.

## V. Đường cáp truyền mạng

Đường cáp truyền mạng là cơ sở hạ tầng của một hệ thống mạng, nên nó rất quan trọng và ảnh hưởng rất nhiều đến khả năng hoạt động của mạng. Hiện nay người ta thường dùng 3 loại dây cáp là cáp xoắn cặp, cáp đồng trục và cáp quang.

### 1. Cáp xoắn cặp

Đây là loại cáp gồm hai đường dây dẫn đồng được xoắn vào nhau nhằm làm giảm nhiễu điện từ gây ra bởi môi trường xung quanh và giữa chúng với nhau.

Hiện nay có hai loại cáp xoắn là cáp có bọc kim loại ( STP - Shield Twisted Pair) và cáp không bọc kim loại (UTP -Unshield Twisted Pair).

- Cáp có bọc kim loại (STP): Lớp bọc bên ngoài có tác dụng chống nhiễu điện từ, có loại có một đôi giây xoắn vào nhau và có loại có nhiều đôi giây xoắn với nhau.

- Cáp không bọc kim loại (UTP): Tính tương tự như STP nhưng kém hơn về khả năng chống nhiễu và suy hao vì không có vỏ bọc.

STP và UTP có các loại (Category - Cat) thường dùng:

- Loại 1 & 2 (Cat 1 & Cat 2): Thường dùng cho truyền thoại và những đường truyền tốc độ thấp (nhỏ hơn 4Mb/s).

- Loại 3 (Cat 3): tốc độ truyền dữ liệu khoảng 16 Mb/s , nó là chuẩn cho hầu hết các mạng điện thoại.

- Loại 4 (Cat 4): Thích hợp cho đường truyền 20Mb/s.

- Loại 5 (Cat 5): Thích hợp cho đường truyền 100Mb/s.

- Loại 6 (Cat 6): Thích hợp cho đường truyền 300Mb/s.

Đây là loại cáp rẻ, dễ cài đặt tuy nhiên nó dễ bị ảnh hưởng của môi trường.

### 2. Cáp đồng trục

Cáp đồng trục có hai đường dây dẫn và chúng có cùng một trục chung, một dây dẫn trung tâm (thường là dây đồng cứng) đường dây còn lại tạo thành đường ống bao xung quanh dây dẫn trung tâm (dây dẫn này có thể là dây bện kim loại và vì nó có chức năng

chống nhiễu nên còn gọi là lớp bọc kim). Giữa hai dây dẫn trên có một lớp cách ly, và bên ngoài cùng là lớp vỏ plastic để bảo vệ cáp.

| *Các loại cáp* | *Dây xoắn cặp* | *Cáp đồng trục mỏng* | *Cáp đồng trục dày* | *Cáp quang* |
|---|---|---|---|---|
| ***Chi tiết*** | Bằng đồng, có 4 và 25 cặp dây (loại 3, 4, 5) | Bằng đồng, 2 dây, đường kính 5mm | Bằng đồng, 2 dây, đường kính 10mm | Thủy tinh, 2 sợi |
| ***Loại kết nối*** | RJ-25 hoặc 50-pin telco | BNC | N-series | ST |
| ***Chiều dài đoạn tối đa*** | 100m | 185m | 500m | 1000m |
| ***Số đầu nối tối đa trên 1 đoạn*** | 2 | 30 | 100 | 2 |
| ***Chạy 10 Mbit/s*** | Được | Được | Được | Được |
| ***Chạy 100 Mbit/s*** | Được | Không | Không | Được |
| ***Chống nhiễu*** | Tốt | Tốt | Rất tốt | Hoàn toàn |
| ***Bảo mật*** | Trung bình | Trung bình | Trung bình | Hoàn toàn |
| ***Độ tin cậy*** | Tốt | Trung bình | Tốt | Tốt |
| ***Lắp đặt*** | Dễ dàng | Trung bình | Khó | Khó |
| ***Khắc phục lỗi*** | Tốt | Dở | Dở | Tốt |
| ***Quản lý*** | Dễ dàng | Khó | Khó | Trung bình |
| ***Chi phí cho 1 trạm*** | Rất thấp | Thấp | Trung bình | Cao |
| ***Ứng dụng tốt nhất*** | Hệ thống Workgroup | Đường backbone | Đường backbone trong tủ mạng | Đường backbone dài trong tủ mạng hoặc các tòa nhà |

*Hình 5.3: Tính năng kỹ thuật của một số loại cáp mạng*

Cáp đồng trục có độ suy hao ít hơn so với các loại cáp đồng khác (ví dụ như cáp xoắn đôi) do ít bị ảnh hưởng của môi trường. Các mạng cục bộ sử dụng cáp đồng trục có thể có kích thước trong phạm vi vài ngàn mét, cáp đồng trục được sử dụng nhiều trong các mạng dạng đường thẳng. Hai loại cáp thường được sử dụng là cáp đồng trục mỏng và cáp đồng trục dày trong đường kính cáp đồng trục mỏng là 0,25 inch, cáp đồng trục dày là 0,5 inch. Cả hai loại cáp đều làm việc ở cùng tốc độ nhưng cáp đồng trục mỏng có độ hao suy tín hiệu lớn hơn

Hiện nay có cáp đồng trục sau:

- RG -58,50 ohm: dùng cho mạng Thin Ethernet
- RG -59,75 ohm: dùng cho truyền hình cáp
- RG -62,93 ohm: dùng cho mạng ARCnet

Các mạng cục bộ thường sử dụng cáp đồng trục có dải thông từ 2,5 - 10 Mb/s, cáp đồng trục có độ suy hao ít hơn so với các loại cáp đồng khác vì nó có lớp vỏ bọc bên ngoài, độ dài thông thường của một đoạn cáp nối trong mạng là 200m, thường sử dụng cho dạng Bus.

### 3. Cáp sợi quang (Fiber - Optic Cable)

Cáp sợi quang bao gồm một dây dẫn trung tâm (là một hoặc một bó sợi thủy tinh có thể truyền dẫn tín hiệu quang) được bọc một lớp vỏ bọc có tác dụng phản xạ các tín hiệu trở lại để giảm sự mất mát tín hiệu. Bên ngoài cùng là lớp vỏ plastic để bảo vệ cáp. Như vậy cáp sợi quang không truyền dẫn các tín hiệu điện mà chỉ truyền các tín hiệu quang (các tín hiệu dữ liệu phải được chuyển đổi thành các tín hiệu quang và khi nhận chúng sẽ lại được chuyển đổi trở lại thành tín hiệu điện).

Cáp quang có đường kính từ 8.3 - 100 micron, Do đường kính lõi sợi thuỷ tinh có kích thước rất nhỏ nên rất khó khăn cho việc đấu nối, nó cần công nghệ đặc biệt với kỹ thuật cao đòi hỏi chi phí cao.

Dải thông của cáp quang có thể lên tới hàng Gbps và cho phép khoảng cách đi cáp khá xa do độ suy hao tín hiệu trên cáp rất thấp. Ngoài ra, vì cáp sợi quang không dùng tín hiệu điện từ để truyền dữ liệu nên nó hoàn toàn không bị ảnh hưởng của nhiễu điện từ và tín hiệu truyền không thể bị phát hiện và thu trộm bởi các thiết bị điện tử của người khác.

Chỉ trừ nhược điểm khó lắp đặt và giá thành còn cao , nhìn chung cáp quang thích hợp cho mọi mạng hiện nay và sau này.

### 4. Các yêu cầu cho một hệ thống cáp

- An toàn, thẩm mỹ: tất cả các dây mạng phải được bao bọc cẩn thận, cách xa các nguồn điện, các máy có khả năng phát sóng để tránh trường hợp bị nhiễu. Các đầu nối phải đảm bảo chất lượng, tránh tình trạng hệ thống mạng bị chập chờn.

- Đúng chuẩn: hệ thống cáp phải thực hiện đúng chuẩn, đảm bảo cho khả năng nâng cấp sau này cũng như dễ dàng cho việc kết nối các thiết bị khác nhau của các nhà sản xuất khác nhau. Tiêu chuẩn quốc tế dùng cho các hệ thống mạng hiện nay là EIA/ TIA 568B.

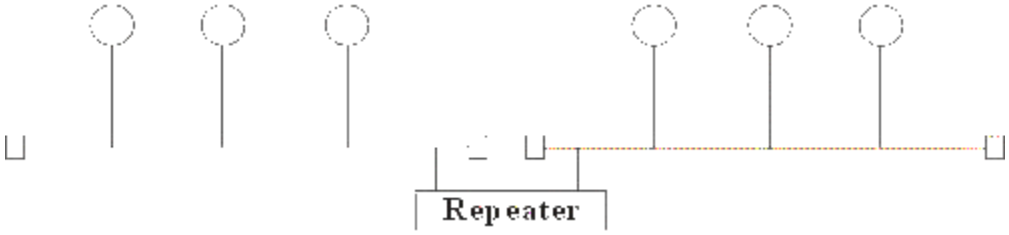
- Tiết kiệm và "linh hoạt" (flexible): hệ thống cáp phải được thiết kế sao cho kinh tế nhất, dễ dàng trong việc di chuyển các trạm làm việc và có khả năng mở rộng sau này.

**Chương 6**

# Các thiết bị liên kết mạng

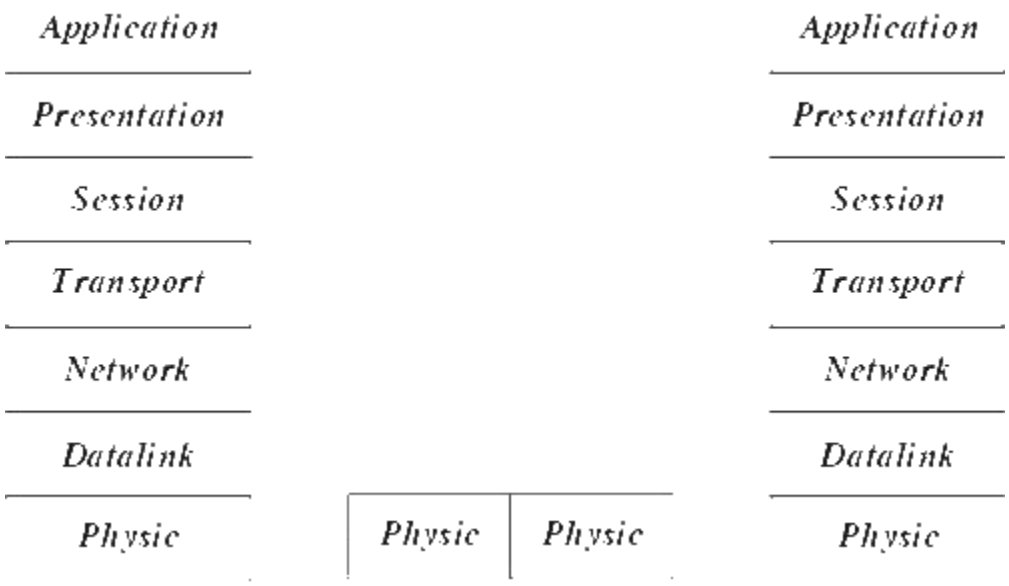
## I. Repeater (Bộ tiếp sức)

Repeater là loại thiết bị phần cứng đơn giản nhất trong các thiết bị liên kết mạng, nó được hoạt động trong tầng vật lý của mô hình hệ thống mở OSI. Repeater dùng để nối 2 mạng giống nhau hoặc các phần một mạng cùng có một nghi thức và một cấu hình. Khi Repeater nhận được một tín hiệu từ một phía của mạng thì nó sẽ phát tiếp vào phía kia của mạng.




*Hình 6.1: Mô hình liên kết mạng của Repeater.*

Repeater không có xử lý tín hiệu mà nó chỉ loại bỏ các tín hiệu méo, nhiễu, khuếch đại tín hiệu đã bị suy hao (vì đã được phát với khoảng cách xa) và khôi phục lại tín hiệu ban đầu. Việc sử dụng Repeater đã làm tăng thêm chiều dài của mạng.




*Hình 6.2: Hoạt động của bộ tiếp sức trong mô hình OSI*

Hiện nay có hai loại Repeater đang được sử dụng là Repeater điện và Repeater điện quang.

- ***Repeater điện*** nối với đường dây điện ở cả hai phía của nó, nó nhận tín hiệu điện từ một phía và phát lại về phía kia. Khi một mạng sử dụng Repeater điện để nối các phần của mạng lại thì có thể làm tăng khoảng cách của mạng, nhưng khoảng cách đó luôn bị hạn chế bởi một khoảng cách tối đa do độ trễ của tín hiệu. Ví dụ với mạng sử dụng cáp đồng trục 50 thì khoảng cách tối đa là 2.8 km, khoảng cách đó không thể kéo thêm cho dù sử dụng thêm Repeater.

- ***Repeater điện quang*** liên kết với một đầu cáp quang và một đầu là cáp điện, nó chuyển một tín hiệu điện từ cáp điện ra tín hiệu quang để phát trên cáp quang và ngược lại. Việc sử dụng Repeater điện quang cũng làm tăng thêm chiều dài của mạng.

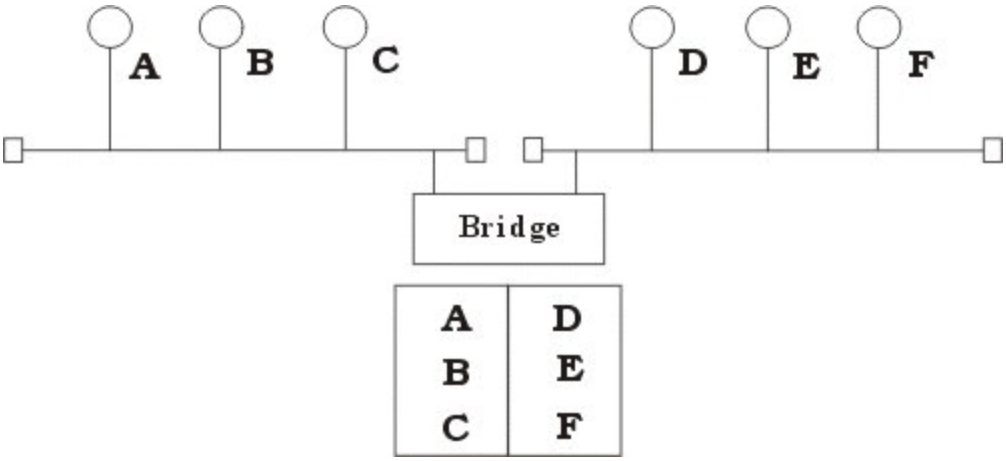
Việc sử dụng Repeater không thay đổi nội dung các tín hiện đi qua nên nó chỉ được dùng để nối hai mạng có cùng giao thức truyền thông (như hai mạng Ethernet hay hai mạng Token ring) nhưng không thể nối hai mạng có giao thức truyền thông khác nhau (như một mạng Ethernet và một mạng Token ring). Thêm nữa Repeater không làm thay đổi khối lượng chuyển vận trên mạng nên việc sử dụng không tính toán nó trên mạng lớn sẽ hạn chế hiệu năng của mạng. Khi lựa chọn sử dụng Repeater cần chú ý lựa chọn loại có tốc độ chuyển vận phù hợp với tốc độ của mạng.

**II. Bridge (Cầu nối)**

Bridge là một thiết bị có xử lý dùng để nối hai mạng giống nhau hoặc khác nhau, nó có thể được dùng với các mạng có các giao thức khác nhau. Cầu nối hoạt động trên tầng liên kết dữ liệu nên không như bộ tiếp sức phải phát lại tất cả những gì nó nhận được thì cầu nối đọc được các gói tin của tầng liên kết dữ liệu trong mô hình OSI và xử lý chúng trước khi quyết định có chuyển đi hay không.

Khi nhận được các gói tin Bridge chọn lọc và chỉ chuyển những gói tin mà nó thấy cần thiết. Điều này làm cho Bridge trở nên có ích khi nối một vài mạng với nhau và cho phép nó hoạt động một cách mềm dẻo.

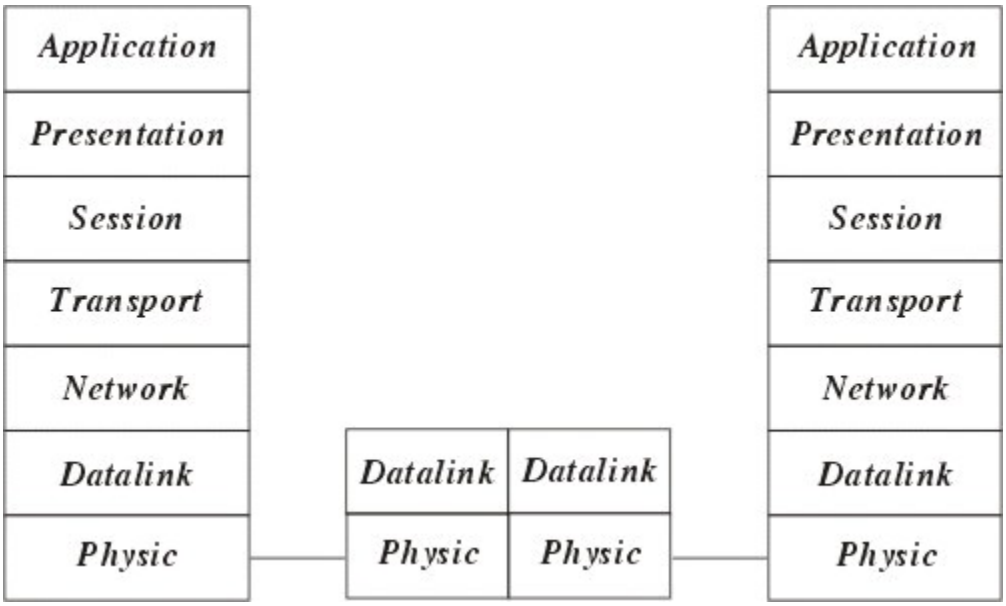
Để thực hiện được điều này trong Bridge ở mỗi đầu kết nối có một bảng các địa chỉ các trạm được kết nối vào phía đó, khi hoạt động cầu nối xem xét mỗi gói tin nó nhận được bằng cách đọc địa chỉ của nơi gửi và nhận và dựa trên bảng địa chỉ phía nhận được gói tin nó quyết định gửi gói tin hay không và bổ xung bảng địa chỉ.




*Hình 6.3: Hoạt động của Bridge*

Khi đọc địa chỉ nơi gửi Bridge kiểm tra xem trong bảng địa chỉ của phần mạng nhận được gói tin có địa chỉ đó hay không, nếu không có thì Bridge tự động bổ xung bảng địa chỉ (cơ chế đó được gọi là tự học của cầu nối).

Khi đọc địa chỉ nơi nhận Bridge kiểm tra xem trong bảng địa chỉ của phần mạng nhận được gói tin có địa chỉ đó hay không, nếu có thì Bridge sẽ cho rằng đó là gói tin nội bộ thuộc phần mạng mà gói tin đến nên không chuyển gói tin đó đi, nếu ngược lại thì Bridge mới chuyển sang phía bên kia. Ở đây chúng ta thấy một trạm không cần thiết chuyển thông tin trên toàn mạng mà chỉ trên phần mạng có trạm nhận mà thôi.




*Hình 6.4: Hoạt động của Bridge trong mô hình OSI*

Để đánh giá một Bridge người ta đưa ra hai khái niệm : Lọc và chuyển vận. Quá trình xử lý mỗi gói tin được gọi là quá trình lọc trong đó tốc độ lọc thể hiện trực tiếp khả

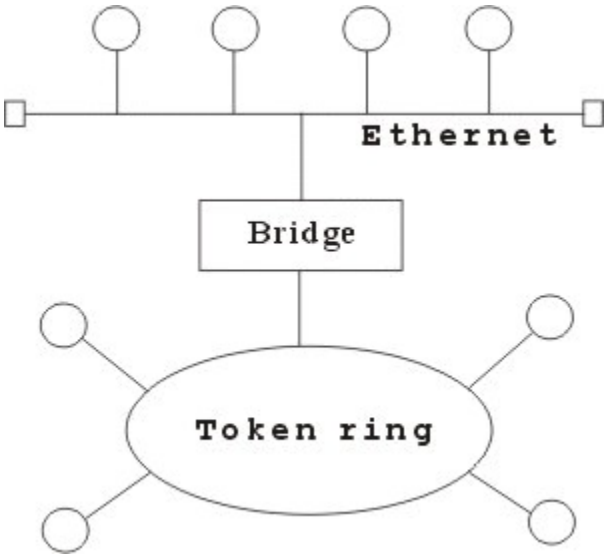
năng hoạt động của Bridge. Tốc độ chuyển vận được thể hiện số gói tin/giây trong đó thể hiện khả năng của Bridge chuyển các gói tin từ mạng này sang mạng khác.

Hiện nay có hai loại Bridge đang được sử dụng là Bridge vận chuyển và Bridge biên dịch. Bridge *vận chuyển* dùng để nối hai mạng cục bộ cùng sử dụng một giao thức truyền thông của tầng liên kết dữ liệu, tuy nhiên mỗi mạng có thể sử dụng loại dây nối khác nhau. Bridge vận chuyển không có khả năng thay đổi cấu trúc các gói tin mà nó nhận được mà chỉ quan tâm tới việc xem xét và chuyển vận gói tin đó đi.

Bridge biên dịch dùng để nối hai mạng cục bộ có giao thức khác nhau nó có khả năng chuyển một gói tin thuộc mạng này sang gói tin thuộc mạng kia trước khi chuyển qua

***Ví dụ :*** Bridge biên dịch nối một mạng Ethernet và một mạng Token ring. Khi đó Cầu nối thực hiện như một nút token ring trên mạng Token ring và một nút Enthernet trên mạng Ethernet. Cầu nối có thể chuyển một gói tin theo chuẩn đang sử dụng trên mạng Enthernet sang chuẩn đang sử dụng trên mạng Token ring.

Tuy nhiên chú ý ở đây cầu nối không thể chia một gói tin ra làm nhiều gói tin cho nên phải hạn chế kích thước tối đa các gói tin phù hợp với cả hai mạng. Ví dụ như kích thước tối đa của gói tin trên mạng Ethernet là 1500 bytes và trên mạng Token ring là 6000 bytes do vậy nếu một trạm trên mạng token ring gửi một gói tin cho trạm trên mạng Ethernet với kích thước lớn hơn 1500 bytes thì khi qua cầu nối số lượng byte dư sẽ bị chặt bỏ.




*Hình 6.5: Ví dụ về Bridge biên dịch*

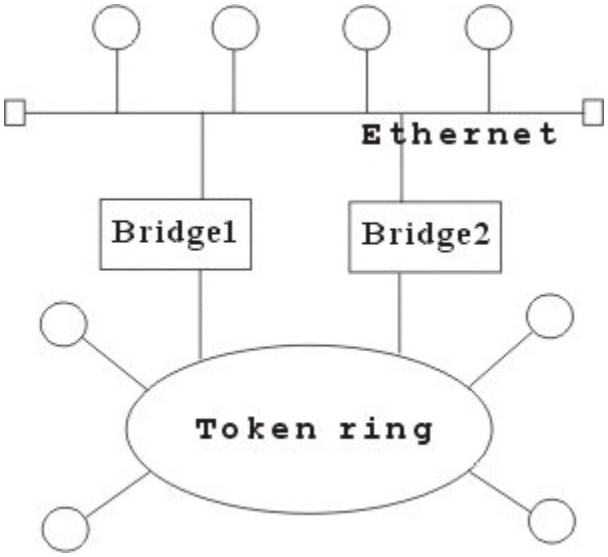
Người ta sử dụng Bridge trong các trường hợp sau :

- Mở rộng mạng hiện tại khi đã đạt tới khoảng cách tối đa do Bridge sau khi sử lý gói tin đã phát lại gói tin trên phần mạng còn lại nên tín hiệu tốt hơn bộ tiếp sức.

- Giảm bớt tắc nghẽn mạng khi có quá nhiều trạm bằng cách sử dụng Bridge, khi đó chúng ta chia mạng ra thành nhiều phần bằng các Bridge, các gói tin trong nội bộ tùng phần mạng sẽ không được phép qua phần mạng khác.

- Để nối các mạng có giao thức khác nhau.

Một vài Bridge còn có khả năng lựa chọn đối tượng vận chuyển. Nó có thể chỉ chuyển vận những gói tin của những địa chỉ xác định. Ví dụ : cho phép gói tin của máy A, B qua Bridge 1, gói tin của máy C, D qua Bridge 2.

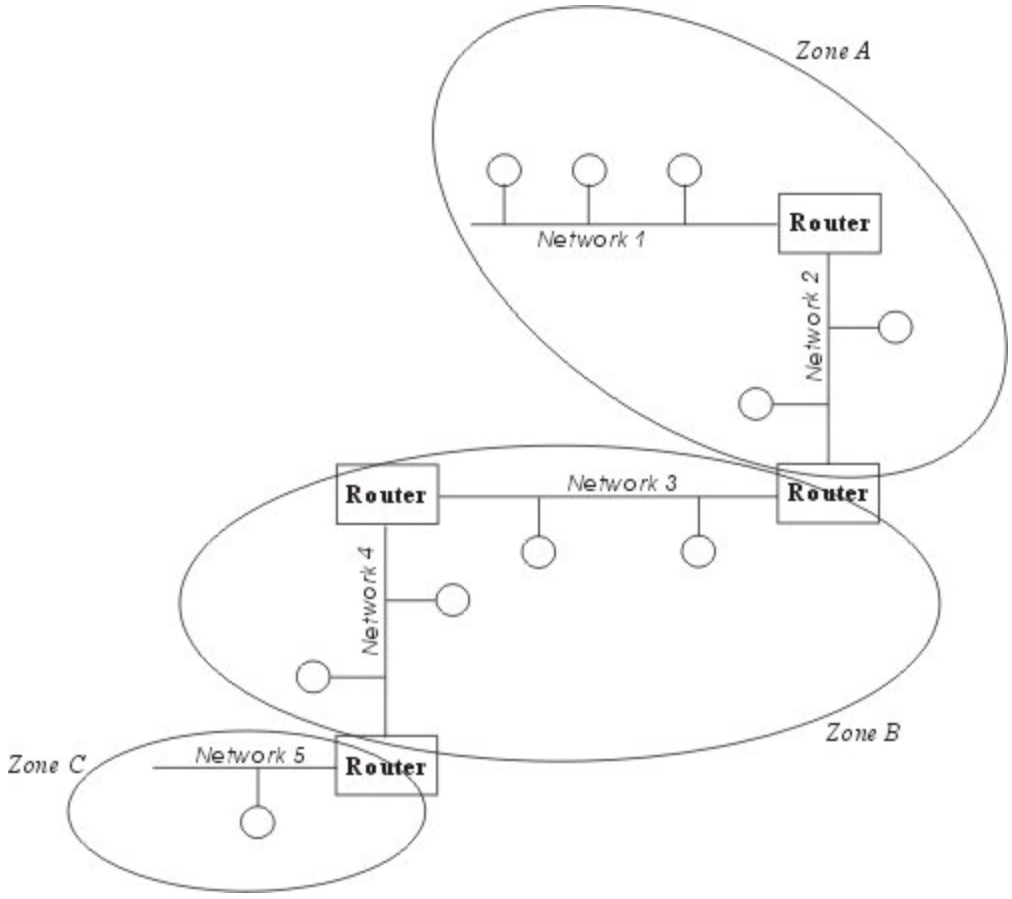



*Hình 6.6 : Liên kết mạng với 2 Bridge*

Một số Bridge được chế tạo thành một bộ riêng biệt, chỉ cần nối dây và bật. Các Bridge khác chế tạo như card chuyên dùng cắïm vào máy tính, khi đó trên máy tính sẽ sử dụng phần mềm Bridge. Việc kết hợp phần mềm với phần cứng cho phép uyển chuyển hơn trong hoạt động của Bridge.

### III. Router (Bộ tìm đường)

Router là một thiết bị hoạt động trên tầng mạng, nó có thể tìm được đường đi tốt nhất cho các gói tin qua nhiều kết nối để đi từ trạm gửi thuộc mạng đầu đến trạm nhận thuộc mạng cuối. Router có thể được sử dụng trong việc nối nhiều mạng với nhau và cho phép các gói tin có thể đi theo nhiều đường khác nhau để tới đích.




*Hình 6.7: Hoạt động của Router.*

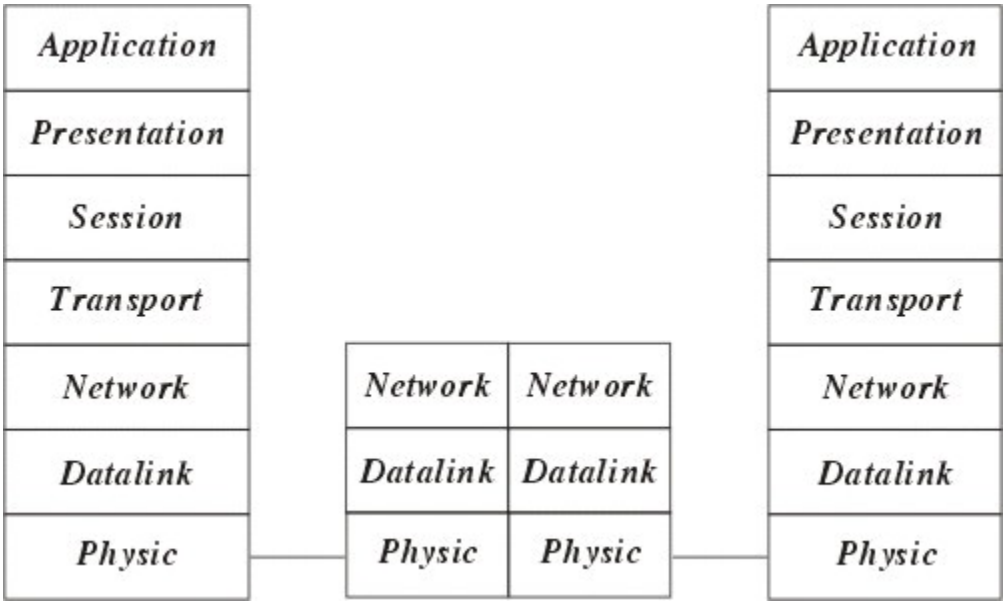
Khác với Bridge hoạt động trên tầng liên kết dữ liệu nên Bridge phải xử lý mọi gói tin trên đường truyền thì Router có địa chỉ riêng biệt và nó chỉ tiếp nhận và xử lý các gói tin gửi đến nó mà thôi. Khi một trạm muốn gửi gói tin qua Router thì nó phải gửi gói tin với địa chỉ trực tiếp của Router (Trong gói tin đó phải chứa các thông tin khác về đích đến) và khi gói tin đến Router thì Router mới xử lý và gửi tiếp.

Khi xử lý một gói tin Router phải tìm được đường đi của gói tin qua mạng. Để làm được điều đó Router phải tìm được đường đi tốt nhất trong mạng dựa trên các thông tin nó có về mạng, thông thường trên mỗi Router có một bảng chỉ đường (Router table). Dựa trên dữ liệu về Router gần đó và các mạng trong liên mạng, Router tính được bảng chỉ đường (Router table) tối ưu dựa trên một thuật toán xác định trước.

Người ta phân chia Router thành hai loại là Router có phụ thuộc giao thức (The protocol dependent routers) và Router không phụ thuộc vào giao thức (The protocol independent router) dựa vào phương thức xử lý các gói tin khi qua Router.

- *Router có phụ thuộc giao thức:* Chỉ thực hiện việc tìm đường và truyền gói tin từ mạng này sang mạng khác chứ không chuyển đổi phương cách đóng gói của gói tin cho nên cả hai mạng phải dùng chung một giao thức truyền thông.

- *Router không phụ thuộc vào giao thức*: có thể liên kết các mạng dùng giao thức truyền thông khác nhau và có thể chuyển đôiø gói tin của giao thức này sang gói tin của giao thức kia, Router cũng ù chấp nhận kích thức các gói tin khác nhau (Router có thể chia nhỏ một gói tin lớn thành nhiều gói tin nhỏ trước truyền trên mạng).




*Hình 6.8: Hoạt động của Router trong mô hình OSI*

Để ngăn chặn việc mất mát số liệu Router còn nhận biết được đường nào có thể chuyển vận và ngừng chuyển vận khi đường bị tắc.

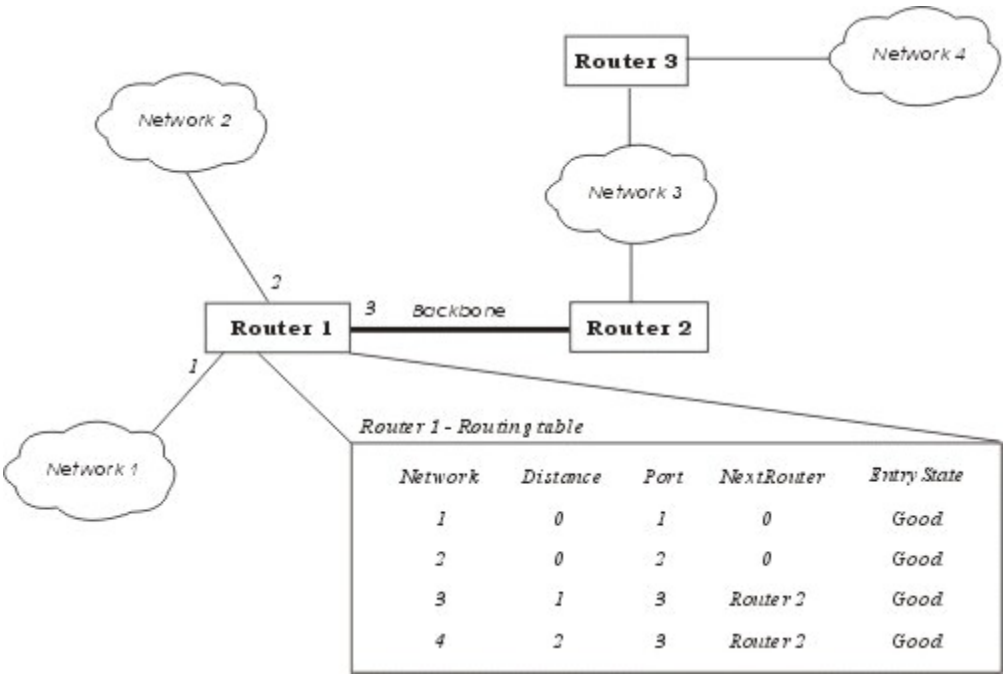
Các lý do sử dụng Router :

- Router có các phần mềm lọc ưu việt hơn là Bridge do các gói tin muốn đi qua Router cần phải gửi trực tiếp đến nó nên giảm được số lượng gói tin qua nó. Router thường được sử dụng trong khi nối các mạng thông qua các đường dây thuê bao đắt tiền do nó không truyền dư lên đường truyền.

- Router có thể dùng trong một liên mạng có nhiều vùng, mỗi vùng có giao thức riêng biệt.

- Router có thể xác định được đường đi an toàn và tốt nhất trong mạng nên độ an toàn của thông tin được đảm bảo hơn.

- Trong một mạng phức hợp khi các gói tin luân chuyển các đường có thể gây nên tình trạng tắc nghẽn của mạng thì các Router có thể được cài đặt các phương thức nhằm tránh được tắc nghẽn.




| Network | Distance | Port | NextRouter | Entry State |
|---|---|---|---|---|
| 1 | 0 | 1 | 0 | Good |
| 2 | 0 | 2 | 0 | Good |
| 3 | 1 | 3 | Router 2 | Good |
| 4 | 2 | 3 | Router 2 | Good |

*Hình 6.9: Ví dụ về bảng chỉ đường (Routing table) của Router.*

## Các phương thức hoạt động của Router

Đó là phương thức mà một Router có thể nối với các Router khác để qua đó chia sẻ thông tin về mạng hiện co. Các chương trình chạy trên Router luôn xây dựng bảng chỉ đường qua việc trao đổi các thông tin với các Router khác.

- Phương thức véc tơ khoảng cách : mỗi Router luôn luôn truyền đi thông tin về bảng chỉ đường của mình trên mạng, thông qua đó các Router khác sẽ cập nhật lên bảng chỉ đường của mình.

- Phương thức trạng thái tĩnh : Router chỉ truyền các thông báo khi có phát hiện có sự thay đổi trong mạng vàchỉ khi đó các Routerkhác ù cập nhật lại bảng chỉ đường, thông tin truyền đi khi đó thường là thông tin về đường truyền.

## Một số giao thức hoạt động chính của Router

- *RIP(Routing Information Protocol)* được phát triển bởi Xerox Network system và sử dụng SPX/IPX và TCP/IP. RIP hoạt động theo phương thức véc tơ khoảng cách.

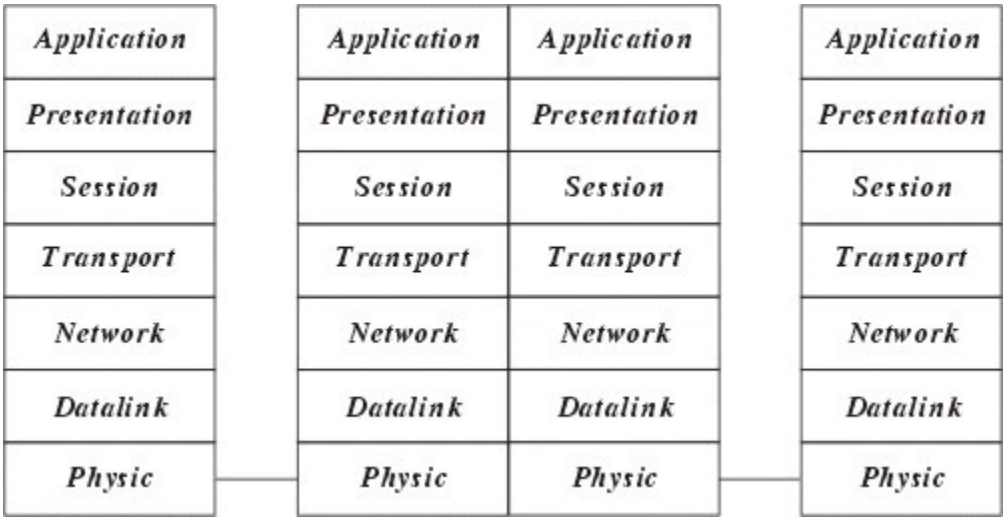
- *NLSP (Netware Link Service Protocol)* được phát triển bởi Novell dùng để thay thế RIP hoạt động theo phương thứcvéctơ khoảng cách, mỗi Router được biết cấu trúc của mạng và việc truyền các bảng chỉ đường giảm đi..

- *OSPF (Open Shortest Path First)* là một phần của TCP/IP với phương thức trạng thái tĩnh, trong đó có xét tới ưu tiên, giá đường truyền, mật độ truyền thông...

- *OSPF-IS (Open System Interconnection Intermediate System to Intermediate System)* là một phần của TCP/IP với phương thức trạng thái tĩnh, trong đó có xét tới ưu tiên, giá đường truyền, mật độ truyền thông...

## IV. Gateway (cổng nối)

Gateway dùng để kết nối các mạng không thuần nhất chẳng hạn như các mạng cục bộ và các mạng máy tính lớn (Mainframe), do các mạng hoàn toàn không thuần nhất nên việc chuyển đổi thực hiện trên cả 7 tầng của hệ thống mở OSI. Thường được sử dụng nối các mạng LAN vào máy tính lớn. Gateway có các giao thức xác định trước thường là nhiều giao thức, một Gateway đa giao thức thường được chế tạo như các Card có chứa các bộ xử lý riêng và cài đặt trên các máy tính hoặc thiết bị chuyên biệt.




*Hình 6.10: Hoạt động của Gateway trong mô hình OSI*

Hoạt động của Gateway thông thường phức tạp hơn là Router nên thông suất của nó thường chậm hơn và thường không dùng nối mạng LAN -LAN.

## V. Hub (Bộ tập trung)

Hub thường được dùng để nối mạng, thông qua những đầu cắm của nó người ta liên kết với các máy tính dưới dạng hình sao.

Người ta phân biệt các Hub thành 3 loại như sau sau :

- ***Hub bị động (Passive Hub) :*** Hub bị động không chứa các linh kiện điện tử và cũng không xử lý các tín hiệu dữ liệu, nó có chức năng duy nhất là tổ hợp các tín hiệu từ một số đoạn cáp mạng. Khoảng cách giữa một máy tính và Hub

không thể lớn hơn một nửa khoảng cách tối đa cho phép giữa 2 máy tính trên mạng (ví dụ khoảng cách tối đa cho phép giữa 2 máy tính của mạng là 200m thì khoảng cách tối đa giữa một máy tính và hub là 100m). Các mạng ARCnet thường dùng Hub bị động.

- ***Hub chủ động (Active Hub) :*** Hub chủ động có các linh kiện điện tử có thể khuyếch đại và xử lý các tín hiệu điện tử truyền giữa các thiết bị của mạng. Qúa trình xử lý tín hiệu được gọi là tái sinh tín hiệu, nó làm cho tín hiệu trở nên tốt hơn, ít nhạy cảm với lỗi do vậy khoảng cách giữa các thiết bị có thể tăng lên. Tuy nhiên những ưu điểm đó cũng kéo theo giá thành của Hub chủ động cao hơn nhiều so với Hub bị động. Các mạng Token ring có xu hướng dùng Hub chủ động.

- ***Hub thông minh (Intelligent Hub):*** cũng là Hub chủ động nhưng có thêm các chức năng mới so với loại trước, nó có thể có bộ vi xử lý của mình và bộ nhớ mà qua đó nó không chỉ cho phép điều khiển hoạt động thông qua các chương trình quản trị mạng mà nó có thể hoạt động như bộ tìm đường hay một cầu nối. Nó có thể cho phép tìm đường cho gói tin rất nhanh trên các cổng của nó, thay vì phát lại gói tin trên mọi cổng thì nó có thể chuyển mạch để phát trên một cổng có thể nối tới trạm đích.

**Chương 7**

# Giao thức TCP/IP

Giao thức TCP/IP được phát triển từ mạng ARPANET và Internet và được dùng như giao thức mạng và vận chuyển trên mạng Internet. TCP (Transmission Control Protocol) là giao thức thuộc tầng vận chuyển và IP (Internet Protocol) là giao thức thuộc tầng mạng của mô hình OSI. Họ giao thức TCP/IP hiện nay là giao thức được sử dụng rộng rãi nhất để liên kết các máy tính và các mạng.

Hiện nay các máy tính của hầu hết các mạng có thể sử dụng giao thức TCP/IP để liên kết với nhau thông qua nhiều hệ thống mạng với kỹ thuật khác nhau. Giao thức TCP/IP thực chất là một họ giao thức cho phép các hệ thống mạng cùng làm việc với nhau thông qua việc cung cấp phương tiện truyền thông liên mạng.

## I. Giao thức IP

### 1. Tổng quát

Nhiệm vụ chính của giao thức IP là cung cấp khả năng kết nối các mạng con thành liên kết mạng để truyền dữ liệu, vai trò của IP là vai trò của giao thức tầng mạng trong mô hình OSI. Giao thức IP là một giao thức kiểu không liên kết (connectionlees) có nghĩa là không cần có giai đoạn thiết lập liên kết trước khi truyền dữ liệu.

Sơ đồ địa chỉ hóa để định danh các trạm (host) trong liên mạng được gọi là địa chỉ IP 32 bits (32 bit IP address). Mỗi giao diện trong 1 máy có hỗ trợ giao thức IP đều phải được gán 1 địa chỉ IP (một máy tính có thể gắn với nhiều mạng do vậy có thể có nhiều địa chỉ IP). Địa chỉ IP gồm 2 phần: địa chỉ mạng (netid) và địa chỉ máy (hostid). Mỗi địa chỉ IP có độ dài 32 bits được tách thành 4 vùng (mỗi vùng 1 byte), có thể biểu thị dưới dạng thập phân, bát phân, thập lục phân hay nhị phân. Cách viết phổ biến nhất là dùng ký pháp thập phân có dấu chấm (dotted decimal notation) để tách các vùng. Mục đích của địa chỉ IP là để định danh duy nhất cho một máy tính bất kỳ trên liên mạng.

Do tổ chức và độ lớn của các mạng con (subnet) của liên mạng có thể khác nhau, người ta chia các địa chỉ IP thành 5 lớp, ký hiệu là A, B, C, D và E. Trong lớp A, B, C chứa địa chỉ có thể gán được. Lớp D dành riêng cho lớp kỹ thuật multicasting. Lớp E được dành những ứng dụng trong tương lai.

Netid trong địa chỉ mạng dùng để nhận dạng từng mạng riêng biệt. Các mạng liên kết phải có địa chỉ mạng (netid) riêng cho mỗi mạng. Ở đây các bit đầu tiên của byte đầu tiên được dùng để định danh lớp địa chỉ (0 - lớp A, 10 - lớp B, 110 - lớp C, 1110 - lớp D và 11110 - lớp E).

Ơû đây ta xét cấu trúc của các lớp địa chỉ có thể gán được là lớp A, lớp B, lớp C

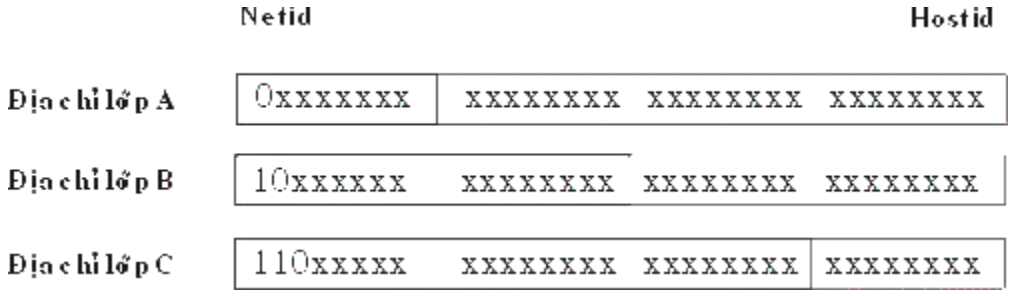
Cấu trúc của các địa chỉ IP như sau:

- Mạng lớp A: địa chỉ mạng (netid) là 1 Byte và địa chỉ host (hostid) là 3 byte.
- Mạng lớp B: địa chỉ mạng (netid) là 2 Byte và địa chỉ host (hostid) là 2 byte.
- Mạng lớp C: địa chỉ mạng (netid) là 3 Byte và địa chỉ host (hostid) là 1 byte.

Lớp A cho phép định danh tới 126 mạng, với tối đa 16 triệu host trên mỗi mạng. Lớp này được dùng cho các mạng có số trạm cực lớn.

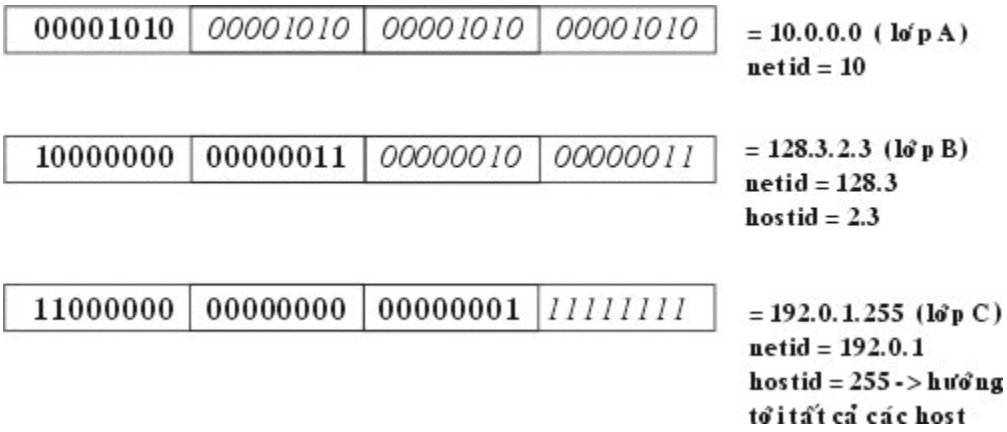
Lớp B cho phép định danh tới 16384 mạng, với tối đa 65534 host trên mỗi mạng.

Lớp C cho phép định danh tới 2 triệu mạng, với tối đa 254 host trên mỗi mạng. Lớp này được dùng cho các mạng có ít trạm.




*Hình 7.1: Cấu trúc các lớp địa chỉ IP*

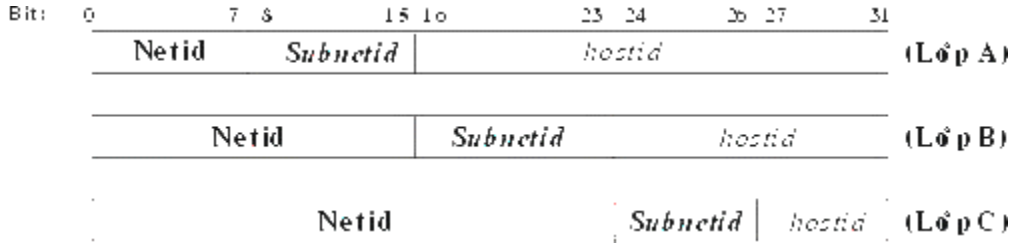
*Một số địa chỉ có tính chất đặc biệt*: Một địa chỉ có hostid = 0 được dùng để hướng tới mạng định danh bởi vùng netid. Ngược lại, một địa chỉ có vùng hostid gồm toàn số 1 được dùng để hướng tới tất cả các host nối vào mạng netid, và nếu vùng netid cũng gồm toàn số 1 thì nó hướng tới tất cả các host trong liên mạng




*Hình 7.2: Ví dụ cấu trúc các lớp địa chỉ IP*

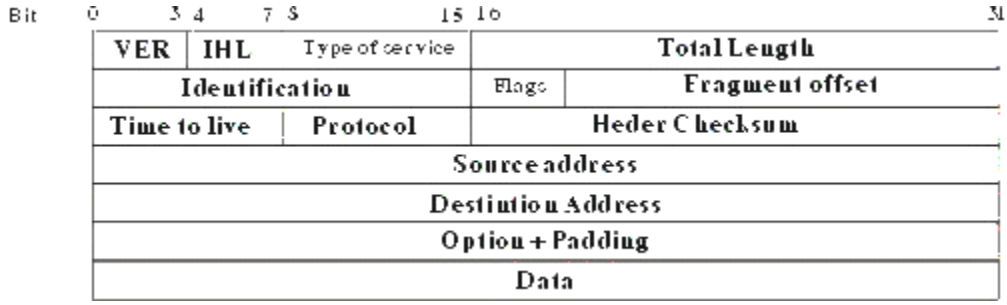
Cần lưu ý rằng các địa chỉ IP được dùng để định danh các host và mạng ở tầng mạng của mô hình OSI, và chúng không phải là các địa chỉ vật lý (hay địa chỉ MAC) của các trạm trên đó một mạng cục bộ (Ethernet, Token Ring.).

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




*Hình 7.3: Ví dụ địa chỉ khi bổ sung vùng subnetid*

Đơn vị dữ liệu dùng trong IP được gọi là gói tin (datagram), có khuôn dạng



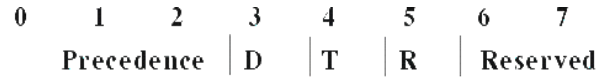

*Hình 7.4: Dạng thức của gói tin IP*

Ý nghĩa của thông số như sau:

- *VER* (4 bits): chỉ version hiện hành của giao thức IP hiện được cài đặt, Việc có chỉ số version cho phép có các trao đổi giữa các hệ thống sử dụng version cũ và hệ thống sử dụng version mới.

- *IHL* (4 bits): chỉ độ dài phần đầu (Internet header Length) của gói tin datagram, tính theo đơn vị từ ( 32 bits). Trường này bắt buột phải có vì phần đầu IP có thể có độ dài thay đổi tùy ý. Độ dài tối thiểu là 5 từ (20 bytes), độ dài tối đa là 15 từ hay là 60 bytes.

- *Type of service* (8 bits): đặc tả các tham số về dịch vụ nhằm thông báo cho mạng biết dịch vụ nào mà gói tin muốn được sử dụng, chẳng hạn ưu tiên, thời hạn chậm trễ, năng suất truyền và độ tin cậy. Hình sau cho biết ý nghĩ của trường 8 bits này.




- Precedence (3 bit): chỉ thị về quyền ưu tiên gửi datagram, nó có giá trị từ 0 (gói tin bình thường) đến 7 (gói tin kiểm soát mạng).

- D (Delay) (1 bit): chỉ độ trễ yêu cầu trong đó
  - D = 0 gói tin có độ trễ bình thường
  - D = 1 gói tin độ trễ thấp

- T (Throughput) (1 bit): chỉ độ thông lượng yêu cầu sử dụng để truyền gói tin với lựa chọn truyền trên đường thông suất thấp hay đường thông suất cao.
  - T = 0 thông lượng bình thường và
  - T = 1 thông lượng cao

- R (Reliability) (1 bit): chỉ độ tin cậy yêu cầu
  - R = 0 độ tin cậy bình thường
  - R = 1 độ tin cậy cao

- *Total Length* (16 bits): chỉ độ dài toàn bộ gói tin, kể cả phần đầu tính theo đơn vị byte với chiều dài tối đa là 65535 bytes. Hiện nay giới hạn trên là rất lớn nhưng trong tương lai với những mạng Gigabit thì các gói tin có kích thước lớn là cần thiết.

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

- *Flags (3 bits):* liên quan đến sự phân đoạn (fragment) các datagram, Các gói tin khi đi trên đường đi có thể bị phân thành nhiều gói tin nhỏ, trong trường hợp bị phân đoạn thì trường Flags được dùng điều khiển phân đoạn và tái lắp ghép bó dữ liệu. Tùy theo giá trị của Flags sẽ có ý nghĩa là gói tin sẽ không phân đoạn, có thể phân đoạn hay là gói tin phân đoạn cuối cùng. Trường ***Fragment Offset*** cho biết vị trí dữ liệu thuộc phân đoạn tương ứng với đoạn bắt đầu của gói dữ liệu gốc. Ý nghĩa cụ thể của trường Flags là:


  - bit 0: reserved - chưa sử dụng, luôn lấy giá trị 0.

- bit 1: (DF) = 0 (May Fragment) = 1 (Don't Fragment)
- bit 2: (MF) = 0 (Last Fragment) = 1 (More Fragments)

- *Fragment Offset (13 bits)*: chỉ vị trí của đoạn (fragment) ở trong datagram tính theo đơn vị 8 bytes, có nghĩa là phần dữ liệu mỗi gói tin (trừ gói tin cuối cùng) phải chứa một vùng dữ liệu có độ dài là bội số của 8 bytes. Điều này có ý nghĩa là phải nhân giá trị của Fragment offset với 8 để tính ra độ lệch byte.

- *Time to Live (8 bits)*: qui định thời gian tồn tại (tính bằng giây) của gói tin trong mạng để tránh tình trạng một gói tin bị quẩn trên mạng. Thời gian này được cho bởi trạm gửi và được giảm đi (thường qui ước là 1 đơn vị) khi datagram đi qua mỗi router của liên mạng. Thời lượng này giảm xuống tại mỗi router với mục đích giới hạn thời gian tồn tại của các gói tin và kết thúc những lần lặp lại vô hạn trên mạng. Sau đây là 1 số điều cần lưu ý về trường ***Time To Live***:
  - Nút trung gian của mạng không được gởi 1 gói tin mà trường này có giá trị= 0.
  - Một giao thức có thể ấn định ***Time To Live*** để thực hiện cuộc ra tìm tài nguyên trên mạng trong phạm vi mở rộng.
  - Một giá trị cố định tối thiểu phải đủ lớn cho mạng hoạt động tốt.

- *Protocol (8 bits):* chỉ giao thức tầng trên kế tiếp sẽ nhận vùng dữ liệu ở trạm đích (hiện tại thường là TCP hoặc UDP được cài đặt trên IP). Ví dụ: **TCP** có giá trị trường **Protocol** là 6, **UDP** có giá trị trường **Protocol** là 17

- *Header Checksum (16 bits)*: Mã kiểm soát lỗi của header gói tin IP.

- *Source Address (32 bits)*: Địa chỉ của máy nguồn.

- *Destination Address (32 bits)*: địa chỉ của máy đích

- *Options (độ dài thay đổi)*: khai báo các lựa chọn do người gửi yêu cầu (tuỳ theo từng chương trình).

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

- *Data (độ dài thay đổi)*: Trên một mạng cục bộ như vậy, hai trạm chỉ có thể liên lạc với nhau nếu chúng biết địa chỉ vật lý của nhau. Như vậy vấn đề đặt ra là phải thực hiện ánh xạ giữa địa chỉ IP (32 bits) và địa chỉ vật lý (48 bits) của một trạm.

### 2. Các giao thức trong mạng IP

Để mạng với giao thức IP hoạt động được tốt người ta cần một số giao thức bổ sung, các giao thức này đều không phải là bộ phận của giao thức IP và giao thức IP sẽ dùng đến chúng khi cần.

- *Giao thức ARP (Address Resolution Protocol):* Ở đây cần lưu ý rằng các địa chỉ IP được dùng để định danh các host và mạng ở tầng mạng của mô hình OSI, và chúng không phải là các địa chỉ vật lý (hay địa chỉ MAC) của các trạm trên đó một mạng cục bộ (Ethernet, Token Ring.). Trên một mạng cục bộ hai trạm chỉ có thể liên lạc với nhau nếu chúng biết địa chỉ vật lý của nhau. Như vậy vấn đề đặt ra là phải tìm được ánh xạ giữa địa chỉ IP (32 bits) và địa chỉ vật lý của một trạm. *Giao thức ARP* đã được xây dựng để tìm địa chỉ vật lý từ địa chỉ IP khi cần thiết.

- *Giao thức RARP (Reverse Address Resolution Protocol)*: Là giao thức ngược với *giao thức ARP*. Giao thức RARP được dùng để tìm địa chỉ IP từ địa chỉ vật lý.

- *Giao thức ICMP (Internet Control Message Protocol):* Giao thức này thực hiện truyền các thông báo điều khiển (báo cáo về các tình trạng các lỗi trên mạng.) giữa các gateway hoặc một nút của liên mạng. Tình trạng lỗi có thể là: một gói tin IP không thể tới đích của nó, hoặc một router không đủ bộ nhớ đệm để lưu và chuyển một gói tin IP, Một thông báo ICMP được tạo và chuyển cho IP. IP sẽ "bọc" (encapsulate) thông báo đó với một IP header và truyền đến cho router hoặc trạm đích.

### 3. Các bước hoạt động của giao thức IP

Khi giao thức IP được khởi động nó trở thành một thực thể tồn tại trong máy tính và bắt đầu thực hiện những chức năng của mình, lúc đó thực thể IP là cấu thành của tầng mạng, nhận yêu cầu từ các tầng trên nó và gửi yêu cầu xuống các tầng dưới nó.

Đối với thực thể IP ở máy nguồn, khi nhận được một yêu cầu gửi từ tầng trên, nó thực hiện các bước sau đây:

- Tạo một IP datagram dựa trên tham số nhận được.

- Tính checksum và ghép vào header của gói tin.

- Ra quyết định chọn đường: hoặc là trạm đích nằm trên cùng mạng hoặc một gateway sẽ được chọn cho chặng tiếp theo.

- Chuyển gói tin xuống tầng dưới để truyền qua mạng.

Đối với router, khi nhận được một gói tin đi qua, nó thực hiện các động tác sau:

1) Tính chesksum, nếu sai thì loại bỏ gói tin.

2) Giảm giá trị tham số Time - to Live. nếu thời gian đã hết thì loại bỏ gói tin.

3) Ra quyết định chọn đường.

4) Phân đoạn gói tin, nếu cần.

5) Kiến tạo lại IP header, bao gồm giá trị mới của các vùng Time - to -Live, Fragmentation và Checksum.

6) Chuyển datagram xuống tầng dưới để chuyển qua mạng.

Cuối cùng khi một datagram nhận bởi một thực thể IP ở trạm đích, nó sẽ thực hiện bởi các công việc sau:

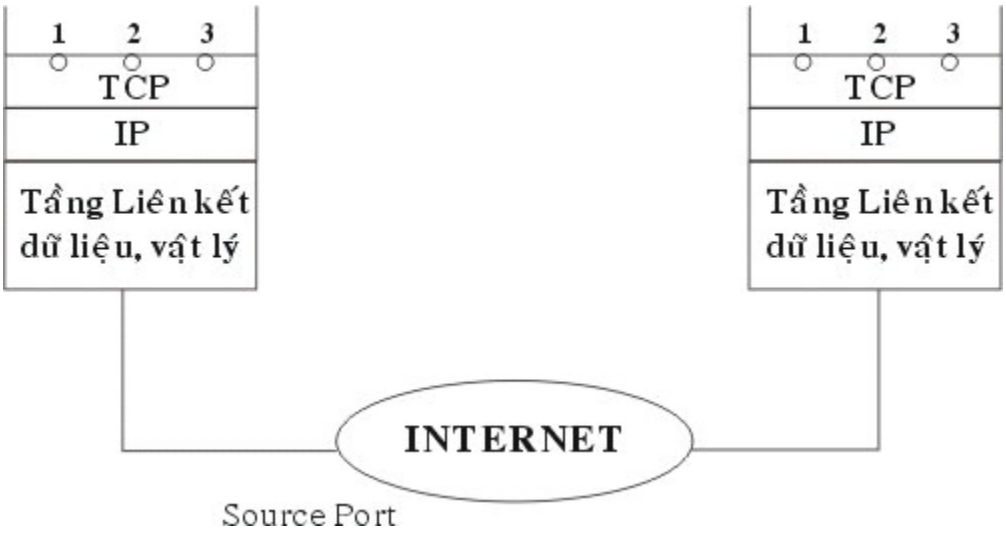
1) Tính checksum. Nếu sai thì loại bỏ gói tin.

2) Tập hợp các đoạn của gói tin (nếu có phân đoạn)

3) Chuyển dữ liệu và các tham số điều khiển lên tầng trên.

## II. Giao thức điều khiển truyền dữ liệu TCP

TCP là một giao thức "có liên kết" (connection - oriented), nghĩa là cần phải thiết lập liên kết giữa hai thực thể TCP trước khi chúng trao đổi dữ liệu với nhau. Một tiến trình ứng dụng trong một máy tính truy nhập vào các dịch vụ của giao thức TCP thông qua một cổng (port) của TCP. Số hiệu cổng TCP được thể hiện bởi 2 bytes.




*Hình 7.5: Cổng truy nhập dịch vụ TCP*

Một cổng TCP kết hợp với địa chỉ IP tạo thành một đầu nối TCP/IP (socket) duy nhất trong liên mạng. Dịch vụ TCP được cung cấp nhờ một liên kết logic giữa một cặp đầu nối TCP/IP. Một đầu nối TCP/IP có thể tham gia nhiều liên kết với các đầu nối TCP/IP ở xa khác nhau. Trước khi truyền dữ liệu giữa 2 trạm cần phải thiết lập một liên kết TCP giữa chúng và khi không còn nhu cầu truyền dữ liệu thì liên kết đó sẽ được giải phóng.

Các thực thể của tầng trên sử dụng giao thức TCP thông qua các hàm gọi (function calls) trong đó có các hàm yêu cầu để yêu cầu, để trả lời. Trong mỗi hàm còn có các tham số dành cho việc trao đổi dữ liệu.

 *Các bước thực hiện để thiết lập một liên kết TCP/IP*: Thiết lập một liên kết mới có thể được mở theo một trong 2 phương thức: chủ động (active) hoặc bị động (passive).

- Phương thức bị động, người sử dụng yêu cầu TCP chờ đợi một yêu cầu liên kết gửi đến từ xa thông qua một đầu nối TCP/IP (tại chỗ). Người sử dụng dùng hàm passive Open có khai báo cổng TCP và các thông số khác (mức ưu tiên, mức an toàn)

- Với phương thức chủ động, người sử dụng yêu cầu TCP mở một liên kết với một một đầu nối TCP/IP ở xa. Liên kết sẽ được xác lập nếu có một hàm Passive Open tương ứng đã được thực hiện tại đầu nối TCP/IP ở xa đó.

**Bảng liệt kê một vài cổng TCP phổ biến.**

| Số hiệu cổng | Mô tả |
|---|---|
| 0 | Reserved |
| 5 | Remote job entry |
| 7 | Echo |
| 9 | Discard |
| 11 | Systat |
| 13 | Daytime |
| 15 | Nestat |
| 17 | Quotd (quote odd day |

| | |
|---|---|
| 20 | ftp-data |
| 21 | ftp (control) |
| 23 | Telnet |
| 25 | SMTP |
| 37 | Time |
| 53 | Name Server |
| 102 | ISO - TSAP |
| 103 | X.400 |
| 104 | X.400 Sending |
| 111 | Sun RPC |
| 139 | Net BIOS Session source |
| 160 - 223 | Reserved |

Khi người sử dụng gửi đi một yêu cầu mở liên kết sẽ được nhận hai thông số trả lời từ TCP.

- Thông số Open ID được TCP trả lời ngay lập tức để gán cho một liên kết cục bộ (local connection name) cho liên kết được yêu cầu. Thông số này về sau được dùng để tham chiếu tới liên kết đó. (Trong trường hợp nếu TCP không thể thiết lập được liên kết yêu cầu thì nó phải gửi tham số Open Failure để thông báo.)

- Khi TCP thiết lập được liên kết yêu cầu nó gửi tham số Open Sucsess được dùng để thông báo liên kết đã được thiết lập thành công. Thông báo này dược chuyển đến trong cả hai trường hợp bị động và chủ động. Sau khi một liên kết được mở, việc truyền dữ liệu trên liên kết có thể được thực hiện.

*Các bước thực hiện khi truyền và nhận dữ liệu:* Sau khi xác lập được liên kết người sữ dụng gửi và nhận dữ liệu. Việc gửi và nhận dữ liệu thông qua các hàm Send và receive.

- *Hàm Send:* Dữ liệu được gửi xuống TCP theo các khối (block). Khi nhận được một khối dữ liệu, TCP sẽ lưu trữ trong bộ đệm (buffer). Nếu cờ PUSH được dựng thì toàn bộ dữ liệu trong bộ đệm được gửi, kể cả khối dữ liệu mới đến sẽ được gửi đi. Ngược lại cờ PUSH không

được dựng thì dữ liệu được giữ lại trong bộ đệm và sẽ gửi đi khi có cơ hội thích hợp (chẳng hạn chờ thêm dữ liệu nữa để gửi đi với hiệu quả hơn).

- *Hàm reveive*: Ở trạm đích dữ liệu sẽ được TCP lưu trong bộ đệm gắn với mỗi liên kết. Nếu dữ liệu được đánh dấu với một cờ PUSH thì toàn bộ dữ liệu trong bộ đệm (kể cả các dữ liệu được lưu từ trước) sẽ được chuyển lên cho người sữ dụng. Còn nếu dữ liệu đến không được đánh dấu với cờ PUSH thì TCP chờ tới khi thích hợp mới chuyển dữ liệu với mục tiêu tăng hiệu quả hệ thống.

Nói chung việc nhận và giao dữ liệu cho người sử dụng đích của TCP phụ thuộc vào việc cài đặt cụ thể. Trường hợp cần chuyển gấp dữ liệu cho người sử dụng thì có thể dùng cờ URGENT và đánh dấu dữ liệu bằng bit URG để báo cho người sử dụng cần phải sử lý khẩn cấp dữ liệu đó.

*Các bước thực hiện khi đóng một liên kết:* Việc đóng một liên kết khi không cần thiết được thực hiên theo một trong hai cách: *dùng hàm Close* hoặc *dùng hàm Abort.*

- *Hàm Close*: yêu cầu đóng liên kết một cách bình thường. Có nghĩa là việc truyền dữ liệu trên liên kết đó đã hoàn tất. Khi nhận được một *hàm Close* TCP sẽ truyền đi tất cả dữ liệu còn trong bộ đệm thông báo rằng nó đóng liên kết. Lưu ý rằng khi một người sử dụng đã gửi đi một *hàm Close* thì nó vẫn phải tiếp tục nhận dữ liệu đến trên liên kết đó cho đến khi TCP đã báo cho phía bên kia biết về việc đóng liên kết và chuyển giao hết tất cả dữ liệu cho người sử dụng của mình.

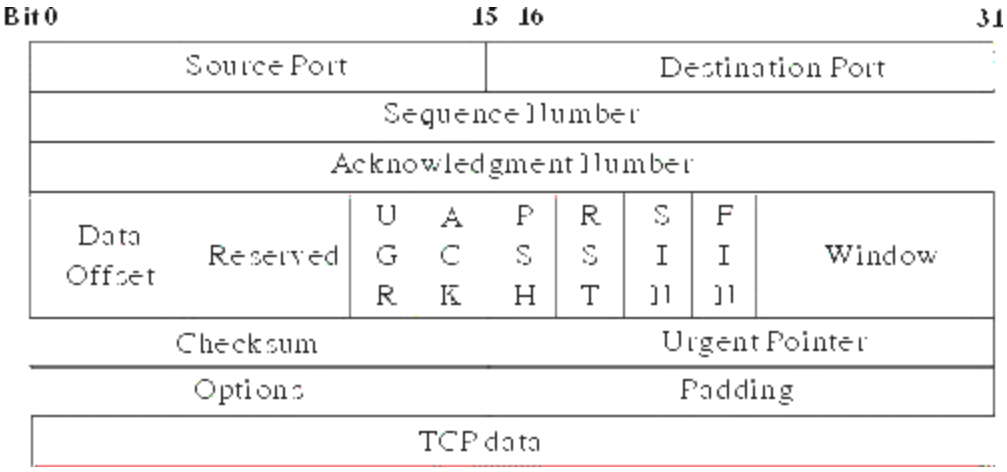
- *Hàm Abort*: Người sử dụng có thể đóng một liên kết bất và sẽ không chấp nhận dữ liệu qua liên kết đó nữa. Do vậy dữ liệu có thể bị mất đi khi đang được truyền đi. TCP báo cho TCP ở xa biết rằng liên kết đã được hủy bỏ và TCP ở xa sẽ thông báo cho người sử dụng cũa mình.

Một số hàm khác của TCP:

- *Hàm Status*: cho phép người sử dụng yêu cầu cho biết trạng thái của một liên kết cụ thể, khi đó TCP cung cấp thông tin cho người sử dụng.

- *Hàm Error*: thông báo cho người sử dụng TCP về các yêu cầu dịch vụ bất hợp lệ liên quan đến một liên kết có tên cho trước hoặc về các lỗi liên quan đến môi trường.

Đơn vị dữ liệu sử dụng trong TCP được gọi là segment (đoạn dữ liệu), có các tham số với ý nghĩa như sau:




*Hình 7.5: Dạng thức của segment TCP*

- Source Por (16 bits): Số hiệu cổng TCP của trạm nguồn.

- Destination Port (16 bit): Số hiệu cổng TCP của trạm đích.

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

- Acknowledgment Number (32 bit): số hiệu của segment tiếp theo mà trạm nguồn đang chờ để nhận. Ngầm ý báo nhận tốt (các) segment mà trạm đích đã gửi cho trạm nguồn.

- Data offset (4 bit): số lượng bội của 32 bit (32 bit words) trong TCP header (tham số này chỉ ra vị trí bắt đầu của nguồn dữ liệu).

- Reserved (6 bit): dành để dùng trong tương lai

- Control bit (các bit điều khiển):

    - URG: Vùng con trỏ khẩn (Ucgent Poiter) có hiệu lực.

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

    - PSH: Chức năng PUSH.

    - RST: Khởi động lại (reset) liên kết.

    - SYN: Đồng bộ hóa số hiệu tuần tự (sequence number).

    - FIN: Không còn dữ liệu từ trạm nguồn.

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

- Checksum (16 bit): mã kiểm soát lỗi cho toàn bộ segment (header + data)

- Urgemt Poiter (16 bit): con trỏ này trỏ tới số hiệu tuần tự của byte đi theo sau dữ liệu khẩn. Vùng này chỉ có hiệu lực khi bit URG được thiết lập.

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

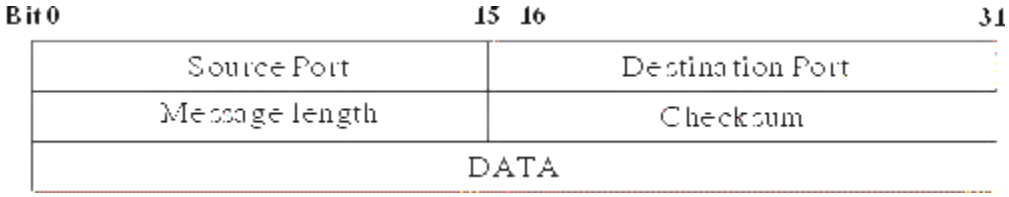
- Paddinh (độ dài thay đổi): phần chèn thêm vào header để đảm bảo phần header luôn kết thúc ở một mốc 32 bit. Phần thêm này gồm toàn số 0.

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

## III. Giao thức UDP (User Datagram Protocol)

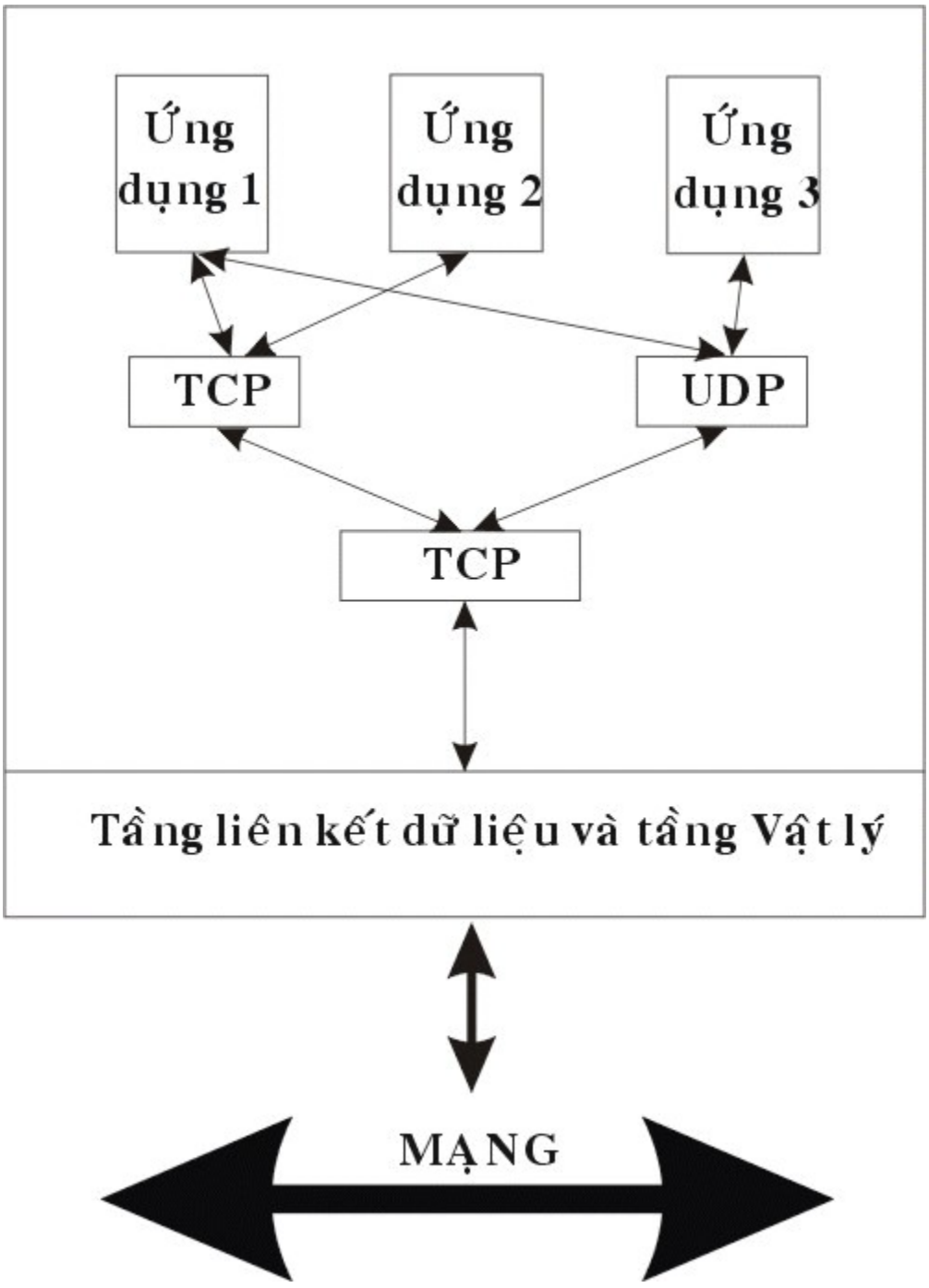
UDP (User Datagram Protocol) là giao thức theo phương thức không liên kết được sử dụng thay thế cho TCP ở trên IP theo yêu cầu của từng ứng dụng. Khác với TCP, UDP không có các chức năng thiết lập và kết thúc liên kết. Tương tự như IP, nó cũng không cung cấp cơ chế báo nhận (acknowledgment), không sắp xếp tuần tự các gói tin (datagram) đến và có thể dẫn đến tình trạng mất hoặc trùng dữ liệu mà không có cơ chế thông báo lỗi cho người gửi. Qua đó ta thấy UDP cung cấp các dịch vụ vận chuyển không tin cậy như trong TCP.

Khuôn dạng UDP datagram được mô tả với các vùng tham số đơn giản hơn nhiều so với TCP segment.




*Hình 7.7: Dạng thức của gói tin UDP*

UDP cũng cung cấp cơ chế gán và quản lý các số hiệu cổng (port number) để định danh duy nhất cho các ứng dụng chạy trên một trạm của mạng. Do ít chức năng phức tạp nên UDP thường có xu thế hoạt động nhanh hơn so với TCP. Nó thường được dùng cho các ứng không đòi hỏi độ tin cậy cao trong giao vận.




*Hình 7.8: Mô hình quan hệ họ giao thức TCP/IP*

**Chương 8**

# Các dịch vụ của mạng diện rộng (WAN)

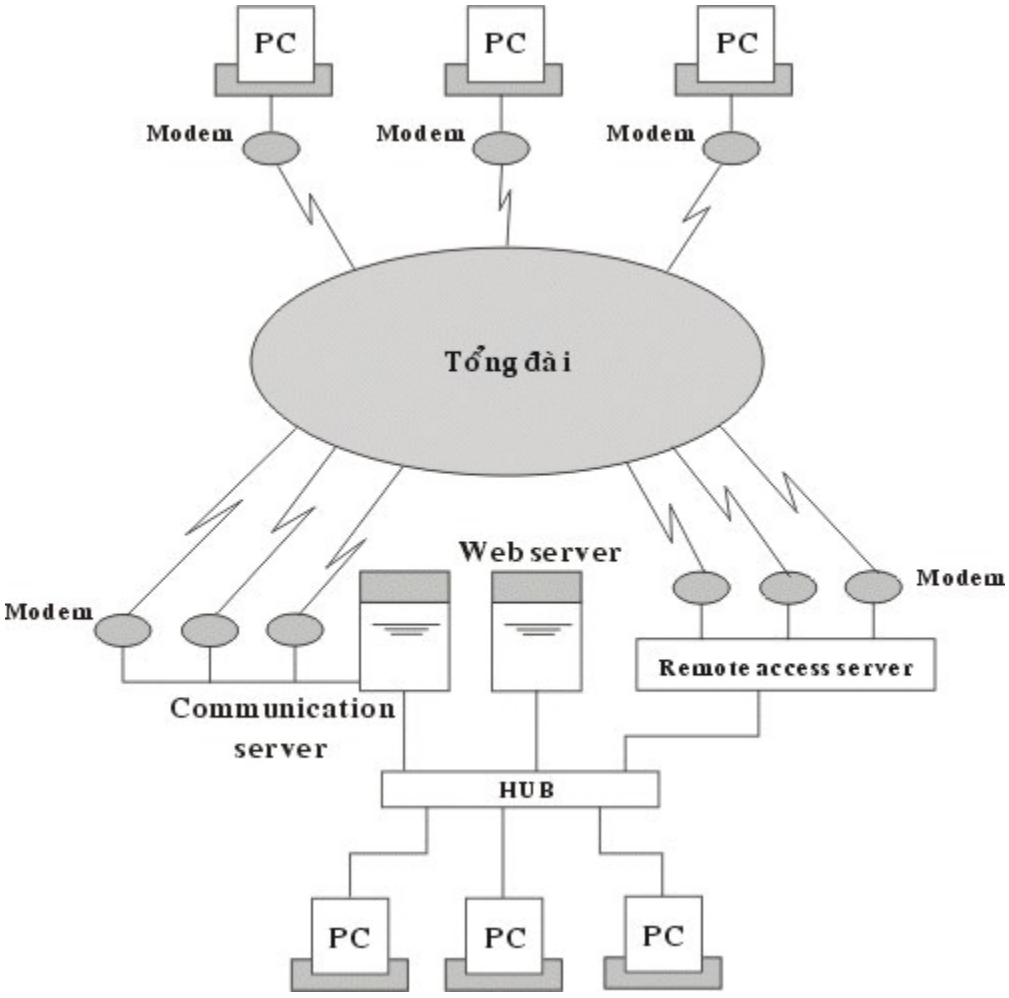
Hiện nay trên thế giới có nhiều dịch vụ dành cho việc chuyển thông tin từ khu vực này sang khu vực khác nhằm liên kết các mạng LAN của các khu vực khác nhau lại. Để có được những liên kết như vậy người ta thường sử dụng các dịch vụ của các mạng diện rộng. Hiện nay trong khi giao thức truyền thông cơ bản của LAN là Ethernet, Token Ring thì giao thức dùng để tương nối các LAN thông thường dựa trên chuẩn TCP/IP. Ngày nay khi các dạng kết nối có xu hướng ngày càng đa dạng và phân tán cho nên các mạng WAN đang thiên về truyền theo đơn vị tập tin thay vì truyền một lần xử lý.

Có nhiều cách phân loại mạng diện rộng, ở đây nếu phân loại theo phương pháp truyền thông tin thì có thể chia thành 3 loại mạng như sau:

- Mạng chuyển mạch (Circuit Swiching Network)
- Mạng thuê bao (Leased lines Network)
- Mạng chuyển gói tin (Packet Switching Network)

## I. Mạng chuyển mạch (Circuit Swiching Network)

Để thực hiện được việc liên kết giữa hai điểm nút, một đường nối giữa điểm nút này và điêm nút kia được thiết lập trong mạng thể hiện dưới dạng cuộc gọi thông qua các thiết bị chuyển mạch.




*Hình 8.1: Mô hình mạng chuyển mạch*

Một ví dụ của mạng chuyển mạch là hoạt động của mạng điện thoại, các thuê bao khi biết số của nhau có thể gọi cho nhau và có một đường nối vật lý tạm thời được thiết lập giữa hai thuê bao.

Với mô hình này mọi đường đều có thể một đường bất kỳ khác, thông qua những đường nối và các thiết bị chuyên dùng người ta có thể liên kết một đường tạm thời từ nơi gửi tới nơi nhận một đường nối vật lý, đường nối trên duy trì trong suốt phiên làm việc và chỉ giải phóng sau khi phiên làm việc kết thúc. Để thực hiện một phiên làm việc cần có các thủ tục đầy đủ cho việc thiết lập liên kết trong đó có việc thông báo cho mạng biết địa chỉ của nút nhận.

Hiện nay có 2 loại mạng chuyển mạch là chuyển mạch tương tự (analog) và chuyển mạch số (digital)

- *Chuyển mạch tương tự (Analog):* Việc chuyển dữ liệu qua mạng chuyển mạch tương tự được thực hiện qua mạng điện thoại. Các trạm sử dụng một

thiết bị có tên là modem, thiết bị này sẽ chuyển các tín hiệu số từ máy tính sao tín hiệu tuần tự có trể truyền đi trên mạng điện thoại và ngược lại.


*Hình 8.2: Mô hình chuyển mạch tương tự*

Khi sử dụng đường truyền điện thoại để truyền số liệu thì các chuẩn của modem và các tính chất của nó sẽ quyết định tốc độ của đường truyền. Cùng với các kỹ thuật chuyển đổi tín hiệu các tính năng mới như nén tín hiệu cho phép nâng tốc độ truyền dữ liệu lên rất cao.

| Loại | Tốc độ (bps)ä | Loại nén | Tốc độ thực tế (bps) |
|---|---|---|---|
| Bell 212A | 1200 | | |
| CCITT V22 | 1200 | | |
| CCITT V22 bis | 2400 | MNP Class 5 | 2400 - 3600 |
| CCITT V32 | 9600 | MNP Class 5, V42 bis | 9600 - 19200 |
| CCITT V32 bis | 14400 | MNP Class 5, V42 bis | 14400 - 33600 |

*Hình 8.3: Bảng kỹ thuật modem*

Các kỹ thuật nén thường dùng là MNP Class 5 và V42 bis, MNP Class 5 cho phép nén với tỷ lệ 1.5:1 và V42 bis nén với tỷ lệ 2:1. Tuy nhiên trên thực tế tỷ lệ nén có thể thay đổi dựa vào dạng dữ liệu được truyền.

- *Chuyển mạch số (Digital):* Đường truyền chuyển mạch số lần đầu tiên được AT&T thiệu vào cuối 1980 khi AT&T giới thiệu mạng chuyển mạch số Acnet với đường truyền 56 kbs. Việc sử dụng đường chuyển mạch số cũng đòi hỏi sử dụng thiết bị phục vụ truyền dữ liệu số (Data Service Unit - DSU) vào vị trí modem trong chuyển mạch tương tự. Thiết bị phục vụ truyền dữ liệu số có nhiệm vụ chuyển các tín hiệu số đơn chiều (unipolar) từ máy tính ra thành tín hiệu số hai chiều (bipolar) để truyền trên đường truyền.

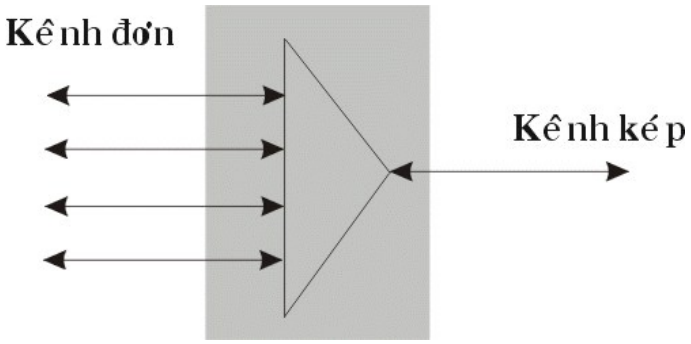

*Hình 8.3: Mô hình chuyển mạch số*

Mạng chuyển mạch số cho phép người sử dụng nâng cao tốc độ truyền (ở đây do khác biệt giữa kỹ thuật truyền số và kỹ thuật truyền tương tự nên hiệu năng của truyền mạch số cao hơn nhiều so với truyền tương tự cho dù cùng tốc độ), độ an toàn.

Vào năm 1991 AT&T giới thiệu mạng chuyển mạch số có tốc độ 384 Kbps. Người ta có thể dùng mạng chuyển mạch số để tạo các liên kết giữa các mạng LAN và làm các đường truyền dự phòng.

## II. Mạng thuê bao (Leased line Network)

Với kỹ thuật chuyển mạch giữa các nút của mạng (tương tự hoặc số) có một số lượng lớn đường dây truyền dữ liệu, với mỗi đường dây trong một thời điểm chỉ có nhiều nhất một phiên giao dịch, khi số lượng các trạm sử dụng tăng cao người ta nhận thấy việc sử dụng mạng chuyển mạch trở nên không kinh tế. Để giảm bớt số lượng các đường dây kết nối giữa các nút mạng người ta đưa ra một kỹ thuật gọi là ghép kênh.




*Hình 8.4: Mô hình ghép kênh*

Mô hình đó được mô tả như sau: tại một nút người ta tập hợp các tín hiệu trên của nhiều người sử dụng ghép lại để truyền trên một kênh nối duy nhất đến các nút khác, tại nút cuối người ta phân kênh ghép ra thành các kênh riêng biệt và truyền tới các người nhận.

Có hai phương thức ghép kênh chính là ghép kênh theo tần số và ghép kênh theo thời gian, hai phương thức này tương ứng với mạng thuê bao tuần tự và mạng thuê bao kỹ thuật số. trong thời gian hiện nay mạng thuê bao kỹ thuật số sử dụng kỹ thuật ghép kênh theo thời gian với đường truyền T đang được sử dụng ngày một rộng rãi và dần dần thay thế mạng thuê bao tuần tự.

### 1. Phương thức ghép kênh theo tần số

Để sử dụng phương thức ghép kênh theo tần số giữa các nút của mạng được liên kết bởi đường truyền băng tần rộng. Băng tần này được chia thành nhiều kênh con được phân biệt bởi tần số khác nhau. Khi truyền dữ liệu, mỗi kênh truyền từ người sử dụng đến nút sẽ được chuyển thành một kênh con với tần số xác định và được truyền thông qua bộ ghép kênh đến nút cuối và tại đây nó được tách ra thành kênh riêng biệt để truyền tới người nhận. Theo các chuẩn của CCITT có các phương thức ghép kênh cho phép ghép 12, 60, 300 kênh đơn.

Người ta có thể dùng đường thuê bao tuần tự (Analog) nối giữa máy của người sử dụng tới nút mạng thuê bao gần nhất. Khi máy của người sử dụng gửi dữ liệu thì kênh dữ liệu được ghép với các kênh khác và truyền trên đường truyền tới nút đích và được phân ra thành kênh riêng biệt trước khi gửi tới máy của người sử dụng. Đường nối giữa máy trạm của người sử dụng tới nút mạng thuê bao cũng giống như mạng chuyển mạch tuần tự sử dụng đường dây điện thoại với các kỹ thuật chuyển đổi tín hiệu như V22, V22 bis, V32, V32 bis, các kỹ thuật nén V42 bis, MNP class 5.

### 2.Phương thức ghép kênh theo thời gian:

Khác với phương thức ghép kênh theo tần số, phương thức ghép kênh theo thời gian chia một chu kỳ thời gian hoạt động của đường truyền trục thành nhiều khoảng nhỏ và mỗi kênh tuyền dữ liệu được một khoảng. Sau khi ghép kênh lại thành một kênh chung dữ liệu được truyền đi tương tự như phương thức ghép kênh theo tần số. Người ta dùng đường thuê bao là đường truyền kỹ thuật số nối giữa máy của người sử dụng tới nút mạng thuê bao gần nhất.

Hiện nay người ta có các đường truyền thuê bao như sau :

Đường T1 với tốc độ 1.544 Mbps nó bao gồm 24 kênh vớp tốc độ 64 kbps và 8000 bits điều khiển trong 1 giây.

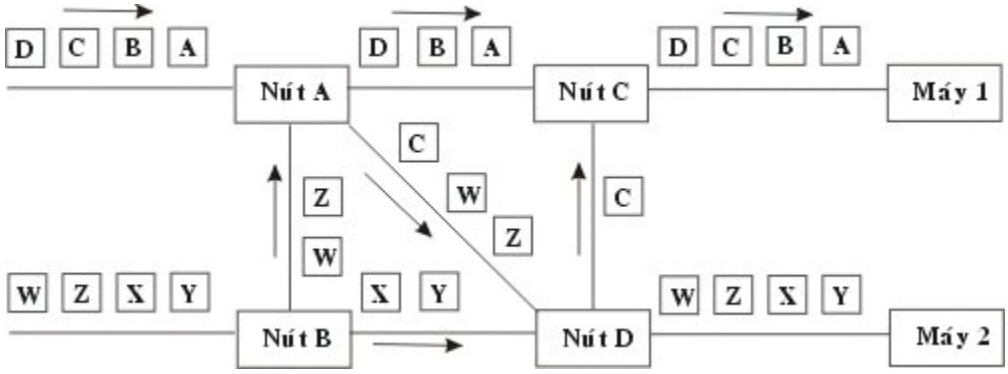
## III. Mạng chuyển gói tin (Packet Switching NetWork)

Mạng chuyển mạch gói hoạt động theo nguyên tắc sau : Khi một trạm trên mạng cần gửi dữ liệu nó cần phải đóng dữ liệu thành từng gói tin, các gói tin đó được đi trên mạng từ nút này tới nút khác tới khi đến được đích. Do việc sử dụng kỹ thuật trên nên khi một trạm không gửi tin thì mọi tài nguyên của mạng sẽ dành cho các trạm khác, do vậy mạng tiết kiệm được các tài nguyên và có thể sử dụng chúng một cách tốt nhất.

Người ta chia các phương thức chuyển mạch gói ra làm 2 phương thức:

- Phương thức chuyển mạch gói theo sơ đồ rời rạc.
- Phương thức chuyển mạch gói theo đường đi xác định.

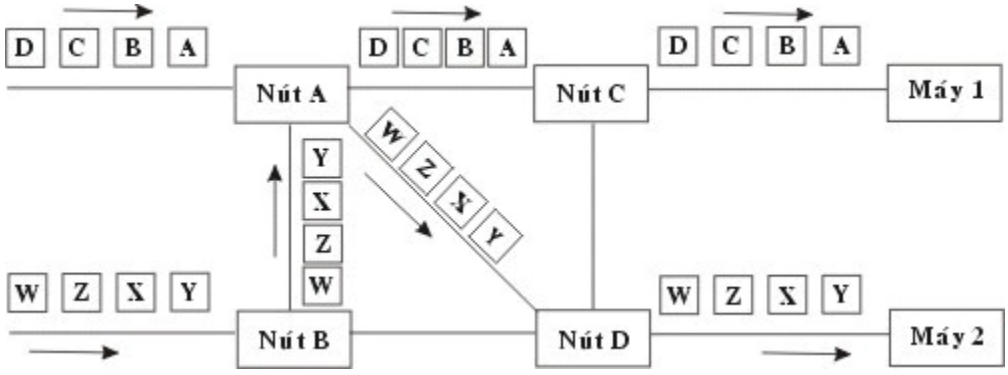
Với phương thức chuyển mạch gói theo sơ đồ rời rạc các gói tin được chuyển đi trên mạng một cách độc lập, mỗi gói tin đều có mang địa chỉ nơ i gửi và nơi nhận. Mỗi nút trong mạng khi tiếp nhận gói tin sẽ quyết định xenm đường đi của gói tin phụ thuộc vào thuật toán tìm đường tại nút và những thông tin về mạng mà nút đó có. Việc truyền theo phương thức này cho ta sự mềm dẻo nhất định do đường đi với mỗi gói tin trở nên mềm dẻo tuy nhiên điều này yêu cầu một số lượng tính toán rất lớn tại mỗi nút nên hiện nay phần lớn các mạng chuyển sang dùng phương chuyển mạch gói theo đường đi xác định.




*Hình 8.5: Ví dụ phương thức sơ đồ rời rạc.*

Phương thức chuyển mạch gói theo đường đi xác định:

Trước khi truyền dữ liệu một đường đi (hay còn gọi là đường đi ảo) được thiết lập giữa trạm gửi và trạm nhận thông qua các nút của mạng. Đường đi trên mang số hiệu phân biệt với các đường đi khác, sau đó các gói tin được gửi đi theo đường đã thiết lập để tới đích, các gói tin mang số hiệu củ đường ảo để có thể được nhận biết khi qua các nút. Điều này khiến cho việc tính toán đường đi cho phiên liên lạc chỉ cần thực hiện một lần.




*Hình 8.6: Ví dụ phương thức đường đi xác định*

## 1. Mạng X25

Được CCITT công bố lần đầu tiên vào 1970 lúc lĩnh vực viễn thông lần đầu tiên tham gia vào thế giới truyền dữ liệu với các đặc tính:

- X25 cung cấp quy trình kiểm soát luồng giữa các đầu cuối đem lại chất lương đường truyền cao cho dù chất lương đương dây truyền không cao.
- X25 được thiết kế cho cả truyền thông chuyển mạch lẫn truyền thông kiểu điểm nối điểm.
- Được quan tâm và tham gia nhanh chóng trên toàn cầu.

Trong X25 có chức năng dồn kênh (multiplexing) đối với liên kết logic (virtual circuits) chỉ làm nhiệm vụ kiểm soát lỗi cho các frame đi qua. Điều này làm tăng độ phức tạp trong việc phối hợp các thủ tục giữa hai tầng kề nhau, dẫn đến thông lượng bị hạn chế do tổng phí xử lý mỗi gói tin tăng lên. X25 kiểm tra lỗi tại mỗi nút trước khi truyền tiếp, điều này làm cho đường truyền chó chất lượng rất cao gần như phi lỗi. Tuy nhiên do vậy khối lượng tích toán tại mỗi nút khá lớn, đối với những đường truyền của những năm 1970 thì điều đó là cần thiết nhưng hiện nay khi kỹ thuật truyền dẫn đã đạt được những tiến bộ rất cao thì việc đó trở nên lãng phí

### 2. Mạng Frame Relay

Mỗi gói tin trong mạng gọi là Frame, do vậy mạng gọi là Frame relay. Đặc điểm khác biệt giữa mạng Frame Relay và mạng X25 mạng Frame Relay là chỉ kiểm tra lỗi tại hai trạm gửi và trạm nhận còn trong quá trình chuyển vận qua các nút trung gian gói tin sẽ không được kiểm lỗi nữa. Do vậy thời gian xử lý trên mỗi nút nhanh hơn, tuy nhiên khi có lỗi thì gói tin phải được phát lại từ trạm đầu. Với độ an toàn cao của đường truyền hiện nay thì chi phí việc phát lại đó chỉ chiếm một tỷ lệ nhỏ nếu so với khối lượng tính toán được giảm đi tại các nút nên mạng Frame Relay tiết kiệm được tài nguyên của mạng hơn so với mạng X25.

Frame relay không chỉ là một kỹ thuật mà còn là thể hiện một phương pháp tổ chức mới. Với nguyên lý là truyền mạch gói nhưng các thao tác kiểm soát giữa các đầu cuối giảm đáng kể Kỹ thuật Frame Relay cho phép thông lượng tối đa đạt tới 2Mbps và hiện nay nó đang cung cấp các giải pháp để tương nối các mạng cục bộ LAN trong một kiến trúc xương sống tạo nên môi trường cho ứng dụng multimedia.

### 3. Mạng ATM (Cell relay)

Hiện nay kỹ thuật Cell Relay dựa trên phương thức truyền thông không đồng bộ (ATM) có thể cho phép thông lương hàng trăm Mbps. Đơn vị dữ liệu dùng trong ATM được gọi là tế bào (cell). các tế bào trong ATM có độ dài cố định là 53 bytes, trong đó 5 bytes dành cho phần chứa thông tin điều khiển (cell header) và 48 bytes chứa dữ liệu của tầng trên.

Trong kỹ thuật ATM, các tế bào chứa các kiểu dữ liệu khác nhau được ghép kênh tới một đường dẫn chung được gọi là đường dẫn ảo (virtual path). Trong đường dẫn ảo đó có thể gồm nhiều kênh ảo (virtual chanell) khác nhau, mỗi kênh ảo được sử dụng bởi một ứng dung nào đó tại một thời điểm.

ATM đã kết hợp những đặc tính tốt nhất của dạng chuyển mạch liên tục và dạng chuyển mạch gói, nó có thể kết hợp dải thông linh hoạt và khả năng chuyển tiếp cao tốc và có khả năng quản lý đồng thời dữ liệu số, tiếng nói, hình ành và multimedia tương tác.

Mục tiêu của kỹ thuật ATM là nhằm cung cấp một mạng dồn kênh, và chuyển mạch tốc độ cao, độ trễ nhỏ dáp ứng cho các dạng truyền thông đa phương tiện (multimecdia)

Chuyển mạch cell cần thiết cho việc cung cấp các kết nối đòi hỏi băng thông cao, tình trạng tắt nghẽn thấp, hổ trợ cho lớp dịch vụ tích hợp lưu thông dữ liệu âm thanh hình ảnh. Đặc tính tốc độ cao là đặc tính nổi bật nhất của ATM.

ATM sử dụng cơ cấu chuyển mạch đặc biệt: ma trận nhị phân các thành tố chuyển mạch (a matrix of binary switching elements) để vận hành lưu thông. Khả năng vô hướng (scalability) là một đặc tính của cơ cấu chuyển mạch ATM. Đặc tính này tương phản trực tiếp với những gì diễn ra khi các trạm cuối được thêm vào một thiết bị liên mạng như router. Các router có năng suất tổng cố định được chia cho các trạm cuối có kết nối với chúng. Khi số lượng trạm cuối gia tăng, năng suất của router tương thích cho trạm cuối thu nhỏ lại. Khi cơ cấu ATM mở rộng, mỗi thiết bị thu trạm cuối, bằng con đường của chính nó đi qua bộ chuyển mạch bằng cách cho mỗi trạm cuối băng thông chỉ định. Băng thông rộng được chỉ định của ATM với đặc tính có thể xác nhận khiến nó trở thành một kỹ thuật tuyệt hảo dùng cho bất kỳ nơi nào trong mạng cục bộ của doanh nghiệp.

Như tên gọi của nó chỉ rõ, kỹ thuật ATM sử dụng phương pháp truyền không đồng bộ (asynchronouns) các tề bào từ nguồn tới đích của chúng. Trong khi đó, ở tầng vật lý người ta có thể sử dụng các kỹ thuật truyền thông đồng bộ như SDH (hoặc SONET).

Nhận thức được vị trí chưa thể thay thế được (ít nhất cho đến những năm đầu của thế kỷ 21) của kỹ thuật ATM, hầu hết các hãng khổng lồ về máy tính và truyền thông như IBM, ATT, Digital, Hewlett - Packard, Cisco Systems, Cabletron, Bay Network,... đều đang quan tâm đặc biệt đến dòng sản phẩm hướng đến ATM của mình để tung ra thị trường. Có thể kể ra đây một số sản phẩm đó như DEC 900 Multiwitch, IBM 8250 hub, Cisco 7000 rounter, Cablectron, ATM module for MMAC hub.

Nhìn chung thị trường ATM sôi động do nhu cầu thực sự của các ứng dụng đa phương tiện. Sự nhập cuộc ngày một đông của các hãng sản xuất đã làm giảm đáng kể giá bán của các sản phẩm loại này, từ đó càng mở rộng thêm thị trường. Ngay ở Việt Nam, các dự án lớn về mạng tin học đều đã được thiết kế với hạ tầng chấp nhận được với công nghệ ATM trong tương lai.

**Chương 9**

# Ví dụ một số mạng LAN và WAN

Hiện nay trên thế giới có rất nhiều mạng máy tính, chúng được sử dụng để phục vụ cho nhiều lĩnh vực khác nhau như nghiên cứu khoa học, truyền dữ liệu, kinh doanh. Vì vậy nên các mạng này cũng rất đa dạng về chủng loại. Trong phần này ta xem xét một số mạng LAN và WAN thông dụng.

## I. Mạng Novell NetWare

Được đưa ra bởi hãng Novell từ những năm 80 và đã được sử dụng nhiều trong các mạng cục bộ với số lượng ước tính hiện nay vào khoảng 50 -60%. Hệ điều hành mạng Novell NetWare là một hệ điều hành có độ an toàn cao đặc biệt là với các mạng có nhiều người sử dụng. Hệ điều hành mạng Netware khá phức tạp để lắp đặt và quản lý nhưng nó là một hệ điều hành mạng đang được dùng phổ biến nhất hiện nay. Hệ điều hành mạng Novell NetWare được thiết kế như một hệ thống mạng *client-server* trong đó các máy tính được chia thành hai loại:

- Những máy têêính cung cấp tài nguyên cho mạng gọi là *server* hay còn gọi là máy chủ mạng.
- Máy sử dụng tài nguyên mạng gọi là *clients* hay còn gọi là trạm làm việc.

Các server (File server) của Netware không chạy DOS mà bản thân Netware là một hệ điều hành cho server điều đó đã giải phóng Netware ra khỏi những hạn chế của DOS. Server của Netware dùng một cấu trúc hiệu quả hơn DOS để tổ chức các tập tin và thư mục, với Netware, chúng ta có thể chia mỗi ổ đĩa thành một hoặc nhiều tập đĩa (volumes), tương tự như các ổ đĩa logic của DOS. Các tập đĩa của Novell có tên chứ không phải là chữ cái. Tuy nhiên, để truy cập một tập đĩa của Netware từ một trạm làm việc chạy DOS, một chữ cái được gán cho tập đĩa.

Với các hệ điều hành Netware 3.x và 4.x các server phải được dành riêng, trong đó chúng ta không thể dùng một file server làm thêm việc cùa Workstation, tuy điều đó tốn kém hơn vì phải mua một máy tính để làm server nhưng nó có hiệu quả hơn vì máy tính server có thể tập trung để phục vụ mạng. Còn với Netware 2.x thì có thể lựa chọn trong đó một file server có thể làm việc như một Workstation như hai tiến trình Server và Workstation tách tời nhau hoàn toàn.

Các trạm làm việc trên một mạng Netware có thể là các máy tính DOS, chạy OS/2 hoặc các máy Macintosh. Nếu mạng vừa có máy PC và Macintosh thì Netware có thể là sự lựa chọn tốt.

Tất cả các phiên bản của Netware đều có đặc trưng được gọi là tính chịu đựng sai hỏng của hệ (System Fault Tolerance SFT) được thiết kế để giữ cho mạng vẫn chạy ngay cả khi phần cứng có sai hỏng.

NetWare là một hệ điều hành nhưng không phải là một hệ điều hành đa năng mà tập trung chủ yếu cho các ứng dụng truy xuất tài nguyên trên mạng, nó có một tập hợp xác định saün các dịch vụ dành cho người sử dụng. Tại đây Novell NetWare có một hệ thống các yêu cầu và trả lời mà Client và Server đều hiểu, nó bao gồm:

- Nhóm chương trình trên máy người dùng: Hệ điều hành trạm, các giao diện cho phép nhười sử dụng chi xuất các tài nguyên của mạng như là các tài nguyên của máy cục bộ, chương trình truyền số liệu qua mạng.

- Hệ điều hành trên máy máy chủ: Chương trình thực hiên từ DOS, Lưu các thông số của DOS, chuyển CPU của server qua chế độ protectied mode, quản lý việc sử dụng tài nguyên của mạng cho người sử dụng.

- Các tiện ích trên mạng: dành cho người sử dụng và người quản trị mạng.

- Novell NetWare hỗ trợ các giao thức cơ bản sau:

- Giao thức truy xuất (Access Protocol) (Ethernet, Token Ring, ARCnet, ProNET-10, FDDI)

- Giao thức trao đổi gói tin trên mạng (Internet Packet Exchange -IPX)

- Giao thức thông tin tìm đường (Routing Information Protocol - RIP)

- Giao thức thông báo dịch vụ (Sevice Advertising Protocol - SAP)

- Giao thức nhân NetWare (NetWare Core Protocol - NCP) cho phép người dùng truy xuất vào file server

Do nhu cầu cần thích nghi với nhiều kiểu mạng và để dễ dàng nâng cấp và quản lý, Novell NetWare cũng được chia thành nhiều tầng giao thức tương tự cấu trúc 7 tầng cuả hệ thống mở OSI.

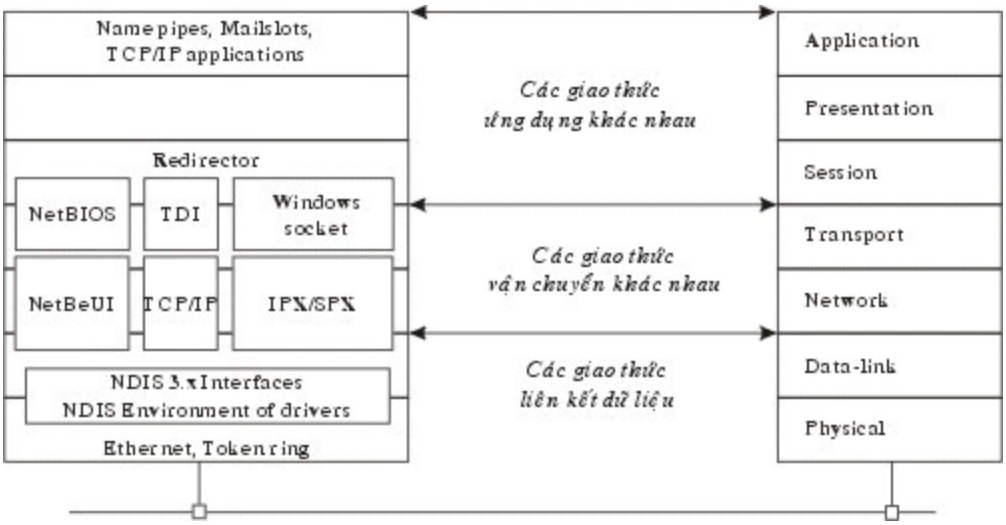
<table>
<tr><td>Tầng ứng dụng<br>(Application)</td><td rowspan="2">Giao thức<br>thông báo dịch vụ<br>(Service advertising<br>protocol - SAP)</td><td rowspan="2">Giao thức thông<br>tin tìm đường<br>(Routing Information<br>Protocol - RIP)</td><td rowspan="2">Giao thức<br>nhân NetWare<br>(NetWare core<br>protocol - NCP)</td></tr>
<tr><td>Tầng trình bày<br>(Presentation)</td></tr>
<tr><td>Tầng giao dịch<br>(Session)</td><td colspan="3">Hệ thống nhập xuất cơ bản trên mạng<br>(NetBIOS)</td></tr>
<tr><td>Tầng vận chuyển<br>(Transport)</td><td colspan="3">Trao đổi gói tin tuần tự<br>(Sequence Packet eXchange - SPX)</td></tr>
<tr><td>Tầng mạng<br>(Network)</td><td colspan="3">Trao đổi gói tin liên mạng<br>(Internet Packet Exchange - IPX)</td></tr>
<tr><td>Tầng liên kết dữ liệu<br>(Data link)</td><td colspan="3">Giao thức truy xuất và kỹ thuật mạng lưới<br>(Access protocol and wiring techniques)<br>(Chuẩn giao tiếp liên kết dữ liệu mở ODI)</td></tr>
<tr><td>Tầng vật lý<br>(Physical)</td><td colspan="3">Ethernet, Token Ring, ARCnet<br>cáp đồng trục, cáp trần xoắn cặp<br>(IEEE 802.X hoặc FDDI)</td></tr>
</table>

*Hình 9.1: Cấu trúc của Hệ điều hành Novell NetWare*

## II. Mạng Windows NT

Mạng dùng hệ điều hành **Windows NT** được đưa ra bởi hãng Microsoft với phiên bản mới nhất hiện nay là Windows NT 5.0, cụm từ windows NT được hiểu là công nghệ mạng trong môi trường Windows (Windows Network Technology). Hiện mạng Windows NT đang được đánh giá cao và được đua vào sử dụng ngày một nhiều. Windows NT là một hệ điều hành đa nhiệm, đa xử lý với địa chỉ 32 bit bộ nhớ. Ngoài việc yểm trơ các ứng dụng DOS, Windows 3.x, Win32 GUI và các ứng dụng dựa trên ký tự, Windows NT còn bao gồm các thành phần mạng, cơ chế an toàn, các công cụ quản trị có khả năng mạng diện rộng, các phần mềm truy cập từ xa. Windows NT cho phép kết nối với máy tính lớn, mini và máy Mac.

Hệ điều hành mạng Windows NT có thể chay trên máy có một CPU cũng như nhiều CPU. Hệ điều hành mạng còn có đưa vào kỹ thuật gương đĩa qua đó sử dụng tốt hệ thống nhiều đĩa nâng cao năng lực hoạt động. Hệ điều hành mạng Windows NT đảm bảo tránh được những người không được phép vào trong hệ thống hoặc thâm nhập vào các file và chương trình trên đĩa cứng. Hệ điều hành mạng Windows NT cung cấp các công cụ để thiết lập các lớp quyền dành cho nhiều nhiệm vụ khác nhau làm cho phép xây dựng hệ thống an toàn một cách mềm dẻo. Windows NT được thiết kế dành cho giải pháp nhóm (Workgroup) khi bạn muốn có kiểm soát nhiều hơn đối với mạng ngang hàng (như Windows For Workgroup, LANtastic hay Novell lite). Ngoài ra chức năng mới của Windows NT server là mô hình vùng (Domain) được thiết lập cho các mạng lớn với khả năng kết nối các mạng toàn xí nghiệp hay liên kết các kết nối mạng với các mạng khác và những công cụ cần thiết để điều hành.



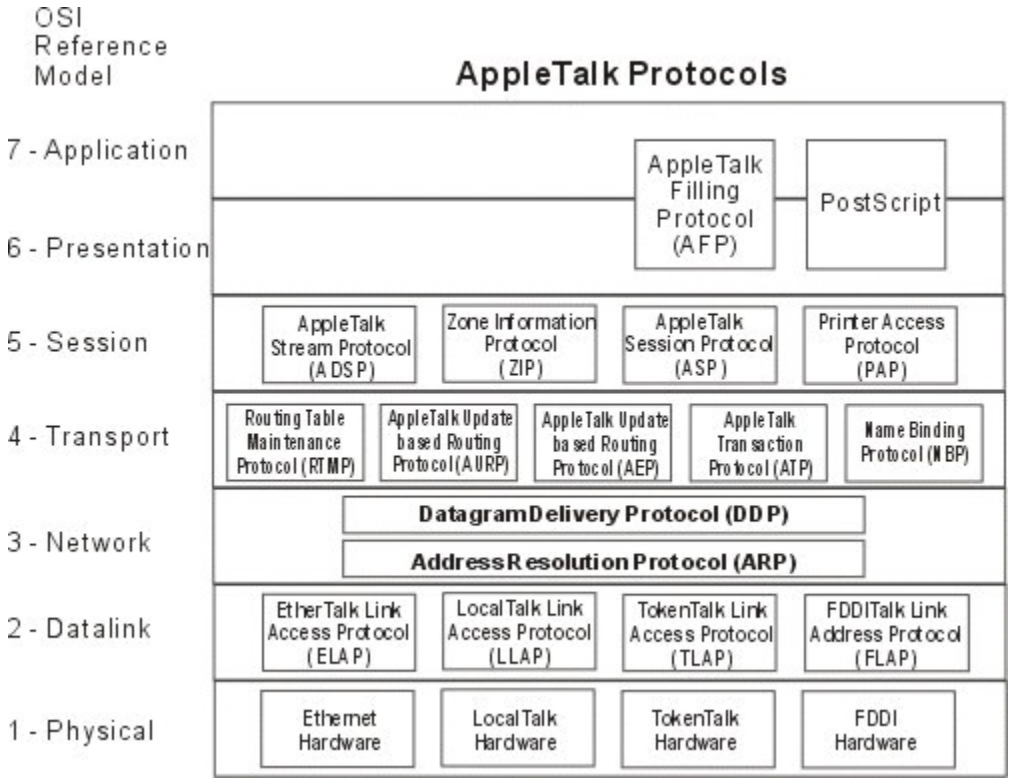

*Hình 9.2: Cấu trúc của Hệ điều hành Windows NT*

## III. Mạng Apple talk

Vào đầu những năm 1980, khi công ty máy tính Apple chuẩn bị giới thiệu máy tính Macintosh, các kỹ sư Apple đã thấy rằng mạng sẽ trở nên rất cần thiết. Họ muốn rằng mạng MAC cũng là một bước tiến mới trong cuộc cách mạng về giao diện thân thiện người dùng do Apple khởi xướng. Với ý định như vậy, Apple xây dựng một giao thức mạng cho họ máy Macintosh, và tích hợp giao thức trên vào máy tính để bàn. Cấu trúc mạng mới do Apple xây dựng được gọi là Apple Talk.

Mặc dù Apple Talk là giao thức mạng độc quyền của Apple, nhưng Apple cũng đã ấn hành nhiều tài liệu về Apple Talk trong cố gắng khuyến khích các nhà sản xuất phần mềm khác phát triển trên Apple Talk. Ngày nay đã có nhiều sản phẩm thương mại trên nền Apple Talk như của Novell, Microsoft.

Ban đầu **AppleTalk** chỉ cài đặt trên hệ thống cáp riêng của hãng là LocalTalk và có phạm vi ứng dụng rất hạn chế. Phiên bản đầu của Apple Talk được thiết kế cho nhóm người dùng cục bộ hay được gọi là *Apple Talk phase 1*. Sau khi tung ra thị trường 5 năm, số người dùng đã vượt quá 1,5 triệu người cài đặt, Apple nhận thấy những nhóm người dùng lớn đã vượt quá giới hạn của *Apple Talk phase 1*, nên họ đã nâng cấp giao thức. Giao thức đã được cải tiến được biết dưới cái tên *Apple Talk phase 2*, cải tiến khả năng tìm đường của Apple Talk và cho phép Apple Talk chạy trên những mạng lớn hơn.




*Hình 9.3: Cấu trúc của Hệ điều hành Appletalk*

Hãng Apple thiết kế Apple Talk độc lập với tầng liên kết dữ liệu. Apple hỗ trợ nhiều loại cài đặt của tầng liên kết dữ liệu, bao gồm *Ethernet, Token Ring, Fiber Distributed Data Interface* (FDDI), và *Local Talk*. Trên Apple Talk, Apple xem Ethernet như *ethertalk*, Token Ring như *tokentalk*, và FDDI như *fdditalk*.

**Các giao thức chính của mạng AppleTalk:**

- ***LLAP*** *(Local Talk Link Access)* là giao thức do Apple phát triển để hoạt động với cáp riêng của hãng (cũng được gọi là LocalTalk) dựa trên cáp xoắn đôi bọc kim (STP), thích hợp với các mạng nhỏ, hiệu năng thấp. Tốc độ tối đa là 230,4 Kb/s và khoảng cách các đoạn cáp có độ dài giới hạn là 300m, số lượng trạm tối đa là 32.

- ***ELAP*** *(Ethertalk Link Access)* và *TLAP (tokentalk Link Access)* là các giao thức cho phép sử dụng các mạng vật lý tương ứng là Ethernet và Token Ring.

- ***AARP*** *(AppleTalk Addresss Resolution Protocol)* là các giao thức cho phép ánh xạ giữa các địa chỉ vật lý của Ethernet và Token Ring, là giao diện giữa các tầng cao của AppleTalk với các tầng vật lý của Ethernet và Token Ring.

- ***DDP*** *(Datagram Delivery Protocol)* là giao thức tầng Mạng cung cấp dịch vụ theo phương thức không liên kết giữa 2 sockets (để chỉ 1 địa chỉ dịch vụ; một tổ hợp của địa chỉ thiết bị, địa chỉ mạng và socket sẽ định danh 1 cách duy nhất

cho môãi tiến trình). DDP thực hiện chức năng chọn đường (routing) dựa trên các bảng chọn đường cho RTMP bảo trì.

- ***RTMP*** *(Routing Table Maintenance protocol)* cung cấp cho DDP thông tin chọn đường trên phương pháp vector khoảng cách tương tự như RIP (Routing Information Protocol) dùng trong Netware IPX/SPX.

- ***NBP*** *(Naming Binding Protocol)*: cho phép định danh các thiết bị bởi các tên lôgic (ngoài địa chỉ của chúng). Các tên này ẩn dấu địa chỉ tầng thấp đối với người sử dụng và đối với các tầng cao hơn.

- ***ATP*** *(AppleTalk Transaction Protocol)* là giao thức thức tầng vận chuyển hoạt động với phương thức không liên kết. Dich vụ vận chuyển này được cung cấp thông qua một hệ thống các thông báo nhận và truyền lại. Độ tin cậy cũa ATP dựa trên các thao tác (transaction) (một thao tác bao gồm một cặp các thao tác hỏi-đáp).

- ***ASP*** *(AppleTalk Section Protocol)* là giao thức tầng giao dịch của AppleTalk, cho phép thiết lập, duy trì và hủy bỏ các phiên liên lạc giữa người yêu cầu dịch vụ và người cung cấp dịch vụ.

- ***ADSP*** *(AppleTalk Data Stream Protocol)* là một giao thức phủ cả tầng vận chuyển và tầng giao dịch, có thể thay cho nhóm giao thức dùng với ATP.

- ***ZIP*** *(Zone Information Protocol)* là giao thức có chức năng tổ chức các thiết bị thành các vùng (zone) để làm giảm độ phức tạp của 1 mạng bằng cách giới hạn sự tương tác của người sử dụng vào đúng các thiết bị mà anh ta cần.

- ***PAP*** *(Printer Access protocol)* cũng là 1 giao thức của tầng giao dịch tương tự như ASP. Nó không chỉ cung cấp các dịch vụ in như tên gọi mà còn yểm trợ các kiểu liên kết giữa người yêu cầu và người cung cấp dịch vụ.

- ***AFP*** *(AppleTalk Filling Protocol)* là giao thức cung cấp dịch vụ File và đảm nhận việc chuyển đổi cú pháp dữ liệu, bảo vệ an toàn dữ liệu (tương tự tầng trình bày trong mô hình OSI).

## IV. Mạng Arpanet

Đây là mạng được thiết lập tại Mỹ vào giữa những năm 60 khi bộ quốc phòng Mỹ muốn có một mạng dùng để ra lệnh và kiểm soát mà có khả năng sống còn cao trong trường hợp có chiến tranh hạt nhân. Những mạng sử dụng đường điện thoại thông thường vào lúc đó tỏ ra không đủ an toàn khi mà một đường dây hay một tổng đài bị phá hủy cũng có thể dẫn đến mọi cuộc nói chuyện hay liên lạc thông qua nó bị gián đoạn, việc đó còn đôi khi dẫn đến cắt rời liên lạc.

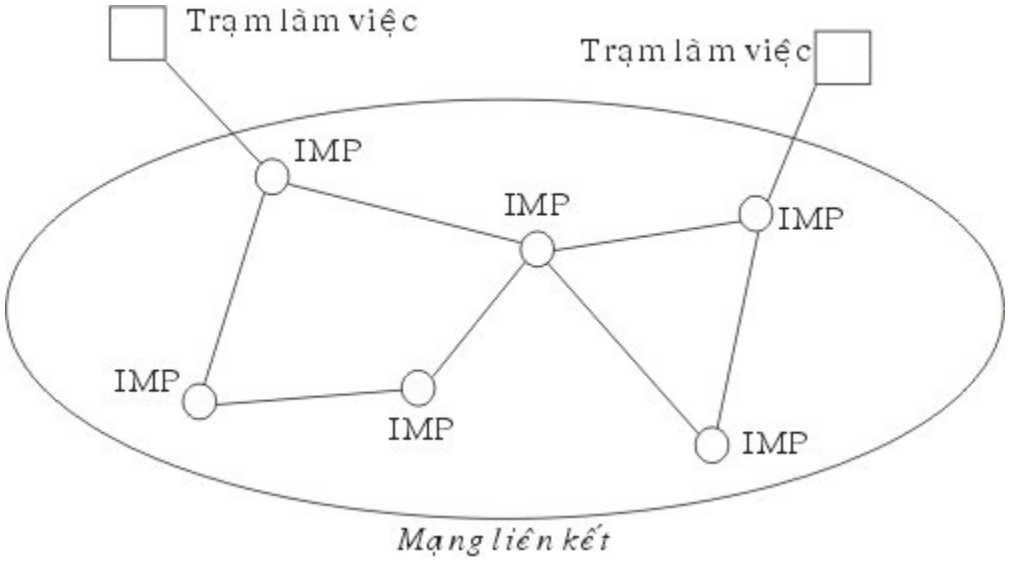
Để làm được điều này khi bộ quốc phòng Mỹ đưa ra chương trình ARPA (Advanced Research Projects Agency) với sự tham gia của nhiều trường đại học và công ty dưới sự quản lý của khi bộ quốc phòng Mỹ.

Vào đầu những năm 1960 những ý tưởng chủ yếu của chuyển mạch gói đã được Paul Baran công bố và sau khi tham khảo nhiều chuyên gia thì chương trình ARPA quyết định mạng tương lai của khi bộ quốc phòng Mỹ sẽ là mạng chuyển mạch gói và nó bao gồm một mạng liên kết và các trạm (host). Mạng liên kết bao gồm các máy tính dùng để liên kết các đường truyền dữ liệu được gọi là các điểm trung chuyển thôâng tin (IMP - Interface Message Processor).

Một IMP sẽ được liên kết với ít nhất là hai IMP khác với độ an toàn cao, các thông tin được chuyển trên mạng liên kết dưới dạng các gói dữ liệu tách rời, có nghĩa là khi có một số đường và nút bị phá hủy thì các gói tin tự động được chuyển theo những đường khác. Mỗi nút một máy tính của hệ thống bao gồm một trạm có được kết nối với một IMP trên mạng, nó gửi thông tin của mình đến IMP để rồi sau đó IMP sẽ phân gói, rồi lần lượt gửi các gói tin theo những đường mà nó lựa chọn để đến đích.

Tháng 10 năm 1968 ARPA quyết định lựa chọn hãng BBN một hãng tư vấn tại Cambridge, Massachsetts làm tổng thầu. Lúc đó BBN đã lựa chon máy DDP-316 làm IMP, các IMP được nối với đường thuê bao 56 Kbps từ các công ty điện thoại. Phần mềm được chia làm hai phần: phần liên kết mạng và phần cho nút, với phần mềm cho liên kết mạng bao gồm phần mềm tại các IMP đầu cuối và các IMP trung gian, các giao thức liên kết IMP với khả năng đảm bảo an toàn cao.

Phần mềm tại nút bao gồm phần mềm danh cho việc liên kết giữa nút với IMP, các giao thức giữa các nút với nhau trong quá trình truyền dữ liệu.




*Hình 9.4: Cấu trúc ban đầu của mạng ARPANET*

Vào tháng 10 năm 1969 mạng ARPANET bắt đầu được đưa vào hoạt động thử nghiệm với 4 nút là những trường đại học và trung tâm nghiên cứu tham gia chính vào dự án, mạng phát triển rất nhanh đến tháng 3 năm 1971 đã có 15 nút và tháng 9 năm 1972 đã có tới 35 nút. Các cải tiến tiếp theo cho phép nhiều trạm có thể liên kết với một IMP do vậy sẽ tiết kiệm tài nguyên và một trạm có thể liên kết với nhiều IMP nhằm tránh việc IMP hư hỏng làm gián đoạn liên lạc.

Cùng với việc phát triển các nút ARPA cũng dành ngân khoản cho phát triển các mạng truyền dữ liệu dùng kỹ thuật vệ tinh và dùng kỹ thuật radio. Điều đó cho phép thiết lập các nút tại những điểm các khoảng cách rất xa. Về các giao thức truyền thông thì sau khi thấy rằng các giao thức của mình không chạy được trên nhiều liên kết mạng vào năm 1974 ARPA đã đầu tư nghiên cứu hệ giao thức TCP/IP và dựa trên hợp đồng giữa BBN và Trường đại học tổng hợp Berkeley - California các nhà nghiên cứu của trường đại học đã viết rất nhiều phần mềm, chương trình quản trị trên cơ ở hệ điều hành UNIX. Dựa trên các phần mềm mới về truyền thông trên cơ sở TCP/IP đã cho phép dễ dành liên kết các mạng LAN vào mạng ARPANET. Vào năm 1983 khi mạng đã hoạt động ổn định thì phần quốc phòng của mạng (gồm khoảng 160 IMP với 110 IMP tại nước Mỹ và 50 IMP ở nước ngoài, hàng trăm nút) được tách ra thành mạng MILNETvà phần còn lại vẫn tiếp tục hoạt động như là một mạng nghiên cứu.

Trong những năm 1980 khi có nhiều mạng LAN được nối vào ARPANET để giảm việc tìm kiếm địa chỉ trên mạng người ta chia vùng các máy tính đưa tên các máy vào địa chỉ IP và xây dựng hệ quản trị cơ sở phân tán các tên các trạm của mạng Hệ cơ sở dữ liệu đó gọi là DNS (Domain Naming System) trong đó có chức mọi thông tin liên quan đến tên các trạm.

Vào năm 1990 với sự phát triển của nhiều mạng khác mà ARPANET là khởi xướng thì ARPANET đã kết thúc hoạt động của mình, tuy nhiên MILNET vẫn hoạt động cho đến ngày nay.

**V. Mạng NFSNET**

Vào cuối những năm 1970 khi Quỹ khoa học quốc gia Hoa kỳ (NFS - The U.S. National Science Foundation) thấy được sự thu hút của ARPANET trong nghiên cứu khoa học mà qua đó các nhà khoa học có thể chia sẻ thông tin hay cùng nhau nghiên cứu các đề án. Tuy nhiên việc sử dụng ARPANET cần thông qua bộ quốc phòng Mỹ với nhiều hạn chế và nhiều cơ sở nghiên cứu khoa học không có khả năng đó. Điều đó khiến NFS thiết lập một mạng ảo có tên là CSNET trong đó sử dụng các máy tính tại công ty BBN cho phép các nhà nghiên cứu có thể kết nối vào để tiếp tục nối với mạng ARPANET hay gửi thư điện tử cho nhau. Vào năm 1984 NFS bắt đầu nghiên cứu tới việc thiết lập một mạng tốc độ cao dành cho các nhóm nghiên cứu khoa học nhằm thay thế mạng ARPANET, bước đầu NFS quyết định xây dựng được đường trục truyền số liệu nối 6 máy tính lớn (Supercomputer) tại 6 trung tâm máy tính. Tại mỗi trung tâm máy tính lớn tại đây được nối với một máy mini loại LSI-11 và các máy mini được nối với nhau bằng đường thuê bao 56 Kbps tương tự như kỹ thuật đã sử dụng ở mạng ARPANET. Đồng thời NFS cũng cung cấp ngân khoản cho khoảng 20 mạng

vùng để liên kết với các máy tính lớn trên và qua đó tới các máy tính lớn khác. Toàn bộ mạng bao gồm mạng trục và các mạng vùng được gọi là NFSNET, mạng NFS có được kết nối với mạng ARPANET.

Mạng NFS được phát triển rất nhanh, sau một thời gian hoạt động đường trục chính được thay thế bằng đường cáp quang 448 Kbps và các máy IBM RS6000 được sử dụng làm công việc kết nối. Đến năm 1990 đường trục đã được nâng lên đến 1.5 Mbps.

Với việc phát triển rất nhanh và NFS thấy rằng chính quyền không có khả năng tiếp tục tài trợ nhưng do các công ty kinh doanh không thể sử dụng mạng NFSNET (do bin cấm theo luật) nên NFS yểm trợ các công ty MERIT, MCI, IBM thành lập một công ty không sinh lợi (nonprofit corporation) có tên là ANS (Advanced Networks and Services) nhằm phát triển việc kinh doanh hóa mạng. ASN tiếp nhận mạng NFSNET và bắt đầu nâng cấp đường trục lên từ 1.5 Mbps lên 45 Mbps để thành lập mạng ANSNET.

Vào năm 1995 khi các công ty cung cấp dịch vụ liên kết phát triển khắp nơi thì mạng trục ANSNET không còn cần thiết nữa và ANSNET được bán cho công ty America Online. Hiện nay các mạng vùng của NFS mua các dịch vụ truyền dữ liệu để liên kết với nhau, mạng NFS đang sử dụng dịch vụ của 4 mạng truyền dữ liệu là PacBell, Ameritech, MFS, Sprint mà qua đó các mạng vùng NFS có thể lựa chọn để kết nối với nhau.

**VI. Mạng Internet**

Cùng với sự phát triển của NFSNET và ARPANET nhất là khi giao thức TCP/IP đã trở thành giao thức chính thước duy nhất trên các mạng trên thì số lượng các mạng, nút muốn tham gia kết nối vào hai mạng trên đã tăng lên rất nhanh. Rất nhiều các mạng vùng được kết nối với nhau và còn liên kết với các mạng ở Canada, châu Aâu.

Vào khoảng giữa những năm 1980 người ta bắt đầu thấy được sự hình thành của một hệ thống liên mạng lớn mà sau này được gọi là Internet. Sự phát triển của Internet được tính theo cấp số nhân, nếu như năm 1990 có khoảng 200.000 máy tính với 3.000 mạng con thì năm 1992 đã có khoảng 1.000.000 máy tính được kết nối, đến năm 1995 đã có hàng trăm mạng cấp vùng, chục ngàn mạng con và nhiều triệu máy tính. Rất nhiều mạng lớn đang hoạt động cũng đã được kết nối vào Internet như các mạng SPAN, NASA network, HEPNET, BITNET, IBM network, EARN. Việc liên kết các mạng được thực hiện thông qua rất nhiều đường nối có tốc độ rất cao.

Hiện nay một máy tính được gọi là thành viên của Internet nếu máy tính đó có giao thức truyền dữ liệu TCP/IP, có một địa chỉ IP trên mạng và nó có thể gửi các gói tin IP đến tất cả các máy tính khác trên mạng Internet.

Tuy nhiên trong nhiều trường hợp thông qua một nhà cung cấp dịch vụ Internet người sử dụng kết nối máy của mình với máy chủ của nhà phục vụ và được cung cấp một địa chỉ tạm thời trước khi khai thác các tài nguyên của Internet. Máy tính của người đó

có thể gửi các gói tin cho các máy khác bằng địa chỉ tạm thời đó và địa chỉ đó sẽ trả lại cho nhà cung cấp khi kết thúc liên lạc. Vì máy tính của người đó sử dụng trong thời gian liên kết với Internet cũng có một địa chỉ IP nên người ta vẫn coi máy tính đó là thành viên của Internet.

Vào năm 1992 cộng đồng Internet đã ra đời nhằm thúc đẩy sự phát triển của Internet và điều hành nó. Hiện nay Internet có 5 dịch vụ chính:

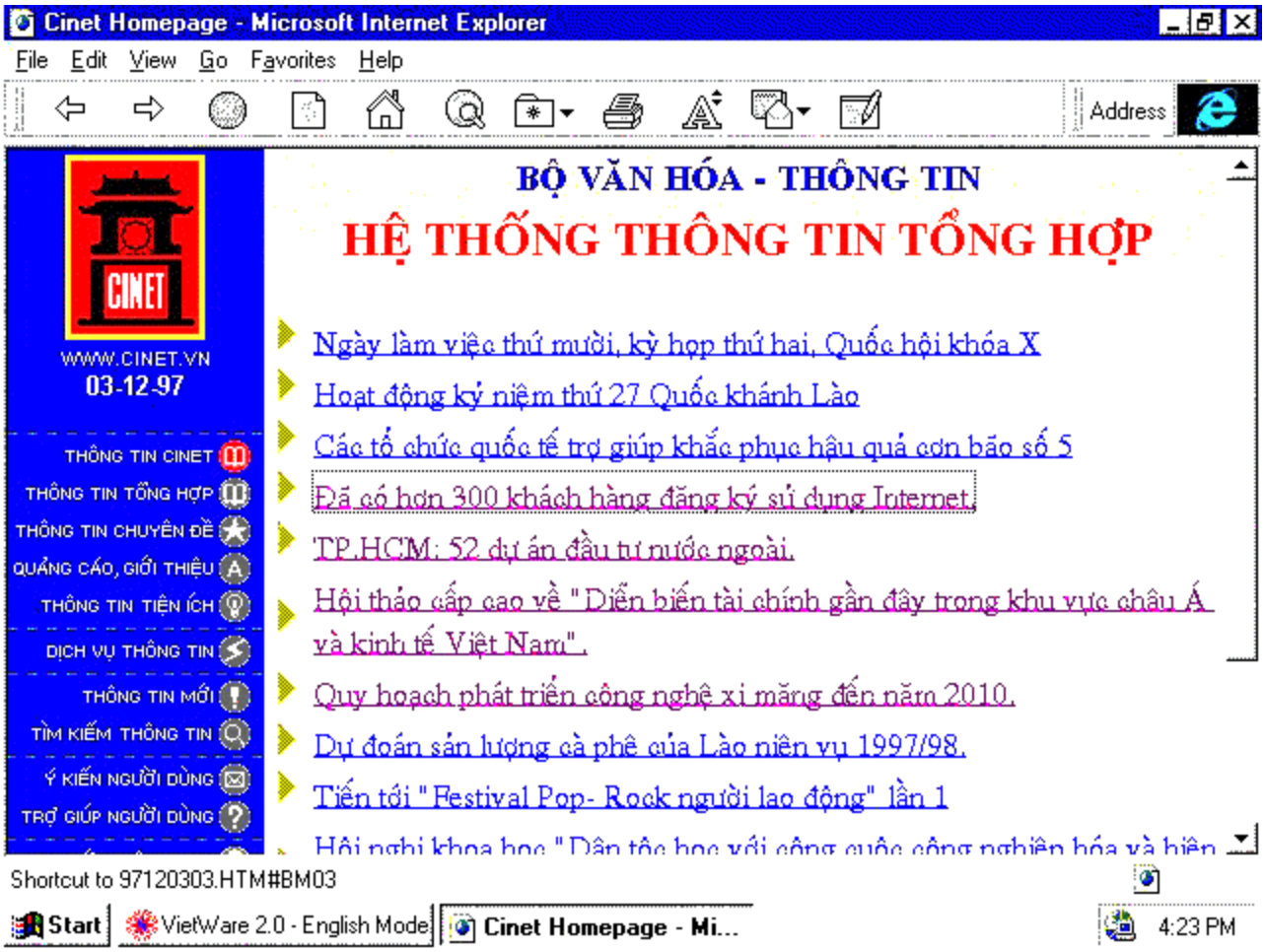
- **Thư điện tử** (Email): đây là dịch vụ đã có từ khi mạng ARPANET mới được thiết lập, nó cho phép gửi và nhận thư điến tử cho mọi thành viên khác trong mạng.

- **Thông tin mới** (News): Các vân đề thời sự được chuyển thành các diễn đàn cho phép mọi người quan tâm có thể trao đổi các thông tin cho nhau, hiện nay hiện nay có hàng nghìn diễ đàn về mọi mặt trên Internet.

- **Đăng nhập từ xa** (Remote Login): Bằng các chương trình như Telnet, Rlogin người sử dụng có thể từ một trạm của Internet đăng nhập (logon) vào một trạm khác nếu như người đó được đăng ký trên máy tính kia.

- **Chuyển file** (File transfer): Bằng chương trình FTP người sử dụng có thể chép các file từ một máy tính trên mạng Internet tới một máy tính khác. Người ta có thể chép nhiều phần mềm, cơ sở dữ liệu, bài báo bằng cách trên.

- **Dịch vụ WWW** (World Wide Web): WWW là một dịch vụ đặc biệt cung cấp thông tin từ xa trên mạng Internet. Các tập tin siêu văn bản được lưu trữ trên máy chủ sẽ cung cấp các thông tin và dẫn đường trên mạng cho phép người sử dụng dễ dàng Truy cập các tập tin văn bản, đồ họa, âm thanh.




*Hình 9.5: Ví dụ một trang Web cho phép dễ dàng khai thác các trang Web khác*

Người sử dụng nhận được thông tin dưới dạng các trang văn bản, một trang là một đơn thể nằm trong máy chu. Đây là dịch vụ đang mang lại sức thu hút to lớn cho mạng Internet, chúng ta có thể xây dựng các trang Web bằng ngôn ngữ HTML (Hypertext Markup Language) với nhiều dạng phong phú như văn bản, hình vẽ, video, tiếng nói và có thể có các kết nối với các trang Web khác. Khi các trang đó được đặt trên các máy chủ Web thì thông qua Internet người ta có thể xem được sự thể hiện của các trang Web trên và có thể xem các trang web khác mà nó chỉ đến.

Các phần mềm thông dụng được sử dụng hiện nay để xây dựng và duyệt các trang Web là Mosaic, Navigator của Netscape, Internet Explorer của Microsoft, Web Access của Novell.

**Chương 10 :**

# Giới thiệu về hệ điều hành mạng Windows NT

## I. Thế nào là một hệ điều hành mạng

Với việc ghép nối các máy tính thành mạng thì cần thiết phải có một hệ thống phần mềm có chức năng quản lý tài nguyên, tính toán và xử lý truy nhập một cách thống nhất trên mạng, hệ như vậy được gọi là hệ điều hành mạng. Mỗi tài nguyên của mạng như tệp, đĩa, thiết bị ngoại vi được quản lý bởi một tiến trình nhất định và hệ điều hành mạng điều khiển sự tương tác giữa các tiến trình và truy cập tới các tiến trình đó.

Căn cứ vào việc truy nhập tài nguyên trên mạng người ta chia các thực thể trong mạng thành hai loại chủ và khách, trong đó máy khách (Client) truy nhập được vào tài nguyên của mạng nhưng không chia sẻ tài nguyên của nó với mạng, còn máy chủ (Server) là máy tính nằm trên mạng và chia sẻ tài nguyên của nó với các người dùng mạng.

Hiện nay các hệ điều hành mạng thường được chia làm hai loại là hệ điều hành mạng ngang hàng (Peer-to-peer) và hệ điều hành mạng phân biệt (client/server).

Với hệ điều hành mạng ngang hàng mỗi máy tính trên mạng có thể vừa đóng vai trò chủ lẫn khách tức là chúng vừa có thể sử dụng tài nguyên của mạng lẫn chia sẻ tài nguyên của nó cho mạng, ví dụ: LANtastic của Artisoft, NetWare lite của Novell, Windows (for Workgroup, 95, NT Client) của Microsoft.

Với hệ điều hành mạng phân biệt các máy tính được phân biệt chủ và khách, trong đó máy chủ mạng (Server) giữ vai trò chủ và các máy cho người sử dụng giữ vai trò khách (các trạm). Khi có nhu cầu truy nhập tài nguyên trên mạng các trạm tạo ra các yêu cầu và gửi chúng tới máy chủ sau đó máy chủ thực hiện và gửi trả lời. Ví dụ các hệ điều hành mạng phân biệt: Novell Netware, LAN Manager của Microsoft, Windows NT Server của Microsoft, LAN Server của IBM, Vines của Banyan System với server dùng hệ điều hành Unix.

## II. Hệ điều hành mạng Windows NT

Windows NT là hệ điều hành mạng cao cấp của hãng Microsoft. Phiên bản đầu có tên là Windows NT 3.1 phát hành năm 1993, và phiên bản server là Windows NT Advanced Server (trước đó là LAN Manager for NT). Năm 1994 phiên bản Windows NT Server và Windows NT Workstation version 3.5 được phát hành. Tiếp theo đó ra đời các bản version 3.51. Các phiên bản workstation có sử dụng để thành lập mạng ngang hàng; còn các bản server dành cho quản lý file tập trung, in ấn và chia sẻ các ứng dụng.

Năm 1995, Windows NT Workstation và Windows NT Server version 4.0 ra đời đã kết hợp shell của người anh em Windows 95 nổi tiếng phát hành trước đó không lâu (trước

đây shell của Windows NT giống shell của Windows 3.1) đã kết hợp được giao diện quen thuộc, dễ sử dụng của Windows 95 và sự mạnh mẽ, an toàn, bảo mật cao của Windows NT.

Windows NT có hai bản mà nó đi đôi với hai cách tiếp cận mạng khác nhau. Hai bản này gọi là Windows NT Workstation và Windows NT server. Với hệ điều hành chuẩn của NT ta có thể xây dựng mạng ngang hàng, máy chủ mạng và mọi công cụ quản trị cần thiết cho một máy chủ mạng ngoài ra còn có thể có nhiều giải pháp về xây dựng mạng diện rộng. Cả hai bản Windows NT station và Windows NT server cùng được xây dựng trên cơ sở nhân NT chung và các giao diện và cả hai cùng có những đặc trưng an toàn theo tiêu chuẩn C2. Windows NT Wordstation được sử dụng để kết nối những nhóm người sử dụng nhỏ, thường cùng làm việc trong một văn phòng. Tuy nhiên với Windows NT server ta có được một khả năng chống hỏng hóc cao, những khả năng cung cấp dịch vụ mạng lớn và những lựa chon kết nối khác nhau, Windows NT Server không hạn chế về số người có thể thâm nhập vào mạng.

Với Windows NT ta cũng có những công cụ quản trị từ xa vào mạng mà có thể thực hiện được việc quản trị từ những máy tính ở xa. Nó thích hợp với tất cả các sơ đồ mạng BUS, STAR, RING và hỗn hợp.

Windows NT là hệ điều hành có sức mạnh công nghiệp đầu tiên cho số lượng khổng lồ các máy tính IBM compatible. Windows NT là một hệ điều hành thực sự dành cho người sử dụng, các cơ quan, các công ty xí nghiệp. Windows NT là một hệ điều hành đa nhiệm, đa xử lý với địa chỉ 32 bit bộ nhớ. Nó yểm trợ các ứng dụng DOS, Windows, Win32 GUI và các ứng dụng dựa trên ký tự. Windows NT server là một hệ điều hành mạng hoàn chỉnh, nó nhanh chóng được thừa nhận là một trong những hệ điều hành tốt nhất hiện nay vì:

- Là hệ điều hành mạng đáp ứng tất cả các giao thức truyền thông phổ dụng nhất. Ngoài ra nó vừa cho phép giao lưu giữa các máy trong mạng, vừa cho phép truy nhập từ xa, cho phép truyền file v.v... Windows NT là hệ điều hành vừa đáp ứng cho mạng cục bộ (LAN) vừa đáp ứng cho mạng diện rộng (WAN) như Intranet, Internet.

- Windows NT server hơn hẳn các hệ điều hành khác bởi tính mềm dẻo, đa dạng trong quản lý. Nó vừa cho phép quản lý mạng theo mô hình mạng phân biệt (Clien/Server), vừa cho phép quản lý theo mô hình mạng ngang hàng (peer to peer).

- Windows NT server đáp ứng tốt nhất các dịch vụ viễn thông, một dịch vụ được sử dụng rộng rãi trong tương lai.

- Windows NT server cài đặt đơn giản, nhẹ nhàng và điều quan trọng nhất là nó tương thích với hầu như tất cả các hệ mạng, nó không đòi hỏi người ta phải thay đổi những gì đã có.

- Cho phép dùng các dịch vụ truy cập từ xa (Remote access service - RAS), có khả năng phụp vụ đến 64 cổng truy nhập từ xa (trong đó Lan manager 16 cổng).

- Đáp ứng cho cả các máy trạm Macintosh nối với Windows NT server.

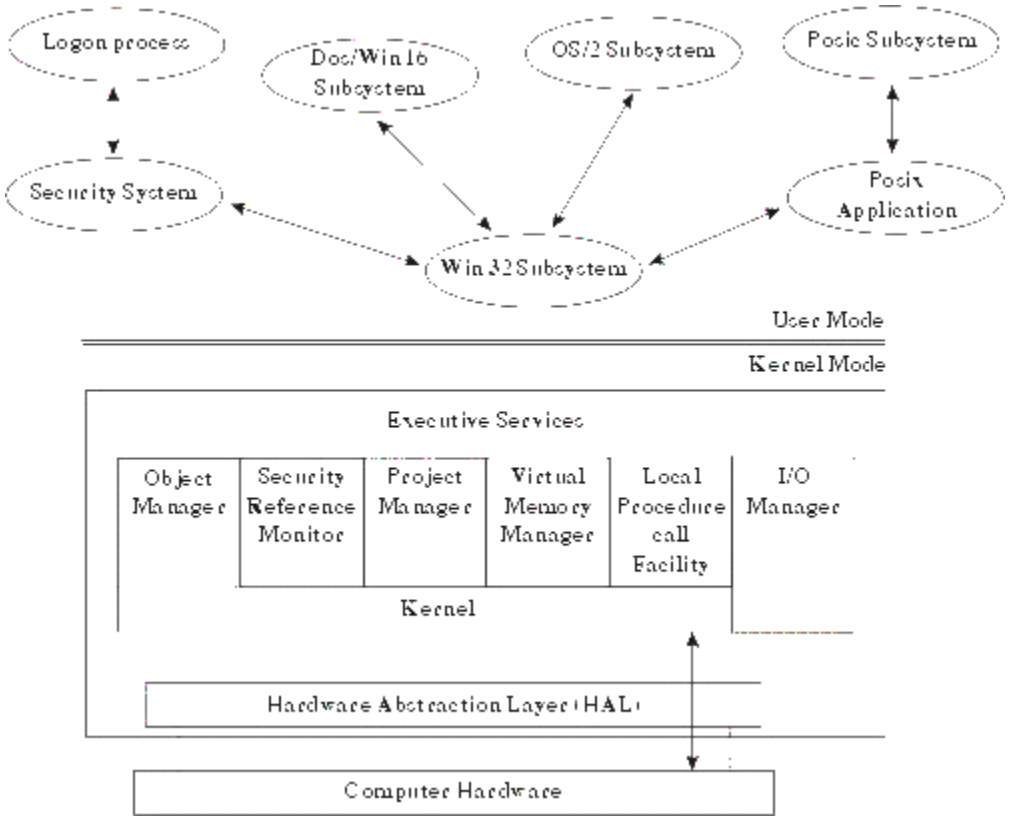
Windows NT yểm trợ mọi nghi thức mạng chuẩn như NetBUEI, IPX/SPX, TCP/IP và các nghi thức khác. Windows NT cũng tương thích với những mạng thông dụng hiên nay như Novell NetWare, Banyan VINES, và Microsoft LAN Manager. Đối với mạng lớn và khả năng thâm nhập từ xa sản phẩm Windows NT Server cũng cũng cấp các chức năng bổ xung nhu khả năng kết nối với máy tính lớn và máy MAC.

**III. Cấu trúc của hệ điều hành Windows NT**

Windows NT được thiết kế sử dụng cách tiếp cận theo đơn thể (modular). Các đơn thể khác nhau (còn được gọi là các bộ phận, thành phần) của Windows NT được trình bày trong hình 1 Các bộ phận của Windows NT có thể chạy dưới hai chế độ: User (người sử dụng) và Kernel (cốt lõi của hệ điều hành). Khi một thành phần của hệ điều hành chạy dưới cốt lõi của hệ điều hành (Kernel), nó truy cập đầy đủ các chỉ thị máy cho bộ xử lý đó và có thể truy cập tổng quát toàn bộ tài nguyên trên hệ thống máy tính.

Trong Windows NT: Executive Services, Kernel và HAL chạy dưới chế độ cốt lõi của hệ điều hành.

Hệ thống con (Subsystem) Win 32 và các hệ thống con về môi trường, chẳng hạn như DOS/Win 16.0S/2 và hệ thống con POSIX chạy dưới chế độ user. Bằng cách đặt các hệ thống con này trong chế độ user, các nhà thiết kế Windows NT có thể hiệu chỉnh chúng dễ dàng hơn mà không cần thay đổi các thành phần được thiết kế để chạy dưới chế độ Kernel.




*Hình 10.1: Cấu trúc Windows NT*

**Các lớp chính của hệ điều hành WINDOWS NT SERVER gồm:**

- ***Lớp phần cứng trừu tượng (Hardware Astraction Layer - HAL):*** Là phần cứng máy tính mà cốt lõi của hệ điều hành (Kernel) có thể được ghi vào giao diện phần cứng ảo, thay vì vào phần cứng máy tính thực sự. Phần lớn cốt lõi của hệ điều hành sử dụng HAL để truy cập các tài nguyên máy tính. Điều này có nghĩa là cốt lõi của hệ điều hành và tất cả các thành phần khác phụ thuộc vào cốt lõi có thể dễ dàng xuất (Ported) thông qua Microsoft đến các nền ( Platform ) phần cứng khác. Một thành phân nhỏ trong cốt lõi của hệ điều hành, cũng như bộ quản lý Nhập / Xuất truy cập phần cứng máy tính trực tiếp mà không cần bao gồm HAL.

- ***Lớp Kernel cốt lõi của hệ điều hành):*** Cung cấp các chức năng hệ điều hành cơ bản được sử dụng bởi các thành phần thực thi khác. Thành phần Kernel tương đối nhỏ và cung cấp các thành phần cốt yếu cho những chức năng của hệ điều hành. Kernel chủ yếu chịu trách nhiệm quản lý luồng, quản lý phần cứng và đồng bộ đa sử lý.

- **Các thành phần Executive:** Là các thành phần hệ điều hành ở chế độ Kernel thi hành các dịch vụ như :

  - Quản lý đối tượng (object manager)

- Bảo mật (security reference monitor)
- Quản lý tiến trình (process manager)
- Quản lý bộ nhớ ảo (virtual memory manager)
- Thủ tục cục bộ gọi tiện ích, và quản trị nhập/xuất (I/O Manager)

## IV.Cơ chế quản lý của Windows NT

### *1. Quản lý đối tượng* (Object Manager):

Tất cả tài nguyên của hệ điều hành được thực thi như các đối tượng. Một đối tượng là một đại diện trừu tượng của một tài nguyên. Nó mô tả trạng thái bên trong và các tham số của tài nguyên và tập hợp các phương thức (method) có thể được sử dụng để truy cập và điều khiển đối tượng.

Ví dụ một đối tượng tập tin sẽ có một tên tập tin, thông tin trạng thái trên file và danh sách các phương thức, như tạo, mở,đóng và xóa, đối tượng mô tả các thao tác có thể được thực hiện trên đối tượng file.

Bằng cách xử lý toàn bộ tài nguyên như đối tượng Windows NT có thể thực hiện các phương thức giống nhau như: tạo đối tượng, bảo vệ đối tượng, giám sát việc sử dụng đối tượng (Client object) giám sát những tài nguyên được sử dụng bởi một đối tượng.

Việc quản lý đối tượng (Object Manager) cung cấp một hệ thống đặt tên phân cấp cho tất cả các đối tượng trong hệ thống. Do đó, tên đối tượng tồn tại như một phần của không gian tên toàn cục và được sử dụng để theo dõi việc tạo và sử dụng đối tượng.

Sau đây là một số ví dụ của loại đối tượng Windows NT :

- Đối tượng Directory (thư mục).
- Đối tượng File (tập tin).
- Đối tượng kiểu object.
- Đối tượng Process (tiến trình).
- Đối tượng thread (luồng).
- Đối tượng Section and segment (mô tả bộ nhớ).
- Đối tượng Port (cổng).
- Đối tượng Semaphore và biến cố.

- Đối tượng liên kết Symbolic (ký hiệu).

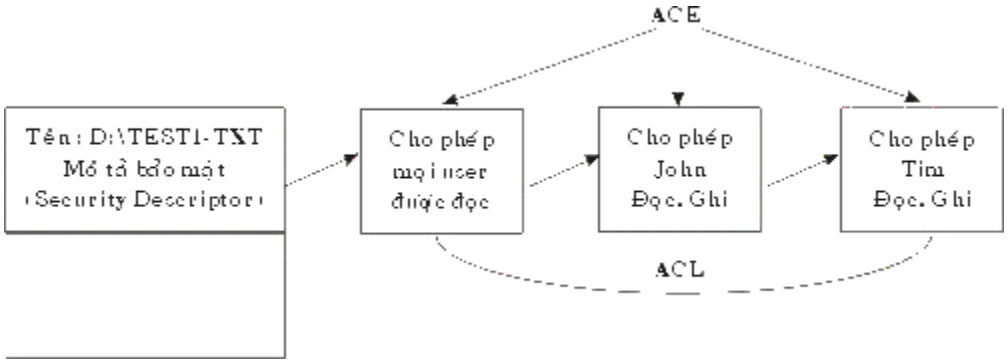
### *2. Cơ chế bảo mật* (SRM - Security Reference Monitor):

Được sử dụng để thực hiện vấn đề an ninh trong hệ thống Windows NT. Các yêu cầu tạo một đối tượng phải được chuyển qua SRM để quyết định việc truy cập tài nguyên được cho phép hay không. SRM làm việc với hệ thống con bảo mật trong chế độ user. Hệ thống con này được sử dụng để xác nhận user login vào hệ thống Windows NT.

Để kiểm soát việc truy cập, mỗi đối tượng Windows NT có một danh sách an toàn (Access Control List - ACL). Danh sách an toàn của mỗi đối tượng gồm những phần tử riêng biệt gọi là Access Control Entry (ACE). Mỗi ACE chứa một SecurityID (SID: số hiệu an toàn) của người sử dụng hoặc nhóm. Một SID là một số bên trong sử dụng với máy tính Windows NT mô tả một người sử dụng hoặc một nhóm duy nhất giữa các máy tính Windows NT.

Ngoài SID, ACE chứa một danh sách các hành động (action) được cho phép hoặc bị từ chối của một user hoặc một nhóm. Khi người sử dụng đăng nhập vào mạng Windows NT, sau khi việc nhận dạng thành công, một Security Access Token (SAT) được tạo cho người dùng đó. SAT chứa SID của người dùng và SID của tất cả các nhóm người dùng thuộc mạng Windows NT. Sau đó SAT hoạt động như một "passcard" (thẻ chuyển) cho phiên làm việc của người dùng đó và được sử dụng để kiểm tra tất cả hoạt động của người dùng.

Khi người dùng tham gia mạng truy cập một đối tượng, Security Reference Monitor kiểm tra bộ mô tả bảo mật của đối tượng xem SID liệt kê trong SAT có phù hợp với giá trị trong ACE không. Nếu phù hợp, các quyền về an ninh được liệt trong ACE áp dụng cho người dùng đó.




*Hình 10.2: Ví dụ về danh sách an toàn (Access Control List).*

### *3. Quản lý nhập / xuất (I/O Manager) :*

Chịu trách nhiệm cho toàn bộ các chức năng nhập / xuất trong hệ điều hành Windows NT. I/O Manager liên lạc với trình điều khiển của các thiết bị khác nhau.

**4. I/O *Manager:***

Ssử dụng một kiến trúc lớp cho các trình điều khiển. Mỗi bộ phận điều khiển trong lớp này thực hiện một chức năng được xác định rõ. Phương pháp tiếp cận này cho phép một thành phần điều khiển được thay thế dễ dàng mà không ảnh hưởng phần còn lại của các bộ phận điều khiển.


*Hình 10.3:Các trình điều khiển thiết bị theo lớp của I / O Manager*

## V. Các cơ chế bảo vệ dữ liệu trong Windows NT

Cơ chế bảo vệ dữ liệu của Windows NT gọi là fault tolerance, nó cho phép hệ thống khả năng tiếp tục làm việc và bảo toàn dữ liệu của hệ thống trong trường hợp một phần của hệ thống có sự cố hỏng hóc sai lệch. Trong Windows NT cơ chế fault tolerance bao gồm các biện pháp sau:

- Chống cúp điện bất thường.
- Cung cấp khả năng bảo vệ hệ thống đĩa (fault tolerance disk subsystem).
- Cung cấp khả năng sao chép dự phòng (backup) từ băng từ.

Khả năng bảo vệ hệ thống đĩa của Windows NT là RAID ø (viết tắt của Redundant Array of Inexpensiredisk). Thực chất RAID là một loạt các biện pháp để bảo vệ hệ thống đĩa. Các biện pháp trong RIAD được chia thành 6 mức sau:

- ***Mức 0*:** Đây là mức ứng với biện pháp chia nhỏ đĩa (disk striping). Thực chất nội dung của biện pháp này là phân chia dữ liệu thành khối và sau đó sắp xếp các khối dữ liệu theo thứ tự trong tất cả các đĩa thành 1 mảng.
- ***Mức 1*:** Mức này ứng với biện pháp disk Mirroring, biện pháp này cho phép tạo ra 2 đĩa giống nhau. Nếu trong quá trình vận hành mạng một đĩa có sự cố thì hệ thống sử dụng dữ liệu của đĩa kia.
- ***Mức 2*:** Mức này ứng với biện pháp phân chia nhỏ đĩa bằng cách phân chia các file thành các byte và sắp xếp các byte sang nhiều đĩa. Mức này sử dụng mã

sửa sai (error correcting code) trong quá trình phân chia đĩa. Nói chung biện pháp dùng ở mức này tốt hơn biện pháp dùng trong mức 1.

- ***Mức 3*:** Mức này sử dụng biện pháp giống mức 2. Tuy nhiên mã sửa sai (error correction code) chỉ sử dụng cho một đĩa. Không áp dụng cho nhiều đĩa như ở mức 2. Người ta thường dùng mức này để truy nhập vào một số ít file có dung tích lớn.

- ***Mức 4*:** Mức này sử dụng biện pháp giống ở mức 2 và 3 nhưng bằng phương pháp phân chia đĩa thành các khối lớn. Giống như mức 3 tất cả các mã sửa sai (error correction code) được hgi vào một đĩa và tách khỏi khối dữ liệu.

- ***Mức 5*:** Trong mức này người ta sử dụng biện pháp phân chia đĩa thành từng phần gọi là Striping with party. Biện pháp sử dụng ở mức này tương tự như ức 4, số liệu được phân nhỏ thành các khối lớn và sau đó ghi vào tất cả các đĩa. Các thông tin (party Infomation) được coi như các dữ liệu dùng tạm thời (data redundancy).

**Ngoài ra chúng ta còn có thể áp dụng các biện pháp bảo vệ dữ liệu trong Windows NT:**

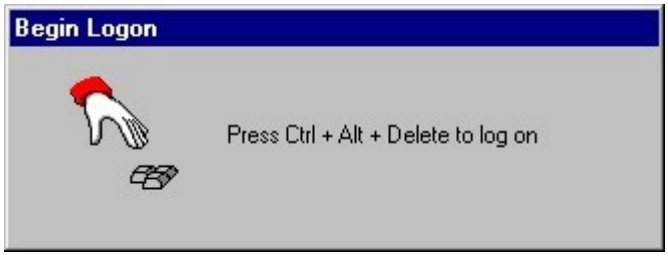
- ***Biện pháp Disk mirroring:*** Disk mirroring là cách sao tạm (redundant) lại đĩa hoặc partition. Biện pháp này bảo vệ dữ liệu tránh các sự cố bằng cách dưa ra chế độ thường xuyên backup đĩa hoặc partition. Hình dưới chỉ ra cách dùng biện pháp Mirroring:

- ***Disk Duplexing:*** Biện pháp dùng đĩa kép (Disk Duplexing) tường tự như disk mirroring chỉ khác là chúng dùng 2 disk controler. Diều này cho thên hả năng bảo vệ khi controler của một đĩa có sự cố. Trong khi đó biện pháp Mirror không thể khắc phục được tình huống này.

- ***Mirror Set:*** Các partition hoặc đĩa trong chế độ Mirror được tạo ra bằng cách lặp sao lại partition hoặc đĩa trên đĩa khác cùng một tên ổ đĩa được gán cho cả 2 partition. Ta có thể dùng establish Mirror trong menu Fault tolerance. Nếu đĩa hoặc partition trong chế độ Mirror bị lỗi thì chế độ Mirror cần phải ngắt để thực hiện chế độ sao chép dự phòng vào một đĩa riệng. Sau đó sao backup trở lại.

## VI. Giới thiệu về hoạt động của Windows NT Server

Khi chúng ta khởi động Windows NT Server hộp Begin logon sẽ hiện ra, server chờ đợi để chúng ta bấm Ctrl+Alt +Del để có thể tiếp tục hoạt động. Ở đây có điểm khác với các hệ điều hành DOS, Windows 95 là tổ hợp Ctrl+Alt +Del không phải là khởi động lại máy. Trong trường hợp này Windows NT loại bỏ mọi chương trình Virus hay không có phép đang hoạt động trước khi bước vào làm việc.




*Hình 10.4: Thông báo gia nhập mạng*

Lúc này chúng ta sẽ thấy hộp Logon Information xuất hiện và yếu cầu chúng ta phải đánh đúng tên và mật khẩu thì mới được đăng nhập vào Server. Nếu là người dùng mới thì phải được người quản trị khai báo tên và mật khẩu trước khi đăng nhập..


*Hình 10.5: Màn hình gia nhập mạng*

Cũng giống như màn hình nền của hệ điều hành Windows 95 khi muốn thực hiện các trình, gọi các menu hệ thống chúng ta dùng nút Start ở cuối màn hình


*Hình 10.6: Điểm khởi đầu của Windows*

Trước muốn kết thúc chương trình và tắt máy chúng ta phải bấm phím Start rồi chọn ShutDown, màn hình kết thúc sẽ hiện ra cho chúng ta lựa chon công yêu cầu về tắt hay khởi động lại.


*Hình 10.7: Màn hình thoát khỏi Windows*

**Chương 11**

# Hệ thống quản lý của mạng Windows NT

Các mạng máy tính hiện nay được thiết kế rất đa dạng và đang thực hiện những ứng dụng trên nhiều lĩnh vực của đời sống xã hội. Điều đó có nghĩa là các thông tin lưu trữ trên mạng và các thông tin truyền giao trên mạng ngày càng mang nhiều giá trị có ý nghĩa sống còn. Do vậy những người quản trị mạng ngày càng phải quan tâm đến việc bảo vệ các tài nguyên của mình.

Việc bảo vệ an toàn là quá trình bảo vệ mạng khỏi bị xâm nhập hoặc mất mát, khi thiết kế các hệ điều hành mạng người ta phải xây dựng một hệ thống quản lý nhiều tầng và linh hoạt giúp cho người quản trị mạng có thể thực hiện những phương án về quản lý từ đơn giản mức độ thấp cho đến phức tạp mức độ cao trong những mạng có nhiều người tham gia. Thông qua những công cụ quản trị đã được xây dựng saün người quản trị có thể xây dựng những cơ chế về an toàn phù hợp với cơ quan của mình.

Thông thường hệ thống mạng có những mức quản lý chính sau:

- **Mức quản lý việc thâm nhập mạng (Login/Password):** Mức quản lý việc thâm nhập mạng (Login/Password) xác định những ai và lúc nào có thể vào mạng. Đối với người quản trị và người sử dụng mạng, mức an toàn này dường như khá đơn giản mà theo đó mỗi người sử dụng (người sử dụng) có một tên login và mật khẩu duy nhất.

- **Mức quản lý trong việc quản lý sử dụng các tài nguyên của mạng:** Kiểm soát những tài nguyên nào mà người sử dụng được phép truy cập, sử dụng và sử dụng như thế nào.

- **Mức quản lý với thư mục và file:** Mức an toàn của file kiểm soát những file và thư mục nào người sử dụng được dùng trên mạng và được sử dụng ở mức độ nào

- **Mức quản lý việc điều khiển File Server:** Mức an toàn trên máy chủ kiểm soát ai có thể được thực hiện các thao tác trên máy chủ như bật, tắt, chạy các chương trình khác. Người ta cần có cơ chế như mật khẩu để bảo vệ.

## I. Quản lý các tài nguyên trong mạng

Như chúng ta đã biết, mạng LAN cung cấp các dịch vụ theo hai cách: qua cách chia sẻ tài nguyên theo nguyên tắc ngang hàng và thông qua những máy chủ trung tâm. Dù bất cứ phương pháp nào được sử dụng, vấn đề cần phải giải quyết là là giúp người sử dụng xác định được các tài nguyên có saün ở đâu để có thể sử dụng.

Các kỹ thuật sau đây đã được sử dụng để tổ chức tài nguyên mạng máy tính:

- Quản lý đơn lẻ từng máy chủ (stand-alone services).
- Quản lý theo dịch vụ thư mục (directory services).
- Quản lý theo nhóm (workgroups).
- Quản lý theo domain (domains).

### 1. Quản lý đơn lẻ từng máy chủ (Stand-alone Services)

Với cách quản lý này trong mạng LAN thường chỉ có một vài máy chủ, mỗi máy chủ sẽ quản lý tài nguyên của mình, mỗi người sử dụng muốn thâm nhập những tài nguyên của máy chủ nào thì phải khai báo và chịu sự quản lý của máy chủ đó. Mô hình trên phù hợp với những mạng nhỏ với ít máy chủ và khi có trục trặc trên một máy chủ thì toàn mạng vẫn hoạt động. Cũng vì trong mạng LAN chỉ có ít máy chủ, do đó người sử dụng không mấy khó khăn để tìm các tập tin, máy in và các tài nguyên khác của mạng (plotter, CDRom, modem...).

Việc tổ chức như vậy không cần những dịch vụ quản lý tài nguyên phức tạp. Tuy nhiên khi trong mạng có từ hai máy chủ trở lên vấn đề trở nên phức tạp hơn vì mỗi máy chủ riêng lẻ giữ riêng bảng danh sách các người sử dụng và tài nguyên của mình. Khi đó mỗi người sử dụng phải tạo lập và bảo trì tài khoản của mình ở hai máy chủ khác nhau mới có thể đăng nhập (logon) và truy xuất đến các máy chủ này. Ngoài ra việc xác định vị trí của các tài nguyên trong mạng cũng rất khó khăn khi mạng có qui mô lớn.

### 2. Quản lý theo dịch vụ thư mục (Directory Services)

Hệ thống các dịch vụ thư mục cho phép làm việc với mạng như là một hệ thống thống nhất, tài nguyên mạng được nhóm lại một cách logic để dễ tìm hơn. Giải pháp này có thể được dùng cho những mạng lớn. Ở đây thay vì phải đăng nhập vào nhiều máy chủ, người sử dụng chỉ cần đăng nhập vào mạng và được các dịch vụ thư mục cấp quyền truy cập đến tài nguyên mạng, cho dù được cung cấp bởi bất kể máy chủ nào.

Người quản trị mạng chỉ cần thực hiện công việc của mình tại một trạm trên mạng mặc dù các điểm nút của nó có thể nằm trên cả thế giới. Hệ điều hành Netware 4.x cung cấp dịch vụ nổi tiếngi và đầy ưu thế cạnh tranh này với tên gọi ***Netware Directory Services (NDS).***

Giải pháp này thích hợp với những mạng lớn. Các thông tin của NDS được đặt trong một hệ thống cơ sở dữ liệu đồng bộ, rộng khắp được gọi là DIB (Data Information Base). Cơ sở dữ liệu trên quản lý các dữ liệu dưới dạng các đối tượng phân biệt trên toàn mạng. Các định nghĩa đối tượng sẽ được đặt trên các tập tin riêng của một số

máy chủ đặc biệt, mỗi đối tượng có các tính chất và giá trị của mỗi tính chất. Đối tượng bao hàm tất cả những gì có tên phân biệt như Người sử dụng, File server, Print server, group. Mỗi loại đối tượng có những tính chất khác nhau ví dụ như đối tượng Người sử dụng có tính chất về nhóm mà người sử dụng đó thuộc, còn nhóm có các tính chất về người sử dụng mà nhóm đó chứa.

Việc thiết lập các dịch vụ như vậy cần được lập kế hoạch, thiết kế rất cẩn thận, liên quan đến tất cả các đơn vị phòng ban có liên quan. Loại mạng này có khuyết điểm là việc thiết kế, thiết lập mạng rất phức tạp, mất nhiều thời gian nên không thích hợp cho các mạng nhỏ.

### 3. Quản lý theo nhóm (Workgroup)

Các nhóm làm việc làm việc theo ý tưởng ngược lại với các dịch vụ thư mục. Nhóm làm việc dựa trên nguyên tắc mạng ngang hàng (peer-to-peer network), các người sử dụng chia sẻ tài nguyên trên máy tính của mình với những người khác, máy nào cũng vừa là chủ (server) vừa là khách (client). Người sử dụngï có thể cho phép các người sử dụng khác sử dụng tập tin, máy in, modem... của mình, và đến lượt mình có thể sử dụng các tài nguyên được các người sử dụng khác chia sẻ trên mạng. Mỗi cá nhân người sử dụng quản lý việc chia sẻ tài nguyên trên máy của mình bằng cách xác định cái gì sẽ được chia sẻ và ai sẽ có quyền truy cập. Mạng này hoạt động đơn giản: sau khi logon vào, người sử dụng có thể duyệt (browse) để tìm các tài nguyên có saün trên mạng.

Workgroup là nhóm logic các máy tính và các tài nguyên của chúng nối với nhau trên mạng mà các máy tính trong cùng một nhóm có thể cung cấp tài nguyên cho nhau. Mỗi máy tính trong một workgroup duy trì chính sách bảo mật và CSDL quản lý tài khoản bảo mật SAM (Security Account Manager) riêng ở mỗi máy. Do đó quản trị workgroup bao gồm việc quản trị CSDL tài khoản bảo mật trên mỗi máy tính một cách riêng lẻ, mang tính cục bộ, phân tán. Điều này rõ ràng rất phiền phức và có thể không thể làm được đối với một mạng rất lớn.

Nhưng workgroup cũng có điểm là đơn giản, tiện lợi và chia sẽ tài nguyên hiệu quả, do đó thích hợp với các mạng nhỏ, gồm các nhóm người sử dụng tương tự nhau.

Tuy nhiên Workgroup dựa trên cơ sở mạng ngang hàng (peer-to-peer), nên có hai trở ngại đối với các mạng lớn như sau:

- Đối với mạng lớn, có quá nhiều tài nguyên có saün trên mạng làm cho các người sử dụng khó xác định chúng để khai thác.

- Người sử dụng muốn chia sẻ tài nguyên thường sử dụng một cách dễ hơn để chia sẻ tài nguyên chỉ với một số hạn chế người sử dụng khác.

Điển hình cho loại mạng này là Windws for Workgroups, LANtastic, LAN Manager... Window 95, Windows NT Workstation.

### 4. Quản lý theo vùng (Domain)

Domain mượn ý tưởng từ thư mục và nhóm làm việc. Giống như một workgroup, domain có thể được quản trị bằng hỗn hợp các biện pháp quản lý tập trung và địa phương. Domain là một tập hợp các máy tính dùng chung một nguyên tắc bảo mật và CSDL tài khoản người dùng (người sử dụng account). Những tài khoản người dùng và nguyên tắc an toàn có thể được nhìn thấy khi thuộc vào một CSDL chung và được tập trung.

Giống như một thư mục, một domain tổ chức tài nguyên của một vài máy chủ vào một cơ cấu quản trị. Người sử dụng được cấp quyền logon vào domain chứ không phải vào từng máy chủ riêng lẻ. Ngoài ra, vì domain điều khiển tài nguyên của một số máy chủ, nên việc quản lý các tài khoản của người sử dụng được tập trung và do đó trở nên dễ dàng hơn là phải quản lý một mạng với nhiều máy chủ độc lập.

Các máy chủ trong một domain cung cấp dịch vụ cho các người sử dụng. Một người sử dụng khi logon vào domain thì có thể truy cập đến tất cả tài nguyên thuộc domain mà họ được cấp quyền truy cập. Họ có thể dò tìm (browse) các tài nguyên của domain giống như trong một workgroup, nhưng nó an toàn, bảo mật hơn.

Để xây dựng mạng dựa trên domain, ta phải có ít nhất một máy Windows NT Server trên mạng. Một máy tính Windows NT có thể thuộc vào một workgroup hoặc một domain, nhưng không thể đồng thời thuộc cả hai. Mô hình domain được thiết lập cho các mạng lớn với khả năng kết nối các mạng toàn xí nghiệp hay liên kết các kết nối mạng với các mạng khác và những công cụ cần thiết để điều hành.

Việc nhóm những người sử dụng mạng và tài nguyên trên mạng thành domain có lợi ích sau:

- Mã số của người sử dụng được quản lý tập trung ở một nơi trong một cơ sở dữ liệu của máy chủ, do vậy quản lý chặt chẽ hơn.

- Các nguồn tài nguyên cục bộ được nhóm vào trong một domain nên dễ khai thác hơn.

*Quản lý theo Workgroup và domain là hai mô hình mà Windows NT lựa chọn. Sự khác nhau căn bản giữa Workgroup và domain là trong một domain phải có ít nhất một máy chủ (máy chủ) và tài nguyên người sử dụng phải được quản lý bởi máy chủ đó.*

## II. Hệ thống quản lý trên Hệ điều hành mạng Windows NT Server

Windows NT cung cấp những chức năng tuân theo chuẩn C2 (chuẩn về an toàn quốc tế) trong đó Windows NT đảm bảo tránh được những người không được phép vào trong hệ thống hoặc thâm nhập vào các file và chương trình trên đĩa cứng. Người ta không thể thâm nhập vào được nếu không có mật khẩu đúng. và qua đó đã bảo vệ

được các file. Windows NT cung cấp công cụ để xây dựng các lớp quyền dành cho nhiều nhiệm vụ khác nhau nhằm xây dựng hệ thống an toàn một cách mềm dẻo.

Nhiều người sử dụng có thể có quyền vào một máy chủ Windows NT. Một tài khoản của người sử dụng trên máy bao gồm tên, mật khẩu và nhiều tính chất được cho bởi người quản trị mạng. Người sử dụng có thể che các thư mục hay file của mình từ những người khác và cài đặt các thông số của File manager, Programe Manager, Control Panel một cách phù hợp.

Khi người dùng thâm nhập vào hệ thống thì tự động khởi động mọi thông số đã được lưu trữ từ trước. Nếu người sử dụng có quyền cao hơn thì họ có thể chia sẻ hoặc ngừng các tài nguyên đang dùng chung trên mạng như máy in hay file hoặc họ có thể thay đổi quyền của những người dùng mạng khác khi thâm nhập vào mạng.

### 1. Mô hình Workgroup (nhóm) của mạng Windows NT

Mỗi người truy cập vào mạng Windows NT tổ chức theo mô hình Workgroup cần phải đăng ký:

- Tên vào mạng
- Mật khẩu vào mạng

Dựa vào tên và mật khẩu đã cho, Windows NT cung cấp cho người một số gọi là mã số của người sử dụng (user account). Mã số này được lưu dữ trong cơ sở dữ liệu là hệ thống quản trị tài nguyên (SAM - Security Account Manager database). Hệ thống quản trị tài nguyên dùng để đảm bảo an toàn về tài nguyên trên mạng. Người vào mạng muốn truy nhập vào tài nguyên phải qua sự kiểm duyệt của hệ thống quản trị tài nguyên. Trong mô hình Workgroup mỗi máy trạm có một nguồn tài nguyên tương ứng với một hệ thống quản trị tài nguyên bảo vệ nó.

**Chú ý:** Mỗi người khai thác mạng phải nhớ nhiều mã số, vì ứng với mỗi máy trạm có một hệ thống quản trị tài nguyên riêng của nó.

### 2. Mô hình vùng (Domain)

Domain là một khái niệm rất cơ bản trong Windows NT server, nó là hạt nhân để tổ chức các mạng có quy mô lớn.

Mỗi người tham gia trong Domain cần phải đăng ký thông tin sau:

- Tên Domain
- Tên người sử dụng
- Mật khẩu

Các thông tin này được lưu ở máy chủ dưới dạng một mã số, gọi là tài khoản người sử dụng (user account) và các mã số cũa người sử dụng trong một domain được tổ chức thành một cơ sở dữ liệu trên máy chủ. Khi người sử dụng muốn truy nhập vào một Domain người đó phải chọn tên Domain trong hộp thoại trên máy trạm. Máy trạm sẽ chuyển các thông tin về hệ thống quản trị tài nguyên (SAM - Security Account Manager database) của Domain để kiểm tra. Khi đó hệ thống quản trị tài nguyên trên máy chủ sẽ kiểm tra các thông tin này, nếu kết quả kiểm tra là đúng, người khai thác mới được quyền truy nhập vào tài nguyên của Domain.

Một máy Windows NT mà không tham gia vào một Domain có nhược điểm sau:

- Máy trạm chỉ có thể cung cấp các mã số được tạo ra trên nó. Nếu máy này bị hư hỏng thì những người khai thác mạng không thể truy nhập bằng mã số của họ. Nếu máy này nằm trong một Domain nào đó thì các mã số này còn được lưu trong SAM của một Domain trên máy Máy chủ.

- Qua máy trạm không tham gia vào Domain, người khai thác mạng không thể truy nhập vào tài nguyên của Domain, mặc dù mã số của của người này có trong SAM của Domain

Trong một Domain thường có các loại máy thực hiện những công việc sau:

- Primary domain Controller (PDC), bao giờ cũng phải có để quản trị hệ thống các người sử dụng và các tài khoản trong Domain (hệ thống này gọi là cơ sở dữ liệu SAM - Security Account Manager của Domain). SAM trên máy chủ được thiết kế như hệ thống kiểm soát Domain. Trong một Domain chỉ có duy nhất một PDC.

- Ngoài ra hệ thống còn có một hay nhiều máy làm Backup Domain Controller (BDC). Các BDC có thể dùng thay thế cho máy PDC trong trường hợp cần thiết, chẳng hạn máy PDC bị hư

Người quản trị Domain chỉ cần tạo tài khoản người sử dụng (user account) chỉ một lần trên máy Primary Domain Controller, thông tin được tự động copy đến các máy Backup Domain Controller.

### 3. Mô hình quan hệ giữa các Domain trong mạng Windows NT

Trong một mạng có thể có nhiều Domain nhưng một máy tính Windows NT là thành viên của chỉ một domain tại mỗi thời điểm. Tuy nhiên, có một vài trường hợp đôi khi chúng ta cần truy cập tài nguyên trong những domain khác, để là được điều này hệ điều hành Windows NT server cho phép giữa các Domain có thể tồn tại một quan hệ gọi là quan hệ tin cậy (trust relationship). Chúng ta có thể sử dụng quan hệ tin cậy giữa các Domain cho phép người dùng trên một Domain truy cập tài nguyên trong Domain khác.

Hai Domain A, B gọi là quan hệ tin cậy (trust relationship) mà trong đó Domain A tin cậy Domain B nếu giữa chúng có một mối liên kết sao cho người khai thác mạng của Domain B có thể truy nhập vào Domain A từ một máy trạm trong Domain B.

Từ góc độ của người quản trị mạng mục đích của việc thiết lập quan hệ tin cậy giữa các Domain là làm cho việc quản lý mạng trở lên đơn giản hơn bằng cách kết hợp các Domain vào một đơn vị quản lý. Trong quan hệ tin cậy các Domain được chia ra như sau:

- Domain được tin cậy (trusted domain)
- Domain tin cậy (trusting domain)

Một Domain là loại này hoặc loại kia *thông thường* phụ thuộc vào nó chứa mã số của người sử dụng (người sử dụng account) hay chỉ chứa tài nguyên (resource)

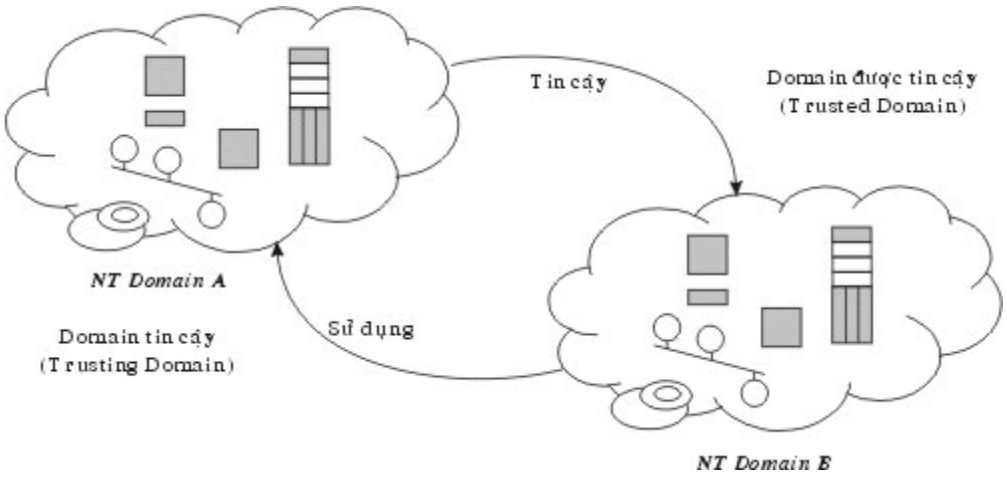
- Domain tin cậy (trusting domain) là Domain chứa tài nguyên.
- Domain được tin cậy (trusted domain) là Domain chứa mã số người sử dụng.

Khi người sử dụng truy nhập từ một máy trạm trong Domain tin cậy (trusting domain) vào Domain được tin cậy (trusted domain) thì quá trình kiểm soát diễn ra như sau:

- Người sử dụng phải cho mã số (mã số này ứng với tên, mật khẩu, tên domain cần truy nhập)
- Mã số được chuyển về máy chủ của Domain tin cậy.
- Máy chủ của Domain tin cậy chuyển mã số này sang Domain được tin cậy.
- Kết quả kiểm tra của máy chủ trong Domain được tin cậy diễn ra theo quá trình ngược lại.

**Ở đây chúng ta chú ý:**

- Việc liên kết giữa các Domain không có tính bắc cầu.
- Thông qua việc thiết lập mối quan hệ tin tưởng, chúng ta có thể sử dụng một tài khoản để truy xuất đến nhiều tài nguyên của nhiều Domain. Có thể quản trị nhiều Domain từ một vị trí tập trung.




*Hình 11.1: Mô hình tin cậy của các Domain trong mạng Windows NT*

### 4. Nhóm (group) trong Windows NT

Trong mạng Windows NT khái niệm nhóm (group) là một trong những khái niệm quan trọng đối với công việc quản lý, điều hành mạng Windows NT. Nhóm làm cho việc khai thác tài nguyên được dễ dàng thuận lợi và đơn giản hóa việc quản trị. Mỗi nhóm được đăng ký bởi một tài khoản (group account) và có các thành viên của nó. Các quyền đã được gán cho nhóm sẽ tự động gán cho các người sử dụng là thành viên của nhóm. Các tiện lợi của nhóm như sau:

- Quyền có thể được gán cho, hoặc hủy đi trên mọi thành viên của nhóm.
- Khi một người sử dụng bị loại ra khỏi nhóm, thì tự động bị mất các quyền đã được cấp khi còn trong nhóm.

Trong mạng Windows NT người ta phân biệt phân biệt hai loại nhóm là nhóm toàn cục (global group) và nhóm cục bộ (local group).

### 5. Nhóm toàn cục (global group)

Nhóm toàn cục còn được gọi là nhóm vùng (domain group). Thành viên của nhóm là các người dùng cấp vùng (domain user). Họ ngược lại với người dùng cục bộ (local user) là người có phạm vi giới hạn trong máy tính mà họ được xác định. Thành viên của nhóm toàn cục được phép chuyển ra ngoài (export) một Domain khác. Phạm vi của nhóm toàn cục là toàn bộ vùng trên đó user dược xác định, và thấy được từ bất kỳ máy tính NT nào trong vùng đó. Quyền có thể được gán cho nhóm toàn cục cho các tài nguyên trên một máy NT Server hay NT Workstation trong vùng.

Các tài khoản nhóm toàn cục được lưu ở PDC (Primary DomainController) của Domain, và được sao lưu đến các BDC (Backup Domain Controller) trong Domain đó.

Nhóm toàn cục có những đặc trưng sau:

- Thành viên của nhóm phải là các người sử dụng của domain (domain user account).
- Nhóm toàn cục có thể được gán quyền cho tài nguyên bất kỳ trong vùng mà chúng được xác định.
- Nhóm toàn cục có thể được gán quyền đến các tài nguyên trong vùng khác với vùng chúng được xác định khi quan hệ tin cậy (trust relationship) giữa các vùng có hiệu lực.
- Các thành viên của nhóm toàn cục có thể sử dụng nguồn tài nguyên trong vùng bất kỳ mà nhóm toàn cục có quyền.
- Nhóm toàn cục chỉ chứa mã số của người sử dụng trong Domain của nó. Nó không thể chứa các nhóm cục bộ và nhóm toàn cục khác.

### 6. Nhóm cục bộ (local group)

Nhóm cục bộ, trái lại, được gán quyền cho nguồn tài nguyên trên máy NT mà nó được xác định. Nếu máy NT là một phần của vùng, thì để tiện cho việc gán quyền, một nhóm cục bộ có thể chứa các tài khoản người dùng cấp vùng (domain user account) và các nhóm toàn cục trong Domain đó, nơi máy tính NT là thành viên, hoặc những người dùng từ Domain được tin cậy. Các người dùng cấp vùng (domain user) có thể được gán quyền truy cập đến tài nguyên bất kỳ trong Domain đó.

Nếu Windows NT computer không nối với mạng thì các thành viên trong local group có thể được gán quyền để truy xuất đến tài nguyên trên máy tính mà trong đó các thành viên được tạo ra còn nếu Windows NT computer nối vào mạng thì để tiện lợi cho việc phân quyền thì người quản trị mạng có thể đưa global group và domain user vào trong local group .

Có hai loại nhóm cục bộ: ***nhóm cục bộ trạm làm việc (workstation local group)*** và ***nhóm cục bộ vùng (domain local group).*** Một mạng làm việc theo cơ chế vùng bao gồm cả Windows NT Server và Windows NT Workstation việc hiểu rõ sự khác nhau giữa hai loại nhóm cục bộ là rất quan trọng.

#### *a. Nhóm cục bộ trạm làm việc (Workstation local group):*

Nhóm cục bộ trạm làm việc hiện diện trên Windows NT Workstation trên đó chúng được tạo ra. Chúng được chứa trong dữ liệu SAM lưu trữ trên Windows NT Workstation. Một người dùng cục bộ được tạo ra bằng công cụ *User Manager* của Windows NT Workstation (khác với công cụ *User Manager for Domains* trên Windows NT Server) có thể có quan hệ thành viên chỉ trong nhóm cục bộ của trạm làm việc đó.

Một nhóm cục bộ trong một trạm làm việc chỉ có thể được dùng trên máy tính trên đó nhóm được tạo ra, và không thể làm việc rên bất kỳ máy Windows NT nào khác.

Nhóm cục bộ trạm làm việc có thể chứa:

- Các tài khoản người dùng cục bộ từ trạm làm việc trên đó nó được xác định.
- Các tái khoản người dùng cấp vùng (domain user account) và các nhóm toàn cục từ vùng trong đó họ được xác định.
- Các tái khoản người dùng cấp vùng (domain user account) và các nhóm toàn cục từ các vùngï được ủy quyền.

### *b. Nhóm cục bộ vùng (Domain local group):*

**N**hóm cục bộ vùng hoạt động trên Windows NT Server ở mức vùng, và được tạo ra bằng *User Manager for Domains* (trên Windows NT Server). Các nhóm cục bộ vùng chỉ có thể hiện hữu trên máy Windows NT Server tạo ra nó. Do đó, các nhóm cục bộ vùng có thể dùng để truy cập nguồn tài nguyên trên máy tính Windows NT Server trong vùng đó, mà không dùng để truy cập nguồn tài nguyên trên máy tính Windows NT Workstation trong vùng này. Nhóm cục bộ vùng không thể được gán quyền trên bộ điều khiển không có cấp vùng, thậm chí cả các máy chủ.

## III. Các mô hình Domain trong mạng Windows NT

Windows NT máy chủ cung cấp 4 kiểu tổ chức domain gọi tắt là các mô hình domain (domain models). Dưới đây là 4 mô hình tổ chức của nó:

- Mô hình domain đơn (single domain)
- Mô hình domain chính (master domain)
- Mô hình multiple master domain
- Mô hình complete truts

### 1. Mô hình Domain đơn (single domain)

Mô hình domain đơn là mô hình trong mạng chỉ có một domain. Mô hình này thích hợp cho mạng ít người khai thác, cần quản lý tập trung. Mô hình đơn nói chung tương tự như mô hình workgroup, trong mô hình này người sử dụng có thể xem xét, khai thác tài nguyên theo cả mô hình workgroup và mô hình domain.

Loại mô hình này không có các quan hệ ủy quyền vì chỉ có một domain duy nhất, domain này cũng chứa CSDL SAM cho toàn bộ mạng và việc quản trị mạng có thể thực hiện từ một vị trí trung tâm.

Các tài khoản người dùng trong vùng (domain user account) và tài khoản nhóm trong vùng (domain group acconunt) có thể được xây dựng và có các quyền truy cập tài nguyên được gán trên các nhóm và người dùng riêng rẽ và có một phạm vi bao gồm tất cả các máy vi tính trong vùng.

Trong mô hình Domain đơn vấn đề an toàn dữ liệu, quản lý hệ thống được xem xét một cách tốt hơn so với Workgroup.

### 2. Mô hình Domain chính (Master domain)

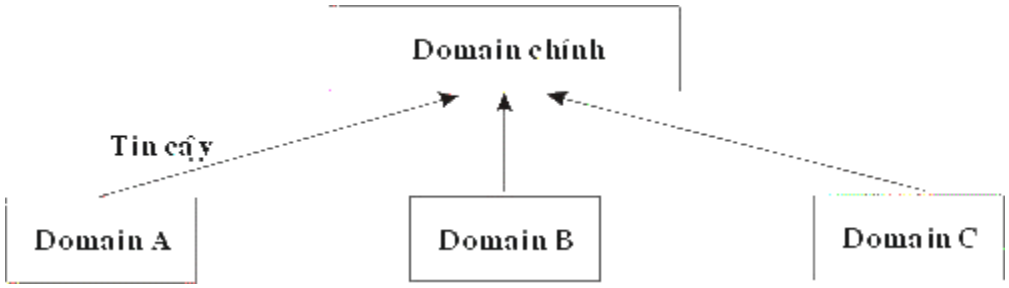
Mô hình Domain chính có thể được sử dụng cho các cơ quan khi họ muốn tổ chức mạng thành nhiều Domain tài nguyên (Resource domain) nhưng vẫn có những tiện lợi trong việc quản lý tập trung. Bằng cách phân chia tài nguyên mạng vào nhiều Domain, chúng ta sẽ tiện tổ chức và quản lý một lượng tài nguyên lớn. Một Domain chủ (master domain) được sử dụng để hổ trợ việc quản trị tập trung mà trong đó tất cả mã số của người sử dụng và mã số các nhóm toàn cục (global group) trên mạng được lưu giữ.

Đặc điểm của mô hình domain chính :

- Mô hình Master Domain là mô hình có nhiều Domain, trong đó có 1 Domain là Domain chính (premery domain). Mô hình này thích hợp cho mạng có số người dùng không quá lớn, nhưng cần phải phân chia thành các đơn vị nhỏ hơn nhưng việc quản lý được tiến hành tập trung.

- Trong mô hình này tất cả mã số của người khai thác mạng và mã số của các nhóm toàn cục (global group) đều chứa trên server trên Domain chính.

- Trong mô hình này tất cả các khác Domain đều tin cậy với Domain chính.




*Hình 11.2: Mô hình Domain chính*

Trong mô hình này mã số của người sử dụng quản lý tập trung và các nhóm toàn cục chỉ cần xác định một lần trong Domain chính. Tài nguyên được nhóm logic thành các đơn vị nhỏ hơn để có thể quản lý bởi từng Domain.

Mô hình Domain chính là mô hình quản lý tập trung vì vậy chiến lược phát triển mạng cần dựa vào các nhóm cục bộ và các nhóm toàn cục.

Mô hình này không những quản lý tập trung các mã số của người sử dụng mà còn cung cấp các dịch vụ như cài đặt phần mềm, sao chép backup cho tất cả các máy chủ trên mạng.

Tuy nhiên mô hình này có nhược điểm có thể gây ùn tắc nếu có quá nhiều nhóm và nhiều người dùng và các nhóm cục bộ cần phải xác định trong mỗi Domain mà chúng được sử dụng.

### 3. Mô hình nhiều Domain chính (muliple master domain)

Mô hình **nhiều Domain chính** (muliple master domain) có thể được sử dụng cho các tổ chức có nhiều khu vực và mỗi khu vực có nhiều bộ phận. Trong nhiều mạng kiểu như vậy, bộ phận điều hành riêng biệt cho mỗi khu vực muốn quản lý tập trung các tài nguyên mạng trong khu vực. Chúng ta xây dựng một Domain chủ (master domain) cho mỗi khu vực và chia các tài nguyên trong mỗi khu vực thành nhiều Domain tài nguyên (resoure domain) riêng biệt.

Trên mô hình này tồn tại các quan hệ sau:

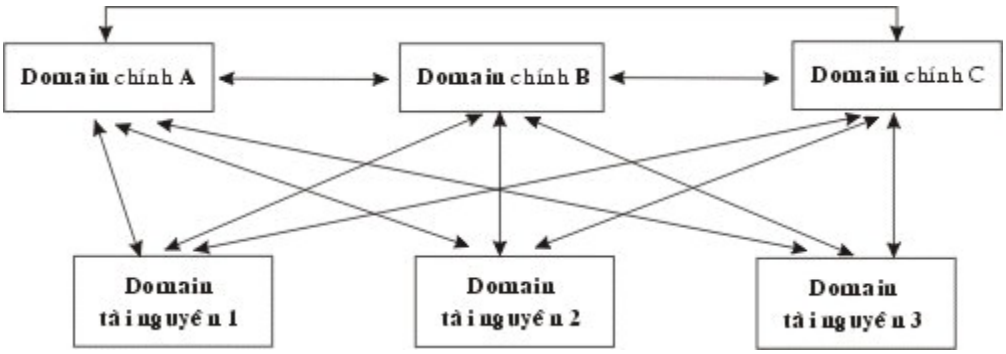
- Mỗi Domain chính quan hệ tin cậy hai chiều với các domain chính khác. Điều này cho phép mỗi Domain chính có thể quản lý các domain chính khác.

- Các Domain không phải là chính không có mã số của người sử dụng mà chỉ cung cấp tài nguyên trên mạng.

- Các Domain không phải là chính tin cậy đối với tất cả các Domain chính. Nhờ điều này mỗi mã số của người sử dụng sẽ được sử dụng trên tất cả các Domain chính và có được quyền truy nhập vào tài nguyên trong các tài nguyên trên các Domain khác của mạng.

Bằng cách phân chia tài nguyên mạng thành nhiều Domain, chúng ta có nhiều thuận lợi trong việc tổ chức quản lý một số lượng lớn các tài nguyên trong các đơn vị phù hợp.

Mô hình nhiều Domain chính có ưu điểm đối với mạng nhiều người dùng trong đó các tài nguyên được nhóm một cách logic theo công việc. Tuy nhiên các nhóm cục bộ và toàn cục phải xác định nhiều lần và mã số của người sử dụng phải chứa ở nhiều Domain chính .

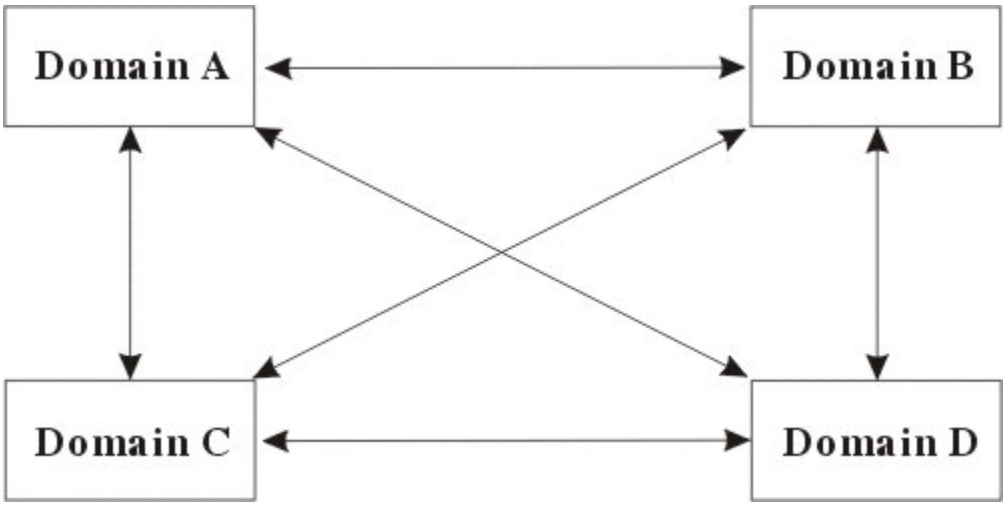



*Hình 11.3: Mô hình nhiều Domain chính*

### 4. Mô hình tin cậy hoàn toàn (complete trust)

Mô hình tin cậy hoàn toàn là mô hình mà trong đó mỗi Domain là quan hệ tin cậy 2 chiều với các Domain khác. Với mô hình này, người sử dụng có thể truy nhập vào bất kỳ Domain nào trên mạng từ một máy trạm nào đó.

Mô hình này có thể áp dụng với qui mô mạng tùy ý và phù hợp cho các cơ quan không có nhóm quản trị tập trung, nó cho phép không hạn chế số người khai thác mạng và số nhóm. Mỗi bộ phận trong đơn vị có thể kiểm soát được mã số của người sử dụng cũng như tài nguyên của bộ phận mình trong đó tài nguyên và mã số người sử dụng được nhóm thành một Domain.




*Hình 11.4: Mô hình nhiều Mô hình tin cậy hoàn toàn*

## IV. Các mặt hạn chế của những mô hình Domain

Mô hình vùng có một số kẽ hở về cấu trúc. Những hạn chế về domain được thảo luận ở đây nhằm mục đích giúp bạn thiết kế mạng chính xác và hoàn hảo.

- Domain NT đơn điệu theo nghĩa là không có cách nào diễn tả quan hệ phân cấp hoặc nhóm tài nguyên trong một vùng đơn. Người dùng có thể sử dụng những quyền được ủy thác thể hiện các quan hệ giữa những vùng, nhưng đây là quan hệ sử dụng và không thích hợp cho việc tổ chức mạng dựa trên phạm vi địa lý, tài nguyên sở hữu, logic hoặc nền tảng sơ đồ tổ chức.

- Mô hình vùng Domain chính duy nhất theo Microsoft thích hợp cho các mạng ít hơn 40.000 người dùng và nhóm. Khi số người dùng và nhóm tăng lên, số quan hệ ủy quyền và chi phí quản lý quan hệ cũng tăng. Nói cách khác chi phí quản lý mạng có thể tăng bất thình lình khi kích thước mạng tăng.

- Người dùng phải cẩn trọng về kẻ hở của quan hệ ủy quyền - đặc biệt quan hệ ủy quyền hai chiều. Nếu không cẩn thận trong việc gán các quan hệ ủy quyền và không có kế hoạch đúng đắn, người sử dụng có thể kết thúc bằng một mô hình ủy quyền trọn vẹn, với tất cả những hạn chế của mô hình đi kèm.

- Ngoài ra có một nguy cơ thực sự sẽ xảy ra là người cài đặt mạng có thể cài đặt một mạng hoạt động tốt trong thời gian ngắn còn khi mạng hoạt động dài hạn này sẽ ù nảy sinh vấn đề về mặt chính sách là ai ủy quyền cho ai.

**Chương 12**

# Cài đặt, quản trị, sử dụng mạng Windows NT

## I. Cài đặt hệ điều hành mạng Windows NT server

Trước khi cài đặt mạng Windows NT thì cũng giống như cài các hệ điều hành khác chúng ta phải cắm card mạng vào máy, thiết lập mạng và đảm bảo nó được hoạt động tốt. Khi cài chúng ta có thể sử dụng phần mềm trên đĩa CD ROM (nếu máy của chúng ta là PC thì chúng ta sử dụng thư mục I386) hoặc chúng ta chép thư mục I386 lên đĩa cứng trước khi cài đặt. Để cài đặt Windows NT ta và trong thư mục I386 và chạy lệnh "WINNT"

Chú ý trong trường hợp này chương trình sẽ yêu cầu chuẩn bị 3 đĩa mềm loại 1.44Mb để cài các chương trình khởi động cần thiết và trong quá trình cài đặt các đĩa mềm trên sẽ được sử dụng. Nếu ta không muốn thì thực hiện lệnh "WINNT /B" và phải chỉ đường dẫn của chương trình nguồn như d:\I386.

**Yêu cầu về phần cứng cho việc cài đặt windows NT**

| Thiết bị phần cứng | Yêu cầu |
|---|---|
| Processor | Intel 486, Pentium, Pentium Pro, những hệ thống chạy trên RISC (Ex: MIPS R4x00, DEC?s Alpha AXP). Windows NT hỗ trợ lên đến 4 CPU ở Mode Symmetriccal Multi-Processing |
| Display device | VGA hay những thiêt bị có độ phân giải cao hơn |
| Hard disk | Tối thiểu phải có 110 MB Hard Disk còn trống trong suốt quá trình cài đặt |
| Floppy disk | 31/2 inch hay 51/4 inch |
| CD-ROM | CD-ROM drive hay đĩa CD-ROM mà ta có thể truy xuất được thông qua đường mạng |
| Network adapter | Một hay nhiều card mạng, card mạng không có cũng được nhưng chức năng mạng sẽ không có |
| Memory | NT khuyến cáo ít nhất phải có 16 MB Ram cho cả hai hệ thống chạy trên Intel và RISC |

**Chương 13 :**

# Quản lý và khai thác File, thư mục trong mạng Windows NT

Trong số các tài nguyên của mạng chia sẻ cho người sử dụng thông tin lưu trữ trên đĩa cứng của các máy chủ là tài nguyên quan trọng nhất. Không phải ngẫu nhiên mà cái tên "File server" trở nên rất quen thuộc với những người dùng mạng giống như "Network server". Tuy nhiên để làm sao có thể sử dụng, quản lý các tài nguyên đó một cách tốt nhất Windows NT cung cấp cho chúng ta một cơ chế quản lý và phương thức khai thác. Thông thường chúng ta phải khai báo các tài nguyên trước khi chúng được người sử dụng khai thác. Ngoài ra người sử dụng cũng được cung cấp quyền sử dụng một cách phù hợp.

## I. Cơ chế an toàn của File và thư mục trong Windows NT

***Quá trình truy cập tập tin (File hoặc thư mục)* trong Windows NT:** Khi một người sử dụng muốn truy cập một tập tin thì tất cả các thông tin về phương thức phục hồi giao dịch và phục hồi giao dịch khi bị lỗi sẽ được đăng ký bởi Log File Server. Nếu giao dịch thành công, tập tin đó sẽ truy xuất được, ngược lại giao dịch sẽđược phục hồi. Nếu có lỗi trong quá trình giao dịch, tiến trình giao dịch sẽ kết thúc.

Việc truy xuất tập tin (File hoặc thư mục) được quản lý thông qua các quyền truy cập (right), quyền đó sẽ quyết định ai có thể truy xuất và truy xuất đến tập tin đó với mức độ giới hạn nào. Những Quyền đó là Read, Execute, Delete, Write, Set Permission, Take Ownership.

**Trong đó:**

- **Read (R):** Được đọc dữ liệu, các thuộc tính, chủ quyền của tập tin.
- **Execute (X):** Được chạy tập tin.
- **Write (W):** Được phép ghi hay thay đổi thuộc tính.
- **Delete (D):** Được phép xóa tập tin.
- **Set Permission (P):** Được phép thay đổi quyền hạn của tập tin.
- **Take Ownership (O):** Được đặt quyền chủ sở hữu của tập tin.

**Bảng tóm tắt các mức cho phép**

| Permission | R | X | W | D | P | O |
|---|---|---|---|---|---|---|
| No Access | | | | | | |
| Read | X | X | | | | |
| Change | X | X | X | X | | |
| Full Control | X | X | X | X | X | X |
| Special Access | ? | ? | ? | ? | ? | ? |

Để đảm bảo an toàn khi truy xuất đến tập tin (File và thư mục)ä, chúng ta có thể gán nhiều mức truy cập (permission) khác nhau đến các tập tin thông qua các quyền được gán trên tập tin. Có 5 mức truy cập được định nghĩa trước liên quan đến việc truy xuất tập tin (File và thư mục) là: No Access, Read, Change, FullControl, Special Access. Special Access được tạo bởi người quản trị cho bất cứ việc chọn đặt sự kết hợp của R, X, W, D, P, O. Những người có quyền hạn Full Control, P, O thì họ có quyền thay đổi việc gán các quyền hạn cho Special Access.

- Khi một người quản trị mạng định dạng một partition trong Windows NT, hệ thống sẽ mặc định có cấp cho quyền Full Control tới partition đó cho nhóm Everyone. Điều này có nghĩa không hạn chế truy xuất của tất cả người dùng.

- Tùy thuộc trên yêu cầu bảo mật cho các tập người quản lý sẽ cân nhắc việc xóa bỏ nhóm Everyone trong danh sách các quyền hạn sau khi định dạng hay hạn chế nhóm Everyone với quyền Read. Nếu sự hạn chế này là cần thiết, người quản trị nên cấp quyền hạn Full Control cho nhóm Administrators tới partition gốc.

Ở đây quyền truy cập được gán cho người sử dụng và nhóm người sử dụng do vậy quyền truy cập của một người sử dụng được tính bởi quyền hạn người đó và các nhóm mà người đó là thành viên. Khi người dùng đó truy xuất tài nguyên, các quyền hạn của người dùng được tính theo lối sau:

- Những quyền hạn của ngươì dùng và các nhóm trùng nhau.

- Nếu một trong những quyền là No Access thì quyền hạn chung là No Access.

- Nếu những quyền hạn đã yêu cầu được liệt kê không rõ ràng trong danh sách các quyền hạn, yêu cầu truy xuất này là không chấp nhận.

Một người sử dụng thuộc hai nhóm, nếu một nhóm quyền hạn của người dùng là No Access, nó luôn được liệt kê đầu tiên trong danh sách Access Control List.

**Quyền sở hữu của các tập tin:** Người tạo ra tập tin đó có thể cho các nhóm khác hay người dùng khác khả năng làm quyền sở hữu. Administrator luôn có khả năng làm quyền sở hữu của các tập tin.

Nếu thành viên của nhóm Administrator có quyền sở hữu một tập tin thì nhóm những Aministrator trở thành chủ nhân. Nếu người dùng không phải là thành viên của nhóm Administrator có quyền sở hữu thì chỉ người dùng đó là chủ nhân.

Những chủ nhân của tập tin có quyền điều khiển của tập tin đó và có thể luôn luôn thay đổi các quyền hạn. Trong File Manager, dưới Security Menu, sau khi xuất hiện hộp thoại Owner, chúng ta lựa chọn tập tin, chủ nhân hiện thời và nhấn nút Take Ownership, cho phép lập quyền sở hữu nếu được cấp quyền đó.

**Để có quyền sở hữu một tập tin chúng ta cần một trong những điều kiện sau:**

- Có quyền Full Control.
- Có những quyền Special Access bao gồm Take Ownership.
- Là thành viên của nhóm Administrator.

**II. Các thuộc tính của File và thư mục**

- **Archive:** Thuộc tính này được gán bởi hệ điều hành chỉ định rằng một File đã được sửa đổi từ khi nó được Backup. Các phần mềm Backup thường xóa thuộc tính lưu trữ đó. Thuộc tính lưu trữ này có thể chỉ định các File đã được thay đổi khi thực thi việc Backup.
- **Compress:** Chỉ định rằng các File hay các thư mục đã được nén hay nên được nén. Thông số này chỉ được sử dụng trên các partition loại NTFS.
- **Hidden:** Các File và các thư mục có thuộc tính này thường không xuất hiện trong các danh sách thư mục.
- **Read Only:** Các File và các thư mục có thuộc tính này sẽ không thể bị xóa hay sửa đổi.
- **System:** Các File thường được cho thuộc tính này bởi hệ điều hành hay bởi chương trình OS setup. Thuộc tính này ít khi được sửa đổi bởi người quản trị mạng hay bởi các User.
- Ngoài ra các File hệ thống và các thư mục còn có cả hai thuộc tính chỉ đọc và ẩn.

**Lưu ý:** Việc gán thuộc tính nén cho các File hay thư mục mà ta muốn Windows NT nén sẽ xảy ra trong chế độ ngầm (background). Việc nén này làm giảm vùng không

gian đĩa mà File chiếm chỗ. Có một vài thao tác chịu việc xử lý chậm vì các File nén phải được giải nén trước khi sử dụng. Tuy nhiên việc nén File thường xảy ra thường xuyên như là các File dữ liệu quá lớn mà có nhiều người dùng chia sẻ.

### III. Chia sẻ Thư mục trên mạng

Không có một người sử dụng nào có thể truy xuất các File hay thư mục trên mạng bằng cách đăng nhập vào mạng khi không có một thư mục nào được chia se.

Việc chia sẻ này sẽ làm việc với bảng FAT và NTFS file system. Để nâng cao khả năng an toàn cho việc chia sẻ, chúng ta cần phải gán các mức truy cập cho File và Thư mục.

Khi chúng ta chia sẻ một thư mục, thì chúng ta sẽ chia sẻ tất cả các File và các Thư mục con. Nếu cần thiết phải hạn chế việc truy xuất tới một phần của cây thư mục, chúng ta phải sử dụng việc cấp các quyền cho một user hay một nhóm đối với các Thư mục và các File đó.

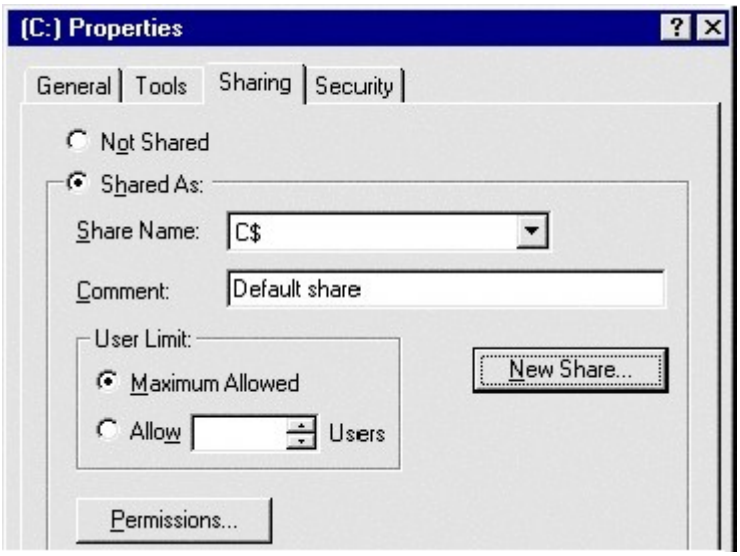
Để chia sẻ một Thư mục, ta phải Login như một thành viên của nhóm quản trị mạng hay nhóm điều hành server.

Tất cả các thủ tục chia sẻ thư mục được thực thi trong Windows NT Explorer.

**Để chia sẻ một thư mục ta phải thực hiện các bước sau:**

- **Right-click** lên Thư mục đó trong Windows NT Explorer. Hiện ra menu


- Click **Properties** trong Menu. Hiện ra hộp đối thoại sau:

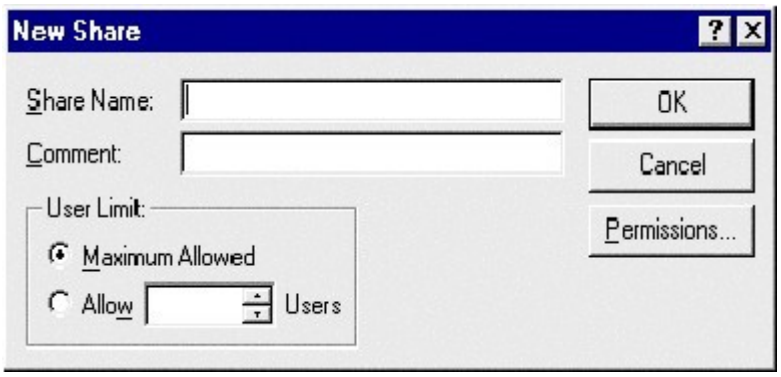



- Chọn **Sharing tab** hiện ra hộp đối thoại sau:
- Chọn **Shared As** để kích hoạt việc chia sẻ.
- Đưa một tên cần chia sẻ vào hộp **Share name**. Mặc nhiên tên Thư mục được chọn sẽ hiện ra. Đưa dòng ghi chú liên quan đến việc chia sẻ thư mục đó vào hộp **Comment**
- Thiết lập giới hạn số lượng các user bằng cách gỏ một con số vào hộp **Allow**
- Nếu muốn hạn chế việc truy xuất thì click **Permissions button.**
- **Click OK.**

Sau khi một thư mục được chia sẻ Icon cho thư mục đó có 1 bàn tay chỉ định rằng thư mục đó đã được chia sẻ.

Nếu chúng ta muốn thêm một chia sẻ mới với cùng một thư mục đã được chia sẻ (có thể với hai chia sẻ có hai quyền truy cập khác nhau), ta thực hiện các bước sau:

- **Right-click** vào thư mục đã được chia sẻ trong Windows NT Explorer.
- Click **Properties** trong **Menu** rút gọn, hiện ra hộp đối thoại **Properties**
- Click **Sharing tab.**
- Click button **New Share** để tạo một sự chia sẻ mới, hiện ra hộp đối thoại sau

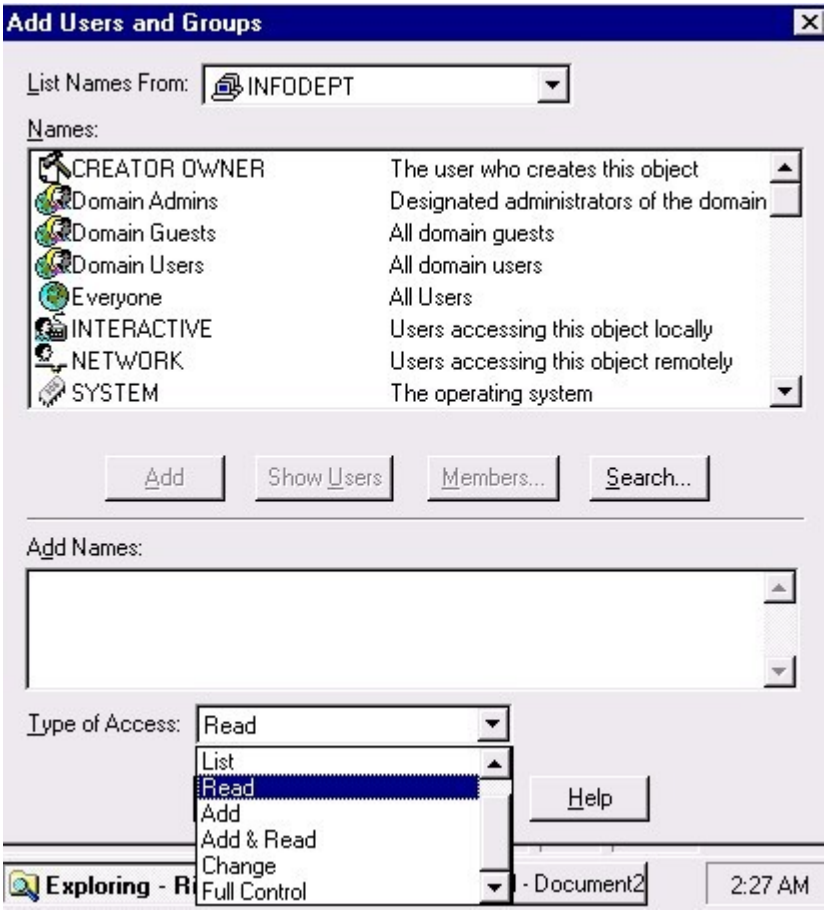



- Mỗi lần tạo một sự chia sẻ chúng ta phải đưa một tên mới cũng như những lời chú thích việc chia sẻ đó sẽ cho ai sử dụng.

## IV. Thiết lập quyền truy cập cho một người sử dụng hay một nhóm

Để thiết lập các quyền truy cập đối với một thư mục đã được chia sẻ cho một người sử dụng hay một nhóm ta thực hiện:

- **Right-click** lên thư mục đó trong Windows NT Explorer.
- Click **Properties** trong menu rút gọn**.**
- Chọn **Sharing** tab để hiện các tính chất của thư mục đó
- Click button **Permissions** trong **sharing tab** . Hiện ra Cửa sổ ***The Access Through Share Permissions.***
- Chọn button **Add**, hiện ra cửa sổ ***Add User and group.***




- Chọn một tên trong hộp ***Names*** và click button **Add.** Kết quả là tên đó được đưa vào hộp ***Add Names.***

- Chọn quyền truy xuất trong hộp ***Type of Access*** cho các tên đã chọn .

- Click button **OK.**

Khi chúng ta tạo một sự chia sẻ mới, quyền truy cập mặc nhiên cho nhóm **Everyone** là đầy đủ (**Full Control**). Giả sử rằng chúng ta sẽ gán giá trị mặc nhiên này cho quyền truy cập của thư mục và File. Khi cần thiết sẽ hạn chế việc truy xuất tới thư mục đó.

**Ở đây có một vài chú ý:**

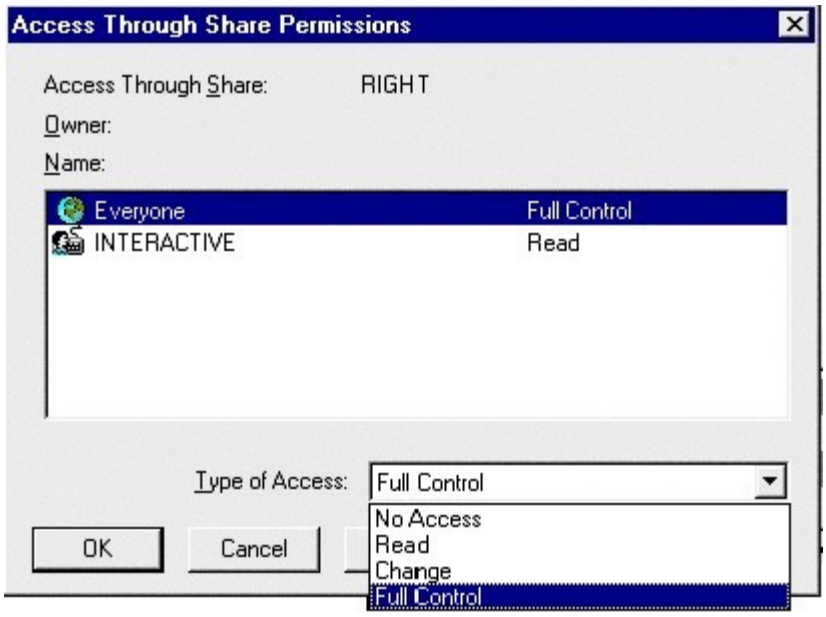
- Các người sử dụng thường chỉ cóù quyền đọc trong các thư mục chứa các chương trình ứng dụng vì họ không cần phải sửa đổi các File.

- Trong một vài trường hợp, các chương trình ứng dụng đòi hỏi các user chia sẻ một thư mục cho các File tạm thời. Nếu thư mục đó nằm trong cùng thư mục chứa trình ứng dụng, chúng ta có thể cho phép user tạo hay xóa các File trong thư mục đó bằng việc gán quyền **Change**.

- Thông thường các người sử dụng cần quyền **Change** trong bất kỳ thư mục nào chứa các Files dữ liệu và chỉ trong các thư mục cá nhân của ho là có đầy đủ các quyền truy cậpï.

**Để sửa đổi các quyền truy cập đối với một thư mục đã được chia sẻ ta thực hiện:**

- **Right-click** lên thư mục được chia sẻ trong Windows NT Explorer.
- Click **Properties**
- Click **Sharing** tab.
- Click button **Permissions** hiện ra cửa sổ ***Access Through Share Permissions*** sau:




- Chọn 1 tên trong hộp ***Name***
- Chọn một quyền khác trong hộp ***Type of Access*** mà ta muốn gán.
- Click **OK**.

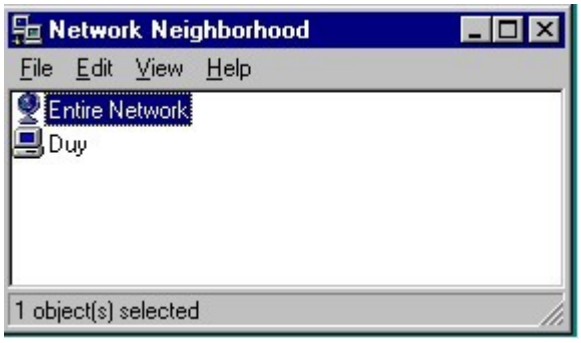
Thông qua việc chia sẻ một thư mục cho một user hay một nhóm cũng góp phần vào việc bảo đảm an toàn cho một thư mục không cho user khác hay nhóm khác truy xuất thư mục đó.

**V. Sử dụng các thư mục mạng**

Muốn sử dụng các thư mục mạng thì trước hết thư mục đó được cho phép chia sẻ, chúng ta phải liên kết thư mục mạng đó với tên một chữ cái tương ứng như một tên đĩa mạng (E,F ,G ,H I,...). Sau khi thư mục được chia sẻ đã kết nối với ký tự ổ đĩa mạng người dùng có thể truy cập thư mục được chia sẻ, các thư mục và file con của nó như là nó đang ở trên máy tính của mình .

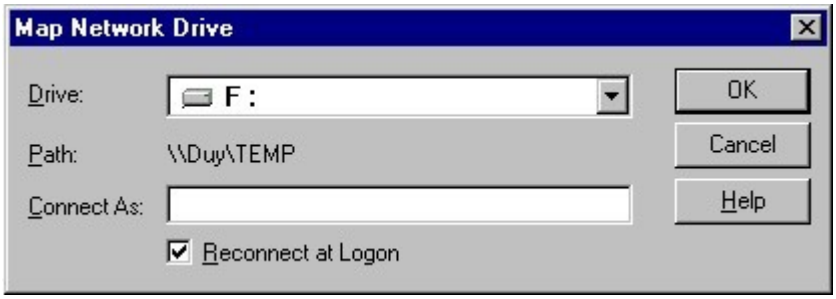
**Có thể dùng Network Neighborhood để thực hiện công việc trên như sau :**

- Click đúp trên **Network Neighborhood** để mở trình duyệt mạng.




- Duyệt qua **Network Neighborhood** để tìm nơi muốn liên kết.

- Click phải vào thư mục đã được chia sẻ mà chúng ta muốn truy cập và chọn **Map Network Drive** trong thực đơn **Options** ta thấy hộp **Map Network Drive** hiện ra




- Trong trường **Drive** của hộp thoại **Map Network Drive**, chọn ổ đĩa mạng chúng muốn liên kết với thư mục chia sẻ.

- Nếu thấy cần, chọn Path và gõ vào tên theo tổng quát UNC (Universal Naming Convention - xem cấu trúc ở phần dưới) để sửa lại đường dẫn tới tài nguyên được chia sẻ. (Việc này chỉ thực hiện khi sử dụng Network Neighborhood.)

- Nếu chúng ta không được quyền để truy cập vào tài nguyên chia sẻ trên nhưng trong cương vị người dùng khác thì chúng ta được quyền truy cập, trong trường hợp đó hãy gõ tên người dùng đó vào trường **Connect As**.

- Kích hoạt hộp kiểm tra **Reconnect at Logon** nếu muốn liên kết lâu dài, đó là loại kết nối được phục hồi mỗi lần chú ta đăng nhập vào mạng.

- Chọn **OK** để lưu các thông tin trên.

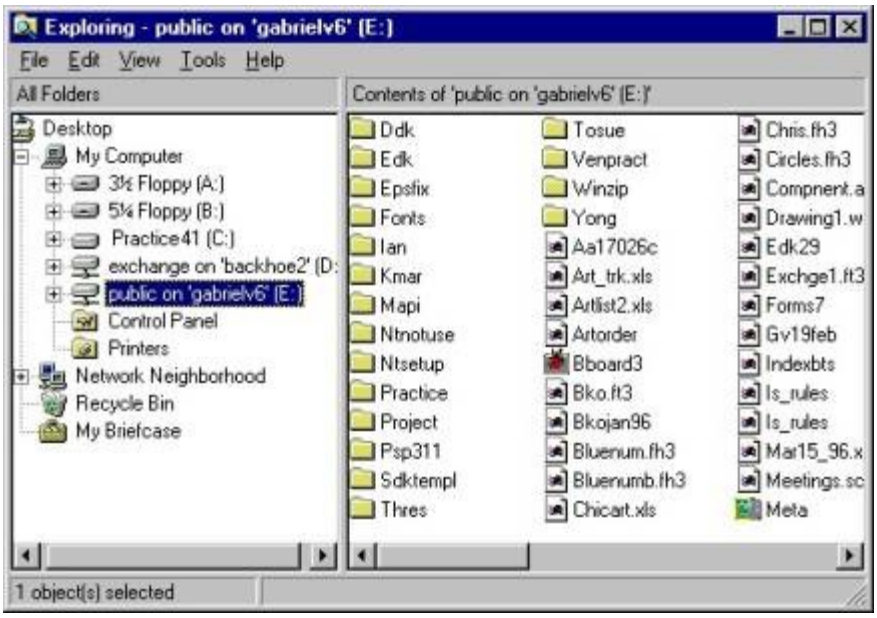
Ngoài ra ta có thể dùng lệnh **NET USE** để thực hiện các công việc trên.

Lệnh NET USE dùng Universal Naming Convention (UNC) để truy cập các tài nguyên dùng chung. Tên UNC bắt đầu bằng một dấu phân cách đặt biệt \\, dấu này chỉ sự bắt đầu của tên UNC (tên UNC có dạng "\\computer_name\share_name[\sub_directory]". NET USE đượcc dùng đểû truy cập một nguồn tài nguyên dùng chung. Lệnh NET USE dùng bộ hướng dẫn mạng (Network Redirector) trên máy tính NT để thiết lập sự nối kết dùng nguồn tài nguyên chung.

Chúng ta có thể xem ai dùng các file dùng chung khi ta đang xem trạng thái của một file dùng chung, File Manager sẽ cung cấp cho ta các thông tin bằng dùng chọn Properties trong thực đơn File

| Đề mục | Nội dung |
|---|---|
| Total Opens | Tổng số các user đang làm việc với file đó |
| Total Locks | Tổng số các khóa trên file |
| Open By | Tên của người dùng đã mở file |
| For | Loại truy xuất mà người dùng đã mở file |
| Locks | Một số khóa mà người dùng đặt trên file |
| File ID | Con số nhận diện của file |

Khi chúng ta dùng Windows Explorer để xem các tài nguyên chúng ta có thì các ổ đĩa mạng xuất hiện và cho chúng ta khai thác.


Exploring - public on 'gabrielv6' (E:)
File Edit View Tools Help
All Folders
Contents of 'public on 'gabrielv6' (E:)'
Desktop
My Computer
3½ Floppy (A:)
5¼ Floppy (B:)
Practice41 (C:)
exchange on 'backhoe2' (D:
public on 'gabrielv6' (E:)
Control Panel
Printers
Network Neighborhood
Recycle Bin
My Briefcase
Ddk
Edk
Epsfix
Fonts
Ian
Kmar
Mapi
Ntnotuse
Ntsetup
Practice
Project
Psp311
Sdktempl
Thres
Tosue
Venpract
Winzip
Yong
Aa17026c
Art_trk.xls
Artlist2.xls
Artorder
Bboard3
Bko.ft3
Bkojan96
Bluenum.fh3
Bluenumb.fh3
Chicart.xls
Chris.fh3
Circles.fh3
Compnent.a
Drawing1.w
Edk29
Exchge1.ft3
Forms7
Gv19feb
Indexbts
Is_rules
Is_rules
Mar15_96.x
Meetings.sc
Meta
1 object(s) selected

**Chương 14 :**

# Sử dụng máy in trong mạng Windows NT

Hiện nay máy in trên mạng cũng là một tài nguyên việc chia sẻ của mạng cho người sử dụng. Tuy các máy in đang ngày càng rẻ đi nhưng với nhu cầu về chất lượng đang ngày một cao thì việc chia sẻ các máy in đắt tiền trên mạng vẫn đang cần thiết. Windows NT là một hệ điều hành mạng mà bất kỳ máy tính Windows NT nào cũng có thể cung cấp các dịch vụ in ấn cho người sử dụng trong mạng.

Khi chia sẻ một máy in trên mạng (cho nhiều người có thể cùng sử dụng) chúng ta cần phải giải quyết những vấn đề sau :

- Máy in không làm được 2 việc một lúc, nếu phải nhận cùng một lúc thì sẽ có va chạm, do vậy mạng phải có cơ chế sắp xếp công việc sao cho máy in có thể thực hiện một cách lần lượt các công việc in.

- Các công việc in được thực hiện bởi những người sử dụng khác nhau có thể cần những mức độ ưu tiên khác nhau và hệ thống quan lý in cần có khả năng thực hiện điều này.

## I. Cơ chế in trong mạng Windows NT

Thông thường máy in mạng được quản lý thông qua một máy chủ mà trên đó thực hiện nhiệm vụ quản lý các công việc in, máy chủ đó thường được gọi là máy chủ in (Print server) và chạy chương trình quản lý in. Windows NT cho phép cài đặt máy in tại bất cứ đâu trên mạng, mỗi một máy có cài đặt Windows NT đều có thể thực hiện nhiệm vụ máy chủ in. Nó có thể quản lý máy in gắn trực tiếp vào nó hay một máy in gắn vào máy khác trên mạng.

Để giải quyết những vấn đề đặt ra với công việc in trên mạng Windows NT sử dụng kỹ thuật gọi là Spooling mà chủ yếu như sau:

- Khi người sử dụng quyết định thực hiện một công việc in thì công việc in đó không trực tiếp gửi ra máy in mà nó được đặt trong một file tại máy chủ in. Ở đây việc thực hiện giống như hàng đợi rạp hát, nó là một vùng lưu trữ các công việc in và có nhiệm vụ ngăn chặn xung đột khi các user chi xuất đồng thời ra máy in.

- Máy chủ in duy trì các hàng đợi để cất giữ các công việc in và đưa chúng tới máy in ngay khi có thể. Trong khi đó người sử dụng có thể làm tiếp công việc ngay khi công việc in được cất vào hàng đợi.

- Khi máy in rảnh máy chủ in sẽ chuyển lần lượt các công việc in đang đứng đợi trong hàng tới máy in. Tại đây máy chủ in phải có một khả năng lưu trữ dữ

liệu lớn để có thể lưu trữ nhiều công việc in một lúc và cần phải có khả năng đáp ứng những yêu cầu đa dạng của các công việc in.

Để giải quyết vấn đề nẩy sinh với máy in trong mạng Windows NT tiến hành phân biệt giữa máy in vật lý gọi là Printing device và một thực thể logic của máy in gọi là logic printer. Máy in logic được sử dụng để kiểm soát các tác vụ sau đây :

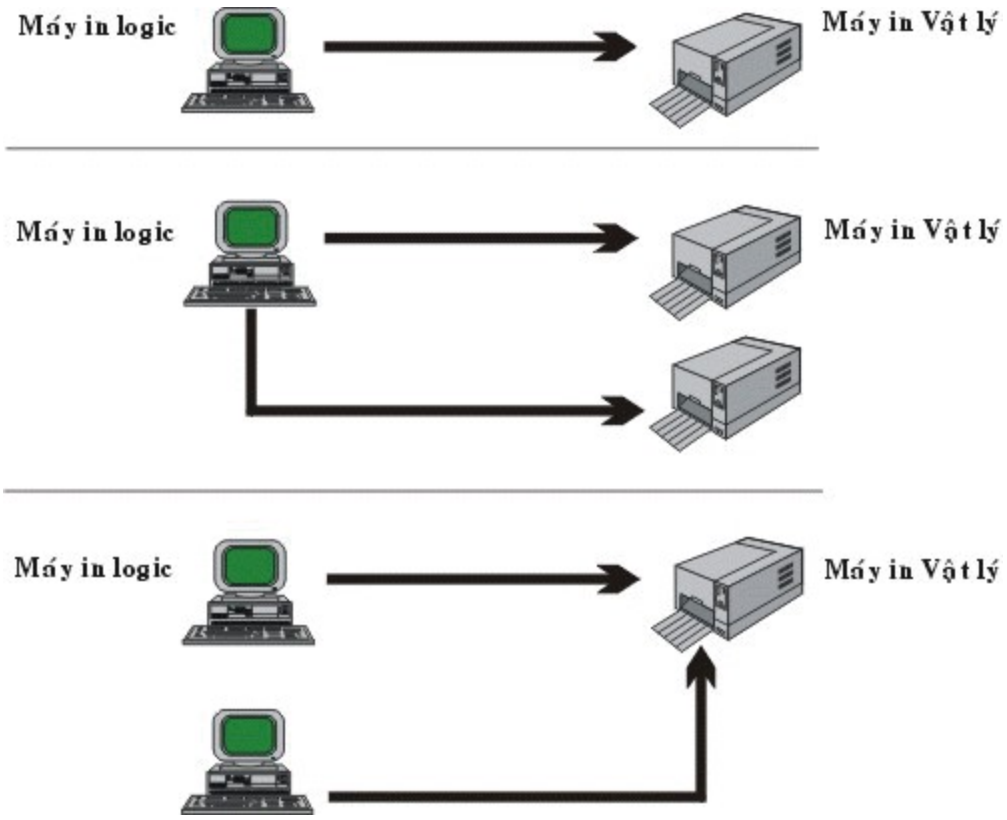
- Công việc in được gởi đi đâu.
- Công việc in ấn gởi đi khi nào.
- Thứ tự ưu tiên của các tác vụ in.

Người sử dụng in ra spool thông qua việc in ra máy in logic, họ sử dụng máy in logic như là máy in đang được gắn là máy của họ nhưng thực sự các dữ liệu được in ra máy in logic được chuyển cho mạng và qua đó đến máy chủ in trước khi được đưa ra máy in mạng.


*Hình 14.1: Máy chủ in và spool*

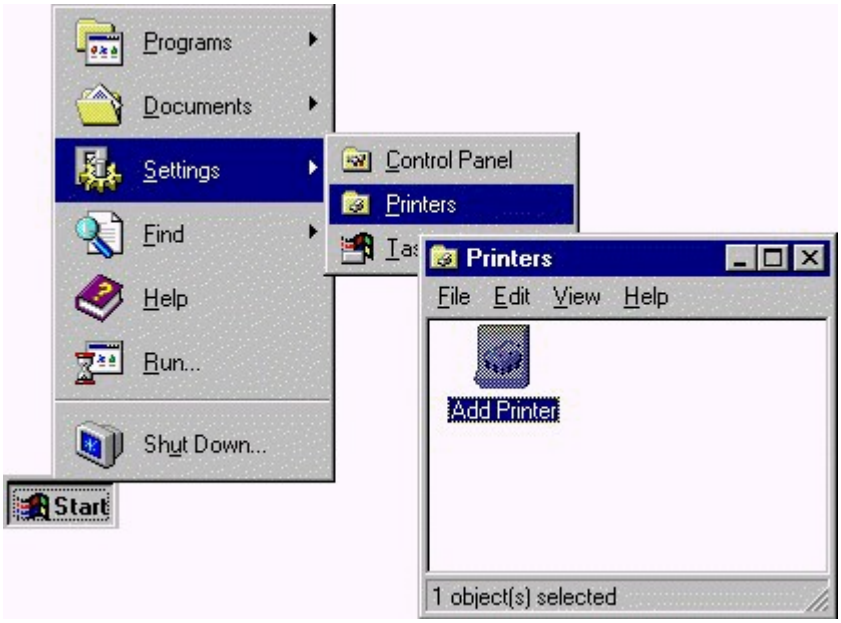
Máy chủ in sẽ liên kết các máy in logic với máy in vật lý, nó phải đảm bảo các công việc in phải được đưa đúng đến máy in vật lý. Tại đây có 3 trường hợp có thể đối với mối quan hệ giữa máy in logic và máy in vật lý

- Một máy in logic liên kết với một máy in vật lý.
- Nhiều máy in logic liên kết với một máy in vật lý.
- Một máy in logic liên kết với nhiều máy in vật lý.

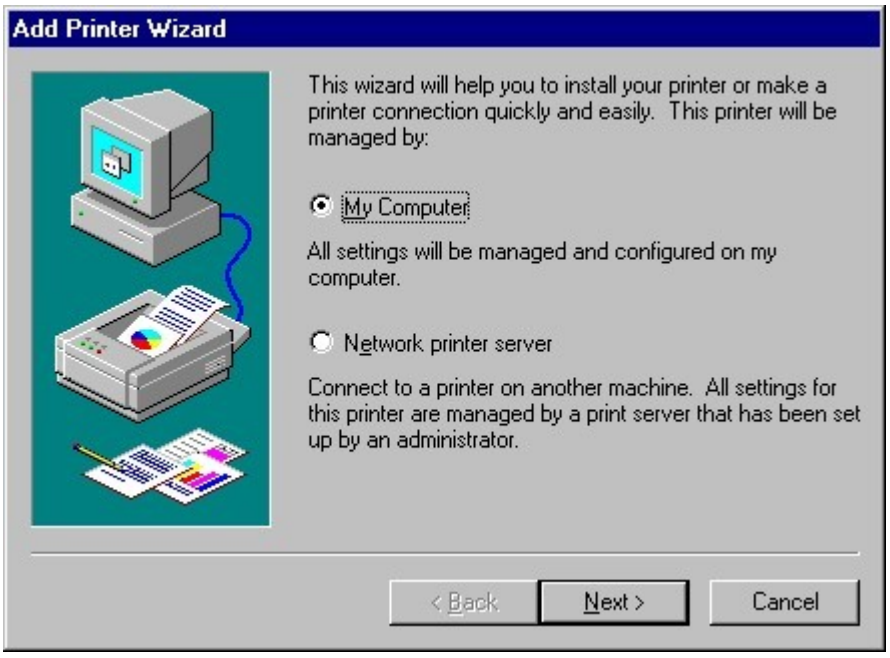



*Hình 14.2: Liên kết giữa máy in Logic và máy in vật lý*

Nếu Server chưa cài đặt máy in logic, ta phải cài đặt máy in logic tương ứng với một máy in thực tế cho Server. Vào menu **Start**, chọn **Settings**, chọn **Printers**, chọn **Add Printer** như:



Hộp sau đó hộp hội thoại **Add printer** winzar hiện ra

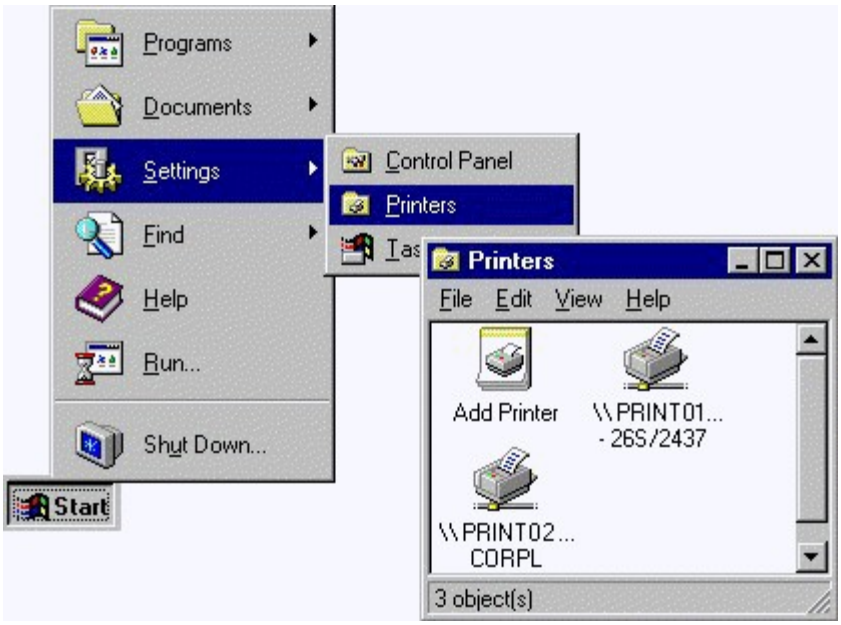



- Chọn My Computer nếu máy in của chúng ta không có card mạng và được nối trực tiếp vào Server.

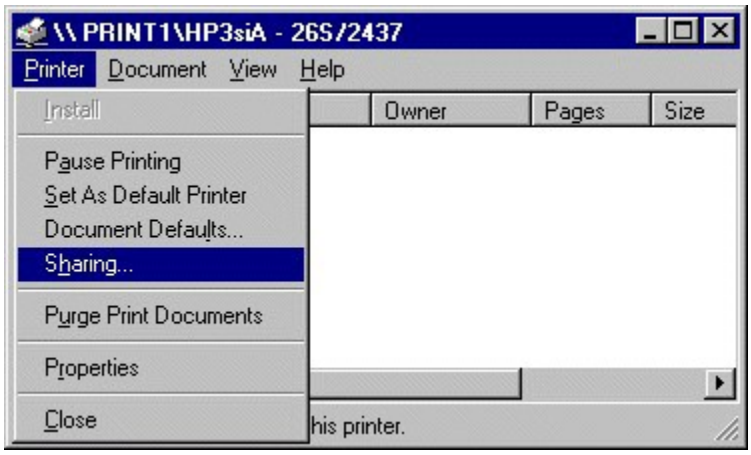
- Chọn Network printer server nếu máy in của chúng ta nối trực tiếp vào mạng.

- Chọn Next, chọn cổng nối với máy in (thường là LPT1). Chọn tên hãng sản xuất và loại máy in ta đang dùng, chọn Next, ta phải trả lời thêm vài câu hỏi phụ như ta có muốn in trang test không? Có muốn đặt máy in này là ngầm định không?

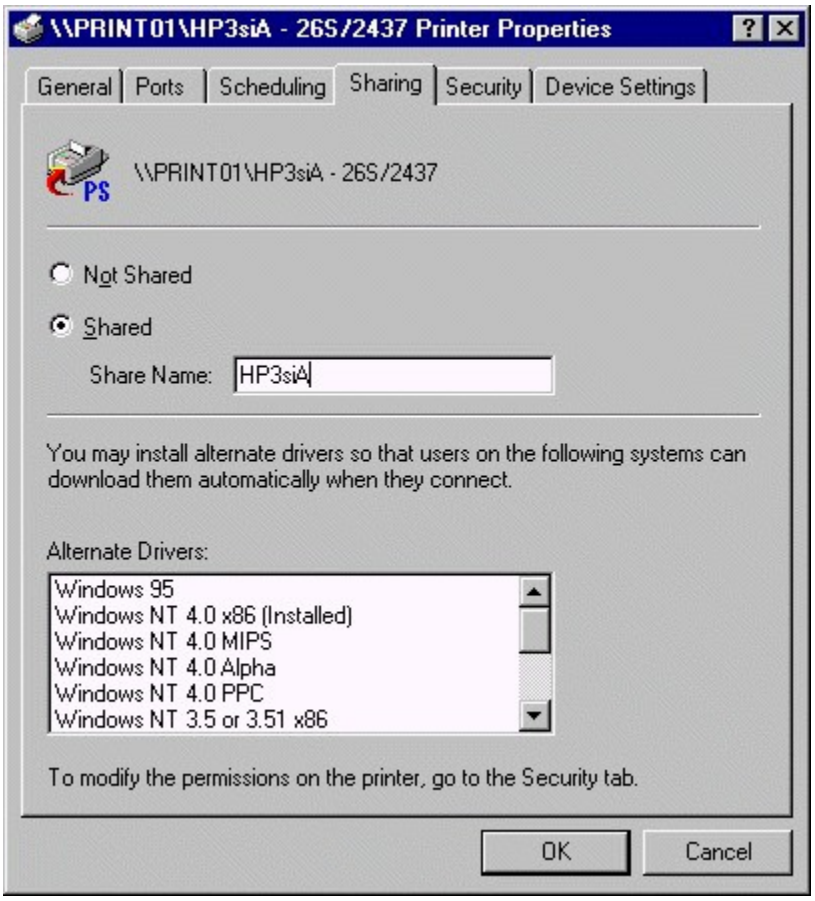
Sau khi cài đặt, chúng ta sẽ thấy xuất hiện thêm biểu tượng máy in mà vừa được cài đặt trong khung máy in. Chúng ta phải cho phép dùng chung máy in nàybằng cách lựa chọn máy in đó Trong khung Printers




- Ta nhắp chuột phải vào tên máy in đó, chọn **Sharing** như hình sau:




Khung **Printer properties** hiện ra cho chúng ta nhập các thông số như: tên máy in logic (Share namem), các tính chất khác như về an toàn. mà chúng ta muốn khi phục vụ mạng.




- Cuối cùng chọn **OK**, lúc này, ta sẽ thấy ở dưới biểu tượng máy in có bàn tay đỡ chứng tỏ máy in này đã được phép dùng chung. Nếu trên Server cài đặt nhiều loại máy in với nhiều chế độ khác nhau, ta có thể chọn máy in ngầm định bằng cách đánh dấu vào mục **Set As Default**.

- Để máy trạm có thể in được qua Server, nếu chưa cài đặt chúng ta phải cài máy in như sau: nhắp đúp vào tên Server có nối với máy in, khung **Shared Printers** sẽ hiện ra danh sách các máy in đã cài trên Server, chúng ta chọn tên máy in cần nối rồi bấm **OK**.

Quay trở lại khung màn hình **Print Manager** chúng ta nhìn thấy thông báo máy in này đã được phép sử dụng. Thoát ra khỏi **Print Manager** và chúng ta có thể in qua máy in mạng trên bất cứ một phần mềm nào trên Windows như Winword, Excel, v.v...

Bất kỳ máy tính Windows NT có thể được cấu hình như là một **print server**. Tuy nhiên chỉ có những người là thành viên của những nhóm sau đây mới có quyền tạo ra các máy in:

- Administrator (NT Worstation and Server).

- Server Operator (NT Server).

- Print Operator (NT Server).
- Power Users (NT Worstation).

## II. Bảo mật của máy in

### Windows NT có các mức độ bảo mật trong in ấn như sau:

- **Quyền sở hửu máy in (Ownership) :** người sử dụng tạo ra một máy in chính là người chủ sở hửu máy in đó và có toàn quyền trên tất cả các thuộc tính của máy in logic. Người chủ sở hửu máy in có thể gán quyền cho những người dùng khác quản lý tài liệu hay toàn quyền điều khiển việc in ấn. Một người sử dụng có toàn quyền thì họ toàn quyền sở hửu máy in logic đó.

- **Quản lý thuộc tính máy in (Permissions):** quyền quản lý máy in bao gồm 4 quyền sau:

  - **No access:** không được phép truy cập.
  - **Print:** in
  - **Manage document:** quản lý văn bản, có khả năng thực hiện các thao tác: Điều khiển khởi đặt tài liệu, Ngừng, phục hồi, khởi động lại,và xóa các tài liệu.
  - **Full control:** toàn quyền điều khiển, thực hiện các quyền quản lý tài liệu và các quyền sau đây:
    - Thay đổi trật tự in ấn tài liệu.
    - Ngừng, tổng hợp lại,che dấu các máy in logic.
    - Thay đổi thuộc tính của máy in logic.
    - Hủy các máy in logic.
    - Thay đổi quyền của máy in logic

Có thể xem tài liệu ở máy in logic và quản lý chúng theo nhiều cách. Người sử dụng luôn quản lý được tất cả các tài liệu mà họ tạo ra. Để quản lý được các tài liệu của các người sử dụng khác, phải là người chủ sở hửu của máy in logic hay là thành viên của các nhóm:

- Administrator.
- Server Operator

- Print operator.

Bất kỳ một máy in nào cũng có thể làm việc trong môi trường mạng nhưng điều quan trọng là xem xét **chu kỳ làm việc (duty cycle)** của máy in. Nghĩa là phải xem xét số lượng trang in tối đa mà máy in có thể in ra trong một khoảng thời gian nhất định.

Các máy in được thiết kế cho mạng thường có **chu kỳ làm việc (duty cycle)** cao. Các máy in có thể gắn vào bất cứ nơi đâu trên mạng. Công việc in không phù thuộc vào các thiết bị phần cứng hay các thiết bị kết nối mà do được quản lý bởi một **print server** và dữ liệu được chuyển vận trên mạng.

**Chương 15 :**

# Các dịch vụ mạng của Windows NT Server

Cũng như các hệ điều hành khác Windows NT cũng có những ưu, khuyết điểm của nó, tuy nhiên Windows NT hiện nay chinh phục được nhiều người dùng với những ưu điểm không thể chối cãi. Là hệ điều hành mạng cho phép tổ chức quản lý một cách chủ động theo nhiều mô hình khác nhau: peer-to-peer, clien/server. Nó thích hợp với tất cả các kiến trúc mạng hiện nay như: hình sao (start), đường thẳng (bus), vòng (ring) và phức hợp. Nó có một số đặc tính ưu việt bảo đảm thực hiện cùng lúc nhiều chương trình mà không bị lỗi. Bản thân Windows NT đáp ứng được hầu hết các giao thức phổ biến nhất trên mạng và cũng hỗ trợ được rất nhiều những dịch vụ truyền thông trên mạng. Nó vừa đáp ứng được cho mạng cục bộ (LAN) và cho cả mạng diện rộng (WAN).

Windows NT cho phép dùng giao thức Windows NT TCP/IP, vốn là một giao thức được sử dụng rất phổ biến trên hầu hết các mạng diện rộng và trên Internet. Giao thức TCP/IP dùng tốt cho nhiều dịch vụ mạng trên môi trường Windows NT.

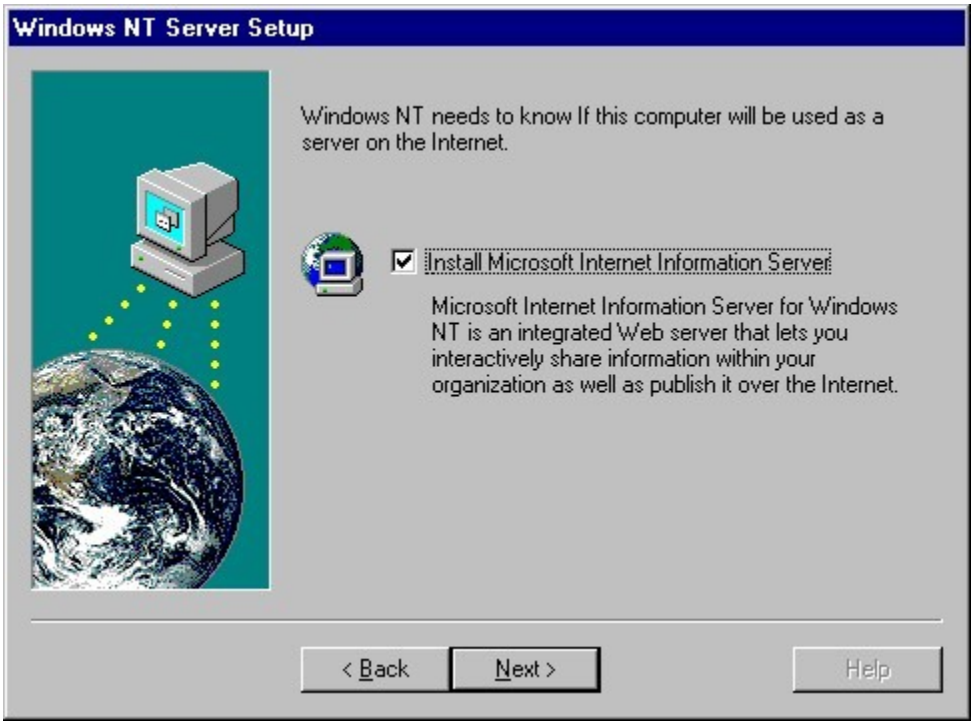
## I. Internet Information Server (IIS)

Internet Information Server là một ứng dụng chạy trên Windows NT, tích hợp chặt với Windows NT, khi cài đặt IIS, IIS có đưa thêm vào tiện ích màn hình kiểm soát (Performance monitor) một số mục như thống kê số lượng truy cập, số trang truy cập. Việc kiểm tra người dùng truy cập cũng dựa trên cơ chế quản lý người sử dụng của Windows NT. Sau khi cài đặt IIS, trong thư mục InetSrv sẽ có các thư mục gốc tương ứng cho từng dịch vụ chọn cài đặt.

IIS bao gồm 3 dịch vụ: World Wide Web (WWW), chuyển file (FTP - File Transfer Protocol) và Gopher. Cả 3 dịch vụ này đều sử dụng kết nối theo giao thức TCP/IP.

### 1. Cài đặt dịch vụ Internet Information Server

Khi cài đặt hệ điều hành Windows NT đến phần mạng Windows NT sẽ hỏi chúng ta xem có cài đặt dịch vụ Internet Information Server hay không với hộp hội thoại




*Hình 15.1: Màn hình cài đặt của IIS*

Để thực hiện việc cài đặt chúng ta Click vào phím Next và Hệ thống sẽ bắt đầu cài đặt các dịch vụ Internet Information Server.

## 2. Các dịch vụ trong IIS

### *a. WWW (World Wide Web) :*

Là một trong những dịch vụ chính trên Internet cho phép người sử dụng xem thông tin một cách dễ dàng, sinh động. Dữ liệu chuyển giữa Web Server và Web Client thông qua nghi thức HTTP (Hypertext Transfer Protocol).

Người quản trị có thể xem các thông tin như các người dùng đã truy cập, các trang được truy cập, các yêu cầu được chấp nhận, các yêu cầu bị từ chối. thông qua các file có thể được lưu dưới dạng cơ sở dữ liệu.

### *b. FTP (File Transfer Protocol)*

Sử dụng giao thức TCP để chuyển file giữa 2 máy và cũng hoạt động theo mô hình Client/Server, khi nhận được yêu cầu từ client, đầu tiên FTP Server sẽ kiểm tra tính hợp lệ của người dùng thông qua tên và mật mã. Nếu hợp lệ, FTP Server sẽ kiểm tra quyền người dùng trên tập tin hay thư mục được xác định trên FTP Server. Nếu hợp lệ và hệ thống file là NTFS thì sẽ có thêm kiểm tra ở mức thư mục, tập tin theo NTFS. Sau khi tất cả hợp lệ, người dùng sẽ được quyền tương ứng trên tập tin, thư mục đó.

**Để sử dụng FTP có nhiều cách:**

- Sử dụng Web Browser.
- Sử dụng Command line.
- Sử dụng từ <Run> command trong Windows.

***c. Gopher***

Là một dịch vụ sử dụng giao diện menu để Gopher Client tìm và chuyển bất kỳ thông tin nào mà Gopher Server đã được cấu hình. Gopher cũng sử dụng kết nối theo giao thức TCP/IP.

**II. Dynamic Host Configuration Protocol (DHCP) :**

Trong một mạng máy tính, việc cấp các địa chỉ IP tĩnh cố định cho các host sẽ dẫn đến tình trạng lãng phí địa chỉ IP, vì trong cùng một lúc không phải các host hoạt động đồng thời với nhau, do vậy sẽ có một số địa chỉ IP bị thừa. Để khắc phục tình trạng đó, dịch vụ DHCP đưa ra để cấp phát các địa chỉ IP động trong mạng.

Trong mạng máy tính NT khi một máy phát ra yêu cầu về các thông tin của TCPIP thì gọi là DHCP client, còn các máy cung cấp thông tin của TCPIP gọi là DHCP server. Các máy DHCP server bắt buộc phải là Windows NT server.

Cách cấp phát địa chỉ IP trong DHCP: Một user khi log on vào mạng, nó cần xin cấp 1 địa chỉ IP, theo 4 bước sau :

- Gởi thông báo đến tất cả các DHCP server để yêu cầu được cấp địa chỉ.
- Tất cả các DHCP server gởi trả lời địa chỉ sẽ cấp đến cho user đó.
- User chọn 1 địa chỉ trong số các địa chỉ, gởi thông báo đến server có địa chỉ được chọn.
- Server được chọn gởi thông báo khẳng định đến user mà nó cấp địa chỉ.

**Quản trị các địa chỉ IP của DHCP server:** Server quản trị địa chỉ thông qua thời gian thuê bao địa chỉ (lease duration). Có ba phương pháp gán địa chỉ IP cho các Worstation :

- Gán thủ công.
- Gán tự động.
- Gán động .

Trong phương pháp gán địa chỉ IP thủ công thì địa chỉ IP của DHCP client được gán thủ công bởi người quản lý mạng tại DHCP server và DHCP được sử dụng để chuyển tới DHCP client giá trị địa chỉ IP mà được định bởi người quản trị mạng

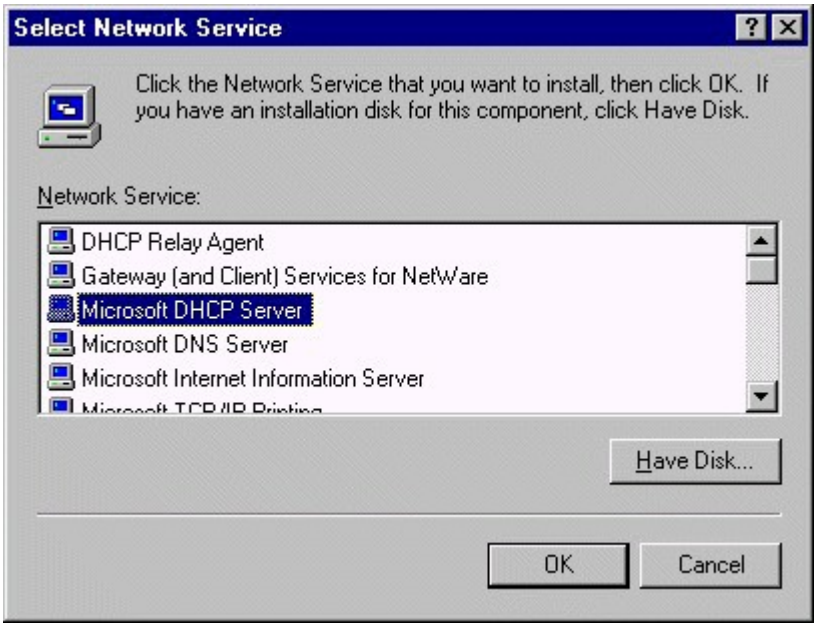
Trong phương pháp gán địa chỉ IP tự động DHCP client được gán địa chỉ IP khi lần đầu tiên nó nối vào mạng. Địa chỉ IP được gán bằng phương pháp này sẽ được gán vĩnh viễn cho DHCP client và địa chỉ này sẽ không bao giờ được sử dụng bởi một DHCP client khác

Trong phương pháp gán địa chỉ IP động thì DHCP server gán địa chỉ IP cho DHCP client tạm thời. Sau đó địa chỉ IP này sẽ được DHCP client sử dụng trong một thời gian đặc biệt. Đến khi thời gian này hết hạn thì địa chỉ IP này sẽ bị xóa mất. Sau đó nếu DHCP client cần nối kết vào mạng thì nó sẽ được cấp một địa chủ IP khác

Phương pháp gán địa chỉ IP động này đặc biệt hữu hiệu đối với những DHCP client chỉ cần địa chỉ IP tạm thời để kết nối vào mạng. Ví dụ một tình huống trên mạng có 300 users và sử dụng subnet là lớp C. Điều này cho phép trên mạng có 253 nodes trên mạng. Bởi vì mỗi computer nối kết vào mạng sử dụng TCP/IP cần có một địa chỉ IP duy nhất do đó tất cả 300 computer không thể đồng thời nối kết vào mạng. Vì vậy nếu ta sử dụng phương pháp này ta có thể sử dụng lại những IP mà đã được giải phóng từ các DHCP client khác.

Cài đặt DHCP chỉ có thể cài trên Windows NT server mà không thể cài trên Client. Các bước thực hiện như sau:

- Login vào Server với tên Administrator .
- Click hai lần vào icon **Network** . Ta sẽ thấy hộp hội thoại **Network dialog box**



*Hình 15.2: Màn hình cài đặt của DHCP*

- Chọn tab **service** và click vào nút **Add** .

- Ta sẽ thấy một loạt các service của Windows NT server nằm trong hộp hội thoại **Select Network Service**. Chọn **Microsoft DHCP server** từ danh sách các service được liệt kê ở phía dưới và nhấn **OK** và thực hiện các yêu cầu tiếp theo của Windows NT.

Để cập nhật và khai thác DHCP server chúng ta chọn mục DHCP manager trong Netwrok Administrator Tools.

**III. Dịch vụ Domain Name Service (DNS)**

Hiện nay trong mạng Internet số lượng các nút (host) lên tới hàng triệu nên chúng ta không thể nhớ hết địa chỉ IP được, Mỗi host ngoài địa chỉ IP còn có một cái tên phân biệt, DNS là 1 cơ sở dữ liệu phân tán cung cấp ánh xạ từ tên host đếùn địa chỉ IP. Khi đưa ra 1 tên host, DNS server sẽ trả về địa chỉ IP hay 1 số thông tin của host đó. Điều này cho phép người quản lý mạng dễ dàng trong việc chọn tên cho host của mình

**DNS server được dùng trong các trường hợp sau :**

- Chúng ta muốn có 1 tên domain riêng trên Interner để có thể tạo, tách rời các domain con bên trong nó.

- Chúng ta cần 1 dịch vụ DNS để điều khiển cục bộ nhằm tăng tính linh hoạt cho domain cục bộ của bạn.

- Chúng ta cần một bức tường lửa để bảo vệ không cho người ngoài thâm nhập vào hệ thống mạng nội bộ của mình

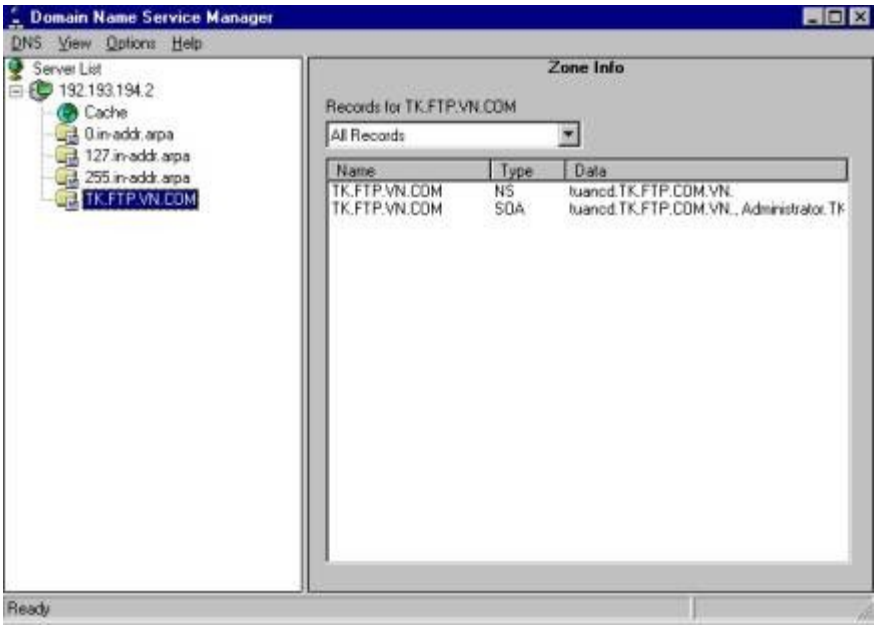
Có thể quản lý trực tiếp bằng các trình soạn thảo text để tạo và sửa đổi các file hoặc dùng DNS manager để tạo và quản lý các đối tượng của DNS như: Servers, Zone, Các mẫu tin, các Domains, Tích hợp với Win, .

Cài đặt DNS chỉ có thể cài trên Windows NT server mà không thể cài trên Client. Các bước thực hiện như sau:

- Login vào Server với tên **Administrator**.

- Click hai lần vào icon **Network**. Ta sẽ thấy hộp hội thoại **Network dialog box** tương tụ như trên và lựa chọn **Microsoft DNS Server**.

Để cập nhật và khai thác DNS server chúng ta chọn mục **DNS manager trong Netwrok Administrator Tools**. Hộp hội thoại sau đây sẽ hiện ra




*Hình 15.3: Màn hình DNS Manager*

Mỗi một tập hợp thông tin chứa trong **DNS database** được coi như là **Resourse record**. Những **Resourse record** cần thiết sẽ được liệt kê dưới đây:

| Tên Record | Mô tả |
|---|---|
| A (Address) | Dẫn đường một tên host computer hay tên của một thiết bị mạng khác trên mạng tới một địa chỉ IP trong DNS zone |
| CNAME () | Tạo một tên Alias cho tên một host computer trên mạng |
| MX () | Định nghĩa một sự trao đổi mail cho host computer đó |
| NS (name server) | Định nghĩa tên server DNS cho DNS domain |
| PTR (Pointer) | Dẫn đường một địa chỉ IP đến tên host trong DNS server zone |
| SOA (Start of authority) | Hiển thị rằng tên server DNS này thì chứa những thông tin tốt nhất |

## IV. Remote Access Service (RAS)

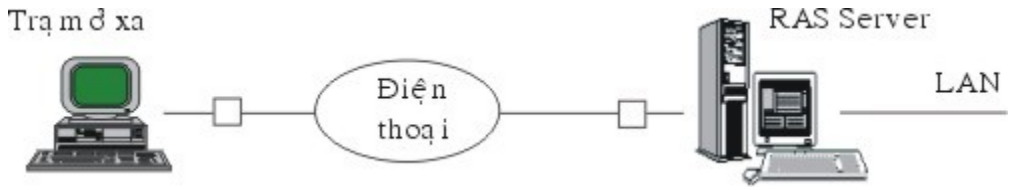
Ngoài những liên kết tại chỗ với mạng cục bộ (LAN) các nối kết từ xa vào mạng LAN hiện đang là những yêu cầu cần thiết của người sử dụng. Việc liên kết đó cho phép một máy từ xa như của một người sử dụng tại nhà có thể qua đường dây điện

thoại thâm nhập vào một mạng LAN và sử dụng tài nguyên của nó. Cách thông dụng nhất hiện nay là dùng modem để có thể truyền trên đường dây điện thoại.

Windows NT cung cấp Dịch vụ Remote access Service cho phép các máy trạm có thể nối với tài nguyên của Windows NT server thông qua đường dây điện thoại. RAS cho phép truyền nối với các server, điều hành các user và các server, thực hiện các chương trình khai thác số liệu, thiết lập sự an toàn trên mạng. .

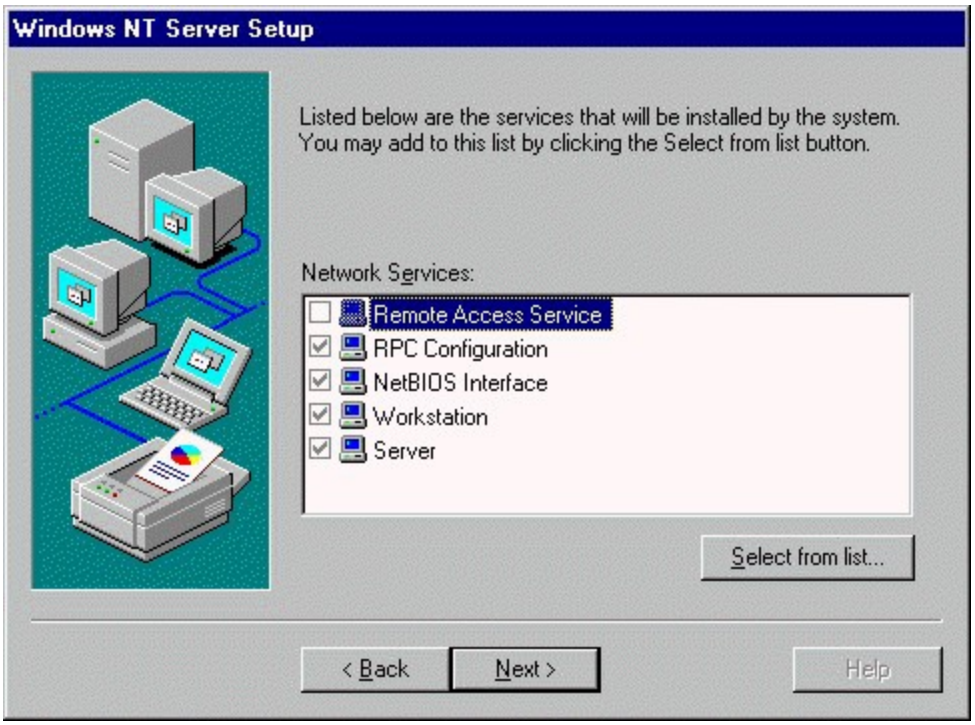
Máy trạm có thể được nối với server có dịch vụ RAS thông qua modem hoạc pull modem, cable null modem (RS232) hoặc X.25 network.

Khi đã cài đặt dịch vụ RAS, cần phải đảm bảo quyền truy nhập từ xa cho người sử dụng bằng tiện ích remote access amind để gán quyền hoặc có thể đăng ký người sử dụng ở remote access server. RAS cũng có cơ chế đảm bảo an toàn cho tài nguyên bằng cách kiểm soát các yếu tố sau: quyền sử dụng, kiểm tra mã số, xác nhận người sử dụng, đăng ký sử dụng tài nguyên và xác nhận quyền gọi lại.




*Hình 15.4: Mô hình truy cập từ xa bằng dịch vụ RAS*

Để cài đặt RAS chúng ta lựa chọn yêu cầu hộp Windows NT server setup hiện ra lúc cài đặt hệ điều hành Windows NT.




Với RAS tất cả các ứng dụng đều thực hiện trên máy từ xa, thay vì kết nối với mạng thông qua card mạng và đường dây mạng thì máy ở xa sẽ liên kết qua modem tới một RAS Server. Tất cả dữ liệu cần thiết được truyền qua đường điện thoại, mặc dù tốc độ truyền qua modem chậm hơn so với qua card mạng nhưng với những tác vụ của LAN không phải bao giờ dữ liệu cũng truyền nhiều.

Với những khả năng to lớn của mình trong các dịch vụ mạng, hệ điều hành Windows NT là một trong những hệ điều hành mạng tốt nhất hiện nay. Hệ điều hành Windows NT vừa cho phép giao lưu giữa các máy trong mạng, vừa cho phép truy nhập từ xa, cho phép truyền file, vừa đáp ứng cho mạng cục bộ (LAN) vừa đáp ứng cho mạng diện rộng (WAN) như Intranet, Internet. Với những khả năng như vậy hiện nay hệ điều hành Windows NT đã có những vị trí vững chắc trong việc cung cấp các giải pháp mạng trên thế giới.

# Mục lục


Mục lục ..... 2
GIỚI THIỆU ..... 16
GIÁO TRÌNH LÝ THUYẾT ..... 18
TÀI LIỆU THAM KHẢO ..... 18
Bài 1 GIỚI THIỆU VỀ MẠNG ..... 19
Tóm tắt ..... 19
Bài 1 GIỚI THIỆU VỀ MẠNG ..... 20
I. CÁC KIẾN THỨC CƠ SỞ ..... 20
II. CÁC LOẠI MẠNG MÁY TÍNH ..... 21
II.1. Mạng cục bộ LAN (Local Area Network) ..... 21
II.2. Mạng đô thị MAN (Metropolitan Area Network) ..... 21
II.3. Mạng diện rộng WAN (Wide Area Network) ..... 21
II.4. Mạng Internet ..... 22
III. CÁC MÔ HÌNH XỬ LÝ MẠNG ..... 22
III.1. Mô hình xử lý mạng tập trung ..... 22
III.2. Mô hình xử lý mạng phân phối ..... 23
III.3. Mô hình xử lý mạng cộng tác. ..... 23
IV. CÁC MÔ HÌNH QUẢN LÝ MẠNG ..... 24
IV.1. Workgroup ..... 24
IV.2. Domain ..... 24
V. CÁC MÔ HÌNH ỨNG DỤNG MẠNG ..... 24
V.1. Mạng ngang hàng (peer to peer) ..... 24
V.2. Mạng khách chủ (client- server) ..... 25
VI. CÁC DỊCH VỤ MẠNG ..... 25
VI.1. Dịch vụ tập tin (Files Services) ..... 26
VI.2. Dịch vụ in ấn (Print Services) ..... 26
VI.3. Dịch vụ thông điệp (Message Services) ..... 26
VI.4. Dịch vụ thư mục (Directory Services) ..... 27
VI.5. Dịch vụ ứng dụng (Application Services) ..... 27
VI.6. Dịch vụ cơ sở dữ liệu (Database Services) ..... 27
VI.7. Dịch vụ Web ..... 27
VII. CÁC LỢI ÍCH THỰC TẾ CỦA MẠNG ..... 27
VII.1.Tiết kiệm được tài nguyên phần cứng. ..... 27
VII.2.Trao đổi dữ liệu trở nên dễ dàng hơn. ..... 28
VII.3.Chia sẻ ứng dụng. ..... 28
VII.4.Tập trung dữ liệu, bảo mật và backup tốt. ..... 28
VII.5.Sử dụng các phần mềm ứng dụng trên mạng. ..... 28
VII.6.Sử dụng các dịch vụ Internet. ..... 28
Bài 2 MÔ HÌNH THAM CHIẾU OSI ..... 29
Tóm tắt ..... 29
I. MÔ HÌNH OSI. ..... 30
I.1. Khái niệm giao thức (protocol). ..... 30
I.2. Các tổ chức định chuẩn. ..... 30
I.3. Mô hình OSI. ..... 30
I.4. Chức năng của các lớp trong mô hình tham chiếu OSI ..... 31
II. QUÁ TRÌNH XỬ LÝ VÀ VẬN CHUYỂN CỦA MỘT GÓI DỮ LIỆU. ..... 33




Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

II.1. Quá trình đóng gói dữ liệu (tại máy gửi) .....33
II.2. Quá trình truyền dữ liệu từ máy gửi đến máy nhận. .....34



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

II.3. Chi tiết quá trình xử lý tại máy nhận ..... 34
III. MÔ HÌNH THAM CHIẾU TCP/IP. ..... 35
III.1. Vai trò của mô hình tham chiếu TCP/IP. ..... 35
III.2. Các lớp của mô hình tham chiếu TCP/IP. ..... 35
III.3. Các bước đóng gói dữ liệu trong mô hình TCP/IP. ..... 36
III.4. So sánh mô hình OSI và TCP/IP. ..... 36
Bài 3 ĐỊA CHỈ IP ..... 38
Tóm tắt ..... 38
I. TỔNG QUAN VỀ ĐỊA CHỈ IP ..... 39
II. MỘT SỐ KHÁI NIỆM VÀ THUẬT NGỮ LIÊN QUAN. ..... 39
III. GIỚI THIỆU CÁC LỚP ĐỊA CHỈ. ..... 40
III.1. Lớp A. ..... 40
III.2. Lớp B. ..... 41
III.3. Lớp C. ..... 41
III.4. Lớp D và E. ..... 42
III.5. Bảng tổng kết. ..... 42
III.6. Ví dụ cách triển khai đặt địa chỉ IP cho một hệ thống mạng. ..... 42
III.7. Chia mạng con (subnetting). ..... 42
III.8. Địa chỉ riêng (private address) và cơ chế chuyển đổi địa chỉ mạng (Network Address Translation - NAT) ..... 45
III.9. Cơ chế NAT ..... 45
IV. MỘT SỐ CÂU HỎI THƯỜNG ĐẶT RA KHI LÀM VIỆC VỚI ĐỊA CHỈ IP. ..... 45
IV.1. Ví dụ 1. ..... 45
IV.2. Ví dụ 2. ..... 47
Bài 4 PHƯƠNG TIỆN TRUYỀN DẪN VÀ CÁC THIẾT BỊ MẠNG ..... 48
Tóm tắt ..... 48
I. GIỚI THIỆU VỀ MÔI TRƯỜNG TRUYỀN DẪN ..... 49
I.1. Khái niệm ..... 49
I.2. Tần số truyền thông ..... 49
I.3. Các đặc tính của phương tiện truyền dẫn ..... 49
I.4. Các kiểu truyền dẫn. ..... 50
II. CÁC LOẠI CÁP ..... 51
II.1. Cáp đồng trục (coaxial). ..... 51
II.2. Cáp xoắn đôi. ..... 53
II.3. Cáp quang (Fiber-optic cable). ..... 56
III. ĐƯỜNG TRUYỀN VÔ TUYẾN. ..... 58
III.1. Sóng vô tuyến (radio). ..... 58
III.2. Sóng viba. ..... 59
III.3. Hồng ngoại. ..... 59
IV. CÁC THIẾT BỊ MẠNG. ..... 60
IV.1. Card mạng (NIC hay Adapter). ..... 60
IV.2. Card mạng dùng cáp điện thoại. ..... 61
IV.3. Modem. ..... 62
IV.4. Repeater. ..... 63
IV.5. Hub. ..... 63
IV.6. Bridge (cầu nối). ..... 64
IV.7. Switch ..... 64
IV.8. Wireless Access Point. ..... 66



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

IV.9. Router. .....67



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

IV.10. Thiết bị mở rộng. ..... 68
IV.10.1 Gateway – Proxy: ..... 68
IV.10.2 Thiết bị truy cập Internet. ..... 68
Bài 5 CÁC KIẾN TRÚC VÀ CÔNG NGHỆ MẠNG LAN ..... 70
Tóm tắt ..... 70
I. CÁC KIẾN TRÚC MẠNG (TOPOLOGY). ..... 71
I.1. Khái niệm. ..... 71
I.2. Các kiểu kiến trúc mạng chính. ..... 71
I.3. Các kiến trúc mạng kết hợp. ..... 73
II. CÁC CÔNG NGHỆ MẠNG LAN. ..... 74
II.1. Khái niệm. ..... 74
II.2. Ethernet ..... 74
II.2.1 Chuẩn 10Base2 ..... 75
II.2.2 Chuẩn 10Base5 ..... 76
II.2.3 Chuẩn 10BaseT. ..... 77
II.2.4 Chuẩn 10BaseFL. ..... 78
II.2.5 Chuẩn 100VG-AnyLAN. ..... 78
II.2.6 Chuẩn 100BaseX. ..... 79
II.3. FDDI. ..... 80
Bài 6 KHẢO SÁT CÁC LỚP TRONG MÔ HÌNH OSI ..... 83
Tóm tắt ..... 83
I. KHẢO SÁT CHI TIẾT LỚP 2 (DATA LINK). ..... 84
I.1. Lớp con LLC. ..... 84
I.2. Lớp con MAC. ..... 84
I.3. Quá trình tìm địa chỉ MAC: ..... 84
I.4. Các phương pháp truy cập đường truyền ..... 85
I.4.1 Cảm sóng đa truy (CSMA/CD). ..... 85
I.4.2 Chuyển thẻ bài (Token-passing): ..... 86
II. KHẢO SÁT CHI TIẾT LỚP 3 (NETWORK). ..... 86
III. KHẢO SÁT CHI TIẾT LỚP 4 (TRANSPORT) ..... 88
III.1. Giao thức TCP (TCP protocol). ..... 88
III.2. Giao thức UDP (UDP protocol). ..... 90
III.3. Khái niệm Port. ..... 91
IV. CÁC MÔ HÌNH FIREWALL. ..... 92
IV.1. Giới thiệu về Firewall. ..... 92
IV.2. Dual homed host. ..... 92
IV.3. Screened Host. ..... 92
IV.4. Screened Subnet. ..... 93
Bài 7 CÁC DỊCH VỤ MẠNG CƠ SỞ ..... 95
Tóm tắt ..... 95
Bài 7 CÁC DỊCH VỤ MẠNG CƠ SỞ ..... 96
V. DỊCH VỤ WORLD WIDE WEB. ..... 96
V.1. Một số khái niệm về Internet. ..... 96
V.2. Giới thiệu mô hình hoạt động của Web. ..... 99
V.3. Khảo sát web browser Internet Explorer. ..... 100
V.4. Search Engine và tìm kiếm thông tin trên Web. ..... 113
VI. DỊCH VỤ FTP. ..... 116



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

VI.1. Mô hình hoạt động của FTP.....116



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

VI.2. Tập hợp các lệnh FTP. ..... 116
VI.3. Dùng FTP trong Windows Commander. ..... 119
VII. E-MAIL. ..... 120
VII.1.Mô hình hoạt động. ..... 120
VII.2.Các loại mail. ..... 120
VII.3.Sử dụng WebMail. ..... 120
VII.4.Sử dụng Outlook Express. ..... 125
VIII. XÂY DỰNG TRANG WEB. ..... 136
VIII.1. Giới thiệu ngôn ngữ HTML. ..... 136
VIII.2. Các thẻ (Tag) trong HTML. ..... 136
VIII.3. Các ví dụ về HTML. ..... 138
VIII.4. Giới thiệu công cụ tạo web FrontPage. ..... 142
IX. GIỚI THIỆU VỀ JAVA SCRIPT VÀ VB SCRIPT. ..... 150
IX.1. Giới thiệu về ngôn ngữ script. ..... 150
IX.2. Tổng quan Java Script. ..... 151
IX.3. Sự kiện trong html và java script. ..... 152
IX.4. VB Script và OLE Controls. ..... 154
Bài 8 GIỚI THIỆU VÀ CÀI ĐẶT WINDOWS SERVER 2003 ..... 157
Bài 8 GIỚI THIỆU VÀ CÀI ĐẶT WINDOWS SERVER 2003 ..... 157
Tóm tắt ..... 157
I. TỔNG QUAN VỀ HỌ HỆ ĐIỀU HÀNH WINDOWS SERVER 2003 ..... 158
II. CHUẨN BỊ CÀI ĐẶT WINDOWS SERVER 2003. ..... 159
II.1. Yêu cầu phần cứng ..... 160
II.2. Tương thích phần cứng ..... 160
II.3. Cài đặt mới hoặc nâng cấp ..... 161
II.4. Phân chia ổ đĩa. ..... 161
II.5. Chọn hệ thống tập tin. ..... 162
II.6. Chọn chế độ sử dụng giấy phép. ..... 162
II.7. Chọn phương án kết nối mạng. ..... 162
II.7.1 Các giao thức kết nối mạng. ..... 162
II.7.2 Thành viên trong Workgroup hoặc Domain. ..... 162
III. CÀI ĐẶT WINDOWS SERVER 2003. ..... 163
III.1. Giai đoạn Preinstallation. ..... 163
III.1.1 Cài đặt từ hệ điều hành khác. ..... 163
III.1.2 Cài đặt trực tiếp từ đĩa CD Windows 2003. ..... 163
III.1.3 Cài đặt Windows 2003 Server từ mạng. ..... 163
III.2. Giai đoạn Text-Based Setup. ..... 163
III.3. Giai đoạn Graphical-Based Setup. ..... 166
IV. TỰ ĐỘNG HÓA QUÁ TRÌNH CÀI ĐẶT. ..... 170
IV.1. Giới thiệu kịch bản cài đặt. ..... 170
IV.2. Tự động hóa dùng tham biến dòng lệnh. ..... 170
IV.3. Sử dụng Setup Manager để tạo ra tập tin trả lời. ..... 171
IV.4. Sử dụng tập tin trả lời ..... 178
IV.4.1 Sử dụng đĩa CD Windows 2003 Server có thể khởi động được ..... 178
IV.4.2 Sử dụng một bộ nguồn cài đặt Windows 2003 Server ..... 178
Bài 9 ACTIVE DIRECTORY ..... 179
Tóm tắt ..... 179



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

I. CÁC MÔ HÌNH MẠNG TRONG MÔI TRƯỜNG MICROSOFT. ..... 180



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

I.1. Mô hình Workgroup. 180
I.2. Mô hình Domain. 180
II. ACTIVE DIRECTORY. 181
II.1. Giới thiệu Active Directory. 181
II.2. Chức năng của Active Directory. 181
II.3. Directory Services. 182
II.3.1 Giới thiệu Directory Services. 182
II.3.2 Các thành phần trong Directory Services. 182
II.4. Kiến trúc của Active Directory. 183
II.4.1 Objects. 184
II.4.2 Organizational Units. 184
II.4.3 Domain. 185
II.4.4 Domain Tree. 186
II.4.5 Forest. 186
III. CÀI ĐẶT VÀ CẤU HÌNH ACTIVE DIRECTORY. 187
III.1. Nâng cấp Server thành Domain Controller. 187
III.1.1 Giới thiệu. 187
III.1.2 Các bước cài đặt. 187
III.2. Gia nhập máy trạm vào Domain. 194
III.2.1 Giới thiệu. 194
III.2.2 Các bước cài đặt. 195
III.3. Xây dựng các Domain Controller đồng hành. 196
III.3.1 Giới thiệu. 196
III.3.2 Các bước cài đặt. 196
III.4. Xây dựng Subdomain. 200
III.5. Xây dựng Organizational Unit. 203
III.6. Công cụ quản trị các đối tượng trong Active Directory. 206
Bài 10 QUẢN LÝ TÀI KHOẢN NGƯỜI DÙNG VÀ NHÓM. 208
Tóm tắt. 208
I. ĐỊNH NGHĨA TÀI KHOẢN NGƯỜI DÙNG VÀ TÀI KHOẢN NHÓM. 209
I.1. Tài khoản người dùng. 209
I.1.1 Tài khoản người dùng cục bộ. 209
I.1.2 Tài khoản người dùng miền. 209
I.1.3 Yêu cầu về tài khoản người dùng. 210
I.2. Tài khoản nhóm. 210
I.2.1 Nhóm bảo mật. 210
I.2.2 Nhóm phân phối. 211
I.2.3 Qui tắc gia nhập nhóm. 211
II. CHỨNG THỰC VÀ KIỂM SOÁT TRUY CẬP. 212
II.1. Các giao thức chứng thực. 212
II.2. Số nhận diện bảo mật SID. 212
II.3. Kiểm soát hoạt động truy cập của đối tượng. 213
III. CÁC TÀI KHOẢN TẠO SẴN. 213
III.1. Tài khoản người dùng tạo sẵn. 213
III.2. Tài khoản nhóm Domain Local tạo sẵn. 214



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

III.3. Tài khoản nhóm Global tạo sẵn. .....216



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

III.4. Các nhóm tạo sẵn đặc biệt. ....217
IV. QUẢN LÝ TÀI KHOẢN NGƯỜI DÙNG VÀ NHÓM CỤC BỘ. ....217
IV.1. Công cụ quản lý tài khoản người dùng cục bộ. ....217
IV.2. Các thao tác cơ bản trên tài khoản người dùng cục bộ. ....219
IV.2.1 Tạo tài khoản mới. ....219
IV.2.2 Xóa tài khoản. ....219
IV.2.3 Khóa tài khoản. ....220
IV.2.4 Đổi tên tài khoản. ....221
IV.2.5 Thay đổi mật khẩu. ....221
V. QUẢN LÝ TÀI KHOẢN NGƯỜI DÙNG VÀ NHÓM TRÊN ACTIVE DIRECTORY. ....221
V.1. Tạo mới tài khoản người dùng. ....221
V.2. Các thuộc tính của tài khoản người dùng ....223
V.2.1 Các thông tin mở rộng của người dùng ....224
V.2.2 Tab Account. ....226
V.2.3 Tab Profile. ....228
V.2.4 Tab Member Of. ....230
V.2.5 Tab Dial-in. ....231
V.3. Tạo mới tài khoản nhóm. ....232
V.4. Các tiện ích dòng lệnh quản lý tài khoản người dùng và tài khoản nhóm. ....232
V.4.1 Lệnh net user. ....232
V.4.2 Lệnh net group. ....233
V.4.3 Lệnh net localgroup. ....234
V.4.4 Các lệnh hỗ trợ dịch vụ Active Driectory trong môi trường Windows Server 2003. 234
Bài 11 CHÍNH SÁCH HỆ THỐNG ....236
Tóm tắt ....236
I. CHÍNH SÁCH TÀI KHOẢN NGƯỜI DÙNG. ....237
I.1. Chính sách mật khẩu. ....237
I.2. Chính sách khóa tài khoản. ....238
II. CHÍNH SÁCH CỤC BỘ. ....238
II.1. Chính sách kiểm toán. ....239
II.2. Quyền hệ thống của người dùng. ....240
II.3. Các lựa chọn bảo mật. ....243
III. IPSec. ....244
III.1. Các tác động bảo mật. ....244
III.2. Các bộ lọc IPSec. ....245
III.3. Triển khai IPSec trên Windows Server 2003. ....245
III.3.1 Các chính sách IPSec tạo sẵn. ....246
III.3.2 Ví dụ tạo chính sách IPSec đảm bảo một kết nối được mã hóa. ....246
Bài 12 CHÍNH SÁCH NHÓM ....251
Tóm tắt ....251
I. GIỚI THIỆU. ....252
I.1. So sánh giữa System Policy và Group Policy. ....252
I.2. Chức năng của Group Policy. ....252
II. TRIỂN KHAI MỘT CHÍNH SÁCH NHÓM TRÊN MIỀN. ....253
II.1. Xem chính sách cục bộ của một máy tính ở xa. ....253



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

II.2. Tạo các chính sách trên miền. .....254



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

III. MỘT SỐ MINH HỌA GPO TRÊN NGƯỜI DÙNG VÀ CẤU HÌNH MÁY. 256
III.1. Khai báo một logon script dùng chính sách nhóm. 256
III.2. Hạn chế chức năng của Internet Explorer. 258
III.3. Chỉ cho phép một số ứng dụng được thi hành. 258
Bài 13 QUẢN LÝ ĐĨA 260
Tóm tắt 260
I. CẤU HÌNH HỆ THỐNG TẬP TIN. 261
II. CẤU HÌNH ĐĨA LƯU TRỮ. 261
II.1. Basic storage. 261
II.2. Dynamic storage 262
II.2.1 Volume simple. 262
II.2.2 Volume spanned. 262
II.2.3 Volume striped. 262
II.2.4 Volume mirrored. 263
II.2.5 Volume RAID-5. 264
III. SỬ DỤNG CHƯƠNG TRÌNH DISK MANAGER. 264
III.1. Xem thuộc tính của đĩa. 265
III.2. Xem thuộc tính của volume hoặc đĩa cục bộ. 265
III.2.1 Tab General. 266
III.2.2 Tab Tools. 266
III.2.3 Tab Hardware. 266
III.2.4 Tab Sharing. 267
III.2.5 Tab Security. 267
III.2.6 Tab Quota. 268
III.2.7 Shadow Copies. 268
III.3. Bổ sung thêm một ổ đĩa mới. 268
III.3.1 Máy tính không hỗ trợ tính năng “hot swap”. 268
III.3.2 Máy tính hỗ trợ “hot swap”. 269
III.4. Tạo partition/volume mới. 269
III.5. Thay đổi ký tự ổ đĩa hoặc đường dẫn. 272
III.6. Xoá partition/volume. 273
III.7. Cấu hình Dynamic Storage. 273
III.7.1 Chuyển chế độ lưu trữ. 273
III.7.2 Tạo Volume Spanned. 274
III.7.3 Tạo Volume Striped. 276
III.7.4 Tạo Volume Mirror. 277
III.7.5 Tạo Volume Raid-5. 277
IV. QUẢN LÝ VIỆC NÉN DỮ LIỆU. 278
V. THIẾT LẬP HẠN NGẠCH ĐĨA (DISK QUOTA). 279
V.1. Cấu hình hạn ngạch đĩa. 279
V.2. Thiết lập hạn ngạch mặc định. 280
V.3. Chỉ định hạn ngạch cho từng cá nhân. 281
VI. MÃ HOÁ DỮ LIỆU BẰNG EFS. 282
Bài 14 TẠO VÀ QUẢN LÝ THƯ MỤC DÙNG CHUNG 283
Tóm tắt 283
I. TẠO CÁC THƯ MỤC DÙNG CHUNG. 284



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

I.1. Chia sẻ thư mục dùng chung. .....284



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

I.2. Cấu hình Share Permissions. ....285
I.3. Chia sẻ thư mục dùng lệnh netshare. ....286
II. QUẢN LÝ CÁC THƯ MỤC DÙNG CHUNG. ....287
II.1. Xem các thư mục dùng chung. ....287
II.2. Xem các phiên làm việc trên thư mục dùng chung. ....287
II.3. Xem các tập tin đang mở trong các thư mục dùng chung. ....288
III. QUYỀN TRUY CẬP NTFS. ....288
III.1. Các quyền truy cập của NTFS. ....289
III.2. Các mức quyền truy cập được dùng trong NTFS. ....290
III.3. Gán quyền truy cập NTFS trên thư mục dùng chung. ....290
III.4. Kế thừa và thay thế quyền của đối tượng con. ....292
III.5. Thay đổi quyền khi di chuyển thư mục và tập tin. ....293
III.6. Giám sát người dùng truy cập thư mục. ....294
III.7. Thay đổi người sở hữu thư mục. ....294
IV. DFS. ....295
IV.1. So sánh hai loại DFS. ....295
IV.2. Cài đặt Fault-tolerant DFS. ....296
Bài 15 DỊCH VỤ DHCP ....300
Tóm tắt ....300
I. GIỚI THIỆU DỊCH VỤ DHCP. ....301
II. HOẠT ĐỘNG CỦA GIAO THỨC DHCP. ....301
III. CÀI ĐẶT DỊCH VỤ DHCP. ....301
IV. CHỨNG THỰC DỊCH VỤ DHCP TRONG ACTIVE DIRECTORY. ....303
V. CẤU HÌNH DỊCH VỤ DHCP. ....304
VI. CẤU HÌNH CÁC TUỲ CHỌN DHCP. ....308
VII. CẤU HÌNH DÀNH RIÊNG ĐỊA CHỈ. ....309
Bài 16 QUẢN LÝ IN ẤN ....311
Tóm tắt ....311
I. CÀI ĐẶT MÁY IN. ....312
II. QUẢN LÝ THUỘC TÍNH MÁY IN. ....313
II.1. Cấu hình Layout. ....313
II.2. Giấy và chất lượng in. ....313
II.3. Các thông số mở rộng. ....314
III. CẤU HÌNH CHIA SẺ MÁY IN. ....314
IV. CẤU HÌNH THÔNG SỐ PORT. ....316
IV.1. Cấu hình các thông số trong Tab Port. ....316
IV.2. Printer Pooling. ....317
IV.3. Điều hướng tác vụ in đến một máy in khác. ....318
V. CẤU HÌNH TAB ADVANCED. ....319
V.1. Các thông số của Tab Advanced. ....319
V.2. Khả năng sẵn sàng phục vụ của máy in. ....319
V.3. Độ ưu tiên (Printer Priority). ....320
V.4. Print Driver. ....320
V.5. Spooling. ....320
V.6. Print Options. ....320
V.7. Printing Defaults. ....321
V.8. Print Processor. ....321
V.9. Separator Pages. ....322
VI. CẤU HÌNH TAB SECURITY. ....323



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

VI.1. Giới thiệu Tab Security. .....323



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

VI.2. Cấp quyền in cho người dùng/nhóm người dùng. ....324
VII. CẤU HÌNH TAB DEVICES. ....325
VIII. QUẢN LÝ PRINT SERVER. ....325
VIII.1. Hộp thoại quản lý Print Server. ....325
VIII.2. Cấu hình các thuộc tính của biểu mẫu in. ....326
VIII.3. Cấu hình các thuộc tính Port của Print Server. ....327
VIII.4. Cấu hình Tab Driver. ....328
IX. GIÁM SÁT TRẠNG THÁI HÀNG ĐỢI MÁY IN. ....329
Bài 17 DỊCH VỤ TRUY CẬP TỪ XA ....332
Tóm tắt ....332
I. XÂY DỰNG MỘT REMOTE ACCESS SERVER. ....333
I.1. Cấu hình RAS server. ....333
I.2. Cấu hình RAS client. ....338
II. XÂY DỰNG MỘT INTERNET CONNECTION SERVER. ....340
II.1. Cấu hình trên server. ....340
II.2. Cấu hình trên máy trạm. ....344
Bài 18 DỊCH VỤ DNS ....346
Tóm tắt ....346
I. Tổng quan về DNS. ....347
I.1. Giới thiệu DNS. ....347
I.2. Đặt điểm của DNS trong Windows 2003. ....349
II. Cách phân bố dữ liệu quản lý domain name. ....350
III. Cơ chế phân giải tên. ....351
III.1. Phân giải tên thành IP. ....351
III.2. Phân giải IP thành tên máy tính. ....353
IV. Một số Khái niệm cơ bản. ....354
IV.1. Domain name và zone. ....354
IV.2. Fully Qualified Domain Name (FQDN). ....355
IV.3. Sự ủy quyền(Delegation). ....355
IV.4. Forwarders. ....355
IV.5. Stub zone. ....356
IV.6. Dynamic DNS. ....356
IV.7. Active Directory-integrated zone. ....357
V. Phân loại Domain Name Server. ....358
V.1. Primary Name Server. ....358
V.2. Secondary Name Server. ....358
V.3. Caching Name Server. ....359
VI. Resource Record (RR). ....359
VI.1. SOA(Start of Authority). ....360
VI.2. NS (Name Server). ....361
VI.3. A (Address) và CNAME (Canonical Name). ....361
VI.4. AAAA. ....361
VI.5. SRV. ....362
VI.6. MX (Mail Exchange). ....362
VI.7. PTR (Pointer). ....363
VII. Cài đặt và cấu hình dịch vụ DNS. ....363
VII.1.Các bước cài đặt dịch vụ DNS. ....363
VII.2.Cấu hình dịch vụ DNS ....364



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

VII.2.1 Tạo Forward Lookup Zones. ..... 365



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

VII.2.2 Tạo Reverse Lookup Zone. 366
VII.2.3 Tạo Resource Record(RR). 367
VII.2.4 Kiểm tra hoạt động dịch vụ DNS. 370
VII.2.5 Tạo miền con(Subdomain). 374
VII.2.6 Ủy quyền cho miền con. 375
VII.2.7 Tạo Secondary Zone. 376
VII.2.8 Tạo zone tích hợp với Active Directory. 378
VII.2.9 Thay đổi một số tùy chọn trên Name Server. 380
VII.2.10 Theo dõi sự kiện log trong DNS. 384
Bài 19 DỊCH VỤ FTP 385
Tóm tắt 385
I. Giới thiệu về FTP. 386
I.1. Giao thức FTP. 386
I.1.1 Active FTP. 386
I.1.2 Passive FTP. 387
I.1.3 Một số lưu ý khi truyền dữ liệu qua FTP. 389
I.1.4 Cô lập người dùng truy xuất FTP Server (FTP User Isolation). 389
II. Chương trình FTP client. 390
III. Giới thiệu FTP Server. 392
III.1. Cài đặt dịch vụ FTP. 392
III.2. Cấu hình dịch vụ FTP. 393
III.2.1 Tạo mới FTP site. 394
III.2.2 Tạo và xóa FTP Site bằng dòng lệnh. 395
III.2.3 Theo dõi các user login vào FTP Server. 396
III.2.4 Điều khiển truy xuất đến FTP Site. 396
III.2.5 Tạo Virtual Directory. 398
III.2.6 Tạo nhiều FTP Site. 399
III.2.7 Cấu hình FTP User Isolate. 400
III.2.8 Theo dõi và cấu hình nhật ký cho FTP. 402
III.2.9 Khởi động và tắt dịch vụ FTP. 404
III.2.10 Lưu trữ và phục hồi thông tin cấu hình. 404
Bài 20 DỊCH VỤ WEB 406
Tóm tắt 406
I. Giao thức HTTP 407
II. Nguyên tắc hoạt động của Web Server. 407
II.1. Cơ chế nhận kết nối. 408
II.2. Web Client. 408
II.3. Web động. 409
III. Đặc điểm của IIS 6.0. 409
III.1. Các thành phần chính trong IIS. 409
III.2. IIS Isolation mode. 410
III.3. Chế độ Worker process isolation. 410
III.3.1 IIS 5.0 Isolation Mode. 411
III.3.2 So sánh các chức năng trong IIS 6.0 mode. 411
III.4. Nâng cao tính năng bảo mật. 412



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

III.5. Hỗ trợ ứng dụng và các công cụ quản trị.....413



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

IV. Cài đặt và cấu hình IIS 6.0. ..... 414
IV.1. Cài đặt IIS 6.0 Web Service. ..... 414
IV.2. Cấu hình IIS 6.0 Web service. ..... 417
IV.2.1 Một số thuộc tính cơ bản. ..... 418
IV.2.2 Tạo mới một Web site. ..... 420
IV.2.3 Tạo Virtual Directory. ..... 422
IV.2.4 Cấu hình bảo mật cho Web Site. ..... 423
IV.2.5 Cấu hình Web Service Extensions. ..... 425
IV.2.6 Cấu hình Web Hosting. ..... 426
IV.2.7 Cấu hình IIS qua mạng (Web Interface for Remote Administration). ..... 428
IV.2.8 Quản lý Web site bằng dòng lệnh. ..... 430
IV.2.9 Sao lưu và phục hồi cấu hình Web Site. ..... 431
IV.2.10 Cấu hình Forum cho Web Site. ..... 432
Bài 21 DỊCH VỤ MAIL ..... 435
Tóm tắt ..... 435
I. Các giao thức được sử dụng trong hệ thống Mail. ..... 436
I.1. SMTP(Simple Mail Transfer Protocol). ..... 436
I.2. Post Office Protocol. ..... 438
I.3. Internet Message Access Protocol. ..... 439
I.4. MIME. ..... 439
I.5. X.400. ..... 439
II. Giới thiệu về hệ thống mail. ..... 440
II.1. Mail gateway. ..... 440
II.2. Mail Host. ..... 440
II.3. Mail Server. ..... 440
II.4. Mail Client. ..... 441
II.5. Một số sơ đồ hệ thống mail thường dùng. ..... 441
II.5.1 Hệ thống mail cục bộ. ..... 441
II.5.2 Hệ thống mail cục bộ có kết nối ra ngoài. ..... 441
II.5.3 Hệ thống hai domain và một gateway. ..... 442
III. Một số khái niệm. ..... 442
III.1. Mail User Agent (MUA). ..... 442
III.2. Mail Transfer Agent (MTA). ..... 442
III.3. Mailbox. ..... 443
III.4. Hàng đợi mail (mail queue). ..... 443
III.5. Alias mail. ..... 443
IV. Mối liên hệ giữa DNS và Mail Server. ..... 443
V. Giới thiệu các chương trình Mail Server. ..... 444
VI. Cài đặt Exchange 2003 Server. ..... 444
VI.1. Một số phiên bản chính của Exchange. ..... 444
VI.2. Yêu cầu cài đặt. ..... 444
VI.3. Kiểm tra Active directory. ..... 445
VI.4. Cài đặt Microsoft Exchange 2003 Server. ..... 445
VII. Cấu hình Microsoft Exchange 2003. ..... 447
VII.1.Khởi động các dịch vụ trong Exchange 2003. ..... 447
VII.2.Quản lý tài khoản mail. ..... 448



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

VII.2.1 Tạo tài khoản mail. ..... 448



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

VII.2.2 Truy cập thuộc tính của tài khoản mail. 449
VII.2.3 Một số tác vụ về tài khoản. 453
VII.3. Administrative và routing group. 454
VII.3.1 Administrative group. 454
VII.3.2 Routing group. 455
VII.4. Microsoft Outlook Web Access. 457
VII.4.1 Kiến trúc của OWA. 457
VII.4.2 Thư mục lưu trữ và Virtual Directory của OWA. 458
VII.4.3 Quản trị OWA. 458
VII.4.4 Sử dụng OWA. 459
VII.5. Thiết lập một số luật phân phối message. 461
VII.5.1 Thiết lập bộ lọc thư. 461
VII.5.2 Sử dụng mail thông qua điện thoại di động. 463
VII.5.3 Relay mail. 463
VII.5.4 Chỉ định smart host. 465
VII.5.5 Định kích thước của message. 466
VII.6. Public Folder. 466
VII.6.1 Các thành phần trong Public Folders. 466
VII.6.2 Quản lý Public Folder. 467
VII.7. Một số thao tác quản lý Exchange server. 469
VII.7.1 Lập chính sách nhận thư. 469
VII.7.2 Quản lý Storage group. 472
VIII. Một số tiện ích cần thiết của Exchange Server. 473
VIII.1. GFI MailEssentials. 473
VIII.2. GFI MailSecurity. 474
Bài 22 DỊCH VỤ PROXY 476
Tóm tắt 476
I. Firewall. 477
I.1. Giới thiệu về Firewall. 477
I.2. Kiến Trúc Của Firewall. 477
I.2.1 Kiến trúc Dual-homed host. 477
I.2.2 Kiến trúc Screened Host. 478
I.2.3 Sreened Subnet. 479
I.3. Các loại firewall và cách hoạt động. 480
I.3.1 Packet filtering (Bộ lọc gói tin). 480
I.3.2 Application gateway. 480
II. Giới Thiệu ISA 2004. 482
III. Đặc Điểm Của ISA 2004. 482
IV. Cài Đặt ISA 2004. 483
IV.1. Yêu cầu cài đặt. 483
IV.2. Quá trình cài đặt ISA 2004. 483
IV.2.1 Cài đặt ISA trên máy chủ 1 card mạng. 483
IV.2.2 Cài đặt ISA trên máy chủ có nhiều card mạng. 484
V. Cấu hình ISA Server. 487
V.1. Một số thông tin cấu hình mặc định. 487



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

V.2. Một số chính sách mặc định của hệ thống.....488



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

V.3. Cấu hình Web proxy cho ISA. 493
V.4. Tạo Và Sử Dụng Firewall Access Policy. 496
V.4.1 Tạo một Access Rule. 496
V.4.2 Thay đổi thuộc tính của Access Rule. 498
V.5. Publishing Network Services. 499
V.5.1 Web Publishing and Server Publishing. 499
V.5.2 Publish Web server. 500
V.5.3 Publish Mail Server. 502
V.5.4 Tạo luật để publish Server. 504
V.6. Kiểm tra trạng thái và bộ lọc ứng dụng. 506
V.6.1 Lập bộ lọc ứng dụng. 506
V.6.2 Thiết lập bộ lọc Web. 508
V.6.3 Phát Hiện Và Ngăn Ngừa Tấn Công. 510
V.7. Một số công cụ bảo mật. 512
V.7.1 Download Security. 512
V.7.2 Surfcontrol Web Filter. 514
V.8. Thiết lập Network Rule. 515
V.8.1 Thay đổi thuộc tính của một Network Rule. 515
V.8.2 Tạo Network Rule. 515
V.9. Thiết lập Cache, quản lý và theo dõi traffic. 516
V.9.1 Thiết lập Cache. 516
V.9.2 Thay đổi tùy chọn về vùng Cache. 517
V.9.3 Tạo Cache Rule. 517
V.9.4 Quản lý và theo dõi traffic. 520
Bài 23 PHỤ LỤC 524
Tóm tắt 524
QUẢN TRỊ MAIL SERVER- MDAEMON 525
I. Cài Đặt Mdaemon. 525
II. Cấu hình Mail Server. 526
II.1. Cấu hình Domain/ISP. 527
II.2. Cấu hình Ports. 527
III. Cấu hình lịch kết nối và dịch vụ quay số. 528
III.1. Lập lịch kết nối. 528
III.2. Cấu hình Quay số. 529
III.2.1 Dialup Settings. 529
III.2.2 ISP Logon Settings. 530
III.2.3 LAN Domains. 530
IV. Cấu hình DomainPOP Mail. 531
V. WorldClient Server. 532
V.1. Cách Cấu Hình WorldClient server. 532
V.2. Sử dụng WorldClient. 534
VI. Quản trị người dùng. 535
VI.1. Tạo và thay đổi thuộc tính người dùng. 535
VI.1.1 Thông tin của Account. 536
VI.1.2 Thông tin của Mailbox. 536



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

VI.1.3 Forwarding. ..... 537



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

VI.1.4 Thiết lập hạn ngạch cho mailbox. 537
VI.1.5 Webmail cho tài khoản. 538
VI.1.6 MultiPOP. 539
VI.2. Tạo bí danh cho tài khoản. 540
VI.3. Tạo Mailing List cho tài khoản. 541
QUẢN TRỊ PROXY SERVER – WINGATE 542
Giới thiệu WinGate Proxy. 542
I. Cài đặt Wingate. 542
I.1. Yêu cầu phần cứng. 542
I.2. Cài đặt Wingate proxy. 542
I.3. Khởi động/tạm ngưng WinGate. 544
II. Cấu hình Wingate. 544
II.1. Khảo sát các thông tin chung. 544
III. Cấu Hình Các Dịch Vụ Hệ Thống. 547
III.1. Cấu hình Caching. 547
III.2. Extended Network Support (ENS): 549
III.3. Cấu hình các dịch vụ proxy. 551
III.3.1 Cấu hình FTP Proxy. 551
III.3.2 Cấu Hình Dịch Vụ WWW Proxy. 553



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

# GIỚI THIỆU

Sau khi hoàn tất khoá học, học viên có khả năng:

- Hiểu được các khái niệm, lý thuyết về mạng máy tính như: **OSI, TCP/IP**.
- Hiểu được các chức năng và mô hình hoạt động của các thiết bị mạng như: Hub, Switch, Router, Modem, Network Card…
- Sử dụng được các tiện ích mạng thông dụng như: web, mail, ftp…
- Cài đặt và quản trị hệ điều hành **Windows Server 2003**.
- Tổ chức và quản lý người dùng trên môi trường **Windows Server 2003**.
- Tổ chức phân quyền NTFS và quản lý tài nguyên dùng chung trên mạng như: thư mục, máy in, tập tin…
- Quản lý đĩa theo công nghệ **Dynamic Storage**.
- Xây dựng được hệ thống mạng kết nối từ xa (**Remote Access Services**).
- Xây dựng và quản trị được các dịch vụ cơ sở như: DNS, FTP, Web, Mail...
- Chia sẻ kết nối internet thông qua các kỹ thuật như: ICS, NAT, Proxy trên môi trường Windows Server 2003.
- Bảo mật hệ thống mạng thông qua phần mềm ISA 2004.

Với thời lượng 108 tiết LT và 180 tiết TH được phân bổ như sau :

| STT | Bài học | Số tiết LT | Số tiết TH |
|---|---|---|---|
| 1 | Giới thiệu về mạng | 4 | 5 |
| 2 | Mô hình tham chiếu OSI | 4 | 0 |
| 3 | Địa chỉ IP | 5 | 5 |
| 4 | Phương tiện truyền dẫn và các thiết bị mạng | 6 | 10 |
| 5 | Các kiến trúc và công nghệ mạng LAN | 5 | 10 |
| 6 | Khảo sát các lớp trong mô hình OSI | 6 | 10 |
| 7 | Các dịch vụ mạng cơ sở | 6 | 20 |
| 8 | Giới thiệu và cài đặt Windows Server 2003 | 4 | 3 |
| 9 | Active Directory | 4 | 8 |
| 10 | Quản lý tài khoản người dùng và nhóm | 4 | 10 |
| 11 | Chính sách hệ thống | 5 | 6 |
| 12 | Chính sách nhóm | 3 | 3 |



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

| | | | |
|---|---|---|---|
| 13 | Quản lý đĩa | 3 | 5 |
| 14 | Tạo và quản lý thư mục dùng chung | 4 | 10 |
| 15 | Dịch vụ DHCP | 2 | 3 |
| 16 | Quản lý in ấn | 2 | 2 |
| 17 | Dịch vụ truy cập từ xa | 5 | 10 |
| 18 | Dịch vụ DNS | 6 | 12 |
| 19 | Dịch vụ FTP | 3 | 6 |
| 20 | Dịch vụ WEB | 5 | 10 |
| 21 | Dịch vụ MAIL | 8 | 16 |
| 22 | Dịch vụ Proxy | 8 | 16 |
| 23 | Giới thiệu về hai phần mềm Mdaemon và Wingate | 6 | 0 |
| | Tổng số tiết : | 108 | 180 |



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

# GIÁO TRÌNH LÝ THUYẾT

Sử dụng giáo trình **Mạng Máy Tính** của tác giả Trần Văn Thành, tái bản lần thứ 2, nhà xuất bản Đại Học Quốc Gia Tp.HCM.

Sử dụng giáo trình **Quản trị Windows Server 2003** của tác giả Trần Văn Thành, tái bản lần thứ 2, nhà xuất bản Đại Học Quốc Gia Tp.HCM.

Sử dụng giáo trình **Dịch Vụ Mạng Windows 2003** của tác giả Tiêu Đông Nhơn tái bản lần thứ 2, nhà xuất bản Đại Học Quốc Gia Tp.HCM.

# TÀI LIỆU THAM KHẢO

Giáo Trình **Windows Server 2003** của Sybex.

Các giáo trình MCSE của Microsoft.

Các tài liệu trên website http://support.microsoft.com/winsrv2003



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

# Bài 1
# GIỚI THIỆU VỀ MẠNG

## Tóm tắt

Lý thuyết 4 tiết - Thực hành 5 tiết

| Mục tiêu | Các mục chính | Bài tập bắt buộc | Bài tập làm thêm |
|---|---|---|---|
| Kết thúc bài học này cung cấp học viên kiến thức tổng quát về mạng máy tính, các loại mạng, các mô hình xử lý mạng… | I. Các kiến thức cơ sở.<br>II. Các loại mạng máy tính.<br>III. Các mô hình xử lý mạng.<br>IV. Các mô hình ứng dụng mạng.<br>V. Các lợi ích thực tế của mạng | Dựa vào bài tập môn mạng máy tính. | Dựa vào bài tập môn mạng máy tính. |



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

# Bài 1
# GIỚI THIỆU VỀ MẠNG

## I. CÁC KIẾN THỨC CƠ SỞ

Mạng máy tính là một nhóm các máy tính, thiết bị ngoại vi được nối kết với nhau thông qua các phương tiện truyền dẫn như cáp, sóng điện từ, tia hồng ngoại... giúp cho các thiết bị này có thể trao đổi dữ liệu với nhau một cách dễ dàng.

Các thành phần cơ bản cấu thành nên mạng máy tính:

- Các loại máy tính: **Palm, Laptop, PC, MainFrame**...
- Các thiết bị giao tiếp: Card mạng (**NIC** hay **Adapter**), **Hub, Switch, Router**...
- Môi trường truyền dẫn: cáp, sóng điện từ, sóng vi ba, tia hồng ngoại...
- Các protocol: **TCP/IP, NetBeui, Apple Talk, IPX/SPX...**
- Các hệ điều hành mạng: **WinNT, Win2000, Win2003, Novell Netware, Unix...**
- Các tài nguyên: file, thư mục
- Các thiết bị ngoại vi: máy in, máy fax, **Modem**, **Scanner**...
- Các ứng dụng mạng: phần mềm quản lý kho bãi, phần mềm bán vé tàu...

**Server** (máy phục vụ): là máy tính được cài đặt các phần mềm chuyên dụng làm chức năng cung cấp các dịch vụ cho các máy tính khác. Tùy theo dịch vụ mà các máy này cung cấp, người ta chia thành các loại **server** như sau: **File server** (cung cấp các dịch vụ về file và thư mục), **Print server** (cung cấp các dịch vụ về in ấn). Do làm chức năng phục vụ cho các máy tính khác nên cấu hình máy server phải mạnh, thông thường là máy chuyên dụng của các hãng như: Compaq, Intel, IBM...

**Client** (máy trạm): là máy tính sử dụng các dịch vụ mà các máy server cung cấp. Do xử lý số công việc không lớn nên thông thường các máy này không yêu cầu có cấu hình mạnh.

**Peer**: là những máy tính vừa đóng vai trò là máy sử dụng vừa là máy cung cấp các dịch vụ. Máy peer thường sử dụng các hệ điều hành như: **DOS, WinNT Workstation, Win9X, Win Me, Win2K Professional, WinXP...**

**Media** (phương tiện truyền dẫn): là cách thức và vật liệu nối kết các máy lại với nhau.

**Shared data** (dữ liệu dùng chung): là tập hợp các tập tin, thư mục mà các máy tính chia sẻ để các máy tính khác truy cập sử dụng chúng thông qua mạng.

**Resource** (tài nguyên): là tập tin, thư mục, máy in, máy Fax, Modem, ổ CDROM và các thành phần khác mà người dùng mạng sử dụng.

**User** (người dùng): là người sử dụng máy trạm (**client**) để truy xuất các tài nguyên mạng. Thông thường một user sẽ có một username (**account**) và một password. Hệ thống mạng sẽ dựa vào username và password để biết bạn là ai, có quyền vào mạng hay không và có quyền sử dụng những tài nguyên nào trên mạng.

**Administrator**: là nhà quản trị hệ thống mạng.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

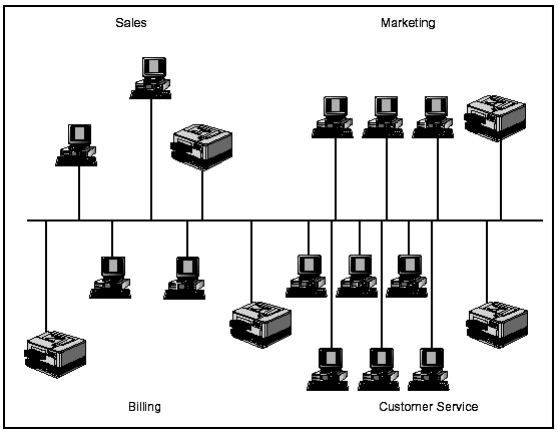
# II. CÁC LOẠI MẠNG MÁY TÍNH

## II.1. Mạng cục bộ LAN (Local Area Network)

Mạng LAN là một nhóm máy tính và các thiết bị truyền thông mạng được nối kết với nhau trong một khu vực nhỏ như một toà nhà cao ốc, khuôn viên trường đại học, khu giải trí ...

Các mạng LAN thường có đặc điểm sau:

- Băng thông lớn, có khả năng chạy các ứng dụng trực tuyến như xem phim, hội thảo qua mạng.
- Kích thước mạng bị giới hạn bởi các thiết bị.
- Chi phí các thiết bị mạng LAN tương đối rẻ.
- Quản trị đơn giản.




Hình 1.1 – Mô hình mạng cục bộ (LAN)

## II.2. Mạng đô thị MAN (Metropolitan Area Network)

Mạng MAN gần giống như mạng LAN nhưng giới hạn của nó là một thành phố hay một quốc gia. Mạng MAN nối kết các mạng LAN lại với nhau thông qua các phương tiện truyền dẫn khác nhau (cáp quang, cáp đồng, sóng...) và các phương thức truyền thông khác nhau.

Đặc điểm của mạng MAN:

- Băng thông mức trung bình, đủ để phục vụ các ứng dụng cấp thành phố hay quốc gia như chính phủ điện tử, thương mại điện tử, các ứng dụng của các ngân hàng...
- Do MAN nối kết nhiều LAN với nhau nên độ phức tạp cũng tăng đồng thời công tác quản trị sẽ khó khăn hơn.
- Chi phí các thiết bị mạng MAN tương đối đắt tiền.

## II.3. Mạng diện rộng WAN (Wide Area Network)

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 mạng của các công ty đa quốc gia hay toàn cầu, điển hình là mạng Internet. Do phạm vi rộng lớn của mạng WAN nên thông thường mạng WAN là tập hợp các mạng LAN, MAN nối lại với nhau bằng các phương tiện như: vệ tinh (**satellites**), sóng viba (**microwave**), cáp quang, cáp điện



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

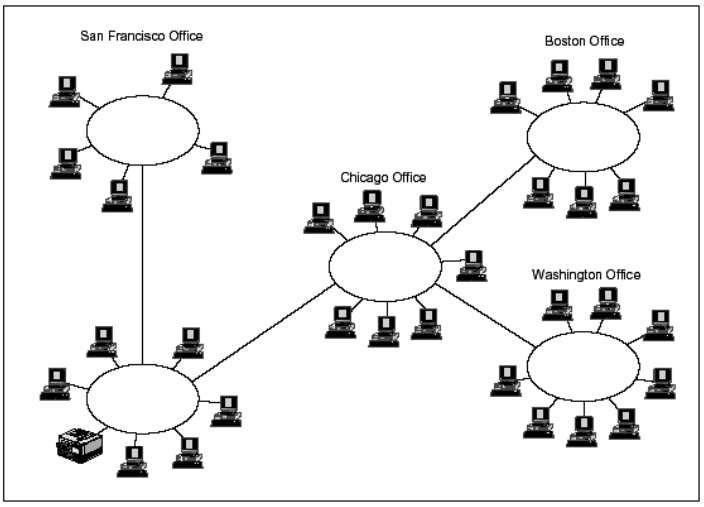
thoại...



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Đặc điểm của mạng WAN:

- Băng thông thấp, dễ mất kết nối, thường chỉ phù hợp với các ứng dụng offline như e-mail, web, ftp ...
- Phạm vi hoạt động rộng lớn không giới hạn.
- Do kết nối của nhiều LAN, MAN lại với nhau nên mạng rất phức tạp và có tính toàn cầu nên thường là có tổ chức quốc tế đứng ra quản trị.
- Chi phí cho các thiết bị và các công nghệ mạng WAN rất đắt tiền.




Hình 1.2 – Mô hình mạng diện rộng (WAN)

## II.4. Mạng Internet

Mạng Internet là trường hợp đặc biệt của mạng WAN, nó cung cấp các dịch vụ toàn cầu như mail, web, chat, ftp và phục vụ miễn phí cho mọi người.

# III. CÁC MÔ HÌNH XỬ LÝ MẠNG

Cơ bản có ba loại mô hình xử lý mạng bao gồm:

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

## III.1. Mô hình xử lý mạng tập trung

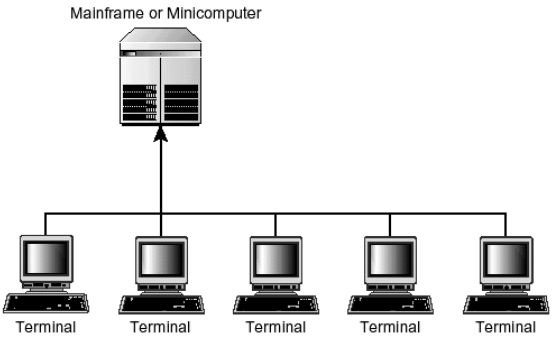
Toàn bộ các tiến trình xử lý diễn ra tại máy tính trung tâm. Các máy trạm cuối (**terminals**) được nối mạng với máy tính trung tâm và chỉ hoạt động như những thiết bị nhập xuất dữ liệu cho phép người dùng xem trên màn hình và nhập liệu bàn phím. Các máy trạm đầu cuối không lưu trữ và xử lý dữ liệu. Mô hình xử lý mạng trên có thể triển khai trên hệ thống phần cứng hoặc phần mềm được cài đặt trên server.



Ưu điểm: dữ liệu được bảo mật an toàn, dễ backup và diệt virus. Chi phí cho các thiết bị thấp.

Khuyết điểm: khó đáp ứng được các yêu cầu của nhiều ứng dụng khác nhau, tốc độ truy xuất chậm.

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net



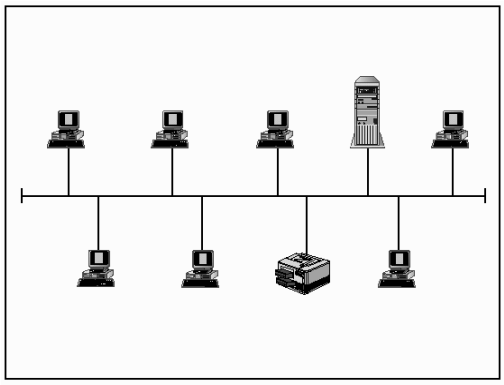

Hình 1.3 – Mô hình xử lý mạng tập trung

## III.2. Mô hình xử lý mạng phân phối

Các máy tính có khả năng hoạt động độc lập, các công việc được tách nhỏ và giao cho nhiều máy tính khác nhau thay vì tập trung xử lý trên máy trung tâm. Tuy dữ liệu được xử lý và lưu trữ tại máy cục bộ nhưng các máy tính này được nối mạng với nhau nên chúng có thể trao đổi dữ liệu và dịch vụ.

Ưu điểm: truy xuất nhanh, phần lớn không giới hạn các ứng dụng.

Khuyết điểm: dữ liệu lưu trữ rời rạc khó đồng bộ, backup và rất dễ nhiễm virus.



Hình 1.4 – Mô hình xử lý mạng phân phối

## III.3. Mô hình xử lý mạng cộng tác.

Mô hình xử lý cộng tác bao gồm nhiều máy tính có thể hợp tác để thực hiện một công việc. Một máy tính có thể mượn năng lực xử lý bằng cách chạy các chương trình trên các máy nằm trong mạng.

Ưu điểm: rất nhanh và mạnh, có thể dùng để chạy các ứng dụng có các phép toán lớn.

Khuyết điểm: các dữ liệu được lưu trữ trên các vị trí khác nhau nên rất khó đồng bộ và backup, khả năng nhiễm virus rất cao.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

# IV. CÁC MÔ HÌNH QUẢN LÝ MẠNG

## IV.1. Workgroup

Trong mô hình này các máy tính có quyền hạn ngang nhau và không có các máy tính chuyên dụng làm nhiệm vụ cung cấp dịch vụ hay quản lý. Các máy tính tự bảo mật và quản lý các tài nguyên của riêng mình. Đồng thời các máy tính cục bộ này cũng tự chứng thực cho người dùng cục bộ.

## IV.2. Domain

Ngược lại với mô hình Workgroup, trong mô hình Domain thì việc quản lý và chứng thực người dùng mạng tập trung tại máy tính **Primary Domain Controller**. Các tài nguyên mạng cũng được quản lý tập trung và cấp quyền hạn cho từng người dùng. Lúc đó trong hệ thống có các máy tính chuyên dụng làm nhiệm vụ cung cấp các dịch vụ và quản lý các máy trạm.

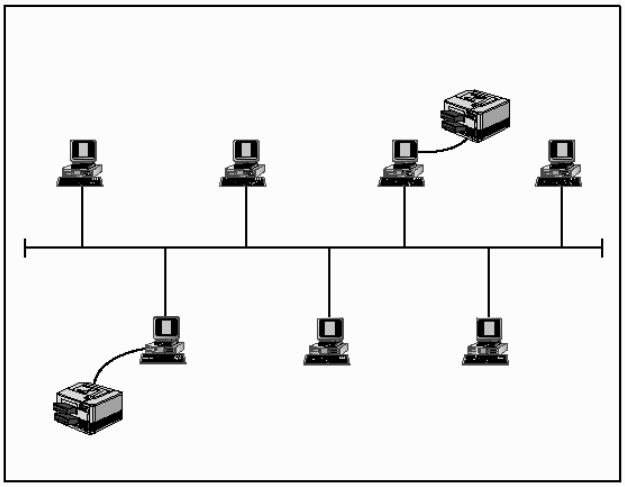
# V. CÁC MÔ HÌNH ỨNG DỤNG MẠNG

## V.1. Mạng ngang hàng (peer to peer)

Mạng ngang hàng cung cấp việc kết nối cơ bản giữa các máy tính nhưng không có bất kỳ một máy tính nào đóng vai trò phục vụ. Một máy tính trên mạng có thể vừa là **client**, vừa là **server**. Trong môi trường này, người dùng trên từng máy tính chịu trách nhiệm điều hành và chia sẻ các tài nguyên của máy tính mình. Mô hình này chỉ phù hợp với các tổ chức nhỏ, số người giới hạn (thông thường nhỏ hơn 10 người), và không quan tâm đến vấn đề bảo mật. Mạng ngang hàng thường dùng các hệ điều hành sau: **Win95, Windows for workgroup, WinNT Workstation, Win2000 Proffessional, OS/2...**

Ưu điểm: do mô hình mạng ngang hàng đơn giản nên dễ cài đặt, tổ chức và quản trị, chi phí thiết bị cho mô hình này thấp.

Khuyết điểm: không cho phép quản lý tập trung nên dữ liệu phân tán, khả năng bảo mật thấp, rất dễ bị xâm nhập. Các tài nguyên không được sắp xếp nên rất khó định vị và tìm kiếm.



Hình 1.5 – Mô hình ứng dụng mạng ngang hàng (**Peer-to-Peer**)



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

## V.2. Mạng khách chủ (client- server)

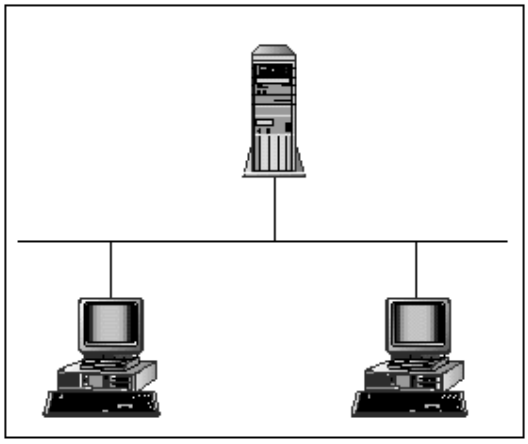
Trong mô hình mạng khách chủ có một hệ thống máy tính cung cấp các tài nguyên và dịch vụ cho cả hệ thống mạng sử dụng gọi là các máy chủ (**server**). Một hệ thống máy tính sử dụng các tài nguyên và dịch vụ này được gọi là máy khách (**client**). Các server thường có cấu hình mạnh (tốc độ xử lý nhanh, kích thước lưu trữ lớn) hoặc là các máy chuyên dụng. Dựa vào chức năng có thể chia thành các loại server như sau:

- **File Server**: phục vụ các yêu cầu hệ thống tập tin trong mạng.
- **Print Server**: phục vụ các yêu cầu in ấn trong mạng.
- **Application Server**: cho phép các ứng dụng chạy trên các server và trả về kết quả cho client.
- **Mail Server**: cung cấp các dịch vụ về gởi nhận e-mail.
- **Web Server**: cung cấp các dịch vụ về web.
- **Database Server**: cung cấp các dịch vụ về lưu trữ, tìm kiếm thông tin.
- **Communication Server**: quản lý các kết nối từ xa.

Hệ điều hành mạng dùng trong mô hình client - server là **WinNT, Novell NetWare, Unix, Win2K...**

Ưu điểm: do các dữ liệu được lưu trữ tập trung nên dễ bảo mật, backup và đồng bộ với nhau. Tài nguyên và dịch vụ được tập trung nên dễ chia sẻ và quản lý và có thể phục vụ cho nhiều người dùng.

Khuyết điểm: các server chuyên dụng rất đắt tiền, phải có nhà quản trị cho hệ thống.



Hình 1.6 – Mô hình ứng dụng mạng khách chủ (**Client-Server**)

# VI. CÁC DỊCH VỤ MẠNG

Các dịch vụ mạng phổ biến nhất là:

- Dịch vụ tập tin.
- Dịch vụ in ấn.
- Dịch vụ thông điệp.
- Dịch vụ thư mục.
- Dịch vụ ứng dụng.
- Dịch vụ cơ sở dữ liệu.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

- Dịch vụ Web.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

## VI.1. Dịch vụ tập tin (Files Services)

Dịch vụ tập tin cho phép các máy tính chia sẻ các tập tin, thao tác trên các tập tin chia sẻ này như: lưu trữ, tìm kiếm, di chuyển...

Truyền tập tin: không có mạng, các khả năng truyền tải tập tin giữa các máy tính bị hạn chế. Ví dụ như chúng ta muốn sao chép một tập tin từ máy tính cục bộ ở Việt Nam sang một máy tính server đặt tại Pháp thì chúng ta dùng dịch vụ FTP để sao chép. Dịch vụ này rất phổ biến và đơn giản.

Lưu trữ tập tin: phần lớn các dữ liệu quan trọng trên mạng đều được lưu trữ tập trung theo nhiều cách khác nhau:

Lưu trữ trực tuyến (**online storage**): dữ liệu được lưu trữ trên đĩa cứng nên truy xuất dễ dàng, nhanh chóng, bất kể thời gian. Nhưng phương pháp này có một khuyết điểm là chúng không thể tháo rời để trao đổi hoặc lưu trữ tách rời, đồng thời chi phí lưu trữ một MB dữ liệu tương đối cao.

Lưu trữ ngoại tuyến (**offline storage**): thường áp dụng cho dữ liệu ít khi cần truy xuất (lưu trữ, backup). Các thiết bị phổ biến dùng cho phương pháp này là băng từ, đĩa quang.

Lưu trữ cận tuyến (**near- line storage**): phương pháp này giúp ta khắc phục được tình trạng truy xuất chậm của phương pháp lưu trữ ngoại tuyến nhưng chi phí lại không cao đó là chúng ta dùng thiết bị **Jukebox** để tự động quản lý các băng từ và đĩa quang.

Di trú dữ liệu (**data migration**) là công nghệ tự động dời các dữ liệu ít dùng từ kho lưu trữ trực tuyến sang kho lưu trữ cận tuyến hay ngoại tuyến. Nói cách khác đây là quá trình chuyển các tập tin từ dạng lưu trữ này sang dạng lưu trữ khác.

Đồng bộ hóa việc cập nhật tập tin: dịch vụ này theo dõi các thay đổi khác nhau lên cùng một tập tin để đảm bảo rằng tất cả mọi người dùng đều có bản sao mới nhất của tập tin và tập tin không bị hỏng.

Sao lưu dự phòng (**backup**) là quá trình sao chép và lưu trữ một bản sao dữ liệu từ thiết bị lưu trữ chính. Khi thiết bị lưu trữ chính có sự cố thì chúng ta dùng bản sao này để phục hồi dữ liệu.

## VI.2. Dịch vụ in ấn (Print Services)

Dịch vụ in ấn là một ứng dụng mạng điều khiển và quản lý việc truy cập các máy in, máy fax mạng. Các lợi ích của dịch vụ in ấn:

Giảm chi phí cho nhiều người có thể chia nhau dùng chung các thiết bị đắt tiền như máy in màu, máy vẽ, máy in khổ giấy lớn.

Tăng độ linh hoạt vì các máy tính có thể đặt bất kỳ nơi nào, chứ không chỉ đặt cạnh PC của người dùng.

Dùng cơ chế hàng đợi in để ấn định mức độ ưu tiên nội dung nào được in trước, nội dung nào được in sau.

## VI.3. Dịch vụ thông điệp (Message Services)

Là dịch vụ cho phép gởi/nhận các thư điện tử (**e-mail**). Công nghệ thư điện tử này rẻ tiền, nhanh chóng, phong phú cho phép đính kèm nhiều loại file khác nhau như: phim ảnh, âm thanh... Ngoài ra dịch vụ này còn cung cấp các ứng dụng khác như: thư thoại (**voice mail**), các ứng dụng nhóm làm việc (**workgroup application**).



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

## VI.4. Dịch vụ thư mục (Directory Services)

Dịch vụ này cho phép tích hợp mọi thông tin về các đối tượng trên mạng thành một cấu trúc thư mục dùng chung nhờ đó mà quá trình quản lý và chia sẻ tài nguyên trở nên hiệu quả hơn.

## VI.5. Dịch vụ ứng dụng (Application Services)

Dịch vụ này cung cấp kết quả cho các chương trình ở **client** bằng cách thực hiện các chương trình trên **server**. Dịch vụ này cho phép các ứng dụng huy động năng lực của các máy tính chuyên dụng khác trên mạng.

## VI.6. Dịch vụ cơ sở dữ liệu (Database Services)

Dịch vụ cơ sở dữ liệu thực hiện các chức năng sau:

- Bảo mật cơ sở dữ liệu.
- Tối ưu hóa tiến trình thực hiện các tác vụ cơ sở dữ liệu.
- Phục vụ số lượng người dùng lớn, truy cập nhanh vào các cơ sở dữ liệu.
- Phân phối dữ liệu qua nhiều hệ phục vụ CSDL.

## VI.7. Dịch vụ Web

Dịch vụ này cho phép tất cả mọi người trên mạng có thể trao đổi các siêu văn bản với nhau. Các siêu bản này có thể chứa hình ảnh, âm thanh giúp các người dùng có thể trao đổi nhanh thông tin và sống động hơn.

# VII. CÁC LỢI ÍCH THỰC TẾ CỦA MẠNG.

## VII.1. Tiết kiệm được tài nguyên phần cứng.

Khi các máy tính của một phòng ban được nối mạng với nhau thì chúng ta có thể chia sẻ những thiết bị ngoại vi như máy in, máy FAX, ổ đĩa CDROM... Thay vì trang bị cho từng máy PC thì thông qua mạng chúng ta có thể dùng chung các thiết bị này.

Ví dụ 1: trong một phòng máy thực hành có khoảng 30 máy, nếu trang bị cho tất cả các máy trạm có đĩa cứng thì rất phí mà chúng ta lại không tận dụng được hết năng suất của các đĩa cứng đó. Giải pháp tập trung tất cả các ứng dụng vào server và dùng công nghệ mạng bootrom để chạy các máy trạm sẽ làm giảm chi phí phần cứng đồng thời tiện dụng cho công tác quản trị phòng máy hạn chế được tình trạng các học viên vô tình làm hỏng các máy trạm.

Ví dụ 2: Một công ty muốn rằng tất cả các phòng ban đều được sử dụng Internet thông qua modem và đường điện thoại. Nếu chúng ta trang bị cho mỗi phòng ban 1 modem và 1 đường điện thoại thì không khả thi vì vậy chúng ta phải tận dụng cơ sở hạ tầng mạng để chia sẻ 1 modem và đường điện thoại cho cả công ty đều có thể truy cập Internet.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

## VII.2. Trao đổi dữ liệu trở nên dễ dàng hơn.

Theo phương pháp truyền thống muốn chép dữ liệu giữa hai máy tính chúng ta dùng đĩa mềm hoặc dùng cáp **link** để nối hai máy lại với nhau sau đó chép dữ liệu. Chúng ta thấy rằng hai giải pháp trên sẽ không thực tế nếu một máy đặt tại tầng trệt và một máy đặt tại tầng 5 trong một tòa nhà. Việc trao đổi dữ liệu giữa các máy tính ngày càng nhiều hơn, đa dạng hơn, khoảng cách giữa các phòng ban trong công ty ngày càng xa hơn nên việc trao đổi dữ liệu theo phương thức truyền thống không còn được áp dụng nữa, thay vào đó là các máy tính này được nối với nhau qua công nghệ mạng.

## VII.3. Chia sẻ ứng dụng.

Các ứng dụng thay vì trên từng máy trạm chúng ta sẽ cài trên một máy server và các máy trạm dùng chung ứng dụng đó trên **server**. Lúc đó ta tiết kiệm được chi phí bản quyền và chi phí cài đặt, quản trị.

## VII.4. Tập trung dữ liệu, bảo mật và backup tốt.

Đối với các công ty lớn dữ liệu lưu trữ trên các máy trạm rời rạc dễ dẫn đến tình trạng hư hỏng thông tin và không được bảo mật. Nếu các dữ liệu này được tập trung về server để tiện việc bảo mật, backup và quét virus.

## VII.5. Sử dụng các phần mềm ứng dụng trên mạng.

Nhờ các công nghệ mạng mà các phần mềm ứng dụng phát triển mạnh và được áp dụng vào nhiều lĩnh vực như hàng không (phần mềm bán vé máy bay tại các chi nhánh), đường sắt (phần mềm theo dõi đăng ký vé và bán vé tàu), cấp thoát nước (phần mềm quản lý công ty cấp thoát nước thành phố)...

## VII.6. Sử dụng các dịch vụ Internet.

Ngày nay Internet rất phát triển, tất cả mọi người trên thế giới đều có thể trao đổi E-mail với nhau một cách dễ dàng hoặc có thể trò chuyện với nhau mà chi phí rất thấp so với phí viễn thông. Đồng thời các công ty cũng dùng công nghệ Web để quảng cáo sản phẩm, mua bán hàng hóa qua mạng (thương mại điện tử) ...

Dựa trên cơ sở hạ tầng mạng chúng ta có thể xây dựng các hệ thống ứng dụng lớn như chính phủ điện tử, thương mại điện tử, điện thoại Internet nhằm giảm chi phí và tăng khả năng phục vụ ngày càng tốt hơn cho con người.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

# Bài 2
# MÔ HÌNH THAM CHIẾU OSI

## Tóm tắt

Lý thuyết 4 tiết - Thực hành 0 tiết

| Mục tiêu | Các mục chính | Bài tập bắt buộc | Bài tập làm thêm |
|---|---|---|---|
| Kết thúc bài học này cung cấp học viên kiến thức về giao thức, mô hình OSI, TCP/IP và quá trình xử lý, vận chuyển của một gói tin … | I. Mô hình OSI.<br>II. Quá trình xử lý và vận chuyển của một gói dữ liệu.<br>III. Mô hình tham chiếu TCP/IP. | Dựa vào bài tập môn mạng máy tính. | Dựa vào bài tập môn mạng máy tính. |



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

# I. MÔ HÌNH OSI.

## I.1. Khái niệm giao thức (protocol).

Là quy tắc giao tiếp (tiêu chuẩn giao tiếp) giữa hai hệ thống giúp chúng hiểu và trao đổi dữ liệu được với nhau.

Ví dụ: **Internetwork Packet Exchange** (**IPX**), **Transmission control protocol/ Internetwork Protocol** (**TCP/IP**), **NetBIOS Extended User Interface** (**NetBEUI**)…

## I.2. Các tổ chức định chuẩn.

ITU (**International Telecommunication Union**): Hiệp hội Viễn thông quốc tế.

IEEE (**Institute of Electrical and Electronic Engineers**): Viện các kĩ sư điện và điện tử.

ISO (**International Standardization Organization**): Tổ chức Tiêu chuẩn quốc tế, trụ sở tại Geneve, Thụy Sĩ. Vào năm 1977, ISO được giao trách nhiệm thiết kế một chuẩn truyền thông dựa trên lí thuyết về kiến trúc các hệ thống mở làm cơ sở để thiết kế mạng máy tính. Mô hình này có tên là OSI (**Open System Interconnection** - tương kết các hệ thống mở)

## I.3. Mô hình OSI.

Mô hình OSI (**Open System Interconnection**): là mô hình được tổ chức ISO đề xuất từ 1977 và công bố lần đầu vào 1984. Để các máy tính và các thiết bị mạng có thể truyền thông với nhau phải có những qui tắc giao tiếp được các bên chấp nhận. Mô hình OSI là một khuôn mẫu giúp chúng ta hiểu dữ liệu đi xuyên qua mạng như thế nào đồng thời cũng giúp chúng ta hiểu được các chức năng mạng diễn ra tại mỗi lớp.

Trong mô hình OSI có bảy lớp, mỗi lớp mô tả một phần chức năng độc lập. Sự tách lớp của mô hình này mang lại những lợi ích sau:

- Chia hoạt động thông tin mạng thành những phần nhỏ hơn, đơn giản hơn giúp chúng ta dễ khảo sát và tìm hiểu hơn.
- Chuẩn hóa các thành phần mạng để cho phép phát triển mạng từ nhiều nhà cung cấp sản phẩm.
- Ngăn chặn được tình trạng sự thay đổi của một lớp làm ảnh hưởng đến các lớp khác, như vậy giúp mỗi lớp có thể phát triển độc lập và nhanh chóng hơn.

Mô hình tham chiếu OSI định nghĩa các qui tắc cho các nội dung sau:

- Cách thức các thiết bị giao tiếp và truyền thông được với nhau.
- Các phương pháp để các thiết bị trên mạng khi nào thì được truyền dữ liệu, khi nào thì không được.
- Các phương pháp để đảm bảo truyền đúng dữ liệu và đúng bên nhận.
- Cách thức vận tải, truyền, sắp xếp và kết nối với nhau.
- Cách thức đảm bảo các thiết bị mạng duy trì tốc độ truyền dữ liệu thích hợp.
- Cách biểu diễn một bit thiết bị truyền dẫn.

Mô hình tham chiếu OSI được chia thành bảy lớp với các chức năng sau:



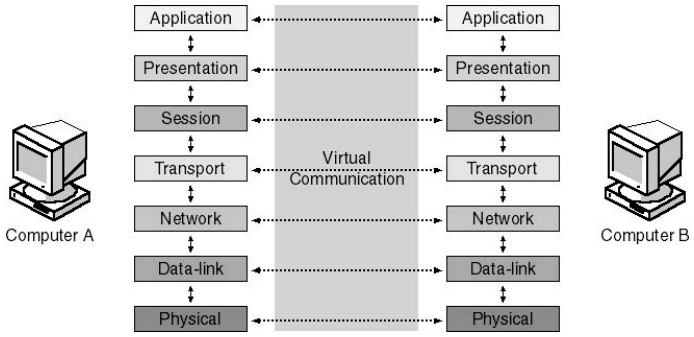
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

- **Application Layer** (lớp ứng dụng): giao diện giữa ứng dụng và mạng.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

- **Presentation Layer** (lớp trình bày): thoả thuận khuôn dạng trao đổi dữ liệu.
- **Session Layer** (lớp phiên): cho phép người dùng thiết lập các kết nối.
- **Transport Layer** (lớp vận chuyển): đảm bảo truyền thông giữa hai hệ thống.
- **Network Layer** (lớp mạng): định hướng dữ liệu truyền trong môi trường liên mạng.
- **Data link Layer** (lớp liên kết dữ liệu): xác định việc truy xuất đến các thiết bị.
- **Physical Layer** (lớp vật lý): chuyển đổi dữ liệu thành các bit và truyền đi.




Hình 2.1 – Mô hình tham chiếu OSI

## I.4. Chức năng của các lớp trong mô hình tham chiếu OSI

Lớp ứng dụng (**Application Layer**): là giao diện giữa các chương trình ứng dụng của người dùng và mạng. Lớp **Application** xử lý truy nhập mạng chung, kiểm soát luồng và phục hồi lỗi. Lớp này không cung cấp các dịch vụ cho lớp nào mà nó cung cấp dịch vụ cho các ứng dụng như: truyền file, gởi nhận E-mail, Telnet, HTTP, FTP, SMTP…

Lớp trình bày (**Presentation Layer**): lớp này chịu trách nhiệm thương lượng và xác lập dạng thức dữ liệu được trao đổi. Nó đảm bảo thông tin mà lớp ứng dụng của một hệ thống đầu cuối gởi đi, lớp ứng dụng của hệ thống khác có thể đọc được. Lớp trình bày thông dịch giữa nhiều dạng dữ liệu khác nhau thông qua một dạng chung, đồng thời nó cũng nén và giải nén dữ liệu. Thứ tự byte, bit bên gởi và bên nhận qui ước qui tắc gởi nhận một chuỗi byte, bit từ trái qua phải hay từ phải qua trái. Nếu hai bên không thống nhất thì sẽ có sự chuyển đổi thứ tự các byte bit vào trước hoặc sau khi truyền. Lớp **presentation** cũng quản lý các cấp độ nén dữ liệu nhằm giảm số bit cần truyền. Ví dụ: **JPEG, ASCCI, EBCDIC....**

Lớp phiên (**Session Layer**): lớp này có chức năng thiết lập, quản lý, và kết thúc các phiên thông tin giữa hai thiết bị truyền nhận. Lớp phiên cung cấp các dịch vụ cho lớp trình bày. Lớp **Session** cung cấp sự đồng bộ hóa giữa các tác vụ người dùng bằng cách đặt những điểm kiểm tra vào luồng dữ liệu. Bằng cách này, nếu mạng không hoạt động thì chỉ có dữ liệu truyền sau điểm kiểm tra cuối cùng mới phải truyền lại. Lớp này cũng thi hành kiểm soát hội thoại giữa các quá trình giao tiếp, điều chỉnh bên nào truyền, khi nào, trong bao lâu. Ví dụ như: **RPC, NFS**,... Lớp này kết nối theo ba cách: **Haft-duplex, Simplex, Full-duplex.**



Lớp vận chuyển (**Transport Layer**): lớp vận chuyển phân đoạn dữ liệu từ hệ thống máy truyền và tái thiết lập dữ liệu vào một luồng dữ liệu tại hệ thống máy nhận đảm bảo rằng việc bàn giao các thông điệp giữa các thiết bị đáng tin cậy. Dữ liệu tại lớp này gọi là **segment**. Lớp này thiết lập, duy trì và kết

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

thúc các mạch ảo đảm bảo cung cấp các dịch vụ sau:



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

- Xếp thứ tự các phân đoạn: khi một thông điệp lớn được tách thành nhiều phân đoạn nhỏ để ban giao, lớp vận chuyển sẽ sắp xếp thứ tự các phân đoạn trước khi ráp nối các phân đoạn thành thông điệp ban đầu.
- Kiểm soát lỗi: khi có phân đoạn bị thất bại, sai hoặc trùng lắp, lớp vận chuyển sẽ yêu cầu truyền lại.
- Kiểm soát luồng: lớp vận chuyển dùng các tín hiệu báo nhận để xác nhận. Bên gửi sẽ không truyền đi phân đoạn dữ liệu kế tiếp nếu bên nhận chưa gởi tín hiệu xác nhận rằng đã nhận được phân đoạn dữ liệu trước đó đầy đủ.

Lớp mạng (**Network Layer**): lớp mạng chịu trách nhiệm lập địa chỉ các thông điệp, diễn dịch địa chỉ và tên logic thành địa chỉ vật lý đồng thời nó cũng chịu trách nhiệm gởi packet từ mạng nguồn đến mạng đích. Lớp này quyết định đường đi từ máy tính nguồn đến máy tính đích. Nó quyết định dữ liệu sẽ truyền trên đường nào dựa vào tình trạng, ưu tiên dịch vụ và các yếu tố khác. Nó cũng quản lý lưu lượng trên mạng chẳng hạn như chuyển đổi gói, định tuyến, và kiểm soát sự tắc nghẽn dữ liệu. Nếu bộ thích ứng mạng trên bộ định tuyến (router) không thể truyền đủ đoạn dữ liệu mà máy tính nguồn gởi đi, lớp **Network** trên bộ định tuyến sẽ chia dữ liệu thành những đơn vị nhỏ hơn, nói cách khác, nếu máy tính nguồn gởi đi các gói tin có kích thước là 20Kb, trong khi **Router** chỉ cho phép các gói tin có kích thước là 10Kb đi qua, thì lúc đó lớp **Network** của **Router** sẽ chia gói tin ra làm 2, mỗi gói tin có kích thước là 10Kb. Ở đầu nhận, lớp **Network** ráp nối lại dữ liệu. Ví dụ: một số giao thức lớp này: IP, IPX,... Dữ liệu ở lớp này gọi packet hoặc datagram.

Lớp liên kết dữ liệu (**Data link Layer**): cung cấp khả năng chuyển dữ liệu tin cậy xuyên qua một liên kết vật lý. Lớp này liên quan đến:

- Địa chỉ vật lý.
- Mô hình mạng.
- Cơ chế truy cập đường truyền.
- Thông báo lỗi.
- Thứ tự phân phối frame.
- Điều khiển dòng.

Tại lớp **data link**, các bít đến từ lớp vật lý được chuyển thành các frame dữ liệu bằng cách dùng một số nghi thức tại lớp này. Lớp **data link** được chia thành hai lớp con:

- Lớp con LLC (**logical link control**).
- Lớp con MAC (**media access control**).

Lớp con LLC là phần trên so với các giao thức truy cập đường truyền khác, nó cung cấp sự mềm dẻo về giao tiếp. Bởi vì lớp con LLC hoạt động độc lập với các giao thức truy cập đường truyền, cho nên các giao thức lớp trên hơn (ví dụ như IP ở lớp mạng) có thể hoạt động mà không phụ thuộc vào loại phương tiện LAN. Lớp con LLC có thể lệ thuộc vào các lớp thấp hơn trong việc cung cấp truy cập đường truyền.

Lớp con MAC cung cấp tính thứ tự truy cập vào môi trường LAN. Khi nhiều trạm cùng truy cập chia sẻ môi trường truyền, để định danh mỗi trạm, lớp cho MAC định nghĩa một trường địa chỉ phần cứng, gọi là địa chỉ MAC address. Địa chỉ MAC là một con số đơn nhất đối với mỗi giao tiếp LAN (card mạng).

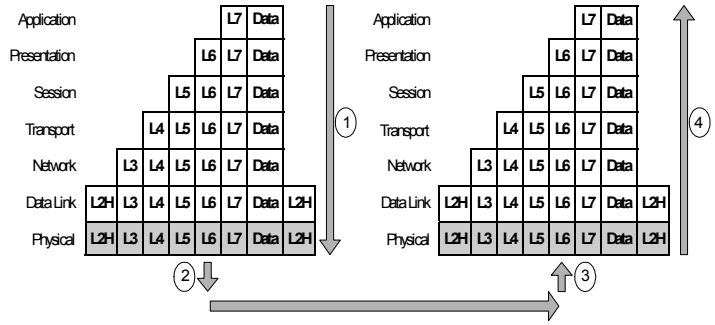


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Lớp vật lý (**Physical Layer**): định nghĩa các qui cách về điện, cơ, thủ tục và các đặc tả chức năng để kích hoạt, duy trì và dừng một liên kết vật lý giữa các hệ thống đầu cuối. Một số các đặc điểm trong lớp vật lý này bao gồm:

- Mức điện thế.
- Khoảng thời gian thay đổi điện thế.
- Tốc độ dữ liệu vật lý.
- Khoảng đường truyền tối đa.
- Các đầu nối vật lý.

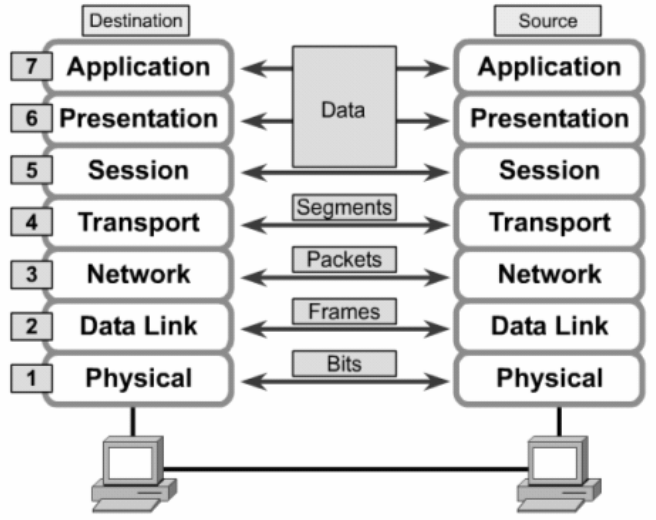
# II. QUÁ TRÌNH XỬ LÝ VÀ VẬN CHUYỂN CỦA MỘT GÓI DỮ LIỆU.




Hình 2.2 – Quá trình xử lý và vận chuyển của gói tin

## II.1. Quá trình đóng gói dữ liệu (tại máy gửi)

Đóng gói dữ liệu là quá trình đặt dữ liệu nhận được vào sau **header** (và trước **trailer**) trên mỗi lớp. Lớp **Physical** không đóng gói dữ liệu vì nó không dùng **header** và **trailer**. Việc đóng gói dữ liệu không nhất thiết phải xảy ra trong mỗi lần truyền dữ liệu của trình ứng dụng. Các lớp 5, 6, 7 sử dụng **header** trong quá trình khởi động, nhưng trong phần lớn các lần truyền thì không có **header** của lớp 5, 6, 7 lý do là không có thông tin mới để trao đổi.






Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Hình 2.3 – Tên gọi dữ liệu ở các tầng trong mô hình OSI



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Các dữ liệu tại máy gửi được xử lý theo trình tự như sau:

- Người dùng thông qua lớp **Application** để đưa các thông tin vào máy tính. Các thông tin này có nhiều dạng khác nhau như: hình ảnh, âm thanh, văn bản…
- Tiếp theo các thông tin đó được chuyển xuống lớp **Presentation** để chuyển thành dạng chung, rồi mã hoá và nén dữ liệu.
- Tiếp đó dữ liệu được chuyển xuống lớp **Session** để bổ sung các thông tin về phiên giao dịch này.
- Dữ liệu tiếp tục được chuyển xuống lớp **Transport**, tại lớp này dữ liệu được cắt ra thành nhiều **Segment** và bổ sung thêm các thông tin về phương thức vận chuyển dữ liệu để đảm bảo độ tin cậy khi truyền.
- Dữ liệu tiếp tục được chuyển xuống lớp **Network**, tại lớp này mỗi **Segment** được cắt ra thành nhiều **Packet** và bổ sung thêm các thông tin định tuyến.
- Tiếp đó dữ liệu được chuyển xuống lớp **Data Link**, tại lớp này mỗi **Packet** sẽ được cắt ra thành nhiều **Frame** và bổ sung thêm các thông tin kiểm tra gói tin (để kiểm tra ở nơi nhận).
- Cuối cùng, mỗi **Frame** sẽ được tầng Vật Lý chuyển thành một chuỗi các bit, và được đẩy lên các phương tiện truyền dẫn để truyền đến các thiết bị khác.

## II.2. Quá trình truyền dữ liệu từ máy gửi đến máy nhận.

Bước 1: Trình ứng dụng (trên máy gửi) tạo ra dữ liệu và các chương trình phần cứng, phần mềm cài đặt mỗi lớp sẽ bổ sung vào header và trailer (quá trình đóng gói dữ liệu tại máy gửi).

Bước 2: Lớp **Physical** (trên máy gửi) phát sinh tín hiệu lên môi trường truyền tải để truyền dữ liệu.

Bước 3: Lớp **Physical** (trên máy nhận) nhận dữ liệu.

Bước 4: Các chương trình phần cứng, phần mềm (trên máy nhận) gỡ bỏ **header** và **trailer** và xử lý phần dữ liệu (quá trình xử lý dữ liệu tại máy nhận).

Giữa bước 1 và bước 2 là quá trình tìm đường đi của gói tin. Thông thường, máy gửi đã biết địa chỉ IP của máy nhận. Vì thế, sau khi xác định được địa chỉ IP của máy nhận thì lớp Network của máy gửi sẽ so sánh địa chỉ IP của máy nhận và địa chỉ IP của chính nó:

- Nếu cùng địa chỉ mạng thì máy gửi sẽ tìm trong bảng **MAC Table** của mình để có được địa chỉ MAC của máy nhận. Trong trường hợp không có được địa chỉ MAC tương ứng, nó sẽ thực hiện giao thức ARP để truy tìm địa chỉ MAC. Sau khi tìm được địa chỉ MAC, nó sẽ lưu địa chỉ MAC này vào trong bảng **MAC Table** để lớp **Datalink** sử dụng ở các lần gửi sau. Sau khi có địa chỉ MAC thì máy gửi sẽ gởi gói tin đi (giao thức ARP sẽ được nói thêm trong chương 6).
- Nếu khác địa chỉ mạng thì máy gửi sẽ kiểm tra xem máy có được khai báo **Default Gateway** hay không.
    + Nếu có khai báo **Default Gateway** thì máy gửi sẽ gởi gói tin thông qua **Default Gateway**.
    + Nếu không có khai báo **Default Gateway** thì máy gởi sẽ loại bỏ gói tin và thông báo "**Destination host Unreachable**"



## II.3. Chi tiết quá trình xử lý tại máy nhận

Bước 1: Lớp **Physical** kiểm tra quá trình đồng bộ bit và đặt chuỗi bit nhận được vào vùng đệm. Sau đó thông báo cho lớp **Data Link** dữ liệu đã được nhận.

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Bước 2: Lớp **Data Link** kiểm lỗi frame bằng cách kiểm tra FCS trong trailer. Nếu có lỗi thì frame bị bỏ. Sau đó kiểm tra địa chỉ lớp **Data Link** (địa chỉ MAC) xem có trùng với địa chỉ máy nhận hay không. Nếu đúng thì phần dữ liệu sau khi loại header và trailer sẽ được chuyển lên cho lớp Network.

Bước 3: Địa chỉ lớp **Network** được kiểm tra xem có phải là địa chỉ máy nhận hay không (địa chỉ IP) ? Nếu đúng thì dữ liệu được chuyển lên cho lớp **Transport** xử lý.

Bước 4: Nếu giao thức lớp **Transport** có hỗ trợ việc phục hồi lỗi thì số định danh phân đoạn được xử lý. Các thông tin **ACK, NAK** (gói tin **ACK, NAK** dùng để phản hồi về việc các gói tin đã được gởi đến máy nhận chưa) cũng được xử lý ở lớp này. Sau quá trình phục hồi lỗi và sắp thứ tự các phân đoạn, dữ liệu được đưa lên lớp **Session**.

Bước 5: Lớp **Session** đảm bảo một chuỗi các thông điệp đã trọn vẹn. Sau khi các luồng đã hoàn tất, lớp Session chuyển dữ liệu sau header lớp 5 lên cho lớp **Presentation** xử lý.

Bước 6: Dữ liệu sẽ được lớp **Presentation** xử lý bằng cách chuyển đổi dạng thức dữ liệu. Sau đó kết quả chuyển lên cho lớp **Application**.

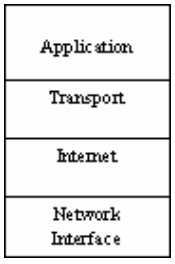
Bước 7: Lớp **Application** xử lý **header** cuối cùng. **Header** này chứa các tham số thoả thuận giữa hai trình ứng dụng. Do vậy tham số này thường chỉ được trao đổi lúc khởi động quá trình truyền thông giữa hai trình ứng dụng.

# III. MÔ HÌNH THAM CHIẾU TCP/IP.

## III.1. Vai trò của mô hình tham chiếu TCP/IP.

Các bộ phận, văn phòng của Chính phủ Hoa Kỳ đã nhận thức được sự quan trọng và tiềm năng của kĩ thuật Internet từ nhiều năm trước, cũng như đã cung cấp tài chánh cho việc nghiên cứu, để thực sự có được một mạng Internet toàn cầu. Sự hình thành kĩ thuật Internet là kết quả nghiên cứu dưới sự tài trợ của **Defense/Advanced Research Projects Agency** (**ARPA/DARPA**). Kĩ thuật **ARPA** bao gồm một tập hợp của các chuẩn mạng, đặc tả chi tiết cách thức mà các máy tính thông tin liên lạc với nhau, cũng như các quy ước cho các mạng **interconnecting** và định tuyến giao thông. Tên chính thức là **TCP/IP Internet Protocol Suite** và thường được gọi là **TCP/IP**, có thể dùng để thông tin liên lạc qua tập hợp bất kỳ các mạng **interconnected**. Nó có thể dùng để liên kết mạng trong một công ty, không nhất thiết phải nối kết với các mạng khác bên ngoài.

## III.2. Các lớp của mô hình tham chiếu TCP/IP.




Hình 2.4 – Mô hình tham chiếu TCP/IP

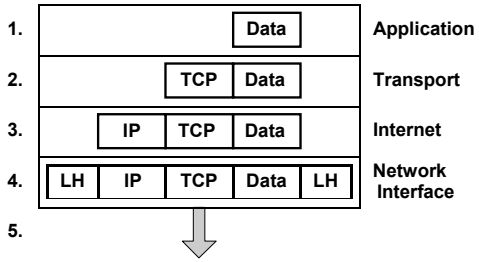
Mô hình tham chiếu TCP/IP tương tự như kiến trúc OSI, sau đây là một số tính chất của các lớp trong mô hình tham chiếu TCP/IP:



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

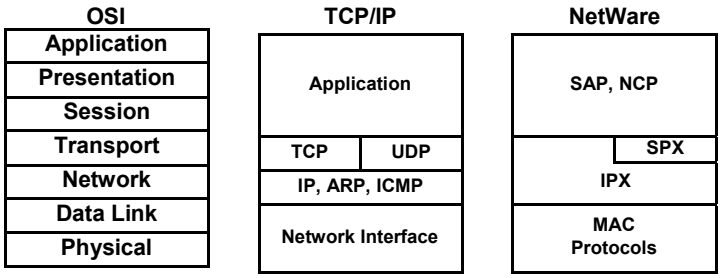
- Lớp **Application**: quản lý các giao thức, như hỗ trợ việc trình bày, mã hóa, và quản lý cuộc gọi. Lớp **Application** cũng hỗ trợ nhiều ứng dụng, như: FTP (**File Transfer Protocol**), HTTP (**Hypertext Transfer Protocol**), SMTP (**Simple Mail Transfer Protocol**), DNS (**Domain Name System**), TFTP (**Trivial File Transfer Protocol**).
- Lớp **Transport**: đảm nhiệm việc vận chuyển từ nguồn đến đích. Tầng **Transport** đảm nhiệm việc truyền dữ liệu thông qua hai nghi thức: TCP (**Transmission Control Protocol**) và UDP (**User Datagram Protocol**).
- Lớp **Internet**: đảm nhiệm việc chọn lựa đường đi tốt nhất cho các gói tin. Nghi thức được sử dụng chính ở tầng này là nghi thức IP (**Internet Protocol**).
- Lớp **Network Interface**: có tính chất tương tự như hai lớp **Data Link** và **Physical** của kiến trúc OSI.

## III.3. Các bước đóng gói dữ liệu trong mô hình TCP/IP.




Hình 2.5 – Các bước đóng gói trong mô hình TCP/IP

## III.4. So sánh mô hình OSI và TCP/IP.




Hình 2.6 – So sánh mô hình OSI và mô hình TCP/IP

Các điểm giống nhau:

- Cả hai đều có kiến trúc phân lớp.
- Đều có lớp **Application**, mặc dù các dịch vụ ở mỗi lớp khác nhau.
- Đều có các lớp **Transport** và **Network**.
- Sử dụng kĩ thuật chuyển packet (**packet-switched**).
- Các nhà quản trị mạng chuyên nghiệp cần phải biết rõ hai mô hình trên.

Các điểm khác nhau:

- Mô hình TCP/IP kết hợp lớp **Presentation** và lớp **Session** vào trong lớp **Application**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

- Mô hình TCP/IP kết hợp lớp **Data Link** và lớp **Physical** vào trong một lớp.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

- Mô hình TCP/IP đơn giản hơn bởi vì có ít lớp hơn.
- Nghi thức TCP/IP được chuẩn hóa và được sử dụng phổ biến trên toàn thế giới.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

# Tóm tắt

Lý thuyết 5 tiết - Thực hành 5 tiết

| Mục tiêu | Các mục chính | Bài tập bắt buộc | Bài tập làm thêm |
|---|---|---|---|
| Kết thúc bài học này cung cấp học viên kiến thức về cấu trúc của một địa chỉ IP, các lớp địa chỉ, kỹ thuật chia mạng con, kỹ thuật NAT… | I. Tổng quan về địa chỉ IP.<br>II. Giới thiệu các lớp địa chỉ.<br>III. Các ví dụ khi tính toán trên địa chỉ mạng. | Dựa vào bài tập môn mạng máy tính. | Dựa vào bài tập môn mạng máy tính. |



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

# I. TỔNG QUAN VỀ ĐỊA CHỈ IP

Là địa chỉ có cấu trúc, được chia làm hai hoặc ba phần là: **network_id&host_id** hoặc **network_id&subnet_id&host_id**.

Là một con số có kích thước 32 bit. Khi trình bày, người ta chia con số 32 bit này thành bốn phần, mỗi phần có kích thước 8 bit, gọi là **octet** hoặc **byte**. Có các cách trình bày sau:

- Ký pháp thập phân có dấu chấm (**dotted-decimal notation**). Ví dụ: 172.16.30.56.
- Ký pháp nhị phân. Ví dụ: 10101100 00010000 00011110 00111000.
- Ký pháp thập lục phân. Ví dụ: AC 10 1E 38.

Không gian địa chỉ IP (gồm $2^{32}$ địa chỉ) được chia thành nhiều lớp (class) để dễ quản lý. Đó là các lớp: A, B, C, D và E; trong đó các lớp A, B và C được triển khai để đặt cho các host trên mạng **Internet**; lớp D dùng cho các nhóm **multicast**; còn lớp E phục vụ cho mục đích nghiên cứu.

Địa chỉ IP còn được gọi là địa chỉ **logical**, trong khi địa chỉ **MAC** còn gọi là địa chỉ vật lý (hay địa chỉ **physical**).

# II. MỘT SỐ KHÁI NIỆM VÀ THUẬT NGỮ LIÊN QUAN.

**Network_id**: là giá trị để xác định đường mạng. Trong số 32 bit dùng địa chỉ IP, sẽ có một số bit đầu tiên dùng để xác định network_id. Giá trị của các bit này được dùng để xác định đường mạng.

**Host_id**: là giá trị để xác định host trong đường mạng. Trong số 32 bit dùng làm địa chỉ IP, sẽ có một số bit cuối cùng dùng để xác định host_id. Host_id chính là giá trị của các bit này.

Địa chỉ **host**: là địa chỉ IP, có thể dùng để đặt cho các interface của các host. Hai host nằm thuộc cùng một mạng sẽ có **network_id** giống nhau và **host_id** khác nhau.

Mạng (**network**): một nhóm nhiều host kết nối trực tiếp với nhau. Giữa hai host bất kỳ không bị phân cách bởi một thiết bị layer 3. Giữa mạng này với mạng khác phải kết nối với nhau bằng thiết bị layer 3.

Địa chỉ mạng (**network address**): là địa chỉ IP dùng để đặt cho các mạng. Địa chỉ này không thể dùng để đặt cho một **interface**. Phần **host_id** của địa chỉ chỉ chứa các bit 0. Ví dụ 172.29.0.0 là một địa chỉ mạng.

Mạng con (**subnet network**): là mạng có được khi một địa chỉ mạng (thuộc lớp A, B, C) được phân chia nhỏ hơn (để tận dụng số địa chỉ mạng được cấp phát). Địa chỉ mạng con được xác định dựa vào địa chỉ IP và mặt nạ mạng con (**subnet mask**) đi kèm (sẽ đề cập rõ hơn ở phần sau).

Địa chỉ **broadcast**: là địa chỉ IP được dùng để đại diện cho tất cả các host trong mạng. Phần **host_id** chỉ chứa các bit 1. Địa chỉ này cũng không thể dùng để đặt cho một host được. Ví dụ 172.29.255.255 là một địa chỉ **broadcast**.



Các phép toán làm việc trên bit:

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

| Phép AND | | | Phép OR | | |
|---|---|---|---|---|---|
| A | B | A and B | A | B | A or B |
| 1 | 1 | 1 | 1 | 1 | 1 |
| 1 | 0 | 0 | 1 | 0 | 1 |
| 0 | 1 | 0 | 0 | 1 | 1 |
| 0 | 0 | 0 | 0 | 0 | 0 |

Ví dụ sau minh hoạ phép AND giữa địa chỉ 172.29.14.10 và mask 255.255.0.0

172.29.14.10 = 10101100000111010000111000001010AND

255.255.0.0 = 11111111111111110000000000000000

172.29.0.0 = 10101100000111010000000000000000

Mặt nạ mạng (**network mask**): là một con số dài 32 bit, là phương tiện giúp máy xác định được địa chỉ mạng của một địa chỉ IP (bằng cách AND giữa địa chỉ IP với mặt nạ mạng) để phục vụ cho công việc routing. Mặt nạ mạng cũng cho biết số bit nằm trong phần **host_id**. Được xây dựng theo cách: bật các bit tương ứng với phần **network_id** (chuyển thành bit 1) và tắt các bit tương ứng với phần **host_id** (chuyển thành bit 0).

Mặt nạ mặc định của lớp A: sử dụng cho các địa chỉ lớp A khi không chia mạng con, mặt nạ có giá trị 255.0.0.0.

Mặt nạ mặc định của lớp B: sử dụng cho các địa chỉ lớp B khi không chia mạng con, mặt nạ có giá trị 255.255.0.0.

Mặt nạ mặc định của lớp C: sử dụng cho các địa chỉ lớp C khi không chia mạng con, mặt nạ có giá trị 255.255.255.0.

# III. GIỚI THIỆU CÁC LỚP ĐỊA CHỈ.

## III.1. Lớp A.

Dành một byte cho phần **network_id** và ba byte cho phần **host_id**.

| network_id | | host_id | |
|---|---|---|---|

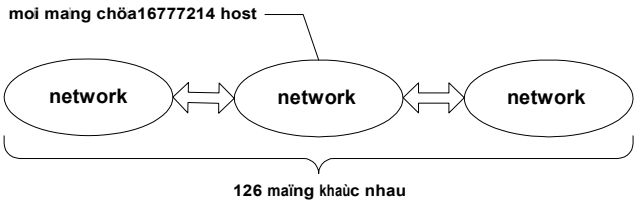
Để nhận diện ra lớp A, bit đầu tiên của byte đầu tiên phải là bit 0. Dưới dạng nhị phân, byte này có dạng 0xxxxxxx. Vì vậy, những địa chỉ IP có byte đầu tiên nằm trong khoảng từ 0 (00000000) đến 127 (01111111) sẽ thuộc lớp A. Ví dụ địa chỉ 50.14.32.8 là một địa chỉ lớp A (50 < 127).

Byte đầu tiên này cũng chính là **network_id**, trừ đi bit đầu tiên làm ID nhận dạng lớp A, còn lại bảy bit để đánh thứ tự các mạng, ta được 128 ($2^7$) mạng lớp A khác nhau. Bỏ đi hai trường hợp đặc biệt là 0 và 127. Kết quả là lớp A chỉ còn 126 ($2^7$-2) địa chỉ mạng, 1.0.0.0 đến 126.0.0.0.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Phần host_id chiếm 24 bit, tức có thể đặt địa chỉ cho 16.777.216 ($2^{24}$) host khác nhau trong mỗi mạng. Bỏ đi một địa chỉ mạng (phần **host_id** chứa toàn các bit 0) và một địa chỉ **broadcast** (phần **host_id** chứa toàn các bit 1) như vậy có tất cả 16.777.214 ($2^{24}$-2) host khác nhau trong mỗi mạng lớp A. Ví dụ, đối với mạng 10.0.0.0 thì những giá trị host hợp lệ là 10.0.0.1 đến 10.255.255.254.




Hình 3.1 – Mô tả các mạng lớp A kết nối với nhau

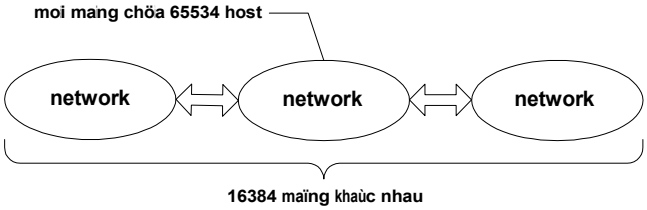
## III.2. Lớp B.

Dành hai byte cho mỗi phần **network_id** và **host_id**.


Dấu hiệu để nhận dạng địa chỉ lớp B là byte đầu tiên luôn bắt đầu bằng hai bit 10. Dưới dạng nhị phân, octet có dạng 10xxxxxx. Vì vậy những địa chỉ nằm trong khoảng từ 128 (10000000) đến 191 (10111111) sẽ thuộc về lớp B. Ví dụ 172.29.10.1 là một địa chỉ lớp B (128 < 172 < 191).

Phần **network_id** chiếm 16 bit bỏ đi 2 bit làm ID cho lớp, còn lại 14 bit cho phép ta đánh thứ tự 16.384 ($2^{14}$) mạng khác nhau (128.0.0.0 đến 191.255.0.0)

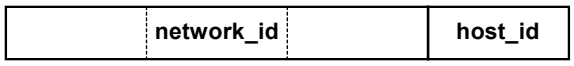
Phần **host_id** dài 16 bit hay có 65536 ($2^{16}$) giá trị khác nhau. Trừ 2 trường hợp đặc biệt còn lại 65534 host trong một mạng lớp B. Ví dụ, đối với mạng 172.29.0.0 thì các địa chỉ host hợp lệ là từ 172.29.0.1 đến 172.29.255.254.




Hình 3.2 – Mô tả các mạng lớp B kết nối với nhau

## III.3. Lớp C.

Dành ba byte cho phần **network_id** và một byte cho phần **host_id**.




Byte đầu tiên luôn bắt đầu bằng ba bit 110 và dạng nhị phân của octet này là 110xxxxx. Như vậy những địa chỉ nằm trong khoảng từ 192 (**110**00000) đến 223 (**110**11111) sẽ thuộc về lớp C. Ví dụ một địa chỉ lớp C là 203.162.41.235 (192 < 203 < 223).

Phần **network_id** dùng ba byte hay 24 bit, trừ đi 3 bit làm ID của lớp, còn lại 21 bit hay 2.097.152 ($2^{21}$)



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

địa chỉ mạng (từ **192.0.0**.0 đến **223.255.255**.0).



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Phần **host_id** dài một byte cho 256 ($2^8$) giá trị khác nhau. Trừ đi hai trường hợp đặc biệt ta còn 254 host khác nhau trong một mạng lớp C. Ví dụ, đối với mạng 203.162.41.0, các địa chỉ host hợp lệ là từ 203.162.41.1 đến 203.162.41.254.

## III.4. Lớp D và E.

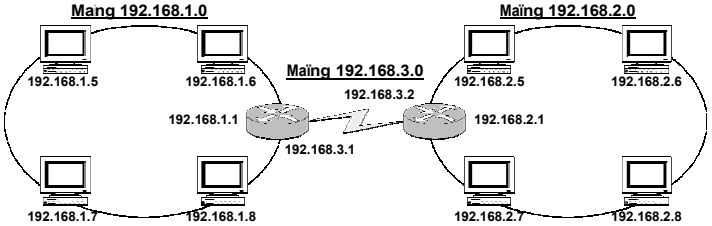
Các địa chỉ có byte đầu tiên nằm trong khoảng 224 đến 255 là các địa chỉ thuộc lớp D hoặc E. Do các lớp này không phục vụ cho việc đánh địa chỉ các host nên không trình bày ở đây.

## III.5. Bảng tổng kết.

| | Lớp A | Lớp B | Lớp C |
|---|---|---|---|
| Giá trị của byte đầu tiên | 0 – 127 | 128 – 191 | 192 – 223 |
| Số byte phần Network_id | 1 | 2 | 3 |
| Số byte phần Host_id | 3 | 2 | 1 |
| Network mask | 255.0.0.0 | 255.255.0.0 | 255.255.255.0 |
| Broadcast | XX.255.255.255 | XX.XX.255.255 | XX.XX.XX.255 |
| Network Address | XX.0.0.0 | XX.XX.0.0 | XX.XX.XX.0 |
| Số đường mạng | 128 | 16.384 | 2.097.152 |
| Số host trên mỗi đường mạng | 16.777.214 | 65.534 | 254 |

* Ghi chú: XX là số bất kỳ trong miền cho phép.

## III.6. Ví dụ cách triển khai đặt địa chỉ IP cho một hệ thống mạng.



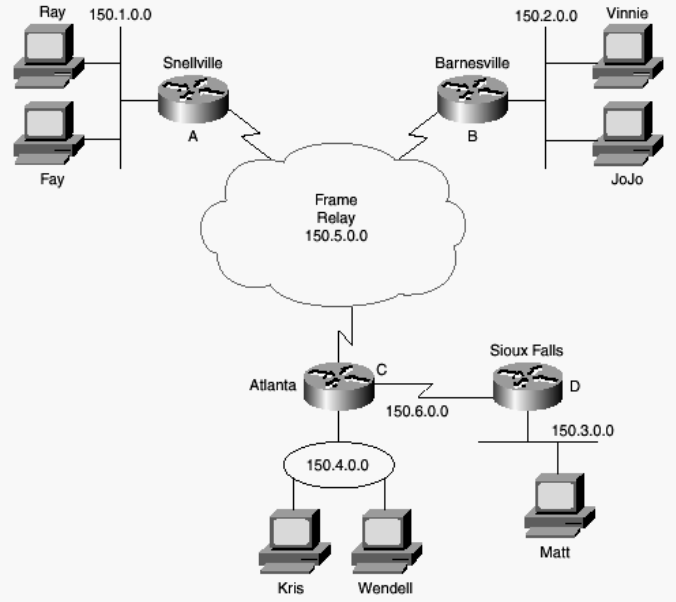

Hình 3.3 – Minh họa một hệ thống mạng

## III.7. Chia mạng con (subnetting).

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

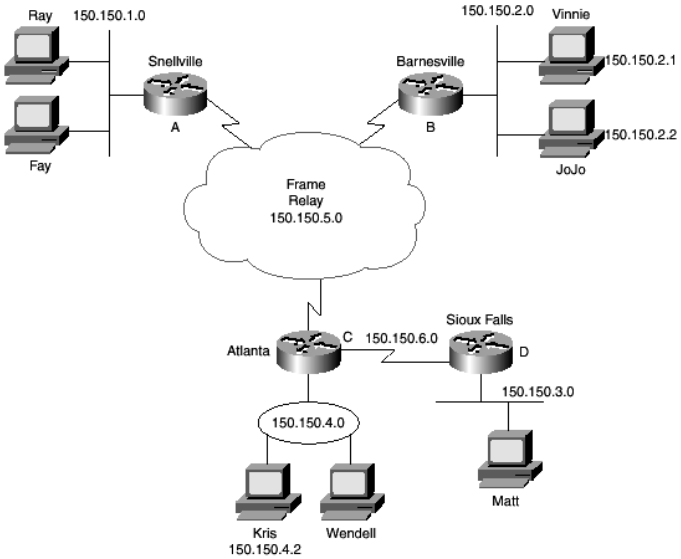


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 3.4 – Hệ thống mạng có 6 đường mạng

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 150.150.0.0 và chia đường mạng này thành sáu mạng con theo hình bên dưới:



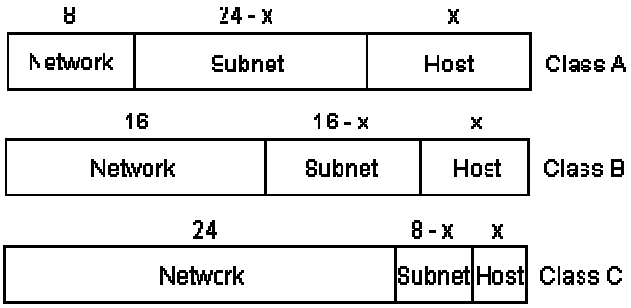

Hình 3.5 – Hệ thống mạng có 6 đường mạng (sau khi chia Subnet)

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.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

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 con. Lúc này, cấu trúc của địa chỉ IP gồm có ba phần: ***network_id***, ***subnet_id*** và ***host_id***. Số bit dùng cho phần **subnet_id** bao nhiêu là tuỳ thuộc vào chiến lược chia mạng con của người quản trị, có thể là một con số tròn byte (8 bit) hoặc một số bit lẻ vẫn được. Tuy nhiên **subnet_id** không thể chiếm trọn số bit có trong **host_id** ban đầu, cụ thể là (số bit làm **subnet_id**) ≤ (số bit làm host_id)-2.




Hình 3.6 – Số lượng **Subnet** tối đa được phép

Số lượng host trong mỗi mạng con được xác định bằng số bit trong phần host_id; $2^x - 2$ là số địa chỉ hợp lệ có thể đặt cho các host trong mạng con. Tương tự, số bit trong phần **subnet_id** xác định số lượng mạng con. Giả sử số bit là y ⇨ $2^y - 2$ là số lượng mạng con có được (trường hợp đặc biệt thì có thể sử dụng được $2^y$ mạng con).

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. 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). 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**).



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

+ 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.8. Địa chỉ riêng (private address) và cơ chế chuyển đổi địa chỉ mạng (Network Address Translation - NAT)

Tất cả các IP host khi kết nối vào mạng Internet đều phải có một địa chỉ IP do tổ chức IANA (**Internet Assigned Numbers Authority**) cấp phát – gọi là địa chỉ hợp lệ (hay là được đăng ký). Tuy nhiên số lượng host kết nối vào mạng ngày càng gia tăng dẫn đến tình trạng khan hiếm địa chỉ IP. Một giải pháp đưa ra là sử dụng cơ chế NAT kèm theo là RFC 1918 qui định danh sách địa chỉ riêng. Các địa chỉ này sẽ không được IANA cấp phát - hay còn gọi là địa chỉ không hợp lệ. Bảng sau liệt kê danh sách các địa chỉ này:

| Nhóm địa chỉ | Lớp | Số lượng mạng |
|---|---|---|
| 10.0.0.0 đến 10.255.255.255 | A | 1 |
| 172.16.0.0 đến 172.31.255.255 | B | 16 |
| 192.168.0.0 đến 192.168.255.255 | C | 256 |

## III.9. Cơ chế NAT

**NAT** được sử dụng trong thực tế là tại một thời điểm, tất cả các host trong một mạng **LAN** thường không truy xuất vào Internet đồng thời, chính vì vậy ta không cần phải sử dụng một số lượng tương ứng địa chỉ IP hợp lệ. **NAT** cũng được sử dụng khi nhà cung cấp dịch vụ Internet (ISP) cung cấp số lượng địa chỉ IP hợp lệ ít hơn so với số máy cần truy cập Internet. **NAT** được sử dụng trên các router đóng vai trò là gateway cho một mạng. Các host bên trong mạng **LAN** sẽ sử dụng một lớp địa chỉ riêng thích hợp. Còn danh sách các địa chỉ IP hợp lệ sẽ được cấu hình trên **Router NAT**. Tất cả các packet của các host bên trong mạng **LAN** khi gửi đến một host trên Internet đều được router **NAT** phân tích và chuyển đổi các địa chỉ riêng có trong packet thành một địa chỉ hợp lệ trong danh sách rồi mới chuyển đến host đích nằm trên mạng Internet. Sau đó nếu có một packet gửi cho một host bên trong mạng **LAN** thì **Router NAT** cũng chuyển đổi địa chỉ đích thành địa chỉ riêng của host đó rồi mới chuyển cho host ở bên trong mạng **LAN**.

Một cơ chế mở rộng của **NAT** là **PAT** (**Port Address Translation**) cũng dùng cho mục đích tương ứng. Lúc này thay vì chỉ chuyển đổi địa chỉ IP thì cả địa chỉ cổng dịch vụ (port) cũng được chuyển đổi (do **Router NAT** quyết định).

# IV. MỘT SỐ CÂU HỎI THƯỜNG ĐẶT RA KHI LÀM VIỆC VỚI ĐỊA CHỈ IP.

## IV.1. Ví dụ 1.

**Người ta ghi nhận được địa chỉ IP của một host như sau: 172.29.32.30/255.255.240.0, hãy trả lời các câu hỏi sau:**

- Hãy cho biết mạng chứa host đó có chia mạng con hay không? Nếu có thì cho biết có bao nhiêu mạng con tương tự như vậy? Và có bao nhiêu host trong mỗi mạng con?



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

- Hãy cho biết host nằm trong mạng có địa chỉ là gì?



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

- Hãy cho biết địa chỉ broadcast dùng cho mạng đó?
- Liệt kê danh sách các địa chỉ host nằm chung mạng con với host trên.

Hướng dẫn trả lời:

**Hãy cho biết mạng chứa host đó có chia mạng con hay không? Nếu có thì cho biết có bao nhiêu mạng con tương tự như vậy? Và có bao nhiêu host trong mỗi mạng con?**

1. Xác định lớp địa chỉ ⇨ xác định mặt nạ mặc định của lớp, so khớp với mặt nạ của địa chỉ ⇨ kết luận có chia mạng con hay không?
2. Xác định số bit trong subnet_id = ***x*** ⇨ số mạng con = $2^x-2$.
3. Xác định số bit trong host_id = ***y*** ⇨ số host trong mạng con = $2^y-2$.

   ⇨ Như vậy, Host này có địa chỉ IP thuộc lớp B, trong khi subnet mask của Host lại là 255.255.240.0 (khác với subnet mask mặc định của lớp B) ⇨ nên host trên nằm trong mạng có chia mạng con.

| | | | | | | |
|---|---|---|---|---|---|---|
| Subnet mask mặc định của lớp B | 255.255.0.0 | = | 11111111 | 11111111 | 00000000 | 00000000 |
| Subnet mask của Host | 255.255.240.0 | = | 11111111 | 11111111 | **1111**0000 | 00000000 |

   ⇨ So sánh số bit dùng làm subnet mask của Host với số bit dùng làm subnet mask mặc định của lớp B, sẽ có được số bit dùng làm subnet_id là 4 bit. Nên số bit dùng làm host_id sẽ là (16-4) = 12 bit.

   ⇨ Số mạng con tương tự là 14.

   ⇨ Số host trong mỗi mạng con là 4094.

**Hãy cho biết host nằm trong mạng có địa chỉ là gì?**

1. Duyệt mặt nạ mạng con và địa chỉ IP theo từng byte tương ứng, từ trái qua phải.
   + Byte nào của subnet mask mang giá trị 255 thì ghi lại byte tương ứng của địa chỉ IP.
   + Byte nào của subnet mask là 0 thì ghi lại byte tương ứng ở địa chỉ IP là 0.
   + Nếu giá trị của byte nào ở subnet mask khác 255 và 0 thì để trống byte tương ứng ở địa chỉ IP và gọi byte này là **số khó chịu**.
2. Tìm số cơ sở = 256-số khó chịu.
3. Tìm bội số lớn nhất của số cơ sở nhưng bội số này phải bé hơn hoặc bằng số tương ứng trong địa chỉ IP và ghi lại số này.

   ⇨ 172.29.___.0. **Số khó chịu** = 240.

   ⇨ **Số cơ sở** = 256 – 240 = 16.

   ⇨ Bội số của 16 lớn nhất nhưng bé hơn hoặc bằng 32 là 32

   ⇨ địa chỉ đường mạng cần tìm là 172.29.32.0.

**Hãy cho biết địa chỉ broadcast dùng cho mạng đó?**



1. Duyệt mặt nạ mạng con và địa chỉ IP theo từng byte tương ứng, từ trái qua phải.

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

+ Byte nào của subnet mask mang giá trị 255 thì ghi lại byte tương ứng của địa chỉ IP,
+ Byte nào của subnet mask là 0 thì ghi vào byte tương ứng của địa chỉ IP là 255
+ Nếu byte của subnet mask có giá trị khác 255 và 0 thì để trống byte tương ứng ở địa chỉ IP và gọi byte này là **số khó chịu**.

2. Tìm số cơ sở = 256 - số khó chịu.
3. Tìm bội số nhỏ nhất của **số cơ sở** nhưng bội số này phải lớn hơn số tương ứng trong địa chỉ IP, đem số này trừ đi 1 thì được kết quả.

   - 172.29.___.255. **Số khó chịu** = 240.
   - **Số cơ sở** = 256 – 240 = 16.
   - Bội số nhỏ nhất của 16 nhưng lớn hơn 32 là 48. 48 – 1 =47
   - Địa chỉ broadcast cần tìm là 172.29.47.255.

**Liệt kê danh sách các địa chỉ host nằm chung mạng con với host trên?**

Các địa chỉ host hợp lệ có thể đặt cho các host nằm chung mạng con với host ở trên là: các địa chỉ sau địa chỉ mạng và trước địa chỉ broadcast.

- Các địa chỉ từ 172.29.32.1 đến 172.29.47.254.

## IV.2. Ví dụ 2.

**Cho host có địa chỉ 10.8.100.49/19. Hãy trả lời các câu hỏi trên cho host này.**

- **Subnet mask** là 19 bit hay 255.255.224.0 ⇨ có chia mạng con. Số bit trong subnet_id là 11 ⇨ số subnet = $2^{11}$-2 = 2046. Số bit trong host_id là 13 ⇨ số host hợp lệ = $2^{13}$ – 2 = 8190.
- Địa chỉ mạng: 10.8.___.0. **Số khó chịu** = 224 ⇨ **Số cơ sở** = 256 – 224 = 32. Bội số lớn nhất của 32 nhưng bé hơn 100 là 96 ⇨ địa chỉ mạng là 10.8.96.0.
- Địa chỉ broadcast: 10.8.127.255.
- Các địa chỉ hợp lệ của mạng con: 10.8.96.1 đến 10.8.127.254



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

# Tóm tắt

Lý thuyết 6 tiết - Thực hành 10 tiết

| Mục tiêu | Các mục chính | Bài tập bắt buộc | Bài tập làm thêm |
|---|---|---|---|
| Kết thúc bài học này cung cấp học viên kiến thức về các môi trường truyền dẫn, chức năng và mô hình hoạt động của các thiết bị mạng… | I. Giới thiệu về môi trường truyền dẫn.<br>II. Các loại cáp mạng.<br>III. Đường truyền vô tuyến.<br>IV. Các thiết bị mạng | Dựa vào bài tập môn mạng máy tính. | Dựa vào bài tập môn mạng máy tính. |



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

# I. GIỚI THIỆU VỀ MÔI TRƯỜNG TRUYỀN DẪN

## I.1. Khái niệm

Trên một mạng máy tính, các dữ liệu được truyền trên một môi trường truyền dẫn (**transmission media**), nó là phương tiện vật lý cho phép truyền tải tín hiệu giữa các thiết bị. Có hai loại phương tiện truyền dẫn chủ yếu:

- Hữu tuyến (**bounded media**)
- Vô tuyến (**boundless media**)

Thông thường hệ thống mạng sử dụng hai loại tín hiệu là: digital và analog.

## I.2. Tần số truyền thông

Phương tiện truyền dẫn giúp truyền các tín hiệu điện tử từ máy tính này sang máy tính khác. Các tín hiệu điện tử này biểu diễn các giá trị dữ liệu theo dạng các xung nhị phân (bật/tắt). Các tín hiệu truyền thông giữa các máy tính và các thiết bị là các dạng sóng điện từ trải dài từ tần số radio đến tần số hồng ngoại.

Các sóng tần số radio thường được dùng để phát tín hiệu LAN. Các tần số này có thể được dùng với cáp xoắn đôi, cáp đồng trục hoặc thông qua việc truyền phủ sóng radio.

Sóng viba (**microware**) thường dùng truyền thông tập trung giữa hai điểm hoặc giữa các trạm mặt đất và các vệ tinh, ví dụ như mạng điện thoại cellular.

Tia hồng ngoại thường dùng cho các kiểu truyền thông qua mạng trên các khoảng cách tương đối ngắn và có thể phát được sóng giữa hai điểm hoặc từ một điểm phủ sóng cho nhiều trạm thu. Chúng ta có thể truyền tia hồng ngoại và các tần số ánh sáng cao hơn thông qua cáp quang.

## I.3. Các đặc tính của phương tiện truyền dẫn

Mỗi phương tiện truyền dẫn đều có những tính năng đặc biệt thích hợp với mỗi kiểu dịch vụ cụ thể, nhưng thông thường chúng ta quan tâm đến những yếu tố sau:

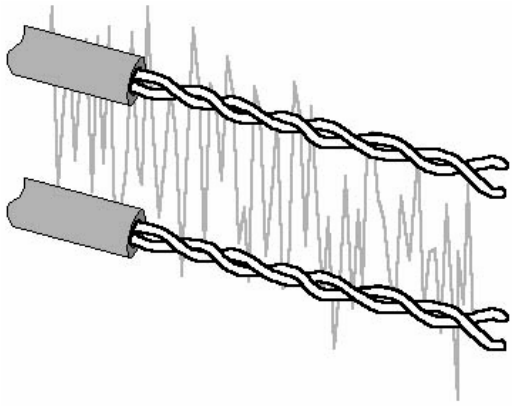
- Chi phí
- Yêu cầu cài đặt
- Độ bảo mật
- Băng thông (**bandwidth**): được xác định bằng tổng lượng thông tin có thể truyền dẫn trên đường truyền tại một thời điểm. Băng thông là một số xác định, bị giới hạn bởi phương tiện truyền dẫn, kỹ thuật truyền dẫn và thiết bị mạng được sử dụng. Băng thông là một trong những thông số dùng để phân tích độ hiệu quả của đường mạng. Đơn vị của băng thông:



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

+ Bps (**Bits per second**-số bit trong một giây): đây là đơn vị cơ bản của băng thông.
+ KBps (**Kilobits per second**): 1 KBps=$10^3$ bps=1000 Bps
+ MBps (**Megabits per second**): 1 MBps = $10^3$ KBps
+ GBps (**Gigabits per second**): 1 GBps = $10^3$ MBps
+ TBps (**Terabits per second**): 1 TBps = $10^3$ GBPS.

- Thông lượng (**Throughput**): lượng thông tin thực sự được truyền dẫn trên thiết bị tại một thời điểm.
- Băng tầng cơ sở (**baseband**): dành toàn bộ băng thông cho một kênh truyền, băng tầng mở rộng (**broadband**):cho phép nhiều kênh truyền chia sẻ một phương tiện truyền dẫn (chia sẻ băng thông).
- Độ suy giảm (**attenuation**): độ đo sự suy yếu đi của tín hiệu khi di chuyển trên một phương tiện truyền dẫn. Các nhà thiết kế cáp phải chỉ định các giới hạn về chiều dài dây cáp vì khi cáp dài sẽ dẫn đến tình trạng tín hiệu yếu đi mà không thể phục hồi được.
- Nhiễu điện từ (**Electromagnetic interference - EMI**): bao gồm các nhiễu điện từ bên ngoài làm biến dạng tín hiệu trong một phương tiện truyền dẫn.
- Nhiễu xuyên kênh (**crosstalk**): hai dây dẫn đặt kề nhau làm nhiễu lẫn nhau.



Hình 4.1 – Mô phỏng trường hợp nhiễu xuyên kênh (**crosstalk**)

## I.4. Các kiểu truyền dẫn.

Có các kiểu truyền dẫn như sau:



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

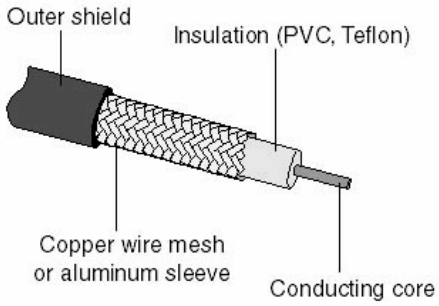
+ Đơn công (**Simplex**): trong kiểu truyền dẫn này, thiết bị phát tín hiệu và thiết bị nhận tín hiệu được phân biệt rõ ràng, thiết bị phát chỉ đảm nhiệm vai trò phát tín hiệu, còn thiết bị thu chỉ đảm nhiệm vai trò nhận tín hiệu. Truyền hình là một ví dụ của kiểu truyền dẫn này.
+ Bán song công (**Half-Duplex**): trong kiểu truyền dẫn này, thiết bị có thể là thiết bị phát, vừa là thiết bị thu. Nhưng tại một thời điểm thì chỉ có thể ở một trạng thái (phát hoặc thu). Bộ đàm là thiết bị hoạt động ở kiểu truyền dẫn này.
+ Song công (**Full-Duplex**): trong kiểu truyền dẫn này, tại một thời điểm, thiết bị có thể vừa phát vừa thu. Điện thoại là một minh họa cho kiểu truyền dẫn này.

# II. CÁC LOẠI CÁP.

## II.1. Cáp đồng trục (coaxial).

Là kiểu cáp đầu tiên được dùng trong các **LAN**, cấu tạo của cáp đồng trục gồm:

- Dây dẫn trung tâm: dây đồng hoặc dây đồng bện.
- Một lớp cách điện giữa dây dẫn phía ngoài và dây dẫn phía trong.
- Dây dẫn ngoài: bao quanh dây dẫn trung tâm dưới dạng dây đồng bện hoặc lá. Dây này có tác dụng bảo vệ dây dẫn trung tâm khỏi nhiễu điện từ và được nối đất để thoát nhiễu.
- Ngoài cùng là một lớp vỏ **plastic** bảo vệ cáp.




Hình 4.2 – Chi tiết cáp đồng trục

Ưu điểm của cáp đồng trục: là rẻ tiền, nhẹ, mềm và dễ kéo dây.

Cáp mỏng (**thin cable/thinnet**): có đường kính khoảng 6mm, thuộc họ RG-58, chiều dài đường chạy tối đa là 185 m.

- Cáp RC-58, trở kháng 50 ohm dùng với Ethernet mỏng.
- Cáp RC-59, trở kháng 75 ohm dùng cho truyền hình cáp.
- Cáp RC-62, trở kháng 93 ohm dùng cho ARCnet.

Cáp dày (**thick cable/thicknet**): có đường kính khoảng 13mm thuộc họ RG-58, chiều dài đường chạy tối đa 500m.




Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Hình 4.3 – So sánh cáp đồng trục: **Thicknet** và **Thinnet.**

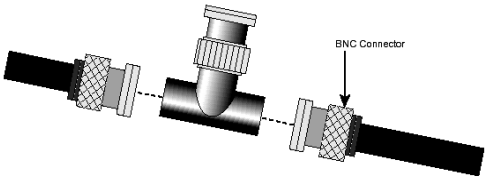


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

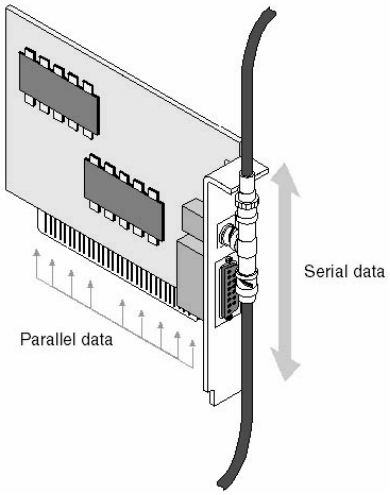
So sánh giữa cáp đồng trục mỏng và đồng trục dày:

- Chi phí: cáp đồng trục thinnet rẻ nhất, cáp đồng trục **thicknet** đắt hơn.
- Tốc độ: mạng Ethernet sử dụng cáp thinnet có tốc độ tối đa 10Mbps và mạng ARCNet có tốc độ tối đa 2.5Mbps.
- **EMI**: có lớp chống nhiễu nên hạn chế được nhiễu.
- Có thể bị nghe trộm tín hiệu trên đường truyền.

Cách lắp đặt dây: muốn nối các đoạn cáp đồng trục mỏng lại với nhau ta dùng đầu nối chữ T và đầu **BNC** như hình vẽ.




Hình 4.4 – Đầu nối BNC và đầu nối  chữ T

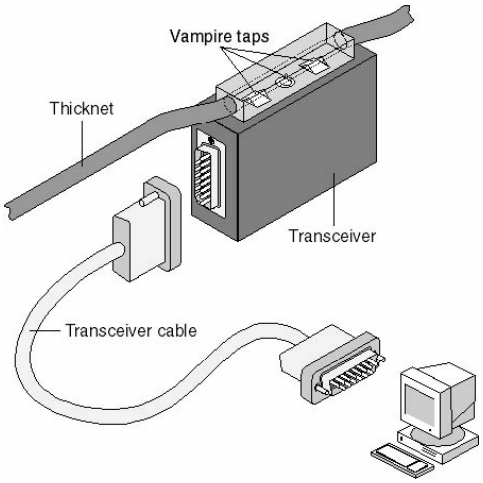



Hình 4.5 – Đầu chuyển đổi (gắn vào máy tính)

Muốn đấu nối cáp đồng trục dày ta phải dùng một đầu chuyển đổi **transceiver** và nối kết vào máy tính thông qua cổng **AUI**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 4.6 – Kết nối cáp **Thicknet** vào máy tính.

## II.2. Cáp xoắn đôi.


Hình 4.7 – Mô tả cáp xoắn đôi

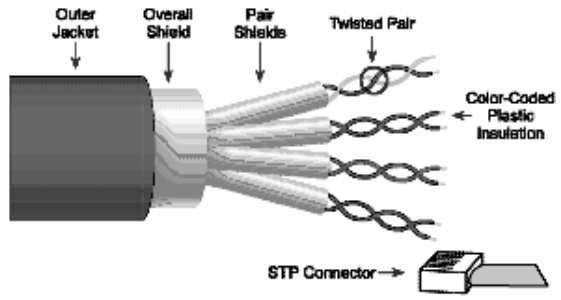
Cáp xoắn đôi gồm nhiều cặp dây đồng xoắn lại với nhau nhằm chống phát xạ nhiễu điện từ. Do giá thành thấp nên cáp xoắn được dùng rất rộng rãi. Có hai loại cáp xoắn đôi được sử dụng rộng rãi trong LAN là: loại có vỏ bọc chống nhiễu và loại không có vỏ bọc chống nhiễu.

**Cáp xoắn đôi có vỏ bọc chống nhiễu STP (Shielded Twisted- Pair).**

- Gồm nhiều cặp xoắn được phủ bên ngoài một lớp vỏ làm bằng dây đồng bện. Lớp vỏ này có tác dụng chống **EMI** từ ngoài và chống phát xạ nhiễu bên trong. Lớp vỏ bọc chống nhiễu này được nối đất để thoát nhiễu. Cáp xoắn đôi có bọc ít bị tác động bởi nhiễu điện và truyền tín hiệu xa hơn cáp xoắn đôi trần.
- Chi phí: đắt tiền hơn **Thinnet** và **UTP** nhưng lại rẻ tiền hơn **Thicknet** và cáp quang.
- Tốc độ: tốc độ lý thuyết 500Mbps, thực tế khoảng 155Mbps, với đường chạy 100m; tốc độ phổ biến 16Mbps (Token Ring).
- Độ suy dần: tín hiệu yếu dần nếu cáp càng dài, thông thường chiều dài cáp nên ngắn hơn 100m.
- Đầu nối: STP sử dụng đầu nối DIN (DB –9).



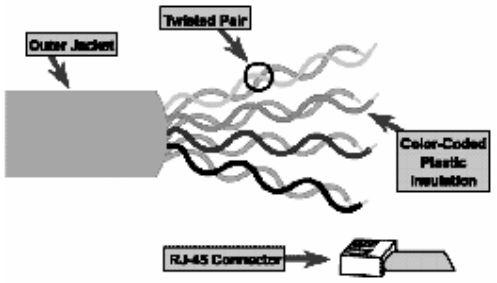
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 4.8 – Mô tả cáp STP.

**Cáp xoắn đôi không có vỏ bọc chống nhiễu UTP (Unshielded Twisted- Pair).**

Gồm nhiều cặp xoắn như cáp **STP** nhưng không có lớp vỏ đồng chống nhiễu. Cáp xoắn đôi trần sử dụng chuẩn 10BaseT hoặc 100BaseT. Do giá thành rẻ nên đã nhanh chóng trở thành loại cáp mạng cục bộ được ưu chuộng nhất. Độ dài tối đa của một đoạn cáp là 100 mét. Do không có vỏ bọc chống nhiễu nên cáp **UTP** dễ bị nhiễu khi đặt gần các thiết bị và cáp khác do đó thông thường dùng để đi dây trong nhà. Đầu nối dùng đầu RJ-45.




Hình 4.9 – Mô tả cáp UTP

Cáp UTP có năm loại:

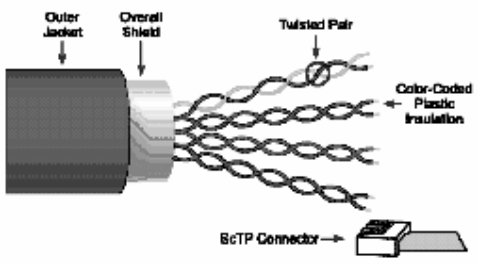
- Loại 1: truyền âm thanh, tốc độ < 4Mbps.
- Loại 2: cáp này gồm bốn dây xoắn đôi, tốc độ 4Mbps.
- Loại 3: truyền dữ liệu với tốc độ lên đến 10 Mbps. Cáp này gồm bốn dây xoắn đôi với ba mắt xoắn trên mỗi **foot** ( **foot** là đơn vị đo chiều dài, 1 foot = 0.3048 mét).
- Loại 4: truyền dữ liệu, bốn cặp xoắn đôi, tốc độ đạt được 16 Mbps.
- Loại 5: truyền dữ liệu, bốn cặp xoắn đôi, tốc độ 100Mbps.

**Cáp xoắn có vỏ bọc ScTP-FTP (Screened Twisted-pair).**

**FTP** là loại cáp lai tạo giữa cáp **UTP** và **STP**, nó hỗ trợ chiều dài tối đa 100m.



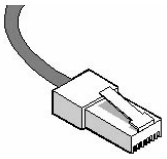
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net



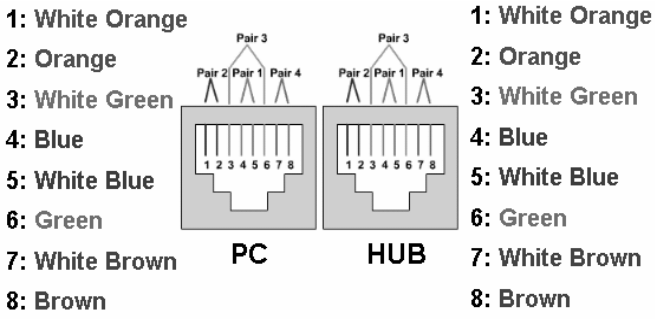

Hình 4.10 – Mô tả cáp FTP

**Các kỹ thuật bấm cáp mạng.**

- Cáp thẳng (**Straight-through cable**): là cáp dùng để nối PC và các thiết bị mạng như **Hub**, **Switch**, **Router**… Cáp thẳng theo chuẩn 10/100 Base-T dùng hai cặp dây xoắn nhau và dùng chân 1, 2, 3, 6 trên đầu RJ45. Cặp dây xoắn thứ nhất nối vào chân 1, 2, cặp xoắn thứ hai nối vào chân 3, 6. Đầu kia của cáp dựa vào màu nối vào chân của đầu RJ45 và nối tương tự.

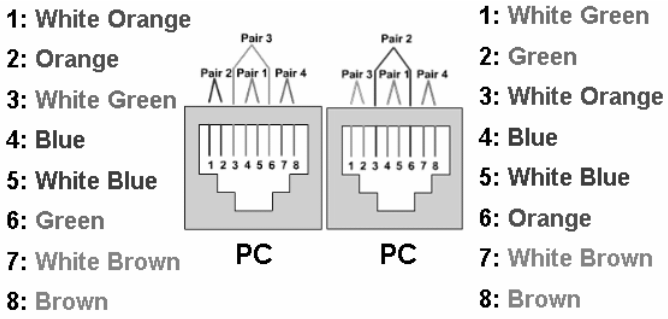


Hình 4.11 – Đầu RJ45.




Hình 4.12 – Cách đấu dây thẳng.

- Cáp chéo (**Crossover cable**): là cáp dùng nối trực tiếp giữa hai thiết bị giống nhau như **PC – PC**, **Hub – Hub**, **Switch – Switch**. Cáp chéo trật tự dây cũng giống như cáp thẳng nhưng đầu dây còn lại phải chéo cặp dây xoắn sử dụng (vị trí thứ nhất đổi với vị trí thứ 3, vị trí thứ hai đổi với vị trí thứ sáu) .






Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Hình 4.13 – Cách đấu dây chéo.

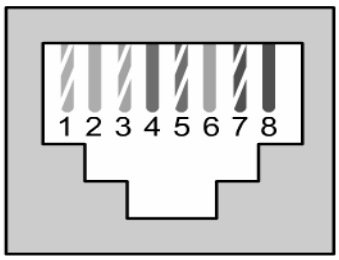


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

- Cáp **Console**: dùng để nối PC vào các thiết bị mạng chủ yếu dùng để cấu hình các thiết bị. Thông thường khoảng cách dây **Console** ngắn nên chúng ta không cần chọn cặp dây xoắn, mà chọn theo màu từ 1-8 sao cho dễ nhớ và đầu bên kia ngược lại từ 8-1.

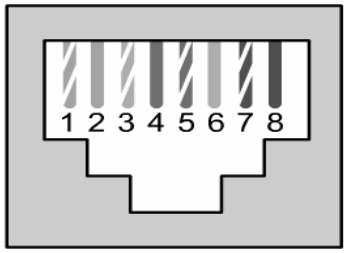
**ANSI** (Viện tiêu chuẩn quốc gia Hoa kỳ), **TIA** (hiệp hội công nghiệp viễn thông), **EIA** (hiệp hội công nghiệp điện tử) đã đưa ra 2 cách xếp đặt vị trí dây như sau:

- Chuẩn T568-A (còn gọi là Chuẩn A):



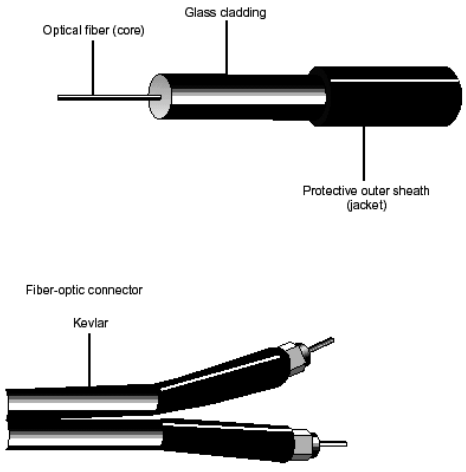

1. Trắng Xanh lá cây (White Green)
2. Xanh lá cây (Green)
3. Trắng Cam (White Orange)
4. Xanh đậm (Blue)
5. Trắng Xanh đậm (White Blue)
6. Cam (Orange)
7. Trắng Nâu (White Brown)
8. Nâu (Brown)

- Chuẩn T568-B (còn gọi là Chuẩn B):




1. Trắng Cam (White Orange)
2. Cam (Orange)
3. Trắng Xanh lá cây (White Green)
4. Xanh đậm (Blue)
5. Trắng Xanh đậm (White Blue)
6. Xanh lá cây (Green)
7. Trắng Nâu (White Brown)
8. Nâu (Brown)

## II.3. Cáp quang (Fiber-optic cable).




Hình 4.14 – Mô tả cáp quang.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Cáp quang có cấu tạo gồm dây dẫn trung tâm là sợi thủy tinh hoặc plastic đã được tinh chế nhằm cho phép truyền đi tối đa các tín hiệu ánh sáng. Sợi quang được tráng một lớp nhằm phản chiếu các tín hiệu. Cáp quang chỉ truyền sóng ánh sáng (không truyền tín hiệu điện) với băng thông rất cao nên không gặp các sự cố về nhiễu hay bị nghe trộm. Cáp dùng nguồn sáng laser, diode phát xạ ánh sáng. Cáp rất bền và độ suy giảm tín hiệu rất thấp nên đoạn cáp có thể dài đến vài km. Băng thông cho phép đến 2Gbps. Nhưng cáp quang có khuyết điểm là giá thành cao và khó lắp đặt. Các loại cáp quang:

- Loại lõi 8.3 micron, lớp lót 125 micron, chế độ đơn.
- Loại lõi 62.5 micron, lớp lót 125 micron, đa chế độ.
- Loại lõi 50 micron, lớp lót 125 micron, đa chế độ.
- Loại lõi 100 micron, lớp lót 140 micron, đa chế độ.

Hộp đấu nối cáp quang: do cáp quang không thể bẻ cong nên khi nối cáp quang vào các thiết bị khác chúng ta phải thông qua hộp đấu nối.


Hình 4.15 – Mô tả hộp đấu nối cáp quang.

Đầu nối cáp quang: đầu nối cáp quang rất đa dạng thông thường trên thị trường có các đầu nối như sau: **FT**, **ST**, **FC**…


Hình 4.16 – Một số loại đầu nối cáp quang.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

# III. ĐƯỜNG TRUYỀN VÔ TUYẾN.

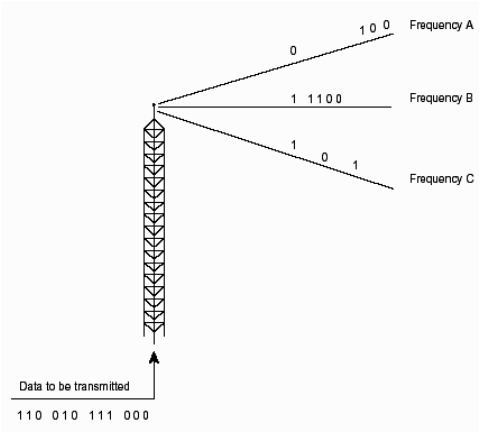
Khi dùng các loại cáp ta gặp một số khó khăn như cơ sở cài đặt cố định, khoảng cách không xa, vì vậy để khắc phục những khuyết điểm trên người ta dùng đường truyền vô tuyến. Đường truyền vô tuyến mang lại những lợi ích sau:

- Cung cấp nối kết tạm thời với mạng cáp có sẵn.
- Những người liên tục di chuyển vẫn nối kết vào mạng dùng cáp.
- Lắp đặt đường truyền vô tuyến ở những nơi địa hình phức tạp không thể đi dây được.
- Phù hợp cho những nơi phục vụ nhiều kết nối cùng một lúc cho nhiều khách hàng. Ví dụ như: dùng đường vô tuyến cho phép khách hàng ở sân bay kết vào mạng để duyệt Internet.
- Dùng cho những mạng có giới hạn rộng lớn vượt quá khả năng cho phép của cáp đồng và cáp quang.
- Dùng làm kết nối dự phòng cho các kết nối hệ thống cáp.

Tuy nhiên, đường truyền vô tuyến cũng có một số hạn chế:

- Tín hiệu không an toàn.
- Dễ bị nghe lén.
- Khi có vật cản thì tín hiệu suy yếu rất nhanh.
- Băng thông không cao.

## III.1. Sóng vô tuyến (radio).




Hình 4.16 – Truyền dữ liệu qua sóng vô tuyến.

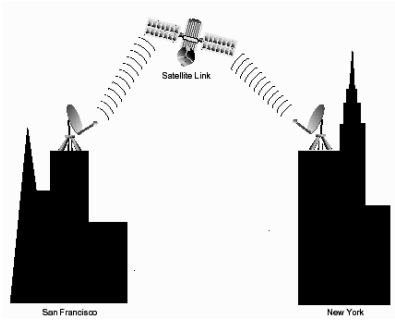
Sóng **radio** nằm trong phạm vi từ 10 KHz đến 1 GHz, trong miền này ta có rất nhiều dải tần ví dụ như: sóng ngắn, **VHF** (dùng cho tivi và radio FM), **UHF** (dùng cho tivi). Tại mỗi quốc gia, nhà nước sẽ quản lý cấp phép sử dụng các băng tần để tránh tình trạng các sóng bị nhiễu. Nhưng có một số băng tần được chỉ định là vùng tự do có nghĩa là chúng ta dùng nhưng không cần đăng ký (vùng này thường có dải tần 2,4 Ghz). Tận dụng lợi điểm này các thiết bị Wireless của các hãng như **Cisco**, **Compex** đều dùng ở dải tần này. Tuy nhiên, chúng ta sử dụng tần số không cấp phép sẽ có nguy cơ nhiễu nhiều hơn.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

## III.2. Sóng viba.

Truyền thông viba thường có hai dạng: truyền thông trên mặt đất và các nối kết với vệ tinh. Miền tần số của viba mặt đất khoảng 21-23 GHz, các kết nối vệ tinh khoảng 11-14 Mhz. Băng thông từ 1-10 MBps. Sự suy yếu tín hiệu tùy thuộc vào điều kiện thời tiết, công suất và tần số phát. Chúng dễ bị nghe trộm nên thường được mã hóa.




Hình 4.17 – Truyền dữ liệu thông qua vệ tinh.

Hình 4.18 – Truyền dữ liệu trực tiếp giữa hai thiết bị.

## III.3. Hồng ngoại.

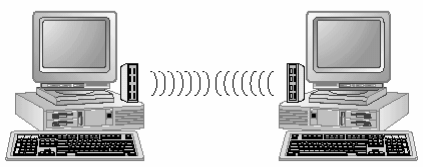
Tất cả mạng vô tuyến hồng ngoại đều hoạt động bằng cách dùng tia hồng ngoại để truyền tải dữ liệu giữa các thiết bị. Phương pháp này có thể truyền tín hiệu ở tốc độ cao do dải thông cao của tia hồng ngoại. Thông thường mạng hồng ngoại có thể truyền với tốc độ từ 1-10 Mbps. Miền tần số từ 100 Ghz đến 1000 GHz. Có bốn loại mạng hồng ngoại:

- Mạng đường ngắm: mạng này chỉ truyền khi máy phát và máy thu có một đường ngắm rõ rệt giữa chúng.
- Mạng hồng ngoại tán xạ: kỹ thuật này phát tia truyền dội tường và sàn nhà rồi mới đến máy thu. Diện tích hiệu dụng bị giới hạn ở khoảng 100 feet (35m) và có tín hiệu chậm do hiện tượng dội tín hiệu.
- Mạng phản xạ: ở loại mạng hồng ngoại này, máy thu-phát quang đặt gần máy tính sẽ truyền tới một vị trí chung, tại đây tia truyền được đổi hướng đến máy tính thích hợp.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

- **Broadband optical telepoint**: loại mạng cục bộ vô tuyến hồng ngoại cung cấp các dịch vụ đài rộng. Mạng vô tuyến này có khả năng xử lý các yêu cầu đa phương tiện chất lượng cao, vốn có thể trùng khớp với các yêu cầu đa phương tiện của mạng cáp.



Hình 4.19 – Truyền dữ liệu giữa 2 máy tính thông qua hồng ngoại.

# IV. CÁC THIẾT BỊ MẠNG.

## IV.1. Card mạng (NIC hay Adapter).

Card mạng là thiết bị nối kết giữa máy tính và cáp mạng. Chúng thường giao tiếp với máy tính qua các khe cắm như: **ISA**, **PCI** hay **USP**… Phần giao tiếp với cáp mạng thông thường theo các chuẩn như: **AUI**, **BNC**, **UTP**… Các chức năng chính của card mạng:

- Chuẩn bị dữ liệu đưa lên mạng: trước khi đưa lên mạng, dữ liệu phải được chuyển từ dạng byte, bit sang tín hiệu điện để có thể truyền trên cáp.
- Gởi dữ liệu đến máy tính khác.
- Kiểm soát luồng dữ liệu giữa máy tính và hệ thống cáp.

Địa chỉ **MAC** (**Media Access Control**): mỗi card mạng có một địa chỉ riêng dùng để phân biệt card mạng này với card mạng khác trên mạng. Địa chỉ này do **IEEE** – Viện Công nghệ Điện và Điện tử – cấp cho các nhà sản xuất card mạng. Từ đó các nhà sản xuất gán cố định địa chỉ này vào chip của mỗi card mạng. Địa chỉ này gồm 6 byte (48 bit), có dạng XXXXXX.XXXXXX, 3 byte đầu là mã số của nhà sản xuất, 3 byte sau là số serial của các card mạng do hãng đó sản xuất. Địa chỉ này được ghi cố định vào **ROM** nên còn gọi là địa chỉ vật lý. Ví dụ địa chỉ vật lý của một card Intel có dạng như sau: 00A0C90C4B3F.

Hình dưới là card mạng RE100TX theo chuẩn Ethernet IEEE 802.3 và IEEE 802.3u. Nó hỗ trợ cả hai băng thông 10Mbps và 100Mbps theo chuẩn 10Base-T và 100Base-TX. Ngoài ra card này còn cung cấp các tính năng như **Wake On LAN**, **Port Trunking**, hỗ trợ cơ chế truyền **full duplex**. Card này cũng hỗ trợ hai cơ chế boot ROM 16 bit (RPL) và 32 bit (PXE).

Hình 4.20 – Card RE100TX.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Hình dưới là card FL1000T 10/100/1000Mbps Gigabit Adapter, nó là card mạng theo chuẩn **Gigabit** dùng đầu nối RJ45 truyền trên môi trường cáp UTP cat 5. Card này cung cấp đường truyền với băng thông lớn và tương thích với card PCI 64 và 32 bit đồng thời nó cũng hỗ trợ cả hai cơ chế truyền **full/half duplex** trên cả ba loại băng thông 10/100/1000 Mbps.

Hình 4.21 – Card FL1000T 10/100/1000Mbps **Gigabit**.

Hình dưới là card mạng không dây WL11A 11Mbps **Wireless PCMCIA LAN Card**, card này giao tiếp với máy theo chuẩn **PCMCIA** nên khi sử dụng cho PC chúng ta phải dùng thêm card chuyển đổi từ PCI sang **PCMCIA**. Card được thiết kế theo chuẩn IEEE802.11b ở dải tần 2.4GHz ISM, dùng cơ chế **CSMA/CA** để xử lý đụng độ, băng thông của card là 11Mbps, có thể mã hóa 64 và 128 bit. Đặc biệt card này hỗ trợ cả hai kiến trúc kết nối mạng là **Infrastructure** và **AdHoc**.


Hình 4.22 – Card WL11A.

## IV.2. Card mạng dùng cáp điện thoại.

Card HP10 10Mbps **Phoneline Network Adapter** là một card mạng đặc biệt vì nó không dùng cáp đồng trục cũng không dùng cáp UTP mà dùng cáp điện thoại. Một đặc tính quan trọng của card này là truyền số liệu song song với truyền âm thanh trên dây điện thoại. Card này dùng đầu kết nối RJ11 và băng thông 10Mbps, chiều dài cáp có thể dài đến gần 300m.

Hình 4.23 - Card HP10 10Mbps **Phoneline.**

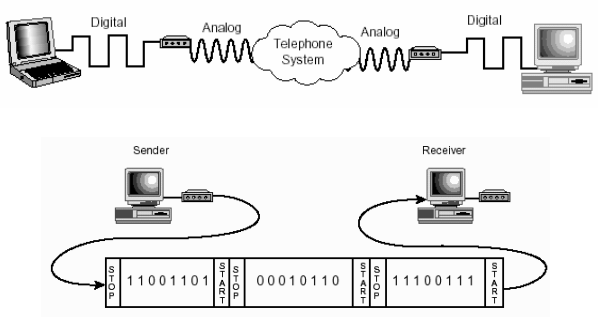


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

## IV.3. Modem.

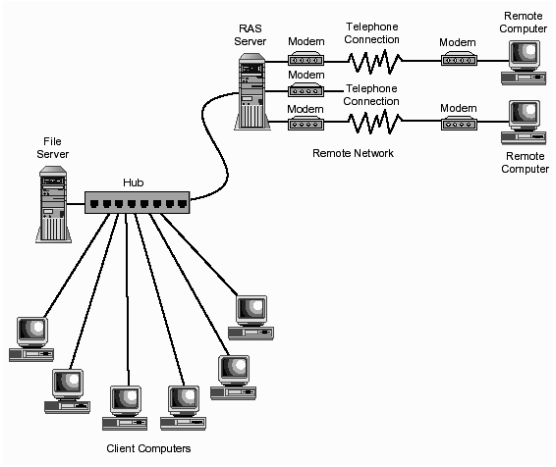
Là thiết bị dùng để nối hai máy tính hay hai thiết bị ở xa thông qua mạng điện thoại. **Modem** thường có hai loại: **internal** (là loại được gắn bên trong máy tính giao tiếp qua khe cắm **ISA** hoặc PCI), **external** (là loại thiết bị đặt bên ngoài **CPU** và giao tiếp với **CPU** thông qua cổng **COM** theo chuẩn RS-232). Cả hai loại trên đều có cổng giao tiếp RJ11 để nối với dây điện thoại.

Chức năng của **Modem** là chuyển đổi tín hiệu số (**digital**) thành tín hiệu tương tự (**analog**) để truyền dữ liệu trên dây điện thoại. Tại đầu nhận, **Modem** chuyển dữ liệu ngược lại từ dạng tín hiệu tương tự sang tín hiệu số để truyền vào máy tính. Thiết bị này giá tương đối thấp nhưng mang lại hiệu quả rất lớn. Nó giúp nối các mạng **LAN** ở xa với nhau thành các mạng **WAN**, giúp người dùng có thể hòa vào mạng nội bộ của công ty một cách dễ dàng dù người đó ở nơi nào.




Hình 4.24 – Mô hình truyền dữ liệu thông qua **Modem**.

**Remote Access Services** (**RAS**): là một dịch vụ mềm trên một máy tính hoặc là một dịch vụ trên thiết bị phần cứng. Nó cho phép dùng **Modem** để nối kết hai mạng **LAN** với nhau hoặc một máy tính vào mạng nội bộ.



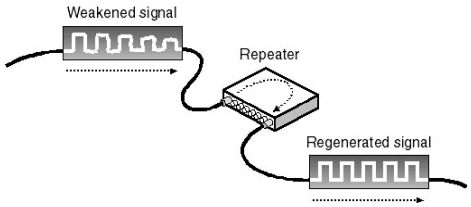

Hình 4.25 – Sử dụng **RAS** để liên lạc.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

## IV.4. Repeater.

Là thiết bị dùng để khuếch đại tín hiệu trên các đoạn cáp dài. Khi truyền dữ liệu trên các đoạn cáp dài tín hiệu điện sẽ yếu đi, nếu chúng ta muốn mở rộng kích thước mạng thì chúng ta dùng thiết bị này để khuếch đại tín hiệu và truyền đi tiếp. Nhưng chúng ta chú ý rằng thiết bị này hoạt động ở lớp vật lý trong mô hình **OSI**, nó chỉ hiểu tín hiệu điện nên không lọc được dữ liệu ở bất kỳ dạng nào, và mỗi lần khuếch đại các tín hiệu điện yếu sẽ bị sai do đó nếu cứ tiếp tục dùng nhiều **Repeater** để khuếch đại và mở rộng kích thước mạng thì dữ liệu sẽ ngày càng sai lệch.



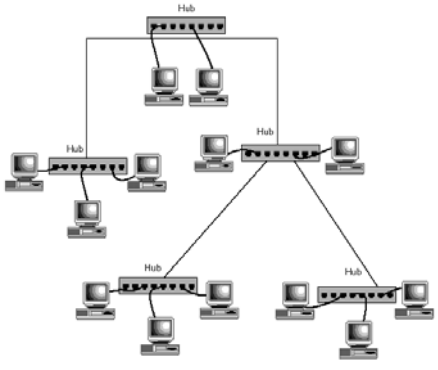

Hình 4.26 – Thiết bị **Repeater**.

## IV.5. Hub.

Là thiết bị giống như **Repeater** nhưng nhiều port hơn cho phép nhiều máy tính nối tập trung về thiết bị này. Các chức năng giống như **Repeater** dùng để khuếch đại tín hiệu điện và truyền đến tất cả các port còn lại đồng thời không lọc được dữ liệu. Thông thường **Hub** hoạt động ở lớp 1 (lớp vật lý). Toàn bộ **Hub** (hoặc **Repeater**) được xem là một **Collision Domain**.

Hub gồm có ba loại:

- **Passive Hub**: là thiết bị đấu nối cáp dùng để chuyển tiếp tín hiệu từ đoạn cáp này đến các đoạn cáp khác, không có linh kiện điện tử và nguồn riêng nên không không khuếch đại và xử lý tín hiệu;
- **Active Hub**: là thiết bị đấu nối cáp dùng để chuyển tiếp tín hiệu từ đoạn cáp này đến các đoạn cáp khác với chất lượng cao hơn. Thiết bị này có linh kiện điện tử và nguồn điện riêng nên hoạt động như một repeater có nhiều cổng (**port**);
- **Intelligent Hub**: là một **active hub** có thêm các chức năng vượt trội như cho phép quản lý từ các máy tính, chuyển mạch (**switching**), cho phép tín hiệu điện chuyển đến đúng port cần nhận không chuyển đến các port không liên quan.




Hình 4.27 – Mô hình mạng sử dụng **Hub**.



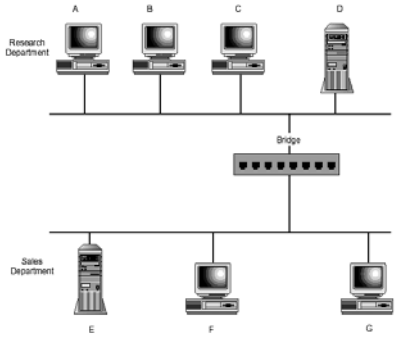
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

## IV.6. Bridge (cầu nối).

Là thiết bị cho phép nối kết hai nhánh mạng, có chức năng chuyển có chọn lọc các gói tin đến nhánh mạng chứa máy nhận gói tin. Trong **Bridge** có bảng địa chỉ **MAC**, bảng địa chỉ này sẽ được dùng để quyết định đường đi của gói tin (cách thức truyền đi của một gói tin sẽ được nói rõ hơn ở trong phần trình bày về thiết bị **Switch**). Bảng địa chỉ này có thể được khởi tạo tự động hoặc phải cấu hình bằng tay. **Bridge** hoạt động ở lớp hai (lớp **Data link**) trong mô hình **OSI**.

*Ưu điểm* của **Bridge** là: cho phép mở rộng cùng một mạng logic với nhiều kiểu cáp khác nhau. Chia mạng thành nhiều phân đoạn khác nhau nhằm giảm lưu lượng trên mạng.

*Khuyết điểm*: chậm hơn **Repeater** vì phải xử lý các gói tin, chưa tìm được đường đi tối ưu trong trường hợp có nhiều đường đi. Việc xử lý gói tin dựa trên phần mềm.




Hình 4.28 – Mô hình mạng sử dụng **Bridge**.

## IV.7. Switch

Là thiết bị giống như bridge nhưng nhiều **port** hơn cho phép ghép nối nhiều đoạn mạng với nhau. **Switch** cũng dựa vào bảng địa chỉ **MAC** để quyết định gói tin nào đi ra **port** nào nhằm tránh tình trạng giảm băng thông khi số máy trạm trong mạng tăng lên. **Switch** cũng hoạt động tại lớp hai trong mô hình **OSI**. Việc xử lý gói tin dựa trên phần cứng (**chip**).

Khi một gói tin đi đến **Switch** (hoặc **Bridge**), **Switch** (hoặc **Bridge**) sẽ thực hiện như sau:

- Kiểm tra địa chỉ nguồn của gói tin đã có trong bảng **MAC** chưa, nếu chưa có thì nó sẽ thêm địa chỉ **MAC** này và **port** nguồn (nơi gói tin đi vào **Switch** (hoặc **Bridge**)) vào trong bảng **MAC**.
- Kiểm tra địa chỉ đích của gói tin đã có trong bảng **MAC** chưa:
  - + Nếu chưa có thì nó sẽ gởi gói tin ra tất cả các **port** (ngoại trừ port gói tin đi vào).
  - + Nếu địa chỉ đích đã có trong bảng **MAC**:
    - ③ Nếu port đích trùng với port nguồn thì **Switch** (hoặc **Bridge**) sẽ loại bỏ gói tin.
    - ③ Nếu port đích khác với **port** nguồn thì gói tin sẽ được gởi ra **port** đích tương ứng.

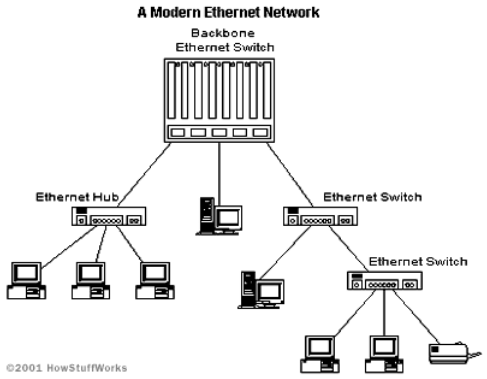
Chú ý:

- Địa chỉ nguồn và địa chỉ đích được nói ở trên đều là địa chỉ **MAC**.
- **Port** nguồn là **Port** mà gói tin đi vào.
- **Port** đích là **Port** mà gói tin đi ra.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Do cách hoạt động của **Switch** (hoặc **Bridge**) như vậy, nên mỗi **Port** của **Switch** là một **Collision Domain**, và toàn bộ **Switch** được xem là một **Broadcast Domain** (khái niệm **Collision Domain** và **Broadcast Domain** sẽ được giới thiệu trong chương 5, phần "các công nghệ mạng **LAN**").




Hình 4.29 – Mô hình mạng sử dụng **Switch**.

Ngoài các tính năng cơ sở, **Switch** còn các tính năng mở rộng như sau:

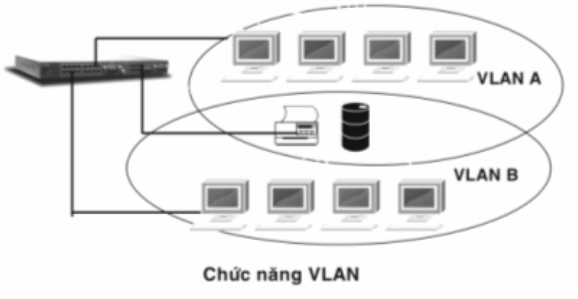
- Phương pháp chuyển gói tin (**Switching mode**): trong thiết bị của **Cisco** có thể sử dụng một trong ba loại sau:
  - + **Store and Forward**: là tính năng lưu dữ liệu trong bộ đệm trước khi truyền sang các port khác để tránh đụng độ (**collision**), thông thường tốc độ truyền khoảng 148.800 pps. Với kỹ thuật này toàn bộ gói tin phải được nhận đủ trước khi **Switch** truyền frame này đi do đó độ trễ (**latency**) lệ thuộc vào chiều dài của frame.
  - + **Cut Through**: **Switch** sẽ truyền gói tin ngay lập tức một khi nó biết được địa chỉ đích của gói tin. Kỹ thuật này sẽ có độ trễ thấp hơn so với kỹ thuật **Store and Forward** và độ trễ luôn là con số xác định, bất chấp chiều dài của gói tin.
  - + **Fragment Free**: thì **Switch** đọc 64 byte đầu tiên và sau đó bắt đầu truyền dữ liệu.
- **Trunking** (**MAC Base**): ở một số thiết bị **Switch**, tính năng **Trunking** được hiểu là tính năng giúp tăng tốc độ truyền giữa hai **Switch**, nhưng chú ý là hai **Switch** phải cùng loại. Riêng trong thiết bị **Switch** của **Cisco**, Trunking được hiểu là đường truyền dùng để mang thông tin cho các **VLAN**.


Hình 4.30 – Mô tả cách dùng đường **Trunking**.

- **VLAN**: tạo các mạng ảo, nhằm đảm bảo tính bảo mật khi mở rộng mạng bằng cách nối các **Switch** với nhau. Mỗi **VLAN** có thể được xem là một **Broadcast Domain**, nên khi chia các mạng ảo giúp ta sẽ phân vùng miền **broadcast** nhằm cải tiến tốc độ và hiệu quả của hệ thống. Nói cách khác, **VLAN** là một nhóm logic các thiết bị hoặc người sử dụng. Nhóm logic này được chia dựa vào chức năng, ứng dụng, … mà không phụ thuộc vào vị trí địa lý. Chỉ có các thiết bị trong cùng **VLAN** mới liên lạc được với nhau. Nếu muốn các **VLAN** có thể liên lạc được với nhau thì phải sử dụng **Router** để liên kết các **VLAN** lại.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net



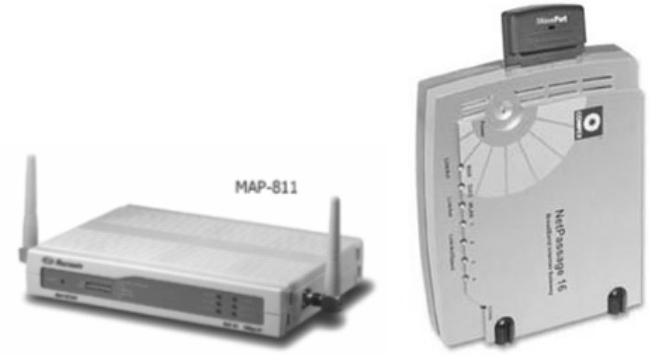

Hình 4.31 – Mô tả cách sử dụng **VLAN**.

- **Spanning Tree**: tạo đường dự phòng, bình thường dữ liệu được truyền trên một cổng mang số thứ tự thấp. Khi mất liên lạc thiết bị tự chuyển sang cổng khác, nhằm đảm bảo mạng hoạt động liên tục. **Spanning Tree** thực chất là hạn chế các đường dư thừa trên mạng.

Hình dưới là **Switch Compex** SRX2216 được thiết kế theo chuẩn IEEE 802.3, IEEE802.3u, **Switch** này thường dùng trong các giải pháp mạng vừa và nhỏ. Thiết bị này hỗ trợ 16 port RJ45 tốc độ 10/100Mbps, 12K **MAC Address**, 2K bộ đệm (**buffer**). Ngoài ra thiết bị này còn có những tính năng như: **Store and Forward**, **Spanning Tree**, **Port Trunking**, **Virtual LAN** giúp chúng ta mở rộng mạng mà không sợ xảy ra đụng độ (**collision**).

Hình 4.31 - **Switch Compex SRX2216**.

## IV.8. Wireless Access Point.




Hình 4.32 – Thiết bị Wireless

**Wireless Access Point** là thiết bị kết nối mạng không dây được thiết kế theo chuẩn IEEE802.11b, cho phép nối **LAN to LAN**, dùng cơ chế **CSMA/CA** để giải quyết tranh chấp, dùng cả hai kiến trúc kết nối mạng là **Infrastructure** và **AdHoc**, mã hóa theo 64/128 Bit. Nó còn hỗ trợ tốc độ truyền không dây lên 11Mbps trên băng tần 2,4GHz ISM dùng công nghệ **radio DSSS** (**Direct Sequence Spread Spectrum**)



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net


Hình 4.33 – Mạng sử dụng **Wireless**.

## IV.9. Router.

Là thiết bị dùng nối kết các mạng **logic** với nhau, kiểm soát và lọc các gói tin nên hạn chế được lưu lượng trên các mạng **logic** (thông qua cơ chế **Access-list**). Các **Router** dùng bảng định tuyến (**Routing table**) để lưu trữ thông tin về mạng dùng trong trường hợp tìm đường đi tối ưu cho các gói tin. Bảng định tuyến chứa các thông tin về đường đi, thông tin về ước lượng thời gian, khoảng cách… Bảng này có thể cấu hình tĩnh hay tự động. **Router** hiểu được địa chỉ logic **IP** nên thông thường **Router** hoạt động ở lớp mạng (**network**) hoặc cao hơn.

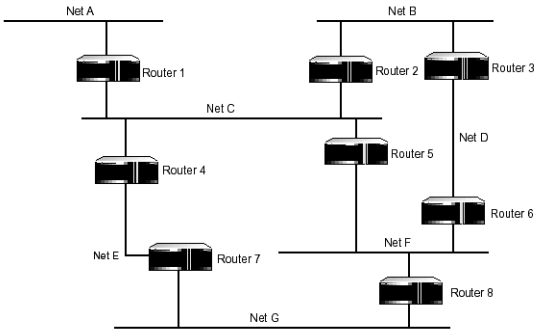
Người ta cũng có thể thực hiện **firewall** ở mức độ đơn giản trên **Router** thông qua tính năng **Access-list** (tạo một danh sách truy cập hợp lệ), thực hiện việc ánh xạ địa chỉ thông qua tính năng **NAT** (chuyển đổi địa chỉ).

Khi một gói tin đến **Router**, **Router** sẽ thực hiện các việc kiểm tra địa chỉ **IP** đích của gói tin:

- Nếu địa chỉ mạng của **IP** đích này có trong bảng định tuyến của **Router**, **Router** sẽ gởi ra port tương ứng.
- Nếu địa chỉ mạng của **IP** đích này không có trong bảng định tuyến, **Router** sẽ kiểm tra xem trong bảng định tuyến của mình có khai báo **Default Gateway** hay không:
    + Nếu có khai báo **Default Gateway** thì gói tin sẽ được **Router** đưa đến **Default Gateway** tương ứng.
    + Nếu không có khai báo **Default Gateway** thì gói tin sẽ bị loại bỏ.

Chú ý: địa chỉ được xét ở đây là địa chỉ **IP**.

Do cách hoạt động của **Router** như đã trình bày, nên mỗi **port** của **Router** là một **Broadcast Domain**.






Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Hình 4.34 – Mô hình mạng sử dụng **Router**.



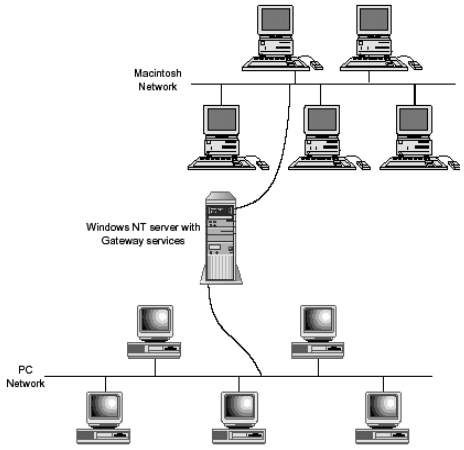
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

## IV.10. Thiết bị mở rộng.

### IV.10.1 Gateway – Proxy:

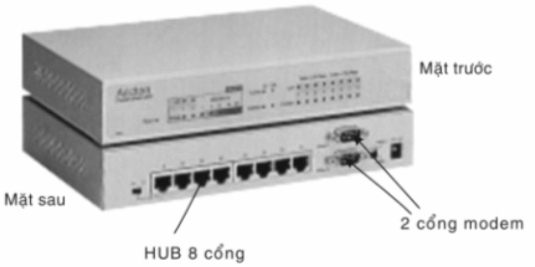
Là thiết bị trung gian dùng để nối kết mạng nội bộ bên trong và mạng bên ngoài. Nó có chức năng kiểm soát tất cả các luồng dữ liệu đi ra và vào mạng nhằm ngăn chặn **hacker** tấn công. **Gateway** cũng hỗ trợ chuyển đổi giữa các giao thức khác nhau, các chuẩn dữ liệu khác nhau (ví dụ **IP/IPX**).

**Proxy** giống như một **firewall** (bức tường lửa), nâng cao khả năng bảo mật giữa mạng nội bộ bên trong và mạng bên ngoài. **Proxy** cho phép thiết lập các danh sách được phép truy cập vào mạng nội bộ bên trong, cũng như danh sách các ứng dụng mà mạng nội bộ bên trong có thể truy cập ra mạng bên ngoài. Ngoài ra **Proxy** còn là máy đại điện cho các máy trạm bên trong mạng nội bộ truy cập ra Internet, đây là chức năng quan trọng nhất của **Proxy**.




Hình 4.35 – Mô hình mạng sử dụng **Gateway**.

### IV.10.2 Thiết bị truy cập Internet.



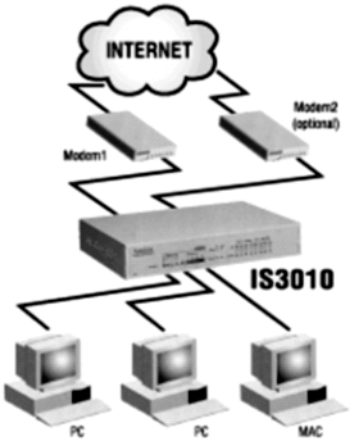

Hình 4.36 - Thiết bị IS3010

Có nhiều thiết bị dùng để truy cập **Internet**. Hình vẽ trên là một trong những thiết bị vừa cho phép chia sẻ **Internet**, vừa cho phép nâng cao tốc độ đường truyền thông qua việc sử dụng 02 modem cùng một lúc.

Ứng dụng: nhiều máy tính (**LAN**) truy cập **Internet** chung một **account** qua hai **Modem**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 4.37 – Truy cập **Internet** bằng thiết bị IS3010.

Thiết bị này cấu hình rất đơn giản dùng **Web browser**, **Telnet**, **Console**. Có hai cổng **Modem** cho phép **dial out** hoặc **dial in**, tích hợp sẵn dịch vụ **NAT**, **Default GateWay**, **DHCP** dùng cấp phát **IP** động cho các máy trạm. Hỗ trợ cả hai nghi thức thẩm định quyền truy cập **PAP/CHAP**, hỗ trợ **Filter** (cho hoặc cấm người dùng truy cập **Internet**).



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

# Tóm tắt

Lý thuyết 5 tiết - Thực hành 10 tiết

| Mục tiêu | Các mục chính | Bài tập bắt buộc | Bài tập làm thêm |
|---|---|---|---|
| Kết thúc bài học này cung cấp học viên kiến thức về các kiến trúc và công nghệ mạng LAN … | I. Các kiến trúc mạng.<br>II. Các công nghệ mạng LAN. | Dựa vào bài tập môn mạng máy tính. | Dựa vào bài tập môn mạng máy tính. |



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

# I. CÁC KIẾN TRÚC MẠNG (TOPOLOGY).

## I.1. Khái niệm.

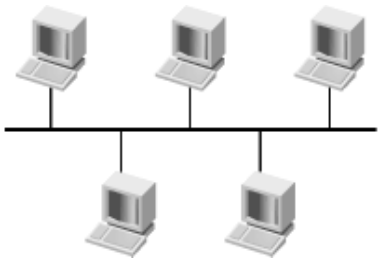
**Network topology** là sơ đồ dùng biểu diễn các kiểu sắp xếp, bố trí vật lý của máy tính, dây cáp và những thành phần khác trên mạng theo phương diện vật lý.

Có hai kiểu kiến trúc mạng chính là: kiến trúc vật lý (mô tả cách bố trí đường truyền thực sự của mạng), kiến trúc logic (mô tả con đường mà dữ liệu thật sự di chuyển qua các node mạng)

## I.2. Các kiểu kiến trúc mạng chính.

**Mạng Bus (tuyến)**

- Kiến trúc **Bus** là một kiến trúc cho phép nối mạng các máy tính đơn giản và phổ biến nhất. Nó dùng một đoạn cáp nối tất cả máy tính và các thiết bị trong mạng thành một hàng. Khi một máy tính trên mạng gởi dữ liệu dưới dạng tín hiệu điện thì tín hiệu này sẽ được lan truyền trên đoạn cáp đến các máy tính còn lại, tuy nhiên dữ liệu này chỉ được máy tính có địa chỉ so khớp với địa chỉ mã hóa trong dữ liệu chấp nhận. Mỗi lần chỉ có một máy có thể gởi dữ liệu lên mạng vì vậy số lượng máy tính trên bus càng tăng thì hiệu suất thi hành mạng càng chậm.
- Hiện tượng dội tín hiệu: là hiện tượng khi dữ liệu được gởi lên mạng, dữ liệu sẽ đi từ đầu cáp này đến đầu cáp kia. Nếu tín hiệu tiếp tục không ngừng nó sẽ dội tới lui trong dây cáp và ngăn không cho máy tính khác gởi dữ liệu. Để giải quyết tình trạng này người ta dùng một thiết bị terminator (điện trở cuối) đặt ở mỗi đầu cáp để hấp thu các tín hiệu điện tự do.
- *Ưu điểm*: kiến trúc này dùng ít cáp, dễ lắp đặt, giá thành rẻ. Khi mở rộng mạng tương đối đơn giản, nếu khoảng cách xa thì có thể dùng repeater để khuếch đại tín hiệu.
- *Khuyết điểm*: khi đoạn cáp đứt đôi hoặc các đầu nối bị hở ra thì sẽ có hai đầu cáp không nối với terminator nên tín hiệu sẽ dội ngược và làm cho toàn bộ hệ thống mạng sẽ ngưng hoạt động. Những lỗi như thế rất khó phát hiện ra là hỏng chỗ nào nên công tác quản trị rất khó khi mạng lớn (nhiều máy và kích thước lớn).



Hình vẽ 5.1 – Kiến trúc mạng **Bus**.

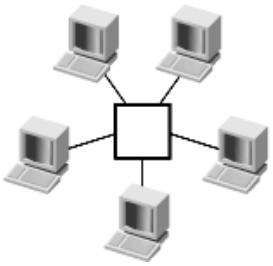
**Mạng star (sao)**

- Trong kiến trúc này, các máy tính được nối vào một thiết bị đấu nối trung tâm (**Hub** hoặc **Switch**). Tín hiệu được truyền từ máy tính gởi dữ liệu qua hub tín hiệu được khuếch đại và truyền đến tất cả các máy tính khác trên mạng.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

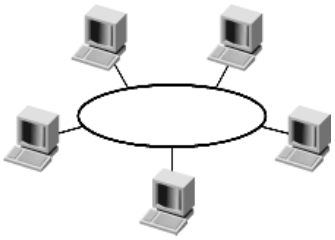
- *Ưu điểm*: kiến trúc star cung cấp tài nguyên và chế độ quản lý tập trung. Khi một đoạn cáp bị hỏng thì chỉ ảnh hưởng đến máy dùng đoạn cáp đó, mạng vẫn hoạt động bình thường. Kiến trúc này cho phép chúng ta có thể mở rộng hoặc thu hẹp mạng một cách dễ dàng.
- *Khuyết điểm*: do mỗi máy tính đều phải nối vào một trung tâm điểm nên kiến trúc này đòi hỏi nhiều cáp và phải tính toán vị trí đặt thiết bị trung tâm. Khi thiết bị trung tâm điểm bị hỏng thì toàn bộ hệ thống mạng cũng ngừng hoạt động.



Hình 5.2 – Kiến trúc mạng **Star**.

**Mạng Ring (vòng)**

- Trong mạng ring các máy tính và các thiết bị nối với nhau thành một vòng khép kín, không có đầu nào bị hở. Tín hiệu được truyền đi theo một chiều và qua nhiều máy tính. Kiến trúc này dùng phương pháp chuyển thẻ bài (**token passing**) để truyền dữ liệu quanh mạng.
- Phương pháp chuyển thẻ bài là phương pháp dùng thẻ bài chuyển từ máy tính này sang máy tính khác cho đến khi tới máy tính muốn gởi dữ liệu. Máy này sẽ giữ thẻ bài và bắt đầu gởi dữ liệu đi quanh mạng. Dữ liệu chuyển qua từng máy tính cho đến khi tìm được máy tính có địa chỉ khớp với địa chỉ trên dữ liệu. Máy tính đầu nhận sẽ gởi một thông điệp cho máy tính đầu gởi cho biết dữ liệu đã được nhận. Sau khi xác nhận máy tính đầu gởi sẽ tạo thẻ bài mới và thả lên mạng. Vận tốc của thẻ bài xấp xỉ với vận tốc ánh sáng.



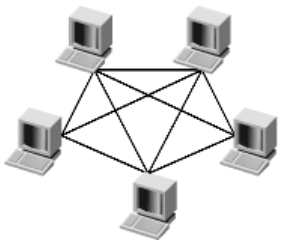
Hình 5.3 – Kiến trúc mạng **Ring**.

**Mạng Mesh (lưới).**

Từng cặp máy tính thiết lập các tuyến kết nối liên điểm do đó số lượng tuyến kết nối nhanh chóng gia tăng khi số lượng máy tính trong mạng tăng lên nên người ta ít dùng cho các mạng lưới lớn.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net



Hình 5.4 – Kiến trúc mạng **Mesh**.

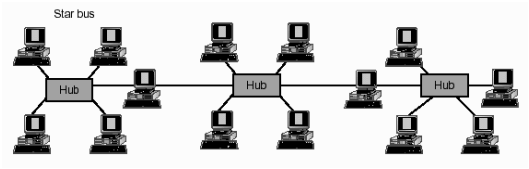
**Mạng Cellular (tế bào).**

Các mạng tế bào chia vùng địa lý đang được phục vụ thành các tế bào, mỗi tế bào được một trạm trung tâm phục vụ. Các thiết bị sử dụng các tín hiệu radio để truyền thông với trạm trung tâm, và trạm trung tâm sẽ định tuyến các thông điệp đến các thiết bị. Ví dụ điển hình của mạng tế bào là mạng điện thoại di động.

## I.3. Các kiến trúc mạng kết hợp.

**Mạng star bus.**

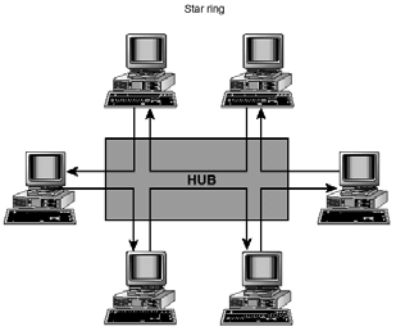
**Star bus** là mạng kết hợp giữa mạng **star** và mạng **bus**. Trong kiến trúc này một vài mạng có kiến trúc hình **star** được nối với trục cáp chính (**bus**). Nếu một máy tính nào đó bị hỏng thì nó không ảnh hưởng đến phần còn lại của mạng. Nếu một **Hub** bị hỏng thì toàn bộ các máy tính trên **Hub** đó sẽ không thể giao tiếp được.




Hình 5.5 – Kiến trúc mạng **Star-Bus**.

**Mạng star ring.**

Mạng **Star Ring** tương tự như mạng **Star Bus**. Các **Hub** trong kiến trúc **Star Bus** đều được nối với nhau bằng trục cáp thẳng (**bus**) trong khi **Hub** trong cấu hình **Star Ring** được nối theo dạng hình **Star** với một **Hub** chính.






Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Hình 5.6 – Kiến trúc mạng **Star-Ring**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

# II. CÁC CÔNG NGHỆ MẠNG LAN.

## II.1. Khái niệm.

- **Collision Domain**: đây là một vùng có khả năng bị đụng độ do hai hay nhiều máy tính cùng gởi tín hiệu lên môi trường truyền thông.
- **Broadcast Domain**: đây là một vùng mà gói tin phát tán (gói tin **broadcast**) có thể đi qua được. Trong vùng **Broadcast Domain** có thể là vùng bao gồm nhiều **Collision Domain**.

## II.2. Ethernet

Đầu tiên, **Ethernet** được phát triển bởi các hãng **Xerox**, **Digital**, **Intel** vào đầu những năm 1970. Phiên bản đầu tiên của **Ethernet** được thiết kế như một hệ thống 2,94 Mbps để nối hơn 100 máy tính vào một sợi cáp dài 1 Km. Sau đó các hãng lớn đã thảo luận và đưa ra chuẩn dành cho **Ethernet** 10 Mbps.

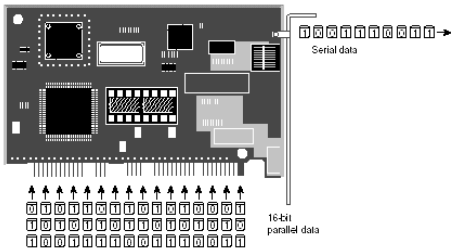
**Ethernet** chuẩn thường có cấu hình bus, truyền với tốc độ 10Mbps và dựa vào **CSMA/CD** (**Carrier Sense Multiple Access** / **Collision Detection**) để điều chỉnh lưu thông trên đường cáp chính. Tóm lại những đặc điểm cơ bản của **Ethernet** như sau:

- Cấu hình: **bus** hoặc **star**.
- Phương pháp chia sẻ môi trường truyền: **CSMA/CD**.
- Quy cách kỹ thuật IEEE 802.3
- Vận tốc truyền: 10 – 100 Mbps.
- Cáp: cáp đồng trục mảnh, cáp đồng trục lớn, cáp **UTP**.
- Tên của chuẩn **Ethernet** thể hiện 3 đặc điểm sau:
- Con số đầu tiên thể hiện tốc độ truyền tối đa.
- Từ tiếp theo thể hiện tín hiệu dải tần cơ sở được sử dụng (Base hoặc Broad).
    + **Ethernet** dựa vào tín hiệu **Baseband** sẽ sử dụng toàn bộ băng thông của phương tiện truyền dẫn. Tín hiệu dữ liệu sẽ được truyền trực tiếp trên phương tiện truyền dẫn mà không cần thay đổi kiểu tín hiệu.
    + Trong tín hiệu Br**o**adband (**ethernet** không sử dụng), tín hiệu dữ liệu không bao giờ gởi trực tiếp lên phương tiện truyền dẫn mà phải thực hiện điều chế.
- Các ký tự còn lại thể hiện loại cáp được sử dụng. Ví dụ: chuẩn 10Base2, tốc độ truyền tối đa là 10Mbps, sử dụng tín hiệu **Baseband**, sử dụng cáp **Thinnet**.

Card mạng **Ethernet**: hầu hết các **NIC** cũ đều được cấu hình bằng các **jump** (các chấu cắm chuyển) để ấn định địa chỉ và ngắt. Các **NIC** hiện hành được cấu hình tự động hoặc bằng một chương trình chạy trên máy chứa card mạng, nó cho phép thay đổi các ngắt và địa chỉ bộ nhớ lưu trữ trong một chip bộ nhớ đặc biệt trên **NIC**.

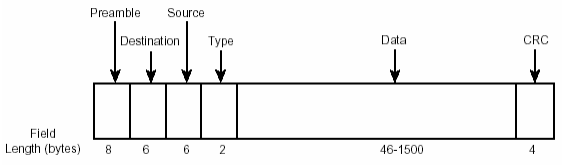


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 5.7 – Card mạng **Ethernet**.

Dạng thức khung trong **Ethernet**: **Ethernet** chia dữ liệu thành nhiều khung (**frame**). Khung là một gói thông tin được truyền như một đơn vị duy nhất. Khung trong **Ethernet** có thể dài từ 64 đến 1518 byte, nhưng bản thân khung **Ethernet** đã sử dụng ít nhất 18 byte, nên dữ liệu một khung **Ethernet** có thể dài từ 46 đến 1500 byte. Mỗi khung đều có chứa thông tin điều khiển và tuân theo một cách tổ chức cơ bản. Ví dụ khung **Ethernet** (dùng cho TCP/IP) được truyền qua mạng với các thành phần sau:




Hình 5.8 – Cấu trúc khung **Ethernet**.

Các trường trong **Frame Ethernet**:

- **Preamble**: 8 byte mở đầu.
- **Destination**: 6 byte thể hiện địa chỉ **MAC** đích.
- **Source**: 6 byte thể hiện địa chỉ **MAC** nguồn.
- **Type**: 2 byte thể hiện kiểu giao thức ở tầng trên.
- **Data**: dữ liệu của **Frame**.
- **CRC**: 4 byte dùng để kiểm lỗi của **Frame**.

Các loại **Ethernet** với băng tần cơ sở:

- 10Base2: tốc độ 10, chiều dài cáp nhỏ hơn 200 m, dùng cáp **thinnet** (cáp đồng trục mảnh).
- 10Base5: tốc độ 10, chiều dài cáp nhỏ hơn 500 m, dùng cáp **thicknet** (cáp đồng trục dày).
- 10BaseT: tốc độ 10, dùng cáp xoắn đôi (**Twisted-Pair**).
- 10BaseFL: tốc độ 10, dùng cáp quang (**Fiber optic**).
- 100BaseT: tốc độ 100, dùng cáp xoắn đôi (**Twisted-Pair**).
- 100BaseX: tốc độ 100, dùng cho **multiple media type**.
- 100VG-AnyLAN: tốc độ 100, dùng **voice grade**.



### II.2.1 Chuẩn 10Base2

Cấu hình này được xác định theo tiêu chuẩn IEEE 802.3 và bảo đảm tuân thủ các quy tắc sau:

- Khoảng cách tối thiểu giữa hai máy trạm phải cách nhau 0.5m.

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

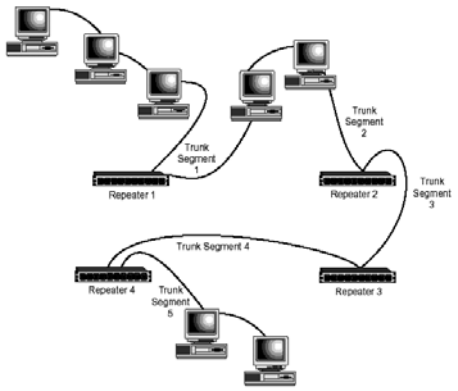
- Dùng cáp **Thinnet** (RG-58).



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

- Tốc độ 10 Mbps.
- Dùng đầu nối chữ T (**T-connector**).
- Không thể vượt quá phân đoạn mạng tối đa là 185m. Toàn bộ hệ thống cáp mạng không thể vượt quá 925m.
- Số nút tối đa trên mỗi phân đoạn mạng là 30.
- **Terminator** (thiết bị đầu cuối) phải có trở kháng 50 ohm và được nối đất.
- Mỗi mạng không thể có trên năm phân đoạn. Các phân đoạn có thể nối tối đa bốn bộ khuếch đại và chỉ có ba trong số năm phân đoạn có thể có nút mạng (tuân thủ quy tắc 5-4-3).

*Quy tắc 5-4-3*: quy tắc này cho phép kết hợp đến năm đoạn cáp được nối bởi 4 bộ chuyển tiếp, nhưng chỉ có 3 đoạn là nối trạm. Theo hình trên ta thấy đoạn 3, 4 chỉ tồn tại nhằm mục đích làm tăng tổng chiều dài mạng và cho phép máy tính trên đoạn 1, 2, 5 nằm cùng trên một mạng.




Hình 5.9 – Qui tắc 5-4-3.

Ưu điểm chuẩn 10Base2: giá thành rẻ, đơn giản.

### II.2.2 Chuẩn 10Base5

Chuẩn mạng này tuân theo các quy tắc sau:

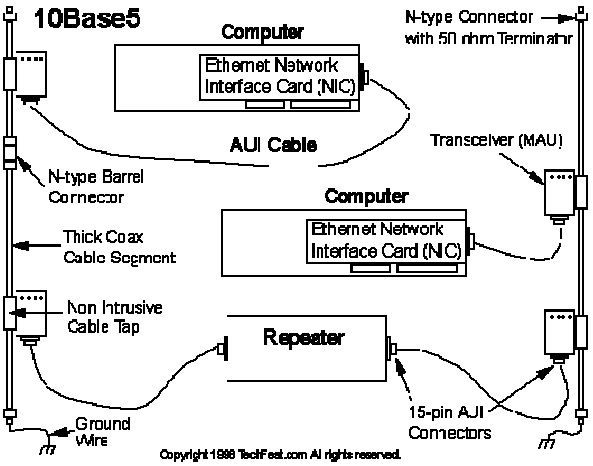
- Khoảng cách tối thiểu giữa hai nút là 2.5m.
- Dùng cáp **thicknet** (cáp đồng dày).
- Băng tần cơ sở 10Mbps.
- Chiều dài phân đoạn mạng tối đa là 500m.
- Toàn bộ chiều dài mạng không thể vượt quá 2500m.
- Thiết bị đầu cuối (**terminator**) phải được nối đất.
- Cáp thu phát (**tranceiver cable**), nối từ máy tính đến bộ thu phát, có chiều dài tối đa 50m.
- Số nút tối đa cho mỗi phân đoạn mạng là 100 (bao gồm máy tính và tất cả các **repeater**).
- Tuân theo quy tắc 5-4-3.



*Ưu điểm*: khắc phục được khuyết điểm của mạng 10Base2, hỗ trợ kích thước mạng lớn hơn.

*Chú ý*: trong các mạng lớn người ta thường kết hợp cáp dày và cáp mảnh. Cáp dày dùng làm cáp chính rất tốt, còn cáp mảnh dùng làm đoạn nhánh.

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 5.10 - Một ví dụ về chuẩn 10Base5.

### II.2.3 Chuẩn 10BaseT.

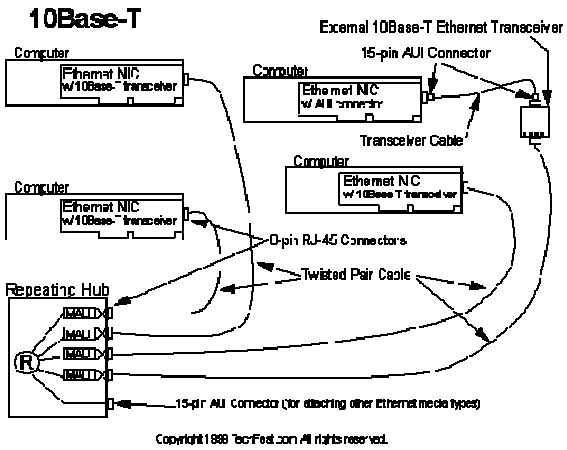
Chuẩn mạng này tuân theo các quy tắc sau:

- Dùng cáp UTP loại 3, 4, 5 hoặc **STP**, có mức trở kháng là 85-115 ohm, ở 10Mhz.
- Dùng quy cách kỹ thuật 802.3.
- Dùng thiết bị đấu nối trung tâm **Hub**.
- Tốc độ tối đa 10Mbps.
- Dùng đầu nối RJ-45.
- Số nút tối đa là 512 và chúng có thể nối vào 3 phân đoạn bất kỳ với năm phân tuyến tối đa có sẵn.
- Chiều dài tối đa một phân đoạn cáp là 100m.
- Dùng mô hình vật lý **star**.
- Có thể nối các phân đoạn mạng 10BaseT bằng cáp đồng trục hay cáp quang.
- Số lượng máy tính tối đa là 1024.
- Khoảng cách tối thiểu giữa hai máy tính là 2,5m.
- Khoảng cách cáp tối thiểu từ một **Hub** đến một máy tính hoặc một **Hub** khác là 0,5m.

*Ưu điểm*: do trong mạng 10BaseT dùng thiết bị đấu nối trung tâm nên dữ liệu truyền tin cậy hơn, dễ quản lý. Điều này cũng tạo thuận lợi cho việc định vị và sửa chữa các phân đoạn cáp bị hỏng. Chuẩn này cho phép bạn thiết kế và xây dựng trên từng phân đoạn một trên LAN và có thể tăng dần khi mạng cần phát triển. 10BaseT cũng tương đối rẻ tiền so với các phương án đấu cáp khác.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 5.11 – Một ví dụ về chuẩn 10BaseT.

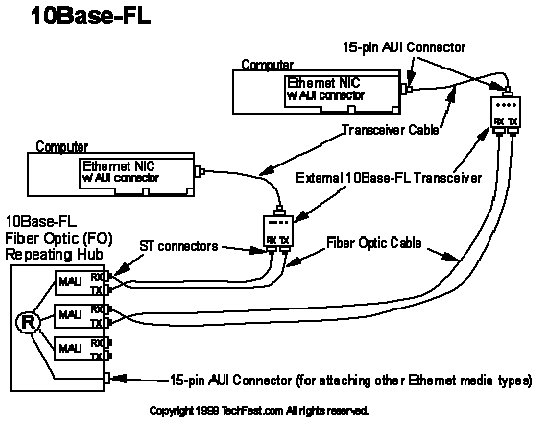
### II.2.4 Chuẩn 10BaseFL.

Các đặc điểm của 10BaseFL:

- Tốc độ tối đa 10 Mbps.
- Truyền qua cáp quang.

Ưu điểm:

- Do dùng cáp quang nối các **Repeater** nên khoảng cách tối đa cho một đoạn cáp là 2000m.
- Không sợ bị nhiễu điện từ.
- Số nút tối đa trên một đoạn cáp lớn hơn nhiều so với 10Base2, 10Base5, 10BaseT.




Hình 5.12 – Một ví dụ về chuẩn 10Base-FL.

### II.2.5 Chuẩn 100VG-AnyLAN.

100VG (Voice Grade) **AnyLan** là công nghệ mạng kết hợp các thành phần của **Ethernet** và **Token Ring**, dùng quy cách kỹ thuật 802.12. Các đặc điểm kỹ thuật:

- Tốc độ truyền dữ liệu tối thiểu là 100Mbps.



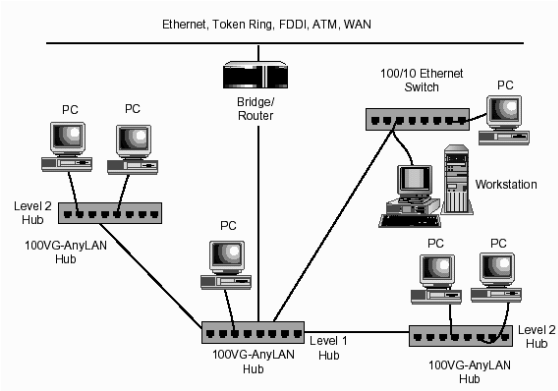
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

- Sử dụng cáp xoắn đôi gồm bốn cặp xoắn (**UTP** loại 3, 4, 5 hoặc **STP**) và cáp quang.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

- Khả năng hỗ trợ sàng lọc từng khung có địa chỉ tại **Hub** nhằm tăng cường tính năng bảo mật.
- Chấp nhận cả khung **Ethernet** lẫn gói **Token Ring**.
- Định nghĩa trong IEEE 802.12.
- Mô hình vật lý: **cascaded star**, mọi máy tính được nối với một **Hub**. Có thể mở rộng mạng bằng cách thêm **Hub** con vào **Hub** trung tâm, **Hub** con đóng vai trò như máy tính đối với **Hub** mẹ.
- Chiều dài tối đa của đoạn chạy cáp nối hai **Hub** là 250m.

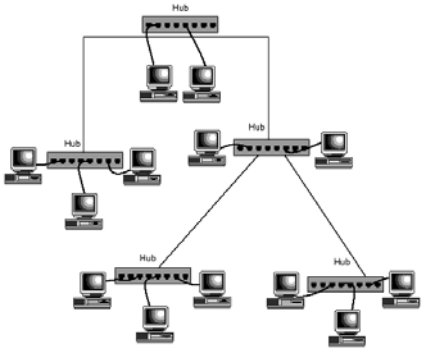



Hình 5.13 – Một ví dụ về chuẩn 100VG-AnyLAN.

### II.2.6 Chuẩn 100BaseX.

Tiêu chuẩn 100BaseX **Ethernet** còn gọi là **Fast Ethernet** là sự mở rộng của tiêu chuẩn **Ethernet** có sẵn. Tiêu chuẩn này dùng cáp **UTP Cat5** và phương pháp truy cập **CSMA/CD** trong cấu hình **star bus** với mọi đoạn cáp nối vào một **Hub** tương tự 10BaseT. Tốc độ 100Mbps. Chuẩn 100BaseX có các đặc tả ứng với các loại đường truyền khác nhau:

- 100BaseT4: dùng cáp **UTP** loại 3, 4, 5 có bốn cặp xoắn đôi.
- 100BaseTX: dùng cáp **UTP** loại 5 có hai cặp xoắn đôi hoặc **STP**.
- 100BaseFX: dùng cáp quang có hai dây lõi.




Hình 5.14 – Một ví dụ về chuẩn 100Base-X.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Bảng dưới đây sẽ tóm tắt lại các thông số của một số loại cáp.

| Chuẩn | Loại cáp | Chiều dài tối đa | Đầu nối |
|---|---|---|---|
| 10Base2 | Thinnet | 185m | BNC |
| 10Base5 | Thicknet | 500m | AUI |
| 10Base-T | UTP cat 3-4-5, 2 cặp dây | 100m | RJ45 |
| 100Base-TX | UTP cat 5, 2 cặp dây | 100m | RJ45 |
| 100Base-FX | Cáp quang Multimode, lõi 62.5 hoặc 125 micro | 400m | MIC, ST, SC |
| 1000Base-CX | STP | 25m | RJ45 |
| 1000Base-T | UTP cat 5, 4 cặp dây | 100m | RJ45 |
| 1000Base-SX | Cáp quang Multimode, lõi 62.5 hoặc 50 micro | 62.5 micro thì được 275m<br>50 micro thì được 550m | SC |
| 1000Base-LX | Cáp quang Multimode, lõi 62.5 hoặc 50 micro<br>Cáp quang Singlemode, lõi 9 micro | 62.5 micro thì được 440m<br>50 micro thì được 550m<br>9 micro thì được 3-10Km | SC |

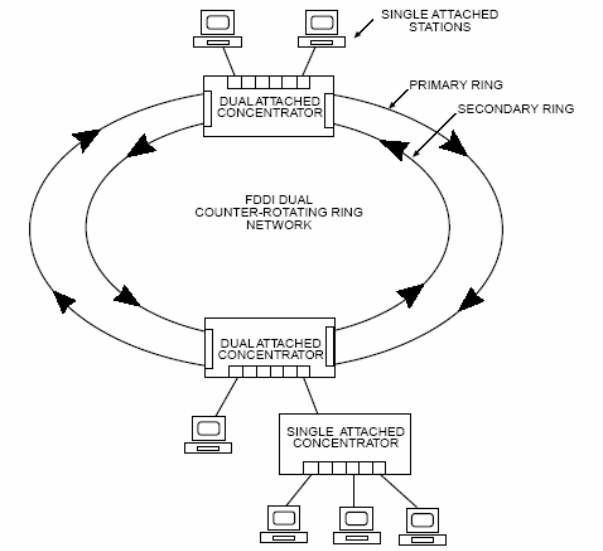
## II.3. FDDI.

Một trong những bất lợi chính của các mạng vòng tín bài là sự nhạy cảm của chúng với bất trắc. Vì mỗi máy gắn trên vòng phải chuyển khung cho máy kế nên một hỏng hóc trên máy sẽ làm cho toàn mạng ngưng hoạt động. Phần cứng vòng tín bài thường được thiết kế để tránh những hư hỏng như thế. Tuy nhiên hầu hết các mạng vòng tín bài không thể vượt qua khi sự kết nối bị cắt như khi đường cáp nối hai máy bỗng nhiên bị đứt.

Một số công nghệ mạng vòng đã được thiết kế để khắc phục được hỏng hóc nghiêm trọng. Ví dụ **FDDI** (**Fiber Distributed Data Interconnection**) là công nghệ mạng vòng tín bài có thể truyền dữ liệu ở tốc độ 100 triệu bit/giây, nhanh gấp 8 lần mạng vòng tín bài **IBM**, và nhanh hơn 10 lần mạng **Ethernet**. Để cung ứng tốc độ dữ liệu nhanh như vậy, **FDDI** dùng sợi quang để nối các máy thay cho cáp đồng.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

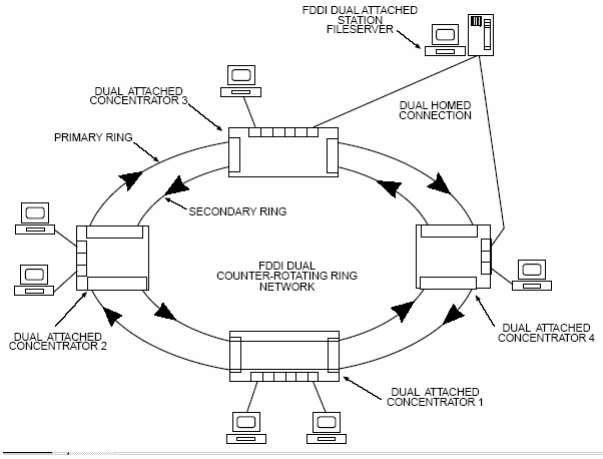



Hình 5.14 - Mạng **FDDI**.

Mạng **FDDI** sử dụng cáp quang có đặc điểm sau:

- Chiều dài của cáp: chiều dài tối đa của cáp (2 vòng) là 100Km, nếu cáp (1 vòng) thì chiều dài tối đa là 200Km.
- Số trạm trên mạng: có khả năng hỗ trợ 500 máy trong một mạng.
- Bảo mật: chỉ bị nghe lén khi vòng cáp bị đứt.
- Nhiễu điện từ: không bị nhiễu điện từ.

**FDDI** dùng tính năng dự phòng để khắc phục sự cố. Một mạng **FDDI** gồm hai vòng - một dùng để gởi dữ liệu khi mọi việc đều ổn, và chỉ sử dụng vòng thứ hai khi vòng một hỏng. Về mặt vật lý, hai đường nối với một cặp máy tính là không hoàn toàn cách biệt. Mỗi sợi quang được bọc trong một vỏ nhựa dẻo và có một vỏ bọc cặp sợi bao bên ngoài tương tự như các đường dây điện trong nhà. Vì vậy có thể lắp đặt hai vòng cùng một lúc.

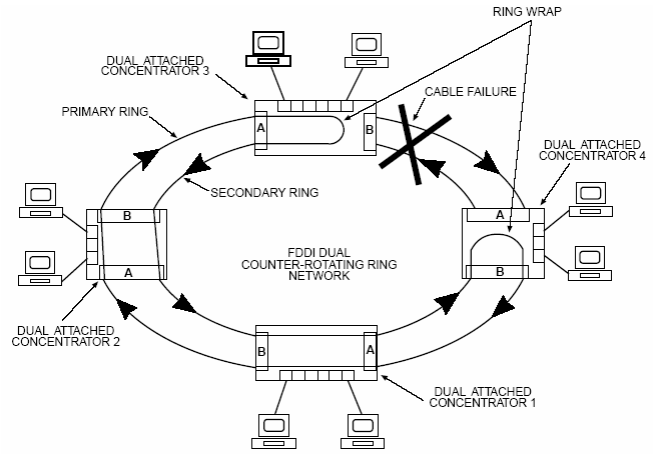



Hình 5.15 – Sơ đồ hoạt động của mạng **FDDI**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Điều thú vị là các vòng trong mạng **FDDI** được gọi là xoay ngược (**counter rotating**) vì dữ liệu chạy trong vòng thứ hai ngược lại với hướng dữ liệu vòng thứ nhất. Để hiểu tại sao lại dùng các vòng xoay ngược, hãy xét trường hợp có sự cố nghiêm trọng xảy ra. Thứ nhất vì cặp sợi nối hai trạm thường đi trên cùng đường nên khi đứt một sợi thì thường là đứt luôn sợi kia. Thứ hai, nếu dữ liệu luôn luôn đi theo một hướng trên cả hai sợi, việc ngắt một trạm ra khỏi vòng (ví dụ khi di chuyển máy) sẽ ngắt truyền thông các máy khác. Tuy nhiên, nếu dữ liệu chuyển theo hướng ngược lại ở đường dự trữ, các trạm còn lại có thể cấu hình mạng để sử dụng đường dự phòng.




Hình vẽ 5.16 – Khi cáp giữa hai máy kế tiếp bị đứt.

Phương pháp truy cập mà mạng **FDDI** sử dụng là phương pháp **Token-Ring**. Thẻ **Token** là một **Frame** đặc biệt, chạy xoay vòng trên đường mạng. Khi máy trạm cần truyền dữ liệu, nó sẽ bắt thẻ **Token**, sau khi bắt được thẻ thì nó bắt đầu truyền dữ liệu, sau khi truyền dữ liệu xong thì nó sẽ giải phóng thẻ **Token**. Chỉ có máy trạm nào giữ thẻ **Token** mới được phép truyền dữ liệu lên trên đường mạng.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

# Tóm tắt

Lý thuyết 6 tiết - Thực hành 10 tiết

| Mục tiêu | Các mục chính | Bài tập bắt buộc | Bài tập làm thêm |
|---|---|---|---|
| Kết thúc bài học này cung cấp học viên kiến thức về các lớp con LLC, MAC của lớp 2 và các giao thức TCP, UDP, khái niệm port, đặc biệt là các mô hình firewall … | I. Khảo sát chi tiết lớp 2.<br>II. Khảo sát chi tiết lớp 3.<br>III. Khảo sát chi tiết lớp 4.<br>IV. Các mô hình Firewall. | Dựa vào bài tập môn mạng máy tính. | Dựa vào bài tập môn mạng máy tính. |



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

# I. KHẢO SÁT CHI TIẾT LỚP 2 (DATA LINK).

Lớp 1 liên quan đến môi trường, liên quan các tín hiệu, các luồng bit di chuyển trên môi trường, các thành phần dựa dữ liệu ra môi trường và các cấu hình khác nhau. Nó thực hiện vai trò thiết yếu cho hoạt động truyền tin khả thi giữa các máy tính, nhưng với nỗ lực một mình của nó thì không đủ. Mỗi chức năng có các hạn chế của nó. Lớp 2 hướng tới khắc phục hạn chế này. Ứng với mỗi hạn chế trong lớp 1, lớp 2 có một giải pháp. Ví dụ lớp 1 không thể thông tin với các lớp trên, lớp 2 làm việc này thông qua **LLC** (**Logical Link Control**). Lớp 1 không đặt tên hay định danh cho máy tính thì lớp 2 dùng một lược đồ địa chỉ. Lớp 1 không thể quyết định máy tính nào sẽ truyền dữ liệu nhị phân từ một nhóm cùng muốn truyền tại cùng một thời điểm. Lớp 2 dùng một hệ thống gọi là **MAC** (**Media Access Control**).

## I.1. Lớp con LLC.

Lớp con **LCC** tạo ra tính năng linh hoạt trong việc phục vụ cho các giao thức lớp mạng trên nó, trong khi vẫn liên lạc hiệu quả với các kỹ thuật khác nhau bên dưới nó. **LLC** với vai trò là lớp phụ tham gia vào quá trình đóng gói. **LLC** nhận đơn vị dữ liệu giao thức lớp mạng, như là các gói **IP**, và thêm nhiều thông tin điều khiển vào để giúp phân phối gói IP đến đích của nó. Nó thêm hai thành phần địa chỉ của đặc tả 802.2 điểm truy xuất dịch vụ đích **DSAP** (**Destination Service Access Point**) và điểm truy xuất dịch vụ nguồn **SSAP** (**Source Service Access Point**). Nó đóng gói trở lại dạng **IP**, sau đó chuyển xuống lớp phụ **MAC** để tiến hành các kỹ thuật đặc biệt được yêu cầu cho đóng gói tiếp theo. Lớp phụ **LLC** quản lý hoạt động thông tin giữa các thiết bị qua một liên kết đơn trên một mạng. **LLC** được định nghĩa trong đặc tả **IEEE 802.2** và hỗ trợ các dịch vụ kết nối có cả tạo cầu nối và không tạo cầu nối, được dùng bởi các giao thức lớp cao hơn. **IEEE 802.2** định nghĩa ra một số **field** trong các **frame** của lớp liên kết dữ liệu cho phép nhiều giao thức lớp cao hơn chia sẻ một liên kết vật lý đơn.

## I.2. Lớp con MAC.

Lớp con **MAC** đề cập đến các giao thức chủ yếu phải theo để truy xuất vào môi trường vật lý. Tóm lại, lớp 2 có 4 khái niệm chính mà cần phải biết:

- Lớp 2 thông tin với các lớp trên thông qua **LLC**.
- Lớp 2 dùng chuẩn địa chỉ hóa ngang bằng (đó là gán các định danh duy nhất-các địa chỉ).
- Lớp 2 dùng kỹ thuật đóng frame để tổ chức hay nhóm dữ liệu.
- Lớp 2 dùng **MAC** để chọn máy tính nào sẽ truyền các dữ liệu nhị phân, từ một nhóm trong đó tất cả các máy tính đều muốn truyền cùng một lúc.

## I.3. Quá trình tìm địa chỉ MAC:

Với mạng **TCP/I**P, thì gói tin phải chứa cả địa chỉ **MAC** đích và địa chỉ **IP** đích. Nếu một trong hai địa chỉ này không đúng thì gói tin cũng xem như là không gởi được đến đích. **ARP** là một giao thức dùng để tìm địa chỉ MAC của một thiết bị mạng dựa trên địa chỉ **IP** đã biết.

Một vài thiết bị có lưu trữ bảng chứa địa chỉ **IP** và địa chỉ **MAC** tương ứng với **IP** đó (của các thiết bị trong cùng mạng **LAN** với nó). Bảng này được gọi là bảng **ARP**. Bảng **ARP** này được lưu giữ trong



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

**RAM**, và khi thiết bị gởi gói tin lên mạng thì nó sử dụng thông tin trong bảng **ARP** này.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Có 2 cách để thu thập thông tin cho bảng địa chỉ **MAC**.

- Khi có một gói tin được gởi trên đường truyền, thiết bị luôn kiểm tra địa chỉ đích của gói tin (địa chỉ **IP** và địa chỉ **MAC**) có phải là của mình hay không? Sau khi kiểm tra, địa chỉ **IP** và địa chỉ **MAC** đều được lưu vào trong bảng **ARP**.
- Cách thu thập thông tin thứ 2 là thu thập qua gói tin broadcast **ARP request**. Khi máy tính gởi một gói tin **broadcast** dạng **ARP request** thì tất cả các máy khác trên mạng đều phân tích gói tin này.
    + Nếu như địa chỉ **IP** đích của thiết bị mạng cần tìm là địa chỉ thuộc cùng đường mạng với địa chỉ máy gửi.
        ③ Nếu máy đó nhận được gói tin thì máy sẽ trả lời bằng một gói tin **ARP reply** (trong đó có địa chỉ **MAC** và địa chỉ **IP** của máy).
        ③ Nếu địa chỉ đích không tồn tại hoặc thiết bị chưa hoạt động thì sẽ không có gói tin **ARP reply**.
    + Nếu địa chỉ **IP** đích của thiết bị mạng cần tìm là địa chỉ khác đường mạng thì việc tìm địa chỉ **MAC** thường được làm thông qua **Router**, có hai cách để thực hiện:
        ③ Nếu **Router** bật tính năng cho phép thực hiện **Proxy ARP**. Thì khi nhận được gói tin **broadcast ARP request**, **Router** sẽ kiểm tra xem địa chỉ đích có khác đường mạng với địa chỉ nguồn không? Nếu khác địa chỉ nguồn thì **Router** sẽ trả về một **ARP response** để trả lời (trong gói tin này sẽ chứa địa chỉ **MAC** – địa chỉ **MAC** của **interface** nhận gói tin **ARP request**).
        ③ Nếu máy tính gửi có khai báo địa chỉ **Default Gateway** thì máy tính sẽ gởi gói tin đến **Default Gateway** để **Default Gateway** gởi tiếp.

Nếu máy tính nguồn không khai báo **Default Gateway** và tính năng thực hiện **Proxy ARP** không bật thì hai máy tính có địa chỉ đường mạng khác nhau sẽ không thể liên lạc được với nhau.

## I.4. Các phương pháp truy cập đường truyền.

### I.4.1 Cảm sóng đa truy (CSMA/CD).

Khía cạnh thú vị nhất của **Ethernet** là kỹ thuật đường dùng trong việc phối hợp truyền thông. Mạng **Ethernet** không điều khiển tập trung đến việc các máy luân phiên chia sẻ đường cáp. Lúc đó các máy nối với **Ethernet** sẽ tham gia vào một lược đồ phối hợp phân bổ gọi là Cảm sóng đa truy (**CSMA – Carrier Sence with Multiple Access**). Để xác định cáp có đang dùng không, máy tính có thể kiểm tra sóng mang (**carrier** - dạng tín hiệu mà máy tính truyền trên cáp). Nếu có sóng mang, máy phải chờ cho đến khi bên gởi kết thúc. Về mặt kỹ thuật, kiểm tra một sóng mang được gọi là cảm sóng (**carrier sence**), và ý tưởng sử dụng sự hiện hữu của tín hiệu để quyết định khi nào thì truyền gọi là Cảm sóng đa truy (**CSMA**).



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Vì **CSMA** cho phép mỗi máy tính xác định đường cáp chia sẻ có đang được máy khác sử dụng hay không nên nó ngăn cấm một máy cắt ngang việc truyền đang diễn ra. Tuy nhiên, **CSMA** không thể ngăn ngừa tất cả các xung đột có thể xảy ra. Để hiểu lý do tại sao, hãy tưởng tượng chuyện gì xảy ra nếu hai máy tính ở hai đầu cáp đang nghỉ nhận được yêu cầu gởi khung. Cả hai cùng kiểm tín hiệu mang, cùng thấy cáp đang trống và cả hai bắt đầu gởi khung. Các tín hiệu phát từ hai máy sẽ gây nhiễu lẫn nhau. Hai tín hiệu gây nhiễu lẫn nhau gọi là xung đột hay đụng độ (**collision**). Vùng có khả năng xảy ra đụng độ khi truyền gói tin được gọi là **Collision Domain**. Máy đầu tiên trên đường truyền phát hiện được xung đột sẽ phát sinh tín hiệu xung đột cho các máy khác. Tuy xung đột không làm hỏng phần cứng nhưng nó tạo ra một sự truyền thông méo mó và hai khung nhận được sẽ không chính xác. Để xử lý các biến cố như vậy, **Ethernet** yêu cầu mỗi bên gởi tín hiệu giám sát (monitor) trên cáp để bảo đảm không có máy nào khác truyền đồng thời. Khi máy gởi phát hiện đụng độ, nó ngưng truyền ngay lập tức, và tiếp tục bắt đầu lại quá trình chuẩn bị việc truyền tin sau một khoảng thời gian ngẫu nhiên. Việc giám sát cáp như vậy gọi là phát hiện đụng (**CD – collision detect**), và kỹ thuật **Ethernet** đó được gọi là Cảm sóng đa truy với phát hiện đụng (**CSMA/CD**).

### I.4.2 Chuyển thẻ bài (Token-passing):

Chúng ta đã biết mạng **LAN** vòng nối các máy thành một vòng tròn kín. Hầu hết các **LAN** dùng đồ hình vòng cũng sử dụng một kỹ thuật truy cập gọi là chuyển thẻ bài (**token-passing**). Khi một máy cần chuyển dữ liệu, nó phải chờ phép trước khi truy cập mạng. Khi giữ được thẻ bài, máy gởi hoàn toàn giữ quyền điều khiển vòng – không có các truyền thông nào khác xảy ra đồng thời. Khi máy gởi truyền frame, các bit chuyển từ máy gởi sang máy kế, và chuyển tiếp sang máy kế và cứ thế cho đến khi các **bit** đi hết vòng và trở về máy gởi.

Tín bài là một khuôn mẫu bit khác với khung dữ liệu thông thường. Thực chất là tín bài trao quyền cho một máy được gởi khung. Như vậy trước khi gởi khung, máy phải chờ tín bài đến. Khi tín bài đến, máy tạm thời loại bỏ tín bài ra khỏi vòng và bắt đầu truyền dữ liệu trên vòng. Tuy có thể có nhiều khung đang chờ gởi đi nhưng máy chỉ gởi một **frame** và truyền lại tín bài. Không như khung dữ liệu dữ liệu đi hết một vòng khi được gởi, tín bài chỉ đi thẳng từ một máy đến máy kế tiếp.

Nếu tất cả các máy trên mạng vòng cần gởi dữ liệu, chuyển tín bài bảo đảm chúng sẽ đến lược và mỗi máy sẽ gởi một frame trước khi chuyển tín bài. Lưu ý là lược đồ này bảo đảm truy cập công bằng: khi tín bài chuyển trên vòng, mỗi máy sẽ có cơ hội sử dụng mạng. Nếu một máy nào đó không gởi dữ liệu khi nhận được tín bài, nó chỉ việc chuyển tín bài mà không trì hoãn. Trong trường hợp đặc biệt không có máy nào truyền dữ liệu, tín bài sẽ quay vòng liên tục, mỗi máy khi nhận được tín bài sẽ chuyển ngay lập tức đến máy kế. Thời gian chuyển tín bài một vòng trong trường hợp này là cực ngắn, vì 2 lý do. Thứ nhất, vì tín bài nhỏ nên có thể chuyển rất nhanh trên đường dây. Thứ hai, sự chuyển tiếp trên mỗi máy được thực hiện bởi phần cứng vòng, điều đó có nghĩa tốc độ không phụ thuộc vào **CPU** của máy.

# II. KHẢO SÁT CHI TIẾT LỚP 3 (NETWORK).

Chức năng quan trọng nhất của lớp **Network** là định tuyến (**Routing**), định tuyến là quá trình chuyển thông tin qua mạng từ nơi gởi tới nơi nhận. Định tuyến có hai thành phần là chuyển mạch (**switching**) và chọn đường (**path determination**).



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Trong quá trình **switching**, bên gởi (**source or sender**) thêm vào địa chỉ bên gởi, địa chỉ bên nhận, địa chỉ vật lý (**MAC**), địa chỉ của **Router** đầu tiên (hay là địa chỉ **Default-Gateway**) mà packet tới. Khi packet tới **Router**, **Router** sẽ xác định địa chỉ **IP** đích của **packet** (còn gọi là **destination IP address**), nếu như **Router** không nhận ra **IP** đích thì nó sẽ bỏ **packet**, nếu ngược lại thì **Router** sẽ chuyển **packet** tới địa chỉ đích hoặc chuyển packet tới **Router** kế tiếp (**next Router**), khi đó **Router** nó sẽ thay thế **MAC** nguồn, và **MAC** đích bằng **MAC** trên **interface** của nó và **MAC** trên **next hop Router**, khi **packet** chuyển qua mạng lớn (qua nhiều **Router**) thì địa chỉ **IP** nguồn (**source address**) và địa chỉ **IP** đích (**destination address**) không thay đổi nhưng địa chỉ vật lý (địa chỉ **MAC**) bị thay đổi tại mỗi hop.

Thành phần thứ hai của **routing** là **Path-Determination**, **Router** cần có một số cách xác định con đường đi ngắn nhất để chuyển packet tới đích, **Router** cần có nhiều thông tin từ người quản trị (người quản trị phải làm công việc định tuyến) hay từ các **Router** khác để xây dựng bảng **routing** (**Router** tự học định tuyến thông qua các giao thức) mà thông tin này giúp cho nó định tuyến packet đi tới đích.

Trong bảng **routing** địa chỉ mạng đích được ánh xạ tới **interface** (cổng) thích hợp trên **Router**, thông qua **interface** này packet có thể đi tới nó.

Khi có sự thay đổi trên mạng các **Router** trao đổi với nhau bằng các **exchanging message** để cập nhật lại bảng **routing**. Các **exchanging message** bao gồm:

- **Routing update message**.
- **Link-state advertiment** (trạng thái của **sender's link**).

Theo định nghĩa của một số nghi thức **routing** như **RIP**, **IGRP**,… cứ sau một khoảng thời gian (**interal time**) nó sẽ gởi **update message** tới các **Router** khác để cập nhật về sự thay đổi thông tin trên mạng. Khi các **Router** này nhận được thông tin **update**, nó sẽ kiểm tra trong bảng **routing table** của nó với thông tin **update** nếu có sự thay đổi thì nó sẽ xóa **entry** tương ứng và cập nhật thông tin mới vào, ngược lại thì nó sẽ không cập nhật thông tin.

**Routing Algorithm** là thuật toán định tuyến cho phép chọn **Router**, chọn con đường đi tốt nhất để gởi dữ liệu đến đích. **Routing Algorithm** tùy thuộc vào các yếu tố sau :

- **Design**.
- **Metrics**.
- **Type**.

**Design bao gồm:**

- Tính đơn giản (**simplicity**) là thành phần rất quan trọng trong hệ thống giúp giới hạn tài nguyên vật lý (**physical resource**).
- Tính linh hoạt (**plexibility**) để cho phép mạng thích ứng nhanh với sự thay đổi và phát triển của hệ thống, ví dụ như sự thay đổi về băng thông kích thước hàng đợi, độ trễ,…
- Sự hội tụ (**convergence**) tính hội tụ thông tin là mục đích quan trọng của thuật toán **routing**, tính hội tụ nhanh làm cho thông tin trong bảng **routing** được thống nhất một cách nhanh chóng. Ngược lại nó sẽ làm phá vỡ tính thống nhất thông tin định tuyến giữa các **Router**.
- Tính tối ưu (**optimality**): là khả năng mà nghi thức định tuyến lựa chọn đường đi tốt nhất để truyền dữ liệu, để xác định con đường đi tốt nhất **Router** dựa vào metric và **weighting** (trọng lượng) của mỗi **metric**.

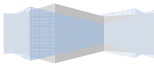


**Metric được sử dụng trong thuật toán định tuyến để lựa chọn con đường đi tốt nhất, nó bao**

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

**gồm:**





Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

- **Hop count và path length**.
- **Reliability**.
- **Load**.
- **Delay**.
- **Bandwidth**.
- **Maximum Tranmission Unit** (**MTU**).

**Hop count** là số lượng host (hay là số lượng **Router**) mà packet phải đi qua từ nguồn tới đích.

Mỗi một đường truyền được gán bởi một giá trị, chỉ có người quản trị mạng mới thay đổi giá trị này, tổng giá trị của các đường truyền đó gọi là **path length**.

**Reliability** là **metric** cho phép đánh giá mức độ lỗi của một đường truyền.

**Load** khả năng tải hiện tại trên đường truyền (**busy link**) dựa vào số lượng packet được truyền trong thời gian 1 giây, mức độ xử lý hiện tại của cpu (**CPU Utilization**).

**Delay metric** thực sự để đo lường một số tác động của một số đại lượng trên đường truyền như băng thông (**bandwidth**), tắc nghẽn đường truyền (**conguestion**), khoảng cách đường truyền (**distance**), khả năng mang thông tin trên đường truyền còn gọi là băng thông của đường truyền được tính băng số bit/giây mà đường truyền đó có thể truyền thông tin, số lượng traffic trên đường truyền quá nhiều sẽ làm giảm băng thông có sẵn cho đường truyền.

**MTU** là chiều dài tối đa của thông điệp (tính bằng **byte**) mà nó có thể truyền trên đường truyền. MTU của mỗi môi truyền truyền vật lý thì khác nhau. Ví dụ **MTU** cho **ethernet** là 1500.

# III. KHẢO SÁT CHI TIẾT LỚP 4 (TRANSPORT)

Các dịch vụ trên lớp **transport** cho phép phân mảnh và tập hợp dữ liệu vào cùng transport-layer data stream, **Transport-layer data stre**am là một kết nối logic giữa bên gởi và bên nhận trên mạng. Lớp **Transport** cung cấp các đặc tính sau :

- **Reliability** (tin cậy) bằng cách đánh số thứ tự của các **segment** (**source secquence**), bên nhận thông báo cho bên gởi biết rằng nó đã nhận được dữ liệu bằng cách thông báo các **ACK** (**acknownledgements**).
- **Flow Control**: là kỹ thuật cho phép điều khiển buffer bên nhận, bên nhận sử dụng kỹ thuật này để ngăn không cho bên gởi gởi dữ liệu quá nhanh làm tràn buffer của bên nhận.
- Hai **protocol** ở lớp **transport layer** là **TCP** và **UDP**,

## III.1. Giao thức TCP (TCP protocol).

**TCP** cung cấp kết nối tin cậy giữa hai máy tính, kết nối được thiết lập trước khi dữ liệu bắt đầu truyền. **TCP** còn gọi là nghi thức hướng kết nối, với nghi thức **TCP** thì quá trình hoạt động trải qua ba bước sau:

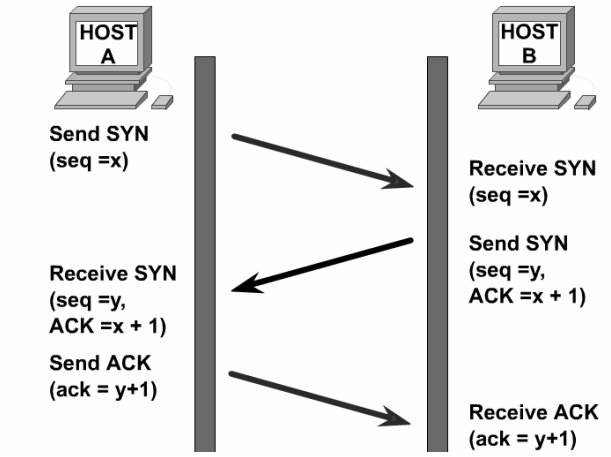
- Thiết lập kết nối (**connection establishment**).
- Truyền dữ liệu (**data tranfer**).
- Kết thúc kết nối (**connection termination**).



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

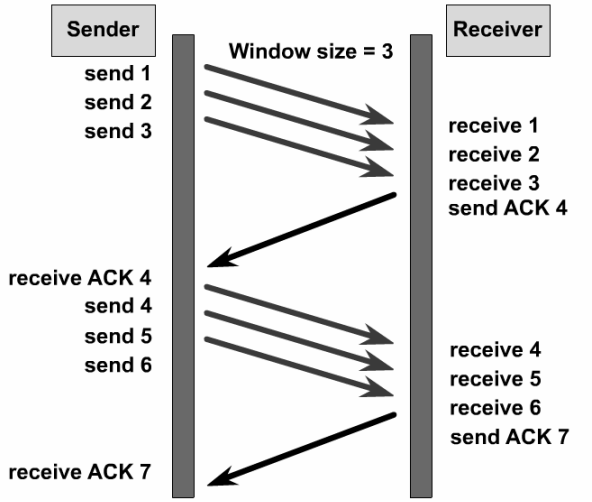
**TCP** phân chia các thông điệp thành các segment, sau đó nó ráp các segment này lại tại bên nhận, và nó có thể truyền lại những gói dữ liệu nào đã bị mất. Với **TCP** thì dữ liệu đến đích là đúng thứ tự, **TCP** cung cấp **Virtual Circuit** giữa các ứng dụng bên gởi và bên nhận.

Giao thức **TCP** thiết lập một kết nối bằng phương pháp "Bắt tay 3 lần" (**three-way handshake**)




Hình 6.1 – Cách thiết lập kết nối của giao thức **TCP**.

Hình vẽ dưới đây là một ví dụ về cách thức truyền, nhận gói tin bằng giao thức **TCP.**



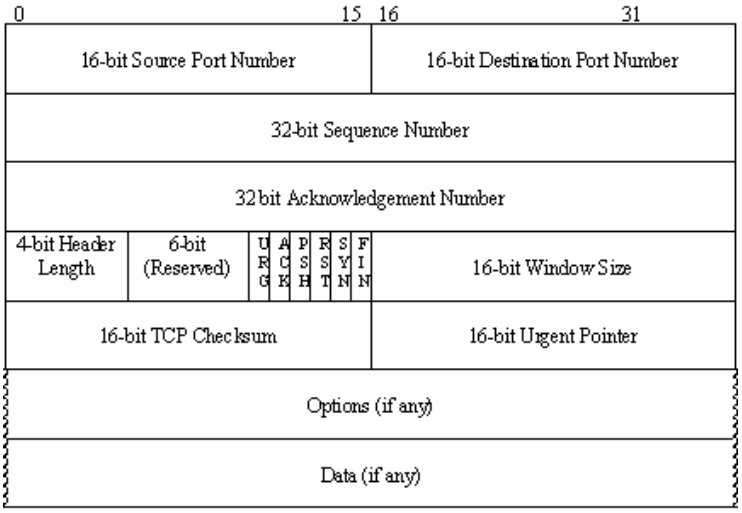

Hình 6.2 – Minh họa cách truyền, nhận gói tin trong giao thức **TCP**.

Giao thức **TCP** là giao thức có độ tin cậy cao, nhờ vào phương pháp truyền gói tin, như cơ chế điều khiển luồng (**flow control**), các gói tin **ACK**,…

Hình vẽ sau đây thể hiện gói tin của **TCP.**



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 6.3 – Cấu trúc gói tin của **TCP**.

Các thành phần trong gói tin:

- **Source port**: port nguồn
- **Destination Port**: port đích
- **Sequence number**: số tuần tự (để sắp xếp các gói tin theo đúng trật tự của nó).
- **Acknowledgment number** (**ACK** số): số thứ tự của Packet mà bên nhận đang chờ đợi.
- **Header Length**: chiều dài của gói tin.
- **Reserved**: trả về 0
- **Code bit**: các cờ điều khiển.
- **Windows**: kích thước tối đa mà bên nhận có thể nhận được
- **Checksum**: máy nhận sẽ dùng 16 bit này để kiểm tra dữ liệu trong gói tin có đúng hay không.
- **Data**: dữ liệu trong gói tin (nếu có).

## III.2. Giao thức UDP (UDP protocol).

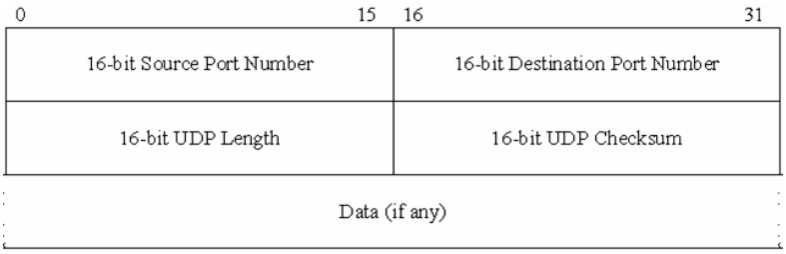
**UDP** không giống như **TCP**, **UDP** là nghi thức phi kết nối, nghĩa là dữ liệu gởi tới đích là không tin cậy. Bởi vì kết nối không được tạo trước khi dữ liệu truyền, do đó **UDP** nhanh hơn **TCP**.

**UDP** là nghi thức không tin cậy, nó không đảm bảo dữ liệu đến đích là không bị mất, đúng thứ tự mà nó nhờ các nghi thức ở lớp trên đảm nhận chức năng này. **UDP** có ưu thế hơn **TCP**:

- Nhờ vào việc không phải thiết lập kết nối trước khi thật sự truyền dẫn dữ liệu nên truyền với tốc độ nhanh hơn.
- Bên nhận không cần phải trả về gói tin xác nhận (**ACK**) nên giảm thiểu sự lãng phí băng thông.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 6.4 – Cấu trúc gói tin của **UDP**.

Các thành phần trong gói tin **UDP**:

- **Source Port**: port nguồn.
- **Destination Port**: port đích.
- **UDP Length**: chiều dài của gói tin.
- **UDP Checksum**: dùng để kiểm tra gói tin có bị sai lệch hay không
- **Data**: dữ liệu đi kèm trong gói tin (nếu có).

## III.3. Khái niệm Port.

Trong cùng một thời điểm, một máy tính có thể có nhiều chương trình đang chạy. Vậy làm sao để xác định một gói tin sẽ được chương trình nào sử dụng?

Khái niệm **Port** ra đời để giải quyết chuyện đó. Mỗi chương trình ứng dụng mạng đều có một **Port** xác định. Để gởi gói tin đến một chương trình tại máy tính A, ta chỉ cần gởi gói tin đến địa chỉ **IP** của máy A, và **Port** mà chương trình đó đang sử dụng.

**TCP** hoặc **UDP** dùng **port** hoặc **socket**, nó là con số mà thông qua đó thông tin được truyền lên các lớp cao hơn. Các con số **port** được dùng trong việc lưu vết các cuộc hội thoại khác nhau trên mạng xảy ra trong cùng một thời điểm. P**o**rt là một loại địa chỉ **logic** trên một máy tính, là con số 2 byte. Các **port** có giá trị nhỏ hơn 1024 được dùng làm các **port** chuẩn. Các ứng dụng dùng port riêng có giá trị lớn hơn 1024. Các giá trị **port** được chứa trong phần địa chỉ nguồn và đích của mỗi **segment TCP**.

Một ứng dụng có thể sử dụng port riêng trong miền cho mình để giao dịch trên mạng nhưng chú ý là không được trùng với các **port** chuẩn.

**Ví dụ một số port chuẩn mà các phần mềm sử dụng**

- **HTTP**: Port number 80
- **FTP**: Port number 21
- **DNS**: Port number 53
- **Telnet**: Port number 23
- **SMTP**: Port number 25
- **TFTP**: Port number 69
- **SNMP**: Port number 161
- **RIP**: Port number 520



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

# IV. CÁC MÔ HÌNH FIREWALL.

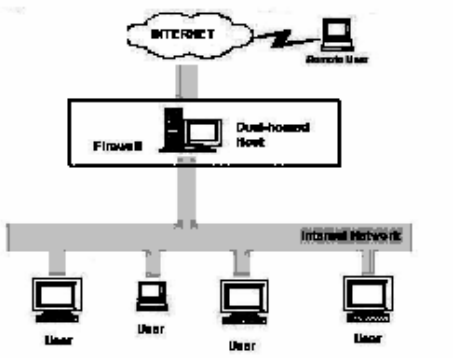
## IV.1. Giới thiệu về Firewall.

**Firewall** hay còn gọi là bức tường lửa được hiểu như là một hệ thống máy tính và thiết bị mạng giúp ta có thể bảo mật và giám sát các truy xuất từ bên trong ra ngoài và ngược lại từ bên ngoài vào trong từ đó ta có thể phòng chống các truy cập bất hợp pháp.

## IV.2. Dual homed host.

**Firewall** kiến trúc kiểu ***Dual-homed host*** được xây dựng dựa trên máy tính **dual-homed host**. Một máy tính được gọi là **dual-homed host** nếu nó có ít nhất hai **network interface**, có nghĩa là máy đó có gắn hai card mạng giao tiếp với hai mạng khác nhau và như thế máy tính này đóng vai trò là **Router** mềm. Kiến trúc **dual-homed** host rất đơn giản. **Dual-homed host** ở giữa, một bên được kết nối với **Internet** và bên còn lại nối với mạng nội bộ (**LAN**).

**Dual-homed host** chỉ có thể cung cấp các dịch vụ bằng cách ủy quyền (**proxy**) chúng hoặc cho phép **users** đăng nhập trực tiếp vào **dual-homed host**. Mọi giao tiếp từ một **host** trong mạng nội bộ và **host** bên ngoài đều bị cấm, **dual-homed host** là nơi giao tiếp duy nhất.




Hình 6.4 – Kiến trúc **Firewall Dual homed host**.

## IV.3. Screened Host.

**Screened Host** có cấu trúc ngược lại với cấu trúc **Dual-homed host**. Kiến trúc này cung cấp các dịch vụ từ một **host** bên trong mạng nội bộ, dùng một **Router** tách rời với mạng bên ngoài. Trong kiểu kiến trúc này, bảo mật chính là phương pháp ***Packet Filtering***.

**Bastion host** được đặt bên trong mạng nội bộ. **Packet Filtering** được cài trên **Router**. Theo cách này, **Bastion host** là hệ thống duy nhất trong mạng nội bộ mà những **host** trên **Internet** có thể kết nối tới. Mặc dù vậy, chỉ những kiểu kết nối phù hợp (được thiết lập trong **Bastion host**) mới được cho phép kết nối. Bất kỳ một hệ thống bên ngoài nào cố gắng truy cập vào hệ thống hoặc các dịch vụ bên trong đều phải kết nối tới **host** này. Vì thế **Bastion host** là **host** cần phải được duy trì ở chế độ bảo mật cao.

**Packet filtering** cũng cho phép **bastion host** có thể mở kết nối ra bên ngoài. Cấu hình của **packet filtering** trên **screening router** như sau:

- Cho phép tất cả các host bên trong mở kết nối tới **host** bên ngoài thông qua một số dịch vụ cố định.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

- Không cho phép tất cả các kết nối từ các **host** bên trong (cấm những **host** này sử dụng dịch **proxy** thông qua **bastion host**).

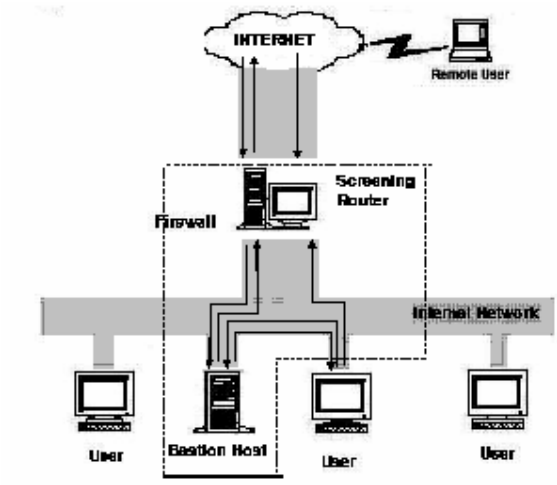
Bạn có thể kết hợp nhiều lối vào cho những dịch vụ khác nhau:

- Một số dịch vụ được phép đi vào trực tiếp qua packet filtering.
- Một số dịch vụ khác thì chỉ được phép đi vào gián tiếp qua **proxy**.

Bởi vì kiến trúc này cho phép các packet đi từ bên ngoài vào mạng bên trong, nó dường như là nguy hiểm hơn kiến trúc **Dual-homed host**, vì thế nó được thiết kế để không một packet nào có thể tới được mạng bên trong. Tuy nhiên trên thực tế thì kiến trúc **dual-homed host** đôi khi cũng có lỗi mà cho phép các packet thật sự đi từ bên ngoài vào bên trong (bởi vì những lỗi này hoàn toàn không biết trước, nó hầu như không được bảo vệ để chống lại những kiểu tấn công này). Hơn nữa, kiến trúc **dual-homed host** thì dễ dàng bảo vệ **Router** (là máy cung cấp rất ít các dịch vụ) hơn là bảo vệ các host bên trong mạng.

Xét về toàn diện thì kiến trúc ***Screened host*** cung cấp độ tin cậy cao hơn và an toàn hơn kiến trúc ***Dual-homed host***.

So sánh với một số kiến trúc khác, chẳng hạn như kiến trúc ***Screened subnet*** thì kiến trúc **Screened host** có một số bất lợi. Bất lợi chính là nếu kẻ tấn công tìm cách xâm nhập ***Bastion Host*** thì không có cách nào để ngăn tách giữa ***Bastion Host*** và các **host** còn lại bên trong mạng nội bộ. **Router** cũng có một số điểm yếu là nếu **Router** bị tổn thương, toàn bộ mạng sẽ bị tấn công. Vì lý do này mà **Sceened *subnet*** trở thành kiến trúc phổ biến nhất.




Hình 6.5 – Kiến trúc **Firewall Screened host**.

## IV.4. Screened Subnet.

Nhằm tăng cường khả năng bảo vệ mạng nội bộ, thực hiện chiến lược phòng thủ theo chiều sâu, tăng cường sự an toàn *cho **bastion host***, tách **bastion host** khỏi các **host** khác, phần nào tránh lây lan một khi **bastion host** bị tổn thương, người ta đưa ra kiến trúc **firewall** có tên là **Sreened Subnet**.

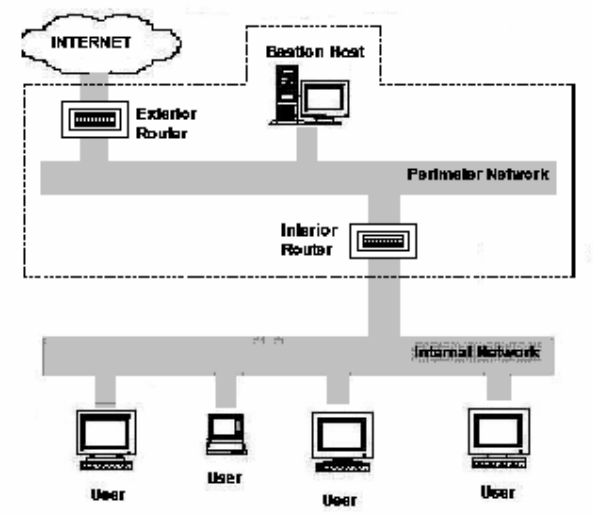


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Kiến trúc **Screened *subnet*** dẫn xuất từ kiến trúc **screened host** bằng cách thêm vào phần an toàn: mạng ngoại vi (**perimeter network**) nhằm cô lập mạng nội bộ ra khỏi mạng bên ngoài, tách **bastion host** ra khỏi các host thông thường khác. Kiểu **screened subnet** đơn giản bao gồm hai **screened router**:

**Router** ngoài (**External router** còn gọi là **access router**): nằm giữa mạng ngoại vi và mạng ngoài có chức năng bảo vệ cho mạng ngoại vi (**bastion host**, **interior router**). Nó cho phép hầu hết những gì outbound từ mạng ngoại vi. Một số qui tắc **packet filtering** đặc biệt được cài đặt ở mức cần thiết đủ để bảo vệ **bastion host** và **interior router** vì **bastion host** còn là **host** được cài đặt an toàn ở mức cao. Ngoài các qui tắc đó, các qui tắc khác cần giống nhau giữa hai **Router**.

**Interior Router** (còn gọi là **choke router**): nằm giữa mạng ngoại vi và mạng nội bộ, nhằm bảo vệ mạng nội bộ trước khi ra ngoài và mạng ngoại vi. Nó không thực hiện hết các qui tắc **packet filtering** của toàn bộ **firewall**. Các dịch vụ mà **interior router** cho phép giữa **bastion host** và mạng nội bộ, giữa bên ngoài và mạng nội bộ không nhất thiết phải giống nhau. Giới hạn dịch vụ giữa **bastion host** và mạng nội bộ nhằm giảm số lượng máy (số lượng dịch vụ trên các máy này) có thể bị tấn công khi bastion host bị tổn thương và thoả hiệp với bên ngoài. Chẳng hạn nên giới hạn các dịch vụ được phép giữa bastion host và mạng nội bộ như **SMTP** khi có **Email** từ bên ngoài vào, có lẽ chỉ giới hạn kết nối **SMTP** giữa **bastion host** và **Email server** bên trong.




Hình 6.6 – Kiến trúc **Firewall Screened Subnet**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

# Tóm tắt

Lý thuyết 6 tiết - Thực hành 20 tiết

| Mục tiêu | Các mục chính | Bài tập bắt buộc | Bài tập làm thêm |
|---|---|---|---|
| Kết thúc bài học này cung cấp học viên kỹ năng sử dụng các công cụ client của các dịch vụ mạng cơ sở như: web, ftp, mail… | I. Dịch vụ Web.<br>II. Dịch vụ FTP.<br>III. Dịch vụ e-mail.<br>IV. Ngôn ngữ HTML. | Dựa vào bài tập môn mạng máy tính. | Dựa vào bài tập môn mạng máy tính. |



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

# V. DỊCH VỤ WORLD WIDE WEB.

## V.1. Một số khái niệm về Internet.

**Các thuật ngữ cơ sở.**

- **HTTP** (**Hypertext Transfer Protocol**): là giao thức cho phép các máy tính giao tiếp qua **World Wide Web** và kết nối với nhau qua các **hyperlink**.
- **Gopher**: là hệ thống cho phép ta duyệt các tài nguyên trên mạng **Internet**, dịch vụ này ra đời trước **Web** và hoạt động giống như một danh bạ, liệt kê các tập tin sắp xếp theo tầng.
- Dịch vụ trực tuyến (**Online Service**): là những dịch vụ truy cập **Internet** có thu cước phí do các công ty lớn cung cấp như: **AOL** (**America Online**), **CompuServe** hoặc **MSN** (**Microsoft Network**).
- **HTML** (**Hypertext Markup Language**): là ngôn ngữ định dạng dùng để tạo ra các trang Web giúp người dùng có thể đọc và truy cập từ bất kỳ máy nào trên mạng, dùng bất kỳ hệ điều hành nào.
- **WebPage**: là một trang tư liệu Web.
- **WebSite**: là tập hợp các trang Web của một tổ chức, một công ty, một web site có thể có nhiều **Web Server**.
- **Home page**: là trang Web đầu tin của một Web Site hoặc trang Web xuất hiện đầu tin khi khởi động **Web Browser**, đồng thời trang này chứa các liên kết tiêu biểu đến các trang Web còn lại.
- **HyperLink** (**link**): là các mối liên kết giữa các tư liệu. Thông thường, trong một trang Web, các mối liên kết có màu xanh dương và được gạch dưới. Ngoài ra, bất kỳ một hình ảnh, văn bản nào khi di chuyển con trỏ chuột tới chuyển sang hình  đều là các liên kết (**link**).
- **URL** (**Uniform Resource Locator**): là đường dẫn chỉ tới một tập tin trong một máy chủ trên **Internet**. Chuỗi **URL** thường bao gồm: tên giao thức, tên máy chủ và đường dẫn đến tập tin trong máy chủ đó. Ví dụ: http://www.hcmuns.edu.vn/TongQuan/Tongquan.htm có nghĩa là: giao thức sử dụng http:// (**Hypertext Transfer Protocol**), tên máy chủ: **www.hcmuns.edu.vn**, đường dẫn và tên tập tin: /TongQuan/Tongquan.htm.
- Lưu ý: đường dẫn sử dụng dấu "/" thay cho dấu "\".
- **IXP** (**Internet Exchange Provider**): là nhà cung cấp đường truyền và cổng truy cập **Internet**.
- **ISP** (**Internet Service Provider**): là nhà cung cấp dịch vụ Internet cho người dùng trực tiếp qua mạng điện thoại như là cấp quyền truy cập **Internet**, cung cấp các dịch vụ như **Web**, **E-mail**, **Chat**, **Telnet**…
- **ICP** (**Internet Content Provider**): là nhà cung cấp thông tin lên **Internet**, thông tin được cập nhật định kỳ hay thường xuyên và thuộc nhiều lĩnh vực như thể thao, kinh tế giáo dục, chính trị, quân sự …



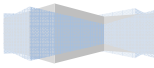
**Các hoạt động chính trên Web.**

- Duyệt **Web** tìm kiếm thông tin như số điện thoại, địa chỉ nhà, tin tức, tin dự báo thời tiết, bảng giá

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

chứng khoán, các phần mềm miễn phí…





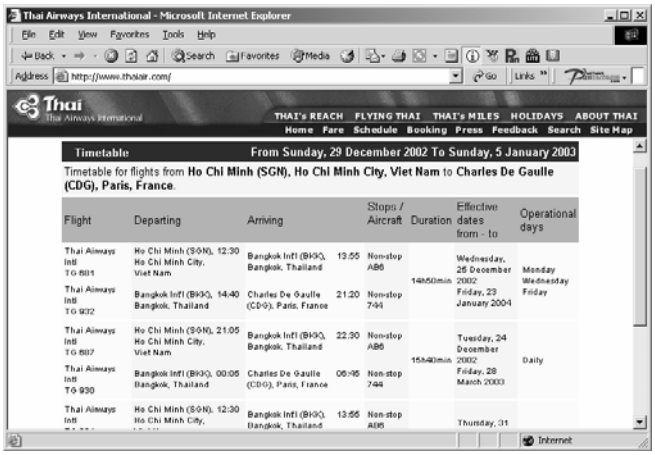
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net


Hình 7.1 – Minh họa một số trang **Web** để tìm kiếm thông tin.

- Giải trí như nghe nhạc,xem phim, chơi game trên mạng.
- Trao đổi **E-mail**.
- Truy xuất và **download** các tập tin.
- Tán ngẫu (chat).
- Sắp xếp các chuyến đi du lịch như đặt vé máy bay, đăng ký phòng khách sạn...

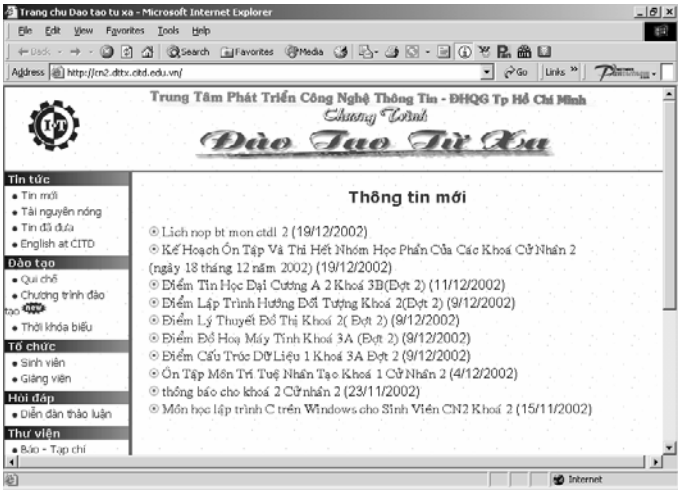


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 7.2 – Minh họa một trang **Web** dùng để tìm thông tin các chuyến bay.

- Đào tạo từ xa qua mạng.

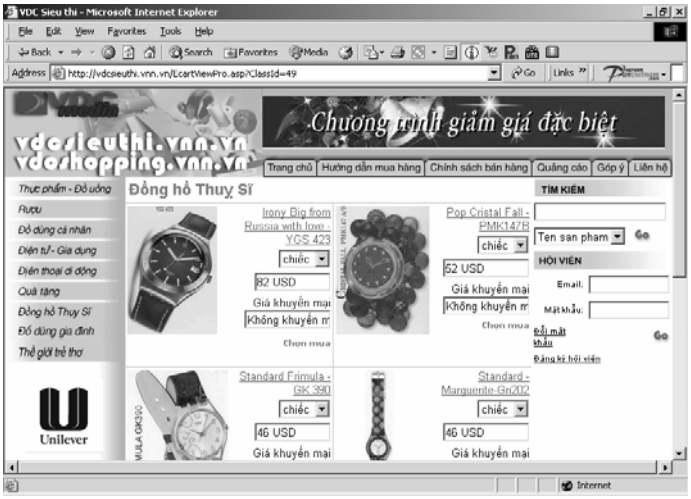



Hình 7.3 – Minh họa một trang **Web** dùng để đào tạo từ xa.

- Hội thảo từ xa.
- Quảng cáo sản phẩm.
- Đặt mua hàng.

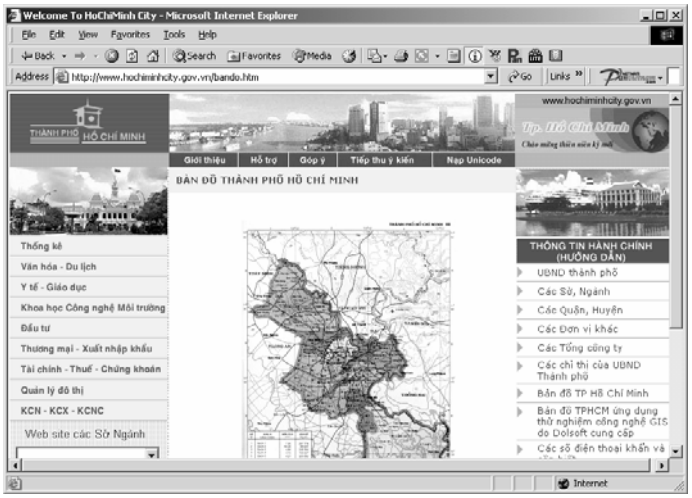


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 7.4 – Minh họa một số trang **Web** dùng để mua bán qua mạng.

- Thực hiện các giao dịch ngân hàng.
- Hỗ trợ chính phủ điện tử và thương mại điện tử.



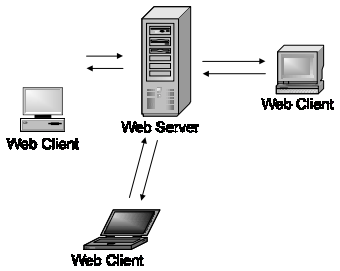

Hình 7.5 – Minh họa một trang **Web** của Tp HCM.

## V.2. Giới thiệu mô hình hoạt động của Web.

Dịch vụ **World Wide Web** (viết tắt là **www** hoặc **Web**) là một dịch vụ cung cấp thông tin trên hệ thống mạng. Các thông tin này được lưu trữ dưới dạng siêu văn bản (**hypertext**) và thường được thiết kế bằng ngôn ngữ **HTML** (**Hypertext Markup Language**). Siêu văn bản là các tư liệu có thể là văn bản (**text**), hình ảnh tĩnh (**image**), hình ảnh động (**video**), âm thanh (**audio**)...., được liên kết với nhau qua các mối liên kết (**link**) và được truyền trên mạng dựa trên giao thức **HTTP** (**Hypertext Transfer Protocol**), qua đó người dùng có thể xem các tư liệu có liên quan một cách dễ dàng. Mô hình hoạt động:



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 7.6 – Mô hình hoạt động của **Web Server**.

**Web server**: là một ứng dụng được cài đặt trên máy chủ trên mạng với chức năng là tiếp nhận các yêu cầu dạng **HTTP** từ máy trạm và tùy theo yêu cầu này máy chủ sẽ cung cấp cho máy trạm các thông tin web dạng **HTML**.

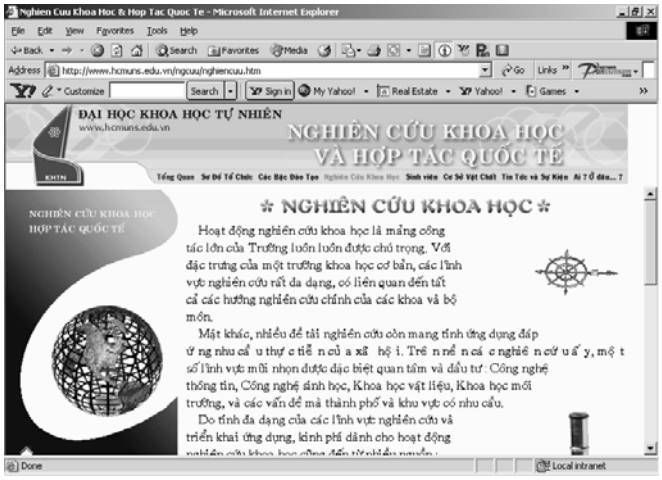
**Web Client**: là một ứng dụng cài trên máy trạm (máy của người dùng đầu cuối) gọi là **Web Browser** để gởi yêu cầu đến **Web Server** và nhận các thông tin phản hồi rồi hiện lên màn hình giúp người dùng có thể truy xuất được các thông tin trên máy **Server**. Một trong những trình duyệt **Web** (**Web Browser**) phổ biến nhất hiện nay là **Internet Explorer**.

## V.3. Khảo sát web browser Internet Explorer.

Chương trình **Internet Explorer** rất quen thuộc với người dùng vì nó đã tích hợp sẵn trong các hệ điều hành của **Microsoft** như **Win9x**, **Win2K**, **WinXP**… Nhưng chú ý là các phiên bản **IE** trên các hệ điều hành **Win9X**, **WinME** là những phiên bản cũ và có nhiều lỗ hổng cần cài phiên bản mới và cài các chương trình sửa lỗi cho các phiên bản đó. (Để sửa lỗi ta nên vào trang **Web Support** của **Microsoft**, rồi **download** các chương trình sửa lỗi cho **IE** và cài lên máy)

**Truy cập vào các Web site.**

Trước khi duyệt các **Website** ta phải khởi động chương trình bằng cách click **Start/Programs/Internet Explorer/Internet Explorer**, đối với **Win2K** thì **Start/Programs/Internet Explorer**. Sau khi chương trình đã chạy, ta nhập địa chỉ **Website** mà ta cần truy cập vào ô **Address**. Ví dụ: trong hình dưới đây là địa chỉ: **http://www.hcmuns.edu.vn/ngcuu/nghiencuu.htm**. (1)

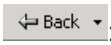



Hình 7.7 – Nội dung của trang Web (1)



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

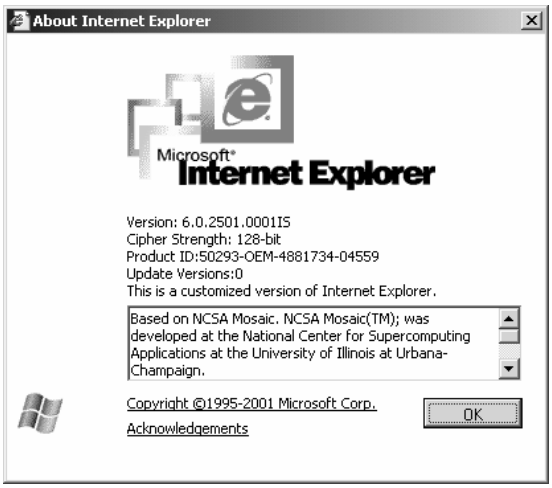
Ngoài ra để duyệt thông tin trên **Website** nhanh ta có thể sử dụng các nút trên thanh công cụ sau:


- Nút quay về trang trước 

: các trang Web đã duyệt qua phần lớn chứa trong thư mục **Temporary Internet Files** (trong **Win98** thì thư mục cache là C**:\Windows\Temporary Internet Files**, trong **Win2K** trở lên là **C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files**), do đó khi cần quay về trang Web trước ta dùng chức năng **Back** để **IE** đọc thông tin trong đĩa cứng không cần lấy từ **Internet** nữa, nhằm tăng tốc độ duyệt **Web**.
- Nút tới trang sau  : cũng tương tự như chức năng **Back**, tính năng **Forward** giúp ta truy cập nhanh trang Web phía sau đã duyệt rồi chứa trong đĩa cứng.
- Nút ngừng tải dữ liệu  : khi ta muốn ngừng truy xuất vào một **Website** hiện tại ta chọn tính năng **Stop**.
- Nút về trang chủ  (**HomePage** hay trang mặc định): giúp ta trở về trang default được quy định trong mục **Option**.
- Nút cập nhật lại thông tin  : khi duyệt các trang Web cũ mà **IE** không chịu lấy thông tin mới trên **Internet** mà cứ lấy thông tin trong đĩa cứng, ta cần chọn chức năng **Refresh** để cập nhật thông tin mới từ **Internet**.

**Kiểm tra phiên bản và nâng cấp IE**

Trước khi dùng **IE** duyệt **Web** ta cần kiểm tra phiên bản hiện tại để quyết định nâng cấp hoặc cài chương trình sửa lỗi tránh trường hợp duyệt **Web** không an toàn. Xem phiên bản của **IE** Click vào menu **Help** - **About Internet Explorer**, như hình sau là phiên bản 6.0.




Hình 7.8 – Hộp thoại hiển thị phiên bản **Internet Explorer 6.0**.

**Lưu hình và nội dung văn bản từ trang Web.**

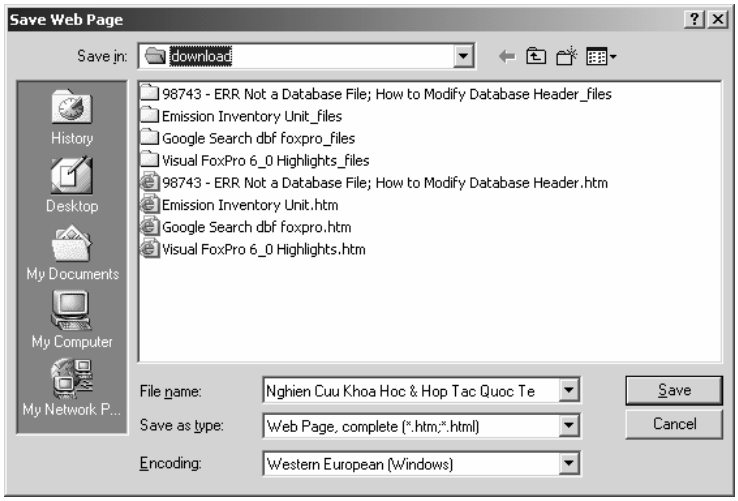
Như là bạn thấy trên trang Web, có rất nhiều nội dung hay mà bạn cần lưu trữ lại và chia sẻ cho nhiều người cùng biết. Bạn có thể lưu trữ toàn bộ trang web hoặc một phần trang Web như: một đoạn văn bản, hình hoặc những liên kết. Bạn cũng có thể in toàn bộ trang Web ra giấy.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

| Yêu cầu | Thao tác |
|---|---|
| Lưu một trang hoặc một hình mà không cần mở nó lên. | Click phải chuột vào kết nối của biểu tượng mà bạn cần muốn lưu và sau đó click **Save Target As** |
| Copy thông tin từ một trang Web vào một tài liệu. | Chọn thông tin mà bạn muốn sao chép trên trang Web và sau đó vào menu **Edit**, click **Copy**. Bạn chuyển qua tài liệu cần lưu trữ và chọn **Paste**. |
| Tạo một **shortcut** trên **desktop** cho trang Web hiện tại. | Click phải chuột vào trang hiện tại, và sau đó click **Create Shortcut** |
| Dùng hình trên trang Web như là hình nền | Click phải chuột vào hình trên trang Web và click vào **Set As Wallpaper** (hoặc **Set As Background**) |
| Gởi một trang Web trong **E-mail** | Trên menu **File**, chọn **Send**, sau đó click vào **Page by E-mail** hoặc **Link by E-mail**. Một cửa sổ của **mail** mới hiện ra, bạn nhập nội dung vào và gởi **mail**. Chú ý là bạn phải có tài khoản mail và chương trình **E-mail** đã cài đặt trên máy tính của bạn. |

Lưu toàn bộ trang Web: vào menu **File** chọn **Save As**, sau đó chọn đường dẫn và nhập tên tập tin cần lưu trữ.

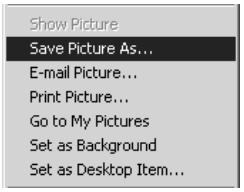



Hình 7.9 – Hộp thoại hiển thị sau khi chọn **Save As**.

Lưu hình trên trang Web: click phải chuột trên hình cần lưu trữ và chọn chức năng **Save Picture As**, sau đó chọn đường dẫn và tên tập tin cần lưu trữ.



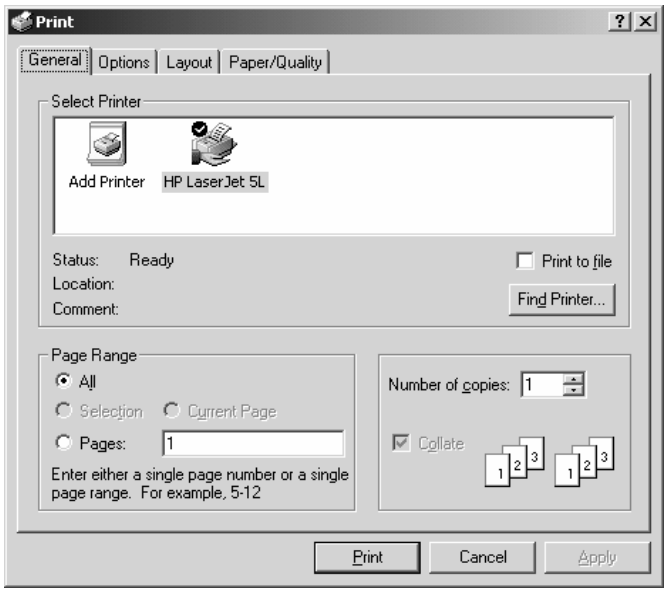
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 7.10 – Danh sách các thuộc tính sau khi click chuột phải lên hình ảnh.

**In trang Web.**

Muốn in trang Web hiện tại, ta vào menu **File**, chọn chức năng **Print** hoặc ấn phím tắt **Ctrl+P**, nhưng bạn chú ý là phải chọn khổ giấy và canh lề cho phù hợp.



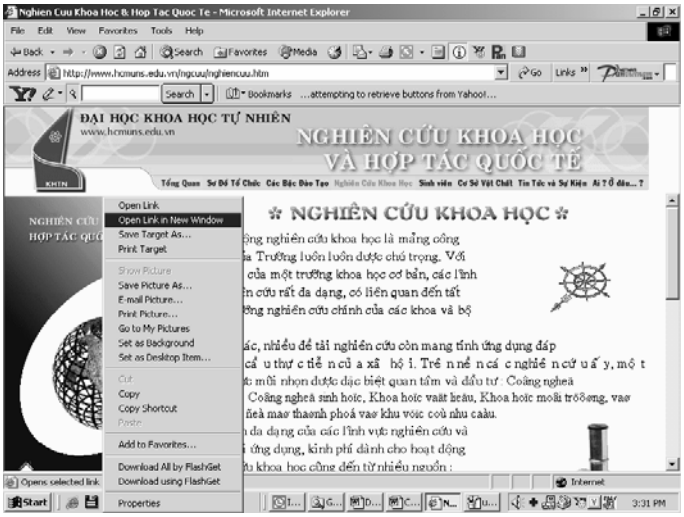

Hình 7.11 – Hộp thoại hiển thị sau khi chọn lựa **Print** (hoặc **Ctrl-P**).

**Liên kết đến các trang Web khác.**

Bạn có thể click chuột vào các liên kết để truy cập vào các trang Web khác, nhưng khi đó nội dung trang web mới sẽ chồng lên trang cũ, nếu bạn muốn nội dung trang Web mới hiển thị trong một cửa sổ khác thì bạn click phải chuột vào liên kết và chọn **Open Link in New Windows**



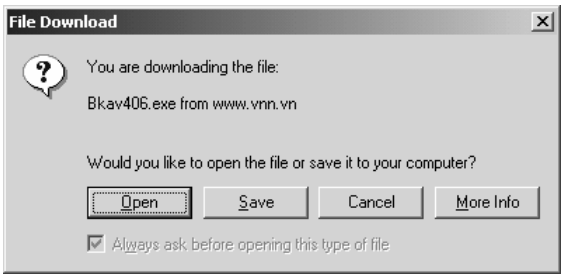
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 7.12 – Hộp thoại hiển thị khi click chuột phải vào Link “Nghiên cứu”.

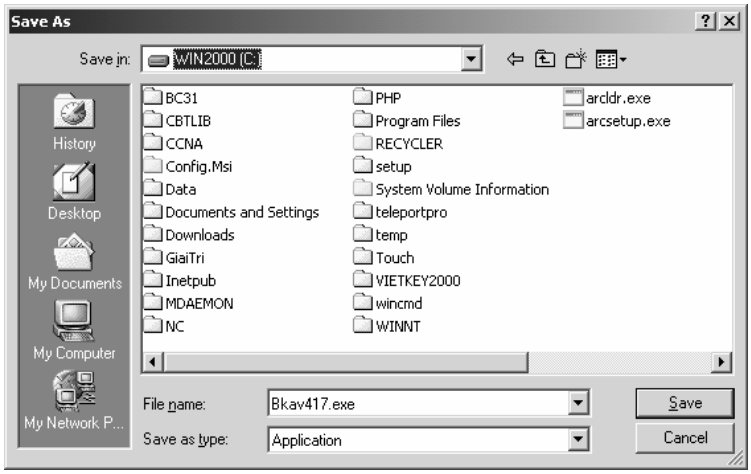
**Download.**

**Download file** là quá trình tải một file từ **Internet** về máy trạm, bạn click vào liên kết, **IE** xuất hiện hộp thoại **download**, bạn chọn **Save**, hộp thoại **Save As** xuất hiện, bạn chọn đường dẫn và nhập tên tập tin cần lưu trữ. Click vào nút **Save**.




Hình 7.13 – Hộp thoại hiển thị sau khi chọn **Download**.

Chỉ ra đường dẫn và nhập vào tên tập tin, Click nút **Save.**





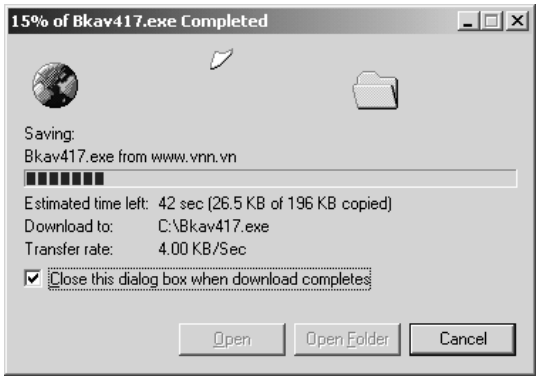

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Hình 7.14 – Hộp thoại hiển thị sau khi chọn **Save**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

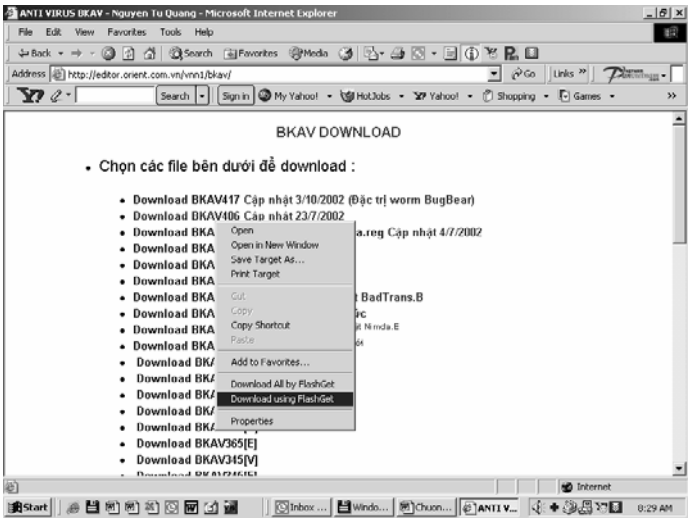
Hình dưới là hiển thị trạng thái **download** như thời gian dự đoán sẽ hoàn thành, số **byte** đã **download**, số **byte** cần **download**, tên tập tin, tốc độ truyền.




Hình 7.15 – Hộp thoại hiển thị quá trình download của tập tin Bkav417.exe

Một lưu ý quan trọng là khi đang **download** đường mạng bị nghẽn hoặc đứt kết nối thì xem như phần đã **download** không còn được sử dụng nữa. Khi **download** những tập tin có kích thước lớn thì làm theo cách này là không khả thi vì kết nối mạng rất dễ đứt trong khi thời gian **download** rất lâu. Muốn vậy ta phải dùng phần mềm **download** chuyên nghiệp có tính năng **download** tiếp tục (**resume**) khi kết nối mạng đứt và cho phép cắt tập tin thành nhiều phần nhỏ giúp **download** nhanh hơn ví dụ như: **FlashGet**, **NetAnt**…

Ví dụ sau ta dùng **FlashGet** để **download** một chương trình diệt **Virus**, chú ý trước khi bạn dùng theo hướng dẫn bạn phải cài đặt chương trình **FlashGet** trước trên máy của bạn.



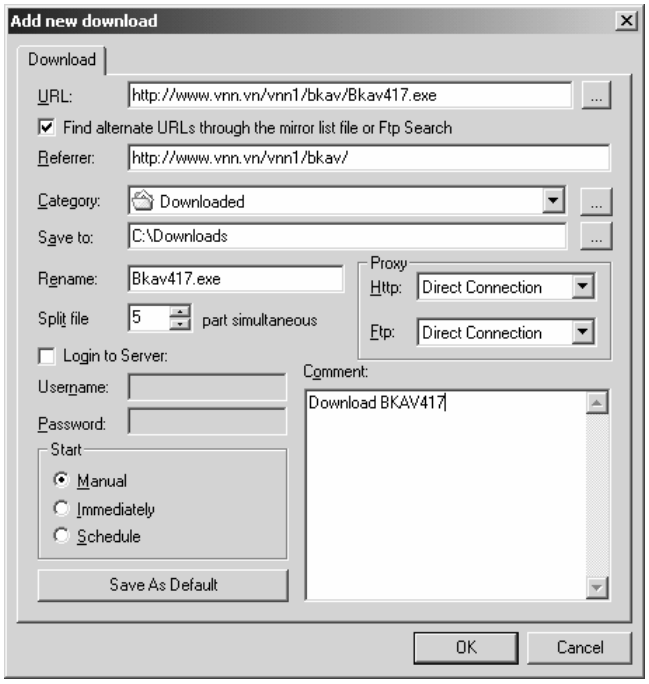

Hình 7.16 – Hộp thoại hiển thị khi click chuột phải vào **Bkav406**.

Bạn click phải chuột vào **link** và chọn chức năng **Download using FlashGet**, hộp thoại **Add New Download** xuất hiện và bạn nhập một số thông tin phù hợp như **proxy**, số phần chia tập tin, sau đó chọn **OK**.



Trong mục **Split File** ta nhập giá trị số phần tập tin bị cắt ra, mục **Proxy** là cổng ra ngoài **Internet** của máy bạn.

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 7.17 – Hộp thoại hiển thị sau khi chọn **Download using FlashGet**.

Trong ví dụ này file **Bkav405**.exe được phân ra thành 5 tập tin và trên màn hình hiển thị tiến độ **download** của mỗi phần.

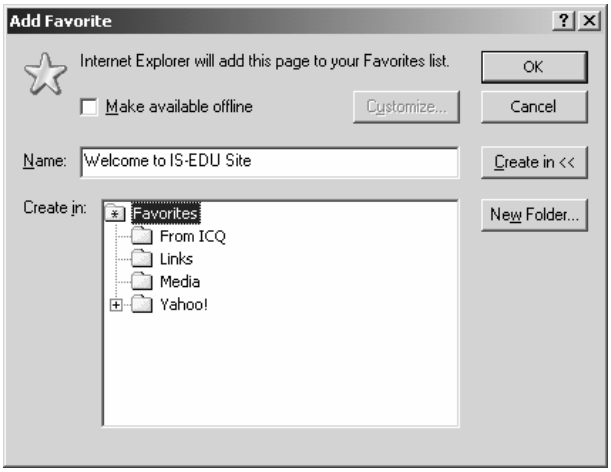

Hình 7.18 – Hộp thoại hiển thị tiến trình download tập tin Bkav405.exe

**Tổ chức lưu trữ địa chỉ các trang Web thường truy cập.**

Khi duyệt Web, ta muốn lưu lại địa chỉ một số trang Web hay và tổ chức theo trật tự dễ nhớ, dễ tìm kiếm. Muốn lưu địa chỉ trang Web hiện hành bạn vào menu **Favorites** chọn **Add to Favorites**, hộp thoại **Add Favorites** xuất hiện, bạn chọn vị trí lưu và nhập tên của trang Web, sau đó chọn **OK**. Nếu bạn muốn tạo thêm thư mục riêng thì chọn **New Folder.**

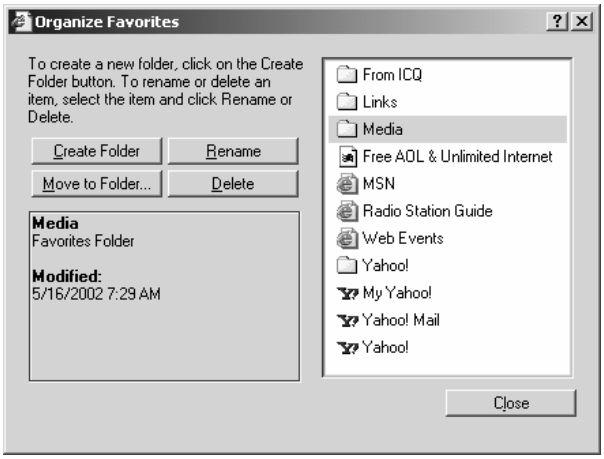


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 7.19 – Hộp thoại hiển thị sau khi chọn **Add Favorites**.

Bạn muốn tìm địa chỉ các trang Web đã lưu hay sắp xếp các địa chỉ của các trang này theo tổ chức nhất định bạn vào menu **Favorites** và chọn chức năng **Organize Favorites**. Hộp thoại **Organize Favorites** xuất hiện, bạn Click vào **Create Folder** để tạo mục mới, thay đổi tên thư mục click vào **Rename**, di chuyển thư mục chọn **Move to Folder**, xóa chọn **Delete**. Bạn muốn xem nội dung mục nào thì **Double Click** vào mục đó. Muốn di chuyển trang Web hoặc một thư mục con vào một thư mục khác thì bạn click và kéo thả vào thư mục đó.



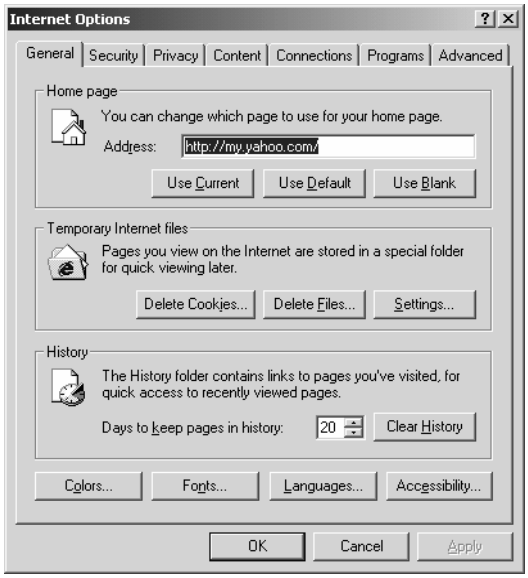

Hình 7.20 – Hộp thoại **Organize Favorites**.

**Cấu hình Internet Option.**

Phần lớn các cấu hình quan trọng của **IE** đều tập trung trong hộp thoại **Internet Options**. Muốn mở hộp thoại này bạn vào menu **Tools** chọn **Internet Option**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 7.21 – Hộp thoại **Internet Options**.

Trong phần **HomePage**, chỉ ra địa chỉ trang Web làm **HomePage** trong ô **Address**. Ngoài ra, còn có thể sử dụng các nút lệnh như : sử dụng trang Web hiện hành làm **HomePage** click vào **Use Current**, sử dụng http://www.adminviet.net/ làm **HomePage** click vào **Use Default**, không sử dụng **HomePage** click vào **Use Blank**.

Khi truy cập thông tin Web, để tiết kiệm thời gian cho các lần truy cập sau, các **Web Browser** thường lưu trữ tạm các thông tin đã truy cập trên đĩa. Vùng lưu trữ tạm này gọi là **Cache**. Như vậy, khi truy cập một trang Web, trước tiên **Web Browser** sẽ kiểm tra trang Web cần truy cập đã có trong **cache** hay chưa, nếu có nó sẽ hiển thị thông tin trong **cache** thay vì phải truy cập vào **Web Server** để lấy thông tin. Tuy nhiên, thông tin lưu trữ trong **cache** có thể bị lạc hậu so với thông tin thực tế do đó các **Web Browser** phải có cơ chế kiểm tra. Trong **Internet Explorer**, có bốn cơ chế:

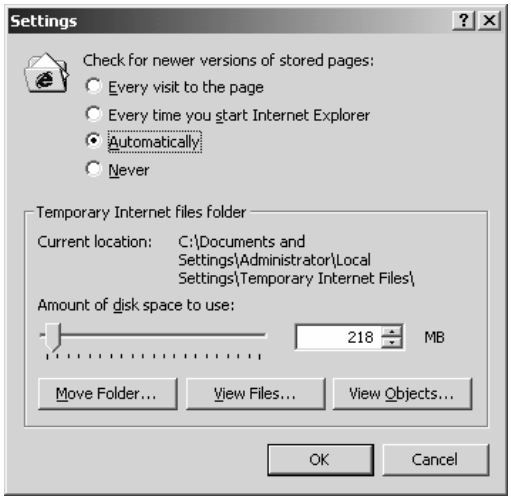
- **Every visit to the page**: kiểm tra thông tin trong **cache** so với thông tin thực tế mỗi lần truy cập vào một trang Web.
- **Every time you start Internet Explorer**: kiểm tra thông tin trong **cache** so với thông tin thực tế mỗi lần khởi động **Internet Explorer**.
- **Automatically**: tự động hệ thống **IE** sẽ kiểm tra.
- **Never**: không cần kiểm tra, luôn lấy thông tin trong **Cache**.

Cấu hình **Temporary Internet Files**:

- Click vào **Delete Cookies** để xoá các thông tin mà **IE** lưu trữ trong **Cookies**.
- Click vào **Delete Files** để xoá các file được lưu trữ trong vùng lưu trữ tạm (**cache**)
- Click vào **Setting** để cấu hình các thông số cho vùng lưu trữ tạm. Bạn chọn cách thức kiểm tra của **IE** và thay đổi kích thước của vùng lưu trữ tạm.



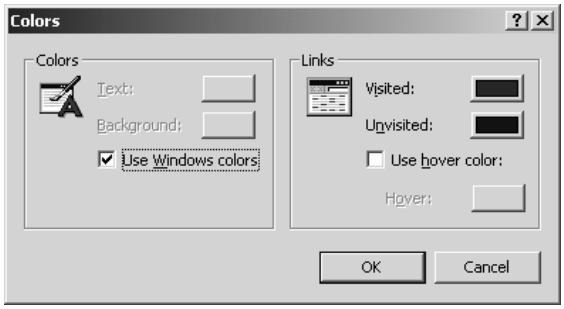
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 7.22 – Hộp thoại **Settings**.

Cấu hình **History**: trong mục **Days to keep pages in history** cho phép ta quy định số ngày mà **IE** nhớ các địa chỉ trang Web mà ta đã duyệt qua. Muốn xóa tất cả các địa chỉ này ta click và nút **Clear History**.

Click vào nút **Colors** để thay đổi màu của các thành phần sau như : màu của văn bản bình thường (các văn bản không phải link), màu nền, màu của các **Link** chưa duyệt qua, màu của các **Link** đã duyệt qua. Ngoài ra, để các link đổi màu khi di chuyển con trỏ chuột tới thì chọn **Use Hover color**, sau đó chỉ định màu cho **Hover**.

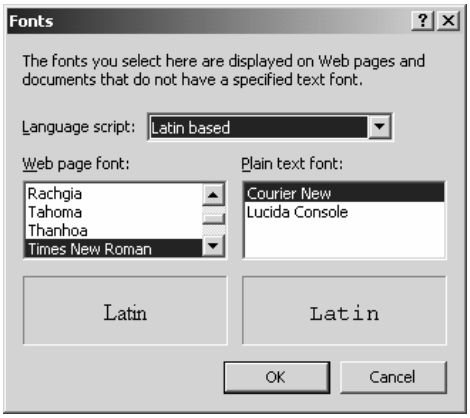



Hình 7.23 – Hộp thoại **Colors**.

Click vào nút **Font** để thay đổi cấu hình của **Font**.

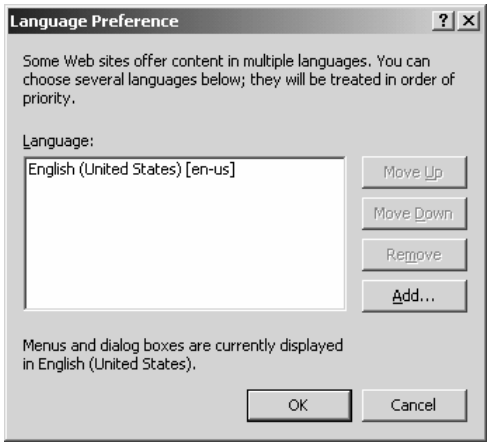


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 7.24 – Hộp thoại **Fonts**.

Click vào nút **Language** để chọn ngôn ngữ hiển thị nếu Website đó hỗ trợ đa ngôn ngữ.



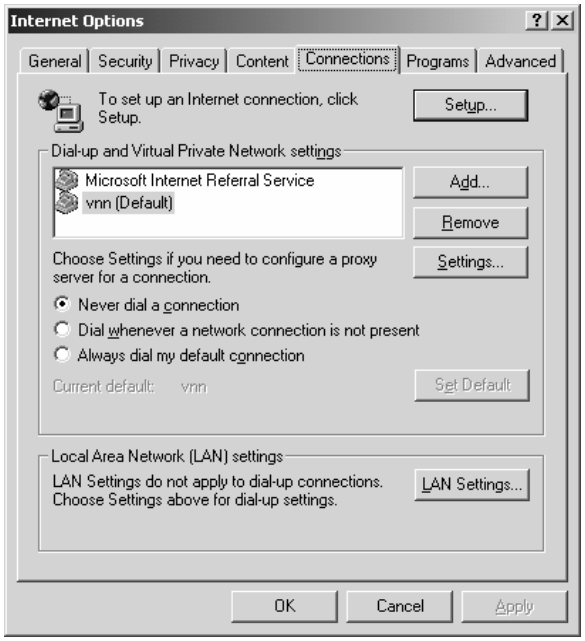

Hình 7.25 – Hộp thoại **Language**.

**Cấu hình kết nối Internet.**

Muốn truy cập được **Internet**, bạn phải tạo các kết nối **Internet**, hai kết nối thông dụng là **Dial-up** và **LAN**. Trong **Tab Connections** bạn có thể chọn các kết nối **Dial-up** có sẵn hay tạo kết nối khác. Nếu bạn chọn hình thức kết nối **Internet** qua mạng **LAN** thì bạn click vào nút **LAN Settings**.

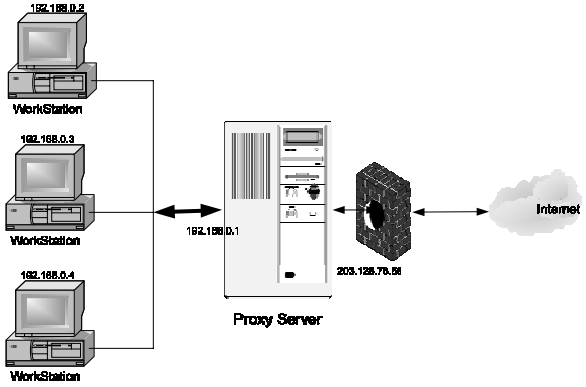


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 7.26 – Hộp thoại **Internet Options – Tab Connections**.

Thông thường các máy trạm truy cập **Internet** qua mạng **LAN** thì các máy trạm này không trực tiếp lên **Internet** để lấy thông tin mà gởi yêu cầu đến một máy làm đại diện (**proxy**). Máy đại diện này được kết trực tiếp lên **Internet**, do đó máy này sẽ lấy thông tin giúp các máy trạm và gởi trả các thông tin về cho các máy trạm. Máy trạm nhận thông tin và hiển thị nội dung lên màn hình giúp cho người dùng cảm giác như mình được trực tiếp sử dụng các dịch vụ **Internet** nhưng thực tế thì không. Như vậy, các máy trạm muốn truy cập **Internet** thì phải khai báo địa chỉ máy **Proxy**.

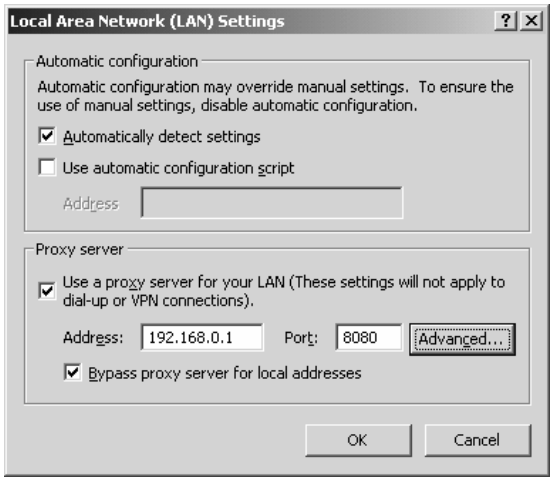



Hình 7.27 – Mô tả mô hình hoạt động của **Proxy**.

Trong hộp thoại **LAN Setting**, bạn nhập địa chỉ **IP** của **Proxy** và giá trị **port** mà **proxy** cho phép các máy trạm đi qua.

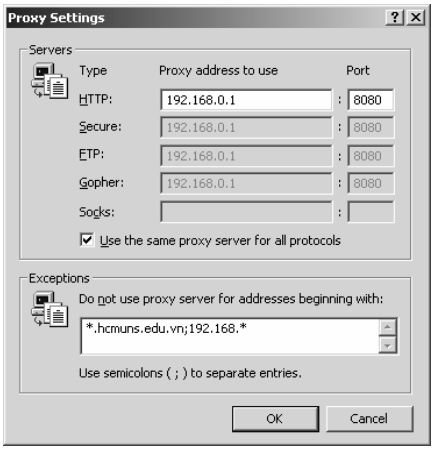


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 7.28 – Hộp thoại **LAN Settings**.

Ngoài ra có một số địa chỉ mà ta muốn truy cập trực tiếp mà không cần qua **Proxy**, thì ta nhập vào ô **Exceptions**.



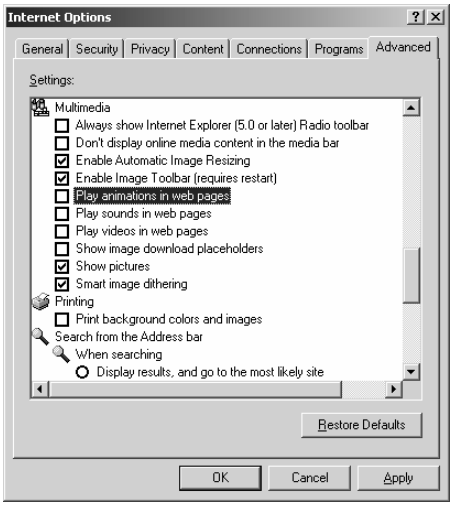

Hình 7.29 – Hộp thoại **Proxy Settings**.

**Duyệt web không trình diễn hình và nhạc**

Đôi lúc ta cần tìm nhanh một tài liệu nào đó trên mạng mà chỉ cần text không cần hình ảnh thì ta nên tắt chế độ trình diễn hình và nhạc trên **IE** vì khi tắt các chế độ này đi thì trang web sẽ được duyệt nhanh hơn. Ta vào menu **Tools/Internet Option** chọn **Tab Advanced**, trong mục **Multimedia** bỏ các đánh dấu vào các mục: **play animations**, **play sounds**, **play videos**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 7.30 – Hộp thoại **Internet Options – Tab Advance**.

## V.4. Search Engine và tìm kiếm thông tin trên Web.

**Giới thiệu về Search Engine.**

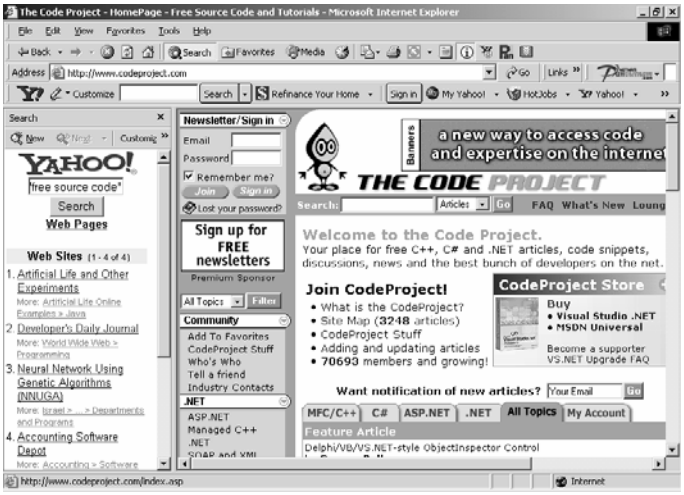
**Search Engine** thông thường là một hệ thống mạng lớn chạy song song và có thể xử lý phân tán chạy trên nhiều máy tính. Hệ thống này được chia thành ba tầng chính, gồm tầng thu thập thông tin, nhận dạng và chuyển đổi thông tin thành dạng text, lập cơ sở dữ liệu cho các thông tin dạng text. Mỗi tầng được chia thành nhiều đơn vị độc lập hoạt động theo kiểu chia sẻ tính toán hoặc dự trữ (redundant), từ đó tính tin cậy và hiệu năng của hệ thống rất cao. Đơn vị khai thác dữ liệu được tích hợp cùng với phần lập chỉ mục cơ sở dữ liệu, cho phép khai thác qua các client sử dụng giao thức **TCP/IP** trên bất kỳ hệ thống nào (**Windows**, **Unix**…). Việc chia hệ thống thành các khối chức năng phối hợp với nhau thông qua bộ điều phối, hệ thống có thể phân tán để xử lý trên nhiều máy tính nhỏ hay tập trung toàn bộ trên hệ thống máy lớn. Vì vậy, lượng dữ liệu mà hệ thống có thể phục vụ, về mặt nguyên tắc cho phép đến hàng trăm triệu tài liệu.

**Tìm kiếm thông tin trên Web**

Công cụ tìm kiếm trên **IE**, bạn muốn tìm kiếm trong **IE** bạn click vào nút **Search** trên thanh trạng thái, bên trái của cửa sổ **IE** xuất hiện hộp thoại tìm kiếm, bạn nhập chuỗi cần tìm kiếm. Ví dụ như hình sau ta tìm kiếm các trang Web cung cấp miễn phí các **source code** hỗ trợ học tập.



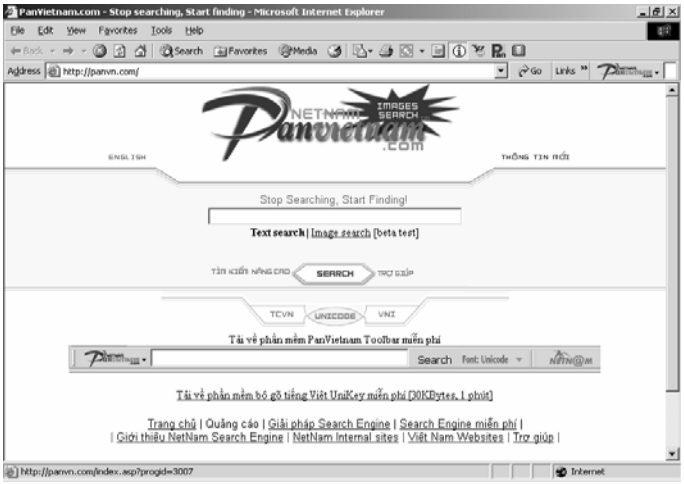
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 7.31 – Kết quả sau khi **Search** bằng từ khóa "**free source code**".

*Công cụ tìm kiếm* ***Panvietnam***, **Panvietnam** sử dụng hầu hết các công nghệ mới nhất trong tìm kiếm thông tin tương tự như **Google** nhưng nó còn tích hợp thêm các công nghệ đặc thù dành cho **Việt Nam** như:

- Hỗ trợ tiếng việt với cả ba bộ mã chính như : **Unicode**, **TCVN**, **VNI**. Suy đoán bộ mã tiếng việt thông minh.
- Xử lý song song.
- Cơ chế trả lời kết quả thông minh.
- Hỗ trợ mọi hệ thống sử dụng chuẩn giao tiếp **TCP** (**Windows**, **Unix**, **Macitosh**).
- Không giới hạn số lượng tài liệu tìm kiếm.
- Tốc độ cập nhật thông tin mới nhanh.
- Hỗ trợ trên 200 định dạng tài liệu phổ biến nhất.




Hình 7.32 – Trang Web **Panvietnam**.

Bạn nhập vào chuỗi cần tìm kiếm mạng máy tính thì kết quả trả về như hình sau. Mỗi kết quả tìm được là một đường link đến một Website chứa thông tin mà ta cần tìm. Muốn xem chi tiết nội dung thì ta

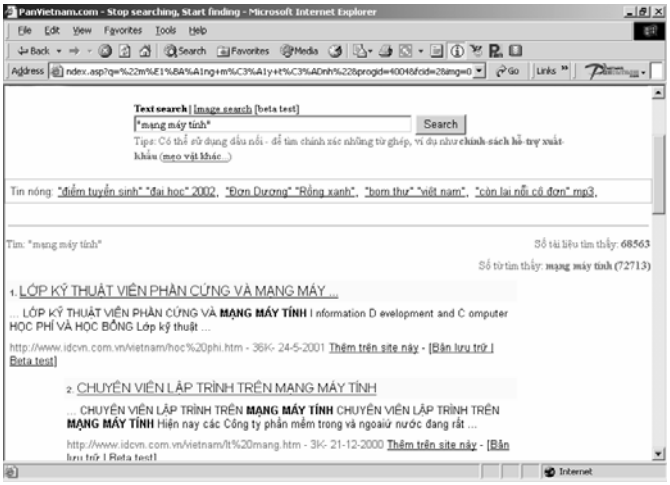


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

click chuột vào đường **link** này.

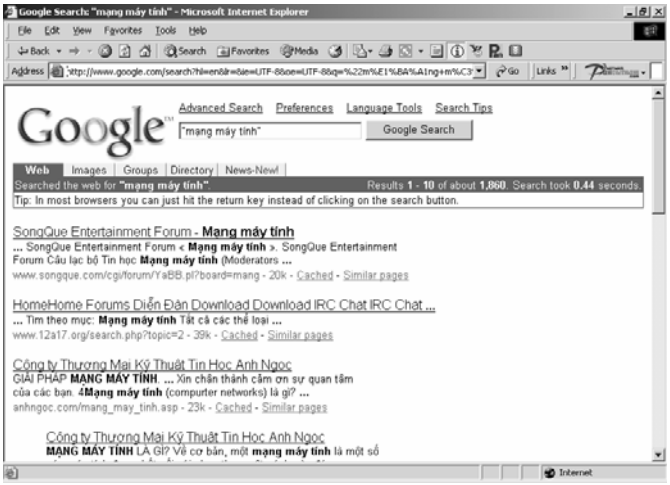


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 7.33 – Kết quả search từ khóa “mạng máy tính” trên **PanVietnam**.

*Công cụ tìm kiếm* ***Google***, **Google** là một công cụ tìm kiếm thông tin toàn cầu trên **Internet** mạnh nhất hiện nay. Tiện ích này giúp ta có thể tìm kiếm thông tin với rất nhiều ngôn ngữ khác nhau. Trong hình sau ta cũng tìm kiếm các trang Web chứa thông tin mạng máy tính.




Hình 7.34 – Kết quả **search** từ khóa “mạng máy tính” trên **Google**.

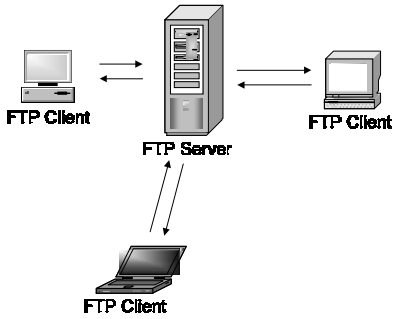


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

# VI. DỊCH VỤ FTP.

## VI.1. Mô hình hoạt động của FTP.

**FTP** (**File Transfer Protocol**) là một dịch vụ cho phép ta truyền tải file giữa hai máy tính ở xa dùng giao thức **TCP/IP**. **FTP** cũng là một ứng dụng theo mô hình **client-server**, nghĩa là máy làm **FTP Server** sẽ quản lý các kết nối và cung cấp dịch vụ tập tin cho các máy trạm. Nói tóm lại **FTP Server** thường là một máy tính phục vụ cho việc quảng bá các tập tin cho người dùng hoặc là một nơi cho phép người dùng chia sẻ tập tin với những người dùng khác trên **Internet**. Máy trạm muốn kết nối vào **FTP Server** thì phải được **Server** cấp cho một **account** có đầy đủ các thông tin như: địa chỉ máy **Server** (tên hoặc địa chỉ **IP**), **username** và **password**. Phần lớn các **FTP Server** cho phép các máy trạm kết nối vào mình thông qua **account anonymous** (**account anonymous** thường được truy cập với **password** rỗng). Các máy trạm có thể sử dụng các lệnh **ftp** đã tích hợp sẵn trong hệ điều hành hoặc phần mềm chuyên dụng khác để tương tác với máy **FTP Server**.




Hình 7.35 – Mô hình hoạt động của **FTP Server**.

## VI.2. Tập hợp các lệnh FTP.

| Lệnh | Chức năng |
|---|---|
| ! | Chạy chương trình **command dos** trên máy tính cục bộ. |
| ? | Hiển thị giúp đỡ của các lệnh **Ftp**, lệnh này giống với lệnh **Help**. |
| Append | Chèn nội dung của một tập tin trên máy tính cục bộ vào cuối của một tập tin trên máy tính ở xa (máy **FTP Server**), dùng định dạng tập tin hiện tại. |
| Ascii | Đặt loại định dạng truyền file là **ASCII**, giá trị này là mặc định khi khởi tạo kết nối **FTP**. |



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

| | |
|---|---|
| Bell | Bật trạng thái chuông là **on/off**. Nếu là **on** thì sau mỗi lần lệnh truyền file hoàn thành thì máy phát ra tiếng chuông. Mặc định trạng thái này là **off**. |
| Binary | Đặt loại định dạng truyền file là **binary**. |
| Bye | Tắt kết nối với máy tính ở xa và thoát khỏi chương trình **FTP**. |
| Cd | Thay đổi thư mục hiện thành trên máy ở xa(**Server**). |
| Close | Ngừng phiên giao dịch với máy tính ở xa và trở về dòng lệnh của chương trình **ftp**. |
| Debug | Bật trạng thái **Debugg on/off**. Nếu là **on** thì mỗi lệnh gởi đến máy tính ở xa thì chương trình sẽ in ra các thông báo. Mặc định là trạng thái là **off**. |
| Delete | Xoá tập tin trên máy tính ở xa. |
| Dir | Hiển thị danh sách các tập tin và thư mục con trong thư mục hiện tại. |
| Disconnect | Tắt kết nối với máy tính ở xa và trở về dòng lệnh **FTP**. |
| Get | Chép một tập tin từ máy tính ở xa về máy tính cục bộ, dùng định dạng truyền file hiện tại. |
| Help | Hiển thị giúp đỡ của các lệnh **Ftp**. |
| Lcd | Thay đổi thư mục hiện trên máy tính cục bộ. Mặc định là thư mục đang làm việc trên máy tính cục bộ. |
| Ls | Hiển thị danh sách các tập tin và thư mục con trong thư mục hiện tại. |
| Mdelete | Xóa nhiều tập tin cùng trên một máy tính ở xa. |



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

| | |
|---|---|
| Mget | Chép nhiều tập tin từ máy tính ở xa về máy tính cục bộ dùng định dạng truyền file hiện tại. |
| mkdir | Tạo thư mục trên máy tính ở xa. |
| Mput | Chép nhiều tập tin ở máy tính cục bộ lên máy tính ở xa dùng định dạng truyền file hiện tại. |
| open | Mở một kết nối đến máy **FTP Server**. |
| Put | Chép một tập tin ở máy tính cục bộ lên máy tính ở xa dùng định dạng truyền file hiện tại. |
| Pwd | Hiển thị thư mục hiện hành trên máy tính ở xa. |
| Quit | Tắt kết nối với máy tính ở xa và thoát khỏi chương trình **FTP**. |
| Recv | Chép một tập tin từ máy tính ở xa về máy tính cục bộ, dùng định dạng truyền file hiện tại. Tương tự như lệnh Get. |
| Rename | Đổi tên tập tin, thư mục trên máy tính ở xa. |
| Rmdir | Xóa một thư mục ở xa. |
| Send | Chép một tập tin ở máy tính cục bộ lên máy tính ở xa dùng định dạng truyền file hiện tại. Tương tự như Put. |
| Status | Hiển thị các trạng thái lựa chọn của kết nối FTP. |
| type | Đặt hoặc hiển thị định dạng truyền file. |
| user | Định người dùng khi kết nối đến máy tính ở xa. |



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

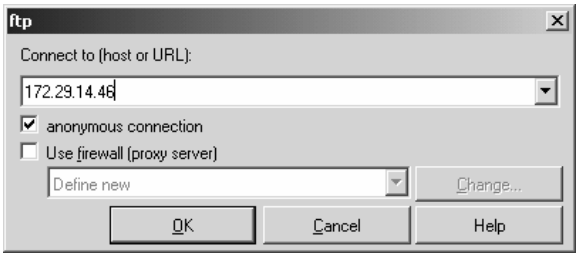
## VI.3. Dùng FTP trong Windows Commander.

**Giới thiệu.**

**Windows Commander** là chương trình quản lý tập tin và thư mục được sử dụng rộng rãi nhất hiện nay. Đồng thời **Windows Commander** cũng đã tích hợp chương trình **FTP Client**. Với chương trình trạm này, bạn có thể truy cập đến 10 **FTP Server** cùng lúc trên **Internet** hoặc trên **Intranet**. Chương trình **FTP client** này không chỉ cho phép **upload** và **download file** mà còn hỗ trợ truyền files trực tiếp từ máy tính ở xa đến một máy tính khác. Bạn có thể thao tác trên **FTP Client** giống như các tính năng của **Windows Commander**. Ví dụ như: sao chép (F5), đổi tên (SHIFT+F6), xóa (F8), tạo thư mục (F7).

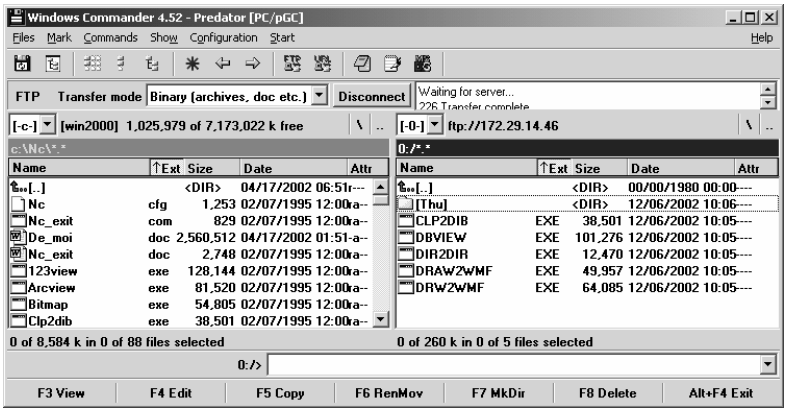
**Tạo kết nối mới:**

Bạn vào menu **Commands** chọn **FTP New Connection**. Hộp thoại **FTP** xuất hiện, trong mục **Connection to** bạn nhập vào địa chỉ của máy **FTP Server** mà bạn cần kết nối, chọn **OK**.




Hình 7.36 – Hộp thoại sau khi chọn **FTP New Connection**.

Sau đó chương trình yêu cầu bạn nhập **User** và **Password** vào. Nếu đúng chương trình sẽ kết nối vào **Server** và lúc đó trên màn hình có hai cửa sổ. Cửa sổ bên trái hiển thị các tập tin trên máy cục bộ, cửa sổ bên phải hiển thị các tập tin trên máy tính ở xa (máy **Server**).




Hình 7.37 – Giao diện chương trình **Windows Commander**.

Sau khi đã kết nối bạn có thể thực hiện các thao tác tập tin giữa máy tính cục bộ và máy tính ở xa thông qua hai cửa sổ trên. Khi muốn hủy kết nối bạn click chuột vào nút **Disconnect**, chương trình sẽ trở về trạng thái bình thường.



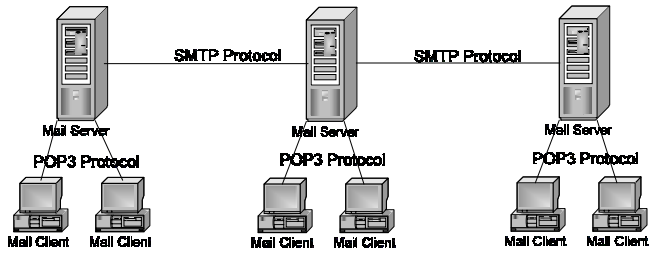
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

# VII. E-MAIL.

## VII.1. Mô hình hoạt động.

**E-mail** (**electronic mail**) là thư điện tử, là một hình thức trao đổi thư từ nhưng thông qua mạng **Internet**. Dịch vụ này được sử dụng rất phổ biến và không đòi hỏi hai máy tính gởi và nhận thư phải kết nối **online** trên mạng..

Tại mỗi **Mail Server** thông thường gồm hai dịch vụ: **POP3** (**Post Office Protocol 3**) làm nhiệm vụ giao tiếp mail giữa **Mail Client** và **Mail Server**, **SMTP** (**Simple E-mail Transfer Protocol**) làm nhiệm vụ giao tiếp **mail** giữa các máy **Mail Server**.




Hình 7.38 – Mô hình hoạt động của **Mail Server**.

Để sử dụng **E-mail**, người dùng cần có một **account mail** do nhà cung cấp dịch vụ **Internet** (**ISP**) cấp bao gồm các thông tin sau: địa chỉ **mail** (ví dụ: **nvteo@hcm.vnn.vn**), **username**, **password** và địa chỉ của **Mail Server** mà mình đăng ký. Sau đó chọn một chương trình **Mail Client** (**Outlook Express**, **Eudora**, **Netscape**...) và cấu hình các thông số trên vào chương trình đó. Từ đó bạn có thể sử dụng chương trình này để soạn thảo và gởi nhận mail một cách dễ dàng.

## VII.2. Các loại mail.

Thông thường có hai loại mail thông dụng là WebMail và **POP Mail**. **Webmail** là loại mail mà hình thức giao dịch mail giữa **Client** và **Server** dựa trên giao thức **Web** (**http**), thông thường **Webmail** là miễn phí. Còn **POP Mail** là loại mail mà các **Mail Client** tương tác với **MAIL SERVER** bằng giao thức **POP3**. Mail loại này tiện lợi và an toàn hơn nên thông thường là phải đăng ký thuê bao với nhà cung cấp dịch vụ.

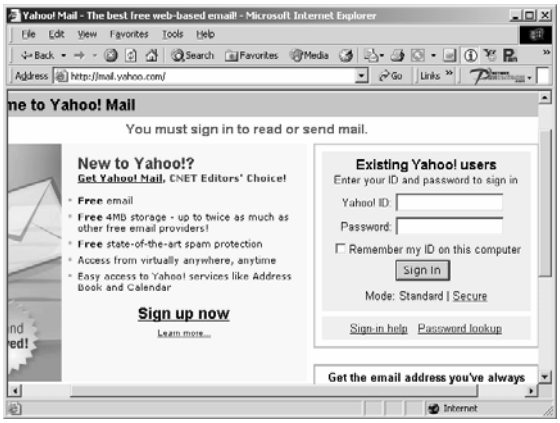
## VII.3. Sử dụng WebMail.

Bạn muốn có một địa chỉ mail **Internet** để giao dịch với bạn bè trên thế giới, bạn có thể đến nhà cung cấp dịch vụ **Internet** để đăng ký hoặc tự tạo cho mình một địa chỉ mail miễn phí trên các **Website** nổi tiếng như **Yahoo**, **Hotmail**, **Fpt**, **Vnn**... Trong ví dụ này sẽ hướng dẫn bạn tạo một địa chỉ mail miễn phí trên **Yahoo**.

Đầu tiên bạn vào **Website** của **Yahoo** và bạn click vào **Sign up now**.

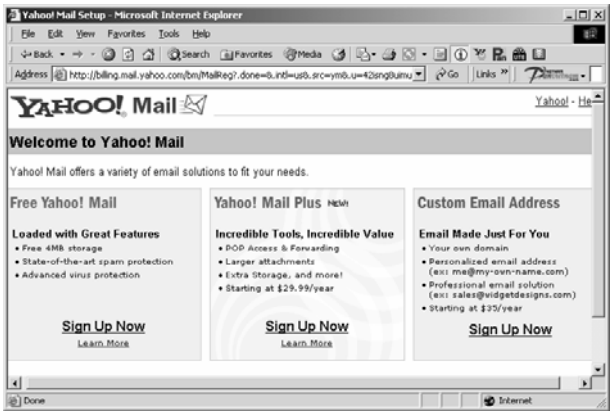


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 7.39 – Trang Web Mail của **Yahoo**.

**Yahoo** sẽ hiện ra ba dịch vụ mail cung cấp cho khách hàng và bạn chọn dịch vụ đầu tiên vì đây là dịch vụ miễn phí. Hai dịch vụ sau đều phải thuê bao. Bạn click vào **Sign up now** trong phần **Free Yahoo Mail**.




Hình 7.40 – Giao diện sau khi chọn **Sign up now**.

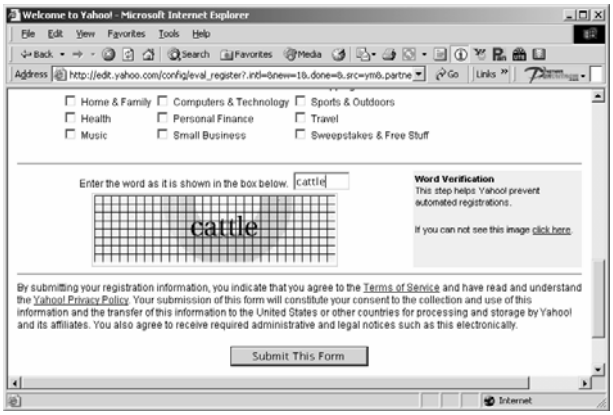
**Yahoo** sẽ hiện bảng thông tin cá nhân và bạn nhập vào các thông tin này như: địa chỉ mail mà bạn đề xuất, password, ngày tháng năm sinh, tên, mã vùng.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net


Hình 7.41 – Giao diện để tạo một địa chỉ mail **Yahoo** mới.

Để tránh các **hacker** tạo tự động địa chỉ mail, **Yahoo** xây dựng tính năng **Word Verification**. Do đó bạn phải quan sát chữ trên hình và nhập chữ đó vào **textbox** của mục **Word Verification**. Sau đó click vào **Submit This Form** để cập nhật các thông tin vừa nhập lên **Yahoo Server**.

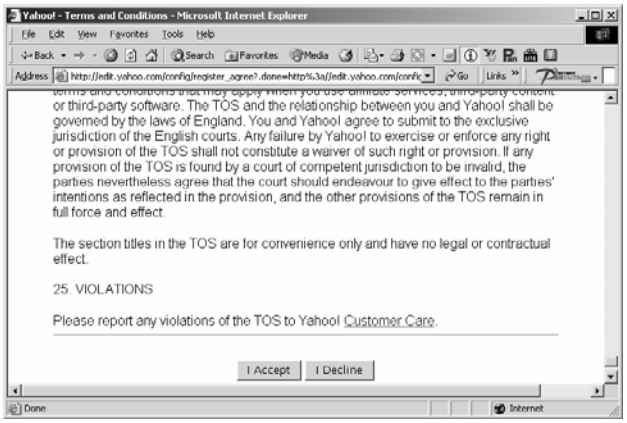



Hình 7.42 – Giao diện để tạo một địa chỉ mail **Yahoo** mới (tt).

Nếu thông tin nào không phù hợp thì **Yahoo** sẽ tô màu đỏ, lúc đó bạn xem hướng dẫn của **Yahoo** và điều chỉnh cho phù hợp. Sau khi đăng ký thành công **Yahoo** sẽ thông báo với bạn các thông tin về **Yahoo**, bạn click vào **I Accept** để hoàn thành quá trình đăng ký.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 7.43 – Giao diện gởi các thông tin tạo một địa chỉ mail mới.

Nếu quá trình đăng ký thành công thì **Yahoo** sẽ thông báo như màn hình sau. Từ đây bạn có thể sử dụng địa chỉ mail **hocvienmang02@yahoo.com** để giao dịch với mọi người trên thế giới.


Hình 7.44 – Giao diện sau khi tạo thành công một địa chỉ mail **Yahoo** mới.

Bạn đã có một **account mail** trên **Yahoo**, mỗi lần bạn muốn gởi nhận mail thì bạn vào trang Web **http://mail.yahoo.com**, sau đó bạn nhập **ID mail** và **password** vào chọn **Sign in**


Hình 7.45 – Giao diện để bắt đầu đăng nhập vào **Mail Yahoo**.

**Yahoo** cung cấp cho bạn một giao diện tương tác mail rất tiện lợi. Muốn xem các mail mới nhận được bạn click vào **Inbox**, lúc đó cửa sổ bên phải sẽ hiện toàn bộ các mail mà bạn nhận được. Bạn click vào chủ đề của mail để đọc nội dung chi tiết của mail. Bạn click vào các mục còn lại như: **Draft** chứa các mail soạn chưa hoàn thành, **Sent** chứa các mail đã gởi đi, **Trash** chứa các mail đã xóa giúp bạn có thể

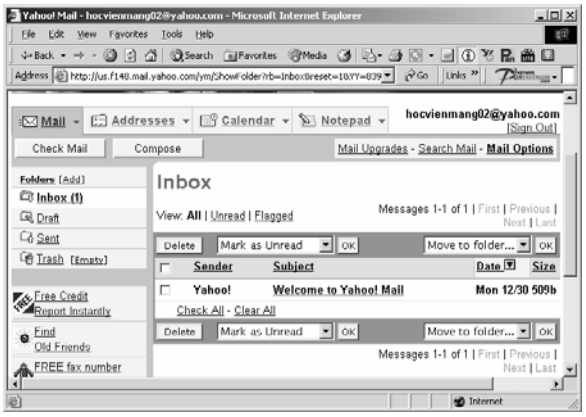


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

phục hồi các mail bị xóa nhầm.

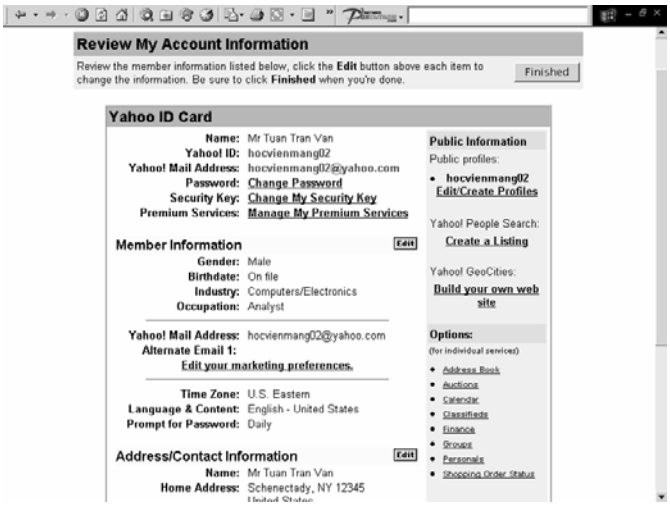


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 7.46 – Giao diện sau khi đăng nhập vào **Mail Yahoo**.

Muốn thay đổi các thông tin cá nhân hoặc thay đổi **password** bạn click vào **Mail Option**, sau đó bạn thay đổi những thông tin cần thiết.

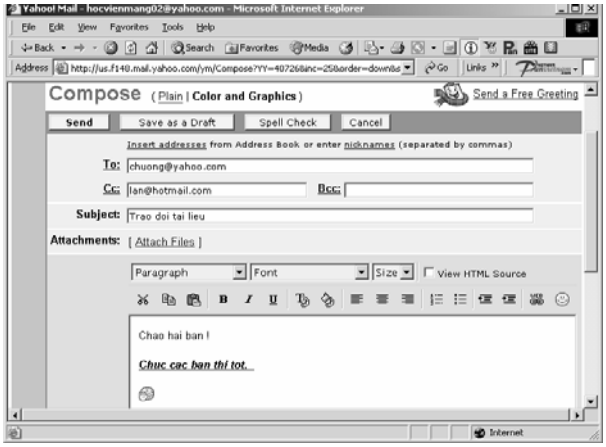



Hình 7.47 – Giao diện sau khi chọn lựa **Mail Option**.

Bạn muốn gởi mail thì click vào **Compose**, màn hình soạn thảo mail xuất hiện. Trong mục **To** bạn nhập địa chỉ mail mà bạn cần gởi đến. Mục **Cc** và **Bcc** bạn nhập vào địa chỉ mail của những người cùng nhận mail này. Mục **Subject** bạn nhập chủ đề của mail, **Attachments** cho phép bạn gởi mail có file đính kèm. Các nút khác trên thanh công cụ giúp bạn soạn thảo mail, các tính năng này giống như các tính năng của các nút trên thanh công cụ của **Word**. Sau khi soạn thảo xong bạn click vào **Send** để gởi mail đi.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 7.48 – Giao diện sau khi chọn lựa **Compose** (để tạo một mail mới).

## VII.4. Sử dụng Outlook Express.

**Giới thiệu:**

Với một kết nối **Internet** và chương trình **Outlook Express**, bạn có thể trao đổi thư điện tử (**E-mail**) với tất cả mọi người trên **Internet** và gia nhập vào bất kỳ một nhóm tin (**newsgroup**) nào.

Chương trình **Internet Connection Wizard** giúp bạn kết nối với một hoặc nhiều **Mail** hoặc **News Server**. Khi bạn cấu hình thì bạn cần những thông tin từ nhà cung cấp dịch vụ **Internet** (**ISP**) hoặc người quản trị mạng nội bộ (**LAN administrator**) như:

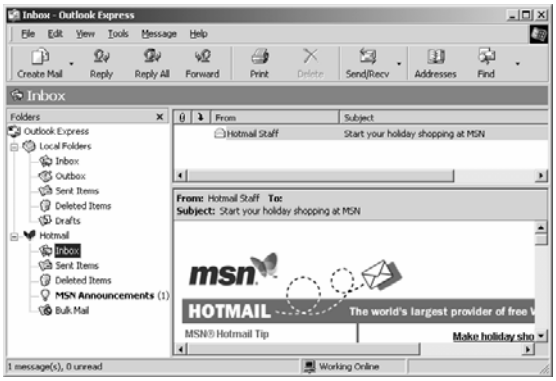
- Cấu hình tài khoản mail, bạn cần tên tài khoản của bạn (**account name**) và mật khẩu (**password**). Đồng thời bạn phải có tên (**mail.hcm.vnn.vn**) hoặc địa chỉ (**203.168.10.200**) của **Incoming** và **Outcoming Mail Server**.
- Đọc tin, bạn cần tên của **News Server** mà bạn muốn kết nối. Nếu có yêu cầu bạn phải có tên tài khoản và mật khẩu.

Một chương trình **Mail Client** cơ bản thông thường có các folder sau:

- **Inbox**: chứa các thư đã nhận
- **Outbox**: chứa các thư chuẩn bị gởi đi
- **Send** Items: chứa các thư đã gởi đi
- **Deleted Items**: chứa các thư đã xóa, giúp ta có thể phục hồi khi xoá nhập một thư nào đó.
- **Drafts**: chứa các mail đang soạn dở dang.



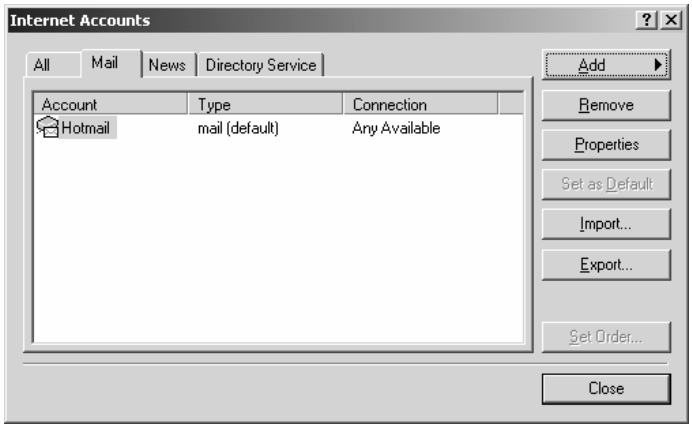
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 7.49 – Giao diện của **Outlook Express**.

**Các cấu hình cơ bản.**

Thêm tài khoản mail: muốn cấu hình mail bạn phải biết loại **Mail Server** bạn dùng (**POP3**, **IMAP**, **HTTP**), tài khoản, mật khẩu, tên của **incoming mail server** loại P**O**P3 và **IMAP**, tên của **outcoming mail server**. Sau khi có đủ các thông tin bạn vào menu **Tools**, click vào **Account**, hội thoại **Internet Account** xuất hiện, click vào nút **Add**, chọn **mail**.

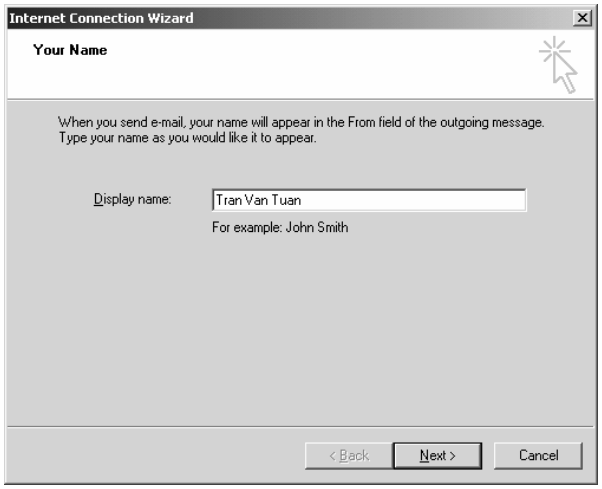



Hình 7.50 – Hộp thoại **Internet Accounts**.

Sau khi hộp thoại **Internet Connection Wizard** xuất hiện, trong mục **Display name** bạn nhập tên của bạn vào, chọn **Next.**

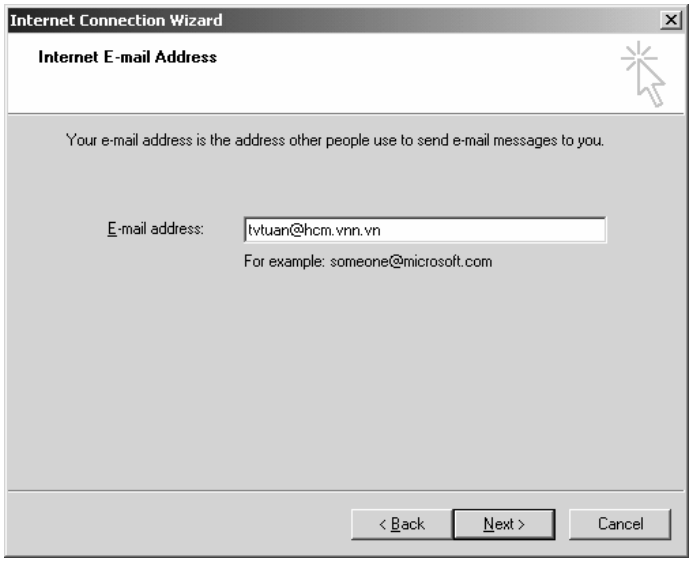


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 7.51 – Giao diện hộp thoại **Internet Connection Wizard**.

Trong hộp thoại **Internet E-Mail Address**, trong mục **E-mail address** bạn nhập vào địa chỉ mail của bạn vào.

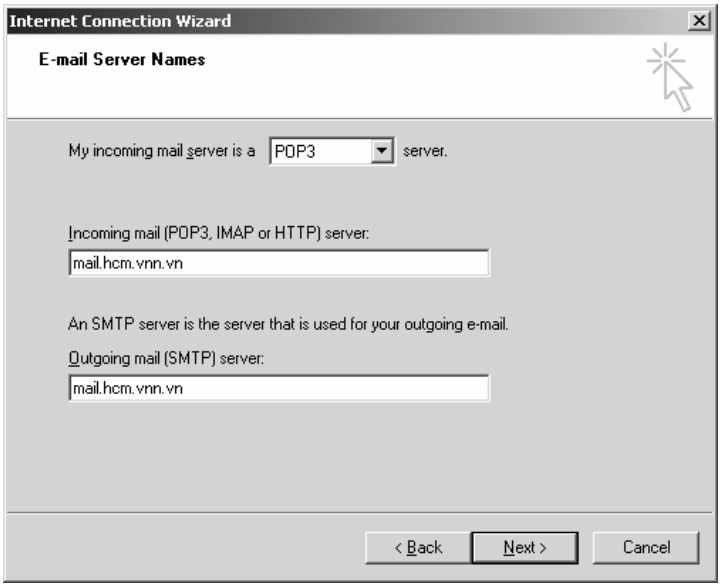



Hình 7.52 – Hộp thoại **Internet Connection Wizard** (tt).

Trong hộp thoại **E-mail Server Name** bạn nhập vào tên hoặc địa chỉ của **Server Incoming** và **Outcoming**. Đồng thời bạn chú ý là hiện tại mình đang dùng **protocol pop3** để tương tác với **Server Mail** (bạn có thể sử dụng các protocol khác như **imap**, **http** nhưng với điều kiện là **Server Mail** phải hỗ trợ), sau đó chọn **Next**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 7.53 – Hộp thoại **Internet Connection Wizard** (tt).

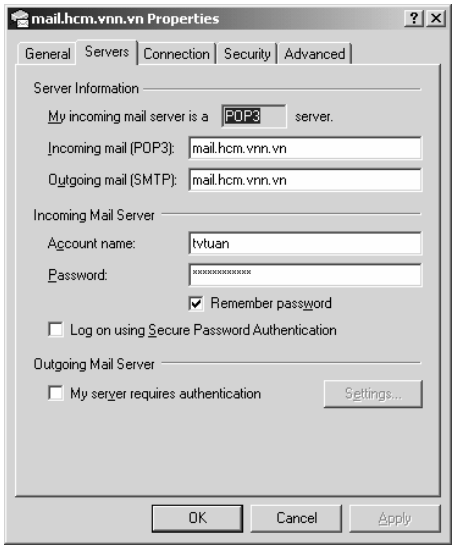
Trong hộp thoại **Internet Mail Logon**, trong mục **account name** bạn nhập vào tài khoản của bạn, mục **password** bạn nhập vào mật khẩu của bạn. Nếu bạn đánh dấu vào **Remember password** thì **password** sẽ được nhớ, lần sau bạn check mail thì **outlook** không yêu cầu bạn nhập **password** nữa.


Hình 7.54 – Hộp thoại **Internet Connection Wizard** (tt).

Chọn **Finish** để hoàn thành. Bạn muốn kiểm tra lại các thông tin mình vừa cấu hình bạn chọn **Account** trong **Tab Mail** và click vào nút **Properties.**



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 7.55 – Hộp thoại **Mail Properties**.

Nhận và đọc thư: sau khi click vào nút **Send/Recv** trên thanh công cụ, **Outlook** sẽ gởi các mail trong **Outbox** ra ngoài và nhận các mail mới đưa vào **Inbox**. Muốn đọc nội dung các mail mới này, ta click chuột vào **Inbox**, lúc đó bên phải sẽ xuất hiện thông tin chi tiết của các mail này và bên dưới là nội dung của mail. Bạn xem hình phía trên.

Xem tập tin gởi kèm: trong màn hình **Preview**, click chuột vào biểu tượng chiếc kẹp giấy, sau đó chọn tập tin gởi kèm rồi chọn **Open** để mở tập tin hoặc chọn **Save to disk** để lưu tập tin vào đĩa.

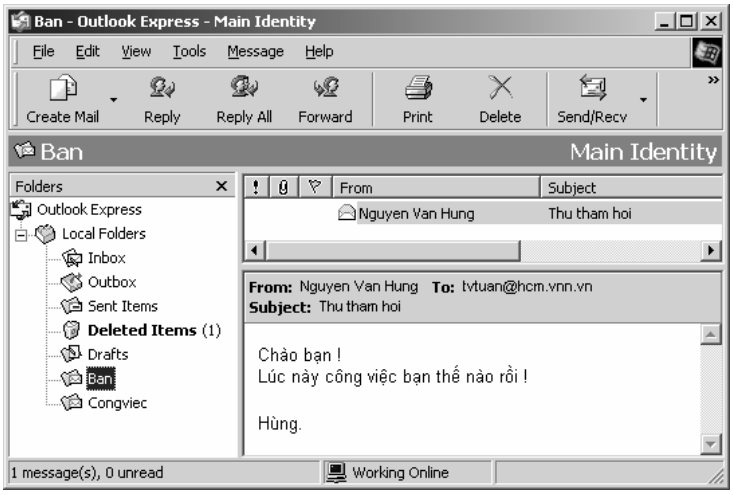
Trả lời thư: chọn thư cần trả lời và click vào nút **Reply** trên thanh công cụ, sau đó nhập nội dung trả lời và click vào **Send** để gởi đi.

Chuyển tiếp thư: đôi lúc ta muốn chuyển toàn bộ nội dung một mail mà ta nhận được đến một người khác thì ta click phải chuột trên mail đó và chọn chức năng **Forward**, sau đó nhập địa chỉ cần gởi đến. Nếu có nhiều địa chỉ thì các địa chỉ này cách nhau bởi dấu chấm hoặc chấm phẩy.

Tổ chức và sắp xếp thư: để tiện lợi cho việc tìm kiếm và xử lý mail ta nên sắp xếp các mail theo một tổ chức thư mục nhất định. Trước tiên  ta cần tạo thêm các thư mục mở rộng bằng cách click phải chuột vào **Local Folders**, chọn **New Folders** và nhập tên thư mục cần tạo. Trong ví dụ sau ta tạo folder **Ban** để chứa các mail của bạn bè, folder **Congviec** để chứa các mail công việc. Sau đó ta vào **Inbox** chọn mail cần di chuyển rồi click phải chuột trên mail đó, chọn **Move to Folder**.

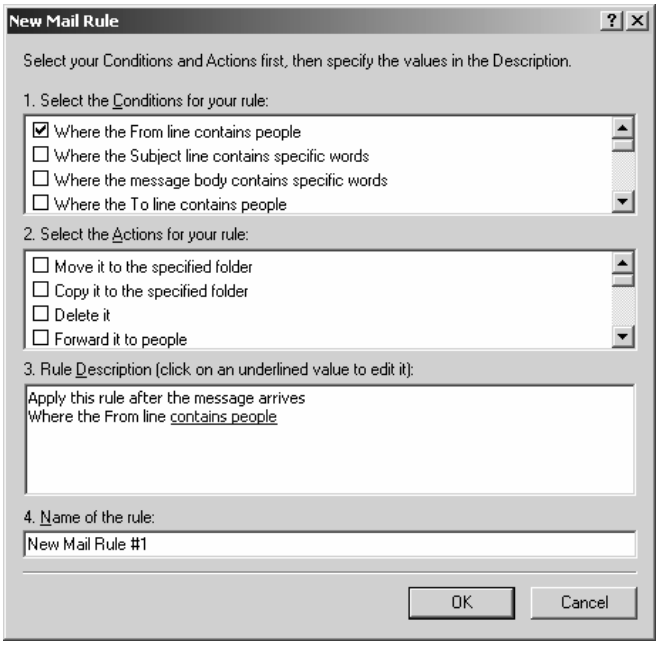


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 7.56 – Mail của "Nguyen Van Hung" đã được gởi vào thư mục "Ban".

Quản lý thư bằng các quy tắc (**Rules**): khi bạn giao dịch mail với nhiều người mà bạn sắp xếp các mail bằng tay thì mất rất nhiều thời gian. **Outlook** cung cấp cho ta công cụ **Message Rules** giúp ta có thể quản lý tự động các mail một cách dễ dàng. Một quy tắc (**Rule**) gồm hai phần: phần điều kiện (**Conditions**) chứa một hoặc nhiều điều kiện về mail, phần hành động (**Actions**) chứa một hoặc nhiều hành động ứng với các diều kiện trên. Ví dụ ta muốn khi nhận bất kỳ mail nào của anh Nguyen Van Hung thì tự động chuyển vào Folder **Ban**. Ta làm các bước như sau: vào menu **Tools**/**Message Rules/Mail**… Hộp thoại **New Mail Rules** xuất hiện, trong mục điều kiện (**Select the conditions for your rule**) bạn check vào **Where the from line contains people** thì phía dưới mục **Rules Decription** chứa hàng chữ màu xanh **contains people**.

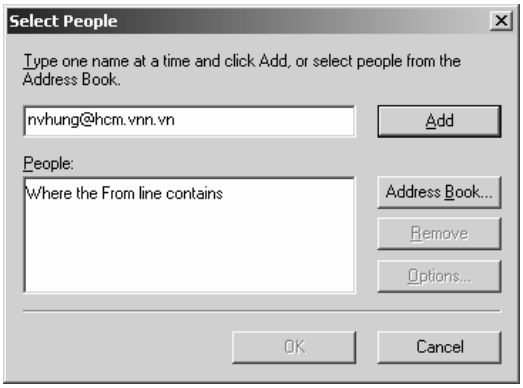





Hình 7.57 – Hộp thoại **New Mail Rule**.

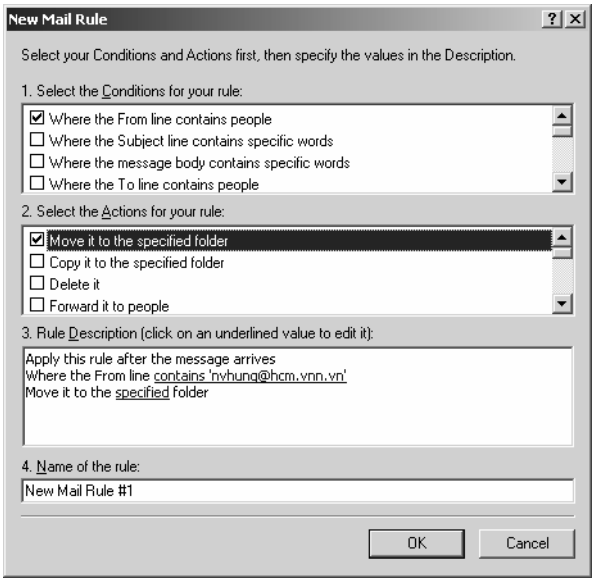
Bạn click vào hàng chữ màu xanh **contains people**, hộp thoại **Select People** xuất hiện. Bạn nhập vào địa chỉ mai của anh Nguyễn Văn Hùng: **nvhung@hcm.vnn.vn**, chọn Add, chọn OK.

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 7.58 - Hộp thoại sau khi chọn **Contains people**.

Bước kế tiếp là bạn chọn hành động cho điều kiện này, trong mục **Select the Actions for your rule** bạn check vào **Move it to the specified folder**.

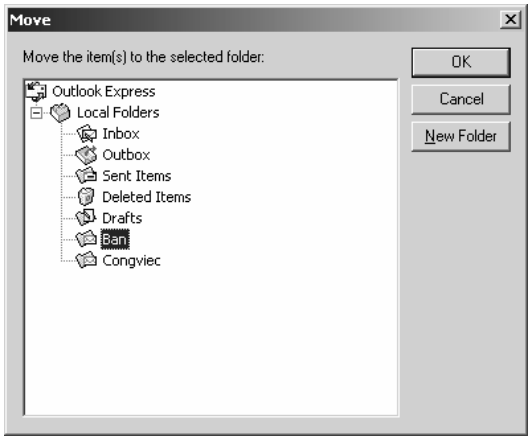



Hình 7.59 – Hộp thoại **New Mail Rule** (tt).

Trong mục **Rule Description**, click vào hàng chữ màu xanh **specified** để chỉ ra thư mục mail sẽ di chuyển đến.

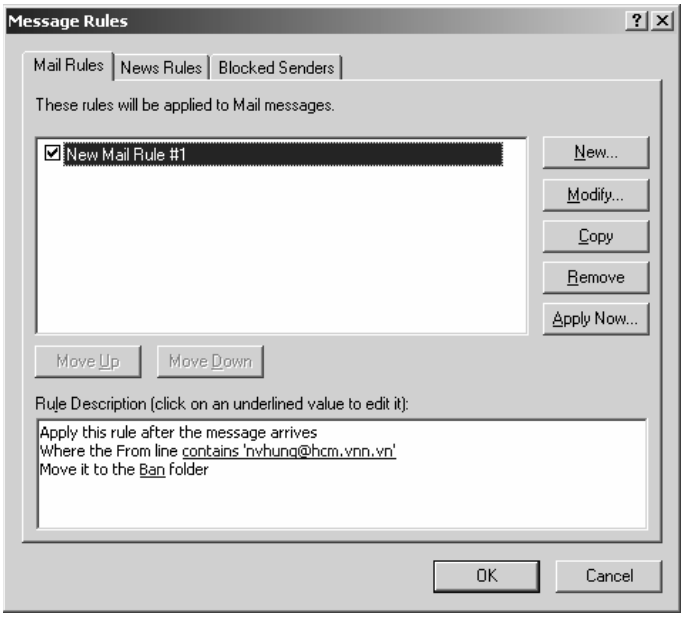


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 7.60 – Hộp thoại sau khi chọn **Specified Folder**.

Sau khi hoàn thành bạn sẽ có một quy tắc như sau:

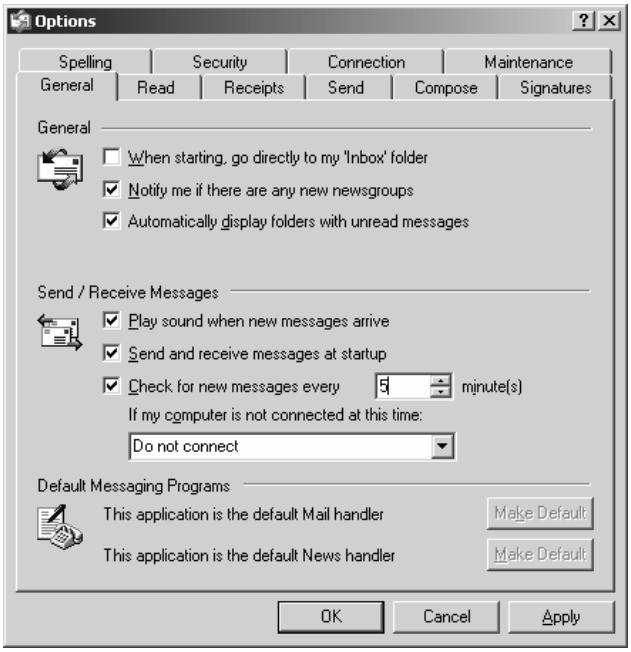



Hình 7.61 – Hộp thoại **Message Rules**.

Xác định thời gian check mail tự động: bạn vào menu **Tools/Option**, hộp thoại **Option** xuất hiện, trong **Tab General**, mục **Send/Receive Messages** bạn check vào **Check for new message every XX minute**, đồng thời bạn nhập vào thời gian check mail tự động.

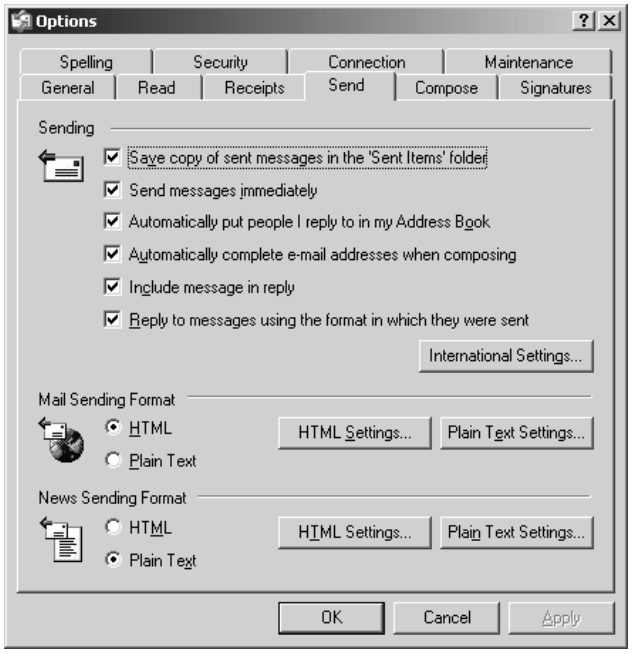


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 7.62 – Hộp thoại **Options**.

Mail có hai định dạng cơ bản là: **HTML** và **Plain Text**. Dạng **HTML** cho phép ta soạn thảo mail như một trang Web có thể chèn hình ảnh, âm thanh vào mail, làm cho mail có thể sống động hơn. Dạng **Plain Text** chỉ cho phép ta soạn thảo mail như một tài liệu văn bản trong suốt. Muốn chọn định dạng mail bạn vào **Tab Send** trong hộp thoại **Option**, mục **Mail Sending Format** bạn chọn định dạng mà bạn muốn.






Hình 7.63 – Hộp thoại **Options** – **Tab Send**.

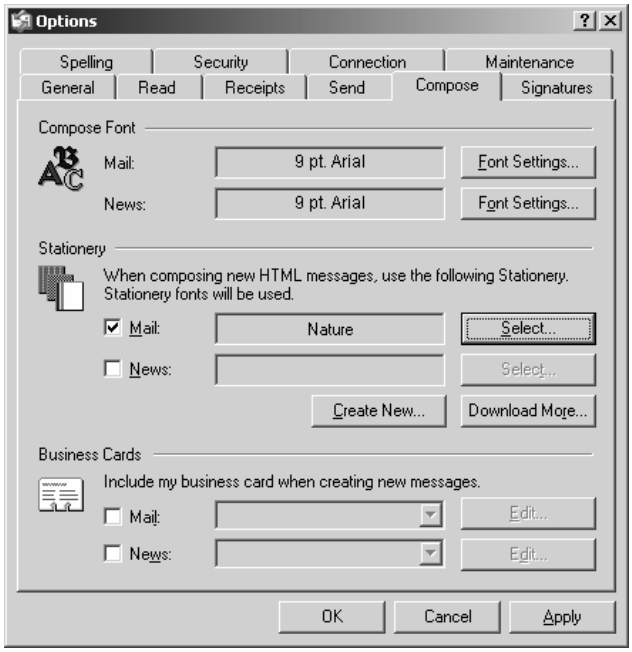
Sử dụng **Stationary**: **Stationary** là một khuôn mẫu mail được thiết kế sẵn giúp bạn có thể soạn thảo

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

mail nhanh và trình bày đẹp. Bạn vào **tab Compose** trong hộp thoại **Option**, mục **Stationery**, check vào mail và bạn click vào **Select** để chọn khuôn mẫu vừa ý.

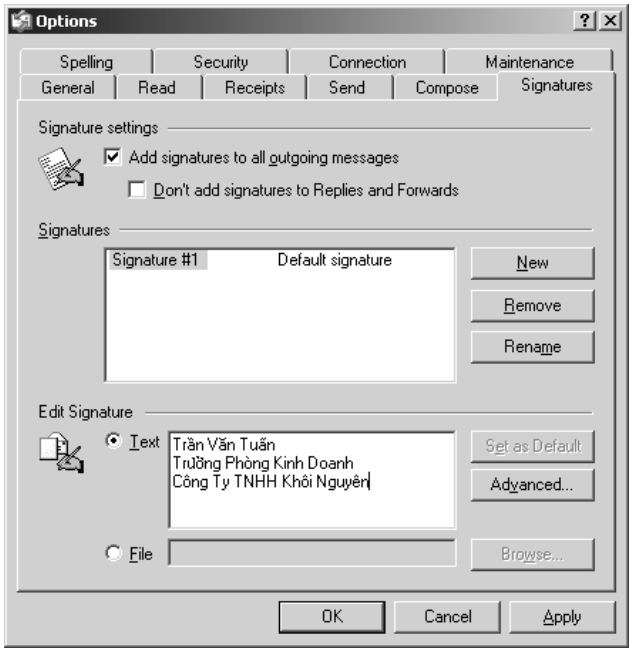


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 7.64 – Hộp thoại **Options** – **Tab Compose**.

Chèn đối tượng **Signatures**: **Signature** là những thông tin cá nhân được gởi tự động kèm theo thư. Thông thường các thông tin này là tên công ty, số điện thoại, fax… Bạn muốn chèn các thông tin này bạn vào **Tab Signatures** trong hộp thoại **Option**. Click và **New** để tạo **Signature** mới, trong mục **Text** nhập vào các thông tin cần thiết.

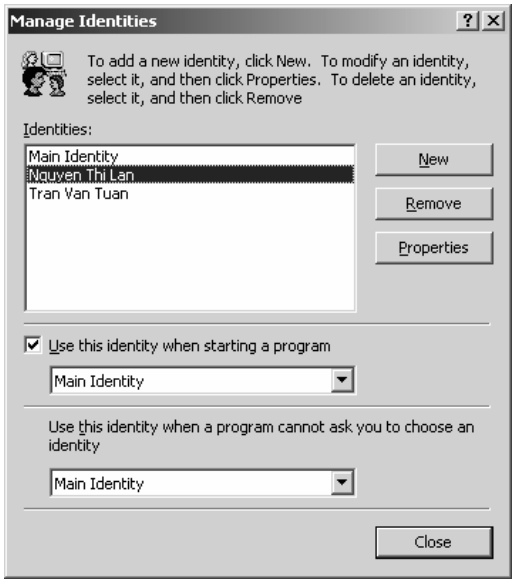



Hình 7.65 – Hộp thoại **Options** – **Tab Signatures**.



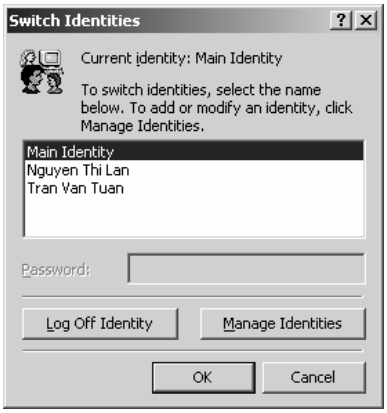
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Quản lý nhiều người dùng trong **Outlook**: đôi lúc nhiều người dùng chung một chương trình **Outlook** để gởi nhận mail và họ muốn mail của họ được bảo mật có nghĩa là mail của riêng người nào thì người đó mới được đọc. Lúc đó ta sử dụng tính năng Identity của **Outlook**, trước hết ta tạo ra **Identity** cho từng người bằng cách vào menu **File/Identities/Manager Identities**, sau đó click vào New và nhập tên của các thành viên. Nếu muốn bảo mật tuyệt đối thì check vào mục sử dụng **password**.




Hình 7.66 – Hộp thoại **Manage Identities**.

Ta chuyển vào **Identity** bằng cách vào menu **File/Switch Indentity** và chọn người cần chuyển vào, sau đó bạn cấu hình từ đầu cho riêng bạn xem như là bạn sở hữu riêng một chương trình **Outlook Express**. Chú ý là sau khi sử dụng xong bạn phải chọn chức năng **Log off** để thoát khỏi **Identity** của mình tránh tình trạng người khác đọc được mail của mình.




Hình 7.67 – Hộp thoại **Switch Identities**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

# VIII. XÂY DỰNG TRANG WEB.

## VIII.1. Giới thiệu ngôn ngữ HTML.

Ngôn ngữ **HTML** (**HyperText Markup Language**) là một ngôn ngữ mô tả, bao gồm tập hợp các thẻ (tag) dùng để mô tả các trang Web. Mỗi thẻ thông thường là một cặp chỉ vị trí bắt đầu thẻ và vị trí kết thúc thẻ.

## VIII.2. Các thẻ (Tag) trong HTML.

- <HTML></HTML> :thẻ nhận dạng tài liệu, đặt ở vị trí bắt đầu và kết thúc tập tin.
- <TITLE></TITLE>: chỉ ra nội dung tiêu đề của trang Web, nội dung này sẽ được hiển thị trên thanh tiêu đề của chương trình **Browser**. Thẻ này chỉ đặt trong phần **Header**.
- <HEAD></HEAD>: chỉ ra phần header của trang Web, thẻ này có thể bỏ qua.
- <BODY></BODY>: thẻ này chỉ ra phần nội dung của trang Web.
- <H?></H?>: định dạng văn bản theo **heading**, giá trị này từ 1 đến 6, giá trị càng nhỏ chữ càng lớn.
- <H? ALIGN=LEFT | CENTER | RIGHT></H?> : định dạng canh lề cho văn bản.
- <EM></EM>: hiển thị văn bản ở dạng nghiêng theo **logical type**.
- <STRONG></STRONG>: hiển thị văn bản ở dạng in đậm theo **logical type.**
- <BIG></BIG> : chọn kích thước **font** lớn.
- <SMALL></SMALL>: chọn kích thước **font** nhỏ.
- <B></B> :hiển thị văn bản ở dạng in đậm theo **physical type**.
- <I></I>: hiển thị văn bản ở dạng nghiêng theo **physical type**.
- <U></U>: hiển thị văn bản ở dạng gạch dưới theo **physical type**.
- <STRIKE></STRIKE>: hiển thị văn bản ở dạng **strikeout** theo **logical type**.
- <S></S>: hiển thị văn bản ở dạng **strikeout** theo **physical type**.
- <SUB></SUB>:hiển thị văn bản ở dạng **Subscript** theo **logical type**.
- <SUP></SUP>: hiển thị văn bản ở dạng **superscript** theo **logical type**.
- <CENTER></CENTER>: định dạng canh giữa cho văn bản và hình.
- <BLINK></BLINK>: hiển thị văn bản dạng nhấp nháy.
- <FONT SIZE=?></FONT>: chọn kích thước **font** có giá trị từ 1 đến 7.
- <BASEFONT SIZE=?> : chỉ định kích thước font dạng văn bản, có giá trị từ 1-7. Mặc định là 3.
- <FONT COLOR="#$$$$$$"></FONT> : chỉ định màu của văn bản, giá trị dưới dạng **hexa**.
- <FONT FACE="***"></FONT>: chọn **font** cho văn bản
- <MULTICOL COLS=?></MULTICOL>: tạo văn bản có nhiều cột.
- <A HREF="URL"></A> : tạo một link đến một đối tượng **URL**.
- <A HREF="URL#***"></A>: tạo một link đến một đối tượng **URL** được chỉ định.
- <A HREF="URL" TARGET="*** | _blank | _self | _parent|_top"></A>: tạo một link đến một đối tượng URL chỉ định cửa sổ hiển thị.
- <IMG SRC="URL">: hiển thị ảnh.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

- <IMG SRC="URL" ALIGN=TOP | BOTTOM | MIDDLE | LEFT | RIGHT>: canh lề trái phải của ảnh



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

- <IMG SRC="URL" ALIGN=TEXTTOP | ABSMIDDLE | BASELINE | ABSBOTTOM >: canh phía trên và phía dưới của ảnh.
- <HR> : Tạo hàng ngang
- <HR ALIGN=LEFT | RIGHT | CENTER > : canh lề
- <HR SIZE=?>: độ dày tính theo **pixel**.
- <HR WIDTH=?>: độ rộng tính theo **pixel**.
- <UL><LI></UL>: tạo danh sách không sắp xếp, đặt <LI> trước mỗi đối tượng của danh sách.
- <BODY BACKGROUND="URL">: tạo nền của trang Web.
- <BODY BGCOLOR="#$$$$$$">: đặt màu nền cho trang Web, giá trị này hệ hexa theo thứ tự red/green/blue.
- <BODY TEXT="#$$$$$$"> : màu chữ.
- <BODY LINK="#$$$$$$">: màu link.
- <BODY VLINK="#$$$$$$">: màu các trang link đã duyệt qua.
- <BODY ALINK="#$$$$$$"> : màu link đang được chọn.
- <FORM ACTION="URL" METHOD=GET | POST></FORM> : định nghĩa một **form** và phương thức hoạt động của **form**.
- <INPUT TYPE="TEXT | PASSWORD | CHECKBOX | RADIO | IMAGE | HIDDEN | SUBMIT | RESET "> : đưa các đối tượng vào **form**.
- <INPUT NAME="***"> : tên của trường trong **form**.
- <INPUT VALUE="***"> :giá trị của trường trong **form**.
- <INPUT SIZE=?> : kích thước của **field** tính bằng **characters**.
- <SELECT></SELECT>: tạo list lựa chọn.
- <SELECT NAME="***"></SELECT> : tên của **list**.
- <TEXTAREA ROWS=? COLS=?></TEXTAREA>: tạo một hộp nhập liệu.
- <TABLE></TABLE> : định nghĩa một bảng.
- <TABLE BORDER=?></TABLE>: kích thước **border**.
- <TABLE WIDTH=?>: độ rộng của bảng tính theo **pixel**.
- <TR></TR> : tạo dòng của bảng.
- <TR ALIGN=LEFT | RIGHT | CENTER | MIDDLE | BOTTOM VALIGN=TOP | BOTTOM | MIDDLE>: canh lề trong dòng của bảng.
- <TD></TD> : tạo ô trong bảng
- <TD ALIGN=LEFT | RIGHT | CENTER | MIDDLE | BOTTOM VALIGN=TOP | BOTTOM | MIDDLE> : canh lề trong ô củabảng.
- <TD BGCOLOR="#$$$$$$"> : định màu trong ô của bảng.
- <FRAMESET> </FRAMESET>: khai báo **frame**.
- <FRAMESET ROWS=,,,></FRAMESET>: độ rộng của hàng tính theo **pixel** hoặc %.
- <FRAMESET COLS=,,,></FRAMESET>: độ rộng của cột tính theo **pixel** hoặc %.
- <FRAMESET BORDER=?>: độ rộng của **border**.
- <FRAMESET BORDERCOLOR="#$$$$$$"> : màu của **border.**



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

- <FRAME SRC="URL">: hiển thị nội dung của tài liệu trong **Frame**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

- <FRAME SCROLLING="YES | NO | AUTO">: đặt thuộc tính **Scrollbar** cho **frame**.

## VIII.3. Các ví dụ về HTML.

Cấu trúc cơ bản của một trang html gồm hai phần chính: phần **header** (nằm giữa tag **<head>** và tag **</head>**) chứa thông tin chung về trang Web, phần nội dung chính của trang Web (đặt giữa hai tag **<body>** và **</body>** chứa nội dung sẽ được hiển thị trên trang web.

```
<HTML>
<HEAD>
<TITLE></TITLE>
</HEAD>
<BODY>
Noi dung trang Web
</BODY>
</HTML>
```

Đặt màu nền cho trang Web:

```
<BODY BGCOLOR="#FF0000">
Noi dung trang Web
</BODY>
```

Đặt **picture** làm nền:

```
<BODY BACKGROUND="swirlies.gif">
Noi dung trang Web
</BODY>
```

Đặt chế độ nghiêng, đậm, gạch dưới:

```
<BODY BGCOLOR="#FFFFFF">
<U>Noi dung </U> <I>trang </I> <B>Web</B>
</BODY>
```

Chọn **font** :

```
<font color="#00FF00" face=".VnArial" size="7">font chu</font>
```

Các thuộc tính của **text**:

```
<BODY BGCOLOR="#FFFFFF">
Noi dung <U><I><B><FONT COLOR="#FF0000" FACE="ARIAL"
SIZE="7">trang Web</FONT></B></I></U>
</BODY>
```

Xuống dòng:

```
<BODY BGCOLOR="#FFFFFF">
   Hey!<BR>
   What's<BR>
   going<BR>
```



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

***on<BR>***



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

*here??*

*</BODY>*

Canh **text**:

```
<BODY BGCOLOR="#FFFFFF">
<CENTER>Something really cool</CENTER>
 </BODY>
```

Chèn hình vào trang Web:

```
<BODY BGCOLOR="#FFFFFF">
<IMG SRC="copper.gif" WIDTH=82 HEIGHT=68>
</BODY>
```

Cấp thư mục: SRC="../../copper.gif"

Liên kết:

```
<BODY BGCOLOR="#FFFFFF">
Go to <A HREF="http://home.netscape.com/">Netscape!</A>
</BODY>
```

hoặc :

```
Click <A HREF="lesson04.html">here</A> to be magically
```

Gởi mail:

```
<BODY BGCOLOR="#FFFFFF">
Send me <A HREF="mailto:forrest@bubbagump.com">Mail!</A>
</BODY>
```

Liên kết bằng hình:

```
<BODY BGCOLOR="#FFFFFF">
Go to <A HREF="http://home.netscape.com/"> <IMG SRC="copper.gif"
WIDTH=82 HEIGHT=68 BORDER=0></A>
</BODY>
```

Danh sách trang trí kiểu (‘.’)

```
<BODY BGCOLOR="#FFFFFF">
What I want for Christmas
<UL>
<LI>a big red truck
<LI>a real fast speedboat
<LI>a drum set
<LI>a BB gun
<LI>a Melanie Griffith
</UL>
</BODY>
```



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Danh sách trang trí kiểu số:(1,2,3..)



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

```
<BODY BGCOLOR="#FFFFFF">
 What I want for Christmas
<OL>
<LI>a big red truck
<LI>a real fast speedboat
 <LI>a drum set
<LI>a BB gun
<LI>a Melanie Griffith
</OL>
</BODY>
```

Đường kẻ ngang:

```
<HR WIDTH=20%>
hoặc:
<HR >
<HR WIDTH=60% SIZE=1>
<HR WIDTH=60% SIZE=3 NOSHADE>
```

**Frame**

**Frame** chia theo cột:

```
<FRAMESET COLS="50%,50%">
<FRAME SRC="lisa.html">
<FRAME SRC="terri.html">
</FRAMESET>
```

**Frame** chia theo dòng:

```
<FRAMESET ROWS="10%,20%,30%,15%,25%">
<FRAME SRC="lisa.html">
<FRAME SRC="terri.html">
<FRAME SRC="kim.html">
<FRAME SRC="tina.html">
<FRAME SRC="shannon.html">
</FRAMESET>
```

**Frame** chia tự động:

```
<FRAMESET COLS="50,*">
<FRAME SRC="lisa.html">
<FRAME SRC="terri.html">
</FRAMESET>
```

**Frame** chia frame:

```
<FRAMESET COLS="50,*,2*">
<FRAMESET ROWS="50,*,*">
```



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

< *FRAME SRC="lisa.html">*



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

<FRAME SRC="lisa.html">
<FRAME SRC="lisa.html">
</FRAMESET>
<FRAME SRC="terri.html">
<FRAMESET ROWS="50%,50%">
<FRAME SRC="kim.html">
<FRAME SRC="tina.html">
</FRAMESET>
</FRAMESET>

Độ rộng của **line**, màu **line** của **frame**:

<FRAMESET COLS="154,*" BORDER=20 BORDERCOLOR="#FFOOOO">
<FRAMESET ROWS="170,*" FRAMEBORDER=NO >
<FRAME SRC="world.gif" WIDTH=146 HEIGHT=162 SCROLLING=NO
MARGINWIDTH=1 MARGINHEIGHT=1>
<FRAME SRC="lisa.html">
</FRAMESET>
<FRAME SRC="terri.html">
</FRAMESET>

**Form**

Gởi mail:

<FORM METHOD=POST ACTION="mailto:xxx@xxx.xxx"
ENCTYPE="application/x-www-form-urlencoded">
</FORM>

Các đối tượng trong **form**:

<INPUT TYPE=TEXT NAME="ADDRESS" VALUE="44 Cherry St" SIZE=30>
<INPUT TYPE=PASSWORD NAME="USER PASSWORD">

**Radio button**:

<INPUT TYPE=RADIO NAME="BEST FRIEND" VALUE="Ed" CHECKED> Ed Holleran<BR>
<INPUT TYPE=RADIO NAME="BEST FRIEND" VALUE="Rick"> Rick Weinberg<BR>
<INPUT TYPE=RADIO NAME="BEST FRIEND" VALUE="Tom"> Tom Studd<P>

**Check Box**:

<INPUT TYPE=CHECKBOX NAME="ED" VALUE="YES" CHECKED> Ed Holleran<BR>
<INPUT TYPE=CHECKBOX NAME="Rick" VALUE="YES"> Rick Weinberg<BR>

**ComboBox**:

<SELECT NAME="BEST FRIEND">
<OPTION VALUE="Ed">Ed
<OPTION VALUE="Rick">Rick
<OPTION VALUE="Tom" SELECTED>Tom



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

< ***OPTION VALUE="Guido">Guido***



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

```
</SELECT>
```

**List Box**:

```
<SELECT NAME="BEST FRIEND" SIZE=4>
<OPTION VALUE="Ed">Ed
<OPTION VALUE="Rick">Rick
<OPTION VALUE="Tom" SELECTED>Tom
<OPTION VALUE="Guido">Guido
<OPTION VALUE="Horace">Horace
<OPTION VALUE="Reggie">Reggie
<OPTION VALUE="Myron">Myron
</SELECT>
```

**Text Area**:

```
<TEXTAREA NAME="COMMENTS" ROWS=6 COLS=50>
</TEXTAREA>
```

Nút **Submit, Reset**:

```
<INPUT TYPE=SUBMIT>
<INPUT TYPE=RESET>
```

**Table**

Chia dòng, cột:

```
<table border="1" width="100%">
<tr>
<td width="50%"> </td>
<td width="50%"> </td>
</tr>
<tr>
<td width="50%"> </td>
<td width="50%"> </td>
</tr>
</table>
```

## VIII.4. Giới thiệu công cụ tạo web FrontPage.

**Giới thiệu về FrontPage.**

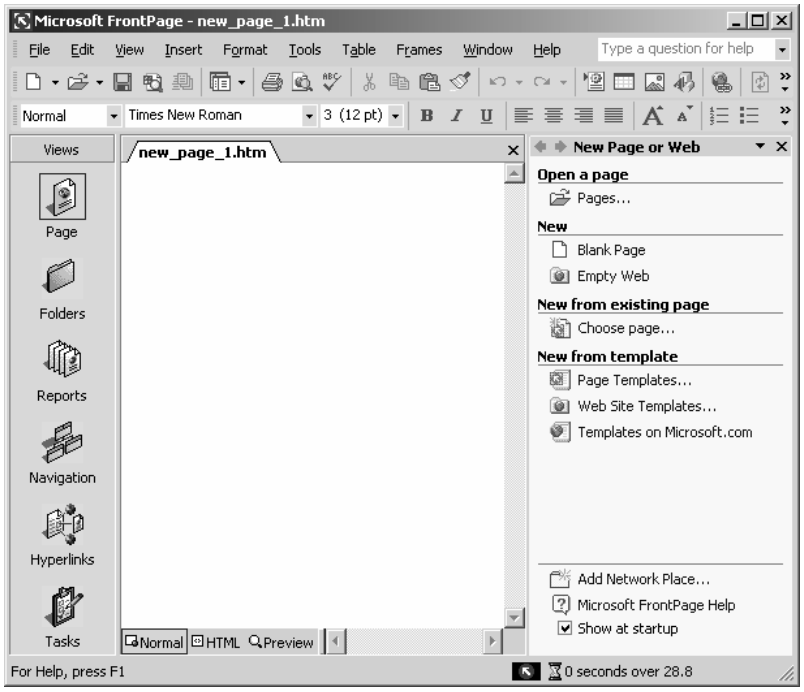
**FrontPage** là chương trình giúp ta soạn thảo nhanh các trang Web là không cần thuộc các **tag html**. Đồng thời công cụ này cũng giúp ta kiểm tra các liên kết của các trang Web và duyệt trước nội dung các trang web giống như khi duyệt bằng trình duyệt Web.

**FrontPage** là một trong các chương trình ứng dụng trong bộ **Office** của **Microsoft**, nên cách sử dụng của chương trình này cũng tương tự như **Word** hay **Excel**, do đó người dùng rất dễ làm quen.

Khởi động chương trình **FrontPage**: chọn **Start/Programs/Microsoft FrontPage**



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 7.68 – Giao diện chương trình **FrontPage**.

Tạo một trang Web mới: trong **FrontPage** vào menu **File/New/Page** or **Web** hoặc click chuột vào icon "**New**" trên thanh công cụ. Sau đó vào menu **File** chọn **Save** và nhập tên trang Web cần lưu trữ. Thông thường phần mở rộng của tập tin Web là **htm** hoặc **html**. Trong cửa sổ làm việc của **ProntPage** có ba chế độ hiển thị là "**Normal**", "**HTML**", "**Preview**".

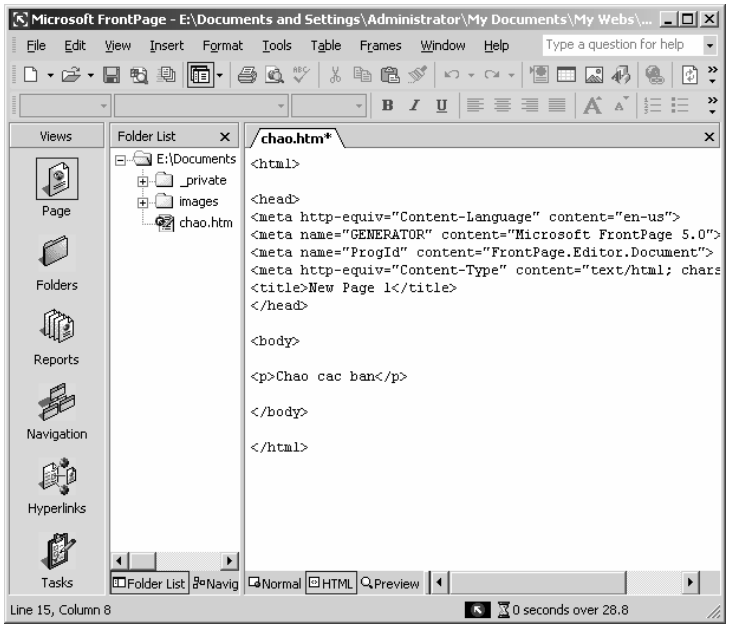

**Normal** là chế độ soạn thảo Web.

**HTML** là chế độ hiển thị nội dung **source html** của trang Web.

**Preview** là chế độ duyệt Web giống như trình duyệt web dùng để kiểm tra trước khi đưa trang Web lên mạng.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 7.69 – Giao diện khi chọn chế độ xem là HTML.

Thanh công cụ định dạng văn bản với các tính năng thông dụng sau:


Hình 7.70 – Thanh công cụ định dạng văn bản.

- Chọn kiểu văn bản
- Chọn loại font thích hợp
- Chọn kích thước chữ
- Định dạng in đậm, in nghiêng, gạch dưới
- Canh lề trái, phải, giữa, đều hai bên lề
- Tăng giảm kích thước chữ
- Định dạng danh sách sắp xếp dạng number, bullet
- Định dạng Tab sang trái hay sang phải
- Chọn đường viền khung
- Chọn màu văn bản, màu nền

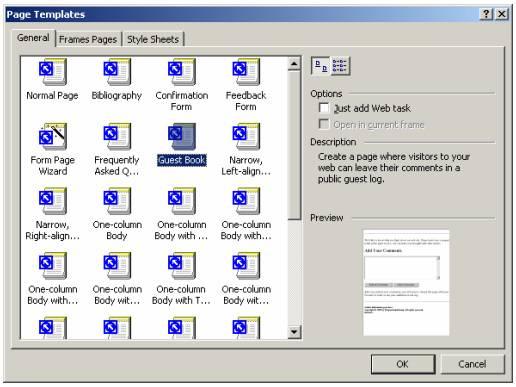
Tạo trang Web mới theo các mẫu định sẵn: ta chọn "**Page Templates**" để tạo các trang Web theo các mẫu định sẵn.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

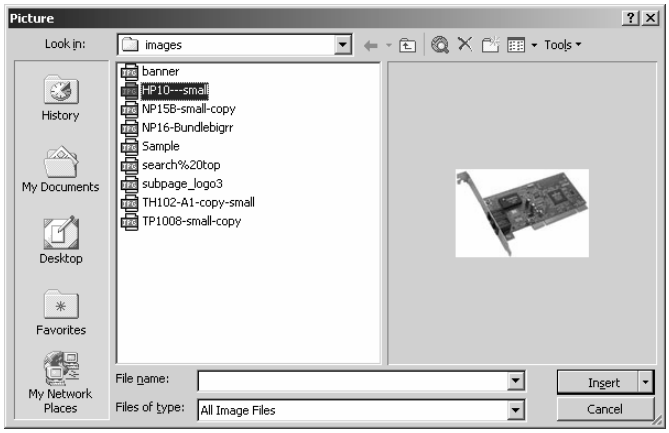

Hình 7.71 – Các cách tạo một trang mới.

Sao đó ta chọn mẫu phù hợp như hình sau và chọn OK.




Hình 7.72 – Các **Page Templates** định sẵn.

Chèn hình ảnh: ta chọn vị trí chèn ảnh bằng cách đặt con trỏ tại vị trí này, sau đó vào menu **Insert/Picture/From File**… Hộp thoại **Picture** xuất hiện, ta chọn tên tập tin ảnh cần chèn.




Hình 7.73 – Hộp thoại **Picture**.

Kết quả được hiển thị trên trang Web như sau:

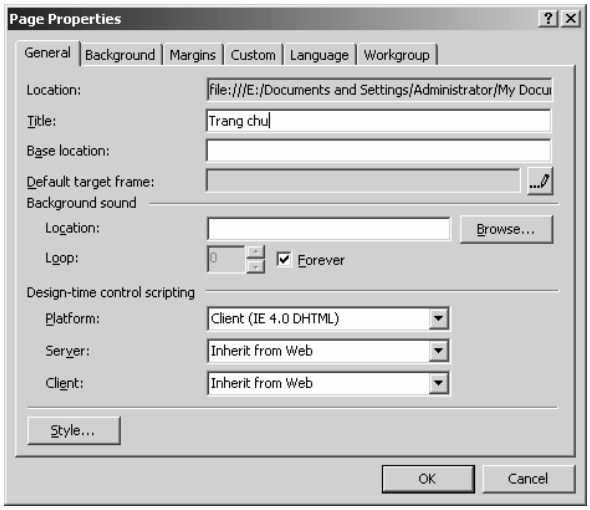


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

- **Đây là card mạng:**

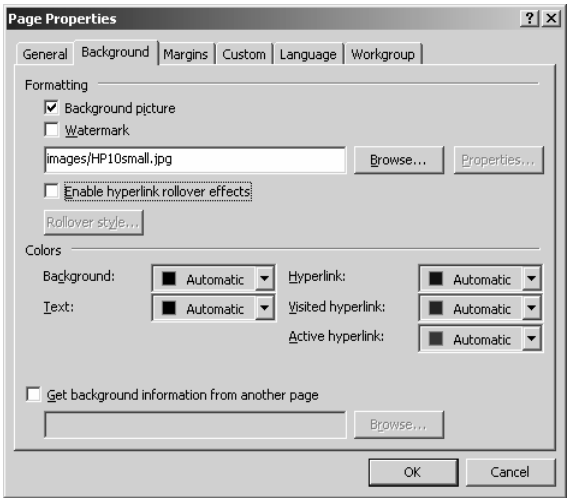
Hình 7.74 – Kết quả hiển thị của trang Web.

Đặt tiêu đề và chương trình điều khiển script cho trang web: chọn chức năng **file/properties** và nhập nội dung tiêu đề vào ô "**Title**" và chọn OK.




Hình 7.75 – Hộp thoại **Page Properties**.

Định nền cho trang Web: ta có thể chọn màu hoặc một hình ảnh bất kỳ để làm nền cho trang Web bằng cách chọn menu **Format/Background**… Nếu chọn hình làm nền thì check vào "**Background Image**" và click chuột vào nút "**Browse**" để chỉ ra tập tin ảnh cần làm nền, sau đó chọn **OK**.

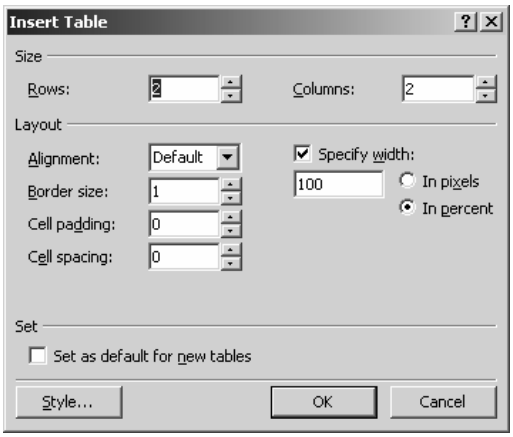



Hình 7.75 – Hộp thoại **Page Properties** – **Tab Background**.



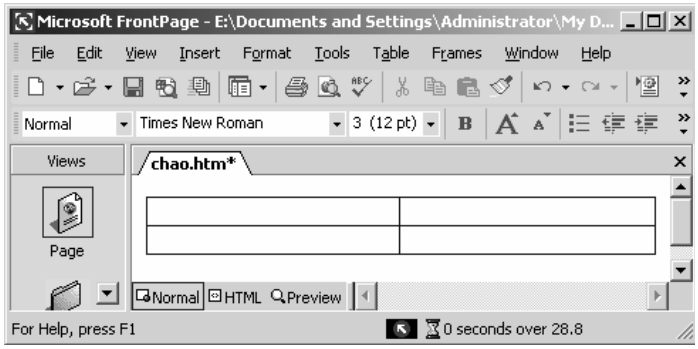
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Tạo bảng (**Table**): công cụ chính để bố trí các đối tượng trên trang Web là bảng. Bảng giúp ta có thể chia nhỏ trang Web thành nhiều ô (**cell**). Tại mỗi ô ta có thể trình bày dạng văn bản hoặc hình ảnh. Muốn tạo một bảng mới trước tiên ta đặt con trỏ tại vị trí cần chèn bảng, sau đó chọn menu **Table/Insert/Table**… Trong hộp thoại "**Insert Table**" ta nhập số dòng cần tạo vào mục "**Rows**" và số cột vào mục "**Columns**". Các thông số trình bày khác như: **Alignment** (canh lề bảng), **Border size** (kích thước của đường viền), **Cell padding** (độ cao của ô), **Cell spacing** (khoảng cách giữa hai ô)…




Hình 7.76 – Hộp thoại **Insert Table**.

Trên trang Web sẽ xuất hiện một bảng như sau:

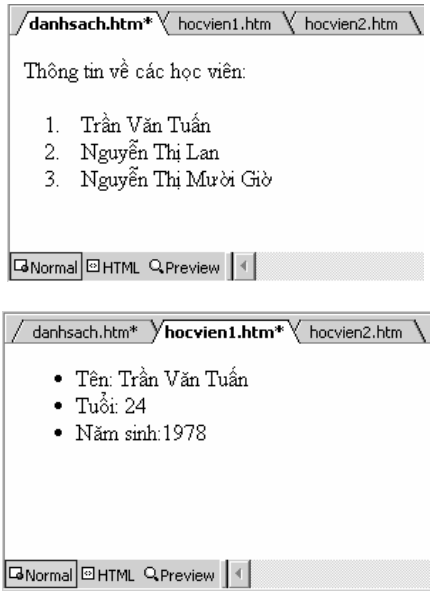



Hình 7.77 – Kết quả sau khi **Insert table**.

Tạo liên kết (**hyperlink**): liên kết giúp ta kết nối các trang Web đơn thành một **Website**. Muốn tạo các liên kết trước hết ta phải có các trang Web đã thiết kế hoàn chỉnh và chú ý đến vị trí (đường dẫn) của trang Web này. Ví dụ ta có ba trang Web: danhsach.htm (chứa tin danh sách các học viên), hocvien1.htm (chứa thông tin chi tiết của học viên 1), hocvien2.htm (chứa thông tin chi tiết của học viên 2).

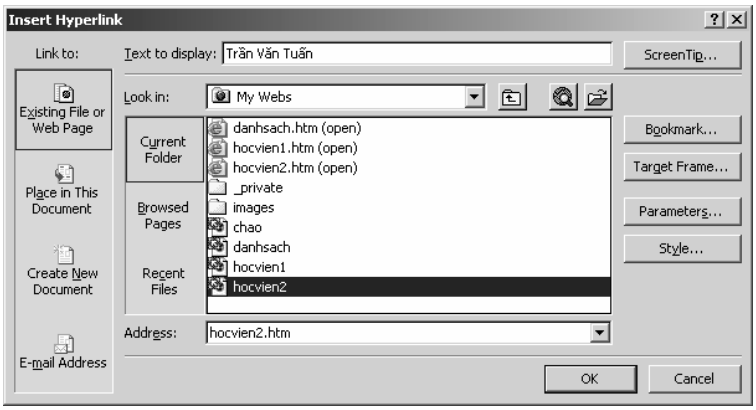


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 7.78 – Nội dung của các trang Web (danhsach.htm và hocvien1.htm).

Bây giờ, ta muốn tạo liên kết giữa trang danhsach.htm đến các trang hocvien.htm nhằm giúp người duyệt web muốn xem thông tin của học viên nào thì click vào tên của học viên đó. Tạo liên kết cho một đoạn văn bản ta phải tô đen đoạn văn bản, sau đó click phải chuột chọn "Hyperlink…" hoặc tạo liên kết cho một hình ta cũng làm tương tự chọn hình ảnh cần tạo liên kết và click phải chuột chọn "**Hyperlink**…". Hộp thoại "**Insert Hyperlink**" xuất hiện, ta chọn tên tập tin trang Web cần liên kết đến và chọn **OK**.




Hình 7.79 – Hộp thoại **Insert Hyperlink**.

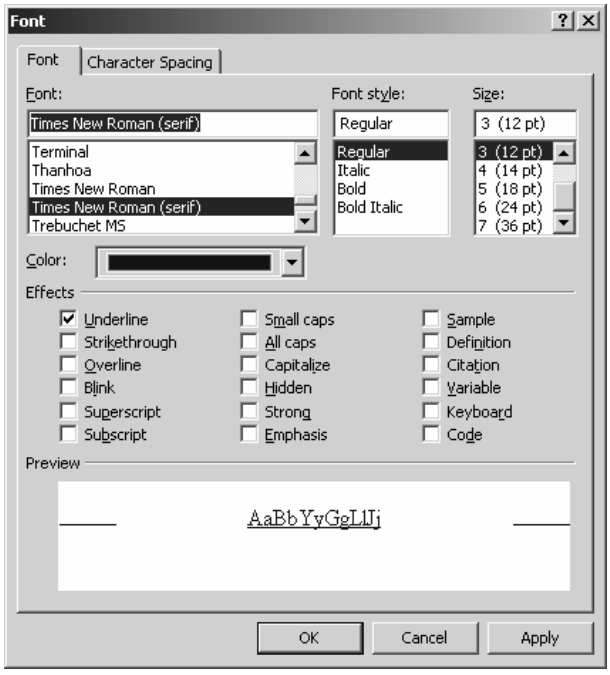
Bạn kiểm tra lại các mối liên kết bằng cách mở trang danhsach.htm và chuyển qua chế độ hiển thị **Preview**, sau đó rê chuột đến tên của các học viên thì thấy con chuột có biểu tượng hình bàn tay, khi click vào thì nội dung trang Web hocvien.htm sẽ được hiển thị.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net


Hình 7.80 – Kết quả sau khi **insert hyperlink**.

Các lựa chọn trong hộp thoại **Font**: chọn menu **Format/Font**, hộp thoại **Font** xuất hiện




Hình 7.81 – Hộp thoại **Font**.

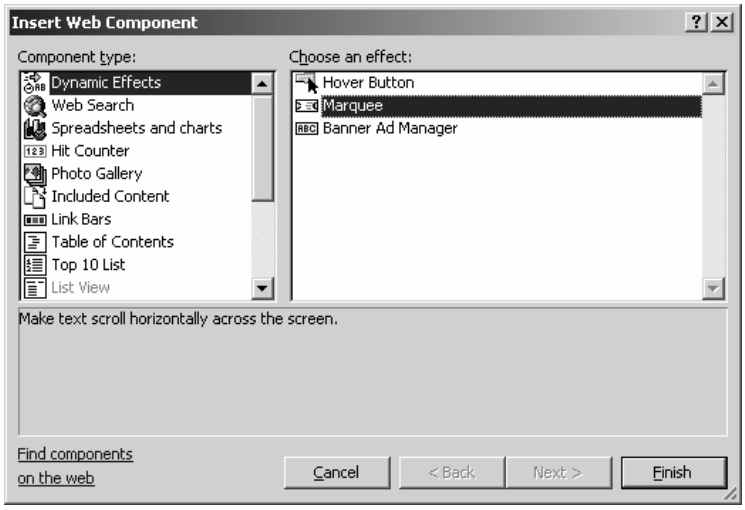
Các hiệu ứng thông dụng là:

- **Underline**: gạch dưới
- **Strikethrough**: gạch ngang
- **Overline**: gạch trên
- **Blink**: nhấp nháy
- **SuperScript**: dạng lũy thừa trên
- **SubScript**: dạng số dưới

Tạo dòng chữ chạy **Marquee**: đặt con trỏ đến vị trí cần chèn, chọn menu **Insert/Web Component/Marquee**… Hộp thoại "**Insert Web Component**" xuất hiện, trong danh sách "**Component type**" chọn "**Dynamic Effect**", mục "**Effect**" chọn **Marquee**, sau đó chọn **Finish**.

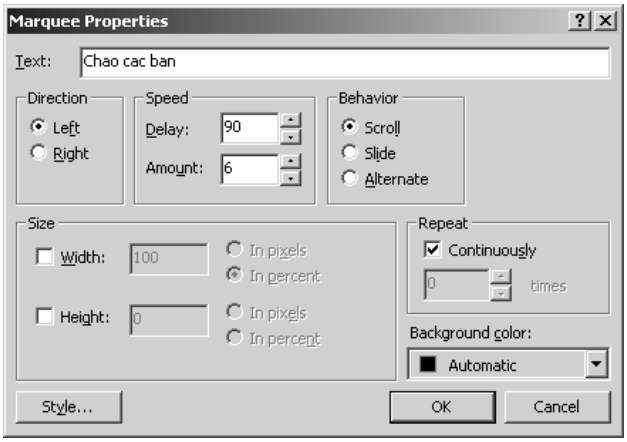


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 7.82 – Hộp thoại **Insert Web Component**.

Hộp thoại "**Marquee Properties**" xuất hiện, ta nhập nội dung cần hiển thị vào mục **Text** và chọn **OK**.




Hình 7.83 – Hộp thoại **Marquee Properties**.

# IX. GIỚI THIỆU VỀ JAVA SCRIPT VÀ VB SCRIPT.

## IX.1. Giới thiệu về ngôn ngữ script.

Ngôn ngữ **Script** là một ngôn ngữ lập trình nhằm bổ sung tính năng động của trang Web (**Dynamic HTML**). Ngôn ngữ này giúp giảm xử lý cho **Server** thay vì dùng **CGI script** tại **Server** thì ta dùng **Java script** tại **Client**.

Các ngôn ngữ **script** thông dụng như: **javascript** (**NetScape**), **jscript** (**Microsoft**), **VBScript** (**Microsoft**).

**VBScript** có lợi thế trong môi trường **Windows**, dùng cho các **ActiveX control** và rất giống **VB**. **VBScript** cũng là ngôn ngữ dùng cho **Server**, nó phối hợp với những đối tượng **Server** để tạo ra những trang Web động từ **Server** (ví dụ như **ASP**).



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

## IX.2. Tổng quan Java Script.

Khi cần thiết kế một trang Web động như máy tính tay (***Calculators***), hiển thị giờ (**D*isplay time***), hiển thị trạng thái thông tin phản hồi(***Feedback***), giải trí trên web (**Entertainment**) thì ta dùng các ngôn ngữ **script** này… **Java Script** không phải là java.

Cú pháp:

Gần giống như các ngôn ngữ lập trình khác như **Pascal, C++, Java**...

**Khai báo và dùng biến**

- var x = 7
- var y,z = "19"
- var lk = "lucky"
- 5 + x // giá trị là 12
- lk + z // giá trị là "lucky19"
- lk + x // giá trị là "lucky7"
- x + z // giá trị là 26
- **Java script** tự động chuyển kiểu cho phù hợp và tự gán giá trị ban đầu là 0 khi ta khai báo biến.

**Các loại dữ liệu trong Java Script**

- Số như -5, 0 hoặc 3.3333
- Chuỗi như "Click Here" hoặc "JavaScript"
- Giá trị logic như: `true` hoặc `false`
- **JavaScript element** xem như là một hàm hoặc một đối tượng
- Giá trị `null`

**Các hằng**

- Hệ thập phân 123, -3434
- Hệ 8(octal): 017
- Hệ 16(hexadecimal): 0x12EF5
- Kiểu dữ liệu số trong **java script** dùng 32 bit

**Chuỗi**

- Khởi tạo, phép toán trên chuỗi
- \t tab
- \n return
- \b backspace

**Đổi kiểu**

- stringthing + numberthing= string
- numberthing + stringthing= number

**Các phép toán:** +, -, *, /, %, ++, --, = =, !=, <, <=, >, >=, …



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

```
x = 4 + y;
y = 5.5 - z;
z = 10 / w;
w = 1.4e5 * v;
  n = -m;
 y = ++x;
 z = x++;
if (x = 3) { }
(x < 17) && buttonPressed && (z == "Meta")
(x < 17) || buttonPressed || (z == "Meta")
(x < 25) && beaupage()
(x - 3.0) < epsilon || (3.0 - x) < epsilon
```

**Chú thích**

```
/* …… */
//…….
Trong htnl <!--  …… -->
```

**Cấu trúc điều khiển**

```
if (điều kiện) { câu lệnh}
if (điều kiện) { câu lệnh} else {câu lệnh}
Cấu trúc While:
                        while (điều kiện) { câu lệnh}
```

## IX.3. Sự kiện trong html và java script.

Các tác động thông thường lên trang web là:

- Chọn một liên kết.
- Di chuyển đến trang trước hoặc trang sau trong các trang đã duyệt.
- Mở một trang Web mới dùng chức năng "**New Window**".
- Thoát khỏi trình duyệt web.

Các sự kiện thường gặp đối với các đối tượng là:

- Di chuyển chuột
- Thay đổi trạng thái.

Chèn đoạn mã **java script** trong **html**:

```
<SCRIPT LANGUAGE="LangName" [SRC="URL"]>
<SCRIPT LANGUAGE="JavaScript" SRC="jscode/click.js"> </SCRIPT>
```

Ẩn nội dung **source** đi:

```
<SCRIPT LANGUAGE="JavaScript">
<!--
```



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

```
function dontclickme()     {
```



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

```
    alert("Ban da click chuot");
    return(false);
}
<!-- end script -->
</SCRIPT>
```

Một trang Web hoàn chỉnh dùng **code Jaca Script**: ví dụ tạo một nút "Chao", khi click vào nút này xuất hiện thông báo "Chao cac ban"

```
<HTML>
<HEAD>
<TITLE>Chao ban</TITLE>
<SCRIPT LANGUAGE="JavaScript">
<!--
function dontclickme() {
    alert("Chao cac ban");
}
<!-- end script -->
</SCRIPT>
</HEAD>
<BODY>
<FORM>
<INPUT TYPE="button" NAME="chao" VALUE="Chao!" onClick="dontclickme()">
</FORM>
</BODY>
</HTML>
```

Ta có thể viết lệnh **Java script** trực tiếp vào sự kiện:

```
<HTML>
<HEAD>
<TITLE>Chao ban</TITLE>
</HEAD>
<BODY>
<FORM>
<INPUT TYPE="button" NAME="chao" VALUE="Chao!"
 onClick="alert('Chao cac ban');">
</FORM>
</BODY>
</HTML>
```



Bắt sự kiện của **List**: ví dụ kiểm tra sự thay đổi giá trị **listbox** dùng hàm onChange()

```
<HTML><HEAD>
<TITLE>Su kien List</TITLE>
```

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

```
<SCRIPT LANGUAGE="JavaScript">
```



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

```
<!--
function Thongbao(str) {
    alert(str);
}
<!-- end script -->
</SCRIPT>
</HEAD>
<BODY>
<SELECT NAME="Ten" onChange="Thongbao('Co su thay doi')">
<OPTION SELECTED>Lan</OPTION>
<OPTION>Cuc</OPTION>
<OPTION>Hong</OPTION>
</SELECT>
</BODY>
</HTML>
```

Bắt sự kiện của **document** (dùng khi cần gọi hàm lúc trang Web vừa mở hoặc khi đóng trang Web):

```
<BODY onLoad="loadfunc()" onUnload="unloadfunc()">
```

## IX.4. VB Script và OLE Controls.

**Khai báo biến**

Dùng từ khóa **Dim** để khai báo biến:

```
<SCRIPT LANGUAGE="VBS">
<!--
Dim MyVariable
-->
</SCRIPT>
```

**Mảng**

```
<SCRIPT LANGUAGE="VBS">
<!- -Một mảng 3 D
    Dim theArray(99, 49, 9)
-->
</SCRIPT>
```

**Cấu trúc điều khiển trong VBScript**

Cấu trúc IF...THEN...ELSE

```
<SCRIPT LANGUAGE="VBS">
        <!--
         If (điều kiện) Then
```



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Mã lệnh



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

```
            Else
                Mã lệnh
            End If
        -->
        </SCRIPT>
```

Cấu trúc DO...WHILE

```
<SCRIPT LANGUAGE="VBS">
        <!--
            Do While (Điều kiện)
Mã lệnh
            Loop
        -->
    </SCRIPT>
```

**Hàm trong VB Script**

Cách tạo hàm:

```
<SCRIPT LANGUAGE="VBS">
        <!--
      Sub TenHam()
            Mã lệnh
        End Sub
        Function TenHam(biến)
            Mã lệnh
        End Function
        -->
        </SCRIPT>
```

**VB Script trong HTML**

Ví dụ Hello:

```
        <HTML>
        <HEAD><TITLE>Trang Web Thu Nghiem</TITLE>
        <SCRIPT LANGUAGE="VBS">
        <!--
        Sub Button1_OnClick
            MsgBox "Chao ban!"
        End Sub     -->
        </SCRIPT>
        </HEAD>
        <BODY>
```



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

```
<H3>Trang Web Thu Nghiem VB Script</H3><HR>
```



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

```
<FORM><INPUT NAME="Button1" TYPE="BUTTON" VALUE="Ban Click vao day"> </FORM>
        </BODY>
        </HTML>
```

Cách viết khác của ví dụ trên:

```
<SCRIPT LANGUAGE="VBS" EVENT="OnClick" FOR="Button1">
<!-- the message
    MsgBox "HELLO THERE!"
-->
</SCRIPT>
```



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

# Tóm tắt

Lý thuyết 4 tiết - Thực hành 3 tiết

| Mục tiêu | Các mục chính | Bài tập bắt buộc | Bài tập làm thêm |
|---|---|---|---|
| Kết thúc bài học này cung cấp học viên kiến thức về họ hệ điều hành Windows Server 2003, cách thức cài đặt Server bằng tay và cài đặt tự động … | I. Tổng quan về họ hệ điều hành Windows Server 2003.<br>II. Cài đặt Windows Server 2003.<br>III. Tự động hóa quá trình cài đặt. | Dựa vào bài tập môn Quản trị Windows Server 2003. | Dựa vào bài tập môn Quản trị Windows Server 2003. |



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

# I. TỔNG QUAN VỀ HỌ HỆ ĐIỀU HÀNH WINDOWS SERVER 2003

Như chúng ta đã biết họ hệ điều hành **Windows 2000 Server** có 3 phiên bản chính là: **Windows 2000 Server**, **Windows 2000 Advanced Server**, **Windows 2000 Datacenter Server**. Với mỗi phiên bản **Microsoft** bổ sung các tính năng mở rộng cho từng loại dịch vụ. Đến khi họ **Server 2003** ra đời thì **Mircosoft** cũng dựa trên tính năng của từng phiên bản để phân loại do đó có rất nhiều phiên bản của họ **Server 2003** được tung ra thị trường. Nhưng 4 phiên bản được sử dụng rộng rãi nhất là: **Windows Server 2003 Standard Edition**, **Enterprise Edition**, **Datacenter Edition**, **Web Edition**.

So với các phiên bản 2000 thì họ hệ điều hành **Server** phiên bản 2003 có những đặc tính mới sau:

- Khả năng kết chùm các **Server** để san sẻ tải (**Network Load Balancing Clusters**) và cài đặt nóng RAM (**hot swap**).
- **Windows Server 2003** hỗ trợ hệ điều hành **WinXP** tốt hơn như: hiểu được chính sách nhóm (**group policy**) được thiết lập trong **WinXP**, có bộ công cụ quản trị mạng đầy đủ các tính năng chạy trên **WinXP.**
- Tính năng cơ bản của **Mail Server** được tính hợp sẵn: đối với các công ty nhỏ không đủ chi phí để mua **Exchange** để xây dựng **Mail Server** thì có thể sử dụng dịch vụ **POP3** và **SMTP** đã tích hợp sẵn vào **Windows Server 2003** để làm một hệ thống mail đơn giản phục vụ cho công ty.
- Cung cấp miễn phí hệ cơ sở dữ liệu thu gọn **MSDE (Mircosoft Database Engine)** được cắt xén từ **SQL Server 2000**.Tuy **MSDE** không có công cụ quản trị nhưng nó cũng giúp ích cho các công ty nhỏ triển khai được các ứng dụng liên quan đến cơ sở dữ liệu mà không phải tốn chi phí nhiều để mua bản **SQL Server**.
- **NAT Traversal** hỗ trợ **IPSec** đó là một cải tiến mới trên môi trường 2003 này, nó cho phép các máy bên trong mạng nội bộ thực hiện các kết nối **peer-to-peer** đến các máy bên ngoài **Internet**, đặt biệt là các thông tin được truyền giữa các máy này có thể được mã hóa hoàn toàn.
- Bổ sung thêm tính năng **NetBIOS over TCP/IP** cho dịch vụ **RRAS (Routing and Remote Access)**. Tính năng này cho phép bạn duyệt các máy tính trong mạng ở xa thông qua công cụ **Network Neighborhood**.
- Phiên bản **Active Directory 1.1** ra đời cho phép chúng ta ủy quyền giữa các gốc rừng với nhau đồng thời việc backup dữ liệu của **Active Directory** cũng dễ dàng hơn.
- Hỗ trợ tốt hơn công tác quản trị từ xa do **Windows 2003** cải tiến **RDP (Remote Desktop Protocol)** có thể truyền trên đường truyền 40Kbps. **Web Admin** cũng ra đời giúp người dùng quản trị Server từ xa thông qua một dịch vụ Web một cách trực quan và dễ dàng.
- Hỗ trợ môi trường quản trị **Server** thông qua dòng lệnh phong phú hơn
- Các **Cluster NTFS** có kích thước bất kỳ khác **với Windows 2000 Server** chỉ hỗ trợ 4KB.
- Cho phép tạo nhiều gốc **DFS (Distributed File System)** trên cùng một Server.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

| | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | |

Bảng so sánh các đặc tính của Windows Server 2003:

# II. CHUẨN BỊ CÀI ĐẶT WINDOWS SERVER 2003.

Hoạch định và chuẩn bị đầy đủ là yếu tố quan trọng quyết định quá trình cài đặt có trơn tru hay không. Trước khi cài đặt, bạn phải biết được những gì cần có để có thể cài đặt thành công và bạn đã có được tất cả những thông tin cần thiết để cung cấp cho quá trình cài đặt. Để lên kế hoạch cho việc nâng cấp hoặc cài mới các **Server** bạn nên tham khảo các hướng dẫn từ **Microsoft Windows Server 2003 Deployment Kit** . Các thông tin cần biết trước khi nâng cấp hoặc cài mới hệ điều hành:

- Phần cứng đáp ứng được yêu cầu của **Windows Server 2003**.
- Làm sao để biết được phần cứng của hệ thống có được **Windows Server 2003** hỗ trợ hay không.
- Điểm khác biệt giữa cách cài đặt mới và cách nâng cấp (**upgrade**).
- Những lựa chọn cài đặt nào thích hợp với hệ thống của bạn, chẳng hạn như chiến lược chia



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

**partition** đĩa, và bạn sẽ sử dụng hệ thống tập tin nào…



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

## II.1. Yêu cầu phần cứng

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | x86, 2GB cho máy | dòng x86 32bit, 64CPU | | x86, 733MHz cho máy | x86, 512GB cho máy | | | |

## II.2. Tương thích phần cứng

Một bước quan trọng trước khi nâng cấp hoặc cài đặt mới Server của bạn là kiểm tra xem phần cứng của máy tính hiện tại có tương thích với sản phẩm hệ điều hành trong họ **Windows Server 2003**. Bạn có thể làm việc này bằng cách chạy chương trình kiểm tra tương thích có sẵn trong đĩa CD hoặc từ trang Web **Catalog**. Nếu chạy chương trình kiểm tra từ đĩa CD, tại dấu nhắc lệnh bạn nhập: ***\i386\winnt32 /checkupgradeonly***.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

## II.3. Cài đặt mới hoặc nâng cấp

Trong một số trường hợp hệ thống **Server** chúng ta đang hoạt động tốt, các ứng dụng và dữ liệu quan trọng đều lưu trữ trên **Server** này, nhưng theo yêu cầu chúng ta phải nâng cấp hệ điều hành **Server** hiện tại thành **Windows Server 2003**. Chúng ta cần xem xét nên nâng cấp hệ điều hành đồng thời giữ lại các ứng dùng và dữ liệu hay cài đặt mới hệ điều hành rồi sau cấu hình và cài đặt ứng dụng lại. Đây là vấn đề cần xem xét và lựa chọn cho hợp lý.

Các điểm cần xem xét khi nâng cấp:

- Với nâng cấp (**upgrade**) thì việc cấu hình **Server** đơn giản, các thông tin của bạn được giữ lại như: người dùng (**users**), cấu hình (**settings**), nhóm (**groups**), quyền hệ thống (**rights**), và quyền truy cập (**permissions**)…
- Với nâng cấp bạn không cần cài lại các ứng dụng, nhưng nếu có sự thay đổi lớn về đĩa cứng thì bạn cần backup dữ liệu trước khi nâng cấp.
- Trước khi nâng cấp bạn cần xem hệ điều hành hiện tại có nằm trong danh sách các hệ điều hành hỗ trợ nâng cấp thành **Windows Server 2003** không ?
- Trong một số trường hợp đặc biệt như bạn cần nâng cấp một máy tính đang làm chức năng **Domain Controller** hoặc nâng cấp một máy tính đang có các phần mềm quan trọng thì bạn nên tham khảo thêm thông tin hướng dẫn của **Microsoft** chứa trong thư mục **\Docs** trên đĩa CD **Windows Server 2003 Enterprise**.

Các hệ điều hành cho phép nâng cấp thành **Windows Server 2003 Enterprise Edition**:

- **Windows NT Server 4.0** với **Service Pack 5** hoặc lớn hơn.
- **Windows NT Server 4.0**, **Terminal Server Edition**, với **Service Pack 5** hoặc lớn hơn.
- **Windows NT Server 4.0**, **Enterprise Edition**, với **Service Pack 5** hoặc lớn hơn.
- **Windows 2000 Server.**
- **Windows 2000 Advanced Server.**
- **Windows Server 2003, Standard Edition.**

## II.4. Phân chia ổ đĩa.

Đây là việc phân chia ổ đĩa vật lý thành các **partition logic**. Khi chia **partition**, bạn phải quan tâm các yếu tố sau:

- **Lượng không gian cần cấp phát:** bạn phải biết được không gian chiếm dụng bởi hệ điều hành, các chương trình ứng dụng, các dữ liệu đã có và sắp phát sinh.
- **Partition system và boot:** khi cài đặt **Windows 2003 Server** sẽ được lưu ở hai vị trí là **partition system** và **partition boot**. **Partition system** là nơi chứa các tập tin giúp cho việc khởi động **Windows 2003 Server**. Các tập tin này không chiếm nhiều không gian đĩa. Theo mặc định, **partition active** của máy tính sẽ được chọn làm **partition system**, vốn thường là ổ đĩa C:. **Partition boot** là nơi chứa các tập tin của hệ điều hành. Theo mặc định các tập tin này lưu trong thư mục **WINDOWS**. Tuy nhiên bạn có thể chỉ định thư mục khác trong quá trình cài đặt. **Microsoft** đề nghị **partition** này nhỏ nhất là 1,5 GB.
- Cấu hình đĩa đặc biệt: **Windows 2003 Server** hỗ trợ nhiều cấu hình đĩa khác nhau. Các lựa chọn có thể là **volume simple**, **spanned**, **striped**, **mirrored** hoặc là **RAID-5**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

- **Tiện ích phân chia partition:** nếu bạn định chia **partition** trước khi cài đặt, bạn có thể sử dụng nhiều chương trình tiện ích khác nhau, chẳng hạn như **FDISK** hoặc **PowerQuest Partition Magic**. Có thể ban đầu bạn chỉ cần tạo một **partition** để cài đặt **Windows 2003 Server**, sau đó sử dụng công cụ **Disk Management** để tạo thêm các **partition** khác.

## II.5. Chọn hệ thống tập tin.

Bạn có thể chọn sử dụng một trong ba loại hệ thống tập tin sau:

- ***FAT16*** (**file allocation table**)***:*** là hệ thống được sử dụng phổ biến trên các hệ điều hành **DOS** và **Windows 3.x**. Có nhược điểm là **partition** bị giới hạn ở kích thước 2GB và không có các tính năng bảo mật như **NTFS.**
- ***FAT32:*** được đưa ra năm 1996 theo bản **Windows 95 OEM Service Release 2 (OSR2)**. Có nhiều ưu điểm hơn **FAT16** như: hỗ trợ **partition** lớn đến 2TB; có các tính năng dung lỗi và sử dụng không gian đĩa cứng hiệu quả hơn do giảm kích thước **cluster**. Tuy nhiên **FAT32** lại có nhược điểm là không cung cấp các tính năng bảo mật như **NTFS**.
- ***NTFS:*** là hệ thống tập tin được sử dụng trên các hệ điều hành **Windows NT, Windows 2000**, **Windows 2003**. **Windows 2000, Windows 2003** sử dụng **NTFS** phiên bản 5. Có các đặc điểm sau: chỉ định khả năng an toàn cho từng tập tin, thư mục; nén dữ liệu, tăng không gian lưu trữ; có thể chỉ định hạn ngạch sử dụng đĩa cho từng người dùng; có thể mã hoá các tập tin, nâng cao khả năng bảo mật.

## II.6. Chọn chế độ sử dụng giấy phép.

Bạn chọn một trong hai chế độ giấy phép sau đây:

- **Per server licensing**: là lựa chọn tốt nhất trong trường hợp mạng chỉ có một Server và phục cho một số lượng Client nhất định. Khi chọn chế độ giấy phép này, chúng ta phải xác định số lượng giấy phép tại thời điểm cài đặt hệ điều hành. Số lượng giấy phép tùy thuộc vào số kết nối đồng thời của các Client đến Server. Tuy nhiên, trong quá trình sử dụng chúng ta có thể thay đổi số lượng kết nối đồng thời cho phù hợp với tình hình hiện tại của mạng.
- **Per Seat licensing**: là lựa chọn tốt nhất trong trường hợp mạng có nhiều Server. Trong chế độ giấy phép này thì mỗi Client chỉ cần một giấy phép duy nhất để truy xuất đến tất cả các Server và không giới hạn số lượng kết nối đồng thời đến Server.

## II.7. Chọn phương án kết nối mạng.

### II.7.1 Các giao thức kết nối mạng.

**Windows 2003** mặc định chỉ cài một giao thức **TCP/IP**, còn những giao thức còn lại như **IPX**, **AppleTalk** là những tùy chọn có thể cài đặt sau nếu cần thiết. Riêng giao thức **NetBEUI**, **Windows 2003** không đưa vào trong các tùy chọn cài đặt mà chỉ cung cấp kèm theo đĩa **CD-ROM** cài đặt **Windows 2003** và được lưu trong thư mục **\VALUEADD\MSFT\NET\NETBEUI**.



### II.7.2 Thành viên trong Workgroup hoặc Domain.

Nếu máy tính của bạn nằm trong một mạng nhỏ, phân tán hoặc các máy tính không được nối mạng với nhau, bạn có thể chọn cho máy tính làm thành viên của **workgroup**, đơn giản bạn chỉ cần cho biết tên

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

**workgroup** là xong.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Nếu hệ thống mạng của bạn làm việc theo cơ chế quản lý tập trung, trên mạng đã có một vài máy **Windows 2000 Server** hoặc **Windows 2003 Server** sử dụng **Active Directory** thì bạn có thể chọn cho máy tính tham gia **domain** này. Trong trường hợp này, bạn phải cho biết tên chính xác của **domain** cùng với tài khoản (gồm có **username** và **password**) của một người dùng có quyền bổ sung thêm máy tính vào **domain**. Ví dụ như tài khoản của người quản trị mạng (**Administrator**).

Các thiết lập về ngôn ngữ và các giá trị cục bộ.

**Windows 2000 Server** hỗ trợ rất nhiều ngôn ngữ, bạn có thể chọn ngôn ngữ của mình nếu được hỗ trợ. Các giá trị **local** gồm có hệ thống số, đơn vị tiền tệ, cách hiển thị thời gian, ngày tháng.

# III. CÀI ĐẶT WINDOWS SERVER 2003.

## III.1. Giai đoạn Preinstallation.

Sau khi kiểm tra và chắc chắn rằng máy của mình đã hội đủ các điều kiện để cài đặt **Windows 2003 Server**, bạn phải chọn một trong các cách sau đây để bắt đầu quá trình cài đặt.

### III.1.1 Cài đặt từ hệ điều hành khác.

Nếu máy tính của bạn đã có một hệ điều hành và bạn muốn nâng cấp lên **Windows 2003 Server** hoặc là bạn muốn khởi động kép, đầu tiên bạn cho máy tính khởi động bằng hệ điều hành có sẵn này, sau đó tiến hành quá trình cài đặt **Windows 2003 Server**.

Tuỳ theo hệ điều hành đang sử dụng là gì, bạn có thể sử dụng hai lệnh sau trong thư mục **I386**:

- **WINNT32.EXE** nếu là Windows 9x hoặc Windows NT.
- **WINNT.EXE** nếu là hệ điều hành khác.

### III.1.2 Cài đặt trực tiếp từ đĩa CD Windows 2003.

Nếu máy tính của bạn hỗ trợ tính năng khởi động từ đĩa CD, bạn chỉ cần đặt đĩa CD vào ổ đĩa và khởi động lại máy tính. Lưu ý là bạn phải cấu hình **CMOS Setup**, chỉ định thiết bị khởi động đầu tiên là ổ đĩa **CDROM**. Khi máy tính khởi động lên thì quá trình cài đặt tự động thi hành, sau đó làm theo những hướng dẫn trên màn hình để cài đặt **Windows 2003**.

### III.1.3 Cài đặt Windows 2003 Server từ mạng.

Để có thể cài đặt theo kiểu này, bạn phải có một Server phân phối tập tin, chứa bộ nguồn cài đặt **Windows 2003 Server** và đã chia sẻ thư mục này. Sau đó tiến hành theo các bước sau:

- Khởi động máy tính định cài đặt.
- Kết nối vào máy Server và truy cập vào thư mục chia sẻ chứa bộ nguồn cài đặt.
- Thi hành lệnh **WINNT.EXE** hoặc **WINNT32.EXE** tuỳ theo hệ điều hành đang sử dụng trên máy.
- Thực hiện theo hướng dẫn của chương trình cài đặt.

## III.2. Giai đoạn Text-Based Setup.



Trong qúa trình cài đặt nên chú ý đến các thông tin hướng dẫn ở thanh trạng thái.

Giai đoạn **Text-based setup** diễn ra một số bước như sau:

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

(1) Cấu hình **BIOS** của máy tính để có thể khởi động từ ổ đĩa **CD-ROM.**



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

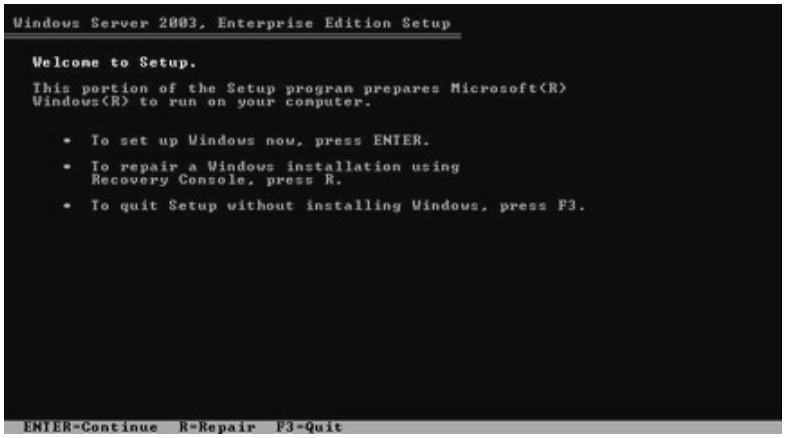
(2) Đưa đĩa cài đặt **Windows 2003 Server** vào ổ đĩa **CD-ROM** và khởi động lại máy.

(3) Khi máy khởi động từ đĩa **CD-ROM** sẽ xuất hiện một thông báo "**Press any key to continue…**" yêu cầu nhấn một phím bất kỳ để bắt đầu quá trình cài đặt.

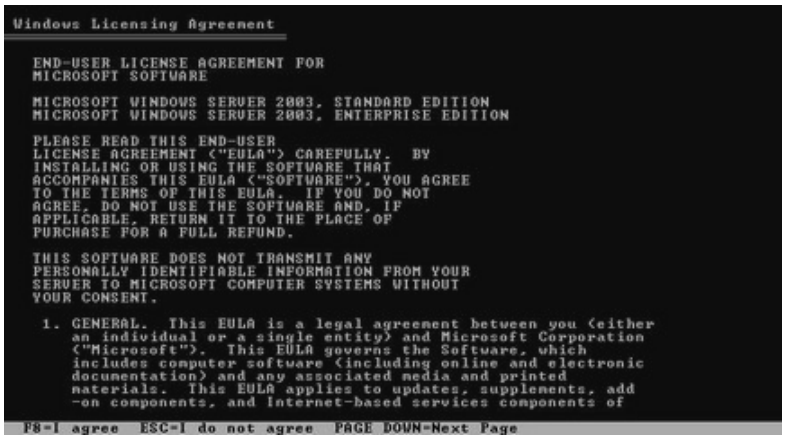
(4) Nếu máy có ổ đĩa **SCSI** thì phải nhấn phím F6 để chỉ Driver của ổ đĩa đó.

(5) Trình cài đặt tiến hành chép các tập tin và **driver** cần thiết cho quá trình cài đặt.

(6) Nhấn **Enter** để bắt đầu cài đặt.



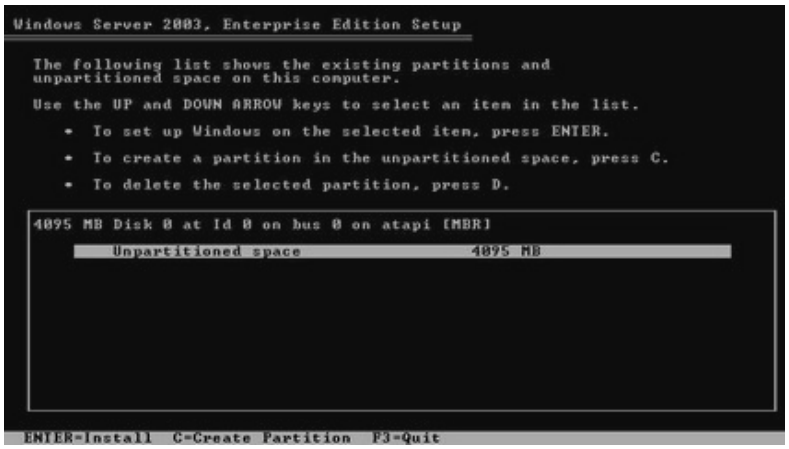

(7) Nhấn phím **F8** để chấp nhận thỏa thuận bản quyền và tiếp tục quá trình cài đặt. Nếu nhấn **ESC**, thì chương trình cài đặt kết.



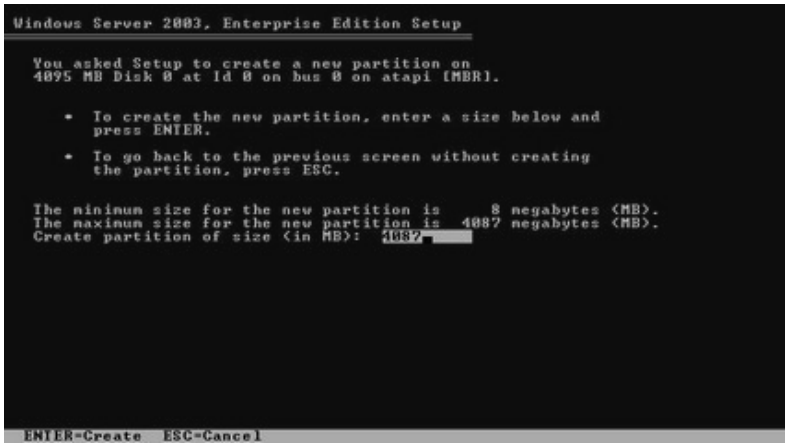

(8) Chọn một vùng trống trên ổ đĩa và nhấn phím **C** để tạo một **Partition** mới chứa hệ điều hành.



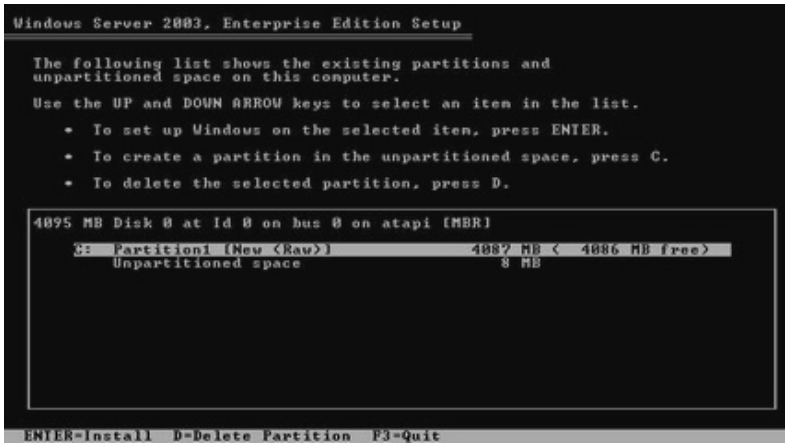
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




(9) Nhập vào kích thước của **Partition** mới và nhấn **Enter**.



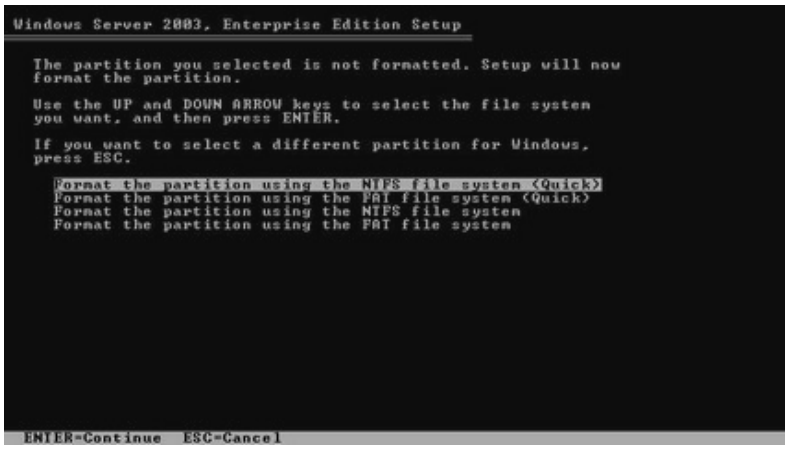

(10) Chọn **Partition** vừa tạo và nhấn **Enter** để tiếp tục.



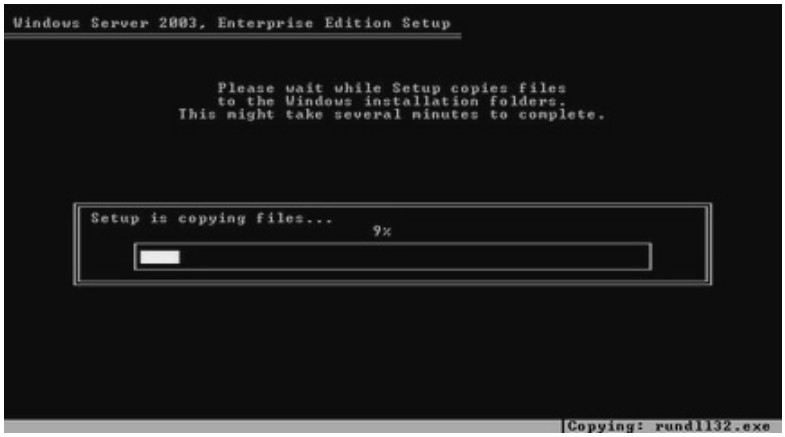

(11) Chọn kiểu hệ thống tập tin (**FAT** hay **NTFS**) để định dạng cho **partition**. Nhấn **Enter** để tiếp tục.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




(12) Trình cài đặt sẽ chép các tập tin của hệ điều hành vào **partition** đã chọn.




(13) Khởi động lại hệ thống để bắt đầu giai đoạn **Graphical Based**. Trong khi khởi động, không nhấn bất kỳ phím nào khi hệ thống yêu cầu "**Press any key to continue…**"

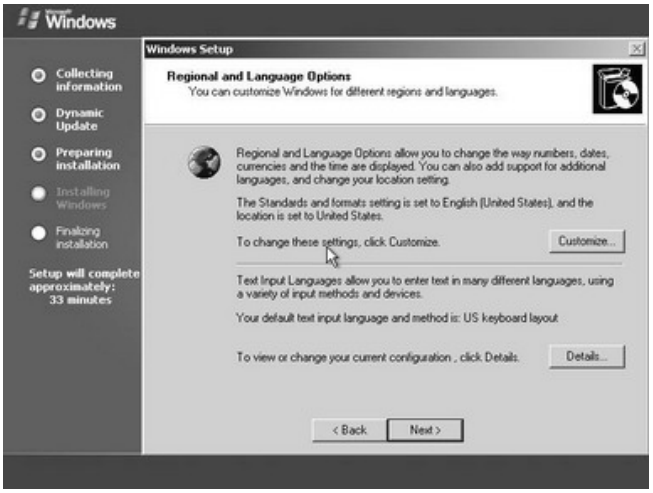
## III.3. Giai đoạn Graphical-Based Setup.

(1) Bắt đầu giai đoạn **Graphical**, trình cài đặt sẽ cài **driver** cho các thiết bị mà nó tìm thấy trong hệ thống.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net


(2) Tại hộp thoại **Regional and Language Options**, cho phép chọn các tùy chọn liên quan đến ngôn ngữ, số đếm, đơn vị tiền tệ, định dạng ngày tháng năm,….Sau khi đã thay đổi các tùy chọn phù hợp, nhấn **Next** để tiếp tục.




(3) Tại hộp thoại **Personalize Your Software**, điền tên người sử dụng và tên tổ chức. Nhấn **Next**.

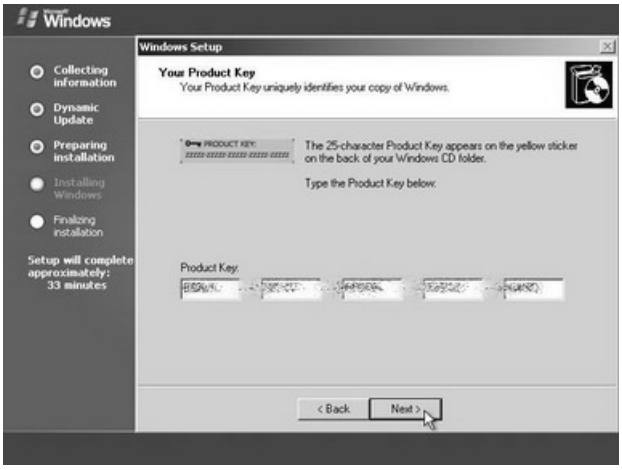



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

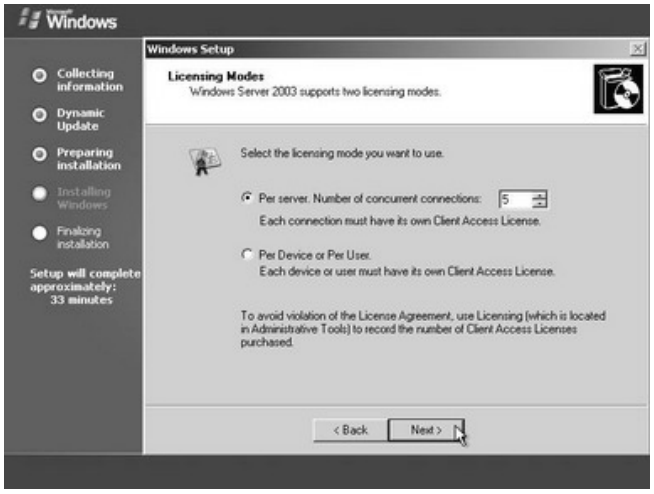
(4) Tại hộp thoại **Your Product Key**, điền vào 25 số **CD-Key** vào 5 ô trống bên dưới. Nhấn **Next**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




(5) Tại hộp thoại **Licensing Mode**, chọn chế độ bản quyền là **Per Server** hoặc **Per Seat** tùy thuộc vào tình hình thực tế của mỗi hệ thống mạng.




(6) Tại hộp thoại **Computer Name and Administrator Password**, điền vào tên của **Server** và **Password** của người quản trị (**Administrator**).

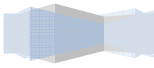



(7) Tại hộp thoại **Date and Time Settings**, thay đổi ngày, tháng, và múi giờ (**Time zone**) cho thích

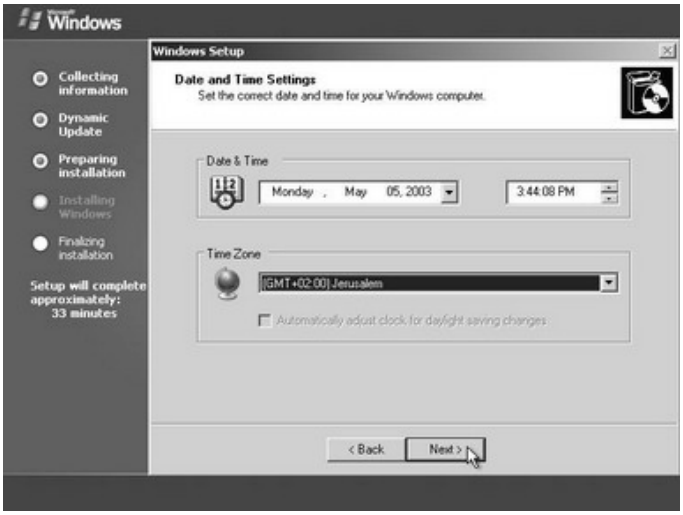
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

hợp.

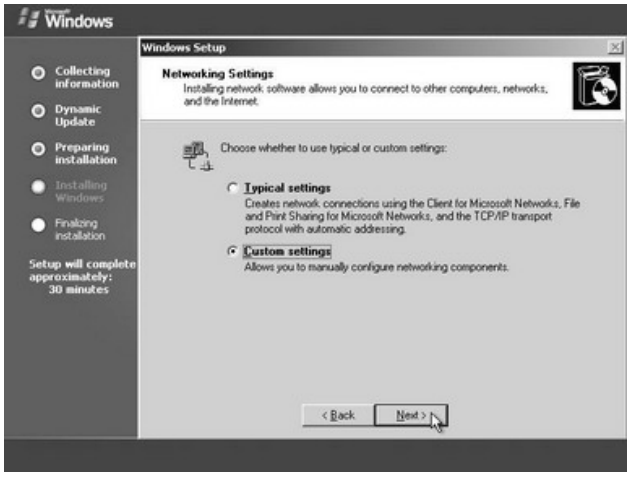




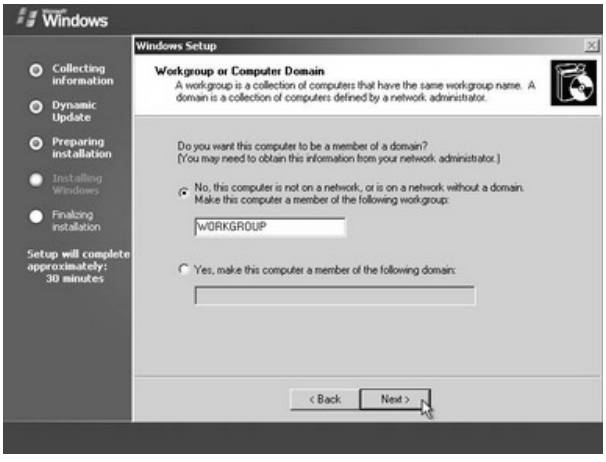
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




(8) Tại hộp thoại **Networking Settings**, chọn **Custom settings** để thay đổi các thông số giao thức **TCP/IP**. Các thông số này có thể thay đổi lại sau khi quá trình cài đặt hoàn tất.




(9) Tại hộp thoại **Workgroup or Computer Domain**, tùy chọn gia nhập **Server** vào một **Workgroup** hay một **Domain** có sẵn. Nếu muốn gia nhập vào **Domain** thì đánh vào tên **Domain** vào ô bên dưới.






Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

(10) Sau khi chép đầy đủ các tập tin, quá trình cài đặt kết thúc.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

# IV. TỰ ĐỘNG HÓA QUÁ TRÌNH CÀI ĐẶT.

Nếu bạn dự định cài đặt hệ điều hành **Windows 2003 Server** trên nhiều máy tính, bạn có thể đến từng máy và tự tay thực hiện quá trình cài đặt như đã hướng dẫn trong chương trước. Tuy nhiên, chắc chắn công việc này sẽ vô cùng nhàm chán và không hiệu quả. Lúc này việc tự động hoá quá trình cài đặt sẽ giúp công việc của bạn trở nên đơn giản, hiệu quả và ít tốn kém hơn.

Có nhiều phương pháp hỗ trợ việc cài đặt tự động. Chẳng hạn, bạn có thể sử dụng phương pháp dùng ảnh đĩa (**disk image**) hoặc phương pháp cài đặt không cần theo dõi (**unattended installation**) thông qua một kịch bản (**script**) hay tập tin trả lời.

## IV.1. Giới thiệu kịch bản cài đặt.

Kịch bản cài đặt là một tập tin văn bản có nội dung trả lời trước tất cả các câu hỏi mà trình cài đặt hỏi như: tên máy, **CD-Key**,….Để trình cài đặt có thể đọc hiểu các nội dung trong kịch bản thì nó phải được tạo ra theo một cấu trúc được quy định trước. Để tạo ra được các kịch bản cài đặt, có thể dùng bất kỳ chương trình soạn thảo văn bản nào, chẳng hạn như **Notepad**. Tuy nhiên, kịch bản là một tập tin có cấu trúc nên trong quá trình soạn thảo có thể xảy ra các sai sót dẫn đến quá trình tự động hóa cài đặt không diễn ra theo ý muốn. Do đó, **Microsoft** đã tạo ra một tiện ích có tên là **Setup Manager** (**setupmgr.exe**) để giúp cho việc tạo ra kịch bản cài đặt được dễ dàng hơn. Sau khi có được kịch bản, có thể sử dụng **Notepad** để thêm, sửa lại một số thông tin để sử dụng kịch bản vào quá trình cài đặt tự động hiệu quả hơn.

## IV.2. Tự động hóa dùng tham biến dòng lệnh.

Khi tiến hành cài đặt **Windows 2003 Server**, ngoài cách khởi động và cài trực tiếp từ đĩa **CD-ROM**, còn có thể dùng một trong hai lệnh sau: **winnt.exe** dùng với các máy đang chạy hệ điều hành DOS, **windows 3.x** hoặc **Windows for workgroup**; **winnt32.exe** khi máy đang chạy hệ điều hành **Windows 9x**, **Windows NT** hoặc mới hơn. Hai lệnh trên được đặt trong thư mục **I386** của đĩa cài đặt.

Sau đây là cú pháp cài đặt từ 2 lệnh trên:

winnt [/s:[sourcepath]] [/t:[tempdrive]] [/u:[answer_file]]

[/udf:id [,UDB_file]]

Ý nghĩa các tham số:

**/s**

Chỉ rỏ vị trí đặt của bộ nguồn cài đặt (thư mục I386). Đường dẫn phải là dạng đầy đủ, ví dụ: e:\i386 hoặc **\\server\i386**. Giá trị mặc định là thư mục hiện hành.

**/t**

Hướng chương trình cài đặt đặt thư mục tạm vào một ổ đĩa và cài **Windows** vào ổ đĩa đó. Nếu không chỉ định, trình cài đặt sẽ tự xác định.

**/u**

Cài đặt không cần theo dõi với một tập tin trả lời tự động (kịch bản). Nếu sử dụng /u thì phải sử dụng /s.

**/udf**



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Chỉ định tên của **Server** và tập tin cơ sở dữ liệu chứa tên, các thông tin đặc trưng cho mỗi máy (unattend.udf).

**winnt32** [**/checkupgradeonly**] [**/s:***sourcepath*] [**/tempdrive:***drive_letter***:**] [**/unattend**[*num*]**:**[*answer_file*]]

[**/udf:***id* [,*UDB_file*]]

Ý nghĩa của các tham số:

**/checkupgradeonly**

Kiểm tra xem máy có tương thích để nâng cấp và cài đặt **Windows 2003 Server** hay không?

**/tempdrive**

Tương tự như tham số /t

**/unattend**

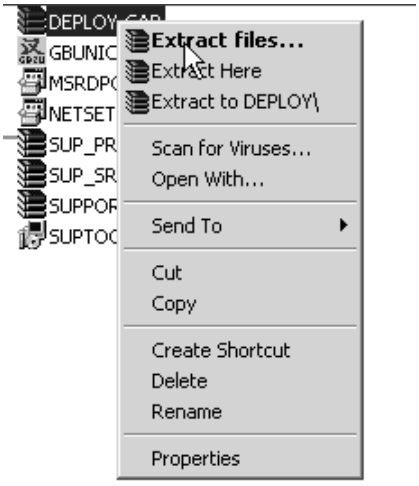
Tương tư như tham số /u

## IV.3. Sử dụng Setup Manager để tạo ra tập tin trả lời.

**Setup Manager** là một tiện ích giúp cho việc tạo các tập tin trả lời sử dụng trong cài đặt không cần theo dõi. Theo mặc định, **Setup Manager** không được cài đặt, mà được đặt trong tập tin **Deploy.Cab**. Chỉ có thể chạy tiện ích **Setup Manager** trên các hệ điều hành **Windows 2000, Windows XP, Windows 2003**.

Tạo tập tin trả lời tự động bằng **Setup Manager**:

(1) Giải nén tập tin **Deploy.cab** được lưu trong thư mục **Support\Tools** trên đĩa cài đặt **Windows 2003**.

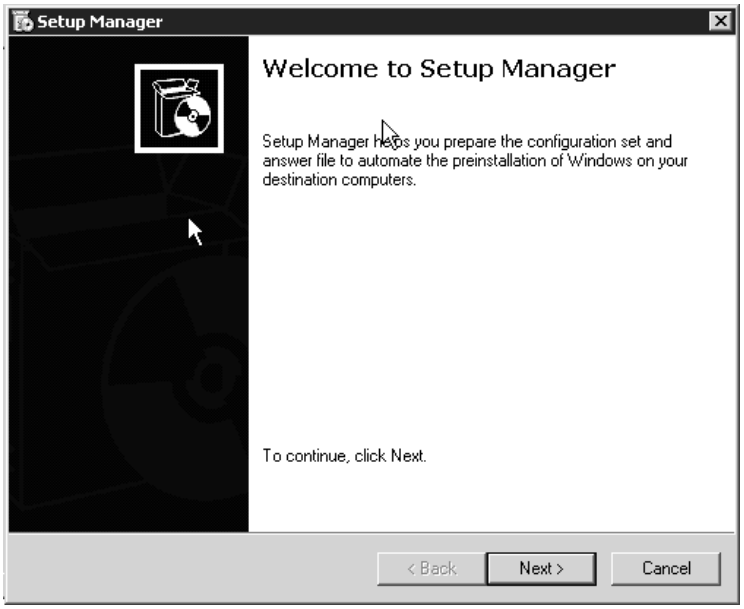



(2) Thi hành tập tin **Setupmgr.exe**

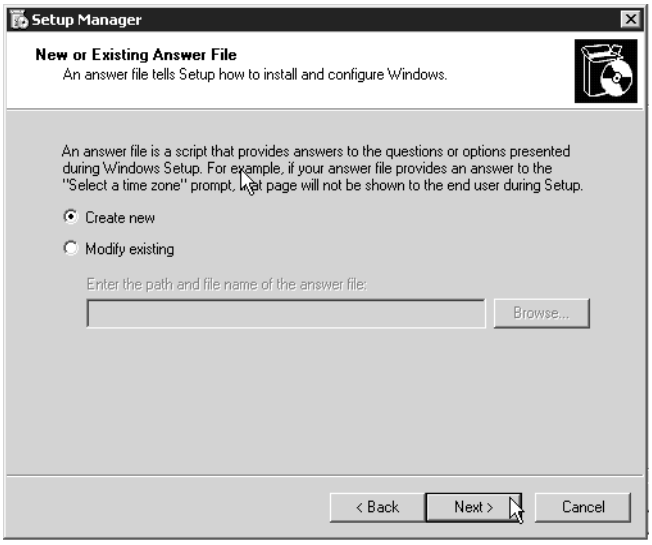
(3) Hộp thoại **Setup Manager** xuất hiện, nhấn **Next** để tiếp tục.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net



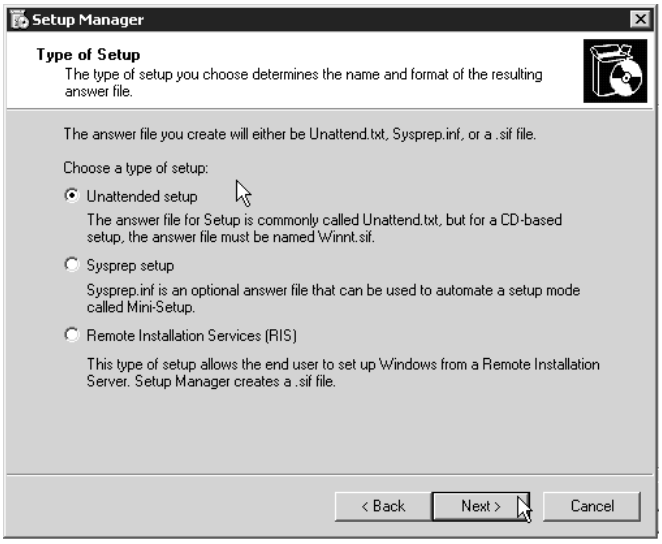

(4) Xuất hiện hộp thoại **New or Existing Answer File**. Hộp thoại này cho phép bạn chỉ định tạo ra một tập tin trả lời mới, một tập tin trả lời phản ánh cấu hình của máy tính hiện hành hoặc là chỉnh sửa một tập tin sẵn có. Bạn chọn **Create new** và nhấn **Next**.



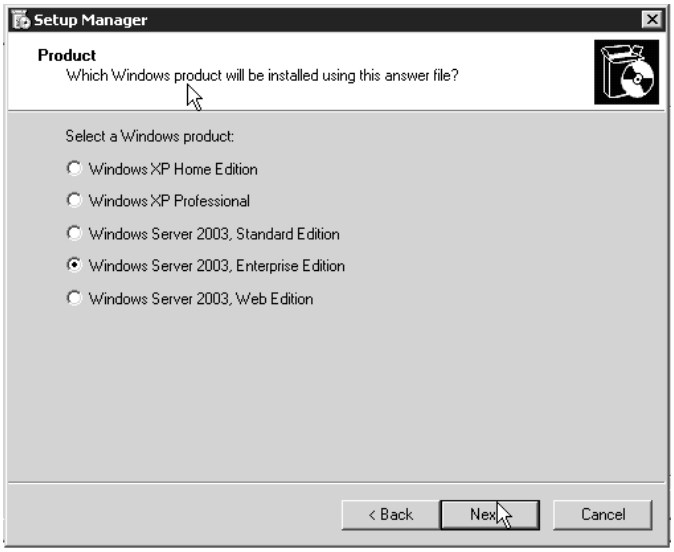

(5) Tiếp theo là hộp thoại **Type of Setup**. Chọn **Unattended Setup** và chọn **Next**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net



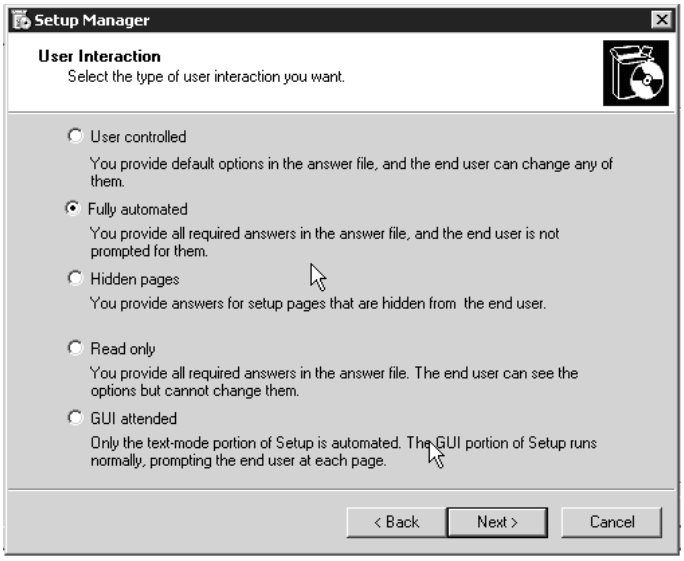

(6) Trong hộp thoại **Product**, chọn hệ điều hành cài đặt sử dụng tập tin trả lời tự động. Chọn **Windows Server 2003, Enterprise Edition**, nhấn **Next**.



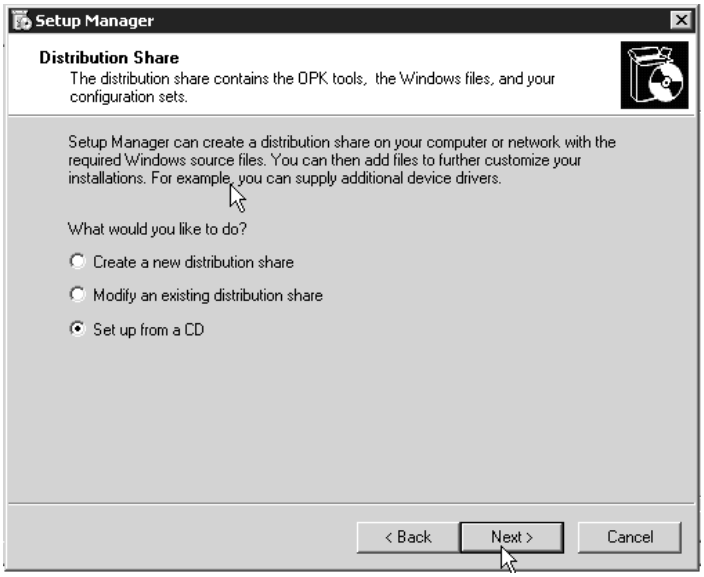

(7) Tại hộp thoại **User Interaction**, chọn mức độ tương tác với trình cài đặt của người sử dụng. Chọn **Fully Automated**, nhấn **Next**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net



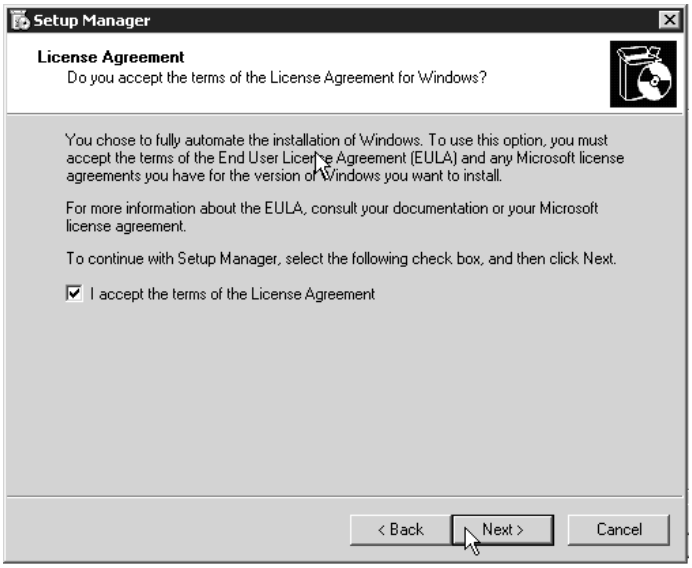

(8) Xuất hiện hộp thoại **Distribution Share**, chọn **Setup from a CD**, nhấn **Next**.



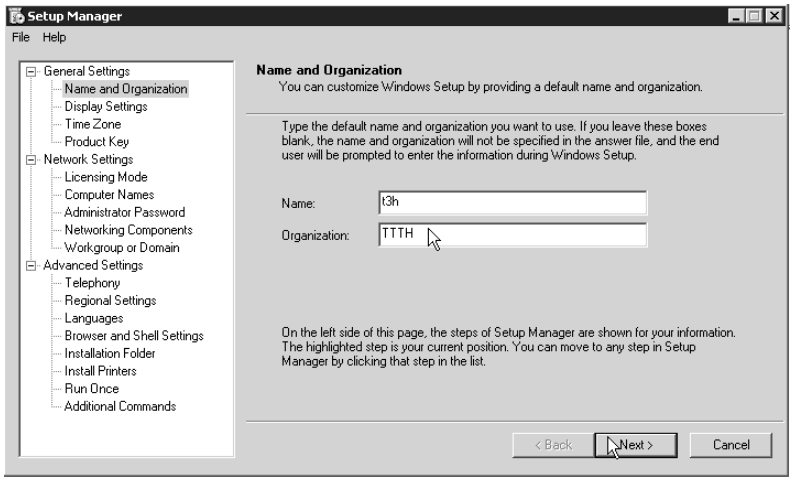

(9) Tại hộp thoại **License Agreement**, đánh dấu vào **I accept the terms of …**, nhấn **Next**.



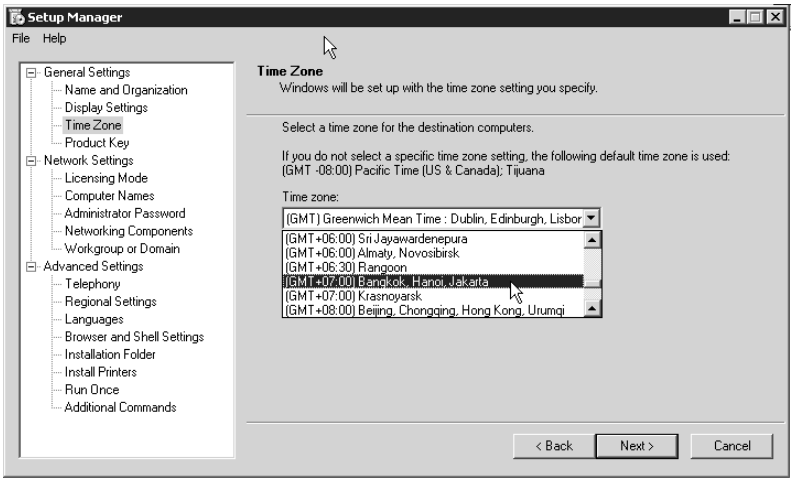
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




(10) Tại cửa sổ **Setup Manager**, chọn mục **Name and Organization**. Điền tên và tổ chức sử dụng hệ điều hành. Nhấn **Next**.



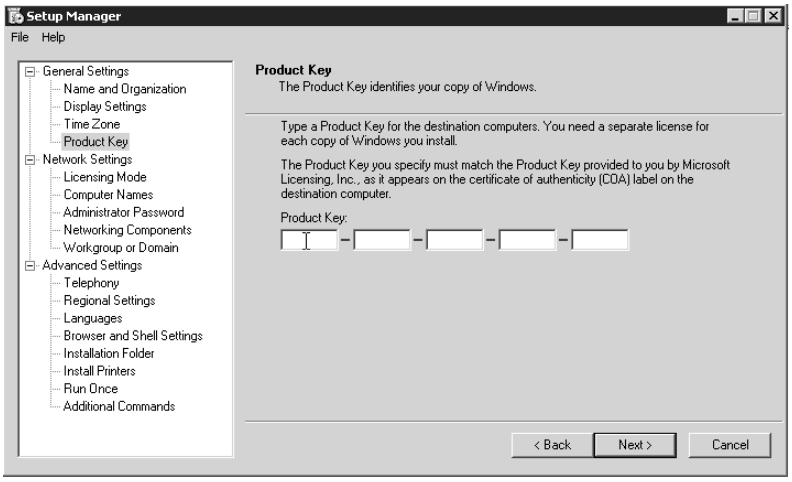

(11) Chọn mục **Time Zone** chọn múi giờ (**GMT+7:00) Bangkok, Hanoi, Jarkata**. Nhấn **Next**.



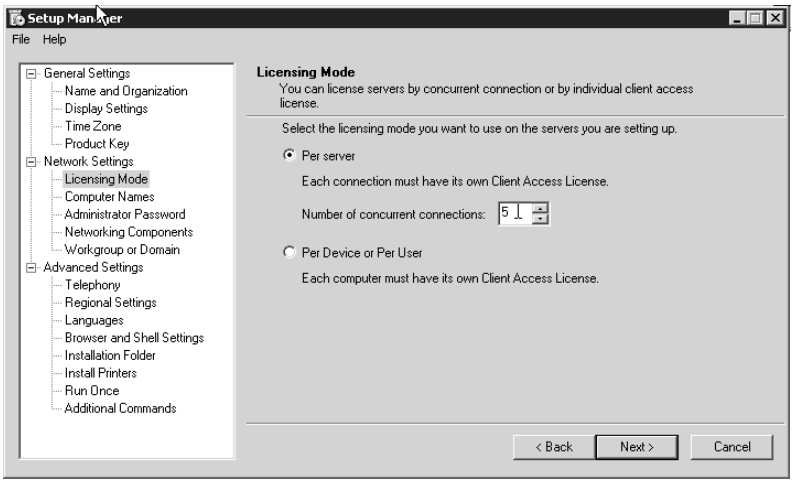



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

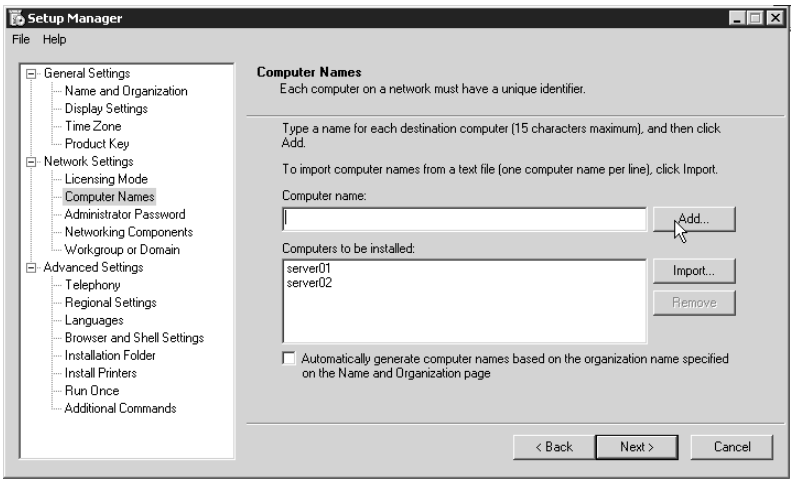
(12) Tại mục **Product Key**, điền **CD-Key** vào trong 5 ô trống. Nhấn **Next**.




(13) Tại mục **Licensing Mode**, chọn loại bản quyền thích hợp. Nhấn **Next**.



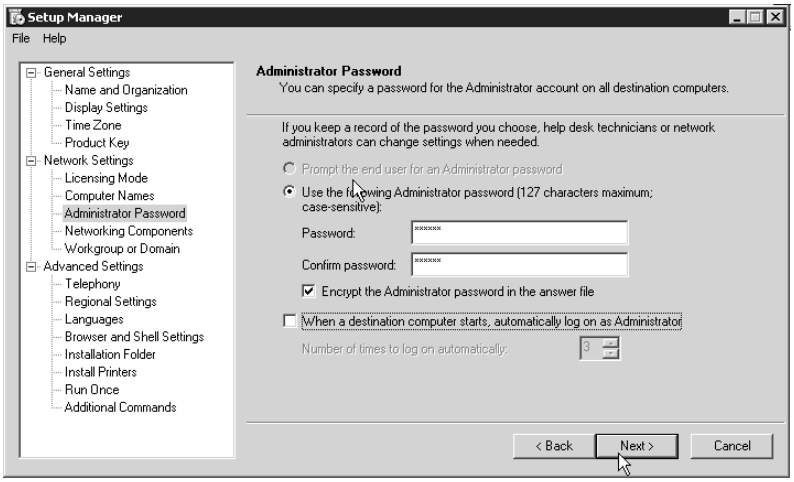

(14) Tại mục **Computer Names**, điền tên của các máy dự định cài đặt. Nhấn **Next**.



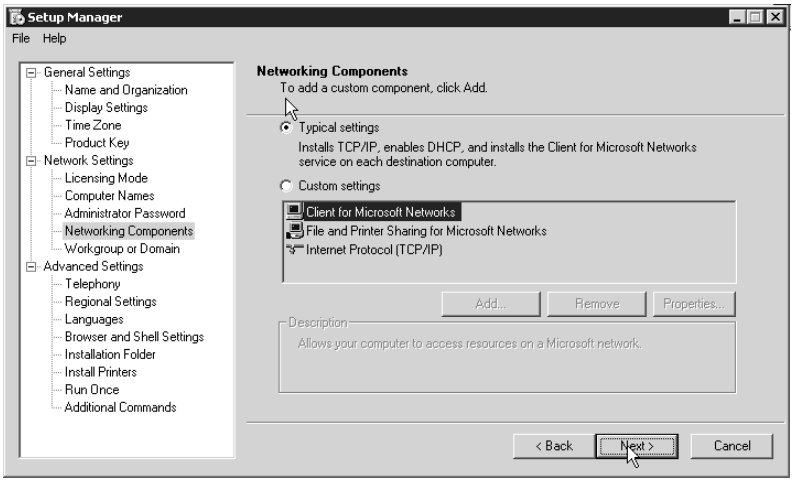



(15) Tại mục **Administrator Password**, nhập vào **password** của người quản trị. Nếu muốn mã hóa **password** thì đánh dấu chọn vào mục "**Encrypt the Administrator password…**". Nhấn **Next**.

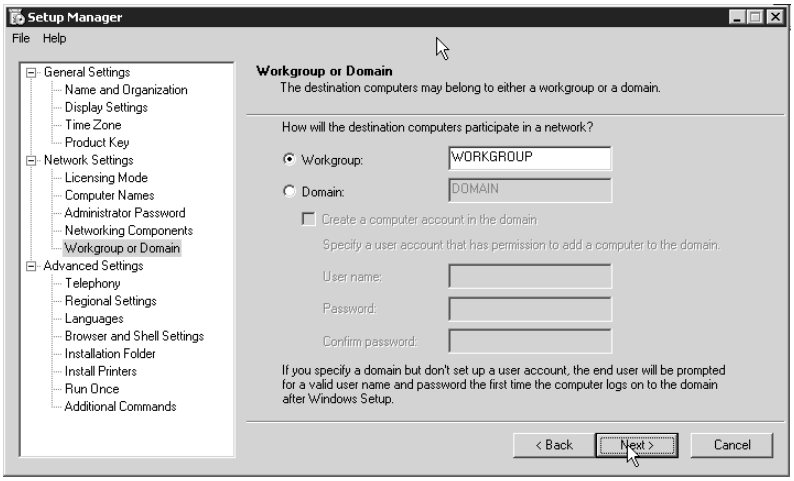
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




(16) Tại mục **Network Component**, cấu hình các thông số cho giao thức **TCP/IP** và cài thêm các giao thức. Nhấn **Next**.




(17) Tại mục **Workgroup or Domain**, gia nhập máy vào **Workgroup** hoặc **Domain** có sẵn. Nhấn **Next**.






(18) Cuối cùng, trong thư mục đã chỉ định, **Setup Manager** sẽ tạo ra ba tập tin. Nếu bạn không thay đổi tên thì các tập tin là:

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

**Unattend.txt**: đây là tập tin trả lời, chứa tất cả các câu trả lời mà **Setup Manager** thu thập được.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

**Unattend.udb**: đây là tập tin cơ sở dữ liệu chứa tên các máy tính sẽ được cài đặt. Tập tin này chỉ được tạo ra khi bạn chỉ định danh sách các tập tin và được sử dụng khi bạn thực hiện cài đặt không cần theo dõi.

**Unattend.bat**: chứa dòng lệnh với các tham số được thiết lập sẵn. Tập tin này cũng thiết lập các biến môi trường chỉ định vị trí các tập tin liên quan.

## IV.4. Sử dụng tập tin trả lời

Có nhiều cách để sử dụng các tập tin được tạo ra trong bước trên. Bạn có thể thực hiện theo một trong hai cách dưới đây:

### IV.4.1 Sử dụng đĩa CD Windows 2003 Server có thể khởi động được

Sửa tập tin **Unattend.txt** thành **WINNT.SIF** và lưu lên đĩa mềm.

Đưa đĩa CD **Windows 2000 Server** và đĩa mềm trên vào ổ đĩa, khởi động lại máy tính, đảm bảo ổ đĩa CD là thiết bị khởi động đầu tiên. Chương trình cài đặt trên đĩa CD sẽ tự động tìm đọc tập tin **WINNT.SIF** trên đĩa mềm và tiến hành cài đặt không cần theo dõi.

### IV.4.2 Sử dụng một bộ nguồn cài đặt Windows 2003 Server

Chép các tập tin đã tạo trong bước trên vào thư mục **I386** của nguồn cài đặt **Windows 2003 Server**.

Chuyển vào thư mục **I386**.

Tuỳ theo hệ điều hành đang sử dụng mà sử dụng lệnh **WINNT.EXE** hoặc **WINNT32.EXE** theo cú pháp sau:

```
WINNT /s:e:\i386 /u:unattend.txt
```

hoặc

```
WINNT32 /s:e:\i386 /unattend:unattend.txt
```

Nếu chương trình **Setup Manager** tạo ra tập tin **Unatend.UDB** do bạn đã nhập vào danh sách tên các máy tính, và giả định bạn định đặt tên máy tính này là **server01** thì cú pháp lệnh sẽ như sau:

```
WINNT /s:e:\i386 /u:unattend.txt /udf:server01,unattend.udf
```



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

# Tóm tắt

Lý thuyết 4 tiết - Thực hành 8 tiết

| Mục tiêu | Các mục chính | Bài tập bắt buộc | Bài tập làm thêm |
|---|---|---|---|
| Kết thúc bài học này cung cấp học viên kiến thức về hệ thống Active Directory trên Windows Server 2003, cách tổ chức, nâng cấp để tạo thành Domain Controller … | I. Các mô hình mạng trong môi trường Microsoft.<br>II. Active Directory.<br>III. Cài đặt và cấu hình Active Directory. | Dựa vào bài tập môn Quản trị Windows Server 2003. | Dựa vào bài tập môn Quản trị Windows Server 2003. |



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

# I. CÁC MÔ HÌNH MẠNG TRONG MÔI TRƯỜNG MICROSOFT.

## I.1. Mô hình Workgroup.

Mô hình mạng **workgroup** còn gọi là mô hình mạng **peer-to-peer**, là mô hình mà trong đó các máy tính có vai trò như nhau được nối kết với nhau. Các dữ liệu và tài nguyên được lưu trữ phân tán tại các máy cục bộ, các máy tự quản lý tài nguyên cục bộ của mình. Trong hệ thống mạng không có máy tính chuyên cung cấp dịch vụ và quản lý hệ thống mạng. Mô hình này chỉ phù hợp với các mạng nhỏ, dưới mười máy tính và yêu cầu bảo mật không cao.

Đồng thời trong mô hình mạng này các máy tính sử dụng hệ điều hành hỗ trợ đa người dùng lưu trữ thông tin người dùng trong một tập tin **SAM (Security Accounts Manager)** ngay chính trên máy tính cục bộ. Thông tin này bao gồm: **username** (tên đăng nhập), **fullname**, **password**, **description**… Tất nhiên tập tin **SAM** này được mã hóa nhằm tránh người dùng khác ăn cấp mật khẩu để tấn công vào máy tính. Do thông tin người dùng được lưu trữ cục bộ trên các máy trạm nên việc chứng thực người dùng đăng nhập máy tính cũng do các máy tính này tự chứng thực.

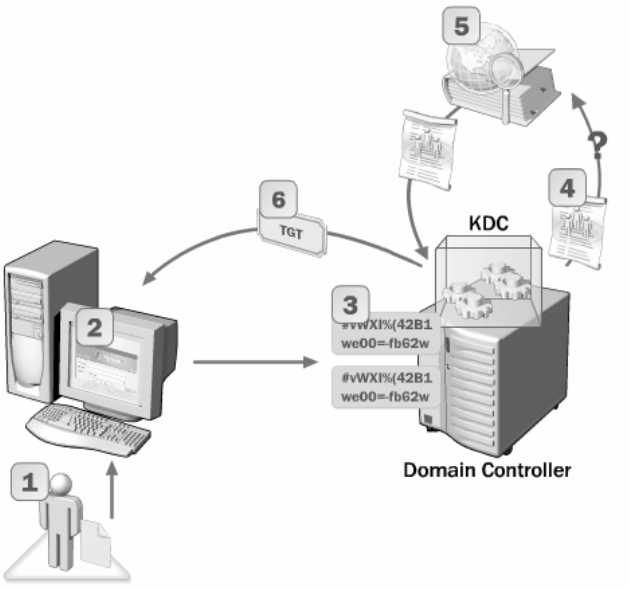
## I.2. Mô hình Domain.

Khác với mô hình **Workgroup**, mô hình **Domain** hoạt động theo cơ chế **client-server**, trong hệ thống mạng phải có ít nhất một máy tính làm chức năng điều khiển vùng (**Domain Controller**), máy tính này sẽ điều khiển toàn bộ hoạt động của hệ thống mạng. Việc chứng thực người dùng và quản lý tài nguyên mạng được tập trung lại tại các **Server** trong miền. Mô hình này được áp dụng cho các công ty vừa và lớn.

Trong mô hình **Domain** của **Windows Server 2003** thì các thông tin người dùng được tập trung lại do dịch vụ **Active Directory** quản lý và được lưu trữ trên máy tính điều khiển vùng (**domain controller**) với tên tập tin là **NTDS.DIT**. Tập tin cơ sở dữ liệu này được xây dựng theo công nghệ tương tự như phần mềm **Access** của **Microsoft** nên nó có thể lưu trữ hàng triệu người dùng, cải tiến hơn so với công nghệ cũ chỉ lưu trữ được khoảng 5 nghìn tài khoản người dùng. Do các thông tin người dùng được lưu trữ tập trung nên việc chứng thực người dùng đăng nhập vào mạng cũng tập trung và do máy điều khiển vùng chứng thực.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 2.1: các bước chứng thực khi người dùng đăng nhập.

# II. ACTIVE DIRECTORY.

## II.1. Giới thiệu Active Directory.

Có thể so sánh **Active Directory** với **LANManager** trên **Windows NT 4.0**. Về căn bản, **Active Directory** là một cơ sở dữ liệu của các tài nguyên trên mạng (còn gọi là đối tượng) cũng như các thông tin liên quan đến các đối tượng đó. Tuy vậy, **Active Directory** không phải là một khái niệm mới bởi **Novell** đã sử dụng dịch vụ thư mục (**directory service**) trong nhiều năm rồi.

Mặc dù **Windows NT 4.0** là một hệ điều hành mạng khá tốt, nhưng hệ điều hành này lại không thích hợp trong các hệ thống mạng tầm cỡ xí nghiệp. Đối với các hệ thống mạng nhỏ, công cụ **Network Neighborhood** khá tiện dụng, nhưng khi dùng trong hệ thống mạng lớn, việc duyệt và tìm kiếm trên mạng sẽ là một ác mộng (và càng tệ hơn nếu bạn không biết chính xác tên của máy in hoặc **Server** đó là gì). Hơn nữa, để có thể quản lý được hệ thống mạng lớn như vậy, bạn thường phải phân chia thành nhiều domain và thiết lập các mối quan hệ uỷ quyền thích hợp. **Active Directory** giải quyết được các vấn đề như vậy và cung cấp một mức độ ứng dụng mới cho môi trường xí nghiệp. Lúc này, dịch vụ thư mục trong mỗi **domain** có thể lưu trữ hơn mười triệu đối tượng, đủ để phục vụ mười triệu người dùng trong mỗi **domain**.

## II.2. Chức năng của Active Directory.

- Lưu giữ một danh sách tập trung các tên tài khoản người dùng, mật khẩu tương ứng và các tài khoản máy tính.
- Cung cấp một **Server** đóng vai trò chứng thực (**authentication server**) hoặc **Server** quản lý đăng nhập (**logon Server**), **Server** này còn gọi là **domain controller** (máy điều khiển vùng).
- Duy trì một bảng hướng dẫn hoặc một bảng chỉ mục (**index**) giúp các máy tính trong mạng có thể dò tìm nhanh một tài nguyên nào đó trên các máy tính khác trong vùng.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

- Cho phép chúng ta tạo ra những tài khoản người dùng với những mức độ quyền (**rights**) khác nhau như: toàn quyền trên hệ thống mạng, chỉ có quyền **backup** dữ liệu hay **shutdown Server** từ xa…
- Cho phép chúng ta chia nhỏ miền của mình ra thành các miền con (**subdomain**) hay các đơn vị tổ chức **OU** (**Organizational Unit**). Sau đó chúng ta có thể ủy quyền cho các quản trị viên bộ phận quản lý từng bộ phận nhỏ.

## II.3. Directory Services.

### II.3.1 Giới thiệu Directory Services.

**Directory Services** (dịch vụ danh bạ) là hệ thống thông tin chứa trong **NTDS.DIT** và các chương trình quản lý, khai thác tập tin này. Dịch vụ danh bạ là một dịch vụ cơ sở làm nền tảng để hình thành một hệ thống **Active Directory**. Một hệ thống với những tính năng vượt trội của **Microsoft**.

### II.3.2 Các thành phần trong Directory Services.

Đầu tiên, bạn phải biết được những thành phần cấu tạo nên dịch vụ danh bạ là gì? Bạn có thể so sánh dịch vụ danh bạ với một quyển sổ lưu số điện thoại. Cả hai đều chứa danh sách của nhiều đối tượng khác nhau cũng như các thông tin và thuộc tính liên quan đến các đối tượng đó.

a. **Object** (đối tượng).

Trong hệ thống cơ sở dữ liệu, đối tượng bao gồm các máy in, người dùng mạng, các server, các máy trạm, các thư mục dùng chung, dịch vụ mạng, … Đối tượng chính là thành tố căn bản nhất của dịch vụ danh bạ.

b. **Attribute** (thuộc tính).

Một thuộc tính mô tả một đối tượng. Ví dụ, mật khẩu và tên là thuộc tính của đối tượng người dùng mạng. Các đối tượng khác nhau có danh sách thuộc tính khác nhau, tuy nhiên, các đối tượng khác nhau cũng có thể có một số thuộc tính giống nhau. Lấy ví dụ như một máy in và một máy trạm cả hai đều có một thuộc tính là địa chỉ **IP**.

c. **Schema** (cấu trúc tổ chức).

Một **schema** định nghĩa danh sách các thuộc tính dùng để mô tả một loại đối tượng nào đó. Ví dụ, cho rằng tất cả các đối tượng máy in đều được định nghĩa bằng các thuộc tính tên, loại **PDL** và tốc độ. Danh sách các đối tượng này hình thành nên **schema** cho lớp đối tượng "máy in". **Schema** có đặc tính là tuỳ biến được, nghĩa là các thuộc tính dùng để định nghĩa một lớp đối tượng có thể sửa đổi được. Nói tóm lại **Schema** có thể xem là một danh bạ của cái danh bạ **Active Directory**.

d. **Container** (vật chứa).

Vật chứa tương tự với khái niệm thư mục trong **Windows**. Một thư mục có thể chứa các tập tin và các thư mục khác. Trong **Active Directory**, một vật chứa có thể chứa các đối tượng và các vật chứa khác. Vật chứa cũng có các thuộc tính như đối tượng mặc dù vật chứa không thể hiện một thực thể thật sự nào đó như đối tượng. Có ba loại vật chứa là:



- **Domain**: khái niệm này được trình bày chi tiết ở phần sau.
- **Site**: một **site** là một vị trí. **Site** được dùng để phân biệt giữa các vị trí cục bộ và các vị trí xa xôi. Ví dụ, công ty XYZ có tổng hành dinh đặt ở **San Fransisco**, một chi nhánh đặt ở **Denver** và một văn

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

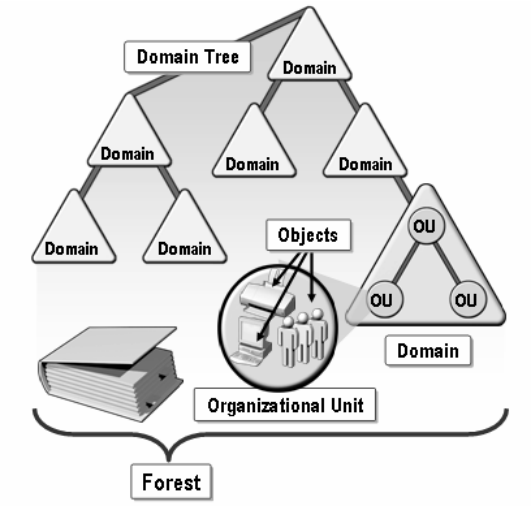
phòng đại diện đặt ở **Portland** kết nối về tổng hành dinh bằng **Dialup Networking**. Như vậy hệ thống mạng này có ba **site**.

- **OU (Organizational Unit):** là một loại vật chứa mà bạn có thể đưa vào đó người dùng, nhóm, máy tính và những **OU** khác. Một **OU** không thể chứa các đối tượng nằm trong domain khác. Nhờ việc một **OU** có thể chứa các **OU** khác, bạn có thể xây dựng một mô hình thứ bậc của các vật chứa để mô hình hoá cấu trúc của một tổ chức bên trong một domain. Bạn nên sử dụng **OU** để giảm thiểu số lượng domain cần phải thiết lập trên hệ thống.

**e. Global Catalog.**

- Dịch vụ **Global Catalog** dùng để xác định vị trí của một đối tượng mà người dùng được cấp quyền truy cập. Việc tìm kiếm được thực hiện xa hơn những gì đã có trong **Windows NT** và không chỉ có thể định vị được đối tượng bằng tên mà có thể bằng cả những thuộc tính của đối tượng.
- Giả sử bạn phải in một tài liệu dày 50 trang thành 1000 bản, chắc chắn bạn sẽ không dùng một máy in **HP Laserjet 4L**. Bạn sẽ phải tìm một máy in chuyên dụng, in với tốc độ 100ppm và có khả năng đóng tài liệu thành quyển. Nhờ **Global Catalog**, bạn tìm kiếm trên mạng một máy in với các thuộc tính như vậy và tìm thấy được một máy **Xerox Docutech 6135**. Bạn có thể cài đặt **driver** cho máy in đó và gửi **print job** đến máy in. Nhưng nếu bạn ở **Portland** và máy in thì ở **Seattle** thì sao? **Global Catalog** sẽ cung cấp thông tin này và bạn có thể gửi **email** cho chủ nhân của máy in, nhờ họ in giùm.
- Một ví dụ khác, giả sử bạn nhận được một thư thoại từ một người tên **Betty Doe** ở bộ phận kế toán. Đoạn thư thoại của cô ta bị cắt xén và bạn không thể biết được số điện thoại của cô ta. Bạn có thể dùng **Global Catalog** để tìm thông tin về cô ta nhờ tên, và nhờ đó bạn có được số điện thoại của cô ta.
- Khi một đối tượng được tạo mới trong **Active Directory**, đối tượng được gán một con số phân biệt gọi là **GUID** (**Global Unique Identifier**). **GUID** của một đối tượng luôn luôn cố định cho dù bạn có di chuyển đối tượng đi đến khu vực khác.

## II.4. Kiến trúc của Active Directory.



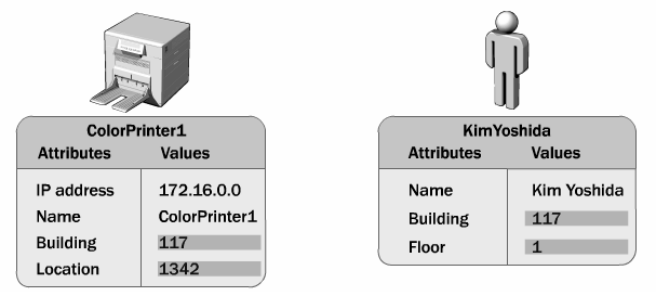

Hình 2.2: kiến trúc của **Active Directory**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

### II.4.1 Objects.

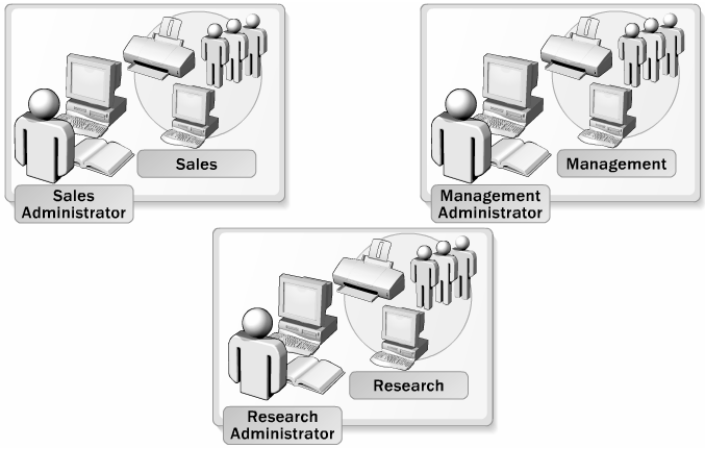
Trước khi tìm hiểu khái niệm **Object**, chúng ta phải tìm hiểu trước hai khái niệm **Object classes và Attributes**. **Object classes** là một bản thiết kế mẫu hay một khuôn mẫu cho các loại đối tượng mà bạn có thể tạo ra trong **Active Directory**. Có ba loại **object classes** thông dụng là: **User, Computer, Printer**. Khái niệm thứ hai là **Attributes**, nó được định nghĩa là tập các giá trị phù hợp và được kết hợp với một đối tượng cụ thể. Như vậy **Object** là một đối tượng duy nhất được định nghĩa bởi các giá trị được gán cho các thuộc tính của object **classes**. Ví dụ hình sau minh họa hai đối tượng là: máy in **ColorPrinter1** và người dùng **KimYoshida**.




### II.4.2 Organizational Units.

**Organizational Unit** hay **OU** là đơn vị nhỏ nhất trong hệ thống **AD**, nó được xem là một vật chứa các đối tượng (**Object**) được dùng để sắp xếp các đối tượng khác nhau phục vụ cho mục đích quản trị của bạn. **OU** cũng được thiết lập dựa trên **subnet IP** và được định nghĩa là "một hoặc nhiều **subnet** kết nối tốt với nhau". Việc sử dụng **OU** có hai công dụng chính sau:

- Trao quyền kiểm soát một tập hợp các tài khoản người dùng, máy tính hay các thiết bị mạng cho một nhóm người hay một phụ tá quản trị viên nào đó (sub-administrator), từ đó giảm bớt công tác quản trị cho người quản trị toàn bộ hệ thống.
- Kiểm soát và khóa bớt một số chức năng trên các máy trạm của người dùng trong OU thông qua việc sử dụng các đối tượng chính sách nhóm (**GPO**), các chính sách nhóm này chúng ta sẽ tìm hiểu ở các chương sau.



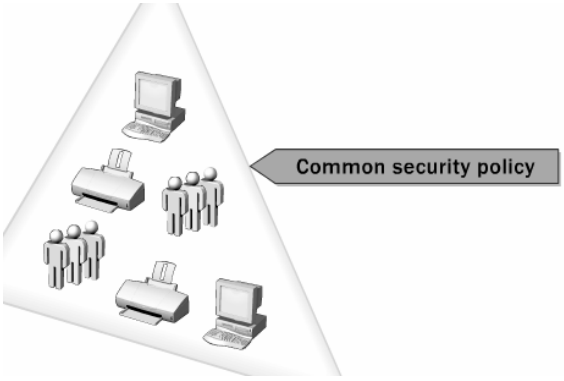



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

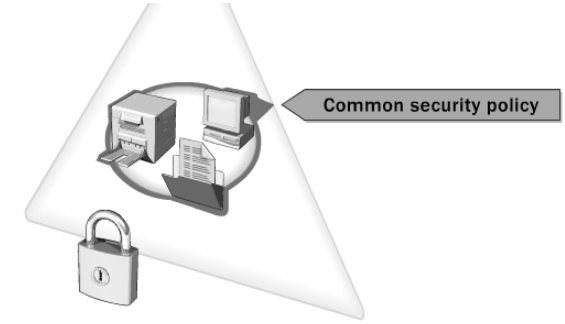
### II.4.3 Domain.

**Domain** là đơn vị chức năng nòng cốt của cấu trúc **logic Active Directory**. Nó là phương tiện để qui định một tập hợp những người dùng, máy tính, tài nguyên chia sẻ có những qui tắc bảo mật giống nhau từ đó giúp cho việc quản lý các truy cập vào các **Server** dễ dàng hơn. **Domain** đáp ứng ba chức năng chính sau:

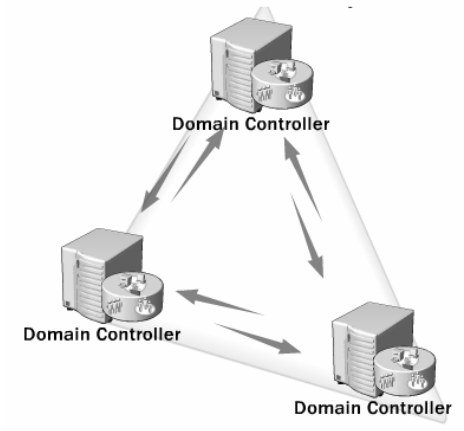
- Đóng vai trò như một khu vực quản trị (**administrative boundary**) các đối tượng, là một tập hợp các định nghĩa quản trị cho các đối tượng chia sẻ như: có chung một cơ sở dữ liệu thư mục, các chính sách bảo mật, các quan hệ ủy quyền với các **domain** khác.




- Giúp chúng ta quản lý bảo mật các các tài nguyên chia sẻ.




- Cung cấp các **Server** dự phòng làm chức năng điều khiển vùng (**domain controller**), đồng thời đảm bảo các thông tin trên các **Server** này được được đồng bộ với nhau.

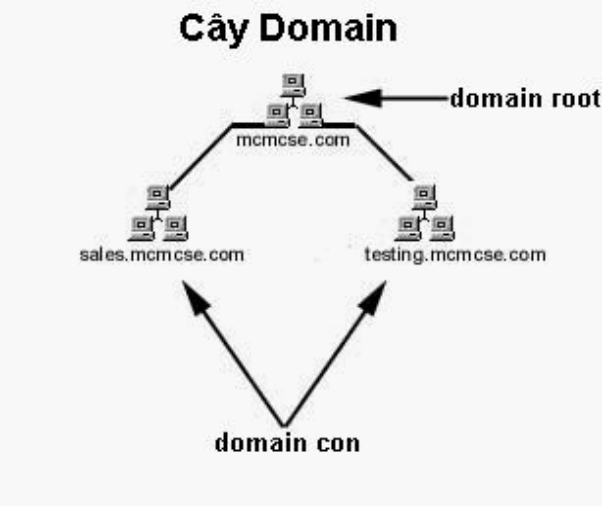





Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

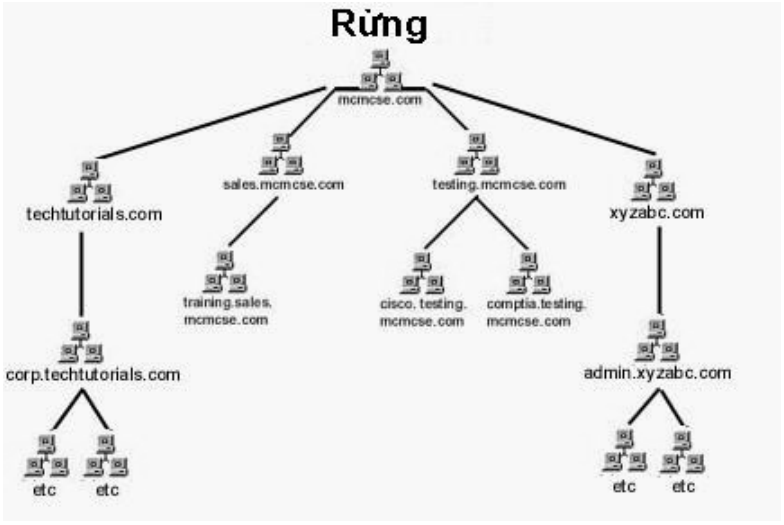
### II.4.4 Domain Tree.

**Domain Tree** là cấu trúc bao gồm nhiều **domain** được sắp xếp có cấp bậc theo cấu trúc hình cây. **Domain** tạo ra đầu tiên được gọi là **domain root** và nằm ở gốc của cây thư mục. Tất cả các **domain** tạo ra sau sẽ nằm bên dưới **domain root** và được gọi là **domain** con (**child domain**). Tên của các **domain** con phải khác biệt nhau. Khi một **domain root** và ít nhất một **domain** con được tạo ra thì hình thành một cây **domain**. Khái niệm này bạn sẽ thường nghe thấy khi làm việc với một dịch vụ thư mục. Bạn có thể thấy cấu trúc sẽ có hình dáng của một cây khi có nhiều nhánh xuất hiện.




### II.4.5 Forest.

**Forest** (rừng) được xây dựng trên một hoặc nhiều **Domain Tree**, nói cách khác **Forest** là tập hợp các **Domain Tree** có thiết lập quan hệ và ủy quyền cho nhau. Ví dụ giả sử một công ty nào đó, chẳng hạn như **Microsoft**, thu mua một công ty khác. Thông thường, mỗi công ty đều có một hệ thống **Domain Tree** riêng và để tiện quản lý, các cây này sẽ được hợp nhất với nhau bằng một khái niệm là rừng.






Trong ví dụ trên, công ty mcmcse.com thu mua được techtutorials.com và xyzabc.com và hình thành rừng từ gốc mcmcse.com.

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

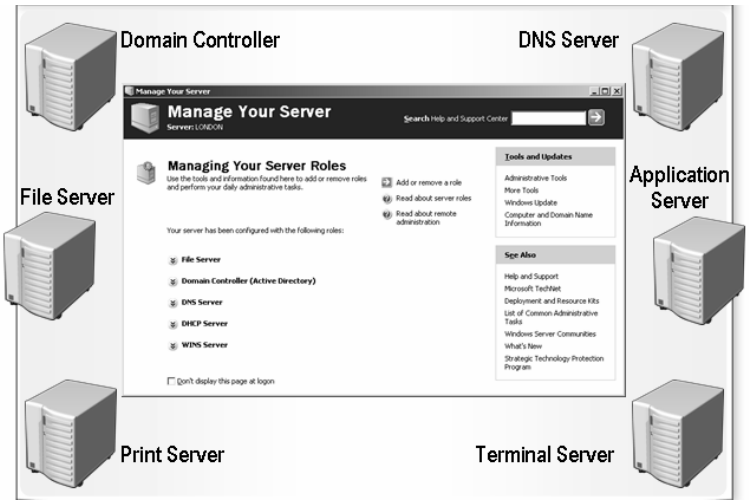
# III. CÀI ĐẶT VÀ CẤU HÌNH ACTIVE DIRECTORY.

## III.1. Nâng cấp Server thành Domain Controller.

### III.1.1 Giới thiệu.

Một khái niệm không thay đổi từ **Windows NT 4.0** là **domain**. Một **domain** vẫn còn là trung tâm của mạng **Windows 2000** và **Windows 2003**, tuy nhiên lại được thiết lập khác đi. Các máy điều khiển vùng (**domain controller – DC**) không còn phân biệt là **PDC (Primary Domain Controller)** hoặc là **BDC (Backup Domain Controller)**. Bây giờ, đơn giản chỉ còn là **DC**. Theo mặc định, tất cả các máy **Windows Server 2003** khi mới cài đặt đều là **Server** độc lập (**standalone server**). Chương trình **DCPROMO** chính là **Active Directory Installation Wizard** và được dùng để nâng cấp một máy không phải là **DC** (**Server Stand-alone**) thành một máy **DC** và ngược lại giáng cấp một máy **DC** thành một **Server** bình thường. Chú ý đối với **Windows Server 2003** thì bạn có thể đổi tên máy tính khi đã nâng cấp thành **DC**.

Trước khi nâng cấp **Server** thành **Domain Controller**, bạn cần khai báo đầy đủ các thông số **TCP/IP**, đặc biệt là phải khai báo **DNS Server** có địa chỉ chính là địa chỉ IP của **Server** cần nâng cấp. Nếu bạn có khả năng cấu hình dịch vụ **DNS** thì bạn nên cài đặt dịch vụ này trước khi nâng cấp **Server**, còn ngược lại thì bạn chọn cài đặt **DNS** tự động trong quá trình nâng cấp. Có hai cách để bạn chạy chương trình **Active Directory Installation Wizard**: bạn dùng tiện ích **Manage Your Server** trong **Administrative Tools** hoặc nhấp chuột vào **Start** ◴ **Run**, gõ lệnh **DCPROMO**.




### III.1.2 Các bước cài đặt.

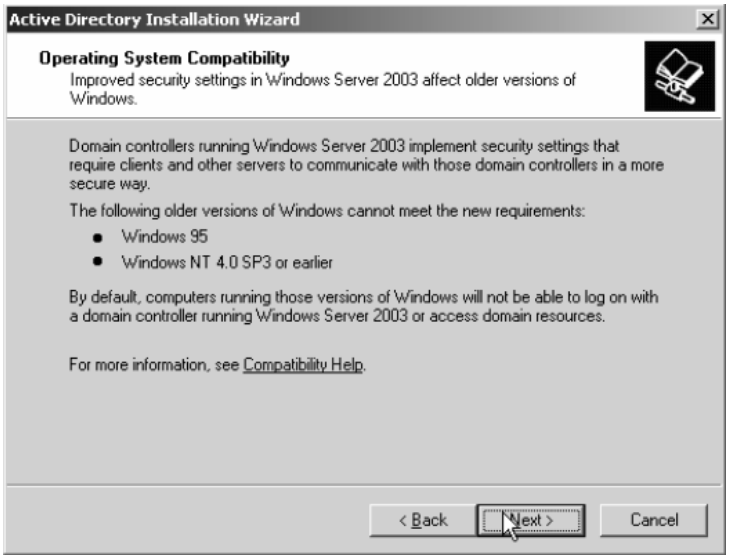
Chọn menu **Start** ◴ **Run**, nhập **DCPROMO** trong hộp thoại **Run**, và nhấn nút **OK**.

Khi đó hộp thoại **Active Directory Installation Wizard** xuất hiện. Bạn nhấn **Next** để tiếp tục.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

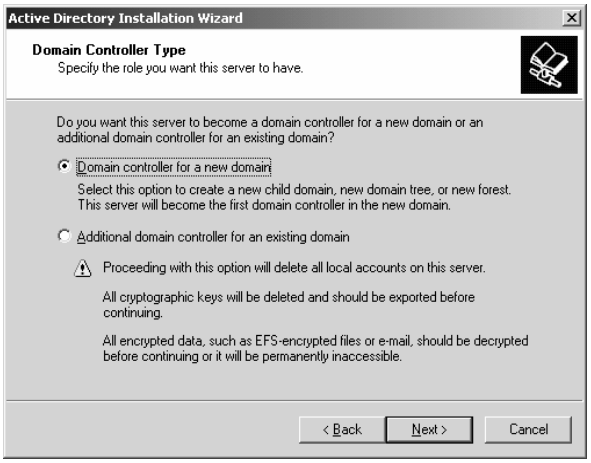

Chương trình xuất hiện hộp thoại cảnh báo: **DOS, Windows 95** và **WinNT SP3** trở về trước sẽ bị loại ra khỏi miền **Active Directory** dựa trên **Windows Server 2003**. Bạn chọn **Next** để tiếp tục.



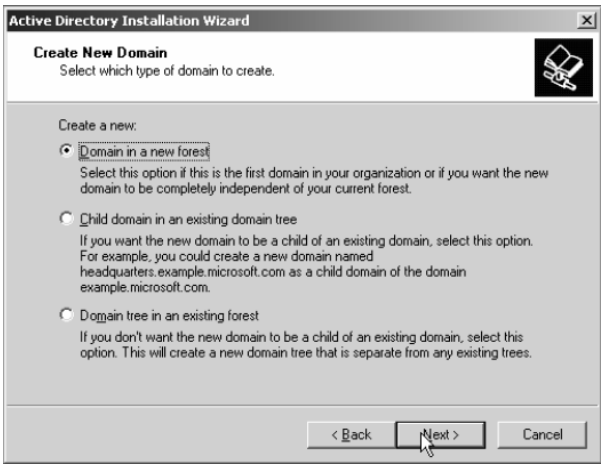

Trong hộp thoại **Domain Controller Type**, chọn mục **Domain Controller for a New Domain** và nhấn chọn **Next**. (Nếu bạn muốn bổ sung máy điều khiển vùng vào một **domain** có sẵn, bạn sẽ chọn **Additional domain cotroller for an existing domain**.)



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net



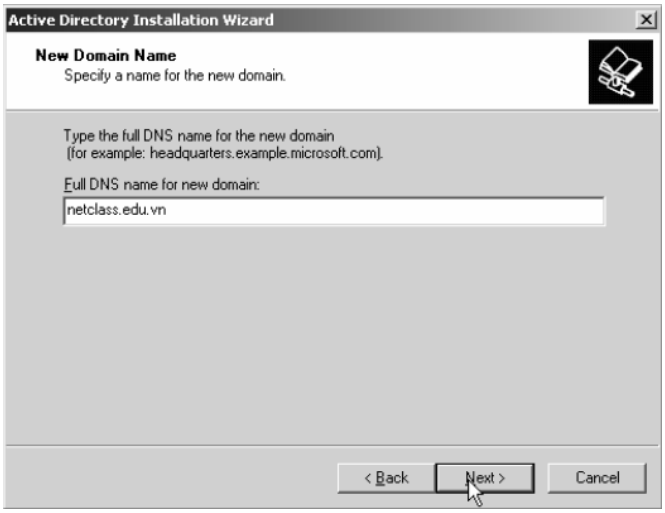

Đến đây chương trình cho phép bạn chọn một trong ba lựa chọn sau: chọn **Domain in new forest** nếu bạn muốn tạo **domain** đầu tiên trong một rừng mới, chọn **Child domain in an existing domain tree** nếu bạn muốn tạo ra một **domain** con dựa trên một cây **domain** có sẵn, chọn **Domain tree in an existing forest** nếu bạn muốn tạo ra một cây **domain** mới trong một rừng đã có sẵn.



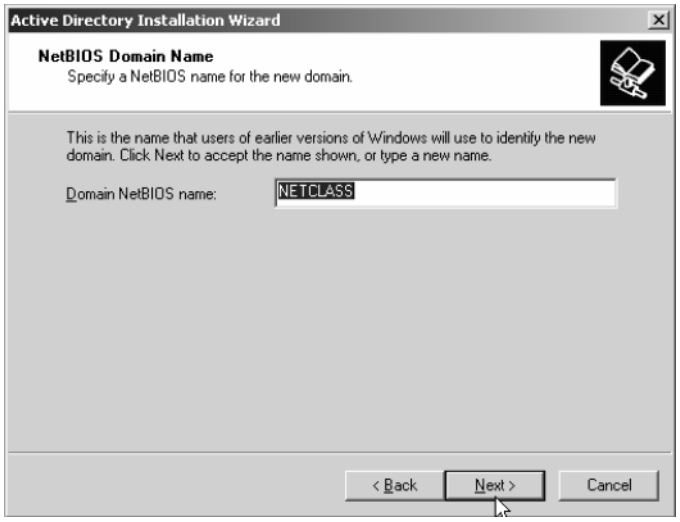

Hộp thoại **New Domain Name** yêu cầu bạn tên **DNS** đầy đủ của **domain** mà bạn cần xây dựng.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net



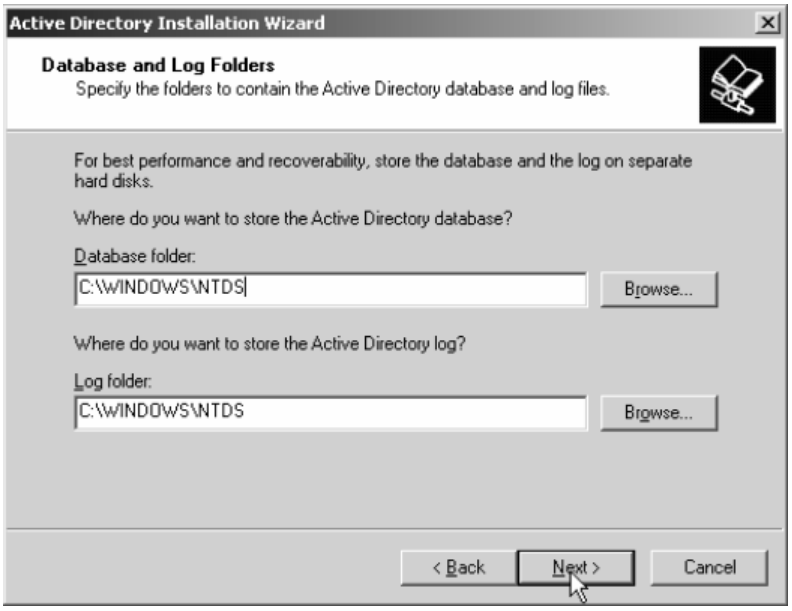

Hộp thoại **NetBIOS Domain Name**, yêu cầu bạn cho biết tên **domain** theo chuẩn **NetBIOS** để tương thích với các máy **Windows NT**. Theo mặc định, tên **Domain NetBIOS** giống phần đầu của tên **Full DNS**, bạn có thể đổi sang tên khác hoặc chấp nhận giá trị mặc định. Chọn **Next** để tiếp tục.



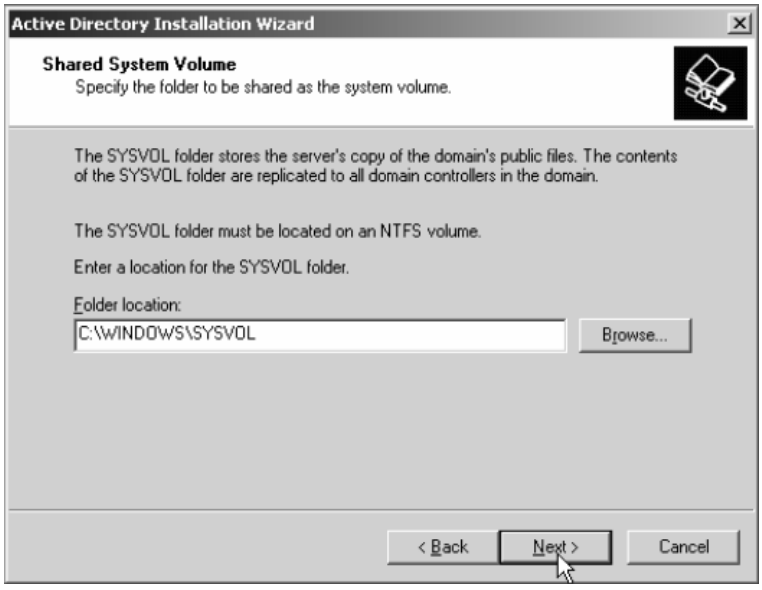

Hộp thoại **Database and Log Locations** cho phép bạn chỉ định vị trí lưu trữ **database Active Directory** và các tập tin **log**. Bạn có thể chỉ định vị trí khác hoặc chấp nhận giá trị mặc định. Tuy nhiên theo khuyến cáo của các nhà quản trị mạng thì chúng ta nên đặt tập tin chứa thông tin giao dịch (**transaction log**) ở một đĩa cứng vật lý khác với đĩa cứng chứa cơ sở dữ liệu của **Active Directory** nhằm tăng hiệu năng của hệ thống. Bạn chọn **Next** để tiếp tục.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net



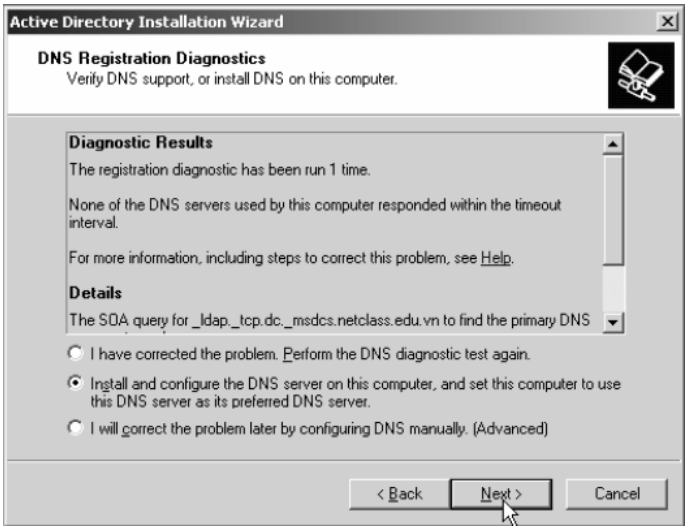

Hộp thoại **Shared System Volume** cho phép bạn chỉ định ví trí của thư mục **SYSVOL**. Thư mục này phải nằm trên một **NTFS5 Volume**. Tất cả dữ liệu đặt trong thư mục **Sysvol** này sẽ được tự động sao chép sang các **Domain Controller** khác trong miền. Bạn có thể chấp nhận giá trị mặc định hoặc chỉ định ví trí khác, sau đó chọn **Next** tiếp tục. (Nếu **partition** không sử dụng định dạng **NTFS5**, bạn sẽ thấy một thông báo lỗi yêu cầu phải đổi hệ thống tập tin).



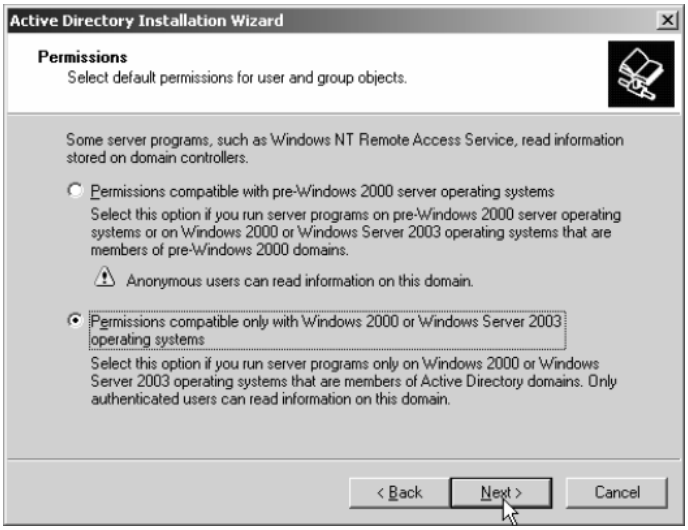

**DNS** là dịch vụ phân giải tên kết hợp với **Active Directory** để phân giải tên các máy tính trong miền. Do đó để hệ thống **Active Directory** hoạt động được thì trong miền phải có ít nhất một **DNS Server** phân giải miền mà chúng ta cần thiết lập. Theo đúng lý thuyết thì chúng ta phải cài đặt và cấu hình dịch vụ **DNS** hoàn chỉnh trước khi nâng cấp **Server**, nhưng do hiện tại các bạn chưa học về dịch vụ này nên chúng ta chấp nhận cho hệ thống tự động cài đặt dịch vụ này. Chúng ta sẽ tìm hiểu chi tiết dịch vụ **DNS** ở giáo trình "Dịch Vụ Mạng". Trong hộp thoại xuất hiện bạn chọn lựa chọn thứ hai để hệ thống tự động cài đặt và cấu hình dịch vụ **DNS**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net



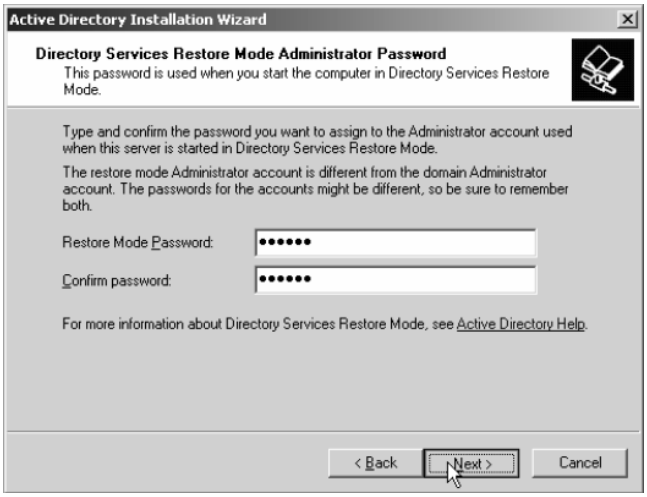

Trong hộp thoại **Permissions**, bạn chọn giá trị **Permission Compatible with pre-Windows 2000 servers** khi hệ thống có các **Server** phiên bản trước **Windows 2000**, hoặc chọn **Permissions compatible only with Windows 2000 servers** or **Windows Server 2003** khi hệ thống của bạn chỉ toàn các **Server Windows 2000** và **Windows Server 2003**.



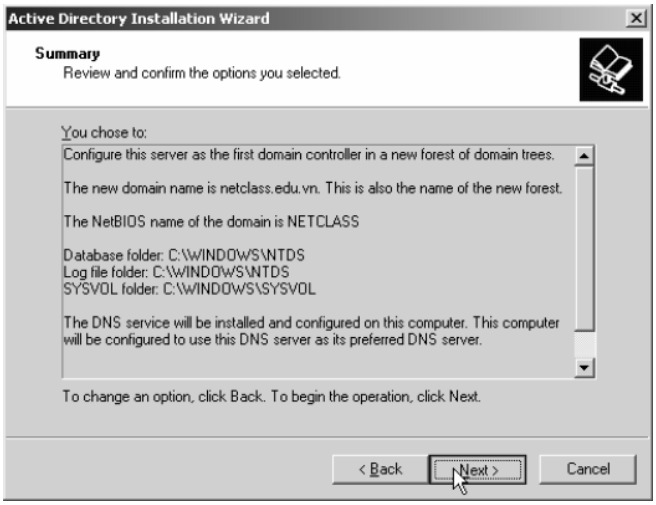

Trong hộp thoại **Directory Services Restore Mode Administrator Password**, bạn sẽ chỉ định mật khẩu dùng trong trường hợp **Server** phải khởi động vào chế độ **Directory Services Restore Mode**. Nhấn chọn **Next** để tiếp tục.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net



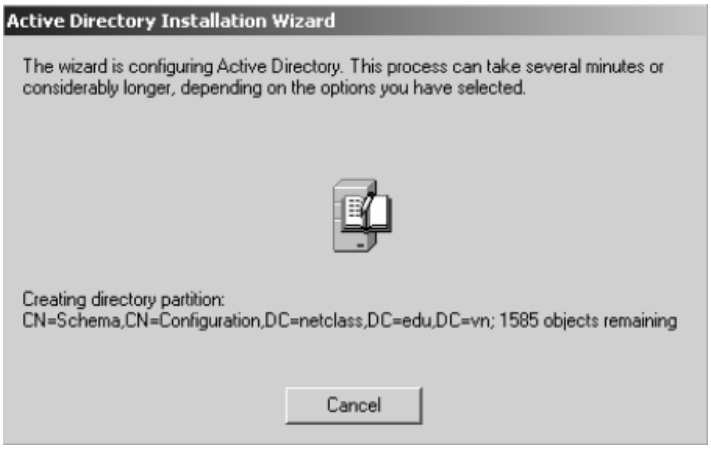

Hộp thoại **Summary** xuất hiện, trình bày tất cả các thông tin bạn đã chọn. Nếu tất cả đều chính xác, bạn nhấn **Next** để bắt đầu thực hiện quá trình cài đặt, nếu có thông tin không chính xác thì bạn chọn **Back** để quay lại các bước trước đó.




Hộp thoại **Configuring Active Directory** cho bạn biết quá trình cài đặt đang thực hiện những gì. Quá trình này sẽ chiếm nhiều thời gian. Chương trình cài đặt cũng yêu cầu bạn cung cấp nguồn cài đặt **Windows Server 2003** để tiến hành sao chép các tập tin nếu tìm không thấy.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Sau khi quá trình cài đặt kết thúc, hộp thoại **Completing the Active Directory Installation Wizard** xuất hiện. Bạn nhấn chọn **Finish** để kết thúc.


Cuối cùng, bạn được yêu cầu phải khởi động lại máy thì các thông tin cài đặt mới bắt đầu có hiệu lực. Bạn nhấn chọn nút **Restart Now** để khởi động lại. Quá trình thăng cấp kết thúc.

## III.2. Gia nhập máy trạm vào Domain.

### III.2.1 Giới thiệu.

Một máy trạm gia nhập vào một **domain** thực sự là việc tạo ra một mối quan hệ tin cậy (**trust relationship**) giữa máy trạm đó với các máy **Domain Controller** trong vùng. Sau khi đã thiết lập quan hệ tin cậy thì việc chứng thực người dùng **logon** vào mạng trên máy trạm này sẽ do các máy điều khiển vùng đảm nhiệm. Nhưng chú ý việc gia nhập một máy trạm vào miền phải có sự đồng ý của người quản trị mạng cấp miền và quản trị viên cục bộ trên máy trạm đó. Nói cách khác khi bạn muốn gia nhập một máy trạm vào miền, bạn phải đăng nhập cục bộ vào máy trạm với vai trò là **administrator**, sau đó gia nhập vào miền, hệ thống sẽ yêu cầu bạn xác thực bằng một tài khoản người dùng cấp miền có quyền **Add Workstation to Domain** (bạn có thể dùng trực tiếp tài khoản **administrator** cấp miền).



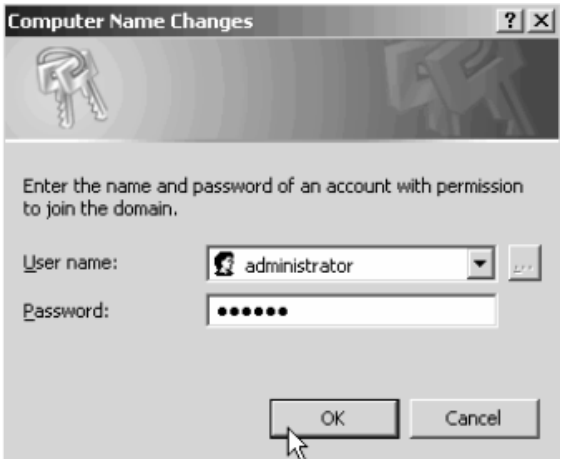
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

### III.2.2 Các bước cài đặt.

Đăng nhập cục bộ vào máy trạm với vai trò người quản trị (có thể dùng trực tiếp tài khoản **administrator**).

Nhấp phải chuột trên biểu tượng My Computer, chọn **Properties**, hộp thoại **System Properties** xuất hiện, trong **Tab Computer Name**, bạn nhấp chuột vào nút **Change**. Hộp thoại nhập liệu xuất hiện bạn nhập tên miền của mạng cần gia nhập vào mục **Member of Domain**.


Máy trạm dựa trên tên miền mà bạn đã khai báo để tìm đến **Domain Controller** gần nhất và xin gia nhập vào mạng, **Server** sẽ yêu cầu bạn xác thực với một tài khoản người dùng cấp miền có quyền quản trị.




Sau khi xác thực chính xác và hệ thống chấp nhận máy trạm này gia nhập vào miền thì hệ thống xuất hiện thông báo thành công và yêu cầu bạn **reboot** máy lại để đăng nhập vào mạng.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Đến đây, bạn thấy hộp thoại **Log on to Windows** mà bạn dùng mỗi ngày có vài điều khác, đó là xuất hiện thêm mục **Log on to**, và cho phép bạn chọn một trong hai phần là: **NETCLASS**, **This Computer**. Bạn chọn mục **NETCLASS** khi bạn muốn đăng nhập vào miền, nhớ rằng lúc này bạn phải dùng tài khoản người dùng cấp miền. Bạn chọn mục **This Computer** khi bạn muốn **logon** cục bộ vào máy trạm nào và nhớ dùng tài khoản cục bộ của máy.


## III.3. Xây dựng các Domain Controller đồng hành.

### III.3.1 Giới thiệu.

**Domain Controller** là máy tính điều khiển mọi hoạt động của mạng nếu máy này có sự cố thì toàn bộ hệ thống mạng bị tê liệt. Do tính năng quan trọng này nên trong một hệ thống mạng thông thường chúng ta phải xây dựng ít nhất hai máy tính **Domain Controller**. Như đã trình bày ở trên thì **Windows Server 2003** không còn phân biệt máy **Primary Domain Controller** và **Backup Domain Controller** nữa, mà nó xem hai máy này có vai trò ngang nhau, cùng nhau tham gia chứng thực người dùng. Như chúng ta đã biết, công việc chứng thực đăng nhập thường được thực hiện vào đầu giờ mỗi buổi làm việc, nếu mạng của bạn chỉ có một máy điều khiển dùng và 10.000 nhân viên thì chuyện gì sẽ xẩy ra vào mỗi buổi sáng? Để giải quyết trường hợp trên, **Microsoft** cho phép các máy điều khiển vùng trong mạng cùng nhau hoạt động đông thời, chia sẻ công việc của nhau, khi có một máy bị sự cố thì các máy còn lại đảm nhiệm luôn công việc máy này. Do đó trong tài liệu này chúng tôi gọi các máy này là các máy điều khiển vùng đồng hành. Nhưng khi khảo sát sâu về **Active Directory** thì máy điều khiển vùng được tạo đầu tiên vẫn có vai trò đặc biệt hơn đó là **FSMO (flexible single master of operations)**.

Chú ý để đảm bảo các máy điều khiển vùng này hoạt động chính xác thì chúng phải liên lạc và trao đổi thông tin với nhau khi có các thay đổi về thông tin người dùng như: tạo mới tài khoản, đổi mật khẩu, xóa tài khoản. Việc trao đổi thông tin này gọi là **Active Directory Replication**. Đặc biệt các server **Active Directory** cho phép nén dữ liệu trước khi gởi đến các server khác, tỉ lệ nén đến **10:1**, đo đó chúng có thể truyền trên các đường truyền **WAN** chậm chạp.

Trong hệ thống mạng máy tính của chúng ta nếu tất cả các máy điều khiển vùng đều là **Windows Server 2003** thì chúng ta nên chuyển miền trong mạng này sang cấp độ hoạt động **Windows Server 2003** (**Windows Server 2003 functional level**) để khai thác hết các tính năng mới của **Active Directory**.



### III.3.2 Các bước cài đặt.

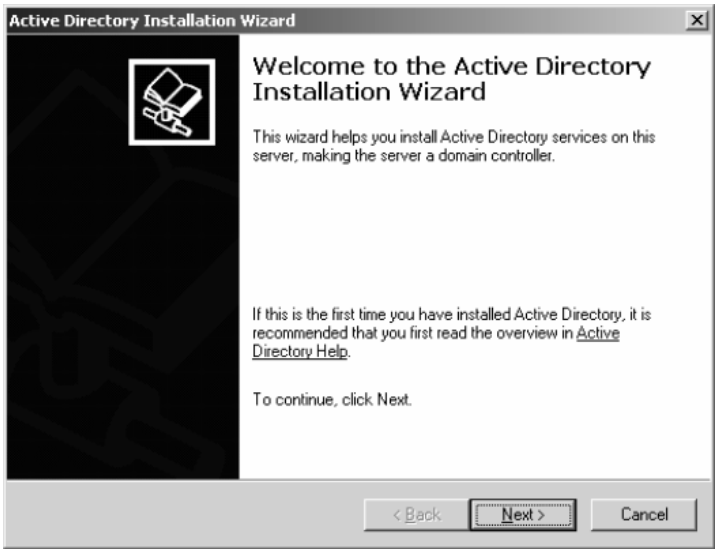
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Chọn menu **Start** 🕘 **Run**, nhập **DCPROMO** trong hộp thoại **Run**, và nhấn nút **OK**.

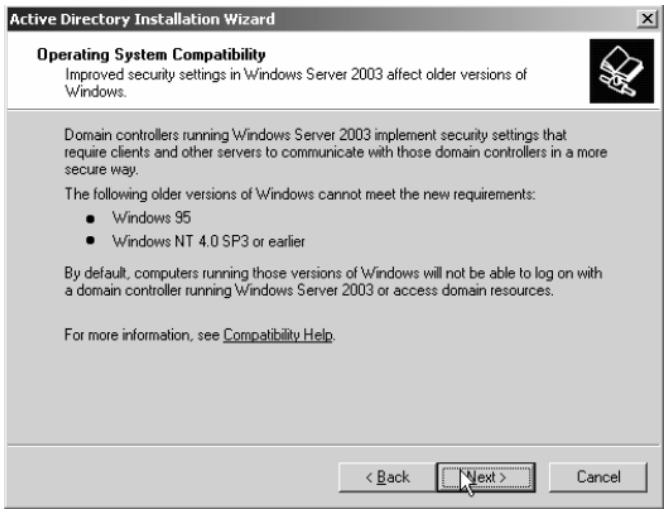


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Khi đó hộp thoại **Active Directory Installation Wizard** xuất hiện. Bạn nhấn **Next** để tiếp tục.



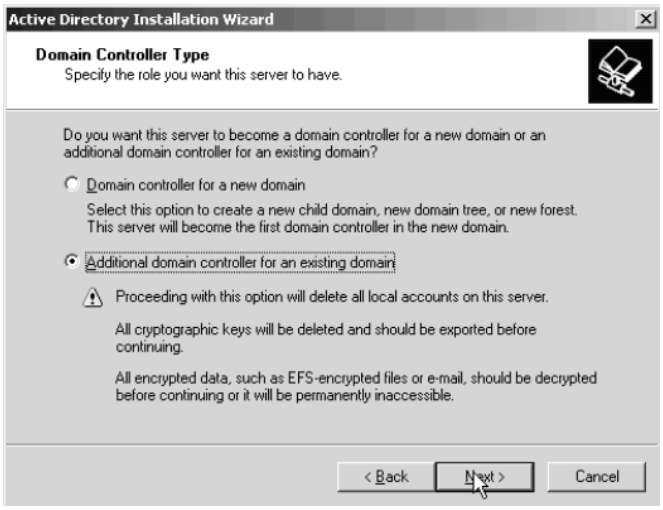

Chương trình xuất hiện hộp thoại cảnh báo: **DOS, Windows 95** và **WinNT SP3** trở về trước sẽ bị loại ra khỏi miền **Active Directory** dựa trên **Windows Server 2003**. Bạn chọn **Next** để tiếp tục.



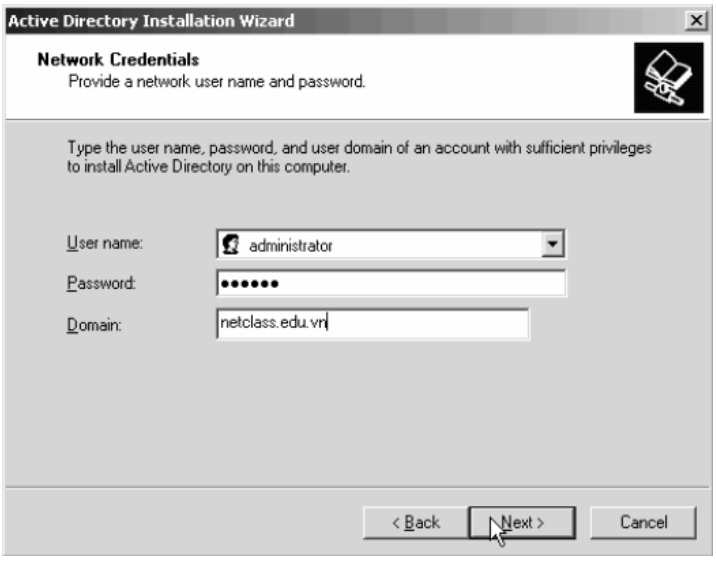

Trong hộp thoại **Domain Controller Type**, chọn mục **Additional domain cotroller for an existing domain** và nhấn chọn **Next**, vì chúng ta muốn bổ sung thêm máy điều khiển vùng vào một **domain** có sẵn.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net



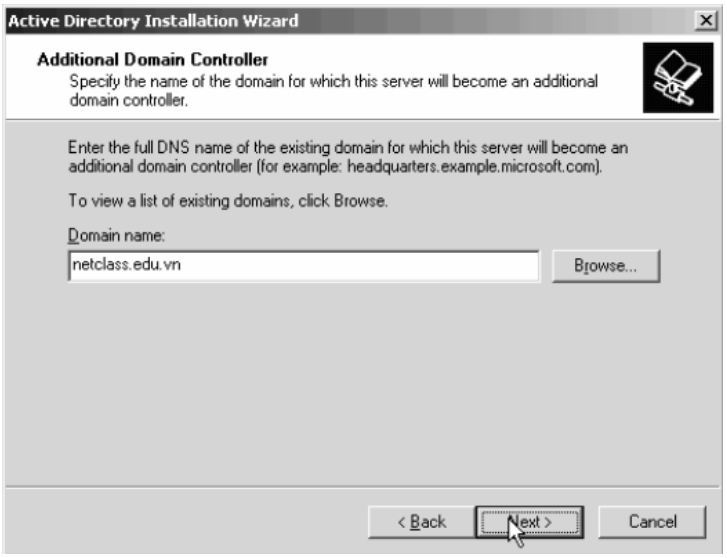

Tiếp theo hệ thống yêu cầu bạn xác thực bạn phải người quản trị cấp miền thì mới có quyền tạo các **Domain Controller**. Bạn nhập tài khoản người dùng có quyền quản trị vào hộp thoại này.




Chương trình yêu cầu bạn nhập **Full DNS Name** của miền mà bạn cần tạo thêm **Domain Controller**.

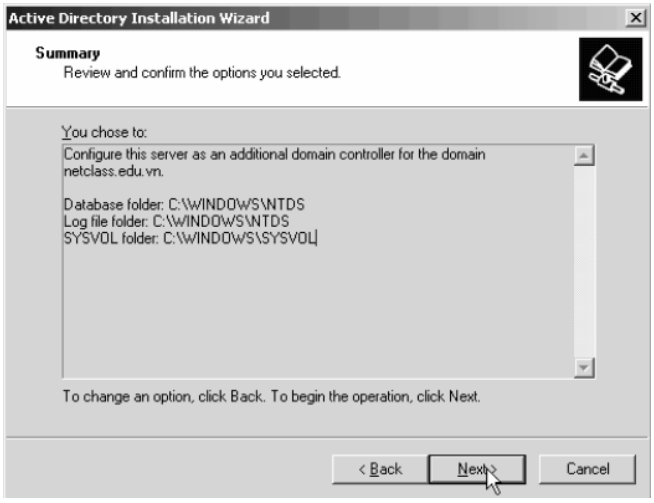


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Tương tự như quá trình nâng cấp **Server** thành **Domain Controller** đã trình bày ở trên, các bước tiếp theo chúng ta chỉ định thư mục chứa cơ sở dữ liệu của **Active Directory**, **Transaction Log** và thư mục **Sysvol**.

Hộp thoại **Summary** xuất hiện, trình bày tất cả các thông tin bạn đã chọn. Nếu tất cả đều chính xác, bạn nhấn **Next** để bắt đầu thực hiện quá trình cài đặt, nếu có thông tin không chính xác thì bạn chọn **Back** để quay lại các bước trước đó.

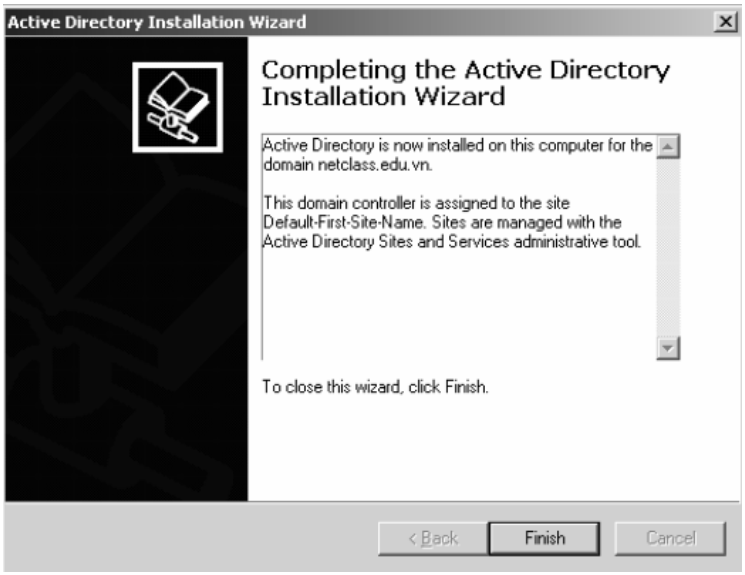



Đến đây hệ thống sẽ xây dựng một **Domain Controller** mới và đồng bộ dữ liệu **Active Directory** giữa hai **Domain Controller** này.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net


Sau khi quá trình cài đặt kết thúc, hộp thoại **Completing the Active Directory Installation Wizard** xuất hiện. Bạn nhấn chọn **Finish** để kết thúc.




Cuối cùng, bạn được yêu cầu phải khởi động lại máy thì các thông tin cài đặt mới bắt đầu có hiệu lực. Bạn nhấn chọn nút **Restart Now** để khởi động lại. Quá trình xây dựng thêm một **Domain Controller** đồng hành đã hoàn tất.

## III.4. Xây dựng Subdomain.

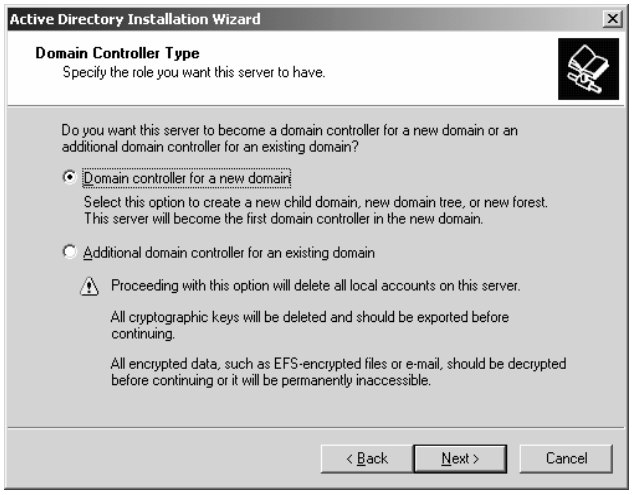
Sau khi bạn đã xây dựng **Domain Controller** đầu tiên quản lý miền, lúc ấy **Domain Controller** này là một gốc của rừng hoặc **Domain Tree** đầu tiên, từ đây bạn có thể tạo thêm các **subdomain** cho hệ thống. Để tạo thêm một **Domain Controller** cho một **subdomain** bạn làm các bước sau:

Tại **member server**, bạn cũng chạy chương trình **Active Directory Installation Wizard**, các bước đầu bạn cũng chọn tương tự như phần nâng cấp phía trên.

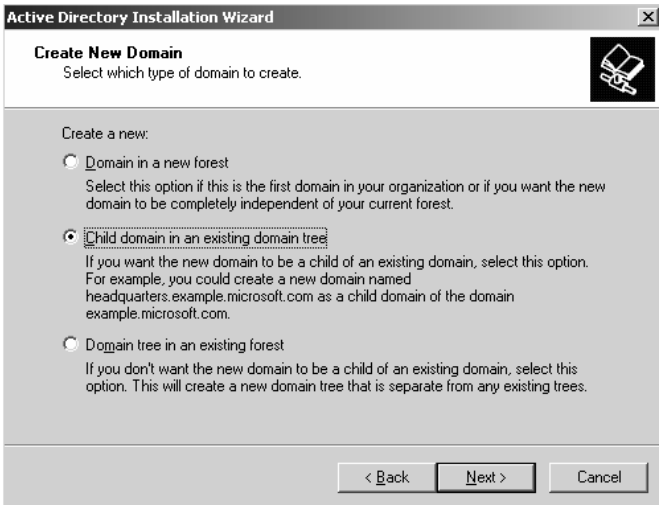


Trong hộp thoại **Domain Controller Type**, chọn mục **Domain Controller for a New Domain** và nhấn chọn **Next**. (Nếu bạn muốn bổ sung máy điều khiển vùng vào một **domain** có sẵn, bạn sẽ chọn **Additional domain cotroller for an existing domain**.)

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net



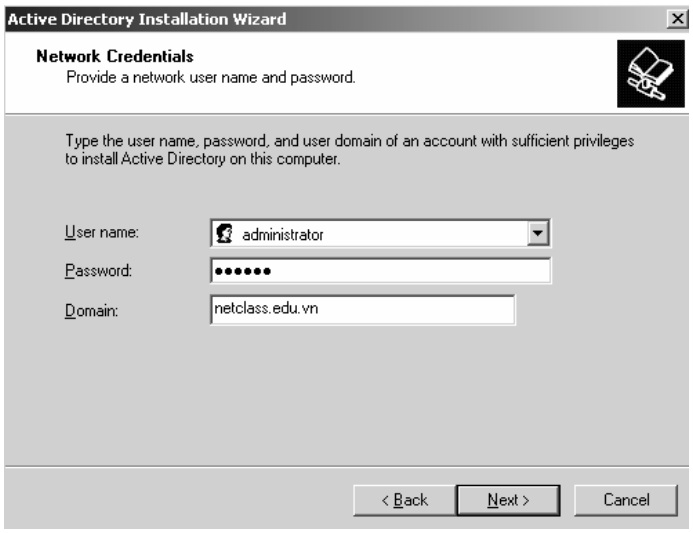

Đến đây chương trình cho phép bạn chọn một trong ba lựa chọn sau: chọn **Domain in new forest** nếu bạn muốn tạo domain đầu tiên trong một rừng mới, chọn **Child domain in an existing domain tree** nếu bạn muốn tạo ra một domain con dựa trên một cây **domain** có sẵn, chọn **Domain tree in an existing forest** nếu bạn muốn tạo ra một cây **domain** mới trong một rừng đã có sẵn. Trong trường hợp này bạn cần tạo một **Domain Controller** cho một **Child domain,** nên bạn đánh dấu vào mục lựa chọn thứ hai.



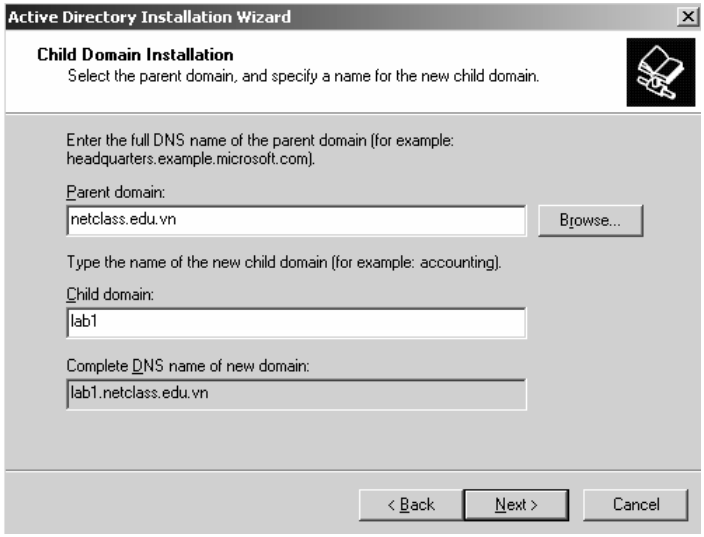

Để tạo một **child domain** trong một **domain tree** có sẵn, hệ thống yêu cầu bạn phải xác nhận bạn là người quản trị cấp **domain tree**. Trong hộp thoại này bạn nhập tài khoản và mật khẩu của người quản trị cấp rừng và tên của **domain tree** hiện tại.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Tiếp theo bạn nhập tên của **domain tree** hiện đang có và tên của **child domain** cần tạo.

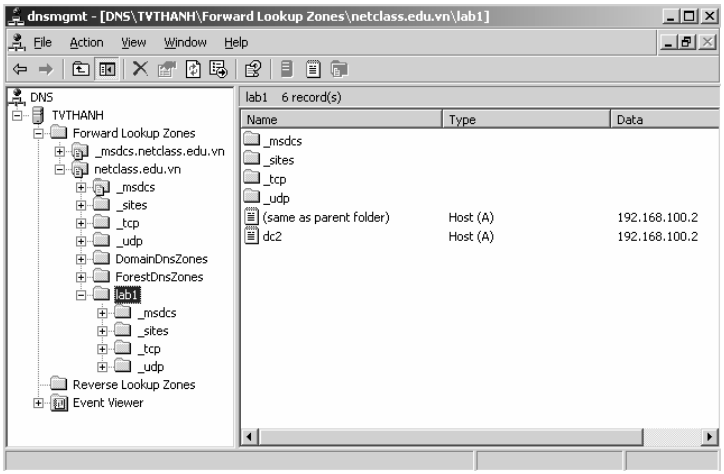



Các quá trình tiếp theo tương tự như quá trình tạo **Domain Controller** của phần trên.

Cuối cùng bạn có thể kiểm tra cây **DNS** của hệ thống trên **Server** quản lý gốc rừng có tạo thêm một **child domain** không, đồng thời bạn có thể cấu hình thêm chi dịch vụ **DNS** nhằm phục vụ tốt hơn cho hệ thống.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

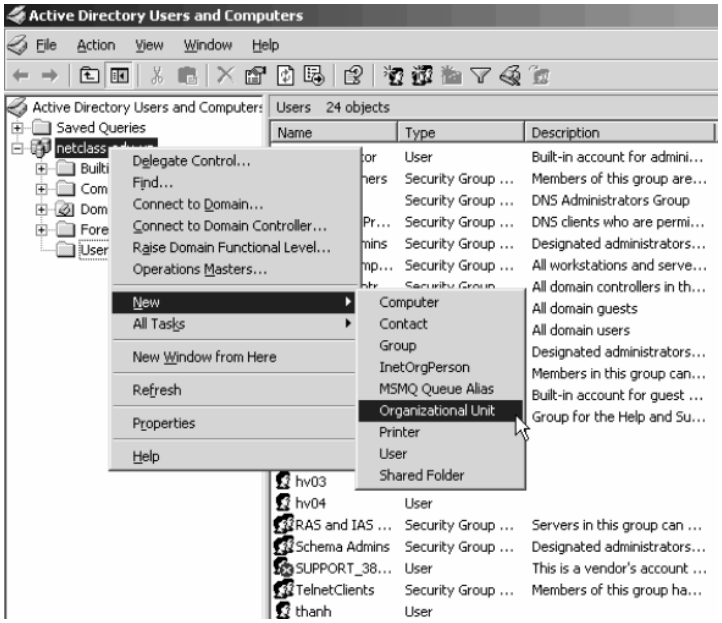



## III.5. Xây dựng Organizational Unit.

Như đã trình bày ở phần lý thuyết thì **OU** là một nhóm tài khoản người dùng, máy tính và tài nguyên mạng được tạo ra nhằm mục đích dễ dàng quản lý hơn và ủy quyền cho các quản trị viên địa phương giải quyết các công việc đơn giản. Đặc biệt hơn là thông qua **OU** chúng ta có thể áp đặt các giới hạn phần mềm và giới hạn phần cứng thông qua các **Group Policy**. Muốn xây dựng một **OU** bạn làm theo các bước sau:

Chọn menu **Start** ⏲ **Programs** ⏲ **Administrative Tools** ⏲ Active **Directory User and Computer**, để mở chương trình **Active Directory User and Computer**.

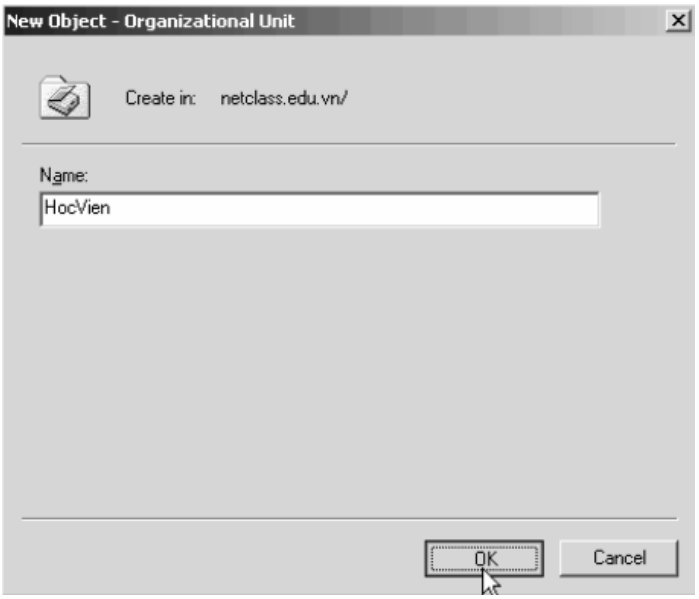
Chương trình mở ra, bạn nhấp phải chuột trên tên miền và chọn **New-Organizational Unit**.



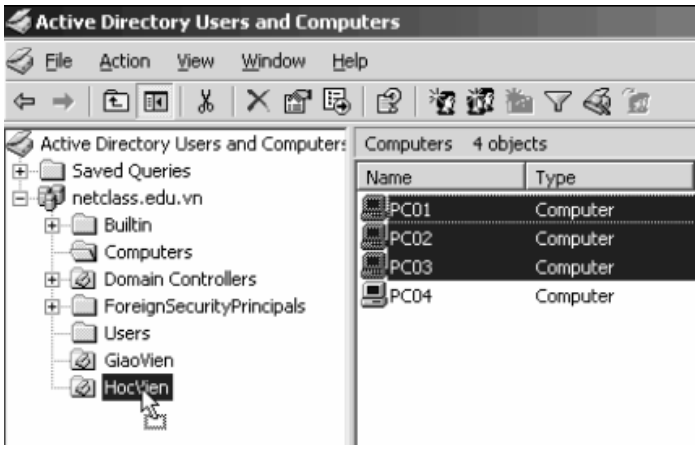

Hộp thoại xuất hiện, yêu cầu chúng ta nhập tên **OU** cần tạo, trong ví dụ này **OU** cần tạo có tên là **HocVien**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net



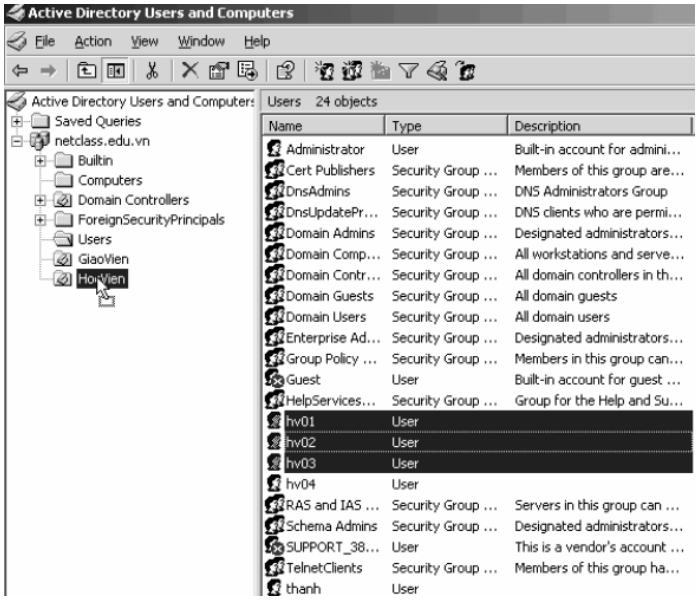

Đưa các máy trạm đã gia nhập nhập mạng cần quản lý vào **OU** vừa tạo.



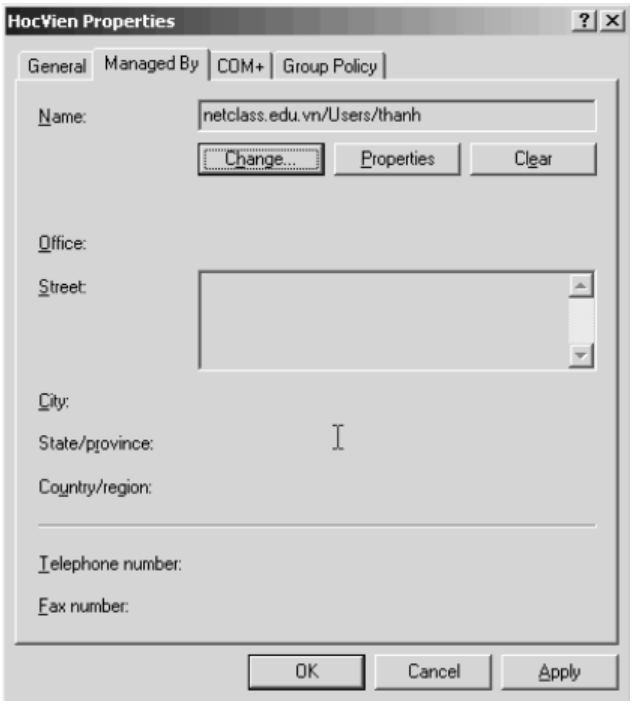

Tiếp theo bạn đưa các tài khoản người dùng cần quản lý vào **OU** vừa tạo.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net



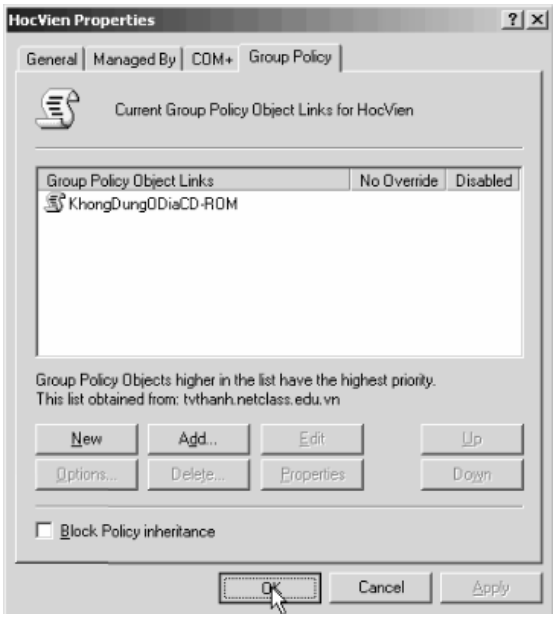

Sau khi đã đưa các máy tính và tài khoản người dùng vào **OU**, bước tiếp theo là bạn chỉ ra người nào hoặc nhóm nào sẽ quản lý **OU** này. Bạn nhấp phải chuột vào **OU** vừa tạo, chọn **Properties**, hộp thoại xuất hiện, trong **Tab Managed By**, bạn nhấp chuột vào nút **Change** để chọn người dùng quản lý **OU** này, trong ví dụ này chúng ta chọn tài khoản Thanh quản lý **OU**.




Bước cuối cùng này rất quan trọng, chúng ta sẽ tìm hiểu chi tiết ở chương **Group Policy**, đó là thiết lập các **Group Policy** áp dụng cho **OU** này. Bạn vào **Tab Group Policy**, nhấp chuột vào nút **New** để tạo mới một **GPO**, sau đó nhấp chuột vào nút **Edit** để hiệu chỉnh chính sách. Trong ví dụ này chúng ta tạo một chính sách cấm không cho phép dùng ổ đĩa **CD-ROM** áp dụng cho tất cả các người dùng trong **OU**.

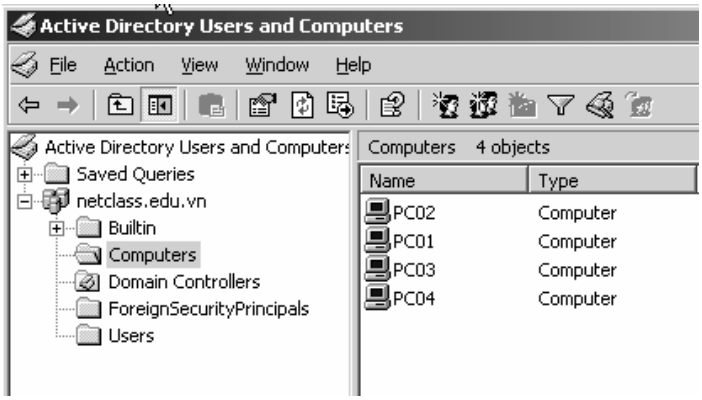


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




## III.6. Công cụ quản trị các đối tượng trong Active Directory.

Một trong bốn công cụ quản trị hệ thống **Active Directory** thì công cụ **Active Directory User and Computer** là công cụ quan trọng nhất và chúng ta sẽ gặp lại nhiều trong trong giáo trình này, từng bước ta sẽ khảo sát hết các tính năng trong công cụ này. Công cụ này có chức năng tạo và quản lý các đối tượng cơ bản của hệ thống **Active Directory**.

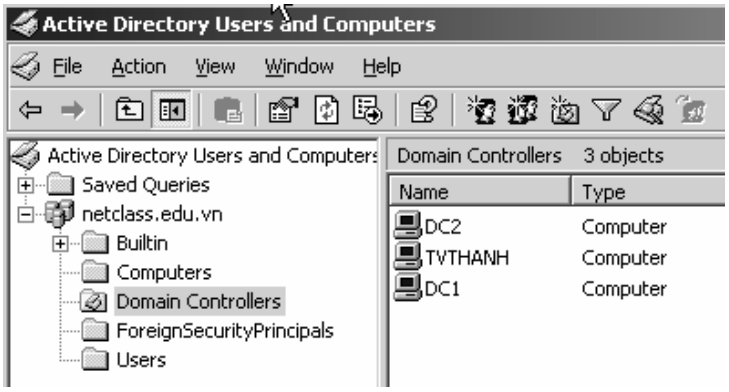



Theo hình trên chúng ta thấy trong miền netclass.edu.vn có các mục sau:

- **Builtin**: chứa các nhóm người dùng đã được tạo và định nghĩa quyền sẵn.
- **Computers**: chứa các máy trạm mặc định đang là thành viên của miền. Bạn cũng có thể dùng tính năng này để kiểm tra một máy trạm gia nhập vào miền có thành công không.
- **Domain Controllers**: chứa các điều khiển vùng (**Domain Controller**) hiện đang hoạt động trong miền. Bạn cũng có thể dùng tính năng này để kiểm tra việc tạo thêm **Domain Controller** đồng hành có thành công không.
- **ForeignSecurityPrincipals**: là một vật chứa mặc định dành cho các đối tượng bên ngoài miền đang xem xét, từ các miền đã thiết lập quan hệ tin cậy (**trusted domain**).
- **Users**: chứa các tài khoản người dùng mặc định trên miền.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net






Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

# Tóm tắt

Lý thuyết 4 tiết - Thực hành 10 tiết

| Mục tiêu | Các mục chính | Bài tập bắt buộc | Bài tập làm thêm |
|---|---|---|---|
| Kết thúc bài học này cung cấp học viên kiến thức về tài khoản người dùng, nhóm, các thuộc tính của tài khoản người dùng, các nhóm tạo sẵn … | I. Định nghĩa tài khoản người dùng và tài khoản nhóm.<br>II. Chứng thực và kiểm soát truy cập.<br>III. Các tài khoản tạo sẵn.<br>IV. Quản lý tài khoản người dùng và nhóm cục bộ.<br>V. Quản lý tài khoản người dùng và nhóm trên Active Directory. | Dựa vào bài tập môn Quản trị Windows Server 2003. | Dựa vào bài tập môn Quản trị Windows Server 2003. |



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

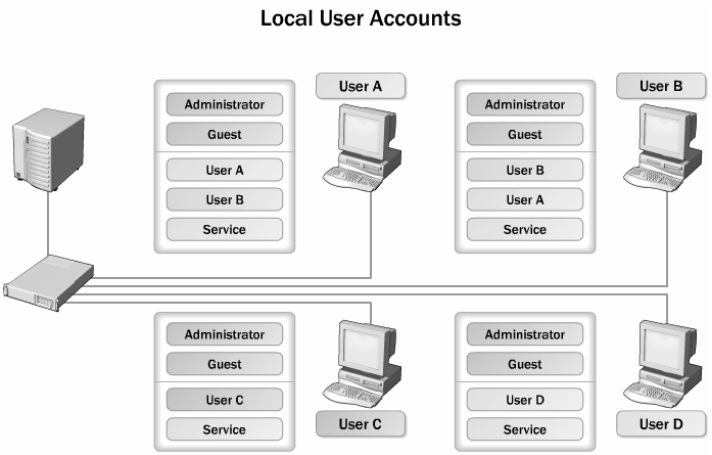
# I. ĐỊNH NGHĨA TÀI KHOẢN NGƯỜI DÙNG VÀ TÀI KHOẢN NHÓM.

## I.1. Tài khoản người dùng.

Tài khoản người dùng (**user account**) là một đối tượng quan trọng đại diện cho người dùng trên mạng, chúng được phân biệt với nhau thông qua chuỗi nhận dạng **username**. Chuỗi nhận dạng này giúp hệ thống mạng phân biệt giữa người này và người khác trên mạng từ đó người dùng có thể đăng nhập vào mạng và truy cập các tài nguyên mạng mà mình được phép.

### I.1.1 Tài khoản người dùng cục bộ.

Tài khoản người dùng cục bộ (**local user account**) là tài khoản người dùng được định nghĩa trên máy cục bộ và chỉ được phép **logon**, truy cập các tài nguyên trên máy tính cục bộ. Nếu muốn truy cập các tài nguyên trên mạng thì người dùng này phải chứng thực lại với máy **domain controller** hoặc máy tính chứa tài nguyên chia sẻ. Bạn tạo tài khoản người dùng cục bộ với công cụ **Local Users and Group** trong **Computer Management (COMPMGMT.MSC)**. Các tài khoản cục bộ tạo ra trên máy **stand-alone server**, **member server** hoặc các máy trạm đều được lưu trữ trong tập tin cơ sở dữ liệu **SAM** (**Security Accounts Manager**). Tập tin **SAM** này được đặt trong thư mục **\Windows\system32\config**.



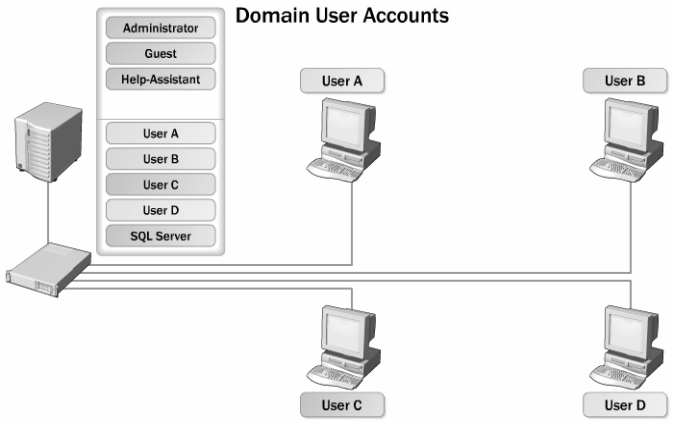

Hình 3.1: lưu trữ thông tin tài khoản người dùng cục bộ

### I.1.2 Tài khoản người dùng miền.

Tài khoản người dùng miền (**domain user account**) là tài khoản người dùng được định nghĩa trên **Active Directory** và được phép đăng nhập (**logon**) vào mạng trên bất kỳ máy trạm nào thuộc vùng. Đồng thời với tài khoản này người dùng có thể truy cập đến các tài nguyên trên mạng. Bạn tạo tài khoản người dùng miền với công cụ **Active Directory Users and Computer (DSA.MSC)**. Khác với tài khoản người dùng cục bộ, tài khoản người dùng miền không chứa trong các tập tin cơ sở dữ liệu **SAM** mà chứa trong tập tin **NTDS.DIT**, theo mặc định thì tập tin này chứa trong thư mục **\Windows\NTDS**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 3.2: lưu trữ thông tin tài khoản người dùng miền.

### I.1.3 Yêu cầu về tài khoản người dùng.

- Mỗi **username** phải từ 1 đến 20 ký tự (trên **Windows Server 2003** thì tên đăng nhập có thể dài đến 104 ký tự, tuy nhiên khi đăng nhập từ các máy cài hệ điều hành **Windows NT 4.0** về trước thì mặc định chỉ hiểu 20 ký tự).
- Mỗi **username** là chuỗi duy nhất của mỗi người dùng có nghĩa là tất cả tên của người dùng và nhóm không được trùng nhau.
- **Username** không chứa các ký tự sau: " / \ [ ] : ; | = , + * ? < >
- Trong một **username** có thể chứa các ký tự đặc biệt bao gồm: dấu chấm câu, khoảng trắng, dấu gạch ngang, dấu gạch dưới. Tuy nhiên, nên tránh các khoảng trắng vì những tên như thế phải đặt trong dấu ngoặc khi dùng các kịch bản hay dòng lệnh.

## I.2. Tài khoản nhóm.

Tài khoản nhóm (**group account**) là một đối tượng đại diện cho một nhóm người nào đó, dùng cho việc quản lý chung các đối tượng người dùng. Việc phân bổ các người dùng vào nhóm giúp chúng ta dễ dàng cấp quyền trên các tài nguyên mạng như thư mục chia sẻ, máy in. Chú ý là tài khoản người dùng có thể đăng nhập vào mạng nhưng tài khoản nhóm không được phép đăng nhập mà chỉ dùng để quản lý. Tài khoản nhóm được chia làm hai loại: nhóm bảo mật (**security group**) và nhóm phân phối (**distribution group**).

### I.2.1 Nhóm bảo mật.

Nhóm bảo mật là loại nhóm được dùng để cấp phát các quyền hệ thống (**rights**) và quyền truy cập (**permission**). Giống như các tài khoản người dùng, các nhóm bảo mật đều được chỉ định các **SID**. Có ba loại nhóm bảo mật chính là: **local**, **global** và **universal**. Tuy nhiên nếu chúng ta khảo sát kỹ thì có thể phân thành bốn loại như sau: **local, domain local, global và universal**.

**Local group** (nhóm cục bộ) là loại nhóm có trên các **máy stand-alone Server, member server, Win2K Pro hay WinXP**. Các nhóm cục bộ này chỉ có ý nghĩa và phạm vi hoạt động ngay tại trên máy chứa nó thôi.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

**Domain local group** (nhóm cục bộ miền) là loại nhóm cục bộ đặc biệt vì chúng là **local group** nhưng nằm trên máy **Domain Controller**. Các máy **Domain Controller** có một cơ sở dữ liệu **Active Directory** chung và được sao chép đồng bộ với nhau do đó một **local group** trên một **Domain Controller** này thì cũng sẽ có mặt trên các **Domain Controller** anh em của nó, như vậy **local group** này có mặt trên miền nên được gọi với cái tên nhóm cục bộ miền. Các nhóm trong mục **Built-in** của **Active Directory** là các **domain local**.

**Global group** (nhóm toàn cục hay nhóm toàn mạng) là loại nhóm nằm trong **Active Directory** và được tạo trên các **Domain Controller**. Chúng dùng để cấp phát những quyền hệ thống và quyền truy cập vượt qua những ranh giới của một miền. Một nhóm **global** có thể đặt vào trong một nhóm **local** của các server thành viên trong miền. Chú ý khi tạo nhiều nhóm **global** thì có thể làm tăng tải trọng công việc của **Global Catalog**.

**Universal group** (nhóm phổ quát) là loại nhóm có chức năng giống như **global group** nhưng nó dùng để cấp quyền cho các đối tượng trên khắp các miền trong một rừng và giữa các miền có thiết lập quan hệ tin cậy với nhau. Loại nhóm này tiện lợi hơn hai nhóm **global group** và **local group** vì chúng dễ dàng lồng các nhóm vào nhau. Nhưng chú ý là loại nhóm này chỉ có thể dùng được khi hệ thống của bạn phải hoạt động ở chế độ **Windows 2000 native functional level** hoặc **Windows Server 2003 functional level** có nghĩa là tất cả các máy **Domain Controller** trong mạng đều phải là **Windows Server 2003** hoặc **Windows 2000 Server**.

### I.2.2 Nhóm phân phối.

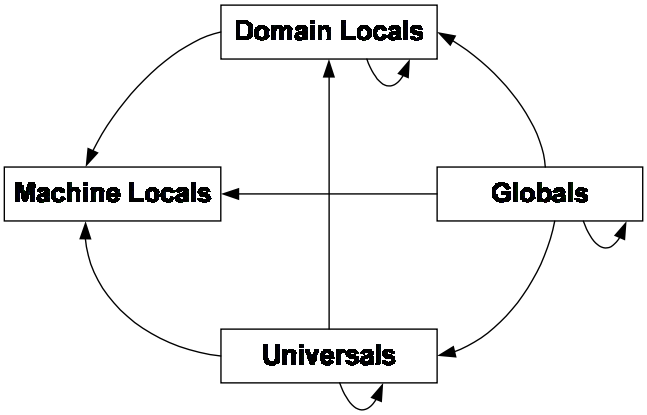
Nhóm phân phối là một loại nhóm phi bảo mật, không có **SID** và không xuất hiện trong các **ACL (Access Control List)**. Loại nhóm này không được dùng bởi các nhà quản trị mà được dùng bởi các phần mềm và dịch vụ. Chúng được dùng để phân phố thư (**e-mail**) hoặc các tin nhắn (**message**). Bạn sẽ gặp lại loại nhóm này khi làm việc với phần mềm **MS Exchange**.

### I.2.3 Qui tắc gia nhập nhóm.

- Tất cả các nhóm **Domain local**, **Global**, **Universal** đều có thể đặt vào trong nhóm **Machine Local**.
- Tất cả các nhóm **Domain local**, **Global**, **Universal** đều có thể đặt vào trong chính loại nhóm của mình.
- Nhóm **Global** và **Universal** có thể đặt vào trong nhóm **Domain local**.
- Nhóm **Global** có thể đặt vào trong nhóm **Universal**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 3.3: khả năng gia nhập của các loại nhóm.

# II. CHỨNG THỰC VÀ KIỂM SOÁT TRUY CẬP.

## II.1. Các giao thức chứng thực.

Chứng thực trong **Windows Server 2003** là quy trình gồm hai giai đoạn: đăng nhập tương tác và chứng thực mạng. Khi người dùng đăng nhập vùng bằng tên và mật mã, quy trình đăng nhập tương tác sẽ phê chuẩn yêu cầu truy cập của người dùng. Với tài khoản cục bộ, thông tin đăng nhập được chứng thực cục bộ và người dùng được cấp quyền truy cập máy tính cục bộ. Với tài khoản miền, thông tin đăng nhập được chứng thực trên **Active Directory** và người dùng có quyền truy cập các tài nguyên trên mạng. Như vậy với tài khoản người dùng miền ta có thể chứng thực trên bất kỳ máy tính nào trong miền. **Windows 2003** hỗ trợ nhiều giao thức chứng thực mạng, nổi bật nhất là:

- **Kerberos V5**: là giao thức chuẩn **Internet** dùng để chứng thực người dùng và hệ thống.
- **NT LAN Manager** (**NTLM**): là giao thức chứng thực chính của **Windows NT**.
- **Secure Socket Layer/Transport Layer Security** (**SSL/TLS**): là cơ chế chứng thực chính được dùng khi truy cập vào máy phục vụ **Web** an toàn.

## II.2. Số nhận diện bảo mật SID.

Tuy hệ thống **Windows Server 2003** dựa vào tài khoản người dùng (**user account**) để mô tả các quyền hệ thống (**rights**) và quyền truy cập (**permission**) nhưng thực sự bên trong hệ thống mỗi tài khoản được đặc trưng bởi một con số nhận dạng bảo mật **SID (Security Identifier)**. **SID** là thành phần nhận dạng không trùng lặp, được hệ thống tạo ra đồng thời với tài khoản và dùng riêng cho hệ thống xử lý, người dùng không quan tâm đến các giá trị này. **SID** bao gồm phần **SID** vùng cộng thêm với một **RID** của người dùng không trùng lặp. **SID** có dạng chuẩn "**S-1-5-21-D1-D2-D3-RID**", khi đó tất cả các **SID** trong miền đều có cùng giá trị **D1, D2, D3**, nhưng giá trị **RID** là khác nhau. Hai mục đích chính của việc hệ thống sử dụng **SID** là:

- Dễ dàng thay đổi tên tài khoản người dùng mà các quyền hệ thống và quyền truy cập không thay đổi.
- Khi xóa một tài khoản thì **SID** của tài khoản đó không còn giá trị nữa, nếu chúng ta có tạo một tài khoản mới cùng tên với tài khoản vừa xóa thì các quyền cũ cũng không sử dụng được bởi vì khi



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

tạo tài khoản mới thì giá trị **SID** của tài khoản này là một giá trị mới.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

## II.3. Kiểm soát hoạt động truy cập của đối tượng.

**Active Directory** là dịch vụ hoạt động dựa trên các đối tượng, có nghĩa là người dùng, nhóm, máy tính, các tài nguyên mạng đều được định nghĩa dưới dạng đối tượng và được kiểm soát hoạt động truy cập dựa vào bộ mô tả bảo mật **ACE**. Chức năng của bộ mô tả bảo mật bao gồm:

- Liệt kê người dùng và nhóm nào được cấp quyền truy cập đối tượng.
- Định rõ quyền truy cập cho người dùng và nhóm.
- Theo dõi các sự kiện xảy ra trên đối tượng.
- Định rõ quyền sở hữu của đối tượng.

Các thông tin của một đối tượng **Active Directory** trong bộ mô tả bảo mật được xem là mục kiểm soát hoạt động truy cập **ACE** (**Access Control Entry**). Một **ACL (Access Control List)** chứa nhiều **ACE**, nó là danh sách tất cả người dùng và nhóm có quyền truy cập đến đối tượng. **ACL** có đặc tính kế thừa, có nghĩa là thành viên của một nhóm thì được thừa hưởng các quyền truy cập đã cấp cho nhóm này.

# III. CÁC TÀI KHOẢN TẠO SẴN.

## III.1. Tài khoản người dùng tạo sẵn.

Tài khoản người dùng tạo sẵn (**Built-in**) là những tài khoản người dùng mà khi ta cài đặt **Windows Server 2003** thì mặc định được tạo ra. Tài khoản này là hệ thống nên chúng ta không có quyền xóa đi nhưng vẫn có quyền đổi tên (chú ý thao tác đổi tên trên những tài khoản hệ thống phức tạp một chút so với việc đổi tên một tài khoản bình thường do nhà quản trị tạo ra). Tất cả các tài khoản người dùng tạo sẵn này đều nằng trong **Container Users** của công cụ **Active Directory User and Computer**. Sau đây là bảng mô tả các tài khoản người dùng được tạo sẵn:

| Tên tài khoản | Mô tả |
|---|---|



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

| | |
|---|---|
| Administrator | **Administrator** là một tài khoản đặc biệt, có toàn quyền trên máy tính hiện tại. Bạn có thể đặt mật khẩu cho tài khoản này trong lúc cài đặt **Windows Server 2003**. Tài khoản này có thể thi hành tất cả các tác vụ như tạo tài khoản người dùng, nhóm, quản lý các tập tin hệ thống và cấu hình máy in… |
| Guest | Tài khoản **Guest** cho phép người dùng truy cập vào các máy tính nếu họ không có một tài khoản và mật mã riêng. Mặc định là tài khoản này không được sử dụng, nếu được sử dụng thì thông thường nó bị giới hạn về quyền, ví dụ như là chỉ được truy cập **Internet** hoặc in ấn. |
| ILS_Anonymous_ User | Là tài khoản đặc biệt được dùng cho dịch vụ **ILS**. **ILS** hỗ trợ cho các ứng dụng điện thoại có các đặc tính như: **caller ID**, **video conferencing**, **conference calling**, và **faxing**. Muốn sử dụng **ILS** thì dịch vụ **IIS** phải được cài đặt. |
| IUSR_computer-name | Là tài khoản đặc biệt được dùng trong các truy cập giấu tên trong dịch vụ **IIS** trên máy tính có cài **IIS**. |
| IWAM_computer-name | Là tài khoản đặc biệt được dùng cho **IIS** khởi động các tiến trình của các ứng dụng trên máy có cài **IIS**. |
| Krbtgt | Là tài khoản đặc biệt được dùng cho dịch vụ trung tâm phân phối khóa (**Key Distribution Center**) |
| TSInternetUser | Là tài khoản đặc biệt được dùng cho **Terminal Services**. |

## III.2. Tài khoản nhóm Domain Local tạo sẵn.

Nhưng chúng ta đã thấy trong công cụ **Active Directory User** and **Computers**, **container Users** chứa nhóm **universal**, nhóm **domain** local và nhóm **global** là do hệ thống đã mặc định quy định trước. Nhưng một số nhóm **domain** local đặc biệt được đặt trong **container Built-in**, các nhóm này không được di chuyển sang các **OU** khác, đồng thời nó cũng được gán một số quyền cố định trước nhằm phục vụ cho công tác quản trị. Bạn cũng chú ý rằng là không có quyền xóa các nhóm đặc biệt này.

| Tên nhóm | Mô tả |
|---|---|



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

| | |
|---|---|
| Administrators | Nhóm này mặc định được ấn định sẵn tất cả các quyền hạn cho nên thành viên của nhóm này có toàn quyền trên hệ thống mạng. Nhóm **Domain Admins** và **Enterprise Admins** là thành viên mặc định của nhóm **Administrators**. |
| Account Operators | Thành viên của nhóm này có thể thêm, xóa, sửa được các tài khoản người dùng, tài khoản máy và tài khoản nhóm. Tuy nhiên họ không có quyền xóa, sửa các nhóm trong **container Built-in** và **OU**. |
| Domain Controllers | Nhóm này chỉ có trên các **Domain Controller** và mặc định không có thành viên nào, thành viên của nhóm có thể đăng nhập cục bộ vào các **Domain Controller** nhưng không có quyền quản trị các chính sách bảo mật. |
| Backup Operators | Thành viên của nhóm này có quyền lưu trữ dự phòng (**Backup**) và phục hồi (**Retore**) hệ thống tập tin. Trong trường hợp hệ thống tập tin là **NTFS** và họ không được gán quyền trên hệ thống tập tin thì thành viên của nhóm này chỉ có thể truy cập hệ thống tập tin thông qua công cụ **Backup**. Nếu muốn truy cập trực tiếp thì họ phải được gán quyền. |
| Guests | Là nhóm bị hạn chế quyền truy cập các tài nguyên trên mạng. Các thành viên nhóm này là người dùng vãng lai không phải là thành viên của mạng. Mặc định các tài khoản **Guest** bị khóa |
| Print Operator | Thành viên của nhóm này có quyền tạo ra, quản lý và xóa bỏ các đối tượng máy in dùng chung trong Active Directory. |
| Server Operators | Thành viên của nhóm này có thể quản trị các máy server trong miền như: cài đặt, quản lý máy in, tạo và quản lý thư mục dùng chung, backup dữ liệu, định dạng đĩa, thay đổi giờ… |
| Users | Mặc định mọi người dùng được tạo đều thuộc nhóm này, nhóm này có quyền tối thiểu của một người dùng nên việc truy cập rất hạn chế. |
| Replicator | Nhóm này được dùng để hỗ trợ việc sao chép danh bạ trong **Directory Services**, nhóm này không có thành viên mặc định. |
| Incoming Forest Trust Builders | Thành viên nhóm này có thể tạo ra các quan hệ tin cậy hướng đến, một chiều vào các rừng. Nhóm này không có thành viên mặc định. |
| Network Configuration Operators | Thành viên nhóm này có quyền sửa đổi các thông số **TCP/IP** trên các máy **Domain Controller** trong miền. |



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

| | |
|---|---|
| Pre-Windows 2000 Compatible Access | Nhóm này có quyền truy cập đến tất cả các tài khoản người dùng và tài khoản nhóm trong miền, nhằm hỗ trợ cho các hệ thống **WinNT** cũ. |
| Remote Desktop User | Thành viên nhóm này có thể đăng nhập từ xa vào các **Domain Controller** trong miền, nhóm này không có thành viên mặc định. |
| Performace Log Users | Thành viên nhóm này có quyền truy cập từ xa để ghi nhận lại những giá trị về hiệu năng của các máy **Domain Controller**, nhóm này cũng không có thành viên mặc định. |
| Performace Monitor Users | Thành viên nhóm này có khả năng giám sát từ xa các máy **Domain Controller**. |

Ngoài ra còn một số nhóm khác như **DHCP Users, DHCP Administrators, DNS Administrators**… các nhóm này phục vụ chủ yếu cho các dịch vụ, chúng ta sẽ tìm hiểu cụ thể trong từng dịch vụ ở giáo trình "Dịch Vụ Mạng". Chú ý theo mặc định hai nhóm **Domain Computers** và **Domain Controllers** được dành riêng cho tài khoản máy tính, nhưng bạn vẫn có thể đưa tài khoản người dùng vào hai nhóm này.

## III.3. Tài khoản nhóm Global tạo sẵn.

| Tên nhóm | Mô tả |
|---|---|
| Domain Admins | Thành viên của nhóm này có thể toàn quyền quản trị các máy tính trong miền vì mặc định khi gia nhập vào miền các **member server** và các máy trạm (**Win2K Pro, WinXP**) đã đưa nhóm **Domain Admins** là thành viên của nhóm cục bộ **Administrators** trên các máy này. |
| Domain Users | Theo mặc định mọi tài khoản người dùng trên miền đều là thành viên của nhóm này. Mặc định nhóm này là thành viên của nhóm cục bộ **Users** trên các máy **server** thành viên và máy trạm. |
| Group Policy Creator Owners | Thành viên nhóm này có quyền sửa đổi chính sách nhóm của miền, theo mặc định tài khoản **administrator** miền là thành viên của nhóm này. |
| Enterprise Admins | Đây là một nhóm **universal**, thành viên của nhóm này có toàn quyền trên tất cả các miền trong rừng đang xét. Nhóm này chỉ xuất hiện trong miền gốc của rừng thôi. Mặc định nhóm này là thành viên của nhóm **administrators** trên các **Domain Controller** trong rừng. |
| Schema Admins | Nhóm **universal** này cũng chỉ xuất hiện trong miền gốc của rừng, thành viên của nhóm này có thể chỉnh sửa cấu trúc tổ chức (**schema**) của **Active Directory**. |



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

## III.4. Các nhóm tạo sẵn đặc biệt.

Ngoài các nhóm tạo sẵn đã trình bày ở trên, hệ thống **Windows Server 2003** còn có một số nhóm tạo sẵn đặt biệt, chúng không xuất hiện trên cửa sổ của công cụ **Active Directory User** and **Computer**, mà chúng chỉ xuất hiện trên các **ACL** của các tài nguyên và đối tượng. Ý nghĩa của nhóm đặc biệt này là:

- **Interactive**: đại diện cho những người dùng đang sử dụng máy tại chỗ.
- **Network**: đại diện cho tất cả những người dùng đang nối kết mạng đến một máy tính khác.
- **Everyone**: đại diện cho tất cả mọi người dùng.
- **System**: đại diện cho hệ điều hành.
- **Creator owner**: đại diện cho những người tạo ra, những người sở hữa một tài nguyên nào đó như: thư mục, tập tin, tác vụ in ấn (**print job**)…
- **Authenticated users**: đại diện cho những người dùng đã được hệ thống xác thực, nhóm này được dùng như một giải pháp thay thế an toàn hơn cho nhóm **everyone**.
- **Anonymous logon**: đại diện cho một người dùng đã đăng nhập vào hệ thống một cách nặc danh, chẳng hạn một người sử dụng dịch vụ **FTP**.
- **Service**: đại diện cho một tài khoản mà đã đăng nhập với tư cách như một dịch vụ.
- **Dialup**: đại diện cho những người đang truy cập hệ thống thông qua **Dial-up Networking**.

# IV. QUẢN LÝ TÀI KHOẢN NGƯỜI DÙNG VÀ NHÓM CỤC BỘ.

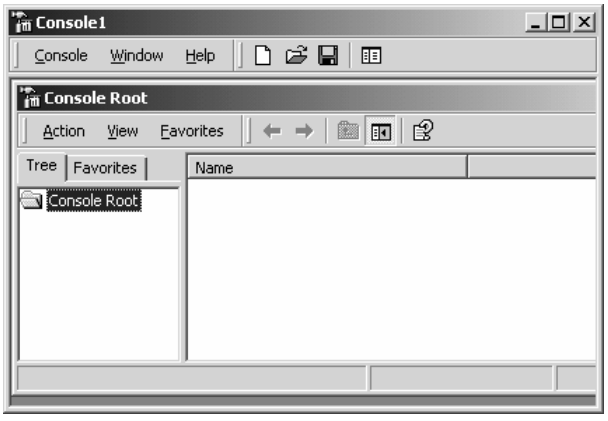
## IV.1. Công cụ quản lý tài khoản người dùng cục bộ.

Muốn tổ chức và quản lý người dùng cục bộ, ta dùng công cụ **Local Users and Groups**. Với công cụ này bạn có thể tạo, xóa, sửa các tài khoản người dùng, cũng như thay đổi mật mã. Có hai phương thức truy cập đến công cụ **Local Users and Groups**:

- Dùng như một **MMC** (**Microsoft Management Console**) snap-in.
- Dùng thông qua công cụ **Computer Management.**

Các bước dùng để chèn **Local Users and Groups snap-in** vào trong **MMC**:

Chọn **Start** ⏲ **Run**, nhập vào hộp thoại **MMC** và ấn phím **Enter** để mở cửa sổ **MMC**.




Chọn **Console** ⏲ **Add/Remove Snap-in** để mở hộp thoại **Add/Remove Snap-in**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

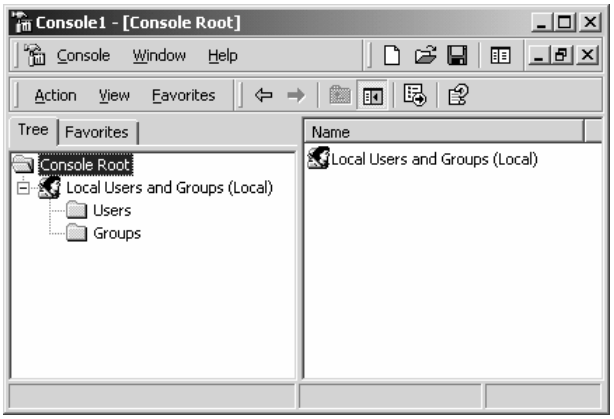
Nhấp chuột vào nút **Add** để mở hộp thoại **Add Standalone Snap-in**.

Chọn **Local Users and Groups** và nhấp chuột vào nút **Add**.

Hộp thoại **Choose Target Machine** xuất hiện, ta chọn **Local Computer** và nhấp chuột vào nút **Finish** để trở lại hộp thoại **Add Standalone Snap-in**.

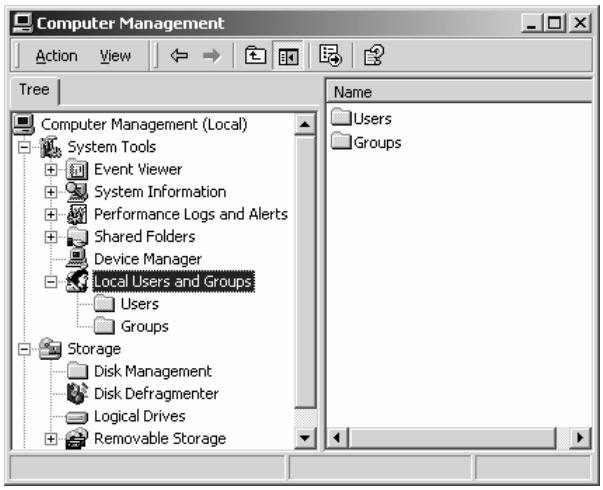
Nhấp chuột vào nút **Close** để trở lại hộp thoại **Add/Remove Snap-in**.

Nhấp chuột vào nút **OK**, ta sẽ nhìn thấy **Local Users and Groups snap-in** đã chèn vào **MMC** như hình sau.




Lưu **Console** bằng cách chọn **Console** 🕘 **Save**, sau đó ta nhập đường dẫn và tên file cần lưu trữ. Để tiện lợi cho việc quản trị sau này ta có thể lưu **console** ngay trên **Desktop**.

Nếu máy tính của bạn không có cấu hình **MMC** thì cách nhanh nhất để truy cập công cụ **Local Users and Groups** thông qua công cụ **Computer Management**. Nhấp phải chuột vào **My Computer** và chọn **Manage** từ **pop-up menu** và mở cửa sổ **Computer Management**. Trong mục **System Tools**, ta sẽ nhìn thấy mục **Local Users and Groups**




Cách khác để truy cập đến công cụ **Local Users and Groups** là vào **Start** 🕘 **Programs** 🕘 **Administrative Tools** 🕘 **Computer Management**.

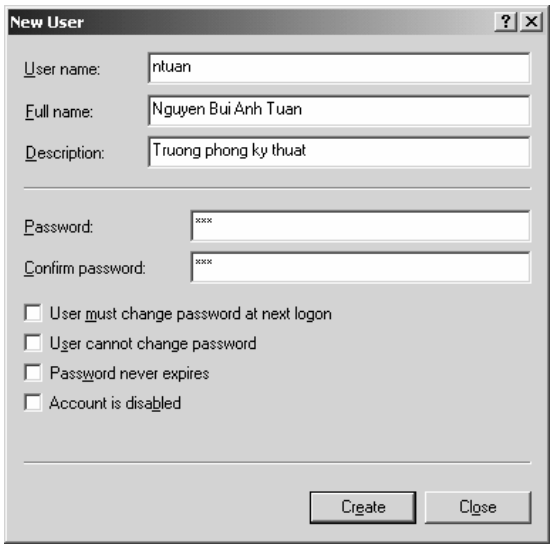


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

## IV.2. Các thao tác cơ bản trên tài khoản người dùng cục bộ.

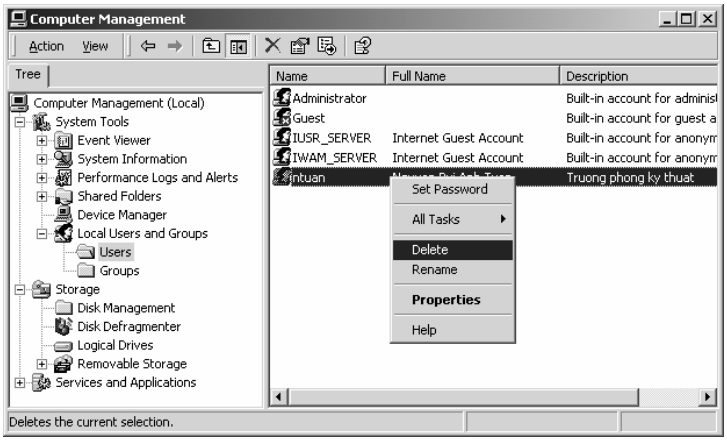
### IV.2.1 Tạo tài khoản mới.

Trong công cụ **Local Users and Groups**, ta nhấp phải chuột vào **Users** và chọn **New User**, hộp thoại **New User** hiển thị bạn nhập các thông tin cần thiết vào, nhưng quan trọng nhất và bắt buộc phải có là mục **Username**.




### IV.2.2 Xóa tài khoản.

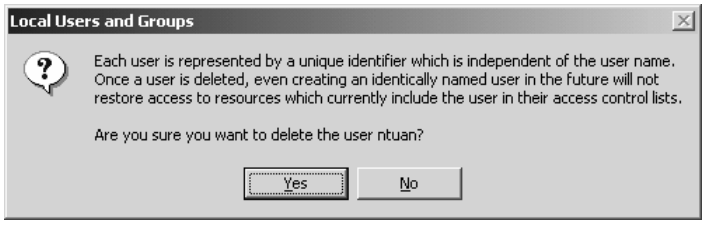
Bạn nên xóa tài khoản người dùng, nếu bạn chắc rằng tài khoản này không bao giờ cần dùng lại nữa. Muốn xóa tài khoản người dùng bạn mở công cụ **Local Users and Groups**, chọn tài khoản người dùng cần xóa, nhấp phải chuột và chọn **Delete** hoặc vào thực đơn **Action** ⏲ **Delete**.




*Chú ý*: khi chọn **Delete** thì hệ thống xuất hiện hộp thoại hỏi bạn muốn xóa thật sự không vì tránh trường hợp bạn xóa nhầm. Bởi vì khi đã xóa thì tài khoản người dùng này không thể phục hồi được.

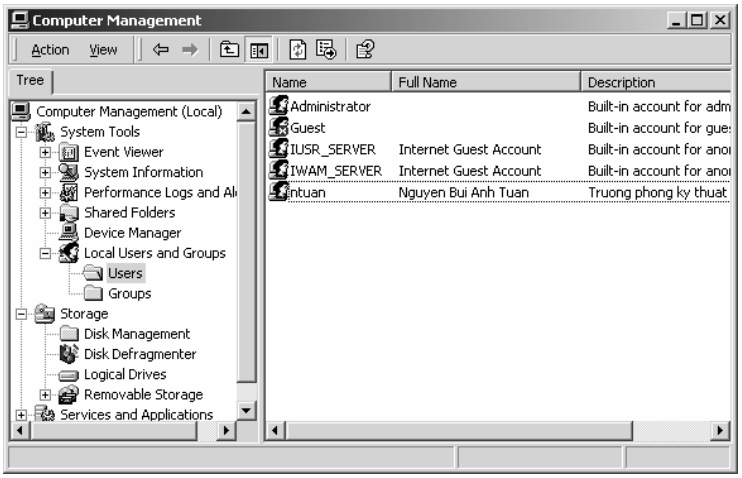


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




### IV.2.3 Khóa tài khoản.

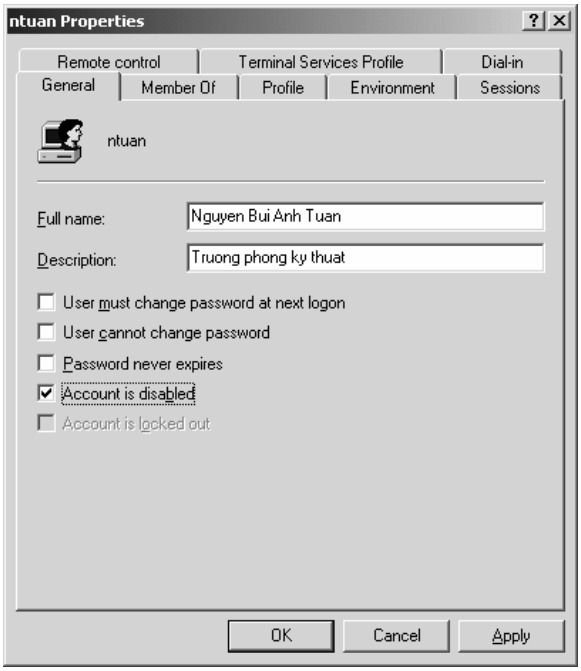
Khi một tài khoản không sử dụng trong thời gian dài bạn nên khóa lại vì lý do bảo mật và an toàn hệ thống. Nếu bạn xóa tài khoản này đi thì không thể phục hồi lại được do đó ta chỉ tạm khóa. Trong công cụ **Local Users and Groups**, nhấp đôi chuột vào người dùng cần khóa, hộp thoại **Properties** của tài khoản xuất hiện.




Trong **Tab General**, đánh dấu vào mục **Account is disabled**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




### IV.2.4 Đổi tên tài khoản.

Bạn có thể đổi tên bất kỳ một tài khoản người dùng nào, đồng thời bạn cũng có thể điều chỉnh các thông tin của tài khoản người dùng thông qua chức năng này. Chức năng này có ưu điểm là khi bạn thay đổi tên người dùng nhưng **SID** của tài khoản vẫn không thay đổi. Muốn thay đổi tên tài khoản người dùng bạn mở công cụ **Local Users and Groups**, chọn tài khoản người dùng cần thay đổi tên, nhấp phải chuột và chọn **Rename**.

### IV.2.5 Thay đổi mật khẩu.

Muốn đổi mật mã của người dùng bạn mở công cụ **Local Users and Groups**, chọn tài khoản người dùng cần thay đổi mật mã, nhấp phải chuột và chọn **Reset password**.

# V. QUẢN LÝ TÀI KHOẢN NGƯỜI DÙNG VÀ NHÓM TRÊN ACTIVE DIRECTORY.

## V.1. Tạo mới tài khoản người dùng.

Bạn có thể dùng công cụ **Active Directory User and Computers** trong **Administrative Tools** ngay trên máy **Domain Controller** để tạo các tài khoản người dùng miền. Công cụ này cho phép bạn quản lý tài khoản người dùng từ xa thậm chí trên các máy trạm không phải dùng hệ điều hành **Server** như **WinXP, Win2K Pro**. Muốn thế trên các máy trạm này phải cài thêm bộ công cụ **Admin Pack**. Bộ công cụ này nằm trên **Server** trong thư mục **\Windows\system32\ADMINPAK.MSI**. Tạo một tài khoản người dùng trên **Active Directory**, ta làm các bước sau:



Chọn **Start** ◴ **Programs** ◴ **Administrative Tools** ◴ **Active Directory Users and Computers**.

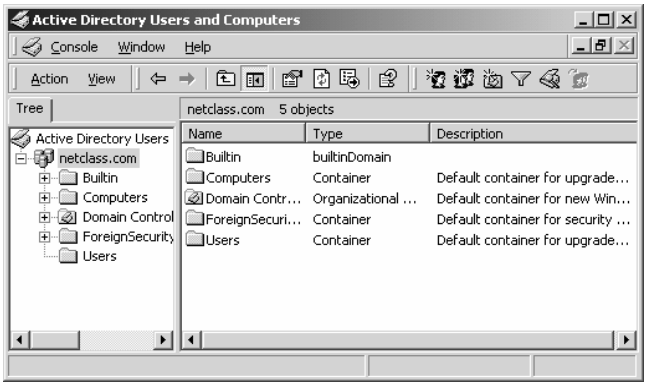
Cửa sổ **Active Directory Users and Computers** xuất hiện, bạn nhấp phải chuột vào mục **Users**, chọn

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

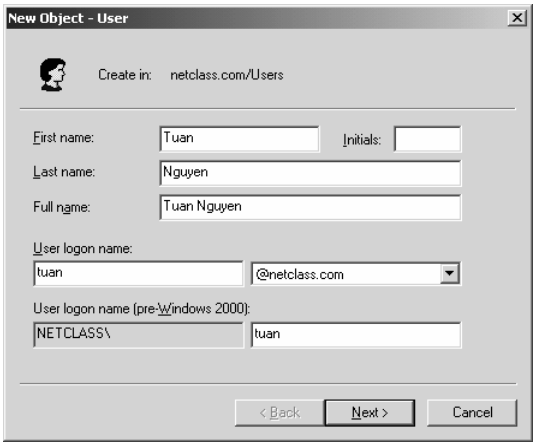
**New** ⏲ **User**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net



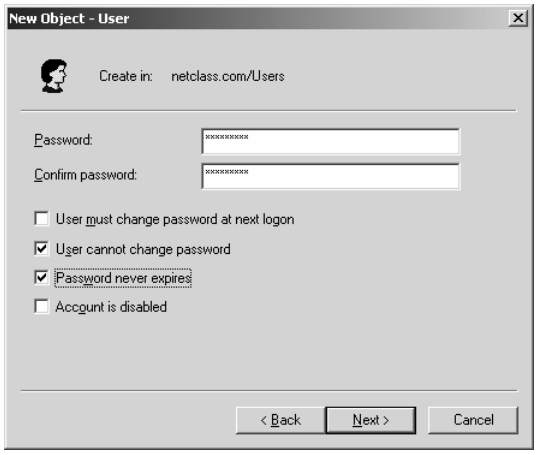

Hộp thoại **New Object-User** xuất hiện như hình sau, bạn nhập tên mô tả người dùng, tên tài khoản logon vào mạng. Giá trị **Full Name** sẽ tự động phát sinh khi bạn nhập giá trị **First Name** và **Last Name**, nhưng bạn vẫn có thể thay đổi được. Chú ý: giá trị quan trọng nhất và bắt buộc phải có là **logon name** (**username**). Chuỗi này là duy nhất cho một tài khoản người dùng theo như định nghĩa trên phần lý thuyết. Trong môi trường **Windows 2000** và **2003**, Microsoft đưa thêm một khái niệm hậu tố **UPN** (**Universal Principal Name**), trong ví dụ này là **"@netclass.edu.vn"**. Hậu tố **UPN** này gắn vào sau chuỗi **username** dùng để tạo thành một tên **username** đầy đủ dùng để chứng thực ở cấp rừng hoặc chứng thực ở một miền khác có quan hệ tin cậy với miền của người dùng đó, trong ví dụ này thì tên **username** đầy đủ là "**tuan@netclass.edu.vn**". Ngoài ra trong hộp thoại này cũng cho phép chúng ta đặt tên **username** của tài khoản người dùng phục vụ cho hệ thống cũ (**pre-Windows 2000**). Sau khi việc nhập các thông tin hoàn thành bạn nhấp chuột vào nút **Next** để tiếp tục.




Hộp thoại thứ hai xuất hiện, cho phép bạn nhập vào mật khẩu (**password**) của tài khoản người dùng và đánh dấu vào các lựa chọn liên quan đến tài khoản như: cho phép đổi mật khẩu, yêu cầu phải đổi mật khẩu lần đăng nhập đầu tiên hay khóa tài khoản. Các lựa chọn này chúng ta sẽ tìm hiểu chi tiết ở phần tiếp theo.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net



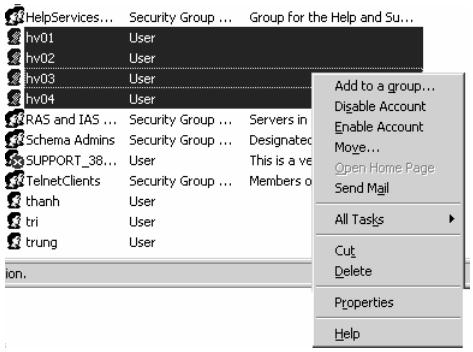

Hộp thoại cuối cùng xuất hiện và nó hiển thị các thông tin đã cấu hình cho người dùng. Nếu tất cả các thông tin đã chính xác thì bạn nhấp chuột vào nút **Finish** để hoàn thành, còn nếu cần chỉnh sửa lại thì nhấp chuột vào nút **Back** để trở về các hộp thoại trước.


## V.2. Các thuộc tính của tài khoản người dùng

Muốn quản lý các thuộc tính của các tài khoản người ta dùng công cụ **Active Directory Users and Computers** (bằng cách chọn **Start** 🕘 **Programs** 🕘 **Administrative Tools** 🕘 **Active Directory Users and Computers**), sau đó chọn thư mục **Users** và nhấp đôi chuột vào tài khoản người dùng cần khảo sát. Hộp thoại **Properties** xuất hiện, trong hộp thoại này chứa 12 **Tab** chính, ta sẽ lần lượt khảo sát các **Tab** này. Ngoài ra bạn có thể gom nhóm (dùng hai phím **Shift, Ctrl**) và hiệu chỉnh thông tin của nhiều tài khoản người dùng cùng một lúc.

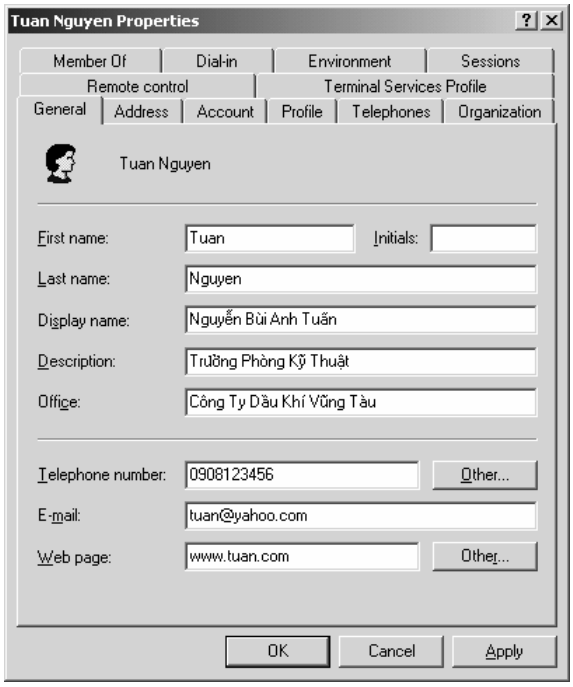


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




### V.2.1 Các thông tin mở rộng của người dùng

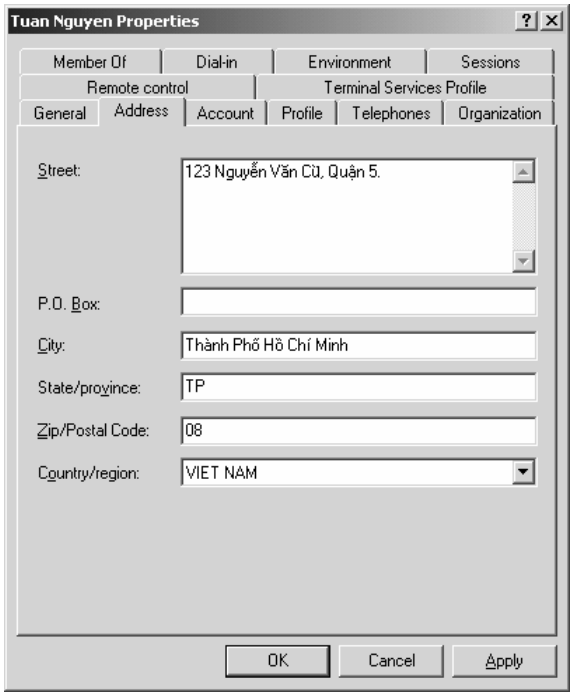
Tab **General** chứa các thông tin chung của người dùng trên mạng mà bạn đã nhập trong lúc tạo người dùng mới. Đồng thời bạn có thể nhập thêm một số thông tin như: số điện thoại, địa chỉ mail và trang địa chỉ trang Web cá nhân…



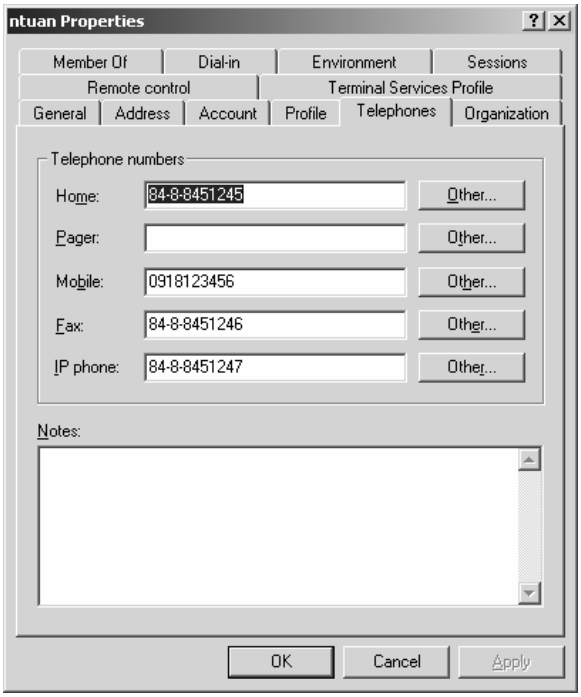

Tab **Address** cho phép bạn có thể khai báo chi tiết các thông tin liên quan đến địa chỉ của tài khoản người dùng như: địa chỉ đường, thành phố, mã vùng, quốc gia…



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net



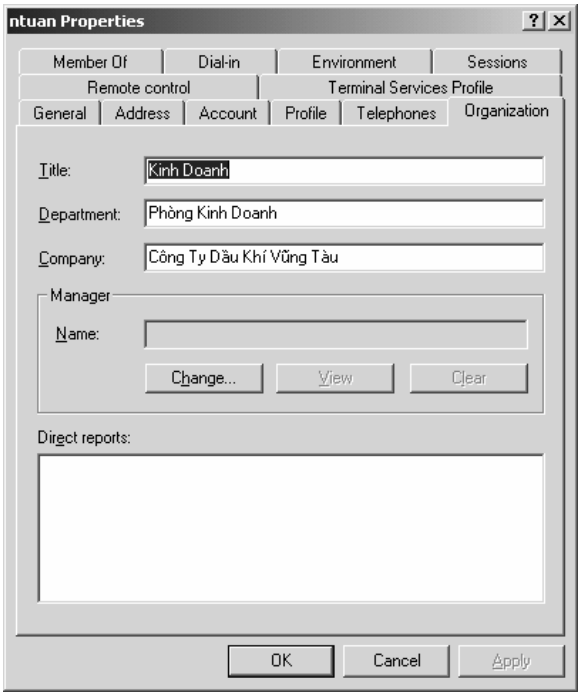

Tab **Telephones** cho phép bạn khai báo chi tiết các số điện thoại của tài khoản người dùng.




Tab **Organization** cho phép bạn khai báo các thông tin người dùng về: chức năng của công ty, tên phòng ban trực thuộc, tên công ty …

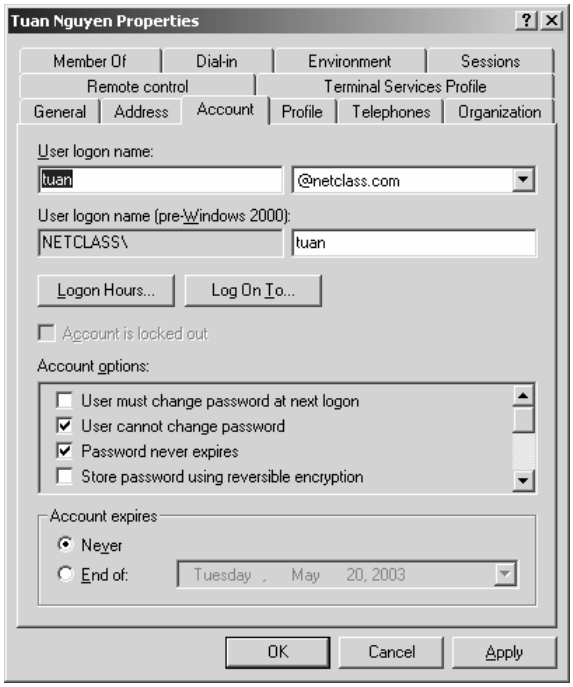


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




### V.2.2 Tab Account.

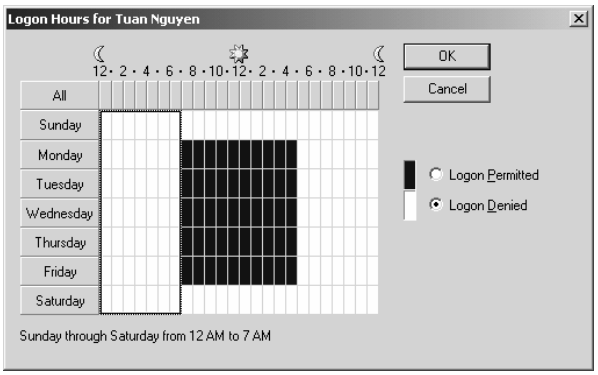
Tab **Account** cho phép bạn khai báo lại **username**, quy định giờ **logon** vào mạng cho người dùng, quy định máy trạm mà người dùng có thể sử dụng để vào mạng, quy định các chính sách tài khoản cho người dùng, quy định thời điểm hết hạn của tài khoản…



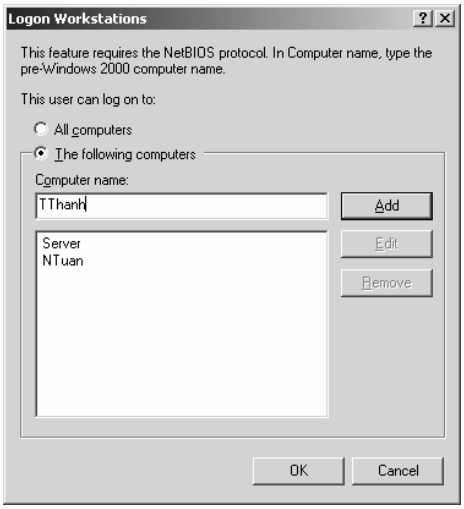



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Điều khiển giờ **logon** vào mạng: bạn nhấp chuột vào nút **Logon Hours**, hộp thoại **Logon Hours** xuất hiện. Mặc định tất cả mọi người dùng đều được phép truy cập vào mạng 24 giờ mỗi ngày, trong tất cả 7 ngày của tuần. Khi một người dùng **logon** vào mạng thì hệ thống sẽ kiểm tra xem thời điểm này có nằm trong khoảng thời gian cho phép truy cập không, nếu không phù hợp thì hệ thống sẽ không cho vào mạng và thông báo lỗi **Unable to log you on because of an account restriction**. Bạn có thể thay đổi quy định giờ **logon** bằng cách chọn vùng thời gian cần thay đổi và nhấp chuột vào nút lựa chọn **Logon Permitted**, nếu ngược lại không cho phép thì nhấp chuột vào nút lựa chọn **Logon Denied**. Sau đây là hình ví dụ chỉ cho phép người dùng làm việc từ 7h sáng đến 5h chiều, từ thứ 2 đến thứ 6. Chú ý: mặc định người dùng không bị **logoff** tự động khi hết giờ đăng nhập nhưng bạn có thể điều chỉnh điều này tại mục **Automatically Log Off Users When Logon Hours Expire** trong **Group Policy** phần **Computer Configuration\ Windows Settings\Security Settings\ Local Policies\ Security Option**. Ngoài ra bạn cũng có cách khác để điều chỉnh thông tin **logoff** này bằng cách dùng công cụ **Domain Security Policy** hoặc **Local Security Policy** tùy theo bối cảnh.




Chọn lựa máy trạm được truy cập vào mạng: bạn nhấp chuột vào nút **Log On To**, bạn sẽ thấy hộp thoại **Logon Workstations** xuất hiện. Hộp thoại này cho phép bạn chỉ định người dùng có thể **logon** từ tất cả các máy tính trong mạng hoặc giới hạn người dùng chỉ được phép **logon** từ một số máy tính trong mạng. Ví dụ như người quản trị mạng làm việc trong môi trường bảo mật nên tài khoản người dùng này chỉ được chỉ định **logon** vào mạng từ một số máy tránh tình trạng người dùng giả dạng quản trị để tấn công mạng. Muốn chỉ định máy tính mà người dùng được phép **logon** vào mạng, bạn nhập tên máy tính đó vào mục **Computer Name** và sau đó nhấp chuột vào nút **Add**.






Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

**Bảng mô tả chi tiết các tùy chọn liên quan đến tài khoản người dùng:**

| Tùy Chọn | Ý Nghĩa |
|---|---|
| User must change password at next logon | Người dùng phải thay đổi mật khẩu lần đăng nhập kế tiếp, sau đó mục này sẽ tự động bỏ chọn. |
| User cannot change password | Nếu được chọn thì ngăn không cho người dùng tùy ý thay đổi mật khẩu. |
| Password never expires | Nếu được chọn thì mật khẩu của tài khoản này không bao giờ hết hạn. |
| Store password using reversible encryption | Chỉ áp dụng tùy chọn này đối với người dùng đăng nhập từ các máy **Apple**. |
| Account is disabled | Nếu được chọn thì tài khoản này tạm thời bị khóa, không sử dụng được. |
| Smart card is required for interactive login | Tùy chọn này được dùng khi người dùng đăng nhập vào mạng thông qua một thẻ thông minh (**smart card**), lúc đó người dùng không nhập username và password mà chỉ cần nhập vào một số **PIN**. |
| Account is trusted for delegation | Chỉ áp dụng cho các tài khoản dịch vụ nào cần giành được quyền truy cập vào tài nguyên với vai trò những tài khoản người dùng khác |
| Account is sensitive and cannot be delegated | Dùng tùy chọn này trên một tài khoản khách vãng lai hoặc tạm để đảm bảo rằng tài khoản đó sẽ không được đại diện bởi một tài khoản khác. |
| Use DES encryption types for this account | Nếu được chọn thì hệ thống sẽ hỗ trợ **Data Encryption Standard** (**DES**) với nhiều mức độ khác nhau. |
| Do not require Kerberos preauthentication | Nếu được chọn hệ thống sẽ cho phép tài khoản này dùng một kiểu thực hiện giao thức **Kerberos** khác với kiểu của **Windows Server 2003**. |

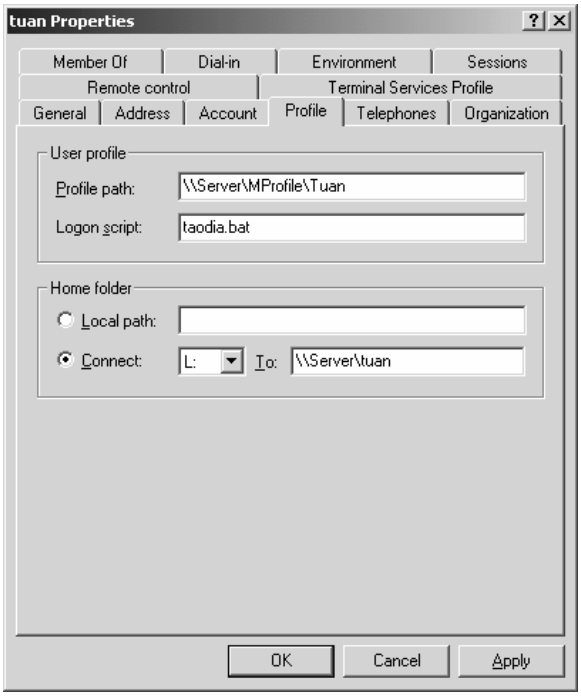
Mục cuối cùng trong **Tab** này là quy định thời gian hết hạn của một tài khoản người dùng. Trong mục **Account Expires**, nếu ta chọn **Never** thì tài khoản này không bị hết hạn, nếu chọn **End of: ngày tháng hết hạn** thì đến ngày này tài khoản này bị tạm khóa.

### V.2.3 Tab Profile.

**Tab Profile** cho phép bạn khai báo đường dẫn đến **Profile** của tài khoản người dùng hiện tại, khai báo tập tin **logon script** được tự động thi hành khi người dùng đăng nhập hay khai báo **home folder**. Chú ý các tùy chọn trong **Tab Profile** này chủ yếu phục vụ cho các máy trạm trước **Windows 2000**, còn đối với các máy trạm từ **Win2K** trở về sau như: **Win2K Pro, WinXP, Windows Server 2003** thì chúng ta có thể cấu hình các lựa chọn này trong **Group Policy**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Trước tiên chúng ta hãy tìm hiểu khái niệm **Profile**. **User Profiles** là một thư mục chứa các thông tin về môi trường của **Windows Server 2003** cho từng người dùng mạng. **Profile** chứa các qui định về màn hình **Desktop**, nội dung của menu **Start,** kiểu cách phối màu sắc, vị trí sắp xếp các **icon**, biểu tượng chuột…

Mặc định khi người dùng đăng nhập vào mạng, một **profile** sẽ được mở cho người dùng đó. Nếu là lần đăng nhập lần đầu tiên thì họ sẽ nhận được một **profile** chuẩn. Một thư mục có tên giống như tên của người dùng đăng nhập sẽ được tạo trong thư mục **Documents and Settings**. Thư mục **profile** người dùng được tạo chứa một tập tin **ntuser.dat**, tập tin này được xem như là một thư mục con chứa các liên kết thư mục đến các biểu tượng nền của người dùng. Trong **Windows Server 2003** có ba loại **Profile**:

**Local Profile**: là **profile** của người dùng được lưu trên máy cục bộ và họ tự cấu hình trên **profile** đó.

**Roaming Profile**: là loại **Profile** được chứa trên mạng và người quản trị mạng thêm thông tin đường dẫn **user profile** vào trong thông tin tài khoản người dùng, để tự động duy trì một bản sao của tài khoản người dùng trên mạng.

**Mandatory Profile**: người quản trị mạng thêm thông tin đường dẫn **user profile** vào trong thông tin tài khoản người dùng, sau đó chép một profile đã cấu hình sẵn vào đường dẫn đó. Lúc đó các người dùng dùng chung **profile** này và không được quyền thay đổi profile đó.

Kịch bản đăng nhập (**logon script** hay **login script**) là những tập tin chương trình được thi hành mỗi khi người dùng đăng nhập vào hệ thống, với chức năng là cấu hình môi trường làm việc của người dùng và phân phát cho họ những tài nguyên mạng như ổ đĩa, máy in (được ánh xa từ **Server**). Bạn có thể dùng nhiều ngôn ngữ kịch bản để tạo ra **logon script** như: lệnh **shell** của **DOS/NT/Windows**, **Windows Scripting Host (WSH), VBScript, Jscript**…



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

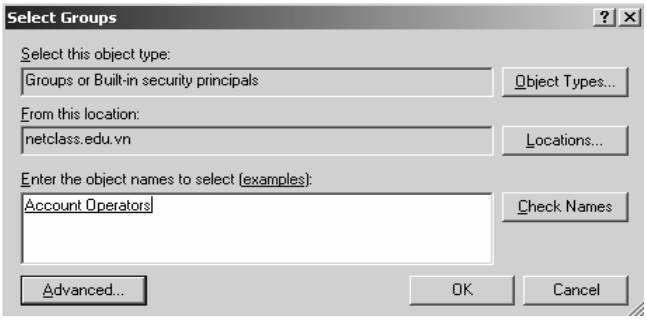
Đối với **Windows Server 2003** thì có hai cách để khai báo **logon script** là: khai báo trong thuộc tính của tài khoản người dùng thông qua công cụ **Active Directory User and Computers**, khai báo thông qua **Group Policy**. Nhưng chú ý trong cả hai cách, các tập tin **script** và mọi tập tin cần thiết khác phải được đặt trong thư mục chia sẻ **SYSVOL**, nằm trong **\Windows\SYSVOL\sysvol**, nếu các tập tin script này phục vụ cho các máy tiền **Win2K** thì phải đặt trong thư mục **\Windows\Sysvol\sysvol\domainname\scripts**. Để các tập tin **script** thi hành được bạn nhớ cấp quyền cho các người dùng mạng có quyền **Read** và **Excute** trên các tập tin này. Sau đây là một ví dụ về một tập tin **logon script**.

```
@echo off
rem Taodia.bat Version 1.0
rem neu nguoi dung logon ngay tai server thi khong lam gi ca.
ff %computername%.== tvthanh. goto END
rem xoa cac o dia anh xa dang ton tai
net use h: /delete >nul
net use j: /delete >nul
rem anh xa o dia h va j
net use h: \\tvthanh\users  /yes >nul
net use j: \\tvthanh\apps  /yes >nul
rem dong bo thoi gian voi Server
net time \\tvthanh /set /yes
:END
```

Thư mục cá nhân (**home folder hay home directory**) là thư mục dành riêng cho mỗi tài khoản người dùng, giúp người dùng có thể lưu trữ các tài liệu và tập tin riêng, đồng thời đây cũng là thư mục mặc định tại dấu nhắc lệnh. Muốn tạo một thư mục nhân cho người dùng thì trong mục **Connect** bạn chọn ổ đĩa hiển thị trên máy trạm và đường dẫn mà đĩa này cần ánh xạ đến (chú ý là các thư mục dùng chung đảm bảo đã chia sẻ). Trong ví dụ này bạn chỉ thư mục cá nhân cho tài khoản Tuan là "\\server\tuan", nhưng bạn có thể thay thế tên tài khoản bằng biến môi trường người dùng như: "\\server\%username%".

### V.2.4 Tab Member Of.

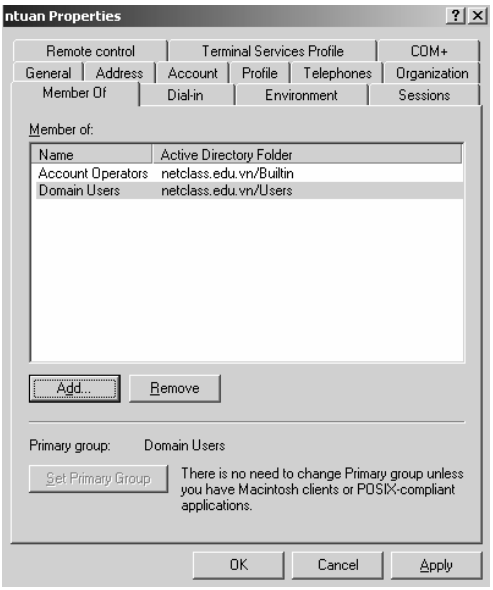
**Tab Member Of** cho phép bạn xem và cấu hình tài khoản người dùng hiện tại là thành viên của những nhóm nào. Một tài khoản người dùng có thể là thành viên của nhiều nhóm khác nhau và nó được thừa hưởng quyền của tất cả các nhóm này. Muốn gia nhập vào nhóm nào bạn nhấp chuột vào nút **Add**, hộp thoại chọn nhóm sẽ hiện ra.






Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

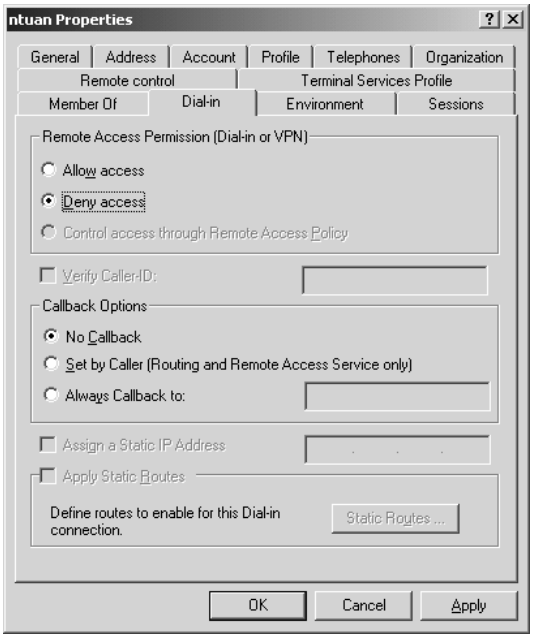
Trong hộp thoại chọn nhóm, nếu bạn nhớ tên nhóm thì có thể nhập trực tiếp tên nhóm vào và sau đó nhấp chuột vào nút **Check Names** để kiểm tra có chính xác không, bạn có thể nhập gần đúng để hệ thống tìm các tên nhóm có liên quan. Đây là tính năng mới của **Windows Server 2003** tránh tình trạng tìm kiếm và hiển thị hết tất cả các nhóm hiện có trong hệ thống. Nếu bạn không nhớ tên nhóm thì chấp nhận nhấp chuột vào nút **Advanced** và **Find Now** để tìm hết tất cả các nhóm.




Nếu bạn muốn tài khoản người dùng hiện tại thoát ra khỏi một nhóm nào đó thì bạn chọn nhóm sau đó nhấp chuột vào nút **Remove**.

### V.2.5 Tab Dial-in.

Tab **Dial-in** cho phép bạn cấu hình quyền truy cập từ xa của người dùng cho kết nối **dial-in** hoặc **VPN**, chúng ta sẽ khảo sát chi tiết ở chương **Routing and Remote Access**.






Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

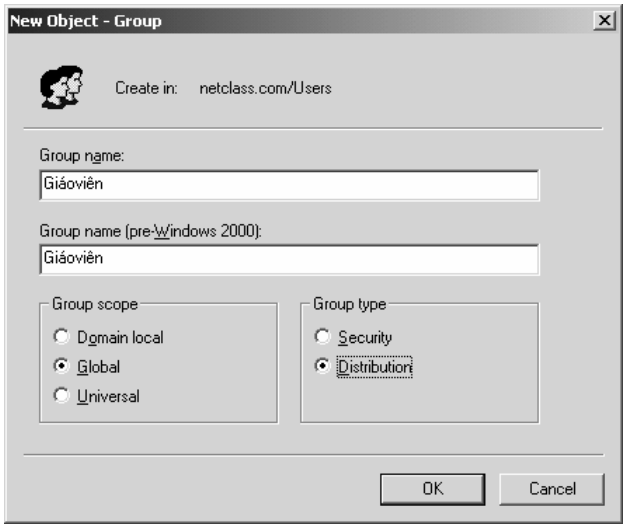
## V.3. Tạo mới tài khoản nhóm.

Bạn tạo và quản lý tài khoản nhóm trên **Active Directory** thông qua công cụ **Active Directory Users and Computers**. Trước khi tạo nhóm bạn phải xác định loại nhóm cần tạo, phạm vi hoạt động của nhóm như thế nào. Sau khi chuẩn bị đầy đủ các thông tin bạn thực hiện các bước sau:

Chọn **Start** 🕘 **Programs** 🕘 **Administrative Tools** 🕘 **Active Directory Users and Computers** để mở công cụ **Active Directory Users and Computers** lên.

Nhấp phải chuột vào mục **Users**, chọn **New** trên **pop-up menu** và chọn **Group**.

Hộp thoại **New Object – Group** xuất hiện, bạn nhập tên nhóm vào mục **Group name**, trường tên nhóm cho các hệ điều hành trước **Windows 2000 (pre-Windows 2000)** tự động phát sinh, bạn có thể hiệu chỉnh lại cho phù hợp.




Nhấp chuột vào nút **OK** để hoàn tất và đóng hộp thoại.

## V.4. Các tiện ích dòng lệnh quản lý tài khoản người dùng và tài khoản nhóm.

So với **Windows 2000 Server** thì **Windows Server 2003** cung cấp thêm nhiều công cụ dòng lệnh mạnh mẽ, có thể được dùng trong các tập tin xử lý theo lô (**batch**) hoặc các tập tin kịch bản (**script**) để quản lý tài khoản người dùng như thêm, xóa, sửa. **Windows 2003** còn hỗ trợ việc nhập và xuất các đối tượng từ **Active Directory**. Hai tiện ích **dsadd.exe** và **admod.exe** với đối số **user** cho phép chúng ta thêm và chỉnh sửa tài khoản người dùng trong **Active Directory**. Tiện ích **csvde.exe** được dùng để nhập hoặc xuất dữ liệu đối tượng thông qua các tập tin kiểu **CSV** (**comma-separated values**). Đồng thời hệ thống mới này vẫn còn sử dụng hai lệnh **net user** và **net group** của **Windows 2000**.

### V.4.1 Lệnh net user.

Chức năng: tạo thêm, hiệu chỉnh và hiển thị thông tin của các tài khoản người dùng .



Cú pháp:

net user [username [password | *] [options]] [/domain]

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

net user username {password | *} /add [options] [/domain]



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

net user username [/delete] [/domain]

Ý nghĩa các tham số:

- Không tham số: dùng để hiển thị danh sách của tất cả các tài khoản người dùng trên máy tính
- [**Username**]: chỉ ra tên tài khoản người dùng cần thêm, xóa, hiệu chỉnh hoặc hiển thị. Tên của tài khoản người dùng có thể dài đến 20 ký tự.
- [**Password**]: ấn định hoặc thay đổi mật mã của tài khoản người dùng. Một mật mã phải có chiều dài tối thiểu bằng với chiều dài quy định trong chính sách tài khoản người dùng. Trong **Windows 2000** thì chiều dài của mật mã có thể dài đến 127 ký tự, nhưng trên hệ thống **Win9X** thì chỉ hiểu được 14 ký tự, do đó nếu bạn đặt mật mã dài hơn 14 ký tự thì có thể tài khoản này không thể **logon** vào mạng từ máy trạm dùng **Win9X**.
- [**/domain**]: các tác vụ sẽ thực hiện trên máy điều khiển vùng. Tham số này chỉ áp dụng cho **Windows 2000 Server** là **primary domain controller** hoặc **Windows 2000 Professional** là thành viên của máy **Windows 2000 Server domain**.
- [**/add**]: thêm một tài khoản người dùng vào trong cơ sở dữ liệu tài khoản người dùng.
- [**/delete**]: xóa một tài khoản người dùng khỏi cơ sở dữ liệu tài khoản người dùng.
- [**/active:{no | yes}**]: cho phép hoặc tạm khóa tài khoản người dùng. Nếu tài khoản bị khóa thì người dùng không thể truy cập các tài nguyên trên máy tính. Mặc định là cho phép (**active**).
- [**/comment:"text"**]: cung cấp mô tả về tài khoản người dùng, mô tả này có thể dài đến 48 ký tự.
- [**/countrycode:nnn**]: chỉ định mã quốc gia và mã vùng.
- [**/expires:{date | never}**]: quy định ngày hết hiệu lực của tài khoản người dùng.
- [**/fullname:"name"**]: khai báo tên đầy đủ của người dùng.
- [**/homedir:path**]: khai báo đường dẫn thư mục cá nhân của tài khoản, chú ý đường dẫn này đã tồn tại.
- [**/passwordchg:{yes | no}**]: chỉ định người dùng có thể thay đổi mật mã của mình không, mặc định là có thể.
- [**/passwordreq:{yes | no}**]: chỉ định một tài khoản người dùng phải có một mật mã, mặc định là có mật mã.
- [**/profilepath:[path]**]: khai báo đường dẫn **Profile** của người dùng, nếu không hệ thống sẽ tự tạo một profile chuẩn cho người dùng lần **logon** đầu tiên.
- [**/scriptpath:path**]: khai báo đường dẫn và tập tin **logon script**. Đường dẫn này có thể là đường dẫn tuyệt đối hoặc đường dẫn tương đối (ví dụ: %systemroot%\System32\Repl\Import\Scripts).
- [**/times:{times | all}**]: quy định giờ cho phép người dùng logon vào mạng hay máy tính cục bộ. Các thứ trong tuần được đại diện bởi ký tự : M, T, W, Th, F, Sa, Su. Giờ ta dùng AM, PM để phân biệt buổi sáng hoặc chiều. Ví dụ sau chỉ cho phép người dùng làm việc trong giờ hành chính từ thứ 2 đến thứ 6: “M,7AM-5PM; T,7AM-5PM; W,7AM-5PM; Th,7AM-5PM; F,7AM-5PM;”
- [**/workstations:{computername[,...] | *}**]: chỉ định các máy tính mà người dùng này có thể sử dụng để logon vào mạng. Nếu **/workstations** không có danh sách hoặc danh sách là ký tự ‘*’ thì người dùng có thể sử dụng bất kỳ máy nào để vào mạng.



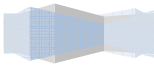
### V.4.2 Lệnh net group.

Chức năng: tạo mới thêm, hiển thị hoặc hiệu chỉnh nhóm toàn cục trên **Windows 2000 Server**

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

**domains**, lệnh này chỉ có hiệu lực khi dùng trên máy **Windows 2000 Server Domain Controllers**.





Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Cú pháp:

net group [groupname [/comment:"text"]] [/domain]

net group groupname {/add [/comment:"text"] | /delete} [/domain]

net group groupname username[ ...] {/add | /delete} [/domain]

Ý nghĩa các tham số:

- Không tham số: dùng để hiển thị tên của Server và tên của các nhóm trên Server đó.
- [**Groupname**]: chỉ định tên nhón cần thêm, mở rộng hoặc xóa.
- [**/comment:"text"**]: thêm thông tin mô tả cho một nhóm mới hoặc có sẵn, nội dung này có thể dài đến 48 ký tự.
- [**/domain**]: các tác vụ sẽ thực hiện trên máy điều khiển vùng. Tham số này chỉ áp dụng cho **Windows 2000 Server** là **primary domain controller** hoặc **Windows 2000 Professional** là thành viên của máy **Windows 2000 Server domain**.
- [**username[ ...]**]: danh sách một hoặc nhiều người dùng cần thêm hoặc xóa ra khỏi nhóm, các tên này cách nhau bởi khoảng trắng.
- [**/add**]: thêm một nhóm hoặc thêm một người dùng vào nhóm.
- [**/delete**]: xóa một nhóm hoặc xóa một người dùng khỏi nhóm.

### V.4.3 Lệnh net localgroup.

Chức năng: thêm, hiển thị hoặc hiệu chỉnh nhóm cục bộ.

Cú pháp:

net localgroup [groupname [/comment:"text"]] [/domain]

net localgroup groupname {/add [/comment:"text"] | /delete} [/domain]

net localgroup groupname name [ ...] {/add | /delete} [/domain]

Ý nghĩa các tham số:

- Không tham số: dùng hiển thị tên server và tên các nhóm cục bộ trên máy tính hiện tại.
- [**Groupname**]: chỉ định tên nhón cần thêm, mở rộng hoặc xóa.
- [**/comment:"text"**]: thêm thông tin mô tả cho một nhóm mới hoặc có sẵn, nội dung này có thể dài đến 48 ký tự.
- [**/domain**]: các tác vụ sẽ thực hiện trên máy điều khiển vùng. Tham số này chỉ áp dụng cho **Windows 2000 Server** là **primary domain controller** hoặc **Windows 2000 Professional** là thành viên của máy **Windows 2000 Server domain**.
- [**name** [ ...]]: danh sách một hoặc nhiều tên người dùng hoặc tên nhóm cần thêm vào hoặc xóa khỏi nhóm cục bộ. Các tên này cách nhau bởi khoảng trắng.
- [**/add**]: thêm tên một nhóm toàn cục hoặc tên người dùng vào nhóm cục bộ.
- [**/delete**]: xóa tên một nhóm toàn cục hoặc tên người dùng khỏi nhóm cục bộ.



### V.4.4 Các lệnh hỗ trợ dịch vụ Active Driectory trong môi trường Windows Server 2003.

Trên hệ thống **Windows Server 2003**, **Microsoft** phát triển thêm một số lệnh nhằm hỗ trợ tốt hơn cho dịch vụ **Directory** như: **dsadd**, **dsrm**, **dsmove**, **dsget**, **dsmod**, **dsquery**. Các lệnh này thao tác chủ

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

yếu trên các đối tượng **computer, contact, group, ou, user, quota**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

- **Dsadd**: cho phép bạn thêm một **computer**, **contact**, **group**, **ou** hoặc **user** vào trong dịch vụ **Directory**.
- **Dsrm**: xóa một đối tượng trong dịch vụ **Directory**.
- **Dsmove**: di chuyển một đối tượng từ vị trí này đến vị trí khác trong dịch vụ **Directory**.
- **Dsget**: hiển thị các thông tin lựa chọn của một đối tượng **computer**, **contact**, **group**, **ou**, **server** hoặc **user** trong một dịch vụ **Directory**.
- **Dsmod**: chỉnh sửa các thông tin của **computer**, **contact**, **group**, **ou** hoặc **user** trong một dịch vụ **Directory**.
- **Dsquery**: truy vấn các thành phần trong dịch vụ **Directory**.
- Ví dụ:
- Tạo một **user** mới: dsadd user “CN=hv10, CN=Users, DC=netclass, DC=edu, DC=vn” –samid hv10 –pwd 123
- Xóa một **user**: dsrm “CN=hv10, CN=Users, DC=netclass, DC=edu, DC=vn”
- Xem các **user** trong hệ thống: ***dsquery user***
- Gia nhập **user** mới vào nhóm: dsmod group “CN=hs, CN=Users, DC=netclass, DC=edu, DC=vn” –addmbr “CN=hv10, CN=Users, DC=netclass, DC=edu, DC=vn”



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

# Tóm tắt

Lý thuyết 5 tiết - Thực hành 6 tiết

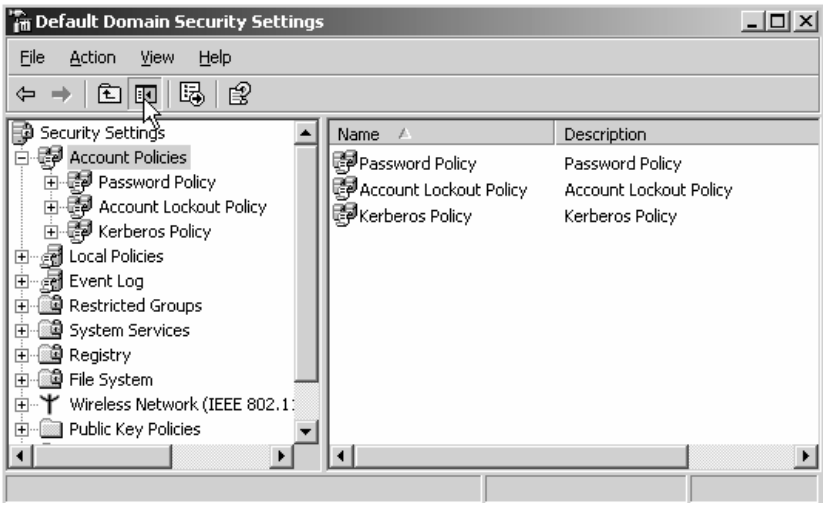
| Mục tiêu | Các mục chính | Bài tập bắt buộc | Bài tập làm thêm |
|---|---|---|---|
| Kết thúc bài học này cung cấp học viên kiến thức về chính sách mật khẩu, chính sách khóa tài khoản người dùng, quyền hệ thống của người dùng, IPSec … | I. Chính sách tài khoản người dùng.<br>II. Chính sách cục bộ.<br>III. IPSec. | Dựa vào bài tập môn Quản trị Windows Server 2003. | Dựa vào bài tập môn Quản trị Windows Server 2003. |



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

# I. CHÍNH SÁCH TÀI KHOẢN NGƯỜI DÙNG.

Chính sách tài khoản người dùng (**Account Policy**) được dùng để chỉ định các thông số về tài khoản người dùng mà nó được sử dụng khi tiến trình **logon** xảy ra. Nó cho phép bạn cấu hình các thông số bảo mật máy tính cho mật khẩu, khóa tài khoản và chứng thực **Kerberos** trong vùng. Nếu trên **Server** thành viên thì bạn sẽ thấy hai mục **Password Policy** và **Account Lockout Policy**, trên máy **Windows Server 2003** làm **domain controller** thì bạn sẽ thấy ba thư mục **Password Policy**, **Account Lockout Policy** và **Kerberos Policy**. Trong **Windows Server 2003** cho phép bạn quản lý chính sách tài khoản tại hai cấp độ là: cục bộ và miền. Muốn cấu hình các chính sách tài khoản người dùng ta vào **Start** 🕘 **Programs** 🕘 **Administrative Tools** 🕘 **Domain Security Policy** hoặc **Local Security Policy**.




## I.1. Chính sách mật khẩu.

Chính sách mật khẩu (**Password Policies**) nhằm đảm bảo an toàn cho mật khẩu của người dùng để trách các trường hợp đăng nhập bất hợp pháp vào hệ thống. Chính sách này cho phép bạn qui định chiều dài ngắn nhất của mật khẩu, độ phức tạp của mật khẩu…




Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Các lựa chọn trong chính sách mật mã:

| Chính sách | Mô tả | Mặc định |
|---|---|---|
| Enforce Password History | Số lần đặt mật mã không được trùng nhau | 24 |
| Maximum Password Age | Quy định số ngày nhiều nhất mà mật mã người dùng có hiệu lực | 42. |
| Minimum Password Age | Quy số ngày tối thiểu trước khi người dùng có thể thay đổi mật mã. | 1 |
| Minimum Password Length | Chiều dài ngắn nhất của mật mã | 7 |
| Passwords Must Meet Complexity Requirements | Mật khẩu phải có độ phức tạp như: có ký tự hoa, thường, có ký số. | Cho phép |
| Store Password Using Reversible Encryption for All Users in the Domain | Mật mã người dùng được lưu dưới dạng mã hóa | Không cho phép |

## I.2. Chính sách khóa tài khoản.

Chính sách khóa tài khoản (**Account Lockout Policy**) quy định cách thức và thời điểm khóa tài khoản trong vùng hay trong hệ thống cục bộ. Chính sách này giúp hạn chế tấn công thông qua hình thức **logon** từ xa.

Các thông số cấu hình chính sách khóa tài khoản:

| Chính sách | Mô tả | Giá trị mặc định |
|---|---|---|
| Account Lockout Threshold | Quy định số lần cố gắng đăng nhập trước khi tài khoản bị khóa | 0 (tài khoản sẽ không bị khóa) |
| Account Lockout Duration | Quy định thời gian khóa tài khoản | Là 0, nhưng nếu Acc**ount Lockout Threshold** được thiết lập thì giá trị này là 30 phút. |
| Reset Account Lockout Counter After | Quy định thời gian đếm lại số lần đăng nhập không thành công | Là 0, nhưng nếu **Account Lockout Threshold** được thiết lập thì giá trị này là 30 phút. |

# II. CHÍNH SÁCH CỤC BỘ.

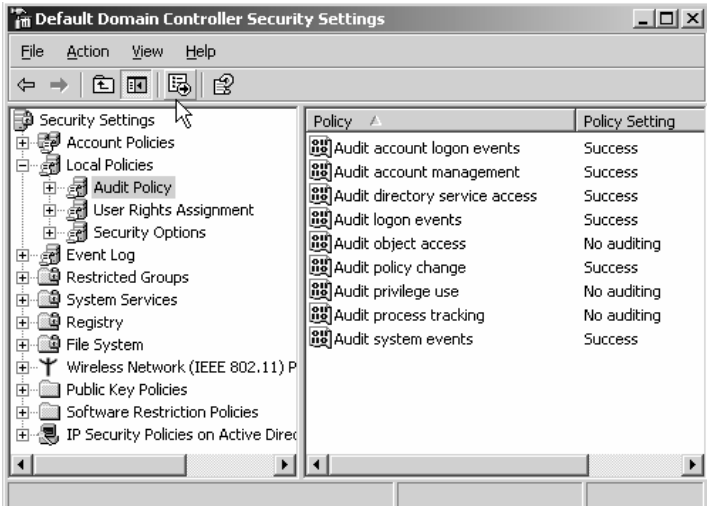


Chính sách cục bộ (**Local Policies**) cho phép bạn thiết lập các chính sách giám sát các đối tượng trên mạng như người dùng và tài nguyên dùng chung. Đồng thời dựa vào công cụ này bạn có thể cấp quyền hệ thống cho các người dùng và thiết lập các lựa chọn bảo mật.

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

## II.1. Chính sách kiểm toán.

Chính sách kiểm toán (**Audit Policies**) giúp bạn có thể giám sát và ghi nhận các sự kiện xảy ra trong hệ thống, trên các đối tượng cũng như đối với các người dùng. Bạn có thể xem các ghi nhận này thông qua công cụ **Event Viewer**, trong mục **Security**.




Các lựa chọn trong chính sách kiểm toán:

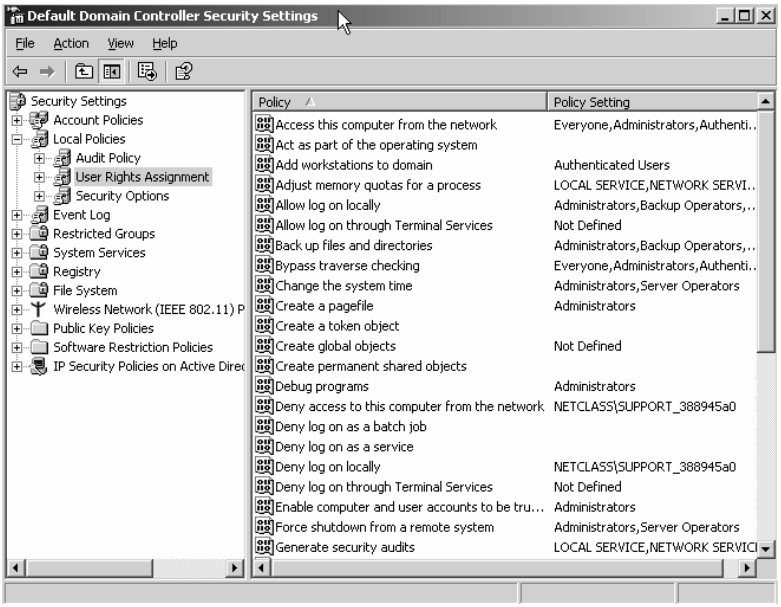
| Chính sách | Mô tả |
|---|---|
| Audit Account Logon Events | Kiểm toán những sự kiện khi tài khoản đăng nhập, hệ thống sẽ ghi nhận khi người dùng **logon**, **logoff** hoặc tạo một kết nối mạng |
| Audit Account Management | Hệ thống sẽ ghi nhận khi tài khoản người dùng hoặc nhóm có sự thay đổi thông tin hay các thao tác quản trị liên quan đến tài khoản người dùng. |
| Audit Directory Service Access | Ghi nhân việc truy cập các dịch vụ thư mục |
| Audit Logon Events | Ghi nhân các sự kiện liên quan đến quá trình logon như thi hành một **logon script** hoặc truy cập đến một **roaming profile**. |
| Audit Object Access | Ghi nhận việc truy cập các tập tin, thư mục, và máy tin. |
| Audit Policy Change | Ghi nhận các thay đổi trong chính sách kiểm toán |
| Audit privilege use | Hệ thống sẽ ghi nhận lại khi bạn bạn thao tác quản trị trên các quyền hệ thống như cấp hoặc xóa quyền của một ai đó. |
| Audit process tracking | Kiểm toán này theo dõi hoạt động của chương trình hay hệ điều hành. |
| Audit system event | Hệ thống sẽ ghi nhận mỗi khi bạn khởi động lại máy hoặc tắt máy. |



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

## II.2. Quyền hệ thống của người dùng.

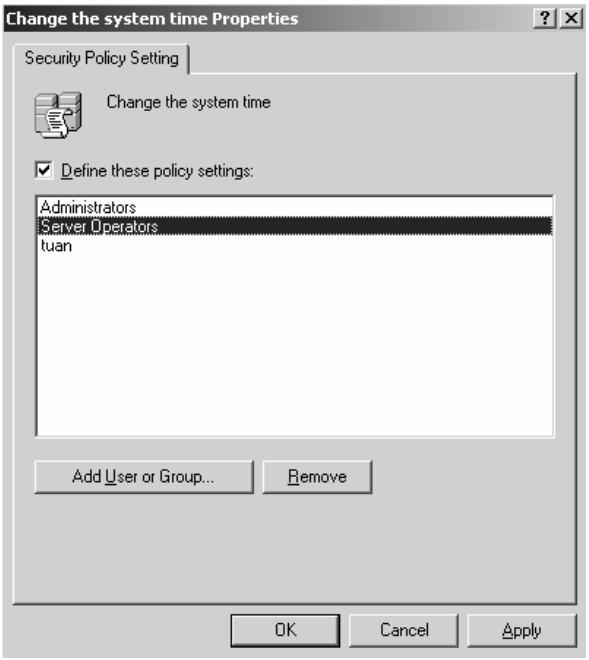
Đối với hệ thống **Windows Server 2003**, bạn có hai cách cấp quyền hệ thống cho người dùng là: gia nhập tài khoản người dùng vào các nhóm tạo sẵn (**built-in**) để kế thừa quyền hoặc bạn dùng công cụ **User Rights Assignment** để gán từng quyền rời rạc cho người dùng. Cách thứ nhất bạn đã biết sử dụng ở chương trước, chỉ cần nhớ các quyền hạn của từng nhóm tạo sẵn thì bạn có thể gán quyền cho người dùng theo yêu cầu. Để cấp quyền hệ thống cho người dùng theo theo cách thứ hai thì bạn phải dùng công cụ **Local Security Policy** (nếu máy bạn không phải **Domain Controller**) hoặc **Domain Controller Security Policy** (nếu máy bạn là **Domain Controller**). Trong hai công cụ đó bạn mở mục **Local Policy\ User Rights Assignment**.




Để thêm, bớt một quyền hạn cho người dùng hoặc nhóm, bạn nhấp đôi chuột vào quyền hạn được chọn, nó sẽ xuất hiện một hộp thoại chứa danh sách người dùng và nhóm hiện tại đang có quyền này. Bạn có thể nhấp chuột vào nút **Add** để thêm người dùng, nhóm vào danh sách hoặc nhấp chuột vào nút **Remove** để xóa người dùng khỏi danh sách. Ví dụ minh họa sau là bạn cấp quyền thay đổi giờ hệ thống (**change the system time**) cho người dùng "Tuan".



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Danh sách các quyền hệ thống cấp cho người dùng và nhóm:

| Quyền | Mô tả |
|---|---|
| Access This Computer from the Network | Cho phép người dùng truy cập máy tính thông qua mạng. Mặc định mọi người đều có quyền này. |
| Act as Part of the Operating System | Cho phép các dịch vụ chứng thực ở mức thấp chứng thực với bất kỳ người dùng nào. |
| Add Workstations to the Domain | Cho phép người dùng thêm một tài khoản máy tính vào vùng. |
| Back Up Files and Directories | Cho phép người dùng sao lưu dự phòng (**backup**) các tập tin và thư mục bất chấp các tập tin và thư mục này người đó có quyền không. |
| Bypass Traverse Checking | Cho phép người dùng duyệt qua cấu trúc thư mục nếu người dùng không có quyền xem (**list**) nội dung thư mục này. |
| Change the System Time | Cho phép người dùng thay đổi giờ hệ thống của máy tính. |
| Create a Pagefile | Cho phép người dùng thay đổi kích thước của **Page File**. |
| Create a Token Object | Cho phép một tiến trình tạo một thẻ bài nếu tiến trình này dùng **NTCreate Token API**. |
| Create Permanent Shared Objects | Cho phép một tiến trình tạo một đối tượng thư mục thông qua **Windows 2000 Object Manager**. |



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

| | |
|---|---|
| Debug Programs | Cho phép người dùng gắn một chương trình **debug** vào bất kỳ tiến trình nào. |
| Deny Access to This Computer from the Network | Cho phép bạn khóa người dùng hoặc nhóm không được truy cập đến các máy tính trên mạng. |
| Deny Logon as a Batch File | Cho phép bạn ngăn cản những người dùng và nhóm được phép logon như một **batch file**. |
| Deny Logon as a Service | Cho phép bạn ngăn cản những người dùng và nhóm được phép **logon** như một **services**. |
| Deny Logon Locally | Cho phép bạn ngăn cản những người dùng và nhóm truy cập đến máy tính cục bộ. |
| Enable Computer and User Accounts to Be Trusted by Delegation | Cho phép người dùng hoặc nhóm được ủy quyền cho người dùng hoặc một đối tượng máy tính. |
| Force Shutdown from a Remote System | Cho phép người dùng shut down hệ thống từ xa thông qua mạng |
| Generate Security Audits | Cho phép người dùng, nhóm hoặc một tiến trình tạo một **entry** vào **Security log**. |
| Increase Quotas | Cho phép người dùng điều khiển các hạn ngạch của các tiến trình. |
| Increase Scheduling Priority | Quy định một tiến trình có thể tăng hoặc giảm độ ưu tiên đã được gán cho tiến trình khác. |
| Load and Unload Device Drivers | Cho phép người dùng có thể cài đặt hoặc gỡ bỏ các driver của các thiết bị. |
| Lock Pages in Memory | Khóa trang trong vùng nhớ. |
| Log On as a Batch Job | Cho phép một tiến trình **logon** vào hệ thống và thi hành một tập tin chứa các lệnh hệ thống. |
| Log On as a Service | Cho phép một dịch vụ **logon** và thi hành một dịch vụ riêng. |
| Log On Locally | Cho phép người dùng **logon** tại máy tính **Server**. |
| Manage Auditing and Security Log | Cho phép người dùng quản lý **Security log**. |



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

| | |
|---|---|
| Modify Firmware Environment Variables | Cho phép người dùng hoặc một tiến trình hiệu chỉnh các biến môi trường hệ thống. |

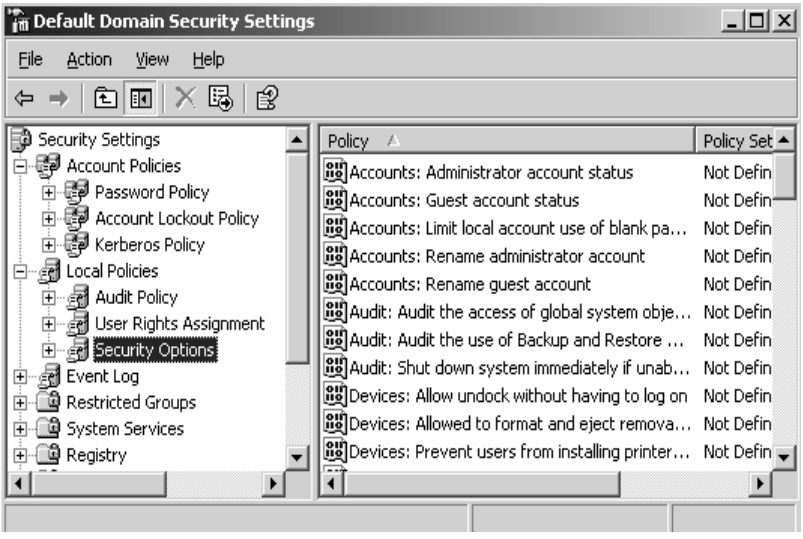


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

| | |
|---|---|
| Profile Single Process | Cho phép người dùng giám sát các tiến trình bình thường thông qua công cụ **Performance Logs and Alerts**. |
| Profile System Performance | Cho phép người dùng giám sát các tiến trình hệ thống thông qua công cụ **Performance Logs and Alerts**. |
| Remove Computer from Docking Station | Cho phép người dùng gỡ bỏ một **Laptop** thông qua giao diện người dùng của **Windows 2000**. |
| Replace a Process Level Token | Cho phép một tiến trình thay thế một token mặc định mà được tạo bởi một tiến trình con. |
| Restore Files and Directories | Cho phép người dùng phục hồi tập tin và thư mục, bất chấp người dùng này có quyền trên tập tin và thư mục này hay không. |
| Shut Down the System | Cho phép người dùng **shut down** cục bộ máy **Windows 2000**. |
| Synchronize Directory Service Data | Cho phép người dùng đồng bộ dữ liệu với một dịch vụ thư mục. |
| Take Ownership of Files or Other Objects | Cho người dùng tước quyền sở hữu của một đối tượng hệ thống. |

## II.3. Các lựa chọn bảo mật.

Các lựa chọn bảo mật (**Security Options**) cho phép người quản trị **Server** khai báo thêm các thông số nhằm tăng tính bảo mật cho hệ thống như: không cho phép hiển thị người dùng đã **logon** trước đó hay đổi tên tài khoản người dùng tạo sẵn (**administrator, guest**). Trong hệ thống **Windows Server 2003** hỗ trợ cho chúng ta rất nhiều lựa chọn bảo mật, nhưng trong giáo trình này chúng ta chỉ khảo sát các lựa chọn thông dụng.






Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Một số lựa chọn bảo mật thông dụng:

| Tên lựa chọn | Mô tả |
|---|---|
| Shutdown: allow system to be shut down without having to log on | Cho phép người dùng **shutdown** hệ thống mà không cần logon. |
| Audit : audit the access of global system objects | Giám sát việc truy cập các đối tượng hệ thống toàn cục. |
| Network security: force logoff when logon hours expires. | Tự động **logoff** khỏi hệ thống khi người dùng hết thời gian sử dụng hoặc tài khoản hết hạn. |
| Interactive logon: do not require CTRL+ALT+DEL | Không yêu cầu ấn ba phím **CTRL+ALT+DEL** khi logon. |
| Interactive logon: do not display last user name | Không hiển thị tên người dùng đã logon trên hộp thoại **Logon**. |
| Account: rename administrator account | Cho phép đổi tên tài khoản **Administrator** thành tên mới |
| Account: rename guest account | Cho phép đổi tên tài khoản **Guest** thành tên mới |

# III. IPSec.

**IP Security (IPSec)** là một giao thức hỗ trợ thiết lập các kết nối an toàn dựa trên **IP**. Giao thức này hoạt động ở tầng ba (**Network**) trong mô hình **OSI** do đó nó an toàn và tiện lợi hơn các giao thức an toàn khác ở tầng **Application** như **SSL**. **IPSec** cũng là một thành phần quan trọng hỗ trợ giao thức **L2TP** trong công nghệ mạng riêng ảo **VPN (Virtual Private Network).** Để sử dụng **IPSec** bạn phải tạo ra các qui tắc (**rule**), một qui tắc **IPSec** là sự kết hợp giữa hai thành phần là các bộ lọc **IPSec (filter)** và các tác động **IPSec (action).** Ví dụ nội dung của một qui tắc **IPSec** là "Hãy mã hóa tất cả những dữ liệu truyền **Telnet** từ máy có địa chỉ 192.168.0.10", nó gồm hai phần, phần bộ lọc là "qui tắc này chỉ hoạt động khi có dữ liệu được truyền từ máy có địa chỉ 192.168.0.10 thông qua cổng 23", phần hành động là "mã hóa dữ liệu.

## III.1. Các tác động bảo mật.

**IPSec** của Microsoft hỗ trợ bốn loại tác động (**action**) bảo mật, các tác động bảo mật này giúp hệ thống có thể thiết lập những cuộc trao đổi thông tin giữa các máy được an toàn. Danh sách các tác động bảo mật trong hệ thống **Windows Server 2003** như sau:

- **Block transmissons**: có chức năng ngăn chặn những gói dữ liệu được truyền, ví dụ bạn muốn **IPSec** ngăn chặn dữ liệu truyền từ máy A đến máy B, thì đơn giản là chương trình **IPSec** trên máy B loại bỏ mọi dữ liệu truyền đến từ máy A.
- **Encrypt transmissions**: có chức năng mã hóa những gói dữ liệu được truyền, ví dụ chúng ta



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

muốn dữ liệu được truyền từ máy A đến máy B, nhưng chúng ta sợ rằng có người sẽ nghe trộm



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

trên đường truyền nối kết mạng giữa hai máy A và B. Cho nên chúng ta cần cấu hình cho **IPSec** sử dụng giao thức **ESP** (**encapsulating security payload**) để mã hóa dữ liệu cần truyền trước khi đưa lên mạng. Lúc này những người xem trộm sẽ thấy những dòng **byte** ngẫu nhiên và không hiểu được dữ liệu thật. Do **IPSec** hoạt động ở tầng **Network** nên hầu như việc mã hóa được trong suốt đối với người dùng, người dùng có thể gởi **mail**, truyền **file** hay **telnet** như bình thường.

- **Sign transmissions**: có chức năng ký tên vào các gói dữ liệu truyền, nhằm tránh những kẻ tấn công trên mạng giả dạng những gói dữ liệu được truyền từ những máy mà bạn đã thiết lập quan hệ tin cậy, kiểu tấn công này còn có cái tên là **main-in-the-middle**. **IPSec** cho phép bạn chống lại điều này bằng một giao thức **authentication header**. Giao thức này là phương pháp ký tên số hóa (**digitally signing**) vào các gói dữ liệu trước khi truyền, nó chỉ ngăn ngừa được giả mạo và sai lệnh thông tin chứ không ngăn được sự nghe trộm thông tin. Nguyên lý hoạt động của phương pháp này là hệ thống sẽ thêm một **bit** vào cuối mỗi gói dữ liệu truyền qua mạng, từ đó chúng ta có thể kiểm tra xem dữ liệu có bị thay đổi khi truyền hay không.
- **Permit transmissions**: có chức năng là cho phép dữ liệu được truyền qua, chúng dùng để tạo ra các qui tắc (**rule**) hạn chế một số điều và không hạn chế một số điều khác. Ví dụ một qui tắc dạng này "Hãy ngăn chặn tất cả những dữ liệu truyền tới, chỉ trừ dữ liệu truyền trên các cổng 80 và 443".

Chú ý: đối với hai tác động bảo mật theo phương pháp ký tên và mã hóa thì hệ thống còn yêu cầu bạn chỉ ra l**IPSec** dùng phương pháp chứng thực nào. **Microsoft** hỗ trợ ba phương pháp chứng thực: **Kerberos**, chứng chỉ (**certificate**) hoặc một khóa dựa trên sự thỏa thuận (**agreed-upon key**). Phương pháp **Kerberos** chỉ áp dụng được giữa các máy trong cùng một miền **Active Directory** hoặc trong những miền **Active Directory** có ủy quyền cho nhau. Phương pháp dùng các chứng chỉ cho phép bạn sử dụng các chứng chỉ **PKI** (**public key infrastructure**) để nhận diện một máy. Phương pháp dùng chìa khóa chia sẻ trước thì cho phép bạn dùng một chuỗi ký tự văn bản thông thường làm chìa khóa (**key**).

## III.2. Các bộ lọc IPSec.

Để **IPSec** hoạt động linh hoạt hơn, **Microsoft** đưa thêm khái niệm bộ lọc (**filter**) **IPSec**, bộ lọc có tác dụng thống kê các điều kiện để qui tắc hoạt động. Đồng thời chúng cũng giới hạn tầm tác dụng của các tác động bảo mật trên một phạm vị máy tính nào đó hay một số dịch vụ nào đó. Bộ lọc **IPSec** chủ yếu dự trên các yếu tố sau:

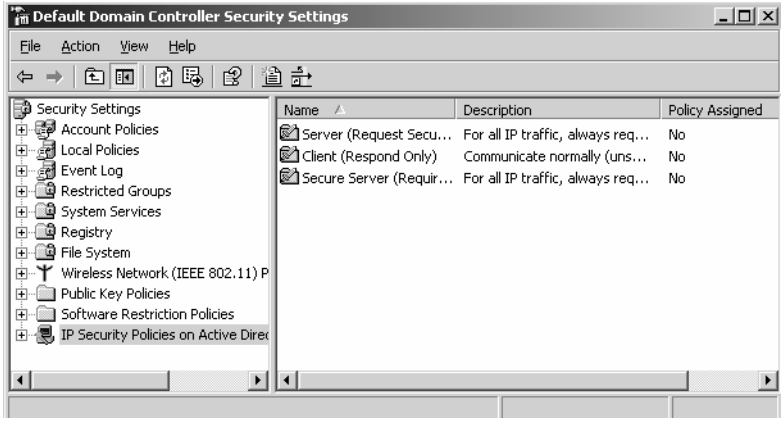
- Địa chỉ **IP**, subnet hoặc tên **DNS** của máy nguồn.
- Địa chỉ **IP**, subnet hoặc tên **DNS** của máy đích.
- Theo số hiệu cổng (**port**) và kiển cổng (**TCP, UDP, ICMP**…)

## III.3. Triển khai IPSec trên Windows Server 2003.

Trong hệ thống **Windows Server 2003** không hỗ trợ một công cụ riêng cấu hình **IPSec**, do đó để triển khai I**PSec** chúng ta dùng các công cụ thiết lập chính sách dành cho máy cục bộ hoặc dùng cho miền. Để mở công cụ cấu hình **IPSec** bạn nhấp chuột vào **Start** ◴ **Run** rồi gõ **secpol.msc** hoặc nhấp chuột vào **Start** ◴ **Programs** ◴ **Administrative Tools** ◴ **Local Security Policy**, trong công cụ đó bạn chọn **IP Security Policies on Local Machine**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Tóm lại, các điều mà bạn cần nhớ khi triển khai **IPSec**:

- Bạn triển khai **IPSec** trên **Windows Server 2003** thông qua các chính sách, trên một máy tính bất kỳ nào đó vào tại một thời điểm thì chỉ có một chính sách **IPSec** được hoạt động.
- Mỗi chính sách **IPSec** gồm một hoặc nhiều qui tắc (**rule**) và một phương pháp chứng thực nào đó. Mặc dù các qui tắc **permit** và **block** không dùng đến chứng thực nhưng **Windows** vẫn đòi bạn chỉ định phương pháp chứng thực.
- **IPSec** cho phép bạn chứng thực thông qua **Active Directory**, các chứng chỉ **PKI** hoặc một khóa được chia sẻ trước.
- Mỗi qui tắc (**rule**) gồm một hay nhiều bộ lọc (**filter**) và một hay nhiều tác động bảo mật (**action**).
- Có bốn tác động mà qui tắc có thể dùng là: **block**, **encrypt**, **sign** và **permit**.

### III.3.1 Các chính sách IPSec tạo sẵn.

Trong khung cửa sổ chính của công cụ cấu hình **IPSec**, bên phải chúng ta thấy xuất hiện ba chính sách được tạo sẵn tên là: **Client**, **Server** và **Secure**. Cả ba chính sách này đều ở trạng thái chưa áp dụng (**assigned**). Nhưng chú ý ngay cùng một thời điểm thì chỉ có thể có một chính sách được áp dụng và hoạt động, có nghĩa là khi bạn áp dụng một chính sách mới thì chính sách đang hoạt động hiện tại sẽ trở về trạng thái không hoạt động. Sau đây chúng ta sẽ khảo sát chi tiết ba chính sách tạo sẵn này.

- **Client (Respond Only)**: chính sách qui định máy tính của bạn không chủ động dùng **IPSec** trừ khi nhận được yêu cầu dùng **IPSec** từ máy đối tác. Chính sách này cho phép bạn có thể kết nối được cả với các máy tính dùng **IPSec** hoặc không dùng **IPSec**.
- **Server (Request Security)**: chính sách này qui định máy server của bạn chủ động cố gắng khởi tạo **IPSec** mỗi khi thiết lập kết nối với các máy tính khác, nhưng nếu máy **client** không thể dùng **IPSec** thì **Server** vẫn chấp nhận kết nối không dùng **IPSec**.
- **Secure Server (Require Security)**: chính sách này qui định không cho phép bất kỳ cuộc trao đổi dữ liệu nào với **Server** hiện tại mà không dùng **IPSec**.

### III.3.2 Ví dụ tạo chính sách IPSec đảm bảo một kết nối được mã hóa.



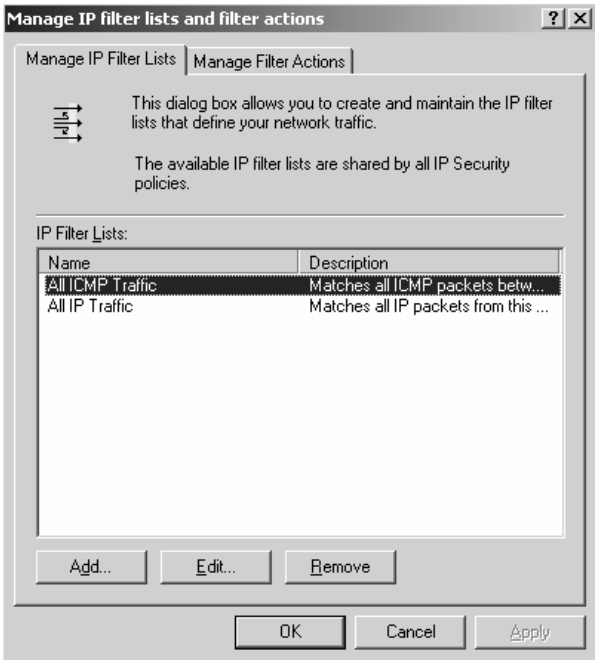
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Trong phần này chúng ta bắt tay vào thiết lập một chính sách **IPSec** nhằm đảm bảo một kết nối được mã hóa giữa hai máy tính. Chúng ta có hai máy tính, máy A có địa chỉ 203.162.100.1 và máy B có địa chỉ 203.162.100.2. Chúng ta sẽ thiết lập chính sách I**PSec** trên mỗi máy thêm hai qui tắc (**rule**), trừ hai qui tắc của hệ thống gồm: một qui tắc áp dụng cho dữ liệu truyền vào máy và một qui tắc áp dụng cho dữ liệu truyền ra khỏi máy. Ví dụ qui tắc đầu tiên trên máy A bao gồm:

- Bộ lọc **(filter):** kích hoạt qui tắc này khi có dữ liệu truyền đến địa chỉ 203.162.100.1, qua bất kỳ cổng nào.
- Tác động bảo mật (**action**): mã hóa dữ liệu đó.
- Chứng thực: chìa khóa chia sẻ trước là chuỗi "quantri".

Qui tắc thứ hai áp dụng cho máy A cũng tương tự nhưng bộ lọc có nội dung ngược lại là "dữ liệu truyền đi từ địa chỉ 203.162.100.1". Chú ý: cách dễ nhất để tạo ra một qui tắc là trước tiên bạn phải qui định các bộ lọc và tác động bảo mật, rồi sau đó mới tạo ra qui tắc từ các bộ lọc và tác động bảo mật này. Các bước để thực hiện một chính sách **IPSec** theo yêu cầu như trên:

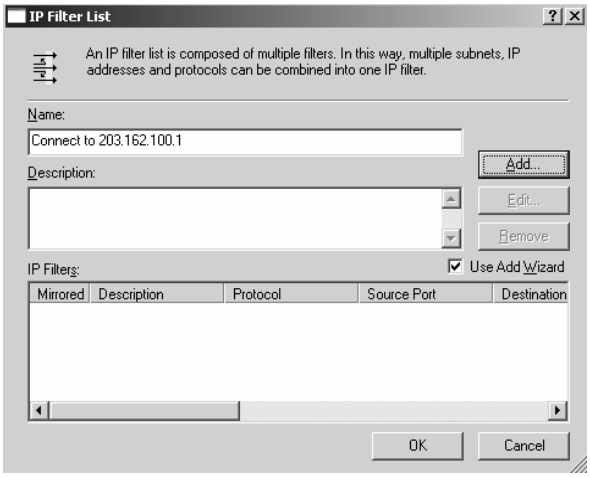
Trong công cụ **Domain Controller Security Policy**, bạn nhấp phải chuột trên mục **IP Security Policies on Active Directory**, rồi chọn **Manage IP filter lists and filter actions**.



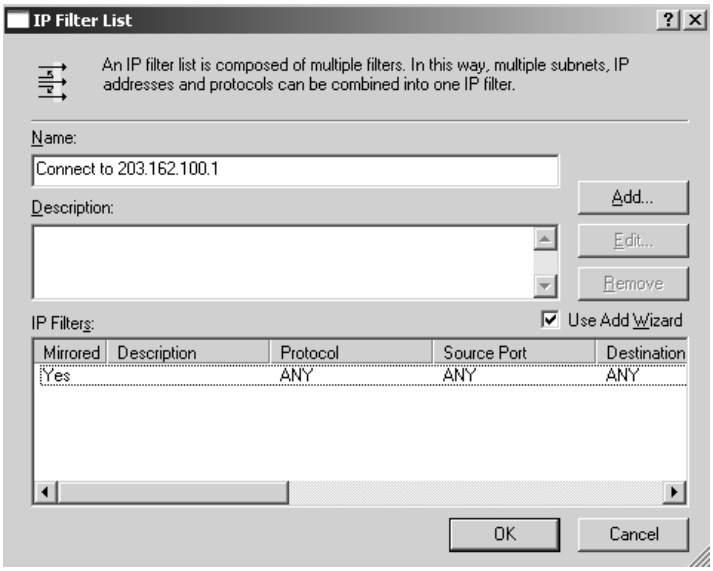

Hộp thoại xuất hiện, bạn nhấp chuột vào nút **add** để thêm một bộ lọc mới. Bạn nhập tên cho bộ lọc này, trong ví dụ này chúng ta đặt tên là "**Connect to 203.162.100.1**". Bạn nhấp chuột tiếp vào nút **Add** để hệ thống hướng dẫn bạn khai báo các thông tin cho bộ lọc.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Bạn theo hướng dẫn của hệ thống để khai báo các thông tin, chú ý nên đánh dấu vào mục **Mirrored** để qui tắc này có ý nghĩa hai chiều bạn không phải tốn công để tạo ra hai qui tắc. Mục **Source address** chọn **My IP Address**, mục **Destination address** chọn **A specific IP Address** và nhập địa chỉ "203.162.100.1" vào, mục **IP Protocol Type** bạn để mặc định. Cuối cùng bạn chọn **Finish** để hoàn thành phần khai báo, bạn nhấp chuột tiếp vào nút **OK** để trở lại hộp thoại đầu tiên.

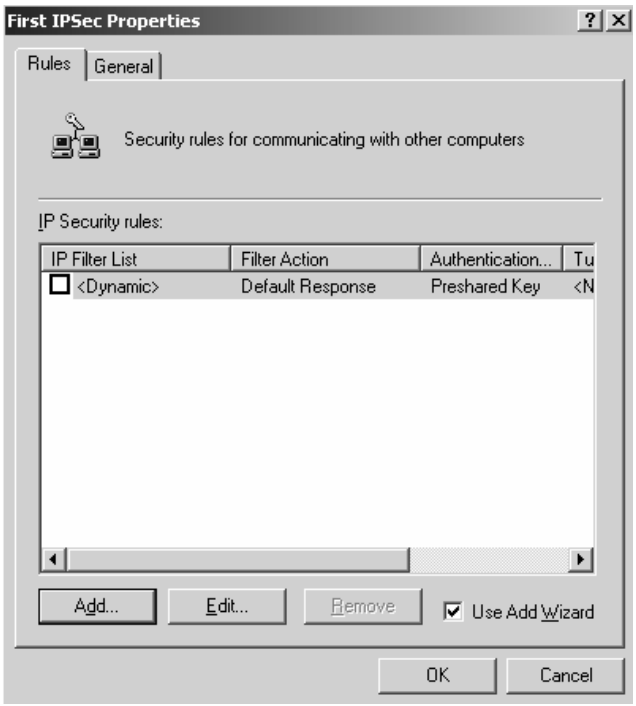



Tiếp theo bạn chuyển sang Tab **Manage Filter Actions** để tạo ra các tác động bảo mật. Bạn nhấp chuột vào nút **Add** hệ thống sẽ hướng dẫn bạn khai báo các thông tin về tác động. Trước tiên bạn đặt tên cho tác động này, ví dụ như là **Encrypt**.Tiếp tục trong mục **Filter Action** bạn chọn **Negotiate security**, trong mục **IP Traffic Security** bạn chọn **Integrity and encryption**. Đến đây bạn đã hoàn thành việc tạo một tác động bảo mật.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

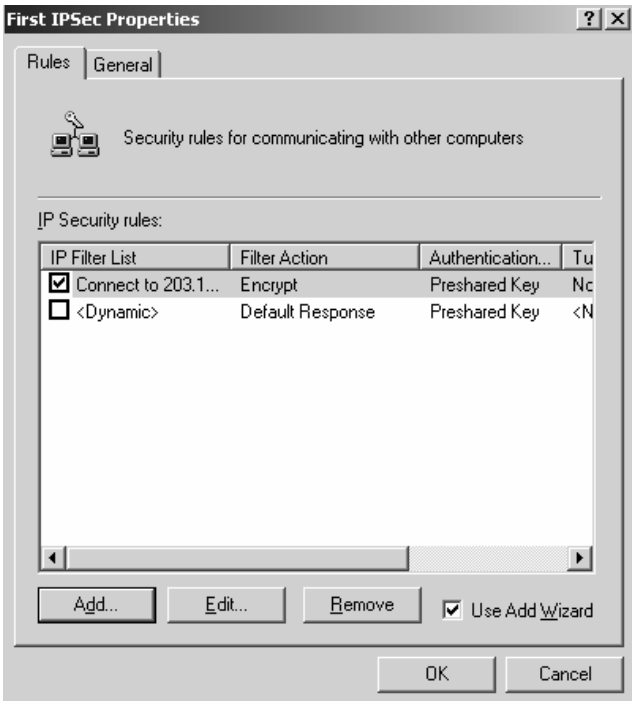

Công việc tiếp theo là bạn một chính sách **IPSec** trong đó có chứa một qui tắc kết hợp giữa bộ lọc và tác động vừa tạo ở phía trên. Trong công cụ **Domain Controller Security Policy**, bạn nhấp phải chuột trên mục **IP Security Policies on Active Directory**, rồi chọn **Create IP Security Policy**, theo hướng dẫn bạn nhập tên của chính vào, ví dụ là **First IPSec**, tiếp theo bạn phải bỏ đánh dấu trong mục **Active the default response rule**. Các giá trị còn lại bạn để mặc định vì qui tắc **Dynamic** này chúng ta không dùng và sẽ tạo ra một qui tắc mới.



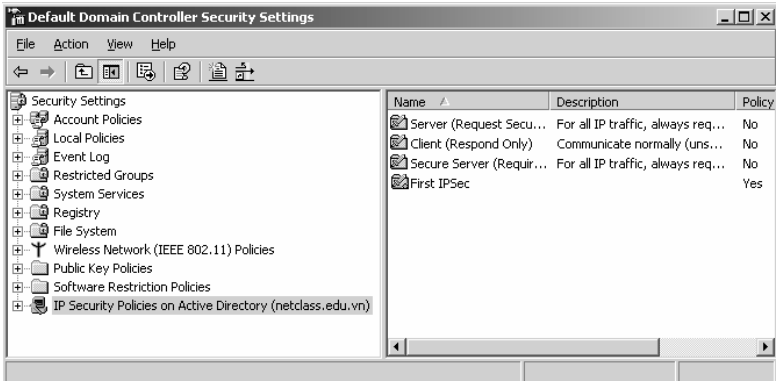



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Trong hộp thoại chính sách **IPSec**, bạn nhấp chuột vào nút **Add** để tạo ra qui tắc mới. Hệ thống sẽ hướng dẫn bạn từng bước thực hiện, đến mục chọn bộ lọc bạn chọn bộ lọc vừa tạo phía trên tên "**Connect to 203.162.100.1**", mục chọn tác động bạn chọn tác động vừa tạo tên **Encypt**. Đến mục chọn phương pháp chứng thực bạn chọn mục **Use this string to protect the key exchange** và nhập chuỗi làm khóa để mã hóa dữ liệu vào, trong ví dụ này là "quantri".




Đến bước này thì công việc thiết lập chính sách **IPSec** theo yêu cầu trên của bạn đã hoàn thành, trong khung của sổ chính của công cụ **Domain Controller Security Policy,** bạn nhấp phải chuột lên chính sách **First IPSec** và chọn **Assign** để chính sách này được hoạt động trên hệ thống **Server**.






Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Bài 12
CHÍNH SÁCH NHÓM

# Tóm tắt

Lý thuyết 3 tiết - Thực hành 3 tiết

| Mục tiêu | Các mục chính | Bài tập bắt buộc | Bài tập làm thêm |
|---|---|---|---|
| Kết thúc bài học này cung cấp học viên kiến thức về Group Policy, các chính sách đối với máy trạm, chính sách đối với người dùng… | I. Giới thiệu về chính sách nhóm.<br>II. Triển khai một chính sách nhóm trên miền.<br>III. Các ví dụ minh họa. | Dựa vào bài tập môn Quản trị Windows Server 2003. | Dựa vào bài tập môn Quản trị Windows Server 2003. |



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

# I. GIỚI THIỆU.

## I.1. So sánh giữa System Policy và Group Policy.

Vừa rồi ở chương trước, chúng ta đã tìm hiểu về chính sách hệ thống (**System Policy**), tiếp theo chúng ta sẽ tìm hiểu về chính sách nhóm (**Group Policy**). Vậy hai chính sách này khác nhau như thế nào.

- Chính sách nhóm chỉ xuất hiện trên miền **Active Directory** , nó không tồn tại trên miền **NT4**.
- Chính sách nhóm làm được nhiều điều hơn chính sách hệ thống. Tất nhiên chính sách nhóm chứa tất cả các chức năng của chính sách hệ thống và hơn thế nữa, bạn có thể dùng chính sách nhóm để triển khai một phần mềm cho một hoặc nhiều máy một cách tự động.
- Chính sách nhóm tự động hủy bỏ tác dụng khi được gỡ bỏ, không giống như các chính sách hệ thống.
- Chính sách nhóm được áp dụng thường xuyên hơn chính sách hệ thống. Các chính sách hệ thống chỉ được áp dụng khi máy tính đăng nhập vào mạng thôi. Các chính sách nhóm thì được áp dụng khi bạn bật máy lên, khi đăng nhập vào một cách tự động vào những thời điểm ngẫu nhiên trong suốt ngày làm việc.
- Bạn có nhiều mức độ để gán chính sách nhóm này cho người từng nhóm người hoặc từng nhóm đối tượng.
- Chính sách nhóm tuy có nhiều ưu điểm nhưng chỉ áp dụng được trên máy **Win2K**, **WinXP** và **Windows Server 2003**.

## I.2. Chức năng của Group Policy.

- **Triển khai phần mềm ứng dụng**: bạn có thể gom tất cả các tập tin cần thiết để cài đặt một phần mềm nào đó vào trong một gói (**package**), đặt nó lên **Server**, rồi dùng chính sách nhóm hướng một hoặc nhiều máy trạm đến gói phần mềm đó. Hệ thống sẽ tự động cài đặt phần mềm này đến tất cả các máy trạm mà không cần sự can thiệp nào của người dùng.
- **Gán các quyền hệ thống cho người dùng**: chức năng này tương tự với chức năng của chính sách hệ thống. Nó có thể cấp cho một hoặc một nhóm người nào đó có quyền tắt máy **server**, đổi giờ hệ thống hay **backup** dữ liệu…
- **Giới hạn những ứng dụng mà người dùng được phép thi hành**: chúng ta có thể kiểm soát máy trạm của một người dùng nào đó và cho phép người dùng này chỉ chạy được một vài ứng dụng nào đó thôi như: **Outlook Express**, **Word** hay **Internet Explorer**.
- **Kiểm soát các thiết lập hệ thống**: bạn có thể dùng chính sách nhóm để qui định hạn ngạch đĩa cho một người dùng nào đó. Người dùng này chỉ được phép lưu trữ tối đa bao nhiêu MB trên đĩa cứng theo qui định.
- **Thiết lập các kịch bản đăng nhập, đăng xuất, khởi động và tắt máy**: trong hệ thống NT4 thì chỉ hỗ trợ kịch bản đăng nhập (**logon script**), nhưng **Windows 2000** và **Windows Server 2003** thì hỗ trợ cả bốn sự kiện này được kích hoạt (**trigger**) một kịch bản (**script**). Bạn có thể dùng các **GPO** để kiểm soát những kịch bản nào đang chạy.
- **Đơn giản hóa và hạn chế các chương trình**: bạn có thể dùng **GPO** để gỡ bỏ nhiều tính năng khỏi Internet **Explorer**, **Windows Explorer** và những chương trình khác.

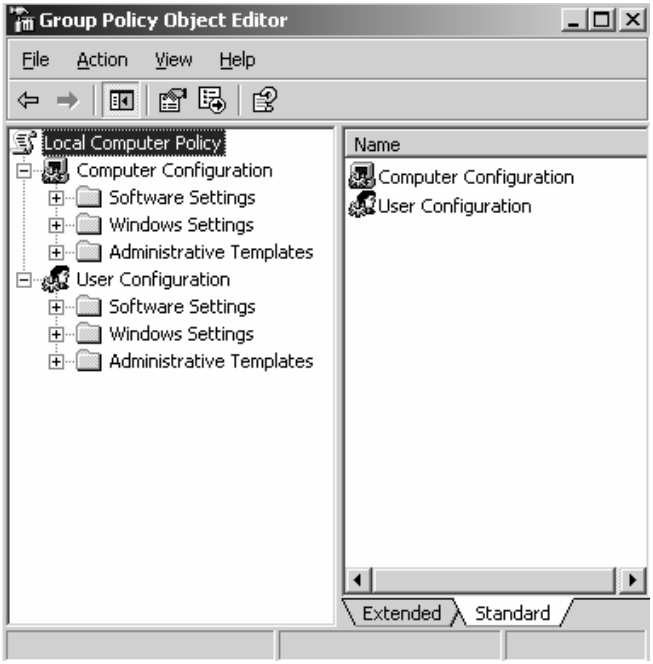


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

- Hạn chế tổng quát màn hình Desktop của người dùng: bạn có thể gỡ bỏ hầu hết các đề mục trên menu **Start** của một người dùng nào đó, ngăn chặn không cho người dùng cài thêm máy in, sửa đổi thông số cấu hình của máy trạm…

# II. TRIỂN KHAI MỘT CHÍNH SÁCH NHÓM TRÊN MIỀN.

Chúng ta cấu hình và triển khai **Group Policy** bằng cách xây dựng các đối tượng chính sách (**GPO**). Các **GPO** là một vật chứa (**container**) có thể chứa nhiều chính sách áp dụng cho nhiều người, nhiều máy tính hay toàn bộ hệ thống mạng. Bạn dùng chương trình **Group Policy Object Editor** để tạo ra các đối tượng chính sách. Trong của sổ chính của **Group Policy Object Editor** có hai mục chính: cấu hình máy tính (**computer configuration**) và cấu hình người dùng (**user configuration**).




Điều kế tiếp bạn cũng chú ý khi triển khai **Group Policy** là các cấu hình chính sách của **Group Policy** được tích lũy và kề thừa từ các vật chứa (**container**) bên trên của **Active Directory**. Ví dụ các người dùng và máy tính vừa ở trong miền vừa ở trong **OU** nên sẽ nhận được các cấu hình từ cả hai chính sách cấp miền lẫn chính sách cấp **OU**. Các chính sách nhóm sau 90 phút sẽ được làm tươi và áp dụng một lần, nhưng các chính nhóm trên các **Domain Controller** được làm tươi 5 phút một lần. Các **GPO** hoạt động được không chỉ nhờ chỉnh sửa các thông tin trong **Registry** mà còn nhờ các thư viện liên kết động (**DLL**) làm phần mở rộng đặt tại các máy trạm. Chú ý nếu bạn dùng chính sách nhóm thì chính sách nhóm tại chỗ trên máy cục bộ sẽ xử lý trước các chính sách dành cho **site**, miền hoặc **OU**.

## II.1. Xem chính sách cục bộ của một máy tính ở xa.

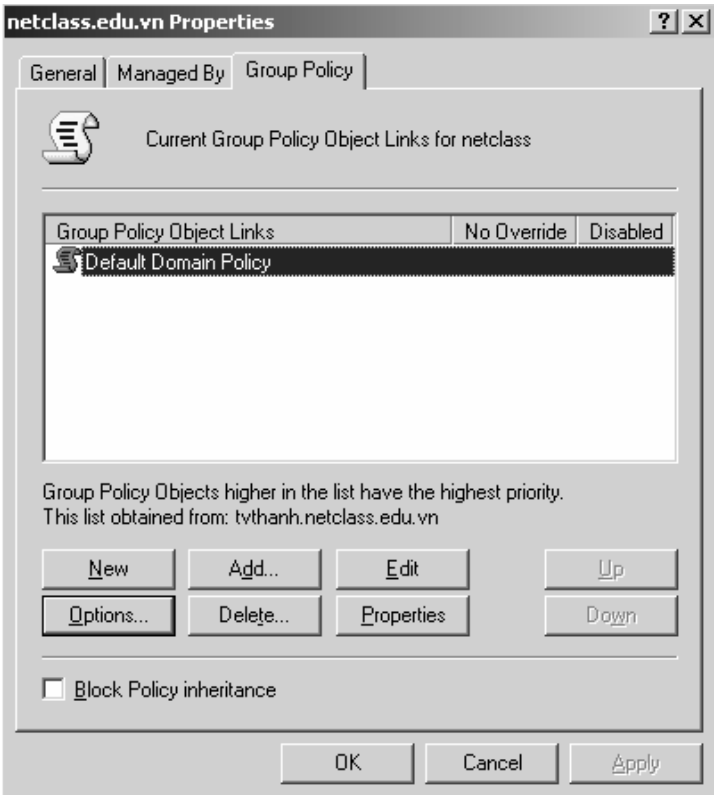
Để xem một chính sách cục bộ trên các máy tính khác trong miền, bạn phải có quyền quản trị trên máy đó hoặc quản trị miền. Lúc đó bạn có thể dùng lệnh **GPEDIT.MSC /gpcomputer:machinename**, ví dụ bạn muốn xem chính sách trên máy PCO1 bạn gõ lệnh **GPEDIT.MSC /gpcomputer: PCO1**. Chú ý là bạn không thể dùng cách này để thiết lập các chính sách nhóm ở máy tính ở xa, do tính chất bảo mật **Microsoft** không cho phép bạn ở xa thiết lập các chính sách nhóm.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

## II.2. Tạo các chính sách trên miền.

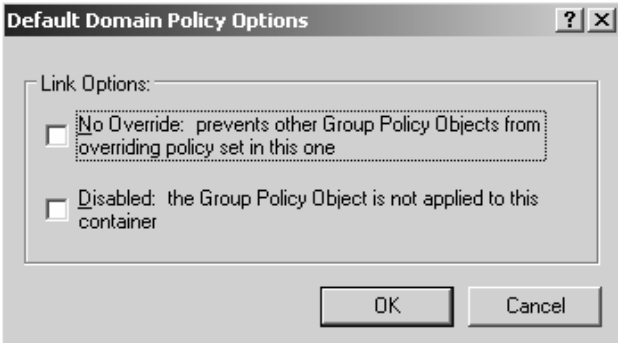
Chúng ta dùng **snap-in Group Policy** trong **Active Directory User and Computer** hoặc gọi trực tiếp tiện ích **Group Policy Object Editor** từ dòng lệnh trên máy **Domain Controller** để tạo ra các chính sách nhóm cho miền. Nếu bạn mở **Group Policy** từ **Active Directory User and Computer** thì trong khung cửa sổ chính của chương trình bạn nhấp chuột phải vào biểu tượng tên miền (trong ví dụ này là netclass.edu.vn), chọn **Properties**. Trong hộp thoại xuất hiện bạn chọn **Tab Group Policy**.



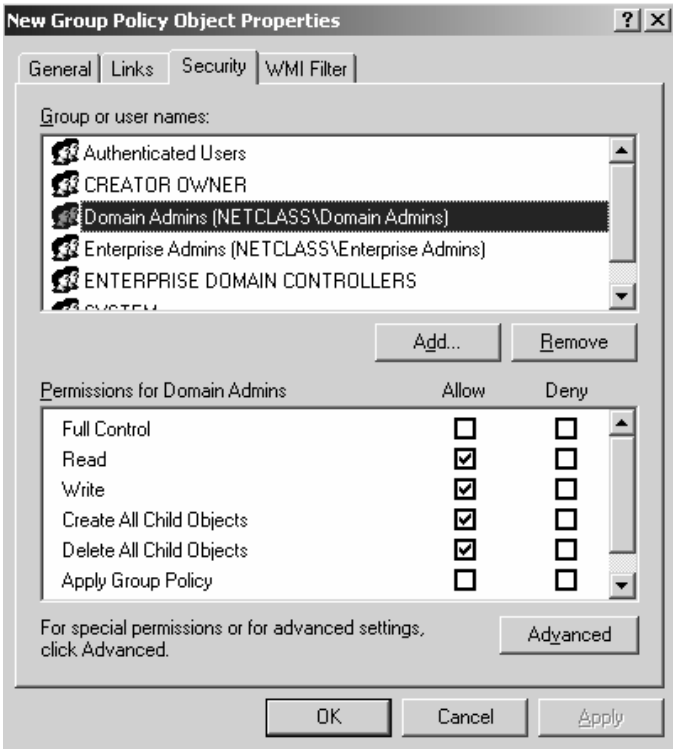

Nếu bạn chưa tạo ra một chính sách nào thì bạn chỉ nhìn thấy một chính sách tên **Default Domain Policy**. Cuối hộp thoại có một **checkbox** tên **Block Policy inheritance**, chức năng của mục này là ngăn chặn các thiết định của mọi chính sách bất kỳ ở cấp cao hơn lan truyền xuống đến cấp đang xét. Chú ý rằng chính sách được áp dụng đầu tiên ở cấp **site**, sau đó đến cấp miền và cuối cùng là cấp **OU**. Bạn chọn chính sách **Default Domain Policy** và nhấp chuột vào nút **Option** để cấu hình các lựa chọn việc áp dụng chính sách. Trong hộp thoại **Options**, nếu bạn đánh dấu vào mục **No Override** thì các chính sách khác được áp dụng ở dòng dưới sẽ không phủ quyết được những thiết định của chính sách này, cho dù chính sách đó không đánh dấu vào mục **Block Policy inheritance**. Tiếp theo nếu bạn đánh dấu vào mục **Disabled**, thì chính sách này sẽ không hoạt động ở cấp này, Việc **disbale** chính sách ở một cấp không làm **disable** bản thân đối tượng chính sách.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net



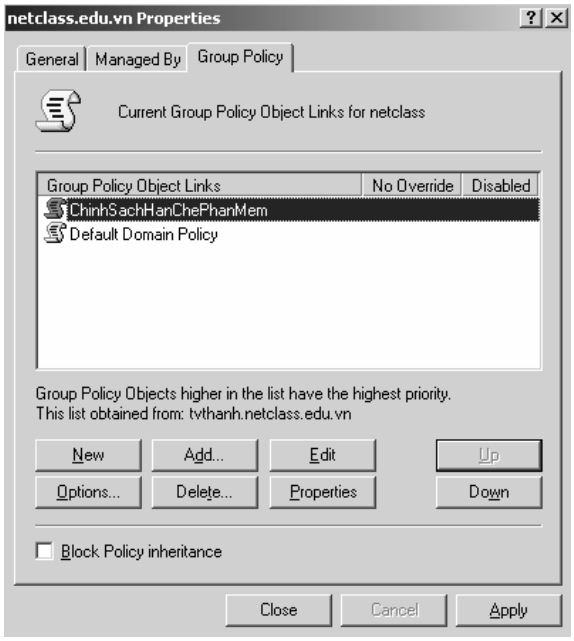

Để tạo ra một chính sách mới bạn nhấp chuột vào nút **New**, sau đó nhập tên của chính sách mới. Để khai báo thêm thông tin cho chính sách này bạn có thể nhấp chuột vào nút **Properties**, hộp thoại xuất hiện có nhiều **Tab**, bạn có thể vào **Tab Links** để chỉ ra các **site**, **domain** hoặc **OU** nào liên kết với chinh sách. Trong **Tab Security** cho phép bạn cấp quyền cho người dùng hoặc nhóm người dùng có quyền gì trên chính sách này.



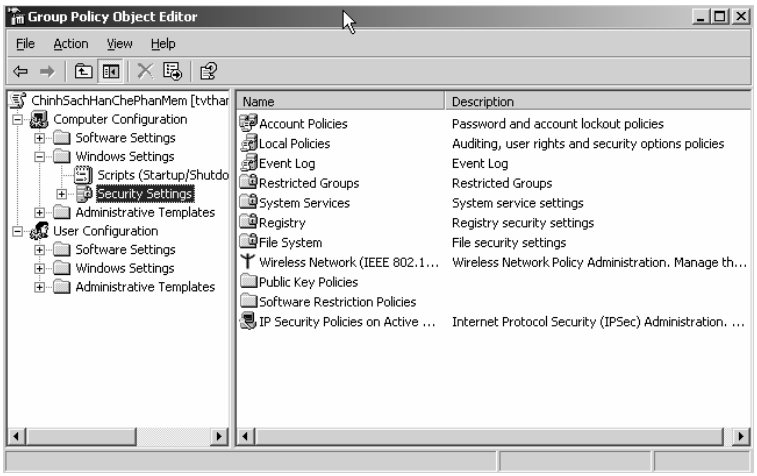

Trong hộp thoại chính của **Group Policy** thì các chính sách được áp dụng từ dưới lên trên, cho nên chính sách nằm trên cùng sẽ được áp dụng cuối cùng. Do đó, các **GPO** càng nằm trên cao trong danh sách thì càng có độ ưu tiên cao hơn, nếu chúng có những thiết định mâu thuẫn nhau thì chính sách nào nằm trên sẽ thắng. Vì lý do đó nên **Microsoft** thiết kế hai nút **Up** và **Down** giúp chúng ta có thể di chuyển các chính sách này lên hay xuống.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Trong các nút  mà chúng ta chưa khảo sát thì có một nút quan trọng nhất trong hộp thoại này đó là nút **Edit**. Bạn nhấp chuột vào nút **Edit** để thiết lập các thiết định cho chính sách này, dựa trên các khả năng của **Group Policy** bạn có thể thiết lập bất cứ thứ gì mà bạn muốn. Chúng ta sẽ khảo sát một số ví dụ minh họa ở phía sau.




# III. MỘT SỐ MINH HỌA GPO TRÊN NGƯỜI DÙNG VÀ CẤU HÌNH MÁY.

## III.1. Khai báo một logon script dùng chính sách nhóm.

Trong **Windows Server 2003** hỗ trợ cho chúng ta bốn sự kiện để có thể kích hoạt các kịch bản (**script**) hoạt động là: **startup**, **shutdown, logon, logoff**. Trong công cụ **Group Policy Object Editor**, bạn có thể vào **Computer Configuration** 🕘 **Windows Setttings** 🕘 **Scripts** để khai báo các kịch bản sẽ hoạt động khi **startup, shutdown**. Đồng thời để khai báo các kịch bản sẽ hoạt động khi **logon, logoff** thì bạn vào **User Configuration** 🕘 **Windows Setttings** 🕘 **Scripts**. Trong ví dụ này chúng ta



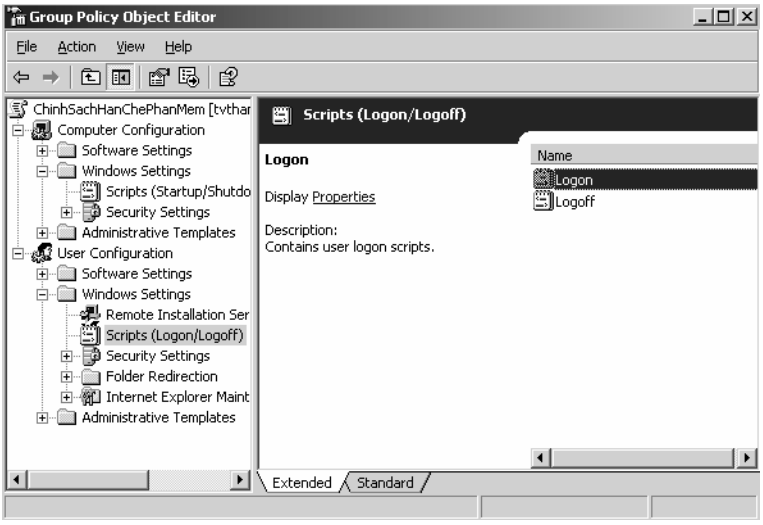
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

tạo một **logon script**, quá trình gồm các bước sau:

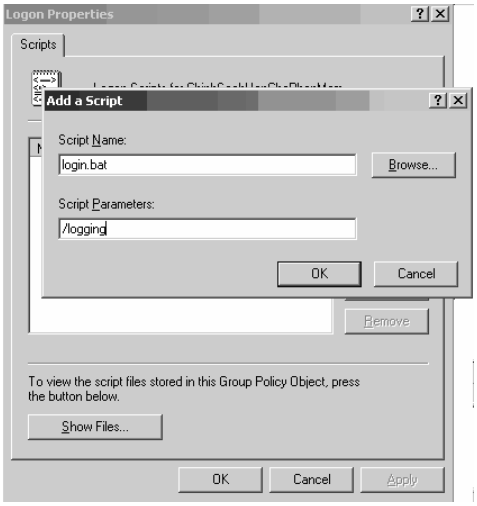


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Mở công cụ **Group Policy Object Editor**, vào mục **User Configuration** ⏲ **Windows Setttings** ⏲ **Scripts**.



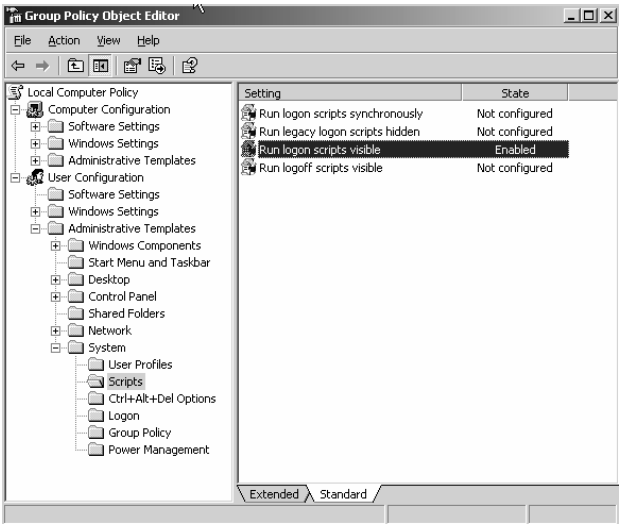

Nhấp đúp chuột vào mục **Logon** bên của sổ bên phải, hộp thoại xuất hiện, bạn nhấp chuột tiếp vào nút **Add** để khai báo tên tập tin kịch bản cần thi hành khi đăng nhập. Chú ý tập tin kịch bản này phải được chứa trong thư mục **c:\windows\system32\ grouppolicy\user\script\logon**. Thư mục này có thể thay đổi, tốt nhất bạn nên nhấp chuột vào nút **Show Files** phía dưới hộp thoại để xem thư mục cụ thể chứa các tập tin kịch bản này. Nội dung tập tin kịch bản có thể thay đổi tùy theo yêu cầu của bạn, bạn có thể tham khảo tập tin kịch bản ở chương trước.




Tiếp theo để kiểm soát quá trình thi hành của tập tin kịch bản, bạn cần hiệu chỉnh chính sách **Run logon scripts visible** ở trạng thái **Enable**. Trạng thái này giúp bạn có thể phát hiện ra các lỗi phát sinh khi tập tin kịch bản thi hành từ đó chúng ta có thể sửa chữa. Để thay đổi chính sách này bạn nhấp chuột vào mục **User Configuration** ⏲ **Administrative Templates** ⏲ **System** ⏲ **Scripts,** sau đó nhấp đúp chuột vào mục **Run logon scripts visible** để thay đổi trạng thái.

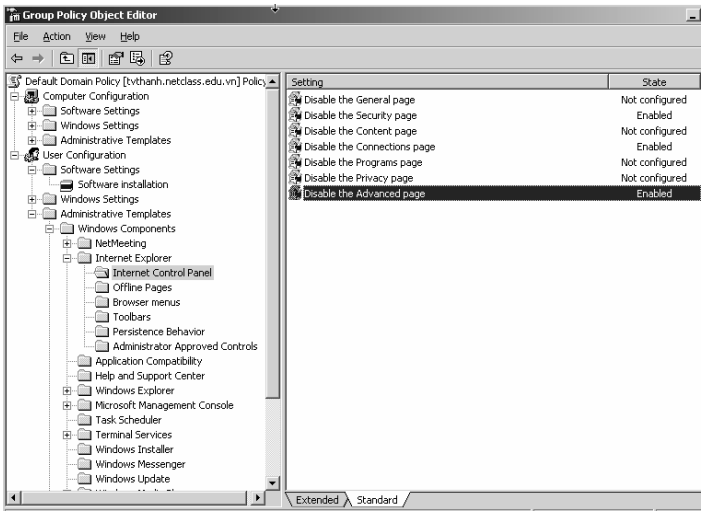


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




## III.2. Hạn chế chức năng của Internet Explorer.

Trong ví dụ này chúng ta muốn các người dùng dưới máy trạm không được phép thay đổi bất kì thông số nào trong **Tab Security**, **Connection** và **Advanced** trong hộp thoại **Internet Options** của công cụ **Internet Explorer**. Để làm việc này, trong công cụ **Group Policy Object Editor**, bạn vào **User Configuration** 🕘 **Administrative Templates** 🕘 **Windows Components** 🕘 **Internet Explorer** 🕘 **Internet Control Panel**, chương trình sẽ hiện ra các mục chức năng của **IE** có thể giới hạn, bạn chọn khóa các chức năng cần thiết.

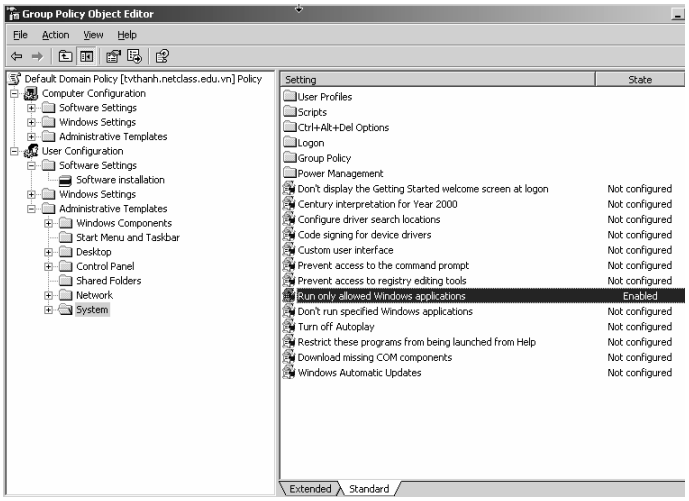



## III.3. Chỉ cho phép một số ứng dụng được thi hành.

Để cấu hình **Group Policy** chỉ cho phép các người dùng dưới máy trạm chỉ sử dụng được một vài ứng dụng nào đó, trong công cụ **Group Policy Object Editor**, bạn vào **User Configuration** 🕘 **Administrative Templates**. Sau đó nhấp đúp chuột vào mục **Run only allowed windows applications** để chỉ định các phần mềm được phép thi hành.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net






Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

# Tóm tắt

Lý thuyết 3 tiết - Thực hành 5 tiết

| Mục tiêu | Các mục chính | Bài tập bắt buộc | Bài tập làm thêm |
|---|---|---|---|
| Kết thúc bài học này cung cấp học viên kiến thức về các loại định dạng đĩa, công nghệ lưu trữ mới Dynamic Storage, kỹ thuật nén và mã hóa dữ liệu… | I. Các cấu hình hệ thống tập tin.<br>II. Cấu hình đĩa lưu trữ.<br>III. Sử dụng chương trình Disk Manager.<br>IV. Quản lý việc nén dữ liệu<br>V. Thiết lập hạn ngạch đĩa<br>VI. Mã hóa dữ liệu bằng EFS | Dựa vào bài tập môn Quản trị Windows Server 2003. | Dựa vào bài tập môn Quản trị Windows Server 2003. |



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

# I. CẤU HÌNH HỆ THỐNG TẬP TIN.

Hệ thống tập tin quản lý việc lưu trữ và định vị các tập tin trên đĩa cứng. **Windows Server 2003** hỗ trợ ba hệ thống tập tin khác nhau: **FAT16**, **FAT32** và **NTFS5**. Bạn nên chọn **FAT16** hoặc **FAT32** khi máy tính sử dụng nhiều hệ điều hành khác nhau. Nếu bạn định sử dụng các tính năng như bảo mật cục bộ, nén và mã hoá các tập tin thì bạn nên dùng **NTFS5**. Bảng sau trình bày khả năng của từng hệ thống tập tin trên **Windows Server 2003**:

| Khả năng | FAT16 | FAT32 | NTFS |
|---|---|---|---|
| Hệ điều hành hỗ trợ | Hầu hết các hệ điều hành | Windows 95 OSR2, Windows 98, Windows 2000, 2003 | Windows 2000, 2003 |
| Hỗ trợ tên tập tin dài | 256 ký tự trên Windows, 8.3 trên Dos | 256 ký tự | 256 ký tự |
| Sử dụng hiệu quả đĩa | Không | Có | Có |
| Hỗ trợ nén đĩa | Không | Không | Có |
| Hỗ trợ hạn ngạch | Không | Không | Có |
| Hỗ trợ mã hoá | Không | Không | Có |
| Hỗ trợ bảo mật cục bộ | Không | Không | Có |
| Hỗ trợ bảo mật trên mạng | Có | Có | Có |
| Kích thước Volume tối đa được hỗ trợ | 4GB | 32GB | 1024GB |

Trên **Windows Server 2003/Windows 2000/NT**, bạn có thể sử dụng lệnh **CONVERT** để chuyển đổi hệ thống tập tin từ **FAT16, FAT32** thành **NTFS**. Cú pháp của lệnh như sau:

CONVERT [ổ đĩa:] /fs:ntfs

# II. CẤU HÌNH ĐĨA LƯU TRỮ.

**Windows Server 2003** hỗ trợ hai loại đĩa lưu trữ: **basic** và **dynamic**.

## II.1. Basic storage.

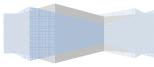


Bao gồm các **partition primary** và **extended**. **Partition** tạo ra đầu tiên trên đĩa được gọi là **partition primary** và toàn bộ không gian cấp cho **partition** được sử dụng trọn vẹn. Mỗi ổ đĩa vật lý có tối đa bốn **partition**. Bạn có thể tạo ba **partition primary** và một **partition extended**. Với **partition extended**,

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

bạn có thể tạo ra nhiều **partition logical**.





Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

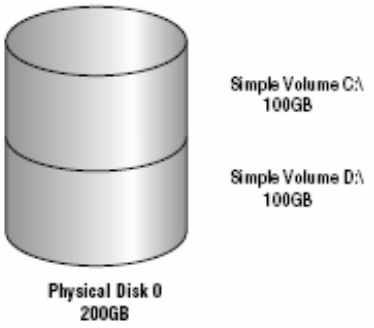
## II.2. Dynamic storage

Đây là một tính năng mới của **Windows Server 2003**. Đĩa lưu trữ **dynamic** chia thành các **volume dynamic**. **Volume dynamic** không chứa **partition** hoặc ổ đĩa **logic**, và chỉ có thể truy cập bằng **Windows Server 2003** và **Windows 2000**. **Windows Server 2003/ Windows 2000** hỗ trợ năm loại **volume dynamic**: **simple**, **spanned**, **striped**, **mirrored** và **RAID-5**. Ưu điểm của công nghệ **Dynamic storage** so với công nghệ **Basic storage**:

- Cho phép ghép nhiều ổ đĩa vật lý để tạo thành các ổ đĩa **logic** (**Volume**).
- Cho phép ghép nhiều vùng trống không liên tục trên nhiều đĩa cứng vật lý để tạo ổ đĩa logic.
- Có thể tạo ra các ổ đĩa **logic** có khả năng dung lỗi cao và tăng tốc độ truy xuất…

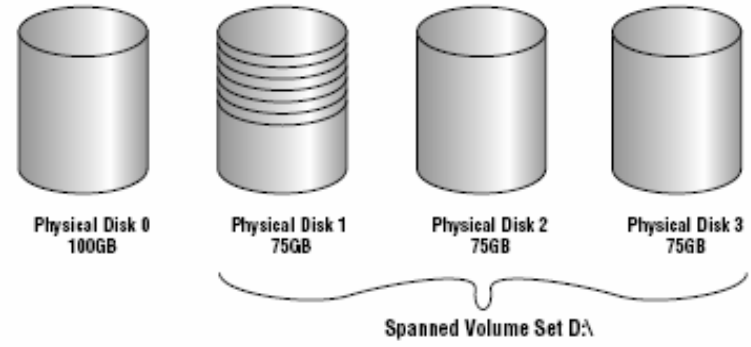
### II.2.1 Volume simple.

Chứa không gian lấy từ một đĩa **dynamic** duy nhất. Không gian đĩa này có thể liên tục hoặc không liên tục. Hình sau minh hoạ một đĩa vật lý được chia thành hai **volume** đơn giản.




### II.2.2 Volume spanned.

Bao gồm một hoặc nhiều đĩa **dynamic** (tối đa là 32 đĩa). Sử dụng khi bạn muốn tăng kích cỡ của **volume**. Dữ liệu ghi lên **volume** theo thứ tự, hết đĩa này đến đĩa khác. Thông thường người quản trị sử dụng **volume spanned** khi ổ đĩa đang sử dụng trong **volume** sắp bị đầy và muốn tăng kích thước của **volume** bằng cách bổ sung thêm một đĩa khác.



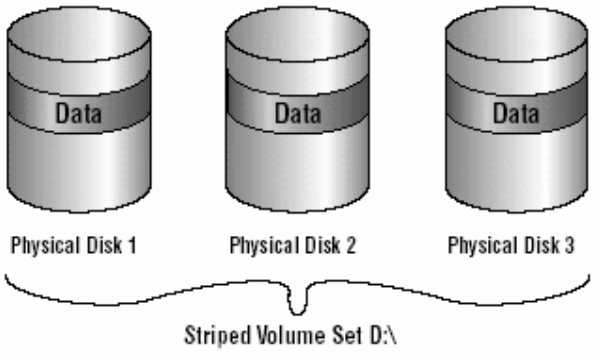

Do dữ liệu được ghi tuần tự nên **volume** loại này không tăng hiệu năng sử dụng. Nhược điểm chính của **volume spanned** là nếu một đĩa bị hỏng thì toàn bộ dữ liệu trên **volume** không thể truy xuất được.



### II.2.3 Volume striped.

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

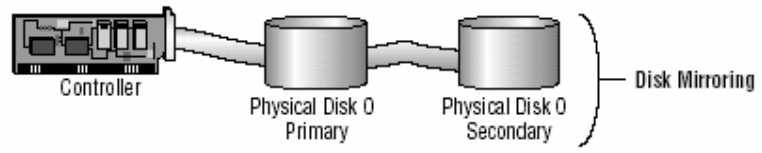
Lưu trữ dữ liệu lên các dãy (**strip**) bằng nhau trên một hoặc nhiều đĩa vật lý (tối đa là 32). Do dữ liệu được ghi tuần tự lên từng dãy, nên bạn có thể thi hành nhiều tác vụ **I/O** đồng thời, làm tăng tốc độ truy xuất dữ liệu. Thông thường, người quản trị mạng sử dụng **volume striped** để kết hợp dung lượng của nhiều ổ đĩa vật lý thành một đĩa **logic** đồng thời tăng tốc độ truy xuất.



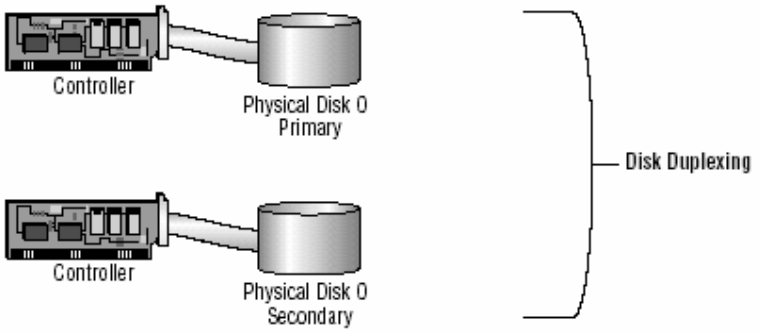

Nhược điểm chính của **volume striped** là nếu một ổ đĩa bị hỏng thì dữ liệu trên toàn bộ **volume** mất giá trị.

### II.2.4 Volume mirrored.

Là hai bản sao của một **volume** đơn giản. Bạn dùng một ổ đĩa chính và một ổ đĩa phụ. Dữ liệu khi ghi lên đĩa chính đồng thời cũng sẽ được ghi lên đĩa phụ. **Volume** dạng này cung cấp khả năng dung lỗi tốt. Nếu một đĩa bị hỏng thì ổ đĩa kia vẫn làm việc và không làm gián đoạn quá trình truy xuất dữ liệu. Nhược điểm của phương pháp này là bộ điều khiển đĩa phải ghi lần lượt lên hai đĩa, làm giảm hiệu năng.




Để tăng tốc độ ghi đồng thời cũng tăng khả năng dung lỗi, bạn có thể sử dụng một biến thể của **volume mirrored** là **duplexing**. Theo cách này bạn phải sử dụng một bộ điều khiển đĩa khác cho ổ đĩa thứ hai.



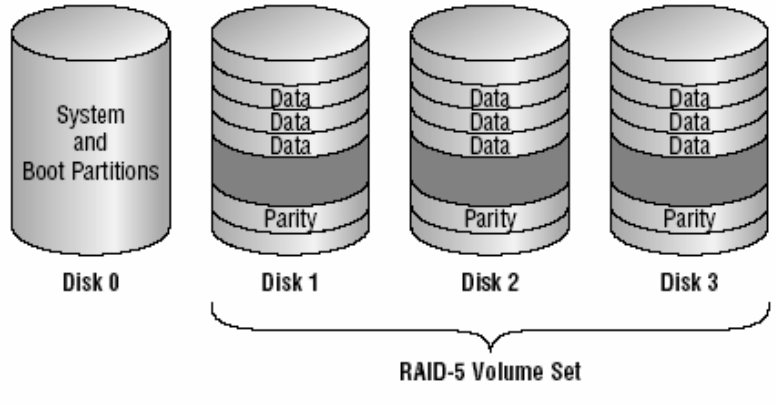



Nhược điểm chính của phương pháp này là chi phí cao. Để có một **volume 4GB** bạn phải tốn đến **8GB** cho hai ổ đĩa.

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

### II.2.5 Volume RAID-5.

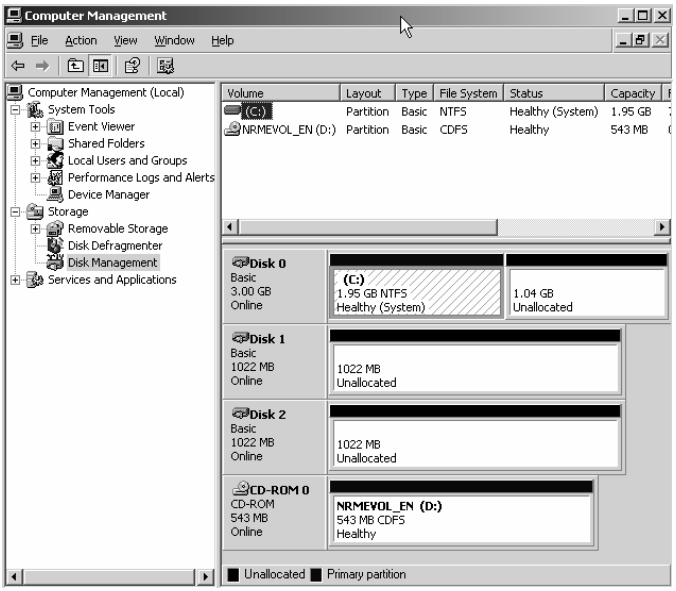
Tương tự như **volume striped** nhưng **RAID-5** lại dùng thêm một dãy (**strip**) ghi thông tin kiểm lỗi **parity**. Nếu một đĩa của **volume** bị hỏng thì thông tin **parity** ghi trên đĩa khác sẽ giúp phục hồi lại dữ liệu trên đĩa hỏng. **Volume RAID-5** sử dụng ít nhất ba ổ đĩa (tối đa là 32).




Ưu điểm chính của kỹ thuật này là khả năng dung lỗi cao và tốc độ truy xuất cao bởi sử dụng nhiều kênh I/O.

# III. SỬ DỤNG CHƯƠNG TRÌNH DISK MANAGER.

**Disk Manager** là một tiện ích giao diện đồ hoạ phục vụ việc quản lý đĩa và **volume** trên môi trường **Windows 2000** và **Windows Server 2003**. Để có thể sử dụng được hết các chức năng của chương trình, bạn phải đăng nhập vào máy bằng tài khoản **Administrator**. Vào **menu Start** 🕘 **Programs** 🕘 **Administrative Tools** 🕘 **Computer Management**. Sau đó mở rộng mục **Storage** và chọn **Disk Management**. Cửa sổ **Disk Management** xuất hiện như sau:



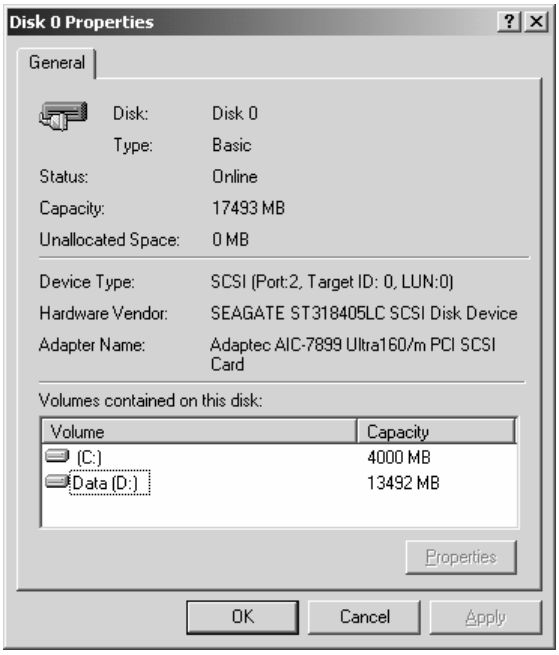

Phần sau sẽ hướng dẫn bạn thực hiện các thao tác căn bản bằng **Disk Manager**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

## III.1. Xem thuộc tính của đĩa.

Nhấp phải chuột lên ổ đĩa vật lý muốn biết thông tin và chọn **Properties**. Hộp thoại **Disk Properties** xuất hiện như sau:




Hộp thoại cung cấp các thông tin:

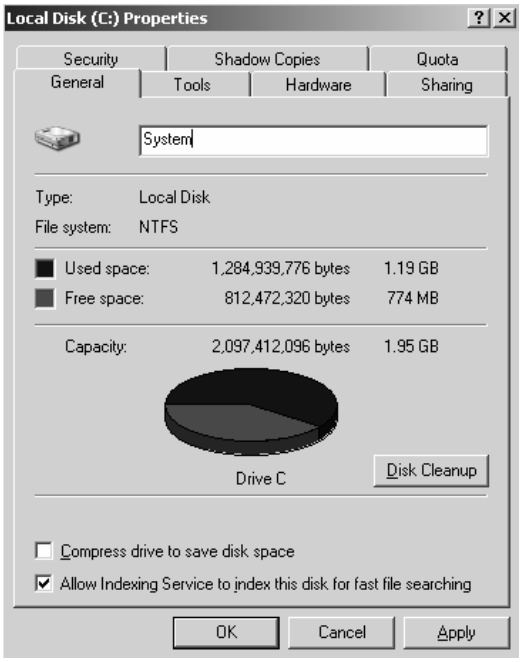
- Số thứ tự của ổ đĩa vật lý
- Loại đĩa (**basic**, **dynamic**, **CD-ROM**, **DVD,** đĩa chuyển dời được, hoặc **unknown**)
- Trạng thái của đĩa (**online** hoặc **offline**)
- Dung lượng đĩa
- Lượng không gian chưa cấp phát
- Loại thiết bị phần cứng
- Nhà sản xuất thiết bị
- Tên của **adapter**
- Danh sách các **volume** đã tạo trên đĩa

## III.2. Xem thuộc tính của volume hoặc đĩa cục bộ.

Trên một ổ đĩa **dynamic**, bạn sử dụng các **volume**. Ngược lại trên một ổ đĩa **basic**, bạn sử dụng các đĩa cục bộ (**local disk**). **Volume** và đĩa cục bộ đều có chức năng như nhau, do vậy các phần sau dựa vào đĩa cục bộ để minh hoạ. Để xem thuộc tính của một đĩa cục bộ, bạn nhấp phải chuột lên đĩa cục bộ đó và chọn **Properties** và hộp thoại **Local Disk Properties** xuất hiện.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

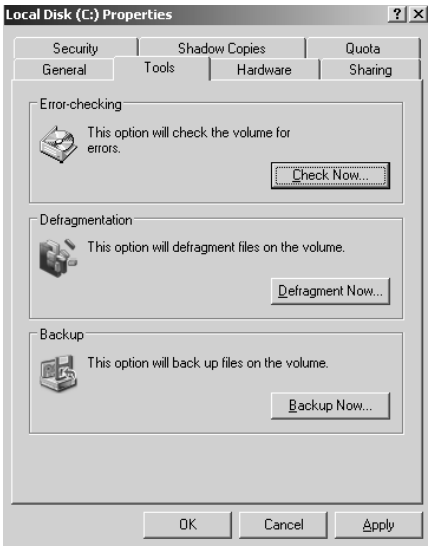



### III.2.1 Tab General.

Cung cấp các thông tin như nhãn đĩa, loại, hệ thống tập tin, dung lượng đã sử dụng, còn trống và tổng dung lượng. Nút **Disk Cleanup** dùng để mở chương trình **Disk Cleanup** dùng để xoá các tập tin không cần thiết, giải phóng không gian đĩa.

### III.2.2 Tab Tools.

Bấm nút **Check Now** để kích hoạt chương trình **Check Disk** dùng để kiểm tra lỗi như khi không thể truy xuất đĩa hoặc khởi động lại máy không đúng cách. Nút **Backup Now** sẽ mở chương trình **Backup Wizard**, hướng dẫn bạn các bước thực hiện việc sao lưu các tập tin và thư mục trên đĩa. Nút **Defragment Now** mở chương trình **Disk Defragment**, dùng để dồn các tập tin trên đĩa thành một khối liên tục, giúp ích cho việc truy xuất đĩa.





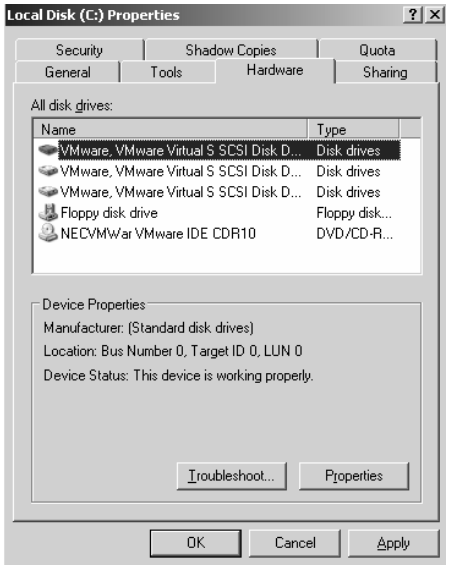

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

### III.2.3 Tab Hardware.



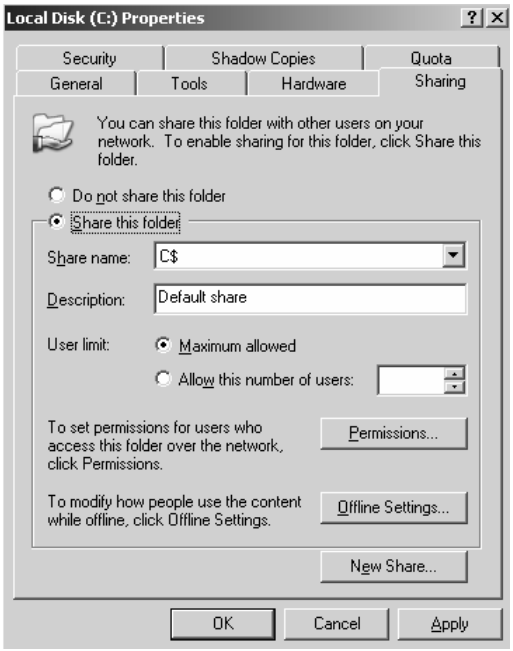
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Liệt kê các ổ đĩa vật lý **Windows Server 2003** nhận diện được. Bên dưới danh sách liệt kê các thuộc tính của ổ đĩa được chọn.




### III.2.4 Tab Sharing.

Cho phép chia sẻ hoặc không chia sẻ ổ đĩa cục bộ này. Theo mặc định, tất cả các ổ đĩa cục bộ đều được chia sẻ dưới dạng ẩn (có dấu **$** sau tên chia sẻ).

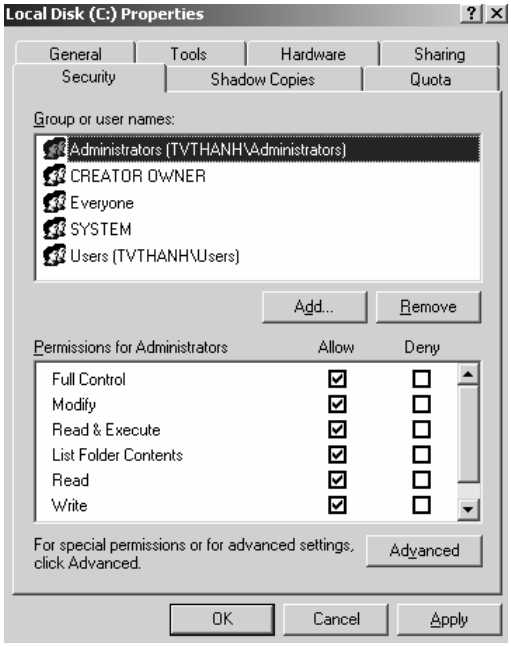



### III.2.5 Tab Security.

Chỉ xuất hiện khi đĩa cục bộ này sử dụng hệ thống tập tin **NTFS**. Dùng để thiết lập quyền truy cập lên đĩa. Theo mặc định, nhóm **Everyone** được toàn quyền trên thư mục gốc của đĩa.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

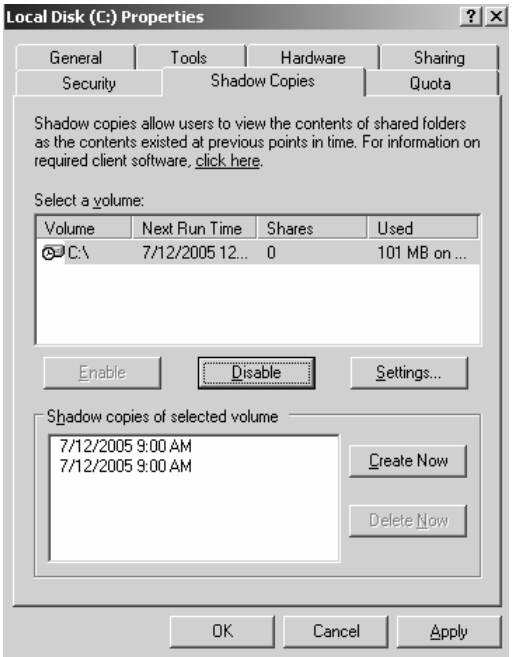



### III.2.6 Tab Quota.

Chỉ xuất hiện khi sử dụng **NTFS**. Dùng để quy định lượng không gian đĩa cấp phát cho người dùng.

### III.2.7 Shadow Copies.

**Shadow Copies** là dịch vụ cho phép người dùng truy cập hoặc khôi phục những phiên bản trước đây của những tập tin đã lưu, bằng cách dùng một tính năng ở máy trạm gọi là **Previous Versions**.






## III.3. Bổ sung thêm một ổ đĩa mới.

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

### III.3.1 Máy tính không hỗ trợ tính năng “hot swap”.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Bạn phải tắt máy tính rồi mới lắp ổ đĩa mới vào. Sau đó khởi động máy tính lại. Chương trình **Disk Management** sẽ tự động phát hiện và yêu cầu bạn ghi một chữ ký đặc biệt lên ổ đĩa, giúp cho **Windows Server 2003** nhận diện được ổ đĩa này. Theo mặc định, ổ đĩa mới được cấu hình là một đĩa **dynamic**.

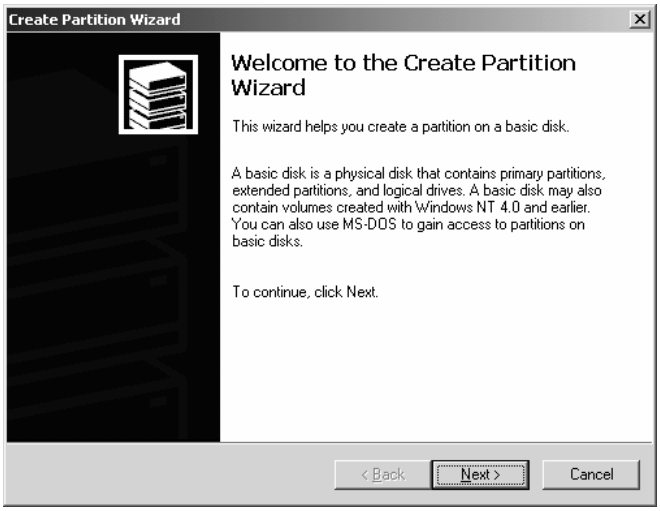
### III.3.2 Máy tính hỗ trợ "hot swap".

Bạn chỉ cần lắp thêm ổ đĩa mới vào theo hướng dẫn của nhà sản xuất mà không cần tắt máy. Rồi sau đó dùng chức năng **Action** ◴ **Rescan Disk** của **Disk Manager** để phát hiện ổ đĩa mới này.

## III.4. Tạo partition/volume mới.

Nếu bạn còn không gian chưa cấp phát trên một đĩa **basic** thì bạn có thể tạo thêm **partition** mới, còn trên đĩa **dynamic** thì bạn có thể tạo thêm **volume** mới. Phần sau hướng dẫn bạn sử dụng **Create Partition Wizard** để tạo một **partition** mới:

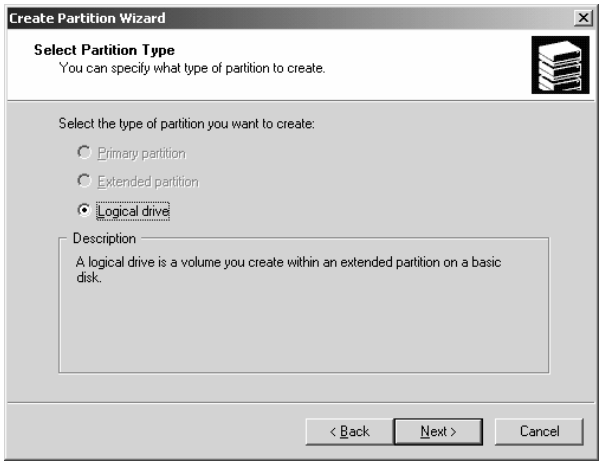
Nhấp phải chuột lên vùng trống chưa cấp phát của đĩa **basic** và chọn **Create Logical Drive**.



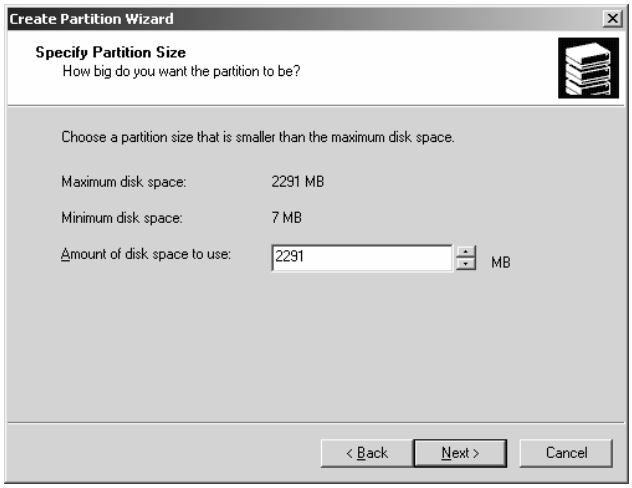

Xuất hiện hộp thoại **Create Partition Wizard**. Nhấn nút **Next** trong hộp thoại này.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net



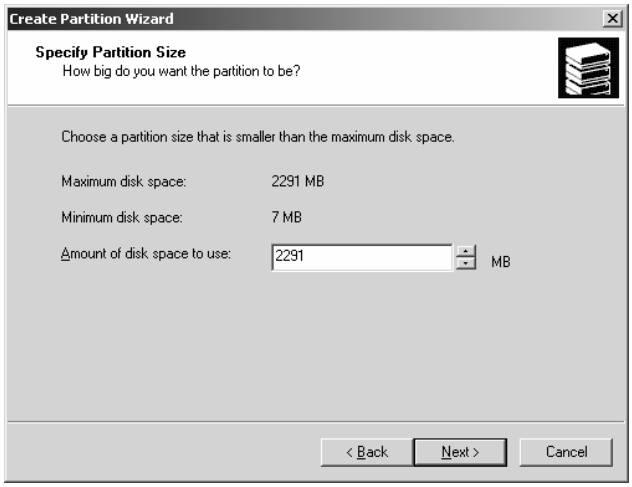

Trong hộp thoại **Select Partition Type**, chọn loại **partition** mà bạn định tạo. Chỉ có những loại còn khả năng tạo mới được phép chọn (tuỳ thuộc vào ổ đĩa vật lý của bạn). Sau khi chọn loại **partition** xong nhấn **Next** để tiếp tục.



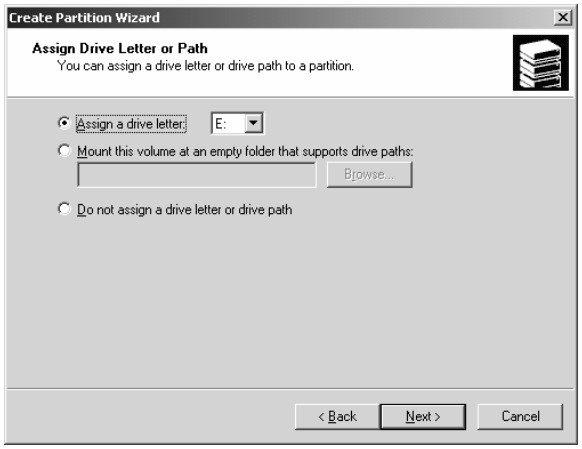

Tiếp theo, hộp thoại **Specify Partition Size** yêu cầu bạn cho biết dung lượng định cấp phát. Sau khi chỉ định xong, nhấn **Next**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net



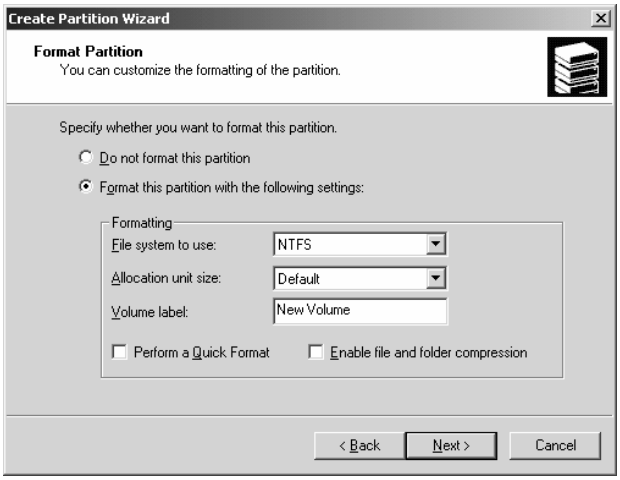

Trong hộp thoại **Assign Drive Letter or Path**, bạn có thể đặt cho **partition** này một ký tự ổ đĩa, hoặc gắn (**mount**) vào một thư mục rỗng, hoặc không làm đặt gì hết. Khi bạn chọn kiểu gắn vào một thư mục rỗng thì bạn có thể tạo ra vô số **partition** mới. Sau khi đã quyết định xong, nhấn **Next** để tiếp tục.



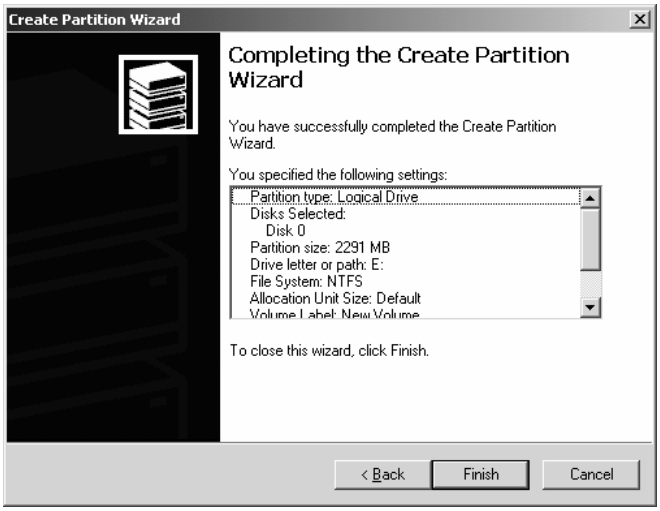

Hộp thoại **Format Partition** yêu cầu bạn quyết định có định dạng **partition** này không. Nếu có thì dùng hệ thống tập tin là gì? đơn vị cấp phát là bao nhiêu? nhãn của **partition** (**volume label**) là gì? có định dạng nhanh không? Có nén tập tin và thư mục không? Sau khi đã chọn xong, nhấn **Next** để tiếp tục.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

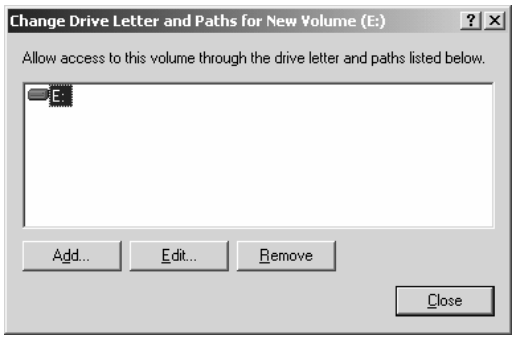



Hộp thoại **Completing** the **Create Partition Wizard** tóm tắt lại các thao tác sẽ thực hiện, bạn phải kiểm tra lại xem đã chính xác chưa, sau đó nhấn **Finish** để bắt đầu thực hiện.




## III.5. Thay đổi ký tự ổ đĩa hoặc đường dẫn.

Muốn thay đổi ký tự ổ đĩa cho **partition/volume** nào, bạn nhấp phải chuột lên **volume** đó và chọn **Change Drive Letter and Path**. Hộp thoại **Change Drive Letter and Path** xuất hiện.





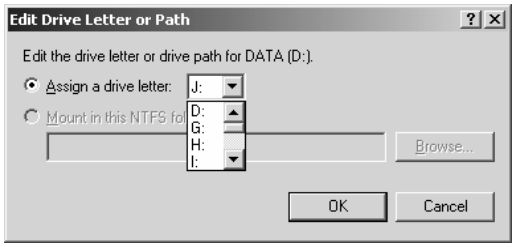

Trong hộp thoại này, nhấn nút **Edit** để mở tiếp hộp thoại **Edit Drive Letter and Path**, mở danh sách **Assign a drive letter** và chọn một ký tự ổ đĩa mới định đặt cho **partition/volume** này. Cuối cùng đồng

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

ý xác nhận các thay đổi đã thực hiện.

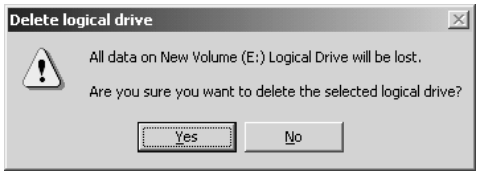


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




## III.6. Xoá partition/volume.

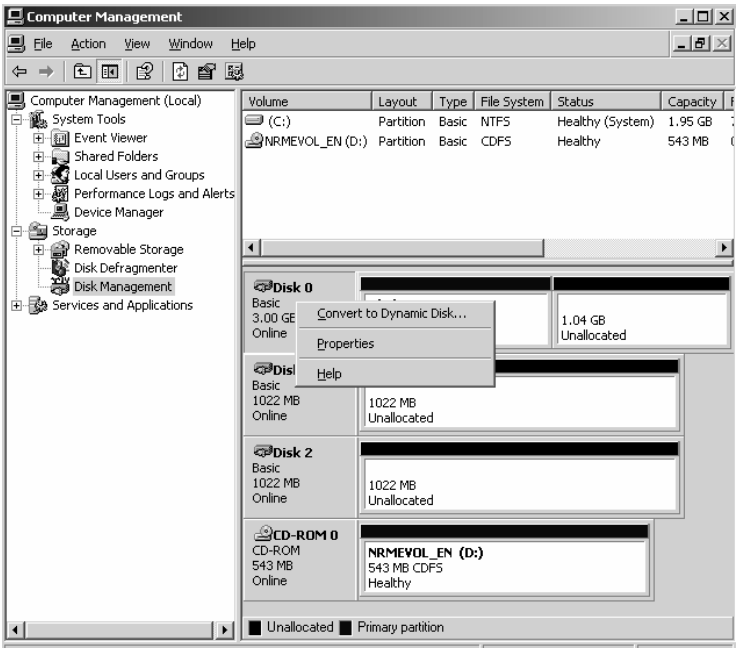
Để tổ chức lại một ổ đĩa hoặc huỷ các dữ liệu có trên một **partition/volume**, bạn có thể xoá nó đi. Để thực hiện, trong cửa sổ **Disk Manager**, bạn nhấp phải chuột lên **partition/volume** muốn xoá và chọn **Delete Partition** (hoặc **Delete Volume**). Một hộp thoại cảnh báo xuất hiện, thông báo dữ liệu trên **partition** hoặc **volume** sẽ bị xoá và yêu cầu bạn xác nhận lại lần nữa thao tác này.




## III.7. Cấu hình Dynamic Storage.

### III.7.1 Chuyển chế độ lưu trữ.

Để sử dụng được cơ chế lưu trữ **Dynamic**, bạn phải chuyển đổi các đĩa cứng vật lý trong hệ thống thành **Dynamic Disk**. Trong công cụ **Computer Management** ⏲ **Disk Management**, bạn nhấp phải chuột trên các ổ đĩa bên của sổ bên phải và chọn **Convert to Dynamic Disk….** Sau đó đánh dấu vào tất cả các đĩa cứng vật lý cần chuyển đổi chế độ lưu trữ và chọn **OK** để hệ thống chuyển đổi. Sau khi chuyển đổi xong hệ thống sẽ yêu cầu bạn **restart** máy để áp dụng chế độ lưu trữ mới.



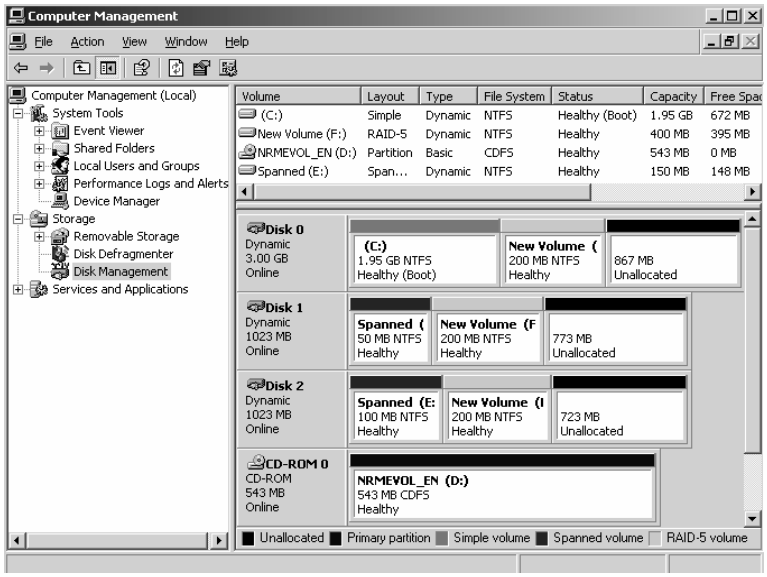



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Các loại **Volume** mà chúng ta sẽ tạo ở phần sau:

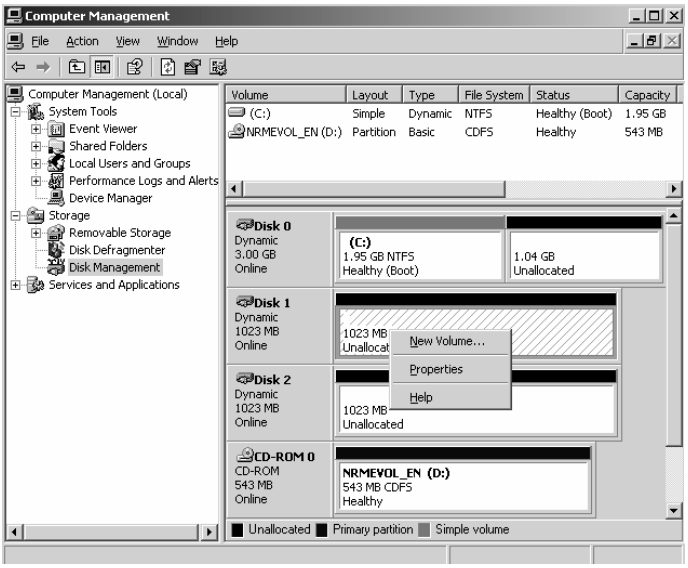


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




### III.7.2 Tạo Volume Spanned.

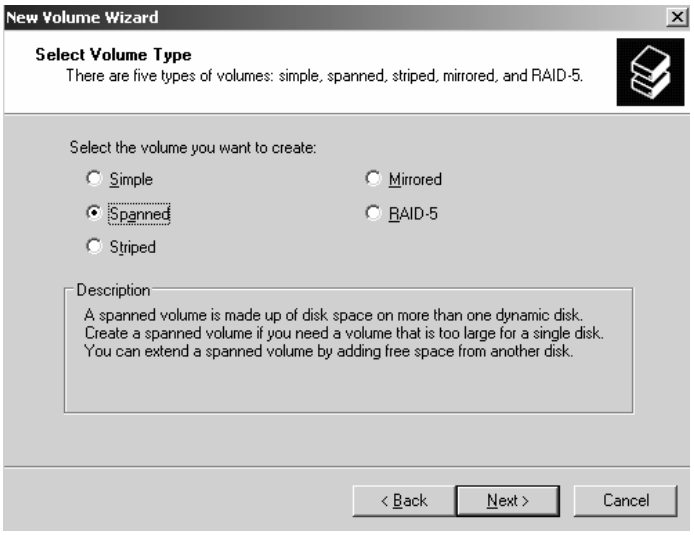
Trong công cụ **Disk Management**, bạn nhấp phải chuột lên vùng trống của đĩa cứng cần tạo **Volume**, sau đó chọn **New Volume.**



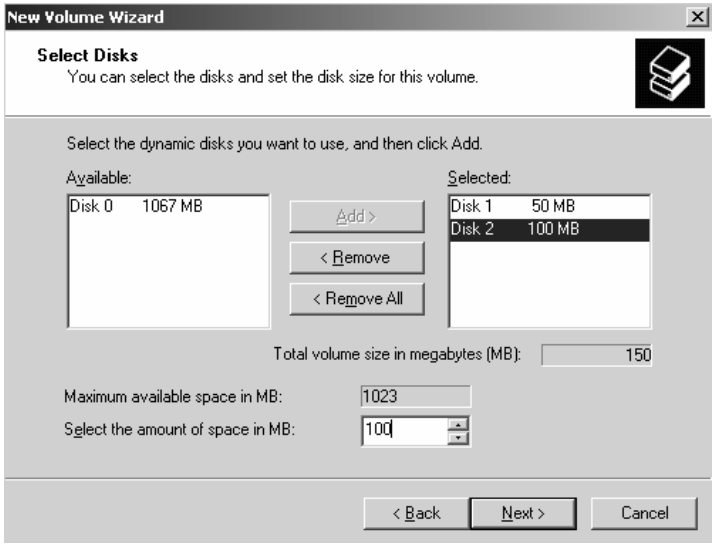

Tiếp theo, bạn chọn loại **Volume** cần tạo. Trong trường hợp này chúng ta chọn **Spanned**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Bạn chọn những đĩa cứng dùng để tạo **Volume** này, đồng thời bạn cũng nhập kích thước mà mỗi đĩa giành ra để tạo **Volume**. Chú ý đối với loại **Volume** này thì kích thước của các đĩa giành cho **Volume** có thể khác nhau.

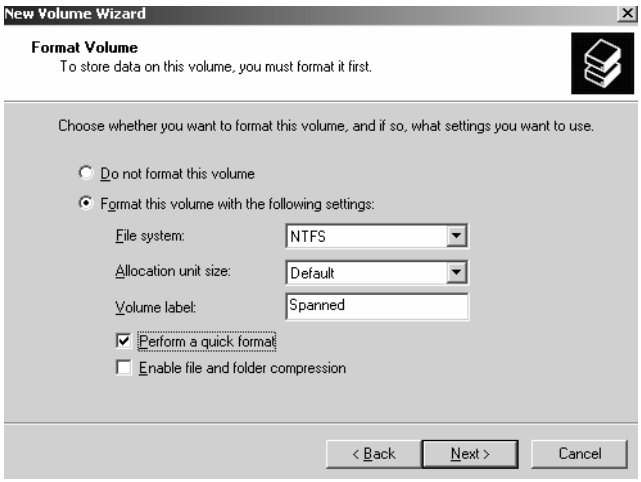



Bạn gán ký tự ổ đĩa cho **Volume**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net


Bạn định dạng **Volume** mà bạn vừa tạo để có thể chứa dữ liệu.



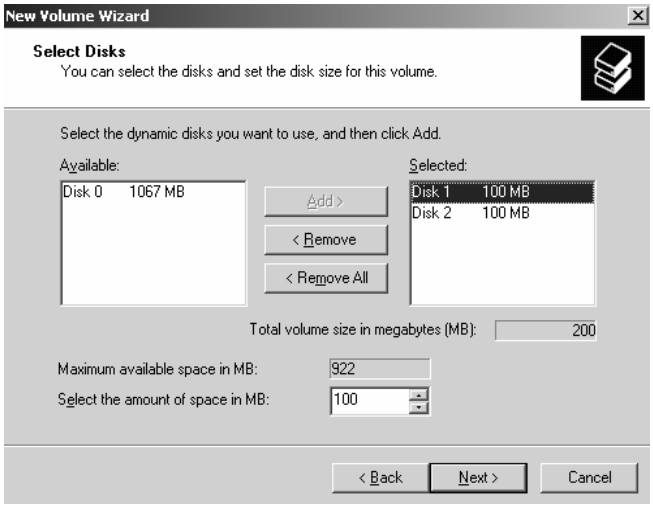

Đến đây đã hoàn thành việc tạo **Volume**, bạn có thể lưu trữ dữ liệu trên **Volume** này theo cơ chế đã trình bày ở phần lý thuyết.

### III.7.3 Tạo Volume Striped.

Các bước tạo **Volume Striped** cũng tương tự như việc tạo các **Volume** khác nhưng chú ý là kích thước của các đĩa cứng giành cho loại **Volume** này phải bằng nhau và kích thước của **Volume** bằng tổng các kích thước của các phần trên.

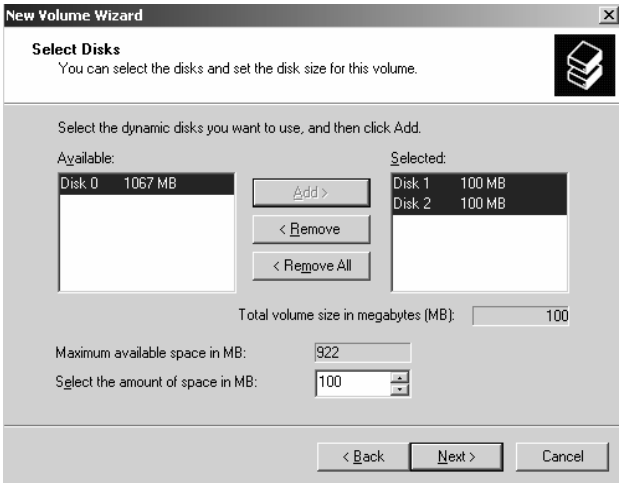


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




### III.7.4 Tạo Volume Mirror.

Các bước tạo **Volume Mirror** cũng tương tự như trên, chú ý kích thước của các đĩa cứng giành cho loại **Volume** này phải bằng nhau và kích thước của **Volume** bằng chính kích thước của mỗi phần trên.

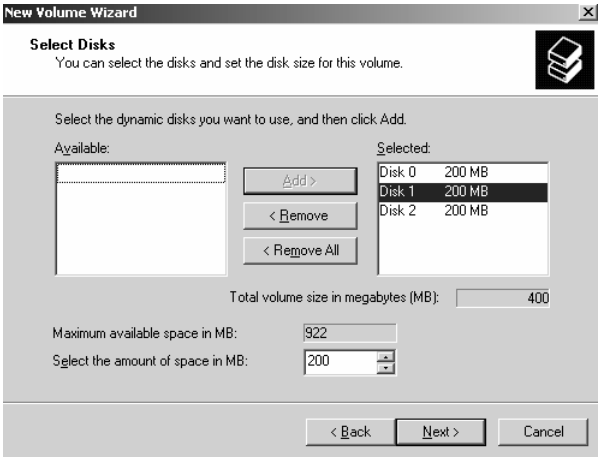



### III.7.5 Tạo Volume Raid-5.

Các bước tạo **Volume Raid-5** cũng tương tự như trên nhưng chú ý là loại **Volume** yêu cầu tối thiểu đến 3 đĩa cứng. Kích thước của các đĩa cứng giành cho loại **Volume** này phải bằng nhau và kích thước của **Volume** bằng 2/3 kích thước của mỗi phần cộng lại.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

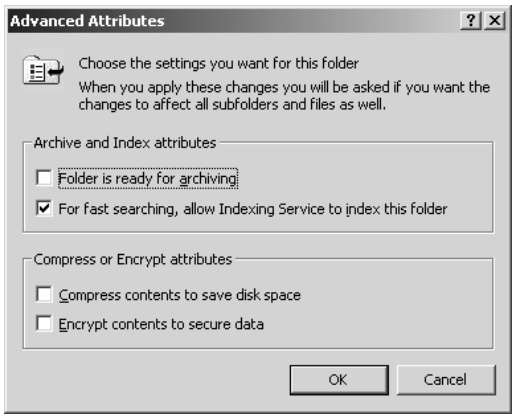



# IV. QUẢN LÝ VIỆC NÉN DỮ LIỆU.

Nén dữ liệu là quá trình lưu trữ dữ liệu dưới một dạng thức chiếm ít không gian hơn dữ liệu ban đầu. **Windows Server 2003** hỗ trợ tính năng nén các tập tin và thư mục một cách tự động và trong suốt. Các chương trình ứng dụng truy xuất các tập tin nén một cách bình thường do hệ điều hành tự động giải nén khi mở tập tin và nén lại khi lưu tập tin lên đĩa. Khả năng này chỉ có trên các **partition NTFS**. Nếu bạn chép một tập tin/thư mục trên một **partition** có tính năng nén sang một partition **FAT** bình thường thì hệ điều hành sẽ giải nén tập tin/thư mục đó trước khi chép đi.

Để thi hành việc nén một tập tin/thư mục, bạn sử dụng chương trình **Windows Explorer** và thực hiện theo các bước sau:

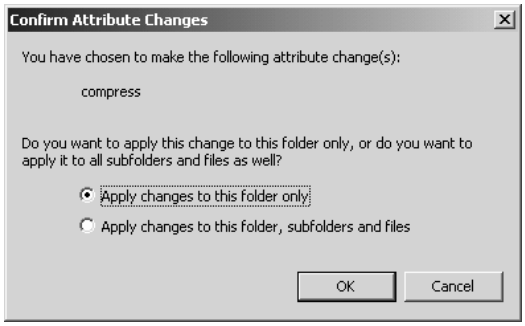
- Trong cửa sổ **Windows Explorer**, duyệt đến tập tin/thư mục định nén và chọn tập tin/thư mục đó.
- Nhấp phải chuột lên đối tượng đó và chọn **Properties**.
- Trong hộp thoại **Properties**, nhấn nút **Advanced** trong **tab General**.
- Trong hộp thoại **Advanced Properties**, chọn mục "**Compress contents to save disk space**" và nhấn chọn **OK**.




Nhấn chọn **OK** trong hộp thoại **Properties** để xác nhận thao tác. Nếu bạn định nén một thư mục, hộp thoại **Confirm Attribute Changes** xuất hiện, yêu cầu bạn lựa chọn hoặc là chỉ nén thư mục này thôi (**Apply changes to this folder only**) hoặc nén cả các thư mục con và tập tin có trong thư mục (**Apply changes to this folder, subfolders and files**). Thực hiện lựa chọn của bạn và nhấn **OK**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Để thực hiện việc giải nén một thư mục/tập tin, bạn thực hiện tương tự theo các bước ở trên và bỏ chọn mục **Compress contents to save disk space** trong hộp thoại **Advanced Properties**.

# V. THIẾT LẬP HẠN NGẠCH ĐĨA (DISK QUOTA).

Hạn ngạch đĩa được dùng để chỉ định lượng không gian đĩa tối đa mà một người dùng có thể sử dụng trên một **volume NTFS**. Bạn có thể áp dụng hạn ngạch đĩa cho tất cả người dùng hoặc chỉ đối với từng người dùng riêng biệt.

Một số vấn đề bạn phải lưu ý khi thiết lập hạn ngạch đĩa:

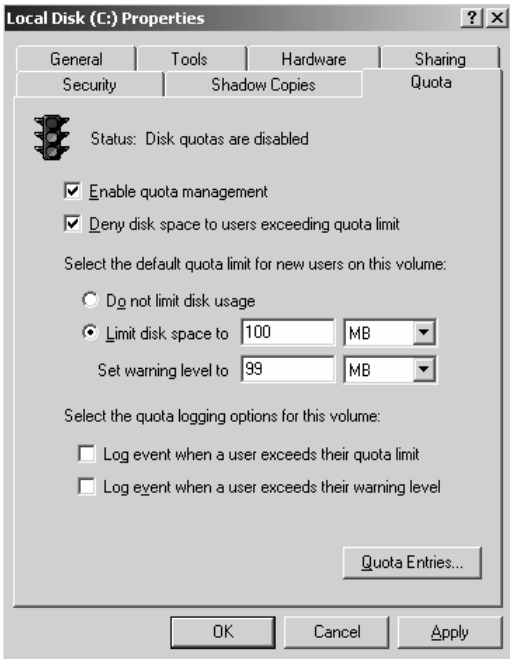
- Chỉ có thể áp dụng trên các volume **NTFS**.
- Lượng không gian chiếm dụng được tính theo các tập tin và thư mục do người dùng sở hữu.
- Khi người dùng cài đặt một chương trình, lượng không gian đĩa còn trống mà chương trình thấy được tính toán dựa vào hạn ngạch đĩa của người dùng, không phải là lượng không gian còn trống trên **volume**.
- Được tính toán trên kích thước thật sự của tập tin trong trường hợp tập tin/thư mục được nén.

## V.1. Cấu hình hạn ngạch đĩa.

Bạn cấu hình hạn ngạch đĩa bằng hộp thoại **Volume Propertise** đã giới thiệu trong phần trên. Bạn cũng có thể mở hộp thoại này bằng cách nhấp phải chuột lên ký tự ổ đĩa trong **Windows Explorer** và chọn **Propertise**. Trong hộp thoại này nhấp chọn **tab Quota**. Theo mặc định tính năng hạn ngạch đĩa không được kích hoạt.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Các mục trong hộp thoại có ý nghĩa như sau:

- **Enable quota management**: thực hiện hoặc không thực hiện quản lý hạn ngạch đĩa.
- **Deny disk space to users exceeding quota limit**: người dùng sẽ không thể tiếp tục sử dụng đĩa khi vượt quá hạn ngạch và nhận được thông báo **out of disk space.**
- **Select the default quota limit for new users on this volume**: định nghĩa các giới hạn sử dụng. Các lựa chọn bao gồm "không định nghĩa giới hạn" (**Do not limit disk space**), "giới hạn cho phép" (**Limit disk space to**) và "giới hạn cảnh báo" (**Set warning level to**).
- **Select the quota logging options for this volume**: có ghi nhận lại các sự kiện liên quan đến sử dụng hạn ngạch đĩa. Có thể ghi nhận khi người dùng vượt quá giới hạn cho phép hoặc vượt quá giới hạn cảnh báo.
- Biểu tượng đèn giao thông trong hộp thoại có các trạng thái sau:
- Đèn đỏ cho biết tính năng quản lý hạn ngạch không được kích hoạt.
- Đèn vàng cho biết **Windows Server 2003** đang xây dựng lại thông tin hạn ngạch.
- Đèn xanh cho biết tính năng quản lý đang có tác dụng.

## V.2. Thiết lập hạn ngạch mặc định.

Khi bạn thiết lập hạn ngạch mặc định áp dụng cho các người dùng mới trên volume, chỉ những người dùng chưa bao giờ tạo tập tin trên volume đó mới chịu ảnh hưởng. Có nghĩa là những người dùng đã sở hữu các tập tin/thư mục trên volume này đều không bị chính sách hạn ngạch quy định. Như vậy, nếu bạn dự định áp đặt hạn ngạch cho tất cả các người dùng, bạn phải chỉ định hạn ngạch ngay từ khi tạo lập **volume**.



Để thực hiện, bạn mở hộp thoại **Volume Properties** và chọn tab **Quota**. Đánh dấu chọn mục **Enable quota management** và điền vào các giá trị giới hạn sử dụng và giới hạn cảnh báo.

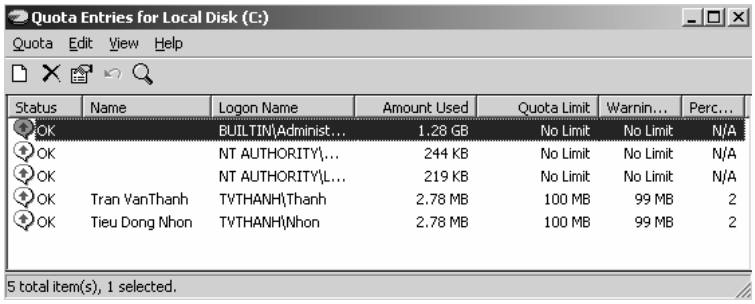
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

## V.3. Chỉ định hạn ngạch cho từng cá nhân.

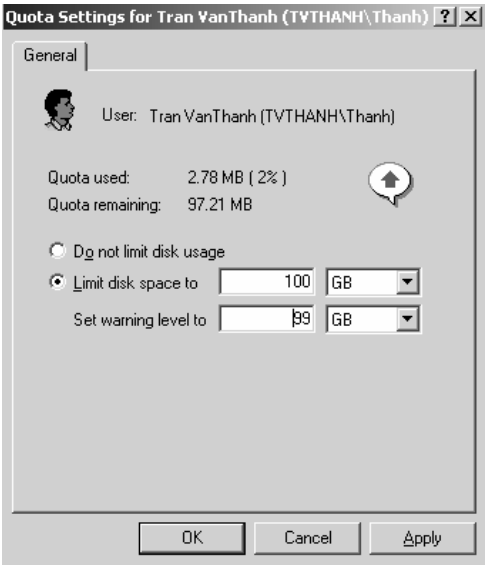
Trong một vài trường hợp, bạn cần phải chỉ định hạn ngạch cho riêng một người nào đó, chẳng hạn có thể là các lý do sau:

- Người dùng này sẽ giữ nhiệm vụ cài đặt các phần mềm mới, và như vậy họ phải có được lượng không gian đĩa trống lớn.
- Hoặc là người dùng đã tạo nhiều tập tin trên **volume** trước khi thiết lập hạn ngạch, do vậy họ sẽ không chịu tác dụng. Bạn phải tạo riêng một giới hạn mới áp dụng cho người đó.

Để thiết lập, nhấn nút **Quota Entries** trong tab **Quota** của hộp thoại **Volume Properties**. Cửa sổ **Quota Entries** xuất hiện.




**Chỉnh sửa thông tin hạn ngạch của một người dùng:** nhấn đúp vào mục của người dùng tương ứng, hộp thoại **Quota Setting** xuất hiện cho phép bạn thay đổi các giá trị hạn ngạch.




**Bổ sung thêm một mục quy định hạn ngạch:** trong cửa sổ **Quota Entries**, vào menu **Quota** chọn mục **New Quota Entry** ⏲ xuất hiện hộp thoại **Select Users**, bạn chọn người dùng rồi nhấn **OK** ⏲ xuất hiện hộp thoại **Add New Quota Entry**, bạn nhập các giá trị hạn ngạch thích hợp và nhấn **OK**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

# VI. MÃ HOÁ DỮ LIỆU BẰNG EFS.

**EFS (Encrypting File System)** là một kỹ thuật dùng trong **Windows Server 2003** dùng để mã hoá các tập tin lưu trên các **partition NTFS**. Việc mã hoá sẽ bổ sung thêm một lớp bảo vệ an toàn cho hệ thống tập tin. Chỉ người dùng có đúng khoá mới có thể truy xuất được các tập tin này còn những người khác thì bị từ chối truy cập. Ngoài ra, người quản trị mạng còn có thể dùng tác nhân phục hồi (**recovery agent**) để truy xuất đến bất kỳ tập tin nào bị mã hoá. Để mã hoá các tập tin, tiến hành theo các bước sau:

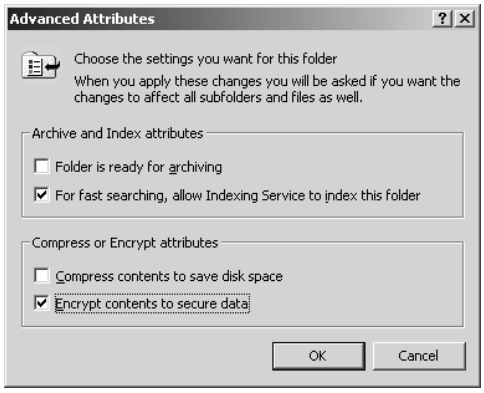
Mở cửa sổ **Windows Explorer**.

Trong cửa sổ **Windows Explorer**, chọn các tập tin và thực mục cần mã hoá.

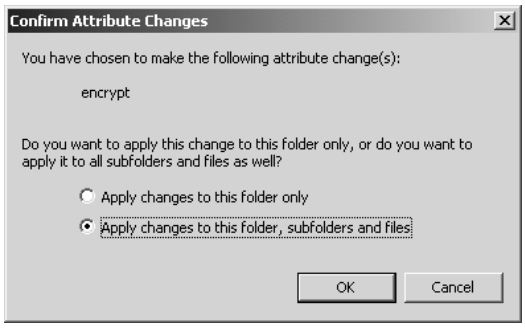
Nhấp phải chuột lên các tập tin và thư mục, chọn **Properties**.

Trong hộp thoại **Properties**, nhấn nút **Advanced**.

Hộp thoại **Advanced Properties** xuất hiện, đánh dấu mục **Encrypt contents to secure data** và nhấn OK.




Trở lại hộp thoại **Properties**, nhấn **OK**, xuất hiện hộp thoại **Confirm Attribute Changes** yêu cần bạn cho biết sẽ mã hoá chỉ riêng thư mục được chọn (**Apply changes to this folder only**) hoặc mã hoá toàn bộ thư mục kể các các thư mục con (**Apply changes to this folder, subfolders and files**). Sau đó nhấn **OK**.






Để thôi không mã hoá các tập tin, bạn thực hiện tương tự theo các bước trên nhưng bỏ chọn mục **Encrypt contents to secure data**.

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Bài 14
# TẠO VÀ QUẢN LÝ THƯ MỤC DÙNG CHUNG

## Tóm tắt

Lý thuyết 4 tiết - Thực hành 10 tiết

| Mục tiêu | Các mục chính | Bài tập bắt buộc | Bài tập làm thêm |
|---|---|---|---|
| Kết thúc bài học này cung cấp học viên kiến thức về các loại quyền truy cập, tạo và quản lý các thư mục dùng chung trên mạng, NTFS, DFS… | I. Tạo các thư mục dùng chung.<br>II. Quản lý các thư mục dùng chung.<br>III. Quyền truy cập NTFS.<br>IV. DFS. | Dựa vào bài tập môn Quản trị Windows Server 2003. | Dựa vào bài tập môn Quản trị Windows Server 2003. |

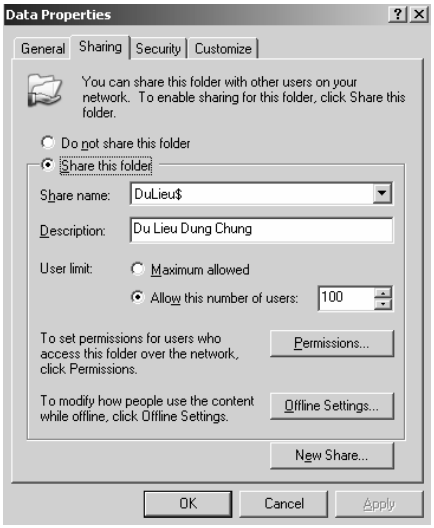


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

# I. TẠO CÁC THƯ MỤC DÙNG CHUNG.

## I.1. Chia sẻ thư mục dùng chung.

Các tài nguyên chia sẻ là các tài nguyên trên mạng mà các người dùng có thể truy xuất và sử dụng thông qua mạng. Muốn chia sẻ một thư mục dùng chung trên mạng, bạn phải **logon** vào hệ thống với vai trò người quản trị (**Administrators**) hoặc là thành viên của nhóm **Server Operators**, tiếp theo trong **Explorer** bạn nhấp phải chuột trên thư mục đó và chọn **Properties**, hộp thoại **Properties** xuất hiện, chọn **Tab Sharing**.




Ý nghĩa của các mục trong **Tab Sharing**:

| Mục | Mô tả |
|---|---|
| Do not share this folder | Chỉ định thư mục này chỉ được phép truy cập cục bộ |
| Share this folder | Chỉ định thư mục này được phép truy cập cục bộ và truy cập qua mạng |
| Share name | Tên thư mục mà người dùng mạng nhìn thấy và truy cập |
| Comment | Cho phép người dùng mô tả thêm thông tin về thư mục dùng chung này |
| User Limit | Cho phép bạn khai báo số kết nối tối đa truy xuất vào thư mục tại một thời điểm |
| Permissions | Cho phép bạn thiết lập danh sách quyền truy cập thông qua mạng của người dùng |
| Offline Settings | Cho phép thư mục được lưu trữ tạm tài liệu khi làm việc dưới chế độ **Offline**. |



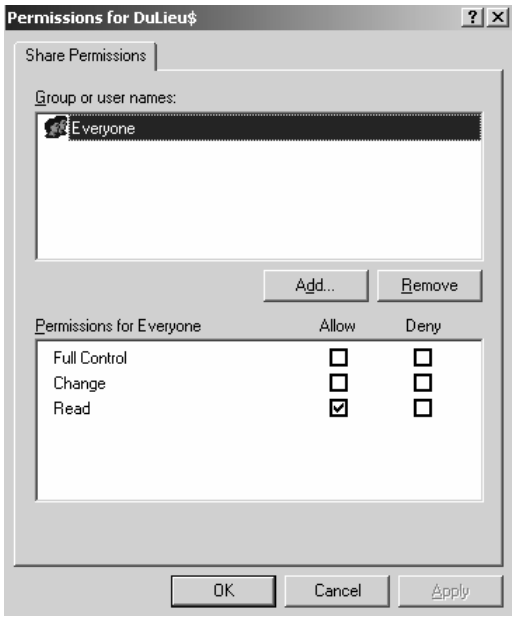
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

## I.2. Cấu hình Share Permissions.

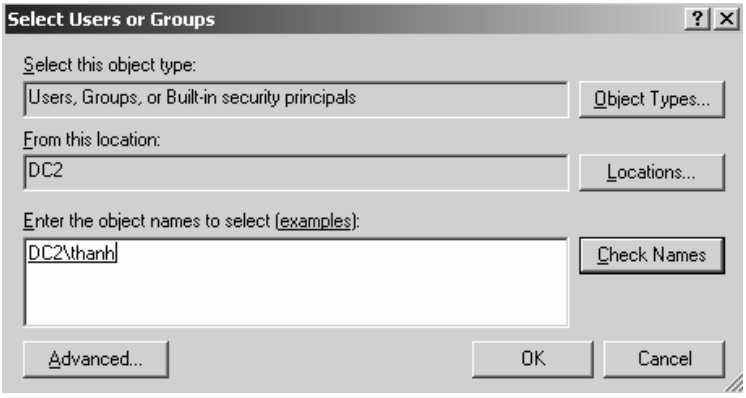
Bạn muốn cấp quyền cho các người dùng truy cập qua mạng thì dùng **Share Permissions**. **Share Permissions** chỉ có hiệu lực khi người dùng truy cập qua mạng chứ không có hiệu lực khi người dùng truy cập cục bộ. Khác với **NTFS Permissions** là quản lý người dùng truy cập dưới cấp độ truy xuất đĩa. Trong hộp thoại **Share Permissions**, chứa danh sách các quyền sau:

- **Full Control**: cho phép người dùng có toàn quyền trên thư mục chia sẻ.
- **Change**: cho phép người dùng thay đổi dữ liệu trên tập tin và xóa tập tin trong thư mục chia sẻ.
- **Read**: cho phép người dùng xem và thi hành các tập tin trong thư mục chia sẻ.

Bạn muốn cấp quyền cho người dùng thì nhấp chuột vào nút **Add**.



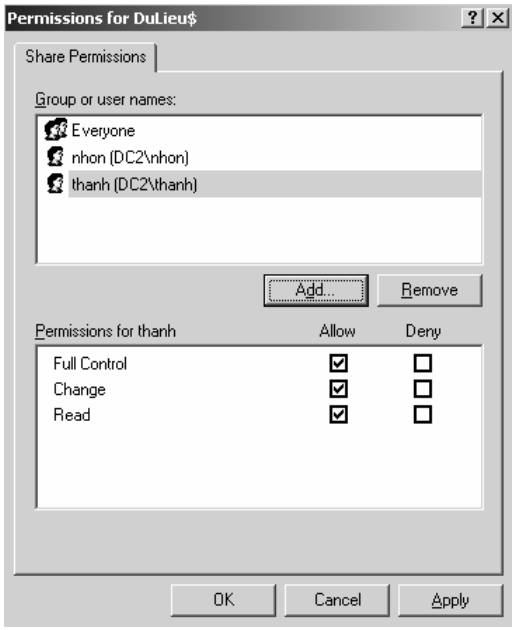

Hộp thoại chọn người dùng và nhóm xuất hiện, bạn nhấp đôi chuột vào các tài khoản người dùng và nhóm cần chọn, sau đó chọn **OK**.




Trong hộp thoại xuất hiện, muốn cấp quyền cho người dùng bạn đánh dấu vào mục **Allow**, ngược lại khóa quyền thì đánh dấu vào mục **Deny**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




## I.3. Chia sẻ thư mục dùng lệnh netshare.

Chức năng: tạo, xóa và hiển thị các tài nguyên chia sẻ.

Cú pháp:

net share sharename

net share sharename=drive:path [/users:number | /unlimited] [/remark:"text"]

net share sharename [/users:number | unlimited] [/remark:"text"]

net share {sharename | drive:path} /delete

Ý nghĩa các tham số:

- [Không tham số]: hiển thị thông tin về tất cả các tài nguyên chia sẻ trên máy tính cục bộ
- [**Sharename**]: tên trên mạng của tài nguyên chia sẻ, nếu dùng lệnh **net share** với một tham số **sharename** thì hệ thống sẽ hiển thị thông tin về tài nguyên dùng chung này.
- [**drive:path**]: chỉ định đường dẫn tuyệt đối của thư mục cần chia sẻ.
- [**/users:number**]: đặt số lượng người dùng lớn nhất có thể truy cập vào tài nguyên dùng chung này.
- [**/unlimited**]: không giới hạn số lượng người dùng có thể truy cập vào tài nguyên dùng chung này.
- [**/remark:"text"**]: thêm thông tin mô tả về tài nguyên này.
- **/delete**: xóa thuộc tính chia sẻ của thư mục hiện tại.

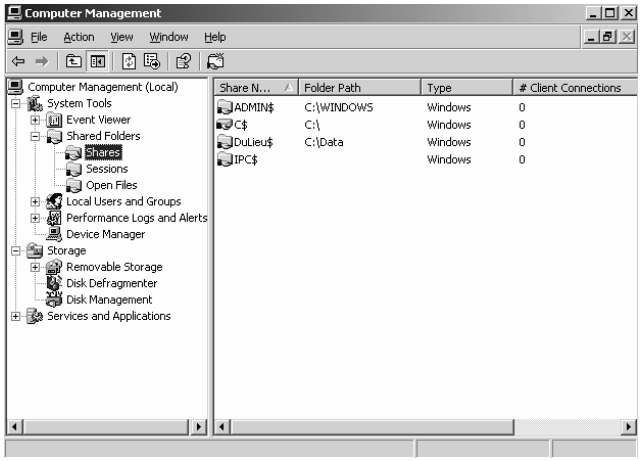


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

# II. QUẢN LÝ CÁC THƯ MỤC DÙNG CHUNG.

## II.1. Xem các thư mục dùng chung.

Mục **Shared Folders** trong công cụ **Computer Management** cho phép bạn tạo và quản lý các thư mục dùng chung trên máy tính. Muốn xem các thư mục dùng chung trên máy tính bạn chọn mục **Shares**. Nếu thư mục dùng chung nào có phần cuối của tên chia sẻ (**share name**) là dấu **$** thì tên thư mục dùng chung này được ẩn đi và không tìm thấy khi bạn tìm kiếm thông qua **My Network Places** hoặc duyệt các tài nguyên mạng.



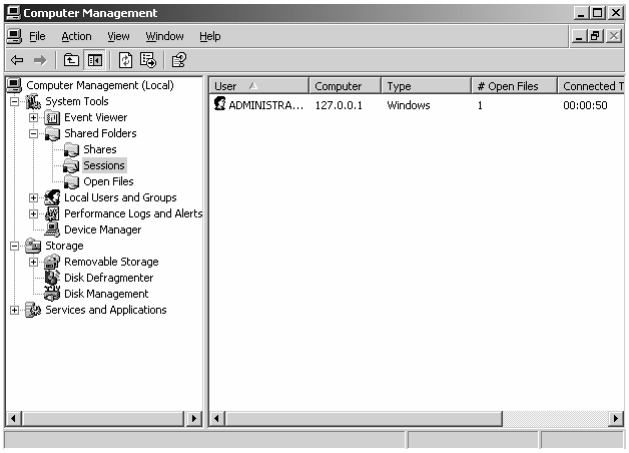

## II.2. Xem các phiên làm việc trên thư mục dùng chung.

Muốn xem tất cả các người dùng đang truy cập đến các thư mục dùng chung trên máy tính bạn chọn mục **Session**. Mục **Session** cung cấp các thông tin sau:

- Tên tài khoản người dùng đang kết nối vào tài nguyên chia sẻ.
- Tên máy tính có người dùng kết nối từ đó.
- Hệ điều hành mà máy trạm đang sử dụng để kết nối.
- Số tập tin mà người dùng đang mở.
- Thời gian kết nối của người dùng.
- Thời gian chờ xử lý của kết nối.
- Phải là truy cập của người dùng **Guest** không?



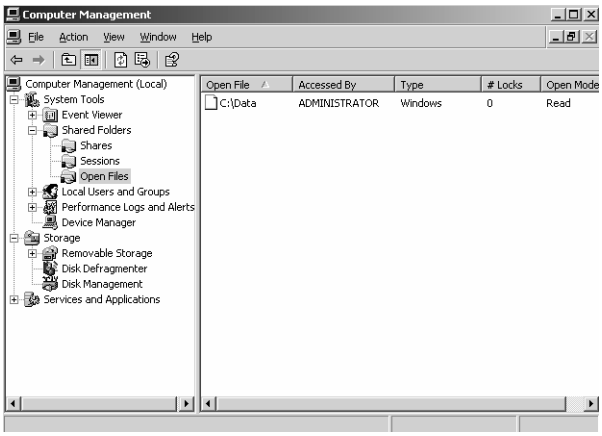
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




## II.3. Xem các tập tin đang mở trong các thư mục dùng chung.

Muốn xem các tập đang mở trong các thư mục dùng chung bạn nhấp chuột vào mục **Open Files**. Mục **Open Files** cung cấp các thông tin sau:

- Đường dẫn và tập tin hiện đang được mở.
- Tên tài khoản người dùng đang truy cập tập tin đó.
- Hệ điều hành mà người dùng sử dụng để truy cập tập tin.
- Trạng thái tập tin có đang bị khoá hay không.
- Trạng thái mở sử dụng tập tin (**Read** hoặc **Write**).

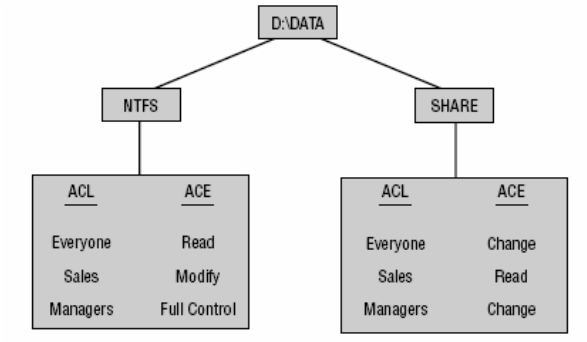



# III. QUYỀN TRUY CẬP NTFS.

Có hai loại hệ thống tập được dùng cho **partition** và **volume** cục bộ là **FAT** (bao gồm **FAT16** và **FAT32**). **FAT partition** không hỗ trợ bảo mật nội bộ, còn **NTFS partition** thì ngược lại có hỗ trợ bảo mật; có nghĩa là nếu đĩa cứng của bạn định dạng là **FAT** thì mọi người đều có thể thao tác trên các file chứa trên đĩa cứng này, còn ngược lại là định dạng **NTFS** thì tùy theo người dùng có quyền truy cập không, nếu người dùng không có quyền thì không thể nào truy cập được dữ liệu trên đĩa. Hệ thống **Windows Server 2003** dùng các **ACL (Access Control List)** để quản lý các quyền truy cập của đối tượng cục bộ và các đối tượng trên **Active Directory**. Một **ACL** có thể chứa nhiều **ACE (Access Control Entry)** đại diện cho một người dùng hay một nhóm người.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




## III.1. Các quyền truy cập của NTFS.

| Tên quyền | Chức năng |
|---|---|
| Traverse Folder/Execute File | Duyệt các thư mục và thi hành các tập tin chương trình trong thư mục |
| List Folder/Read Data | Liệt kê nội dung của thư mục và đọc dữ liệu của các tập tin trong thư mục |
| Read Attributes | Đọc các thuộc tính của các tập tin và thư mục |
| Read Extended Attributes | Đọc các thuộc tính mở rộng của các tập tin và thư mục |
| Create File/Write Data | Tạo các tập tin mới và ghi dữ liệu lên các tập tin này |
| Create Folder/Append Data | Tạo thư mục mới và chèn thêm dữ liệu vào các tập tin |
| Write Attributes | Thay đổi thuộc tính của các tập tin và thư mục |
| Write Extendd Attributes | Thay đổi thuộc tính mở rộng của các tập tin và thư mục |
| Delete Subfolders and Files | Xóa thư mục con và các tập tin |
| Delete | Xóa các tập tin |
| Read Permissions | Đọc các quyền trên các tập tin và thư mục |
| Change Permissions | Thay đổi quyền trên các tập tin và thư mục |
| Take Ownership | Tước quyền sở hữu của các tập tin và thư mục |



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

## III.2. Các mức quyền truy cập được dùng trong NTFS.

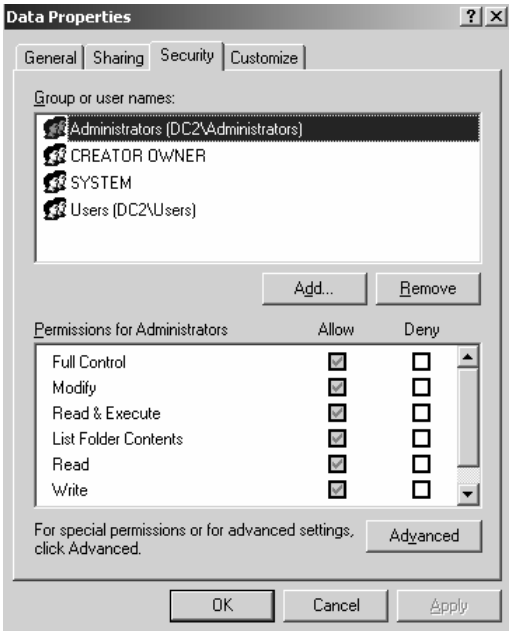
| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| X | X | X | X | X | X | X | X | X | X | X | X | X | |
| | | X | X | | X | X | X | X | X | X | X | X | |
| | | | | | | | | | X | X | X | X | |
| | | X | | | | | | | X | X | X | X | |
| | | X | | | | | | | X | X | X | | |
| | | X | | | X | X | X | | | | | | |

## III.3. Gán quyền truy cập NTFS trên thư mục dùng chung.

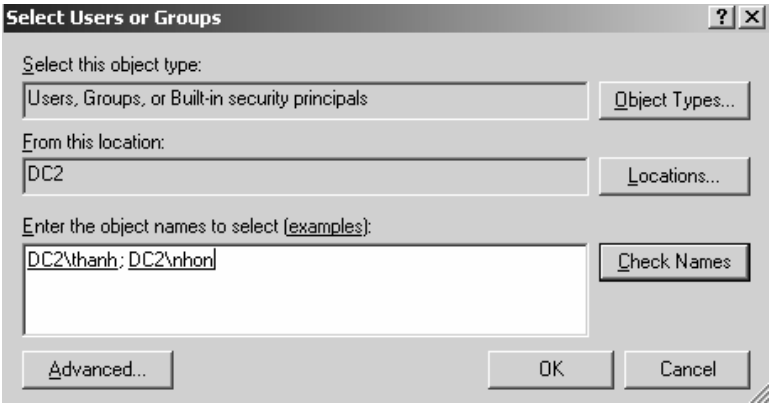
Bạn muốn gán quyền **NTFS**, thông qua **Windows Explorer** bạn nhấp phải chuột vào tập tin hay thư mục cần cấu hình quyền truy cập rồi chọn **Properties**. Hộp thoại **Properties** xuất hiện. Nếu ổ đĩa của bạn định dạng là **FAT** thì hộp thoại chỉ có hai **Tab** là **General** và **Sharing**. Nhưng nếu đĩa có định dạng là **NTFS** thì trong hộp thoại sẽ có thêm một **Tab** là **Security**. Tab này cho phép ta có thể quy định quyền truy cập cho từng người dùng hoặc một nhóm người dùng lên các tập tin và thư mục. Bạn nhấp chuột vào **Tab Security** để cấp quyền cho các người dùng.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net



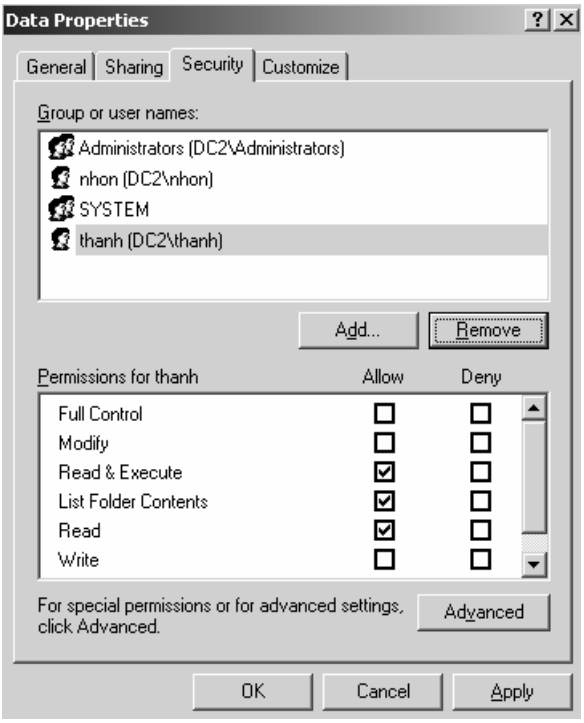

Muốn cấp quyền truy cập cho một người dùng, bạn nhấp chuột vào nút **Add**, hộp thoại chọn lựa người dùng và nhóm xuất hiện, bạn chọn người dùng và nhóm cần cấp quyền, nhấp chuột vào nút **Add** để thêm vào danh sách, sau đó nhấp chuột vào nút **OK** để trở lại hộp thoại chính.




Hộp thoại chính sẽ xuất hiện các người dùng và nhóm mà bạn mới thêm vào, sau đó chọn người dùng và nhóm để cấp quyền. Trong hộp thoại đã hiện sẵn danh sách quyền, bạn muốn cho người dùng đó có quyền gì thì bạn đánh dấu vào phần **Allow**, còn ngược lại muốn cấm quyền đó thì đánh dấu vào mục **Deny**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

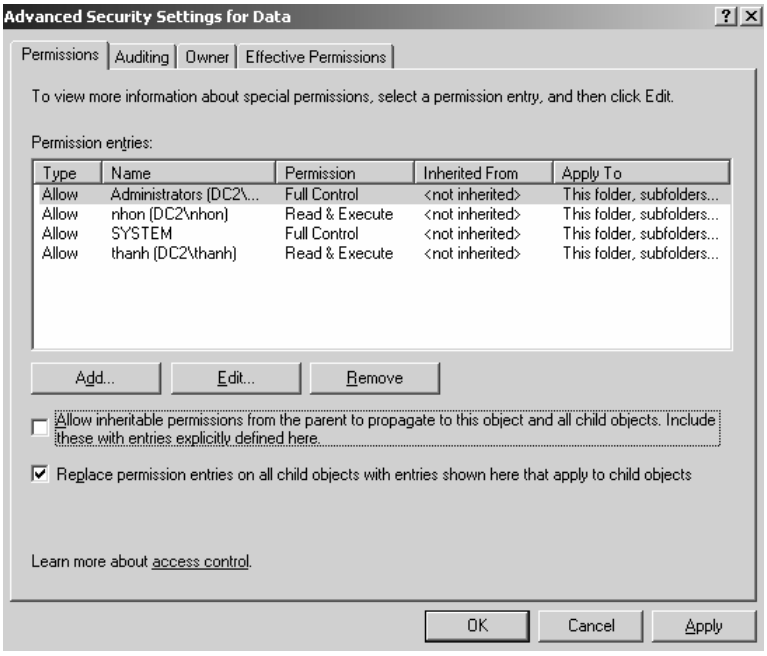



## III.4. Kế thừa và thay thế quyền của đối tượng con.

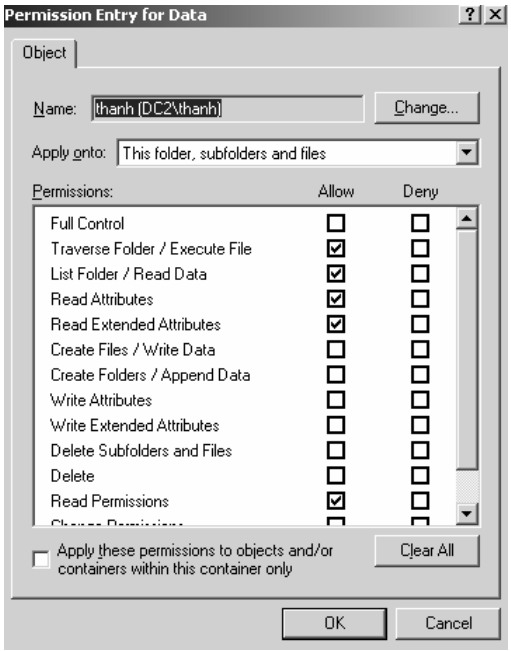
Trong hộp thoại chính trên, chúng ta có thể nhấp chuột vào nút **Advanced** để cấu hình chi tiết hơn cho các quyền truy cập của người dùng. Khi nhấp chuột vào nút **Advanced**, hộp thoại **Advanced Security Settings** xuất hiện, trong hộp thoại, nếu bạn đánh dấu vào mục **Allow inheritable permissions from parent to propagate to this object and child objects** thì thư mục hiện tại được thừa hưởng danh sách quyền truy cập từ thư mục cha, bạn muốn xóa những quyền thừa hưởng từ thư mục cha bạn phải bỏ đánh dấu này. Nếu danh sách quyền truy cập của thư mục cha thay đổi thì danh sách quyền truy cập của thư mục hiện tại cũng thay đổi theo. Ngoài ra nếu bạn đánh dấu vào mục **Replace permission entries on all child objects with entries shown here that apply to child objects** thì danh sách quyền truy cập của thư mục hiện tại sẽ được áp dụng xuống các tập tin và thư mục con có nghĩa là các tập tin và thư mục con sẽ được thay thế quyền truy cấp giống như các quyền đang hiển thị trong hộp thoại.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Trong hộp thoại này, **Windows Server 2003** cũng cho phép chúng ta kiểm tra và cấu hình lại chi tiết các quyền của người dùng và nhóm, để thực hiện, bạn chọn nhóm hay người dùng cần thao tác, sau đó nhấp chuột vào nút **Edit.**




## III.5. Thay đổi quyền khi di chuyển thư mục và tập tin.

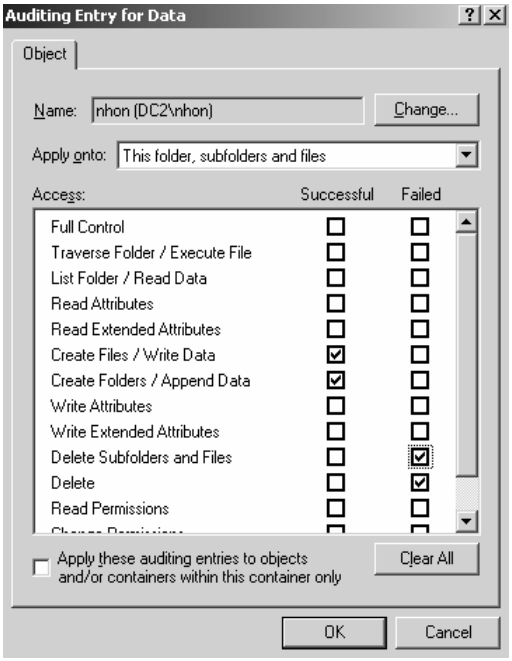
Khi chúng ta sao chép (**copy**) một tập tin hay thư mục sang một vị trí mới thì quyền truy cập trên tập tin hay thư mục này sẽ thay đổi theo quyền trên thư mục cha chứa chúng, nhưng ngược lại nếu chúng ta di chuyển (**move**) một tập tin hay thư mục sang bất kì vị trí nào thì các quyền trên chúng vẫn được giữ nguyên.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

## III.6. Giám sát người dùng truy cập thư mục.

Bạn muốn giám sát và ghi nhận lại các người dùng thao tác trên thư mục hiện tại, trong hộp thoại **Advanced Security Settings**, chọn **Tab Auditing**, nhấp chuột vào nút **Add** để chọn người dùng cần giám sát, sau đó bạn muốn giám sát việc truy xuất thành công thì đánh dấu vào mục **Successful**, ngược lại giám sát việc truy xuất không thành công thì đánh dấu vào mục **Failed**.

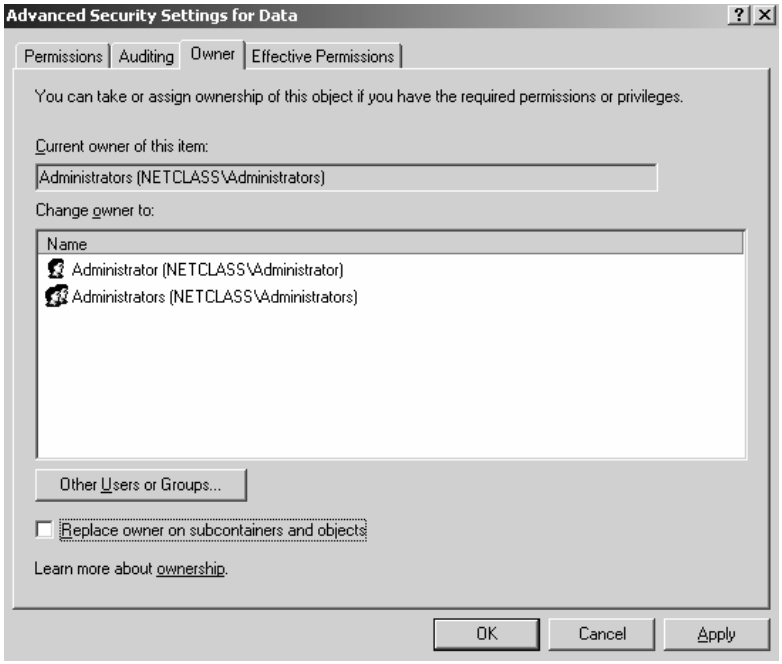



## III.7. Thay đổi người sở hữu thư mục.

Bạn muốn xem tài khoản người và nhóm người dùng sở hữa thư mục hiện tại, trong hộp thoại **Advanced Security Settings**, chọn **Tab Owner.** Đồng thời bạn cũng có thể thay đổi người và nhóm người sở hữu thư mục này bằng cách nhấp chuột vào nút **Other Users or Groups**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




# IV. DFS.

**DFS** (**Distributed File System**) là hệ thống tổ chức sắp xếp các thư mục, tập tin dùng chung trên mạng mà **Server** quản lý, ở đó bạn có thể tập hợp các thư mục dùng chung nằm trên nhiều **Server** khác nhau trên mạng với một tên chia sẻ duy nhất. Nhờ hệ thống này mà người dùng dễ dàng tìm kiếm một tài nguyên dùng chung nào đó trên mạng… **DFS** có hai loại **root**: **domain root** là hệ thống **root** gắn kết vào **Active Directory** được chứa trên tất cả **Domain Controller**, **Stand-alone root** chỉ chứa thông tin ngay tại máy được cấu hình. Chú ý **DFS** không phải là một **File Server** mà nó là chỉ là một "bảng mục lục" chỉ đến các thư mục đã được tạo và chia sẻ sẵn trên các **Server**. Để triển khai một hệ thống **DFS** trước tiên bạn phải hiểu các khái niệm sau:

- Gốc **DFS** (**DFS root**) là một thư mục chia sẻ đại diện cho chung cho các thư mục chia sẻ khác trên các **Server**.
- Liên kết **DFS** (**DFS link**) là một thư mục nằm trong **DFS root**, nó ánh xạ đến một tài nguyên chia sẻ các **Server** khác.

## IV.1. So sánh hai loại DFS.

| Stand-alone DFS | Fault-tolerant DFs |
|---|---|
| - Là hệ thống DFS trên một máy **Server Stand-alone**, không có khả năng dung lỗi.<br>- Người dùng truy xuất hệ thống DFS thông qua đường dẫn \\servername\dfsname. | - Là hệ thống **DFS** dựa trên nền **Active Directory** nên có chính dung lỗi cao.<br>- Hệ thống **DFS** sẽ tự động đồng bộ giữa các **Domain Controller** và người dùng có thể truy xuất đến **DFS** thông qua đường dẫn **\\domainname\dfsname**. |

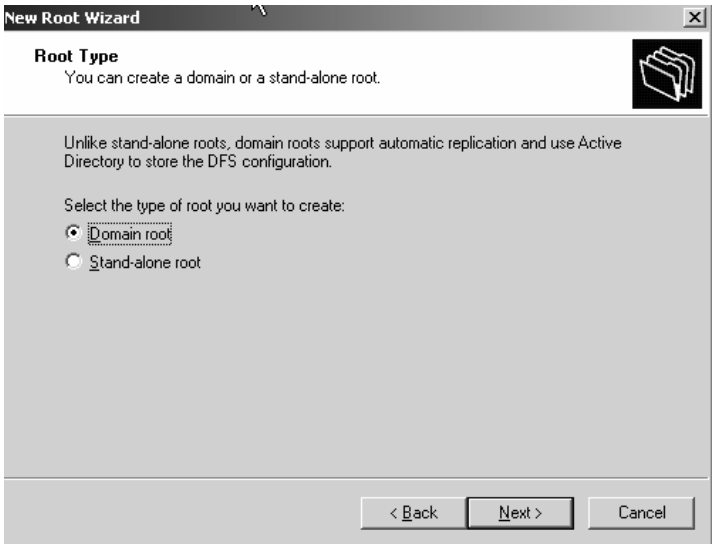


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

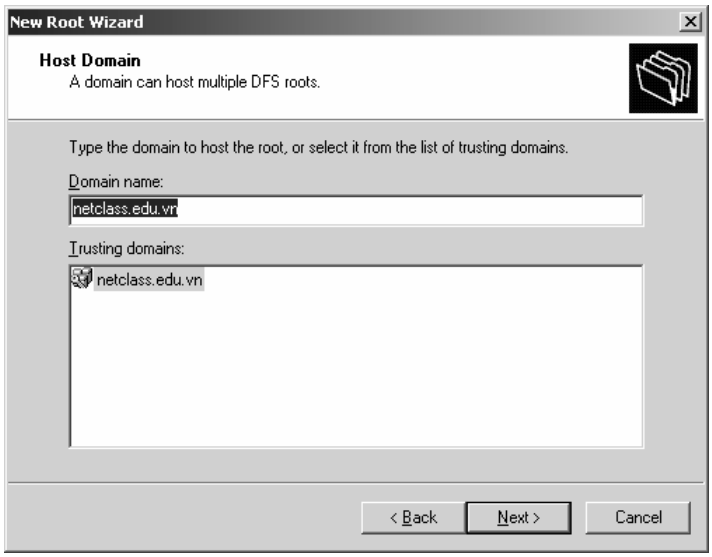
## IV.2. Cài đặt Fault-tolerant DFS.

Để tạo một hệ thống **Fault-tolerant DFS** bạn làm theo các bước sau:

Bạn nhấp chuột vào **Start** 🕘 **Programs** 🕘 **Administrative Tools** 🕘 **Distributed File System**. Hộp thoại **Welcome** xuất hiện, bạn nhấn **Next** để tiếp tục. Hộp thoại **Root Type** xuất hiện, bạn chọn mục **Domain Root**, nhấn **Next** để tiếp tục.



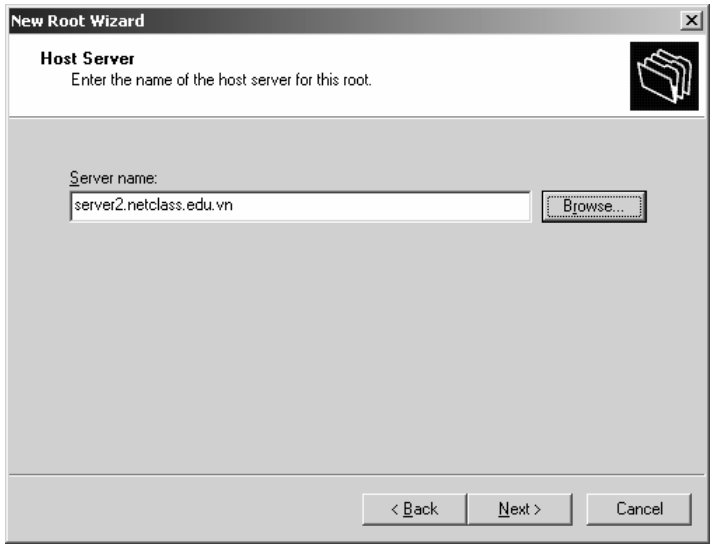

Hệ thống yêu cầu bạn chọn tên miền **(domain name**) kết hợp với hệ thống **DFS** cần tạo.




Tiếp theo bạn khai báo tên của **Domain Controller** chưa **root DFS** cần tạo.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

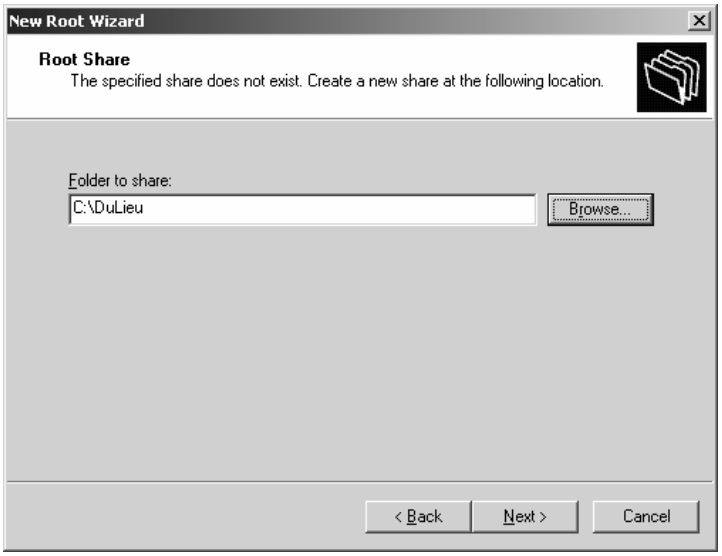



Đến đây bạn khai báo tên chia sẻ gốc (**Root Name**) của hệ thống **DFS**, đây chính là tên chia sẻ đại diện cho các tài nguyên khác trên mạng. Bạn nhập đầy đủ các thông tin chọn **Next** để tiếp tục.

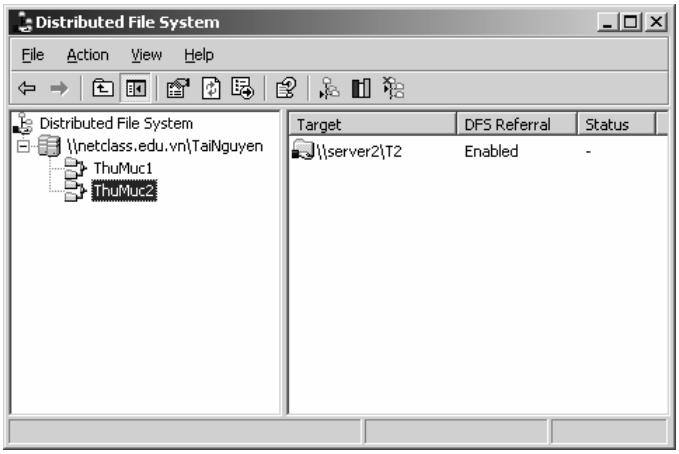

Trong hộp thoại xuất hiện, bạn khai báo tên thư mục chia sẻ gốc của hệ thống **DFS**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Sau khi cấu hình hệ thống **DFS** hoàn tất, tiếp theo bạn tạo các liên kết đến các tài nguyên dùng chung trên các **Server** khác trong mạng.




Để sử dụng hệ thống **DFS** này, tại máy trạm bạn ánh xạ (**map**) thư mục chia sẻ gốc thành một ổ đĩa mạng. Trong ổ đĩa mạng này bạn có thể nhìn thấy tất cả các thư mục chia sẻ trên các **Server** khác nhau trên hệ thống mạng.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net


Tương tự như **Fault-tolerant DFS**, bạn có thể tạo ra một **Stand-alone DFS** trên một máy **Server Stand-alone**, tất nhiên là hệ thống đó không có khả năng dung lỗi có nghĩa là khi **Server** chứa **DFS Root** hỏng thì các máy trạm sẽ không tìm thấy các tài nguyên chia sẻ trên các **Server** khác. Nhưng hệ thống **Stand-alone DFS** được sử dụng rộng rải vì nó đơn giản, tiện dụng.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

# Tóm tắt

Lý thuyết 2 tiết - Thực hành 3 tiết

| Mục tiêu | Các mục chính | Bài tập bắt buộc | Bài tập làm thêm |
|---|---|---|---|
| Kết thúc bài học này cung cấp học viên kiến thức về dịch vụ cấp phát địa chỉ IP động cho các máy trạm … | I. Giới thiệu dịch vụ DHCP.<br>II. Hoạt động của giao thức DHCP.<br>III. Cài đặt dịch vụ DHCP.<br>IV. Chứng thực dịch vụ DHCP trong Active Directory.<br>V. Cấu hình dịch vụ DHCP | Dựa vào bài tập môn Quản trị Windows Server 2003. | Dựa vào bài tập môn Quản trị Windows Server 2003. |



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

# I. GIỚI THIỆU DỊCH VỤ DHCP.

Mỗi thiết bị trên mạng có dùng bộ giao thức **TCP/IP** đều phải có một địa chỉ **IP** hợp lệ, phân biệt. Để hỗ trợ cho vấn đề theo dõi và cấp phát các địa chỉ **IP** được chính xác, tổ chức **IETF** (**Internet Engineering Task Force**) đã phát triển ra giao thức **DHCP** (**Dynamic Host Configuration Protocol**). Giao thức này được mô tả trong các **RFC 1533, 1534, 1541** và **1542**. Bạn có thể tìm thấy các **RFC** này tại địa chỉ **http://www.ietf.org/rfc.html**. Để có thể làm một **DHCP Server**, máy tính **Windows Server 2003** phải đáp ứng các điều kiện sau:

- Đã cài dịch vụ **DHCP**.
- Mỗi **interface** phải được cấu hình bằng một địa chỉ **IP** tĩnh.
- Đã chuẩn bị sẵn danh sách các địa chỉ **IP** định cấp phát cho các máy **client**.

Dịch vụ **DHCP** này cho phép chúng ta cấp động các thông số cấu hình mạng cho các máy trạm (**client**). Các hệ điều hành của **Microsoft** và các hệ điều hành khác như **Unix** hoặc **Macintosh** đều hỗ trợ cơ chế nhận các thông số động, có nghĩa là trên các hệ điều hành này phải có một **DHCP Client**. Cơ chế sử dụng các thông số mạng được cấp phát động có ưu điểm hơn so với cơ chế khai báo tĩnh các thông số mạng như:

- Khắc phục được tình trạng đụng địa chỉ **IP** và giảm chi phí quản trị cho hệ thống mạng.
- Giúp cho các nhà cung cấp dịch vụ (**ISP**) tiết kiệm được số lượng địa chỉ **IP** thật (**Public IP**).
- Phù hợp cho các máy tính thường xuyên di chuyển qua lại giữa các mạng.
- Kết hợp với hệ thống mạng không dây (**Wireless**) cung cấp các điểm **Hotspot** như: nhà ga, sân bay, trường học…

# II. HOẠT ĐỘNG CỦA GIAO THỨC DHCP.

Giao thức **DHCP** làm việc theo mô hình **client/server**. Theo đó, quá trình tương tác giữa **DHCP client** và **server** diễn ra theo các bước sau:

- Khi máy **client** khởi động, máy sẽ gửi **broadcast** gói tin **DHCPDISCOVER**, yêu cầu một **server** phục vụ mình. Gói tin này cũng chứa địa chỉ **MAC** của máy **client.**
- Các máy **Server** trên mạng khi nhận được gói tin yêu cầu đó, nếu còn khả năng cung cấp địa chỉ **IP**, đều gửi lại cho máy **Client** gói tin **DHCPOFFER**, đề nghị cho thuê một địa chỉ **IP** trong một khoản thời gian nhất định, kèm theo là một **subnet mask** và địa chỉ của **Server**. **Server** sẽ không cấp phát địa chỉ **IP** vừa đề nghị cho những **Client** khác trong suốt quá trình thương thuyết.
- Máy **Client** sẽ lựa chọn một trong những lời đề nghị (**DHCPOFFER**) và gửi **broadcast** lại gói tin **DHCPREQUEST** chấp nhận lời đề nghị đó. Điều này cho phép các lời đề nghị không được chấp nhận sẽ được các **Server** rút lại và dùng để cấp phát cho **Client** khác.
- Máy **Server** được **Client** chấp nhận sẽ gửi ngược lại một gói tin **DHCPACK** như là một lời xác nhận, cho biết là địa chỉ **IP** đó, **subnet mask** đó và thời hạn cho sử dụng đó sẽ chính thức được áp dụng. Ngoài ra **Server** còn gửi kèm theo những thông tin cấu hình bổ sung như địa chỉ của **gateway** mặc định, địa chỉ **DNS Server**, …



# III. CÀI ĐẶT DỊCH VỤ DHCP.

Thực hiện theo các bước sau:

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Chọn menu **Start** 🕘 **Settings** 🕘 **Control Panel**.

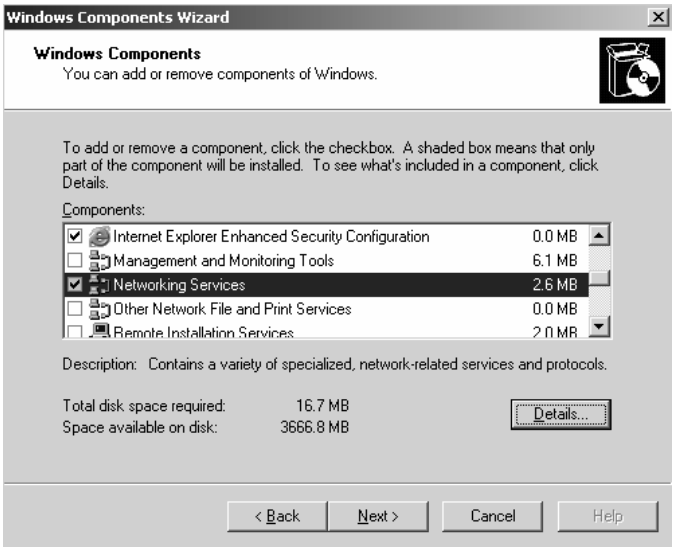


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

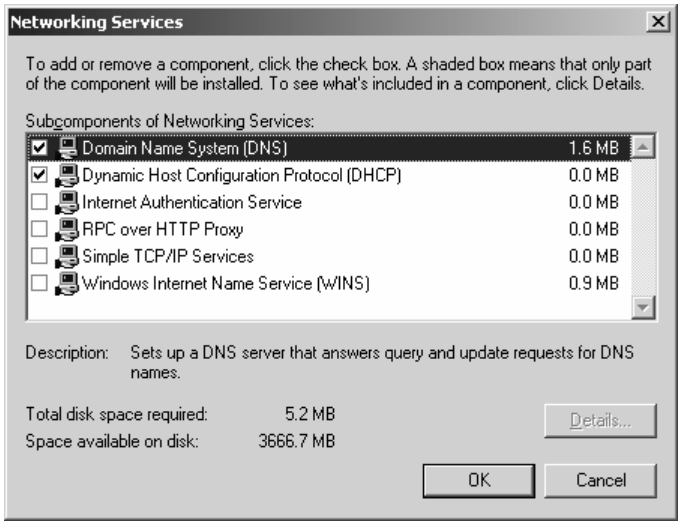
Trong cửa sổ **Control Panel**, nhấp đôi chuột vào mục **Add/Remove Programs.**

Trong hộp thoại **Add/Remove Programs**, nhấp chọn mục **Add/Remove Windows Components**.

Trong hộp thoại **Windows Components Wizard**, tô sáng **Networking Services** và nhấn nút **Details**.




Trong hộp thoại **Networking Services**, nhấn chọn mục **Dynamic Host Configuration Protocol** (**DHCP**) và nhấn nút **OK**.

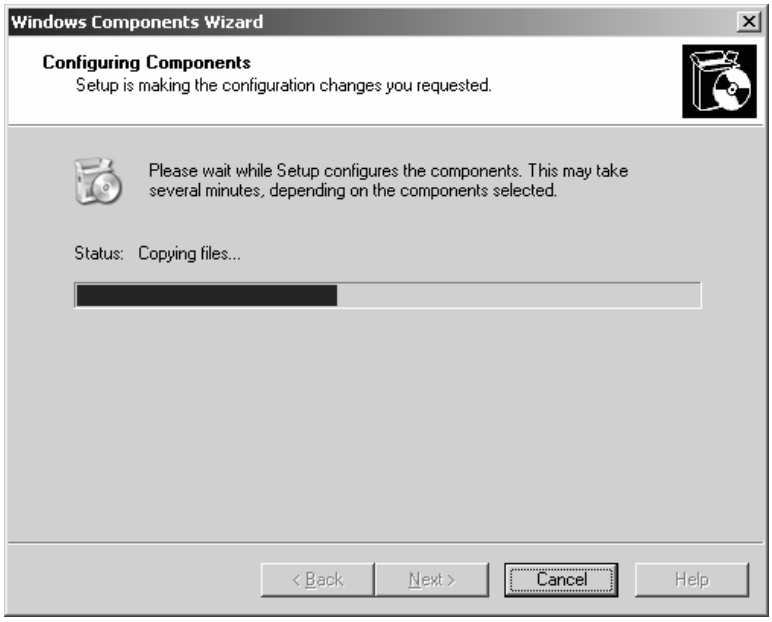



Trở lại hộp thoại **Windows Components Wizard**, nhấn chọn **Next**.

**Windows 2000** sẽ cấu hình các thành phần và cài đặt dịch vụ **DHCP.**



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Cuối cùng, trong hộp thoại **Completing the Windows Components Wizard**, nhấn chọn **Finish** để kết thúc.

# IV. CHỨNG THỰC DỊCH VỤ DHCP TRONG ACTIVE DIRECTORY.

Nếu máy tính **Windows Server 2003** chạy dịch vụ **DHCP** trên đó lại làm việc trong một **domain** (có thể là một **Server** thành viên bình thường hoặc là một máy điều khiển vùng), dịch vụ muốn có thể hoạt động bình thường thì phải được chứng thực bằng **Active Directory**.

Mục đích của việc chứng thực này là để không cho các **Server** không được chứng thực làm ảnh hưởng đến hoạt động mạng. Chỉ có những **Windows 2003 DHCP seRver** được chứng thực mới được phép hoạt động trên mạng. Giả sử có một nhân viên nào đó cài đặt dịch vụ **DHCP** và cấp những thông tin **TCP/IP** không chính xác. **DHCP Server** của nhân viên này không thể hoạt động được (do không được quản trị mạng cho phép) và do đó không ảnh hưởng đến hoạt động trên mạng. Chỉ có **Windows 2003 DHCP Server** mới cần được chứng thực trong **Active Directory**. Còn các **DHCP server** chạy trên các hệ điều hành khác như **Windows NT, UNIX**, … thì không cần phải chứng thực.

Trong trường hợp máy **Windows Server 2003** làm **DHCP Server** không nằm trong một **domain** thì cũng không cần phải chứng thực trong **Active Directory**. Bạn có thể sử dụng công cụ quản trị **DHCP** để tiến hành việc chứng thực một **DHCP Server**. Các bước thực hiện như sau:

Chọn menu **Start** 🕘 **Administrative Tools** 🕘 **DHCP**.

Trong ô bên trái của cửa sổ **DHCP,** tô sáng **Server** bạn định chứng thực. Chọn **menu Action** 🕘 **Authorize.**

Đợi một hoặc hai phút sau, chọn lại menu **Action** 🕘 **Refresh.**

Bây giờ **DHCP** đã được chứng thực, bạn để ý biểu tượng kế bên tên **Server** là một mũi tên màu xanh hướng lên (thay vì là mũi tên màu đỏ hướng xuống).



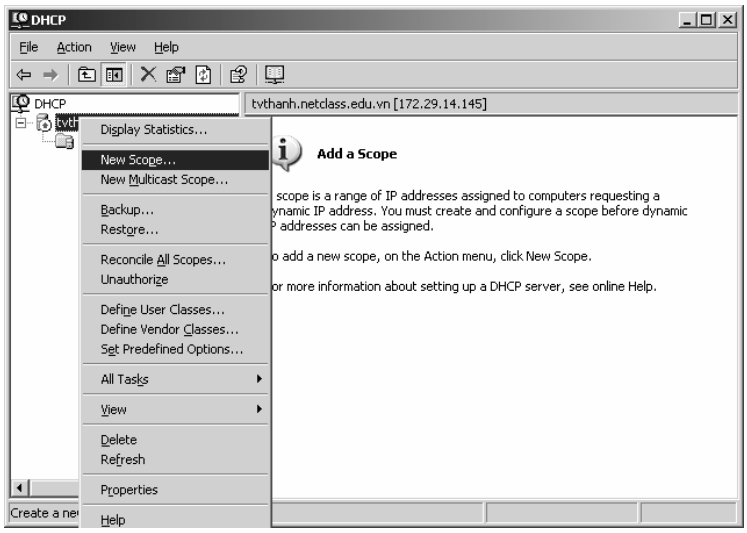
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

# V. CẤU HÌNH DỊCH VỤ DHCP.

Sau khi đã cài đặt dịch vụ **DHCP**, bạn sẽ thấy biểu tượng **DHCP** trong menu **Administrative Tools**. Thực hiện theo các bước sau để tạo một **scope** cấp phát địa chỉ:

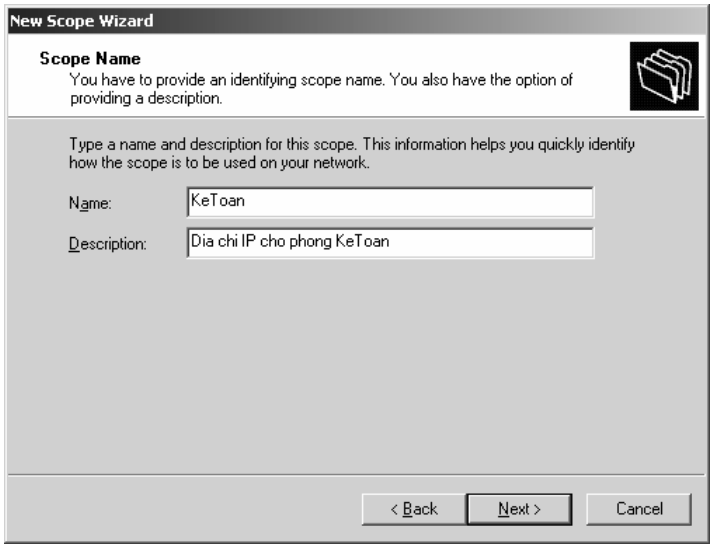
Chọn menu **Start** ⏲ **Programs** ⏲ **Administrative Tools** ⏲ **DHCP**.

Trong cửa sổ **DHCP**, nhấp phải chuột lên biểu tượng **Server** của bạn và chọn mục **New Scope** trong **popup menu**.




Hộp thoại **New Scope Wizard** xuất hiện. Nhấn chọn **Next**.

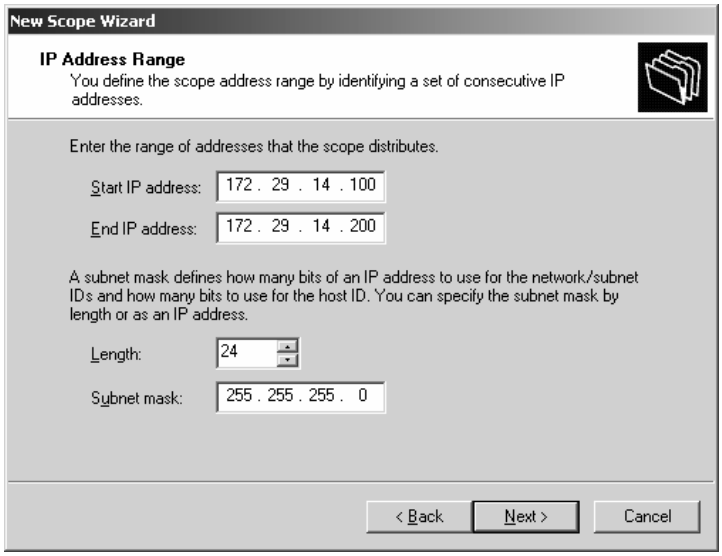
Trong hộp thoại **Scope Name**, bạn nhập vào tên và chú thích, giúp cho việc nhận diện ra **scope** này. Sau đó nhấn chọn **Next**.



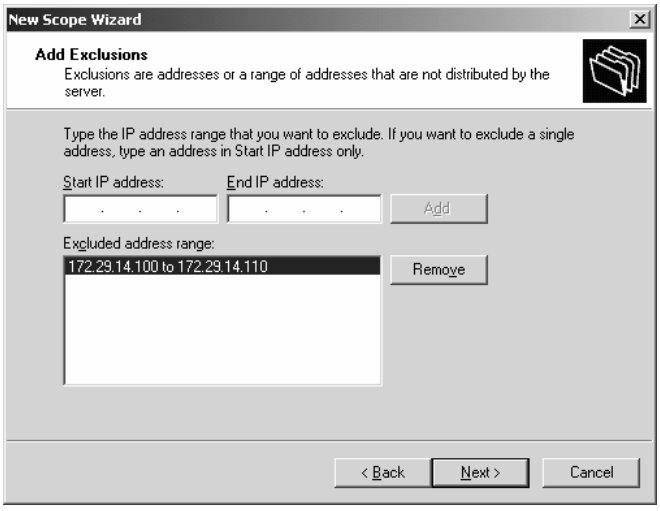

Hộp thoại **IP Address Range** xuất hiện. Bạn nhập vào địa chỉ bắt đầu và kết thúc của danh sách địa chỉ cấp phát. Sau đó bạn chỉ định **subnet mask** bằng cách cho biết số **bit** 1 hoặc hoặc nhập vào chuỗi số. Nhấn chọn **Next**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net



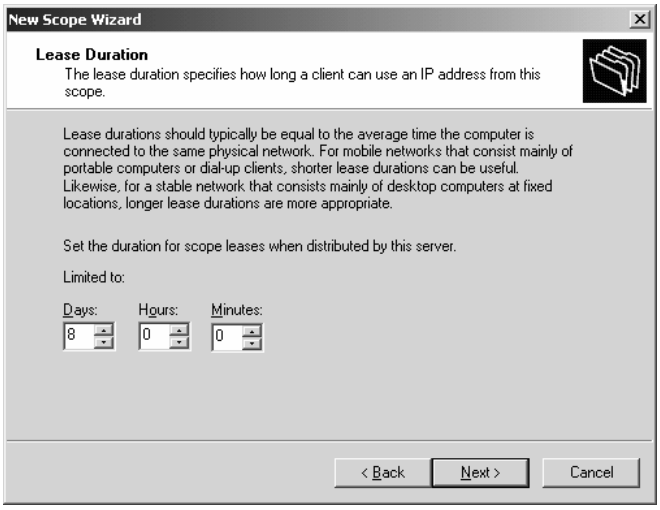

Trong hộp thoại **Add Exclusions**, bạn cho biết những địa chỉ nào sẽ được loại ra khỏi nhóm địa chỉ đã chỉ định ở trên. Các địa chỉ loại ra này được dùng để đặt cho các máy tính dùng địa chỉ tĩnh hoặc dùng để dành cho mục đích nào đó. Để loại một địa chỉ duy nhất, bạn chỉ cần cho biết địa chỉ trong ô **Start IP Address** và nhấn **Add**. Để loại một nhóm các địa chỉ, bạn cho biết địa chỉ bắt đầu và kết thúc của nhóm đó trong **Start IP Address** và **Stop IP Address**, sau đó nhấn **Add**. Nút **Remove** dùng để huỷ một hoặc một nhóm các địa chỉ ra khỏi danh sách trên. Sau khi đã cấu hình xong, bạn nhấn nút **Next** để tiếp tục.



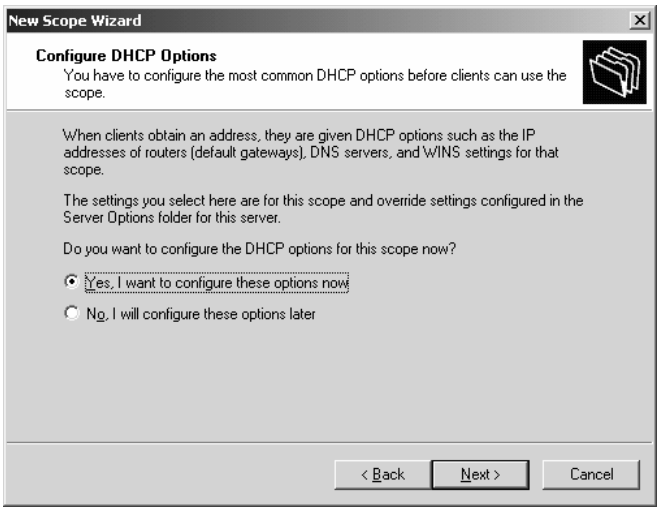

Trong hộp thoại **Lease Duration** tiếp theo, bạn cho biết thời gian các máy trạm có thể sử dụng địa chỉ này. Theo mặc định, một máy **Client** sẽ cố làm mới lại địa chỉ khi đã sử dụng được phân nửa thời gian cho phép. Lượng thời gian cho phép mặc định là 8 ngày. Bạn có thể chỉ định lượng thời gian khác tuỳ theo nhu cầu. Sau khi đã cấu hình xong, nhấn **Next** để tiếp tục.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net



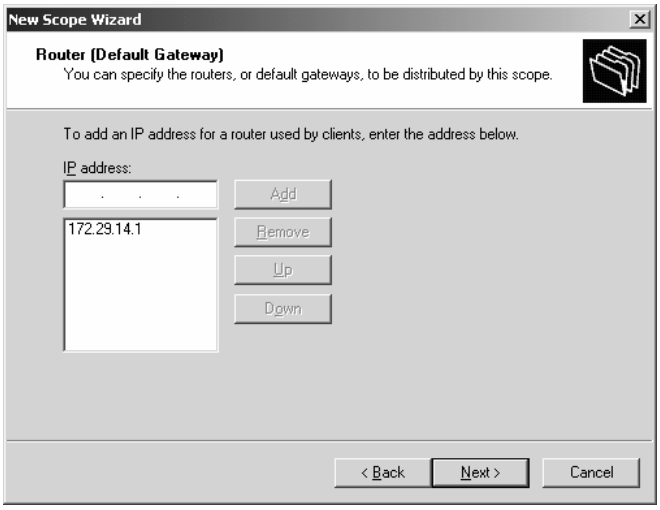

Hộp thoại **Configure DHCP Options** xuất hiện. Bạn có thể đồng ý để cấu hình các tuỳ chọn phổ biến (chọn **Yes, I want to configure these options now**) hoặc không đồng ý, để việc thiết lập này thực hiện sau (chọn **No, I will configure these options later**). Bạn để mục chọn đồng ý và nhấn chọn **Next**.



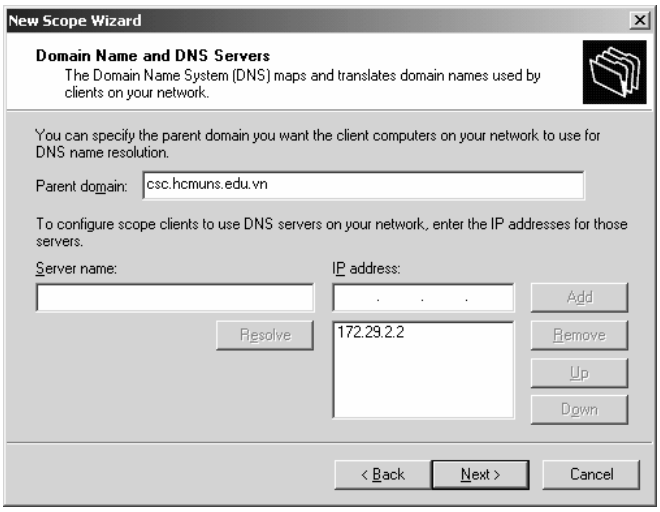

Trong hộp thoại **Router (Default Gateway)**, bạn cho biết địa chỉ **IP** của **default gateway** mà các máy **DHCP Client** sẽ sử dụng và nhấn **Add**. Sau đó nhấn **Next**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Trong hộp thoại **Domain Name and DNS Server**, bạn sẽ cho biết tên **domain** mà các máy **DHCP client** sẽ sử dụng, đồng thời cũng cho biết địa chỉ **IP** của **DNS Server** dùng phân giải tên. Sau khi đã cấu hình xong, nhấn **Next** để tiếp tục.

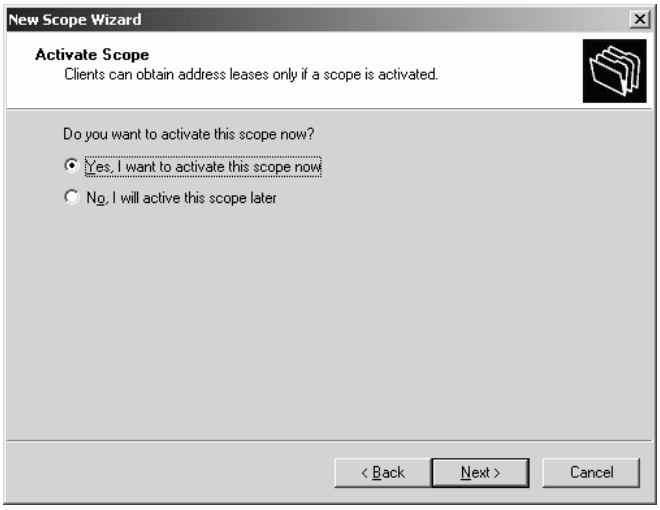



Trong hộp thoại **WINS SERVER** tiếp theo, bạn có thể cho biết địa chỉ của của **WINS Server** chính và phụ dùng phân giải các tên **NetBIOS** thành địa chỉ **IP**. Sau đó nhấn chọn **Next**. (Hiện nay dịch vụ **WINS** ít được sử dụng, do đó bạn có thể bỏ qua bước này, không nhập thông tin gì hết.)

Tiếp theo, hộp thoại **Activate Scope** xuất hiện, hỏi bạn có muốn kích hoạt **scope** này hay không. **Scope** chỉ có thể cấp địa chỉ cho các máy **Client** khi được kích hoạt. Nếu bạn định cấu hình thêm các thông tin tuỳ chọn cho **scope** thì chưa nên kích hoạt bây giờ. Sau khi đã lựa chọn xong, nhấn chọn **Next**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Trong hộp thoại **Complete the New Scope Wizard**, nhấn chọn **Finish** để kết thúc.

# VI. CẤU HÌNH CÁC TUỲ CHỌN DHCP.

Các tuỳ chọn **DHCP** là các thông tin phụ gửi kèm theo địa chỉ **IP** khi cấp phát cho các máy **Client**. Bạn có thể chỉ định các tuỳ chọn ở hai mức độ: **scope** và **Server**. Các tuỳ chọn mức scope chỉ áp dụng cho riêng **scope** đó, còn các tuỳ chọn mức **Server** sẽ áp đặt cho tất cả các **scope** trên toàn **Server**. Tuỳ chọn mức **scope** sẽ che phủ tuỳ chọn mức server cùng loại nếu có.

Các bước thực hiện:

Chọn menu **Start** ⏲ **Programs** ⏲ **Administrative Tools** ⏲ **DHCP**.

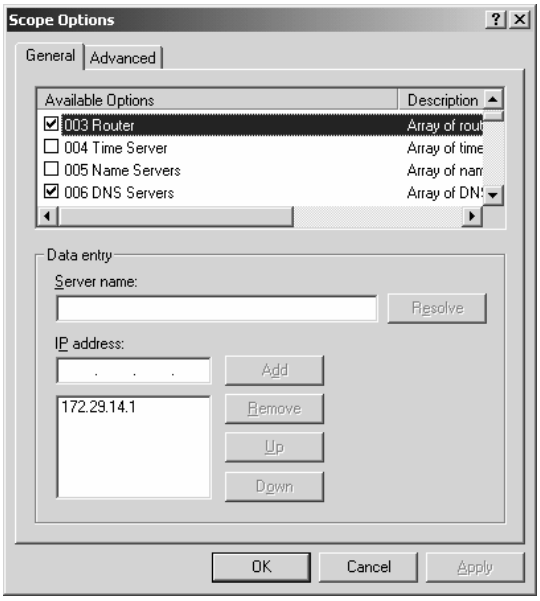
Trong cửa sổ **DHCP,** ở ô bên trái, mở rộng mục **Server** để tìm **Server Options** hoặc mở rộng một **scope** nào đó để tìm **Scope Options**.

Nhấn phải chuột lên mục tuỳ chọn tương ứng và chọn **Configure Options**.

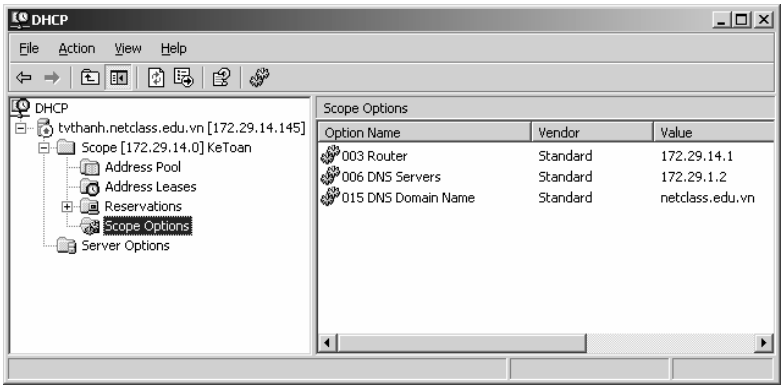
Hộp thoại cấu hình các tuỳ chọn xuất hiện (mức **Server** hoặc **scope** đều giống nhau). Trong mục **Available Options**, chọn loại tuỳ chọn bạn định cấp phát và nhập các thông cấu hình kèm theo. Sau khi đã chọn xong hoặc chỉnh sửa các tuỳ chọn xong, nhấn **OK** để kết thúc.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Trong cửa sổ **DHCP**, mục tuỳ chọn tương ứng sẽ xuất hiện các thông tin định cấp phát.




# VII. CẤU HÌNH DÀNH RIÊNG ĐỊA CHỈ.

Giả sử hệ thống mạng của bạn sử dụng việc cấp phát địa chỉ động, tuy nhiên trong đó có một số máy tính bắt buộc phải sử dụng một địa chỉ **IP** cố định trong một thời gian dài. Bạn có thể thực hiện được điều này bằng cách dành một địa chỉ **IP** cho riêng máy đó. Việc cấu hình này được thực hiện trên từng **scope** riêng biệt.

Các bước thực hiện:

Chọn menu **Start** 🕘 **Programs** 🕘 **Administrative Tools** 🕘 **DHCP**.

Trong ô bên trái của cửa sổ **DHCP**, mở rộng đến **scope** bạn định cấu hình, chọn mục **Reservation**, chọn menu **Action** 🕘 **New Reservation.**

Xuất hiện hộp thoại **New Reservation**. Đặt tên cho mục này dành riêng này trong ô **Reservation Name**, có thể là tên của máy tính được cấp địa chỉ đó. Trong mục **IP Address**, nhập vào địa chỉ **IP** định cấp cho máy đó. Tiếp theo, trong mục **MAC Address**, nhập vào địa chỉ **MAC** của máy tính đó (là một chuỗi liên tục 12 ký số thập lục phân). Bạn có thể ghi một dòng mô tả về địa chỉ vào mục **Description**. **Supported Types** có ý nghĩa:



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

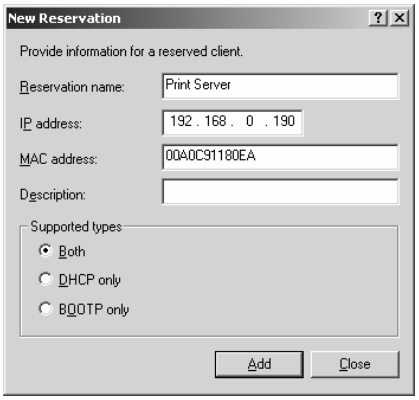
**DHCP only**: chỉ cho phép máy **client DHCP** yêu cầu địa chỉ này bằng cách sử dụng giao thức **DHCP**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

**BOOTP only**: chỉ cho phép máy **client DHCP** yêu cầu địa chỉ này bằng cách sử dụng giao thức **BOOTP** (là tiền thân của giao thức **DHCP**).

**Both**: máy **client DHCP** có thể dùng giao thức **DHCP** hoặc **BOOTP** để yêu cầu địa chỉ này.




Lặp lại thao tác trên cho các địa chỉ dành riêng khác. Cuối cùng nhấn chọn **Close**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

# Tóm tắt

Lý thuyết 2 tiết - Thực hành 2 tiết

| Mục tiêu | Các mục chính | Bài tập bắt buộc | Bài tập làm thêm |
|---|---|---|---|
| Kết thúc bài học này cung cấp học viên kiến thức về dịch vụ in ấn trên mạng như cài đặt máy in mạng, quản lý, cấp quyền sử dụng máy in mạng … | I. Cài đặt máy in mạng.<br>II. Quản lý thuộc tính máy in.<br>III. Cấu hình thông số port.<br>IV. Cấp quyền trên máy in mạng<br>V. Cấu hình Print Server | Dựa vào bài tập môn Quản trị Windows Server 2003. | Dựa vào bài tập môn Quản trị Windows Server 2003. |



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

# I. CÀI ĐẶT MÁY IN.

Trước khi bạn có thể truy xuất vào thiết bị máy in vật lý thông qua hệ điều hành **Windows Server 2003** thì bạn phải tạo ra một máy in **logic**. Nếu máy in của bạn có tính năng **Plug and Play** thì máy in đó sẽ được nhận diện ra ngay khi nó được gắn vào máy tính dùng hệ điều hành **Windows Server 2003**. Tiện ích **Found New Hardware Wizard** sẽ tự động bật lên. Tiện ích này sẽ hướng dẫn cho bạn từng bước để cài đặt máy in. Nếu hệ điều hành nhận diện không chính xác thì bạn dùng đĩa **CD** được hãng sản xuất cung cấp kèm theo máy để cài đặt.

Ngoài ra, bạn cũng có thể tự mình thực hiện tạo ra một máy in **logic** bằng cách sử dụng tiện ích **Add Printer Wizard**. Để có thể tạo ra một máy in **logic** trong **Windows Server 2003** thì trước hết bạn phải đăng nhập vào hệ thống với vai trò là một thành viên của nhóm **Administrators** hay nhóm **Power Users** (trong trường hợp đây là một **Server** thành viên) hay nhóm **Server Operators** (trong trường hợp đây là một **domain controller**).

Bạn có thể tạo ra một máy in logic cục bộ tương ứng với một máy in vật lý được gắn trực tiếp vào máy tính cục bộ của mình hoặc tương ứng với một máy in mạng (máy in mạng được gắn vào một máy tính khác trong mạng hay một thiết bị **Print Server**). Muốn thao tác bằng tay để tạo ra một máy in cục bộ hay một máy in mạng, chúng ta lần lượt thực hiện các thao tác sau đây:

Nhấp chuột chọn **Start**, rồi chọn **Printers And Faxes**.

Nhấp chuột vào biểu tượng **Add Printer**, tiện ích **Add Printer Wizard** sẽ được khởi động. Nhấp chuột vào nút **Next** để tiếp tục.

Hộp thoại **Local Or Network Printer** xuất hiện. Bạn nhấp vào tùy chọn **Local Printer Attached To This Computer** trong trường hợp bạn có một máy in vật lý gắn trực tiếp vào máy tính của mình. Nếu trường hợp ta đang tạo ra một máy in **logic** ứng với một máy in mạng thì ta nhấp vào tùy chọn **A Printer Attached To Another Computer**. Nếu máy in được gắn trực tiếp vào máy tính, bạn có thể chọn thêm tính năng **Automatically Detect And Install My Plug And Play Printer**. Tùy chọn này cho phép hệ thống tự động quét máy tính của bạn để phát hiện ra các máy in **Plug and Play**, và tự động cài đặt các máy in đó cho bạn. Khi đã hoàn tất việc chọn lựa, nhấp chuột vào nút **Next** để sang bước kế tiếp.

Nếu máy in vật lý đã được tự động nhận diện bằng tiện ích **Found New Hardware Wizard**. Tiện ích này sẽ hướng dẫn bạn tiếp tục cài đặt **driver** máy in qua từng bước.

Hộp thoại **Print Test Page** xuất hiện. Nếu thiết bị máy in được gắn trực tiếp vào máy tính của bạn, bạn nên in thử một trang kiểm tra để xác nhận rằng mọi thứ đều được cấu hình chính xác. Ngược lại, nếu máy in là máy in mạng thì bạn nên bỏ qua bước này. Nhấp chuột vào nút **Next** để sang bước kế tiếp.

Hộp thoại **Completing The Add Printer Wizard** hiện ra. Hộp thoại này đem đến cho chúng ta một cơ hội để xác nhận rằng tất cả các thuộc tính máy in đã được xác lập chính xác. Nếu bạn phát hiện có thông tin nào không chính xác, hãy nhấp chuột vào nút **Back** để quay lại sửa chữa thông tin cho đúng. Còn nếu nhận thấy mọi thứ đều ổn cả thì bạn nhấp chuột vào nút **Finish**.

Một biểu tượng máy in mới sẽ hiện ra trong cửa sổ **Printer And Faxes**. Theo mặc định, máy in sẽ được chia sẻ.

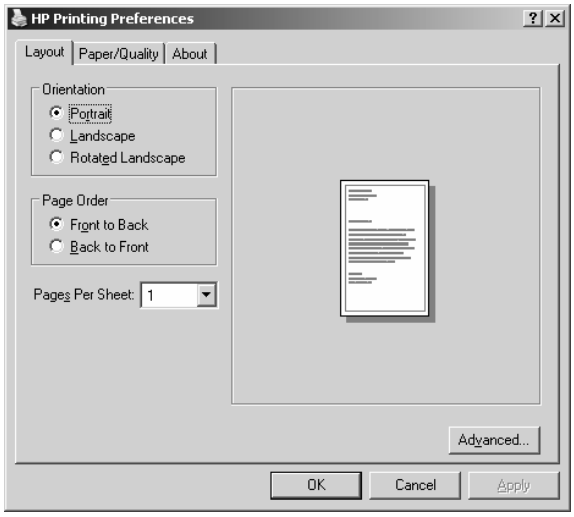


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

# II. QUẢN LÝ THUỘC TÍNH MÁY IN.

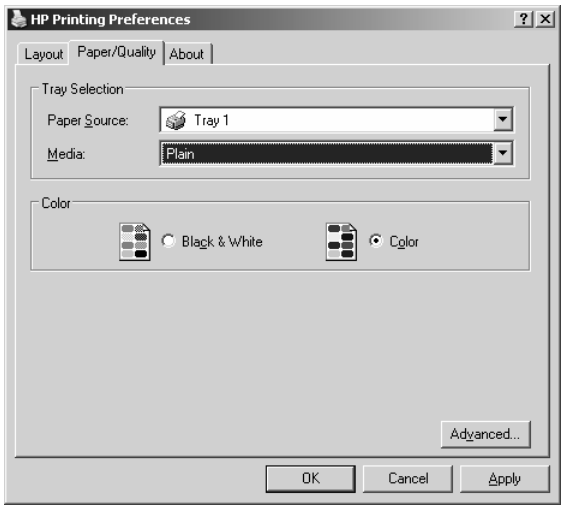
## II.1. Cấu hình Layout.

Trong hộp thoại **Printing Preferences**, chọn **Tab Layout**. Sau đó trong mục **Orientation**, bạn chọn cách thức in trang theo chiều ngang hay chiều dọc. Trong mục **Page Order**, bạn chọn in từ trang đầu đến trang cuối của tài liệu hoặc in theo thứ tự ngược lại. Trong mục **Pages Per Sheet**, bạn chọn số trang tài liệu sẽ được in trên một trang giấy.




## II.2. Giấy và chất lượng in.

Cũng trong hộp thoại **Printing Preferences,** để qui định giấy và chất lượng in, chúng ta chọn **Tab Paper/Quality**. Các tùy chọn trong **Tab Paper/Quality** phụ thuộc vào đặc tính của máy in. Ví dụ, máy in chỉ có thể cung cấp một tùy chọn là **Paper Source.** Còn đối với máy in **HP OfficeJet Pro Cxi,** chúng ta có các tùy chọn là: **Paper Source**, **Media, Quality Settings** và **Color**.

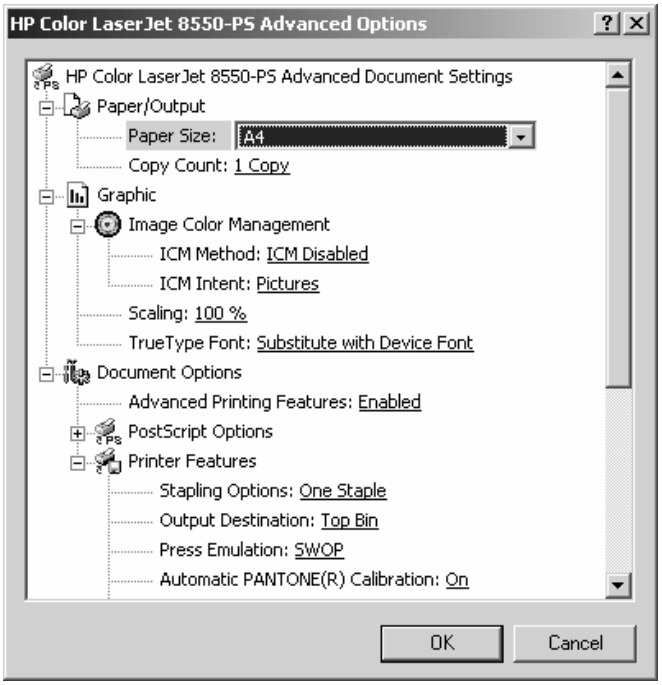





Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

## II.3. Các thông số mở rộng.

Nhấp chuột vào nút **Advanced** ở góc dưới bên phải của hộp thoại **Printing Preferences**. Hộp thoại **Advanced Options** xuất hiện cho phép bạn điều chỉnh các thông số mở rộng. Chúng ta có thể có các tùy chọn của máy in như: **Paper/Output, Graphic, Document Options, và Printer Features**. Các thông số mở rộng có trong hộp thoại **Advanced Options** phụ thuộc vào driver máy in mà bạn đang sử dụng.

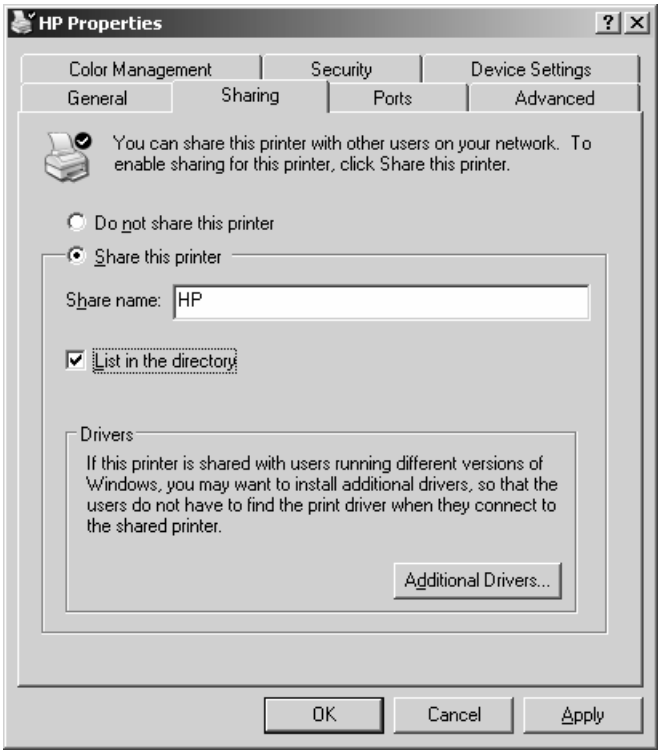



# III. CẤU HÌNH CHIA SẺ MÁY IN.

Nhấp phải chuột lên máy in, chọn **Properties.** Hộp thoại **Properties** xuất hiện, bạn chọn **Tab Sharing**. Để chia sẻ máy in này cho nhiều người dùng, bạn nhấp chuột chọn **Share this printer**. Trong mục **Share name**, bạn nhập vào tên chia sẻ của máy in, tên này sẽ được nhìn thấy trên mạng. Bạn cũng có thể nhấp chọn mục **List In** The **Directory** để cho phép người dùng có thể tìm kiếm máy in thông qua **Active Directory** theo một vài thuộc tính đặc trưng nào đó.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

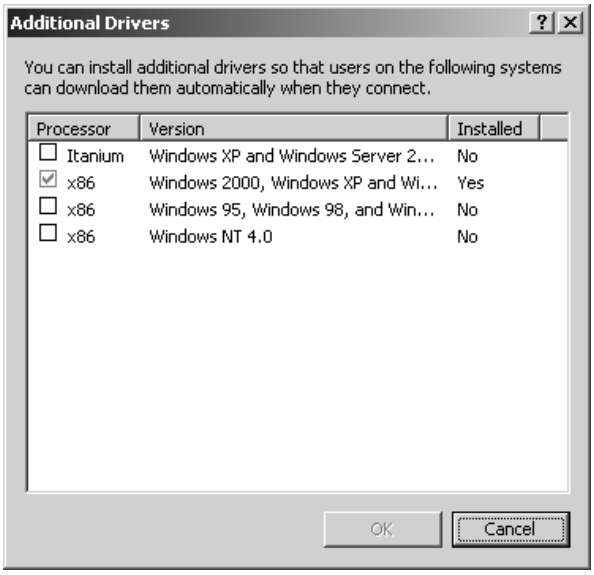



Ngoài ra, trong **Tab Sharing**, ta có thể cấu hình **driver** hỗ trợ cho các máy trạm sử dụng máy in trong trường hợp máy trạm không phải là **Windows Server 2003**. Đây là một tính năng cần thiết vì nó cho phép chỉ định các **driver** hỗ trợ in để các máy trạm có thể tải về một cách tự động. Mặc định, **driver** duy nhất được nạp vào là **driver** của hãng **Intel** cho các máy trạm là **Windows 2000, Windows Server 2003**, và **Windows XP**. Để cung cấp thêm các **driver** cho máy trạm khác, bạn nhấp chuột vào nút **Additional Drivers** nằm phía dưới **Tab Sharing**. Hộp thoại **Additional Drivers** xuất hiện. **Windows Server 2003** hỗ trợ các **driver** thêm vào cho các **Client** là một trong những hệ điều hành sau:

- Itanium Windows XP hay Windows Server 2003.
- x86 Windows 2000, Windows XP, hay Windows Server 2003 (mặc định).
- x86 Windows 95, Windows 98, hay Windows Millennium Edition.
- x86 Windows NT 4.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




# IV. CẤU HÌNH THÔNG SỐ PORT.

## IV.1. Cấu hình các thông số trong Tab Port.

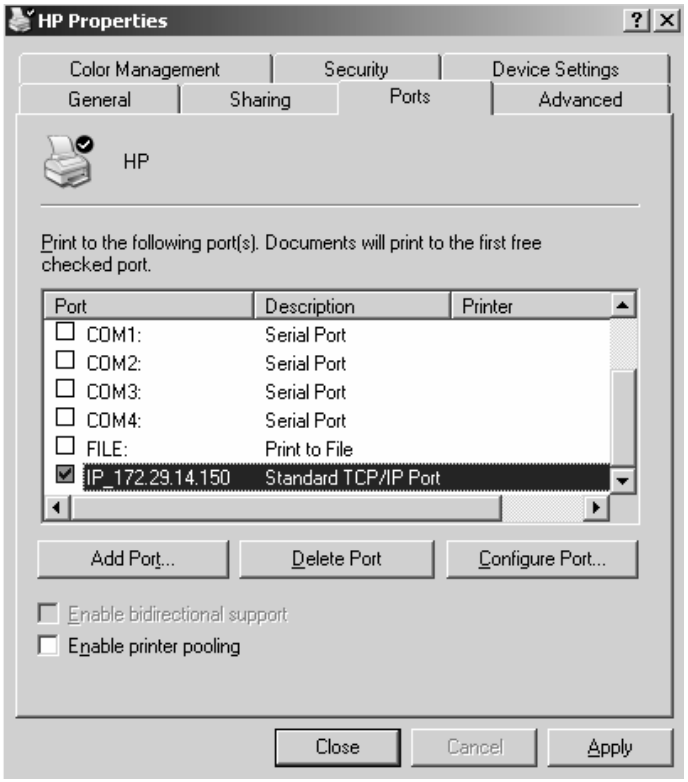
Trong hộp thoại **Properties**, bạn chọn **Tab Port** để cấu hình tất cả các **port** đã được định nghĩa cho máy in sử dụng. Một **port** được định nghĩa như một **interface** sẽ cho phép máy tính giao tiếp với thiết bị máy in. **Windows Server 2003** hỗ trợ các port vật lý (**local port**) và các **port TCP/IP** chuẩn (**port logic**).

**Port** vật lý chỉ được sử dụng khi ta gắn trực tiếp máy in vào máy tính. Trong trường hợp **Windows Server 2003** đang được triển khai trong một nhóm làm việc nhỏ, hầu như bạn phải gắn máy in vào **port LPT1**.

**Port TCP/IP** chuẩn được sử dụng khi máy in có thể kết nối trực tiếp vào mạng (trên máy in có hỗ trợ **port RJ45)** và máy in này có một địa chỉ **IP** để nhận dạng. Ưu điểm của máy in mạng là tốc độ in nhanh hơn máy in cục bộ và máy in có thể đặt bất kì nơi nào trong hệ thống mạng. Khi đó bạn cần chỉ định một port **TCP/IP** và khai báo địa chỉ **IP** của máy in mạng. Cùng với việc xoá và cấu hình lại một **port** đã tồn tại, bạn cũng có thể thiết lập **printer pooling** và điều hướng các công việc in ấn đến một máy in khác.

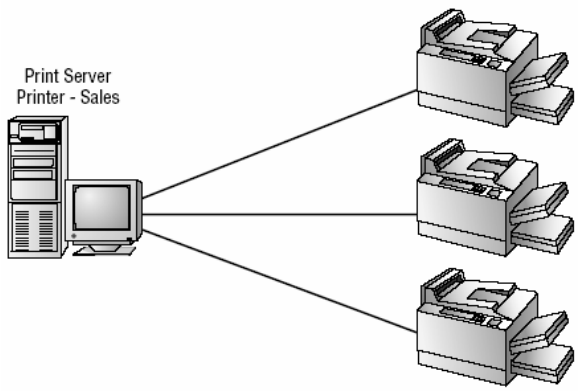


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




## IV.2. Printer Pooling.

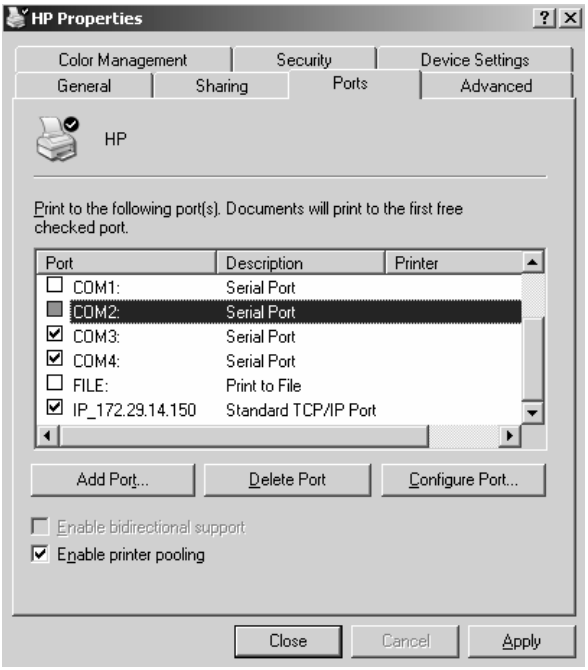
**Printer pool** được sử dụng nhằm phối hợp nhiều máy in vật lý với một máy in **logic**, được minh họa như hình bên dưới. Lợi ích của việc sử dụng **printer pool** là máy in rảnh đầu tiên sẽ thực hiện thao tác in ấn cho bạn. Tính năng này rất hữu dụng trong trường hợp ta có một nhóm các máy in vật lý được chia sẻ cho một nhóm người dùng, ví dụ như là nhóm các thư ký.




Để cấu hình một **printer pool**, bạn nhấp chuột vào tùy chọn **Enable Printer Pooling** nằm ở phía dưới **Tab Port** trong hộp thoại **Properties**. Sau đó, kiểm tra lại tất cả các **port** mà ta dự định gắn các máy in vật lý trong **printer pool** vào. Nếu ta không chọn tùy chọn **Enable Printer Pooling** thì ta chỉ có một port duy nhất cho mỗi máy in. Chú ý tất cả các máy in vật lý trong một **printer pool** phải sử dụng cùng một **driver** máy in.

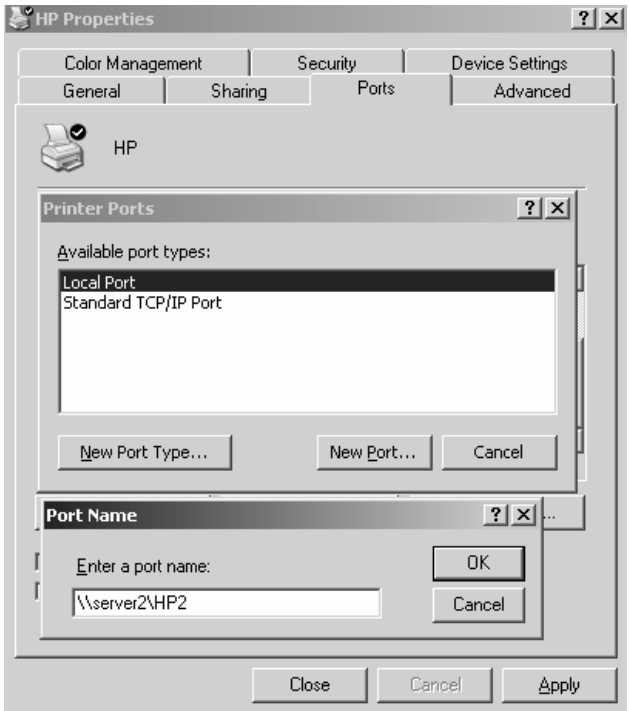


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




## IV.3. Điều hướng tác vụ in đến một máy in khác.

Nếu một máy in vật lý của bạn bị hư, bạn có thể chuyển tất cả các tác vụ in ấn của máy in bị hư sang một máy in khác. Để làm được điều này, trước hết bạn phải đảm bảo máy in mới phải có **driver** giống với máy in cũ. Sau đó, trong **Tab Port**, bạn nhấp chuột vào nút **Add Port**, chọn **Local port** rồi chọn tiếp **New Port**. Hộp thoại **Port Name** xuất hiện, gõ vào tên **UNC** của máy in mới theo định dạng: **\\computername\printer_sharename.**





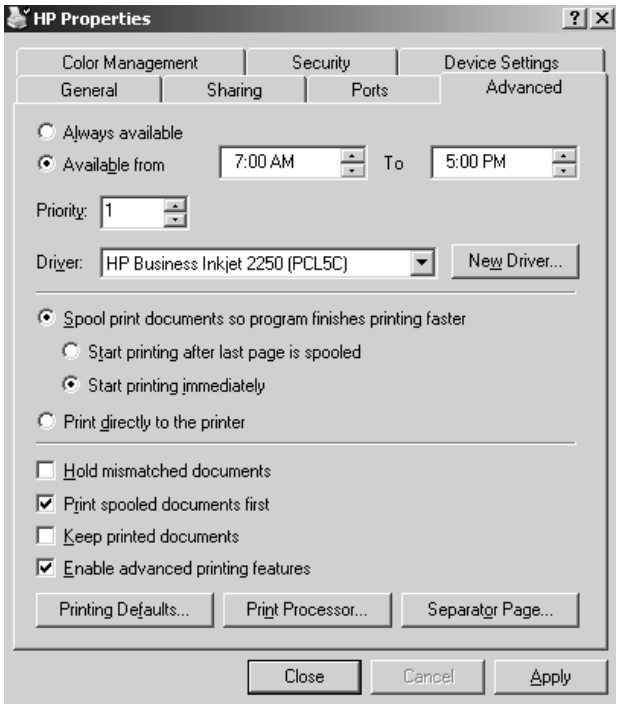

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

# V. CẤU HÌNH TAB ADVANCED.

## V.1. Các thông số của Tab Advanced.

Trong hộp thoại **Properties**, bạn nhấp chuột vào **Tab Advanced** để điều khiển các đặc tính của máy in. Bạn có thể cấu hình các thuộc tính sau:

- Khả năng của máy in
- Độ ưu tiên của máy in
- Driver mà máy in sẽ sử dụng
- Các thuộc tính đồng tác (**spooling**) của máy in
- Cách thức in tài liệu theo biểu mẫu
- Chế độ in mặc định
- Sử dụng bộ xử lý in ấn nào
- Các trang độc lập




## V.2. Khả năng sẵn sàng phục vụ của máy in.

Thông thường, chúng ta cần kiểm tra khả năng sẵn sàng phục vụ của máy in trong trường hợp chúng ta có nhiều máy in cùng sử dụng một thiết bị in. Mặc định thì tùy chọn **Always Available** luôn được bật lên. Do đó, người dùng có thể sử dụng máy in 24 tiếng một ngày. Để giới hạn khả năng phục vụ của máy in, bạn chọn **Available From** và chỉ định khoảng thời gian mà máy in sẽ phục vụ. Ngoài khoảng thời gian này, máy in sẽ không phục vụ cho bất kì người dùng nào.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

## V.3. Độ ưu tiên (Printer Priority).

Khi bạn đặt độ ưu tiên, bạn sẽ định ra bao nhiêu công việc sẽ được gửi trực tiếp vào thiết bị in. Ví dụ, bạn có thể sử dụng tùy chọn này khi 2 nhóm người dùng cùng chia sẻ một máy in và bạn cần điều khiển độ ưu tiên đối với các thao tác in ấn trên thiết bị in này. Trong **Tab Advanced** của hộp thoại **Properties**, bạn sẽ đặt độ ưu tiên bằng các giá trị từ 1 đến 99, với 1 là có độ ưu tiên thấp nhất và 99 là có độ ưu tiên cao nhất.

Ví dụ: giả sử có một máy in được phòng kế toán sử dụng. Những người quản lý trong phòng kế toán luôn luôn muốn tài liệu của họ sẽ được ưu tiên in ra trước các nhân viên khác. Để cấu hình cho việc sắp xếp thứ tự này, ta tạo ra một máy in tên là **MANAGERS** gắn vào **port LPT1** với độ ưu tiên là 99. Sau đó, cũng trên port **LPT1**, ta tạo thêm một máy in nữa tên là **WORKERS** với độ ưu tiên là 1. Sau đó, ta sẽ sử dụng **Tab Security** trong hộp thoại **Properties** để giới hạn quyền sử dụng máy in **MANAGERS** cho những người quản lý. Đối với các nhân viên còn lại trong phòng kế toán, ta cho phép họ sử dụng máy in **WORKERS** (chúng ta sẽ tìm hiểu rõ hơn về **Security** trong phần sau). Khi các tác vụ in xuất phát từ máy in **MANAGERS**, nó sẽ đi vào hàng đợi của của máy in vật lý với độ ưu tiên cao hơn là các tác vụ xuất phát từ máy in **WORKERS**. Do đó, tài liệu của những người quản lý sẽ được ưu tiên in trước.

## V.4. Print Driver.

Mục **Drive**r trong **Tab Advanced** cho phép bạn chỉ định driver sẽ dùng cho máy in. Nếu bạn đã cấu hình nhiều máy in trên một máy tính thì bạn có thể chọn bất kì **driver** nào trong các **driver** đã cài đặt. Thao tác thực hiện như sau: Nhấp chuột vào nút **New Driver** để khởi động **Add Printer Driver Wizard**. **Add Printer Driver Wizard** cho phép bạn thực hiện cập nhật cũng như thêm driver mới.

## V.5. Spooling.

Khi bạn cấu hình tùy chọn **spooling**, bạn cần chỉ định rõ các tác vụ in ấn sẽ được đẩy ra đường ống máy in hay được gửi trực tiếp đến thiết bị máy in. **Spooling** có nghĩa là các thao tác in ấn sẽ được lưu trữ xuống đĩa thành một hàng đợi trước khi các thao tác in này được gửi đến máy in. Có thể xem **spooling** giống như là bộ điều phối in ấn nếu như tại một thời điểm có nhiều người dùng cùng lúc gởi yêu cầu đến máy in. Theo chế độ mặc định, tùy chọn **spooling** sẽ được bật lên sẵn.

## V.6. Print Options.

Phía dưới **Tab Advance** có chứa bốn tùy chọn in ấn. Đó là các tùy chọn:

- **Hold Mismatched Documents**: tùy chọn này hữu dụng trong trường hợp bạn sử dụng chế độ nhiều biểu mẫu trong một máy in. Mặc định thì tùy chọn này sẽ không được bật lên. Các tác vụ sẽ được in theo chế độ **first-in-first-out (FIFO).** Nếu bạn bật tùy chọn này lên, hệ thống sẽ chọn ưu tiên in trước những tác vụ có chung một biểu mẫu.
- **Print Spooled Documents First**: tùy chọn này qui định rằng các tác vụ in ấn được điều hướng xong trước các loại tác vụ lớn khác. Điều này có nghĩa là các tác vụ in ấn sẽ có độ ưu tiên lớn hơn các loại tác vụ khác trong quá trình điều hướng. Mặc định thì tùy chọn này luôn được bật lên giúp gia tăng hiệu quả làm việc của máy in.
- **Keep Printed Documents**: tùy chọn này qui định rằng các tác vụ in ấn phải được xóa khỏi hàng đợi điều hướng in ấn khi các tác vụ này đã hoàn tất quá trình in. Thông thường, bạn muốn xóa các



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

tác vụ in ấn ngay khi nó bắt đầu in bởi vì nếu chúng ta tiếp tục lưu trữ các tác vụ này trong hàng



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

đợi điều hướng và đợi cho đến khi chúng được in xong mới xóa thì sẽ phải tốn dung lượng ổ đĩa cho việc lưu trữ. Mặc định thì tùy chọn này sẽ không được bật lên.

- **Enable Advanced Printing Features**: tùy chọn này qui định rằng bất kì các tính năng mở rộng nào mà máy in của bạn có hỗ trợ ví dụ như **Page Order** và **Pages Per Sheet** nên được bật lên. Mặc định thì tùy chọn này luôn được bật lên. Chỉ trong trường hợp xảy ra các vấn đề về tương thích thì bạn có thể tắt tùy chọn này. Ví dụ như bạn đang sử dụng **driver** cho một thiết bị máy in tương tự nhưng nó không hỗ trợ tất cả các tính năng của máy in. Trong trường hợp đó, bạn nên tắt tùy chọn này đi.

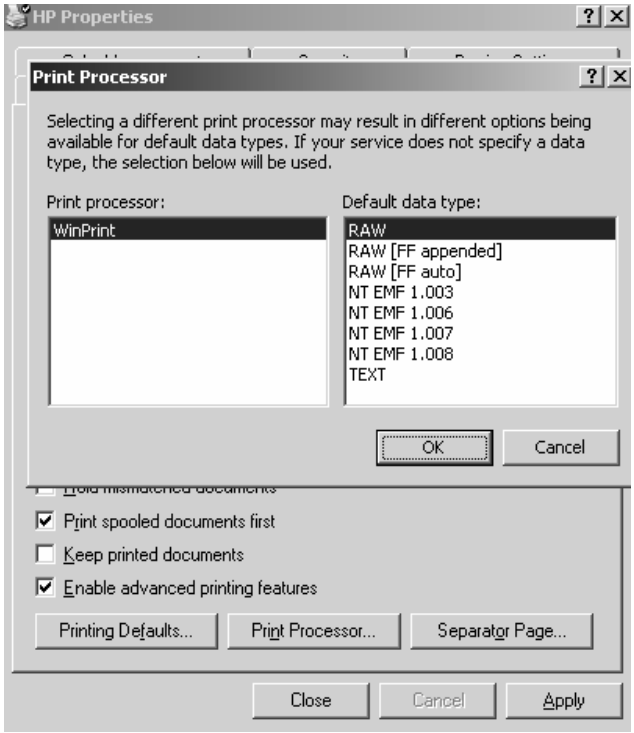
## V.7. Printing Defaults.

Nút **Printing Defaults** nằm ở góc trái phía dưới của **Tab Advance**. Nếu bạn nhấp chuột vào nút **Printing Defaults**, hộp thoại **The Printing Preferences** sẽ xuất hiện. Đây cũng chính là hộp thoại sẽ xuất hiện khi bạn nhấp chuột vào nút **Printing Preferences** trong **Tab General**.

## V.8. Print Processor.

Bộ xử lý in ấn được sử dụng để qui định **Windows Server 2003** có cần phải thực hiện các xử lý bổ sung trong công việc in ấn hay không. Bộ xử lý in ấn **WinPrint** mặc định được cài đặt và được **Windows Server 2003** sử dụng. Bộ xử lý in ấn **WinPrint** có thể hỗ trợ một vài kiểu dữ liệu.

Theo mặc định thì hầu hết các ứng dụng trên nền **Window** sử dụng chuẩn **EMF (enhanced metafile)** để gởi các tác vụ đến máy in. Chuẩn **EMF** dùng kiểu dữ liệu **RAW**. Kiểu dữ liệu này sẽ báo với bộ xử lý in ấn là tác vụ này không cần phải sửa đổi độ ưu tiên khi in. Điều này là do nhà sản xuất phần mềm qui định.






Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

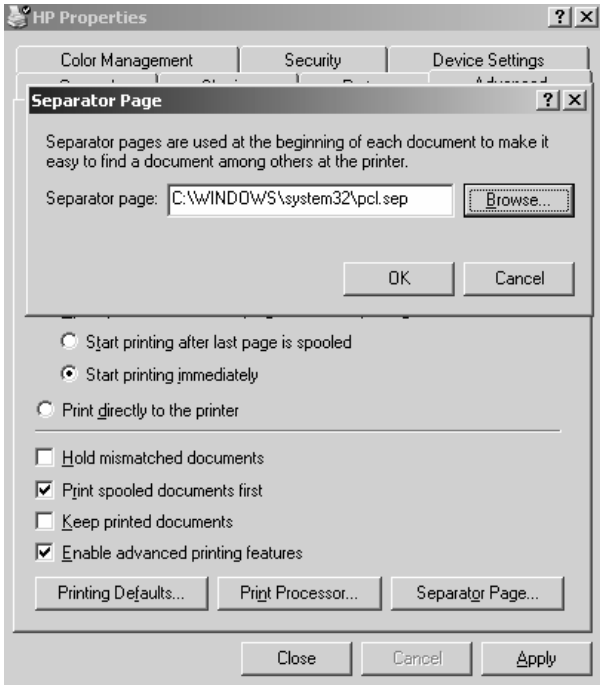
Bảng danh sách các kiểu dữ liệu được bộ xử lý in ấn trong **Windows Server 2003** hỗ trợ:

| Kiểu dữ liệu | Mô tả |
|---|---|
| RAW | Không làm thay đổi tài liệu in ấn |
| RAW (FF appended) | Không làm thay đổi tài liệu in ấn ngoại trừ việc thêm vào một kí tự **form-feed** |
| RAW (FF Auto) | Không làm thay đổi tài liệu in ấn ngoại trừ việc kiểm tra xem có cần thêm vào một kí tự **form-feed** hay không |
| NT EMF 1.00x | Thường điều hướng các tài liệu được gửi từ các máy tính **Window** khác |
| TEXT | Phiên dịch tất cả các kiểu dữ liệu văn bản đơn giản và máy in sẽ thực hiện in bằng cách sử dụng các lệnh văn bản chuẩn. |

## V.9. Separator Pages.

**Separator pages** được sử dụng tại thời điểm bắt đầu của mỗi tài liệu nhằm mục đích định dạng rõ người dùng nào đã thực hiện việc in tài liệu này. Nếu như máy in không được chia sẻ thì chế độ **Separator pages** vô hình chung sẽ gây ra lãng phí giấy in. Nếu trong trường hợp máy in được chia sẻ cho nhiều người dùng thì chế độ **Separator pages** sẽ hữu dụng trong việc phân phối các tác vụ in ấn đã hoàn tất.

Để thêm một **Separator page**, bạn thực hiện như sau: nhấp chuột vào nút **Separator page** nằm ở góc phải phía **dưới Tab Advance**. Hộp thoại **Separator page** hiện ra, bạn nhấp chuột vào nút **Browse** để chọn tập tin **Separator page** nào bạn muốn sử dụng.



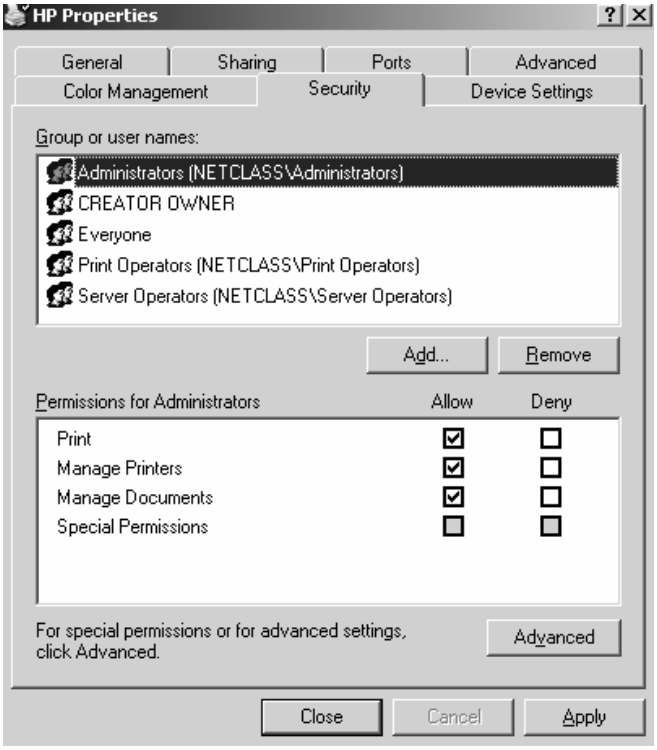



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

# VI. CẤU HÌNH TAB SECURITY.

## VI.1. Giới thiệu Tab Security.

Chúng ta có thể kiểm soát quyền truy cập vào máy in **Windows Server 2003** của người dùng cũng như các nhóm người dùng bằng cách cấu hình quyền in ấn. Chúng ta có thể cho phép hoặc không cho phép người dùng truy xuất máy in. Chúng ta cấp quyền in ấn cho người dùng và nhóm người dùng thông qua **Tab Security** trong hộp thoại **Properties** của máy in.




Bảng phân quyền in ấn cho người dùng

| Quyền hạn | Mô tả |
|---|---|
| Print | Cho phép người dùng hoặc một nhóm người dùng có thể kết nối và gửi tác vụ in ấn đến máy in. |
| Manage Printers | Cho phép thực hiện thao tác điều khiển, quản lý máy in. Với quyền này, người dùng hoặc nhóm người dùng có thể dừng hoặc khởi động lại máy in, thay đổi cấu hình của bộ điều tác, chia sẻ hoặc không chia sẻ máy in, thay đổi quyền in ấn, và quản trị các thuộc tính của máy in. |
| Manage Documents | Cho phép người dùng quản lý các tài liệu in qua các thao tác dừng việc in, khởi động lại, phục hồi lại, hoặc là xoá tài liệu ra khỏi hàng đợi máy in. Người dùng không thể điều khiển trạng thái của máy in. |



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

| | |
|---|---|
| Special Permissions | Bằng cách chọn **Tab Advanced** trong hộp thoại **Print Permissions**, bạn có thể quản lý các quyền đặc biệt. |



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

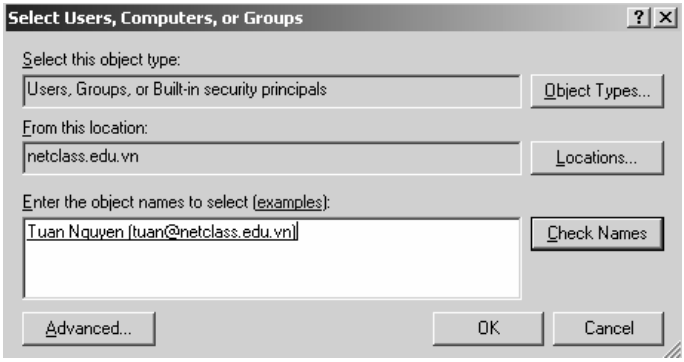
Theo mặc định, bất kì khi nào một máy in được tạo ra, các quyền in ấn mặc định sẽ được thiết lập. Bảng các quyền in ấn mặc định:

| Nhóm quyền | Được phép in | Quản lý máy in | Quản lý tài liệu in |
|---|---|---|---|
| Administrators | ✓ | ✓ | ✓ |
| Creator Owner | | | ✓ |
| Everyone | ✓ | | |
| Print Operators | ✓ | ✓ | ✓ |
| Server Operators | ✓ | ✓ | ✓ |

## VI.2. Cấp quyền in cho người dùng/nhóm người dùng.

Thông thường, bạn có thể chấp nhận quyền in ấn mặc định đã được thiết lập sẵn. Tuy nhiên, trong một số trường hợp đặc biệt, bạn cần phải hiệu chỉnh lại các quyền in cho thích hợp. Ví dụ: Công ty của bạn vừa trang bị cho phòng **Marketing** một máy in **laser** màu đắt tiền, bạn không muốn ai cũng được phép sử dụng máy in này. Trong trường hợp này, trước tiên bạn phải bỏ tùy chọn **Allow checkbox for the Everyone group**. Sau đó, thêm nhóm **Marketing** vào trong danh sách của **Tab Security**. Cuối cùng bạn cấp cho nhóm **Marketing** quyền **Print**. Muốn thêm các quyền in ấn, bạn thực hiện các bước sau:

1. Ở **Tab Security** trong hộp thoại **Properties** của máy in, nhấp chuột vào nút **Add.**
2. Hộp thoại **Select Users**, **Computers**, **Or Groups** xuất hiện, bạn nhập vào tên của người dùng hoặc nhóm người dùng mà bạn định cấp quyền in ấn rồi nhấp chuột vào nút **Add**. Sau đó, bạn chọn tất cả các người dùng mà bạn muốn cấp quyền và nhấp chuột vào nút **OK**




3. Chọn người dùng hoặc nhóm người dùng từ danh sách các phân quyền, sau đó chọn **Allow** để cấp quyền hoặc chọn **Deny** để không cấp quyền in ấn, các quyền quản lý máy in hay các quyền quản lý tài liệu in.

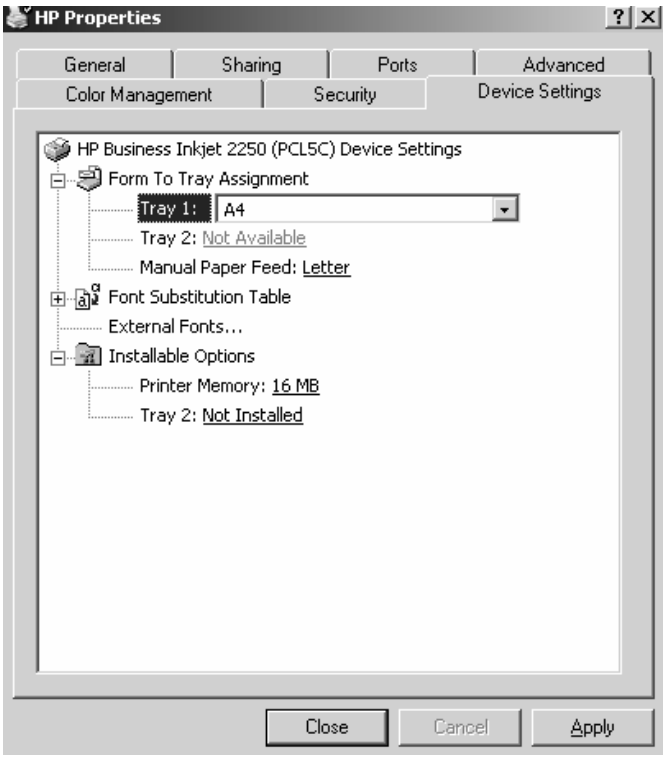
Để loại bỏ một nhóm có sẵn trong danh sách phân quyền, ta sẽ chọn nhóm đó và nhấp chuột vào nút **Remove.** Nhóm vừa chọn sẽ không còn được liệt kê trong **Tab Security** nữa và không thể được cấp bất kì quyền hạn in ấn nào.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

# VII. CẤU HÌNH TAB DEVICES.

Trong hộp thoại **Properties**, chọn mở **Tab Devices**. Các thuộc tính hiển thị trong **Tab Devices** phụ thuộc vào đặc tính của máy in và **driver** máy in mà bạn đã cài đặt.




# VIII. QUẢN LÝ PRINT SERVER.

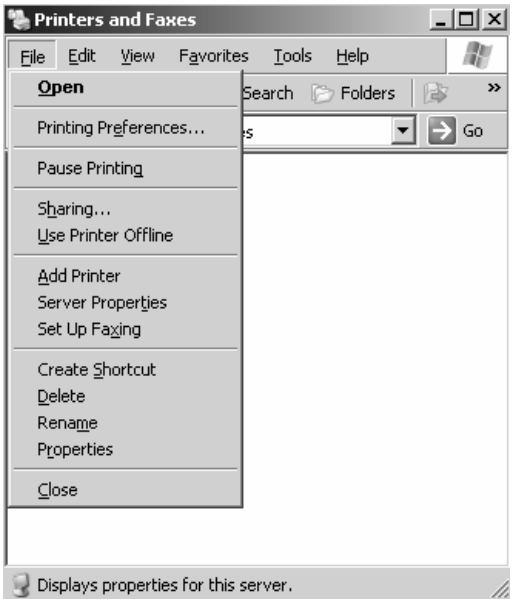
## VIII.1. Hộp thoại quản lý Print Server.

**Print Server** là một một máy tính trên đó có định nghĩa sẵn các máy in. Khi người dùng gửi một yêu cầu in ấn đến một máy in mạng, thì trước tiên, yêu cầu đó phải được gửi đến **Print Server**. Nói cách khác **Print Server** sẽ có nhiệm vụ quản lý tất cả các máy in **logic** đã được tạo ra trên máy tính. Với tư cách là một **Print Server**, máy tính này phải đủ mạnh để hỗ trợ cho việc đón nhận các tác vụ in ấn và nó cũng phải đủ không gian đĩa trống để chứa các tác vụ in trong hàng đợi.

Bạn có thể quản lý **Print Server** bằng cách cấu hình các thuộc tính trong hộp thoại **Print Server Properties**. Chúng ta mở hộp thoại **Print Server Properties** bằng cách: mở hộp thoại **Printers And Faxes**, chọn **File** rồi chọn tiếp **Server Properties**. Hộp thoại **Print Server Properties** bao gồm các **Tab: Forms, Ports, Drivers** và **Advanced.**



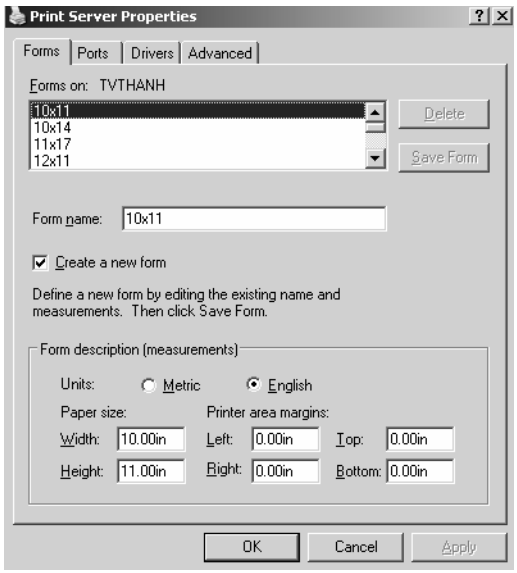
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




## VIII.2. Cấu hình các thuộc tính của biểu mẫu in.

Nếu máy in của bạn có nhiều khay giấy và ở mỗi khay, bạn đặt vào đó các loại giấy khác nhau, bạn có thể cấu hình các thuộc tính trong **Tab Form** để tạo ra và quản lý nhiều biểu mẫu cho máy in. Một biểu mẫu chủ yếu được cấu hình dựa vào kích cỡ. Muốn tạo ra một biểu mẫu mới, ta thực hiện theo bốn bước sau:

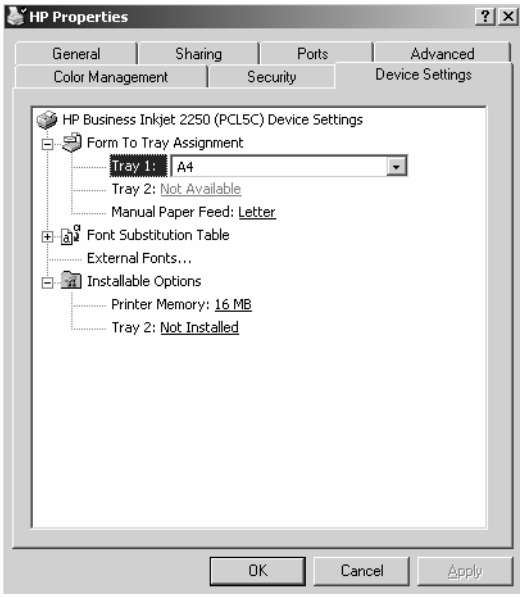
(1) Trong **Tab Forms**, bạn nhấp chuột vào tùy chọn **Create A New Form**.
(2) Trong mục **Form Name**, bạn nhập vào tên của biểu mẫu.
(3) Trong mục **Form Description**, bạn lựa chọn kích thước cho biểu mẫu
(4) Nhấp chuột vào nút **Save Form** để hoàn tất việc tạo biểu mẫu






Chúng ta vừa tạo ra một biểu mẫu. Tiếp theo, chúng ta cần kết hợp biểu mẫu với khay giấy của máy in. Để làm được điều này, chúng ta phải sử dụng **Tab Devices** trong hộp thoại **Properties** của máy in.

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net



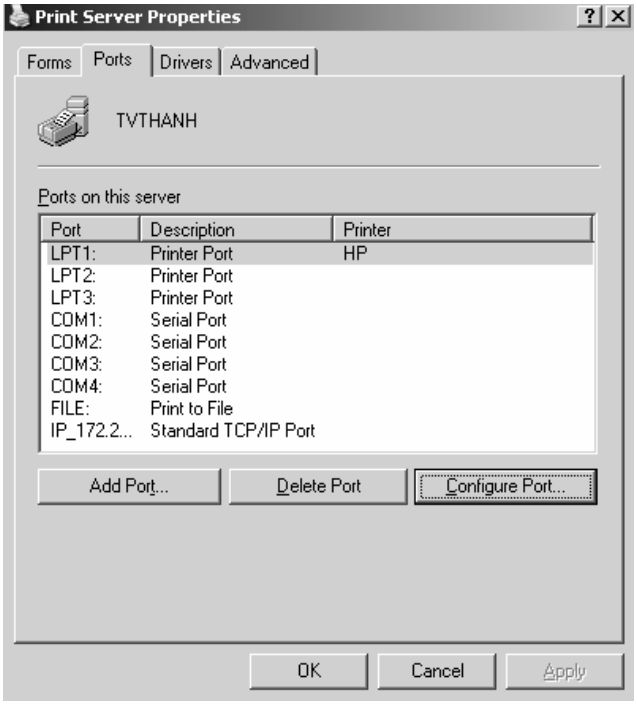

Phía dưới phần **Form To Tray Assignment**, trước tiên bạn chọn khay giấy, rồi chọn biểu mẫu để kết hợp với khay giấy đó.

## VIII.3. Cấu hình các thuộc tính Port của Print Server.

Trong hộp thoại **Printer Server Properties**, bạn mở **Tab Port**. **Tab** này cũng tương tự như **Tab Port** trong hộp thoại **Properties** của máy in. Sự khác nhau giữa hai **Tab Port** là: **Tab Port** trong hộp thoại **Print Server Properties** được sử dụng để quản lý tất cả các port trên **Print Server**. Còn **Tab port** trong hộp thoại **Properties** của máy in quản lý các **port** của thiết bị máy in vật lý.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




## VIII.4. Cấu hình Tab Driver.

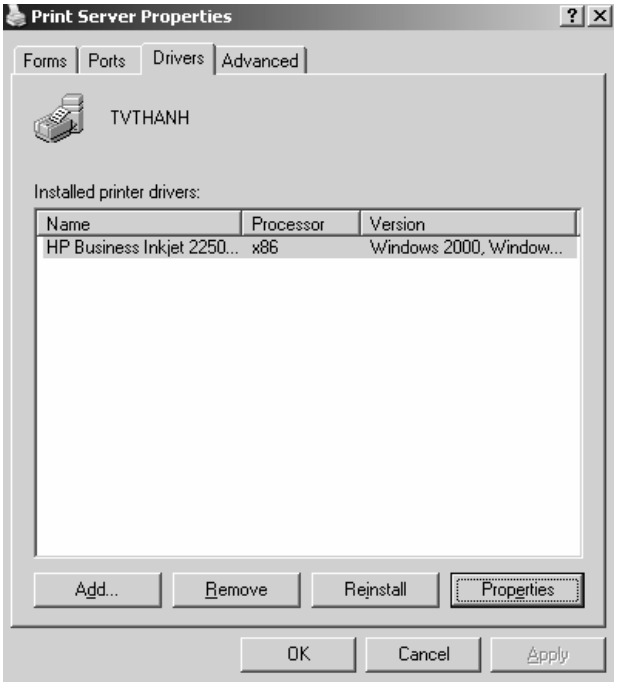
Trong hộp thoại **Printer Server Properties**, bạn mở **tab Driver**. **Tab Driver** cho phép bạn quản lý các **driver** máy in đã được cài đặt trên **Print Server**. Đối với mỗi **driver** máy in, **Tab** này sẽ hiển thị tên, môi trường và hệ điều hành mà **driver** hỗ trợ.

Sử dụng các tùy chọn trong **Tab Driver**, bạn có thể thêm vào hay loại bỏ hay cập nhật **driver** máy in. Để nhìn thấy các thuộc tính của một **driver** máy in, ta chọn **driver** cần hiển thị và nhấp chuột vào nút **Properties**. Các thuộc tính của một **driver** máy in gồm có:

- Tên **driver**.
- Phiên bản.
- Bộ xử lý.
- Ngôn ngữ.
- Loại dữ liệu mặc định.
- Đường dẫn của **driver**.



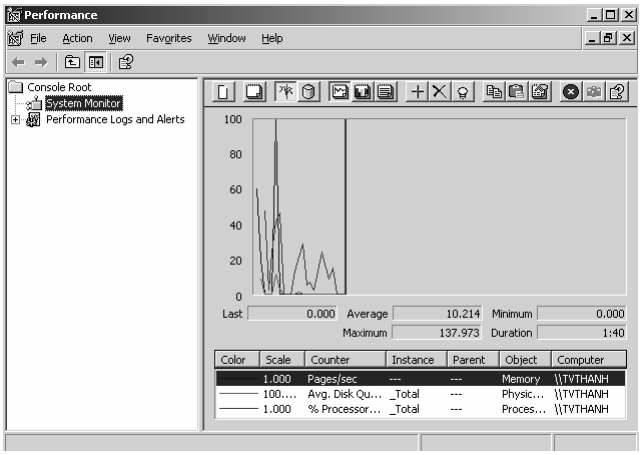
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




# IX. GIÁM SÁT TRẠNG THÁI HÀNG ĐỢI MÁY IN.

Chúng ta có thể dùng tiện ích **System Monitor** để quản lý hàng đợi máy in. **System Monitor** được dùng để theo dõi các **counter** liên quan đến thao tác thực hiện cho nhiều đối tượng máy tính. Muốn quản lý hàng đợi máy in bằng **System Monitor**, ta thực hiện theo các bước sau:

1. Chọn **Start** ⏲ **Administrative Tools** ⏲ **Performance**.
2. Hộp thoại **Performance** sẽ xuất hiện. Mặc định thì tiện ích **System Monitor** sẽ được chọn như hình sau:




3. Nhấp chuột vào nút **Add** (có biểu tượng dấu +) để truy xuất vào hộp thoại **Add Counters**. Sau đó, nhấp chọn **Print Queue Performance Object.**



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net


4. Trong hộp thoại **Add Counters**, bạn có thể chỉ định ra máy tính mà bạn muốn giám sát (cả máy tính cục bộ và máy tính ở xa). **Performance Object** mà bạn cần theo dõi (trong trường hợp này là hàng đợi - **Print Queue**), các **counter** mà bạn muốn theo dõi, và bạn cũng chỉ ra là bạn có muốn theo dõi tất cả các thể hiện hay là bạn chỉ muốn theo dõi một số thể hiện của **counter** được bạn lựa chọn. Nếu bạn chọn tất cả các thể hiện được lựa chọn sẽ cho phép tất cả dữ liệu của tất cả các hàng đợi in ấn đã được định nghĩa trong máy in. Còn nếu bạn chọn chỉ theo dõi một số thể hiện của **counter** thì bạn chỉ theo dõi được dữ liệu từ một số hàng đợi in ấn cá nhân.

Bảng danh sách các hàng đợi in ấn đã được định nghĩa:

| Print Queue Counter | Mô tả |
|---|---|
| Add Network Printer Calls | Counter này sẽ chỉ ra bao nhiêu **Print Server** đã được thêm vào các máy in được chia sẻ trong mạng. Con số này được tích lũy từ lần khởi động cuối cùng của **server.** |
| Bytes Printed/Sec | Số **byte** trong thực tế đã được in trên một hàng đợi trong mỗi giây |
| Enumerate Network Printer Calls | Chỉ ra có bao nhiêu yêu cầu đã được gửi đến **Print Server** từ các danh sách duyệt mạng. Con số này được tích luỹ từ lần khởi động cuối cùng của **Server**. |
| Job Errors | Tổng số các lỗi thao tác đã được tường trình bởi hàng đợi in ấn. Con số này được tích luỹ từ lần khởi động cuối cùng của **Server**. |
| Jobs | Chỉ ra con số hiện tại các thao tác in ấn vẫn còn trong hàng đợi chưa được xử lý. |
| Job Spooling | Chỉ ra con số hiện tại các thao tác in ấn đã được điều hướng đến hàng đợi in ấn.. |



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

| | |
|---|---|
| Max Jobs Spooling | Chỉ ra con số tối đa các thao tác in ấn đã được lưu trữ trong hàng đợi in |



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

| | |
|---|---|
| | ấn kể từ lần khởi động cuối cùng của **Server**. |
| Max References | Chỉ ra con số tối đa các tác vụ mở (tham chiếu) đã được gửi đến máy in kể từ lần khởi động cuối cùng của **Server**. |
| Not Ready Errors | Chỉ ra số lượng các lỗi máy in "chưa sẵn sàng phục vụ" đã được phát sinh trong hàng đợi in ấn. Con số này được tích luỹ từ lần khởi động cuối cùng của **Server**. |
| Out of Paper Errors | Chỉ ra số lượng các lỗi máy in không có giấy đã được phát sinh trong hàng đợi in ấn. Con số này được tích luỹ từ lần khởi động cuối cùng của **Server**. |
| Total Jobs Printed | Được sử dụng để hiển thị bao nhiêu tác vụ in ấn đã được thực hiện thành công. Con số này được tích luỹ từ lần khởi động cuối cùng của **Server**. |
| Total Pages Printed | Được sử dụng để hiển thị bao nhiêu trang đã được in thành công. Con số này được tích luỹ từ lần khởi động cuối cùng của **Server**. |



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Bài 17
DỊCH VỤ TRUY CẬP TỪ XA

# Tóm tắt

Lý thuyết 5 tiết - Thực hành 10 tiết

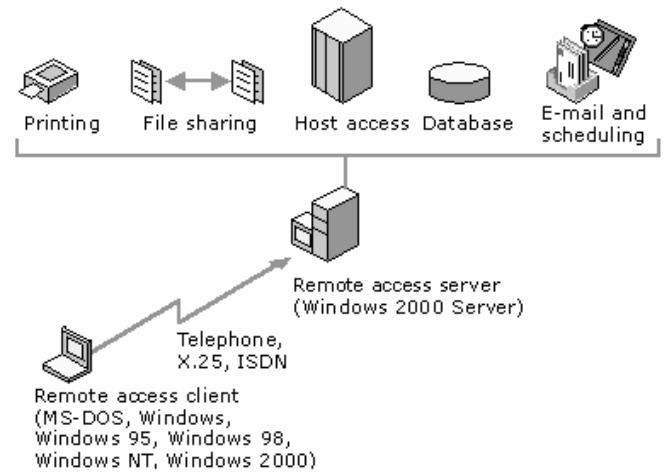
| Mục tiêu | Các mục chính | Bài tập bắt buộc | Bài tập làm thêm |
|---|---|---|---|
| Kết thúc bài học này cung cấp học viên kiến thức về dịch vụ truy cập từ xa, cho phép máy trạm ở xa có thể quay số kết nối vào công ty thông qua đường dây điện thoại, chia sẻ Internet đơn giản … | I. Xây dựng một Remote Access Server.<br>II. Xây dựng một Internet Connection Server. | Dựa vào bài tập môn Quản trị Windows Server 2003. | Dựa vào bài tập môn Quản trị Windows Server 2003. |



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

# I. XÂY DỰNG MỘT REMOTE ACCESS SERVER.

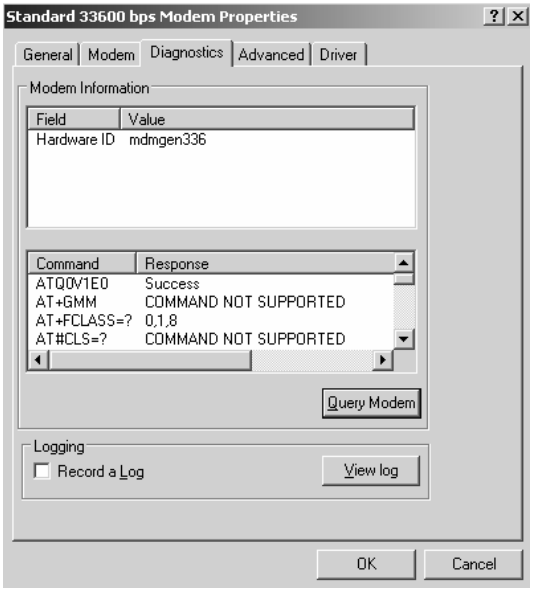
Giả sử bạn định xây dựng một hệ thống mạng cho phép các người dùng di động (**mobile user**) hoặc các văn phòng chi nhánh ở xa kết nối về. Để đáp ứng được nhu cầu trên bạn phải thiết lập một **Remote Access Server** (**RAS**). Khi máy tính **Client** kết nối thành công vào **RAS**, máy tính này có thể truy xuất đến toàn bộ hệ thống mạng phía sau **RAS**, nếu được cho phép, và thực hiện các thao tác như thể máy đó đang kết nối trực tiếp vào hệ thống mạng.




## I.1. Cấu hình RAS server.

Sau đây là các bước xây dựng một **RAS Server** dùng các kết nối quay số.

Đầu tiên, bạn phải đảm bảo đã cài **driver** cho các modem định dùng để nhận các cuộc gọi vào. Để kiểm tra, bạn vào **Start** ◴ **Settings** ◴ **Control Panel** ◴ **Phone and Modem Options**, trong hộp thoại **Phone and Modem Options**, bạn chọn **Modem** cần kiểm tra và nhấp chuột vào nút **Properties**. Tại hộp thoại **Properties**, bạn chọn **Tab Diagnostics** và nhấp chuột vào nút **Query Modem** để hệ thống kiểm tra **Modem** hiện tại, nếu có lỗi thì hệ thống sẽ thông báo.

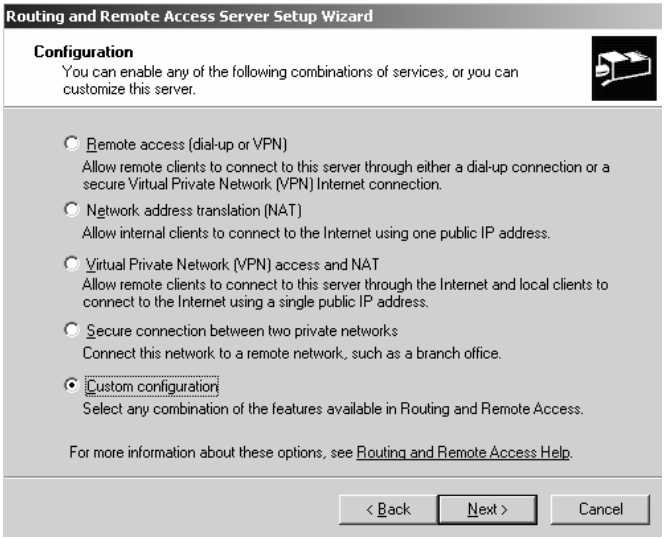




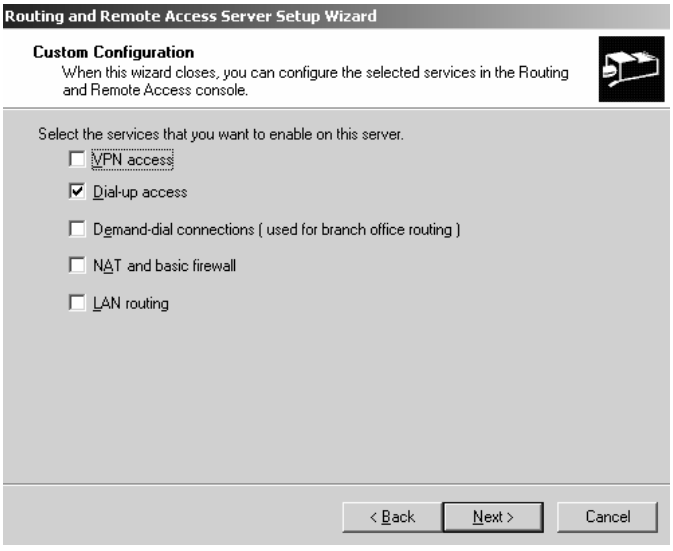

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Tiếp theo bạn cần kích hoạt dịch vụ **Routing and Remote Access** trên **Windows Server 2003**. Bạn nhấp chuột vào **Start** 🕘 **Programs** 🕘 **Administrative Tools** 🕘 **Routing and Remote Access**, hộp thoại mở ra bạn nhấp phải chuột lên biểu tượng server của bạn, chọn **Configure and Enable Routing and Remote Access**. Chương trình sẽ xuất hiện hộp thoại **Welcome to the Routing and Remote Access Server Setup Wizard**. Nhấn **Next** để tiếp tục.

Trong hộp thoại tiếp theo, **Configuration**, bạn chọn **Custom configuration** và chọn **Next**.



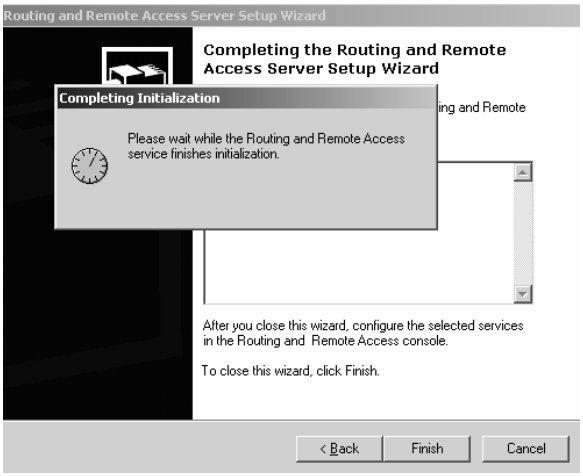

Tiếp theo hộp thoại **Custom Configuration** xuất hiện, bạn chọn mục **Dial-up access** vì chúng ta cần xây dựng một **Server** cho phép các máy tính ở xa truy cập vào. Sau đó bạn nhấp chuột vào nút **Next** để tiếp tục. Hộp thoại **Completing the Routing and Remote Access Server Setup Wizard** xuất hiện, chọn **Finish** để kết thúc.



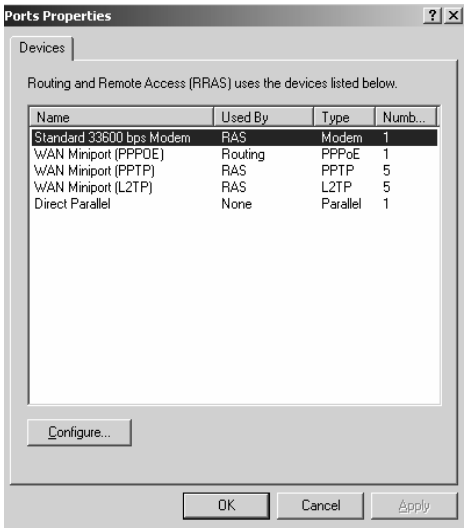

Một hộp thoại cảnh báo xuất hiện, yêu cầu bạn cho biết có khởi động dịch vụ này lên hay không? Bạn chọn **Yes** để khởi động dịch vụ.



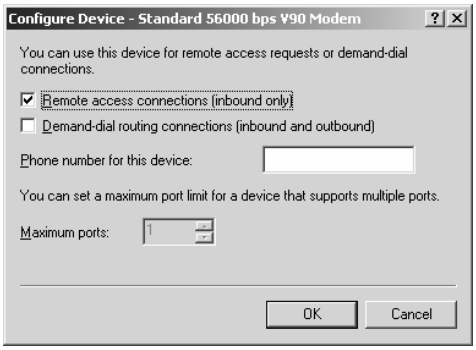
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Trong cửa sổ chính của chương trình, bạn cấu hình cho phép hệ thống dùng **modem** để nhận các cuộc gọi. Nhấp phải chuột lên mục **Ports**, chọn **Properties**. Hộp thoại **Ports Properties** xuất hiện. Trong hộp thoại này, chọn một thiết bị **Modem** và nhấn **Configure** để cấu hình.




Xuất hiện hộp thoại **Configure Device**. Trong hộp thoại này, chọn vào mục **Remote access connections (inbound only)**, chỉ chấp nhận các cuộc gọi hướng vào. Sau đó nhấn nút **OK**.





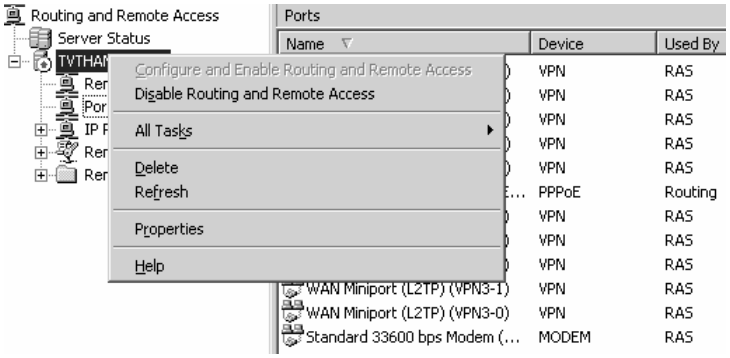

Lặp lại bước (7) cho các thiết bị **modem** khác. Sau khi đã thực hiện xong, nhấn nút **OK** để đóng hộp thoại **Ports Properties** lại. Tiếp theo, bạn sẽ cấu hình để **Server** thực hiện chức năng RAS. Nhấn phải

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

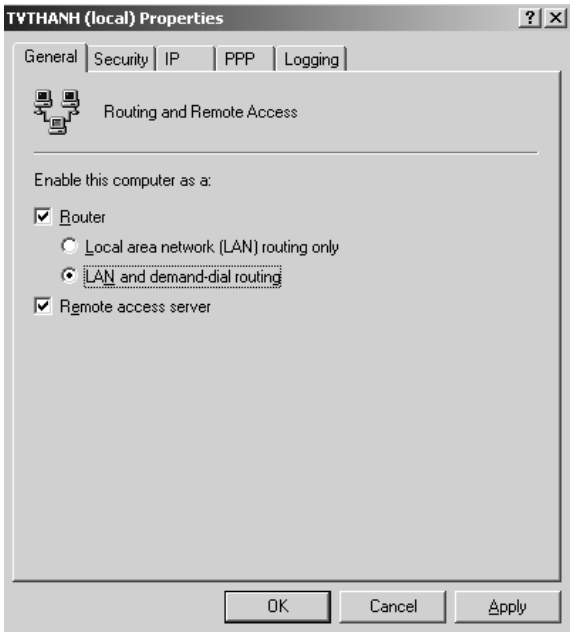
chuột lên biểu tượng **Server** và chọn **Properties**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net



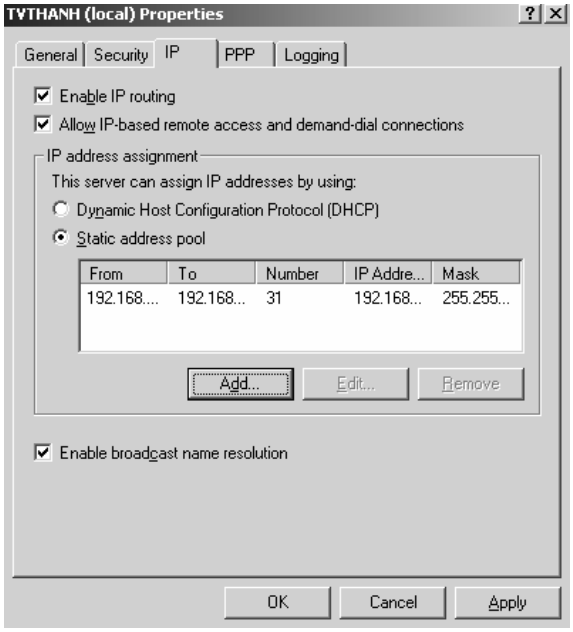

Hộp thoại **Server Properties** xuất hiện. Trong **Tab General**, bạn chọn các mục **Router**, **LAN and dial-demand routing** và mục **Remote access server**.



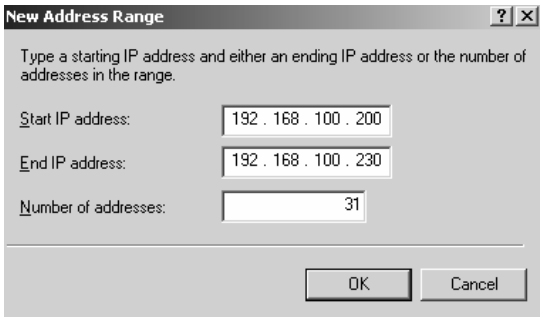

Tiếp theo, bạn chọn Tab **IP**. Tab này chỉ xuất hiện khi hệ thống mạng của bạn có sử dụng bộ giao thức TCP/IP. Phần **IP address assignment** chỉ định cách cấp phát địa chỉ IP cho các **RAS Client** khi quay số vào. Nếu hệ thống mạng đã thiết lập một **DHCP Server** thì bạn có thể nhờ **DHCP Server** này cấp phát địa chỉ cho các **RAS Client** (chọn mục **Dynamic Host Configuration Protocol**). Nếu không có, bạn phải chỉ định danh sách các địa chỉ sẽ cấp phát (chọn mục **Static address pool**). Trong ví dụ này, bạn sẽ nhập vào danh sách địa chỉ **IP**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Để bổ sung danh sách địa chỉ, chọn mục **Static address pool** và nhấn **Add**. Xuất hiện hộp thoại **New Address Range**. Trong hộp thoại này, bạn nhập vào địa chỉ bắt đầu và địa chỉ kết thúc của danh sách. Các địa chỉ này nên lấy từ đường mạng của **RAS Server**. Nếu bạn sử dụng đường mạng khác, bạn phải đặt các đường đi tĩnh cho từng đường mạng mới đó. Sau đó nhấn **OK** để đồng ý tạo.



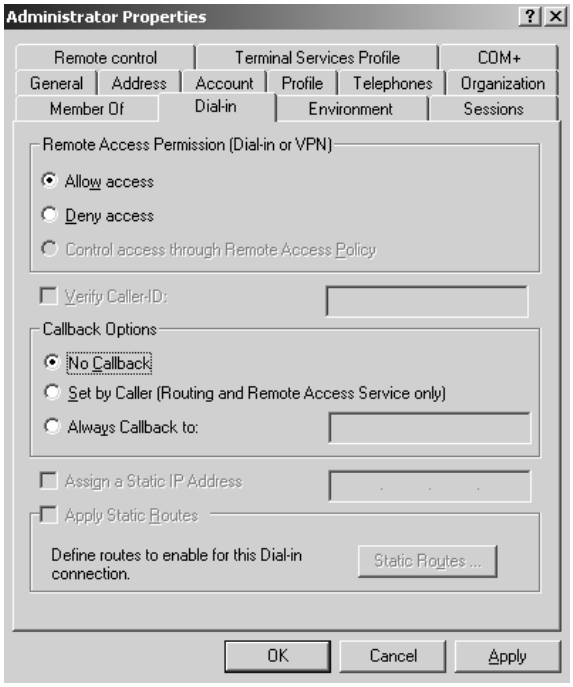

Các Tab khác chúng ta để mặc định, sau khi đã cấu hình xong, nhấn **OK** để đóng hộp thoại **Server Properties** lại.

Bước tiếp theo là cấu hình các tài khoản dùng để quay số. Bạn có thể tạo trong **local security database** nếu **RAS Server** nằm trong **workgroup** hoặc tạo trên **Active Directory database** nếu là thành viên của một **domain**. Kích hoạt chương trình **Local User and Group** (hoặc **Active Directory Users and Computers** tuỳ theo ví trị tạo tài khoản), nhấp phải chuột lên tài khoản định cấu hình và chọn **Properties**.

Hộp thoại **User Properties** xuất hiện. Bạn chọn Tab **Dial-in** và chọn mục **Allow Access** để cho phép người dùng này được phép truy cập từ xa thông qua quay số. Ngoài ra trong hộp thoại này cũng cho phép bạn chọn chế độ quay số, nếu chọn mặc định (**No Callback**) thì phía máy trạm sẽ trả phí điện thoại, nhưng nếu bạn chọn chế độ **Callback** thì phía Server sẽ trả chi phí điện thoại trong quá trình quay số để truyền dữ liệu. Sau đó nhấn **OK** để đóng hộp thoại lại.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Như vậy là bạn đã cấu hình xong một **RAS Server**. Người dùng có thể bắt đầu dùng tài khoản đã cấp thực hiện kết nối từ xa qua đường quay số, truy xuất vào hệ thống mạng ở cơ quan.

## I.2. Cấu hình RAS client.

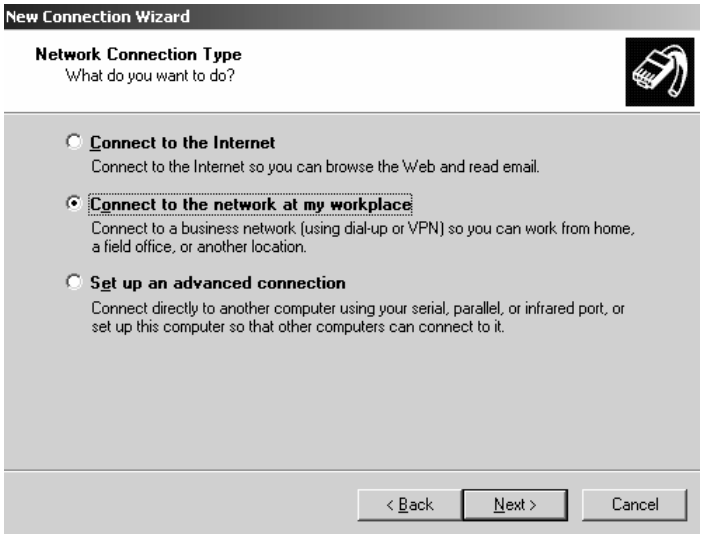
Tiếp theo chúng ta tạo một **network connection** trên máy trạm để quay số đến một **RAS Server**. Máy trạm có thể sử dụng hệ điều hành **Win98**, **WinME**, **Win2000**, **WinXP**… Để kết nối đến một **RAS Server**, bạn cần tối thiểu ba thông tin như: số điện thoại của **RAS Server**, **username** và **passwork** do **RAS Server** cấp. Trong ví dụ này chúng ta dùng máy **Windows Server 2003 Stand-alone** để minh họa, các bước thực hiện như sau:

Mở menu **Start** ⏲ **Settings** ⏲ **Network and Dial-up Connections**. Trong cửa sổ **Network and Dial-up Connections**, nhấp đôi chuột vào **Make New Connection**. Xuất hiện hộp thoại **Welcome to the Network Connection Wizard**, bạn nhấn **Next** để tiếp tục.

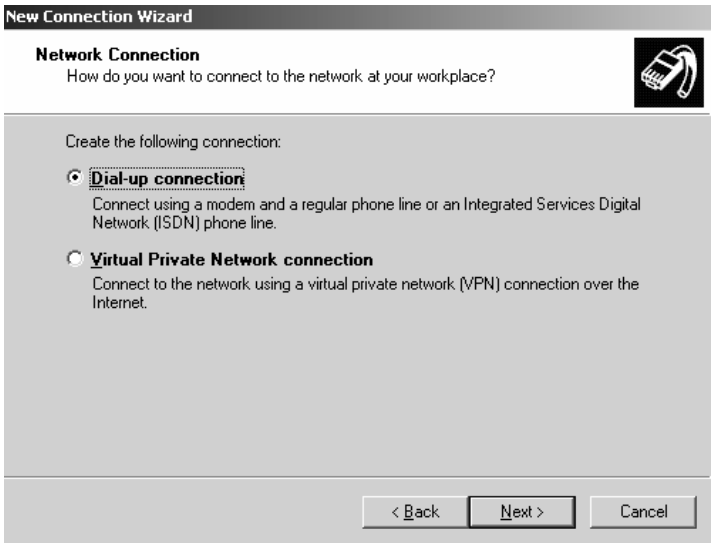
Trong hộp thoại **Network Connection Type**, bạn chọn mục **Connect to the network at my workplace** vì ở đây chúng ta kết nối với **RAS Server** nội bộ của công ty, không kết nối **Internet**. Sau đó nhấn nút **Next** để tiếp tục.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Tiếp theo bạn chọn loại kết nối là **Dial-up** hay **VPN**, ở đây chúng ta chọn kết nối kiểu quay số dùng **Modem**.



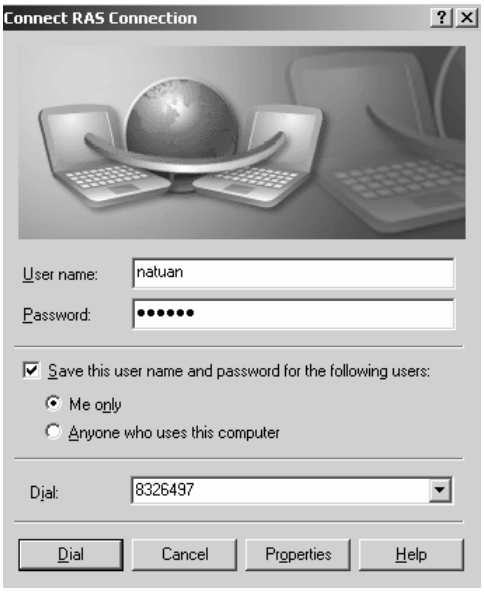

Theo hướng dẫn của chương trình, bạn sẽ nhập tên của kết nối này, số điện thoại cần gọi đến của **RAS Server**, kết nối này chỉ dùng cho người dùng hiện tại hay cho mọi người.

Cuối cùng, hộp thoại **Completing the Network Connection Wizard** xuất hiện bạn nhấn nút **Finish** để hoàn thành quá trình tạo kết nối.

Khi muốn thiết lập kết nối, bạn kích hoạt biểu tượng của **Connection** mới tạo, hộp thoại **Connect** xuất hiện, bạn nhập vào **username** và **password** đã được tạo ra trên **RAS Server** (hay nói cách khác là đã được quản trị **RAS Server** cấp phát), kiểm tra lại số điện thoại của **RAS Server** và nhấn nút **Dial**.

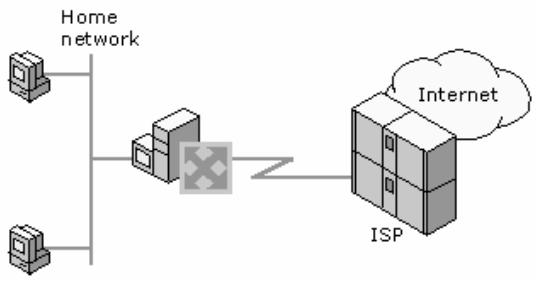


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




# II. XÂY DỰNG MỘT INTERNET CONNECTION SERVER.

Bạn đang quản lý một hệ thống mạng nhỏ, sử dụng giao thức **TCP/IP** và bạn định thiết lập kết nối Internet cho hệ thống mạng của mình. Thông thường, các hệ thống mạng như vậy sử dụng địa chỉ riêng (**private address**). Để các máy tính bên trong mạng có thể truy xuất ra mạng **Internet**, bạn cần phải có một máy tính đóng vai trò như một **Router** hỗ trợ **NAT** (**Network Address Translation**).



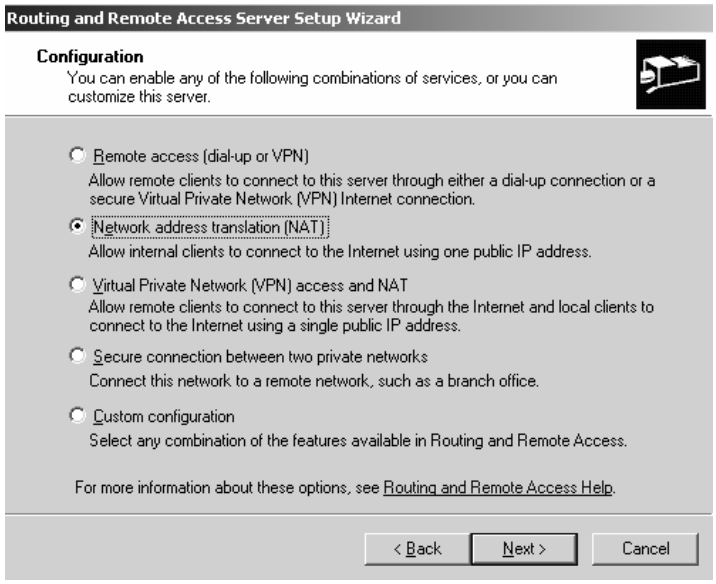

## II.1. Cấu hình trên server.

Bạn có thể sử dụng dịch vụ **Routing and Remote Access** để xây dựng một **Internet Connection Server** hỗ trợ **NAT**, phục vụ cho mục đích trên. Cách thực hiện như sau:

Đầu tiên, bạn phải đảm bảo đã cài driver cho các modem. Thực hiện kiểm tra như hướng dẫn trong phần trên. Cấu hình để các **Modem** này chấp nhận các cuộc gọi ra ngoài khi có nhu cầu (**demand-dial**). Thực hiện theo các bước như trong mục trên nhưng đến hộp thoại **Configuration**, bạn chọn trong **Network address translation (NAT)**.

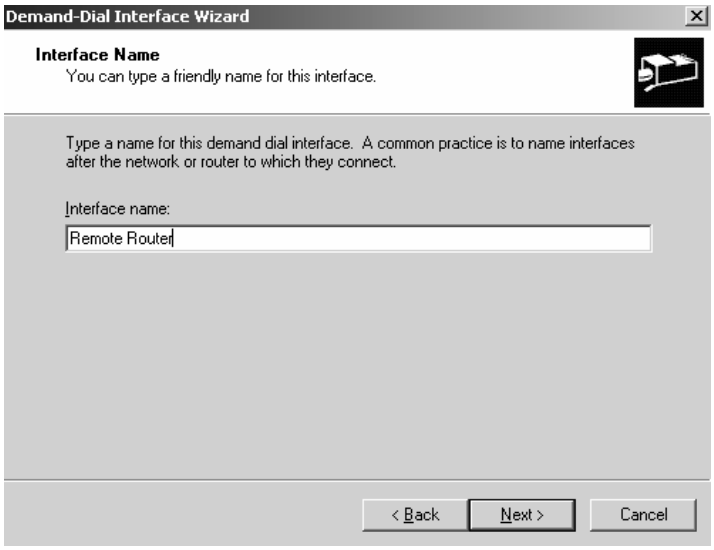


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Tiếp theo hộp thoại **NAT Internet Connection** xuất hiện, bạn để mặc định vì chúng ta cần tạo một **demand-dial interface**. Bạn nhấn **Next** để chương trình tiếp tục.

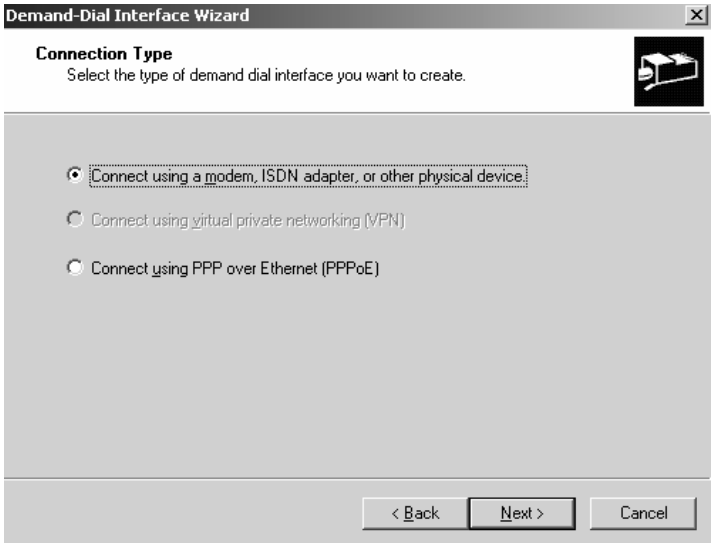
Hộp thoại **Interface Name** yêu cầu bạn đặt cho **interface** mới này một cái tên. Thông thường bạn nên đặt tên của **Router** ở xa để dễ quản lý.




Hộp thoại **Connection Type** yêu cầu bạn chọn loại kết nối mà **interface** này sử dụng.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

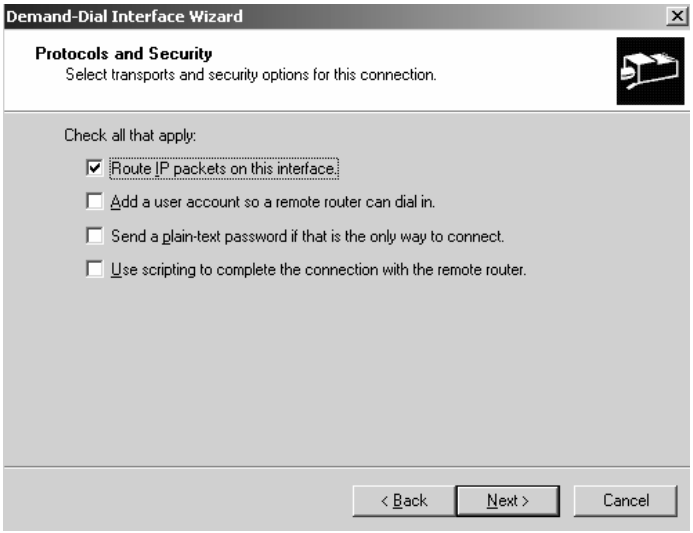



Hộp thoại **Select a device** yêu cầu bạn chọn loại thiết bị kết nối dùng cho **interface**.

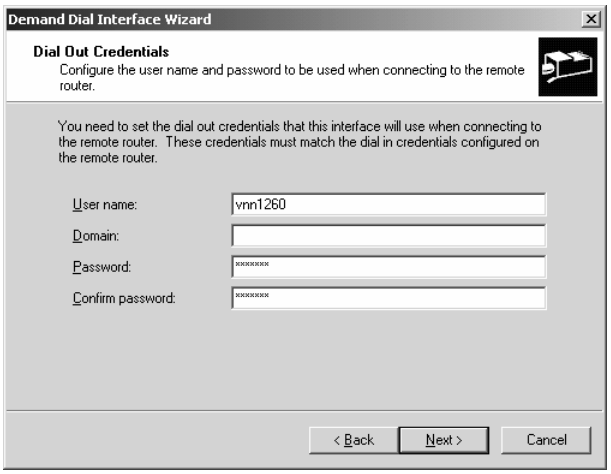

Trong hộp thoại **Phone Number**, bạn nhập vào số điện thoại mà **ISP** cung cấp cho bạn. Hộp thoại **Protocols and Security** yêu cầu bạn chọn loại giao thức chuyển vận và các tuỳ chọn an toàn cho kết nối. Thông thường, bạn nên chọn **Route IP packets on this interface**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Trong hộp thoại **Dial Out Credentials**, bạn nhập vào thông tin tài khoản dùng để kết nối đến **ISP** (cũng chính **ISP** sẽ cung cấp cho bạn).

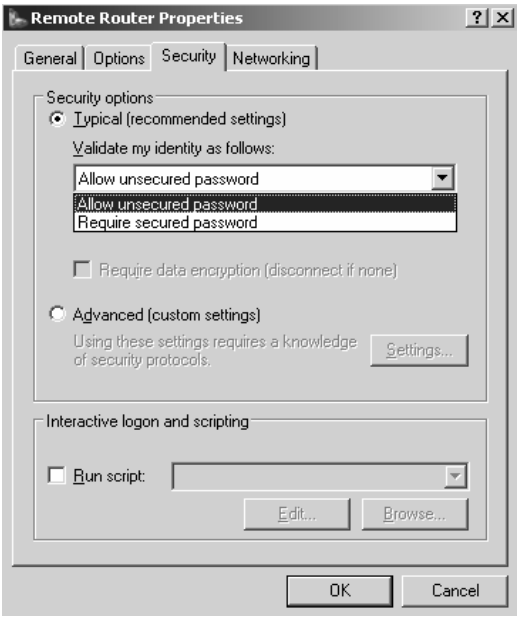



Cuối cùng hộp thoại **Completing the demand dial interface wizard** cho biết kết thúc quá trình cấu hình. Bạn nhấn **Finish** để kết thúc.

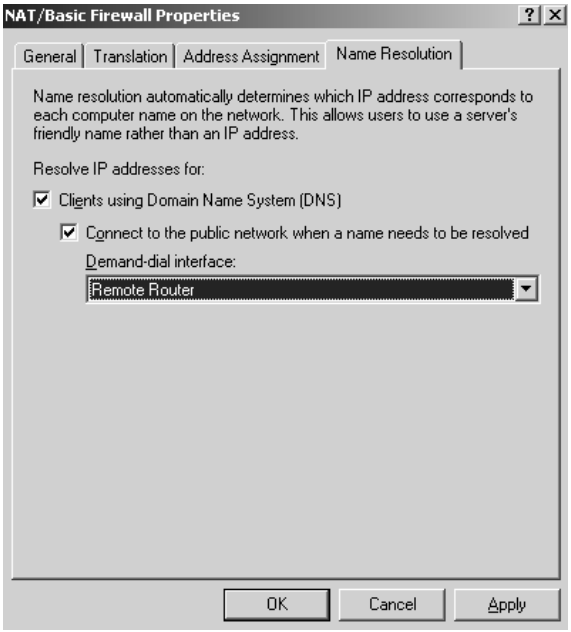
Sau khi đã tạo xong **demand-dial interface**, tuỳ theo **ISP** có chấp nhận việc thiết lập kết nối an toàn hoặc không an toàn. Hiện tại các nhà cung cấp dịch vụ ở Việt Nam cung cấp các kết nối không mã hóa. Trong mục **Network Interfaces**, nhấn phải chuột lên **demand-dial interface** mới tạo, chọn **Properties**. Trong hộp thoại **Properties**, chọn Tab **Security**. Trong phần **Security options**, mục **Validate my identity as follows**, bạn có thể chọn **Require secured password** hoặc **Allow unsecured password** (nếu quay số vào **ISP** thông thường thì nên chọn mục này).



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Mở rộng mục **IP Routing** trong cửa sổ **Routing and Remote Access**, nhấn phải chuột lên mục **NAT** và chọn **Properties**. Trong hộp thoại **NAT Properties**, bạn chọn Tab **Name Resolution**. Trong Tab này, bạn chọn mục **Clients using Domain Name System (DNS)**. Nếu muốn mỗi khi có yêu cầu phân giải tên thì **Server** sẽ kết nối vào mạng thì bạn chọn luôn mục **Connect to the public network when a name needs to be resolved** và chọn **demand-dial interface** vừa tạo. Sau khi chọn xong nhấn **OK** để kết thúc.




## II.2. Cấu hình trên máy trạm.



Do server bạn vừa thiết lập trên đây là một **NAT router** và một **Forwarder DNS Server**, cho nên trên các máy trạm, ngoài việc cấu hình TCP/IP về địa chỉ **IP**, **subnet mask**, bạn phải chỉ định **default gateway** và **DNS Server** là địa chỉ của **Server** trên.

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

# Tóm tắt

Lý thuyết 6 tiết - Thực hành 12 tiết

| Mục tiêu | Các mục chính | Bài tập bắt buộc | Bài tập làm thêm |
|---|---|---|---|
| Kết thúc bài học giúp học viên hiểu nguyên tắc hoạt động, tổ chức, cài đặt và quản trị dịch vụ phân giải tên miền DNS, hiểu được mô hình phân giải tên trên hệ thống mạng Internet. | I. Tổng quan về DNS<br>II. Cách phân bổ dữ liệu quản lý Domain Name.<br>III. Cơ chế phân giải tên miền<br>IV. Một số khái niệm cơ bản.<br>V. Phân loại Domain Name Server.<br>VI. Resource Record (RR)<br>VII. Cài đặt và cấu hình dịch vụ DNS | Dựa vào bài tập môn Dịch vụ mạng Windows 2003. | Dựa vào bài tập môn Dịch vụ mạng Windows 2003. |



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

# I. Tổng quan về DNS.

## I.1. Giới thiệu DNS.

Mỗi máy tính trong mạng muốn liên lạc hay trao đổi thông tin, dữ liệu cho nhau cần phải biết rõ địa chỉ **IP** của nhau. Nếu số lượng máy tính nhiều thì việc nhớ những địa chỉ **IP** này rất là khó khăn.

Mỗi máy tính ngoài địa chỉ **IP** ra còn có một tên (hostname). Đối với con người việc nhớ tên máy dù sao cũng dễ dàng hơn vì chúng có tính trực quan và gợi nhớ hơn địa chỉ **IP**. Vì thế, người ta nghĩ ra cách làm sao ánh xạ địa chỉ **IP** thành tên máy tính.

Ban đầu do quy mô mạng **ARPA NET** (tiền thân của mạng **Internet**) còn nhỏ chỉ vài trăm máy, nên chỉ có một tập tin đơn HOSTS.TXT lưu thông tin về ánh xạ tên máy thành địa chỉ **IP**. Trong đó tên máy chỉ là 1 chuỗi văn bản không phân cấp (**flat name**). Tập tin này được duy trì tại 1 máy chủ và các máy chủ khác lưu giữ bản sao của nó. Tuy nhiên khi quy mô mạng lớn hơn, việc sử dụng tập tin **HOSTS.TXT** có các nhược điểm như sau:

- Lưu lượng mạng và máy chủ duy trì tập tin HOSTS.TXT bị quá tải do hiệu ứng “cổ chai”.
- Xung đột tên: Không thể có 2 máy tính có cùng tên trong tập tin HOSTS.TXT . Tuy nhiên do tên máy không phân cấp và không có gì đảm bảo để ngăn chặn việc tạo 2 tên trùng nhau vì không có cơ chế uỷ quyền quản lý tập tin nên có nguy cơ bị xung đột tên.
- Không đảm bảo sự toàn vẹn: việc duy trì 1 tập tin trên mạng lớn rất khó khăn. Ví dụ như khi tập tin HOSTS.TXT vừa cập nhật chưa kịp chuyển đến máy chủ ở xa thì đã có sự thay đổi địa chỉ trên mạng rồi.

Tóm lại việc dùng tập tin HOSTS.TXT không phù hợp cho mạng lớn vì thiếu cơ chế phân tán và mở rộng. Do đó, dịch vụ **DNS** ra đời nhằm khắc phục các nhược điểm này. Người thiết kế cấu trúc của dịch vụ **DNS** là **Paul Mockapetris** - **USC's Information Sciences Institute**, và các khuyến nghị **RFC** của **DNS** là **RFC** 882 và 883, sau đó là **RFC** 1034 và 1035 cùng với 1 số **RFC** bổ sung như bảo mật trên hệ thống **DNS**, cập nhật động các bản ghi **DNS** …

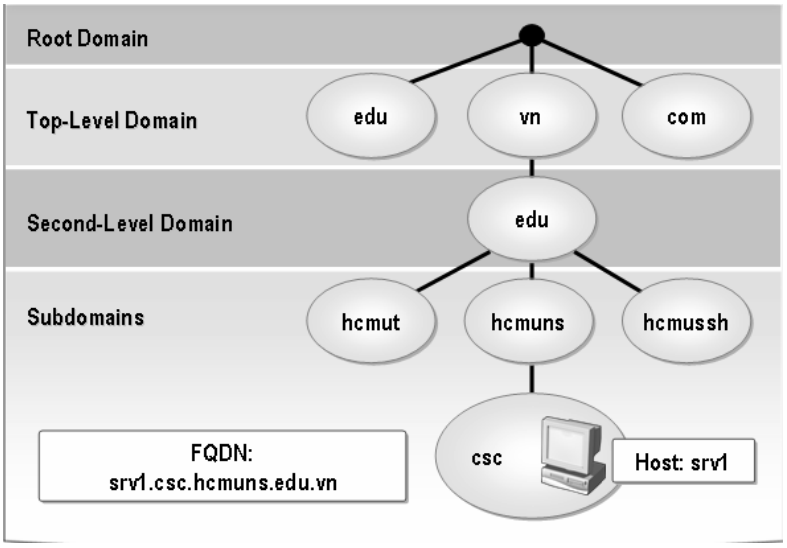
**Lưu ý:** Hiện tại trên các máy chủ vẫn sử dụng được tập tin hosts.txt để phân giải tên máy tính thành địa chỉ **IP** (trong Win**d**ows tập tin này nằm trong thư mục **WINDOWS\system32\drivers\etc**)

Dịch vụ **DNS** hoạt động theo mô hình **Client-Server**: phần **Server** gọi là máy chủ phục vụ tên hay còn gọi là **Name Server**, còn phần **Client** là trình phân giải tên - **Resolver**. **Name Server** chứa các thông tin CSDL của **DNS**, còn **Resolver** đơn giản chỉ là các hàm thư viện dùng để tạo các truy vấn (**query**) và gửi chúng qua đến **Name Server**. **DNS** được thi hành như một giao thức tầng **Application** trong mạng **TCP/IP**.

**DNS** là 1 CSDL phân tán. Điều này cho phép người quản trị cục bộ quản lý phần dữ liệu nội bộ thuộc phạm vi của họ, đồng thời dữ liệu này cũng dễ dàng truy cập được trên toàn bộ hệ thống mạng theo mô hình **Client-Server**. Hiệu suất sử dụng dịch vụ được tăng cường thông qua cơ chế nhân bản (**replication**) và lưu tạm (**caching**). Một **hostname** trong domain là sự kết hợp giữa những từ phân cách nhau bởi dấu chấm(.).



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 1.1: Sơ đồ tổ chức DNS

Cơ sở dữ liệu(CSDL) của **DNS** là một cây đảo ngược. Mỗi nút trên cây cũng lại là gốc của 1 cây con. Mỗi cây con là 1 phân vùng con trong toàn bộ CSDL **DNS** gọi là 1 miền (**domain**). Mỗi domain có thể phân chia thành các phân vùng con nhỏ hơn gọi là các miền con (**subdomain**).

Mỗi **domain** có 1 tên (**domain name**). Tên **domain** chỉ ra vị trí của nó trong CSDL **DNS**. Trong **DNS** tên miền là chuỗi tuần tự các tên nhãn tại nút đó đi ngược lên nút gốc của cây và phân cách nhau bởi dấu chấm.

Tên nhãn bên phải trong mỗi **domain name** được gọi là **top-level domain**. Trong ví dụ trước srv1.csc.hcmuns.edu.vn, vậy miền ".vn" là **top-level domain**. Bảng sau đây liệt kê **top-level domain**.

| Tên miền | Mô tả |
|---|---|
| .com | Các tổ chức, công ty thương mại |
| .org | Các tổ chức phi lợi nhuận |
| .net | Các trung tâm hỗ trợ về mạng |
| .edu | Các tổ chức giáo dục |
| .gov | Các tổ chức thuộc chính phủ |
| .mil | Các tổ chức quân sự |
| .int | Các tổ chức được thành lập bởi các hiệp ước quốc tế |



Vì sự quá tải của những **domain name** đã tồn tại, do đó đã làm phát sinh những **top-level domain**

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

mới. Bảng sau đây liệt kê những **top-level domain** mới.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

| Tên miền | Mô tả |
|---|---|
| .arts | Những tổ chức liên quan đến nghệ thuật và kiến trúc |
| .nom | Những địa chỉ cá nhân và gia đình |
| .rec | Những tổ chức có tính chất giải trí, thể thao |
| .firm | Những tổ chức kinh doanh, thương mại. |
| .info | Những dịch vụ liên quan đến thông tin. |

Bên cạnh đó, mỗi nước cũng có một **top-level domain**. Ví dụ **top-leveldomain** của Việt Nam là .vn, Mỹ là .us, ta có thể tham khảo thêm thông tin địa chỉ tên miền tại địa chỉ: **http://www.thrall.org/domains.htm**

Ví dụ về tên miền của một số quốc gia.

| Tên miền quốc gia | Tên quốc gia |
|---|---|
| .vn | Việt Nam |
| .us | Mỹ |
| .uk | Anh |
| .jp | Nhật Bản |
| .ru | Nga |
| .cn | Trung Quốc |
| … | … |

## I.2. Đặt điểm của DNS trong Windows 2003.

- **Conditional forwarder**: Cho phép **Name Server** chuyển các yêu cầu phân giải dựa theo tên domain trong yêu cầu truy vấn.
- **Stub zone**: hỗ trợ cơ chế phân giải hiệu quả hơn.
- Đồng bộ các **DNS zone** trong **Active Directory** (**DNS zone replication in Active Directory**).
- Cung cấp một số cơ chế bảo mật tốt hơn trong các hệ thống **Windows** trước đây.
- Luân chuyển (**Round robin**) tất cả các loại **RR**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

- Cung cấp nhiêu cơ chế ghi nhận và theo dõi sự cố lỗi trên **DNS**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

- Hỗ trợ giao thức **DNS Security Extensions** (**DNSSEC**) để cung cấp các tính năng bảo mật cho việc lưu trữ và nhân bản (**replicate**) **zone**.
- Cung cấp tính năng **EDNS0** (**Extension Mechanisms for DNS**) để cho phép **DNS Requestor** quản bá những **zone transfer packet** có kích thước lớn hơn 512 byte.

# II. Cách phân bổ dữ liệu quản lý domain name.

Những **root name server** (.) quản lý những **top-level domain** trên **Internet**. Tên máy và địa chỉ **IP** của những **name server** này được công bố cho mọi người biết và chúng được liệt kê trong bảng sau. Những **name server** này cũng có thể đặt khắp nơi trên thế giới.

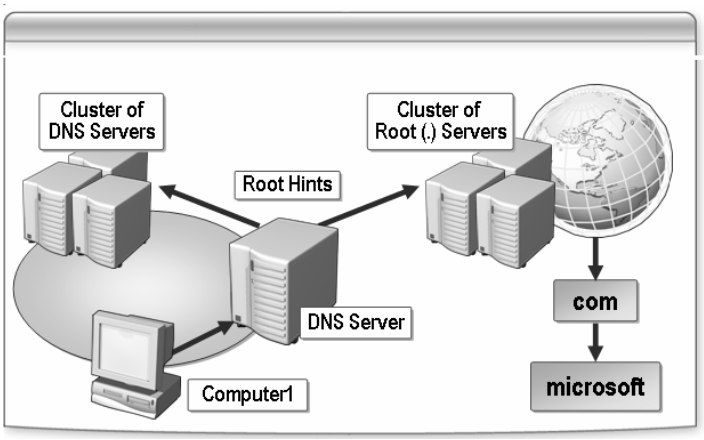
| Tên máy tính | Địa chỉ IP |
|---|---|
| H.ROOT-SERVERS.NET | 128.63.2.53 |
| B.ROOT-SERVERS.NET | 128.9.0.107 |
| C.ROOT-SERVERS.NET | 192.33.4.12 |
| D.ROOT-SERVERS.NET | 128.8.10.90 |
| E.ROOT-SERVERS.NET | 192.203.230.10 |
| I.ROOT-SERVERS.NET | 192.36.148.17 |
| F.ROOT-SERVERS.NET | 192.5.5.241 |
| F.ROOT-SERVERS.NET | 39.13.229.241 |
| G.ROOT-SERVERS.NET | 192.112.88.4 |
| A.ROOT-SERVERS.NET | 198.41.0.4 |

Thông thường một tổ chức được đăng ký một hay nhiều **domain name**. Sau đó, mỗi tổ chức sẽ cài đặt một hay nhiều **name server** và duy trì cơ sở dữ liệu cho tất cả những máy tính trong **domain**. Những **name server** của tổ chức được đăng ký trên **Internet**. Một trong những **name server** này được biết như là **Primary Name Server**. Nhiều **Secondary Name Server** được dùng để làm **backup** cho **Primary Name Server**. Trong trường hợp **Primary** bị lỗi, **Secondary** được sử dụng để phân giải tên.

**Primary Name Server** có thể tạo ra những **subdomain** và ủy quyền những **subdomain** này cho những **Name Server** khác.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 1.2: **Root hints**.

# III. Cơ chế phân giải tên.

## III.1. Phân giải tên thành IP.

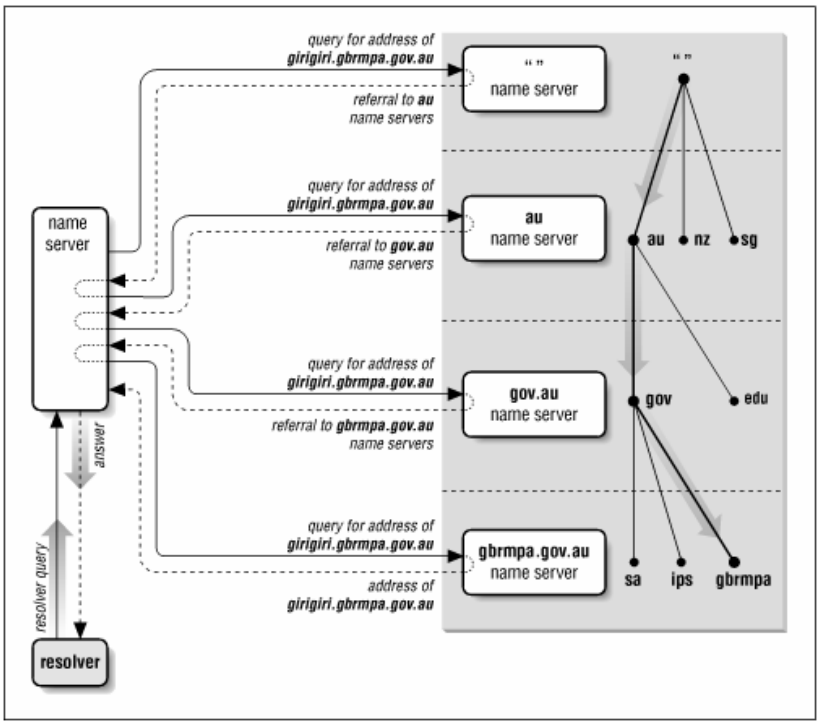
**Root name server** : Là máy chủ quản lý các **name server** ở mức **top-level domain**. Khi có truy vấn về một tên miền nào đó thì **Root Name Server** phải cung cấp tên và địa chỉ **IP** của **name server** quản lý **top-level domain** (Thực tế là hầu hết các **root server** cũng chính là máy chủ quản lý **top-level domain**) và đến lượt các **name server** của **top-level domain** cung cấp danh sách các **name server** có quyền trên các **second-level domain** mà tên miền này thuộc vào. Cứ như thế đến khi nào tìm được máy quản lý tên miền cần truy vấn.

Qua trên cho thấy vai trò rất quan trọng của **root name server** trong quá trình phân giải tên miền. Nếu mọi **root name server** trên mạng **Internet** không liên lạc được thì mọi yêu cầu phân giải đều không thực hiện được.

Hình vẽ dưới mô tả quá trình phân giải grigiri.gbrmpa.gov.au trên mạng **Internet**



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 1.3: Phân giải **hostname** thành địa **IP**.

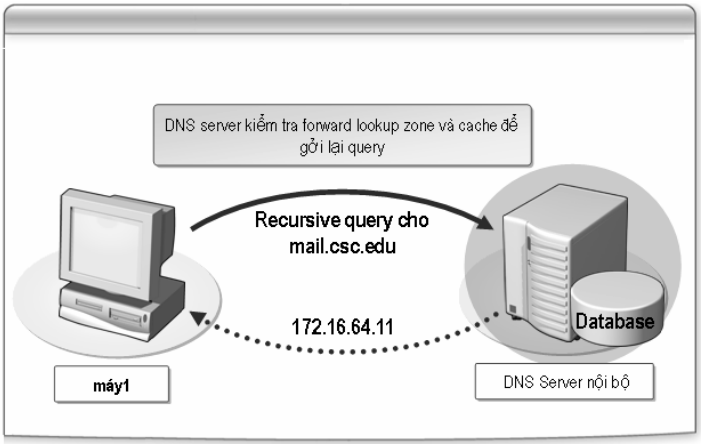
**Client** sẽ gửi yêu cầu cần phân giải địa chỉ **IP** của máy tính có tên girigiri.gbrmpa.gov.au đến **name server** cục bộ. Khi nhận yêu cầu từ **Resolver**, **Name Server** cục bộ sẽ phân tích tên này và xét xem tên miền này có do mình quản lý hay không. Nếu như tên miền do **Server** cục bộ quản lý, nó sẽ trả lời địa chỉ **IP** của tên máy đó ngay cho **Resolver**. Ngược lại, server cục bộ sẽ truy vấn đến một **Root Name Server** gần nhất mà nó biết được. **Root Name Server** sẽ trả lời địa chỉ IP của **Name Server** quản lý miền au. Máy chủ **name server** cục bộ lại hỏi tiếp **name server** quản lý miền au và được tham chiếu đến máy chủ quản lý miền gov.au. Máy chủ quản lý gov.au chỉ dẫn máy **name server** cục bộ tham chiếu đến máy chủ quản lý miền gbrmpa.gov.au. Cuối cùng máy **name server** cục bộ truy vấn máy chủ quản lý miền gbrmpa.gov.au và nhận được câu trả lời.

Các loại truy vấn : Truy vấn có thể ở 2 dạng :

- Truy vấn đệ quy (**recursive query**) : khi **name server** nhận được truy vấn dạng này, nó bắt buộc phải trả về kết quả tìm được hoặc thông báo lỗi nếu như truy vấn này không phân giải được. **Name server** không thể tham chiếu truy vấn đến một **name server** khác. **Name server** có thể gửi truy vấn dạng đệ quy hoặc tương tác đến **name server** khác nhưng phải thực hiện cho đến khi nào có kết quả mới thôi.

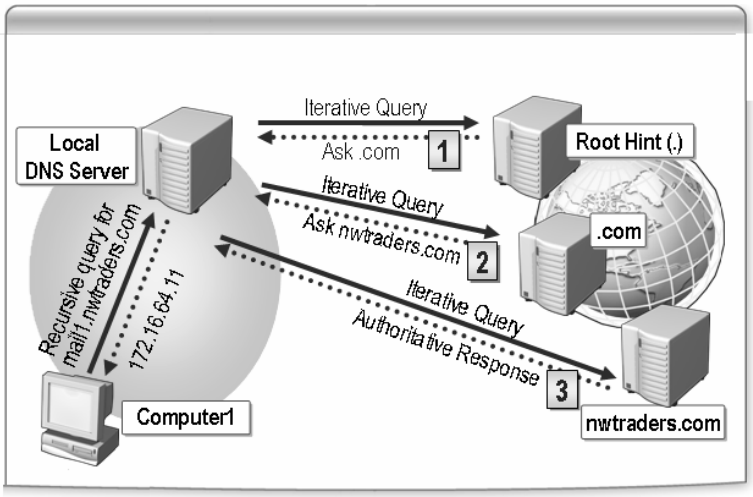


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 1.4: **Recursive query**.

- Truy vấn tương tác (**Iteractive query**): khi **name server** nhận được truy vấn dạng này, nó trả lời cho **Resolver** với thông tin tốt nhất mà nó có được vào thời điểm lúc đó. Bản thân **name server** không thực hiện bất cứ một truy vấn nào thêm. Thông tin tốt nhất trả về có thể lấy từ dữ liệu cục bộ (kể cả **cache**). Trong trường hợp **name server** không tìm thấy trong dữ liệu cục bộ nó sẽ trả về tên miền và địa chỉ IP của **name server** gần nhất mà nó biết.




Hình 1.5: Iteractive query

## III.2. Phân giải IP thành tên máy tính.

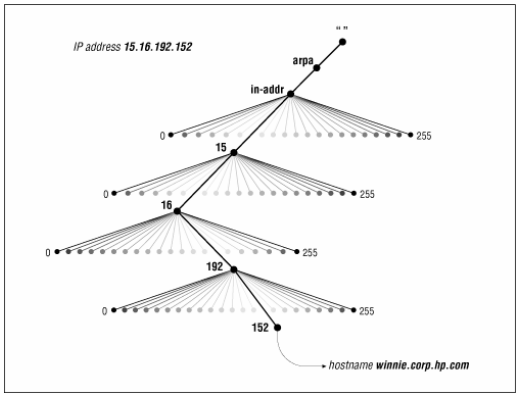
Ánh xạ địa chỉ **IP** thành tên máy tính được dùng để diễn dịch các tập tin log cho dễ đọc hơn. Nó còn dùng trong một số trường hợp chứng thực trên hệ thống **UNIX** (kiểm tra các tập tin .rhost hay host.equiv). Trong không gian tên miền đã nói ở trên dữ liệu -bao gồm cả địa chỉ **IP**- được lập chỉ mục theo tên miền. Do đó với một tên miền đã cho việc tìm ra địa chỉ **IP** khá dễ dàng.

Để có thể phân giải tên máy tính của một địa chỉ **IP**, trong không gian tên miền người ta bổ sung thêm một nhánh tên miền mà được lập chỉ mục theo địa chỉ **IP**. Phần không gian này có tên miền là **in-addr.arpa**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Mỗi nút trong miền **in-addr.arpa** có một tên nhãn là chỉ số thập phân của địa chỉ **IP**. Ví dụ miền **in-addr.arpa** có thể có 256 **subdomain**, tương ứng với 256 giá trị từ 0 đến 255 của byte đầu tiên trong địa chỉ IP. Trong mỗi **subdomain** lại có 256 **subdomain** con nữa ứng với byte thứ hai. Cứ như thế và đến byte thứ tư có các bản ghi cho biết tên miền đầy đủ của các máy tính hoặc các mạng có địa chỉ **IP** tương ứng.



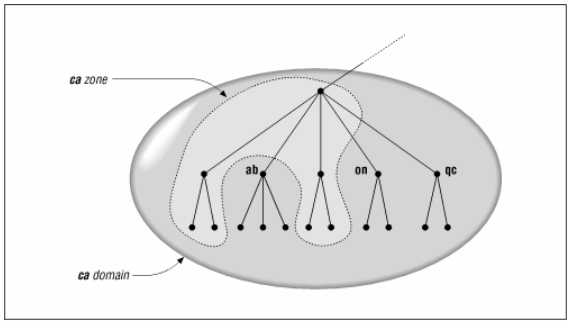

Hình 1.6: **Reverse Lookup Zone**.

- Lưu ý khi đọc tên miền địa chỉ **IP** sẽ xuất hiện theo thứ tự ngược. Ví dụ nếu địa chỉ **IP** của máy winnie.corp.hp.com là 15.16.192.152, khi ánh xạ vào miền in-addr.arpa sẽ là 152.192.16.15.in-addr.arpa.

# IV. Một số Khái niệm cơ bản.

## IV.1. Domain name và zone.

Một miền gồm nhiều thực thể nhỏ hơn gọi là miền con (**subdomain**). Ví dụ, miền **ca** bao gồm nhiều miền con như **ab.ca, on.ca, qc.ca,...**(như Hình 1.7). Bạn có thể ủy quyền một số miền con cho những **DNS Server** khác quản lý. Những miền và miền con mà **DNS Server** được quyền quản lý gọi là **zone**. Như vậy, một **Zone** có thể  gồm một miền, một hay nhiều miền con. Hình sau mô tả sự khác nhau giữa **zone** và **domain**.




Hình 1.7: **Zone** và **Domain**



Các loại **zone**:

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

- **Primary zone** : Cho phép đọc và ghi cơ sở dữ liệu.
- **Secondary zone** : Cho phép đọc bản sao cơ sở dữ liệu.
- **Stub zone** : chứa bản sao cơ sở dữ liệu của **zone** nào đó, nó chỉ chứa chỉ một vài **RR**.

## IV.2. Fully Qualified Domain Name (FQDN).

Mỗi nút trên cây có một tên gọi(không chứa dấu chấm) dài tối đa 63 ký tự. Tên rỗng dành riêng cho gốc (**root**) cao nhất và biểu diễn bởi dấu chấm. Một tên miền đầy đủ của một nút chính là chuỗi tuần tự các tên gọi của nút hiện tại đi ngược lên nút gốc, mỗi tên gọi cách nhau bởi dấu chấm. Tên miền có xuất hiện dấu chấm sau cùng được gọi là tên tuyệt đối (**absolute**) khác với tên tương đối là tên không kết thúc bằng dấu chấm. Tên tuyệt đối cũng được xem là tên miền đầy đủ đã được chứng nhận (**Fully Qualified Domain Name – FQDN**).

## IV.3. Sự ủy quyền(Delegation).

Một trong các mục tiêu khi thiết kế hệ thống **DNS** là khả năng quản lý phân tán thông qua cơ chế uỷ quyền (**delegation**). Trong một miền có thể tổ chức thành nhiều miền con, mỗi miền con có thể được uỷ quyền cho một tổ chức khác và tổ chức đó chịu trách nhiệm duy trì thông tin trong miền con này. Khi đó, miền cha chỉ cần một con trỏ trỏ đến miền con này để tham chiếu khi có các truy vấn.

Không phải một miền luôn luôn tổ chức miền con và uỷ quyền toàn bộ cho các miền con này, có thể chỉ có vài miền con được ủy quyền. Ví dụ miền **hcmuns.edu.vn** của Trường ĐHKHTN chia một số miền con như **csc.hcmuns.edu.vn** (Trung Tâm Tin Học), **fit.hcmuns.edu.vn** (Khoa CNTT) hay math.hcmuns.edu.vn (Khoa Toán), nhưng các máy chủ phục vụ cho toàn trường thì vẫn thuộc vào miền **hcmuns.edu.vn.**

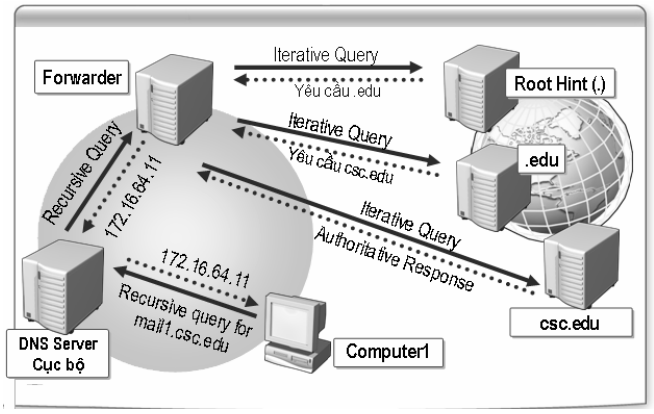
## IV.4. Forwarders.

Là kỹ thuật cho phép **Name Server** nội bộ chuyển yêu cầu truy vấn cho các **Name Server** khác để phân giải các miền bên ngoài.

Ví dụ: Trong Hình 1.8, ta thấy khi **Internal DNS Servers** nhận yêu cầu truy vấn của máy trạm nó kiểm tra xem có thể phân giải được yêu cầu này hay không, nếu không thì nó sẽ chuyển yêu cầu này lên **Forwarder DNS server** (**multihomed**) để nhờ **name server** này phân giải dùm, sau khi xem xét xong thì **Forwarder DNS server** (**multihomed**) sẽ trả lời yêu cầu này cho **Internal DNS Servers** hoặc nó sẽ tiếp tục **forward** lên các **name server** ngoài **Internet**.



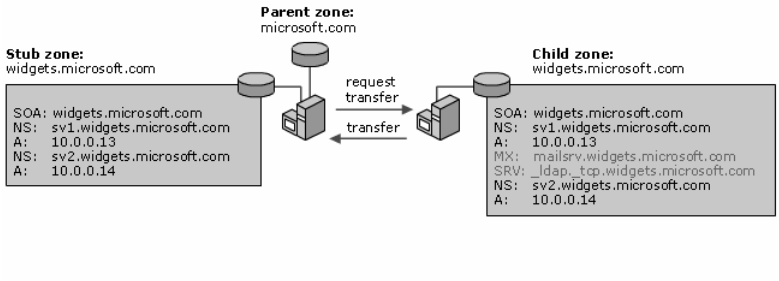
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 1.8: **Forward DNS queries**.

## IV.5. Stub zone.

Là **zone** chứa bảng sao cơ sở dữ liệu **DNS** từ **master name server**, **Stub zone** chỉ chứa các **resource record** cần thiết như : **A**, **SOA**, **NS**, một hoặc vài địa chỉ của **master name server** hỗ trợ cơ chế cập nhật **Stub zone**, chế chứng thực **name server** trong **zone** và cung cấp cơ chế phân giải tên miền được hiệu quả hơn, đơn giản hóa công tác quản trị (Tham khảo Hình 1.9).




Hình 1.9: **Stub zone**.

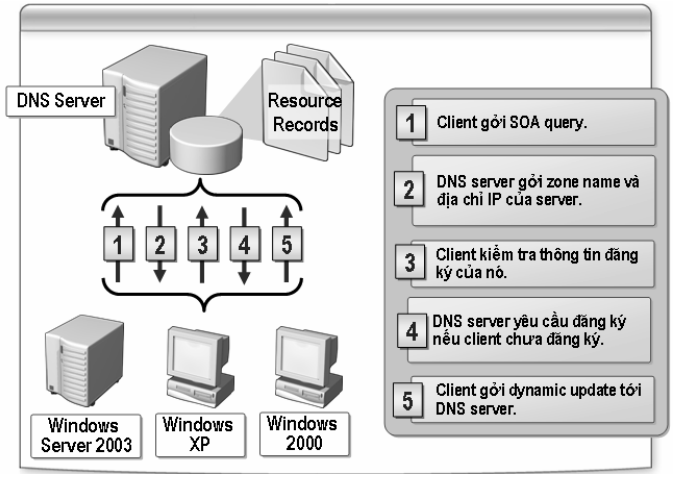
## IV.6. Dynamic DNS.

**Dynamic DNS** là phương thức ánh xạ tên miền tới địa chỉ **IP** có tần xuất thay đổi cao. Dịch vụ **DNS** động (**Dynamic DNS**) cung cấp một chương trình đặc biệt chạy trên máy tính của người sử dụng dịch vụ **dynamic DNS** gọi là **Dynamic Dns Client**. Chương trình này giám sát sự thay đổi địa chỉ **IP** tại **host** và liên hệ với hệ thống **DNS** mỗi khi địa chỉ **IP** của **host** thay đổi và sau đó **update** thông tin vào cơ sở dữ liệu **DNS** về sự thay đổi địa chỉ đó.

**DNS Client** đăng ký và cập nhật **resource record** của nó bằng cách gởi **dynamic update**.

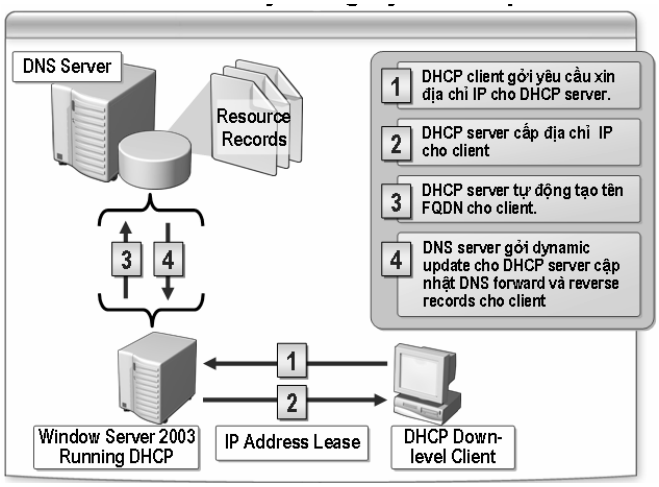


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 1.10: **Dynamic update**.

Các bước **DHCP Server** đăng ký và cập nhật **resource record** cho **Client**.




Hình 1.11: DHCP server cập nhật dynamic update.

## IV.7. Active Directory-integrated zone.

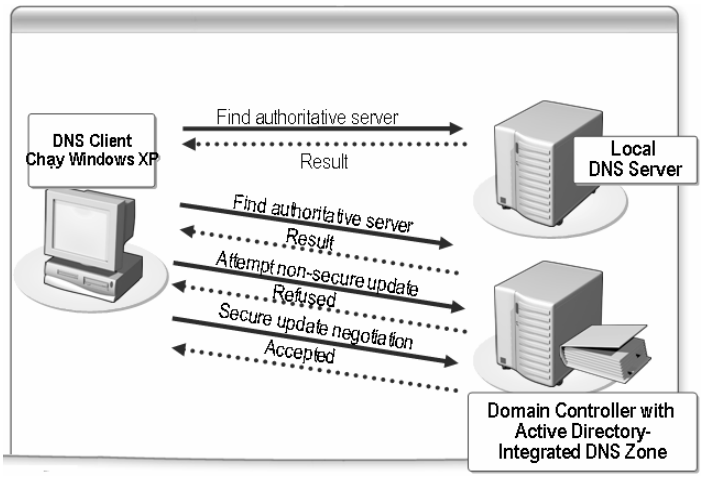
Sử dụng **Active Directory-integrated zone** có một số thuận lợi sau:

- **DNS zone** lưu trữ trong trong **Active Directory**, nhờ cơ chế này mà dữ liệu được bảo mật hơn.
- Sử dụng cơ chế nhân bản của **Active Directory** để cập nhận và sao chép cơ sở dữ liệu **DNS**.
- Sử dụng **secure dynamic update**.
- Sử dụng nhiều **master name server** để quản lý tên miền thay vì sử dụng một **master name server**.

Mô hình **Active Directory-integrated zone** sử dụng **secure dynamic update**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 1.12: Secure dynamic update

# V. Phân loại Domain Name Server.

Có nhiều loại **Domain Name Server** được tổ chức trên Internet. Sự phân loại này tùy thuộc vào nhiệm vụ mà chúng sẽ đảm nhận. Tiếp theo sau đây mô tả những loại **Domain Name Server**.

## V.1. Primary Name Server.

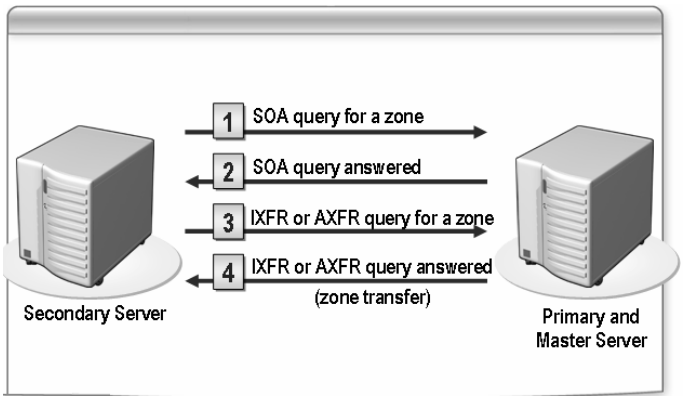
Mỗi miền phải có một **Primary Name Server**. **Server** này được đăng kí trên **Internet** để quản lý miền. Mọi người trên **Internet** đều biết tên máy tình và địa chỉ **IP** của **Server** này. Người quản trị **DNS** sẽ tổ chức những tập tin CSDL trên **Primary Name Server**. **Server** này có nhiệm vụ phân giải tất cả các máy trong miền hay **zone**.

## V.2. Secondary Name Server.

Mỗi miền có một **Primary Name Server** để quản lý CSDL của miền. Nếu như **Server** này tạm ngưng hoạt động vì một lý do nào đó thì việc phân giải tên máy tính thành địa chỉ **IP** và ngược lại xem như bị gián đoạn. Việc gián đoạn này làm ảnh hưởng rất lớn đến những tổ chức có nhu cầu trao đổi thông tin ra ngoài **Internet** cao. Nhằm khắc phục nhược điểm này, những nhà thiết kế đã đưa ra một **Server** dự phòng gọi là **Secondary**(hay **Slave**) **Name Server**. **Server** này có nhiệm vụ sao lưu tất cả những dữ liệu trên **Primary Name Server** và khi **Primary Name Server** bị gián đoạn thì nó sẽ đảm nhận việc phân giải tên máy tính thành địa chỉ **IP** và ngược lại. Trong một miền có thể có một hay nhiều **Secondary Name Server**. Theo một chu kỳ, **Secondary** sẽ sao chép và cập nhật CSDL từ **Primary Name Server**. Tên và địa chỉ **IP** của **Secondary Name Server** cũng được mọi người trên **Internet** biết đến.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

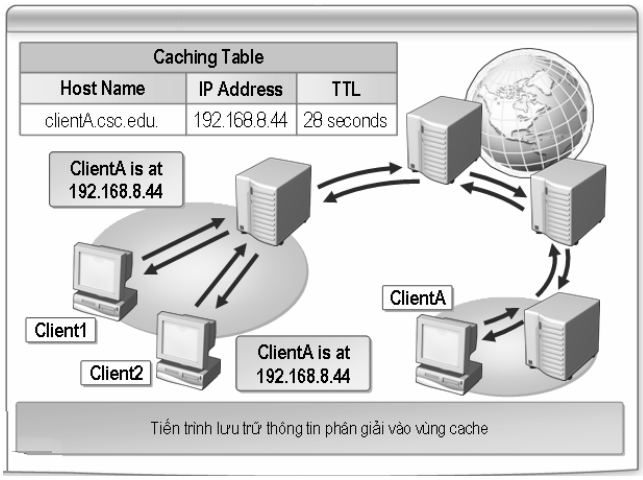



Hình 1.13: Zone tranfser

## V.3. Caching Name Server.

**Caching Name Server** không có bất kỳ tập tin CSDL nào. Nó có chức năng phân giải tên máy trên những mạng ở xa thông qua những **Name Server** khác. Nó lưu giữ lại những tên máy đã được phân giải trước đó và được sử dụng lại những thông tin này nhằm mục đích:

- Làm tăng tốc độ phân giải bằng cách sử dụng **cache**.
- Giảm bớt gánh nặng phân giải tên máy cho các **Name Server**.
- Giảm việc lưu thông trên những mạng lớn.



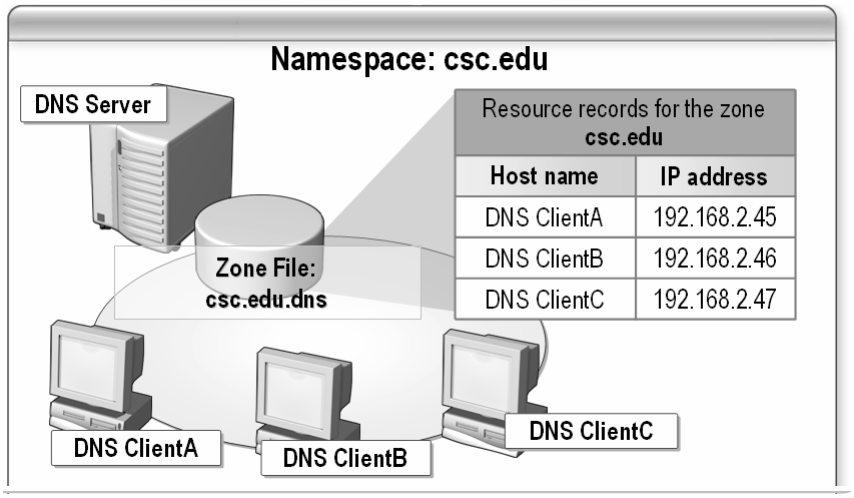

Hình .1.14: Bảng cache

# VI. Resource Record (RR).

**RR** là mẫu thông tin dùng để mô tả các thông tin về cơ sở dữ liệu **DNS**, các mẫu tin này được lưu trong các file cơ sở dữ liệu **DNS** (**\systemroot\system32\dns**).



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 1.15: cơ sở dữ liệu

## VI.1. SOA(Start of Authority).

Trong mỗi tập tin CSDL phải có một và chỉ một **record SOA** (**start of authority**). **Record SOA** chỉ ra rằng máy chủ **Name Server** là nơi cung cấp thông tin tin cậy từ dữ liệu có trong **zone**. Cú pháp của **record SOA**.

[tên-miền] IN SOA [tên-server-dns] [địa-chỉ-email] (

serial number;

refresh number;

retry number;

experi number;

Time-to-live number)

- **Serial :** Áp dụng cho mọi dữ liệu trong zone và là 1 số nguyên. Trong ví dụ, giá trị này bắt đầu từ 1 nhưng thông thường người ta sử dụng theo định dạng thời gian như 1997102301. Định dạng này theo kiểu YYYYMMDDNN, trong đó YYYY là năm, MM là tháng, DD là ngày và NN số lần sửa đổi dữ liệu **zone** trong ngày. Bất kể là theo định dạng nào, luôn luôn phải tăng số này lên mỗi lần sửa đổi dữ liệu **zone**. Khi máy máy chủ **Secondary** liên lạc với máy chủ **Primary**, trước tiên nó sẽ hỏi số **serial**. Nếu số **serial** của máy **Secondary** nhỏ hơn số serial của máy **Primary** tức là dữ liệu **zone** trên **Secondary** đã cũ và sau đó máy **Secondary** sẽ sao chép dữ liệu mới từ máy **Primary** thay cho dữ liệu đang có hiện hành.
- **Refresh:** Chỉ ra khoảng thời gian máy chủ **Secondary** kiểm tra dữ liệu **zone** trên máy **Primary** để cập nhật nếu cần. Trong ví dụ trên thì cứ mỗi 3 giờ máy chủ **Secondary** sẽ liên lạc với máy chủ **Primary** để cập nhật dữ liệu nếu có. Giá trị này thay đổi tuỳ theo tần suất thay đổi dữ liệu trong zone.
- **Retry:** nếu máy chủ **Secondary** không kết nối được với máy chủ **Primary** theo thời hạn mô tả trong **refresh** (ví dụ máy chủ **Primary** bị **shutdown** vào lúc đó thì máy chủ **Secondary** phải tìm cách kết nối lại với máy chủ **Primary** theo một chu kỳ thời gian mô tả trong **retry**. Thông thường giá trị này nhỏ hơn giá trị **refresh**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

- **Expire:** Nếu sau khoảng thời gian này mà máy chủ **Secondary** không kết nối được với máy chủ **Primary** thì dữ liệu **zone** trên máy **Secondary** sẽ bị quá hạn. Một khi dữ liệu trên **Secondary** bị quá hạn thì máy chủ này sẽ không trả lời mọi truy vấn về **zone** này nữa. Giá trị **expire** này phải lớn hơn giá trị **refresh** và giá trị **retry**.
- **TTL:** Viết tắt của **time to live**. Giá trị này áp dụng cho mọi record trong **zone** và được đính kèm trong thông tin trả lời một truy vấn. Mục đích của nó là chỉ ra thời gian mà các máy chủ **Name Server** khác **cache** lại thông tin trả lời. Việc cache thông tin trả lời giúp giảm lưu lượng truy vấn **DNS** trên mạng.

## VI.2. NS (Name Server).

**Record** tiếp theo cần có trong **zone** là **NS** (**name server**) **record**. Mỗi **Name Server** cho **zone** sẽ có một **NS record**.

Cú pháp:

[domain_name] IN NS [DNS-Server_name]

Ví dụ 2: Record NS sau:

t3h.com. IN NS dnsserver.t3h.com.

t3h.com. IN NS server.t3h.com.

chỉ ra 2 name servers cho miền t3h.com

## VI.3. A (Address) và CNAME (Canonical Name).

**Record A** (**Address**) ánh xạ tên máy (**hostname**) vào địa chỉ **IP**. **Record CNAME** (**canonical name**) tạo tên bí danh **alias** trỏ vào một tên **canonical**. Tên **canonical** là tên **host** trong **record A** hoặc lại trỏ vào 1 tên **canonical** khác.

Cú pháp record A:

[tên-máy-tính] IN A [địa-chỉ-IP]

Ví dụ 1: record A trong tập tin db.t3h

server.t3h.com. IN A 172.29.14.1

diehard.t3h.com. IN A 172.29.14.4

// Multi-homed hosts

server.t3h.com. IN A 172.29.14.1

server.t3h.com. IN A 192.253.253.1

## VI.4. AAAA.

Ánh xạ tên máy (**hostname**) vào địa chỉ **IP version 6**

Cú pháp:

[tên-máy-tính] IN AAAA [địa-chỉ-IPv6]

Ví dụ:



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

```
Server    IN AAAA 1243:123:456:789:1:2:3:456ab
```



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

## VI.5. SRV.

Cung cấp cơ chế định vị dịch vụ, **Active Directory** sử dụng **Resource Record** này để xác định **domain controllers**, **global catalog servers**, **Lightweight Directory Access Protocol** (**LDAP**) **servers**.

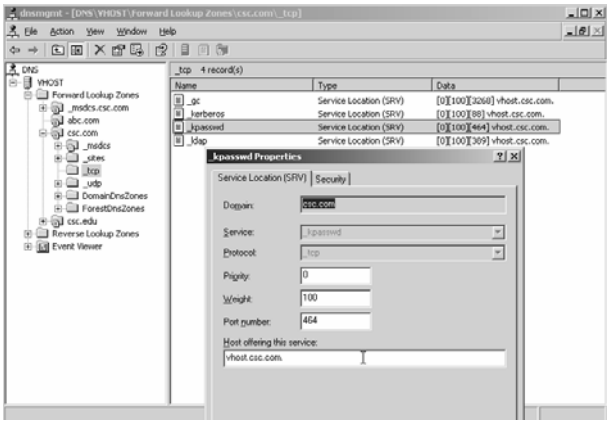
Các **field** trong **SVR**:

- Tên dịch vụ ***service.***
- Giao thức sử dụng.
- Tên miền (**domain name**).
- **TTL** và **class.**
- **Priority**.
- **Weight** (hỗ trợ **load balancing**).
- Port của dịch vụ.
- **Target** chỉ định **FQDN** cho **host** hỗ trợ dịch vụ.

Ví dụ:

_ftp._tcp.somecompany.com. IN SRV 0 0 21 ftpsvr1.somecompany.com.

_ftp._tcp.somecompany.com. IN SRV 10 0 21 ftpsvr2.somecompany.com.(Tham khảo hình 1.16)




Hình 1.16: Thông tin về RR SRV

## VI.6. MX (Mail Exchange).

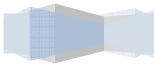
**DNS** dùng **record MX** trong việc chuyển **mail** trên mạng **Internet**. Ban đầu chức năng chuyển **mail** dựa trên 2 **record**: **record MD** (**mail destination**) và **record MF** (**mail forwarder**) **records**. **MD** chỉ ra đích cuối cùng của một thông điệp **mail** có tên miền cụ thể. **MF** chỉ ra máy chủ trung gian sẽ chuyển tiếp **mail** đến được máy chủ đích cuối cùng. Tuy nhiên, việc tổ chức này hoạt động không tốt. Do đó, chúng được tích hợp lại thành một **record** là **MX**. Khi nhận được mail, trình chuyển **mail** (**mailer**) sẽ dựa vào **record MX** để quyết định đường đi của mail. **Record MX** chỉ ra một mail **exchanger** cho một miền - **mail exchanger** là một máy chủ xử lý (chuyển **mail** đến **mailbox** cục bộ hay làm **gateway** chuyển sang một giao thức chuyển **mail** khác như **UUCP**) hoặc chuyển tiếp **mail** đến một **mail exchanger** khác (trung gian) gần với mình nhất để đến tới máy chủ đích cuối cùng hơn dùng giao thức



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

**SMTP** (**Simple Mail Transfer Protocol**).





Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Để tránh việc gửi **mail** bị lặp lại, **record MX** có thêm 1 giá trị bổ sung ngoài tên miền của **mail exchanger** là 1 số thứ tự tham chiếu. Đây là giá trị nguyên không dấu 16-bit (0-65535) chỉ ra thứ tự ưu tiên của các **mail exchanger**.

Cú pháp **record MX**:

[domain_name] IN MX [priority] [mail-host]

Ví dụ record MX sau :

t3h.com. IN MX 10 mailserver.t3h.com.

Chỉ ra máy chủ **mailserver.t3h.com** là một **mail exchanger** cho miền **t3h.com** với số thứ tự tham chiếu 10.

**Chú ý:** các giá trị này chỉ có ý nghĩa so sánh với nhau. Ví dụ khai báo 2 record MX:

t3h.com. IN MX 1 listo.t3h.com.

t3h.com. IN MX 2 hep.t3h.com.

Trình chuyển thư **mailer** sẽ thử phân phát thư đến **mail exchanger** có số thứ tự tham chiếu nhỏ nhất trước. Nếu không chuyển thư được thì **mail exchanger** với giá trị kế sau sẽ được chọn. Trong trường hợp có nhiều **mail exchanger** có cùng số tham chiếu thì **mailer** sẽ chọn ngẫu nhiên giữa chúng.

## VI.7. PTR (Pointer).

**Record PTR** (**pointer**) dùng để ánh xạ địa chỉ **IP** thành **Hostname**.

Cú pháp:

[Host-ID.{Reverse_Lookup_Zone}] IN PTR [tên-máy-tính]

Ví dụ:

Các **record PTR** cho các host trong mạng 192.249.249:

1.**14.29.172.in-addr.arpa.** IN PTR server.t3h.com.

# VII. Cài đặt và cấu hình dịch vụ DNS.

Có nhiều cách cài đặt dịch vụ **DNS** trên môi trường **Windows** như: Ta có thể cài đặt **DNS** khi ta nâng cấp máy chủ lên **domain controllers** hoặc cài đặt **DNS** trên máy **stand-alone Windows 2003 Server** từ tùy chọn **Networking services** trong thành phần **Add/Remove Program**.

## VII.1. Các bước cài đặt dịch vụ DNS.

Khi cài đặt dịch vụ **DNS** trên **Windows 2003 Server** đòi hỏi máy này phải được cung cấp địa chỉ **IP** tĩnh, sau đây là một số bước cơ bản nhất để cài đặt dịch vụ **DNS** trên **Windows 2003 stand-alone Server.**

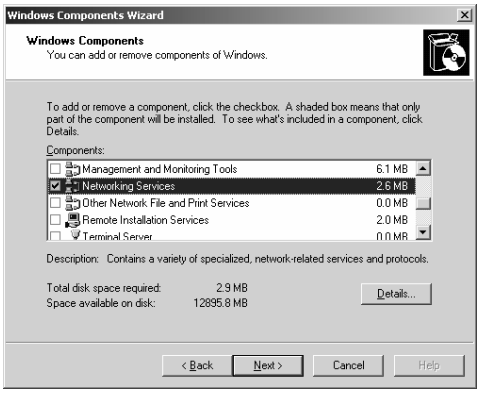
Chọn **Start** | **Control Panel** | **Add/Remove Programs.**

Chọn **Add or Remove Windows Components** trong hộp thoại **Windows components.**

Từ hộp thoại ở bước 2 ta chọn **Network Services** sau đó chọn nút **Details** (Tham khảo hình 1.17)

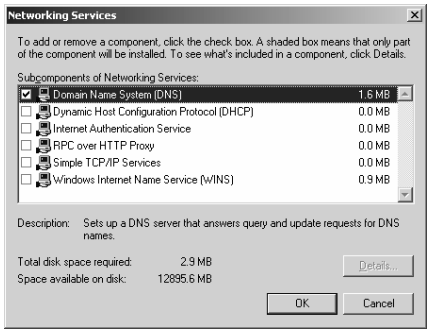


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 1.17: Thêm các dịch vụ mạng trong **Windows**.

Chọn tùy chọn **Domain Name System**(**DNS**), sau đó chọn nút **OK**(Tham khảo hình 1.18)




Hình 1.18: Thêm dịch vụ DNS

Chọn **Next** sau đó hệ thống sẽ chép các tập tin cần thiết để cài đặt dịch vụ (bạn phải đảm bảo có đĩa **CDROM Windows 2003** trên máy cục bộ hoặc có thể truy xuất tài nguyên này từ mạng).

Chọn nút **Finish** để hoàn tất quá trình cài đặt.

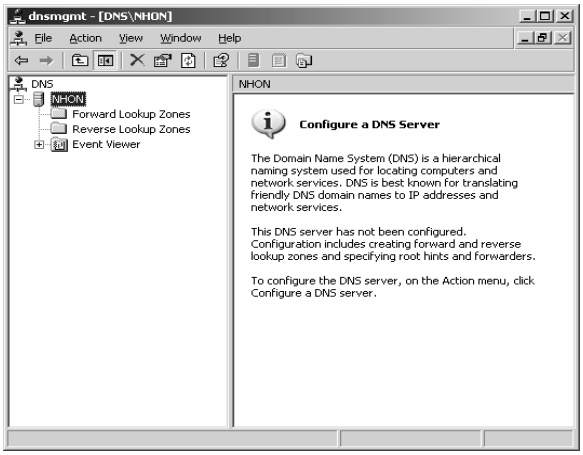
## VII.2. Cấu hình dịch vụ DNS

Sau khi ta cài đặt thành công dịch vụ **DNS**, ta có thể tham khảo trình quản lý dịch vụ này như sau:

Ta chọn **Start** | **Programs** | **Administrative Tools** | **DNS**. Nếu ta không cài **DNS** cùng với quá trình cài đặt **Active Directory** thì không có **zone** nào được cấu hình mặc định. Một số thành phần cần tham khảo trong **DNS Console** (Tham khảo hình 1.19)



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 1.19: DNS console

- **Event Viewer**: Đây trình theo dõi sự kiện nhật ký dịch vụ **DNS**, nó sẽ lưu trữ các thông tin về: cảnh giác (**alert**), cảnh báo (**warnings**), lỗi (**errors**).
- **Forward Lookup Zones**: Chứa tất cả các **zone** thuận của dịch vụ **DNS**, **zone** này được lưu tại máy **DNS Server**.
- **Reverse Lookup Zones**: Chứa tất cả các **zone** nghịch của dịch vụ **DNS**, **zone** này được lưu tại máy **DNS Server**.

### VII.2.1 Tạo Forward Lookup Zones.

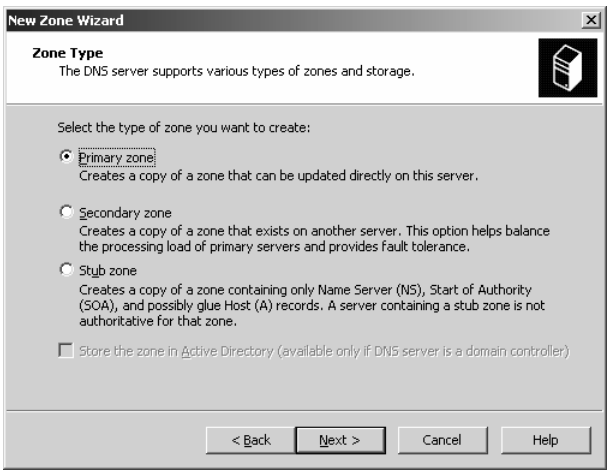
**Forward Lookup Zone** để phân giải địa chỉ Tên máy (**hostname**) thành địa chỉ **IP**. Để tạo **zone** này ta thực hiện các bước sau:

Chọn nút **Start** | **Administrative Tools** | **DNS**.

Chọn tên **DNS server**, sau đó Click chuột phải chọn **New Zone**.

Chọn **Next** trên hộp thoại **Welcome to New Zone Wizard**.

Chọn **Zone Type** là **Primary Zone** | **Next**.




Hình 1.20: Hộp thoại Zone Type



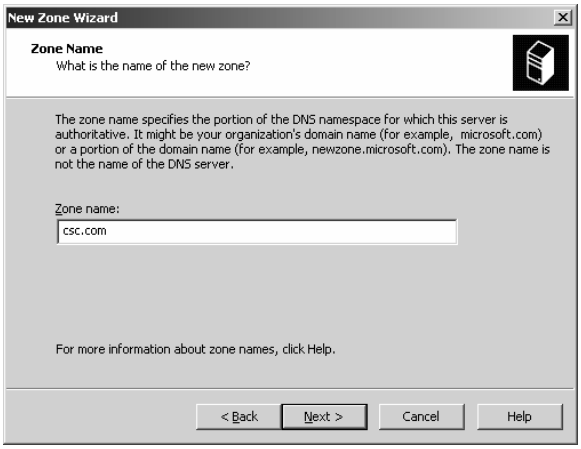
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Chọn **Forward Lookup Zone** | **Next**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

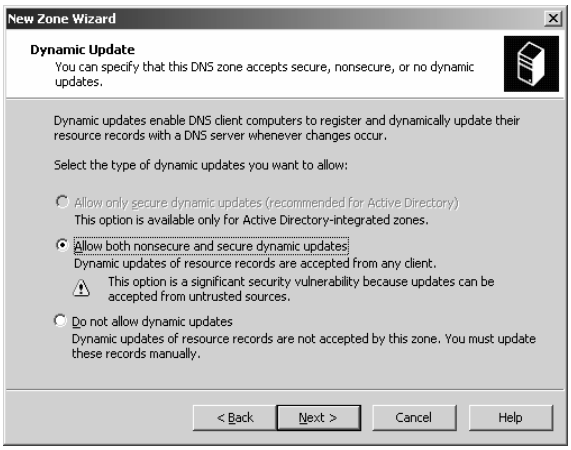
Chỉ định **Zone Name** để khai báo tên **Zone** (Ví dụ: csc.com), chọn **Next**.




Hình 1.21: Chỉ định tên zone

Từ hộp thoại **Zone File**, ta có thể tạo file lưu trữ cơ sở dữ liệu cho **Zone**(**zonename.dns**) hay ta có thể chỉ định **Zone File** đã tồn tại sẵn (tất cả các file này được lưu trữ tại **%systemroot%\system32\dns**), tiếp tục chọn **Next**.

Hộp thoại **Dynamic Update** để chỉ định **zone** chấp nhận **Secure Update**, **nonsecure Update** hay chọn không sử dụng **Dynamic Update**, chọn **Next**.




Hình 1.22: Chỉ định **Dynamic Update**.

Chọn **Finish** để hoàn tất.

### VII.2.2 Tạo Reverse Lookup Zone.

Sau khi ta hoàn tất quá trình tạo **Zone** thuận ta sẽ tạo **Zone** nghịch (**Reverse Lookup Zone**) để hỗ trợ cơ chế phân giải địa chỉ **IP** thành tên máy(**hostname**).



Để tạo **Reverse Lookup Zone** ta thực hiện trình tự các bước sau:

Chọn **Start** | **Programs** | **Administrative Tools** | **DNS**.

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Chọn tên của **DNS server**, Click chuột phải chọn **New Zone**.



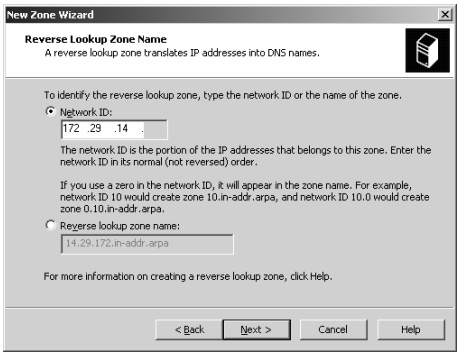
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Chọn **Next** trên hộp thoại **Welcome to New Zone Wizard**.

Chọn **Zone Type** là **Primary Zone** | **Next**.

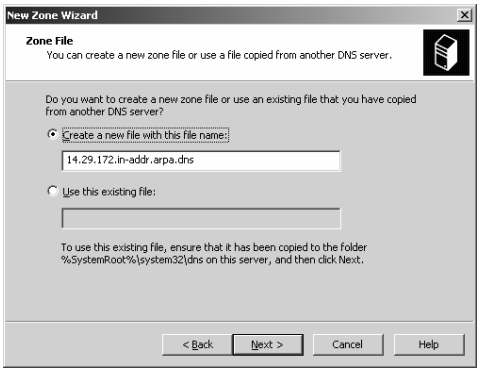
Chọn **Reverse Lookup Zone** | **Next**.

Gõ phần địa chỉ mạng(**NetID**) của địa chỉ **IP** trên **Name Server** | **Next**.




Hình 1.23: Chỉ định **zone** ngược.

Tạo mới hay sử dụng tập tin lưu trữ cơ sở dữ liệu cho **zone** ngược, sau đó chọn **Next**.




Hình 1.24: Chỉ định zone file.

Hộp thoại **Dynamic Update** để chỉ định **zone** chấp nhận **Secure Update**, **nonsecure Update** hay chọn không sử dụng **Dynamic Update**, chọn **Next**.

Chọn **Finish** để hoàn tất.

### VII.2.3 Tạo Resource Record(RR).

Sau khi ta tạo **zone** thuận và **zone** nghịch, mặc định hệ thống sẽ tạo ra hai **resource record NS** và **SOA**.

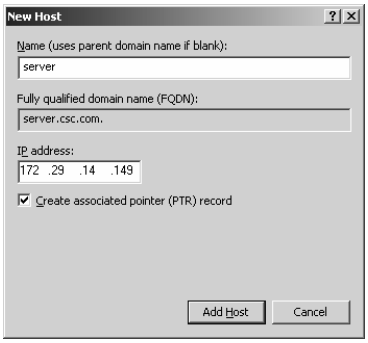
Tạo **RR A**.

Để tạo **RR A** để ánh xạ **hostname** thành tên máy, để làm việc này ta Click chuột **Forward Lookup Zone**, sau đó Click chuột phải vào tên **Zone | New Host** (tham khảo hình 1), sau đó ta cung cấp một số thông tin về **Name**, **Ip address,** sau đó chọn **Add Host.**



Chọn **Create associated pointer (PTR) record** để tạo **RR PTR** trong **zone** nghịch (trong ví dụ Hình 1.25 ta tạo **hostname** là **server** có địa chỉ **IP** là 172.29.14.149).

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

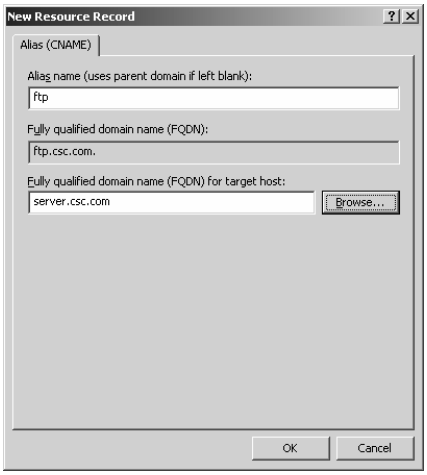



Hình 1.25: Tạo **Resource record A**.

Tạo **RR CNAME**.

Trong trường hợp ta muốn máy chủ **DNS Server** vừa có tên **server.csc.com** vừa có tên **ftp.csc.com** để phản ánh đúng chức năng là một **DNS Server**, **FTP server**,…Để tạo **RR Alias** ta thực hiện như sau:

- Click chuột **Forward Lookup Zone**, sau đó Click chuột phải vào tên **Zone | New Alias (CNAME)** (tham khảo Hình 1.26), sau đó ta cung cấp một số thông tin về:
- **Alias Name**: Chỉ định tên **Alias** (ví dụ ftp).
- **Full qualified domain name(FQDN) for target host:** chỉ định tên **host** muốn tạo **Alias**(ta có thể gõ tên **host** vào mục này hoặc ta chọn nút **Browse** sau đó chọn tên host).




Hình 1.26: Tạo RR CNAME

Tạo **RR MX** (**Mail Exchanger**).

Trong trường hợp ta tổ chức máy chủ **Mail** hỗ trợ việc cung cấp hệ thống thư điện tử cho miền cục bộ, ta phải chỉ định rõ địa chỉ của **Mail Server** cho tất cả các miền bên ngoài biết được địa chỉ này thông qua việc khai báo **RR MX**. Mục đích chính của **RR** này là giúp cho hệ thống bên ngoài có thể chuyển thư vào bên trong miền nội bộ. Để tạo **RR** này ta thực hiện như sau:

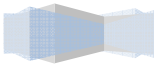


- Click chuột **Forward Lookup Zone**, sau đó Click chuột phải vào tên **Zone | New Mail Exchanger (MX) …** (tham khảo hình 3), sau đó ta cung cấp một số thông tin về:
- **Host or child domain:** Chỉ định tên máy hoặc địa chỉ miền con mà **Mail Server** quản lý, thông

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

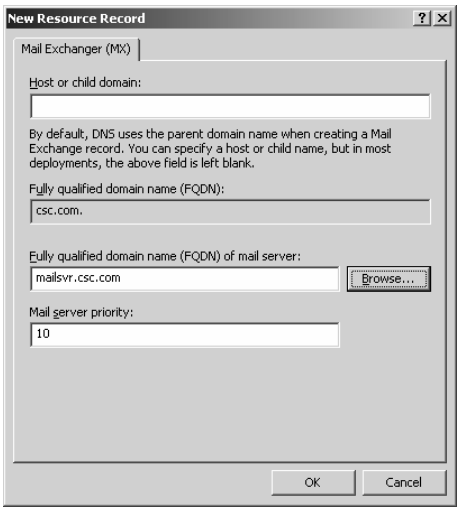
thường nếu ta tạo **MX** cho miền hiện tại thì ta không sử dụng thông số này.





Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

- **Full qualified domain name(FQDN) of mail server:** Chỉ định tên của máy chủ **Mail Server** quản lý mail cho miền nội bộ hoặc miền con.
- **Mail server priority:** Chỉ định độ ưu tiên của **Mail Server** (Chỉ định máy nào ưu tiên xử lý **mail** trước máy nào).
- Trong Hình 1.27 ta tạo một **RR MX** để khai báo máy chủ **mailsvr.csc.com** là máy chủ quản lý **mail** cho miền **csc.com**.




Hình 1.27: Tạo RR MX

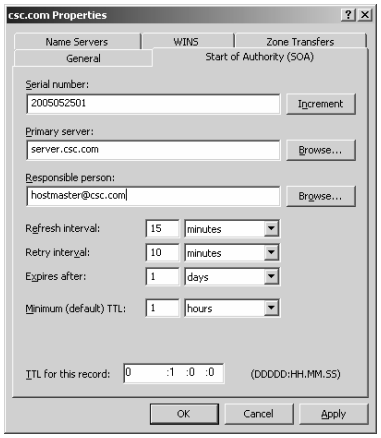
Thay đổi thông tin về **RR SOA** và **NS**.

Hai **RR NS** và **SOA** được tạo mặc định khi ta tạo mới một **Zone**, nếu như ta cài đặt **DNS** cùng với **Active Directory** thì ta thường không thay đổi thông tin về hai **RR** này, tuy nhiên khi ta cấu hình **DNS Server** trên **stand-alone server** thì ta phải thay đổi một số thông tin về hai **RR** này để đảm bảo tính đúng đắn, không bị lỗi. Để thay đổi thông tin này ta thực hiện như sau:

- Click chuột **Forward Lookup Zone**, sau đó Click vào tên **zone** sẽ hiển thị danh sách các **RR**, Click đôi vào **RR SOA** (tham khảo Hình 1.28).
- **Serial number:** Chỉ định chỉ số thay đổi thao cú pháp (năm_tháng_ngày_sốlầnthayđổitrongngày)
- **Primary server:** Chỉ định tên **FQDN** cho máy chủ **Name Server**(ta có thể click và nút **Browse…** để chỉ định tên của **Name Server** tồn tại sẵn trong **zone**).
- **Responsible person:** Chỉ định địa chỉ **email** của người quản trị hệ thống **DNS**.

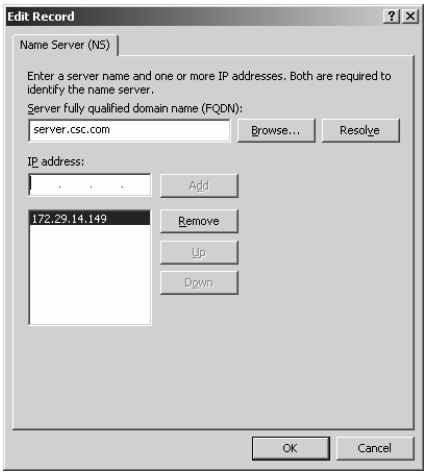


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 1.28: Thay đổi thông tin về RR SOA.

- Từ hộp thoại (ở Hình 1.28) ta chọn **Tab Name Servers | Edit** để thay đổi thông tin về **RR NS** (Tham khảo Hình 1.29).
- **Server Full qualified domain name(FQDN):** Chỉ định tên đầy đủ của **Name Server**, ta có thể chọn nút **Browser** để chọn tên của **Name Server** tồn tại trong **zone file**(khi đó ta không cần cung cấp thông tin về địa chỉ **IP** cho **server** này).
- **IP address:** Chỉ định địa chỉ **IP** của máy chủ **Name Server**, sau đó chọn nút **Add**.




Hình 1.29: Thay đổi thông tin về RR NS

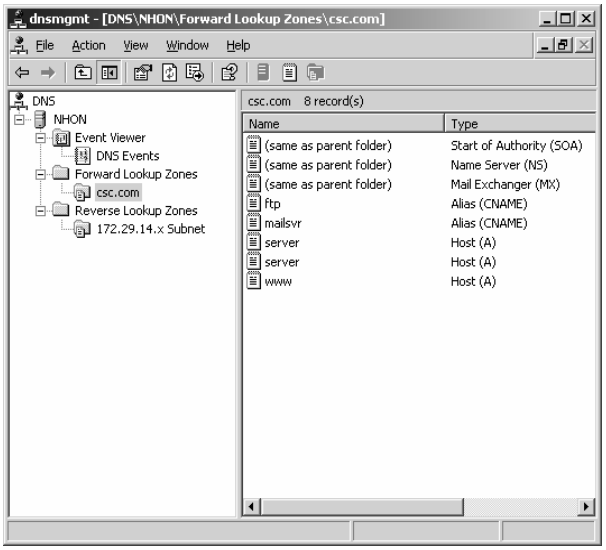
- Thay đổi thông tin về **RR SOA** và **NS** trong **zone** nghịch (**Reverse Lookup Zone**) ta thực hiện tương tự như ta đã làm trong **zone** nghịch.

### VII.2.4 Kiểm tra hoạt động dịch vụ DNS.

Sau khi ta hoàn tất quá trình tạo **zone** thuận, **zone** nghịch, và mô tả một số **RR** cần thiết (tham khảo Hình 1.30).



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

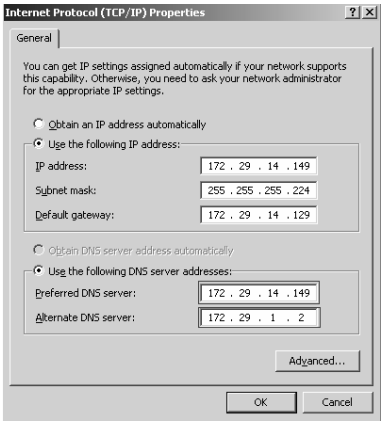



Hình 1.30: Một số cơ sở dữ liệu cơ bản của dịch vụ **DNS**.

Muốn kiểm tra quá trình hoạt động của dịch vụ **DNS** ta thực hiện các bước sau:

Khai báo **Resolver**:

- Để chỉ định rõ cho **DNS Client** biết địa chỉ máy chủ **DNS Server** hỗ trợ việc phân giải tên miền.
- Để thực hiện khai báo **Resolver** ta chọn **Start | Settings | Network Connections** | Chọn **Properties** của **Local Area Connection** | Chọn **Properties** của **Internet Control (TCP/IP)** (ta tham khảo Hình 1.31), sau đó chỉ định hai thông số .
- **Referenced DNS server**: Địa chỉ của máy chủ **Primary DNS Server**.
- **Alternate DNS server**: Địa chỉ của máy chủ **DNS** dự phòng hoặc máy chủ **DNS** thứ hai.



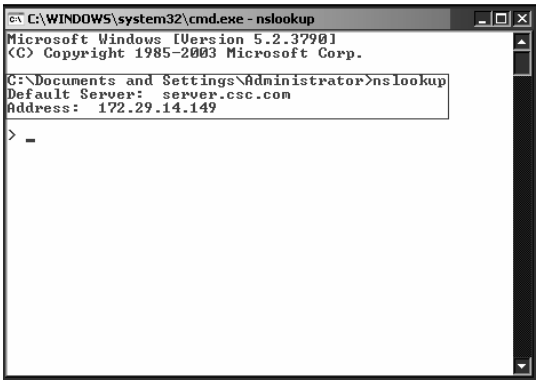

Hình 1.31: Khai báo Resolver cho máy trạm.

Kiểm tra hoạt động.

Ta có thể dùng công cụ **nslookup** để kiểm tra quá trình hoạt động của dịch vụ **DNS**, phân giải **resource record** hoặc phân giải tên miền. để sử dụng được công cụ **nslookup** ta vào **Start | Run | nslookup**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 1.32: Kiểm tra **DNS**.

Cần tìm hiểu một vài tập lệnh của công cụ **nslookup**.

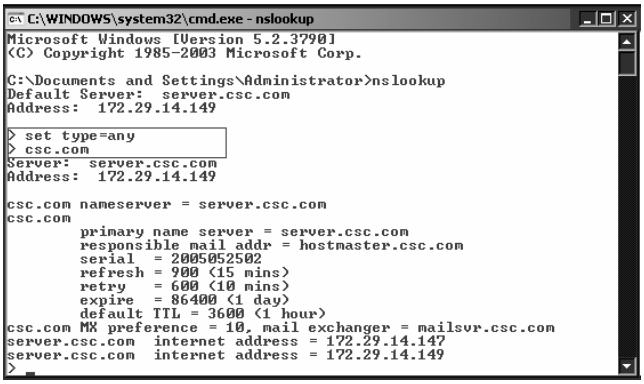
>set type=<RR_Type>

Trong đó <**RR_Type**> là loại **RR** mà ta muốn kiểm tra, sau đó gõ tên của **RR** hoặc tên miền cần kiểm tra

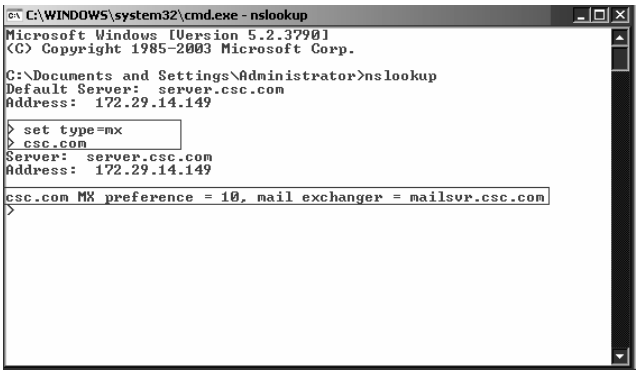
**>set type=any:** Để xem mọi thông tin về **RR** trong miền, sau đó ta gõ <**domain name**> để xem thông tin về các **RR** như **A**, **NS**, **SOA**, **MX** của miền này.



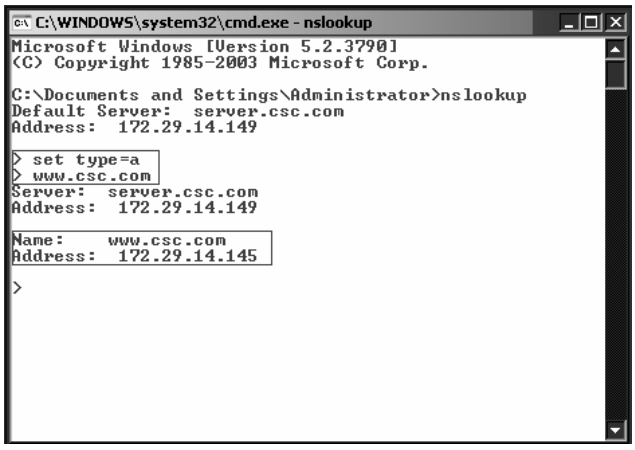
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 1.33: Ví dụ về **nslookup**.



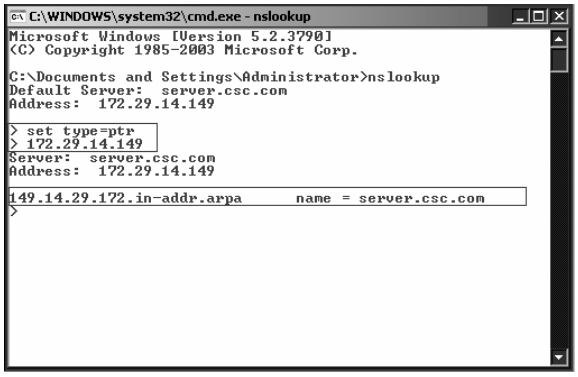

Hình 1.34: Xem **RR MX**.




Hình 1.35: Xem địa chỉ **IP** của một **hostname**.

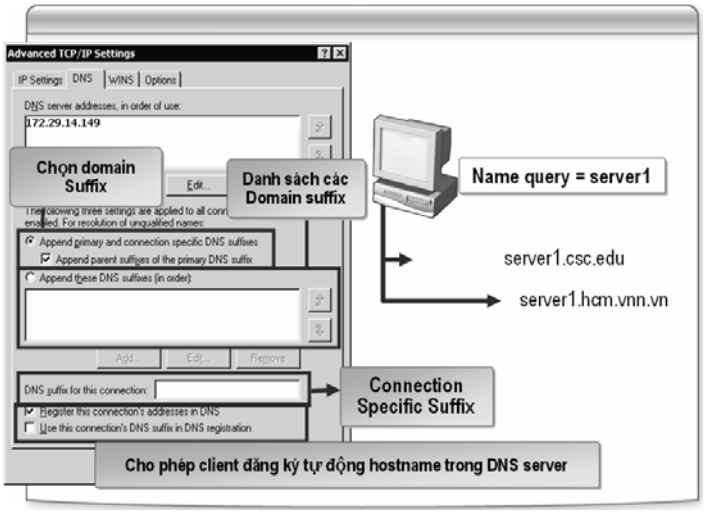


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 1.36: Kiểm tra phân giải ngược.

Một số thông số cấu hình cần thiết cho **DNS Client**:



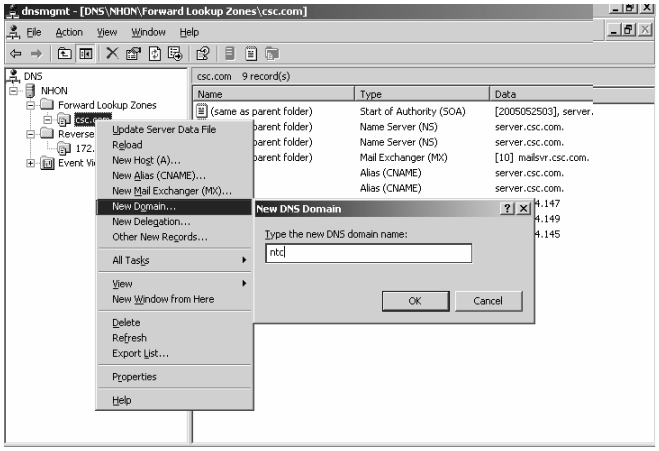

Hình 1.37: Một số thông tin cấu hình khác.

### VII.2.5 Tạo miền con(Subdomain).

Trong miền có thể có nhiều miền con, việc tạo miền con giúp cho người quản trị cung cấp tên miền cho các tổ chức, các bộ phận con trong miền của mình thông qua đó nó cho phép người quản trị có thể phân loại và tổ chức hệ thống dễ dàng hơn. Để tạo miền con ta chọn **Forward Lookup Zone**, sau đó ta click chuột phải vào tên **Zone** chọn **New Domain**…(tham khảo Hình 1.38)



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

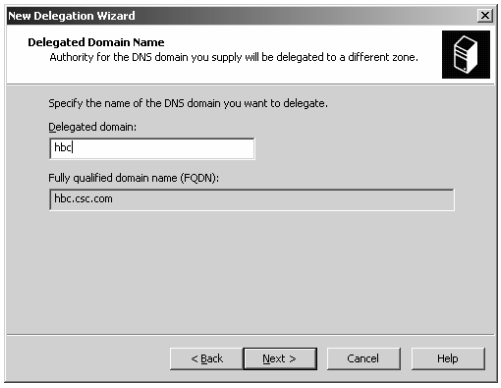



Hình 1.38: Tạo miền con.

### VII.2.6 Ủy quyền cho miền con.

Giả sử ta ủy quyền tên miền **subdomain hbc.csc.com** cho **server serverhbc** có địa chỉ 172.29.14.150 quản lý, ta thực hiện các thao tác sau:

- Tạo **resource record A** cho **serverhbc** trong miền **csc.com**(tham khảo trong phần tạo RR A).
- Chọn **Forward Lookup Zone**, sau đó Click chuột phải vào tên **Zone** chọn **New delegation… | Next** (tham khảo Hình 1.39),.

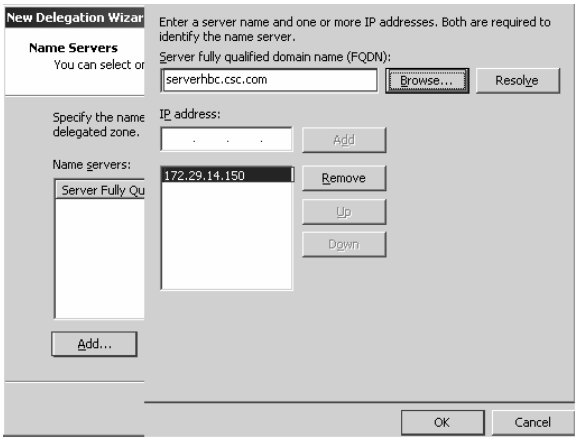



Hình 1.39: **delegation domain**.

- **Add Name Server** quản lý cơ cở dữ liệu cho miền con **hbc.csc.com** trong hộp thoại **Name Server** (tham khảo Hình 1.40).



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 1.40: **Add Name Server**.

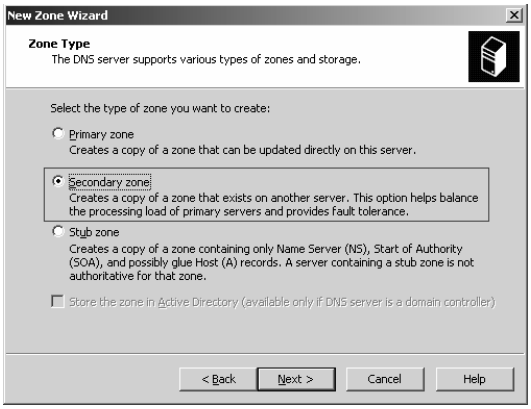
- Sau khi add xong **Name Server** ở bước trên ta chọn **Next | Finish** để hoàn tất.

### VII.2.7 Tạo Secondary Zone.

Thông thường trong một **domain** ta có thể tổ chức một **Primary Name Server**(**PNS**) và một **Secondary Name Server**(**SNS**), **SNS** đóng vai trò là máy dự phòng, nó lưu trữ bảng sao dữ liệu từ máy **PNS**, một khi **PNS** bị sự cố thì ta có thể sử dụng **SNS** thay cho máy **PNS**.

Sau đây ta sử dụng máy chủ **server1** có địa chỉ 172.29.14.151 làm máy chủ dự phòng (**SNS**) cho miền **csc.edu** từ **Server** chính (**PNS**) có địa chỉ 172.29.14.149.

- Click chuột phải vào tên **Name Server** trong giao diện **DNS management console** chọn **New Zone** | **Next** | **Secondary Zone** (tham khảo Hình 1.41)
- **Secondary Zone** : Khi ta muốn sao chép dự phòng cơ sở dữ liệu **DNS** từ **Name Server** khác, **SNS** hỗ trợ cơ chế chứng thực, cân bằng tải với máy **PNS**, cung cấp cơ chế dung lỗi tốt.
- **Stub Zone**: Khi ta muốn sao chép cơ sở dữ liệu chỉ từ **PNS**, **Stub Zone** sẽ chỉ chứa một số **RR** cần thiết như **NS**, **SOA**, **A** hỗ trợ cơ chế phân giải được hiệu quả hơn.




Hình 1.41: Tạo Secondary Zone



- Chọn **Forward Lookup Zone** nếu ta muốn tạo sao chép **Zone** thuận, chọn **Reverse Lookup Zone** nếu ta muốn sao chép **Zone** nghịch. Trong trường hợp này ta chọn **Forward Lookup Zone |**

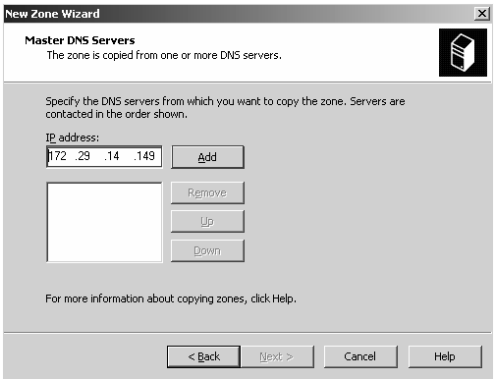
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

**Next**.



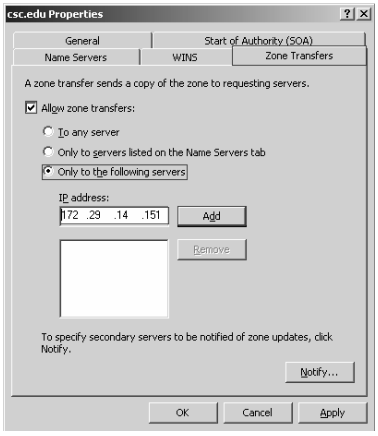
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

- Chỉ định **Zone Name** mà ta muốn sao chép (ví dụ **csc.edu**), tiếp theo ta chọn **Next**.
- Chỉ định địa chỉ của máy chủ **Master Name Server**(còn gọi là **Primary Name Server**), sao đó chọn **Add** | **Next** (tham khảo Hình 1.42).




Hình 1.42: Tạo Secondary Zone

- Chọn **Finish** để hoàn tất quá trình. ta kiểm tra xem trong **Zone** csc.edu mới tạo sẽ có cơ sở dữ liệu được sao chép từ **PNS**, ngược lại trong **zone csc.edu** không có cơ sở dữ liệu thì ta hiệu chỉ lại thông số **Zone Transfer** trên máy **Master Name Server** để cho phép máy **SNS** được sao chép cơ sở dữ liệu, ta thực hiện điều này bằng cách Click chuột phải vào **Zone csc.edu** trên máy **Master Name Server**, chọn **Properties** | chọn **Tab Zone Transfer** (Tham khảo Hình 1.43).

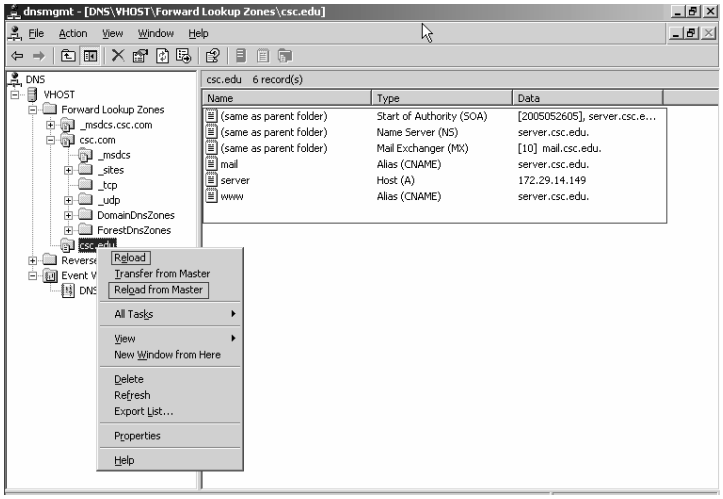



Hình 1.43: Allow Zone Transfer.

- Sau khi ta hiệu chỉ xong thông tin **Zone Transfer ta Reload** cơ sở dữ liệu từ máy **SNS** để cho máy **SNS** sao chép lại cơ sở dữ liệu từ **PNS** (Tham khảo hình 1.44)



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

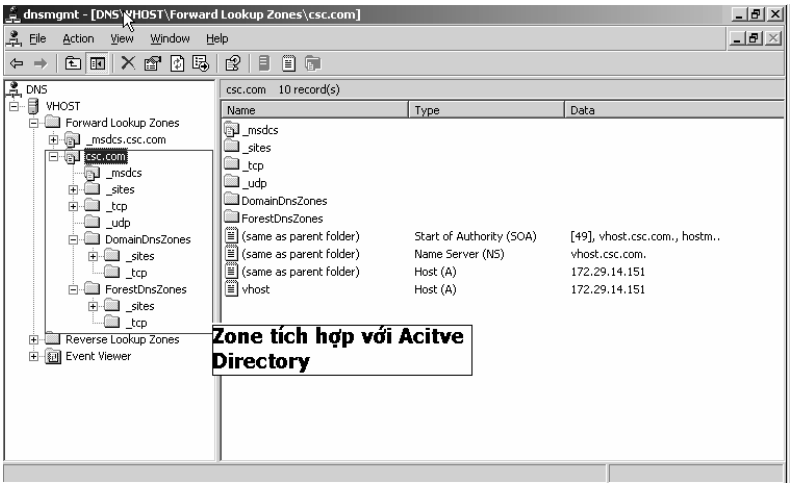



Hình 1.44: **Reload Secondary Zone**.

### VII.2.8 Tạo zone tích hợp với Active Directory.

Trong quá trình nâng cấp máy **Stand-Alone Server** thành **Domain Controller** bằng cách cài **Active Directory** ta có thể chọn cơ chế cho phép hệ thống tự động cài đặt và cấu hình dịch vụ **DNS** tích hợp chung với **Active Directory**, nếu ta chọn theo cách này thì sau khi quá trình nâng cấp hoàn tất, ta có thể tham khảo cơ sở dữ liệu của **DNS** tích hợp chung với **Active Directory** thông qua trình quản lý dịch vụ **DNS**(tham khảo Hình 1.45).

Trong Hình 1.45 này ta tham khảo cơ sở dữ liệu của **DNS** quản lý tên miền **csc.com** được tích hợp chung với **Active Directory**.




Hình 1.45: **Active Integrated zone**.

Tuy nhiên khi ta cho hệ thống tự động cấu hình cơ sở dữ liệu cho **zone** thì nó chỉ tạo một số cơ sở dữ liệu cần thiết ban đầu để nó thực hiện một số thao tác truy vấn và quản lý cơ sở dữ liệu cho **Active Directory**. Để cho **DNS** hoạt động tốt hơn thì ta mô tả thêm thông tin **resource record** cần thiết vào, điều cần thiết nhất là ta tạo **Reverse Lookup Zone** cho **Active Integrated Zone** vì ban đầu hệ thống không tạo ra **zone** này, mô tả thêm thông tin **record PTR** cho từng **resource record A** trong **Forward**



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

**Lookup Zone**.

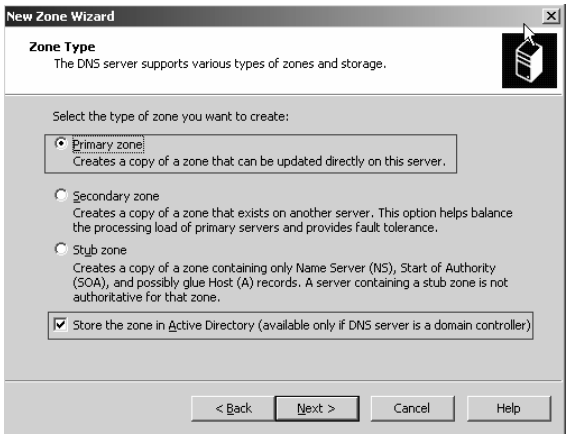


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Ta có thể tạo một **zone** mới tích hợp với **Active Directory** theo các bước sau:

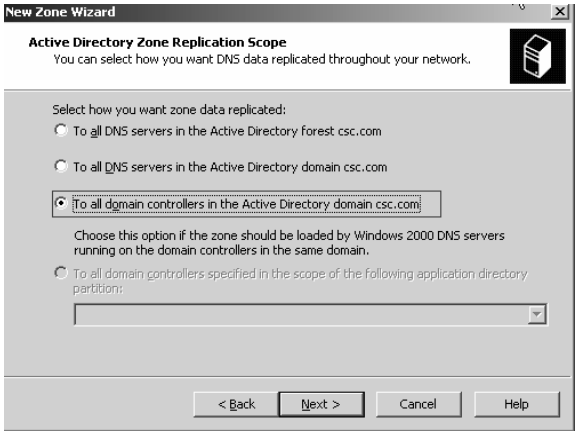
Bấm chuột phải vào tên **DNS Server** trong **DNS management console**, chọn **New Zone**…| chọn **Next**.

Trong hộp thoại **zone type** ta chọn **Primary Zone** với cơ chế lưu trữ zone trong **AD**(tham khảo hình 1.46), tiếp tục chọn **Next**.




Hình 1.46: Chọn zone type

Chọn cơ chế nhân bản dữ liệu tới tất cả các **Domain Controller** trong **Active Directory Zone** | **Next** (tham khảo Hình 1.47)




Hình 1.47: Nhân bản dữ liệu cho **zone**.

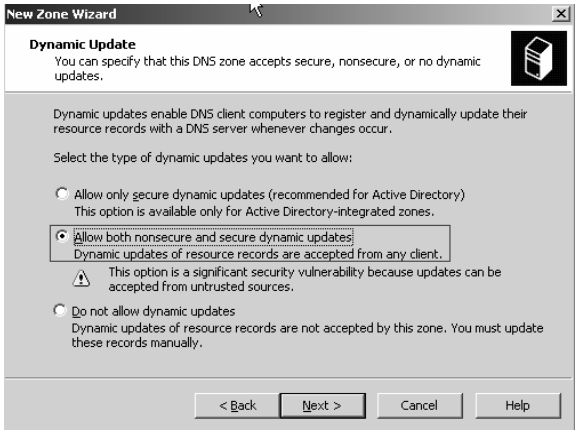
Chọn tạo **zone** thuận (**Forward Lookup Zone**) | **Next**.

Chỉ định tên **zone** (**Zone Name**) | **Next**.

Chỉ định **Dynamic Update** trong trường hợp ta muốn tạo **DDNS** cho **zone** này (tham khảo Hình 1.48), trong trường hợp này ta chọn **Allow both nonsecure and secure dynamic updates | Next**.

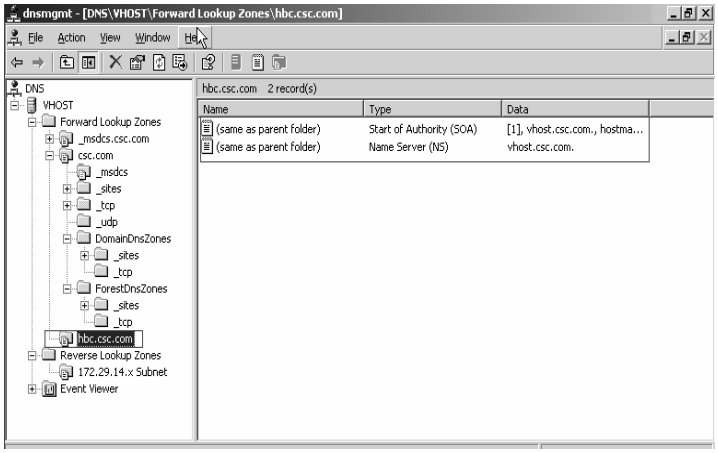


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 1.48: Dynamic update

Chọn **Finish** để hoàn tất quá trình, sau khi hoàn thành ta có thể mô tả **resource record** cho **zone** này, tạo thêm **Reverse Lookup Zone** trong trường hợp ta muốn hỗ trợ phân giải nghịch.




Hình 1.49: Cơ sở dữ liệu **zone**.

### VII.2.9 Thay đổi một số tùy chọn trên Name Server.

Trong phần này ta khảo sát một vài tùy chọn cần thiết để tạo hiệu chỉnh thông tin cấu hình cho **DNS**. Thông thường có ba phần chính trong việc thay đổi tùy chọn.

- Tùy chọn cho **Name Server**.
- Tùy chọn cho từng **zone name**.
- Tùy chọn cho từng **RR** trong **zone name**.

Tùy chọn cho **Name Server**.



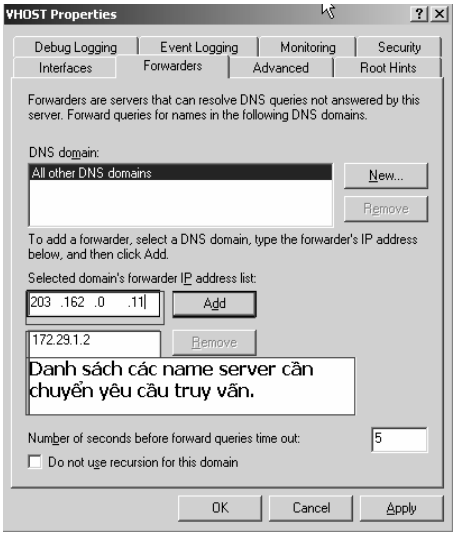
Cho phép thay đổi một số tùy chọn chính của **Name Server** bao gồm: Cấu hình **Forwarder**, Cấu hình **Root hints**, đặt một số tùy chọn cho phép theo dõi **log** (**Event Logging**), quản lý các truy vấn (**Monitoring query**), **debug logging**,... và một số hiệu chỉnh khác.

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Để sử dụng tùy chọn này ta chọn **Properties** của tên **server** trong **DNS management console** (tham khảo Hình 1.50).


Hình 1.50: **Name server properties**.

- **Cấu hình Forwader**: Chọn **Tab Forwarders** từ màn hình **properties** của **Name Server** (tham khảo hình 1.51).

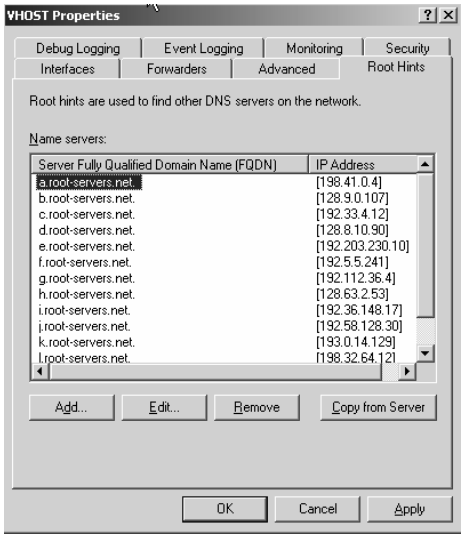



Hình 1.51: Cấu hình **Forwarder**.

- **Cấu hình Root hints:** Ta có thể tham khảo danh sách các **Root name server** quản lý các **Top-Level domain**, thông qua hộp thoại này ta có thể thêm, xóa, hiệu chỉnh địa chỉ của **Root hints**, thông thường các địa chỉ này hệ thống có thể tự nhận biết (tham khảo hình 1.52).

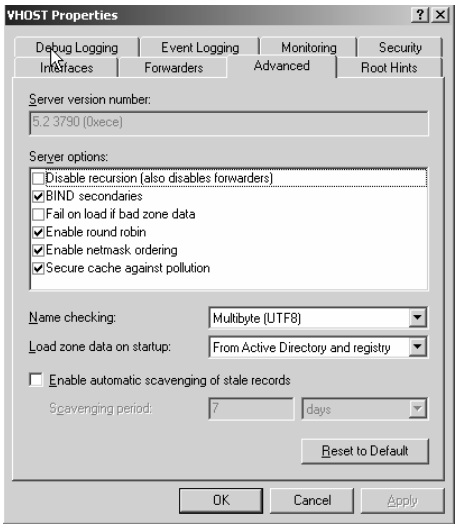


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 1.52: **Root Name Server**.

- Hiệu chỉnh một số thông số cấu hình nâng cao như (tham khảo Hình 1.53):
- **Disable recursion:** bỏ cơ chế truy vấn đệ qui, nếu ta chọn tùy chọn này thì **Forwarder** cũng bị **disable**.
- **BIND secondaries:** Cho phép **secondary** là **Name server** trên môi trường **Unix**.
- **Fail on load if bad zone data** : Nếu **zone data** bị lỗi thì không cho **name server load** dữ liệu.
- **Enable round robin**: Cho phép cơ chế luân chuyển giữa các **server** trong quá trình phân giải tên miền.
- **Enable netmask ordering**: Cho phép **client** dựa vào **local subnet** để nó lựa chọn **host** gần với **client** nhất (một khi **client** nhận được câu trả lời truy vấn ánh xạ một **hostname** có nhiều địa chỉ IP)
- **Secure cache agianst pollution**: Bảo mật vùng nhớ tạm lưu trữ các **RR** đã phân giải trước.




Hình 1.53: Tùy chọn nâng cao.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

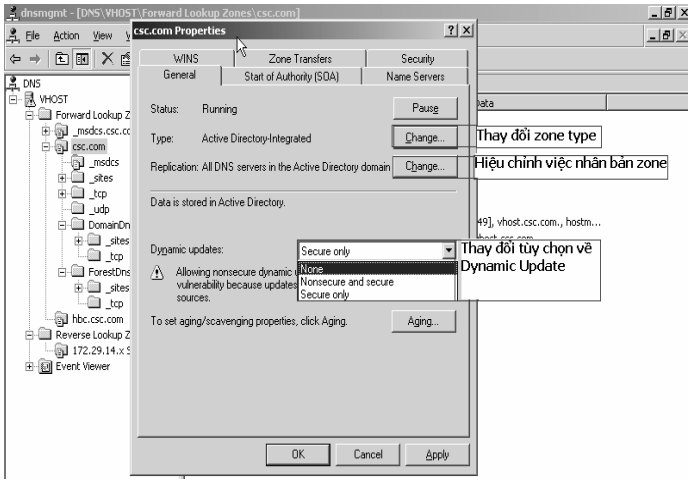
Tùy chọn cho từng **Zone**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

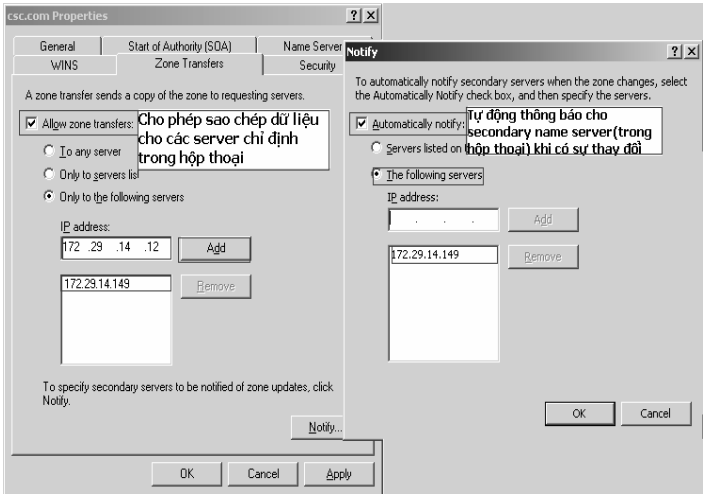
Để sử dụng tùy chọn này ta chọn **Properties** của tên **zone** trong **DNS management console**.

- Trong phần này ta có thể :
- Thay đổi **Zone Type**, cho phép **zone** hỗ trợ hay không hỗ trợ **Dynamic update** (**DDNS**) (tham khảo Hình 1.54)




Hình 1.54: Tùy chọn chung của **zone name**.

- Thay đổi thông tin **resource record SOA**, **NS** (ta có thể tham khảo trong phần cấu hình trước)
- Cho phép hay không cho phép sao chép dữ liệu **zone** giữa các **Name Server** (tham khảo hình 1.55).



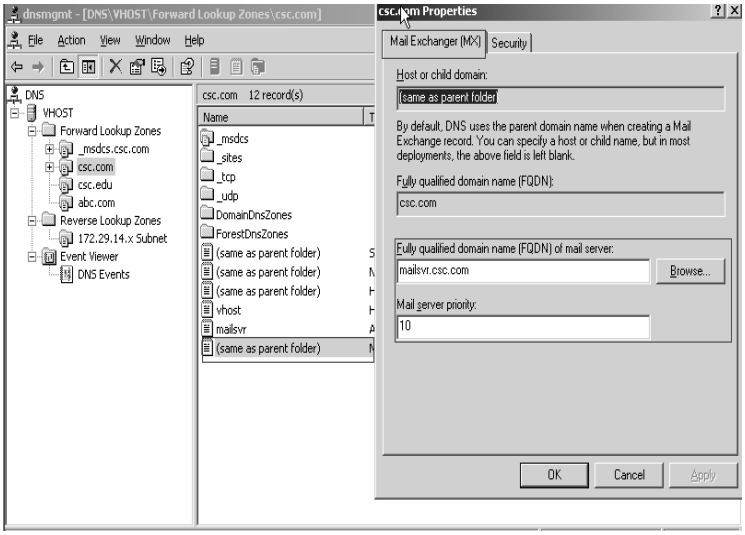

Hình 1.55: **Zone transfer**.

Tùy chọn cho từng **Resource Record**.

Thông qua tùy chọn này ta có thể thay đổi thông tin của từng **resource record** cho **zone name**, mỗi một **resource record** có thông tin khác nhau: để thực hiện điều này ta chỉ cần bấm đôi vào tên **resource record** tương ứng (tham khảo ví dụ trong Hình 1.56 về **RR MX**)



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net



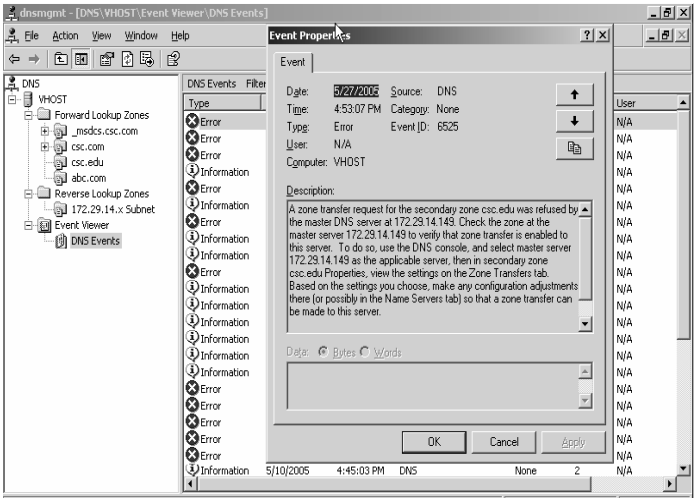

Hình 1.56: Thuộc tính của **MX record**.

### VII.2.10 Theo dõi sự kiện log trong DNS.

Khi quản trị dịch vụ **DNS**, việc ghi nhận và theo dõi sự kiện xảy ra cho dịch vụ **DNS** là rất quan trọng, thông qua đó ta có thể đưa ra một số giả pháp khác phục một khi có sự cố xảy ra,…Trong **DNS** management console cung cấp mục **Event Viewer** để cho ta có thể thực hiện điều này, trong phần này ta cần lưu ý một số biểu tượng như:

Theo dõi sự kiện:

- Error : Chỉ thị lỗi nghiêm trọng, đối với lỗi này ta cần theo xử lý nhanh chóng.




Hình 1.57: Theo dõi sự kiện lỗi

- Information : Thông tin ghi nhận các sự kiện bình thường như **shutdown**, **start**, **stop DNS**,….



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

# Tóm tắt

Lý thuyết 3 tiết - Thực hành 6 tiết

| Mục tiêu | Các mục chính | Bài tập bắt buộc | Bài tập làm thêm |
|---|---|---|---|
| Kết thúc bài học giúp học viên hiểu nguyên tắc hoạt động của dịch vụ FTP và thiết lập một FTP Server hỗ trợ cho việc truyền file trên mạng. | I. Giới thiệu FTP<br>II. Chương trình FTP client.<br>III. Giới thiệu FTP server. | Dựa vào bài tập môn Dịch vụ mạng Windows 2003. | Dựa vào bài tập môn Dịch vụ mạng Windows 2003. |



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

# I. Giới thiệu về FTP.

## I.1. Giao thức FTP.

**FTP** là từ viết tắt của **File Transfer Protocol**. Giao thức này được xây dựng dựa trên chuẩn **TCP**, **FTP** cung cấp cơ chế truyền tin dưới dạng tập tin (**file**) thông qua mạng **TCP/IP**, **FTP** là 1 dịch vụ đặc biệt vì nó dùng đến 2 cổng: cổng 20 dùng để truyền dữ liệu (**data port**) và cổng 21 dùng để truyền lệnh (**command port**).

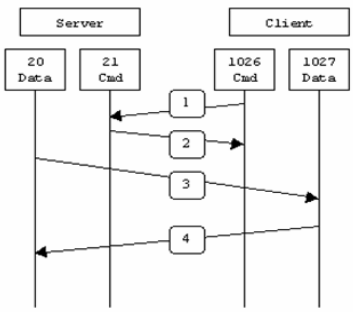
### I.1.1 Active FTP.

Ở chế độ chủ động (**active**), máy khách **FTP** (**FTP client**) dùng 1 cổng ngẫu nhiên không dành riêng (cổng N > 1024) kết nối vào cổng 21 của **FTP Server**. Sau đó, máy khách lắng nghe trên cổng N+1 và gửi lệnh **PORT** N+1 đến **FTP Server**. Tiếp theo, từ cổng dữ liệu của mình, **FTP Server** sẽ kết nối ngược lại vào cổng dữ liệu của **Client** đã khai báo trước đó (tức là N+1)

Ở khía cạnh **firewall**, để **FTP Server** hỗ trợ chế độ **Active** các kênh truyền sau phải mở:

- Cổng 21 phải được mở cho bất cứ nguồn gửi nào (để **Client** khởi tạo kết nối)
- **FTP Server's** port 21 to **ports** > 1024 (**Server** trả lời về cổng điều khiển của **Client**)
- Cho kết nối từ cổng 20 của **FTP Server** đến các cổng > 1024 (**Server** khởi tạo kết nối vào cổng dữ liệu của **Client**)
- Nhận kết nối hướng đến cổng 20 của **FTP Server** từ các cổng > 1024 (**Client** gửi xác nhận **ACKs** đến cổng **data** của **Server**)

Sơ đồ kết nối:




Hình 2.1: Mô hình hoạt động của **Active FTP**.

- Bước 1: **Client** khởi tạo kết nối vào cổng 21 của **Server** và gửi lệnh PORT 1027.
- Bước 2: **Server** gửi xác nhận **ACK** về cổng lệnh của **Client**.
- Bước 3: **Server** khởi tạo kết nối từ cổng 20 của mình đến cổng dữ liệu mà **Client** đã khai báo trước đó.
- Bước 4: **Client** gửi **ACK** phản hồi cho **Server**.



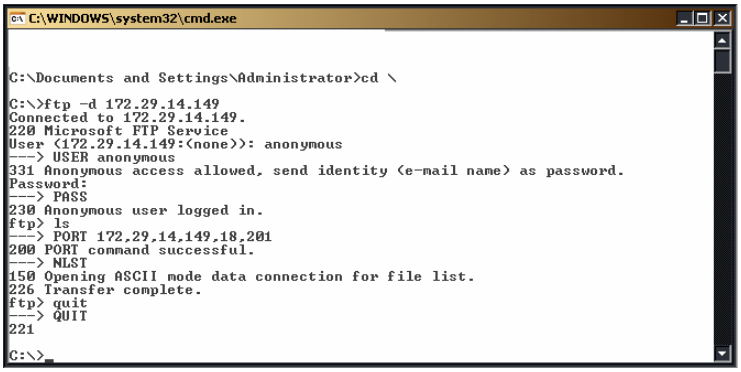
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Khi **FTP Server** hoạt động ở chế độ chủ động, **Client** không tạo kết nối thật sự vào cổng dữ liệu của **FTP server**, mà chỉ đơn giản là thông báo cho **Server** biết rằng nó đang lắng nghe trên cổng nào và **Server** phải kết nối ngược về **Client** vào cổng đó. Trên quan điểm **firewall** đối với máy **Client** điều này giống như 1 hệ thống bên ngoài khởi tạo kết nối vào hệ thống bên trong và điều này thường bị ngăn chặn trên hầu hết các hệ thống **Firewall**.

Ví dụ phiên làm việc **active FTP**:

Trong ví dụ này phiên làm việc **FTP** khởi tạo từ máy **testbox1.slacksite.com** (192.168.150.80), dùng chương trình **FTP Client** dạng dòng lệnh, đến máy chủ **FTP testbox2.slacksite.com** (192.168.150.90). Các dòng có dấu --> chỉ ra các lệnh **FTP** gửi đến **Server** và thông tin phản hồi từ các lệnh này. Các thông tin người dùng nhập vào dưới dạng chữ đậm.

Lưu ý là khi lệnh **PORT** được phát ra trên **Client** được thể hiện ở 6 byte. 4 byte đầu là địa chỉ IP của máy **Client** còn 2 byte sau là số cổng. Giá trị cổng được tính bằng (byte_5*256) + byte_6, ví dụ ( (14*256) + 178) là 3762.




Phiên làm việc active FTP.

### I.1.2 Passive FTP.

Để giải quyết vấn đề là **Server** phải tạo kết nối đến **Client**, một phương thức kết nối **FTP** khác đã được phát triển. Phương thức này gọi là **FTP** thụ động (**passive**) hoặc **PASV** (là lệnh mà **Client** gửi cho **Server** để báo cho biết là nó đang ở chế độ **passive**).

Ở chế độ thụ động, **FTP Client** tạo kết nối đến **Server**, tránh vấn đề **Firewall** lọc kết nối đến cổng của máy bên trong từ **Server**. Khi kết nối **FTP** được mở, client sẽ mở 2 cổng không dành riêng N, N+1 (N > 1024). Cổng thứ nhất dùng để liên lạc với cổng 21 của **Server**, nhưng thay vì gửi lệnh **PORT** và sau đó là server kết nối ngược về **Client**, thì lệnh **PASV** được phát ra. Kết quả là **Server** sẽ mở 1 cổng không dành riêng bất kỳ P (P > 1024) và gửi lệnh **PORT P** ngược về cho **Client**.. Sau đó client sẽ khởi tạo kết nối từ cổng N+1 vào cổng P trên **Server** để truyền dữ liệu.

Từ quan điểm **Firewall** trên **Server FTP**, để hỗ trợ **FTP** chế độ **passive**, các kênh truyền sau phải được mở:

- Cổng FTP 21 của **Server** nhận kết nối từ bất nguồn nào (cho **Client** khởi tạo kết nối)
- Cho phép trả lời từ cổng 21 **FTP Server** đến cổng bất kỳ trên 1024 (**Server** trả lời cho cổng **control** của **Client**)
- Nhận kết nối trên cổng **FTP server** > 1024 từ bất cứ nguồn nào (**Client** tạo kết nối để truyền dữ



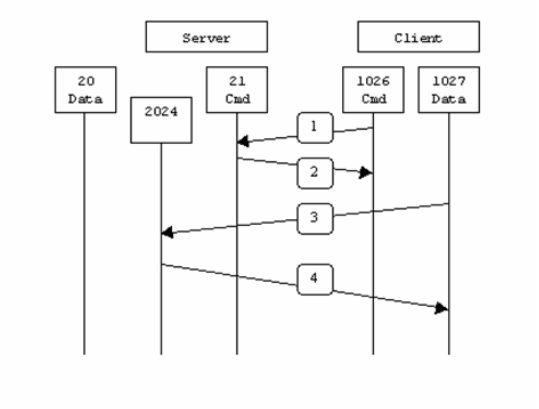
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

liệu đến cổng ngẫu nhiên mà **Server** đã chỉ ra)



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

- Cho phép trả lời từ cổng **FTP Server** > 1024 đến các cổng > 1024 (**Server** gửi xác nhận **ACKs** đến cổng dữ liệu của **Client**)




Hình 2.2: Mô hình hoạt động của **Active FTP**.

- Bước 1: **Client** kết nối vào cổng lệnh của **Server** và phát lệnh **PASV**.
- Bước 2: **Server** trả lời bằng lệnh **PORT** 2024, cho **Client** biết cổng 2024 đang mở để nhận kết nối dữ liệu.
- Bước 3: **Client** tạo kết nối truyền dữ liệu từ cổng dữ liệu của nó đến cổng dữ liệu 2024 của **Server**.
- Bước 4: **Server** trả lời bằng xác nhận **ACK** về cho cổng dữ liệu của **Client**.

Trong khi **FTP** ở chế độ thụ động giải quyết được vấn đề phía **Client** thì nó lại gây ra nhiều vấn đề khác ở phía **Server**. Thứ nhất là cho phép máy ở xa kết nối vào cổng bất kỳ > 1024 của **Server**. Điều này khá nguy hiểm trừ khi FTP cho phép mô tả dãy các cổng >= 1024 mà **FTP Server** sẽ dùng (ví dụ WU-FTP **Daemon**).

Vấn đề thứ hai là một số **FTP Client** lại không hỗ trợ chế độ thụ động. Ví dụ tiện ích **FTP Client** mà **Solaris** cung cấp không hỗ trợ **FTP** thụ động. Khi đó cần phải có thêm trình **FTP Client**. Một lưu ý là hầu hết các trình duyệt **Web** chỉ hỗ trợ **FTP** thụ động khi truy cập **FTP Server** theo đường dẫn URL ftp://.

Ví dụ phiên làm việc **passive FTP**:

Trong ví dụ này phiên làm việc **FTP** khởi tạo từ máy **testbox1.slacksite.com** (192.168.150.80), dùng chương trình **FTP Client** dạng dòng lệnh, đến máy chủ **FTP testbox2.slacksite.com** (192.168.150.90), máy chủ **Linux** chạy **ProFTPd 1.2.2RC2**. Các dòng có dấu --> chỉ ra các lệnh **FTP** gửi đến **Server** và thông tin phản hồi từ các lệnh này. Các thông tin người nhập vào dưới dạng chữ đậm.

Lưu ý: đối với **FTP** thụ động, cổng mà lệnh **PORT** mô tả chính là cổng sẽ được mở trên **Server**. Còn đối với **FTP** chủ động  cổng này sẽ được mở ở **Client**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

```
bash-2.05# ftp -d localhost
Connected to localhost.
220 nhon FTP server ready.
Name (localhost:root): hv
---> USER hv
331 Password required for hv.
Password:
---> PASS XXXX
230-No directory! Logging in with home=/
230 User hv logged in.
---> SYST
215 UNIX Type: L8 Version: SUNOS
Remote system type is UNIX.
---> TYPE I
200 Type set to I.
Using binary mode to transfer files.
ftp> cd /home
---> CWD /home
250 CWD command successful.
ftp> ls
---> EPSV
229 Entering Extended Passive Mode (|||64948|)
---> TYPE A
200 Type set to A.
---> NLST
550 *: No such file or directory.
---> TYPE I
200 Type set to I.
ftp>
```

Phiên giao dịch **Passive FTP**.

### I.1.3 Một số lưu ý khi truyền dữ liệu qua FTP.

**IIS** hỗ trợ cả hai chế độ kết nối **Active** và **Passive**, do đó việc kết nối theo phương thức **Active** hay **passive** tùy thuộc vào từng **Client**. **IIS** không hỗ trợ cơ chế vô hiệu hóa (**disable**) chế độ kết nối **Active** hay **Passive**.

Khi ta sử dụng dịch vụ **FTP** để truyền dữ liệu trên mạng **Internet** thông qua một hệ thống bảo mật như **Proxy**, **Firewall**, **NAT**, thông thường các hệ thống bảo mật này chỉ cho phép kết nối **TCP** theo cổng dịch vụ 21 do đó **user** gặp vấn đề trong việc sử dụng các lệnh **DIR**, **LS**, **GET**, or **PUT** để truyền dữ liệu vì các lệnh này đòi hỏi hệ thống bảo mật phải cho phép sử dụng cổng TCP 20. Cho nên khi sử dụng **FTP** để truyền tin trên mạng Internet thông qua mạng các hệ thống bảo mật (**Proxy**, **Firewall**, **NAT**) thì những hệ thống này phải mở **TCP port** 20 của **FTP**.

Danh sách các ứng dụng **Microsoft** cung cấp làm **FTP Client**.

| FTP Client | Transfer Mode |
|---|---|
| Command-line | Active |
| Internet Explorer 5.1 và các phiên bản trước đó | Passive |
| Internet Explorer 5.5 và các phiên bản sau này | Active and Passive |
| Từ FrontPage 1.1 tới FrontPage 2002 | Active |

### I.1.4 Cô lập người dùng truy xuất FTP Server (FTP User Isolation).



**FTP User Isolation** đặc tính mới trên **Windows 2003**, hỗ trợ cho **ISP** và **Aplication Service Provider** cung cấp cho người dùng **upload** và cập nhật nội dung **Web**, chứng thực cho từng người dùng. **FTP user Isolation** cấp mỗi người dùng một thư mục riêng rẻ, người dùng chỉ có khả năng xem, thay đổi,

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

xóa nội dung trong thư mục của mình.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

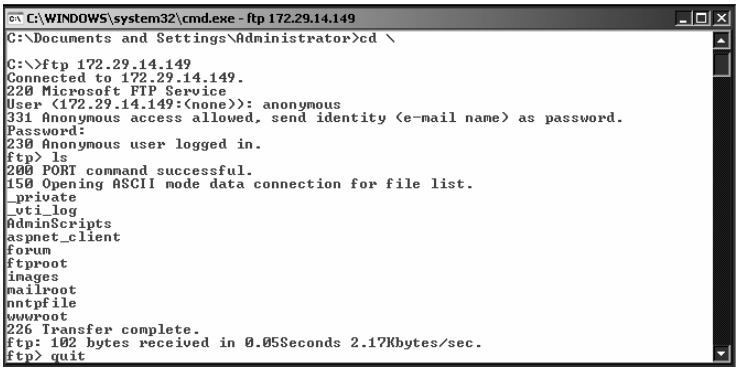
| Isolation Mode | Chức năng |
|---|---|
| Do not isolate users | Đây là chế độ không sử dụng **FTP User Isolation**, ở **mode** này không giới hạn truy xuất của người dùng. Thông thường ta sử dụng **mode** này để tạo một **public FTP Site**. |
| Isolate users | Mode này chứng thực người dùng cục bộ (**Local User**) và người dùng miền (**Domain User**) truy xuất vào **FTP Site**. Đối với **mode** người quản trị phải tạo cho mỗi người dùng một thư mục con của thư mục **FTP Root**, với tên thư mục này là **username** của người dùng. |
| Isolate users using Active Directory | Sử dụng **Active Directory** để tách lập từng **user** truy xuất vào **FTP Server**. |

# II. Chương trình FTP client.

Là chương trình giao tiếp với **FTP Server**, hầu hết các hệ điều hành đều hỗ trợ **FTP Client**, trên **Linux** hoặc **Windows** để mở kết nối tới **FTP Server** ta dùng lệnh #ftp <ftp_address>.

Để thiết lập một phiên giao dịch, ta cần phải có địa chỉ **IP** (hoặc tên máy tính), một tài khoản (**username**, **password**). **Username** mà **FTP** hỗ trợ sẵn cho người dùng để mở một giao dịch **FTP** có tên là **anonymous** với **password** rỗng.

Sau đây là một ví dụ về mở một phiên giao dịch đến **FTP Server**:




Hình 2.3: Sử dụng **FTP Client**.

Một số tập lệnh của **FTP Client**:

| Tên lệnh | Cú pháp | Ý nghĩa |
|---|---|---|
| ? hoặc lệnh help | ? [command] | Hiển thị giúp đỡ về [**command**]. |
| append | append local-file [remote-file] | Ghép một tập tin cục bộ với 1 tập tin trên **Server**. |



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

| | | |
|---|---|---|
| ascii | ASCII | Chỉ định kiểu truyền file là **ascii** (đây là kiểu |



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

| | | |
|---|---|---|
| | | truyền mặc định). |
| binary | Binary | Chỉ định kiểu truyền file là **binary**(đây là kiểu truyền mặc định). |
| Bye | Bye | Kết thúc **ftp session**. |
| Cd | cd remote-directory | Thay đổi đường dẫn thư mục trên **FTP Server.** |
| delete | delete remote-file | Xóa file trên **FTP Server**. |
| Dir | dir remote-directory | Liệt kê danh sách tập tin. |
| Get | get remote-file [local-file] | **Download** tập tin từ **FTP Server** về máy cục bộ. |
| Lcd | lcd [directory] | Thay đổi thư mục trên máy cục bộ. |
| Ls | ls [remote-directory] [local-file] | Liệt kê các tập tin và thư mục. |
| mdelete | mdelete remote-files [ ...] | Xóa nhiều tập tin. |
| Mget | mget remote-files [ ...] | **Download** nhiều tập tin. |
| Mkdir | mkdir directory | Tạo thư mục. |
| Put | put local-file [remote-file] | **Upload** tập tin. |
| Mput | mput local-files [ ...] | **Upload** nhiều tập tin. |
| Open | open computer [port] | Kết nối tới **ftp server**. |
| prompt | Prompt | Tắt cơ chế **confirm** sau mỗi lần **download** tập tin. |
| disconnect | Disconnect | Hủy kết nối **FTP**. |
| Pwd | Pwd | Xem thư mục hiện tại. |
| Quit | Quit | Thoát khỏi **ftp session**. |
| Recv | recv remote-file [local-file] | Copy tập tin từ **remote** về local. |
| Rename | rename filename newfilename | Thay đổi tên tập tin. |
| Rmdir | rmdir directory | Xóa thư mục. |



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

| | | |
|---|---|---|
| Send | send local-file [remote-file] | Copy tập tin từ **local** đến **remote**. |

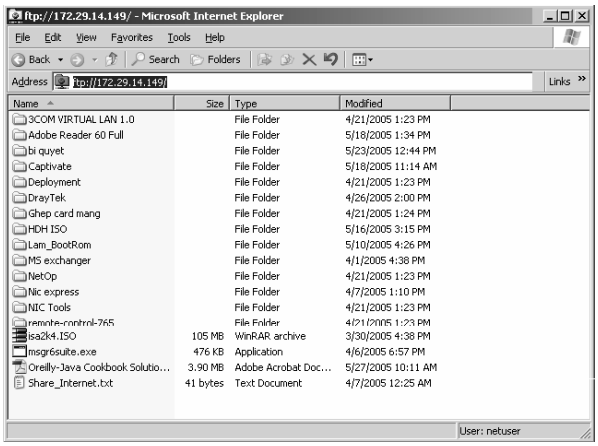


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

| | | | |
|---|---|---|---|
| User | user | user-name [password] [account] | Chuyển đổi **user** khác. |

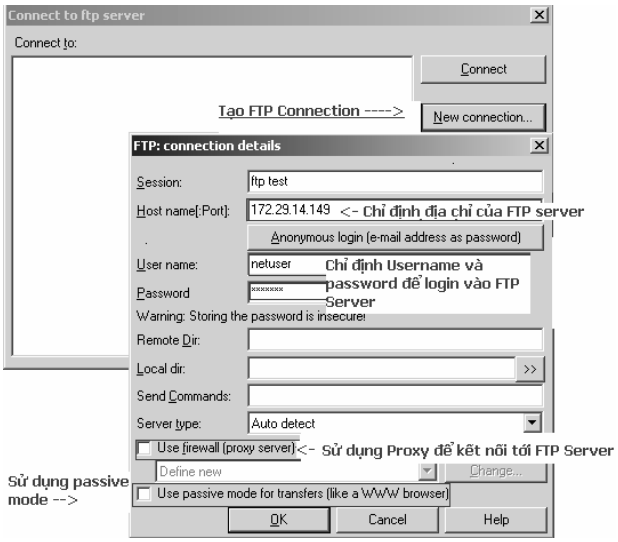
Ta có thể sử dụng chương trình Internet **Explorer** để kết nối với **FTP Server** theo cú pháp sau:

ftp://<username:password>@<Địa chỉ **FTP_Server**>




Hình 2.4: Sử dụng **IE** làm **FTP Client**.

Dùng **Windows commander** làm **FTP Client** để kết nối vào **FTP Server**, để thực hiện điều này ta mở chương trình **Windows Commander** | **Command** | **FTP Connect**…




Hình 2.5: Sử dụng **Windows commander** để kết nối vào **FTP Server**.

# III. Giới thiệu FTP Server.

Là máy chủ lưu trữ tập trung dữ liệu, cung cấp dịch vụ **FTP** để hỗ trợ cho người dùng có thể cung cấp, truy xuất tài nguyên qua mạng **TCP/IP**. **FTP** là một trong các dịch vụ truyền file rất thông dụng, người dùng có thể **upload** và **download** thông tin một cách dễ dàng hơn.



## III.1. Cài đặt dịch vụ FTP.

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Để cài đặt dịch vụ **FTP** trên **Windows 2003** ta thực hiện các bước sau:



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Chọn **Start** | **Control Panel**.

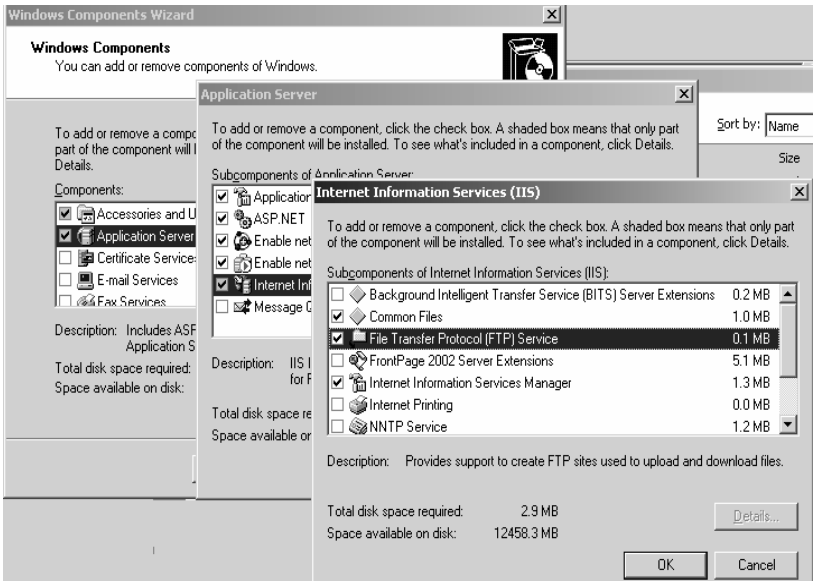
Bấm đôi vào **Add or Remove Programs**.

Từ ô vuông bên trái(pane) của cửa sổ "**Add or Remove Programs**" chọn **Add/Remove Windows Components**.

Từ danh sách **Components**, chọn **Application Server** và chọn nút **Details**.

Từ danh sách các **Application Server** chọn **Internet Information Services** và chọn nút **Details**.

Chọn mục **File Transfer Protocol** (**FTP**) **Service**.




Hình 2.6: Cài đặt **FTP Service**.

Bấm nút **OK**.

Click vào nút **Next** để hệ thống cài đặt dịch vụ **FTP** (đôi khi hệ thống yêu cầu chỉ bộ nguồn **I386** hoặc đường dẫn có chứa thư mục này để hệ thống chép một số file cần thiết khi cài đặt).

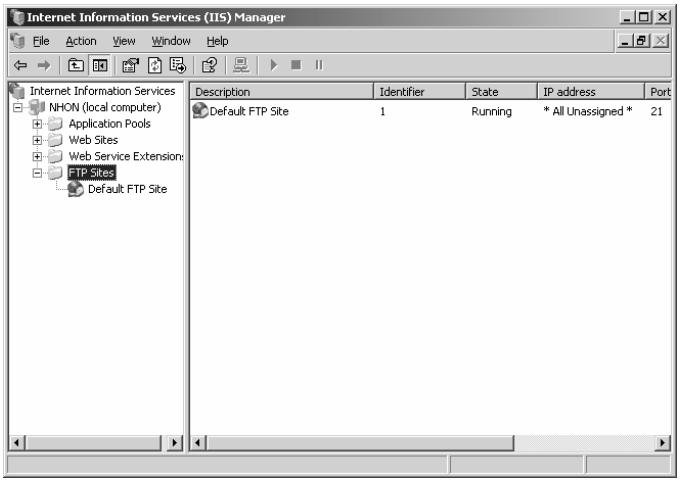
Bấm vào nút **Finish** để hoàn tất quá trình cài đặt.

## III.2. Cấu hình dịch vụ FTP.

Sau khi ta cài đặt hoàn tất dịch vụ **FTP**, để quản lý dịch vụ này ta chọn **Start** | **Programs** | **Administrative Tools** | **Internet Information Services**(**IIS**) **Manager** | **Computer name** | **FTP sites** (tham khảo Hình 2.7).



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 2.7: **IIS Manager**.

Mặc định khi cài xong dịch vụ **FTP**, hệ thống tự tạo một **FTP site** có tên **Default FTP Site** với một số thông tin sau:

- **FTP name: Default FTP Site**.
- **TCP Port**: 21
- **Connection Limited to:** Giới hạn tối đa 100.000 kết nối.
- **Enable logging:** để cho phép ghi nhận log vào file **\systemRoot \system32\LogFiles**
- Cho phép **Anonymous** và người dùng cục bộ được đăng nhập vào **FTP Server**.
- Thư mục gốc của **FTP server** là **<ổ đĩa>\Inetpub\ftproot.**
- Quyền hạn truy xuất (cho **Anonymous** và **user** cục bộ) là **read** và **log visits**.
- Cho phép tất cả các máy tính được phép truy xuất vào **FTP Server**.

Do đó khi ta cài đặt xong ta có thể sử dụng dịch vụ **FTP** ngay mà không cần cấu hình, tuy nhiên chỉ sử dụng được một số chức năng cơ bản mà hệ thống cấu hình ban đầu. Điều tốt nhất là ta xóa đi rồi tạo **FTP Site** mới để cấu hình lại từ đầu.

### III.2.1 Tạo mới FTP site.

Để tạo mới một **FTP site** ta thực hiện các bước sau:

Trong **IIS Manager** ta bấm chuột phải vào vào thư mục **FTP Sites** | **New** | **FTP Site**…| **Next**.

Mô tả tên **FTP site** trong hộp thoại "**FTP Site Desciption**" | **Next**.

Chỉ định **IP Address** và **Port** sử dụng cho **FTP Site**, trong phần này ta để mặc định, tiếp theo chọn **Next**.

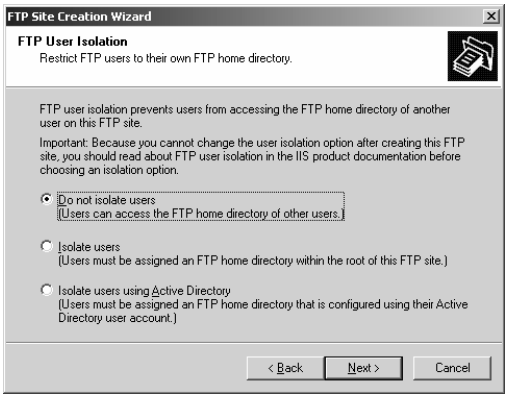
Trong hộp thoại "**FTP User Isolation**", chọn tùy chọn **Do not isolate users** để cho phép mọi người dùng được sử dụng **FTP server**, chọn **Next** (tham khảo hình 2.8), ta cần tham khảo một số mục chọn sao



- **Do not isolate users**: Không giới hạn truy xuất tài nguyên cho từng người dùng.
- **Isolate users**: Giới hạn truy xuất tài nguyên **FTP** cho từng người dùng (tham khảo trong cấu hình **FTP User Isolation**).

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

- **Isolate users using Active Directory**: Dùng **AD** để giới hạn việc sử dụng tài nguyên cho từng người (tham khảo trong mục cấu hình **FTP User Isolation**).



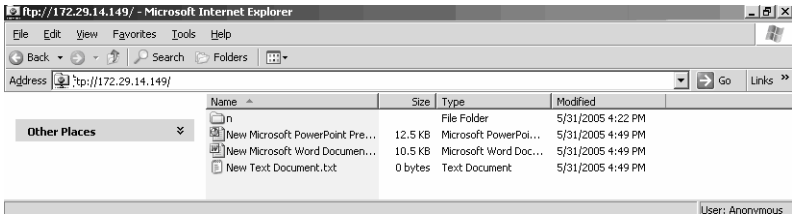

Hình 2.8: FTP User Isolation

Chọn đường dẫn chỉ định **Home Directory** cho **FTP Site**, chọn **Next**.

Chọn quyền hạn truy xuất cho **FTP site**, mặc định hệ thống chọn quyền **Read**, chọn **Next**.

Chọn **Finish** để hoàn tất quá trình tạo **FTP Site**.

Ta có thể kiểm tra bằng cách vào **Internet Explorer** đánh địa chỉ **URL** sau: ftp://172.29.14.149 (tham khảo Hình 2.9)




Hình 2.9: Truy xuất **FTP Server** bằng **IE**.

### III.2.2 Tạo và xóa FTP Site bằng dòng lệnh.

Để tạo một **FTP Site** ta dùng lệnh:

iisftp /create <Home Dir> "Description" /i <IP address>

Trong đó <**IP address**> để cho **FTP** lắng nghe tại port 21.

Xóa ftp dùng lệnh:

iisftp /delete "<Tên FTP>"

Ta tham khảo **Hình 2.10** cung cấp một số thông tin khi tạo như:

- "Connecting to server ...Done"
- "Server = NHON" : Tên FTP Server
- "Site Name= FTP – TTTH" : Tên FTP Site
- **"Metabase Path = MSFTPSVC/303020280"**: biểu diễn registry key cho thư mục Home Directory.
- **"IP = 172.29.14.149"** : Địa chỉ IP listen port 21



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

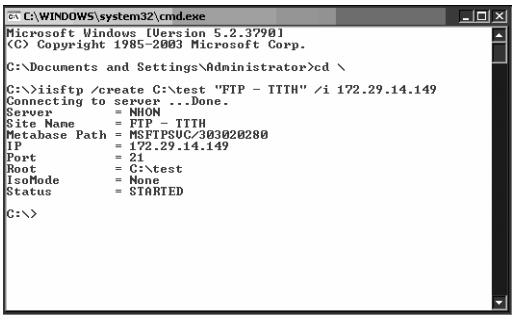
- “Port= 21” : TCP port



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

- **"Root= C:\test" :** Home directory của FTP Site.
- **"IsoMode= None" :** Không sử dụng Isolation mode.
- **"Status= STARTED" :** Mô tả trạng thái hoạt động.

Ví dụ: Tạo **FTP Site** bằng lệnh:

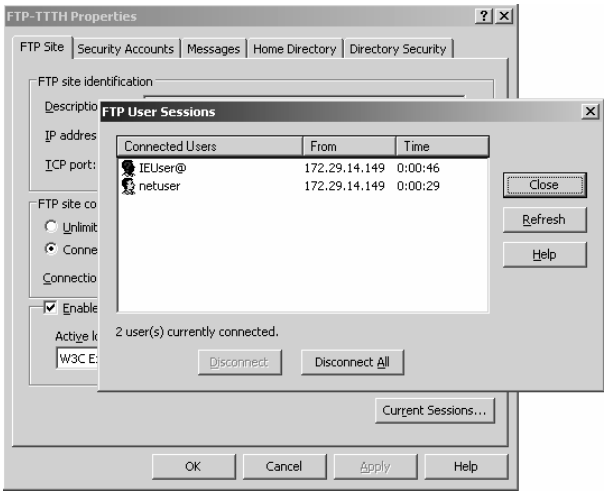



Hình 2.10: Tạo **FTP** bằng lệnh.

### III.2.3 Theo dõi các user login vào FTP Server.

Để theo dõi các **user** đăng nhập vào **FTP Server** ta bấm chuột phải vào **FTP site** | **Properties** | **General** | **Current sessions**…(tham khảo Hình 2.10)

- **Connected Users**: để chỉ định tên người dùng đang **login** vào **FTP Server** (IEUser@ là **Anonymous user**).
- **From**: Chỉ địa chỉ máy trạm đăng nhập vào **FTP Server**.
- **Time**: Thời gian đăng nhập.
- Nút **Disconect** : Để hủy kết nối của **user** đang login.
- Nút **Disconect All**: Để hủy tất cả các kết nối của **user** đang **login**.




Hình 2.11: Theo dõi **user session**.



### III.2.4 Điều khiển truy xuất đến FTP Site.

Ta có 4 cách điều khiển việc truy xuất đến **FTP Site** trên **IIS** như sau:

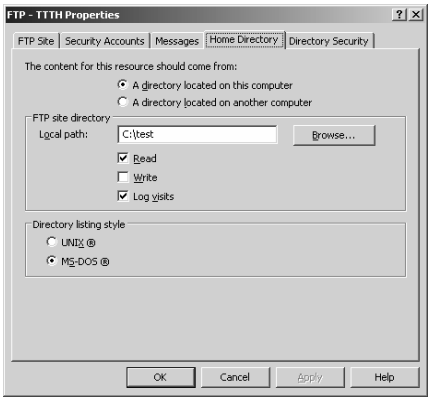
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

- **NTFS Permissions**: áp đặt quyền **NTFS** vào các thư mục liên quan đến **FTP Site**.



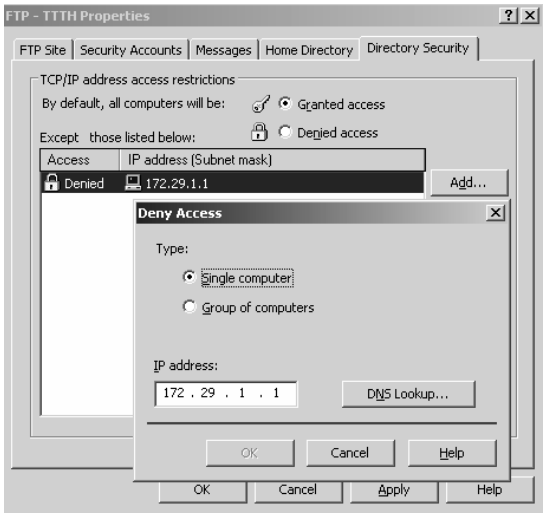
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

- **IIS Permissions**: Gán quyền **FTP** cho thư mục, thông thường chỉ có quyền **Read** và **Write**. Để gán quyền này ta chọn **properties** của **FTP Site** | **Tab Home Directory**(tham khảo Hình 2.12).




Hình 2.12: Gán quyền **FTP** cho thư mục.

- **IP address restrictions**: Giới hạn việc truy xuất vào **FTP** theo địa chỉ **IP**. Để gán quyền này ta chọn **properties** của **FTP Site** | **Tab Home Directory** (tham khảo Hình 2.13).
- Nếu ta chọn **Granted access: FTP Server** cho phép tất các **host** khác truy xuất, trừ các **host** được mô tả trong hộp thoại.
- Nếu ta chọn **Denied access: FTP Server** chỉ cho phép các **host** trong hộp thoại được truy xuất.




Hình 2.13: Giới hạn truy xuất **FTP** cho **host**.

- **Authentication**: **Tab Security Account** để cho chứng thực người dùng **Anonymous** và người dùng cục bộ được phép hay không được phép truy xuất vào **FTP Server**.
- Mặc định **Anonymous** được login vào **FTP Server**. Ta chọn mục này khi ta muốn **public FTP** cho mọi người khác được sử dụng.
- Nếu ta chọn mục **"Allow only anonymous connections"** có nghĩa ta chỉ cho phép **Anonymous** truy xuất vào **FTP Server**.
- Thông thường để tổ chức một **FTP Server** riêng biệt và ta không muốn **public FTP** cho mọi người sử dụng thì ta bỏ tùy chọn **Allow anonymous connections"**, lúc này **FTP Server** chỉ cho phép

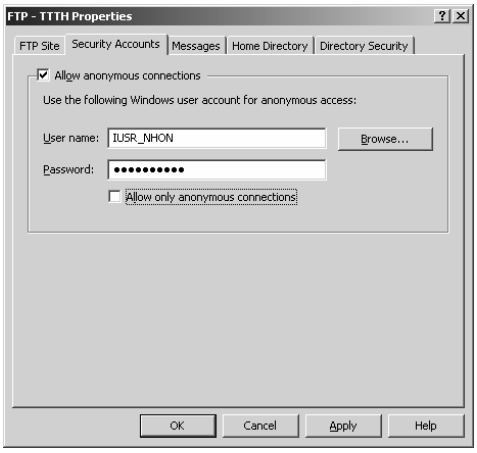


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

các người dùng cục bộ truy xuất.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 2.14: Cấp truy xuất cho **Account**.

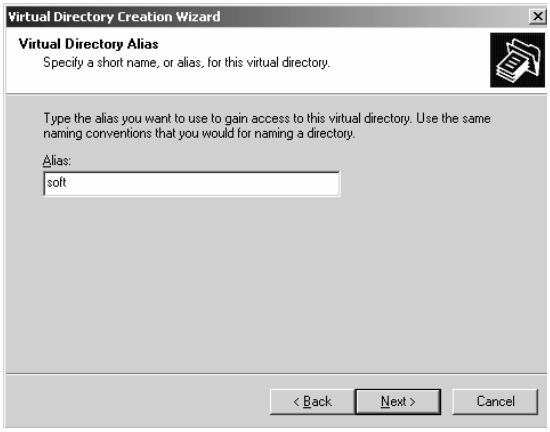
### III.2.5 Tạo Virtual Directory.

Thông thường các thư mục con của **FTP r**oot đều có thể truy xuất thông qua đường dẫn **URL** của dịch vụ **FTP** như: "ftp://<địa_chỉ_của_FTP_server>/<tên_thư_mục_con>", để cho phép người dùng có thể truy xuất một tài nguyên bên ngoài **FTP root** thì ta phải làm cách nào? **FTP server** cung cấp tính năng **virtual directory** để cho phép ta có thể giải quyết trường hợp này, thông **virtual directory** ta tạo một thư mục ảo bên trong **FTP Site** ánh xạ vào bất kỳ một thư mục nào đó trên ổ đĩa cục bộ hoặc ánh xạ vào một tài nguyên chia sẻ trên mạng. sao khi ánh xạ xong ta có thể truy xuất tài nguyên theo địa chỉ "ftp://<địa_chỉ_của_FTP_server>/<tên_thư_mục_ảo >"

Các bước tạo thư mục ảo (**virtual directory**):

Bấm chuột phải vào **FTP Site** chọn **New** | **Virtual Directory**…| **Next**.

Enter vào tên **virtual directory** trong ô **Alias** (tham khảo hình 2.15)

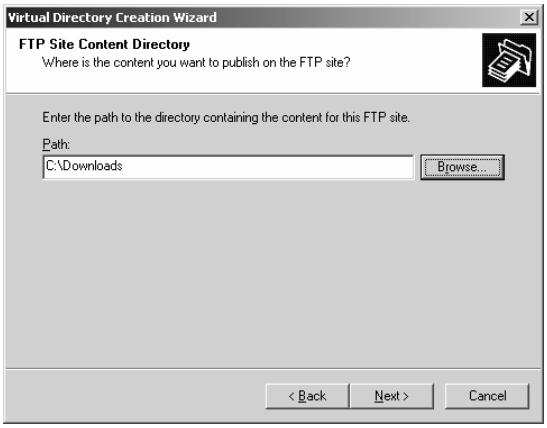



Hình 2.15: Tạo tên **Alias**.

Chỉ định tên thư mục trong ổ đĩa.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net



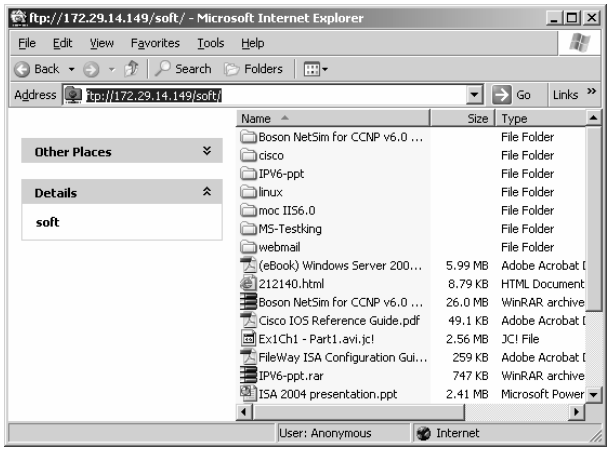

Hình 2.16: Chỉ định thư mục.

Chỉ định quyền hạn truy xuất vào thư mục.


Hình 2.17: Đặt quyền truy xuất vào **Virtual Directory**.

Chọn **Finish** để hoàn tất quá trình.

Truy xuất **Virtual directory** (minh họa ở Hình 2.18)




Hình 2.18: Truy xuất **Virtual Directory**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

### III.2.6 Tạo nhiều FTP Site.



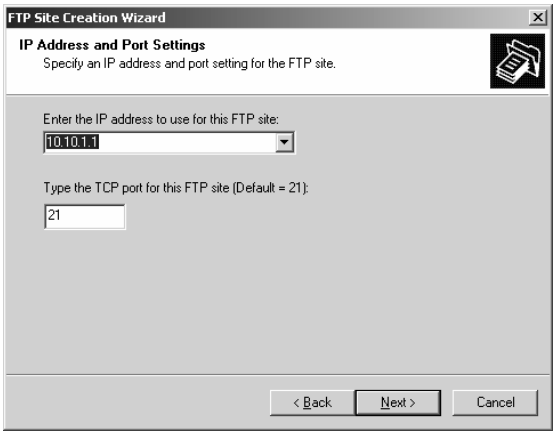
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Ta có thể tạo nhiều **FTP Site** trên một **FTP Server** bằng cách sử dụng nhiều địa chỉ **IP** và nhiều **FTP port**.

Các bước thực hiện:

Bấm đôi vào tên máy tính cục bộ trong **IIS manager**, sau đó bấm chuột phải **FTP Sites** | **New** | **FTP Site**…| **Next** | **Description** | **Next**.

Trong hộp thoại "**IP Address and Port Settings**" ta chọn địa chỉ **IP** cụ thể từ hộp thoại "**Enter IP address to use for this FTP site**" (tham khảo hình 2.19), chọn Next.



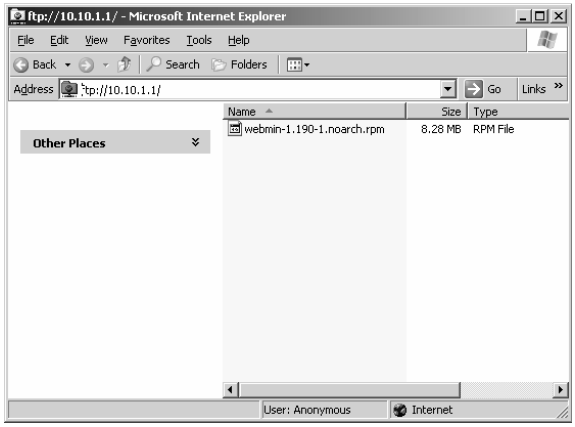

Hình 2.19: Chọn **IP address** và **Port**.

Chọn "**do not isolate user**" trong hộp thoại "**FTP User Isolation**", chọn **Next**.

Chọn đường dẫn thư mục gốc của **FTP**, chọn **Next**.

Chọn quyền truy xuất, sau đó chọn **Next** | **Finish** để hoàn tất.

Truy xuất **FTP site**:




Hình 2.20: Truy xuất **vftp**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

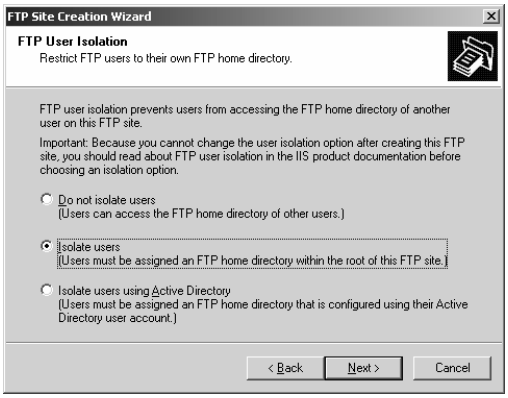
### III.2.7 Cấu hình FTP User Isolate.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Tạo **FTP Site** dùng **User Isolate**.

- Trong **IIS Manager**, Bấm chuột phải vào **FTP Sites folder** | **New** | **FTP Site**.
- Cung cấp các thông tin về "**FTP Site Description**" và "**IP Address and Port Settings**", chọn **Next**.
- Chọn **Isolate users**, chọn **Next** (tham khảo hình 2.21).




Hình 2.21: Tạo **FTP** sử dụng **Isolate Users**.

- Sau đó ta chỉ định thư mục gốc của **FTP**, quyền hạn truy xuất thư mục, sau cùng chọn **Finish** để hoàn tất quá trình.
- Nếu ta cho phép **User Anonymous** truy xuất vào **FTP Site** này thì trong thư mục gốc của **FTP Site** ta tạo một thư mục con có tên **LocalUser** (hoặc tên miền (tên **domain**) trong trường hợp máy chủ là **domain controller**), sau đó tạo **LocalUser\Public** (hoặc **domain_name\Public**) để **anonymous** truy xuất vào thư mục này.
- Nếu cho phép mỗi **người dùng cục bộ** truy xuất vào **FTP** thì ta tạo thư mục con của thư mục **FTP Root** với tên **LocalUser** và **LocalUser*username*.**
- Nếu cho phép mỗi **người dùng trong domain** truy xuất vào **FTP** thì ta tạo thư mục con của thư mục **FTP Root** với tên **<domain_name>** và thư mục con **<domain_name>\username.**

Tạo **FTP Site** dùng **Isolate User** với **Active Directory**.

Khi ta cấu hình **FTP Server** để cô lập các người dùng (**isolate users**) với **Active Directory**, khi tạo ta cần hiệu chỉnh hai thông số:

- **FTPRoot**: Chỉ định thông số **UNC** (**Universal Naming Convention**) của máy chủ chia sẻ tài nguyên (ví dụ **\\servername\sharename**), tuy nhiên ta cũng có thể chỉ định **FTP root** trên ổ đĩa cục bộ.
- **FTPDir**: Chỉ định đường dẫn thư mục cho từng user trong **Active Directory**.

Với **Windows 2003 family** hoặc **Windows 2003 enterprise** Để chỉ định hai thông số **FTPRoot** và FTPDir ta có thể vào **Properties** của từng người dùng hiệu chỉ hai thông số **msIIS-FTPRoot, msIIS-FTPDir** (trên **windows 2003 standard** không tồn tại cơ chế hiệu chỉnh này, ta phải dùng dòng lệnh để định nghĩa). Ta cũng có thể dùng lệnh **iisftp.vbs** để thay đổi hai thông số này.



Cú pháp lệnh như sau:

Định FTP Root:

```
<cmd_prompt>iisftp.vbs /SetADProp <username> FTPRoot <Local_dir>
```

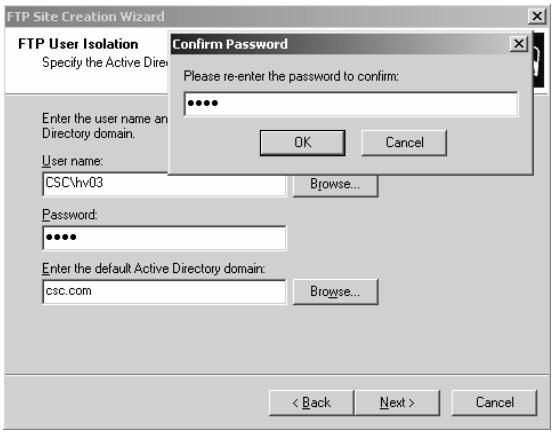
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

<cmd_prompt>iisftp.vbs /SetADProp <user_name> FTPDir <sub_FTPRoot>

Sau đây là các bước tạo **FTP User Isolate** với **Active Directory**:

- Bấm chuột phải vào **FTP Sites** folder | **New** | **FTP Site**.
- Cung cấp các thông tin về **FTP Site Description**, chọn cụ thể địa chỉ **IP** trong hộp thoại "**IP Address and Port Settings**", chọn **Next**.
- Trong hộp thoại "**FTP User Isolation**", ta chọn "**Isolate users using Active Directory**", chọn **Next**.
- Cung cấp thông tin về **username**, **password**, **domain name**, sau đó chọn **Next** để xác nhập lại mật khẩu của người dùng (tham khảo Hình 2.22 ta FTP cho hv03)




Hình 2.22: **FTP User Isolation**.

- Sau đó cấp quyền truy xuất cho **user**, sau cùng ta chọn **Finish**.
- Dùng lệnh:

<cmd_prompt>iisftp.vbs /SetADProp <username> FTPRoot <Local_dir>

<cmd_prompt>iisftp.vbs /SetADProp <user_name> FTPDir <sub_FTPRoot>

- Ví dụ:

iisftp.vbs /SetADProp hv03 FTPRoot c:\ftproot

iisftp.vbs /SetADProp hv03 FTPDir \hv03

- Trong đó \hv03 là thư mục con của c:\ftproot.

### III.2.8 Theo dõi và cấu hình nhật ký cho FTP.

Mặc định **FTP** lưu lại một số sự kiện như: Địa chỉ của **FTP Client** truy xuất vào **FTP Server**, thời gian truy xuất của máy trạm, trạng thái hoạt động của dịch vụ,… để hỗ trợ cho người quản trị có thể theo dõi quản lý hệ thống hiệu quả hơn.

- Tất cả các sự kiện này lưu trữ trong các file trong thư mục **%systemroot%\system32\LogFiles\MSFTPSVnnnnnnnn**, trong đó **nnnnnnnn** là số **ID** của **FTP Site**.
- Để hiệu chỉ lại thông tin ghi nhận nhật ký (**logging**) của dịch vụ ta chọn **properties** của **FTP Site** | Tab **FTP Site** | **Properties** (tham khảo hình 2.23).



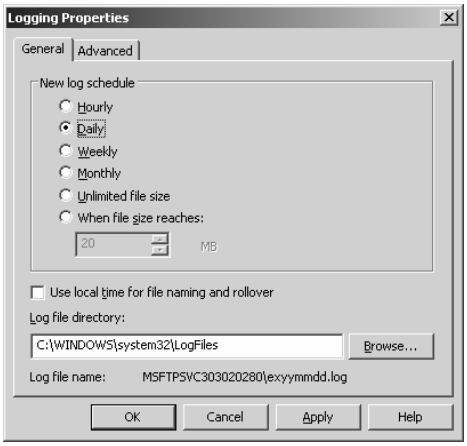
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

- **New log schedule:** Chỉ định ghi nhận theo lịch biểu, kích thước tập tin.



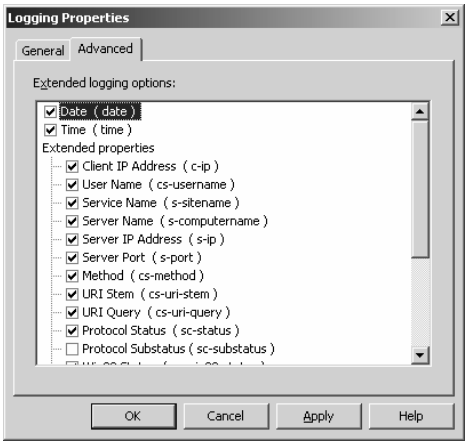
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

- **Log file directory:** Chỉ định thư lưu trữ **log file**.




Hình 2.23: Thay đổi nhật ký.

- **Tab Advanced** để cho phép ta có thể chọn một số tùy chọn theo dõi khác như: **Username**, **service name**, **server name**, **server IP**…(Tham khảo hình 2.24)

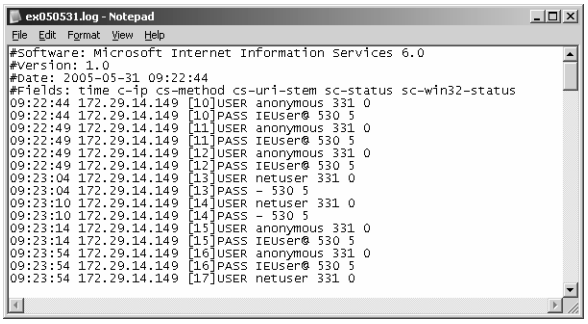



Hình 2.24: Tùy chọn **logging**.

- Để xem thông tin nhật ký trên ta mở các tập tin trong thư mục **%systemroot%\system32\LogFiles\MSFTPSVCnnnnnnnn**, ví dụ ta xem tập tin nhật ký ex050531.log (dùng **notepad** để mở) (tham khảo hình 2.25).



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 2.25: Xem tập tin nhật ký.

### III.2.9 Khởi động và tắt dịch vụ FTP.

Ta có thể dùng trình tiện ích **IIS** bằng cách bấm chuộc phải vào **FTP Site** chọn **Stop** để dùng dịch vụ và chọn **Start** để khởi động dịch vụ. Tuy nhiên ta có thể sử dụng dòng lệnh để khởi động và tắt dịch vụ **FTP**:

<command_prompt>net <stop/start> msftpsvc

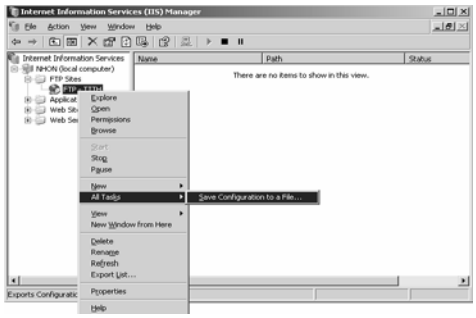
Hoặc có thể dùng lệnh **iisreset** để **restart** lại dịch vụ này:

< command_prompt >**iisreset**

### III.2.10 Lưu trữ và phục hồi thông tin cấu hình.

Sau khi ta cấu hình hoàn tất các thông tin cần thiết cho **FTP Site** ta có thể lưu trữ thông tin cấu hình này dưới dạng tập tin *.xml, sau đó ta có thể tạo mới hoặc phục hồi lại cấu hình cũ từ tập tin *.xml này.

- Lưu trữ thông tin cấu hình vào tập tin *xml ta bấm chuột phải vào **FTP Site** cần lưu thông tin cấu hình, chọn **All Task | Save Configuration to a File…**(Tham khảo hình 2.26)

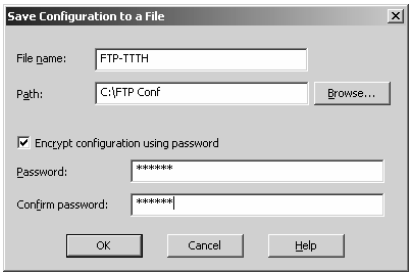



Hình 2.26: Lưu trữ thông tin cấu hình.

- Chỉ định tên tập tin và thư mục lưu trữ thông tin cho **FTP server**.
- **Encrypt configuration using password**: Sử dụng mật khẩu để mã hóa thông tin cấu hình (mặc định tùy chọn này không được chọn).

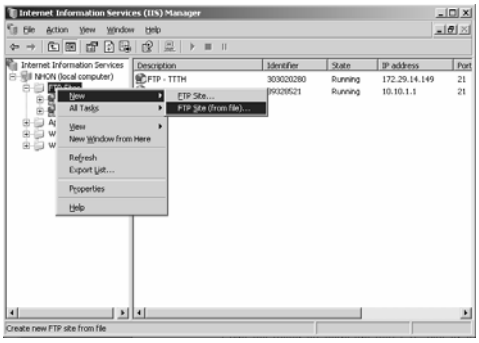


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net



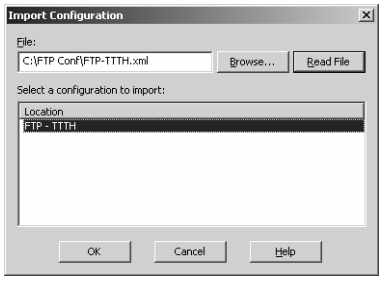

Hình 2.27: Chỉ định tên tập tin cấu hình.

- Phục hồi thông tin hoặc tạo mới **FTP site** từ tập tin cấu hình *.xml.




Hình 2.28

- Sau đó ta chọn nút **Browse**… để chọn tập tin cấu hình và chọn nút **Read File**, sau đó chọn tên mô tả trong hộp thoại **Location**, chọn **OK**.




Hình 2.29: **Import file** cấu hình.

- Sau đó chọn **OK** để đồng ý **import file** theo cách tạo mới **site** hay thay thế **site** hiện tại đã tồn tại.




Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Hình 2.30



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

# Tóm tắt

Lý thuyết 5 tiết - Thực hành 10 tiết

| Mục tiêu | Các mục chính | Bài tập bắt buộc | Bài tập làm thêm |
|---|---|---|---|
| Kết thúc bài học cho học viên có thể tổ chức, triển khai, quản trị một WebServer trên môi trường MS Windows, cụ thể là IIS 6.0 | I. Giao thức HTTP.<br>II. Nguyên tắc hoạt động của Web Server.<br>III. Đặc điểm của IIS.<br>IV. Cài đặt và cấu hình IIS 6.0. | Dựa vào bài tập môn Dịch vụ mạng Windows 2003. | Dựa vào bài tập môn Dịch vụ mạng Windows 2003. |



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

# I. Giao thức HTTP.

**HTTP** là một giao thức cho phép **Web Browser** và **Web Server** có thể giao tiếp với nhau. **HTTP** bắt đầu là 1 giao thức đơn giản giống như với các giao thức chuẩn khác trên **Internet**, thông tin điều khiển được truyền dưới dạng văn bản thô thông qua kết nối **TCP**. Do đó, kết nối **HTTP** có thể thay thế bằng cách dùng lệnh **telnet** chuẩn.

Ví dụ:

> telnet www.extropia 80

GET /index.html HTTP/1.0

<- Có thể cần thêm ký tự xuống dòng

Để đáp ứng lệnh **HTTP GET** , **Web server** trả về cho **Client** trang "**index.html**" thông qua phiên làm việc **telnet** này, và sau đó đóng kết nối chỉ ra kết thúc tài liệu.

Thông tin gởi trả về dưới dạng:

<HTML>

<HEAD>

<TITLE>eXtropia Homepage</TITLE>

[...]

</HEAD>

</HTML>

Giao thức đơn giản yêu-cầu/đáp-ứng (**request/response**) này đã phát triển nhanh chóng và được định nghĩa lại thành một giao thức phức tạp (phiên bản hiện tại HTTP/1.1) . Một trong các thay đổi lớn nhất trong **HTTP/1.1** là nó hỗ trợ kết nối lâu dài (**persistent connection**).

Trong **HTTP/1.0**, một kết nối phải được thiết lập đến **Server** cho mỗi đối tượng mà **Browser** muốn **download**. Nhiều trang Web có rất nhiều hình ảnh, ngoài việc tải trang **HTML** cơ bản, **Browser** phải lấy về một số lượng hình ảnh. Nhiều cái trong chúng thường là nhỏ hoặc chỉ đơn thuần là để trang trí cho phần còn lại của trang **HTML**.

# II. Nguyên tắc hoạt động của Web Server.

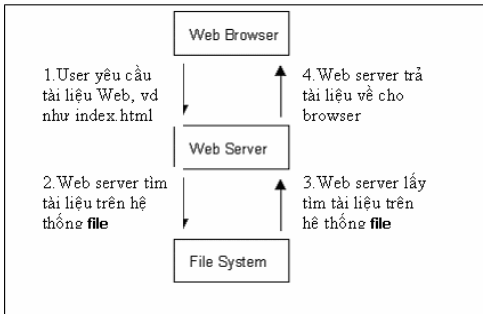
Ban đầu **Web Server** chỉ phục vụ các tài liệu **HTML** và hình ảnh đơn giản. Tuy nhiên, đến thời điểm hiện tại nó  có thể làm nhiều hơn thế.

Đầu tiên xét **Web Server** ở mức độ cơ bản, nó chỉ phục vụ các nội dung tĩnh. Nghĩa là khi **Web Server** nhận 1 yêu cầu từ **Web Browser**, nó sẽ ánh xạ đường dẫn này **URL** (ví dụ: http://www.hcmuns.edu.vn/index.html) thành một tập tin cục bộ trên máy **Web Server**.

Máy chủ sau đó sẽ nạp tập tin này từ đĩa và gởi tập tin đó qua mạng đến **Web Browser** của người dùng. **Web Browser** và **Web Server** sử dụng giao thức **HTTP** trong quá trình trao đổi dữ liệu.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 3.1: Sơ đồ hoạt động của **Web Server**.

Trên cơ sở phục vụ những trang Web tĩnh đơn giản này, ngày nay chúng đã phát triển với nhiều thông tin phức tạp hơn được chuyển giữa **Web Server** và **Web Browser**, trong đó quan trọng nhất có lẽ là nội dung động (**dynamic content**).

## II.1. Cơ chế nhận kết nối.

Với phiên bản đầu tiên, **Web Server** hoạt động theo mô hình sau:

- Tiếp nhận các yêu cầu từ **Web Browser**.
- Trích nội dung từ đĩa .
- Chạy các chương trình **CGI**.
- Truyền dữ liệu ngược lại cho **Client**.

Tuy nhiên, cách hoạt động của mô hình trên không hoàn toàn tương thích lẫn nhau. Ví dụ, một **Web Server** đơn giản phải theo các luật logic sau:

- Chấp nhận kết nối.
- Sinh ra các nội dung tĩnh hoặc động cho **Browser**.
- Đóng kết nối.
- Chấp nhận kết nối.
- Lập lại quá trình trên ...

Điều này sẽ chạy tốt đối với các **Web Sites** đơn giản, nhưng **Server** sẽ bắt đầu gặp phải vấn đề khi có nhiều người truy cập hoặc có quá nhiều trang Web động phải tốn thời gian để tính toán cho ra kết quả.

Ví dụ: Nếu một chương trình **CGI** tốn 30 giây để sinh ra nội dung, trong thời gian này **Web Server** có thể sẽ không phục vụ các trang khác nữa .

Do vậy, mặc dù mô hình này hoạt động được, nhưng nó vẫn cần phải thiết kế lại để phục vụ được nhiều người trong cùng 1 lúc. **Web Server** có xu hướng tận dụng ưu điểm của 2 phương pháp khác nhau để giải quyết vấn đề này là: đa tiểu trình (**multi-threading**) hoặc đa tiến trình (**multi-processing**) hoặc các hệ lai giữa **multi-processing** và **multi-threading**.

## II.2. Web Client.



Là những chương trình duyệt Web ở phía người dùng, như **Internet Explorer**, **Netscape Communicator**.., để hiển thị những thông tin trang Web cho người dùng. **Web Client** sẽ gửi yêu cầu đến **Web Server**. Sau đó, đợi **Web Server** xử lý trả kết quả về cho **Web Client** hiển thị cho người

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

dùng. Tất cả mọi yêu cầu đều được xử lý bởi **Web Server**.



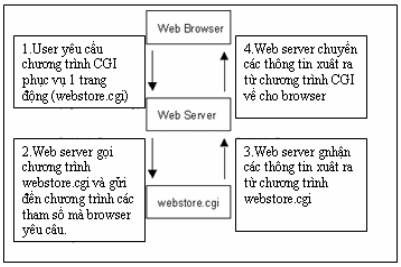
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

## II.3. Web động.

Một trong các nội dung động (thường gọi tắt là Web động) cơ bản là các trang Web được tạo ra để đáp ứng các dữ liệu nhập vào của người dùng trực tiếp hay gián tiếp.

Cách cổ điển nhất và được dùng phổ biến nhất cho việc tạo nội dung động là sử dụng **Common Gateway Interface** (**CGI**). Cụ thể là **CGI** định nghĩa cách thức **Web Server** chạy một chương trình cục bộ, sau đó nhận kết quả và trả về cho **Web Browser** của người dùng đã gửi yêu cầu.

**Web Browser** thực sự không biết nội dung của thông tin là động, bởi vì **CGI** về cơ bản là một giao thức mở rộng của **Web Server**. Hình vẽ sau minh hoạ khi **Web Browser** yêu cầu một trang Web động phát sinh từ một chương trình **CGI**.




Hình 3.2: Mô hình Xử lý.

Một giao thức mở rộng nữa của **HTTP** là **HTTPS** cung cấp cơ chế bảo mật thông tin "nhạy cảm" khi chuyển chúng xuyên qua mạng.

# III. Đặc điểm của IIS 6.0.

IIS 6.0 có sẵn trên tất cả các phiên của **Windows 2003**, **IIS** cung cấp một số đặc điểm mới giúp tăng tính năng tin cậy, tính năng quản lý, tính năng bảo mật, tính năng mở rộng và tương thích với hệ thống mới.

## III.1. Các thành phần chính trong IIS.

Hai thành phần chính trong **IIS 6.0** là **kernel-mode processes** và **user-mode processes**, ta sẽ khảo sát một số thành phần sau:

- **HTTP.sys**: Là trình điều khiển thuộc loại **kernel-mode device** hỗ trợ chứng năng chuyển **HTTP request** đến tới các ứng dụng trên **user-mode**:
- Quản lý các kết nối **Transmission Control Protocol** (**TCP**).
- Định tuyến các **HTTP requests** đến đúng hàng đợi xử lý yêu cầu (**correct request queue**).
- Lưu giữ các **response** vào vùng nhớ (**Caching of responses in kernel mode**).
- Ghi nhận nhật ký cho dịch vụ **WWW** (**Performing all text-based logging for the WWW service**).
- Thực thi các chức năng về **Quality of Service** (**QoS**) bao gồm: connection limits, **connection time-outs**, **queue-length limits**, **bandwidth throttling**.
- **WWW Service Administration and Monitoring Component**: cung cấp cơ chế cấu hình dịch vụ **WWW** và quản lý **worker process**.
- **Worker process**: Là bộ xử lý các yêu cầu (**request**) cho ứng dụng **Web**, **worker process** có thể



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

xử lý các yêu cầu và gởi trả kết quả dưới dạng trang Web tĩnh, gọi các **ISAPI Extensions**, kích



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

hoạt các **CGI handler**, tập tin thực thi của **worker process** có tên là **W3wp.exe**. **Worker process** chạy trong **user-mode**.

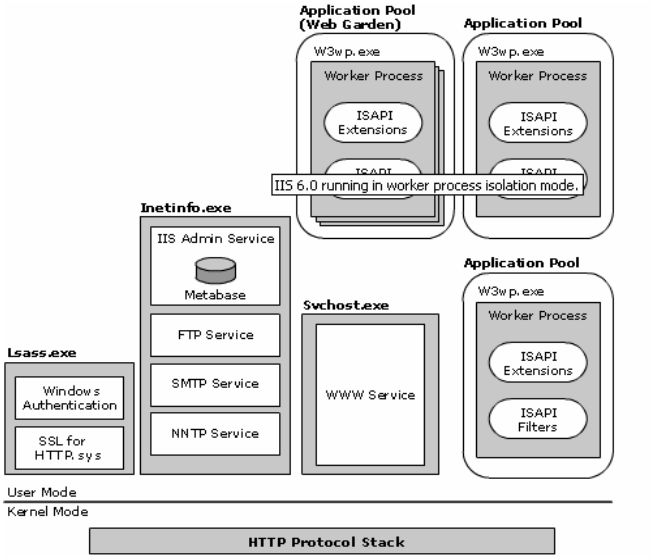
- **Inetinfo.exe** là một thành phần trong **user-mode**, nó có thể nạp (**host**) các dịch vụ trong **IIS 6.0**, các dịch vụ này bao gồm: **File Transfer Protocol service** (**FTP service**), **Simple Mail Transfer Protocol service** (**SMTP service**), **Network News Transfer Protocol service** (**NNTP service**), **IIS metabase**.

## III.2. IIS Isolation mode.

Trong **IIS** có hai chế độ hoạt động tách biệt là ***worker process isolation mode*** *và* ***IIS 5.0 isolation mode***. Cả hai chế độ này đều dựa vào đối tượng **HTTP Listener**, tuy nhiên nguyên tắc hoạt động bên trong của hai chế độ này hoạt về cơ bản là khác nhau.

## III.3. Chế độ Worker process isolation.

- Trong chế độ này mọi thành phần chính trong dịch vụ **Web** được tách thành các tiến trình xử lý riêng biệt (gọi là các **Worker process**) để bảo vệ sự tác động của các ứng dụng khác trong **IIS**, đây là chế độ cung cấp tính năng bảo mật ứng dụng rất cao vì hệ thống nhận diện mỗi ứng dụng chạy trên **Worker process** được xem là một **network service** trong khi đó các ứng dụng chạy trên **IIS 5.0** được xem là **LocalSystem** và nó có thể truy xuất và thay đổi hầu hết các tài nguyên được cung cấp trên hệ thống nội bộ.
- Sử dụng **worker process isolation** mode cho phép tích hợp thêm các tính năng mới như : **application pooling**, **recycling** và **health detection**, các tính năng này không được hỗ trợ trên **IIS 5.0**.
- Mô hình xử lý của **Worker process Isolation mode**:




Hình 3.3: Kiến trúc của **IIS 6.0** chạy trên chế độ **Worker Process Isolation**.



Trong hình 3.3, ta thấy các đoạn mã xử lý cho từng ứng dụng đặc biệt như **ASP**, **ASP.NET** được nạp vào bộ xử lý tiến trình (**Worker process**) bởi vì các bộ xử lý định thời(**run-time engine**) của ngôn ngữ lập trình này được thực thi như một Internet server **API** (**ISAPI**)

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Các bước minh họa cho một yêu cầu xử lý trong **worker process**:



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Yêu cầu của **Client** được chuyển đến đối tượng **HTTP Listener** (**HTTP.sys**)

**HTTP.sys** xác định yêu cầu có hợp lệ không?. Nếu yêu cầu không hợp lệ **HTTP.sys** sẽ gởi đoạn mã báo lỗi về cho **Client**.

Nếu yêu cầu hợp lệ **HTTP.sys** sẽ kiểm tra xem **response** của **request** này có trong **kernel-mode cache** không, nếu có thì nó sẽ đọc **response** này và gởi về cho **Client**.

Nếu **response** không có trong **cache** thì **HTTP.sys** xác định **request queue** phù hợp và đặt **request** vào trong **request queue**.

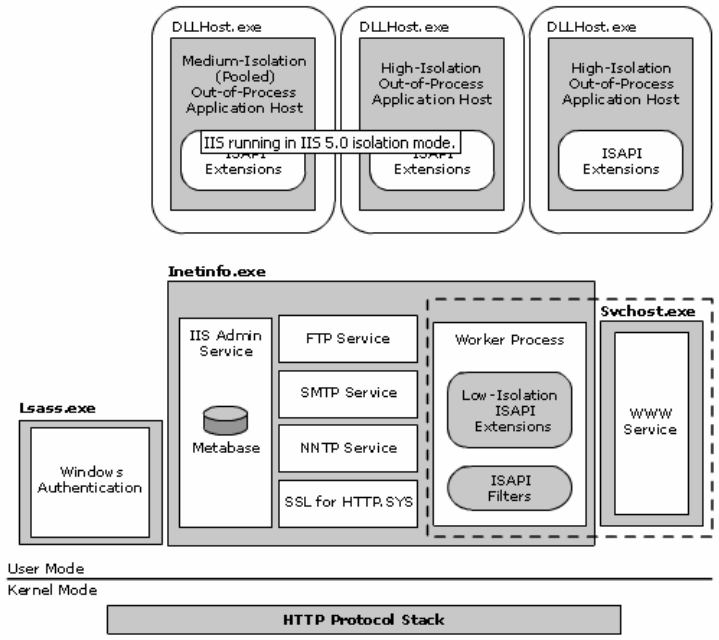
Nếu hàng đợi (**request queue**) không được cung cấp một **worker processes** thì **HTTP.sys** báo hiệu cho **WWW service** khởi tạo **worker processes** cho hành đợi (**request queue**).

Sau đó **worker process** xử lý các **request** và gởi trả kết quả về cho **HTTP.sys**.

**HTTP.sys** gởi kết quả về cho **Client** và **log** lại các yêu cầu này.

### III.3.1 IIS 5.0 Isolation Mode.

**IIS 5.0 Isolation mode** đảm bảo tính tương thích cho ứng dụng được phát triển từ phiên bản **IIS 5.0**.




Hình 3.4: **IIS** chạy trên **IIS 5.0 Isolation mode**.

### III.3.2 So sánh các chức năng trong IIS 6.0 mode.

Bảng mô tả vai trò của **IIS 6.0** khi chạy trong **IIS 5.0 isolation mode** và **worker process isolation mode**.

| Các chức năng của IIS | IIS 5.0 Isolation Mode Host/Component | Worker Process Isolation Mode Host/Component |
|---|---|---|
| Worker process management | | Svchost.exe (WWW service) |



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

| | | |
|---|---|---|
| Worker process | | W3wp.exe (Worker process) |
| Running in-process ISAPI extensions | Inetinfo.exe | W3wp.exe |
| Running out-of-process ISAPI extensions | DLLHost.exe | N/A (all of ISAPI extensions are in-process) |
| Running ISAPI filters | Inetinfo.exe | W3wp.exe |
| HTTP.sys configuration | Svchost.exe/WWW service | Svchost.exe/WWW service |
| HTTP protocol support | Windows kernel/HTTP.sys | Windows kernel/HTTP.sys |
| IIS metabase | Inetinfo.exe | Inetinfo.exe |
| FTP | Inetinfo.exe | Inetinfo.exe |
| NNTP | Inetinfo.exe | Inetinfo.exe |
| SMTP | Inetinfo.exe | Inetinfo.exe |

Các Isolation mode mặc định:

| Loại cài đặt | Isolation mode |
|---|---|
| Cài đặt mới IIS 6.0 | Worker process isolation mode |
| Nâng cấp từ các phiên bản trước lên IIS 6.0 | Vẫn giữ nguyên Isolation mode cũ. |
| Nâng cấp từ IIS 5.0 | IIS 5.0 isolation mode |
| Nâng cấp từ IIS 4.0 | IIS 5.0 isolation mode |

## III.4. Nâng cao tính năng bảo mật.

- **IIS 6.0** không được cài đặt mặc định trên **Windows 2003**, người quản trị phải cài đặt IIS và các dịch vụ liên quan tới **IIS**.
- **IIS 6.0** được cài trong **secure mode** do đó mặc định ban đầu khi cài đặt xong **IIS** chỉ cung cấp một số tính năng cơ bản nhất, các tính năng khác như **Active Server Pages** (**ASP**), **ASP.NET**, **WebDAV publishing**, **FrontPage Server Extensions** người quản trị phải kích hoạt khi cần thiết.
- Hỗ trợ nhiều tính năng chứng thực:
- **Anonymous authentication** cho phép mọi người có thể truy xuất mà không cần yêu cầu **username** và **password**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

- **Basic authentication:** Yêu cầu người dùng khi truy xuất tài nguyên phải cung cấp **username** và mật khẩu thông tin này được **Client** cung cấp và gởi đến **Server** khi **Client** truy xuất tài nguyên. **Username** và **password** không được mã hóa khi qua mạng.
- **Digest authentication:** Hoạt động giống như phương thức **Basic authentication**, nhưng **username** và mật khẩu trước khi gởi đến **Server** thì nó phải được mã hóa và sau đó **Client** gởi thông tin này dưới một giá trị của băm (***hash value***). **Digest authentication** chỉ sử dụng trên **Windows domain controller**.
- **Advanced Digest authentication:** Phương thức này giống như **Digest authentication** nhưng tính năng bảo mật cao hơn. **Advanced Digest** dùng **MD5 hash** thông tin nhận diện cho mỗi **Client** và lưu trữ trong **Windows Server 2003 domain controller**.
- **Integrated Windows authentication:** Phương thức này sử dụng kỹ thuật băm để xác nhận thông tin của **users** mà không cần phải yêu cầu gởi mật khẩu qua mạng.
- **Certificates:** Sử dụng thẻ chứng thực điện tử để thiết lập kết nối **Secure Sockets Layer** (**SSL**).
- **.NET Passport Authentication**: là một dịch vụ chứng thực người dùng cho phép người dùng tạo **sign-in name** và **password** để người dùng có thể truy xuất vào các dịch vụ và ứng dụng **Web** trên nền **.NET**.
- IIS sử dụng **account** (**network service**) có quyền ưu tiên thấp để tăng tính năng bảo mật cho hệ thống.
- Nhận dạng các phần mở rộng của file qua đó **IIS** chỉ chấp nhận một số định dạng mở rộng của một số tập tin, người quản trị phải chỉ định cho **IIS** các định dạng mới khi cần thiết.

## III.5. Hỗ trợ ứng dụng và các công cụ quản trị.

**IIS 6.0** có hỗ trợ nhiều ứng dụng mới như **Application Pool**, **ASP.NET**.

- **Application Pool**: là một nhóm các ứng dụng cùng chia sẻ một **worker process** (**W3wp.exe**).
- **worker process** (**W3wp.exe**) cho mỗi **pool** được phân cách với **worker process** (**W3wp.exe**) trong **pool** khác.
- Một ứng dụng nào đó trong một **pool** bị lỗi (**fail**) thì nó không ảnh hưởng tới ứng dụng đang chạy trong **pool** khác.
- Thông qua **Application Pool** giúp ta có thể hiệu chỉnh cơ chế tái sử dụng vùng nhớ ảo, tái sử dụng **worker process**, hiệu chỉnh **performance** (về **request queue**, **CPU**), **health**, **Identity** cho **application pool**.
- **ASP.NET:** là một **Web Application platform** cung cấp các dịch vụ cần thiết để xây dựng và phân phối ứng dụng **Web** và dịch vụ **XML Web**.

**IIS 6.0** cung cấp một số công cụ cần thiết để hỗ trợ và quản lý **Web** như:

- **IIS Manager**: Hỗ trợ quản lý và cấu hình **IIS 6.0**
- **Remote Administration** (**HTML**) T**o**ol: Cho phép người quản trị sử dụng **Web Browser** để quản trị **Web** từ xa.
- **Command –line administration scipts**: Cung cấp các **scipts** hỗ trợ cho công tác quản trị **Web**, các tập tin này lưu trữ trong thư mục **%systemroot%\System32**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

# IV. Cài đặt và cấu hình IIS 6.0.

## IV.1. Cài đặt IIS 6.0 Web Service.

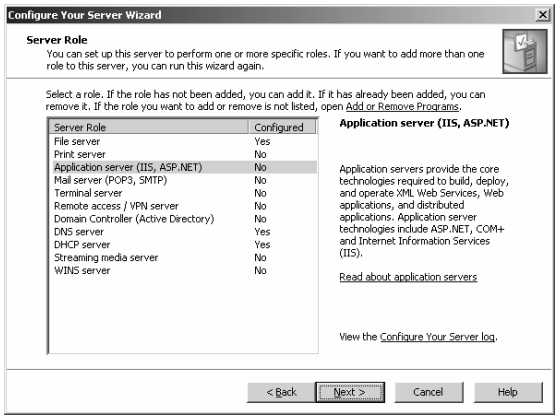
**IIS 6.0** không được cài đặt mặc định trong **Windows 2003 server**, để cài đặt **IIS 6.0** ta thực hiện các bước như sau:

Chọn **Start** | **Programs** | **Administrative Tools** | **Manage Your Server**.


Hình 3.5: **Manage Your Server Roles**.

Từ hình 3.6 ta chọn biểu tượng **Add or remove a role**, chọn **Next** trong hợp thoại **Preliminitary Steps**

Chọn **Application server** (IIS, **ASP.NET**) trong hộp thoại **server role**, sau đó chọn **Next**.

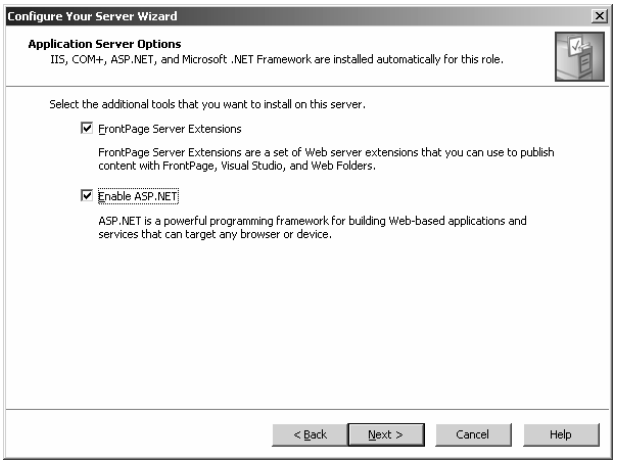



Hình 3.6: Chọn loại **Server**.

Chọn hai mục cài đặt **FrontPage Server Extentions** và **Enable ASP.NET**, sau đó chọn **Next**, chọn **Next** trong hộp thoại tiếp theo.

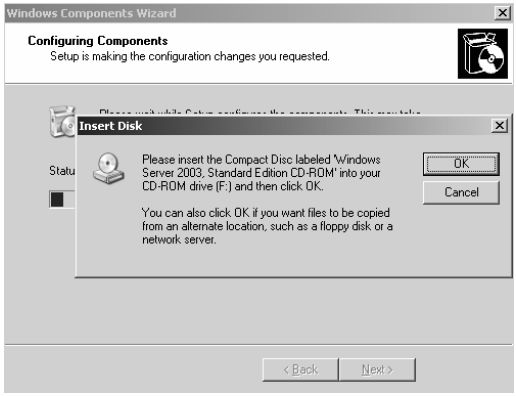


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 3.7: lựa chọn tùy chọn cho **Server**.

Sau đó hệ thống sẽ tìm kiếm **I386 source** để cài đặt **IIS**, nếu không tìm được xuất hiện yêu cầu chỉ định đường dẫn chứa bộ nguồn **I386**, sau đó ta chọn **Ok** trong hộp thoại Hình 3.8.




Hình 3.8: Chỉ định **I386 source**.

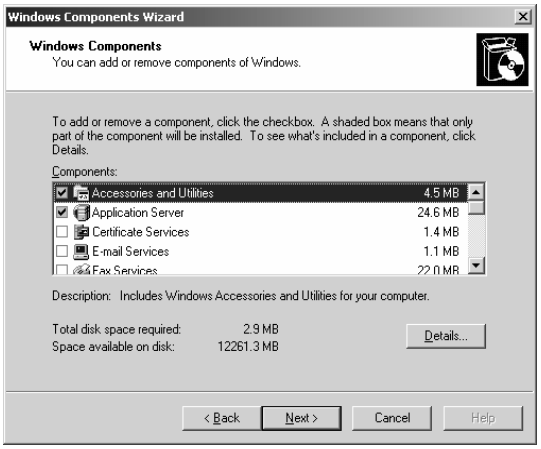
Chọn **Finish** để hoàn tất quá trình.

Tuy nhiên ta cũng có thể cài đặt **IIS 6.0** trong **Add or Remove Programs** trong **Control Panel** bằng cách thực hiện một số bước điển hình sau:

Mở cửa sổ **Control Panel** | **Add or Remove Programs** | **Add/Remove Windows Components**.



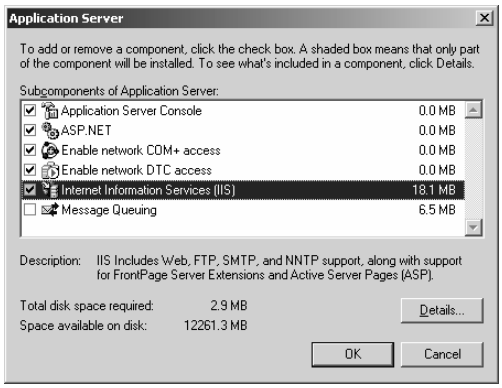
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 3.9: Chọn **Application Server**.

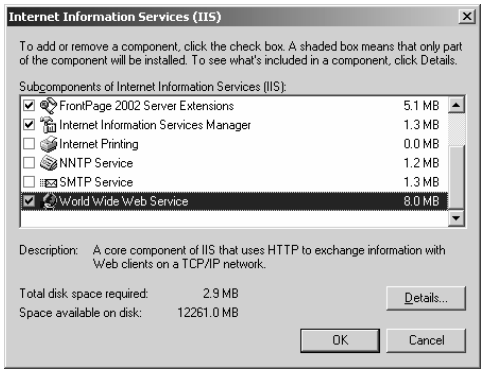
Chọn **Application Server**, sau đó chọn nút **Details**…

Chọn **Internet Information Services**, sau đó chọn nút **Details**…




Hình 3.10: Chọn **IIS subcomponents**.

Chọn mục **World Wide Web service**, sau đó chọn nút **Details**…

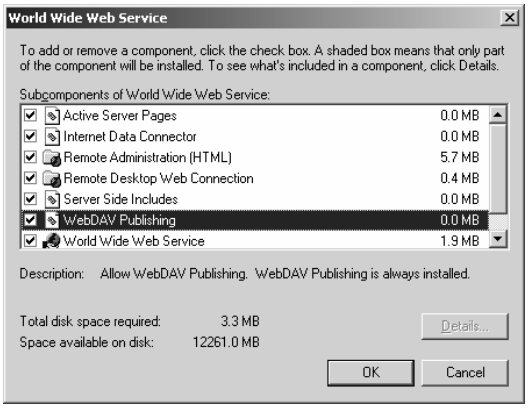



Hình 3.11: Chọn **WWW service**.

Sau đó ta chọn tất cả các **Subcomponents** trong **Web Service**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net



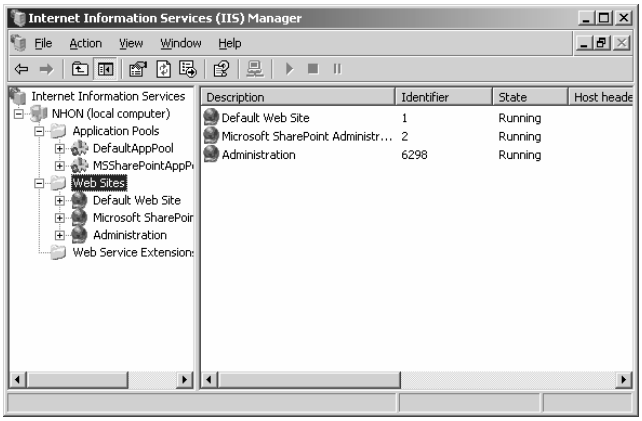

Hình 3.12: Chọn các thành phần trong **WWW service**.

## IV.2. Cấu hình IIS 6.0 Web service.

Sau khi ta cài đặt hoàn tất, ta chọn **Administrative Tools** | **Information Service (IIS) Manager**, sau đó chọn tên **Server** (**local computer**)

Trong hộp thoại **IIS Manager** có xuất hiện 3 thư mục:

- **Application Pools**: Chứa các ứng dụng sử dụng **worker process** xử lý các yêu cầu của **HTTP request**.
- **Web Sites**: Chứa danh sách các **Web Site** đã được tạo trên **IIS**.
- **Web Service Extensions**: Chứa danh sách các **Web Services** để cho phép hay không cho phép **Web Server** có thể thực thi được một số ứng dụng Web như: **ASP**, **ASP.NET**, **CGI**, **WebDAV**,…




Hình 3.13: **IIS Manager**.

Trong thư mục **Web Sites** ta có ba **Web Site** thành viên bao gồm:

- **Default Web Site**: **Web Site** mặc định được hệ thống tạo sẵn.
- **Microsoft SharePoint Administration**: Đây là **Web Site** được tạo cho **FrontPage Server Extensions 2002 Server Administration**
- **Administration**: **Web Site** hỗ trợ một số thao tác quản trị hệ thống qua **Web**.

Khi ta cấu hình **Web Site** thì ta không nên sử dụng **Default Web Site** để tổ chức mà chỉ dựa **Web Site**



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

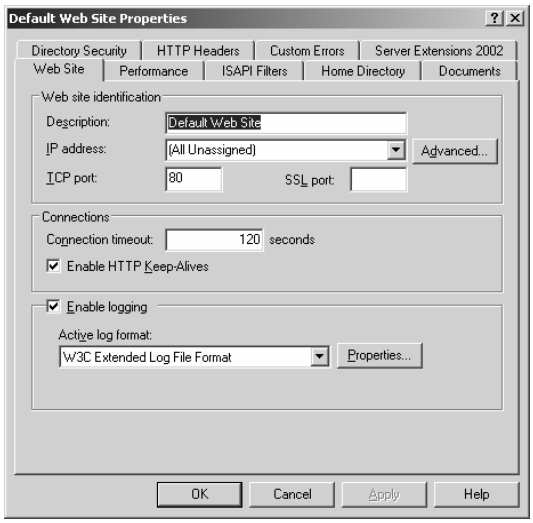
này để tham khảo một số thuộc tính cần thiết do hệ thống cung cấp để cấu hình **Web Site** mới của mình.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

### IV.2.1 Một số thuộc tính cơ bản.

Trước khi cấu hình **Web Site** mới trên **Web Server** ta cần tham khảo một số thông tin cấu hình do hệ thống gán sẵn cho **Default Web Site**. Để tham khảo thông tin cấu hình này ta nhấp chuột phải vào **Default Web Site** chọn **Properties**.

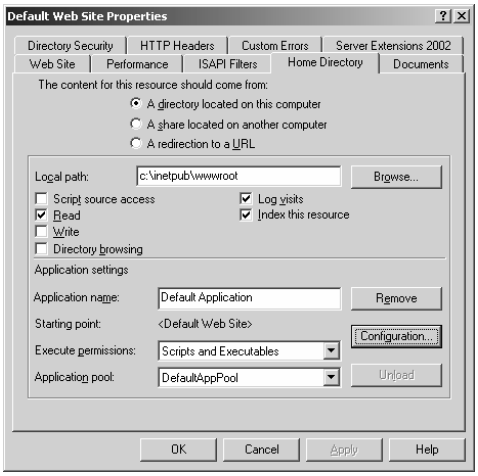



Hình 3.14: Thuộc tính **Web Site**.

- Tab **Web Site**: mô tả một số thông tin chung về dịch vụ Web như:
- **TCP port**: chỉ định cổng hoạt động cho dịch vụ **Web**, mặc định giá trị này là 80.
- **SSL Port**: Chỉ định port cho **https**, mặc định **https** hoạt động trên **port 443**. **https** cung cấp một số tính năng bảo mật cho ứng dụng **Web** cao hơn **http**.
- **Connection timeout** : Chỉ định thời gian duy trì một **http session**.
- Cho phép sử dụng **HTTP Keep-Alives**.
- Cho phép ghi nhận nhật ký (**Enable logging**)
- **Performance Tab**: cho phép đặt giới hạn băng thông, giới hạn **connection** cho **Web site**.
- **Home Directory Tab**: Cho phép ta thay đổi **Home Directory** cho **Web Site**, giới hạn quyền truy xuất, đặt một số quyền hạn thực thi **script** cho ứng dụng **Web** ( như ta đặt các thông số: **Application name**, **Execute permission**, **Application pool**)

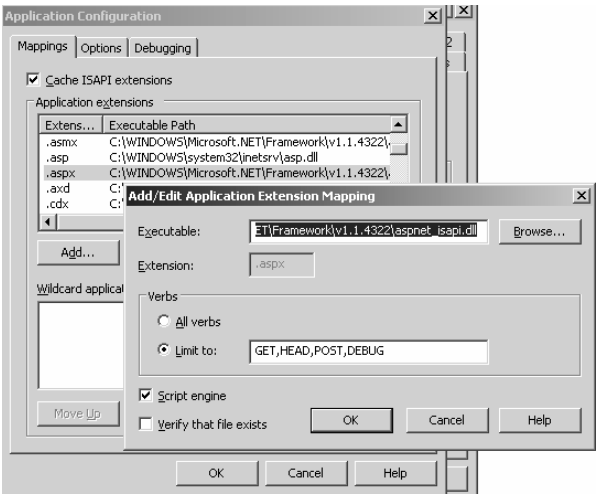


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 3.15: **Home Directory Tab**.

- Từ Hình 3.15 ta chọn nút **Configuration…** để có thể cấu hình các **extensions** về **.asp**, **.aspx**, **.asa**, … cho **Web Application** (tham khảo Hình 3.16)

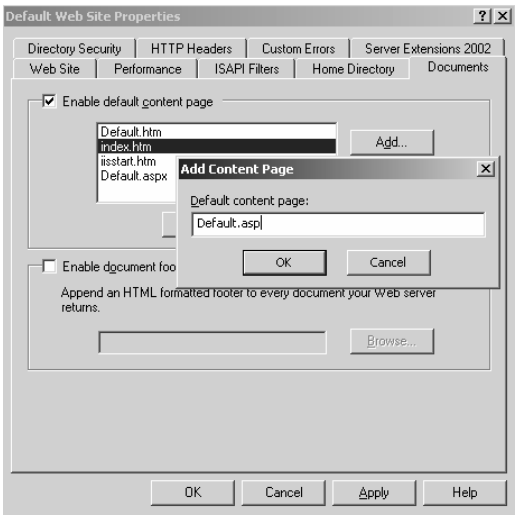



Hình 3.16: Cấu hình **Script** cho **Web Application**.

- **Documents Tab**: Để thêm hoặc thay đổi trang **Web** mặc định cho **Web Site** (tham khảo hình 3.17).



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 3.17: Chỉ định trang Web mặc định cho **Web Site**.

- **Directory Security Tab**: Đặt một số phương thức bảo mật cho **IIS** (tham khảo chi tiết trong mục "bảo mật cho dịch vụ Web")

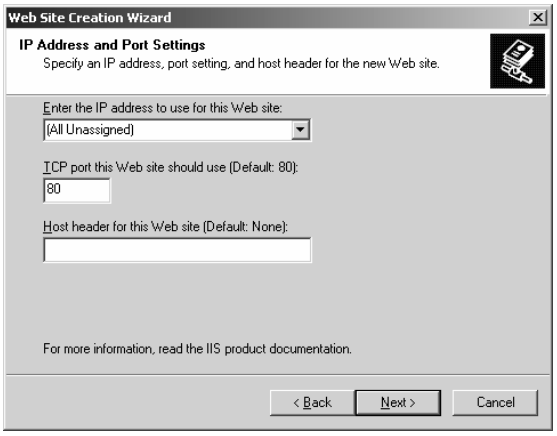
### IV.2.2 Tạo mới một Web site.

**IIS** cung cấp hai phương thức tạo mới **Web Site**:

- Tạo **Web Site** thông qua **Creation Wizard của IIS manager**.
- Tạo **Web Site** thông qua lệnh **iisweb.vbs**.
- Tạo **Web Site** thông qua "**Web Site Creation Wizard**" của **IIS manager**.
- Nhấp chuột phải vào thư mục **Web Sites** | **New | Web Site** | **Next**.
- Ta cung cấp tên **Web Site** trong hộp thoại **Description** | **Next**.
- Chỉ định các thông số về (Tham khảo Hình 3.18):
- **"Enter the IP address to use for this Web site"**: Chỉ định địa chỉ sử dụng cho **Web Site**, nếu ta chỉ định "**All Unassigned**" có nghĩa là **HTTP** được hoạt động trên tất cả các địa chỉ của **Server**.
- **"TCP port this Web site should use"**: Chỉ định cổng hoạt động cho dịch vụ.
- **"Host Header for this Web site (Default:None)"**: Thông số này để nhận diện tên **Web Site** khi ta muốn tạo nhiều **Web Site** cùng sử dụng chung một địa chỉ **IP** thì ta thường dùng thông số này để mô tả tên các **Web Site** đó, do đó khi ta chỉ tổ chức một **Web Site** tương ứng với 1 địa chỉ **IP** thì ta có thể không cần sử dụng thông số này.

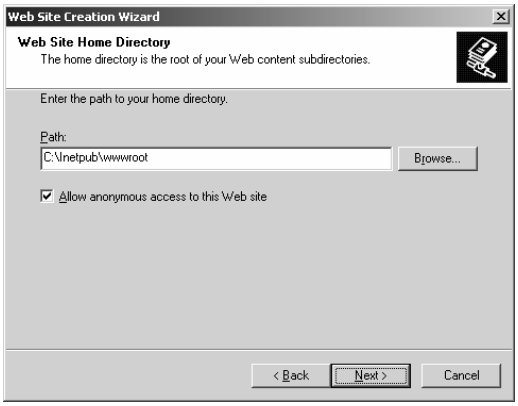


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 3.18: Chỉ định **IP Address** và **Port**.

- Trong hộp thoại "**Web Site Home Directory**" để chỉ định thư mục **home** của **Web Site** (thư mục lưu trữ nội dung của **Web Site)** và chỉ định **Anonymous** có được quyền truy xuất **Web Site** hay không (tham khảo Hình 3.19)

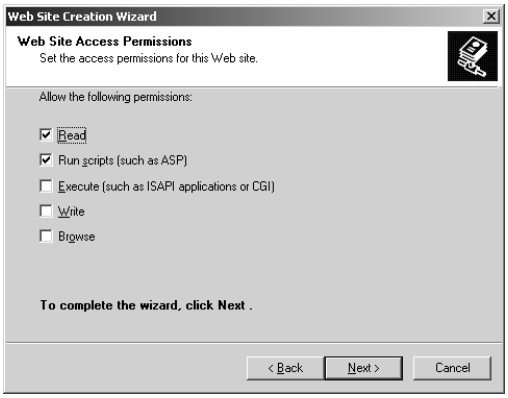



Hình 3.19: Chỉ định **Home Directory** cho **Web**.

- Chỉ định quyền hạn truy xuất cho **Web Site** (tham khảo Hình 3.20):
- **Read**: Quyền được truy xuất nội dung thư mục.
- **Run scripts** (**such as ASP**): Quyền được thực thi các trang **ASP**.
- **Execute** (**such as ISAPI Application for CGI**): Quyền được thực thi các ứng dụng **ISAPI**.
- **Write**: Quyền ghi và cập nhật dữ liệu của **Web Site**.
- **Browse**: Quyền liệt kê nội dung thư mục (khi không tìm được trang chủ mặc định)



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 3.20: Thiết lập quyền hạn truy xuất.

- Chọn **Finish** để hoàn tất quá trình.
- Tạo **Web Site** thông qua lệnh **iisweb.vbs**

Cú pháp lệnh:

iisweb.vbs /create <Home Directory> "Site Description" /i <IP Address> /b <Port>.

Các bước thực hiện:

- Nhấp chuột vào **Start** | **Run** | **cmd**.
- Từ dấu nhắc lệnh (**command prompt**) nhập vào lệnh: iisweb.vbs /create *c:\inetpub\wwwroot\newdirectory* "*MyWebSite*" /i *123.456.789* /b *80*.

### IV.2.3 Tạo Virtual Directory.

Thông thường để ta tạo thư mục ảo (**Virtual Directory** hay còn gọi là **Alias**) để ánh xạ một tài nguyên từ đường dẫn thư mục vật lý thành đường dẫn **URL**, thông qua đó ta có thể truy xuất tài nguyên này qua **Web Browser**.

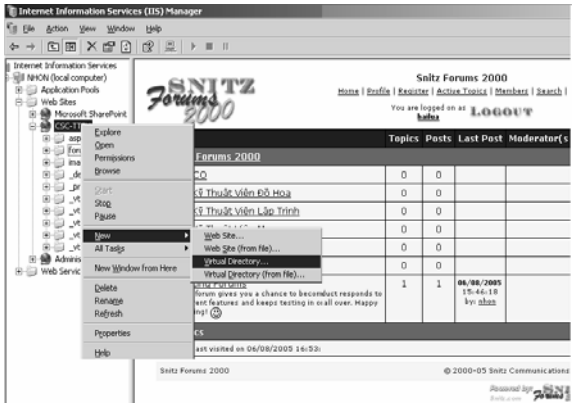
| Đường dẫn vật lý | Tên Alias | Địa chỉ URL |
|---|---|---|
| *C*:\Inetpub\wwwroot | Tên thư mục gốc (none) | http://SampleWebSite |
| \\Server2\SalesData | Customers | http://SampleWebSite/Customers |
| D:\Inetpub\wwwroot\Quotes | None | http://SampleWebSite/Quotes |
| D:\Marketing\PublicRel | Public | http://SampleWebSite/public |

Các bước tạo **Virtual Directory**

Nhấp chuột phải vào tên **Web Site** cần tạo chọn **New**, chọn **Virtual Directory** (tham khảo Hình 3.21).



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 3.21: Tạo **Virtual Directory**.

Chọn **Next**, sau đó chỉ định tên **Alias** cần tạo (tham khảo Hình 3.22)


Hình 3.22: Chỉ định tên Alias

Chọn **Next** từ bước 2, sau đó chỉ định thư mục cục bộ hoặc đường dẫn mạng cần ánh xạ, Chỉ định quyền hạn truy xuất cho **Alias**, cuối cùng ta chọn **Finish** để hoàn tất quá trình.

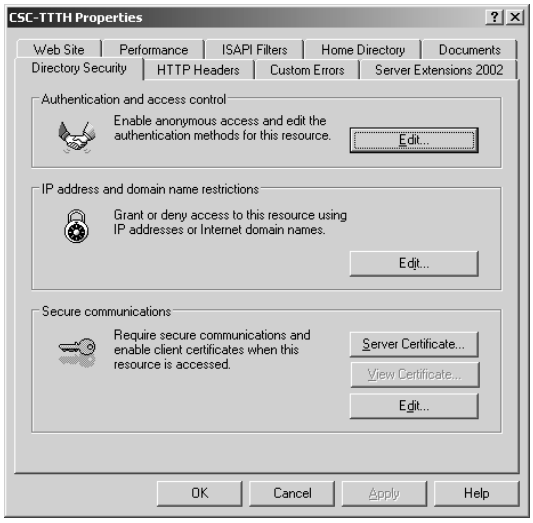
### IV.2.4 Cấu hình bảo mật cho Web Site.

**IIS** cung cấp một số tính năng bảo mật cho **Web Site** như (tham khảo Hình 3.23):

- **Authentication And Access Control**: **IIS** cung cấp 6 phương thức chứng thực, kết hợp quyền truy cập **NTFS** để bảo vệ việc truy xuất tài nguyên trong hệ thống.
- **IP address and domain name restriction**: Cung cấp một số tính năng giới hạn **host** và **network** truy xuất vào **Web Site**.
- **Secure communication**: Cung cấp một số tính năng bảo mật trong giao tiếp giữa **Client** và **Server** bằng cách **Server** tạo ra các giấy chứng nhận cho **Client** (**Client Certificate**) và yêu cầu **Client** khi truy xuất tài nguyên vào **Server** thì phải gởi giấy chứng nhận để **Server** xác nhận yêu cầu có hợp lệ hay không.

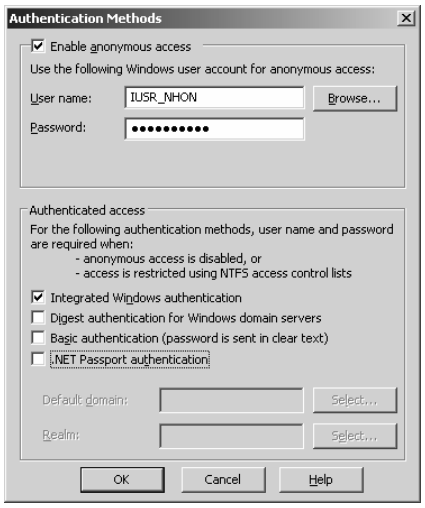


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 3.23: **Directory Security Tab**.

- Cấu hình **Authentication And Access Control:** từ Hình 3.23 ta chọn nút **Edit…**chọn các phương thức chứng thực cho phù hợp, mặc định hệ thống không yêu cầu chứng thực và cho mọi người sử dụng anonymous để truy xuất **Web Site**:

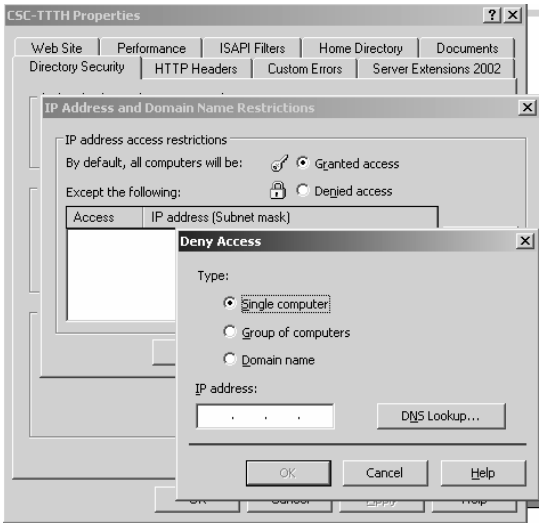



Hình 3.24: Chọn Phương thức chứng thực.

- Cấu hình **IP address and domain name restriction**: Từ hình 3.23 ta chọn nút **Edit**…



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 3.25: Giới hạn truy xuất cho **host**, **network** và **domain**.

- Cấu hình **Secure communication**: Từ hình 3.23 nút **Server Certificate**…để tạo giấy chứng nhận **Client**, nút **Edit** hiệu chỉnh các yêu cầu chứng nhận cho **Client** (tham khảo Hình 3.26).

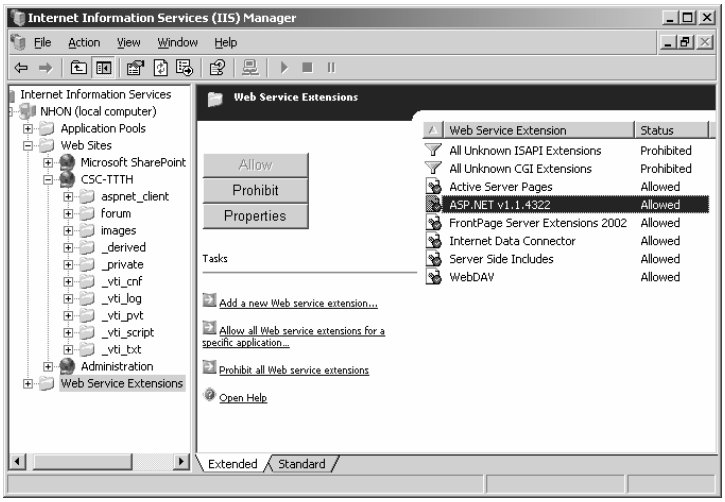

Hình 3.26: Thay đổi thao tác chứng nhận.

### IV.2.5 Cấu hình Web Service Extensions.

**IIS Web Service Extensions** cung cấp rất nhiều các dịch vụ mở rộng như: **ASP**, **ASP.NET**, **Frontpage Server Extensions 2002 WebDAV**, **Server Side Includes**, **CGI Extensions**, **ISAPI Extensions**. Thông qua **IIS Web Service Extensions** ta có thể cho phép hoặc cấm **Web Site** hỗ trợ các dịch vụ tương ứng (Nếu trên **Web Application** của ta có sử dụng các ứng dụng trên thì ta phải kích hoạt **Web Service** tương ứng)



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 3.27: Cấu hình **Web service extensions**.

### IV.2.6 Cấu hình Web Hosting.

**IIS** cho phép ta tạo nhiều **Web Site** trên một **Web Server**, kỹ thuật này còn gọi là **Web Hosting**. Để nhận diện được từng **Web Site Server** phải dựa vào các thông số như **host header name, địa chỉ IP và số hiệu cổng Port**.

Tạo nhiều **Web Site** dựa vào **Host Header Names**:

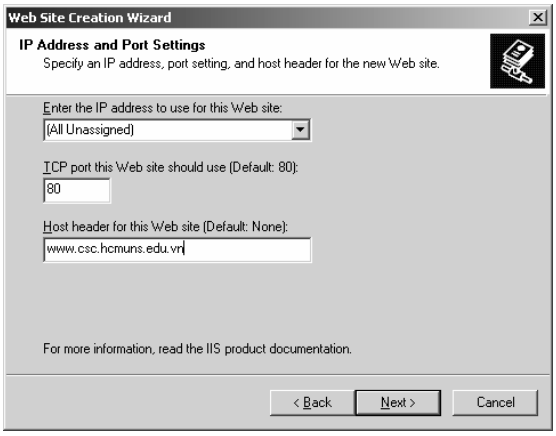
Đây là phương thức tạo nhiều **Web Site** dựa vào tên **host** , có nghĩa rằng ta chỉ cần một địa chỉ **IP** để đại diện cho tất cả các **host name**.

Các bước tạo:

- Dùng **DNS** để tạo tên (**hostname**) cho **Web Site**.
- Nhấp chuột phải vào thư mục **Web Sites** trong **IIS Manager** chọn **New**, chọn **Web Site**, tiếp theo chọn **Next**, mô tả tên (**Descriptions**) chọn **Web Site**.
- Cung cấp **host name** (Ví dụ ta nhập tên: www.csc.hcmuns.edu.vn) cho **Web Site** cần tạo trong **Textbox Host Header Name** của hộp thoại "**IP Address And Port Settings"** (tham khảo Hình 3.28).



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 3.28: Tạo **Host Header Name**.

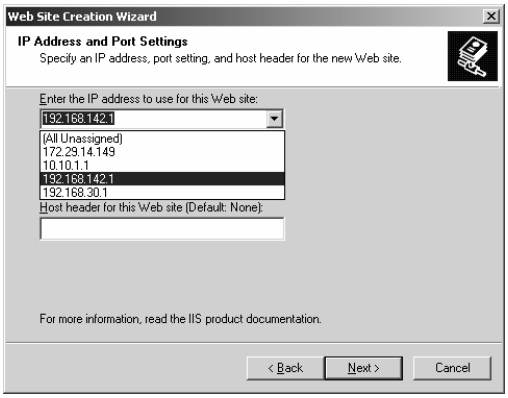
- Sau đó ta thực hiện các thao tác chọn **Home Directory**, đặt quyền hạn cho **Web Site**…Cuối cùng chọn **Finish** để hoàn tất quá trình.

Tạo nhiều **Web Site** dựa vào địa chỉ **IP**

Đối với phương thức này tương ứng một tên **Web Site** ta phải cung cấp một địa chỉ **IP**. Do đó nếu như ta tạo n **Web Site** thì ta phải tạo n địa chỉ, chính vì lẽ này nên phương thức này ít sử dụng hơn phương thức 1.

Các bước tạo:

- Ta phải thêm một hoặc nhiều địa chỉ **IP** cho card mạng.
- Dùng **DNS** tạo một **hostname** tương ứng với **IP** mới vừa tạo.
- Nhấp chuột phải vào thư mục **Web Sites** trong **IIS Manager** chọn **New**, chọn **Web Site**, tiếp theo chọn **Next**, mô tả tên (**Descriptions**) chọn **Web Site**.
- Chọn một địa chỉ **IP** cụ thể cho **Web Site** cần tạo trong tùy chọn "**Enter the IP address to use for this Web site**" của hộp thoại "**IP Address And Port Settings"** (tham khảo Hình 3.29).




Hình 3.29: Chọn địa chỉ **IP** cho **Web site**.



- Sau đó ta thực hiện các thao tác chọn **Home Directory**, đặt quyền hạn cho **Web Site**…Cuối cùng chọn **Finish** để hoàn tất quá trình.

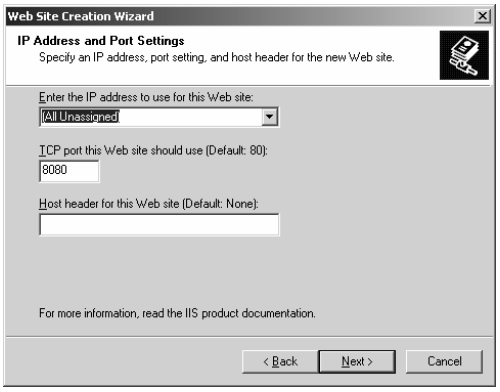
Tạo nhiều **Web Site** dựa vào **Port**.

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Mặc định **HTTP port** hoạt động trên **port 80** và **HTTPS** hoạt động trên **port 443**, thay vì mọi **Web Site** điều hoạt động trên cổng 80 hoặc 443 thì ta sẽ đổi **Web Site** hoạt động trên cổng (**port**) khác (ví dụ như 8080), vì thế ta chỉ cần dùng một địa chỉ **IP** để cung cấp cho tất cả các **Web Site**. Do đó khi ta truy xuất vào **Web Site** thì ta phải chỉ định cổng hoạt động cho dịch vụ (**http://www.csc.hcmuns.edu.vn:8080**).

Các cấu hình:

- Dùng **DNS** tạo một **hostname** tương ứng cho từng **Web Site** ánh xạ về cùng một địa chỉ **IP**.
- Nhấp chuột phải vào thư mục **Web Sites** trong **IIS Manager** chọn **New**, chọn **Web Site**, tiếp theo chọn **Next**, mô tả tên (**Descriptions**) chọn **Web Site**.
- Ta chỉ định thông số **Port** (ví dụ: **8080**) trong **Textbox** có tên "**TCP port for this Web site should use**" của hộp thoại "**IP Address And Port Settings"** (tham khảo Hình 3.30).

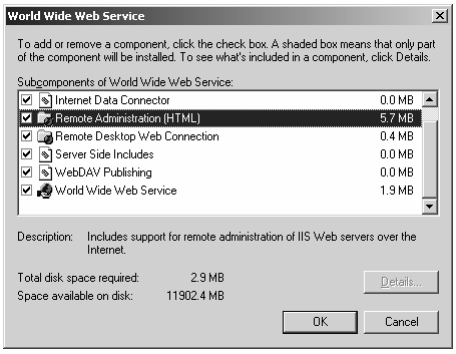



Hình 3.30: Chọn địa chỉ **IP** cho **Web Site**.

- Sau đó ta thực hiện các thao tác chọn **Home Directory**, đặt quyền hạn cho **Web Site**…Cuối cùng chọn **Finish** để hoàn tất quá trình.

### IV.2.7 Cấu hình IIS qua mạng (Web Interface for Remote Administration).

IIS cung cấp cơ chế quản trị dịch **Web** và quản trị một số tính năng cơ bản của hệ thống qua mạng, để sử dụng công cụ này ta phải cài thêm công cụ **Remote Administration (HTML)**






Hình 3.31: Cài đặt công cụ quản trị.

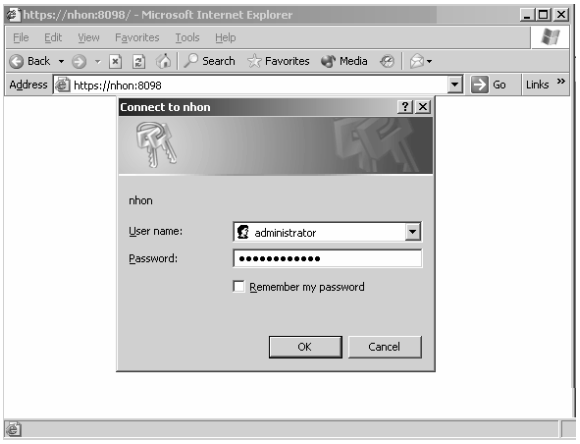
Truy cập vào **Administration Web Server** qua trình duyệt (**Web Browser**) thông qua địa chỉ **URL**: http://<Web Server>:8099 (tham khảo Hình 3.32), sau chỉ định **username**, **password** để truy xuất vào

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

**Server**.

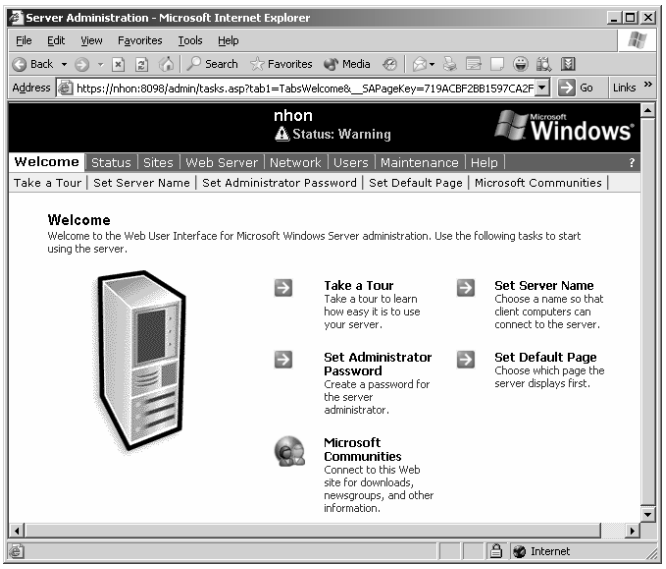


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 3.32: Truy xuất vào **Administration Web Server**.

Sau khi đăng nhập thành công, giao diện **Server Administration** hiển thị (tham khảo hình 3.33):




Hình 3.33: Giao diện quản trị hệ thống qua **Web**.

Một số chức năng chính được cung cấp trong **Administration Server**.

| Tên Tab | Chức năng |
|---|---|
| Welcome | Cho phép hiển thị lời chào, thay đổi mật khẩu của **administrator**, thay đổi tên máy,…. |
| Status | Theo dõi trạng thái của hệ thống. |
| Sites | Quản lý các **Web Site** cấu hình. |
| Web Server | Thay đổi thông tin cấu hình cho **Web Service** và **FTP Service**. |
| Network | Thay đổi thông tin cấu hình mạng cho **Server**. |



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

| | |
|---|---|
| Users | Quản lý **user**. |
| Maintenance | Cung cấp một số thao tác để duy trì và sửa lỗi cho hệ thống. |
| Help | Cung cấp các trợ giúp về cấu hình. |

### IV.2.8 Quản lý Web site bằng dòng lệnh.

1. Tạo **Web Site**.

Ta dùng lệnh **iisweb.vbs** (**file scripte** này được lưu trữ trong thư mục *systemroot*\System32) để tạo một **Web** site mới trên máy nội bộ hoặc trên máy khác là **Windows 2003 member server** chạy **IIS 6.0**.

Cú pháp lệnh:

**Iisweb.vbs** /create Path SiteName [/b Port] [/I IPAddress] [/d HostHeader] [/dontstart] [/s Computer] [/u [Domain\]User [/p password] ]

Danh sách tham số:

| Tên tham số | Ý nghĩa |
|---|---|
| Path | Chỉ định vị trí đường dẫn ổ đĩa lưu trữ nội dung Web site. |
| SiteName | Mô tả tên **Web** site. |
| /b Port | Chỉ định **TCP Port** cho **Web Site**. |
| /I IPAddress | Chỉ định địa chỉ ip cho **Web Site**. |
| /d HostHeader | Chỉ định hostheader name cho **Web Site**. |
| /dontstart | Chỉ định cho **Web Site** không khởi tạo tự động khi tạo. |
| /s Computer | Chỉ định tên máy hoặc địa chỉ **IP** trên máy ở xa (sử dụng trong trường hợp tạo mới một **Web Site** trên máy tính ở xa) |
| /u [Domain\]User | Chạy script lệnh với **username** được chỉ định, **account** này phải là thành viên của nhóm **Administrators**, mặc định chay **script** với **username** hiện hành. |
| /p password | Chỉ định mật khẩu cho **account** chỉ định trong tham số /u |

Ví dụ:

```
iisweb /create C:\Rome "My Vacations" /d www.reskit.com /dontstart
```

Hoặc dùng lệnh:

```
iisweb /create C:\New Initiatives\Marketing\HTMFiles "Marketing" /i 172.30.163.244 /s SVR01
/u Admin6 /p A76QVJ32#
```

2. Xóa **Web Site**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Cú pháp lệnh:



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

iisweb /delete WebSite [WebSite...] [/s Computer [/u [Domain\]User/p Password]]

Ví dụ:

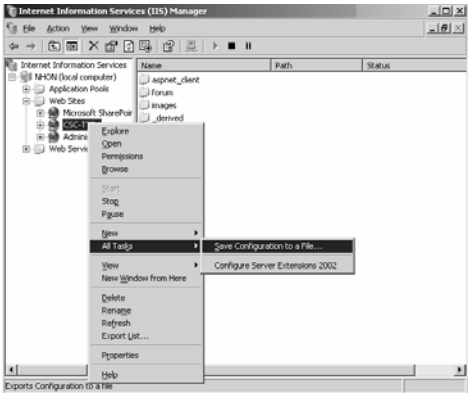
iisweb /delete "My First Novel"

### IV.2.9 Sao lưu và phục hồi cấu hình Web Site.

**IIS** lưu trữ thông tin cấu hình theo định dạng **Extensible Markup Language** (**XML**) có tên **MetaBase.xml** và **MBSchema.xml**, các tập tin này thường lưu trữ trong thư mục *systemroot*\System32\Inetsrv. Do đó người quản trị có thao tác trực tiếp vào hai tập tin này để thay đổi thông tin cấu hình về IIS.

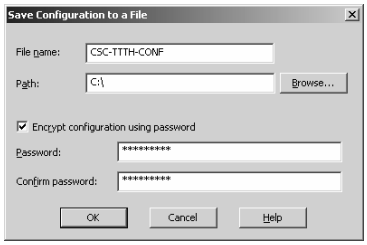
Lưu thông tin cấu hình

- Để sao lưu (**backup**) thông tin cấu hình cho **Web Site** ta nhấp chuột phải vào tên **Web Site** chọn **All Task**, chọn tiếp **Save Configuration to a file…**(tham khảo Hình 3.34)




Hình 3.34: sao lưu cấu hình Web site

- Sau đó ta chỉ định tập tin cấu hình, đường dẫn thư mục lưu trữ thông tin cấu hình, mật khẩu mã hóa cho tập tin cấu hình.




Hình 3.35: Sao lưu cấu hình **Web Site**.

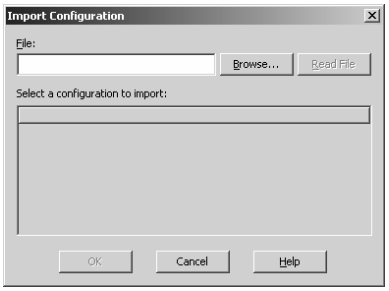
Phục hồi cấu hình **Web Site** từ file cấu hình *.XML

Để phục hồi thông tin cấu hình từ tập tin cấu hình *.xml ta thực hiện các thao thác sau:

- Nhấp chuột phải vào tên thư mục **Web Sites** chọn **New**, chọn **Web Site (from file)…** sau đó hộp thoại **Import configuration** xuất hiện (tham khảo Hình 3.36)

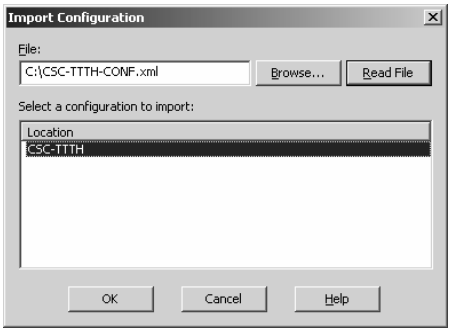


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 3.36: Phục hồi thông tin cấu hình.

- Chỉ định tập tin cấu hình từ nút Browse… sau đó nhấp chuột vào nút **Read File**, tập tin chỉ định được **Import** vào hộp thoại **Select a configuration to import**, cuối cùng chọn nút **OK** để hoàn tất quá trình (tham khảo Hình 3.37).




Hình 3.37: Phục hồi cấu hình cho Web Site.

### IV.2.10 Cấu hình Forum cho Web Site.

Trong phần này ta cấu hình một **Web** diễn đàn thảo luận **Snitz™ Forums 2000** được viết bằng ngôn ngữ **ASP** của nhóm tác giả "**Michael Anderson**, **Pierre Gorissen**, **Huw Reddick** and **Richard Kinser**", thông qua việc triển khai **forum** này giúp chúng ta phần nào hiểu được bản chất cơ bản của cơ chế cấu hình **Web** động (hỗ trợ kết nối cơ sở dữ liệu **MS Access**, **MS SQL Server**, **MySQL**) viết bằng ngôn ngữ **ASP**, **ASP.NET**, **PHP**,…Ta có thể **download forum** này từ URL: http://forum.snitz.com/.

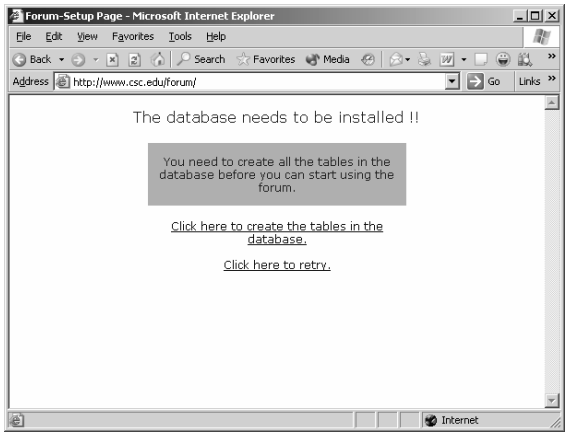
Một số bước cơ bản để cấu hình **forum**:

- Sau khi ta **download** tập tin **sf2k_v34_051.zip** (đối với phiên bản V3.4.051) hoàn tất ta giải nén và lưu trữ nội dung trong thư mục nào đó (Ví dụ C:\Inetpub\forum).
- Sau đó ta mở tập tin **config.asp** (dùng tiện ích **notepad**) để thay đổi một số thông tin cấu hình kết nối đến tập tin lưu trữ cơ sở dữ liệu **MS Access** có tên **snitz_forums_2000.mdb**
- strDBType = "access"
- strConnString="Provider=Microsoft.Jet.OLEDB.4.0;
- DataSource=" & Server.MapPath("snitz_forums_2000.mdb")
- Nếu thư mục lưu trữ nội dung của **forum** không phải là thư mục con của **WebRoot** thì ta phải tạo một **Virtual Directory** có tên **forum** để ánh xạ thư mục ổ đĩa (C:\Inetpub\forum) thành **URL Path** cho **Web Site**.



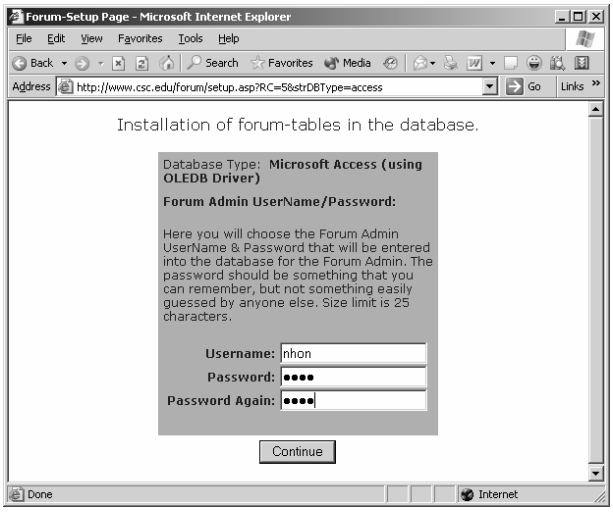
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

- Nhấp chuột phải vào **Virtual Directory** có tên **forum** chọn **Permissions** để cấp quyền cho mọi người được quyền **NTFS** là **Full** trên thư mục này.
- Sau đó ta vào **Internet Explorer** để truy xuất vào **forum** và cấu hình thêm một số thông tin mới (tham khảo Hình 3.38)




Hình 3.38: Tạo **table** cho **database**.

- Tạo **Admin Account** cho **forum**.

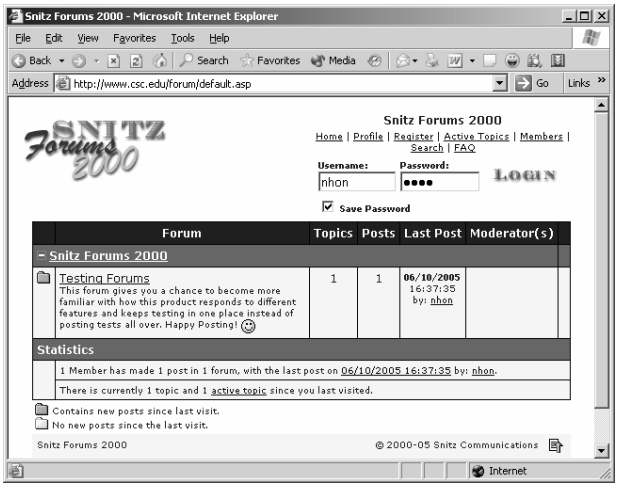



Hình 3.39: Tạo **Admin account** cho **forum**.

- Đăng nhập bằng **user** quản trị và tổ chức **forum**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 3.40: Đăng nhập **forum**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

# Tóm tắt

Lý thuyết 8 tiết - Thực hành 16 tiết

| Mục tiêu | Các mục chính | Bài tập bắt buộc | Bài tập làm thêm |
|---|---|---|---|
| Kết thúc bài học này giúp cho học viên có thể tổ chức, cài đặt, quản trị một hệ thống Mail Server phục vụ việc trao đổi thư điện tử trong hệ thống mạng nội bộ và mạng Internet. | I. Các giao thức được sử dụng trong hệ thống Mail.<br>II. Giới thiệu về hệ thống mail.<br>III. Một số khái niệm.<br>IV. Mối liên hệ giữa DNS và Mail Server.<br>V. Giới thiệu các chương trình Mail Server.<br>VI. Cài đặt Exchange 2003 Server.<br>VII. Cấu hình Microsoft Exchange 2003.<br>VIII. Một số tiện ích cần thiết của Exchange Server. | Dựa vào bài tập môn Dịch vụ mạng Windows 2003. | Dựa vào bài tập môn Dịch vụ mạng Windows 2003. |



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

# I. Các giao thức được sử dụng trong hệ thống Mail.

Hệ thống Mail được xây dựng dựa trên một số giao thức sau: **Simple Mail Transfer Protocol** (**SMTP**), **Post Office Protocol** (**POP**), **Multipurpose Internet Mail Extensions** (**MIME**) và **Interactive Mail Access Protocol** (**IMAP** ) được định trong **RFC 1176** là một giao thức quan trọng được thiết kế để thay thế **POP**, nó cung cấp nhiều cơ chế tìm kiếm văn bản, phân tích **message** từ xa mà ta không tìm thấy trong **POP**..

## I.1. SMTP(Simple Mail Transfer Protocol).

**SMTP** là giao thức tin cậy chịu trách nhiệm phân phát Mail, nó chuyển Mail từ hệ thống mạng này sang hệ thống mạng khác, chuyển Mail trong hệ thống mạng nội bộ. Giao thức **SMTP** được định nghĩa trong **RFC 821**, **SMTP** là một dịch vụ tin cậy, hướng kết nối( **connection-oriented**) được cung cấp bởi giao thức **TCP**(**Transmission Control Protocol** ), nó sử dụng số hiệu cổng (**well-known port**) 25. Sau đây là danh sách các tập lệnh trong giao thức **SMTP**.

| Lệnh | Cú pháp | chức năng |
|---|---|---|
| Hello | HELO <sending-host> | Lệnh nhận diện SMTP. |
| From | MAIL FROM:<from-address> | Địa chỉ người gởi. |
| Recipient | RCPT TO:<to-address> | Địa chỉ người nhận. |
| Data | DATA | Bắt đầu gởi thông điệp. |
| Reset | RSET | Huỷ bỏ thông điệp. |
| Verify | VRFY <string> | Kiểm tra **username**. |
| Expand | EXPN <string> | Mở rộng danh sách Mail. |
| Help | HELP [string] | Yêu cầu giúp đỡ. |
| Quit | QUIT | Kết thúc phiên giao dịch **SMTP**. |

Để sử dụng các lệnh **SMTP** ta dùng lệnh telnet theo port 25 trên hệ thống ở xa sau đó gởi Mail thông qua cơ chế dòng lệnh. Kỹ thuật này thỉnh thoảng cũng được sử dụng để kiểm tra hệ thống **SMTP Server**, nhưng điều chính yếu ở đây là chúng ta sử dụng **SMTP** để minh hoạ làm cách nào Mail được gởi qua các hệ thống khác nhau. Trong ví dụ sau minh hoạ quá trình gởi Mail thông qua cơ chế dòng lệnh **SMTP**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

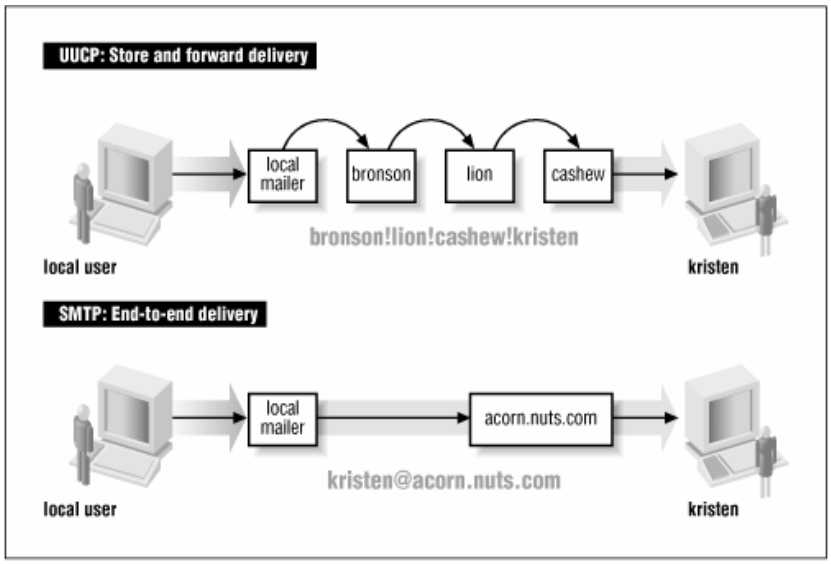

Hình 4.1: SMTP Session

Ngoài ra còn có một số lệnh khác như: **SEND**, **SOML**, **SAML**, và **TURN** được định trong **RFC 821** là những câu lệnh tuỳ chọn và không được sử dụng thường xuyên.

Lệnh **HELP** in ra tóm tắt các lệnh được thực thi. Ví dụ ta dùng lệnh **HELP RSET** chỉ định các thông tin được yêu cầu khi sử dụng lệnh **RSET**, Lệnh **VRFY** và **EXPN** thì hữu dụng hơn nhưng nó thường bị khoá vì lý do an ninh mạng bởi vì nó cung cấp cho người dùng chiếm dụng băng thông mạng. Ví dụ lênh **EXPN** <**admin**> yêu cầu liệt kê ra danh sách địa chỉ email nằm trong nhóm **Mail Admin**. Lệnh **VRFY** để lấy các thông tin cá nhân của một tài khoản nào đó, ví dụ lệnh **VRFY** <mac>, mac là một tài khoản cục bộ. Trường hợp ta dùng lệnh **VRFY** <**jane**>, **jane** là một bí danh nằm trong tập tin **aliases** thì giá trị trả về là địa chỉ Email được tìm thấy trong tập tin **aliases** này.

**SMTP** là hệ thống phân phát mail trực tiếp từ đầu đến cuối(từ nơi bắt đầu phân phát cho đến trạm phân phát cuối cùng), điều này rất hiếm khi sử dụng. hầu hết hệ thống mail sử dụng giao thức store and forward như **UUCP** và X.400, hai giao thức này di chuyển Mail đi qua mỗi hop, nó lưu trữ thông điệp tại mỗi hop và sau đó chuyển tới hệ thống tiếp theo, thông điệp đươc chuyển tiếp cho tới khi nó tới hệ thống phân phát cuối cùng.

Trong hình sau minh hoạ cả hai kỹ thuật store and forward và phân phát trực tiếp tới hệ thống Mail. Địa chỉ **UUCP** chỉ định đường đi mà Mail đi qua để tới người nhận, trong khi đó địa chỉ mail **SMTP** ngụ ý là hệ thống phân phát sau cùng.




Hình 4.2: Sơ đồ phân phối thư.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Phân phát trực tiếp(**Direct delivery**) cho phép **SMTP** phân phát mail mà không dự vào host trung gian nào. Nếu như **SMTP** phân phát bị lỗi thì hệ thống cục bộ sẽ thông báo cho người gởi hay nó đưa mail vào hàng đợi mail để phân phát sau. Bất lợi của việc phân phát trực tiếp(**direct delivery**) là nó yêu cầu hai hệ thống cung cấp đầu đủ các thông tin điều khiển mail, một số hệ thống không thể điều khiển Mail như **PC**, các hệ thống **mobile** như **laptops**, những hệ thống này thường tắt máy vào cuối ngày hay thường xuyên không trực tuyến (**mail offline**). Để điều khiển những trường hợp này cần phải có hệ thống **DNS** được sử dụng để chuyển thông điệp tới máy chủ mail thay cho hệ thống phân phát mail trực tiếp. Mail sau đó được chuyển từ **Server** tới máy trạm khi máy trạm kết nối mạng trở lại, giao thức mạng **POP** cho phép thực hiện chức năng này.

## I.2. Post Office Protocol.

**POP** là giao thức cung cấp cơ chế truy cập và lưu trữ hộp thư cho người dùng.

Có hai phiên bản của **POP** được sử dụng rộng rãi là **POP2**, **POP3**. **POP2** được định nghĩa trong **RFC 937**, **POP3** được định nghĩa trong **RFC 1725**. **POP2** sử dụng 109 và **POP3** sử dụng **Port 110**. Các câu lệnh trong hai giao thức này không giống nhau nhưng chúng cùng thực hiện chức năng cơ bản là kiểm tra tên đăng nhập và **password** của **user** và chuyển Mail của người dùng từ **Server** tới hệ thống đọc Mail cục bột của **user**.

Trong khi đó tập lệnh của **POP3** hoàn toàn khác với tập lệnh của **POP2**.

| Lệnh | Chức năng |
|---|---|
| USER username | Cho biết thông tin về **username** cần nhận Mail. |
| PASS password | Password của username cần nhận Mail. |
| STAT | Hiển thị số thông điệp chưa được đọc tính bằng bytes. |
| RETR n | Nhận thông điệp thứ n. |
| DELE n | Xoá thông điệp thứ n. |
| LAST | Hiển thị thông tin **message** cuối cùng. |
| LIST [n] | Hiển thị kích thước của thông điệp thứ n. |
| RSET | Không xoá tất cả thông điệp, và quay lại thông điệp đầu tiên. |
| TOP n | In ra các **HEADER** và dòng thứ n của thông điệp. |
| NOOP | Không làm gì. |
| QUIT | Kết thúc phiên giao dịch **POP3**. |

Mặc dù các câu lệnh của **POP3** và **POP2** khác nhau như chúng cùng thực hiện một chức năng, sau



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

đây là ví dụ về phiên giao dịch **POP3** :



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net


Hình 4.3: **POP3 Session**.

## I.3. Internet Message Access Protocol.

Là giao thức hỗ trợ việc lưu trữ và truy xuất hộp thư của người dùng, thông qua **IMAP** người dùng có thể sử dụng **IMAP Client** để truy cập hộp thư từ mạng nội bộ hoặc mạng **Internet** trên một hoặc nhiều máy khác nhau.

Một số đặc điểm chính của **IMAP**:

- Tương thích đầy đủ với chuẩn **MIME**.
- Cho phép truy cập và quản lý message từ một hay nhiều máy khác nhau.
- Hỗ trợ các chế độ truy cập "**online**", "**offline**".
- Hỗ trợ truy xuất mail đồng thời cho nhiều máy và chia sẽ **mailbox**.
- **Client** không cần quan tâm về định dạng file lưu trữ trên **Server**.

## I.4. MIME.

**MIME** (**Multipurpose Internet Mail Extensions**) cung cấp cách thức kết hợp nhiều loại dữ liệu khác nhau vào trong một thông điệp duy nhất có thể được gởi qua Internet dùng **Email** hay **Newgroup**. Thông tin được chuyển đổi theo cách này trông giống như những khối ký tự ngẫu nhiên. Những thông điệp sử dụng chuẩn **MIME** có thể chứa hình ảnh, âm thanh và bất kỳ những loại thông tin nào khác có thể lưu trữ được trên máy tính. Hầu hết những chương trình xử lý thư điện tử sẽ tự động giải mã những thông báo này và cho phép bạn lưu trữ dữ liệu chứa trong chúng vào đĩa cứng. Nhiều chương trình giải mã **MIME** khác nhau có thể được tìm thấy trên **NET**.

## I.5. X.400.

**X.400** là giao thức được **ITU-T** và **ISO** định nghĩa và đã được ứng dụng rộng rải ở Châu Âu và Canada, **X.400** cung cấp tính năng điều khiển và phân phối E-mail, **X.400** sử dụng định dạng nhị phân do đó nó không cần mã hóa nội dung khi truyền dữ liệu trên mạng.

Một số đặc điểm của giống nhau giữa **X.400** và **SMTP**.

- Cả hai đều là giao thức tin cậy (cung cấp tính năng thông báo khi gởi và nhận message).
- Cung cấp nhiều tính năng bảo mật.
- Lập lịch biểu phân phối Mail.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

- Thiết lập độ ưu tiên cho Mail.



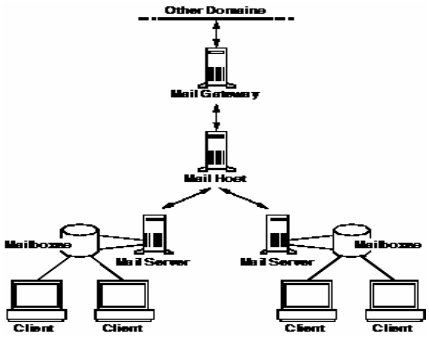
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

- **SMTP** có một số chức năng mà trên **X.400** không hỗ trợ.
- Kiểm tra địa chỉ người nhận trước khi phân phối **message** còn X.400 thì ngược lại.
- Kiểm tra kích thước của message trước khi gởi nó.
- Có khả năng chèn thêm bất kỳ loại dữ liệu nào vào **header** của **message**.
- Khả năng tương thích tốt với chuẩn **MIME**.

# II. Giới thiệu về hệ thống mail.

Một hệ thống Mail yêu cầu phải có ít nhất hai thành phần, nó có thể định vị trên hai hệ thống khác nhau hoặc trên cùng một hệ thống, **Mail Server** và **Mail Client**. Ngoài ra, nó còn có những thành phần khác như **Mail Host**, **Mail Gateway**.

Sơ đồ về một hệ thống Email đầy đủa các thành phần:




Hình 4.4: Hệ thống Mail.

## II.1. Mail gateway.

Một mail **gateway** là máy kết nối giữa các mạng dùng các giao thức truyền thông khác nhau hoặc kết nối các mạng khác nhau dùng chung giao thức. Ví dụ một **mail gateway** có thể kết nối một mạng **TCP/IP** với một mạng chạy bộ giao thức **Systems Network Architecture** (**SNA**).

Một mail gateway đơn giản nhất dùng để kết nối 2 mạng dùng chung giao thức hoặc mailer. Khi đó mail gateway chuyển mail giữa domain nội bộ và các domain bên ngoài.

## II.2. Mail Host.

Một **mail host** là máy giữ vai trò máy chủ Mail chính trong hệ thống mạng. Nó dùng như thành phần trung gian để chuyển Mail giữa các vị trí không kết nối trực tiếp được với nhau.

Mail host phân giải địa chỉ người nhận để chuyển giữa các **Mail server** hoặc chuyển đến **Mail gateway**.

Một ví dụ về **Mail host** là máy trong mạng cục bộ **LAN** có **modem** được thiết lập liên kết **PPP** hoặc **UUCP** dùng đường dây thoại. **Mail host** cũng có thể là máy chủ đóng vai trò **router** giữa mạng nội bộ và mạng **Internet**.



## II.3. Mail Server.

**Mail Server** chứa **mailbox** của người dùng. **Mail Server** nhận mail từ mail **Client** gửi đến và đưa vào

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

hàng đợi để gửi đến **Mail Host**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

**Mail Server** nhận mail từ **Mail Host** gửi đến và đưa vào **mailbox** của người dùng.

Người dùng sử dụng **NFS** (**Network File System**) để **mount** thư mục chứa **mailbox** trên **Mail Server** để đọc. Nếu **NFS** không được hỗ trợ thì người dùng phải **login** vào **Mail Server** để nhận thư.

Trong trường hợp **Mail Client** hỗ trợ **POP/IMAP** và trên **Mail Server** cũng hỗ trợ **POP/IMAP** thì người dùng có thể đọc thư bằng **POP/IMAP**.

## II.4. Mail Client.

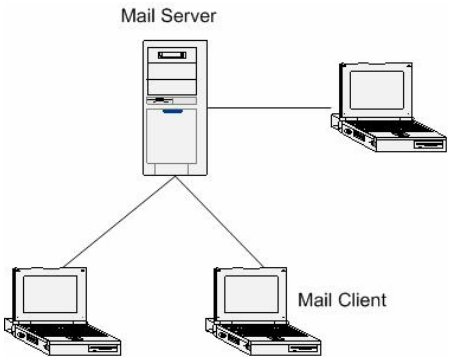
Là những chương trình hỗ trợ chức năng đọc và soạn thảo thư, **Mail Client** tích hợp hai giao thức **SMTP** và **POP**, **SMTP** hỗ trợ tính năng chuyển thư từ **Client** đến **Mail Server**, **POP** hỗ trợ nhận thư từ **Mail Server** về **Mail Client**. Ngoài giao thức việc tích hợp giao thức **POP Mail Client** còn tích hợp giao thức **IMAP**, **HTTP** để hỗ trợ chức năng nhận thư cho **Mail Client**.

Các chương trình **Mail Client** thường sử dụng như: **Microsoft Outlook Express**, **Microsoft Office Outlook**, **Eudora**,…

## II.5. Một số sơ đồ hệ thống mail thường dùng.

### II.5.1 Hệ thống mail cục bộ.

Cấu hình hệ thống Mail đơn giản gồm một hoặc nhiều trạm làm việc kết nối vào một **Mail Server**. Tất cả Mail đều chuyển cục bộ.



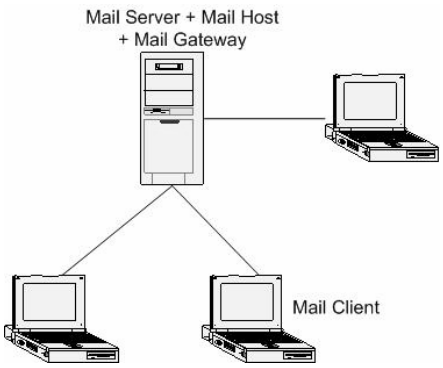

Hình 4.5: Hệ thống Mail cụ bộ.

### II.5.2 Hệ thống mail cục bộ có kết nối ra ngoài.

Hệ thống Mail trong một mạng nhỏ gồm một **Mail Server**, một **Mail Host** và một **Mail Gateway** kết nối với hệ thống bên ngoài. Không cần **DNS Server**.



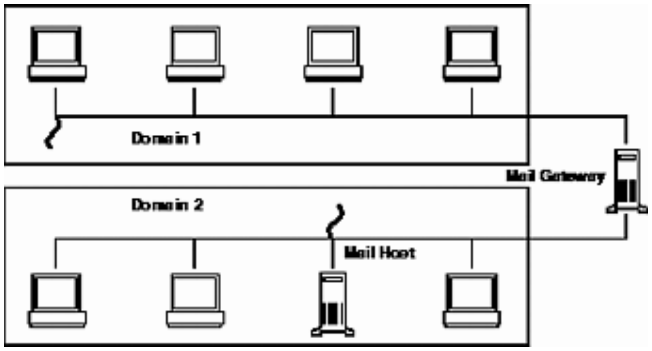
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 4.6: Hệ thống Mail có kết nối ra ngoài.

### II.5.3 Hệ thống hai domain và một gateway.

Cấu hình dưới đây gồm 2 **domain** và một **Mail Gateway**. Trong cấu hình này **Mail Server**, **Mail Host**, và **Mail Gateway** (hoặc **gateways**) cho mỗi **domain** hoạt động như một hệ thống độc lập. Để quản trị và phân phối Mail cho 2 **domain** thì dịch vụ **DNS** buộc phải có.




Hình 4.7: hệ thống kết nối mail thông qua **Mail gateway**.

# III. Một số khái niệm.

## III.1. Mail User Agent (MUA).

**MUA** : là những chương trình mà người sử dụng dùng để đọc, soạn thảo và gửi Mail.

## III.2. Mail Transfer Agent (MTA).

**MTA** : là chương trình chuyển thư giữa các máy **Mail Hub**. **Exchange** là một **Mail Transfer Agent** (**MTA**) dùng giao thức **SMTP** để đóng vai trò là một **SMTP Server** làm nhiệm vụ định tuyến trong việc phân thư . Nó nhận Mail từ những **Mail User Agent** (**MUA**) và những **MTA** khác, sau đó chuyển Mail đến đó đến các **MTA** trên máy khác hay **MTA** trên máy của mình. Để nó không đóng vai trò là một trạm phân thư đến cho người dùng, ta phải dùng một chương trình khác như **POP**, **IMAP** để thực hiện việc này.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

## III.3. Mailbox.

**Mailbox** là một tập tin lưu trữ tất cả các Mail của người dùng. Trên hệ thống **Unix**, khi ta thêm một tài khoản người dùng vào hệ thống đồng thời sẽ tạo ra một **mailbox** cho người dùng đó. Thông thường, tên của **mailbox** trùng với tên đăng nhập của người dùng. Khi có Mail gửi đến cho người dùng, chương trình xử lý Mail của **Server** cục bộ sẽ phân phối Mail này vào **mailbox** tương ứng.

Khi người dùng đăng nhập vào hệ thống và sử dụng **Mail Client** để nhận Mail (hoặc **telnet** trực tiếp vào **Mail Server** để nhận), **POP Server** sẽ vào thư mục chứa **mailbox** lấy Mail từ **mailbox** chuyển cho người dùng.

Thông thường, sau khi **Client** nhận Mail, các Mail trong **mailbox** sẽ bị xóa. Tuy nhiên, người dùng cũng có thể yêu cầu giữ lại Mail trên **mailbox**, điều này thực hiện nhờ vào một tùy chọn của **Mail Client**.

## III.4. Hàng đợi mail (mail queue).

Các Mail gởi đi có thể được chuyển đi ngay khi gởi hoặc cũng có thể được chuyển vào hàng đợi. Có nhiều nguyên nhân khiến một Mail bị giữ lại trong hàng đợi :

- Khi mail đó tạm thời chưa thể chuyển đi được hoặc có một số địa chỉ trong danh sách người nhận chưa thể chuyển đến được vào thời điểm hiện tại.
- Một số tùy chọn cấu hình yêu cầu lưu trữ Mail vào hàng đợi.
- Khi số lượng tiến trình phân phối bị tắt nghẽn vượt quá giới hạn quy định.

## III.5. Alias mail.

Một số vấn đề phức tạp thường gặp trong quá trình phân thư là :

- Phân phối đến cho cùng một người qua nhiều địa chỉ khác nhau.
- Phân phối đến nhiều người nhưng qua cùng một địa chỉ.
- Kết nối thư với một tập tin để lưu trữ hoặc dùng cho các mục đích khác nhau.
- Lọc thư thông qua các chương trình hay các script.

Để giải quyết các vấn đề trên ta phải sử dụng **Alias**. **Alias** là sự thay thế một địa chỉ người nhận bằng một hay nhiều địa chỉ khác, địa chỉ dùng thay thế có thể là một người nhận, một danh sách người nhận, một chương trình, một tập tin hay là sự kết hợp của những loại này.

# IV. Mối liên hệ giữa DNS và Mail Server.

**DNS** và **Mail** là 2 dịch vụ có mối quan hệ mật thiết với nhau. Dịch vụ Mail dựa vào dịch vụ **DNS** để chuyển Mail từ mạng bên trong ra bên ngoài và ngược lại. Khi chuyển Mail, **Mail Server** nhờ **DNS** để tìm **MX record** để xác định máy chủ nào cần chuyển Mail đến.

Cú pháp record MX:

```
[Domain_name]  IN  MX  0  [Mail_Host]
```



Thông qua việc khai báo trên cho ta biết tương ứng với **domain_name** được ánh xạ trực tiếp vào **Mail Host** để chỉ định máy chủ nhận và xử lý Mail cho tên miền.

Ví dụ:

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

t3h.com. IN MX 0 mailserver.t3h.com.

# V. Giới thiệu các chương trình Mail Server.

Hiện tại có rất nhiều chương trình **Mail Server**, tương ứng với từng môi trường thì chỉ có một số chương trình được sử dụng thông dụng, ví dụ trên môi trường Windows:

- **Microsoft Exchange Server**: Là chương trình **Mail Server** rất thông dụng được **Microsoft** phát triển để cung cấp cho các doanh nghiệp tổ chức hệ thống thư điện tử **E-mail** cho người dùng.
- **Mdaemon**: Là chương trình **Mail Server** do công ty **Alt-N Technologies**, phát triển để hỗ trợ cho các doanh nghiệp tổ chức hệ thống thư tính điện tử (**E-mail**) cho người dùng.

# VI. Cài đặt Exchange 2003 Server.

## VI.1. Một số phiên bản chính của Exchange.

- Exchange Server 5.5
- Hoạt động trên hệ điều hành Windows NT 4 Server, Windows 2000 Server có sử dụng service pack.
- Không cần cài đặt Active Directory nhưng có thể nhân bảng dữ liệu đến Active Directory sử dụng Active Directory Connector (ADC).
- Exchange 2000 Server
- Windows 2000 Server (kèm theo Service pack 1 hoặc cao hơn)
- Có thể cài đặt trên member server hoặc domain controller.
- Exchange Server 2003
- Windows 2000 Server (yêu cầu SP3, SP4)
- Windows 2003Server
- Có thể cài đặt trên member server hoặc domain controller.

## VI.2. Yêu cầu cài đặt.

Khi cài đặt **Microsoft Exchange 2003** ta cần tham khảo bảng yêu cầu về phần cứng:

| Thành phần | Yêu cầu đề nghị |
|---|---|
| Bộ xử lý (CPU) | Pentium III 500 (Exchange Server 2003, Standard Edition)<br>Pentium III 733 (Exchange Server 2003, Enterprise Edition) |
| Hệ điều hành (OS) | Windows 2003 |
| Bộ nhớ (Memory) | 512MB |
| không gian đĩa (Disk space) | 200MB trên ổ đĩa hệ thống, 500MB trên ổ đĩa cài đặt Exchange. |



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

| | |
|---|---|
| Hệ thống tập tin (File System) | Tất cả các partition có liên qua đến Exchange phải được định dạng là NTFS. |



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Ngoài yêu cầu về phần cứng ta cần phải cài đặt thêm các dịch vụ hệ thống như:

- Microsoft .NET Framework.
- Microsoft ASP.NET.
- World Wide Web service.
- Simple Mail Transfer Protocol (SMTP) service.
- Network News Transfer Protocol (NNTP) service.

## VI.3. Kiểm tra Active directory.

Để tăng tốc quá trình cài đặt **Exchange Server** cũng như để tránh một số lỗi không cần thiết ta cần cập nhật các thông tin về **Forest** và **Domain** trong **Active Directory** thông qua hai tiện ích **ForestPrep** và **DomainPrep**. **Active Directory** lưu trữ dữ liệu trong ba phân vùng.

- **Schema partition** (phân vùng lưu trữ loại **object** và thuộc tính của **object** được lưu trữ trong **Active Directory**)
- **Configuration partition**: Phân vùng lưu trữ thông tin cấu hình.
- **Domain partition**: Lưu trữ các đối tượng trong domain (**Domain Object**) như **Users**, **Groups**,….
- **ForestPrep** cập nhật thông tin trong **schema partitions**, **configuration partitions** của **Active Directory**.
- **DomainPrep** cập nhật thông tin trong domain partition:

Để chạy **ForestPrep** bạn phải đăng nhập vào hệ thống bằng tài khoản là thành viên của nhóm **Schema Admins** và **Enterprise**. Chạy **DomainPrep** bạn phải đăng nhập vào hệ thống bằng tài khoản là thành viên của nhóm **Domain Admins group** mới có quyền chạy **DomainPrep**.

Các bước chạy **ForestPrep**:

Từ **Run command line** ta truy cập vào thư mục **\setup\i386** trên đĩa **CDROM Exchange Server 2003** thực thi lệnh "**D:\setup\i386\setup.exe**" **/ForestPrep**.

khi hộp thoại "**Microsoft Exchange Installation Wizard**" xuất hiện ta chọn **Next** để tiếp tục.

Tham khảo một số thông tin **Licenses Agreement** và chọn "**I Agree**", chọn **Next** để tiếp tục.

Chọn **Next** để tiếp tục quá trình cho tới khi hộp thoại **Finish** xuất hiện báo hiệu hoàn tất quá trình.

Các bước chạy **DomainPrep** (tương tự như các bước của **ForestPrep** nhưng ta thay đổi tùy chọn trong bước đầu tiên là **/DomainPrep**)

## VI.4. Cài đặt Microsoft Exchange 2003 Server.

Các bước cài đặt:

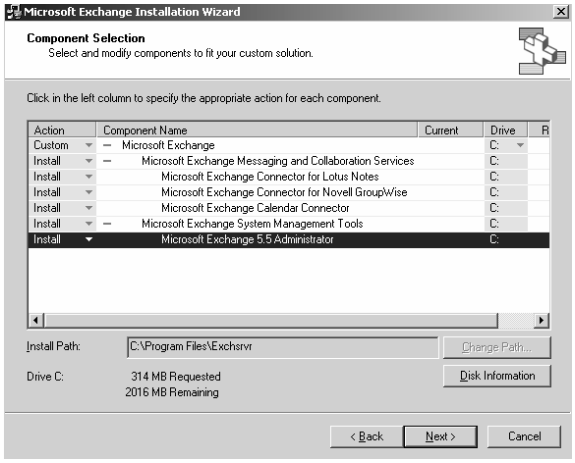
Từ **Run command line** ta truy cập vào thư mục **\setup\i386** trên đĩa **CDROM Exchange Server 2003** thực thi lệnh **D:\setup\i386\setup.exe**

Chọn tùy chọn **I Agree** trong hộp thoại **Licence Agreement**, Chọn **Next**.

Lựa chọn các thành phần cần cài đặt trong hộp thoại **"Component Seclection"**, chọn **Next**.



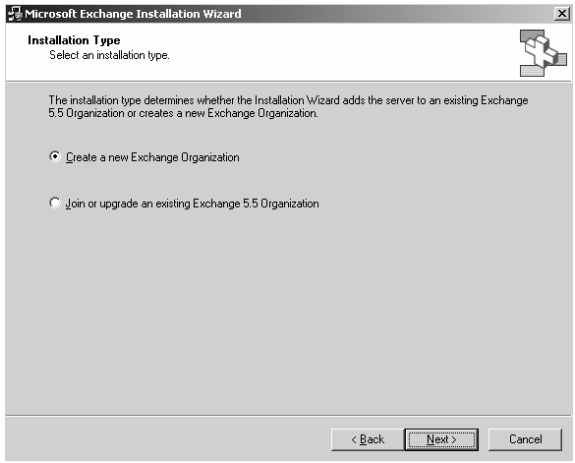
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 4.8: Lựa chọn các thành phần cài đặt cho **Exchange**.

Chọn loại cài đặt trong hộp thoại "**Installation Type**"

- Ta chỉ được chọn một trong hai tùy chọn sau:
- **Create a new Exchange Organization**: Tạo tổ chức (**Organization**) mới hoàn toàn.
- **Join or upgrade an existing Exchange 5.5 Organization** : khi ta muốn gia nhập vào nhóm **Exchange 5.5 Organization** hoặc khi ta muốn nâng cấp phiên bản **Exchange 5.5** thành **Exchange 2003**.



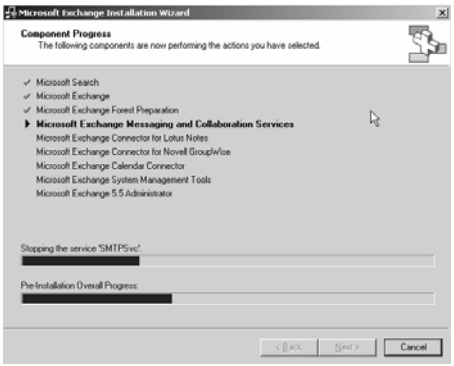

Hình 4.9: Chọn loại cài đặt.

Sau khi ta chọn "**Create a new Exchange Organization**" ở bước 4, ta phải chỉ định **Organization Name** trong hộp thoại **Organization Name**, chọn **Next** để tiếp tục.

Hộp thoại **Installation Summary** xuất hiện, tiếp tục chọn **Next** để bắt đầu tiến trình cài đặt.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 4.10: Tiến trình cài đặt **Exchange**.

# VII. Cấu hình Microsoft Exchange 2003.

## VII.1. Khởi động các dịch vụ trong Exchange 2003.

Một số dịch vụ liên quan tới **Exchange 2003 Server**:

| Tên dịch vụ | Ý nghĩa |
|---|---|
| Microsoft Exchange Event | Quản lý và theo dõi sự kiện cho **Exchange**. |
| Microsoft Exchange IMAP4 | Cung cấp dịch vụ **Internet Message Access Protocol 4** (**IMAP4**) cho Client. |
| Microsoft Exchange Information Store | Quản lý các thông tin lưu trữ cho **Exchange** như: **Mailbox** và **Public Folder**. |
| Microsoft Exchange Management | Cung cấp cơ chế quản lý **Exchange** bằng cách sử dụng **Windows Management Instrumentation** (**WMI**). |
| Microsoft Exchange MTA Stacks | Cung cấp dịch vụ **Microsoft Exchange X.400 services** được sử dụng để kết nối với **Exchange 5.5 Server** thông qua **Connector**. |
| Microsoft Exchange POP3 | Cung cấp dịch vụ **POP3** cho **Client** hỗ trợ nhận thư cho từng **Client**. |
| Microsoft Exchange Routing Engine | Cung cấp kiến trúc và thông tin định tuyến cho **Exchange 2003 Server**. |
| Microsoft Exchange Site Replication Service | Cho phép **Exchange 2003** có thể tương tích và đồng bộ dữ liệu với **Exchange 5.5**. |



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

| | |
|---|---|
| Microsoft Exchange System Attendant | Cung cấp cơ chế quan sát duy trì và tìm kiếm một số dịch vụ trong **Active Directory** ( **monitoring Services**, **connectors**, **defragmenting Exchange store**, **forwarding Active Directory**, **lookups global catalog** |



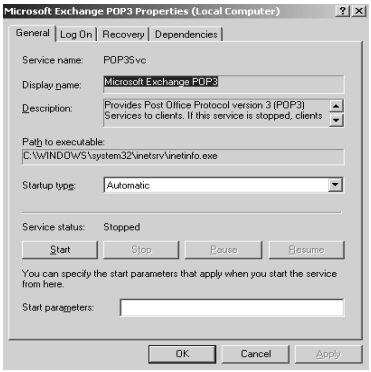
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

**server**).

| | |
|---|---|
| | |

Hoạt động của hệ thống **Exchange** phụ thuộc vào một số dịch vụ được tô đậm trong bảng trên. Các bước kích hoạt dịch vụ:

Chọn **Start | Programs | Administrative Tools | Services**, sau đó nhấp đôi vào dịch vụ cần kích hoạt, sau đó chọn **Startup type: Automatic**, chọn nút **Apply,** cuối cùng nhấp vào nút **Start** để khởi động dịch vụ.




Hình 4.11: khởi động dịch vụ **Microsoft Exchange POP3**.

## VII.2. Quản lý tài khoản mail.

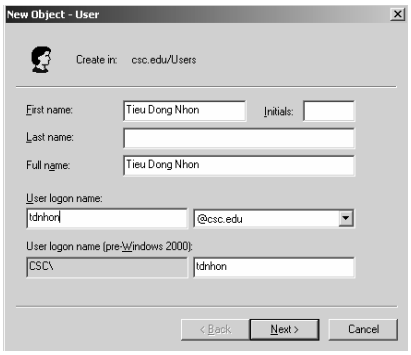
### VII.2.1 Tạo tài khoản mail.

**Mail Exchange** sử dụng **Account** của hệ thống làm **Account Mail**, để tạo **Account Mail** ta thực hiện các bước sau:

Chọn **Start** | **Programs** | **Microsoft Exchange** | **Active Directory Users and Computers**.

Chọn tên **Domain**, nhấp chuột phải vào đối tượng **Users**, chọn **New**, tiếp tục chọn **User**.

- Cung cấp các thông tin **First name**, **Initials**, **Last name** cho người dùng.
- Tên đăng đăng nhập của người dùng (**Users logon name**:)




Hình 4.12: Tạo người dùng.

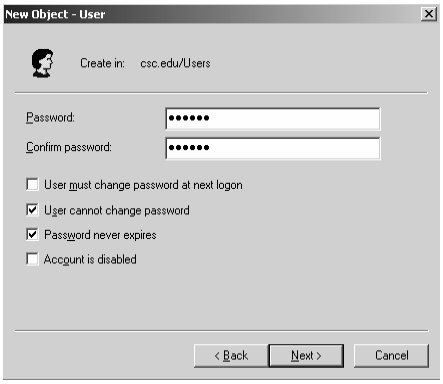


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Cung cấp thông tin mật khẩu cho tài khoản.



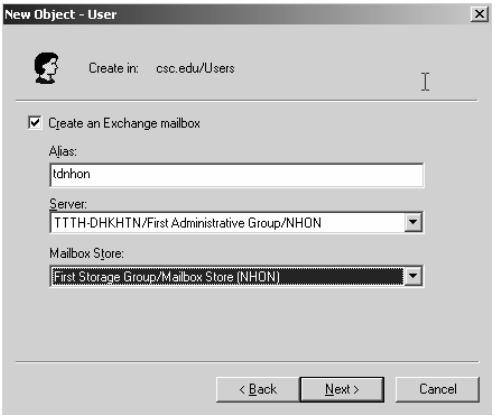
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 4.13: Đặt mật khẩu cho người dùng.

Chọn **Next** để tiếp tục

- Chọn **Create an Exchange mailbox**.
- Tạo **Alias mail** cho người dùng trong **Exchange** trong **Textbox Alias:**




Hình 4.14: Tạo **mailbox** cho người dùng.

Chọn **Next** và **Finish** để hoàn tất.

### VII.2.2 Truy cập thuộc tính của tài khoản mail.

Thông qua việc tìm hiểu thuộc tính của từng tài khoản Mail ta có thể di chuyển hoặc xóa **mailbox**, cấp nhận hạn ngạch **mailbox**, hiệu chỉnh một số thông tin cấu hình về một số tùy chọn mà Exchange gán cho tài khoản.

Một số **Tab** thuộc tính của tài khoản Mail:

| Tên Tab thuộc tính | Ý nghĩa |
|---|---|
| Exchange General | Chứa các thuộc tính **mailbox Alias**, vị trí lưu trữ **mailbox**, một số tùy chọn về giới hạn phân phối thư, giới hạn kích thước lưu trữ **mailbox**,… |
| Email Addresses | Chứa danh sách các địa chỉ mail của tài khoản được cung cấp bởi giao thức **SMTP** và các **connector** khác. |



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

| | |
|---|---|
| Exchange Features | Cung cấp một số tùy chọn để người quản trị có thể chỉ định một số |

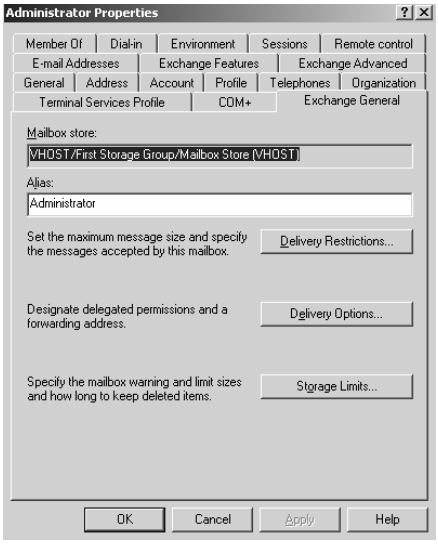


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

| | |
|---|---|
| | phương thức truy cập Mail cho tài khoản như: **Outlook web access**, **POP3**, **IMAP4**, **Outlook mobie access**,…. |
| Exchange Advanced | Hiệu chỉnh một số thuộc tính, quyền hạn về **mailbox**. |

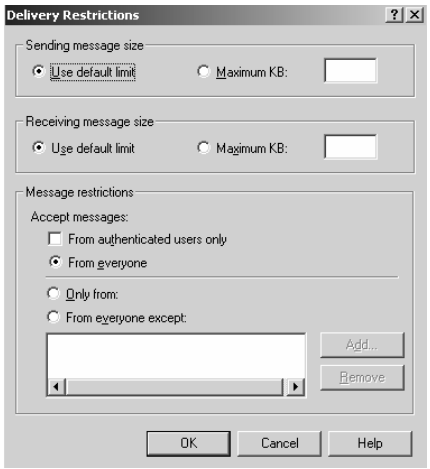
**Exchange general Tab**

Cho phép hiệu chỉnh thuộc tính **mailbox Alias**, trí lưu trữ **mailbox**, một số tùy chọn về giới hạn phân phối thư, giới hạn kích thước lưu trữ **mailbox**,…




Hình 4.15: thay đổi thông tin Mail cho người dùng.

- Đặt giới hạn về phân phối thư cho người dùng bao gồm:
- Định nghĩa kích thước của thông điệp gởi(**send message size**)
- Định nghĩa kích thước của thông điệp nhận (**receiving message size**)
- Mặc định không giới hạn nhận thư cho tài khoản (**accept message size**)

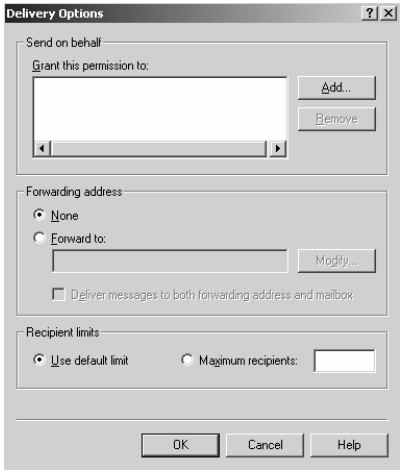



Hình 4.16: Giới hạn phân phối thư.



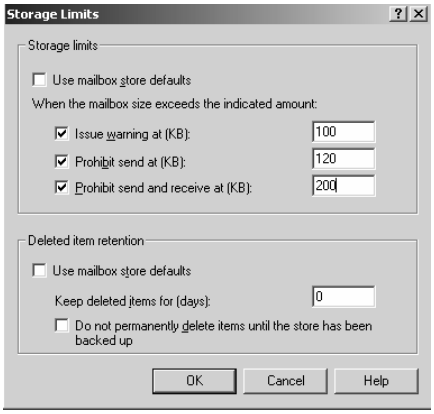
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

- Chỉ định cơ chế ủy quyền và chuyển Mail cho tài khoản.
- **Send on behalf:** chọn người dùng cần ủy quyền (nhấp chuột vào nút **Add**, chọn tên người dùng)
- **Forwarding address:** Chỉ định địa chỉ cần **forward**.
- **Recipient limits:** Chỉ định số lượng người nhận cho tài khoản.




Hình 4.17: Các tùy chọn trong phân phát thư.

- Đặt giới hạn về kích thước của **mailbox**.
- **Storage limits**: Chỉ định một số thông tin cần thiết các thao tác cần thiết hỗ trợ giới hạn lưu trữ **mailbox** của người dùng.
- **Delete item retention**: Đặt một số tùy chọn giúp duy trì hoặc xóa **mailbox** của tài khoản.



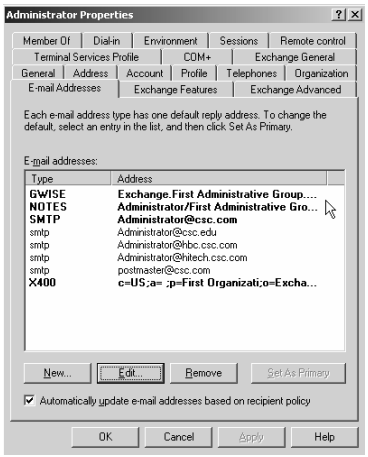

Hình 4.18: Các tùy chọn giới hạn lưu trữ thư.

**E-mail addresses Tab**

Chứa danh sách các địa chỉ Mail của tài khoản được cung cấp bởi giao thức **SMTP** và các **connector** khác, thông qua tab này giúp ta có thể tạo **alias mail** cho tài khoản.

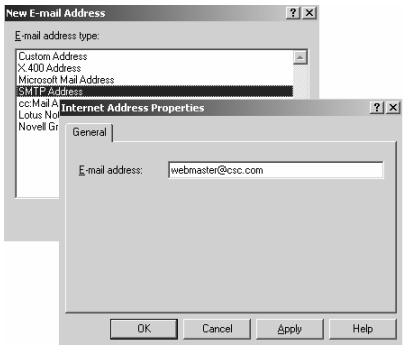


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 4.19: **E-mail addresses Tab**.

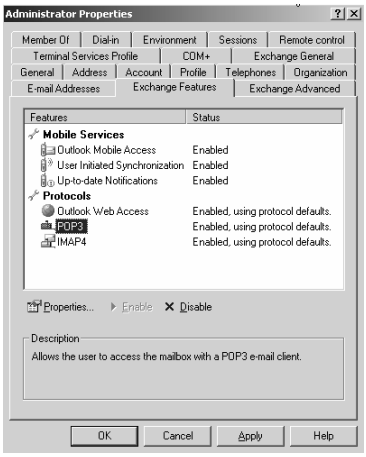
Để tạo **Alias mail** cho tài khoản ta chọn nút **New** từ **E-mail Addresses Tab**.




Hình 4.20: **E-mail addresses Tab**.

**Exchange Features Tab**

Cung cấp một số tùy chọn để người quản trị có thể chỉ định một số phương thức truy cập Mail cho tài khoản như: **Outlook Web Access**, **POP3**, **IMAP4**, **Outlook Mobie Access**,….(tham khảo Hình 4.20)




Hình 4.21: **Exchange Features Tab**.

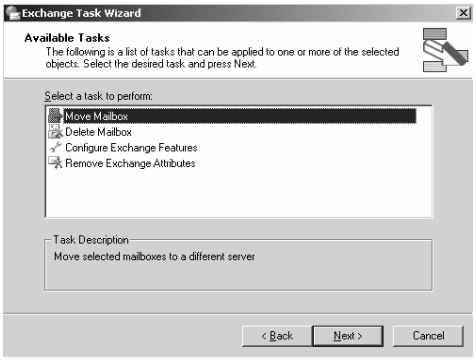


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

### VII.2.3 Một số tác vụ về tài khoản.

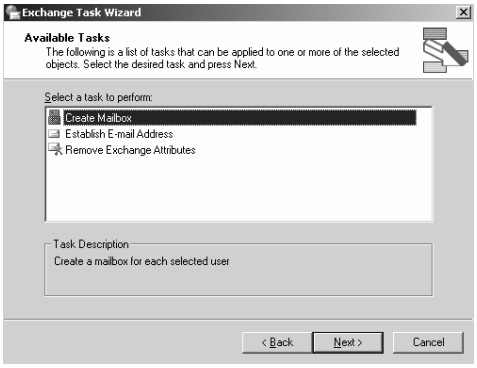
Thông qua tác vụ **Exchange Task** ta có thể xóa **mailbox**, di chuyển Mail, xóa thuộc tính Mail, cấu hình một số phương thức truy xuất Mail cho tài khoản.

Để thực thi các tác vụ về tài khoản ta nhấp chuột phải vào tên tài khoản, chọn **Exchange tasks**… xuất hiện màn hình **Welcome Exchange tasks wizard**, chọn **Next**.



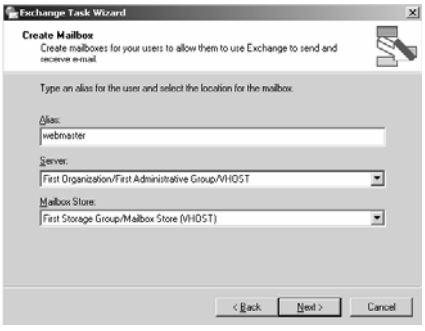

Hình 4.22: Di chuyển **mailbox**.

- Sau khi ta loại bỏ hoặc xóa địa chỉ Mail của **account** ta có thể dùng **Exchange task** để tạo Mail cho tài khoản.
- Để tạo Mail cho tài khoản ta chọn tác vụ **Create Mailbox**, chọn **Next**.




Hình 4.23: Tạo **mailbox** cho tài khoản.

- Tạo **mailbox** cho tài khoản với **mailbox alias** là **webmaster**.




Hình 4.24: Tạo **mailbox** cho tài khoản.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

- Chọn **Finish** để hoàn tất quá trình.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

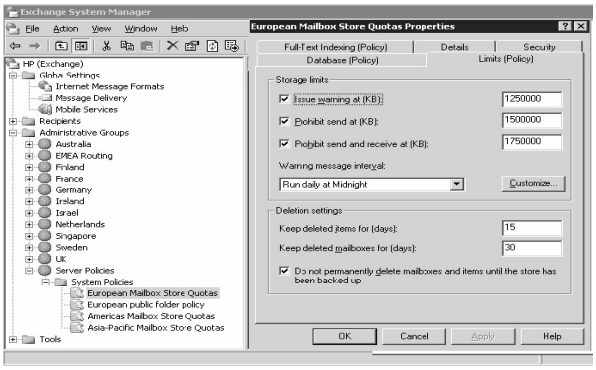
# VII.3. Administrative và routing group.

### VII.3.1 Administrative group.

Là một nhóm đối tượng của **Exchange** cùng chia sẻ chung một số quyền hạn nhất định nào đó. Thông qua Administrative group cung cấp quyền sử dụng **public folder**, đặt một số chính sách lưu trữ, quản lý các **mailbox server** trong cùng **site**,…

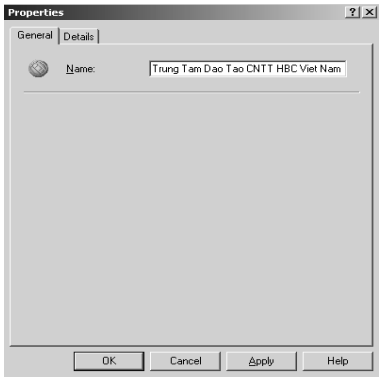
**Administrative group** chứa các nhóm:

- **Routing group:** Là nhóm chứa các **connector** hỗ trợ tính năng định tuyến thông điệp giữa các **Exchange server**.
- **System policy** : Chỉ định các chính sách về hộp thư (**mailbox**), thư mục dùng chung (**public folder**).
- **Public folder :** Thư mục dùng chung cho mọi người dùng.




Hình 4.25: Chỉ định hạn ngạch cho **mailbox**.

Ta có thể sử dụng **Administrative group** để tạo nhóm quản lý cho công ty hoặc cơ qua có nhiều chi nhánh nhằm đơn giản hóa thao tác quản lý trong tổ chức hoặc trong **Active Directory**, để tạo **administrative group** ta nhấp chuột phải vào thư mục **Administrative Groups** chọn **New**, chọn **Administrative group**…

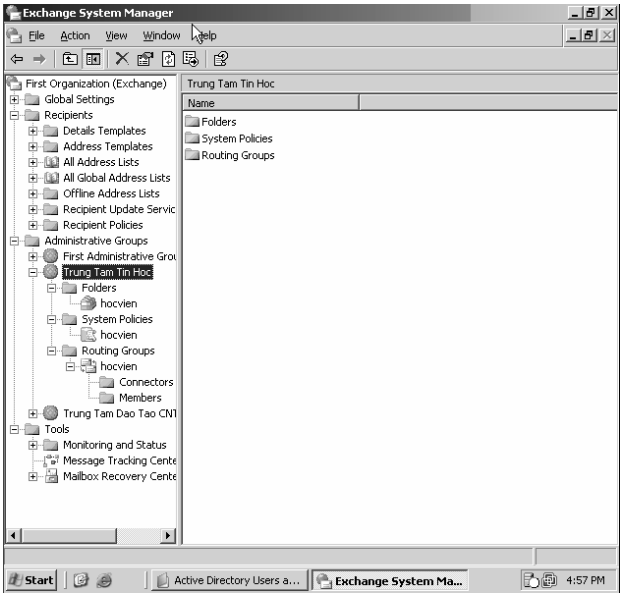



Hình 4.26: Tạo **Administrative group**.

Sau khi ta tạo xong ta cần tạo các group như: **s folder**, **security group**, **routing group**, sau đó tạo các **object** cần thiết khác,….



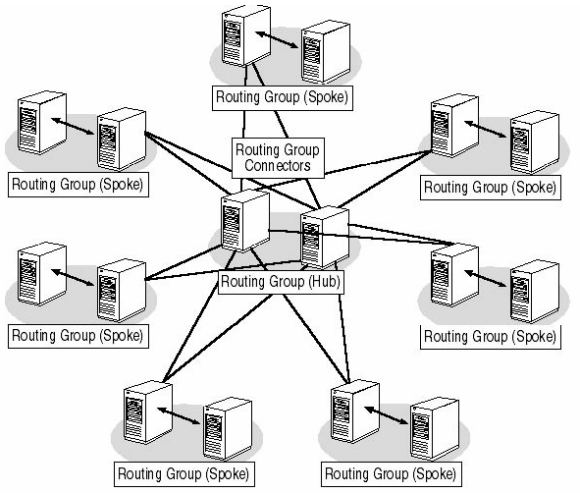
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 4.27: Một số đối tượng trong **Administrative group**.

### VII.3.2 Routing group.

**Routing group** là một nhóm các **Exchange Server** có kết nối **point to point** với nhau tạo nên một kiến trúc truyền thông điệp (**message topology**) để chỉ định phương thức chuyển thư giữa các **Exchange Server** và chuyển thư ra các tổ chức bên ngoài khi có yêu cầu.




Hình 4.28: Kiến trúc của **Routing Group**.

- **Administrative group** quản lý các đối tượng (**objects**) bao gồm **server**, **routing group**, **system policy**, **public folder**.
- **Routing group** quản lý **routing topology** hỗ trợ tính năng định tuyến thông điệp đi đến **Exchange Server** khác.
- **Routing group** là thành phần con trong **administrative group** và nó luôn luôn được tạo bên trong **administrative group**.
- Trong một tổ chức, một **administrative group** có thể chưa tất cả **routing group**, các



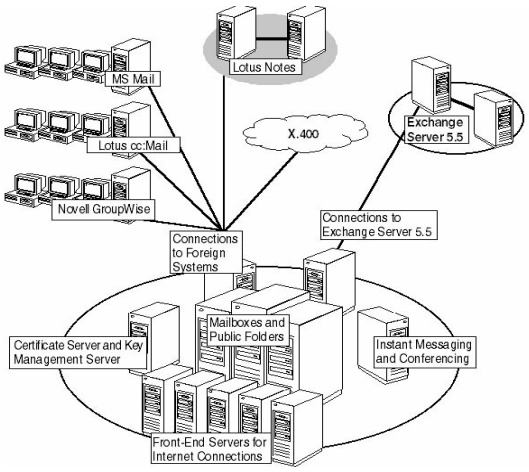
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

**administrative group** khác được sử dụng để quản lý hoạt động của **Server**.



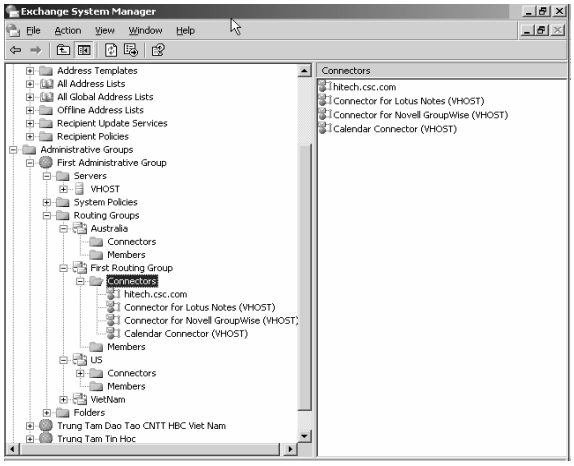
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

- **Routing group** sử dụng các **connector** để kết nối các **Exchange Server** lại với nhau tạo nên một kiến trúc định tuyến thông điệp (**routing topology**), các **connector** này bao gồm: **SMTP connector**, **X.400 connector**.




Hình 4.29: Kết nối các **Mail Server** thông qua **conectors**.

- Các yếu tố cần quan tâm khi tạo **routing group**:
- Đảm bảo tính ổn định trong kết nối mạng.
- Băng thông cần thiết cho việc thiết lập kết nối **on-demain** giữa các **Server**.
- Cần để lập lịch kết nối giữa các **Server**.
- Cần để điều khiển việc truyền **message** có kích thước lớn (>=10MB).
- Cần giới hạn kết nối cho từng **user**.




Hình 4.30: **Routing group** và các **Connector**.

Các bước để tạo **connector** kết nối **point to point** tới **Exchange Server** khác.

Nhấp chuột phải vào **Connectors**, chọn **Properties**, chọn tiếp **SMTP connector** hoặc **X.400 connector**

Chỉnh định một số thông số sau:



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

- **Name:** Chỉ định tên **connector**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

- Tùy chọn **"Use DNS to route to each address space on this connector":** cho phép ta sử dụng **DNS** để định tuyến các Mail gởi ra ngoài thông qua **SMTP connector**.
- Tùy chọn "**Forward all mail through this connector to the following smart host"** cho phép chỉ định máy chủ **mail gateway** để phân phối thư ra ngoài cho Mail nội bộ, nếu ta chỉ định địa chỉ IP thì phải chỉ định theo cú pháp [192.168.114.201], **giá trị này sẽ override lên địa chỉ smart host được chỉ định trong Delivery tab của SMTP virtual server properties**.
- **Local bridgeheads:** Chỉ định **SMTP virtual server** từ các **routing group**.
- Tùy chọn "**Do not allow public folder referrals**" không cho chuyển **public folder** qua **connector**.


Hình 4.31: Tạo **conector** cho **routing group**.

## VII.4. Microsoft Outlook Web Access.

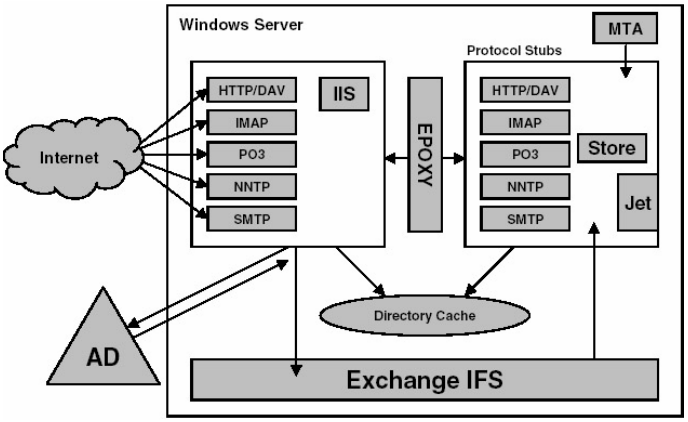
**Outlook Web Access** (**OWA**) cung cấp cho người dùng sử dụng mail qua trình duyệt **Web**. **OWA** hỗ trợ **e-mail**, **calendar**, **contact management**, **server-side rules**, **spell checking**, **junk mail processing**,…

### VII.4.1 Kiến trúc của OWA.

- Một số thành phần của **OWA** và các phương thức giao tiếp giữa **Browser** và **Exchange**.
- **Web Browser** gởi yêu cầu **HTTP request** hoặc **HTTPS request** đến **Server** thông qua **URL** (ví dụ: http://server/exchange).
- **HTTP request** sẽ được chuyển đến **IIS server** được chỉ định trong địa chỉ **URL**. **IIS Server** sẽ chuyển yêu cầu đến bộ xử lý **davex.dll** sẽ nhận và xử lý các **incoming request** cho **Exchange Application** được đăng ký trên **IIS**, tiếp theo **davex.dll** dịch các **request** và liên hệ với bộ lưu trữ dữ liệu (**Store**) thông qua kênh giao tiếp (**interprocess communication channel**) **epoxy** đến **HTTP epoxy stub**. Vì bộ giao tiếp trong (**interprocess communication**) sử dụng bộ nhớ chung (**share memory**) nên **epoxy** chỉ có thể hoạt động khi cả hai **IIS** và **Store processes** hoạt động trên cùng một máy. Mỗi giao thức có riêng một **epoxy stub** chạy trong **Store process**. **HTTP epoxy stub** lấy dữ liệu cần thiết từ bộ lưu trữ **Store** (**exoledb.dll**).
- **OWA** có thể sử dụng **ExIFS** nếu như nó muốn truy xuất thông tin từ file dữ liệu (**streaming file**). **ExIFS** có thể gởi dữ liệu trực tiếp đến **Browser**.
- **OWA** gởi dữ liệu theo định dạng **HTML** về cho **Web Browser** qua giao thức **HTTP**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 4.32: Kiến trúc của **OWA**.

### VII.4.2 Thư mục lưu trữ và Virtual Directory của OWA.

Danh sách các thư mục của **OWA** được lưu trữ tại **Program Files\ Exchsrvr\Exchweb**

| Tên thư mục | Chức năng |
|---|---|
| Exchsrvr\Bin | Chứa các tập tin thực thi bên **sever-side** và các **DLL** để định các **default** template cho **HTML form**. |
| Exchsrvr\Exchweb\Bin | **Exwform.dll-handles** hiệu chỉnh định dạng xử lý. |
| Exchsrvr\Exchweb\Controls | Lưu trữ các tập tin có định dạng .css (**cascading style sheets**), **html file**, **client Jscript libraries**. Ví dụ: **OWA** sử dụng **calendarprint.css** để xem **calendar**. |
| Exchsrvr\Exchweb\Img | OWA image files. |
| Exchsrvr\exchweb\help | Chứa các tập tin trợ giúp của **OWA**. |
| Exchsrvr\exchweb\views | Chứa các **XSL style sheet files** được sử dụng để xây dựng **OWA folder views**. |

### VII.4.3 Quản trị OWA.

**Exchange Application** tự động được thêm vào to the **IIS default Web site** hỗ trợ **OWA** để hỗ trợ **Web mail** cho người dùng (tham khảo Hình 4.29).

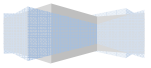
- Một số **Virtual Directory** của **Exchange Server**:
- **Exchange**: Là **Virtual Directory** để cho phép **Browser** truy xuất đến **mailboxe** của người dùng.
- **Exadmin**: là thư mục gốc lưu trữ các **ASP file** hỗ trợ cơ chế quản lý quá trình hoạt động của **Exchange Server**.
- **Public**: là thư mục gốc để cho phép **Browser** truy xuất tới **public folder**.
- **Exchweb**: lưu trữ đoạn mã của **Exchange application**.



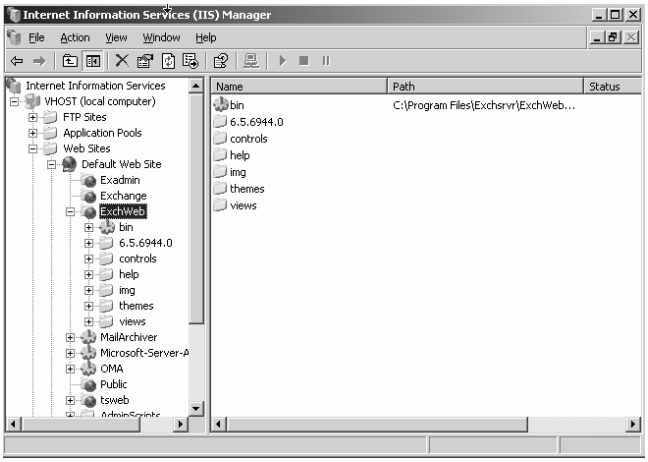
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

- **OMA** và **Microsoft-Server-Active-Sync** hỗ trợ cho **Exchange Mobile Services**.





Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 4.33: **Exchange Web**.

### VII.4.4 Sử dụng OWA.

Để sử dụng **OWA** ta phải truy xuất vào đường dẫn **URL**: http://IIS-Server/exchange.

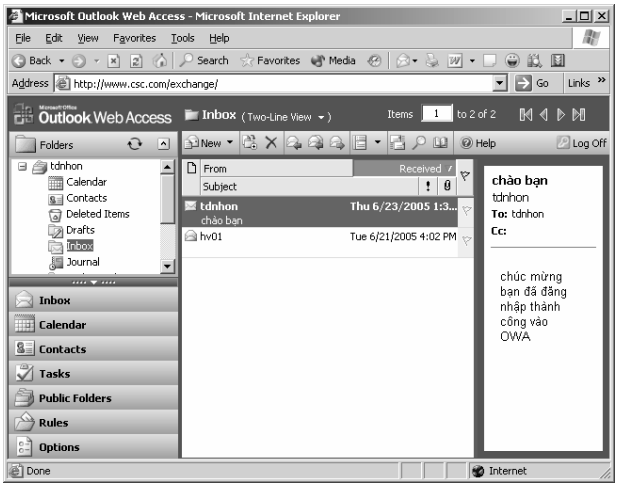
Nhập **Username** và mật khẩu đăng nhập cho **mailbox**.


Hình 4.34: Đăng nhập vào **OWA**.

Chọn **OK** sau đó sẽ hiểu thị giao diện **Web** của **OWA**.



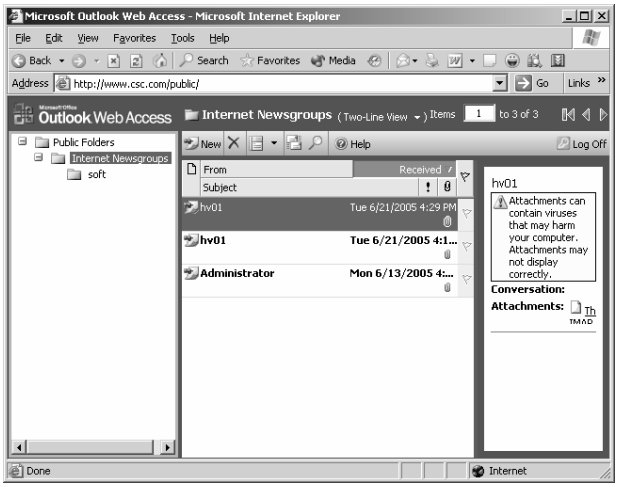
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 4.35: Giao diện sử dụng **OWA** cho **mailbox**.

Truy cập **Public folders** của **OWA**: từ giao diện **OWA** của **mailbox** ta chọn thư mục **Public Folders**

- **Public Folders** chứa danh sách các tài nguyên dùng chung cho phép mọi người dùng có thể truy cập và sử dụng.
- Thông qua **Public Folder** này cho phép các **user** cũng có thể chia sẻ tài nguyên của mình bằng cách gởi dữ liệu qua phương thức **post**.

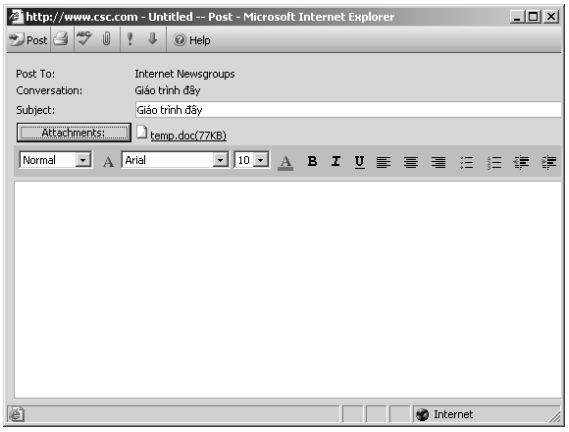



Hình 4.36: Truy cập **Public Folders**.

**Post** một **E-mail** vào **Public Folders**: Từ giao diện **Public Folders** ta chọn biểu tượng **New**, sau đó ta nhập chủ đề cần **Post**, chọn nút **Attachments** để thêm tài nguyên đính kèm, tiếp theo ta nhấp chuột vào biểu tượng **Post**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 4.37: **Post** tài nguyên vào **Public Folders**.

## VII.5. Thiết lập một số luật phân phối message.

### VII.5.1 Thiết lập bộ lọc thư.

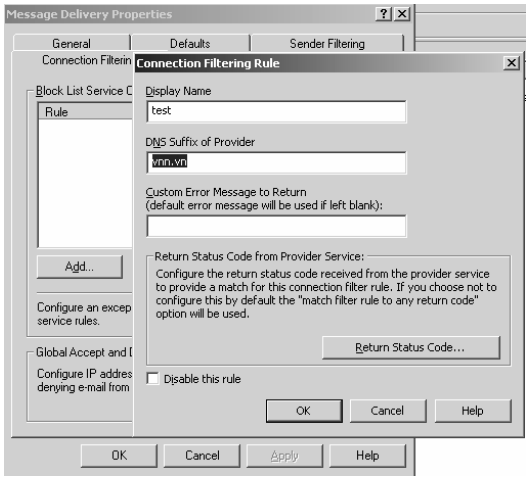
Mục đích của việc thiết lập bộ lọc thư là giới hạn việc gởi nhận thư một số người dùng và kết nối. để thiết lập bộ lọc nhấp đôi chuột vào thư mục **Global settings**, sau đó nhấp chuột phải vào **Message Delivery**,


Hình 4.38: **Message delivery**.

- **Connection Filtering**:
- Ngăn một số kết nối dịch vụ dựa vào tên miền của nhà cung cấp dịch vụ (tham khảo hình 4.37).
- Cho phép hoặc cấm **host** truy xuất vào **Mail Server** thông qua tùy chọn **Global Accept and Deny List Configuration**.

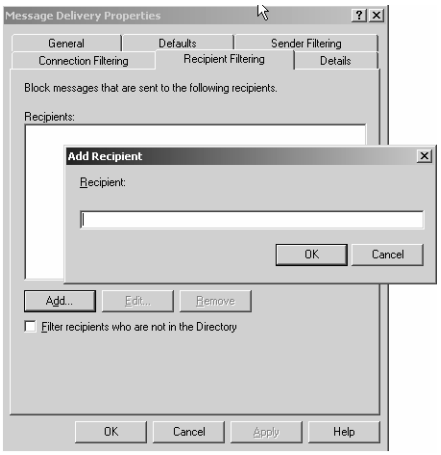


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 4.39: Thiết lậpluật cho **connection**.

- **Recipient Filtering**: Cấm một số người dùng gởi vào một đia chỉ nào đó được mô tả trong **textbox Recipients**(tham khảo Hình 4.38)

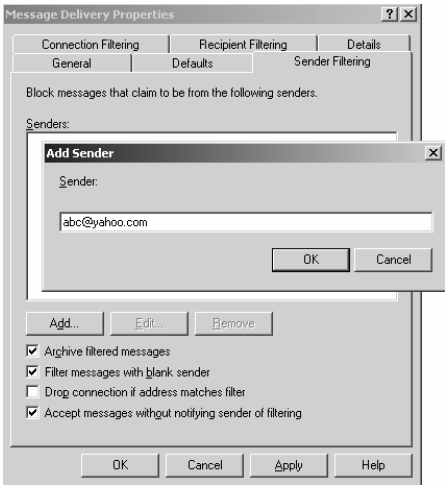



Hình 4.40: Giới hạn địa chỉ người nhận.

- **Sender Filtering**: Cấm một số người dùng gởi tới địa chỉ mail nào đó được mô tả trong **textbox Senders**.
- **Archive filrered messages**: Lưu trữ các **filter message**.
- **Filter messages with blank sender**: Lọc **message** mà không chứa địa chỉ người gởi.
- **Drop connection if address matches filter**: Hủy kết nối khi **message** thỏa bộ lọc.
- **Accept messages without notifying sender of filtering**: Lọc **message** mà không cần thông báo đến người gởi.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

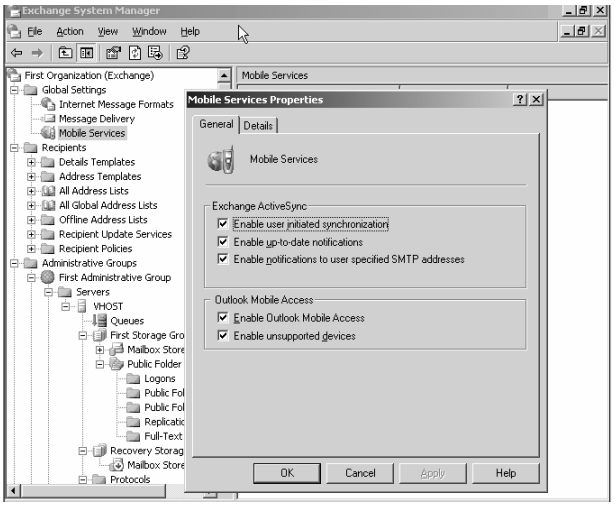



Hình 4.41: Giới hạn người gởi.

### VII.5.2 Sử dụng mail thông qua điện thoại di động.

**Exchange** tích hợp **Mobie services** để cho phép người dùng có thể dùng phương tiện di động để **check mail** (tham khảo Hình 4.40 )

- **Exchange ActiveAsync**: Cho phép một số cơ chế đồng bộ khi sử dụng thiết bị **mobie** để truy xuất **Exchange server**.
- **Outlook Mobie Access**: Cho phép thiết bị di động truy cập mail thông qua **Web** sử dụng **Outlook Mobie Access** (**OMA**), các thiết bị di động có thể truy xuất Mail thông qua địa chỉ http://mailhost/OMA.




Hình 4.42: **Mobie services**.

### VII.5.3 Relay mail.

**Relay mail** là kỹ thuật chấp nhận xử lý Mail cho một **host/subnet/domain** nào đó gởi Mail vào **SMTP Virtual Server** nội bộ, sở dĩ **SMTP Virtual Serv**er định nghĩa **relay mail** để phòng chống những **sparm mail** không cần thiết từ bên ngoài gởi đến **Mail Server** nội bộ. một số bước cấu hình **relay mail**.

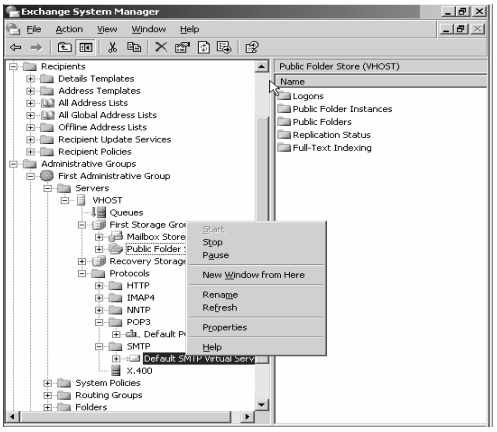


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Nhấp chuột phải vào **Default SMTP Virtual Server** chọn thuộc tính **Properties**.



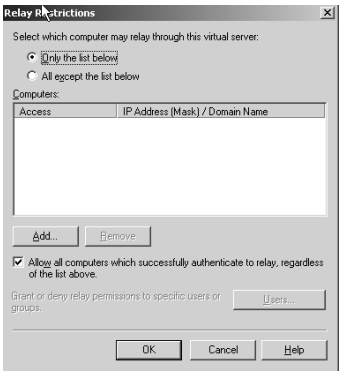
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 4.43: Cấu hình relay mail cho SMTP Server.

Chọn **Access Tab**, chọn tiếp nút **Relay**… xuất hiện hộp thoại **Relay Restrictions**, một số tùy chọn của hộp thoại.

- **Only the list below:** Chỉ cho phép **relay** cho các **host**, **subnet**, **domain** được mô tả trong **textbox Computers**.
- **All accept the list below:** Cho phép **relay** cho tất cả các **host** khác ngoại trừ các **host**. **Subnet**, **domain**.



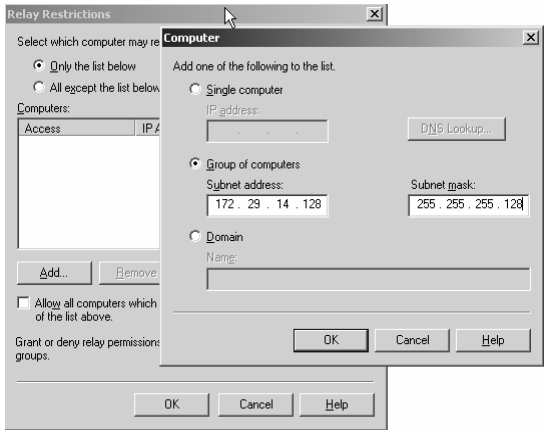

Hình 4.44: Chỉ định **relay mai**.

Ta sẽ chọn tùy chọn **"Only the list below"**, sau đó chỉ định các **host/subnet/domain** cho phép **relay**.

- **Single computer:** Relay cho host.
- **Group of computers**: Relay cho subnet.
- **Domain:** Relay cho domain.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 4.45: Chỉ định **Relay** cho **subnet** nội bộ.

Chọn nút **OK** để hoàn tất quá trình

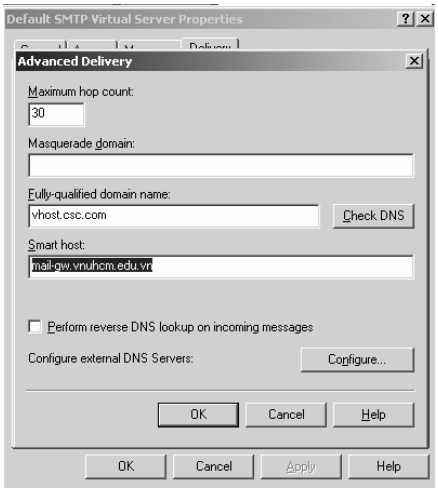
### VII.5.4 Chỉ định smart host.

Khi **SMTP Server** nhận thư nó sẽ kiểm tra xem địa chỉ của người nhận là địa chỉ thuộc **domain** trong hay **domain** ngoài, nếu địa chỉ người nhận nằm ngoài **domain** nội bộ thì **SMTP** sẽ phân phối đến **smart host** hoặc chuyển thư trực tiếp đến **Mail Server** quản lý Mail của người nhận dựa vào **MX record** thông qua **DNS Server**. Ta lưu ý rằng trong **Exchange Server** có cung cấp cơ chế chuyển Mail ra ngoài qua **connectors** trong **routing group**, nếu cả hai thông tin **connector** và **smart host** được cấu hình thì **Mail Server** sẽ ưu tiên chuyển Mail đến **connector** xử lý. Đôi khi thao tác chỉ định smart host cho mail cũng có thể được gọi thao tác chỉ định **Mail Gateway**.

Các bước chỉ định **smart host**:

Nhấp chuột phải vào **Default SMTP Virtual Server** chọn thuộc tính **Properties**.

Chọn **Delivery Tab**, sau đó chọn nút **Advanced…** xuất hiện hộp thoại **Advanced Delivery**.






Hình 4.46: Chỉ định **smart host** cho **Mail Server**.

Ta chỉ định địa chỉ **Smart host** cho **Mail Server** trong **textbox smart host**, sau đó chọn nút **OK** để hoàn tất quá trình.

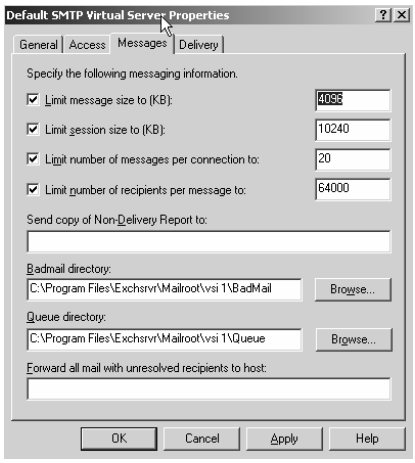
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

### VII.5.5 Định kích thước của message.

Mặc định **SMTP** không giới hạn kích thước của **message** khi gởi ra ngoài, việc giới hạn kích thước của mỗi **message** giúp cho **Mail Server** không quá tải khi xử lý, cũng như quá tải trong quá trình phân phối. Để chỉ định kích thước tối đa được phép gởi ra ngoài mạng ta thực hiện các thao tác sau:

Nhấp chuột phải vào **Default SMTP Virtual Server** chọn thuộc tính **Properties**.

Chọn **Message Tab**, sau đó ta **Check** vào mục chọn **"Limit message size to (KB):"** để chỉ định kích thước của **message**.




Hình 4.47: Giới hạn kích thước của **sending message**.

Chọn nút **OK** để hoàn tất quá trình.

## VII.6. Public Folder.

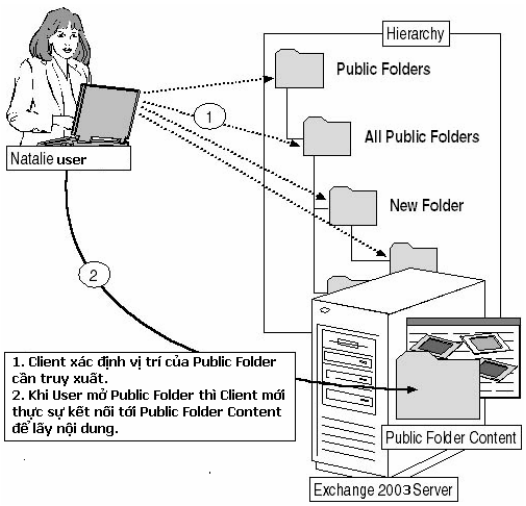
**Public folders** là thư mục chứa các thông tin dùng chung. Thông tin này thường là các **E-mail** có chứa các **multimedia clips**, **text documents**, **spreadsheets**... Người dùng có thể sử dụng chương trình **Outlook 2000**, **Internet mail clients**, **newsreaders**, và **Web browsers**, để truy xuất **Public Folder** này.

### VII.6.1 Các thành phần trong Public Folders.

**Public Folder** cung cấp hai thành phần chính: **Public folder hierarchy** và **public folder content** (Tham khảo hình 4.43). **Public folder hierarchy** lưu trữ các **Folder** theo dạng cây thư mục. **Public Folder Content** lưu trữ nội dung của thư mục bao gồm **messages**, **attachment**, **contact object**, **document**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net



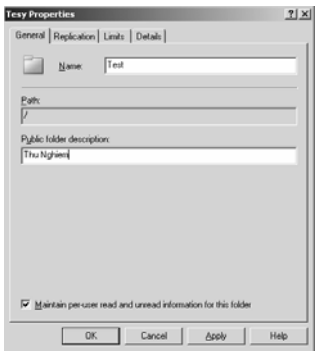

Hình 4.48: Các thành phần của **Public Folder**.

Người dùng có thể sử dụng địa chỉ **URL** http://mail_host/Public để truy xuất vào **Public Folder**, mặc định hệ thống có cung cấp sẵn thư mục **Internet Newsgroups** trong **Public Folder**. Mọi người dùng có thể gởi (Post) thông tin của mình lên **Public Folder**.

### VII.6.2 Quản lý Public Folder.

Tạo mới **Public Folder** :

- Chọn **Folders** từ **Exchange System Manager**, Nhấp chuột phải vào thư mục **Public Folders** chọn **New**, chọn **Public Folder**…
- Chỉ định **Folder Name** và **Public Folder description**.




Hình 4.49: Tạo **Public Folder**.

Quản lý thuộc tính của **Public Folder**

Thông qua việc quản lý thuộc tính của **Public Folder** ta có thể chỉ định giới hạn lưu trữ, đồng bộ dữ liệu (**replicate**), cung cấp quyền truy xuất cho người dùng truy xuất **Public Folder**,…Để truy xuất thuộc tính của **Public Folder** ta nhấp chuột phải vào tên thư mục chọn **Properties**.



- **General Tab**: Mô tả thông tin chung về **Public Folder**.
- **Replication Tab:** Chỉ định một số thông tin giúp **Public Folder** nhân bản dữ liệu lưu trữ trong một số **storage group**.

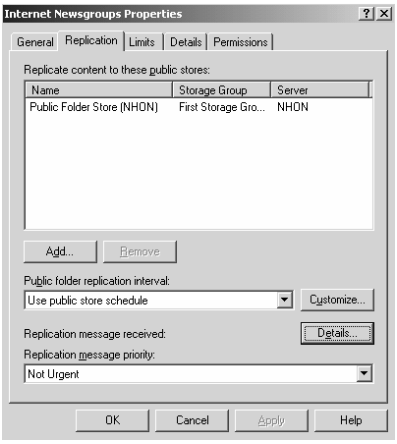
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

- **Replication content to these Public stores**: Chỉ định bộ lưu trữ cho **Public Folder**.



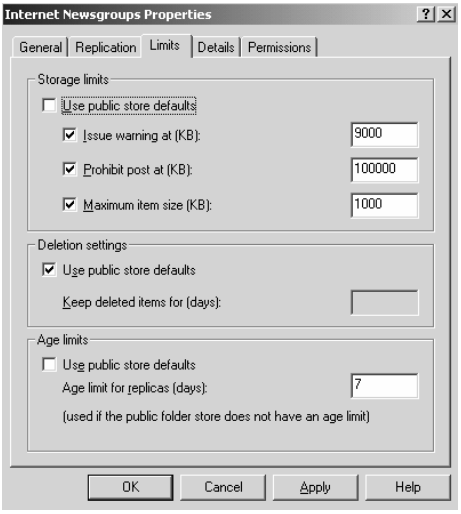
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

- **Public Folder Replication Interval**: Chỉ định lịch biểu nhân bản cho **Public Folder**, mặc định **Public Folder** được lưu trữ tại **First Storage Group** của Mail Server
- **Replication Message Priority:** Chỉ định độ ưu tiên cho quá trình nhân bản.




Hình 4.50: **Replication Public Folder**.

- **Limits Tab:** Chỉ định giới hạn dung lượng lưu trữ cho **Public Folder**:
- **Use public store defaults:** Định kích thước mặc định do hệ thống chỉ định.
- **Issue Warning at(KB):** Định kích thước cảnh báo.
- **Prohibit post at(KB):** không được phép **post** lên **Public Folder** khi kích thước đạt ngưỡng chỉ định,
- **Maximum item size(KB):** Kích thước của một **item** khi **post**.
- **Delete setting:** Chỉ định thời hạn xóa dung lượng trong **Public Folder**.
- **Age limit:** Chỉ định thời hạn **replication** dữ liệu trong **Public Folder**.




Hình 4.51: Giới hạn dung lượng lưu trữ cho **Public Folder**.

- **Details Tab:** Chỉ định một số mô tả khi cần thiết.
- **Permission Tab:** Chỉ định quyền hạn cho người dùng truy xuất vào **Public Folder** và quyền hạn



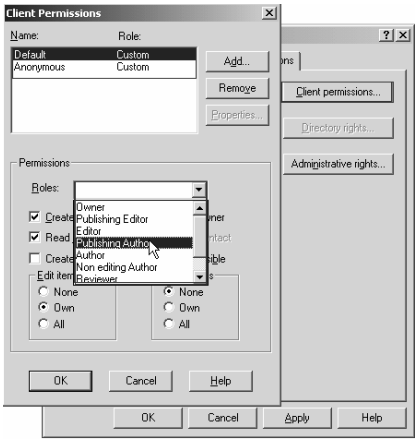
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

của người quản lý **Public Folder**. (Tham khảo Hình 4.47 )



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

- **Client Permission:** Chỉ định người dùng được quyền truy xuất vào **Public Folder**, các người dùng này được chỉ định quyền hạn cụ thể trong mục chọn **Roles,** mặc định **Public Folder** cho phép mọi người truy xuất thông qua **Username** của mình hoặc thông qua **Anonymous user**.
- **Administrator Right:** Chỉ định quyền hạn của người quản lý **Public Folder.**
-




Hình 4.52: Thay đổi thuộc tính của **Public Folder**.

## VII.7. Một số thao tác quản lý Exchange server.

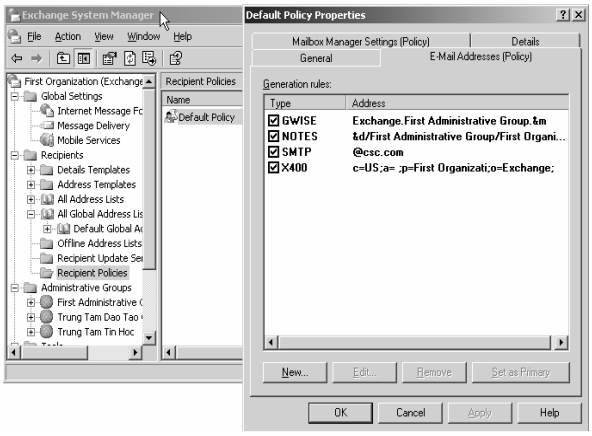
### VII.7.1 Lập chính sách nhận thư.

**Recipient policies** là tập hợp các chính sách và luật áp đặt trên tất cả các **mailbox** của người dùng bao gồm gởi thông báo đến người dùng khi xử lý thư, đặt các luật di chuyển và xóa thư của người dùng…

- Một số chức năng chính trong **Recipient policies**:
- Đặt một số chính sách về xử lý trên **mailbox**.
- Chỉ định tên **domain** cho phép **SMTP virtual server** nhận và xử lý thư thông qua **SMTP E-mail**.
- Để thay đổi một số chính sách nhận thư ta nhấp đôi chuột vào **default policy** trong thư mục **recipient policies** (tham khảo hình 3.30)
- Trong **E-mail Addresses** (**policy**) chứa một số luật được hệ thống tạo sẵn như dạng "**SMTP @csc.com**" để chỉ định **SMTP** chấp nhận xử lý **incoming mail** cho miền csc.com.
- Nút **New** để chỉ định các luật mới cần thêm vào **Generation rules.**



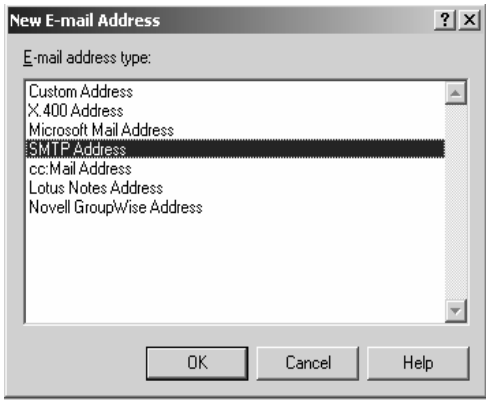
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 4.53: E-mail Addresses (policy) Tab.

Các bước tạo một **SMTP E-mail**:

Từ Hình 4.28 ta chọn New để tạo **SMTP E-mail**.



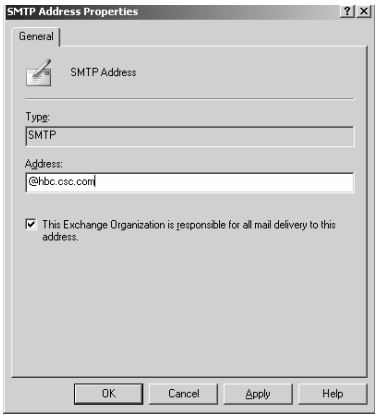

Hình 4.54: Tạo **E-mail** cho **SMTP**.

Chọn **Ok** để tiếp tục.

- Chỉ định địa chỉ mail @domain_name để cho phép **SMTP** nhận và xử lý Mail cho **domain** này.
- Chọn nút **Apply** và chọn **OK** để hoàn tất quá trình tạo **SMTP E-mail address**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 4.55: Tạo **E-mail** cho **SMTP**.

Chọn mục luật có dòng mô tả “SMTP @hbc.csc.com”.


Hình 4.56: Tạo **E-mail** cho **SMTP**.

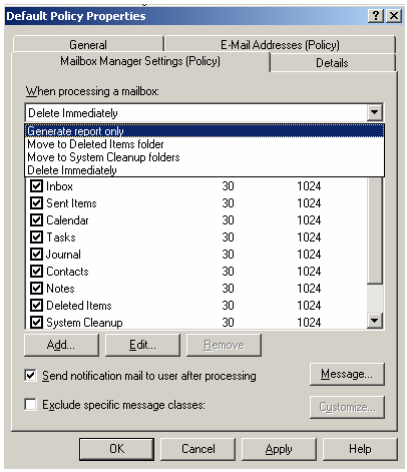
Nhấp chuột phải vào **Default Policy** chọn **Apply this policy now…** để áp đặt luật vào hệ thống.

Thiết lập luật quản lý **mailbox**: để thiết lập luật quản lý **mailbox** ta nhấp đôi chuột vào **default policy** chọn **Mailbox manager settings (policy) Tab**

- **When processing a mailbox**: Cho phép ta chọn chế độ xử lý khi **mailbox** của người dùng khi nó đạt giới hạn lưu trữ trong thời hạn mặc định là 30 ngày, với dung lượng mặc định là 1M thì sẽ:
- **Generation report only**: Gởi thông báo cho người dùng với thông điệp được chỉ định trong nút **Message**.
- **Move to Deleted Items folder**: Tự động chuyển thư đến thư mục **Deleted**.
- **Move to System Cleanup folders**: Tự động chuyển thư đến thư mục **System Cleanup**.
- **Delete Immediately**: Xóa ngay lập tức.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 4.57: Đặt luật quản lý **mailbox**.

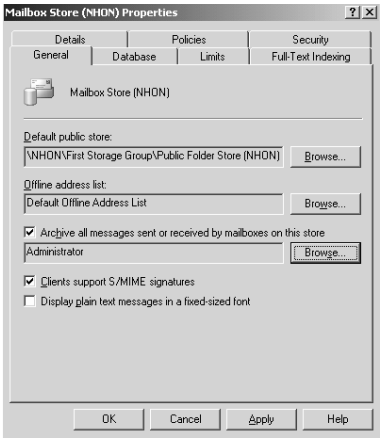
### VII.7.2 Quản lý Storage group.

**Storage group** còn gọi là bộ lưu trữ thông tin, nó lưu trữ **mailbox** và **Public Folder** của hệ thống:

**Mailbox Stores** cho phép quản lý theo dõi bộ lưu trữ **mailbox** của hệ thống.

**Public Folder Stores** cho phép quản lý và theo dõi bộ lưu trữ **Public Folder**.

- Một số thuộc tính chính của **Mailbox Store**.
- **General Tab**.
- **Default public store:** Thư mục lưu trữ **public store**.
- **Default Offline Address list: maibox** được xem như **Offline address**.
- **Archive all message sent or received by mailbox on this store:** Chỉ định phương thức ghi nhận thư gởi ra hoặc gởi vào bằng cách chép bản sao của các thư này cho **administrator**.

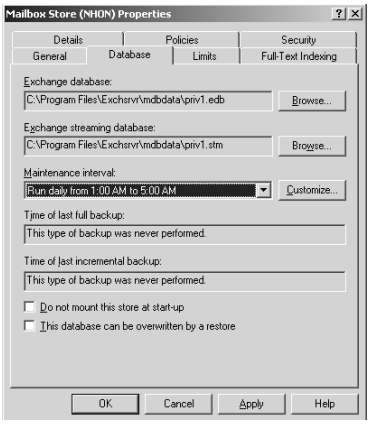



Hình 4.58: **Mailbox Store**.

- **Database Tab:** Chỉ định thư mục tập tin lưu trữ **mailbox** của người dùng (tham khảo hình 4.33).



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

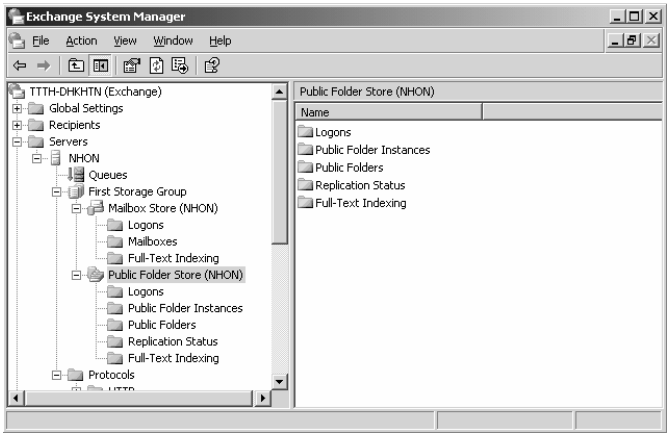



Hình 4.59: **Mailbox Database**.

- **Public Folder Stores**.

Cung cấp một số thao tác theo dõi, quản lý **public folder** của hệ thống cũng như một số dữ liệu do người dùng tạo ra, trạng thái nhân bản của **public folder**,…

- **Logons:** Hiển thị một số người dùng đang sử dụng **public folder**.
- **Public Folder Instances:** Chứa các **public folder** đang sử dụng.
- **Public Folders:** Chứa tất cả các **public folder** có sẵn trong hệ thống.
- **Replication Status:** Chứa trạng thái nhân bản của **public folder**.




Hình 4.60: **Public Folder Store**.

# VIII. Một số tiện ích cần thiết của Exchange Server.

## VIII.1. GFI MailEssentials.

**GFI MailEssentials** được tổ chức **GFI Software Ltd**. phát phát triển nhằm tích hợp thêm một số công cụ hỗ trợ công tác quản trị **Mail Server**.



- Một số đặc điểm của **GFI MailEssentials**:
- **Anti spam:** Cung cấp một số cơ chế chống **sparm mail**.
- **Company-wide disclaimer/footer text:** Được sử dụng để thêm một số thông tin chuẩn (**standard**

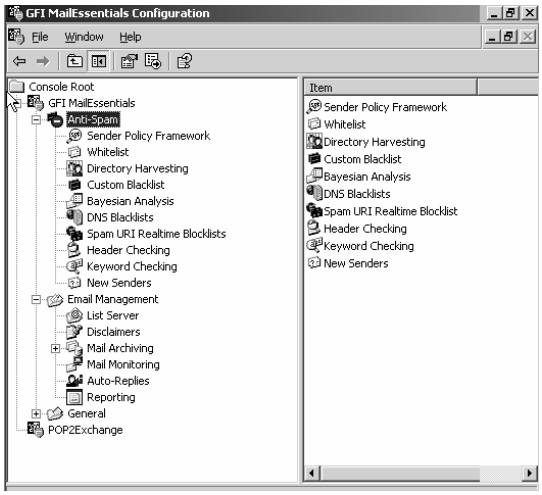
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

**corporate message**) cho **outgoing mail**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

- **Mail archiving to a database:** cho phép nhận tất cả các **inbound** và **outbound Internet mail** để ta có thể theo dõi hoặc **backup** tất cả các **E-mail** này.
- **Reporting:** Cho phép ta có thể thống kê hiện trạng sử dụng Mail của hệ thống
- **Personalized server-based auto replies with tracking number**: Cung cấp kỹ thuật tự động **reply message**.
- **POP3 downloader:** Một số **Mail Servers** như **Exchange Server** và **Lotus Notes**, không thể **download mail** từ **POP3 mailboxes**. **GFI MailEssentials** cung cấp tiện ích này để có thể chuyển Mail và phân phối Mail từ **POP3 mailboxes** tới **mailbox server** nội bộ.
- **Mail monitoring:** cung cấp một số cơ chế giúp theo dõi và giám sát hệ thống.




Hình 4.61: GFI MailEssentials.

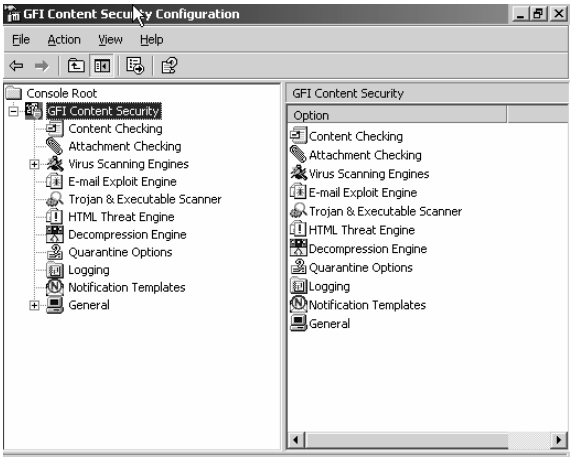
## VIII.2. GFI MailSecurity.

**GFI MailEssentials** được tổ chức **GFI Software Ltd.** phát phát triển, **GFI MailEssentials** tích hợp một số công cụ bảo mật như: **Content checking**, **Attachment Checking**, **Virus Scanning Engine**, **Trojan and Executables Scanner**,….**GFI MailSecurity** có thể được cài đặt trong hai mode: **the Exchange 2000 VS API mode** hoặc **SMTP gateway mode**. **Exchange 2000 VS API** được cài đặt và tích hợp chung với **Exchange Server 2000**. **SMTP gateway mode** thường được cài đặt trong mạng ngoại vi (**perimeter of the network**) dùng làm **mail gateway** cho các **mail host** khác.

- Một số đặc điểm chính của **GFI MailSecurity**:
- Kiểm tra và lọc nội dung thư (**Email Content checking/filtering**)
- Cung cấp bộ phân tích nội dung thư (**Email exploit detection engine**)
- Tự động loại bỏ các **HTML Scripts** (**Automatic removal of HTML scripts**)
- Tự động cô lập các **virus macros** trong các tài liệu về **Microsoft Word**.
- Cung cấp nhiều cơ chế **scanning virus** cho hệ thống (**Virus checking using multiple virus engines**)
- Trojan **Executable scanner**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 4.62: **GFI MailSecurity**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

# Tóm tắt

Lý thuyết 8 tiết - Thực hành 16 tiết

| Mục tiêu | Các mục chính | Bài tập bắt buộc | Bài tập làm thêm |
|---|---|---|---|
| Kết thúc bài học này giúp cho học viên có thể tổ chức và triển khai một Proxy Server phục vụ chia sẻ và quản lý kết nối Internet của các máy trạm, đồng thời học viên cũng có thể xây dựng một hệ thống Firewall để bảo vệ hệ thống mạng cục bộ của mình. | I. Firewall<br>II. Giới thiệu ISA 2004<br>III. Đặt điểm của ISA 2004.<br>IV. Cài đặt ISA 2004.<br>V. Cấu hình ISA Server | Dựa vào bài tập môn Dịch vụ mạng Windows 2003. | Dựa vào bài tập môn Dịch vụ mạng Windows 2003. |



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

# I. Firewall.

**Internet** là một hệ thống mở, đó là điểm mạnh và cũng là điểm yếu của nó. Chính điểm yếu này làm giảm khả năng bảo mật thông tin nội bộ của hệ thống. Nếu chỉ là mạng **LAN** thì không có vấn đề gì, nhưng khi đã kết nối **Internet** thì phát sinh những vấn đề hết sức quan trọng trong việc quản lý các tài nguyên quý giá - nguồn thông tin - như chế độ bảo vệ chống việc truy cập bất hợp pháp trong khi vẫn cho phép người được ủy nhiệm sử dụng các nguồn thông tin mà họ được cấp quyền, và phương pháp chống rò rỉ thông tin trên các mạng truyền dữ liệu công cộng (**Public Data Communication Network**).

## I.1. Giới thiệu về Firewall.

Thuật ngữ **firewall** có nguồn gốc từ một kỹ thuật thiết kế trong xây dựng để ngăn chặn, hạn chế hỏa hoạn. Trong công nghệ thông tin, **firewall** là một kỹ thuật được tích hợp vào hệ thống mạng để chống lại việc truy cập trái phép, bảo vệ các nguồn tài nguyên cũng như hạn chế sự xâm nhập vào hệ thống của một số thông tin khác không mong muốn. Cụ thể hơn, có thể hiểu **firewall** là một cơ chế bảo vệ giữa mạng tin tưởng (**trusted network**), ví dụ mạng **intranet** nội bộ, với các mạng không tin tưởng mà thông thường là **Internet**. Về mặt vật lý, firewall bao gồm một hoặc nhiều hệ thống máy chủ kết nối với bộ định tuyến (**Router**) hoặc có chức năng **Router**. Về mặt chức năng, **firewall** có nhiệm vụ:

- Tất cả các trao đổi dữ liệu từ trong ra ngoài và ngược lại đều phải thực hiện thông qua **firewall**.
- Chỉ có những trao đổi được cho phép bởi hệ thống mạng nội bộ (**trusted network**) mới được quyền lưu thông qua **firewall**.
- Các phần mềm quản lý an ninh chạy trên hệ thống máy chủ bao gồm :

Quản lý xác thực (**Authentication**): có chức năng ngăn cản truy cập trái phép vào hệ thống mạng nội bộ. Mỗi người sử dụng muốn truy cập hợp lệ phải có một tài khoản (**account**) bao gồm một tên người dùng (**username**) và mật khẩu (**password**).

Quản lý cấp quyền (**Authorization**): cho phép xác định quyền sử dụng tài nguyên cũng như các nguồn thông tin trên mạng theo từng người, từng nhóm người sử dụng.

Quản lý kiểm toán (**Accounting Management**): cho phép ghi nhận tất cả các sự kiện xảy ra liên quan đến việc truy cập và sử dụng nguồn tài nguyên trên mạng theo từng thời điểm (ngày/giờ) và thời gian truy cập đối với vùng tài nguyên nào đã được sử dụng hoặc thay đổi bổ sung …

## I.2. Kiến Trúc Của Firewall.

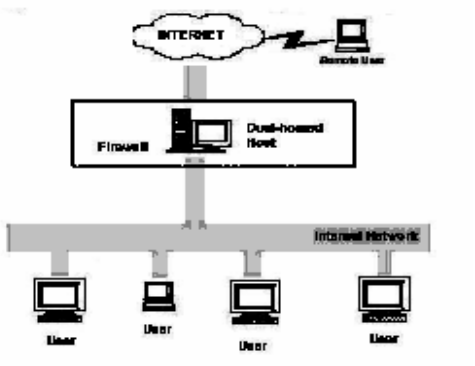
### I.2.1 Kiến trúc Dual-homed host.

**Firewall** kiến trúc kiểu ***Dual-homed host*** được xây dựng dựa trên máy tính **dual-homed host**. Một máy tính được gọi là **dual-homed host** nếu nó có ít nhất hai **network interfaces**, có nghĩa là máy đó có gắn hai card mạng giao tiếp với hai mạng khác nhau và như thế máy tính này đóng vai trò là **Router** mềm. Kiến trúc **dual-homed host** rất đơn giản. **Dual-homed host** ở giữa, một bên được kết nối với **Internet** và bên còn lại nối với mạng nội bộ (**LAN**).



**Dual-homed host** chỉ có thể cung cấp các dịch vụ bằng cách ủy quyền (**proxy**) chúng hoặc cho phép **users** đăng nhập trực tiếp vào **dual-homed host**. Mọi giao tiếp từ một **host** trong mạng nội bộ và **host** bên ngoài đều bị cấm, **dual-homed host** là nơi giao tiếp duy nhất.

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 5.1: Kiến trúc **Dual-Home Host**.

### I.2.2 Kiến trúc Screened Host.

**Screened Host** có cấu trúc ngược lại với cấu trúc **Dual-homed host**. Kiến trúc này cung cấp các dịch vụ từ một **host** bên trong mạng nội bộ, dùng một **Router** tách rời với mạng bên ngoài. Trong kiểu kiến trúc này, bảo mật chính là phương pháp ***Packet Filtering***.

**Bastion host** được đặt bên trong mạng nội bộ. **Packet Filtering** được cài trên **Router**. Theo cách này, **Bastion host** là hệ thống duy nhất trong mạng nội bộ mà những **host** trên **Internet** có thể kết nối tới. Mặc dù vậy, chỉ những kiểu kết nối phù hợp (được thiết lập trong **Bastion host**) mới được cho phép kết nối. Bất kỳ một hệ thống bên ngoài nào cố gắng truy cập vào hệ thống hoặc các dịch vụ bên trong đều phải kết nối tới host này. Vì thế **Bastion host** là host cần phải được duy trì ở chế độ bảo mật cao.

**Packet filter**ing cũng cho phép **bastion host** có thể mở kết nối ra bên ngoài. Cấu hình của **packet filtering** trên **screening router** như sau:

- Cho phép tất cả các host bên trong mở kết nối tới host bên ngoài thông qua một số dịch vụ cố định.
- Không cho phép tất cả các kết nối từ các **host** bên trong (cấm những **host** này sử dụng dịch **proxy** thông qua **bastion host**).
- Bạn có thể kết hợp nhiều lối vào cho những dịch vụ khác nhau.
- Một số dịch vụ được phép đi vào trực tiếp qua **packet filtering**.
- Một số dịch vụ khác thì chỉ được phép đi vào gián tiếp qua **proxy**.

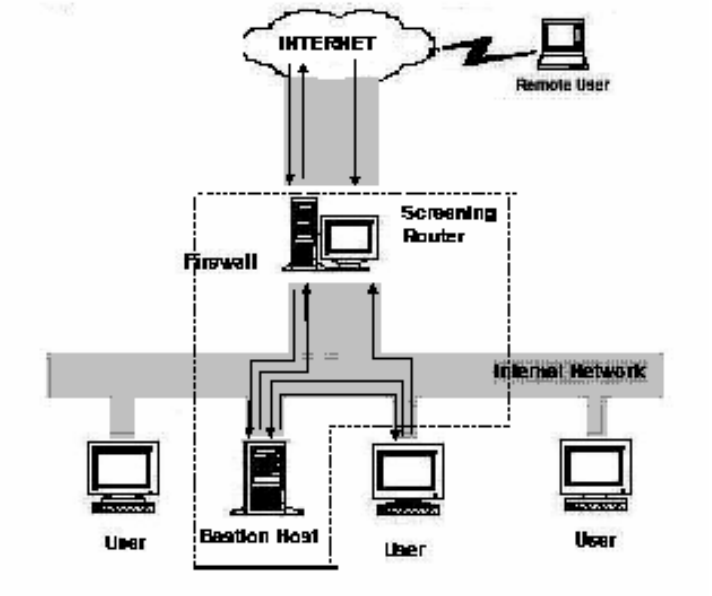
Bởi vì kiến trúc này cho phép các **packet** đi từ bên ngoài vào mạng bên trong, nó dường như là nguy hiểm hơn kiến trúc **Dual-homed host**, vì thế nó được thiết kế để không một **packet** nào có thể tới được mạng bên trong. Tuy nhiên trên thực tế thì kiến trúc **dual-homed host** đôi khi cũng có lỗi mà cho phép các **packet** thật sự đi từ bên ngoài vào bên trong (bởi vì những lỗi này hoàn toàn không biết trước, nó hầu như không được bảo vệ để chống lại những kiểu tấn công này. Hơn nữa, kiến trúc **dual-homed host** thì dễ dàng bảo vệ **Router** (là máy cung cấp rất ít các dịch vụ) hơn là bảo vệ các **host** bên trong mạng.

Xét về toàn diện thì kiến trúc ***Screened host*** cung cấp độ tin cậy cao hơn và an toàn hơn kiến trúc ***Dual-homed host***.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

So sánh với một số kiến trúc khác, chẳng hạn như kiến trúc ***Screened subnet*** thì kiến trúc **Screened host** có một số bất lợi. Bất lợi chính là nếu kẻ tấn công tìm cách xâm nhập ***Bastion Host*** thì không có cách nào để ngăn tách giữa ***Bastion Host*** và các **host** còn lại bên trong mạng nội bộ. **Router** cũng có một số điểm yếu là nếu **Router** bị tổn thương, toàn bộ mạng sẽ bị tấn công. Vì lý do này mà **Sceened *subnet*** trở thành kiến trúc phổ biến nhất.




Hình 5.2: Mô hình Screened host.

### I.2.3 Sreened Subnet.

Nhằm tăng cường khả năng bảo vệ mạng nội bộ, thực hiện chiến lược phòng thủ theo chiều sâu, tăng cường sự an toàn *cho **bastion host***, tách **bastion host** khỏi các **host** khác, phần nào tránh lây lan một khi **bastion host** bị tổn thương, người ta đưa ra kiến trúc **firewall** có tên là **Sreened Subnet**.

Kiến trúc **Screened *subnet*** dẫn xuất từ kiến trúc **screened host** bằng cách thêm vào phần an toàn: mạng ngoại vi (**perimeter network**) nhằm cô lập mạng nội bộ ra khỏi mạng bên ngoài, tách **bastion host** ra khỏi các host thông thường khác. Kiểu **screened subnet** đơn giản bao gồm hai **screened router**:

**Router** ngoài (**External router** còn gọi là **access router**): nằm giữa mạng ngoại vi và mạng ngoài có chức năng bảo vệ cho mạng ngoại vi (**bastion host**, **interior router**). Nó cho phép hầu hết những gì **outbound** từ mạng ngoại vi. Một số qui tắc **packet filtering** đặc biệt được cài đặt ở mức cần thiết đủ để bảo vệ **bastion host** và **interior router** vì **bastion host** còn là **host** được cài đặt an toàn ở mức cao. Ngoài các qui tắc đó, các qui tắc khác cần giống nhau giữa hai **Router**.

**Interior Router** (còn gọi là **choke router**): nằm giữa mạng ngoại vi và mạng nội bộ, nhằm bảo vệ mạng nội bộ trước khi ra ngoài và mạng ngoại vi. Nó không thực hiện hết các qui tắc **packet filtering** của toàn bộ **firewall**. Các dịch vụ mà **interior router** cho phép giữa **bastion host** và mạng nội bộ, giữa bên ngoài và mạng nội bộ không nhất thiết phải giống nhau. Giới hạn dịch vụ giữa **bastion host** và mạng nội bộ nhằm giảm số lượng máy (số lượng dịch vụ trên các máy này) có thể bị tấn công khi **bastion host** bị tổn thương và thoả hiệp với bên ngoài. Chẳng hạn nên giới hạn các dịch vụ được phép giữa **bastion host** và mạng nội bộ như **SMTP** khi có **Email** từ bên ngoài vào, có lẽ chỉ giới hạn

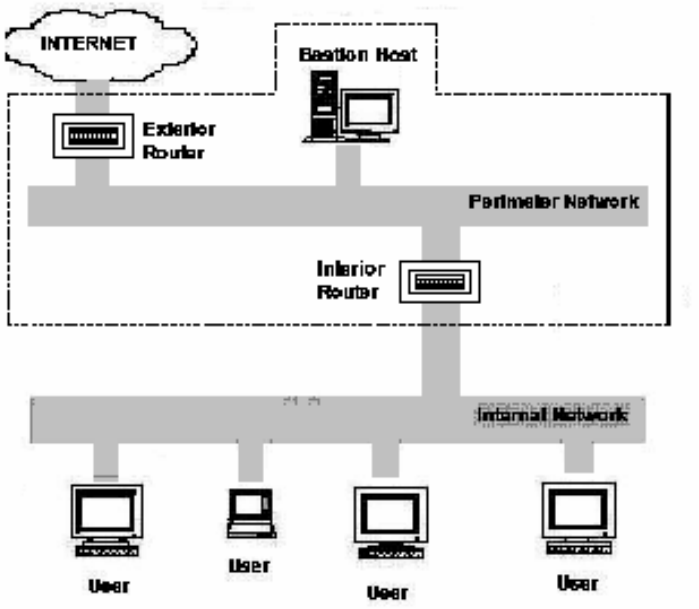


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

kết nối **SMTP** giữa **bastion host** và **Email Server** bên trong.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 5.3: Mô hình Screened Subnet.

## I.3. Các loại firewall và cách hoạt động.

### I.3.1 Packet filtering (Bộ lọc gói tin).

Loại **firewall** này thực hiện việc kiểm tra số nhận dạng địa chỉ của các **packet** để từ đó cấp phép cho chúng lưu thông hay ngăn chặn . Các thông số có thể lọc được của một **packet** như:

- Địa chỉ IP nơi xuất phát (**source IP address**).
- Địa chỉ IP nơi nhận (**destination IP address**).
- Cổng TCP nơi xuất phát (**source TCP port**).
- Cổng TCP nơi nhận (**destination TCP port**).

Loại **Firewall** này cho phép kiểm soát được kết nối vào máy chủ, khóa việc truy cập vào hệ thống mạng nội bộ từ những địa chỉ không cho phép. Ngoài ra, nó còn kiểm soát hiệu suất sử dụng những dịch vụ đang hoạt động trên hệ thống mạng nội bộ thông qua các cổng **TCP** tương ứng.

### I.3.2 Application gateway.

Đây là loại **firewall** được thiết kế để tăng cường chức năng kiểm soát các loại dịch vụ dựa trên những giao thức được cho phép truy cập vào hệ thống mạng. Cơ chế hoạt động của nó dựa trên mô hình **Proxy Service**. Trong mô hình này phải tồn tại một hay nhiều máy tính đóng vai trò **Proxy Server**. Một ứng dụng trong mạng nội bộ yêu cầu một đối tượng nào đó trên Internet, **Proxy Server** sẽ nhận yêu cầu này và chuyển đến **Server** trên **Internet**. Khi **Server** trên **Internet** trả lời, **Proxy Server** sẽ nhận và chuyển ngược lại cho ứng dụng đã gửi yêu cầu. Cơ chế lọc của **packet filtering** kết hợp với cơ chế "đại diện" của **application gateway** cung cấp một khả năng an toàn và uyển chuyển hơn, đặc biệt khi kiểm soát các truy cập từ bên ngoài.



Ví dụ: Một hệ thống mạng có chức năng **packet filtering** ngăn chặn các kết nối bằng **TELNET** vào hệ

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

thống ngoại trừ một máy duy nhất - **TELNET application gateway** là được phép. Một người muốn kết nối vào hệ thống bằng **TELNET** phải qua các bước sau:

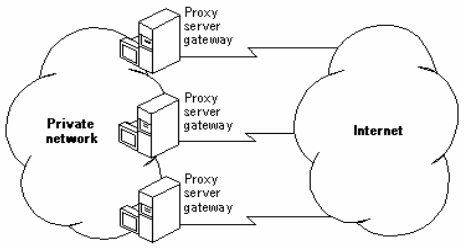


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

- Thực hiện **telnet** vào máy chủ bên trong cần truy cập.
- **Gateway** kiểm tra địa chỉ **IP** nơi xuất phát của người truy cập để cho phép hoặc từ chối.
- Người truy cập phải vượt qua hệ thống kiểm tra xác thực.
- **Proxy Service** tạo một kết nối **Telnet** giữa **gateway** và máy chủ cần truy nhập.
- **Proxy Ser**vice liên kết lưu thông giữa người truy cập và máy chủ trong mạng nội bộ.

Cơ chế bộ lọc **packet** kết hợp với cơ chế **proxy** có nhược điểm là hiện nay các ứng dụng đang phát triển rất nhanh, do đó nếu các **proxy** không đáp ứng kịp cho các ứng dụng, nguy cơ mất an toàn sẽ tăng lên.

Thông thường những phần mềm **Proxy Server** hoạt động như một **gateway** nối giữa hai mạng, mạng bên trong và mạng bên ngoài.




Hình 5.4: Mô hình hoạt động của **Proxy**.

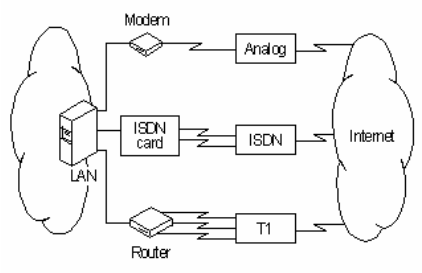
Đường kết nối giữa **Proxy Server** và **Internet** thông qua nhà cung cấp dịch vụ **Internet** (**Internet Service Provider - ISP**) có thể chọn một trong các cách sau:

- Dùng **Modem analog**: sử dụng giao thức **SLIP/PPP** để kết nối vào **ISP** và truy cập **Internet**. Dùng **dial-up** thì tốc độ bị giới hạn, thường là 28.8 Kbps - 36.6 Kbps. Hiện nay đã có **Modem analog** tốc độ 56 Kbps nhưng chưa được thử nghiệm nhiều. Phương pháp dùng **dial-up** qua **Modem analog** thích hợp cho các tổ chức nhỏ, chỉ có nhu cầu sử dụng dịch vụ **Web** và **E-Mail**.
- Dùng đường **ISDN**: Dịch vụ **ISDN** (**Integrated Services Digital Network**) đã khá phổ biến ở một số nước tiên tiến. Dịch vụ này dùng tín hiệu số trên đường truyền nên không cần **Modem analog**, cho phép truyền cả tiếng nói và dữ liệu trên một đôi dây. Các kênh thuê bao **ISDN** (đường truyền dẫn thông tin giữa người sử dụng và mạng) có thể đạt tốc độ từ 64 Kbps đến 138,24 Mbps. Dịch vụ **ISDN** thích hợp cho các công ty vừa và lớn, yêu cầu băng thông lớn mà việc dùng **Modem analog** không đáp ứng được.

Phần cứng dùng để kết nối tùy thuộc vào việc nối kết trực tiếp **Proxy Server** với **Internet** hoặc thông qua một **Router**. Dùng **dial-up** đòi hỏi phải có **Modem analog**, dùng **ISDN** phải có bộ phối ghép **ISDN** cài trên **Server**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 5.5: Mô hình kết nối mạng **Internet**.

Việc chọn lựa cách kết nối và một **ISP** thích hợp tùy thuộc vào yêu cầu cụ thể của công ty, ví dụ như số người cần truy cập **Internet**, các dịch vụ và ứng dụng nào được sử dụng, các đường kết nối và cách tính cước mà **ISP** có thể cung cấp.

# II. Giới Thiệu ISA 2004.

**Microsoft Internet Security and Acceleration Sever** (**ISA Server**) là phần mềm **share internet** của hãng phần mềm **Microsoft**, là bản nâng cấp từ phần mềm **MS ISA 2000 Server**. Có thể nói đây là một phần mềm **share internet** khá hiệu quả, ổn định, dễ cấu hình, thiết lập tường lửa (**firewall**) tốt, nhiều tính năng cho phép bạn cấu hình sao cho tương thích với mạng **LAN** của bạn. Tốc độ nhanh nhờ chế độ **cache** thông minh, với tính năng lưu **Cache** trên đĩa giúp bạn truy xuất thông tin nhanh hơn, và tính năng **Schedule Cache** (Lập lịch cho tự động **download** thông tin trên các **WebServer** lưu vào **Cache** và máy con chỉ cần lấy thông tin trên các **Webserver** đó bằng mạng **LAN**)

# III. Đặc Điểm Của ISA 2004.

Các đặc điểm của **Microsoft ISA 2004**:

- Cung cấp tính năng **Multi-networking**: Kỹ thuật thiết lập các chính sách truy cập dựa trên địa chỉ mạng, thiết lập **firewall** để lọc thông tin dựa trên từng địa chỉ mạng con,…
- **Unique per-network policies**: Đặc điểm **Multi-networking** được cung cấp trong **ISA Server** cho phép bảo vệ hệ thống mạng nội bộ bằng cách giới hạn truy xuất của các **Client** bên ngoài **internet**, bằng cách tạo ra một vùng mạng ngoại vi **perimeter network** (được xem là vùng **DMZ**, **demilitarized zone**, hoặc **screened subnet**), chỉ cho phép **Client** bên ngoài truy xuất vào các **Server** trên mạng ngoại vi, không cho phép **Client** bên ngoài truy xuất trực tiếp vào mạng nội bộ.
- **Stateful inspection of all traffic**: Cho phép giám sát tất cả các lưu lượng mạng.
- **NAT and route network relationships**: Cung cấp kỹ thuật **NAT** và định tuyến dữ liệu cho mạng con.
- **Network templates**: Cung cấp các mô hình mẫu (network templates) về một số kiến trúc mạng, kèm theo một số luật cần thiết cho network templates tương ứng.
- Cung cấp một số đặc điểm mới để thiết lập mạng riêng ảo (**VPN network**) và truy cập từ xa cho doanh nghiệp như giám sát, ghi nhận **log**, quản lý **session** cho từng **VPN Server**, thiết lập **access policy** cho từng **VPN Client**, cung cấp tính năng tương thích với **VPN** trên các hệ thống khác.
- Cung cấp một số kỹ thuật bảo mật (**security**) và thiết lập **Firewall** cho hệ thống như **Authentication**, **Publish Server**, giới hạn một số **traffic**.
- Cung cấp một số kỹ thuật **cache** thông minh (**Web cache**) để làm tăng tốc độ truy xuất mạng,



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

giảm tải cho đường truyền, **Web proxy** để chia sẻ truy xuất **Web**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

- Cung cấp một số tính năng quản lý hiệu quả như: giám sát lưu lượng, **reporting** qua **Web**, **export** và **import** cấu hình từ **XML configuration file**, quản lý lỗi hệ thống thông qua kỹ thuật gởi thông báo qua **E-mail**,..
- **Application Layer Filtering** (**ALF**): là một trong những điểm mạnh của **ISA Server 2004**, không giống như **packet filtering firewall** truyền thống, **ISA 2004** có thể thao tác sâu hơn như có thể lọc được các thông tin trong tầng ứng dụng. Một số đặc điểm nổi bậc của **ALF**:
- Cho phép thiết lập bộ lọc **HTTP inbound** và **outbound HTTP**.
- Chặn được các cả các loại tập tin thực thi chạy trên nền **Windows** như .pif, .com,…
- Có thể giới hạn **HTTP download**.
- Có thể giới hạn truy xuất **Web** cho tất cả các **Client** dựa trên nội dung truy cập.
- Có thể điều kiển truy xuất **HTTP** dựa trên chữ ký (**signature**).
- Điều khiển một số phương thức truy xuất của **HTTP**.

# IV. Cài Đặt ISA 2004.

## IV.1. Yêu cầu cài đặt.

| Thành phần | Yêu cầu đề nghị |
|---|---|
| Bộ xử lý (CPU) | **Intel** hoặc **AMD 500Mhz** trở lên. |
| Hệ điều hành (OS) | **Windows 2003** hoặc **Windows 2000** (**Service pack 4**). |
| Bộ nhớ (Memory) | 256 (MB) hoặc 512 MB cho hệ thống không sử dụng **Web caching**, **1GB** cho **Web-caching ISA firewalls**. |
| không gian đĩa (Disk space) | ổ đĩa cài đặt **ISA** thuộc loại **NTFS file system**, ít nhất còn 150 MB dành cho **ISA**. |
| NIC | Ít nhất phải có một card mạng (khuyến cáo phải có 2 NIC) |

## IV.2. Quá trình cài đặt ISA 2004.

### IV.2.1 Cài đặt ISA trên máy chủ 1 card mạng.

Khi ta cài đặt **ISA** trên máy **Server** chỉ có một card mạng (còn gọi là **Unihomed ISA Firewall**), chỉ hỗ trợ **HTTP**, **HTTPS**, **HTTP-tunneled** (**Web proxied**) **FTP**. **ISA** không hỗ trợ một số chức năng:

- SecureNAT client.
- Firewall Client.
- Server Publishing Rule.
- Remote Access VPN.
- Site-to-Site VPN.
- Multi-networking.
- Application-layer inspection ( trừ giao thức HTTP)



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Các bước cài đặt **ISA firewall** trên máy chủ chỉ có một **NIC**:



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

**Chạy tập tin isaautorun.exe** từ **CDROM ISA 2004** hoặc từ **ISA 2004 source**.

Nhấp chuột vào "**Install ISA Server 2004**" trong hộp thoại "**Microsoft Internet Security and Acceleration Server 2004**".

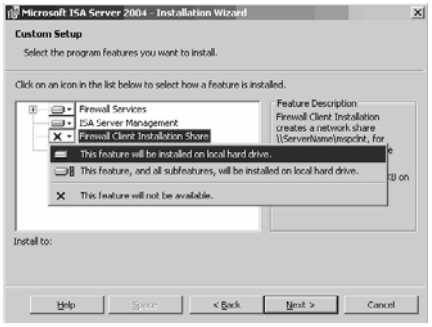
Nhấp chuột vào nút **Next** trên hộp thoại "**Welcome to the Installation Wizard for Microsoft ISA Server 2004**" để tiếp tục cài đặt.

Chọn tùy chọn **Select** "**I accept**" trong hộp thoại " **License Agreement**", chọn **Next**.

Nhập một số thông tin về tên **username** và tên tổ chức sử dụng phần mềm trong **User Name** và **Organization** textboxe. Nhập **serial number** trong **Product Serial Number textbox**. Nhấp **Next** để tiếp tục .

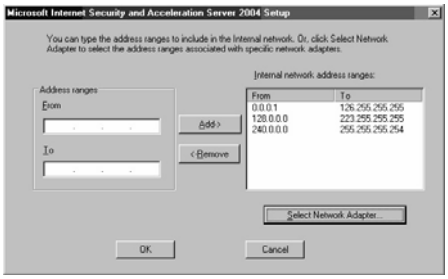
Chọn loại cài đặt (**Installation type**) trong hộp "**Setup Type"**, chọn tùy chọn **Custom,** chọn **Next.**.

trong hộp thoại "**Custom Setup"** mặc định hệ thống đã chọn **Firewall Services**, **Advanced Logging**, và **ISA Server Management**. Trên **Unihomed ISA firewall** chỉ hỗ trợ **Web Proxy Client** nên ta có thể không chọn tùy chọn **Firewall client Installation share** tuy nhiên ta có thể chọn nó để các **Client** có thể sử dụng phần mềm này để hỗ trợ truy xuất **Web** qua **Web Proxy**. Chọn **Next** để tiếp tục.




Hình 5.6: Chọn Firewall Client Installation Share.

Chỉ định **address range** cho cho **Internet network** trong hộp thoại "**Internal Network"**, sau đó chọn nút **Add**. Trong nút **Select Network Adapter, chọn Internal ISA NIC.**




Hình 5.7: Mô tả **Internal Network Range**.

Sau khi mô tả xong "**Internet Network address ranges**", chọn **Next** trong hộp thoại "**Firewall Client Connection Settings**".

Sau đó chương trình sẽ tiến hành cài đặt vào hệ thống, chọn nút **Finish** để hoàn tất quá trình.



### IV.2.2 Cài đặt ISA trên máy chủ có nhiều card mạng.

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

**ISA Firewall** thường được triển khai trên **dual-homed host** (máy chủ có hai **Ethernet cards**) hoặc **multi-homed host** (máy chủ có nhiều card mạng) điều này có nghĩa **ISA server** có thể thực thi đầy đủ các tính năng của nó như **ISA Firewall**, **SecureNAT**, **Server Publishing Rule**, **VPN**,…

Các bước cài đặt **ISA firewall software** trên **multihomed host**:

**Chạy tập tin isaautorun.exe** từ **CDROM ISA 2004** hoặc từ **ISA 2004 source**.

Nhấp chuột vào "**Install ISA Server 2004**" trong hộp thoại "**Microsoft Internet Security and Acceleration Server 2004**".

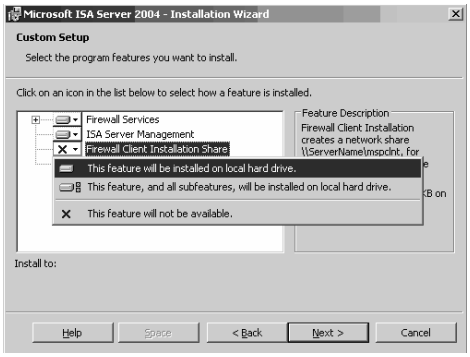
Nhấp chuột vào nút **Next** trên hộp thoại "**Welcome to the Installation Wizard for Microsoft ISA Server 2004**" để tiếp tục cài đặt.

Chọn tùy chọn **Select** "**I accept**" trong hộp thoại " **License Agreement**", chọn **Next**.

Nhập một số thông tin về tên **username** và tên tổ chức sử dụng phần mềm trong **User Name** và **Organization textboxe**. Nhập **serial number** trong **Product Serial Number textbox**. Nhấp **Next** để tiếp tục .

Chọn loại cài đặt (**Installation type**) trong hộp "**Setup Type"**, chọn tùy chọn **Custom,** chọn **Next.**

Trong hộp thoại "**Custom Setup**" mặc định hệ thống đã chọn **Firewall Services**, **Advanced Logging**, và **ISA Server Management**. Ta chọn tùy chọn **Firewall client Installation share** . Chọn **Next** để tiếp tục.



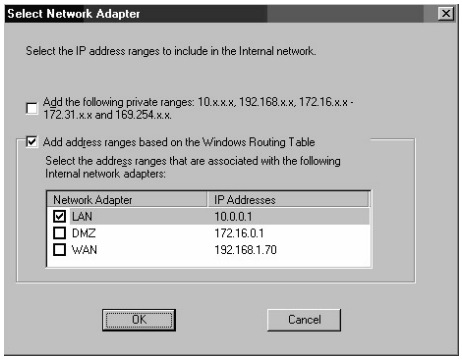

Hình 5.8: Chọn **Firewall Client Installation Share**.

Ta có hai cách Định nghĩa **internet network addresses** trong hộp thoại **Internal Network setup.** Cách thứ nhất ta mô tả dãy địa chỉ nội bộ (**Internal Network range**) từ **From** và **To text boxes**. Cách thứ hai ta cấu hình **default Internal Network** bằng cách chọn nút "**Select Network Adapter"** Sau đó ta nhấp chuột vào dấu chọn "**Select Network Adapter"** kết nối vào mạng nội bộ.

Trong hộp thoại **Configure Internal Network,** loại bỏ dấu check trong tùy chọn tên **Add the following private ranges**. Sau đó check vào mục chọn **Network Adapter**, chọn **OK**.



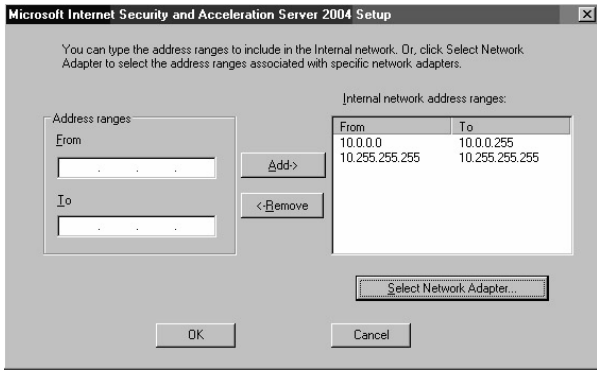
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




**Hình 5.9: Chọn Network Adapter**.

Xuất hiện thông báo cho biết **Internal network** được định nghĩa dựa vào **Windows routing table**.

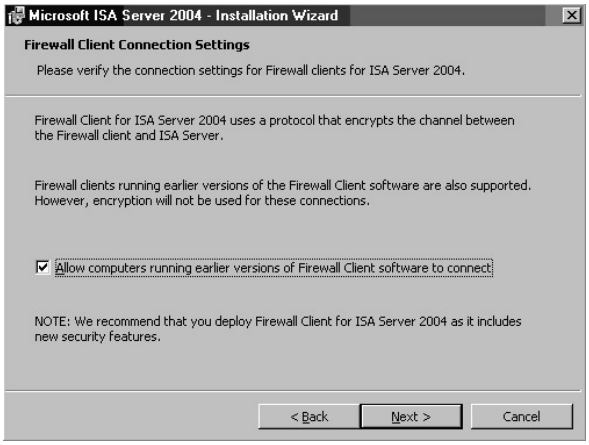
Chọn **OK** trong hộp thoại **Internal network address ranges**.




Hình 5.10: **Internal Network Address Ranges**.

Chọn **Next** trong hộp thoại "**Internal Network**" để tiếp tục quá trình cài đặt.

Chọn dấu check "**Allow computers running earlier versions of Firewall Client software to connect**" nếu ta muốn **ISA** hỗ trợ những phiên bản **Firewall client** trước, chọn **Next**.




Hình 5.11: Tùy chọn tương thích với **ISA Client**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Xuất hiện hộp thoại **Services** để cảnh báo **ISA Firewall** sẽ stop một sốdịch vụ **SNMP** và **IIS Admin Service** trong quá cài đặt. **ISA Firewall** cũng sẽ vô hiệu hóa (**disable**) **Connection Firewall** (**ICF**) / **Internet Connection Sharing** (**ICF**), và **IP Network Address Translation** (**RRAS NAT service**) **services**.

Chọn **Finish** để hoàn tất quá trình cài đặt.

# V. Cấu hình ISA Server.

## V.1. Một số thông tin cấu hình mặc định.

- Tóm tắt một số thông tin cấu hình mặc định:
- **System Policies** cung cấp sẵn một số luật để cho phép truy cập vào/ra **ISA firewall**. Tất cả các **traffic** còn lại đều bị cấm.
- Cho phép định tuyến giữa VPN/**VPN-Q Networks** và **Internal Network**.
- Cho phép **NAT** giữa **Internal Network** và **External Network**.
- Chỉ cho phép **Administrator** có thể thay đổi chính sách bảo mật cho **ISA firewall**.

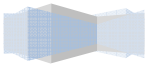
| Đặc điểm | Cấu hình mặc định (Post-installation Settings) |
|---|---|
| User permissions | Cấp quyền cho **user** có quyền cấu hình **firewall policy** (chỉ có thành viên của **Administrators group** trên máy tính nội bộ có thể cấu hình **firewall policy**). |
| Network settings | Các **Network Rules** được tạo sau khi cài đặt:<br>**Local Host Access**: Định nghĩa đường đi (**route**) giữa **Local Host network** và tất cả các mạng khác.<br>**Internet Access**: Định nghĩa **Network Address Translation** (**NAT**).<br>**VPN Clients to Internal Network** dùng để định nghĩa đường đi **VPN Clients Network** và **Internal Network**. |
| Firewall policy | Cung cấp một **Access Rule** mặc định tên là **Default Rule** để cấm tất cả các traffic giữa các mạng. |
| System policy | **ISA firewall** sử dụng **system policy** để bảo mật hệ thống. một số **system policy rule** chỉ cho phép truy xuất một số **service** cần thiết. |
| Web chaining | Cung cấp một luật mặc định có tên **Default Rule** để chỉ định rằng tất cả các request của **Web Proxy Client** được nhận trực tiếp từ **Internet**, hoặc có thể nhận từ **Proxy Server** khác. |
| Caching | Mặc định ban đầu **cache size** có giá trị 0 có nghĩa rằng cơ chế cache sẽ bị vô hiệu hóa. Ta cần định nghĩa một cache drive để cho phép sử dụng **Web caching**. |
| Alerts | Hầu hết cơ chế cảnh báo được cho phép để theo dõi và gián sát sự kiện. |



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

| | |
|---|---|
| Client configuration | **Web Proxy Client** tự động tìm kiếm **ISA Firewall** và sau đó nó sẽ cấu hình |





Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

## V.2. Một số chính sách mặc định của hệ thống

| Order/Comments | Name | Action | Protocol | from/Listener | To | Condition |
|---|---|---|---|---|---|---|
| 1. Chỉ sử dụng khi ISA Firewall là thành viên của Domain | Allow access to Directory services purposes | Allow | LDAP ;LDAP (UDP)<br>LDAP GC (global catalog)<br>LDAPS ;LDAPS GC<br>(Global Catalog) | Local Host | Internal | All Users |
| 2. Cho phép quản lý ISA Firewall từ xa thông qua công cụ MMC | Allow remote management from selected computers using MMC | Allow | NetBIOS datagram<br>NetBIOS<br>Name Service NetBIOS | Remote Management Computers | Local Host | All Users |
| 3. Cho phép quản lý ISA Firewall thông qua Terminal Services Protocol | Allow remote management from selected computers using Terminal Server Name | Allow | RDP (Terminal Services) Protocols | Remote Management<br>Computers From/Listener | Local Host | All Users Continued Condition |
| 4. Cho phép login tới một số server sử dụng giao thức NetBIOS | Allow remote logging to trusted servers using NETBIOS | Allow | NetBIOS Datagram<br>NetBIOS Name Service NetBIOS Session | Local Host | Internal | All Users |
| 5. Cho phép RADIUS authentication từ ISA đến một số trusted RADIUS servers | Allow RADIUS authentication from ISA Server to trusted RADIUS servers | Allow | RADIUS<br>RADIUS Accounting | Local Host | Internal | All Users |

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

| Order/Comments | Name | Action | Protocol | from/Listener | To | Condition | Order/Comments |
|---|---|---|---|---|---|---|---|
| 6. Cho phép chứng thực kerberos từ ISA Server tới trusted server | Allow Kerberos authentication from ISA Server to trusted servers | Allow | Kerberos-Sec (TCP) Kerberos-Sec (UDP) | Local Host | Internal | All Users | 11. Cho phép ISA Server gởi ICMP request tới một số server |
| 7. Cho phép sử dụng DNS từ ISA tới một số DNS Server | Allow DNS from ISA Server to selected servers | Allow | DNS | Local Host | All Networks (and Local Host) | All Users | 12. Cho phép tất cả các VPN Client bên ngoài kết nối vào ISA Server |
| 8. Cho phép DHCP Request từ ISA gởi đến tất cả các mạng | Allow DHCP requests from ISA Server to all networks Name | Allow | DHCP(request) Protocols | Local Host From/Listener | Anywhere To | All Users Continued Condition | 13. Cho phép DHCP Request từ ISA gởi đến tất cả các mạng |
| 9. Chấp nhận DHCP replies từ DHCP Server tới ISA Server | Allow DHCP replies from DHCP servers to ISA Server | Allow | DHCP (reply) | Internal | Local Host | All Users | 14. Cho phép ISA thiết lập kết nối VPN (site to site) đến VPN Server khác |
| 10. Cho phép một số máy được quyền gởi ICMP request đến ISA Server | Allow ICMP (PING) requests from selected computers to ISA Server | Allow | Ping | Remote Management Computers | Local Host | All Users | 15. Cho phép sử dụng CIFS để truy xuất share file từ ISA đến các server khác |



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

| Name | Action | Protocol | from/Listener | To | Condition | Order/Comments | Name | Action |
|---|---|---|---|---|---|---|---|---|
| Allow ICMP requests from ISA Server to selected servers | Allow | ICMP Information Request ICMP Timestamp | Local Host | All Networks (and Local Host Network) | All Users | 16. Cho phép login từ xa bằng SQL qua ISA server | Allow remote SQL logging from ISA servers | Allow |
| All VPN client traffic to ISA Server | Allow | PPTP | External | Local Host | All Users | 17. Cho phép truy xuất HTTP/HTTPS từ ISA đến một số site chỉ định | Allow HTTP/HTTPS requests from ISA Server to specified sites Name | Allow |
| Allow VPN site-to-site traffic to ISA Server Name | Allow | NONE | External IPSec Remote Gateways From/Listener | Local Host To | All Users Continued Condition | 18. Cho phép HTTP/HTTPS từ ISA đến một số server khác | Allow HTTP/HTTPS requests from ISA Server to selected servers for connectivity verifiers | Allow |
| Allow VPN site-to-site traffic from ISA Server | Allow | NONE | Local Host | External IPSec Remote Gateways | All Users | 19. Cho phép một số máy được truy xuất Firewall Client installation share trên ISA Server | Allow access from trusted computers to the Firewall Client installation share on ISA Server | Allow |
| CIFS (Common Internet File System) from ISA Server to trusted | Allow | Microsoft CIFS (TCP) Microsoft CIFS (UDP) | Local Host | Internal | All Users | 20. Cho phép quan sát thông suất của ISA Server từ xa | Allow remote performance monitoring of ISA Server from trusted servers | Allow |





Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

| Protocol | from/Listener | To | Condition | Order/Comments | Name | Action | Protocol | from/Listener |
|---|---|---|---|---|---|---|---|---|
| Microsoft SQL (TCP) Microsoft SQL (UDP) | Local Host | Internal | All Users | 21. Cho phép sử dụng NetBIOS từ ISA Server đến một số Server chỉ định sẵn | Allow NetBIOS from ISA Server to trusted servers Name | Allow | NetBIOS Datagram NetBIOS Name Service NetBIOS Sessions Protocols | Local Host From/Listener |
| HTTP HTTPS Protocols | HTTP HTTPS Protocols | System Policy Allowed Sites To | All Users Continued Condition | 21. Cho phép sử dụng RPC từ ISA truy xuất đến một số server khác | Allow RPC from ISA Server to trusted servers | Allow | RPC (all interfaces) | Local Host |
| HTTP HTTPS | Local Host | All Networks (and Local Host Network) | All Users | 23. Cho phép truy xuất HTTP/HTTPS từ ISA Server tới một số Microsoft error reporting site | Allow HTTP/HTTPS from ISA Server to specified | Allow | HTTP HTTPS | Local Host |
| (TCP) Microsoft CIFS (UDP) NetBIOS Datagram NetBIOS Name Service NetBIOS Session | Internal | Local Host | All Users | 24. Cho phép chứng thực SecurID từ ISA đến một số server | authentication from ISA Server to trusted servers | Allow | SecurID | Local Host |
| NetBIOS Datagram NetBIOS Name Service NetBIOS Session | Remote Management Computers | Local Host | All Users | 25. Cho phép giám sát từ xa thông qua giao thức Microsoft Operations | Allow remote monitoring from ISA Server to | | Microsoft Operations Manager Agent | Local Host |





Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

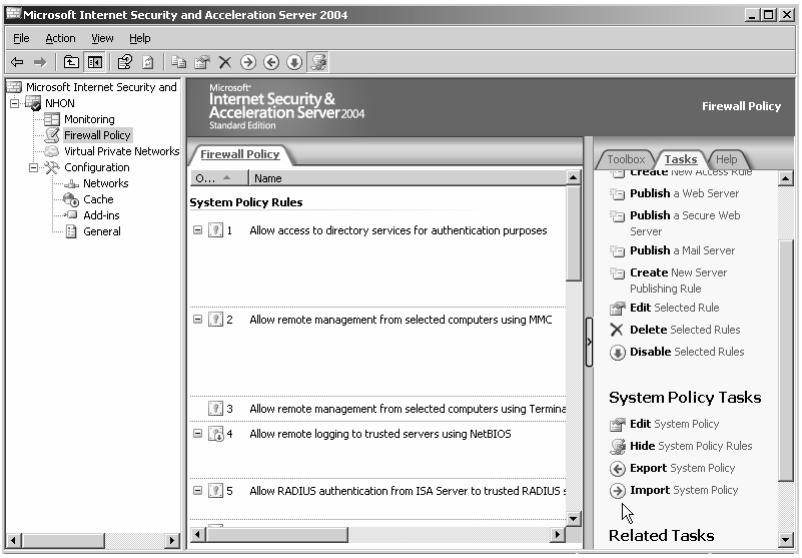
| To | Condition | Order/Comments | Name | Action | Protocol | from/Listener | To | Condition |
|---|---|---|---|---|---|---|---|---|
| Internal To | All Users Continued Condition | 26. Cho phép HTTP traffic từ ISA Server tới một số network hỗ trợ dịch vụ chứng thực download CRL | Traffic from ISA Server to all networks (for CRL downloads) Name | Allow + Action | HTTP Protocols | Local Host From/Listener | All Networks (and Local Host) To | All Users Continued Condition |
| Internal | All Users | 27. Cho phép sử dụng NTP (giao thức đồng bộ thời gian trên Windows NT 2k, XP) từ ISA tới một | Allow NTP from ISA Server to trusted NTP servers | Allow | NTP (UDP) | Local Host | Internal | All Users |
| Microsoft Error Reporting sites | All Users | 28. Cho phép traffic SMTP từ ISA Server tới một số Server | Allow SMTP from Allow ISA Server to trusted servers | | SMTP | Local Host | Internal | All Users |
| Internal | All Users | 29. Cho phép một số máy sử dụng Content Download Jobs. | ISA Server to selected computers for Content Download Jobs | Allow | HTTP | Local Host | All Networks (and Local Host) | System and Network Service |
| Internal | All Users | 30. Cho phép một số máy khác sử dụng MMC điều khiển ISA | Allow Microsoft communication to selected computers | Allow | All Outbound traffic | Local Host | Remote Management Computers | All Users |





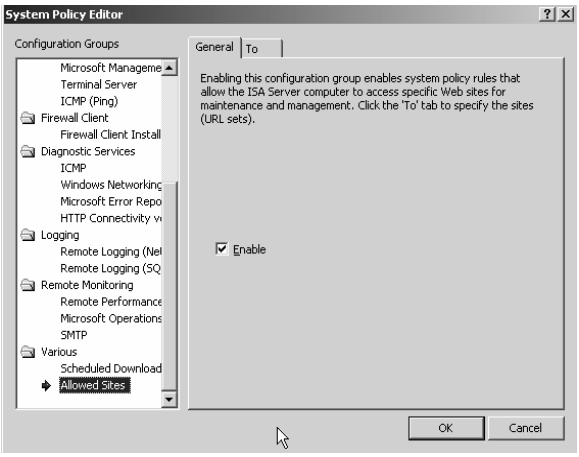
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Ta có thể xem các chính sách mặc định của hệ thống **ISA Firewall** (**system policy rule)** bằng cách chọn **Filewall Policy** từ hộp thoại **ISA Management**, sau đó chọn item **Show system policy rule** trên cột **System policy**.




Hình 5.12: **System policy Rules**.

Ta cũng có thể hiệu chỉnh từng **system policy** bằng cách nhấp đôi chuột vào **system policy item**.



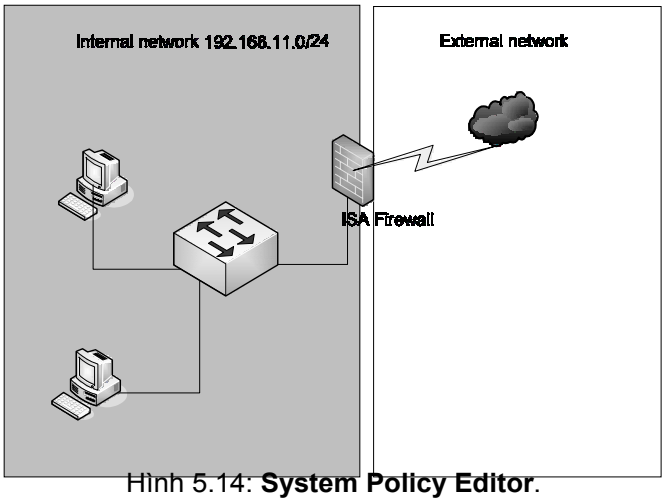

Hình 5.13: System Policy Editor.

## V.3. Cấu hình Web proxy cho ISA.

Trong phần này ta sẽ khảo sát nhanh các bước làm sao để cấu hình **ISA Firewall** cung cấp dịch vụ **Web Proxy** để chia sẻ kết nối **Internet** cho mạng nội bộ.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 5.14: **System Policy Editor**.

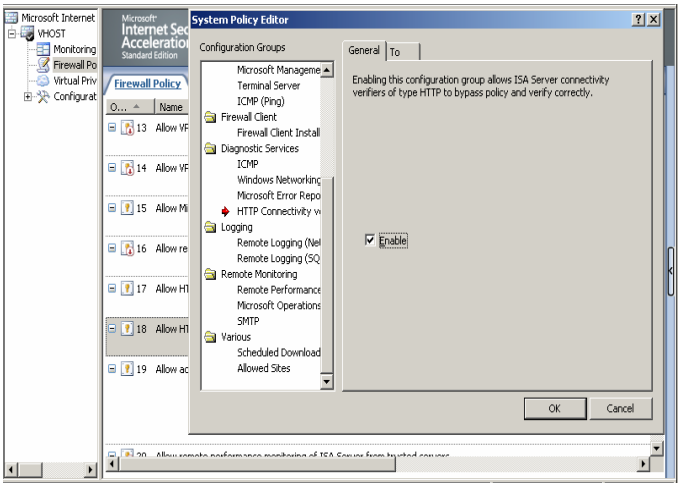
- Mặc định **ISA Firewall** cho phép tất cả mạng nội bộ chỉ có thể truy xuất **Internet Web** thông qua giao thức **HTTP/HTTPS** tới một số **site** được chỉ định sẵn trong **Domain Name Sets** được mô tả dưới tên là "**system policy allow sites"** bao gồm:
- *.windows.com
- *.windowsupdate.com
- *.microsoft.com

Do đó khi ta muốn cấu hình cho mạng nội bộ có thể truy xuất đến bất kỳ một **Internet Web** nào bên ngoài thì ta phải hiệu chỉnh lại thông tin trong **System Policy Allowed Sites** hoặc hiệu chỉ lại **System Policy Rule** có tên

  + Hiệu chỉnh **System Policy Allowed Sites** bằng cách Chọn **Firewall Policy** trong ISA **Management Console**, sau đó chọn cột **Toolbox**, chọn **Domain Name Sets**, nhấp đôi vào item **System Policy Allowed Sites** để mô tả một số site cần thiết cho phép mạng nội bộ truy xuất theo cú pháp *.domain_name.
- Nếu ta muốn cho mạng nội bộ truy xuất bất kỳ **Internet Website** nào thì ta phải **Enable** luật 18 có tên "**Allow HTTP/HTTPS requests from ISA Server to selected servers for connectivity verifiers**" (tham khảo Hình 5.15)**,** sau đó ta chọn nút **Apply** trong **Firewall Policy** pannel để áp đặt sự thay đổi vào hệ thống.



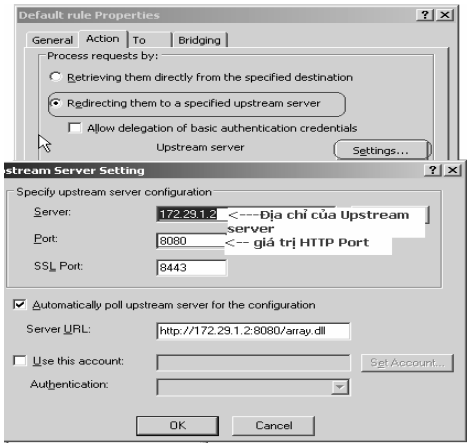
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 5.15: Mô tả **System Policy Sites**.

Chú ý:

- Nếu **ISA Firewall** kết nối trực tiếp **Internet** thì ta chỉ cần cấu hình một số thông số trên, ngược lại nếu **ISA Firewall** còn phải thông qua một hệ thống **ISA Firewall** hoặc **Proxy** khác thì ta cần phải mô tả thêm tham số **Uptream Server** để chuyển yêu cầu truy xuất lên **Proxy** cha để nhờ **Proxy** cha lấy thông tin từ **Internet Web Server**.
  + Để cấu hình **Uptream Server** cho **ISA Server** nội bộ ta chọn **Configuration panel** từ **ISA Management Console**, sau đó chọn item **Network** , chọn **Web Chaining Tab**, Nhấp đôi vào **Rule Set** có tên **Last default rule**, chọn **Action Tab**, chọn tùy chọn **Redirecting them to specified upstream server**, chọn tiếp nút **Settings…**Chỉ định địa chỉ của **upstream server**.




Hình 5.16: Chỉ định **Upstream server**.

  + Ta cần chỉ định **DNS Server** cho **ISA Server** để khi **ISA** có thể phân giải **Internet Site** khi có yêu cầu, ta có thể sử dụng **DNS Server** nội bộ hoặc **Internet DNS Server**, tuy nhiên ta cần lưu ý rằng phải cấu hình **ISA Firewall** để cho phép **DNS request** và **DNS reply**.
- Để cho phép **Client** có thể sử dụng **Web Proxy** ta cấu hình **Proxy Server** có địa chỉ là địa chỉ của Internal interface của **ISA Firewall** trong trình duyệt **Web** cho từng **Client**, hoặc ta cài **ISA Client**



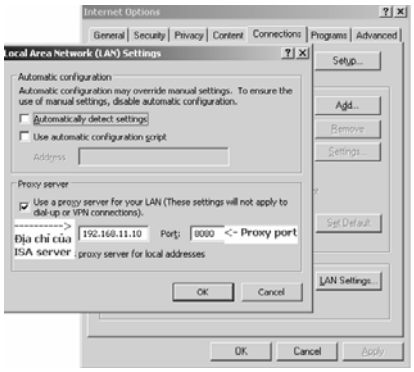
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

**Share** trên từng **Client** để **Client** đóng vai trò lài **ISA Firewall Client**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

- Chỉ định địa chỉ của **Web Proxy** trong **textbox Address.**
- Chỉ **Web Proxy Port** trong Textbox **Port** là **8080.**




Hình 5.16: Chỉ định **Client** sử dụng **Proxy Server**.

## V.4. Tạo Và Sử Dụng Firewall Access Policy.

- **Access Policy** của **ISA Firewall** bao gồm các tính năng như: **Web Publishing Rules**, **Server Publishing Rules** và **Access Rules**.
  - + **Web Publishing Rules** và **Server Publishing Rules** được sử dụng để cho phép **inbound access**.
    - o **Access rules dùng để điều khiển outbound access.**
- **ISA Firewall** kiểm tra **Access Rules** trong **Access Policy** theo cơ chế **top down** (Lưu ý rằng **System Policy** được kiểm tra trước **Access Policy** do **user** định nghĩa), nếu **packet** phù hợp với một luật nào đó thì **ISA Firewall** thì **ISA Firewall** sẽ thực thi **action** (**permit/deny**) tùy theo luật, sau đó **ISA Firewall** sẽ bỏ qua tất cả các luật còn lại. Nếu **packet** không phù hợp với bất kỳ **System Access Policy** và **User-Defined Policy** thì **ISA Firewall deny packet** này.
- Một số tham số mà **Access Rule** sẽ kiểm tra trong **connection request**:
  - + **Protocol**: Giao thức sử dụng.
  - + **From**: Địa chỉ nguồn.
  - + **Schedule**: Thời gian thực thi luật.
  - + **To**: Địa chỉ đích.
  - + **Users**: Người dùng truy xuất.
  - + **Content type**: Loại nội dung cho **HTTP connection**.

### V.4.1 Tạo một Access Rule.

**Access Rules** trên **ISA Firewall** luôn luôn áp đặt luật theo hướng ra (**outbound**). Ngược lại, **Web Publishing Rules**, **Server Publishing Rules** áp đặt theo hướng vào (**inbound**). **Access Rules** điều khiển truy xuất từ **source** tới **destination** sử dụng **outbound protocol**. Một số bước tạo **Access Rule**:

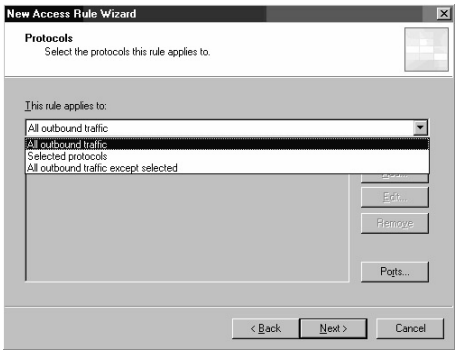
3. Kích hoạt **Microsoft Internet Security and Acceleration Server 2004 management console**, mở rộng **server name**, nhấp chuột vào **Firewall Policy panel**, chọn **Tasks tab** trong **Task Pane**, nhấp chuột vào liên kết **Create New Access Rule**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

4. Hiển thị hộp thoại **"Welcome to the New Access Rule Wizard"**. Điền vào tên **Access Rule name**, nhấp chuột vào nút **Next** để tiếp tục.
5. Hiển thị hộp thoại **Rule Action** có hai tùy chọn: **Allow** hoặc **Deny**. Tùy chọn **Deny** được đặt mặc định, tùy vào loại Rule ta cần mô tả mà chọn **Allow** hoặc **Deny** cho phù hợp, chọn **Next** để tiếp tục.
6. Hiển thị hộp thoại "**Protocols"** (tham khảo Hình 5.17). Ta sẽ chọn giao thức (protocol) để cho phép/cấm **outbound traffic** từ **source** đến **destination**. Ta có thể chọn ba tùy chọn trong danh sách **This rule applies to.**

- **All outbound traffic**: Để cho phép tất cả các protocols **outbound**. Tầm ảnh hưởng của tùy chọn này phụ thuộc vào loại **Client** (**client type**) sử dụng để truy xuất luật. đối với **Firewall clients**, thì tùy chọn này cho phép tất cả các **Protocol** ra ngoài (**outbound**), bao gồm cả **secondary protocols** đã được định nghĩa hoặc chưa được định trong **ISA firewall**. Tuy nhiên đối với **SecureNAT client** kết nối **ISA Firewall** thì **outbound access** chỉ cho phép các protocol mà đã được định nghĩa trong **Protocols list** của **ISA firewall**, nếu **SecureNAT client** không thể truy xuất tài nguyên nào đó bên ngoài bằng một **protocol** nào đó thì ta phải mô tả **protocol** vào **Protocol Panel** được cung cấp trên **ISA firewall** để nó có thể hỗ trợ kết nối cho **SecureNAT client**.
- **Selected protocols**: Tùy chọn này cho phép ta có thể lựa chọn từng **protocols** để áp đặt vào luật (**rule**). Ta có thể lựa chọn một số **protocol** có sẵn trong hộp thoại hoặc có thể tạo mới một **Protocol Definition**.
- **All outbound traffic except selected**: Tùy chọn này cho phép tất cả các **protocol** cho luật mà không được định nghĩa trong hộp thoại.

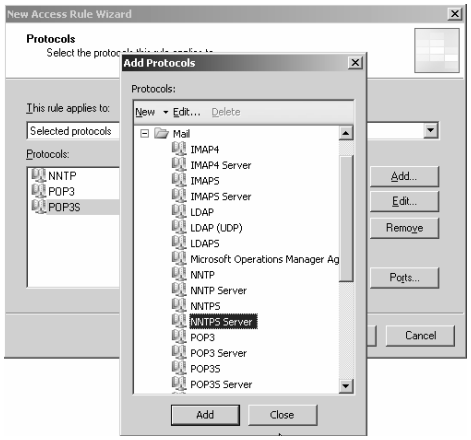



Hình 5.17: Lựa chọn **protocol** để mô tả cho **Rule**.

Nếu ta chọn tùy chọn **Selected Protocols** ta sẽ chọn danh sách các **protocol** cần mô tả cho luật (tham khảo hình 5.18).



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 5.18: Lựa chọn **protocol** để mô tả cho **Rule**.

1. Hiển thị hộp thoại **Access Rule Sources**, chọn địa chỉ nguồn (**source location**) để áp đặt vào luật bằng cách chọn nút **Add**, hiển thị hộp thoại **Add Network Entities**, sau đó ta có thể chọn địa chỉ nguồn từ hộp thoại này (tham khảo hình), chọn **Next** để thực hiện bước tiếp theo.


Hình 5.19: Chọn địa chỉ nguồn.

2. Hiển thị hộp thoại **Access Rule Destinations** cho phép chọn địa chỉ đích (**destination**) cho luật bằng cách chọn nút **Add** sau đó xuất hiện hộp thoại **Add Network Entities**, trong hộp thoại này cho phép ta chọn địa chỉ đích (**Destination**) được mô tả sẵn trong hộp thoại hoặc có thể định nghĩa một **destination** mới, thông thường ta chọn **External network** cho **destination rule**, sau khi hoàn tất quá trình ta chọn nút **Next** để tiếp tục.
3. Hiển thị hộp thoại **User Sets** cho phép ta lựa chọn **User** truy xuất cho **access Rule**. Mặc định luật sẽ áp đặt cho tất cả user (**All Users)**, ta có thể hiệu chỉnh thông số này bằng cách chọn **Edit** hoặc thêm **user** mới vào **rule** thông qua nút **Add**, chọn **Next** để tiếp tục
4. Chọn **Finish** để hoàn tất.



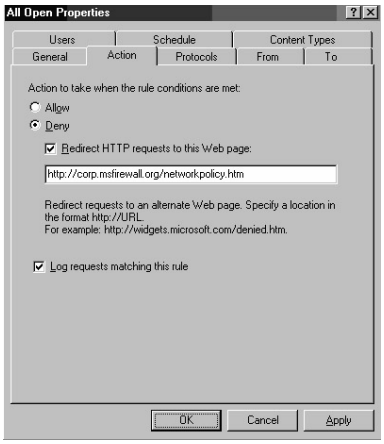
### V.4.2 Thay đổi thuộc tính của Access Rule.

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Trong hộp thoại thuộc tính của **Access Rule** chứa đầy đủ các thuộc tính cần thiết để thiết lập luật, có một số thuộc tính chỉ có thể cấu hình trong hộp thoại này mà không thể cấu hình trong quá trình tạo **Access Rule**, thông thường ta truy xuất hộp thoại thuộc tính của luật khi ta muốn kiểm tra hoặc thay đổi các điều kiện đã đặt trước đó. Để truy xuất thuộc tính của **Access Rule** ta nhấp đôi chuột vào tên luật trong **Firewall Policy Panel**.

**Một số Tab thuộc tính của Access Rule:**

- **General tab:** Cho phép ta có thể thay đổi tên **Access rule**, **Enable/Disable Access rule**.
- **Action tab:** Cung cấp một số tùy chọn để hiệu chỉnh luật như (Tham khảo hình 5.20):
- **Allow:** Tùy chọn cho phép các kết nối phù hợp (**matching**) với các điều kiện được mô tả trong **Access rule** đi qua **ISA firewall**.
- **Deny:** Tùy chọn cấm các kết nối phù hợp (**matching**) với các điều kiện được mô tả trong **Access rule** đi qua **ISA firewall**.
- **Redirect HTTP requests to this Web page**: Tùy chọn được cấu hình để chuyển hướng **HTTP requests** (phù hợp với điều kiện của **Access rule**) tới một **Web page** khác.
- **Log requests matching this rule** Cho phép ghi nhận lại tất cả các **request** phù hợp với **Access Rule**.




Hình 5.20: Thuộc tính của **Access Rule**.

- **Protocols tab:** Cung cấp các tùy chọn để cho phép ta hiệu chỉnh giao thức (**protocol**) cho **Access rule**.
- **From tab:** Cung cấp các tùy chọn để hiệu chỉnh địa chỉ nguồn cho **Access rule**.
- **To tab:** Cung cấp các tùy chọn để hiệu chỉnh địa chỉ đích cho **Access rule**.
- **Users tab:** Cung cấp các tùy chọn để hiệu chỉnh thông tin **User** trong **Access rule**.
- **Schedule tab:** Hiệu chỉnh thời gian áp đặt (**apply**) luật.
- **Content Types tab:** Cho phép hiệu chỉnh **Content Type** chỉ áp đặt **HTTP connection**.

## V.5. Publishing Network Services.

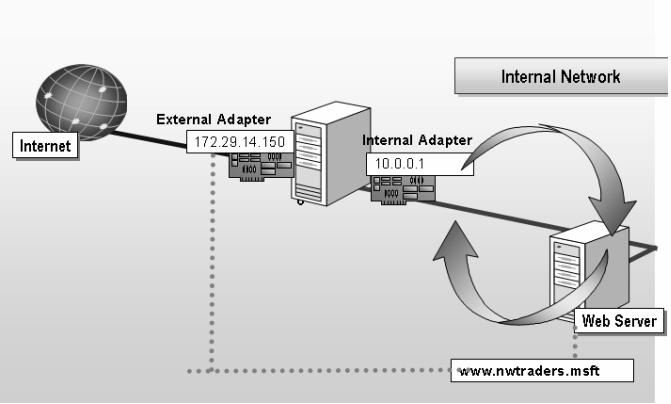


### V.5.1 Web Publishing and Server Publishing.

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

**Publishing services** là một kỹ thuật dùng để công bố (**publishing**) dịch vụ nội bộ ra ngoài mạng Internet thông qua **ISA Firewall**. Thông qua **ISA Firewall** ta có thể publish các dịch vụ **SMTP**, **NNTP**, **POP3**, **IMAP4**, **Web**, **OWA**, **NNTP**, **Terminal Services**,,,.

- **Web publishing:** Dùng để **publish** các **Web Site** và dịch vụ **Web**. **Web Publishing** đôi khi được gọi là **'reverse proxy'** trong đó **ISA Firewall** đóng vai trò là **Web Proxy** nhận các Web request từ bên ngoài sau đó nó sẽ chuyển yêu cầu đó vào **Web Site** hoặc **Web Services** nội bộ xử lý (tham khảo hình 5.21), Một số đặc điểm của **Web Publishing**:
- Cung cấp cơ chế truy xuất ủy quyền **Web Site** thông qua **ISA firewall**.
- Chuyển hướng theo đường dẫn truy xuất **Web Site** (**Path redirection**)
- **Reverse Caching of published Web Site**.
- Cho phép **publish** nhiều **Web Site** thông qua một địa chỉ **IP**.
- Có khả năng thay đổi (**re-write**) **URLs** bằng cách sử dụng **Link Translator** của **ISA firewall**.
- Thiết lập cơ chế bảo mật và hỗ trợ chứng thực truy xuất cho **Web Site** (**SecurID authentication**, **RADIUS authentication**, **Basic Authentication**)
- Cung cấp cơ chế chuyển theo **Port** và **Protocol**.




Hình 5.21: Mô hình **Web Publishing**.

- **Server publishing:** Tương tự như **Web Publishing**, **Server publishing** cung cấp một số cơ chế công bố (**publishing**) các **Server** thông qua **ISA Firewall**.

### V.5.2 Publish Web server.

Để **publish** một **Web Services** ta thực hiện các bước sau:

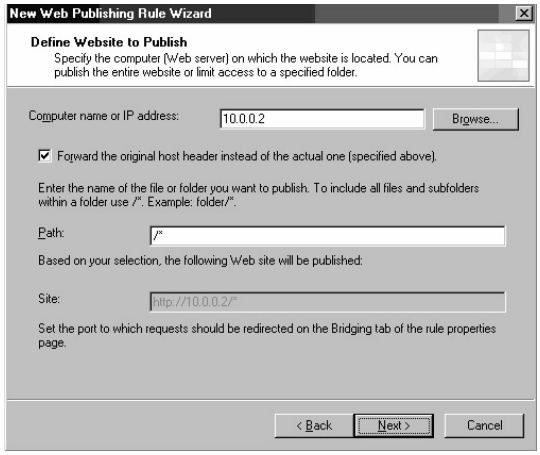
1. kích hoạt màn hình "**Microsoft Internet Security and Acceleration Server 2004 management console**", mở rộng mục chọn **Server Name**, chọn nút **Firewall policy**, chọn **Tasks tab**.
2. Trên **Tasks tab**, chọn liên kết "**Publish a Web Server**", hiển thị hộp thoại "**Welcome to the New Web Publishing Rule Wizard**" yêu cầu nhập tên **Web publishing rule**, chọn **Next** để tiếp tục.
3. Chọn tùy chọn **Allow** trong hộp thoại "**Select Rule Action**", chọn **Next**.
4. Cung cấp một số thông tin về **Web Site** cần được **publish** trong hộp thoại **"Define Website to Publish"** (tham khảo hình 5.22):

- **"Computer name or IP address"**: chỉ định địa chỉ của **Web Server** nội bộ.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

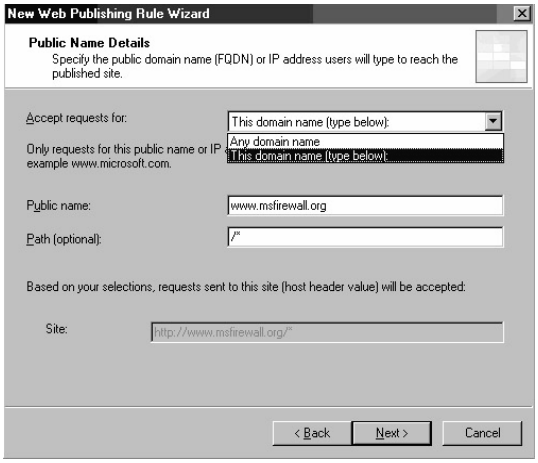
- **"Forward the original host header instead of the actual one (specified above)":** Chỉ định cơ chế chuyển yêu cầu vào **Web Server** nội bộ theo dạng **host header name**, tùy chọn này được sử dụng trong trường hợp ta muốn **publish Web hosting** cho một **Web Server**.
- **"Path"**: Chỉ định tên tập tin hoặc thư mục ta muốn truy xuất vào **Web Server** nội bộ.
- **"Site"**: Chỉ định tên **Web Site** được **publish**.




Hình 5.22: Chỉ định **Web Site** cần **Publish**.

1. Chỉ định một số thông tin về **FQDN** hoặc **IP addresses** được phép truy xuất tới **publish Web Site** thông qua **Web Publishing Rule** (tham khảo hình 5.23). Các tùy chọn cần thiết:

- **Accept requests for**: Chỉ định tên **publish** được **Web listener** chấp nhận.
- **Path** (**optional**): Chỉ định đường dẫn **Web Site** cho phép truy xuất
- **Site**: Tên **Web Site** được phép truy xuất **Web Site** nội bộ.




Hình 5.23: Chỉ định tên **domain** được truy xuất **publish site**.

2. Chọn **Web Listener** cho **Web Publishing Rule** (là một **Network Object** được sử dụng cho **Web Publishing Rule** để **listen** các kết nối đi vào **interface** (**incoming connection**) theo port được định nghĩa trước), ở bước này ta có thể lựa chọn **Web Listener** đã tạo trước đó hoặc ta có thể tạo mới **Web Listener**. Sau đây là một số bước tạo mới **Web Listener.**

- Từ hộp thoại "**Seclect Web Listener**" bằng cách nhấp chuột vào nút **New**…, cung cấp tên **Web**



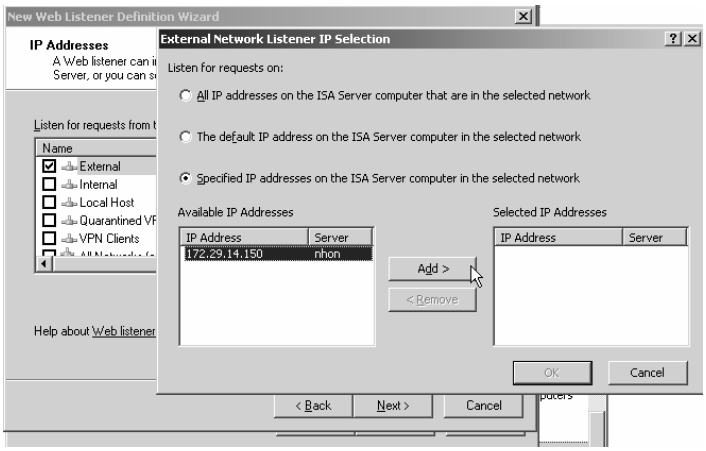
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

**Listener** trong hộp thoại "**Welcome to the New Web Listener Wizard**", chọn **Next**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

- Chọn tên **Interface** cho phép chấp nhận kết nối **Incoming Web**, sau đó ta có thể chọn nút **Address** để chỉ định địa chỉ **IP** cụ thể trên **interface** đã lựa chọn, Chọn nút **Add>** (tham khảo hình 5.24), cuối cùng ta chọn nút **OK** để chấp nhận quá trình tạo mới **Web Listener**, chọn **Next** để tiếp tục.




Hình 5.24: Chọn địa chỉ chấp nhận **incoming web request**.

3. Chỉ định **HTTP port** và **SSL port** trong hộp thoại **Port Specification** cho phép **ISA Server** sử dụng để chấp nhận **incoming web requests**, chọn **Next**.
4. Chọn **Finish** để hoàn tất quá trình.

### V.5.3 Publish Mail Server.

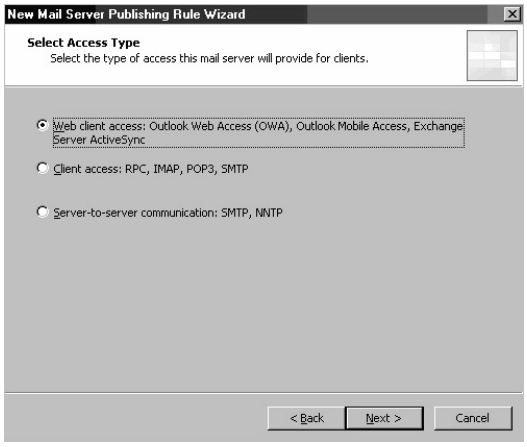
**Các bước tiến hành publish Mail server:**

1. Kích hoạt màn hình "**Microsoft Internet Security and Acceleration Server 2004 management console**", mở rộng mục chọn **Server Name**, chọn nút **Firewall policy**, chọn **Tasks tab**.
2. Trên **Tasks tab**, chọn liên kết "**Publish a Mail Server**", hiển thị hộp thoại "**Welcome to the New Mail Server Publishing Rule Wizar**d" yêu cầu nhập tên **Mail Server Publishing Rule**, chọn **Next** để tiếp tục.
3. Chọn các tùy chọn về loại truy xuất cho **Client** trong hộp thoại "**Select Client Type**" (Tham khảo hình 5.25).

- **Web client access: Outlook Web Access (OWA), Outlook Mobile Access, Exchange Server ActiveSync**: **Publish Web Mail Server** để cho phép **client** có thể truy xuất **E-Mail** qua **Web** thông qua **OWA**, **OMA**, **ESA**,..
- **Client access: RPC, IMAP, POP3, SMTP**: **Publish** các giao thức **IMAP**, **POP3**, **SMTP** cho **Mail Server**.
- **Server-to-server communication: SMTP, NNTP**: Cho phép **Server Mail** bên ngoài có thể giao tiếp với **Server Mail** nội bộ thông qua giao thức **SMTP**, **NNTP**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 5.25: Chọn **Client Type**.

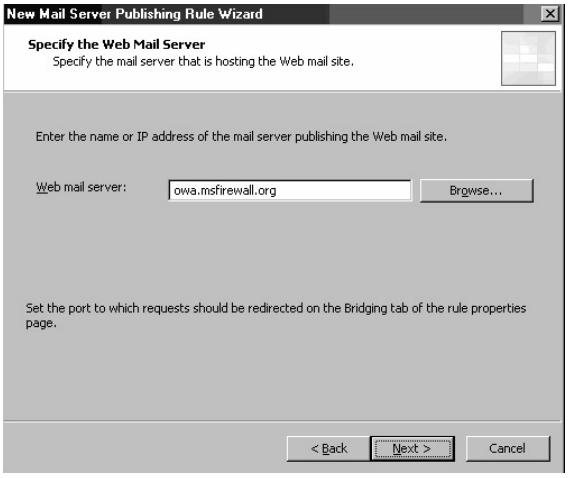
1. Ví dụ trong bước 3 ta chọn tùy chọn **Web Client Access**, chọn **Next**, sau đó xuất hiện hộp thoại "**Select Services**" cho phép ta chọn các dịch vụ **Exchange Web Services** bao gồm: **Outlook Web Access**, **Outlook Mobile Access**, **Exchange ActiveAsync** (tham khảo hình 5.26), chọn **Next** để tiếp tục.


Hình 5.26: Chọn **Exchange Web Services**.

2. Chỉ định địa chỉ **Web Mail Server** trong hộp thoại "**Specify the Web Mail Server"**, chọn **Next.**

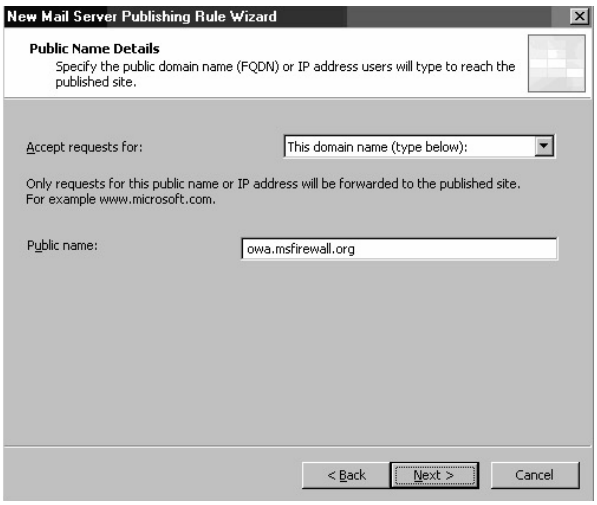


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 5.27: Chỉ định địa chỉ **Web Mail Server**.

3. Chỉ định **Publish Name** được **Web Listener** chấp nhận trong hộp thoại "**Public Name Details"**, chọn **Next.**




Hình 5.28: Chỉ định **Publish Name**.

4. Chọn **Finish** để hoàn tất quá trình.

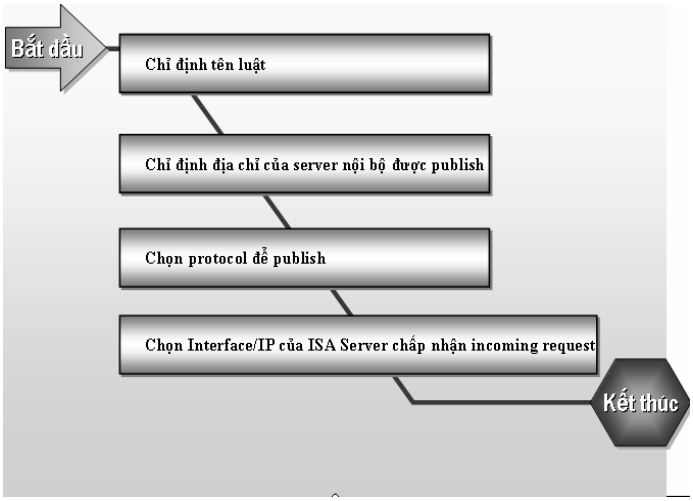
### V.5.4 Tạo luật để publish Server.

Tạo luật để **publish** một **Server** thực chất các thao tác cũng tương tự như ta **publish** một **Web** hoặc **Mail** chỉ có điều ta được phép lựa chọn **protocol** cần được **publish**, khi ta **publish** một **Server** ta cần chuẩn bị một số thông số sau:

- **Protocol** mà ta cần **publish** là **protocol** gì?
- Địa chỉ **IP** trên **ISA firewall** chấp nhận **incoming connection**.
- Địa chỉ **IP address** của **Publish Server** nội bộ (**Protected Network server**).



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 5.29: Mô hình tạo luật để **publish server**.

Các bước tạo một **Publish Server**:

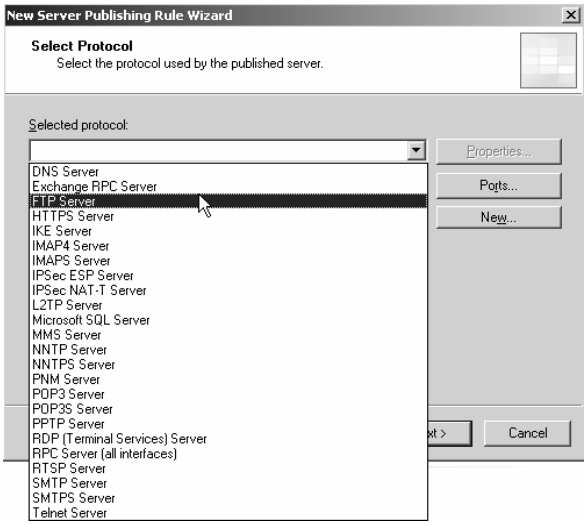
1. Kích hoạt màn hình "M**icrosoft Internet Security and Acceleration Server 2004 management console**", mở rộng mục chọn **Server Name**, chọn nút **Firewall policy**, chọn **Tasks tab**.
2. Trên **Tasks tab**, chọn liên kết "**Create New Server Publishing Rule**", hiển thị hộp thoại "**Welcome to the New Server Publishing Rule Wizard**" yêu cầu nhập tên **Server Publishing** Rule, chọn **Next** để tiếp tục.
3. Chỉ định địa chỉ của server nội bộ cần để **publish**, chọn **Next** để tiếp tục.


Hình 5.30: Chỉ định địa chỉ của **Server** để **publish**.

4. Chọn **Protocol** cần để **Publish**, chọn **Next**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 5.31: Chọn **protocol**.

5. Chọn tên **Interface** cho phép chấp nhận kết nối **Incoming Web**, sau đó ta có thể chọn nút **Address** để chỉ định địa chỉ IP cụ thể trên **interface** đã lựa chọn, Chọn nút **Add>** (tham khảo hình 5.24), cuối cùng ta chọn nút **OK** để chấp nhận quá trình tạo mới **Web Listener**, chọn **Next** để tiếp tục.
6. Chọn **Finish** để hoàn tất quá trình.

## V.6. Kiểm tra trạng thái và bộ lọc ứng dụng.

**ISA firewall** có thể thực thi được hai chức năng quan trọng **stateful filtering** và **stateful application layer inspection**. **stateful filtering** kiểm tra và thiết lập bộ lọc tại tầng **network**, **transport**. **Stateful filtering** thường được gọi là bộ kiểm tra trạng thái **packet** (***stateful packet inspection***). Trái ngược với phương thức **packet filtering** dựa trên **hardware firewalls**, **ISA firewall** có thể kiểm tra thông tin tại tầng ứng dụng (**stateful application layer inspection**). **stateful application layer inspection** yêu cầu **Firewall** có thể kiểm tra đầy đủ thông tin trên tất cả các tầng giao tiếp bao gồm hầu hết các tầng qua trọng và **application layer** trong mô hình tham chiếu **OSI**.

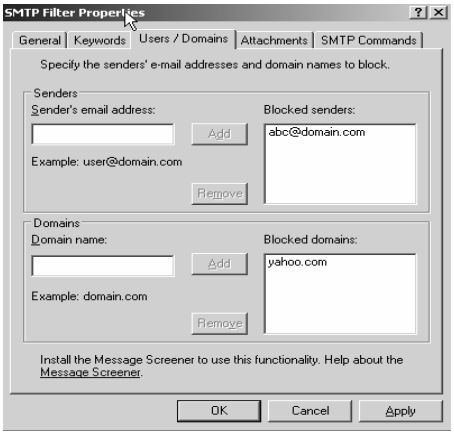
### V.6.1 Lập bộ lọc ứng dụng.

**ISA firewall** thiết lập bộ lọc ứng dụng (**Application filters**) với mục đích bảo vệ các **publish server** chống lại một số cơ chế tấn công bất hợp pháp từ bên ngoài mạng, để hiệu chỉnh bộ lọc ta chọn mục **Add-ins** trong **Configuration Panel**, sau đó ta nhấp đôi chuột vào tên bộ lọc cần hiệu chỉnh,…Một số các bộ lọc ứng dụng cần tham khảo như:

- **SMTP filter and Message Screener: SMTP filter** và **Message Screener** được sử dụng để bảo vệ **publish SMTP server** chống lại cơ chế tấn công làm tràn bộ nhớ (**buffer overflow attacks**), **SMTP Message Screener** bảo vệ mạng nội bộ ngăn một số **E-mail messages** không cần thiết.
- Dùng **SMTP filter** để ngăn chặn địa chỉ Mail hoặc **domain** truy xuất **Publish STMP Server** (tham khảo hình 5.32)

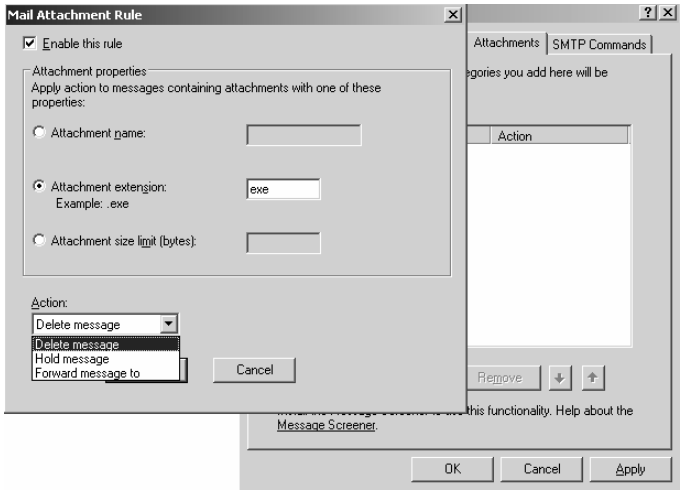


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 5.32: ngăn chặn **Users/domain** sử dụng **SMTP**.

- Dùng **SMTP filte**r để ngăn chặn gởi file đính kèm (tham khảo hình 5.33), ta có thể xóa, lưu giữ **message**, chuyển **message** đối với file đính kèm có tên file giống với tên được mô tả trong **Attachment name:**, hoặc file đính kèm có phần mở rộng được mô tả trong **Textbox Attachment Extensions**, hoặc file đính kèm có kích thước lớn hơn hay bằng kích thước mô tả trong **textbox Attachment size limit (bytes):**,




Hình 5.33: ngăn chặn **Users/domain** sử dụng **SMTP**.

- **DNS filter:** Được sử dụng để bảo vệ **Publish DNS Server** để ngăn, chống lại một số cơ chế tấn công từ bên ngoài vào dịch vụ **DNS**.
- **POP Intrusion Detection filter:** Được sử dụng để bảo vệ **Publish POP Server** để ngăn, chống lại một số cơ chế tấn công từ bên ngoài vào dịch vụ **POP**.
- **SOCKS V4 filter:** được sử dụng để chấp nhận yêu cầu kết nối **SOCKS version 4**. **SOCKS v4 filter** mặc định không được kích hoạt. Thông thường hệ thống Windows không cần sử dụng SOCKS filter vì ta có thể cài đặt **Firewall client** trên các máy mà ta muốn chứng thực trong suốt (**transparently authenticate**) với **ISA firewall**. Ta có thể enable **SOCK v4 fileter** để cung cấp dịch vụ **SOCK** cho các **host** không thể cài đặt **Firewall clients** như **Linux** và **Mac hosts**. Để **enbale SOCK services** ta nhấp đôi chuột vào mục **SOCK V4 Filter**, sau đó chọn tùy chọn **Enable**

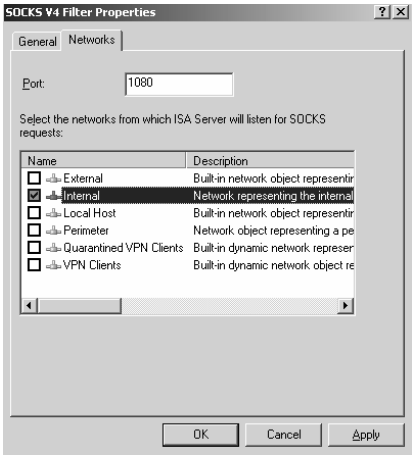


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

**this filter**, chọn **Networks Tab** để chọn **interface** trên **ISA Firewall** cho phép **listen** tại **port 1080.**



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 5.32: Kích hoạt **SOCK Service**.

### V.6.2 Thiết lập bộ lọc Web.

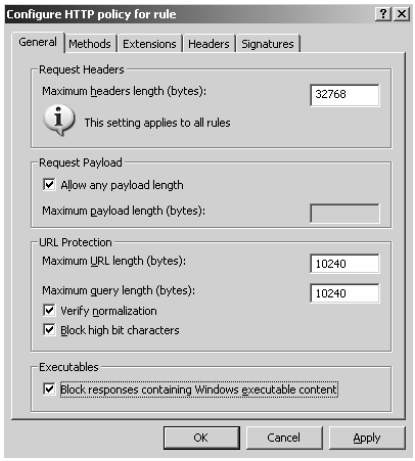
**ISA firewall Web filters** được sử dụng để **ISA firewall** lọc các kết nối thông qua giao thức **HTTP**, **HTTPS**, and **FTP tunneled** (**Web proxied**).

**HTTP Security filter:** Là một trong những kỹ thuật chính yếu để thiết lập bộ lọc ứng dụng, **HTTP Security filter** cho phép **ISA firewall** thực hiện một số cơ chế kiểm tra thông tin ứng dụng (**application layer inspection**) dựa trên tất cả các **HTTP traffic** qua **ISA firewall** và chặn các kết nối không phù hợp với yêu cầu được mô tả trong **HTTP security**, để thay đổi **HTTP Security Filter** ta nhấp đôi chuột vào **Web Publishing Rule** | **Traffic Tab** | **Filtering** | **Configure HTTP**.

- **General Tab**: Quy định chiều dài tối đa của **HTTP Request Header**, **URL Length**, giới hạn thông tin trả về có chứa các code thực thi,..
- **Methods Tab**: Điều khiển các HTTP method như: **GET**, **PUT**, **POST**, **HEAD**, **SEARCH**, **CHECKOUT**,…
- **Extensions Tab**: Giới hạn **file extensions** trong các thông tin **request** của **user**, như ta có thể block các **user** truy xuất file có phần mở rộng là .exe, .com, .zip.
- **Headers Tab**: Giới hạn **HTTP header** trong các thông tin yêu cầu cũng như thông tin trả lời từ **Web client**.
- **Signatures Tab**: Cho phép điều khiển truy xuất dựa vào **HTTP signature**. Thông tin chữ ký (**signatures**) dựa vào chuỗi ký tự có trong **HTTP communication**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 5.32: Cấu hình **HTTP policy**.

**ISA Server Link Translator: Link Translator** là một trong những kỹ thuật được xây dựng sẵn trong **ISA firewall Web filter** để thực hiện biến đổi địa chỉ **URL** cho các kết nối của **user** bên ngoài truy xuất vào **Web publishing** nội bộ, **Link Translation dictionary** được tạo khi ta kích hoạt (**enable**) **link translation** cho **Web Publishing Rule**. Một số **Link Translator dictionary** mặc định:

- Bất kỳ sự kiện nào xảy ra trên **Web Site** được chỉ định trong **Tab To** của **Web Publishing** Rule được thay thế bằng một tên **Web Site** (hoặc địa chỉ **IP**). Ví dụ, nếu ta đặt một luật cho **Web Publishing** là chuyển tất cả các **incoming request** theo địa chỉ http://www.microsoft.com của **Client** truy xuất vào **ISA Server** thì sẽ chuyển tới **Web Server** nội bộ có tên là SERVER1 (có địa chỉ192.168.1.1), khi đó **ISA Server** sẽ thay thế tất cả các **response** của http://SERVER1 thành địa chỉ http://www.microsoft.com gởi trả lại cho **Client** bên ngoài.
- Nếu không chỉ định **port** mặc định trên **Web listener**, thì **port** đó sẽ được gởi trả lại cho **Client**. Ví dụ, nếu có chỉ định **port** mặc định trên **Web listener** thì thông số **port** sẽ được loại bỏ khi thay thế địa chỉ **URL** trong trang trả về (**response page**). Nếu **Web listener** lắng nghe (**listening**) trên port 88 của giao thức **TCP** thì thông tin trả về cho **Web Client** có chứa giá trị port 88 của giao thức **TCP**.
- Nếu **Client** sử dụng **HTTPS** gởi yêu cầu đến **ISA firewall** thì **firewall** sẽ thay thế **HTTP** thành **HTTPS** gởi trả về **Client**.
- Ví dụ: Giả sử **ISA firewall publish** một site trên máy có tên là SERVER1. **ISA firewall publish** site sử dụng tên chính (**public name**) là www.msfirewall.org/docs. **External Web client** gởi một **request** với thông tin "GET /docs HTTP/1.1Host: www.msfirewall.org" Khi **Internet Information Services** (**IIS**) **Server** nhận **request** thì nó sẽ tự động trả về mã số 302 **response** với **header** được mô tả là http://SERVER1/docs/, đây là tên nội bộ (**Internal Name**) **Web server**. **Link Translator** của **ISA firewall** sẽ thay đổi (**translates**) **header** trả lời (**response header**) với giá trị là http://www.msfirewall.org/docs/. Trong ví dụ trên thì một số thông tin (**entries**) sẽ tự động thêm vào **Link Translation dictionary**:

***http://SERVER1*** --> ***http://www.msfirewall.org***

***http://SERVER1:80*** --> ***http://www.msfirewall.org***

https://SERVER1 **-->** https://***www.msfirewall.org***



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

- Nếu **ISA firewall publish** một site sử dụng **Web listener** không phải trên **port** mặc định (**nondefault ports**) ( ví dụ: 85 cho HTTP và 885 cho SSL),thì địa chỉ **URL** sẽ được thay đổi như sau theo các mục ánh xạ địa chỉ URL như sau:

http://SERVER1 **-->** http://www.msfirewall.org:85

http://SERVER1:80 **-->** http://www.msfirewall.org:85

https://SERVER1 **-->** https://www.msfirewall.org:885

https://SERVER1:443 **-->** https://www.msfirewall.org:885

### V.6.3 Phát Hiện Và Ngăn Ngừa Tấn Công.

- Một số phương thức tấn công thông dụng:

**Denial-of-Service Attacks:** Là kiểu tấn công rất lợi hại, với kiểu tấn công này ,bạn chỉ cần 1 máy tính kết nối đến **internet** là đã có thể thực hiện việc tấn công đối phương. thực chất của **DoS** là **attacker** sẽ chiếm dụng 1 lượng lớn tài nguyên trên **Server** làm cho **Server** không thể nào đáp ứng yêu cầu của người dùng khác và **Server** có thể nhanh chóng bị ngừng hoạt động hay bị treo. **Attacker** làm tràn ngập hệ thống có thể là bằng tin nhắn, tiến trình, hay gửi những yêu cầu đến hệ thống mạng từ đó buộc hệ thống mạng sẽ sử dụng tất cả thời gian để khứ hồi tin nhắn và yêu cầu. nhiều lúc dẫn đến việc bị tràn bộ nhớ. Khi sự làm tràn ngập dữ liệu là cách đơn giản và thông thường nhất để phủ nhận dịch vụ thì 1 **attacker** không ngoan hơn sẽ có thể tắt dịch vụ, định hướng lại và thay thế theo chiều hướng có lợi cho **attacker.**

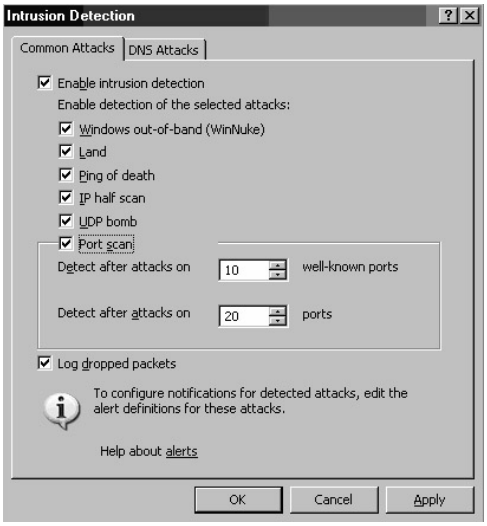
**SYN Attack/LAND Attack:** bằng cách lợi dụng cơ chế bắt tay đối với một số dịch vụ dựa trên chuẩn giao thức **TCP**, **Client** tấn công theo kiểu **SYN attack** bằng cách gởi một loạt **SYN packets** mà có địa chỉ nguồn giả, điều này **Client** có thể làm tràn ngập (**flooded**) hàng đợi **ACK** của gói **SYN/ACK** gởi cho **Client** từ **Server**, đến một lúc nào đó **Server** sẽ bị quá tải.

**Ngoài ra còn có một số phương thức tấn công khác như: Ping of Death**, **Teardrop**, **Ping Flood** (**ICMP Flood**), **SMURF Attack**, **UDP Bomb**, **UDP Snork Attack**, **WinNuke** (**Windows Out-of-Band Attack**), **Mail Bomb Attack**, **Scanning and Spoofing**, **Port Scan**.

Để cho phép **ISA Firewall** có thể **dectect** và ngăn một số phương thức tấn công trên ta truy xuất vào hộp thoại **Intrusion Detection** bằng cách mở giao diện "**Microsoft Internet Security and Acceleration Server 2004 management console**", chọn nút **Configuration**. Chọn nút **General,** sau đó ta nhấp chuột vào liên kết "**Enable Intrusion Detection and DNS Attack Detection"** (tham khảo hình 5.33)

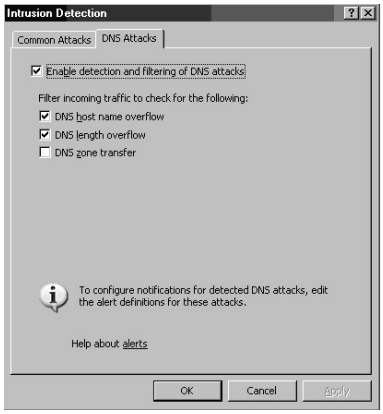


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 5.33: Phát hiện một số cơ chế tấn công.

Chọn **DNS Attacks Tab** để hiệu chỉnh một số phương thức ngăn, ngừa tấn công theo dịch vụ **DNS** (tham khảo hình 5.34 ).



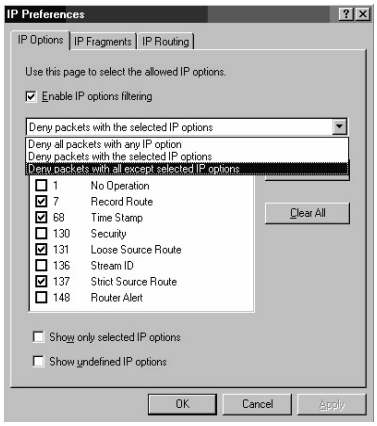

Hình 5.34: Phát hiện và ngăn tấn công DNS.

- **IP option filtering**.

Ta có thể thiết lập một số bộ lọc cho giao thức **IP** để chống lại một số cơ chế tấn công dựa vào một số tùy chọn của giao thức này. Để cấu hình ta chọn liên kết **Define IP preferences** trong nút **Configuration** (tham khảo hình 5.35).



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 5.35: IP option filtering.

## V.7. Một số công cụ bảo mật.

### V.7.1 Download Security.

**DownloadSecurity** là một công cụ tích hợp với **ISA** được tổ chức **GFI Software LtdGFI** phát triển. **DownloadSecurity** được thiết kế để tăng cường khả năng kiểm soát và quản lý thông tin **download** từ **Internet**. Một số chức năng về **DownloadSecurity**:

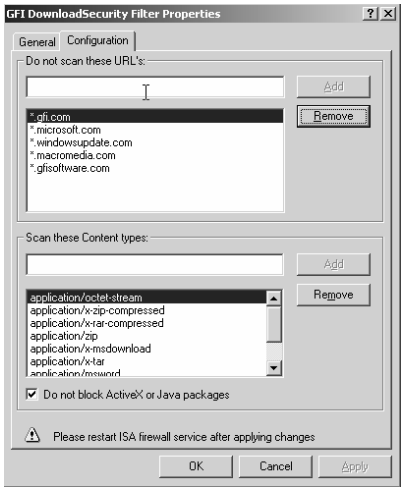
- **Scan viruses** cho tất cả các tập tin được **download** từ **internet**.
- Tự động cập nhật **Anti-virus signature**.
- Tự động kiểm tra một số loại file nguy hiểm như *.exe, *.doc,…
- Cung cấp cơ chế cảnh báo an ninh cho người quản trị.
- Được tích hợp với **ISA Firewall**, dễ quản lý và cấu hình.
- Tính hiệu quả cao trong việc thực hiện một số chức năng như lọc nội dung, chống virus, kiểm soát truy xuất internet.
- Cung cấp cơ chế cảnh báo **user** hoặc trình duyệt chặn một số **ActiveX Control** và **Java applet** nguy hiểm.
- Phân tích các đoạn code thực thi nguy hiểm để chống **Trojans**.
- Cấu hình **ISA Web Filtering**.

Mặc định sau khi ta cài phần mềm **DownloadSecurity**, **DownloadSecurity** sẽ tự động được kích hoạt để hỗ trợ thiết lập bộ lọc **Web Filters**. Để hiệu chỉnh bộ lọc ta chọn **Configuration | Add-ins | Web Filters | GFI DownloadSecurity Filter | Configuration Tab** (tham khảo Hình 5.36).

- **Do not scan these URLs:** Chỉ định danh sách địa chỉ **URL** không cần kiểm tra nội dung và virus.
- **Scan these Content types:** Chỉ định loại nội dung cần kiểm tra bao gồm các đoạn code có thể thực thi, **Java applets**, **ActiveX Control**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

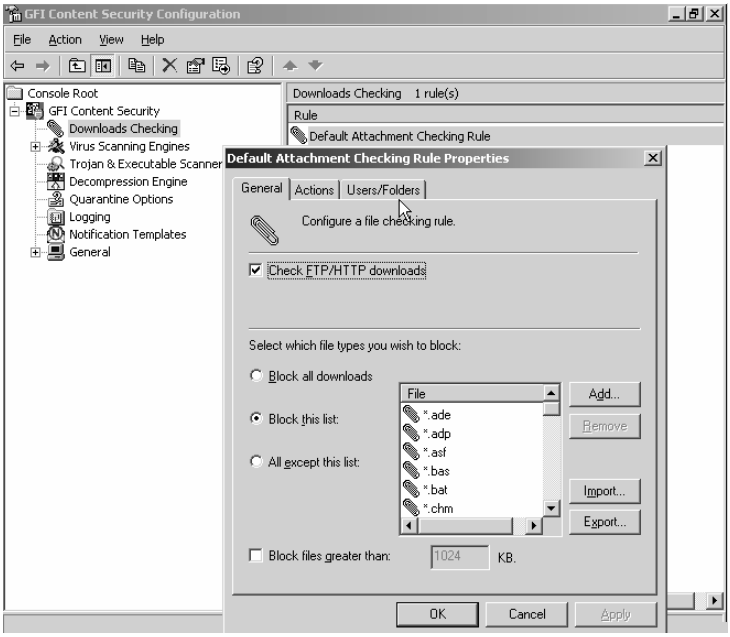



Hình 5.36: Download security Web Filter.

Thiết lập một số chính sách kiểm tra **download**.

Thiết lập chính sách kiểm tra **download** để giới hạn hoặc cô lập loại **file**, dung lượng **file download**,… để thay đổi luật **download** mặc định trong hệ thống bằng cách chọn **Start | Programs | GFI DownloadSecurity | DownloadSecurity Configuration | Download Checking**, Nhấp đôi chuột vào rule có tên **"Default Attachment Download Checking Rule"** (tham khảo hình 5.37)

- **General Tab:** Cho phép lựa chọn một số chế độ cấm **download**, cấm **download** các tập tin có dung lượng lớn hơn dung lượng định nghĩa.
- **Actions Tab:** Hiệu chỉnh các **Action** khi cấm như thông báo Mail, quản lý thông báo qua mail, ghi nhận nhật ký,…
- **Users/Folders Tab:** Chọn **User** hoặc thư mục cần thiết để thiết lập luật.




Hình 5.37: Thay đổi thuộc tính của **Download checking rule**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

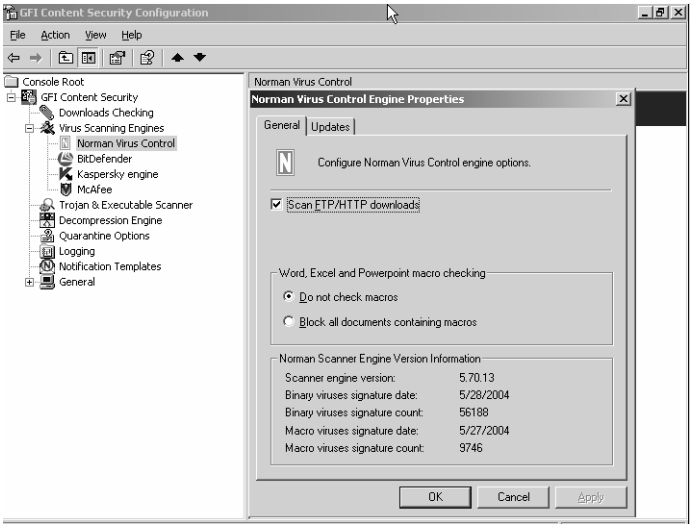
Cấu hình kiểm tra **Virus**, chống **Trojans**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

**DownloadSecurity** tích hợp sẵn các chương trình kiểm tra và quét **virus** cho các **file download**, các chương trình này được cập nhận thường xuyên để có thể ngăn chặn sự tấn công của các loại **Virus** mới. Ngoài ra **DownloadSecurity** còn tích hợp một số scanners để **scan** và kiểm tra **Trojans**, đoạn mã thực thi nguy hiểm (**Executable**)

Để thay đổi hiệu chỉnh một số bộ kiểm tra **Virus** (**Virus Engine**) ta chọn **Start | Programs | GFI DownloadSecurity | DownloadSecurity Configuration | Virus Scanning Engines**, Nhấp đôi chuột vào một **engine** cụ thể (Tham khảo hình 5.38)




hình 5.38: Hiệu chỉnh thuộc tính của **Virus Control Engine**.

### V.7.2 Surfcontrol Web Filter.

**SurfControl Web Filter** giúp nâng cao tính năng bảo mật, tối ưu hóa băng thông của hệ thống. **SurfControl Web Filter** thiết sẵn một group các đối tượng để cho phép ta quản lý và thiết lập luật để giới hạn truy xuất **Internet** dễ dàng hơn.

**Một số công cụ hỗ trợ trong SurfControl Web Filter:**

- **Monitor**: Cung cấp một số cách theo dõi và giám sát **traffic** của các **user** trong mạng, thông tin về giám sát hoạt động của **user** được lưu trong **SurfControl database**, chúng được hiển thị trong cửa sổ **the Monitor window**.
- **Real Time Monitor:** Giám sát và hiển thị **traffic** mạng theo thời gian thực.
- **Rules Administrator:** Cho phép ta có thể tạo luật để điều khiển truy xuất **internet**.
- **Scheduler:** Cho phép thiết lập lịch biểu để theo dõi sự kiện hệ thống.
- **Virtual Control Agent (VCA)**: Phân loại **Web site** theo nội dung truy xuất.
- **Report Central**: là công cụ mạng hỗ trợ tạo **report** để thống kê **traffic**.
- **Remote Administration:** Cho phép điều khiển từ xa **SurfControl Web Filter**.

Database của chương trình **SurfControl Web Filter** được lưu trên một hệ quản trị cơ sở dữ liệu, có thể là **MS SQL Se**rver, **msde2000**, do đó trước khi cài đặt **SurfControl Web Filter** ta cần phải cài đặt một trong hai hệ quản trị cơ sở dữ liệu trên.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

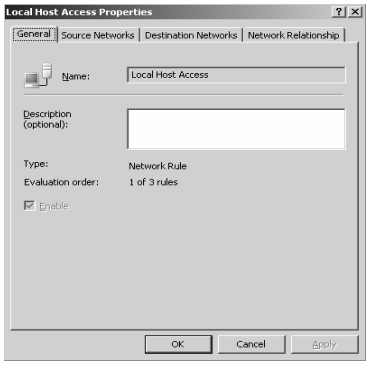
## V.8. Thiết lập Network Rule.

Mặc định hệ thống tạo ra các **Network rule** để cho phép thiết lập một số cơ chế như định tuyến (**Route**) giữa hai mạng (tham khảo hình 5.39), thay đổi đĩa chỉ (**NAT**). Mặc định hệ thống tạo ra một số **Network rule** sau:

- **Local Host Access**: Định tuyến traffic localhost đến mạng nội bộ.
- **VPN Client to Internal Network**: Định tuyến từ **VPN Client** đến **Internal network**.
- **Internet Access**: **NAT Internal network** ra ngoài mạng **internet**.

### V.8.1 Thay đổi thuộc tính của một Network Rule.

Để thay đổi thuộc tính của **Network Rule** ta nhấp đôi chuột vào tên luật trong **Network Rules tab** (tham khảo hình 5.39).

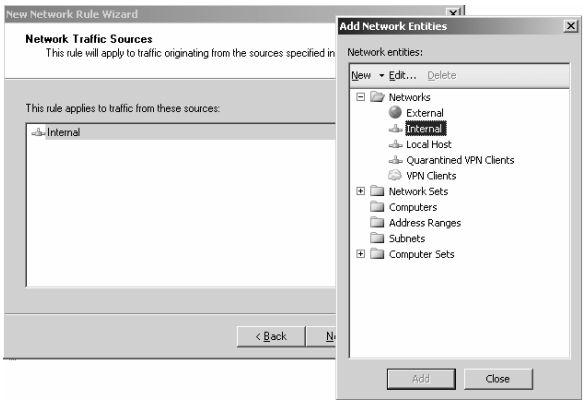



Hình 5.39: Thay đổi thuộc tính cho **Network Rule**.

### V.8.2 Tạo Network Rule.

Để tạo **Network Rule** ta thực hiện các bước sau:

1. Chọn nút **Configuration**, chọn **Network**, chọn **Network Rules tab**, **Create a New Network Rule** trong **Task Panel**, chỉ định tên **Network Rule**, chọn **Next**.
2. Chỉ định địa chỉ nguồn trong hộp thoại **Network Traffic Source**.

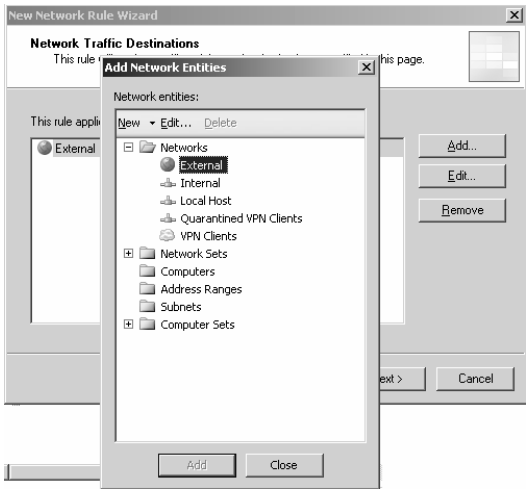



Hình 5.40: Chỉ định địa chỉ nguồn.

3. Chỉ định địa chỉ đích trong hộp thoại **Network Traffic Destination**.

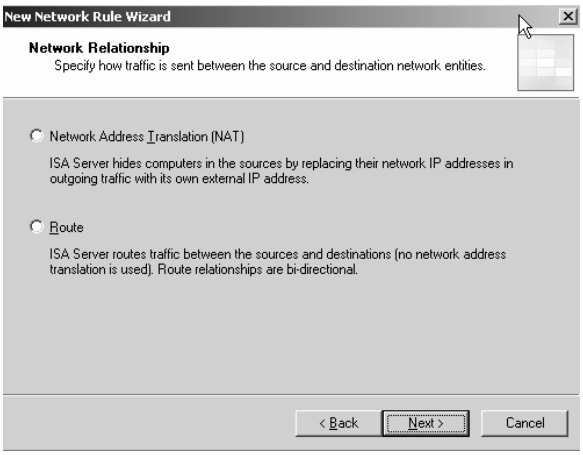


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 5.41: Chỉ định địa chỉ đích cho **Network Rule**.

4. Chọn phương thức đặt **Network Rule** theo **NAT** (khi ta muốn **NAT** cho mạng nội bộ ra ngoài mạng **Internet**) hay **Route** (khi ta muốn định tuyến mạng nội bộ ra ngoài mạng khác)




Hình 4.42: Chỉ định **Network Relationship**.

5. Chọn **Finish** để hoàn tất quá trình.

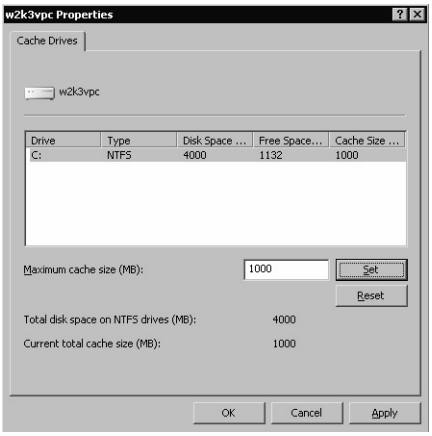
## V.9. Thiết lập Cache, quản lý và theo dõi traffic.

### V.9.1 Thiết lập Cache.

- Để cấu hình **Cache** ta chọn nút **Configuration -> Cache** của trình quản lý **ISA management**:
- Nhấp chuột phải vào nút **Cache** chọn **Define Cache Drives,** hoặc ta có thể nhấp chuột vào **Cache Rules** sau đó chọn **Define Cache Drives (enable caching)** từ **Tasks** panel**.**
- Trong hộp thoại **"Define Cache Drives"** chọn một ổ địa định dạng **NTFS** và chỉ định kích thước cache **Maximum cache size** , chọn nút **Set** (tham khảo hình 5.39).



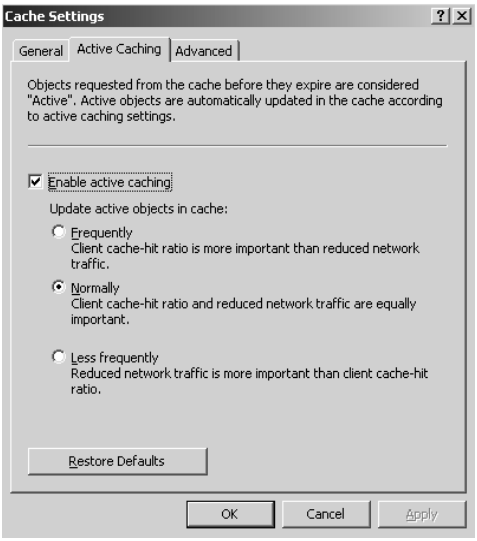
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 5.43: Chỉ định dung lượng Cache.

### V.9.2 Thay đổi tùy chọn về vùng Cache.

- Để cấu hình **Cache** ta chọn nút **Configuration -> Cache** của trình quản lý **ISA management**, nhấp chuột phải vào nút **Cache** chọn liên kết **Configure Cache Settings** từ **Tasks** panel, chọn **Active Caching** tab, chọn **Enable active caching** (tham khảo hình 5.40)**.**




Hình 5.44: **Enable cache**.

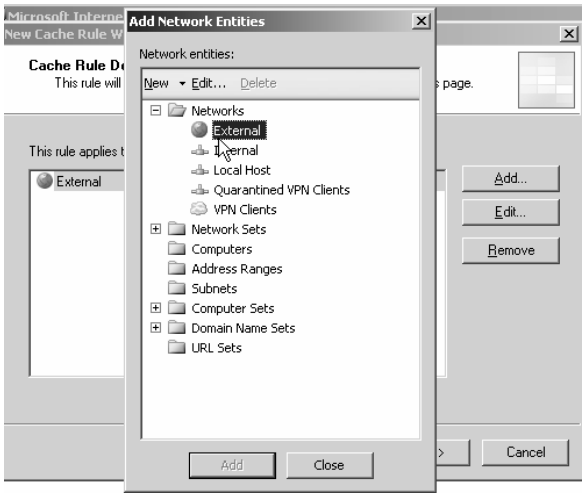
### V.9.3 Tạo Cache Rule.

Tạo **Cache Rule** để cho phép ta có thể đặt một số luật quy định đối tượng (**Object**) cần **cache**, thời gian lưu trữ **cache**, kích thước của từng đối tượng **cache**, … Các bước tạo **cache rule** như sau:

1. Nhấp chuột phải vào nút **Cache**, chọn **New,** chọn **Cache Rule…**
2. Chỉ định tên **cache rule** trong hộp thoại **"Welcome to the New Cache Rule Wirzard**", chọn **Next**.
3. Chọn nút **Add** để chỉ **Distination** cho **Cache Rule** (tham khảo hình), chọn **Next**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

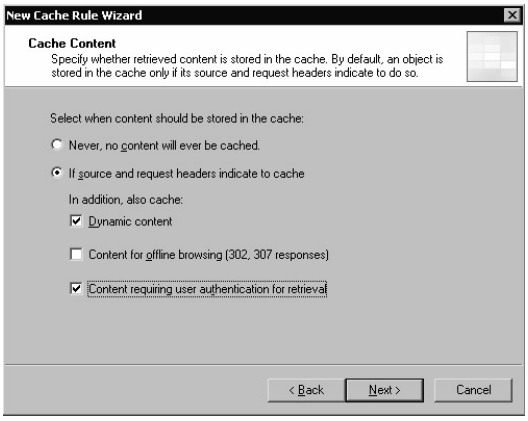



Hình 5.45: Destination cache.

4. Chỉ định loại **Object** nào được nhận cho một **request** cụ thể nào đó trong hộp thoại **Cache retrieval**. Một số tùy chọn cần lưu ý:
   + **"Only if a valid version of the object exists in the cache if no valid object exists, the request will be routed to the Web server"**: Cho phép nhận những **Object** hợp lệ (**Valid Object)** trong **cache** ngược lại tồn tại hoặc không tồn tại **Object** hợp lệ thì **request** sẽ được chuyển đến **Web Server** để nhận các **Object** cần thiết.
   + **"If any version of the object exists in the cache it will be returned from cache If no version exists route request server"** : Cho phép **request** có thể nhận **Valid Object** hoặc **Invalid Object** trong **cache**, nếu không có **Object** nào trong **cache** thì **Server** sẽ chuyển **request** tới **server**.
   + **"If any version of the object exists in cache if no exists the request will be dropped"** Nếu **request** yêu cầu một **Object** nào đó không tồn tại trong **cache** thì nó sẽ bị ngăn chặn (**Drop**)
5. Trong hộp thoại **Cache Content**, chỉ định nội dung cần lưu trong **cache**(tham khảo hình 5.41), chọn **Next**.

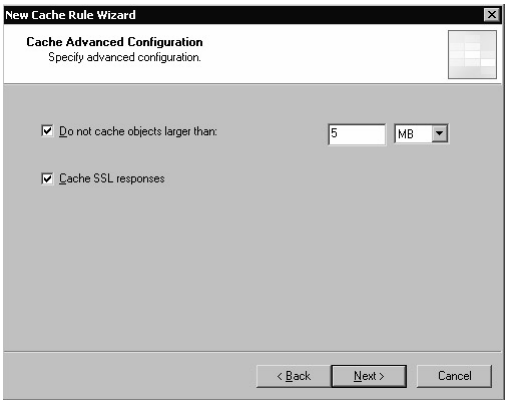


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net



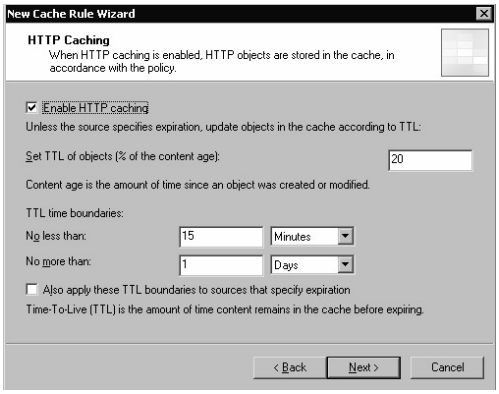

Hình 5.46: **cache content**.

6. Trong hộp thoại **Cache Advanced Configuration**, định giới hạn kích thước của các object cần được **cache** trong **textbox "Do not cache objects larger than"** (tham khảo hình 4.42), chọn **Next**.




Hình 5.47: Giới hạn kích thước cho đối tượng **cache**.

7. Chỉ định thời gian lưu trữ **HTTP Object** trong **cache**, chọn **Next**.

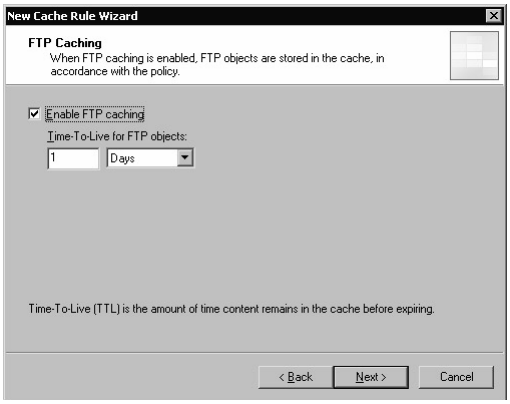



Hình 5.48: Chỉ định **TTL** cho **HTTP Object**.

8. Chỉ định thời gian lưu trữ **FTP Object** trong **cache**, chọn **Next**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net



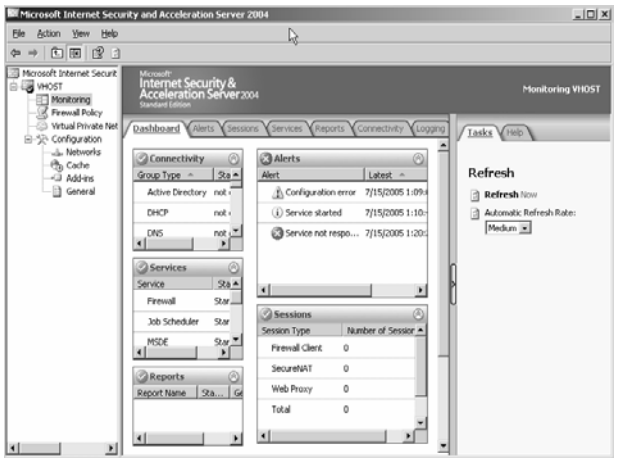

Hình 5.49: **TTL** của **HTTP Object**.

9. Chọn **Finish** để hoàn tất quá trình.

### V.9.4 Quản lý và theo dõi traffic.

Một trong những chức năng qua trong của **Firewall** là khả năng giám sát (**monitoring**) và thống kê (**reporting**) sự kiện xảy ra trong hệ thống, nó giúp cho Người quản trị mạng (**Network administrator**) có thể theo dõi sự xâm nhập (**attempted intrusions**) và tấn công từ bên ngoài.

**ISA Server 2004** bao gồm một số công cụ như: giám sát hoạt động của hệ thống (**monitor ISA Server activities**), tạo và cấu hình cơ chế cảnh báo, thống kê thông tin hệ thống, giám sát thông suất (**performance**) của **ISA Server**. Tất cả các công cụ này đề được đặt tại **Monitoring node** của trình quản lý **"ISA Server 2004 management console"** (tham khảo hình 5.44).




Hình 5.50: Dashboard theo dõi **log**.

Thiết lập một số cảnh báo (**alert**) cho hệ thống



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

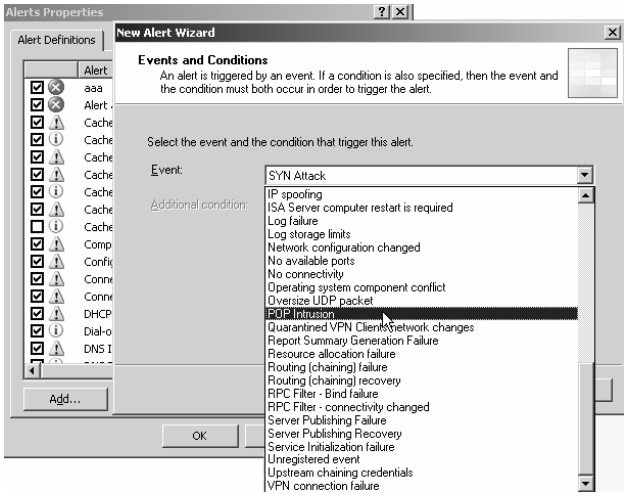
+ Chọn **Tab Alerts**, chọn liên kết **Configure Alert Definitions** trên **Task** panel, chọn nút **Add** từ hộp thoại **Alert properties,** chỉ định tên **Alerts,** chọn **Next** (tham khảo hình 5.45).


Hình 5.51: Lập cảnh báo cho hệ thống.



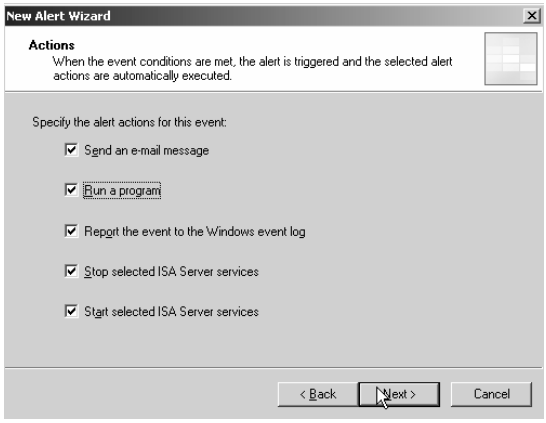
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

+ Chọn loại sự kiện để lập cảnh báo cho hệ thống, chọn **Next**.




Hình 5.52: Chọn loại cảnh báo cho hệ thống.

+ Chỉ định loại cảnh báo (**Alert**) và mức độ kiểm soát (lỗi, cảnh báo, thông báo) trong hộp thoại **Category and Severity**, chọn **Next**.
+ Chỉ định các **action** để thực hiện cơ chế cảnh báo cho hệ thống, có thể cảnh báo qua Mail, chương trình, …(tham khảo hình 5.46)

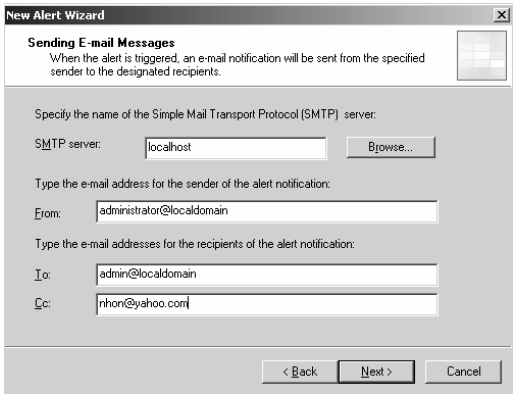



Hình 5.53: Chọn cơ chế cảnh báo.

+ Chỉ định địa chỉ Email sẽ nhận cảnh báo của hệ thống, chọn **Next**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net





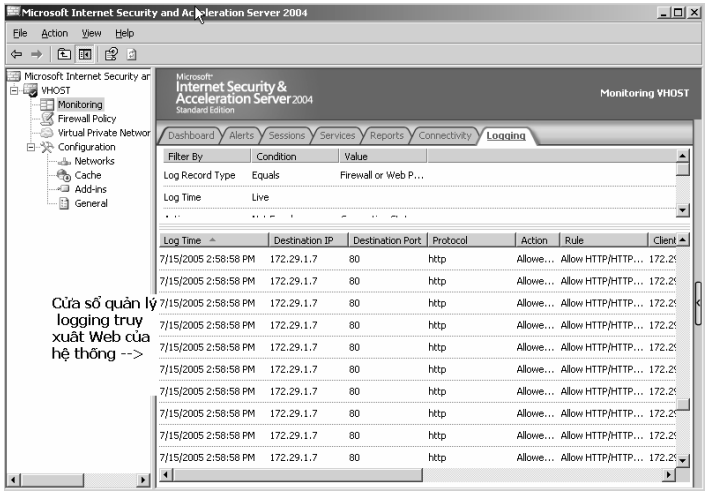

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Hình 5.54: Chọn cơ chế cảnh báo.

+ Chọn dịch vụ sẽ bị **stop** khi **Alert** gặp sự cố, chọn **Next**.
+ Chọn **Finish để hoàn tất quá trình.**

Theo dõi thông tin truy xuất **Web** trong mạng nội bộ

Để theo dõi từng máy tình hoặc từng **host** trong mạng nội bộ truy xuất **internet** ta chọn **Logging Tab** từ màn hình chính của **Monitoring node** (tham khảo hình 5.47).




Hình 5.55: Theo dõi log truy xuất **Web**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

# Tóm tắt

Lý thuyết 6 tiết - Thực hành 0 tiết

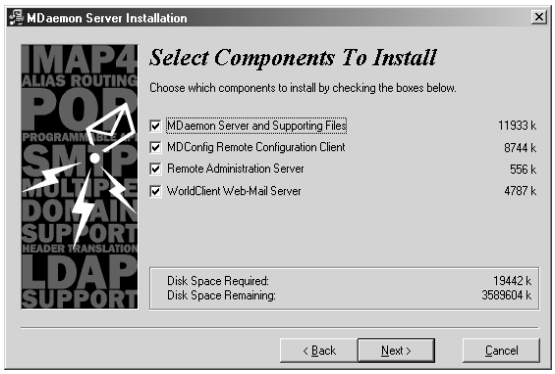
| Mục tiêu | Các mục chính | Bài tập bắt buộc | Bài tập làm thêm |
|---|---|---|---|
| Kết thúc bài học này giúp cho học viên biết thêm một số phần mềm Mail Server và Proxy Server được sử dụng rộng rãi trên thị trường. Đồng thời học viên cũng có thể so sánh với các phần mềm đã học để có một lựa chọn chính xác khi triển khai trong một môi trường thực tế. | I. Phần mềm Mail Server - MDaemon<br>II. Phần mềm Proxy Server - WinGate | Dựa vào bài tập môn Dịch vụ mạng Windows 2003. | Dựa vào bài tập môn Dịch vụ mạng Windows 2003. |



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

# I. Cài Đặt Mdaemon.

1. Click vào tập tin cài đặt có tên **setup.exe** sau đó màn hình **License** sẽ hiện ra. Để tiếp tục, hãy nhấn nút **I Agree**.
2. Chọn thư mục để cài đặt, mặc định chương trình **MDaemon** sẽ cài vào ổ đĩa cài hệ điều hành. Ta có thể cài **Mdaemon** ở một vị trí khác bằng cách chọn nút **Browse**, chọn **Next** để tiếp tục việc cài đặt.
3. Nhập tên **user** và tên công ty, chọn **Next** để tiếp tục việc cài đặt.
4. Chọn các thành phần sẽ cài đặt
   - + **MDaemon server and supporting Files**: cài chương trình **Mdaemon Server**.
   - + **MDConfig Remote Configuration Client :** điều khiển những biến cấu hình **MDaemon** từ xa.
   - + **Remote Administration Server:** Quản trị **Mail Server** từ xa
   - + **WorldClient Web-Mail Server:** Cấu hình **Web-Mail Server** để cho phép những **Client** gửi/nhận mail ở bất kỳ nơi nào.

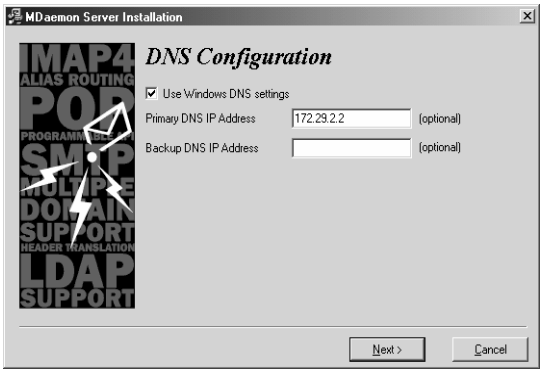



Hình 6.1: Chọn thành phần cài đặt.

5. Sau khi nhấn **Next**, trình **Setup MDaemon** sẽ sao chép các file vào thư mục đã chọn, tạo folder chương trình **MDaemon** và bước kế tiếp là cấu hình cho **MDaemon**.

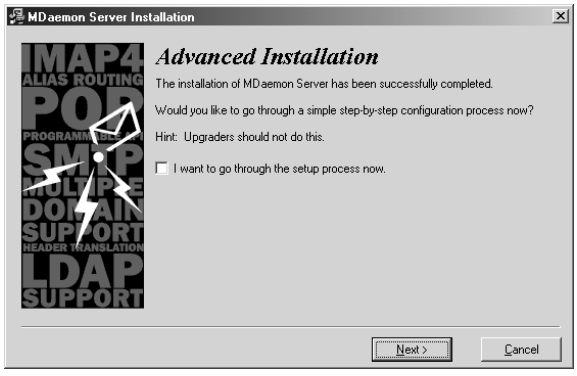


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 6.2: Chỉ định **DNS Server**.

6. Cấu hình **DNS Server**: Trong quá trình cài đặt bạn không cần hoặc cần chỉ ra những **DNS Server** bằng cách chọn nút **Use Windows DNS Se**ttings. Sau đó, chỉ ra địa chỉ **IP** của **Primary DNS Server** và **Backup DNS Server**.
7. Nhập vào những thông tin của **user** để **MDaemon** tạo ta **account** trong quá trình setup.
   + **Full Name:** nhập vào tên đầy đủ của **account**. Ví dụ Tran Thanh Tri
   + **Mailbox:** địa chỉ Email của **account** (không bao gồm tên domain)
   + **Password:** nhập vào **password** cho **account** (Không có khoảng trắng)
   + **This account is the Postmaster:** chỉ định **account** này là **Postmaster alias**.
   + **This account has Administration level web access**: cho phép **account** này có quyền quản trị khi truy cập Mail qua **Web**.
   + Nhấn **Next để tiếp tục việc cài đặt.**
8. Chọn chế độ khởi động **MDaemon Server**: Nếu bạn muốn chương trình **MDaemon** khởi động khi máy tính bật lên thì chọn **Setup MDaemon as a system service**. Khi cấu hình ở chế độ này, bạn không cần **logon** vào **Server** để thao tác.
9. Tiếp theo là màn hình cho phép lựa chọn việc cấu hình theo hướng dẫn (**wizard**) hay không?




Hình 6.3 chọn chế độ **configure** qua **Wizard**.



# II. Cấu hình Mail Server.

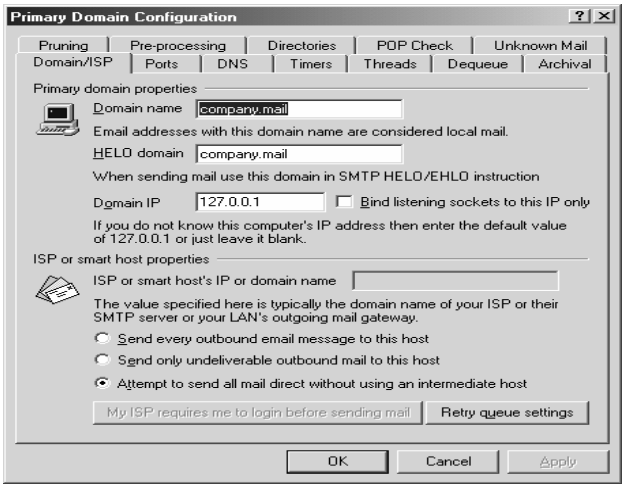
- Sau khi cài đặt chương trình **Mdaemon**, bước quan trọng kế tiếp là chúng ta phải cấu hình **Domain** của mình để người dùng trong **domain** có thể gửi/ nhận mail.

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

- Tất cả những thao tác cấu hình **domain** thông qua menu **Setup | Primary Domain.**



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 6.4: Cấu hình domain cho **Mail Server**.

## II.1. Cấu hình Domain/ISP.

Hộp thoại này lưu những thông tin về địa chỉ **IP** và **domain name**. Thêm vào đó, chúng ta sẽ chỉ ra mức độ mà **Mail Server** sẽ chuyển mail đến **ISP** hay **gateway**.

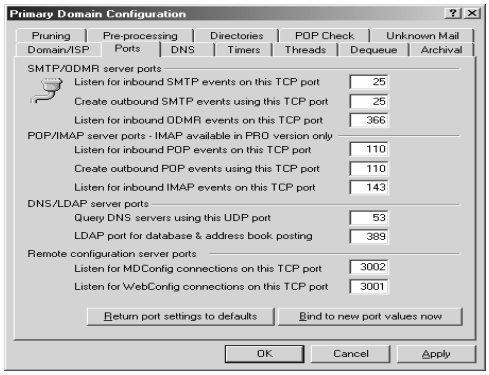
- **Domain Name:** Nhập vào tên **domain**. Tên **domain** này mặc định khi tạo **account** và nó được đăng ký trên **Internet**.
- **HELO domain:** Tên **domain** này sẽ được sử dụng trong câu lệnh **SMTP HELO/EHLO**.
- **Domain IP:** Địa chỉ **IP** của **Primary Domain**.
- **ISP or smart ...:** chỉ ra **ISP** của bạn hoặc tên của máy Mail hoặc địa chỉ **IP**. Thông thường, chúng ta chỉ ra địa chỉ IP của **SMTP Server ISP**.
- **Send every outbound ...:** tất cả những Mail gửi ra khỏi domain đều chuyển đến máy gateway. Máy **gateway** được chỉ ra trong ISP or smart...
- **Send only ...:** chỉ những Mail gửi ra ngoài mà không được chuyển đến đích sẽ được chuyển đến **Mail Gateway** chỉ ra trong **ISP or Smart**...
- **Attempt ...:** Gửi tất cả những **mail** ra ngoài đến một máy trung gian. Những **mail** không gửi được sẽ được gửi lại theo những cấu hình trong phần **Retry queue setting**.

## II.2. Cấu hình Ports.

Chỉ ra những port mà chương trình **Mdaemon** giám sát. Và những **port** mà chúng ta cấp cho **SMTP**, **POP**, **IMAP** hay **UDP** để truy vấn **DNS**. Thông thường, chúng ta không thay đổi những thông số mặc định này.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

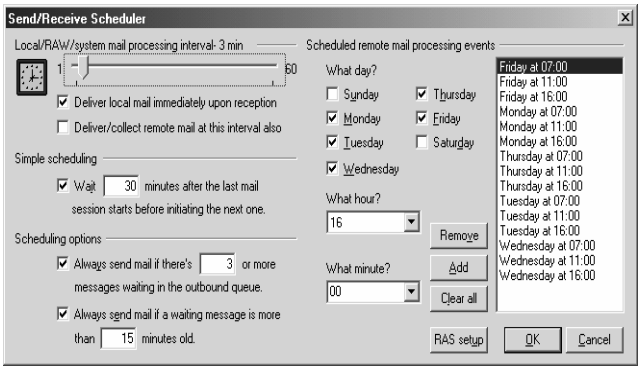



Hình 6.5: Chỉ định giá trị **Port**.

# III. Cấu hình lịch kết nối và dịch vụ quay số.

## III.1. Lập lịch kết nối.

- Click vào menu **Setup** | **Send/receive scheduling**




Hình 6.6: Lập lịch biểu kết nối quay số.

- **Local/RAW/system mail processing interval- 3 min**: thời gian nghỉ giữa các giao dịch xử lý Mail là 1 – 60 phút.
  + **Deliver/collect remote mail...:** nếu **checkbox** này được chọn thì thời gian phân phối/tập hợp mail sẽ dựa trên **Local/RAW/system mail**.... Ngược lại, nó sẽ hoạt động dựa trên lịch mà chúng ta lập.
  + **Deliver local mail... :** xử lý và phân phát ngay sau khi một giao dịch **SMTP** hoàn thành. Điều này có tác dụng phân phát Mail cục bộ ngay lập tức.
- **Simple scheduling:** thời gian nghỉ giữa lần giao dịch Mail cuối cùng được **start** trước khi khởi tạo một giao dịch mới.

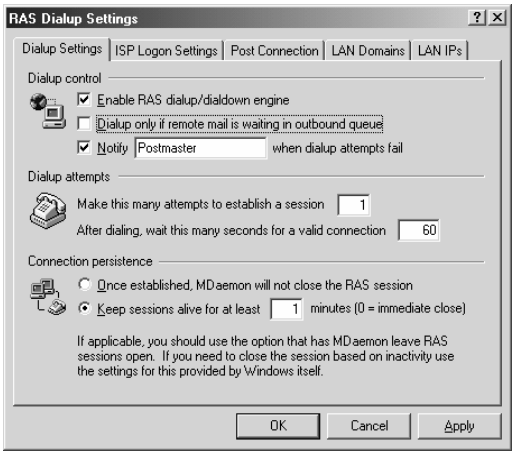


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

+ **Scheduling options:** Hiệu chỉnh tùy chọn về lịch biểu.
+ **Always send mail if there's ...: Mdaemon** sẽ khởi tạo một giao dịch nếu trong hàng đợi ra ngoài có từ **xx messages** trở lên.
+ **Always send mail if a waiting...: Mdaemon** sẽ khởi tạo một giao dịch nếu có một **message** trong hàng đợi ra ngoài đợi đến số phút chỉ định.
+ **Scheduled remote mail ...:** lập lịch để **Mdaemon** xử lý Mail bao gồm ngày, giờ, phút.

## III.2. Cấu hình Quay số.

- Click vào **Setup | Dialup/Dialdown**.




Hình 6.7: Cấu hình kết nối quay số.

- Dialup Settings.
- ISP Logon Settings.
- Post Connection.
- LAN Domains.
- LAN Ips.

### III.2.1 Dialup Settings.

- **Dialup control**:
  + **Enable RAS Dialup/Dialdown Engine**: Chọn tuỳ chọn này cho phép dùng dịch vụ **RAS** kết nối vào **ISP** để gửi và nhận thư.
  + **Dialup Only if Remote Mail is Waiting in Outbound Queue** Chọn tuỳ chọn này để **MDaemon** chỉ quay số kết nối khi có thư gửi ra (**outbound message**) trong hàng đợi chờ gửi. Tuỳ chọn này cho phép tiết kiệm thời gian quay số tuy nhiên nếu không quay số thì **MDaemon** sẽ không lấy được thư từ bên ngoài gửi vào.
  + **Notify Postmaster When Dialup Attempts Fail** Gửi thông báo đến **Postmaster** xử lý khi có lỗi không quay số được.
- **Dialup attempts**:

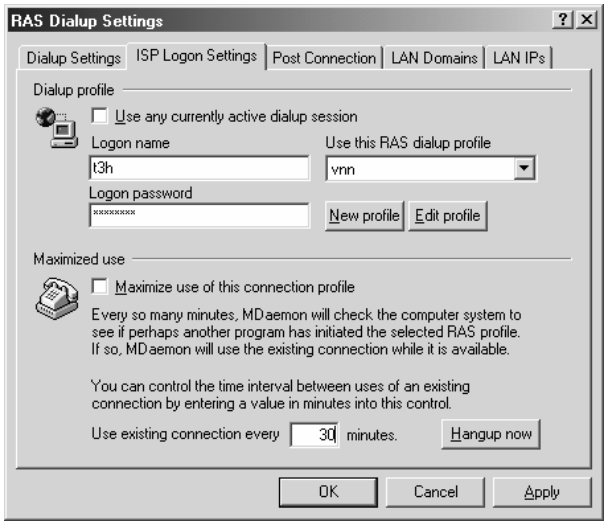


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

+ **Make This Many Attempts To Establish A Session:** Số lần thử quay số kết nối máy ở xa.
+ **After Dialing, Wait This Many Seconds For A Valid Connection**: Thời gian **MDaemon** chờ cho máy ở xa trả lời và hoàn thành kết nối **RAS**.

- **Connection persistance**:
  + **Once Established, MDaemon Will Not Close The RAS Session** Mặc định **MDaemon** sẽ đóng phiên kết nối **RAS** sau khi việc gửi nhận Mail với máy ở xa hoàn tất. Đánh dấu tuỳ chọn này cho phép phiên làm việc cho dù đã hoàn thành việc gửi nhận.
  + **Keep Sessions Alive For At Least XX Minutes** Thời gian giữ kết nối trước khi đóng.

### III.2.2 ISP Logon Settings.



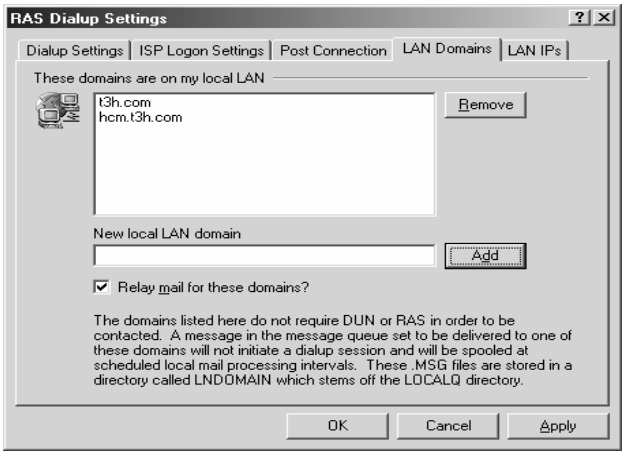

Hình 6.8: Chỉ định **Account** kết nối quay số.

- **Logon Name:** Tên logon dùng để chuyển cho máy ở xa trong quá trình đăng nhập
- **Password:** Mật khẩu dùng để chuyển cho máy ở xa trong quá trình đăng nhập
- **Use This RAS Dialup Profile:** Tên **profile** đã tạo dùng cho kết nối từ xa trong cửa sổ **Dialup Networking**.
- **Maximize Use of this Connection Profile:** Cho phép **MDaemon** theo dõi **profile** được mô tả ở trên, trong trường hợp **profile** này đang dùng để kết nối thì **Mdaemon** sẽ dùng luôn kết nối này để gửi nhận Mail mà không theo lịch.
- **New Profile:** Tạo mới **profile Dialup Networking**.
- **Edit Profile:** Sửa **profile Dialup Networking**.
- **Hang-up Now:** Ngắt kết nối **RAS** với **ISP**. Nút này chỉ sáng lên khi đang có kết nối.

### III.2.3 LAN Domains.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net



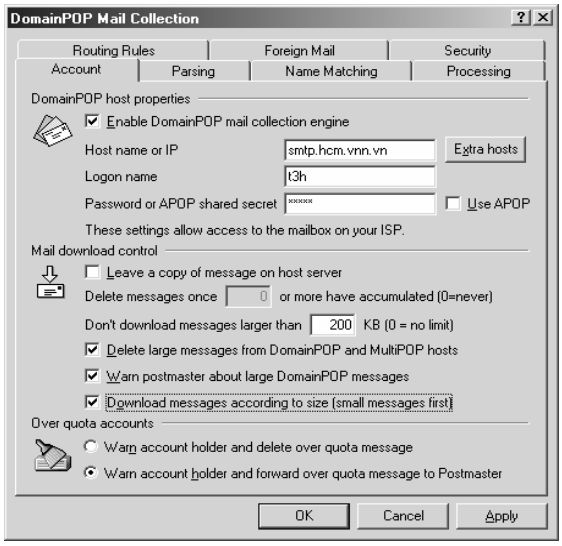

Hình 6.9: Chỉ định tên **domain** cho **Mail Server** quản lý.

- **These Domains Are On My Local LAN** Các domain liệt kê ở đây được **MDaemon** xem như domain cục bộ của mạng cục bộ **LAN**. Như vậy không cần phải quay số khi có thư gửi cho **domain** cục bộ.
- **New Local LAN Domain** Thêm 1 tên **domain LAN** cục bộ và nhấn nút **ADD**.
- **Relay Mail For These Domains** Nếu chọn tuỳ chọn này **MDaemon** sẽ chuyển tiếp mail cho các **domain** trên.

# IV. Cấu hình DomainPOP Mail.

Cấu hình **DomainPOP** nhằm mục đích nhận mail từ **POP mailbox** từ **ISP** để phân phát lại cho người dùng trong **domain**.

- Từ menu **Setup** chọn **DomainPOP mail collection**...
- Chọn tab **Account** để khai báo những thông số.




Hình 6.10: Chỉ định **pop Mail Server**.

- **DomainPOP host properties**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

+ **Enable Domain Pop Mail Collection:** Chọn tuỳ chọn này cho phép **MDaemon** lấy thư từ hộp thư trên **POP server** của **ISP** về phân phát lại cho các **user** nội bộ.
+ **Host name or IP:** Tên **DNS** hoặc địa chỉ **IP** của máy chủ **POP** của **ISP**.
+ **Logon name/Password:** Tên **user** và mật khẩu dùng để lấy thư trên máy chủ **ISP**.

- **Mail download control**.
  + **Leave a copy of message on host server:** nếu chọn, **Mdaemon** sẽ không xóa những mail được tập hợp từ **ISP**.
  + **Don't download messages larger than [XX] KB (0 = no limit) :** không **download** những messages > xx KB.
  + **Delete large messages from DomainPOP and MultiPOP hosts: Mdaemon** sẽ xóa những message có kích thước vượt quá qui định bằng cách xóa chúng từ **DomainPOP** và không **download** về.
    - **Warn postmaster about large DomainPOP messages: gửi một thông báo đến Postmaster khi có một message lớn được phát hiện trong DomainPOP mailbox.**
  + **Download messages according to size (small messages first):** cho phép **Mdaemon download message** theo kích thước từ nhỏ nhất đến lớn nhất.
- **Over quota accounts**.
  + **Warn account holder and delete over quota message**: nếu chọn, **Mdaemon** sẽ gửi **message** đến cho **user** khi dung lượng đĩa của **user** vượt quá giới hạn cho phép. Những **message** sau đó sẽ bị hủy.
  + **Warn account holder and forward over quota message to Postmaster**: nếu chọn, **Mdaemon** sẽ gửi **message** đến cho **user** và **Postmaster** thông báo dung lượng đĩa của **user** vượt quá giới hạn cho phép.

# V. WorldClient Server.

- **World Client** là một giải pháp của **webmail**, cho phép các máy trạm có thể sử dụng mail thông qua trình duyệt Web, các **user** có thể truy cập Mail của mình ất cứ nơi nào.
- Các tính năng lợi của **workclient server**: cho phép tìm kiếm thư, đọc thư từ trình duyệt Web, Client có thể giao tiếp bằng nhiều ngôn ngữ, hỗ trợ cơ chế lưu địa chỉ, có thể quản lý các thư mục(chứa danh sách các Mail được lưu trữ ), gởi nhận **file attachment**…
- Ngoài ra **world client** còn cung cấp:
  + **Calendar and scheduling system**(lập lịch biểu cho hệ thống )
  + **ComAgent's Instant Messaging System**: cung cấp các thông báo(**sound**, **visual alert**) khi có thư mới.

## V.1. Cách Cấu Hình WorldClient server.

Khởi tạo **world client** ta chọn **Setup**->**WorldClient/RelayFax**… -> **Enable worldclient server**.

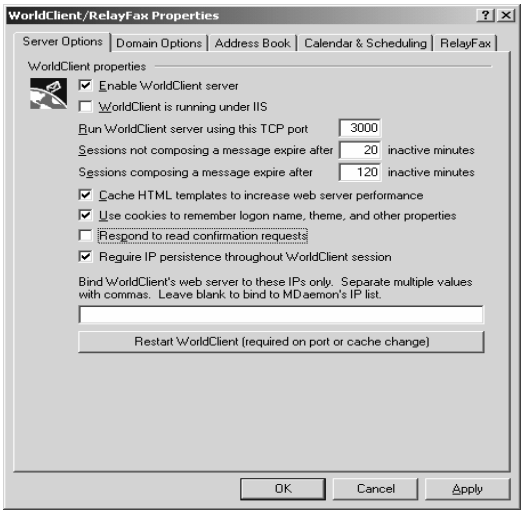
- **Login** vào **worldclient**:



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

+ Từ trình duyệt Web ta gõ địa chỉ http://<mailserver>:port. Thông thường **worldclient** mặc định được đặt **portnumber** là 3000.
+ Nhập vào **MDaemon account's user name and password**.
+ Chọn nút **Sign-in**.

- Thay đổi **WorldClient's Port**.
  + Chọn **Setup->WorldClient Server**…
  + Nhập vào **port number** trong hộp thoại "**Run WorldClient Server using this TCP Port**".
- Các thuộc tính của **worldclient**: Để xem các thuộc tính của **worldclient** ta thực hiện: Từ menu **setup** chọn **worldclient/relay fax**:
  + Server Options.
  + Domain Options.
  + Address Book.
  + Calendar & Scheduling.
  + RelayFax.




Hình 6.11: Thay đổi thuộc tính của **World Client**.

- **Server Options Tab**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

+ **Enable WorldClient server:** Nếu **checkbox** này được lựa chọn nghĩa là ta cho phép **workclient server** hoạt động ngược lại nếu ta không chọn tức là ta khoá **workclient server**(**disable**).
+ **WorldClient is running under IIS:** nếu tuỳ chọn này được chọn thì **WorldClient** được chạy dưới **Internet Information Server** (**IIS**) mà không chạy dưới **webserver** của **WorldClient**.
+ **Run WorldClient server using this TCP port**: Mặc định **WorldClient** sẽ lắng nghe kết nối từ **webbrowser** của **user** trên port**n**umber là 3000.
+ **Sessions not composing a message expire after xx inactive minutes:** định thời gian tồn tại cho một **session** khi một **user login** vào **worldclient** mà không gởi **message**.
+ **Sessions composing a message expire after xx inactive minutes:** định thời gian cho một **session** gởi thông điệp.
+ **Cache HTML templates to increase web server performance:** cho phép **worldclient** lưu trữ lại các mẫu **HTML** vào trong bộ nhớ để phục vụ cho các lần truy cập sau này của **browser**, điều này sẽ làm tăng thông suất của **server**.
+ **Use cookies to remember logon name, theme, and other properties:** cho phép sử dụng **cookies** để nhớ lại các thông tin của **user**(**logon name**, **theme** và những thông tin khác) tại máy tính cục bộ của người dùng.
+ **Respond to read confirmation requests**: tuỳ chọn này cho phép **worldclient** các thông điệp yêu cầu xác nhận thông tin.
+ **Require IP persistence throughout WorldClient session**: yêu cầu **session** của **user** phải sử dụng địa chỉ **IP** tĩnh khi **connect** tới **worldclient server**.
+ **Bind WorldClient's web server to these IPs only:** cho phép ta giới hạn **WorldClient server** lắng nghe trên các địa chỉ **IP** cụ thể nào. Chú ý rằng nếu ta chỉ định nhiều địa chỉ IP thì giữa chúng phải cách nhau bằng dấu phẩy. Nếu chúng ta không chỉ định địa chỉ IP nào thì mặc định **WorldClient** sẽ hoạt động trên các địa chỉ chỉ định cho miền **Primary** and **Secondary**.
+ **Restart WorldClient (required to recognize new TCP port):** cho phép khởi động lại **WorldClient server**. Chú ý: khi ta thay đổi cấu hình **Port** của **WorldClient** thì ta phải khởi động lại dịch vụ này.

## V.2. Sử dụng WorldClient.

- **WorldClient** cho phép ta có thể sử dụng Mail bằng trình duyệt Web(còn gọi là **webmail**). để sử dụng Mail này ta truy cập vào địa chỉ http:// địa chỉ **IP** của **Server** hay địa chỉ **DNS** của **Server** kèm theo dấu ":" và số hiệu **Port**.
- Tuy nhiên ta có thể sử dụng cách truy cập thông thường vào địa chỉ **mailserver** mà không cần kèm theo số hiệu **Port** theo sau địa chỉ **URL**, để làm điều này ta phải hiệu chỉnh lại số hiệu **Port** cho phép **WorldClient** lắng nghe trên **Port 80**. Ví dụ http://www.nhon.com:3000



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net


Hình 6.12: Truy cập **Web Mail**.

- Để **Logon** vào và sử dụng hệ thống ta phải được **Mail Server** cung cấp một **Account**. Sau khi nhập vào **Username** và **Password** chọn nút **Sign In**, lúc này màn hình sử dụng Mail được hiển thị.


Hình 6.13: Sử dụng **Web mail**.

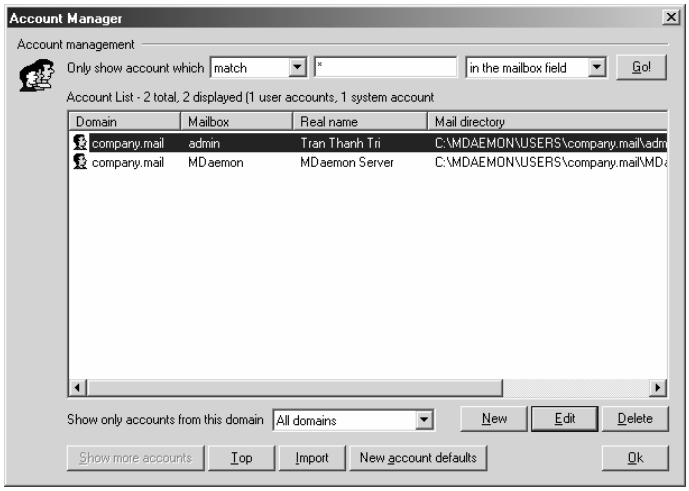
# VI. Quản trị người dùng.

## VI.1. Tạo và thay đổi thuộc tính người dùng.

- Tạo account bằng cách từ menu **Account** | **New account** hoặc **Account Manager**. **Account Manager** là một công cụ giúp quản lý những **account**.

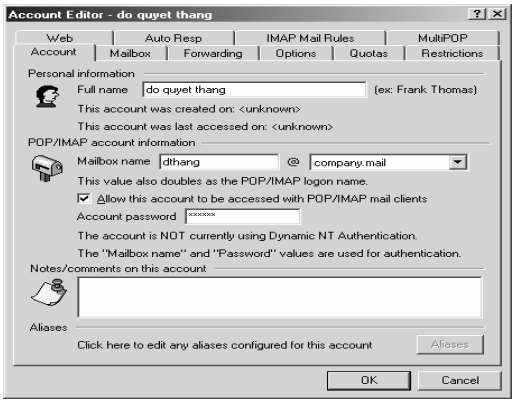


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 6.14: Quản lý tài khỏan Mail.

- Khi tạo mới một **account** click vào nút **New**, chỉnh sửa hay hủy **account** thì chọn **account** sau đó click vào **Edit** hay **Delete**.




Hình 6.15: Tạo tài khoản Mail.

### VI.1.1 Thông tin của Account.

- **Full name**: Họ tên đầy đủ. Các thông tin khác sẽ được phát sinh từ các macro. Có thể để nguyên hoặc sửa đổi nếu cần
- **Mailbox name**: tên hộp thư của **user**. Tên hộp thư này kết hợp với tên **domain** trong cấu hình **Setup\Primary Domain name** để tạo thành địa chỉ **E-mail** của **user** này theo dạng MailboxName@DomainName
- **Allow This Account To Be** : cho phép **user** truy cập hộp thư bằng các phần mềm **POP3 Client** như **Eudora** hoặc **Outlook Express**.
- **Account password**: mật khẩu cho **user** dùng khi truy cập bằng **POP3 client**.
- **Note/Comment**...:



### VI.1.2 Thông tin của Mailbox.

- **Message Directory** : đường dẫn thư mục **mailbox** chứa các thư nhận trên máy chủ chờ **user** kết nối vào và lấy thư về đọc

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

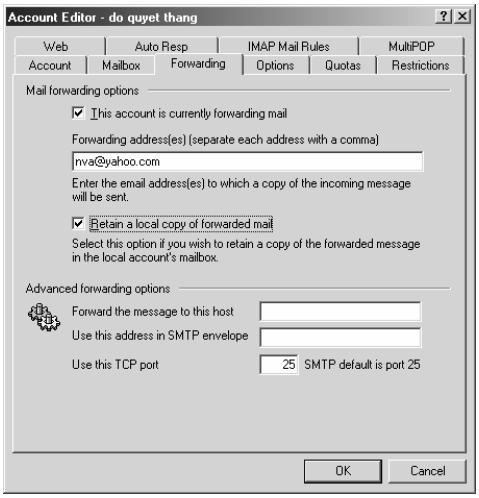
- **Storage Format** : định dạng tên file mail lưu trong thư mục **mailbox**. Mặc định là theo **RFC822**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

### VI.1.3 Forwarding.

- Cho phép chuyển tiếp Mail nhận đến 1 địa chỉ khác



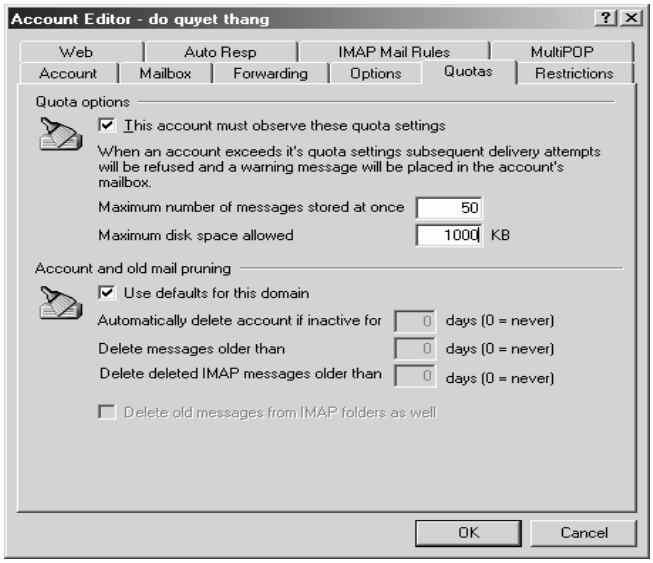

Hình 6.16: Chỉ định **forward mail**.

- **This Account is Currently Forwaring Mail** : **user** này cho phép chuyển Mail đến địa chỉ nhập vào bên dưới. Tính năng này dùng cho người đi công tác xa không có điều kiện truy cập hộp thư cục bộ, khi đó họ đăng ký 1 hộp thư khác và chuyển mail đến hộp thư mới.
- **Retain A Local Copy Of Forwarded mail** : giữ lại 1 bản sao của thư chuyển tiếp trong hộp thư cục bộ.
- **Advanced Forwarding Option**.
  - + **Forward The Message To This Host**: chuyển thư đến 1 máy chủ khác mô tả trong ô này.
  - + **Use This Address In SMTP Envelope**: địa chỉ Mail dùng trong cấu trúc của thư chuyển tiếp.
  - + **Use This TCP Port**: kết nối vào cổng nào trên máy chủ nhận thư chuyển tiếp.

### VI.1.4 Thiết lập hạn ngạch cho mailbox.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 6.17: Giới hạn hạn nghạch đĩa.

- **This Account must Observe These Quota Settings** : **user** bị giới hạn số thư lưu trong hộp thư và giới hạn dung lương hộp thư.
  - + **Maximum Number Of Messages Stored At Once**: tổng số thư được lưu trong **mailbox**.
  - + **Maximum Disk Space Allowed**: dung lượng tối đa của **mailbox**. Khi **user** đạt tới 2 giới hạn trên thì thư gửi đến cho **user** này sẽ bị từ chối.

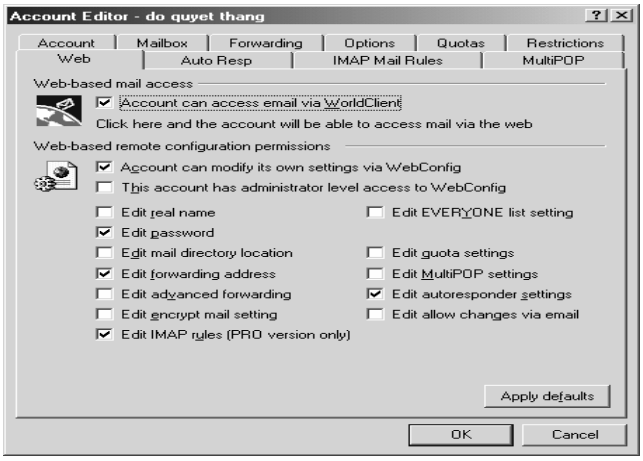
### VI.1.5 Webmail cho tài khoản.

- **Account can access email**...: đánh dấu tuỳ chọn này cho phép **user** truy cập **mailbox** qua **Web**.
- **This Account can Config Itself Via Web** : cho phép **user** tự cấu hình qua **Web**.
- Chọn các tham số cấu hình mà **user** có thể thay đổi qua **Web**, ví dụ:



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

+ **Edit Real Name:** đổi tên.
+ **Edit POP logon:** đổi tên logon vào **POP server**.
+ **Edit POP password**: đổi mật khẩu **logon** vào **POP server**.




Hình 6.18: **Webmail** cho tài khoản.

### VI.1.6 MultiPOP.

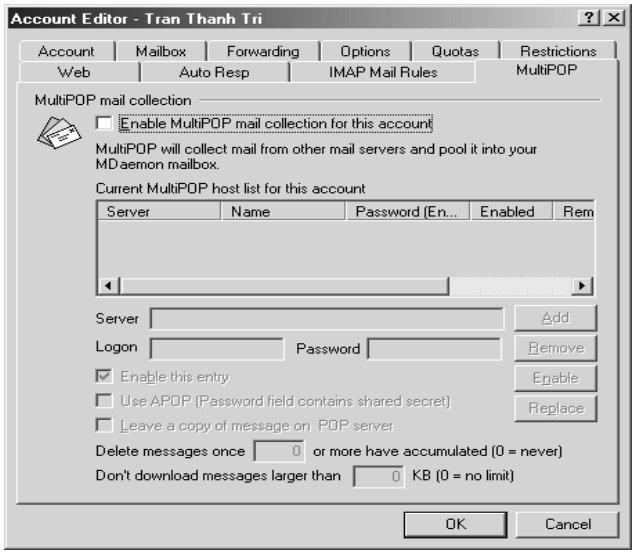
Cho phép **user** truy cập vào nhiều **mailbox** trên nhiều **POP Server**.

- **Enable MultiPOP Mail Collection For This Account :** đánh dấu tuỳ chọn này cho phép lấy thư từ nhiều **mailbox** trên các **POP Server** khác về đưa vào **mailbox** này của **user**. Với mỗi **Server**, nhập vào các tham số.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

+ **Server** : địa chỉ **IP** hoặc tên **DNS** của **POP Server**.
+ **Logon :** tên **logon**.
+ **Pass** : mật khẩu.
+ Nhấn nút **Add** để đưa vào danh sách hoặc **Remove** để loại bỏ.
+ Nhấn nút **Enable** để cho phép truy cập vào **Server**.
+ Đánh dấu **Leave A Copy Of Message On POP Server**: để lại bản sao trên **POP Server** sau khi lấy Mail về.
+ **Don't download Messages Lager Than n KB**: không lấy các thư kích thước lớn hơn n KB.




Hình 6.19: Hiệu chỉnh **MultiPOP Mail**.

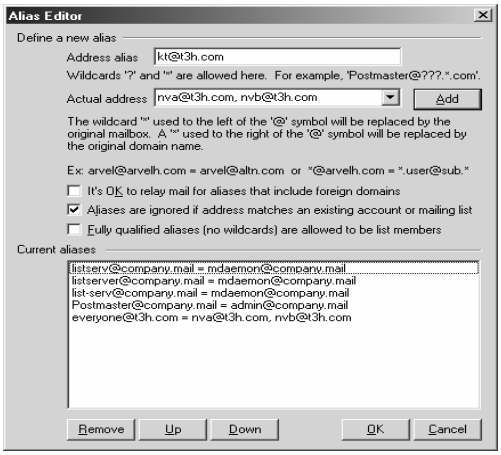
## VI.2. Tạo bí danh cho tài khoản.

- Chọn menu **Accounts** | **Address Aliases**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

+ **Address Alias :** tên bí danh.
+ **Actual address** : tên **user** mà bí danh này trỏ đến.
+ Nhấp chuột vào nút **Add** để tạo bí danh.
+ Nhấp chuột vào nút **Remove** để bỏ bí danh đáng chọn.

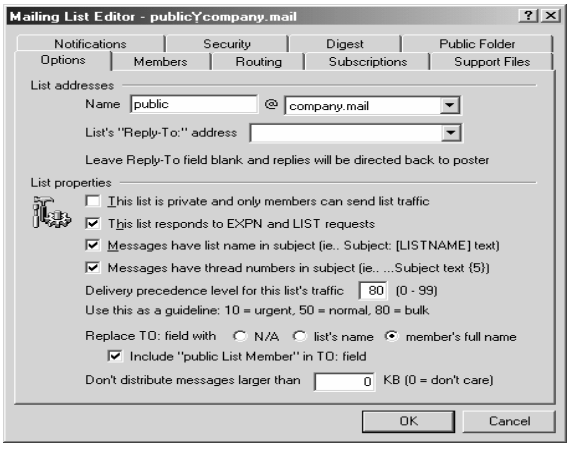



Hình 6.20: Tạo **Alias** cho tài khoản.

## VI.3. Tạo Mailing List cho tài khoản.

Chọn menu **Lists** | **New List**.

- **Tab Options** :
  + Đặt tên cho **mailing list**.
  + **Name Of Mailing List**: tên danh sách thư tín. Tên này kết hợp với tên **domain** để trở thành địa chỉ **E-mail** của nhóm.
  + **List Reply To Address**: địa chỉ **E-mail** trả về của nhóm thư tín.




Hình 6.21: Tạo **group mail**.



- **Tab Members:** Cho phép thêm, hủy thành viên của nhóm thư tín, để thêm một thành viên ta thực hiện như sau: chọn tên **user** trong danh sách **New Member's E-mail Address** và nhấn nút **Add**.

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

# Giới thiệu WinGate Proxy.

**WinGate** là 1 dịch vụ chạy trên máy tính đơn và cung cấp cho nhiều máy tính khác truy cập vào **Internet** . Nó làm được điều này bằng cách cho phép tất cả máy tính đó chia sẻ đồng thời một kết nối **Internet** . **WinGate** cung cấp 3 phương pháp để hỗ trợ việc chia sẽ một kết nối Internet (**Proxies** , **WinGate Internet Client** , **NAT-based General Purpose Internet Sharing**) , và cho phép ta tùy chỉnh **WinGate** lệ thuộc vào người dùng mạng .

**WinGate** cho phép kết nối toàn bộ mạng cục bộ vào **Internet** bằng 1 **Modem** đơn.

## I. Cài đặt Wingate.

### I.1. Yêu cầu phần cứng.

Để cài đặt chương trình **WinGate** , ta cần phải chuẩn bị các yêu cầu về phần cứng và phần mềm như sau :

- **Windows 95** , **98** , **NT** ( đối với các phiên bản từ 4.0 trở về sau ) . Phiên bản **WinGate** từ 3.0.5 trở đi không thể chạy trên môi trường **Windows NT 3.5.1** .
- Nếu cài trên máy tính chạy hệ điều hành **Windows NT**, cần phải cài phiên bản **Service Pack 4** trở đi .
- Cần có 1 kết nối trực tiếp ra **Internet** .
- Cả hai loại máy **WinGate Server** và máy **Client** đều phải cài bộ nghi thức **TCP/IP**.
- Cài đặt **Winsock 2** đối với một số phiên bản của **Windows 95**.

### I.2. Cài đặt Wingate proxy.

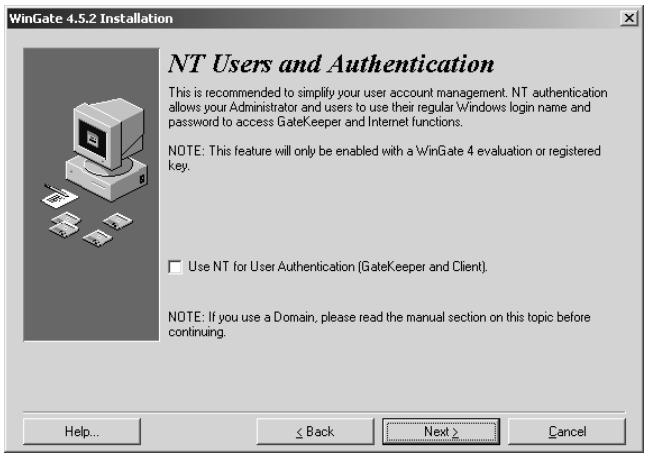
- Kiểm tra cấu hình phần cứng và phần mềm theo đúng yêu cầu.
- Từ thư mục của đĩa/thư-mục cài đặt , chạy tập tin **WinGate.exe**.
- Chọn nút **I Agree** để đồng ý các điều kiện của phần mềm đề ra.
- Xuất hiện cửa sổ yêu cầu chọn loại dịch vụ cần cài đặt , có 2 loại:
    + **Configure this Computer as a WinGate Internet Client** : cấu hình máy tính như là 1 máy **Client** ( máy trạm ).
    + **Configure this Computer as the WinGate Server** : cấu hình máy tính như là 1 máy **WinGate Server**.
    + Trong phần hướng dẫn này ta chọn vào nút cấu hình như là 1 máy **Server**. Sau đó nhấn nút **Continue**.
- Xuất hiện cửa sổ thông báo cài đặt **WinGate Server**, nhấn nút chọn **Next** để tiếp tục.
- Xuất hiện cửa sổ yêu cầu ta chọn loại cài đặt:



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

+ **Install WinGate (Enter your WinGate key below):** cài đặt WinGate , khi chọn nút này ta phải nhập vào **Lincense Name** và **Lincense Key** .
+ **Evaluate WinGate Home , Standard or Pro (Free 30 day trial):** cài đặt thử nghiệm **WinGate** trong vòng 30 ngày .
+ **Purchase WinGate now (Online):** Vào trang Web của **WinGate** để mua 1 **license** dùng để cài đặt sử dụng.

- Trong trường hợp này, chọn nút ở trên cùng (**Install WinGate**) , nhập vào **License Name** và **Lincense Key** và nhấn nút **Next** để tiếp tục .
- Màn hình kế tiếp đưa ra lựa chọn **Use NT for User Authentication** ( **GateKeeper and Client** ) . Nếu chọn lựa chọn này thì các tài khoản người dùng được tạo sẵn trong **Windows NT/2000** sẽ đồng bộ với các tài khoản tạo trong **WinGate** .
- Trong trường hợp này ta không cần chọn lựa chọn này , nhấn **Next** để tiếp tục .

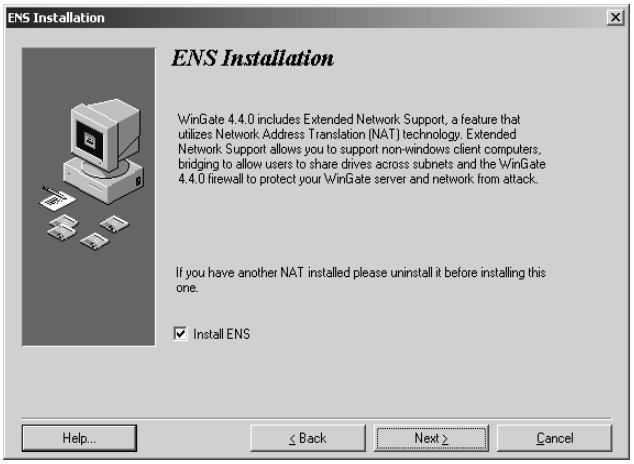



Hình 6.22: **NT User and Authentication**.

- Trong bước cài đặt kế tiếp, màn hình cài đặt đưa ra 1 lựa chọn **Install ENS**. Nếu chọn lựa chọn này, quá trình cài đặt sẽ cài thêm vào **Extended Network Support** (**ENS**) hỗ trợ kĩ thuật **Network Address Translation** (**NAT**), **firewall** .



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 6.23: Chọn **ENS**.

- Nhấp chuột vào lựa chọn **Enable Auto Update** để tự động cập nhật phiên bản mới của **WinGate**. Chọn **Next** để tiếp tục.
- Màn hình cài đặt cho biết vị trí thư mục cài dịch vụ **WinGate** . nhấp chuột vào **Begin** để tiếp tục .
- Sau khi cài đặt xong dịch vụ , quá trình cài đặt hiển thị màn hình thông báo hoàn tất việc cài đặt. chọn **Finish**.
- Nhấp chuột vào nút **Ok** để khởi động lại máy tính .
- Sau khi cài đặt xong, ta sẽ thấy biểu tượng của **WinGate** được tạo ra tại thanh tác vụ.

## I.3. Khởi động/tạm ngưng WinGate.

- Khởi động **Wingate**: Chọn **Start | Programs | WinGate | Start WinGate Engine**.
- Tạm ngừng dịch vụ **WinGate** bằng cách nhấp chuột vào phải vào biểu tượng **WinGate** , chọn **Stop Engine**.

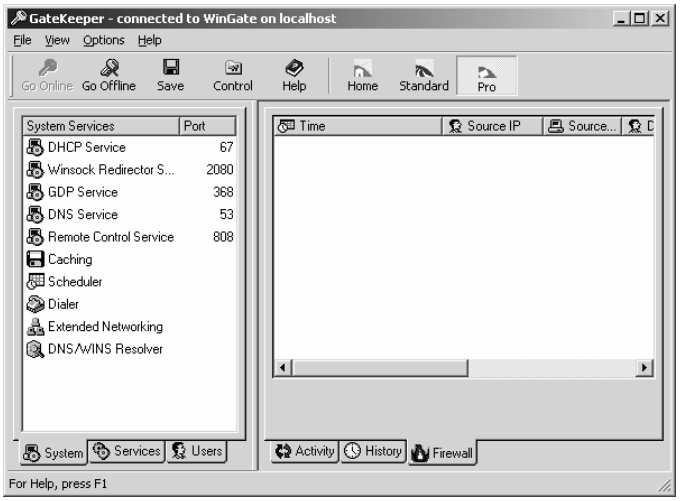
# II. Cấu hình Wingate.

## II.1. Khảo sát các thông tin chung.

- **Use current Windows login:** Dùng lựa chọn này khi ta đang dùng định danh trên **NT Server** . Khi bật lựa chọn này cho phép ta tự động đăng nhập, **WinGate** sử dụng **username** và **password** của **NT Server** hiện hành.
- **Log on to local machine:** Đăng nhập vào máy cục bộ.
- **Use these details next time to login directly :** Các lần đăng nhập kế tiếp không đưa ra yêu cầu nhập **username** và **password** . Lưu ý là **GateKeeper** không lưu lại các **password**, do đó chỉ dùng lựa chọn này khi dùng lựa chọn **User current Windows login**.
- Sau khi khởi động chương trình **WinGate** lên, xuất hiện **GateKeeper**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net



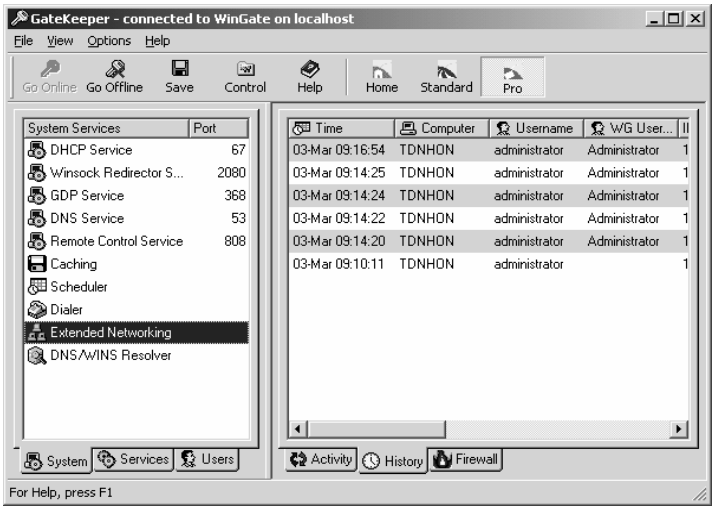

Hình 6.24: Giao diện **GateKeeper**.

- **Activity Panel**.
  - + Hiển thị tất cả các phiên làm việc của người dùng và được cập nhật theo thời gian. Người quản trị có thể dùng màn hình này để quan sát và có thể xóa đi những phiên làm việc cụ thể nào đó.
  - + Có nhiều biểu tượng thể hiện các phiên làm việc trong màn hình **Activity**. Những biểu tượng này xuất hiện khi các phiên làm việc còn hoạt động, và biến mất khi các phiên làm việc hoàn tất.
  - + **Data sessions :** thể hiện thực thể của proxy hoặc dịch vụ đang dùng.
  - + **User sessions :** thể hiện người dùng nào đang sử dụng **WinGate** và đang mở phiên làm việc dữ liệu nào. Nếu một người dùng chưa được định danh, họ chỉ xuất hiện khi có một phiên làm việc dữ liệu đang hoạt động. Nếu một người dùng được định danh, họ sẽ xuất hiện với một biểu tượng chìa khóa, và ở màn hình **Activity** cho tới khi thoát ra.
  - + **Computer Session :** Có dạng biểu tượng máy tính, chỉ ra máy tính nào đang sử dụng **WinGate** .
  - + **Authenticated User:** Người dùng được định danh.
  - + **Assumed User:** Người dùng sử dụng **WinGate** từ 1 vị trí có thể nhận biết được, nhưng chưa đăng nhập vào **WinGate**.
  - + **Unknow User:** người dùng sử dụng **WinGate** từ 1 vị trí không nhận biết được, và chưa đăng nhập vào **WinGate**.
- History Panel.



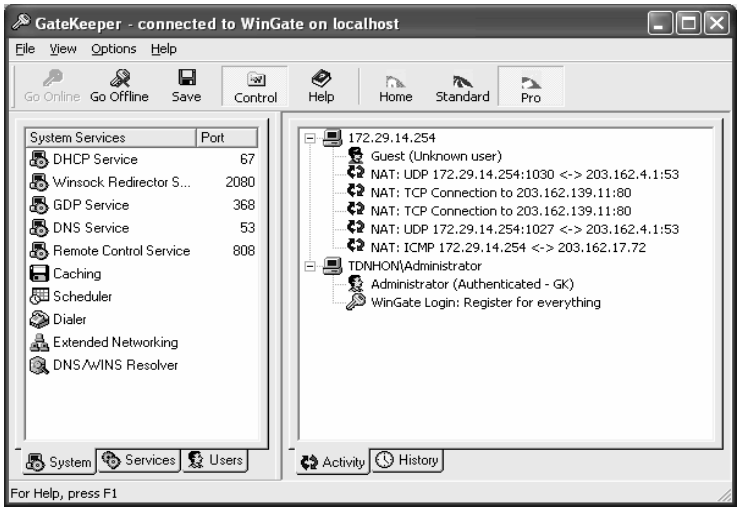
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

Hiển thị thông tin về các lần truy cập sử dụng dịch vụ WinGate.




Hình 6.25: **Active Panel**.

- Firewall Panel.
  + Hiển thông về connection của các máy trạm bị bộ lọc của **wingate** ngăn chặn.
- System Tab.
  + Trong tab này giúp chúng ta theo dõi và đặt cấu hình về **caching**, **dialer**, **ENS**, **Scheduler** … trong hệ thống **wingate**.



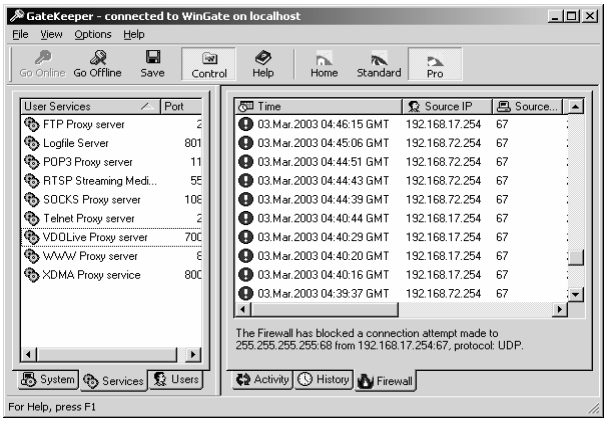

Hình 6.26: **System Tab**.

- **Service Tab**.

Cho phép **user** có thể cấu hình, **start** hoặc **stop** các **service**, thêm hoặc loại bỏ một dịch vụ.

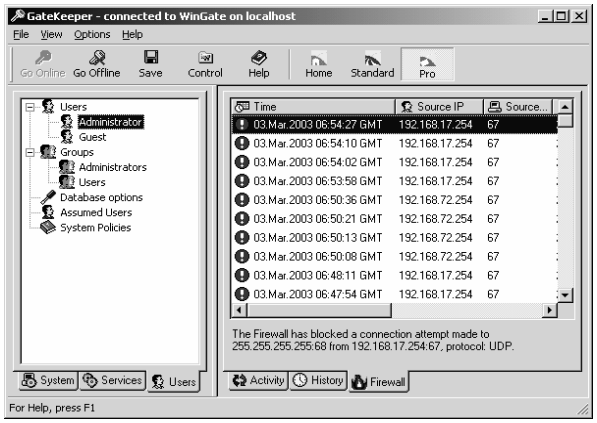


Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 6.27: **Services tab**.

- **Users Tab :** Cho phép ta quản lý, kiểm toán, tạo mới, ghi nhận các thông tin của các **wingate user**, giới hạn quyền truy cập các dịch vụ trong **wingate** cho các **user**, giới hạn các **user logon** vào **wingate** thông qua **wingate keeper**.




Hình 6.28: User tab.

# III. Cấu Hình Các Dịch Vụ Hệ Thống.

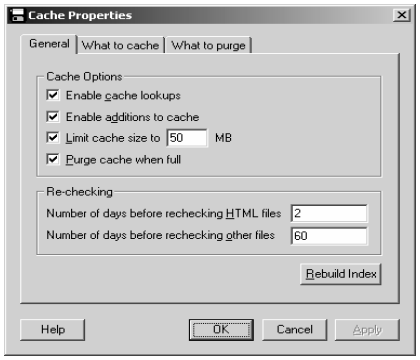
## III.1. Cấu hình Caching.

- **Caching** : Lưu trữ dữ liệu dùng chung tại 1 nơi mà nó có thể được truy xuất nhanh chóng và thuận tiện khi cần thiết. **WinGate** cung cấp việc **caching** các tài nguyên **Internet**, bao gồm : đồ họa, các tài liệu **HTML** hoặc các tập tin khác.
- Điều thuận lợi của **Caching** đó là nó chia sẽ cho tất cả các người dùng sử dụng dịch vụ **WWW Proxy Service**, giúp người dùng có thể truy cập thông tin nhanh chóng các **website** mà họ thường xuyên vào (do **website** được lưu trữ lại cho các lần truy cập sau).
- Từ cửa sổ **GateKeeper** : Chọn **tab System** – click đôi vào **Caching**. Cửa sổ **Caching Properties** hiện ra.
- Tab **General**.



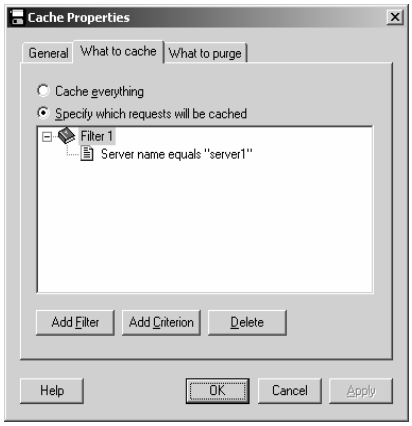
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

+ **Enable cache lookups :** cho phép tìm kiếm trong **cache**.
+ **Enable additions to cache** : cho phép thêm thông tin vào **cache**.
+ **Limit cache size to ... MB :** giới hạn kích thước của **cache**.
+ **Purge cache when full :** xoá sạch thông tin được lưu khi **cache** đầy.
+ **Number of days before rechecking HTML files :** số lượng ngày trước khi kiểm tra lại các tập tin dạng **HTML**.
+ **Number of days before rechecking HTML files :** số lượng ngày trước khi kiểm tra lại các tập tin dạng khác.




Hình 6.28: Cấu hình **Cache**.

- **What to cache tab**.




Hình 6.29: Thay đổi thuộc tính cho **Cache**.



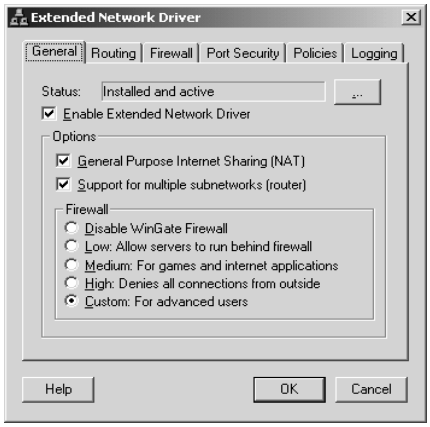
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

+ **Cache everything** : lưu trữ mọi thông tin.
+ **Specify which request will be cached** : lưu lại những dữ liệu được chỉ định trong các bộ lọc phía dưới.
+ **Add Filters** : thêm vào một bộ lọc thông tin mới.
+ **Add Criterion** : thêm vào các tiêu chuẩn lọc thông tin cho bộ lọc.
+ **Delete** : xóa đi các thông tin theo qui định trong các bộ lọc phía dưới.

## III.2. Extended Network Support (ENS):

**ENS** cung cấp các công cụ mới cho phép quản trị kết nối của **user** trong mạng **wingate**, cung cấp các cơ chế lọc packet thông qua **firewall**, hỗ trợ **NAT**, hỗ trợ **Multisubnetwork**.

- **General tab**.



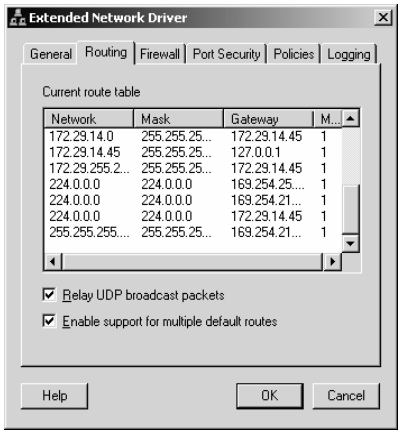

Hình 6.30: **General tab**.

+ **General Purpose Internet Sharing (NAT)**:Tuỳ chọn này là một công cụ dịch địa chỉ(**NAT**) cho phép bất kỳ một máy tính nào trong mạng nội bộ có thể truy cập trực tiếp **Internet** qua **wingate server** mà không cần phải thông qua **www proxy server**.
+ **Support for Multiple Subnetworks (router)**:Tuỳ chọn này cho phép chia sẻ các tài nguyên mạng(**drive**, **data**, **resource**…) giữa các máy tính trên các đường mạng khác nhau và chúng được liên thông với nhau thông qua một **Router** mềm có cài đặt **wingate**.
+ **Security Firewall Protection**: **Wingate** còn cung cấp một kỹ thuật lọc **packet**(**packet**-filtering), ở những phiên bản trước wingate chỉ được cung cấp ở mức độ **proxy firewall**, trong phiên bản mới này cung cấp chức năng **packet-filtering** mạnh hơn chức năng trước để chống sự tấn công trên mạng bao gồm : cấm dịch vụ (**denial of service** (**DOS**)), tấn công thông qua cơ chế **ping** (**ping of death**), quét **port** (**port scanners**), **Trojans** và nhiều cơ chế khác.

- **Routing Tab**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net



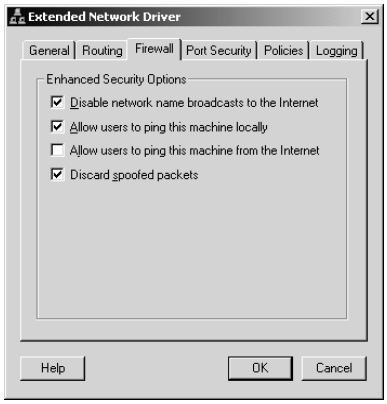

Hình 6.31: Cấu hình **routing**.

+ Hiển thị bảng **routing table** hiện tại trên **Server** bao gồm các thông số về **network**, **gateway** và **subnetmask**, **metric**.
+ **Relay UDP broadcast Packets**: cho phép cơ chế tiếp nhận và chuyển tiếp **UDP packet** từ **subnet** này sang **subnet** khác.
+ **Enable support for multiple default routes**: Khi **connection** được tạo thì **default gateway** khác được chỉ định tới **Router**, và **default gateway** này được gán mức độ ưu tiên cao hơn **default gateway** thông thường, và thường xảy ra lỗi **routing** giữa hai **subnet**, vì **packet** được gởi từ **subnet** này sang **subnet** khác dự vào **gateway** có độ ưu tiên cao hơn do đó làm **packet** không tới đích được, khi tuỳ chọn này được lựa chọn thì chức năng **routing** trong **wingate** dự vào **gateway** được **Router** chỉ định ban đầu.

- **Firewall tab**.
  + **Extended Security Options:** Cung cấp các chức năng cơ sở về an ninh mật giúp ta có thể bảo vệ hệ thống chống lại một số phương pháp tấn công thông dụng.
  + **Advanced Packet-Filtering:** Các gói tin (**packets**) có thể được lọc (**filtered**) thông qua **protocol**, **interface**, **port** và có thể cho phép (**allowed**), không cho phép (**denied**) hay giới hạn (**redirected**) việc truy cập của các máy tính khác trong mạng đi qua **proxy** (ta có thể xem tab **Port Security** và **Policies**)
  + **Intrusion Logging**: Ghi nhận về các sự kiện về bất kỳ sự tấn công từ bên ngoài vào, hay các dấu hiệu của sự tấn công vào hệ thống(xem tab **Logging**).



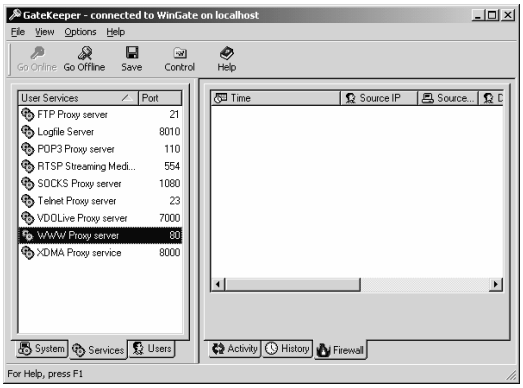
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 6.32: Cấu hình **Firewall**.

## III.3. Cấu hình các dịch vụ proxy.

**Wingate proxy** cung cấp các dịch vụ **user** như: **ftp proxy server**, **Logfile Server**, **Pop3 Proxy server**, **RTSP Streaming Media**, **SockProxy server**, **Telnet Proxy server**, **VDOlive proxy server**, **WWW proxy server**, **XDMA Proxy service**, trong phần này ta sẽ thảo luận một số dịch vụ đặc trưng như: **www proxy server**, **sockproxy server**, **ftp proxy server**.



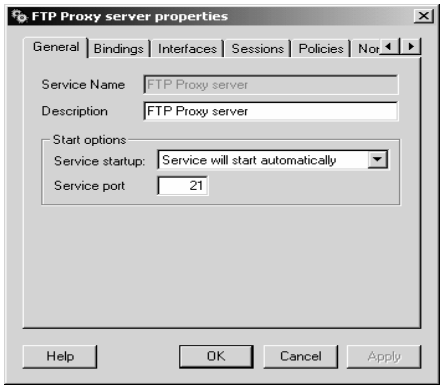

Hình 6.33: Cấu hình dịch vụ **proxy**.

### III.3.1 Cấu hình FTP Proxy.

**FTP Proxy Server** cho phép sử dụng các trình ứng dụng **FTP Client** mà có hỗ trợ phương thức username@hostname qua firewall. Ví dụ: **WS_FTP**, **CuteFTP**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net




Hình 6.33: Cấu hình dịch vụ **FTP Proxy**.

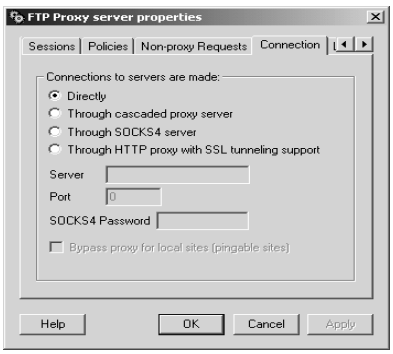
**Port 21** thường được sử dụng cho **FTP proxy server**. **FTP service** cho phép chúng ta có thể kết nối qua **firewall** khác.Trong phần **Connection** tab trong tuỳ chọn **cascaded proxy server** cho phép ta thực hiện điều này, các tab về **binding** và **interface**, **session**, **Policies**, **logging** chúng tôi đã khảo sát qua trên phần **DHCP Server**.

- **None-proxy Requests tab**.
  - + **FTP Proxy Service** có thể được cấu hình để phục vụ cho cả 2 loại yêu cầu: **proxy** ( ủy quyền ) và **non-proxy** ( không ủy quyền ). Các yêu cầu không ủy quyền thường xuất phát từ các người dùng bên ngoài **Internet** .
  - + Sau đây là các xử lý của dịch vụ đối với các yêu cầu không ủy quyền **Reject request** : loại bỏ yêu cầu.
  - + **Pipe request through to predetermined server** : chuyển yêu cầu sang một máy **Server** khác được xác định trước bởi các tham số phía dưới (**Server – Port**)
  - + **Redirect client to predetermined location** : chuyển hướng máy trạm sang vị trí khác trong **URL** .
  - + **Server Request** : phục vụ yêu cầu này dựa vào các thiết lập **Web Server** (ví dụ như thư mục gốc của **Server** , tên tập tin mặc định,..).
- **Connection tab**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

+ **Directly:** đây là **Option** mặc định được sử dụng khi **wingate server** được kết nối trực tiếp tới **internet**.
+ **Through cascaded proxy server**: sử dụng khi ta muốn **wingate proxy** truy cập qua **proxy** khác, trước khi nó truy cập **internet**.
+ **Through SOCKS4 server:** kết nối qua **SOCK4 Server** kèm theo **password**.
+ **Through HTTP proxy with SSL support:** tuỳ chọn này được sử dụng khi ta muốn **tunneling SSL** thông qua **http proxy**.




**Hình 6.34: Connection tab**.

### III.3.2 Cấu Hình Dịch Vụ WWW Proxy.

Cung cấp việc truy cập **Internet** cho các máy trạm sử dụng nghi thức **HTTP**.

- Mở cửa sổ **GateKeeper**, chọn tab **Service**, double click vào biểu tượng **WWW Proxy Server**.


Hình 6.35: Cấu hình **WWW proxy**.

- **General tab**.
  + **Service Name:** Tên loại dịch vụ
  + **Description:** Dòng mô tả về dịch vụ.
  + **Service will start automatically**: dịch vụ tự động được khởi động.
  + **Manual start/stop:** Dịch vụ được khởi động hoặc ngừng bằng tay.
  + **Service is disabled:** Dịch vụ mặc định bị tắt đi.
  + **Service port:** Cổng cho phép máy trạm kết nối vào dịch vụ **proxy**.
  + **Use java client authentication as required by policies:** Cho phép kiểm tra định danh các máy trạm sử dụng trình duyệt có khả năng **Java**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

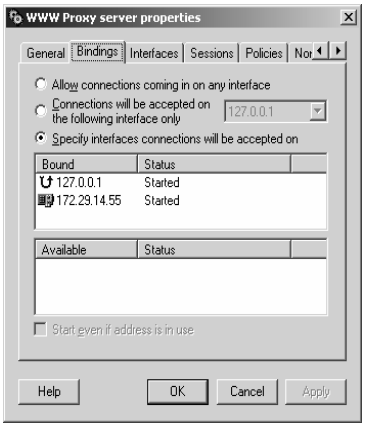
- **Bindings tab**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

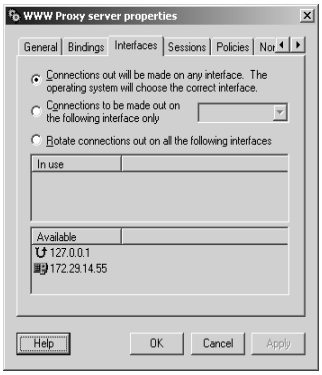
+ **Allow connections coming in on any interface**: cho phép các kết nối đến từ mọi **interface**.
+ **Connecitons will be accepted on the following interface only** : chỉ chấp nhận các kết nối đến từ **interface** được chỉ định.
+ **Specify interfaces connections will be accepted on** : chấp nhận các kết nối từ các **interface** mô tả phía dưới.

-




Hình 6.36: **Bindings tab**.

- **Interfaces tab**.
  + **Connections out will be made on any interface . The operating system will choose the correct interface**: sử dụng tất cả các **interface** để quay kết nối ra ngoài (**Internet**)
  + **Connections to be made out on the following interface only** : chỉ sử dụng **interface** được chỉ định để quay kết nối ra ngoài.
  + **Rotate connections out on all the following interfaces** : sử dụng luân phiên các **interface** được chỉ định phía dưới để quay số ra ngoài.



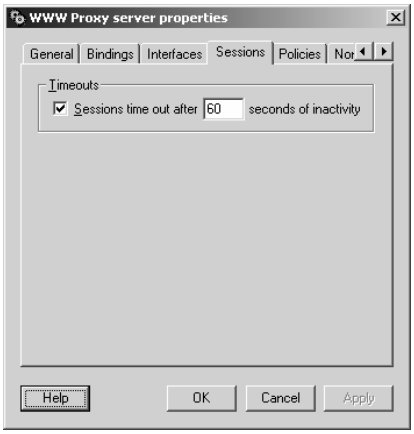

Hình 6.37: **Interface tab**.

- **Sessions tab**.



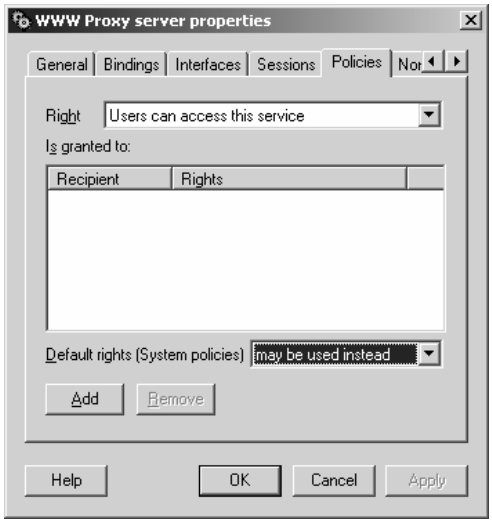
Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

+ **Sessions time out after ... seconds of inactivity** : thời gian hết hạn một phiên làm việc không còn hoạt động.




Hình 6.38: **Session tab**.

- **Polices tab**.
  + **Right:** một số quyền người dùng đối với dịch vụ này.
  + **User can access this service**: người dùng có khả năng truy cập vào dịch vụ này.
  + **User can modify this service:** người dùng có thể thay đổi cấu hình dịch vụ này.
  + **User can start/stop this service:** người dùng có thể khởi động hoặc ngừng dịch vụ này.
  + **Add:** thêm vào người dùng mới có quyền được chỉ định trong **Right**.




Hình 6.39: **Policies tab**.

- **Non-proxy Requests tab**.

**WWW Proxy Service** có thể được cấu hình để phục vụ cho cả 2 loại yêu cầu: **proxy** (ủy quyền) và **non-proxy** (không ủy quyền). Các yêu cầu không ủy quyền thường xuất phát từ các người dùng bên ngoài **Internet** .

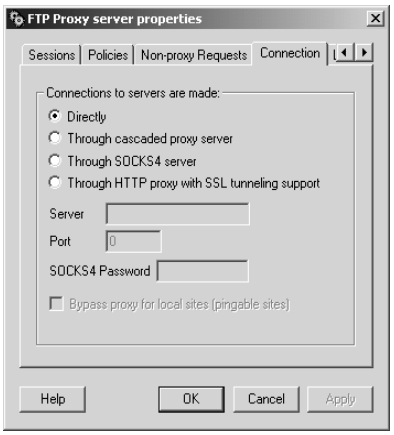


Sau đây là các xử lý của dịch vụ đối với các yêu cầu không ủy quyền.

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net

+ **Reject request :** loại bỏ yêu cầu.
+ **Pipe request through to predetermined server** : chuyển yêu cầu sang một máy **Server** khác được xác định trước bởi các tham số phía dưới (**Server** – **Port**).
+ **Redirect client to predetermined location** : chuyển hướng máy trạm sang vị trí khác trong **URL**.
+ **Server Request** : phục vụ yêu cầu này dựa vào các thiết lập **Web Server** (ví dụ như thư mục gốc của **Server** , tên tập tin mặc định , ...).

- **Connection tab**.
  + **Directly:** đây là **Option** mặc định được sử dụng khi **wingate server** được kết nối trực tiếp tới **internet**.
  + **Through cascaded proxy server:** sử dụng khi ta muốn **wingate proxy** truy cập qua **proxy** khác, trước khi nó truy cập **internet**.
  + **Through SOCKS4 server:** kết nối qua **SOCK4 server** kèm theo **password**.




Hình 6.40: **Connection tab**.



Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | http://www.adminviet.net