

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

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

http://mientayvn.com/Tai_lieu_da_dich.html

Thông tin liên hệ:

Yahoo mail: thanhlam1910_2006@yahoo.com

Gmail: frbwrtres@gmail.com

Theo yêu cầu của khách hàng, trong một năm qua, chúng tôi đã dịch qua 16 môn học, 34 cuốn sách, 43 bài báo, 5 sổ tay (chưa tính các tài liệu từ năm 2010 trở về trước) Xem ở đây

DỊCH VỤ
DỊCH
TIẾNG
ANH
CHUYÊN
NGÀNH
NHANH
NHẤT VÀ
CHÍNH
XÁC
NHẤT

Chỉ sau một lần liên lạc, việc dịch được tiến hành

Giá cả: có thể giảm đến 10 nghìn/1 trang

Chất lượng: Tạo dựng niềm tin cho khách hàng bằng công nghệ 1. Bạn thấy được toàn bộ bản dịch; 2. Bạn đánh giá chất lượng. 3. Bạn quyết định thanh toán.

Nhập môn Mạng Máy Tính



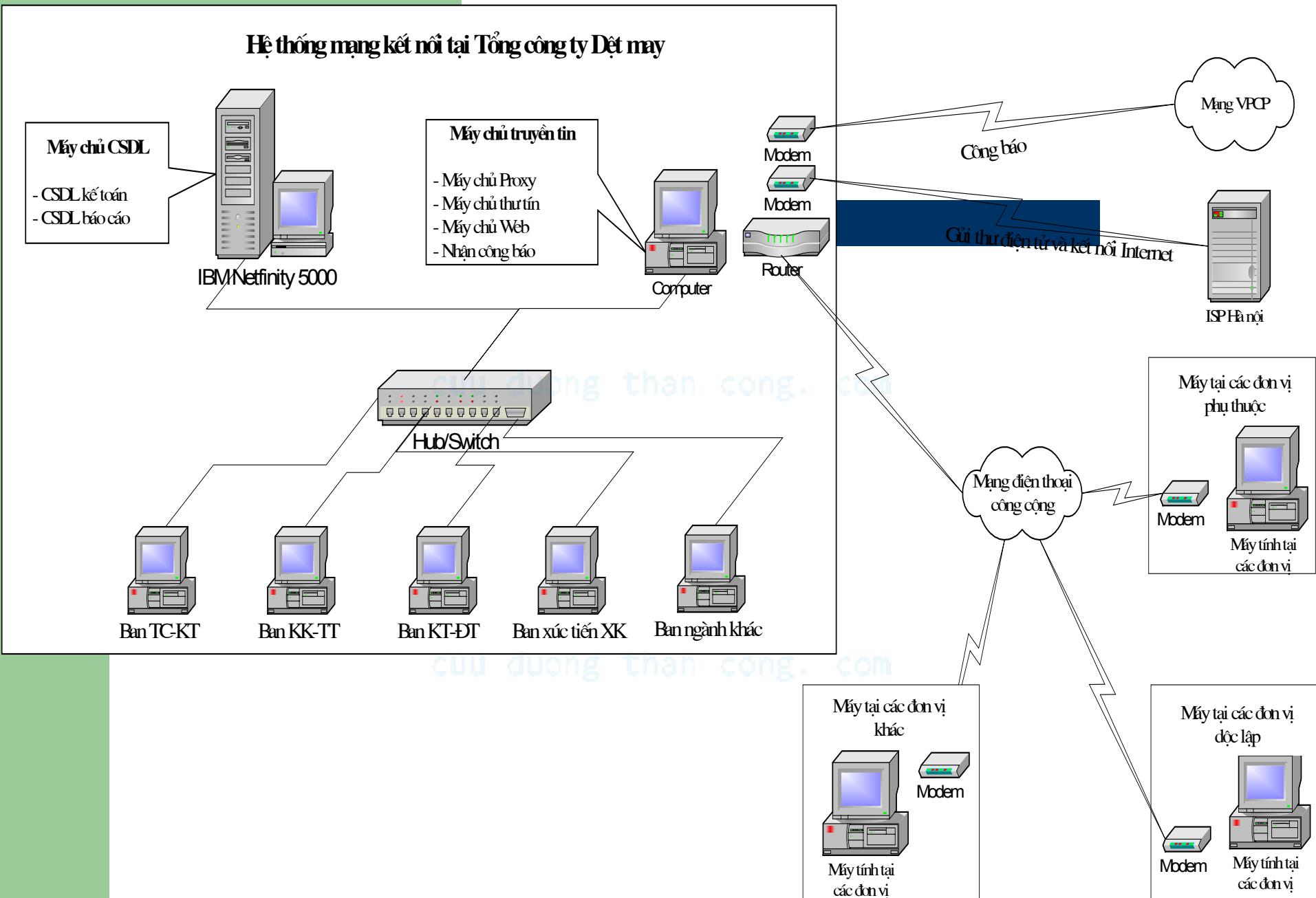
Nội dung

- Các kiến thức chung
- Các loại mạng chủ yếu
- Thiết kế mạng
- Mô hình mạng OSI
- Cáp mạng - phương tiện vật lý
- Giao thức công. cơm
- Kiểm soát lỗi
- Đánh giá độ tin cậy trên mạng
- An toàn thông tin trên mạng
- Quản trị mạng

cuu duong than cong. com

Bài 1: Các kiến thức chung

cuu duong than cong. com



I. Mạng truyền thông và công nghệ mạng

1. Giới thiệu chung:

- Mạng máy tính là một hệ thống các máy tính tự trị (Autonomous Computer) được kết nối với nhau bởi các đường truyền vật lý và theo một kiến trúc nào đó.
- Từ những năm 70 bắt đầu xuất hiện khái niệm mạng truyền thông (Communication Network) trong đó các thành phần chính của mạng là các nút mạng, được gọi là bộ chuyển mạch (Switching Unit) dùng để hướng thông tin tới đích. Các nút mạng được nối với nhau bằng các đường truyền (Communication Subnet hay Communication Line). Các máy tính xử lý thông tin của người sử dụng - (Host) và các trạm cuối (Terminal) được nối trực tiếp vào các nút mạng khi cần có thể trao đổi thông tin qua mạng. Bản thân các nút thường cũng là một máy tính nên có thể đồng thời đóng vai trò máy của người sử dụng.

1. Giới thiệu chung

Các máy tính được kết nối thành mạng nhằm:

- Làm cho các tài nguyên có giá trị cao, đắt tiền (thiết bị, chương trình, dữ liệu,...) trở nên khả dụng đối với mọi người trên mạng, không phụ thuộc vào khoảng cách địa lý.
- Tăng độ tin cậy của hệ thống nhờ khả năng thay thế khi xảy ra sự cố đối với một máy nào đó.

2. Khái niệm về mạng

- Ở mức độ cơ bản nhất, mạng bao gồm hai máy tính nối với nhau bằng cáp sao cho có thể dùng chung dữ liệu. Trong mọi mạng máy tính, dù có phức tạp đến đâu chăng nữa, chúng cũng đều bắt nguồn từ hệ thống đơn giản đó.
- Mạng máy tính phát sinh từ nhu cầu muốn chia sẻ và dùng chung tài nguyên. Nếu không có hệ thống mạng, để gửi thông tin từ một máy tính này đến một máy tính khác, dữ liệu tin phải được in ra giấy hoặc ghi ra đĩa mềm hoặc các thiết bị nhớ ngoài để chuyển đi.

2. Khái niệm về mạng

- Các máy tính khi đã được nối mạng với nhau, chúng có thể dùng chung các tài nguyên như:
 - Dữ liệu
 - Thông điệp
 - Hình ảnh
 - Máy fax
 - Modem
 - Các tài nguyên khác...

2. Khái niệm về mạng

Mạng liên quan đến nhiều vấn đề bao gồm:

- Giao thức truyền thông (protocol): Mô tả những nguyên tắc mà các thành phần mạng cần phải tuân thủ để có thể trao đổi được với nhau.
- Topo (mô hình ghép nối mạng): Mô tả cách thức nối các thiết bị với nhau.
- Địa chỉ: Mô tả cách định vị một thực thể
- Định tuyến (routing): Mô tả cách dữ liệu được chuyển từ một thiết bị này sang một thiết bị khác thông qua mạng.
- Tính tin cậy (reliability): Giải quyết vấn đề tính toàn vẹn dữ liệu, đảm bảo rằng dữ liệu nhận được chính xác như dữ liệu gửi đi.

2. Khái niệm về mạng

- **Khả năng liên tác (interoperability):** Chỉ mức độ các sản phẩm phần mềm và phần cứng của các hãng sản xuất khác nhau có thể giao tiếp với nhau trong mạng.
- **An ninh (security):** Gắn liền với việc đảm bảo an toàn hoặc bảo vệ tất cả các thành phần của mạng.
- **Chuẩn hoá (standard):** Thiết lập các quy tắc và luật lệ cụ thể cần phải được tuân theo.

3. Tại sao phải dùng mạng?

- **Thiết bị ngoại vi:** Máy in và các thiết bị ngoại vi khác: Trước khi mạng máy tính được đưa vào sử dụng, người ta thường phải tự trang bị máy in, máy vẽ cho máy tính của riêng mình, và mọi người phải thay phiên nhau ngồi trước máy tính được nối với máy máy in đó.
- **Dữ liệu:** Nếu không có mạng máy tính, việc chia sẻ thông tin sẽ bị giới hạn ở: phải truyền đạt thông tin trực tiếp (bằng miệng), gửi thư thông báo, chép thông tin vào đĩa mềm để chuyển thông tin điện tử sang máy tính khác.
- **Ứng dụng:** Mạng được dùng để chuẩn hóa các ứng dụng, chẳng hạn chương trình xử lý văn bản, nhằm đảm bảo rằng mọi người dùng trên mạng đều sử dụng cùng phiên bản của cùng ứng dụng.

4. Thế nào là một mạng máy tính

Mạng bao gồm nhiều thành phần và được nối với nhau theo một cách thức nào đó và sử dụng chung 1 ngôn ngữ:

- Các thiết bị đầu cuối (end system) kết nối với nhau tạo thành mạng có thể là các máy tính hoặc các thiết bị khác.
- Môi trường truyền (media) mà truyền thông được thực hiện qua đó. Môi trường truyền có thể là các loại dây dẫn (cáp), sóng (đối với mạng không dây).
- Giao thức (protocol) là quy tắc quy định cách thức trao đổi dữ liệu giữa các thực thể.

4. Thế nào là một mạng máy tính

- Các thành phần mạng: thiết bị, nút, máy tính
 - Thiết bị được dùng để nối đến bất cứ một thực thể phần cứng nào. Những thực thể này có thể là các thiết bị cuối như: máy tính, máy in, ... hoặc một thiết bị phần cứng đặc biệt liên quan đến mạng, ví dụ như các server truyền thông, repeater (bộ lặp), bridge (cầu), switch, router (bộ định tuyến), ...
 - Các thiết bị mạng đều dùng 1 số phương pháp cho phép xác định duy nhất chúng, thường thì thiết bị được chính hãng sản xuất gắn 1 số nhận dạng duy nhất. Ví dụ card Ethernet được gán 1 địa chỉ duy nhất bởi hãng sản xuất – địa chỉ này không trùng với bất kỳ địa chỉ nào khác.
 - Khi mô tả các thành phần mạng cần phân biệt giữa khái niệm thiết bị và máy tính. Xem xét ở khía cạnh mạng máy tính thường được gọi là host (hoặc server) hoặc trạm làm việc.

4. Thế nào là một mạng máy tính

- Phương tiện và giao thức truyền thông trên mạng
 - Để chia sẻ thông tin và sử dụng các dịch vụ trên mạng, các thành phần của mạng phải có khả năng truyền thông được với nhau.
 - Để đáp ứng được yêu cầu này chúng ta phải xét tới hai tiêu chí cụ thể của mạng: khả năng liên kết và ngôn ngữ.
 - Khả năng liên kết chỉ đường truyền hoặc kết nối vật lý giữa các thành phần
 - Ngôn ngữ chỉ 1 bảng từ vựng cùng các quy tắc truyền thông mà các thành phần phải tuân theo.

4. Thế nào là một mạng máy tính

- Phương tiện truyền thông (media)
 - Môi trường vật lý được sử dụng để kết nối các thành phần của mạng thường được gọi là phương tiện truyền thông.
 - Phương tiện truyền thông mạng được chia thành 2 loại:
 - Cáp (cable): ví dụ cáp xoắn đôi, cáp đồng trực và cáp sợi quang
 - Không dây (wireless): Có thể là sóng radio (sóng cực ngắn hay truyền thông qua vệ tinh), bức xạ hồng ngoại.

II. Các yếu tố của mạng máy tính

1. Đường truyền vật lý:

Đường truyền vật lý dùng để chuyển các tín hiệu điện tử giữa các máy tính. Các tín hiệu điện tử đó biểu thị các giá trị dữ liệu dưới dạng các xung nhị phân (on- off). Chúng hoặc là các sóng điện từ hoặc là tia hồng ngoại. Hiện nay có hai loại đường truyền: hữu tuyến (cable) và vô tuyến (wireless).

1. Đường truyền vật lý:

- Đường truyền hữu tuyến gồm có:
 - Cáp đồng trục (coaxial)
 - Cáp đôi xoắn (twisted-pair cable), có hai loại bọc kim (shielded) và không bọc kim (nushielded).
 - Cáp sợi quang (fiber-optic cable).
- Đường truyền vô tuyến gồm có:
 - Radio
 - Sóng cực ngắn (viba) (microware).
 - Tia hồng ngoại (infrared)

2. Kiến trúc mạng

- Kiến trúc mạng máy tính (network architecture) thể hiện cách nối các máy tính với nhau và **tập hợp các quy tắc, quy ước** mà tất cả các thực thể tham gia truyền thông trên mạng phải tuân theo để đảm bảo cho mạng hoạt động tốt. Cách kết nối các máy tính được gọi là **hình trạng** hay **topo** của mạng, còn tập các quy tắc, quy ước truyền thông gọi là **các giao thức** (protocol) của mạng. Tôpô và giao thức mạng là hai khái niệm rất căn bản của mạng máy tính.

2. Kiến trúc mạng

a) Tôpô mạng.

Có hai kiểu kết nối mạng chủ yếu là điểm - điểm (Point to point) và khuếch tán (Broadcast hay Point to multipoint).

- **Kiểu điểm - điểm**

Theo kiểu nối này, các đường truyền nối từng cặp nút với nhau và mỗi nút đều có trách nhiệm lưu trữ tạm thời sau đó khi đường truyền rỗi, nó sẽ chuyển tiếp dữ liệu đi cho tới đích. Do vậy mà mạng loại này còn được gọi là mạng "lưu và chuyển tiếp" (store and forward). Nói chung các mạng diện rộng sử dụng nguyên tắc này.

2. Kiến trúc mạng

- **Kiểu khuếch tán**

- Theo kiểu nối này, tất cả các nút (các máy tính) dùng chung một đường truyền vật lý. Dữ liệu chuyển đi từ một máy nào đó (một nút) có thể được tất cả các máy khác tiếp nhận. Chỉ cần chỉ ra địa chỉ đích của dữ liệu để mỗi nút kiểm tra xem dữ liệu có phải gửi cho mình hay không.

- Trong các tông dạng **xa lộ** (bus) và **dạng vòng** (ring) cần có cơ chế "trọng tài" để giải quyết "xung đột" khi nhiều nút muốn truyền tin cùng một lúc. Việc cấp phát đường truyền có thể là "tĩnh" hoặc là "động". Cấp phát "tĩnh" thường dùng cơ chế quay vòng (round robin) để phân chia đường truyền theo các khoảng thời gian định trước. Còn cấp phát "động" là cấp phát theo yêu cầu để hạn chế thời gian "chết" vô ích của đường truyền.

2. Kiến trúc mạng

b) Giao thức mạng

- Việc trao đổi thông tin cho dù đơn giản nhất, đều phải tuân theo những quy tắc nhất định. Hai người nói chuyện muốn cho cuộc nói chuyện kết quả thì ít nhất cả hai người cũng phải tuân theo nguyên tắc "khi người này nói thì người kia phải nghe và ngược lại".
- Việc truyền tín hiệu trên mạng cũng vậy, cần phải có những quy tắc, quy ước về nhiều mặt từ khuôn dạng (cú pháp, ngữ nghĩa) của dữ liệu cho tới các thủ tục gửi nhận dữ liệu, kiểm soát hiệu quả và chất lượng truyền tin và xử lý các lỗi và sự cố nếu có.
- Tập hợp tất cả các quy tắc, quy ước đó được gọi là giao thức của mạng. Rõ ràng là các mạng có thể tùy ý dùng các giao thức khác nhau tùy sự lựa chọn của người thiết kế.

III. Phân loại mạng máy tính

Có nhiều cách phân loại mạng máy tính tùy thuộc yếu tố chính được chọn để làm chỉ tiêu phân loại, chẳng hạn đó là "khoảng cách địa lý", "kỹ thuật chuyển mạch" hay "kiến trúc mạng",...

1. Nếu lấy "**khoảng cách địa lý**" làm chỉ tiêu phân loại thì ta có các *mạng cục bộ*, *mạng đô thị*, *mạng diện rộng* và *mạng toàn cầu*, *mạng cá nhân*, *mạng lưu trữ*.
- **Mạng cục bộ (Local Area Network - viết tắt là LAN)** là mạng được lắp đặt trong một phạm vi tương đối nhỏ (trong một tòa nhà, khu trường học...) với khoảng cách lớn nhất giữa các máy tính nút mạng chỉ trong vòng vài chục mét đến vài km trở lại.

III. Phân loại mạng máy tính

- **Mạng đô thị (Metropolitain Area Networks - viết tắt là MAN)** là mạng được lắp đặt trong phạm vi một đô thị hay một trung tâm kinh tế-xã hội có bán kính khoảng 100 km trở lại.
- **Mạng diện rộng (Wide Area Networks- viết tắt là WAN)** có phạm vi vượt qua biên giới quốc gia thậm chí cả lục địa.
- **Mạng toàn cầu (Global Area Networks - viết tắt là GAN)** có phạm vi trải rộng khắp các lục địa.
- Một loại mạng nữa là **Mạng cá nhân (PAN)** một mạng máy tính nhỏ sử dụng trong gia đình
- *Chú ý rằng khoảng cách địa lý dùng làm mốc để phân biệt các loại mạng chỉ có tính tương đối.*

III. Phân loại mạng máy tính

2. Nếu lấy "**kỹ thuật chuyển mạch**" (switching) làm yếu tố chính để phân loại thì ta có: *mạng chuyển mạch kênh*, *mạng chuyển mạch thông báo* và *mạng chuyển mạch gói*.

- **Mạng chuyển mạch kênh (circuit-switched networks).** Khi có hai thực thể cần trao đổi thông tin thì giữa chúng sẽ thiết lập một "kênh" (circuit) cố định và duy trì cho đến khi một trong hai bên ngắt liên lạc. Các dữ liệu chỉ được truyền theo con đường cố định đó.
 - **Có 2 nhược điểm:** một là tiêu tốn thời gian để thiết lập kênh cố định giữa hai thực thể và hai là hiệu suất sử dụng đường truyền không cao vì khi hai bên hết thông tin cần truyền, kênh bị bỏ không trong khi các thực thể khác cần không được phép sử dụng kênh.
 - Mạng điện thoại là một ví dụ điển hình của mạng chuyển mạch kênh

III. Phân loại mạng máy tính

- **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 quy định trước. Mỗi thông báo đều có chứa vùng thông tin điều khiển trong đó chỉ rõ đích của thông báo. Căn cứ vào thông tin này mà mỗi nút trung gian có thể chuyển thông báo tới nút kế tiếp theo đường dẫn tới đích của nó. Như vậy, mỗi nút cần phải lưu trữ tạm thời để "đọc" thông tin điều khiển trên thông báo rồi sau đó mới chuyển tiếp thông báo đi. Tùy điều kiện cụ thể của mạng, các thông báo khác nhau có thể được gửi đi trên các con đường khác nhau.

III. Phân loại mạng máy tính

Những ưu điểm:

- Hiệu suất sử dụng đường truyền cao vì không chiếm dụng độc quyền đường truyền mà đường truyền được phân chia giữa nhiều thực thể.
- Mỗi nút mạng có thể lưu trữ thông báo cho tới khi kênh truyền rõi mới gửi thông báo đi, do đó giảm được tình trạng tắc nghẽn (congestion) mạng.
- Có thể điều khiển việc truyền tin bằng cách sắp xếp theo độ ưu tiên cho các thông báo.
- Có thể tăng hiệu suất sử dụng giải thông của mạng bằng cách gán địa chỉ quảng bá (broadcast addressing) để gửi thông báo đồng thời tới nhiều nút

III. Phân loại mạng máy tính

Những nhược điểm: Không hạn chế kích thước thông báo dẫn đến phí tổn lưu trữ tạm thời cao và ảnh hưởng đến thời gian đáp ứng (response time) và chất lượng truyền. Nó thích hợp với dịch vụ thông tin kiểu thư điện tử (electronic mail) hơn là cho các ứng dụng thời gian thực vì có độ trễ nhất định cho việc lưu trữ và xử lý thông tin điều khiển tại mỗi nút.

- **Mạng chuyển mạch gói (packet-switched networks).** Trong mạng loại này mỗi thông báo được chia ra thành nhiều phần nhỏ hơn gọi là các gói tin (packet) có khuôn dạng quy định trước. Mỗi gói tin cũng có các thông tin điều khiển trong đó có địa chỉ nguồn (người gửi) và địa chỉ đích (người nhận) của gói tin. Các gói tin của một thông báo nào đó có thể được chuyển đi qua mạng để tới đích bằng nhiều con đường khác nhau.

III. Phân loại mạng máy tính

- Phương pháp chuyển mạch thông báo và chuyển mạch gói là gần giống nhau. Điều khác biệt là ở chỗ các gói tin được giới hạn kích thước tối đa sao cho các nút mạng (nút chuyển mạch) có thể xử lý toàn bộ gói tin trong bộ nhớ mà không cần phải lưu trữ tạm thời trên đĩa. Chính vì vậy mạng chuyển mạch gói truyền các gói tin qua mạng nhanh hơn và hiệu quả hơn so với mạng chuyển mạch thông báo.
- Vấn đề khó khăn nhất của mạng loại này là việc tập hợp các gói tin để tạo thành bản thông báo ban đầu của người sử dụng, đặc biệt trong trường hợp các gói được truyền theo nhiều đường khác nhau. Cần phải đặt các cơ chế "đánh dấu" gói tin và phục hồi các gói

III. Phân loại mạng máy tính

- Do các ưu điểm mềm dẻo và hiệu suất cao hơn nên hiện nay các 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 gói) trong một mạng thống nhất (được gọi là mạng dịch vụ tích hợp số - Integrated Service Digital Networks - viết tắt là ISDN) đang là một trong những xu thế phát triển hiện nay.
- Cuối cùng, có thể phân loại mạng theo kiến trúc mạng (tôpô và giao thức sử dụng). Chẳng hạn mạng SNA của IBM, mạng ISO (theo kiến trúc chuẩn quốc tế) hay mạng TCP/IP v.v...

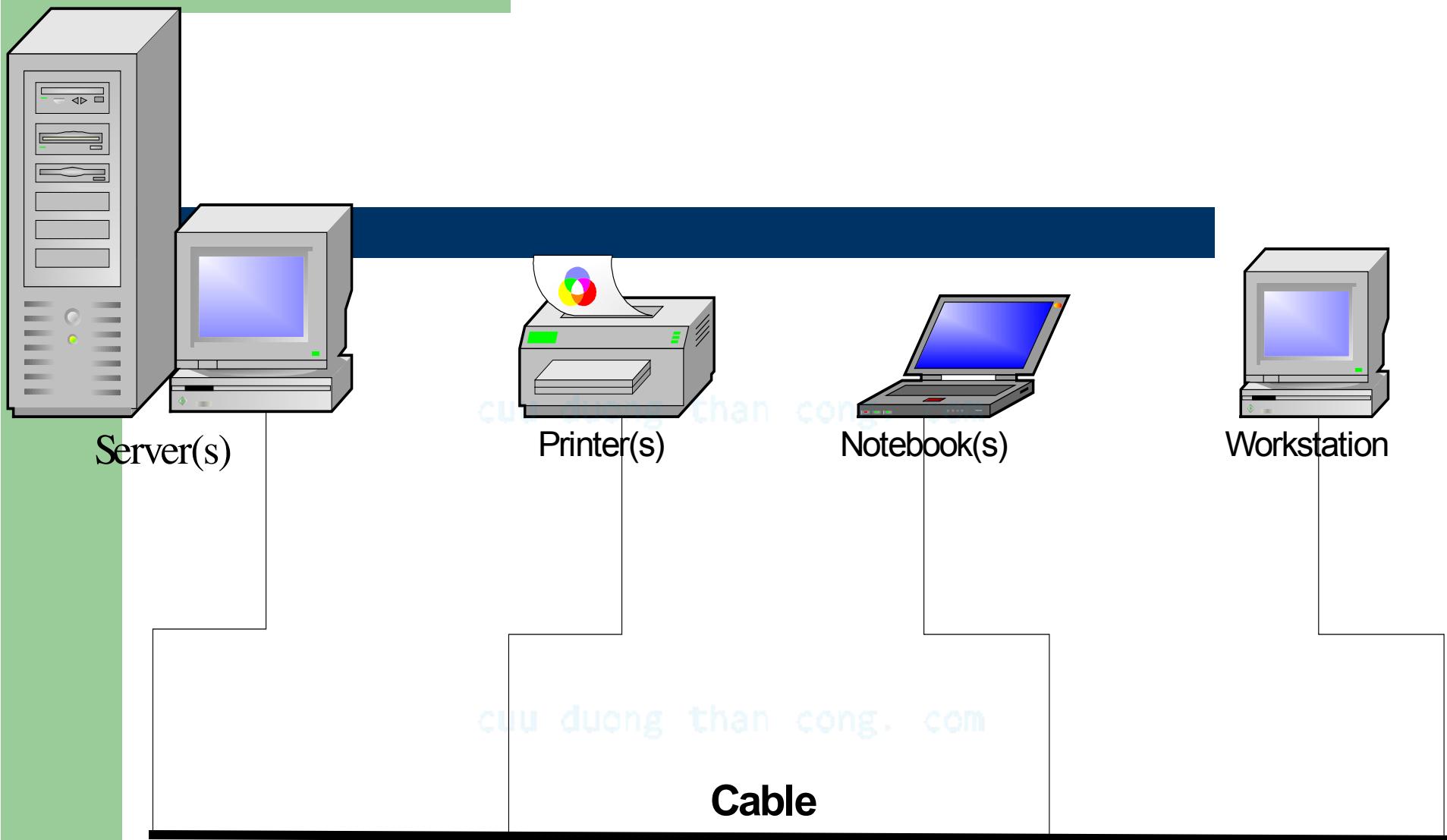
III. Phân loại mạng máy tính

3. Nếu lấy "kỹ thuật ghép nối" mô hình Topo gần giống như bản đồ đường phố. Có 3 chiến lược kết nối tổng quát: điểm – điểm (point – to – point), broadcast (điểm – nhiều điểm) và multidrop (đa chặng).

Các cấu hình dạng chuẩn:

- **Mạng bus**

- Cấu hình vật lý: bao gồm một dây cáp đơn lẻ nối tất cả các máy tính trong mạng theo một hàng. Đây là phương pháp nối mạng đơn giản và phổ biến nhất.
- Truyền thông: dữ liệu được gửi và nhận đến một máy tính xác định và đưa dữ liệu đó lên cáp dưới dạng tín hiệu điện tử. Sự hỏng hóc của một máy không ảnh hưởng đến hoạt động của toàn mạng.

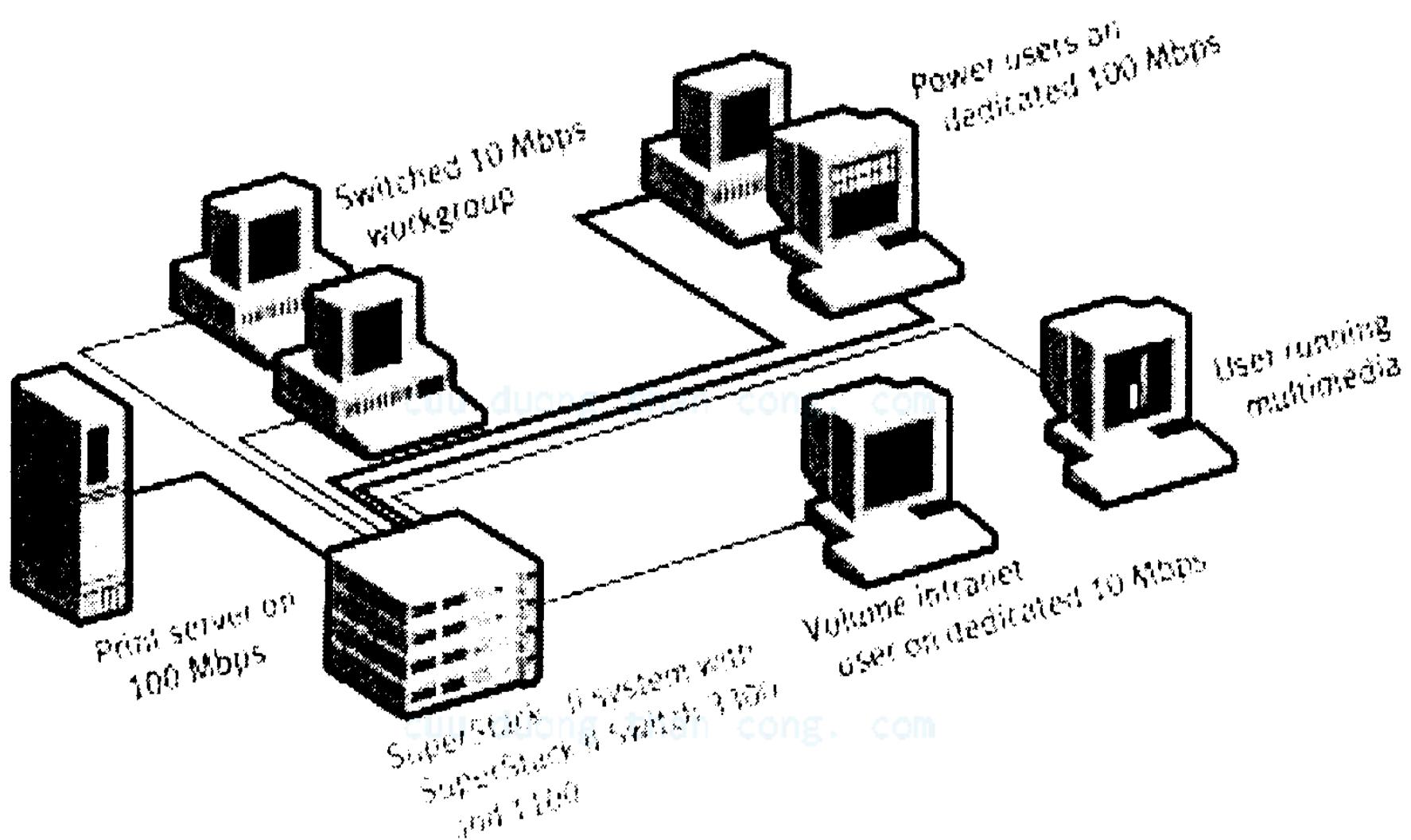


Sơ đồ BUS tuyến tính

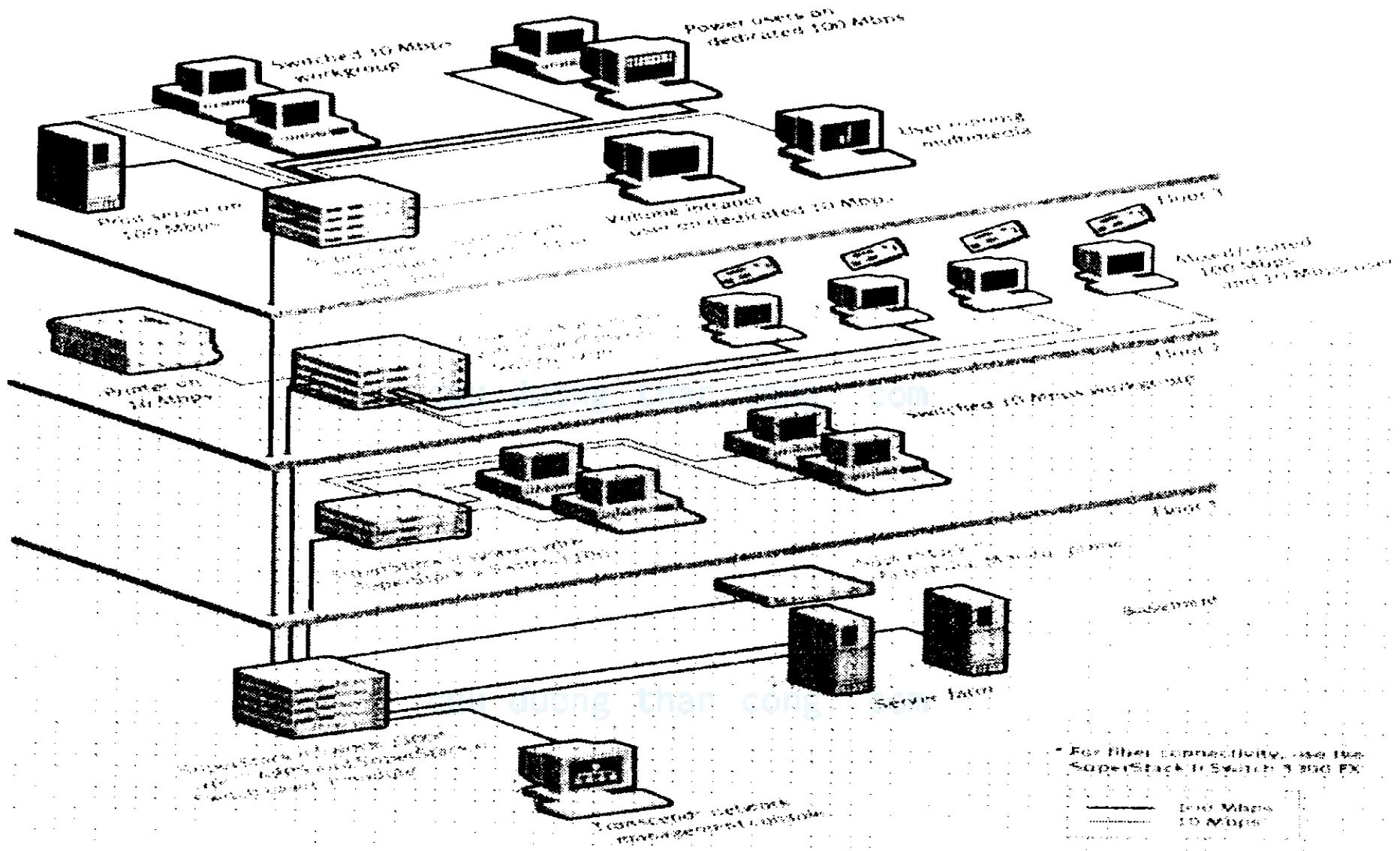
III. Phân loại mạng máy tính

● Mạng star (hình sao)

- Cấu hình vật lý: Các máy tính được nối cáp vào một bộ phận được gọi là hub (đầu nối trung tâm). Cấu hình này bắt nguồn từ thời kì đầu, khi việc tính toán dựa trên hệ thống máy tính nối vào một máy chính trung tâm.
- Truyền thông: Tín hiệu được truyền từ máy tính đến hub để đến tất cả các máy tính trên mạng. Nếu hub trung tâm hỏng, toàn bộ hệ thống sẽ sụp đổ.



Mô hình mạng hình sao tập trung



Mô hình mạng hình sao phân tán

III. Phân loại mạng máy tính

- **Mạng ring (vòng khép kín)**

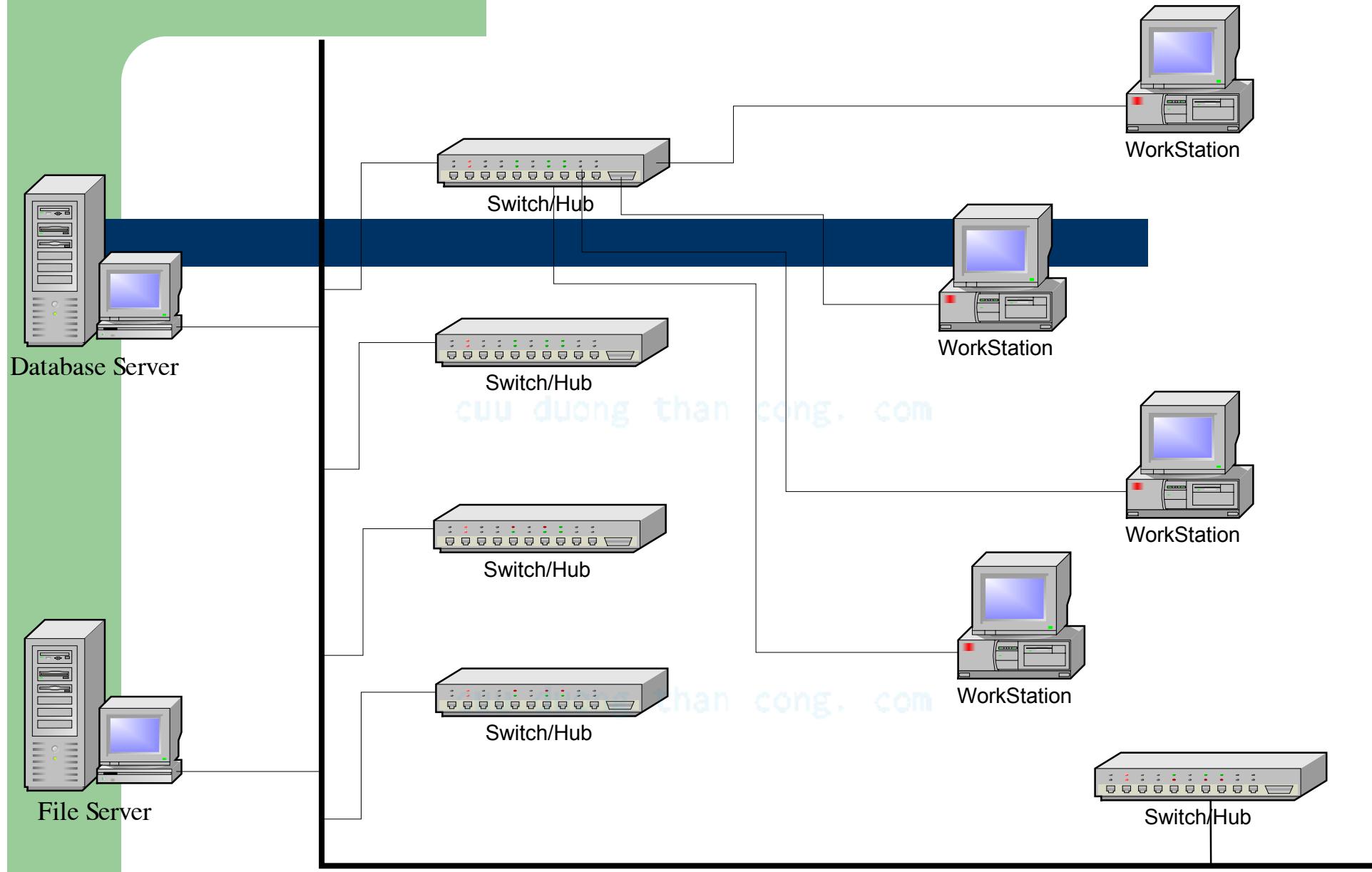
- Cấu hình vật lý: các máy tính được nối với nhau trên một vòng cáp. Không có đầu nào bị hở.
 - Truyền thông: Tín hiệu được đi qua một chiều và đi qua từng máy tính, mỗi máy tính đóng vai trò như một trạm chuyển tiếp, khuếch đại tín hiệu và gửi nó đến máy tính tiếp theo. Do tín hiệu đi qua từng máy nên sự hỏng hóc của một máy có thể ảnh hưởng đến toàn mạng.

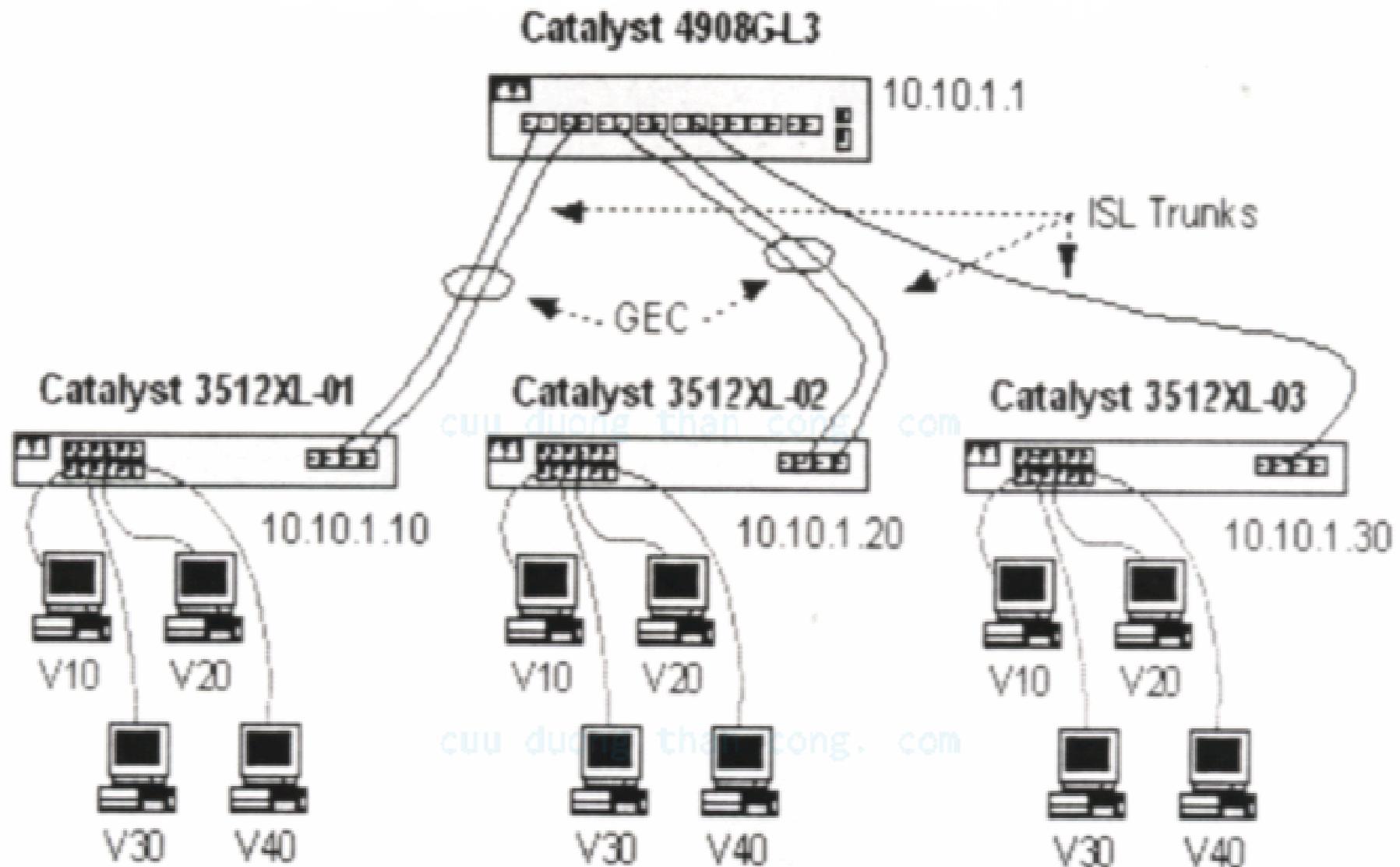
- **Mạng kết hợp**

- Mạng kết hợp là kiểu ghép nối sắp xếp các máy tính trong mạng kết hợp các cấu hình ghép nối trên (bus, start, ring) để lợi dụng được tối đa ưu nhược điểm của mỗi cấu hình.

Lương Việt Nguyên

Nhập môn mạng máy tính





Một số ví dụ về kết nối VLAN

Cấu hình mạng	Ưu điểm	Nhược điểm
Bus	Dùng cáp tiết kiệm Phương tiện rẻ tiền và dễ làm việc Đơn giản, đáng tin cậy Để mở rộng	Chạy chậm khi lưu lượng mạng tăng Khó phát hiện và tách ly các vấn đề Cáp đứt có thể ảnh hưởng nhiều đến hoạt động của toàn mạng
Ring	Mọi máy đều có quyền truy cập như nhau Tiến độ thi hành ổn định bất chấp nhiều người dùng	Sự hỏng hóc của một máy tính có thể ảnh hưởng đến các máy còn lại trên mạng Khó phát hiện và tách ly các vấn đề Tái cấu hình mạng sẽ làm mạng ngừng hoạt động
Star	Dễ chỉnh sửa và bổ sung máy tính mới. Theo dõi và quản lý tập trung Sự hỏng hóc của một máy tính không ảnh hưởng đến các máy còn lại trên mạng	Nếu điểm trung tâm bị hỏng thì ảnh hưởng đến toàn mạng.

IV. Địa chỉ mạng, định tuyến, tính tin cậy, tính liên tác và an ninh mạng

1. Địa chỉ mạng:

- Gán cho mỗi nút mạng 1 địa chỉ duy nhất – cho phép các thiết bị khác định vị được nó.
 - Ví dụ: Mỗi điện thoại (1 nút) có mã vùng và 1 số (địa chỉ). Mã vùng cung cấp thông tin về vị trí của nút đó trong 1 vùng nào đó, còn số điện thoại là số xác định duy nhất máy điện thoại trong vùng đó. Về thực chất mã vùng lại được phân cấp thành mã quốc gia và mã khu vực.

IV. Địa chỉ mạng, định tuyến, tính tin cậy, tính liên tác và an ninh mạng

2. Routing – Định tuyến

- Quyết định tuyến đường mà dữ liệu sẽ đi qua khi chuyển từ nút nhận đến nút gửi.
- Chức năng định tuyến được thực hiện bởi 1 thiết bị phần cứng đặc biệt: router (định tuyến).
- Việc lựa chọn tuyến đường tốt nhất phải dựa trên 1 tiêu chuẩn cụ thể - được gọi là độ đo (met).
- Các độ đo định tuyến phổ biến là: khoảng cách, số chặng (hop) và băng thông.

IV. Địa chỉ mạng, định tuyến, tính tin cậy, tính liên tác và an ninh mạng

3. Tính tin cậy:

- Chỉ tính toàn vẹn dữ liệu – đảm bảo rằng dữ liệu nhận được giống hệt dữ liệu được gửi đi. Trong thực tế lỗi có thể xảy ra ở tất cả các môi trường truyền mạng. Vì vậy phải thiết kế sao cho hệ thống có khả năng xử lý lỗi.
- Một trong những chiến lược điển hình là thêm thông tin vào dữ liệu được truyền đi sao cho phía bên nhận phát hiện được lỗi (nếu có). Khi phát hiện lỗi nó có thể thực hiện:
 - Yêu cầu truyền lại dữ liệu bị lỗi
 - Kiểm tra xem dữ liệu đúng là gì và sửa đổi dữ liệu bị truyền lỗi.
- Cách thứ nhất sửa lỗi bằng cách yêu cầu truyền lại, cách thứ hai gọi là khả năng tự sửa lỗi. Việc sửa lỗi nói chung khó thực hiện.

IV. Địa chỉ mạng, định tuyến, tính tin cậy, tính liên tác và an ninh mạng

4. Tính liên tác:

- Các sản phẩm của các hãng khác nhau có thể giao tiếp thành công với nhau trên mạng.
- Ngày nay với bộ giao thức “mở” TCP/IP các hãng sản xuất – những người viết và bán các ứng dụng dựa trên TCP/IP được tự do làm những thứ họ muốn, không lo ngại về vi phạm bản quyền.

IV. Địa chỉ mạng, định tuyến, tính tin cậy, tính liên tác và an ninh mạng

5. An ninh:

- An ninh mạng chỉ việc bảo vệ mọi thứ liên quan đến 1 mạng bao gồm dữ liệu, phương tiện truyền thông và các thiết bị. An ninh mạng còn bao gồm các chức năng quản trị, các công cụ kỹ thuật và thiết bị như các sản phẩm mã hoá, các sản phẩm kiểm soát truy cập mạng (ví dụ: firewall – thiết bị phần cứng đặc biệt bảo vệ 1 mạng khỏi thế giới bên ngoài).
- An ninh mạng bao gồm việc quy định những chính sách sử dụng tài nguyên mạng, kiểm tra xem tài nguyên mạng có được sử dụng phù hợp với chính sách đã định trước hay không, quy định và kiểm tra những người có đủ quyền mới được sử dụng các tài nguyên đó.

V. Mô hình mạng OSI

Truyền thông mạng: Hoạt động mạng là quá trình gửi dữ liệu từ máy tính này sang máy tính khác. Quá trình này có thể được chia thành các tác vụ riêng biệt:

- Nhận biết dữ liệu
- Chia dữ liệu thành từng gói để có thể quản lý được
- Thêm thông tin vào từng gói để xác định địa chỉ máy nhận và vị trí của gói tin.
- Bổ sung thông tin để kiểm tra lỗi và thời lượng
- Đưa dữ liệu lên mạng và gửi đi

Các thủ tục này được HĐH tuân theo một cách nghiêm ngặt, những thủ tục này được gọi là giao thức. Mô hình OSI (Open Systems Interconnection) được tổ chức tiêu chuẩn quốc tế ISO bàn hành để mô tả kiến trúc mạng dành cho việc nối kết những thiết bị không cùng chủng loại.

V. Mô hình mạng OSI

Mô hình OSI:

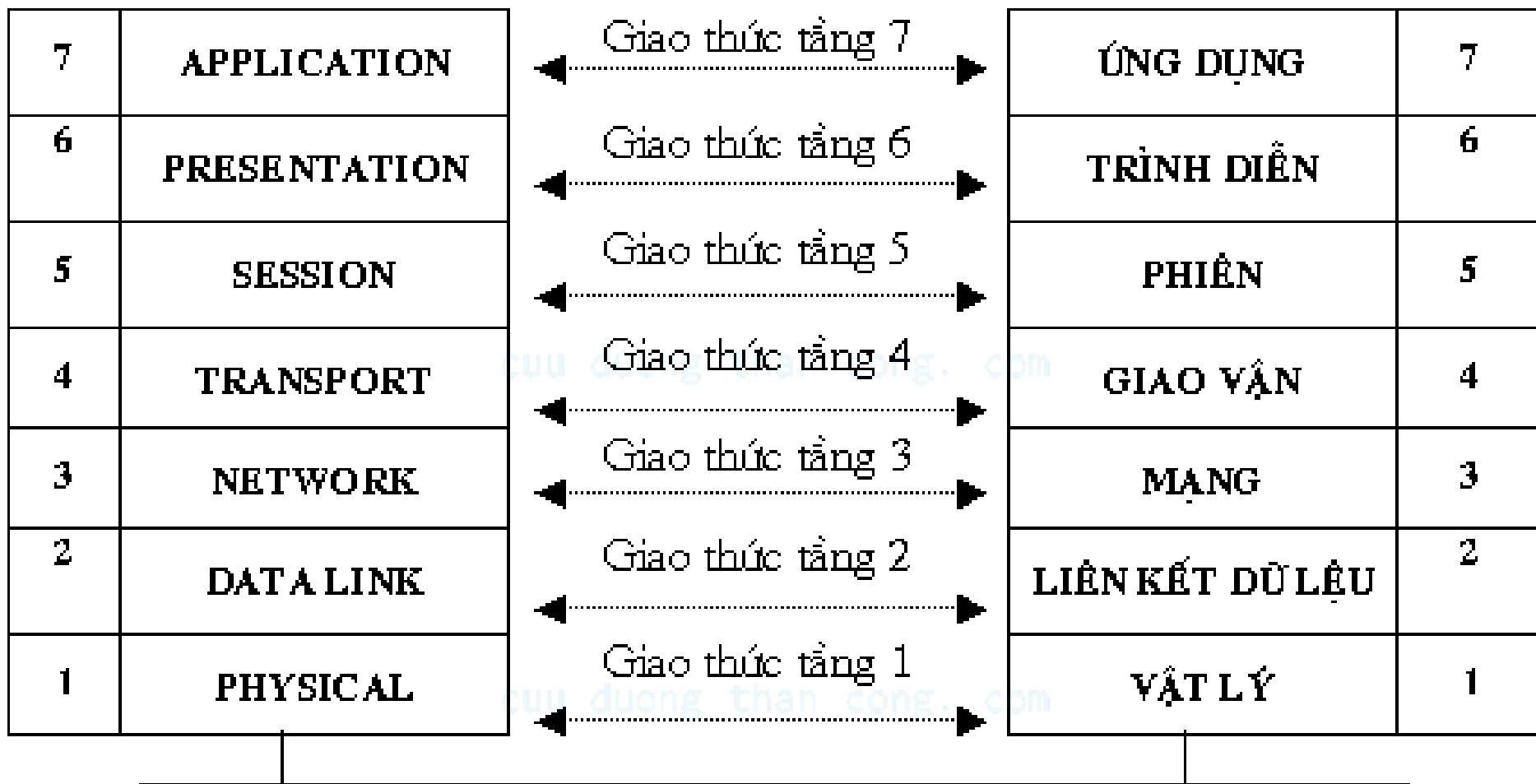
- Mô hình OSI là kiến trúc chia mạng truyền thông thành 7 tầng.
- Mỗi tầng bao gồm những hoạt động, thiết bị và giao thức mạng khác nhau.
- Mỗi tầng cung cấp dịch vụ hoặc hoạt động chuẩn bị dữ liệu để chuyển giao qua mạng đến máy tính khác.
- Các tầng đều được phân chia bằng ranh giới được gọi là giao diện.
- Mọi yêu cầu đều được chuyển từ tầng này sang tầng khác thông qua giao diện rồi đến tầng tiếp theo. Mỗi tầng đều phải tuân theo chuẩn và hoạt động của tầng bên dưới.

Lương Việt Nguyên

Hệ thống mở A

Nhập môn mạng máy tính

Hệ thống mở B



Đường truyền vật lý

Hình 1.I2 Mô hình OSI 7 tầng.

V. Mô hình mạng OSI

1. Tầng Ứng dụng

- Đóng vai trò như cửa sổ dành cho các hoạt động xử lý của trình ứng dụng nhằm truy nhập các dịch vụ mạng. Tầng này biểu diễn những dịch vụ hỗ trợ trực tiếp các ứng dụng người dùng, như các phần mềm chuyển tập tin, truy cập cơ sở dữ liệu và email

2. Tầng Presentation

- Tầng này quyết định dạng thức dùng trao đổi dữ liệu giữa các máy tính mạng. Tầng Presentation ở máy gửi diễn dịch dữ liệu được truyền từ tầng Ứng dụng sang dạng thức trung gian mà ứng dụng nào cũng có thể nhận biết, phía máy nhận, tầng này kết hợp dữ liệu từ dạng thức trung gian và truyền lên tầng ứng dụng.

V. Mô hình mạng OSI

3. Tầng Session (phiên)

- Cho phép hai chương trình ứng dụng trên các máy tính khác nhau thiết lập, sử dụng và chấm dứt một nối kết gọi là phiên làm việc. Tầng này thi hành các thủ tục cho phép nhận biết tên và thực hiện các chức năng cần thiết như bảo mật. Tiến hành việc đồng bộ hóa bằng cách đặt các điểm check point vào luồng dữ liệu, bằng cách này, nếu mạng bị ngắt, chỉ những dữ liệu sau điểm kiểm tra cuối cùng mới phải chuyển lại.

4. Tầng Transport (giao vận)

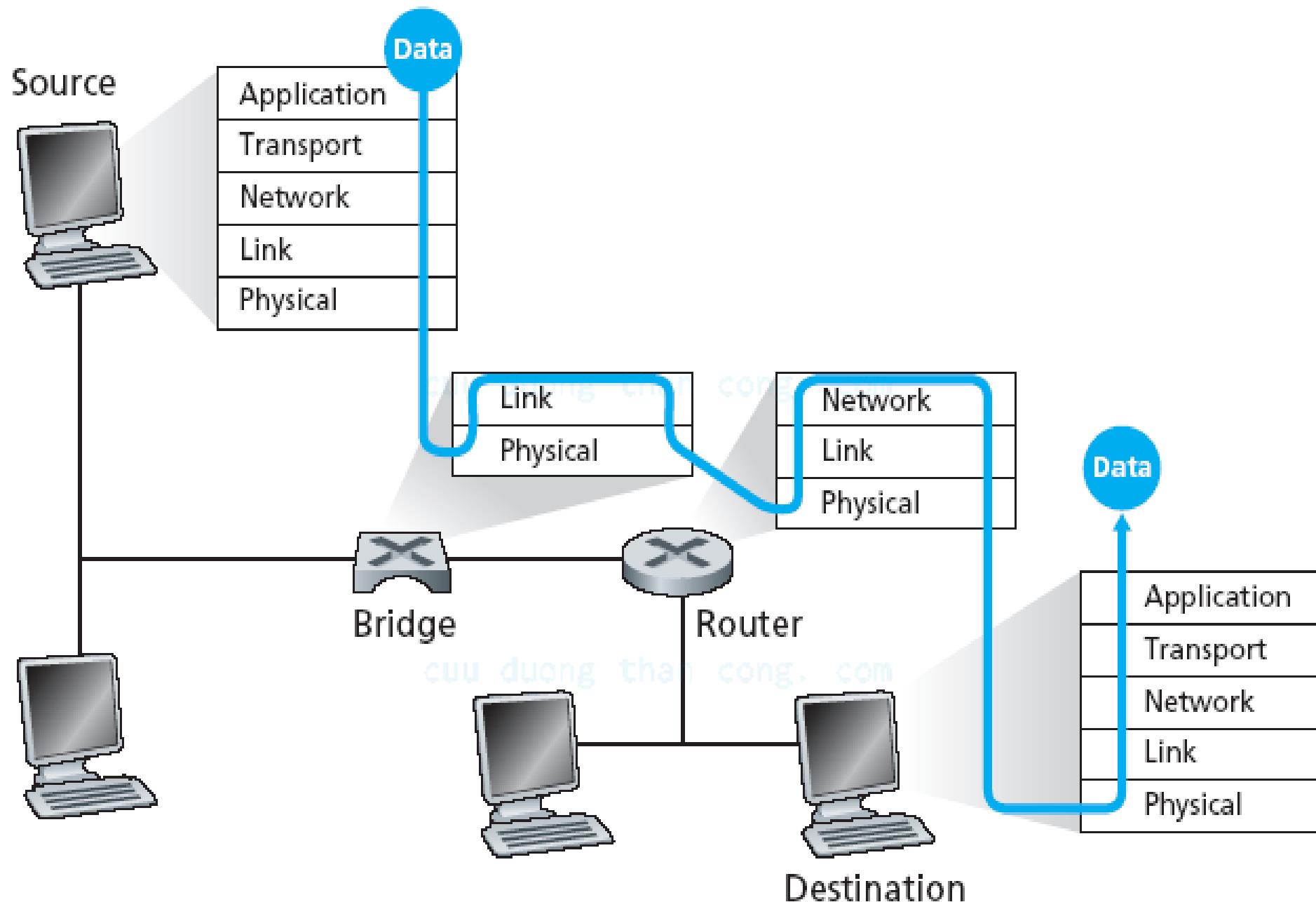
- Tầng này bảo đảm gói tin truyền đi không có lỗi, theo đúng thứ tự, không bị mất mát hay sao chép. Tầng này đóng gói thông điệp, chia thông điệp dài thành nhiều gói. Tại đầu nhận, tầng này mở gói thông điệp, lắp ghép lại cho đúng thứ tự

V. Mô hình mạng OSI

5. Tầng Network (mạng): Chịu trách nhiệm lập địa chỉ các thông điệp, diễn dịch địa chỉ và tên logic thành địa chỉ vật lý. Tầng này quyết định đường đi từ máy chủ đến máy đích, nó sẽ quyết định chọn đường mạng nào để đi

6. Tầng Data Link (Liên kết dữ liệu): Gửi khung dữ liệu từ tầng Network đến tầng Physical. Ở đầu nhận, tầng này đóng gói dữ liệu thô (chưa được xử lý) từ tầng Physical thành khung dữ liệu.

7. Tầng Physical: Tầng này chuyển luồng bit thô qua phương tiện vật lý. Tầng này chịu trách nhiệm liên kết các giao diện hàm, cơ, quang và điện với cáp. Nó định nghĩa cách kết nối cáp với card mạng như thế nào, định rõ từng kĩ thuật truyền nào sẽ được đối với từng loại cáp mạng.



VI. Kết nối các mạng máy tính

- Do nhu cầu trao đổi thông tin ngày càng cao nên việc kết nối các mạng máy tính lại với nhau đã trở thành một vấn đề được quan tâm đặc biệt. Mục tiêu đặt ra là phải làm sao để những người sử dụng trên mạng khác nhau (về chủng loại, về kiến trúc hoặc vị trí địa lý) có thể trao đổi thông tin với nhau một cách dễ dàng và hiệu quả.

VI. Kết nối các mạng máy tính

1. Các chiến lược kết nối.

- Để kết nối các mạng máy tính đang tồn tại lại với nhau người ta thường xuất phát từ hai quan điểm sau:
 - 1. Xem mỗi nút của mạng con như một hệ thống mở.
 - 2. Xem mỗi mạng con như một hệ thống mở.
- Quan điểm 1 cho phép mỗi nút của mạng con có thể truyền thông trực tiếp với mỗi nút của mạng con bất kỳ khác. Như vậy toàn bộ các mạng con cũng sẽ là nút của mạng lớn và tuân thủ một kiến trúc chung.
- Trong khi đó theo cách tiếp cận thứ 2 thì hai nút thuộc hai mạng con khác nhau không thể trực tiếp "bắt tay" nhau được mà phải qua một phần tử trung gian gọi là giao diện kết (Interconnection Interface) đặt giữa hai mạng con đó có nghĩa là cũng hình thành một mạng lớn gồm các giao diện kết nối và các máy chủ (Host) được nối với nhau bởi các mạng con.

VI. Kết nối các mạng máy tính

- Tương ứng với hai quan điểm trên có hai chiến lược kết nối các mạng.
 - Tìm cách xây dựng các chuẩn chung cho các mạng (các công trình chuẩn hoá của CCITT và ISO)
 - Cố gắng xây dựng các giao diện nối kết đảm bảo tính độc lập của các mạng con hiện có.
- Sự hội tụ về một chuẩn chung là điều lý tưởng, nhưng thực tế không thể loại bỏ hàng ngàn mạng khác nhau đang tồn tại trên thế giới. Vì vậy trên thị trường xuất hiện hàng loạt các sản phẩm giao diện kết nối cho phép chuyển đổi giữa các mạng khác nhau. Đó là biểu thị tính thực tế hơn của chiến lược thứ 2.

VI. Kết nối các mạng máy tính

2. Giao diện kết nối

- Chức năng cụ thể của một giao diện kết nối phụ thuộc vào sự khác biệt về kiến trúc của các mạng con. Sự khác biệt càng lớn thì chức năng của giao diện càng phức tạp. Một giao diện kết nối có thể thực hiện nối "tay đôi" hoặc "tay ba" hoặc "nhiều tay" tùy người thiết kế. Hơn nữa chúng có thể là một máy tính độc lập nhưng cũng có thể được cài đặt ghép vào một nút của một mạng con nào đó.

VI. Kết nối các mạng máy tính

- Tuỳ thuộc vào chức năng cụ thể mà giao diện kết nối có thể có các tên gọi riêng như bridge, router, gateway. Gateway (cửa khẩu) là tên gọi chung nhất cho các giao diện kết nối và thường dùng trong những trường hợp chức năng của các giao diện này là phức tạp, đòi hỏi sự chuyển đổi giữa các họ giao thức khác nhau được dùng trong các mạng con. Trong khi đó bridge (cầu) được dùng để chỉ giao diện kết nối trong trường hợp đơn giản nhất, ví dụ kết nối giữa các mạng cục bộ (LAN) cùng loại. Còn router (bộ chọn đường) hoạt động ở mức cao hơn so với bridge vì nó còn đảm nhận cả việc chọn đường cho các đơn vị dữ liệu để hướng chúng tới đích.

VII. Mô hình tham chiếu TCP/IP

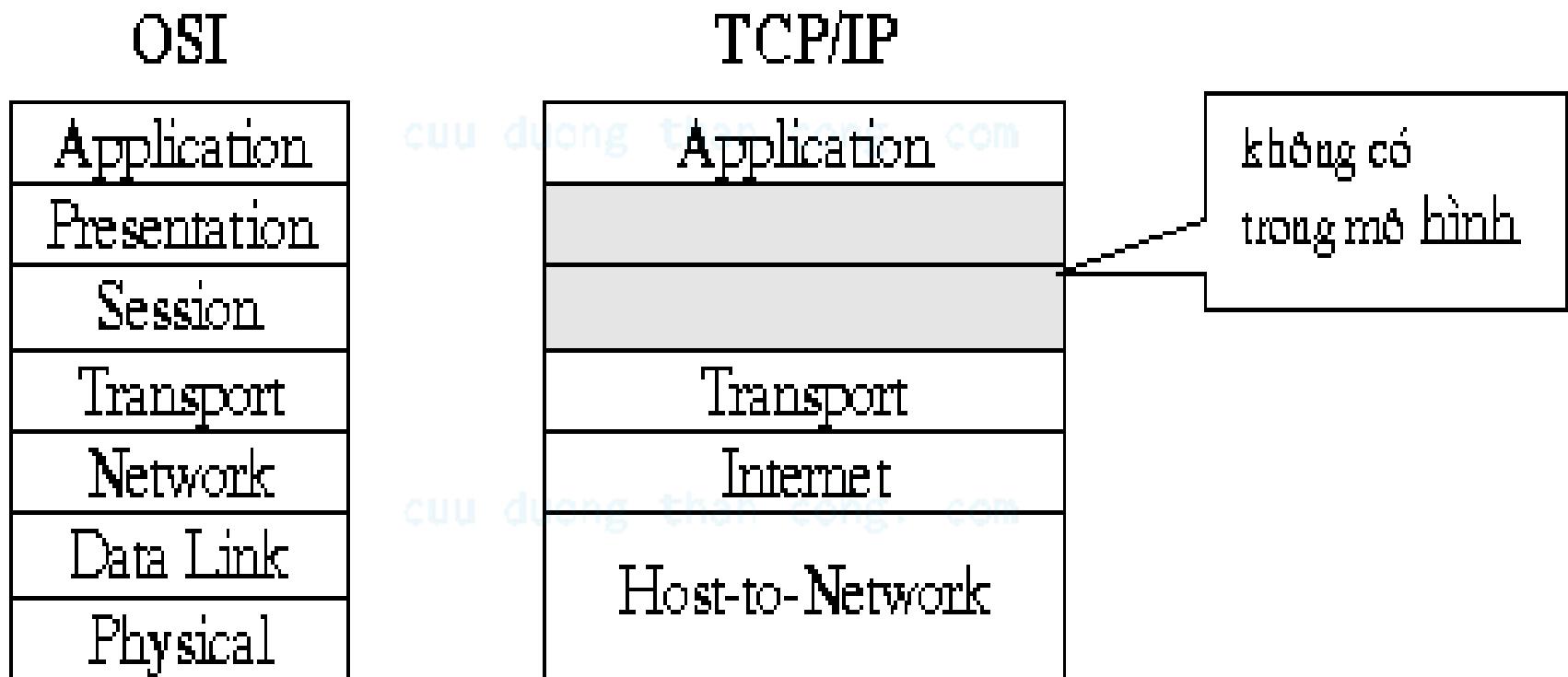
- Mạng ARPANET được xây dựng bởi Bộ Quốc phòng Mỹ từ 1969 với họ giao thức TCP/IP nổi tiếng và là tiền thân của INTERNET ngày nay. Bộ Quốc phòng Mỹ sợ rằng nếu chiến tranh hạt nhân xảy ra, các đường truyền vật lý cũng như các Host, router, Gateway đắt tiền của họ sẽ có thể bị phá hủy ngay từ phút đầu tiên. Mạng ARPANET cần có khả năng hoạt động ngay cả trong trường hợp đó, miễn là máy nguồn và máy đích vẫn còn hoạt động và còn có một đường truyền (vật lý) giữa chúng.
- Sau này khi các mạng vệ tinh và mạng vô tuyến ra đời và bổ sung vào thì các giao thức đang được dùng của ARPANET không đáp ứng được yêu cầu liên mạng. Cần phải có một mô hình kiến trúc mới có khả năng liên kết nhiều mạng với nhau một cách trong suốt. Kiến trúc này có tên Mô hình tham chiếu TCP/IP. đặt theo tên của 2 giao thức cơ bản của nó.

VII. Mô hình tham chiếu TCP/IP

1. Tầng Internet (The Internet Layer).

- Các yêu cầu nêu trên dẫn tới một lựa chọn một mạng chuyển mạch gói dựa trên một tầng internetwork không hướng nối. Tầng này được gọi là Internet Layer. Nhiệm vụ của lớp này là chọn đường cho các gói tin (packets routing) và tránh tắc nghẽn (avoiding congestion). Nó cho phép các Host truyền các packet vào mọi mạng, mỗi packet có thể đi đến đích theo các con đường khác nhau, thứ tự nhận các gói tin có thể khác với thứ tự mà chúng được gửi đi, các tầng trên tự giải quyết vấn đề thứ tự các packet.
- Tầng internet định nghĩa một khuôn dạng packet và giao thức chính thức (official) được gọi là IP (Intetnet Protocol). Công việc của Tầng Internet là phân phát các IP packet tới đích của chúng.

VII. Mô hình tham chiếu TCP/IP



Hình I.13 Mô hình tham chiếu TCP/IP

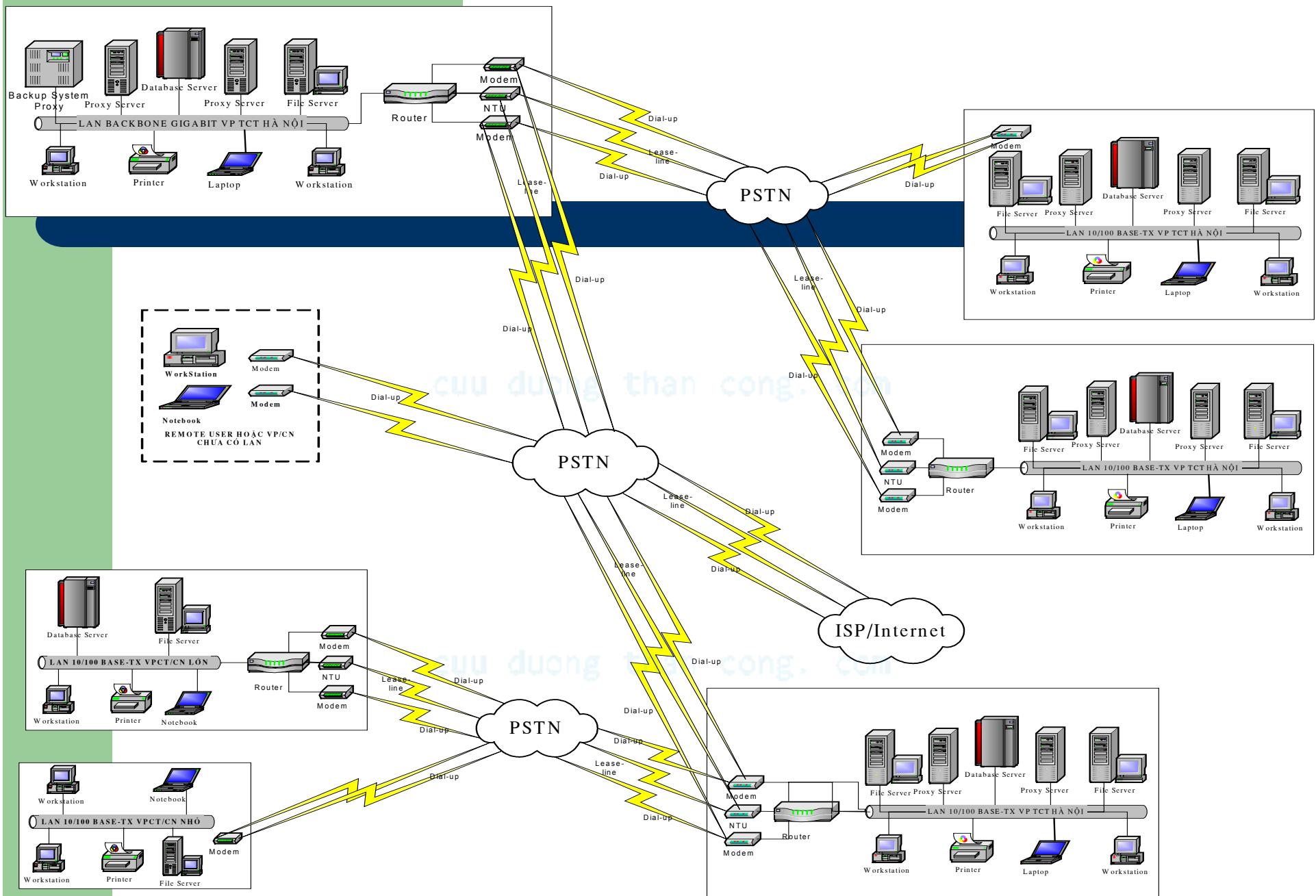
VIII. Ví dụ mạng

cuu duong than cong. com

cuu duong than cong. com

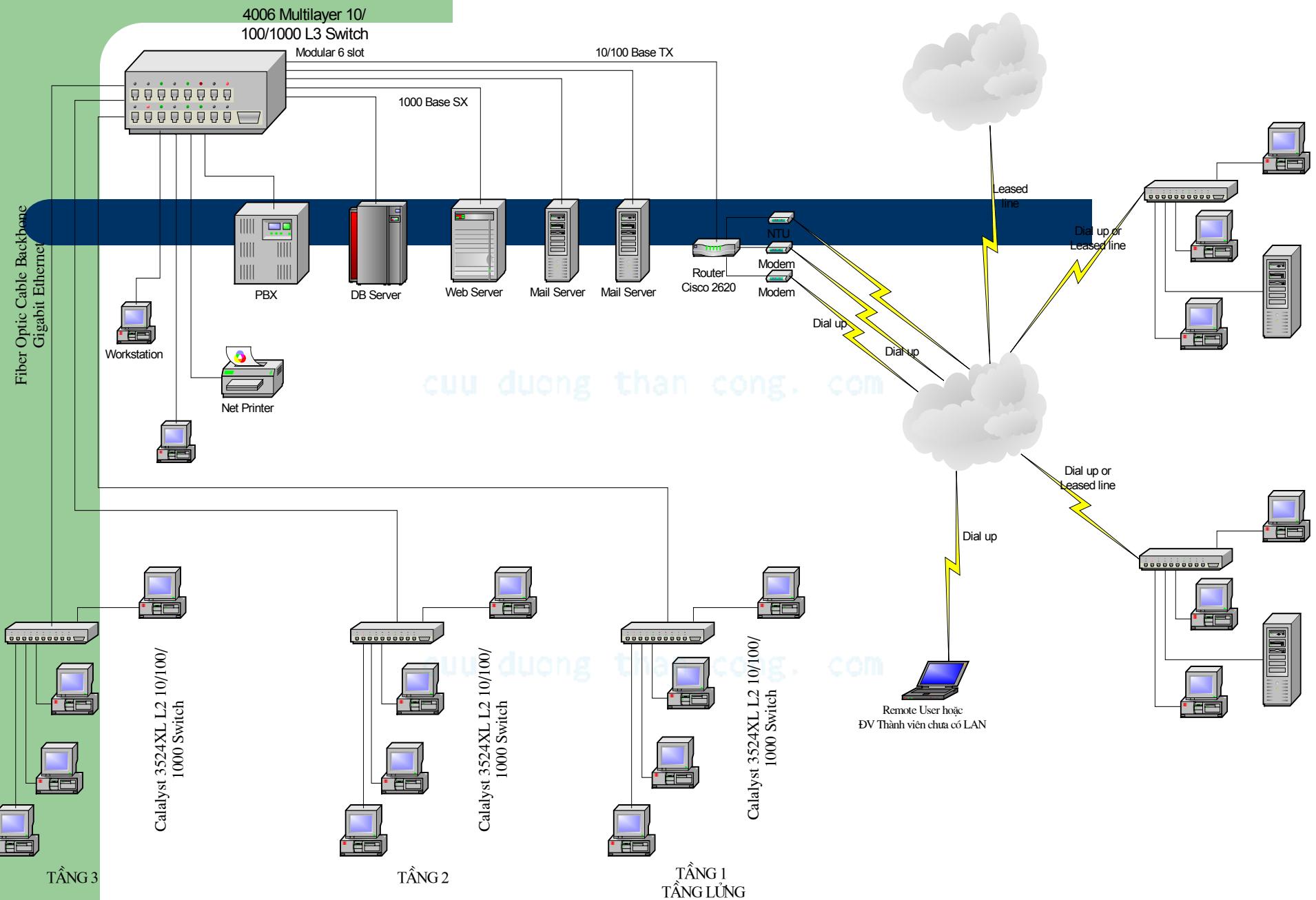
Lương Việt Nguyên

Nhập môn mạng máy tính



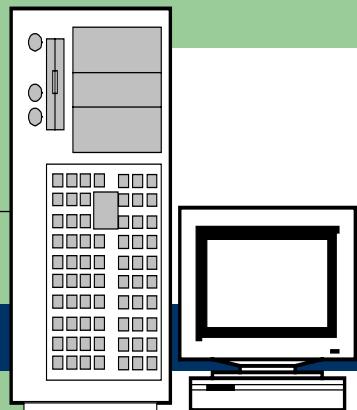
Lương Việt Nguyên

Nhập môn mạng máy tính

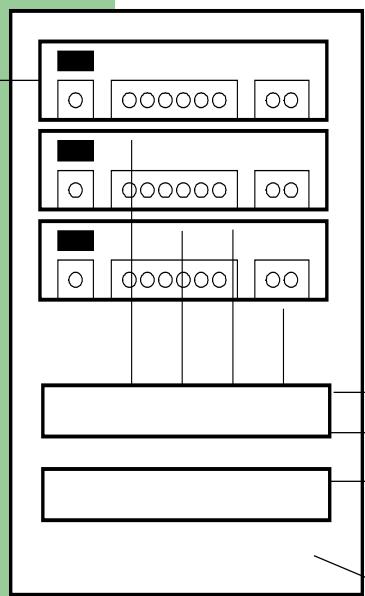


Lương Việt Nguyên

Nhập môn mạng máy tính



File Server



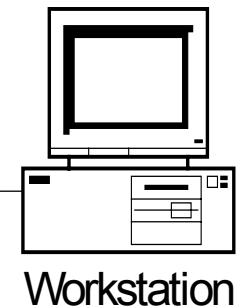
Switch
Hub

Patch Panel

CABINET

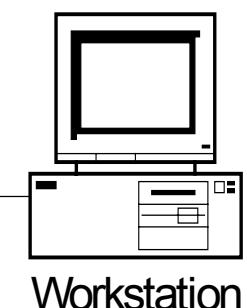
cuuduongthancong.com

WallPlate



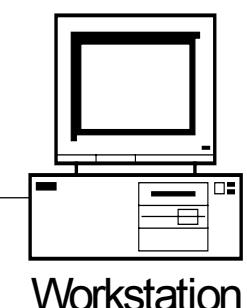
Workstation

WallPlate



Workstation

WallPlate



Workstation

Bài 2: Các loại mạng chủ yếu

- Nói chung, tất cả các mạng máy tính đều có chung một số thành phần, chức năng, và đặc tính nhất định. Đó là:
 - Máy phục vụ (Server) - Máy cung cấp tài nguyên chung cho người dùng mạng *cuu duong than cong. com*
 - Máy khách (Client) - Máy truy cập tài nguyên mạng dùng chung do máy phục vụ cung cấp
 - Phương tiện truyền dẫn (media) - Cách thức và vật liệu nối máy tính
 - Dữ liệu dùng chung (shared data) - Các tập tin do máy phục vụ cung cấp ngang qua mạng
 - Máy in và các thiết bị ngoại vi - Các tài nguyên khác do máy phục vụ cung cấp *cuu duong than cong. com*
 - Tài nguyên (resource) - Tập tin, máy in, hoặc những thành phần khác mà người dùng mạng sử dụng
- Mặc dù những điểm tương đồng trên, mạng máy tính vẫn được chia làm hai loại rõ rệt:
- Ngang hàng và Dựa trên máy phục vụ

I. Mạng ngang hàng:

- Trong hệ thống mạng ngang hàng, không có bất kỳ máy phục vụ chuyên dụng nào. Mọi máy tính trong hệ thống mạng đều bình đẳng và có vai trò như nhau.
- Vì mỗi máy đều hoạt động với vai trò vừa là máy chủ, vừa là máy phục vụ. Người dùng trên tự quyết định tài nguyên nào sẽ được dùng chung trên mạng.

1. Quy mô: Mạng ngang hàng còn được gọi là nhóm làm việc. Mỗi nhóm có khoảng 8 - 10 máy tính

I. Mạng ngang hàng:

2. Phí tổn

- Mạng ngang hàng tương đối đơn giản. Vì mỗi máy tính kiêm cả hai chức năng phục vụ và máy khách, nên không cần phải có máy chủ trung tâm thật mạnh. Mạng ngang hàng có thể rẻ tiền hơn mạng dựa trên máy phục vụ.
- Nên dùng mạng ngang hàng khi:
 - Có dưới 10 người dùng
 - Mọi người dùng đều trong một khu vực
 - Tính bảo mật không là yêu cầu bắt buộc

I. Mạng ngang hàng:

3. Hệ điều hành ngang hàng

- Phần mềm hệ điều hành mạng không nhất thiết phải có khả năng thi hành và tính bảo mật tương xứng với phần mềm điều hành cho máy phục vụ chuyên dụng.
- Chỉ cần sử dụng những hệ điều hành đơn giản như: MS Windows NT Workstations, MS Windows for Workgroups, MS Windows 95 để thích hợp cho mô hình mạng ngang hàng.
- Không cần phải có thêm phần mềm nào khác để thiết lập mạng.

II. Mạng dựa trên máy phục vụ

- Nếu môi trường có nhiều người sử dụng (trên 10 máy), mạng ngang hàng chắc chắn sẽ không thỏa đáng. Vì thế, hầu hết các mạng đều có máy chủ phục vụ chuyên dụng. Máy phục vụ chỉ hoạt động như một máy phục vụ chứ không là máy khách như máy trạm làm việc.
- Tuy nhiên với sự phát triển về quy mô và lưu lượng thông tin trên mạng, một mạng máy tính yêu cầu phải có nhiều máy chủ. Phân phối tác vụ giữa các máy chủ để đạt được hiệu quả công việc cao nhất.

II. Mạng dựa trên máy phục vụ

1. Máy phục vụ chuyên dụng

- Máy phục vụ dành cho các mạng lớn được chuyên môn hoá nhằm đáp ứng trọn vẹn nhu cầu của người dùng. Ví dụ, mạng Windows NT có nhiều loại máy phục vụ khác nhau như:
 - Máy phục vụ tập tin/in ấn (file/print server)
 - Máy phục vụ chương trình ứng dụng (application server)
 - Máy phục vụ thư tín (mail server)
 - Máy phục vụ fax (fax server)
 - Máy phục vụ truyền thông (communication server)

II. Mạng dựa trên máy phục vụ

2. Vai trò của phần mềm

- Một máy phục vụ mạng và hệ điều hành mạng phối hợp với nhau như một đơn vị. Cho dù là mạnh mẽ tới đâu chăng nữa, nếu máy chủ không có được một hệ điều hành có khả năng vận dụng tối đa tài nguyên vật lý của nó.
- Hiện nay, có nhiều hệ điều hành mạng được sử dụng để đáp ứng nhu cầu công việc khác nhau như:
 - UNIX
 - Linux
 - Windows NT, Window 2000 family

II. Mạng dựa trên máy phục vụ

3. Ưu điểm của mạng dựa trên máy phục vụ

- Dùng chung tài nguyên: Máy chủ được thiết kế để cung cấp khả năng truy cập nhiều tập tin và máy in, đồng thời duy trì hiệu suất thi hành và sự an toàn cho người dùng. Tài nguyên trên máy chủ phục vụ thường được lắp đặt tập trung nên dễ tìm kiếm và truy xuất hơn là tài nguyên được đặt nầm rải rác ở các máy.
- An toàn và bảo mật: Giải pháp mạng dựa trên máy chủ phục vụ chiếm ưu thế hơn trong các vấn đề về an toàn và bảo mật. Trong một hệ điều hành mạng, người quản trị thường đặt ra các chính sách và áp chính sách đó cho từng người dùng trên mạng.

II. Mạng dựa trên máy phục vụ

- Sao lưu: Do những dữ liệu quan trọng có thể phải đặt tập trung lên một hoặc hai máy chủ để đảm bảo cho dữ liệu được an toàn tuyệt đối.
- Sự dư thừa: Thông qua hệ thống dư thừa dữ liệu, bất cứ dữ liệu nào cũng được sao chép và lưu trữ trên mạng, sao cho vẫn có thể phục hồi lại dữ liệu ban đầu từ các vùng bản sao dữ liệu đó.
- Các yêu cầu về phần cứng: Phần cứng của máy khách thường nhỏ, chỉ đủ cho người dùng. Nhưng phần cứng cho máy chủ phục vụ phải yêu cầu cao hơn, tùy thuộc vào mục đích sử dụng của máy chủ phục vụ.

II. Mạng dựa trên máy phục vụ

4. Mạng kết hợp

- Việc kết hợp hai loại mạng trên với nhau để lợi dụng được các đặc tính ưu việt của cả hai loại mạng không có gì lạ. Trong mạng kết hợp, các hệ điều hành hoạt động phối hợp với nhau nhằm tạo cảm giác về một hệ thống hoàn chỉnh.
- Hệ điều hành mạng dựa trên máy chủ phục vụ: như MS Windows NT Server hoặc Novell, NetWare. Hệ điều hành máy khách có thể là MS Windows NT Workstation, MS Windows 98.
- Loại mạng này tuy phổ biến, nhưng nó đòi hỏi nhiều công sức và thời gian hoạch định và đào tạo, để bảo đảm sự thi hành đúng đắn và mức độ an toàn tốt.

III. Cấu hình mạng

- Cấu hình mạng là việc sắp xếp, bố trí vật lý của máy tính, dây cáp, và các thành phần khác trên mạng theo phương diện vật lý. Cấu hình mạng ảnh hưởng đến các khả năng của mạng. Một cấu hình mạng có thể ảnh hưởng đến:
 - Loại thiết bị mạng cần
 - Các khả năng của thiết bị
 - Sự phát triển của mạng
 - Cách thức quản lý mạng

III. Cấu hình mạng

- Cấu hình mạng hay cách xếp đặt các máy tính trong mạng phụ thuộc vào card mạng, dây cáp mạng, hệ điều hành mạng và các thành phần phụ trợ khác.
- Một cấu hình mạng không chỉ quyết định loại cáp sử dụng mà còn quyết định phải đi cáp qua môi trường thực tế như thế nào (trần nhà, sàn nhà, tường). Thậm chí nó còn quyết định đến giao thức giao tiếp giữa các máy tính trong mạng. Cấu hình khác nhau sẽ đòi hỏi phương pháp giao tiếp khác nhau.

Bài 3: Phương tiện vật lý cho việc thiết kế mạng

I. Cáp mạng

Các loại cáp chính:

- Ngày nay, phần lớn các mạng được nối bằng dây dẫn hoặc cáp, dây dẫn và cáp đóng vai trò như phương tiện truyền tín hiệu giữa các máy tính trên mạng.
- Có 3 nhóm cáp chính:
 - Cáp đồng trục (coaxial)
 - Cáp xoắn đôi (twisted-pair)
 - Cáp xoắn đôi trần
 - Cáp xoắn đôi có bọc
 - Cáp sợi quang (fiber-optic)

I. Cáp mạng

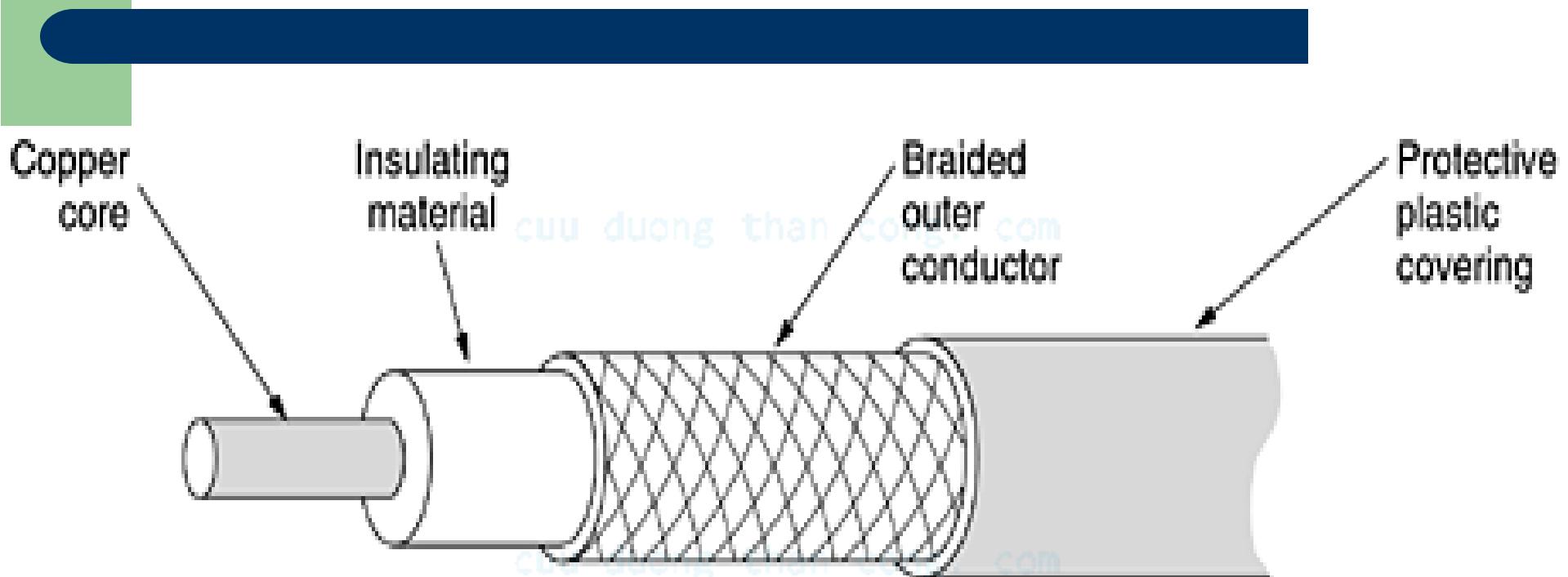
1. Cáp đồng trục

- Cáp đồng trục gồm một lõi đồng nguyên chất được bọc chất cách ly, một lớp bảo vệ bằng lưới kim loại và một lớp vỏ bọc ngoài.
- Lớp bảo vệ là tấm lưới kim loại bọc quanh một số loại cáp, có tác dụng hút tín hiệu điện tử chạy lạc không cho ảnh hưởng đến tín hiệu dữ liệu được truyền trên dây cáp.
- Lõi đồng trục mang tín hiệu điện tử tạo thành dữ liệu. Đây là lõi đặc hoặc lõi có dạng bện.
- Bao quanh lõi là một lớp cách ly, ngăn cách lõi với lưới kim loại.

I. Cáp mạng

Các loại cáp đồng trục:

- ***Loại cáp mảnh (thinnet)***
 - Có đường kính khoảng 0.5cm.
 - Mang tín hiệu đi xa tới 185m
- ***Loại cáp dày (thicknet)***
 - Có đường kính khoảng 1.3cm
 - Mang tín hiệu đi xa tới 500m



I. Cáp mạng

2. Cáp xoắn đôi

- Gồm hai sợi dây đồng cách ly quấn vào nhau, có hai loại: Cáp xoán đôi trần (UTP) và Cáp xoán đôi có bọc (STP).
- Cáp xoán đôi sử dụng bộ nối điện thoại RJ-45 để nối tới máy tính

I. Cáp mạng

3. Cáp sợi quang

- Trong cáp sợi quang, sợi quang truyền tín hiệu dữ liệu dạng số ở hình thái xung ánh sáng điều biến. Cáp sợi quang truyền khối lượng dữ liệu với vận tốc rất cao do tín hiệu không bị suy yếu trong quá trình truyền và do độ trong sạch (không bị nhiễu) của tín hiệu.
- Sợi quang gồm một sợi thuỷ tinh cực mảnh, gọi là lõi, được bao quanh bởi một lớp thuỷ tinh đồng tâm gọi là lớp vỏ bọc.

I. Cáp mạng

4. Chọn kiểu đi cáp

- Muốn xác định kiểu đi cáp nào thích hợp nhất cho một địa điểm, người thiết kế đường mạng phải quan tâm đến các vấn đề sau:
 - Lưu lượng truyền trên mạng có nhiều không?
 - Yêu cầu an toàn mạng là gì?
 - Khoảng cách mà mạng phải kéo tới là bao nhiêu?
 - Các chọn lựa cáp là gì?
 - Tiền kéo cáp là bao nhiêu?

I. Cáp mạng

- **Những yêu tố phải quan tâm đến:**

- Tính hợp lý: Cáp có dễ lắp đặt không? Nếu lắp đặt mạng ở phạm vi hẹp, và độ bảo mật không thành vấn đề, không cần phải chọn cáp dày, cồng kềnh và đắt tiền.
- Vỏ bọc bảo vệ: Nếu môi trường có nhiều nhiễu điện thì đường cáp cần có vỏ bọc bảo vệ nhiễu điện.
- Tốc độ truyền: Tuỳ thuộc vào nhu cầu cần thiết mà người thiết kế mạng lựa chọn loại cáp nào để thi công. Nói chung các loại cáp đồng thường có tốc độ chậm khoảng 10Mbps đến 100Mbps.
- Phí tổn: Sự chọn lựa loại cáp tốt, tốc độ truyền cao thường làm cho phí tổn rất lớn.
- Sự suy yếu: Sự suy yếu tín hiệu thường xảy ra khi đường đi cáp quá dài, máy nhận sẽ không hiểu được tín hiệu từ máy truyền tới. Trong trường hợp đó, ta phải thiết lập các hệ thống kích tín hiệu và kiểm tra lỗi.

II. Các thiết bị mạng

1. NIC – Network Interface Card

- Là thiết bị phổ dụng nhất đối với máy tính. Trong NIC có bộ thu phát (Tranceiver) hoạt động như một Transmitter và một Receiver. Transmitter chuyển đổi các tín hiệu bên trong máy tính thành tín hiệu có thể truyền đi được qua đường mạng. Receiver làm ngược lại.

II. Các thiết bị mạng

2. Hub

2.1 HUB bị động (HUB – Passive)

- Không chứa các linh kiện điện tử các xử lý tín hiệu, chỉ có chức năng tổ hợp các tin hiệu từ một số các đoạn mạng. Khoảng cách lớn nhất giữa một máy tính với hub không thể lớn hơn một nửa khoảng cách cho phép giữa 2 máy tính.

2.2 HUB chủ động (HUB – Active)

- Có các linh kiện điện tử có thể khuyếch đại và xử lý tín hiệu. Cho phép khoảng cách giữa các thiết bị tăng lên.

II. Các thiết bị mạng

2.3 HUB thông minh (Intelligent Hub)

- Là hub chủ động nhưng có thêm các chức năng mới sau:
 - Quản trị hub: được bổ sung các giao thức quản trị mạng, cho phép hub gửi các thông tin về trạm điều khiển mạng trung tâm. Và cho phép trạm trung tâm quản lý hub.
 - Chuyển mạch: chứa các vi mạch cho phép chọn đường nhanh cho các tín hiệu giữa các cổng trên hub. Thay vì chuyển gói tin cho toàn bộ các cổng của hub, chúng đang thay thế dần cho các bridge và router.

II. Các thiết bị mạng

3. Repeater (Bộ chuyển tiếp)

- Có chức năng tiếp nhận và chuyển tiếp các tín hiệu dữ liệu, thường được dùng nối 2 đoạn cáp mạng Ethernet để mở rộng mạng. Có khả năng khuếch đại và tái sinh tín hiệu.

cuuduongthancong.com

II. Các thiết bị mạng

4. Bridge (Cầu)

- Là một thiết bị mềm dẻo hơn repeater. Một repeater chuyển đi tất cả các tín hiệu mà nó nhận được. Nhưng Bridge có chọn lọc và chỉ chuyển đi các tín hiệu có đích ở phần mạng phía bên kia.

cuuduongthancong.com

II. Các thiết bị mạng

5. Multiplexor (bộ dồn kênh)

- Là thiết bị có chức năng tổ hợp một số tín hiệu để chúng có thể truyền được với nhau và sau đó khi nhận, lại được tách ra trở lại các tín hiệu gốc.

cuuduongthancong.com

II. Các thiết bị mạng

6. Modem (Modulation/Demodulation)

- Là thiết bị có chức năng chuyển đổi tín hiệu thành tín hiệu tương tự và ngược lại, để kết nối các máy tính qua đường điện thoại.
- Cho phép trao đổi thư điện tử, truyền tệp, truyền fax và trao đổi dữ liệu theo yêu cầu.

cuuduongthancong.com

II. Các thiết bị mạng

7. Router (Bộ chọn đường)

- Là thiết bị thông minh Bridge vì có còn thực hiện các giải thuật chọn đường đi tối ưu cho các gói tin. Bridge hoạt động ở hai tầng Physical và Datalink, trong khi router có thể hoạt động lên tới tầng 3 (Network).
- Cho phép kết nối nhiều mạng với nhau tạo thành liên mạng.

II. Card mạng

Vai trò của card mạng

- Card mạng đóng vai trò như giao diện hoặc kết nối vật lý giữa máy tính và cáp mạng. Có những vai trò sau:
 - Chuẩn bị dữ liệu cho cáp mạng
 - Gửi dữ liệu đến máy tính khác
 - Kiểm soát luồng dữ liệu giữa máy tính và hệ thống cáp

II. Card mạng

1. Chuẩn bị dữ liệu:

- Dữ liệu trước khi truyền đi phải được card mạng chuyển đổi từ dạng mà máy tính có thể hiểu được sang dạng tín hiệu mà có thể gửi được qua cáp mạng. Trên cáp mạng, dữ liệu phải đi theo một luồng bit đơn lẻ. Khi chúng đi trên cáp mạng, các bit được truyền đi nối đuôi nhau, dữ liệu chạy trên cáp chỉ theo một hướng.
- Điều này có nghĩa là: tại mỗi thời điểm, máy tính chỉ có thể hoặc đang nhận dữ liệu, hoặc đang gửi dữ liệu.

II. Card mạng

2. Địa chỉ mạng:

- Bên cạnh việc biến đổi dữ liệu, card mạng còn phải cho biết địa chỉ của nó để phân biệt với các card mạng khác trong mạng. Việc định địa chỉ cho card mạng cho viện công nghệ điện và điện tử (IEEE – Institute of Electrical and Electrics Engineers) quyết định.
- Việc này cung cấp cho mỗi hãng sản xuất một địa chỉ, các hãng sản xuất sẽ nối thêm mã để tích hợp vào từng card mạng. Vì thế tất cả các card mạng trên thế giới đều có địa chỉ khác nhau.

II. Card mạng

3. Gửi và kiểm soát dữ liệu:

- Trước khi gửi dữ liệu, hai card mạng ở hai máy tính đều phải thống nhất với nhau cách thức truyền dữ liệu như: kích thước cụm dữ liệu, lượng dữ liệu được gửi đi, thời gian chờ ngắt quãng giữa các cụm dữ liệu.

cuuduongthancong.com

II. Card mạng

4. *Khả năng tương thích của card mạng*

- Card mạng là một modun được gắn với máy tính, vì thế để máy tính và card mạng có thể làm việc được với nhau, card mạng phải:
 - Vừa vặn với cấu trúc bên trong của máy tính
 - Có bộ nối cáp thích hợp với hệ thống cáp

Mạng máy tính & Hệ thống thông tin công nghiệp

Đào Đức Thịnh
BM Kỹ thuật đo & THCN

Chức năng điều khiển các quá trình

- Điều khiển các quá trình nhiệt độ, áp suất, lưu lượng..Theo một hàm thời gian.
- Các bộ điều khiển tương tự 4-20 mA.
- Các bộ điều khiển lai, số.
- DCS

Chương 1: Các khái niệm cơ bản trong hệ đo & điều khiển Công nghiệp.

- 1.1 Chức năng của một hệ thống đo và điều khiển trong CN
 - 1.1.1 Chức năng điều khiển các quá trình.
 - 1.1.2 Chức năng điều khiển logic, liên động cảnh báo.
 - 1.1.3 Chức năng giao tiếp người và hệ thống.
 - 1.1.4 Chức năng thu thập và quản lý thông tin
- 1.2 Các khái niệm về các hệ và các thiết bị hiện đại trong CN:
 - 1.2.1 Smart Device.
 - 1.2.2 PLC (Programmable Logic Controller).
 - 1.2.3 SCADA (Supervisory Control And Data Acquisition)
 - 1.2.4 DCS(Distributed Control System)

Chức năng điều khiển Logic, liên động, cảnh báo

- Điều khiển logic, liên động các thiết bị , điều khiển tuân tự, cảnh báo.
- Relay cơ điện, Timer, Counter.
- IC số.
- PLC.

Chức năng giao tiếp giữa người và hệ thống

- Người vận hành có thể theo dõi quá trình, điều khiển quá trình, thay đổi Setpoint..
- Panel điều khiển, công tắc, nút ấn, chiết áp.
- Đèn báo, đồng hồ (Analog, digital)
- Giao diện bằng máy tính dựa trên phần mềm HMI

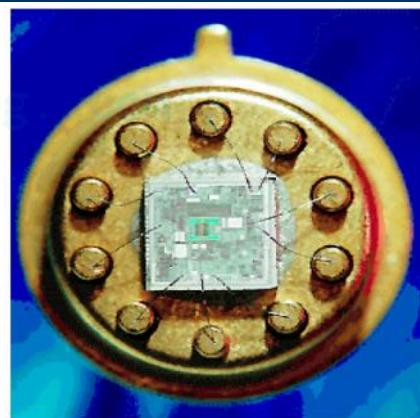
Chức năng thu thập và quản lý thông tin

- Đo, thu thập và quản lý thông tin.
- bằng tay (thủ công).
- Các đồng hồ tự ghi, relay tự rơi, recorder.
- Sử dụng máy tính.

Smart Device

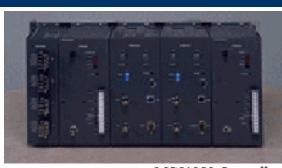
- Thiết bị số trên cơ sở uP có khả năng xử lý thông tin.
- Hiển thị tại chỗ hay từ xa.
- Mềm dẻo, kinh tế.
- Có khả năng tự động kiểm tra, chuẩn đoán.

Smart Device



PLC (Programmable Logic Controller)

Thiết bị điều khiển khả trình (PLC, programmable logic controller) là một loại máy tính điều khiển chuyên dụng, do nhà phát minh người Mỹ Richard Morley lần đầu tiên đưa ra ý tưởng vào năm 1968. Dựa trên yêu cầu kỹ thuật của General Motors là xây dựng một thiết bị có khả năng lập trình mềm dẻo thay thế cho mạch điều khiển logic cứng, hai công ty độc lập là Allen Bradley và Bedford Associates (sau này là Modicon) đã đưa ra trình bày các sản phẩm đầu tiên. Các thiết bị này chỉ xử lý được một tập lệnh logic cơ bản, 128 điểm vào/ra (1 bit) và 1kByte bộ nhớ.



21x CPUs
S7-200 Quick Reference Information



PLC (Programmable Logic Controller)

- Thiết bị số trên cơ sở uP
- Phát triển để thay thế cho Relay, Timer....
- Sử dụng để điều khiển quá trình, liên động với các đầu I/O số.
- Chương trình viết bằng ngôn ngữ Ladder Logic.

SCADA (Supervisory Control And Data Acquisition)

- Điều khiển giám sát (và thu thập dữ liệu)
- Hỗ trợ con người trong việc quan sát và điều khiển từ xa
- Có giao diện người-máy
- HMI (Human-Machine Interface) - Giao diện người-máy
 - + Thành phần trong một hệ SCADA, hoặc
 - + Các phương tiện quan sát/thao tác ở cấp thấp hơn
- Các trạm điều khiển giám sát trung tâm
 - + Engineering Station (ES)
 - + Operator Station (OS)
 - + Server Station (SS)

SCADA (Supervisory Control And Data Acquisition)

- Các trạm thu thập dữ liệu trung gian
 - + Remote Terminal Unit (RTU)
 - + Data Collection Unit (DCU): PLC, PC, I/O
- Hệ thống truyền thông
 - + Mạng truyền thông công nghiệp
 - + Mạng viễn thông/truyền dữ liệu đường dài (vô tuyến, huu tuyến)
 - + Các thiết bị chuyển đổi, dồn kênh (Modem, Multiplexer)

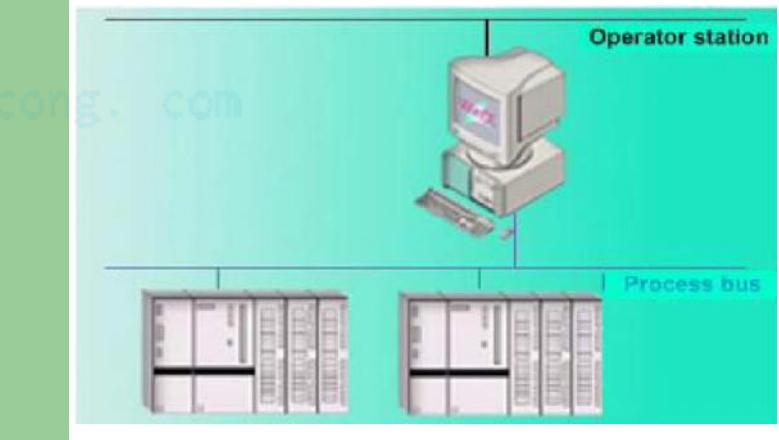
SCADA (Supervisory Control And Data Acquisition)

- Các công cụ phát triển ứng dụng
 - *Giao diện người-máy (HMI)
 - +Sơ đồ hệ thống, sơ đồ công nghệ
 - +Hiển thị các biến quá trình qua các "thiết bị áo"
 - +Đồ thị thời gian thực, đồ thị dữ liệu tĩnh
 - + Các phím thao tác, nút điều khiển (controls)
 - * Hỗ trợ trao đổi tin tức (Messaging), xử lý sự kiện (Event), sự cố (Alarm)
 - * Hỗ trợ việc thống kê và lập báo cáo (Reporting)

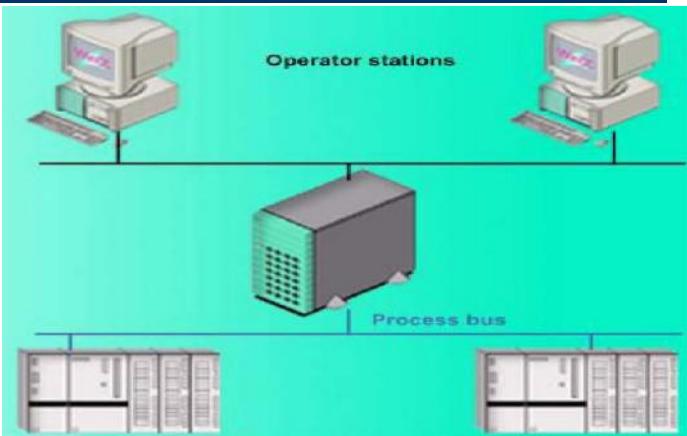
SCADA (Supervisory Control And Data Acquisition)

- * Phần mềm kết nối với các nguồn dữ liệu (drivers cho các PLC, các module vào/ra, cho các hệ thống bus trường)
- * Cơ sở dữ liệu quá trình, dữ liệu cấu hình hệ thống

Hệ một người dùng



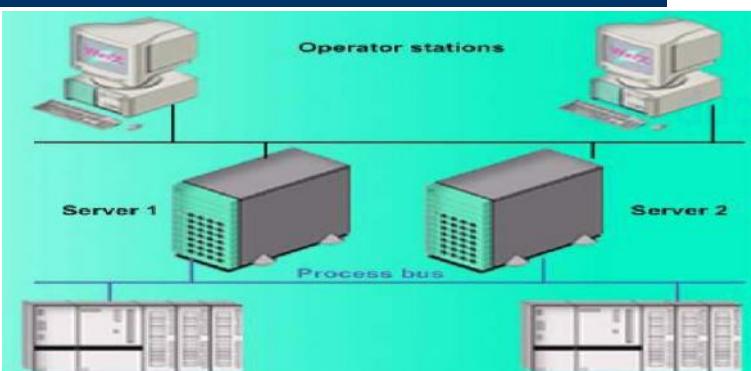
Hệ nhiều người dùng



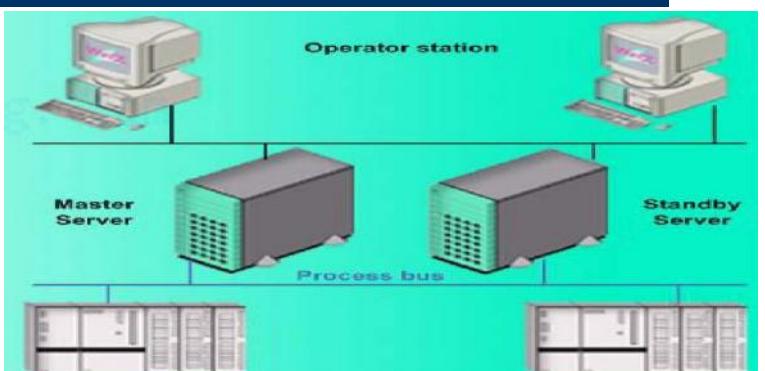
Hệ Web Client



Hệ phân tán



Hệ chạy dự phòng



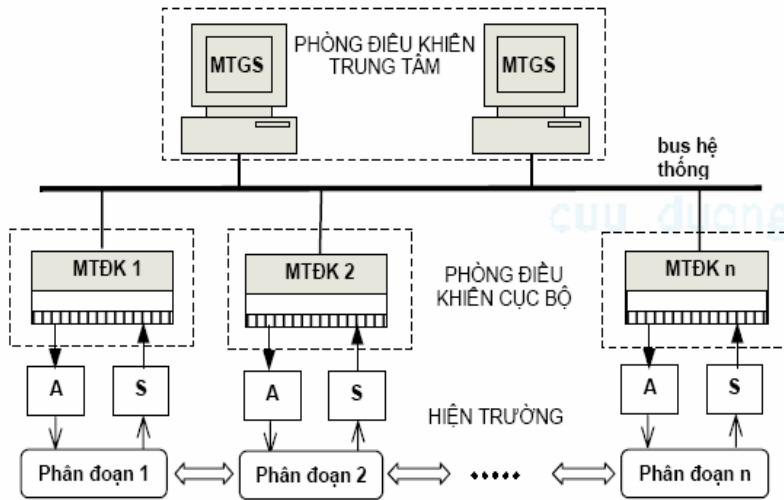
Communication



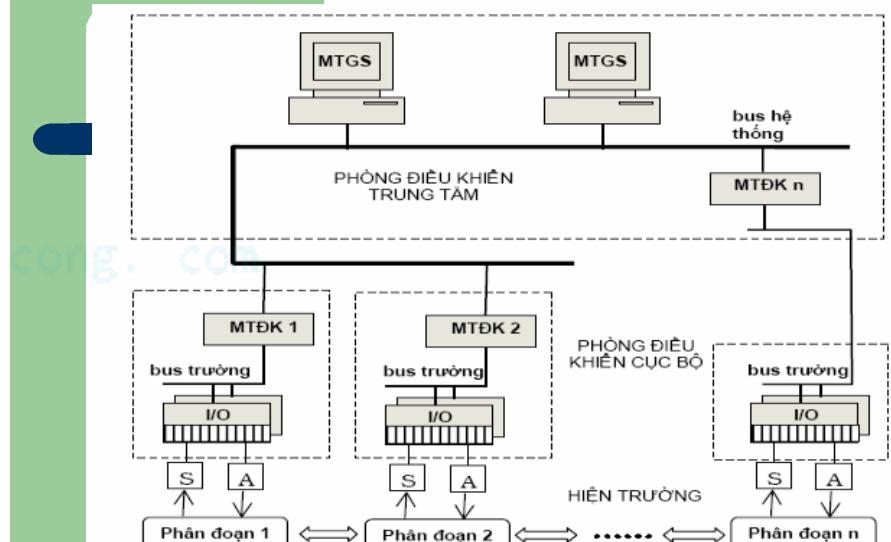
DCS (Distributed Control System)

- Các thiết bị điều khiển số + Phần cứng phần mềm thu thập thông tin.
- Đường truyền tốc độ cao.
- Các module bố trí phân tán.
- Mỗi Module thực hiện một chức năng riêng.
- Có giao diện để nối các máy tính điều khiển giám sát và các bộ điều khiển.

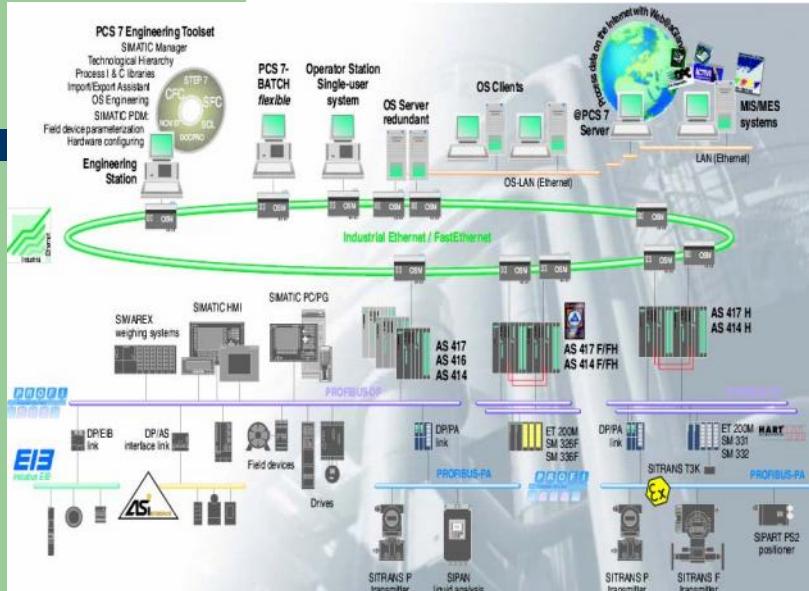
DCS (Distributed Control System)



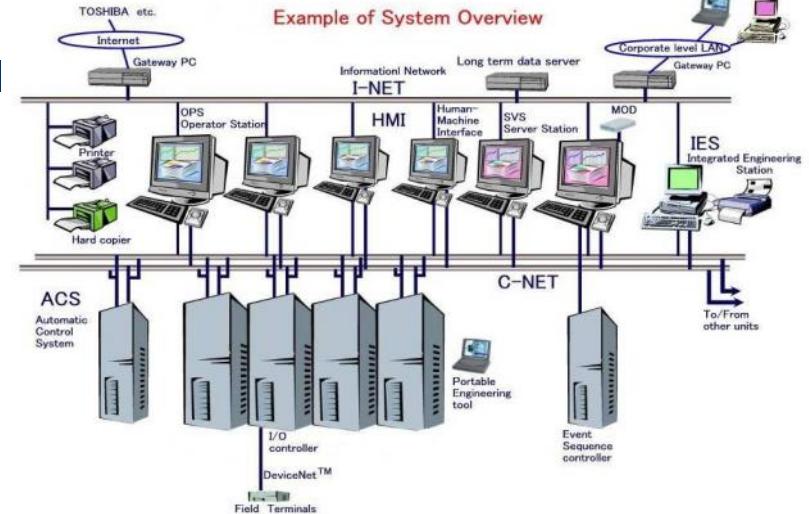
DCS (Distributed Control System)



DCS (Distributed Control System)



DCS (Distributed Control System)



DCS (Distributed Control System)

DCS Truyền thống.

- Các hệ này sử dụng các bộ điều khiển quá trình đặc chủng theo kiến trúc riêng của nhà sản xuất.
- Các hệ cũ thường đóng kín, ít tuân theo các chuẩn giao tiếp công nghiệp, các bộ điều khiển được sử dụng cũng thường chỉ làm nhiệm vụ điều khiển quá trình, vì vậy phải sử dụng kết hợp PLC cho các bài toán điều khiển logic và điều khiển trình tự.
- Các hệ mới có tính năng mở tốt hơn, một số bộ điều khiển lai đảm nhiệm cả các chức năng điều khiển quá trình, điều khiển trình tự và điều khiển logic (hybrid controller).

DCS (Distributed Control System)

- Để hỗ trợ các bài toán điều khiển quá trình diễn ra đồng thời, khối xử lý trung tâm được cài đặt một hệ điều hành thời gian thực, đa nhiệm - hoặc của riêng nhà sản xuất phát triển hoặc một sản phẩm thông dụng như pSOS, TSOS, VRTX,... Chu kỳ thời gian nhỏ nhất thực hiện các mạch vòng điều khiển thường nằm trong khoảng 10-100ms, trong trường hợp đặc biệt (ví dụ cho nhà máy điện) có thể tới 1ms.

DCS (Distributed Control System)

- Một số sản phẩm tiêu biểu cùng với tên trạm điều khiển cục bộ được liệt kê dưới đây:
 - AdvantOCS (ABB): Advant Controller, hệ điều hành riêng
 - Freelance 2000 (ABB): D-PS học D-FC, hệ điều hành pSOS
 - DeltaV (Fisher-Rosemount): Visual Controller, hệ điều hành TSOS
 - PlantScape (Honeywell): PlantScape Controller, hệ điều hành riêng
 - Centum CS1000/CS3000 (Yokogawa): PFCx-E, AFS10x/AFS20x, hệ điều hành ORKID

DCS (Distributed Control System)

DSC trên nền PLC

Một số hệ DCS trên nền PLC tiêu biểu là SattLine (ABB), Process Logix (Rockwell), Modicon TSX (Schneider Electric), PCS7 (Siemens),... Thực chất, ngày nay đa số các PLC vừa có thể sử dụng cho bài toán điều khiển logic và điều khiển quá trình. Tuy nhiên, các PLC được sử dụng trong các hệ điều khiển phân tán thường có cấu hình mạnh, hỗ trợ điều khiển trình tự cùng với các phương pháp lập trình hiện đại (ví dụ SFC).

DCS (Distributed Control System)

DSC trên nền PC

Giải pháp sử dụng máy tính cá nhân (PC) trực tiếp làm thiết bị điều khiển không những được bàn tới rộng rãi, mà đã trở thành thực tế phổ biến trong những năm gần đây. Nếu so sánh với các bộ điều khiển khả trình (PLC) và các bộ điều khiển DCS đặc chung thì thế mạnh của PC không những nằm ở tính năng mở, khả năng lập trình tự do, hiệu năng tính toán cao và đa chức năng, mà còn ở khía cạnh kinh tế. Các bước tiến lớn trong kỹ thuật máy tính, công nghiệp phần mềm và công nghệ bus trường chính là các yếu tố thúc đẩy khả năng cạnh tranh của PC trong điều khiển công nghiệp.

DCS (Distributed Control System)

DCS trên nền PC là một hướng giải pháp tương đối mới, mới có một số sản phẩm trên thị trường như PCS7 (Siemens, giải pháp Slot-PLC), 4Control (Softing), Stardom (Yokogawa), Ovation (Westinghouse-Emerson Process Management)... Hướng giải pháp này thể hiện nhiều ưu điểm về mặt giá thành, hiệu năng tính toán và tính năng mở. Một trạm điều khiển cục bộ chính là một máy tính cá nhân công nghiệp được cài đặt một hệ điều hành thời gian thực và các card giao diện bus trường và card giao diện bus hệ thống.

Mạng máy tính & Hệ thống thông tin công nghiệp

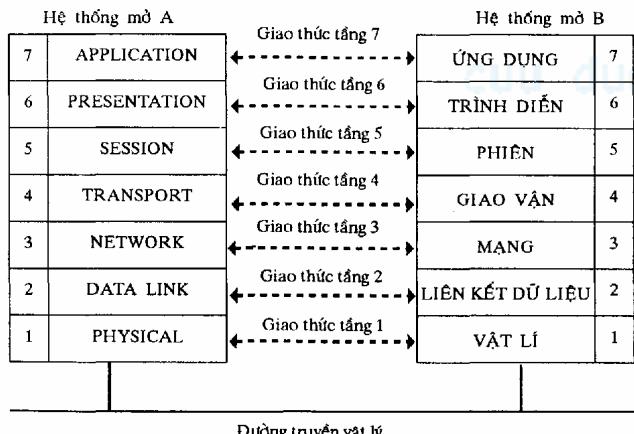
Đào Đức Thịnh
BM Kỹ thuật đo & THCN

Thế nào là hệ kín, hệ mở,mô tả chung về OSJ

- Mạng mà chỉ có thiết bị của một nhà sản xuất và nó làm việc với phần cứng và giao thức đặc biệt gọi là hệ kín.
- Hệ mở được thiết kế theo nguyên tắc mở cho tất cả, nó cho phép tất cả các thiết bị phù hợp với chuẩn thì có thể tham gia vào mạng chuẩn

cuuduongthancong.com

Thế nào là hệ kín, hệ mở,mô tả chung về OSJ



Thế nào là hệ kín, hệ mở,mô tả chung về OSJ

Mô hình hệ mở có thể coi như là tập hợp của các thực thể (chương trình phần mềm và mạch phần cứng) đặt trong các lớp. Các thực thể trong cùng một lớp nhưng ở các nút khác nhau gọi là thực thể tương đương. Các thực thể chỉ có thể thông tin với thực thể tương đương trong hệ khác. Mặc dù các thực thể tương đương có thể thông tin với nhau nhưng số liệu thực sự cần phải đi qua các lớp bên dưới trong hệ truyền và đi theo chiều ngược lại trong hệ nhận.

Lớp vật lý

Theo định nghĩa của ISO, tầng vật lý định nghĩa các thông số điện, cơ, các chức năng, thủ tục để kích hoạt, duy trì và đình chỉ liên kết vây lý giữa các hệ thống. Thuộc tính điện, cơ:

- Cấu trúc mạng (dạng vòng, dạng sao, dạng Bus....).
- Định nghĩa khía cạnh dòng điện, điện áp biểu diễn các bit.
- Kỹ thuật điều chế tín hiệu sử dụng trong mạng.
- Định nghĩa về mặt cơ học của kết nối (kiểu đầu nối, chân tín hiệu, kiểu cáp).

Lớp liên kết dữ liệu

Tầng Liên kết dữ liệu 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.

- Định nghĩa giao thức cần phải tuân theo cho việc truy nhập mạng để truyền và nhận bản tin.
- Chia một khối lớn thông tin ra thành các khung định dạng nhỏ hơn (Framming).
- Trả lời các thông tin đã nhận được (thông tin đồng bộ hóa, kiểm soát lỗi, kiểm soát luồng dữ liệu).

Lớp liên kết dữ liệu

* DLP *dị bộ*: Các DLP *dị bộ* sử dụng phương thức truyền *dị bộ*, trong đó 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. Phương thức này được gọi là *dị bộ* là vì không cần có sự đồng bộ liên tục giữa người gửi và người nhận tin. Nó cho phép một ký tự dữ liệu được truyền đi bất kỳ lúc nào mà không cần quan tâm đến các tín hiệu đồng bộ trước đó.

Lớp liên kết dữ liệu

* DLP *đồng bộ*: Phương thức truyền đồng bộ không dùng các bit đặc biệt START, STOP để đóng khung mỗi ký tự mà 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 người sử dụng để báo hiệu cho người nhận biết được dữ liệu "đang đến" hoặc "đã đến". Cần lưu ý rằng các hệ thống truyền thông đòi hỏi hai mức đồng bộ hóa :

- ở mức vật lý : để giữ đồng bộ giữa các đồng hồ của người gửi và người nhận.
- ở mức liên kết dữ liệu : để phân biệt dữ liệu của người sử dụng với các "cờ" và các vùng thông tin điều khiển khác.

Lớp vận chuyển

Các nhiệm vụ cụ thể của lớp vận chuyển bao gồm:

- Quản lý về tên hình thức cho các trạm sử dụng
- Định vị các đối tác truyền thông qua tên hình thức và/hoặc địa chỉ
- Xử lý lỗi và kiểm soát dòng thông tin, trong đó có cả việc lập lại quan hệ liên kết và thực hiện các thủ tục gửi lại dữ liệu khi cần thiết
- Dồn kênh các nguồn dữ liệu khác nhau
- Đồng bộ hóa giữa các trạm đối tác.

Để thực hiện việc vận chuyển một cách hiệu quả, tin cậy, một dữ liệu cần chuyển đi có thể được chia thành nhiều đơn vị vận chuyển (*data segment unit*) có đánh số thứ tự kiểm soát trước khi bổ sung các thông tin kiểm soát lưu thông.

Lớp phiên

Tầng phiên (Session) là tầng thấp nhất trong nhóm các tầng cao và nằm ở ranh giới giữa hai nhóm tầng nói trên. Mục tiêu của nó là cung cấp cho người sử dụng cuối các chức năng cần thiết để quản trị các *phiên 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 hộp *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 quá trình trao đổi dữ liệu.

Lớp biểu diễn

Mục đích của tầng Trình diễn (Presentation layer) 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.

Lớp ứng dụng

Bên cạnh truyền tải thông tin, lớp ứng dụng còn cung cấp các dịch vụ như sau:

- Nhận dạng các chủ thể tham gia thông tin qua tên và địa chỉ
- Xác định khả năng hiện hành của một chủ thể tham gia thông tin
- Thiết lập thẩm quyền thông tin
- Thống nhất cơ cấu bảo mật
- Cấp quyền cho các chủ thể tham gia thông tin
- Chọn qui tắc đàm thoại, bao gồm các thủ tục khởi tạo và xóa bỏ
- Thống nhất trách nhiệm khắc phục lỗi
- Xác nhận các ràng buộc trên cú pháp dữ liệu (các tập ký tự, các cấu trúc dữ liệu..)

Mô hình hệ mở đơn giản

- Application.
- Data Link.
- Physical.

Mô hình hệ mở đơn giản

Khi giảm mô hình thì việc thực hiện sẽ có các giới hạn sau:

- Kích thước lớn nhất của bản tin sẽ bị giới hạn bởi kích thước kênh truyền (Transport).
- Không thể định tuyến bản tin giữa các mạng (Network).
- Chỉ cho phép thông tin Full-duplex (Session)
- Định dạng của bản tin phải như nhau ở mọi nút (Presentation).

Mạng máy tính & Hệ thống thông tin công nghiệp

Đào Đức Thịnh
Bộ Kỹ thuật đo & THCN

Chương 2: Các giao thức công nghiệp

2.3 ModBus:

- Mô tả chung về giao thức.
- Hai chế độ truyền ASCII và RTU.
- Khung bản tin của ModBus.
- Các phương pháp kiểm tra lỗi.
- Dữ liệu và các chức năng điều khiển.
- Các hàm phụ chuẩn đoán trong mạng.
- Báo lỗi.

Chương 2: Các giao thức công nghiệp

2.1 Khái niệm về giao thức:

- Giao thức ?
- Các đặc điểm quan trọng của giao thức.

2.2 Các yêu cầu riêng cho giao thức CN.

Giao thức (Protocol)

- Giao thức thiết lập một tiêu chuẩn chung cho việc trao dữ liệu giữa phần thu và phát trên mạng.
- Nó thường kết hợp với gói tin.
- Giao thức điều khiển một khung bản tin chung cho tất cả các thiết bị trên mạng.
- Giao thức thiết lập hoạt động đúng cho hệ thống tin

Giao thức (Protocol)

Các đặc điểm của giao thức:

- Khởi động: Khởi động các thông số của giao thức để bắt đầu truyền số liệu qua kênh liên lạc.
- Tạo khung và đồng bộ khung.
- Điều khiển luồng dữ liệu.
- Điều khiển truy nhập đường truyền.
- Phát hiện và sửa lỗi.
- Kiểm soát Time-out.

Các yêu cầu riêng cho giao thức CN

- Đơn giản nhất có thể để dễ khắc phục sự cố:

- + CN là nơi có sự hiểu biết về mạng thông tin CN ít.
- + Đòi hỏi hoạt động liên tục.
- + Có ý thức lựa chọn giao thức đơn giản nhất có thể.

- Độ đảm bảo dữ liệu truyền cao:

- + Hoạt động trong môi trường có nhiễu điện lớn.
- + Các thiết bị công suất lớn tập trung với mật độ cao.
- + Đòi hỏi không có lỗi khi truyền.
- + Chọn giao thức có mức độ cao của việc kiểm tra lỗi.

Các yêu cầu riêng cho giao thức CN

- Chuẩn hoá giao thức:

- + Có thể có nhu cầu cho việc kết nối giữa các thiết bị của các nhà SX khác nhau hay các hệ khác nhau.
- + Cần phải chuẩn hoá giao thức.

- Tốc độ cập nhật thông số cao:

- + Không đòi hỏi số lượng thông số lớn.
- + Yêu cầu cập nhật một loạt các setpoint cho một loạt các thiết bị gần như đồng thời.
- + Một số giao thức Field Bus mới có thể đáp ứng yêu cầu này.

Modbus

Mô tả chung về Modbus:

- + Modbus được phát triển bởi Modicon (AEG) cho hệ thống điều khiển các quá trình

ModBus

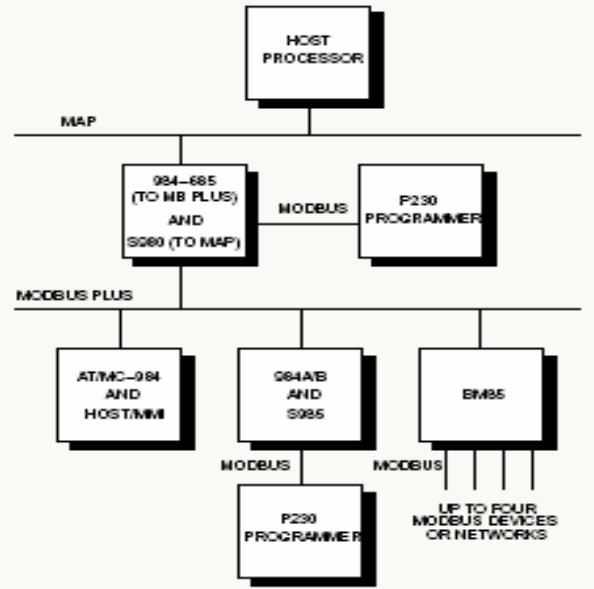


Figure 1 Overview of Modbus Protocol Application

ModBus

- + Master có thể địa chỉ từng Slave riêng hay gửi một bản tin quảng bá tới tất cả các Slave.
- + Khi có yêu cầu bởi địa chỉ riêng thì sẽ có bản tin trả lời. Không có bản tin trả lời với yêu cầu quảng bá.
- + Modbus cung cấp một định dạng khung bản tin chung cho các bản tin truyền giữa Master và Slave. Bản tin bao gồm địa chỉ của thiết bị, mã chức năng định nghĩa các hoạt động yêu cầu, số liệu cần gửi và trường kiểm tra lỗi.
- + Slave trả lời bằng một bản tin nó chính là kết quả của hoạt động. Nếu có lỗi thì nó cũng báo lỗi nào đã xảy ra.

ModBus

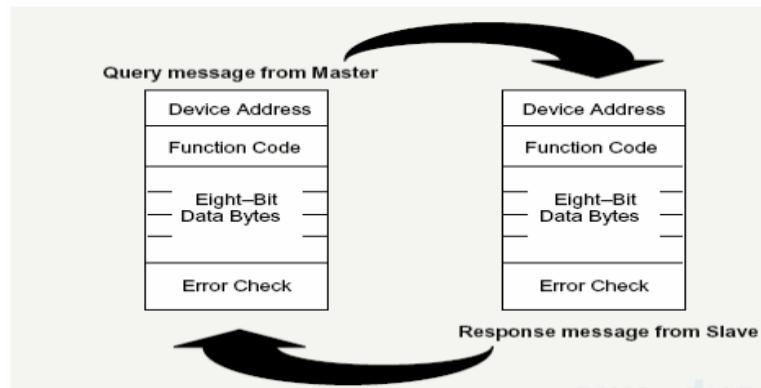
- + Modbus chuẩn của bộ điều khiển Modicon sử dụng cổng RS-232. Bộ điều khiển có thể nối mạng trực tiếp hay qua Modem.
- + Người dùng có thể lựa chọn các chuẩn RS-422, RS-485, 20mA Current loop, tất cả các chuẩn trên đều tương thích với tốc độ truyền của giao thức.
- + Thông tin giữa các bộ điều khiển sử dụng kỹ thuật Master-Slave. Chỉ có Master mới có quyền khởi động việc truyền dữ liệu, các thiết bị khác là Slave trả lời bằng cách cung cấp các dữ liệu được yêu cầu từ Master hoặc đáp lại các hoạt động.
- + Master có thể là các máy chủ, PC hay các Panel lập trình.
- + Slave là các bộ điều khiển có tối đa 247 Slave.

ModBus

- + Ngoài ra các bộ điều khiển Modbus có thể thông tin trên Modbus Plus sử dụng cổng thông tin có sẵn hay cộng mạng và truyền trên MAP.
- + ở đây thông tin giữa các bộ điều khiển dùng kỹ thuật Peer-Peer.(Ứng dụng vẫn là Master-Slave).

ModBus

The Query–Response Cycle



ModBus - ASCII Mode

- + Khi các bộ điều khiển sử dụng chế độ ASCII mỗi một byte-8bits truyền như là 2 ký tự ASCII.
- + Ưu điểm chính là cho thời gian truyền giữa các ký tự lên đến 1s mà không gây ra lỗi
- + Mã: Hexadecimal, ASCII 0-9,A-F. 1 Hexa ->ASCII
- + Bit trên ký tự: 1 Start bit; 7 data bit; 1,0 Parity bit; 1,2 Stop bit (10 bit).
- + Kiểm tra lỗi: LRC

ModBus - Hai chế độ truyền

- + Bộ điều khiển trên mạng Modbus có thể truyền ở hai chế độ: ASCII và RTU.
- + Ta có thể chọn chế độ truyền cũng như các thông số của cổng thông tin nhưng nó phải như nhau ở tất cả các bộ điều khiển.

ModBus - RTU Mode

- + Khi các bộ điều khiển hoạt động ở chế độ RTU mỗi một Byte-8bit gửi như là hai số Hexadecimal -4 bit.
- + Ưu điểm của phương pháp này là có mật độ ký tự lớn cho phép truyền tốt hơn chế độ ASCII với cùng một tốc độ bit.
- + Mỗi một bản tin cần phải truyền thành một chuỗi liên tục.
- + Mã: 8 bit, Hexa 0-9,A-F. Hai số Hexa chứa trong một trường 8 bit.
- + Số bit trên Byte: 1 Start bit; 8 data bit; 1,0 Parity bit; 1,2 Stop bit (11 bit).
- + Kiểm tra lỗi: CRC

ModBus - Cấu trúc khung bản tin

- + Trong cả hai chế độ truyền bản tin Modbus được bên phát đặt trong một khung có điểm bắt đầu, kết thúc.
- + Bên thu nhận bản tin định vị các trường khác và phát hiện ra lỗi có trong bản tin.
- + Có hai chế độ truyền có hai kiểu khung bản tin

ModBus - ASCII Frame

START	ADDRESS	FUNCTION	DATA	LRC CHECK	END
1 CHAR :	2 CHARS	2 CHARS	n CHARS	2 CHARS	2 CHARS CRLF

ModBus - ASCII Frame

- + Tất cả các thiết bị nối vào mạng sẽ kiểm tra bus liên tục cho đến khi nhận được ký tự '!'. Nó sẽ giải mã trường địa chỉ. Nếu gửi cho nó thì nó nhận và xử lý các trường tiết theo.
- + Thời gian cho phép giữa các ký tự có thể lên đến 1 s-> không gây ra lỗi.

ModBus - RTU Frame

START	ADDRESS	FUNCTION	DATA	CRC CHECK	END
T1-T2-T3-T4	8 BITS	8 BITS	n×8 BITS	16 BITS	T1-T2-T3-T4

ModBus - RTU Frame

- + Các thiết bị nối vào mạng sẽ kiểm tra bus trong suốt quá trình rối của bus. Trường đầu tiên nhận được sẽ là trường địa chỉ và nó sẽ so sánh với địa chỉ của nó.
- + Nếu thời gian nghỉ > 3.5 lần thời gian truyền 1 byte thì kết thúc bản tin.

ModBus - Cấu trúc khung bản tin

Trường địa chỉ:

- + Chứa 2 ký tự ASCII hay 8 bit.
- + Giá trị từ 0-247.
- + Từng Slave địa chỉ hóa từ 1-247.
- + Master địa chỉ hóa Slave bằng cách đặt địa chỉ của nó vào trường địa chỉ.
- + Slave trả lời báo cho Master biết Slave nào đã trả lời.
- + Địa chỉ 0 sử dụng ở chế độ quảng bá.

ModBus - Cấu trúc khung bản tin

Trường chức năng:

- + Bao gồm 2 ký tự ASCII hay 1 byte.
- + Giá trị từ 1-255.
- + Một vài mã áp dụng cho các bộ điều khiển. Một vài mã chỉ áp dụng cho một mô hình nào đó. Một số dành cho tương lai.
- + Master->Slave chỉ ra Slave phải làm gì?
- + Slave->Master báo là hoạt động bình thường hay báo lỗi. Nếu bình thường thì phản hồi về mã chức năng ban đầu. Nếu có lỗi thì phản hồi về mã chức năng ban đầu với bit cao nhất bằng 1.

ModBus - Cấu trúc khung bản tin

Trường dữ liệu:

- Master->Slave các dữ liệu cần cho hoạt động được định nghĩa bởi mã chức năng.
- Slave->Master nếu không có lỗi nó chứa các dữ liệu trả về. Nếu có lỗi nó chứa mã lỗi.
- Trường dữ liệu có thể không có trong một số bản tin.

ModBus - Cấu trúc khung bản tin

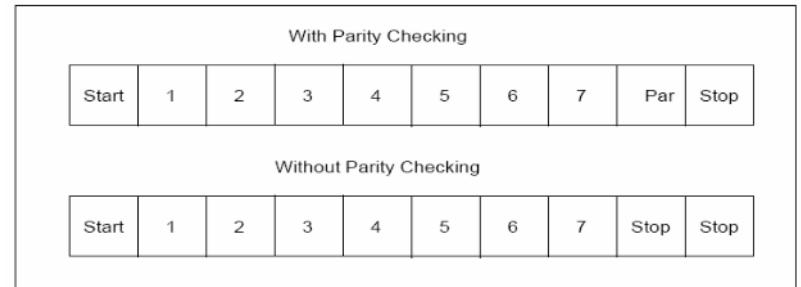
Kiểm tra lỗi:

- + ASCII mode: kết quả kiểm tra theo LRC -> 1byte -> 2 ký tự ASCII.
- + RTU mode: kiểm tra theo PP CRC nội dung bản tin. 16 bit -> 2 byte

ModBus - Cấu trúc khung bản tin

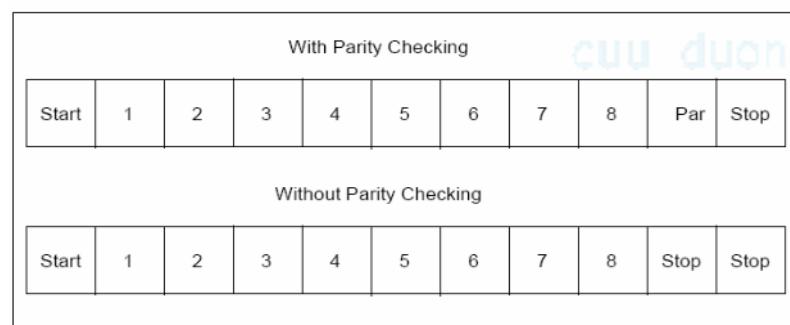
- Khi truyền ở chế độ Modbus chuẩn các ký tự hay các byte được truyền các bit thấp trước, cao sau.

With ASCII character framing, the bit sequence is:



ModBus - Cấu trúc khung bản tin

With RTU character framing, the bit sequence is:



ModBus - Các phương pháp kiểm tra lỗi

- Modbus chuẩn được áp dụng hai phương pháp kiểm tra lỗi. Kiểm tra chẵn lẻ áp dụng cho từng ký tự. Kiểm tra khung (LRC, CRC) được áp dụng cho toàn bộ khung bản tin.

- Cả hai phương pháp này sẽ được Master thực hiện trước khi truyền khung bản tin và được Slave kiểm tra trong quá trình nhận bản tin.

- Nếu Slave phát hiện ra lỗi trong bản tin thì bản tin sẽ bị bỏ đi, không có đáp ứng cho Master. Master đợi quá thời gian Time-out để bỏ quá trình truyền. Thời gian Time-out đủ lớn để cho bất kỳ Slave nào có thể trả lời bình thường được. Như vậy khi Time-out chương trình ứng dụng trên Master biết có một lỗi xảy ra.

ModBus - Các phương pháp kiểm tra lỗi

Kiểm tra chẵn lẻ:

- Ta có thể đặt là kiểm tra chẵn, kiểm tra lẻ hay không kiểm tra chẵn lẻ.
- Khi truyền các bit chẵn lẻ sẽ được tính toán và truyền cùng với ký tự. Bên thu sẽ kiểm tra lại. Tất cả các thiết bị phải dùng chung một phương pháp.

ModBus - Các phương pháp kiểm tra lỗi

Kiểm tra LRC:

Kiểm tra CRC:

ModBus - Các chức năng của Modbus

Modbus cung cấp một loạt các chức năng sau:

Code	Name	384	484	584	884	M84	984
01	Read Coil Status	Y	Y	Y	Y	Y	Y
02	Read Input Status	Y	Y	Y	Y	Y	Y
03	Read Holding Registers	Y	Y	Y	Y	Y	Y
04	Read Input Registers	Y	Y	Y	Y	Y	Y
05	Force Single Coil	Y	Y	Y	Y	Y	Y
06	Preset Single Register	Y	Y	Y	Y	Y	Y
07	Read Exception Status	Y	Y	Y	Y	Y	Y
08	Diagnostics (see Chapter 3)						

ModBus - Các chức năng của Modbus

09	Program 484	N	Y	N	N	N	N
10	Poll 484	N	Y	N	N	N	N
11	Fetch Comm. Event Ctr.	Y	N	Y	N	N	Y
12	Fetch Comm. Event Log	Y	N	Y	N	N	Y
13	Program Controller	Y	N	Y	N	N	Y
14	Poll Controller	Y	N	Y	N	N	Y
15	Force Multiple Coils	Y	Y	Y	Y	Y	Y
16	Preset Multiple Registers	Y	Y	Y	Y	Y	Y
17	Report Slave ID	Y	Y	Y	Y	Y	Y
18	Program 884/M84	N	N	N	Y	Y	N
19	Reset Comm. Link	N	N	N	Y	Y	N
20	Read General Reference	N	N	Y	N	N	Y
21	Write General Reference	N	N	Y	N	N	Y

ModBus - Các chức năng của Modbus

Code	Name	384	484	584	884	M84	984
22	Mask Write 4X Register	N	N	N	N	N	(1)
23	Read/Write 4X Registers	N	N	N	N	N	(1)
24	Read FIFO Queue	N	N	N	N	N	(1)

ModBus - Các chức năng của Modbus

QUERY		ASCII Characters	RTU 8-Bit Field
Field Name	Example (Hex)		
Header		:	(colon)
Slave Address	06	0 6	0000 0110
Function	03	0 3	0000 0011
Starting Address Hi	00	0 0	0000 0000
Starting Address Lo	6B	6 B	0110 1011
No. of Registers Hi	00	0 0	0000 0000
No. of Registers Lo	03	0 3	0000 0011
Error Check		LRC (2 chars.)	CRC (16 bits)
Trailer		CR LF	None
Total Bytes:		17	8

ModBus - Các chức năng của Modbus

RESPONSE			
Field Name	Example (Hex)	ASCII Characters	RTU 8-Bit Field
Header		:	(colon)
Slave Address	06	0 6	0000 0110
Function	03	0 3	0000 0011
Byte Count	06	0 6	0000 0110
Data Hi	02	0 2	0000 0010
Data Lo	2B	2 B	0010 1011
Data Hi	00	0 0	0000 0000
Data Lo	00	0 0	0000 0000
Data Hi	00	0 0	0000 0000
Data Lo	63	6 3	0110 0011
Error Check		LRC (2 chars.)	CRC (16 bits)
Trailer		CR LF	None
Total Bytes:		23	11

ModBus - Các kiểu dữ liệu của Modbus

- Modbus sử dụng 4 kiểu dữ liệu khác nhau:
 - + Đầu vào số.
 - + Đầu ra số (Coil).
 - + Thanh ghi vào (Input Register).
 - + Thanh ghi giữ (Holding Register)
- Các biến đầu vào và ra số là 1 bit.
- Các biến thanh ghi là 2 byte.
- Mỗi một chức năng gắn liền với một kiểu dữ liệu.
- Địa chỉ mà khung bản tin sử dụng là địa chỉ offset tương đối với địa chỉ thấp nhất của kiểu dữ liệu.

ModBus -Mô tả chi tiết các mã chức năng

QUERY

Field Name	Example (Hex)
Slave Address	11
Function	01
Starting Address Hi	00
Starting Address Lo	13
No. of Points Hi	00
No. of Points Lo	25
Error Check (LRC or CRC)	—

ModBus -Mô tả chi tiết các mã chức năng

RESPONSE

Field Name	Example (Hex)
Slave Address	11
Function	01
Byte Count	05
Data (Coils 27–20)	CD
Data (Coils 35–28)	6B
Data (Coils 43–36)	B2
Data (Coils 51–44)	0E
Data (Coils 56–52)	1B
Error Check (LRC or CRC)	—

ModBus -Mô tả chi tiết các mã chức năng

QUERY

Field Name	Example (Hex)
Slave Address	11
Function	02
Starting Address Hi	00
Starting Address Lo	C4
No. of Points Hi	00
No. of Points Lo	16
Error Check (LRC or CRC)	—

ModBus -Mô tả chi tiết các mã chức năng

RESPONSE

Field Name	Example (Hex)
Slave Address	11
Function	02
Byte Count	03
Data (Inputs 10204–10197)	AC
Data (Inputs 10212–10205)	DB
Data (Inputs 10218–10213)	35
Error Check (LRC or CRC)	—

ModBus -Mô tả chi tiết các mã chức năng

QUERY	
Field Name	Example (Hex)
Slave Address	11
Function	05
Coil Address Hi	00
Coil Address Lo	AC
Force Data Hi	FF
Force Data Lo	00
Error Check (LRC or CRC)	—

ModBus -Mô tả chi tiết các mã chức năng

RESPONSE	
Field Name	Example (Hex)
Slave Address	11
Function	05
Coil Address Hi	00
Coil Address Lo	AC
Force Data Hi	FF
Force Data Lo	00
Error Check (LRC or CRC)	—

ModBus -Function 08 Diagnostics

QUERY	
Field Name	Example (Hex)
Slave Address	11
Function	08
Subfunction Hi	00
Subfunction Lo	00
Data Hi	A5
Data Lo	37
Error Check (LRC or CRC)	—

ModBus -Function 08 Diagnostics

RESPONSE	
Field Name	Example (Hex)
Slave Address	11
Function	08
Subfunction Hi	00
Subfunction Lo	00
Data Hi	A5
Data Lo	37
Error Check (LRC or CRC)	—

ModBus -Function 08 Diagnostics

Code	Name	384	484	584	884	M84	984
00	Return Query Data	Y	Y	Y	Y	Y	Y
01	Restart Comm Option	Y	Y	Y	Y	Y	Y
02	Return Diagnostic Register	Y	Y	Y	Y	Y	Y
03	Change ASCII Input Delimiter	Y	Y	Y	N	N	Y
04	Force Listen Only Mode	Y	Y	Y	Y	Y	Y
05-09	Reserved						
10	Clear Ctrs and Diagnostic Reg.	Y	Y	(1)	N	N	(1)
11	Return Bus Message Count	Y	Y	Y	N	N	Y
12	Return Bus Comm. Error Count	Y	Y	Y	N	N	Y

cuuduongthancong.com

ModBus -Trả lời báo lỗi

Ngoại trừ bản tin quảng bá. Khi Master gửi một bản tin trả lời Slave thì có 4 trường hợp có thể xảy ra:

- + Slave nhận bản tin không có lỗi và có thể trả lời bản tin. Trả lời thường.

- + Nếu Slave không nhận được bản tin hỏi vì lỗi thông tin, sẽ không có bản tin trả lời.Master sử lý sự kiện Time-out.

- + Nếu Slave nhận được bản tin hỏi nhưng có lỗi thông tin (Parity, LRC,CRC), sẽ không có bản tin trả lời.Master sử lý sự kiện Time-out.

- +Nếu Slave nhận được bản tin không bị lỗi thông tin nhưng không thể thực hiện được thì nó sẽ trả lời bản tin báo lỗi. Nó báo cho Master lỗi nào đã xảy ra.

ModBus -Function 08 Diagnostics

13	Return Bus Exception Error Cnt	Y	Y	Y	N	N	Y
14	Return Slave Message Count	Y	Y	Y	N	N	N
15	Return Slave No Response Cnt	Y	Y	Y	N	N	N
16	Return Slave NAK Count	Y	Y	Y	N	N	Y
17	Return Slave Busy Count	Y	Y	Y	N	N	Y
18	Return Bus Char. Overrun Cnt	Y	Y	Y	N	N	Y
19	Return Overrun Error Count	N	N	N	Y	N	N
20	Clear Overrun Counter and Flag	N	N	N	Y	N	N
21	Get/Clear Modbus Plus Statistics	N	N	N	N	N	Y
22-up	Reserved						

ModBus -Trả lời báo lỗi

Bản tin báo lỗi bao gồm:

- + Trường địa chỉ báo thiết bị nào trả lời.
- + Trường chức năng với bit cao nhất bằng 1.
- + Trường dữ liệu báo lỗi nào đã xảy ra.
- + Trường kiểm tra lỗi.

ModBus - Trả lời báo lỗi

QUERY		
Byte	Contents	Example
1	Slave Address	0A
2	Function	01
3	Starting Address Hi	04
4	Starting Address Lo	A1
5	No. of Coils Hi	00
6	No. of Coils Lo	01
7	LRC	4F

EXCEPTION RESPONSE		
Byte	Contents	Example
1	Slave Address	0A
2	Function	81
3	Exception Code	02
4	LRC	73

ModBus - Trả lời báo lỗi

04	SLAVE DEVICE FAILURE	An unrecoverable error occurred while the slave was attempting to perform the requested action.
05	ACKNOWLEDGE	The slave has accepted the request and is processing it, but a long duration of time will be required to do so. This response is returned to prevent a timeout error from occurring in the master. The master can next issue a Poll Program Complete message to determine if processing is completed.
06	SLAVE DEVICE BUSY	The slave is engaged in processing a long-duration program command. The master should retransmit the message later when the slave is free.

ModBus - Trả lời báo lỗi

Code	Name	Meaning
01	ILLEGAL FUNCTION	The function code received in the query is not an allowable action for the slave. If a Poll Program Complete command was issued, this code indicates that no program function preceded it.
02	ILLEGAL DATA ADDRESS	The data address received in the query is not an allowable address for the slave.
03	ILLEGAL DATA VALUE	A value contained in the query data field is not an allowable value for the slave.

ModBus - Trả lời báo lỗi

07	NEGATIVE ACKNOWLEDGE	The slave cannot perform the program function received in the query. This code is returned for an unsuccessful programming request using function code 13 or 14 decimal. The master should request diagnostic or error information from the slave.
08	MEMORY PARITY ERROR	The slave attempted to read extended memory, but detected a parity error in the memory. The master can retry the request, but service may be required on the slave device.

ModBus Plus

- Là một hệ thống Bus dựa trên Modbus nhưng có giá thành thấp, dễ lắp đặt, cài đặt.
- Cho phép đàm thoại chỉ 64 nút trên mạng, tốc độ truyền 1 Mbps.
- Mạng Peer-to-peer, sử dụng MAC là Token passing.

ModBus Plus

HDLC LEVEL:

PREAMBLE	OPENING FLAG	BDCST ADDRESS	MAC / LLC FIELD	CRC	CLOSING FLAG
----------	--------------	---------------	-----------------	-----	--------------

MAC LEVEL:

DEST ADDRESS	SOURCE ADDRESS	MAC FUNCTION	BYTE COUNT	LLC FIELD
--------------	----------------	--------------	------------	-----------

LLC LEVEL:

OUTPUT PATH	ROUTER COUNTER	TRANS SEQUENCE	ROUTING PATH	MODBUS FRAME (MODIFIED)
-------------	----------------	----------------	--------------	-------------------------

MODBUS MESSAGE:

SLAVE ADDR	FUNCTION CODE	STARTING ADDRESS HI	STARTING ADDRESS LO	NUMBER OF REGISTERS HI	NUMBER OF REGISTERS LO
------------	---------------	---------------------	---------------------	------------------------	------------------------

ModBus Plus

- Output Path (1 byte): Đường dẫn đầu ra chỉ một kênh logic của trạm chủ, có vai trò trong việc dồn kênh/phân kênh.
- Router counter (1 byte): đếm số router mà khung bản tin đã đi qua.
- Transaction Sequence Number: Mã số giao dịch
- Routing Path (5 byte): Mã số đường dẫn chức thông tin chọn đường tối ưu trong liên mạng.
- DA (1 byte): địa chỉ trạm đích.
- SA (1 byte): Địa chỉ trạm nguồn.
- MAC Function (1 byte): mã hàm điều khiển truy nhập đường truyền.

ModBus Plus

- Byte Count (2 byte) số lượng byte trong phần LLC được truyền.
- Preamble (1 byte): dãy bit báo hiệu đầu khung.
- Opening Flag (1 byte): Cờ mở đầu khung.
- Broadcast Address (1 byte): địa chỉ gửi đồng loạt.
- CRC (2 byte): kiểm tra lỗi CRC.
- Closing Flag (1 byte): cờ báo kết thúc

Mạng máy tính & Hệ thống thông tin công nghiệp

Đào Đức Thịnh
BM Kỹ thuật đo & THCN

CAN (Controller Area Network)

CAN bao gồm các lớp sau:

- the (CAN-) object layer
- the (CAN-) transfer layer
- the physical layer.

CAN (Controller Area Network)

Mô tả chung về giao thức:

- CAN là một giao thức thông tin nối tiếp, cung cấp hệ điều khiển thời gian thực, phân tán với độ tin cậy cao.
- CAN là một chuẩn của ISO (ISO11898).
- CAN được phát triển năm 1980 bởi BOSCH.
- Nó ứng dụng trong CN SX ô-tô, máy công cụ, máy đóng bao...

CAN (Controller Area Network)

- Object:

- + Phát hiện các bản tin đã được truyền đi.
- + Quyết định bản tin nào sẽ được nhận bởi lớp Transfer và được sử dụng.
- + Cung cấp giao diện tới người dùng và các phần cứng liên quan.

Người dùng có thể định nghĩa các đối tượng kết nối.

CAN (Controller Area Network)

- Transfer:

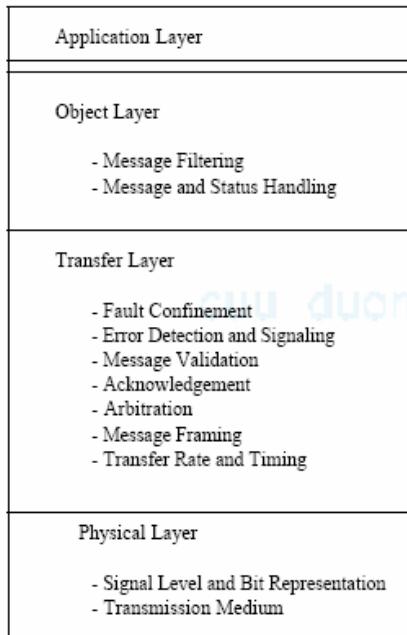
Điều khiển việc định khung, định thời, thực hiện chức năng trọng tài, kiểm tra lỗi, phát hiện lỗi và hạn chế lỗi. Quyết định khi nào thì truyền và nhận bản tin. Người dùng không được tự do thay đổi phần này.

- Physical:

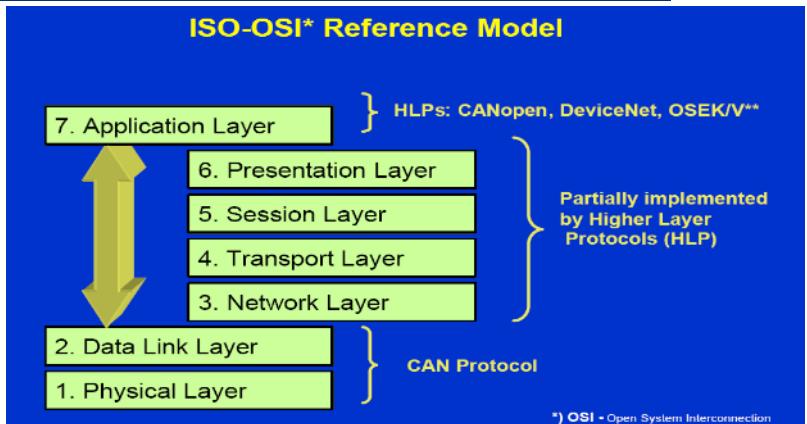
Truyền các bit giữa các nút với 1 tiêu chuẩn về điện.

CAN

Layered Structure of a CAN Node



CAN (Controller Area Network)



CAN - Các khái niệm cơ bản

- Bản tin: thông tin được truyền theo 1 vài định dạng cố định, có độ dài hạn chế. Khi Bus rỗng một thiết bị có thể truyền 1 bản tin.
- Định tuyến thông tin: Một nút CAN không chứa bất kỳ thông tin nào về hệ
 - + Hệ mềm dẻo.
 - + Định tuyến bản tin: sử dụng Identifier và Message Filtering.
- Multi Cast.
- Độ bảo toàn dữ liệu.

CAN - Các khái niệm cơ bản

- Tốc độ truyền.
- Mức độ ưu tiên của bản tin.
- Yêu cầu dữ liệu từ xa.
- Multi Master.
- Trọng tài.

CAN - Các khái niệm cơ bản

- An toàn dữ liệu:
 - + Kiểm tra lỗi:
 - . Giám sát.
 - .CRC
 - . Nhồi bit.
 - .Kiểm tra khung bản tin.
 - + Hiệu quả:
 - .Tất cả các lỗi toàn cục.
 - .Lỗi tại bộ truyền.
 - . 5 lỗi phân bố ngẫu nhiên.
 - .chuỗi lỗi < 15 bit
 - . Các lỗi lẻ
 - . Còn lại 4.7 10-11

CAN - Các khái niệm cơ bản

- Báo lỗi và thời gian phục hồi.
- Hạn chế lỗi.
- Kết nối trong CAN
- Kênh truyền.
- Giá trị bit.
- ACK
- Sleep/Wake up.

CAN - Cấu trúc bản tin

- Các bản tin được truyền và xử lý trong CAN theo 4 kiểu khác nhau của khung bản tin:
- Data Frame: mang thông tin từ nơi phát đến nơi thu.
 - Remote Frame: gửi đi một yêu cầu truyền một Data Frame với cùng một Identifier.
 - Error Frame: truyền đi bởi bất kỳ một nút nào phát hiện ra lỗi trên Bus.
 - Overload Frame: cung cấp một thời gian trễ giữa Data Frame và Remote Frame.
- Giữa Data Frame và Remote Frame được phân biệt với nhau bởi InterFrame Space.

CAN - Cấu trúc bản tin

Data Frame: bao gồm 7 trường bit.

- START OF FRAME.
- ARBITRATION FIELD
- CONTROL FIELD
- DATA FIELD
- CRC FIELD
- ACK FIELD
- END OF FRAME

cuu duong thanh cong. com

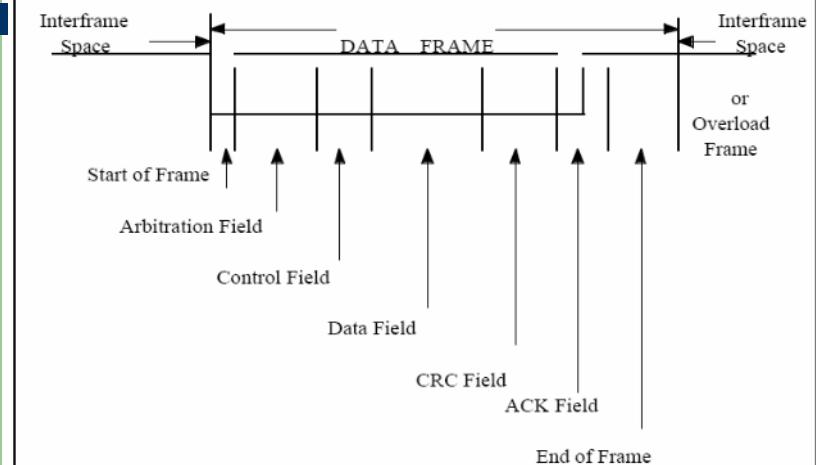
CAN - Cấu trúc bản tin

- START OF FRAME: đánh dấu việc bắt đầu một Data Frame, hay Remote Frame. Nó gồm 1 bit "trội" (Dominant)

- Trạm có thể gửi số liệu khi bus rỗi.
- Các trạm sẽ đồng bộ với sườn của START OF FRAME.

cuu duong thanh cong. com

CAN - Cấu trúc bản tin



CAN - Cấu trúc bản tin

ARBITRATION FIELD: bao gồm IDENTIFIER and the RTR-BIT.

IDENTIFIER bao gồm 11 bit ID10 - ID0. Các bit cao truyền đi trước.

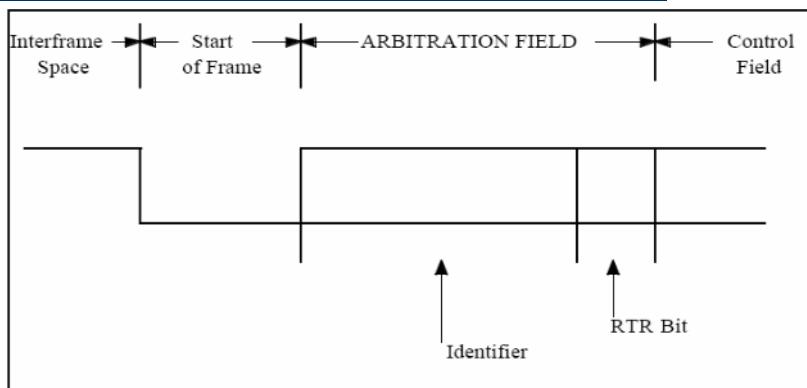
7 bit cao nhất từ ID10-ID4 không được tất cả là "lặn" (Recessive)

RTR BIT (Remote Transmission Request BIT)

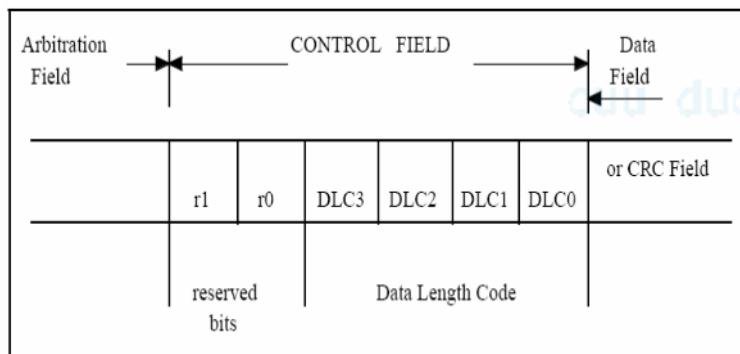
"trội" nếu là Data Frame.

"lặn" nếu là Remote Frame.

CAN - Cấu trúc bản tin



CAN - Cấu trúc bản tin



CAN - Cấu trúc bản tin

CONTROL FIELD: bao gồm 6 bit.
4 bit mã hoá độ dài của trường dữ liệu 0...8
2 bit danh cho mở rộng trong tương lai

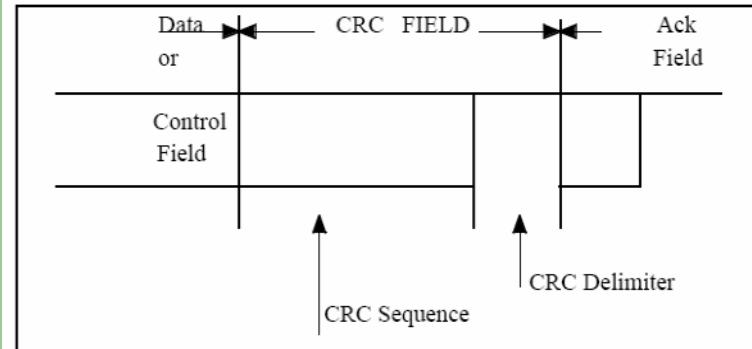
CAN - Cấu trúc bản tin

Number of Data Bytes	Data Length Code			
	DLC3	DLC2	DLC1	DLC0
0	d	d	d	d
1	d	d	d	r
2	d	d	r	d
3	d	d	r	r
4	d	r	d	d
5	d	r	d	r
6	d	r	r	d
7	d	r	r	r
8	r	d	d	d

CAN - Cấu trúc bản tin

- Data Field : Chứa 0...8 byte dữ liệu.
 - CRC Field: bao gồm CRC sequence và CRC delimiter
- CRC sequence là kết quả tính toán theo phương pháp CRC các trường: START OF FRAME, ARBITRATION FIELD, CONTROL FIELD, DATA FIELD
- Sử dụng đa thức: $X^{15} + X^{14} + X^{10} + X^8 + X^7 + X^4 + X^3 + 1$.
 - CRC delimiter bao gồm một bit lặn.

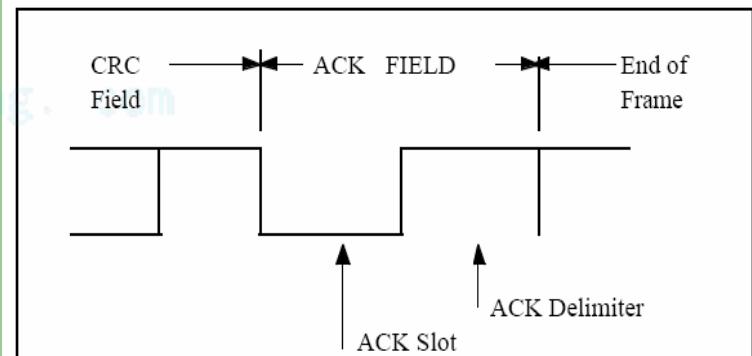
CAN - Cấu trúc bản tin



CAN - Cấu trúc bản tin

- ACK FIELD bao gồm 2 bit ACK SLOT và ACK DELIMITER.
 - Khi truyền bên truyền sẽ gửi đi hai bit lặn.
 - Nếu bên nhận nhận tốt bản tin sẽ gửi bit trống vào ACK SLOT
- End of Frame: là một cờ bao gồm 7 bit lặn.

CAN - Cấu trúc bản tin



CAN - Cấu trúc bản tin

Remote Frame: bao gồm 6 trường bit.

- START OF FRAME.
 - ARBITRATION FIELD
 - CONTROL FIELD
 - CRC FIELD
 - ACK FIELD
 - END OF FRAME
- (Tương tự như Data Frame)

cuu duong than cong. com

CAN - Cấu trúc bản tin

Error Frame bao gồm Error Flag + Error Delimiter.

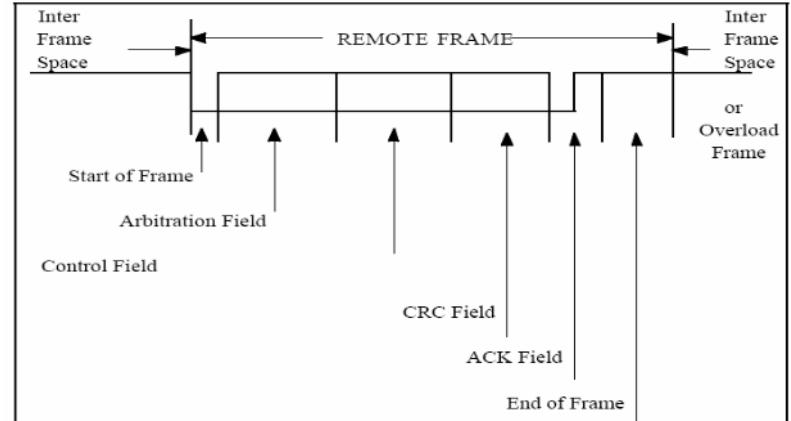
Error Flag : bao gồm hai loại

ACTIVE ERROR FLAG bao gồm 6 bit trội

PASSIVE ERROR FLAG bao gồm 6 bit lặn

- Một trạm ở trạng thái lỗi tích cực nếu phát hiện ra lỗi sẽ truyền đi một cờ lỗi tích cực. Luật của cờ lỗi sẽ phá huỷ luật chèn bit hay định dạng cố định của bản tin.
- Một trạm ở trạng thái lỗi bị động nếu phát hiện ra lỗi thi sẽ truyền đi cờ lỗi bị động.

CAN - Cấu trúc bản tin

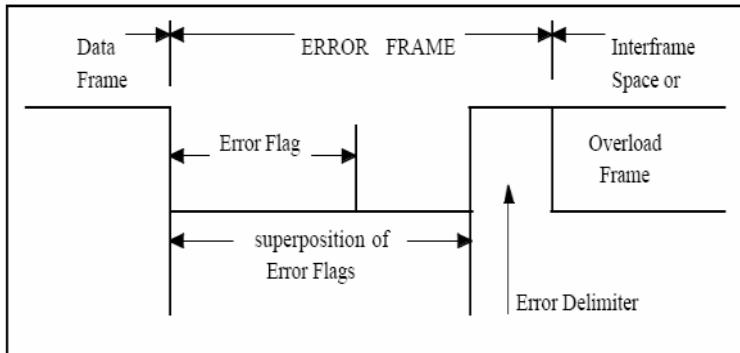


CAN - Cấu trúc bản tin

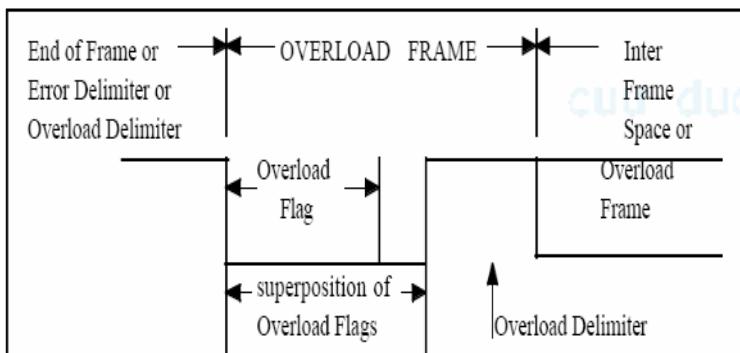
- ERROR DELIMITER: bao gồm 8 bit lặn.

Sau khi truyền đi cờ lỗi trạm sẽ truyền đi các bit lặn sau đó sẽ giám sát Bus cho tới khi nhận được các bit lặn thì truyền thêm 7 hay nhiều hơn các bit lặn.

CAN - Cấu trúc bản tin



CAN - Cấu trúc bản tin



CAN - Cấu trúc bản tin

OVERLOAD FRAME bao gồm hai trường OVERLOAD FLAG và OVERLOAD DELIMITER.

Có hai điều kiện quá tải:

- Điều kiện bên trong bộ nhận mà nó yêu cầu một thời gian trễ cho Data Frame và Remote Frame tiếp theo.
- Phát hiện ra một bit trội trong quá trình Intermission.

OVERLOAD FLAG bao gồm 6 bit trội.

OVERLOAD DELIMITER bao gồm 8 bit lặn

CAN - Cấu trúc bản tin

INTERFRAME SPACE bao gồm hai trường INTERMISSION và BUS IDLE

INTERMISSION bao gồm 3 bit lặn.

Các Data Frame và Remote Frame được cách nhau bởi INTERFRAME SPACE.

INTERMISSION các trạm không được truyền các Data hay Remote Frame mà chỉ có thể truyền điều khiển quá tải.

BUS IDLE trạm có thể truyền các bản tin.

CAN

- Mã hoá thông tin: Các trường START OF FRAME, ARBITRATION FIELD, CONTROL FIELD, DATA FIELD and CRC SEQUENCE của bản tin được mã hoá bởi PP nhồi bit.
- Nếu bên phát hiện ra 5 bit liền nhau giống nhau trong chuỗi bit đã truyền đi thì nó sẽ tự động chèn một bit đảo vào.
- Các trường còn lại của DATA FRAME hay REMOTE FRAME (CRC DELIMITER, ACK FIELD and END OF FRAME) không bị chèn. ERROR FRAME và OVERLOAD FRAME duy trì định dạng cố định không bị chèn.
- các bit mã hoá NRZ.

CAN - Kiểm soát lỗi.

Báo lỗi: Một trạm khi phát hiện ra lỗi thì sẽ gửi đi một cờ lỗi. Các lỗi như BIT ERROR, STUFF ERROR, FORM ERROR, ACKNOWLEDGEMENT ERROR phát hiện ra ở bit nào thì cờ lỗi sẽ truyền ở bit tiếp theo.

Nếu lỗi CRC được phát hiện thì cờ lỗi sẽ truyền sau ACK delimiter.

CAN - Kiểm soát lỗi.

Phát hiện lỗi: Có 5 kiểu lỗi khác nhau

- BIT ERROR
- STUFF ERROR
- CRC ERROR
- FORM ERROR
- ACKNOWLEDGEMENT ERROR

CAN - Hạn chế lỗi

Hạn chế lỗi các nút CAN chia ra làm 3 trạng thái:

- error active
- error passive
- bus off

Mỗi một nút có hai bộ đếm:

TRANSMIT ERROR COUNT
RECEIVE ERROR COUNT

CAN - Hạn chế lỗi

Các luật thay đổi giá trị bộ đếm:

1. Khi bộ nhận phát hiện ra 1 lỗi thì bộ đếm lỗi nhận tăng lên 1. Ngoại trừ trường hợp lỗi bit khi truyền cờ lỗi tích cực hay quá tải.
2. Khi bộ nhận phát hiện ra một bit trội là bit đầu tiên sau khi truyền đi cờ lỗi thì bộ đếm lỗi nhận tăng lên 8.
3. Khi bộ truyền phát hiện ra một lỗi thì nó sẽ truyền đi 1 cờ lỗi và bộ đếm lỗi truyền sẽ tăng lên 8.
4. Nếu bộ truyền phát hiện ra lỗi bit khi truyền cờ lỗi tích cực hay cờ quá tải thì bộ đếm lỗi truyền tăng lên 8.
5. Nếu bộ nhận phát hiện ra lỗi bit khi truyền cờ lỗi tích cực hay cờ quá tải thì bộ đếm lỗi nhận tăng lên 8.

CAN - Hạn chế lỗi

6. Nếu bất kỳ nút nào chịu 7 bit trội liền nhau sau khi truyền đi cờ lỗi tích cực, bị động, cờ quá tải thì bộ đếm lỗi truyền và nhận tăng lên 8.
7. Sau khi truyền tốt một bản tin thì bộ đếm lỗi truyền giảm đi 1 ngoại trừ nó đã =0.
8. Sau khi nhận tốt một bản tin bộ đếm lỗi nhận:
 - giảm đi 1 nếu nó <127
 - =0 nếu =0.
 - 119-127 nếu nó >128.
9. Nút lỗi bị động nếu có BĐLT hay BĐLN >127.

CAN - Hạn chế lỗi

10. Bus off nếu có BĐLT>256
11. Lỗi bị động nếu BĐLT và BĐLN <=127 .
12. Bus off-> lỗi tích cực với BĐLT=BĐLN=0 sau 128 sự kiện 11 bit lặp liên nhau được ghi nhận trên Bus.

CAN - Hạn chế lỗi

Mạng máy tính & Hệ thống thông tin công nghiệp

Đào Đức Thịnh
BM Kỹ thuật đo & THCN

Foundation Fieldbus - Lịch sử phát triển

Điều này dẫn tới việc các thành phần đại diện châu Âu đã rút lui và quay trở lại với hệ thống của họ trong khuôn khổ PNO (*PROFIBUS Nutzerorganisation*) cũng như Worldfip.

Hiện nay Fieldbus Foundation có hơn 130 công ty thành viên trên khắp thế giới, chiếm đa số các nhà cung cấp thiết bị đo lường và điều khiển. Hệ thống bus trường wợc phát triển trong khuôn khổ của FF được gọi là *Foundation fieldbus*.

Foundation Fieldbus - Lịch sử phát triển

Sự xuất hiện của nhiều hệ bus trường khác nhau dẫn đến việc ra đời của hai tổ chức ISP và Worldfip vào năm 1993, với cùng mục đích là xây dựng một chuẩn bus trường thống nhất. Trong khi ISP về cơ bản dựa trên nền tảng là PROFIBUS, Worldfip đại diện cho giới sản xuất và sử dụng các sản phẩm FIP. Cuối năm 1994, các thành phần đại diện phía Bắc Mỹ trong hai tổ chức này đi tới thống nhất thành lập hiệp hội mang tên Fieldbus Foundation (FF) nhằm chấm dứt sự phân nhánh trong việc xây dựng chuẩn. Tuy nhiên, các tư tưởng đại diện trong tổ chức mới này không dựa hẳn vào PROFIBUS hay FIP, mà hướng tới một hệ bus trường mới sử dụng lớp vật lý theo IEC 1158-2.

Foundation Fieldbus - Lịch sử phát triển

Tương tự như PROFIBUS-PA, phạm vi ứng dụng tiêu biểu của H1 là các ngành công nghiệp chế biến. Các công ty lớn như ABB, Fisher-rosemount (Emerson Process Management), Honeywell, National Instruments, Endress+hauser và Yokogawa đều có hàng loạt sản phẩm hỗ trợ .

Foundation Fieldbus - Tại sao?

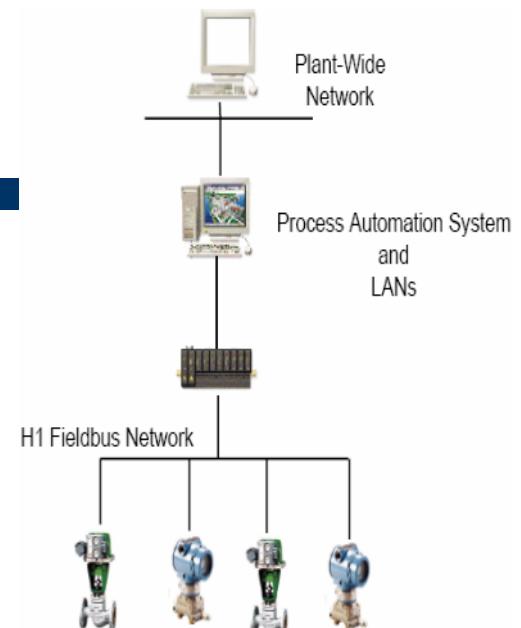
FF không chỉ là một giao thức thông tin mà nó còn có các đặc điểm sau:

- Thay thế hoàn toàn cho hệ thống cũ 4-20 mA.
- Các chức năng điều khiển, cảnh báo, theo dõi quá trình...được phân tán tới các thiết bị trong hệ.
- Cho phép các nhà thiết bị của các nhà SX nhau.
- Hệ thống mở

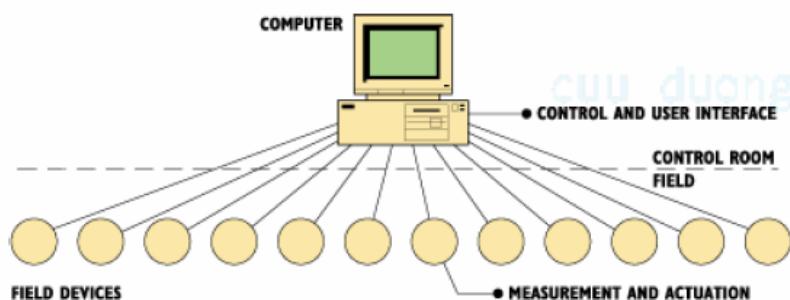
Các thiết bị FF là các thiết bị thông minh.

FF là hệ đầy đủ với các chức năng điều khiển phân tán ở các thiết bị nhưng nó vẫn cho phép hoạt động và điều khiển từ phòng điều khiển trung tâm

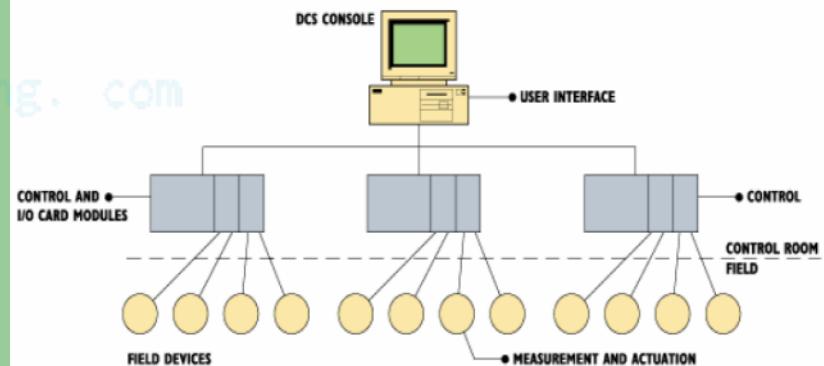
Foundation Fieldbus - Tại sao?



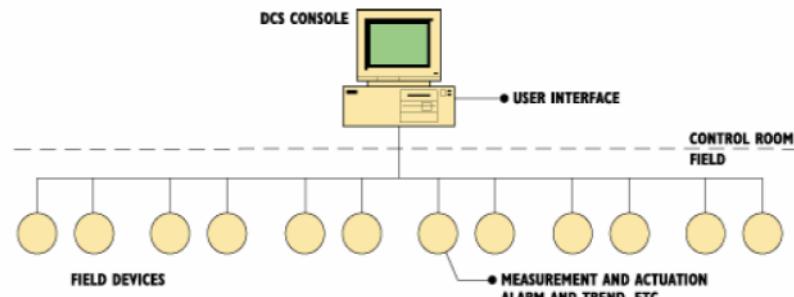
Foundation Fieldbus - Tại sao?



Foundation Fieldbus - Tại sao?



Foundation Fieldbus - Tại sao?



Foundation Fieldbus - Tại sao?

Các nhược điểm của hệ thống thông tin số so với chuẩn 4-20 mA:

- Tốc độ thông tin chậm so với đề điều vòng kín.
- Không có giao tiếp của các nhà SX khác nhau.
- Phải kiểm tra trạng thái theo kiểu hỏi vòng.
-

Foundation Fieldbus - Tại sao?

Các ưu điểm của hệ thống thông tin số so với chuẩn 4-20 mA:

- Độ chính xác cao, độ đảm bảo dữ liệu cao.
- Cho phép đa biến.
- Có thể đặt cấu hình và chuẩn đoán từ xa.
- Giảm đấu dây.
-

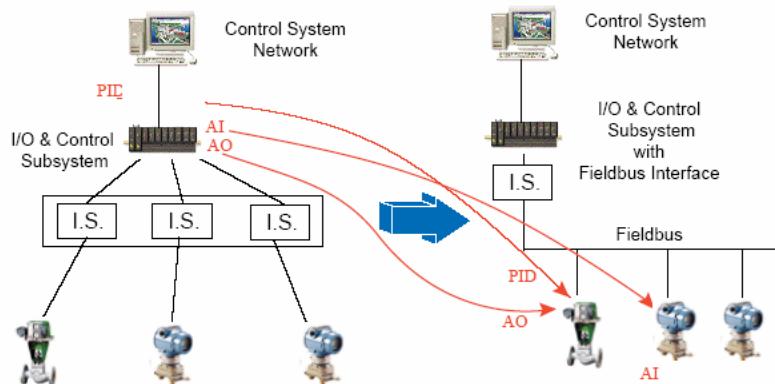
Foundation Fieldbus - Lợi Ích

- Hoạt động với độ tin cậy cao hơn.
- Độ mềm dẻo hầu như không có giới hạn.
- Giảm giá thành thiết bị.
- Giảm giá thành lắp đặt.
- Lượng thông tin lớn.

Hệ tương tự dễ hiểu hơn (người dùng chỉ cần 1 screwdriver, và 1 đồng hồ đo dòng có thể kiểm tra, cấu hình các thiết bị).

FF báo các vấn đề một cách trực tiếp, thậm chí trước khi nó xảy ra.

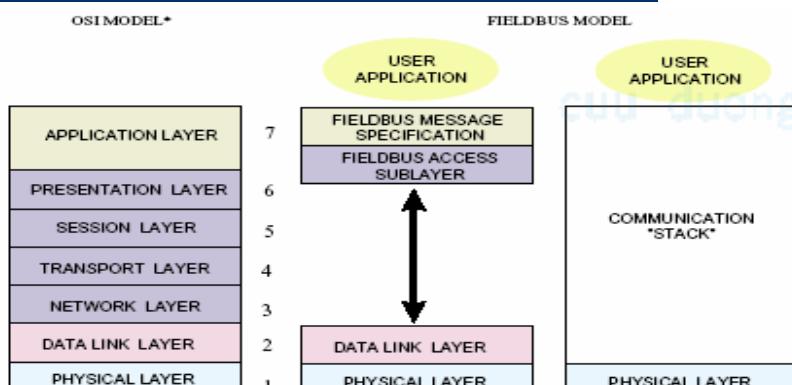
Foundation Fieldbus - Lợi ích



Foundation Fieldbus - Lợi ích

- Khả năng đa biến có thể cho phép kết hợp các bộ điều khiển và các bộ xử lý tín hiệu.
- FF cho phép kết nối vài trăm thiết bị, khoảng cách vài km với 1 đôi dây.
- FF có các khối chức năng phần mềm thay thế cho các khối phần cứng-> thay đổi hệ điều khiển mà không cần đi lại dây hay thay đổi phần cứng.
- Các kết nối có thể thay đổi, các khối chức năng có thể thêm vào hay bớt đi, ta có thực hiện gần như là vô hạn các khối chức năng, hệ có thể mở rộng với phần cứng tối thiểu.

Foundation Fieldbus - Kiến trúc giao thύc



Foundation Fieldbus - Physical

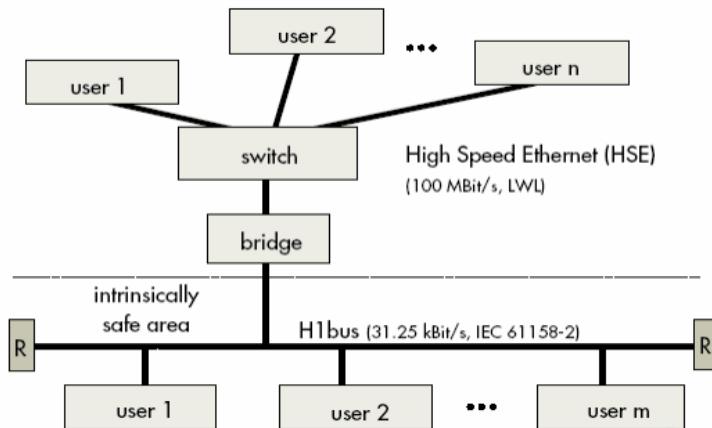
Môi trường truyền dẫn:

- Cáp điện (hay dùng cáp xoắn)
- Cáp quang.

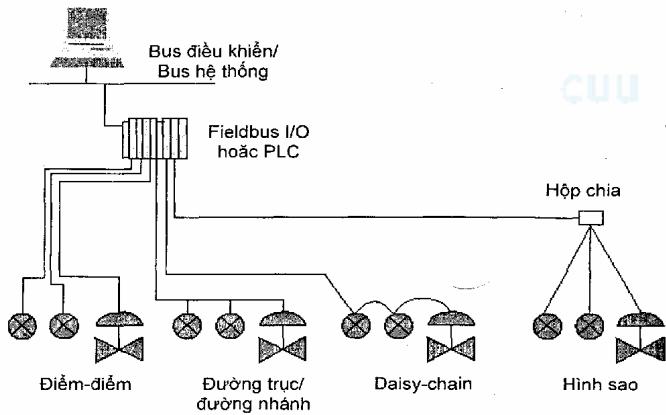
Tốc độ truyền:

- 31,25 kbps (H1)
- 1 Mbps (H2)
- 2,5 Mbps (H2)

Foundation Fieldbus - Physical



Foundation Fieldbus - Physical



Foundation Fieldbus - Physical

Cấu trúc mạng:

- Cấu trúc dạng Bus (Đường trực/nhánh, Daisy-chain)
- P-to-P.
- Cây.

Foundation Fieldbus - Physical

Số thiết bị	Chiều dài lớn nhất của nhánh
25 – 32	1 m (3.28 ft)
19 – 24	30 m (98.42 ft)
15 – 18	60 m (196.8 ft)
13 – 14	90 m (295.2 ft)
1 – 12	120 m (393.6 ft)

Quan hệ giữa số lượng thiết bị và chiều dài cung cấp của nhánh

Foundation Fieldbus - Physical

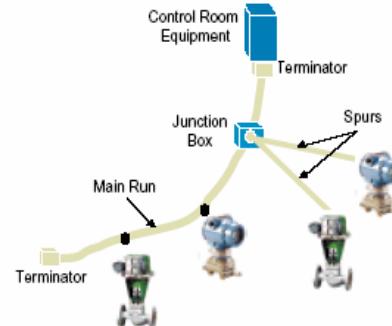
Khoảng cách truyền tối đa phụ thuộc vào tốc độ truyền:

- 31,25 kbps - 1900 m
- 1 Mbps - 750 m
- 2,5 Mbps - 500 m

Số trạm trên 1 đoạn mạng phụ thuộc vào công suất nguồn, loại cáp. tuy nhiên tối đa là 32 trạm.

Sử dụng 4 Repaeter : 9500 m, 240 trạm

Foundation Fieldbus - Physical



Foundation Fieldbus - Physical

Characteristics	Data Rate	31.25 kbit/s	31.25 kbit/s	31.25 kbit/s
Type	31.25 kbit/s	31.25 kbit/s	31.25 kbit/s	31.25 kbit/s
Topology	Bus/tree	Bus/tree	Bus/tree	Bus/tree
Power	none	DC	DC	DC
Classification		Intrinsically Safe		
Number of Devices	2-32	2-32	2-32	2-32
Cable Length	1900 m	1900 m	1900 m	1900 m
Spur Length	120 m	120 m	120 m	120 m

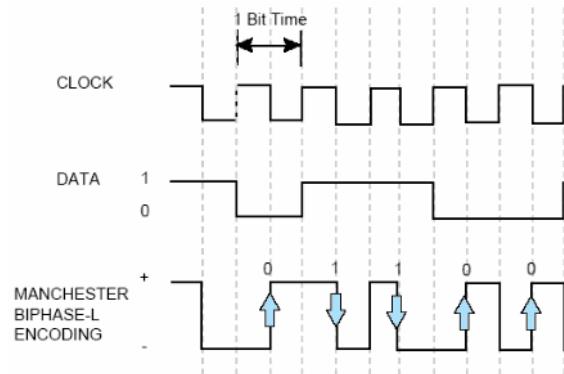
Foundation Fieldbus - Physical

Số liệu được trao đổi theo phương thức truyền đồng bộ, bán song công sử dụng mã Manchester.

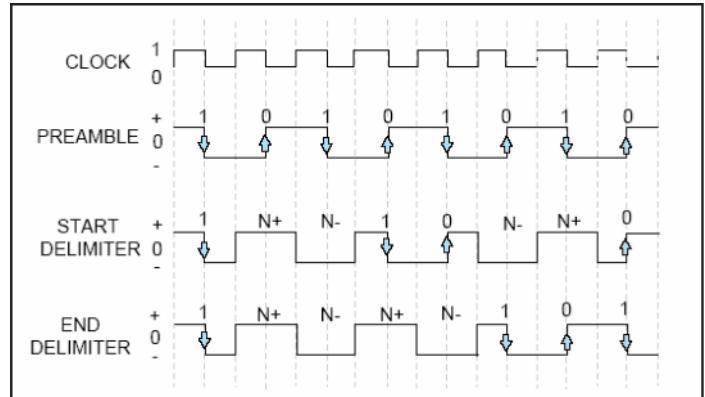
Có khả năng đồng tải nguồn trên đường truyền.
Nguồn từ 9-32 VDC

Terminator có dạng R-C

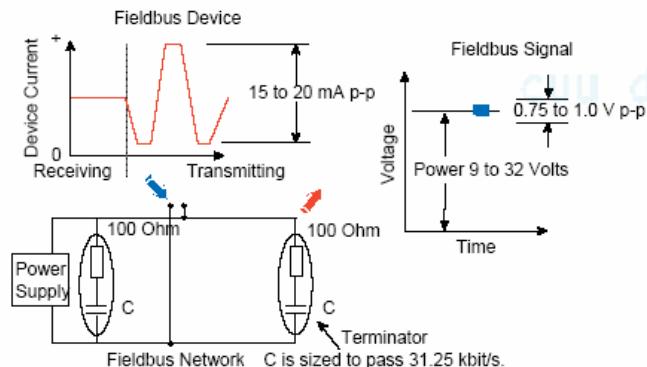
Foundation Fieldbus - Physical



Foundation Fieldbus - Physical



Foundation Fieldbus - Physical



Foundation Fieldbus - Data Link

FMAC:

- Là sự kết hợp của các phương pháp Master/Slave, Token Passing và TDMA.
- Một thiết bị đóng vai trò trạm chủ gọi là LAS (Link Active Scheduler) phân chia và kiểm soát quyền truy nhập cho toàn mạng.
- Các thiết bị FF chia 2 loại Basic Device, Link Master. Chỉ có Link Master mới có thể trở thành LAS.

Foundation Fieldbus - Data Link

FDLC: Có hai cơ chế giao tiếp là lập lịch và không lập lịch.

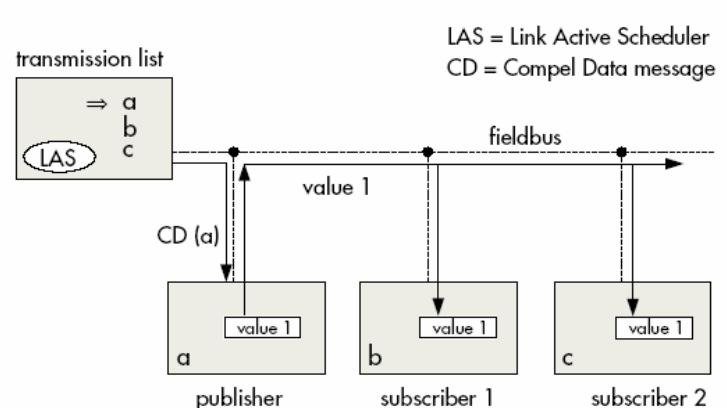
- LAS có một danh sách các thời điểm truyền cho tất cả các vùng đệm dữ liệu trong tất cả các thiết bị điều này cần thiết để việc truyền dữ liệu có chu kỳ. Khi đến thời điểm truyền dữ liệu của một thiết bị nào đó, LAS cấp cho thiết bị đó một bản tin cưỡng bức. Sau khi nhận bản tin này, thiết bị truyền thông tin trong vùng đệm của mình tới toàn bộ thiết bị trên bus. Thiết bị có nhu cầu nhận bản tin đó gọi là Người thuê bao. Việc truyền dữ liệu tiền định được sử dụng trong các trường hợp bình thường, chu kỳ truyền của vòng dữ liệu được kiểm soát giữa thiết bị và Bus.

cuu duong than cong. com

Foundation Fieldbus - Data Link

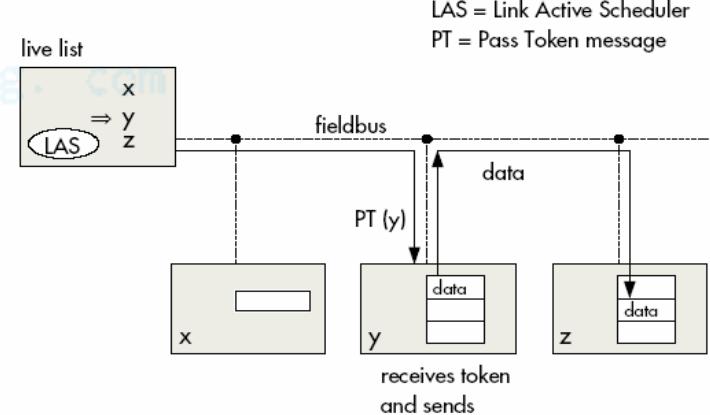
Tất cả các thiết bị trên bus đều có cơ hội gửi các bản tin không định trước giữa các bản tin tiền định. LAS cấp quyền truy cập cho một thiết bị trên bus bằng việc cấp cho thiết bị đó một thẻ bài. Khi thiết bị nhận được thẻ bài nó được phép gửi bản tin cho tới khi vượt quá thời gian giữ thẻ bài lớn nhất có thể. Bản tin có thể được gửi tới một đích hoặc nhiều đích khác nhau.

Foundation Fieldbus - Data Link



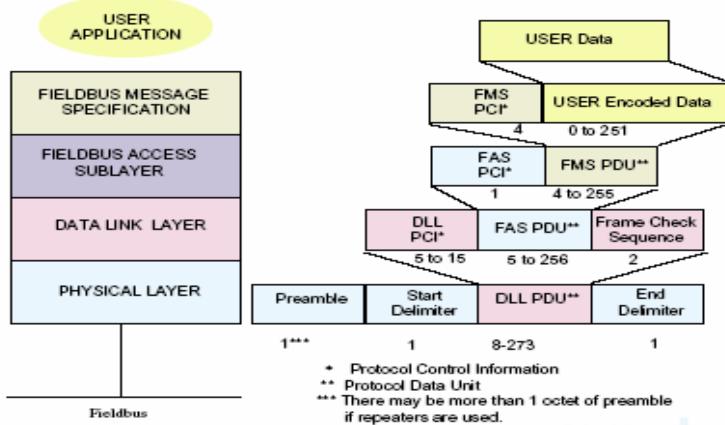
LAS = Link Active Scheduler
CD = Compel Data message

Foundation Fieldbus - Data Link



LAS = Link Active Scheduler
PT = Pass Token message

Foundation Fieldbus - Cấu trúc bức điện



Foundation Fieldbus - Các dịch vụ giao tiếp

- Khi giải quyết một bài toán phức tạp như FF người ta cần phải phân tích bài toán ra thành các phần, thậm chí thành các phần tử cơ bản.
- Sử dụng thiết kế hướng đối tượng để thiết kế quá trình ứng dụng và các khối chức năng của QTUD.
- Object là một thực thể có thể thực hiện 1 công việc nào đó.
- Phần mềm trên cơ sở các Obj sẽ thực thi công việc khi có bản tin gửi nhiệm vụ tới chúng → TKHDT không có Angorithm.
- Đối tượng được chia thành các lớp phù hợp

Foundation Fieldbus - Các dịch vụ giao tiếp

Fieldbus Access Sublayer (FAS)

Lớp con FAS sử dụng hai cơ chế giao tiếp ở lớp 2 để cung cấp các dịch vụ cho lớp FMS. Kiểu dịch vụ FAS được mô tả bởi các quan hệ giao tiếp ảo VCR (*Virtual Communication Relationships*). Ba kiểu VCR được định nghĩa sau:

- **Kiểu Client/server:** Giao tiếp không lập lịch giữa một trạm gửi (*server*) và một trạm nhận (*client*). Các thông báo được xếp trong hàng đợi theo thứ tự có ưu tiên. Kiểu VCR này thường được sử dụng trong việc nạp chương trình lên xuống, thay đổi các tham số điều khiển hoặc xác nhận báo cáo.

Foundation Fieldbus - Các dịch vụ giao tiếp

- **Kiểu phân phối báo cáo (Report Distribution):** Giao tiếp không lập lịch giữa một trạm gửi và một nhóm trạm nhận, thường được sử dụng trong việc gửi các thông báo báo động.
- **Kiểu Publisher/subscriber:** Giao tiếp lập lịch giữa một trạm gửi (*publisher*) và nhiều trạm nhận (*subscriber*), dữ liệu được cập nhật mang tính toàn cục như nằm trong một vùng nhớ chung cho toàn bộ mạng.

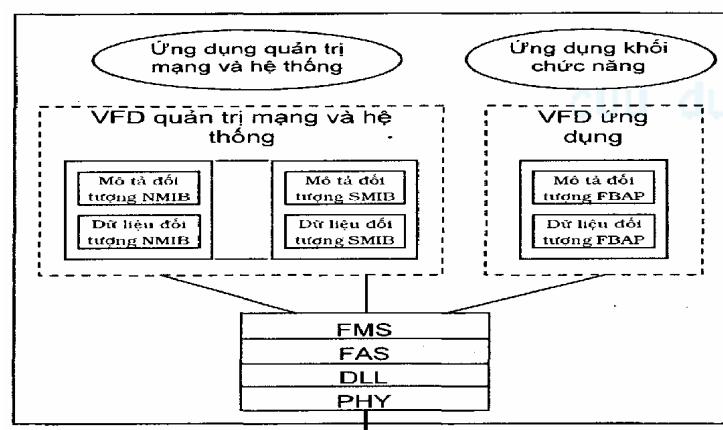
Foundation Fieldbus - Các dịch vụ giao tiếp

Fieldbus Message Specification (FMS)

Các dịch vụ FMS cho phép các chương trình ứng dụng gửi thông báo cho nhau trên bus theo một chuẩn thống nhất về tập dịch vụ cũng như cấu trúc thông báo. Ngoại trừ một số dịch vụ báo cáo thông tin và sự kiện, hầu hết các dịch vụ FMS khác đều sử dụng kiểu VCR Client/server.

Dữ liệu cần trao đổi qua bus được biểu diễn qua một "Mô tả đối tượng (object description). Các mô tả đối tượng wợc tập hợp thành một cấu trúc gọi là danh mục đối tượng (object dictionary, OD). Mỗi mô tả đối tượng được phân biệt qua chỉ số trong danh mục đối tượng.

Foundation Fieldbus - Các dịch vụ giao tiếp



Foundation Fieldbus - Các dịch vụ giao tiếp

Trong FMS, mô hình thiết bị trường ảo (*Virtual Field Device*, VFD) đóng vai trò trung tâm. Một VFD là một đối tượng mang tính chất logic được sử dụng để quan sát dữ liệu từ xa mô tả trong danh mục đối tượng

Một thiết bị thông thường có ít nhất hai VFD,

Foundation Fieldbus - Các dịch vụ giao tiếp

Quản lý mạng và hệ thống:

- Phần chính: cung cấp các chức năng cơ bản mà từ đó CT ứng dụng có thể xây dựng lên.
- Phần tiện ích: Cung cấp các dịch vụ tối ưu hoá hoạt động và chuẩn đoán các vấn đề xảy ra với mạng.

Foundation Fieldbus - Các dịch vụ giao tiếp

Phần chính bao gồm:

- Gán tên vật lý cho thiết bị
- Phân địa chỉ cho thiết bị.
- Các khối chức năng có liên quan.
- Đồng bộ hóa đồng hồ hệ thống.
- Lập danh mục các quá trình điều khiển phân tán

Foundation Fieldbus - Các dịch vụ giao tiếp

Các khối chức năng: các khối chức năng này dùng để cấu trúc nền các ứng dụng đo và điều khiển.

+ Khối chức năng;

- Khối chức năng vào.
- Khối chức năng ra.
- Khối chức năng điều khiển.
- Khối chức năng tính toán

+ Các bộ biến đổi;

- Khối chức năng bộ biến đổi vào.
- Khối chức năng bộ biến đổi ra.
- Khối chức năng bộ biến đổi hiển thị.

Foundation Fieldbus - Các dịch vụ giao tiếp

+ Khối đối tượng vật lý;

- Cảnh báo
- Sự kiện.
- Trend
- Danh sách hiển thị

Foundation Fieldbus - Các dịch vụ giao tiếp

- Mô hình khối cho phép người dùng sử dụng các khối để cấu trúc nền các ứng dụng.

- Trong FF nó là các khối phần mềm nằm trong thiết bị.
- Trong FF các khối cung cấp phần lớn các chức năng cho các hệ thống điều khiển.
- Người dùng có thể cấu trúc nền hệ ĐK bằng cách liên kết các khối chức năng.

Mạng máy tính & Hệ thống thông tin công nghiệp

Đào Đức Thịnh
BM Kỹ thuật đo & THCN

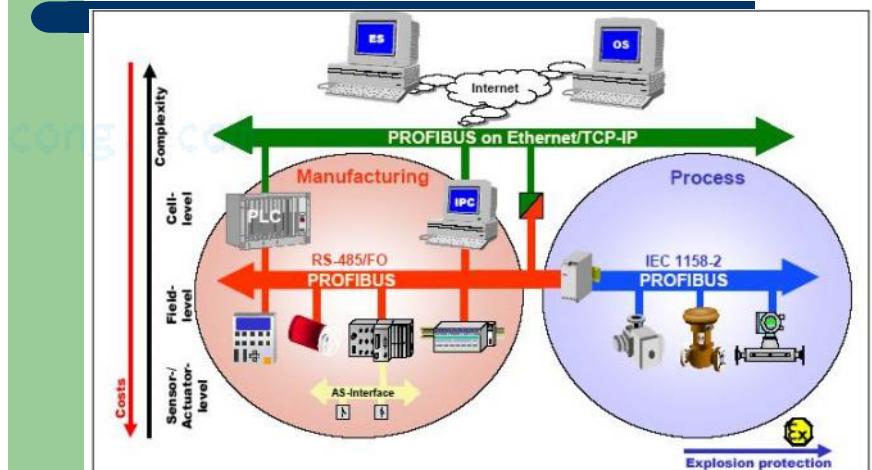
Profibus - Lịch sử phát triển

- Với mục đích quảng bá cũng như hỗ trợ việc phát triển và sử dụng các sản phẩm tương thích PROFIBUS, một tổ chức người sử dụng đã được thành lập, mang tên *PROFIBUS Nutzerorganisation* (PNO). Từ năm 1995, tổ chức này nằm trong một hiệp hội lớn mang tên *PROFIBUS International* (PI) với hơn 1.100 thành viên trên toàn thế giới.

Profibus - Lịch sử phát triển

- PROFIBUS (*Process Field Bus*) là một hệ thống bus trường được phát triển tại Đức từ năm 1987 do 21 công ty và cơ quan nghiên cứu hợp tác. Sau khi được chuẩn hóa quốc gia với DIN 19245, PROFIBUS đã trở thành chuẩn châu Âu EN 50 170 trong năm 1996 và chuẩn quốc tế IEC 61158 vào cuối năm 1999. Bên cạnh đó, PROFIBUS còn được đưa vào trong chuẩn IEC 61784 - một chuẩn mở rộng trên cơ sở IEC 61158 cho các hệ thống sản xuất công nghiệp. Với sự ra đời của các chuẩn mới IEC 61158 và IEC 61784 cũng như với các phát triển mới gần đây, PROFIBUS không chỉ dừng lại là một hệ thống truyền thông, mà còn được coi là một *công nghệ tự động hóa*.

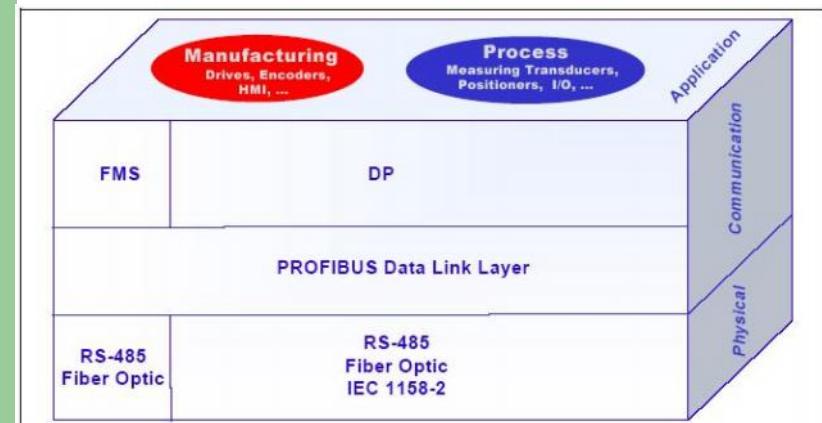
Profibus - Kỹ thuật



Profibus - Kỹ thuật

- Profibus là một chuẩn bus trường mở, không phụ thuộc vào nhà cung cấp, nó được sử dụng trong một phạm vi rộng các ứng dụng trong tự động hóa sản xuất và tự động hóa quá trình.
- Sự không phụ thuộc vào các nhà cung cấp và tính chất mở được đảm bảo bởi tiêu chuẩn quốc tế EN 50170 và EN 50254. PROFIBUS cho phép giao tiếp giữa các thiết bị của các hãng sản xuất khác nhau mà không cần sự điều chỉnh đặc biệt nào về giao diện.
- PROFIBUS có thể dùng cho cả ứng dụng đòi hỏi tính năng thời gian với tốc độ cao và các nhiệm vụ truyền thông phức tạp.
- Qua sự tiếp tục phát triển về kỹ thuật, PROFIBUS sẽ vẫn là hệ thống giao thức công nghiệp được dùng trong tương lai.

Profibus - Kỹ thuật



Profibus - Kỹ thuật

- PROFIBUS định nghĩa ba loại giao thức là PROFIBUS-FMS, PROFIBUS-DP và PROFIBUS-PA.
- FMS là profile giao tiếp đa năng cho tất cả các đòi hỏi về giao tiếp cấp cao. FMS đưa ra nhiều chức năng ứng dụng tinh vi cho sự giao tiếp giữa các thiết bị thông minh. Tuy nhiên gần đây, vai trò của PROFIBUS-FMS ngày càng mờ nhạt bởi sự cạnh tranh của các hệ dựa trên nền Ethernet (Ethernet/IP, PROFINET, High-speed Ethernet).

Profibus - Kỹ thuật

- DP là giao thức truyền thông được sử dụng thường xuyên nhất. Nó được dùng tối ưu cho tốc độ, hiệu quả và chi phí kết nối thấp, được thiết kế đặc biệt cho sự giao tiếp giữa hệ thống điều khiển và các ngoại vi phân tán. DP thích hợp để thay thế cách truyền tín hiệu song song kiểu thông thường với điện áp 24 V trong tự động hóa sản xuất cũng như cho tín hiệu tương tự truyền với 4...20 mA hoặc Hart trong điều khiển quá trình.

Profibus - Kỹ thuật

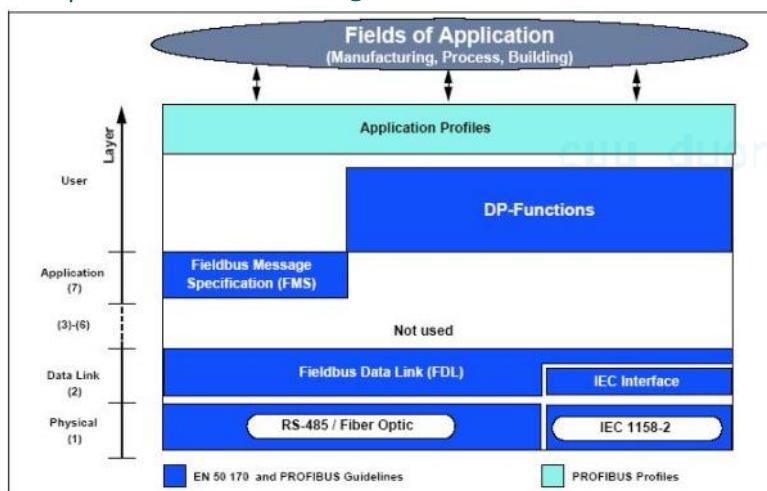
- PROFIBUS-PA là kiểu đặc biệt được sử dụng ghép nối trực tiếp các thiết bị trường trong các lĩnh vực tự động hóa các quá trình có môi trường dễ cháy nổ, đặc biệt trong công nghiệp chế biến. Thực chất, PROFIBUS-PA chính là sự mở rộng của PROFIBUS-DP xuống cấp trường cho lĩnh vực công nghiệp chế biến.

Profibus - Kỹ thuật

- Ngày nay, PROFIBUS là hệ bus trường hàng đầu thế giới với hơn 20% thị phần và với hơn 5 triệu thiết bị lắp đặt trong khoảng 500.000 ứng dụng. Có thể nói, PROFIBUS là giải pháp chuẩn, đáng tin cậy cho nhiều phạm vi ứng dụng khác nhau, đặc biệt là các ứng dụng có yêu cầu cao về tính năng thời gian.

cuuduongthancong.com

Profibus - Kiến trúc giao thức



Profibus - Kiến trúc giao thức

- DP và PA, đây là giao thức giao tiếp có hiệu suất cao, sử dụng các lớp 1 và 2 cũng như lớp giao diện sử dụng. Các lớp từ 3 đến 7 không được sử dụng. Kiến trúc tổ chức hợp lý này đảm bảo truyền dữ liệu nhanh và hiệu quả. Lớp ánh xạ ở trên lớp 7 liên kết với lớp 2 (DDLM) cung cấp giao diện sử dụng để dàng truy nhập vào lớp 2. Các chức năng ứng dụng có sẵn cho người sử dụng, cũng như hành vi thiết bị và hệ thống của các kiểu thiết bị DP khác nhau được định rõ trong lớp giao diện sử dụng.

Profibus - Kiến trúc giao thức

- Trong giao thức truyền thông đa chức năng FMS, sự quan trọng đặc biệt nằm ở các lớp 1, 2 và 7. Lớp application (7) bao gồm hai lớp con là FMS (Fieldbus Message Specification) và LLI (Lower Layer Interface). Lớp FMS đảm nhiệm việc xử lý giao thức sử dụng và các dịch vụ truyền thông cho các giao tiếp chủ-chủ và chủ-tớ. Lớp LLI có vai trò trung gian cho FMS kết nối với lớp 2 mà không phụ thuộc vào các thiết bị riêng biệt.

Profibus - Lớp vật lý

- Truyền dẫn RS-485 là công nghệ truyền dẫn được sử dụng thông dụng nhất trong PROFIBUS. Phạm vi ứng dụng bao gồm tất cả các phạm vi truyền dẫn yêu cầu tốc độ truyền cao và lắp đặt đơn giản, giá thành rẻ. Cáp dẫn được sử dụng là đôi dây xoắn có bảo vệ.
- Công nghệ truyền dẫn với RS-485 dễ sử dụng. Việc lắp đặt các cáp xoắn không yêu cầu hiểu biết nhiều về chuyên môn. Cấu trúc của bus cho phép việc thêm và bớt các trạm hoặc từng bước đưa hệ thống hoạt động mà không bị ảnh hưởng của các trạm khác. Sự mở rộng sau không làm ảnh hưởng đến các trạm đang hoạt động.

Profibus - Lớp vật lý

- Tốc độ truyền từ 9,6 kbps đến 12 Mbps.
- Chiều dài tối đa 1200m và phụ thuộc vào tốc độ truyền
Tốc độ truyền phụ thuộc vào độ dài cáp:

Band rate (kbit/s)	9.6	19.2	93.75	187.5	500	1500	12000
Range/Segment	1200 m	1200 m	1200 m	1000 m	400 m	200 m	100 m

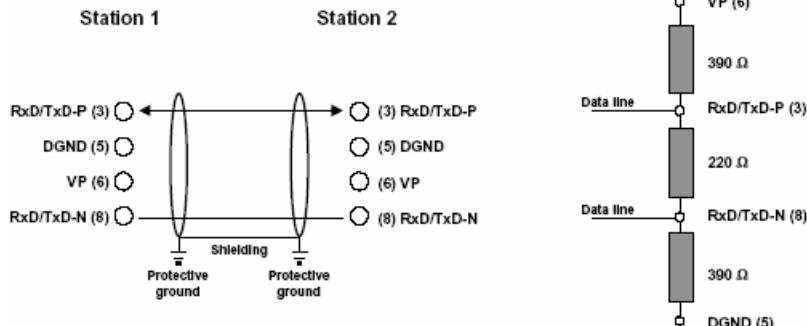
Table 2: Range based on transmission speed for type-A cable

Profibus - Lớp vật lý

- Cấu trúc mạng dạng Bus (Trunk-line/Drop-line, daisy-chain).
- Cáp dùng đôi dây xoắn có vỏ bảo vệ (PI khuyến cáo dùng cáp loại A có các thông số như sau:
 - * Trở kháng : 125 đến 165 Ω
 - * Điện dung : < 30 pf/m
 - * Trở vòng : 110 Ω/km
 - * Tiết diện dây dẫn : > 0.34 mm²)

Profibus - Lớp vật lý

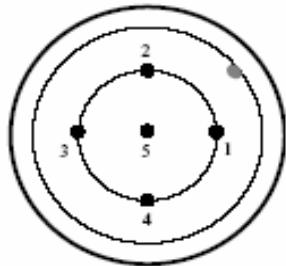
- Điện trở kết thúc dạng Fail-safe Biasing:



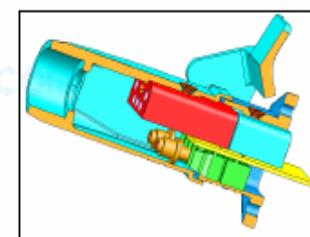
Profibus - Lớp vật lý

- Số trạm tối đa trên 1 đoạn mạng là 32. Có thể dùng tối đa 9 bộ Repeater -> 10 đoạn mạng. Tổng số trạm là 126.
- Chế độ truyền không đồng bộ, Half-duplex.
- Sử dụng mã NRZ.
- Không định nghĩa đầu nối cơ học.

Profibus - Lớp vật lý

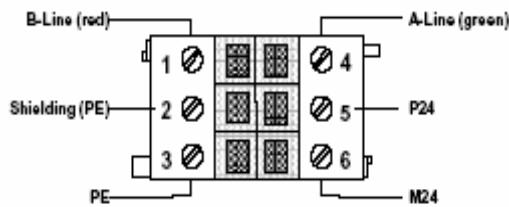


M12 Connector for RS-485 in IP65/67
Pin assignment: 1: VP, 2: RxD/TxD-N
3: DGND; 4: RxD/TxD-P; 5: Shield



Han-Brid Connector in Cu-Fo Version
for transmission of data via the fibers and 24 volt power supply for the peripherals in a single connector. This connector is also available in Cu/Cu version.

Profibus - Lớp vật lý



Siemens-Hybrid-Connector for transmission of both 24 volt power supply and PROFIBUS data via copper wires for devices with IP 65 protection.

Profibus - Lớp vật lý

- Do đặc điểm liên kết điểm-điểm ở cáp quang, cấu trúc mạng chỉ có thể là hình sao hoặc hạn hữu là mạch vòng. Trong thực tế, cáp quang thường được sử dụng hỗn hợp với RS-485 nên cấu trúc mạng phức tạp hơn. Các bộ chuyển đổi giữa 485 và cáp quang cho phép việc kết nối hỗn hợp.

Profibus - Lớp vật lý

- Cáp quang thích hợp đặc biệt trong các lĩnh vực ứng dụng có môi trường làm việc nhiễu mạnh, hoặc đòi hỏi tốc độ truyền dẫn cực cao và phạm vi phủ mạng lớn.
- Có nhiều loại cáp quang khác nhau cùng với các đặc tính khác nhau dựa trên khoảng cách, giá thành và ứng dụng.
- Hai loại cáp quang có thể sử dụng ở đây: loại sợi thuỷ tinh với chiều dài tối đa 2-3 km và loại sợi nhân tạo với chiều dài tối đa 50m không cần khuyếch đại.

Profibus - Lớp vật lý

- Truyền đồng bộ trong IEC 1158-2 (MPB) với tốc độ bót 31.25 kbit/s được sử dụng trong các hệ thống xử lý tự động. Nó thỏa mãn các yêu cầu quan trọng trong công nghệ hoá học và công nghệ hoá dầu: sự an toàn bên trong và cấp nguồn qua bus sử dụng hai dây. Do đó PROFIBUS có thể được sử dụng trong các khu vực nguy hiểm.

Profibus - Lớp vật lý

Các nguyên tắc kết nối với IEC1158-2 :

- Mỗi đoạn mạng chỉ được phép có một bộ nguồn cung cấp điện
- Không có năng lượng được cung cấp cho bus khi các trạm đang gửi tin
- Mọi thiết bị trường tiêu thụ dòng không đổi tại trạng thái tĩnh
- Mỗi thiết bị trường hoạt động như một bộ tiêu hao dòng bị động.
- Mỗi đầu cuối được kết thúc bằng một trở đầu cuối bị động.
- Cấu trúc mạng ở đây là cấu trúc đường thẳng, cây hoặc sao.

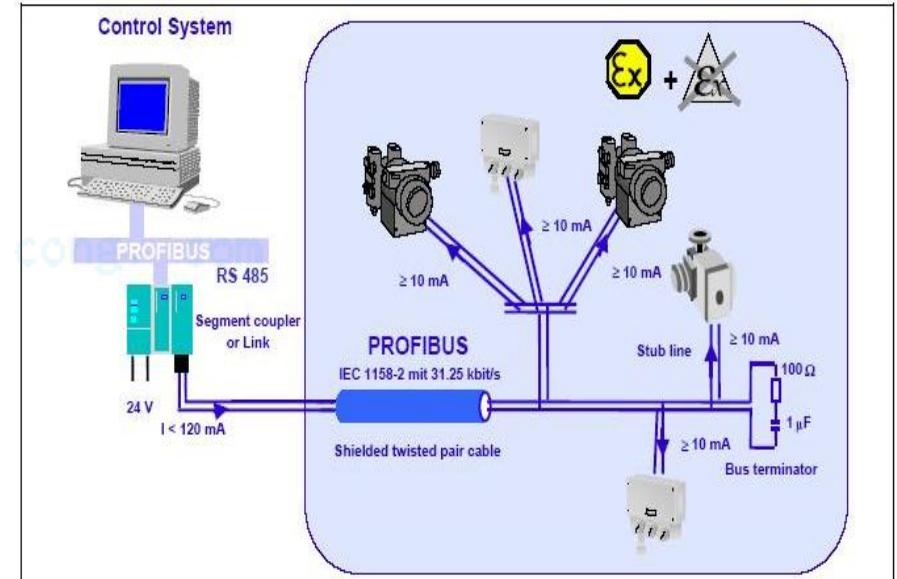
Profibus - Lớp vật lý

- Chế độ truyền	Số, đồng bộ bit, dùng mã Manchester
- Tốc độ truyền	31,25 kbit/s
- Cáp truyền	Hai đôi dây xoắn
- Cung cấp nguồn từ xa	Tùy chọn, sử dụng đường dây tải dữ liệu
- Mức bảo vệ cháy nổ	EEx ia(ib) và EEx d(m)p/q
Cấu trúc mạng	Đường thẳng, cây hoặc phôi hợp
Số trạm	Tối đa 32 trong một đoạn mạng, tổng tối đa 126
Số bộ lặp	Tối đa là 4 bộ lặp
Độ dài 1 đoạn mạng	1900m tổng 9500m

Profibus - Lớp vật lý

- Cáp bus chính được lắp ráp tại hai đầu cùng với trở đầu cuối bị động, bao gồm một bộ RC nối tiếp nhau với $R=100 \Omega$ và $C = 1\mu F$.
- Các bộ nối đoạn mạng là các bộ chuyển đổi tín hiệu, nó thích ứng các tín hiệu RS-485 với tín hiệu IEC 1158-2. Nếu các bộ nối được sử dụng, tốc độ trong đoạn mạng của RS-485 được giới hạn lớn nhất là 93.75 kbit/s
- Các bộ liên kết, chúng miêu tả tất cả các thiết bị trường kết nối trong đoạn mạng IEC 1158-2 như là một trạm tó trong đoạn mạng RS-485. Không có giới hạn về tốc độ trong đoạn mạng RS-485 khi sử dụng để liên kết. Điều đó có nghĩa rằng nó cũng có thể thực hiện với các mạng nhanh, với chức năng điều khiển, bao gồm các cả thiết bị trường kết nối bằng IEC 1158-2.

Profibus - Lớp vật lý



Profibus - Điều khiển truy nhập Bus

- Điều khiển truy nhập trung gian (MAC) xác định thủ tục khi một trạm cho phép truyền dữ liệu. MAC phải chắc chắn rằng chỉ có một trạm có quyền truyền dữ liệu tại mỗi thời điểm.

Profibus - Điều khiển truy nhập Bus

- Giao thức PROFIBUS được thiết kế để thỏa mãn hai yêu cầu của MAC, đó là:

* Trong lúc giao tiếp giữa các hệ thống tự động hóa phức tạp (các trạm chủ – masters) mỗi trạm phải có đủ thời gian để thực hiện công việc truyền thông trong một khoảng thời gian chính xác nhất định.

* Mặt khác, đối với truyền thông giữa một bộ điều khiển khả năng phức tạp và thiết bị ngoại vi đơn giản được chỉ định (các trạm tớ – slaves) thì việc truyền dữ liệu một cách tuần hoàn và tính năng thời gian thực cần phải được thực hiện càng nhanh và càng đơn giản càng tốt.

Profibus - Điều khiển truy nhập Bus

- Do vậy, giao thức truy nhập trung gian PROFIBUS bao gồm cả truy cập kiểu thẻ bài khi các trạm chủ giao tiếp với nhau và truy cập kiểu chủ/tớ khi trạm chủ giao tiếp với thiết bị ngoại vi đơn giản.

- Truy cập kiểu thẻ bài đảm bảo quyền truy nhập bus (thẻ bài) được chỉ định cho mỗi trạm chủ trong một khung thời gian xác định chính xác. Thông tin trong thẻ bài, một bản tin đặc biệt để việc chuyển thẻ bài từ trạm chủ này sang trạm chủ khác phải đi theo một vòng logic một lần tới tất cả các trạm chủ trong một thời gian luân chuyển thẻ bài cực đại. Trong PROFIBUS truy cập kiểu thẻ bài chỉ dùng cho giao tiếp giữa các trạm chủ.

Profibus - Điều khiển truy nhập Bus

- Truy cập kiểu chủ/tớ cho phép trạm chủ (trạm tích cực) đang giữ thẻ bài được quyền truy nhập các trạm tớ được chỉ định (các trạm bị động). Nó cho phép trạm chủ có thể gửi bản tin hay khôi phục bản tin từ các trạm tớ.

- Phương pháp truy nhập này cho phép thực hiện với các kiểu cấu trúc hệ thống sau:

Hệ thống một trạm chủ

Hệ thống nhiều chủ

Profibus - Điều khiển truy nhập Bus



Profibus - Dịch vụ truyền số liệu

- Lớp thứ 2 của PROFIBUS hoạt động trong một chế độ không nối. Ngoài việc truyền dữ liệu cùng cấp, nó cung cấp giao tiếp nhiều đích (Broadcast và Multicast).
- Giao tiếp Broadcast có nghĩa rằng một trạm chủ tịch trực tiếp gửi một tin không phản hồi tới tất cả các trạm (chủ và tớ).
- Giao tiếp Multicast có nghĩa rằng một trạm chủ tịch trực tiếp gửi một tin không phản hồi tới một nhóm các trạm đã được định trước (chủ và tớ).

Profibus - Dịch vụ truyền số liệu

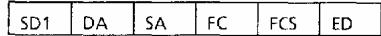
- Một nhiệm vụ quan trọng của lớp thứ 2 là bảo vệ dữ liệu. Định dạng khung lớp thứ 2 PROFIBUS đảm bảo độ toàn vẹn dữ liệu rất cao. Tất cả các bản tin đều có một khoảng cách Hamming HD=4, thông qua các dấu tách bắt đầu và kết thúc bản tin, bit chẵn lẻ và kiểm tra byte.

Profibus - Dịch vụ truyền số liệu

- Mỗi Profile giao tiếp trong profibus sử dụng một tập hợp riêng biệt các dịch vụ của lớp 2. Các dịch vụ này được gọi bởi các lớp cao hơn thông qua các điểm truy nhập dịch vụ (SAPs). Trong FMS các điểm truy nhập dịch vụ được dùng để đánh địa chỉ cho các quan hệ giao tiếp logic.
 - SDA-Send Data With Acknowledge
 - SRD-Send Data Request Data With Reply
 - SDN-Send Data With No Acknowledge
 - CSRD- Cyclic Send And Request Data With Reply

Profibus - Cấu trúc bức điện

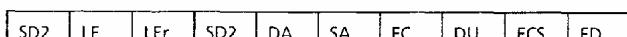
- Khung với chiều dài thông tin cố định, không mang dữ liệu:



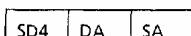
- Khung với chiều dài thông tin cố định, mang 8 byte dữ liệu:



- Khung với chiều dài thông tin khác nhau, với 1-246 byte dữ liệu:



- Token:

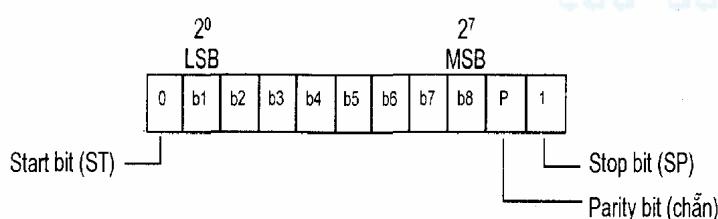


Profibus - Cấu trúc bức điện

Ký hiệu	Tên đầy đủ	Ý nghĩa
SD1...	Start Delimiter	Byte khởi đầu, phân biệt giữa các loại khung
SD4		SD1 = 10H, SD2=68H, SD3 = A2H, SD4=DCH
LE	Length	Chiều dài thông tin (4-246 byte)
LER	Length repeated	Chiều dài thông tin nhắc lại vì lý do an toàn
DA	Destination Address	Địa chỉ đích (trạm nhận), từ 0-127
SA	Source Address	Địa chỉ nguồn (trạm gửi), từ 0-126
DU	Data Unit	Khối dữ liệu sử dụng
FC	Frame Control	Byte điều khiển khung
FCS	Frame Check Sequence	Byte kiểm soát lỗi, HD = 4
ED	End Delimiter	Byte kết thúc, ED = 16H

Profibus - Cấu trúc bức điện

Dãy bit truyền đi 1 2 3 4 5 6 7 8 9 10 11



Profibus - Cấu trúc bức điện

Việc thực hiện truyền tuân thủ theo các nguyên tắc sau đây:

- Trạng thái bus rỗi tương ứng với mức tín hiệu của bit 1, tức mức tín hiệu thấp theo phương pháp mã hóa bit NRZ (0 ứng với mức cao).
- Trước một khung yêu cầu (request frame) cần một thời gian rỗi tối thiểu là 33 bit phục vụ mục đích đồng bộ hóa giữa hai bên gửi và nhận.
- Không cho phép thời gian rỗi giữa các ký tự UART của một khung.
- Với mỗi ký tự UART, bên nhận kiểm tra các bit khởi đầu, bit cuối và bit chẵn lẻ (parity chẵn). Với mỗi khung, bên nhận kiểm tra các byte SD, DA, SA, FCS, ED, LE/LER (nếu có) cũng như thời gian rỗi trước mỗi khung yêu cầu. Nếu có lỗi, toàn bộ khung phải hủy bỏ.

Profibus - Cấu trúc bức điện

Trong trường hợp gửi dữ liệu với xác nhận (SDA), bên nhận có thể dùng một ký tự duy nhất SC=E5H để xác nhận. Ký tự duy nhất SC này cũng được sử dụng để trả lời yêu cầu dữ liệu (SRD) trong trường hợp bên được yêu cầu không có dữ liệu đáp ứng.

Profibus - FMS

Mặc dù PROFIBUS-FMS không được chuẩn hóa trong IEC 6158 và một phần vì thế vai trò của nó cũng mờ nhạt dần trong các phát triển tiếp theo, ứng dụng của nó đã có một vai trò nhất định trong một số lĩnh vực công nghiệp chế tạo, lắp ráp. Sử dụng PROFIBUS-FMS là bus hệ thống, các máy tính điều khiển có thể được ghép nối theo cấu hình nhiều chủ để giao tiếp với nhau và với các thiết bị trường thông minh dưới hình thức gửi các thông báo. Ở đây, phạm vi chức năng, dịch vụ cao cấp là tính năng được coi trọng hơn so với thời gian phản ứng của hệ thống.

Profibus - FMS

Lớp ứng dụng của PROFIBUS-FMS bao gồm hai lớp con là FMS và LLI (Lower Layer Interface). Bởi các lớp từ 3 đến 6 không xuất hiện ở đây, lớp LLI có vai trò thích ứng, chuyển dịch các dịch vụ giữa lớp FMS và lớp FDL lớp 2. Giao diện giữa FMS với các quá trình ứng dụng được thực hiện bởi lớp ALI (Application Layer Interface).

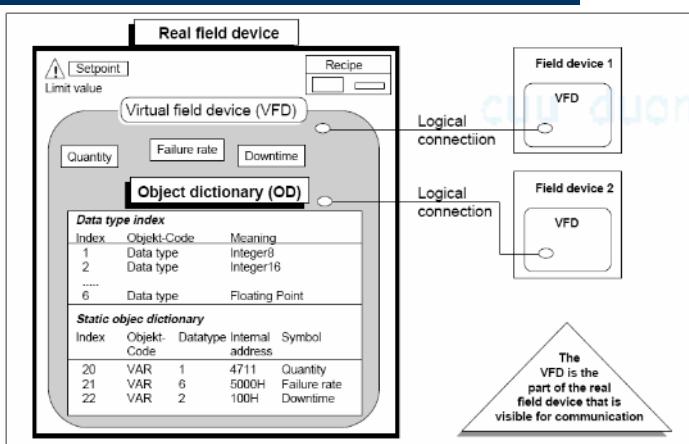
Profibus - FMS

Giao tiếp hướng đối tượng

- PROFIBUS-FMS cho phép thực hiện các hoạt động giao tiếp hướng đối tượng theo cơ chế Client/server. Ở đây, ý nghĩa của phương thức hướng đối tượng là quan điểm thống nhất trong giao tiếp dữ liệu, không phụ thuộc vào các đặc điểm của nhà sản xuất thiết bị hay của lĩnh vực ứng dụng cụ thể.
- Các phần tử có thể truy nhập được từ một trạm trong mạng, đại diện cho các đối tượng thực hay các biến quá trình được gọi là các đối tượng giao tiếp. Các thành viên trong mạng giao tiếp thông qua các đối tượng này.

Profibus - FMS

- Việc truy nhập các đối tượng có thể thực hiện theo nhiều cách khác nhau. Phương pháp hiệu quả nhất là sử dụng chỉ số đối tượng (*object index*), còn gọi là phương pháp định địa chỉ logic. Chỉ số có thể coi là cẩn cước của một đối tượng nội trong một thành viên của mạng, được biểu diễn bằng một số thứ tự 16 bit. Nhờ vậy, các khung thông báo sẽ có chiều dài ngắn nhất so với các phương pháp khác.
- Một khả năng thứ hai là truy nhập thông qua tên hình thức của đối tượng, hay còn gọi là *tag*.



Profibus - FMS

Thiết bị trường ảo (VFD)

- Thiết bị trường ảo (*virtual Field Device*, VFD) là một mô hình trừu tượng, mô tả các dữ liệu, cấu trúc dữ liệu và đặc tính của một thiết bị tự động hóa dưới giác độ của một đối tác giao tiếp.
- Một đối tượng VFD chứa tất cả các đối tượng giao tiếp và danh mục mô tả các đối tượng mà các đối tác giao tiếp có thể truy nhập qua các dịch vụ. Một đối tượng VFD được sắp xếp tương ứng với đúng một quá trình ứng dụng.
- Một thiết bị thực có thể chứa nhiều đối tượng VFD, trong đó địa chỉ của mỗi đối tượng VFD được xác định qua các điểm đầu cuối giao tiếp của nó.

Profibus - FMS

Profibus - FMS

Đối tượng truyền thông

Đối tượng được mô tả thông qua các thuộc tính của đối tượng.

- Những đối tượng truyền thông tĩnh được đưa vào danh mục đối tượng tĩnh. Chúng được định dạng một lần và không bị thay đổi trong khi vận hành. FMS ghi nhận các kiểu đối tượng truyền thông tĩnh:

- * Biến đơn,
- * Ma trận (dãy các biến đơn của cùng một kiểu)
- * Bản ghi (dãy các biến đơn của các kiểu khác nhau)
- * Vùng nhớ (Domain): chỉ vùng nhớ có liên kết logic chứa chương trình hay dữ liệu.
- * Sự kiện (event) các thông báo, cảnh báo

Profibus - FMS

- Những đối tượng truyền thông động được đưa vào phần động của danh mục đối tượng và có thể bị thay đổi khi vận hành.
 - * Danh sách biến (Variable List).
 - * Program invocation.
- Định địa chỉ logic là một phương pháp được ưa dùng hơn để đánh địa chỉ cho các đối tượng. Việc truy cập được thực hiện bởi một địa chỉ ngắn (chỉ số) là một số kiểu không dấu hexa. Mỗi đối tượng chỉ có một chỉ số. Một mục chọn được thêm vào để định địa chỉ cho các đối tượng bằng tên.
- Các đối tượng truyền thông có thể được bảo vệ khỏi bị truy cập bởi những đối tượng không có quyền truy nhập thông qua sự bảo vệ truy cập, hay những dịch vụ được cho phép để truy cập một đối tượng (ví dụ chỉ được đọc) bị hạn chế.

Profibus - FMS

Quan hệ giao tiếp

- Ngoại trừ các hình thức gửi đồng loạt (*broadcast* và *multicast*). việc trao đổi thông tin trong FMS luôn được thực hiện giữa hai đối tác truyền thông với hình thức có nối theo cơ chế Client/server. Một client được hiểu là một chương trình ứng dụng (nói chính xác hơn là một quá trình ứng dụng) gửi yêu cầu để truy nhập các đối tượng. Còn một server chính là một chương trình cung cấp các dịch vụ truyền thông thông qua các đối tượng.

Profibus - FMS

Quan hệ giao tiếp

- Mỗi quan hệ giao tiếp giữa một client và một server được gọi là một kênh logic. Về nguyên tắc, một chương trình ứng dụng có thể đóng cả hai vai trò là client và server.
- Mỗi thành viên trong mạng có thể đồng thời có nhiều quan hệ giao tiếp với cùng một thành viên khác, hoặc với các thành viên khác nhau. Mỗi quan hệ giao tiếp được mô tả bởi một số các thông số trong một *communication reference* (CR), bao gồm địa chỉ trạm đối tác (*remote address*), điểm truy nhập dịch vụ (*service access point*, SAP), các loại dịch vụ được hỗ trợ và chiều dài các bộ nhớ đệm.

Profibus - FMS

Các dịch vụ của FMS

- Các dịch vụ FMS là một tập con của các dịch vụ MMS (Manufacturing Message Specification, ISO9506) được tối ưu hóa cho các ứng dụng của bus trường và được mở rộng cho quản lý đối tượng truyền thông và quản lý mạng.

Các dịch vụ có xác nhận chỉ có thể được sử dụng cho các mối quan hệ truyền thông có kết nối định hướng.

Các dịch vụ không xác nhận chỉ được dùng trong các mối quan hệ truyền thông không kết nối (truyền broadcast và multicast). Chúng có thể được truyền với mức ưu tiên cao hoặc thấp.

Profibus - FMS

Các dịch vụ trong FMS được chia thành các nhóm sau:

- Dịch vụ **Variable Access** được dùng cho truy cập biến, bản ghi, ma trận hay danh sách biến.
- Dịch vụ **Domain Management** được dùng để truyền những vùng nhớ lớn. Dữ liệu phải được người dùng chia thành các phần nhỏ.
- Dịch vụ **Program Invocation Management** được dùng để điều khiển theo chương trình.
- Dịch vụ **Event Management** được dùng để truyền thông tin cảnh báo. Những thông tin này được gửi theo chế độ broadcast hay multicast.

Profibus - FMS

- Dịch vụ **VFD Support** được dùng để xác minh và thăm dò trạng thái. Chúng có thể được gửi đồng thời khi yêu cầu theo chế độ truyền multicast hay broadcast.
- Dịch vụ **OD Management** được dùng để đọc hay ghi khi truy cập vào danh mục đối tượng.
- Dịch vụ **Context Management** phục vụ cho việc thiết lập và kết thúc các kết nối logic.

Profibus - FMS

LLI (Lower Layer Interface)

- Liên hệ của lớp thứ 7 với lớp thứ 2 được thực hiện bởi LLI. Nhiệm vụ bao gồm điều khiển luồng dữ liệu và giám sát kết nối. Người dùng giao tiếp với các quá trình thông qua các kênh logic được gọi là các **mối quan hệ truyền thông**. LLI cung cấp nhiều kiểu mối quan hệ truyền thông để thực hiện FMS và các dịch vụ quản lý. Các mối quan hệ truyền thông có những khả năng kết nối khác nhau (ví dụ: quan sát, truyền dẫn, yêu cầu đối với đối tác truyền thông).

Profibus - FMS

- Các mối quan hệ truyền thông có kết nối thể hiện kết nối logic cùng cấp (peer-to-peer) giữa hai quá trình ứng dụng. Trước hết kết nối phải được thiết lập bởi dịch vụ khởi đầu trước khi có thể sử dụng cho truyền dữ liệu. Sau khi được thiết lập thành công, kết nối được bảo vệ khỏi bị truy cập bởi những đối tác không có quyền truy cập và sẵn sàng để truyền dữ liệu. Khi một kết nối không còn cần nữa thì nó được giải phóng. LLI cho phép giám sát kết nối điều khiển theo thời gian cho các mối quan hệ truyền thông có kết nối.

Profibus - FMS

- Các mối quan hệ truyền thông không kết nối cho phép một thiết bị giao tiếp đồng thời với một vài trạm sử dụng các dịch vụ không xác nhận. Trong các mối quan hệ truyền thông broadcast, một dịch vụ không xác nhận FMS được gửi đồng thời tới tất cả các trạm khác. Trong mối quan hệ truyền thông multicast, một dịch vụ không xác nhận FMS được gửi đồng thời tới một nhóm trạm đã định trước. Tất cả các mối quan hệ truyền thông của một thiết bị FMS được đưa vào một CRL.

Profibus - FMS

Quản lý mạng

- Ngoài các dịch vụ của FMS ra, các hàm quản lý mạng (Fieldbus MAnagement Layer 7 = FMA7) cũng có sẵn. Các hàm FMA7 là không bắt buộc và tùy theo sự cấu hình hoá trung tâm. Chúng có thể được khởi đầu riêng hay từ xa.
- **Quản lý theo ngữ cảnh** được dùng để thiết lập hay ngắt các kết nối FMA7.
- **Quản lý cấu hình hoá** được dùng để truy cập các CRL, biến, các bộ đếm số và các tham số của lớp 1/2. Nó cũng được dùng cho sự xác minh và đăng ký của các trạm trên bus

Profibus - FMS

- **Quản lý lỗi** được dùng để biểu diễn lỗi/sự kiện và reset các thiết bị.

Nguyên tắc truy cập của các thiết bị cấu hình hoá đạt được bằng sự xác định của quản lý nối mặc định. Một kết nối quản lý mặc định phải được đưa vào với CREF=1 trong CRL đối với mọi thiết bị có hỗ trợ dịch vụ FMA7 như một bộ đáp ứng.

Profibus - DP

PROFIBUS DP được thiết kế hiệu quả cho việc trao đổi dữ liệu ở cấp trường. Những thiết bị điều khiển trung tâm, như PLC/PC hay các hệ thống điều khiển quá trình, giao tiếp thông qua một chuỗi kết nối với các thiết bị cấp trường phân tán như thiết bị vào ra, thiết bị truyền dẫn và các van, cũng như các bộ biến nồng độ lường. Dữ liệu trao đổi với các thiết bị phân tán chủ yếu là tuần hoàn. Các chức năng truyền thông đòi hỏi ở đây được xác định bởi các chức năng DP cơ bản phù hợp với EN50-170. Ngoài các chức năng cơ bản, DP cũng đưa ra các dịch vụ truyền thông không tuần hoàn mở rộng để phục vụ cho việc tham số hóa, vận hành, theo dõi và cảnh báo của các thiết bị trường thông minh.

Profibus - DP

- DP cho phép hệ thống một trạm chủ hay nhiều trạm chủ. Nó cho độ mềm dẻo cao trong suốt cấu trúc hệ thống. Số trạm cực đại (cả trạm chủ và trạm tớ) nối trong mỗi bus là 126. Xác lập cấu hình hệ thống xác định số trạm, đánh địa chỉ cho mỗi trạm cho các địa chỉ I/O, tính nhất quán của dữ liệu I/O, định dạng bản tin chuẩn đoán lỗi và tham số bus sử dụng.
- Trong cấu hình nhiều trạm chủ các trạm chủ đều có thể đọc dữ liệu ảnh đầu I/O từ trạm tớ nhưng chỉ có 1 trạm có quyền ghi dữ liệu đầu ra.

Profibus - DP

- Có 3 loại thiết bị khác nhau:
 - * DP master class 1 (DPM1)
- Đây là một bộ điều khiển trung tâm trao đổi thông tin tuần hoàn với các trạm tớ theo một chu trình thông tin đã định trước. Thiết bị loại này điển hình là các PLC hay PC.
- * DP master class 2 (DPM2)
- Thiết bị loại này là các máy lập trình, công cụ cấu hình và thiết bị vận hành. Ngoài các dịch vụ của DPM1, các thiết bị này còn cung cấp các hàm đặc biệt phục vụ cho việc đặt cấu hình hệ thống, chuẩn đoán trạng thái, truyền nạp chương trình...

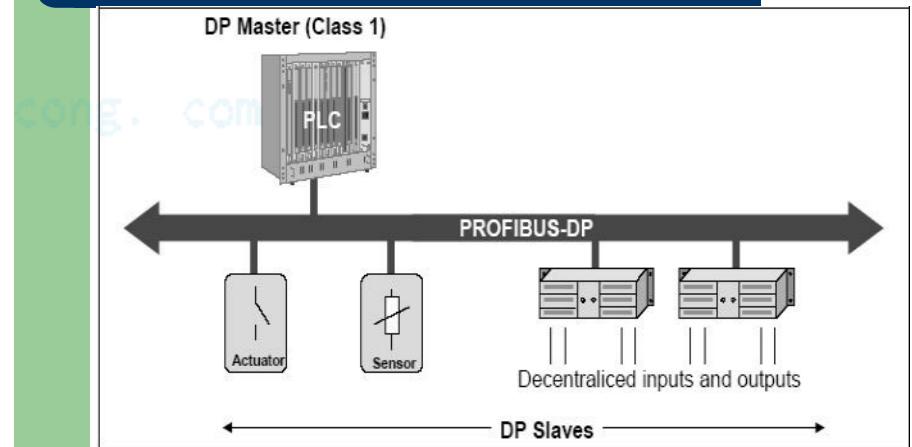
Profibus - DP

* DP slave:

Một DP slave là một thiết bị truwòng (thiết bị vào/ra, kích thích, van, bộ biến đổi đo lường...) thu thập thông tin ở đầu vào và gửi thông tin ra đầu ra tới các thiết bị ngoại vi. Cũng có những thiết bị chỉ cung cấp thông tin đầu vào hoặc đầu ra.

Lượng thông tin đầu vào và đầu ra phụ thuộc vào kiểu thiết bị. Cá thông tin đầu vào và thông tin đầu ra cực đại cho phép đều là 246 bytes

Profibus - DP



Profibus - DP

Đặc tính vận hành của hệ thống:

- Chuẩn DP bao gồm cả việc mô tả chi tiết hành vi của hệ thống để đảm bảo tính tương thích và khả năng thay thế lẫn nhau của các thiết bị. Hành vi của hệ thống được xác định trước hết qua trạng thái vận hành của các thiết bị DPM1.

Profibus - DP

- DPM1 có thể được điều khiển cục bộ hay qua bus bởi thiết bị cấu hình. Có 3 trạng thái chính:

*Stop: Trong trạng thái này, không có sự truyền dữ liệu giữa DPM1 và các trạm tớ. Chỉ có thể chuẩn đoán và tham số hoá.

*Clear: Trong trạng thái này, DPM1 đọc thông tin đầu vào của các trạm tớ và giữ các đầu ra ở giá trị an toàn.

*Operate: Trong trạng thái này, DPM1 ở chế độ trao đổi dữ liệu đầu vào và đầu ra tuần hoàn với các trạm tớ. Thông tin đầu vào của các trạm tớ được đọc và thông tin đầu ra được ghi cho các trạm tớ.

Profibus - DP

- DPM1 gửi một cách tuần hoàn thông tin về tình trạng của nó tới tất cả các trạm tớ đã chỉ định cho nó có sử dụng lệnh gửi đồng loạt vào các khoảng thời gian đặt trước.

- Phản ứng của hệ thống đối với một lỗi trong khi DPM1 ở chế độ trao đổi dữ liệu được xác định bằng tham số cấu hình auto-clear. Nếu tham số này được đặt là TRUE thì DPM1 sẽ khoá đầu ra của tất cả các trạm tớ được chỉ định tới trạng thái an toàn ngay khi một trạm tớ không sẵn sàng cho việc truyền dữ liệu sử dụng. Sau đó DPM1 chuyển sang trạng thái Clear.

Nếu tham số này là FALSE thì DPM1 giữ nguyên ở trạng thái Operate ngay cả khi có lỗi xảy ra và người dùng có thể xác định được phản ứng của hệ thống.

Profibus - DP

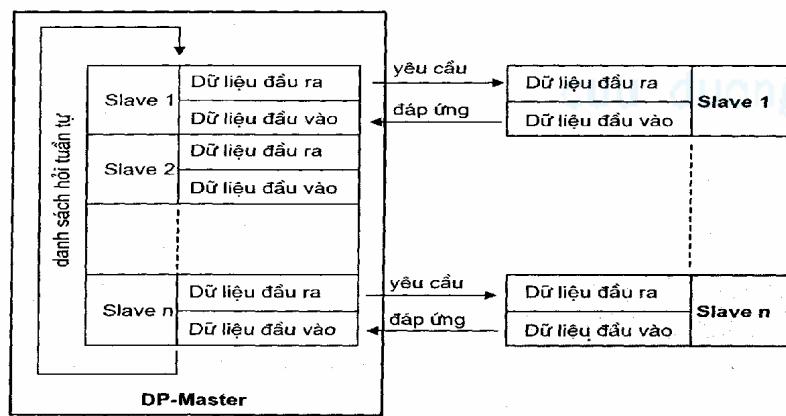
Trao đổi dữ liệu tuần hoàn

- Trao đổi dữ liệu giữa trạm chủ và các trạm tớ gán cho nó được thực hiện tự động theo một trình tự qui định sẵn. Khi đặt cấu hình hệ thống bus, người sử dụng định nghĩa các trạm tớ cho một thiết bị DPM1, qui định các trạm tớ tham gia và các trạm tớ không tham gia trao đổi dữ liệu tuần hoàn.

Profibus - DP

- Trước khi thực hiện trao đổi dữ liệu tuần hoàn, trạm chủ chuyển thông tin cấu hình và các tham số đã được đặt xuống các trạm tớ. Mỗi trạm tớ sẽ kiểm tra các thông tin về kiểu thiết bị, khuôn dạng và chiều dài dữ liệu, số lượng các đầu vào/ra. Chỉ khi thông tin cấu hình đúng với cấu hình thực của thiết bị và các tham số hợp lệ thì nó mới bắt đầu thực hiện trao đổi dữ liệu tuần hoàn với trạm chủ.

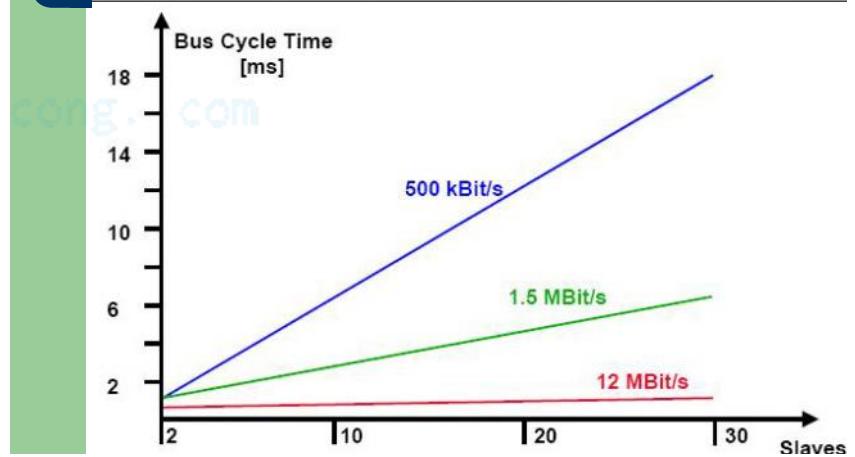
Profibus - DP



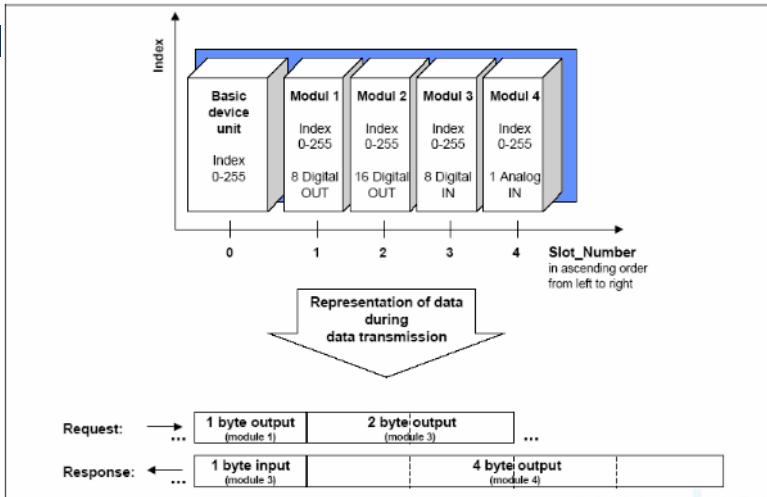
Profibus - DP

- Trong mỗi chu kỳ, trạm chủ đọc các thông tin đầu vào lần lượt từ các trạm tớ lên bộ nhớ đệm cũng như đưa các thông tin đầu ra từ bộ nhớ đệm xuống lần lượt các trạm tớ theo một trình tự qui định sẵn trong danh sách (polling list). Mỗi trạm tớ cho phép truyền tối đa 246 Byte dữ liệu đầu vào và 246 Byte dữ liệu đầu ra.
- Với mỗi trạm tớ, trạm chủ gửi một khung yêu cầu và chờ đợi một khung đáp ứng (bức điện trả lời hoặc xác nhận). Thời gian trạm chủ cần để xử lý một lượt danh sách hỏi tuần tự chính là chu kỳ bus.

Profibus - DP



Profibus - DP



Profibus - DP

- Đầu ra của tất cả các trạm tớ đã đánh địa chỉ được giữ nguyên ở trạng thái hiện tại. Trong suốt quá trình truyền dữ liệu tiếp theo, dữ liệu đầu ra được lưu trữ tại các trạm tớ, nhưng các trạng thái đầu ra được giữ không đổi. Dữ liệu đầu ra được lưu trữ sẽ không được gửi tới các đầu ra cho tới khi nhận được một lệnh Sync tiếp theo. Chế độ Sync kết thúc bằng một lệnh Unsync.
- Tương tự, một lệnh điều khiển Freeze sẽ chuyển các trạm tớ sang chế độ Freeze. Trong chế độ này, trạng thái của các đầu vào được giữ nguyên tại giá trị hiện tại. Dữ liệu đầu vào không được cập nhật cho đến khi trạm chủ gửi một lệnh Freeze tiếp theo. Chế độ Freeze kết thúc bằng một lệnh Unfreeze.

Profibus - DP

Đồng bộ hóa dữ liệu vào ra:

- Trong truyền dữ liệu sử dụng do trạm chủ thực hiện tự động, trạm chủ có thể gửi lệnh điều khiển tới một trạm tớ đơn lẻ, một nhóm trạm tớ hay tới tất cả các trạm tớ một cách đồng thời. Những lệnh điều khiển này được truyền như một lệnh gửi đồng loạt. Chúng cho phép sử dụng chế độ Sync và Freeze cho việc đồng bộ hóa điều khiển theo sự kiện của các trạm tớ.

Profibus - DP

Chuẩn đoán hệ thống:

- Chức năng chuẩn đoán lỗi của DP cho phép định vị lỗi nhanh. Thông tin chuẩn đoán lỗi được truyền qua bus và được tập trung tại trạm chủ. Thông tin này được chia làm 3 cấp:
 1. Mức trạm: Thông tin này có liên quan đến tình trạng vận hành chung của trạm, ví dụ như: quá nhiệt độ, điện áp thấp...
 2. Chuẩn đoán module: Thông tin này thể hiện rằng trong một phạm vi nhất định của đầu vào/ra ví dụ như module đầu ra 8bit.. của một trạm, chuẩn đoán là chưa xác định.
 3. Chuẩn đoán kênh: Trong trường hợp này, nguyên nhân lỗi được xác định trong mối liên hệ với từng bit vào/ra riêng biệt (kênh) ví dụ như ngắn mạch đầu ra 7.

Profibus - DP

Các chức năng sau đây có sẵn khi truyền dữ liệu không tuân hoán giữa hệ thống điều khiển trung tâm (DPM1) và các trạm tớ:

MSAC1_Read: Trạm chủ đọc một khối dữ liệu từ trạm tớ.

MSAC1_Write: Trạm chủ ghi một khối dữ liệu tới trạm tớ.

MSAC1_Alarm: Thông tin cảnh báo truyền từ trạm tớ tới trạm chủ. Có bản tin báo nhận của trạm chủ. Chỉ sau khi thông tin báo nhận sự cảnh báo đã được nhận thì trạm tớ mới có thể gửi một thông tin cảnh báo mới. Điều đó có nghĩa rằng thông tin cảnh báo không bao giờ bị ghi đè.

Profibus - DP

Các chức năng sau đây có sẵn để truyền dữ liệu không tuân hoán giữa những công cụ lập trình và vận hành (DPM2) và các trạm tớ:

MSAC2_khởi đầu và MSAC2_Kết thúc: Thiết lập và kết thúc của các nối cho việc truyền dữ liệu không tuân hoán giữa DPM2 và trạm tớ.

MSAC2_đọc: Trạm chủ đọc một khối dữ liệu từ trạm tớ.

MSAC2_ghi: Trạm chủ ghi một khối dữ liệu tới trạm tớ.

MSAC2_vận chuyển dữ liệu: Với dịch vụ này, trạm chủ có thể ghi dữ liệu một cách không tuân hoán tới cáo trạm tớ và nếu yêu cầu thì cũng có thể đọc dữ liệu từ trạm tớ trong cùng một chu trình dịch vụ.

Profibus - DP

MSAC1 nhận thông tin cảnh báo: Trạm chủ nhận gửi một thông tin cho trạm tớ với thông báo đã nhận được thông tin cảnh báo.

Trạng thái MSAC1: Thông tin về trạng thái được gửi từ trạm tớ tới trạm chủ. Và thông tin này không được báo nhận. Do vậy thông tin về trạng thái có thể bị ghi đè.

Profibus - DP

Giao tiếp trực tiếp giữa các trạm tớ

Trao đổi dữ liệu giữa các trạm tớ là một yêu cầu thiết thực đối với cấu trúc điều khiển phân tán thực sự sử dụng các thiết bị trường thông minh. Như ta đã biết, cơ chế giao tiếp chủ-tớ thuần túy làm giảm hiệu suất trao đổi dữ liệu cho trường hợp này. Chính vì thế, phiên bản DP-V2 đã bổ sung một cơ chế trao đổi dữ liệu trực tiếp theo kiểu chào hàng đặt hàng giữa các trạm tớ.

Profibus - DP

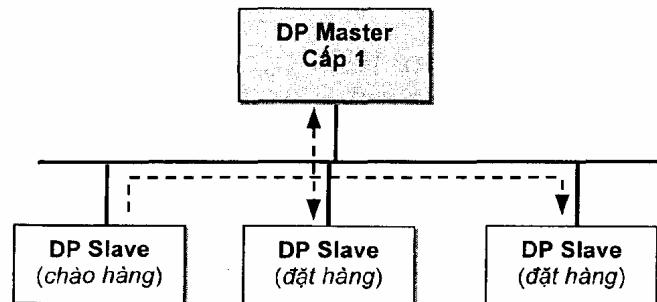
Một trạm tớ (ví dụ một cảm biến) có thể đóng vai trò là "nhà xuất bản" hay "nhà cung cấp" dữ liệu. Khối dữ liệu sẽ được gửi đồng loạt tới tất cả các trạm tớ (ví dụ một van điều khiển, một biến tần) đã đăng ký với vai trò "người đặt hàng" mà không cần đi qua trạm chủ. Với cơ chế này, không những hiệu suất sử dụng đường truyền được nâng cao, mà tính năng đáp ứng của hệ thống còn được cải thiện rõ rệt.

Profibus - DP

Chế độ đẳng thời

Đối với một số ứng dụng như điều khiển truyền động điện, điều khiển chuyển động, cơ chế giao tiếp theo kiểu hỏi trả lời tự hoặc giao tiếp trực tiếp tớ-tớ chưa thể đáp ứng được đòi hỏi cao về tính năng thời gian thực. Vì vậy, phiên bản DP-V2 bổ sung chế độ đẳng thời (*isochronous mode*), cho phép thực hiện giao tiếp theo cơ chế chủ/tớ kết hợp với TDMA.

Profibus - DP



Hình 4.8: Giao tiếp trực tiếp giữa các trạm tớ

Profibus - DP

Nhờ một thông báo điều khiển toàn cục gửi đồng loạt, toàn bộ các trạm trong mạng được đồng bộ hóa thời gian với độ chính xác tới micro-giây. Việc giao tiếp được thực hiện theo một lịch trình đặt trước, không phụ thuộc vào tải tức thời trên bus. Cơ chế này cho phép phối hợp hoạt động một cách chặt chẽ và nhịp nhàng giữa các trạm trên bus.

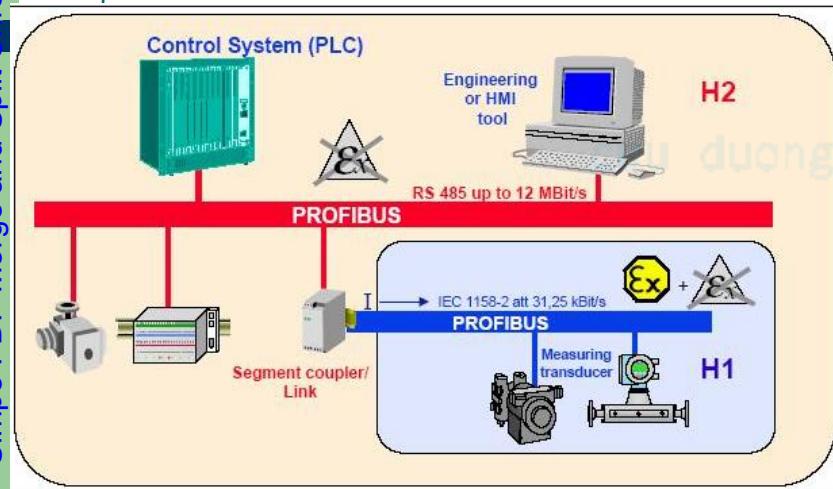
Profibus - PA

- PROFIBUS PA thực chất được xây dựng trên mô hình giao thức PROFIBUS DP với chuẩn truyền dẫn IEC 1158-2(MBP), và một số các thông số- đặc tính cho các thiết bị trường.
- Ưu điểm của nó là cho phép các thiết bị của những nhà sản xuất khác nhau có thể tương tác với nhau hoặc thay thế lẫn nhau.
- Những đặc tính hữu dụng của PROFIBUS PA khiến giao thức này có thể thay thế phương thức truyền tín hiệu với 4..20 mA hoặc HART.

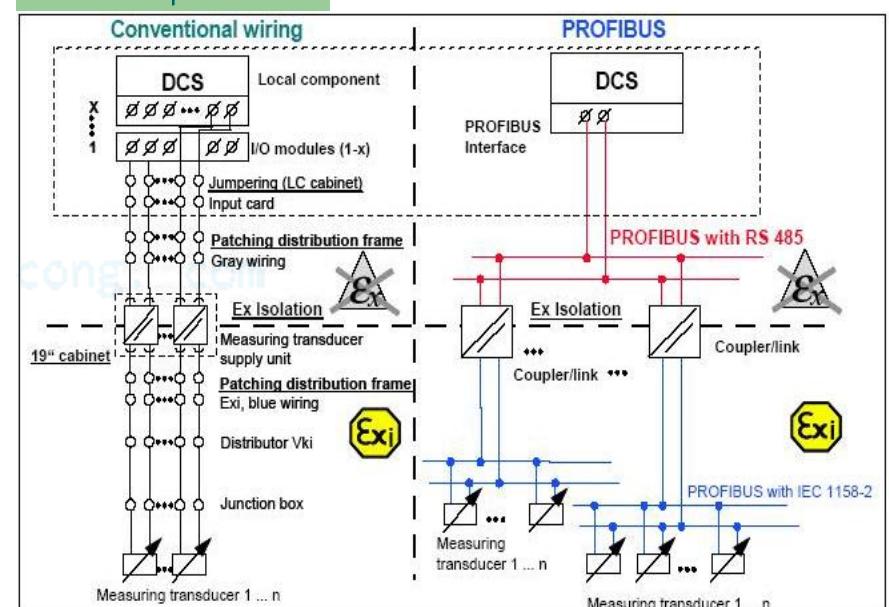
Profibus - PA

- Xét về mặt đặc tính hoạt động-chức năng, PROFIBUS PA dựa trên mô hình khối hàm chức năng(Function Block Model).
- PROFIBUS PA cho phép kết nối các hệ thống thiết bị trường bằng cáp đôi dây xoắn đơn giản, với tốc độ truyền cố định 31,5kbps.
- Khi sử dụng giao thức này, ta có thể bảo dưỡng, thay thế một số thiết bị nếu cần thiết trong khi đang vận hành. Đặc biệt, nó còn rất hữu ích khi sử dụng ở những khu vực nguy hiểm, dễ cháy nổ với phương thức bảo vệ kiểu "an toàn riêng" (EEX ia/ib) hoặc kiểu "đóng kín" (EExd).

Profibus - PA



Profibus - PA



Profibus - PA

Giao diện Bus an toàn riêng:

- Trường thiết bị trong những vùng nguy hiểm được kết nối với công nghệ truyền dẫn sử dụng chuẩn 1158-2. Chuẩn này cho phép truyền dẫn thông tin cũng như năng lượng giữa các trường thiết bị chỉ với 2 dây dẫn.
- Khác với những phương thức truyền dẫn quen thuộc trước đây, PROFIBUS PA chỉ cần dùng một đường dây truyền dẫn tín hiệu từ những điểm đo đặc tới bộ I/O của hệ thống điều khiển. Với một nguồn công suất (nguồn chống nổ - nếu cần, ở những khu vực nguy hiểm), tín hiệu sẽ được truyền khắp mạng PROFIBUS tới những nơi yêu cầu.

Profibus - PA

- Tuỳ vào mức độ cháy nổ của khu vực và sự tiêu tốn năng lượng của thiết bị, có từ 9 tới 32 bộ truyền tín hiệu đo đặc được kết nối trong mạng truyền thông.

Profibus - PA

Các yêu cầu cụ thể cho BUS an toàn riêng:

- Một đoạn mạng chỉ có một nguồn nuôi tích cực.
- Mỗi một trạm tiêu thụ dòng cố định($\geq 10mA$) ở trạng thái xác lập.
- Mỗi một trạm được coi là tải tiêu thụ dòng thụ động(bỏ qua thành phần dung, cảm kháng).
- Một trạm khi phát tín hiệu 0 được nạp thêm nguồn.

Profibus - PA

- Các giá trị đo, biến trạng thái và biến điều khiển của giao thức PROFIBUS PA được truyền dẫn tuần hoàn với quyền ưu tiên cao tới DP Master (DPM1) thông qua các bộ DP cơ sở. Điều này đảm bảo các giá trị đo cũng như các biến trạng thái luôn luôn được cập nhật và luân chuyển kịp thời đến DP Master.
- Mặt khác, các thông số thiết bị không tuần hoàn như thông tin bảo dưỡng- chuẩn đoán, chế độ vận hành ...được trao đổi tuần hoàn tới công cụ phát triển - engineering tool (DPM2) thông qua các hàm DP mở rộng kết nối với quyền ưu tiên thấp.

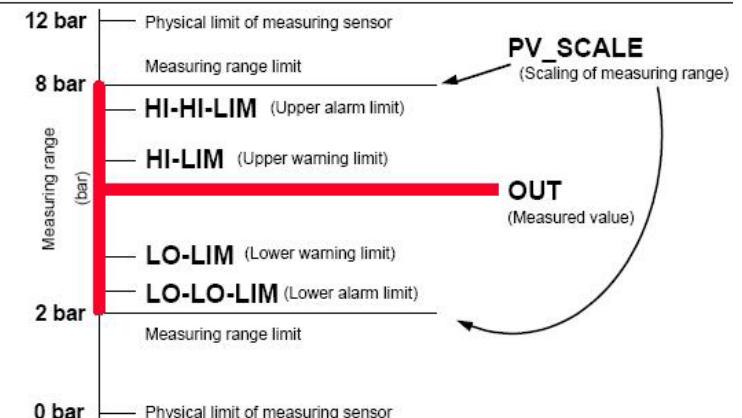
Profibus - PA

Các thiết bị trường PA tuỳ theo các đặc tính (profile) có thể chia thành 2 nhóm :

- Đặc tính nhóm A (Profile class A) : quy định đặc tính và chức năng cho các thiết bị đơn giản như : bộ cảm biến áp suất, nhiệt độ các cơ cấu truyền động. Ta cũng có thể truy nhập các thông số hệ thống như tốc độ, thời gian trễ, ngưỡng cảnh báo vào mạng thông tin.
- Đặc tính nhóm B (Profile Class B): quy định chức năng, đặc tính cho các thiết bị phức hợp, còn gọi là các thiết bị thông minh. Các chức năng này của giao thức cho phép gán địa chỉ tự động, đồng bộ hóa thời gian , phân tán dữ liệu tới các bộ I/O phân tán, mô tả thiết bị qua ngôn ngữ DDL (Device Description Language) cũng như lập lịch khối hàm (Function Block).

để cung cấp thông tin về trạng thái

Profibus - PA



Profibus - PA

Giao thức PROFIBUS PA cho phép tương tác, thay thế lẫn nhau giữa các thiết bị của những nhà sản xuất khác nhau. Nó sử dụng mô hình khối hàm để mô tả chức năng tham số thiết bị. Mỗi khối hàm mô tả một chức năng sử dụng, chẳng hạn vào hoặc ra tương tự. Trên thực tế, hai khối hàm - tuỳ theo chức năng cụ thể, có thể một khối hàm vật lý và một khối chuyển đổi, được kết nối với nhau thông qua mối liên kết truyền thông của hệ tạo thành chương trình điều khiển.

để cung cấp thông tin về trạng thái

Profibus - PA

Thường có những loại khối hàm sau đây :

- Khối hàm vật lý (Physical Block) : chứa những thông tin chung về thiết bị như tên, nhà sản xuất, chủng loại, mã số.
- Khối hàm chuyển đổi (Transducer Block) chứa những thông số kết nối giữa các thiết bị
- Khối đầu vào tương tự (Analog Input) : cung cấp giá trị đo được bởi cảm biến như các thông số trạng thái, nhiệt độ, áp suất.
- Khối đầu ra tương tự (AO) : cung cấp các giá trị tương tự ở đầu ra hệ thống điều khiển.

Profibus - PA

- Khối đầu vào số (Digital Input) : chứa giá trị đầu vào ở dạng số
- Khối đầu ra số (DO) : đưa ra thông số đầu ra của hệ thống điều khiển ở dạng số.

Trong mạng truyền thông, nhiều khối hàm được các nhà sản xuất tích hợp với nhau thông qua thiết bị trung gian, do đó ta có thể truy nhập vào hệ thống lấy ra các thông số, kết nối các khối hàm tạo nên trình ứng dụng giao thức PROFIBUS PA.

Thiết bị Profibus

Các thiết bị PROFIBUS có những đặc điểm cấu trúc khác nhau. Sự khác nhau về cấu trúc giữa chúng tùy thuộc vào chức năng của từng thiết bị (ví dụ như thiết bị truyền tín hiệu đầu vào/đầu ra, các bộ chẩn đoán) và phụ thuộc vào các tham số đường truyền như tốc độ truyền dữ liệu, các giá trị thời gian giám sát. Những tham số này thay đổi tùy theo từng loại thiết bị và hệ thống điều khiển. Để mạng truyền thông với giao thức PROFIBUS có cấu trúc đơn giản, các thiết bị thường sử dụng GSD files.

Thiết bị Profibus

- Tất cả các nhà sản xuất đều phải cung cấp file GSD trong các thiết bị PROFIBUS của mình.
- GSD files được ứng dụng rộng rãi, từ hệ thống truyền tin mở đến các hệ thống điều khiển vận hành. GSD files được dùng trên mọi cấu hình từ loại đơn giản nhất đến loại phức tạp nhất. Điều này có nghĩa là tích hợp giữa các thiết bị thuộc những nhà sản xuất khác nhau trong mạng PROFIBUS không là vấn đề khó khăn.

Thiết bị Profibus

- GSD files chứa những đặc điểm đặc trưng cơ bản giống nhau giữa các thiết bị PROFIBUS, đó chính là lý do vì sao GSD files tương thích được với nhiều loại thiết bị. Thông qua những file này, kỹ sư dự án không phải nắm bắt các thông số kỹ thuật theo cách đo đạc bằng tay thông thường như trước nữa. Thời gian được tiết kiệm đáng kể và trong suốt quá trình, hệ thống điều khiển sẽ tự động kiểm tra (check) các sai số đầu vào, sai số truyền dữ liệu và nhiều loại sai số khác.

Thiết bị Profibus

- Nhìn chung một file GSD bao gồm ba khu vực (sections) sau:
 - * Khu vực chứa thông tin chung: những thông tin chung chẳng hạn như tên thiết bị, mã đăng ký phần mềm, phần cứng, tốc độ truyền dữ liệu của đường truyền, thời gian giám sát.
 - * Khu vực liên kết với trạm chủ (Master - related): chứa những tham số liên kết với trạm chủ, ví dụ số lượng lớn nhất các slave có thể kết nối... Khu vực này không có trong các thiết bị slave.
 - * Khu vực liên kết với trạm tớ (Slave - related): khu vực này chứa những thông tin liên quan đến trạm slave như số lượng và chủng loại đầu vào/ đầu ra, các thông tin chẩn đoán về các module thiết bị.

cuu duong than cong. com

Thiết bị Profibus



Thiết bị Profibus

- Các tham số của từng khu vực riêng biệt được tách biệt ra bởi các từ khoá - key words. Từ khoá A chỉ những tham số uỷ nhiệm (ví dụ tên hãng sản xuất), tham số lựa chọn (options) như mã số đồng bộ. Sự khác biệt từng nhóm tham số cho phép ta lựa chọn options được hiệu quả. Ngoài ra, các file bit map với những biểu tượng của thiết bị có thể được tích hợp. Dung lượng thông tin các file GSD có thể chứa rất lớn. Nó chứa thông số về tốc độ truyền dữ liệu cũng như cả không gian mô tả các module hữu ích trong các module thiết bị. Nó còn chứa cả các thông tin chẩn đoán.

Thiết bị Profibus

Nhà cung cấp	Chip	Kiểu	Đặc tính	FMS	DP	Vi xử lý	Giao thức SW	Tốc độ (Mbit/s)
AGE	Agent-PB	Chủ/tổ	Chip giao thức đa chức năng dựa trên FPGA	•	•	•	•	12
IAM	PBM	Chủ	Chip giao thức ngoại vi	•	•	•	•	3
M2C	IX1	Chủ/tổ	Chip đơn hoặc chip giao thức ngoại vi	•	•	•	•	3
Siemens	SPC4	Tổ	Chip giao thức ngoại vi	•	•	•	•	12
Siemens	SPC3	Tổ	Chip giao thức ngoại vi	-	•	•	•	12
Siemens	DPC31	Tổ	Chip giao thức có vi xử lý	-	•	•	•	12
Siemens	ASPC2	Chủ	Chip giao thức ngoại vi	•	•	•	•	12
Siemens	SPM2	Tổ	Chip đơn có kết nối 64 I/O bits	-	•	-	-	12
Siemens	LSPM2	Tổ	Giá rẻ, Chip đơn có kết nối 32 I/O bits	-	•	-	-	12
PROFCHIP	VPC3+	Tổ	Chip giao thức ngoại vi	-	•	•	•	12
PROFCHIP	VPC LS	Tổ	Giá rẻ, Chip đơn có kết nối 32 I/O bits	-	•	-	-	12

Thiết bị Profibus

Phương thức làm việc của bộ slave đơn giản

Đối với các thiết bị đầu vào/ đầu ra đơn giản, giải pháp PROFIBUS với AICs đơn chip là một giải pháp thực tế. Tất cả các chức năng giao thức đã được tích hợp sẵn trong ASICs. Vì vậy không cần bộ vi xử lý hoặc phần mềm mà chỉ cần mạch giao diện truyền tin, tinh thể thạch anh và các thiết bị điện tử công suất đóng vai trò như các thiết bị ngoại vi. Thí dụ bộ slave điển hình bao gồm SPM2 ASIC của Siemens, chip IX1 của M2C và CHIP vpcls-asic của profichip.

Thiết bị Profibus

Phương thức làm việc của bộ slave thông minh

- Đối với bộ slave thông minh, bộ phận thời gian tới hạn của nó sẽ làm việc trên chip giao thức, các phần còn lại làm việc như phần mềm trong bộ vi điều khiển.
- Chip DDC31 của hãng Siemens là sự kết hợp của chip giao thức và bộ vi điều khiển. Còn những chip cơ sở khác, ví dụ như ASICs SPC3 (Siemens), VPC3+ (PROFCHIP) hay IX1 (M2C) thì đã được chế sẵn, chỉ cần lắp ráp. Những con chip ASIC cung cấp giao diện dùng chung với các bộ vi điều khiển. Ngoài ra, ở bộ slave thông minh ta còn có thể dùng các bộ vi xử lý với lõi đã được tích hợp giao thức PROFIBUS.

Thiết bị Profibus

Phương thức làm việc của bộ master phức hợp

- Cũng giống như bộ slave thông minh, ở bộ master phức hợp, bộ phận thời gian tới hạn của nó cũng làm việc trên chip giao thức, còn những phần còn lại làm việc như phần mềm trong bộ vi điều khiển. Các chip ASICs ASPC2 (Siemens), IX1 (M2C) hay VAF PBM (IAM) đều đã được chế sẵn để hỗ trợ các thiết bị master phức hợp hoạt động. Chúng cũng được kết hợp và cùng vận hành với các bộ vi xử lý.

Thiết bị Profibus

Phương thức làm việc theo chuẩn IEC 1158-2

- Đối với các thiết bị trường truyền công suất tuân theo chuẩn IEC 1158-2, một vấn đề cần lưu ý là công suất tiêu tốn phải thấp (vì đây là những thiết bị truyền công suất). Đối với những thiết bị loại này thường thường chỉ dùng nguồn dòng cỡ 10 mA là phù hợp cho việc nuôi các thiết bị đo đạc, cung cấp năng lượng truyền tin.
- Để đáp ứng được các yêu cầu trên, hãng Siemens và hãng Smar đã chế tạo ra những con chip đặc biệt phù hợp. Những con chip này sẽ lấy năng lượng cần thiết để vận hành toàn bộ thiết bị từ đường bus truyền theo chuẩn IEC 1158-2 và khiến đường truyền là nguồn cung cấp điện áp cho các thiết bị trường PA khác trong hệ thống



AS-Interface



AS-i

- AS-i : Actuator Sensor Interface
- Trong CN 80% các cảm biến và cơ cấu chấp hành làm việc với các biến logic.
- Nối mạng giữa chúng phải đảm bảo yêu cầu về giá thành, lắp đặt, vận hành, bảo dưỡng.

cuu duong than cong. com

AS-i

Khả năng đồng tải nguồn.

Khả năng chống nhiễu cao nhưng không đòi hỏi chất lượng đường truyền dẫn tốt.

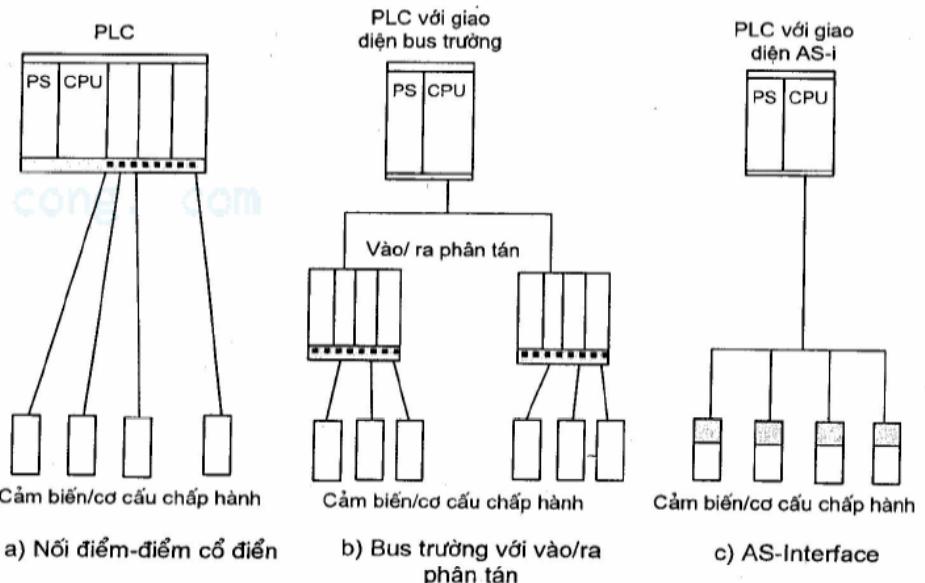
Cấu trúc mạng đường thẳng hay cây.

Các thành phần giao diện thực hiện với giá cả thấp.

Bộ nối phải nhỏ , gọn, đơn giản, giá thành hợp lý.



AS-i



AS-i Kiến trúc giao thức

- Giao tiếp giữa các bộ điều khiển và các thiết bị cảm biến, cơ cấu chấp hành.
- Trao đổi dữ liệu thuận tuý, số lượng nhỏ.
- Nâng cao hiệu suất, đơn giản thực hiện -> sử dụng lớp vật lý trong mô hình hệ mở.

AS-i

- Sử dụng PP mã hoá bit mới để tương thích với truyền trên hai dây, đồng tải nguồn.
- ĐK truy nhập mạng và bảo toàn dữ liệu cũng thực hiện ở lớp vật lý.
- Master/Slave.
- Chẵn lẻ + mã hoá bit

AS-i Cấu trúc mạng

- Tuỳ chọn theo yêu cầu, vị trí, phạm vi đi dây.
- Daisy-chain, Trunk-line/drop-line.
- Cấu trúc hình cây.
- Có thể phân bố đều hay tham gia theo nhóm.
- Không yêu cầu điện trở đầu cuối (terminator).

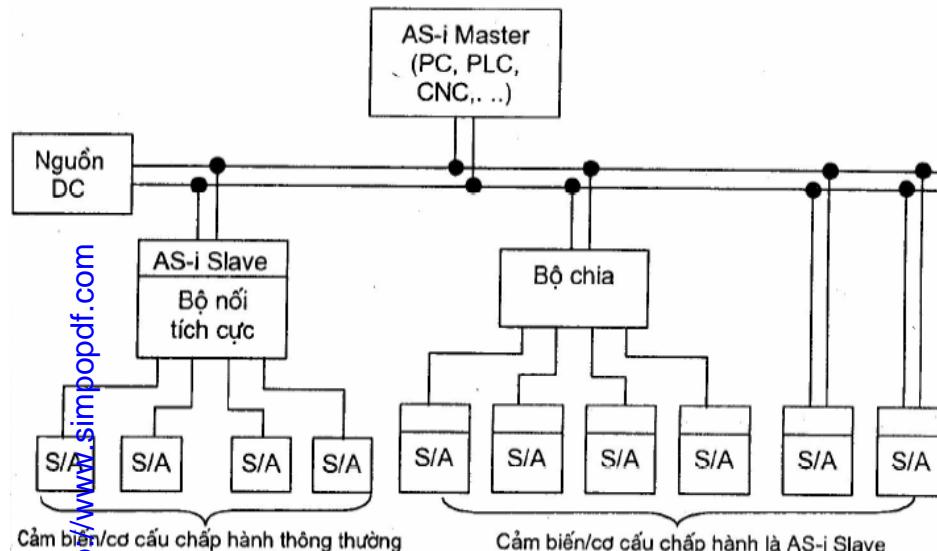
AS-i

- Trạm chủ duy nhất có thể là: PLC, PC, hay bộ ĐK CNC, bộ nối field bus
- Trạm tớ là bộ nối tích cực ghép với 4 AS thông thường hay các AS có AS-i.
- Nối trực tiếp hay qua các bộ chia.

AS-i



AS-i



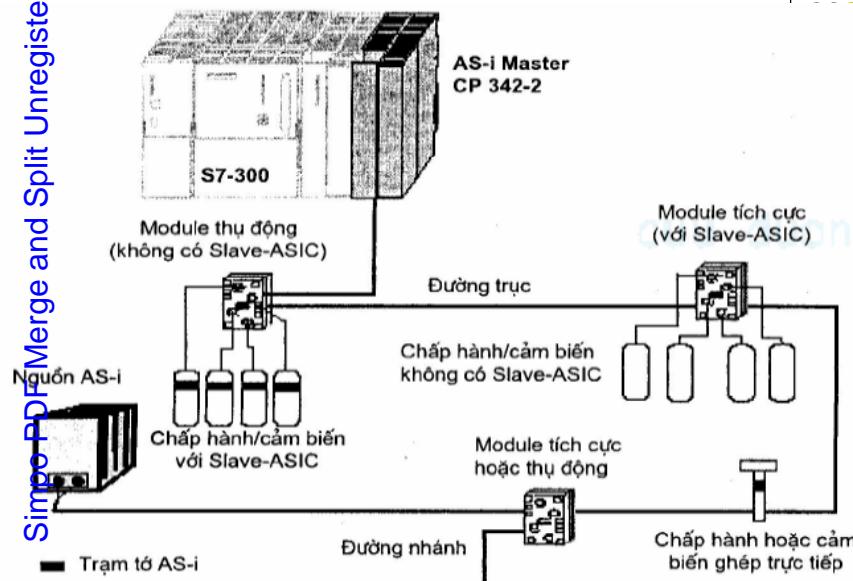
Simpo PDF Merge and Split Unregistered Version - http://www.simpopdf.com

cuu duong than cong. com

AS-i



AS-i



Simpo PDF Merge and Split Unregistered Version - http://www.simpopdf.com

AS-i Cơ chế giao tiếp

- Theo cơ chế Master/Slave.
- Trong một chu kỳ bus Master trao đổi với slave một lần theo phương pháp hỏi tuần tự (polling).
- Trạm chủ gửi bức điện có chiều dài 14 bit, 5bit địa chỉ và 5 bit dữ liệu.
- Nhận tín hiệu trả lời trong t/g định trước.
- Bản tin trả lời có chiều dài 7 bit, 4 bit dữ liệu.

AS-i

Có thể gửi các thông báo khác mà không ảnh hưởng đến chu kỳ bus.

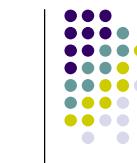
9 loại thông báo: hai phục vụ truyền số liệu và tham số, hai dùng để đặt địa chỉ, năm sử dụng để nhận dạng và xác định trạng thái trạm Slave.

AS-i

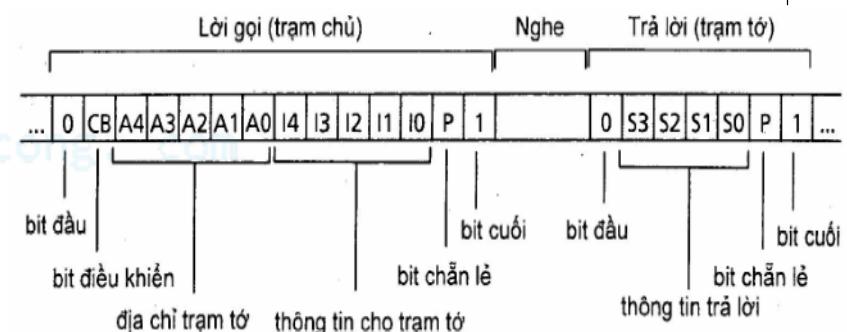
- Chu kỳ bus phụ thuộc vào số trạm.
- Chu kỳ bus tối đa là 5ms với 31 trạm.
- M/S cho mạch ghép nối trạm từ đơn giản, giá thành thực hiện thấp.
- Hệ thống linh hoạt.
- Có thể gửi riêng tín hiệu không trả lời không cần lặp lại cả chu kỳ.

cuuduongthancong.com

AS-i



AS-i Cấu trúc bức điện



AS-i

Trao đổi dữ liệu
Đặt tham số
Đặt địa chỉ
Reset tram tớ
Xóa địa chỉ mặc định
Đọc cấu hình vào/ra
Đọc mã căn cước
Đọc trạng thái
Đọc và xóa trạng thái

0	0	A4	A3	A2	A1	A0	0	D3	D2	D1	D0	P	1
0	0	A4	A3	A2	A1	A0	0	P3	P2	P1	P0	P	1
0	0	0	0	0	0	0	A4	A3	A2	A1	A0	P	1
0	1	A4	A3	A2	A1	A0	1	1	1	0	0	P	1
0	1	A4	A3	A2	A1	A0	0	0	0	0	0	P	1
0	1	A4	A3	A2	A1	A0	1	0	0	0	0	P	1
0	1	A4	A3	A2	A1	A0	1	0	0	0	1	P	1
0	1	A4	A3	A2	A1	A0	1	1	1	1	0	P	1
0	1	A4	A3	A2	A1	A0	1	1	1	1	1	P	1

AS-i

- Giữa yêu cầu và trả lời cần thời gian nghỉ từ 3-8 bit.

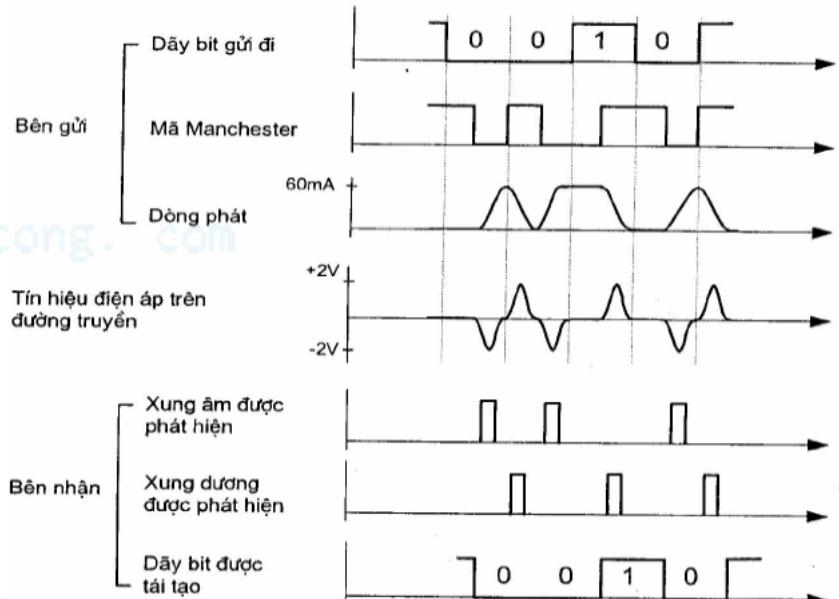
AS-i Mã hoá bit

Cáp hai dây thường suy hao mạnh khi tần số tăng, nhiễu CN nhiều -> hạn chế dải tần của tín hiệu.

Đơn giản, hiệu suất cao, khả năng đồng bộ nhịp, phối hợp phát hiện lỗi.

APM (Alternate Pulse Modulation)

AS-i



AS-i

- Xung áp gần hình sin -> dải tần hẹp tần số tín hiệu tương đương với tần số xung nhịp.
- Thay đổi tuần tự xung dương, âm triệt tiêu dòng một chiều.

AS-i

Chẵn lẻ có HD=2, nhưng tỉ lệ lỗi bit còn lại thấp.

• Khi $p=0,0012$ (200lần lỗi/s) thì $Ttmbf=10$ năm

AS-i Bảo toàn dữ liệu

- Bản tin ngắn, hiệu suất cáo.
- Kiểm tra chẵn lẻ và mã hoá bit hợp lý.
- Trong một chu kỳ bit (6uS) bên thu lấy mẫu tín hiệu 16 lần, mỗi chu kỳ phải có một hay hai xung, các xung kế tiếp phải đảo chiều -> chỉ có tín hiệu dạng này mới được nhận.
- Bức điện có chiều dài cố định, ngăn bởi các t/g nghỉ-> sai lệch cũng được phát hiện.
- Kiểm tra chẵn lẻ.

Mạng máy tính & Hệ thống thông tin công nghiệp

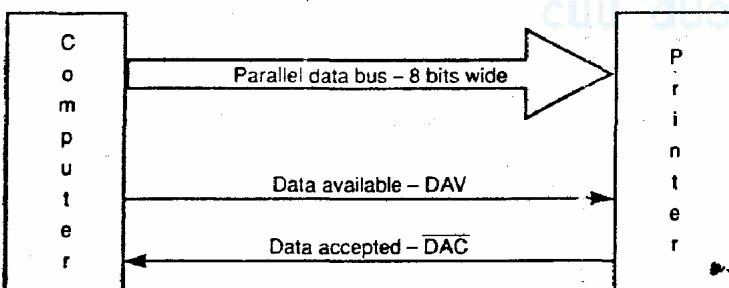
Đào Đức Thịnh
BM Kỹ thuật đo & THCN

Truyền song song.

- Máy tính lưu và xử lý số liệu theo từng từ (có độ dài -8,-16,-32,-64 bit).
- Dữ liệu sẽ được cấp theo dạng song song mỗi lần một từ, mỗi một bit có một đường dẫn riêng.
- Ta có 8 (16,32,64) dây dẫn song song nối giữa 2 điểm truyền đồng thời 8 (16,32,64) mức điện áp (0/1).
- Như vậy truyền song song là truyền từng byte (từ có độ dài 8,16,32,64 bit).
- Phương pháp truyền song song có tốc độ truyền cao, nó thường được sử dụng khi truyền bên trong các thiết bị hay giữa các linh kiện trên cùng một tấm mạch in,
- Tuy nhiên khi truyền ở khoảng cách xa phương pháp này có nhược điểm là tốn dây dẫn và có sự sai khác về mặt thời gian của các tín hiệu

cuuduongthancong.com

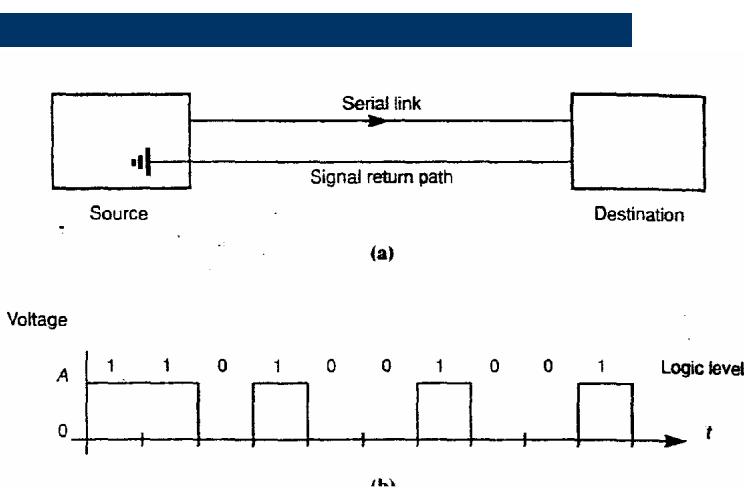
Truyền song song.



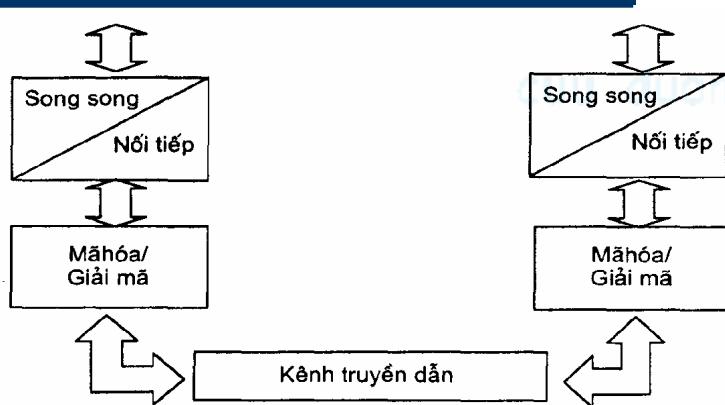
Truyền nối tiếp.

- Sử dụng hai dây dẫn nối giữa hai điểm. Các mức điện áp ON/OFF sẽ được truyền tuần tự với một chuẩn thời gian theo hai dây dẫn.
- Như vậy truyền nối tiếp là truyền từng bit
- Phương pháp này tuy có tốc độ thấp hơn phương pháp song song nhưng nó khắc phục được các hạn chế của phương pháp song song khi truyền ở khoảng cách xa.

Truyền nối tiếp.



Truyền nối tiếp.



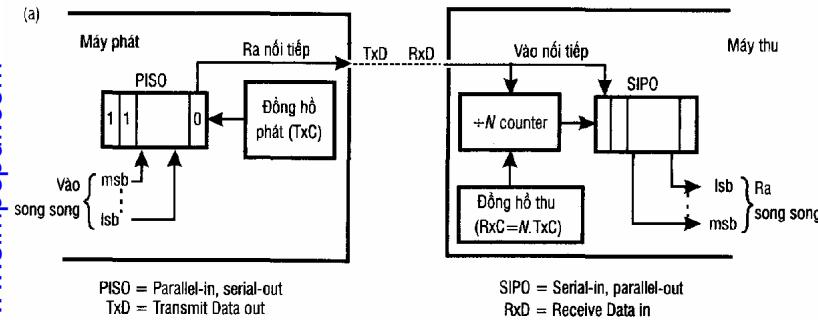
Truyền nối tiếp.

- Máy tính dù tồn tại ở dạng nào đều có các bộ VXL và bus song song và xử lý số liệu song song. Vì vậy, để có thể dùng phương pháp truyền nối tiếp, ta cần có các bộ chuyển đổi song song và nối tiếp

Truyền không đồng bộ

- Có thời gian nghỉ giữa các khung bản không cố định.
- Việc truyền được bắt đầu bởi 1 Start bit, các bit được truyền với một thông số định trước.
- Một đặc điểm quan trọng là thông số của cổng truyền phải giống nhau ở bên phát và bên thu để đảm bảo độ dài của chuỗi bit dữ liệu là như nhau.
- Trong truyền bất đồng bộ, đồng hồ thu chạy một cách bất đồng bộ với tín hiệu thu. Để xử lý tín hiệu thu, cần phải có kế hoạch dùng đồng hồ thu để lấy mẫu tín hiệu đến, ngay điểm giữa thời bit của dữ liệu
- Để đạt được điều này, tín hiệu đồng hồ thu nhanh gấp N lần đồng hồ phát và mỗi bit được dịch vào SIPO sau N chu kỳ xung đồng hồ

Truyền không đồng bộ



Truyền không đồng bộ

Nguyên tắc đồng bộ ký tự

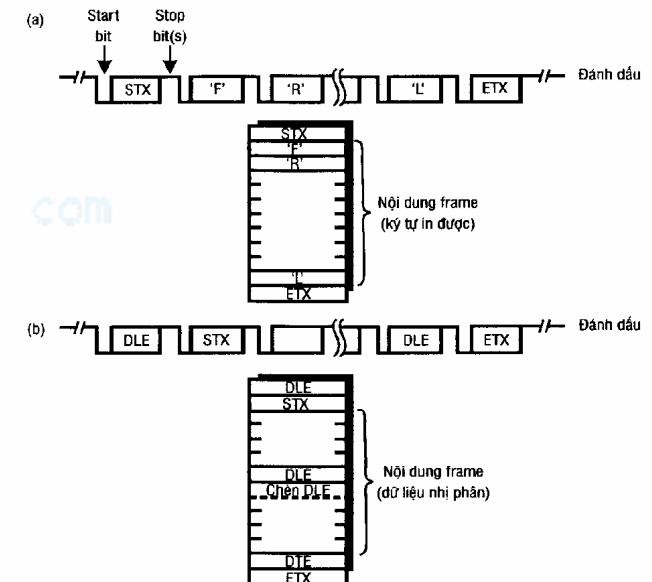
Mạch điều khiển truyền nhận được lập trình để hoạt động với số bit bằng nhau trong một ký tự kể cả số stop bit, start bit và bit kiểm tra giữa thu và phát. Sau khi phát hiện và nhận start bit, việc đồng bộ ký tự đạt được tại đầu thu rất đơn giản, chỉ việc đếm đúng số bit đã được lập trình. Sau đó sẽ chuyển ký tự nhận được vào thanh ghi đệm thu nội bộ và phát tín hiệu thông báo với thiết bị điều khiển (CPU) rằng đã nhận được một ký tự mới. Và sẽ đợi cho đến khi phát hiện một start bit kế tiếp.

Truyền không đồng bộ

Nguyên tắc đồng bộ frame

Khi thông điệp gồm một khối các ký tự thường xem như một frame thông tin (information frame) được truyền, bên cạnh việc đồng bộ bit và đồng bộ ký tự, máy thu còn phải xác định được điểm bắt đầu và điểm kết thúc một frame. Điều này được gọi là sự đồng bộ frame.

Truyền không đồng bộ

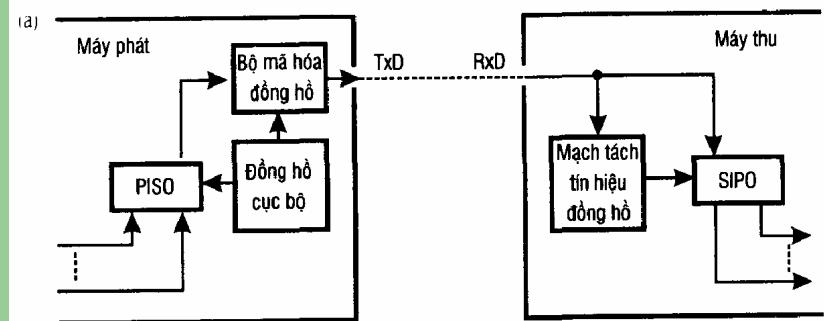


Truyền đồng bộ

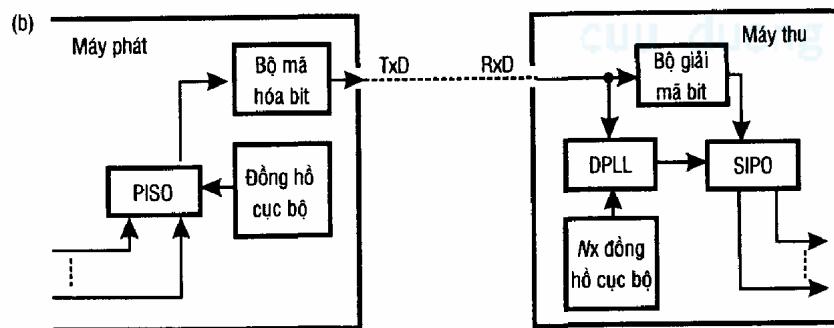
So với truyền không đồng bộ, truyền đồng bộ có một số khác biệt như là:

- Số liệu được truyền liên tục, không có các bit start, stop
- Có khung barker tin lớn hơn
- Cần có giao thức để điều khiển và ổn định luồng dữ liệu.
- Tuy nhiên, cũng giống như truyền bất đồng bộ chúng ta chỉ chấp nhận phương pháp nào cho phép máy thu đạt được sự đồng bộ bit, đồng bộ ký tự và đồng bộ frame.

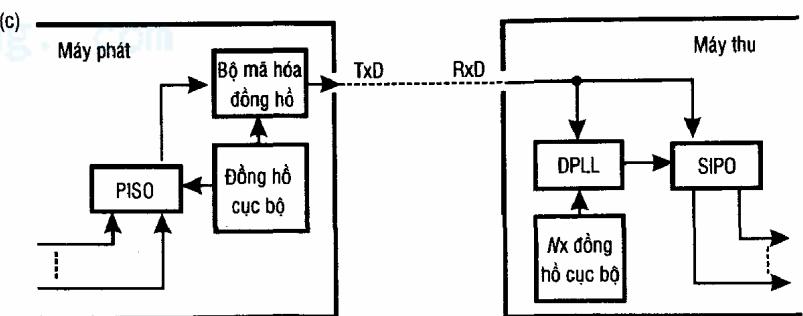
Truyền đồng bộ



Truyền đồng bộ



Truyền đồng bộ

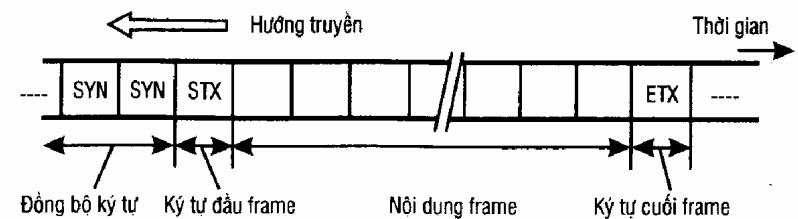


Truyền đồng bộ

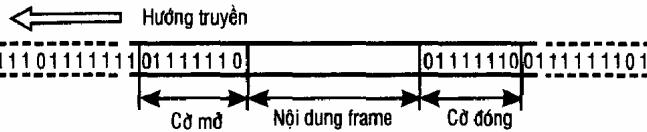
Truyền đồng bộ hướng ký tự:

Để thực hiện việc đồng bộ này, máy phát thêm vào các ký tự điều khiển truyền, gọi là các ký tự đồng bộ SYN, ngay trước các khối ký tự truyền. Các ký tự điều khiển này phải có hai chức năng: trước hết, chúng cho phép máy thu duy trì đồng bộ bit. Thứ hai, khi điều này đã được thực hiện, chúng cho phép máy thu bắt đầu biên dịch luồng bit thu theo các ranh giới ký tự chính xác **sự đồng bộ ký tự**.

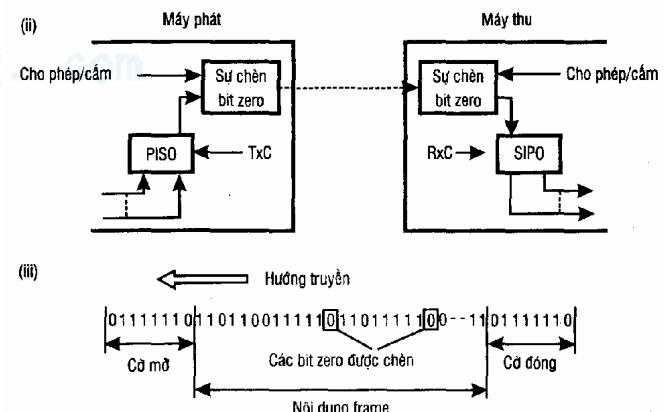
Truyền đồng bộ-Hướng bit



Truyền đồng bộ

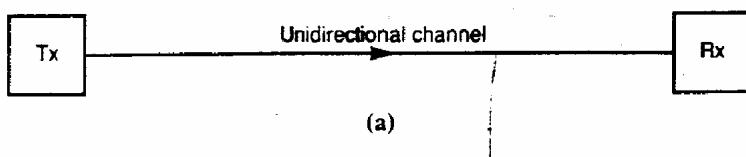


Truyền đồng bộ



Truyền 1 chiều (simplex)

Truyền đơn công (Simplex): Là hệ được thiết kế để truyền số liệu theo một chiều không cung cấp chiều ngược lại.



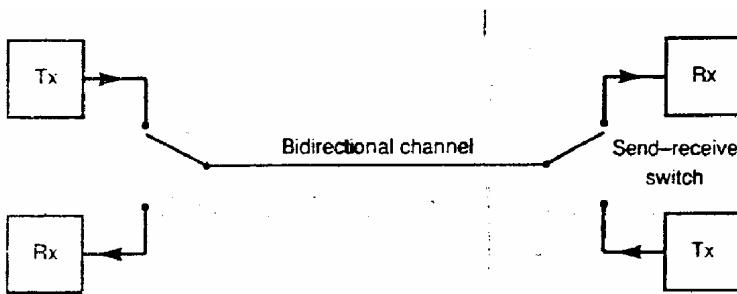
(a)

Truyền 2 chiều (duplex)

Hệ song công (Duplex): Là hệ được thiết kế để truyền số liệu theo cả hai chiều

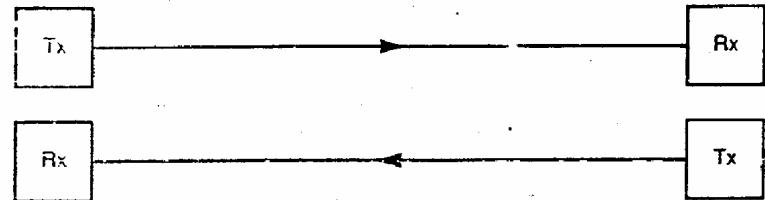
Truyền Half-duplex

Bán song công (Half Duplex): Là hệ có thể truyền số liệu theo cả hai chiều nhưng tại mỗi thời điểm chỉ thực hiện một chiều.



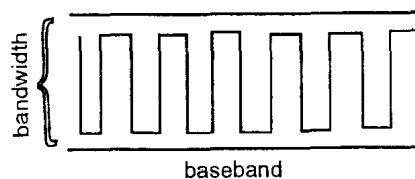
Truyền Full-duplex

Hệ song công (Full Duplex): Là hệ có thể truyền số liệu hai chiều một cách đồng thời



Truyền tải cơ sở

Một tín hiệu mang một nguồn thông tin có thể biểu diễn bằng tổng của nhiều dao động có tần số khác nhau nằm trong một phạm vi hẹp, được gọi là dải tần cơ sở (Base Band) hay dải hẹp. Tín hiệu được truyền đi cũng chính là tín hiệu được tạo ra sau khi mã hóa bit, nên có tần số cố định hoặc nằm trong một khoảng hẹp nào đó, tùy thuộc vào phương pháp mã hóa bit



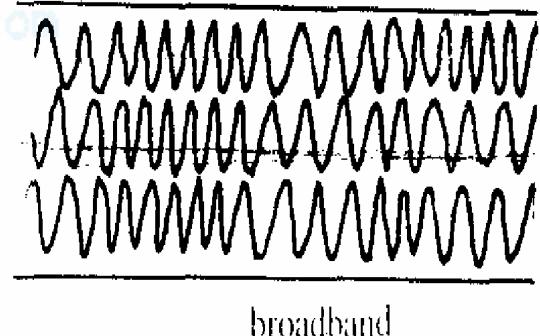
Truyền tải dải mang

Trong một số trường hợp, dải tần cơ sở không tương thích trong môi trường làm việc. Để khắc phục tình trạng này, người ta sử dụng một tín hiệu khác - gọi là tín hiệu mang, có tần số nằm trong một dải tần thích hợp - gọi là dải mang. Dải tần này thường lớn hơn nhiều so với tần số nhịp. Dữ liệu cần truyền tải sẽ dùng để điều chế tần số, biên độ hoặc pha của tín hiệu mang

Truyền tải dải rộng

Một tín hiệu có thể chứa đựng nhiều nguồn thông tin khác nhau bằng cách sử dụng kết hợp một cách thông minh nhiều thông số thông tin. Sau khi nhiều nguồn thông tin khác nhau đã được mã hóa bit, mỗi tín hiệu được tạo ra sẽ dùng để điều biến một tín hiệu khác, thường có tần số lớn hơn nhiều, gọi là tín hiệu mang. Các tín hiệu mang đã được điều biến có tần số khác nhau, nên có thể pha trộn, xếp chồng thành một tín hiệu duy nhất có phổ tần trải rộng. Đây chính là kỹ thuật dồn kênh phân tần trong truyền tải thông tin, nhằm mục đích sử dụng hiệu quả hơn đường truyền. Phía bên nhận sẽ thực hiện việc giải điều biến và phân kênh, hồi phục các tín hiệu mang các nguồn thông tin khác nhau.

Truyền tải dải rộng



Liên kết

* **Liên kết:** Liên kết (link) là mối quan hệ vật lý hoặc logic giữa hai hoặc nhiều đối tác truyền thông. Đối với liên kết vật lý, các đối tác chính là các trạm truyền thông được liên kết với nhau qua một môi trường vật lý.

Có thể phân biệt các kiểu liên kết sau đây:

- **Liên kết điểm-điểm (point-to-point):** Một mối liên kết chỉ có hai đối tác tham gia.
- **Liên kết điểm-nhiều điểm (multi-drop):** Trong một mối liên kết có nhiều đối tác tham gia, tuy nhiên chỉ một đối tác cố định duy nhất (trạm chủ) có khả năng phát trong khi nhiều đối tác còn lại (các trạm tớ) thu nhận thông tin cùng một lúc.

Liên kết

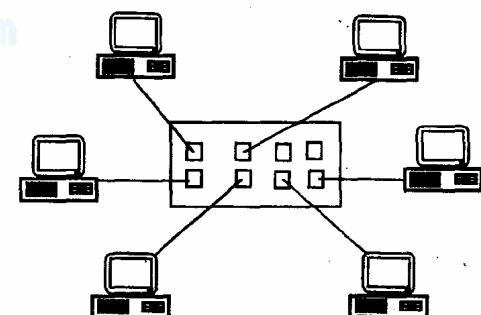
- **Liên kết nhiều điểm (Multipoint):** Trong một mối liên kết có nhiều đối tác tham gia và có thể trao đổi thông tin qua lại tự do theo bất kỳ hướng nào. Bất cứ một đối tác nào cũng có quyền phát và bất cứ trạm nào cũng nghe được. Cũng như kiểu liên kết điểm-nhiều điểm có thể sử dụng một cáp dẫn duy nhất để nối mạng giữa các đối tác.

Topology

* **Topology:**

Topology là cấu trúc liên kết của một mạng, hay nói cách khác chính là tổng hợp của các liên kết. Topology có thể hiểu là cách sắp xếp, tổ chức về mặt vật lý của mạng, nhưng cũng có thể là cách sắp xếp logic của các nút mạng, cách định nghĩa về tổ chức logic các mối liên kết giữa các nút mạng.

Cấu trúc mạng dạng sao



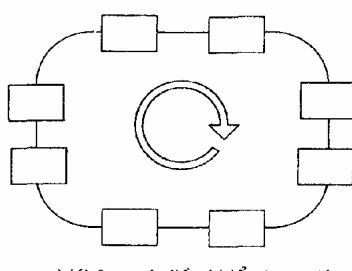
Cấu trúc mạng dạng sao

- Cấu trúc hình sao là một cấu trúc mạng tất cả các trạm được nối vào một trạm trung tâm
- Trạm trung tâm này sẽ điều khiển hoạt động truyền thông của toàn mạng.
- Tuỳ theo yêu cầu truyền thông trạm trung tâm có thể là một bộ chuyển mạch (switch), một bộ chọn đường (router) hay đơn giản là một bộ phân kênh.
- Ta có thể nhận thấy ở đây kiểu liên kết về mặt vật lý là điểm-điểm. Tuy nhiên, liên kết về mặt logic vẫn có thể là nhiều điểm. Nếu trạm trung tâm đóng vai trò tích cực, nó có thể đảm đương nhiệm vụ kiểm soát toàn bộ việc truyền thông của mạng, còn nếu không sẽ chỉ như một bộ chuyển mạch.

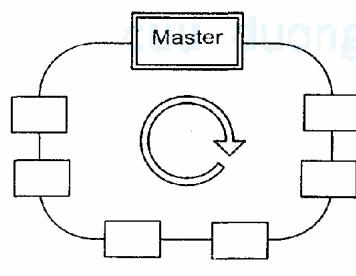
Cấu trúc mạng dạng sao

- Nhược điểm của cấu trúc hình sao là sự cố ở trạm trung tâm sẽ làm tê liệt toàn bộ các hoạt động truyền thông trong mạng, tổn dây dẫn và độ dài của dây nối với trạm trung tâm hạn chế.
- Ưu điểm của cấu trúc hình sao là lắp đặt đơn giản, dễ kiểm soát và khắc phục sự cố. Do sử dụng liên kết điểm-điểm do vậy có thể tận dụng tối đa tốc độ truyền của đường truyền vây lý.

Cấu trúc mạng dạng vòng



a) Không có điều khiển trung tâm



b) Có điều khiển trung tâm

Cấu trúc mạng dạng vòng

- Cấu trúc mạch vòng được thiết kế sao cho các thành viên trong mạng được nối từ điểm này đến điểm kia một cách tuần tự theo một mạch vòng khép kín.
- Trong vòng, tín hiệu được truyền đi theo một chiều qui định. Mỗi trạm nhận được dữ liệu từ trạm đứng trước và chuyển tiếp sang trạm lân cận đứng sau. Quá trình này được lặp lại tới khi dữ liệu quay trở về trạm đã gửi.
- Ưu điểm cơ bản của mạng cấu trúc theo kiểu này là mỗi một nút đồng thời có thể là một bộ khuếch đại, do vậy khi thiết kế mạng theo kiểu cấu trúc vòng có thể thực hiện với khoảng cách và số trạm rất lớn. Mỗi trạm có khả năng vừa nhận vừa phát tín hiệu cùng một lúc. Bởi mỗi thành viên ngăn cách vòng ra làm hai phần.

Cấu trúc mạng dạng vòng

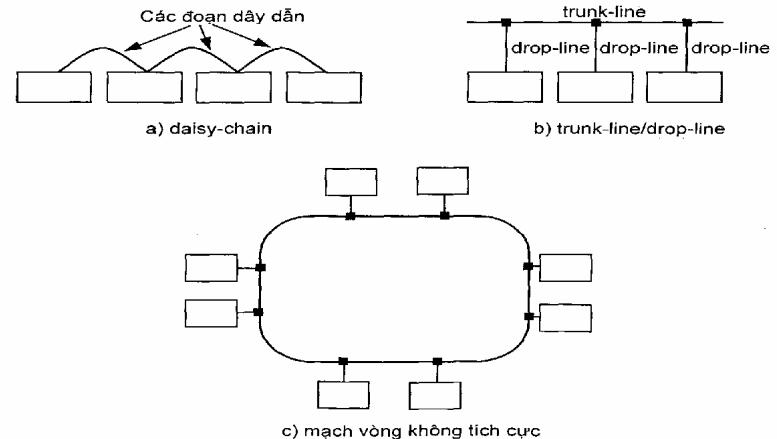
- Với kiểu mạch vòng không có điều khiển trung tâm, các trạm đều bình đẳng như nhau trong quyền nhận và phát tín hiệu. Như vậy việc kiểm soát đường dẫn sẽ do các trạm tự phân chia.
- Với kiểu có điều khiển trung tâm, một trạm chủ sẽ đảm nhiệm vai trò kiểm soát việc truy nhập đường dẫn.
- Cấu trúc mạch vòng thực chất dựa trên cơ sở liên kết điểm-điểm, vì vậy thích hợp cho việc sử dụng các phương tiện truyền tín hiệu hiện đại như cáp quang, tia hồng ngoại, v.v.
- Một ưu điểm tiếp theo của cấu trúc mạch vòng là khả năng xác định vị trí xảy ra sự cố, ví dụ đứt dây hay một trạm ngừng làm việc. Tuy nhiên, sự hoạt động bình thường của mạng còn trong trường hợp này chỉ có thể tiếp tục với một đường dây dự phòng. Mạng dạng vòng đòi hỏi phải có một giao thức điều khiển truy nhập đường truyền khá phức tạp.

cuuduongthancong.com

Cấu trúc mạng dạng Bus

- Trong cấu trúc đơn giản này, tất cả các thành viên của mạng đều được nối trực tiếp với một đường dẫn chung.
- Khi một trạm gửi tín hiệu ra Bus thì nó sẽ quảng bá tới tất cả các trạm còn lại.
- Đặc điểm cơ bản của cấu trúc bus là việc sử dụng chung một đường dẫn duy nhất cho tất cả các trạm, vì thế tiết kiệm được cáp dẫn và công lắp đặt.

Cấu trúc mạng dạng Bus



Cấu trúc mạng dạng Bus

- Bên cạnh việc tiết kiệm dây dẫn thì tính đơn giản, dễ thực hiện là những ưu điểm chính của cấu trúc bus,
 - Mạng cần phải có một giao thức để điều khiển việc truy nhập đường truyền.
- Ngoài việc cần phải kiểm soát truy nhập đường truyền, cấu trúc bus có những nhược điểm sau:
- Một tín hiệu gửi đi có thể tới tất cả các trạm và theo một trình tự không kiểm soát được, vì vậy phải thực hiện phương pháp gán địa chỉ (logic) theo kiểu thủ công cho từng trạm. Trong thực tế, công việc gán địa chỉ này gây ra không ít khó khăn.

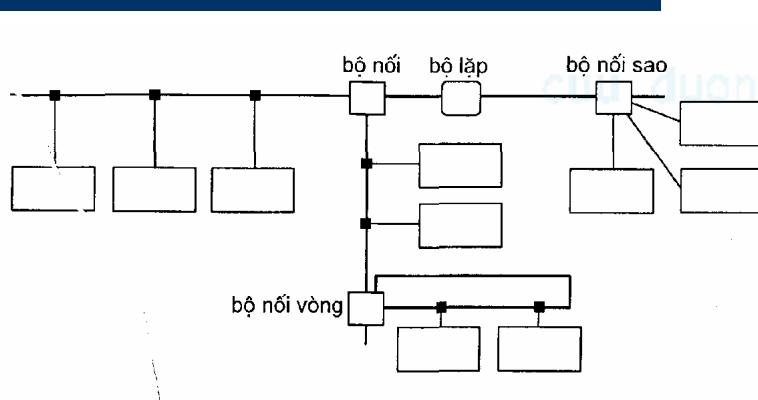
Cấu trúc mạng dạng Bus

- Tất cả các trạm đều có khả năng phát và phải luôn luôn nghe đường dẫn để phát hiện ra một thông tin có phải gửi cho mình hay không, nên phải được thiết kế sao cho đủ tải với số trạm tối đa. Đây chính là lý do phải hạn chế số trạm trong một đoạn mạng. Khi cần mở rộng mạng, phải dùng thêm các bộ lặp.
- Chiều dài dây dẫn thường tương đối dài, vì vậy đối với cấu trúc đường thẳng xảy ra hiện tượng phản xạ tại mỗi đầu dây làm giảm chất lượng của tín hiệu. Để khắc phục vấn đề này người ta chặn hai đầu dây bằng hai trở đầu cuối (Terminator). Việc sử dụng các trở đầu cuối cũng làm tăng tải của hệ thống.

Cấu trúc mạng dạng Bus

- Trường hợp đường dẫn bị đứt, hoặc do ngắn mạch trong phần kết nối bus của một trạm bị hỏng đều dẫn đến ngừng hoạt động của cả hệ thống. Việc định vị lỗi ở đây cũng gặp rất nhiều khó khăn.
- Cấu trúc đường thẳng, liên kết đa điểm gây khó khăn trong việc áp dụng các công nghệ truyền tín hiệu mới như sử dụng cáp quang.

Cấu trúc mạng dạng cây



Điều khiển truy nhập đường truyền

- Trong một mạng có cấu trúc bus, hay dạng vòng, các thành viên phải chia nhau một đường dẫn chung.
- Để tránh sự xung đột về tín hiệu gây ra sai lệnh về thông tin, ở mỗi thời điểm trên một đường dẫn chỉ duy nhất một điện tín được phép truyền đi. Chính vì vậy mạng phải được điều khiển sao cho tại một thời điểm nhất định chỉ một thành viên trong mạng được gửi thông tin đi. Còn số lượng thành viên trong mạng muốn nhận thông tin thì không hạn chế.
- Một trong những vấn đề quan trọng hàng đầu ảnh hưởng tới chất lượng của mỗi hệ thống là phương pháp phân chia thời gian gửi thông tin trên đường dẫn hay phương pháp *truy nhập đường truyền*.

Điều khiển truy nhập đường truyền

- Phương pháp truy nhập đường truyền là một trong những vấn đề cơ bản đối với các hệ thống, bởi mỗi phương pháp có những ảnh hưởng khác nhau tới các tính năng kỹ thuật của hệ thống. Cụ thể, ta phải quan tâm tới ít nhất 3 khía cạnh: độ tin cậy, tính năng thời gian, hiệu xuất sử dụng đường truyền.

Các phương pháp điều khiển truy nhập đường truyền có thể chia thành hai nhóm chính:

- Điều khiển truy nhập ngẫu nhiên: việc truy nhập không được qui định chặt chẽ trước mà xảy ra hoàn toàn ngẫu nhiên theo nhu cầu của các trạm.

- Điều khiển truy nhập có điều khiển: Trình tự truy nhập được xác định rõ ràng từ trước. Việc truy nhập được kiểm soát chặt chẽ theo cách tập trung hay phân tán bởi các thành viên.

CSMA/CD

Carrier Sense Multiple Access with Collision Detection-*Phương pháp đa truy nhập sử dụng sóng mang có phát hiện xung đột*

- Phương pháp truy nhập ngẫu nhiên này được sử dụng cho topo dạng bus, trong đó tất cả các trạm của mạng được nối trực tiếp vào bus.

- Mọi trạm đều có thể truy nhập vào bus chung (đa truy nhập) một cách ngẫu nhiên và do vậy rất có thể dẫn đến xung đột (hai hoặc nhiều trạm đồng thời truyền dữ liệu).

- Dữ liệu được truyền đi theo khuôn dạng chuẩn trong đó có vùng thông tin điều khiển chứa địa chỉ của dữ liệu.

CSMA/CD

- CSMA/CD là phương pháp cải tiến từ phương pháp CSMA, hay còn gọi là LBT (Listen Before Talk - Nghe trước khi nói). Tư tưởng của nó là : một trạm cần truyền dữ liệu trước hết phải "nghe" xem đường truyền xem đang rỗi hay bận. Nếu rỗi thì truyền dữ liệu đi (theo khuôn dạng chuẩn). Ngược lại, nếu đường truyền đang bận (đã có dữ liệu khác) thì trạm phải thực hiện theo một trong 3 giải thuật sau (thường gọi là các giải thuật "kiên nhẫn"-persistent algorithms) :

- (1) Trạm tạm "rút lui" chờ đợi trong một thời đoạn ngẫu nhiên nào đó rồi 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 (1-persistent)
- (3) Trạm tiếp tục "nghe" đến khi đường truyền rỗi thì truyền đi với xác suất p xác định trước ($0 < p < 1$) (p-persistent).

CSMA/CD

- Việc xảy ra xung đột thường là do độ trễ truyền dẫn : một trạm truyền dữ liệu (cùng sóng mang) đi rồi nhưng do độ trễ truyền dẫn nên một trạm khác lúc đó đang "nghe" đường truyền sẽ tưởng là rỗi và cứ thế truyền dữ liệu đi. Mấu chốt vấn đề là ở chỗ : vì các trạm chỉ "nghe trước khi nói" mà không "nghe trong khi nói" nên thực tế có xung đột nhưng các trạm vẫn không hay biết gì và vẫn cứ tiếp tục truyền dữ liệu đi, gây ra việc chiếm dụng đường truyền một cách vô ích.

CSMA/CD

Để có thể phát hiện xung đột, CSMA/CD-hay còn gọi là LWT(Listen While Talk-Nghe trong khi nói) đã bổ sung thêm qui tắc :

- Khi một trạm đang truyền nó vẫn tiếp tục "nghe" đường truyền.Nếu phát hiện thấy xung đột thì nó ngừng ngay việc truyền nhưng vẫn tiếp tục gửi tín hiệu sóng mang thêm một thời gian nữa để đảm bảo rằng tất cả các trạm trên mạng đều có thể "nghe" được sự kiện xung đột đó.
- Sau đó trạm chờ đợi trong một thời đoạn ngẫu nhiên nào đó rồi thử truyền lại theo các qui tắc của CSMA

CSMA/CD

- Rõ ràng với CSMA/CD, thời gian chiếm dụng vô ích đường truyền được giảm xuống bằng thời gian dùng để phát hiện một xung đột.
- Ưu điểm của CSMA/CD là tính chất đơn giản, linh hoạt, việc ghép thêm hay bỏ đi một trạm trong mạng không ảnh hưởng gì tới hoạt động của hệ thống.
- Nhược điểm của CSMA/CD là tính bất định của thời gian phản ứng, hiệu xuất sử dụng đường truyền vì thế cũng thấp.

CSMA/CA

(Carrier Sense Multiple Access with Collision Avoidance)

- Sử dụng cho Topo mạng dạng Bus. Tương tự như CSMA/CD, mỗi trạm đều phải nghe đường dẫn trước khi gửi cũng như sau khi gửi thông tin.
- Ở đây sử dụng một phương pháp mã hóa bit thích hợp để trong trường hợp xảy ra xung đột, một tín hiệu "trội" (dominant) sẽ lấn át tín hiệu kia "lặn" (recessive).
- Nếu một trạm gửi đi tín hiệu "lặn" mà giám sát về tín hiệu "trội" thì nó sẽ mất quyền ưu tiên và phải dừng truyền. Sau đó trạm sẽ chờ một thời gian ngẫu nhiên nào đó và thử nghe lại đường truyền.

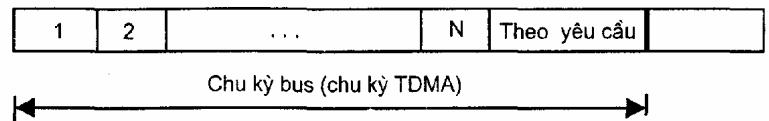
CSMA/CA

- Mỗi bức điện đều được bắt đầu bằng một dãy bit đặc biệt được gọi là cờ hiệu, sau đó là tới các phần khác như thông tin kiểm soát, địa chỉ,...
- Phương pháp CSMA/CA, có thể sử dụng mức ưu tiên cho mỗi trạm (hoặc theo loại thông tin) và gắn mã ưu tiên vào phần đầu sau cờ hiệu của mỗi bức điện.
- Nhờ có phương pháp sử dụng mức ưu tiên mà tính năng thời gian thực của hệ thống được cải thiện. Có thể thấy rõ, tuy bị hạn chế về tốc độ truyền và chiều dài dây dẫn, hiệu suất sử dụng đường truyền ở phương pháp này rất cao. Các trạm chỉ gửi thông tin đi khi có nhu cầu và nếu xảy ra xung đột thì một trong hai bức điện vẫn tiếp tục được gửi đi.

TDMA (Time Division Multiple Access):

- Sử dụng cho Topo mạng dạng Bus. Trong phương pháp kiểm soát truy nhập phân chia thời gian TDMA, mỗi trạm được phân một thời gian truy nhập bus nhất định. Các trạm có thể lần lượt thay nhau gửi thông tin trong khoảng thời gian cho phép gọi là khe thời gian hay lát thời gian (time slot, time slice) theo một tuần tự qui định sẵn. Việc phân chia này được thực hiện trước khi hệ thống đi vào hoạt động (tiền định).
- Hệ thống có thể hoạt động không có trạm chủ. Trong trường hợp có một trạm chủ thì vai trò của nó chỉ hạn chế ở mức độ kiểm soát việc tuân thủ đảm bảo giữ đúng lát thời gian của các trạm khác. Mỗi trạm đều có khả năng đảm nhiệm vai trò chủ động trong giao tiếp trực tiếp với các trạm khác.

TDMA (Time Division Multiple Access):



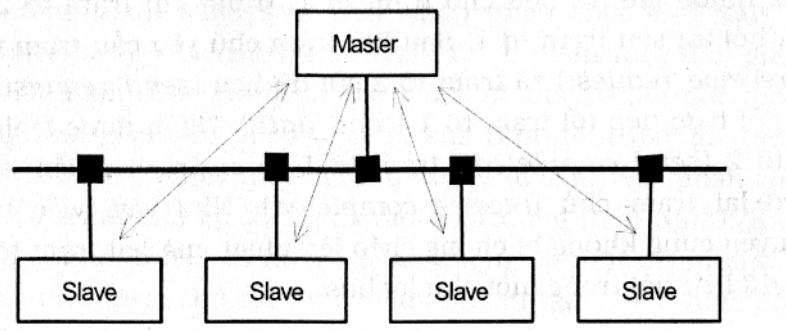
TDMA (Time Division Multiple Access):

- Ngoài các lát thời gian phân chia cố định cho các trạm dùng để trao đổi dữ liệu định kỳ (đánh số từ 1 tới N), thường còn có một khoảng dự trữ dành cho việc trao đổi dữ liệu bất thường theo yêu cầu, ví dụ gửi thông tin cảnh báo, mệnh lệnh đặt cấu hình, dữ liệu tham số, setpoint..

Master/Slave

- Sử dụng cho cấu trúc mạng dạng Bus. Trong phương pháp chủ/tớ, một trạm chủ (master) có trách nhiệm chủ động phân chia quyền truy nhập bus cho các trạm tớ (slave).
- Các trạm tớ đóng vai trò bị động, chỉ có quyền truy nhập bus và gửi tín hiệu đi khi có yêu cầu. Trạm chủ có thể dùng phương pháp hỏi tuần tự (polling) theo chu kỳ để kiểm soát toàn bộ hoạt động giao tiếp của cả hệ thống.

Master/Slave



Master/Slave

- Phương pháp chủ/tớ có một ưu điểm là việc kết nối mạng các trạm tớ đơn giản, đỡ tốn kém bởi gần như toàn bộ "trí tuệ" tập trung tại trạm chủ. Một trạm chủ thường là một thiết bị điều khiển, vì vậy việc tích hợp thêm chức năng xử lý truyền thông là điều không khó khăn.

- Một nhược điểm của phương pháp kiểm soát tập trung chủ/tớ là hiệu suất trao đổi thông tin giữa các trạm tớ bị giảm do phải dữ liệu phải đi qua khâu trung gian là trạm chủ, dẫn đến giảm hiệu suất sử dụng đường truyền.

Master/Slave

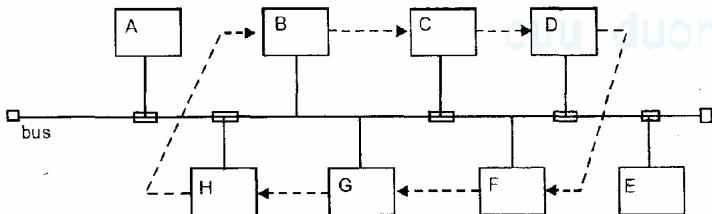
- Trong một số hệ thống, thậm chí các trạm tớ không có quyền giao tiếp trực tiếp với nhau, mà bắt cứ dữ liệu cần trao đổi nào cũng phải qua trạm chủ. Nếu hoạt động giao tiếp diễn ra theo chu kỳ, trạm chủ sẽ có trách nhiệm chủ động yêu cầu dữ liệu từ trạm tớ cần gửi và sau đó sẽ chuyển tới trạm tớ cần nhận. Trong trường hợp một trạm tớ cần trao đổi dữ liệu bất thường với một trạm khác phải thông báo yêu cầu của mình khi được trạm chủ hỏi đến và sau đó chờ được phục vụ. Trình tự tham gia giao tiếp, hay trình tự hỏi/đáp của các trạm tớ có thể do người dùng qui định trước (tiền định) bằng các công cụ đặt cấu hình.

Master/Slave

- Một hạn chế nữa của phương pháp này là độ tin cậy của hệ thống truyền thông phụ thuộc hoàn toàn vào một trạm chủ duy nhất. Trong trường hợp có xảy ra sự cố trên trạm chủ thì toàn bộ hệ thống truyền thông ngừng làm việc. Một cách khắc phục là sử dụng một trạm tớ đóng vai trò giám sát trạm chủ và có khả năng thay thế trạm chủ khi cần thiết.

Token Bus

- Phương pháp này sử dụng cho topo mạng dạng Bus.
- Nguyên lý của phương pháp này là : để cấp phát quyền truy nhập đường truyền cho các trạm đang có nhu cầu truyền dữ liệu, một thẻ bài được lưu chuyển trên một vòng lôgic thiết lập bởi các trạm đó.
- Khi một trạm nhận được thẻ bài thì nó có quyền sử dụng đường truyền trong một thời gian xác định trước. Trong thời gian đó nó có thể truyền một hay nhiều đơn vị dữ liệu. Khi đã hết dữ liệu hoặc hết thời gian cho phép, trạm phải chuyển thẻ bài đến trạm tiếp theo trong vòng lôgic.



→ Đường truyền vật lý
→ Vòng lôgic

Token Bus

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

Token Bus

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

- **Bổ sung một trạm vào vòng lôgic :** các trạm nằm ngoài vòng lôgic cần được xem xét định kỳ để nếu có nhu cầu truyền dữ liệu thì bổ sung vào vòng lôgic.
- **Loại bỏ một trạm khỏi vòng lôgic :** khi một trạm không còn nhu cầu truyền dữ liệu cần loại nó ra khỏi vòng lôgic để tối ưu hóa việc điều khiển truy nhập bằng thẻ bài.
- **Quản lý lỗi :** một số lỗi có thể xảy ra, chẳng hạn trùng địa chỉ (hai trạm đều nghĩ rằng đến lượt mình) hoặc "đứt vòng" không trạm nào nghĩ tới lượt mình.
- **Khởi tạo vòng lôgic :** khi cài đặt mạng hoặc sau khi "đứt vòng", cần phải khởi tạo lại vòng.

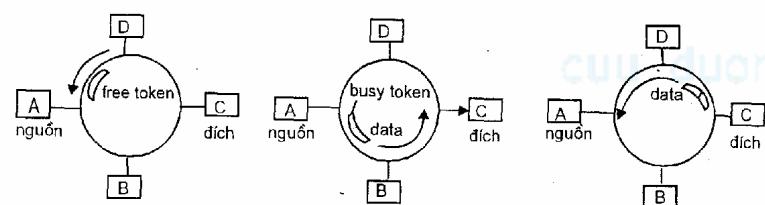
Token Ring

- Phương pháp này áp dụng cho Topo dạng vòng.
- Phương pháp này cũng dựa trên nguyên lý dùng thẻ bài để cấp phát quyền truy nhập đường truyền. Nhưng ở đây thẻ bài lưu chuyển theo vòng vật lý chứ không cần thiết lập vòng lôgic như đối với phương pháp Token Bus.

Token Ring

- 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 "rỗi"* (*free*) . Khi đó trạm sẽ đổi bit trạng thái của thẻ bài thành "*bận*" (*busy*) và truyền một đơn vị dữ liệu cùng với thẻ bài đi theo chiều của vòng. Giờ đây không còn thẻ bài "*rỗi*" trên vòng nữa, do đó các trạm có dữ liệu cần truyền cũng phải đợi. Dữ liệu đến trạm đích sẽ được sao lại, sau đó cùng với thẻ bài đi tiếp cho đến khi quay về trạm nguồn. Trạm nguồn sẽ xóa bỏ dữ liệu và đổi bit trạng thái trở về "*rỗi*" và cho lưu chuyển tiếp trên vòng để các trạm khác có thể nhận được quyền truyền dữ liệu.

Token Ring



A có dữ liệu cần truyền đến C. Nhận được thẻ bài "*rỗi*", nó đổi bit trạng thái thành "*bận*" và truyền dữ liệu đi cùng với thẻ bài.

Trạm đích C sao dữ liệu dành cho nó và chuyển tiếp dữ liệu cùng thẻ bài đi về hướng trạm nguồn A sau khi đã gửi thông tin báo nhận vào đơn vị dữ liệu.

A nhận được dữ liệu cùng thẻ bài quay về, đổi bit trạng thái của thẻ bài thành "*rỗi*" và chuyển tiếp trên vòng, xóa dữ liệu đã truyền.

Token Ring

- Sự quay về lại trạm nguồn của dữ liệu và thẻ bài nhằm tạo một cơ chế báo nhận (acknowledgment) 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.

Token Ring

- Trong phương pháp 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. Có thể có nhiều giải pháp khác nhau cho hai vấn đề này. Sau đây là một giải pháp được khuyến nghị :
 - Đối với vấn đề mất thẻ bài, có thể qui định trước một trạm điều khiển chủ động (active monitor). Trạm này sẽ phát hiện tình trạng mất thẻ bài bằng cách dùng cơ chế ngưỡng thời gian (time-out) và phục hồi bằng cách phát đi một thẻ bài "rồi" mới.

Token Ring

- Đối với vấn đề thẻ bài "bận" lưu chuyển không dừng, trạm monitor sử dụng một bit trên thẻ bài (gọi là monitor bit) để "đánh dấu" (đặt giá trị 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 "rồi" và chuyển tiếp trên vòng. Các trạm còn lại trên vòng sẽ có vai trò bị động : chúng theo dõi phát hiện tình trạng sự cố của trạm monitor chủ động và thay thế vai trò đó.

Mạng máy tính & Hệ thống thông tin công nghiệp

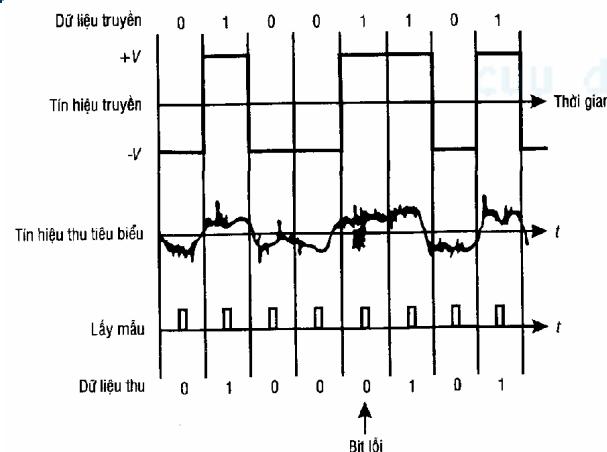
Đào Đức Thịnh
BM Kỹ thuật đo & THCN

Môi trường truyền dẫn và chuẩn vật lý

* Tổng quan: Để truyền dữ liệu nhị phân qua một đường dây, các bit nhị phân truyền đi phải được chuyển thành các tín hiệu điện. Ví dụ có thể truyền một bit nhị phân 1 bằng cách đặt lên đường dây biên độ điện thế +V và truyền bit nhị phân 0 với mức điện thế -V. Khi nhận các tín hiệu điện này, thiết bị thu sẽ dịch +V thành 1 và -V thành 0. Trong thực tế, các tín hiệu điện được truyền đi bị suy giảm và méo dạng bởi môi trường truyền, đôi khi bộ thu không thể phân tách đâu là tín hiệu 1 và đâu là tín hiệu 0.

cuuduongthancong.com

Môi trường truyền dẫn và chuẩn vật lý



Môi trường truyền dẫn và chuẩn vật lý

Mức độ suy giảm và méo dạng chịu ảnh hưởng nhiều nhất bởi:

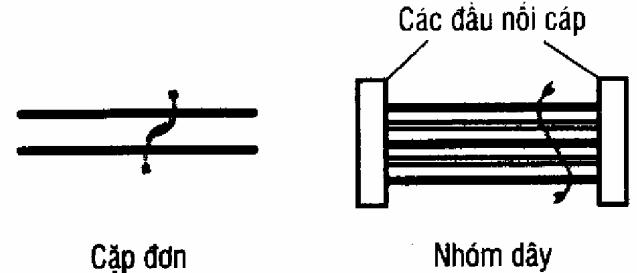
- Loại môi trường truyền
- Tốc độ bit đang truyền
- Cự ly giữa hai thiết bị truyền.

Vì sự suy giảm và méo dạng trong các loại môi trường truyền và các thành phần vật lý khác nhau là khác nhau, nên các tiêu chuẩn quốc tế đã được định nghĩa cho giao tiếp điện giữa hai chủng loại thiết bị truyền dữ liệu.

Môi trường truyền dẫn và chuẩn vật lý

Các chuẩn này không chỉ định nghĩa các mức tín hiệu điện được dùng mà còn chỉ ra cách thức áp dụng và ý nghĩa của bất kỳ tín hiệu điều khiển nào cùng với các tiêu chuẩn được dùng tại giao tiếp vật lý. Trong hầu hết các trường hợp chúng ta sẽ xem xét là giao tiếp của một máy tính với các thành phần giao tiếp truyền số liệu khác nhau, nhưng thường dùng thuật ngữ 'thiết bị đầu cuối' DTE (Data Terminal Equipment) thay cho 'máy tính', đó là ngụ ý cho bất kỳ loại thiết bị đầu cuối nào.

Cáp hai dây không xoắn



Cáp hai dây không xoắn

Một đường truyền 2 dây không xoắn là môi trường truyền dẫn đơn giản nhất. Mỗi dây cách ly với dây kia và cả hai xuyên tự do (không xoắn nhau) qua môi trường không khí. Loại đường dây này thích hợp cho kết nối hai thiết bị cách xa nhau đến 50m dùng tốc độ bit nhỏ hơn 19,2kbps. Tín hiệu thường là mức điện thế hay cường độ dòng điện dựa vào tham chiếu điện thế đất (Ground, không cân bằng) đặt lên một dây trong khi điện thế đất được đặt vào dây kia.

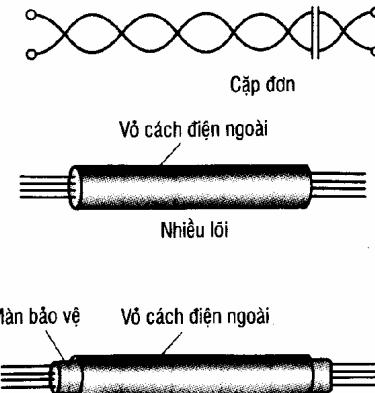
Cáp hai dây không xoắn

Mặc dù một đường hai dây có thể được dùng để nối hai máy tính một cách trực tiếp, nhưng thường dùng nhất là cho kết nối một DTE đến một thiết bị kết nối mạch dữ liệu cục bộ DCE (Data Communication Equipment), ví dụ như Modem. Các kết nối như vậy thường dùng dây đa đường, cách tổ chức thông thường là cách ly riêng một dây cho mỗi tín hiệu và một dây nối đất (Ground). Bộ dây hoàn chỉnh được bọc trong một cáp nhiều lõi được bảo vệ hay dưới dạng một hộp cáp.

Cáp hai dây không xoắn

Với loại dây này cần phải cẩn thận tránh can nhiễu giữa các tín hiệu điện trong các dây dẫn kề nhau trong cùng một cáp. Hiện tượng này gọi là nhiễu xuyên âm. Ngoài ra cấu trúc không xoắn khiến chúng dễ bị thâm nhập bởi các tín hiệu nhiễu bắt nguồn từ các nguồn tín hiệu khác do bức xạ điện từ. Các yếu tố ảnh hưởng này đồng thời tạo ra giới hạn về cự ly cũng như tốc độ truyền.

Cáp hai dây xoắn



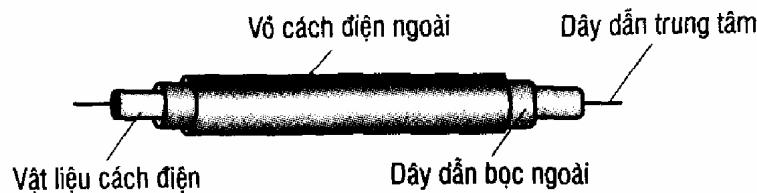
Cáp hai dây xoắn

Chúng ta có thể loại bỏ các tín hiệu nhiễu bằng cách dùng cáp xoắn đôi, trong đó một cặp dây xoắn lại với nhau. Sự xấp xỉ các đường dây tham chiếu đất và dây tín hiệu có ý nghĩa khi bất kỳ tín hiệu nhiễu nào thâm nhập thì sẽ vào cả hai dây, ảnh hưởng của chúng sẽ giảm đi bởi sự triệt lấn nhau. Hơn nữa, nếu có nhiều cặp xoắn trong cùng một cáp thì sự xoắn của mỗi cặp trong cáp cũng làm giảm nhiễu xuyên âm.

Cáp hai dây xoắn

Các đường dây xoắn đôi cùng với mạch phát và thu thích hợp lợi dụng các ưu điểm có được từ phương pháp hình học sẽ là đường truyền tốc độ xấp xỉ 1 Mbps qua cự ly ngắn (ngắn hơn 100m) và tốc độ thấp hơn qua cự ly dài hơn. Các mạch thu phát phức tạp cho phép tốc độ cao hơn qua cự ly dài hơn. Các đường dây này được gọi là cáp xoắn đôi không bảo vệ UTP (Unshielded Twisted Pair), được dùng rộng rãi trong mạng điện thoại và trong nhiều ứng dụng truyền số liệu. Đối với các cặp xoắn được bảo vệ STP (Shielded Twisted Pair), có dùng thêm một lớp bảo vệ để giảm hơn nữa ảnh hưởng của nhiễu.

Cáp đồng trục



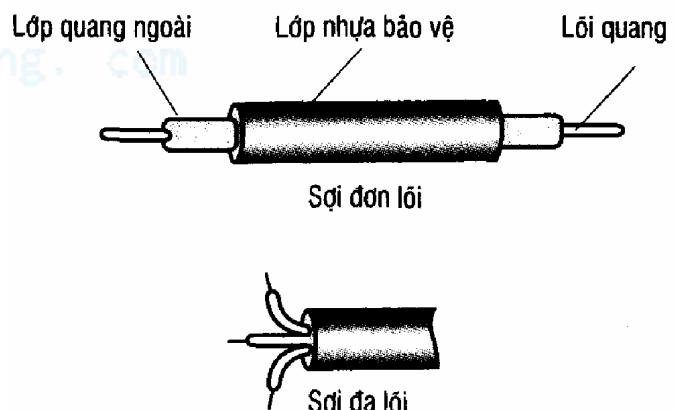
Cáp đồng trục

Dây tín hiệu trung tâm được bảo vệ hiệu quả đối với các tín hiệu xuyên nhiễu từ ngoài nhờ lưới dây bao quanh bên ngoài. Chỉ suy hao lượng tối thiểu do bức xạ điện từ và hiệu ứng ngoài da do có lớp dây dẫn bao quanh. Cáp đồng trục có thể dùng với một số loại tín hiệu khác nhau, nhưng thông dụng nhất là dùng cho tốc độ 10 Mbps trên cự ly vài trăm mét, nếu dùng điều chế tốt thì có thể đạt được thông số cao hơn.

Cáp đồng trục

- Các yếu tố giới hạn chính đối với cáp xoắn là khả năng truyền và hiện tượng được gọi là 'hiệu ứng ngoài da'. Khi tốc độ bit truyền gia tăng, dòng điện chạy trên đường dây có khuynh hướng chỉ chạy trên bề mặt ngoài của dây dẫn, do đó dùng rất ít phần dây có sẵn. Điều này lại làm tăng trở kháng của đường dây đối với các tín hiệu có tần số cao, dẫn đến suy hao lớn đối với tín hiệu.
- Ngoài ra, với tần số cao thì năng lượng tín hiệu bị tiêu hao nhiều do ảnh hưởng bức xạ.
Cáp đồng trục tối thiểu được hai ảnh hưởng trên.

Cáp quang



Cáp quang

- Mặc dù có nhiều cải tiến nhưng các loại cáp kim loại vẫn bị giới hạn về tốc độ truyền dẫn. Cáp quang khác xa với các loại cáp trước đây, cáp quang mang thông tin dưới dạng các chùm dao động của ánh sáng trong sợi thủy tinh. Sóng ánh sáng có băng thông rộng hơn sóng điện từ, điều này cho phép cáp quang đạt được tốc độ truyền khá cao lên đến hàng trăm Mbps.
- Sóng ánh sáng cũng "miễn dịch" đối với các nhiễu điện từ và nhiễu xuyên âm. Cáp quang cũng cực kỳ hữu dụng trong việc truyền các tín hiệu tốc độ thấp trong môi trường xuyên nhiễu năng ví dụ như điện cao thế, chuyển mạch.
- Ngoài ra còn dùng trong các nơi có nhu cầu bảo mật, vì rất khó mắc xen rẽ (câu trộm) về mặt vật lý.

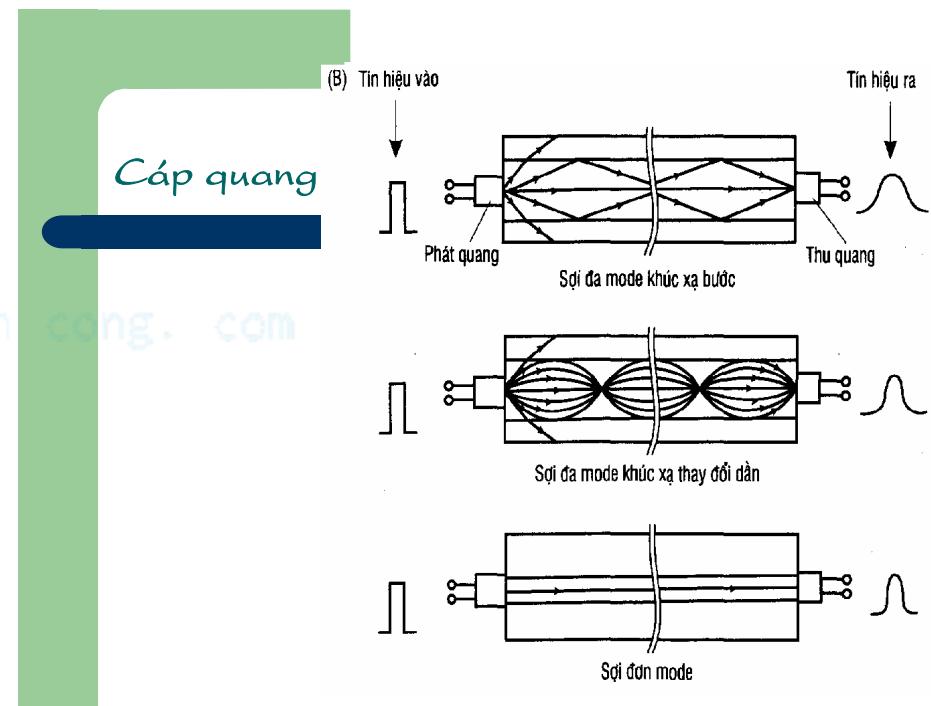
Cáp quang

Bản thân sợi quang gồm hai phần: lõi thủy tinh và lớp phủ thủy tinh có hệ số khúc xạ thấp. ánh sáng lan truyền dọc theo lõi thủy tinh theo một trong ba cách phụ thuộc loại và bề rộng của vật liệu lõi được dùng.

ánh sáng có thể truyền trên cáp theo ba chế độ truyền:

Cáp quang

- Một cáp quang bao gồm một sợi thủy tinh cho mỗi tín hiệu được truyền, được bọc bởi một lớp phủ bảo vệ ngăn ngừa bất kỳ nguồn sáng nào từ bên ngoài. Tín hiệu ánh sáng phát ra bởi một bộ phát quang, thiết bị này thực hiện chuyển đổi các tín hiệu điện thông thường từ một đầu cuối dữ liệu thành tín hiệu quang. Một bộ thu quang được dùng để chuyển ngược lại (từ quang sang điện) tại máy thu. Thông thường bộ phát quang là diode phát quang hay laser thực hiện chuyển đổi tín hiệu điện thành tín hiệu quang. Các bộ thu dùng các photodiode cảm quang hay photo transistor.



Cáp quang

Trong chế độ đa mode khúc xạ bước-multimode *stepped index* vật liệu phủ và lõi khác nhau nhưng hệ số khúc xạ ổn định không thay đổi. Tất cả các ánh sáng phát ra bởi diode có góc phát nhỏ hơn góc tới hạn được phản xạ tại giao tiếp giữa lớp phủ và lõi và lan truyền trong lõi. Tùy vào góc phát mà ánh sáng sẽ mất một lượng thời gian để lan truyền dọc theo dây. Do đó tín hiệu nhận được có bề rộng xung rộng hơn xung gốc.

Cáp quang

Sự phân tán có thể được hạn chế bằng cách dùng vật liệu lõi có hệ số khúc xạ thay đổi hay đa mode khúc xạ tăng dần-*multimode graded index*, ánh sáng bị khúc xạ một lượng lớn khi di chuyển ra xa lõi. Điều này làm hẹp bề rộng xung của tín hiệu nhận, nhờ đó cho phép gia tăng tốc độ bit.

Cáp quang

Một cải tiến cao hơn có thể đạt được bằng cách giảm đường kính lõi đến chiều dài bước sóng đơn (3-10um) để tất cả các ánh sáng phát ra sẽ truyền theo một hướng dọc ống dẫn sóng (sợi quang cũng thường được gọi là ống dẫn sóng), và sợi quang dùng phương pháp này gọi là sợi đơn mode -*monomode fiber*, nhờ vậy bề rộng xung nhận được sẽ xấp xỉ bề rộng xung gốc, nhờ đó tăng được tốc độ truyền.

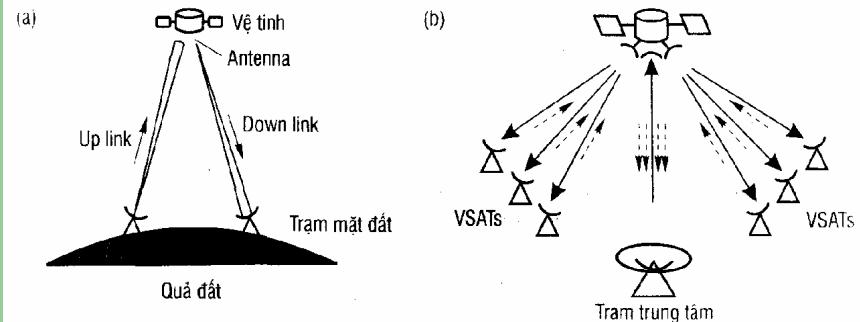
Truyền qua vệ tinh

- Số liệu cũng có thể được truyền bằng cách dùng sóng điện từ qua không gian tự do như trong các hệ thống thông tin vệ tinh.
- Một chùm sóng vi ba trực xạ trên đó mang số liệu đã được điều chế, được truyền đến vệ tinh từ trạm mặt đất. Chùm sóng này được thu và được truyền lại đến các đích xác định trước nhờ một mạch tích hợp thường được gọi là transponder. Một vệ tinh có nhiều transponder, mỗi transponder đảm trách một băng tần đặc biệt. Mỗi kênh vệ tinh thông thường đều có một băng thông cực cao (500MHZ) và có thể cung cấp cho hàng trăm liên kết tốc độ cao thông qua kỹ thuật ghép kênh.

Truyền qua vệ tinh

- Các vệ tinh dùng cho mục đích liên lạc thường thuộc dạng địa tĩnh. Quỹ đạo của vệ tinh được chọn sao cho đường truyền thẳng với trạm thu phát ở mặt đất, mức độ chuẩn trực của chùm sóng truyền lại từ vệ tinh có thể không cao để tín hiệu có thể được tiếp nhận trên một vùng rộng lớn, hoặc có thể hội tụ tốt để chỉ thu được trên một vùng giới hạn. Trong trường hợp thứ hai tín hiệu có năng lượng lớn cho phép dùng các bộ thu có đường kính nhỏ hơn thường gọi là chảo parabol, là các đầu cuối có độ mở rất nhỏ hay VSAT (Very Small Aperture Terminal).

Truyền qua vệ tinh



Truyền qua kênh vi ba

Các liên kết vi ba mặt đất được dùng rộng rãi để thực hiện các liên kết thông tin khi không thể hay quá đắt tiền để thực hiện một môi trường truyền vật lý. Ví dụ khi vượt sông, sa mạc, dồi núi hiểm trở .v.v. Khi chùm sóng vi ba trực xạ đi xuyên ngang môi trường khí quyển, nó có thể bị nhiễu bởi nhiều yếu tố như địa hình và các điều kiện thời tiết bất lợi. Tuy nhiên, liên lạc vi ba trực xạ xuyên môi trường khí quyển có thể dùng một cách tin cậy cho cự ly truyền dài hơn 50km.

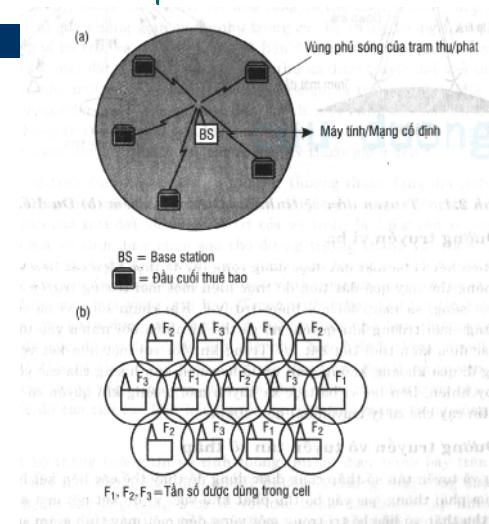
Truyền vô tuyến tần số thấp.

- Sóng vô tuyến tần số thấp cũng được dùng để thay thế các liên kết hữu tuyến có cự ly vừa phải thông qua các bộ thu phát khu vực. Ví dụ kết nối một số lớn các máy tính thu thập số liệu bố trí trong một vùng đến một máy tính giám sát số liệu từ xa, hay kết nối các máy tính trong một thành phố đến máy cục bộ hay ở xa.

- Sẽ rất tốn kém khi lắp đặt các cáp dẫn hữu tuyến cho các ứng dụng như vậy. Sóng vô tuyến thường được dùng để thực hiện các liên kết không dây giữa một điểm kết cuối hữu tuyến và các máy tính phán tán. Một trạm phát vô tuyến được gọi là trạm cơ bản (base station) được đặt tại điểm kết cuối hữu tuyến.

Truyền vô tuyến tần số thấp.

- Cần nhiều trạm cơ bản cho các ứng dụng yêu cầu phạm vi rộng và mật độ phân bố user cao. Phạm vi bao phủ của mỗi trạm cơ bản là giới hạn, do sự giới hạn nguồn phát của nó, nó chỉ đủ kênh để hỗ trợ cho toàn bộ tải trong phạm vi đó.
- Phạm vi rộng hơn có thể được thực hiện bằng cách tổ chức đa trạm theo cấu trúc tế bào (cell). Trong thực tế, kích thước của mỗi tế bào thay đổi và được xác định bởi các yếu tố như mật độ đầu cuối và địa hình cục bộ. Mỗi trạm cơ bản dùng một dải tần khác với trạm kế. Tuy nhiên, vì vùng phủ của mỗi trạm có giới hạn nên có thể dùng lại băng tần của nó cho các phần khác của mạng.



Truyền vô tuyến tần số thấp.

- Các trạm cơ bản được kết nối thành mạng hữu tuyến. Thông thường, tốc độ số liệu của mỗi máy tính trong một tế bào (cell) đạt được vài chục kbps. Dạng tổ chức tương tự có thể được dùng trong một tòa cao ốc để cung cấp các liên kết không dây cho thiết bị máy tính trong mỗi phòng.

Các hiện tượng ảnh hưởng đến tín hiệu trên đường truyền

* Suy hao:

- Khi một tín hiệu lan truyền theo dây dẫn thì biên độ của nó sẽ bị giảm xuống và người ta gọi là sự suy hao của tín hiệu.
- Thông thường mức độ suy giảm cho phép được qui định trên chiều dài cáp dẫn để đảm bảo rằng hệ thống nhận có thể phát hiện và dịch được tín hiệu ở máy thu.
- Nếu trường hợp cáp quá dài thì có một hay nhiều bộ khuếch đại (hay còn gọi là repeater) được thêm vào từng khoảng dọc theo cáp nhằm tiếp nhận và tái sinh tín hiệu.

Các hiện tượng ảnh hưởng đến tín hiệu trên đường truyền

- Sự suy giảm tín hiệu gia tăng theo một hàm của tần số, trong khi đo tín hiệu lại bao gồm một vài tần vì vậy tín hiệu sẽ bị biến dạng do các thành phần suy hao khác nhau. Để khắc phục vấn đề này, các bộ khuếch đại được thiết kế sao cho khuếch đại các tín hiệu có tần số khác nhau với hệ số khuếch đại khác nhau. Ngoài ra còn có thiết bị cân chỉnh gọi là *equalizer* được dùng để cân bằng sự suy hao trong một băng tần xác định.
- Sự suy hao và sự khuếch đại được đánh giá và đo lường bằng đơn vị decibels (dB).

$$\text{dB} = 10 \log_{10} P_1/P_2 \text{ (dB).}$$

Các hiện tượng ảnh hưởng đến tín hiệu trên đường truyền

- * Băng thông của đường truyền:
- Bất kỳ một kênh hay đường truyền nào: cáp xoắn, cáp đồng trực, radio đều có một băng thông xác định liên hệ với nó, băng thông chỉ ra các thành phần tần số nào của tín hiệu sẽ được truyền qua kênh mà không bị suy giảm quá nhiều.
- Băng thông $B = f_{\max} - f_{\min}$
- Công thức Nyquist xác định tốc độ tối đa của kênh trong trường hợp không nhiễu với băng thông của kênh như sau:

$$\text{MTR} = 2 B \log_2 M \text{ (bps)}$$
- B - Băng thông kênh tính bằng Hz.
- M - Số mức trên một phân tử tín hiệu.
- MTR (Max Transfer Rate) - Tín băng bps

Các hiện tượng ảnh hưởng đến tín hiệu trên đường truyền

- * Biến dạng xung do trễ:
- Tốc độ lan truyền của một tín hiệu thuần nhất đọc theo một đường truyền thay đổi tùy tần số.
- Khi truyền một tín hiệu số, nó có thể phân tích ra thành một loạt các thành phần có tần số khác nhau (phân tích Fourier) các thành phần tần số khác nhau tạo nên nó sẽ đến máy thu với độ trễ pha khác nhau, dẫn đến biến dạng do trễ của tín hiệu tại máy thu.
- Sự biến dạng sẽ gia tăng khi tốc độ bit tăng. Khi các thành phần có tần số khác nhau của tín hiệu giao thoa với nhau người ta gọi đó là hiện tượng tự giao thoa.
- Méo do trễ gây khó khăn cho việc lấy mẫu tín hiệu.

Các hiện tượng ảnh hưởng đến tín hiệu trên đường truyền

- * Sự can nhiễu (tạp âm-noise):
- Một thông số quan trọng của đường truyền là tỉ số giữa tín hiệu và tạp âm - người ta gọi là SNR - được đo bằng dB.

$$\text{SNR} = 10 \log_{10}(S/N) \text{ (dB)}$$
- S - Công suất tín hiệu tính bằng W.
- N - Công suất tạp âm tính bằng W.

Các hiện tượng ảnh hưởng đến tín hiệu trên đường truyền

- Rõ ràng nếu tỉ số SNR cao thì chất lượng tín hiệu thu cao, SNR thấp thì chất lượng tín hiệu thu thấp.

- Tốc độ truyền tối đa của kênh có liên hệ chặt chẽ với tỉ số SNR và được xác định theo công thức Shannon-Harley:

$$MTR = B \log_2(1+S/N) \text{ (bps)}$$

B - băng thông tính bằng Hz

S - công suất tín hiệu tính bằng W.

N - Công suất ồn tính bằng W.

Các chuẩn vật lý

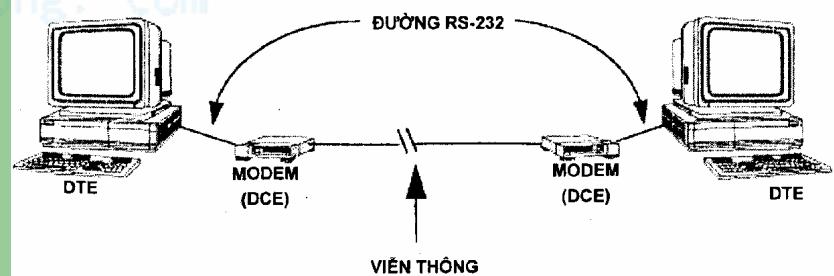
Truyền dữ liệu nồi tiếp, không đồng bộ là phương pháp được sử dụng chủ yếu trong việc kết nối các DTE và DCE cũng như trong hệ thống mạng công nghiệp. Với phương pháp này, các bit được truyền từ bên gửi tới bên nhận một cách tuần tự trên cùng một đường truyền. Cũng chính vì không có một đường dây riêng biệt mang tín hiệu nhịp, nên việc đồng bộ hóa thuộc trách nhiệm do bên gửi và bên nhận thỏa thuận trên cơ sở một giao thức truyền thông. Vậy ta cần phải có chuẩn vật lý cho phần thu và phát.

RS-232

- RS-232 (tương ứng với chuẩn châu Âu là CCITT V.24) lúc đầu được xây dựng phục vụ chủ yếu trong việc ghép nối điểm-điểm giữa hai thiết bị đầu cuối, giữa máy tính và máy in, hoặc giữa một thiết bị đầu cuối và một thiết bị truyền dữ liệu.

- Mặc dù tính *năng hạn chế*, RS-232 là một trong các chuẩn tín hiệu có từ lâu nhất, vì thế được sử dụng rất rộng rãi. Ngày nay, mỗi máy tính cá nhân đều có một vài cổng RS-232 (cổng COM), có thể sử dụng tự do để nối với các thiết bị ngoại vi hoặc với các máy tính khác. Nhiều thiết bị công nghiệp cũng tích hợp cổng RS-232 phục vụ lập trình hoặc tham số hóa.

RS-232



RS-232

- + Đặc tính điện học:
 - RS-232 sử dụng phương thức truyền không đối xứng, tức là sử dụng tín hiệu điện áp chênh lệch giữa một dây dẫn và đất.
 - Mức điện áp logic được định nghĩa $-3V \div -25V$ mức logic "1" và $+3V \div +25V$ mức logic "0".
 - Tốc độ truyền dẫn tối đa phụ thuộc vào chiều dài dây dẫn. Đa số các hệ thống hiện nay chỉ hỗ trợ tới tốc độ 19.2 kbps
 - Chiều dài cho phép 15m (50 feet).
 - Truyền số liệu Full-duplex sử dụng 3 dây: TxD, RxD, GND.
 - Các tín hiệu điều khiển dùng để bắt tay (Handshaking) phần cứng là: RTS, CTS, DSR, DTR. Mức logic: $+3V \div +25V \rightarrow "1"$ và $<0V \rightarrow "0"$.

RS-232

- Truyền không đồng bộ, cấu trúc một khung truyền bao gồm: 1 start bit, 7-8 data bit, 1-0 parity bit, 1-1,5-2 stop bit.

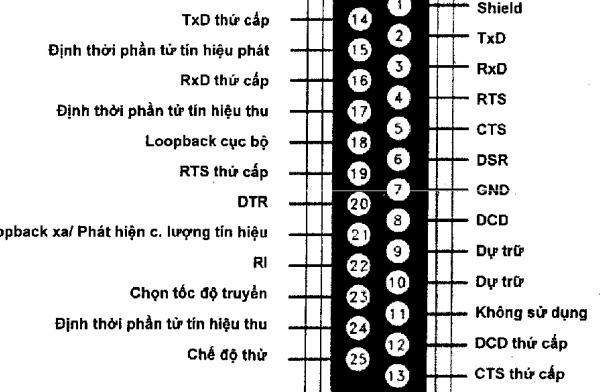
(Gần đây, sự tiến bộ trong vi mạch đã góp phần nâng cao tốc độ của cổng RS-232 lên nhiều lần so với tốc độ 19,2kbps. Hiện nay đã có những mạch thu phát đạt tốc độ 460kbps và hơn nữa, tuy nhiên tốc độ truyền dẫn thực tế lớn hơn 1 15.2 kbps theo chuẩn RS-232 trong một hệ thống làm việc dựa vào ngắt là một điều khó có thể thực hiện).

RS-232

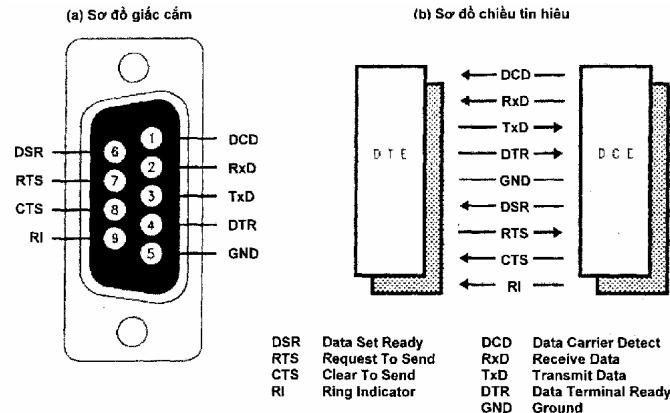
- + Giao diện cơ học:

Chuẩn RS-232 qui định ba loại giắc cắm RS-232 là DB-9, DB-25 và ALT-A, trong đó hai loại đầu được sử dụng rộng rãi hơn.

RS-232



RS-232



RS-232

- RXD (*receive Data*): Đường nhận dữ liệu.
- TXD (*Transmit Data*): Đường gửi dữ liệu.
- DTR (*Data Terminal Ready*): Báo DTE sẵn sàng. Chân DTR thường ở trạng thái ON khi thiết bị đầu cuối sẵn sàng thiết lập kênh truyền thông (tự động quay số hay tự động trả lời). DTR ở trạng thái OFF chỉ khi thiết bị đầu cuối không muốn DCE của nó chấp nhận lời gọi từ xa.
- DSR (*Data Set Ready*): Báo DCE sẵn sàng, ở chế độ trả lời, 1 tone trả lời và DSR ON sau 2 giây khi Modem nháy máy.
- DCD (*Data Carrier Detect*): Tín hiệu này tích cực khi Modem nhận được tín hiệu từ trạm từ xa và nó duy trì trong suốt quá trình liên kết.

RS-232

- RTS (*Request To Send*): Đường RTS kiểm soát chiều truyền dữ liệu. Khi một trạm cần gửi dữ liệu, nó đóng mạch RTS sang ON để báo hiệu với modem của nó.
- CTS (*Clear To Send*): Khi CTS chuyển sang ON, Modem xác nhận là DTE có thể truyền số liệu. Quá trình ngược lại nếu đổi chiều truyền số liệu
- RI (*Ring Indicator*): Khi modem nhận được tín hiệu chuông, RI chuyển ON/OFF một cách tuần tự với chuông điện thoại để báo hiệu cho trạm đầu cuối. Tín hiệu này chỉ thị rằng một modem xa yêu cầu thiết lập liên kết dial-up.

RS-232

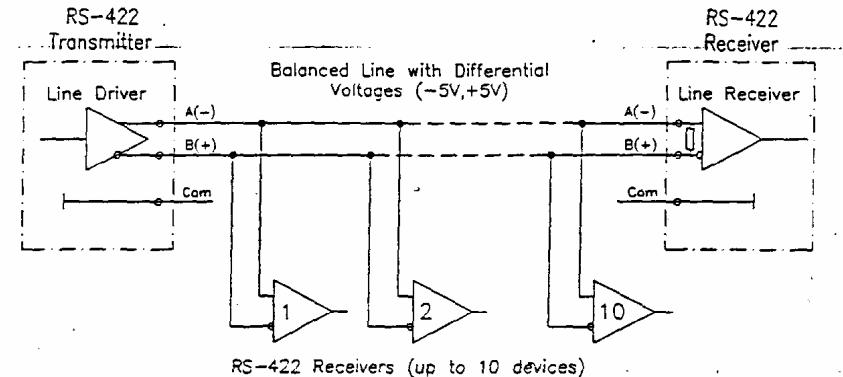
- + Các hạn chế khi ứng dụng RS-232 trong CN:
 - Giao diện thông tin P-P hạn chế khi kết nối 1 vài thiết bị thông minh với nhau.
 - Khoảng cách 15 mét là quá ngắn cho phần lớn các ứng dụng trong CN
 - Tốc độ 19,2 kbps là thấp cho nhiều ứng dụng.
 - Mức điện áp không thực sự tương thích với chuẩn nguồn thiết bị công nghiệp.

RS-422

Đây là chuẩn thông tin đối xứng sử dụng một cặp dây (A-B) cho mỗi tín hiệu, nhờ vậy mà nó có thể giảm được nhiễu, hận chế tối đa các vấn đề do sự thay đổi điện thế đất gây ra, nó phù hợp với các ứng dụng truyền ở tốc độ cao, khoảng cách truyền xa.

- Khoảng cách truyền tối đa 1200m.
- Tốc độ truyền tối đa 10 Mbps.
- Có 1 bộ phát và 10 bộ thu trên một đường truyền.
- Mức Logic: $-2V \div -6V \rightarrow "1"$,
 $+2V \div +6V \rightarrow "0"$

RS-422



RS-422

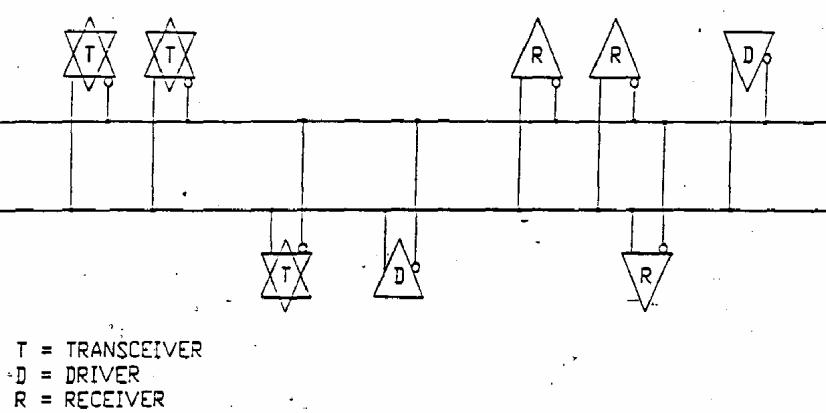
- Chuẩn RS-422 là sự sai khác $\pm 5V$ giữa hai dây do vậy có thể dùng nguồn cung cấp đơn 5V cho bộ phát.
- Truyền ở chế độ Full-duplex sử dụng 5 dây.
- Điểm cuối của đường truyền RS-422 có một trở kháng để cân bằng với trở kháng của đường dây. Giá trị thường dùng là $Z=120\Omega$.

RS-485

Chuẩn RS-485 tương tự như RS-422 nhưng nó có số bộ thu phát trên một đường truyền nhiều hơn. Các đặc điểm chính của RS-485 như sau:

- Khoảng cách truyền tối đa 1200m.
- Tốc độ truyền tối đa 10 Mbps.
- Có 32 bộ phát và 32 bộ thu trên một đường truyền.
- Mức Logic: $-1.5V \div -6V \rightarrow "1"$,
 $+1.5V \div +6V \rightarrow "0"$

RS-485



RS-485

- Các nút mạng phải được đánh địa chỉ và phải có một giao thức điều khiển truy nhập đường truyền. Các đầu ra phải có mạch hạn dòng để tránh hỏng hóc khi có xung đột xảy ra.
- Điểm cuối của đường truyền RS-485 có một trở kháng để cân bằng với trở kháng của đường dây. Giá trị thường dùng là $Z_0=100-120\Omega$.
- Để tăng khoảng cách truyền và số trạm ta cần phải dùng các bộ Repeater.

RS-485

- Chuẩn RS-485 là sự sai khác $\pm 5V$ giữa hai dây do vậy có thể dùng nguồn cung cấp đơn 5V cho bộ phát.
- Truyền ở chế độ Full-duplex sử dụng 5 dây.
- Truyền ở chế độ Half-duplex sử dụng 3 dây.
- Bộ phát của RS-485 có thể hoạt động ở 3 trạng thái: mức logic "1", mức logic "0" và trạng thái cao trào (có thể hiểu như trạng thái cấm và được điều khiển bằng một chân tín hiệu).
- Có 32 bộ phát trên một đường truyền nhưng tại một thời điểm chỉ có một cái hoạt động.

MBP (JEC 1158-2):(Manchester Coded, Bus-powered)

Đây là một kỹ thuật truyền dẫn được đưa ra trong chuẩn IEC 1158-2 cũ nhằm vào các ứng dụng điều khiển quá trình trong công nghiệp chế biến như lọc dầu, hóa chất, nơi có yêu cầu nghiêm ngặt về an toàn cháy nổ và nguồn cung cấp cho các thiết bị trường.

- MBP sử dụng mã Manchester, cho phép đồng tải nguồn trên đường bus, chế độ truyền đồng bộ và tốc độ truyền 31,25 kbit/s.
- Về mặt tín hiệu, thực chất MBP cũng sử dụng phương thức truyền đối xứng, với cáp đôi dây xoắn và trở đầu cuối là 100Ω .
- Mức điện áp tối đa được qui định nằm trong khoảng 0,75-1V.

MBP (JEC 1158-2): (Manchester Coded, Bus-powered)

Các nguyên tắc đảm bảo an toàn cho việc truyền dẫn trong môi trường dễ cháy nổ được đưa ra:

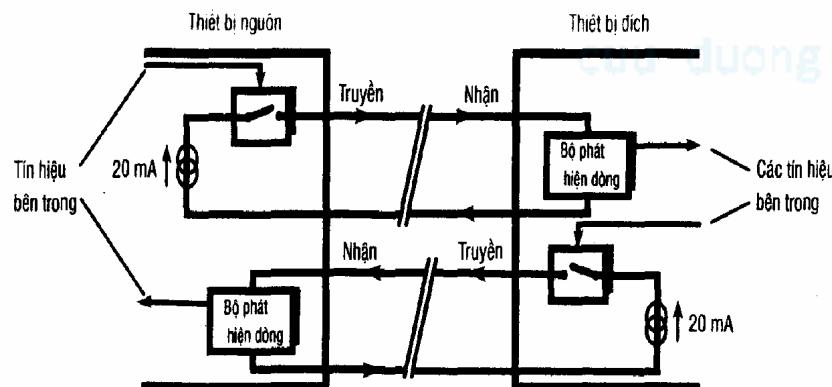
- Một đoạn mạng chỉ được phép có một bộ nguồn cung cấp điện.
- Trong trạng thái bình thường, mỗi thiết bị trường tiêu hao một dòng cơ sở cố định ($> 10 \text{ mA}$).
- Mỗi thiết bị trường hoạt động như một bộ tiêu hao dòng bị động.
- Mỗi đầu dây được kết thúc bằng một trở đầu cuối bị động.

20mA Current-loop

- Một dạng tín hiệu khác có thể chọn bên cạnh RS-232 là giao tiếp vòng 20mA. Tên của giao tiếp này ngụ ý rằng dùng tín hiệu là dòng điện thay cho điện áp. Mặc dù không mở rộng tốc độ nhưng nó tăng khoảng cách vật lý giữa hai thiết bị thông tin.

- Hoạt động chính là trạng thái của chuyển mạch được điều khiển bởi luồng bit dữ liệu truyền: chuyển mạch đóng tương ứng với bit 1, do đó cho dòng 20mA qua, và ngược lại chuyển mạch mở cho bit 0, do đó không cho dòng 20mA qua. Tại đầu thu dòng điện được phát hiện bởi mạch cảm biến dòng và các tín hiệu nhị phân được tái tạo lại. Giao tiếp này loại bỏ nhiễu tốt hơn so với giao tiếp điều khiển bằng điện áp, phù hợp với đường dây dài (đến 1km), nhưng tốc độ vừa phải.

20mA Current-loop



Truyền không đối xứng

- Một tín hiệu chỉ có một dây truyền tín hiệu điện áp so với dây đất.
- Dây đất chung cho nhiều tín hiệu khác nhau vì vậy đòi hỏi có trở kháng nhỏ.
- Khi truyền ở khoảng cách xa không có chung điện thế đất.

Truyền đối xứng

- Sử dụng một cặp dây cho một tín hiệu.
- Triệt tiêu được sự ảnh hưởng của nhiễu.
- Tránh được sự sai khác điện thế đất.
- Thích hợp cho trường hợp truyền ở tốc độ cao, khoảng cách xa và trong môi trường có nhiễu lớn.

Các tiêu chuẩn mã hoá đường truyền

- Tần số của tín hiệu.
- Thông tin đồng bộ hóa.
- Triệt tiêu dòng một chiều.
- Bền vững với nhiễu và có khả năng nhận biết lỗi.

NRZ,RZ

- NRZ (*Non-return To Zero*), RZ (*Return to Zero*) là một trong những phương pháp được sử dụng phổ biến nhất trong các hệ thống.
- NRZ và RZ đều là các phương pháp điều chế biên độ xung.
- NRZ mức bit "0" và "1" được mã hóa với hai mức biên độ tín hiệu khác nhau, mức tín hiệu này không thay đổi trong suốt chu kỳ bit T (một nhịp bus). Cái tên NRZ được sử dụng, bởi mức tín hiệu không quay trở về không sau mỗi nhịp. Các khả năng thể hiện hai mức có thể là:
 - Đất và điện áp dương
 - Điện áp âm và đất
 - Điện áp âm và điện áp dương cùng giá trị (tín hiệu lưỡng cực)

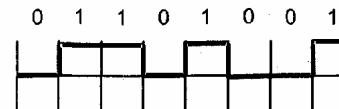
NRZ,RZ

- Một trong những ưu điểm của phương pháp NRZ là tín hiệu có tần số thường thấp hơn nhiều so với tần số nhịp bus.
- Phương pháp này không thích hợp cho việc đồng bộ hóa, bởi một dãy bit "0" hoặc "1" liên tục không làm thay đổi mức tín hiệu.
- Tín hiệu không được triệt tiêu dòng một chiều ngay cả khi sử dụng tín hiệu lưỡng cực, nên không có khả năng đồng tải nguồn.

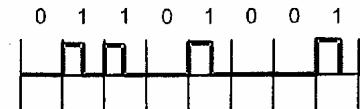
NRZ,RZ

- Phương pháp RZ (*Return to Zero*) cũng mã hóa bit "0" và "1" với hai mức tín hiệu khác nhau giống như ở NRZ. Tuy nhiên, như cái tên của nó hàm ý mức tín hiệu cao chỉ tồn tại trong nửa đầu của chu kỳ bit T, sau đó quay trở lại "0".
- Tần số cao nhất của tín hiệu chính bằng tần số nhịp bus.
- Giống như NRZ, tín hiệu mã RZ không mang thông tin đồng bộ hóa, không có khả năng đồng tải nguồn.

NRZ,RZ



NRZ: 1 ứng với mức tín hiệu cao, 0 với mức thấp trong suốt chu kỳ bit



RZ: 1 ứng với mức tín hiệu cao trong nửa chu kỳ bit T, 0 với mức thấp trong nửa chu kỳ bit

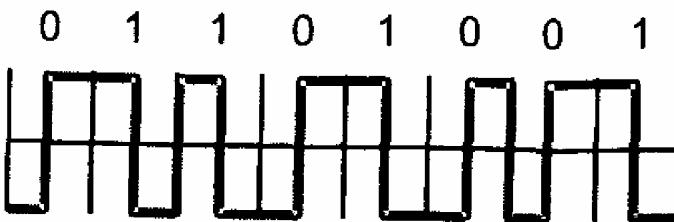
Manchester

- Mã Manchester và các dạng dẫn xuất của nó không những được sử dụng rất rộng rãi trong truyền thông công nghiệp, mà còn phổ biến trong các hệ thống truyền dữ liệu khác.
- Thực chất, đây là một trong các phương pháp điều chế pha xung, tham số thông tin được thể hiện qua các sườn xung. Bit "1" được mã hóa bằng sườn lên, bit "0" bằng sườn xuống của xung ở giữa chu kỳ bit T, hoặc ngược lại (Manchester-II).

Manchester

- Đặc điểm của tín hiệu là có tần số tương đương với tần số nhịp bus, các xung của nó có thể sử dụng trong việc đồng bộ hóa giữa bên gửi và bên nhận.
- Sử dụng tín hiệu lưỡng cực, dòng một chiều sẽ bị triệt tiêu. Do đó phương pháp này thích hợp với các ứng dụng đòi hỏi khả năng đồng tải nguồn.
- Một điểm đáng chú ý nữa là do sử dụng sườn xung, mã Manchester rất bền vững đối với nhiễu bên ngoài. Nhưng ngược lại, nhiễu xạ của tín hiệu cũng tương đối lớn bởi tần số cao.

Manchester



Manchester-II: 1 ứng với sườn xuống, 0 ứng với sườn lên của xung ở giữa chu kỳ bit

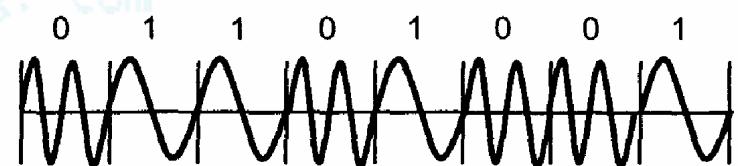
FSK

- Trong phương pháp điều chế tần số FSK (*Frequency Shift Keying*), hai tần số khác nhau được dùng để mã hóa các trạng thái logic "0" và "1".
- Đây chính là phương pháp điều chế tần số tín hiệu mang, hay truyền tải dải mang.
- Tín hiệu có dạng hình sin, các tần số có thể bằng hoặc là bội số tần số nhịp bus nên có thể dùng để đồng bộ nhịp.
- ưu điểm tiếp theo của phương pháp này là độ bền vững đối với tác động của nhiễu.

FSK

- Nhờ tính chất điều hòa của tín hiệu mà dòng một chiều được triệt tiêu, nên có thể sử dụng chính đường truyền để đồng tải nguồn nuôi các thiết bị kết nối mạng.
- Nhược điểm của FSK là tần số tín hiệu tương đối cao. Điều này một mặt dẫn đến khả năng gây nhiễu mạnh đối với bên ngoài và mặt khác hạn chế việc tăng tốc độ truyền. Thực tế, phương pháp này chỉ được sử dụng cho các hệ thống có tốc độ truyền tương đối thấp.

FSK



FSK: 0 và 1 ứng với các tần số khác nhau

Các nguyên nhân gây ra lỗi

- Các hiện tượng tĩnh.
- Ồn nhiệt.
- Các hiện tượng ngẫu nhiên

Các định nghĩa

+ Tỉ lệ bit lỗi: *Tỉ lệ bit lỗi p* là thước đo đặc trưng cho độ nhiễu của kênh truyền dẫn, được tính bằng tỉ lệ giữa số bit bị lỗi trên tổng số bit được truyền đi. Nói một cách khác, tỉ lệ bit lỗi chính là xác suất một bit truyền đi bị lỗi. Lưu ý rằng, tỉ lệ bit lỗi xấu nhất không phải là 1, mà là 0,5. Trong trường hợp $p = 1$ tức là bất cứ bit nào truyền đi cũng bị sai lệch, ta chỉ việc đảo các bit để khôi phục lại dữ liệu. Khi $p = 0,5$ tức xác suất cứ hai bit truyền đi lại có một bit bị lỗi thì đường truyền này hoàn toàn không sử dụng được, bởi theo lý thuyết thông tin thì không thể có một phương pháp bảo toàn dữ liệu nào có thể áp dụng tin cậy, có hiệu quả. Trong kỹ thuật, $p = 10^{-4}$ là một giá trị thường chấp nhận được. Một đường truyền có tỉ lệ bit lỗi như vậy có thể thực hiện được tương đối dễ dàng.

Các định nghĩa

+ Tỉ lệ lỗi còn lại: Tỉ lệ lỗi còn lại R là thông số đặc trưng cho độ tin cậy dữ liệu của một hệ thống truyền thông, sau khi đã thực hiện các biện pháp bảo toàn kể cả truyền lại trong trường hợp phát hiện ra lỗi. Tỉ lệ lỗi còn lại được tính bằng tỉ lệ giữa số bức điện còn bị lỗi không phát hiện được trên tổng số bức điện đã được truyền. Đương nhiên, giá trị này không những phụ thuộc vào tỉ lệ bit lỗi và phương pháp bảo toàn dữ liệu mà còn phụ thuộc vào chiều dài trung bình của các bức điện. Một bức điện càng dài thì xác suất lỗi càng lớn.

Các định nghĩa

+ Thời gian trung bình giữa hai lần lỗi: Tỉ lệ lỗi còn lại là một thông số tương đối khó hình dung, vì vậy trong thực tế người ta hay xét tới thời gian trung bình giữa hai lần lỗi *TMTBF* (*Mean Time Between Failures*). Thông số này có liên quan chặt chẽ tới giá trị tỉ lệ lỗi còn lại:

$$\text{TMTBF} = n / (v * R)$$

Với n là chiều dài bức điện tính bằng bit và v là tốc độ truyền tính bằng bit/s. Giả sử một bức điện có chiều dài $n = 100$ bit được truyền liên tục với tốc độ 1200 bit/s, quan hệ giữa tỉ lệ bit lỗi và thời gian trung bình giữa hai lần lỗi sẽ được thể hiện như sau:

R	TMTBF:
10^{-6}	1 ngày
10^{-10}	26 năm
10^{-14}	260 000 năm

Các định nghĩa

+ Khoảng cách Hamming (Hamming Distance, HD): Khoảng cách Hamming (gọi theo nhà khoa học Mỹ R.W. Hamming) là thông số đặc trưng cho độ bền vững của một mã dữ liệu, hay nói cách khác chính là khả năng phát hiện lỗi của một phương pháp bảo toàn dữ liệu HD có giá trị bằng số lượng bit lỗi tối thiểu mà không đảm bảo chắc chắn phát hiện được trong một bức điện. Nếu trong một bức điện chỉ có thể phát hiện một cách chắc chắn k bit bị lỗi, thì $HD = k+1$. Ví dụ, nếu một lỗi duy nhất có thể phát hiện được một cách chắc chắn (như trong phương pháp dùng parity bit 1 chiều), thì khoảng cách Hamming là 2. Đây là giá trị tối thiểu mà một phương pháp truyền đòi hỏi. Các hệ thống bus trường thông dụng thường có khoảng cách Hamming là 4, các hệ thống đạt độ tin cậy rất cao với $HD = 6$.

Các định nghĩa

+ Hiệu suất truyền dữ liệu: Hiệu suất truyền dữ liệu E là một thông số đặc trưng cho việc sử dụng hiệu quả các bức điện phục vụ chức năng bảo toàn dữ liệu, được tính bằng tỉ lệ số bit mang thông tin nguồn (bit dữ liệu không bị lỗi trên toàn bộ số bit được truyền). Ta có:

$$E = m / (1-p)n/n$$

m - Số lượng bit dữ liệu trong mỗi bức điện

n - Chiều dài bức điện

p - Tỉ lệ bit lỗi

Phát hiện và sửa lỗi

Phần lớn các phương pháp phát hiện lỗi là công thêm vào bản tin các bit vừa giúp để biểu diễn bản tin vừa để phát hiện lỗi.

Phát hiện và sửa lỗi

Có hai cách sửa lỗi cho bản tin:

+ Sửa lỗi có phản hồi: Bộ thu sẽ phân tích và phát hiện ra các lỗi có trong bản tin được gửi đi từ bộ truyền. Đã được định nghĩa ở trong giao thức, bộ thu sẽ yêu cầu bộ phát gửi lại bản tin. Phần lớn các giao thức mạng máy tính và công nghiệp sử dụng cách này.

+ Sửa lỗi không có phản hồi: Trong phương pháp này bộ thu không chỉ phát hiện ra lỗi có ở trong bản tin mà nó còn phục hồi lại bản tin đúng từ các thông tin sửa lỗi đi kèm theo. Cách này thường được sử dụng khi truyền ở khoảng cách lớn trong không gian, ở đây thời gian đòi hỏi cho việc truyền lại bản tin là quá lớn, hay trong hệ truyền thông tin theo một chiều (phát thanh, truyền hình).

Kiểm tra chẵn lẻ ký tự

- Trước khi truyền đi một ký tự, bên phát sẽ căn cứ vào mức độ là chẵn (EVEN) hay lẻ (ODD) để tính toán một bit công thêm vào ký tự.

Lẻ (ODD): số bit "1" trong ký tự là lẻ.

Chẵn (EVEN): số bit "1" trong ký tự là chẵn.

- Phương pháp này cung cấp hiệu quả phát hiện lỗi thấp ($HD=2$), khi có 2 bit cùng thay đổi giá trị thì không phát hiện được.

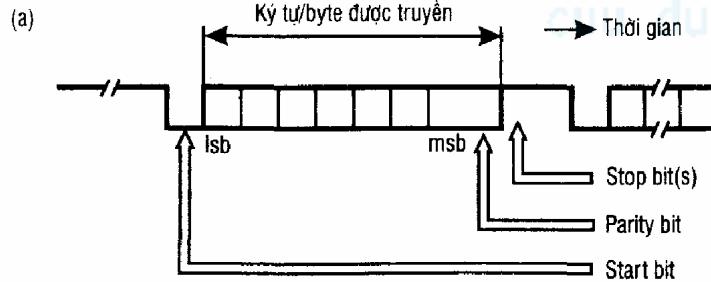
- Phương pháp này phù hợp trong trường hợp đơn giản, giá thành thực hiện thấp, cho phép kiểm tra nhanh độc hính xác của dữ liệu, dễ dàng tính nhẩm để kiểm tra.

Kiểm tra chẵn lẻ ký tự

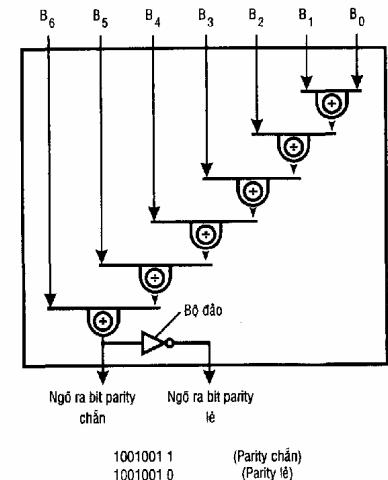
- Mặc dù có nhiều hạn chế, nhưng nó vẫn được dùng trong các ứng dụng không đòi hỏi cao như truyền giữa máy tính và máy in, hay trong các ứng dụng mà các thiết bị đặt gần nhau và trong môi trường có độ ồn thấp.

- Kiểm tra chẵn lẻ phát hiện được 60% lỗi.

Kiểm tra chẵn lẻ ký tự



Kiểm tra chẵn lẻ ký tự

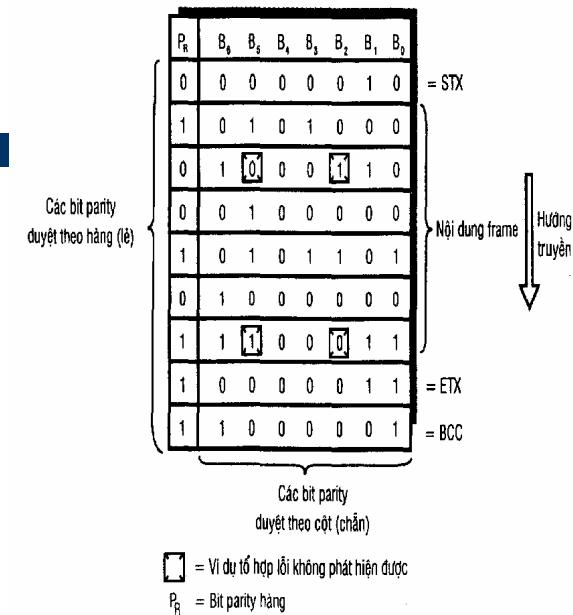


Kiểm tra khối

- Kiểm tra chẵn lẻ khối:
(BCC-Block Check Character ; LRC-Longitudinal Redundancy Check)

Trong cách kiểm tra khối bản tin các ký tự được xem như là mảng bit hai chiều. Một bit chẵn lẻ được gắn thêm cho mỗi ký tự. Sau một số lượng đã định trước các ký tự, 1 ký tự mà nó thực hiện việc kiểm tra chẵn lẻ của cột sẽ được truyền. Mặc dù tốt hơn nhưng phương pháp này cũng không phát hiện hết lỗi.(PP này có HD=4).

Kiểm tra khối



Kiểm tra khối

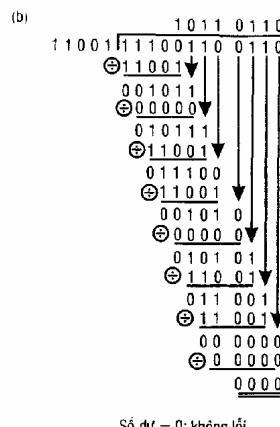
- Lấy Check-sum toán học: Nó đơn giản là lấy tổng của tất cả các ký tự trong khối. Nó cung cấp khả năng kiểm tra tốt hơn nhưng đòi hỏi thêm hai byte khi truyền.

Kiểm tra CRC

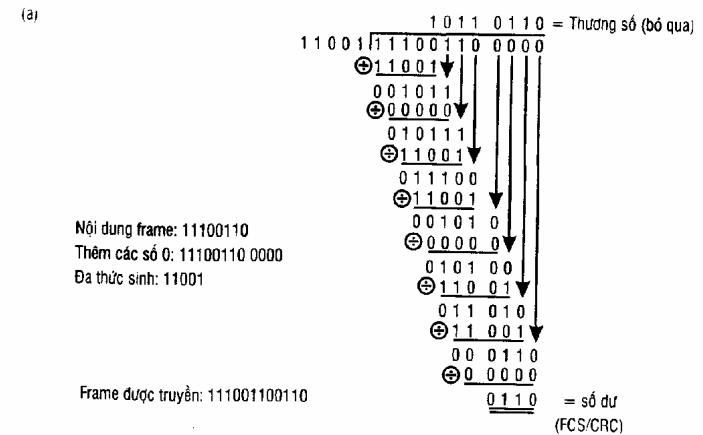
- Phương pháp có tên như vậy do các bit trong một bản tin được dịch chuyển quay vòng qua một thanh ghi. Nó cũng còn được gọi là phương pháp mã đa thức (polynomial code) vì có sử dụng khái niệm đa thức đại số quen thuộc.
- Một xâu bit bất kỳ được xem được xem như là một tập hợp các hệ số (0 và 1) của một đa thức đại số. Nếu xâu bit gồm k bits thì đa thức tương ứng sẽ có bậc $k-1$, gồm k số hạng từ x^0 đến x^{k-1} .

Kiểm tra CRC

- Để tìm tập bits kiểm tra (được gọi là checksum) thích hợp để ghép vào sâu bit cần truyền đi sao cho bên nhận có thể kiểm soát được lỗi, tư tưởng của phương pháp CRC là:
- Chọn trước một đa thức (gọi là đa thức sinh - Generator polynomial) $G(x)$ với hệ số cao nhất và thấp nhất bằng 1.
- Checksum được tìm thỏa mãn điều kiện: đa thức tương ứng với sâu ghép (Gốc và checksum) phải chia hết (Modulo 2) cho $G(x)$.
- Khi nhận tin để kiểm soát lỗi, lấy đa thức tương ứng với sâu bit nhận được chia cho $G(x)$. Nếu chia không hết thì khẳng định là đã có lỗi. Nếu chia hết thì chưa thể khẳng định là đúng.



Kiểm tra CRC



Kiểm tra CRC

Kiểm tra CRC

Hiện nay có một số đa thức sinh chuẩn:

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

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

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

CRC-32=

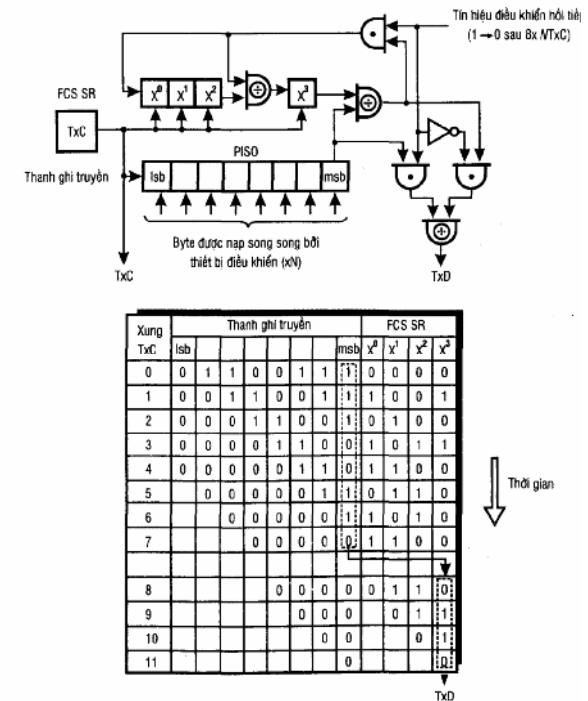
$$x^{32}+x^{26}+x^{23}+x^{16}+x^{12}+x^{11}+x^{10}+x^8+x^7+x^5+x^4+x^2+x+1$$

Kiểm tra CRC

Phương pháp này có hiệu quả phát hiện lỗi tốt. Với CRC-16 và CRC-CCITT như sau:

- Lỗi 1 bit : 100%.
- Lỗi 2 bit: 100%.
- Lỗi lẻ bit: 100%.
- Khối lỗi <16 bit: 100%.
- Khối lỗi >16 bit: 99,9969%
- Các lỗi khác: 99,9984%

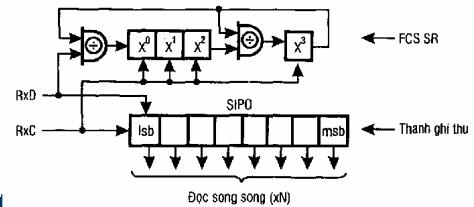
Kiểm tra CRC



Xung Tx C	Thanh ghi truyền								FCS SR			
	lsb					msb	x^0	x^1	x^2	x^3		
0	0	1	1	0	0	1	1	1	1	0	0	0
1	0	0	0	1	1	0	0	1	1	1	0	0
2	0	0	0	0	1	1	0	0	1	0	1	0
3	0	0	0	0	0	1	1	0	0	1	0	1
4	0	0	0	0	0	0	1	1	0	0	1	0
5	0	0	0	0	0	0	0	1	1	0	1	0
6							0	1	0	1	0	0
7							0	0	0	0	1	1
8							0	0	0	0	1	1
9							0	0	0	0	0	1
10								0	0	0	0	0
11								0	0	0	0	0

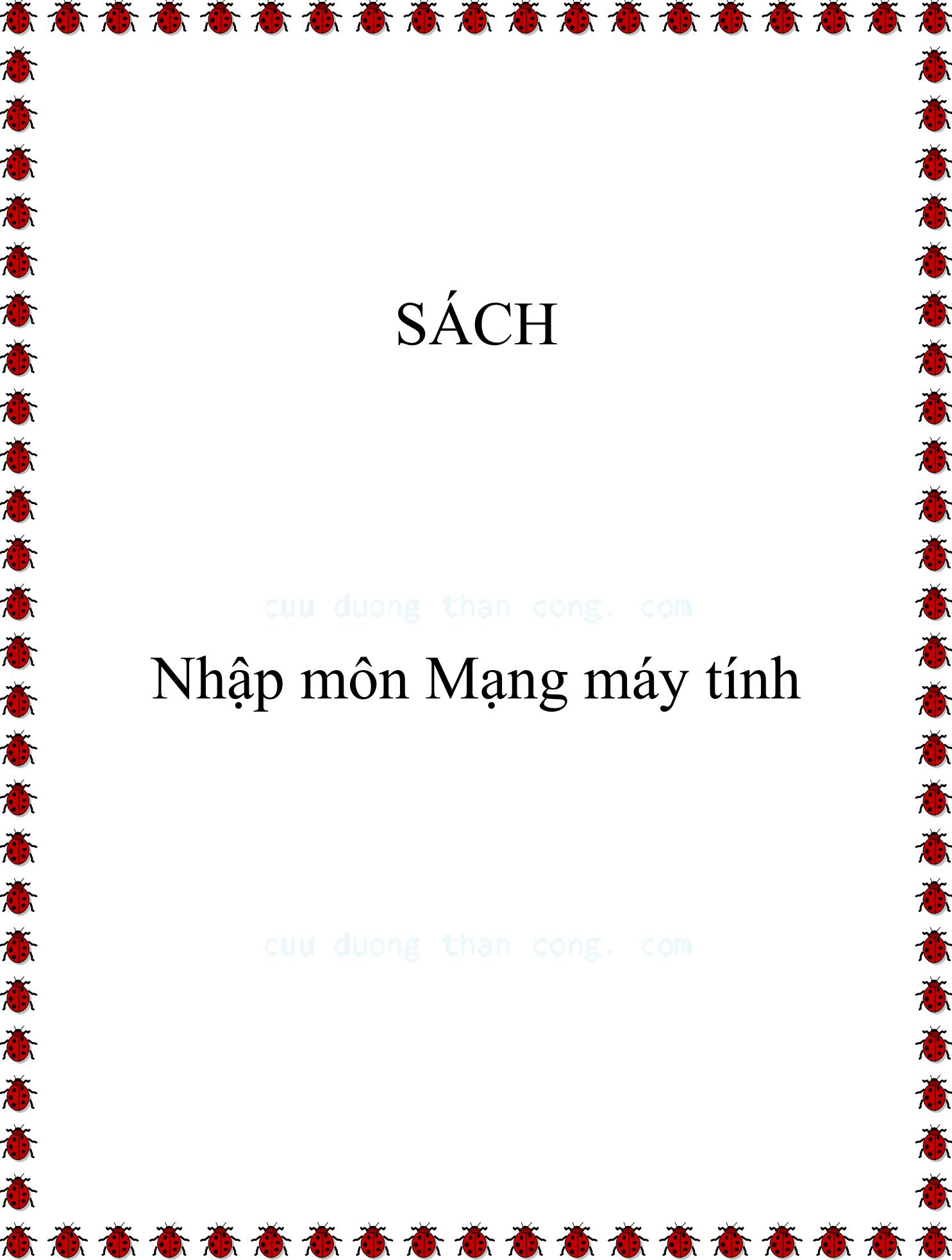
Thời gian

Kiểm tra CRC



RxC	RxD	Thanh ghi thu								FCS SR			
		lsb				msb	x^0	x^1	x^2	x^3			
0	1	0	0	0	0	0	0	0	0	0	0	0	0
1	1	1						1	0	0	0		
2	1	1	1					1	1	0	0		
3	0	1	1	1				1	1	1	0		
4	0	0	1	1	1			0	1	1	1		
5	1	0	0	1	1	1		1	0	1	0		
6	1	1	0	0	1	1	1	1	1	0	1		
7	0	1	1	0	1	1	1	0	1	1	1		
8	0	0	1	1	0	1	1	1	1	0	1	0	
9	1							0	1	0	1		
10	1							0	0	1	1		
11	0							0	0	0	0		
12								0	0	0	0		

Thời gian



SÁCH

cuu duong than cong. com

Nhập môn Mạng máy tính

cuu duong than cong. com

PHẦN I. NHẬP MÔN LÝ THUYẾT MẠNG

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

I. Lịch sử mạng máy tính

II. Giới thiệu mạng máy tính

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

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

 2.1.2. Định nghĩa mạng máy tính

2.2. Đặc trưng kỹ thuật của mạng máy tính

 2.2.1. Đường truyền

 2.2.2. Kỹ thuật chuyển mạch

 2.2.3. Kiến trúc mạng

 2.2.4. Hệ điều hành mạng

2.3. Phân loại mạng máy tính

 2.3.1. Phân loại mạng theo khoảng cách địa lý :

 2.3.2. Phân loại mạng theo kỹ thuật chuyển mạch

 2.3.3. Phân loại theo kiến trúc mạng sử dụng

 2.3.4. Phân loại theo hệ điều hành mạng

2.4. Giới thiệu các mạng máy tính thông dụng nhất

 2.4.1. Mạng cục bộ

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

 2.4.3. Liên mạng INTERNET.

 2.4.4. Mạng INTRANET

III. Mạng cục bộ, kiến trúc mạng cục bộ

3.1. Mạng cục bộ

3.2. Kiến trúc mạng cục bộ.

3.3. Các phương pháp truy cập đường truyền vật lý

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

 3.3.2. Phương pháp Token Bus.

 3.3.2. Phương pháp Token Ring.

IV. Chuẩn hoá mạng máy tính

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

4.2. Mô hình tham chiếu OSI 7 lớp

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

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

I. Các thiết bị mạng thông dụng

1.1. Các loại cáp truyền

1.1.1. Cáp đôi dây xoắn (Twisted pair cable)

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

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

1.1.4. Cáp quang

1.2. Các thiết bị ghép nối.

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

1.2.2. Bộ chuyển tiếp (REPEATER)

1.2.3. Các bộ tập trung (HUB).

1.2.4. Switching Hub

1.2.5. Modem

1.2.6. Router

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

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

2.2. Kiểu 10BASE5

2.3. Kiểu 10BASE2

2.4. Kiểu 10BASE-T

2.5. Kiểu 10BASE-F

Chương 3. Giới thiệu giao thức TCP/IP

I. Giao thức IP.

1.1. Họ giao thức TCP/IP

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

1.2.1. Địa chỉ IP

1.2.2. Cấu trúc gói dữ liệu IP

1.2.3. Phân mảnh và hợp nhất các gói IP

1.2.4. Định tuyến IP

II. Giao thức lớp chuyển tải (Transport Layer)

2.1. Giao thức TCP

2.2 Cấu trúc gói dữ liệu TCP

2.3. Thiết lập và kết thúc kết nối TCP

Chương 4. Giao thức (4)

I. Chức năng của giao thức

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

III. Các giao thức chuẩn

IV. Cài đặt và gỡ bỏ giao thức

Chương 5. Quản trị mạng (6)

I. Khái quát.

II. Quản lý tài khoản mạng

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

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

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

2.4. Duy trì nhật ký mạng.

III. Phòng ngừa mất dữ liệu

3.1. Các loại nguy cơ đe dọa dữ liệu.

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

3.3. Các hệ thống dung lõi.

PHẦN II. QUẢN TRỊ MẠNG

cuu duong than cong. com

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

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

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

I. Lịch sử mạng máy tính

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

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

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

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

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

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

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

II. Giới thiệu mạng máy tính

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

2.1.1. Nhu cầu của việc kết nối mạng máy tính

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

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

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

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

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

2.1.2. Định nghĩa mạng máy tính

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

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

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

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

2.2. Đặc trưng kỹ thuật của mạng máy tính

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

2.2.1. Đường truyền

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

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

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

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

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

2.2.2. Kỹ thuật chuyển mạch:

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

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

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

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

2.2.3. Kiến trúc mạng

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

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

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

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

2.2.4. Hệ điều hành mạng

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

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

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

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

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

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

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

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

2.3. Phân loại mạng máy tính

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

- Khoảng cách địa lý của mạng
- Kỹ thuật chuyển mạch mà mạng áp dụng
- Kiến trúc mạng
- Hệ điều hành mạng sử dụng ...

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

2.3.1. Phân loại mạng theo khoảng cách địa lý :

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

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

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

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

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

2.3.2. Phân loại theo kỹ thuật chuyển mạch:

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

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

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

Ưu điểm của phương pháp này là :

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

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

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

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

Nhược điểm của phương pháp này là:

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

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

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

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

2.3.3. Phân loại theo kiến trúc mạng sử dụng

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

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

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

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

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

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

2.3.4. Phân loại theo hệ điều hành mạng

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

2.4. Giới thiệu các mạng máy tính thông dụng nhất

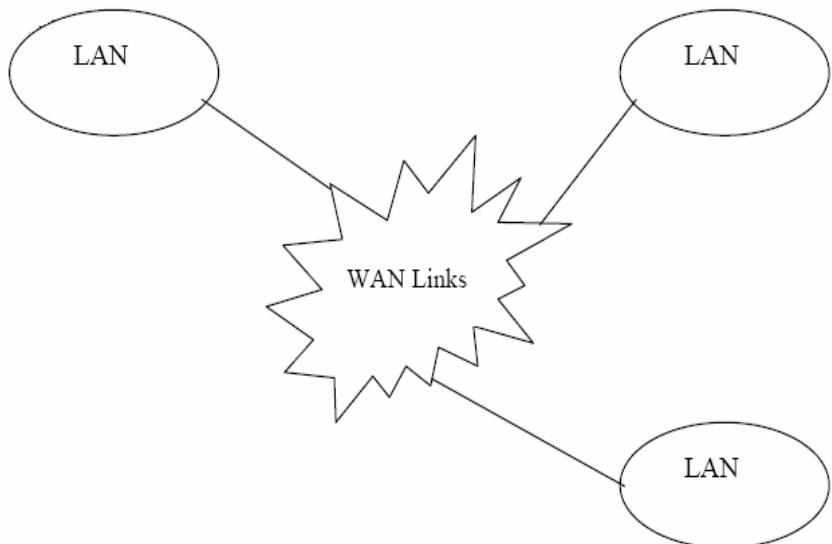
2.4.1. Mạng cục bộ

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

Mạng cục bộ có các đặc tính sau:

- Tốc độ truyền dữ liệu cao
- Phạm vi địa lý giới hạn
- Sở hữu của một cơ quan/tổ chức

2.4.2. Mạng diện rộng với kết nối LAN TO LAN



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

- Tốc độ truyền dữ liệu không cao
- Phạm vi địa lý không giới hạn
- Thường triển khai dựa vào các công ty truyền thông, bưu điện và dùng các hệ thống truyền thông này để tạo dựng đường truyền
- Một mạng WAN có thể là sở hữu của một tập đoàn/tổ chức hoặc là mạng kết nối của nhiều tập đoàn/tổ chức 16

2.4.3. Liên mạng INTERNET

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

- Là một mạng toàn cầu
- Là sự kết hợp của vô số các hệ thống truyền thông, máy chủ cung cấp thông tin và dịch vụ, các máy trạm khai thác thông tin
- Dựa trên nhiều nền tảng truyền thông khác nhau, nhưng đều trên nền giao thức TCP/IP
 - Là sở hữu chung của toàn nhân loại
 - Càng ngày càng phát triển mãnh liệt

2.4.4. Mạng INTRANET

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

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

III. Mạng cục bộ, kiến trúc mạng cục bộ

3.1. Mạng cục bộ

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

Đặc điểm của mạng cục bộ

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

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

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

3.2. Kiến trúc mạng cục bộ

* Định nghĩa Topo mạng:

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

Có hai kiểu nối mạng chủ yếu đó là :

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

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

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

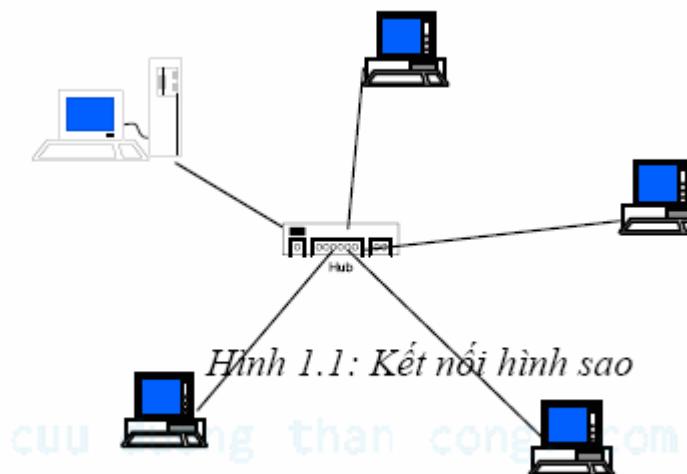
* Phân biệt kiểu tô pô của mạng cục bộ và kiểu tô pô của mạng rộng.

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

a) Mạng hình sao

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

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



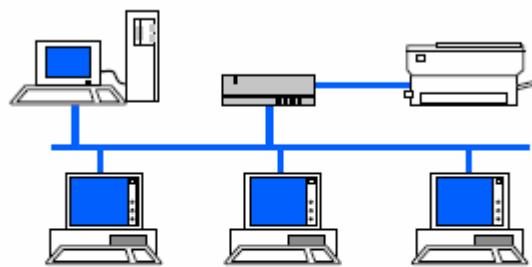
truyền của đường truyền vật lý.

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

b) Mạng trực tuyến tính (Bus):

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

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



Hình 1.2. Kết nối kiểu bus

Ưu điểm : Dễ thiết kế, chi phí thấp

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

c) Mạng hình vòng

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

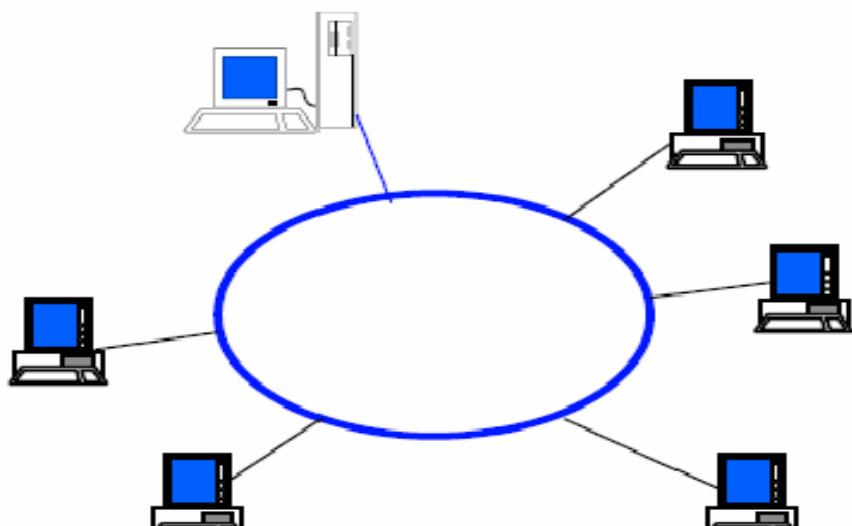
Để tăng độ tin cậy của mạng ta có thể lắp đặt thêm các vòng dự phòng, nếu vòng chính có sự cố thì vòng phụ sẽ được sử dụng.

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

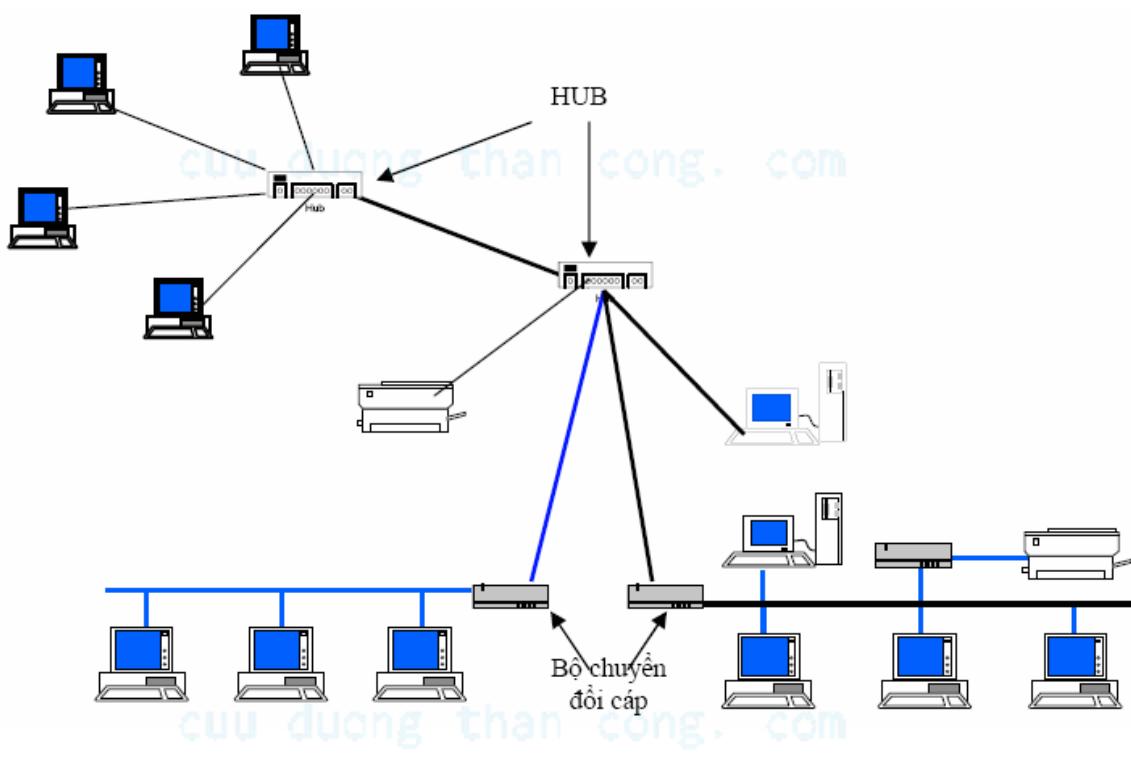
d) Kết nối hỗn hợp

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

cuu duong than cong. com



Hình 1.3 Kết nối kiểu vòng



Hình 1.4. Một kết nối hỗn hợp

3.3. Các phương pháp truy cập đường truyền vật lý

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

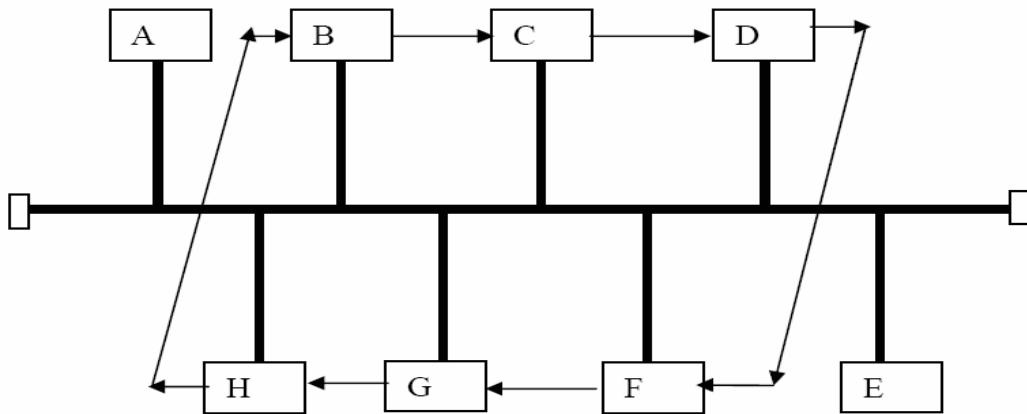
- Sau đó trạm sẽ chờ trong một khoảng thời gian ngẫu nhiên nào đó rồi thử truyền lại theo quy tắc CSMA.

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

3.3.2. Phương pháp Token Bus

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

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



Hình 1.5. Ví dụ về vòng logic

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

- Bổ xung một trạm vào vòng logic : các trạm nằm ngoài vòng logic cần được xem xét một cách định kỳ để nếu có nhu cầu truyền dữ liệu thì được bổ xung vào vòng logic.
- Loại bỏ một vòng khỏi vòng logic : khi một trạm không có nhu cầu truyền dữ liệu thì cần loại bỏ nó ra khỏi vòng logic để tối ưu hóa việc truyền dữ liệu bằng thẻ bài
- Quản lý lỗi : một số lỗi có thể xảy ra như trùng hợp địa chỉ, hoặc đứt vòng logic.
- Khởi tạo vòng logic : khi khởi tạo mạng hoặc khi đứt vòng logic cần phải khởi tạo lại vòng logic.

cuuduongthancong.com

3.3.3. Phương pháp Token Ring

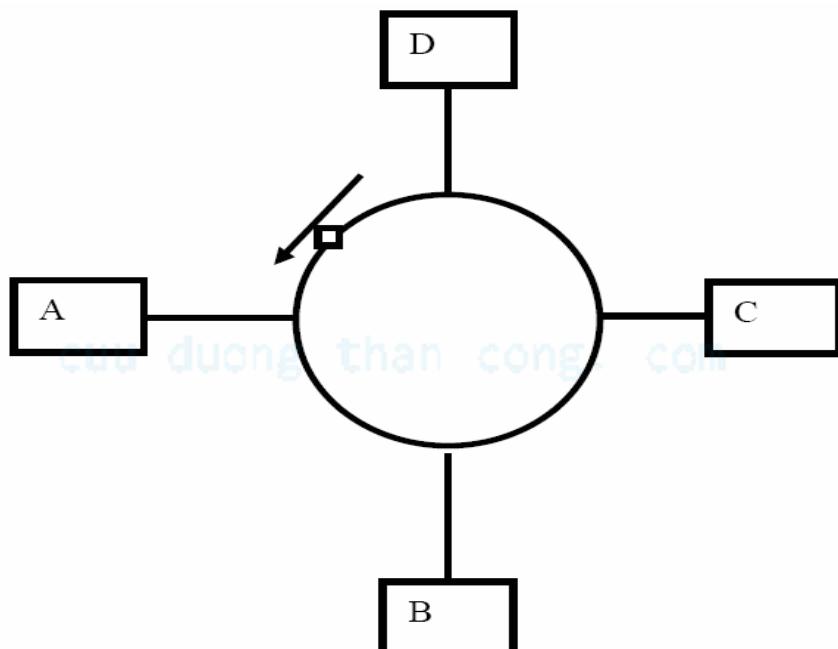
Phương pháp này cũng dựa trên nguyên tắc dùng thẻ bài để cấp phát quyền truy nhập đường truyền. Nhưng ở đây thẻ bài lưu chuyển theo vòng vật lý chứ không theo vòng logic như đối với phương pháp token bus.

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

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

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

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



Hình 1.6. Thẻ bài trong mạng Ring

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

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

IV. Chuẩn hóa mạng máy tính

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

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

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

Có hai loại chuẩn cho mạng đó là :

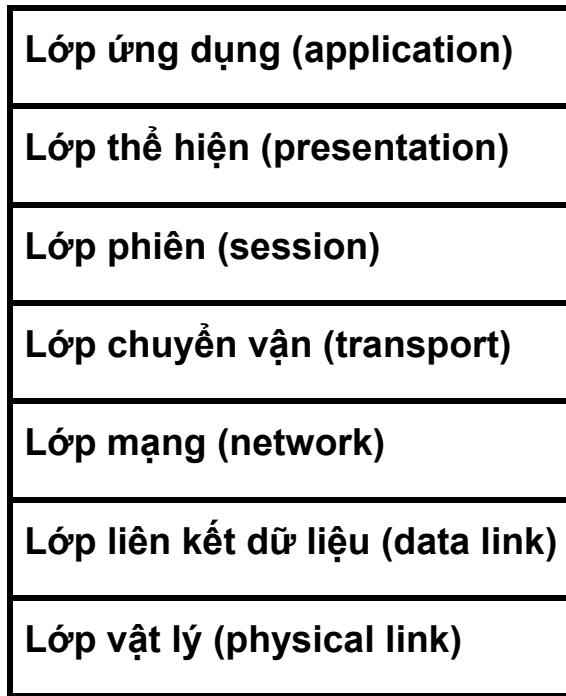
- Các chuẩn chính thức (de jure) do các tổ chức chuẩn quốc gia và quốc tế ban hành.

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

4.2. Mô hình tham chiếu OSI 7 lớp

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

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



Hình 1.7. Mô hình OSI 7 lớp

a) Lớp vật lý

Lớp này bảo đảm các công việc sau:

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

b) Lớp liên kết dữ liệu

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

c) Lớp mạng

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

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

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

d) Lớp chuyển vận

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

e) Lớp phiên

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

f) Lớp thể hiện

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

g) Lớp ứng dụng

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

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

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

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

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

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

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

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

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

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

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

- 10BASE5 : tốc độ 10Mb/s, dùng cáp xoắn đôi không bọc kim UTP (Unshield Twisted Pair), với phạm vi tín hiệu lên tới 500m, topo mạng hình sao.
- 10BASE2 : tốc độ 10Mb/s, dùng cáp đồng trực thin-cable với trở kháng 50 Ohm, phạm vi tín hiệu 200m,topo mạng dạng bus.
- 10BASE5 : tốc độ 10Mb/s, dùng cáp đồng trực thick-cable (đường kính 10mm) với trở kháng 50 Ohm, phạm vi tín hiệu 500m, topo mạng dạng bus.
- 10BASE-F: dùng cáp quang, tốc độ 10Mb/s phạm vi cáp 2000m.

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

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

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

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

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

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

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

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

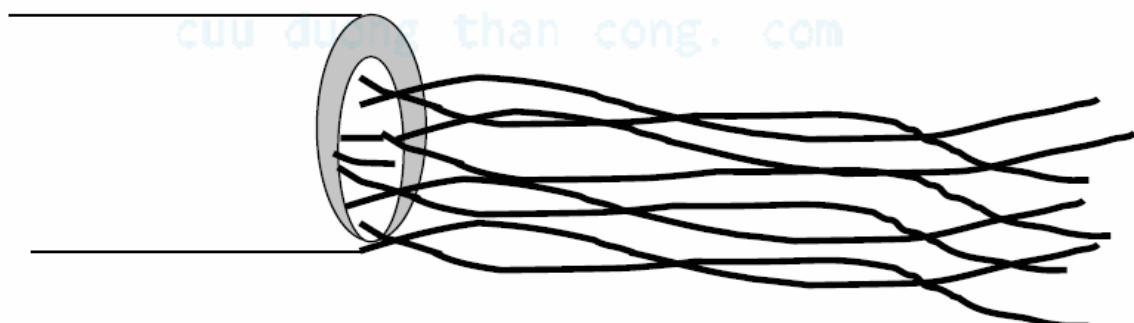
I. Các thiết bị mạng thông dụng

1.1. Các loại cáp truyền

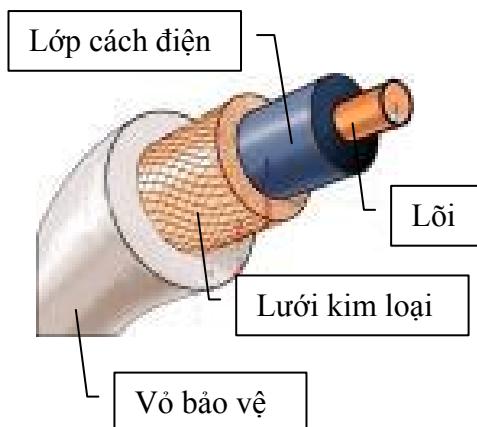
1.1.1. Cáp đôi dây xoắn (Twisted pair cable)

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

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



Hình 2.1 Cáp UTP CAT 5



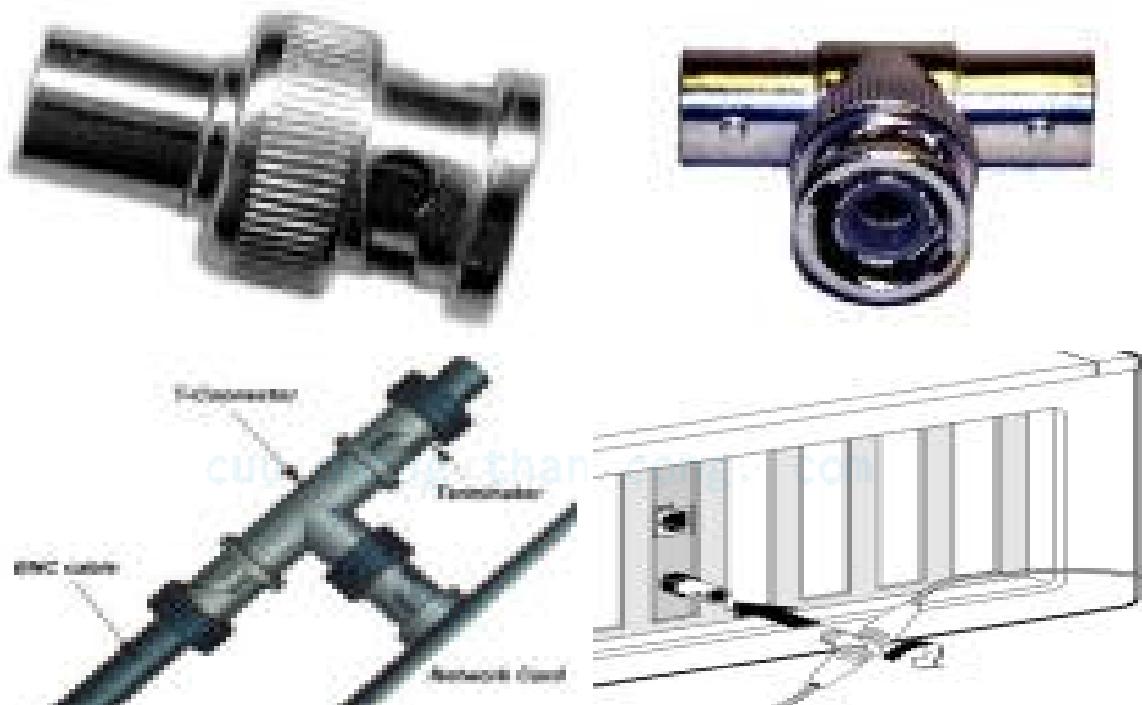
- Loại không bọc kim gọi là UTP (UnShield Twisted Pair), chất lượng kém hơn STP nhưng rất rẻ. Cáp UTP được chia làm 5 hạng tùy theo tốc độ truyền. Cáp loại 3 dùng cho điện thoại. Cáp loại 5 có thể truyền với tốc độ 100Mb/s rất hay dùng trong các mạng cục bộ vì vừa rẻ vừa tiện sử dụng. Cáp này có 4 đôi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

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

Hình 2.2 Cáp đồng trục

Hình 2.2 Cáp đồng trục Là cáp mà hai dây của nó có lõi lồng nhau, lõi ngoài là lưỡi kim loại. , Khả năng chống nhiễu rất tốt nên có thể sử dụng với chiều dài từ vài trăm met đến vài km. Có hai loại được dùng nhiều là loại có trở kháng 50 ohm và loại có trở kháng 75 ohm

Dải thông của cáp này còn phụ thuộc vào chiều dài của cáp. Với khoảng cách 1 km có thể đạt tốc độ truyền từ 1 – 2 Gbps. Cáp đồng trục băng tần cơ sở thường dùng cho các mạng cục bộ. Có thể nối cáp bằng các đầu nối theo chuẩn BNC có hình chữ T. Ở VN người ta hay gọi cáp này là cáp gầy do dịch từ tên trong tiếng Anh là ‘Thin Ethernet’.

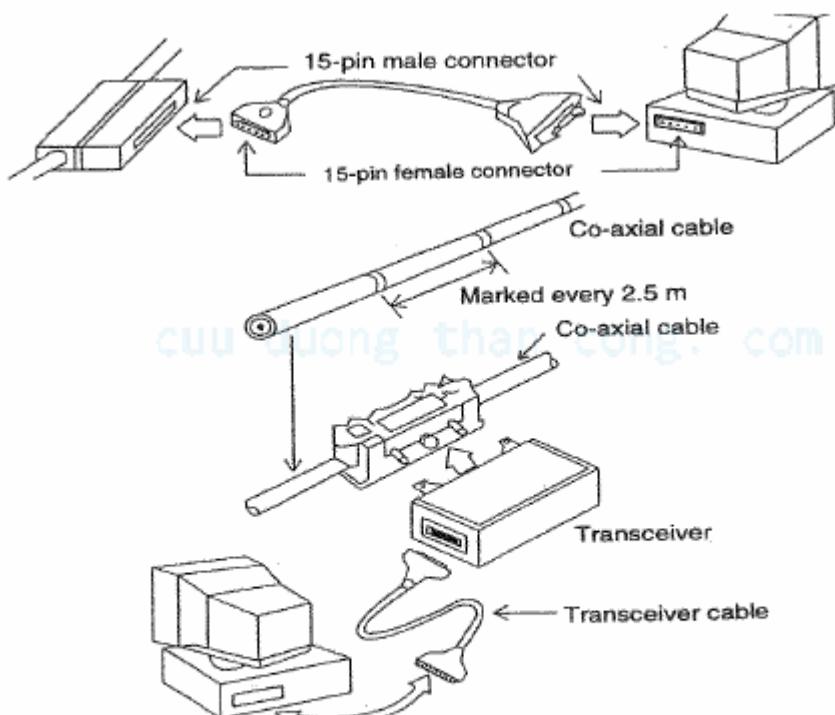


Một loại cáp khác có tên là “Thick Ethernet” mà ta gọi là cáp béo. Loại này thường có màu vàng. Người ta không nối cáp bằng các đầu nối chữ T như cáp giày mà nối qua các kẹp bấm vào dây. Cứ 2m5 lại có đánh dấu để nối dây

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

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

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



Hình 2.3 Kết nối bằng Traceiver

1.1.4. Cáp quang

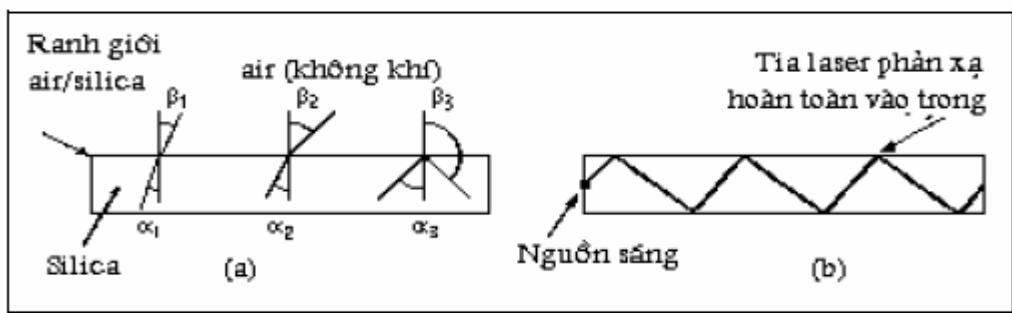
Dùng để truyền các xung ánh sáng trong lòng một sợi thuỷ tinh phản xạ toàn phần. Môi trường cáp quang rất lý tưởng vì

- Xung ánh sáng có thể đi hàng trăm km mà không giảm cường độ sáng.
- Giải thông rất cao vì tần số ánh sáng dùng đối với cáp quang cỡ khoảng 1014 – 1016
- An toàn và bí mật

- Không bị nhiễu điện từ

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

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



Hình 2.4. Truyền tín hiệu bằng cáp quang

Cáp quang cũng có hai loại

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

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

1.2. Các thiết bị ghép nối

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

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

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

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

1.2.2. Bộ chuyển tiếp (REPEATER)

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

1.2.3. Các bộ tập trung (Concentrator hay HUB)

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

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

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

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

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

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

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

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

1.2.5. Modem

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

1.2.6. Router

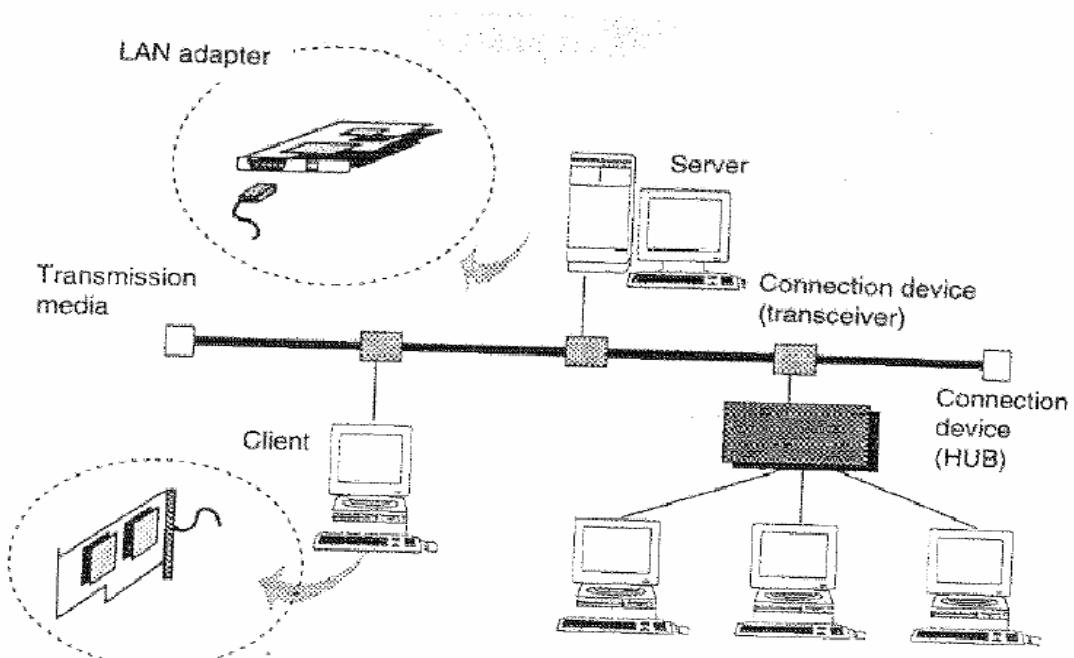
Router là một thiết bị không phải để ghép nối giữa các thiết bị trong một mạng cục bộ mà dùng để ghép nối các mạng cục bộ với nhau thành mạng rộng. Router thực sự là một máy tính làm nhiệm vụ chọn đường cho các gói tin hướng ra ngoài.

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

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

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

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



Hình 2.6. Cấu hình của một mạng cục bộ

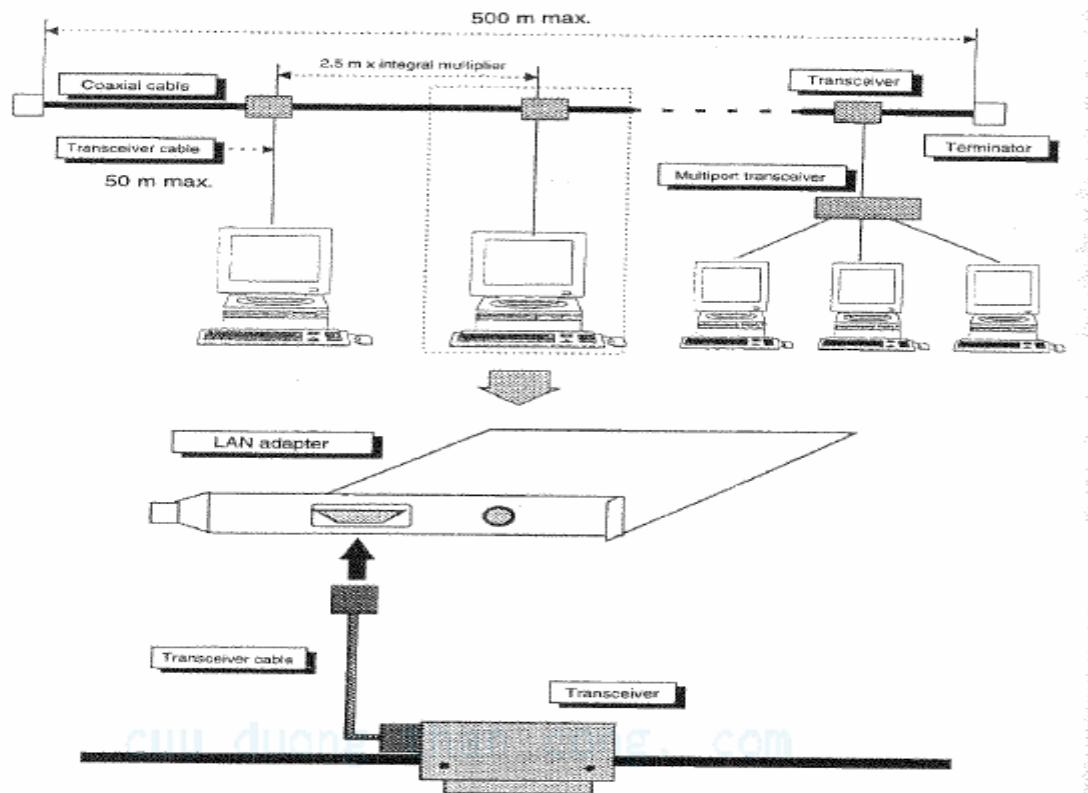
Hai yếu tố được quan tâm hàng đầu khi kết nối mạng cục bộ là tốc độ trong mạng và bán kính mạng. Tên các kiểu mạng dùng theo giao thức CSMA/CD cũng thể hiện điều này. Sau đây là một số kiểu kết nối đó với tốc độ 10 Mb/s khá thông dụng trong thời gian qua và một số thông số kỹ thuật:

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

1.3.2. Kiểu 10BASE5:

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

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



Hình 2.7 Kết nối theo chuẩn 10BASE5

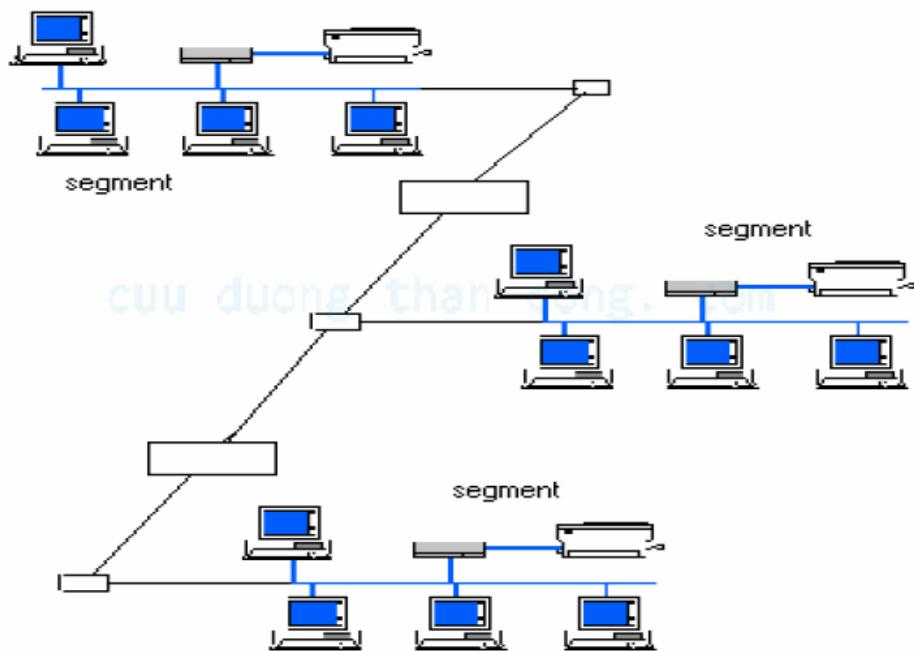
Đặc điểm của chuẩn 10BASE 5

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

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

1.3.3. Kiểu 10BASE2:

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

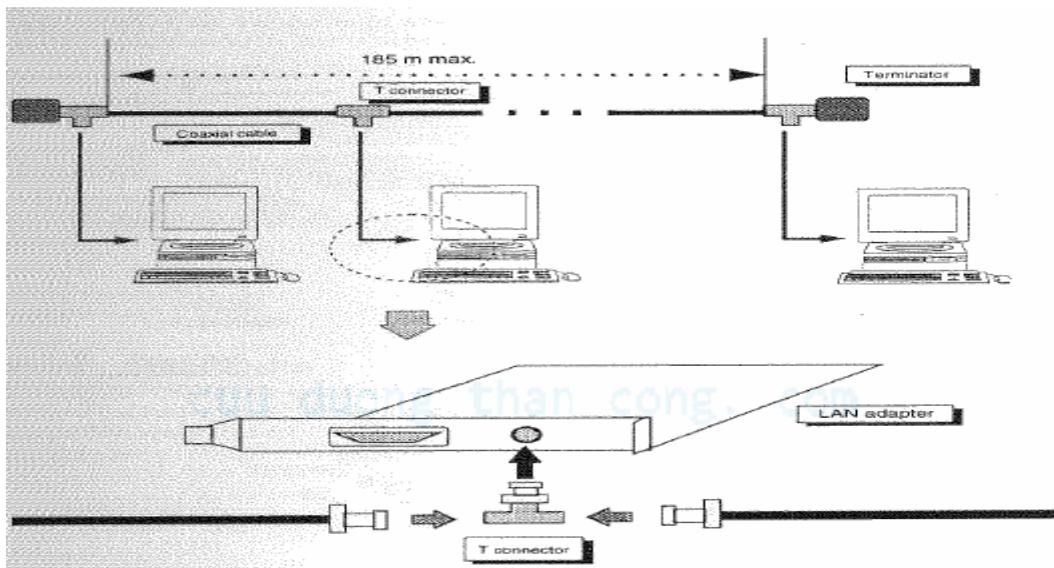


Hình 2.8 Kết nối tối đa 3 phân đoạn mạng

Đặc điểm của chuẩn 10BASE 2

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

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



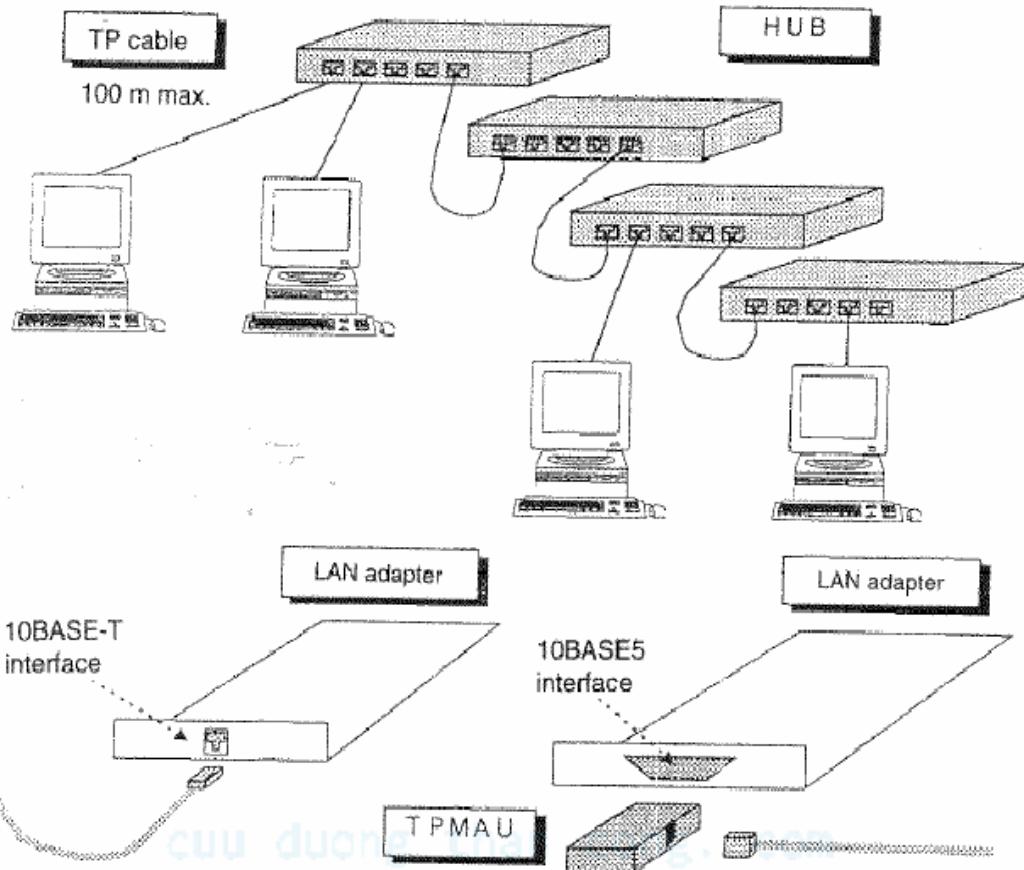
Hình 2.9 Nối theo chuẩn 10BASE2 với cáp đồng trục và đầu nối BNC

1.3.4. Kiểu 10BASE-T

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

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

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



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

1.3.5. Kiểu 10BASE-F

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

Chương 3. Giới thiệu giao thức TCP/IP

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

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

I. Giao thức IP

1.1. Họ giao thức TCP/IP

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

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

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

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

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

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

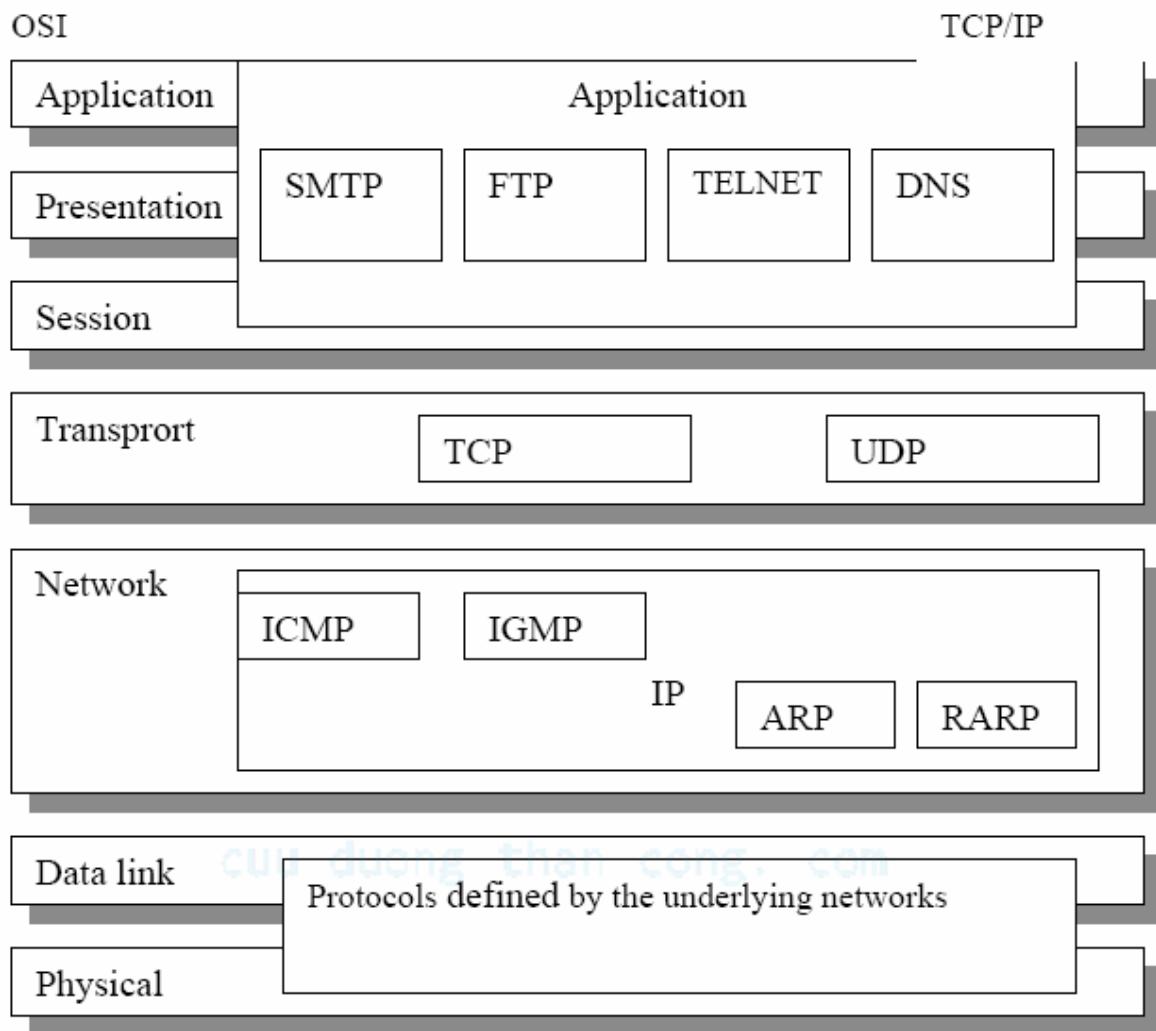
Giao thức trao đổi dữ liệu "có liên kết" (connection - oriented) TCP được sử dụng ở tầng vận chuyển để đảm bảo tính chính xác và tin cậy việc trao đổi dữ liệu dựa trên kiến trúc kết nối "không liên kết" ở tầng liên mạng IP.

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

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

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

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



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

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

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

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

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

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

Application	Stream
Transport	Segment/datagram
Internet	Datagram
Network Access	Frame

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

Lớp truy nhập mạng

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

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

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

Lớp liên mạng

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

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

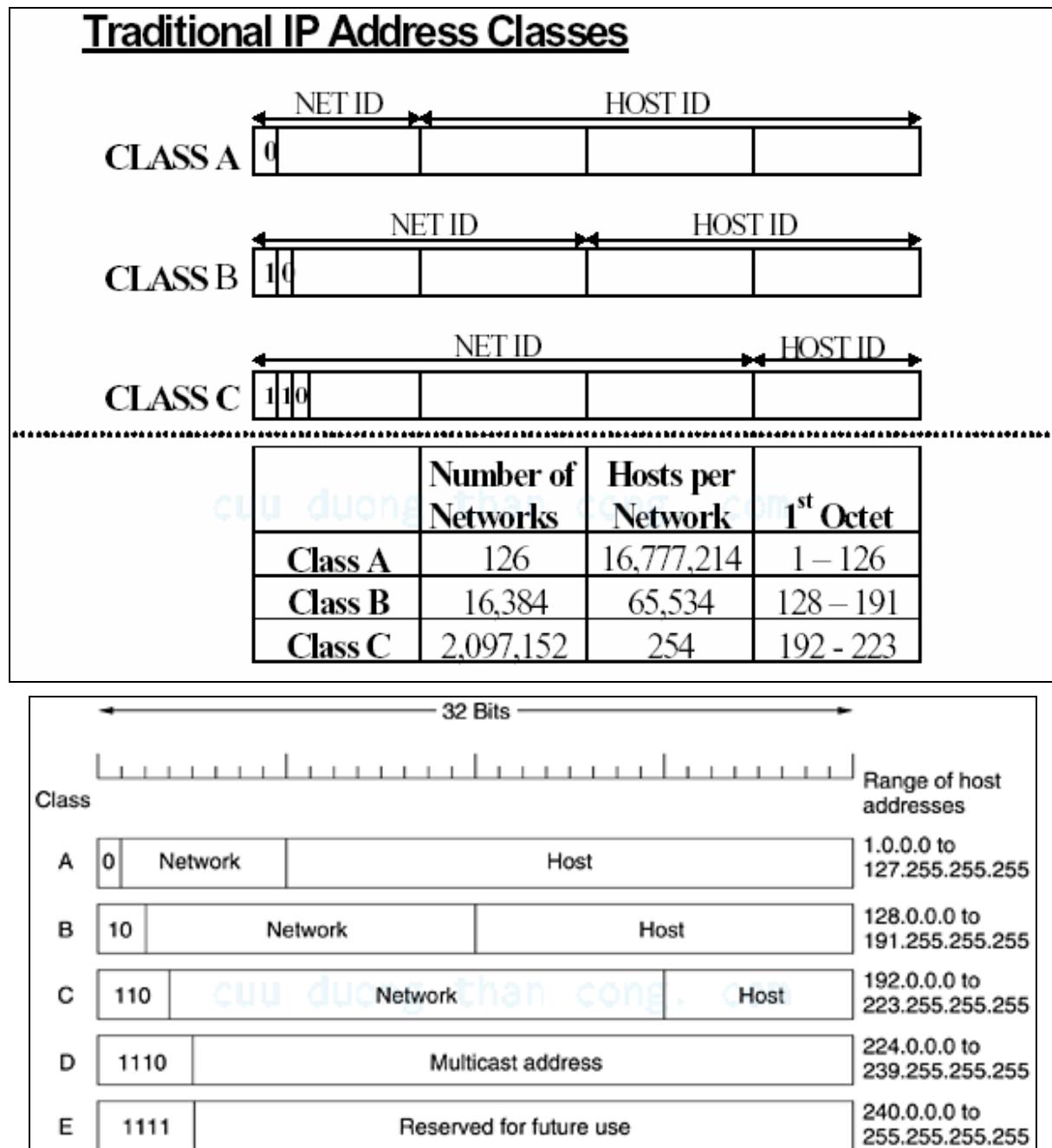
Trong phần này trình bày về giao thức IPv4 (để cho thuận tiện ta viết IP có nghĩa là đề cập đến IPv4).

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

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

- Phân định danh địa chỉ mạng Network Number
 - Phân định danh địa chỉ các trạm làm việc trên mạng đó Host Number
- Ví dụ 128.4.70.9 là một địa chỉ IP

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



Hình 3.4. Cấu trúc địa chỉ IP

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

- Lớp A cho phép định danh tới 126 mạng (sử dụng byte đầu tiên), với tối đa 16 triệu host (3 byte còn lại, 24 bits) cho mỗi mạng. Lớp này được dùng cho các mạng có số trạm cực lớn. Tại sao lại có 126 mạng trong khi dùng 8 bits? Lý do đầu tiên, 127.x (01111111) dùng cho địa chỉ loopback, thứ 2 là bit đầu tiên của byte đầu tiên bao giờ cũng là 0, 111111(127). Dạng địa chỉ lớp A (network number. host.host.host). Nếu dùng ký pháp thập phân cho phép 1 đến 126 cho vùng đầu, 1 đến 255 cho các vùng còn lại.

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

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

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

- Lớp E dự phòng để dùng trong tương lai

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

Ví dụ:

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

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

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

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

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

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

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

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

IP Address	160.30.20.10	10100000 00011110 00010100 00001010
Subnet Mask	255.255.255.0	11111111 11111111 11111111 00000000
Result	160.30.20.0	10100000 00011110 00010100 00000000
IP Address	160.30.20.100	10100000 00011110 11001000 01100100
Subnet Mask	255.255.255.0	11111111 11111111 11111111 00000000
Result	160.30.20.0	10100000 00011110 00010100 00000000

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

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

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

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

lớp B - 255.255.0.0 (/16),

lớp C - 255.255.255.0 (/24).

Subnetting

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

Ví dụ:

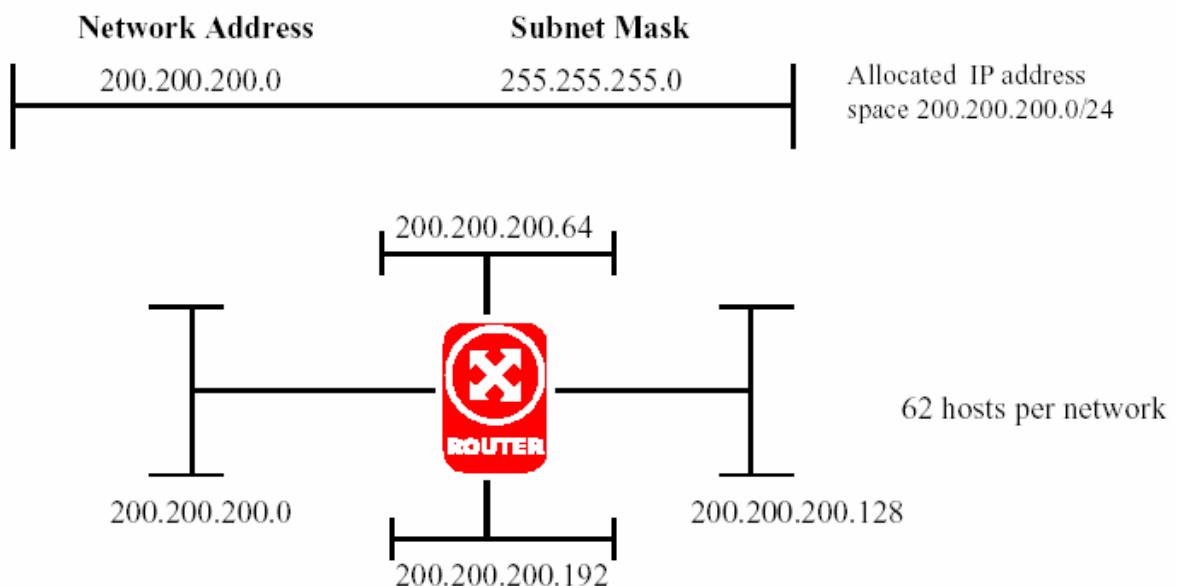
17.1.1.1 địa chỉ lớp A có địa chỉ mạng 17, địa chỉ subnet 1, địa chỉ host 1.1

129.1.1.1 địa chỉ lớp B có địa chỉ mạng 129.1, địa chỉ subnet 1, địa chỉ host 1.1

Netid	Subnetid	hostid	Lớp A
0	7 8	15 16 23 24	31
Netid	Subnetid	hostid	Lớp B
0	7 8	15 16 23 24 26 27	31
Netid	Subnetid	hostid	Lớp C

Hình 3.6 Bố sung vùng subnetid

Subnetting Example



Note: Subnet mask for each subnet = 255.255.255.192

Hình 3.7. Ví dụ SubNet

Subnet Mask là 255.255.255.192 hay là /26

04 mạng nhỏ hơn với địa chỉ mạng là

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

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

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

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

Xác định tên máy tính

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

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

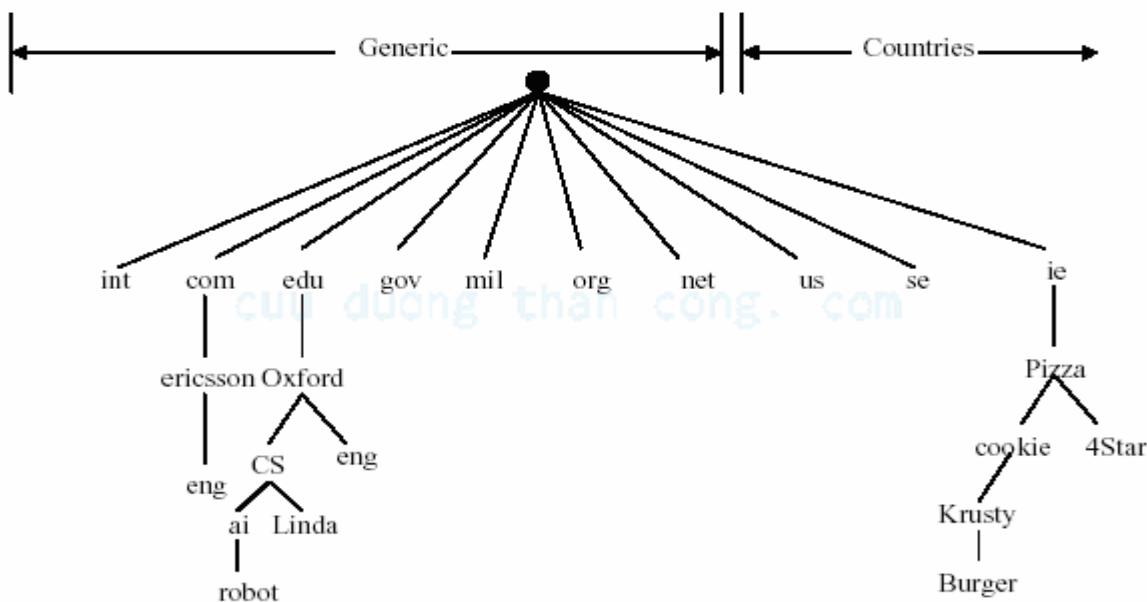
DNS được tổ chức theo cấu trúc phân hệ, phần gần gốc hơn là tên ở phía bên phải, các hệ thống lớn chia ra các hệ thống nhỏ, và lại được chia tiếp theo. Các DNS có các loại chính như sau: loại top-level - bậc cao; loại thông thường; loại theo quốc gia.

Các loại thông thường:

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

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

Internet Domain Name Space

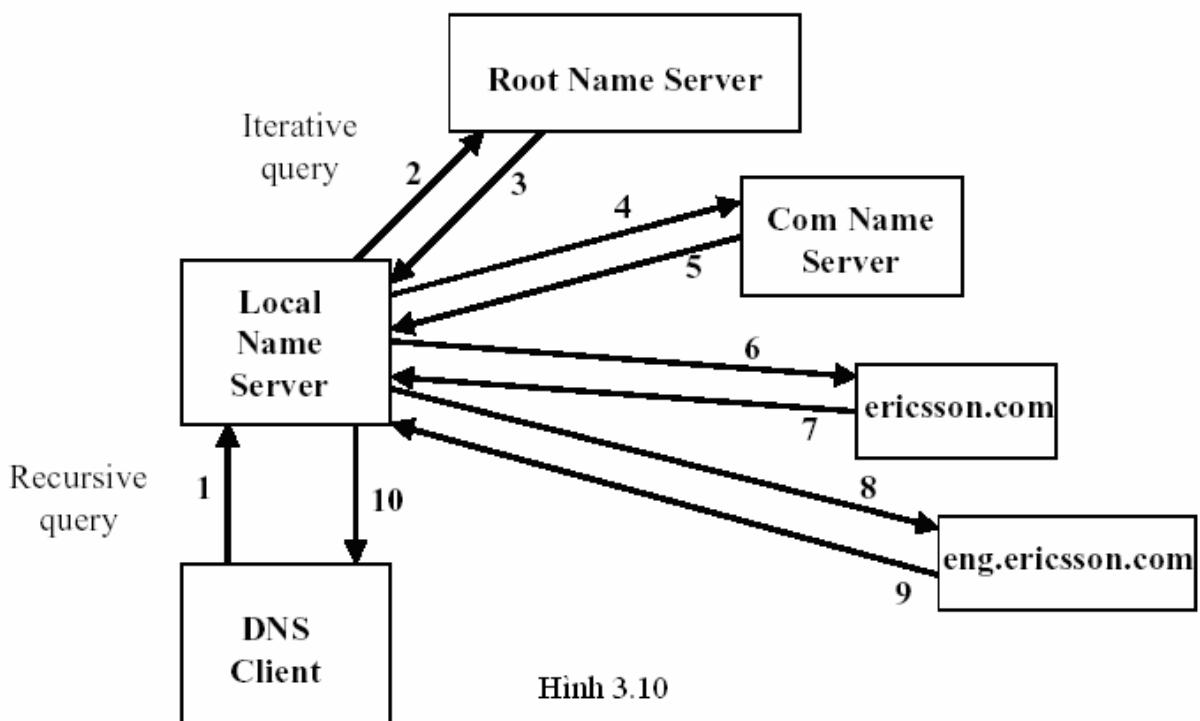


Hình 3.9

Cách thức xác định tên và IP từ tên:

1. Client gửi yêu cầu xác định IP cho tên mr-a.khoacntt.dhsphn.edu.vn tới Local Name Server.
 2. LNS không có quyền đối với tên này nên yêu cầu Root name server.
 3. RNS gửi lại LNS địa chỉ IP của vn name server.
 4. LNS yêu cầu tới vn server
 5. vn server trả lời địa chỉ IP của DNS quản lý tên miền edu.vn.
 6. LNS yêu cầu tới server trên và nhận trả lời cho server name tiếp theo,...
- Quá trình tiếp diễn tới khi đạt được name server quản lý chính xác tên như trên.

Domain Name Resolution



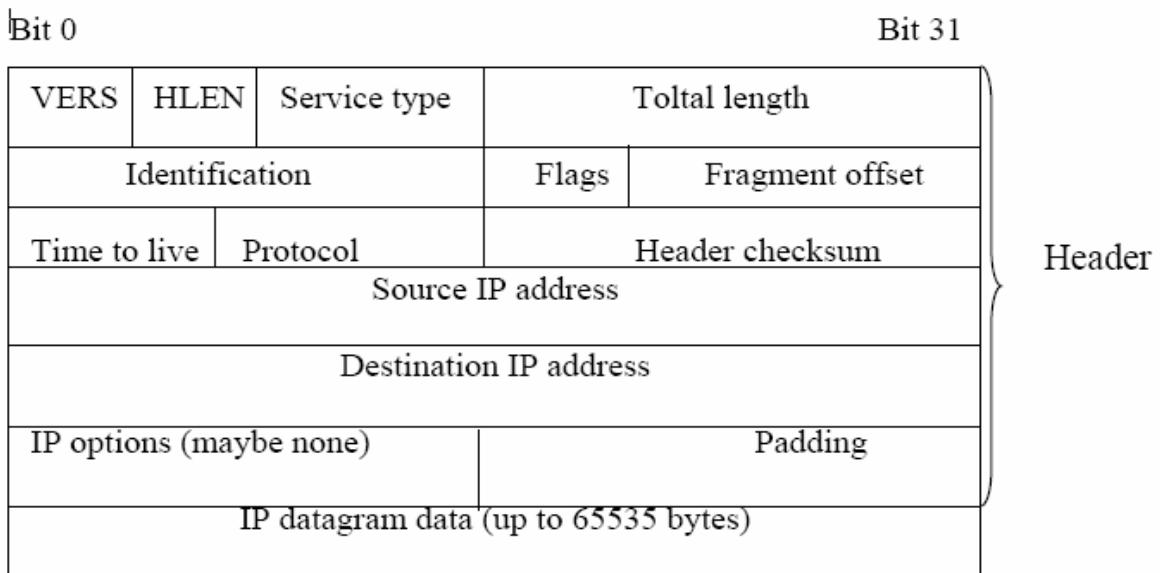
Các Name Server giữ các thông tin về xử lý tên miền trong bộ đệm, khi có thông tin sẽ gửi một thông báo gồm tên miền và địa chỉ IP tới Client và cách liên lạc với name server đó. Do đó việc xử lý tên sẽ nhanh hơn.

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

1.2.2. Cấu trúc gói dữ liệu IP

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

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



Hình 3.11. Cấu trúc gói dữ liệu IP

- VER (4 bits) : chỉ Version hiện hành của IP được cài đặt.
 - IHL (4 bits) : chỉ độ dài phần tiêu đề (Internet Header Length) của datagram, tính theo đơn vị word (32 bits). Nếu không có trường này thì độ dài mặc định của phần tiêu đề là 5 từ.
 - Type of service (8 bits): cho biết các thông tin về loại dịch vụ và mức ưu tiên của gói IP, có dạng cụ thể như sau:

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

Trong đó:

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

111	Network Control (cao nhất)	011- flash
110	Internetwork Control	010 Immediate
101	CRITIC/ECP	001 Priority
100	Flas Override	000 Routine (thấp nhất)

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

D=0 độ trễ bình thường,

D=1 độ trễ thấp

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

T=1 thông lượng bình thường

T=1 thông lượng cao

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

R=0 độ tin cậy bình thường

R=1 độ tin cậy cao

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

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

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

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

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

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

 1 (Don't Fragment)

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

 1 (More Fragment)

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

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

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

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

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

- Destination Address (32 bits): địa chỉ của trạm đích.
- Option (có độ dài thay đổi) sử dụng trong một số trường hợp, nhưng thực tế chúng rất ít dùng. Option bao gồm bảo mật, chức năng định tuyến đặc biệt
 - Padding (độ dài thay đổi): vùng đệm, được dùng để đảm bảo cho phần header luôn kết thúc ở một mốc 32 bits
 - Data (độ dài thay đổi): vùng dữ liệu có độ dài là bội của 8 bits, tối đa là 65535 bytes.

1.2.3. Phân mảnh và hợp nhất các gói IP

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

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

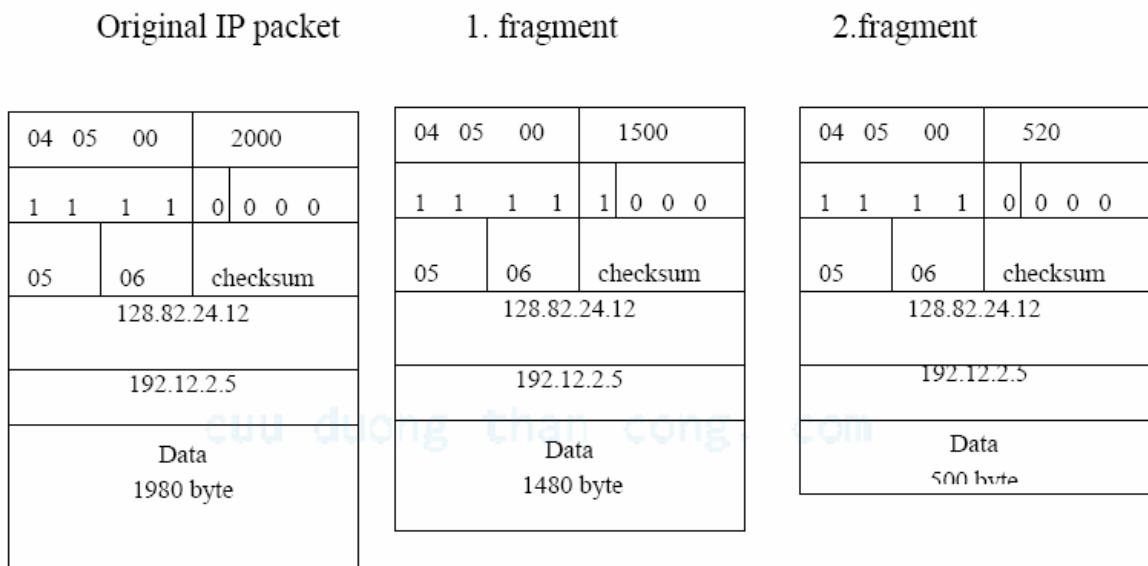
Độ dài tối đa của một gói dữ liệu liên kết là MTU (Maximum Transmit Unit). Khi cần chuyển một gói dữ liệu IP có độ dài lớn hơn MTU của một mạng cụ thể, cần phải chia gói số liệu IP đó thành những gói IP nhỏ hơn để độ dài của nó nhỏ hơn hoặc bằng MTU gọi chung là mảnh (fragment). Trong phần tiêu đề của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

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

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

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

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



Hình 3.12. Nguyên tắc phân mảnh gói dữ liệu

1.2.4. Định tuyến IP

Có hai loại định tuyến:

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

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

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

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

Chiến lược định tuyến:

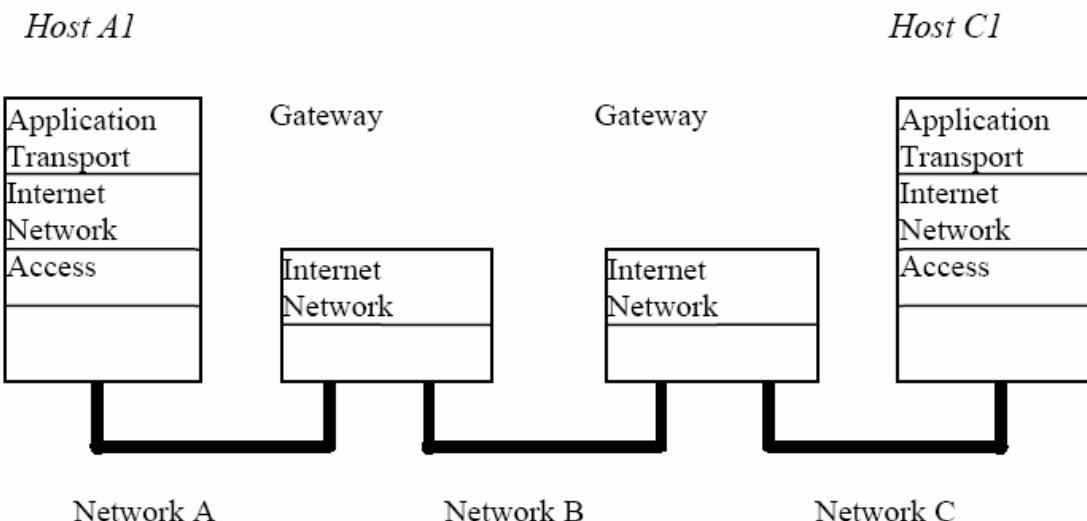
Trong thuật ngữ truyền thông của TCP/IP chỉ có hai kiểu thiết bị, đó là các cổng truyền (gateway) và các trạm (host). Các cổng truyền có vai trò gửi các gói dữ liệu, còn các trạm thì không. Tuy nhiên khi một trạm được nối với nhiều mạng thì nó cũng có thể định hướng cho việc lưu chuyển các gói dữ liệu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

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

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

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

cuuduongthancong.com



Hình 3.13. Định tuyến giữa hai hệ thống

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

I.6. Một số giao thức điều khiển

I.6.1. Giao thức ICMP

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

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

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

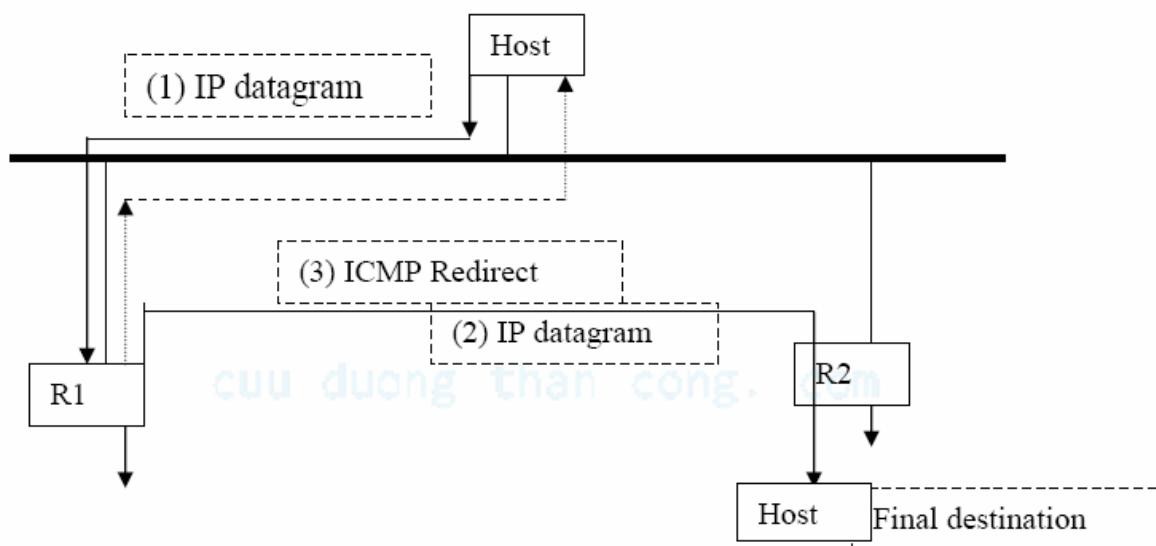
- Định hướng lại các tuyến đường: một thiết bị định tuyến sẽ gửi một thông điệp ICMP "định tuyến lại" (Redirect Router) để thông báo với một trạm là nên dùng thiết bị định tuyến khác để tới thiết bị đích. Thông điệp này có thể chỉ được dùng khi trạm nguồn ở trên cùng một mạng với cả hai thiết bị định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

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

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

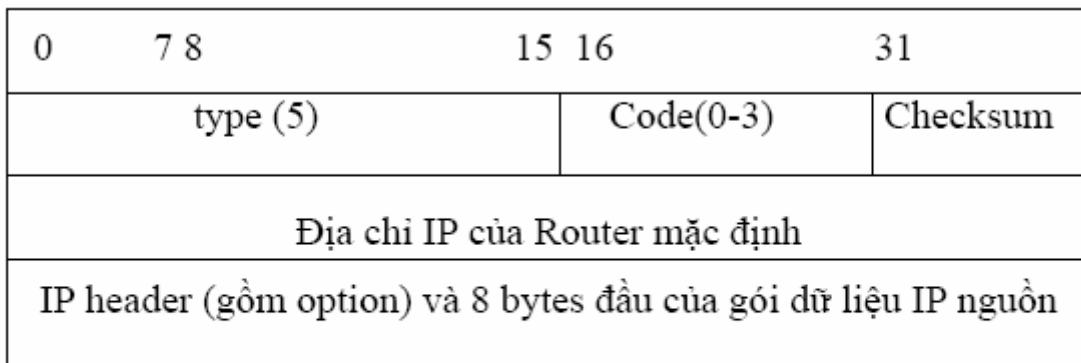
Ví dụ: giả sử host gửi một gói dữ liệu IP tới Router R1. Router R1 thực hiện việc quyết định tuyến vì R1 là router mặc định của host đó. R1 nhận gói dữ liệu và tìm trong bảng định tuyến và nó tìm thấy một tuyến tới R2. Khi R1 gửi gói dữ liệu tới R2 thì R1 phát hiện ra rằng nó đang gửi gói dữ liệu đó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

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



Hình 3.8 Thực hiện việc định tuyến lại

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



Hình 3.9 Dạng thông điệp ICMP redirect

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

Các loại định hướng lại của gói dữ liệu ICMP

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

I.6.2. Giao thức ARP và giao thức RARP

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

Giao thức ARP

Giao thức TCP/IP sử dụng ARP để tìm địa chỉ vật lý của trạm đích. Ví dụ khi cần gửi một gói dữ liệu IP cho một hệ thống khác trên cùng một mạng vật lý Ethernet, hệ 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 thích ứng mới. Khuôn dạng của gói dữ liệu ARP được mô tả trong hình

- Data link type: cho biết loại công nghệ mạng mức liên kết (ví dụ đối với mạng Ethernet trường này có giá trị 01).
- Network type: cho biết loại mạng (ví dụ đối với mạng IPv4, trường này có giá

0		31
	Data link type	Network type
Hlen	plen	Opcode
Sender data link (6byte for Ethernet)		
Sender network (4 byte for IP)		
Target data link (6 byte)		
Target network (4 byte)		
Check sume		

Hình 3.10 Mô tả khuôn dạng của gói ARP

trị 0800_{16}).

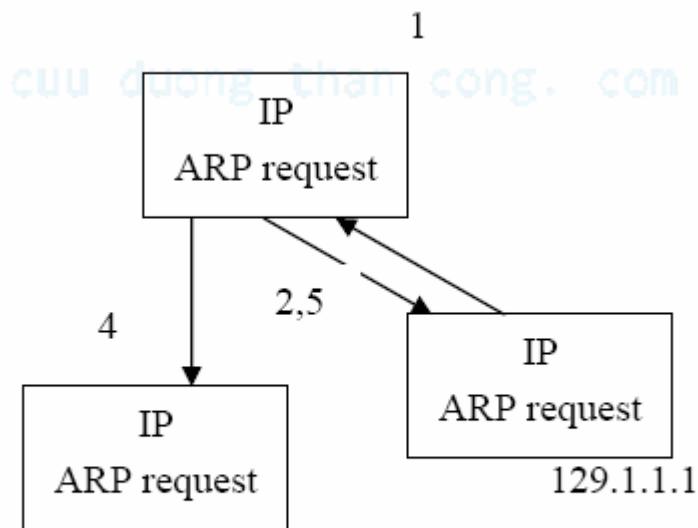
- Hlen (hardware length): độ dài địa chỉ mức liên kết (6 byte).
- Plen (Protocol length): cho biết độ dài địa chỉ mạng (4 byte)
- Opcode (operation code): mã lệnh yêu cầu; ; mã lệnh trả lời .
- Sender data link: địa chỉ mức liên kết của thiết bị phát gói dữ liệu này.
- Sender network : địa chỉ IP của thiết bị phát.

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

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

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

1. IP yêu cầu địa chỉ MAC.



Hình 3.11 Tiến trình ARP

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

Giao thức RARP

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

II. Giao thức lớp chuyển tải (Transport Layer)

2.1. Giao thức TCP

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

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

1. Thiết lập, duy trì, kết thúc liên kết giữa hai quá trình.
2. Phân phát gói tin một cách tin cậy.
3. Đánh số thứ tự (sequencing) các gói dữ liệu nhằm truyền dữ liệu một cách tin cậy.
4. Cho phép điều khiển lỗi.
5. Cung cấp khả năng đa kết nối với các quá trình khác nhau giữa trạm nguồn và trạm đích nhất định thông qua việc sử dụng các cổng.
6. Truyền dữ liệu sử dụng cơ chế song công (full-duplex).

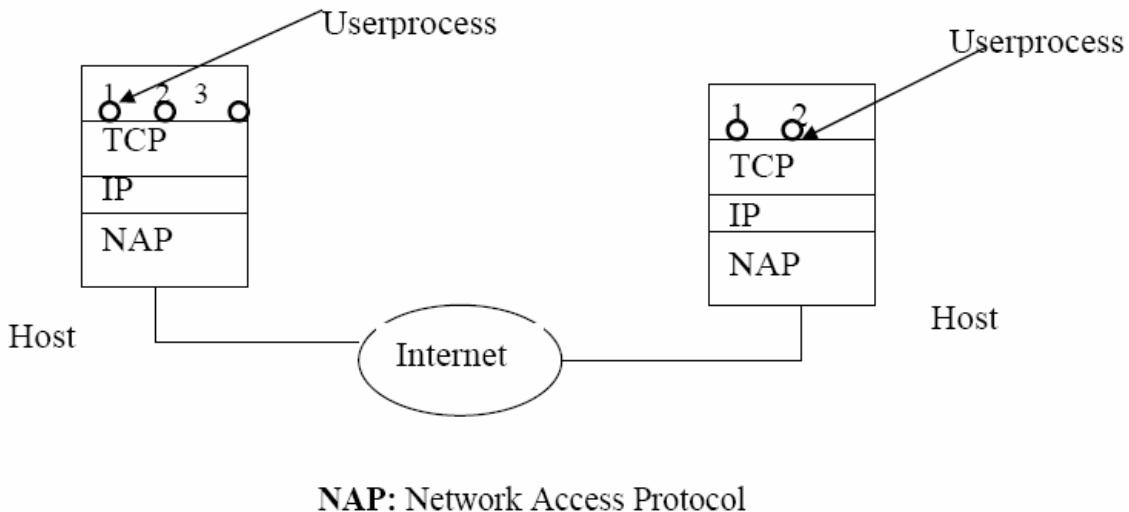
o

31

Source port		Destination port													
Sequence number															
Acknowledgment number															
Data	Resersed	U	A	P	R	S	F								
Offset		R	C	S	S	Y	I	Window							
		G	K	H	T	N	N								
Checksum		Urgent pointer													
Options		Padding													
TCP data															

Hình 3.14. Khuôn dạng của TCP segment

2.2 Cấu trúc gói dữ liệu TCP



NAP: Network Access Protocol

Hình 3.15. Cổng truy cập dịch vụ TCP

- Source port (16 bits) : số hiệu cổng của trạm nguồn
- Destination port (16 bits) : số hiệu cổng của trạm đích
- Sequence Number (32 bits): số hiệu của byte đầu tiên của segment trừ khi bit SYN được thiết lập. Nếu bit SYN được thiết lập thì Sequence Number là số hiệu tuần tự khởi đầu (ISN) và byte dữ liệu đầu tiên là ISN +1.
- Acknowledgment: vị trí tương đối của byte cuối cùng đã nhận đúng bởi thực thể gửi gói ACK cộng thêm 1. Giá trị của trường này còn được gọi là số tuần tự thu. Trường này được kiểm tra chỉ khi bit ACK=1.
- Data offset (4 bits) : số lượng từ 32 bit trong TCP header. Tham số này chỉ ra vị trí bắt đầu của vùng dữ liệu
- Reserved (6 bits) : dành để dùng trong tương lai. Phải được thiết lập là 0.
- Control bits : các bit điều khiển
 - URG : vùng con trả khẩn (Urgent Pointer) có hiệu lực.
 - ACK : vùng báo nhận (ACK number) có hiệu lực.
- PSH : chức năng Push. PSH=1 thực thể nhận phải chuyển dữ liệu này cho ứng dụng tức thời.
- RST : thiết lập lại (reset) kết nối.
- SYN : đồng bộ hóa các số hiệu tuần tự, dùng để thiết lập kết nối TCP.
- FIN : thông báo thực thể gửi đã kết thúc gửi dữ liệu.
- Window (16 bits): cấp phát credit để kiểm soát luồng dữ liệu (cơ chế của sổ). Đây chính là số lượng các byte dữ liệu, bắt đầu từ byte được chỉ ra trong vùng ACK number, mà trạm nguồn đã sẵn sàng để nhận

- Checksum (16 bits) : mã kiểm soát lỗi (theo phương pháp CRC) cho toàn bộ segment (header + data)
- Urgent pointer (16 bits) : con trỏ này trỏ tới số hiệu tuần tự của byte đi theo sau dữ liệu khẩn, cho phép bên nhận biết được độ dài của dữ liệu khẩn. Vùng này chỉ có hiệu lực khi bit URG được thiết lập
- Options (độ dài thay đổi): khai báo các option của TCP, trong đó có độ dài tối đa của vùng TCP data trong một segment
- Padding (độ dài thay đổi) : phần chèn thêm vào header để bảo đảm phần header luôn kết thúc ở một mốc 32 bits. Phần thêm này gồm toàn số 0.
- TCP data (độ dài thay đổi) : chứa dữ liệu của tầng trên, có độ dài tối đa ngầm định là 536 bytes. Giá trị này có thể điều chỉnh bằng cách khai báo trong vùng options.

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

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

2.3. Thiết lập và kết thúc kết nối TCP

Thiết lập kết nối

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

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

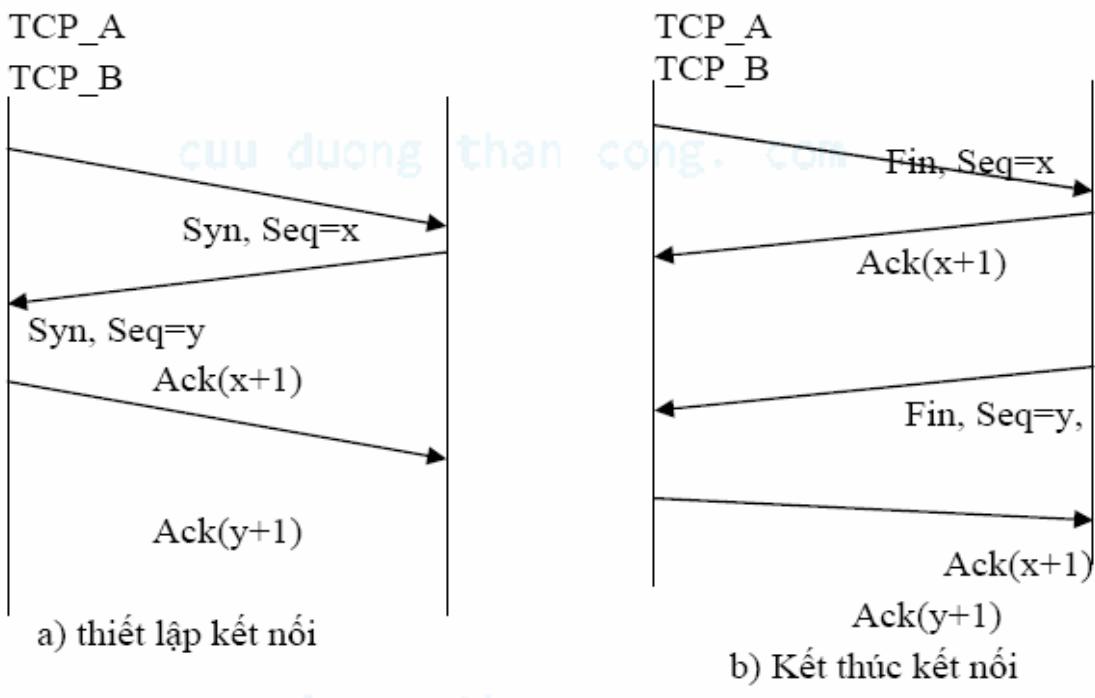
Khi thực thể TCP của phần mềm dịch vụ nhận được thông điệp SYN, nó gửi lại gói SYN cùng giá trị ISN của nó và đặt cờ ACK=1 trong trường hợp sẵn sàng nhận kết nối. Thông điệp này còn chứa giá trị ISN của tiến trình trạm trong

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

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

Kết thúc kết nối

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



Hình 3.16. Quá trình kết nối theo ba bước

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

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

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

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

Mục 1: Mạng máy tính

I. Lịch sử mạng máy tính

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

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

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

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

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

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

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

II. Giới thiệu mạng máy tính

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

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

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

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

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

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

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

I.1.2. Định nghĩa mạng máy tính

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

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

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

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

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

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

I.2.1. Đường truyền

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

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

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

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

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

I.2.2. Kỹ thuật chuyển mạch:

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

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

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

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

I.2.3. Kiến trúc mạng

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

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

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

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

I.2.4. Hệ điều hành mạng

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

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

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

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

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

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

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

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

I.3. Phân loại mạng máy tính

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

- Khoảng cách địa lý của mạng
- Kỹ thuật chuyển mạch mà mạng áp dụng
- Kiến trúc mạng
- Hệ điều hành mạng sử dụng ...

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

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

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

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

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

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

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

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

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

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

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

Ưu điểm của phương pháp này là :

- Hiệu suất sử dụng đường truyền cao vì không bị chiếm dụng độc quyền mà được phân chia giữa nhiều thực thể truyền thông.
- Mỗi nút mạng có thể lưu trữ thông tin tạm thời sau đó mới chuyển thông báo đi, do đó có thể điều chỉnh để làm giảm tình trạng tắc nghẽn trên mạng.
- Có thể điều khiển việc truyền tin bằng cách sắp xếp độ ưu tiên cho các thông báo.

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

Nhược điểm của phương pháp này là:

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

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

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

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

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

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

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

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

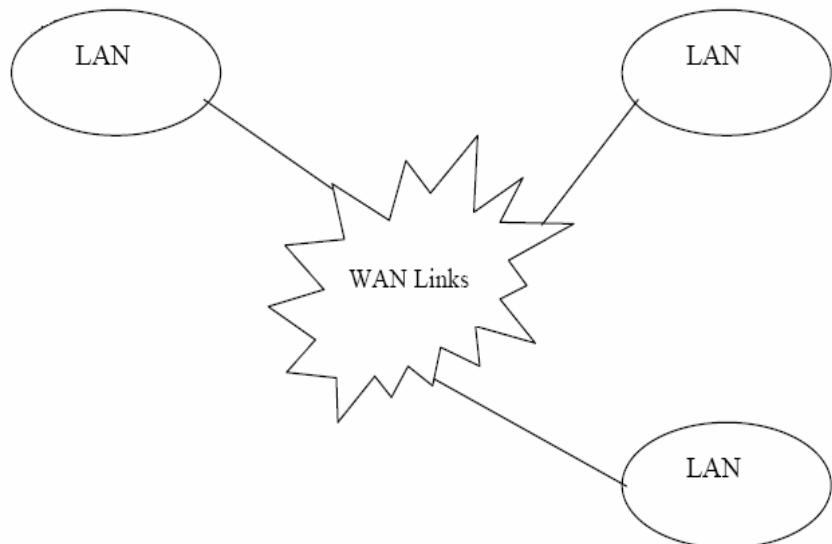
Khi phân loại theo topo mạng người ta thường có phân loại thành: mạng hình sao, tròn, tuyến tính

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

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

I.3.4. Phân loại theo hệ điều hành mạng

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



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

I.4.1. Mạng cục bộ

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

Mạng cục bộ có các đặc tính sau:

- Tốc độ truyền dữ liệu cao
- Phạm vi địa lý giới hạn
- Sở hữu của một cơ quan/tổ chức

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

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

- Tốc độ truyền dữ liệu không cao
- Phạm vi địa lý không giới hạn
- Thường triển khai dựa vào các công ty truyền thông, bưu điện và dùng các hệ thống truyền thông này để tạo dựng đường truyền
- Một mạng WAN có thể là sở hữu của một tập đoàn/tổ chức hoặc là mạng kết nối của nhiều tập đoàn/tổ chức

I.4.3. Liên mạng INTERNET

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

- Là một mạng toàn cầu
- Là sự kết hợp của vô số các hệ thống truyền thông, máy chủ cung cấp thông tin và dịch vụ, các máy trạm khai thác thông tin
- Dựa trên nhiều nền tảng truyền thông khác nhau, nhưng đều trên nền giao thức TCP/IP
- Là sở hữu chung của toàn nhân loại
- Càng ngày càng phát triển mãnh liệt

I.4.4. Mạng INTRANET

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

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

II. Mạng cục bộ, kiến trúc mạng cục bộ

II.1. Mạng cục bộ

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

Đặc điểm của mạng cục bộ

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

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

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

II.2. Kiến trúc mạng cục bộ

II.2.1. Đồ hình mạng (Network Topology)

* Định nghĩa Topo mạng:

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

Có hai kiểu nối mạng chủ yếu đó là :

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

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

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

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

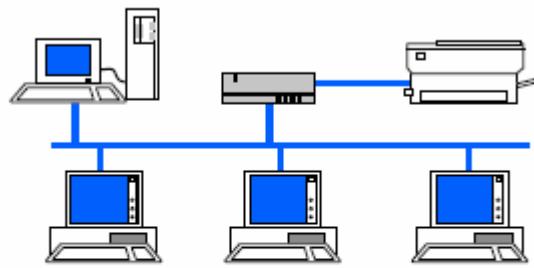
Tó pô của mạng rộng thường là nói đến sự liên kết giữa các mạng cục bộ thông qua các bộ dẫn đường (router). Đối với mạng rộng topo của mạng là hình trạng hình học của các bộ dẫn đường và các kênh viễn thông còn khi nói tới tó pô của mạng cục bộ người ta nói đến sự liên kết của chính các máy tính.

a) **Mạng hình sao**

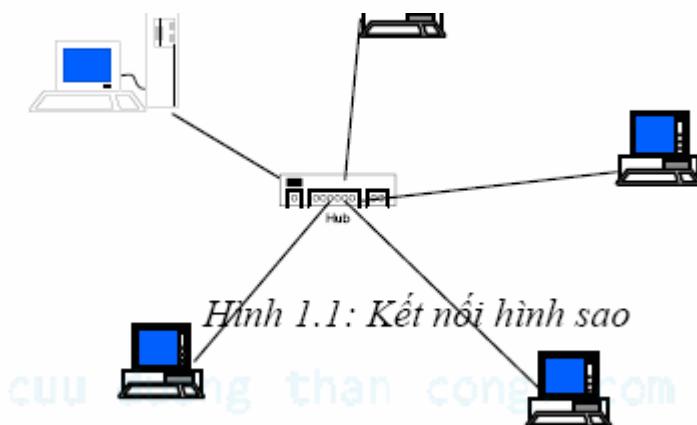
Mạng hình sao có tất cả các trạm được kết nối với một thiết bị trung tâm có nhiệm vụ nhận tín hiệu từ các trạm và chuyển đến trạm đích. Tuỳ theo yêu cầu truyền thông trên mạng mà thiết bị trung tâm có thể là bộ chuyển mạch (switch), bộ chọn đường (router) hoặc là bộ phân kênh (hub). Vai trò của thiết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

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

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



Hình 1.2. Kết nối kiểu bus



Hình 1.1: Kết nối hình sao

b) Mạng trực tuyến tính (Bus):

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

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

Ưu điểm : Dễ thiết kế, chi phí thấp

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

c) Mạng hình vòng

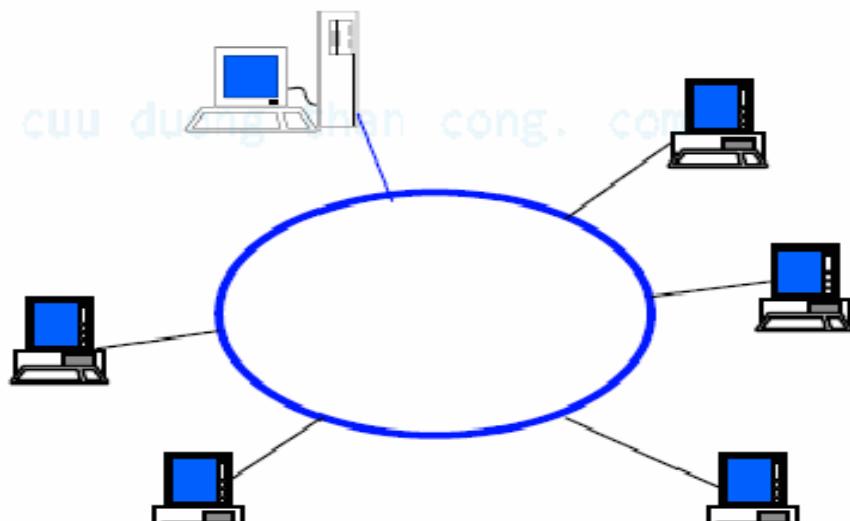
Trên mạng hình vòng tín hiệu được truyền đi trên vòng theo một chiều duy nhất. Mỗi trạm của mạng được nối với vòng qua một bộ chuyển tiếp (repeater) có nhiệm vụ nhận tín hiệu rồi chuyển tiếp đến trạm kế tiếp trên vòng. Như vậy tín hiệu được lưu chuyển trên vòng theo một chuỗi liên tiếp các liên kết điểm-điểm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

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

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

d) Kết nối hỗn hợp

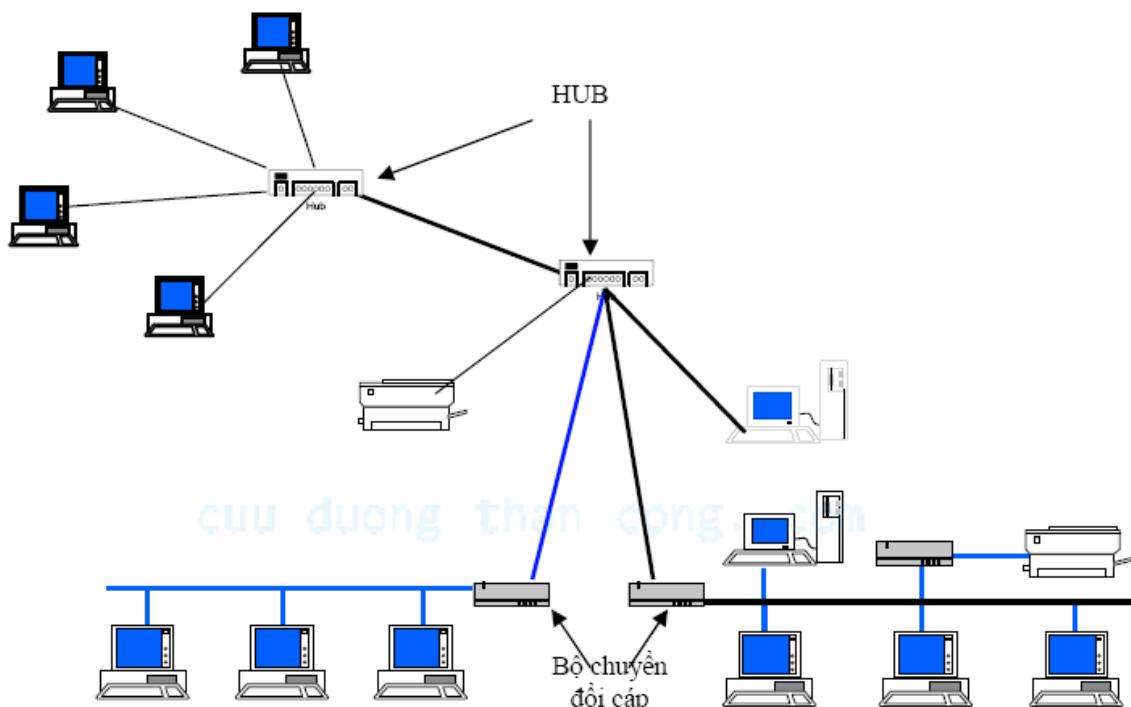
Là sự phối hợp các kiểu kết nối khác nhau, ví dụ hình cây là cấu trúc phân tầng của kiểu hình sao hay các HUB có thể được nối với nhau theo kiểu bus còn từ các HUB nối với các máy theo hình sao.



Hình 1.3 Kết nối kiểu vòng

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

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



Hình 1.4. Một kết nối hỗn hợp

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

- Truy nhập đường truyền một cách ngẫu nhiên, theo yêu cầu. Đường nhiên phải có tính đến việc sử dụng luân phiên và nếu trong trường hợp do có nhiều trạm cùng truyền tin dẫn đến tín hiệu bị trùng lênh nhau thì phải truyền lại.
- Có cơ chế trọng tài để cấp quyền truy nhập đường truyền sao cho không xảy ra xung đột

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

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

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

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

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

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

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

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

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

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

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

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

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

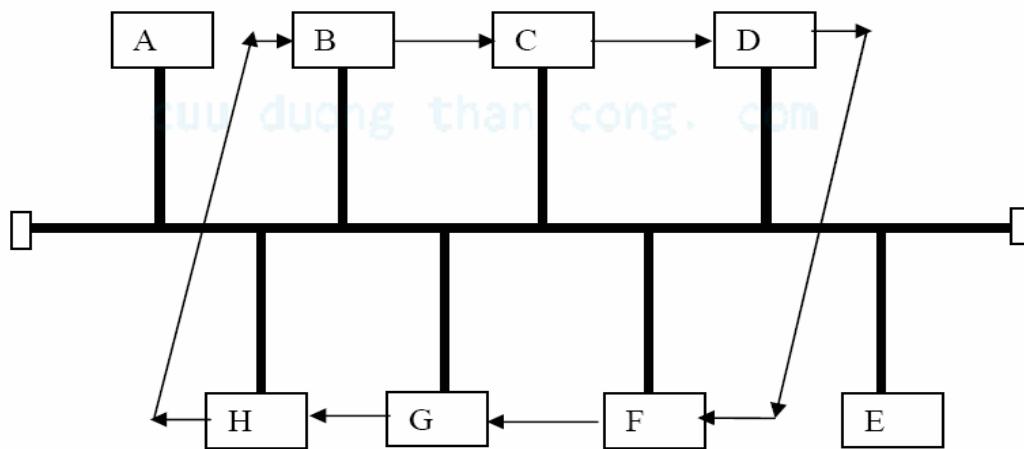
này.(như vậy phải tiếp tục nghe đường truyền trong khi truyền để phát hiện đụng độ (Listening While Talking))

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

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

II.3.2. Phương pháp Token Bus

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



Hình 1.5. Ví dụ về vòng logic

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

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

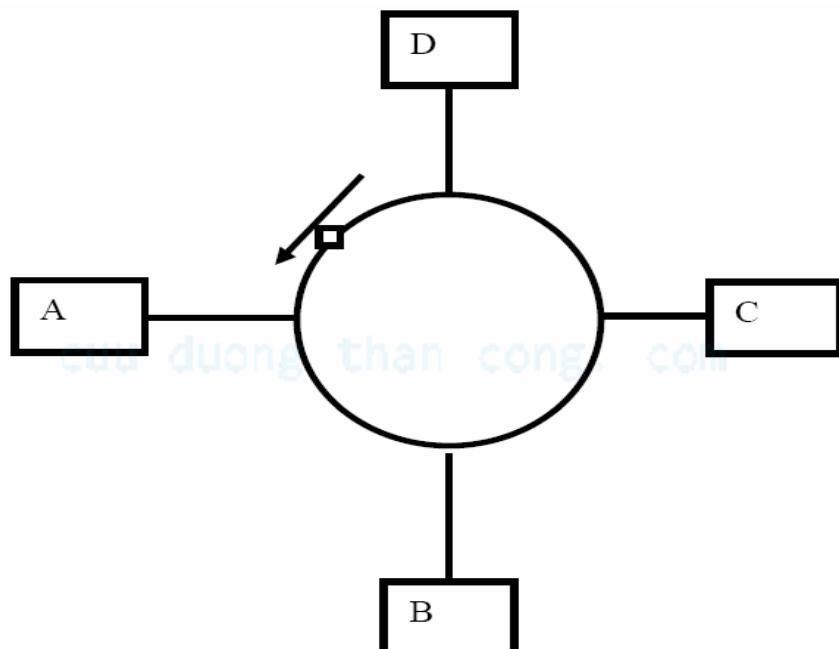
Việc thiết lập vòng logic không khó nhưng việc duy trì nó theo trạng thái thực tế của mạng mới là khó. Cụ thể phải thực hiện các chức năng sau:

- a) Bổ xung một trạm vào vòng logic : các trạm nằm ngoài vòng logic cần được xem xét một cách định kỳ để nếu có nhu cầu truyền dữ liệu thì được bổ xung vào vòng logic.
- b) Loại bỏ một vòng khỏi vòng logic : khi một trạm không có nhu cầu truyền dữ liệu thì cần loại bỏ nó ra khỏi vòng logic để tối ưu hóa việc truyền dữ liệu bằng thẻ bài
- c) Quản lý lỗi : một số lỗi có thể xảy ra như trùng hợp địa chỉ, hoặc đứt vòng logic.
- d) Khởi tạo vòng logic : khi khởi tạo mạng hoặc khi đứt vòng logic cần phải khởi tạo lại vòng logic.

II.3.2. Phương pháp Token Ring

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

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



Hình 1.6. Thẻ bài trong mạng Ring

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

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

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

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

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

III. Chuẩn hóa mạng máy tính

III.1. Vấn đề chuẩn hóa mạng và các tổ chức chuẩn hóa mạng

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

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

Có hai loại chuẩn cho mạng đó là :

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

b) Lớp liên kết dữ liệu

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

c) Lớp mạng

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

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

d) Lớp chuyển vận

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

e) Lớp phiên

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

f) Lớp thẻ hiện

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

g) Lớp ứng dụng

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

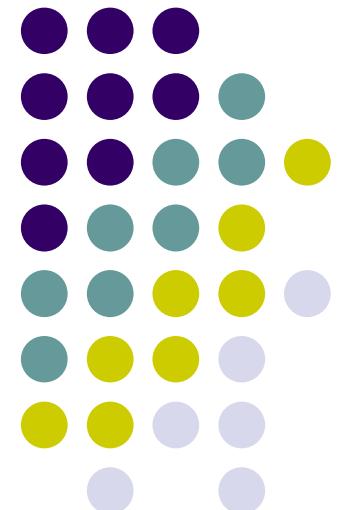
IEEE 802.12: là chuẩn đặc tả mạng cục bộ dựa trên công nghệ được đề xuất bởi AT&T, IBM và HP gọi là 100 VG - AnyLAN. Mạng này có topo mạng hình sao và một phương pháp truy nhập đường truyền có điều khiển tranh chấp. Khi có nhu cầu truyền dữ liệu, một trạm sẽ gửi yêu cầu đến hub và trạm chỉ có truyền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

Mạng máy tính

cuuduongthancong.com

Giảng viên: Ngô Hồng Sơn

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





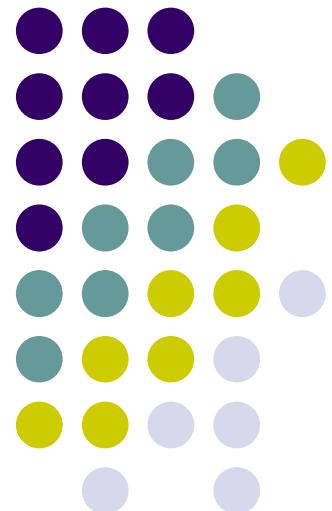
Nội dung

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

cuuduongthancong.com

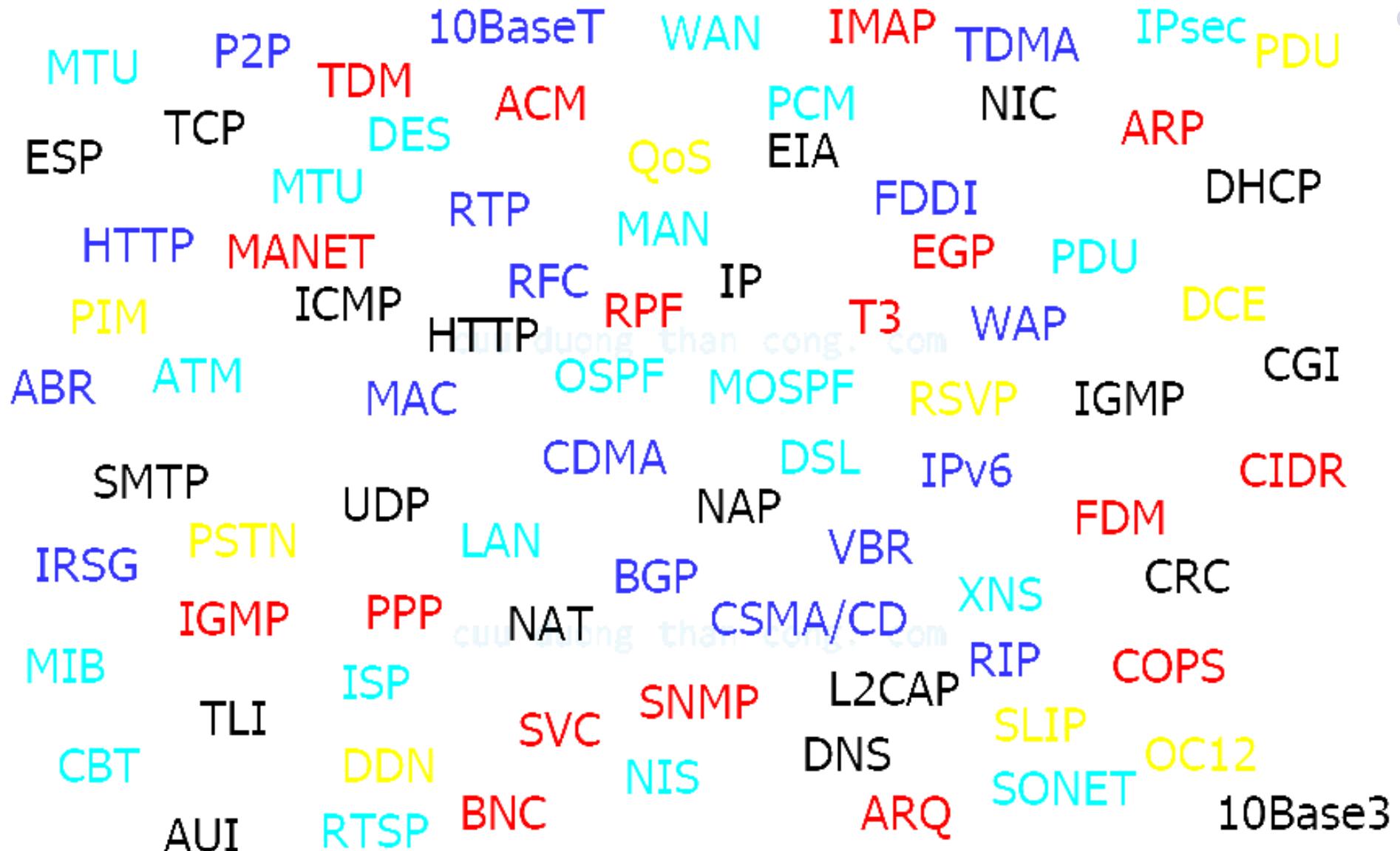
Giới thiệu môn học

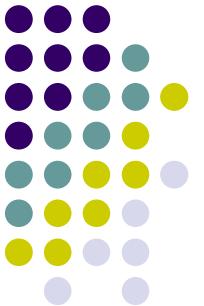
Mục đích
Chủ đề và lịch học
Đánh giá
Liên hệ giáo viên





Mục đích môn học

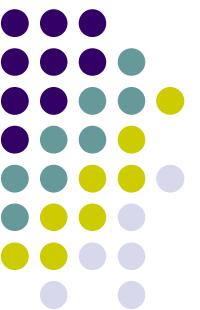




Mục đích môn học

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

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



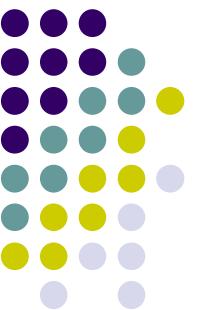
Lịch học dự kiến

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



Lịch học dự kiến

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



Đánh giá kết quả

- Bài tập lớn 40%

 - Hai bài

- Thi cuối kỳ 60%

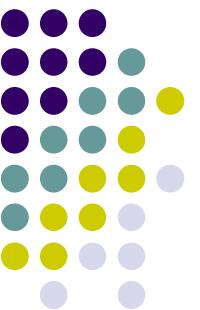
cuuduongthancong.com

cuuduongthancong.com



Cách làm việc

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



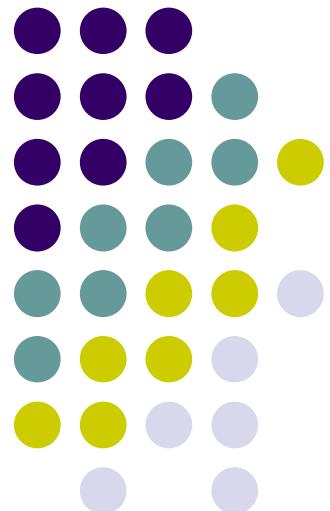
Tài liệu tham khảo

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

cuu duong than cong. com

Cơ bản về mạng máy tính

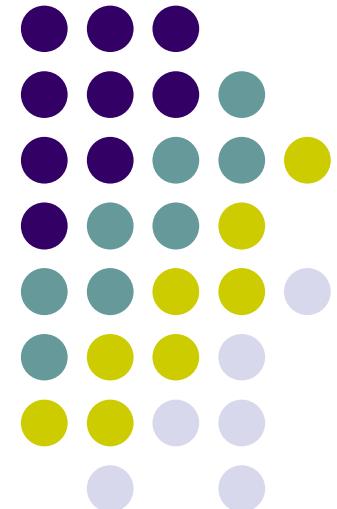
Khái niệm mạng máy tính
Kiến trúc mạng
Chuyển mạch gói vs. chuyển mạch kênh

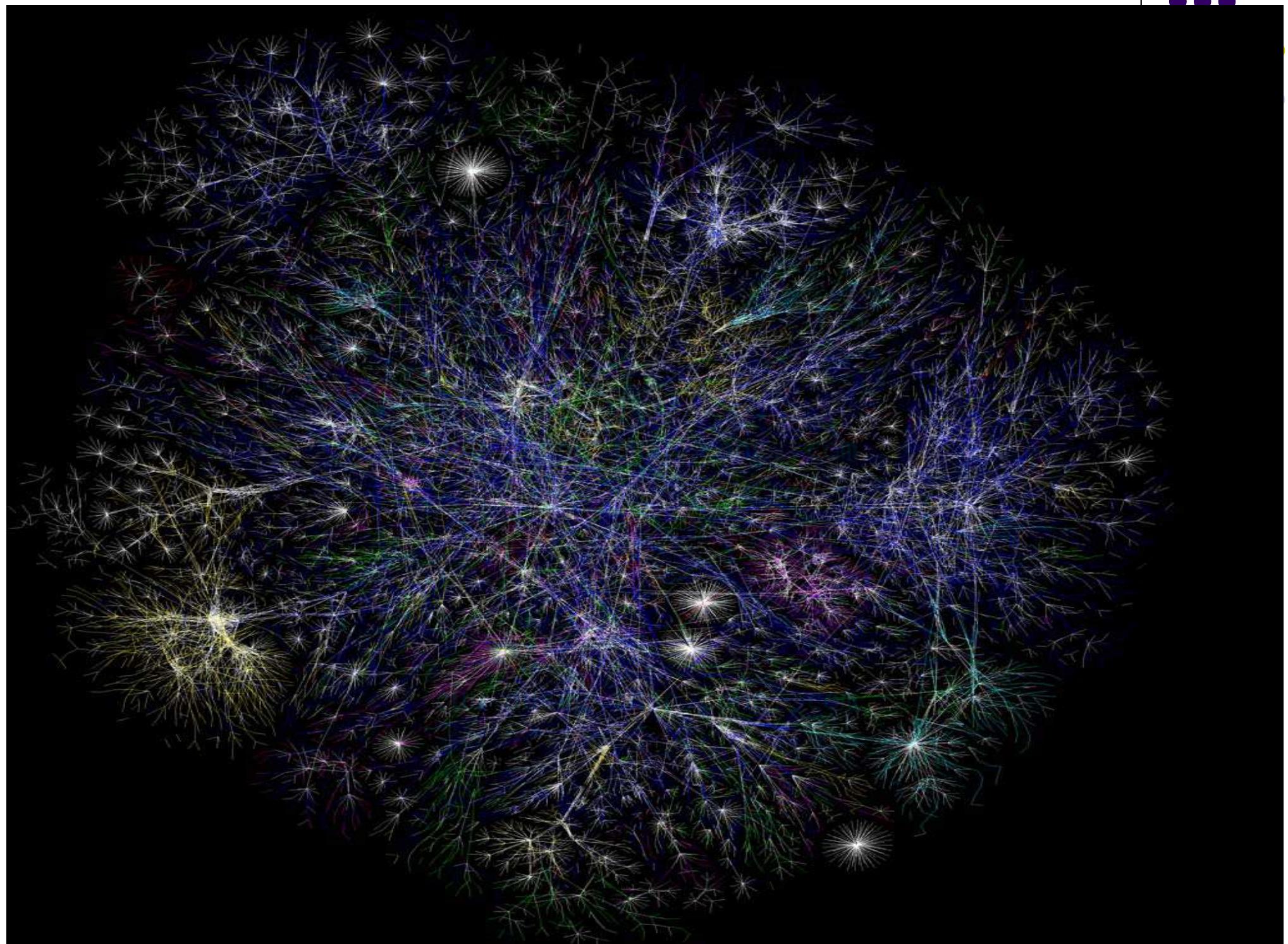


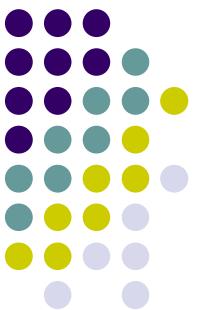
Mạng máy tính là gì

cuuduongthancong.com

cuuduongthancong.com

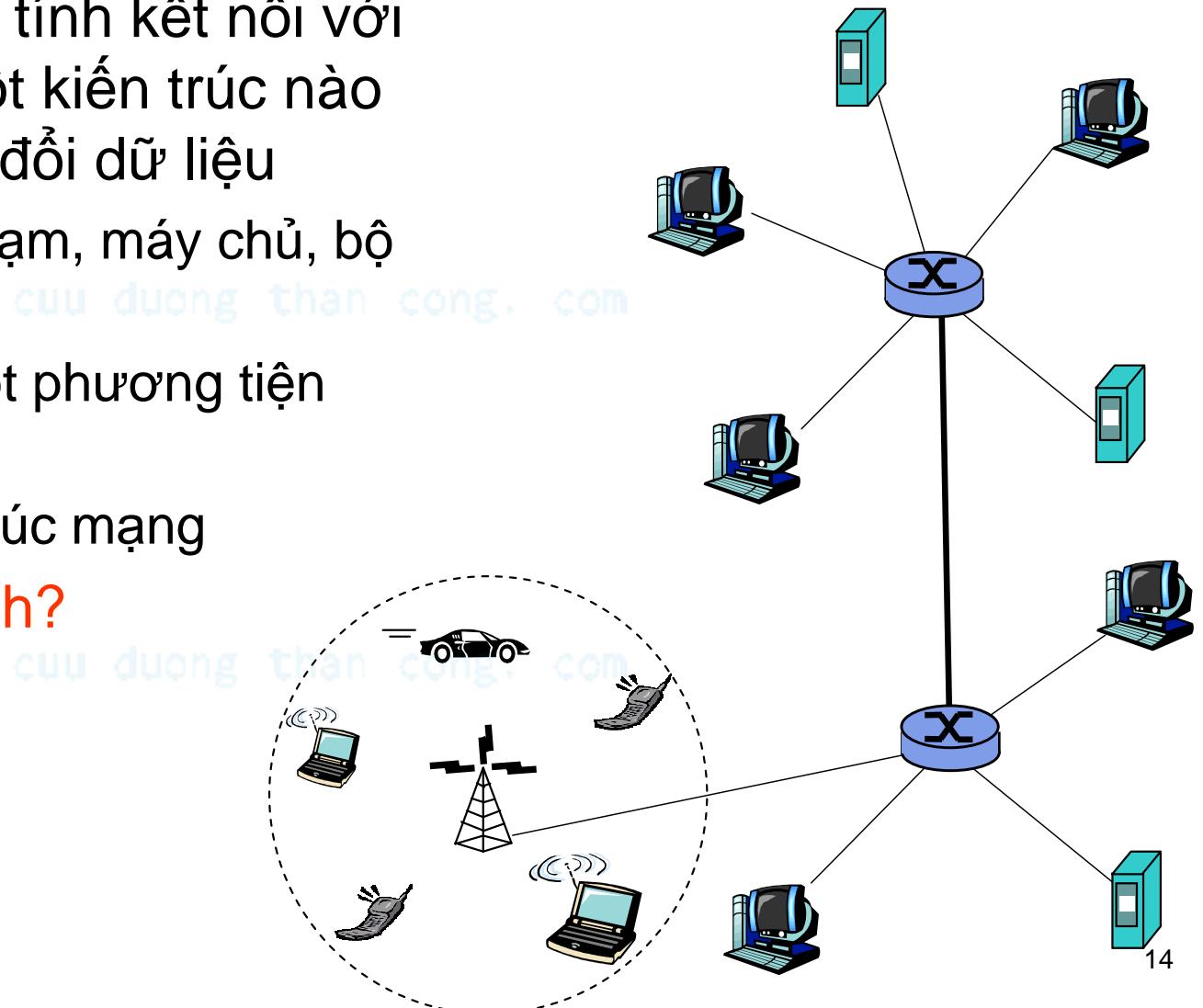
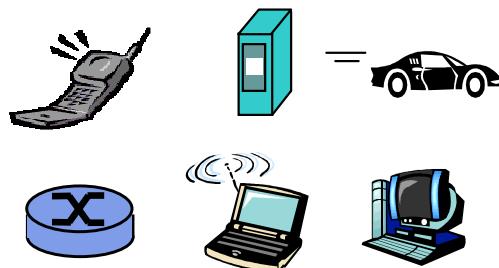


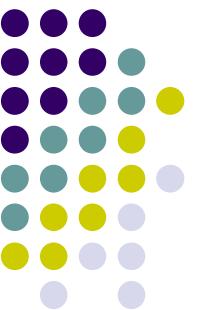




Khái niệm

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

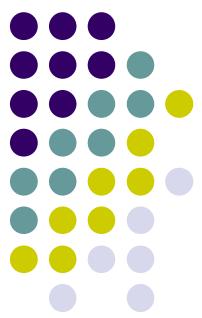




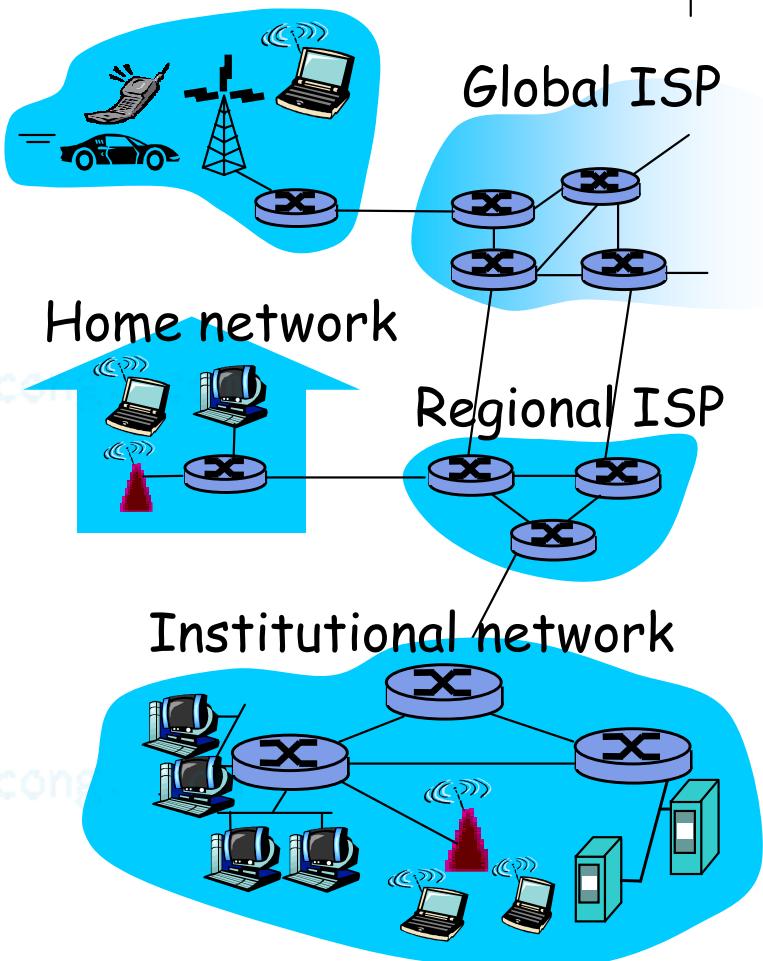
Ví dụ về mạng máy tính

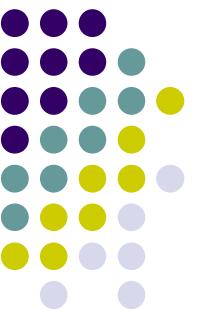
- Mạng Internet
- Mạng Ethernet
- Mạng LAN không dây: 802:11
- Hệ thống mạng ngân hàng: mạng lưới máy rút tiền
- Hệ thống bán vé tàu qua mạng
- ...

Internet ngày nay

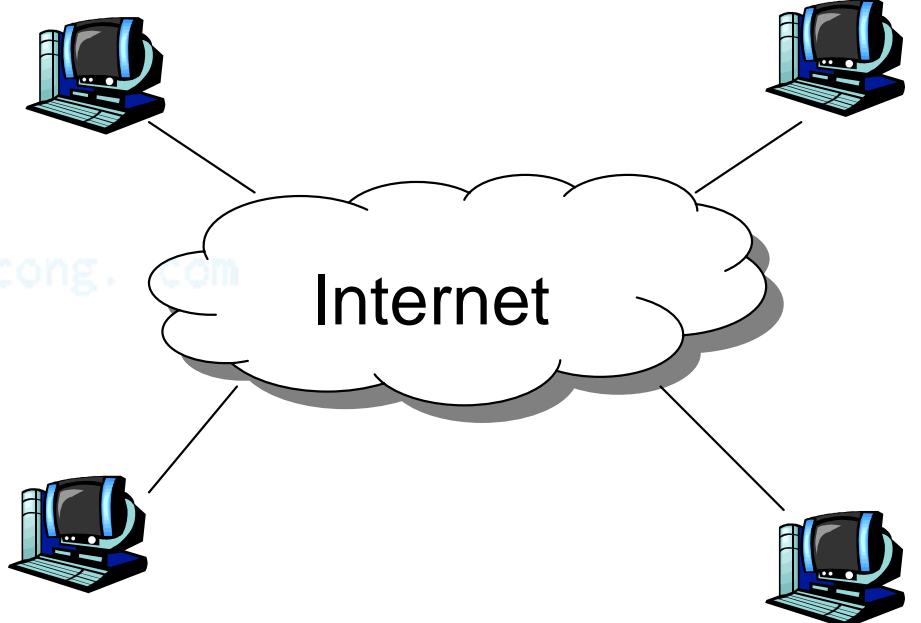
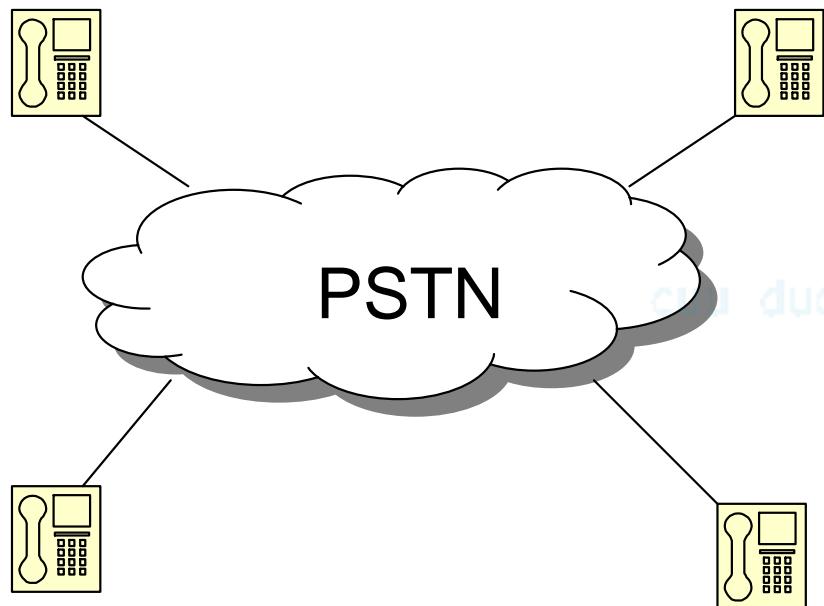


- Hàng triệu thiết bị kết nối: *hosts = end systems*
 - chạy *các ứng dụng mạng*
- *Đường truyền*
 - Cáp quang, đồng, vệ tinh, ...
 - Tốc độ truyền = *băng thông*
- *Bộ định tuyến*: chuyển tiếp các gói tin (dữ liệu)

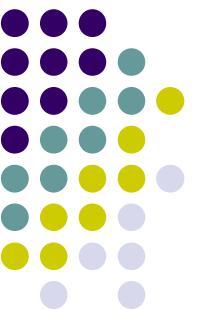




Xử lý tập trung hay phân tán

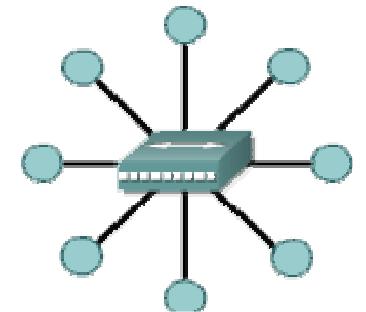
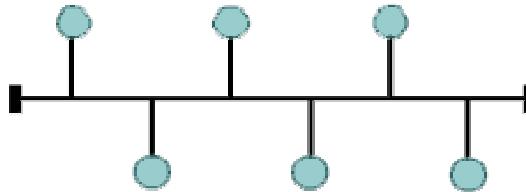


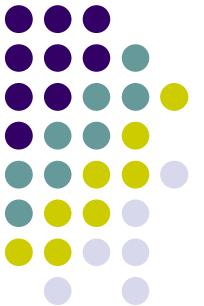
- Mạng điện thoại công cộng, tập trung: mạng xử lý mọi thứ
- Máy tính có khả năng lớn hơn
- Hầu hết các chức năng tập trung ở mạng máy tính
- Mạng: Truyền dữ liệu



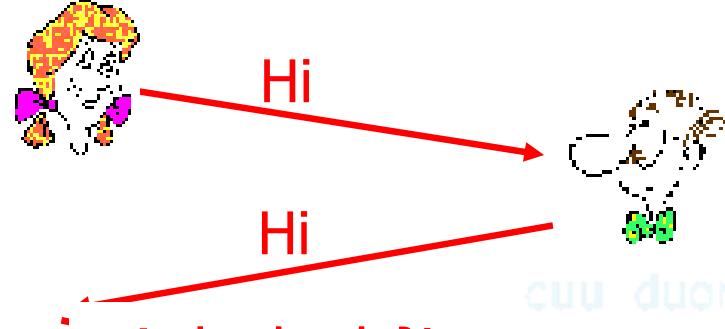
Kiến trúc mạng

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





Giao thức là gì?



Anh cho hỏi
mấy giờ rồi ạ?
→
← 2:00

Thời gian

Giao thức người-người



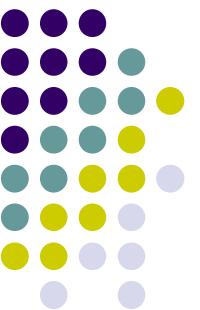
yêu cầu

trả lời

request

response

Giao thức máy-máy



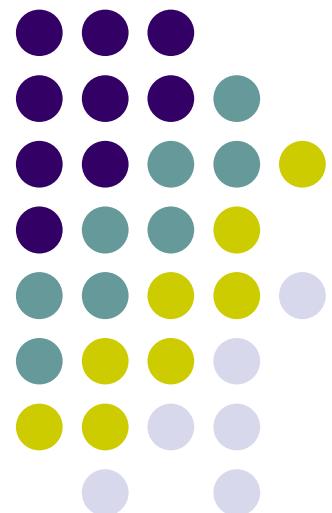
Giao thức mạng

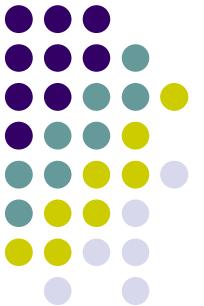
- **Protocol:** Quy tắc để truyền thông
 - Gửi một thông điệp với yêu cầu hoặc thông tin
 - Nhận một thông điệp với thông tin, sự kiện hoặc hành động
- Định nghĩa khuôn dạng và thứ tự truyền, nhận thông điệp giữa các thực thể trên mạng hoặc các hành động tương ứng khi nhận được thông điệp
- Ví dụ về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

Mô hình truyền thông

Chuyển mạch gói vs. Chuyển mạch kênh
Hướng liên kết vs. Không liên kết

cuuduongthancong.com

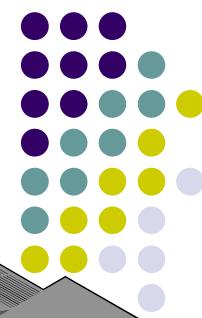




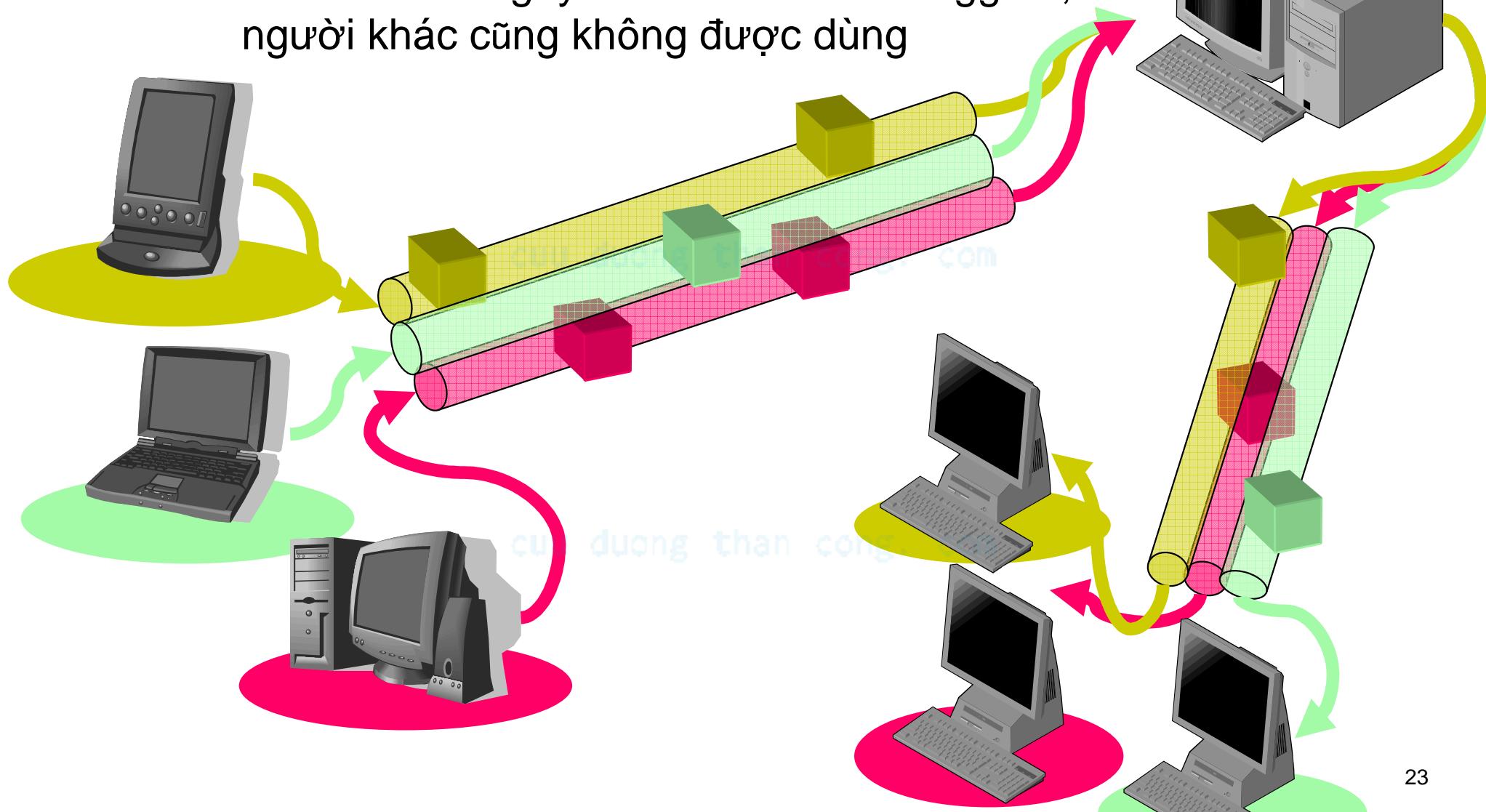
Chuyển mạch gói vs. Chuyển mạch kênh

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

Chuyển mạch kênh



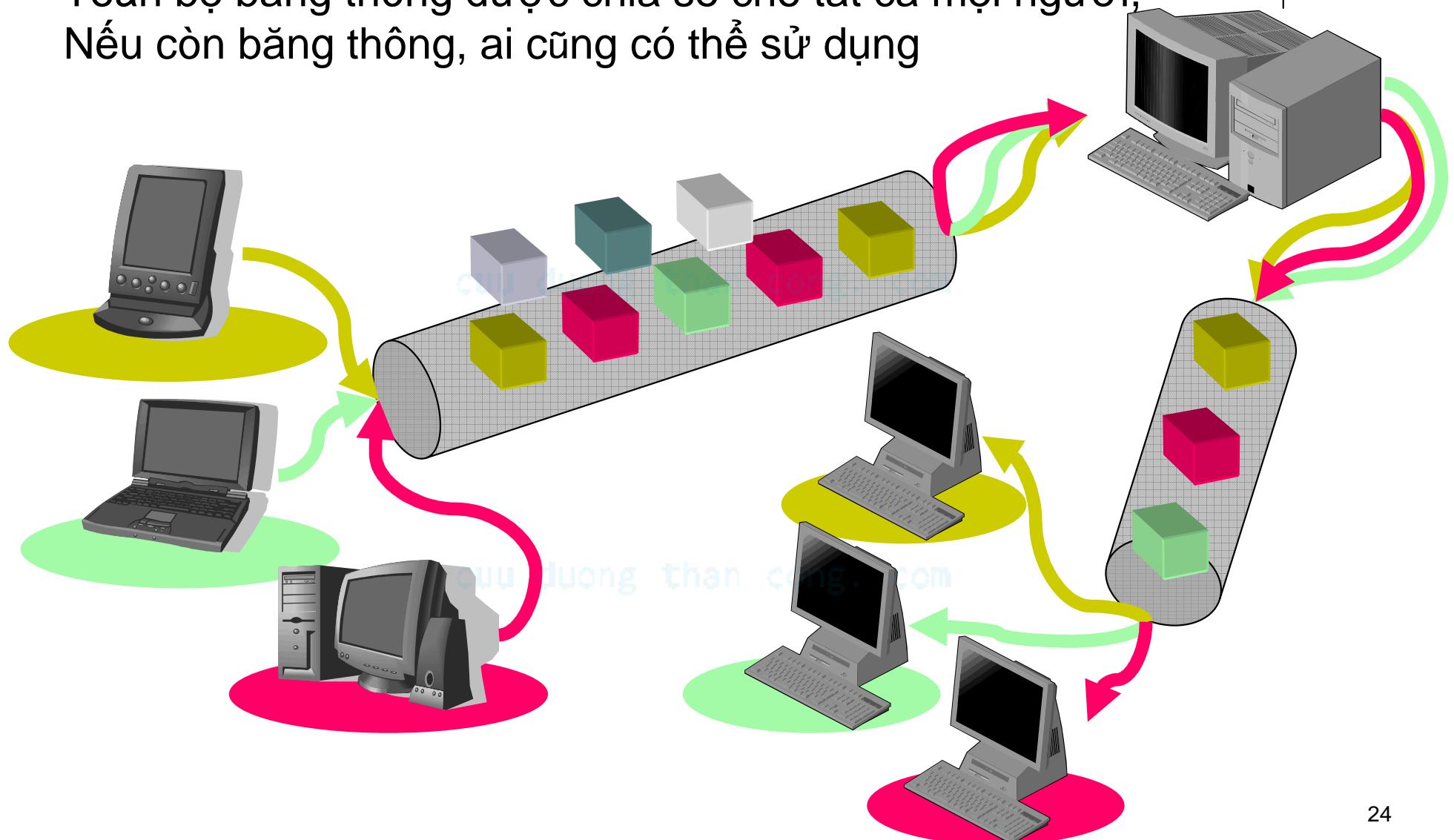
Tài nguyên được gán riêng cho mỗi kênh
Kể cả khi tài nguyên của kênh đó đang rỗi,
người khác cũng không được dùng

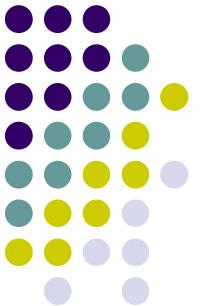


Chuyển mạch gói



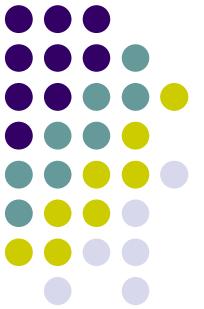
Toàn bộ băng thông được chia sẻ cho tất cả mọi người,
Nếu còn băng thông, ai cũng có thể sử dụng





Chuyển mạch gói vs. Chuyển mạch kênh

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



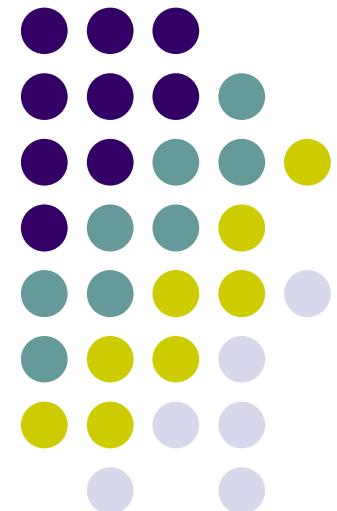
Truyền thông hướng liên kết vs. không liên kết

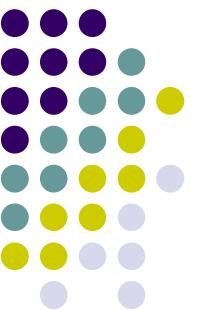
- Truyền thông hướng liên kết :
 - Dữ liệu được truyền qua một liên kết đã được thiết lập
 - Ba giai đoạn: Thiết lập liên kết, truyền dữ liệu, Hủy bỏ liên kết
 - Tin cậy
- Truyền thông không liên kết
 - Không thiết lập liên kết, chỉ có giai đoạn truyền dữ liệu
 - Không tin cậy - “Best effort”

Một số tham số trong mạng

cuuduongthancong.com

cuuduongthancong.com

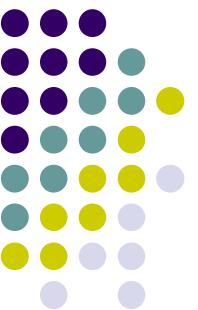




Các tham số cơ bản

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

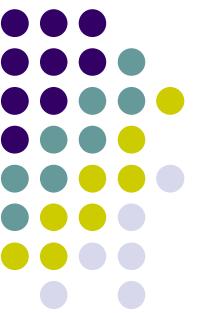
cuuduongthancong.com



Bảng thông

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

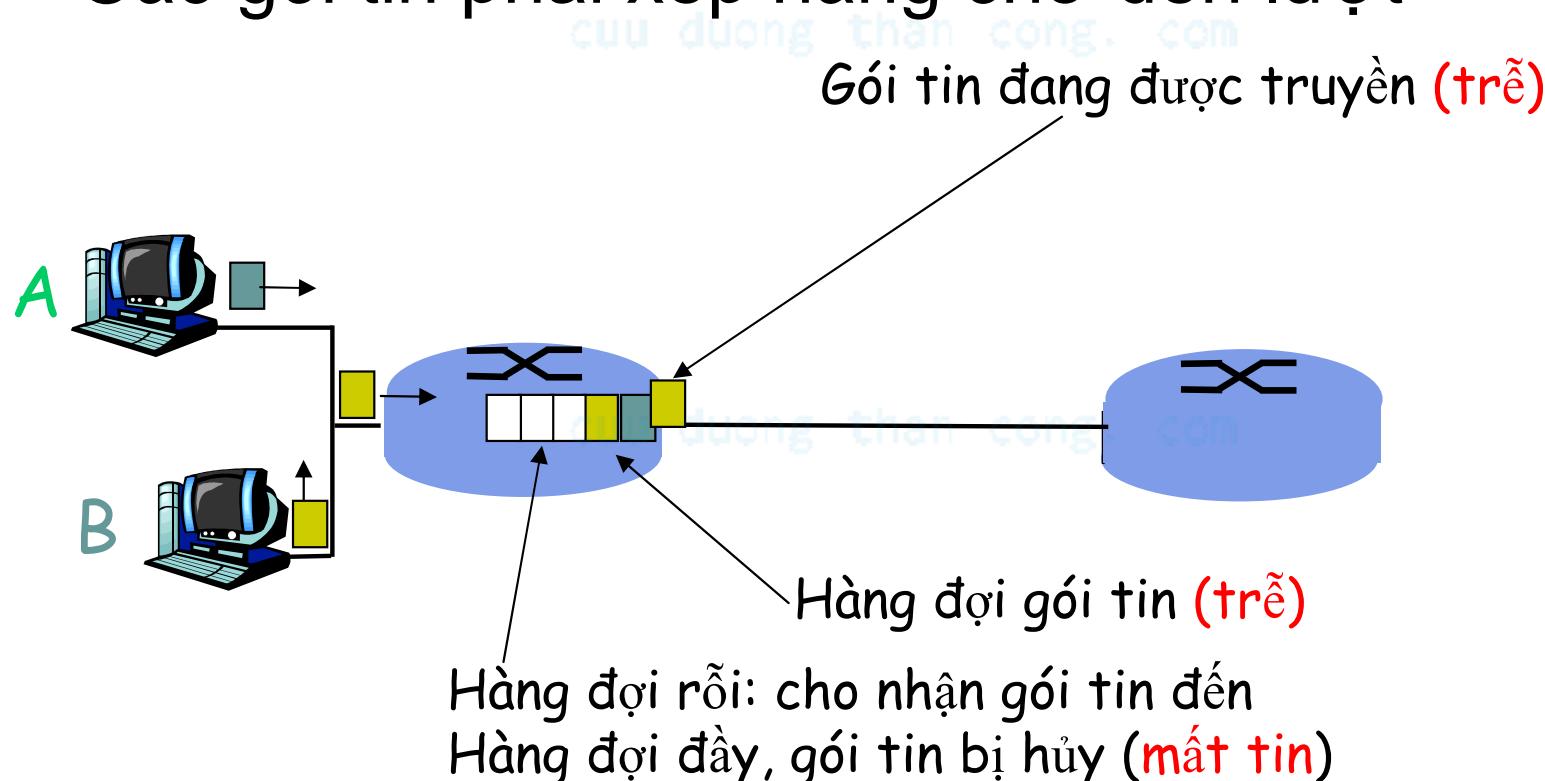
cuu duong than cong. com

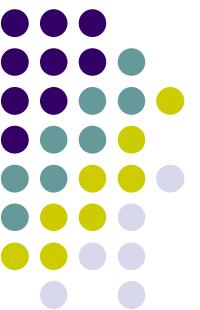


Vì sao có mất và trễ tin?

Các gói tin phải xếp hàng trong bộ định tuyến!

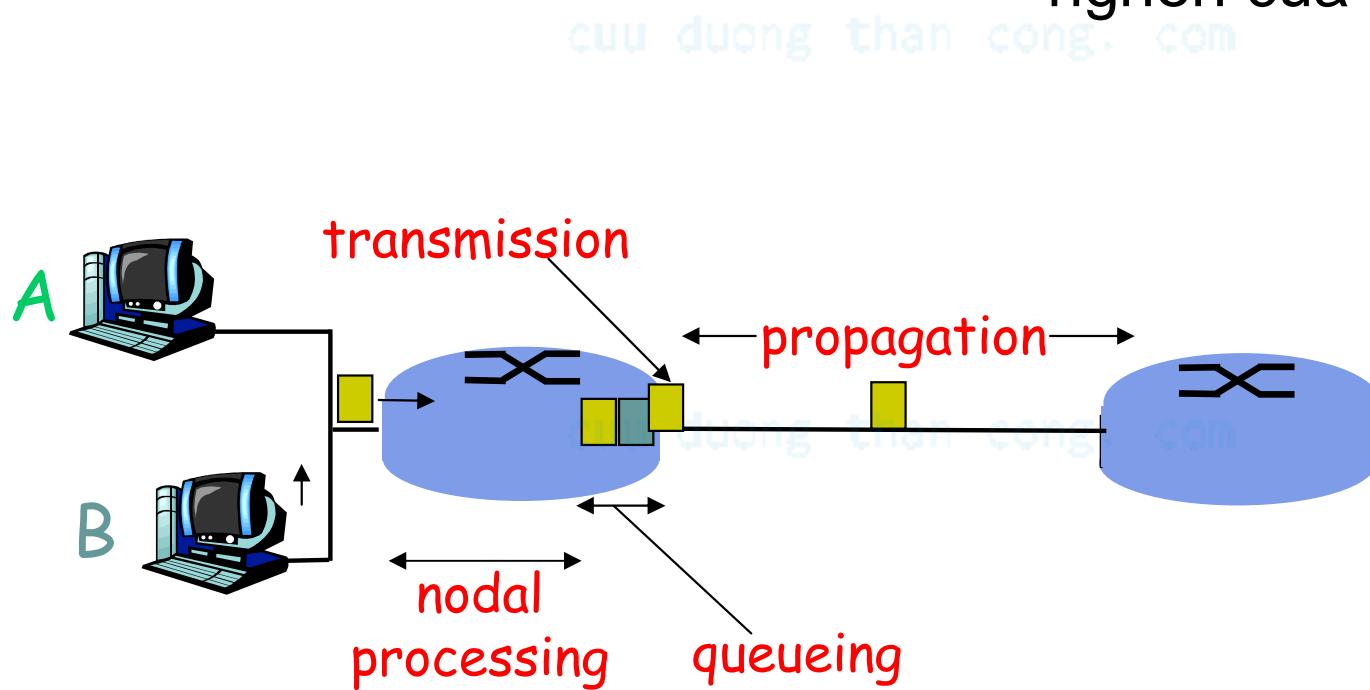
- Tốc độ đến của các gói tin vượt quá khả năng đường ra
- Các gói tin phải xếp hàng chờ đến lượt

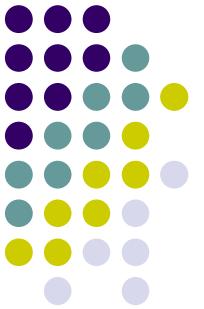




4 nguyên nhân gây trễ tin

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





4 nguyên nhân gây trễ tin

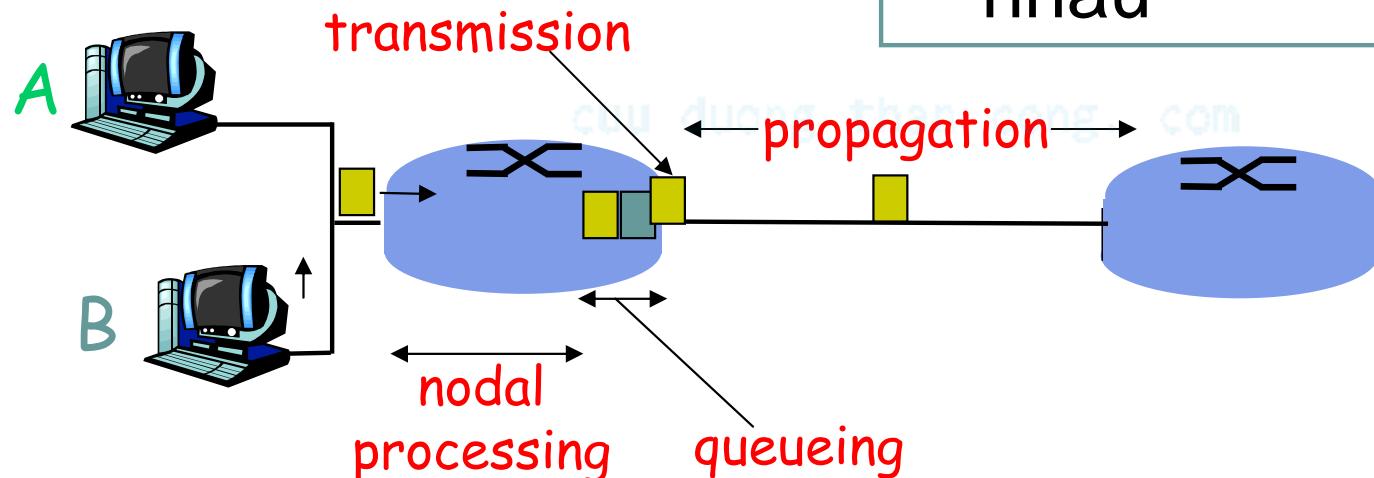
3. Trễ truyền tin:

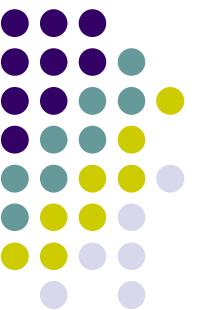
- R = băng thông (bps)
- L = độ dài packet (bits)
- Trễ truyền tin = L/R

4. Trễ lan truyền:

- d = độ dài đường truyền
- s = tốc độ tín hiệu ($\sim 2 \times 10^8$ m/sec)
- Trễ lan truyền = d/s

Chú ý: s và R rất khác nhau





Tổng thời gian trễ

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

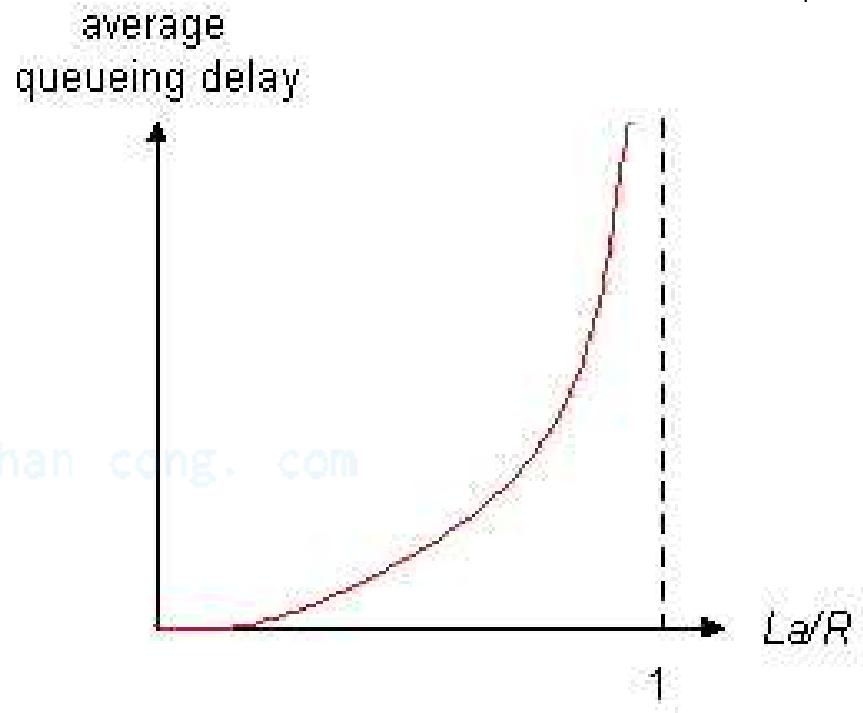
- d_{proc} = processing delay
 - Vài microsecs hay ít hơn
- d_{queue} = queuing delay
 - Phụ thuộc vào độ tắc nghẽn
- d_{trans} = transmission delay
 - = L/R , lớn với những đường truyền tốc độ thấp
- d_{prop} = propagation delay
 - vài microsecs tới hàng trăm msec



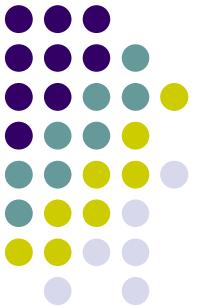
Trễ hàng đợi

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

Lưu lượng đến = La/R

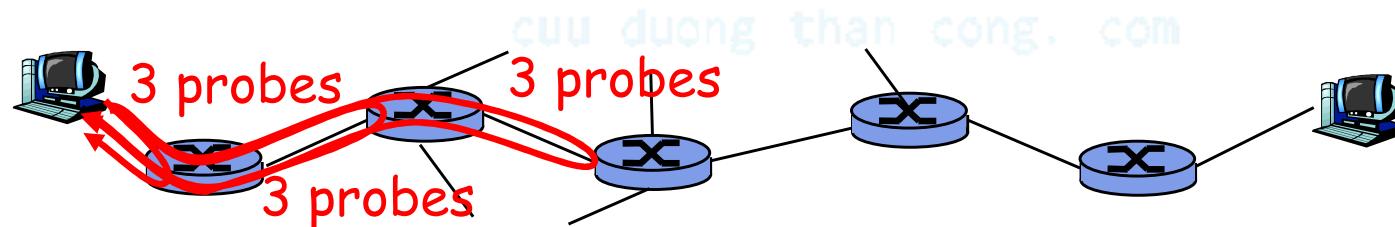


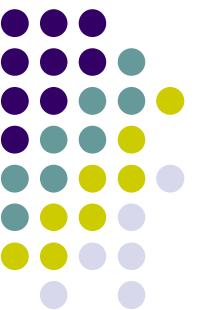
- $La/R \sim 0$: trễ hàng đợi nhỏ
- $La/R \rightarrow 1$: trễ lớn dần lên
- $La/R > 1$: quá khả năng, trễ vô cùng



Độ trễ và đường đi thực tế trên Internet

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

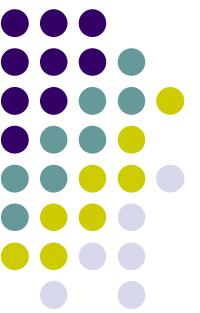




Ví dụ

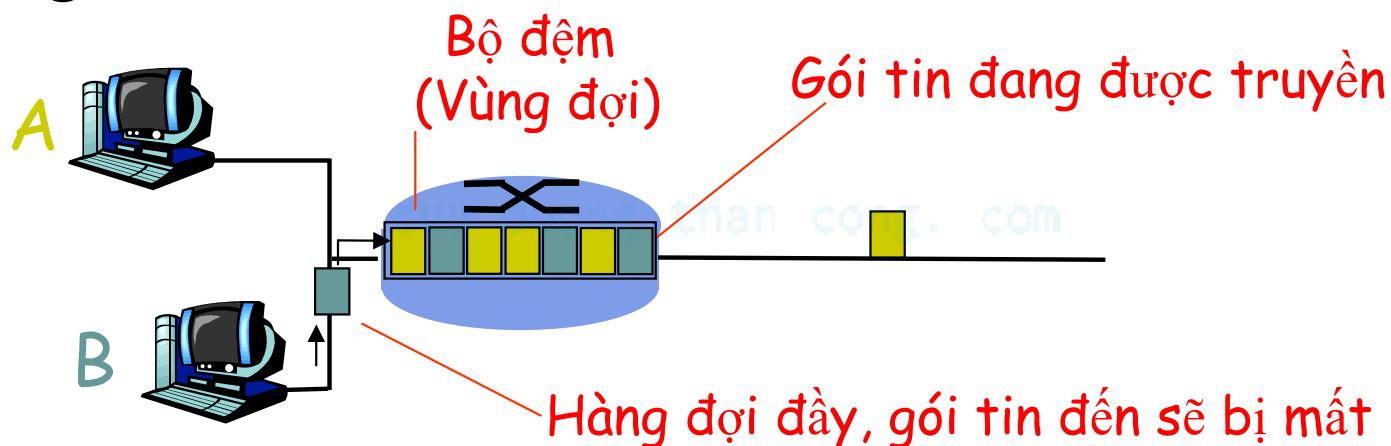
traceroute: gaia.cs.umass.edu to www.eurecom.fr

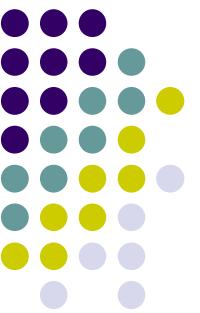
Three delay measurements from gaia.cs.umass.edu to cs-gw.cs.umass.edu						
1	cs-gw (128.119.240.254)	1 ms	1 ms	2 ms		
2	border1-rt-fa5-1-0.gw.umass.edu (128.119.3.145)	1 ms	1 ms	2 ms		
3	cht-vbns.gw.umass.edu (128.119.3.130)	6 ms	5 ms	5 ms		
4	jn1-at1-0-0-19.wor.vbns.net (204.147.132.129)	16 ms	11 ms	13 ms		
5	jn1-so7-0-0-0.wae.vbns.net (204.147.136.136)	21 ms	18 ms	18 ms		
6	abilene-vbns.abilene.ucaid.edu (198.32.11.9)	22 ms	18 ms	22 ms		
7	nycm-wash.abilene.ucaid.edu (198.32.8.46)	22 ms	22 ms	22 ms		
8	62.40.103.253 (62.40.103.253)	104 ms	109 ms	106 ms		
9	de2-1.de1.de.geant.net (62.40.96.129)	109 ms	102 ms	104 ms		
10	de.fr1.fr.geant.net (62.40.96.50)	113 ms	121 ms	114 ms		
11	renater-gw.fr1.fr.geant.net (62.40.103.54)	112 ms	114 ms	112 ms		
12	nio-n2.cssi.renater.fr (193.51.206.13)	111 ms	114 ms	116 ms		
13	nice.cssi.renater.fr (195.220.98.102)	123 ms	125 ms	124 ms		
14	r3t2-nice.cssi.renater.fr (195.220.98.110)	126 ms	126 ms	124 ms		
15	eurecom-valbonne.r3t2.ft.net (193.48.50.54)	135 ms	128 ms	133 ms		
16	194.214.211.25 (194.214.211.25)	126 ms	128 ms	126 ms		
17	***					
18	***					* means no response (probe lost, router not replying)
19	fantasia.eurecom.fr (193.55.113.142)	132 ms	128 ms	136 ms		



Mất tin (loss)

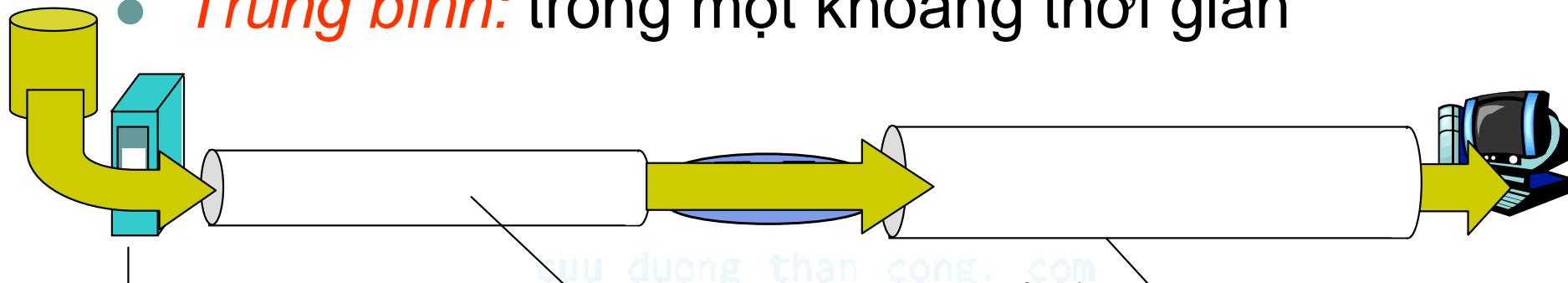
- Hàng đợi (vùng đệm) của mỗi đường truyền có kích thước giới hạn
- Gói tin nào tới hàng đợi đầy sẽ bị mất
- Gói tin bị mất có thể được truyền lại hoặc không.





Thông lượng

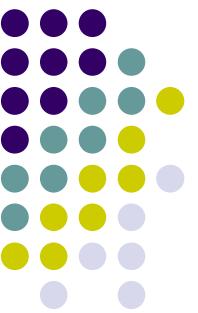
- *Thông lượng*: tốc độ (đơn vị bits/sec) mà tại đó các bits được truyền giữa bên gửi/bên nhận
 - *Tức thời*: tốc độ tại một thời điểm
 - *Trung bình*: trong một khoảng thời gian



Bên gửi: gửi dòng
bits lên trên kênh

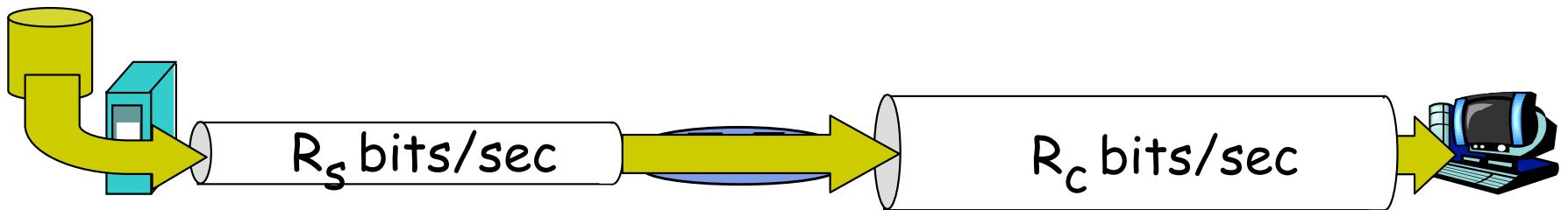
Kênh có khả năng
 R_s bits/sec)

Kênh có khả năng
 R_c bits/sec)



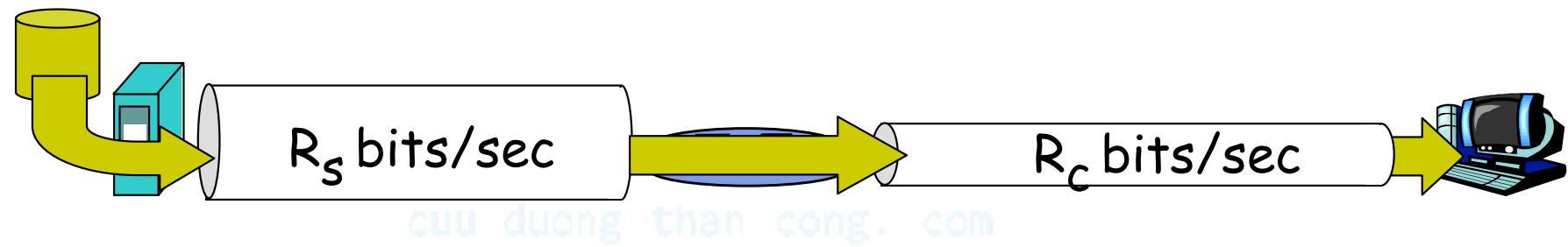
Thông lượng

- $R_s < R_c$ Thông lượng trung bình?



cuu duong than cong. com

- $R_s > R_c$ Thông lượng trung bình?



cuu duong than cong. com

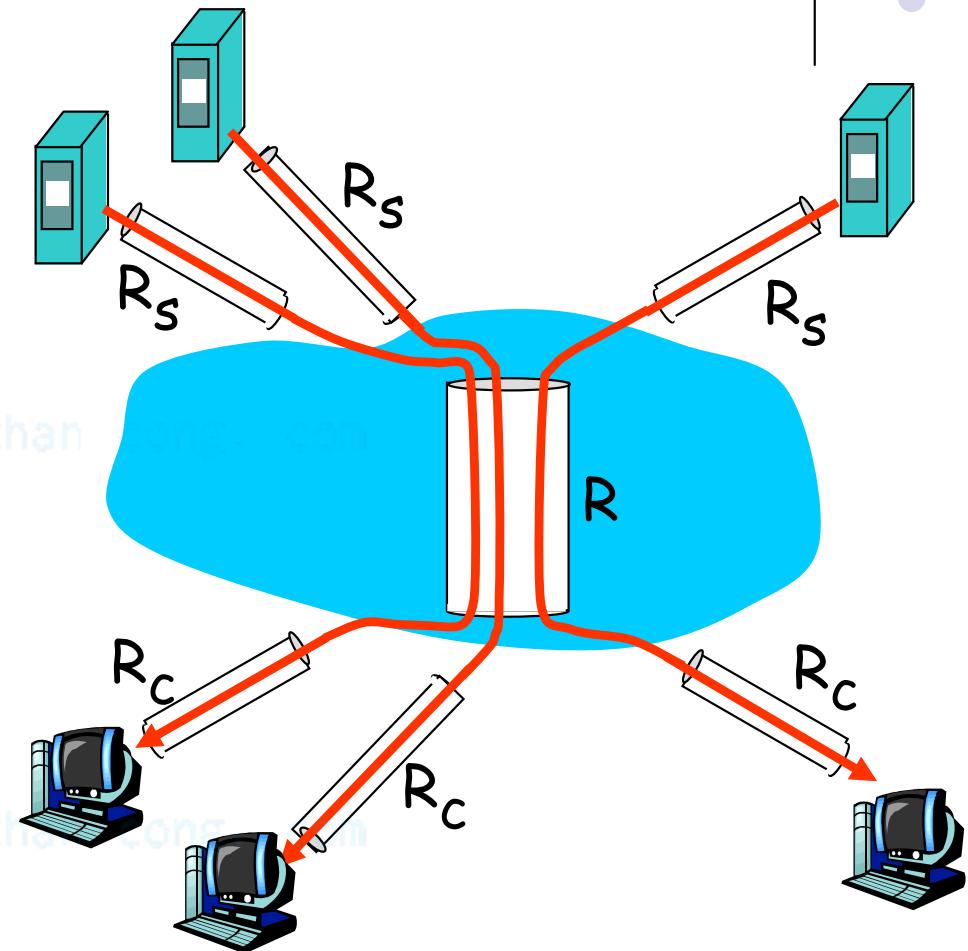
Nút thắt cổ chai

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



Thông lượng: Ví dụ trên Internet

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

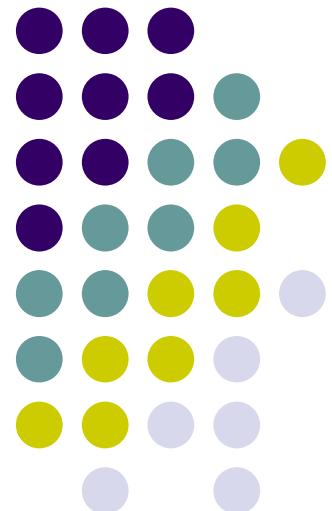


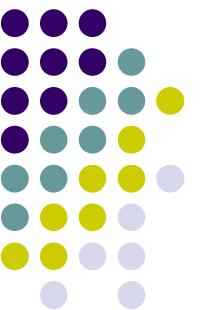
10 liên kết chia sẻ 1 đường R
bits/sec

Lược sử mạng & Internet

cuuduongthancong.com

cuuduongthancong.com

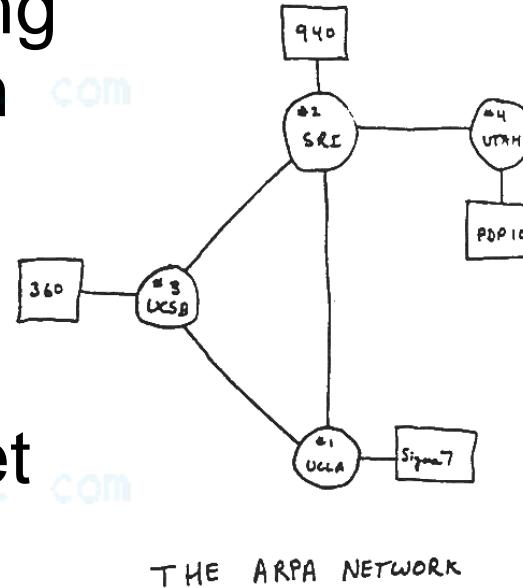


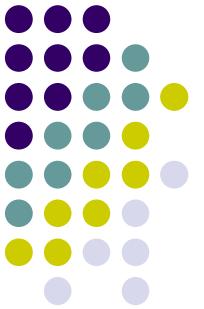


Thời kỳ đầu

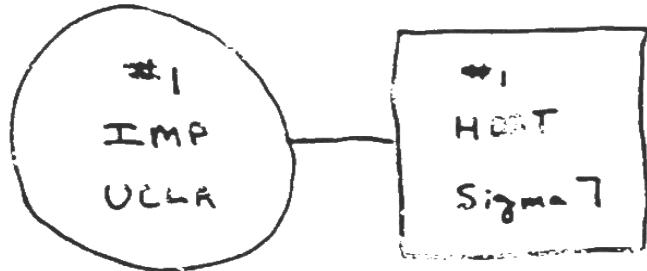
1961-1972: Các nguyên lý mạng chuyển mạch gói

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





Nguồn gốc Internet



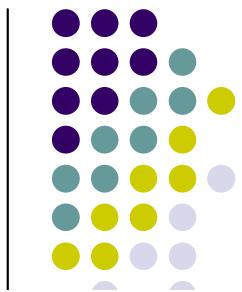
- Bắt đầu từ một thí nghiệm của dự án của ARPA
- Một liên kết giữa hai nút mạng (IMP tại UCLA và IMP tại SRI).

THE ARPA NETWORK DIAGRAM

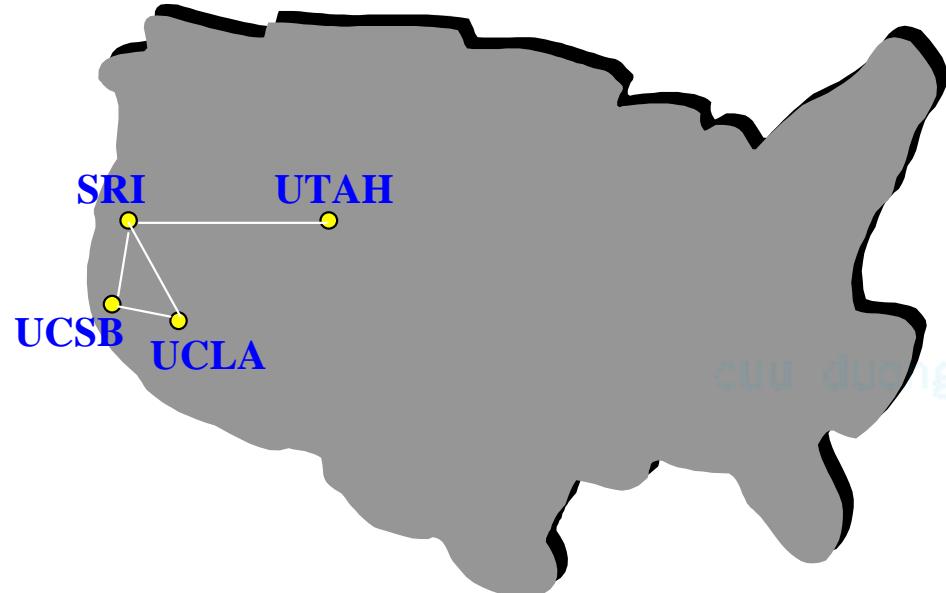
SEPT. 1969
I NODE

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

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



3 tháng sau, 12/1969



Một mạng hoàn chỉnh với 4 nút,
56kbps

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

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

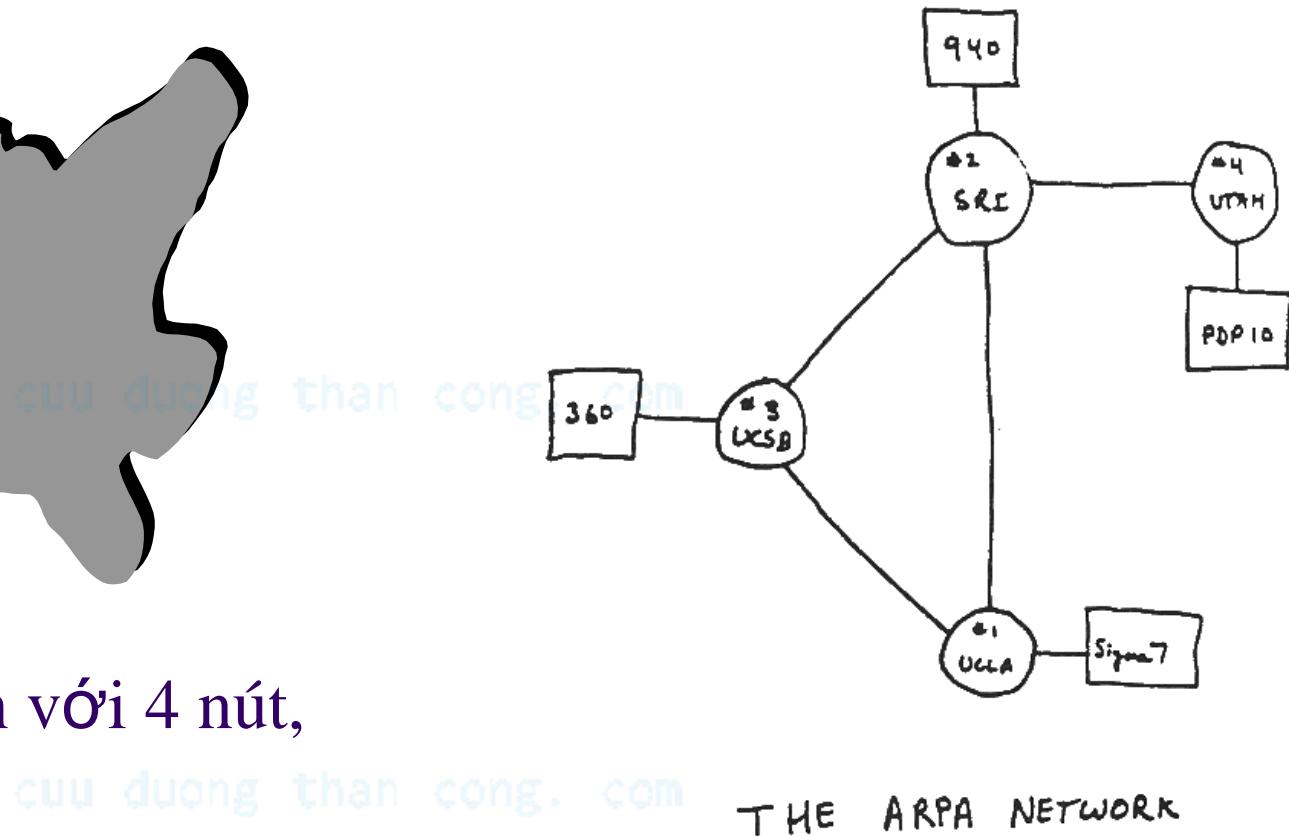
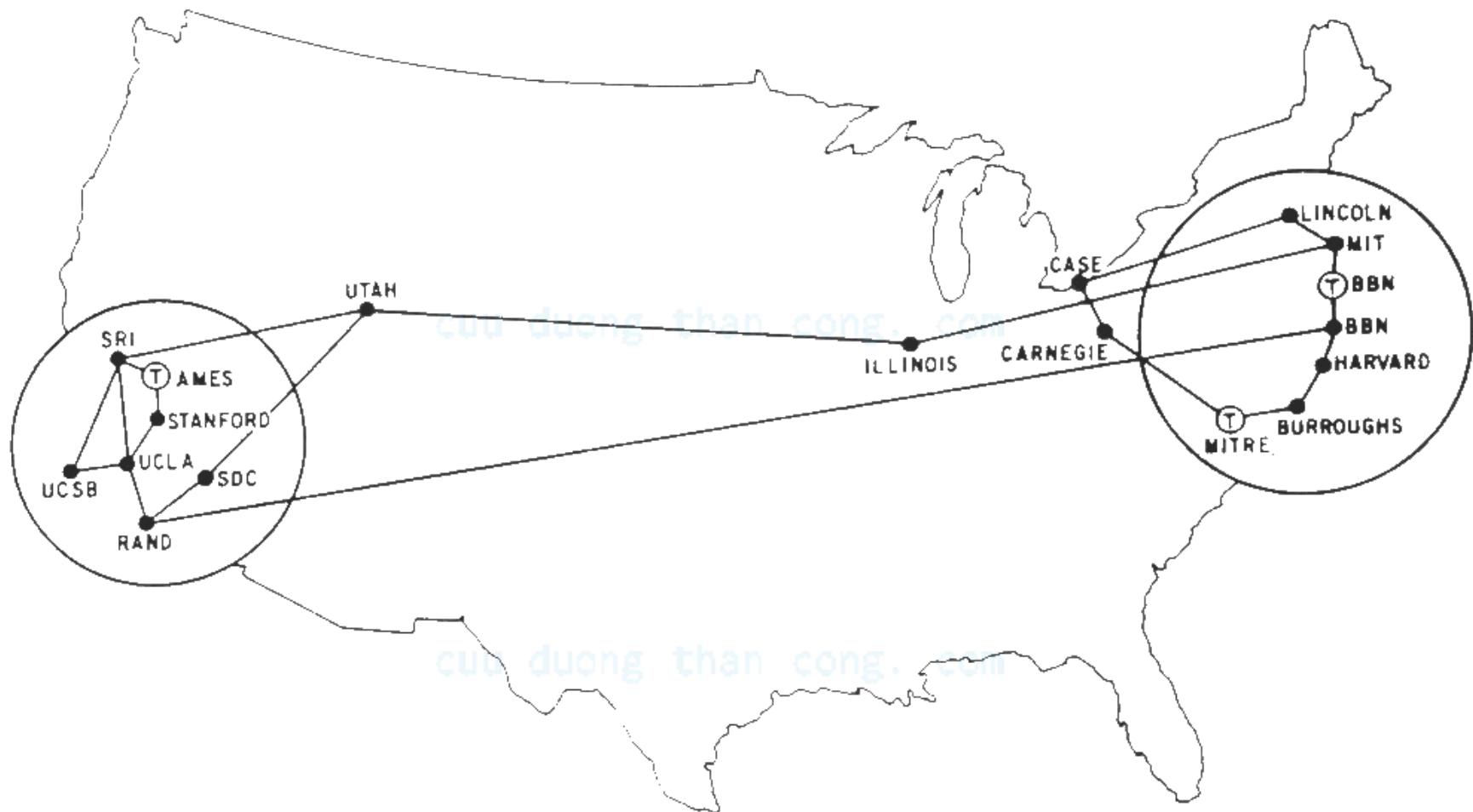
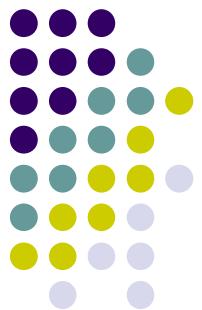


FIGURE 6.2 Drawing of 4 Node Network
(Courtesy of Alex McKenzie)

ARPANET thời kỳ đầu, 1971



Source: MAP 4 September 1971

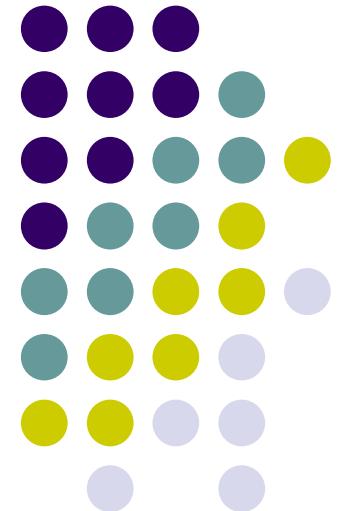
[http://www.cybergeography.org/
atlas/historical.html](http://www.cybergeography.org/atlas/historical.html)

Mạng phát triển với tốc độ thêm mỗi nút một tháng

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

cuuduongthancong.com

cuuduongthancong.com



Sự mở rộng của ARPANET, 1974

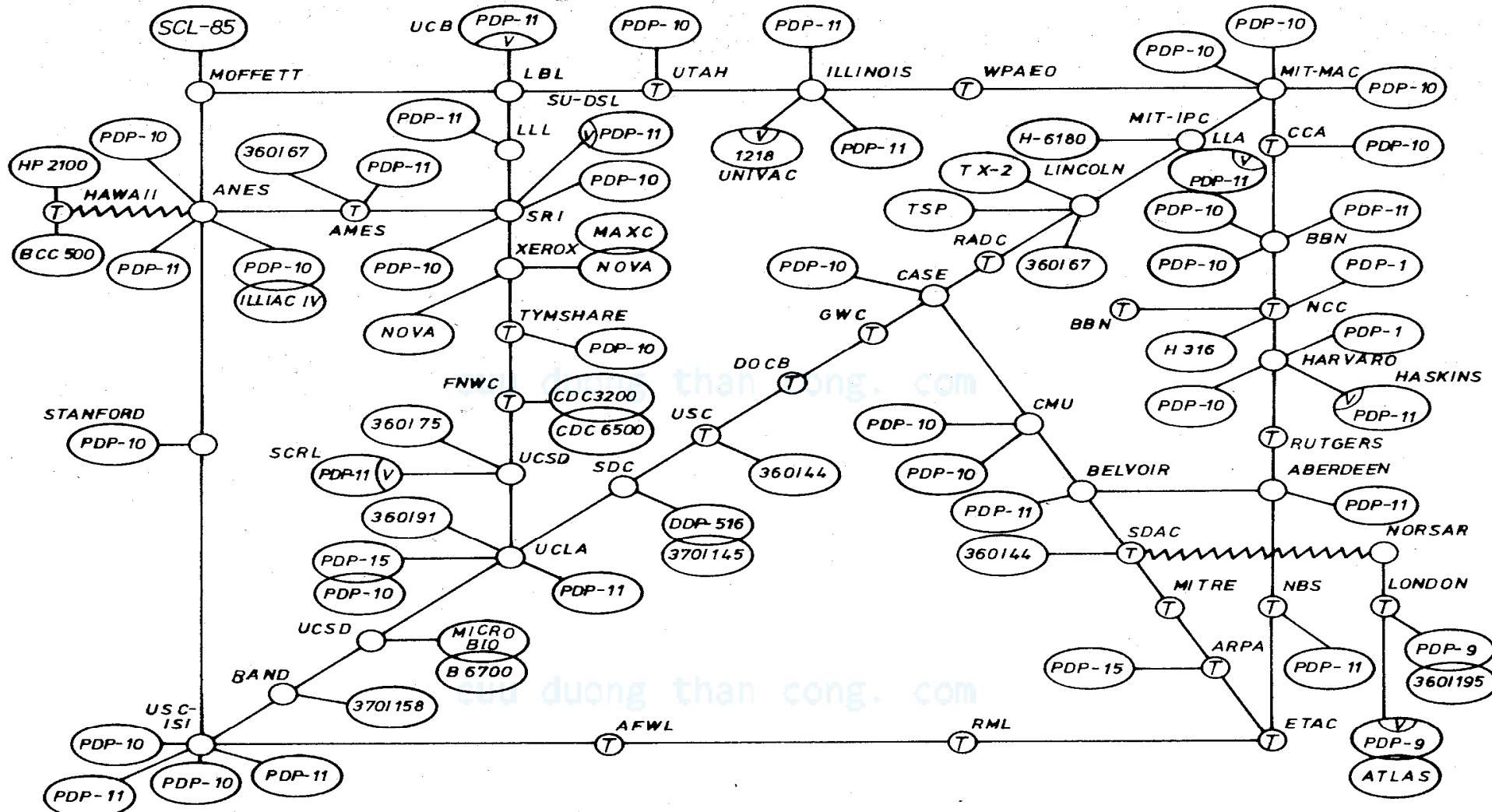
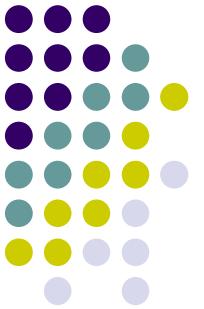


Abb. 4 ARPA NETwork, topologische Karte. Stand Juni 1974.

source:

[http://www.cybergeography.org/
atlas/historical.html](http://www.cybergeography.org/atlas/historical.html)

Lưu lượng mỗi ngày vượt quá 3.000.000 gói tin



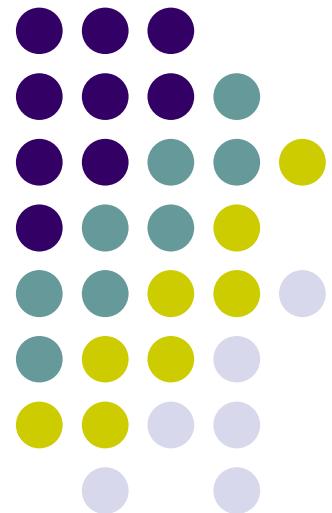
Thập niên 70

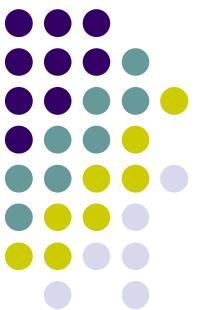
- Từ đầu 1970 xuất hiện các mạng riêng:
 - ALOHAnet tại Hawaii
 - DECnet, IBM SNA, XNA
- 1974: Cerf & Kahn – nguyên lý kết nối các hệ thống mở (**Turing Awards**)
- 1976: Ethernet, Xerox PARC
- Cuối 1970: ATM

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

cuuduongthancong.com

cuuduongthancong.com

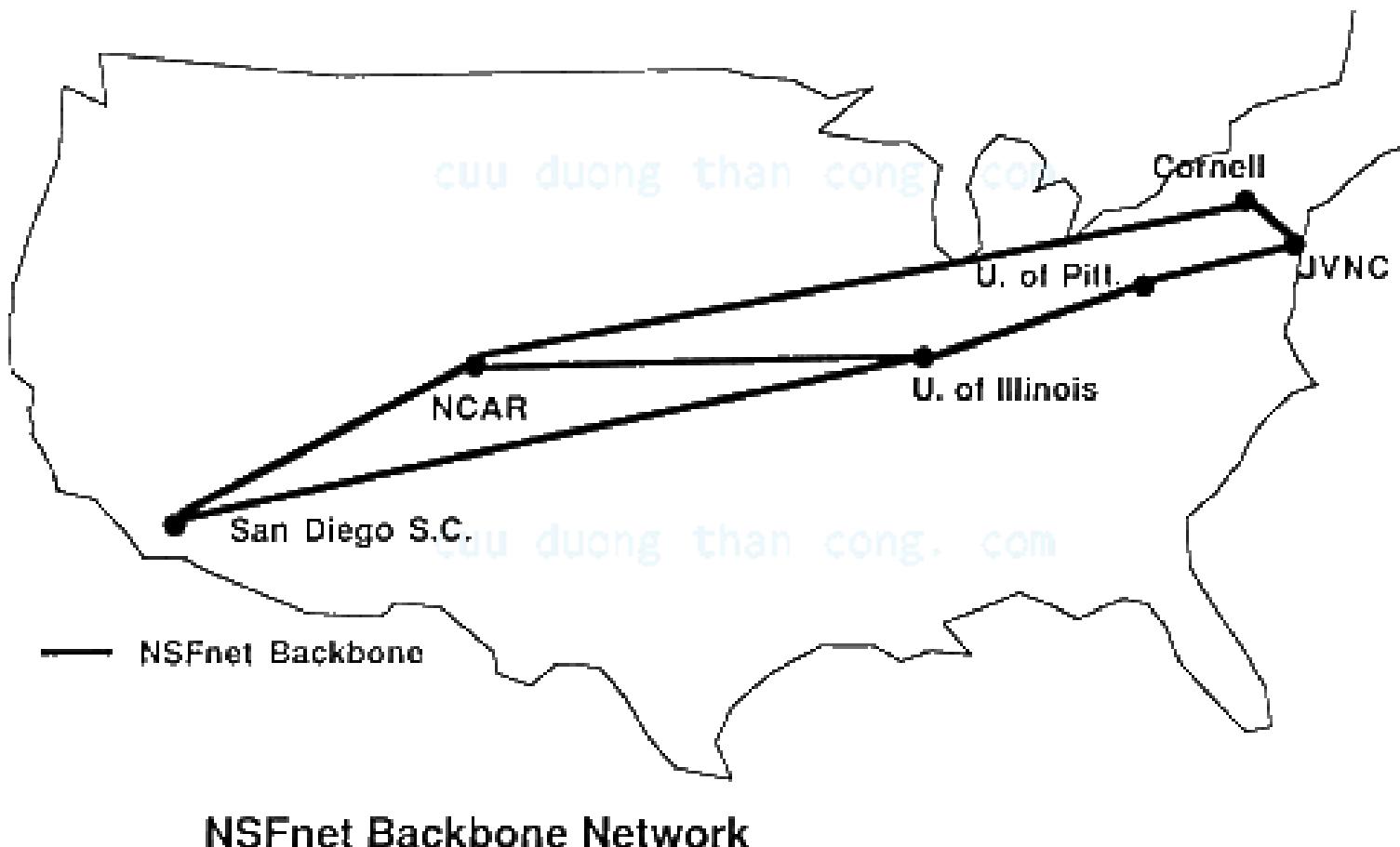




1981: Xây dựng mạng NSFNET

NSF: National Science Foundation

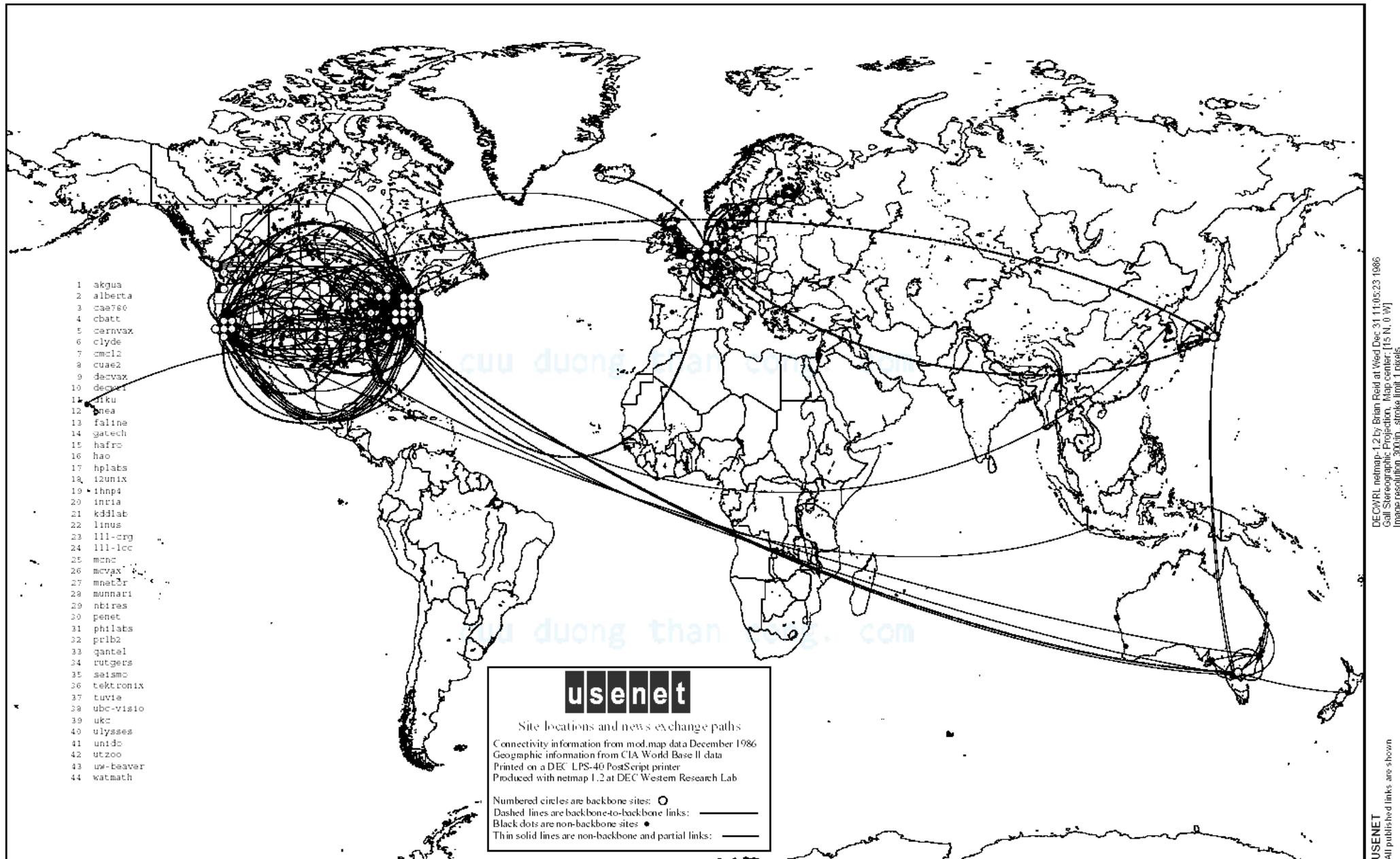
Phục vụ cho nghiên cứu khoa học, do sự quá tải của ARPANET

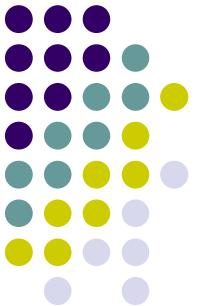


National Center for Atmospheric Research
March 19, 1984



1986: Nối kết USENET & NSFNET





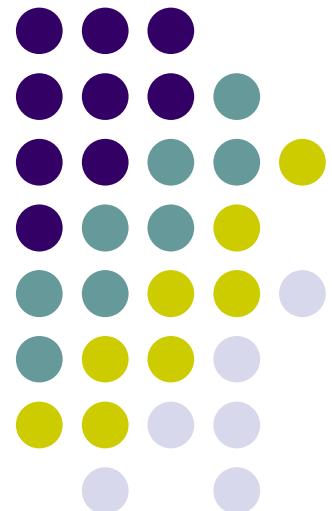
Thêm nhiều mạng và giao thức mới

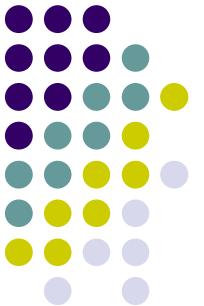
- Thêm nhiều mạng mới nối vào: MFENET, HEPNET (Dept. Energy), SPAN (NASA), BITnet, CSnet, NSFnet, Minitel ...
- TCP/IP được chuẩn hóa và phổ biến vào 1980
- Berkeley tích hợp TCP/IP vào BSD Unix
- Dịch vụ: FTP, Mail, DNS ...

Thập niên 90: Web và thương mại hóa Internet

cuuduongthancong.com

cuuduongthancong.com



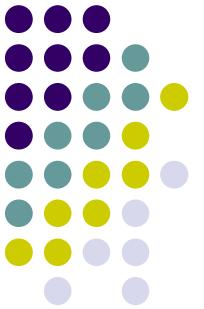


Thập niên 90

- Đầu 90: ARPAnet chỉ là một phần của Internet
- Đầu 90: Web
 - HTML, HTTP: Berners-Lee
 - 1994: Mosaic, Netscape
- Cuối 90: Thương mại hóa Internet

Cuối 1990's – 2000's:

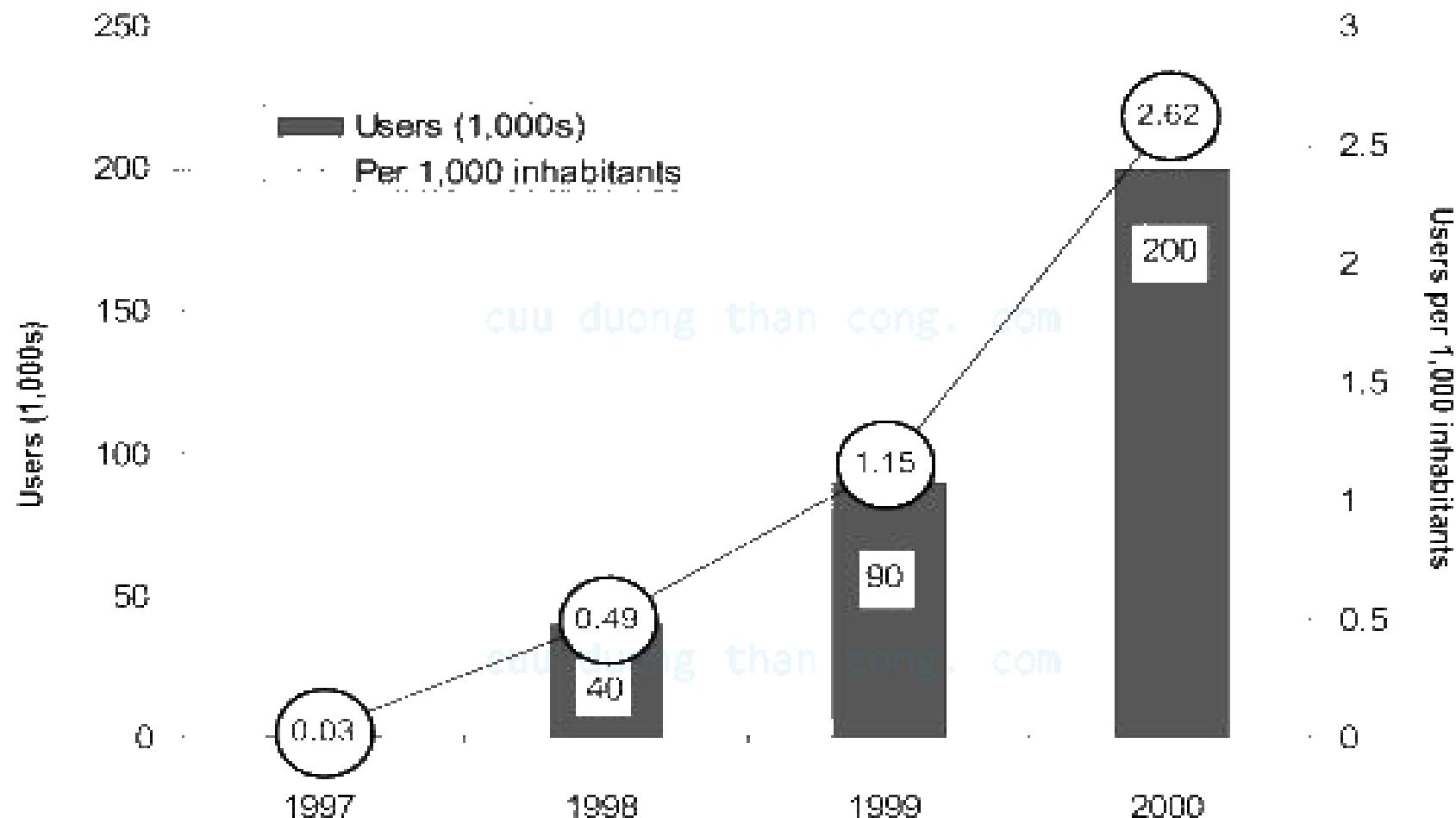
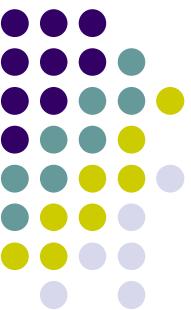
- Nhiều ứng dụng mới: chat, chia sẻ file P2P...
- E-commerce, Yahoo, Amazon, Google...
- > 50 triệu máy trạm, > 100 triệu NSD
- Vấn đề an toàn an ninh thông tin!
 - Internet dành cho tất cả mọi người
 - Tất cả các dịch vụ phải quan tâm tới vấn đề này



Lược sử Internet Việt Nam

- 1991: Nỗ lực kết nối Internet không thành.
:((Vì một lý do nào đó)
- 1996: Giải quyết các cản trở, chuẩn bị hạ tầng Internet
 - ISP: VNPT
 - 64kbps, 1 đường kết nối quốc tế, một số NSD
- 1997: Việt Nam chính thức kết nối Internet
 - 1 IXP: VNPT
 - 4 ISP: VNPT, Netnam (IOT), FPT, SPT
- 2007: “Mười năm Internet Việt Nam”
 - 20 ISPs, 4 IXPs
 - 19 triệu NSD, 22.04% dân số

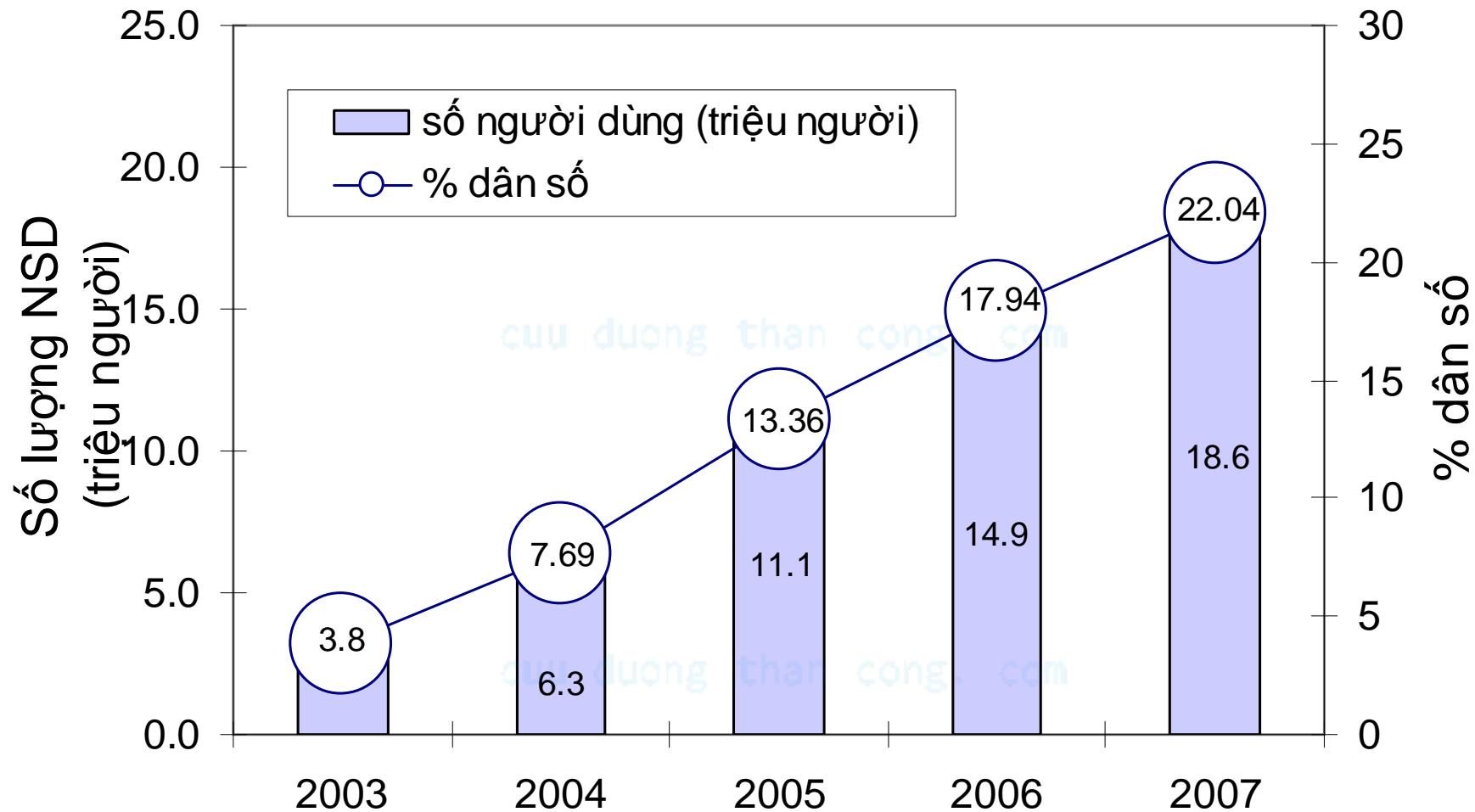
Phát triển Internet ở VN



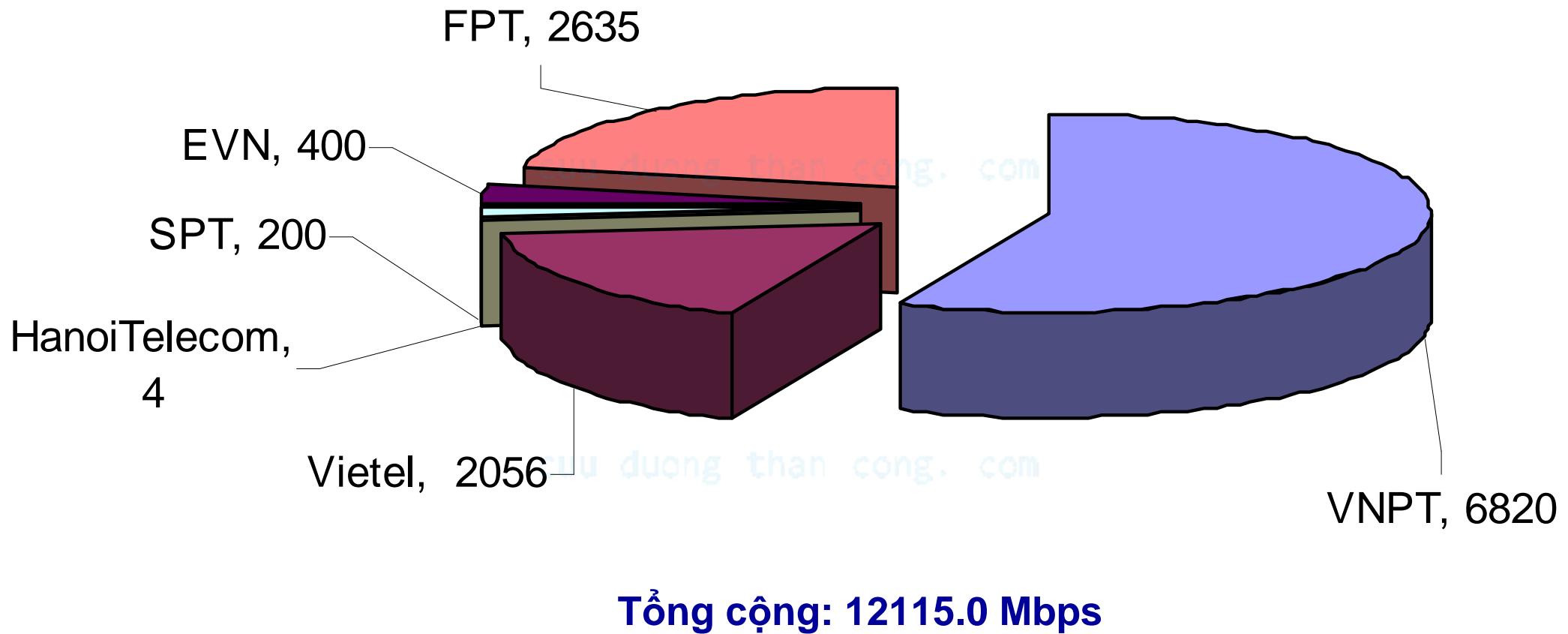
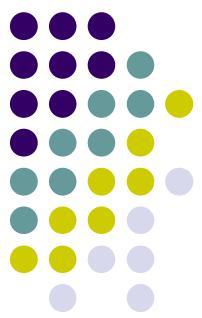
Ước tính số người dùng bằng hai lần số thuê bao

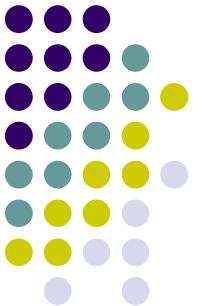
Source: Vietnam Internet Case Study, <http://www.itu.int/asean2001/reports/material/VNM%20CS.pdf>

Thống kê gần đây



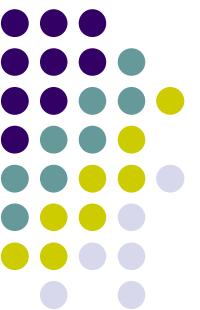
Bảng thông kết nối đi quốc tế (Mbps), Q.3 2007





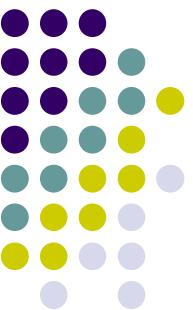
Internet những năm 2000s: Tương lai là của các bạn

- Ứng dụng và công nghệ mới
 - Youtube, Skype, BitTorrent, Video & VoIP...
 - Mạng không dây, mạng quang học, thông tin di động
 -
- Internet sẽ tiếp tục cải tiến dịch vụ và biến đổi không ngừng
 - Mang lại sự thuận tiện cho mọi người
 - Các bạn (**sinh viên CNTT**) sẽ làm được điều đó!



Tóm tắt

- Giới thiệu môn học
- Lược sử Internet
- Khái niệm mạng máy tính
- Kiến trúc mạng
 - Topology
 - Protocol
- Mô hình truyền thông
 - Chuyển mạch kênh vs. chuyển mạch gói
 - Không liên kết vs. Hướng liên kết
- Các tham số cơ bản



Tuần tới...

- Kiến trúc phân tầng
- Mô hình tham chiếu OSI
- Địa chỉ IP, MAC, số hiệu cổng
- DNS và dịch vụ tên miền

cuuduongthancong.com

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

GIÁO TRÌNH MÔN HỌC

MANG MÁY TÍNH

Ths. NGUYỄN TÂN KHÔI

(Lưu hành nội bộ)
Đà Nẵng – 2004

MỤC LỤC

<i>Chương 1</i>	<i>MỞ ĐẦU</i>	<i>1</i>
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
<i>Chương 2</i>	<i>TẦNG VẬT LÝ</i>	<i>16</i>
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
<i>Chương 3</i>	<i>TẦNG LIÊN KẾT DỮ LIỆU</i>	<i>22</i>
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 ỦNG 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 hóa 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

cuu duong than cong. com

cuu duong than cong. com

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 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 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 trớ 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

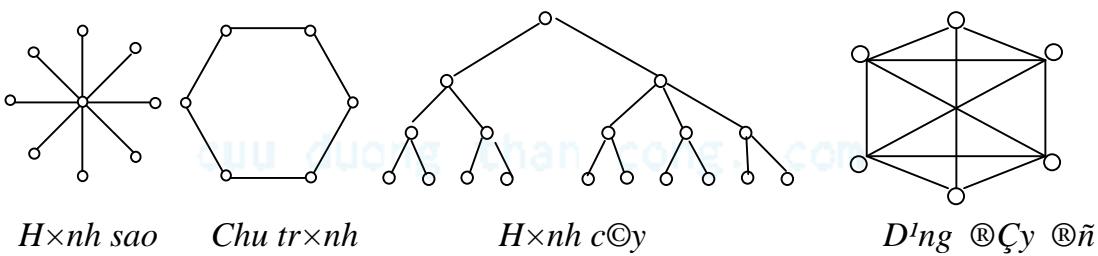
Mạng máy tính có thể phân bố trên một khu vực nhất định hoặc có thể trong một quốc gia hay toàn cầu. Dựa vào phạm vi phân bố, người ta có thể phân ra các loại mạng như sau:

- 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 trực hay cáp quang.
- b. MAN (Metropolitan Area Network - Mạng đô thị) : Kết nối các máy tính trong phạm vi một thành phố. Kết nối này được thực hiện thông qua các môi trường truyền thông tốc độ cao (50-100 Mbit/s).
- c. WAN (Wide Area Network) - Mạng diện rộng, kết nối máy tính trong nội bộ các quốc gia hay giữa các quốc gia trong cùng một châu lục. Thông thường kết nối này được thực hiện thông qua mạng viễn thông. Các WAN có thể được kết nối với nhau thành GAN hay tự nó đã là GAN.
- d. GAN (Global Area Network) : Mạng toàn cầu, kết nối máy tính từ các châu lục khác nhau. Thông thường kết nối này được thực hiện thông qua mạng viễn thông và vệ tinh.

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

1.2.2 Dựa theo cấu trúc mạng

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

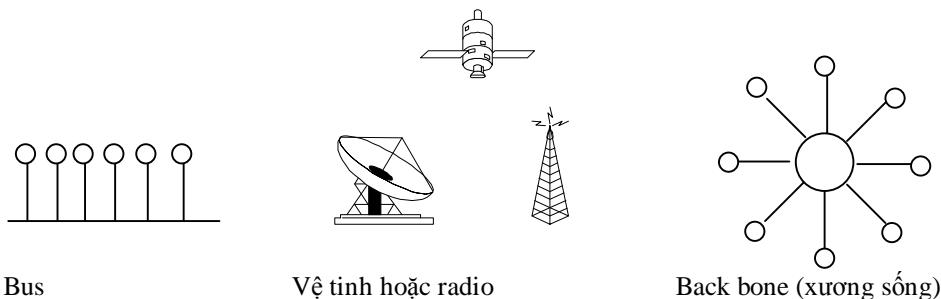


Hình 1-1. Cấu trúc mạng kiểu điểm-điểm.

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

1.2.2.2 Kiểu khuyếch tán

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



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

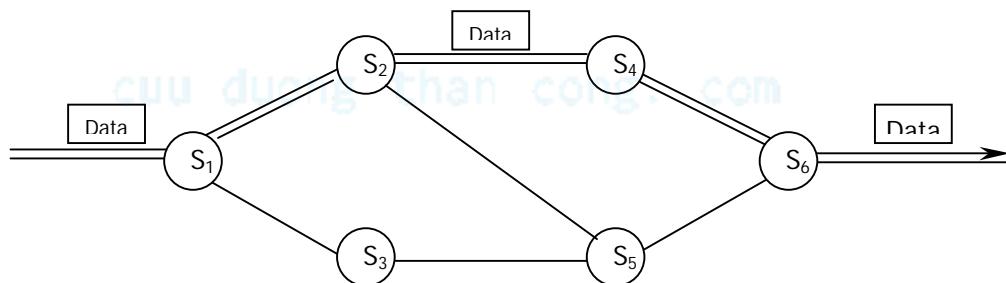
Trong cấu trúc dạng Bus và Vòng cần cơ chế "*trọng tài*" để giải quyết các xung đột (collision) xảy ra khi nhiều nút muốn truyền tin đồng thời. Trong cấu trúc vệ tinh hoặc radio, mỗi nút cần có ăng-ten thu và phát.

1.2.3 Theo phương pháp chuyển mạch

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

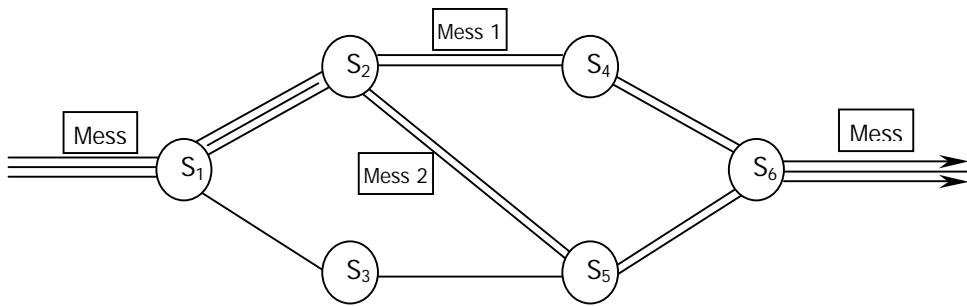
1.2.3.1 Chuyển mạch kênh

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



Hình 1-3. Mạng chuyển mạch kênh.

1.2.3.2 Mạng chuyển mạch bản tin



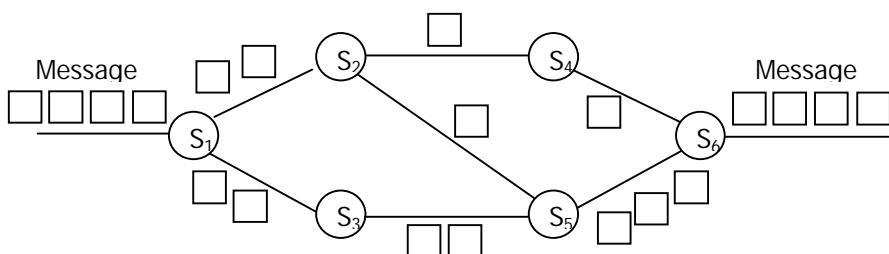
Hình 1-4. Phương pháp chuyển mạch thông báo.

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 khenh:
- 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 rỗng 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 hóa 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 hóa mạng

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

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 tiêu 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 International 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 Manufacturers Association*) : Hiệp hội máy tính châu Âu
6. ATM Forum (*Asynchronous Transfers Mode*) - Thực hiện các giải pháp cho mạng ISDN.
7. IETF (*Internet Engineering 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 vấn 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.

	Số hiệu tầng	Hệ thống A	Hệ thống B	Tên đơn vị dữ liệu
Các tầng cao Xử lý tin	7	Application	G. thức tầng 7	APDU, Message, Packet
	6	Presentation		PPDU, Packet
Các tầng thấp Truyền tin	5	Session		SPDU, Packet
	4	Transport		TPDU, Segment, Packet
	3	Network	G. thức tầng 2	Datagram, Packet
	2	Data link		Frame, Packet
	1	Physical	G. thức tầng 1	Bit, Packet

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 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 thôngảo).

- 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 ISĀ.
- 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	<i>Iêu cầu</i>
indication	<i>Chỉ báo</i>
response	<i>Trả lời</i>
confirm	<i>Xác nhận</i>

request được gửi bởi người sử dụng dịch vụ ở tầng N+1 trong hệ thống A để gọi thủ tục của giao thức ở tầng N. *Iêu cầu* này được cấu tạo dưới dạng một hoặc nhiều đơn vị dữ liệu giao thức (PDU - Protocol Data Unit) để gửi 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 thuỷ *indication*. Sau đó *response* được gửi 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 gửi 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 khenh, 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 chuyền 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.

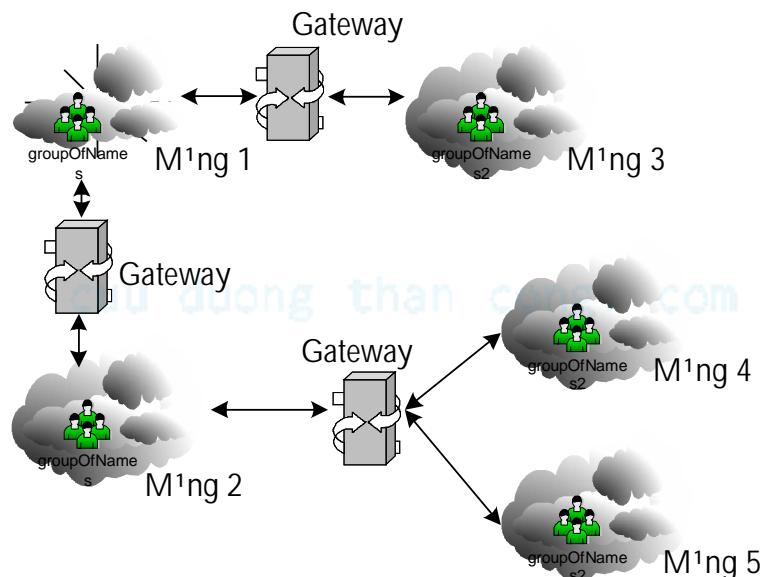
Tháng 09/1983, dưới sự tài trợ của Bộ Quốc phòng Mỹ, Berkeley Software Distribution đưa ra bản Berkeley UNIX 4.2BSD có kết hợp giao thức TCP/IP, biến TCP/IP thành phương tiện kết nối các hệ thống UNIX. Trên cơ sở đó, mạng ARPANET nhanh chóng lan rộng và chuyển từ mạng thực nghiệm sang hoạt động chính 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 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 Qllernet, X.25,...) mà vẫn giao tiếp được với nhau.

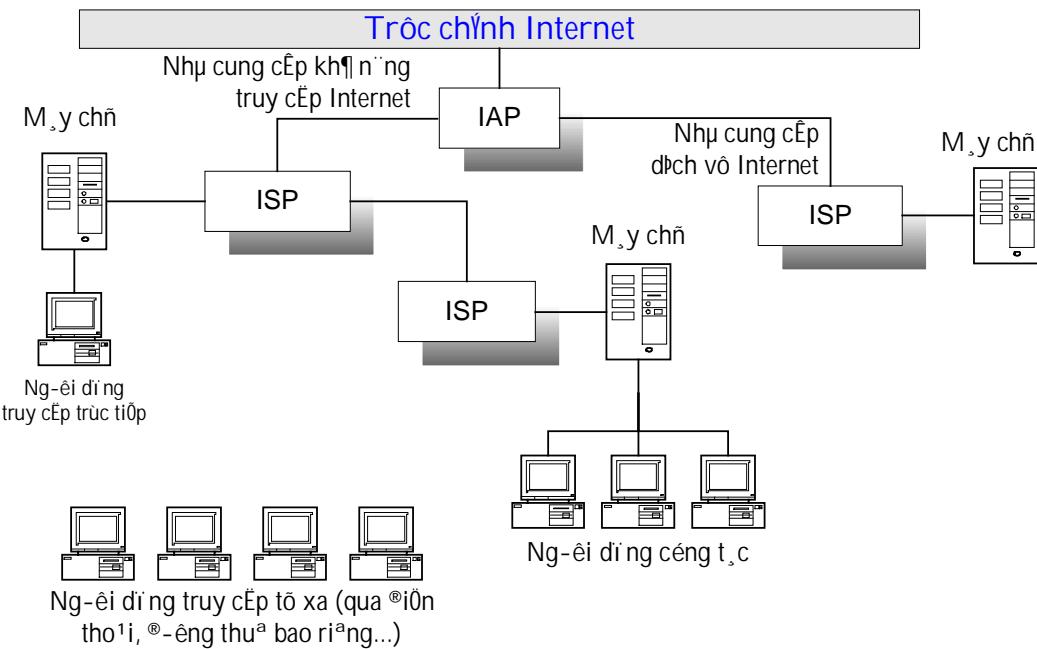


Hình 1-7. Cấu trúc của mạng Internet.

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)
4			Transmision Control	
3	Network	Host - Host		Network Services
2		SRC to DESI - IMP	Path Control	
1	Datalink	IMP - IMP	Data Link Control	Data Link Control
	Physical	Physical	Physical	Physical

ARPANET: Advanced Research Projects Agency

FTP: File Transfer Protocol

SNA: System Network Architecture của IBM

IMP: Interface Message Procesor

NAU: Network Addressable Unit

*Nguyễn Tân Khôi,
Khoa Công nghệ Thông tin, Trường Đại học Bách Khoa Đà Nẵng.*

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).

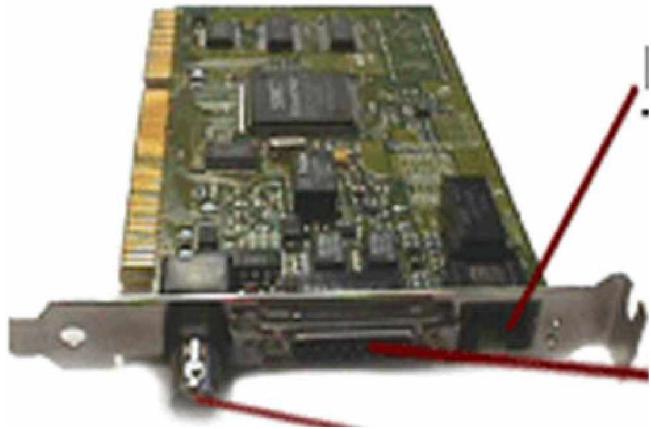
Đặc tính của cáp bao gồm sự nhạy cảm với nhiễu của điện, độ mềm dẻo, khả năng uốn nắn để lắp đặt, cự ly truyền dữ liệu, tốc độ truyền (Mbit/s). Hiện nay, tốc độ truyền dữ liệu trên các loại cáp biến động từ 10Mbit/s đến 100Mbit/s và hơn nữa.

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

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. Hình 2-1. Card mạng (NIC)



- 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 quấn bằng dây bện kim loại dùng làm dây đât. Giữa dây đồng dẫn điện và dây đât 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 khuỷch 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 sáng 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, khuỷch 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 dải 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.

Ủy 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 trực 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 khuỷu ếch 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:

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

2.1.2.2 Độ nhiễu

Điện tử 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) :

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

2.1.2.3 Tốc độ truyền

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

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 :

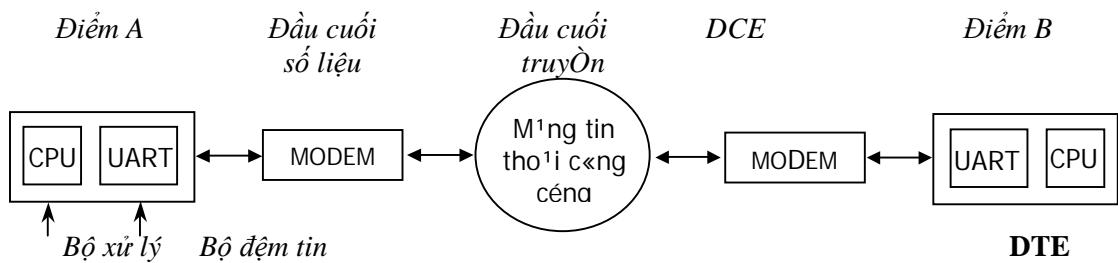
$$\frac{S}{N} = 10 \log_{10} \frac{S}{N} = 20 \rightarrow \frac{S}{N} = 100 \quad C = B \log_2 \left(1 + \frac{S}{N} \right) = 3000 \times \log_2 (1 + 100) = 19963 \text{b/s}$$

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 $47,05\text{mm} \pm 13$ hàng trên đánh số $1 \div 13$ (trái qua phải) hàng dưới $14 \div 25$ (trái qua phải).
- *Phần điện* : gồm qui ước logic $1 <-3\text{V}$ và logic $0 >+ 3\text{V}$.

Tốc độ truyền cho phép 20 kbps qua dây cáp 15m (thường là $9,6\text{ kbps}$)

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 dù 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.

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.

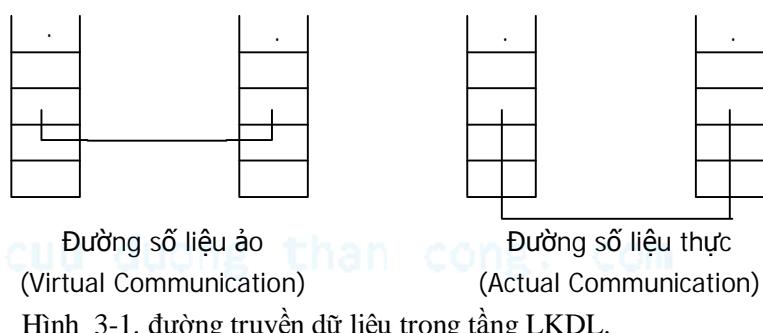
Tầng LKDL nghiên cứu các thuật toán thực hiện thông tin hiệu suất, tin cậy giữa hai máy cạnh nhau ở tầng 2. Đưa ra các thủ tục truyền tin có lưu ý đến lỗi có thể xảy ra do nhiễu trên đường dây, sự trễ do lan truyền.

Thông thường, tầng LKDL có liên quan đến nhiều của tín hiệu của phương tiện truyền vật lý, cho dù là truyền qua dây đồng, cáp quang hay truyền thông qua sóng ngắn. Nhiều 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 xảy 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 kiểm tra tổng là :

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

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

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

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 $T(x) = 1110$

$$\begin{array}{r}
 11010'1'1011 0'00'0' \\
 \oplus 10011 \\
 \hline
 010011 \\
 10011 \\
 \hline
 0000010110 \\
 10011 \\
 \hline
 0010100 \\
 10011 \\
 \hline
 001110 \rightarrow \text{Số dư là } 1110
 \end{array}$$

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 $i = 0, 1, 2, \dots, r-1$ nên độ dài cực đại của các từ mã Hamming là $n \leq 2^r - 1$ và từ đây 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 $11 \leq 2^r - 1 - r$, ta cần 4 bit kiểm tra ($r = 4$) để tạo mã Hamming ($n=11+4=15$)

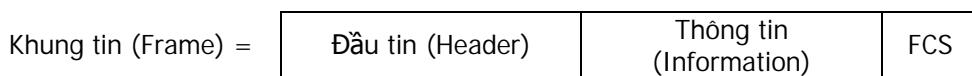
1	0	1	0	1	0	1	C	1	0	0	C	1	C	C
15	14	13	12	11	10	9	<u>8</u>	7	6	5	<u>4</u>	3	<u>2</u>	1

Các bít kiểm tra C được tính như sau:

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 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. Đến đây 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 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 μ s) 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 → 7. Ta có thể dùng n tùy 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 dù thủ tục này cho phép tầng liên kết dữ liệu linh hoạt hơn về thứ tự gửi, 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.

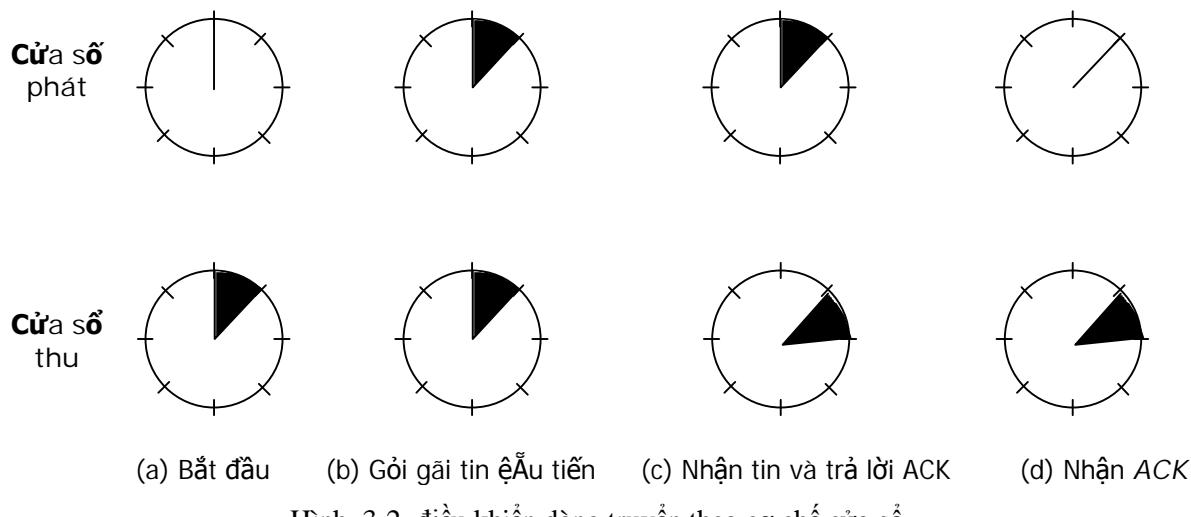
- *Cửa sổ bên phát*

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 kích thước là 3 bit với độ trượt 1 bit như sau :

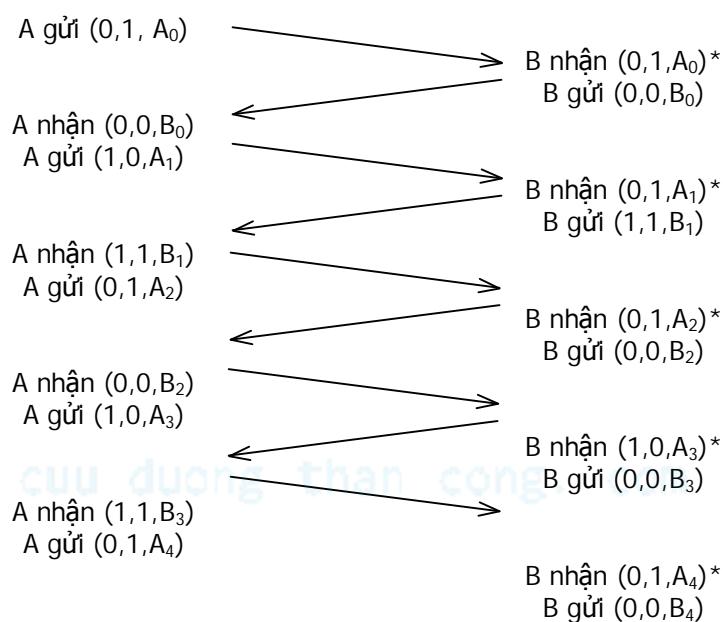


Hình 3-2. Điều khiển dòng truyền theo cơ chế cửa sổ.

3.5.2 Trao đổi bản tin với cửa sổ 1 bit

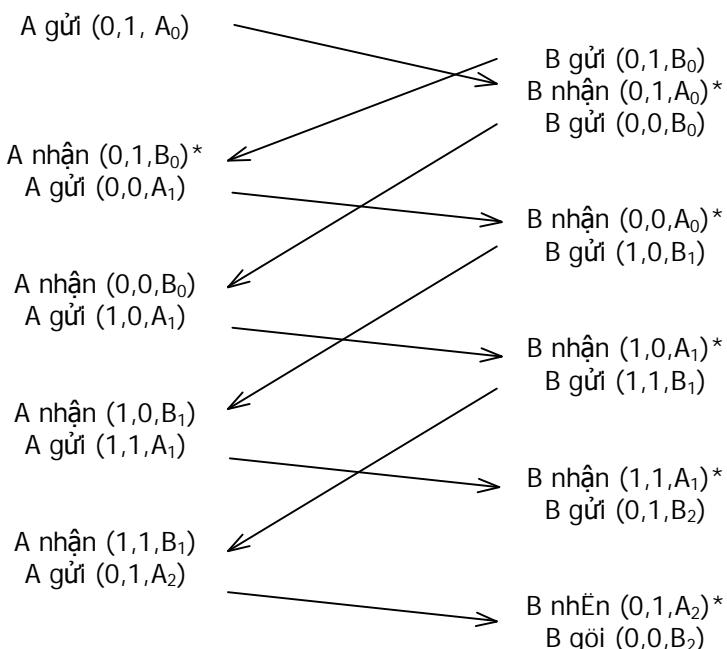
Bản tin gồm có gói tin với phần điều khiển (Header). Phần điều khiển gồm có số gói tin, số thứ tự phát *seq*, số gói tin, số thứ tự nhận là *ack*.

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 nắc.

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.

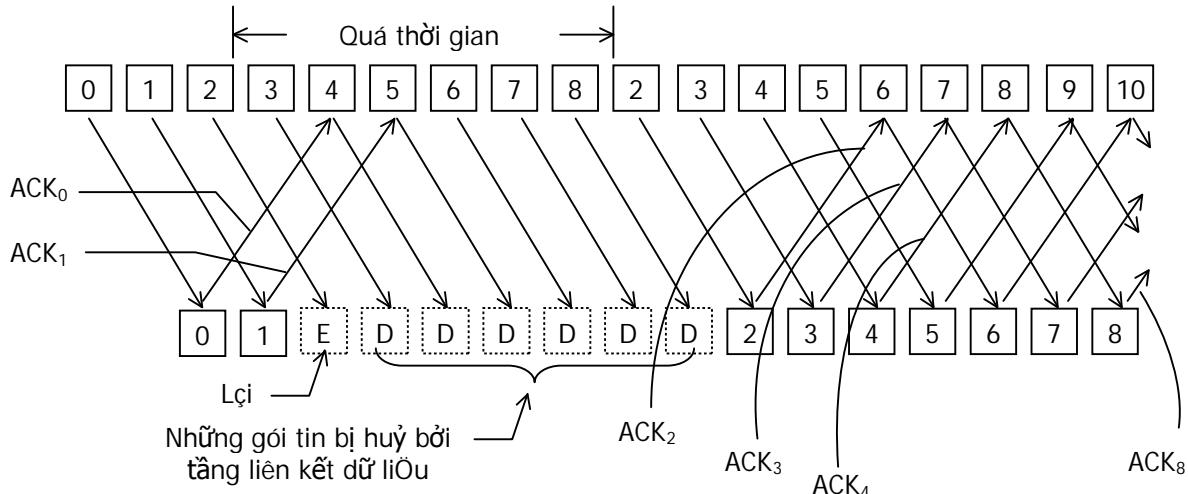
Để nâng cao hiệu suất đường truyền ta không chờ tín hiệu biên nhận mà cứ phát tiếp. Ví dụ, với thời gian phát 20ms cho một gói tin, ta sẽ gửi liên tục 26 gói tin. Như thế khi gửi hết 26 gói tin thì mất khoảng thời gian là 520 ms, đúng lúc tín hiệu biên nhận cho gói tin 0 cũng vừa đến. Kỹ thuật này gọi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

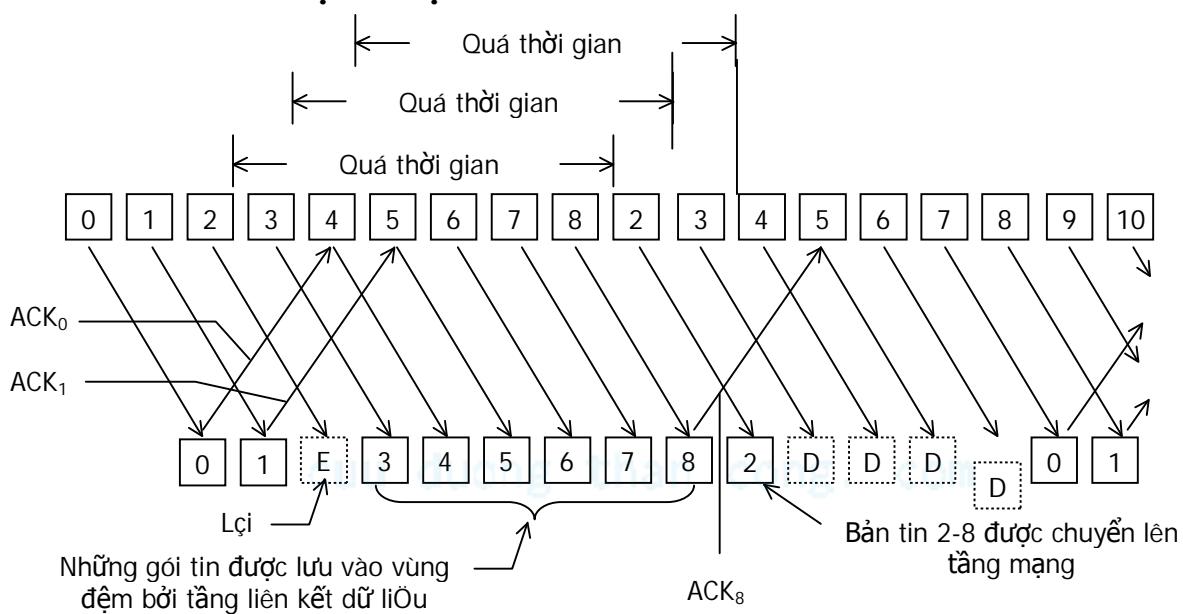
Trong trường hợp này, bên thu huỷ bỏ các gói tin tiếp theo gói tin bị hỏng. Bên phát phát lại tất cả các gói tin chưa được nhận bắt đầu từ gói tin bị hỏng.

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 lọc



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

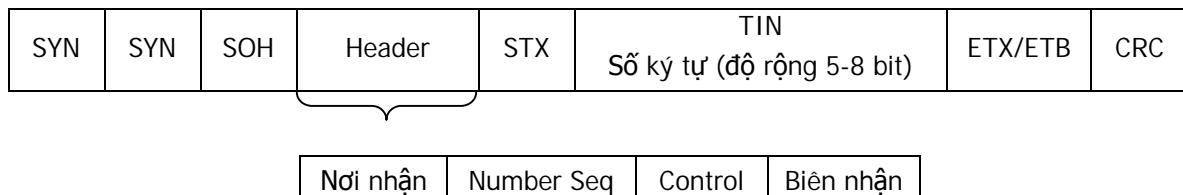
Đây là giao thức *hướng ký tự* (COP - Character Oriented Protocol) được xây dựng dựa trên các ký tự đặc biệt của một bộ mã chuẩn nào đó (như ASCII hoặc EBCDIC) hoạt động theo phương thức hai chiều luân phiên.

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

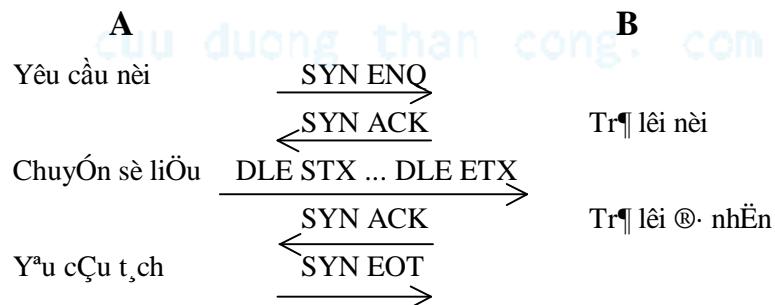


Để thông suốt bản tin, có thể dùng thêm các byte đệm :

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

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

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 '*cúng*' 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 : 0110111111110010

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 phương 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 dịch vụ 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 dịch vụ (ARM).
- LAPB (Link Access Protocol-Balanced) : tương ứng với phương thức trả lời dịch vụ 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 hóa 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 RS232 và các chuẩn khác được phát triển từ chuẩn này.
2. Tìm hiểu các chuẩn mở rộng của giao thức HDLC.

-

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 tòa nhà, hoặc trong một tòa 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 tùy 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 trực 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 trực 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 bít 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 ứn 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 nối 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 đổi với bất cứ tòa 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.

Mỗi 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 tùy 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' : Trạm 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 hiệu 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 suất 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 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 :

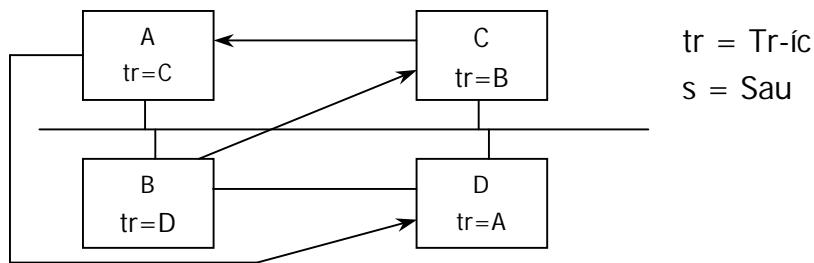
1. Khi đang truyền vẫn tiếp tục nghe đường dây.
2. Nếu phát hiện có xung đột thì *ngừng truyền và tiếp tục gửi sóng mang* thêm một thời gian nữa để bảo đảm các trạm đều có thể nghe được sự kiện xung đột.
3. Sau khi chờ đợi một thời gian ngẫu nhiên thì trạm thử truyền lại bằng cách sử dụng các phương 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 '*I-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 kế sau và kế 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 gửi 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 hòa 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, chúng tôi 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 thảm 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 biến 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 (*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 đòi hỏi 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 chia sẻ 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.

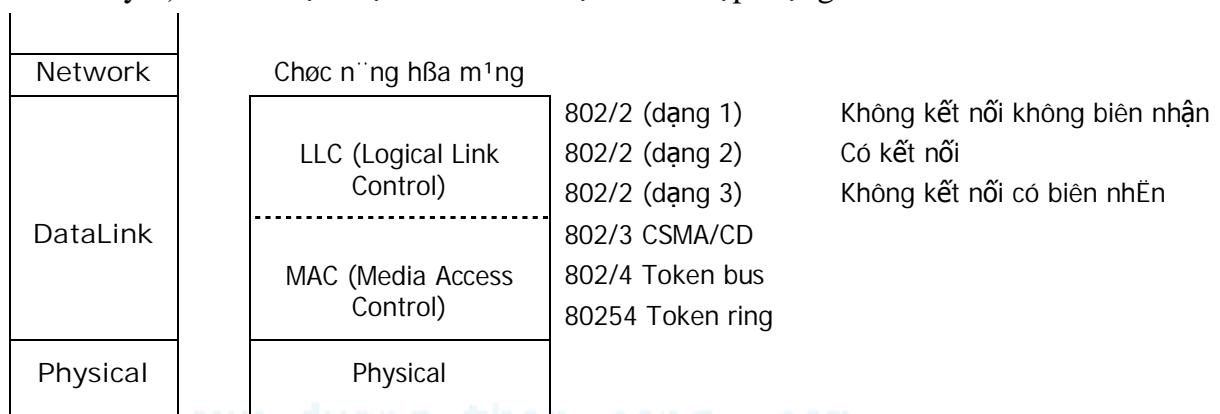
Các chuẩn này quy định môi trường truyền dẫn cũng như cách thức sử dụng chúng trong kết nối LAN; Các giao thức truyền thông ở các tầng vật lý và tầng liên kết dữ liệu của mạng theo mô hình OSI.

Các giao thức truyền thông ở các tầng trên của mô hình OSI hiện 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.

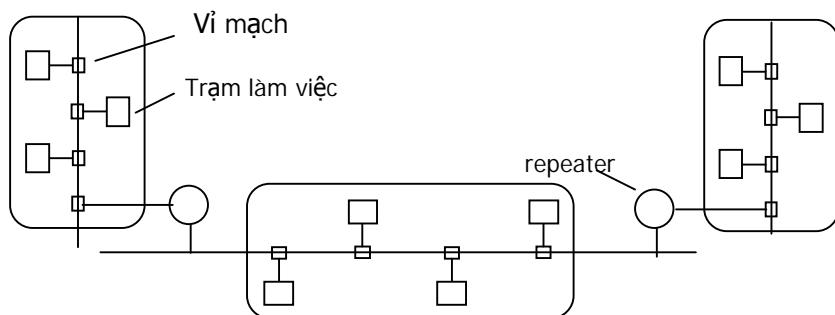
Chuẩn IEEE 802.5 dùng cho mạng dạng vòng và trên cơ sở dùng tín hiệu thăm dò token. Mỗi trạm khi nhận được tín hiệu thăm dò token thì tiếp nhận token và bắt đầu quá trình truyền thông tin dưới dạng các frame. Các frame có cấu trúc tương tự như của chuẩn 802.4. Phương pháp xâm nhập mạng này quy định nhiều 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 tuyền phân đoạn, đường truyền dùng cáp đồng trực, 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 tuyền là 500m, các đoạn tuyền 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 tuyền (bus access) hoặc tuyền 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 trực 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 rỗng. 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.

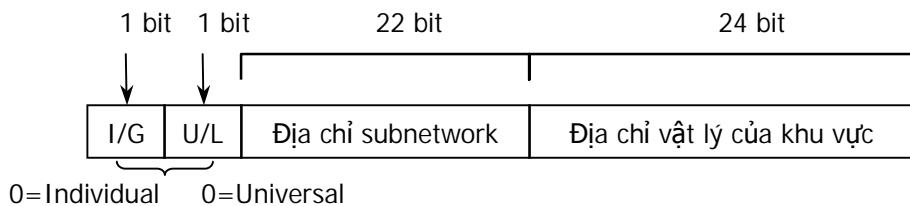
Địa chỉ vật lý của máy trạm :

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 gửi, và địa chỉ của nơi nhận.

Hiện nay IEEE đang đảm nhiệm việc áp định địa chỉ vật lý tổng thể (*universal physical address*) cho các subnet. Đối với mỗi subnet, IEEE áp định một phần địa chỉ đồng nhất đối với tất cả các subnet gọi là OUI (Organization Unique Identifier) phần này có độ dài là 24 bit, cho phép IEEE áp 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 subnet đó. Đó là 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 LAN.

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 Oriented 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
Thư 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. Confirm()

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. Confirmation (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
<i>Khởi động kênh</i>	Không	Cần thiết
<i>Địa chỉ (đ/c) hoá</i>	Gói tin phải có đ/c nguồn và đ/c đích	Gói tin chỉ cần số của kênh ảo
<i>Thông tin tìm đường</i>	Không cần bắt cứ thông tin nào.	Mỗi kênh ảo cần một vùng trong bảng
<i>Tìm đường</i>	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.
<i>Điều khiển</i>	Chỉ mất gói tin ở trong nút hỏng	Kênh ảo đi qua nút hỏng sẽ bị huỷ
<i>Hỗn nút</i>	Khó khắc phục	Dễ khắc phục hơn
<i>Độ phức tạp</i>	Trong tầng giao vận	Trong tầng mạng
<i>Thích hợp</i>	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 dự 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*) đặt giữa hai mạng con đó.

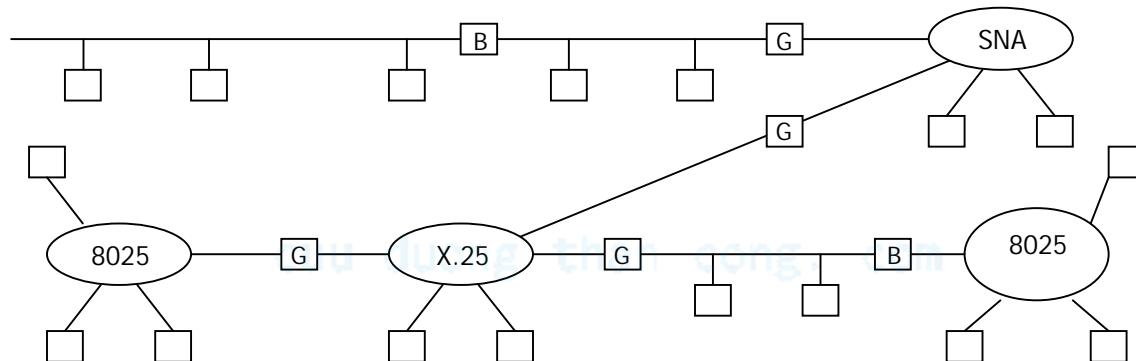
Chức năng của giao diện kết nối phụ thuộc vào sự khác biệt kiến trúc của mạng con : sự khác biệt càng lớn thì chức năng của giao diện càng phức tạp.

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.



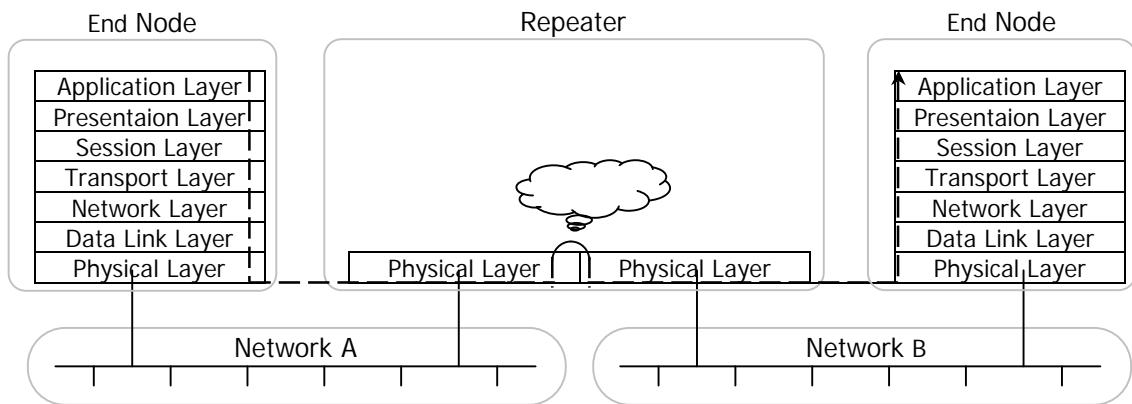
Hình 5-2. Kết nối liên mạng.

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 khuếch 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 cả 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 trực 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)

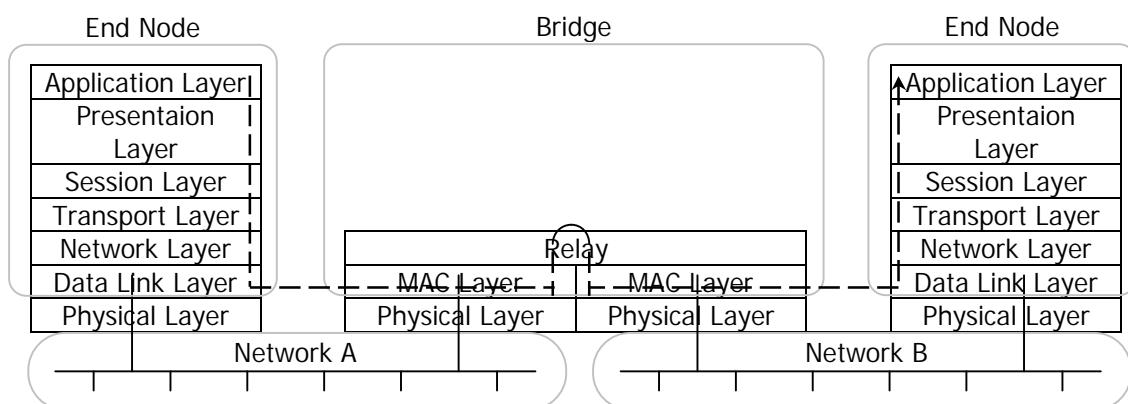
Cầu nối là một thiết bị hoạt động ở tầng liên kết dữ liệu. Dùng để nối hai hoặc nhiều đoạn (*segment*) của mạng LAN khác nhau.

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 lượng 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 động
 - 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 đọc theo mạng. Vì giao thức nào cũng di chuyển ngang qua cầu nối, nên tùy 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 chuyên 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 phôi hợp tốc độ.



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

Ví dụ một Bridge nối giữa IEEE 802.3 và IEEE 802.5. Cầu nối này có hai card mạng: card Token Ring và card Ethernet để giao tiếp với hai mạng.

5.2.1.4 BỘ ĐỊNH TUYẾN (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.



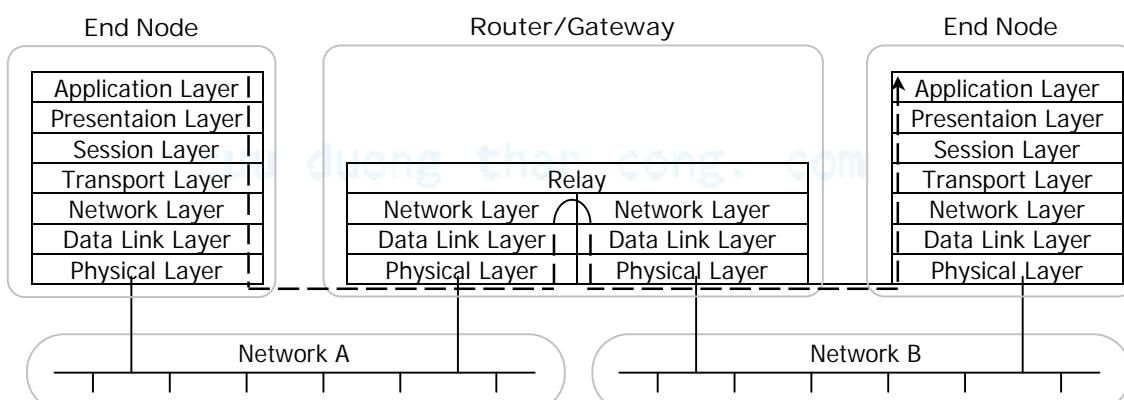
Hình 5-7. Bộ định tuyến.

- 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 sẻ 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 tùy 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 lô trình đó.

Khi bộ định tuyến nhận được một gói dữ liệu cần gửi đến mạng ở xa, nó kiểm tra bảng định 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 gửi 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.

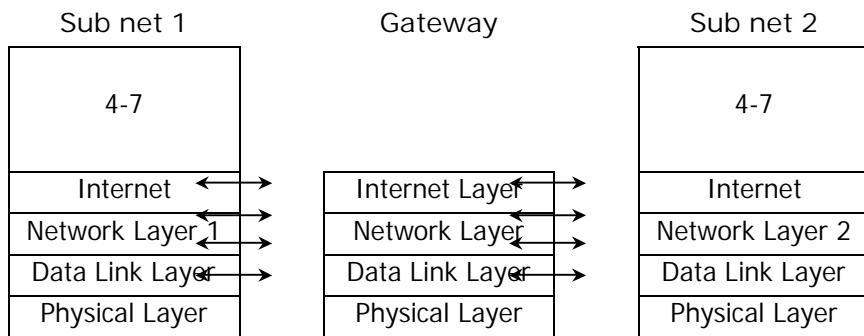
5.2.1.5 *Bộ chuyển mạch*

Chức năng chính của bộ 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 Ethernet LAN hoặc Token Ring. Bộ chuyển mạch kết nối một số LAN riêng biệt và cung cấp khả năng lọc gói dữ liệu giữa chúng.

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

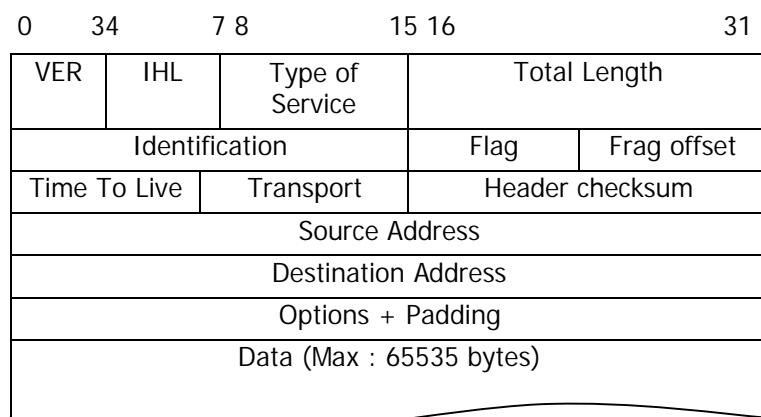
Giao thức IP (Internet Protocol) hoạt động ở tầng mạng, cung cấp dịch vụ dữ liệu không liên kết (connectionless) cho nhiều giao thức liên kết dữ liệu khác. Đơn vị dữ liệu dùng trong giao thức IP được gọi là *datagram*, hay còn gọi là khung tin IP.

- 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 tùy 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 :

0	2	3	4	5	7
Precedence	Delay	Throughput	Reliability	Reserved	

Cấu trúc của trường Type of Service

Precedence (3 bit) : 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 Override | 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 bit 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.

Identification (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 thuật 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 nơi nhận nếu như không tách ra, mà hiện tại bit cờ đang là 1 thì 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 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 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 qua 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 chặng 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 dạng 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 (overflow 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 tùy 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.

Class A	0	Net ID (7 bit)		Host ID
Class B	1 0	Net ID (14 bit)		Host ID
Class C	1 1 0	Net ID (21 bit)		Host ID
Class D	1 1 1 0		Multicast address	
Class E	1 1 1 1 0		Reserved for future use	

Hình 5-11. Các lớp địa chỉ IP.

1. Lớp A ($1 \leq x \leq 126$) : 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 ($128 \leq x \leq 191$) : 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 ($192 \leq x \leq 223$) : 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 ($224 \leq x \leq 239$)

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

5. Lớp E ($240 \leq x \leq 255$) : 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 11001011	160 10100000	9 00001001	0 00000000
------------------	-----------------	-----------------	---------------	---------------

Địa chỉ mạng 2 :	203 11001011	160 10100000	9 00001001	64 01000000
------------------	-----------------	-----------------	---------------	----------------

Địa chỉ mạng 3 :	203 11001011	160 10100000	9 00001001	128 10000000
------------------	-----------------	-----------------	---------------	-----------------

Địa chỉ mạng 4 :	203 11001011	160 10100000	9 00001001	192 11000000
------------------	-----------------	-----------------	---------------	-----------------

Mặt nạ của các mạng con này là : 255.255.255.192

255 11111111	255 11111111	255 11111111	192 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 gửi đến một bộ định tuyến khác. Cú thể 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 vào 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

thúc 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.

Datalink Type (16 bits)		Network Type (16 bits)
Hlen	PLen	Opcode (16 bits)
Sender Datalink (48 bits)		
Sender Network (32 bits)		
00:00:00:00:00:00 Receiver Datalink (48 bits)		
Receiver Network (32 bits)		

Hình 5-12. Khuôn dạng gói tin ARP.

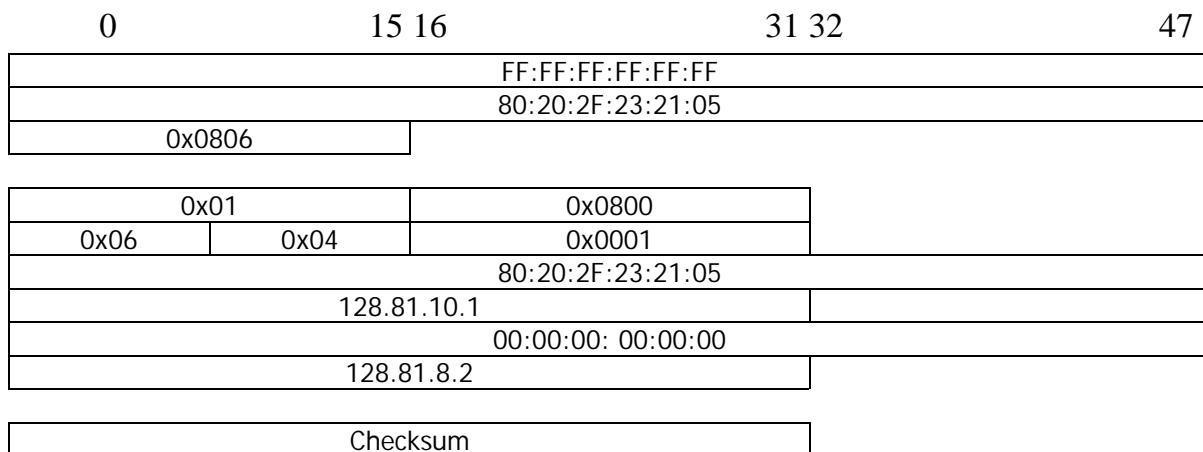
- Data link type: Loại dữ liệu liên kết, với mạng Ethernet thì trường này có giá trị là 0x0001
- Network type : Loại địa chỉ mạng, Ethernet type used for IP (0x0800)
- Hlen : Độ rộng của phần địa chỉ dữ liệu liên kết, với mạng Ethernet độ rộng là 6 bytes
- Plen : Độ rộng của địa chỉ mạng, trong giao 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 :



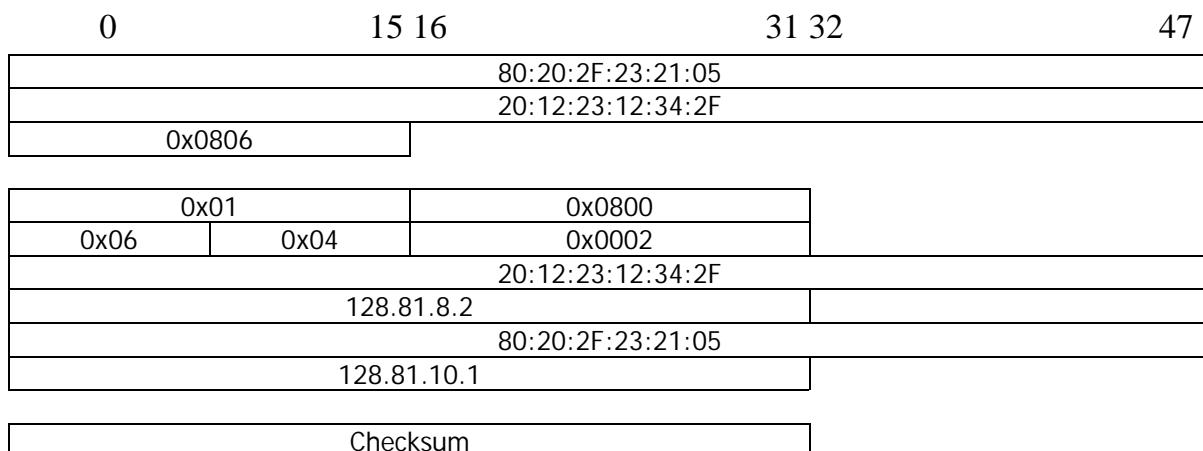
Trạm A biết được địa chỉ mạng của trạm B nhưng không biết địa chỉ vật lý của trạm B. Trạm A cần hỏi địa chỉ vật lý của trạm B để gửi tin. Khi đó trạm A phát đi một gói tin ARP yêu cầu (ARP request packet) đóng gói trong khung tin Ethernet.

- Quá trình gửi 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)

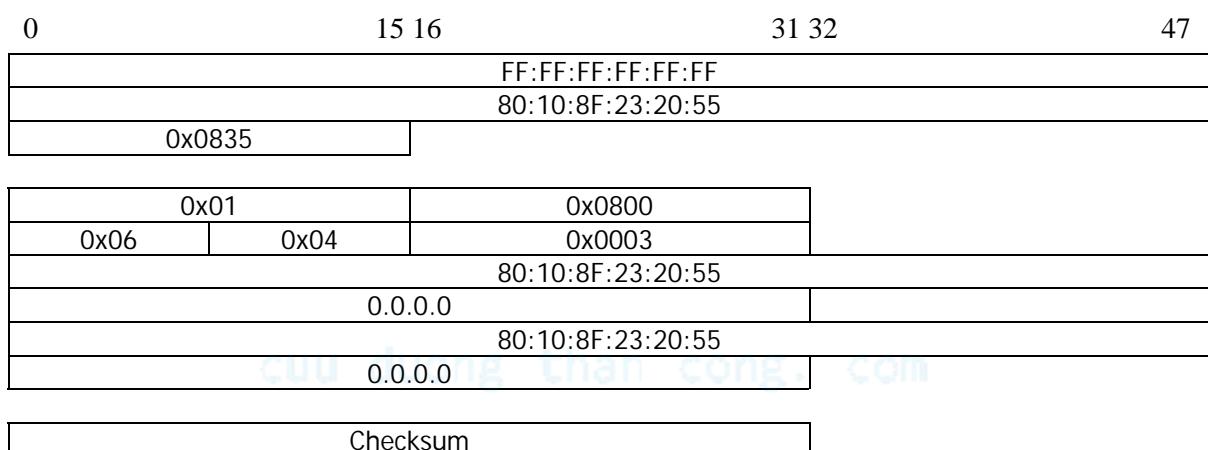
Đôi khi ta cần ánh xạ ngược lại.

Ví dụ một trạm không có 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.

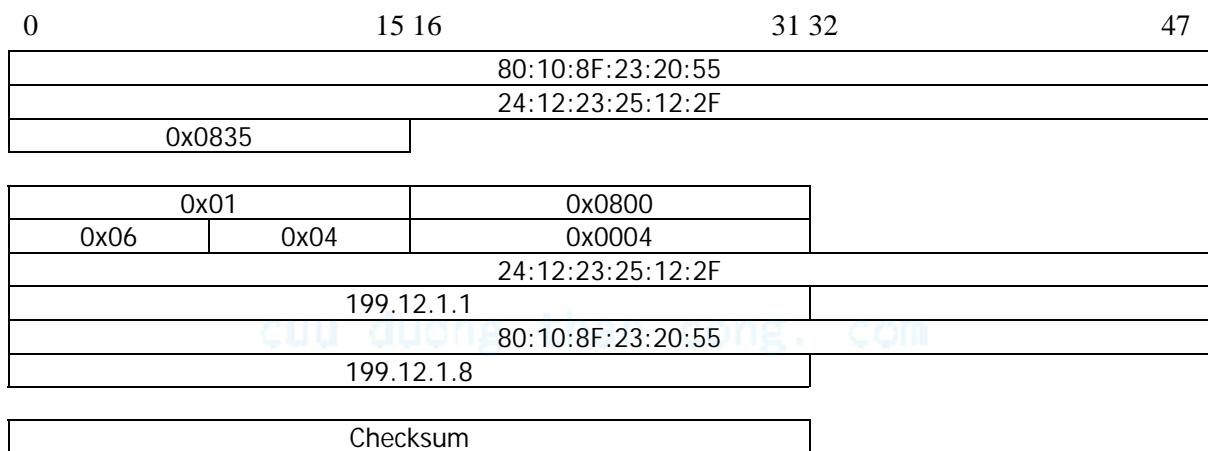
Yêu cầu chuyển đổi (reverse request) là 0x0003 và trả lời chuyển đổi (reverse reply) là 0x0004.

- Quá trình gửi yêu cầu RARP



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

- Quá trình gửi 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 Các 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:

- TYPE: 8 bits, xác định loại thông báo ICMP.
- CODE: 8 bits, cung cấp thông tin chi tiết của từng loại thông báo ICMP.
- 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 :

0	4	8	16	31
Type	Code	Checksum		
Unused				
IP header + 64 bit Original data				

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

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

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 CĂDQ của thông báo này 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 CĂDQ nhận 4 giá trị trong bảng và có định dạng như hình sau:

Code	Nội dung	Type	Code	Checksum	Router IP address	IP header + 64 bit Original data
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 trả 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 Oxceeded.

- *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 CĂDQ của thông báo này nhận 3 giá trị trong bảng và có định dạng như hình sau :

0	8	16	31
Type	Code	Checksum	
Point	Unused		
IP header + 64 bit Original data			

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.

Hình 5-19. Dạng ICMP Parameter Problem

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 :

0	8	16	31
Type	Code	Checksum	
Identifier	Sequence Number		
Data/additional fields			

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

Hình 5-20. Dạng ICMP truy vấn.

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

- Identifier được sử dụng để phân biệt các thông báo được gửi 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 và Echo Reply*

0	8	16	31
Type	Code	Checksum	
Identifier		Sequence Number	
Data			

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 đây vẫn còn hoạt động ngược lại thì đã bị down. Định dạng thông báo như trong hình sau :

Kích thước của DATA thay đổi tùy 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.

0	8	16	31
Type	Code	Checksum	
Identifier		Sequence Number	
OriginateTimeStamp			
ReceiveTimeStamp			
TransmitTimeStamp			

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*

0	8	16	31
Type	Code	Checksum	
Identifier		Sequence Number	

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*

Type	Code	Checksum
Identifier	Sequence Number	
Subnet Address Mask		

Hình 5-24. ICMP Address 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 Oropor**) 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

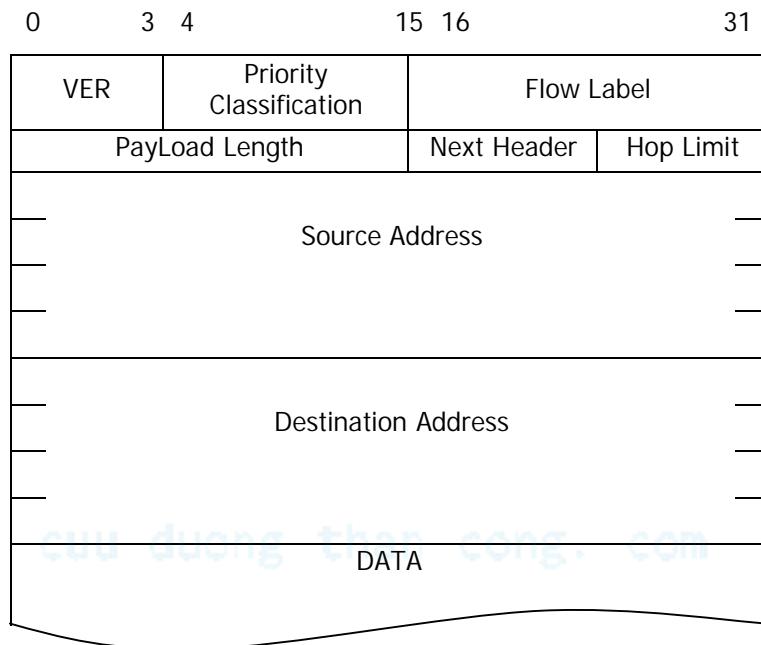
Với sự phát triển nhanh chóng của Internet thì địa chỉ IP 32 bit không thể đáp ứng được nhu cầu sử dụng Internet. Để khắc phục điều này phiên bản IP6 (IP Next Generation) đang được phát triển. Phiên bản IPv6 có các thay đổi như sau :

- 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 :



Hình 5-25. Cấu trúc khung 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

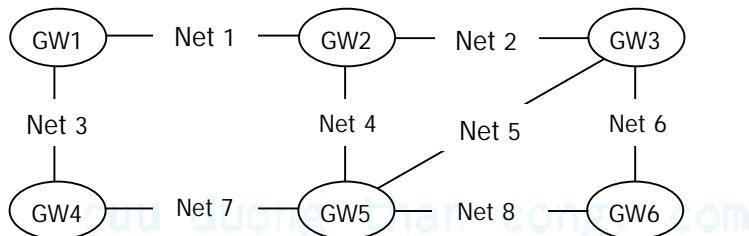
nơi chứa bảng cố định, nó không phức tạp và thích ứng với những thay đổi nhanh chóng trên mạng. Bảng chính thường là tốt hơn bảng cố định bởi vì quản lý một bảng ở trung tâm sẽ dễ dàng hơn quản lý từng bảng được đặt tại mỗi nút mạng.

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 muôn 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.

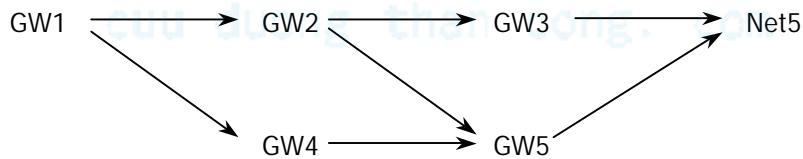
Để xây dựng bảng chọn đường, từ cổng đang đứng ta xét các mạng cạnh đó, sau đó là các mạng ở cạnh các cổng tiếp theo và cứ thế cho đến hết các mạng trong liên mạng.

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



GW1		GW2		GW3		GW4		GW5		GW6	
Neti	D,G										
1	0,1	1	0,2	1	1,2	1	1,2	1	1,2	1	2,3(5)
2	1,2	2	0,2	2	0,3	2	2,1(5)	2	1,2	2	1,3
3	0,1	3	1,1	3	2,2	3	0,4	3	1,4	3	2,5
4	1,2	4	0,2	4	1,2(5)	4	1,5	4	0,5	4	1,5
5	2,2(4)	5	1,3(5)	5	0,3	5	1,5	5	0,5	5	1,3(5)
6	2,2	6	1,3	6	0,3	6	2,5	6	1,3(6)	6	0,6
7	1,4	7	1,5	7	1,5	7	0,4	7	0,5	7	1,5
8	2,2(4)	8	1,5	8	1,5(6)	8	1,5	8	0,5	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 gửi 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).

cuu duong than cong. com

cuu duong than cong. com

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 đường 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

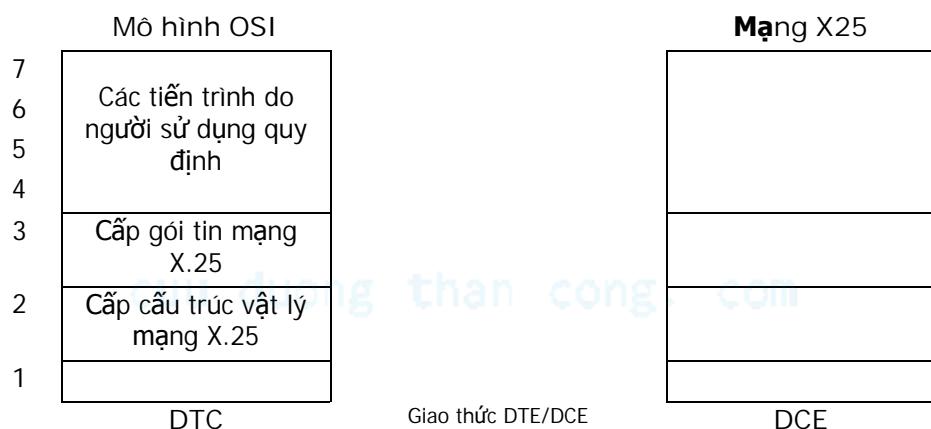
Mạng X.25 là một mạng điện thoại dùng để truyền dữ liệu. Để bắt đầu thực hiện quá trình giao tiếp, một máy tính cần phải liên kết với một máy khác để yêu cầu thực hiện giao tiếp. Máy được yêu cầu liên kết có thể chấp nhận hoặc từ chối việc giao tiếp. Nếu liên kết được chấp nhận, hai hệ thống có thể bắt 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. Mỗi 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

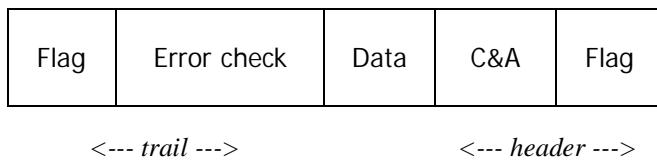
Bước sang thập kỷ 80 và đầu thập kỷ 90, công nghệ thông tin có những bước tiến đặc biệt là chế tạo và sử dụng cáp quang vào mạng truyền dẫn tạo nên chất lượng thông tin rất cao. Sử dụng giao thức X25 để truyền đa số liệu trên mạng cáp quang, dữ liệu nhận được có thể đánh giá là đạt yêu cầu. Tuy nhiên 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 Điện thoại 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 tắc 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 lượng 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

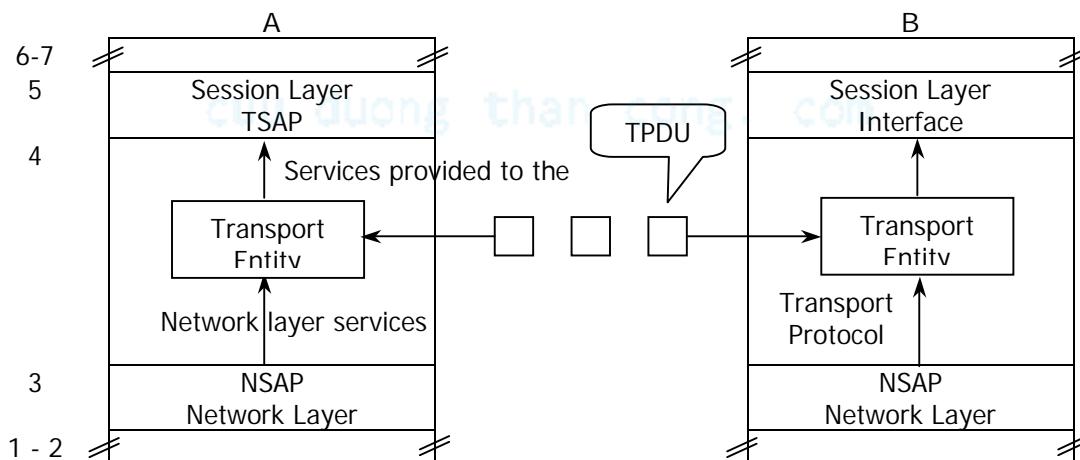
TẦNG GIAO VẬN

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 phát hiện thấy lỗi. Tầng giao vận *quản lý dữ liệu gửi, xác định trạng thái 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 mềm trong phần 4 để thực hiện công việc coi là thực thể giao vận (*transport entity*). Mọi 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 gửi 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

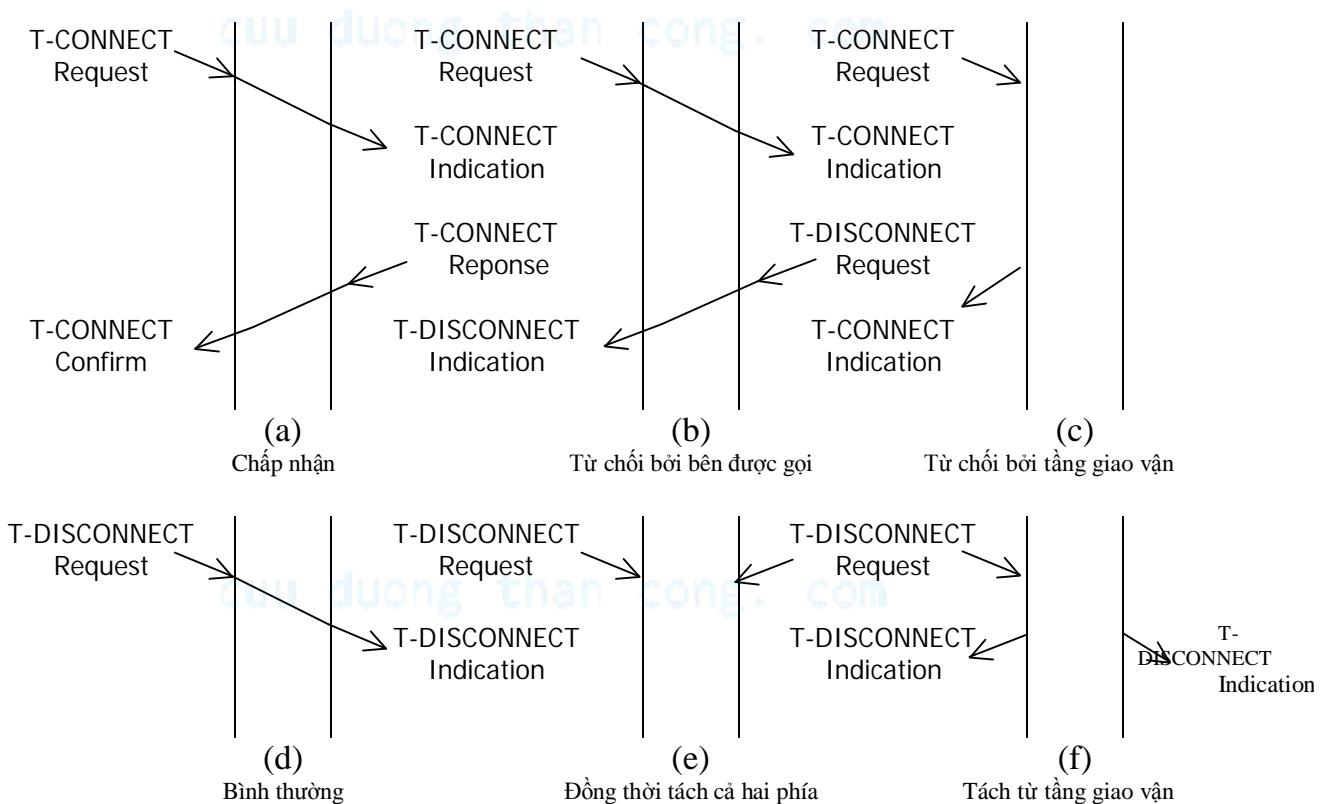
Ngoài phần giao thức chuẩn, ISO còn định nghĩa các dịch vụ mà tầng Giao vận cung cấp cho các thực thể ở tầng Phiên trong trường hợp có liên kết, dưới dạng một tập hợp các hàm dịch vụ nguyên thủy(services primitives) như sau :

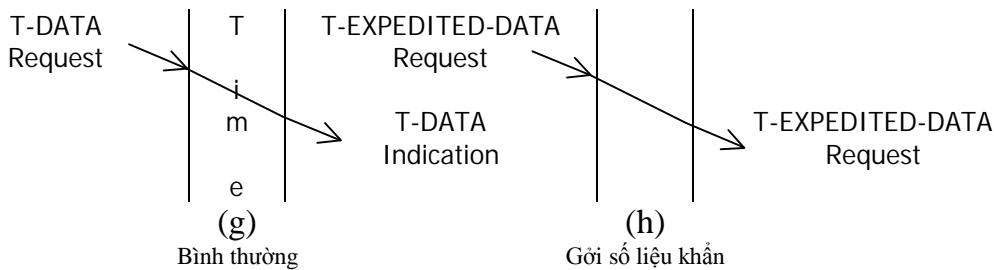
T-CONNECT request (callce, caller, exp wanted, qos, user data)
 T-CONNECT indication (callce, caller, exp wanted, qos, user data)
 T-CONNECT response (qos, responder, exp wanted, user data)
 T-CONNECT confirm (qos, responder, exp wanted, user data)
 T-DISCONNECT request (user data)
 T-DISCONNECT indication (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 ngắn 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 gửi 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 tới 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 cầm 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 gửi 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-RQSOTS. 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 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	<ul style="list-style-type: none"> - Hoàn thiện, tỷ lệ các gói tin bị mất, trùng lặp hoặc bị hỏng không đáng kể. - Lệnh N-RESET có thể bỏ qua. - Tầng giao vận đơn giản, không cần các dịch vụ phục hồi và sắp xếp lại thứ tự gói tin. - Thường là mạng cục bộ.
Nhóm B	<ul style="list-style-type: none"> - Gói tin bị mất, nhưng kiểm soát được. - Thỉnh thoảng tầng mạng gửi lệnh N-RESET do tắc nghẽn, hỏng phần cứng, vấn đề phần mềm. - Thông thường là mạng đường dài <ul style="list-style-type: none"> • Giao thức tầng Giao vận có nhiệm vụ: - Thiết lập tại liên kết. Đồng bộ lại - Theo dõi toàn bộ yêu cầu khởi động lại cho NSD.
Nhóm C	<ul style="list-style-type: none"> - Truyền tin không tin cậy, không liên kết - Mạng đường dài, kết nối nhiều mạng con - 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
<i>Lớp 0</i> <i>Mạng loại A</i>	<ul style="list-style-type: none"> - Lớp thủ tục đơn giản - Kết nối mạng khi có yêu cầu giao vận không phải giải quyết lỗi - Chủ yếu tạo ra trình tự, điều khiển dòng dữ liệu để tầng mạng hoạt động tốt. - Bao gồm cơ cấu thiết lập và huỷ liên kết ở tầng giao diện.
<i>Lớp 1</i> <i>Mạng loại B</i>	<p>Có tính chất tương tự lớp 0, ngoài ra còn thêm:</p> <ul style="list-style-type: none"> - Khởi động lại mạng sau khi N-RESET. Giao thức có khả năng báo nhận (ACK) và truyền dữ liệu khẩn. - Đồng bộ lại và sau đó nối lại liên lạc giữa các thực thể giao vận đã bị gián đoạn - Lớp 1 không kiểm tra lỗi và kiểm soát dòng dữ liệu.
<i>Lớp 2</i> <i>Mạng loại A</i>	<p>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 :</p> <ul style="list-style-type: none"> - Sự ghép kênh : Hai hay nhiều liên kết của tầng giao vận có thể dùng chung một kết nối ở tầng mạng. - Sử dụng khi nhiều liên kết ở tầng giao vận được mở đồng thời, nối liên kết có lưu lượng nhỏ. <p>Ví dụ như hệ thống đặt vé máy bay cho phép tiết kiệm đường truyền.</p>
<i>Lớp 3</i> <i>Mạng loại B</i>	<p>Là tổ hợp lớp 1 và lớp 2</p> <ul style="list-style-type: none"> - Cho phép dồn kênh - Khởi động lại - Điều khiển dòng dữ liệu.
<i>Lớp 4</i> <i>Mạng loại C</i>	<p>Lớp 4 có hầu hết các chức năng của lớp trước và bổ sung thêm một số khả năng kiểm soát luồng dữ liệu.</p> <ul style="list-style-type: none"> - Phải có biện pháp giải quyết vấn đề mất gói tin, gói tin bị hỏng - Phải giải quyết yêu cầu khởi động lại - 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-CREATE.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-CREATE.indication

connum = LISTEN (local)

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

3. Hàm Disconnect thực hiện 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.

Nguyễn Tân Khôi,

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

Chương 7

HỌ GIAO THỨC TCP/IP

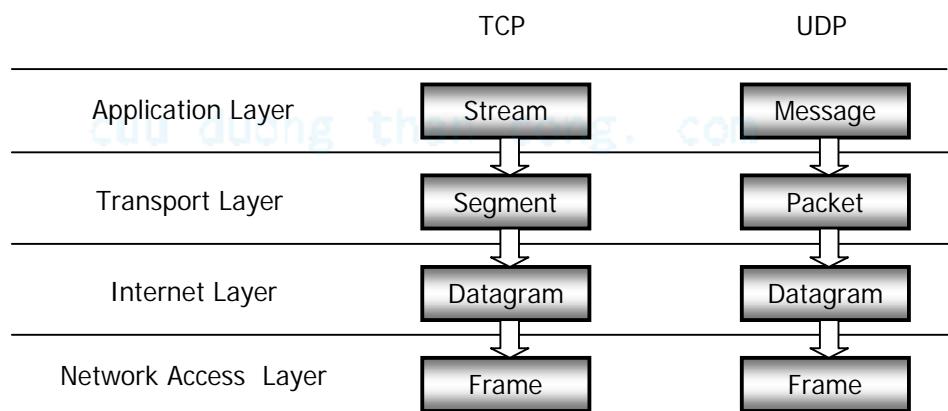
Do đặc tính của mô hình OSI là một mô hình tham chiếu, việc áp dụng mô hình OSI vào thực tế thường có hiệu suất kém do dữ liệu phải truyền qua tất cả các lớp của mô hình OSI ở cả hai máy, mô hình OSI là tiêu chuẩn để các nhà phát triển dựa vào mà phát triển các mô hình khác tối ưu hơn. Có rất nhiều mô 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 gửi 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 phân 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 khôi 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.

Application	Ping	Telnet & Rlogin		SMTP	SNMP	Trace - Route
	DNS	TFTP		RIP	OSPF	etc.
Transport	TCP		UDP		ICMP	
Network	IP					
DataLink	LLC		HDLC		PPP	
	Ethernet	802.3		Frame Relay		SMDS etc.
Physical	Fiber Optics	UTP	Coax	Microwave	Satelite	STP

Hình 7-2. Họ giao thức TCP/IP.

Telnet	Tele Communication	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	Giao 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 gửi và nơi nhận (end-to-end) trong điều kiện lớp mạng loại C không tin cậy. Dòng số liệu có chiều dài tùy 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 gửi 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 gửi 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).

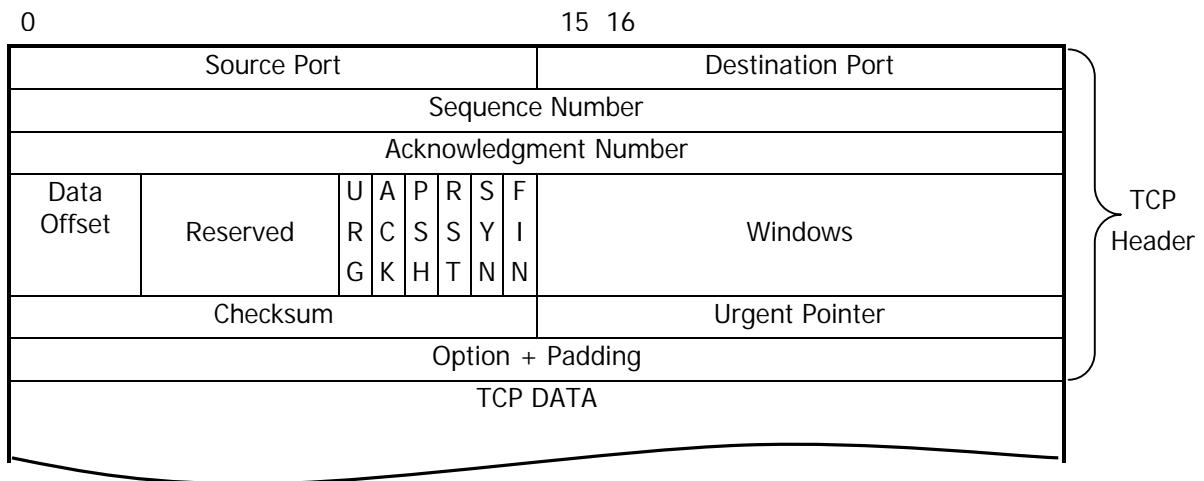
Destination Port - Số hiệu cổng đích (16 bits)

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 tự (32 bits)

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

0	1	2	3	4	5
URG	ACK	PSH	RST	SYN	FIN

Cờ URG : Nếu có giá trị là 1 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 nên có thể có trường hợp là máy gửi sẽ tạo ra một đoạn tin mà phía nhận không thể chấp nhận được.

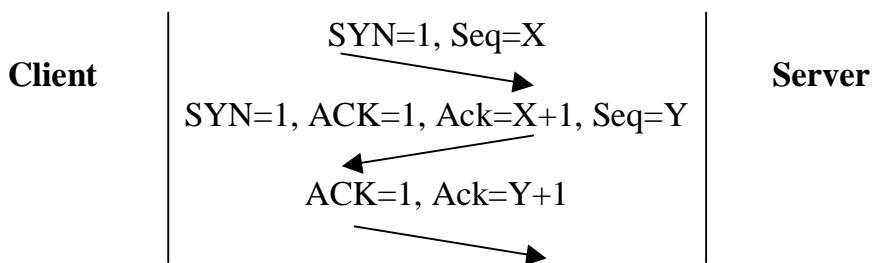
Padding :

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)

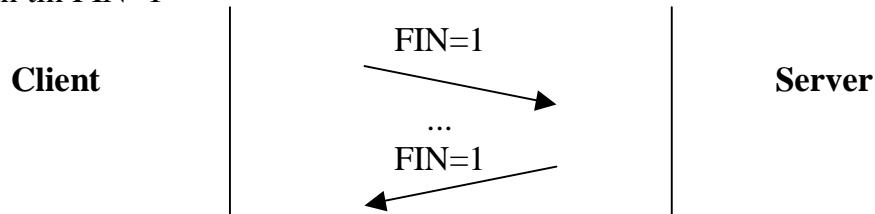
Chứa dữ liệu của tầng trên, độ dài tối đa ngầm định là 536 bytes. Giá trị có thể điều chỉnh bằng cách khai báo trong vùng Options.

7.2.2 Quá trình nối-tách



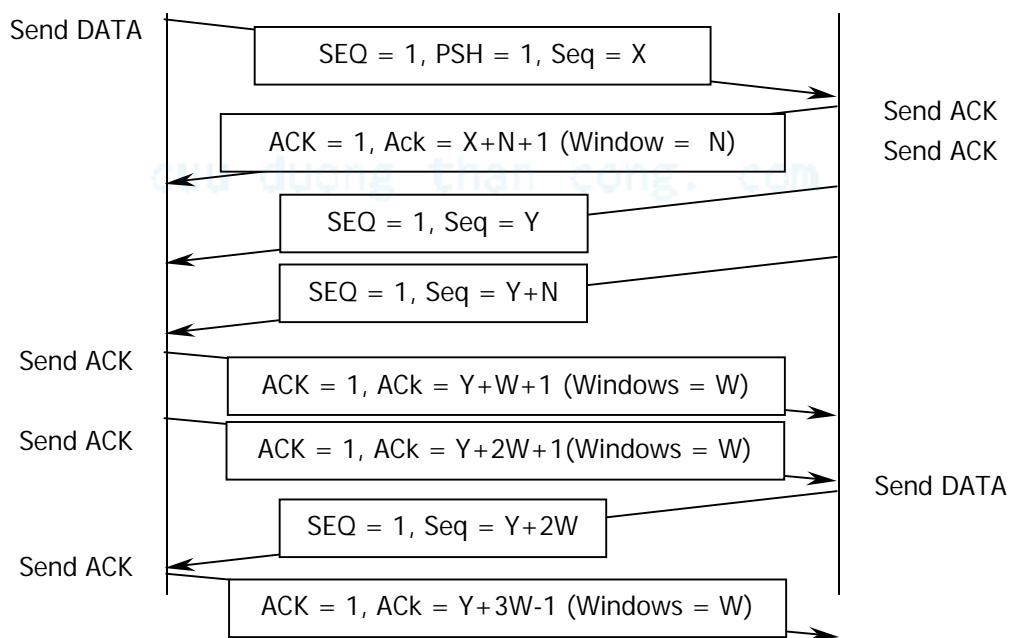
Quá trình thiết lập kết nối bằng thủ tục bắt tay 3 lần (three-way hand). Client gửi bản tin với SYN=1 (yêu cầu kết nối). Server nhận được, gửi bản tin với SYN=1 và ACK=1. Client lại đáp lại với bản tin ACK=1.

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 gởi 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



Hình 7-4. Sơ đồ quá trình trao đổi dữ liệu TCP.

$W = \text{maximum Segment size}$ ($W > N$)

$2W = \text{Windows limit}$

7.2.4 Thủ tục 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.

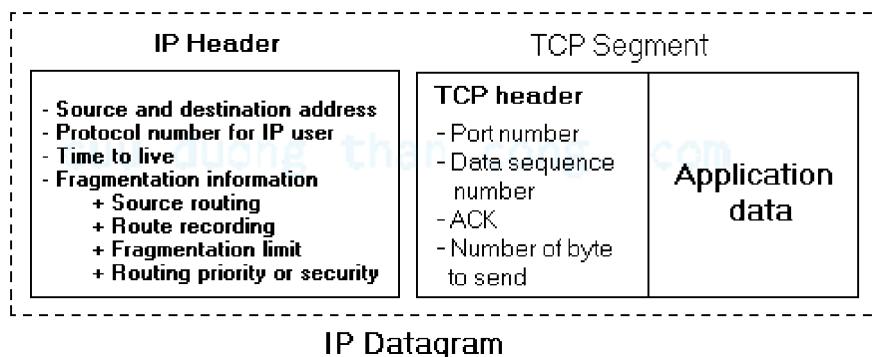
Bước 2: Kiến tạo ra gói tin IP datagram

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

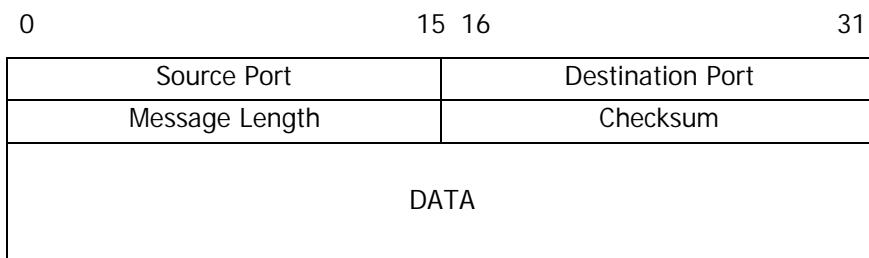
Các IP Datagram chuyển qua các lớp dưới đưa vào và định tuyến để tìm tới địa chỉ đến qua mạng căn cứ vào địa chỉ vật lý của mạng lưới ví dụ như địa chỉ mạng X.25, mạng Frame relay hoặc ngay bản thân của Internet. Tất cả các thông tin này đều nằm trong bảng định tuyến trong các Router. Các mạng X.25 hay 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, đổi chiều số thứ tự, phát hiện những gói thiếu thiêu hay đã nhận được, đồng thời cũng nhận được thông báo (ACK) từ phía phát báo cho biết bên đầy 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 gửi 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 dữ 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 gửi 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 gửi 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 độ 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 gửi và nhận dữ liệu theo quy ước riêng. TCP và UDP chỉ chịu trách nhiệm đưa dữ liệu từ một máy tính này đến một máy tính khác, còn dữ liệu đó được gửi 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 (TFTP)	25 SMTP
514 System Log	42 Name Server
.....	53 Domain Name Server
	79 Finger_find a active user
	80 HTTP

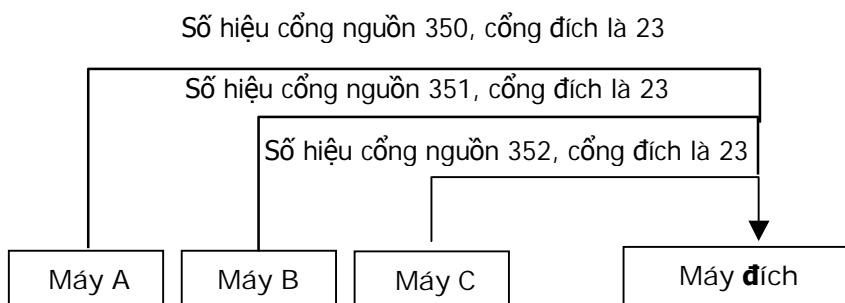
7.4.2 Socket

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 gửi 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 Berkely 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 nhiệm vụ 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 gửi các yêu cầu đến Server và chờ kết quả trả về.

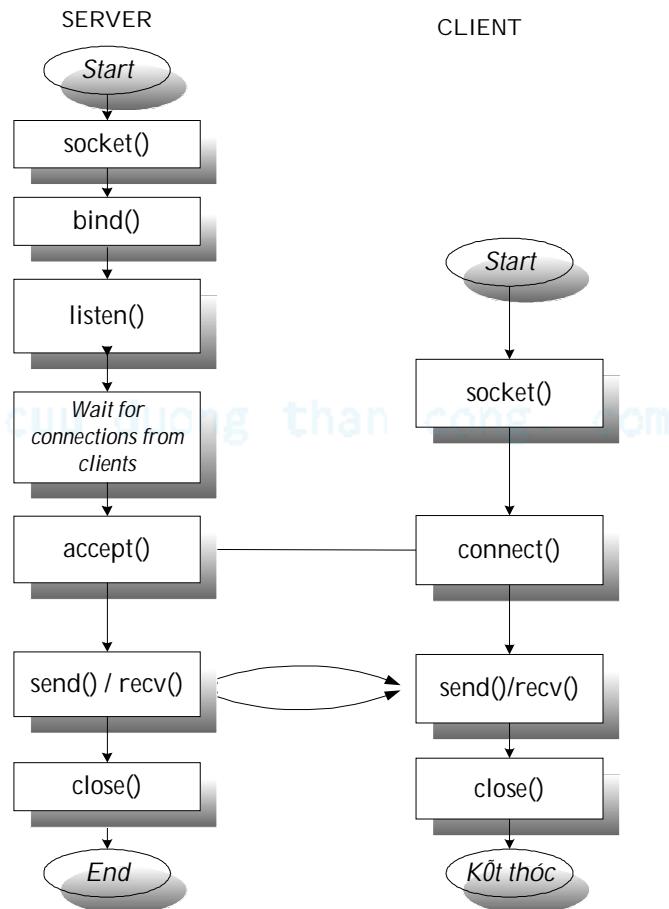
Các chương trình Client và Server thường thực thi trên các máy khác nhau. Mỗi chương trình Server có thể cùng đáp ứng cho nhiều chương trình Client trên nhiều máy tính khác nhau cùng một lúc.

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 lặp, 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 :



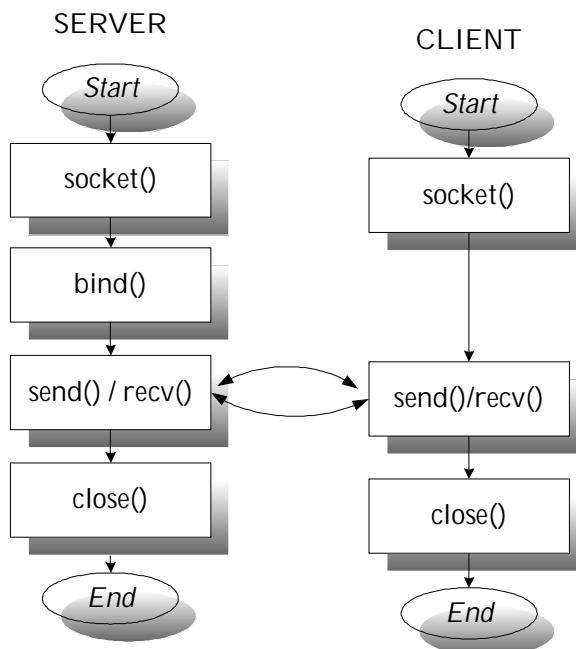
Hình 7-8. Sơ đồ trao đổi dữ liệu giữa Client/Server bằng StreamSocket.

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 mẩu 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 lặp, 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");
    /*unlink("./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.

cuu duong than cong. com

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 lập, 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 thẻ 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 bộ 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 ra sau để thực hiện một trong ba phương thức như sau : hai chiều đồng thời (*full-duplex*), hai chiều luân phiên (*half -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 (diễn 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 lượt 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 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 dịch vụ và một bên cung cấp dịch vụ. Các phiên bản làm việc thường có ít nhất ba giai đoạn :

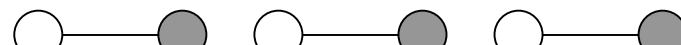
- *Thiết lập tuyến liên kết* : Bên yêu cầu dịch vụ sẽ yêu cầu khởi phát một dịch vụ. Trong quá trình xác lập, phiên truyền thông được thiết lập và các quy tắc được thoả thuận.
- *Chuyển giao dữ liệu* : Do các quy tắc được thoả thuận trong khi xác lập, nên mỗi bên của cuộc thoại sẽ biết nội dung mong 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 :

Liên kết Phiên

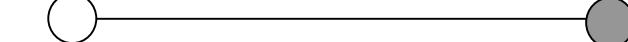


Liên kết Giao vận

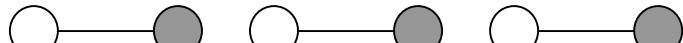


2. Nhiều liên kết giao vận sử dụng cùng một liên kết phi^n:

Liên kết Phiên



Liên kết Giao vận



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 indication, 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	PARAMETERS	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
DISCONNECT	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 settings, resync type, serial number, user data.	Resynchronize
RESYNCHRONIZED ACK	Tokens settings, Serial number, User Data.	Acknowledge resynchronization

PREPARE	Type.	Notify type SPDU is coming
EXCEPTION REDORT	SPDU bit pattern.	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 và 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.

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 thông 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 thỏa 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 gửi 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 phiến 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 bắt 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). Mỗi bối cảnh chỉ rõ cú pháp trùu 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) và 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 một 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 diễn 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 của sự khác biệt đó, ta xem xét hai dịch vụ trình diễn : thiết lập liên kết (connection establishment) và chuyển thẻ bài (token passing).

Khi phát triển các giao thức cho 3 tầng cao của Mô hình OSI, 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 khenh) 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 (embedding), 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 Syntax) và quy tắc mã hóa (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 ASN.1)
- ISO 8825:Basic 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 tùy ý.

TẦNG ỨNG DỤNG

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 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 lưu giữ trong môi trường mạng đầy phức tạp và phải chia sẻ 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, tùy theo lượng thông tin cần bảo vệ và khả năng cho phép của từng hệ thống cụ thể.

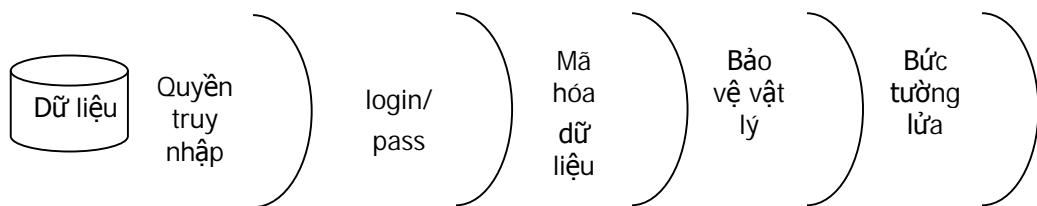
10.1.1 Các chiến lược an toàn hệ thống

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 thống 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.

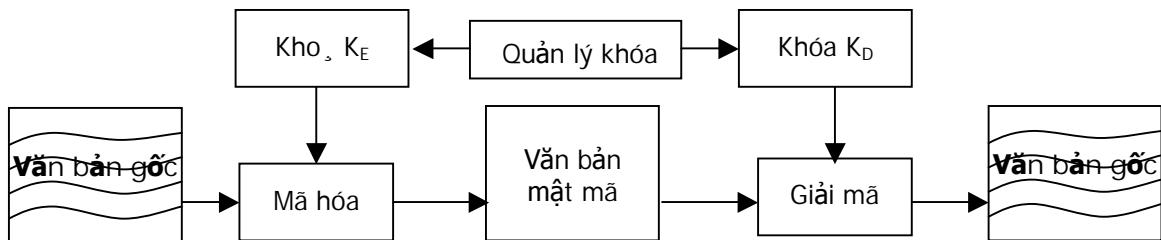
Để bảo vệ thông tin bằng mật mã, người ta thường tiếp cận theo hai hướng:

- 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. Ở 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 đích. Cách này có nhược điểm là chỉ có dữ kiện người dùng mới được mã hoá còn các thông tin điều khiển thì phải giữ nguyên để có thể xử lý 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 hóa.

+ 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 (Decryption 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 khoá:

- 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 ký 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 DHKTĐN 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:

D	A	I	H
O	C	D	A
N	A	N	G

Nếu ta lấy các ký 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 ký tự trong bản mã để suy ra văn bản gốc.

3. Đổi chỗ 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 ký 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 ký 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 hóa 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 hóa được biểu diễn bởi hàm K(T,f). Do vậy, văn bản gốc :

$$M = m_1 \ m_2 \ m_d \ m_{d+1} \dots m_{2d}$$

Trong đó m_i là các kí tự riêng lẻ sẽ được mã hóa thành :

$$Ek(M) = mf_{(1)} \ mf_{(2)} \dots mf_{(d)} \ m_{d+f(1)} \dots m_{d+f(d)}$$

Với $mf_{(1)} \ mf_{(2)} \dots mf_{(d)}$ là một hoán vị của $m_1 \ m_2 \dots m_d$

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	tù	Mã hóa
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 hóa thành RUOTN DAIGH CKYOT UATHD NANAG

10.2.2 Phương pháp thay thế

Phương pháp này mã hóa văn bản bằng cách thay thế mỗi kí tự trong văn 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 hóa và giải mã thông điệp.

2. Thay thế đồng âm

Mỗi kí tự trong văn bản gốc được mã hóa 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 : $f(a) = (a + k) \text{ mod } n$ 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 L M N 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 YWZTS 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.

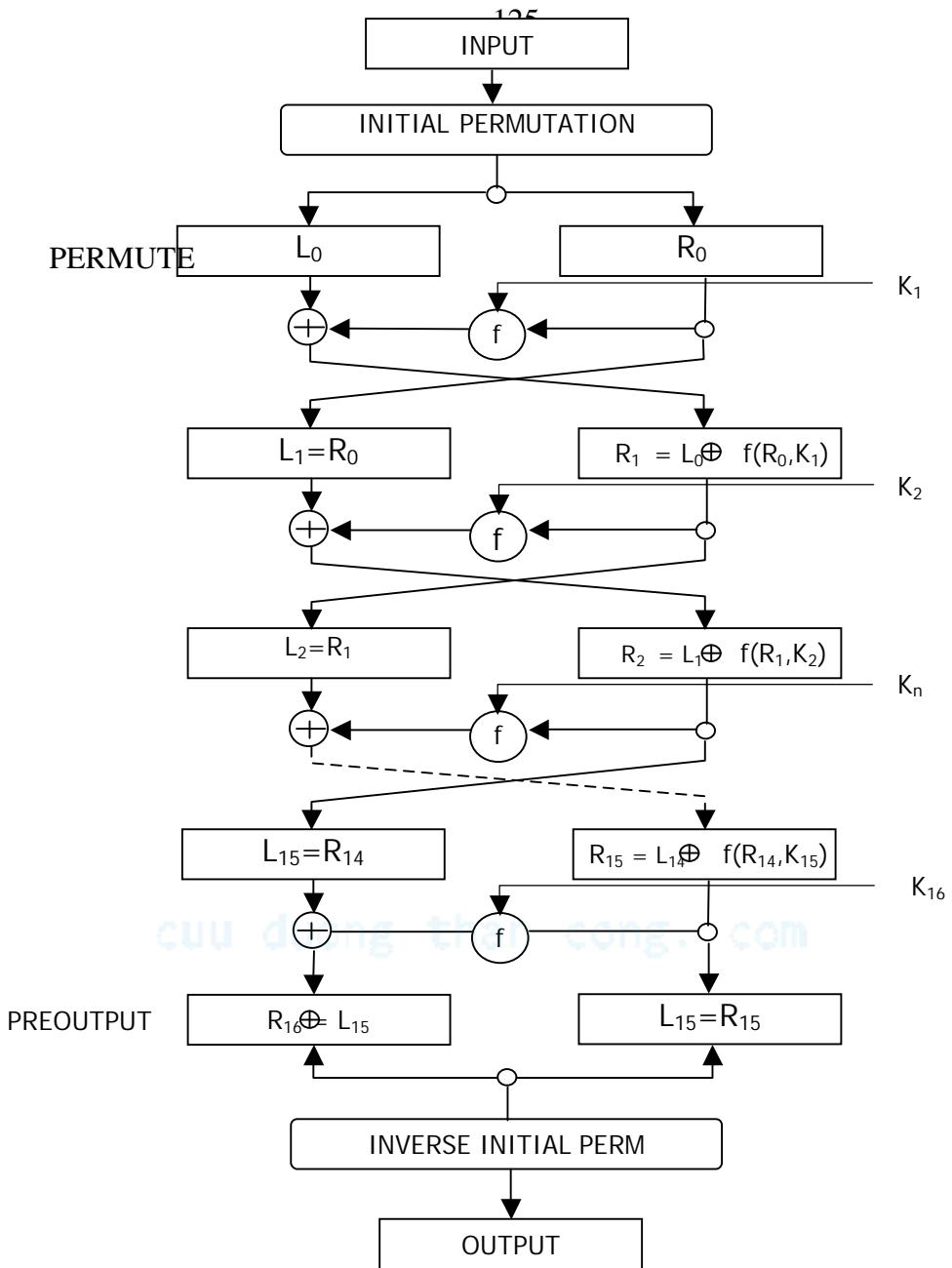
Một phương pháp thay thế khác tốt hơn là dùng từ khoá theo sơ đồ Vignère. Theo sơ đồ này, từ khoá được cộng vào liên tiếp theo từng kí tự một cho văn bản gốc, mỗi kí tự được biểu diễn bởi một vị trí của nó trong bảng kí tự và phép cộng được thực hiện theo môđun 26. Ví dụ, giả sử ta có bảng :

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 hóa dữ liệu DES (Data Encryption Standard) được Mỹ và hãng IBM phát triển trong những năm 70. Lưu đồ mã hóa DES được mô tả như hình sau.

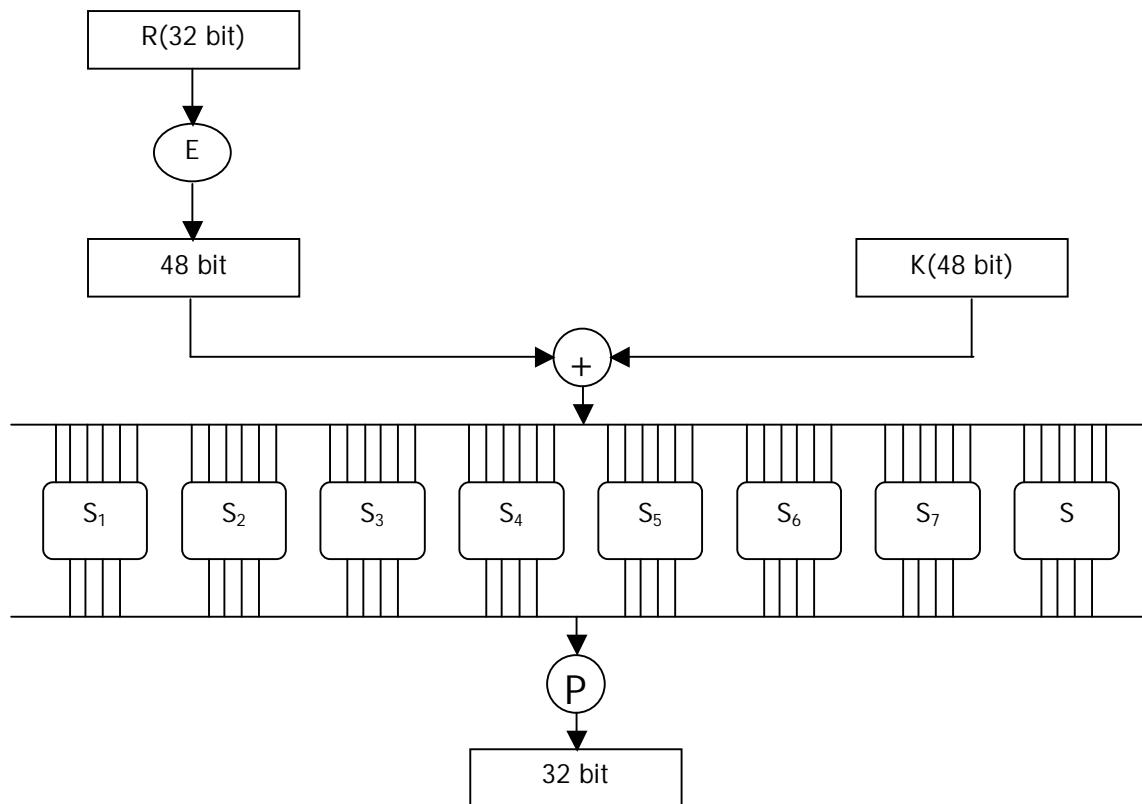


Hình 10-3. Sơ đồ mã hoá DES.

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 :



cuu duong than cong. com

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 modun 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 :

cuu duong than cong. com

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, \dots, 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 họa 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, \dots, 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 điều 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.

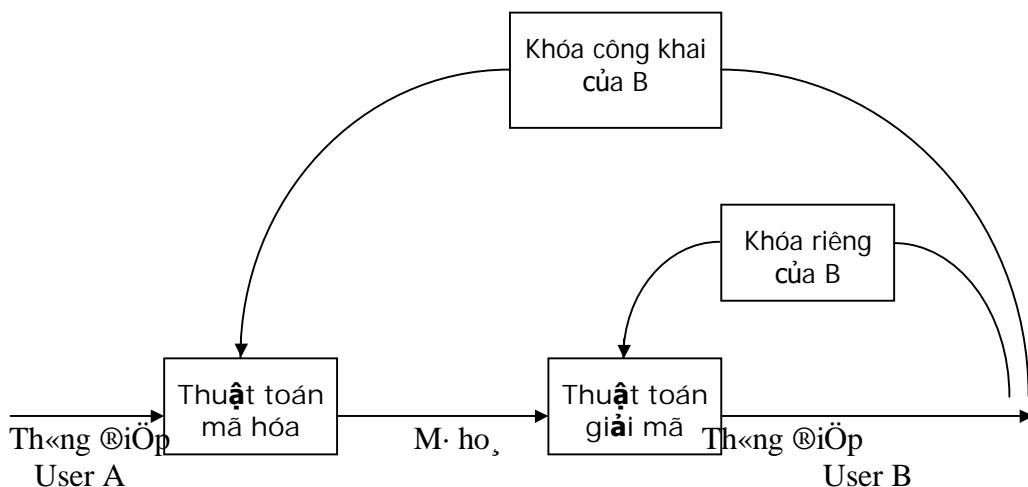
10.2.4 Phương pháp mã hoá khoá công khai

10.2.4.1 Nguyên lý 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 khóa. Có nghĩa là khi khóa này dùng để mã hóa thì khóa kia dùng để giải mã và ngược lại.

Hình sau mô tả nguyên lý quá trình mã hóa/giải mã bằng khóa công khai :



Hình 10-5. Quá trình mã hóa/giải mã bằng khóa công khai.

Quá trình mã hóa/giải mã như sau:

- b. Mỗi hệ thống cuối trong một mạng tạo ra một cặp khóa dùng để mã hóa và giải mã thông tin khi nhận được chúng.
- c. Mỗi hệ thống phải có 2 khóa, khóa công khai và khóa bí mật, khóa công khai được công bố lên mạng tại nơi cho phép đăng ký 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 khóa công khai của B trên mạng để mã hóa nó rồi gửi.
- e. Khi B nhận được thông điệp của A, B sẽ dùng khóa 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 khóa giải mã.

Thông tin về khóa phải được giữ an toàn tuyệt đối và có thể cập nhật hoặc thay đổi lại khóa cũ. Việc tạo ra các hệ thống bảo vệ và quản lý khóa cũng cần hết sức chặt chẽ.

10.2.4.2 Phương pháp mã hóa RSA

Bản thuyết trình đầu tiên của Diffie và Hellman đưa ra năm 1976 tại hội nghị MIT và gần như ngay lập tức, sự thách thức về vấn đề mã hóa đã tìm được câu trả lời bởi hệ thống mã hóa công khai. Một trong những câu trả lời đầu tiên đưa ra vào năm 1977 bởi Ron Rivest, Adi Shamir và Len Adleman 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 : $M = M_1 M_2 \dots M_k$

Văn bản mã hóa : $C = C_1 C_2 \dots C_k$, trong đó $C_i = M_i^E \text{ mod } n$, 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:*

$$(mk^{\phi(n)+1} = mk^{(p-1)(q-1)+1}) \text{ mod } m = n$$

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: $ED \text{ mod } \phi(n) = 1$.

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 $\text{USCLN}(\phi(n), E) = 1$; với $1 < E < \phi(n)$
5. Tìm D thỏa $DE \text{ mod } \phi(n) = 1$.

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 $C = ME \text{ mod } n$, rồi gửi nó đi.
- User A sẽ nhận được thông điệp đã mã hoá và giải mã nó bằng khoá riêng của mình bằng công thức $M = CD \text{ mod } n$

Ví dụ: Chọn $p = 7, q = 17$

$$\text{Tính } n = p * q = 7 * 17 = 119$$

$$\phi(n) = (p-1)*(q-1) = 96$$

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 = 19⁵ mod 119 = 66.

Quá trình giải mã: M = 66⁷⁷ mod 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 Adlertian 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:

$$((a \text{ mod } n) * (b \text{ mod } n)) \text{ mod } n = (a * b) \text{ mod } n$$

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 ký 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 khoá 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 khoá	Thời gian
50	4 giờ

75	104 ngày
100	74 năm
200	4.000.000 năm
300	5×10^{15} năm
500	4×10^{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 ký số (digital signature) có thể dùng để tạo ra một chữ ký 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

Vẫn 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:

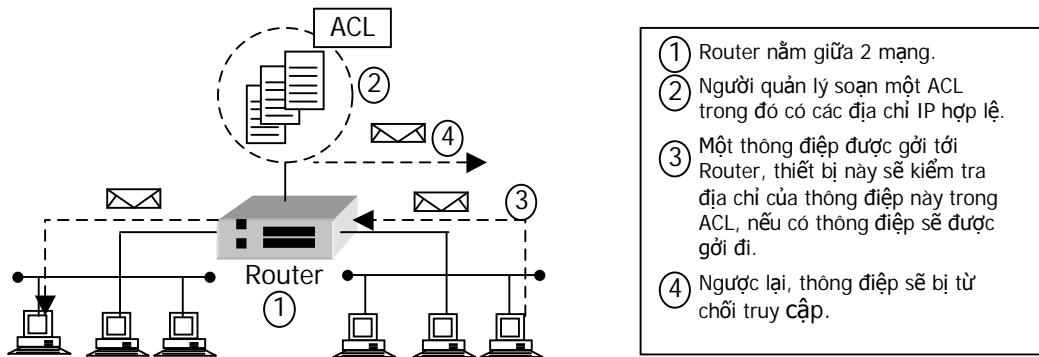
1. Tất cả các trao đổi dữ liệu từ trong ra ngoài và ngược lại phải thực hiện thông qua firewall.
2. Chỉ có những trao đổi nào được phép bởi chế độ an ninh của hệ thống mạng nội bộ (trusted network) mới được quyền lưu thông qua firewall.

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 ở 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 cần 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 đoạn 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 gọi 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.

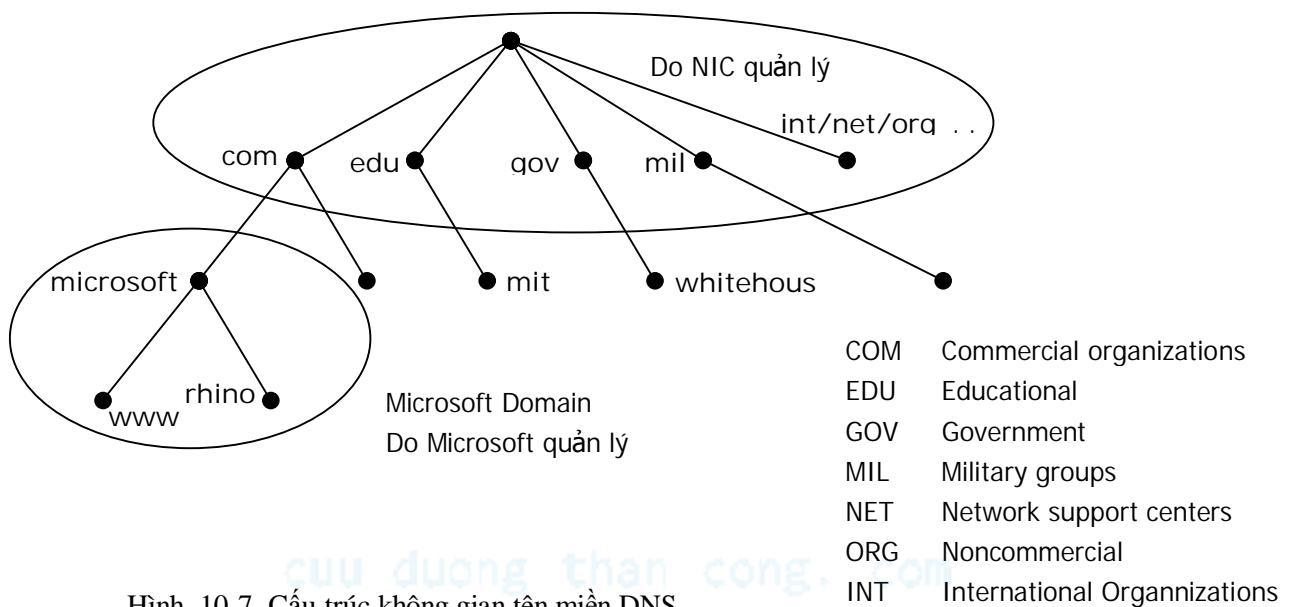
Theo Paul Mockepetris, người thiết kế chính DNS, mục tiêu thiết kế bắt đầu của DNS là để thay thế các tập tin host phức tạp bằng một cơ sở dữ liệu phân tán nhẹ hơn có khả năng cung cấp một *không gian tên thứ bậc, sự quản lý phân tán, có bộ đệm cục bộ (caching), các kiểu dữ liệu mở rộng, kích thước cơ 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 Berkeley 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 định : Miền gốc và các miền mức định của cây DNS do NIC quản lý. Các tên miền mức 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 dùng để ánh xạ địa chỉ thành tên.

Trách nhiệm quản lý không gian tên DNS dưới mức định 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 hằng 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, . . .

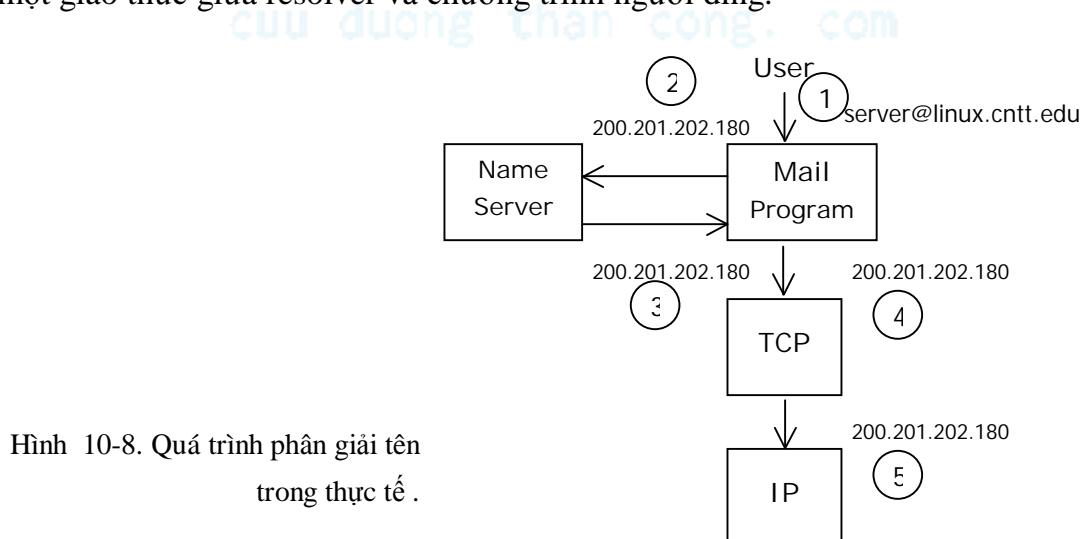
```
<domain> ::= <subdomain> | ""
<subdomain> ::= <label> | <subdomain> "." <label>
<label> ::= <letter> [[<ldh-str>] <let-dig>]
<ldh-str> ::= <let-dig-hyp> | <let-hyp> <ldh-str>
<let-dig-hyp> ::= <let-dig> | "-"
<let-dig> ::= <letter> | <digit>
<letter> ::= ký tự từ A-Z, a-z
<digit> ::= chữ số 0-9
```

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 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 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 dùng.



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 tượng quản trị (manager objects).
- Tiến trình Agent thực hiện các thao tác quản trị mạng như đặt các tham số cấu hình và các thông 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 và đánh 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 giao thức TCP/IP, không phụ thuộc vào IP. SNMP 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 :

- **Phân 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 dụng:

Trường	Chức năng
DATE	Chỉ ngày giờ nhận mail.
FROM	Chỉ địa chỉ người gửi.
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 gửi.
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 sau là cũng giống như ta thấy trên một trường chuẩn.

- **Phần nội dung**

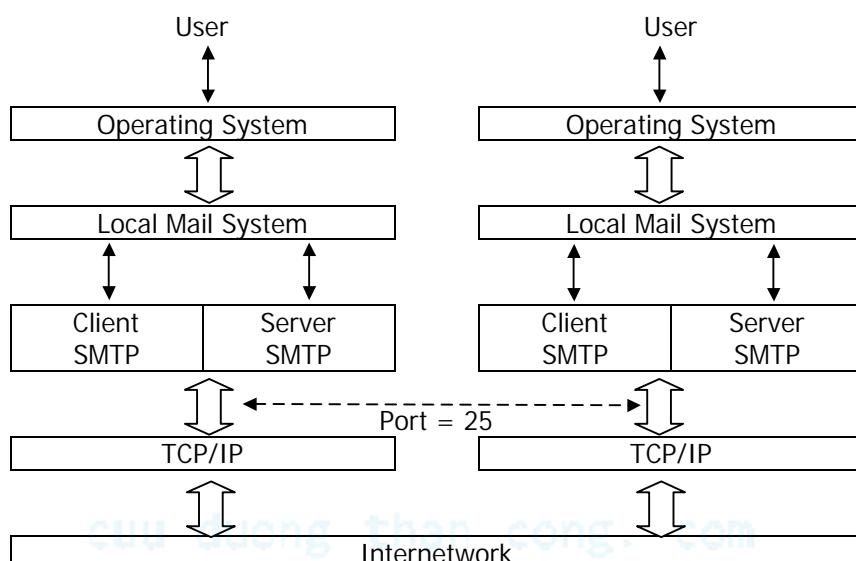
Để phân biệt phần tiêu đề và phần nội dung của e-Mail, người ta qui ước đặt ranh giới là một dòng trắng (chuỗi ký tự "`\r\n`"). Kết thúc của phần nội dung là chuỗi ký tự "`\r\n.\r\n`".

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. Một 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.

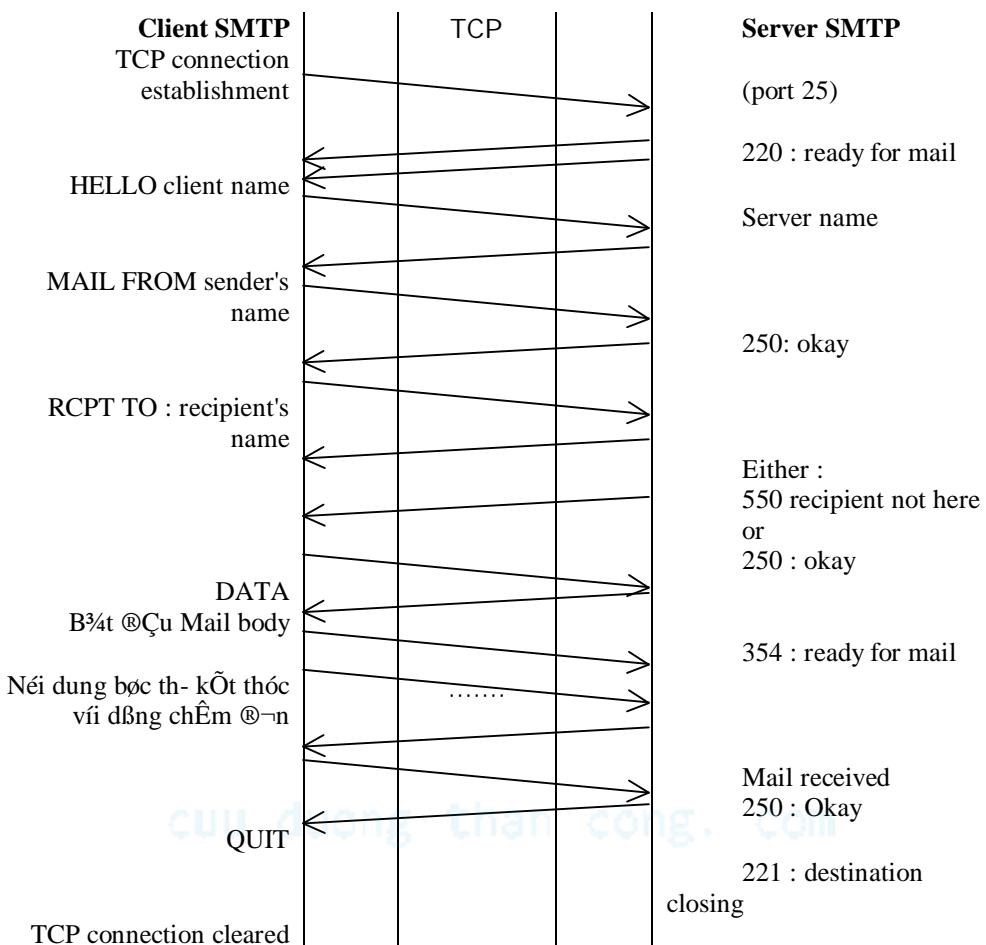
Sau khi tháo bức thư trong khuôn dạng chuẩn, hệ thống mail cục bộ xác định tên người nhận ở hộp thư cục bộ hay phải gửi ra ngoài. để gửi bức thư Client SMTP

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 mỗi 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	Xung danh với SMTP bên nhận, báo cho bên nhận biết bên gửi là ai. SMTP bên gửi 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 gửi theo dòng lệnh.
SEND	Khởi động một cuộc giao dịch mà mail sẽ được gửi tới một hay nhiều thiết bị đầu cuối chứ không phải mailbox.
SOML	Khởi động một cuộc giao dịch mà mail sẽ được gửi tới một hay nhiều thiết bị đầu cuối hay mailbox.
SAML	Khởi động một cuộc giao dịch mà mail sẽ được gửi 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 gửi 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 gửi OK và đổi vai trò trở thành SMTP gửi.

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 lý 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 gửi đến một SMTP nhận và đến lượt SMTP nhận trở thành SMTP gửi 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 gửi 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 gửi tên Thuận ở máy Sample1 muốn gửi cho Tín , Thúc ở máy Sample2, giả sử Thúc không có Mailbox tại Sample2.

Bên gửi 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 gửi biết dịch vụ SMTP đã sẵn sàng.

SENDER : HELO sample1

Bên nhận đã sẵn sàng, bên gửi gửi HELLO và xưng tên người gửi.

RECEIVER : 250 sample2

Trả với mã 250 báo cho biết bên nhận đã sẵn sàng.

SENDER : MAIL FROM: <>

Bên gửi dùng lệnh MAIL để khởi động phiên giao dịch. Cú pháp trên cho bên nhận biết địa chỉ bên gửi (mailbox của bên gửi) để bên nhận gửi thông báo lỗi nếu có về bên gửi.

RECEIVER : 250 OK

Trả lời với mã 250 cho biết đã chấp nhận.

SENDER: RCPT TO: <>

Bên gửi cho biết e-Mail đích

RECEIVER: 250 OK

Trả lời với mã 250 cho biết đã chấp nhận

SENDER : RCPT TO: <>

Muốn gửi 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 đổi 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 gửi 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 Extension) 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 :

{Đòng này xác định MIME message}

MIME-Version: 1.0

To:

Subject: Book CD

{Đòng này xác định đây là một kiểu message 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 sau là dạng text và sử dụng các kí tự theo kiểu text.

Header này có thể hoàn toàn tùy 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 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 tùy 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%.

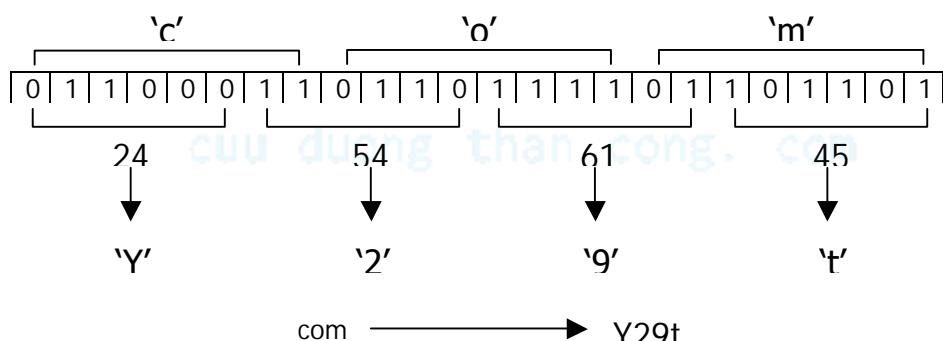
Một tập 65 kí tự US-ASCII được dùng, cho phép 6bits biểu diễn cho các kí tự có thể in được. (Kí tự thứ 65, “=”, là một kí tự xử lý đặc biệt)

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 ký 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 gấp 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..hay yêu cầu gửi 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 TCP 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

```

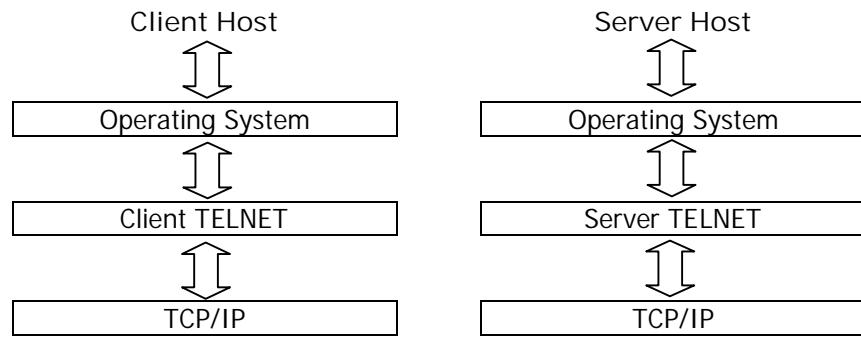
CLIENT : QUIT ; đóng kết nối TCP hiện hành
SERVER : +OK dhbk POP3 server signing off

```

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 gửi 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 ký tự và bàn phím logic có thể tạo các ký 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 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 trả 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 Đề 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, WONT, 'O', SE	: Hoặc từ chối

- Làm việc với Telnet
 - Truy nhập vào mạng TCP/IP từ máy trạm
 - Gõ lệnh : telnet <Địa chỉ IP hoặc tên máy Server>
 - 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).

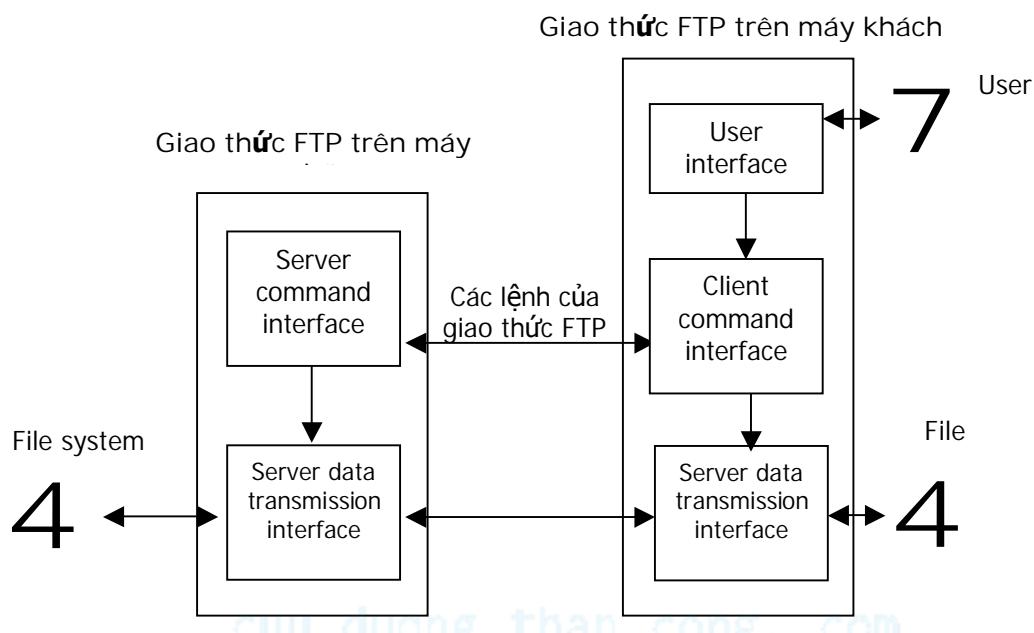
FTP dùng hai kênh TCP, với số hiệu cổng 20 là **kênh dữ liệu**, và số hiệu cổng 21 là **kênh lệnh** (*command channel*). FTP khác các ứng dụng khác của TCP/IP ở là FTP quản lý tất cả việc truyền các tập tin bằng foreground thay vì background. Nói cách khác, FTP không dùng các hàng đợi hay các tiến trình 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 gửi 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 tùy 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 có 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 liệu.



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 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 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 mất đi các kí tự không nén.

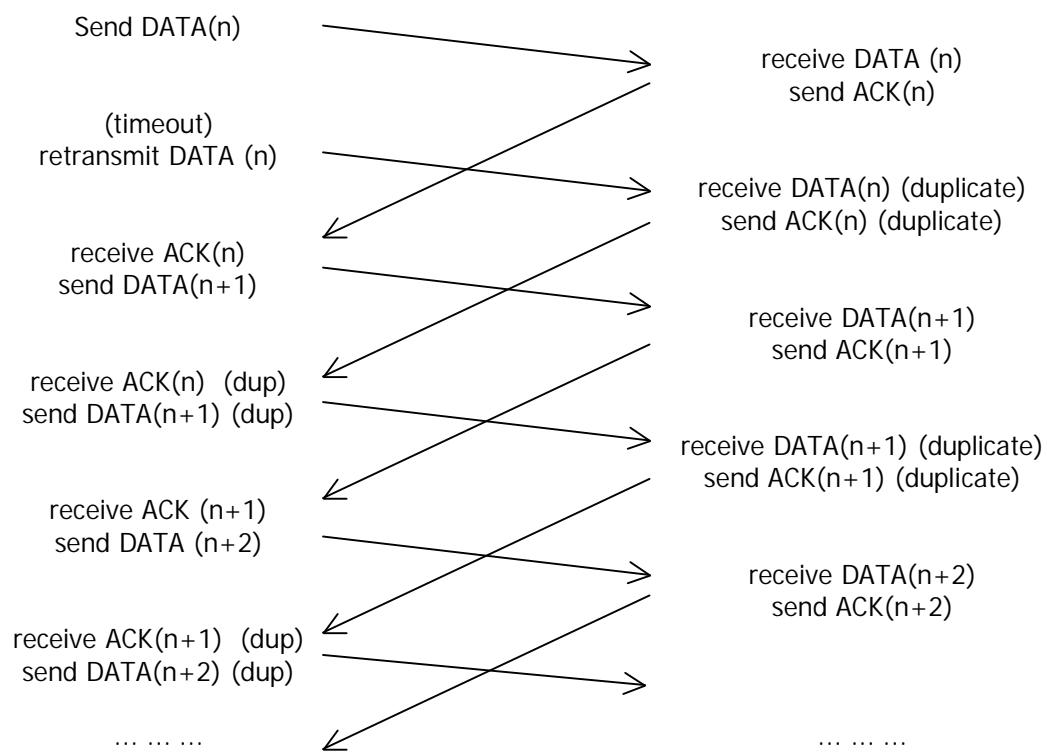
Để bắt đầu, client gửi yêu cầu **read** hay **write**. Gói tin trao đổi có độ dài đến 512 bytes. Mỗi block số liệu có đánh số và phải được nhận để gửi tiếp hay phát lại. Để tránh phát trùng lặp khi hết thời hạn, phát lại bản tin vừa phát và khi nhận ACK (n) trùng lặp thì không phát gì.

10.7.2.2 Dạng bản tin FTP

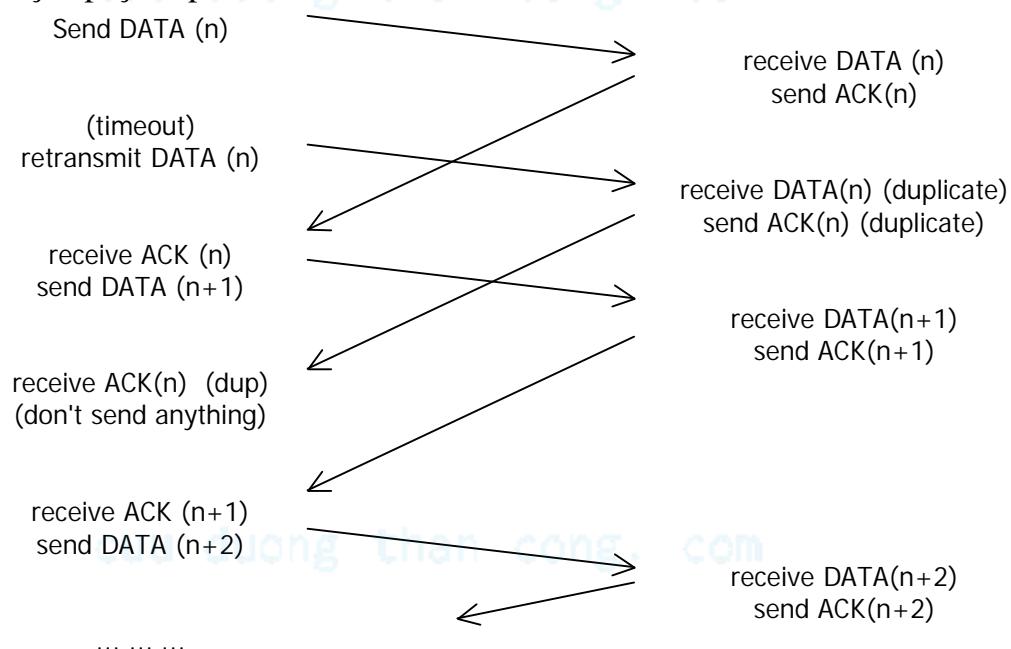
Read request (RRQ)	opcode 01 2 bytes	String File name n bytes	EOs 0 1 byte	String mode n bytes	EOs 0 1 byte
Write request (WRQ)	opcode 02 2 bytes	String File name n bytes	EOs 0 1 byte	String mode n bytes	EOs 0 1 byte
DATA	opcode 03 2 bytes	Block# 2 bytes		Data n bytes, 0≤n≤512	
Acknowled- gement (ACK)	opcode 04 2 bytes	Block# 2 bytes			
Read request (RRQ)	opcode 05 2 bytes	Errorcode 2 bytes	String Err String n bytes	EOs 0 1 byte	(EOs : End of String)

Hình 10-13. Khuôn dạng bản tin FTP.

Ví dụ: Quá trình phát lặp :



+ Trình phết lເບພຸດງອງ ທ່ານ ດອງ.



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.

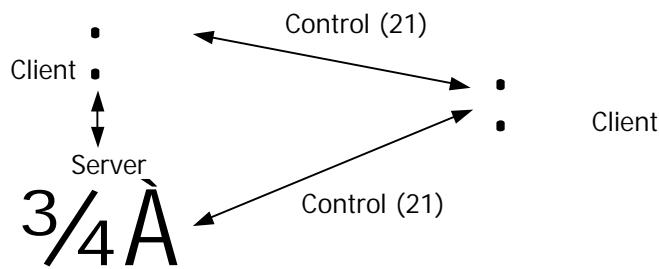
Lệnh FTP	Mô tả
ascii	Chuyển sang chế độ truyền ascii
bell	âm thanh của chương trình sau khi truyền mỗi tập tin
binary	Chuyển sang chế độ truyền nhị phân
cd <i>directory</i>	Chuyển đổi thư mục hiện hành trên server
cdup	Lùi thư mục hiện hành về một cấp trước đó
close	Huỷ kết nối
delete <i>filename</i>	Xoá một tập tin trên server
dir <i>directory</i>	Hiển thị thư mục <i>directory</i> của server
get <i>filename</i>	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 <i>directory</i>	Chuyển đổi thư mục hiện hành trên máy cục bộ
ls <i>directory</i>	Xem danh sách các tập tin trong thư mục <i>directory</i> trên Server
mdelete <i>files</i>	Xóa nhiều tập tin trên máy Server
mdir <i>directories</i>	Liệt kê các tập tin trong nhiều thư mục trên máy Server
mget <i>files</i>	Lấy một số file trên Server về thư mục hiện hành của máy cục bộ
mkdir <i>directory</i>	Tạo thư mục <i>directory</i> trên máy Server
mput <i>files</i>	Gửi một số tập tin từ máy cục bộ lên máy Server
open <i>host</i>	Kết nối với Server host từ xa
put <i>filename</i>	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 <i>file1</i> <i>file2</i>	Đổi tên <i>file1</i> trên máy Server thành <i>file2</i>
quote	Cung cấp một lệnh FTP một cách trực tiếp
quit	Chấm dứt kết nối và thoát khỏi ftp
?	Hiển thị danh sách lệnh

Để 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. Account 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 tùy chọn thứ hai để xác định các ràng buộc dữ liệu. Khi được sử dụng, tham số này là một tùy 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 lý 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 kiểu 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 dụng 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 trực đúng 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, 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 Lincoln
: - (Tôi buồn/ tức giận	=) : =)	Bác Sorkin
: -	Tôi thờ ơ	* < : -)	Ông già Noel
; -)	Tôi nháy mắt	< : - (Người tối dạ
; - (0)	Tôi kêu la	(- :)	Người Uyên
; - (*)	Người nôn (mửa)	; - x	Man with bowtie
; +)	Cắm chè	# -)	Tóc mướt
; -))	Cắm chè	8 -)	Mang kính
; - {)	Rìa	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 chủ đề 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 mẩu 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 (hypertext/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 /hypertext/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 Language) 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 xác 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 đê 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 này. Nội dung văn bản nằm giữa <!-- và --> sẽ được chương trình Browse bỏ qua. Cho phép có khoảng 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...

 ...

Trong đó URL_DATA là địa chỉ tới kiểu dữ liệu cần liên kết. Ví dụ:

d. *Liên kết với các dịch vụ thông tin khác trên mạng*

 ...

Trong đó URL_Service là một địa chỉ đến các dịch vụ trên internet.

 Liên kết với 1 Web Site.

 Với 1 Ftp Site.

 Với 1 Gopher server.

 Liên kết với 1 nhóm Tin.

 liên kết tới 1 địa chỉ gửi Mail. Liên kết này 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

- TARGET: Chương trình Browser có thể nạp đối tượng liên kết vào 1 cửa sổ chỉ định bằng thẻ này. Nếu cửa sổ này cha có, trình Browse sẽ mở 1 cửa sổ mới. Chủ yếu thẻ này dùng cho frames.

Dạng chung:

Link text

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: Link text 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 này lại xuất hiện khi kéo Mouse ra khỏi liên kết. Thí dụ: Link text
OnClick	Khi bấm Mouse lên liên kết, sẽ xuất hiện hộp thoại yêu cầu xác nhận. Thí dụ: Link text

3. Thẻ <INPUT>

Dùng để tạo một field để nhận tác động của người sử dụng.

<INPUT TYPE = “Kiểu” NAME = “TênĐT”
 SIZE = “KíchThước”
 VALUE = “Giá trị” MAXLENGTH = “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 này 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 này. Thí dụ: <input type="button" value="hello" name="btnhello">
HIDDEN	Với thuộc tính này, 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 checkbox vào tài liệu. Thí dụ : <p>So thích <input type="checkbox" name="C1" value="ĂN">The thao <input type="checkbox" name="C2" value="ĂN">Xem phim</p>
RADIO	Chèn 1 field có dạng nút Radio. Ví dụ : <p>Gioi tính <input type="radio" checked value="V1" name="R1">Nam <input type="radio" name="R2" value="V2">Nu</p>
RESET	Chèn 1 nút bấm dùng phục hồi lại tình trạng cũ cho các field. Đặt tên của nút này qua thuộc tính Values.
SUBMIT	Một dạng nút bấm giống ROSQT. Có tác dụng giống nh xác nhận đồng ý. Thí dụ: <p><input type="submit" value="Submit" name="B1"> <input type="reset" value="Reset" name="B2"></p> Chèn 1 nút có tên "SUBMIT" và sẽ hiển thị thông báo "Xin chào các bạn" khi người sử dụng Mouse vào nút này : <INPUT TYPE="SUBMIT" OnClick="Xin chao cac ban">
TEXT	Nhập 1 dòng text vào fields. Dùng thuộc tính SIZE 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. <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 : <p><textarea name="Ghichu" rows="2" cols="20"></textarea></p>

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 gửi 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: Form 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. *The 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. *The SELECT*

- Hiển thị hộp ComboBox cho phép chọn lựa một trong nhiều giá trị :

```
<SELECT NAME =”TenDT”>
    <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. Thể <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 này.

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 <http://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 này. 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. Thể

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 này cũng hiển thị theo dạng ToolTip khi dời chuột đến hình.

Ví dụ: Read these instructions.

- SRC="URL of image": Chỉ định địa chỉ file hình chèn vào trang Web.

Ví dụ : Be sure to read these instructions.

- WIDTH=value/ HEIGHT=value: Chỉ định khoảng cách dành sẵn 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 dưới hình, HSPACE cho trái và phải hình. Value tính theo pixel.
- LOWSRC: Thuộc tính này 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 lượng file lớn hơn:

Ví dụ:

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 thay thế.

10.7.4.2 Chỉ định tài nguyên trong URL

Để chỉ định vị trí của tài nguyên HTTP dùng URL (Uniform Resource 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 bắt 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.
-

cuu duong than cong. com

cuu duong than cong. com

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 réseaux*, EYROLLES, 2003

cuu duong than cong. com

@2004, Nguyễn Tân Khôi

Khoa Công Nghệ Thông Tin - Trường Đại học Bách Khoa Đà Nẵng

-----o& o-----

BÀI GIẢNG

MÔN: MẠNG MÁY TÍNH

Biên soạn: ThS. Trần Bá Nhiệm

cuuduongthancong.com

GIỚI THIỆU MÔN HỌC

- Mục đích của môn học
 - Kiến thức cơ bản về mạng máy tính
 - Mô hình tham khảo OSI
 - Mô hình TCP/IP
- Thời lượng: 5 buổi học

cuu duong than cong. com

GIỚI THIỆU MÔN HỌC

- Nội dung môn học
 - Chương 1: Tổng quan về mạng máy tính
 - Chương 2: Cấu trúc của mạng
 - Chương 3: Phương tiện truyền dẫn và thiết bị mạng
 - Chương 4: Data link
 - Chương 5: TCP/IP
 - Chương 6: Khái niệm cơ bản về bảo mật mạng
 - Bài tập

CHƯƠNG 1: TỔNG QUAN VỀ MẠNG MÁY TÍNH

- Khái niệm về mạng máy tính
- Ứng dụng của mạng máy tính
- Phân loại mạng máy tính
- Mô hình OSI

Khái niệm về mạng máy tính

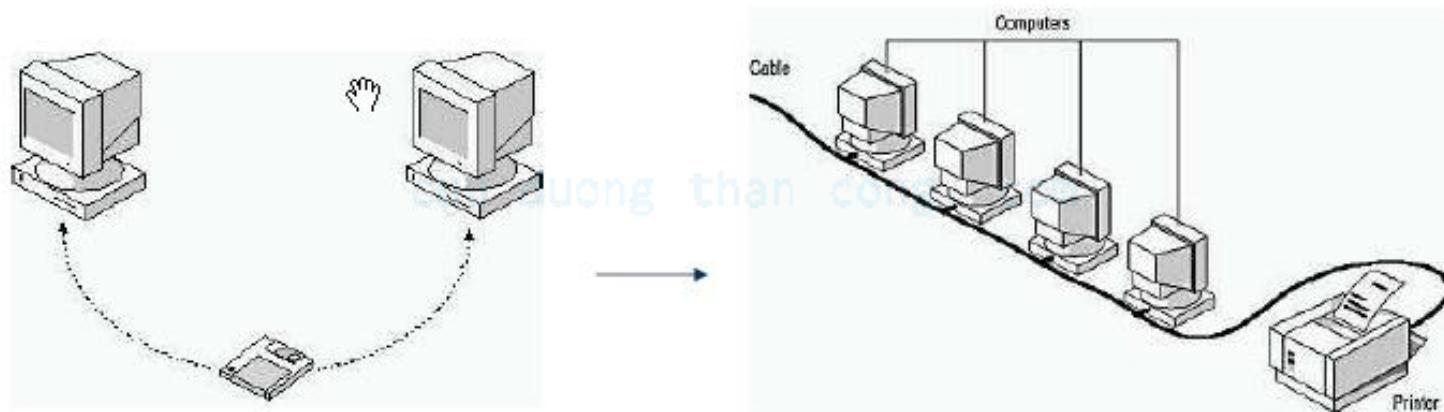
- Một tập hợp của các máy tính độc lập được kết nối bằng một cấu trúc nào đó.
- Hai máy tính được gọi là kết nối nếu chúng có thể trao đổi thông tin.
- Kết nối có thể là dây đồng, cáp quang, sóng ngắn, sóng hồng ngoại, truyền vệ tinh...

cuuduongthancong.com

Ứng dụng của mạng máy tính

- Chia sẻ thông tin
- Chia sẻ phần cứng và phần mềm
- Quản lý tập trung

cuuduongthancong.com

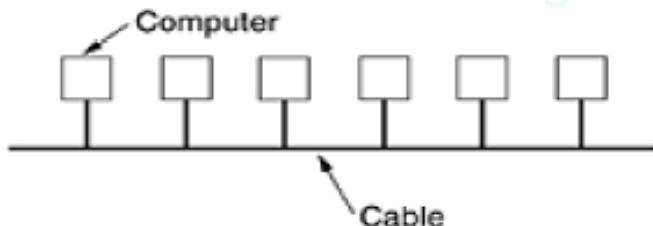


Phân loại mạng máy tính

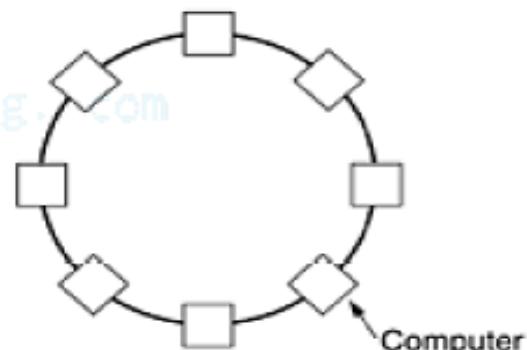
- Cách phân loại mạng máy tính được sử dụng phổ biến nhất là dựa theo khoảng cách địa lý của mạng: Lan, Man, Wan.
- Theo kỹ thuật chuyển mạch mà mạng áp dụng: mạng chuyển mạch kênh, mạng chuyển mạch thông báo, mạng chuyển mạch gói.
- Theo cấu trúc mạng: hình sao, hình tròn, tuyến tính...
- Theo hệ điều hành mà mạng sử dụng: Windows, Unix, Novell...

LANs (Local Area Networks)

- Có giới hạn về địa lý
- Tốc độ truyền dữ liệu cao
- Tỷ lệ lỗi khi truyền thấp
- Do một tổ chức quản lý
- Sử dụng kỹ thuật Ethernet hoặc Token Ring
- Các thiết bị thường dùng trong mạng là Repeater, Bridge, Hub, Switch, Router.

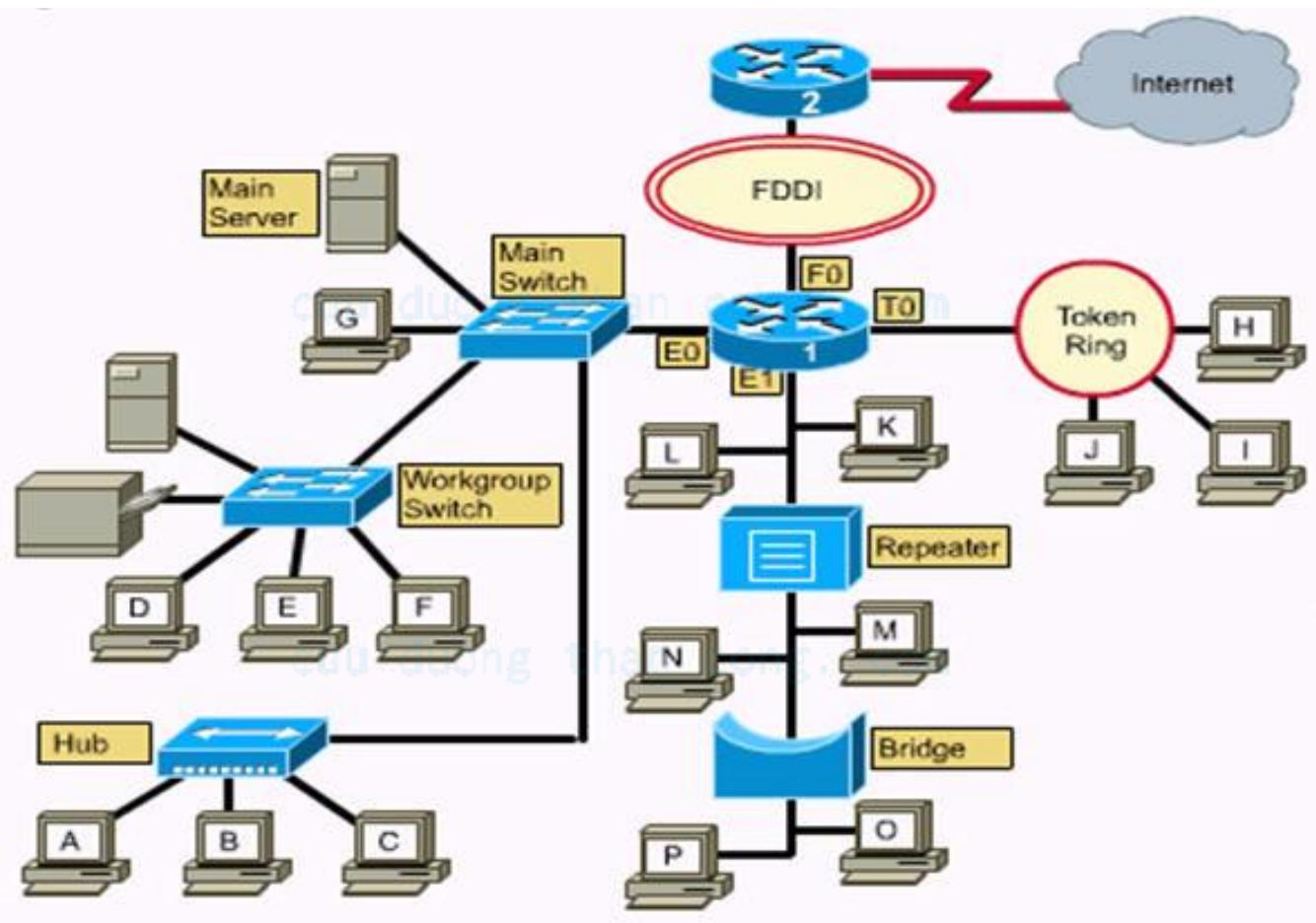


802.3 Ethernet



802.5 Token Ring

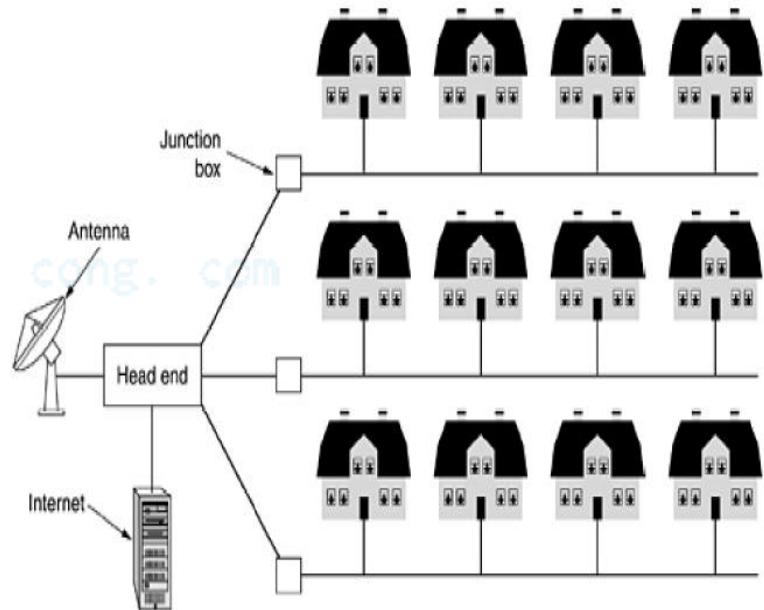
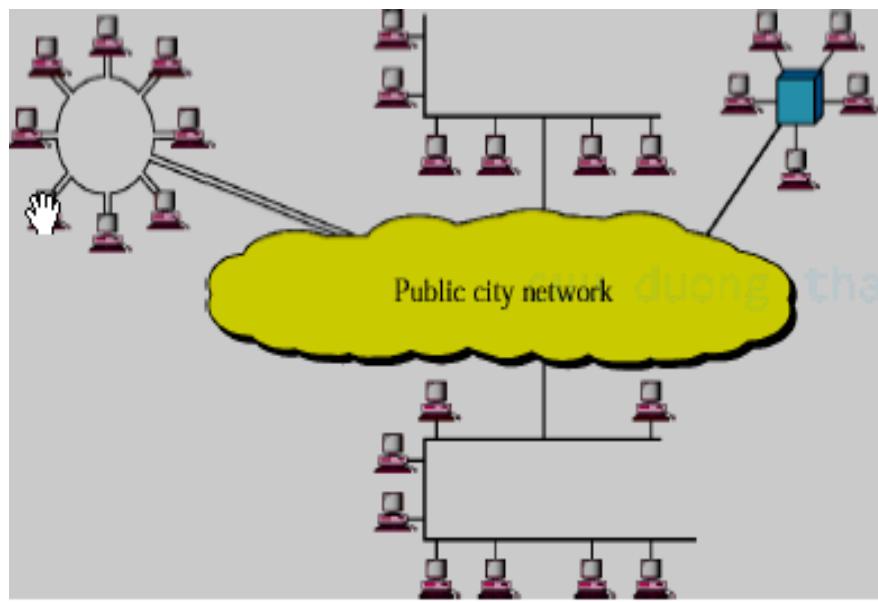
LANs



MANs (Metropolitan Area Networks)

- Có kích thước vùng địa lý lớn hơn LAN
- Do một tổ chức quản lý
- Thường dùng cáp đồng trực hoặc cáp quang

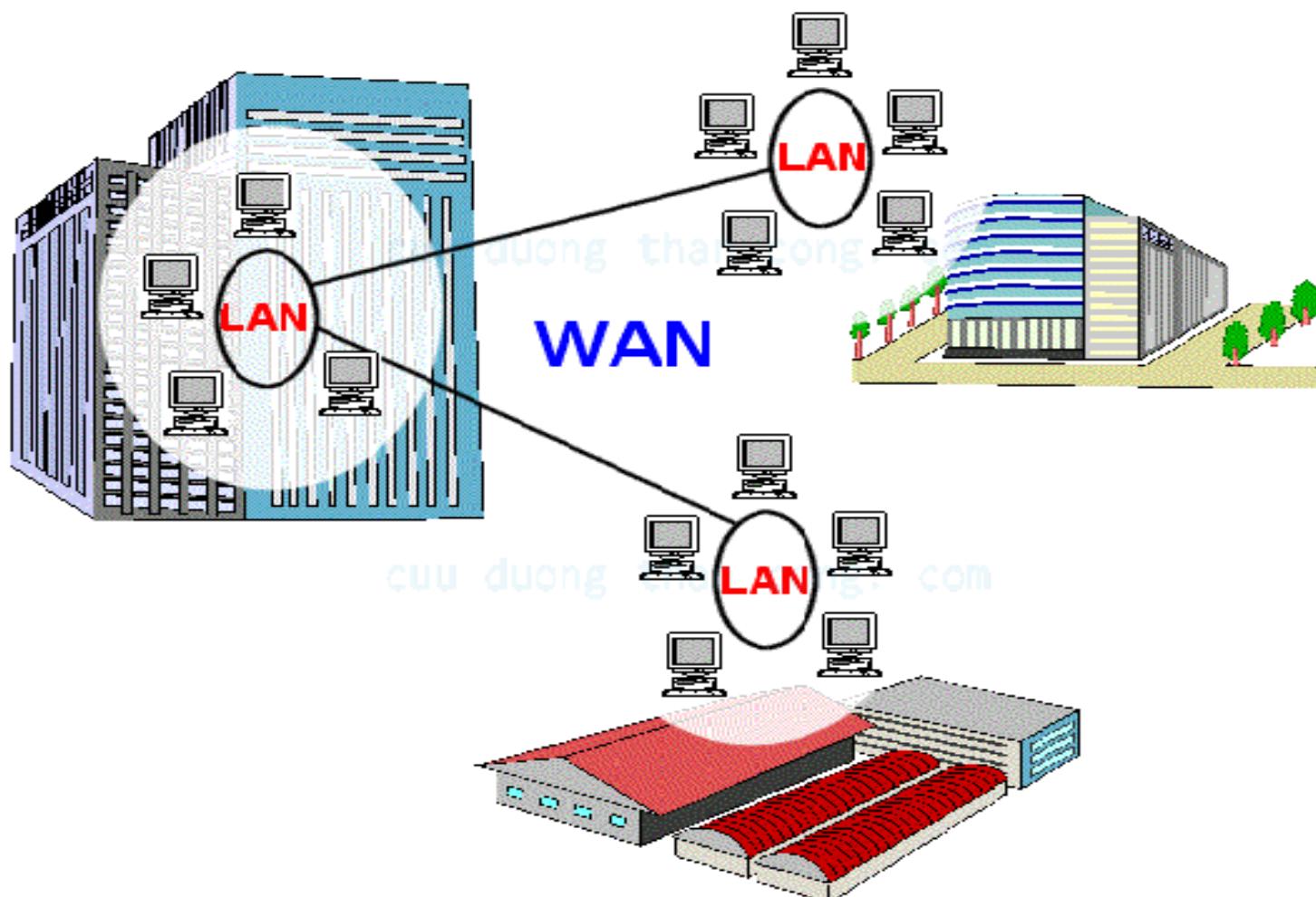
cuuduongthancong.com



WANs (Wide Area Networks)

- Là sự kết nối nhiều LAN
- Không có giới hạn về địa lý
- Tốc độ truyền dữ liệu thấp
- Do nhiều tổ chức quản lý
- Sử dụng các kỹ thuật Modem, ISDN, DSL, Frame Relay, ATM

WANs (Wide Area Networks)



Mạng không dây (Wireless Networking)

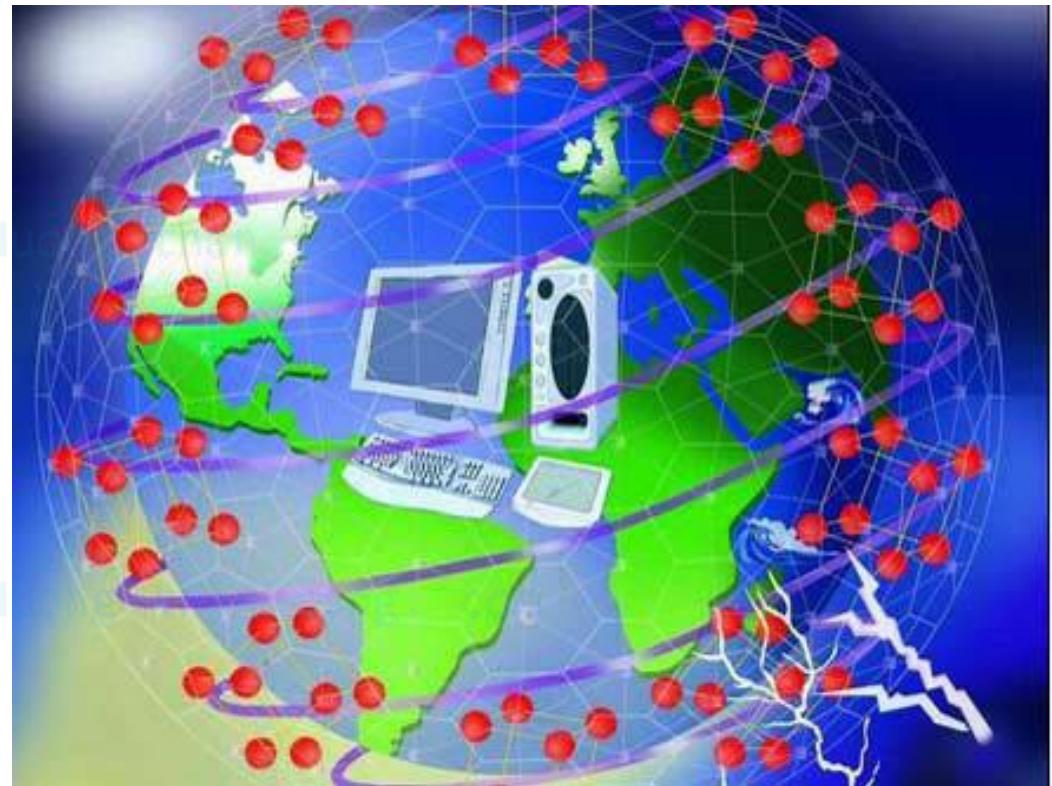
- Do tổ chức IEEE xây dựng và được tổ chức Wi-fi Alliance đưa vào sử dụng trên toàn thế giới.
- Có các tiêu chuẩn: chuẩn 802.11a, chuẩn 802.11b, chuẩn 802.11g (sử dụng phổ biến ở thị trường Việt Nam), chuẩn 802.11n (mới có).
- Thiết bị cho mạng không dây gồm 2 loại: card mạng không dây và bộ tiếp sóng/điểm truy cập (Access Point - AP).

Mạng không dây



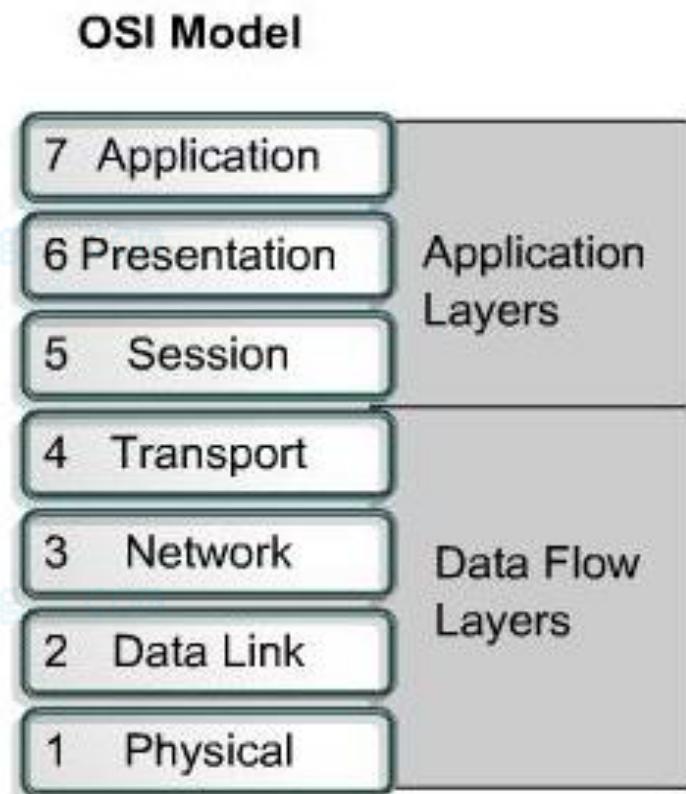
Internet

Một hệ thống mạng của các máy tính được kết nối với nhau qua hệ thống viễn thông trên phạm vi toàn thế giới để trao đổi thông tin.

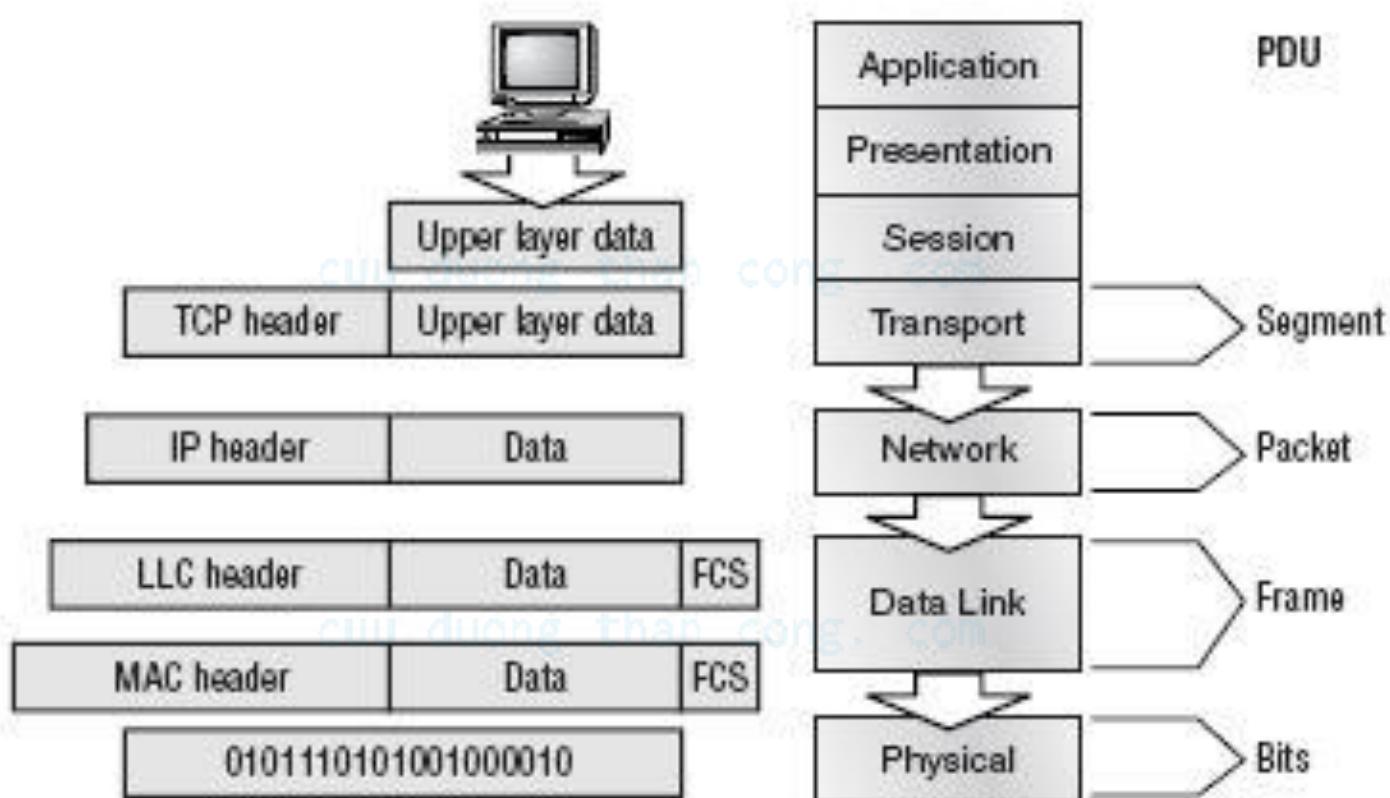


Mô hình OSI (Open Systems Interconnection)

- Lý do hình thành: Sự gia tăng mạnh mẽ về số lượng và kích thước mạng dẫn đến hiện tượng bất tương thích giữa các mạng.
- Ưu điểm của mô hình OSI:
 - Giảm độ phức tạp
 - Chuẩn hóa các giao tiếp
 - Đảm bảo liên kết hoạt động
 - Đơn giản việc dạy và học

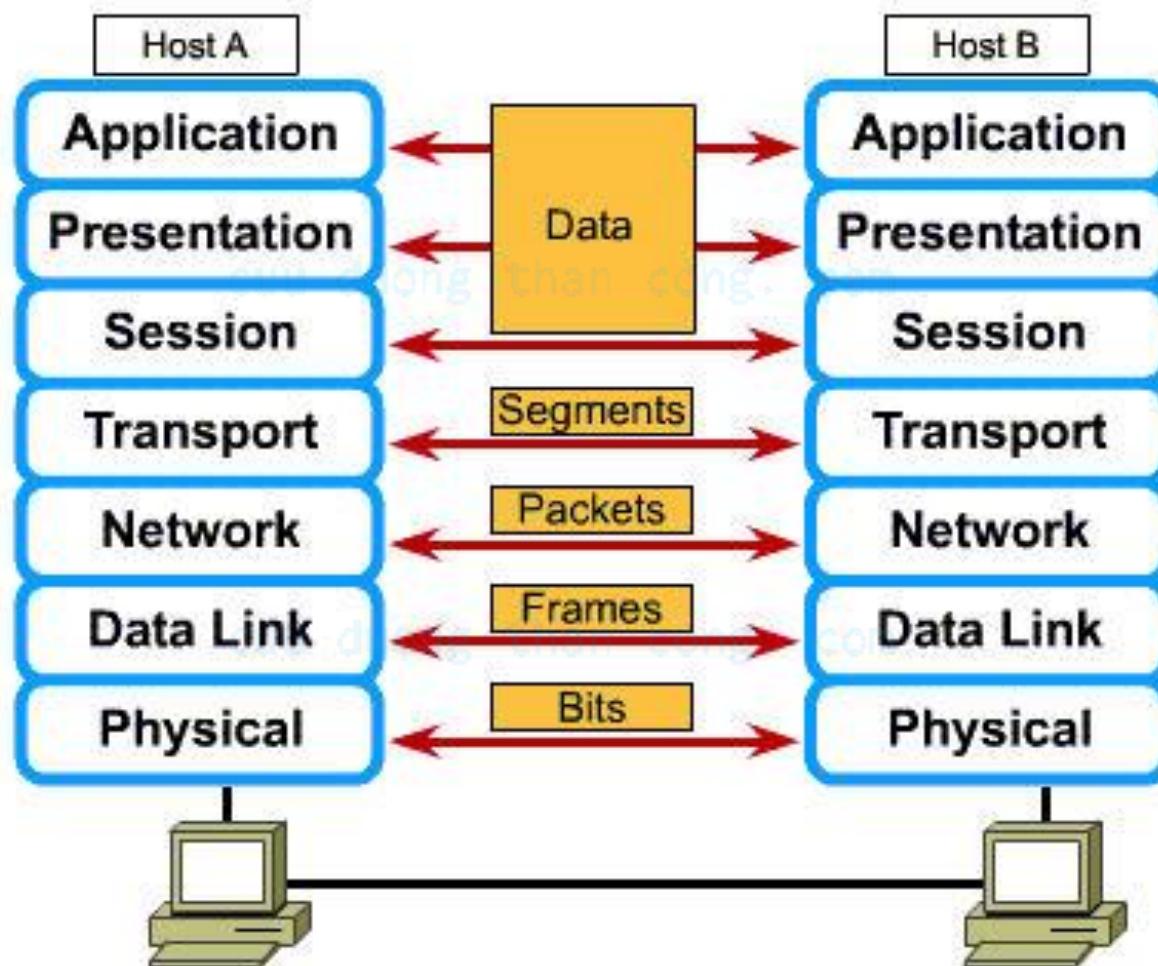


Mô hình OSI

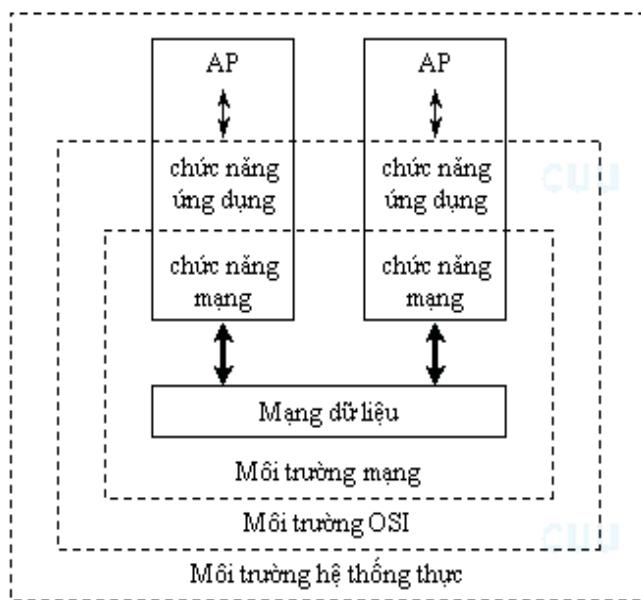


Đóng gói dữ liệu trên mạng

Mô hình OSI



Mô hình OSI



Mô hình OSI



Truyền dẫn nhị phân

- Dây, đầu nối, điện áp
- Tốc độ truyền dữ liệu
- Phương tiện truyền dẫn
- Chế độ truyền dẫn (simplex, half-duplex, full-duplex)

Mô hình OSI



Điều khiển liên kết, truy xuất đường truyền

- Đóng Frame
- Ghi địa chỉ vật lý
- Điều khiển luồng
- Kiểm soát lỗi, thông báo lỗi

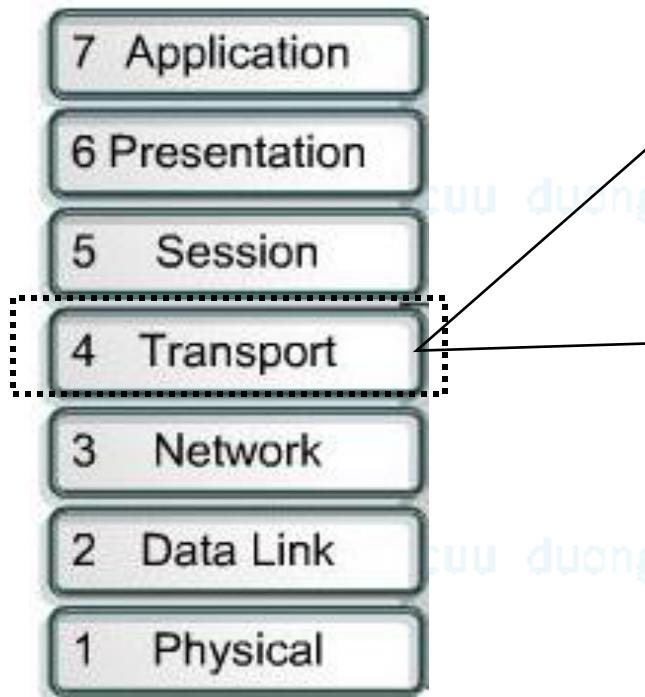
Mô hình OSI



Địa chỉ mạng và xác định đường đi tốt nhất

- Tin cậy
- Địa chỉ luận lý, topo mạng
- Định tuyến (tìm đường đi) cho gói tin

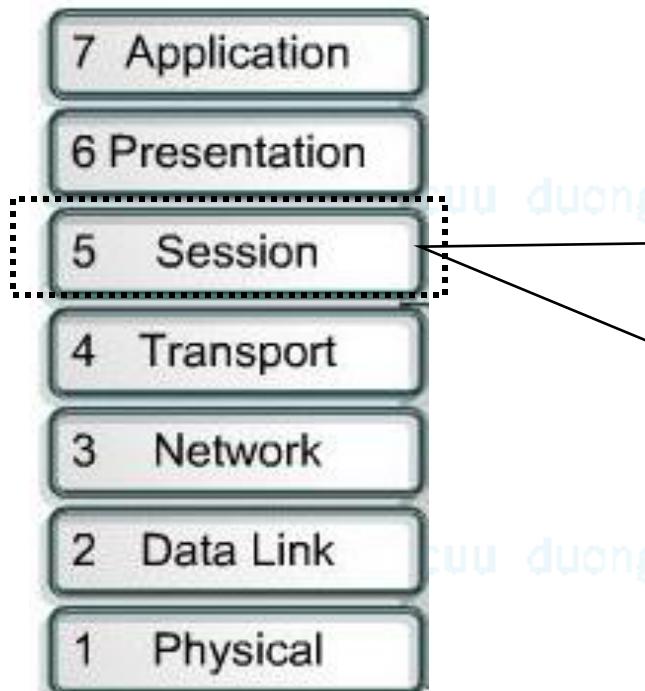
Mô hình OSI



Kết nối end-to-end

- Vận chuyển giữa các host
- Vận chuyển tin cậy
- Thiết lập, duy trì, kết nối các mạch ảo
- Phát hiện lỗi, phục hồi thông tin và điều khiển luồng

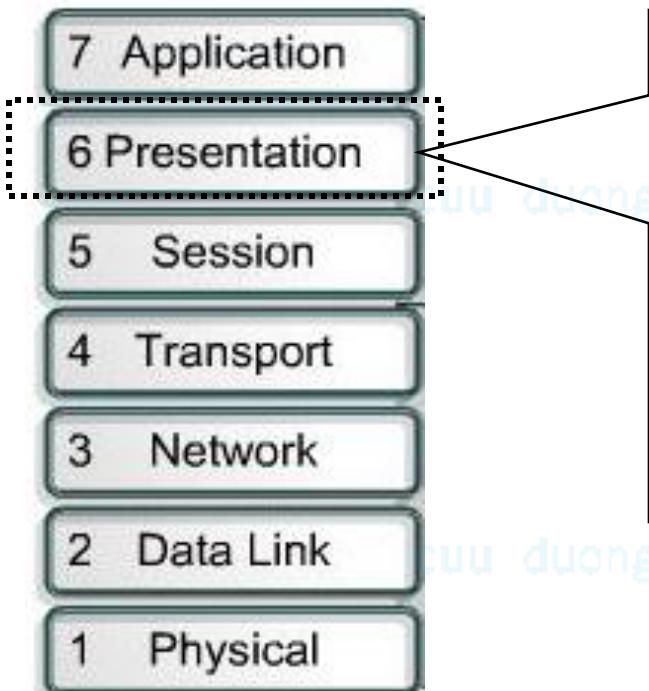
Mô hình OSI



Truyền thông liên host

- Thiết lập, quản lý và kết thúc các phiên giữa các ứng dụng

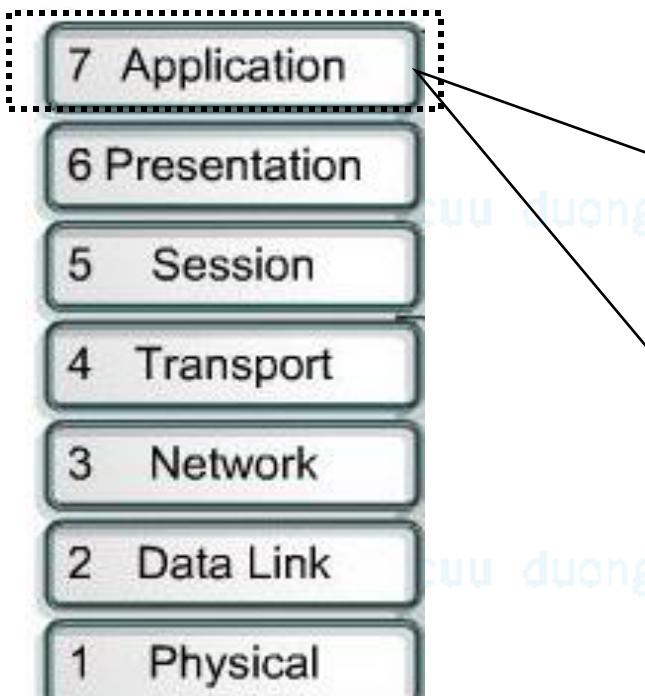
Mô hình OSI



Trình bày dữ liệu

- Định dạng dữ liệu
- Cấu trúc dữ liệu
- Mã hóa
- Nén dữ liệu

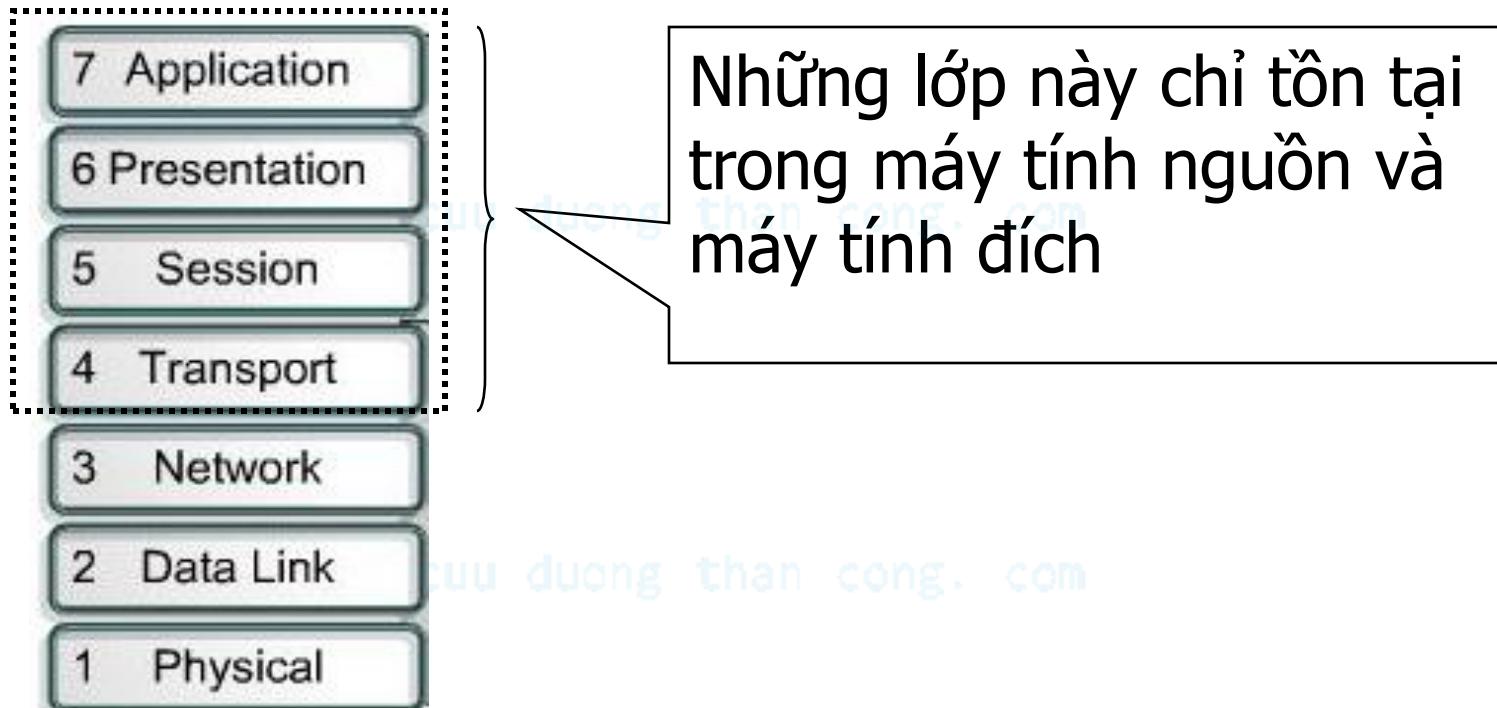
Mô hình OSI



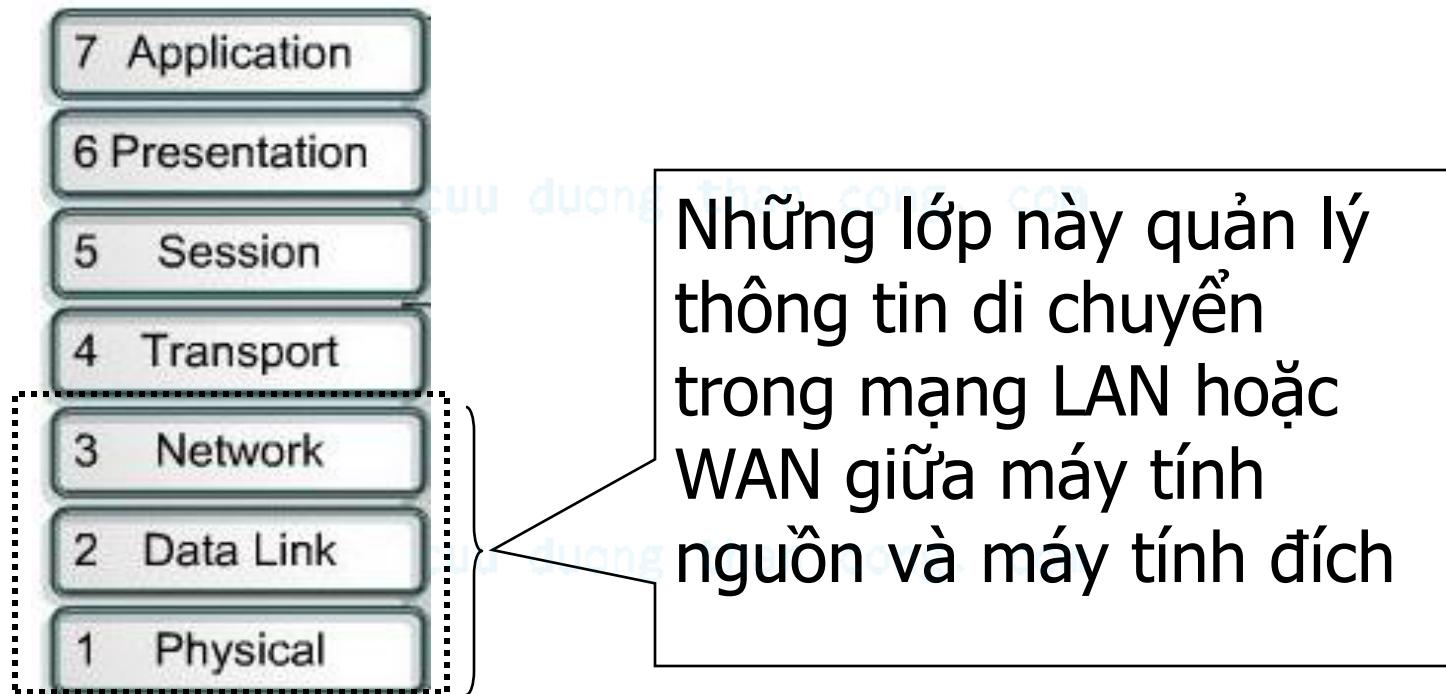
Các quá trình mạng của ứng dụng

- Xác định giao diện giữa người sử dụng và môi trường OSI
- Cung cấp các dịch vụ mạng cho các ứng dụng như email, truyền file...

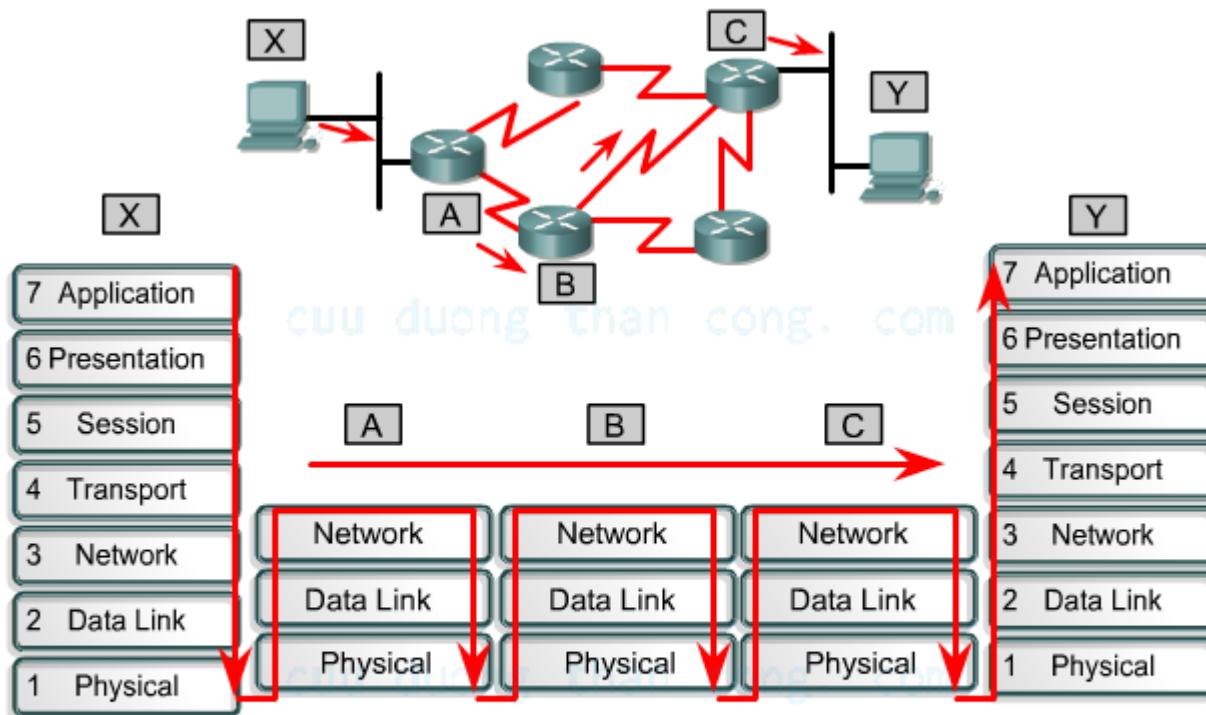
Mô hình OSI



Mô hình OSI



Dòng dữ liệu trên mạng



Data flow in a network focuses on layers one, two and three of the OSI model. This is after being transmitted by the sending host and before arriving at the receiving host.

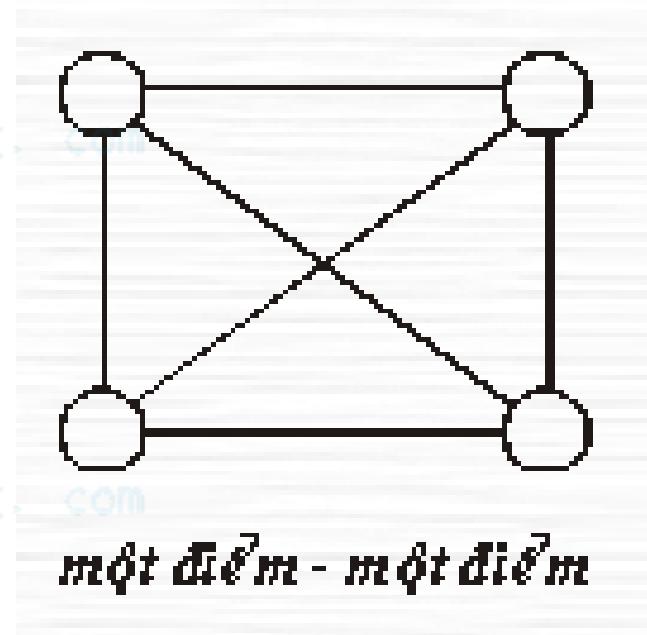
CHƯƠNG 2: CẤU TRÚC MẠNG (TOPOLOGY)

- Phương thức nối mạng
- Cấu trúc vật lý của mạng
- Giao thức truy cập đường truyền trên mạng LAN

cuu duong than cong. com

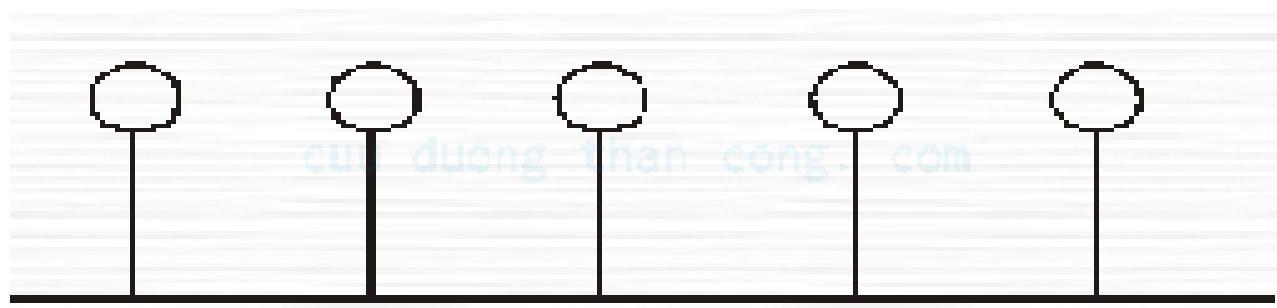
Phương thức nối mạng

- Point-to-point (điểm – điểm): các đường truyền riêng biệt được thiết lập để nối các cặp máy tính lại với nhau.



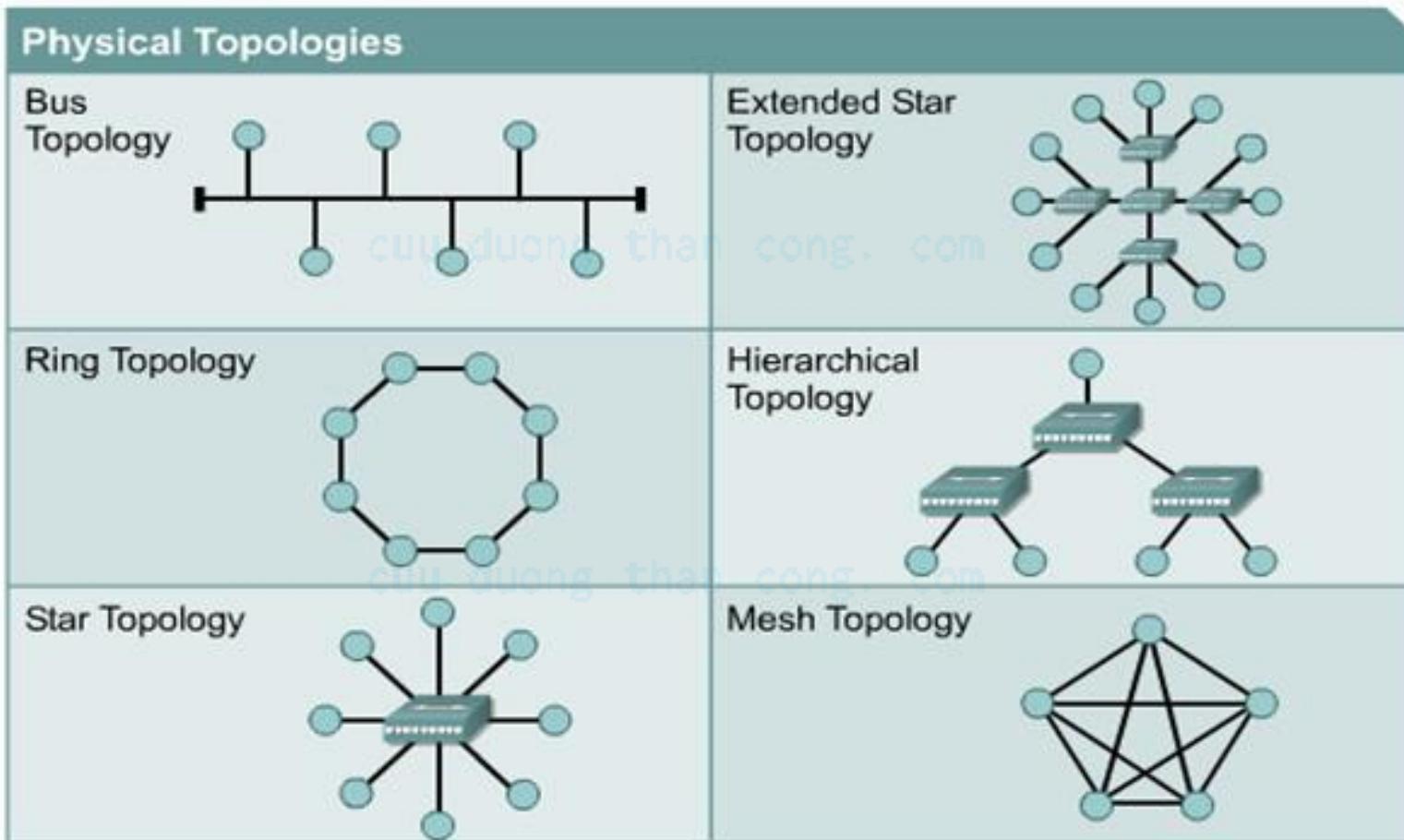
Phương thức nối mạng

- Broadcast (một điểm - nhiều điểm): tất cả các trạm phân chia chung một đường truyền vật lý.



một điểm - nhiều điểm

Cấu trúc vật lý của mạng LAN



Dạng đường thẳng (Bus Topology)

■ Ưu điểm

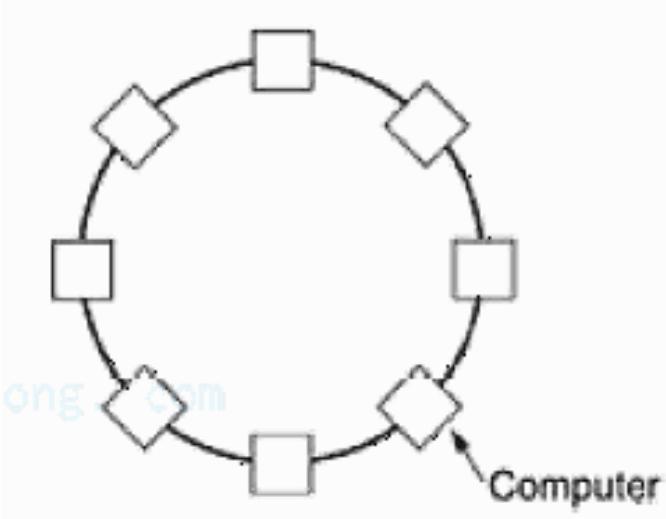
- Dễ dàng cài đặt và mở rộng
- Chi phí thấp
- Một máy hỏng không ảnh hưởng đến các máy khác.

■ Hạn chế

- Khó quản trị và tìm nguyên nhân lỗi
- Giới hạn chiều dài cáp và số lượng máy tính
- Hiệu năng giảm khi có máy tính được thêm vào
- Một đoạn cáp backbone bị đứt sẽ ảnh hưởng đến toàn mạng

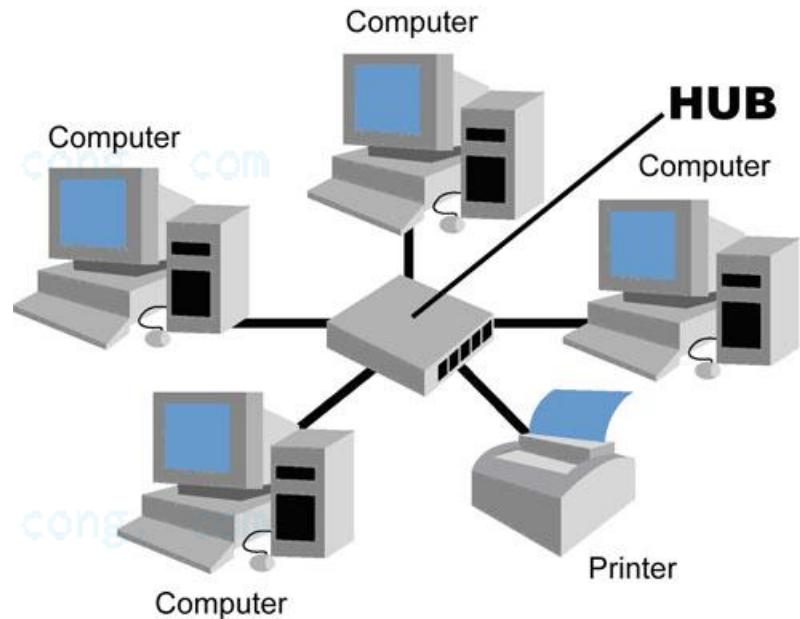
Dạng vòng tròn (Ring Topology)

- **Ưu điểm**
 - Sự phát triển của hệ thống không tác động đáng kể đến hiệu năng
 - Tất cả các máy tính có quyền truy cập nhau
- **Hạn chế**
 - Chi phí thực hiện cao
 - Phức tạp
 - Khi một máy có sự cố thì có thể ảnh hưởng đến các máy tính khác



Dạng hình sao (Star Topology)

- **Ưu điểm**
 - Dễ dàng bổ sung hay loại bỏ một máy tính
 - Dễ dàng theo dõi và giải quyết sự cố
 - Có thể phù hợp với nhiều loại cáp khác nhau
- **Hạn chế**
 - Khi hub không làm việc, toàn mạng cũng sẽ không làm việc
 - Sử dụng nhiều cáp



Giao thức truy cập đường truyền trên mạng LAN

Hai loại giao thức: ngẫu nhiên và có điều khiển

– Ngẫu nhiên

- Giao thức chuyển mạch
- Giao thức đường dây đa truy cập với cảm nhận va chạm

– Có điều khiển

- Giao thức dùng thẻ bài vòng (Token Ring)
- Giao thức dùng thẻ bài cho dạng đường thẳng (Token Bus)

Giao thức truy cập đường truyền trên mạng LAN

- Giao thức chuyển mạch (yêu cầu và chấp nhận)

Khi máy tính yêu cầu, nó sẽ được thâm nhập vào đường cáp nếu mạng không bận, ngược lại sẽ bị từ chối.

cuu duong than cong. com

Giao thức truy cập đường truyền trên mạng LAN

- Giao thức đường dây đa truy cập với cảm nhận va chạm (Carrier Sense Multiple Access/with Collision Detection)
Gói dữ liệu chỉ được gửi nếu đường truyền rảnh, ngược lại mỗi trạm phải đợi theo một trong 3 phương thức:
 - Chờ đợi một thời gian ngẫu nhiên rồi lại bắt đầu kiểm tra đường truyền
 - Kiểm tra đường truyền liên tục cho đến khi đường truyền rảnh ~~đường thanh công.~~ ~~com~~
 - Kiểm tra đường truyền với xác suất p ($0 < p < 1$)

Giao thức truy cập đường truyền trên mạng LAN

- Giao thức dùng thẻ bài vòng (Token Ring)
 - Thẻ bài là một đơn vị dữ liệu đặc biệt có một bit biểu diễn trạng thái bận hoặc rảnh.
 - Thẻ bài chạy vòng quanh trong mạng.
 - Trạm nào nhận được thẻ bài rảnh thì có thể truyền dữ liệu.
- Giao thức dùng thẻ bài cho dạng đường thẳng (Token bus)
 - Tạo ra một vòng logic (vòng ảo) và thực hiện giống Token Ring.

CHƯƠNG 3:

PHƯƠNG TIỆN TRUYỀN DẪN

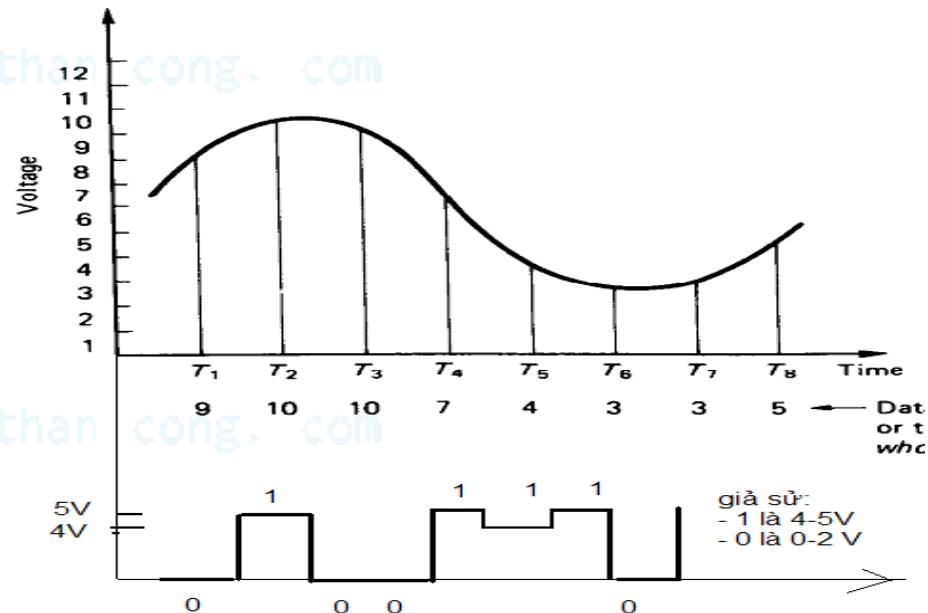
VÀ CÁC THIẾT BỊ LIÊN KẾT MẠNG

- Môi trường truyền dẫn
- Phương tiện truyền dẫn
- Các thiết bị liên kết mạng

cuu duong than cong. com

Môi trường truyền dẫn

- Là phương tiện vật lý cho phép truyền tải tín hiệu giữa các thiết bị.
- Hai loại phương tiện truyền dẫn chính:
 - Hữu tuyến
 - Vô tuyến
- Hệ thống sử dụng hai loại tín hiệu:
 - Digital
 - Analog



Các đặc tính của phương tiện truyền dẫn

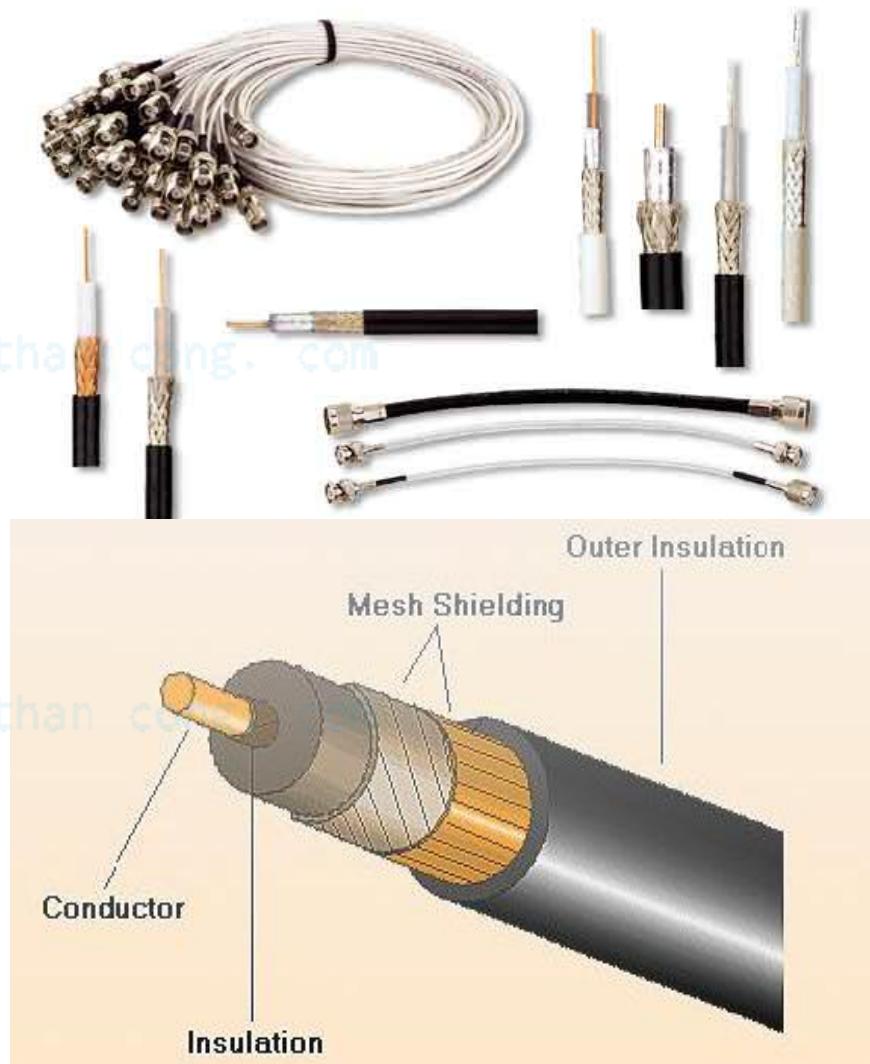
- Chi phí
- Yêu cầu cài đặt
- Băng thông (bandwidth).
- Băng tần (baseband, broadband)
- Độ suy dần (attenuation).
- Nhiễu điện từ (Electromagnetic Interference - EMI)
- Nhiễu xuyên kênh (crosstalk)

Phương tiện truyền dẫn

- Cáp đồng trục
- Cáp xoắn đôi
- Cáp quang
- Wireless

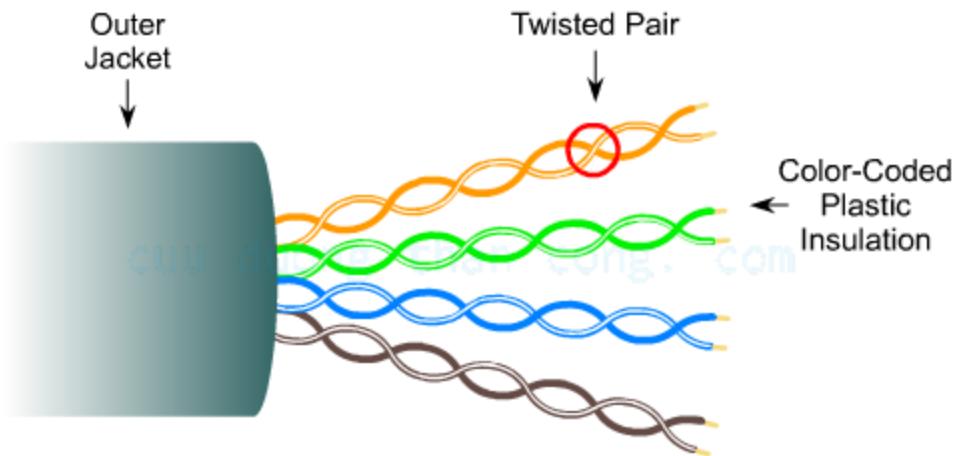
Cáp đồng trục (coaxial)

- Cấu tạo
- Phân loại
 - Thinnet/Thicknet
 - Baseband/
Broadband
- Thông số kỹ thuật
 - Chiều dài cáp
 - Tốc độ truyền
 - Nhiễu
 - Lắp đặt/bảo trì
 - Giá thành
 - Kết nối



Cáp xoắn đôi

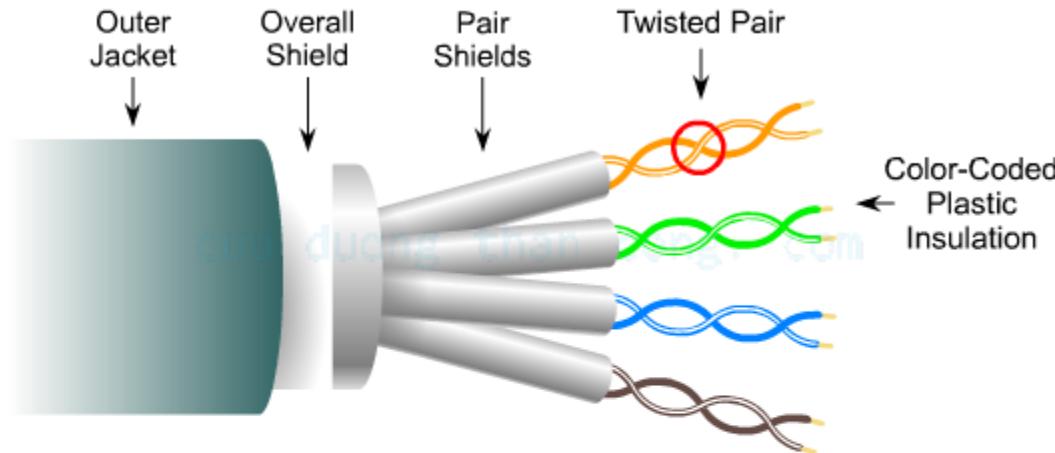
Unshielded Twisted Pair (UTP) Cable



- Speed and throughput: 10 - 100 - 1000 Mbps (depending on the quality/category of cable)
- Average \$ per node: Least Expensive
- Media and connector size: Small
- Maximum cable length: 100m

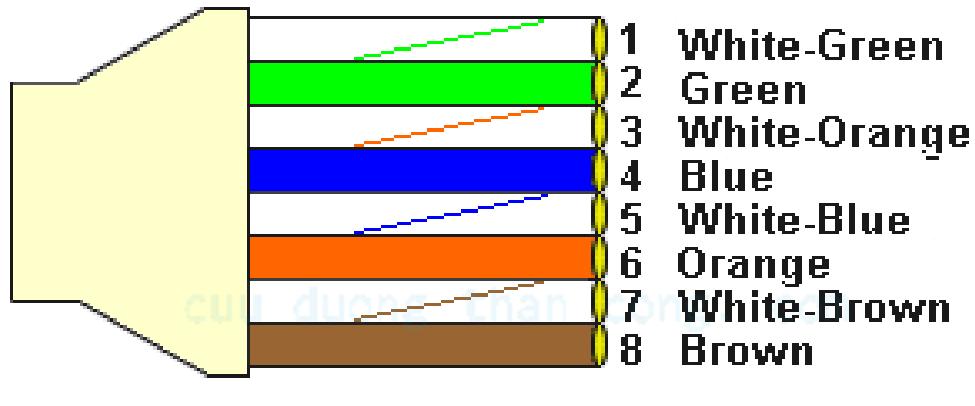
Cáp xoắn đôi

Shielded Twisted Pair (STP) Cable

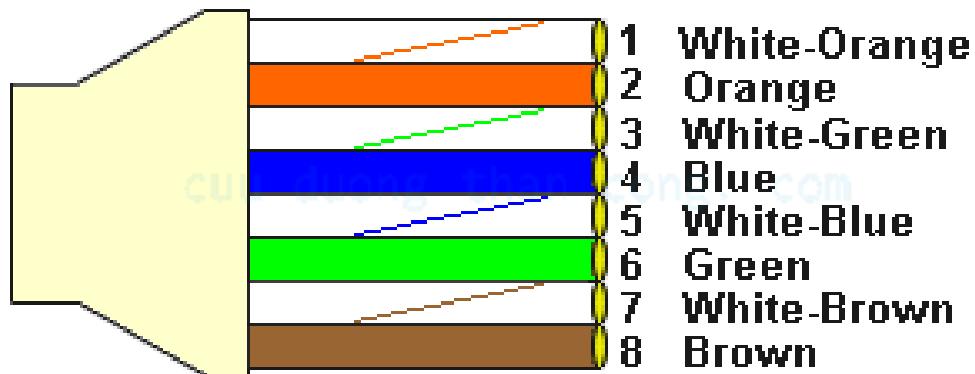


- Speed and throughput: 10 - 100 Mbps
- Average \$ per node: Moderately Expensive
- Media and connector size: Medium to Large
- Maximum cable length: 100m

Chuẩn cáp 568A & 568B

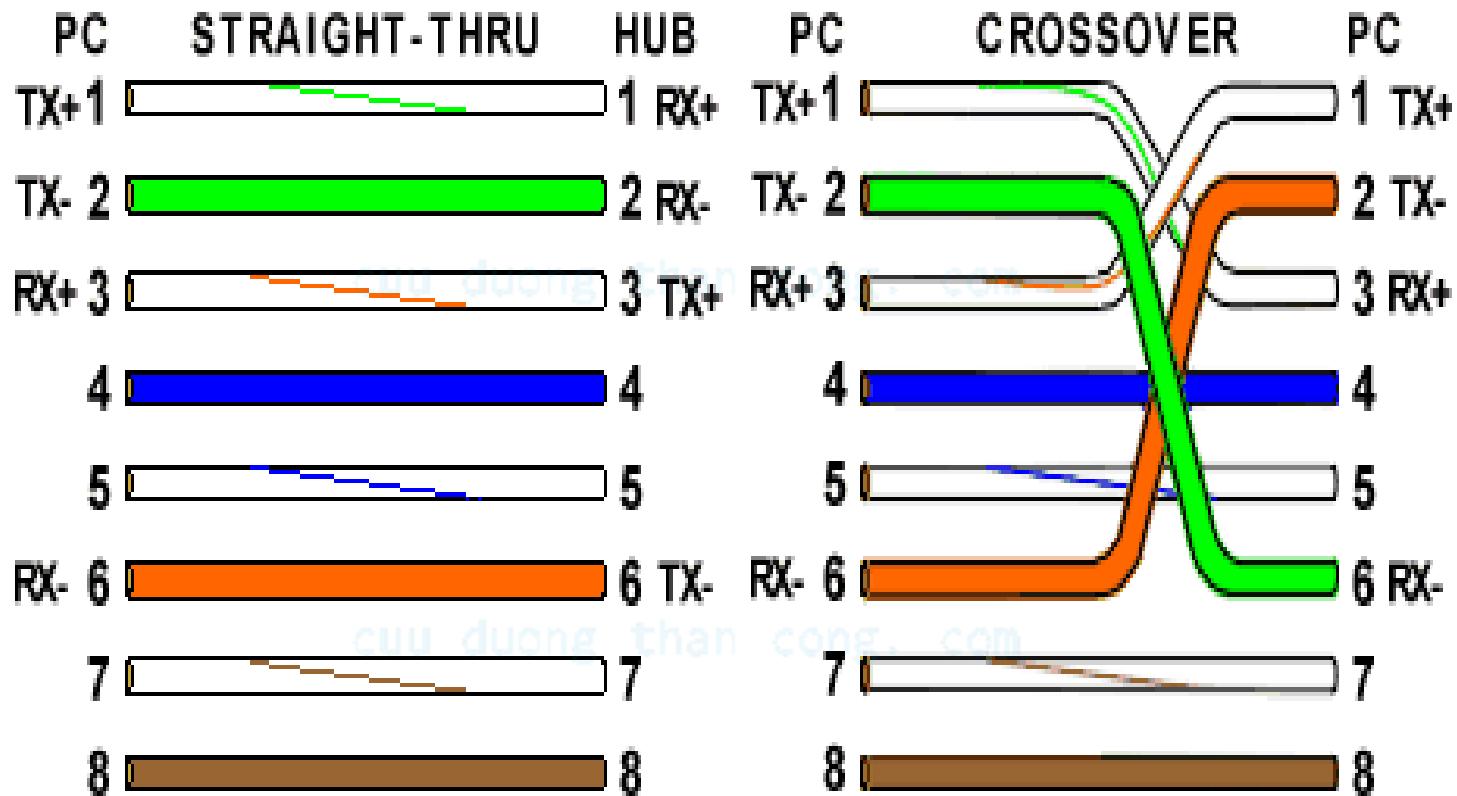


568A CABLE END



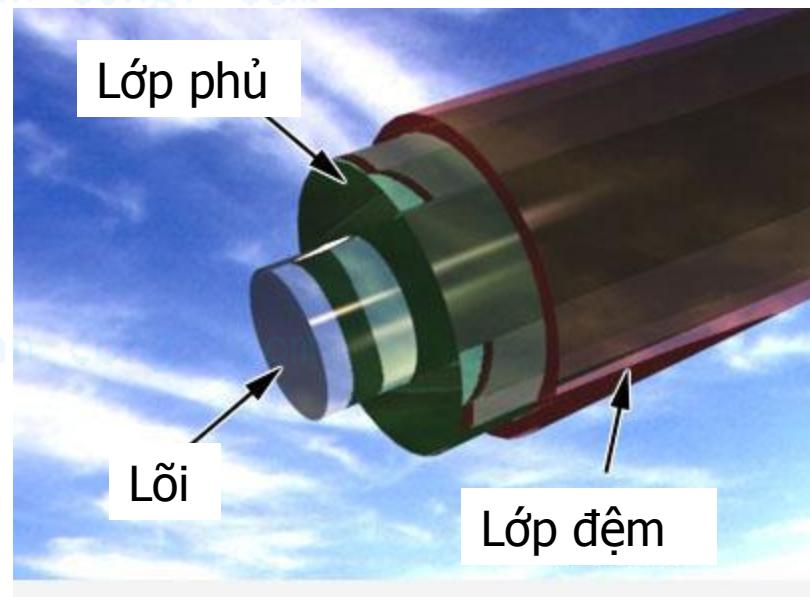
568B CABLE END

Phương thức bấm Cáp



Cáp quang (Fiber optic)

- Thành phần & cấu tạo
 - Dây dẫn
 - Nguồn sáng (LED, Laser)
 - Đầu phát hiện (Photodiode, photo transistor)
- Phân loại
 - Multimode stepped index
 - Multimode graded index
 - Single mode (mono mode)
- Thông số kỹ thuật
 - Chiều dài cáp
 - Tốc độ truyền
 - Nhiễu
 - Lắp đặt/bảo trì
 - Giá thành
 - Kết nối

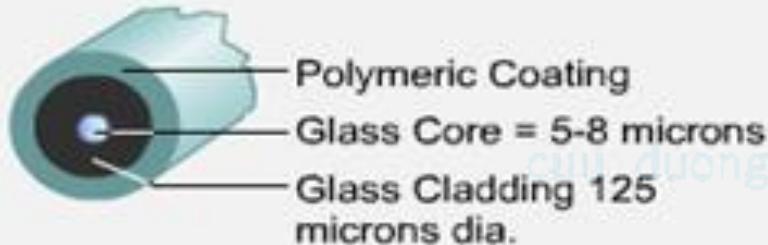


Cáp quang (Fiber optic)

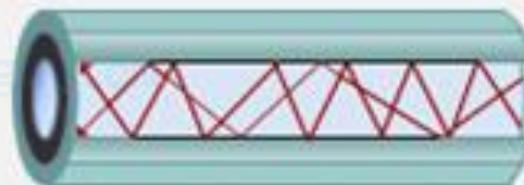
Single-mode



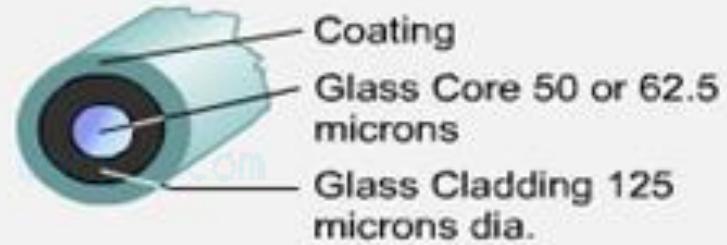
Requires very straight path



Multimode



Multiple paths-sloppy

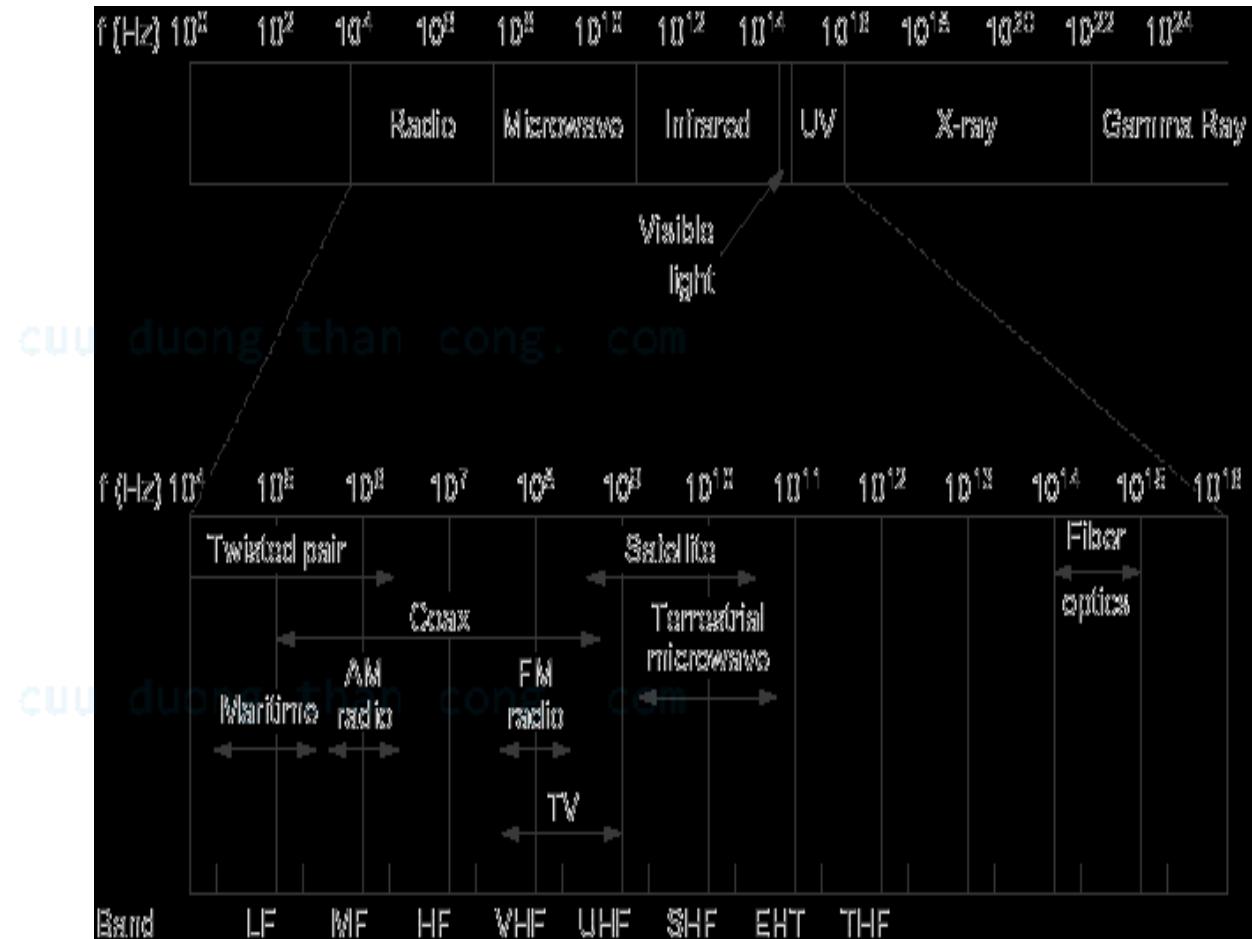


Thông số cơ bản của các loại cáp

Cáp	Chiều dài cáp tối đa	Tốc độ truyền	Lắp đặt	Nhiều	Giá thành
UTP	100 m	10-100 Mbps	Dễ	Cao	Thấp nhất
STP	100 m	16-500 Mbps	Khá dễ	Thấp	Vừa phải
Thinnet	185 m	10 Mbps	Dễ	Thấp	Thấp
Thicknet	500 m	10 Mbps	Khó	Thấp	Cao
Fiber optics	2000 m	2 Gbps	Khó	Không	Đắt

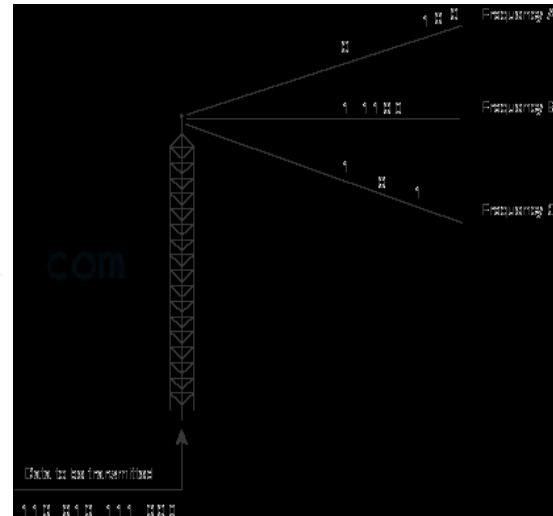
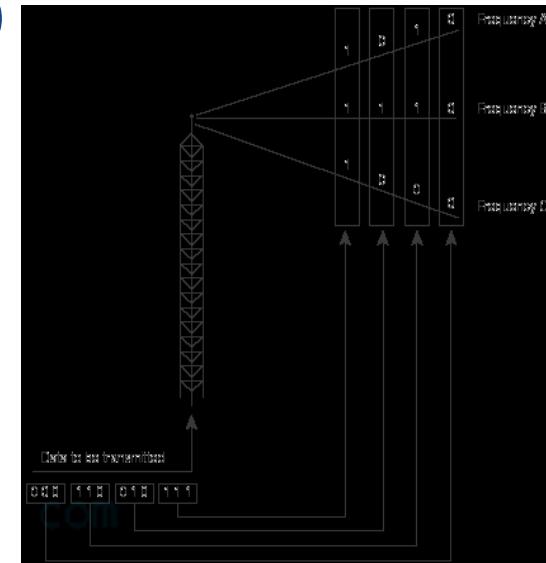
Wireless

- Wireless?
- Các kỹ thuật
 - Radio
 - Microwave
 - Infrared
 - Lightwave



Radio

- Đặc điểm
 - Tần số
 - Thiết bị: antenna, transceiver
- Phân loại
 - Single-Frequency
 - Low power
 - High power
 - Spread-Spectrum
 - Direct-sequence modulation
 - Frequency-hopping



Microwave (sóng cực ngắn)

- **Đặc điểm**
- **Phân loại**
 - Terrestrial Microwave
 - Satellite Microwave
- **Thông số**

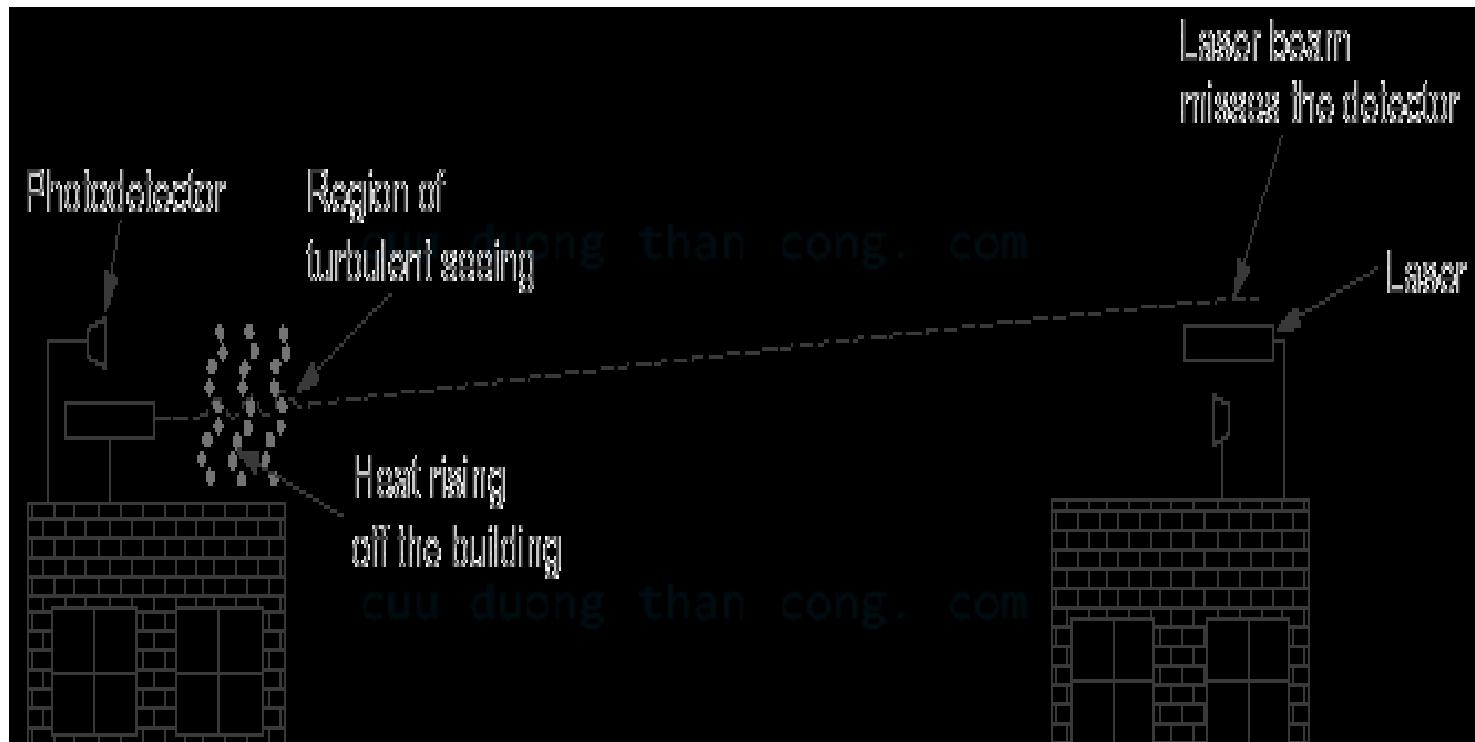
	Terrestrial Microwave	Satellite Microwave
Tần số	4-6 GHz, 21-23 GHz	11-14 GHz
Khoảng cách tối đa	Phụ thuộc công suất và tần số phát (có thể vài chục km)	Toàn cầu
Tốc độ truyền	1 - 10 Mbps	1 - 10 Mbps
Lắp đặt / bảo trì	Khá khó	Khó
Nhiều	Phụ thuộc thiết bị, thời tiết ...	Phụ thuộc thiết bị, thời tiết ...
Giá	Khá cao	Rất cao
Bảo mật	Thấp (thường được mã hoá)	Thấp (thường được mã hoá)

Infrared (Sóng hồng ngoại)

- Đặc điểm
- Phân loại
 - Point-to-point Infrared
 - Broadcast Infrared
- Thông số

	Point-to-point Infrared	Broadcast Microwave
Tần số	100-1000 GHz	100 GHz - 1000 THz
Khoảng cách tối đa	Có thể vài km	Vài chục mét
Tốc độ truyền	100 Kbps - 16 Mbps	Nhỏ hơn 1 Mbps
Lắp đặt / bảo trì	Vừa phải	Dễ
Nhiều	Chống nhiễu điện, bị nhiễu ánh sáng	Chống nhiễu điện, bị nhiễu ánh sáng
Giá	Tùy thuộc thiết bị	Không cao
Bảo mật	Cao (do line-of-sight và độ dài sáng hẹp)	Thấp

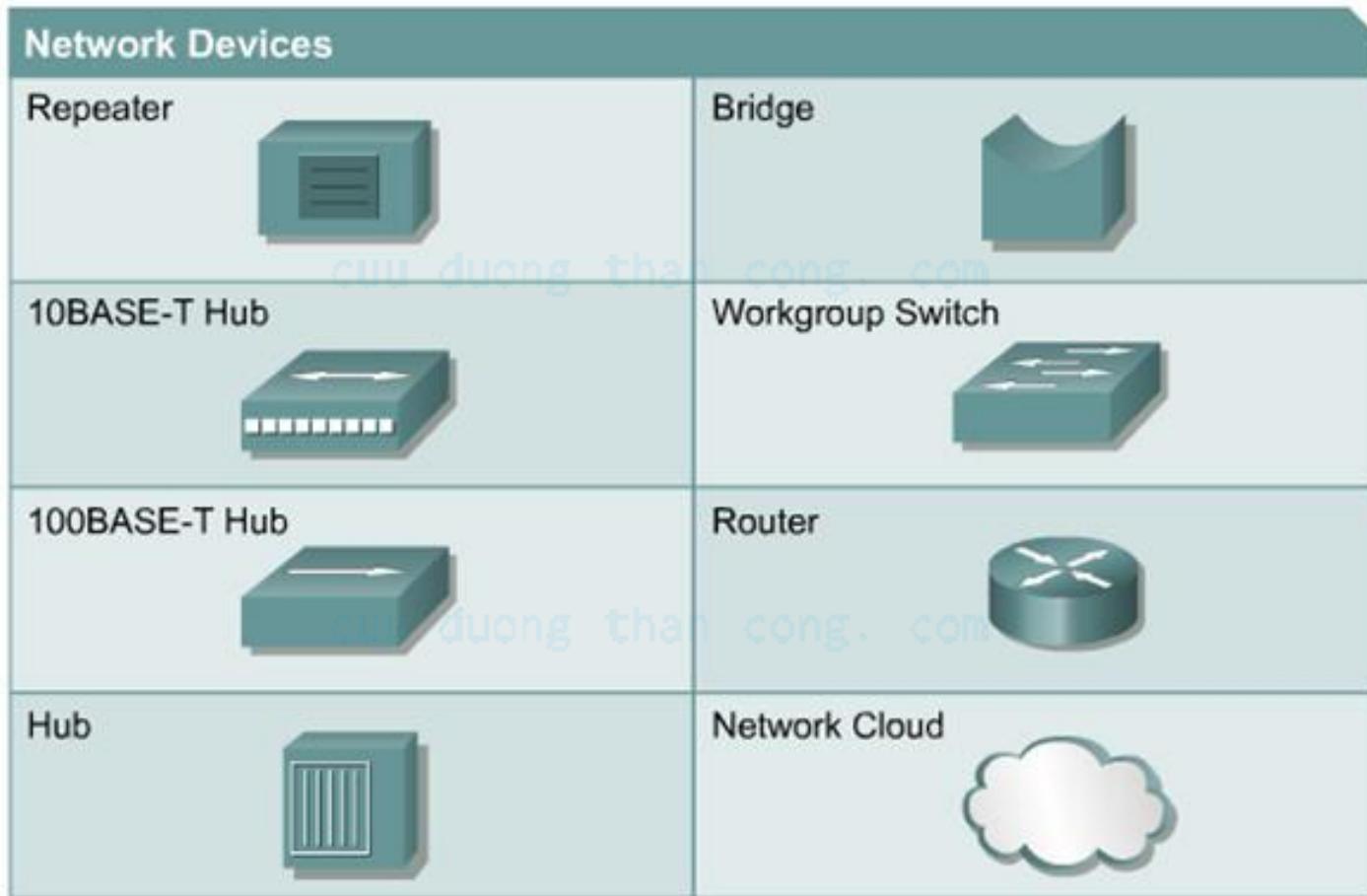
Lightwave



Các thiết bị liên kết mạng

- Card mạng (Network Interface Card - NIC)
- Modem
- Repeater (Bộ chuyển tiếp)
- Hub (Bộ tập trung)
- Bridge (Cầu nối)
- Switch (Bộ chuyển mạch)
- Router (Bộ định tuyến)
- Gateway (Cổng nối)

Biểu diễn của các thiết bị mạng trong sơ đồ mạng



Card mạng

- Kết nối giữa máy tính và cáp mạng để phát hoặc nhận dữ liệu với các máy tính khác thông qua mạng.
- Kiểm soát luồng dữ liệu giữa máy tính và hệ thống cáp.
- Mỗi NIC (Network Interface Adapter Card) có một mã duy nhất gọi là địa chỉ MAC (Media Access Control). MAC address có 6 byte, 3 byte đầu là mã số nhà sản xuất, 3 byte sau là số serial của card.

Cards

Organizational Unique Identifier (OUI)	Vendor Assigned (NIC Cards, Interfaces)
24 bits	24 bits
6 hex digits	6 hex digits
00 60 2F	3A 07 BC
Cisco	particular device

Internal network interface card



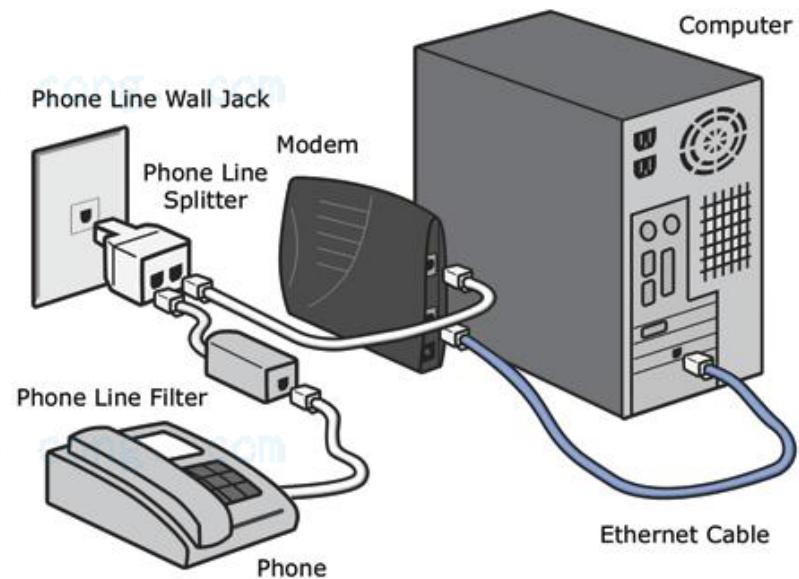
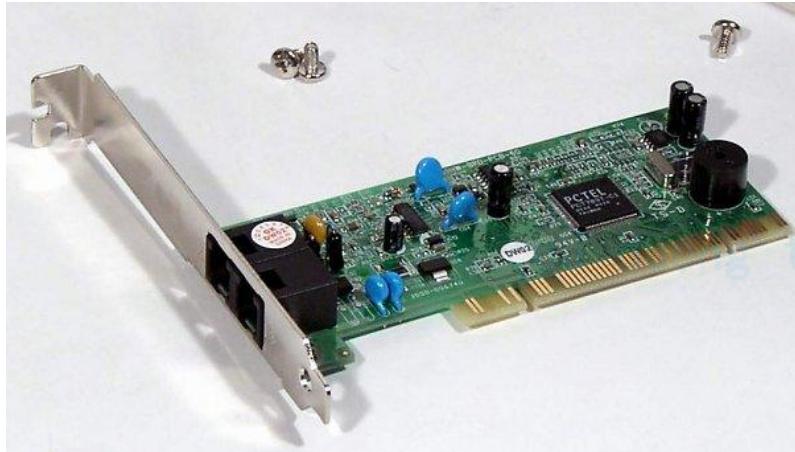
PCMCIA Network interface card



Modem

- Là tên viết tắt của hai từ điều chế (MOdulation) và giải điều chế (DEModulation).
- Điều chế tín hiệu số (Digital) sang tín hiệu tương tự (Analog) để gởi theo đường điện thoại và ngược lại.
- Có 2 loại là Internal và External.

Modem

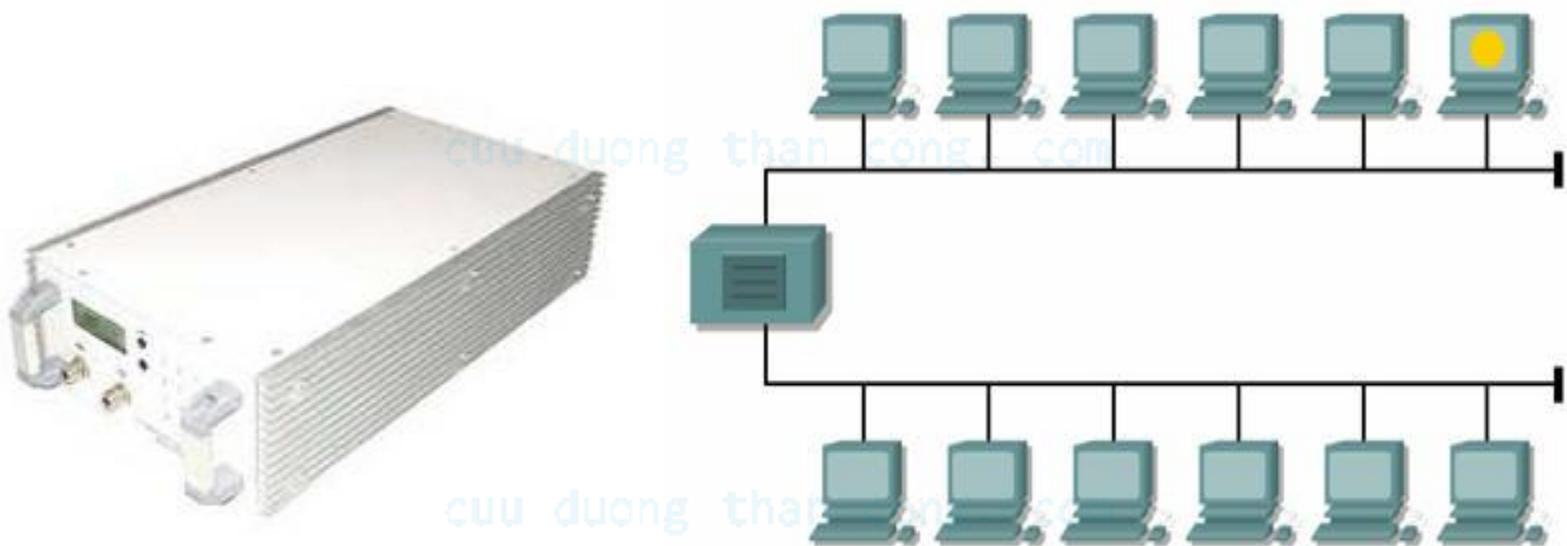


Repeater (bộ chuyển tiếp)

- Khuếch đại, phục hồi các tín hiệu đã bị suy thoái do tổn thất năng lượng trong khi truyền.
- Cho phép mở rộng mạng vượt xa chiều dài giới hạn của một môi trường truyền.
- Chỉ được dùng nối hai mạng có cùng giao thức truyền thông.
- Hoạt động ở lớp Physical.

cuu duong than cong. com

Repeater (bộ chuyển tiếp)



Hub (bộ tập trung)

- Chức năng như Repeater nhưng mở rộng hơn với nhiều đầu cắm các đầu cáp mạng.
- Tạo ra điểm kết nối tập trung để nối mạng theo kiểu hình sao. [cuuduongthancong.com](#)
- Tín hiệu được phân phối đến tất cả các kết nối.
- Có 3 loại Hub: thụ động, chủ động, thông minh.

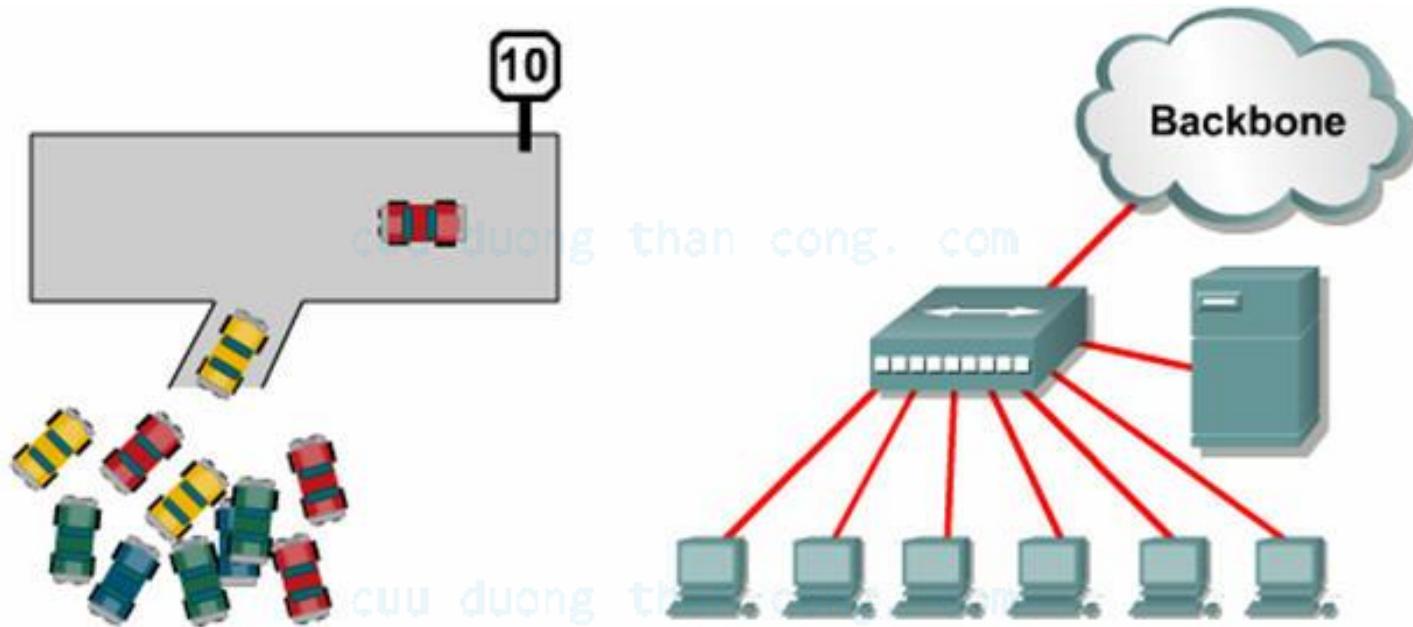
[cuuduongthancong.com](#)

Hub (bộ tập trung)

- Hub thụ động (Passive Hub): chỉ đảm bảo chức năng kết nối, không xử lý lại tín hiệu.
- Hub chủ động (Active Hub): có khả năng khuếch đại tín hiệu để chống suy hao.
- Hub thông minh (Intelligent Hub): là Hub chủ động nhưng có thêm khả năng tạo ra các gói tin thông báo hoạt động của mình giúp cho việc quản trị mạng dễ dàng hơn.



Hub (bộ tập trung)



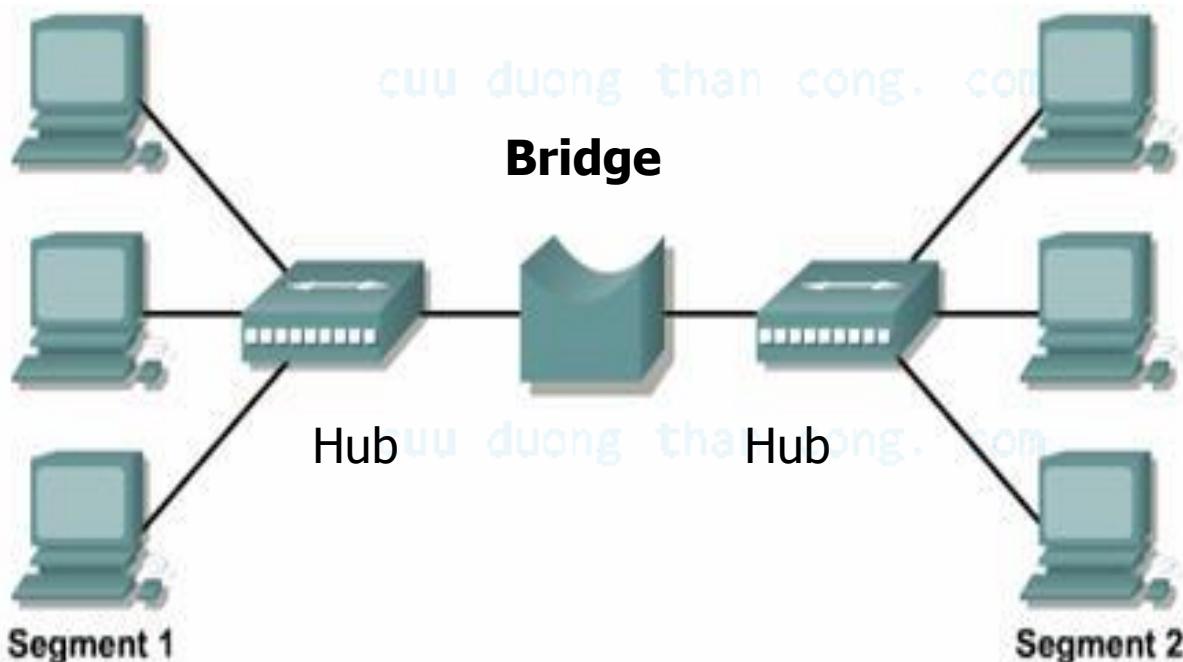
One device sending
at a time

Each node shares 10 Mbps

Bridge (cầu nối)

- Dùng để nối 2 mạng có giao thức giống hoặc khác nhau.
- Chia mạng thành nhiều phân đoạn nhằm giảm lưu lượng trên mạng.
- Hoạt động ở lớp Data Link với 2 chức năng chính là lọc và chuyển vận.
- Dựa trên bảng địa chỉ MAC lưu trữ, Bridge kiểm tra các gói tin và xử lý chúng trước khi có quyết định chuyển đi hay không.

Bridge (cầu nối)



cuuduongthancong.com

Bridge

Hub cuuduongthancong.com

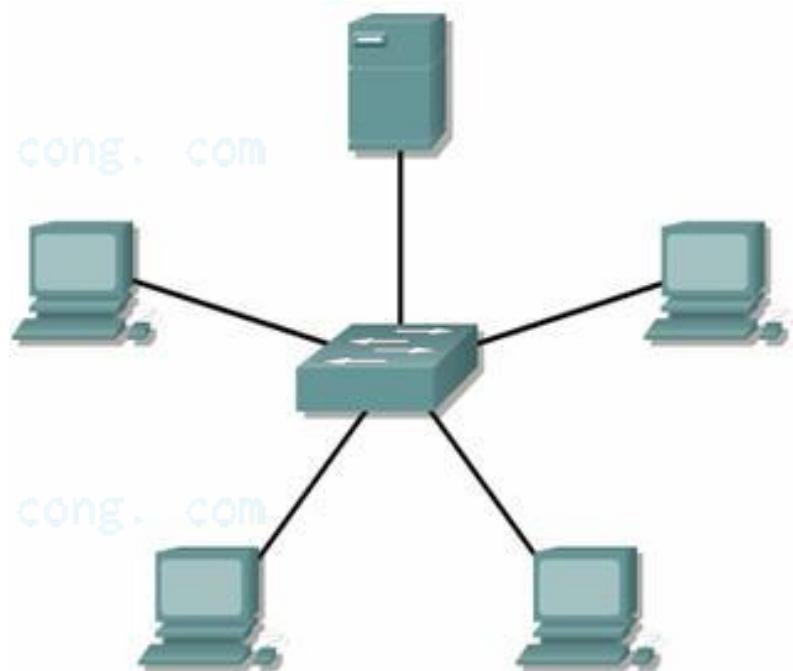
Segment 1

Segment 2

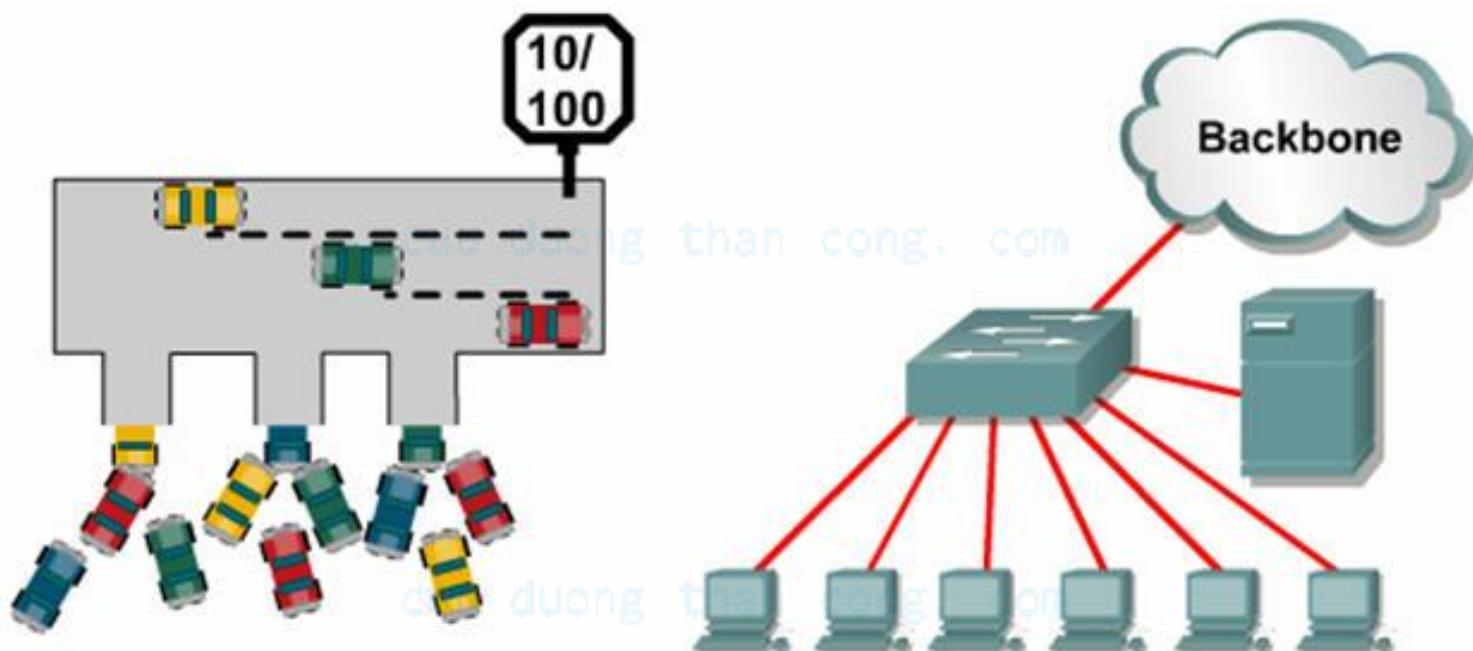
Switch (bộ chuyển mạch)

- Là thiết bị giống Bridge và Hub cộng lại nhưng thông minh hơn.
- Có khả năng chỉ chuyển dữ liệu đến đúng kết nối thực sự cần dữ liệu này làm giảm dung độ trên mạng.
- Dùng để phân đoạn mạng trong các mạng cục bộ lớn (VLAN).
- Hoạt động ở lớp Data Link.

Switch (bộ chuyển mạch)



Switch (bộ chuyển mạch)



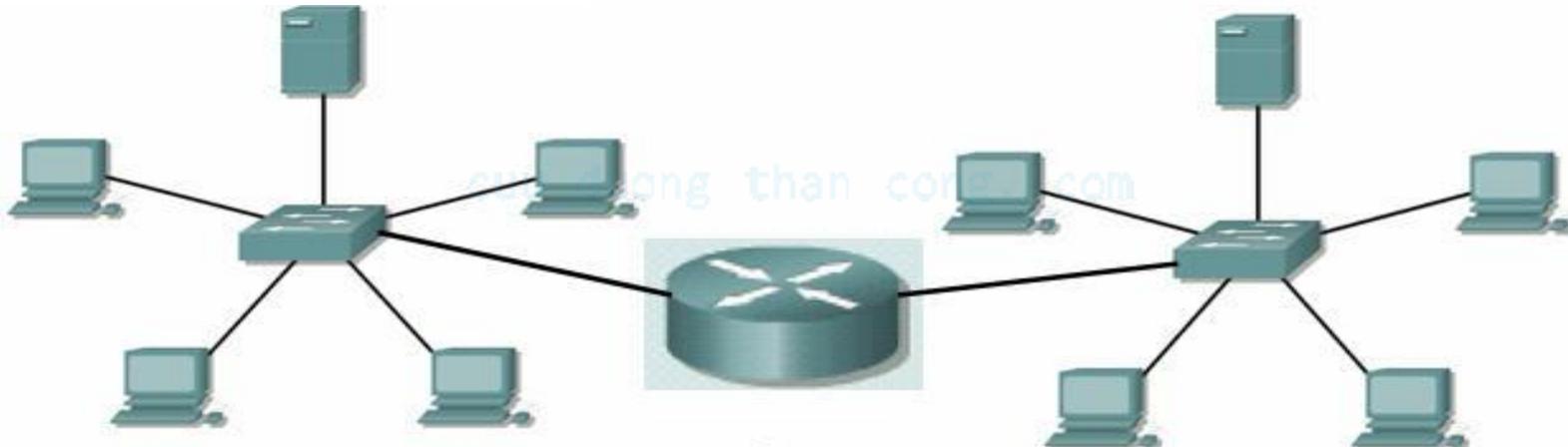
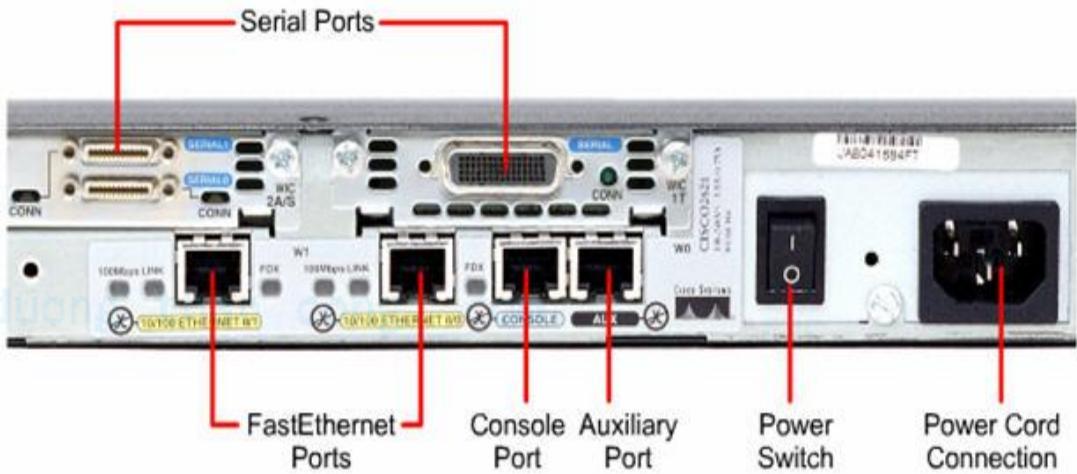
Multiple devices sending
at the same time

Each node has 10/100 Mbps

Router (Bộ định tuyến)

- Dùng để ghép nối các mạng cục bộ lại với nhau thành mạng rộng.
- Lựa chọn đường đi tốt nhất cho các gói tin hướng ra mạng bên ngoài.
- Hoạt động chủ yếu ở lớp Network.
- Có 2 phương thức định tuyến chính:
 - Định tuyến tĩnh: cấu hình các đường cố định và cài đặt các đường đi này vào bảng định tuyến.
 - Định tuyến động:
 - Vectơ khoảng cách: RIP, IGRP, EIGRP, BGP
 - Trạng thái đường liên kết: OSPF

Router (Bộ định tuyến)



Gateway (Proxy - cỗng nối)

- Thường dùng để kết nối các mạng không thuần nhất, chủ yếu là mạng LAN với mạng lớn bên ngoài chứ không dùng kết nối LAN – LAN.
- Kiểm soát luồng dữ liệu ra vào mạng.
- Hoạt động phức tạp và chậm hơn Router.
- Hoạt động từ tầng thứ 4→7



CHƯƠNG 4: DATA LINK

- Điều khiển luồng (dòng)
- Phát hiện lỗi
- Xử lý lỗi

cuu duong than cong. com

Điều khiển luồng

- Là kỹ thuật nhằm đảm bảo rằng bên phát không làm tràn dữ liệu bên nhận
- Hai phương pháp được sử dụng:
 - Phương pháp dừng và chờ (Stop and Wait)
 - Đơn giản nhất,
 - Kém hiệu quả, chỉ có một khung tin được truyền tại một thời điểm
 - Phương pháp cửa sổ trượt –(Sliding Window Flow Control)

Phương pháp dừng và chờ

- Truyền một gói tin và chờ báo nhận
 - Bên phát truyền một khung tin
 - Sau khi nhận được khung tin, bên nhận gửi lại xác nhận
 - Bên phát phải đợi đến khi nhận được xác nhận thì mới truyền khung tin tiếp theo
- Không hiệu quả
 - Bên nhận có thể dừng quá trình truyền bằng cách không gửi khung tin xác nhận
 - Tại một thời điểm chỉ có một khung tin trên đường truyền → chậm
 - Trường hợp độ rộng của kênh truyền lớn hơn độ rộng của khung tin thì nó tỏ ra cực kỳ kém hiệu quả.

Phương pháp cửa sổ trượt

- Cho phép nhiều khung tin được truyền tại một thời điểm -> Truyền thông hiệu quả hơn.
- A và B được kết nối trực tiếp song công (full-duplex).
- B có bộ đệm cho n khung tin -> B có thể chấp nhận n khung tin, A có thể truyền n khung tin mà không cần đợi xác nhận từ bên B
- Mỗi khung tin được gán nhãn bởi một số thứ tự.
- B xác nhận khung tin đã được nhận bằng cách gửi xác nhận cùng với số thứ tự của khung tin tiếp theo mà nó mong muốn nhận

Phương pháp cửa sổ trượt

- A duy trì danh sách các số thứ tự được phép gửi
- B duy trì danh sách số thứ tự chuẩn bị nhận
 - Gọi là cửa sổ của các khung tin
 - Điều khiển dòng cửa sổ trượt

Phương pháp cửa sổ trượt

- Đối với đường truyền 2 chiều thì mỗi bên phải sử dụng hai cửa sổ:
 - Một cho phát và một cho nhận
 - Mỗi bên đều phải gửi dữ liệu và gửi xác nhận tới bên kia
- Số thứ tự được lưu trữ trong khung tin
 - Bị giới hạn, trường k bit thì số thứ tự được đánh số theo Module của 2^k
 - Kích thước của cửa sổ không nhất thiết phải lấy là maximum (ví dụ trường 3 bit, có thể lấy độ dài cửa sổ là 4)

Phát hiện lỗi

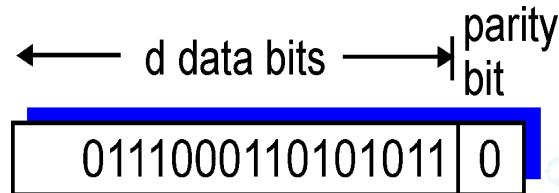
- Lý do một hay nhiều bit thay đổi trong khung tin được truyền:
 - Tín hiệu trên đường truyền bị suy yếu
 - Tốc độ truyền thanh công. com
 - Mất đồng bộ
- Việc phát hiện ra lỗi để khắc phục, yêu cầu phát lại là cần thiết và vô cùng quan trọng trong truyền dữ liệu.

Phát hiện lỗi: Parity Check

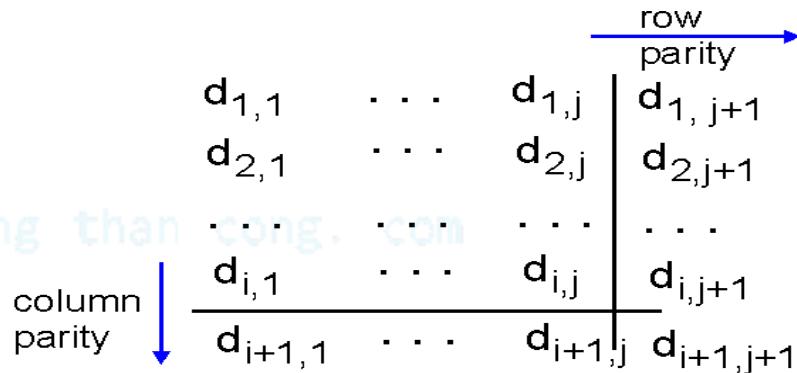
- Là kỹ thuật đơn giản nhất.
- Đưa một bit kiểm tra tính chẵn lẻ vào sau khối tin.
- Giá trị của bit này được xác định dựa trên số các số 1 là chẵn (even parity), hoặc số các số 1 là lẻ (odd parity).
- Lỗi sẽ không bị phát hiện nếu trong khung tin có 2 hoặc một số chẵn các bit bị đảo.
- Không hiệu quả khi xung nhiễu đủ mạnh.

Kiểm tra Parity

Bit Parity đơn:
phát hiện các lỗi bit



Bit Parity 2 chiều:
phát hiện & sửa các lỗi bit



Two examples of a 5x5 matrix of bits:

1	0	1	0	1	1
1	1	1	1	0	0
0	1	1	1	0	1
<hr/>					0
0	0	1	0	1	0

The first example is labeled "no errors". The second example has a red cross over the 3rd row, 4th column cell (containing a 1). It is labeled "parity error" with a red arrow pointing to it. Another red arrow points to the 5th row, 5th column cell (containing a 0), labeled "parity error". Below the second example, the text "correctable single bit error" is written.

Phát hiện lỗi: Cyclic redundancy Check (CRC)

Mô tả:

- Khối dữ liệu k bit
- Mẫu $n+1$ bit ($n < k$)
- Tạo ra dãy n bit gọi là dãy kiểm tra khung tin-FCS, Frame Check Sequence
- Tao ra một khung tin $k+n$ bit
- Bên nhận khi nhận được khung tin sẽ chia cho mẫu, nếu kết quả là chia hết, việc truyền khung tin này là không có lỗi

Phát hiện lỗi: CRC dưới dạng module của 2

M: Khối tin k bit

F: FCS n bit, n bit cuối của T

T: khung tin k+n bit

P: Mẫu n+1 bit, đây là một số chia được chọn trước.

Mục tiêu: xác định F để T chia hết cho P

$$T = 2^nM + F$$

Phát hiện lỗi: Các bước tạo và kiểm tra CRC

- Các bước tạo CRC
 - Dịch trái M đi n bit
 - Chia kết quả cho P
 - Số dư tìm được là F
- Các bước kiểm tra CRC
 - Lấy khung nhận được ($n+k$) bit
 - Chia cho P
 - Kiểm tra số dư, nếu số dư khác 0, khung bị lỗi, ngược lại là không lỗi

Phát hiện lỗi: CRC- Dạng đa thức nhị phân

Cách thứ 2 để biểu thị CRC là biểu diễn các giá trị như là một đa thức với các hệ số là số nhị phân, đây là các bit của số nhị phân. Gọi $T(X)$, $M(X)$, $Q(X)$, $P(X)$, $R(X)$ là các đa thức tương ứng với các số nhị phân T, M, Q, P, R đã trình bày ở trên, khi đó CRC được biểu thị:

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

CRC- Dạng đa thức nhị phân

Một số đa thức P(X) tiêu biểu:

CRC-12: $X^{12}+X^{11}+X^3+X^2+X+1$

CRC-CCITT: $X^{16}+X^{12}+X^5+1$

CRC32: $X^{32}+X^{26}+X^{23}+X^{22}+X^{16}+X^{12}+X^{11}+X^{10}+X^8+X^7+X^5+X^4+X^2+X+1$

CRC-16: $X^{16}+X^{15}+X^2+1$

Ví dụ:

Tạo CRC:

1. Cho tin M=1010001101 (10 bit)

Mẫu P:110101 (6 bit)

FCS R: được tính theo phương pháp CRC v
sẽ có độ dài là 5 bit

2. Nhân M với 2^5 ta được:

$M2^5=101000110100000$

3. Chia kết quả cho P:

4. Số dư là: 01110, được đưa vào sau tin M

Ta có tin T, được truyền đi là:

101000110101110

$$\begin{array}{r} \text{1101010110} \leftarrow Q \\ P \rightarrow 110101 | \underline{\text{101000110100000}} \leftarrow 2^5 M \\ \text{110101} \\ \hline \text{111011} \\ \text{110101} \\ \hline \text{111010} \\ \text{110101} \\ \hline \text{111110} \\ \text{110101} \\ \hline \text{101100} \\ \text{110101} \\ \hline \text{110010} \\ \text{110101} \\ \hline \text{01110} \leftarrow R \end{array}$$

CRC- Dạng đa thức nhị phân

- Kiểm tra CRC:
- Giả sử bên thu nhận được T, khi đó để kiểm tra là phép truyền có lỗi không ta chia T cho P, số dư là 00000, vậy ta kết luận phép truyền tin M, không có lỗi.

$$\begin{array}{r} 1101010110 \leftarrow Q \\ P \rightarrow 110101 | 101000110101110 \leftarrow T \\ \underline{110101} \\ 111011 \\ \underline{110101} \\ 111010 \\ \underline{110101} \\ 111110 \\ \underline{110101} \\ 101111 \\ \underline{110101} \\ 110101 \\ \underline{110101} \\ 00000 \leftarrow R \end{array}$$

Xử lý lỗi

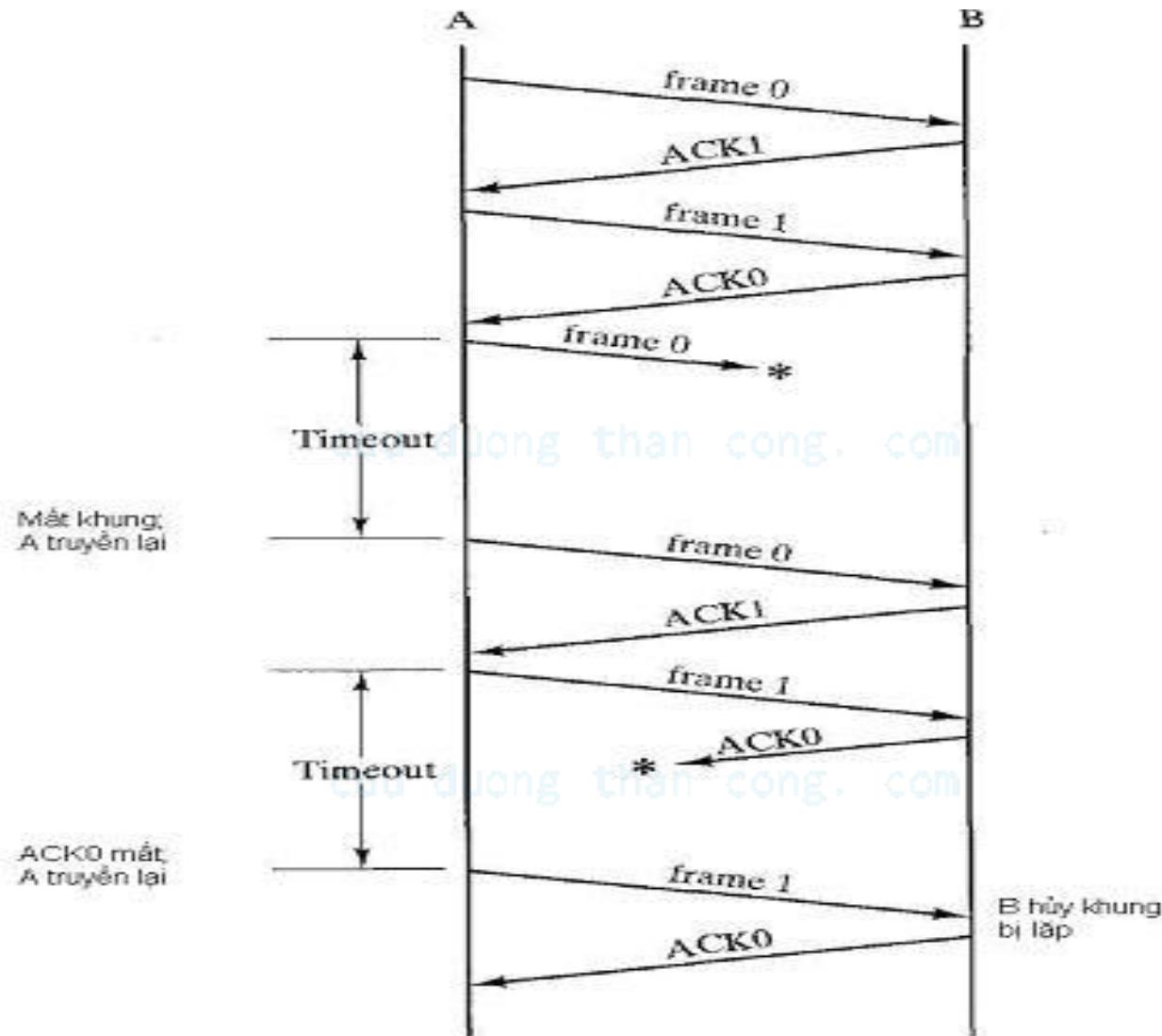
- Lỗi: Mất khung, hỏng khung
- Kiểm soát lỗi:
 - Phát hiện lỗi
 - Báo nhận: khung tin tốt
 - Truyền lại khi hết thời gian định trước
 - Báo nhận: khung tin lỗi và truyền lại

Xử lý lỗi: ARQ dừng và chờ

- Trên cơ sở kĩ thuật điều khiển luồng dừng-và-chờ
- Kiểm soát lỗi:
 - Khung tin tới bên nhận bị hỏng: Truyền lại, sử dụng đồng hồ đếm giờ time-out
 - Báo nhận bị hỏng: Time-out, bên phát gửi lại, sử dụng label 0/1 và ACK0/ACK1 phát hiện lỗi

cuuduongthancong.com

Xử lý lỗi: ARQ dùng và chờ



Xử lý lỗi: ARQ Quay-lui-N

- Trên cơ sở kĩ thuật điều khiển luồng bằng Cửa sổ trượt
- Kiểm soát lỗi:
 - Khung hỏng:
 - Khung i-1 thành công, i lỗi, bên nhận gửi SREJ i, bên phát gửi lại
 - Khung i mất, i+1 được nhận không đúng trình tự, REJ i, bên gửi phát lại i và các khung sau đó
 - Chỉ khung i được truyền và bị mất, bên nhận không biết i đã được truyền đi, bên phát gửi time-out và gửi RR với P=1, khi bên phát nhận được RR từ bên nhận nó sẽ phát lại i

Xử lý lỗi: ARQ Quay-lui-N

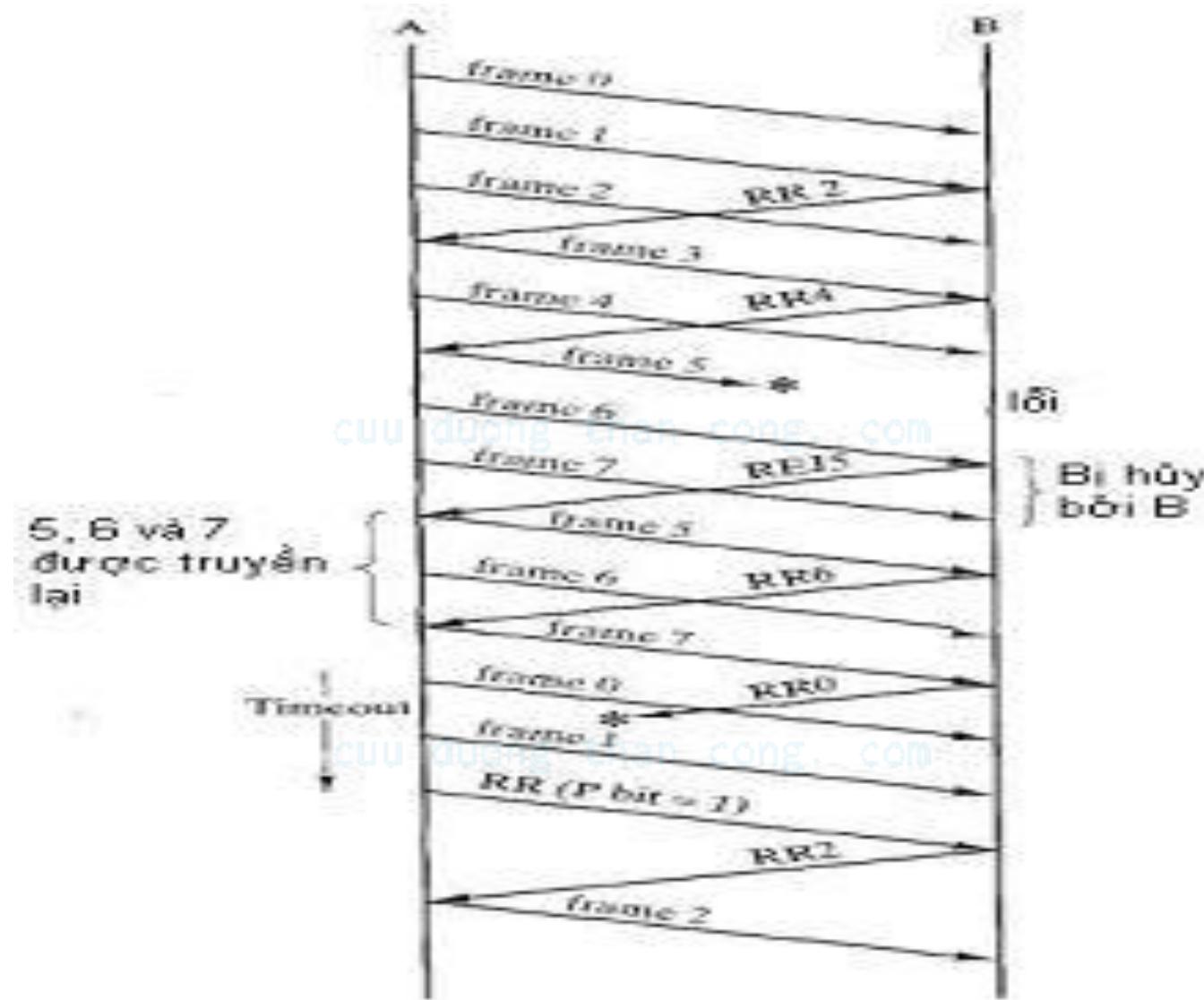
– RR hỏng:

- B nhận khung i và gửi RR(i+1), RR(i+1) mất, A có thể nhận RR(>i+1) trước khi RR(i+1) time-out, và có nghĩa là khung i đã thành công.
- RR(i+1) time-out, A cố gắng gửi RR với P-bit cho đến khi nhận được RR từ B một số lần nhất định, nếu vẫn không nhận được thì Khởi động lại giao thức

– Reject hỏng:

- A time-out, A gửi RR với P=1 cho đến khi nhận được RRi từ B thì A sẽ gửi lại khung i

Xử lý lỗi: ARQ Quay-lui-N



Xử lý lỗi: ARQ Chọn-Hủy (Selective-Reject)

- Chỉ truyền lại những khung có báo nhận là lỗi (SREJ)
- Phải duy trì đủ bộ đệm độ lớn
- Đảm bảo tính logic phức tạp để gửi và nhận các khung theo đúng trình tự.
- ARQ Chọn-Hủy phải giải quyết được sự chồng chéo giữa cửa sổ gửi và nhận.

Xử lý lỗi: ARQ Chọn-Hủy (Selective-Reject)

- Trạm A gửi các khung từ 0 đến 6 tới trạm B.
- Trạm B nhận tất cả 7 khung và báo nhận tích lũy với RR 7
- Vì lí do nào đó ví dụ như nhiễu làm RR 7 bị mất trên đường truyền.
- Đồng hồ ở A hết hạn và A truyền lại khung 0.
- B đã điều chỉnh trước cửa sổ nhận để có thể nhận các khung 7, 0, 1, 2, 3, 4 và 5. Do đó mà khung 7 được coi là bị mất và khung nhận được này là khung số 0 mới, và được chấp nhận bởi B.

CHƯƠNG 5: TCP/IP

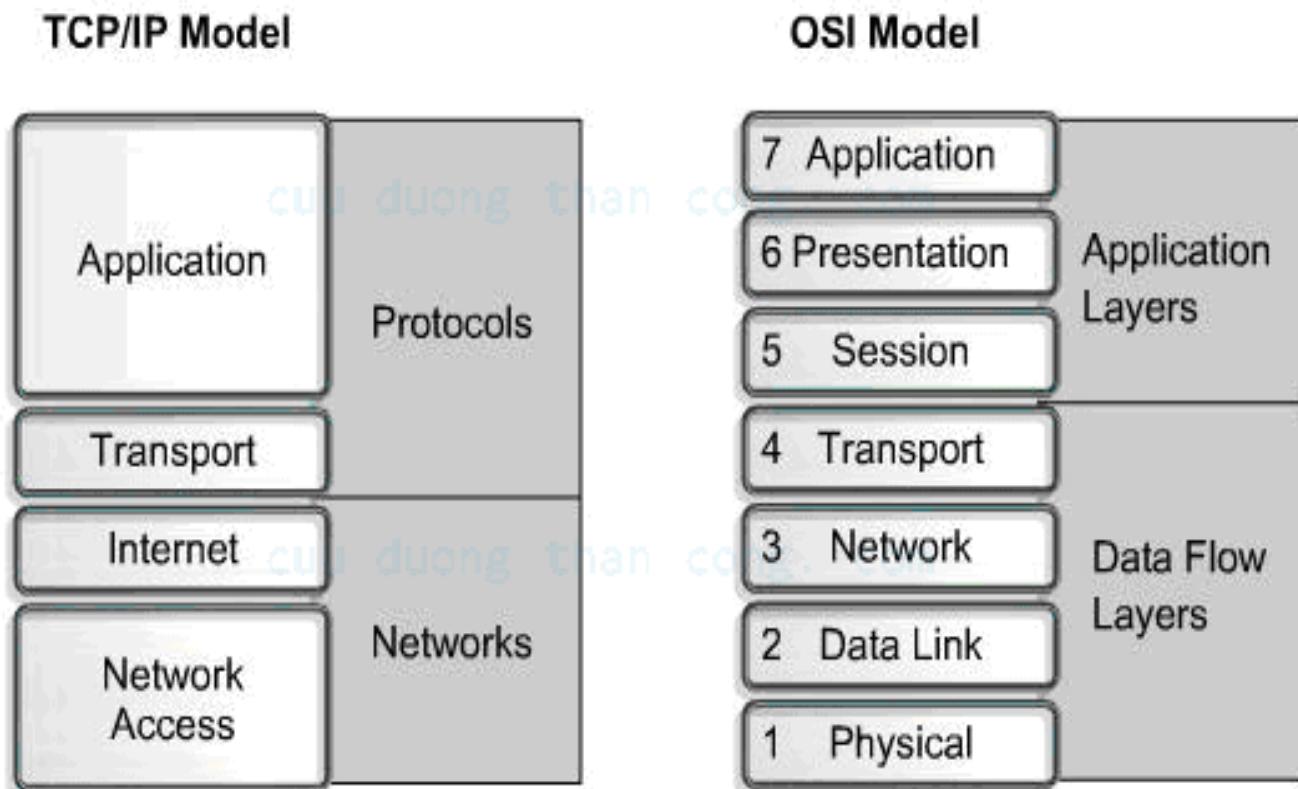
- Khái niệm về TCP và IP
- Mô hình tham chiếu TCP/IP
- So sánh OSI và TCP/IP
- Các giao thức trong mô hình TCP/IP
- Chuyển đổi giữa các hệ thống số
- Địa chỉ IP và các lớp địa chỉ
- NAT
- Mạng con và kỹ thuật chia mạng con
- Bài tập

Khái niệm về TCP và IP

- TCP (Transmission Control Protocol) là giao thức thuộc tầng vận chuyển và là một giao thức có kết nối (connected-oriented).
- IP (Internet Protocol) là giao thức thuộc tầng mạng của mô hình OSI và là một giao thức không kết nối (connectionless).

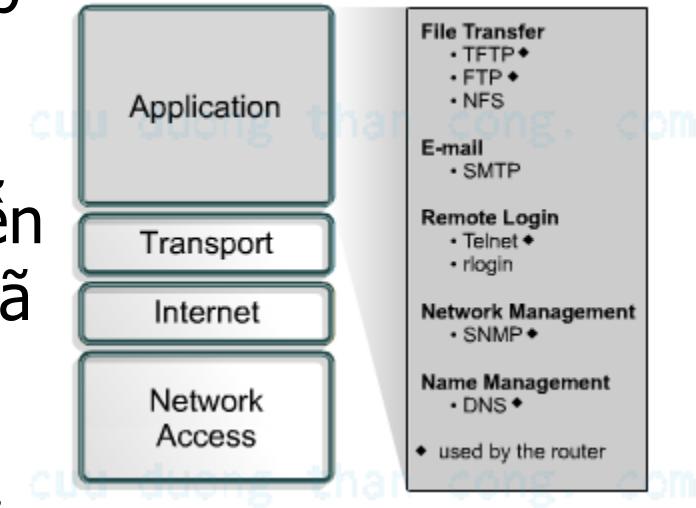
cuu duong than cong. com

Mô hình tham chiếu TCP/IP



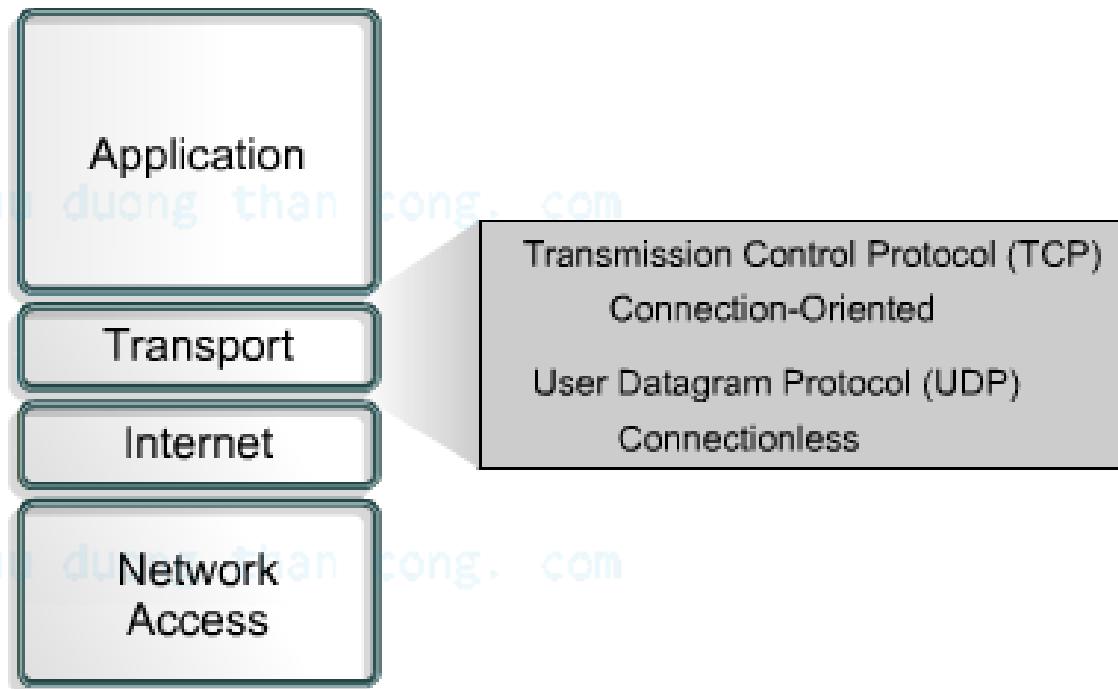
Lớp Ứng dụng

Kiểm soát các giao thức lớp cao, các chủ đề về trình bày, biểu diễn thông tin, mã hóa và điều khiển hội thoại. Đặc tả cho các ứng dụng phổ biến.



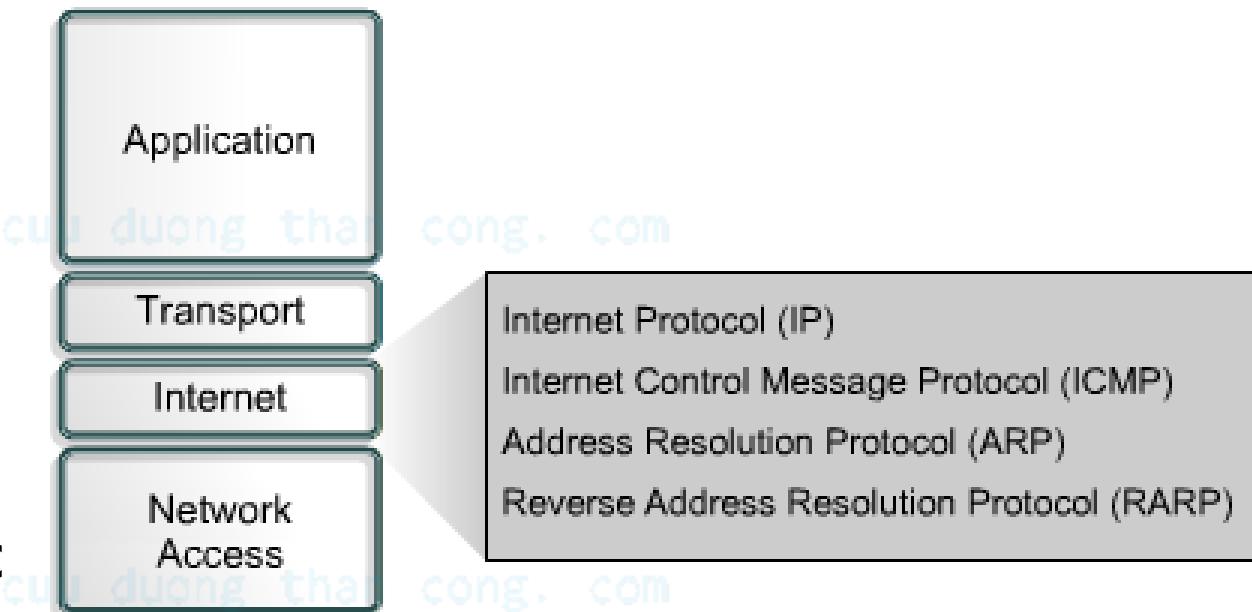
Lớp vận chuyển

Cung ứng dịch vụ vận chuyển từ host nguồn đến host đích. Thiết lập một cầu nối luận lý giữa các đầu cuối của mạng, giữa host truyền và host nhận.



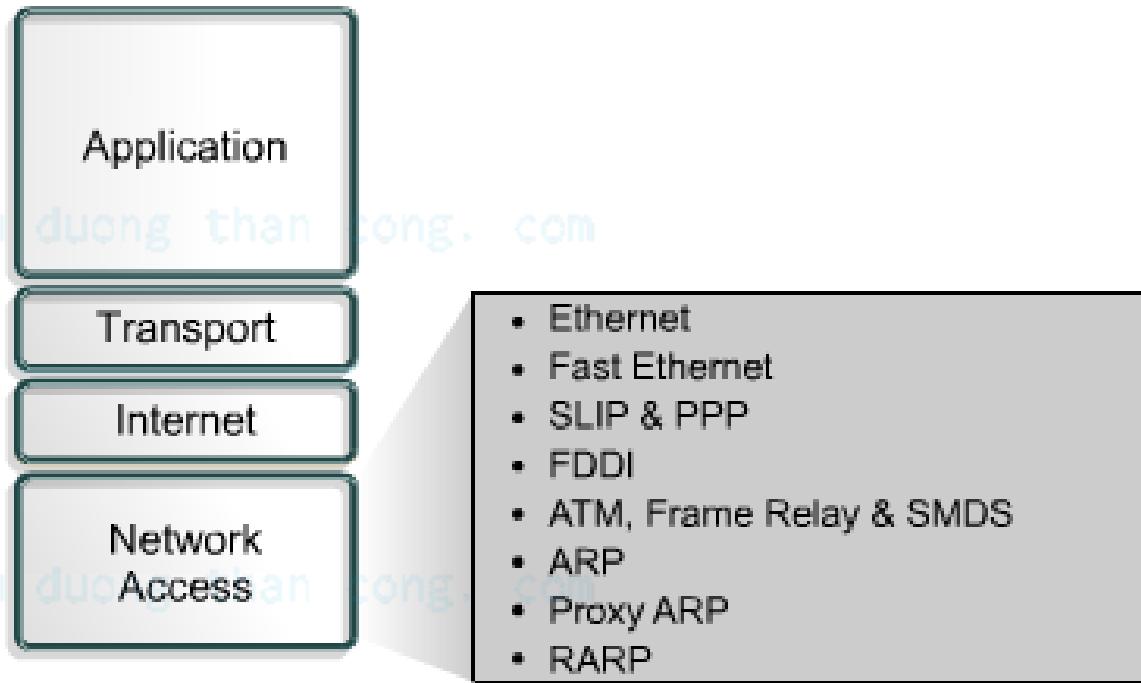
Lớp Internet

Mục đích của lớp Internet là chọn đường đi tốt nhất xuyên qua mạng cho các gói dữ liệu di chuyển tới đích. Giao thức chính của lớp này là Internet Protocol (IP).



Lớp truy nhập mạng

Định ra các thủ tục để giao tiếp với phần cứng mạng và truy nhập môi trường truyền. Có nhiều giao thức hoạt động tại lớp này



So sánh mô hình OSI và TCP/IP

- Giống nhau
 - Đều phân lớp chức năng
 - Đều có lớp vận chuyển và lớp mạng.
 - Chuyển gói là hiển nhiên.
 - Đều có mối quan hệ trên dưới, ngang hàng.
- Khác nhau
 - TCP/IP gộp lớp trình bày và lớp phiên vào lớp ứng dụng.
 - TCP/IP gộp lớp vật lý và lớp liên kết dữ liệu vào lớp truy nhập mạng.
 - TCP/IP đơn giản vì có ít lớp hơn.
 - OSI không có khái niệm chuyển phát thiếu tin cậy ở lớp 4 như UDP của TCP/IP

Các giao thức trong mô hình TCP/IP

DoD Model

Process/ Application	Telnet TFTP	FTP SMTP	LPD NFS	SNMP X Window
Host-to-Host	TCP		UDP	
Internet	ICMP	ARP	RARP	IP
Network Access	Ethernet	Fast Ethernet	Token Ring	FDDI

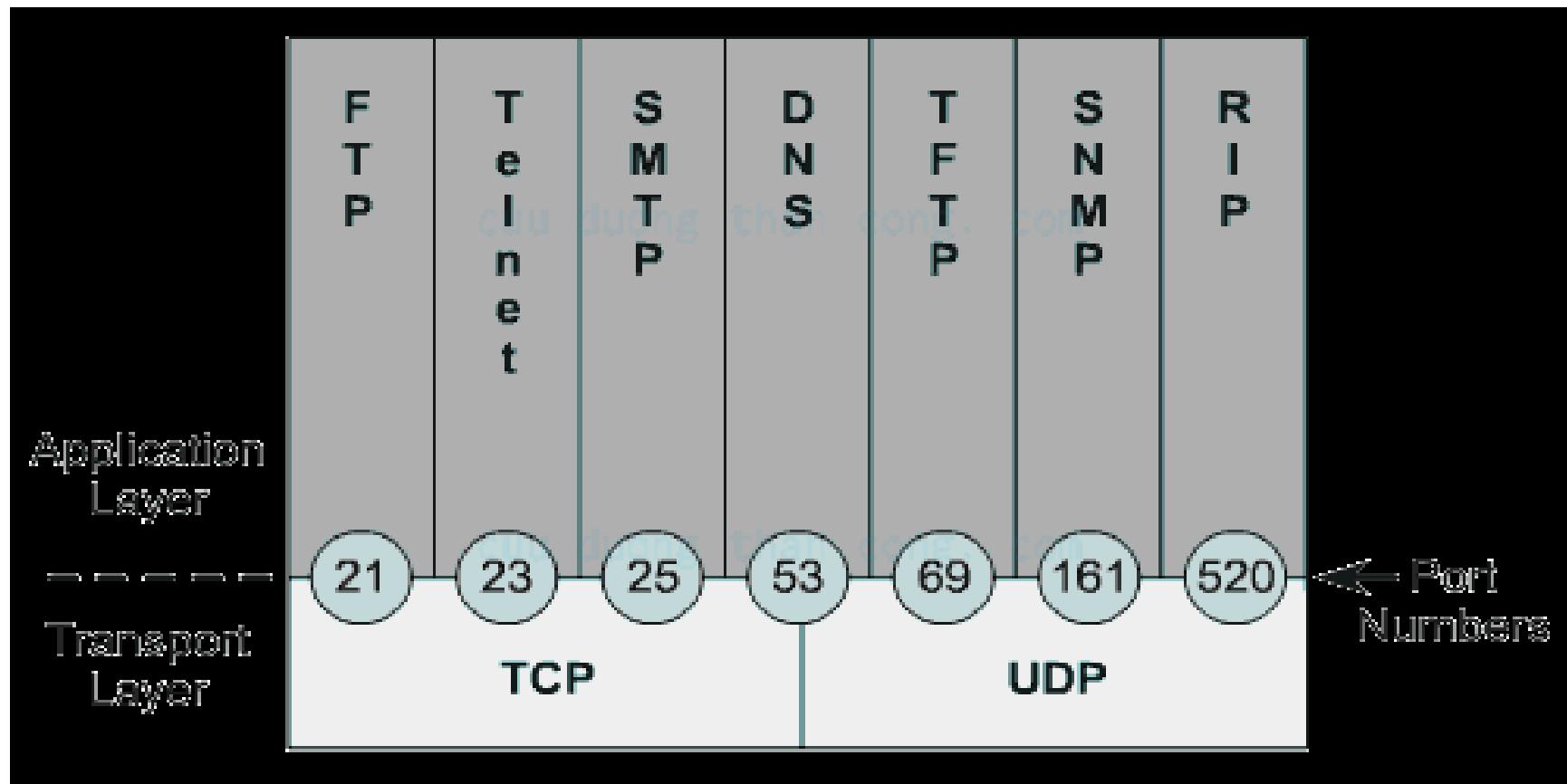
Lớp Ứng dụng

- FTP (File Transfer Protocol): là dịch vụ có tạo cầu nối, sử dụng TCP để truyền các tập tin giữa các hệ thống.
- TFTP (Trivial File Transfer Protocol): là dịch vụ không tạo cầu nối, sử dụng UDP. Được dùng trên router để truyền các file cấu hình và hệ điều hành.
- NFS (Network File System): cho phép truy xuất file đến các thiết bị lưu trữ ở xa như một đĩa cứng qua mạng.
- SMTP (Simple Mail Transfer Protocol): quản lý hoạt động truyền e-mail qua mạng máy tính.

Lớp Ứng dụng

- Telnet (Terminal emulation): cung cấp khả năng truy nhập từ xa vào máy tính khác. Telnet client là host cục bộ, telnet server là host ở xa.
- SNMP (Simple Network Management): cung cấp một phương pháp để giám sát và điều khiển các thiết bị mạng.
- DNS (Domain Name System): thông dịch tên của các miền (Domain) và các node mạng được công khai sang các địa chỉ IP.

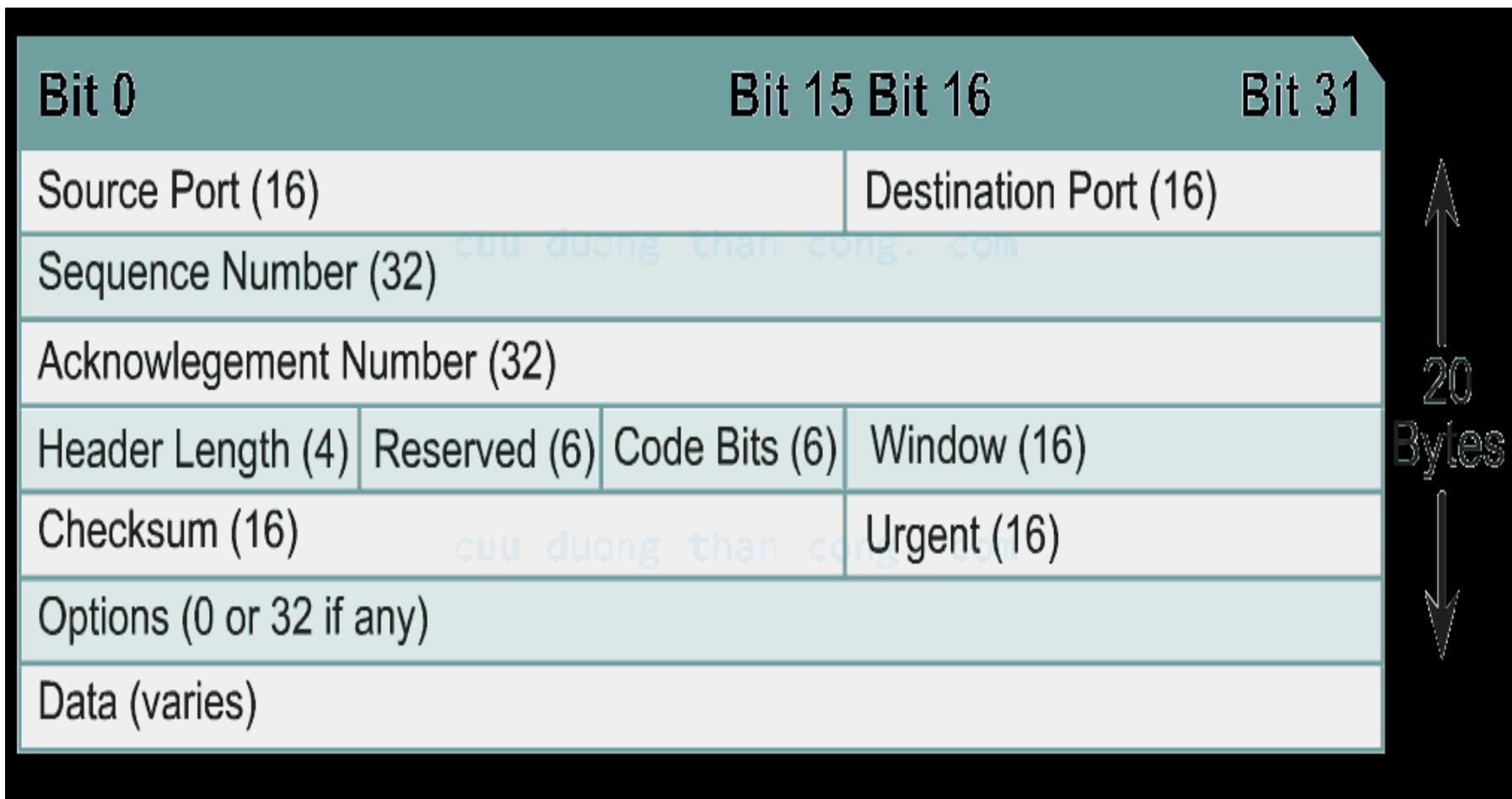
Các cổng phổ biến dùng cho các giao thức lớp ứng dụng



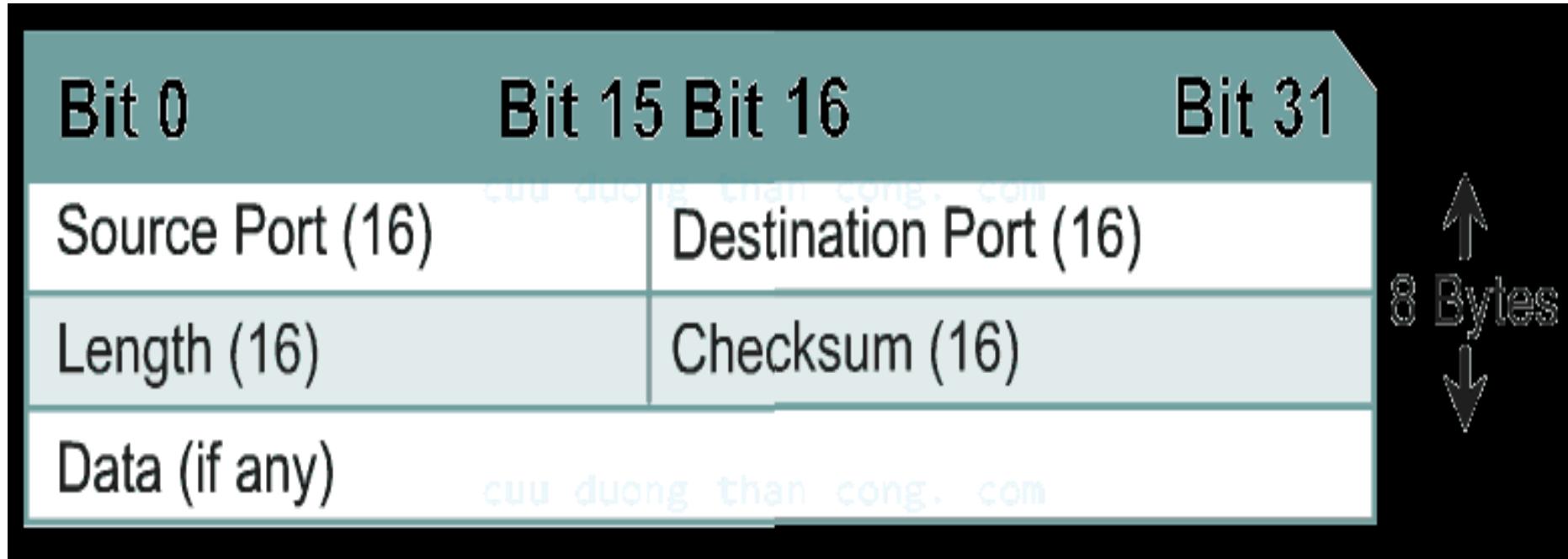
Lớp vận chuyển

- TCP và UDP (User Datagram Protocol):
 - Phân đoạn dữ liệu ứng dụng lớp trên.
 - Truyền các segment từ một thiết bị đầu cuối này đến thiết bị đầu cuối khác
- Riêng TCP còn có thêm các chức năng:
 - Thiết lập các hoạt động end-to-end.
 - Cửa sổ trượt cung cấp điều khiển luồng.
 - Chỉ số tuần tự và báo nhận cung cấp độ tin cậy cho hoạt động.

Khuôn dạng gói tin TCP



Khuôn dạng gói tin UDP



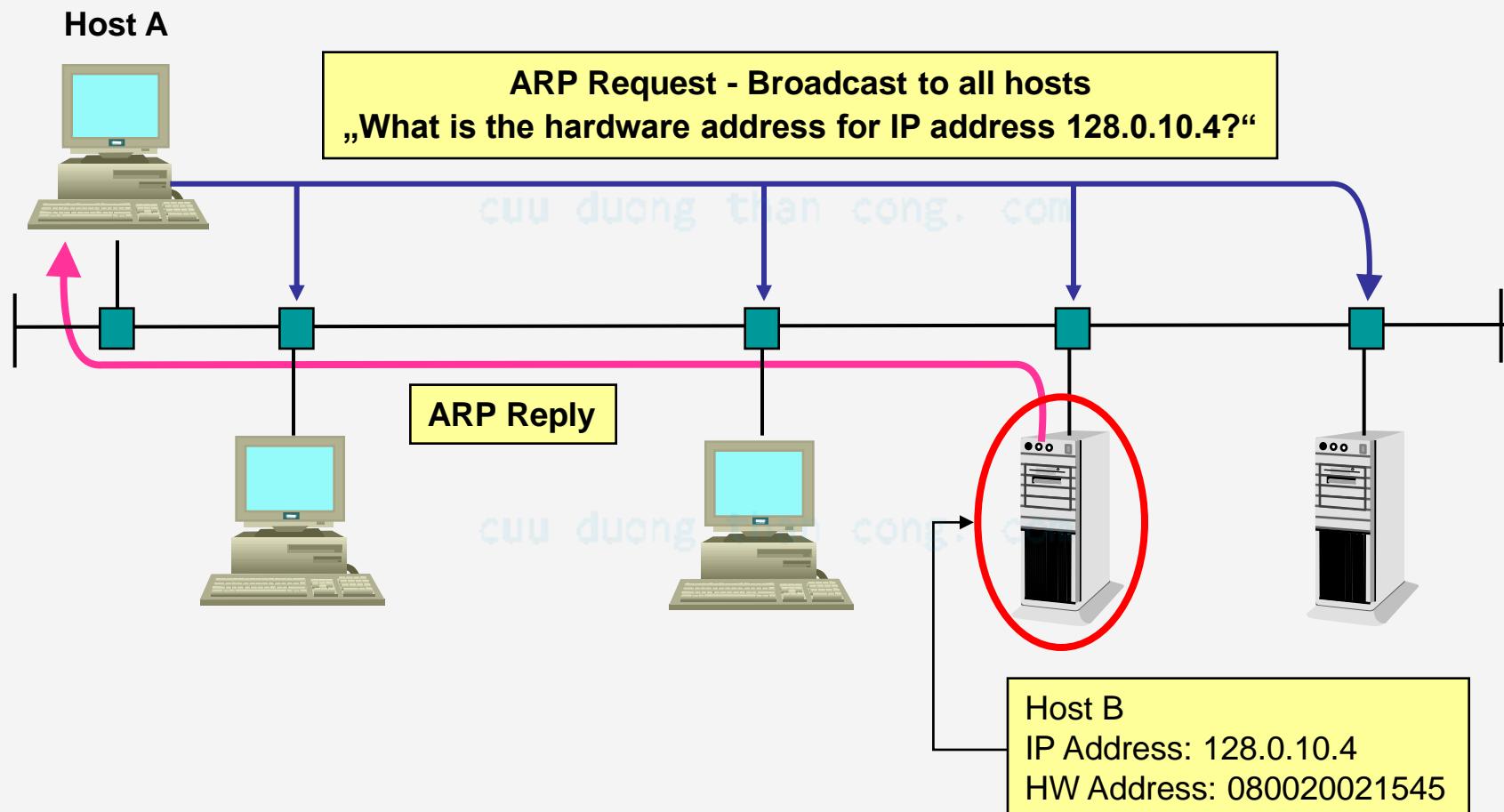
Lớp Internet

- IP: không quan tâm đến nội dung của các gói nhưng tìm kiếm đường dẫn cho gói tới đích.
- ICMP (Internet Control Message Protocol): đem đến khả năng điều khiển và chuyển thông điệp.
- ARP (Address Resolution Protocol): xác định địa chỉ lớp liên kết số liệu (MAC address) khi đã biết trước địa chỉ IP.
- RARP (Reverse Address Resolution Protocol): xác định các địa chỉ IP khi biết trước địa chỉ MAC.

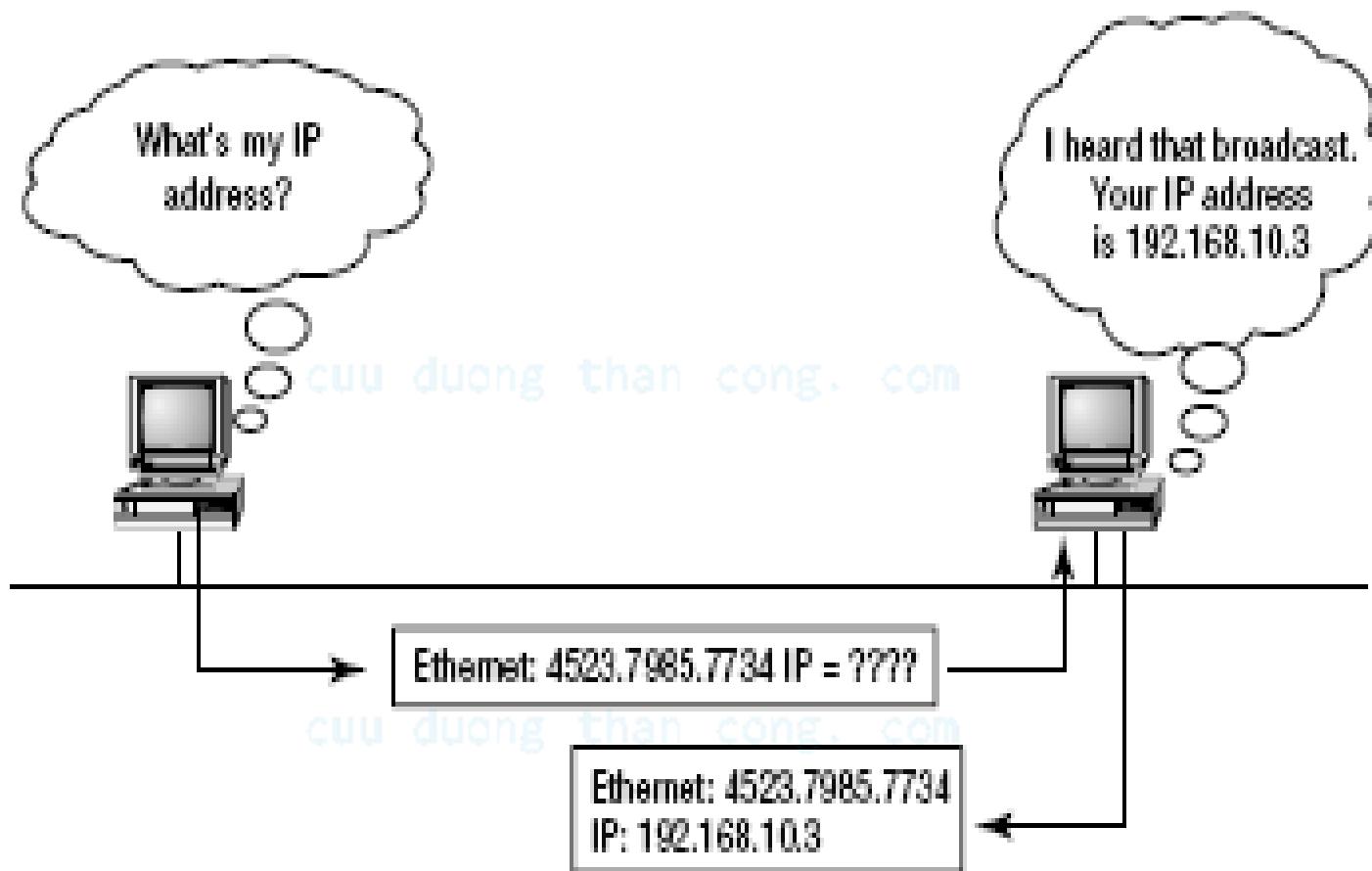
Khuôn dạng gói tin IP

VER	IHL	Type of services	Total lenght
		Identification	Flags Fragment offset
Time to live	Protocol	Header checksum	
Source address			
Destination address			
Options + Padding			
Data			

ARP



RARP



Lớp truy nhập mạng

- Ethernet
 - Là giao thức truy cập LAN phổ biến nhất.
 - Được hình thành bởi định nghĩa chuẩn 802.3 của IEEE (Institute of Electrical and Electronics Engineers).
 - Tốc độ truyền 10Mbps
- Fast Ethernet
- Gigabit Ethernet

Chuyển đổi giữa các hệ thống số

- Hệ 2 (nhị phân): gồm 2 ký số 0, 1
- Hệ 8 (bát phân): gồm 8 ký số 0, 1, ..., 7
- Hệ 10 (thập phân): gồm 10 ký số 0, 1, ..., 9
- Hệ 16 (thập lục phân): gồm các ký số 0, 1, ..., 9 và các chữ cái A, B, C, D, E, F

cuuduongthancong.com

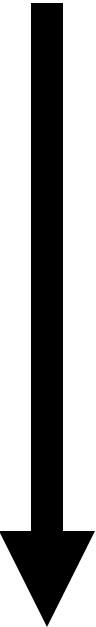
Chuyển đổi giữa hệ nhị phân sang hệ thập phân

$$10110_2 = (1 \times 2^4) + (0 \times 2^3) + (1 \times 2^2) + \\ (1 \times 2^1) + (0 \times 2^0) = 16 + 0 + 4 + 2 + 0 = 22$$

Cửu dường Thanh Công. com								
Place Value	128	64	32	16	8	4	2	1
Base ^{Exponent}	$2^7 = 128$	$2^3 = 8$						
	$2^6 = 64$	$2^2 = 4$						
	$2^5 = 32$	$2^1 = 2$						
	$2^4 = 16$	$2^0 = 1$						
Number of Symbols	2							
Symbols	0, 1							
Rationale	Two-state (discrete binary) voltage systems made from transistors can be diverse, powerful, inexpensive, tiny and relatively immune to noise.							

Chuyển đổi giữa hệ thập phân sang hệ nhị phân

Đổi số 201_{10} sang nhị phân:

	201	/	2	=	100	dư	1
	100	/	2	=	50	dư	0
	50	/	2	=	25	dư	0
	25	/	2	=	12	dư	1
	12	/	2	=	6	dư	0
	6	/	2	=	3	dư	0
	3	/	2	=	1	dư	1
	1	/	2	=	0	dư	1



Khi thương số bằng 0, ghi các số dư theo thứ tự ngược với lúc xuất hiện, kết quả: $201_{10} = 11001001_2$

Chuyển đổi giữa hệ nhị phân sang hệ bát phân và thập lục phân

- Nhị phân sang bát phân:
 - Gom nhóm số nhị phân thành từng nhóm 3 chữ số tính từ phải sang trái. Mỗi nhóm tương ứng với một chữ số ở hệ bát phân.
 - Ví dụ: $1'101'100_{(2)} = 154_{(8)}$
- Nhị phân sang thập lục phân:
 - Tương tự như nhị phân sang bát phân nhưng mỗi nhóm có 4 chữ số.
 - Ví dụ: $110'1100_{(2)} = 6C_{(16)}$

Các phép toán làm việc trên bit

A	B	A and B
1	1	1
1	0	0
0	1	0
0	0	0

Địa chỉ IP và các lớp địa chỉ

- Địa chỉ IP là địa chỉ có cấu trúc với một con số có kích thước 32 bit, chia thành 4 phần mỗi phần 8 bit gọi là octet hoặc byte.
- Ví dụ:
 - 172.16.30.56
 - 10101100 00010000 00011110 00111000.
 - AC 10 1E 38

Địa chỉ IP và các lớp địa chỉ

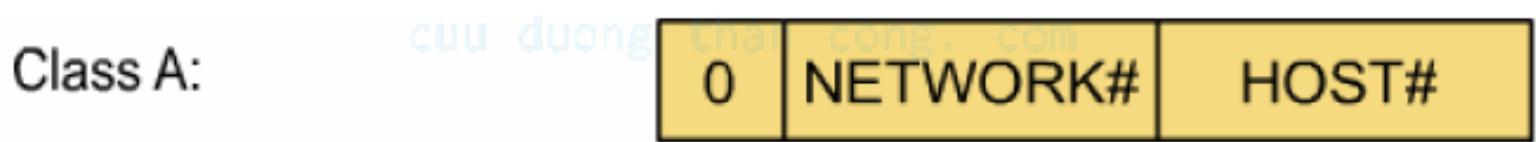
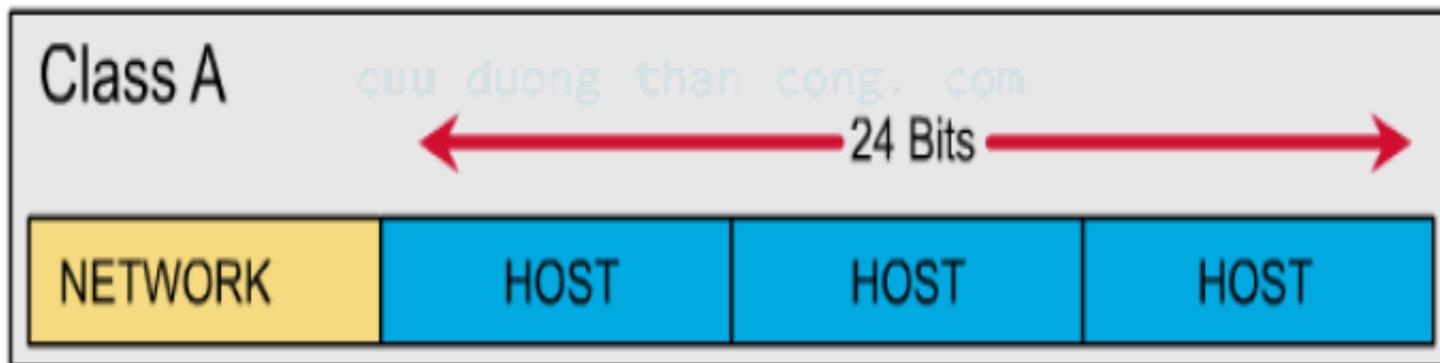
- Địa chỉ host là địa chỉ IP có thể dùng để đặt cho các interface của các host. Hai host nằm cùng một mạng sẽ có network_id giống nhau và host_id khác nhau.
- Khi cấp phát các địa chỉ host thì lưu ý **không được cho tất cả các bit trong phần host_id bằng 0 hoặc tất cả bằng 1**.
- Địa chỉ mạng (network address): là địa chỉ IP dùng để đặt cho các mạng. Phần host_id của địa chỉ chỉ chứa các bit 0. Ví dụ: 172.29.0.0
- Địa chỉ Broadcast: là địa chỉ IP được dùng để đại diện cho tất cả các host trong mạng. Phần host_id chỉ chứa các bit 1. Ví dụ: 172.29.255.255.

Các lớp địa chỉ IP

Không gian địa chỉ IP được chia thành 5 lớp (class) A, B, C, D và E. Các lớp A, B và C được triển khai để đặt cho các host trên mạng Internet, lớp D dùng cho các nhóm multicast, còn lớp E phục vụ cho mục đích nghiên cứu.

Lớp A (Class A)

Dành 1 byte cho phần network_id và 3 byte cho phần host_id.



Lớp A (Class A)

- Bit đầu tiên của byte đầu tiên phải là bit 0. Dạng nhị phân của octet này là **0xxxxxxxx**
- Những địa chỉ IP có byte đầu tiên nằm trong khoảng từ 0 ($=00000000_{(2)}$) đến 127 ($=01111111_{(2)}$) sẽ thuộc lớp A.
- Ví dụ: 50.14.32.8.

Lớp A (Class A)

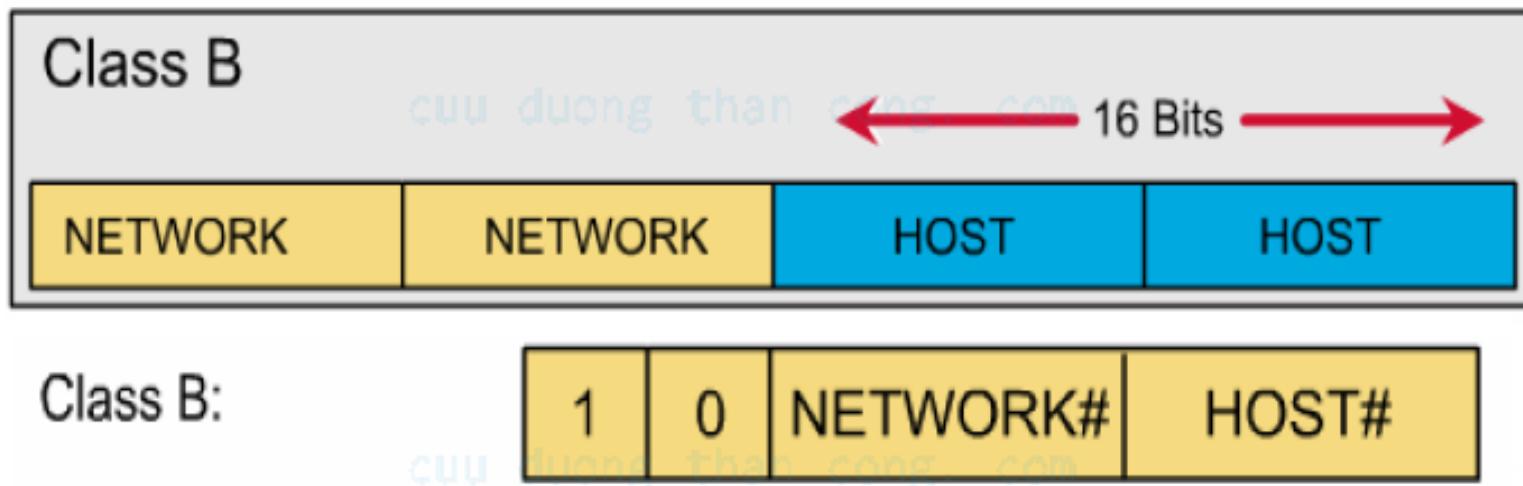
- Byte đầu tiên này cũng chính là network_id, trừ đi bit đầu tiên làm ID nhận dạng lớp A, còn lại 7 bit để đánh thứ tự các mạng, ta được $128 (=2^7)$ mạng lớp A khác nhau. **Bỏ đi hai trường hợp đặc biệt là 0 và 127.** Kết quả là lớp A chỉ còn 126 địa chỉ mạng, **1.0.0.0** đến **126.0.0.0**.

Lớp A (Class A)

- Phần host_id chiếm 24 bit, nghĩa là có $2^{24} = 16777216$ host khác nhau trong mỗi mạng. **Bỏ đi hai trường hợp đặc biệt (phần host_id chứa toàn các bit 0 và bit 1).** Còn lại: 16777214 host.
- Ví dụ đối với mạng 10.0.0.0 thì những giá trị host hợp lệ là 10.0.0.1 đến 10.255.255.254.

Lớp B (Class B)

Dành 2 byte cho phần network_id và 2 byte cho phần host_id.



Lớp B (Class B)

- Hai bit đầu tiên của byte đầu tiên phải là 10. Dạng nhị phân của octet này là **10xxxxxx**
- Những địa chỉ IP có byte đầu tiên nằm trong khoảng từ 128 ($=10000000_{(2)}$) đến 191 ($=10111111_{(2)}$) sẽ thuộc về lớp B
- Ví dụ: 172.29.10.1 .

Lớp B (Class B)

- Phần network_id chiếm 16 bit bỏ đi 2 bit làm ID cho lớp, còn lại 14 bit cho phép ta đánh thứ tự 16384 ($=2^{14}$) mạng khác nhau (128.0.0.0 đến 191.255.0.0).

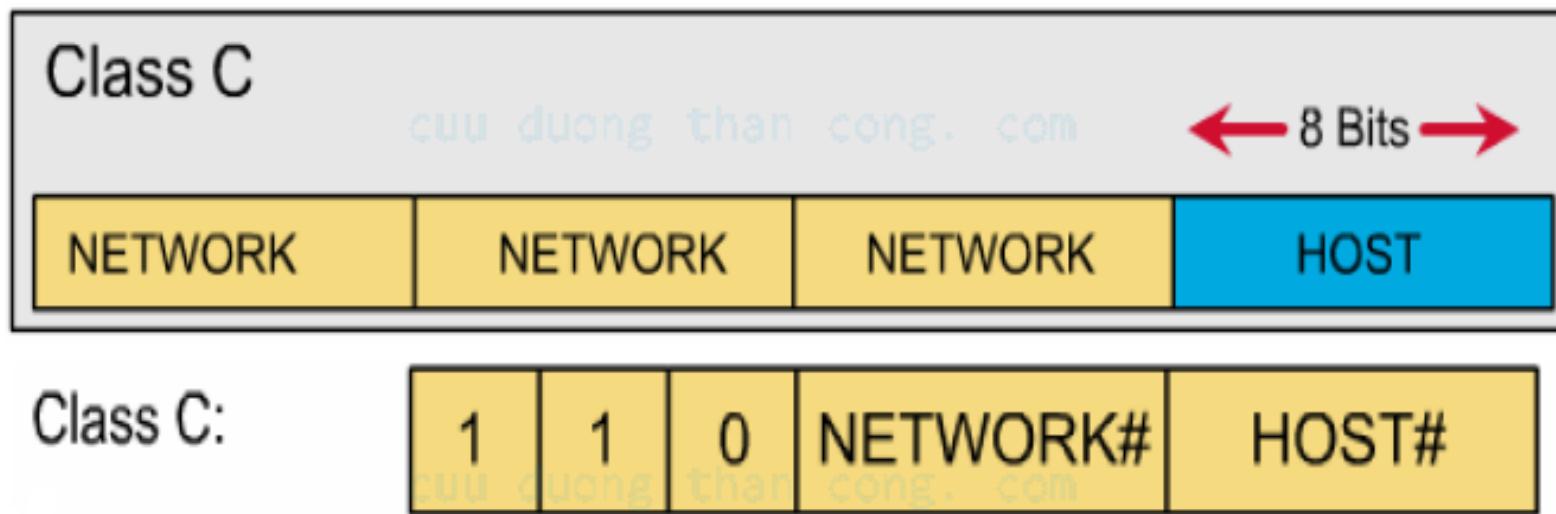
cuu duong than cong. com

Lớp B (Class B)

- Phần host_id dài 16 bit hay có 65536 ($=2^{16}$) giá trị khác nhau. Trừ đi 2 trường hợp đặc biệt còn lại 65534 host trong một mạng lớp B.
- Ví dụ đối với mạng 172.29.0.0 thì các địa chỉ host hợp lệ là từ 172.29.0.1 đến 172.29.255.254.

Lớp C (Class C)

Dành 3 byte cho phần network_id và 1 byte cho phần host_id.



Lớp C (Class C)

- Ba bit đầu tiên của byte đầu tiên phải là 110. Dạng nhị phân của octet này là **110xxxxx**
- Những địa chỉ IP có byte đầu tiên nằm trong khoảng từ 192 ($=11000000_{(2)}$) đến 223 ($=11011111_{(2)}$) sẽ thuộc về lớp C.
- Ví dụ: 203.162.41.235

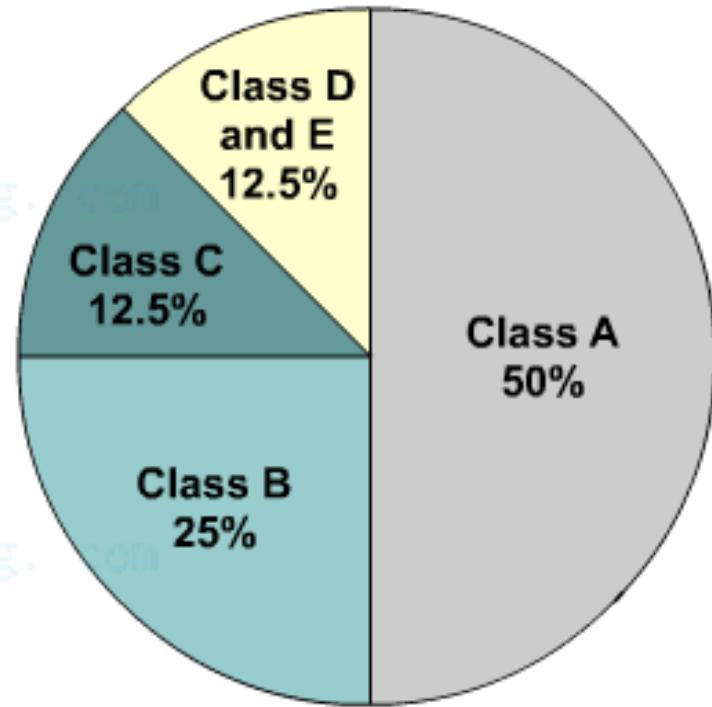
Các lớp địa chỉ IP

Address Class	Number of Networks	Number of Host per Network
A	126 *	16,777,216
B	16,384	65,535
C	2,097,152	254
D (Multicast)	N/A	N/A

IP Address Class	High Order Bits	First Octet Address Range	Number of Bits in the Network Address
Class A	0	0 - 127 *	8
Class B	10	128 - 191	16
Class C	110	192 - 223	24
Class D	1110	224 - 239	28

Các lớp địa chỉ IP

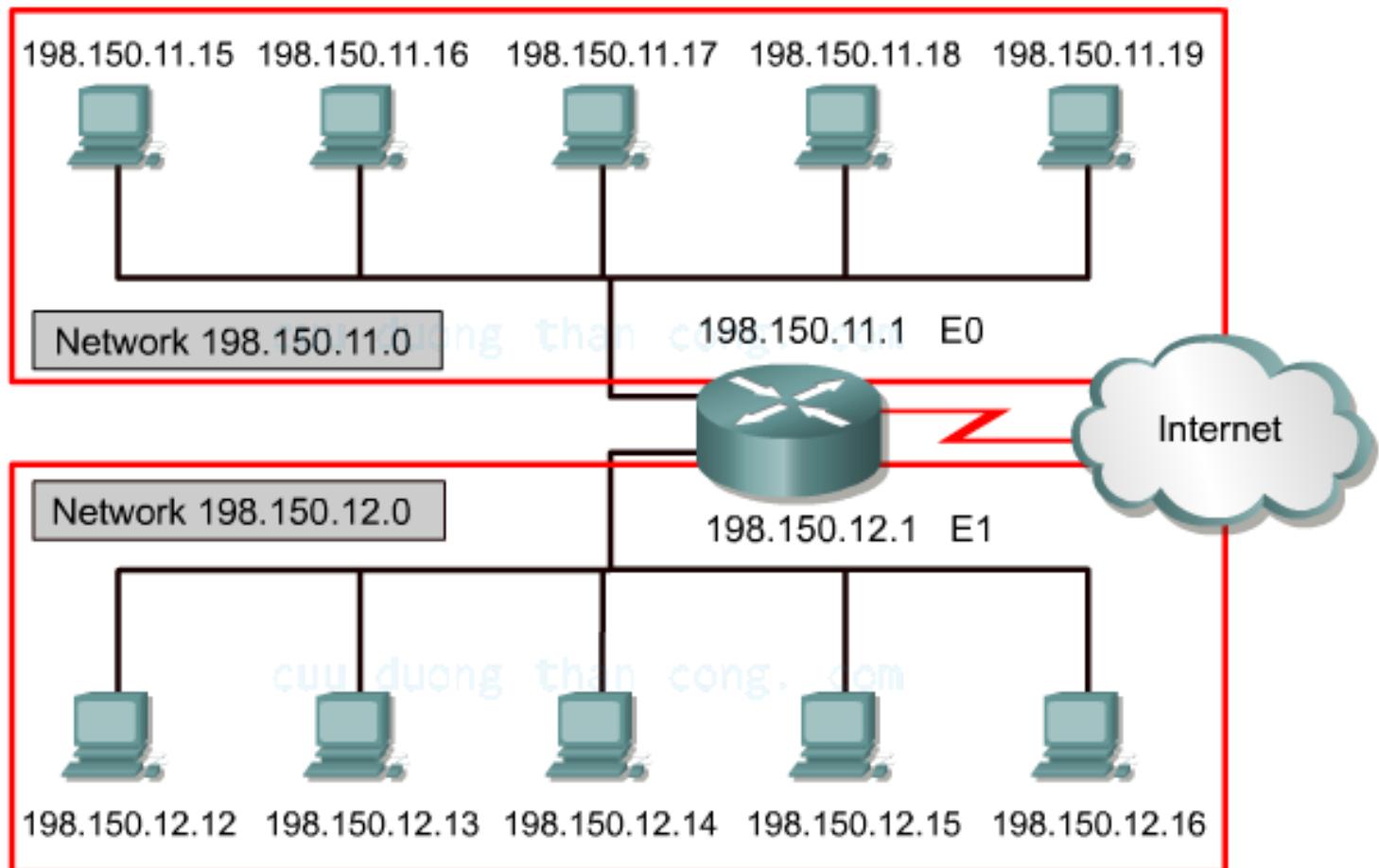
IP address class	IP address range (First Octet Decimal Value)
Class A	1-126 (00000001-01111110)*
Class B	128-191 (10000000-10111111)
Class C	192-223 (11000000-11011111)
Class D	224-239 (11100000-11101111)
Class E	240-255 (11110000-11111111)



Địa chỉ dành riêng

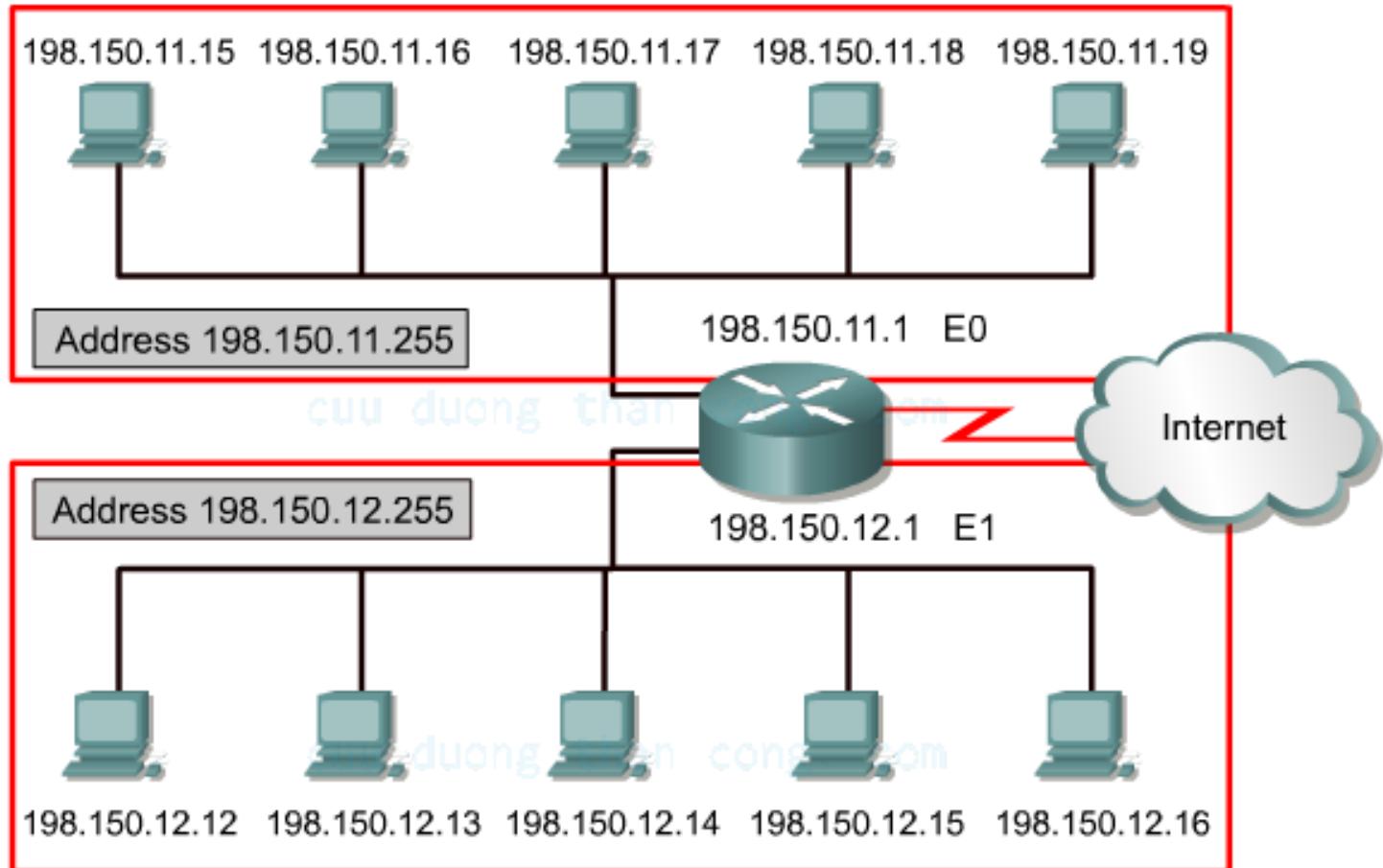
Class	RFC 1918 internal address range
A	10.0.0.0 to 10.255.255.255
B	172.16.0.0 to 172.31.255.255
C	192.168.0.0 to 192.168.255.255

Các lớp địa chỉ IP



Địa chỉ mạng

Các lớp địa chỉ IP



Địa chỉ broadcast

Các lớp địa chỉ IP

Lớp	Byte đầu tiên
A	0xxxxxxx
B	10xxxxxx
C	110xxxxx
D	1110xxxx
E	11110xxx

- **1.0.0.0 - 126.0.0.0 : Class A.**
- **127.0.0.0 : Loopback network.**
- **128.0.0.0 - 191.255.0.0 : Class B.**
- **192.0.0.0 - 223.255.255.0 : Class C.**

NAT: Network Address Translation

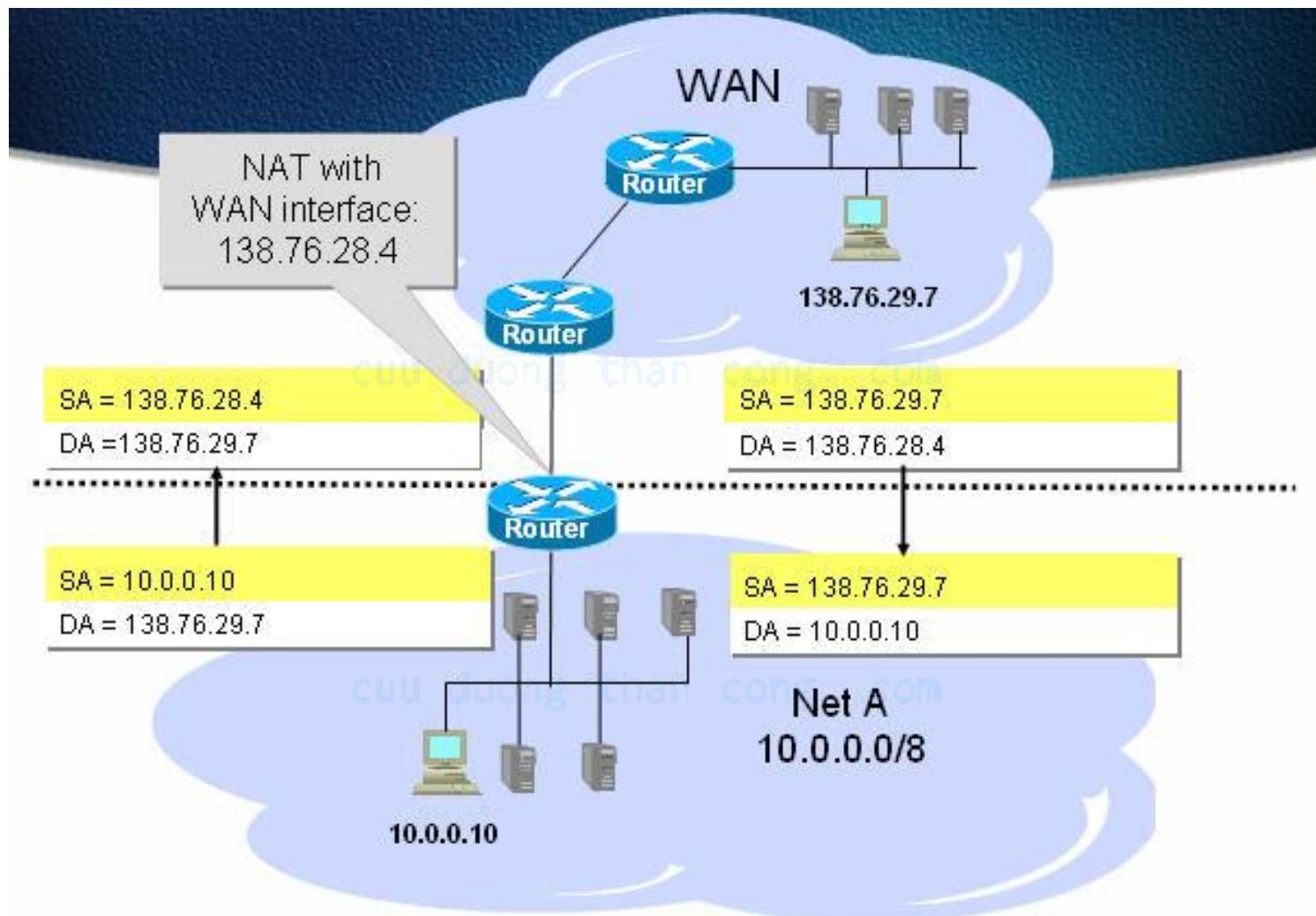
- Được thiết kế để tiết kiệm địa chỉ IP.
- Cho phép mạng nội bộ sử dụng địa chỉ IP riêng.
- Địa chỉ IP riêng sẽ được chuyển đổi sang địa chỉ công cộng định tuyến được.
- Mạng riêng được tách biệt và giấu kín IP nội bộ.
- Thường sử dụng trên router biên của mạng một cửa.

cuuduongthancong.com

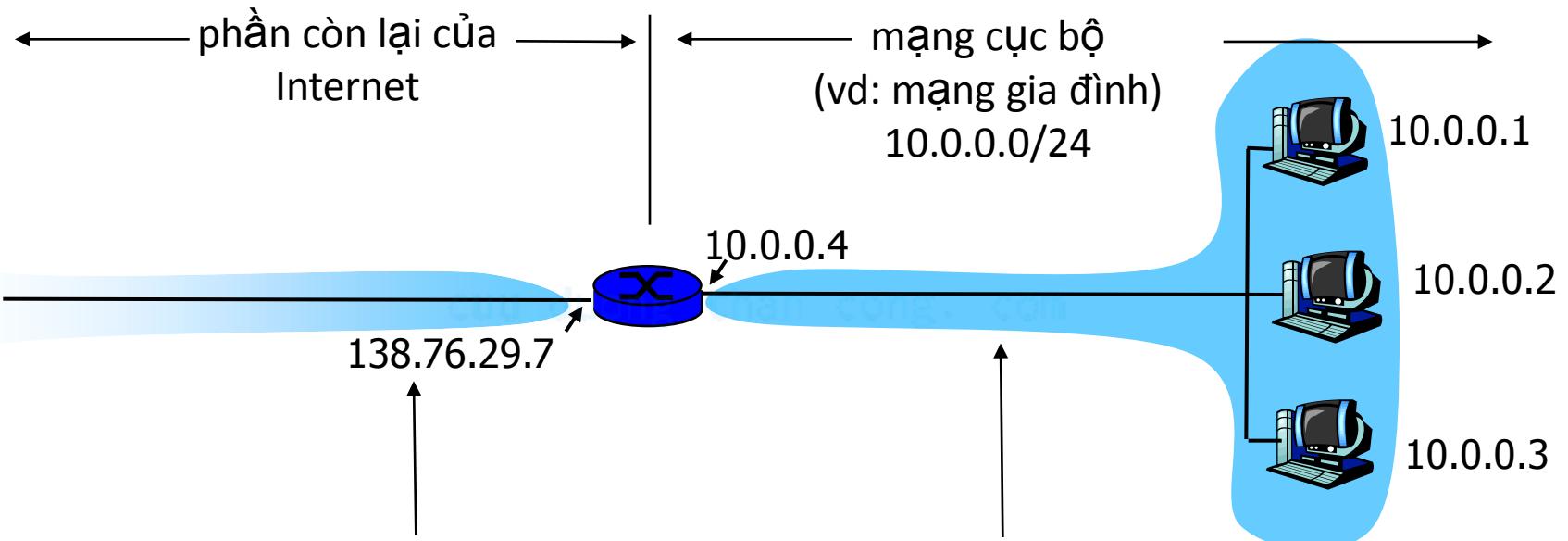
NAT

- Địa chỉ cục bộ bên trong (Inside local address): Địa chỉ được phân phối cho các host bên trong mạng nội bộ.
- Địa chỉ toàn cục bên trong (Inside global address): Địa chỉ hợp pháp được cung cấp bởi InterNIC (Internet Network Information Center) hoặc nhà cung cấp dịch vụ Internet, đại diện cho một hoặc nhiều địa chỉ nội bộ bên trong đối với thế giới bên ngoài.
- Địa chỉ cục bộ bên ngoài (Outside local address): Địa chỉ riêng của host nằm bên ngoài mạng nội bộ.
- Địa chỉ toàn cục bên ngoài (Outside global address): Địa chỉ công cộng hợp pháp của host nằm bên ngoài mạng nội bộ.

NAT



NAT



Tất cả datagram *đi ra khỏi* mạng cục bộ có cùng một địa chỉ IP NAT là: 138.76.29.7, với các số hiệu cổng nguồn khác nhau

các Datagram với nguồn hoặc đích trong mạng này có địa chỉ 10.0.0/24

NAT

- Mạng cục bộ chỉ dùng 1 địa chỉ IP đối với bên ngoài:
 - không cần thiết dùng 1 vùng địa chỉ từ ISP: chỉ cần 1 cho tất cả các thiết bị
 - có thể thay đổi địa chỉ các thiết bị trong mạng cục bộ mà không cần thông báo với bên ngoài
 - có thể thay đổi ISP mà không cần thay đổi địa chỉ các thiết bị trong mạng cục bộ
 - các thiết bị trong mạng cục bộ không nhìn thấy, không định địa chỉ rõ ràng từ bên ngoài (tăng cường bảo mật)

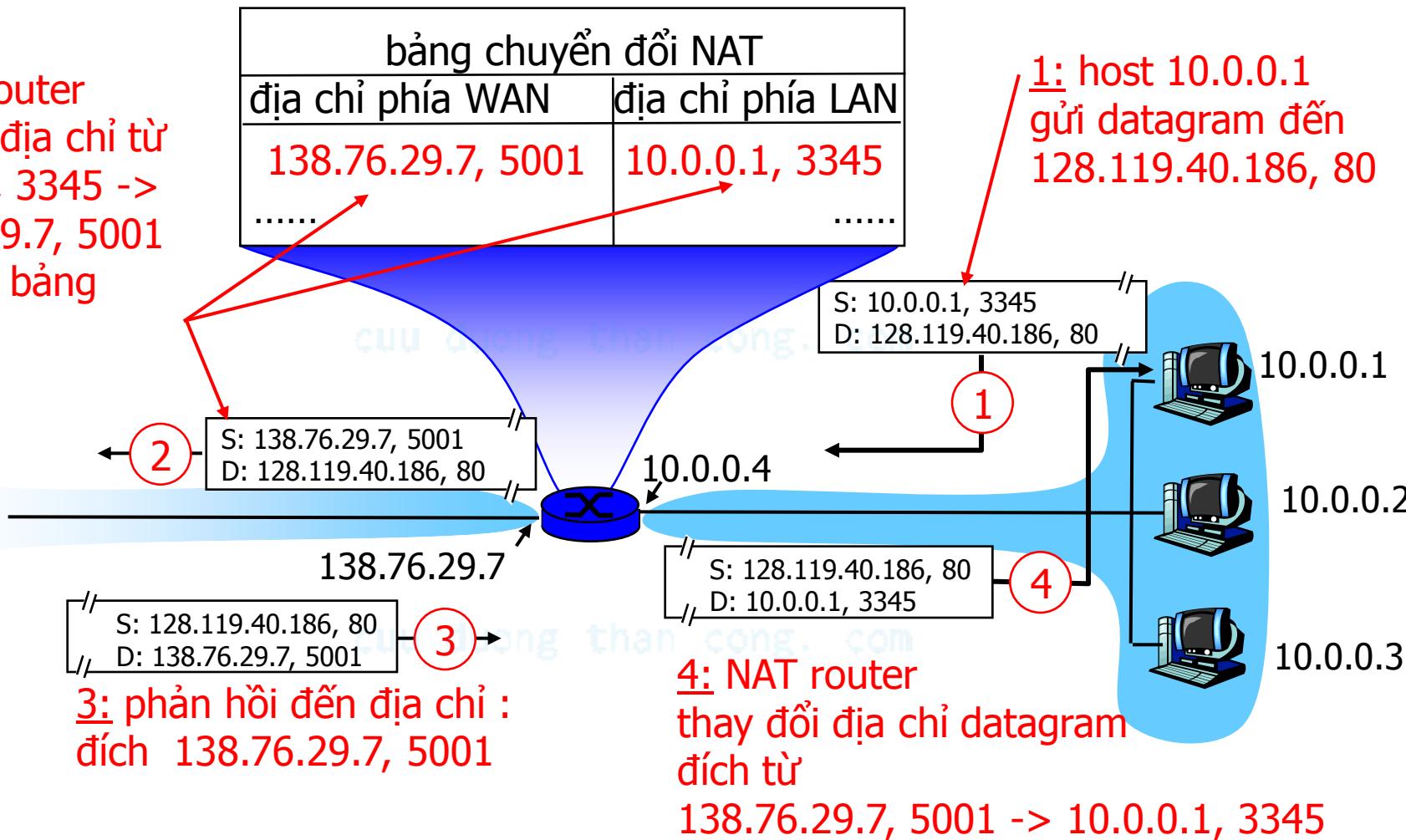
NAT

Hiện thực: NAT router phải:

- **các datagram đi ra:** thay thế (địa chỉ IP và số hiệu cổng nguồn) mọi datagram đi ra bên ngoài bằng (địa chỉ NAT IP và số hiệu cổng nguồn mới)
 - ... các clients/servers ở xa sẽ dùng (địa chỉ NAT IP và số hiệu cổng nguồn mới) đó như địa chỉ đích
- **ghi nhớ (trong bảng chuyển đổi NAT)** mọi cặp chuyển đổi (địa chỉ IP và số hiệu cổng nguồn) sang (địa chỉ NAT IP và số hiệu cổng nguồn mới)
- **các datagram đi đến:** thay thế (địa chỉ NAT IP và số hiệu cổng nguồn mới) trong các trường đích của mọi datagram đến với giá trị tương ứng (địa chỉ IP và số hiệu cổng nguồn) trong bảng NAT

NAT

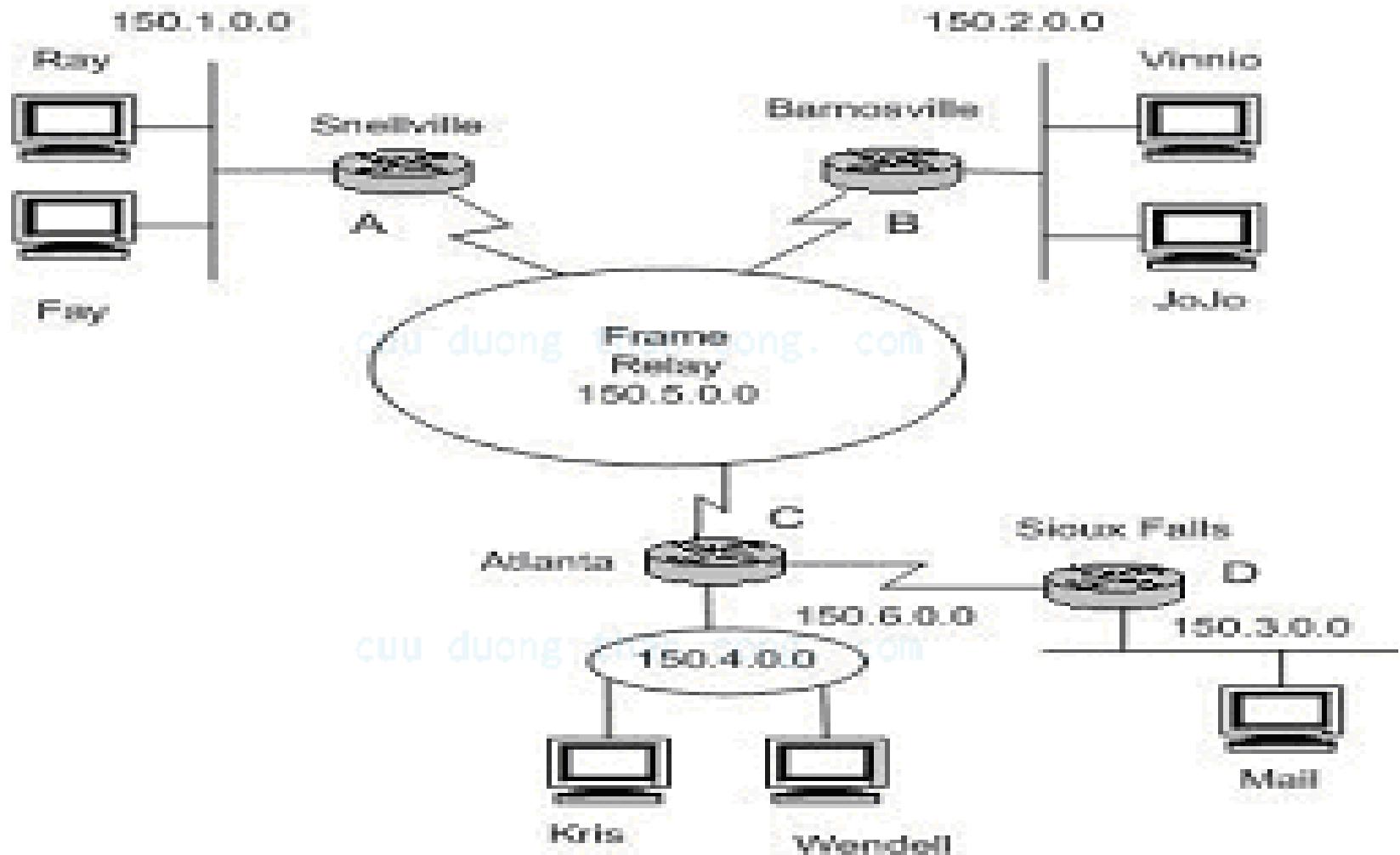
2: NAT router
thay đổi địa chỉ từ
10.0.0.1, 3345 ->
138.76.29.7, 5001
cập nhật bảng



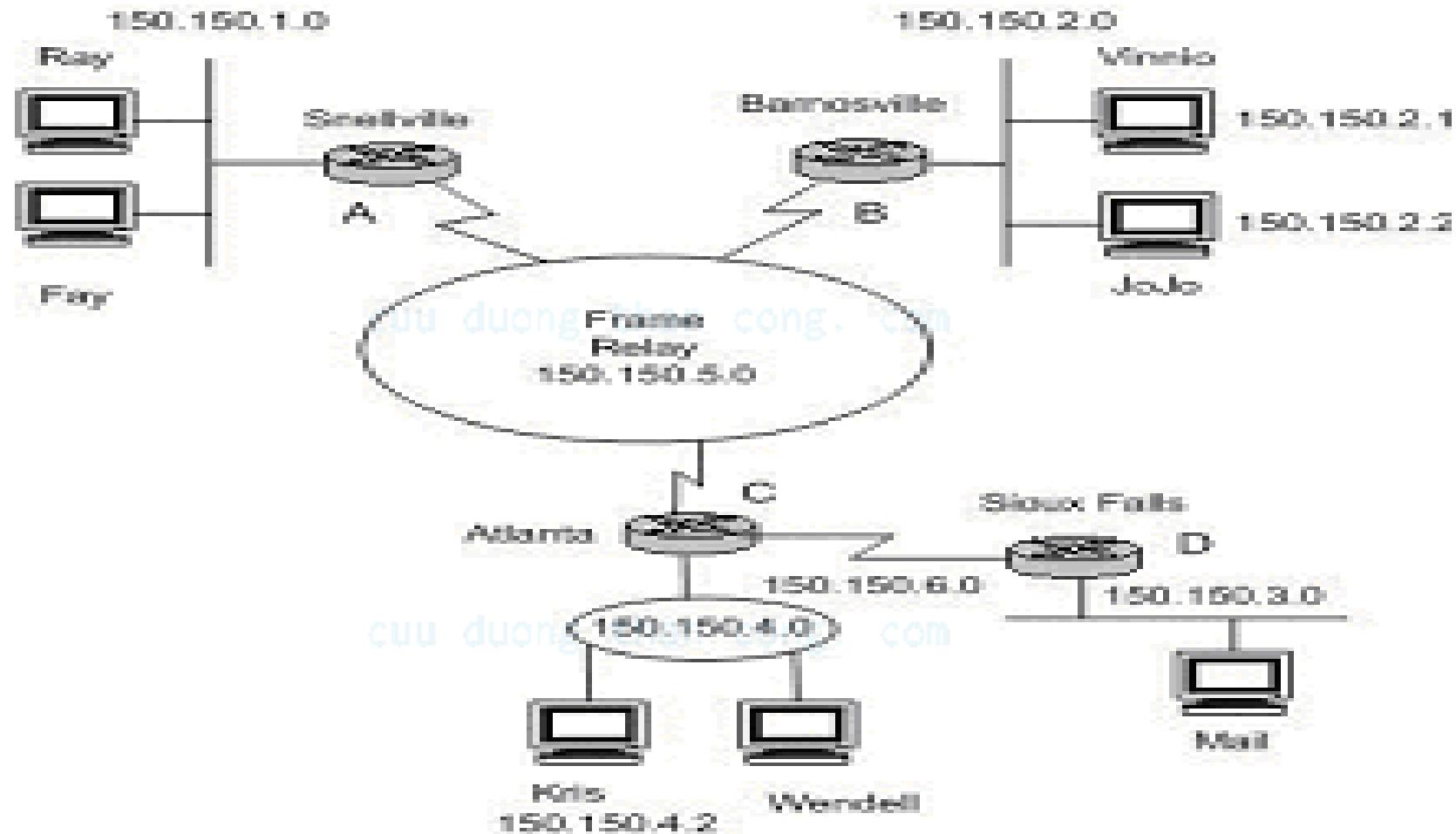
NAT

- Trường số hiệu cổng 16-bit:
 - Cho phép 60000 kết nối đồng thời chỉ với một địa chỉ phía WAN
- NAT còn có thể gây ra tranh luận:
 - các router chỉ xử lý đến lớp 3
 - vi phạm thỏa thuận end-to-end
 - những người thiết kế ứng dụng phải tính đến khả năng NAT, vd: Ứng dụng P2Pong. com
 - sự thiếu thốn địa chỉ IP sẽ được giải quyết khi dùng IPv6

Mạng con



Mạng con



Kỹ thuật chia mạng con

- Mượn một số bit trong phần host_id ban đầu để đặt cho các mạng con
- Cấu trúc của địa chỉ IP lúc này sẽ gồm 3 phần: network_id, subnet_id và host_id.

cuuduongthancong.com

Network	Subnet	Host	Class A
8	24-x	x	
Network	Subnet	Host	Class B
16	16-x	x	
Network	Subnet	Host	Class C
24	8-x	x	
Network	Subnet	Host	Class C

Kỹ thuật chia mạng con

- Số bit dùng trong subnet_id tuỳ thuộc vào chiến lược chia mạng con. Tuy nhiên số bit tối đa có thể mượn phải tuân theo công thức:

Subnet_id <= host_id - 2
- Số lượng bit tối đa có thể mượn:
 - Lớp A: **22** ($= 24 - 2$) bit \rightarrow chia được $2^{22} = 4194304$ mạng con
 - Lớp B: **14** ($= 16 - 2$) bit \rightarrow chia được $2^{14} = 16384$ mạng con
 - Lớp C: **06** ($= 8 - 2$) bit \rightarrow chia được $2^6 = 64$ mạng con

Kỹ thuật chia mạng con

- Số bit trong phần subnet_id xác định số lượng mạng con. Với số bit là x thì 2^x là số lượng mạng con có được.
- Ngược lại từ số lượng mạng con cần thiết, theo nhu cầu, tính được phần subnet_id cần bao nhiêu bit. Nếu muốn chia 6 mạng con thì cần 3 bit ($2^3=8$), chia 12 mạng con thì cần 4 bit ($2^4>=12$).

cuuduongthancong.com

Một số khái niệm mới

- Địa chỉ mạng con (địa chỉ đường mạng): gồm cả phần network_id và subnet_id, phần host_id chỉ chứa các bit 0
- Địa chỉ broadcast trong một mạng con: tất cả các bit trong phần host_id là 1.
- Mặt nạ mạng con (subnet mask): tất cả các bit trong phần host_id là 0, các phần còn lại là 1.

Quy ước ghi địa chỉ IP

- Nếu có địa chỉ IP như 172.29.8.230 thì chưa thể biết được host này nằm trong mạng nào, có chia mạng con hay không và có nêu chia thì dùng bao nhiêu bit để chia. Chính vì vậy khi ghi nhận địa chỉ IP của một host, phải cho biết subnet mask của nó
- Ví dụ: 172.29.8.230/255.255.255.0 hoặc 172.29.8.230/24 (có nghĩa là dùng 24 bit đầu tiên cho NetworkID).

Kỹ thuật chia mạng con

- Thực hiện 3 bước:
 - **Bước 1:** Xác định lớp (class) và subnet mask mặc nhiên của địa chỉ.
 - **Bước 2:** Xác định số bit cần mượn và subnet mask mới, tính số lượng mạng con, số host thực sự có được.
 - **Bước 3:** Xác định các vùng địa chỉ host và chọn mạng con muốn dùng

Bài tập 1

Cho địa chỉ IP sau: 172.16.0.0/16.

Hãy chia thành 8 mạng con và có
tối thiểu 1000 host trên mỗi
mạng con đó.

Bước 1: Xác định class và subnet mask mặc nhiên

Giải:

- Địa chỉ trên viết dưới dạng nhị phân
10101100.00010000.00000000.00000000
- Xác định lớp của IP trên:
Lớp B
- Xác định Subnet mask mặc nhiên:
255.255.0.0

Bước 2: Số bit cần mượn...

- Cần mượn bao nhiêu bit:

N = 3, bởi vì:

Số mạng con có thể: $2^3 = 8$.

Số host của mỗi mạng con có thể:

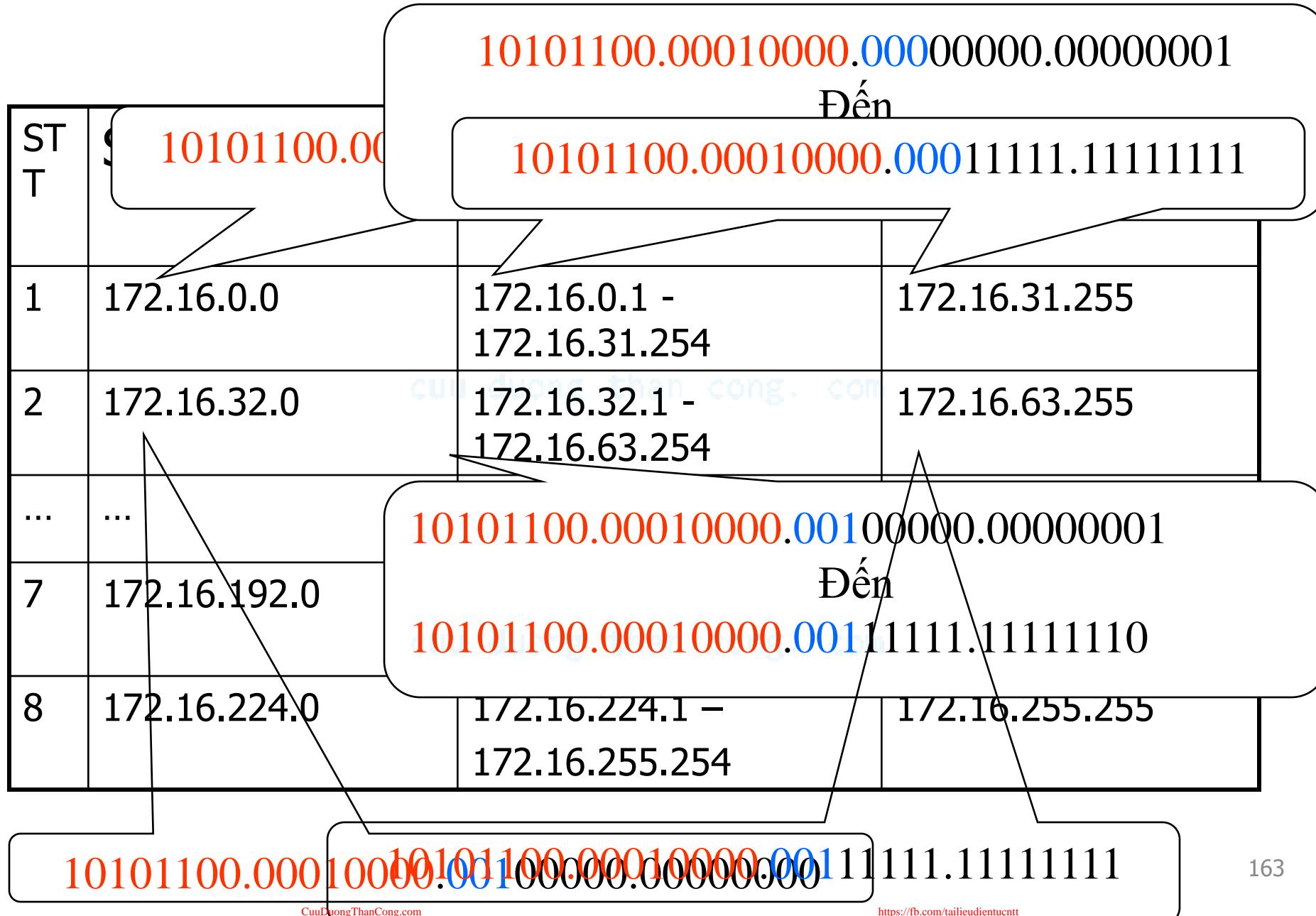
$$2^{(16-3)} - 2 = 2^{13} - 2 > 1000.$$

- Xác định Subnet mask mới:

11111111.11111111.11100000.00000000

hay 255.255.224.0

Bước 3: Xác định vùng địa chỉ host



Bài tập 2

Cho 2 địa chỉ IP sau:

192.168.5.9/28

192.168.5.39/28

- Hãy cho biết các địa chỉ network, host của từng IP trên?
- Các máy trên có cùng mạng hay không ?
- Hãy liệt kê tất cả các địa chỉ IP thuộc các mạng vừa tìm được?

Địa chỉ IP thứ nhất: 192.168.5.9/28

- Chú ý: 28 là số bit dành cho NetworkID
- Đây là IP thuộc lớp C
- Subnet mask mặc nhiên: 255.255.255.0

IP (thập phân)	192	168	5	9
IP (nhi phân)	11000000	10101000	00000101	00001001

Thực hiện AND địa chỉ IP với Subnet mask

IP	11000000	10101000	00000101	00001001
Subnet mask	11111111	11111111	11111111	11110000
Kết quả AND	11000000	10101000	00000101	00000000

Chuyển IP sang dạng thập phân

Kết quả AND	11000000	10101000	00000101	00000000
Net ID	192	168	5	0
Host ID			0000 <u>1001</u>	9

Địa chỉ IP thứ hai: 192.168.5.39/28

IP	192	168	5	39
IP (nhị phân)	11000000	10101000	00000101	00100111
Subnet Mask	11111111	11111111	11111111	11110000
AND	11000000	10101000	00000101	00100000
Network ID	192	168	5	32
HostID				7

Hai địa chỉ trên có cùng mạng?

- 192.168.5.9/28
- 192.168.5.39/28

Kết luận: Hai địa chỉ trên không cùng mạng

Net ID của địa chỉ thứ 1	192	168	5	0
Net ID của địa chỉ thứ 2	192	168	5	32

Liệt kê tất cả các địa chỉ IP

Mạng tương ứng với IP	Vùng địa chỉ HostID với dạng nhị phân <i>cuuduongthancong.com</i>	Vùng địa chỉ HostID với dạng thập phân
1	11000000.10101000.00000101.00000001 Đến 11000000.10101000.00000101.00001110	192.168.5.1/28 Đến 192.168.5.14/28
2	11000000.10101000.00000101.00100001 Đến 11000000.10101000.00000101.00101110	192.168.5.33/28 Đến 192.168.5.46/28

Bài tập 3

Hãy xét đến một địa chỉ IP class B, **139.12.0.0**, với subnet mask là **255.255.0.0**. Một Network với địa chỉ thế này có thể chứa 65534 nodes hay computers. Đây là một con số quá lớn, trên mạng sẽ có đầy broadcast traffic. Hãy chia network thành 5 mạng con.

cuuduongthancong.com

Bước 1: Xác định Subnet mask

- Để chia thành 5 mạng con thì cần thêm 3 bit (vì $2^3 > 5$).
- Do đó Subnet mask sẽ cần: 16 (bits trước đây) + 3 (bits mới) = 19 bits
- Địa chỉ IP mới sẽ là **139.12.0.0/19** (để ý con số **19** thay vì **16** như trước đây).

Bước 2: Liệt kê ID của các Subnet mới

Subnet mask với dạng nhị phân

11111111.11111111.11100000.00000000

Subnet mask
với dạng thập
phân

255.255.224.0

NetworkID của bốn Subnets mới

TT	Subnet ID với dạng nhị phân <i>cuuduongthancong.com</i>	Subnet ID với dạng thập phân
1	10001011.00001100.00000000.00000000	139.12.0.0/19
2	10001011.00001100.00100000.00000000	139.12.32.0/19
3	10001011.00001100.01000000.00000000	139.12.64.0/19
4	10001011.00001100.01100000.00000000	139.12.96.0/19
5	10001011.00001100.10000000.00000000	139.12.128.0/19

Bước 3: Cho biết vùng địa chỉ IP của các HostID

TT	Dạng nhị phân	Dạng thập phân
1	10001011.00001100.00000000.00000001 10001011.00001100.00011111.11111110	139.12.0.1/19 - 139.12.31.254/19
2	10001011.00001100.00100000.00000001 10001011.00001100.00111111.11111110	139.12.32.1/19 - 139.12.63.254/19
3	10001011.00001100.01000000.00000001 10001011.00001100.01011111.11111110	139.12.64.1/19 - 139.12.95.254/19
4	10001011.00001100.01100000.00000001 10001011.00001100.01111111.11111110	139.12.96.1/19 - 139.12.127.254/19
5	10001011.00001100.10000000.00000001 10001011.00001100.10011111.11111110	139.12.128.1/19 - 139.12.159.254/19

Tính nhanh vùng địa chỉ IP

- n – số bit làm subnet
- Số mạng con: $S = 2^n$
- Số gia địa chỉ mạng con: $M = 2^{8-n}$ ($n \leq 8$)
- Byte cuối của IP địa chỉ mạng, ví dụ lớp C: $(k-1)*M$ (với $k=1,2,\dots$)
- Byte cuối của IP host đầu tiên, ví dụ lớp C: $(k-1)*M + 1$ (với $k=1,2,\dots$)
- Byte cuối của IP host cuối cùng, ví dụ lớp C: $k*M - 2$ (với $k=1,2,\dots$)
- Byte cuối của IP broadcast, ví dụ lớp C: $k*M - 1$ (với $k=1,2,\dots$)

Ví dụ tính nhanh vùng địa chỉ IP

- Cho địa chỉ: 192.168.0.0/24
- Với $n=4 \rightarrow M= 16 (= 2^{8-4}) \rightarrow$
 - Network 1: 192.168.0.0. Host range: 192.168.0.1–192.168.0.14. Broadcast: 192.168.0.15
 - Network 2: 192.168.0.16. Host range: 192.168.0.17–192.168.0.30. Broadcast: 192.168.0.31
 - Network 3: 192.168.0.32. Host range: 192.168.0.33–192.168.0.46. Broadcast: 192.168.0.47
 - Network 4: 192.168.0.48. Host range: 192.168.0.49–192.168.0.62. Broadcast: 192.168.0.63

Bài tập 4

- Cho địa chỉ IP: 102.16.10.107/12
 - Tìm địa chỉ mạng con? Địa chỉ host
 - Dải địa chỉ host có cùng mạng với IP trên?
 - Broadcast của mạng mà IP trên thuộc vào?

Bước: Tính subnet mask

- 102.16.10.107/12 →
- Subnet mask:
 $11111111.11110000.00000000.00000000$
- Byte đầu tiên chắc chắn khi dùng phép toán AND ra kết quả bằng 102 → không cần đổi 102 sang nhị phân

Trả lời câu hỏi 1: Địa chỉ mạng con?

- Xét byte kế tiếp là: 16 (10) → **0001**0000 (2)
- Khi AND byte này với Subnet mask, ta được kết quả là: **0001**0000 (2)
- Như vậy địa chỉ mạng con sẽ là:

102.16.0.0/12

- Như vậy địa chỉ host sẽ là:

0.10.107

Trả lời câu hỏi 2: Dải địa chỉ host? Broadcast?

- Dải địa chỉ host sẽ từ:

**01100110 00010000 00000000 00000001
(hay 102.16.0.1/12)**

Đến:

cuu duong than cong. com

**01100110 00011111 11111111 11111110
(hay 102.31.255.254/12)**

- Broadcast:

cuu duong than cong. com

102.31.255.255/12

Bài tập 5: Cho IP 172.19.160.0/21

- Chia làm 4 mạng con
- Liệt kê các thông số gồm địa chỉ mạng, dãy địa chỉ host, địa chỉ broadcast của các mạng con đó

cuu duong than cong. com

Giải BT 5

- Chia làm 4 mạng con nên phải mượn 2 bit
- Do /21 nên 2 byte đầu tiên của IP đã cho không thay đổi. Xét byte thứ 3
 - $160 = \textcolor{red}{10100}\underline{\textcolor{blue}{00}}0_{(2)}$
 - Phần 2 bit 00 là nơi ta mượn làm subnet

Giải BT 5 (tt)

- Xét byte thứ 3
- Mạng con thứ 1: 1010000_2
- Mạng con thứ 2: 1010001_2
- Mạng con thứ 3: 1010010_2
- Mạng con thứ 4: 1010011_2

cuu duong than cong. com

Giải BT 5 (tt)

Địa chỉ mạng	Dải địa chỉ host	Địa chỉ broadcast
172.19.160.0	172.19.160.1 đến 172.19.161.254	172.19.161.255
172.19.162.0	172.19.162.1 đến 172.19.163.254	172.19.163.255
172.19.164.0	172.19.164.1 đến 172.19.165.254	172.19.165.255
172.19.166.0	172.19.166.1 đến 172.19.167.254	172.19.167.255

Bài tập 6: Cho IP 172.16.192.0/18

- Chia làm 4 mạng con
- Liệt kê các thông số gồm địa chỉ mạng, dãy địa chỉ host, địa chỉ broadcast của các mạng con đó

cuu duong than cong. com

Giải BT 6

- Chia làm 4 mạng con nên phải mượn 2 bit
- Do /18 nên 2 byte đầu tiên của IP đã cho không thay đổi. Xét byte thứ 3
 - $192 = \textcolor{red}{11}\underline{\textcolor{blue}{00}}0000_{(2)}$
 - Phần 2 bit 00 là nơi ta mượn làm subnet

Giải BT 6 (tt)

- Xét byte thứ 3
- Mạng con thứ 1: $11000000_{(2)}$
- Mạng con thứ 2: $11010000_{(2)}$
- Mạng con thứ 3: $11100000_{(2)}$
- Mạng con thứ 4: $11110000_{(2)}$

cuu duong than cong. com

Giải BT 6 (tt)

Địa chỉ mạng	Dải địa chỉ host	Địa chỉ broadcast
172.16.192.0	172.16.192.1 đến 172.16.207.254	172.16.207.255
172.16.208.0	172.16.208.1 đến 172.16.223.254	172.16.223.255
172.16.224.0	172.16.224.1 đến 172.16.239.254	172.16.239.255
172.16.240.0	172.16.240.1 đến 172.16.255.254	172.16.255.255

CHƯƠNG 6: BẢO MẬT MẠNG

- Hiểu các nguyên lý của bảo mật mạng:
 - mật mã
 - chứng thực
 - tính toàn vẹn
 - khóa phân bố
- Bảo mật trong thực tế:
 - các firewall
 - bảo mật trong các lớp application, transport, network, data-link

Bảo mật mạng là gì?

Sự bảo mật: chỉ có người gửi, người nhận mới “hiểu” được nội dung thông điệp

- người gửi mã hóa thông điệp
- người nhận giải mã thông điệp

Chứng thực: người gửi, người nhận xác định là nhận ra nhau

Sự toàn vẹn thông điệp: người gửi, người nhận muốn bảo đảm thông điệp không bị thay đổi (trên đường truyền hoặc sau khi nhận)

Truy cập & tính sẵn sàng: các dịch vụ phải có khả năng truy cập và sẵn sàng đối với các user

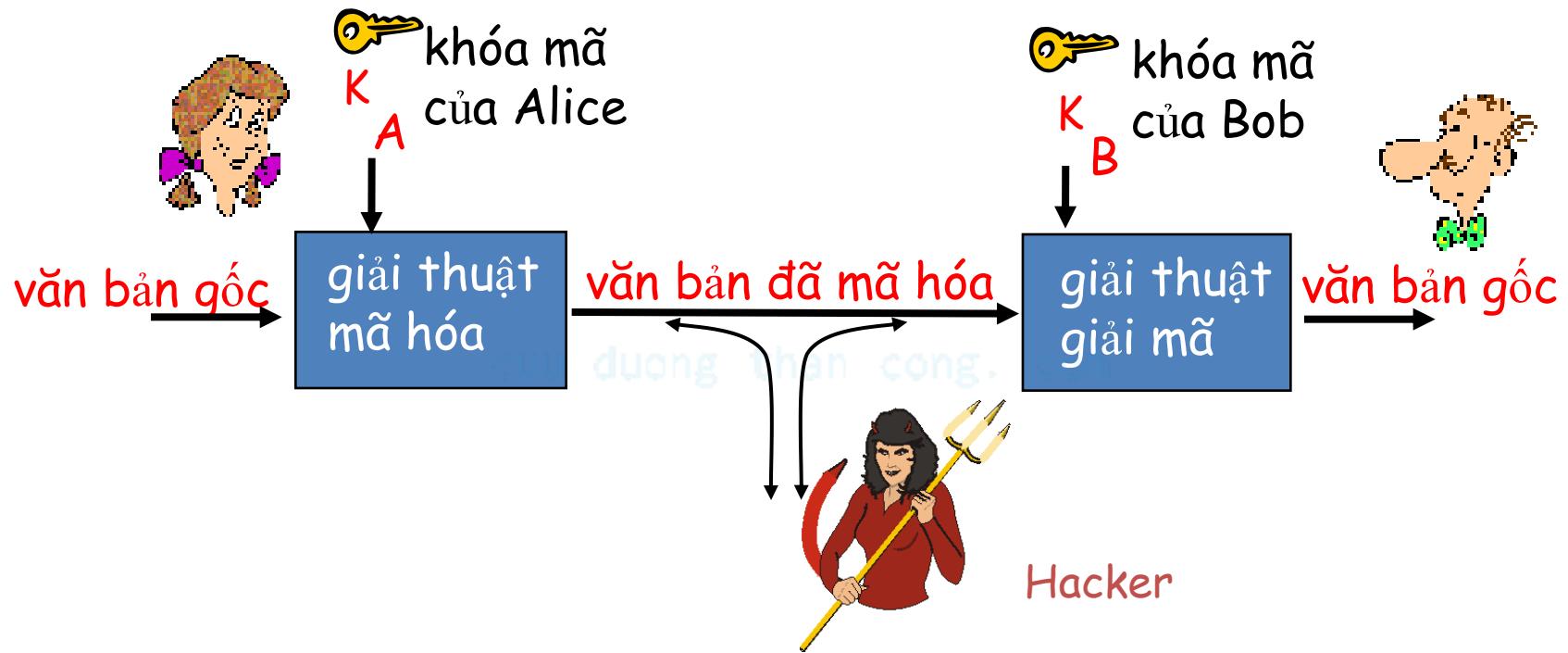
Các đối tượng cần bảo mật

- Trình duyệt Web/server cho các giao dịch điện tử
- Client/Server ngân hàng trực tuyến
- DNS servers *cuu duong than cong. com*
- Các router trao đổi thông tin cập nhật bảng routing
- .v.v. *cuu duong than cong. com*

Kẻ xấu có thể làm những việc gì?

- **nghe lén:** ngăn chặn các thông điệp
- kích hoạt **chèn** các thông điệp vào trong kết nối
- **giả danh:** có thể giả mạo địa chỉ nguồn trong gói (hoặc bất kỳ trường nào trong đó)
- **cướp:** “tiếp tục” kết nối hiện hành nhưng thay người gửi hoặc người nhận bằng chính họ
- **tù chối dịch vụ:** dịch vụ hiện tại bị người khác dùng (đồng nghĩa quá tải)
- .v.v.

Các nguyên lý mã hóa



khóa đối xứng: khóa bên gửi và bên nhận giống nhau

khóa công cộng: khóa mã chung, khóa giải mã bí mật (riêng)

Mã hóa khóa đối xứng

mật mã thay thế: thay thứ này thành thứ khác

– mã hóa ký tự đơn: thay thế từng ký tự một

văn bản gốc: abcdefghijklmnopqrstuvwxyz

văn bản đã mã hóa: mnbvcxzasdfghjklpoiuytrewq

ví dụ: văn bản gốc: Bob. i love you. Alice

mã hóa thành: nko. s gktc wky. mgsbc

• Bẻ khóa kiểu mã hóa đơn giản này dễ không?

- brute force (khó như thế nào?)
- khác?

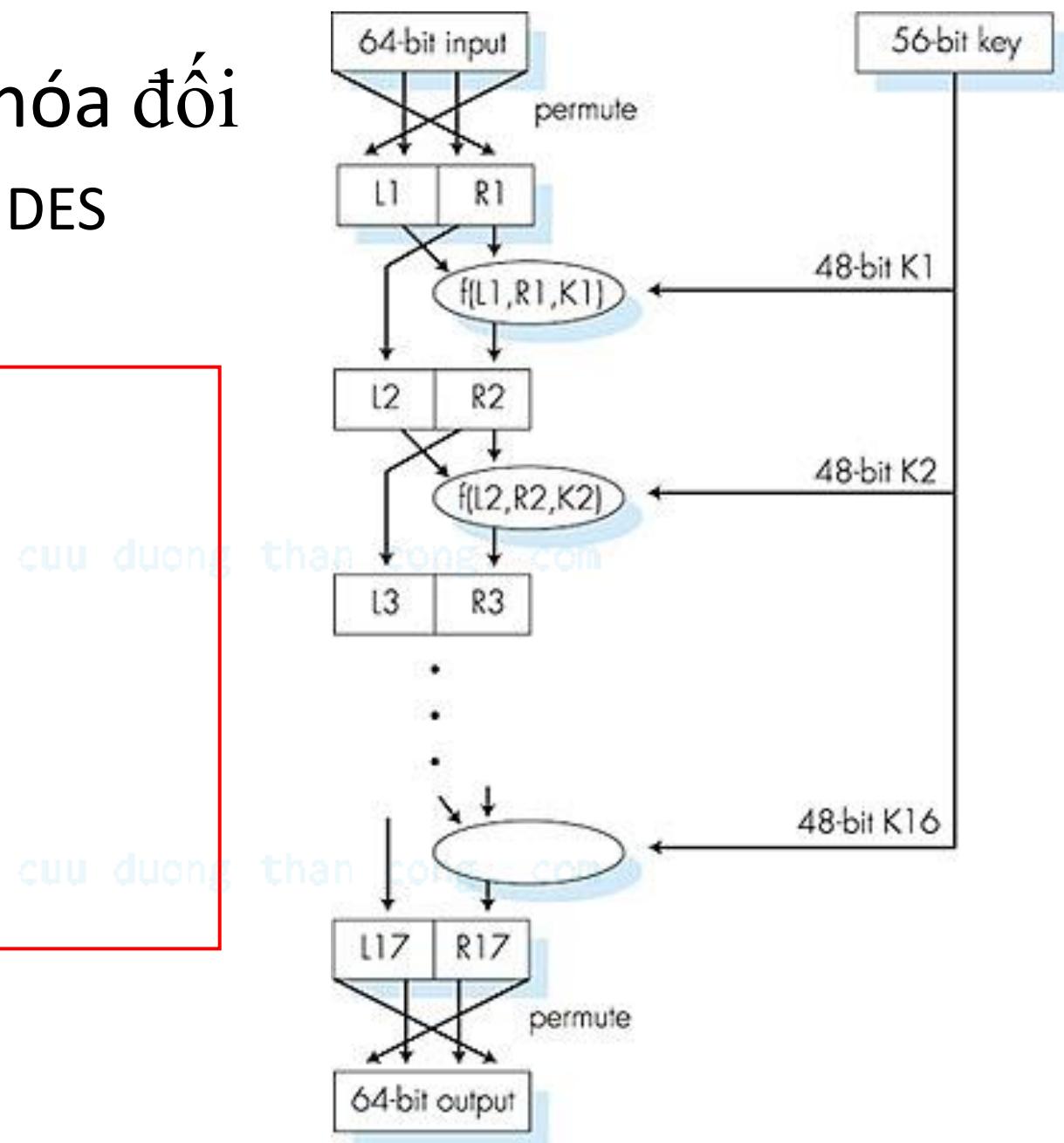
Mã hóa khóa đối xứng: DES

DES: Data Encryption Standard

- Chuẩn mã hóa của Hoa Kỳ [NIST 1993]
- Khóa đối xứng 56-bit, văn bản gốc vào 64-bit
- Bảo mật trong DES như thế nào?
 - chưa có cách tiếp cận “backdoor-cửa sau” để giải mã
- làm cho DES bảo mật hơn:
 - dùng 3 khóa tuần tự (3-DES) trong mỗi datum
 - dùng cơ chế liên kết khối mã

Mã hóa khóa đối xứng: DES

DES hoạt động



AES: Advanced Encryption Standard

- Chuẩn NIST khóa đối xứng mới (tháng 11-2001) thay thế cho DES
- Dữ liệu xử lý từng khối 128 bit
- Các khóa 128, 192 hoặc 256 bit
- Giải mã brute force (thử sai) tốn 1s với DES, tốn 149 tỷ tỷ năm với AES

cuu duong than cong. com

Mã hóa khóa công cộng

khóa đối xứng

- yêu cầu người gửi, người nhận phải biết khóa công cộng
- Làm sao biết khóa công cộng đó trong lần đầu tiên (đặc biệt với những người chưa bao giờ gặp trước)?

Mã hóa khóa công cộng

- tiếp cận khác hoàn toàn
- người gửi, người nhận không chia sẻ khóa công cộng
- khóa công cộng cho mọi người đều biết
- khóa giải mã riêng chỉ có người nhận biết

Giải thuật mã hóa khóa công cộng

Yêu cầu:

- ① cần K_B^t và $K_B^.$ như sau:

$$K_B^-(K_B^+(m)) = m$$

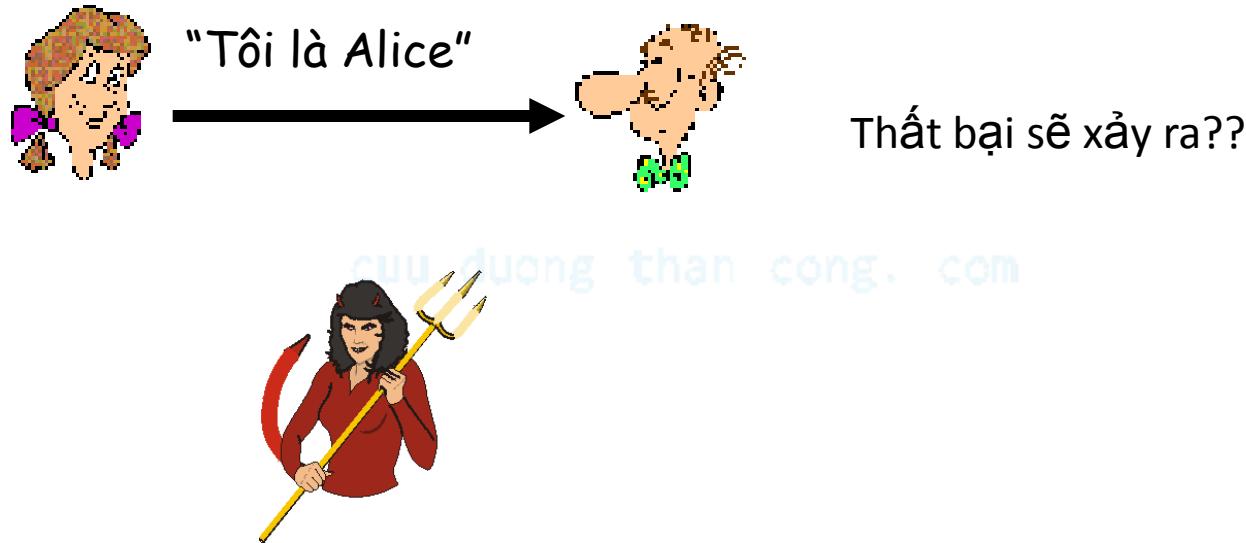
- ② cho khóa công cộng K_B^+ , phải không thể tính toán ra được khóa riêng K_B^-

giải thuật RSA: Rivest, Shamir, Adelson

Sự chứng thực

Mục tiêu: Bob muốn Alice “chứng thực”
nhân dạng của cô đối với anh ta

Mô tả cách thức hiện thực: Alice nói “Tôi là Alice”



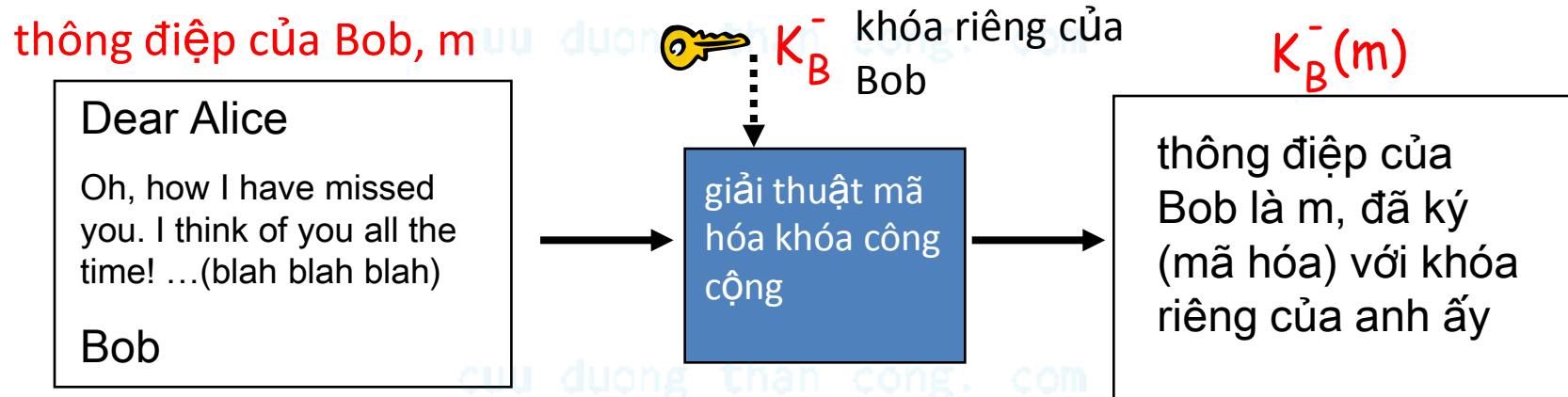
Sự toàn vẹn

- Chữ ký số: Kỹ thuật mã hóa tương tự như các chữ ký bằng tay.
 - người gửi (Bob) đánh dấu (số hóa) tài liệu, thiết lập thuộc tính là người sở hữu/tạo lập tài liệu.
 - có thể kiểm tra, không thể làm giả: người nhận (Alice) có thể chứng thực với người khác là chỉ có Bob chứ ngoài ra không có ai (kể cả Alice) đã ký trên tài liệu đó.

Chữ ký số

Chữ ký số đơn giản cho thông điệp m:

- Bob ký m bằng cách mã hóa với khóa riêng của anh ấy K_B^- , tạo thông điệp “đã được ký”, $K_B^-(m)$



Chữ ký số (tt)

- Giả sử Alice nhận được m , với chữ ký số hóa là $K_B(m)$
- Alice kiểm tra m đã được ký bởi Bob bằng cách áp dụng khóa công cộng của Bob là K_B cho $K_B(m)$ sau đó kiểm tra $K_B(K_B(m)) = m$.
- Nếu $K_B(K_B(m)) = m$, bất cứ ai đã ký m phải dùng khóa riêng của Bob

Alice kiểm tra:

- ✓ Bob đã ký m .
- ✓ Không có ai khác đã ký m .
- ✓ Bob đã ký m và không ký m' .

Không thể phủ nhận:

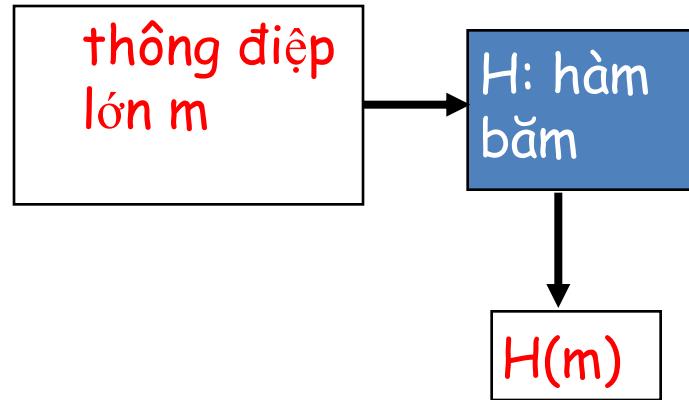
- ✓ Alice có thể giữ m và chữ ký $K_B(m)$ để chứng thực rằng Bob đã ký m .

Phân loại thông điệp

Tính toán các thông điệp dài
có chi phí đắt

Mục tiêu: “dấu tay” số hóa có
kích thước cố định, dễ
tính toán được

- áp dụng hàm băm H vào
m, tính được phân loại
thông điệp kích thước cố
định, $H(m)$.



Các đặc tính hàm băm:

- nhiều-một
- sinh ra phân loại thông điệp
kích thước cố định (“dấu
tay”)
- cho phân loại thông điệp x,
không thể tính toán để tìm
m dùng $x = H(m)$

Khóa phân bố và chứng chỉ

Vấn đề khóa đối xứng:

- Làm thế nào 2 thực thể cùng thiết lập khóa bí mật trên mạng?

Giải pháp:

- Trung tâm phân bố khóa (key distribution center-KDC) được tin cậy – hoạt động trung gian giữa các thực thể

Vấn đề khóa công cộng:

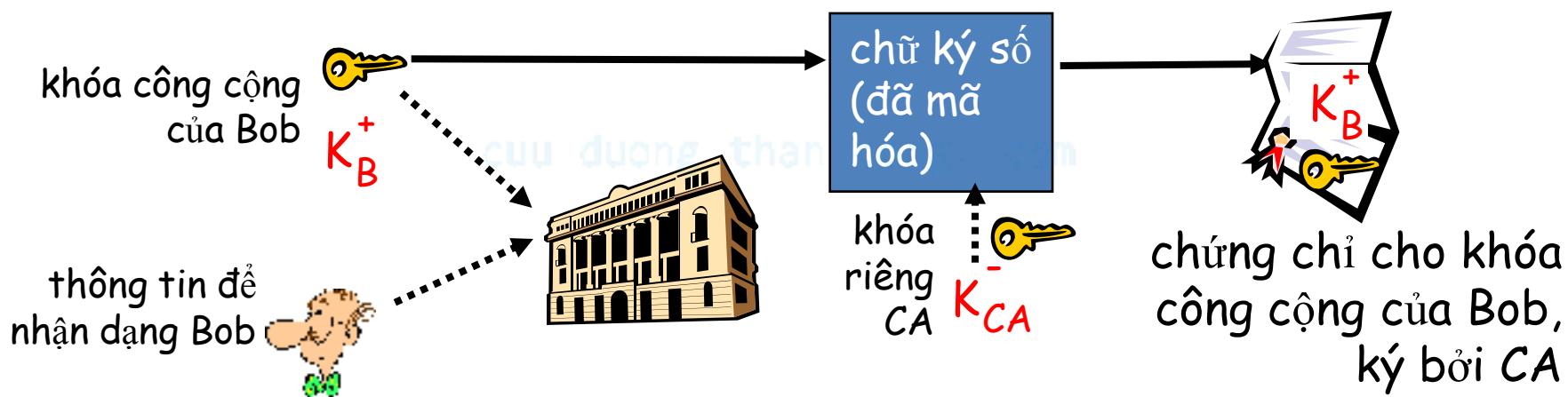
- Khi Alice lấy được khóa công cộng của Bob (từ web site, email, đĩa) làm sao biết khóa công cộng của Bob chứ không phải của Hacker?

Giải pháp:

- Nơi cấp chứng chỉ (certification authority-CA) được tin cậy

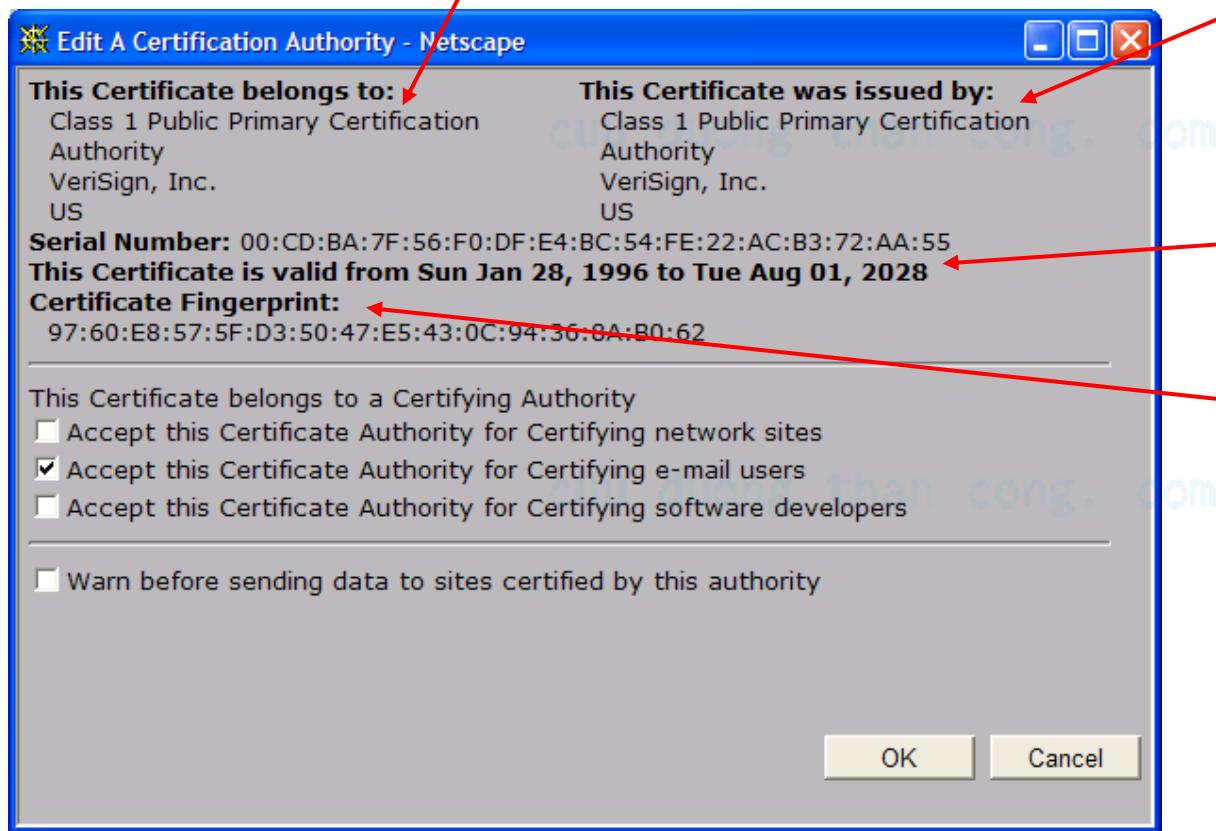
Cấp chứng chỉ

- **Certification authority (CA):** gắn kết khóa công cộng với thực thể E nào đó.
- E (người, router) đăng ký khóa công cộng của họ với CA.
 - E cung cấp “bằng chứng để nhận dạng” cho CA.
 - CA tạo ra chứng chỉ ràng buộc E với khóa công cộng của nó.
 - chứng chỉ chứa khóa công cộng của E được ký số bởi CA – CA nói “đây là khóa công cộng của E”



Mô tả chứng chỉ

- Số thứ tự (duy nhất)
- thông tin về người sở hữu chứng chỉ, bao gồm giải thuật và chính giá trị khóa (không hiển thị ra)



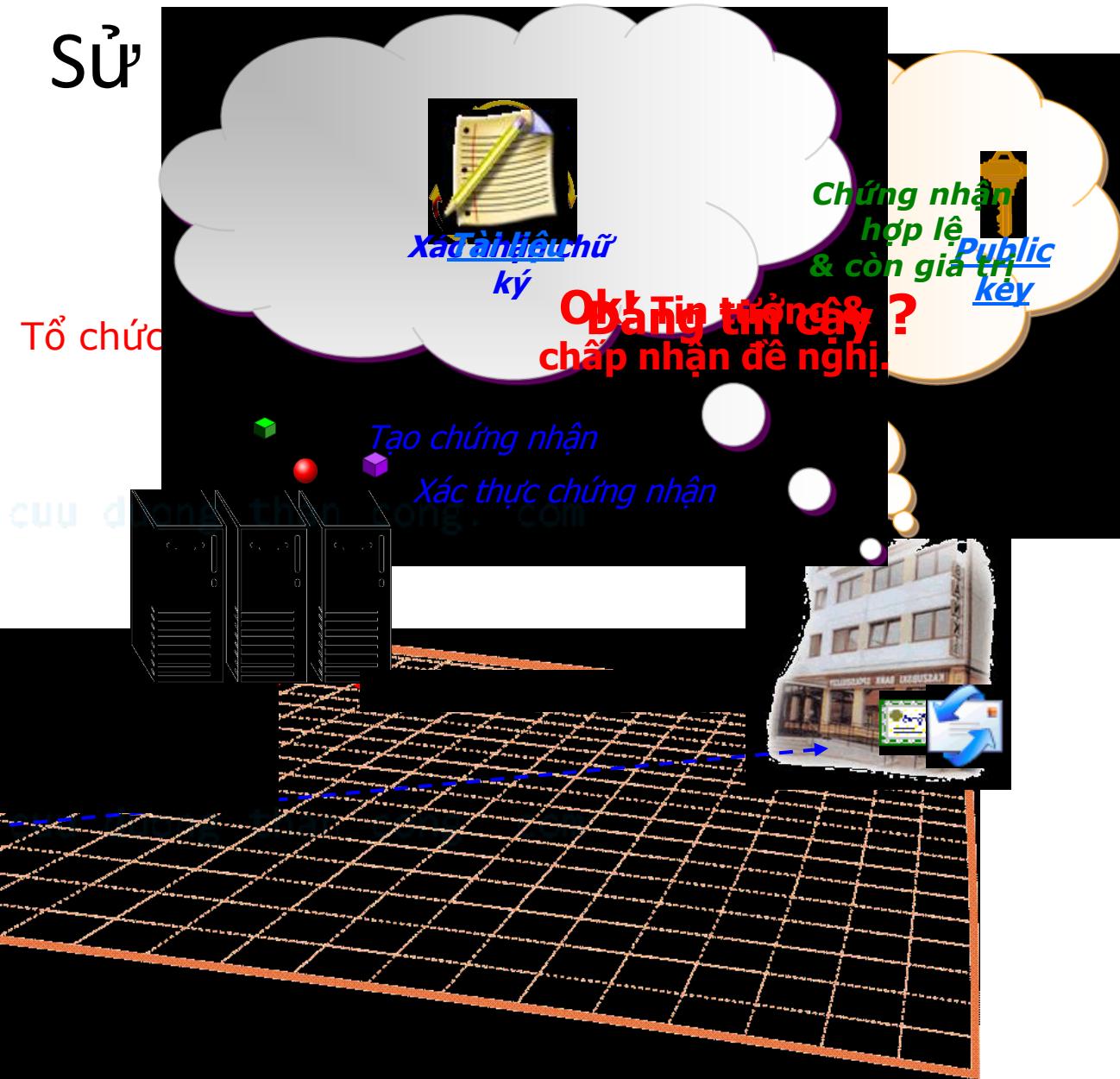
- thông tin về người phát hành chứng chỉ
- ngày kiểm tra tính hợp lệ
- chữ ký số bởi người phát hành chứng chỉ

Sử

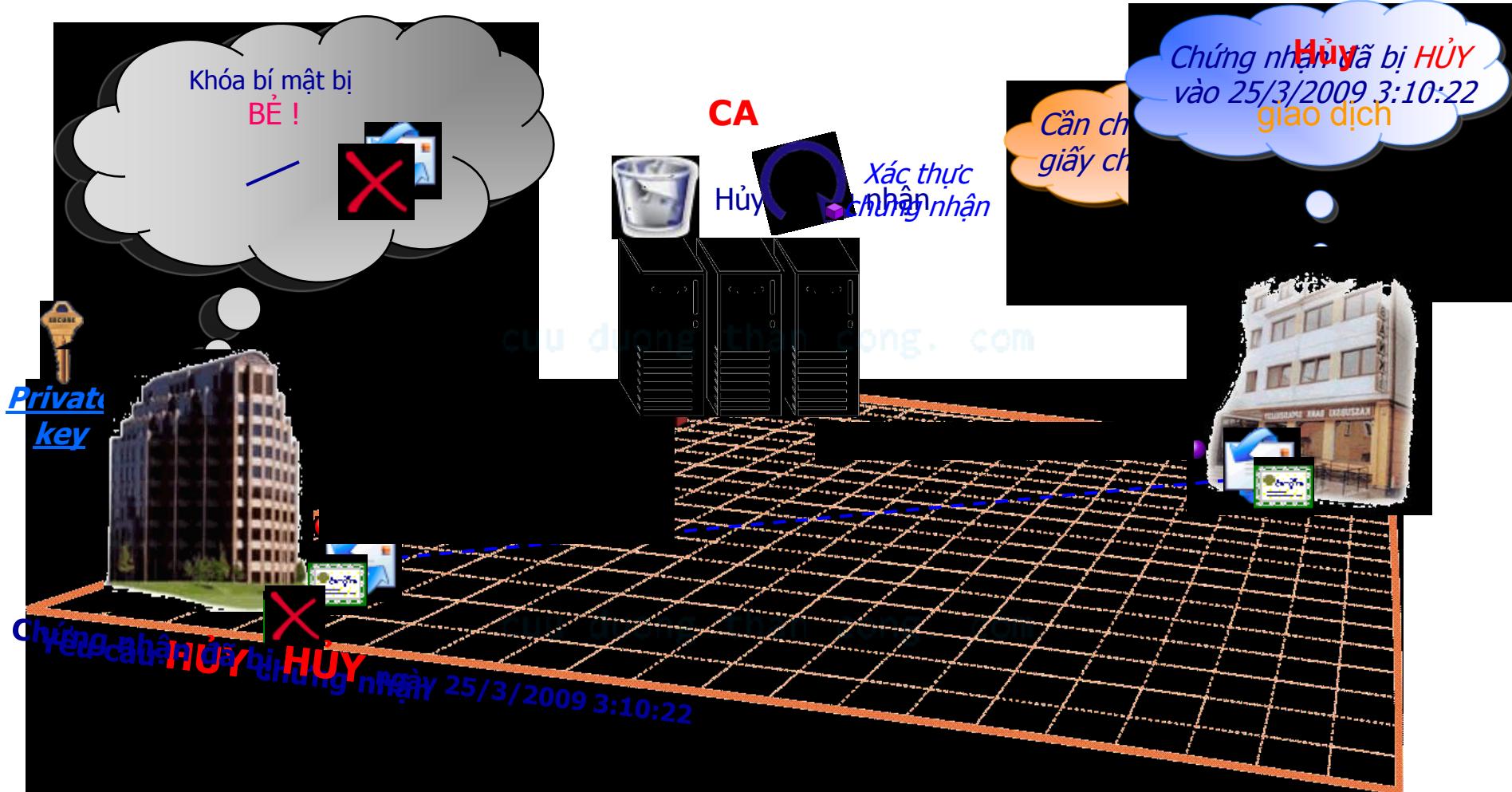
Tổ chức

cuu duong than cong.com

Ký
&
Mã hóa
Private key
và
nhéo
n X.509
key



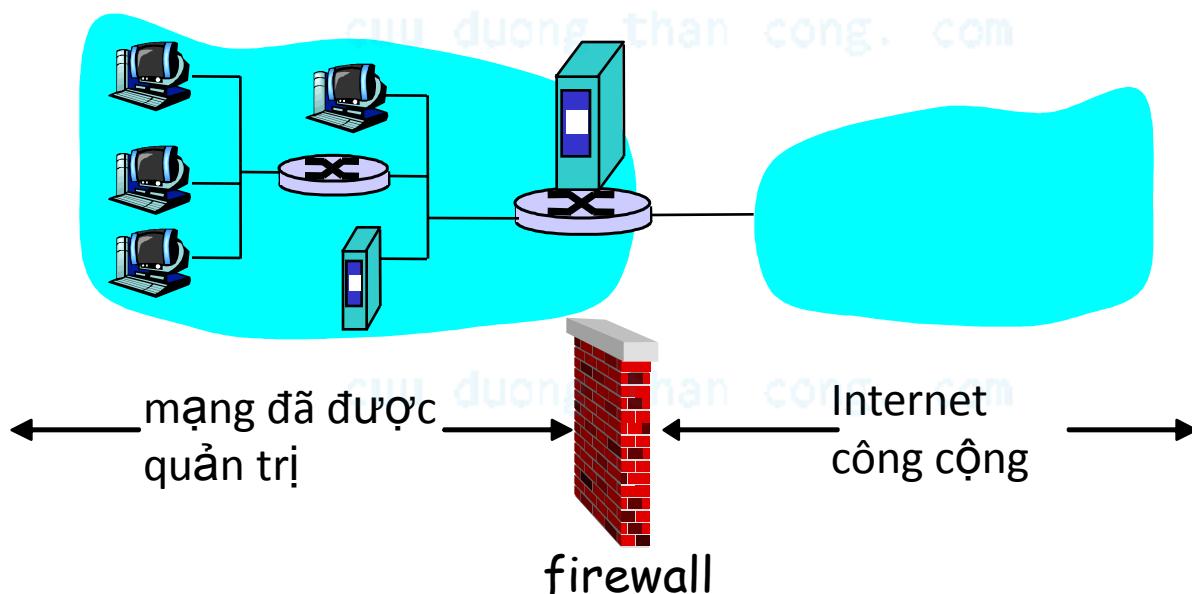
Sử dụng chứng chỉ



Các Firewall-Tường lửa

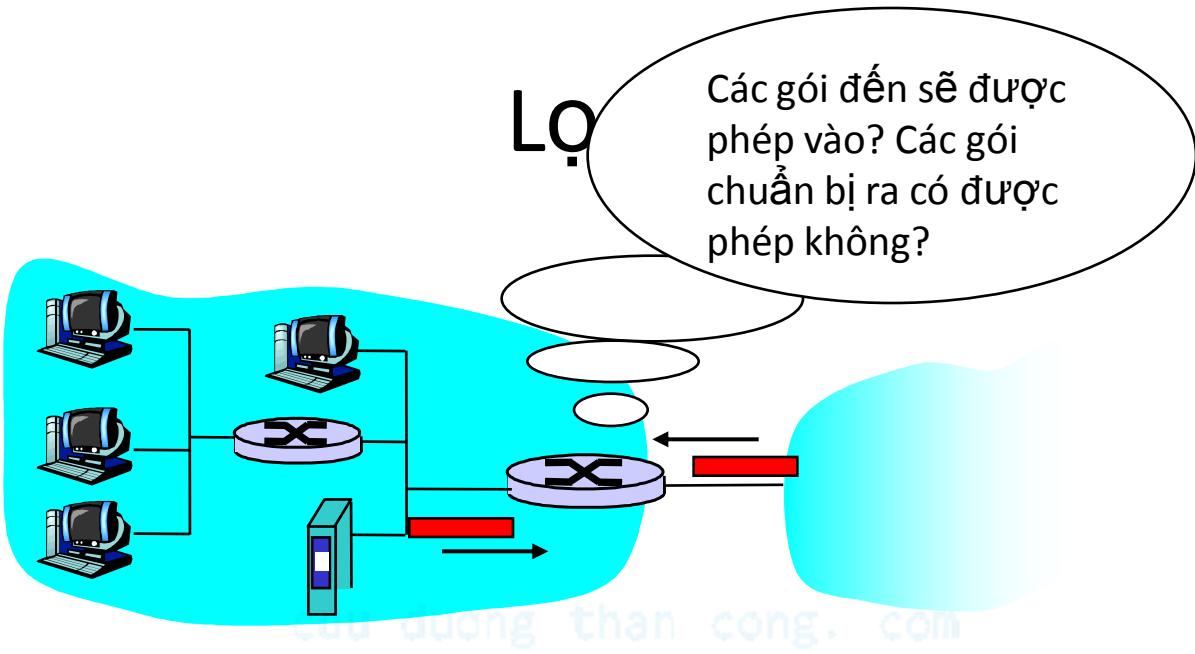
firewall

cô lập mạng nội bộ của tổ chức với Internet, cho phép một số gói được truyền qua, ngăn chặn các gói khác



Firewall: Tại sao phải dùng?

- Ngăn chặn các cuộc tấn công từ chối dịch vụ Denial Of Service (DoS):
 - SYN flooding: kẻ tấn công thiết lập nhiều kết nối TCP “ảo”, không còn tài nguyên cho các kết nối “thật”
- Ngăn chặn việc sửa đổi/truy cập bất hợp pháp các dữ liệu nội bộ.
 - Ví dụ: kẻ tấn công thay thế trang chủ của CIA bằng trang nào đó
- Chỉ cho phép các truy cập hợp pháp vào bên trong mạng (tập hợp các host/user được chứng thực)
- 2 kiểu firewall:
 - mức ứng dụng
 - lọc gói tin



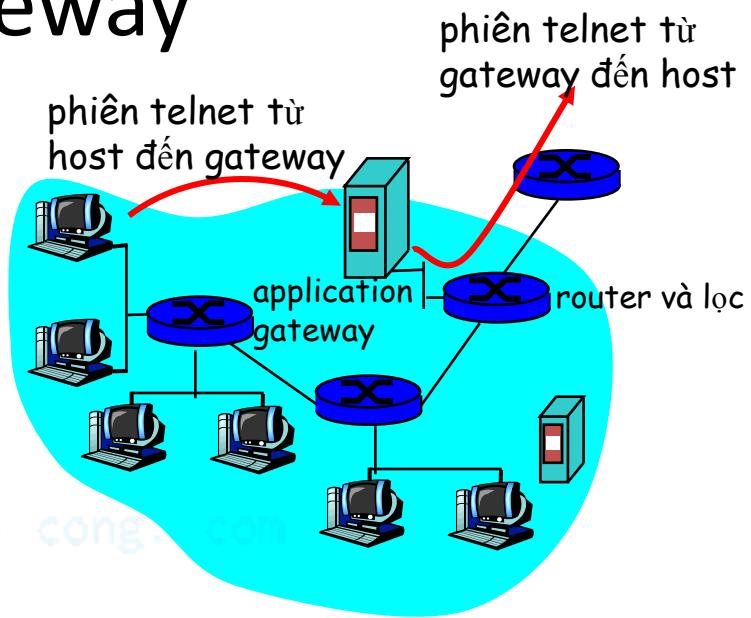
- mạng nội bộ kết nối với Internet thông qua **router firewall**
- router **lọc từng gói một**, xác định chuyển tiếp hoặc bỏ các gói dựa trên:
 - địa chỉ IP nguồn, địa chỉ IP đích
 - các số hiệu port TCP/UDP nguồn và đích
 - kiểu thông điệp ICMP
 - các bit TCP SYN và ACK

Lọc gói tin

- Ví dụ 1: chặn các datagram đến và đi với trường giao thức IP = 17 và port nguồn hoặc đích = 23.
 - Tất cả các dòng UDP đến/đi và các kết nối telnet đều bị chặn lại.
- Ví dụ 2: chặn các đoạn Block TCP với ACK=0.
 - Ngăn chặn các client bên ngoài tạo các kết nối TCP với các client bên trong, nhưng cho phép các client bên trong kết nối ra ngoài.

Các Ứng dụng gateway

- Lọc các gói trên dữ liệu ứng dụng cũng như các trường IP/TCP/UDP.
- Ví dụ: cho phép chọn các user bên trong được telnet ra ngoài.



1. yêu cầu tất cả các user phải telnet thông qua gateway
2. với các user đã được cấp phép, gateway thiết lập kết nối với host đích. gateway tiếp vận dữ liệu giữa 2 kết nối.
3. Router lọc và chặn tất cả các kết nối telnet không xuất phát từ gateway.

Các hạn chế của các firewall và gateway

- giả mạo IP: router không thể biết dữ liệu có thực sự đến từ nguồn tin cậy hay không
- nếu nhiều ứng dụng cần đối xử đặc biệt, mỗi cái sở hữu gateway riêng...
- phần mềm client phải biết cách tiếp xúc với gateway.
 - ví dụ: phải thiết lập địa chỉ IP của proxy trong trình duyệt Web
- các lọc thường dùng tắt cả hoặc không có chính sách nào dành cho UDP
- sự cân bằng: **mức độ truyền thông** với bên ngoài và sự an toàn
- nhiều site bảo vệ mức cao vẫn phải chịu đựng sự tấn công

Các loại tấn công và cách phòng chống

Phương thức:

- Trước khi tấn công: hacker tìm hiểu các dịch vụ đã hiện thực/hoạt động trên mạng
- Dùng ping để xác định các host nào có địa chỉ trên mạng
- Quét port: liên tục thử thiết lập các kết nối TCP với mỗi port (xem thử chuyện gì xảy ra)

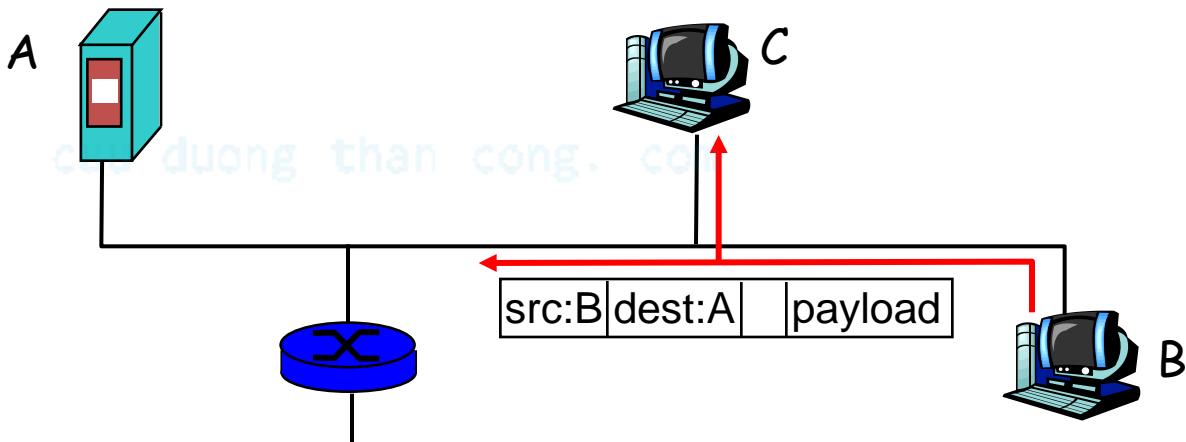
Biện pháp đối phó?

- Ghi nhận lưu thông vào mạng
- Quan tâm các hành vi nghi ngờ (các địa chỉ IP, port bị quét liên tục)

Các mối đe dọa bảo mật Internet

Packet sniffing: Nghe ngóng gói

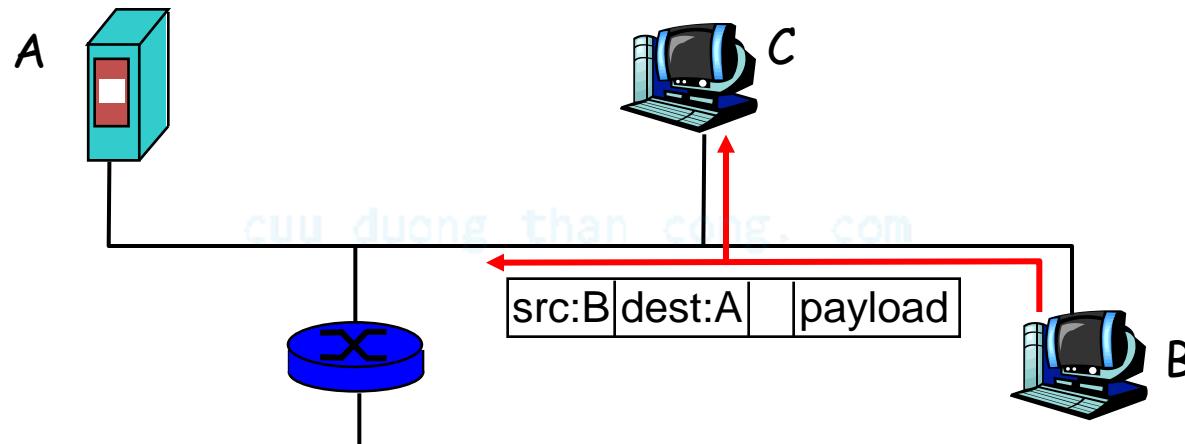
- NIC promiscuous (hỗn tạp) đọc tất cả các gói chuyển qua nó
- Có thể đọc tất cả các dữ liệu được mã hóa (như mật khẩu)
- Ví dụ: C nghe ngóng các gói của B



Các mối đe dọa bảo mật Internet

Packet sniffing: Biện pháp đối phó

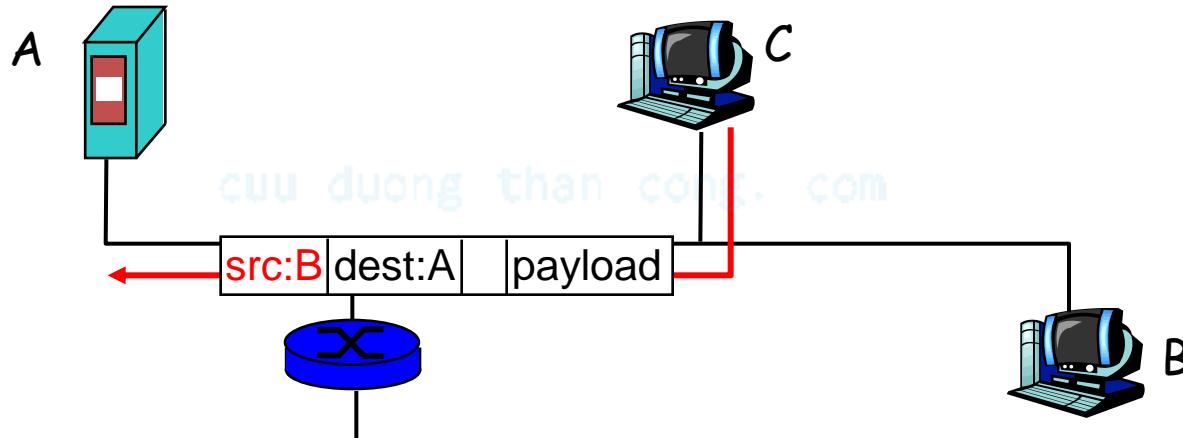
- Tất cả các host trong tổ chức chạy phần mềm kiểm tra định kỳ xem host có ở chế độ promiscuous
- 1 host mỗi đoạn của phương tiện truyền thông



Các mối đe dọa bảo mật Internet

IP Spoofing (giả mạo IP):

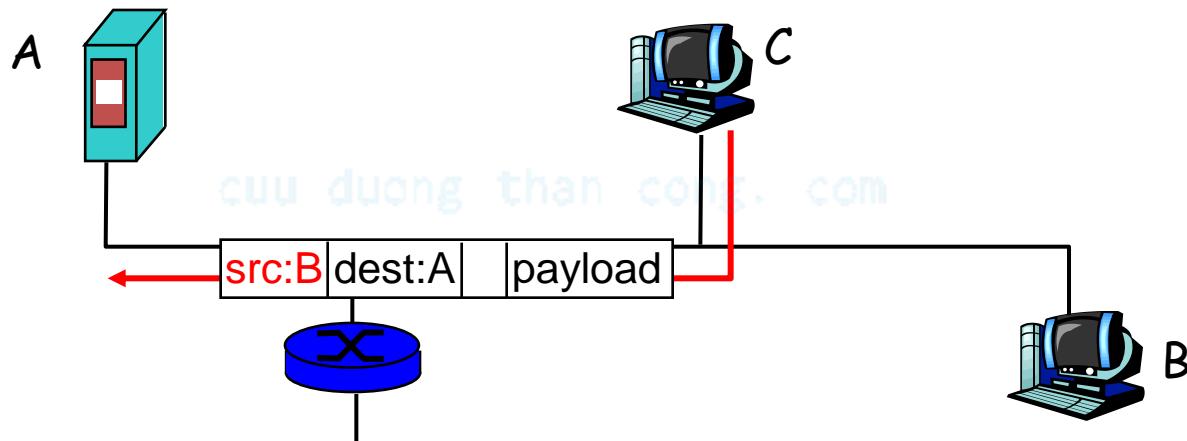
- Có thể sinh ra các gói IP “thô” trực tiếp từ ứng dụng, gán giá trị bất kỳ vào trường địa chỉ IP nguồn
- Bên nhận không thể xác định nguồn bị giả mạo
- Ví dụ: C giả mạo là B



Các mối đe dọa bảo mật Internet

IP Spoofing: lọc quyền vào

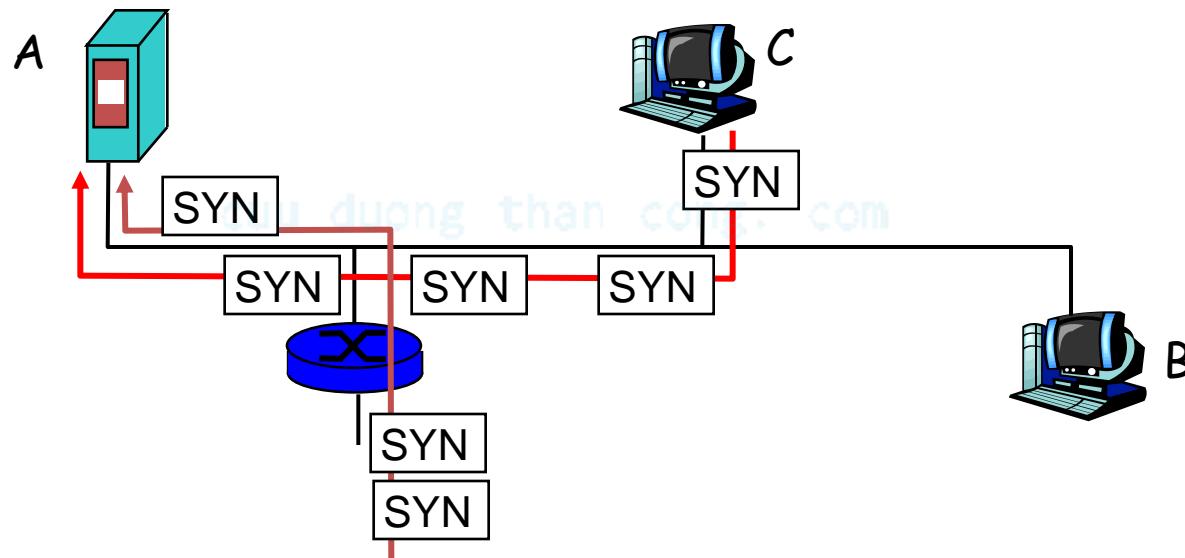
- Router sẽ không chuyển tiếp các gói đi với trường hợp các địa chỉ nguồn không hợp lệ
- Tuyệt vời, nhưng lọc như thế không thể áp dụng cho tất cả các mạng



Các mối đe dọa bảo mật Internet

Denial of Service (DoS):

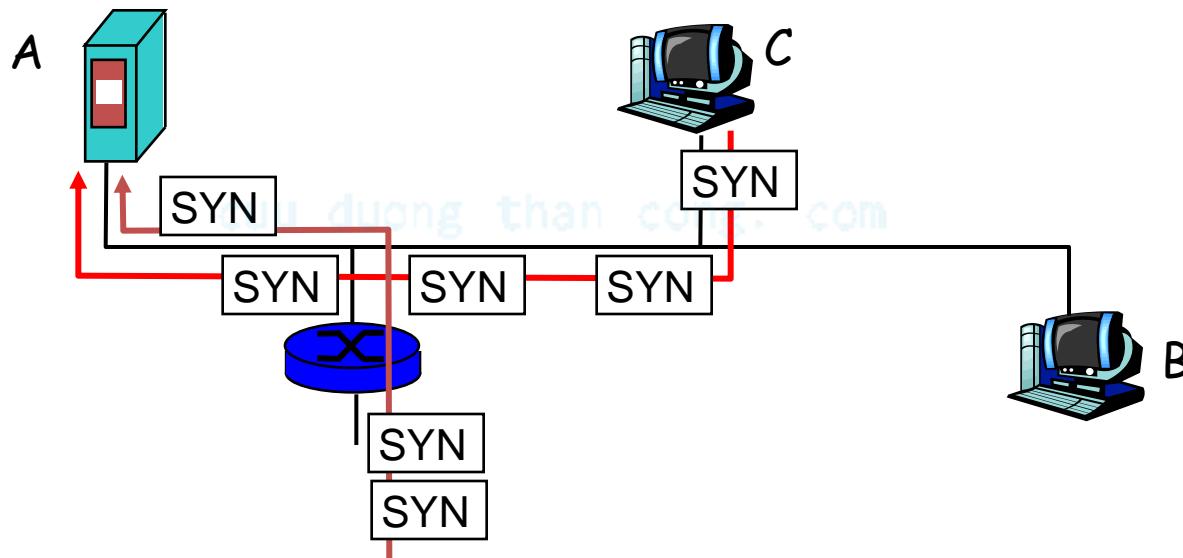
- Gây ra “ngập lụt” bằng các gói sinh ra bởi ý đồ xấu cho bên nhận
- Distributed DOS (DDoS): nhiều nguồn phối hợp làm “ngập lụt” bên nhận
- Ví dụ: C và các host ở xa tấn công SYN A



Các mối đe dọa bảo mật Internet

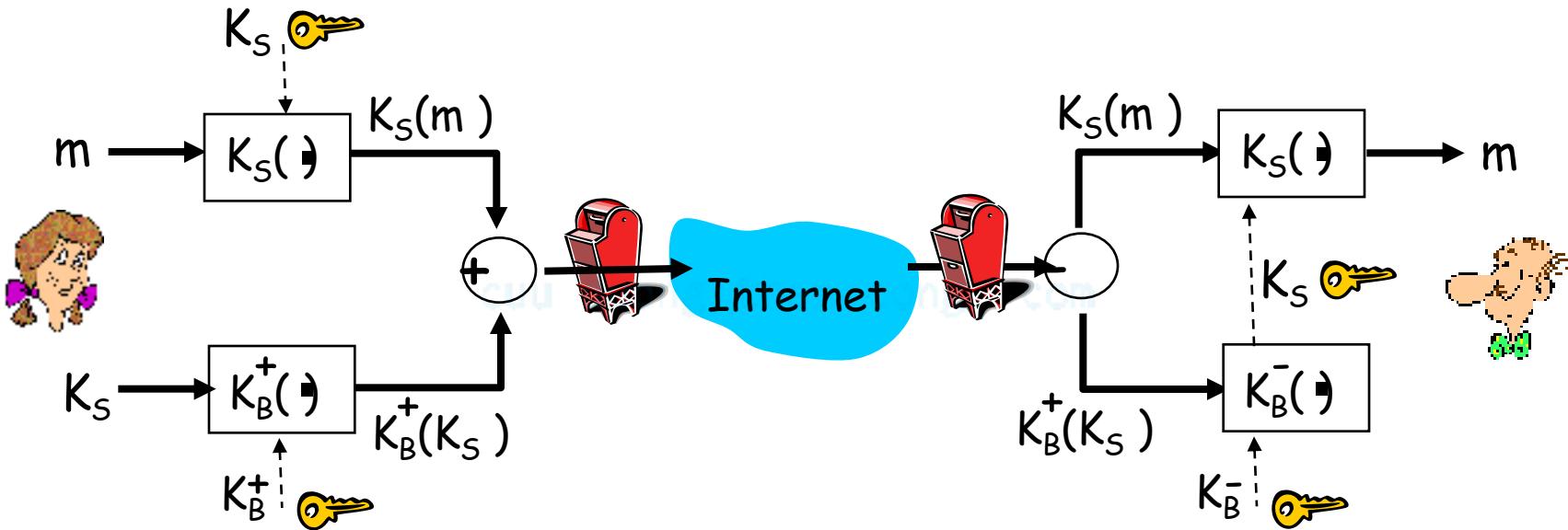
Denial of Service (DoS): Biện pháp đối phó?

- Lọc ra trước các gói dùng làm “ngập lụt” (ví dụ: SYN)
- Theo dõi ngược lại nguồn gây ra “ngập lụt” (cơ chế giống máy phát hiện nói dối của Mỹ)



Bảo mật e-mail

- ❑ Alice muốn gửi 1 e-mail bí mật, m , đến Bob.



Alice:

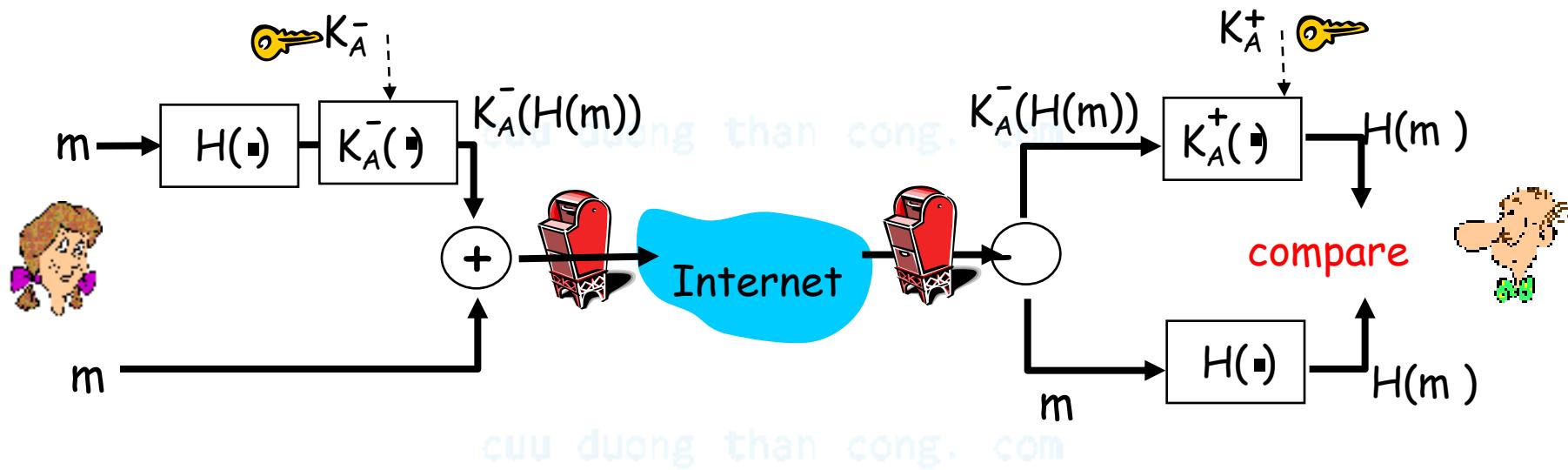
- ❑ sinh ra khóa riêng đối xứng ngẫu nhiên, K_S .
- ❑ mã hóa thông điệp với K_S
- ❑ cũng mã hóa K_S với khóa công cộng của Bob.
- ❑ gửi cả $K_S(m)$ và $K_B^+(K_S)$ cho Bob.

Bob:

- ❑ dùng khóa riêng của anh ấy để giải mã và phục hồi K_S
- ❑ dùng K_S để giải mã $K_S(m)$ và phục hồi m

Bảo mật e-mail

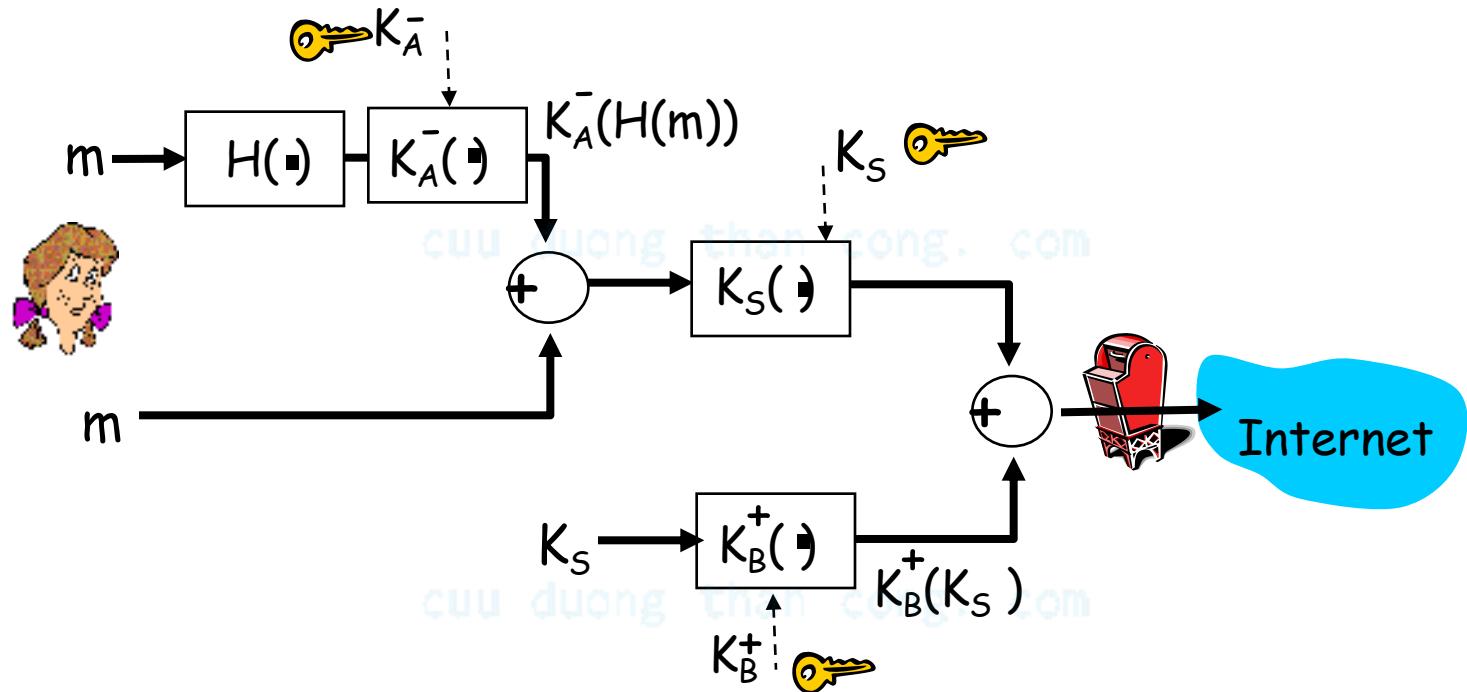
- Alice muốn cung cấp sự toàn vẹn thông điệp chung thực người gửi.



- Alice ký số trên thông điệp.
- gửi cả thông điệp (dạng rõ ràng) và chữ ký số.

Bảo mật e-mail

- Alice muốn cung cấp sự toàn vẹn thông điệp chứng thực người gửi → sự bí mật



Alice dùng 3 khóa: khóa riêng của cô ấy, khóa công cộng của Bob, khóa đối xứng vừa mới tạo

Pretty good privacy (PGP)

- Chuẩn trên thực tế để mã hóa email Internet.
- Dùng mã hóa khóa đối xứng, khóa công cộng, hàm băm và chữ ký số như đã trình bày ở trước.
- Hỗ trợ đồng nhất, chứng thực người gửi, bí mật
- Người phát minh: Phil Zimmerman.

Một thông điệp đã được ký bằng PGP

```
--BEGIN PGP SIGNED MESSAGE--  
Hash: SHA1  
  
Bob:My husband is out of town  
tonight.Passionately yours, A  
  
--BEGIN PGP SIGNATURE--  
Version: PGP 5.0  
Charset: noconv  
yHJRHHGJGhgg/12EpJ+lo8gE4vB3mqJ  
hFEvZP9t6n7G6m5Gw2  
--END PGP SIGNATURE--
```

Secure sockets layer (SSL)

- Bảo mật lớp transport với bất kỳ ứng dụng nào dựa trên TCP dùng các dịch vụ SSL
- Dùng giữa trình duyệt Web, các server trong thương mại điện tử
- Các dịch vụ bảo mật:
 - Chứng thực server
 - Mã hóa dữ liệu
 - Chứng thực client (tùy chọn)
- Chứng thực server:
 - Trình duyệt cho phép SSL chứa các khóa công cộng cho các CA được tin cậy
 - Trình duyệt yêu cầu chứng chỉ server, phát ra bởi CA được tin cậy
 - Trình duyệt dùng khóa công cộng của CA để trích ra khóa công cộng của server từ chứng chỉ
- Kiểm tra trong trình duyệt của bạn để thấy các CA được tin cậy

SSL (tt)

Mã hóa phiên làm việc SSL :

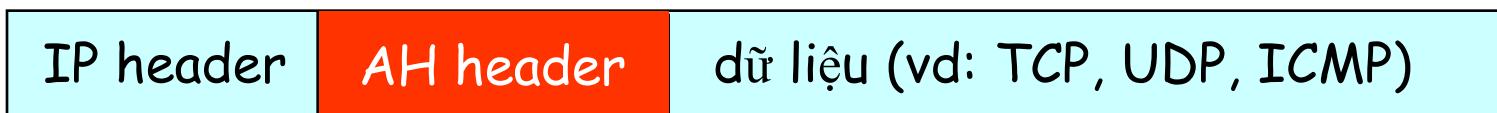
- Trình duyệt sinh ra *khóa phiên đối xứng*, mã hóa nó với khóa công cộng của server, gửi khóa (đã mã hóa) cho server.
 - Dùng khóa riêng, server giải mã khóa phiên
 - Trình duyệt, server biết khóa phiên
 - Tất cả dữ liệu gửi vào trong TCP socket (do client hoặc server) được mã hóa bởi khóa phiên.
- SSL: cơ sở của IETF Transport Layer Security (TLS).
 - SSL có thể dùng cho các ứng dụng không Web, như IMAP.
 - Chứng thực client có thể hoàn thành với các chứng chỉ client

IPSec: bảo mật lớp Network

- **Bảo mật lớp Network:**
 - host gửi mã hóa dữ liệu trong IP datagram
 - các đoạn TCP & UDP; các thông điệp ICMP & SNMP.
- **Chứng thực lớp Network:**
 - host đích có thể chứng thực địa chỉ IP nguồn
- **2 giao thức cơ bản:**
 - authentication header (AH)
 - encapsulation security payload (ESP)
- **Với cả AH và ESP, nguồn – đích bắt tay nhau:**
 - tạo kênh logic lớp network gọi là một security association (SA)
- **Mỗi SA theo 1 chiều duy nhất**
 - **duy nhất xác định bởi:**
 - giao thức bảo mật (AH hoặc ESP)
 - địa chỉ IP nguồn
 - ID của kết nối 32-bit

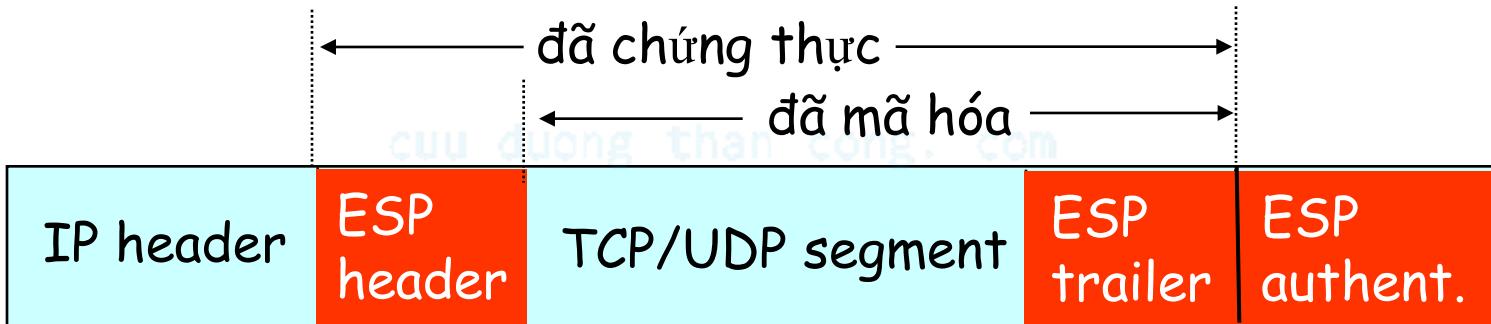
Giao thức AH

- Hỗ trợ chứng thực nguồn, toàn vẹn dữ liệu, không tin cậy
 - AH header được chèn vào giữa IP header, trường dữ liệu.
 - Trường giao thức: 51
 - Trung gian xử lý các datagram như bình thường
- AH header chứa:
- Nhân dạng kết nối
 - Dữ liệu chứng thực: thông điệp đã được ký từ nguồn được tính toán dựa trên IP datagram gốc
 - Trường header kế tiếp: xác định kiểu của dữ liệu (vd: TCP, UDP, ICMP)



Giao thức ESP

- Hỗ trợ toàn vẹn dữ liệu, chứng thực host, tính bí mật
- Mã hóa dữ liệu, ESP trailer
- Trường header kế tiếp nằm trong ESP trailer.
- Trường chứng thực ESP tương tự như của AH
- Protocol = 50.



Bảo mật IEEE 802.11

- *Khảo sát:*
 - 85% việc sử dụng mà không có mã hóa/chứng thực
 - Dễ dàng bị phát hiện/nghe ngóng và nhiều loại tấn công khác!
- *Bảo mật 802.11*
 - Mã hóa, chứng thực
 - Thủ nghiêm bảo mật 802.11 đầu tiên là Wired Equivalent Privacy (WEP): có thiếu sót
 - Thủ nghiêm hiện tại: 802.11i

Wired Equivalent Privacy (WEP):

- Chứng thực như trong giao thức *ap4.0*
 - host yêu cầu chứng thực từ access point
 - access point gửi 128 bit
 - host mã hóa dùng khóa đối xứng chia sẻ
 - access point giải mã, chứng thực host
- Không có cơ chế phân bố khóa
- Chứng thực: chỉ cần biết khóa chia sẻ

cuuduongthancong.com

Wi-Fi Protected Access (WPA)

- Hai sự cải tiến chính so với WEP:
 - Mã hóa dữ liệu cải tiến thông qua giao thức Temporal Key Integrity Protocol (TKIP). TKIP scrambles key sử dụng thuật toán hashing và bằng đặc tính kiểm tra số nguyên, đảm bảo rằng Key sẽ không bị giả mạo.
 - Chứng thực người dùng, thông qua EAP.
- WPA là tiêu chuẩn tạm thời mà sẽ được thay thế với chuẩn IEEE 802.11i

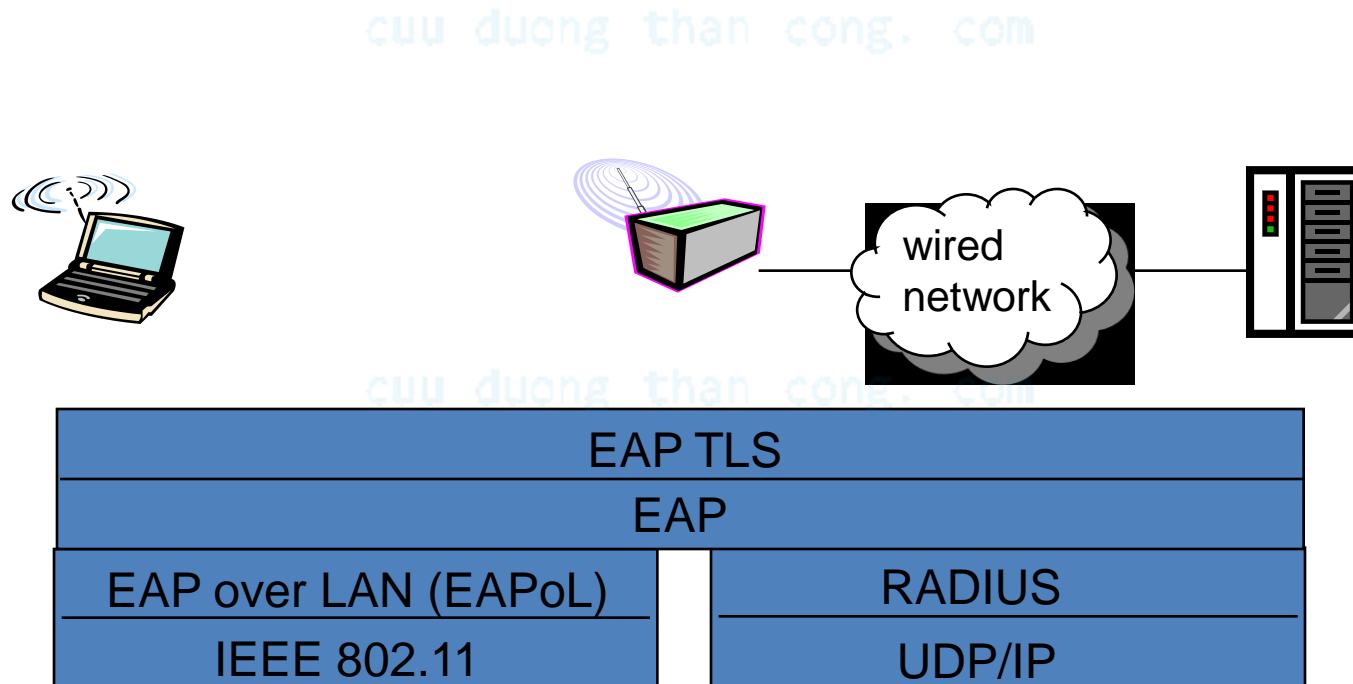
802.11i: cải tiến sự bảo mật

- Rất nhiều (và chắc chắn hơn) dạng mã hóa có thể
- Hỗ trợ phân bổ khóa
cuu duong than cong. com
- Dùng chứng thực server tách riêng khỏi AP

cuu duong than cong. com

EAP: Extensible Authentication Protocol

- EAP được gửi trên các “link” riêng biệt
 - mobile-đến-AP (EAP trên LAN)
 - AP đến server chứng thực (RADIUS trên UDP)



TÀI LIỆU THAM KHẢO, ĐỊA CHỈ LIÊN LẠC

- Giáo trình Mạng máy tính, KS. Nguyễn Bình Dương, TS. Đàm Quang Hồng Hải
- Giáo trình hệ thống Mạng máy tính CCNA, Nguyễn Hồng Sơn
- CCNA: Cisco Certified Network Associate – Study Guide, Todde Lammle - 2007
- Computer Networking: A Top Down Approach Featuring the Internet, 3rd edition. Jim Kurose, Keith Ross. 2004.
- Computer Networks, 4th edition. Andrew S. Tanenbaum. 2003
- Địa chỉ liên lạc: Trần Bá Nhiệm – Khoa Mạng máy tính & Truyền thông – ĐH CNTT – 34 Trương Định, Q3, Tp.HCM.
Email: tranbanhien@yahoo.com

Giáo trình nhập môn mạng máy tính

cuuduongthancong.com

MỤC LỤC

Chương I Nhữn^g khái ni^m c^o b^an c^o m^ang m^ay tⁱnh ...6

I.	Đ ^é nh nghĩa m ^a ng m ^a y t ⁱ nh.....	6
II.	Phân loại m ^a ng m ^a y t ⁱ nh	7
II.1.	D ^u a theo vị tr ⁱ địa l ^y	7
II.2.	D ^u a theo c ^á u tr ^ú c m ^a ng	7
II.2.1	Ki ^{ểu} đ ^í em - đ ^í em (point - to - point).....	7
II.2.2	Ki ^{ểu} khuy ^ê ch t ^{án}	8
II.3.	D ^u a theo ph ^{ương} ph ^{áp} chuy ^ê n m ^a ch	8
II.3.1	M ^a ng chuy ^ê n m ^a ch k ^ê ngh (Line switching network).....	8
II.3.2	M ^a ng chuy ^ê n m ^a ch th ^{ông} đ ^ì ệp (Message switching network).....	8
II.3.3	M ^a ng chuy ^ê n m ^a ch g ^{ói} (Packet switching network)	9
III.	So sánh gi ^{ữa} m ^a ng c ^ú b ^ô v ^a m ^a ng di ^{ện} r ^õ ng	9
IV.	Các thành ph ^{ần} c ^o m ^a ng m ^a y t ⁱ nh	11
IV.1.	M ^ô s ^ố b ^ô g ^{iao} th ^{ức} k ^{ết} n ^{ối} m ^a ng	11
IV.2.	H ^e t di ^{ều} h ^a nh m ^a ng - NOS (<i>Network Operating System</i>)	11
V.	Các lợi ích c ^o m ^a ng m ^a y t ⁱ nh.....	12
V.1.	M ^a ng t ^{ạo} kh ^a n ^ă ng d ^{ùng} chung tài nguy ^{ên} cho các ng ^{ười} d ^{ùng}	12
V.2.	M ^a ng cho phép nâng cao độ tin cậy.....	13
V.3.	M ^a ng gi ^ú p cho công việc đạt hiệu su ^{ất} cao hơn	13
V.4.	Tiết kiệm chi phí.....	13
V.5.	T ^{ăng} c ^{ường} tính bảo mật th ^{ông} tin	13
V.6.	Việc phát triển m ^a ng m ^a y t ⁱ nh đ ^ã t ^{ạo} ra nhiều ứng dụng mới.....	13
VI.	Các dịch vụ ph ^ổ biến trên m ^a ng m ^a y t ⁱ nh	13

Chương II Mô hình truyền thông.....15

I.	S ^ự cần thiết ph ^{ải} có m ^ô h ⁱ m ^o truy ^ê n th ^{ông}	15
II.	Các nhu cầu v ^e chu ^{ẩn} hóa đ ^ó i v ⁱ m ^a ng	16
III.	Mô h ⁱ m ^o OSI (Open Systems Interconnection)	17
III.1.	Nguyên tắc sử dụng khi đ ^é nh nghĩa các t ^ầ ng h ^e t th ^{óng} m ^ở	17
III.2.	Các g ^{iao} th ^{ức} trong m ^ô h ⁱ m ^o OSI.....	18
III.3.	Các ch ^ứ c n ^ă ng ch ^ủ y ^{êu} c ^o c ^á c t ^ầ ng c ^o m ^ô h ⁱ m ^o OSI	19
III.3.1	T ^ầ ng 1: V ^t l ^y (Physical).....	19
III.3.2	T ^ầ ng 2: Li ^ê n k ^{ết} d ^ữ li ^ê u (Data link).....	20

III.3.3 Tầng 3: Mạng (Network)	20
III.3.4 Tầng 4: Vận chuyển (Transport)	22
III.3.5 Tầng 5: Giao dịch (Session)	23
III.3.6 Tầng 6: Trình bày (Presentation).....	23
III.3.7 Tầng 7: Ứng dụng (Application)	24
IV. Quá trình chuyển vận gói tin.....	24
IV.1. Quá trình đóng gói dữ liệu (tại máy gửi).....	24
IV.2. Quá trình truyền dữ liệu từ máy gửi đến máy nhận.	26
IV.3. Chi tiết quá trình xử lý tại máy nhận	26
V. Phương thức truyền tín hiệu.....	27
VI. Mô hình TCP/IP	27
VI.1. Tổng quan về bộ giao thức TCP/IP.....	27
VI.2. So sánh TCP/IP với OSI.....	29
VII. Các giao thức truy cập đường truyền trên mạng LAN	30
VII.1.Giao thức chuyển mạch (yêu cầu và chấp nhận)	30
VII.2.Giao thức đường dây đa truy cập với cảm nhận va chạm	30
VII.3.Giao thức dùng thẻ bài vòng (Token ring)	31
VII.4.Giao thức dung thẻ bài cho dạng đường thẳng (Token bus)	31
VIII. Các phương tiện kết nối mạng liên khu vực (WAN)	31
Chương III Địa chỉ IP.....	33
I. Giao thức TCP/IP	33
II. Địa chỉ IP.....	33
II.1.Tổng quát.....	33
II.2.Cấu trúc của các địa chỉ IP	33
III. Một số khái niệm và thuật ngữ liên quan	37
III.1. Các giao thức trong mạng IP	38
III.2. Các bước hoạt động của giao thức IP	38
IV. Giao thức điều khiển truyền dữ liệu TCP	39
IV.1. Các bước thực hiện để thiết lập một liên kết TCP/IP:	40
IV.2. Các bước thực hiện khi truyền và nhận dữ liệu	41
IV.3. Các bước thực hiện khi đóng một liên kết.....	42
IV.4. Một số hàm khác của TCP	42
V. Giao thức UDP (User Datagram Protocol)	44
VI. Địa chỉ IPv4.....	46

VI.1. Thành phần và hình dạng của địa chỉ IP	46
VI.2. Các lớp địa chỉ IP	46
VII. IPv6	48
VII.1. Giao thức liên mạng thế hệ mới (IPv6)	48
VII.2. Một số đặc điểm mới của IPv6:.....	48
VII.3. Kiến trúc địa chỉ trong IPv6:.....	49
VII.3.1 Không gian địa chỉ:	49
VII.3.2 Cú pháp địa chỉ:	50

Chương IV Thiết bị mạng51

I. Môi trường truyền dẫn	51
I.1. Khái niệm.....	51
I.2. Tần số truyền thông	51
I.3. Các đặc tính của phương tiện truyền dẫn.....	51
I.4. Các kiểu truyền dẫn.	52
II. Đường cáp truyền mạng.....	52
II.1. Cáp xoắn cặp.....	52
II.2. Cáp đồng trục	53
II.3. Cáp sợi quang (Fiber - Optic Cable)	54
II.4. Các yêu cầu cho một hệ thống cáp	54
III. Đường truyền vô tuyến	55
III.1. Sóng vô tuyến (radio)	55
III.2. Sóng viba	55
III.3. Hồng ngoại.....	55
IV. Các kỹ thuật bấm cáp mạng	56
V. Các thiết bị liên kết mạng	57
V.1. Repeater (Bộ tiếp sức)	57
V.2. Bridge (Cầu nối).....	58
V.3. Router (Bộ tìm đường)	61
V.3.1 Các phương thức hoạt động của Router	64
V.3.2 Một số giao thức hoạt động chính của Router	64
V.4. Gateway (cổng nối)	64
V.5. Hub (Bộ tập trung)	65
V.6. Bộ chuyển mạch (switch).....	66
Chương V Mô hình mạng.....67	

I.	Kiến trúc mạng (Topology)	67
II.	Những cấu trúc chính của mạng cục bộ	67
II.1.	Dạng đường thẳng (Bus)	67
II.2.	Dạng vòng tròn (Ring)	68
II.3.	Dạng hình sao (Star)	68
II.4.	Mạng dạng kết hợp	70

Chương VI Các dịch vụ của mạng điện rộng (WAN) 71

I.	Mạng chuyển mạch (Circuit Swiching Network)	71
II.	Mạng thuê bao (Leased line Network)	73
III.	Mạng chuyển gói tin (Packet Switching NetWork)	74
IV.	Mạng X25.....	75
V.	Mạng Frame Relay	76
VI.	Mạng ATM (Cell relay)	76

Chương VII CÁC DỊCH VỤ MẠNG THÔNG DỤNG. 78

I.	DỊCH VỤ WEB.....	78
I.1.	Một số thuật ngữ cơ bản	78
I.2.	Giới thiệu mô hình hoạt động của Web.	80
II.	DỊCH VỤ FTP.....	81
II.1.	Mô hình hoạt động của FTP	81
II.2.	Tập hợp các lệnh FTP	81
III.	E-MAIL.....	83
III.1.	Mô hình hoạt động	83
III.2.	Các loại mail.	83
III.3.	Sử dụng WebMail.	83

Chương I Nhữngh khái niệm cơ bản của mạng máy tính

Mạng máy tính ngày nay đã phát triển một cách nhanh chóng và đa dạng. Hệ điều hành cùng các ứng dụng của mạng ngày càng phong phú, các lợi ích của mạng ngày càng được khẳng định. Mạng máy tính bao gồm rất nhiều loại, nhiều mô hình triển khai. Trong một mạng máy tính lại có nhiều thành phần cấu thành. Trước khi đi chi tiết về mạng máy tính, chúng ta sẽ tìm hiểu các khái niệm cơ bản của mạng máy tính.

I. Định nghĩa mạng máy tính

Mạng máy tính là một tập hợp các máy tính được nối với nhau bởi đường truyền theo một cấu trúc nào đó và thông qua đó các máy tính trao đổi thông tin qua lại với nhau.

Đường truyền là hệ thống các thiết bị truyền dẫn có dây hay không dây dùng để chuyển các tín hiệu điện tử từ máy tính này đến máy tính khác. Các tín hiệu điện tử đó biểu thị các giá trị dữ liệu dưới dạng các xung nhị phân (on - off). Tất cả các tín hiệu được truyền giữa các máy tính đều thuộc một dạng sóng điện từ. Tùy theo tần số của sóng điện từ có thể dùng các đường truyền vật lý khác nhau để truyền các tín hiệu. Ở đây đường truyền được kết nối có thể là dây cáp đồng trực, cáp xoắn, cáp quang, dây điện thoại, sóng vô tuyến ... Các đường truyền dữ liệu tạo nên cấu trúc của mạng.



Hình I-1 Mạng máy tính

Với sự trao đổi qua lại giữa máy tính này với máy tính khác đã phân biệt mạng máy tính với các hệ thống thu phát một chiều như truyền hình, phát thông tin từ vệ tinh xuống các trạm thu thụ động... vì tại đây chỉ có thông tin một chiều từ nơi phát đến nơi thu mà không quan tâm đến có bao nhiêu nơi thu, có thu tốt hay không.

Đặc trưng cơ bản của đường truyền vật lý là giải thông. Giải thông của một đường chuyền chính là độ đo phạm vi tần số mà nó có thể đáp ứng được. Tốc độ truyền dữ liệu trên đường truyền còn được gọi là thông lượng của đường truyền - thường được tính bằng số lượng bit được truyền đi trong một giây (Bps). Thông lượng còn được đo bằng đơn vị khác là Baud (lấy tên nhà bác học - Emile Baudot). Baud biểu thị số lượng thay đổi tín hiệu trong một giây.

Ở đây Baud và Bps không phải bao giờ cũng đồng nhất. Ví dụ: nếu trên đường dây có 8 mức tín hiệu khác nhau thì mỗi mức tín hiệu tương ứng với 3 bit hay là 1 Baud tương ứng với 3 bit. Chỉ khi có 2 mức tín hiệu trong đó mỗi mức tín hiệu tương ứng với 1 bit thì 1 Baud mới tương ứng với 1 bit.

II. Phân loại mạng máy tính

Có nhiều cách để phân biệt mạng máy tính nhưng người ta thường phân biệt mạng máy tính theo vị trí địa lý, cấu trúc mạng, phương pháp chuyển mạch.

II.1. Dựa theo vị trí địa lý

Dựa vào phạm vi phân bố của mạng người ta có thể phân ra các loại mạng như sau:

GAN (Global Area Network) - Kết nối máy tính từ các châu lục khác nhau. Thông thường kết nối này được thực hiện thông qua mạng viễn thông và vệ tinh.

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

MAN (Metropolitan Area Network) - Kết nối các máy tính trong phạm vi một thành phố hay giữa các thành phố với nhau.

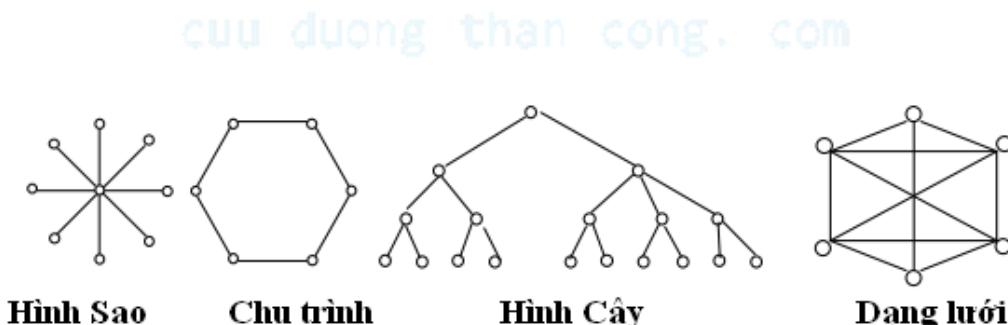
LAN (Local Area Network) - Mạng cục bộ, kết nối các máy tính trong một khu vực bán kính hẹp thông thường khoảng vài trăm mét. Kết nối được thực hiện thông qua các môi trường truyền thông tốc độ cao ví dụ cáp đồng trực thay cáp quang. LAN thường được sử dụng trong nội bộ một cơ quan/tổ chức... Các LAN có thể được kết nối với nhau thành WAN.

Trong các khái niệm nói trên, thường được sử dụng nhất hiện nay là khái niệm Mạng diện rộng WAN và mạng cục bộ LAN.

II.2. Dựa theo cấu trúc mạng

II.2.1 Kiểu điểm - điểm (point - to - point)

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



Hình I-2 Cấu trúc điểm – điểm

II.2.2 Kiểu khuyếch tán

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

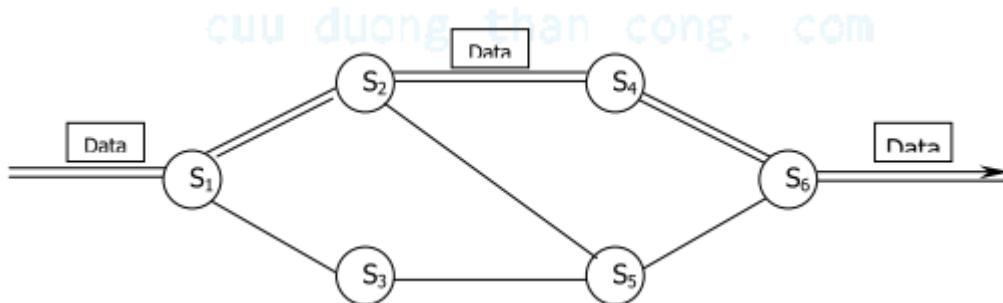


Hình I-3 Cấu trúc kiểu khuyếch tán

II.3. Dựa theo phương pháp chuyển mạch

II.3.1 Mạng chuyển mạch kênh (Line switching network)

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

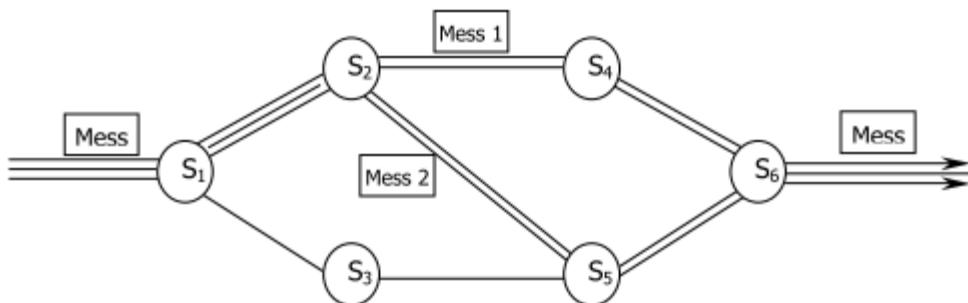


Hình I-4 Mạng chuyển mạch kênh

II.3.2 Mạng chuyển mạch thông điệp (Message switching network)

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

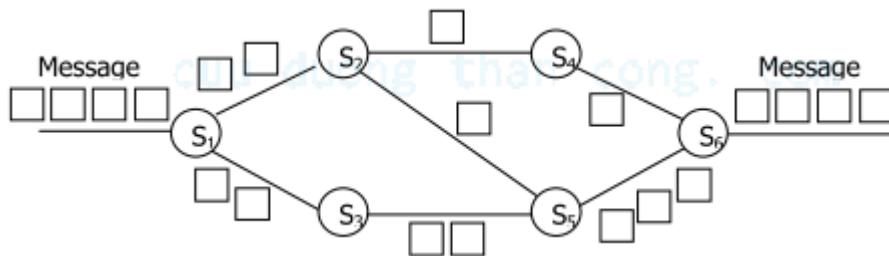
Mạng chuyển mạch thông báo thích hợp với các dịch vụ thông tin kiểu thư điện tử (Email) hơn là đối với các ứng dụng có tính thời gian thực vì tồn tại độ trễ nhất định do lưu trữ và xử lý thông tin điều khiển tại mỗi nút.



Hình I-5 Mạng chuyển mạch thông điệp

II.3.3 Mạng chuyển mạch gói (Packet switching network)

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



Hình I-6 Mạng chuyển mạch gói

III. So sánh giữa mạng cục bộ và mạng diện rộng

Mạng cục bộ và mạng diện rộng có thể được phân biệt bởi: địa phương hoạt động, tốc độ đường truyền và tỷ lệ lỗi trên đường truyền, chủ quản của mạng, đường đi của thông tin trên mạng, dạng chuyển giao thông tin.

Địa phương hoạt động

Liên quan đến khu vực địa lý thì mạng cục bộ sẽ là mạng liên kết các máy tính nằm ở trong một khu vực nhỏ. Khu vực có thể bao gồm một tòa nhà hay là một khu nhà... Điều đó hạn chế bởi khoảng cách đường dây cáp được dùng để liên kết các máy tính của mạng cục bộ (Hạn chế đó còn là hạn chế của khả năng kỹ thuật của đường truyền dữ liệu). Ngược lại mạng diện rộng là mạng có khả năng liên kết các máy tính trong một vùng rộng lớn như là một thành phố, một miền, một đất nước, mạng diện rộng được xây dựng để nối hai hoặc nhiều khu vực địa lý riêng biệt.

Tốc độ đường truyền và tỷ lệ lỗi trên đường truyền

Do các đường cáp của mạng cục bộ 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.

Đơn vị bps (Bit Per Second) là một đơn vị trong truyền thông tương đương với 1 bit được truyền trong một giây, ví dụ như tốc độ đường truyền là 1 Mbps tức là có thể truyền tối đa 1 Megabit trong 1 giây trên đường truyền đó.

Thông thường trong mạng cục bộ tỷ lệ lỗi trong truyền dữ liệu vào khoảng 1/10⁷-10⁸ còn trong mạng diện rộng thì tỷ lệ đó vào khoảng 1/10⁶ - 10⁷

Chủ quản và điều hành của mạng

Do sự phức tạp trong việc xây dựng, quản lý, duy trì các đường truyền dẫn nên khi xây dựng mạng diện rộng người ta thường sử dụng các đường truyền được thuê từ các công ty viễn thông hay các nhà cung cấp dịch vụ truyền số liệu. Tùy theo cấu trúc của mạng những đường truyền đó thuộc cơ quan quản lý khác nhau như các nhà cung cấp đường truyền nội hạt, liên tỉnh, liên quốc gia. Các đường truyền đó phải tuân thủ các quy định của chính phủ các khu vực có đường dây đi qua như: tốc độ, việc mã hóa.

Còn đối với mạng cục bộ thì công việc đơn giản hơn nhiều, khi một cơ quan cài đặt mạng cục bộ thì toàn bộ mạng sẽ thuộc quyền quản lý của cơ quan đó.

Đường đi của thông tin trên mạng

Trong mạng cục bộ thông tin được đi theo con đường xác định bởi cấu trúc của mạng. Khi người ta xác định cấu trúc của mạng thì thông tin sẽ luôn luôn đi theo cấu trúc đã xác định đó. Còn với mạng diện rộng dữ liệu cấu trúc có thể phức tạp hơn nhiều do việc sử dụng các dịch vụ truyền dữ liệu. Trong quá trình hoạt động các điểm nút có thể thay đổi đường đi của các thông tin khi phát hiện ra có trực trặc trên đường truyền hay khi phát hiện có quá nhiều thông tin cần truyền giữa hai điểm nút nào đó. Trên mạng diện rộng thông tin có thể có các con đường đi khác nhau, điều đó cho phép có thể sử dụng tối đa các năng lực của đường truyền hay nâng cao điều kiện an toàn trong truyền dữ liệu.

Dạng chuyển giao thông tin

Phần lớn các mạng diện rộng hiện nay được phát triển cho việc truyền đồng thời trên đường truyền nhiều dạng thông tin khác nhau như: video, tiếng nói, dữ liệu... Trong khi đó các mạng cục bộ chủ yếu phát triển trong việc truyền dữ liệu thông thường. Điều này có thể giải thích do việc truyền các dạng thông tin như video, tiếng nói trong một khu vực nhỏ ít được quan tâm hơn như khi truyền qua những khoảng cách lớn.

Các hệ thống mạng hiện nay ngày càng phức tạp về chất lượng, đa dạng về chủng loại và phát triển rất nhanh về chất. Trong sự phát triển đó số lượng những nhà sản xuất từ phần mềm, phần cứng máy tính, các sản phẩm viễn thông cũng tăng nhanh với nhiều sản phẩm đa dạng. Chính vì vậy vai trò chuẩn hóa cũng mang những ý nghĩa quan trọng. Tại các nước các cơ quan chuẩn quốc gia đã đưa ra các những chuẩn về phần cứng và các quy định về giao tiếp nhằm giúp cho các nhà sản xuất có thể làm ra các sản phẩm có thể kết nối với các sản phẩm do hãng khác sản xuất.

IV. Các thành phần của mạng máy tính

Mạng máy tính bao gồm các thiết bị phần cứng, các giao thức và các phần mềm mạng. Khi nghiên cứu về mạng máy tính, các vấn đề quan trọng cần được xem xét là giao thức mạng, cấu hình kết nối của mạng và các dịch vụ mạng.

IV.1. Một số bộ giao thức kết nối mạng

1. TCP/IP

- Ưu thế chính của bộ giao thức này là khả năng liên kết hoạt động của nhiều loại máy tính khác nhau.
- TCP/IP đã trở thành tiêu chuẩn thực tế cho kết nối liên mạng cũng như kết nối Internet toàn cầu.

2. NetBEUI

- Bộ giao thức nhỏ, nhanh và hiệu quả được cung cấp theo các sản phẩm của hãng IBM, cũng như sự hỗ trợ của Microsoft.
- Bất lợi chính của bộ giao thức này là không hỗ trợ định tuyến và sử dụng giới hạn ở mạng dựa vào Microsoft.

3. IPX/SPX

- Đây là bộ giao thức sử dụng trong mạng Novell.
- Ưu thế: nhỏ, nhanh và hiệu quả trên các mạng cục bộ đồng thời hỗ trợ khả năng định tuyến.

4. DECnet

- Đây là bộ giao thức độc quyền của hãng Digital Equipment Corporation.
- DECnet định nghĩa mô hình truyền thông qua mạng LAN, mạng MAN và WAN. Hỗ trợ khả năng định tuyến

IV.2. Hệ điều hành mạng - NOS (Network Operating System)

Cùng với sự nghiên cứu và phát triển mạng máy tính, hệ điều hành mạng đã được nhiều công ty đầu tư nghiên cứu và đã công bố nhiều phần mềm quản lý và điều hành mạng có hiệu quả như: *NetWare* của công ty NOVELL, *LAN Manager* của Microsoft dùng cho các máy server chạy hệ điều hành OS/2, LAN server của IBM (gần như đồng nhất với *LAN Manager*), *Vines* của *Banyan Systems* là hệ điều hành mạng dùng cho server chạy hệ điều hành UNIX, *Promise LAN* của *Mises Computer* chạy trên *card* điều hợp mạng độc quyền, *Windows for Workgroups* của Microsoft, *LANtastic* của *Artisoft*, *NetWare Lite* của *Novell*,....

Một trong những sự lựa chọn cơ bản mà ta phải quyết định trước là hệ điều hành mạng nào sẽ làm nền tảng cho mạng của ta, việc lựa chọn tuỳ thuộc vào kích cỡ của mạng hiện tại và

sự phát triển trong tương lai, còn tuỳ thuộc vào những ưu điểm và nhược điểm của từng hệ điều hành.

Một số hệ điều hành mạng phổ biến hiện nay:

Hệ điều hành mạng UNIX: Đây là hệ điều hành do các nhà khoa học xây dựng và được dùng rất phổ biến trong giới khoa học, giáo dục. Hệ điều hành mạng UNIX là hệ điều hành đa nhiệm, đa người sử dụng, phục vụ cho truyền thông tốt. Nhược điểm của nó là hiện nay có nhiều Version khác nhau, không thống nhất gây khó khăn cho người sử dụng. Ngoài ra hệ điều hành này khá phức tạp lại đòi hỏi cấu hình máy mạnh (trước đây chạy trên máy mini, gần đây có SCO UNIX chạy trên máy vi tính với cấu hình mạnh).

Hệ điều hành mạng Windows NT: Đây là hệ điều hành của hãng Microsoft, cũng là hệ điều hành đa nhiệm, đa người sử dụng. Đặc điểm của nó là tương đối dễ sử dụng, hỗ trợ mạnh cho phần mềm WINDOWS. Do hãng Microsoft là hãng phần mềm lớn nhất thế giới hiện nay, hệ điều hành này có khả năng sẽ được ngày càng phổ biến rộng rãi. Ngoài ra, Windows NT có thể liên kết tốt với máy chủ Novell Netware. Tuy nhiên, để chạy có hiệu quả, Windows NT cũng đòi hỏi cấu hình máy tương đối mạnh.

Hệ điều hành mạng Windows for Workgroup: Đây là hệ điều hành mạng ngang hàng nhỏ, cho phép một nhóm người làm việc (khoảng 3-4 người) dùng chung ổ đĩa trên máy của nhau, dùng chung máy in nhưng không cho phép chạy chung một ứng dụng. Hệ dễ dàng cài đặt và cũng khá phổ biến.

Hệ điều hành mạng NetWare của Novell: Đây là hệ điều hành phổ biến nhất hiện nay ở nước ta và trên thế giới trong thời gian cuối, nó có thể dùng cho các mạng nhỏ (khoảng từ 5-25 máy tính) và cũng có thể dùng cho các mạng lớn gồm hàng trăm máy tính. Trong những năm qua, Novell đã cho ra nhiều phiên bản của Netware: Netware 2.2, 3.11, 4.0 và hiện có 4.1. Netware là một hệ điều hành mạng cục bộ dùng cho các máy vi tính theo chuẩn của IBM hay các máy tính Apple Macintosh, chạy hệ điều hành MS-DOS hoặc OS/2.

Hệ điều hành này tương đối gọn nhẹ, dễ cài đặt (máy chủ chỉ cần thậm chí AT386) do đó phù hợp với hoàn cảnh trang thiết bị hiện tại của nước ta. Ngoài ra, vì là một phần mềm phổ biến nên Novell Netware được các nhà sản xuất phần mềm khác hỗ trợ (theo nghĩa các phần mềm do các hãng phần mềm lớn trên thế giới làm đều có thể chạy tốt trên hệ điều hành mạng này).

V. Các lợi ích của mạng máy tính

V.1. Mạng tạo khả năng dùng chung tài nguyên cho các người dùng.

Vấn đề là làm cho các tài nguyên trên mạng như chương trình, dữ liệu và thiết bị, đặc biệt là các thiết bị đắt tiền, có thể sẵn dùng cho mọi người trên mạng mà không cần quan tâm đến vị trí thực của tài nguyên và người dùng.

Về mặt thiết bị, các thiết bị chất lượng cao thường đắt tiền, chúng thường được dùng chung cho nhiều người nhằm giảm chi phí và dễ bảo quản.

Về mặt chương trình và dữ liệu, khi được dùng chung, mỗi thay đổi sẽ sẵn dùng cho mọi thành viên trên mạng ngay lập tức. Điều này thể hiện rất rõ tại các nơi như ngân hàng, các đại lý bán vé máy bay...

V.2. Mạng cho phép nâng cao độ tin cậy.

Khi sử dụng mạng, có thể thực hiện một chương trình tại nhiều máy tính khác nhau, nhiều thiết bị có thể dùng chung. Điều này tăng độ tin cậy trong công việc vì khi có máy tính hoặc thiết bị bị hỏng, công việc vẫn có thể tiếp tục với các máy tính hoặc thiết bị khác trên mạng trong khi chờ sửa chữa.

V.3. Mạng giúp cho công việc đạt hiệu suất cao hơn.

Khi chương trình và dữ liệu đã dùng chung trên mạng, có thể bỏ qua một số khâu đối chiếu không cần thiết. Việc điều chỉnh chương trình (nếu có) cũng tiết kiệm thời gian hơn do chỉ cần cài đặt lại trên một máy.

Về mặt tổ chức, việc sao chép dữ liệu phòng ngừa lợi hại hơn do có thể giao cho chỉ một người thay vì mọi người phải tự sao chép phần của mình.

V.4. Tiết kiệm chi phí.

Việc dùng chung các thiết bị ngoại vi cho phép giảm chi phí trang bị tính trên số người dùng. Về phần mềm, nhiều nhà sản xuất phần mềm cung cấp cả những ẩn bản cho nhiều người dùng, với chi phí thấp hơn tính trên mỗi người dùng.

V.5. Tăng cường tính bảo mật thông tin.

Dữ liệu được lưu trên các máy phục vụ tập tin (file server) sẽ được bảo vệ tốt hơn so với đặt tại các máy cá nhân nhờ cơ chế bảo mật của các hệ điều hành mạng.

V.6. Việc phát triển mạng máy tính đã tạo ra nhiều ứng dụng mới

Một số ứng dụng có ảnh hưởng quan trọng đến toàn xã hội: khả năng truy xuất các chương trình và dữ liệu từ xa, khả năng thông tin liên lạc dễ dàng và hiệu quả, tạo môi trường giao tiếp thuận lợi giữa những người dùng khác nhau, khả năng tìm kiếm thông tin nhanh chóng trên phạm vi toàn thế giới,...

VI. Các dịch vụ phổ biến trên mạng máy tính

- **Dịch vụ tập tin (File services)**

Cho phép chia sẻ tài nguyên thông tin chung, chuyển giao các tập tin dữ liệu từ máy này sang máy khác. Tìm kiếm thông tin và điều khiển truy nhập. Dịch vụ thư điện tử E-Mail (Electronic mail) cung cấp cho người sử dụng phương tiện trao đổi, tranh luận bằng thư điện tử. Dịch vụ thư điện tử giá thành hạ, chuyển phát nhanh, an toàn và nội dung có thể tích hợp các loại dữ liệu.

- **Dịch vụ in ấn**

Có thể dùng chung các máy in đặt 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.

cuu duong than cong. com

cuu duong than cong. com

Chương II Mô hình truyền thông

I. Sự cần thiết phải có mô hình truyền thông

Để một mạng máy tính trao đổi một môi trường truyền dữ liệu thì nó cần phải có những yếu tố sau:

Mỗi máy tính cần phải có một địa chỉ phân biệt trên mạng.

Việc chuyển dữ liệu từ máy tính này đến máy tính khác do mạng thực hiện thông qua những quy định thống nhất gọi là giao thức của mạng.

Khi các máy tính trao đổi dữ liệu với nhau thì một quá trình truyền giao dữ liệu đã được thực hiện hoàn chỉnh. Ví dụ như để thực hiện việc truyền một file giữa một máy tính với một máy tính khác cùng được gắn trên một mạng các công việc sau đây phải được thực hiện:

Máy tính cần truyền cần biết địa chỉ của máy nhận.

Máy tính cần truyền phải xác định được máy tính nhận đã sẵn sàng nhận thông tin

Chương trình gửi file trên máy truyền cần xác định được rằng chương trình nhận file trên máy nhận đã sẵn sàng tiếp nhận file.

Nếu cấu trúc file trên hai máy không giống nhau thì một máy phải làm nhiệm vụ chuyển đổi file từ dạng này sang dạng kia.

Khi truyền file máy tính truyền cần thông báo cho mạng biết địa chỉ của máy nhận để các thông tin được mạng đưa tới đích.

Điều trên đó cho thấy giữa hai máy tính đã có một sự phối hợp hoạt động ở mức độ cao. Nay giờ thay vì chúng ta xét cả quá trình trên như là một quá trình chung thì chúng ta sẽ chia quá trình trên ra thành một số công đoạn và mỗi công đoạn con hoạt động một cách độc lập với nhau. Ở đây chương trình truyền nhận file của mỗi máy tính được chia thành ba module là: Module truyền và nhận File, Module truyền thông và Module tiếp cận mạng. Hai module tương ứng sẽ thực hiện việc trao đổi với nhau trong đó:

Module truyền và nhận file cần được thực hiện tất cả các nhiệm vụ trong các ứng dụng truyền nhận file. Ví dụ: truyền nhận thông số về file, truyền nhận các mẫu tin của file, thực hiện chuyển đổi file sang các dạng khác nhau nếu cần. Module truyền và nhận file không cần thiết phải trực tiếp quan tâm tới việc truyền dữ liệu trên mạng như thế nào mà nhiệm vụ đó được giao cho Module truyền thông.

Module truyền thông quan tâm tới việc các máy tính đang hoạt động và sẵn sàng trao đổi thông tin với nhau. Nó còn kiểm soát các dữ liệu sao cho những dữ liệu này có thể trao đổi một cách chính xác và an toàn giữa hai máy tính. Điều đó có nghĩa là phải truyền file trên nguyên tắc đảm bảo an toàn cho dữ liệu, tuy nhiên ở đây có thể có một vài mức độ an toàn khác nhau được dành cho từng ứng dụng. Ở đây việc trao đổi dữ liệu giữa hai máy tính không phụ thuộc vào bản chất của mạng đang liên kết chúng. Những yêu cầu liên quan đến mạng đã được thực hiện ở module thứ ba là module tiếp cận mạng và nếu mạng thay đổi thì chỉ có module tiếp cận mạng bị ảnh hưởng.

Module tiếp cận mạng được xây dựng liên quan đến các quy cách giao tiếp với mạng và phụ thuộc vào bản chất của mạng. Nó đảm bảo việc truyền dữ liệu từ máy tính này đến máy tính khác trong mạng.

Như vậy thay vì xét cả quá trình truyền file với nhiều yêu cầu khác nhau như một tiến trình phức tạp thì chúng ta có thể xét quá trình đó với nhiều tiến trình con phân biệt dựa trên việc trao đổi

giữa các Module tương ứng trong chương trình truyền file. Cách này cho phép chúng ta phân tích kỹ quá trình file và dễ dàng trong việc viết chương trình.

Việc xét các module một cách độc lập với nhau như vậy cho phép giảm độ phức tạp cho việc thiết kế và cài đặt. Phương pháp này được sử dụng rộng rãi trong việc xây dựng mạng và các chương trình truyền thông và được gọi là phương pháp phân tầng (layer).

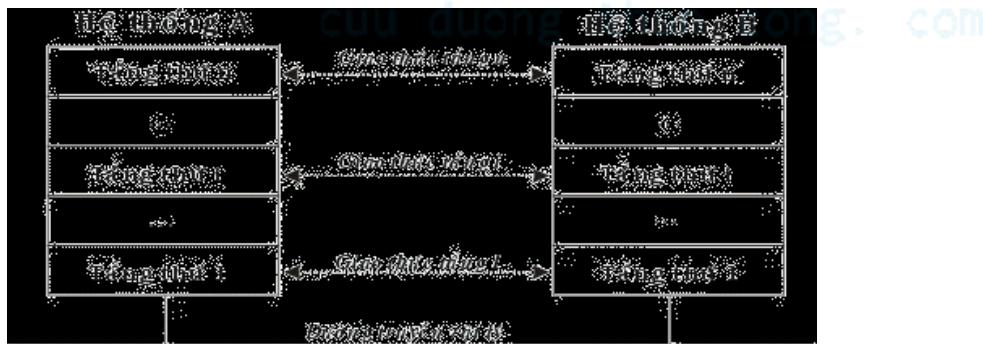
Nguyên tắc của phương pháp phân tầng là:

Mỗi hệ thống thành phần trong mạng được xây dựng như một cấu trúc nhiều tầng và đều có cấu trúc giống nhau như: số lượng tầng và chức năng của mỗi tầng.

Các tầng nằm chồng lên nhau, dữ liệu được chỉ trao đổi trực tiếp giữa hai tầng kề nhau từ tầng trên xuống tầng dưới và ngược lại.

Cùng với việc xác định chức năng của mỗi tầng chúng ta phải xác định mối quan hệ giữa hai tầng kề nhau. Dữ liệu được truyền đi từ tầng cao nhất của hệ thống truyền lần lượt đến tầng thấp nhất sau đó truyền qua đường nối vật lý dưới dạng các bit tới tầng thấp nhất của hệ thống nhận, sau đó dữ liệu được truyền ngược lên lần lượt đến tầng cao nhất của hệ thống nhận.

Chi có hai tầng thấp nhất có liên kết vật lý với nhau còn các tầng trên cùng thứ tự chỉ có các liên kết logic với nhau. Liên kết logic của một tầng được thực hiện thông qua các tầng dưới và phải tuân theo những quy định chặt chẽ, các quy định đó được gọi giao thức của tầng.



Hình II-1 Mô hình phân tầng

II. Các nhu cầu về chuẩn hóa đối với mạng

Trong thực tế việc phân chia các tầng như trong mô hình trên thực sự chưa đủ. Trên thế giới hiện có một số cơ quan định chuẩn, họ đưa ra hàng loạt chuẩn về mạng tuy các chuẩn đó có tính chất khuyến nghị chứ không bắt buộc nhưng chúng rất được các cơ quan chuẩn quốc gia coi trọng.

Hai trong số các cơ quan chuẩn quốc tế là:

ISO (The International Standards Organization) - Là tổ chức tiêu chuẩn quốc tế hoạt động dưới sự bảo trợ của Liên hợp Quốc với thành viên là các cơ quan chuẩn quốc gia với số lượng khoảng hơn 100 thành viên với mục đích hỗ trợ sự phát triển các chuẩn trên phạm vi toàn thế giới. Một trong những thành tựu của ISO trong lãnh vực truyền thông là mô hình hệ thống mở (Open Systems Interconnection - gọi tắt là OSI).

CCITT (Commité Consultatif International pour le Telegraph 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 lĩnh vực viễn thông.

III. Mô hình OSI (Open Systems Interconnection)

Mô hình OSI là một cơ sở dành cho việc chuẩn hóa 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 hóa trong các lĩnh vực viễn thông và hệ thống thông tin. Theo mô hình OSI chương trình truyền thông được chia ra thành 7 tầng với những chức năng phân biệt cho từng tầng. Hai tầng đồng mức khi liên kết với nhau phải sử dụng một giao thức chung.

Việc nghiên cứu về OSI được bắt đầu tại ISO vào năm 1971 với các mục tiêu nhằm nối kết các sản phẩm của các hãng sản xuất khác. Ưu điểm chính của OSI là ở chỗ nó hứa hẹn giải pháp cho vấn đề truyền thông giữa các máy tính không giống nhau. Hai hệ thống, dù có khác nhau đều có thể truyền thông với nhau một cách hiệu quả nếu chúng đảm bảo những điều kiện chung sau đây:

Chúng cài đặt cùng một tập các chức năng truyền thông.

Các chức năng đó được tổ chức thành cùng một tập các tầng. các tầng đồng mức phải cung cấp các chức năng như nhau.

Các tầng đồng mức khi trao đổi với nhau sử dụng chung một giao thức

Mô hình OSI tách các mặt khác nhau của một mạng máy tính thành bảy tầng theo mô hình phân tầng. Mô hình OSI là một khung mà các tiêu chuẩn lập mạng khác nhau có thể khớp vào. Mô hình OSI định rõ các mặt nào của hoạt động của mạng có thể nhằm đến bởi các tiêu chuẩn mạng khác nhau. Vì vậy, theo một nghĩa nào đó, mô hình OSI là một loại tiêu chuẩn của các chuẩn.

III.1. Nguyên tắc sử dụng khi định nghĩa các tầng hệ thống mở

Sau đây là các nguyên tắc mà ISO quy định dùng trong quá trình xây dựng mô hình OSI

Không định nghĩa quá nhiều tầng để việc xác định và ghép nối các tầng không quá phức tạp.

Tạo các ranh giới các tầng sao cho việc giải thích các phục vụ và số các tương tác qua lại hai tầng là nhỏ nhất.

Tạo các tầng riêng biệt cho các chức năng khác biệt nhau hoàn toàn về kỹ thuật sử dụng hoặc quá trình thực hiện.

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 nghĩa thức của chúng có thể thay đổi trên mọi hướng.

Tạo ranh giới các tầng mà ở đó cần có những mức độ trừu tượng khác nhau trong việc sử dụng số liệu.

Cho phép thay đổi các chức năng hoặc giao thức trong tầng không ảnh hưởng đến các tầng khác.

Tạo các ranh giới giữa mỗi tầng với tầng trên và dưới nó.

III.2. Các giao thức trong mô hình OSI

Trong mô hình OSI có hai loại giao thức chính được áp dụng: giao thức có liên kết (connection-oriented) và giao thức không liên kết (connectionless).

Giao thức có liên kết: trước khi truyền dữ liệu hai tầng đồng mức cần thiết lập một liên kết logic và các gói tin được trao đổi thông qua liên kết 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:

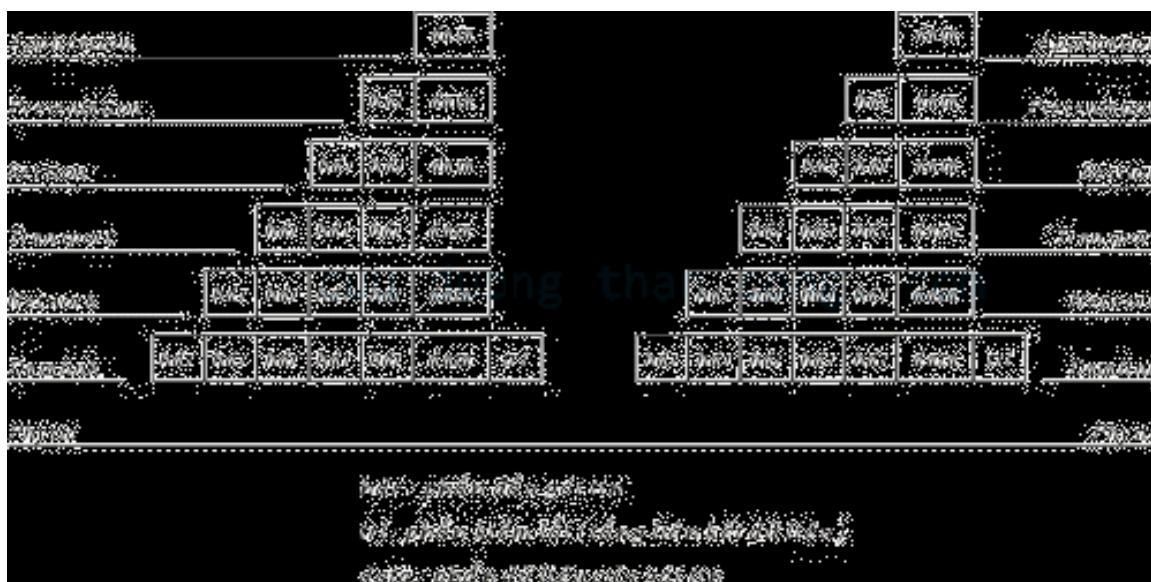
Thiết lập liên kết (logic): hai thực thể đồng mức ở hai hệ thống thương lượng với nhau về tập các tham số sẽ sử dụng trong giai đoạn sau (truyền dữ liệu).

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 mà thôi.

Gói tin của giao thức: Gói tin (Packet) được hiểu như là một đơn vị thông tin dùng trong việc liên lạc, chuyển giao dữ liệu trong mạng máy tính. Những thông điệp (message) trao đổi giữa các máy tính trong mạng, được tạo dạng thành các gói tin ở máy nguồn. Và những gói tin này khi đích sẽ được kết hợp lại thành thông điệp ban đầu. Một gói tin có thể chứa đựng các yêu cầu phục vụ, các thông tin điều khiển và dữ liệu.



Hình II-2 Phương thức xác lập các gói tin trong mô hình OSI

Trên quan điểm mô hình mạng phân tầng tầng mỗi tầng chỉ thực hiện một chức năng là nhận dữ liệu từ tầng bên trên để chuyển giao xuống cho tầng bên dưới và ngược lại. Chức năng này thực chất là gắn thêm và gỡ bỏ phần đầu (header) đối với các gói tin trước khi chuyển nó đi. Nói cách khác, từng gói tin bao gồm phần đầu (header) và phần dữ liệu. Khi đi đến một tầng mới gói tin sẽ được đóng thêm một phần đầu để 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.3. Các chức năng chủ yếu của các tầng của mô hình OSI.

III.3.1 Tầng 1: Vật lý (Physical)

Tầng vật lý (Physical layer) là tầng dưới cùng của mô hình OSI là. Nó mô tả các đặc trưng vật lý của mạng: Các loại cáp được dùng để nối các thiết bị, các loại đầu nối được dùng , các dây cáp có thể dài bao nhiêu v.v... Mặt khác các tầng vật lý cung cấp các đặc trưng điện của các tín hiệu được dùng để khi chuyển dữ liệu trên cáp từ một máy này đến một máy khác của mạng, kỹ thuật nối mạch điện, tốc độ cáp truyền dẫn.

Tầng vật lý không qui định một ý nghĩa nào cho các tín hiệu đó ngoài các giá trị nhị phân 0 và 1. Ở các tầng cao hơn của mô hình OSI ý nghĩa của các bit được truyền ở tầng vật lý sẽ được xác định.

Ví dụ: Tiêu chuẩn Ethernet cho cáp xoắn đôi 10 baseT định rõ các đặc trưng điện của cáp xoắn đôi, kích thước và dạng của các đầu nối, độ dài tối đa của cáp.

Khác với các tầng khác, tầng vật lý là không có gói tin riêng và do vậy không có phần đầu (header) chứa thông tin điều khiển, dữ liệu được truyền đi theo dòng bit. Một giao thức tầng vật lý tồn tại giữa các tầng vật lý để quy định về phương thức truyền (đồng bộ, phi đồng bộ), tốc độ truyền.

Các giao thức được xây dựng cho tầng vật lý được phân chia thành phân chia thành hai loại giao thức sử dụng phương thức truyền thông dị bộ (asynchronous) và phương thức truyền thông đồng bộ (synchronous).

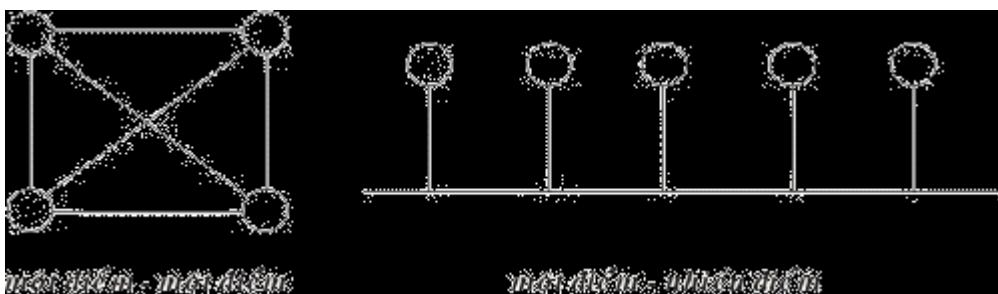
Phương thức truyền dị bộ: Không có một tín hiệu quy định cho sự đồng bộ giữa các bit giữa máy gửi và máy nhận, trong quá trình gửi tín hiệu máy gửi sử dụng các bit đặc biệt START và STOP được dùng để tách các xâu bit biểu diễn các ký tự trong dòng dữ liệu cần truyền đi. Nó cho phép một ký tự được truyền đi bất kỳ lúc nào mà không cần quan tâm đến các tín hiệu đồng bộ trước đó.

Phương thức truyền đồng bộ: Sử dụng phương thức truyền cần có đồng bộ giữa máy gửi và máy nhận, nó chèn các ký tự đặc biệt như SYN (Synchronization), EOT (End Of Transmission) hay đơn giản hơn, một cái "cờ" (flag) giữa các dữ liệu của máy gửi để báo hiệu cho máy nhận biết được dữ liệu đang đến hoặc đã đến.

III.3.2 Tầng 2: Liên kết dữ liệu (Data link)

Tầng liên kết dữ liệu (data link layer) là tầng mà ở đó ý nghĩa được gán cho các bít được truyền trên mạng. Tầng liên kết dữ liệu phải quy định được các dạng thức, kích thước, địa chỉ máy gửi và nhận của mỗi gói tin được gửi đi. Nó phải xác định cơ chế truy nhập thông tin trên mạng và phương tiện gửi mỗi gói tin sao cho nó được đưa đến cho người nhận đã định.

Tầng liên kết dữ liệu có hai phương thức liên kết dựa trên cách kết nối các máy tính, đó là phương thức "một điểm - một điểm" và phương thức "một điểm - nhiều điểm". Với phương thức "một điểm - một điểm" các đường truyền riêng biệt được thiết lập để nối các cặp máy tính lại với nhau. Phương thức "một điểm - nhiều điểm" tất cả các máy phân chia chung một đường truyền vật lý.



Hình II-3 : Các đường truyền kết nối kiểu "một điểm - một điểm" và "một điểm - nhiều điểm"

Tầng liên kết dữ liệu cũng cung cấp cách phát hiện và sửa lỗi cơ bản để đảm bảo cho dữ liệu nhận được giống hoàn toàn với dữ liệu gửi đi. Nếu một gói tin có lỗi không sửa được, tầng liên kết dữ liệu phải chỉ ra được cách thông báo cho nơi gửi biết gói tin đó có lỗi để nó gửi lại.

Các giao thức tầng liên kết dữ liệu chia làm 2 loại chính là các giao thức hướng ký tự và các giao thức hướng bit. Các giao thức hướng ký tự được xây dựng dựa trên các ký tự đặc biệt của một bộ mã chuẩn nào đó (như ASCII hay EBCDIC), trong khi đó các giao thức hướng bit lại dùng các cấu trúc nhị phân (xâu bit) để xây dựng các phần tử của giao thức (đơn vị dữ liệu, các thủ tục.) và khi nhận, dữ liệu sẽ được tiếp nhận lần lượt từng bit một.

III.3.3 Tầng 3: Mạng (Network)

Tầng mạng (network layer) nhằm 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.

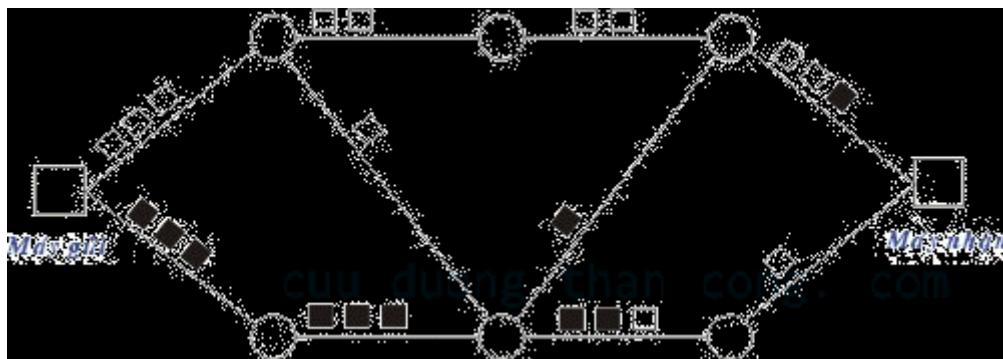
Tầng mạng cung cấp các phương tiện để truyền các gói tin qua mạng, thậm chí qua một mạng của mạng (network of network). Bởi vậy nó cần phải đáp ứng với nhiều kiểu mạng và nhiều kiểu dịch vụ cung cấp bởi các mạng khác nhau. Hai chức năng chủ yếu của tầng mạng là chọn đường (routing) và chuyển tiếp (relaying). 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 chẵng hạn) từ trạm nguồn tới trạm đích của nó. Một kỹ thuật chọn đường phải thực hiện hai chức năng chính sau đây:

Quyết định chọn đường tối ưu dựa trên các thông tin đã có về mạng tại thời điểm đó thông qua những tiêu chuẩn tối ưu nhất định.

Cập nhật các thông tin về mạng, tức là thông tin dùng cho việc chọn đường, trên mạng luôn có sự thay đổi thường xuyên nên việc cập nhật là việc cần thiết.



Hình II-4 Mô hình chuyển vận các gói tin trong mạng chuyển mạch gói

Người ta có hai phương thức đáp ứng cho việc chọn đường là phương thức xử lý tập trung và xử lý tại chỗ.

Phương thức chọn đường xử lý tập trung được đặc trưng bởi sự tồn tại của một (hoặc vài) trung tâm điều khiển mạng, chúng thực hiện việc lập ra các bảng đường đi tại từng thời điểm cho các nút và sau đó gửi các bảng chọn đường tới từng nút dọc theo con đường đã được chọn đó. Thông tin tổng thể của mạng cần dùng cho việc chọn đường chỉ cần cập nhập và được cất giữ tại trung tâm điều khiển mạng.

Phương thức chọn đường xử lý tại chỗ được đặc trưng bởi việc chọn đường được thực hiện tại mỗi nút của mạng. Trong từng thời điểm, mỗi nút phải duy trì các thông tin của mạng và tự xây dựng bảng chọn đường cho mình. Như vậy các thông tin tổng thể của mạng cần dùng cho việc chọn đường cần cập nhập và được cất giữ tại mỗi nút.

Thông thường các thông tin được đo lường và sử dụng cho việc chọn đường bao gồm:

Trạng thái của đường truyền.

Thời gian trễ khi truyền trên mỗi đường dẫn.

Mức độ lưu thông trên mỗi đường.

Các tài nguyên khả dụng của mạng.

Khi có sự thay đổi trên mạng (ví dụ thay đổi về cấu trúc của mạng do sự cố tại một vài nút, phục hồi của một nút mạng, nối thêm một nút mới... hoặc thay đổi về mức độ lưu thông) các thông tin trên cần được cập nhật vào các cơ sở dữ liệu về trạng thái của mạng.

Hiện nay khi nhu cầu truyền thông đa phương tiện (tích hợp dữ liệu văn bản, đồ họa, hình ảnh, âm thanh) ngày càng phát triển đòi hỏi các công nghệ truyền dẫn tốc độ cao nên việc phát triển các hệ thống chọn đường tốc độ cao đang rất được quan tâm.

III.3.4 Tầng 4: Vận chuyển (Transport)

Tầng vận chuyển cung cấp các chức năng cần thiết giữa tầng mạng và các tầng trên. nó là tầng cao nhất có liên quan đến các giao thức trao đổi dữ liệu giữa các hệ thống mở. Nó cùng các tầng dưới cung cấp cho người sử dụng các phục vụ vận chuyển.

Tầng vận chuyển (transport layer) là tầng cơ sở mà ở đó một máy tính của mạng chia sẻ thông tin với một máy khác. Tầng vận chuyển đồng nhất mỗi trạm bằng một địa chỉ duy nhất và quản lý sự kết nối giữa các trạm. Tầng vận chuyển cũng chia các gói tin lớn thành các gói tin nhỏ hơn trước khi gửi đi. Thông thường tầng vận chuyển đánh số các gói tin và đảm bảo chúng chuyển theo đúng thứ tự.

Tầng vận chuyển là tầng cuối cùng chịu trách nhiệm về mức độ an toàn trong truyền dữ liệu nên giao thức tầng vận chuyển phụ thuộc rất nhiều vào bản chất của tầng mạng. Người ta chia giao thức tầng mạng thành các loại sau:

Mạng loại A: Có tỷ suất lỗi và sự cố có báo hiệu chấp nhận được (tức là chất lượng chấp nhận được). Các gói tin được giả thiết là không bị mất. Tầng vận chuyển không cần cung cấp các dịch vụ phục hồi hoặc sắp xếp thứ tự lại.

Mạng loại B: Có tỷ suất lỗi chấp nhận được nhưng tỷ suất sự cố có báo hiệu lại không chấp nhận được. Tầng giao vận phải có khả năng phục hồi lại khi xảy ra sự cố.

Mạng loại C: Có tỷ suất lỗi không chấp nhận được (không tin cậy) hay là giao thức không liên kết. Tầng giao vận phải có khả năng phục hồi lại khi xảy ra lỗi và sắp xếp lại thứ tự các gói tin.

Trên cơ sở loại giao thức tầng mạng chúng ta có 5 lớp giao thức tầng vận chuyển đó là:

Giao thức lớp 0 (Simple Class - lớp đơn giản): cung cấp các khả năng rất đơn giản để thiết lập liên kết, truyền dữ liệu và hủy bỏ liên kết trên mạng "có liên kết" loại A. Nó có khả năng phát hiện và báo hiệu các lỗi nhưng không có khả năng phục hồi.

Giao thức lớp 1 (Basic Error Recovery Class - Lớp phục hồi lỗi cơ bản) dùng với các loại mạng B, ở đây các gói tin (TPDU) được đánh số. Ngoài ra giao thức còn có khả năng báo nhận cho nơi gửi và truyền dữ liệu khẩn. So với giao thức lớp 0 giao thức lớp 1 có thêm khả năng phục hồi lỗi.

Giao thức lớp 2 (Multiplexing Class - lớp đòn kênh) là một cải tiến của lớp 0 cho phép dồn một số liên kết chuyển vận vào một liên kết mạng duy nhất, đồng thời có thể kiểm soát luồng dữ liệu để tránh tắc nghẽn. Giao thức lớp 2 không có khả năng phát hiện và phục hồi lỗi. Do vậy nó cần đặt trên một tầng mạng loại A.

Giao thức lớp 3 (Error Recovery and Multiplexing Class - lớp phục hồi lỗi cơ bản và dồn kênh) là sự mở rộng giao thức lớp 2 với khả năng phát hiện và phục hồi lỗi, nó cần đặt trên một tầng mạng loại B.

Giao thức lớp 4 (Error Detection and Recovery Class - Lớp phát hiện và phục hồi lỗi) là lớp có hầu hết các chức năng của các lớp trước và còn bổ sung thêm một số khả năng khác để kiểm soát việc truyền dữ liệu.

III.3.5 Tầng 5: Giao dịch (Session)

Tầng giao dịch (session layer) thiết lập "các giao dịch" giữa các trạm trên mạng, nó đặt tên nhất quán cho mọi thành phần muốn đối thoại với nhau và lập ánh xa giữa các tên với địa chỉ của chúng. Một giao dịch phải được thiết lập trước khi dữ liệu được truyền trên mạng, tầng giao dịch đảm bảo cho các giao dịch được thiết lập và duy trì theo đúng qui định.

Tầng giao dịch còn cung cấp cho người sử dụng các chức năng cần thiết để quản trị các giao dịch 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 nảy sinh vấn đề: hai người sử dụng luân phiên phải "lấy lượt" để truyền dữ liệu. Tầng giao dịch duy trì tương tác luân phiên bằng cách báo cho mỗi người sử dụng khi đến lượt họ được truyền dữ liệu. Vấn đề đồng bộ hóa trong tầng giao dịch cũng được thực hiện như cơ chế kiểm tra/phục hồi, dịch vụ này cho phép người sử dụng xác định các điểm đồng bộ hóa trong dòng dữ liệu đang chuyển vận và khi cần thiết có thể khôi phục việc hội thoại bắt đầu từ một trong các điểm đó

Ở một thời điểm chỉ có một người sử dụng đó quyền đặc biệt được gọi các dịch vụ nhất định của tầng giao dịch, việc phân bổ các quyền này thông qua trao đổi thẻ bài (token). Ví dụ: Ai có được token sẽ có quyền truyền dữ liệu, và khi người giữ token trao token cho người khác thi cũng có nghĩa trao quyền truyền dữ liệu cho người đó.

Tầng giao dịch có các hàm cơ bản sau:

Give Token cho phép người sử dụng chuyển một token cho một người sử dụng khác của một liên kết giao dịch.

Please Token cho phép một người sử dụng chưa có token có thể yêu cầu token đó.

Give Control dùng để chuyển tất cả các token từ một người sử dụng sang một người sử dụng khác.

III.3.6 Tầng 6: Trình bày (Presentation)

Trong giao tiếp giữa các ứng dụng thông qua mạng với cùng một dữ liệu có thể có nhiều cách biểu diễn khác nhau. Thông thường dạng biểu diễn dùng bởi ứng dụng nguồn và dạng biểu diễn dùng bởi ứng dụng đích có thể khác nhau do các ứng dụng được chạy trên các hệ thống hoàn toàn khác nhau (như hệ máy Intel và hệ máy Motorola). Tầng trình bày (Presentation layer) phải chịu trách nhiệm chuyển đổi dữ liệu gửi đi trên mạng từ một loại biểu diễn này sang một loại

khác. Để đạt được điều đó nó cung cấp một dạng biểu diễn chung dùng để truyền thông và cho phép chuyển đổi từ dạng biểu diễn cục bộ sang biểu diễn chung và ngược lại.

Tầng trình bày cũng có thể được dùng kĩ thuật mã hóa để xáo trộn các dữ liệu trước khi được truyền đi và giải mã ở đầu đến để bảo mật. Ngoài ra tầng biểu diễn cũng có thể dùng các kĩ thuật nén sao cho chỉ cần một ít byte dữ liệu để thể hiện thông tin khi nó được truyền ở trên mạng, ở đầu nhận, tầng trình bày bung trở lại để được dữ liệu ban đầu.

III.3.7 Tầng 7: Ứng dụng (Application)

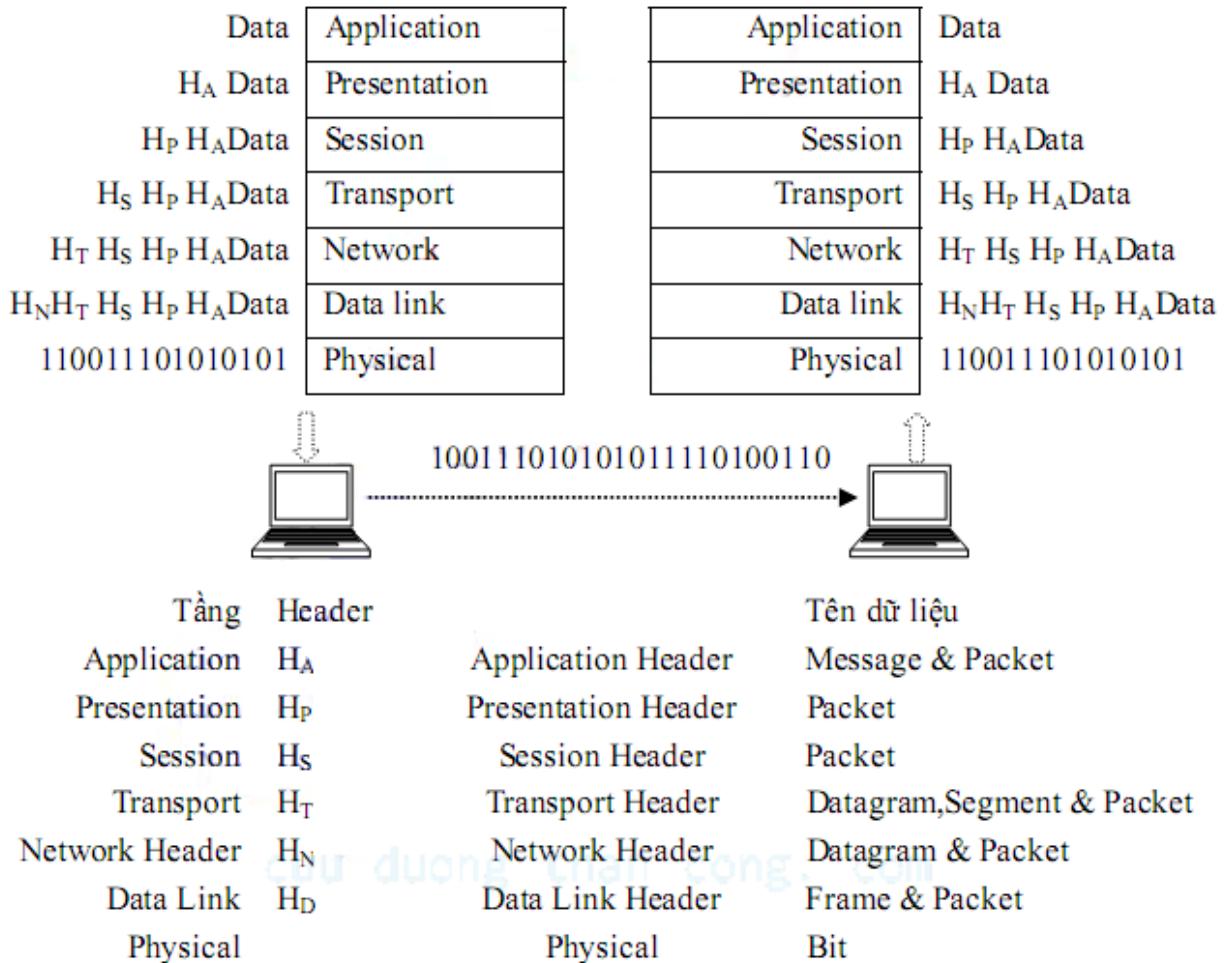
Tầng ứng dụng (Application layer) là tầng cao nhất của mô hình OSI, nó xác định giao diện giữa người sử dụng và môi trường OSI và giải quyết các kĩ thuật mà các chương trình ứng dụng dùng để giao tiếp với mạng.

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 tuân tự hóa các sự kiện đến từ các ASE thành tố của nó.

IV. Quá trình chuyển vận gói tin

IV.1. Quá trình đóng gói dữ liệu (tại máy gửi)

Đóng gói dữ liệu là quá trình đặt dữ liệu nhận được vào sau header (và trước trailer) trên mỗi lớp. Lớp Physical không đóng gói dữ liệu vì nó không dùng header và trailer. Việc đóng gói dữ liệu không nhất thiết phải xảy ra trong mỗi lần truyền dữ liệu của trình ứng dụng. Các lớp 5, 6, 7 sử dụng header trong quá trình khởi động, nhưng trong phần lớn các lần truyền thì không có header của lớp 5, 6, 7 lý do là không có thông tin mới để trao đổi.



Hình II-5 Bổ sung phần đầu thông điệp & tên dữ liệu sử dụng

Các dữ liệu tại máy gửi được xử lý theo trình tự như sau:

- Người dùng thông qua lớp Application để đưa các thông tin vào máy tính. Các thông tin này có nhiều dạng khác nhau như: hình ảnh, âm thanh, văn bản...
- Tiếp theo các thông tin đó được chuyển xuống lớp Presentation để chuyển thành dạng chung, rồi mã hoá và nén dữ liệu.
- Tiếp đó dữ liệu được chuyển xuống lớp Session để bổ sung các thông tin về phiên giao dịch này.
- Dữ liệu tiếp tục được chuyển xuống lớp Transport, tại lớp này dữ liệu được cắt ra thành nhiều Segment và bổ sung thêm các thông tin về phương thức vận chuyển dữ liệu để đảm bảo độ tin cậy khi truyền.
- Dữ liệu tiếp tục được chuyển xuống lớp Network, tại lớp này mỗi Segment được cắt ra thành nhiều Packet và bổ sung thêm các thông tin định tuyến.
- Tiếp đó dữ liệu được chuyển xuống lớp Data Link, tại lớp này mỗi Packet sẽ được cắt ra thành nhiều Frame và bổ sung thêm các thông tin kiểm tra gói tin (để kiểm tra ở nơi nhận).
- Cuối cùng, mỗi Frame sẽ được tầng Vật Lý chuyển thành một chuỗi các bit, và được đẩy lên các phương tiện truyền dẫn để truyền đến các thiết bị khác.

IV.2. Quá trình truyền dữ liệu từ máy gửi đến máy nhận.

Bước 1: Trình ứng dụng (trên máy gửi) tạo ra dữ liệu và các chương trình phần cứng, phần mềm cài đặt mỗi lớp sẽ bổ sung vào header và trailer (quá trình đóng gói dữ liệu tại máy gửi).

Bước 2: Lớp Physical (trên máy gửi) phát sinh tín hiệu lên môi trường truyền tải để truyền dữ liệu.

Bước 3: Lớp Physical (trên máy nhận) nhận dữ liệu.

Bước 4: Các chương trình phần cứng, phần mềm (trên máy nhận) gỡ bỏ header và trailer và xử lý phần dữ liệu (quá trình xử lý dữ liệu tại máy nhận).

Giữa bước 1 và bước 2 là quá trình tìm đường đi của gói tin. Thông thường, máy gửi đã biết địa chỉ IP của máy nhận. Vì thế, sau khi xác định được địa chỉ IP của máy nhận thì lớp Network của máy gửi sẽ so sánh địa chỉ IP của máy nhận và địa chỉ IP của chính nó:

- Nếu cùng địa chỉ mạng thì máy gửi sẽ tìm trong bảng MAC Table của mình để có được địa chỉ MAC của máy nhận. Trong trường hợp không có được địa chỉ MAC tương ứng, nó sẽ thực hiện giao thức ARP để truy tìm địa chỉ MAC. Sau khi tìm được địa chỉ MAC, nó sẽ lưu địa chỉ MAC này vào trong bảng MAC Table để lớp Datalink sử dụng ở các lần gửi sau. Sau khi có địa chỉ MAC thì máy gửi sẽ gói gói tin đi.

- Nếu khác địa chỉ mạng thì máy gửi sẽ kiểm tra xem máy có được khai báo Default Gateway hay không.

- + Nếu có khai báo Default Gateway thì máy gửi sẽ gởi gói tin thông qua Default Gateway.

- + Nếu không có khai báo Default Gateway thì máy gửi sẽ loại bỏ gói tin và thông báo "Destination host Unreachable"

IV.3. Chi tiết quá trình xử lý tại máy nhận

Bước 1: Lớp Physical kiểm tra quá trình đồng bộ bit và đặt chuỗi bit nhận được vào vùng đệm. Sau đó thông báo cho lớp Data Link dữ liệu đã được nhận.

Bước 2: Lớp Data Link kiểm lỗi frame bằng cách kiểm tra FCS trong trailer. Nếu có lỗi thì frame bị bỏ.

Sau đó kiểm tra địa chỉ lớp Data Link (địa chỉ MAC) xem có trùng với địa chỉ máy nhận hay không. Nếu đúng thì phần dữ liệu sau khi loại header và trailer sẽ được chuyển lên cho lớp Network.

Bước 3: Địa chỉ lớp Network được kiểm tra xem có phải là địa chỉ máy nhận hay không (địa chỉ IP) ? Nếu đúng thì dữ liệu được chuyển lên cho lớp Transport xử lý.

Bước 4: Nếu giao thức lớp Transport có hỗ trợ việc phục hồi lỗi thì số định danh phân đoạn được xử lý. Các thông tin ACK, NAK (gói tin ACK, NAK dùng để phản hồi về việc các gói tin đã được gởi đến máy nhận chưa) cũng được xử lý ở lớp này. Sau quá trình phục hồi lỗi và sắp thứ tự các phân đoạn, dữ liệu được đưa lên lớp Session.

Bước 5: Lớp Session đảm bảo một chuỗi các thông điệp đã trọn vẹn. Sau khi các luồng đã hoàn tất, lớp Session chuyển dữ liệu sau header lớp 5 lên cho lớp Presentation xử lý.

Bước 6: Dữ liệu sẽ được lớp Presentation xử lý bằng cách chuyển đổi dạng thức dữ liệu. Sau đó kết quả chuyển lên cho lớp Application.

Bước 7: Lớp Application xử lý header cuối cùng. Header này chứa các tham số thoả thuận giữa hai trình ứng dụng. Do vậy tham số này thường chỉ được trao đổi lúc khởi động quá trình truyền thông giữa hai trình ứng dụng.

V. Phương thức truyền tín hiệu

Thông thường có hai phương thức truyền tín hiệu trong mạng cục bộ là dùng băng tần cơ sở (baseband) và băng tần rộng (broadband). Sự khác nhau chủ yếu giữa hai phương thức truyền tín hiệu này là băng tần cơ sở chỉ chấp nhận một kênh dữ liệu duy nhất trong khi băng tần 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 tín hiệu có thể được truyền đi dưới cả hai dạng: tương tự (analog) hoặc số (digital). Phương thức truyền băng tần rộng chia giải thông (tần số) của đường truyền thành nhiều giải tần con trong đó mỗi dải tần con đó cung cấp một kênh truyền dữ liệu tách biệt nhờ sử dụng một cặp modem đặc biệt gọi là bộ giải / Điều biến RF cai quản việc biến đổi các tín hiệu số thành tín hiệu tương tự có tần số vô tuyến (RF) bằng kỹ thuật ghép kênh.

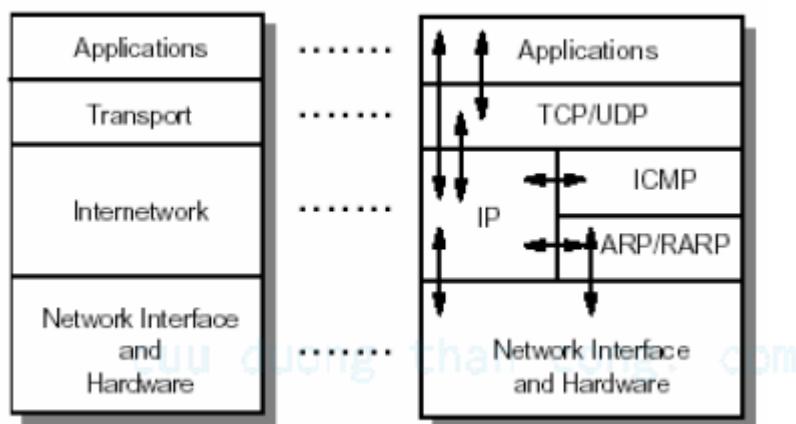
VI. Mô hình TCP/IP

VI.1. Tổng quan về bộ giao thức TCP/IP

TCP/IP là bộ giao thức cho phép kết nối các hệ thống mạng không đồng nhất với nhau. Ngày nay, TCP/IP được sử dụng rộng rãi trong các mạng cục bộ cũng như trên mạng Internet toàn cầu.

TCP/IP được xem là giản lược của mô hình tham chiếu OSI với bốn tầng như sau:

- Tầng liên kết mạng (Network Access Layer)
- Tầng Internet (Internet Layer)
- Tầng giao vận (Host-to-Host Transport Layer)
- Tầng ứng dụng (Application Layer)



Hình II-6 : Kiến trúc TCP/IP

Tầng liên kết:

Tầng liên kết (còn được gọi là tầng liên kết dữ liệu hay là tầng giao tiếp mạng) là tầng thấp nhất trong mô hình TCP/IP, bao gồm các thiết bị giao tiếp mạng và chương trình cung cấp các thông tin cần thiết để có thể hoạt động, truy nhập đường truyền vật lý qua thiết bị giao tiếp mạng đó.

Tầng Internet:

Tầng Internet (còn gọi là tầng mạng) xử lý qua trình truyền gói tin trên mạng. Các giao thức của tầng này bao gồm: IP (Internet Protocol), ICMP (Internet Control Message Protocol), IGMP (Internet Group Messages Protocol).

Tầng giao vận:

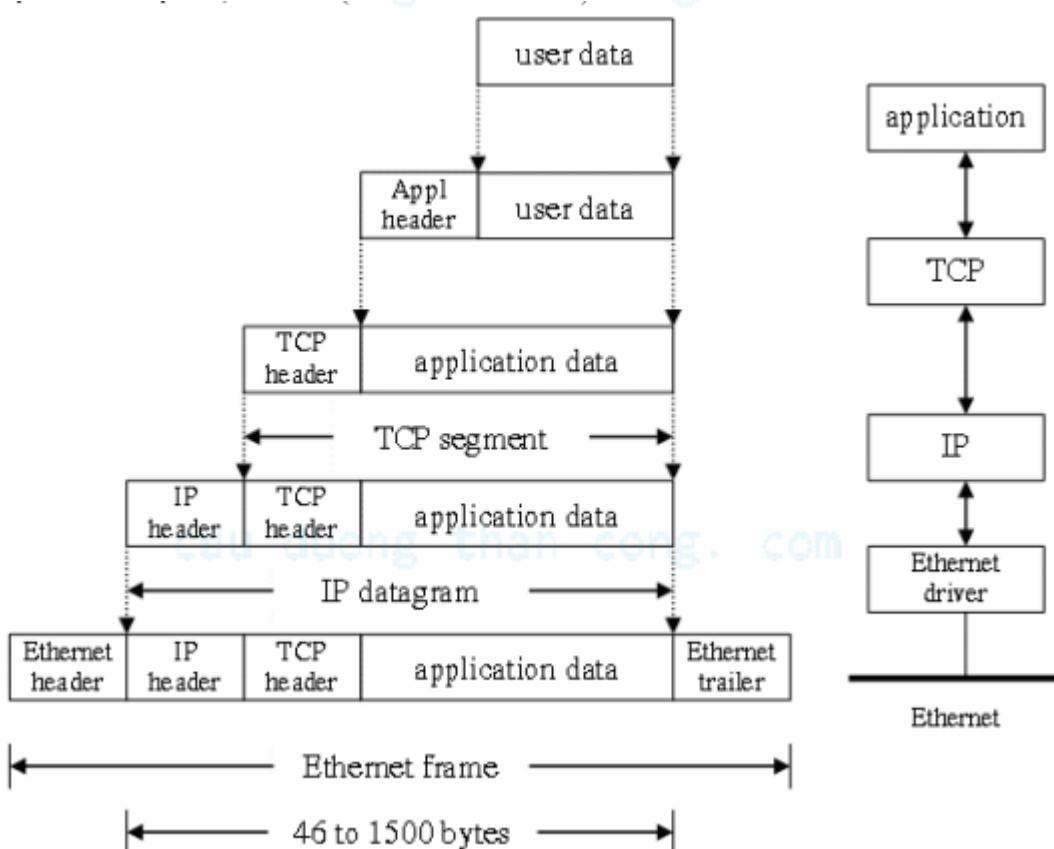
Tầng giao vận phụ trách luồng dữ liệu giữa hai trạm thực hiện các ứng dụng của tầng trên. Tầng này có hai giao thức chính: TCP (Transmission Control Protocol) và UDP (User Datagram Protocol).

TCP cung cấp một luồng dữ liệu tin cậy giữa hai trạm, nó sử dụng các cơ chế như chia nhỏ các gói tin của tầng trên thành các gói tin có kích thước thích hợp cho tầng mạng bên dưới, báo nhận gói tin, đặt hạn chế thời gian time-out để đảm bảo bên nhận biết được các gói tin đã gửi đi. Do tầng này đảm bảo tính tin cậy, tầng trên sẽ không cần quan tâm đến nữa.

UDP cung cấp một dịch vụ đơn giản hơn cho tầng ứng dụng. Nó chỉ gửi các gói dữ liệu từ trạm này tới trạm kia mà không đảm bảo các gói tin đến được tới đích. Các cơ chế đảm bảo độ tin cậy cần được thực hiện bởi tầng trên.

Tầng ứng dụng:

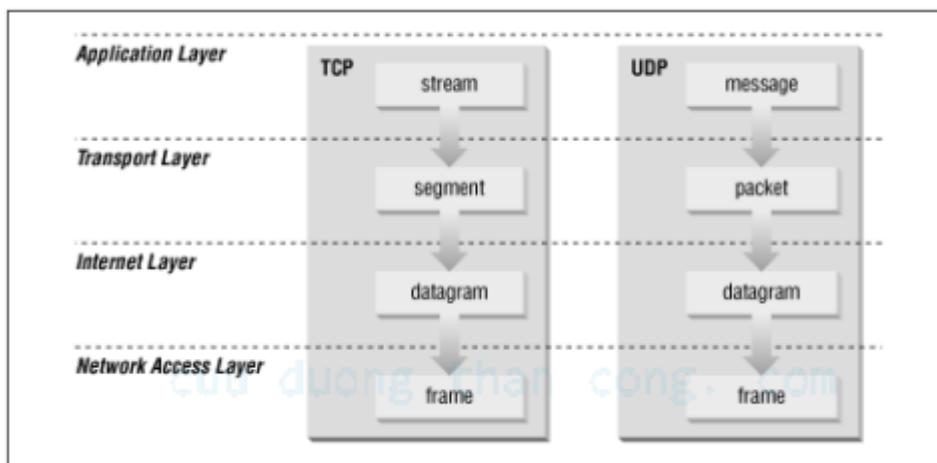
Tầng ứng dụng là tầng trên cùng của mô hình TCP/IP bao gồm các tiến trình và các ứng dụng cung cấp cho người sử dụng để truy cập mạng. Có rất nhiều ứng dụng được cung cấp trong tầng này, mà phổ biến là: Telnet: sử dụng trong việc truy cập mạng từ xa, FTP (File Transfer Protocol): dịch vụ truyền tệp, Email: dịch vụ thư tín điện tử, WWW (World Wide Web).



Hình II-7: Quá trình đóng/mở gói dữ liệu trong TCP/IP

Cũng tương tự như trong mô hình OSI, khi truyền dữ liệu, quá trình tiến hành từ tầng trên xuống tầng dưới, qua mỗi tầng dữ liệu được thêm vào một thông tin điều khiển được gọi là phần header. Khi nhận dữ liệu thì quá trình xảy ra ngược lại, dữ liệu được truyền từ tầng dưới lên và qua mỗi tầng thì phần header tương ứng được lấy đi và khi đến tầng trên cùng thì dữ liệu không còn phần header nữa. Hình vẽ sau cho ta thấy lược đồ dữ liệu qua các tầng. Trong hình vẽ này ta thấy tại các tầng khác nhau dữ liệu được mang những thuật ngữ khác nhau:

- Trong tầng ứng dụng dữ liệu là các luồng được gọi là stream.
- Trong tầng giao vận, đơn vị dữ liệu mà TCP gửi xuống tầng dưới gọi là TCP segment.
- Trong tầng mạng, dữ liệu mà IP gửi tới tầng dưới được gọi là IP datagram.
- Trong tầng liên kết, dữ liệu được truyền đi gọi là frame.



Hình II-8: Cấu trúc dữ liệu trong TCP/IP

VI.2. So sánh TCP/IP với OSI

Mỗi tầng trong TCP/IP có thể là một hay nhiều tầng của OSI.

Bảng sau chỉ rõ mối tương quan giữa các tầng trong mô hình TCP/IP với OSI

OSI	TCP/IP
Physical Layer và Data link Layer	Data link Layer
Network Layer	Internet Layer
Transport Layer	Transport Layer
Session Layer, Presentation Layer, Application Layer	Application Layer

Sự khác nhau giữa TCP/IP và OSI chỉ là:

- Tầng ứng dụng trong mô hình TCP/IP bao gồm luôn cả 3 tầng trên của mô hình OSI
- Tầng giao vận trong mô hình TCP/IP không phải luôn đảm bảo độ tin cậy của việc truyền tin như ở trong tầng giao vận của mô hình OSI mà cho phép thêm một lựa chọn khác là UDP

VII. Các giao thức truy cập đường truyền trên mạng LAN

Để truyền được dữ liệu trên mạng người ta phải có các thủ tục nhằm hướng dẫn các máy tính của mạng làm thế nào và lúc nào có thể thâm nhập vào đường dây cáp để gửi các gói dữ kiện. Ví dụ như đối với các dạng bus và ring thì chỉ có một đường truyền duy nhất nối các trạm với nhau, cho nên cần phải có các quy tắc chung cho tất cả các trạm nối vào mạng để đảm bảo rằng đường truyền được truy nhập và sử dụng một cách hợp lý.

Có nhiều giao thức khác nhau để truy nhập đường truyền vật lý nhưng phân thành hai loại: các giao thức truy nhập ngẫu nhiên và các giao thức truy nhập có điều khiển.

VII.1. Giao thức chuyển mạch (yêu cầu và chấp nhận)

Giao thức chuyển mạch là loại giao thức hoạt động theo cách thức sau: một máy tính của mạng khi cần có thể phát tín hiệu thâm nhập vào mạng, nếu vào lúc này đường cáp không bận thì mạch điều khiển sẽ cho trạm này thâm nhập vào đường cáp còn nếu đường cáp đang bận, nghĩa là đang có giao lưu giữa các trạm khác, thì việc thâm nhập sẽ bị từ chối.

VII.2. Giao thức đường dây đa truy cập với cảm nhận va chạm

Giao thức đường dây đa truy cập (Carrier Sense Multiple Access with Collision Detection hay CSMA/CD) cho phép nhiều trạm thâm nhập cùng một lúc vào mạng, giao thức này thường dùng trong sơ đồ mạng dạng đường thẳng. Mọi trạm đều có thể được truy nhập vào đường dây chung một cách ngẫu nhiên và do vậy có thể dẫn đến xung đột (hai hoặc nhiều trạm đồng thời cùng truyền dữ liệu). Các trạm phải kiểm tra đường truyền gói dữ liệu đi qua có phải của nó hay không. Khi một trạm muốn truyền dữ liệu nó phải kiểm tra đường truyền xem có rảnh hay không để gửi gói dữ liệu của, nếu đường truyền đang bận trạm phải chờ đợi chỉ được truyền khi thấy đường truyền rảnh. Nếu cùng một lúc có hai trạm cùng sử dụng đường truyền thì giao thức phải phát hiện điều này và các trạm phải ngưng thâm nhập, chờ đợi lần sau các thời gian ngẫu nhiên khác nhau.

Khi đường cáp đang bận trạm phải chờ đợi theo một trong ba phương thức sau:

- Trạm tạm chờ đợi một thời gian ngẫu nhiên nào đó rồi lại bắt đầu kiểm tra đường truyền.
- Trạm tiếp tục kiểm tra đường truyền đến khi đường truyền rảnh thì truyền dữ liệu đi.
- Trạm tiếp tục kiểm tra đường truyền đến 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 có gắng giảm thời gian trống của đường truyền bằng cách cho phép trạm có thể truyền ngay sau khi một cuộc truyền kết thúc song nếu lúc đó có thêm một trạm khác đang đợi thì khả năng xảy ra xung đột là rất cao. Phương thức 3 với giá trị p phải lựa chọn hợp lý có thể tối thiểu hóa được khả năng xung đột lẫn thời gian trống của đường truyền.

Khi lưu lượng các gói dữ liệu cần di chuyển trên mạng quá cao, thì việc dung độ có thể xảy ra với số lượng lớn có gây tắc nghẽn đường truyền dẫn đến làm chậm tốc độ truyền tin của hệ thống.

VII.3. Giao thức dùng thẻ bài vòng (Token ring)

Đây là giao thức truy nhập có điều khiển chủ yếu dùng kỹ thuật chuyển thẻ bài (token) để cấp phát quyền truy nhập đường truyền tức là quyền được truyền dữ liệu đi. Thẻ bài ở đây 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, nén gói dữ liệu có kèm theo địa chỉ nơi nhận vào thẻ bài và truyền đi theo chiều của vòng.

Vì thẻ bài chạy vòng quang trong mạng kín và chỉ có một thẻ nên việc đụng độ dữ liệu không thể xảy ra, do vậy hiệu suất truyền dữ liệu của mạng không thay đổi.

Trong các giao thức này cần giải quyết hai vấn đề có thể dẫn đến phá vỡ hệ thống. Một là việc mất thẻ bài làm cho trên vòng không còn thẻ bài lưu chuyển nữa. Hai là một thẻ bài bận lưu chuyển không dừng trên vòng.

VII.4. Giao thức dùng thẻ bài cho dạng đường thẳng (Token bus)

Đây là giao thức truy nhập có điều khiển trong để cấp phát quyền truy nhập đường truyền cho các trạm đang có nhu cầu truyền dữ liệu, một thẻ bài được lưu chuyển trên một vòng logic thiết lập bởi các trạm đó. Khi một trạm có thẻ bài thì nó có quyền sử dụng đường truyền trong một thời gian xác định trước. Khi đã hết dữ liệu hoặc hết thời đoạn cho phép, trạm chuyển thẻ bài đến trạm tiếp theo trong vòng logic.

Như vậy trong mạng phải thiết lập được vòng logic (hay còn gọi là vòng ảo) bao gồm các trạm đang hoạt động nối trong mạng được xác định vị trí theo một chuỗi thứ tự mà trạm cuối cùng của chuỗi sẽ tiếp liền sau bởi trạm đầu tiên. Mỗi trạm được biết địa chỉ của các trạm kè 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 luân chuyển theo dõi sự thay đổi theo trạng thái thực tế của mạng.

VIII. Các phương tiện kết nối mạng liên khu vực (WAN)

Bên cạnh phương pháp sử dụng đường điện thoại thuê bao để kết nối các mạng cục bộ hoặc mạng khu vực với nhau hoặc kết nối vào Internet, có một số phương pháp khác:

Đường thuê bao (leased line). Đây là phương pháp cũ nhất, là phương pháp truyền thống nhất cho sự kết nối vĩnh cửu. Bạn thuê đường dây từ công ty điện thoại (trực tiếp hoặc qua nhà cung cấp dịch vụ). Bạn cần phải cài đặt một "Channel Service Unit" (CSU) để nối đến mạng T, và một "Digital Service Unit" (DSU) để nối đến mạng chủ (primary) hoặc giao diện mạng.

ISDN (Integrated Service Digital Network). Sử dụng đường điện thoại số thay vì đường tương tự. Do ISDN là mạng dùng tín hiệu số, bạn không phải dùng một modem để nối với đường dây mà thay vào đó bạn phải dùng một thiết bị gọi là "codec" với modem có khả năng chạy ở 14.4 kbit/s. ISDN thích hợp cho cả hai trường hợp cá nhân và tổ chức. Các tổ chức có thể quan tâm hơn đến ISDN có khả năng cao hơn ("primary" ISDN) với tốc độ tổng cộng bằng tốc độ 1.544 Mbit/s của đường T1. Cước phí khi sử dụng ISDN được tính theo thời gian, một số trường hợp tính theo lượng dữ liệu được truyền đi và một số thì tính theo cả hai.

CATV link. Công ty dẫn cáp trong khu vực của bạn có thể cho bạn thuê một "chỗ" trên đường cáp của họ với giá hấp dẫn hơn với đường điện thoại. Cần phải biết những thiết bị gì cần cho hệ thống của mình và độ rộng của dải mà bạn sẽ được cung cấp là bao nhiêu. Cũng như việc đóng góp chi phí với những khách hàng khác cho kênh liên lạc đó là như thế nào. Một dạng kỳ lạ hơn được đưa ra với tên gọi là mạng "lai" ("hybrid" Network), với một kênh CATV được sử dụng để lưu thông theo một hướng và một đường ISDN hoặc gọi số sử dụng cho đường trở lại. Nếu muốn cung cấp thông tin trên Internet, bạn phải xác định chắc chắn rằng "kênh ngược" của bạn đủ khả năng phục vụ cho nhu cầu thông tin của khách hàng của bạn.

Frame relay. Frame relay "uyển chuyển" hơn đường thuê bao. Khách hàng thuê đường Frame relay có thể mua một dịch vụ có mức độ xác định - một "tốc độ thông tin uỷ thác" ("Committed Information Rate" - CIR). Nếu nhu cầu của bạn trên mạng là rất "bột phát" (bursty), hay người sử dụng của bạn có nhu cầu cao trên đường liên lạc trong suốt một khoảng thời gian xác định trong ngày, và có ít hoặc không có nhu cầu vào ban đêm - Frame relay có thể sẽ kinh tế hơn là thuê hoàn toàn một đường T1 (hoặc T3). Nhà cung cấp dịch vụ của bạn có thể đưa ra một phương pháp tương tự như là phương pháp thay thế đó là *Switched Multimegabit Data Service*.

Chế độ truyền không đồng bộ (Asynchronous Transfer Mode - ATM). ATM là một phương pháp tương đối mới đầu tiên báo hiệu cùng một kỹ thuật cho mạng cục bộ và liên khu vực. ATM thích hợp cho *real-time multimedia* song song với truyền dữ liệu truyền thống. ATM hứa hẹn sẽ trở thành một phần lớn của mạng tương lai.

Đường vi sóng (Microwave links). Nếu cần kết nối vĩnh viễn đến nhà cung cấp dịch vụ nhưng lại thấy rằng đường thuê bao hay những lựa chọn khác là quá đắt, bạn sẽ thấy *microwave* như là một lựa chọn thích hợp. Bạn không cần trả quá đắt cho cách này của *microwave*, tuy nhiên bạn cần phải đầu tư nhiều tiền hơn vào lúc đầu, và bạn sẽ gặp một số rủi ro như tốc độ truyền đến mạng của bạn quá nhanh.

Đường vệ tinh (satellite links). Nếu bạn muốn được chuyển một lượng lớn dữ liệu đặc biệt là từ những địa điểm từ xa thì đường vệ tinh là câu trả lời. Tầm hoạt động của những vệ tinh cùng vị trí địa lý với trái đất cũng tạo ra một sự chậm trễ (hoặc "bị che dấu") mà những người sử dụng Telnet có thể cảm nhận được.

Chương III Địa chỉ IP

I. Giao thức TCP/IP

Giao thức TCP/IP được phát triển từ mạng ARPANET và Internet và được dùng như giao thức mạng và vận chuyển trên mạng Internet. TCP (Transmission Control Protocol) là giao thức thuộc tầng vận chuyển và IP (Internet Protocol) là giao thức thuộc tầng mạng của mô hình OSI. Họ giao thức TCP/IP hiện nay là giao thức được sử dụng rộng rãi nhất để liên kết các máy tính và các mạng.

Hiện nay các máy tính của hầu hết các mạng có thể sử dụng giao thức TCP/IP để liên kết với nhau thông qua nhiều hệ thống mạng với kỹ thuật khác nhau. Giao thức TCP/IP thực chất là một họ giao thức cho phép các hệ thống mạng cùng làm việc với nhau thông qua việc cung cấp phương tiện truyền thông liên mạng.

II. Địa chỉ IP

II.1. Tổng quát

Nhiệm vụ chính của giao thức IP là cung cấp khả năng kết nối các mạng con thành liên kết mạng để truyền dữ liệu, vai trò của IP là vai trò của giao thức tầng mạng trong mô hình OSI. Giao thức IP là một giao thức kiểu không liên kết (connectionless) có nghĩa là không cần có giai đoạn thiết lập liên kết trước khi truyền dữ liệu.

Sơ đồ địa chỉ hóa để định danh các trạm (host) trong liên mạng được gọi là địa chỉ IP 32 bits (32 bit IP address). Mỗi giao diện trong 1 máy có hỗ trợ giao thức IP đều phải được gán 1 địa chỉ IP (một máy tính có thể gắn với nhiều mạng do vậy có thể có nhiều địa chỉ IP). Địa chỉ IP gồm 2 phần: địa chỉ mạng (netid) và địa chỉ máy (hostid). Mỗi địa chỉ IP có độ dài 32 bits được tách thành 4 vùng (mỗi vùng 1 byte), có thể biểu thị dưới dạng thập phân, bát phân, thập lục phân hay nhị phân. Cách viết phổ biến nhất là dùng ký pháp thập phân có dấu chấm (dotted decimal notation) để tách các vùng. Mục đích của địa chỉ IP là để định danh duy nhất cho một máy tính bất kỳ trên liên mạng.

Do tổ chức và độ lớn của các mạng con (subnet) của liên mạng có thể khác nhau, người ta chia các địa chỉ IP thành 5 lớp, ký hiệu là A, B, C, D và E. Trong lớp A, B, C chứa địa chỉ có thể gán được. Lớp D dành riêng cho lớp kỹ thuật multicasting. Lớp E được dành những ứng dụng trong tương lai.

Netid trong địa chỉ mạng dùng để nhận dạng từng mạng riêng biệt. Các mạng liên kết phải có địa chỉ mạng (netid) riêng cho mỗi mạng. Ở đây các bit đầu tiên của byte đầu tiên được dùng để định danh lớp địa chỉ (0 - lớp A, 10 - lớp B, 110 - lớp C, 1110 - lớp D và 11110 - lớp E).

Ở đây ta xét cấu trúc của các lớp địa chỉ có thể gán được là lớp A, lớp B, lớp C.

II.2. Cấu trúc của các địa chỉ IP

Mạng lớp A: địa chỉ mạng (netid) là 1 Byte và địa chỉ host (hostid) là 3 byte.

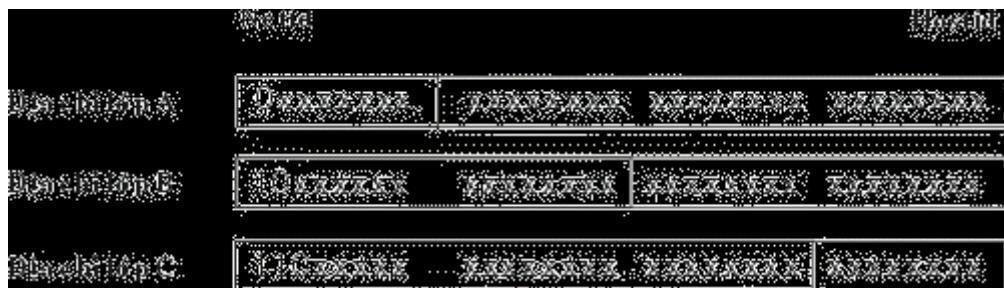
Mạng lớp B: địa chỉ mạng (netid) là 2 Byte và địa chỉ host (hostid) là 2 byte.

Mạng lớp C: địa chỉ mạng (netid) là 3 Byte và địa chỉ host (hostid) là 1 byte.

Lớp A cho phép định danh tới 126 mạng, với tối đa 16 triệu host trên mỗi mạng. Lớp này được dùng cho các mạng có số trạm cực lớn.

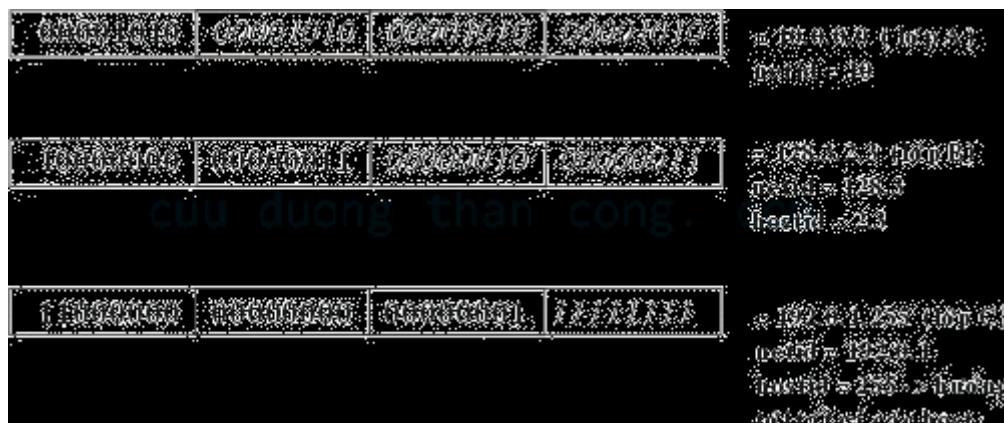
Lớp B cho phép định danh tới 16384 mạng, với tối đa 65534 host trên mỗi mạng.

Lớp C cho phép định danh tới 2 triệu mạng, với tối đa 254 host trên mỗi mạng. Lớp này được dùng cho các mạng có ít trạm.



Hình III-1: Cấu trúc các lớp địa chỉ IP

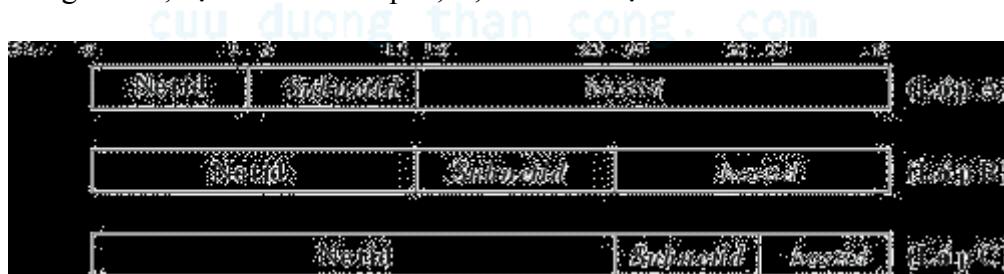
Một số địa chỉ có tính chất đặc biệt: Một địa chỉ có hostid = 0 được dùng để hướng tới mạng định danh bởi vùng netid. Ngược lại, một địa chỉ có vùng hostid gồm toàn số 1 được dùng để hướng tới tất cả các host nói vào mạng netid, và nếu vùng netid cũng gồm toàn số 1 thì nó hướng tới tất cả các host trong liên mạng



Hình III-2: Ví dụ cấu trúc các lớp địa chỉ IP

Cần lưu ý rằng các địa chỉ IP được dùng để định danh các host và mạng ở tầng mạng của mô hình OSI, và chúng không phải là các địa chỉ vật lý (hay địa chỉ MAC) của các trạm trên đó một mạng cục bộ (Ethernet, Token Ring).

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



Hình III-3: Ví dụ địa chỉ khi bổ sung vùng subnetid

Đơn vị dữ liệu dùng trong IP được gọi là gói tin (datagram), có khuôn dạng



Hình III-4: Dạng thức của gói tin IP

Ý nghĩa của thông số như sau:

- **VER** (4 bits): chỉ version hiện hành của giao thức IP hiện được cài đặt, Việc có chỉ số version cho phép có các trao đổi giữa các hệ thống sử dụng version cũ và hệ thống sử dụng version mới.
- **IHL** (4 bits): chỉ độ dài phần đầu (Internet header Length) của gói tin datagram, tính theo đơn vị từ (32 bits). Trường này bắt buộc 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 nghĩa 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:

0	1	2
0	DF	MF

- bit 0: reserved - chưa sử dụng, luôn lấy giá trị 0.
- bit 1: (DF) = 0 (May Fragment) = 1 (Don't Fragment)
- bit 2: (MF) = 0 (Last Fragment) = 1 (More 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 gửi 1 gói tin mà trường này có giá trị= 0.
- Một giao thức có thể áp dụng **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 (tùy theo từng chương trình).
- Padding (độ dài thay đổi): Vùng đệm, được dùng để đảm bảo cho phần header luôn kết thúc ở một mốc 32 bits.
- Data (độ dài thay đổi): Trên một mạng cục bộ như vậy, hai trạm chỉ có thể liên lạc với nhau nếu chúng biết địa chỉ vật lý của nhau. Như vậy vấn đề đặt ra là phải thực hiện ánh xạ giữa địa chỉ IP (32 bits) và địa chỉ vật lý (48 bits) của một trạm.

III. Một số khái niệm và thuật ngữ liên quan

Địa chỉ mạng (Network Address): là địa chỉ IP mà giá trị của tất cả các bits ở phần nhận dạng máy tính đều là 0, được sử dụng để xác định một mạng.

Ví dụ : 10.0.0.0; 172.18.0.0 ; 192.1.1.0

Địa chỉ quảng bá (Broadcast Address) : Là địa chỉ IP mà giá trị của tất cả các bits ở phần nhận dạng máy tính đều là 1, được sử dụng để chỉ tất cả các máy tính trong mạng.

Ví dụ : 10.255.255.255, 172.18.255.255, 192.1.1.255

Mặt nạ mạng chuẩn (Netmask) : Là địa chỉ IP mà giá trị của các bits ở phần nhận dạng mạng đều là 1, các bits ở phần nhận dạng máy tính đều là 0. Như vậy ta có 3 mặt nạ mạng tương ứng cho 3 lớp mạng A, B và C là :

- Mặt nạ mạng lớp A : 255.0.0.0
- Mặt nạ mạng lớp B : 255.255.0.0
- Mặt nạ mạng lớp C : 255.255.255.0

Ta gọi chúng là các mặt nạ mạng mặc định (Default Netmask)

Lưu ý : Địa chỉ mạng, địa chỉ quảng bá, mặt nạ mạng không được dùng để đặt địa chỉ cho các máy tính

Địa chỉ mạng 127.0.0.0 là địa chỉ được dành riêng để đặt trong phạm vi một máy tính. Nó chỉ có giá trị cục bộ (trong phạm vi một máy tính). Thông thường khi cài đặt giao thức IP thì máy tính sẽ được gán địa chỉ 127.0.0.1. Địa chỉ này thông thường để kiểm tra xem giao thức IP trên máy hiện tại có hoạt động không.

Địa chỉ dành riêng cho mạng cục bộ không kết nối trực tiếp Internet: Các mạng cục bộ không nối kết trực tiếp vào mạng Internet có thể sử dụng các địa chỉ mạng sau để đánh địa chỉ cho các máy tính trong mạng của mình :

- Lớp A : 10.0.0.0
- Lớp B : 172.16.0.0 đến 172.32.0.0
- Lớp C : 192.168.0.0

Ý nghĩa của Netmask

Với một địa chỉ IP và một Netmask cho trước, ta có thể dùng phép toán AND BIT để tính ra được địa chỉ mạng mà địa chỉ IP này thuộc về. Công thức như sau :

Network Address = IP Address & Netmask

Ví dụ : Cho địa chỉ IP = 198.53.147.45 và Netmask = 255.255.255.0. Ta thực hiện phép toán AND BIT (&) hai địa chỉ trên:

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

III.1. Các giao thức trong mạng IP

Để mạng với giao thức IP hoạt động được tốt người ta cần một số giao thức bổ sung, các giao thức này đều không phải là bộ phận của giao thức IP và giao thức IP sẽ dùng đến chúng khi cần.

- **Giao thức ARP (Address Resolution Protocol)**: Ở đây cần lưu ý rằng các địa chỉ IP được dùng để định danh các host và mạng ở tầng mạng của mô hình OSI, và chúng không phải là các địa chỉ vật lý (hay địa chỉ MAC) của các trạm trên đó một mạng cục bộ (Ethernet, Token Ring.). Trên một mạng cục bộ hai trạm chỉ có thể liên lạc với nhau nếu chúng biết địa chỉ vật lý của nhau. Như vậy vấn đề đặt ra là phải tìm được ánh xạ giữa địa chỉ IP (32 bits) và địa chỉ vật lý của một trạm. Giao thức ARP đã được xây dựng để tìm địa chỉ vật lý từ địa chỉ IP khi cần thiết.

- **Giao thức RARP (Reverse Address Resolution Protocol)**: Là giao thức ngược với giao thức ARP. Giao thức RARP được dùng để tìm địa chỉ IP từ địa chỉ vật lý.

- **Giao thức ICMP (Internet Control Message Protocol)**: Giao thức này thực hiện truyền các thông báo điều khiển (báo cáo về các tình trạng các lỗi trên mạng.) giữa các gateway hoặc một nút của liên mạng. Tình trạng lỗi có thể là: một gói tin IP không thể tới đích của nó, hoặc một router không đủ bộ nhớ đệm để lưu và chuyển một gói tin IP, Một thông báo ICMP được tạo và chuyển cho IP. IP sẽ "bọc" (encapsulate) thông báo đó với một IP header và truyền đến cho router hoặc trạm đích.

III.2. Các bước hoạt động của giao thức IP

Khi giao thức IP được khởi động nó trở thành một thực thể tồn tại trong máy tính và bắt đầu thực hiện những chức năng của mình, lúc đó thực thể IP là cấu thành của tầng mạng, nhận yêu cầu từ các tầng trên nó và gửi yêu cầu xuống các tầng dưới nó.

Đối với thực thể IP ở máy nguồn, khi nhận được một yêu cầu gửi từ tầng trên, nó thực hiện các bước sau đây:

- Tạo một IP datagram dựa trên tham số nhận được.
- Tính checksum và ghép vào header của gói tin.
- Ra quyết định chọn đường: hoặc là trạm đích nằm trên cùng mạng hoặc một gateway sẽ được chọn cho chặng tiếp theo.
- Chuyển gói tin xuống tầng dưới để truyền qua mạng.

Đối với router, khi nhận được một gói tin đi qua, nó thực hiện các động tác sau:

- 1) Tính checksum, nếu sai thì loại bỏ gói tin.
- 2) Giảm giá trị tham số Time - to Live. nếu thời gian đã hết thì loại bỏ gói tin.
- 3) Ra quyết định chọn đường.
- 4) Phân đoạn gói tin, nếu cần.
- 5) Kiến tạo lại IP header, bao gồm giá trị mới của các vùng Time - to -Live, Fragmentation và Checksum.
- 6) Chuyển datagram xuống tầng dưới để chuyển qua mạng.

Cuối cùng khi một datagram nhận bởi một thực thể IP ở trạm đích, nó sẽ thực hiện bởi các công việc sau:

- 1) Tính checksum. Nếu sai thì loại bỏ gói tin.
- 2) Tập hợp các đoạn của gói tin (nếu có phân đoạn)
- 3) Chuyển dữ liệu và các tham số điều khiển lên tầng trên.

IV. Giao thức điều khiển truyền dữ liệu TCP

TCP là một giao thức "có liên kết" (connection - oriented), nghĩa là cần phải thiết lập liên kết giữa hai thực thể TCP trước khi chúng trao đổi dữ liệu với nhau. Một tiến trình ứng dụng trong một máy tính truy nhập vào các dịch vụ của giao thức TCP thông qua một cổng (port) của TCP. Số hiệu cổng TCP được thể hiện bởi 2 bytes.



Hình III-5: Cổng truy nhập dịch vụ TCP

Một cổng TCP kết hợp với địa chỉ IP tạo thành một đầu nối TCP/IP (socket) duy nhất trong liên mạng. Dịch vụ TCP được cung cấp nhờ một liên kết logic giữa một cặp đầu nối TCP/IP. Một đầu nối TCP/IP có thể tham gia nhiều liên kết với các đầu nối TCP/IP ở xa khác nhau. Trước khi truyền dữ liệu giữa 2 trạm cần phải thiết lập một liên kết TCP giữa chúng và khi không còn nhu cầu truyền dữ liệu thì liên kết đó sẽ được giải phóng.

Các thực thể của tầng trên sử dụng giao thức TCP thông qua các hàm gọi (function calls) trong đó có các hàm yêu cầu để yêu cầu, để trả lời. Trong mỗi hàm còn có các tham số dành cho việc trao đổi dữ liệu.

IV.1. Các bước thực hiện để thiết lập một liên kết TCP/IP:

Thiết lập một liên kết mới có thể được mở theo một trong 2 phương thức: chủ động (active) hoặc bị động (passive).

- Phương thức bị động, người sử dụng yêu cầu TCP chờ đợi một yêu cầu liên kết gửi đến từ xa thông qua một đầu nối TCP/IP (tại chỗ). Người sử dụng dùng hàm passive Open có khai báo cổng TCP và các thông số khác (mức ưu tiên, mức an toàn)
- Với phương thức chủ động, người sử dụng yêu cầu TCP mở một liên kết với một đầu nối TCP/IP ở xa. Liên kết sẽ được xác lập nếu có một hàm Passive Open tương ứng đã được thực hiện tại đầu nối TCP/IP ở xa đó.

Bảng III-1 Lệt kê một vài cổng TCP phổ biến

Số hiệu cổng	Mô tả
0	Reserved
5	Remote job entry
7	Echo

9	Discard
11	Systat
13	Daytime
15	Nestat
17	Quotd (quote odd day)
20	ftp-data
21	ftp (control)
23	Telnet
25	SMTP
37	Time
53	Name Server
102	ISO - TSAP
103	X.400
104	X.400 Sending
111	Sun RPC
139	Net BIOS Session source
160 - 223	Reserved

Khi người sử dụng gửi đi một yêu cầu mở liên kết sẽ được nhận hai thông số trả lời từ TCP.

- Thông số Open ID được TCP trả lời ngay lập tức để gán cho một liên kết cục bộ (local connection name) cho liên kết được yêu cầu. Thông số này về sau được dùng để tham chiếu tới liên kết đó. (Trong trường hợp nếu TCP không thể thiết lập được liên kết yêu cầu thì nó phải gửi tham số Open Failure để thông báo.)
- Khi TCP thiết lập được liên kết yêu cầu nó gửi tham số Open Success được dùng để thông báo liên kết đã được thiết lập thành công. Thông báo này được chuyển đến cả hai trường hợp bị động và chủ động. Sau khi một liên kết được mở, việc truyền dữ liệu trên liên kết có thể được thực hiện.

IV.2. Các bước thực hiện khi truyền và nhận dữ liệu

Sau khi xác lập được liên kết người sử 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 receive:** 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 sử 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 xử lý khẩn cấp dữ liệu đó.

IV.3. Các bước thực hiện khi đóng một liên kết

Việc đóng một liên kết khi không cần thiết được thực hiện 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.

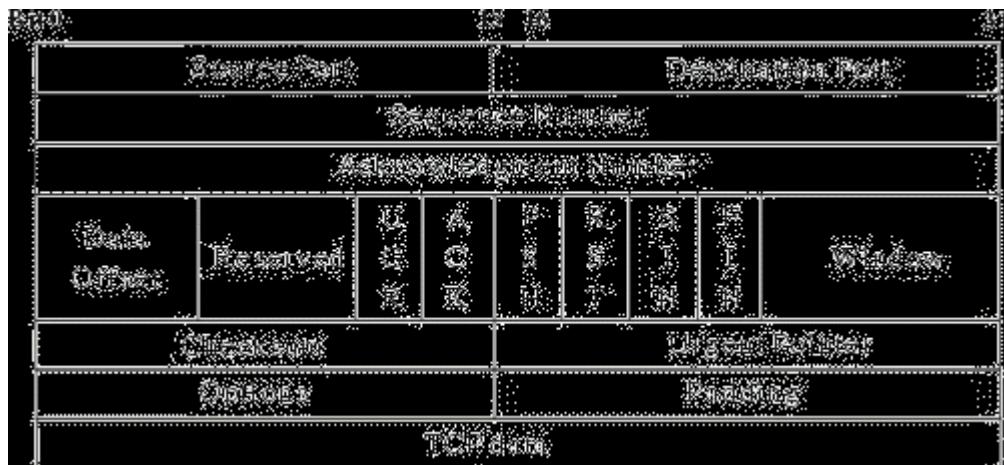
■ **Hàm Abort:** Người sử dụng có thể đóng một liên kết bất và sẽ không chấp nhận dữ liệu qua liên kết đó nữa. Do vậy dữ liệu có thể bị mất đi khi đang được truyền đi. TCP báo cho TCP ở xa biết rằng liên kết đã được hủy bỏ và TCP ở xa sẽ thông báo cho người sử dụng của mình.

IV.4. Một số hàm khác của TCP

■ **Hàm Status:** cho phép người sử dụng yêu cầu cho biết trạng thái của một liên kết cụ thể, khi đó TCP cung cấp thông tin cho người sử dụng.

■ **Hàm Error:** thông báo cho người sử dụng TCP về các yêu cầu dịch vụ bất hợp lệ liên quan đến một liên kết có tên cho trước hoặc về các lỗi liên quan đến môi trường.

Đơn vị dữ liệu sử dụng trong TCP được gọi là segment (đoạn dữ liệu), có các tham số với ý nghĩa như sau:



Hình III-6: Dạng thức của segment TCP

- Source Port (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. 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.
- 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 (Urgent Pointer) có hiệu lực.
 - ACK: Vùng báo nhận (ACK number) có hiệu lực.
 - PSH: Chức năng PUSH.
 - RST: Khởi động lại (reset) liên kết.
 - SYN: Đồng bộ hóa số hiệu tuần tự (sequence number).
 - FIN: Không còn dữ liệu từ trạm nguồn.
- Window (16 bit): cấp phát credit để kiểm soát nguồn dữ liệu (cơ chế cửa sổ). Đây chính là số lượng các byte dữ liệu, bắt đầu từ byte được chỉ ra trong vùng ACK number, mà trạm nguồn đã sẵn sàng để nhận.
- Checksum (16 bit): mã kiểm soát lỗi cho toàn bộ segment (header + data)

- Urgent Pointer (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.
- Padding (độ dài thay đổi): phần chèn thêm vào header để đảm bảo phần header luôn kết thúc ở một mốc 32 bit. Phần thêm này gồm toàn số 0.
- TCP data (độ dài thay đổi): chứa dữ liệu của tầng trên, có độ dài tối đa ngầm định là 536 byte. Giá trị này có thể điều chỉnh bằng cách khai báo trong vùng options.

V. Giao thức UDP (User Datagram Protocol)

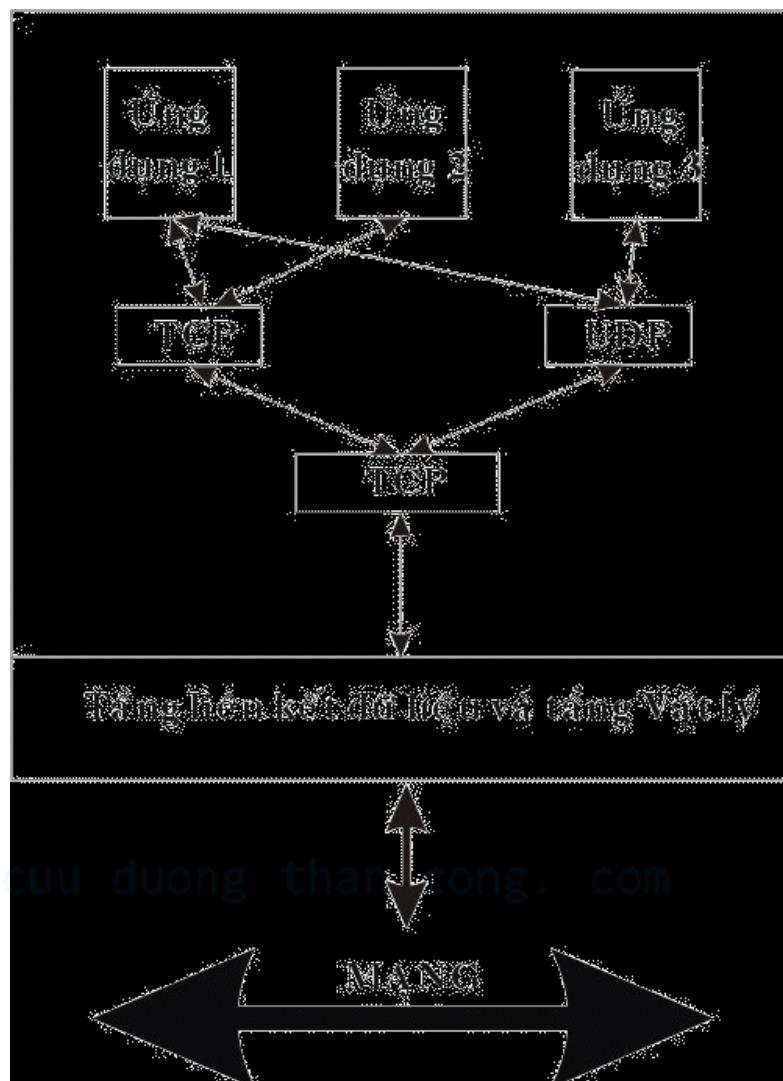
UDP (User Datagram Protocol) là giao thức theo phương thức không liên kết được sử dụng thay thế cho TCP ở trên IP theo yêu cầu của từng ứng dụng. Khác với TCP, UDP không có các chức năng thiết lập và kết thúc liên kết. Tương tự như IP, nó cũng không cung cấp cơ chế báo nhận (acknowledgment), không sắp xếp tuần tự các gói tin (datagram) đến và có thể dẫn đến tình trạng mất hoặc trùng dữ liệu mà không có cơ chế thông báo lỗi cho người gửi. Qua đó ta thấy UDP cung cấp các dịch vụ vận chuyển không tin cậy như trong TCP.

Khuôn dạng UDP datagram được mô tả với các vùng tham số đơn giản hơn nhiều so với TCP segment.



Hình III-7: Dạng thức của gói tin UDP

UDP cũng cung cấp cơ chế gán và quản lý các số hiệu cổng (port number) để định danh duy nhất cho các ứng dụng chạy trên một trạm của mạng. Do ít chức năng phức tạp nên UDP thường có xu hướng hoạt động nhanh hơn so với TCP. Nó thường được dùng cho các ứng không đòi hỏi độ tin cậy cao trong giao vận.



Hình III-8: Mô hình quan hệ họ giao thức TCP/IP

cuu duong than cong. com

VI. Địa chỉ IPv4

VI.1. Thành phần và hình dạng của địa chỉ IP

Địa chỉ IP đang được sử dụng hiện tại (IPv4) có 32 bit chia thành 4 Octet (mỗi Octet có 8 bit, tương đương 1 byte) cách nhau đều từ trái qua phải bit 1 cho đến bit 32, các Octet tách biệt nhau bằng dấu chấm (.), bao gồm có 3 thành phần chính.

class bit	Net ID	Host ID
--------------	--------	---------

Bit 1.....Bit 32

* Bit nhận dạng lớp (Class bit)

* Địa chỉ của đường mạng (Net ID)

* Địa chỉ của máy tính (Host ID).

Bit nhận dạng lớp (Class bit) để phân biệt địa chỉ ở lớp nào.

1. Địa chỉ Internet biểu hiện ở dạng bit nhị phân:

x y x y x y x y. x y x y x y x y. x y x y x y x y. x y x y x y x y

x, y = 0 hoặc 1.

Ví dụ:

0	0 1 0 1 1 0.	0 1 1 1 1 0 1 1.	0 1 1 0 1 1 1 0.	1 1 1 0 0 0 0 0
Bit nhận dạng	Octet 1	Octet 2	Octet 3	Octet 4

2. Địa chỉ Internet biểu hiện ở dạng thập phân:

xxx.xxx.xxx.xxx

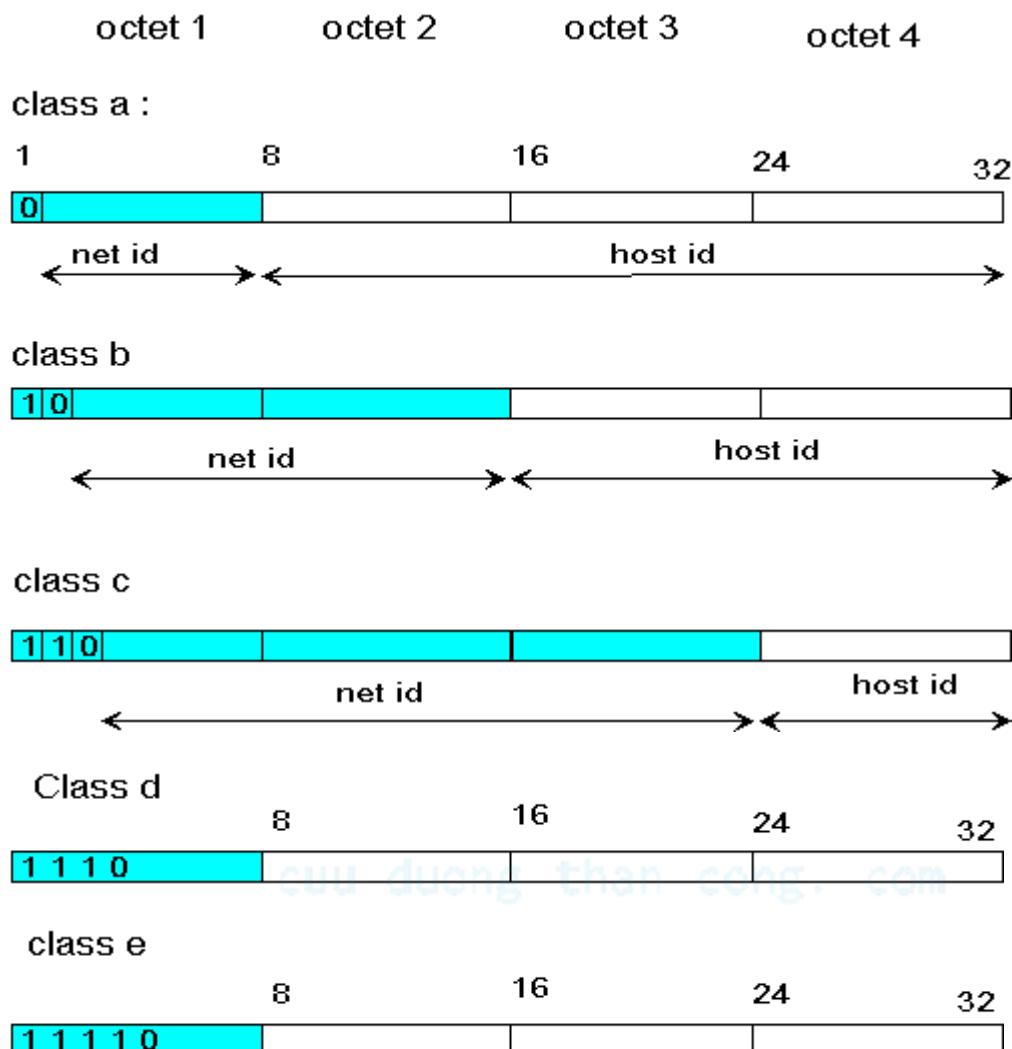
x là số thập phân từ 0 đến 9

Ví dụ: 146. 123. 110. 224

Dạng viết đầy đủ của địa chỉ IP là 3 con số trong từng Octet. Ví dụ: địa chỉ IP thường thấy trên thực tế có thể là 53.143.10.2 nhưng dạng đầy đủ là 053.143.010.002.

VI.2. Các lớp địa chỉ IP

Địa chỉ IP chia ra 5 lớp A,B,C, D, E. Hiện tại đã dùng hết lớp A,B và gần hết lớp C, còn lớp D và E Tổ chức internet đang để dành cho mục đích khác không phân, nên chúng ta chỉ nghiên cứu 3 lớp đầu.



Qua cấu trúc các lớp địa chỉ IP chúng ta có nhận xét sau:

- * Bit nhận dạng là những bit đầu tiên - của lớp A là 0, của lớp B là 10, của lớp C là 110.
 - * Lớp D có 4 bit đầu tiên để nhận dạng là 1110, còn lớp E có 5 bit đầu tiên để nhận dạng là 11110.
 - * Địa chỉ lớp A: Địa chỉ mạng ít và địa chỉ máy chủ trên từng mạng nhiều.
 - * Địa chỉ lớp B: Địa chỉ mạng vừa phải và địa chỉ máy chủ trên từng mạng vừa phải.
 - * Địa chỉ lớp C: Địa chỉ mạng nhiều, địa chỉ máy chủ trên từng mạng ít.

Địa chỉ lớp	Vùng địa chỉ lý thuyết	Số mạng tối đa sử dụng	Số máy chủ tối đa trên từng mạng
A	Từ 0.0.0.0 đến 127.0.0.0	126	16777214
B	Từ 128.0.0.0 đến 191.255.0.0	16382	65534
C	Từ 192.0.0.0 đến 223.255.255.0	2097150	254

D	Từ 224.0.0.0 đến 240.0.0.0	Không phân	
E	Từ 241.0.0.0 đến 255.0.0.0	Không phân	

Bảng III-2 Các lớp địa chỉ IP

Địa chỉ lớp	Vùng địa chỉ sử dụng	Bit nhận dạng	Số bit dùng để phân cho mạng
A	Từ 1 đến 127	0	7
B	Từ 128.1 đến 191.254	10	14
C	Từ 192.0.1 đến 223.255.254	110	21
D		1110	---
E		11110	---

Bảng III-3 Bit nhận dạng các lớp

Như vậy nếu chúng ta thấy 1 địa chỉ IP có 4 nhóm số cách nhau bằng dấu chấm, nếu thấy nhóm số thứ nhất nhỏ hơn 126 biết địa chỉ này ở lớp A, nằm trong khoảng 128 đến 191 biết địa chỉ này ở lớp B và từ 192 đến 223 biết địa chỉ này ở lớp C.

VII. IPv6

VII.1. Giao thức liên mạng thế hệ mới (IPv6)

Giao thức IPv4 đã được coi là nền tảng cho mạng Internet với những tính chất ưu việt của nó, tuy nhiên với sự bùng nổ về Internet giao thức IPv4 đã bộc lộ một số yếu điểm về tính năng, trong đó nổi bật là:

- Thiếu hụt về tính năng xác thực, an ninh của gói tin trên mạng. Khả năng mở rộng hạn chế.
- Thiếu hụt không gian địa chỉ. Với sự phát triển của mạng Internet, không gian địa chỉ IP có thể sử dụng thực sự là rất nhỏ do các địa chỉ lớp A được dành chủ yếu cho các công ty cung cấp dịch vụ lớn tại Mỹ và rất hạn chế trong việc cấp phát. Các địa chỉ lớp B nhanh chóng bị sử dụng hết do nó cung cấp số địa chỉ vừa phải. Hiện nay nhiều yêu cầu chỉ được đáp ứng bằng các địa chỉ lớp C với số địa chỉ rất hạn chế.
- Sự gia tăng số lượng các chỉ mục trong bảng định tuyến do cơ chế định tuyến không phân cấp dẫn đến yêu cầu nâng cấp các router và định tuyến không hiệu quả.
- Ngày nay, với các nhu cầu kết nối vào mạng Internet của các dịch vụ khác như điện thoại di động, truyền hình số,... đòi hỏi giao thức IPv4 cần có các sửa đổi để đáp ứng các nhu cầu mới.

Trước những nhu cầu này, giao thức liên mạng thế hệ mới IPv6 đã ra đời nhằm thay thế cho IPv4, nhưng cho đến nay IPv6 vẫn chỉ mới chủ yếu là đang trong quá trình thử nghiệm và hoàn thiện. Trong khuôn khổ giáo trình cũng đề cập một cách tổng quát về giao thức liên mạng thế hệ mới IPv6.

VII.2. Một số đặc điểm mới của IPv6:

- Khuôn dạng header mới: Header của IPv6 được thiết kế để giảm chi phí đến mức tối thiểu. Điều này đạt được bằng cách chuyển các trường lựa chọn sang các header

mở rộng được đặt phía sau của IPv6 header. Khuôn dạng mới của IPv6 tạo ra sự xử lý hiệu quả hơn tại các router.

- Header của IPv4 và IPv6 không thể xử lý chung. Một trạm hay một router phải cài đặt cả IPv4 và IPv6 để có thể xử lý được cả hai khuôn dạng header này. Header của IPv6 chỉ có kích thước gấp 2 lần header của IPv4 mặc dù không gian địa chỉ của IPv6 lớn gấp 4 lần không gian địa chỉ IPv4.
- Không gian địa chỉ lớn: IPv6 có địa chỉ nguồn và đích dài 128 bit. Mặc dù 128 bit có thể tạo ra hơn 3.4×10^{38} tổ hợp, không gian địa chỉ của IPv6 được thiết kế cho phép phân bổ địa chỉ và mạng con từ trực xuong sống Internet đến từng mạng con trong một tổ chức.
- Hiện tại chỉ một lượng nhỏ các địa chỉ hiện đang được phân bổ để sử dụng bởi các trạm, vẫn còn dư thừa rất nhiều địa chỉ sẵn sàng cho việc sử dụng trong tương lai.
- Hiệu quả, phân cấp địa chỉ hóa và hạ tầng định tuyến: Các địa chỉ toàn cục của IPv6 được thiết kế để tạo ra một hạ tầng định tuyến hiệu quả, phân cấp và có thể tổng quát hóa dựa trên sự phân cấp thường thấy của các nhà cung cấp dịch vụ (ISP) trên thực tế.
- Hỗ trợ chất lượng dịch vụ (QoS) tốt hơn: Các trường mới trong header của IPv6 định ra cách thức xử lý và định danh trên mạng. Giao thông trên mạng được định danh nhờ trường gán nhãn luồng (Flow Label) cho phép router có thể nhận ra và cung cấp các xử lý đặc biệt đối với các gói tin thuộc về một luồng nhất định, một chuẩn các gói tin giữa nguồn và đích.

Do giao thông mạng được xác định trong header, các dịch vụ QoS có thể được thực hiện ngay cả khi phần dữ liệu được mã hóa theo IPSec.

- Khả năng mở rộng: IPv6 có thể dễ dàng mở rộng thêm các tính năng mới bằng việc thêm các header mới sau header IPv6.

VII.3. Kiến trúc địa chỉ trong IPv6:

VII.3.1 Không gian địa chỉ:

- IPv6 sử dụng địa chỉ có độ dài lớn hơn IPv4 (128 bit so với 32 bit) do đó cung cấp không gian địa chỉ lớn hơn rất nhiều. Trong khi không gian địa chỉ 32 bit của IPv4 cho phép khoảng 4 tỷ địa chỉ, không gian địa chỉ của

IPv6 có thể có khoảng 3.4×10^{38} địa chỉ. Số lượng địa chỉ này rất lớn, hỗ trợ khoảng 6.5×10^{23} địa chỉ trên mỗi mét vuông bề mặt trái đất. Địa chỉ IPv6 128 bit được chia thành các miền phân cấp theo trật tự trên Internet.

Nó tạo ra nhiều mức phân cấp và linh hoạt trong địa chỉ hóa và định tuyến còn đang thiếu trong IPv4.

- Không gian địa chỉ IPv6 được chia trên cơ sở các bit đầu trong địa chỉ. Trường có độ dài thay đổi bao gồm các bit đầu tiên trong địa chỉ gọi là tiền tố định dạng (Format Prefix) FP.
- Ban đầu chỉ mới có 15% lượng địa chỉ được sử dụng, 85% còn lại để dùng trong tương lai.
- Các tiền tố định dạng từ 001 đến 111, ngoại trừ kiểu địa chỉ multicast (1111 1111) đều bắt buộc có định danh giao diện theo khuôn dạng EUI-64.

- Các địa chỉ dự trù không lắn với các địa chỉ chưa cấp phát. Chúng chiếm 1/256 không gian địa chỉ ($FP = 0000\ 0000$) và dùng cho các địa chỉ chưa chỉ định, địa chỉ quay vòng và các địa chỉ IPv6 có nhúng IPv4

VII.3.2 Cú pháp địa chỉ:

Các địa chỉ IPv6 dài 128 bit, khi viết mỗi nhóm 16 bit được biểu diễn thành một số nguyên không dấu dưới dạng hệ 16 và được phân tách bởi dấu hai chấm (:),

Ví dụ: FEDC:BA98:7654:3210:FEDC:BA98:7654:3210

Trên thực tế địa chỉ IPv6 thường có nhiều số 0, ví dụ địa chỉ:

1080:0000:0000:0000:0008:0800:200C:417A. Do đó cơ chế nén địa chỉ được dùng để biểu diễn dễ dàng hơn các loại địa chỉ dạng này. Ta không cần viết các số 0 ở đầu mỗi nhóm, ví dụ 0 thay cho 0000, 20 thay cho 0020.

Địa chỉ trong ví dụ trên sẽ trở thành 1080:0:0:8:800:200C:417A.

Hơn nữa ta có thể sử dụng ký hiệu :: để chỉ một chuỗi số 0. Địa chỉ trong ví dụ trên sẽ trở thành: 1080::8:800:200C:417A. Do địa chỉ IPv6 có độ dài cố định, ta có thể tính được số các bit 0 mà ký hiệu đó biểu diễn.

Tiền tố địa chỉ IPv6 được biểu diễn theo ký pháp CIDR như IPv4 như sau:

IPv6-address/prefix length trong đó IPv6-address là bất kỳ kiểu biểu diễn nào, còn prefix length là độ dài tiền tố theo bit.

Ví dụ: biểu diễn mạng con có tiền tố 80 bit: 1080:0:0:0:8::/80.

Với node address: 12AB:0:0:CD30:123:4567:89AB:CDEF,

prefix: 12AB:0:0:CD30::/60 có thể viết tắt thành

12AB:0:0:CD30:123:4567:89AB:CDEF/60

Chương IV Thiết bị mạng

I. Môi trường truyền dẫn

I.1. Khái niệm

Trên một mạng máy tính, các dữ liệu được truyền trên một môi trường truyền dẫn (transmission media), nó là phương tiện vật lý cho phép truyền tải tín hiệu giữa các thiết bị. Có hai loại phương tiện truyền dẫn chủ yếu:

- Hữu tuyến (bounded media)
- Vô tuyến (boundless media)

Thông thường hệ thống mạng sử dụng hai loại tín hiệu là: digital và analog.

I.2. Tần số truyền thông

Phương tiện truyền dẫn giúp truyền các tín hiệu điện tử từ máy tính này sang máy tính khác. Các tín hiệu điện tử này biểu diễn các giá trị dữ liệu theo dạng các xung nhị phân (bật/tắt). Các tín hiệu truyền thông giữa các máy tính và các thiết bị là các dạng sóng điện từ trải dài từ tần số radio đến tần số hồng ngoại.

Các sóng tần số radio thường được dùng để phát tín hiệu LAN. Các tần số này có thể được dùng với cáp xoắn đôi, cáp đồng trực hoặc thông qua việc truyền phủ sóng radio.

Sóng viba (microwave) thường dùng truyền thông tập trung giữa hai điểm hoặc giữa các trạm mặt đất và các vệ tinh, ví dụ như mạng điện thoại cellular.

Tia hồng ngoại thường dùng cho các kiểu truyền thông qua mạng trên các khoảng cách tương đối ngắn và có thể phát được sóng giữa hai điểm hoặc từ một điểm phủ sóng cho nhiều trạm thu. Chúng ta có thể truyền tia hồng ngoại và các tần số ánh sáng cao hơn thông qua cáp quang.

I.3. Các đặc tính của phương tiện truyền dẫn

Mỗi phương tiện truyền dẫn đều có những tính năng đặc biệt thích hợp với mỗi kiểu dịch vụ cụ thể, nhưng thông thường chúng ta quan tâm đến những yếu tố sau:

- Chi phí
- Yêu cầu cài đặt
- Độ bảo mật
- Băng thông (bandwidth): được xác định bằng tổng lượng thông tin có thể truyền dẫn trên đường truyền tại một thời điểm. Băng thông là một số xác định, bị giới hạn bởi phương tiện truyền dẫn, kỹ thuật truyền dẫn và thiết bị mạng được sử dụng. Băng thông là một trong những thông số dùng để phân tích độ hiệu quả của đường mạng. Đơn vị của băng thông:
 - + Bps (Bits per second-số bit trong một giây): đây là đơn vị cơ bản của băng thông.
 - + KBps (Kilobits per second): 1 KBps=103 bps=1000 Bps
 - + MBps (Megabits per second): 1 MBps = 103 KBps
 - + GBps (Gigabits per second): 1 GBps = 103 MBps
 - + TBps (Terabits per second): 1 TBps = 103 GBPS.
- Thông lượng (Throughput): lượng thông tin thực sự được truyền dẫn trên thiết bị tại một thời điểm.

- **Băng tầng cơ sở (baseband)**: dành toàn bộ băng thông cho một kênh truyền, băng tầng mở rộng (broadband): cho phép nhiều kênh truyền chia sẻ một phương tiện truyền dẫn (chia sẻ băng thông).
- **Độ suy giảm (attenuation)**: độ đo sự suy yếu đi của tín hiệu khi di chuyển trên một phương tiện truyền dẫn. Các nhà thiết kế cáp phải chỉ định các giới hạn về chiều dài dây cáp vì khi cáp dài sẽ dẫn đến tình trạng tín hiệu yếu đi mà không thể phục hồi được.
- **Nhiều điện từ (Electromagnetic interference - EMI)**: bao gồm các nhiễu điện từ bên ngoài làm biến dạng tín hiệu trong một phương tiện truyền dẫn.
- **Nhiều xuyên kênh (crosstalk)**: hai dây dẫn đặt kề nhau làm nhiễu lẫn nhau.

I.4. Các kiểu truyền dẫn.

Có các kiểu truyền dẫn như sau:

Đơn công (Simplex): Trong kiểu truyền dẫn này, thiết bị phát tín hiệu và thiết bị nhận tín hiệu được phân biệt rõ ràng, thiết bị phát chỉ đảm nhiệm vai trò phát tín hiệu, còn thiết bị thu chỉ đảm nhiệm vai trò nhận tín hiệu. Truyền hình là một ví dụ của kiểu truyền dẫn này.

Bán song công (Half-Duplex): trong kiểu truyền dẫn này, thiết bị có thể là thiết bị phát, vừa là thiết bị thu. Nhưng tại một thời điểm thì chỉ có thể ở một trạng thái (phát hoặc thu). Bộ đàm là thiết bị hoạt động ở kiểu truyền dẫn này.

Song công (Full-Duplex): trong kiểu truyền dẫn này, tại một thời điểm, thiết bị có thể vừa phát vừa thu. Điện thoại là một minh họa cho kiểu truyền dẫn này.

II. Đường cáp truyền mạng

Đường cáp truyền mạng là cơ sở hạ tầng của một hệ thống mạng, nên nó rất quan trọng và ảnh hưởng rất nhiều đến khả năng hoạt động của mạng. Hiện nay người ta thường dùng 3 loại dây cáp là cáp xoắn cặp, cáp đồng trực và cáp quang.

II.1. Cáp xoắn cặp

Đây là loại cáp gồm hai đường dây dẫn đồng được xoắn vào nhau nhằm làm giảm nhiễu điện từ gây ra bởi môi trường xung quanh và giữa chúng với nhau.

Hiện nay có hai loại cáp xoắn là cáp có bọc kim loại (STP - Shield Twisted Pair) và cáp không bọc kim loại (UTP -Unshield Twisted Pair).

Cáp có bọc kim loại (STP): Lớp bọc bên ngoài có tác dụng chống nhiễu điện từ, có loại có một đôi giây xoắn vào nhau và có loại có nhiều đôi giây xoắn với nhau.

Cáp không bọc kim loại (UTP): Tính tương tự như STP nhưng kém hơn về khả năng chống nhiễu và suy hao vì không có vỏ bọc.

STP và UTP có các loại (Category - Cat) thường dùng:

Loại 1 & 2 (Cat 1 & Cat 2): Thường dùng cho truyền thoại và những đường truyền tốc độ thấp (nhỏ hơn 4Mb/s).

Loại 3 (Cat 3): tốc độ truyền dữ liệu khoảng 16 Mb/s , nó là chuẩn cho hầu hết các mạng điện thoại.

Loại 4 (Cat 4): Thích hợp cho đường truyền 20Mb/s.

Loại 5 (Cat 5): Thích hợp cho đường truyền 100Mb/s.

Loại 6 (Cat 6): Thích hợp cho đường truyền 300Mb/s.

Đây là loại cáp rẻ, dễ cài đặt tuy nhiên nó dễ bị ảnh hưởng của môi trường.

II.2. Cáp đồng trục

Cáp đồng trục có hai đường dây dẫn và chúng có cùng một trục chung, một dây dẫn trung tâm (thường là dây đồng cứng) đường dây còn lại tạo thành đường ống bao xung quanh dây dẫn trung tâm (dây dẫn này có thể là dây bện kim loại và vì nó có chức năng chống nhiễu nên còn gọi là lớp bọc kim). Giữa hai dây dẫn trên có một lớp cách ly, và bên ngoài cùng là lớp vỏ plastic để bảo vệ cáp.

Các loại cáp	Dây xoắn cáp	Cáp đồng trục mỏng	Cáp đồng trục dày	Cáp quang
Chi tiết	Băng đồng, có 4 và 25 cặp dây (loại 3, 4, 5)	Băng đồng, 2 dây, đường kính 5mm	Băng 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	Đở	Đở	Tốt
Quản lý	Dễ dàng	Khó	Khó	Trung bình
Chi phí cho 1 trạm	Rất thấp	Thấp	Trung bình	Cao
Ứng dụng tốt nhất	Hệ thống Workgroup	Đường backbone	Đường backbone trong tủ mạng	Đường backbone dài trong tủ mạng hoặc các tòa nhà

Bảng IV-1 Tính năng kỹ thuật của một số loại cáp mạng

Cáp đồng trục có độ suy hao ít hơn so với các loại cáp đồng khác (ví dụ như cáp xoắn đôi) do ít bị ảnh hưởng của môi trường. Các mạng cục bộ sử dụng cáp đồng trục có thể có kích thước trong phạm vi vài ngàn mét, cáp đồng trục được sử dụng nhiều trong các mạng dạng đường thẳng. Hai loại cáp thường được sử dụng là cáp đồng trục mỏng và cáp đồng trục dày trong đường kính cáp đồng trục mỏng là 0,25 inch, cáp đồng trục dày là

0,5 inch. Cá hai loại cáp đều làm việc ở cùng tốc độ nhưng cáp đồng trục mỏng có độ hao suy tín hiệu lớn hơn

Hiện nay có cáp đồng trục sau:

RG -58,50 ohm: dùng cho mạng Thin Ethernet

RG -59,75 ohm: dùng cho truyền hình cáp

RG -62,93 ohm: dùng cho mạng ARCnet

Các mạng cục bộ thường sử dụng cáp đồng trục có dải thông từ 2,5 - 10 Mb/s, cáp đồng trục có độ suy hao ít hơn so với các loại cáp đồng khác vì nó có lớp vỏ bọc bên ngoài, độ dài thông thường của một đoạn cáp nối trong mạng là 200m, thường sử dụng cho dạng Bus.

II.3. Cáp sợi quang (Fiber - Optic Cable)

Cáp sợi quang bao gồm một dây dẫn trung tâm (là một hoặc một bó sợi thủy tinh có thể truyền dẫn tín hiệu quang) được bọc một lớp vỏ bọc có tác dụng phản xạ các tín hiệu trở lại để giảm sự mất mát tín hiệu. Bên ngoài cùng là lớp vỏ plastic để bảo vệ cáp. Như vậy cáp sợi quang không truyền dẫn các tín hiệu điện mà chỉ truyền các tín hiệu quang (các tín hiệu dữ liệu phải được chuyển đổi thành các tín hiệu quang và khi nhận chúng sẽ lại được chuyển đổi trở lại thành tín hiệu điện).

Cáp quang có đường kính từ 8.3 - 100 micron, Do đường kính lõi sợi thuỷ tinh có kích thước rất nhỏ nên rất khó khăn cho việc đấu nối, nó cần công nghệ đặc biệt với kỹ thuật cao đòi hỏi chi phí cao.

Dải thông của cáp quang có thể lên tới hàng Gbps và cho phép khoảng cách đi cáp khá xa do độ suy hao tín hiệu trên cáp rất thấp. Ngoài ra, vì cáp sợi quang không dùng tín hiệu điện tử để truyền dữ liệu nên nó hoàn toàn không bị ảnh hưởng của nhiễu điện từ và tín hiệu truyền không thể bị phát hiện và thu trộm bởi các thiết bị điện tử của người khác.

Chỉ trừ nhược điểm khó lắp đặt và giá thành còn cao , nhìn chung cáp quang thích hợp cho mọi mạng hiện nay và sau này.

II.4. Các yêu cầu cho một hệ thống cáp

An toàn, thẩm mỹ: Tất cả các dây mạng phải được bao bọc cẩn thận, cách xa các nguồn điện, các máy có khả năng phát sóng để tránh trường hợp bị nhiễu. Các đầu nối phải đảm bảo chất lượng, tránh tình trạng hệ thống mạng bị chập chờn.

Đúng chuẩn: Hệ thống cáp phải thực hiện đúng chuẩn, đảm bảo cho khả năng nâng cấp sau này cũng như dễ dàng cho việc kết nối các thiết bị khác nhau của các nhà sản xuất khác nhau. Tiêu chuẩn quốc tế dùng cho các hệ thống mạng hiện nay là EIA/TIA 568B.

Tiết kiệm và "linh hoạt" (flexible): Hệ thống cáp phải được thiết kế sao cho kinh tế nhất, dễ dàng trong việc di chuyển các trạm làm việc và có khả năng mở rộng sau này.

III. Đường truyền vô tuyến

Khi dùng các loại cáp ta gặp một số khó khăn như cơ sở cài đặt cố định, khoảng cách không xa, vì vậy để khắc phục những khuyết điểm trên người ta dùng đường truyền vô tuyến. Đường truyền vô tuyến mang lại những lợi ích sau:

- Cung cấp nối kết tạm thời với mạng cáp có sẵn.
- Những người liên tục di chuyển vẫn nối kết vào mạng dùng cáp.
- Lắp đặt đường truyền vô tuyến ở những nơi địa hình phức tạp không thể đi dây được.
- Phù hợp cho những nơi phục vụ nhiều kết nối cùng một lúc cho nhiều khách hàng. Ví dụ như: Dùng đường vô tuyến cho phép khách hàng ở sân bay kết vào mạng để duyệt Internet.
- Dùng cho những mạng có giới hạn rộng lớn vượt quá khả năng 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.
- Đề bị nghe lén.
- Khi có vật cản thì tín hiệu suy yếu rất nhanh.
- Băng thông không cao.

III.1. Sóng vô tuyến (radio)

Sóng radio nằm trong phạm vi từ 10 KHz đến 1 GHz, trong miền này ta có rất nhiều dải tần ví dụ như: sóng ngắn, VHF (dùng cho tivi và radio FM), UHF (dùng cho tivi). Tại mỗi quốc gia, nhà nước sẽ quản lý cấp phép sử dụng các băng tần để tránh tình trạng các sóng bị nhiễu. Nhưng có một số băng tần được chỉ định là vùng tự do có nghĩa là chúng ta dùng nhưng không cần đăng ký (vùng này thường có dải tần 2,4 Ghz). Tận dụng lợi điểm này các thiết bị Wireless của các hãng như Cisco, Compex đều dùng ở dải tần này. Tuy nhiên, chúng ta sử dụng tần số không cấp phép sẽ có nguy cơ nhiễu hơn.

III.2. Sóng viba

Truyền thông viba thường có hai dạng: truyền thông trên mặt đất và các kết nối với vệ tinh. Miền tần số của viba mặt đất khoảng 21-23 GHz, các kết nối vệ tinh khoảng 11-14 Mhz. Băng thông từ 1-10 MBps.

Sự suy yếu tín hiệu tùy thuộc vào điều kiện thời tiết, công suất và tần số phát. Chúng dễ bị nghe trộm nên thường được mã hóa.

III.3. Hỗn ngoại

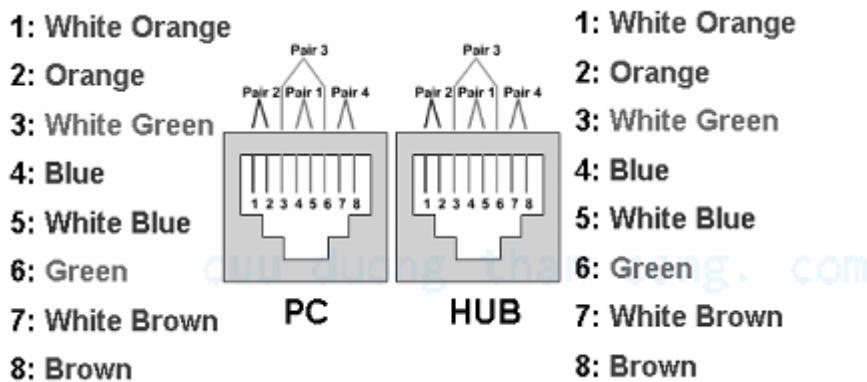
Tất cả mạng vô tuyến hỗn ngoại đều hoạt động bằng cách dùng tia hồng ngoại để truyền tải dữ liệu giữa các thiết bị. Phương pháp này có thể truyền tín hiệu ở tốc độ cao do dải thông cao của tia hồng ngoại. Thông thường mạng hồng ngoại có thể truyền với tốc độ từ 1-10 Mbps. Miền tần số từ 100 Ghz đến 1000 GHz. Có bốn loại mạng hồng ngoại:

- **Mạng đường ngắn:** mạng này chỉ truyền khi máy phát và máy thu có một đường ngắn rõ rệt giữa chúng.

- **Mạng hồng ngoại tán xạ:** kỹ thuật này phát tia truyền dội tường và sàn nhà rồi mới đến máy thu. Diện tích hiệu dụng bị giới hạn ở khoảng 100 feet (35m) và có tín hiệu chậm do hiện tượng dội tín hiệu.
- **Mạng phản xạ:** ở loại mạng hồng ngoại này, máy thu-phát quang đặt gần máy tính sẽ truyền tới một vị trí chung, tại đây tia truyền được đổi hướng đến máy tính thích hợp.
- **Broadband optical telepoint:** loại mạng cục bộ vô tuyến hồng ngoại cung cấp các dịch vụ dải rộng. Mạng vô tuyến này có khả năng xử lý các yêu cầu đa phương tiện chất lượng cao, vốn có thể trùng khớp với các yêu cầu đa phương tiện của mạng cáp.

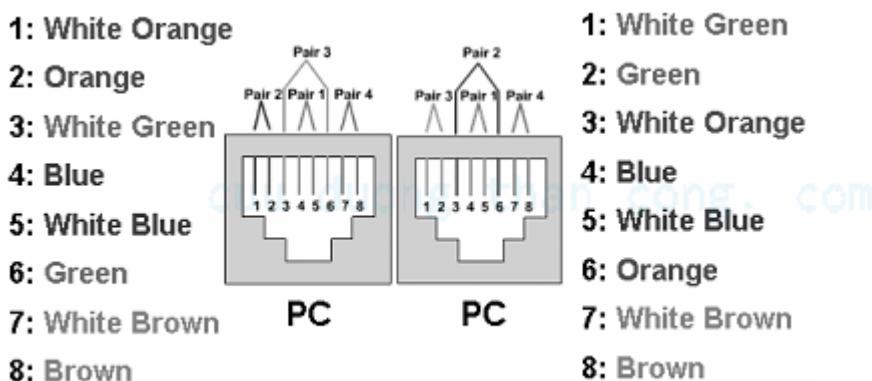
IV. Các kỹ thuật bấm cáp mạng

- **Cáp thẳng (Straight-through cable):** là cáp dùng để nối PC và các thiết bị mạng như Hub, Switch, Router... Cáp thẳng theo chuẩn 10/100 Base-T dùng hai cặp dây xoắn nhau và dùng chân 1, 2, 3, 6 trên đầu RJ45. Cặp dây xoắn thứ nhất nối vào chân 1, 2, cặp xoắn thứ hai nối vào chân 3, 6. Đầu kia của cáp dựa vào màu nối vào chân của đầu RJ45 và nối tương tự.



Hình IV-1: Cách đấu dây thẳng.

- **Cáp chéo (Crossover cable):** là cáp dùng nối trực tiếp giữa hai thiết bị giống nhau như PC – PC, Hub – Hub, Switch – Switch. Cáp chéo trật tự dây cũng giống như cáp thẳng nhưng đầu dây còn lại phải chéo cặp dây xoắn sử dụng (vị trí thứ nhất đổi với vị trí thứ 3, vị trí thứ hai đổi với vị trí thứ sáu).

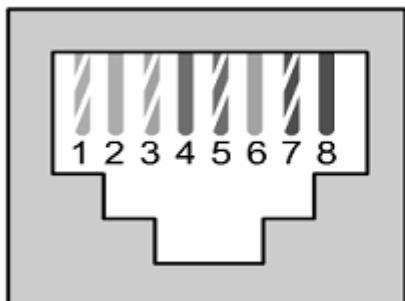


Hình IV-2: Cách đấu dây chéo.

- **Cáp Console:** Dùng để nối PC vào các thiết bị mạng chủ yếu dùng để cấu hình các thiết bị. Thông thường khoảng cách dây Console ngắn nên chúng ta không cần chọn cặp dây xoắn, mà chọn theo màu từ 1-8 sao cho dễ nhớ và đầu bên kia ngược lại từ 8-1.

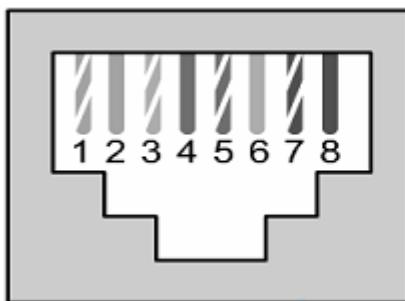
ANSI (Viện tiêu chuẩn quốc gia Hoa Kỳ), TIA (hiệp hội công nghiệp viễn thông), EIA (hiệp hội công nghiệp điện tử) đã đưa ra 2 cách xếp đặt vị trí dây như sau:

- Chuẩn T568-A (còn gọi là Chuẩn A):



1. Trắng Xanh lá cây (White Green)
2. Xanh lá cây (Green)
3. Trắng Cam (White Orange)
4. Xanh đậm (Blue)
5. Trắng Xanh đậm (White Blue)
6. Cam (Orange)
7. Trắng Nâu (White Brown)
8. Nâu (Brown)

- Chuẩn T568-B (còn gọi là Chuẩn B):



1. Trắng Cam (White Orange)
2. Cam (Orange)
3. Trắng Xanh lá cây (White Green)
4. Xanh đậm (Blue)
5. Trắng Xanh đậm (White Blue)
6. Xanh lá cây (Green)
7. Trắng Nâu (White Brown)
8. Nâu (Brown)

V. Các thiết bị liên kết mạng

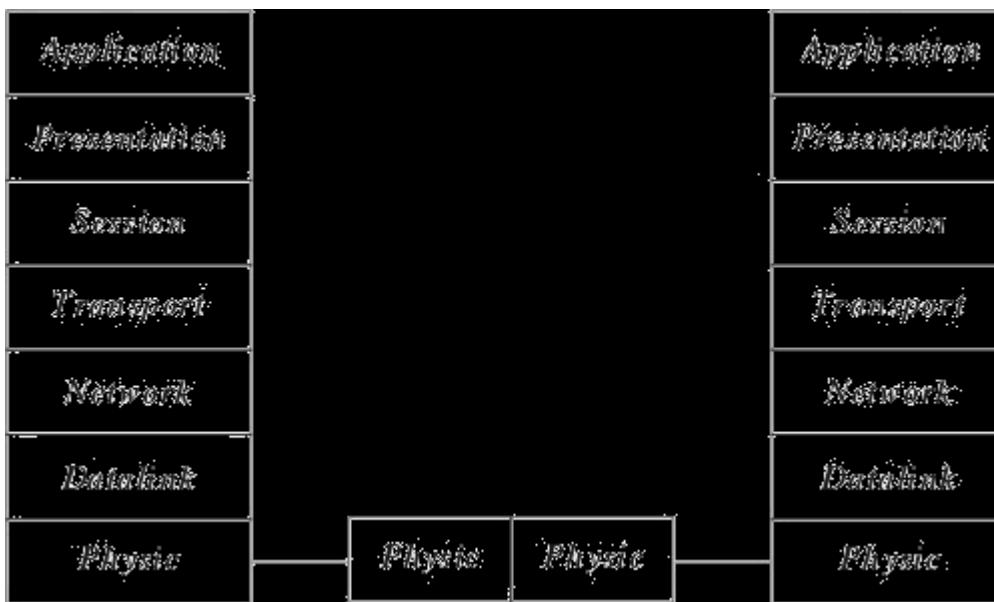
V.1. Repeater (Bộ tiếp sức)

Repeater là loại thiết bị phần cứng đơn giản nhất trong các thiết bị liên kết mạng, nó được hoạt động trong tầng vật lý của mô hình hệ thống mở OSI. Repeater dùng để nối 2 mạng giống nhau hoặc các phần một mạng cùng có một ngữ nghĩa và một cấu hình. Khi Repeater nhận được một tín hiệu từ một phía của mạng thì nó sẽ phát tiếp vào phía kia của mạng.



Hình IV-3: Mô hình liên kết mạng của Repeater.

Repeater không có xử lý tín hiệu mà nó chỉ loại bỏ các tín hiệu méo, nhiễu, khuếch đại tín hiệu đã bị suy hao (vì đã được phát với khoảng cách xa) và khôi phục lại tín hiệu ban đầu. Việc sử dụng Repeater đã làm tăng thêm chiều dài của mạng.



Hình IV-4: Hoạt động của bộ tiếp sức trong mô hình OSI

Hiện nay có hai loại Repeater đang được sử dụng là Repeater điện và Repeater điện quang.

Repeater điện nối với đường dây điện ở cả hai phía của nó, nó nhận tín hiệu điện từ một phía và phát lại về phía kia. Khi một mạng sử dụng Repeater điện để nối các phần của mạng lại thì có thể làm tăng khoảng cách của mạng, nhưng khoảng cách đó luôn bị hạn chế bởi một khoảng cách tối đa do độ trễ của tín hiệu. Ví dụ với mạng sử dụng cáp đồng trực 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.

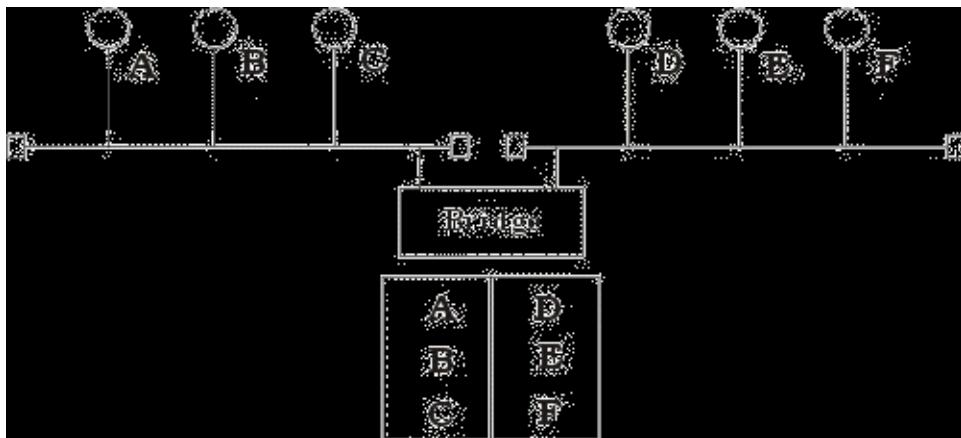
Việc sử dụng Repeater không thay đổi nội dung các tín hiệu đi qua nên nó chỉ được dùng để nối hai mạng có cùng giao thức truyền thông (như hai mạng Ethernet hay hai mạng Token ring) nhưng không thể nối hai mạng có giao thức truyền thông khác nhau (như một mạng Ethernet và một mạng Token ring). Thêm nữa 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.

V.2. Bridge (Cầu nối)

Bridge là một thiết bị có xử lý dùng để nối hai mạng giống nhau hoặc khác nhau, nó có thể được dùng với các mạng có các giao thức khác nhau. Cầu nối hoạt động trên tầng liên kết dữ liệu nên không như bộ tiếp sức phải phát lại tất cả những gì nó nhận được thì cầu nối đọc được các gói tin của tầng liên kết dữ liệu trong mô hình OSI và xử lý chúng trước khi quyết định có chuyển đi hay không.

Khi nhận được các gói tin Bridge chọn lọc và chỉ chuyển những gói tin mà nó thấy cần thiết. Điều này làm cho Bridge trở nên có ích khi nối một vài mạng với nhau và cho phép nó hoạt động một cách mềm dẻo.

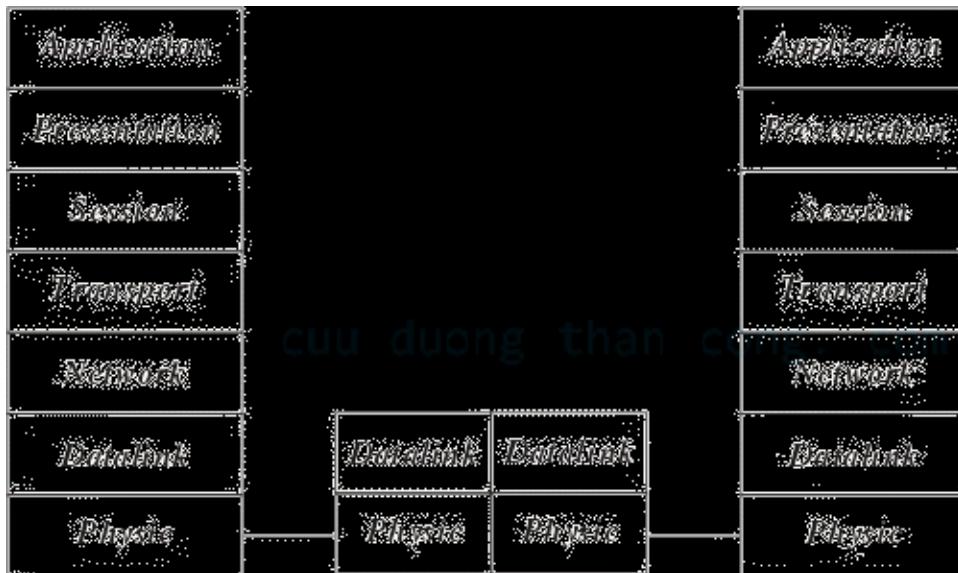
Để thực hiện được điều này trong Bridge ở mỗi đầu kết nối có một bảng các địa chỉ các trạm được kết nối vào phía đó, khi hoạt động cầu nối xem xét mỗi gói tin nó nhận được bằng cách đọc địa chỉ của nơi gửi và nhận và dựa trên bảng địa chỉ phía nhận được gói tin nó quyết định gửi gói tin hay không và bô xung bảng địa chỉ.



Hình IV-5: Hoạt động của Bridge

Khi đọc địa chỉ nơi gửi Bridge kiểm tra xem trong bảng địa chỉ của phần mạng nhận được gói tin có địa chỉ đó hay không, nếu không có thì Bridge tự động bô xung bảng địa chỉ (cơ chế đó được gọi là tự học của cầu nối).

Khi đọc địa chỉ nơi nhận Bridge kiểm tra xem trong bảng địa chỉ của phần mạng nhận được gói tin có địa chỉ đó hay không, nếu có thì Bridge sẽ cho rằng đó là gói tin nội bộ thuộc phần mạng mà gói tin đến nên không chuyển gói tin đó đi, nếu ngược lại thì Bridge mới chuyển sang phía bên kia. Ở đây chúng ta thấy một trạm không cần thiết chuyển thông tin trên toàn mạng mà chỉ trên phần mạng có trạm nhận mà thôi.



Hình IV-6: Hoạt động của Bridge trong mô hình OSI

Để đánh giá một Bridge người ta đưa ra hai khái niệm : Lọc và chuyển vận. Quá trình xử lý mỗi gói tin được gọi là quá trình lọc trong đó tốc độ lọc thể hiện trực tiếp khả năng hoạt động của

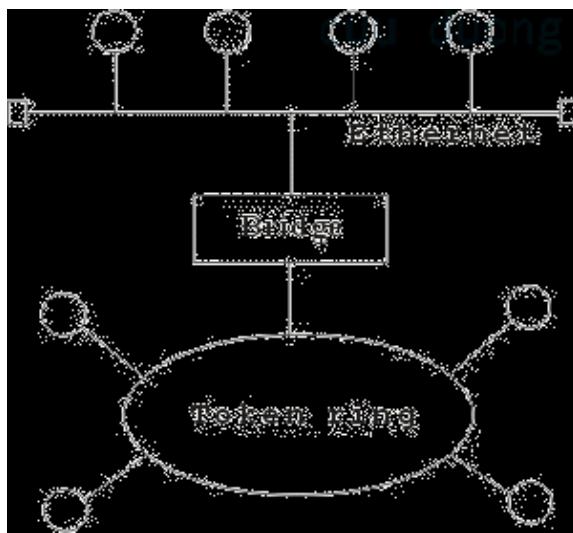
Bridge. Tốc độ chuyển vận được thể hiện số gói tin/giây trong đó thể hiện khả năng của Bridge chuyển các gói tin từ mạng này sang mạng khác.

Hiện nay có hai loại Bridge đang được sử dụng là Bridge vận chuyển và Bridge biên dịch. Bridge *vận chuyển* dùng để nối hai mạng cục bộ cùng sử dụng một giao thức truyền thông của tầng liên kết dữ liệu, tuy nhiên mỗi mạng có thể sử dụng loại dây nối khác nhau. Bridge vận chuyển không có khả năng thay đổi cấu trúc các gói tin mà nó nhận được mà chỉ quan tâm tới việc xem xét và chuyển vận gói tin đó đi.

Bridge biên dịch dùng để nối hai mạng cục bộ có giao thức khác nhau nó có khả năng chuyển một gói tin thuộc mạng này sang gói tin thuộc mạng kia trước khi chuyển qua

Ví dụ : Bridge biên dịch nối một mạng Ethernet và một mạng Token ring. Khi đó Cầu nối thực hiện như một nút token ring trên mạng Token ring và một nút Ethernet trên mạng Ethernet. Cầu nối có thể chuyển một gói tin theo chuẩn đang sử dụng trên mạng Ethernet sang chuẩn đang sử dụng trên mạng Token ring.

Tuy nhiên chú ý ở đây cầu nối không thể chia một gói tin ra làm nhiều gói tin cho nên phải hạn chế kích thước tối đa các gói tin phù hợp với cả hai mạng. Ví dụ như kích thước tối đa của gói tin trên mạng Ethernet là 1500 bytes và trên mạng Token ring là 6000 bytes do vậy nếu một trạm trên mạng token ring gửi một gói tin cho trạm trên mạng Ethernet với kích thước lớn hơn 1500 bytes thì khi qua cầu nối số lượng byte dư sẽ bị chặt bỏ.



Hình IV-7: Ví dụ về Bridge biên dịch

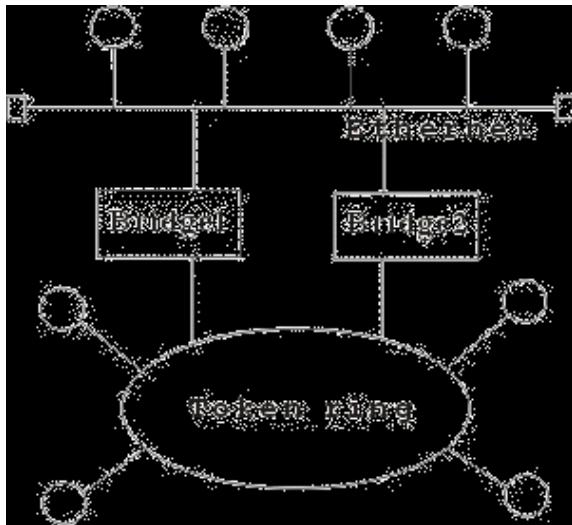
Người ta sử dụng Bridge trong các trường hợp sau :

Mở rộng mạng hiện tại khi đã đạt tới khoảng cách tối đa do Bridge sau khi xử lý gói tin đã phát lại gói tin trên phần mạng còn lại nên tín hiệu tốt hơn bội 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 từng 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 chuyên 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.



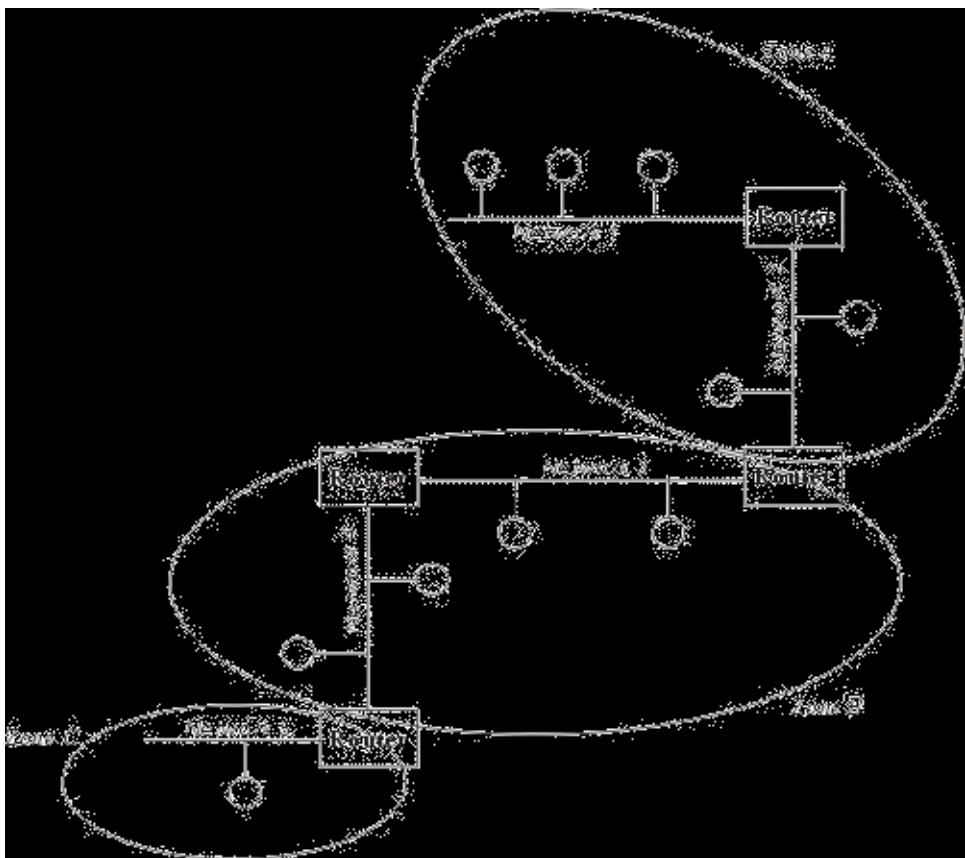
Hình IV-8: Liên kết mạng với 2 Bridge

Một số Bridge được chế tạo thành một bộ riêng biệt, chỉ cần nối dây và bật. Các Bridge khác chế tạo như card chuyên dùng cắm vào máy tính, khi đó trên máy tính sẽ sử dụng phần mềm Bridge. Việc kết hợp phần mềm với phần cứng cho phép uyển chuyển hơn trong hoạt động của Bridge.

V.3. Router (Bộ tìm đường)

Router là một thiết bị hoạt động trên tầng mạng, nó có thể tìm được đường đi tốt nhất cho các gói tin qua nhiều kết nối để đi từ trạm gửi thuộc mạng đầu đến trạm nhận thuộc mạng cuối. Router có thể được sử dụng trong việc nối nhiều mạng với nhau và cho phép các gói tin có thể đi theo nhiều đường khác nhau để tới đích.

cuu duong than cong. com



Hình IV-9: Hoạt động của Router.

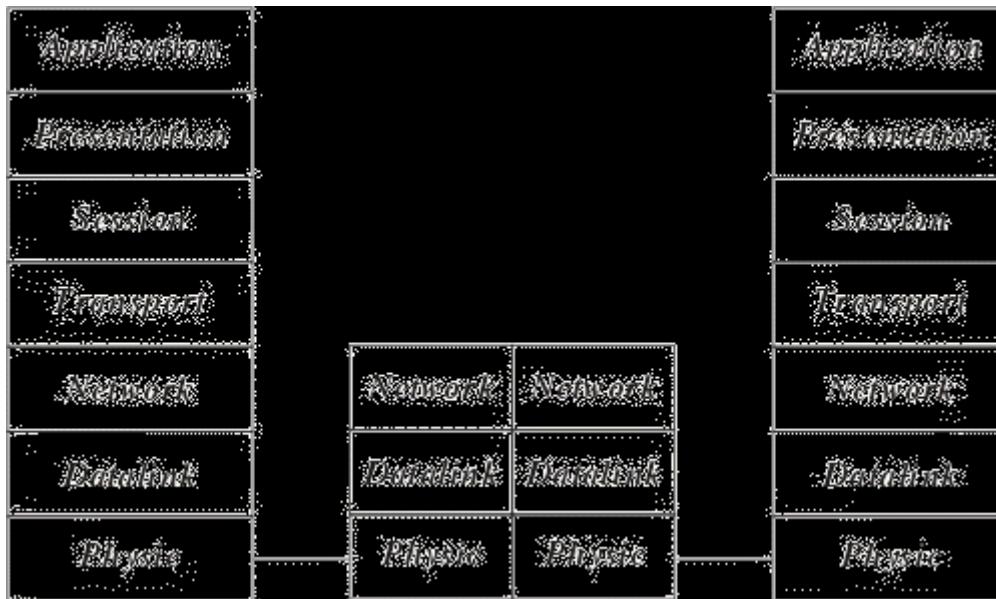
Khác với Bridge hoạt động trên tầng liên kết dữ liệu nên Bridge phải xử lý mọi gói tin trên đường truyền thì Router có địa chỉ riêng biệt và nó chỉ tiếp nhận và xử lý các gói tin gửi đến nó mà thôi. Khi một trạm muốn gửi gói tin qua Router thì nó phải gửi gói tin với địa chỉ trực tiếp của Router (Trong gói tin đó phải chứa các thông tin khác về đích đến) và khi gói tin đến Router thì Router mới xử lý và gửi tiếp.

Khi xử lý một gói tin Router phải tìm được đường đi của gói tin qua mạng. Để làm được điều đó Router phải tìm được đường đi tốt nhất trong mạng dựa trên các thông tin nó có về mạng, thông thường trên mỗi Router có một bảng chỉ đường (Router table). Dựa trên dữ liệu về Router gần đó và các mạng trong liên mạng, Router tính được bảng chỉ đường (Router table) tối ưu dựa trên một thuật toán xác định trước.

Người ta phân chia Router thành hai loại là Router có phụ thuộc giao thức (The protocol dependent routers) và Router không phụ thuộc vào giao thức (The protocol independent router) dựa vào phương thức xử lý các gói tin khi qua Router.

Router có phụ thuộc giao thức: Chỉ thực hiện việc tìm đường và truyền gói tin từ mạng này sang mạng khác chứ không chuyển đổi phương cách đóng gói của gói tin cho nên cả hai mạng phải dùng chung một giao thức truyền thông.

Router không phụ thuộc vào giao thức: có thể liên kết các mạng dùng giao thức truyền thông khác nhau và có thể chuyển đổi gói tin của giao thức này sang gói tin của giao thức kia, Router cũng chấp nhận kích thước các gói tin khác nhau (Router có thể chia nhỏ một gói tin lớn thành nhiều gói tin nhỏ trước truyền trên mạng).



Hình IV-10: Hoạt động của Router trong mô hình OSI

Để ngăn chặn việc mất mát số liệu Router còn nhận biết được đường nào có thể chuyển vận và ngừng chuyển vận khi đường bị tắc.

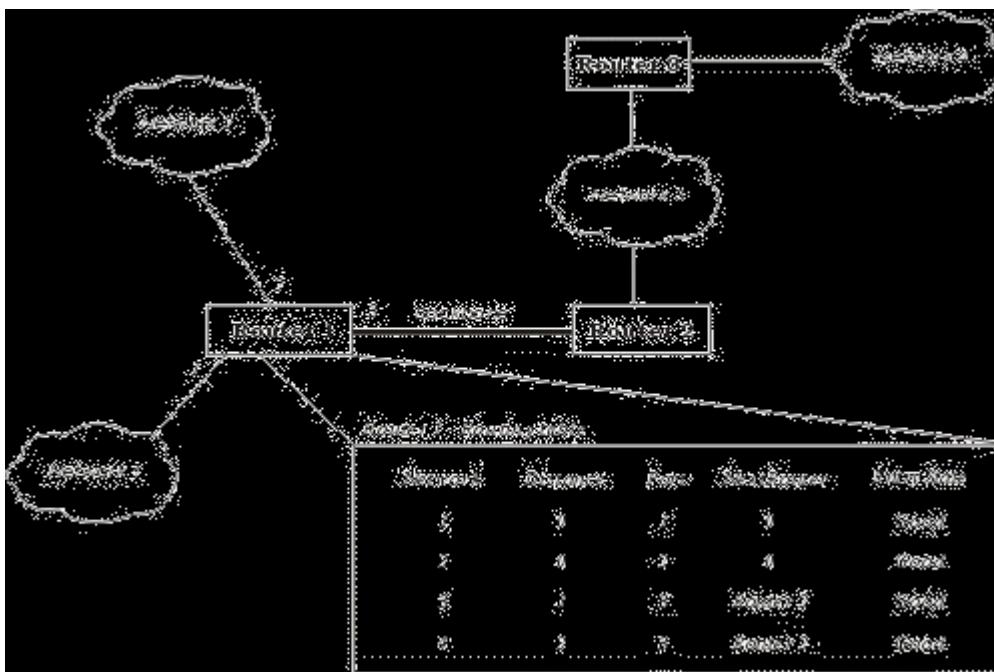
Các lý do sử dụng Router :

Router có các phần mềm lọc ưu việt hơn là Bridge do các gói tin muốn đi qua Router cần phải gửi trực tiếp đến nó nên giảm được số lượng gói tin qua nó. Router thường được sử dụng trong khi nối các mạng thông qua các đường dây thuê bao đất tiền do nó không truyền dữ liệu trên đường truyền.

Router có thể dùng trong một liên mạng có nhiều vùng, mỗi vùng có giao thức riêng biệt.

Router có thể xác định được đường đi an toàn và tốt nhất trong mạng nên độ an toàn của thông tin được đảm bảo hơn.

Trong một mạng phức hợp khi các gói tin luân chuyển các đường có thể gây nên tình trạng tắc nghẽn của mạng thì các Router có thể được cài đặt các phương thức nhằm tránh được tắc nghẽn.



Hình IV-11: Ví dụ về bảng chỉ đường (Routing table) của Router.

V.3.1 Các phương thức hoạt động của Router

Đó là phương thức mà một Router có thể nối với các Router khác để qua đó chia sẻ thông tin về mạng hiện có. 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 truyền đi thông tin về bảng chỉ đường của mình trên mạng, thông qua đó các Router khác sẽ cập nhật lên bảng chỉ đường của mình.

Phương thức trạng thái tĩnh : Router chỉ truyền các thông báo khi có phát hiện có sự thay đổi trong mạng và chỉ khi đó các Router khác cập nhật lại bảng chỉ đường, thông tin truyền đi khi đó thường là thông tin về đường truyền.

V.3.2 Một số giao thức hoạt động chính của Router

RIP (Routing Information Protocol) được phát triển bởi Xerox Network system và sử dụng SPX/IPX và TCP/IP. RIP hoạt động theo phương thức véc tơ khoảng cách.

NLSP (Netware Link Service Protocol) được phát triển bởi Novell dùng để thay thế RIP hoạt động theo phương thức véc tơ khoảng cách, mỗi Router được biết cấu trúc của mạng và việc truyền các bảng chỉ đường giảm đi..

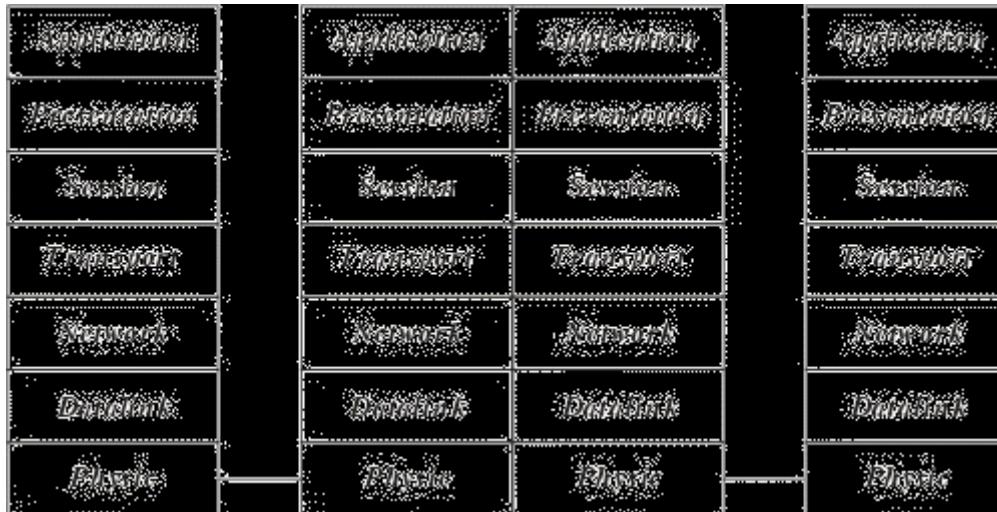
OSPF (Open Shortest Path First) là một phần của TCP/IP với phương thức trạng thái tĩnh, trong đó có xét tới ưu tiên, giá đường truyền, mật độ truyền thông...

OSPF-IS (Open System Interconnection Intermediate System to Intermediate System) là một phần của TCP/IP với phương thức trạng thái tĩnh, trong đó có xét tới ưu tiên, giá đường truyền, mật độ truyền thông...

V.4. Gateway (cổng nối)

Gateway dùng để kết nối các mạng không thuần nhất chẳng hạn như các mạng cục bộ và các mạng máy tính lớn (Mainframe), do các mạng hoàn toàn không thuần nhất nên việc chuyển đổi

thực hiện trên cả 7 tầng của hệ thống mở OSI. Thường được sử dụng nối các mạng LAN vào máy tính lớn. Gateway có các giao thức xác định trước thường là nhiều giao thức, một Gateway đa giao thức thường được chế tạo như các Card có chứa các bộ xử lý riêng và cài đặt trên các máy tính hoặc thiết bị chuyên biệt.



Hình IV-12: Hoạt động của Gateway trong mô hình OSI

Hoạt động của Gateway thông thường phức tạp hơn là Router nên thông suất của nó thường chậm hơn và thường không dùng nối mạng LAN -LAN.

V.5. Hub (Bộ tập trung)

Hub thường được dùng để nối mạng, thông qua những đầu cắm của nó người ta liên kết với các máy tính dưới dạng hình sao.

Người ta phân biệt các Hub thành 3 loại như sau sau :

Hub bị động (Passive Hub) : Hub bị động không chứa các linh kiện điện tử và cũng không xử lý các tín hiệu dữ liệu, nó có chức năng duy nhất là tổ hợp các tín hiệu từ một số đoạn cáp mạng. Khoảng cách giữa một máy tính và Hub không thể lớn hơn một nửa khoảng cách tối đa cho phép giữa 2 máy tính trên mạng (ví dụ khoảng cách tối đa cho phép giữa 2 máy tính của mạng là 200m thì khoảng cách tối đa giữa một máy tính và hub là 100m). Các mạng ARCnet thường dùng Hub bị động.

Hub chủ động (Active Hub) : Hub chủ động có các linh kiện điện tử có thể khuếch đại và xử lý các tín hiệu điện tử truyền giữa các thiết bị của mạng. Quá 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 câu nói. Nó có thể cho phép tìm đường

cho gói tin rất nhanh trên các cổng của nó, thay vì phát lại gói tin trên mọi cổng thì nó có thể chuyển mạch để phát trên một cổng có thể nối tới trạm đích.

V.6. Bộ chuyển mạch (*switch*)

Chức năng chính của *switch* là cùng một lúc duy trì nhiều cầu nối giữa các thiết bị mạng bằng cách dựa vào một loại đường xương sống (*backbone*) nội tại tốc độ cao. *Switch* có nhiều cổng, mỗi cổng có thể hỗ trợ toàn bộ *Ethernet LAN* hoặc *Token Ring*.

Bộ chuyển mạch kết nối một số LAN riêng biệt và cung cấp khả năng lọc gói dữ liệu giữa chúng.

Switch là thiết bị giống như bridge nhưng nhiều port hơn cho phép ghép nối nhiều đoạn mạng với nhau. *Switch* cũng dựa vào bảng địa chỉ MAC để quyết định gói tin nào đi ra port nào nhằm tránh tình trạng giảm băng thông khi số máy trạm trong mạng tăng lên. *Switch* cũng hoạt động tại lớp hai trong mô hình OSI. Việc xử lý gói tin dựa trên phần cứng (chip).

Khi một gói tin đi đến *Switch* (hoặc Bridge), *Switch* (hoặc Bridge) sẽ thực hiện như sau:

- Kiểm tra địa chỉ nguồn của gói tin đã có trong bảng MAC chưa, nếu chưa có thì nó sẽ thêm địa chỉ MAC này và port nguồn (nơi gói tin đi vào *Switch* (hoặc Bridge)) vào trong bảng MAC.
- Kiểm tra địa chỉ đích của gói tin đã có trong bảng MAC chưa:
 - + Nếu chưa có thì nó sẽ gửi gói tin ra tất cả các port (ngoại trừ port gói tin đi vào).
 - + Nếu địa chỉ đích đã có trong bảng MAC:
 - Nếu port đích trùng với port nguồn thì *Switch* (hoặc Bridge) sẽ loại bỏ gói tin.
 - Nếu port đích khác với port nguồn thì gói tin sẽ được gửi ra port đích tương ứng.

Chú ý:

- Địa chỉ nguồn và địa chỉ đích được nói ở trên đều là địa chỉ MAC.
- Port nguồn là Port mà gói tin đi vào.
- Port đích là Port mà gói tin đi ra.

Chương V Mô hình mạng

I. Kiến trúc mạng (Topology)

Hình trạng của mạng cục bộ thể hiện qua cấu trúc hay hình dáng hình học của các đường dây cáp mạng dùng để liên kết các máy tính thuộc mạng với nhau. Các mạng cục bộ thường hoạt động dựa trên cấu trúc đã định sẵn liên kết các máy tính và các thiết bị có liên quan.

Trước hết chúng ta xem xét hai phương thức nối mạng chủ yếu được sử dụng trong việc liên kết các máy tính là "một điểm - một điểm" và "một điểm - nhiều điểm".

Với phương thức "một điểm - một điểm" các đường truyền riêng biệt được thiết lập để nối các cặp máy tính lại với nhau. Mỗi máy tính có thể truyền và nhận trực tiếp dữ liệu hoặc có thể làm trung gian như lưu trữ những dữ liệu mà nó nhận được rồi sau đó chuyển tiếp dữ liệu đi cho một máy khác để dữ liệu đó đạt tới đích.

Theo phương thức "một điểm - nhiều điểm" tất cả các trạm phân chia chung một đường truyền vật lý. Dữ liệu được gửi đi từ một máy tính sẽ có thể được tiếp nhận bởi tất cả các máy tính còn lại, bởi vậy cần chỉ ra địa chỉ đích của dữ liệu để mỗi máy tính căn cứ vào đó kiểm tra xem dữ liệu có phải dành cho mình không nếu đúng thì nhận còn nếu không thì bỏ qua.



Hình V-1 Các phương thức liên kết mạng

Tùy theo cấu trúc của mỗi mạng chúng sẽ thuộc vào một trong hai phương thức nối mạng và mỗi phương thức nối mạng sẽ có những yêu cầu khác nhau về phần cứng và phần mềm.

II. Những cấu trúc chính của mạng cục bộ

II.1. Dạng đường thẳng (Bus)

Trong dạng đường thẳng các máy tính đều được nối vào một đường dây truyền chính (bus). Đường truyền chính này được giới hạn hai đầu bởi một loại đầu nối đặc biệt gọi là terminator (dùng để nhận biết là đầu cuối để kết thúc đường truyền tại đây). Mỗi trạm được nối vào bus qua một đầu nối chữ T (T_connector) hoặc một bộ thu phát (transceiver). Khi một trạm truyền dữ liệu, tín hiệu được truyền trên cả hai chiều của đường truyền theo từng gói một, mỗi gói đều phải mang địa chỉ trạm đích. Các trạm khi thấy dữ liệu đi qua nhận lấy, kiểm tra, nếu đúng với địa chỉ của mình thì nó nhận lấy còn nếu không phải thì bỏ qua.

Sau đây là vài thông số kỹ thuật của topology bus. Theo chuẩn IEEE 802.3 (cho mạng cục bộ) với cách đặt tên qui ước theo thông số: tốc độ truyền tín hiệu (1,10 hoặc 100 Mb/s); BASE (nếu là Baseband) hoặc BROAD (nếu là Broadband).

10BASE5: Dùng cáp đồng trực 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 trực 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 trực trặc trên hành lang chính thì khó phát hiện ra.

Hiện nay các mạng sử dụng hình dạng đường thẳng là mạng Ethernet và G-net.

II.2. Dạng vòng tròn (Ring)

Các máy tính được liên kết với nhau thành một vòng tròn theo phương thức "một điểm - một điểm", qua đó mỗi một trạm có thể nhận và truyền dữ liệu theo vòng một chiều và dữ liệu được truyền theo từng gói một. Mỗi gói dữ liệu đều có mang địa chỉ trạm đích, mỗi trạm khi nhận được một gói dữ liệu nó kiểm tra nếu đúng với địa chỉ của mình thì nó nhận lấy còn nếu không phải thì nó sẽ phát lại cho trạm kế tiếp, cứ như vậy gói dữ liệu đi được đến đích. Với dạng kết nối này có ưu điểm là không tốn nhiều dây cáp, tốc độ truyền dữ liệu cao, không gây ách tắc tuy nhiên các giao thức để truyền dữ liệu phức tạp và nếu có trực trặc trên một trạm thì cũng ảnh hưởng đến toàn mạng.

Hiện nay các mạng sử dụng hình dạng vòng tròn là mạng Token ring của IBM.

II.3. Dạng hình sao (Star)

Ở dạng hình sao, tất cả các trạm được nối vào một thiết bị trung tâm có nhiệm vụ nhận tín hiệu từ các trạm và chuyển tín hiệu đến trạm đích với phương thức kết nối là phương thức "một điểm - một điểm". Thiết bị trung tâm hoạt động giống như một tổng đài cho phép thực hiện việc nhận và truyền dữ liệu từ trạm này tới các trạm khác. Tùy theo yêu cầu truyền thông trong mạng, thiết bị trung tâm có thể là một bộ chuyển mạch (switch), một bộ chọn đường (router) hoặc đơn giản là một bộ phân kênh (Hub). Có nhiều cổng ra và mỗi cổng nối với một máy. Theo chuẩn IEEE 802.3 mô hình dạng Star thường dùng:

10BASE-T: dùng cáp UTP, tốc độ 10 Mb/s, khoảng cách từ thiết bị trung tâm tới trạm tối đa là 100m.

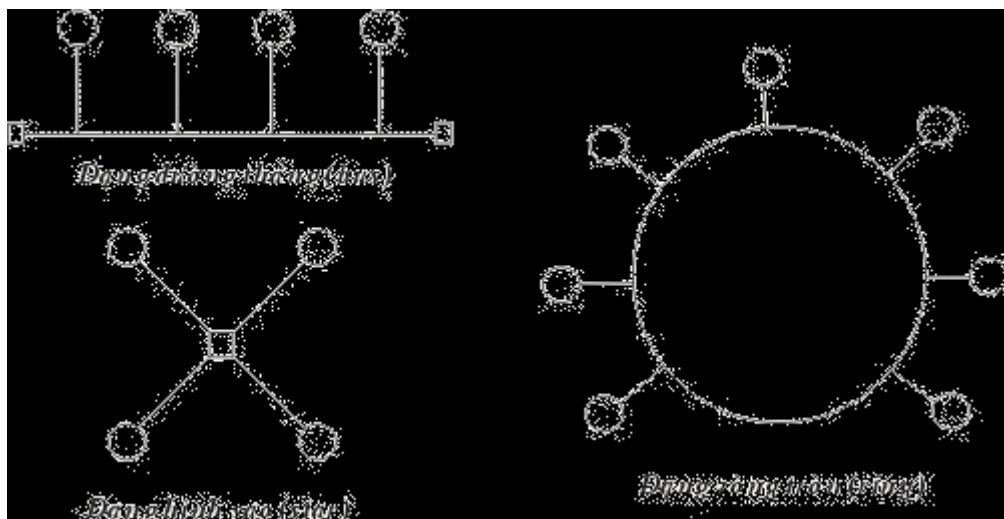
100BASE-T tương tự như 10BASE-T nhưng tốc độ cao hơn 100 Mb/s.

Ưu và khuyết điểm

Ưu điểm: Với dạng kết nối này có ưu điểm là không đụng độ hay ách tắc trên đường truyền, lắp đặt đơn giản, dễ dàng cấu hình lại (thêm, bớt trạm). Nếu có trực trặc trên một trạm thì cũng không gây ảnh hưởng đến toàn mạng qua đó dễ dàng kiểm soát và khắc phục sự cố.

Nhược điểm: Độ dài đường truyền nối một trạm với thiết bị trung tâm bị hạn chế (trong vòng 100 m với công nghệ hiện đại) tốn đường dây cáp nhiều, tốc độ truyền dữ liệu không cao.

Hiện nay các mạng sử dụng hình dạng hình sao là mạng STARLAN của AT&T và S-NET của Novell.



Hình V-2 Các loại cấu trúc chính của mạng cục bộ.

	Đường thẳng	Vòng Tròn	Hình sao
Ứng dụng	Tốt cho trường hợp mạng nhỏ và mạng có giao thông thấp và lưu lượng dữ liệu thấp	Tốt cho trường hợp mạng có số trạm ít hoạt động với tốc độ cao, không cách nhau xa lắm hoặc mạng có lưu lượng dữ liệu phân bố không đều.	Hiện nay mạng sao là cách tốt nhất cho trường hợp phải tích hợp dữ liệu và tín hiệu tiếng. Các mạng điện thoại công cộng có cấu trúc này
Độ phức tạp	Tương đối không phức tạp	Đòi hỏi thiết bị tương đối phức tạp. Một khía cạnh 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 lưu lượng 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 sỉ phẩm ở thị trường	Phải dự trù gấp đôi nguồn lực hoặc phải có 1 phương thức thay thế khi 1 nút không hoạt động nếu vẫn	Tổng phí rất cao khi làm nhiệm vụ của thiết bị trung tâm, thiết bị trung tâm i không được dùng

	Sự dư thừa kênh truyền được khuyến để giảm bớt nguy cơ xuất hiện sự cố trên mạng	muốn mạng hoạt động bình thường	vào việc khác .Số lượng dây riêng cũng nhiều.
Nguy cơ	Một trạm bị hỏng không ảnh hưởng đến cả mạng. Tuy nhiên mạng sẽ có nguy cơ bị tổn hại khi sự cố trên đường dây dẫn chính hoặc có vấn đề với tuyền. Vấn đề trên rất khó xác định được lại rất dễ sửa chữa	Một trạm bị hỏng có thể ảnh hưởng đến cả hệ thống vì các trạm phục thuộc vào nhau. Tìm 1 repeater hỏng rất khó ,và lại việc sửa chữa thằng hay dùng mưu mẹo xác định điểm hỏng trên mạng có địa bàn rõ ràng rất khó	Độ tin cậy của hệ thống phụ thuộc vào thiết bị trung tâm, nếu bị hỏng thì mạng ngưng hoạt động Sự ngưng hoạt động tại thiết bị trung tâm thường không ảnh hưởng đến toàn bộ hệ thống .
Khả năng mở rộng	Việc thêm và định hình lại mạng này rất dễ.Tuy nhiên việc kết nối giữa các máy tính và thiết bị của các hãng khác nhau khó có thể vì chúng phải có thể nhận cùng địa chỉ và dữ liệu	Tương đối dễ thêm và bớt các trạm làm việc mà không phải kết nối cho mỗi thay đổi Giả thành cho việc thay đổi tương đối thấp	Khả năng mở rộng hạn chế, đa số các thiết bị trung tâm chỉ chịu đựng nối 1 số nhất định liên kết. Sự hạn chế về tốc độ truyền dữ liệu và băng tần thường được đòi hỏi ở mỗi người sử dụng. Các hạn chế này giúp cho các chức năng xử lý trung tâm không bị quá tải bởi tốc độ thu nạp tại tại cổng truyền và giá thành mỗi cổng truyền của thiết bị trung tâm thấp .

Bảng V-1 Bảng so sánh tính năng giữa các cấu trúc của mạng LAN

II.4. Mạng dạng kết hợp

Kết hợp hình sao và tuyền (*star/Bus Topology*)

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

Lợi điểm của cấu hình này là mạng có thể gồm nhiều nhóm làm việc ở cách xa nhau, ARCLNET 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 đổi với bất cứ tòa nhà nào.

Kết hợp hình sao và vòng (*Star/Ring Topology*)

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

Chương VI Các dịch vụ của mạng điện rộng (WAN)

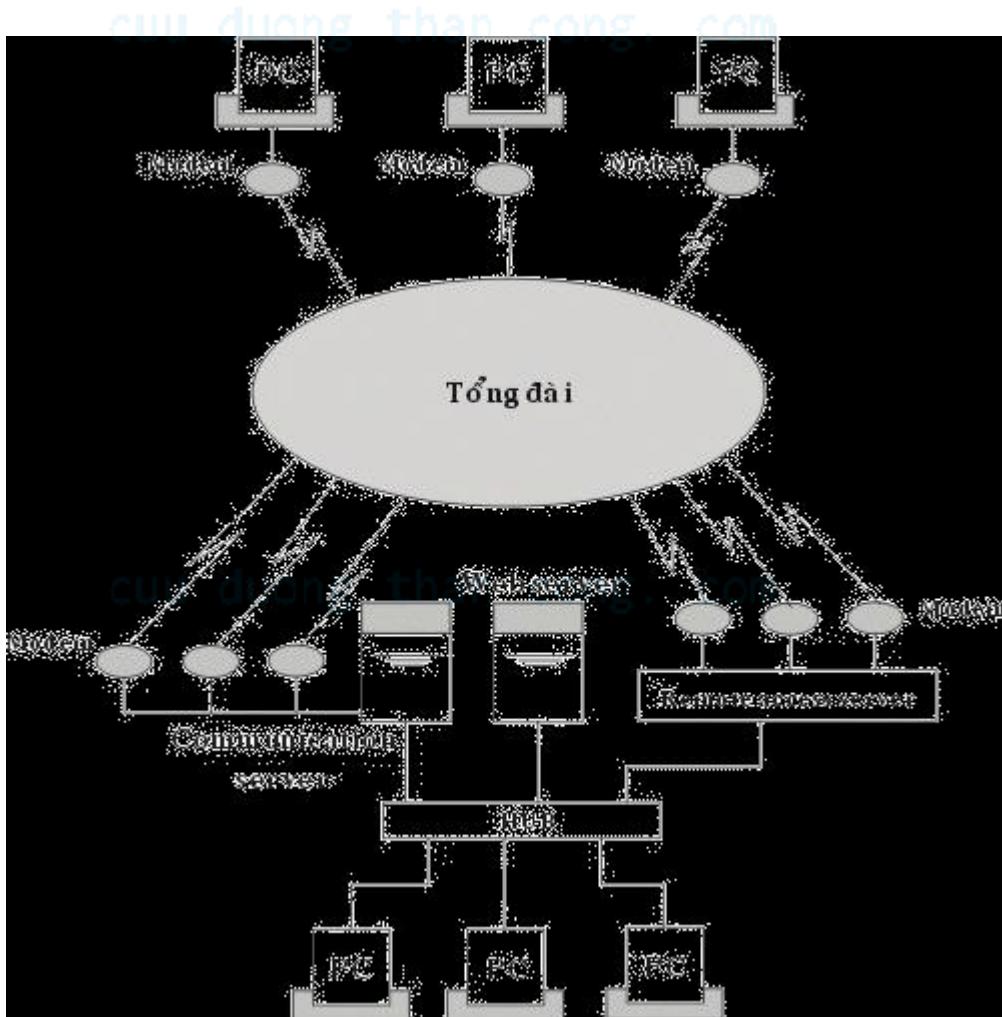
Hiện nay trên thế giới có nhiều dịch vụ dành cho việc chuyển thông tin từ khu vực này sang khu vực khác nhằm kết các mạng LAN của các khu vực khác nhau lại. Để có được những liên kết như vậy người ta thường sử dụng các dịch vụ của các mạng điện rộng. Hiện nay trong khi giao thức truyền thông cơ bản của 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 điện rộng, ở đây nếu phân loại theo phương pháp truyền thông tin thì có thể chia thành 3 loại mạng như sau:

- Mạng chuyên mạch (Circuit Switching Network)
- Mạng thuê bao (Leased lines Network)
- Mạng chuyển gói tin (Packet Switching Network)

I. Mạng chuyên mạch (Circuit Switching Network)

Để thực hiện được việc liên kết giữa hai điểm nút, một đường nối giữa điểm nút này và điểm nút kia được thiết lập trong mạng thể hiện dưới dạng cuộc gọi thông qua các thiết bị chuyên mạch.



Hình VI-1: Mô hình mạng chuyên mạch

Một ví dụ của mạng chuyên 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 chuyên mạch là chuyên mạch tương tự (analog) và chuyên mạch số (digital)

- **Chuyên mạch tương tự (Analog):** Việc chuyển dữ liệu qua mạng chuyên mạch tương tự được thực hiện qua mạng điện thoại. Các trạm sử dụng một thiết bị có tên là modem, thiết bị này sẽ chuyển các tín hiệu số từ máy tính sao tín hiệu tuần tự có trễ truyền đi trên mạng điện thoại và ngược lại.



Hình VI-2: Mô hình chuyên mạch tương tự

Khi sử dụng đường truyền điện thoại để truyền số liệu thì các chuẩn của modem và các tính chất của nó sẽ quyết định tốc độ của đường truyền. Cùng với các kỹ thuật chuyển đổi tín hiệu các tính năng mới như nén tín hiệu cho phép nâng tốc độ truyền dữ liệu lên rất cao.

Loại	Tốc độ(bps)	Loại nén	Tốc độ thực tế (bps)
Bell 212A	1200		
CCITT V22	1200		
CCITT V22 bis	2400	MNP Class 5	2400 - 3600
CCITT V32	9600	MNP Class 5, V42 bis	9600 - 19200
CCITT V32 bis	14400	MNP Class 5, V42 bis	14400 - 33600

Bảng VI-1: Bảng kỹ thuật modem

Các kỹ thuật nén thường dùng là MNP Class 5 và V42 bis, MNP Class 5 cho phép nén với tỷ lệ 1.5:1 và V42 bis nén với tỷ lệ 2:1. Tuy nhiên trên thực tế tỷ lệ nén có thể thay đổi dựa vào dạng dữ liệu được truyền.

• *Chuyển mạch số (Digital)*: Đường truyền chuyển mạch số lần đầu tiên được AT&T thiệu vào cuối 1980 khi AT&T giới thiệu mạng chuyển mạch số Acnet với đường truyền 56 kbs. Việc sử dụng đường chuyển mạch số cũng đòi hỏi sử dụng thiết bị phục vụ truyền dữ liệu số (Data Service Unit - DSU) vào vị trí modem trong chuyển mạch tương tự. Thiết bị phục vụ truyền dữ liệu số có nhiệm vụ chuyển các tín hiệu số đơn chiều (unipolar) từ máy tính ra thành tín hiệu số hai chiều (bipolar) để truyền trên đường truyền.



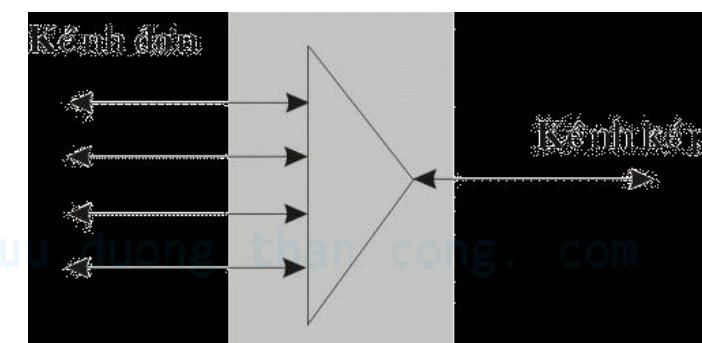
Hình VI-3: *Mô hình chuyển mạch số*

Mạng chuyển mạch số cho phép người sử dụng nâng cao tốc độ truyền (ở đây do khác biệt giữa kỹ thuật truyền số và kỹ thuật truyền tương tự nên hiệu năng của truyền mạch số cao hơn nhiều so với truyền tương tự cho dù cùng tốc độ), độ an toàn.

Vào năm 1991 AT&T giới thiệu mạng chuyển mạch số có tốc độ 384 Kbps. Người ta có thể dùng mạng chuyển mạch số để tạo các liên kết giữa các mạng LAN và làm các đường truyền dự phòng.

II. Mạng thuê bao (Leased line Network)

Với kỹ thuật chuyển mạch giữa các nút của mạng (tương tự hoặc số) có một số lượng lớn đường dây truyền dữ liệu, với mỗi đường dây trong một thời điểm chỉ có nhiều nhất một phiên giao dịch, khi số lượng các trạm sử dụng tăng cao người ta nhận thấy việc sử dụng mạng chuyển mạch trở nên không kinh tế. Để giảm bớt số lượng các đường dây kết nối giữa các nút mạng người ta đưa ra một kỹ thuật gọi là ghép kênh.



Hình VI-4: *Mô hình ghép kênh*

Mô hình đó được mô tả như sau: tại một nút người ta tập hợp các tín hiệu trên của nhiều người sử dụng ghép lại để truyền trên một kênh nối duy nhất đến các nút khác, tại nút cuối người ta phân kênh ghép ra thành các kênh riêng biệt và truyền tới các người nhận.

Có hai phương thức ghép kênh chính là ghép kênh theo tần số và ghép kênh theo thời gian, hai phương thức này tương ứng với mạng thuê bao tuần tự và mạng thuê bao kỹ thuật số. Trong thời gian hiện nay mạng thuê bao kỹ thuật số sử dụng kỹ thuật ghép kênh

theo thời gian với đường truyền T đang được sử dụng ngày một rộng rãi và dần dần thay thế mạng thuê bao tuần tự.

1. Phương thức ghép kênh theo tần số

Để sử dụng phương thức ghép kênh theo tần số giữa các nút của mạng được liên kết bởi đường truyền băng tần rộng. Băng tần này được chia thành nhiều kênh con được phân biệt bởi tần số khác nhau. Khi truyền 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 trực thành nhiều khoảng nhỏ và mỗi kênh truyền 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 với tốc độ 64 kbps và 8000 bits điều khiển trong 1 giây.

III. Mạng chuyển gói tin (Packet Switching NetWork)

Mạng chuyển mạch gói hoạt động theo nguyên tắc sau : Khi một trạm trên mạng cần gửi dữ liệu nó cần phải đóng dữ liệu thành từng gói tin, các gói tin đó được đi trên mạng từ nút này tới nút khác tới khi đến được đích. Do việc sử dụng kỹ thuật trên nên khi một trạm không gửi tin thì mọi tài nguyên của mạng sẽ dành cho các trạm khác, do vậy mạng tiết kiệm được các tài nguyên và có thể sử dụng chúng một cách tốt nhất.

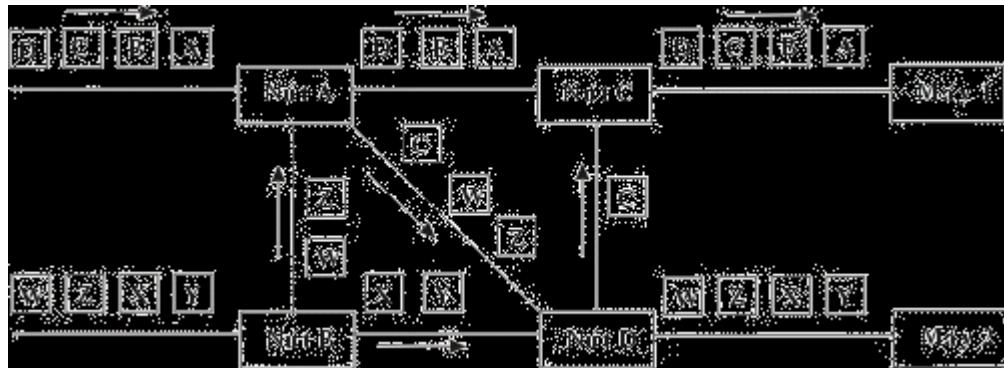
Người ta chia các phương thức chuyển mạch gói ra làm 2 phương thức:

Phương thức chuyển mạch gói theo sơ đồ rời rạc.

Phương thức chuyển mạch gói theo đường đi xác định.

1. Phương thức chuyển mạch gói theo sơ đồ rời rạc:

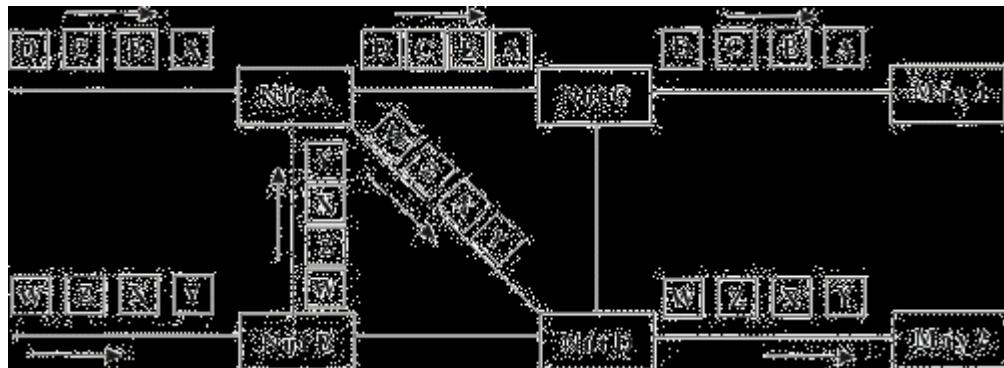
các gói tin được chuyển đi trên mạng một cách độc lập, mỗi gói tin đều có mang địa chỉ nơi gửi và nơi nhận. Mỗi nút trong mạng khi tiếp nhận gói tin sẽ quyết định xem đường đi của gói tin phụ thuộc vào thuật toán tìm đường tại nút và những thông tin về mạng mà nút đó có. Việc truyền theo phương thức này cho ta sự mềm dẻo nhất định do đường đi với mỗi gói tin trở nên mềm dẻo tuy nhiên điều này yêu cầu một số lượng tính toán rất lớn tại mỗi nút nên hiện nay phần lớn các mạng chuyển sang dùng phương chuyển mạch gói theo đường đi xác định.



Hình VI-5: Ví dụ phương thức sơ đồ rời rạc.

2. Phương thức chuyển mạch gói theo đường đi xác định:

Trước khi truyền dữ liệu một đường đi (hay còn gọi là đường đi ảo) được thiết lập giữa trạm gửi và trạm nhận thông qua các nút của mạng. Đường đi trên mạng số hiệu phân biệt với các đường đi khác, sau đó các gói tin được gửi đi theo đường đã thiết lập để tới đích, các gói tin mang số hiệu củ đường ảo để có thể được nhận biết khi qua các nút. Điều này khiến cho việc tính toán đường đi cho phiên liên lạc chỉ cần thực hiện một lần.



Hình VI-6: Ví dụ phương thức đường đi xác định

IV. Mạng X25

Được CCITT công bố lần đầu tiên vào 1970 lúc lĩnh vực viễn thông lần đầu tiên tham gia vào thế giới truyền dữ liệu với các đặc tính:

X25 cung cấp quy trình kiểm soát luồng giữa các đầu cuối đem lại chất lượng đường truyền cao cho dù chất lượng đường dây truyền không cao.

X25 được thiết kế cho cả truyền thông chuyên 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 kè nhau, dẫn đến thông lượng bị hạn chế do tổng phí xử lý mỗi gói tin tăng lên. X25 kiểm tra lỗi tại mỗi nút trước khi truyền tiếp, điều này làm cho đường truyền chó chất lượng rất cao gần như phi lỗi. Tuy nhiên do vậy khối lượng tích toán tại mỗi nút khá lớn, đối với những đường truyền của những năm 1970 thì điều đó là cần thiết nhưng hiện nay khi kỹ thuật truyền dẫn đã đạt được những tiến bộ rất cao thì việc đó trở nên lãng phí

V. Mạng Frame Relay

Mỗi gói tin trong mạng gọi là Frame, do vậy mạng gọi là Frame relay. Đặc điểm khác biệt giữa mạng Frame Relay và mạng X25 mạng Frame Relay là chỉ kiểm tra lỗi tại hai trạm gửi và trạm nhận còn trong quá trình chuyển vận qua các nút trung gian gói tin sẽ không được kiểm lỗi nữa. Do vậy thời gian xử lý trên mỗi nút nhanh hơn, tuy nhiên khi có lỗi thì gói tin phải được phát lại từ trạm đầu. Với độ an toàn cao của đường truyền hiện nay thì chi phí việc phát lại đó chỉ chiếm một tỷ lệ nhỏ nếu so với khối lượng tính toán được giảm đi tại các nút nên mạng Frame Relay tiết kiệm được tài nguyên của mạng hơn so với mạng X25.

Frame relay không chỉ là một kỹ thuật mà còn là thể hiện một phương pháp tổ chức mới. Với nguyên lý là truyền mạch gói nhưng các thao tác kiểm soát giữa các đầu cuối giảm đáng kể Kỹ thuật Frame Relay cho phép thông lượng tối đa đạt tới 2Mbps và hiện nay nó đang cung cấp các giải pháp để tương nối các mạng cục bộ LAN trong một kiến trúc xương sống tạo nên môi trường cho ứng dụng multimedia.

VI. Mạng ATM (Cell relay)

Hiện nay kỹ thuật Cell Relay dựa trên phương thức truyền thông không đồng bộ (ATM) có thể cho phép thông lượng 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 khenh 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 channel) khác nhau, mỗi kênh ảo được sử dụng bởi một ứng dụng nào đó tại một thời điểm.

ATM đã kết hợp những đặc tính tốt nhất của dạng chuyển mạch liên tục và dạng chuyển mạch gói, nó có thể kết hợp dải thông linh hoạt và khả năng chuyển tiếp cao tốc và có khả năng quản lý đồng thời dữ liệu số, tiếng nói, hình ảnh và multimedia tương tác.

Mục tiêu của kỹ thuật ATM là nhằm cung cấp một mạng dồn khenh, và chuyển mạch tốc độ cao, độ trễ nhỏ đáp ứng cho các dạng truyền thông đa phương tiện (multimedcia)

Chuyển mạch cell cần thiết cho việc cung cấp các kết nối đòi hỏi băng thông cao, tình trạng tắt nghẽn thấp, hỗ 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, băng 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 (asynchronous) các gói 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 khỗng 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 router, Cabletron, ATM module for MMAC hub.

Nhìn chung thị trường ATM sôi động do nhu cầu thực sự của các ứng dụng đa phương tiện. Sự nhập cuộc ngày một đông của các hãng sản xuất đã làm giảm đáng kể giá bán của các sản phẩm loại này, từ đó càng mở rộng thêm thị trường. Ngay ở Việt Nam, các dự án lớn về mạng tin học đều đã được thiết kế với hạ tầng chấp nhận được với công nghệ ATM trong tương lai.

Chương VII CÁC DỊCH VỤ MẠNG THÔNG DỤNG

I. DỊCH VỤ WEB

I.1. Một số thuật ngữ cơ bản.

- **HTTP (Hypertext Transfer Protocol)**: là giao thức cho phép các máy tính giao tiếp qua Web và kết nối với nhau qua các siêu liên kết hyperlink.
- **HTML (Hypertext Markup Language)**: là ngôn ngữ định dạng dùng để tạo ra các trang Web giúp người dùng có thể đọc và truy cập từ bất kỳ máy nào trên mạng, dùng bất kỳ hệ điều hành nào.
- **WebPage**: là một trang tư liệu Web.
- **WebSite**: là tập hợp các trang Web của một tổ chức, một công ty, một web site có thể có nhiều Web Server.
- **Home page**: là trang Web đầu tin của một Web Site hoặc trang Web xuất hiện đầu tin khi khởi động Web Browser, đồng thời trang này chứa các liên kết tiêu biểu đến các trang Web còn lại.
- **HyperLink (link)**: là các mối liên kết giữa các tư liệu. Thông thường, trong một trang Web, các mối liên kết có màu xanh dương và được gạch dưới. Ngoài ra, bất kỳ một hình ảnh, văn bản nào khi di chuyển con trỏ chuột tới chuyên sang hình đều là các liên kết (link).
- **URL (Uniform Resource Locator)**: là đường dẫn chỉ tới một tập tin trong một máy chủ trên Internet. Chuỗi URL thường bao gồm: tên giao thức, tên máy chủ và đường dẫn đến tập tin trong máy chủ đó.

Ví dụ: <http://www.mait.vn/index.htm> có nghĩa là: giao thức sử dụng http:// (Hypertext Transfer Protocol), tên máy chủ: www.mait.vn, đường dẫn và tên tập tin: index.htm. Lưu ý: đường dẫn sử dụng dấu "/" thay cho dấu "\".

- **IXP (Internet Exchange Provider)**: là nhà cung cấp đường truyền và cổng truy cập Internet.
- **ISP (Internet Service Provider)**: là nhà cung cấp dịch vụ Internet cho người dùng trực tiếp qua mạng điện thoại như là cấp quyền truy cập Internet, cung cấp các dịch vụ như Web, E-mail, Chat, Telnet...
- **ICP (Internet Content Provider)**: là nhà cung cấp thông tin lên Internet, thông tin được cập nhật định kỳ hay thường xuyên và thuộc nhiều lĩnh vực như thể thao, kinh tế giáo dục, chính trị, quân sự ...

Các hoạt động chính trên Web.

- Duyệt Web tìm kiếm thông tin như số điện thoại, địa chỉ nhà, tin tức, tin dự báo thời tiết, bảng giá chứng khoán, các phần mềm miễn phí...
- Giải trí như nghe nhạc, xem phim, chơi game trên mạng.
- Trao đổi E-mail.
- Truy xuất và download các tập tin.
- Trao đổi thông tin (forum).
- Sắp xếp các chuyến đi du lịch như đặt vé máy bay, đăng ký phòng khách sạn...
- Giao dịch mua bán hàng qua mạng.

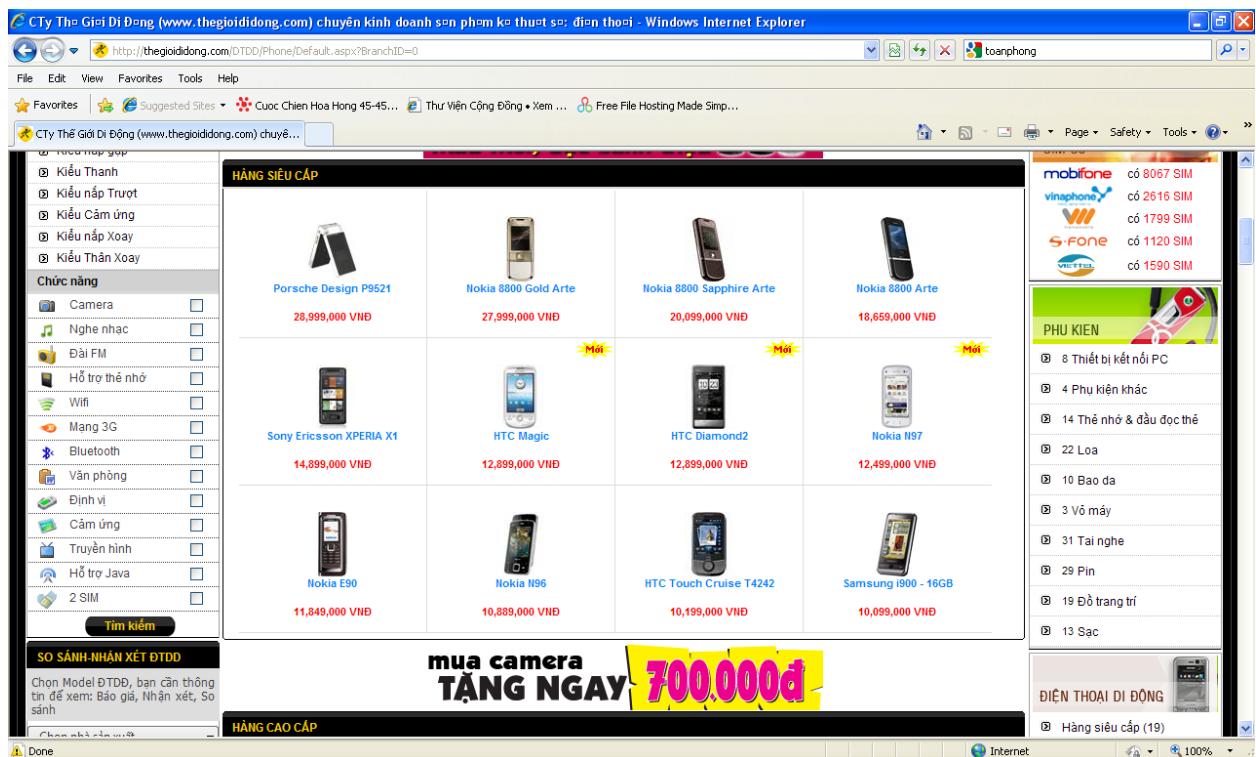


Hình VII-1 Minh họa truy cập trang Web để tìm kiếm thông tin.



Hình VII-2 : Minh họa một trang Web dùng để đào tạo trực tuyến.

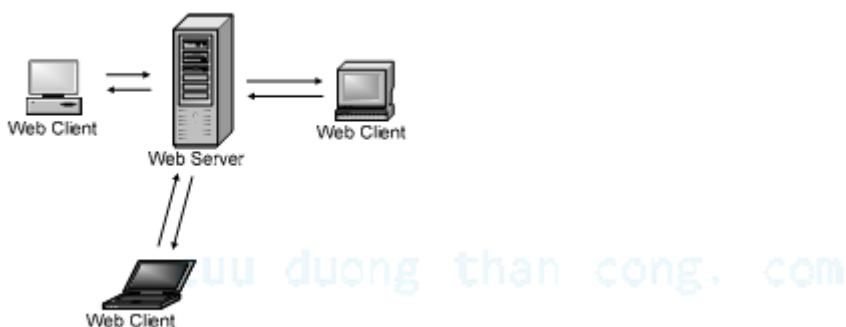
- Hội thảo từ xa.
- Quảng cáo sản phẩm.



Hình VII-3 Minh họa Website giới thiệu sản phẩm

I.2. Giới thiệu mô hình hoạt động của Web.

Dịch vụ World Wide Web (viết tắt là www hoặc Web) là một dịch vụ cung cấp thông tin trên hệ thống mạng. Các thông tin này được lưu trữ dưới dạng siêu văn bản (hypertext) và thường được thiết kế bằng ngôn ngữ HTML (Hypertext Markup Language). Siêu văn bản là các tư liệu có thể là văn bản (text), hình ảnh tĩnh (image), hình ảnh động (video), âm thanh (audio)...., được liên kết với nhau qua các mối liên kết (link) và được truyền trên mạng dựa trên giao thức HTTP (Hypertext Transfer Protocol), qua đó người dùng có thể xem các tư liệu có liên quan một cách dễ dàng. Mô hình hoạt động:



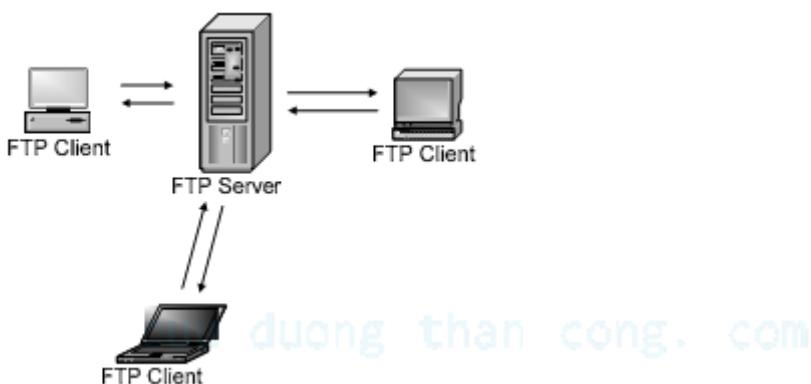
Web server: là một ứng dụng được cài đặt trên máy chủ trên mạng với chức năng là tiếp nhận các yêu cầu dạng HTTP từ máy trạm và tùy theo yêu cầu này máy chủ sẽ cung cấp cho máy trạm các thông tin web dạng HTML.

Web Client: là một ứng dụng cài trên máy trạm (máy của người dùng đầu cuối) gọi là Web Browser để gửi yêu cầu đến Web Server và nhận các thông tin phản hồi rồi hiện lên màn hình giúp người dùng có thể truy xuất được các thông tin trên máy Server. Một trong những trình duyệt Web (Web Browser) phổ biến nhất hiện nay là Internet Explorer.

II. DỊCH VỤ FTP

II.1. Mô hình hoạt động của FTP

FTP (File Transfer Protocol) là một dịch vụ cho phép ta truyền tải file giữa hai máy tính ở xa dùng giao thức TCP/IP. FTP cũng là một ứng dụng theo mô hình client-server, nghĩa là máy làm FTP Server sẽ quản lý các kết nối và cung cấp dịch vụ tập tin cho các máy trạm. Nói tóm lại FTP Server thường là một máy tính phục vụ cho việc quảng bá các tập tin cho người dùng hoặc là một nơi cho phép người dùng chia sẻ tập tin với những người dùng khác trên Internet. Máy trạm muốn kết nối vào FTP Server thì phải được Server cấp cho một account có đầy đủ các thông tin như: địa chỉ máy Server (tên hoặc địa chỉ IP), username và password. Phần lớn các FTP Server cho phép các máy trạm kết nối vào mình thông qua account anonymous (account anonymous thường được truy cập với password rỗng). Các máy trạm có thể sử dụng các lệnh ftp đã tích hợp sẵn trong hệ điều hành hoặc phần mềm chuyên dụng khác để tương tác với máy FTP Server.



Hình VII-4: Mô hình hoạt động của FTP Server.

II.2. Tập hợp các lệnh FTP

Lệnh	Chức năng
!	Chạy chương trình command dos trên máy tính cục bộ
?	Hiển thị giúp đỡ của các lệnh Ftp, lệnh này giống với lệnh Help.
Append	Chèn nội dung của một tập tin trên máy tính cục bộ vào cuối của một tập tin trên máy tính ở xa (máy FTP Server), dùng định dạng tập tin hiện tại.
Ascii	Đặt loại định dạng truyền file là ASCII, giá trị này là mặc định khi khởi tạo kết nối FTP.
Bell	Bật trạng thái chuông là on/off. Nếu là on thì sau mỗi lần lệnh truyền file hoàn thành thì máy phát ra tiếng chuông. Mặc định trạng thái này là off.
Binary	Đặt loại định dạng truyền file là binary.
Bye	Tắt kết nối với máy tính ở xa và thoát khỏi chương trình FTP.
Cd	Thay đổi thư mục hiện hành trên máy ở xa(Server).
Close	Ngừng phiên giao dịch với máy tính ở xa và trở về dòng lệnh

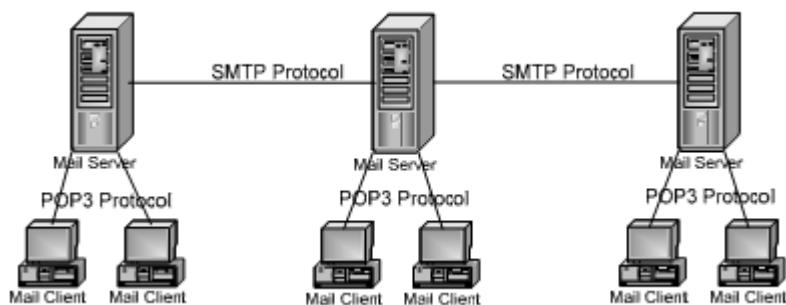
	của chương trình ftp.
Debug	Bật trạng thái Debugg on/off. Nếu là on thì mỗi lệnh gửi đến máy tính ở xa thì chương trình sẽ in ra các thông báo. Mặc định là trạng thái là off.
Delete	Xóa tập tin trên máy tính ở xa.
Dir	Hiển thị danh sách các tập tin và thư mục con trong thư mục hiện tại.
Disconnect	Tắt kết nối với máy tính ở xa và trả về dòng lệnh FTP.
Get	Chép một tập tin từ máy tính ở xa về máy tính cục bộ, dùng định dạng truyền file hiện tại.
Help	Hiển thị giúp đỡ của các lệnh Ftp.
Lcd	Thay đổi thư mục hiện trên máy tính cục bộ. Mặc định là thư mục đang làm việc trên máy tính cục bộ.
Ls	Hiển thị danh sách các tập tin và thư mục con trong thư mục hiện tại.
Mdelete	Xóa nhiều tập tin cùng trên một máy tính ở xa.
Mget	Chép nhiều tập tin từ máy tính ở xa về máy tính cục bộ dùng định dạng truyền file hiện tại.
mkdir	Tạo thư mục trên máy tính ở xa.
Mput	Chép nhiều tập tin ở máy tính cục bộ lên máy tính ở xa dùng định dạng truyền file hiện tại.
open	Mở một kết nối đến máy FTP Server.
Put	Chép một tập tin ở máy tính cục bộ lên máy tính ở xa dùng định dạng truyền file hiện tại.
Pwd	Hiển thị thư mục hiện hành trên máy tính ở xa.
Quit	Tắt kết nối với máy tính ở xa và thoát khỏi chương trình FTP.
Recv	Chép một tập tin từ máy tính ở xa về máy tính cục bộ, dùng định dạng truyền file hiện tại. Tương tự như lệnh
Rename	Đổi tên tập tin, thư mục trên máy tính ở xa.
Rmdir	Xóa một thư mục ở xa.
Send	Chép một tập tin ở máy tính cục bộ lên máy tính ở xa dùng định dạng truyền file hiện tại. Tương tự như Put.
Status	Hiển thị các trạng thái lựa chọn của kết nối FTP.

III. E-MAIL.

III.1. Mô hình hoạt động

E-mail (electronic mail) là thư điện tử, là một hình thức trao đổi thư từ nhưng thông qua mạng Internet. Dịch vụ này được sử dụng rất phổ biến và không đòi hỏi hai máy tính gửi và nhận thư phải kết nối online trên mạng..

Tại mỗi Mail Server thông thường gồm hai dịch vụ: POP3 (Post Office Protocol 3) làm nhiệm vụ giao tiếp mail giữa Mail Client và Mail Server, SMTP (Simple E-mail Transfer Protocol) làm nhiệm vụ giao tiếp mail giữa các máy Mail Server.



Hình VII-5 : Mô hình hoạt động của Mail Server.

Để sử dụng E-mail, người dùng cần có một account mail do nhà cung cấp dịch vụ Internet (ISP) cấp bao gồm các thông tin sau: địa chỉ mail (ví dụ: nvteo@hcm.vnn.vn), username, password và địa chỉ của Mail Server mà mình đăng ký. Sau đó chọn một chương trình Mail Client (Outlook Express, Eudora, Netscape...) và cấu hình các thông số trên vào chương trình đó. Từ đó bạn có thể sử dụng chương trình này để soạn thảo và gửi nhận mail một cách dễ dàng.

III.2. Các loại mail.

Thông thường có hai loại mail thông dụng là WebMail và POP Mail. Webmail là loại mail mà hình thức giao dịch mail giữa Client và Server dựa trên giao thức Web (http), thông thường Webmail là miễn phí. Còn POP Mail là loại mail mà các Mail Client tương tác với MAIL SERVER bằng giao thức POP3. Mail loại này tiện lợi và an toàn hơn nên thông thường là phải đăng ký thuê bao với nhà cung cấp dịch vụ.

III.3. Sử dụng WebMail.

Bạn muốn có một địa chỉ mail Internet để giao dịch với bạn bè trên thế giới, bạn có thể đến nhà cung cấp dịch vụ Internet để đăng ký hoặc tự tạo cho mình một địa chỉ mail miễn phí trên các Website nổi tiếng như Yahoo, Hotmail, Fpt, Vnn...

GIÁO TRÌNH

MẠNG MÁY TÍNH

cuu duong than cong. com

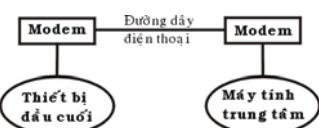
Hà nội 11-2000

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 đọc 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 đọc 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 thông 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

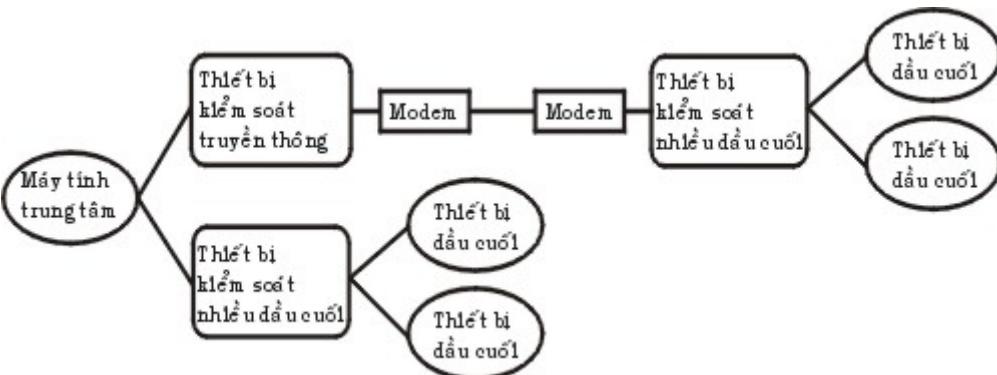
Những dạng đầu tiên của thiết bị đầu cuối bao gồm máy đọc bìa, máy in, thiết bị xử lý tín hiệu, các thiết bị cảm nhận. Việc liên kết từ xa đó có thể thực hiện thông qua những vùng khác nhau và đó là những dạng đầu tiên của hệ thống mạng.

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 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 trung.

• **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 dịch 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 cách 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.

Ấn gày nay với một lượng lớn về thông tin, nhu cầu xử lý thông tin ngày càng cao. Mạng máy tính hiện nay trở nên quá quen thuộc đối với chúng ta, trong mọi lĩnh vực như khoa học, quân sự, quốc phòng, thương mại, dịch vụ, giáo dục... Hiện nay ở nhiều nơi mạng đã trở thành một nhu cầu không thể thiếu được. Ấn gười ta thấy được việc kết nối các máy tính thành mạng cho chúng ta những khả năng mới to lớn như:

• **Sử dụng chung tài nguyên:** Ấn hững tài nguyên của mạng (như thiết bị, chương trình, dữ liệu) khi được trở thành các tài nguyên chung thì mọi thành viên của mạng đều có thể tiếp cận được mà không quan tâm tới những tài nguyên đó ở đâu.

• **Tăng độ tin cậy của hệ thống:** Ấn gười ta có thể dễ dàng bảo trì máy móc và lưu trữ (backup) các dữ liệu chung và khi có trực trặc trong hệ thống thì chúng có thể được khôi phục nhanh chóng. Trong trường hợp có trực 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 sử 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. Ấn hưng 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. Ấn hưng công nghệ cao nhất chưa chắc là công nghệ tốt nhất, mà công nghệ tốt nhất là công nghệ phù hợp nhất.

Chương 2

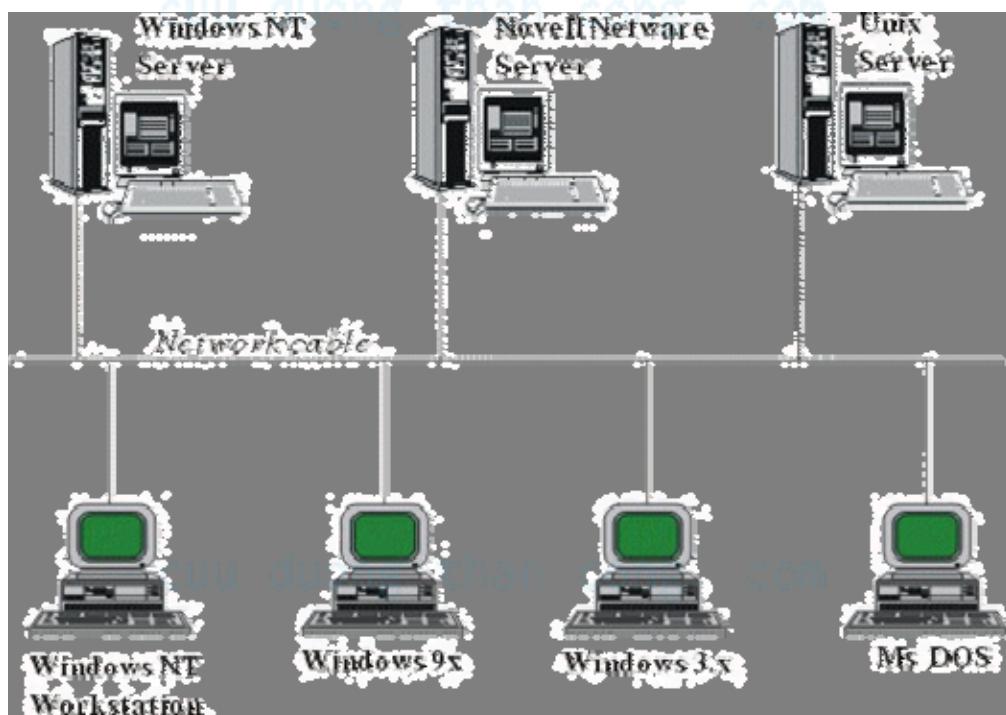
Những khái niệm cơ bản của mạng máy tính

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 trực, 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. Ở gười ta có thể chia các mạng máy tính theo khoảng cách địa lý ra làm hai loại: Mạng diện rộng và Mạng cục bộ.

• **Mạng cục bộ (Local Area Networks - LAN)** là mạng được thiết lập để liên kết các máy tính trong một khu vực như trong một tòa 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). Ở 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. Ở 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 điện 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 điện 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 điện 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 điện 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 điện 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 điện 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 điện 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

www.viet-ebook.co.cc

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.

cuu duong than cong. com

cuu duong than cong. com

Chương 3

Mô hình truyền thông

I. Sự cần thiết phải có mô hình truyền thông

Để một mạng máy tính trở thành môi trường truyền dữ liệu thì nó cần phải có những yếu tố sau:

- Mỗi máy tính cần phải có một địa chỉ phân biệt trên mạng.
- Việc chuyển dữ liệu từ máy tính này đến máy tính khác do mạng thực hiện thông qua những quy định thống nhất gọi là giao thức của mạng.

Khi các máy tính trao đổi dữ liệu với nhau thì một quá trình truyền giao dữ liệu đã được thực hiện hoàn chỉnh. Ví dụ như để thực hiện việc truyền một file giữa một máy tính với một máy tính khác cùng được gắn trên một mạng các công việc sau đây phải được thực hiện:

- Máy tính cần truyền cần biết địa chỉ của máy nhận.
- Máy tính cần truyền phải xác định được máy tính nhận đã sẵn sàng nhận thông tin
- Chương trình gửi file trên máy truyền cần xác định được rằng chương trình nhận file trên máy nhận đã sẵn sàng tiếp nhận file.
- Nếu cấu trúc file trên hai máy không giống nhau thì một máy phải làm nhiệm vụ chuyển đổi file từ dạng này sang dạng kia.
- Khi truyền file máy tính truyền cần thông báo cho mạng biết địa chỉ của máy nhận để các thông tin được mạng đưa tới đích.

Điều trên đó cho thấy giữa hai máy tính đã có một sự phối hợp hoạt động ở mức độ cao. Bây giờ thay vì chúng ta xét cả quá trình trên như là một quá trình chung thì chúng ta sẽ chia quá trình ra thành một số công đoạn và mỗi công đoạn con hoạt động một cách độc lập với nhau. Ở đây chương trình truyền nhận file của mỗi máy tính được chia thành ba module là: Module truyền và nhận File, Module truyền thông và Module tiếp cận mạng. Hai module tương ứng sẽ thực hiện việc trao đổi với nhau trong đó:

- *Module truyền và nhận file* cần được thực hiện tất cả các nhiệm vụ trong các ứng dụng truyền nhận file. Ví dụ: truyền nhận thông số về file, truyền nhận các mẫu tin của file, thực hiện chuyển đổi file sang các dạng khác nhau nếu cần. Module truyền và nhận file không cần thiết phải trực tiếp quan tâm tới việc truyền dữ liệu trên mạng như thế nào mà nhiệm vụ đó được giao cho Module truyền thông.
- *Module truyền thông* quan tâm tới việc các máy tính đang hoạt động và sẵn sàng trao đổi thông tin với nhau. Nó còn kiểm soát các dữ liệu sao cho những dữ liệu

này có thể trao đổi một cách chính xác và an toàn giữa hai máy tính. Điều đó có nghĩa là phải truyền file trên nguyên tắc đảm bảo an toàn cho dữ liệu, tuy nhiên ở đây có thể có một vài mức độ an toàn khác nhau được dành cho từng ứng dụng. Ở đây việc trao đổi dữ liệu giữa hai máy tính không phụ thuộc vào bản chất của mạng đang liên kết chúng. Ảnh hưởng 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.

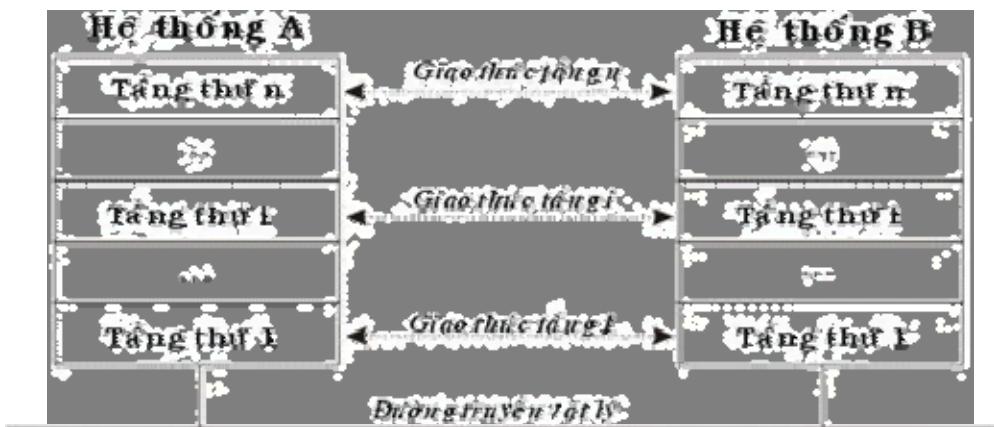
- *Module tiếp cận mạng* được xây dựng liên quan đến các quy cách giao tiếp với mạng và phụ thuộc vào bản chất của mạng. Ảnh hưởng yêu cầu liên quan đến mạng đã được thực hiện ở module thứ ba là module tiếp cận mạng và nếu mạng thay đổi thì chỉ có module tiếp cận mạng bị ảnh hưởng.

Ảnh hưởng này 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).

Ảnh hưởng 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 tự 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

Ảnh 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, U& IX) thường được thực hiện đồng thời nhiều ứng dụng trong đó có những ứng dụng liên quan đến mạng và các ứng dụng khác. Các máy tính được nối với mạng và các dữ liệu được trao đổi thông qua mạng từ máy tính này đến máy tính khác.

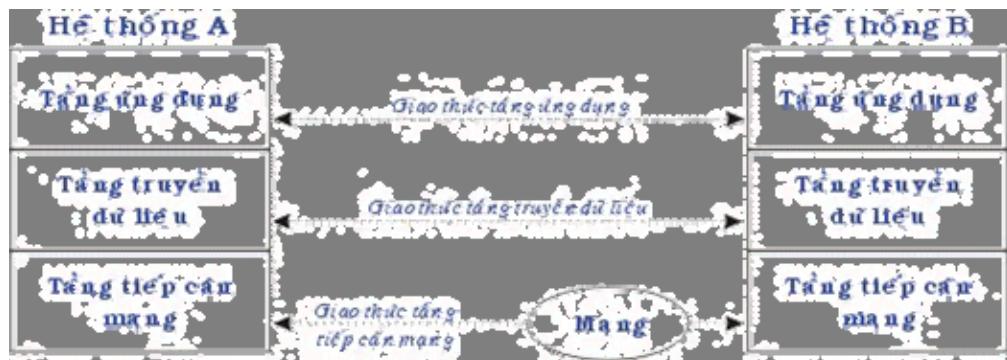
Việc gửi dữ liệu được thực hiện giữa một ứng dụng với một ứng dụng khác trên hai máy tính khác nhau thông qua mạng được thực hiện như sau: Ứng dụng gửi chuyển dữ liệu cho chương trình truyền thông trên máy tính của nó, chương trình truyền thông sẽ gửi chúng tới máy tính nhận. Chương trình truyền thông trên máy nhận sẽ tiếp nhận dữ liệu, kiểm tra nó trước khi chuyển giao cho ứng dụng đang chờ dữ liệu.

Với mô hình truyền thông đơn giản người ta chia chương trình truyền thông thành ba tầng không phụ thuộc vào nhau là: tầng ứng dụng, tầng chuyên 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 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.

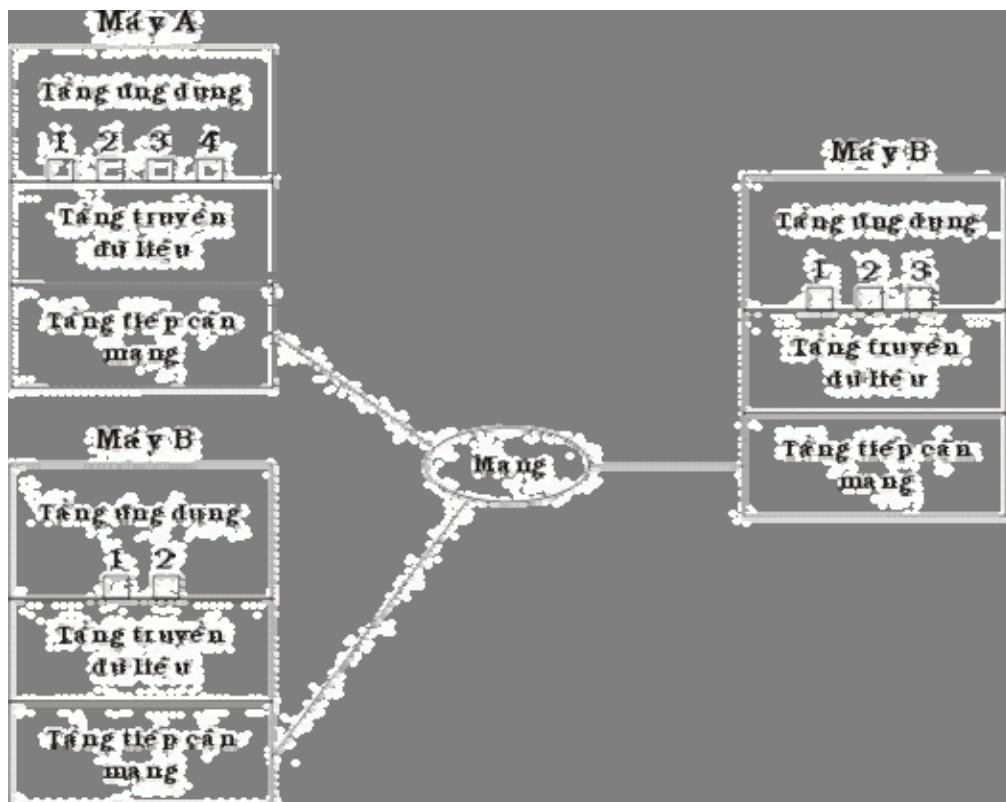


Hình 3.2 Mô hình truyền thông 3 tầng

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 đó. Ở đó 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

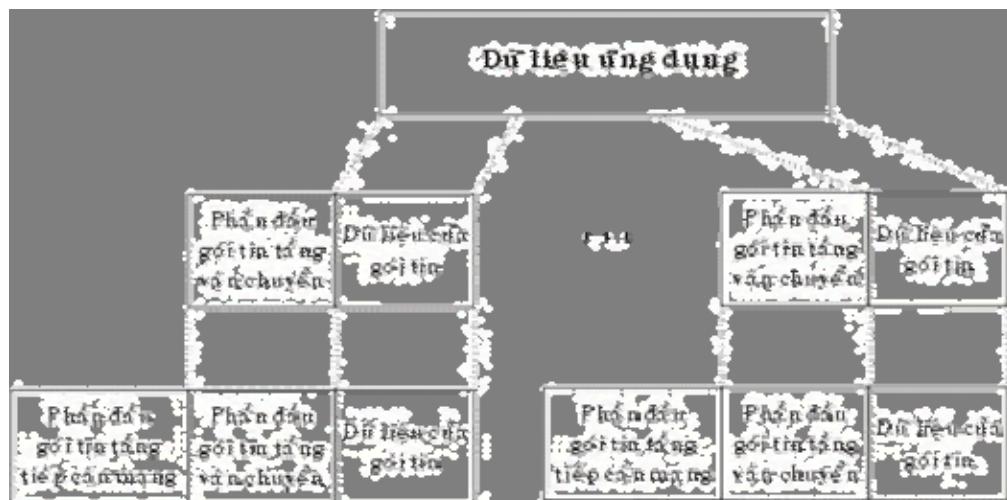
Chúng ta hãy xét trong ví dụ (như hình vẽ trên): giả sử có ứng dụng có điểm tiếp cận giao dịch 1 trên máy tính A muốn gửi thông tin cho một ứng dụng khác trên máy tính B có điểm tiếp cận giao dịch 2. Ứng dụng trên máy tính A chuyển các thông tin xuống tầng truyền dữ liệu của A với yêu cầu gửi chúng cho 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 khôi đó cho tầng vận chuyển. Tầng vận chuyển có thể chia khôi đó ra thành nhiều khôi 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 khôi 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

sẵn 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.

Ấn hứa về 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 lĩnh vực truyền thông là mô hình hệ thống mở (Open Systems Interconnection - gọi tắt là OSI).

- **CCITT (Comité Consultatif International pour le Telegraph 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 lĩnh 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 hóa 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 hóa 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 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.

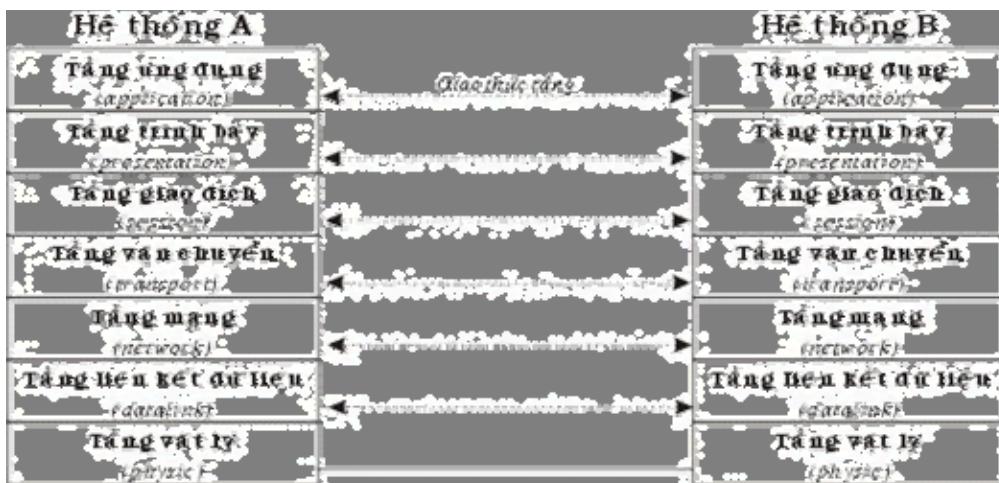
→ Hiệm vụ của các tầng trong mô hình OSI:

• **Tầng ứng dụng (Application layer):** tầng ứng dụng quy định giao diện giữa người sử dụng và môi trường OSI, nó cung cấp các phương tiện cho người sử dụng truy cập và 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 giao dịch (Session layer):** tầng giao dịch quy định một giao diện ứng dụng cho tầng vận chuyển sử dụng. → 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. → 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 chuyền 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..

2. Mô hình SNA (Systems Network Architecture)

Tháng 9/1973, Hãng IBM giới thiệu một kiến trúc mạng máy tính Sâ A (System Network Architecture). Đến năm 1977 đã có 300 trạm Sâ A được cài đặt. Cuối năm 1978, số lượng đã tăng lên đến 1250, rồi cứ theo đó cho đến nay đã có 20.000 trạm Sâ A đang được hoạt động. Qua con số này chúng ta có thể hình dung được mức độ quan trọng và tầm ảnh hưởng của Sâ A trên toàn thế giới.

Cần lưu ý rằng Sâ A không là một chuẩn quốc tế chính thức như OSI nhưng do vai trò to lớn của hãng IBM trên thị trường Cả TT nên Sâ A trở thành một loại chuẩn thực tế và khá phổ biến. Sâ A là một đặc tả gồm rất nhiều tài liệu mô tả kiến trúc của mạng xử lý dữ liệu phân tán. Ở đây 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.

Sâ A được tổ chức xung quanh khái niệm miền (domain). Một Sâ A domain là một điểm điều khiển các dịch vụ hệ thống (Systems Services control point - SSCP) và nó sẽ điều khiển tất cả các tài nguyên đó. Các tài nguyên ở đây có thể là các đơn vị vật lý, các đơn vị logic, các liên kết dữ liệu và các thiết bị. Có thể ví SSCP như là "trái tim và khói óc" của Sâ A. Ở đây điều khiển Sâ A domain bằng cách gói các lệnh tới một đơn vị vật lý, đơn vị vật lý này sau khi nhận được lệnh sẽ quản lý tất cả các tài nguyên trực tiếp với nó. đơn vị vật

lý thực sự là một "đối tác" của SSCP và chứa một tập con các khả năng của SSCP. Các Đơn vị vật lý đảm nhiệm việc quản lý của mỗi nút Sả A.

Sả A phân biệt giữa các nút miền con (Subarea node) và các nút ngoại vi (peripheral node).

- Một nút miền con có thể dẫn đường cho dữ liệu của người sử dụng qua toàn bộ mạng. Ở 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. Ở không dẫn đường giữa các nút miền con. Các nút được nối và điều khiển theo giao thức SDLC (Synchronous Data Link Control). Mỗi nút ngoại vi chỉ liên lạc được với nút miền con mà nó nối vào.

Mạng Sả A dựa trên cơ chế phân tầng, trước đây thì 2 hệ thống ngang hàng không được trao đổi trực tiếp. Sau này phát triển thành Sả A mở rộng: Lúc này hai tầng ngang hàng nhau có thể trao đổi trực tiếp. Với 6 tầng có tên gọi và chức năng tất như sau:

- **Tầng quản trị chức năng SNA (SNA Function Manegement)** Tầng này thật ra có thể chia tầng này làm hai tầng như sau:
 - **Tầng dịch vụ giao tác (Transaction)** cung cấp các dịch vụ ứng dụng đến người dùng một mạng Sả A. Ở hững dịch vụ đó như : DIA cung cấp các tài liệu phân bố giữa các hệ thống văn phòng, Sả A DS (văn phòng dịch vụ phân phối) cho việc truyền thông bất đồng bộ giữa các ứng dụng phân tán và hệ thống văn phòng. Tầng dịch vụ giao tác cũng cung cấp các dịch vụ và cấu hình, các dịch vụ quản lý để điều khiển các hoạt động mạng.
 - **Tầng dịch vụ trình diễn (Presentation Services):** tầng này thì liên quan với sự hiển thị các ứng dụng, người sử dụng đầu cuối và các dữ liệu hệ thống. Tầng này cũng định nghĩa các giao thức cho việc truyền thông giữa các chương trình và điều khiển truyền thông ở mức hội thoại.
 - **Tầng kiểm soát luồng dữ liệu (Data flow control)** tầng này cung cấp các dịch vụ điều khiển luồng lưu thông cho các phiên từ logic này đến đơn vị logic khác (LU - LU). Ở 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 gửi và nhận. Ở chung nó yểm trợ phương thức khai thác hai chiều đồng thời (Full duplex).
 - **Tầng kiểm soát truyền (Transmission control):** Tầng này cung cấp các điều khiển cơ bản của các phần tài nguyên truyền trong mạng, bằng cách xác định số trình tự nhận được, và quản lý việc theo dõi mức phiên. Tầng này cũng hỗ trợ cho việc mã hóa dữ liệu và cung cấp hệ thống hỗ trợ cho các nút ngoại vi.
 - **Tầng kiểm soát đường dẫn (Path control):** Tầng này cung cấp các giao thức để tìm đường cho một gói tin qua mạng Sả A và để kết nối với các mạng Sả A khác, đồng thời nó cũng kiểm soát các đường truyền này.
 - **Tầng kiểm soát liên kết dữ liệu (Data Link Control):** Tầng này cung cấp các giao thức cho việc truyền các gói tin thông qua đường truyền vật lý giữa hai node

và cũng cung cấp các điều khiển lưu thông và phục hồi lỗi, các hỗ trợ cho tầng này là các giao thức SDLC, System/370, X25, IEEE 802.2 và 802.5.

- **Tầng kiểm soát vật lý (Physical control):** Tầng này cung cấp một giao diện vật lý cho bất cứ môi trường truyền thông nào mà gắn với nó. Tầng nào định nghĩa các đặc trưng của tín hiệu cần để thiết lập, duy trì và kết thúc các đường nối vật lý cho việc hỗ trợ kết nối.



Hình 3.6: Tương ứng các tầng các kiến trúc SNI và OSI

cuuduongthancong.com

Chương 4

Mô hình kết nối các hệ thống mở

Open Systems Interconnection

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 cách 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 hiện.
- 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 nghĩa 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).

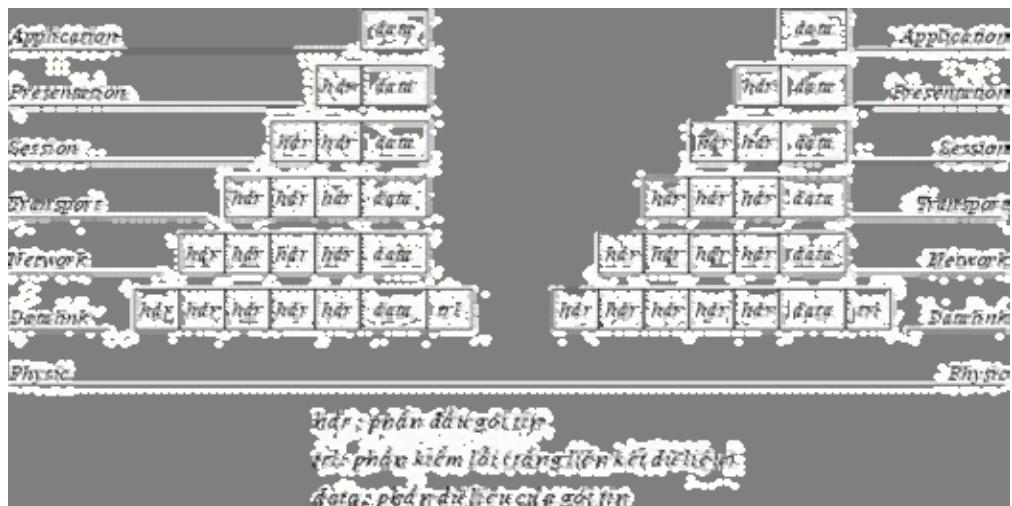
- *Giao thức có liên kết*: trước khi truyền dữ liệu hai tầng đồng mức cần thiết lập một liên kết logic và các gói tin được trao đổi thông qua liên kết này, việc có liên kết logic sẽ nâng cao độ an toàn trong truyền dữ liệu.
- *Giao thức không liên kết*: trước khi truyền dữ liệu không thiết lập liên kết logic và mỗi gói tin được truyền độc lập với các gói tin trước hoặc sau nó.

Ảnh 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. Ảnh 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, 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. Ở 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 để khác và được xem như là gói tin của tầng mới, công việc 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. Ở 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.

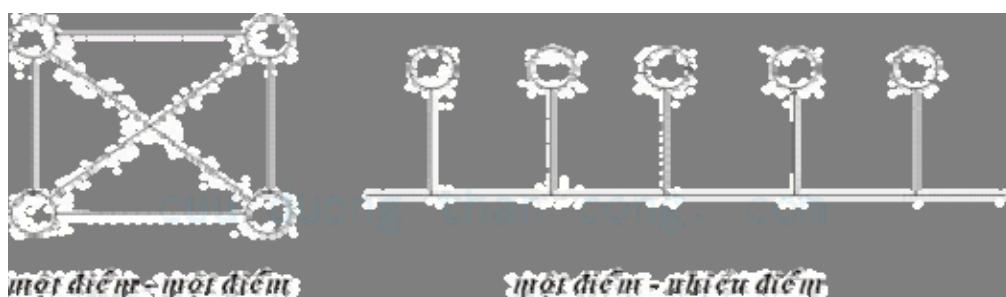
Các giao thức được xây dựng cho tầng vật lý được phân chia thành phân chia thành hai loại giao thức sử dụng phương thức truyền thông dị bộ (asynchronous) và phương thức truyền thông đồng bộ (synchronous).

- *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. Ở đó 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. Ở đó phải xác định cơ chế truy nhập thông tin trên mạng và phương tiện gửi mỗi gói tin sao cho nó được đưa đến cho người nhận đã định.

Tầng liên kết dữ liệu có hai phương thức liên kết dựa trên cách kết nối các máy tính, đó là phương thức "một điểm - một điểm" và phương thức "một điểm - nhiều điểm". Với phương thức "một điểm - một điểm" các đường truyền riêng biệt được thiết lập để nối các cặp máy tính lại với nhau. Phương thức "một điểm - nhiều điểm" tất cả các máy phân chia chung một đường truyền vật lý.



Hình 4.2: Các đường truyền kết nối kiểu "một điểm - một điểm" và "một điểm - nhiều điểm".

Tầng liên kết dữ liệu cũng cung cấp cách phát hiện và sửa lỗi cơ bản để đảm bảo cho dữ liệu nhận được giống hoàn toàn với dữ liệu gửi đi. Ở đó 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 tự 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)

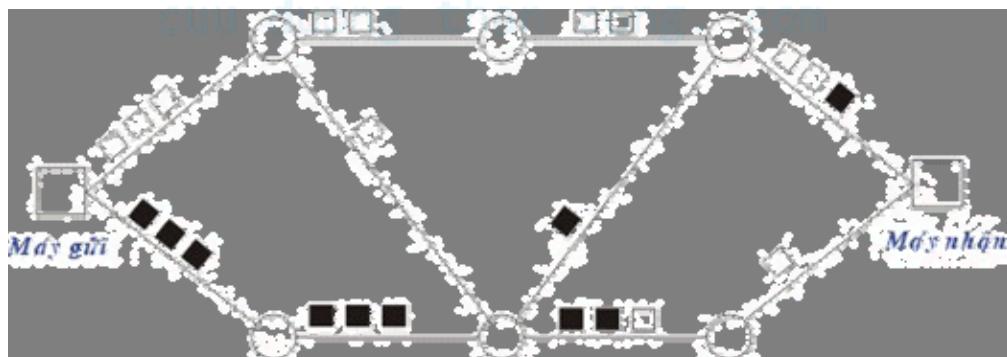
Tầng mạng (network layer) nhằm đến việc kết nối các mạng với nhau bằng cách tìm đường (routing) cho các gói tin từ một mạng này đến một mạng khác. Để xác định việc chuyển hướng, vạch đường các gói tin trong mạng, các gói này có thể phải đi qua nhiều chặng trước khi đến được đích cuối cùng. Để luôn tìm các tuyến truyền thông không tắc nghẽn để đưa các gói tin đến đích.

Tầng mạng cung cấp 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. Để hư vậy ở mỗi nút trung gian nó phải thực hiện các chức năng chọn đường và chuyển tiếp.

Việc chọn đường là sự lựa chọn một con đường để truyền một đơn vị dữ liệu (một gói tin chặng 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

Ở gười ta có hai phương thức đáp ứng cho việc chọn đường là phương thức xử lý tập trung và xử lý tại chỗ.

- *Phương thức chọn đường xử lý tập trung* được đặc trưng bởi sự tồn tại của một (hoặc vài) trung tâm điều khiển mạng, chúng thực hiện việc lập ra các bảng đường đi tại từng thời điểm cho các nút và sau đó gửi các bảng chọn đường tới từng nút đọc 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. Ở hư vậy các thông tin tổng thể của mạng cần dùng cho việc chọn đường cần cập nhập và được cất giữ tại mỗi nút.

Thông thường các thông tin được đo lường và sử dụng cho việc chọn đường bao gồm:

- Trạng thái của đường truyền.
- Thời gian trễ khi truyền trên mỗi đường dẫn.
- Mức độ lưu thông trên mỗi đường.
- Các tài nguyên khả dụng của mạng.

Khi có sự thay đổi trên mạng (ví dụ thay đổi về cấu trúc của mạng do sự cố tại một vài nút, phục hồi của một nút mạng, nối thêm một nút mới... hoặc thay đổi về mức độ lưu thông) các thông tin trên cần được cập nhật vào các cơ sở dữ liệu về trạng thái của mạng.

Hiện nay nhu cầu truyền thông đa phương tiện (tích hợp dữ liệu văn bản, đồ họa, 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. Ở 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. Ở gười ta chia giao thức tầng mạng thành các loại sau:

- Mạng loại A: Có tỷ suất lỗi và sự cố có báo hiệu chấp nhận được (tức là chất lượng chấp nhận được). Các gói tin được giả thiết là không bị mất. Tầng vận chuyển không cần cung cấp các dịch vụ phục hồi hoặc sắp xếp thứ tự lại.
- Mạng loại B: Có tỷ suất lỗi chấp nhận được nhưng tỷ suất sự cố có báo hiệu lại không chấp nhận được. Tầng giao vận phải có khả năng phục hồi lại khi xảy ra sự cố.
- Mạng loại C: Có tỷ suất lỗi không chấp nhận được (không tin cậy) hay là giao thức không liên kết. Tầng giao vận phải có khả năng phục hồi lại khi xảy ra lỗi và sắp xếp lại thứ tự các gói tin.

Trên cơ sở loại giao thức tầng mạng chúng ta có 5 lớp giao thức tầng vận chuyển đó là:

- *Giao thức lớp 0 (Simple Class - lớp đơn giản)*: cung cấp các khả năng rất đơn giản để thiết lập liên kết, truyền dữ liệu và hủy bỏ liên kết trên mạng "có liên kết" loại A. Ở đây 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 ảnh 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 dịch 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" (năm quyền) trong quá trình trao đổi dữ liệu.

Trong trường hợp mạng là hai chiều luân phiên thì诞生 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 chuyên 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 trả 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 tuân tự hóa các sự kiện đến từ các ASE thành tố của nó.

cuu duong than cong. com

cuu duong than cong. com

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 là: tập hợp các quy tắc chuẩn đã được quy ước mà tất cả các thành viên 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

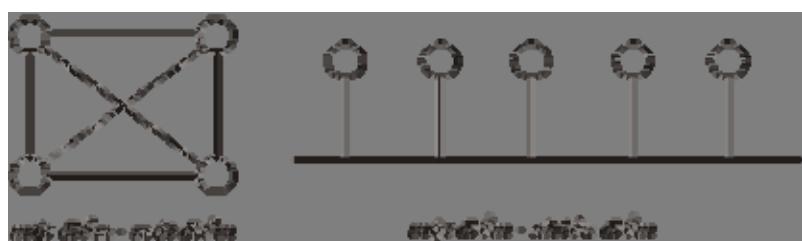
I. Cấu trúc của mạng (Topology)

Hình trạng của mạng cục bộ thể hiện qua cấu trúc hay hình dáng hình học của các đường dây cáp mạng dùng để liên kết các máy tính thuộc mạng với nhau. Các mạng cục bộ thường hoạt động dựa trên cấu trúc đã định sẵn liên kết các máy tính và các thiết bị có liên quan.

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 tín hiệu (1,10 hoặc 100 Mb/s); BASE (nếu là Baseband) hoặc BROAD (nếu là Broadband).

- 10BASE5: Dùng cáp đồng trực 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 trực 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 Token ring của IBM.

3. Dạng hình sao (Star)

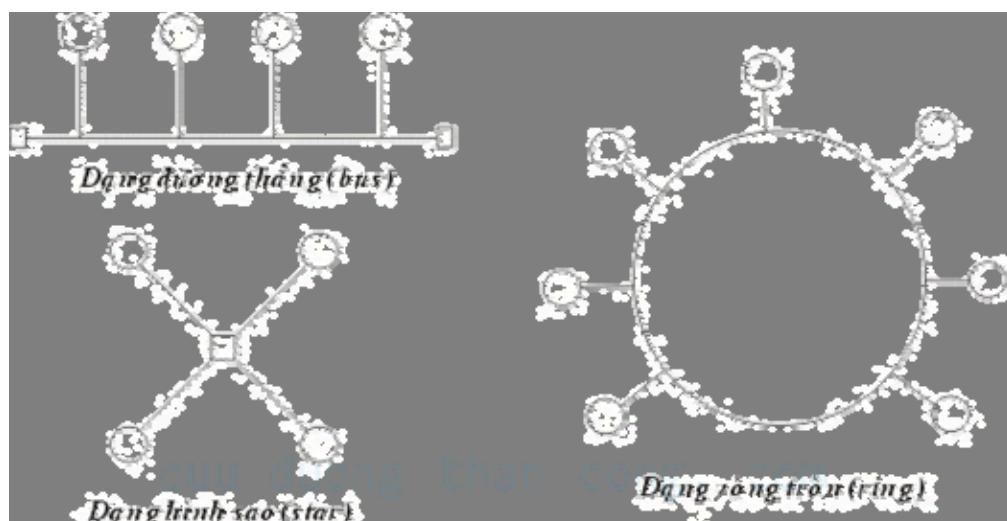
Ở dạng hình sao, tất cả các trạm được nối vào một thiết bị trung tâm có nhiệm vụ nhận tín hiệu từ các trạm và chuyển tín hiệu đến trạm đích với phương thức kết nối là phương thức "một điểm - một điểm". Thiết bị trung tâm hoạt động giống như một tổng đài cho phép thực hiện việc nhận và truyền dữ liệu 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). Ảnh có trực tiếp 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 STARLAnet của AT&T và S-Net của IBM.



Hình 5.2 : Các loại cấu trúc chính của mạng cục bộ.

	Đường thẳng	Vòng Tròn	Hình sao
Ứng dụng	Tốt cho trường hợp mạng nhỏ và mạng có giao thông thấp và	Tốt cho trường hợp mạng có số trạm ít hoạt động với tốc độ cao, không cách nhau xa lắm hoặc mạng có lưu lượng dữ	hiện nay mạng sao là cách tốt nhất cho trường hợp phải tích hợp dữ liệu và tín hiệu tiếng. Các

	lưu lượng dữ liệu thấp	liệu phân bố không đều.	mạng đệm 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 chinh và bán sảm phẩm ở thị trường .Sự thừa kenh truyền được khuyến để giảm bớt nguy cơ xuất hiện sự cố trên mạng	Phải dự trù gấp đôi nguồn lực hoặc phải có 1 phương thức thay thế khi 1 nút không hoạt động nếu vẫn muốn mạng hoạt động bình thường	Tổng phí rất cao khi làm nhiệm vụ của thiết bị trung tâm, thiết bị trung tâm i không được dùng vào việc khác .Số lượng dây riêng cũng nhiều.
Nguy cơ	Một trạm bị hỏng không ảnh hưởng đến cả mạng. Tuy nhiên mạng sẽ có nguy cơ bị tổn hại khi sự cố trên đường dây dẫn chính hoặc có vấn đề với tuyến. Vấn đề trên rất khó xác định được lại rất dễ sửa chữa	Một trạm bị hỏng có thể ảnh hưởng đến cả hệ thống vì các trạm phục thuộc vào nhau. Tim 1 repeater hỏng rất khó ,và lại việc sửa chữa thẳng hay dùng mưu mẹo xác định điểm hỏng trên mạng có địa bàn rõ ràng rất khó	Độ tin cậy của hệ thống phụ thuộc vào thiết bị trung tâm, .nếu bị hỏng thì mạng ngưng hoạt động Sự ngưng hoạt động tại thiết bị trung tâm thường không ảnh hưởng đến toàn bộ hệ thống .
Khả năng mở rộng	Việc thêm và định hình lại mạng này rất dễ.Tuy nhiên việc kết nối giữa các máy tính và thiết bị của các hãng khác nhau khó có thể vì chúng phải có thể nhận cùng	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 rộng hạn chế, đa số các thiết bị trung tâm chỉ chịu đựng nối 1 số nhất định liên kết. Sự hạn chế về tốc độ truyền dữ liệu và băng tần thường được đòi hỏi ở mỗi người sử dụng. Các hạn chế này giúp cho các chức năng xử lý trung tâm không

	địa chỉ và dữ liệu	bị quá tải bởi tốc độ thu nạp tại tại cổng truyền và giá thành mỗi cổng truyền của thiết bị trung tâm thấp .
--	--------------------	--

Hình 6.4 : Bảng so sánh tính năng giữa các cấu trúc của mạng LAN

III. Phương thức truyền tín hiệu

Thông thường có hai phương thức truyền tín hiệu trong mạng cục bộ là dùng băng tần cơ sở (baseband) và băng tần rộng (broadband). Sự khác nhau chủ yếu giữa hai phương thức truyền tín hiệu này là băng tần 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 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 dài 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 rãnh hay không để gửi gói dữ liệu của, nếu đường truyền đang bận trạm phải chờ đợi chỉ được truyền khi thấy đường truyền rãnh. Ở đâu 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 rãnh thì truyền dữ liệu đi.
- Trạm tiếp tục kiểm tra đường truyền đến khi đường truyền rãnh 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. Ở gược lại phương thức 2 cố gắng giảm thời gian trống của đường truyền bằng cách cho phép trạm có thể truyền ngay sau khi một cuộc truyền kết thúc song nếu lúc đó có thêm một trạm khác đang đợi thì khả năng xảy ra xung đột là rất cao. Phương thức 3 với giá trị p phải lựa chọn hợp lý có thể tối thiểu hóa được khả năng xung đột lẫn thời gian trống của đường truyền.

Khi lưu lượng các gói dữ liệu cần di chuyển trên mạng quá cao, thì việc dung độ có thể xảy ra với số 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 đây 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 rỗng). Một trạm muốn truyền dữ liệu thì phải đợi đến khi nhận được một thẻ bài rãnh. Khi đó trạm sẽ đổi bit trạng thái của thẻ bài thành bận, nén gói dữ liệu có kèm theo địa chỉ 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 dung độ dữ liệu không thể xảy ra, do vậy hiệu suất truyền dữ liệu của mạng không thay đổi.

Trong các giao thức này cần giải quyết hai vấn đề có thẻ 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.

Ở hư vậy trong mạng phải thiết lập được vòng logic (hay còn gọi là vòng ảo) bao gồm các trạm đang hoạt động nối trong mạng được xác định vị trí theo một chuỗi thứ tự mà trạm cuối cùng của chuỗi sẽ tiếp liền sau bởi trạm đầu tiên. Mỗi trạm được biết địa chỉ của các trạm kè 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 trực 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 - Unshielded 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	Băng đồng, có 4 và 25 cặp dây (loại 3, 4, 5)	Băng đồng, 2 dây, đường kính 5mm	Băng đồng, 2 dây, đường kính 10mm	Thủy tinh, 2 sợi
Loại kết nối	RJ-25 hoặc 50-pin telco	Bảng C	Âm -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	Đơn giản	Đơn giản	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 dài 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. Ảnh hưởng của 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.

Dài 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 tử để truyền dữ liệu nên nó hoàn toàn không bị ảnh hưởng của nhiễu điện tử 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.

cuu duong than cong. com

cuu duong than cong. com

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 trực 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.

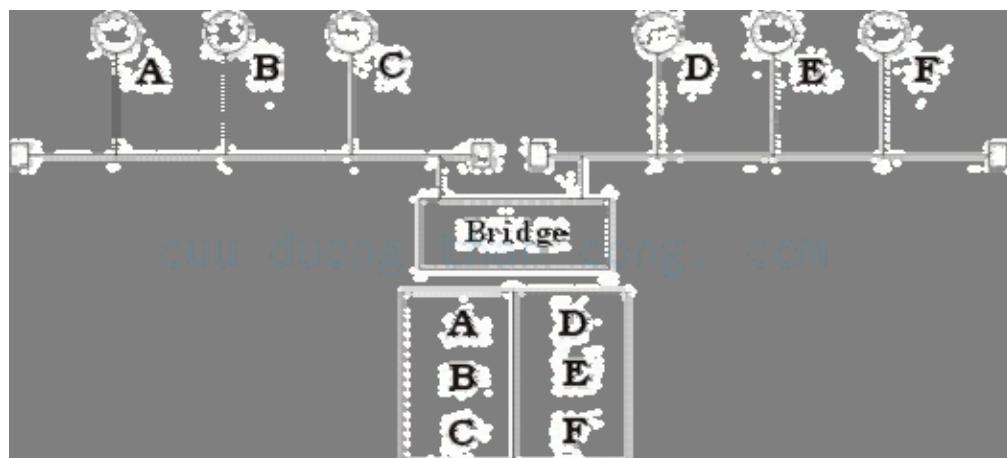
Việc sử dụng Repeater không thay đổi nội dung các tín hiệu đi qua nên nó chỉ được dùng để nối hai mạng có cùng giao thức truyền thông (như hai mạng Ethernet hay hai mạng Token ring) nhưng không thể nối hai mạng có giao thức truyền thông khác nhau (như một mạng Ethernet và một mạng Token ring). Thêm nữa 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.

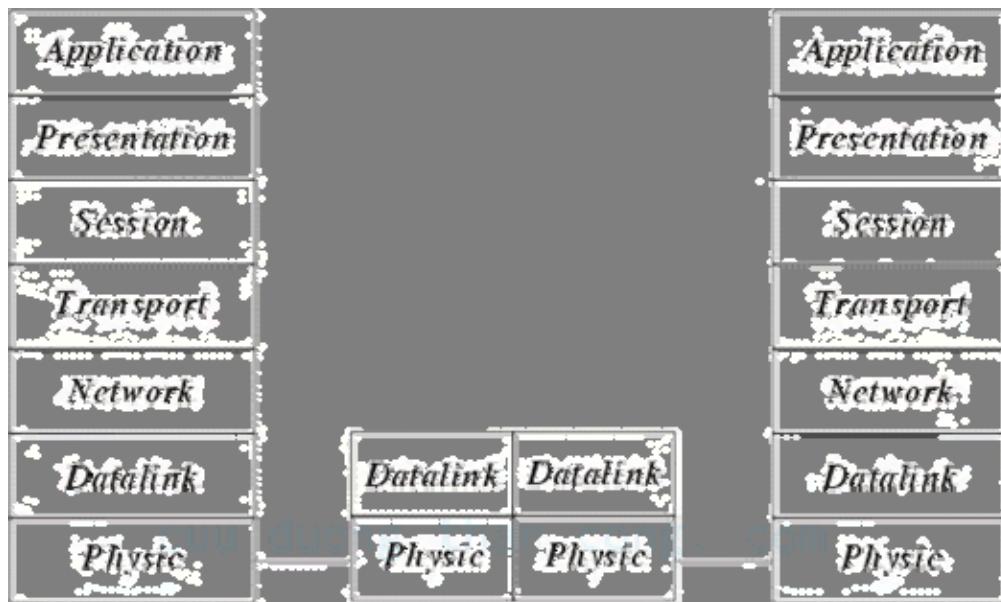
Để thực hiện được điều này trong Bridge ở mỗi đầu kết nối có một bảng các địa chỉ các trạm được kết nối vào phía đó, khi hoạt động cầu nối xem xét mỗi gói tin nó nhận được bằng cách đọc địa chỉ của nơi gửi và nhận và dựa trên bảng địa chỉ phía nhận được gói tin nó quyết định gửi gói tin hay không và bỏ 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 bỏ 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.

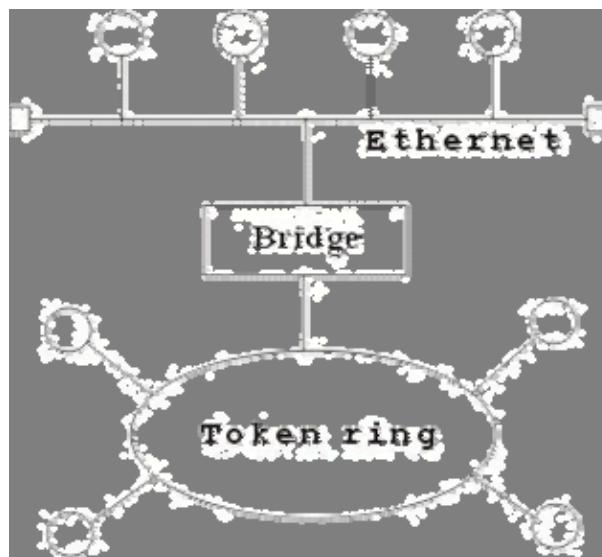
Hiện nay có hai loại Bridge đang được sử dụng là Bridge vận chuyển và Bridge biên dịch. Bridge vận chuyển dùng để nối hai mạng cục bộ cùng sử dụng một giao thức truyền thông của tầng liên kết dữ liệu, tuy nhiên mỗi mạng có thể sử dụng loại dây nối khác nhau. Bridge vận chuyển không có khả năng thay đổi 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 Ethernet trên mạng Ethernet. Cầu nối có thể chuyển một gói tin theo chuẩn đang sử dụng trên mạng Ethernet 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.

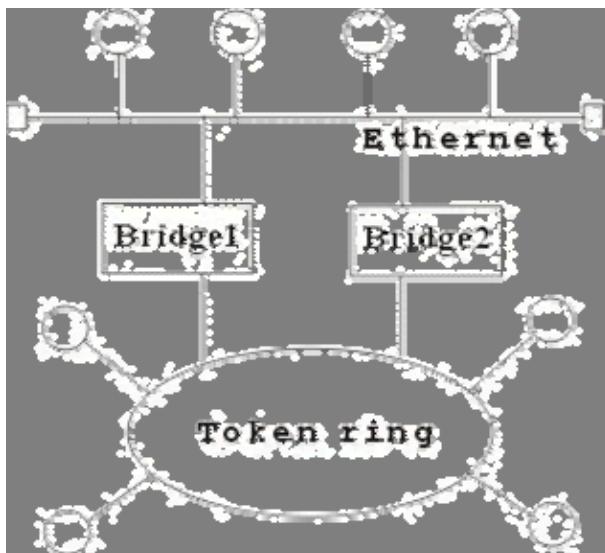


Hình 6.5: Ví dụ về Bridge biên dịch

Ở gười ta sử dụng Bridge trong các trường hợp sau :

- Mở rộng mạng hiện tại khi đã đạt tới khoảng cách tối đa do Bridge sau khi xử 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 từng 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 đôi tượng vận chuyển. Ở đó 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.

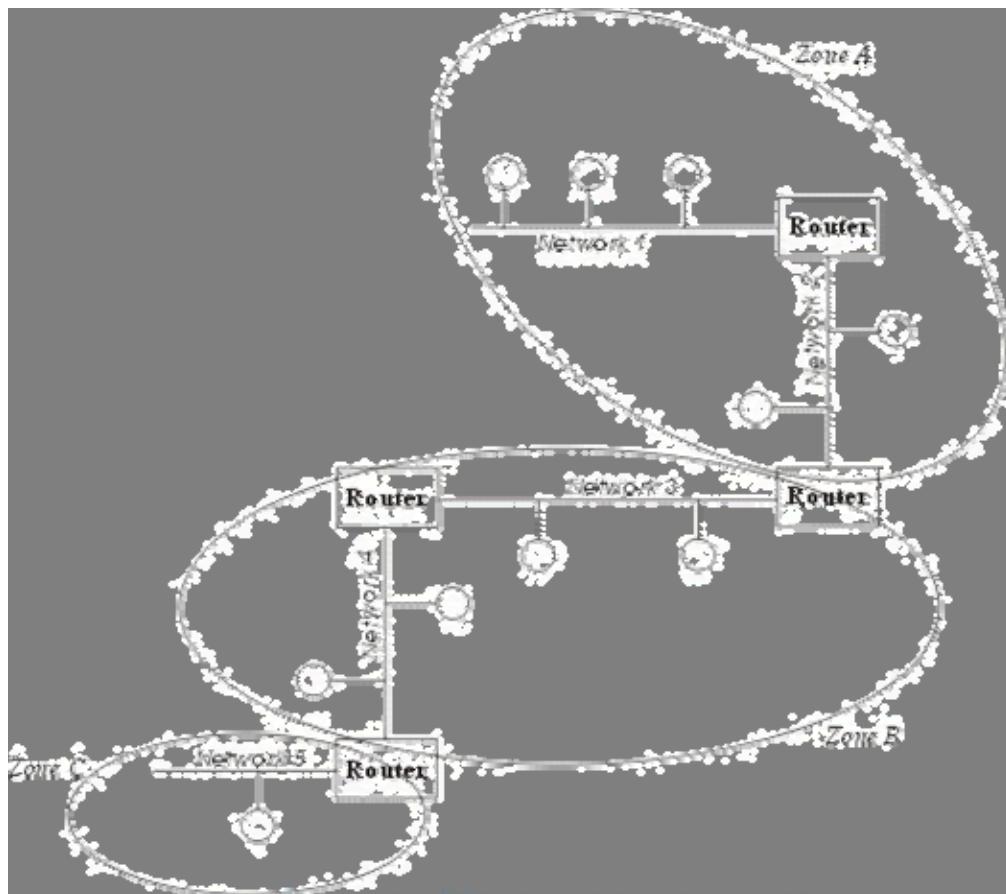


Hình 6.6 : Liên kết mạng với 2 Bridge

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 cắm 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.

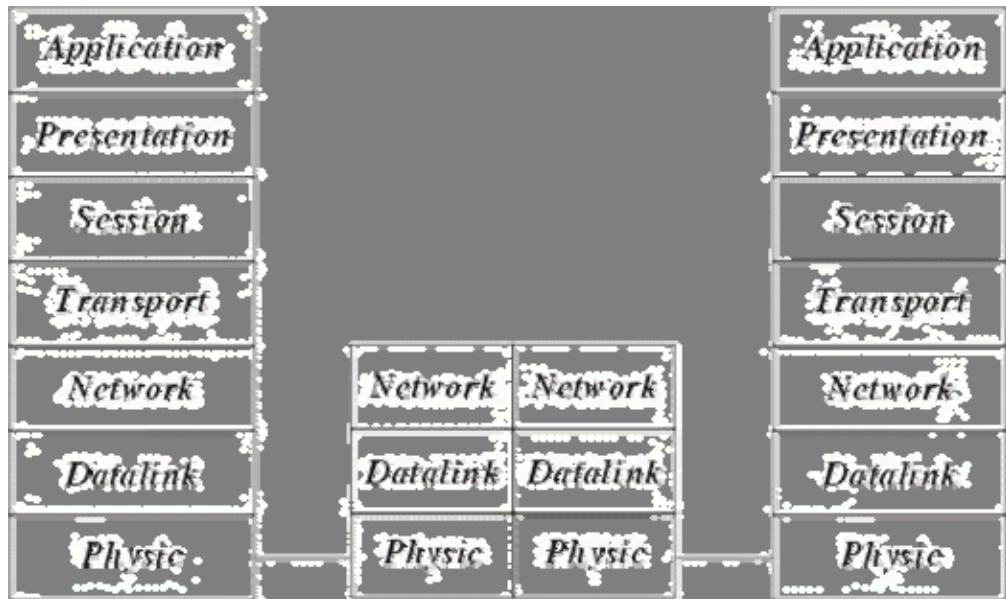
Khác với Bridge hoạt động trên tầng liên kết dữ liệu nên Bridge phải xử lý mọi gói tin trên đường truyền thì Router có địa chỉ riêng biệt và nó chỉ tiếp nhận và xử lý các gói tin gửi đến nó mà thôi. Khi một trạm muốn gửi gói tin qua Router thì nó phải gửi gói tin với địa chỉ trực tiếp của Router (Trong 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.

Ở giao diện 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 đổi gói tin của giao thức này sang gói tin

của giao thức kia, Router cũng xử lý nhận kích thước các gói tin khác nhau (Router có thể chia nhỏ một gói tin lớn thành nhiều gói tin nhỏ trước truyền trên mạng).

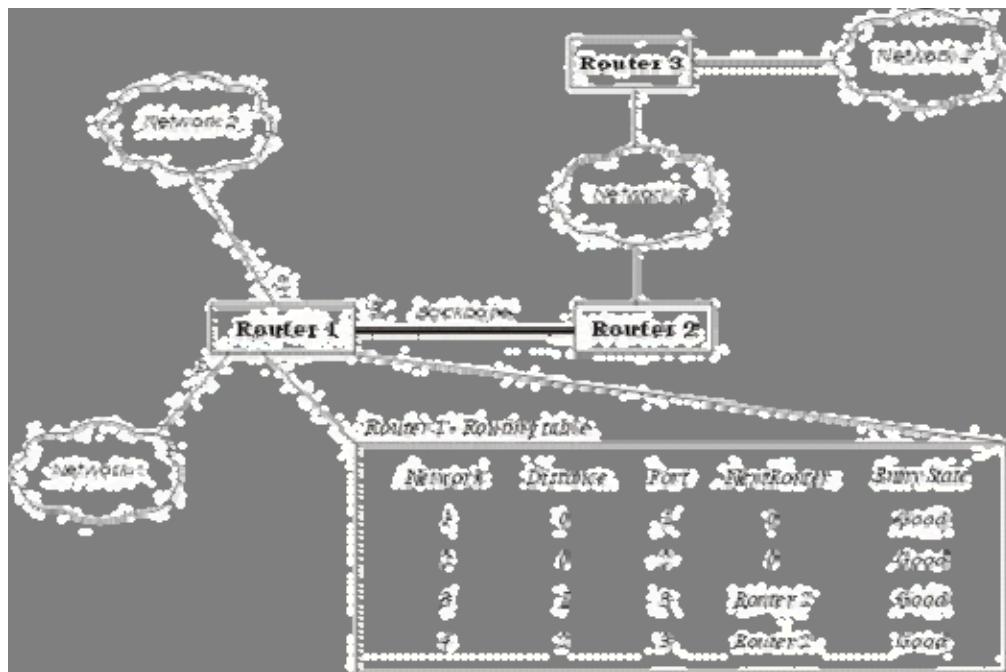


Hình 6.8: Hoạt động của Router trong mô hình OSI

Để ngăn chặn việc mất mát số liệu Router còn nhận biết được đường nào có thể chuyển vận và ngừng chuyển vận khi đường bị tắc.

Các lý do sử dụng Router :

- Router có các phần mềm lọc ưu việt hơn là Bridge do các gói tin muôn 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 dữ liệu lên đường truyền.
- Router có thể dùng trong một liên mạng có nhiều vùng, mỗi vùng có giao thức riêng biệt.
- Router có thể xác định được đường đi an toàn và tốt nhất trong mạng nên độ an toàn của thông tin được đảm bảo hơn.
- Trong một mạng phức hợp khi các gói tin luân chuyển các đường có thể gây nên tình trạng tắc nghẽn của mạng thì các Router có thể được cài đặt các phương thức nhằm tránh được tắc nghẽn.



Hình 6.9: Ví dụ về bảng chỉ đường (Routing table) của Router.

Các phương thức hoạt động của Router

Đó là phương thức mà một Router có thể nối với các Router khác để qua đó chia sẻ thông tin về mạng hiện co. Các chương trình chạy trên Router luôn xây dựng bảng chỉ đường qua việc trao đổi các thông tin với các Router khác.

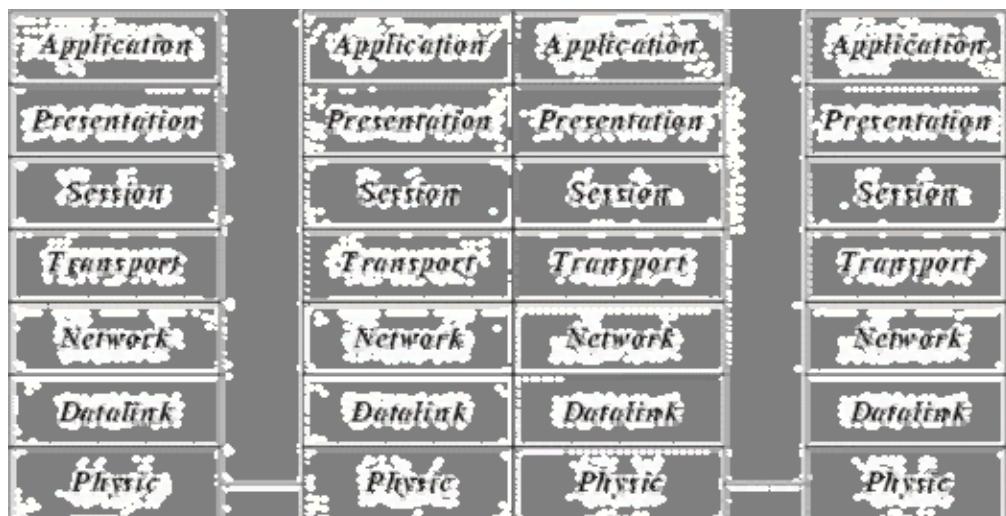
- Phương thức véc tơ khoảng cách : mỗi Router luôn luôn truyền đi thông tin về bảng chỉ đường của mình trên mạng, thông qua đó các Router khác sẽ cập nhật lên bảng chỉ đường của mình.
- Phương thức trạng thái tĩnh : Router chỉ truyền các thông báo khi có phát hiện có sự thay đổi trong mạng và chỉ khi đó các Router khác cập nhật lại bảng chỉ đường, thông tin truyền đi khi đó thường là thông tin về đường truyền.

Một số giao thức hoạt động chính của Router

- *RIP (Routing Information Protocol)* được phát triển bởi Xerox à etwork system và sử dụng SPX/IPX và TCP/IP. RIP hoạt động theo phương thức véc tơ khoảng cách.
- *NLSP (Netware Link Service Protocol)* được phát triển bởi à ovell dùng để thay thế RIP hoạt động theo phương thức véc tơ 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 nội)

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 khuếch đại và xử lý các tín hiệu điện tử truyền giữa các thiết bị của mạng. Quá 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. Ảo 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 chuyên mạch để phát trên một cổng có thể nối tới trạm đích.

cuu duong than cong. com

cuu duong than cong. com

Chương 7

Giao thức TCP/IP

Giao thức TCP/IP được phát triển từ mạng ARPA-ET và Internet và được dùng như giao thức mạng và vận chuyển trên mạng Internet. TCP (Transmission Control Protocol) là giao thức thuộc tầng vận chuyển và IP (Internet Protocol) là giao thức thuộc tầng mạng của mô hình OSI. Họ giao thức TCP/IP hiện nay là giao thức được sử dụng rộng rãi nhất để liên kết các máy tính và các mạng.

Hiện nay các máy tính của hầu hết các mạng có thể sử dụng giao thức TCP/IP để liên kết với nhau thông qua nhiều hệ thống mạng với kỹ thuật khác nhau. Giao thức TCP/IP thực chất là một họ giao thức cho phép các hệ thống mạng cùng làm việc với nhau thông qua việc cung cấp phương tiện truyền thông liên mạng.

I. Giao thức IP

1. Tổng quát

Để hiệm vụ chính của giao thức IP là cung cấp khả năng kết nối các mạng con thành liên kết mạng để truyền dữ liệu, vai trò của IP là vai trò của giao thức tầng mạng trong mô hình OSI. Giao thức IP là một giao thức kiểu không liên kết (connectionless) 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 chưa 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.

Địa chỉ 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).

Ông 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.

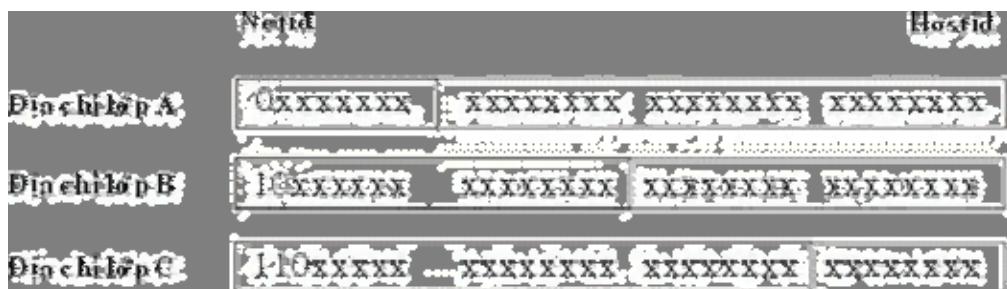
- Mạng lớp B: địa chỉ mạng (netid) là 2 Byte và địa chỉ host (hostid) là 2 byte.

- 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. Ở ngược lại, một địa chỉ có vùng hostid gồm toàn số 1 được dùng để hướng tới tất cả các host nội 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

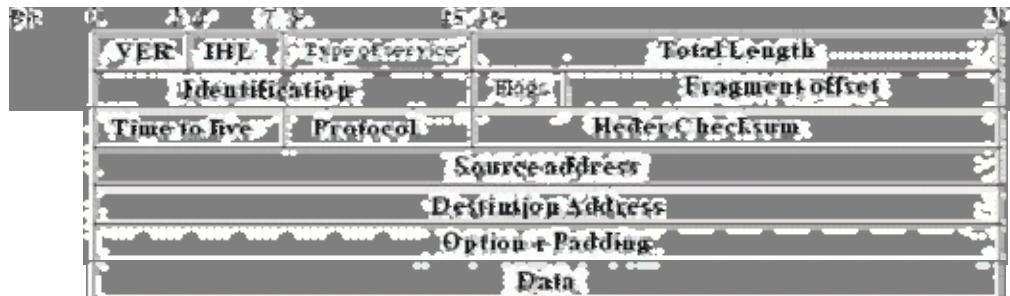
Cần lưu ý rằng các địa chỉ IP được dùng để định danh các host và mạng ở tầng mạng của mô hình OSI, và chúng không phải là các địa chỉ vật lý (hay địa chỉ MAC) của các trạm trên đó một mạng cục bộ (Ethernet, Token Ring.).

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 bỏ 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 buộc 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:

0	1	2
0	DF	MF

- bit 0: reserved - chưa sử dụng, luôn lấy giá trị 0.

- bit 1: (DF) = 0 (May Fragment) = 1 (Don't Fragment)

- bit 2: (MF) = 0 (Last Fragment) = 1 (More 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**:

• ã út trung gian của mạng không được gửi 1 gói tin mà trường này có giá trị= 0.

• Một giao thức có thể xác 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 kê 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. Ảnh 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. Ảnh 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 checksum, 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.

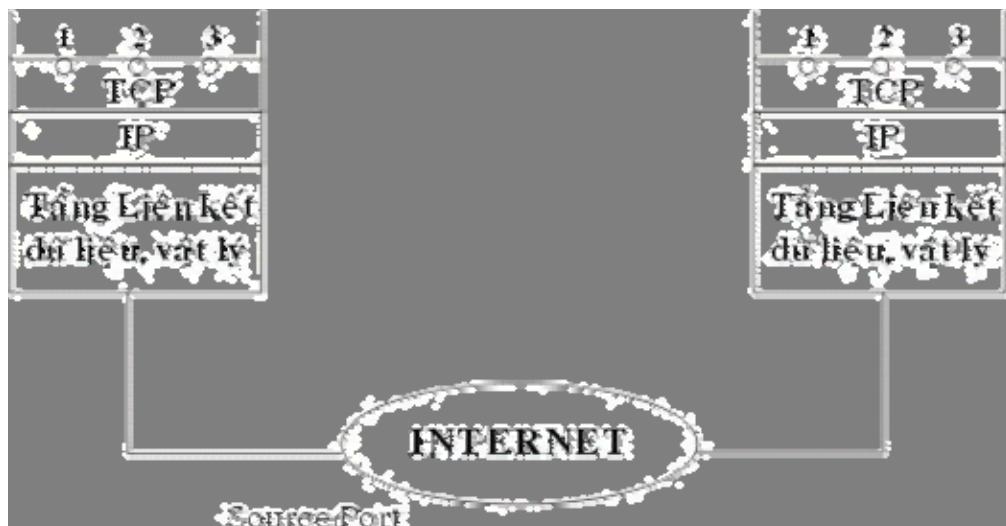
Cuối cùng khi một datagram nhận bởi một thực thể IP ở trạm đích, nó sẽ thực hiện bởi các công việc sau:

- 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 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	à estat
17	Quotd (quote odd day)
20	ftp-data
21	ftp (control)
23	Telnet
25	SMTP
37	Time
53	à ame Server
102	ISO - TSAP
103	X.400
104	X.400 Sending
111	Sun RPC
139	à et BIOS Session source
160 - 223	Reserved

Khi người sử dụng gửi đi một yêu cầu mở liên kết sẽ được nhận hai thông số trả lời từ TCP.

- Thông số Open ID được TCP trả lời ngay lập tức để gán cho một liên kết cục bộ (local connection name) cho liên kết được yêu cầu. Thông số này về sau được dùng để tham chiếu tới liên kết đó. (Trong trường hợp nếu TCP không thể thiết lập được liên kết yêu cầu thì nó phải gửi tham số Open Failure để thông báo.)
- Khi TCP thiết lập được liên kết yêu cầu nó gửi tham số Open Success được dùng để thông báo liên kết đã được thiết lập thành công. Thông báo này được 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 sử 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. Nếu gỡ 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 receive:** 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 sử 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.

Áp dụng 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 URG và đánh dấu dữ liệu bằng bit URG để báo cho người sử dụng cần phải xử 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 hiện 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.

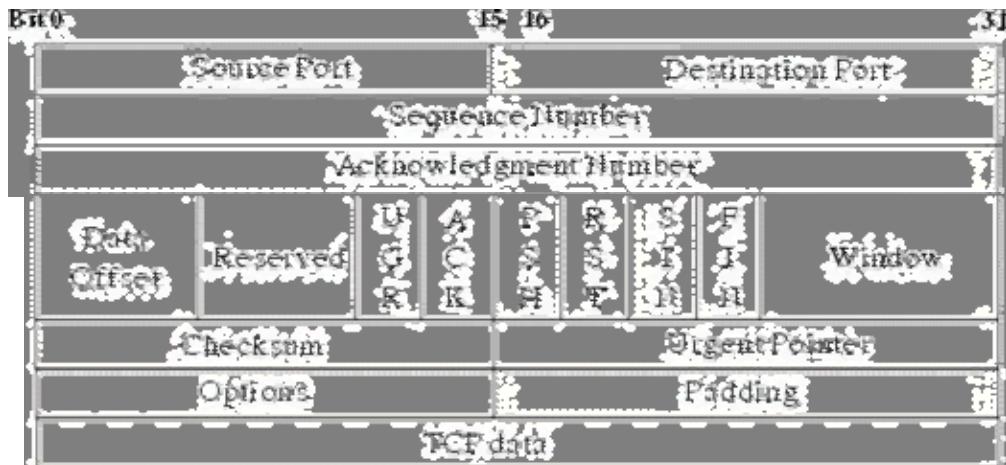
• **Hàm Abort:** Nếu người sử dụng có thể đóng một liên kết bất kỳ và sẽ không chấp nhận dữ liệu qua liên kết đó nữa. Do vậy dữ liệu có thể bị mất đi khi đang được truyền đi. TCP báo cho TCP ở xa biết rằng liên kết đã được hủy bỏ và TCP ở xa sẽ thông báo cho người sử dụng của mình.

 **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 Port (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 SY₀ được thiết lập. Nếu bit SY₀ được thiết lập thì Sequence number là số hiệu tuần tự khởi đầu (IS₀) và byte dữ liệu đầu tiên là IS₀+1.
- Acknowledgment number (32 bit): số hiệu của segment tiếp theo mà trạm nguồn đang chờ để nhận. bao gồm ý báo nhận tốt (các) segment mà trạm đích đã gửi cho trạm nguồn.
- Data offset (4 bit): số lượng bộ 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 trả khẩn (Urgent Pointer) có hiệu lực.
 - ACK: Vùng báo nhận (ACK number) có hiệu lực.
 - PSH: Chức năng PUSH.
 - RST: Khởi động lại (reset) liên kết.
 - SYN : Đồng bộ hóa số hiệu tuần tự (sequence number).
 - FIN : Không còn dữ liệu từ trạm nguồn.

- Window (16 bit): cấp phát credit để kiểm soát nguồn dữ liệu (cơ chế cửa sổ). Đây chính là số lượng các byte dữ liệu, bắt đầu từ byte được chỉ ra trong vùng ACK number, mà trạm nguồn đã sẵn sàng để nhận.
- Checksum (16 bit): mã kiểm soát lỗi cho toàn bộ segment (header + data)
- Urgemt Poiter (16 bit): con trỏ này trả về 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)

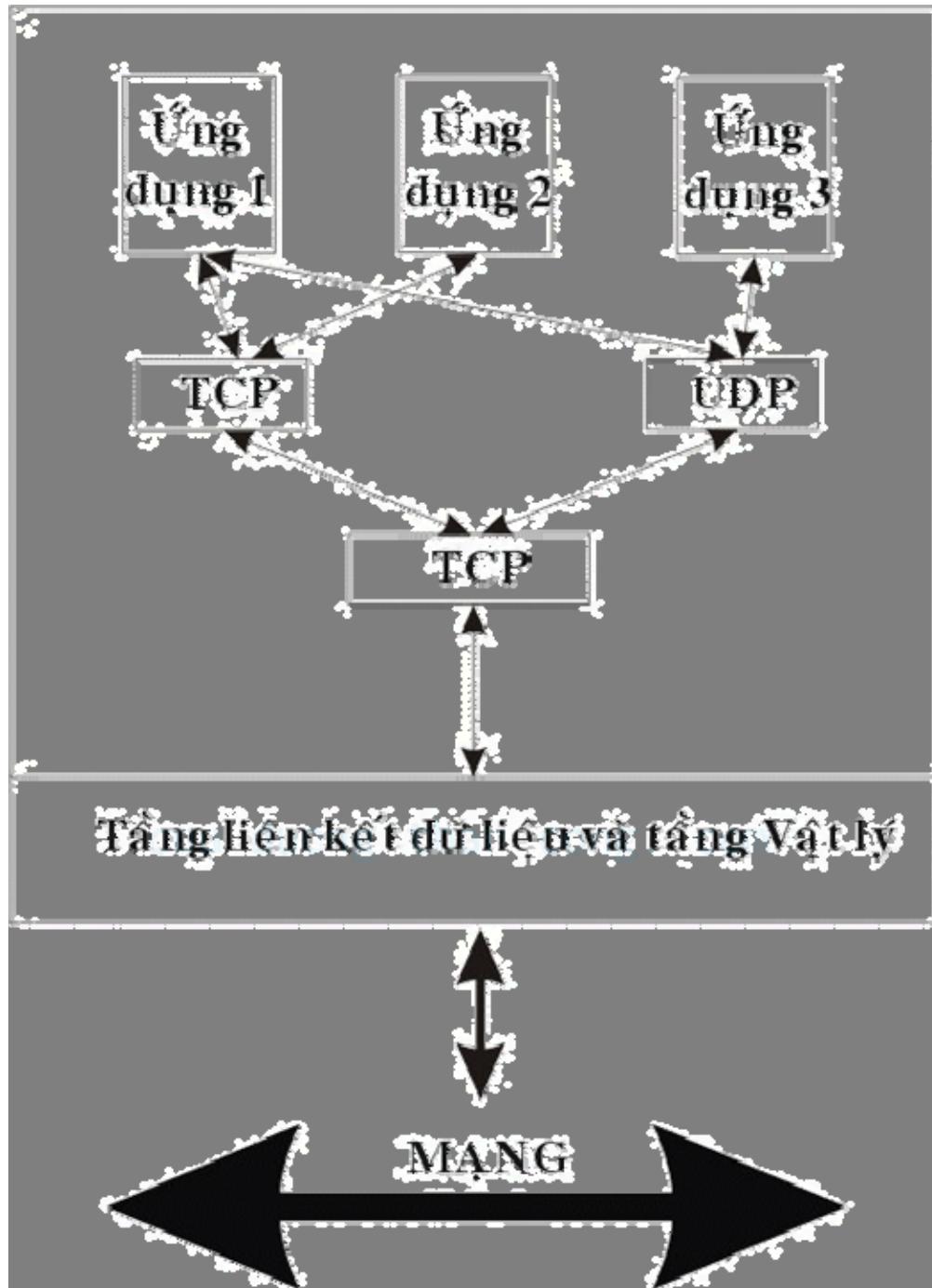
UDP (User Datagram Protocol) là giao thức theo phương thức không liên kết được sử dụng thay thế cho TCP ở trên IP theo yêu cầu của từng ứng dụng. Khác với TCP, UDP không có các chức năng thiết lập và kết thúc liên kết. Tương tự như IP, nó cũng không cung cấp cơ chế báo nhận (acknowledgment), không sắp 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 hướng hoạt động nhanh hơn so với TCP. Ở 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)

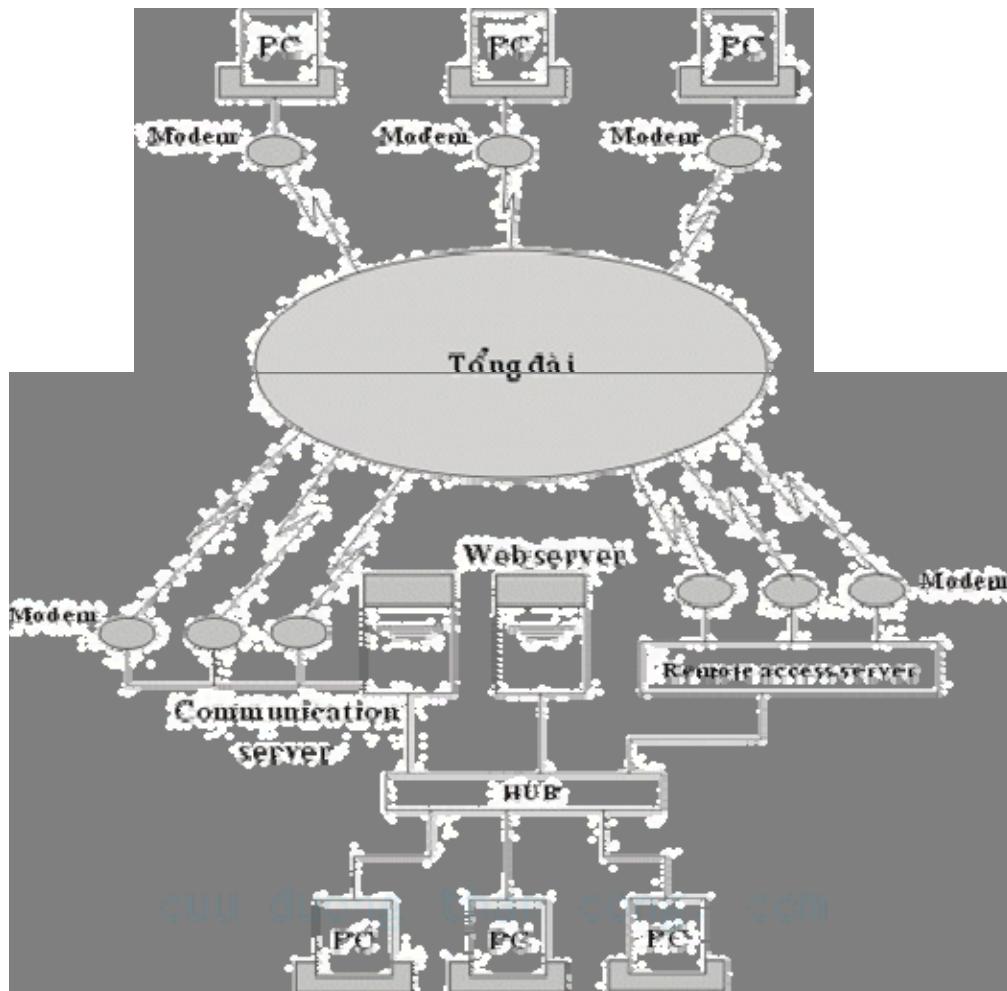
Hiện nay trên thế giới có nhiều dịch vụ dành cho việc chuyển thông tin từ khu vực này sang khu vực khác nhằm liên kết các mạng LAN của các khu vực khác nhau lại. Để có được những liên kết như vậy người ta thường sử dụng các dịch vụ của các mạng diện rộng. Hiện nay trong khi giao thức truyền thông cơ 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 Switching Network)
- Mạng thuê bao (Leased lines Network)
- Mạng chuyển gói tin (Packet Switching Network)

I. Mạng chuyển mạch (Circuit Switching Network)

Để thực hiện được việc liên kết giữa hai điểm nút, một đường nối giữa điểm nút này và điểm nút kia được thiết lập trong mạng để 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 thể 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)	Loại nén	Tốc độ thực tế (bps)
Bell 212A	1200		
CCITT V22	1200		
CCITT V22 bis	2400	Mã P Class 5	2400 - 3600
CCITT V32	9600	Mã P Class 5, V42 bis	9600 - 19200
CCITT V32 bis	14400	Mã P Class 5, V42 bis	14400 - 33600

Hình 8.3: Bảng kỹ thuật modem

Các kỹ thuật nén thường dùng là Mã P Class 5 và V42 bis, Mã P Class 5 cho phép nén với tỷ lệ 1.5:1 và V42 bis nén với tỷ lệ 2:1. Tuy nhiên trên thực tế tỷ lệ nén có thể thay đổi dựa vào dạng dữ liệu được truyền.

- **Chuyển mạch số (Digital):** Đường truyền chuyển mạch số lần đầu tiên được AT&T thiệu vào cuối 1980 khi AT&T giới thiệu mạng chuyển mạch số Acnet với đường truyền 56 kbs. Việc sử dụng đường truyền 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.



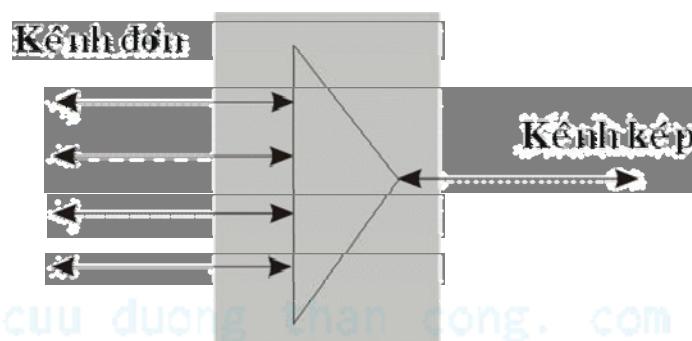
Hình 8.3: Mô hình chuyển mạch số

Mạng chuyên 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 chuyên mạch số có tốc độ 384 Kbps. Ở gười ta có thể dùng mạng chuyên 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 chuyên 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.

Ở gười ta có thể dùng đường truyền 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 tuân 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, Mã P class 5.

2. Phương thức ghép kênh theo thời gian:

Khác với phương thức ghép kênh theo tần số, phương thức ghép kênh theo thời gian chia một chu kỳ thời gian hoạt động của đường truyền trực thành nhiều khoảng nhỏ và mỗi kênh truyền 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. Ở gười ta dùng đường thuê bao là đường truyền kỹ thuật số nối giữa máy của người sử dụng tới nút mạng thuê bao gần nhất.

Hiện nay người ta có các đường truyền thuê bao như sau :

Đường T1 với tốc độ 1.544 Mbps nó bao gồm 24 kênh vớ tốc độ 64 kbps và 8000 bits điều khiển trong 1 giây.

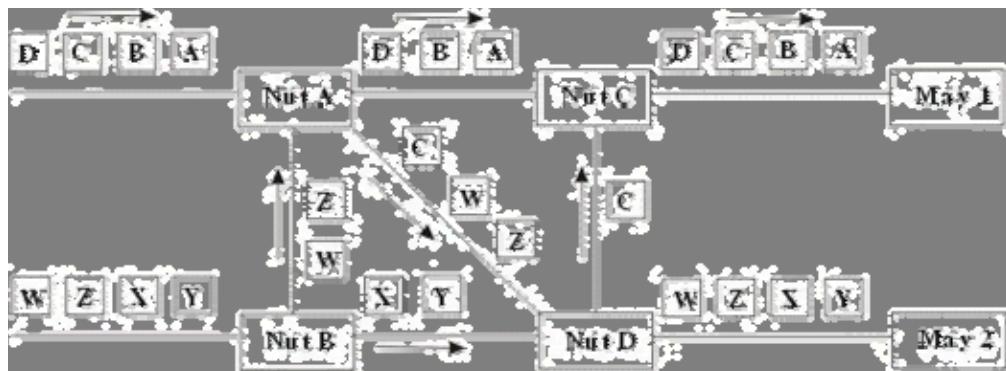
III. Mạng chuyển gói tin (Packet Switching NetWork)

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.

Ở gười ta chia các phương thức chuyển mạch gói ra làm 2 phương thức:

- Phương thức chuyển mạch gói theo sơ đồ rời rạc.
- Phương thức chuyển mạch gói theo đường đi xác định.

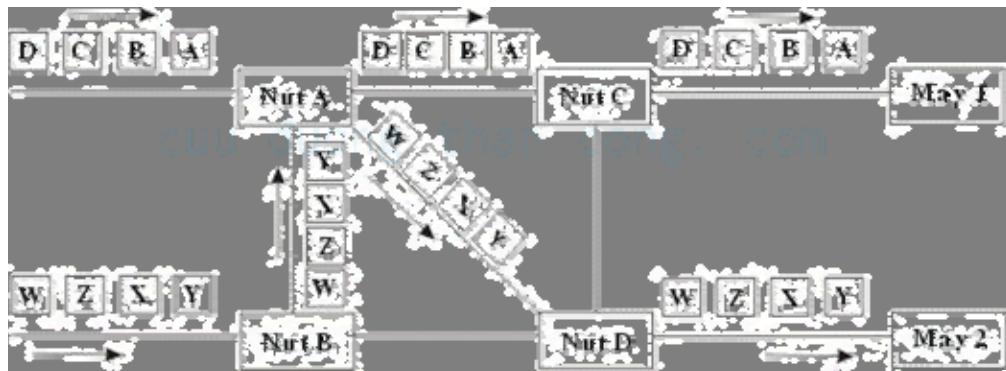
Với phương thức chuyển mạch gói theo sơ đồ rời rạc các gói tin được chuyển đi trên mạng một cách độc lập, mỗi gói tin đều có mang địa chỉ gửi và nơi nhận. Mỗi nút trong mạng khi tiếp nhận gói tin sẽ quyết định xem đường đi của gói tin phụ thuộc vào thuật toán tìm đường tại nút và những thông tin về mạng mà nút đó có. Việc truyền theo phương thức này cho ta sự mềm dẻo nhất định do đường đi với mỗi gói tin trở nên mềm dẻo tuy nhiên điều này yêu cầu một số lượng tính toán rất lớn tại mỗi nút nên hiện nay phần lớn các mạng chuyên 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 cũ 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 lượng đường truyền cao cho dù chất lượng đường 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 tính 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 là mạng Frame Relay 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 lượng 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 channel) khác nhau, mỗi kênh ảo được sử dụng bởi một ứng dụng 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 dài thông linh hoạt và khả năng chuyển tiếp cao tốc và có khả năng quản lý đồng thời dữ liệu số, tiếng nói, hình ảnh và multimedia tương tác.

Mục tiêu của kỹ thuật ATM là nhằm cung cấp một mạng dồn kênh, và chuyển mạch tốc độ cao, độ trễ nhỏ đáp ứng cho các dạng truyền thông đa phương tiện (multimedia)

Chuyển mạch cell cần thiết cho việc cung cấp các kết nối đòi hỏi băng thông cao, tình trạng tắt nghẽn thấp, hỗ 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.

Ảnh tên gọi của nó chỉ rõ, kỹ thuật ATM sử dụng phương pháp truyền không đồng bộ (asynchronous) các gói 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).

Ảnh hận thức được vị trí chưa thể thay thế được (ít nhất cho đến những năm đầu của thế kỷ 21) của kỹ thuật ATM, hầu hết các hãng không lò về máy tính và truyền thông như IBM, AT&T, Digital, Hewlett - Packard, Cisco Systems, Cabletron, Bayetwork,... 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 router, Cabletron, ATM module for MMAC hub.

Ảnh hìn chung thị trường ATM sôi động do nhu cầu thực sự của các ứng dụng đa phương tiện. Sự nhập cuộc ngày một đông của các hãng sản xuất đã làm giảm đáng kể giá bán của các sản phẩm loại này, từ đó càng mở rộng thêm thị trường. Ảnh gay 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 Apple 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 Apple-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 Apple-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 Apple-NetWare được thiết kế như một hệ thống mạng *client-server* trong đó các máy tính được chia thành hai loại:

- Ở hững máy tênh 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 Apple-Netware không chạy DOS mà bản thân Apple-Netware là một hệ điều hành cho server điều đó đã giải phóng Apple-Netware ra khỏi những hạn chế của DOS. Server của Apple-Netware dùng một cấu trúc hiệu quả hơn DOS để tổ chức các tập tin và thư mục, với Apple-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 Apple-Netware có tên chữ không phải là chữ cái. Tuy nhiên, để truy cập một tập đĩa của Apple-Netware từ một trạm làm việc chạy DOS, một chữ cái được gán cho tập đĩa.

Với các hệ điều hành Apple-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 của Workstation, tuy điều đó tồn 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 Apple-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 rời nhau hoàn toàn.

Các trạm làm việc trên một mạng Apple-Netware có thể là các máy tính DOS, chạy OS/2 hoặc các máy Macintosh. Ở đâu mạng vừa có máy PC và Macintosh thì Apple-Netware có thể là sự lựa chọn tốt.

Tất cả các phiên bản của Apple-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.

Apple-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 saùn

các dịch vụ dành cho người sử dụng. Tại đây à ovell à etWare có một hệ thống các yêu cầu và trả lời mà Client và Server đều hiểu, nó bao gồm:

- à hóm chương trình trên máy người dùng: Hệ điều hành trạm, các giao diện cho phép nhười sử dụng chi xuất các tài nguyên của mạng như là các tài nguyên của máy cục bộ, chương trình truyền số liệu qua mạng.
- Hệ điều hành trên máy máy chủ: Chương trình thực hiên từ DOS, Lưu các thông số của DOS, chuyển CPU của server qua chế độ protected 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.
- à ovell à etWare hỗ trợ các giao thức cơ bản sau:
 - Giao thức truy xuất (Access Protocol) (Ethernet, Token Ring, ARCnet, Pro à ET-10, FDDI)
 - Giao thức trao đổi gói tin trên mạng (Internet Packet Exchange -IPX)
 - Giao thức thông tin tìm đường (Routing Information Protocol - RIP)
 - Giao thức thông báo dịch vụ (Sevice Advertising Protocol - SAP)
 - Giao thức nhân à etWare (à etWare Core Protocol - à CP) cho phép người dùng truy xuất vào file server

Do nhu cầu cần thích nghi với nhiều kiểu mạng và để dễ dàng nâng cấp và quản lý, à ovell à etWare cũng được chia thành nhiều tầng giao thức tương tự cấu trúc 7 tầng của hệ thống mở OSI.

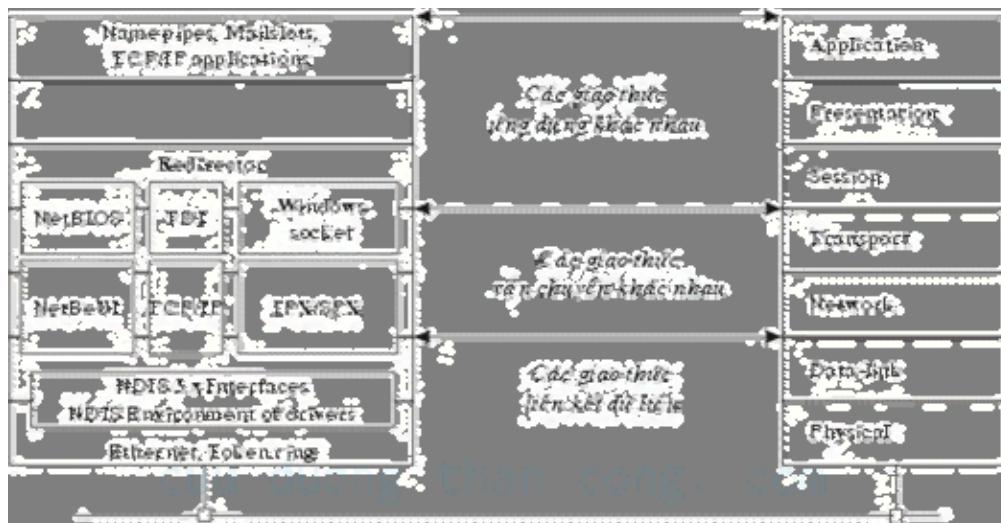
Tầng ứng dụng (Application)	Giao thức thông báo dịch vụ (Service advertising protocol - SAP)	Giao thức thông tìm đường (Routing Information Protocol - RIP)	Giao thức nhân NetWare (NetWare core protocol - NCP)
Tầng trình bày (Presentation)	Hệ thống nhà p xuất cơ bản trên mạng (NetBIOS)		
Tầng giao dịch (Session)	Trao đổi gói tin tuân tu (Sequence Packet Exchange -SPX)		
Tầng mạng (Network)	Trao đổi gói tin tuân tu (Internet Packet Exchange - IPX)		
Tầng liên kết dữ liệu (Data link)	Giao thức truy xuất và kỹ thuật mạng lưới (Access protocol and wiring techniques) (Chuẩn giao tiếp liên kết dữ liệu mở ODI)		
Tầng vật lý (Physical)	Ethernet, Token Ring, ARCnet cáp đồng trục, cáp tròn xoắn cáp (IEEE 802.X hoặc FDDI)		

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 nay Windows NT đang được đánh giá cao và được đưa 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 cung cấp 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 chạy trên máy có một CPU cũng như nhiều CPU. Hệ điều hành mạng còn có đưa vào kỹ thuật giao tiếp 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

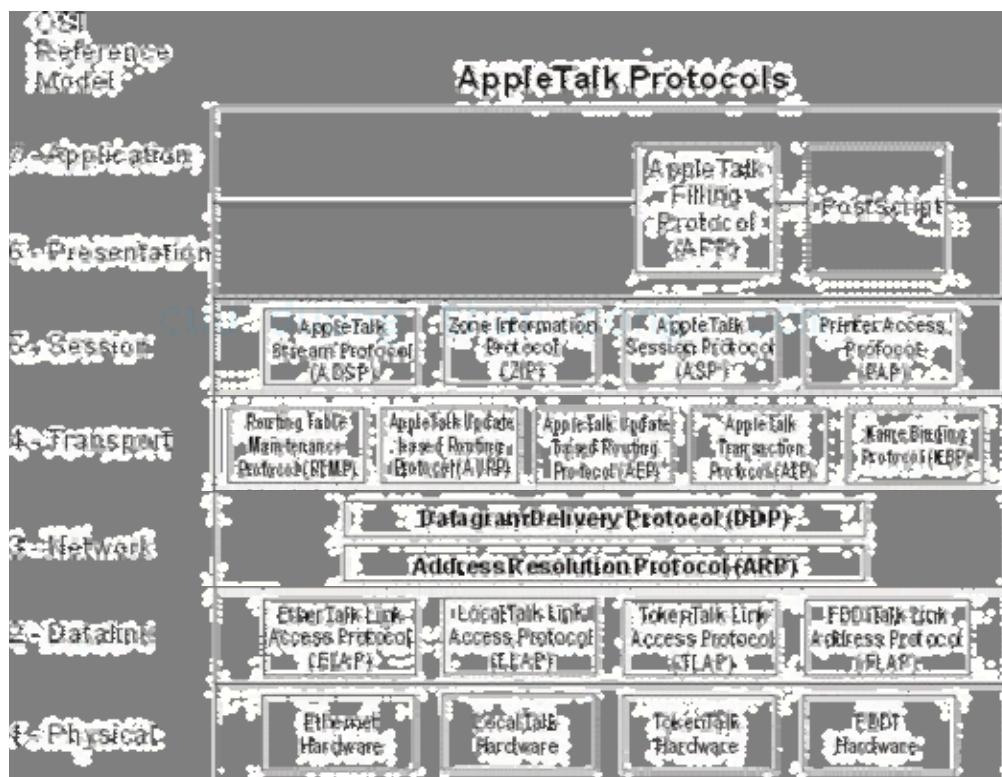
III. Mạng Apple talk

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 Apple, 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 Address 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 mỗi 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 giao thức IPX/SPX.

• **NBP** (*Naming Binding Protocol*): cho phép định danh các thiết bị bởi các tên logic (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 tầng vận chuyển hoạt động với phương thức không liên kết. Dịch vụ vận chuyển này được cung cấp thông qua một hệ thống các thông báo nhận và truyền lại. Độ tin cậy của ATP dựa trên các thao tác (transaction) (một thao tác bao gồm một cặp các thao tác hỏi-đáp).

• **ASP** (*AppleTalk Session 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 Filing 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. Ở hững mạng sử dụng đường điện thoại thông thường vào lúc đó tỏ ra không đủ an toàn khi mà một đường dây hay một tổng đài bị phá hủy cũng có thể dẫn đến mọi cuộc nói chuyện hay liên lạc thông qua nó bị gián đoạn, việc đó còn đôi khi dẫn đến cắt rời liên lạc.

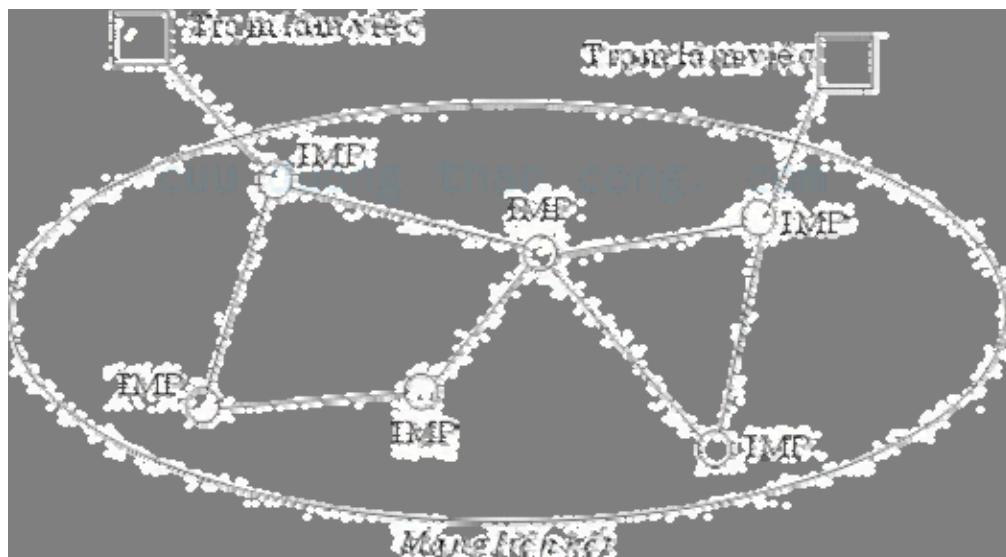
Để làm được điều này khi bộ quốc phòng Mỹ đưa ra chương trình ARPA (Advanced Research Projects Agency) với sự tham gia của nhiều trường đại học và công ty dưới sự quản lý của khi bộ quốc phòng Mỹ.

Vào đầu những năm 1960 những ý tưởng chủ yếu của chuyển mạch gói đã được Paul Baran công bố và sau khi tham khảo nhiều chuyên gia thì chương trình ARPA quyết định mạng tương lai của khi bộ quốc phòng Mỹ sẽ là mạng chuyển mạch gói và nó bao gồm một mạng liên kết và các trạm (host). Mạng liên kết bao gồm các máy tính dùng để liên kết các đường truyền dữ liệu được gọi là các điểm trung chuyển thông 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 BB&T một hãng tư vấn tại Cambridge, Massachusetts làm tổng thầu. Lúc đó BB&T đã lựa chọn 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 ARPA⁴ ET bắt đầu được đưa vào hoạt động thử nghiệm với 4 nút là những trường đại học và trung tâm nghiên cứu tham gia chính vào dự án, mạng phát triển rất nhanh đến tháng 3 năm 1971 đã có 15 nút và tháng 9 năm 1972 đã có tới 35 nút. Các cải tiến tiếp theo cho phép nhiều trạm có thể liên kết với một IMP do vậy sẽ tiết kiệm tài nguyên và một trạm có thể liên kết với nhiều IMP nhằm tránh việc IMP hư hỏng làm gián đoạn liên lạc.

Cùng với việc phát triển các nút ARPA cũng dành ngân khoản cho phát triển các mạng truyền dữ liệu dùng kỹ thuật vệ tinh và dùng kỹ thuật radio. Điều đó cho phép thiết lập các nút tại những điểm cách xa nhau. 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 BB⁵ 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 sở hệ điều hành U⁶ IX. Dựa trên các phần mềm mới về truyền thông trên cơ sở TCP/IP đã cho phép dễ dàng liên kết các mạng LA⁷ vào mạng ARPA⁸ ET. Vào năm 1983 khi mạng đã hoạt động ổn định thì phần quốc phòng của mạng (gồm khoảng 160 IMP với 110 IMP tại nước Mỹ và 50 IMP ở nước ngoài, hàng trăm nút) được tách ra thành mạng MIL⁹ ET và phần còn lại vẫn tiếp tục hoạt động như là một mạng nghiên cứu.

Trong những năm 1980 khi có nhiều mạng LA¹⁰ được nối vào ARPA¹¹ ET để giảm việc tìm kiếm địa chỉ trên mạng người ta chia vùng các máy tính đưa tên các máy vào địa chỉ IP và xây dựng hệ quản trị cơ sở phân tán các tên các trạm của mạng Hệ cơ sở dữ liệu đó gọi là D¹² S (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 ARPA¹³ ET là khởi xướng thì ARPA¹⁴ ET đã kết thúc hoạt động của mình, tuy nhiên MIL¹⁵ ET vẫn hoạt động cho đến ngày nay.

V. Mạng NFSNET

Vào cuối những năm 1970 khi Quỹ khoa học quốc gia Hoa Kỳ (the U.S. National Science Foundation) thấy được sự thu hút của ARPA¹⁶ ET trong nghiên cứu khoa học mà qua đó các nhà khoa học có thể chia sẻ thông tin hay cùng nhau nghiên cứu các đề án. Tuy nhiên việc sử dụng ARPA¹⁷ ET cần thông qua bộ quốc phòng Mỹ với nhiều hạn chế và nhiều cơ sở nghiên cứu khoa học không có khả năng đó. Điều đó khiến FS¹⁸ thiết lập một mạng ảo có tên là CS¹⁹ ET trong đó sử dụng các máy tính tại công ty BB²⁰ cho phép các nhà nghiên cứu có thể kết nối vào để tiếp tục nối với mạng ARPA²¹ ET hay gửi thư điện tử cho nhau. Vào năm 1984 FS²² 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 ARPA²³ ET, bước đầu FS²⁴ quyết định xây dựng được đường trực tuyến 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 ARPA²⁵ ET. Đồng thời FS²⁶ 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 trực và các mạng vùng được gọi là FS²⁷ ET, mạng FS²⁸ có được kết nối với mạng ARPA²⁹ ET.

Mạng à FS được phát triển rất nhanh, sau một thời gian hoạt động đường trực 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 trực đã được nâng lên đến 1.5 Mbps.

Với việc phát triển rất nhanh và à FS thấy rằng chính quyền không có khả năng tiếp tục tài trợ nhưng do các công ty kinh doanh không thể sử dụng mạng à FS à ET (do bị cấm theo luật) nên à FS yểm trợ các công ty MERIT, MCI, IBM thành lập một công ty không sinh lợi (nonprofit corporation) có tên là Aà S (Advanced à etworks and Services) nhằm phát triển việc kinh doanh hóa mạng. Aà S tiếp nhận mạng à FS à ET và bắt đầu nâng cấp đường trực lên từ 1.5 Mbps lên 45 Mbps để thành lập mạng Aà S à ET.

Vào năm 1995 khi các công ty cung cấp dịch vụ liên kết phát triển khắp nơi thì mạng trực Aà S à ET không còn cần thiết nữa và Aà S à ET được bán cho công ty America Online. Hiện nay các mạng vùng của à FS mua các dịch vụ truyền dữ liệu để liên kết với nhau, mạng à FS đang sử dụng dịch vụ của 4 mạng truyền dữ liệu là PacBell, Ameritech, MFS, Sprint mà qua đó các mạng vùng à FS có thể lựa chọn để kết nối với nhau.

VI. Mạng Internet

Cùng với sự phát triển của à FS à ET và ARPA à ET nhất là khi giao thức TCP/IP đã trở thành giao thức chính thức duy nhất trên các mạng trên thì số lượng các mạng, nút muôn 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 Á.

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 SPA à , à ASA network, HEP à ET, BIT à ET, IBM network, EAR à . 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 ARPA à ET mới được thiết lập, nó cho phép gửi và nhận thư điện tử cho mọi thành viên khác trong mạng.

- **Thông tin mới** (news): Các ván 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 diễn 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 vị nằm trong máy chủ. Đây là dịch vụ đang mang lại sức thu hút 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.

cuu duong than cong. com

cuu duong than cong. com

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, etWare lite của Novell, Windows (for Workgroup, 95, LAN 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 etware, LAN Manager của Microsoft, Windows LAN 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 LAN là hệ điều hành mạng cao cấp của hãng Microsoft. Phiên bản đầu có tên là Windows LAN 3.1 phát hành năm 1993, và phiên bản server là Windows LAN Advanced Server (trước đó là LAN Manager for LAN). Năm 1994 phiên bản Windows LAN Server và Windows LAN 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 LAN Workstation và Windows LAN 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 LAN 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 LAN.

Windows LAN có hai bản mà nó đi đôi với hai cách tiếp cận mạng khác nhau. Hai bản này gọi là Windows LAN Workstation và Windows LAN server. Với hệ điều hành chuẩn của LAN 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. Cá hai bản Windows à T station và Windows à T server cùng được xây dựng trên cơ sở nhân à T chung và các giao diện và cả hai cùng có những đặc trưng an toàn theo tiêu chuẩn C2. Windows à T Wordstation được sử dụng để kết nối những nhóm người sử dụng nhỏ, thường cùng làm việc trong một văn phòng. Tuy nhiên với Windows à T server ta có được một khả năng chống hỏng hóc cao, những khả năng cung cấp dịch vụ mạng lớn và những lựa chọn kết nối khác nhau, Windows à T Server không hạn chế về số người có thể thâm nhập vào mạng.

Với Windows 9x 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. Đó thích hợp với tất cả các sơ đồ mạng BUS, STAR, RIêng G và hỗn hợp.

Windows 3.1 là hệ điều hành có sức mạnh công nghiệp đầu tiên cho số lượng khổng lồ các máy tính IBM compatible. Windows 3.1 là một hệ điều hành thực sự dành cho người sử dụng, các cơ quan, các công ty xí nghiệp. Windows 3.1 là một hệ điều hành đa nhiệm, đa xử lý với địa chỉ 32 bit bộ nhớ. 3.1 hỗ trợ các ứng dụng DOS, Windows, Win32 GUI và các ứng dụng dựa trên ký tự. Windows 3.1 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:

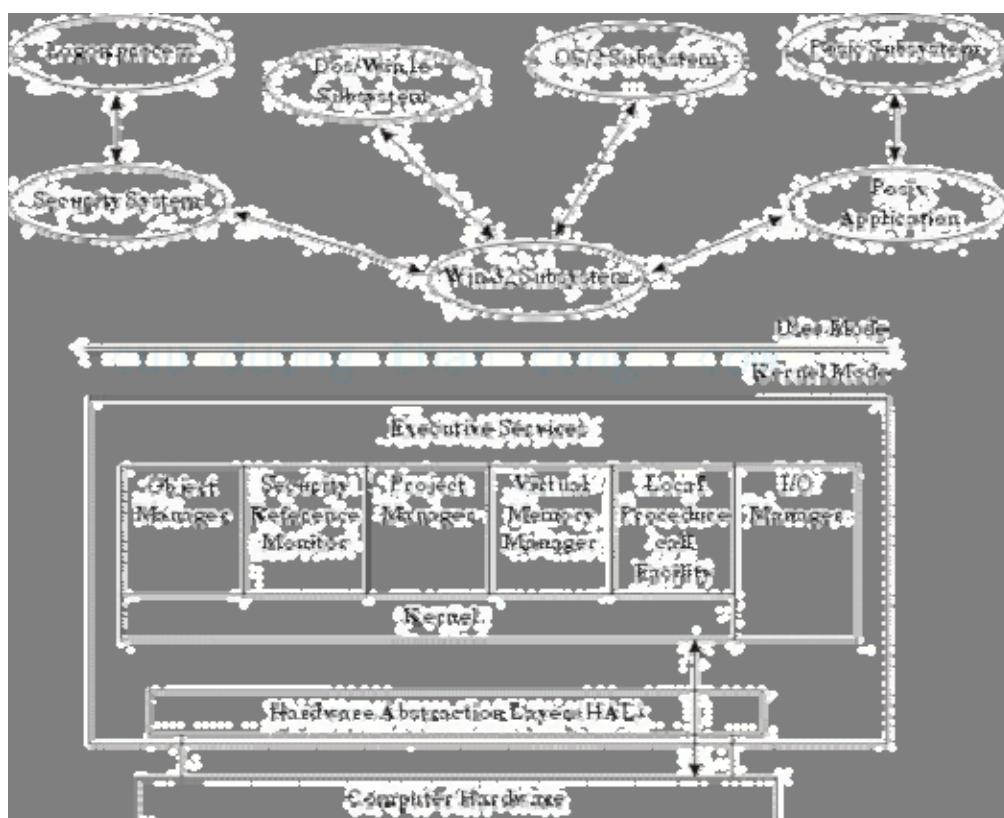
- Là hệ điều hành mạng đáp ứng tất cả các giao thức truyền thông phổ dụng nhất. Ngoài ra nó vừa cho phép giao lưu giữa các máy trong mạng, vừa cho phép truy nhập từ xa, cho phép truyền file v.v... Windows AT là hệ điều hành vừa đáp ứng cho mạng cục bộ (LAN) vừa đáp ứng cho mạng diện rộng (WAN) như Intranet, Internet.
 - Windows AT server hơn hẳn các hệ điều hành khác bởi tính mềm dẻo, đa dạng trong quản lý. AT vừa cho phép quản lý mạng theo mô hình mạng phân biệt (Client/Server), vừa cho phép quản lý theo mô hình mạng ngang hàng (peer to peer).
 - Windows AT server đáp ứng tốt nhất các dịch vụ viễn thông, một dịch vụ được sử dụng rộng rãi trong tương lai.
 - Windows AT 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 phục 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 AT server.

III. Cấu trúc của hệ điều hành Windows NT

Windows NT được thiết kế sử dụng cách tiếp cận theo đơn thê (modular). Các đơn thê 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 Abstraction 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 phần nhỏ trong cốt lõi của hệ điều hành, cũng như bộ quản lý ảo / 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 trùu tượng của một tài nguyên. Ở 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 AT 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 AT :

- Đối tượng Directory (thư mục).
- Đối tượng File (tập tin).
- Đối tượng kiểu object.
- Đối tượng Process (tiến trình).

- Đổi tượng thread (luồng).
- Đổi tượng Section and segment (mô tả bộ nhớ).
- Đổi tượng Port (cổng).
- Đổi tượng Semaphore và biến cờ.
- Đổi tượng liên kết Symbolic (ký hiệu).

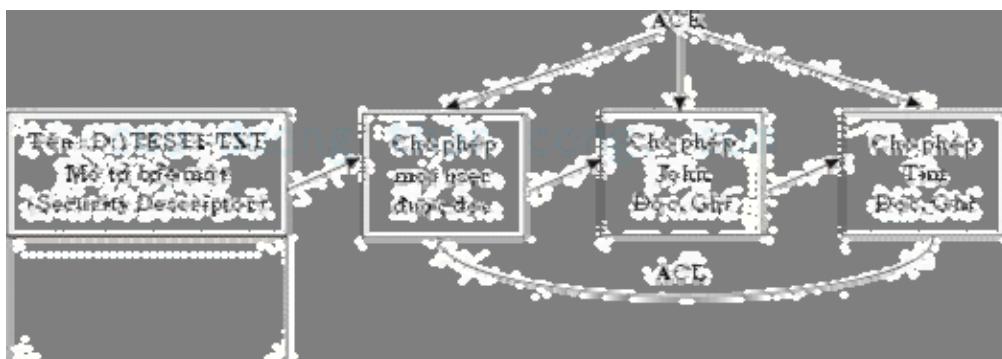
2. Cơ chế bảo mật (SRM - Security Reference Monitor):

Được sử dụng để thực hiện vấn đề an ninh trong hệ thống Windows Ả T. Các yêu cầu tạo một đổi tượng phải được chuyển qua SRM để quyết định việc truy cập tài nguyên được cho phép hay không. SRM làm việc với hệ thống con bảo mật trong chế độ user. Hệ thống con này được sử dụng để xác nhận user login vào hệ thống Windows Ả T.

Để kiểm soát việc truy cập, mỗi đổi tượng Windows Ả T có một danh sách an toàn (Access Control List - ACL). Danh sách an toàn của mỗi đổi tượng gồm những phần tử riêng biệt gọi là Access Control Entry (ACE). Mỗi ACE chứa một SecurityID (SID: số hiệu an toàn) của người sử dụng hoặc nhóm. Một SID là một số bên trong sử dụng với máy tính Windows Ả T mô tả một người sử dụng hoặc một nhóm duy nhất giữa các máy tính Windows Ả T.

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 Ả T, sau khi việc nhận dạng thành công, một Security Access Token (SAT) được tạo cho người dùng đó. SAT chứa SID của người dùng và SID của tất cả các nhóm người dùng thuộc mạng Windows Ả T. Sau đó SAT hoạt động như một "passcard" (thẻ chuyền) 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 đổi tượng, Security Reference Monitor kiểm tra bộ mô tả bảo mật của đổi 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.



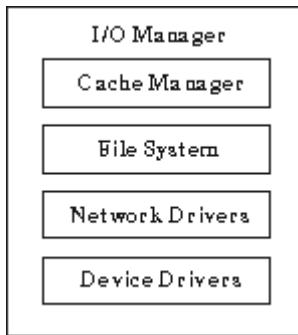
Hình 10.2: Ví dụ về danh sách an toàn (Access Control List).

3. Quản lý nhập / xuất (I/O Manager) :

Chịu trách nhiệm cho toàn bộ các chức năng nhập / xuất trong hệ điều hành Windows là T. I/O Manager liên lạc với trình điều khiển của các thiết bị khác nhau.

4. I/O Manager:

Sử dụng một kiến trúc lớp cho các trình điều khiển. Mỗi bộ phận điều khiển trong lớp này thực hiện một chức năng được xác định rõ. Phương pháp tiếp cận này cho phép một thành phần điều khiển được thay thế dễ dàng mà không ảnh hưởng phần còn lại của các bộ phận điều khiển.



Hình 10.3:Các trình điều khiển thiết bị theo lớp của I / O Manager

V. Các cơ chế bảo vệ dữ liệu trong Windows NT

Cơ chế bảo vệ dữ liệu của Windows là T gọi là fault tolerance, nó cho phép hệ thống khả năng tiếp tục làm việc và bảo toàn dữ liệu của hệ thống trong trường hợp một phần của hệ thống có sự cố hỏng hóc sai lệch. Trong Windows là T cơ chế fault tolerance bao gồm các biện pháp sau:

- Chống cúp điện bất thường.
- Cung cấp khả năng bảo vệ hệ thống đĩa (fault tolerance disk subsystem).
- Cung cấp khả năng sao chép dự phòng (backup) từ băng từ.

Khả năng bảo vệ hệ thống đĩa của Windows là T là RAID 0 (viết tắt của Redundant Array of Inexpensive disk). 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. Ở mức này tốt hơn biện pháp dùng ở 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. Ở gười ta thường dùng mức này để truy nhập vào một số ít file có dung tích lớn.

• **Mức 4:** Mức này sử dụng biện pháp giống ở mức 2 và 3 nhưng bằng phương pháp phân chia đĩa thành các khối lớn. Giống như mức 3 tất cả các mã sửa sai (error correction code) được hgi vào một đĩa và tách khỏi 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 mức 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) tương tự như disk mirroring chỉ khác là chúng dùng 2 disk controler. Điều này cho thêm khả 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. Ở đâu 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 riêng. 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 yêu 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 muôn 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 chọn công việc cần 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 saun 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

Ở hư 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, vẫn đề cần phải giải quyết là là giúp người sử dụng xác định được các tài nguyên có saun 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 muôn 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 trực 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 vẫn 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 quy 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.

Ở gười quản trị mạng chỉ cần thực hiện công việc của mình tại một trạm trên mạng mặc dù các điểm nút của nó có thể nằm trên cả thế giới. Hệ điều hành Netware 4.x cung cấp dịch vụ nổi tiếng 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 DS được đặt trong một hệ thống cơ sở dữ liệu đồng bộ, rộng khắp được gọi là DIB (Data Information Base). Cơ sở dữ liệu trên quản lý các dữ liệu dưới dạng các đối tượng phân biệt trên toàn mạng. Các định nghĩa đối tượng sẽ được đặt trên các tập tin riêng của một số máy chủ đặc biệt, mỗi đối tượng có các tính chất và giá trị của mỗi tính chất. Đối tượng bao hàm tất cả những gì có tên phân biệt như ở gười sử dụng, File server, Print server, group. Mỗi loại đối tượng có những tính chất khác nhau ví dụ như đối tượng ở gười sử dụng có tính chất về nhóm mà người sử dụng đó thuộc, còn nhóm có các tính chất về người sử dụng mà nhóm đó chứa.

Việc thiết lập các dịch vụ như vậy cần được lập kế hoạch, thiết kế rất cẩn thận, liên quan đến tất cả các đơn vị phòng ban có liên quan. Loại mạng này có khuyết điểm là việc thiết kế, thiết lập mạng rất phức tạp, mất nhiều thời gian nên không thích hợp cho các mạng nhỏ.

 **3. Quản lý theo nhóm (Workgroup)**

Các nhóm làm việc làm việc theo ý tưởng ngược lại với các dịch vụ thư mục. 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). Ở người sử dụng 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 sẵn 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.

Ở mạng workgroup cũng có điểm là đơn giản, tiện lợi và chia sẻ 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 sẵn trên mạng làm cho các người sử dụng khó xác định chúng để khai thác.
- Ở 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 Windows for Workgroups, LanManager, LANtastic, LAN Manager... 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). Ở 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. Ở 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 à T Server trên mạng. Một máy tính Windows à T có thể thuộc vào một workgroup hoặc một domain, nhưng không thể đồng thời thuộc cả hai. Mô hình domain được thiết lập cho các mạng lớn với khả năng kết nối các mạng toàn xí nghiệp hay liên kết các kết nối mạng với các mạng khác và những công cụ cần thiết để điều hành.

Việc nhóm những người sử dụng mạng và tài nguyên trên mạng thành domain có lợi ích sau:

- Mã số của người sử dụng được quản lý tập trung ở một nơi trong một cơ sở dữ liệu của máy chủ, do vậy quản lý chặt chẽ hơn.
- Các nguồn tài nguyên cục bộ được nhóm vào trong một domain nên dễ khai thác hơn.

Quản lý theo Workgroup và domain là hai mô hình mà Windows NT lựa chọn. Sự khác nhau căn bản giữa Workgroup và domain là trong một domain phải có ít nhất một máy chủ (máy chủ) và tài nguyên người sử dụng phải được quản lý bởi máy chủ đó.

II. Hệ thống quản lý trên Hệ điều hành mạng Windows NT Server

Windows à T cung cấp những chức năng tuân theo chuẩn C2 (chuẩn về an toàn quốc tế) trong đó Windows à T đảm bảo tránh được những người không được phép vào trong hệ thống hoặc thâm nhập vào các file và chương trình trên đĩa cứng. à gười ta không thể thâm nhập vào được nếu không có mật khẩu đúng. và qua đó đã bảo vệ được các file. Windows à T cung cấp công cụ để xây dựng các lớp quyền dành cho nhiều nhiệm vụ khác nhau nhằm xây dựng hệ thống an toàn một cách mềm dẻo.

à hiều người sử dụng có thể có quyền vào một máy chủ Windows à T. Một tài khoản của người sử dụng trên máy bao gồm tên, mật khẩu và nhiều tính chất được cho bởi người quản trị mạng. à gười sử dụng có thể che các thư mục hay file của mình từ những người khác và cài đặt các thông số của File manager, Program 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. à êu 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 à T tổ chức theo mô hình Workgroup cần phải đăng ký:

- Tên vào mạng
- Mật khẩu vào mạng

Dựa vào tên và mật khẩu đã cho, Windows à T cung cấp cho người một số gọi là mã số của người sử dụng (user account). Mã số này được lưu trữ 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. Ai gõ 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 và T server, nó là hạt nhân để tổ chức các mạng có quy mô lớn.

Mỗi người tham gia trong Domain cần phải đăng ký thông tin sau:

- Tên Domain
- Tên người sử dụng
- Mật khẩu

Các thông tin này được lưu ở máy chủ dưới dạng một mã số, gọi là tài khoản người sử dụng (user account) và các mã số của 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 và T mà không tham gia vào một Domain có nhược điểm sau:

- Máy trạm chỉ có thể cung cấp các mã số được tạo ra trên nó. Nếu máy này bị 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 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 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.

- Ở 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.

Ở gười quản trị Domain chỉ cần tạo tài khoản người sử dụng (user account) chỉ một lần trên máy Primary Domain Controller, thông tin được tự động copy đến các máy Backup Domain Controller.

3. Mô hình quan hệ giữa các Domain trong mạng Windows NT

Trong một mạng có thể có nhiều Domain nhưng một máy tính Windows ở T là thành viên của chỉ một domain tại mỗi thời điểm. Tuy nhiên, có một vài trường hợp đôi khi chúng ta cần truy cập tài nguyên trong những domain khác, để là được điều này hệ điều hành Windows ở T server cho phép giữa các Domain có thể tồn tại một quan hệ gọi là quan hệ tin cậy (trust relationship). Chúng ta có thể sử dụng quan hệ tin cậy giữa các Domain cho phép người dùng trên một Domain truy cập tài nguyên trong Domain khác.

Hai Domain A, B gọi là quan hệ tin cậy (trust relationship) mà trong đó Domain A tin cậy Domain B nếu giữa chúng có một mối liên kết sao cho người khai thác mạng của Domain B có thể truy nhập vào Domain A từ một máy trạm trong Domain B.

Từ góc độ của người quản trị mạng mục đích của việc thiết lập quan hệ tin cậy giữa các Domain là làm cho việc quản lý mạng trở lên đơn giản hơn bằng cách kết hợp các Domain vào một đơn vị quản lý. Trong quan hệ tin cậy các Domain được chia ra như sau:

- Domain được tin cậy (trusted domain)
- Domain tin cậy (trusting domain)

Một Domain là loại này hoặc loại kia *thông thường* phụ thuộc vào nó chứa mã số của người sử dụng (người sử dụng account) hay chỉ chứa tài nguyên (resource).

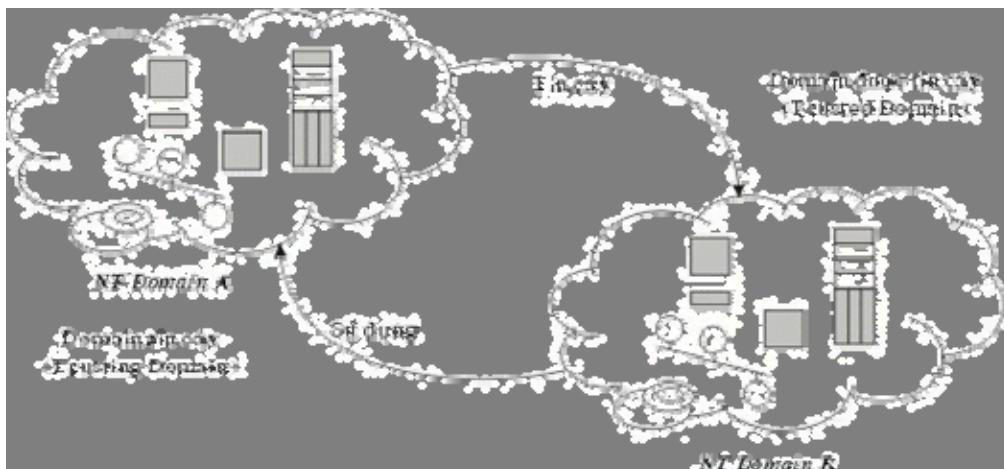
- Domain tin cậy (trusting domain) là Domain chứa tài nguyên.
- Domain được tin cậy (trusted domain) là Domain chứa mã số người sử dụng.

Khi người sử dụng truy nhập từ một máy trạm trong Domain tin cậy (trusting domain) vào Domain được tin cậy (trusted domain) thì quá trình kiểm soát diễn ra như sau:

- Ở gười sử dụng phải cho mã số (mã số này ứng với tên, mật khẩu, tên domain cần truy nhập)
- Mã số được chuyển về máy chủ của Domain tin cậy.
- Máy chủ của Domain tin cậy chuyển mã số này sang Domain được tin cậy.
- Kết quả kiểm tra của máy chủ trong Domain được tin cậy diễn ra theo quá trình ngược lại.

Ở đây chúng ta chú ý:

- Việc liên kết giữa các Domain không có tính bắc cầu.
- Thông qua việc thiết lập mối quan hệ tin tưởng, chúng ta có thể sử dụng một tài khoản để truy xuất đến nhiều tài nguyên của nhiều Domain. Có thể quản trị nhiều Domain từ một vị trí tập trung.



Hình 11.1: Mô hình tin cậy của các Domain trong mạng Windows NT

4. Nhóm (group) trong Windows NT

Trong mạng Windows 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 được xác định, và thấy được từ bất kỳ máy tính nào trong vùng đó. Quyền có thể được gán cho nhóm toàn cục cho các tài nguyên trên một máy Server hay 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.

Để hóm toàn cục có những đặc trưng sau:

- Thành viên của nhóm phải là các người sử dụng của domain (domain user account).
- Để hóm toàn cục có thể được gán quyền cho tài nguyên bất kỳ trong vùng mà chúng được xác định.
- Để hóm toàn cục có thể được gán quyền đến các tài nguyên trong vùng khác với vùng chúng được xác định khi quan hệ tin cậy (trust relationship) giữa các vùng có hiệu lực.
- Các thành viên của nhóm toàn cục có thể sử dụng nguồn tài nguyên trong vùng bất kỳ mà nhóm toàn cục có quyền.
- Để hóm toàn cục chỉ chứa mã số của người sử dụng trong Domain của nó. Để không thể chứa các nhóm cục bộ và nhóm toàn cục khác.

6. Nhóm cục bộ (local group)

Để hóm cục bộ, trái lại, được gán quyền cho nguồn tài nguyên trên máy để T mà nó được xác định. Để máy để T là một phần của vùng, thì để tiện cho việc gán quyền, một nhóm cục bộ có thể chứa các tài khoản người dùng cấp vùng (domain user account) và các nhóm toàn cục trong Domain đó, nơi máy tính để T là thành viên, hoặc những người dùng từ Domain được tin cậy. Các người dùng cấp vùng (domain user) có thể được gán quyền truy cập đến tài nguyên bất kỳ trong Domain đó.

Để Windows để T computer không nối với mạng thì các thành viên trong local group có thể được gán quyền để truy xuất đến tài nguyên trên máy tính mà trong đó các thành viên được tạo ra còn nếu Windows để T computer nối vào mạng thì để tiện lợi cho việc phân quyền thì người quản trị mạng có thể đưa global group và domain user vào trong local group .

Có hai loại nhóm cục bộ: **nhóm cục bộ trạm làm việc (workstation local group)** và **nhóm cục bộ vùng (domain local group)**. Một mạng làm việc theo cơ chế vùng bao gồm cả Windows để T Server và Windows để T Workstation việc hiểu rõ sự khác nhau giữa hai loại nhóm cục bộ là rất quan trọng.

a. Nhóm cục bộ trạm làm việc (Workstation local group):

Để hóm cục bộ trạm làm việc hiện diện trên Windows để T Workstation trên đó chúng được tạo ra. Chúng được chứa trong dữ liệu SAM lưu trữ trên Windows để T Workstation. Một người dùng cục bộ được tạo ra bằng công cụ *User Manager* của Windows để T Workstation (khác với công cụ *User Manager for Domains* trên Windows để T Server) có thể có quan hệ thành viên chỉ trong nhóm cục bộ của trạm làm việc đó. Một nhóm cục bộ trong một trạm làm việc chỉ có thể được dùng trên máy tính trên đó nhóm được tạo ra, và không thể làm việc trên bất kỳ máy Windows để T nào khác.

à hóm cục bộ trạm làm việc có thể chứa:

- Các tài khoản người dùng cục bộ từ trạm làm việc trên đó nó được xác định.
- Các tài khoản người dùng cấp vùng (domain user account) và các nhóm toàn cục từ vùng trong đó họ được xác định.
- Các tài khoản người dùng cấp vùng (domain user account) và các nhóm toàn cục từ các vùng đã được ủy quyền.

b. Nhóm cục bộ vùng (Domain local group):

Nhóm cục bộ vùng hoạt động trên Windows à T Server ở mức vùng, và được tạo ra bằng *User Manager for Domains* (trên Windows à T Server). Các nhóm cục bộ vùng chỉ có thể hiện hữu trên máy Windows à T Server tạo ra nó. Do đó, các nhóm cục bộ vùng có thể dùng để truy cập nguồn tài nguyên trên máy tính Windows à T Server trong vùng đó, mà không dùng để truy cập nguồn tài nguyên trên máy tính Windows à T Workstation trong vùng này. à hóm cục bộ vùng không thể được gán quyền trên bộ điều khiển không có cấp vùng, thậm chí cả các máy chủ.

III. Các mô hình Domain trong mạng Windows NT

Windows à T máy chủ cung cấp 4 kiểu tổ chức domain gọi tắt là các mô hình domain (domain models). Dưới đây là 4 mô hình tổ chức của nó:

- [Mô hình domain đơn \(single domain\)](#)
- [Mô hình domain chính \(master domain\)](#)
- [Mô hình multiple master domain](#)
- [Mô hình complete trusts](#)

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 account) 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 vẫn 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 hỗ 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 (primary 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 khía 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 tắc nghẽn 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 (multiple master domain)

Mô hình **nhiều Domain chính** (multiple 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 (resource 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. Ở hòđiều 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 .

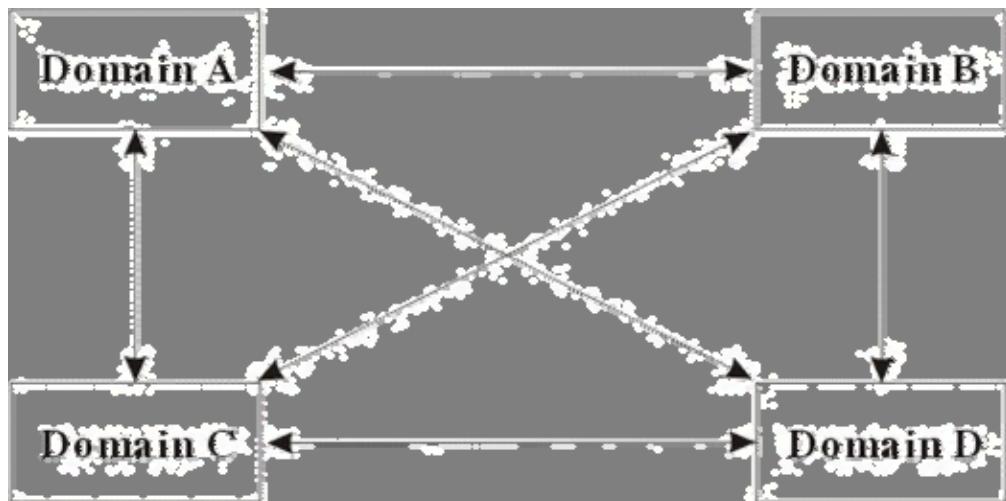


Hình 11.3: Mô hình nhiều Domain chính

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. Ở những hạn chế về domain được thảo luận ở đây nhằm mục đích giúp bạn thiết kế mạng chính xác và hoàn hảo.

- Domain Ở T đơn điệu theo nghĩa là không có cách nào diễn tả quan hệ phân cấp hoặc nhóm tài nguyên trong một vùng đơn. Ở gười dùng có thể sử dụng những quyền được ủy thác thể hiện các quan hệ giữa những vùng, nhưng đây là quan hệ sử dụng và không thích hợp cho việc tổ chức mạng dựa trên phạm vi địa lý, tài nguyên sở hữu, logic hoặc nền tảng sơ đồ tổ chức.
- Mô hình vùng Domain chính duy nhất theo Microsoft thích hợp cho các mạng ít hơn 40.000 người dùng và nhóm. Khi số người dùng và nhóm tăng lên, số quan hệ ủy quyền và chi phí quản lý quan hệ cũng tăng. Ở ói cách khác chi phí quản lý mạng có thể tăng bất thình lình khi kích thước mạng tăng.
- Ở gười dùng phải cẩn trọng về kẻ hở của quan hệ ủy quyền - đặc biệt quan hệ ủy quyền hai chiều. Ở êu 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.
- Ở goài ra có một nguy cơ thực sự sẽ xảy ra là người cài đặt mạng có thể cài đặt một mạng hoạt động tốt trong thời gian ngắn còn khi mạng hoạt động dài hạn này sẽ ù nảy sinh vấn đề về mặt chính sách là ai ủy quyền cho ai.

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 /T"

Chú ý trong trường hợp này chương trình sẽ yêu cầu chuẩn bị 3 đĩa mềm loại 1.44Mb để cài các chương trình khởi động cần thiết và trong quá trình cài đặt các đĩa mềm trên sẽ được sử dụng. 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 thiết 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	3 1/2 inch hay 5 1/4 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 "etwork 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 sẽ không được 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
Không 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), 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: Allow 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 . Allow Access là 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 NTFS , 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 . Điều 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:

- Allow Access của người dùng và các nhóm trùng nhau.
- Allow Access của một trong những quyền là Allow Access thì quyền hạn chung là Allow Access .
- Allow Access của 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 Allow Access , nó luôn được liệt kê đầu tiên trong danh sách Access Control List.

Quyền sở hữu của các tập tin: Allow Access của 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.

Allow Access của thành viên của nhóm Administrator có quyền sở hữu một tập tin thì nhóm những Administrator trở thành chủ nhân. Allow Access của người dùng không phải là thành viên của nhóm Administrator có quyền sở hữu thì chỉ người dùng đó là chủ nhân.

Allow Access của chủ nhân của tập tin có quyền điều khiển của tập tin đó và có thể 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满足 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 chưa được nén. Thông số này chỉ được sử dụng trên các partition loại ổ TFS.
- **Hidden:** Các File và các thư mục có thuộc tính này thường không xuất hiện trong các danh sách thư mục.
- **Read Only:** Các File và các thư mục có thuộc tính này sẽ không thể bị xóa hay sửa đổi.
- **System:** Các File thường được cho thuộc tính này bởi hệ điều hành hay bởi chương trình OS setup. Thuộc tính này ít khi được sửa đổi bởi người quản trị mạng hay bởi các User.
- 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 ẩn T nén sẽ xảy ra trong chế độ ngầm (background). Việc nén này làm giảm vùng không gian đĩa mà File chiếm chỗ. Có một vài thao tác chịu việc xử lý chậm vì các File nén phải được giải nén trước khi sử dụng. Tuy nhiên việc nén File thường xảy ra thường xuyên như là các File dữ liệu quá lớn mà có nhiều người dùng chia sẻ.

III. Chia sẻ Thư mục trên mạng thancong.com

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 sẻ.

Việc chia sẻ này sẽ làm việc với bảng FAT và ổ TFS file system. Để nâng cao khả năng an toàn cho việc chia sẻ, chúng ta cần phải gán các mức truy cập cho File và Thư mục.

Khi chúng ta chia sẻ một thư mục, thì chúng ta sẽ chia sẻ tất cả các File và các Thư mục con. Điều 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.

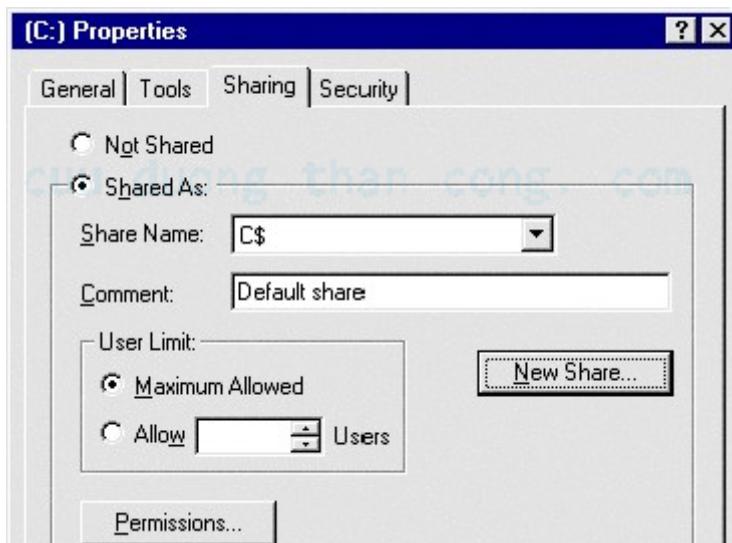
Tất cả các thủ tục chia sẻ thư mục được thực thi trong Windows ở T Explorer.

Để chia sẻ một thư mục ta phải thực hiện các bước sau:

- Right-click lên Thư mục đó trong Windows ở T Explorer. Hiện ra menu



- Click **Properties** trong Menu. Hiện ra hộp thoại sau:



- Chọn **Sharing tab** hiện ra hộp 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 gõ một con số vào hộp **Allow**

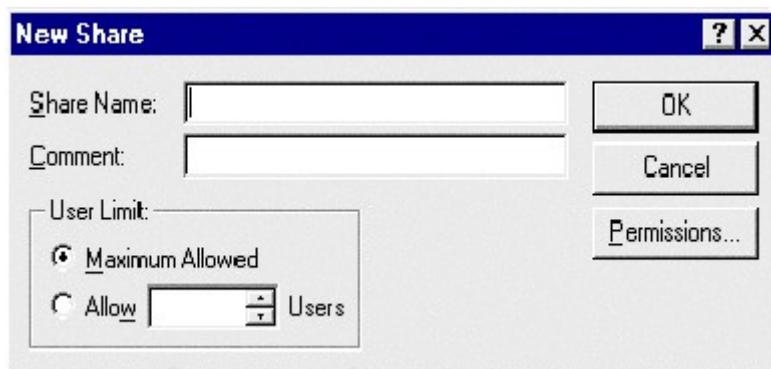
- Nếu muốn hạn chế việc truy xuất thì click **Permissions button**.

- 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.

Để 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 Explorer.
- Click **Properties** trong Menu rút gọn, hiện ra hộp thoại **Properties**
- Click **Sharing tab**.
- Click button **New Share** để tạo một sự chia sẻ mới, hiện ra hộp 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 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**.

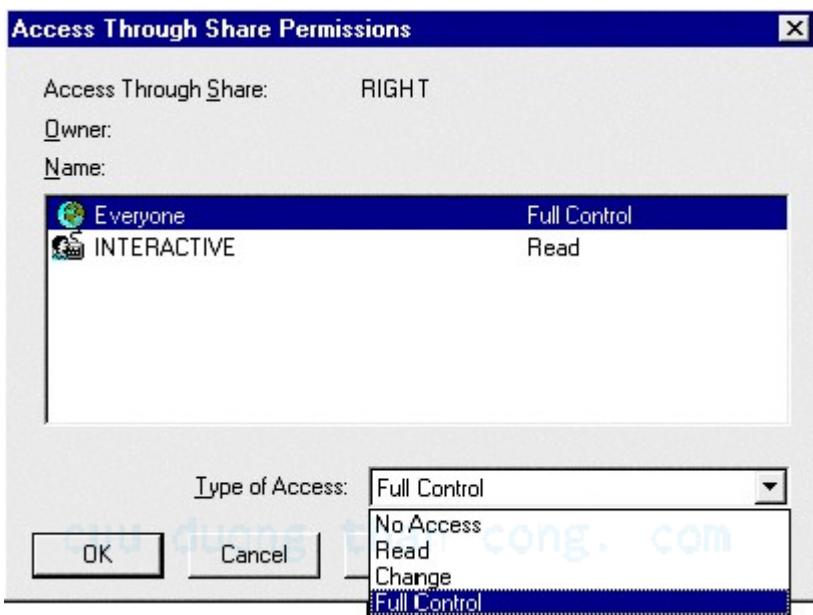
Khi chúng ta tạo một sự chia sẻ mới, quyền truy cập mặc định cho nhóm **Everyone** là đầy đủ (**Full Control**). Giả sử rằng chúng ta sẽ gán giá trị mặc định này cho quyền truy cập của thư mục và File. Khi cần thiết sẽ hạn chế việc truy xuất tới thư mục đó.

Ở đây có một vài chú ý:

- Các người sử dụng thường chỉ có 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. Ở thư mục đó nằm trong cùng thư mục chứa chương 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 họ là có đầy đủ các quyền truy cập.

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 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.

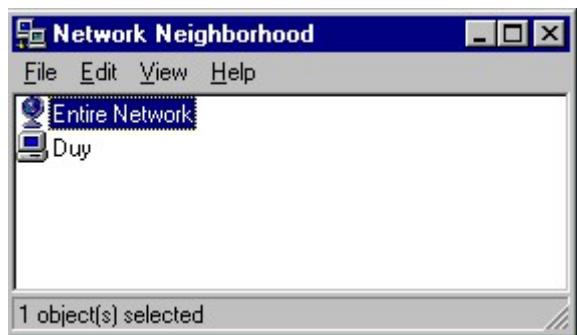
Thông qua việc chia sẻ một thư mục cho một user hay một nhóm cũng góp phần vào việc bảo đảm an toàn cho một thư mục không cho user khác hay nhóm khác truy xuất thư mục đó.

V. Sử dụng các thư mục mạng

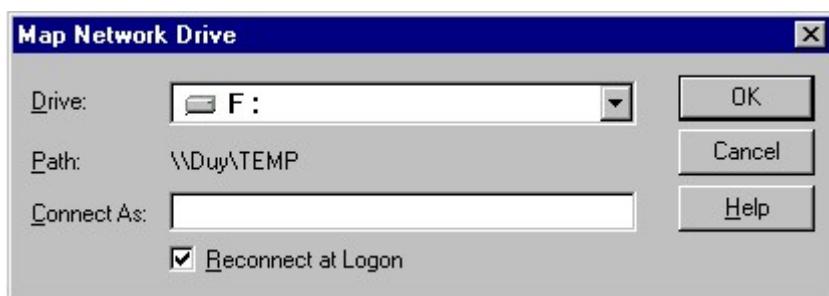
Muốn sử dụng các thư mục mạng thì trước hết thư mục đó được cho phép chia sẻ, chúng ta phải liên kết thư mục mạng đó với tên một chữ cái tương ứng như một tên đĩa mạng (E,F,G,H,I,...). Sau khi thư mục được chia sẻ đã kết nối với ký tự ổ đĩa mạng người dùng có thể truy cập thư mục được chia sẻ, các thư 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 ô địa mạng chúng muốn liên kết với thư mục chia sẻ.
 - Nếu thấy cần, chọn Path và gõ vào tên theo tổng quát U& C (Universal Addressing 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 **etwork neighborhood**.)
 - Nếu chúng ta không được quyền để truy cập vào tài nguyên chia sẻ trên nhưng trong cùng vị trí 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 chúng ta đăng nhập vào mạng.
- Chọn **OK** để lưu các thông tin trên.

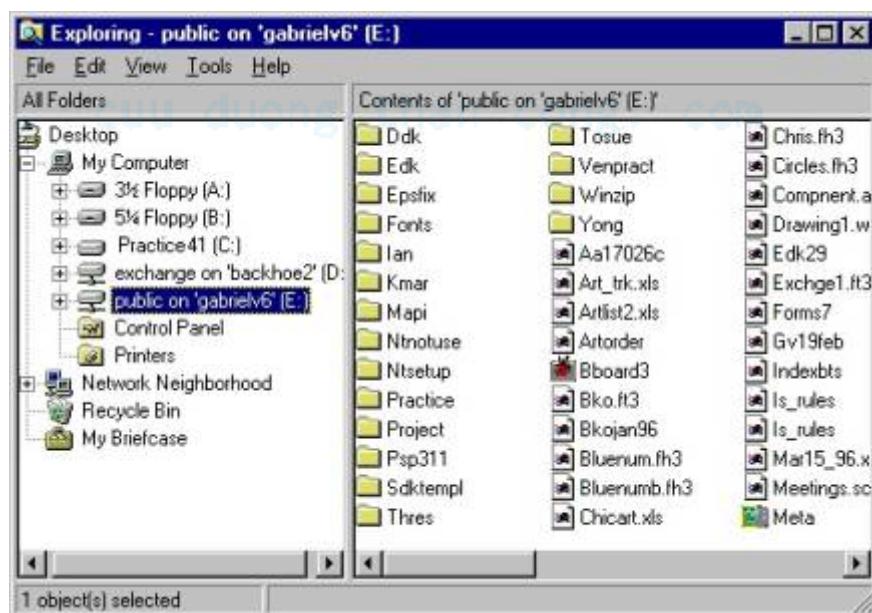
ngoài ra ta có thể dùng lệnh **NET USE** để thực hiện các công việc trên.

Lệnh **NET USE** dùng Universal Addressing Convention (U& C) để truy cập các tài nguyên dùng chung. Tên U& C bắt đầu bằng một dấu phân cách đặt biệt \, dấu này chỉ sự bắt đầu của tên U& C (tên U& C có dạng "\computer_name\share_name[sub_directory]". **NET USE** được dùng để truy cập một nguồn tài nguyên dùng chung. Lệnh **NET USE** dùng bộ hướng dẫn mạng (etwork Redirector) trên máy tính 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 cách 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 ô đĩa mạng xuất hiện và cho chúng ta khai thác.



cuu duong than cong. com

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 quản 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. Ở đó có thể quản lý máy in gắn trực tiếp vào nó hay một máy in gắn vào máy khác trên mạng.

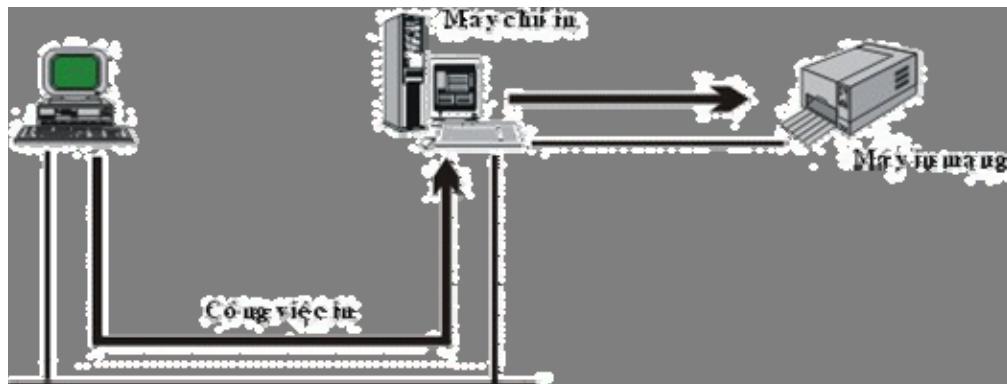
Để giải quyết những vấn đề đặt ra với công việc in trên mạng Windows NT sử dụng kỹ thuật gọi là Spooling mà chủ yếu như sau:

- 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 đợi 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 này 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.

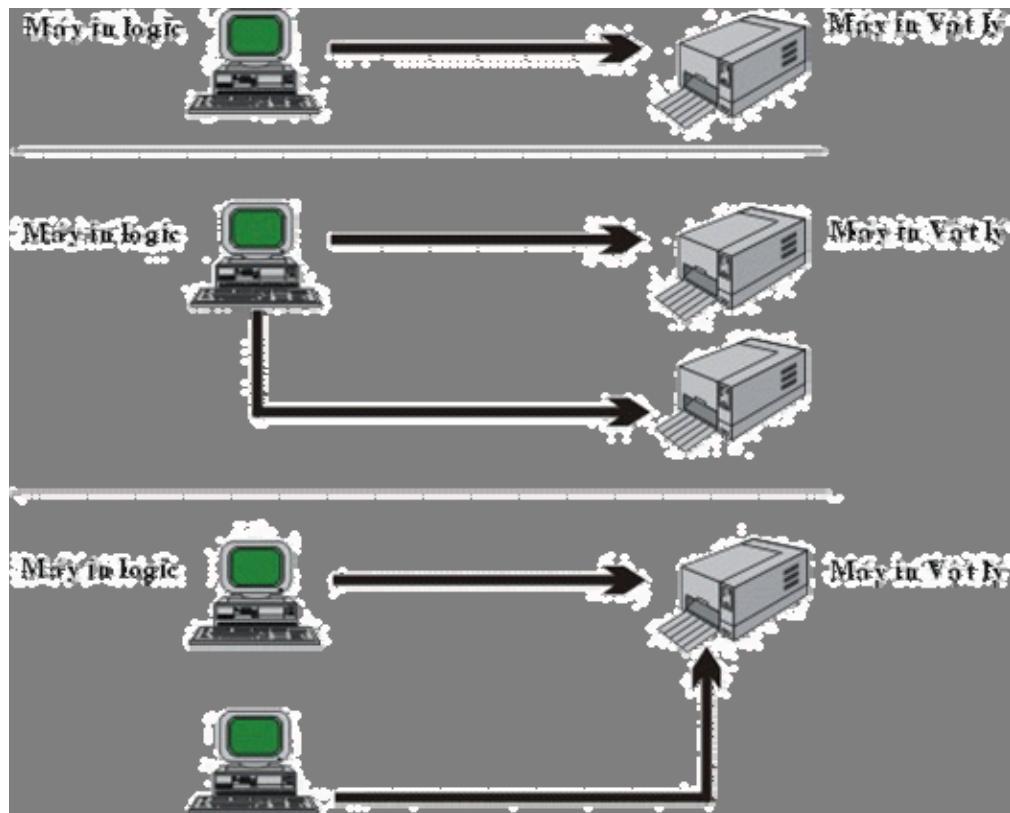
Ở gười sử dụng in ra spool thông qua việc in ra máy in logic, họ sử dụng máy in logic như là máy in đang được gắn là máy của họ nhưng thực sự các dữ liệu được in ra máy in logic được chuyển cho mạng và qua đó đến máy chủ in trước khi được đưa ra máy in mạng.



Hình 14.1: Máy chủ in và spool

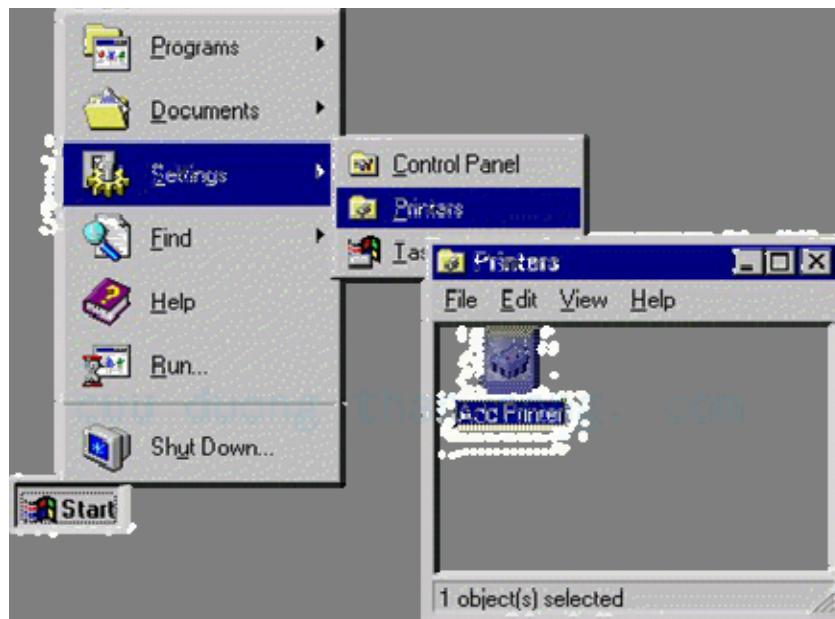
Máy chủ in sẽ liên kết các máy in logic với máy in vật lý, nó phải đảm bảo các công việc in phải được đưa đúng đến máy in vật lý. Tại đây có 3 trường hợp có thể đối với mối quan hệ giữa máy in logic và máy in vật lý

- Một máy in logic liên kết với một máy in vật lý.
- 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:

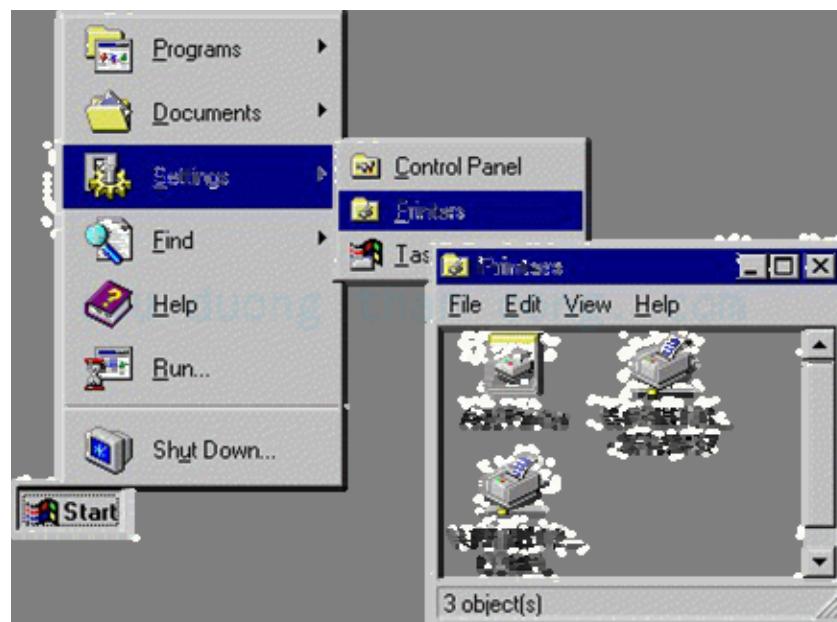


Hộp sau đó hộp hội thoại Add printer winzar hiện ra

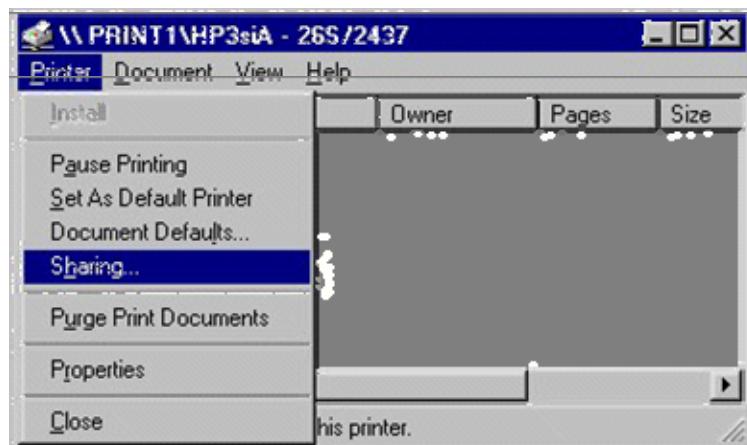


- Chọn My Computer nếu máy in của chúng ta không có card mạng và được nối trực tiếp vào Server.
- Chọn Network printer server nếu máy in của chúng ta nối trực tiếp vào mạng.
- Chọn à ext, chọn cổng nối với máy in (thường là LPT1). Chọn tên hãng sản xuất và loại máy in ta đang dùng, chọn à ext, ta phải trả lời thêm vài câu hỏi phụ như ta có muốn in trang test không? Có muốn đặt máy in này là ngầm định không?

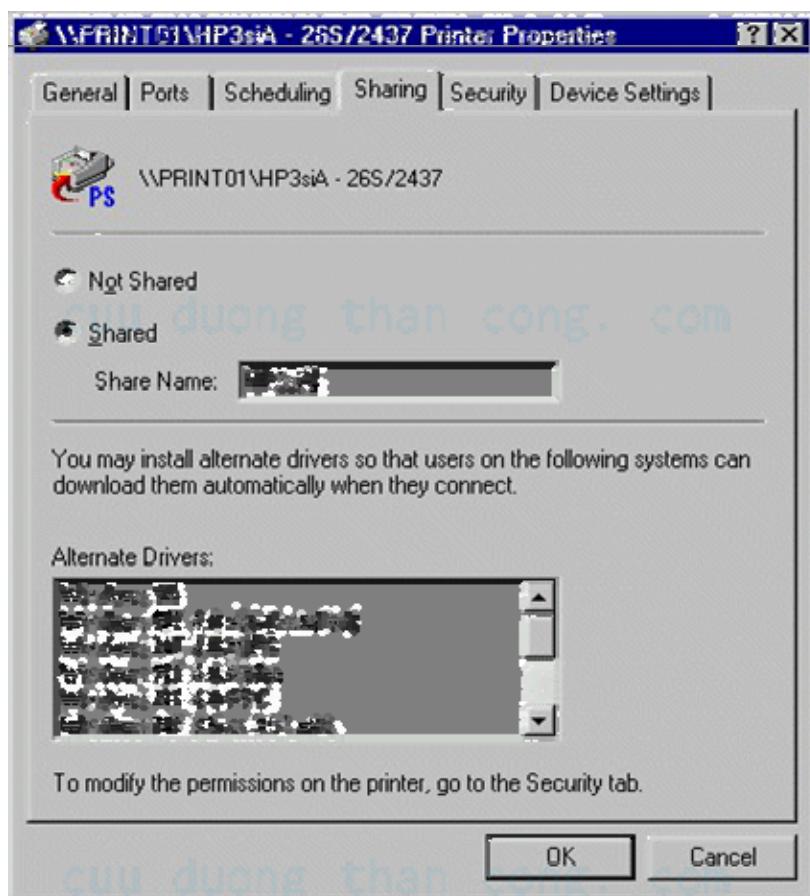
Sau khi cài đặt, chúng ta sẽ thấy xuất hiện thêm biểu tượng máy in mà vừa được cài đặt trong khung máy in. Chúng ta phải cho phép dùng chung máy in này bằng cách lựa chọn máy in đó Trong khung Printers



- Ta nhấp 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 name), 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: nhấp 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 ẩn T có thể được cấu hình như là một **print server**. Tuy nhiên chỉ có những người là thành viên của những nhóm sau đây mới có quyền tạo ra các máy in:

- Administrator (ẩn T Worstation and Server).
- Server Operator (ẩn T Server).
- Print Operator (ẩn T Server).
- Power Users (ẩn T Worstation).

II. Bảo mật của máy in

Windows NT có các mức độ bảo mật trong in ẩn như sau:

•**Quyền sở hữu máy in (Ownership)**: người sử dụng tạo ra một máy in chính là người chủ sở hữu máy in đó và có toàn quyền trên tất cả các thuộc tính của máy in logic. ẩn gười chủ sở hữu máy in có thể gán quyền cho những người dùng khác quản lý tài liệu hay toàn quyền điều khiển việc in ẩn. Một người sử dụng có toàn quyền thì họ toàn quyền sở hữu 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 động tài liệu, ẩn gừng, phục hồi, khởi động lại, và xóa các tài liệu.

•**Full control**: toàn quyền điều khiển, thực hiện các quyền quản lý tài liệu và các quyền sau đây:

•Thay đổi trật tự in ẩn tài liệu.

•ẩn gừng, tổng hợp lại, che dấu các máy in logic.

•Thay đổi thuộc tính của máy in logic.

•Hủy các máy in logic.

•Thay đổi quyền của máy in logic

Có thể xem tài liệu ở máy in logic và quản lý chúng theo nhiều cách. Ở gười sử dụng luôn quản lý được tất cả các tài liệu mà họ tạo ra. Để quản lý được các tài liệu của các người sử dụng khác, phải là người chủ sở hữu 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. Ở 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 phân 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 AT cũng có những ưu, khuyết điểm của nó, tuy nhiên Windows AT 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, client/server. Đó thích hợp với tất cả các kiến trúc mạng hiện nay như: hình sao (start), đường thẳng (bus), vòng (ring) và phức hợp. Đó có một số đặc tính ưu việt bao gồm thực hiện cùng lúc nhiều chương trình mà không bị lỗi. Bản thân Windows AT 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. Đó vừa đáp ứng được cho mạng cục bộ (LAN) và cho cả mạng diện rộng (WAN).

Windows AT cho phép dùng giao thức Windows AT 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 AT.

I. Internet Information Server (IIS)

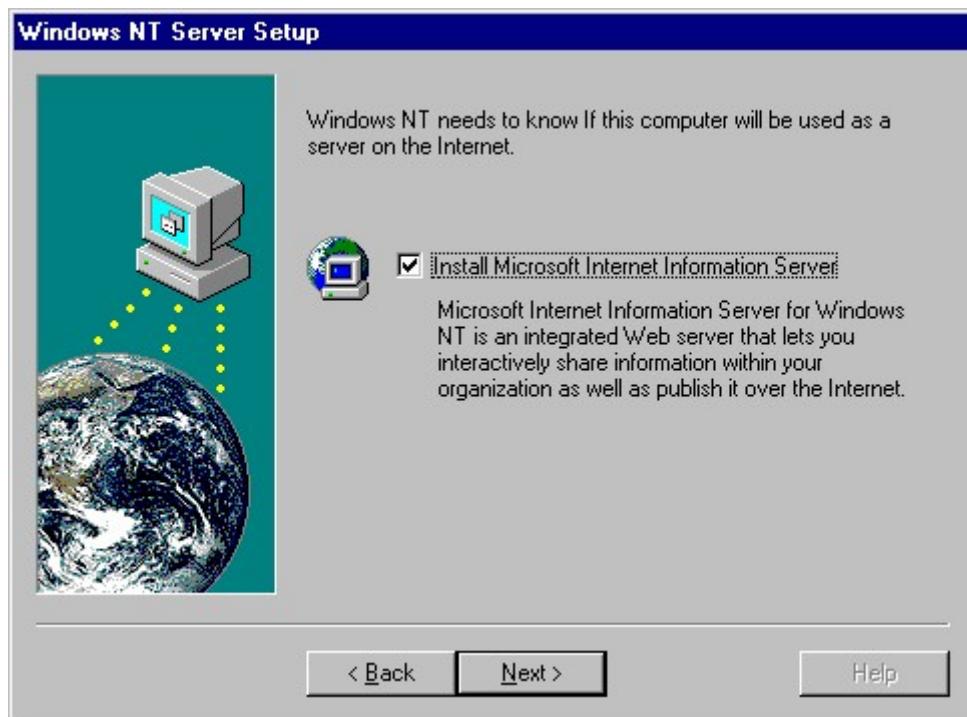
Internet Information Server là một ứng dụng chạy trên Windows AT, tích hợp chặt với Windows AT, khi cài đặt IIS, IIS có đưa thêm vào tiện ích màn hình kiểm soát (Performance monitor) một số mục như thống kê số lượng truy cập, số trang truy cập. Việc kiểm tra người dùng truy cập cũng dựa trên cơ chế quản lý người sử dụng của Windows AT. 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 AT đến phần mạng Windows AT sẽ hỏi chúng ta xem có cài đặt dịch vụ Internet Information Server hay không với hộp thoại

cuuduongthancong.com



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 chuyên giữa Web Server và Web Client thông qua giao thức HTTP (Hypertext Transfer Protocol).

là 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 A T khi một máy phát ra yêu cầu về các thông tin của TCPIP thì gọi là DHCP client, còn các máy cung cấp thông tin của TCPIP gọi là DHCP server. Các máy DHCP server bắt buộc phải là Windows A T server.

Cách cấp phát địa chỉ IP trong DHCP: Một user khi log on vào mạng, nó cần xin cấp 1 địa chỉ IP, theo 4 bước sau :

- Gởi thông báo đến tất cả các DHCP server để yêu cầu được cấp địa chỉ.
- Tất cả các DHCP server gởi trả lời địa chỉ sẽ cấp đến cho user đó.
- User chọn 1 địa chỉ trong số các địa chỉ, gởi thông báo đến server có địa chỉ được chọn.
- Server được chọn gởi thông báo khẳng định đến user mà nó cấp địa chỉ.

Quản trị các địa chỉ IP của DHCP server: Server quản trị địa chỉ thông qua thời gian thuê bao địa chỉ (lease duration). Có ba phương pháp gán địa chỉ IP cho các Workstation :

- 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 tín hiệu DHCP client giá trị địa chỉ IP mà được định bởi người quản trị mạng

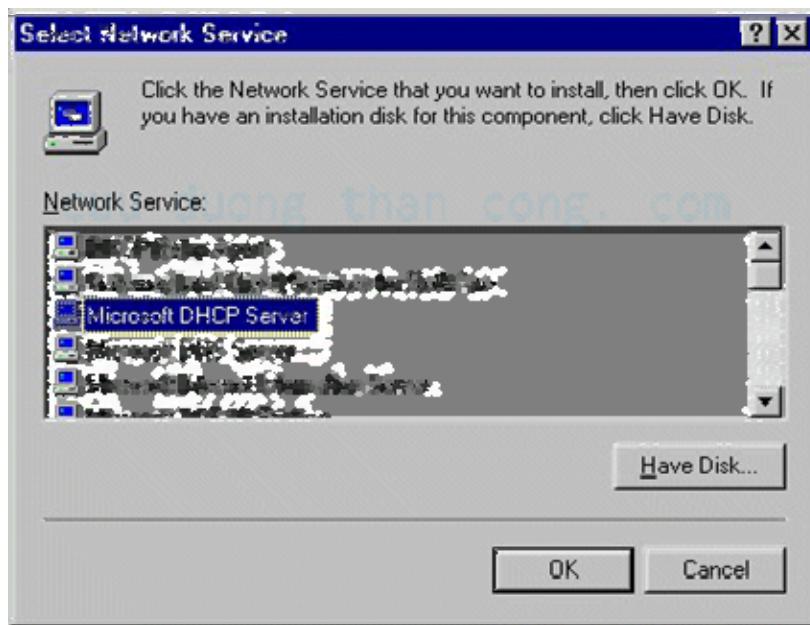
Trong phương pháp gán địa chỉ IP tự động DHCP client được gán địa chỉ IP khi lần đầu tiên nó nối vào mạng. Địa chỉ IP được gán bằng phương pháp này sẽ được gán vĩnh viễn cho DHCP client và địa chỉ này sẽ không bao giờ được sử dụng bởi một DHCP client khác

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 tinh 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 kết nối 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 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 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 Server nằm trong hộp 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 Server.

Để cập nhật và khai thác DHCP server chúng ta chọn mục DHCP manager trong Network 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, Dã S là 1 cơ sở dữ liệu phân tán cung cấp ánh xạ từ tên host đến địa chỉ IP. Khi đưa ra 1 tên host, Dã S server sẽ trả về địa chỉ IP hay 1 số thông tin của host đó. Điều này cho phép người quản lý mạng dễ dàng trong việc chọn tên cho host của mình.

DNS server được dùng trong các trường hợp sau :

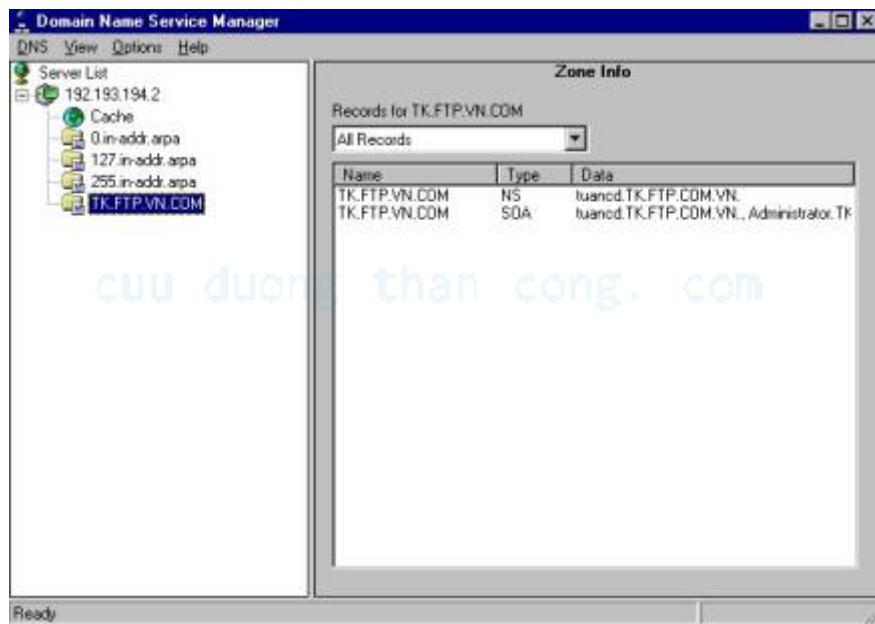
- Chúng ta muốn có 1 tên domain riêng trên Internet để có thể tạo, tách rời các domain con bên trong nó.
- Chúng ta cần 1 dịch vụ Dã S để điều khiển cục bộ nhằm tăng tính linh hoạt cho domain cục bộ của bạn.
- Chúng ta cần một bức tường lửa để bảo vệ không cho người ngoài thâm nhập vào hệ thống mạng nội bộ của mình

Có thể quản lý trực tiếp bằng các trình soạn thảo text để tạo và sửa đổi các file hoặc dùng Dã S manager để tạo và quản lý các đối tượng của Dã S như: Servers, Zone, Các mẫu tin, các Domains, Tích hợp với Win, .

Cài đặt Dã S chỉ có thể cài trên Windows à T server mà không thể cài trên Client. Các bước thực hiện như sau:

- Login vào Server với tên **Administrator**.
- Click hai lần vào icon **Network**. Ta sẽ thấy hộp hội thoại **Network dialog box** tương tự như trên và lựa chọn **Microsoft DNS Server**.

Để cập nhật và khai thác Dã S server chúng ta chọn mục **DNS manager** trong **Netwrok Administrator Tools**. Hộp hội thoại sau đây sẽ hiện ra



Hình 15.3: Màn hình DNS Manager

Mỗi một tập hợp thông tin chứa trong **DNS database** được coi như là **Resource record**. Các **Resource 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
Cổ AME ()	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

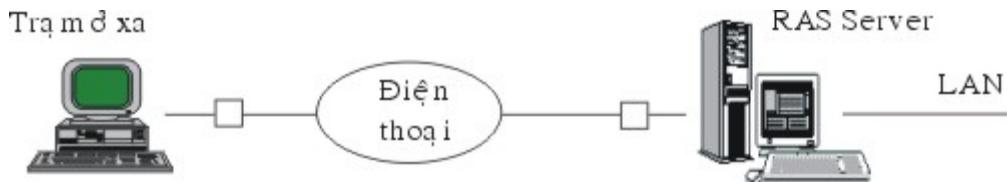
IV. Remote Access Service (RAS)

Besides the local network connection, there are also remote connections (LA) which are established from outside the network to the internal network. These connections are made through various methods such as dial-up, ISDN, or leased lines. In this section, we will focus on the Remote Access Service (RAS) which allows users to connect to the network from anywhere in the world.

Windows provides the Remote Access Service (RAS) to allow users to connect to the network via a modem or a network interface card (NIC). RAS can be used to connect to a server, perform tasks on the server, and execute programs on the server. It also provides security features such as user authentication and encryption.

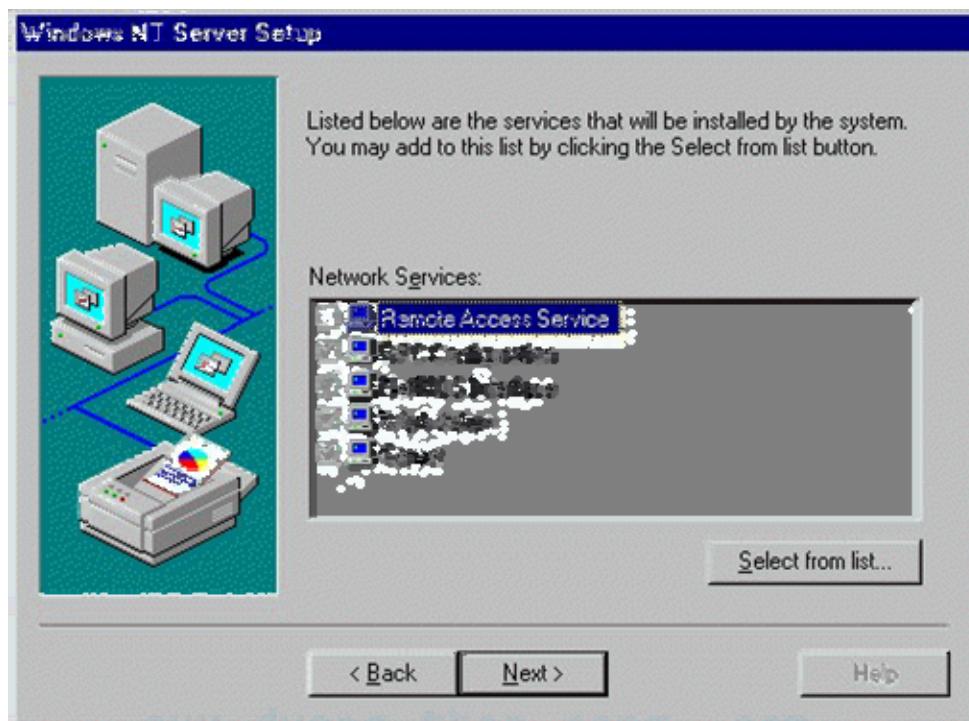
Windows provides the Remote Access Service (RAS) to allow users to connect to the network via a modem or a network interface card (NIC). RAS can be used to connect to a server, perform tasks on the server, and execute programs on the server. It also provides security features such as user authentication and encryption.

When setting up RAS, you need to configure the RAS server to accept incoming connections from the Internet. You can do this by configuring the RAS server's IP address and port number. You can also enable firewalls and other security features to protect your network from unauthorized access.



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 à T server setup hiện ra lúc cài đặt hệ điều hành Windows à T.



Với RAS tất cả các ứng dụng đều thực hiện trên máy từ xa, thay vì kết nối với mạng thông qua card mạng và đường dây mạng thì máy ở xa sẽ liên kết qua modem tới một RAS Server. Tất cả dữ liệu cần thiết được truyền qua đường điện thoại, mặc dù tốc độ truyền qua modem chậm hơn so với qua card mạng nhưng với những tác vụ của LAA 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 à T là một trong những hệ điều hành mạng tốt nhất hiện nay. Hệ điều hành Windows à T vừa cho phép giao lưu giữa các máy trong mạng, vừa cho phép truy nhập từ xa, cho phép truyền file, vừa đáp ứng cho mạng cục bộ (LAA) vừa đáp ứng cho mạng diện rộng (WA) như Intranet, Internet. Với những khả năng như vậy hiện nay hệ điều hành Windows à T đã có những vị trí vững chắc trong việc cung cấp các giải pháp mạng trên thế giới.

cuu duong than cong. com

cuu duong than cong. com

cuu duong than cong. com

2.4.2 So sánh SMTP với HTTP -----	90
2.4.3 Khuôn dạng thư và chuẩn MIME-----	91
2.4.4 Giao thức truy nhập mail. -----	97
2.5 DỊCH VỤ TÊN MIỀN - DNS.-----	102
2.5.1 Các dịch vụ của DNS -----	103
2.5.2 Cơ chế hoạt động của DNS -----	105
2.5.3 Bản ghi DNS -----	112
2.5.4 Thông điệp DNS -----	113
2.6 CÁC ỨNG DỤNG THEO KIẾN TRÚC NGANG HÀNG -----	115
2.6.1 Nhắn tin tức thì -----	117
2.6.6. Kiến trúc Hệ thống MSN. -----	121
2.6.3 Kiến trúc chia sẻ file ngang hàng Gnutella -----	128
2.7 LẬP TRÌNH SOCKET -----	134
2.7.1 Các hàm thao tác trên Socket-----	135
2.7.2 Ví dụ một chương trình client/server đơn giản-----	138
2.7.3 Web server đơn giản -----	140
CHƯƠNG 3 - TẦNG GIAO VẬN -----	148

3.1 DỊCH VỤ VÀ NGUYÊN TẮC CỦA TẦNG GIAO VẬN -----	148
3.1.1 Quan hệ giữa tầng giao vận và tầng mạng -----	150
3.1.2 Tổng quan về tầng giao vận trong Internet.-----	152
3.2 DỊCH VỤ DÒN KÊNH, PHÂN KÊNH -----	153
3.3 UDP – GIAO THỨC KHÔNG HƯỚNG NỐI -----	158
3.3.1 Cấu trúc UDP segment -----	162
3.3.2 UDP checksum-----	162
3.4 CÁC NGUYÊN TẮC TRUYỀN DỮ LIỆU TIN Cậy -----	164
3.4.1 Xây dựng giao thức truyền dữ liệu tin cậy -----	165
3.4.2 Giao thức truyền dữ liệu tin cậy liên tục (Pipeline) -----	175
3.4.3 Go-back-N (GBN)-----	178
3.4.4 Giao thức lặp lại có lựa chọn (Selective Repeat) -----	184
3.5 TCP – GIAO THỨC GIAO VẬN HƯỚNG NỐI -----	189
3.5.1 Kết nối TCP -----	190
3.5.2 Cấu trúc TCP Segment -----	193
3.5.3 Số thứ tự và Số biên nhận-----	195
3.5.4 Telnet: Một ví dụ về số thứ tự và số biên nhận -----	196
3.5.5 Truyền dữ liệu tin cậy -----	199

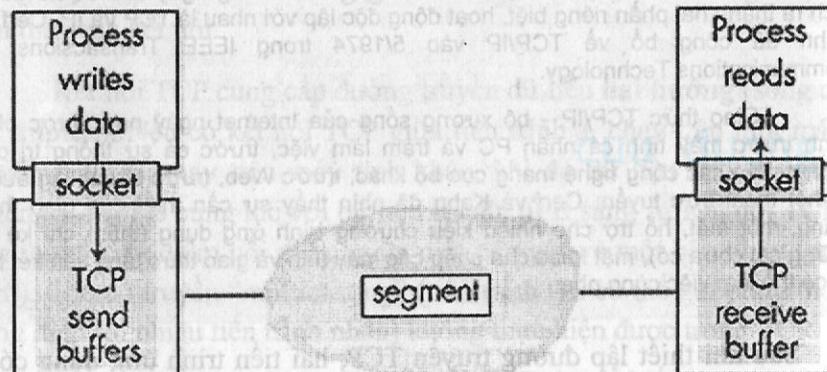
3.5.6 Kiểm soát lưu lượng-----	205
3.5.7 Quản lý kết nối TCP-----	207
3.6 KIỂM SOÁT TẮC NGHẼN TRONG TCP-----	211
CHƯƠNG 4 - TẦNG MẠNG -----	216
4.1 CÁC MÔ HÌNH DỊCH VỤ CỦA TẦNG MẠNG -----	216
4.1.1 Mô hình dịch vụ mạng -----	218
4.1.2 Nguồn gốc của dịch vụ chuyển mạch gói và chuyển mạch ảo.-----	223
4.2 CÁC NGUYÊN LÝ ĐỊNH TUYẾN -----	224
4.2.1. Thuật toán định tuyến link state. -----	227
4.2.2. Thuật toán Distance vector. -----	231
4.3 ĐỊNH TUYẾN PHÂN CẤP -----	236
4.4 INTERNET PTOTOCOL -----	238
4.4.1 Địa chỉ IPv4-----	240
4.4.2 Chuyển datagram từ nguồn tới đích: vấn đề địa chỉ và định tuyến -----	248
4.4.3 Khuôn dạng gói dữ liệu IP -----	251
4.4.4 Phân mảnh (Fragmentation) và Hợp nhất (Reassembly) gói tin IP -----	254
4.4.5 Giao thức kiểm soát lỗi ICMP (Internet Control Message Protocol) -----	258
4.5 ĐỊNH TUYẾN TRÊN INTERNET-----	259
4.5.1 Định tuyến trong một miền (Intra-AS routing) (Định tuyến nội miền) -----	260
4.5.2 Định tuyến giữa các miền (Inter-AS routing) (Định tuyến liên miền) -----	264
4.6 CÁU TẠO CỦA THIẾT BỊ ĐỊNH TUYẾN (ROUTER) -----	264
4.6.1 Cổng vào (Input port) -----	266
4.6.2 Kết cấu chuyển (Switching fabric) -----	268
4.6.3 Cổng ra (Output port) -----	270
4.6.4 Hàng đợi ở router -----	270
4.7 IPv6-----	273
4.7.1 Định dạng gói tin IPv6-----	273
4.7.2 Chuyển từ IPv4 sang IPv6 -----	276
4.8 CƠ CHẾ DỊCH CHUYÊN ĐỊA CHỈ (NAT) -----	279
4.9 KIỂM SOÁT TẮC NGHẼN -----	285
4.9.1 Các nguyên lý Kiểm soát tắc nghẽn.-----	286
4.9.2 Chính sách ngăn chặn tắc nghẽn -----	289
4.9.3 Kiểm soát tắc nghẽn trong mạch ảo -----	290
4.9.4 Kiểm soát tắc nghẽn trong mạng chuyển mạch gói.-----	292
4.9.5 Cắt tài -----	293

cuu duong than cong. com

trình server. Tiết trình client sẽ “đỗ” luồng dữ liệu qua socket (“cửa” của tiết trình - xem mục 2.6). Khi đã qua cửa, tiết trình gửi sẽ không kiểm soát được dữ liệu mà chính thực thể TCP chạy trên máy client sẽ chịu trách nhiệm kiểm soát. Trong Hình 3.27, TCP đẩy dữ liệu vào bộ đệm gửi (send buffer), một trong các bộ đệm được khởi tạo trong quá trình thiết lập kết nối. Sau đó TCP sẽ lấy và gửi dần dữ liệu trong bộ đệm gửi. Tuy nhiên, đặc tả TCP không xác định tường minh khi nào TCP phải gửi dữ liệu trong bộ đệm. Thường nó chỉ yêu cầu TCP “gửi khi thuận tiện”. Lượng dữ liệu ứng dụng lớn nhất có thể đặt trong một segment giới hạn bởi MMS (maximum segment size). Giá trị MMS phụ thuộc vào chính phần mềm triển khai TCP (thường là hệ điều hành) và có thể cấu hình được. Các giá trị MMS phổ biến thường là 1500 byte, 536 byte hay 512 byte. (Độ lớn của segment thường được giới hạn để tránh hiện tượng phân mảnh IP, một hiện tượng sẽ được đề cập trong chương sau). Chú ý MMS là lượng dữ liệu ứng dụng lớn nhất trong segment, chứ không phải là kích thước lớn nhất của segment TCP bao gồm cả tiêu đề (header).

Thực thể TCP gói dữ liệu cùng với TCP header trong TCP segment. TCP segment được chuyển xuống dưới tầng mạng và được đặt trong gói tin của tầng mạng (IP datagram) để gửi qua mạng. Ở phía nhận, thực thể TCP sẽ đặt dữ liệu vào bộ đệm nhận (receiver buffer) của kết nối TCP. Ứng dụng sẽ đọc dòng dữ liệu này từ bộ đệm. Mỗi kết nối đều có bộ đệm gửi và bộ đệm nhận. Bộ đệm gửi và nhận cho dữ liệu được minh họa trên Hình 3.27.

Chú ý rằng bộ đệm, các biến trạng thái, và socket tạo thành kết nối TCP chỉ nằm trên hai thiết bị đầu cuối chứ không nằm trên các thiết bị trung gian (router, hub, switch...).



Hình 3.27 Bộ đệm của thực thể TCP

3.5.2 Cấu trúc TCP Segment

Sau khi đã nói qua về TCP, bây giờ chúng ta sẽ xem xét cấu trúc gói dữ liệu TCP (TCP segment). TCP segment bao gồm các trường tiêu đề và trường dữ liệu. Trường dữ liệu chứa một phần dữ liệu ứng dụng. Như đã nói ở trên, giá trị MMS giới hạn độ lớn trường dữ liệu của segment. Khi TCP gửi một file lớn - ví dụ file ảnh trong trang Web, nó phải chia file thành các đoạn có kích thước MMS (ngoại trừ đoạn cuối cùng có độ lớn bé hơn hoặc bằng MMS). Tuy nhiên độ lớn dữ liệu của các ứng dụng tương tác thường nhỏ hơn MMS. Ví dụ, với ứng dụng đăng nhập từ xa (Telnet), trường dữ liệu trong TCP segment thường chỉ là 1 byte. Độ lớn trường tiêu đề của TCP là 20 byte (của UDP là 12 byte). Segment được Telnet gửi có thể chỉ có 21 byte.

Hình 3.28 minh họa cấu trúc TCP segment. Tương tự UDP, tiêu đề TCP bao gồm trường số hiệu cổng nguồn, số hiệu cổng đích để thực hiện dịch vụ dồn, phân kênh dữ liệu cho các ứng dụng bên trên và trường Checksum. Tuy nhiên tiêu đề của TCP segment còn có các trường sau:

Trường số thứ tự (sequence number) 32 bit và trường **số biên nhận (acknowledge number)** 32 bit được bên gửi và bên nhận sử dụng trong việc cung cấp dịch vụ truyền dữ liệu tin cậy, sẽ được đề cập kĩ hơn trong phần dưới đây.

Trường độ lớn cửa sổ (window size) 16 bit được sử dụng để kiểm soát lưu lượng. Đây chính là số lượng dữ liệu tối đa (tính theo byte) mà bên nhận có thể chấp nhận được.

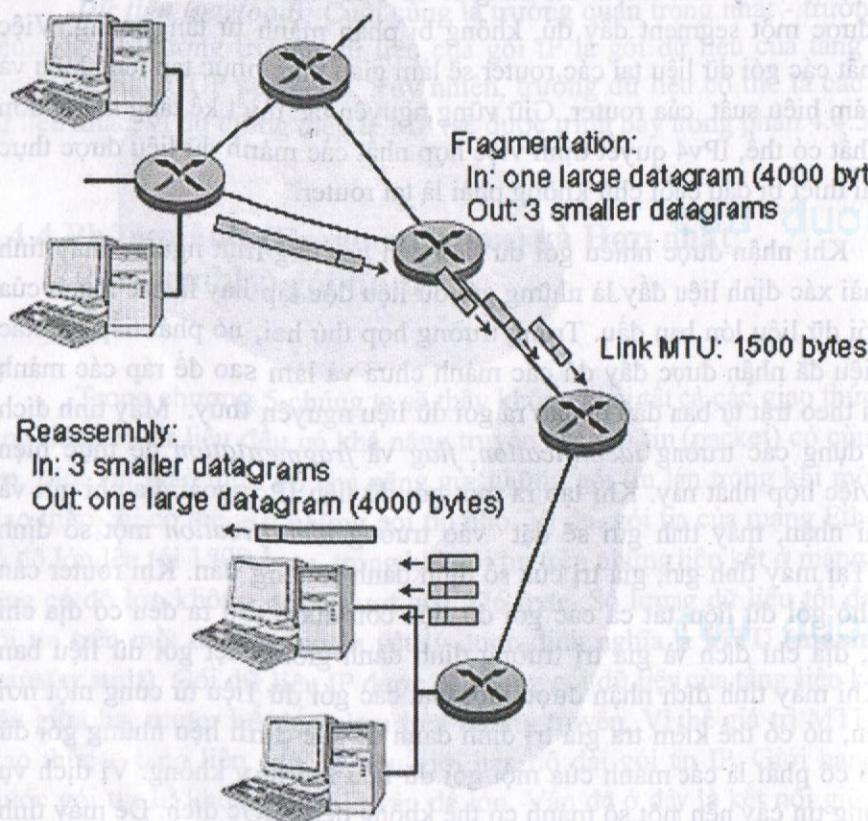
Trường độ dài tiêu đề (length field) 4 bit xác định độ dài của tiêu đề TCP theo đơn vị là các từ 32 bit. Tiêu đề TCP có thể có độ dài thay đổi phụ thuộc trường option (Nếu trường option rỗng, thì chiều dài của tiêu đề TCP là 20 byte).

Trường option là tùy chọn, có thể thay đổi tùy ý. Trường này được sử dụng khi bên gửi, bên nhận có thể thương lượng về giá trị MMS hoặc giá trị gia tăng của cửa sổ trong mạng cao tốc. Lựa chọn nhãn thời gian (timestamping) cũng được định nghĩa. Xem RFC 854 và RFC 1323 để biết thêm chi tiết.

cuu duong than cong. com

của các mảnh khác có giá trị 1. Tương tự để máy nhận xác định được liệu có mảnh nào không (và để ghép các mảnh theo đúng thứ tự), trường Offset được sử dụng để xác định vị trí của mảnh trong gói dữ liệu IP ban đầu.

Xét ví dụ trên Hình 4.21. Một gói dữ liệu có độ lớn 4000 byte đến router và phải gửi qua đường liên kết có MTU là 1500 byte. Điều này có nghĩa rằng 3980 byte dữ liệu trong gói dữ liệu ban đầu phải được tách ra thành ba mảnh phân biệt (mỗi mảnh trở thành một gói dữ liệu IP độc lập). Giá trị trong gói dữ liệu ban đầu giá trị trường định danh là 777. Giá trị các trường trong ba phân mảnh này được chỉ ra trong Bảng 4.3



Hình 4.21 Phân mảnh và hợp nhất gói dữ liệu IP

Dữ liệu của gói IP chỉ được chuyển lên tầng giao vận tại máy tính nhận khi tầng IP tái tạo hoàn chỉnh gói dữ liệu IP ban đầu. Nếu một số mảnh dữ liệu bị mất, không đến được đích, thì toàn bộ gói dữ liệu sẽ bị loại bỏ và không được chuyển lên tầng giao vận. Nhưng như đã nghiên cứu trong chương trước, nếu sử dụng TCP ở tầng giao vận, thì thực thể TCP sẽ khắc phục mất mát do phía gửi sẽ gửi lại gói dữ liệu ban đầu.

Fragment	Bytes	ID	Offset	Flag
1	1480 byte trong trường dữ liệu	identification=777	offset=0 (dữ liệu bắt đầu từ byte thứ 0)	flag=1 (còn mảnh nữa)
2	1480 byte trong trường dữ liệu	identification=777	offset=1480 (dữ liệu bắt đầu từ byte thứ 1480)	flag=1 (còn mảnh nữa)
3	1020 byte (=3980 - 1480 - 1480) trong trường dữ liệu	identification=777	offset=2960 (dữ liệu bắt đầu từ byte thứ 2960)	flag=0 (đây là mảnh cuối cùng)

Bảng 4.3 Ví dụ phân mảnh gói tin

Phân mảnh và hợp nhất nhiệm vụ xử lý gói tin tại router (tạo ra các mảnh) và thiết bị nhận (hợp nhất các mảnh) phức tạp hơn. Vì thế người ta cố gắng giảm thiểu việc phân mảnh dữ liệu. Điều này thường được thực hiện bằng cách giới hạn độ lớn gói dữ liệu của tầng giao vận (TCP hay UDP segment) bởi một giá trị tương đối nhỏ. Khi đó việc phân mảnh trở nên không cần thiết. Vì phần lớn các giao thức liên kết dữ liệu hỗ trợ IP có MTU tối thiểu là 536 byte, có thể loại bỏ hoàn toàn việc phân mảnh nếu đặt giá trị MSS là 536 byte với 20 byte tiêu đề của gói TCP và 20 byte tiêu đề của gói IP. Đây chính là lý do hầu hết các gói TCP khi truyền khôi lượng lớn dữ liệu (chẳng hạn FTP) có độ dài từ 512 đến 536 byte (Khi duyệt WEB, bạn sẽ thấy thường khoảng 500 byte dữ liệu đến cùng một lần).

Nếu gói TCP được lồng trong gói IP và cả hai gói TCP và IP đều không có trường tùy chọn (option) thì gói dữ liệu IP sẽ có 40 byte tiêu đề, phần còn lại là dữ liệu ứng dụng.

cuu duong than cong. com

TRƯỜNG ĐẠI HỌC KINH TẾ QUỐC DÂN
KHOA TIN HỌC KINH TẾ

MẠNG MÁY TÍNH
(TÀI LIỆU THAM KHẢO)

cuu duong than cong. com

cuu duong than cong. com

HÀ NỘI 2004

MỤC LỤC

(TÀI LIỆU THAM KHẢO)	1
PHẦN I NHỮNG VẤN ĐỀ CƠ BẢN VỀ MẠNG MÁY TÍNH	5
§ 1. Các khái niệm về mạng máy tính	5
1.1 Khái niệm về mạng (Network concepts)	5
1.2 Ứng dụng của mạng máy tính trong các tổ chức	5
1.3 Một số yếu tố đặc trưng của mạng	5
1.4 Phân loại mạng máy tính.	7
§ 2. Chuẩn mạng	7
2.1 Chuẩn.....	7
2.2 Mô hình tham chiếu	9
2.2.1 Mô hình tham chiếu OSI (Open System Interconnection)	9
(OSI Reference Model)	9
2.3 Mô hình tham chiếu TCP/IP	16
* So sánh với mô hình tham chiếu OSI:.....	18
2.4 Một số chuẩn mạng	19
§ 3. Hình trạng mạng (Network Topology)	21
§ 4. Các thiết bị liên kết mạng.....	23
4.1. Dây cáp mạng	23
4.2. Ví mạch mạng (Network Interface Card - NIC).....	25
4.3. Bộ tập trung (Hub).....	27
4.4. Chuyên mạch (Switch)	27
4.5. Bộ phát lặp (Repeater).....	26
4.6. Cầu nối (Bridge)	28
4.7. Bộ dẫn đường (Router)	29
4.8. Cổng kết nối (Getway)	29
§ 5. Các giao thức truyền trên mạng (Protocol)	30
5.1 Khái niệm	30
5.2. Các bộ giao thức phổ biến	32
§ 6. Thiết kế mạng cục bộ	32
6.1. Qui tắc thiết kế mạng:.....	33
6.2. Phương pháp thiết kế :	33
6.3. Một số thiết kế mạng	34
PHẦN II HỆ ĐIỀU HÀNH MẠNG NOVEL NETWARE	39
§ 1. Giới thiệu mạng NOVELL NETWARE	39
1.1. Sự phát triển của Novell Netware.....	39
1.2. Novell Directory Services	39
§ 2. Quản trị FILE SERVER	41
§ 3. Cài đặt mạng NOVELL NETWARE.....	42
3.1. Yêu cầu về phần cứng - phần mềm	43

3.2. Các bước cài đặt:	43
3.3. Cài đặt WORK STATIONS (DOS).....	49
3.3. Cài đặt WORK STATIONS (Windows 9.X)	49
§ 4. Quản trị hệ thống thư mục và files.....	52
4.1. Cấu trúc thư mục và files của Novell NetWare.....	52
4.2. Thiết kế hệ thống thư mục và FILES	53
4.3. Quyền hạn.....	54
4.4. Thuộc tính.....	55
§ 5. Quản trị USER Và GROUP.....	56
5.1. Quản trị USER.....	57
5.2. Quản trị GROUP	61
5.3. Quản trị USER ACCOUNT	62
5.4. Thao tác với USER ACCOUNT	63
§ 6. LOGIN SCRIPTS	64
6.1. Khái niệm:	64
6.2. Khởi tạo LOGIN SCRIPT	65
6.3. Các lệnh hệ thống trong LOGIN SCRIPT	66
§ 7. Quản trị dịch vụ in trên mạng	67
7.1.Tổng quan về công việc in trên mạng (DOS client).....	67
7.2. Cài đặt PRINT SERVER , cài đặt máy in, cài đặt PRINT QUEUE,.....	68
7.3. Ở work station : nối máy in với mạng	69
7.4. Tổ chức máy in PRINT SERVER	69
§ 8. Một số lệnh cơ bản của Novell Netware.....	70
PHẦN III HỆ ĐIỀU HÀNH MẠNG WINDOWS 2000	76
§ 1. Tổng quan về Microsoft windows 2000	76
1.1. Windows 2000 Server	76
1.2. Activate Directory (AD).....	77
1. 3. Địa chỉ trong giao thức TCP/IP	79
§ 2. Cài đặt WINDOWS 2000 SERVER.....	80
2.1. Một số vấn đề chung.....	80
2.2. Cài đặt windows 2000 server	81
2.3. Cài đặt Activate Directory	85
2.4. Hiệu chỉnh các tham số.....	89
2.5. Cơ sở dữ liệu Registry	91
§ 3. Quản trị USER và GROUP	94
3.1. Khái niệm user và group.....	94
3.2. Khái niệm quyền hạn	98
3.3. Thiết kế hệ thống user và group	100
3.4. Tạo user và group	101
3.5. Login Script	105
§ 4. Quản trị hệ thống thư mục và files.....	106
4.1 Cấu trúc thư mục của Windows 2000	106

4.2 Thiết kế hệ thống thư mục cho người dùng	107
4.3 Quản lý quyền truy cập.....	107
4.4 Cấp phát hạn ngạch đĩa (quota)	111
§ 5. Cài đặt client, Truy nhập vào mạng.....	113
5.1. Hệ điều hành DOS.....	113
5.2. Hệ điều hành WINDOWS 9X	116
5.3. Truy nhập vào Workstation khác trong mạng (mạng ngang hàng)	118
§ 6. Quản trị phương tiện lưu trữ.....	118
6.1. Một số khái niệm	118
6.2. Quản lý đĩa cứng.....	120
§ 7. Quản trị dịch vụ in ấn trên mạng	121
7.1. Nguyên lý in ấn trên windows 2000 :.....	121
7.2. Một kiểu cấu hình in trên mạng:.....	122
§ 8. Quản trị sao lưu dữ liệu.....	125
8.1. Khái niệm	125
8.2. Sao lưu hệ thống	125
8.3. Sao lưu dữ liệu.....	126
§ 9. Một số dịch vụ mạng của Windows 2000.....	127
9.1. Giao thức cấu hình máy động (Dynamic Host Configuration Protocol -DHCP).127	
9.2. Domain Name System (DNS)	130
§ 10. Tích hợp Novell Netware với Windows 2000	133
X.1. Khả năng liên kết với Novell Netware	134
10.2. Gắn kết với NWLink	134
10.3. Cấu hình dịch vụ cồng nối cho Novell	134
§ 11. Một số tiện ích	136
TÙ ĐIỀN THUẬT NGỮ.....	139
TÀI LIỆU THAM KHẢO.....	144

PHẦN I

NHỮNG VẤN ĐỀ CƠ BẢN VỀ MẠNG MÁY TÍNH

§ 1. CÁC KHÁI NIỆM VỀ MẠNG MÁY TÍNH

1.1 Khái niệm về mạng (Network concepts).

Mạng máy tính là tập hợp các máy tính và các thiết bị được liên kết với nhau thông qua đường truyền vật lý hoặc lôgic (môi trường truyền thông – communication medium) và tuân theo những qui tắc truyền thông nào đó gọi là mạng máy tính.

Mạng máy tính được thiết lập để có thể chia sẻ các tài nguyên mạng.

Đường truyền (môi trường truyền thông) dùng để truyền dẫn tín hiệu điện tử (electronic signal). Đường truyền có thể là hữu tuyến hoặc vô tuyến.

- Các qui tắc truyền thông là cơ sở để các máy tính có thể liên lạc được với nhau.
- Tài nguyên mạng bao gồm: thiết bị phần cứng, dữ liệu và ứng dụng.
- Chủ thể làm việc trên hệ thống mạng: con người

1.2 Ứng dụng của mạng máy tính trong các tổ chức.

Mạng được sử dụng chủ yếu để chia sẻ, dùng chung tài nguyên, và giao tiếp trực tuyến.

Chia sẻ thiết bị ngoại vi (devices): ổ đĩa mạng, máy in, modem, và một số thiết bị khác có thể được cài đặt trên mạng để mọi người có thể dùng chung các thiết bị này.

Chia sẻ dữ liệu (Data): các máy trên mạng đều có thể cập nhật và khai thác thông tin từ máy chủ dùng chung trên hệ thống mạng.

Chia sẻ file (file sharing): các máy tính trên mạng có thể chia sẻ việc sử dụng các file với nhau.

Chia sẻ các ứng dụng: có thể cài đặt các ứng chạy trên mạng để có thể khai thác từ nhiều máy trên mạng hoặc thiết lập các ứng dụng làm việc theo nhóm trên mạng.

Hỗ trợ giao tiếp (liên lạc) trên mạng: chẳng hạn như gửi nhận thông điệp (message), tán gẫu (chat - instant message), thư điện tử (e-mail); reminder, schedule,...

Quản lý tập trung và bảo mật tài nguyên.

...

1.3 Một số yếu tố đặc trưng của mạng

Đường truyền:

Là phương tiện dùng để truyền tín hiệu điện tử (electric signal) giữa các nút mạng, các tín hiệu này là thông tin được biểu thị dưới dạng các xung nhịp. Tùy

theo điều kiện kỹ thuật người ta có thể sử dụng các loại đường truyền khác nhau, có hai kiểu đường truyền:

- Đường truyền hữu tuyến: Các nút mạng được nối với nhau trực tiếp bằng dây cáp kim loại hoặc cáp quang (fibre optic).
- Đường truyền vô tuyến: Các nút mạng được nối với nhau thông qua các thiết bị điều chế/giai điều chế (modulation and demodulation) và truyền tín hiệu qua sóng vô tuyến.

Kiến trúc mạng (network architecture)

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

Kiến trúc mạng bao gồm toàn bộ những thiết kế và nền tảng của mạng.

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

- Network Topology: Cách thức kết nối các máy tính với nhau về mặt hình học mà ta gọi là topo của mạng. Các hình trạng mạng cơ bản đó là: hình sao, hình bus, hình vòng.
- Network Protocol: Tập hợp các quy ước truyền thông giữa các thực thể truyền thông mà ta gọi là giao thức (hay nghi thức) của mạng. Các bộ giao thức thường gặp nhất là: TCP/IP, NETBIOS, IPX/SPX, ...

Hệ điều hành mạng

Hệ điều hành mạng là một phần mềm hệ thống mạng (Network Operating System) làm nhiệm vụ quản lý các luồng thông tin vào ra, kiểm tra và phát hiện sai sót của thiết bị, quản lý và phân chia tài nguyên, quản lý hệ thống tệp tin, thi hành chế độ bảo mật.

Các chức năng chính của hệ điều hành mạng:

- + Quản lý người dùng và các công việc trên hệ thống: Hệ điều hành đảm bảo giao tiếp giữa người sử dụng với các chương trình ứng dụng, giữa các ứng dụng với thiết bị của hệ thống.
- + Cung cấp các dịch vụ mạng (network services) và các tiện ích (utilities) cho việc khai thác hệ thống.
- + Bảo mật hệ thống mạng.

Các hệ điều hành mạng thông dụng hiện nay là: Windows NT, Windows 2000, Unix (Sco Unix, Digital Unix, Sun Solaris), Linux (Redhat Linux, Debian Linux,...), Novell netware.

Máy chủ mạng(Server) và máy trạm (Workstation)

- Server: Máy chủ mạng thường là một máy tính có cấu hình đủ mạnh, được cài đặt hệ điều hành mạng cùng với các dịch vụ mạng (network services) và

các tiện ích để làm nhiệm vụ cung cấp tài nguyên, dịch vụ mạng tới người sử dụng và quản lý mạng (network supervising).

- Workstation: máy thành viên trên mạng thường được người sử dụng dùng để khai thác các tài nguyên và dịch vụ mạng.

1.4 Phân loại mạng máy tính.

* Phân loại mạng theo phạm vi nối máy:

- Mạng LAN (Local Area Network): Là một mạng máy tính ở quy mô nhỏ kết nối các máy tính trong phạm vi một văn phòng, cơ quan hoặc trường học (có bán kính cỡ vài trăm mét đến vài km), mạng này thường có tốc độ truyền thông lớn. Nó còn được gọi là mạng cục bộ.
- Mạng MAN (Metropolitan Area Network): Là một mạng được cài đặt trong phạm vi một đô thị hay trung tâm kinh tế xã hội (bán kính khoảng 100km).
- Mạng WAN (Wide Area Network): Là một mạng máy tính diện rộng có phạm vi bao trùm một quốc gia hay lục địa.
- Mạng GAL (Global Area Network): Một mạng toàn cầu, kết nối các hệ thống mạng trên toàn cầu.

* Phân loại mạng theo cách thức khai thác/chia sẻ dữ liệu

- + Mạng ngang hàng (Peer-to-Peer): Tất cả các máy tính trong mạng đều có vai trò như nhau và tất cả đều có thể chia sẻ tài nguyên với nhau.

Các hệ điều hành được sử dụng trong mạng ngang hàng như:

- Windows for workgroup (Windows 3.11).
- LanTastic Antisoft
- Windows 98/ME/2K/XP

- + Mạng phân quyền (Client/Server): Tất cả các máy tính trong mạng (máy khách – Client) đều khai thác và chia sẻ tài nguyên thông qua một máy chủ phục vụ (Server).

Các hệ điều hành mạng phân quyền (client/server) phổ biến như:

- Novell NetWare (2.x / 3.x / 4.x / 5.x/6.x).
- Windows NT , Windows 2000

* Phân loại theo cách thức nối máy

+ Điểm điểm (point to point)

+ Quảng bá (broadcast)

* Phân loại theo phương thức chuyển mạch

+ Chuyển mạch kênh (Circuit Switching Network)

+ Chuyển mạch thông điệp (Message Switching Network)

+ Chuyển mạch gói (Packet Switching Network)

§ 2. CHUẨN MẠNG

2.1 Chuẩn

2.1.1 Khái niệm

Trong công nghiệp truyền thông, từ lâu các chuẩn đó được chấp nhận như là yêu cầu cần thiết để quản lý các đặc tính về thủ tục, điện tử và vật lý của thiết bị truyền thông. qua đó cho phép các thiết bị tương tác với nhau.

- Các ưu điểm của việc xây dựng và tuân theo chuẩn:
 - o Đảm bảo cho một thị trường rộng lớn cho các thiết bị và phần mềm.
 - o Cho phép các sản phẩm của các nhà cung cấp khác nhau truyền thông được với nhau
- Các nhược điểm:
 - o Không thay đổi công nghệ (Freeze technology)
 - o Cú thể cú nhiều chuẩn cho từng một loại thiết bị.

Các tổ chức quốc tế chính, quan trọng trong việc xây dựng và đưa ra các chuẩn :

- Internet Society
- ISO
- ITU-T (formally CCITT)

...

ISO (International Standards organization): là tổ chức tiêu chuẩn quốc tế làm việc dưới sự bảo trợ của Liên hợp quốc với các thành viên là các cơ quan tiêu chuẩn quốc gia, trong ISO được chia thành các ủy ban kỹ thuật phụ trách các lĩnh vực khác nhau. Các công trình chuẩn hóa sau khi được ISO biểu quyết thông qua sẽ được công bố như tiêu chuẩn quốc tế chính thức (International Standard - IS).

CCITT (Comité Consultatif International pour le Télégraphe et la Téléphone): Tổ chức tư vấn quốc tế về điện tín và điện thoại, làm việc dưới sự bảo trợ của Liên hợp quốc với các thành viên là cơ quan bưu chính viễn thông của các quốc gia hoặc các hảng xuyên quốc gia. Các tiêu chuẩn của CCITT được coi là các khuyến nghị. CCITT đã ban hành khuyến nghị loại V: liên quan đến vấn đề truyền dữ liệu, loại X: liên quan đến các mạng truyền dữ liệu công cộng ...

Sự tồn tại của cả hai tổ chức giải thích cho sự giao thoa giữa các chức năng xử lý và truyền tin trong các ứng dụng viễn thông-tin học.

IEEE (Institute of Electrical and Electronics Engineers) Viện kỹ thuật điện tử, một tổ chức đưa ra các chuẩn cụ thể của mạng.

ANSI (American National Standards Institute): là tổ chức của các nhóm doanh nghiệp và công nghiệp Mỹ, chuyên phát triển các tiêu chuẩn thương mại và truyền thông: mã, bảng chữ cái, lược đồ tín hiệu.

Common Open Software Environment (COSE): Môi trường chung cho phần mềm mở

Open Software Foundation (OSF): cơ sở phần mềm mở

SQL Access Group (SAG): Nhóm truy cập ngôn ngữ hỏi có cấu trúc

Object Management Group (OMG): nhóm quản lý đối tượng

Corporation for Open Systems (COS): tập đoàn các hệ mở

Electronics Industries Association (EIA): Hiệp hội các ngành công nghiệp điện tử

2.1.2 Qui luật và tiến trình liên lạc

Các mạng đều dựa vào nhiều qui luật để trao đổi thông tin. Một số quy trình được các mạng chuẩn định hành như sau:

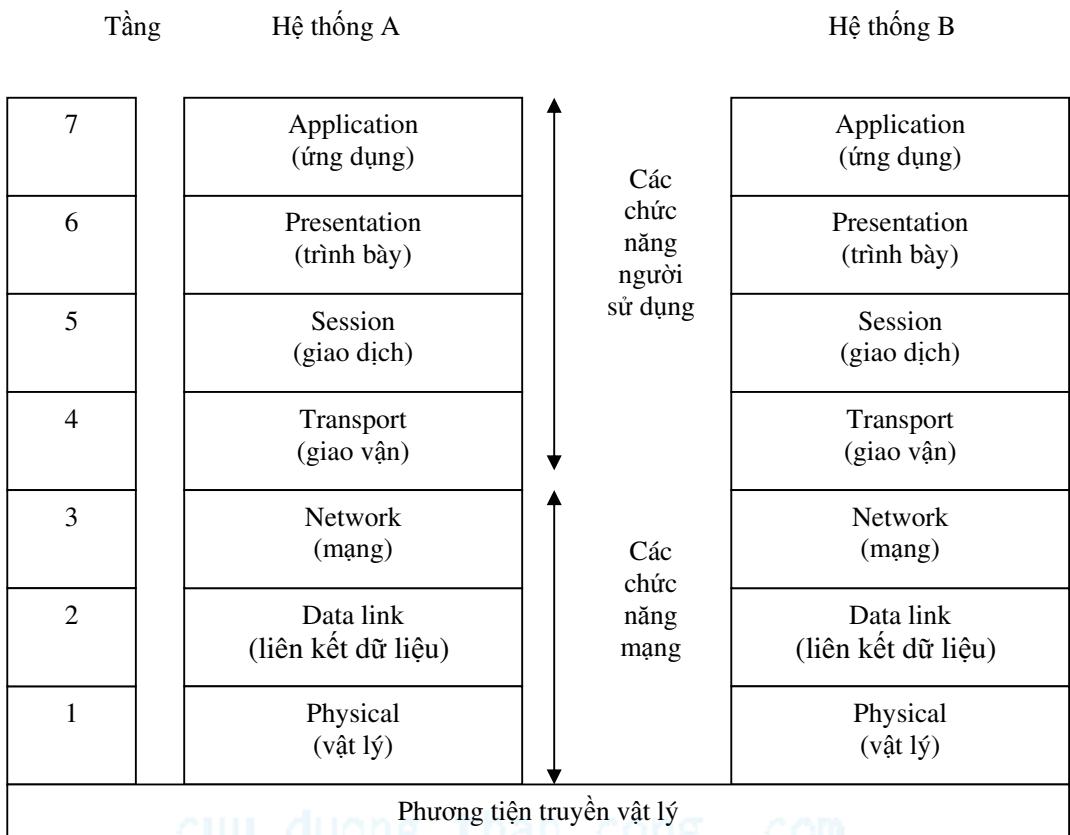
- Qui trình để nối và cắt liên lạc
- Tín hiệu để trình bày dữ liệu trên phương tiện truyền thông.
- Loại tín hiệu được dùng.
- Phương pháp truy cập để chuyển tiếp một tín hiệu liên lạc.
- Phương pháp truyền trực tiếp một thông điệp gửi tới nơi đến.
- Thủ tục dùng để kiểm soát tốc độ truyền dữ liệu.
- Phương pháp dùng cho máy điện toán khác loại liên lạc được với nhau.
- Các cách bảo đảm cho thông điệp được nhận đúng cách

2.2 Mô hình tham chiếu

Năm 1978 tổ chức tiêu chuẩn quốc tế – ISO đã ban hành tập hợp đặc điểm kỹ thuật mô tả kiến trúc mạng dành cho việc kết nối những thiết bị không cùng chủng loại. Ban đầu tài liệu này áp dụng cho những hệ thống mở với nhau do chúng có thể dùng chung giao thức và tiêu chuẩn để trao đổi thông tin. Vào năm 1984, ISO đã phát hành bản sửa đổi mô hình này và gọi là mô hình tham chiếu mạng hệ mở OSI (Open Systems Interconnection)

2.2.1 Mô hình tham chiếu OSI (Open System Interconnection) (OSI Reference Model)

Mô hình tham chiếu OSI: Mô hình này là một khung mà các tiêu chuẩn lập mạng khác nhau có thể khớp vào. Nó định rõ các mặt nào của hoạt động của mạng có thể nhằm đến bởi các tiêu chuẩn mạng khác nhau. Mô hình OSI có 7 tầng, hai tầng đáy là các tầng có tác động thực tế nhất trên các mạng nhỏ. Các tiêu chuẩn mạng như Ethernet và Token Ring là các tiêu chuẩn tầng 1 và tầng 2. Các tầng cao hơn trong mô hình OSI không tạo ra các tiêu chuẩn phổ biến.



Mô hình OSI

Liên lạc giữa các tầng ngang hàng

Tầng thứ i của một máy tính sẽ hội thoại với tầng thứ i của một máy khác. Các qui tắc và qui ước được dùng trong việc hội thoại đó được gọi là **giao thức** (protocol) của mức i.

Giữa mỗi cặp tầng kề nhau tồn tại một **giao diện** (interface) xác định các thao tác và các dịch vụ mà tầng dưới cung cấp cho tầng trên.

Mỗi tầng sẽ truy cập với tầng trên và dưới nó thông qua các điểm truy cập dịch vụ (Service Access Point -SAP).

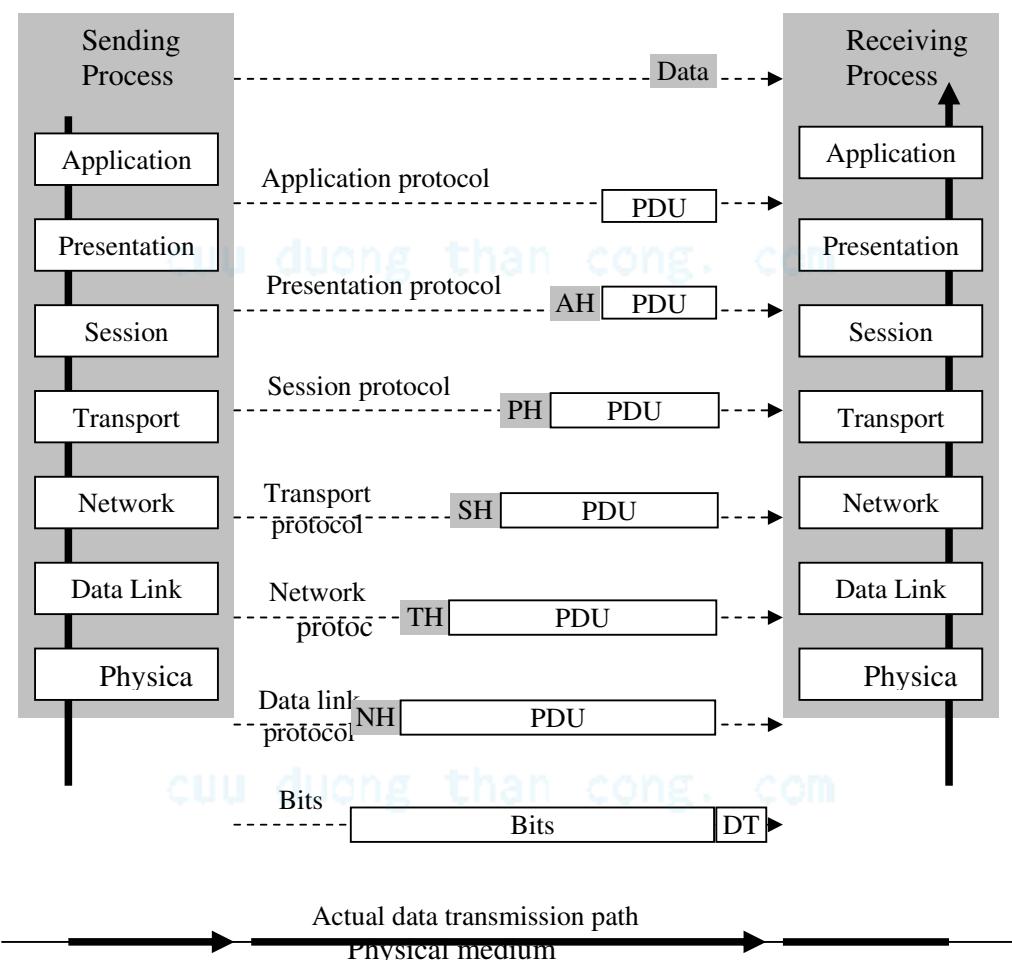
Trong thực tế dữ liệu không được truyền trực tiếp từ tầng thứ i của máy này sang tầng thứ i của máy khác (riêng tầng 1 dữ liệu truyền trực tiếp). Mỗi tầng chuyển dữ liệu và thông tin điều khiển xuống tầng ngay dưới nó và tiếp tục cho đến tầng 1. Ở tầng 1 sẽ có đường truyền thông vật lý tới tầng thấp nhất của máy tương ứng và từ đó dữ liệu và thông tin điều khiển lại được truyền ngược lên các tầng trên. Như vậy ở các tầng trên tầng 1 sẽ chỉ xác định các đường

truyền LOGIC tới tầng tương ứng của các máy khác. (đường đứt nét biểu thị đường truyền LOGIC, đường liền nét biểu thị đường truyền vật lý).

Ví dụ: Giả sử có 2 máy A và B cần truyền dữ liệu cho nhau. (Giả thiết dữ liệu được tạo ra tại tầng ứng dụng - tầng 7 - của máy A).

Thông tin xuất phát từ mức 7 của máy A chuyển tới mức 6 bao gồm thông tin của mức 7 cộng với phần Header của mức sáu. Cứ như vậy cho đến mức 1 và được chuyển ra đường truyền. Thông tin nhận được ở mức 1 của máy B được kiểm tra phần Header của chính mức 1 nếu đúng thì phần Header sẽ được cắt bỏ và chuyển phần còn lại lên mức 2 của máy B. Nếu kiểm tra phần Header không đúng thì sẽ báo lỗi cho máy A truyền lại. Quá trình cứ tiếp tục như vậy cho tới mức 7 của máy B.

Đường truyền dữ liệu trong OSI:



Tầng 1 (physical - vật lý):

Tầng này không xác định rõ phương tiện vật lý nhưng nó vẫn nêu rõ những yêu cầu về những phương tiện kỹ thuật cần thiết trên phương diện vật lý (chẳng hạn các cable mạng phù hợp chuẩn IEEE 802.2). Cung cấp các phương tiện điện, cơ hàm và thủ tục để khởi động, duy trì và hủy bỏ các liên kết vật lý cho phép truyền các dòng dữ liệu ở dạng bit.

Tầng physical định nghĩa cách kết nối dây cáp với card mạng, ví dụ nó định rõ bộ nối có bao nhiêu chân, kỹ thuật truyền nào được dùng để gửi dữ liệu lên cáp mạng. Tầng này chịu trách nhiệm truyền dữ liệu theo mã nhị phân, nó định rõ mã hóa dữ liệu và sự đồng bộ hóa bit, bảo đảm rằng khi máy nguồn gửi bít 1, máy đích sẽ nhận được bít 1.

Các thành phần hoạt động ở tầng vật lý:

Bộ chuyển tiếp (repeater), là một thiết bị mạng nó lặp lại tín hiệu từ một cổng rồi chuyển tiếp đến những cổng khác. Nó không lọc hoặc diễn giải điều gì mà chỉ lặp lại để khuếch đại tín hiệu truyền trên mạng (Amplify signal – khuếch đại tín hiệu). Do vậy các thiết bị loại này thường khuếch đại cả tín hiệu nhiễu (noise signal) .

Tầng 2 (data link - liên kết dữ liệu):

Tầng này làm nhiệm vụ nhận nhận dữ liệu từ tầng mạng (network layer) rồi chia thành các khung dữ liệu (data frame) và gửi đến tầng vật lý (physical layer). Tại đầu nhận, tầng này đóng gói dữ liệu thô (chưa xử lý) từ tầng physical thành từng khung dữ liệu. Tại tầng này có thực hiện việc điều khiển luồng, cắt/hợp dữ liệu và phát hiện sai sót.

Tóm lại tầng data link chịu trách nhiệm chuyển khung dữ liệu không lỗi từ nút mạng này sang nút mạng khác thông qua tầng physical. Thông thường khi gửi một khung dữ liệu nó chờ tín hiệu báo nhận từ nút nhận.

Tầng data link của nút nhận sẽ dò tìm bất cứ vấn đề nào có thể xảy ra trong quá trình truyền. Khung dữ liệu nào không được báo nhận hoặc bị hư tổn trong quá trình truyền sẽ bị gửi trả lại.

Tầng data link được chia làm 2 lớp phụ là:

- Điều khiển truy nhập phương tiện (Media Access Control – MAC): lớp phụ MAC điều khiển việc truy nhập thiết bị, phương tiện truyền thông để truyền dữ liệu từ tầng MAC của thiết bị này sang tầng MAC của thiết bị kia (chẳng hạn card mạng).

Cụ thể tầng MAC sẽ quản lý các thiết bị mạng truy cập vào môi trường truyền thông, cung cấp địa chỉ (MAC Address) để liên lạc giữa các thiết bị trên mạng.

- Điều khiển liên kết logic (Logical Link Control – LLC): tầng này làm nhiệm vụ giao tiếp với tầng trên, kiểm soát luồng và lỗi, thiết lập và duy trì liên kết giữa các thực thể tham gia truyền thông.

Thành phần hoạt động:

Cầu nối (bridge - thiết bị mạng tại tầng liên kết dữ liệu): Bridge làm nhiệm vụ chuyển các khung dữ liệu (data frame) từ mạng này sang mạng khác (cầu nối giữ các mạng). Nhờ việc kiểm tra địa chỉ MAC tại tầng liên kết dữ liệu nên nó có thể phát hiện ra đích đến của khung dữ liệu là nằm **trong** mạng hay **ngoài** mạng dựa vào một bảng địa chỉ MAC (MAC Address table) của các nút (Node) trong mạng. Khi một khung dữ liệu đến, Bridge kiểm tra địa chỉ đích của khung và đưa khung đến mạng chứa thiết bị đích hoặc nút đích. Nếu nút đích ở cùng mạng với nút nguồn bridge sẽ không đưa đến các mạng khác. Nếu cầu không tìm được địa chỉ đích, nó đưa khung đến tất cả các mạng trừ mạng nguồn.

Tầng 3 (network - mạng):

Tầng mạng được hình thành nhằm đảm bảo trao đổi thông tin giữa các mạng con trong một hệ thống mạng lớn. Tầng này quyết định đường đi cho các gói số liệu, khả năng định tuyến dựa trên cơ chế đánh địa chỉ thông nhất mà lớp mạng qui định cho các nút mạng. Ngoài ra nó còn kiểm soát dòng dữ liệu trên các tuyến để tránh tắc nghẽn hoặc mất mát thông tin. Tóm lại tầng này phụ trách những việc sau:

- Chọn đường đi, cung cấp địa chỉ.
- Kiểm soát lỗi và thông lượng.
- Chuyển mạch và dọn đường.
- Chia thông tin lại thành từng bó và lựa chọn đường đi đến đích cho từng bó khác nhau sao cho thời gian truyền tin là ngắn nhất và tin cậy nhất.
- Hợp nhất các bó thông tin tại nút nhận.

Tầng này phụ trách việc thiết lập các tuyến đường giữa các nút mạng khác nhau. Chính nhờ tầng này mà các mạng lắp theo các chuẩn khác nhau có thể liên kết với nhau.

* Định địa chỉ trên tầng mạng: Tầng mạng làm nhiệm vụ đánh địa chỉ các máy tham gia truyền thông trên mạng. Địa chỉ này chỉ là địa chỉ Logic để thay thế cho các địa chỉ vật lý, vì trong các mạng lớn việc sử dụng địa chỉ vật lý là không thực tế, không đáp ứng được yêu cầu truyền tin. Tầng mạng sử dụng địa chỉ logic để định tuyến (Router) và lọc bỏ gói tin (packet filter).

* Phân phối gói tin: Một gói tin được gửi từ một phần trên mạng của máy nguồn và đi theo nhiều con đường khác nhau của mạng để đến máy đích. Tầng mạng sẽ giám sát quá trình chọn đường truyền và phân phối gói tin qua mạng.

* Các kỹ thuật chuyển mạch cơ bản: chuyển mạch kênh (Circuit switching), chuyển mạch thông điệp (Message switching), chuyển mạch gói (Packet switching).

+ Chuyển mạch kênh (Circuit switching): Khi có hai nút cần truyền thông với nhau thì giữa chúng sẽ thiết lập một kênh cố định và duy trì kết nối đó cho tới khi hai bên ngắt liên lạc. Các dữ liệu chỉ truyền đi theo con đường cố định đó. Kỹ thuật này cung cấp cho các thiết bị một băng tần xác định. Phương pháp này

có ưu điểm là đường truyền thông suốt, tốc độ ổn định. Nhưng cũng có các nhược điểm như quá trình thiết lập sự kết nối thiết bị chậm, đường truyền bị chiếm giữ ngay cả khi không có dữ liệu truyền qua dẫn đến lãng phí đường truyền.

+ Kỹ thuật chuyển thông điệp (Message switching): thông điệp là một đơn vị dữ liệu của người sử dụng có khuôn dạng được quy định trước. Mỗi thông điệp tin có chứa các thông tin điều khiển trong đó chỉ rõ đích cần truyền tới của thông điệp. Căn cứ vào thông tin điều khiển này mà mỗi nút trung gian có thể chuyển bản tin tới nút kế tiếp trên con đường dẫn tới đích của bản tin. Kỹ thuật này có thể dùng chung kênh dữ liệu để nâng cao hiệu suất sử dụng giải tần, có khả năng lưu trữ bản tin đến khi có kênh truyền vì vậy giảm mật độ ùn tắc trên mạng. Tuy nhiên nhược điểm chính của nó là không phù hợp với các ứng dụng thực tế như truyền dữ liệu, truyền thanh.

+ Kỹ thuật chuyển mạch gói (Packet switching): ở đây bản tin hoặc thông điệp được chia ra thành nhiều gói nhỏ hơn được gọi là các gói tin (packet/diagram) có khuôn dạng qui định trước. Mỗi gói tin cũng chứa các thông tin điều khiển, trong đó có địa chỉ nguồn (người gửi) và địa chỉ đích (người nhận) của gói tin. Các gói tin của cùng một tin báo có thể được gửi đi qua mạng tới đích theo nhiều con đường khác nhau. Chuyển mạch gói không lưu trữ gói tin lâu (ví kích thước packet < mesage) nên truyền đường của gói tin qua mạng sẽ nhanh và hiệu quả hơn so với kỹ thuật chuyển mạch tin.

* Loại giao thức: Tầng mạng trong mô hình OSI xác định định tuyến để các gói tin từ máy nguồn đến máy đích qua nhiều mạng khác nhau. Trong tầng này sử dụng hai loại giao thức cơ bản để truyền tin là: Giao thức hướng kết nối (Connection Oriented) và Giao thức không hướng kết nối (Connectionless).

+ Giao thức hướng kết nối (Connection Oriented): Trong giao thức bao giờ cũng thiết lập kết nối (Connection) trước khi truyền số liệu, tức là giữa nút đích và nút nguồn sẽ thiết lập một liên kết logic để truyền số liệu (phân phối các một cách có thức tự các gói tin qua kênh logic này và có báo nhận để đảm bảo dữ liệu đến đích một cách tin cậy).

+ Giao thức không hướng kết nối (Connectionless): Trong giao thức này việc phân phối các gói tin dựa vào địa chỉ đích mà không thiết lập kết nối (connectionless) và báo nhận. (tức là nút phân phối gói tin không biết được gói tin phát đi có đến đích hay không).

* Thành phần hoạt động: Bộ định tuyến (router) thiết bị mạng hoạt động tại tầng mạng. Bộ định tuyến tại tầng mạng dựa vào bảng định tuyến (routing table) để lựa chọn đường đi phù hợp cho gói tin nhận được. Các bảng định tuyến có thể tĩnh (static) hoặc động (dynamic).

Tầng 4 (transport - giao vận, vận chuyển):

Trong mô hình tham chiếu thường chia ra 3 tầng cao (Application, Presentation, Session) và 4 tầng thấp (Transport, Network, Data link, Physical). Các tầng thấp quan tâm đến việc đáp ứng việc truyền số liệu giữa các hệ thống cuối (end systems) qua thương tiệm truyền thông, còn tầng cao tập trung đáp ứng các yêu cầu của ứng dụng và người sử dụng.

Tầng giao vận là tầng cao nhất của nhóm các tầng thấp, nó phụ trách việc lưu chuyển thông tin trên mạng một cách “trong suốt” đối với các tầng cao. Do đó các tính năng mức này phải đảm bảo là:

- + Kiểm soát việc truyền số liệu từ nút tới nút (end to end):
 - . Đồng nhất một nút bằng một địa chỉ duy nhất.
 - . Nhận biết mạng và hoạt động được với cả mạng hướng kết nối (Connection oriented) và cả không hướng kết nối (Connectionless).
 - . Phải nhận biết được chất lượng dịch vụ (Quality of Service – QoS) của người sử dụng và khả năng cung cấp dịch vụ của tầng bên dưới.
- + Khắc phục sai sót: Trong quá trình truyền có thể xảy ra sai sót thì tầng giao vận phải có khả năng khắc phục các sai sót đó bằng các cơ chế báo nhận và truyền lại các gói tin (packet/diagram).
- + Ghép kênh, cắt/hợp dữ liệu nếu cần: Khối lượng dữ liệu truyền có thể lớn hoặc nhỏ, đường truyền có thể nhiều hoặc ít, Vì vậy tầng giao vận phải có khả năng cắt/ hợp dữ liệu tại đầu gửi/nhận và phân kênh/hợp kênh khi cần thiết (TDM – Time Division Multiplexing, FDM – Frequency Division Multiplexing).

Tầng 5 (Session – Tầng phiên):

Tầng phiên là tầng thấp nhất trong các tầng cao, nó đáp ứng các yêu cầu của người dùng phục vụ cho các ứng dụng trên mạng thông qua các phương tiện truyền thông cung cấp bởi nhóm các tầng thấp.

Tầng phiên cho phép người sử dụng tiếp xúc với nhau qua mạng. Do đó nhiệm vụ chủ yếu là quản lý các cuộc tiếp xúc (giao dịch) giữa người sử dụng trên mạng tạo, duy trì hay hủy bỏ các cuộc tiếp xúc đó. (tầng này chủ yếu là thiết lập giao dịch giữa các ứng dụng trong mạng).

Tầng phiên thiết lập các giao dịch giữa các nút mạng. Một giao dịch phải được thiết lập trước khi truyền dữ liệu trên mạng. Tầng phiên phải đảm bảo cho các giao dịch được thiết lập và duy trì đúng qui định. Khởi tạo cho các giao dịch đầu cuối. Đồng bộ và đồng bộ lại việc truyền thông tin. Điều khiển hội thoại.

Một số dịch vụ của tầng phiên:

- Thiết lập một liên kết với một người sử dụng ở tầng phiên khác, trao đổi dữ liệu với người sử dụng đó một cách đồng bộ, và huỷ 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 hoá và huỷ bỏ liên kết, sắp xếp phương thức trao đổi dữ liệu
 - + Half-duplex
 - + Full-duplex

- Thiết lập các điểm đồng bộ hoá trong các hội thoại và khi xảy ra sự cố có thể khôi phục lại việc hội thoại bắt đầu từ một điểm đồng bộ hoá đã thỏa thuận.
- Ngắt một hội thoại và khôi phục lại hội thoại sau đó từ một điểm xác định trước.

Tầng 6 (presentation - trình bày):

Tầng trình bày chịu trách nhiệm biểu diễn thông tin, chuyển đổi dữ liệu gửi đi trên mạng từ một loại biểu diễn này sang một loại biểu diễn khác. Chẳng hạn như các kỹ thuật nén dữ liệu trước khi truyền đi, sau đó nhận được và khôi phục trở lại.

Tầng trình bày cũng là tầng có thể dùng kỹ thuật mã hoá để xáo trộn dữ liệu trước khi truyền đi và giải mã sau khi nhận lại nhằm đảm bảo việc bảo mật và an toàn số liệu trên đường truyền.

Tầng này cũng đảm bảo cho các hệ thống cuối thuyền thông được với nhau ngay cả khi chúng sử dụng các biểu diễn dữ liệu khác nhau. Để làm 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, đó là:
 - + Cú pháp dùng bởi thực thể ứng dụng Nguồn
 - + Cú pháp dùng bởi thực thể ứng dụng Đích
 - + Cú pháp được dùng giữa các thực thể tầng trình diễn.

* Dịch vụ của tầng Phiên:

Tầng phiên có hai loại dịch vụ cơ bản

- Dịch vụ loại thứ nhất: dùng để biểu diễn dữ liệu của người dùng (dữ liệu cục bộ) thành dạng dữ liệu chung.

Các nhiệm vụ của loại 1:

- + Thương lượng về cú pháp truyền: với mỗi kiểu dữ liệu người dùng 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 sẽ được chuyển đổi từ biểu diễn theo cú pháp truyền sang biểu diễn của người sử dụng.
- Dịch vụ loại thứ hai: cho phép các thực thể ứng dụng có thể sử dụng các dịch vụ tầng phiên để quản lý hội thoại.

Tầng 7 (application - ứng dụng):

Là tầng cao nhất của mô hình OSI, tầng ứng dụng trên giải quyết các kỹ thuật mà các chương trình ứng dụng có thể trao đổi với mạng.

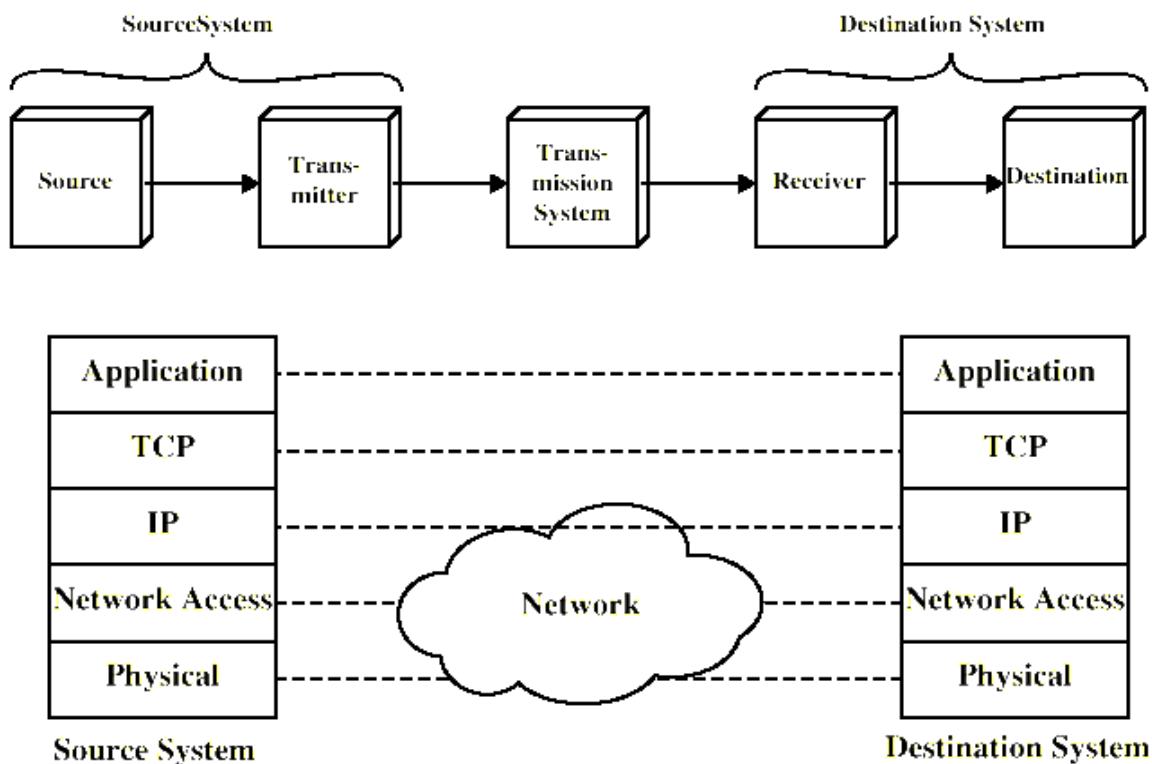
Tầng này phục vụ trực tiếp cho người sử dụng trên mạng với các dịch vụ mạng và phương tiện cần thiết để truy cập môi trường OSI.

2.3 Mô hình tham chiếu TCP/IP

Bộ giao thức TCP/IP phát triển bởi trung tâm nghiên cứu công nghệ cao cấp bộ quốc phòng Mỹ (DARPA) cho hệ thống mạng chuyển mạch giao. Nó được sử dụng bởi mạng Internet toàn cầu (global Internet). Bộ giao thức TCP/IP có thể được xem gồm các tầng sau:

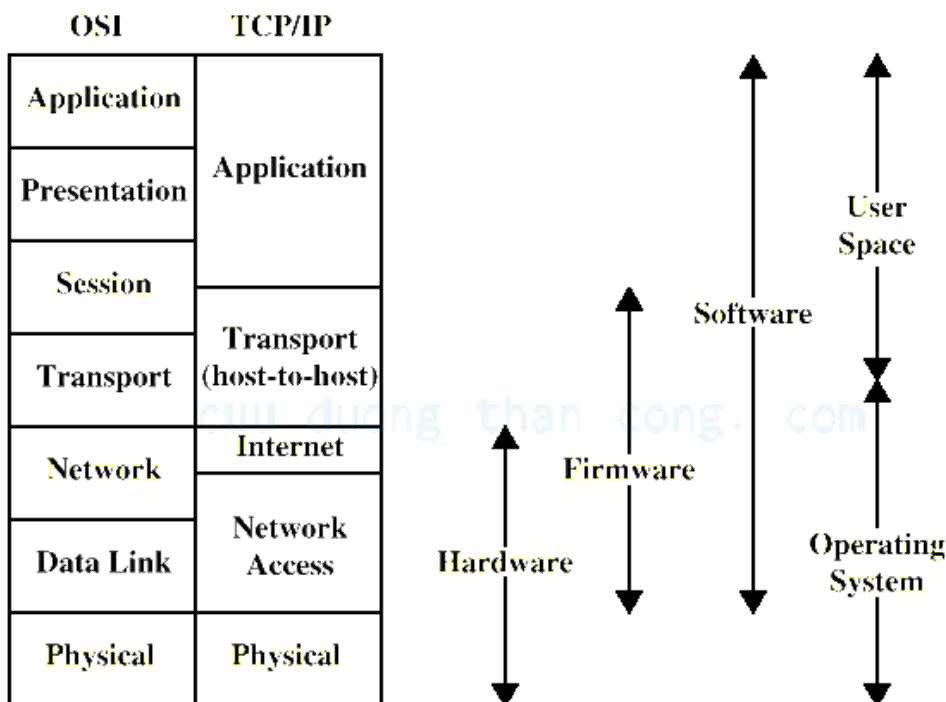
- Tầng ứng dụng (Application layer)
 - Hỗ trợ cho các ứng dụng người sử dụng
 - chẳng hạn như : http, SMTP,...
- Tầng Host to Network hoặc Transport (giao vận)
 - Đảm bảo việc truyền dữ liệu tin cậy
 - Nhận dữ liệu theo đúng thứ tự truyền.
- Tầng Internet (Internet layer)
 - Các hệ thống có thể kết nối được với các mạng khác nhau
 - Các chức năng truyền thông xuyên suốt các mạng đa kênh
 - Được cài đặt ở các end system và router
- Tầng truy cập mạng (Network Access Layer)
 - Trao đổi dữ liệu giữa các hệ thống đầu cuối (end system) và mạng.
 - Kiểm soát địa chỉ đích.
 - Tùy chỉnh dịch vụ.
- Tầng vật lý (Physical layer)
 - Giao tiếp vật lý giữa các thiết bị truyền dữ liệu và môi trường truyền thông hoặc mạng.
 - Đặc tính của môi trường truyền thông
 - Cốc mức tín hiệu
 - Tốc độ truyền dữ liệu
 - ...

Sau đây là mô hình kiến trúc giao thức TCP/IP.



cuu duong than cong. com

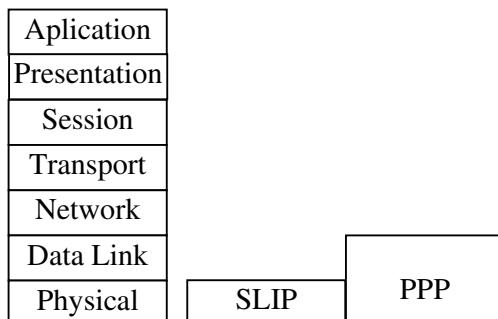
* So sánh với mô hình tham chiếu OSI:



2.4 Một số chuẩn mạng

2.4.1 SLIP và PPP

SLIP là một giao thức đầu tiên (RFC 1055) dùng để chuyển tiếp các gói tin (IP Packets) qua đường truyền quay số (Dial-up lines). Đến nay thì SLIP hoàn toàn bị thay thế bởi PPP (Point-to-Point Protocol). PPP là một giao thức phân tầng (a layered protocol) được thiết kế để hỗ trợ việc thiết lập liên kết để truy cập mạng bằng quay số cho nhiều bộ giao thức truyền tải khác nhau. SLIP là giao thức đơn giản hoạt động như ở tầng vật lý, PPP là một giao thức tăng cường hoạt động giống như tầng vật lý và tầng liên kết dữ liệu. Các hệ điều hành của Microsoft hỗ trợ cả SLIP và PPP ở máy trạm nhưng server chỉ hỗ trợ PPP.



Mối quan hệ giữa SLIP, PPP

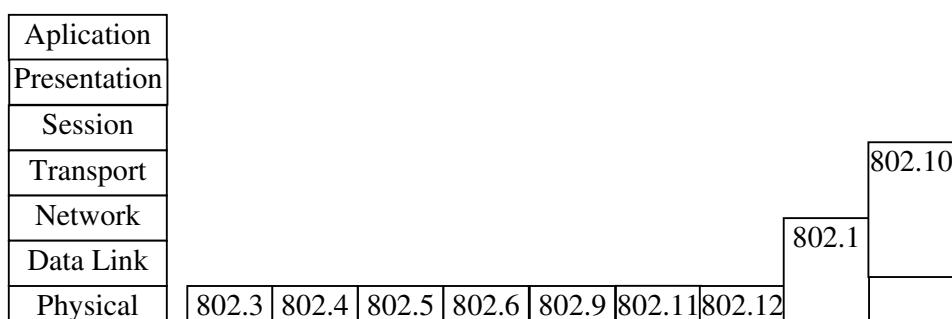
và mô hình OSI

- SLIP được sử dụng trên các hệ thống cũ, chỉ hỗ trợ giao thức TCP/IP và chỉ hoạt động trên hệ thống sử dụng địa chỉ IP tĩnh.

- PPP hỗ trợ giao thức TCP/IP, NetBeui, IPX, AppleTalk và cả DECNet, hỗ trợ các giao thức hỗn hợp. PPP hoạt động cả trên hệ thống dùng địa chỉ tĩnh (static) và động (DHCP).

2.4.2 Bộ tiêu chuẩn IEEE 802

Họ tiêu chuẩn IEEE do Viện kỹ thuật điện tử đưa ra, những tiêu chuẩn này hướng về việc kết nối giữa card giao diện mạng (NIC) và các phương tiện truyền. Những tiêu chuẩn này đã được thông qua hệ thống ISO, họ tiêu chuẩn này bao gồm:



Mối quan hệ giữa các tiêu chuẩn IEEE
NET 802 và mô hình OSI

IEEE 802.1 (High Level Interface): Tiêu chuẩn này đi với tầng Data Link của mô hình OSI, đây là một chuẩn tổng quát cho quản trị mạng và cung cấp các chuẩn quản trị mạng cho các tiêu chuẩn 802 khác.

IEEE 802.2 (Logical Link Control): Tiêu chuẩn này định nghĩa một lớp phụ LLC được sử dụng bởi các giao thức tầng thấp hơn. Các giao thức tầng mạng có thể được thiết kế độc lập trong cả tầng vật lý và sự thực hiện ở lớp phụ MAC, tiêu chuẩn này ít được sử dụng..

IEEE 802.3 (CSMA/CD): Tiêu chuẩn này được phát triển bởi Digital, Intel, Xerox, tiêu chuẩn này định nghĩa các tính chất có liên quan tới tầng con MAC. Lớp con MAC sử dụng kiểu truy cập tranh chấp Carrier Sense Multiple Access with Collision Detection (CSMA/CD). Kỹ thuật này làm giảm sự tác động của xung đột bằng cách giúp cho mỗi thiết bị trong mạng xác định được nó có đang ở trạng thái tĩnh hay không, một thiết bị sẽ thử truyền đi khi nào mạng đang thu động. Khi các thiết bị truyền đi, chúng tiếp tục xem xét rằng nó có đề xảy ra xung đột hay không. Khi có xung đột xảy ra, tất cả các thiết bị đều ngừng truyền và gửi một tín hiệu “jamming” giúp thông báo tất cả các trạm khác về sự xung đột này. Sau đó mỗi thiết bị chờ một khoảng thời gian ngẫu nhiên trước khi truyền thử lại.

IEEE 802.4 (Token Bus): Tiêu chuẩn này định ra một mạng với các giao thức BUS vật lý mà điều khiển sự truy cập các phương tiện với một cơ cấu dấu hiệu. Tiêu chuẩn này được thiết kế để đáp ứng nhu cầu của hệ thống tự động công nghiệp, tiêu chuẩn này ít được sử dụng.

IEEE 802.5 (Token ring): Tiêu chuẩn này bắt nguồn từ IBM, mạng này dùng cấu trúc ring topology và điều khiển phương tiện dựa theo vòng

IEEE 802.6 (Metropolitan Area Network - MAN): Tiêu chuẩn này định nghĩa một tiêu chuẩn MAN gọi là Distributed Queue Dual-Bus (DQDB), DQDB thích hợp với việc truyền dữ liệu, giọng nói và video. Mạng này dựa vào dây cáp quang trong bus topology hai hàng, khả năng tải trên mỗi bus đều được điều khiển nhiều chiều, tiêu chuẩn này ít được sử dụng.

IEEE 802.7 (Broadband Technical Advisory Group): Tiêu chuẩn này giúp giải quyết những giải pháp về băng tần rộng tích hợp trong môi trường mạng, tiêu chuẩn này hiện vẫn đang được phát triển.

IEEE 802.8 (Fiber Optic Technical Advisory Group): Tiêu chuẩn này giải quyết các phương pháp bù xung kỹ thuật cáp quang vào trong môi trường mạng.

IEEE 802.9 (Integrated Data and Voice Networks): Tiêu chuẩn này hỗ trợ kênh truyền bất đồng bộ 10 Mbps cùng với kênh 9664 Kbps dành cho dòng dữ liệu riêng biệt. Tiêu chuẩn này được gọi là Isochromous Ethernet (IsoEonet).

IEEE 802.10 (Standards for Interoperable LAN Security): Tiêu chuẩn này giải quyết những vấn đề về tính bảo mật và mã hóa, hiện đang được phát triển.

IEEE 802.11 (Wireless LAN): Là tiêu chuẩn cho mạng cục bộ LAN không dây, Phương thức CSMA/CD đã được phê chuẩn, hiện đang được phát triển.

IEEE 802.14: Tiêu chuẩn này dùng cho việc truyền dữ liệu qua đường dây cáp TV, tiêu chuẩn này vẫn đang được phát triển nhằm tiếp cận Internet qua đường truyền TV.

IEEE 802.3 và IEEE 802.5 media: Tiêu chuẩn này mô tả tính năng và mục đích của các phương tiện sử dụng trong IEEE 802.3 và IEEE 802.5. IEEE 802.2 độc lập về topology, IEEE 802.3 dựa trên ethernet, IEEE 802.5 dựa trên ring topology là những tiêu chuẩn thông dụng nhất của IEEE 802. Tiêu chuẩn IEEE 802.3 mô tả các phương pháp tín hiệu (cả trên băng tần cơ sở và băng tần rộng), tốc độ dữ liệu, các phương tiện và cấu trúc liên kết. Tiêu chuẩn này quy định cụ thể các phương tiện truyền dẫn vật lý như cáp xoắn, cáp đồng trực, cáp quang.

2.4.3 NDIS và ODI

Tiêu chuẩn NDIS (network driver interface specification), được phát triển bởi Microsoft và 3COM, tiêu chuẩn này mô tả giao diện giữa giao thức vận chuyển mạng và trình điều khiển mạng của tầng datalink. NDIS có chức năng cung cấp một ranh giới trung gian giữa **người cung cấp giao thức vận chuyển** và **bộ điều khiển card mạng**, để các nhóm giao thức tương thích NDIS có thể hoạt động với card mạng. NDIS định nghĩa một phương pháp kết hợp các giao thức hỗn hợp thành một trình điều khiển đơn để bộ điều khiển có thể hỗ trợ đồng thời các giao tiếp.

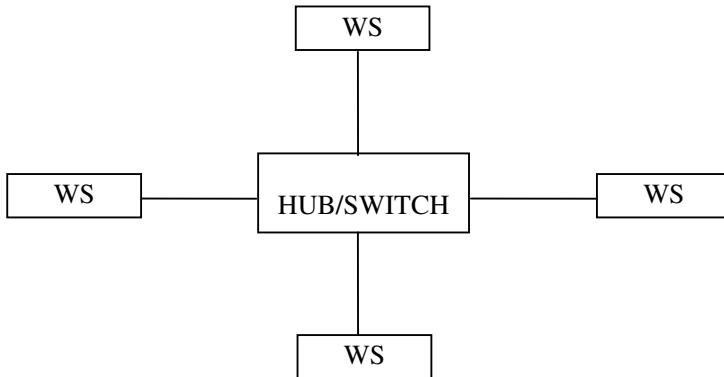
ODI (open datalink interface), phát triển bởi Novell và Apple, hoạt động cùng chức năng như NDIS. ODI cung cấp những qui tắc giúp thiết lập một **giao diện trung gian với người cung cấp, giữa nhóm giao thức và trình điều khiển card mạng**. Giao diện này cũng giúp cho một hay nhiều trình điều khiển mạng có thể hỗ trợ một hay nhiều giao thức.

NDIS và ODI là những tiêu chuẩn giúp cho card mạng hoạt động tốt trong môi trường của hệ điều hành.

§ 3. HÌNH TRẠNG MẠNG (NETWORK TOPOLOGY)

Máy tính và thiết bị xử lý thông tin khác có thể nối với nhau tạo thành một mạng gọi chung là mạng máy tính. Cách nối các máy tính và tập hợp các qui tắc mà tất cả các thực thể tham gia truyền thông trên mạng phải tuân theo để mạng có thể hoạt động được được gọi là kiến trúc mạng. Cách nối các máy tính được gọi là hình trạng (topology) của mạng. Topology của mạng được áp dụng cho mạng cục bộ (LAN) hoặc là mạng diện rộng, trong thực tế chỉ có những mạng máy tính với qui mô nhỏ là áp dụng một topology nào đó, những mạng máy tính lớn thường được tổ chức theo những topology hỗn hợp. Các kiểu topology dưới đây là các kiểu cơ bản.

3.1. Star topology



ở dạng hình sao, tất cả các máy trạm đều nối trực tiếp vào bộ điều khiển trung tâm có nhiệm vụ nhận tín hiệu từ các trạm và chuyển tín hiệu đến trạm đích.

Tùy theo yêu cầu truyền thông trong mạng, thiết bị truyền thông có thể là một bộ chuyển mạch (SWITCH), một bộ chọn đường (Router) hoặc chỉ đơn giản là một bộ phân kẽm (HUB).

Vai trò của bộ trung tâm này là liên kết điểm-điểm (point-to-point) giữa các máy trong mạng.

- **Ưu điểm :**
 - + Lắp đặt đơn giản.
 - + Dễ dàng cấu hình lại (thêm, bớt máy trạm).
 - + Dễ dàng kiểm soát và khắc phục sự cố.
 - + Tận dụng được tối đa tốc độ của đường truyền vật lý.
- **Nhược điểm:**
 - + Độ dài của đường truyền nối từ một máy trạm tới trung tâm bị hạn chế.
 - + Khi bộ điều khiển trung tâm có sự cố sẽ ảnh hưởng đến toàn mạng.
 - + Cần nhiều cáp hơn dạng bus

3.2. Bus topology

ở dạng BUS tất cả các máy trạm phân chia chung một đường truyền chính (bus). Đường truyền chính được giới hạn hai đầu bởi một loại đầu nối đặc biệt gọi là **Terminator**. Mỗi trạm được nối vào bus qua một đầu nối chur T (T-connector) hoặc một bộ thu phát (Transceiver).

Khi một trạm truyền dữ liệu, tín hiệu được quảng bá (broadcast) trên hai chiều của bus, có nghĩa là mọi trạm còn lại đều có thể nhận tín hiệu trực tiếp.

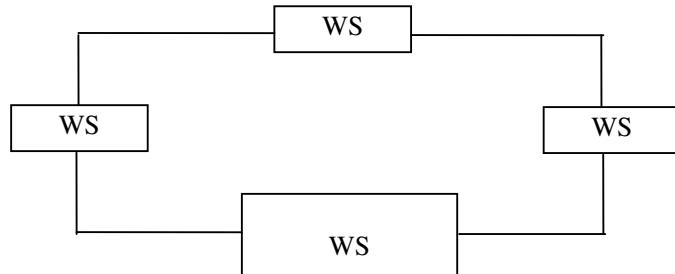
Đối với các bus một chiều thì tín hiệu chỉ đi về một phía, lúc đó terminator phải thiết kế sao cho các tín hiệu phải được “dội lại” trên bus để có thể đến được các trạm còn lại ở phía bên kia.

Như vậy, trong bus topology thì dữ liệu được truyền dựa trên các liên kết điểm-nhiều điểm(point-to-multipoint) hay quảng bá (broadcast).

- **Ưu điểm:** Lắp đặt đơn giản, sử dụng ít cáp.

- Nhược điểm: Khi có sự cố trên đường truyền thì toàn mạng ngừng hoạt động.

3.3. Ring topology (vòng)



Ở dạng vòng mỗi máy trạm được nối với vòng qua một bộ chuyển tiếp (repeater) có nhiệm vụ nhận tín hiệu rồi chuyển đến trạm kế tiếp trên vòng. Như vậy ở dạng này tín hiệu được lưu chuyển trên vòng theo một chiều duy nhất, một chuỗi liên tiếp các liên kết điểm-điểm giữa các repeater.

Giao thức sử dụng cho dạng mạng này là “chuyển thẻ bài” (token passing) để cấp phép truy cập đường truyền.

- Nhược điểm:
- + Đoạn nối giữa hai trạm hỏng sẽ ảnh hưởng đến toàn mạng.
- + Kiến trúc lại mạng khó (thêm, bớt các máy trạm).
- + Giao thức truy cập đường truyền phức tạp.

§ 4. CÁC THIẾT BỊ LIÊN KẾT MẠNG

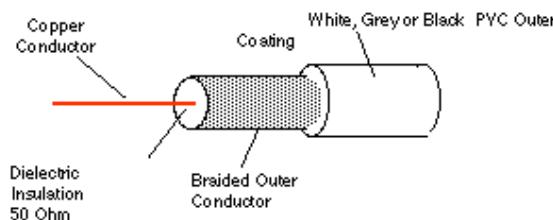
4.1. Dây cáp mạng

Dây cáp đóng vai trò là phương tiện truyền tín hiệu giữa các nút mạng, có nhiều loại cáp nhằm đáp ứng qui mô của nhiều loại mạng khác nhau. Có một số loại cáp thường được như sau.

- Cáp đồng trục (coaxial cable):

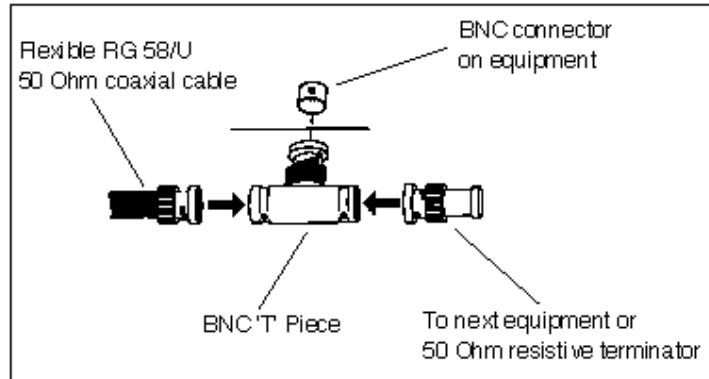
Có độ ảnh hưởng nhiễu thấp, có thể truyền tín hiệu với tốc độ cao trên khoảng cách lớn. Cáp đồng trục có thể dùng cho giải tần cơ sở (Baseband) và giải tần rộng (Broadband).

+ Cáp gầy (thin coaxial cable - 10B2 / IEEE 802.3a): trở kháng 50Ω , có thể đưa tín hiệu đi xa đến 185 mét.

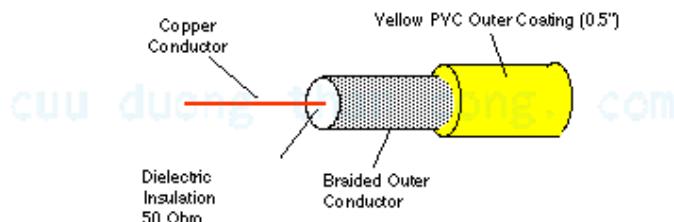


10B2 Cable or "Thin Ethernet"

+ Cáp béo (thick coaxial cable - 10B5): có thể đưa tín hiệu đi xa đến 500 mét. Cáp đồng trục sử dụng các bộ nối cáp BNC để tạo kết nối giữa cáp và máy tính, giữa cáp và đoạn cáp khác. Bộ nối gồm có: bộ nối hình chữ T (T-



connector) để nối cáp và card mạng; bộ nối ống để nối giữa hai đoạn cáp (BNC-connector) ; bộ nối cuối (Terminator).

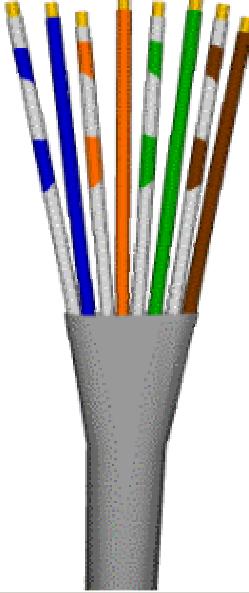


10B5 Cable or "Thick Ethernet"

- Cáp không vỏ chống nhiễu (UTP):

Dây cáp điện thoại có thể sử dụng để truyền dữ liệu khi tín hiệu được lọc nhiễu và khoảng cách không lớn lắm. Với loại cáp này mức độ chống nhiễu, khoảng cách truyền, giải tần cũng như số thiết bị gắn vào được xếp ở mức trung bình. Khi truyền ở mức độ cao (1Mbps) nó tạo ra sóng RF, do đó phải sử dụng thêm các bộ lọc cần thiết. Cáp xoắn đôi tròn 10BASE-T có thể đưa tín hiệu đến 100 mét. Cáp xoắn đôi dùng giắc cắm RJ45.

Wire pair #1:	White/Blue Blue
Wire pair #2:	White/Orange Orange
Wire pair #3:	White/Green Green
Wire pair #4:	White/Brown Brown

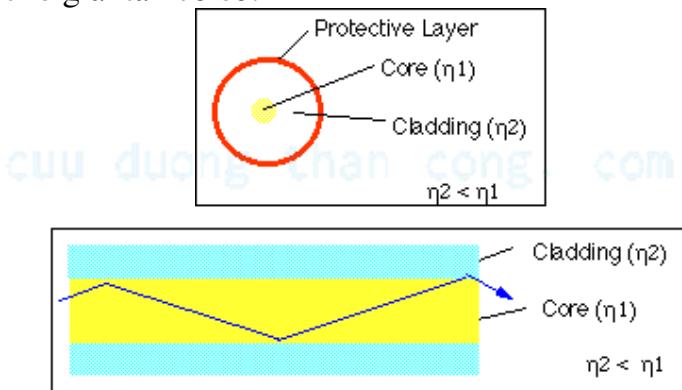


- Cáp có vỏ bọc chống nhiễu (STP)

Là loại cáp có 1 hoặc hai đôi dây nằm trong vỏ bọc kim loại, vỏ bọc giảm nhiễu và giảm phát sinh sóng RF do đó nó cho phép truyền dữ liệu ở tốc độ cao hơn trên khoảng cách lớn hơn loại UTP.

- Cáp quang 10BASEFL, 10BASEFB (công nghệ cao hơn, cho phép truyền tín hiệu đồng bộ)

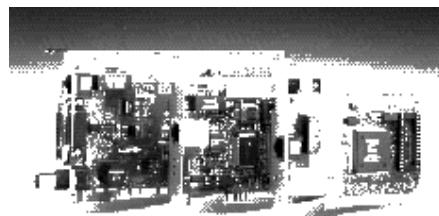
Trong cáp sợi quang, sợi quang truyền tín hiệu dữ liệu dưới dạng số ở hình thái xung ánh sáng. Cáp này không bị ảnh hưởng nhiễu điện, lý tưởng cho cáp chạy ngoài trời hoặc gần những nguồn điện cao thế. Có khả năng truyền dữ liệu với tốc độ rất lớn (hàng trăm đến hàng nghìn Mbps), là giải pháp tốt cho đường truyền tốc độ cao, làm đường trực (backbone) cho mạng. Cáp quang thường được sử dụng cho giải tần cơ sở.



4.2. Vỉ mạch mạng (Network Interface Card - NIC)

Là thiết bị được lắp đặt vào khe mở rộng (expansion slot) của máy tính (có thể được tích hợp trên MainBoard), nó đảm nhiệm truyền dữ liệu từ bus dữ liệu

của một nút (node) (pc, server, printer,...) tới một nút khác trong mạng. Vai trò của NIC là chuẩn bị dữ liệu, gửi dữ liệu đến nút mạng khác, kiểm soát luồng dữ liệu giữa máy tính và hệ thống cáp.



Chuẩn bị dữ liệu: NIC phải chuyển đổi dữ liệu từ dạng thức mà máy tính có thể hiểu được sang dạng thức có thể truyền qua dây cáp mạng. Dữ liệu di chuyển qua một máy tính theo các tuyến gọi là BUS, có thể có nhiều tuyến (8 bits, 16 bits, 32 bits) cùng được truyền dữ liệu dọc theo các tuyến này, gọi là truyền song song. Có một số kiến trúc bus thường dùng như : ISA (16 bit dữ liệu, 32 bit địa chỉ); EISA (32 bit dữ liệu, 16 hoặc 32 bit địa chỉ); PCI (32 hoặc 64 bit dữ liệu, địa chỉ).

Trên cáp mạng, dữ liệu phải đi theo một luồng bít đơn lẻ, dữ liệu được truyền theo một hướng bít này nối đuôi bít kia, gọi là truyền nối tiếp. NIC tiếp nhận tín hiệu chạy song song, sắp xếp lại để có thể truyền nối tiếp theo tuyến rộng một bít của cáp mạng. Việc thực hiện chuyển dịch tín hiệu số của máy tính sang tín hiệu điện và tín hiệu quang do một thiết bị chịu trách nhiệm thi hành gọi là máy thu – phát (Transceiver, transmitter/receiver).

Gửi và kiểm soát dữ liệu: Trước khi NIC ở đầu gửi dữ liệu, nó tiến hành kiểm tra với NIC ở đầu nhận để cả hai cùng thống nhất các tham số:

- + Kích thước tối đa của cụm dữ liệu được gửi
- + Lượng dữ liệu được gửi đi trước khi được xác nhận
- + Thời gian cách quãng giữa những lần gửi dữ liệu
- + Thời gian chờ trước khi tín hiệu báo nhận được gửi đi
- + Mỗi NIC chứa được bao nhiêu dữ liệu
- + Vận tốc truyền dữ liệu
- Các tùy chọn và xác lập cấu hình
- + Ngắt (IRQ)
- + Địa chỉ cổng xuất/ nhập (I/O) cơ sở
- + Địa chỉ bộ nhớ
- + Máy thu – phát (qua giắc cắm RJ45, BUS, AUI)

4.3. Bộ phát lặp (Repeater)

Thiết bị trung gian thực hiện chức năng chuyển tiếp ở mức vật lý, nó có tác dụng khuếch đại tín hiệu trên đường truyền do đó được sử dụng để kéo dài cáp mạng. Nó không thể sử dụng để nối các mạng có công nghệ khác nhau.

Bộ phát lặp hoạt động tại tầng vật lý, nó tiếp nhận tín hiệu từ một đoạn mạng tái tạo và truyền đến đoạn mạng kế tiếp. Muốn chuyển gói dữ liệu qua bộ phát lặp từ đoạn mạng này sang đoạn mạng kế tiếp, gói dữ liệu và giao thức Logical Link Control (LLC) phải giống nhau trên mỗi đoạn mạng. Bộ phát lặp không dịch hoặc lọc bất kỳ tín hiệu nào, để thiết bị này có thể hoạt động, cả hai đoạn mạng nối bộ chuyển tiếp phải có cùng phương pháp truy cập.

4.4. Bộ tập trung (Hub)

Là trung tâm của mạng hình sao (điểm tập trung các đầu dây trong mạng). Hub nhận tín hiệu tại một cổng (port) và lặp lại tín hiệu đó (relay and/or amplify/generate signal) trên tất cả các cổng (port) còn lại. Tại mỗi thời điểm chỉ có một trạm được chuyển dữ liệu. Vì vậy một hub 10Mbps thì có tốc độ tổng cộng là 10Mbps.



8-port 3Com Office Connect Hub

- Hub thụ động (passive hub): chúng đóng vai trò như điểm kết nối và không khuếch đại (amplify) hay tái tạo (generate) tín hiệu.
- Hub chủ động (Active hub): tái tạo và truyền lại tín hiệu theo cách tương tự cách thức vận hành của bộ chuyển tiếp (Repeater).
- Hub lai (hybrid hub): công nghệ cải tiến chấp nhận nhiều loại cáp khác nhau, có thể mở rộng mạng bằng cách liên kết nhiều hub.

Hub là thiết bị đa năng có nhiều tính năng có thể dùng trong Topology: Star, Star-Bus, Star-Ring. Khi thay đổi hoặc mở rộng hệ thống, đường dây sẽ ít ảnh hưởng đến hoạt động của mạng. Thiết bị Hub có thể để tập trung, tiện cho quá trình bảo dưỡng quản lý mạng.

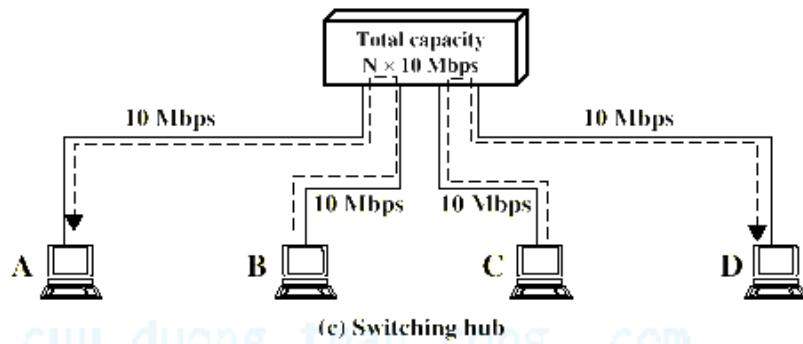
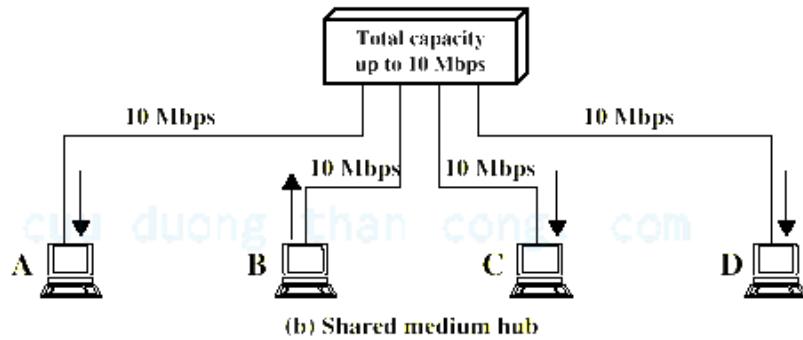
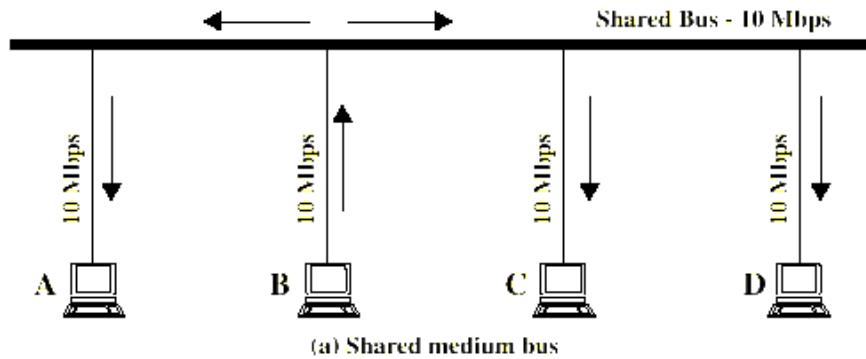
4.5. Chuyển mạch (Switch)

Chuyển mạch được phát triển để thiết kế cho mạng nhiều đoạn, hoặc các mạng máy tính. Chuyển mạch cho phép nối mạng với nhau ở tốc độ cao.

Switch nhận tín hiệu từ một cổng và chuyển tiếp tín hiệu đến cổng kết nối với thiết bị đích. Tại mỗi thời điểm có thể có nhiều hơn một trạm truyền dữ liệu. Vì vậy một switch 10Mbps thì có tốc độ tổng cộng có thể là 10Mbps, 20Mbps, ... qua đó ta thấy tốc độ truyền dữ liệu của một switch trên mạng hiệu quả hơn hub (tham khảo hình vẽ mô tả việc truyền dữ liệu sau).

Chuyển mạch Ethernet: được thiết kế để phân chia mạng thành các segment để tăng giải thông cho từng segment. Các chuyển mạch hiện nay có thể sử dụng ở mạng tốc độ cao như Fast Ethernet, FDDI/CDDI hoặc ATM.

Chuyển mạch cho mạng diện rộng (WAN): được thiết kế để nối các mạng cục bộ thành mạng diện rộng.



4.6. Cầu nối (Bridge)

Nối các đoạn mạng phân biệt lại với nhau và truyền dữ liệu qua lại giữa chúng. Nó cho phép mở rộng kích thước tối đa của mạng khi gặp giới hạn như chiều dài cáp, giới hạn về số lượng trạm.

Cầu nối hoạt động tại tầng Data Link (thuộc tầng con Media Access Control) nên nó không hiểu được các thông tin ở tầng cao hơn. Do vậy nó không phân biệt giao thức này với giao thức khác, cầu nối có nhiệm vụ chuyển tất cả các

giao thức đọc theo mạng. Khi chuyển dữ liệu qua mạng, tùy thuộc vào từng máy tính quyết định chúng có thể nhận giao thức nào. Cầu nối có nhiệm vụ:

- + Lắng nghe các lưu thông trên mạng
- + Kiểm tra địa chỉ nguồn và địa chỉ đích của mỗi gói dữ liệu
- + Xây dựng bảng định tuyến
- + Gói dữ liệu được chuyển theo cách sau: Nếu đích đến không được liệt kê trong bảng định tuyến cầu nối sẽ chuyển dữ liệu đến mọi đoạn mạng. Nếu đích đến được liệt kê, cầu nối sẽ chuyển gói dữ liệu đến đoạn mạng đó. Cầu nối hoạt động trên nguyên tắc mỗi nút mạng có địa chỉ riêng. Một cầu nối chuyển đi các gói dữ liệu dựa trên địa chỉ nút đến.

4.7. Bộ định tuyến (Router)

Bộ định tuyến làm việc tại tầng 3 trong mô hình OSI hay tầng Internet trong mô hình TCP/IP, nó thường được dùng để nối hai hay nhiều đoạn mạng với giao thức và kiến trúc mạng khác nhau. Thiết bị này có chức năng quyết định tuyến đường tốt nhất để truyền dữ liệu và sàng lọc gói tin (Packet filter).

Bộ định tuyến sử dụng bảng định tuyến (routing table) để chứa địa chỉ của các nút mạng, nó sử dụng bảng này để xác định địa chỉ cho dữ liệu đến, bảng này liệt kê các thông tin sau:

- + Toàn bộ số địa chỉ mạng
- + Cách kết nối vào các mạng khác
- + Các lô trình có thể có giữa các bộ định tuyến
- + Phí tổn truyền dữ liệu qua các lô trình đó

Các giao thức định tuyến: DECnet, IP, IPX, OSI, XNS, DDP (AppleTalk)

Các giao thức không hỗ trợ định tuyến: LAT (giao thức của hãng Digital Equipment), NetBEUI.

Bộ dẫn đường chia làm hai loại

- + Tĩnh (static): đòi hỏi người quản trị mạng phải cài đặt và lập cấu hình bảng định tuyến đồng thời tự mình định rõ mỗi lô trình.
- + Động (dynamic): Tự động phát hiện lô trình và do đó được lập cấu hình ít hơn.

4.8. Công kết nối (Getway)

Công kết nối cho phép truyền thông giữa các kiến trúc mạng và môi trường khác nhau. Chúng đóng gói lại và biến đổi gói dữ liệu được truyền từ môi trường này đến môi trường khác, sao cho các môi trường có thể hiểu dữ liệu của nhau. Một kết nối liên kết hai hệ thống không sử dụng cùng giao thức truyền thông, cấu trúc định dạng dữ liệu, ngôn ngữ, kiến trúc mạng.

Cổng kết nối chuyên dùng cho tác vụ cụ thể, chúng được dành riêng cho một truyền tải cụ thể nào đó. Ví dụ cổng kết nối giữa Windows NT, Windows 2000 và SNA. Cổng kết nối tiếp nhận dữ liệu từ môi trường, tước bỏ chòng giao thức cũ và đóng gói chòng giao thức của mạng đích.

Một số cổng kết nối sử dụng toàn bộ 7 tầng của mô hình OSI, nhưng cổng kết nối thường thực hiện việc chuyển đổi giao thức tại tầng Application. Trong thực tế mức độ tính năng thay đổi đáng kể giữa các loại cổng giao tiếp.

§ 5. CÁC GIAO THỨC TRUYỀN TRÊN MẠNG (PROTOCOL)

5.1 Khái niệm

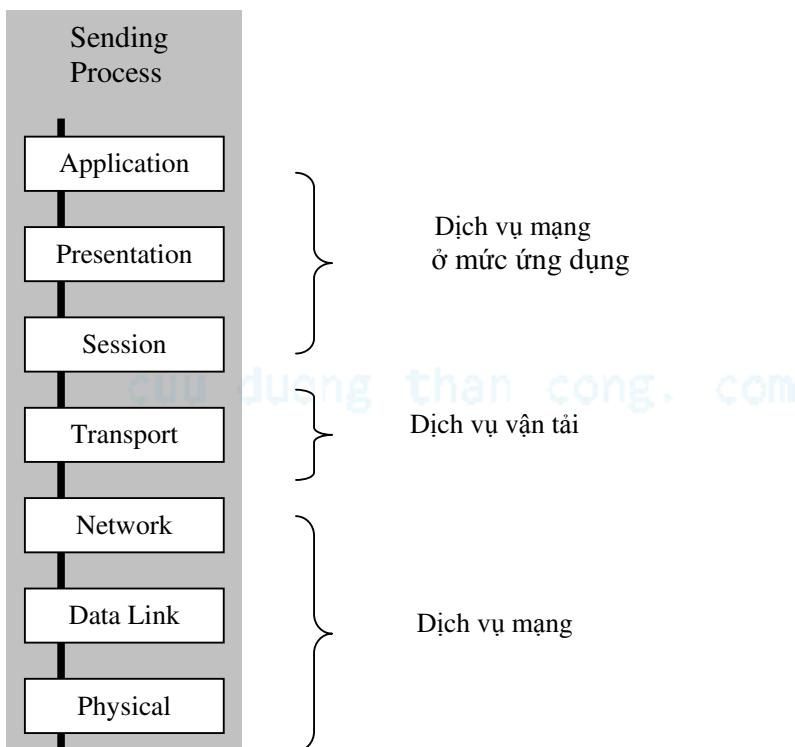
Giao thức là những nguyên tắc và thủ tục điều khiển sự giao tiếp và tương tác khi các máy tính muốn liên hệ với nhau trong môi trường mạng.

Có nhiều giao thức, mỗi giao thức cho phép thực hiện các cuộc giao tiếp cơ bản và thi hành những tác vụ khác nhau.

Một số giao thức hoạt động ở nhiều tầng OSI. Tầng nơi giao thức hoạt động sẽ mô tả chức năng của giao thức đó.

Nhiều giao thức có thể hoạt động phối hợp gọi là chòng giao thức. Cấp độ trong chòng giao thức tương ứng với tầng của mô hình OSI.

Chòng giao thức chuẩn: Giao thức tồn tại ở mỗi tầng của chòng giao thức, làm công việc do tầng đó qui định. Những tác vụ truyền thông cần thi hành qua mạng được gán cho những giao thức đang hoạt động như một trong ba loại giao thức. Ba loại giao thức này ánh xạ đến mô hình OSI



Giao thức ứng dụng:

- FTAM (File Transfer Access and Management): giao thức truy nhập tập tin của mô hình OSI
- X.400: giao thức CCITT cho việc truyền e-mail quốc tế
- X.5000 giao thức CCITT cho dịch vụ tệp tin và thư mục ngang qua nhiều hệ thống
- SMTP (Simple Mail Transfer Protocol): Giao thức Internet cho việc chuyển mail
- FTP (File Transfer Protocol): Giao thức chuyển tệp tin trên Internet
- SNMP (Simple Network Management Protocol): Giao thức Internet cho việc theo dõi mạng và các thành phần mạng
- Telnet : giao thức Internet cho việc đăng nhập máy chủ ở xa và xử lý dữ liệu trên máy cục bộ
- Microsoft SMP (Server Message Block) và shell hoặc bộ đổi hướng (redirector) trên máy khách
- NCP (Novell Netware Core Protocol): và shell hoặc bộ đổi hướng (redirector) trên máy khách của Novell Netware
- Appletalk and Appleshare: Dãy giao thức của Apple
- AFP (Appletalk Filing Protocol): giao thức cho việc truy cập tập tin từ xa của Apple
- DAP (Data Access Protocol): Giao thức truy cập tệp tin Decnet.

Giao thức vận tải:

- TCP (Transmission Control Protocol): giao thức TCP/IP bảo đảm dữ liệu tuần tự
- SPX : một phần của dãy giao thức IPX/SPX (Internetwork Packet Exchange) của Novell Netware
- Nwlink một cài đặt trên IPX/SPX của Microsoft
- NetBEUI (NetBIOS - Network Basic Input/output System) Extended User Interface: thiết lập việc truyền thông giữa các máy tính (Netbios) và cung cấp dịch vụ vận tải dữ liệu (NetBEUI)
- ATP (Appletalk Transaction Protocol), NBP (Name Binding Protocol): Giao thức phiên truyền thông và giao tức vận tải dữ liệu của Apple.

Giao thức mạng

- IP (Internet Protocol)
- IPX: Giao thức của Novell Netware

- Nwlink: một cài đặt trên IPX/SPX của Microsoft
- NetBEUI: Giao thức vận tải cung cấp dịch vụ vận tải dữ liệu cho phiên làm việc và chương trình ứng dụng NetBIOS
- DDP (Datagram Delivery Protocol): Giao thức vận tải dữ liệu của Appletalk

5.2. Các bộ giao thức phổ biến

Trong thực tế các giao thức được dùng phổ biến và được tập hợp thành các giao thức như sau:

1. TCP/IP (transmission Control Protocol / Internet protocol)

- Là giao thức chuẩn cho các hệ trên cơ sở UNIX, đặc biệt sử dụng cho mạng Internet. TCP/IP hỗ trợ việc định tuyến (routing), là giao thức chuẩn cho khả năng liên kết hoạt động của nhiều loại máy tính.

- Mỗi card mạng được gán địa chỉ Internet hay địa chỉ IP
- Địa chỉ IP được phân thành 4 lớp (A B C D)

- TCP/IP là một tập hợp nhiều giao thức nó là tiêu chuẩn thực tế cho liên mạng:

- + FTP (File Transfer Protocol) một ứng dụng để truyền file giữa các máy
- + SMTP (Simple Mail Transfer Protocol) hệ thống thư điện tử
- + SNMP: quản lý mạng

2. IPX/SPX

Giao thức trao đổi thông tin trên mạng của hãng Novell. IPX sử dụng phương thức truyền gói dữ liệu và nguyên tắc tìm đường theo chuẩn IEEE 802.3 , hỗ trợ định tuyến

3. NetBIOS (Network basic input/output system)

Giao thức này được sử dụng trên mạng với các ứng dụng của IBM, Microsoft, và Lotus.

- Chuẩn của IBM về giao diện chương trình cho mạng máy tính
- Cơ sở là ngang hàng
- Nó là giao thức định hướng cho việc nối mạng, không có mức mạng
- Không có giao thức tìm đường
- Kiểm tra được luồng thông tin

Quy tắc của NetBIOS không quy định chặt chẽ về phần cứng, phần mềm, giao thức hay đường truyền vật lý mà mạng sử dụng.

NetBEUI (NetBIOS Extended User Interface): Giao thức kèm theo sản phẩm mạng của Microsoft.

§ 6. THIẾT KẾ MẠNG CỤC BỘ

6.1. Qui tắc thiết kế mạng:

Khoảng cách tối đa cho từng đoạn mạng tùy theo kiểu đường truyền:

- 10Base5: 500 mét cho đoạn cáp không có bộ phát lắp
- 10Base2: 185 mét cho đoạn cáp không có bộ phát lắp
- 10BaseT: 100 mét
- 10BaseFL, 10BaseFB: 2000 mét

Trong thực tế, khoảng cách tối đa còn phụ thuộc vào môi trường lắp đặt, ví dụ như điều kiện thời tiết... có thể làm giảm khoảng cách thực tế. Hoặc việc sử dụng các thiết bị khác như HUB thông minh có thể làm tăng khoảng cách thực tế.

Xác định số các bộ phát lắp tối đa giữa hai trạm trên mạng:

- Theo Ethernet: một cặp bộ phát lắp được đếm là một bộ lắp, chỉ có 2 bộ lắp trên đường truyền giữa hai trạm bất kỳ.
- Theo IEEE: không lớn hơn 5 đoạn phát lắp, không quá 4 bộ phát lắp giữa hai trạm bất kỳ, trong đó 3 đoạn có thể nối máy trạm (5 segments, 4 repeaters, 3 populated segments)

Số trạm tối đa: Tùy theo kiểu đấu nối mà có được số workstations tối đa

- 10Base5: 100 workstations
- 10Base2: 30 workstations
- 10BaseT: 2 workstations
- 10BaseFL, 10BaseFB: 2 workstations

Mạng nhiều đoạn (Multisegment):

- Đoạn mạng là phần dây cáp được chặn bởi các thiết bị như cầu, bộ dọn đường, bộ phát lắp, terminator. Tác dụng của 1 đoạn và nhiều đoạn

- 1 đoạn mạng:

+ Cấu trúc đơn giản

+ Tốc độ bảo đảm vì không bị trễ (do các thiết bị nối đoạn mạng)

+ Giá thành cho một trạm thấp

+ Lưu lượng thông tin trên mạng lớn, sẽ dẫn đến tình trạng quá tải, ảnh hưởng đến toàn bộ mạng.

+ Khó khăn khi mở rộng mạng.

- Nhiều đoạn mạng:

+ Tăng kích thước mạng và số các thiết bị gắn vào mạng.

+ Tính sẵn sàng của mạng cao: các mạng con được tách biệt cả về logic và vật lý, do vậy lỗi từ đoạn này không làm ảnh hưởng đến đoạn khác.

+ Cung cấp các khả năng kết nối giữa các trạm nằm trên các đoạn mạng khác nhau.

+ Dễ dàng mở rộng mạng

Có thể sử dụng cầu (Bridges) hoặc chuyển mạch (Switches) để nối các đoạn mạng.

6.2. Phương pháp thiết kế :

Thiết kế mạng là chọn ra một cấu hình đúng cho một phương án cụ thể, phải thỏa mãn được mục đích và nhu cầu của người sử dụng, đồng thời thỏa mãn các ràng buộc của hệ thống.

Thu thập các nhu cầu, các thông tin về mạng:

Số lượng người dùng của từng ứng dụng, kiểu ứng dụng. Các thông tin này sẽ được xem xét khi lựa chọn thiết kế phân đoạn mạng, cấu hình của các thiết bị.

Xác định nhu cầu về truyền tin của từng trạm, mối quan hệ giữa các trạm. Khi đó xác định những nhóm người sử dụng.

Xem xét khoảng cách vật lý giữa các trạm trong mạng, 1 tòa nhà hay nhiều. Tùy thuộc vào khoảng cách thực tế mà quyết định phân đoạn mạng bằng cầu, chuyển mạch.

Các thông tin phục vụ cho bản vẽ chi tiết:

- + Số lượng các trạm, vị trí ổ cắm.
- + Vị trí, kích thước của tủ đấu dây
- + Độ dài các đoạn cáp giữa các thiết bị
- + Trạng thái nhà cửa, văn phòng
- Sự phát triển của mạng trong tương lai.

Thiết kế chi tiết:

- Bản vẽ chi tiết về cách mắc dây của mạng: kiến trúc mạng, cấu hình các thiết bị trên mạng.

- + Thiết kế tổng thể.
- + Thiết kế cụ thể từng đoạn mạng, khu vực thiết bị để tập trung.

- Các phần mềm sử dụng trên mạng: hệ điều hành, cơ sở dữ liệu, các ứng dụng...

Một số yêu cầu khác

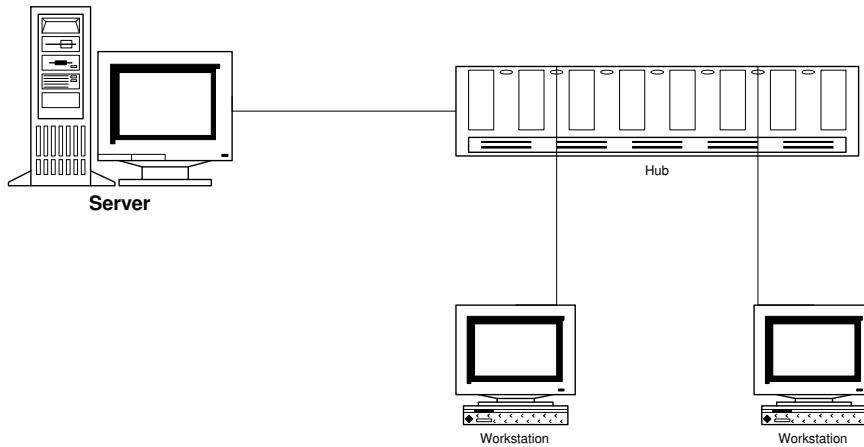
- Qui định về quản lý mạng:

- + Người quản lý mạng: số lượng, vị trí.
- + Các thủ tục phải thực hiện hàng ngày
- + Thủ tục phát hiện và khắc phục sự cố trên mạng
- + Thủ tục lưu trữ dự phòng và khôi phục
- + Theo dõi sử dụng mạng
- + Hướng dẫn người sử dụng tại chỗ
- + Phân phối phần mềm

6.3. Một số thiết kế mạng

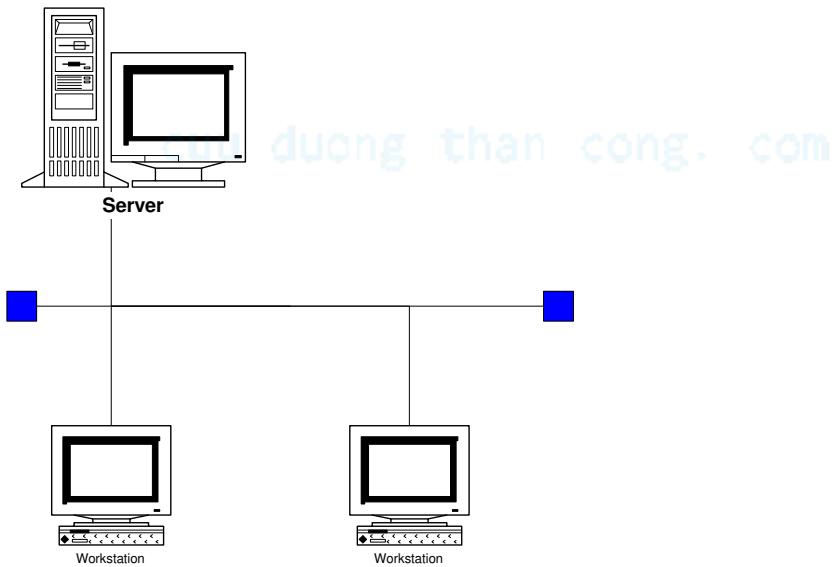
Star Topology : SERVER được nối trực tiếp vào HUB bằng cáp UTP:

Dùng trong mạng nhỏ, bố trí máy tập trung, số lượng trạm phụ thuộc vào số cổng của HUB, có loại Hub 4, 8 ,12, 24 port, ... tùy số lượng máy mà lắp đặt hub phù hợp.



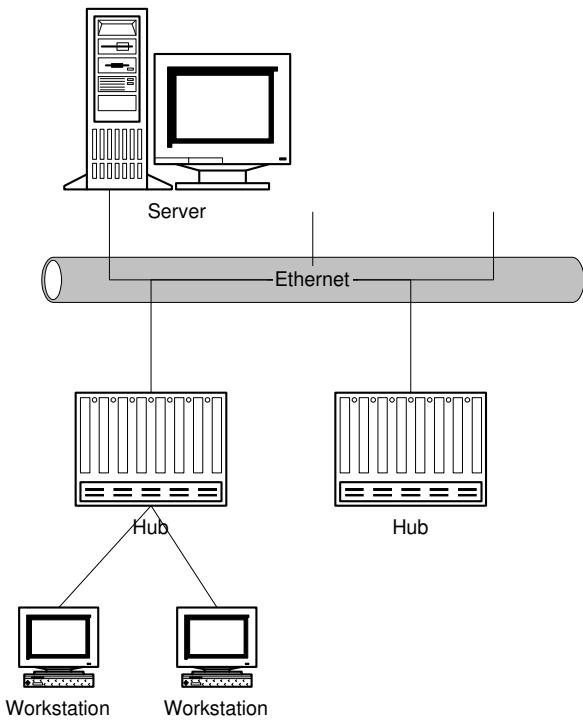
Topology Bus: SERVER nối trực tiếp với các máy bằng cáp BNC

Dùng cho mạng nhỏ, số lượng máy không lớn, thường được dùng cho một văn phòng hoặc một mạng máy tính nhỏ nhưng các máy tính cách nhau khá xa, trong phạm vi cho phép của cáp đồng trục.



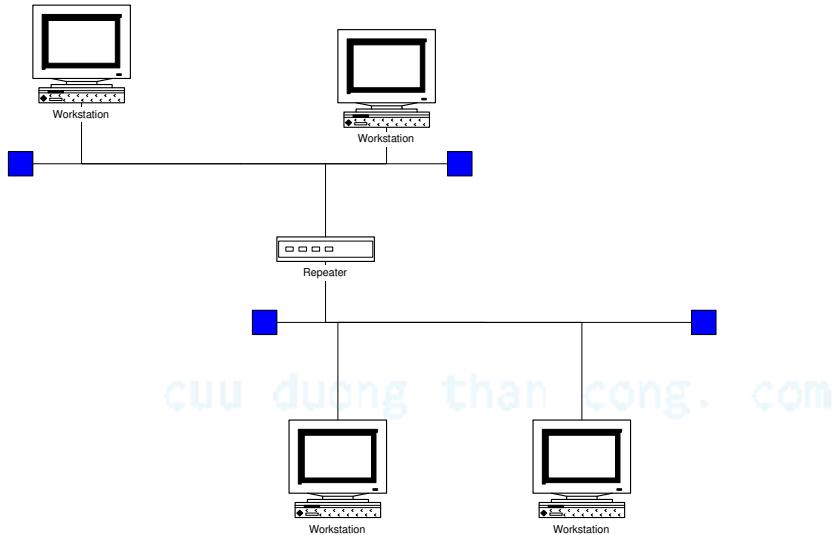
Topology Bus – Star: SERVER nối với HUB - HUB bằng cáp BNC

Dùng cho mạng với qui mô khá lớn, có thể có nhiều phòng máy, các phòng máy lại cách nhau xa (trong phạm vi cho phép của cáp đồng trục), các HUB có thể để ở các phòng khác nhau, mỗi hub có thể cung cấp đường truyền cho 1 hoặc 2 phòng tùy theo số lượng máy.



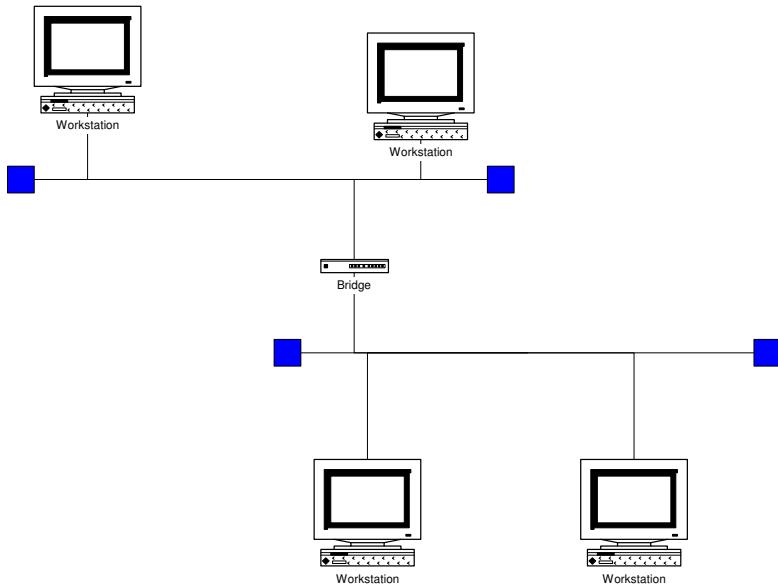
Liên kết hai đoạn mạng bằng Repeater:

Đoạn mạng có thể là 1 tầng nhà hoặc tòa nhà, số lượng máy của mỗi đoạn mạng không lớn lắm, máy trạm để tập trung.



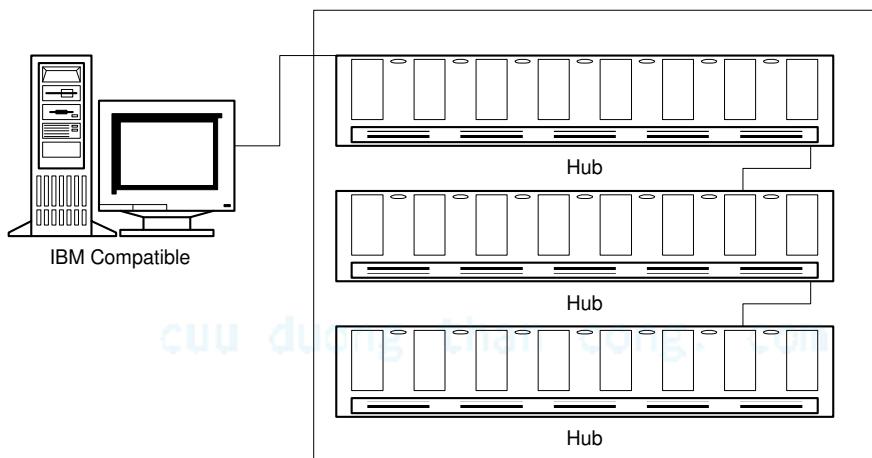
Liên kết hai đoạn mạng bằng Bridge:

Đoạn mạng có cấu trúc mạng khác nhau, mỗi đoạn mạng có thể lắp đặt ở 1 tầng nhà hoặc tòa nhà, mỗi đoạn mạng có thể có số lượng máy khá lớn.



server nối vào các HUB xếp chồng

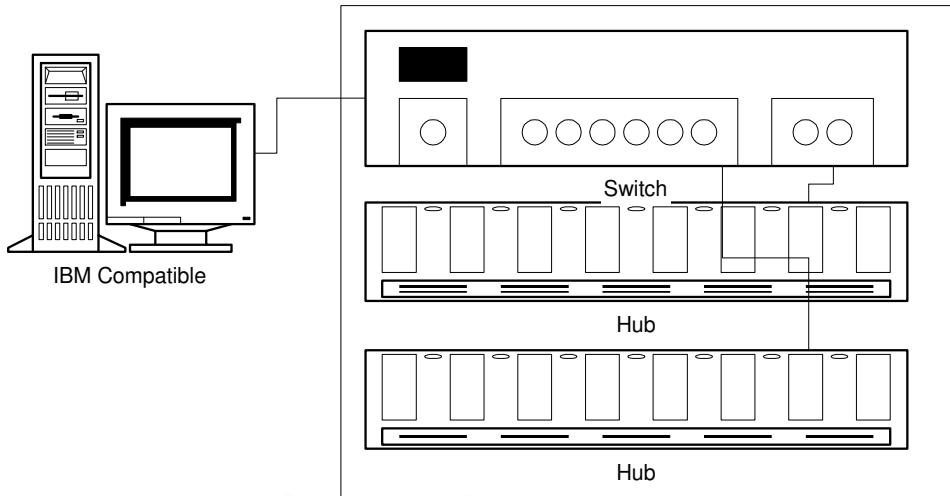
Số lượng máy trạm khá lớn, thường là các máy trạm được để tập trung, khoảng cách máy trong cự ly cho phép, các HUB quản lý tập trung. Tuy nhiên mạng này dùng trong các tổ chức mà lưu lượng thông tin trên mạng không lớn lắm, nếu quá trình truyền tin trên mạng diễn ra liên tục thì người ta thường thiết kế mạng theo mô hình Lan-Switch



Các HUB liên kết qua Switch:

- Switch có nhiệm vụ kết nối các HUB, khi đó Switch có nhiệm vụ quản lý tất cả các đường tín hiệu trên mạng, với cách lắp đặt này có thể cải thiện tốc độ

mạng. Đây là mô hình có thể dùng cho các tổ chức có qui mô máy lớn, các máy trạm đều nằm trong phạm vi nhỏ hơn 150 m so với tủ HUB trung tâm. Theo mô hình này khi cần mở rộng mạng chỉ cần lắp đặt thêm HUB, tuy nhiên số lượng HUB cực đại phụ thuộc vào số cổng ra của Switch. Vì các thiết bị này đặt tập trung nên có thể thiết kế bộ nguồn điện nuôi HUB tập trung, hạn chế sự cố về điện. Tất cả các dây mạng đều tập trung về tủ điều khiển nên cũng dễ dàng xử lý sự cố.



chu duong than cong. com

chu duong than cong. com

PHẦN II

HỆ ĐIỀU HÀNH MẠNG NOVELL NETWARE

§ 1. GIỚI THIỆU MẠNG NOVELL NETWARE

1.1. Sự phát triển của Novell Netware

NOVELL NETWARE được thiết lập năm 1983 với cấu hình tối thiểu và một số dịch vụ đơn giản.

Novell phiên bản 1.X , 2.X, 3.XX được phát hành cho đến năm 1993

Novell phiên bản 4.X được cài đặt quản trị mạng trên hệ thống nhiều FILE SERVER thông qua hệ dịch vụ NDS (Netware Directory Servise) mạng này có thể quản lý trên hệ thống rộng lớn.

Novell 5.X ra đời vào năm 1999, phiên bản này được thiết kế với nhiều tính năng mới, giúp người dùng dễ dàng sử dụng hơn, dễ tích hợp với mạng điện rộng và Internet.

Tài liệu này đề cập đến những nội dung cơ bản của Novell Netware và các chức năng của phiên bản Novell 4.X.

NOVELL NETWARE được dùng rộng rãi trong:

- Các văn phòng: liên kết các bộ phận rời rạc
- Các công ty: liên kết các xí nghiệp thành viên

Novell Netware có thể chạy trên những máy có cấu hình không cao (cả SERVER và WORKSTATION), cài đặt không phức tạp, quản trị mạng đơn giản và có hiệu quả.

Quản trị Novell Netware bao gồm những công việc như sau:

- Quản trị FILE SYSTEM
- Quản trị USER và GROUP
- Quản trị FILESERVER
- Quản trị PRINT SERVICE
- Quản trị các dịch vụ khác

1.2. Novell Directory Services

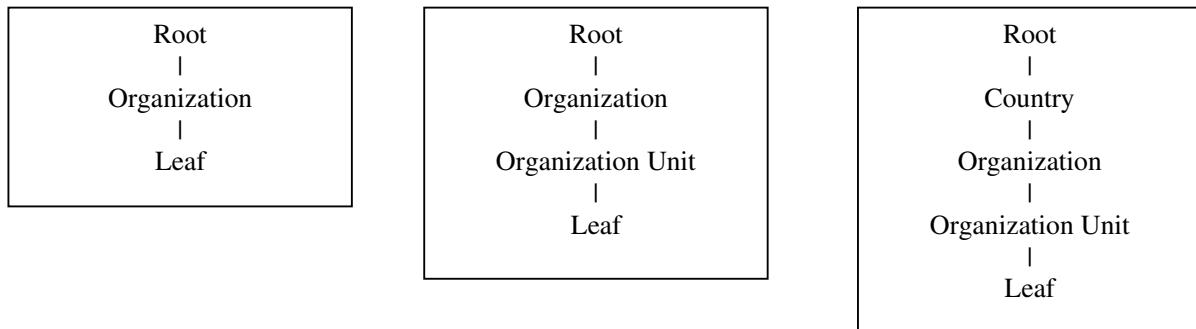
a. Khái niệm

Novell Directory Services (NDS) là dịch vụ đặc trưng của Novell Netware, NDS duy trì cơ sở dữ liệu của tất cả tài nguyên mạng. NDS tạo các mạng thành một mạng thống nhất bằng cách cung cấp một điểm truy nhập và quản lý hầu hết tài nguyên mạng. NDS quản lý tài nguyên theo cấu trúc hình cây, mỗi cây (tree) được đặt tên, nó có thể quản lý nhiều đối tượng (object), có các loại đối tượng sau:

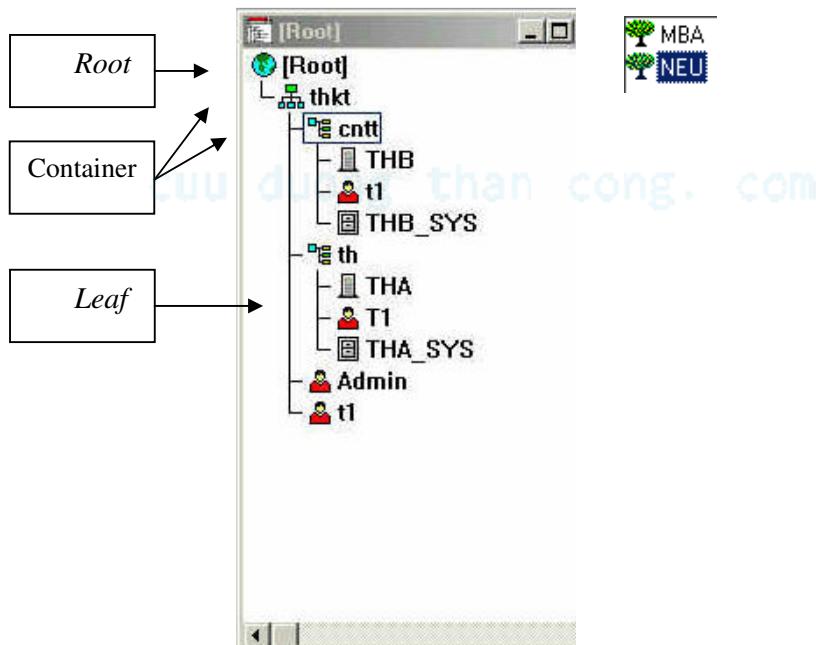
- Đối tượng Root biểu thị cấp cao nhất trong cây thư mục, Root không chứa thông tin, không thể xóa hay đổi tên.
- Đối tượng Container được dùng để tượng trưng cho quốc gia, công ty, phòng ban, nhóm làm việc và tài nguyên dùng chung (Country,

Organization, Organization Unit). Trong đối tượng này có thể chứa các container khác theo 3 mức.

- Đối tượng Leaf đại diện cho tài nguyên mạng như người dùng, máy in, ...

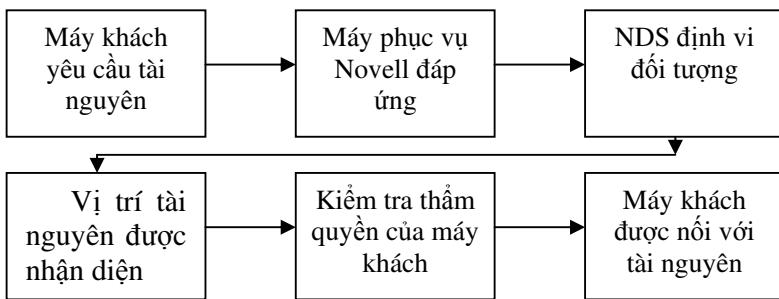


Cấu trúc NDS của tree NEU có Root và container THKT (O), trong đó chứa container CNTT và TH (OU), trong container CNTT chứa server THB user t1 (Leaf), trong container chứa server THB, ... (CN).



b. Vai trò của NDS

Để truy cập tài nguyên của mạng, người sử dụng phải yêu cầu đối tượng theo tên của NDS. Khi NDS trên máy phục vụ nhận biết yêu cầu, nó sẽ kiểm tra trên cây NDS về người sử dụng, quyền sử dụng đối tượng, dựa trên yêu cầu và thẩm quyền người dùng máy dịch vụ sẽ định vị và nối người sử dụng với tài nguyên.



c. *Tên của đối tượng*

Các đối tượng có thể trùng tên, nằm trên các container khác nhau, NDS không tìm kiếm đối tượng trên toàn cây thư mục, do vậy NDS đòi hỏi thông tin chính xác để tìm đúng đối tượng. Khi truy cập phải cung cấp cho NDS đúng tên đối tượng, có thể cung cấp thông tin bằng: tên phân biệt hay tên phân biệt tương đối.

- Tên chung (common name) của đối tượng leaf là tên nằm bên cạnh đối tượng leaf trong cây thư mục. Ví dụ theo cây NEU có CN=T1, THA, ...
- Ngữ cảnh (context) là vị trí của đối tượng trong cây thư mục. Đó là danh sách đối tượng container bắt đầu từ đối tượng đến root. Ví dụ theo cây NEU có THKT, CNTT,...
- Tên phân biệt: sự kết hợp tên chung và ngữ cảnh. Ví dụ theo cây NEU ta có .CN=T1.OU=CNTT.O=THKT
- Tên phân biệt tương đối (relative distinguished name) liệt kê đường dẫn đối tượng từ đầu đối tượng được đặt tên đến ngữ cảnh hiện hành. Tên phân biệt tương đối + ngữ cảnh hiện hành = tên phân biệt.
- Tên có kiểu (Type name): dùng chữ viết tắt để phân biệt các kiểu container và các đối tượng leaf
- Cách gọi tên không có kiểu(Typeless name): không bao gồm các kiểu thuộc tính đối tượng. Ví dụ: .T1.CNTT.THKT. Nếu không cung cấp tên đối tượng có kiểu, NDS sẽ tính toán kiểu thuộc tính cho từng đối tượng.

§ 2. QUẢN TRỊ FILE SERVER

- Thực hiện các tiện ích cơ bản của FILESERVER bằng cách nạp các MODUL chính như INSTALL, MONITOR , VREPAIR , REMOTE
- Cài đặt và bổ sung cấu hình mạng (INSTALL)
- Gửi thông điệp hệ thống hoặc cho từng USER (MONITOR)
- Kiểm tra liên kết hoặc ngắt bỏ liên hệ của các WORK STATION
- Sửa lỗi của VOLUME trong một số trường hợp (VREPAIR)
- Cài đặt hay hủy bỏ các dịch vụ, phần mềm hệ thống khác.
- Đóng FILESERVER

□ Cách nạp các MODULE trên máy SERVER:

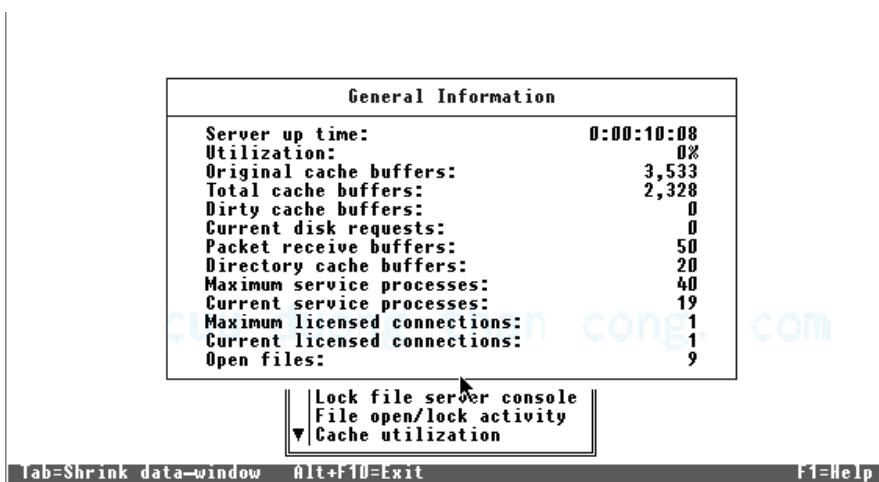
Tại dấu nhắc Novell Netware bấm LOAD <Tên mudul>
Các module sau đây thường được thực hiện:

1. INSTALL

Cài đặt cấu hình hệ thống mạng, tạo các NETWARE PARTITIONS dùng làm các VOLUMES trong mạng. Khởi tạo các VOLUMES, sao chép các FILE hệ thống, cài đặt các phần mềm mạng.

2. MONITOR

Kiểm tra hoạt động của hệ thống, các liên kết trong hệ thống. Ví dụ sau khi load module monitor trên màn hình sẽ hiển thị các thông tin



3. PSERVER

Cài đặt và kiểm soát các hoạt động của PRINT SERVER được cài đặt trực tiếp vào FILESERVER . Điều khiển các máy in trong mạng.

4. VREPAIR

Sửa lỗi khi khởi động mạng. Các lỗi này thường xảy ra khi hệ thống bị tác động đột ngột từ bên ngoài, ví dụ mất điện đột ngột.

Options:

1. Repair a volume
2. Set VRepair options
3. Exit

Enter your choice:

Chọn các chức năng để thực hiện chương trình

Đ3. CÀI ĐẶT MẠNG NOVELL NETWARE

3.1. Yêu cầu về phần cứng - phần mềm

- 1 FILE SERVER (máy chủ) : với cấu hình tối thiểu CPU 486 4MB RAM
- Các Work station (máy làm việc)
- Card mạng (ne2000, 3c503)
- Các phụ kiện khác
 - + Dây cáp: cáp quang, cáp đồng trục,cáp điện thoại
 - + Các thiết bị nối chúng: nối đường thẳng, nối chữ T ...
 - + Hub (thiết bị trung gian nối các work station vào FILE SERVER)
- Phần mềm
 - + 1 bộ đĩa NOVELL NETWARE (hoặc CD ROM)
 - + 1 bộ đĩa DOS
 - + Các chương trình sẽ chạy trên mạng

3.2. Các bước cài đặt:

1. Khởi tạo FILESERVER

- Lắp đặt Card mạng vào slot của main-board, lắp dây mạng. Kiểm tra các thiết bị bảo đảm cho máy có thể hoạt động được.
- Khởi động máy chủ, dùng FDISK tạo trên đĩa cứng của máy chủ một DOS PARTITION FORMAT và nạp phần hệ thống

2. Khởi động lại máy chủ

- Chạy tệp install.bat (Trên bộ đĩa cài đặt)
- Hoặc tạo 1 thư mục, chuyển vào thư mục ; sao chép các tệp sau đây:
 - + SERVER.EXE
 - + Trình điều khiển đĩa cứng (IDE.DSK, ISADISK.DSK, SCSI???.DSK ...)
 - + Trình điều khiển CARD mạng (*.LAN)
 - + Các tệp khác (*.NLM)
- Bấm SERVER trên màn hình hiển thị dấu nháy của NOVELL
- Máy thông báo : FILESERVER NAME - Gõ tên của FILE SERVER (tên do mình đặt, nên đặt tên ngắn gọn)
- Máy thông báo : IPX INTERNAL NETWORK NUMBER - Gõ dãy số đặc trưng của card mạng

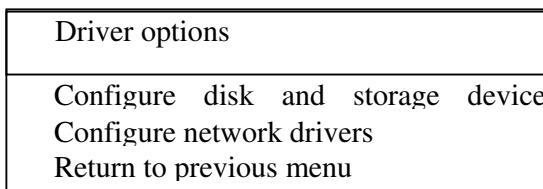
Thực hiện điền các tham số của Modul Install

- Tại dấu nháy của Server Novell Netware gõ LOAD INSTALL, trên màn hình hiển thị thực đơn của module install:

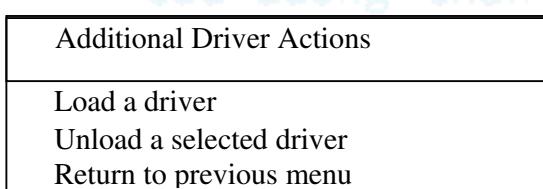
Installation Options	
Driver options	(Load/Unload disk and networkdrive)
Disk options	(configure/mirror/test disk partitions)
Volume options	(configure/mount/dismount volumes)
Licence option	(install the server licence)
Copy files option	(install Netware system files)
Directory options	(install Netware Directory services)
NETCF files options	(create/edit server startup files) ⁴³
Product options	(other optional installation items)
Server options	(install/uninstall this server)

a- Chọn thực đơn DRIVER OPTIONS

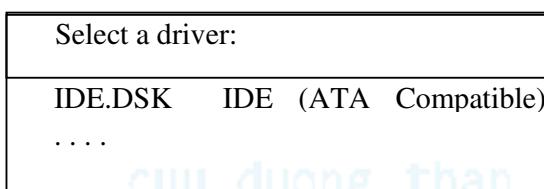
Cài đặt trình điều khiển đĩa cứng và card mạng



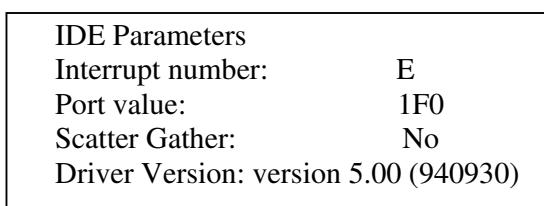
- Đĩa cứng: chọn “Configure disk and storage device drivers” , chọn load a driver



Trên màn hình hiển thị danh mục các driver, chọn loại phù hợp



Điền các tham số cho đĩa cứng (I/O: 1f0,170,1e8,168; interrupt: A,B,C,E,F)



Driver IDE parameter Actions
Select/Modifi driver parameter Save parameters and load driver

- Card mạng : chọn “Configure network drivers ” , chọn load a driver

Select a driver to install
3C503.LAN 3Com 3c503 EtherLink
NE2000.LAN Novell Ethernet NE2000
.....

- Chọn các tham số cho card mạng:

NE2000_1 Protocols
----- IPX (always selected)
[] TCP/IP
[] AppleTalk

Board NE2000_1 (Driver NE2000)
<u>Actions</u>
Select/Modifi driver parameters and Save parameters and load driver

IPX là giao thức ngầm định, Novell Netware luôn sử dụng giao thức này, có thể chọn thêm các giao thức TCP/IP và Appletalk.

b. Chọn thực đơn “DISK OPTIONS”

Available Disk Options
Modifi disk partitions and hot fix
Mirror/Unmirror disk partitions
Perform surface test (optional)
Scan for additional devices (optional)
Return to the previous menu

- Chọn “Modifi disk partitions and hot fix”

Trên màn hình hiển thị bảng phân chia đĩa: partition thứ nhất do DOS quản lý, cần phải khởi tạo Volumes cho partition thứ hai.

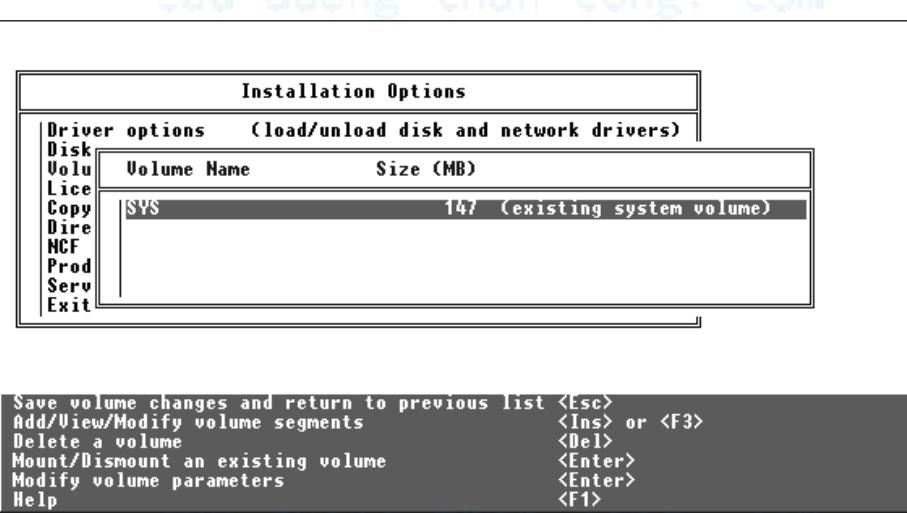
Disk Partition Type	Start	End	Size
Unknown Partition Type 6	0	627	250.2 MB
Netware Partition 628	1008	800.0 MB	

c. Chọn thực đơn “VOLUME OPTIONS ”

Khi chưa có volume nào được khởi tạo

Volume Name	Size (MB)

Chọn các phím tương ứng để tạo Volume mới



Các thông tin về partition của đĩa được hiển thị

Volume Disk Segment List			
Device No.	Segment No.	Size(MB)	Volume Assigment Status
0	0	800 (free space)	

Volume đầu tiên được Novell đặt tên là SYS, dung lượng tối thiểu là 75MB.

Disk segment parameters
Disk segment volume name: SYS
Disk segment size: 500 MB

Nếu chọn dung lượng của volume SYS cực đại thì sẽ không có volume tiếp theo

Tiếp tục khởi tạo các volume

What would you like to do with this free segment
Make this segment a new volume Make this segment part of another volume

d. Chọn thực đơn “LICENCE OPTIONS”

Cài đặt bản quyền cho Novell Netware thường được cài đặt từ đĩa mềm (đĩa bản quyền), bản quyền quy định số user tối đa được nối vào mạng

e. Chọn “COPY FILES OPTIONS”

Lựa chọn cài đặt files hệ thống, nhóm trình nào được đánh dấu [x] sẽ được cài đặt

Indicate which file groups you want installed

- [x] NetWare 4.1 Server executable and boot files (4MB)
- [x] Update NetWare 4.1 boot directory driver files (1MB)
- [x] Pre-Install Files (7MB)
- [x] NetWare System Files (9)
- [x] NetWare DOS Utilities (12MB)
- [x] NetWare MS OS/2 Utilities (2MB)
- [x] NetWare MS Windows Utilities (4MB)
- [x] NetWare UNIX Utilities (1MB)
- [x] ETC Files (1MB)
- [x] Set up a Network Directory for Client Install (7MB)
- [x] Set up a Network Directory for Server Migration (2MB)
- [x] NetWare 4.1 English Language-Specific Files (5MB)

f. Chọn thực đơn “*DIRECTORY OPTIONS*”

Cài đặt NDS và các cập nhật: khi cài phải lựa chọn

Directory name:

Company organization:

+ Level 1:

+ Level 2:

+ Level 3:

- Mật khẩu của ADMIN

Directory Services Options

Install Directory Services onto this server

Remove Directory Services from this server

Upgrade NetWare 3.x bindery information to the Directory

Upgrade mounted volumes into the Directory

Return to the previous menu

g. Chọn thực đơn “*NCF FILES OPTIONS*”

Available NCF Files Options

Create AUTOEXEC.NCF file

Create STARTUP.NCF file

Edit AUTOEXEC.NCF file

Edit STARTUP.NCF file

Upgrade a v3.1x AUTOEXEC.NCF Files

Return to the previous menu

3.3. Cài đặt WORK STATIONS (DOS)

- Yêu cầu về phần cứng: Máy phải được lắp card mạng, nối dây vào mạng
- Yêu cầu về phần mềm: máy đã được cài đặt hệ điều hành DOS, bộ đĩa cài đặt card mạng.

a. Cài đặt tối thiểu: truy cập mạng mức bindery

Khởi tạo tệp tin IPX.COM

- Tạo 1 thư mục tên là WSGEN và sao chép toàn bộ đĩa WSGEN của Novell Netware vào thư mục này.
- Chạy trình cài đặt WSGEN, chọn danh sách card mạng ứng với card mạng đã cài vào WORK STATIONS, điền các tham số (IRQ, I/O, DMA or RAM ...)
Nếu cài đặt thành công tệp tin IPX.COM sẽ được tạo ra

Nối WORK STATIONS vào mạng: khởi động máy ở DOS, bấm các lệnh sau
IPX
NETX
Chuyển vào ổ đĩa mạng
LOGIN <Tên SERVER>/<Tên USER>

b. Cài đặt đầy đủ: truy cập mạng mức NDS

Sử dụng phần mềm đi kèm card mạng, chạy trình cài đặt INSTALL.EXE, điền các tham số liên quan, nếu quá trình cài đặt thành công, các files sau sẽ được tạo:

LSL.COM
3C508.COM
IPXODI.COM
VLM.EXE
*.VLM
NET.CFG

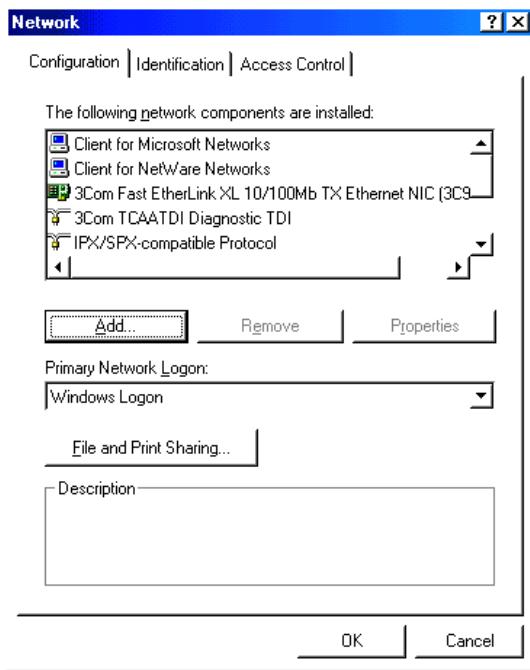
- Khởi động máy từ DOS, chạy lần lượt các tệp trên, có thể chạy các tệp tin trên bằng cách tạo tệp BAT.

Chuyển vào ổ đĩa mạng
LOGIN <Tên SERVER>/<Tên USER>

3.3. Cài đặt WORK STATIONS (Windows 9.X)

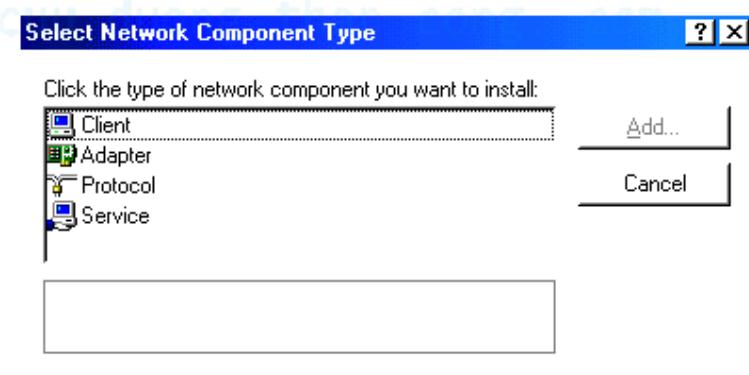
Các máy tính sử dụng hệ điều hành Windows 95, Windows 98, muốn sử dụng tài nguyên của Novell cần phải cài đặt phần mềm client cho máy, có thể dùng hệ điều hành Windows 9.x để cài đặt, các bước cơ bản để cài đặt:

Chọn trong Control Panel – Network: khi đó trên cửa sổ sẽ hiển thị những nội dung được cài đặt



Cài đặt card mạng và các tham số

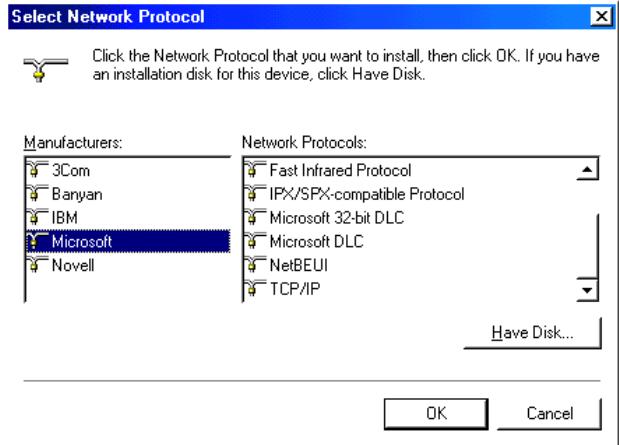
- Chọn ADD – Adapter



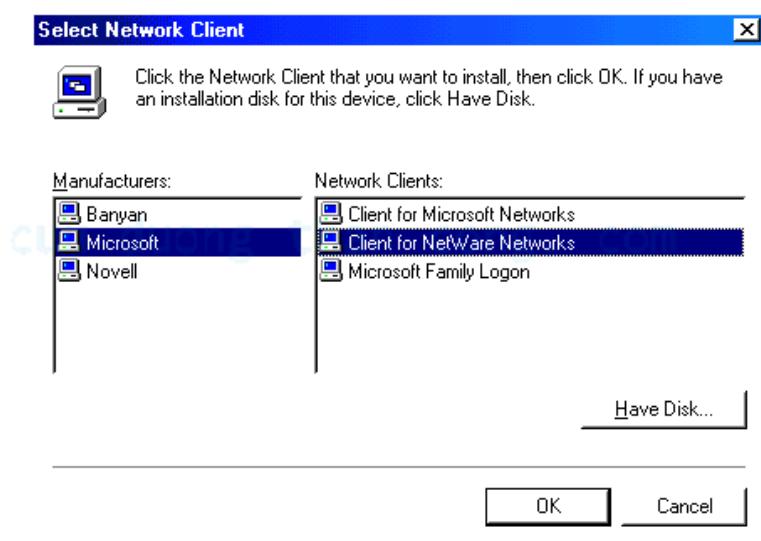
- Chọn card mạng trên danh sách card

Cài đặt Protocol

Chọn ADD - Protocol

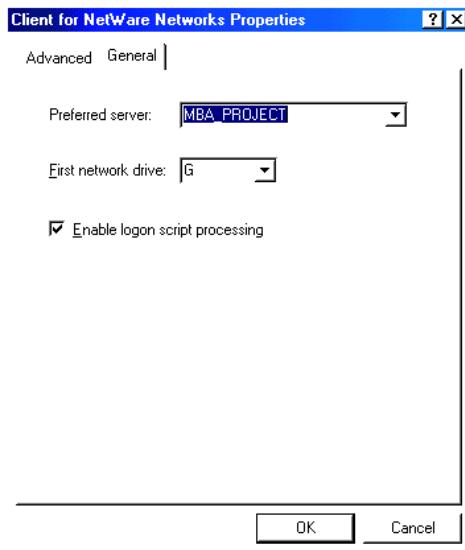


Chọn Microsoft, lựa chọn các Protocol cần thiết, để truy cập mạng Novell
NetWare cần cài IPX/SPX
Cài đặt client (máy khách)

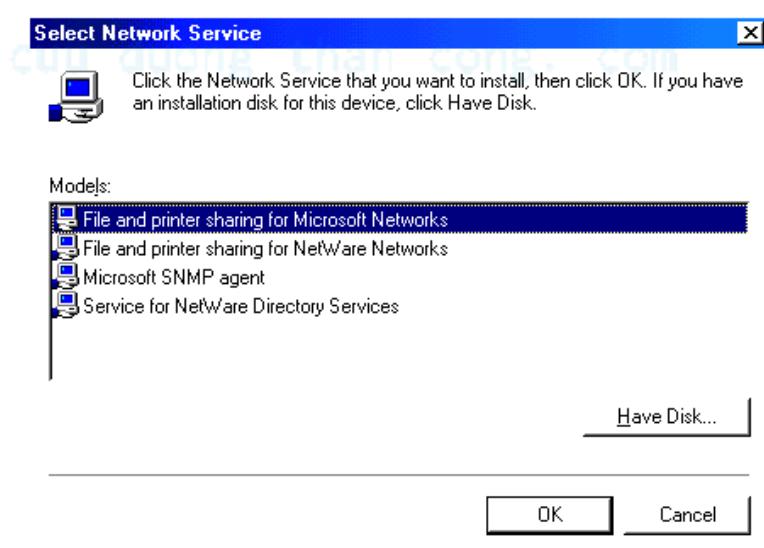


- Chọn Microsoft - client for Netware Networks
Điền tham số khi truy cập vào mạng:

cuu duong than cong. com



- Preferes server: Bấm tên Novell Netware Server mà user muốn truy cập
 - First network drive: ô đĩa mạng (logic) đầu tiên được gán khi user truy cập
 - Enable logon script processing: cho phép thực hiện login script của Novell
- Cài đặt dịch vụ NDS
- Chọn ADD – Service, chọn Service for NetWare Directory Services



§ 4. QUẢN TRỊ HỆ THỐNG THƯ MỤC VÀ FILES

4.1. Cấu trúc thư mục và files của Novell NetWare

Khái niệm VOLUMES

VOLUMES được khởi tạo trong quá trình cài đặt mạng, nó là một phần của Netware partition. Mỗi VOLUMES đều có tên, VOLUMES đầu tiên được khởi

tạo có tên là SYS trên VOLUMES này các FILE hệ thống của NOVELL NETWARE được cài đặt. Các VOLUMES khác có thể đặt tên tùy ý. Để một VOLUMES được sử dụng như một tài nguyên trên mạng VOLUMES này cần được MOUNT.

Cấu trúc của VOLUMES SYS

/LOGIN : Chứa các chương trình dùng để vào ra trên mạng

/PUBLIC: Chứa các tiện ích ở trên mạng, mỗi USER đều có quyền truy nhập đến thư mục này.

/SYSTEM: Chứa các chương trình hệ thống của NOVELL NETWARE. Chỉ có ADMIN mới có quyền đối với thư mục này.

/MAIL : Chứa các thông tin của USER trên mạng

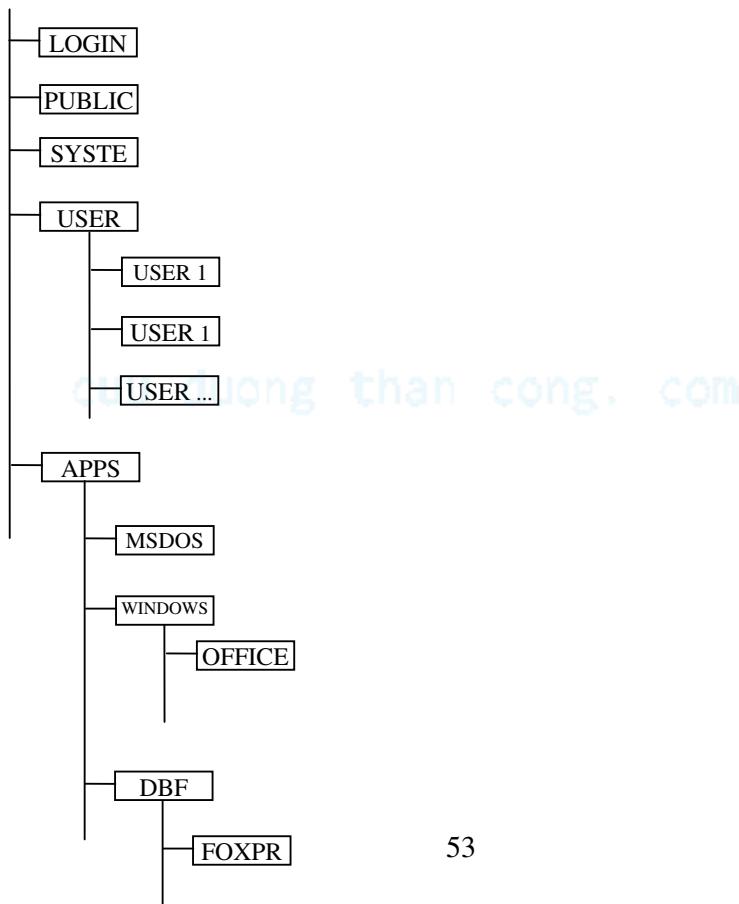
/ETC : Chứa một số FILES ví dụ có thể cài đặt.

/DELETE.SAV: Chứa các FILE được cứu nằm trong thư mục đã bị xóa.

4.2. Thiết kế hệ thống thư mục và FILES

Nguyên lý chung

- Hệ thống thư mục của NOVELL NETWARE để riêng trên volume SYS
- Hệ thống thư mục của các USER nên tập trung để dễ dàng theo dõi và kiểm soát.
- Hệ thống các chương trình ứng dụng nên phân loại và để theo nhóm.
Ví dụ: nếu chỉ có 1 VOLUMES



Nếu có nhiều VOLUMES nên để mỗi VOLUMES lưu trữ một nhóm chương trình. Ví dụ: một volume dành cho các user, một volume dành cho group, một volume dành cho các ứng dụng khác.

Nếu có nhiều đĩa cứng thì nên tạo trên mỗi đĩa cứng thành 1 volume.

4.3. Quyền hạn

Quyền hạn 1 USER qui định khả năng truy nhập đến các tài nguyên của USER này. Như vậy quyền hạn là một trong những chức năng cơ bản để bảo vệ an toàn cho dữ liệu và hệ thống. Nhiệm vụ của ADMIN là gán các quyền này cho hợp lý. Một hệ thống làm việc tốt là một hệ thống trong đó các USER được trao quyền hạn vừa đủ, có khả năng khai thác tối ưu nhất các tài nguyên trên mạng.

Quyền hạn của các user đối với các tài nguyên được qui định bởi một trong hai cách sau:

TRUSTEE ASSIGNMENT

Quyền được gán trực tiếp bởi ADMIN hoặc các WORK GROUP cho các USER sau khi được gán USER này sẽ được gọi là TRUSTEE của tài nguyên tương ứng. Quyền TRUSTEE được chia làm 2 loại:

- Gán cho thư mục: TRUSTEE DIRECTORY RIGHT
- Gán cho FILES: TRUSTEE FILE RIGHT

INHERITED RIGHT MASK (Quyền thừa kế)

Quyền thừa kế được tự động gán cho FILE và thư mục khi USER tạo ra các thư mục hay FILES. Quyền thừa kế được chia làm 2 loại: quyền thừa kế của thư mục và quyền thừa kế của FILES .

Quyền của USER

- user ADMIN

Quyền có thể gán đối với FILES và thư mục

- + Có quyền tuyệt đối
- + Thay đổi các quyền

Các quyền hạn

- SUPERVISOR tất cả các quyền đối với Thư mục hoặc files. User có quyền này có thể gán quyền cho các user khác về thư mục và files

- READ (D,F) mở FILE hay đọc thư mục; khi muốn chạy một chương trình, xem nội dung của 1 tệp dữ liệu phải có quyền này.
- WRITE (D,F) Cho mở FILE và ghi các thay đổi đối với FILE này.
- CREATE (D) Tạo mới tệp tin và các thư mục con
 - (F) Phục hồi các tệp tin sau khi tệp tin bị xóa
- ERASE (D) Xóa 1 thư mục FILE và các thư mục con
 - (F) Xóa 1 tệp tin
- MODIFY (D,F) Thay đổi thuộc tính của thư mục và các tệp tin, đổi tên FILES và tên thư mục.
- FILESCAN (D,F) Cho phép liệt kê các tệp tin trên danh sách các thư mục
- ACCESS CONTROL Quyền thay đổi TRUSTEE, INHERITED trừ quyền SUPERVISOR

4.4. Thuộc tính

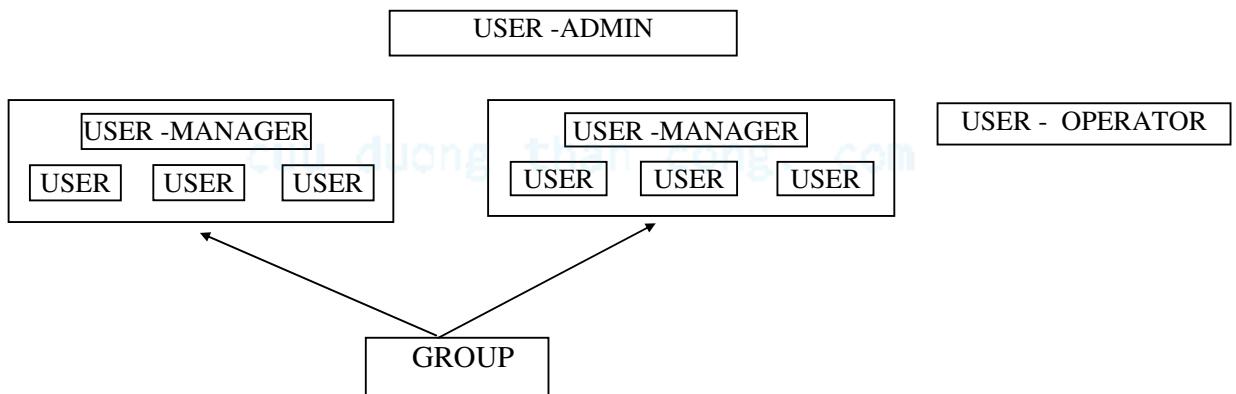
Thuộc tính là tính chất nội tại bên trong các tài nguyên và không phụ thuộc vào các đối tượng bên ngoài. Thuộc tính là một tác nhân bổ sung cho quyền hạn và cùng với quyền hạn tạo nên quyền thực sự của USER

- ARCHIVE NEEDED (A,F,D) Được tự động gán bởi NOVELL NETWARE cho các FILES và thư mục Thuộc tính này là bít ARCHIVE của DOS (DOS có 4 thuộc tính RASH) (Status)
- CAN'T COMPRESS (Cc,F) Không nén files (Status)
- COMPRESSED (C,F) có thể nén files (Status)
- COPY INHIBIT (CI, F) cấm COPY từ Macintosh (Status)
- DELETE INHIBIT (D,F,D) cấm xóa, thuộc tính này mạnh hơn quyền xóa (ERASE) của USER đối với FILES hoặc thư mục (Status)
- DON'T COMPRESS (DC, F,D) Không cho phép nén tệp tin
- DON'T MIGRATE (DM, F,D) Không cho phép di chuyển tệp tin sang thiết bị lưu trữ thứ hai (như đĩa quang)
- EXECUTE ONLY (X,F) Cấm sao chép (*.com, *.exe) , thuộc tính này chỉ có SUPERVISOR có quyền gán và nếu đã một lần gán thì không thể xóa bỏ được nữa
- HIDDEN (H,F,D) ẩn khỏi lệnh DIR của DOS
- IMMEDIATE (IM,F,D) các files được gán thuộc tính này sẽ sớm bị nén
- PURGE (P,F) Thông thường files bị xóa có thể được phục hồi bằng lệnh SALVAGE, ~~luu duong than cong. com~~
- thuộc tính này sẽ làm mất tác dụng của lệnh SALVAGE. Do đó các files với thuộc tính PURGE sau khi bị xóa sẽ không thể cứu lại được.
- READ ONLY (Ro,F) thuộc tính này luôn đi kèm DELETE INHIBIT và RENAME INHIBIT . Chỉ cho phép đọc, không thể xóa hay đổi tên, cũng không thể thay đổi nội dung files . Thuộc tính này có thể bị loại bỏ bởi user có quyền modify đối với files này
- READ WRITE (Rw,F) nếu thuộc tính Ro bị loại bỏ thì thuộc tính Rw sẽ tự động gán.

- RENAME INHIBIT (RI,F,D) Không cho phép đổi tên files hay thư mục. Thuộc tính này mạnh hơn quyền MODIFY.
- SHAREABLE (S,F) Cho phép được sử dụng như tài nguyên chung trong mạng. Thuộc tính này đặc biệt hữu ích trong trường hợp nhiều user sử dụng chung.
- SYSTEM (Sy,F,D) ẩn đối với lệnh DIR, đồng thời không cho phép xóa hay sao chép.
- TRANSACTIONAL (T,F) files được gán thuộc tính này sẽ được bảo vệ trong mạng bởi TTS (TRANSACTIONAL TRACKING SYSTEM)

§ 5. QUẢN TRỊ USER VÀ GROUP

Hệ thống quản trị user trong NOVELL NETWARE được tổ chức:



User là một định danh bao gồm tên và mật khẩu, muốn truy nhập vào mạng phải nhập tên user và mật khẩu. Những thông tin liên quan đến user được tập hợp và gọi là user account bao gồm: tên đầy đủ, mô tả khoản mục, thông tin về môi trường, thời gian được phép làm việc, những hạn chế đối với tài nguyên và những quyền của người sử dụng đối với hệ thống.

- Quản trị user và group bao gồm những công việc cơ bản sau:
 - 1- Khởi tạo USER và GROUP
 - 2- Gán quyền cho USER và GROUP
 - 3- Cài đặt hạn chế của USER
 - 4- Theo dõi và quản trị USER ACCOUNT

5- Khởi tạo các OPERATOR

Các user đặc biệt:

User ADMIN

- Tạo, xóa các USER và GROUP
- Tạo các quyền hạn của từng USER và GROUP
- Chỉ định WORKGROUP MANAGER
- Tạo các OPERATOR
- Kiểm soát USER ACCOUNT
- Tạo các thuộc tính cho toàn bộ tài nguyên được sử dụng trong hệ thống mạng.
- Khởi tạo và điều khiển máy in trong mạng
- Xử lý và điều khiển toàn bộ hoạt động của hệ thống thông qua các lệnh và tiện ích của mạng.

OPERATOR : là 1 user có quyền hạn ngầm định để thực hiện một số nhiệm vụ, có 3 loại OPERATOR

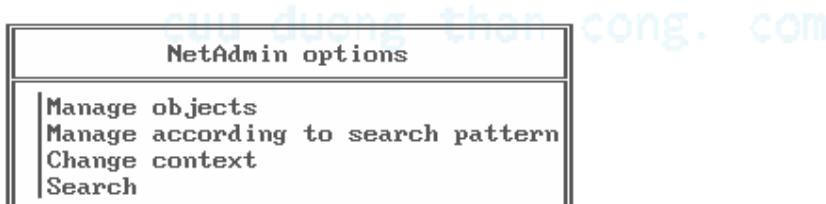
- FILESERVER CONSOLE OPERATOR người có quyền sử dụng FCONSOLE để kiểm soát các liên kết mạng, gửi các thông điệp hệ thống.
- PRINT SERVER OPERATOR quyền được điều khiển công việc in trên PRINT SERVER
- PRINT QUEUE OPERATOR quyền điều khiển các hàng đợi của PRINT SERVICE
- Tất cả các OPERATOR đều do ADMIN khởi tạo và giao quyền.

Thiết kế hệ thống users groups

5.1. Quản trị USER

Quản trị user thông qua chương trình NETADMIN
Tạo USER

- Trong thực đơn của NETADMIN :

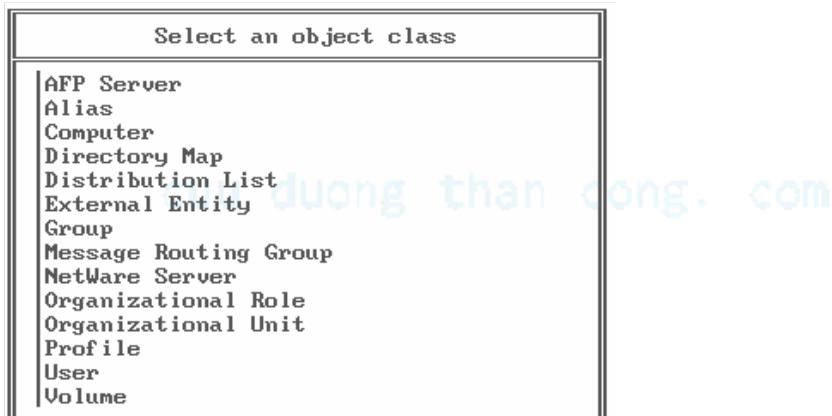


- Chọn Manage object

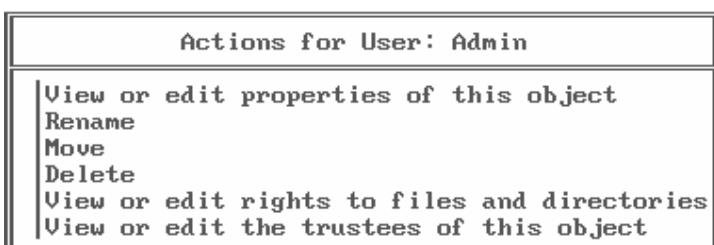
Object, Class	
..	*
.	(parent)
Admin	(current context)
administrator	(User)
Adminstration	(User)
AJESSE	(Group)
AMBA	(User)
arifa	(User)
baron	(User)
berrell	(User)
Big	(Group)
bodie	(User)
gmba	(Group)
GUEST	(User)
Ha	(User)

Trên màn hình hiển thị danh sách các object (user, group, printer ...)

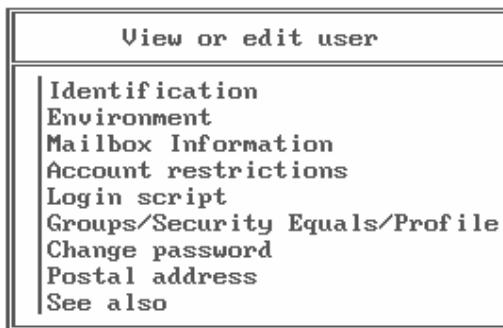
Bấm INSERT để tạo user mới, trên màn hình hiển thị:



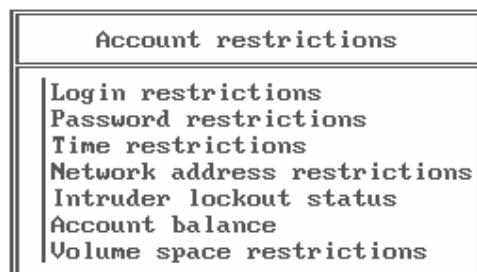
- Chọn “USER”, bấm tên user mới
- Cài đặt các thông số cho user: các thông số cần xác định cho user chính là các hạn chế của user bảo đảm cho sự an toàn và bảo mật của hệ thống
- Trong thực đơn của NETADMIN (Object, Class)
Chọn tên của USER trong danh sách
Trên màn hình hiển thị thực đơn để có thể cài đặt, hiệu chỉnh các tham số của user



Chọn “View or edit properties or this object “



Các tham số sau đây cần hiệu chỉnh:



ACCOUNT RESTRICTION

- ACCOUNT DISABLE: YES user không được phép vào mạng
No user được phép vào mạng

- ACCOUNT HAS EXPRIRATION DATE

NO user vào mạng với tên mình trong cùng một thời gian
YES user chỉ có thể vào mạng với tên mình tại workstation nhiều nhất là số lần được chỉ ra trong MAXIMUM CONECTION

- ALLOW USER TO CHANGE PASSWORD

YES user có quyền thay đổi mật khẩu
NO user không có quyền thay đổi mật khẩu

- MINIMUM PASSWORD LENGTH: độ dài tối thiểu mật khẩu

- FORCE PERIODIC PASSWORD CHANGES

YES user bắt buộc thay đổi mật khẩu định kỳ
CHANGE PASSWORD thay đổi mật khẩu

LOGIN SCRIPT khởi tạo hay sửa nội dung của USER LOGIN SCRIPT

Time RESCTRICKS Khai báo hạn chế về thời gian làm việc của user trong hệ thống

VOLUMES/DISK RESCTRICKS khai báo hạn chế về dung lượng không gian trong các VOLUMES mà các user này có thể sử dụng.

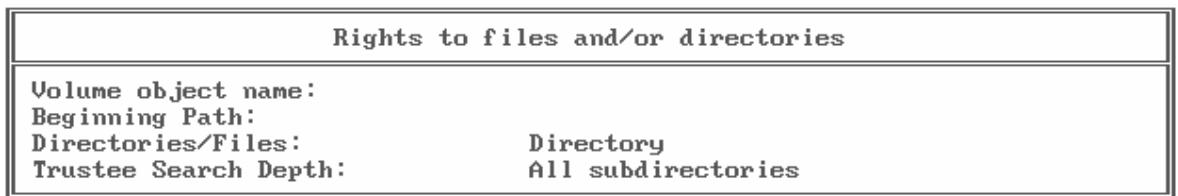
TRUSTEE DIRECTORY ASSIGNMENT

TRUSTEE FILE ASSIGNMENT

Hai lựa chọn trên dùng để gán quyền tương đương cho user sử dụng directory và files

ADMIN hoặc MANAGER có thể gán quyền tương đương cho một user ngang với một user hoặc một nhóm khác.

- Chạy trình NETADMIN
- Chọn USER , Chọn “View or edit right to files and directories “



Chọn “Volume object name” để nhập tên volume cần gán quyền (có thể bấm ENTER sau đó INSERT để chọn trên danh sách)

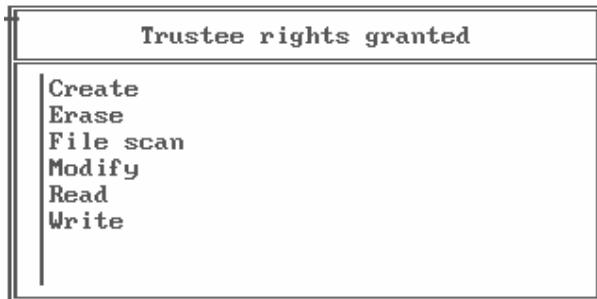
Bấm F10 hiển thị quyền truy nhập các thư mục và các files của user

Trustee directory, rights	
ALLSUB APPS GROUP/VISITING USERS/R3A/BARON	[RWCEMF] [R F] [RWCEMF] [SRWCEMFA]

Quyền truy nhập

- Chọn SECURITY EQUIVALENCES

Trong cửa sổ bấm INSERT để gán quyền, hoặc DETETE để hủy bỏ quyền trong danh sách.

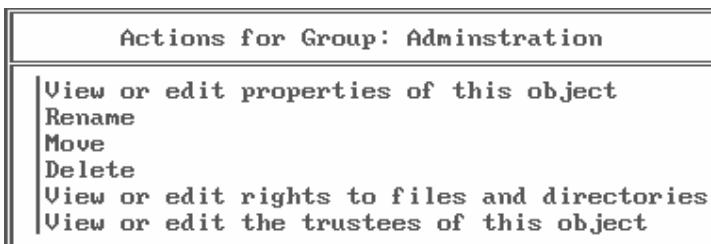


5.2. Quản trị GROUP

Khởi tạo GROUP

- Chạy NETADMIN

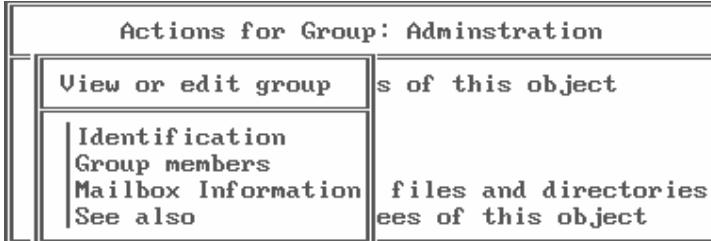
Trên màn hình hiển thị danh sách các object (user, group, printer ...)



Bấm INSERT, chọn “GROUP” để tạo tên cho GROUP

Bổ sung, bớt các thành viên của nhóm

- Chạy NETADMIN ... , chọn group, chọn “view or edit properties of this object”
- Chọn “group members”



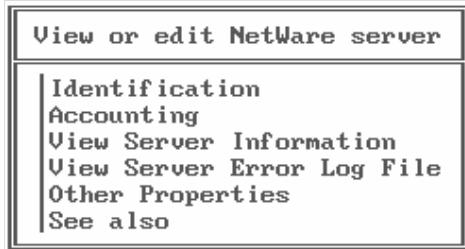
Bấm INSERT để thêm user vào group.

Trên Novell Netware 4.x Group administration là một group đặc biệt, thành viên của group này có quyền tương đương với ADMIN

- Khởi tạo OPERATOR

Tạo FILESERVER CONSOLE OPERATORS

- Chạy NETADMIN
- Chọn object “Netware Server”



Chọn “Identification”

Identification information	
Name:	MBA_PROJECT
Version:	Novell NetWare 4.10[DS]
Status:	Up
Other name:	↓ (Empty List)
Description:	↓ IPX/SPX: 31FA6516:1:451
Network address:	↓ (Empty List)
Operator:	↓ (Empty List)
User:	↓ (Empty List)
Location:	↓ (Empty List)
Department:	↓ (Empty List)
Organization:	↓ (Empty List)
Messaging Server:	

- Chọn “OPERATOR “, chọn user gán thành operator
- Các OPERATOR khác được khởi tạo bằng PCONSOLE

5.3. Quản trị USER ACCOUNT

Quản trị USER ACCOUNT là chức năng cho phép quản trị và theo dõi tiến trình làm việc của từng USER trong hệ thống. Hệ thống tài khoản công nợ ACCOUNTING SYSTEM của NOVELL NETWARE cho phép kiểm tra và tiến hành tính toán cụ thể trên các tham số.

- Đọc dữ liệu: Khối lượng dữ liệu USER đã tiến hành đọc trên các VOLUMES của SERVER

$$=\sum \text{hệ số} * \text{số đơn vị đọc}$$

Số đơn vị đọc: BLOCK/30" (1BLOCK=4KB NOVELL NETWARE)

Hệ số có thể thay đổi theo từng đơn vị thời gian là 30 phút trong ngày (48 hệ số/ngày)

- Ghi dữ liệu: Khối lượng dữ liệu được ghi trên các VOLUMES của SERVER

Cách tính tương tự như đối với đọc dữ liệu

- Thời gian làm việc: Tổng thời gian user làm việc trên mạng, đơn vị tính là 30 phút

$$=\sum \text{hệ số} * \text{số đơn vị làm việc}$$

- Thời gian kết nối trong mạng: tổng số thời gian user kết nối trong hệ thống, đơn vị tính là 30 phút

$$=\sum \text{hệ số} * \text{số đơn vị làm việc}$$

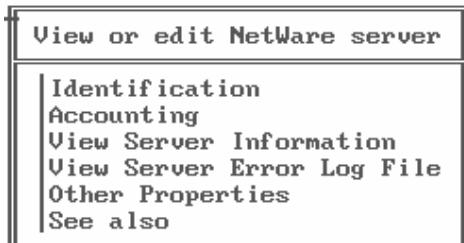
- Dung lượng đĩa đã được sử dụng: Tổng dung lượng đĩa đã được sử dụng

- Các dịch vụ mà user đã tiến hành trên SERVER. Các dịch vụ này được thể hiện thành những request (yêu cầu) gửi lên SERVER như E-mail, in ấn trên mạng ...

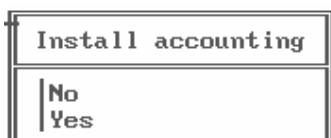
5.4. Thao tác với USER ACCOUNT

Cài đặt Accounting system

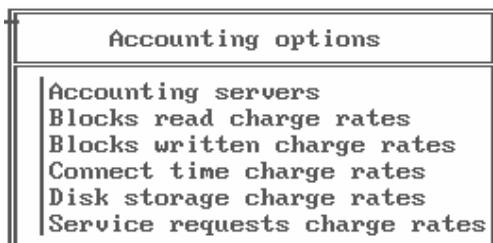
- Chạy NETADMIN, chọn server cần cài đặt, chọn “View or edit properties of this object”



- Chọn ACCOUNTING



- Chọn YES để cài đặt

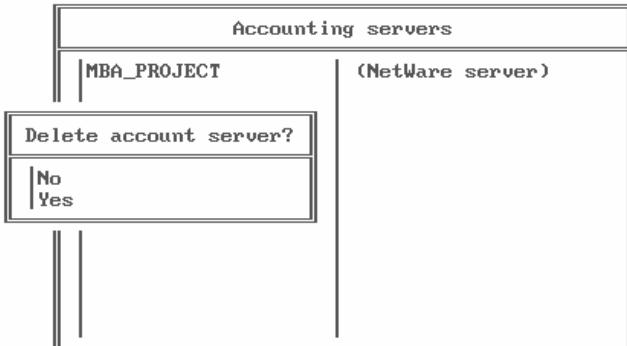


Đặt các yêu cầu:

- BLOCK READ CHARGE RATES: cài đặt hệ số tính toán khói lượng đọc đĩa
- BLOCK WRITTEN CHARGE RATES: cài đặt hệ số tính toán khói lượng ghi đĩa
- CONNECT TIME CHARGE RATES: cài đặt hệ số tính toán thời gian truy cập
- SERVICE REQUEST CHARGE RATES : cài đặt hệ số dịch vụ mạng đã yêu cầu

Xóa SERVER ACCOUNT

- Chạy NETADMIN
- Chọn các bước giống trên, chọn “Accounting server “, bấm DELETE

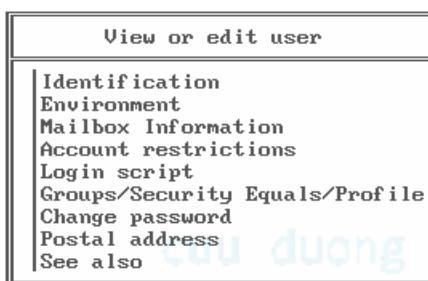


- Danh sách các SERVER ACCOUNT xuất hiện, bấm DELETE để xóa

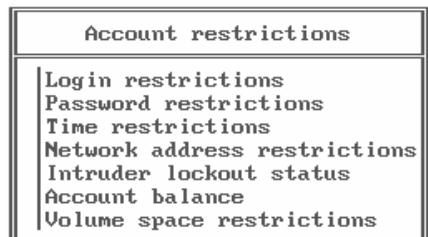
Tính công nợ

Để tính công nợ (BALANCE) của một user :

- Chạy NETADMIN
- Chọn user trong danh sách, chọn “View or edit properties of this object “



- Thực hiện ACCOUNT BALANCE



Trên màn hình hiển thị thực đơn, cần điền các tham số:

Account balance:

Điền số

Allow unlimited credit: (Yes: không giới hạn tài khoản, No: giới hạn)

§ 6. LOGIN SCRIPTS

6.1. Khái niệm:

Những lệnh cần thực hiện một cách tự động khi USER nối vào mạng được tập hợp và ghi trong một tệp được gọi là LOGIN SCRIPT. LOGIN SCRIPT đóng vai trò như AUTOEXEC của DOS .

NOVELL NETWARE phân biệt 3 LOGIN SCRIPT

- SYSTEM LOGIN SCRIPT

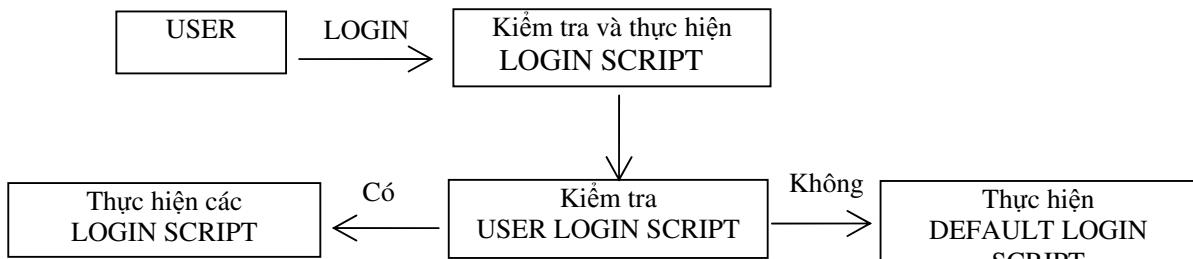
Chứa các lệnh mà mọi user thuộc organization này khi vào mạng sẽ được thực hiện. LOGIN SCRIPT được khởi tạo bằng ADMIN

- PROFILE LOGIN SCRIPT chứa các lệnh trong một object, có thể gán để một số user có thể thực hiện LOGIN SCRIPT này.

- PERSONAL LOGIN SCRIPT

Chứa các lệnh riêng biệt cần thực hiện của user khi vào mạng . Mỗi user có thể khởi tạo riêng cho mình một USER LOGIN SCRIPT.

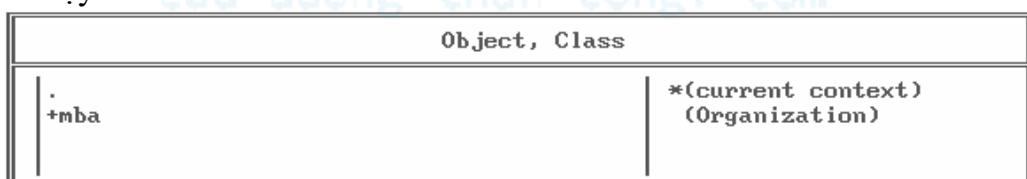
- DEFAULT LOGIN SCRIPT ngầm định của mọi user khi USER LOGIN SCRIPT của user này chưa được khởi tạo



6.2. Khởi tạo LOGIN SCRIPT

Khởi tạo SYSTEM LOGIN SCRIPT

- Chạy NETADMIN



- Chọn tên Organizational Unit

- Bấm F10, chọn “View or edit properties of this object “

- Chọn SYSTEM LOGIN SCRIPT

Khởi tạo hoặc hiệu chỉnh SYSTEM LOGIN SCRIPT viết giống như trên hệ soạn thảo văn bản

Khởi tạo PERSONAL LOGIN SCRIPT

- Chạy NETADMIN

- Chọn tên user, bấm F10, chọn “View or edit properties of this object “

- Chọn LOGIN SCRIPT

Khởi tạo hoặc hiệu chỉnh LOGIN SCRIPT viết giống như trên hệ soạn thảo văn bản

Khởi tạo PROFILE LOGIN SCRIPT

- Tạo một PROFILE (là một object, giống như tạo một user)

- Gán quyền, viết LOGIN SCRIPT ...

- Gán quyền sử dụng PROFILE này cho user

+ Trong NETADMIN chọn user , chọn “View or edit properties of this object “, chọn “Group/Security/Equals/Profile”

Groups/Security Equals/Profile	
Group:	(Empty List)
Security equal to:	TBIG
Profile:	thu

- + Chọn PROFILE và gán tên PROFILE

6.3. Các lệnh hệ thống trong LOGIN SCRIPT

1. COMSPEC

Chức năng: Khi kết thúc 1 ứng dụng bao giờ DOS cũng nạp lại COMMAND.COM, lệnh này chỉ đường dẫn hệ thống chứa tệp COMMAND.COM để hệ điều hành nạp lại tệp tin này.

Cú pháp: COMSPEC <D:> <PATH> COMMAND.COM

2. DRIVE

Chức năng: Chuyển ổ đĩa làm việc, đặt ổ đĩa mạng (được ánh xạ-MAP) như là ổ đĩa DOS mặc nhiên.

Cú pháp:

DRIVE <D:>

DRIVE *n:

n thứ tự ổ đĩa mạng

3. # (exec)

- Chức năng: Thi hành một lệnh ngoại trú ngay trong LOGIN SCRIPT sau đó quay trở về

- Cú pháp: # <Tên lệnh>

Chú ý: Chỉ thực hiện các lệnh ngoại trú

- Không nạp các TSR (thường trú)

- # nằm trên 1 dòng

4. EXIT

- Chức năng: Ngừng thi hành các lệnh còn lại của LOGIN SCRIPT và chuyển về DOS thực hiện tiếp

- Cú pháp: EXIT

EXIT “Lệnh”

- Chú ý: SERVER, STATION phải tương thích với IBM

- “Lệnh” sau EXIT phải nằm trong ổ đĩa đã được ánh xạ

5. IF ... THEN

- Chức năng: cho phép LOGIN SCRIPT thực hiện quyết định dựa trên 1 số điều kiện

Cú pháp:

IF điều kiện THEN lệnh

IF điều kiện AND điều kiện THEN lệnh

IF điều kiện THEN BEGIN

Lệnh

(ELSE)

Lệnh

END

6. WRITE

- Chức năng: hiển thị một đoạn văn bản lên màn hình

- Cú pháp :

WRITE “Text”;”more text “; identifier (biến hệ thống)

WRITE “Text %Biến”

(Tên biến phải viết chữ in hoa)

* Danh sách các biến :

DAY Số ngày trong tháng (1-31)

DAY_OF_WEEK Tên ngày trong tuần (MONDAY, TUESDAY..)

HOUR giờ hiện hành (1-12)

GREETING_TIME “morning”, “afternoon”, “evening” theo đồng hồ

MONTH Tháng (1-12)

FULL_NAME Tên đầy đủ của USER

LOGIN_NAME Tên user khi nối vào mạng

STATION Chỉ số của trạm làm việc

P_STATION Vị trí vật lý của trạm làm việc

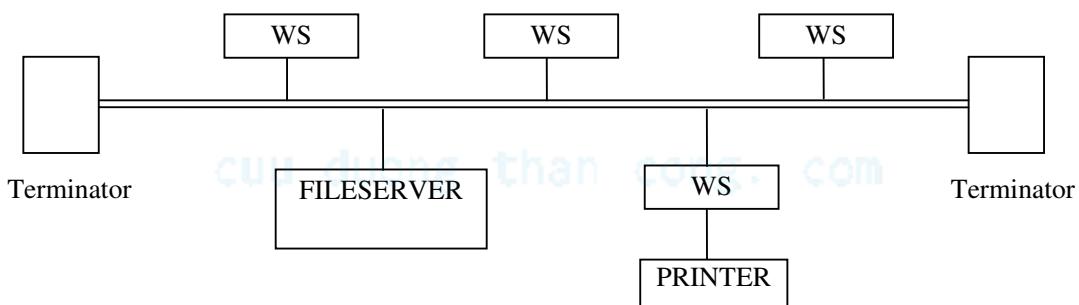
OS Tên của hệ điều hành

Các biến của DOS

7. Lệnh MAP

§ 7. QUẢN TRỊ DỊCH VỤ IN TRÊN MẠNG

7.1. Tổng quan về công việc in trên mạng (DOS client)



- PRINT SERVICE đã được cài đặt

- ở FILESERVER đã được nạp PSERVER

- ở WORKSTATION : đã được chuẩn bị khởi tạo cổng máy in vào mạng và chuyển dữ liệu ra PRINT SERVER
- ở WORKSTATION có nối máy in: máy in đã được nối vào mạng
- ở các chương trình ứng dụng: Khởi tạo máy in, khởi tạo cổng in (LPT logic)

7.2. Cài đặt PRINT SERVER , cài đặt máy in, cài đặt PRINT QUEUE,

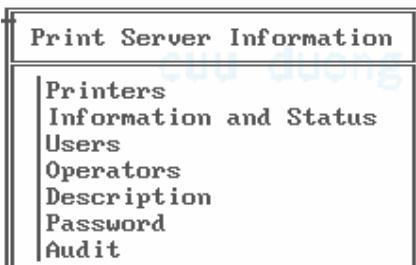
Người thực hiện (user): ADMIN

Chạy PCONSOLE



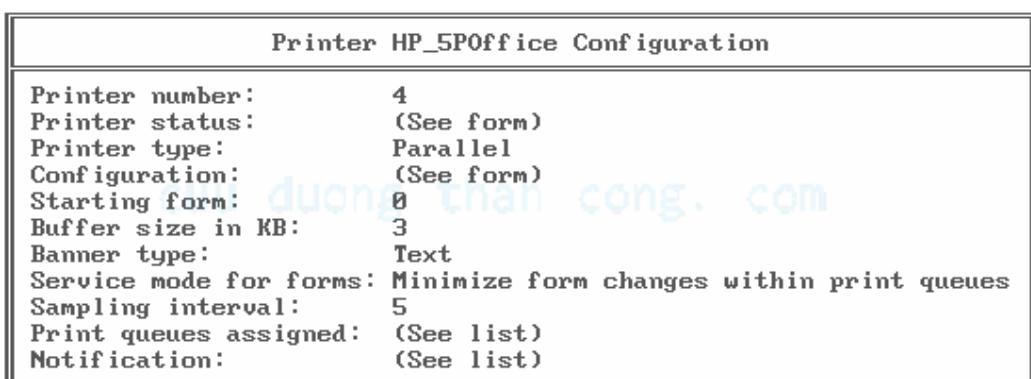
- Cài đặt PRINT SERVER

+ Chọn PRINT SERVERS : Khai báo tên PRINT SERVER



- Cài đặt máy in

+ Chọn PRINTER, khai báo tên máy in



Tiếp theo nhập vào các thông số kỹ thuật của máy

- Cài đặt print queue

Trong thực đơn PCONSOLE

- + Chọn PRINT QUEUES : gõ tên queue
- + Chọn QUEUE SERVERS để gán queue cho print server đã được cài đặt ở phần trên

Thực đơn QUEUE USER dùng để gán các user được quyền sử dụng các queue này

Thực đơn QUEUE OPERATOR dùng để gán USER điều khiển hàng đợi in; các user này có quyền xem và điều khiển print jobs hủy hay thay đổi thứ tự in

- Gán các printer được cài đặt cho print queue
- + Chọn PRINT SERVERS
- + Chọn PRINTER

Một danh sách các printer đã cài đặt xuất hiện, với mỗi máy in làm như sau:

- + Printer queues assigned để gán QUEUE
- + Gõ thứ tự ưu tiên PRIORITY

Khởi động PRINT SERVER tại FILE SERVER

Trong tệp AUTOEXEC.CNF viết dòng lệnh

LOAD PSERVER <Tên PRINT SERVER>

Khai báo, chuẩn bị đường truyền dữ liệu cho WORK STATION

- Dùng lệnh CAPTURE

Có thể dùng lệnh này ở autoexec hoặc trong login script

Cú pháp : CAPTURE q=<tên print queue> L=<từ 1 đến 3 đây là tên cổng LPT>

Có thể có thêm một số tham số:

NB Bỏ qua trang tiêu đề của công việc in

NT Không thay đổi ký tự TAB

NF Máy in không kéo trang trước khi in

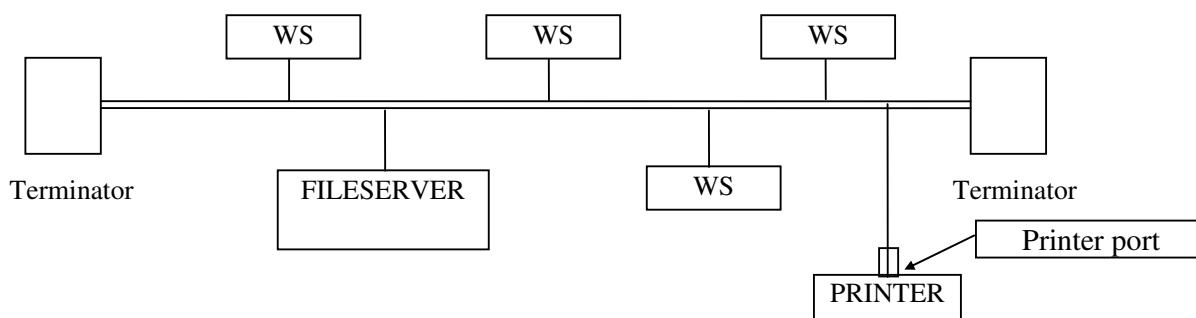
7.3. Ở work station : nối máy in với mạng

- Chạy NPRINTERS
- Chọn PRINT SERVER chọn máy in cần nối vào mạng

Ở work station : chuẩn bị cho việc in, như khai báo cổng máy in, máy in ...

Thông thường các chương trình ứng dụng thường được chuẩn bị cổng in để có thể gửi tín hiệu ra máy in. Cổng này có thể là LPT1, LPT2 cổng in vật lý LPT1, LPT2, LPT3 cổng in LOGIC. Trước khi gửi in phải khai báo cổng in sẽ in ra, cổng in được chọn phải tương ứng với cổng in được khai báo trong CAPTURE

7.4. Tổ chức máy in PRINT SERVER



- Máy in được nối trực tiếp với mạng qua bộ điều khiển cắm ở cổng máy in (Printer connection)
- Tạo PRINT SERVER : thao tác giống như trường hợp máy in nối vào máy tính
- Chạy chương trình SETUP của Printer connection): chọn và điền các tham số
 - + Type: manual load (remote)
 - + Port: other

§ 8. MỘT SỐ LỆNH CƠ BẢN CỦA NOVELL NETWARE

8.1. Lệnh NDIR

NDIR	General Usage Help	4.25
Purpose: View information about files, directories, and volumes.		
For help on: Display format Sorting features Search filters (restrictions) Attribute filters Other options Syntax All help screens	Type: NDIR /? FOR NDIR /? SORT NDIR /? RES NDIR /? AT NDIR /? OPT NDIR /? SYN NDIR /? ALL	
For example, to: See all files in current directory See only directories on drive C:	Type: NDIR *.* NDIR C:*.* /D0	

Chức năng: Xem các thông tin về tệp, thư mục và volume.

Cú pháp:

NDIR / Tham số

Ví dụ:

NDIR

Hiển thị danh sách tệp tin, các thông tin về tệp ở thư mục hiện thời.

8.2. Lệnh NCOPY

NCOPY	General Help	4.13
Purpose: To copy files and directories. Syntax: NCOPY source path [target path] [options]		
To: Copy subdirectories Copy subdirectories including empty directories Copy files with archive bit set Copy files with archive bit set, then clear the bit Copy sparse files Inform when non-DOS file information will be lost Copy only DOS information Read after write verify on local drives (DOS only) Retain compression on supported media Retain compression on unsupported media Display version information	Use: /S /S/E /A /M /F /I /C /U /R /R/U /VER	
For example: To copy all files and subdirectories from volume SYS to drive G:	Type: NCOPY SYS:.*.* G:.*.* /S	

Chức năng: sao chép tệp và thư mục

Cú pháp: NCOPY Tham số nguồn Tham số đích [Options]

Ví dụ: NCOPY *.* C:\ /S

Copy tất cả các tệp, các thư mục con ở thư mục hiện thời sang ổ đĩa C:\

8.3. Lệnh Login.

Chức năng: cho phép user truy nhập vào mạng Novell Netware

Cú pháp:

Ví dụ:

Login [/Ver] [[Server\Tree]/user name] [/optional]

Các option:

/Ver: Cho biết version mạng ta login

/NS: Khi vào mạng không chạy các lệnh trong login script.

/CLS Khi vào mạng, xoá màn hình sau khi chạy các lệnh trong login script.

/S filename Chạy các lệnh login script trong file có tên là filename.

/NB Không hiển thị bảng (banner) trên màn hình khi login.

8.4. Lệnh Logout.

Chức năng: ra khỏi mạng, tạm làm việc chỉ nhìn thấy thư mục LOGIN của máy chủ, trước khi tắt máy người sử dụng cần thực hiện lệnh này.

Cú pháp:

LOGOUT [server name | T | /Ver]

Các option:

Server name Ra khỏi máy chủ có tên là server name.

/T Ra khỏi mạng để lại dịch vụ thư mục bindery connection

/Ver Ra khỏi mạng và cho biết version của mạng đang sử dụng.

Ví dụ:

Máy đang làm việc (login) với 3 máy chủ có tên là FS1, FS2 và FS3.

Muốn ra khỏi máy chủ FS1, ta gõ lệnh: **Logout FS1**

Muốn ra khỏi tất cả các máy chủ, ta gõ: **Logout**

8.5. Lệnh NLIST.

a. **Chức năng:** cho biết các thông tin về các user, group và các đối tượng khác.

Cú pháp:

NLIST Class type [property search option] [display option] [basic option]

Classtype: có các loại như sau:

Server	Profile
Computer	Alias

Directory map	Print queue
Organization Unit	Printer
User	Print server
Group	Organization
Volume	AFP server

Ví dụ:

Nlist Server	Xem các server trong context hiện tại.
Nlist "directory map"	Xem ánh xạ ô đĩa của trạm làm việc hiện tại.
Nlist "organization"	Xem các mức tổ chức của mạng.

b. Chỉ định các option trong khi xem các đối tượng.

Cú pháp:

NLIST Classtype [=object name] [basic option]

Các option:

/A Xem các user và server.

/Ver Cho biết version mạng ta đang làm việc.

/Tree Xem các cây thư mục.

/B Xem các Server trong chế độ bindery

/S Xem các Server trong context hiện tại.

Ví dụ

Nlist server /S	Liệt kê các Server trong context hiện tại.
Nlist server /B	Liệt kê các Server trong chế độ bindery
Nlist User /A	Liệt kê các Server trong context hiện tại.
Nlist Volume /CO "O = Bindery FPT"	Xem các user đang login
	Xem các volume trong context O = FPT

c. Chọn dữ liệu nào sẽ xem.

Cú pháp:

NLIST Classtype [=object name] [display option]

Các option:

/D Xem chi tiết toàn bộ (detail).

/N Chỉ xem tên đối tượng thôi.

Show property chỉ định thuộc tính cần xem là property

Ví dụ:

Nlist Group = Manager /D Xem thông tin chi tiết trong nhóm

Nlist User = ThangC /D Manager

Nlist User Show Xem thông tin chi tiết của user ThangC

"telephone", "street address" Xem địa chỉ, số điện thoại của toàn bộ các user.

8. 6. Lệnh MAP.

Chức năng: ấn định tên ổ đĩa logic tới một đường dẫn (hay một thư mục).

Cú pháp:

MAP [option | /ver] [search:=[driver:=]] [driver:=] [path] [/w]

Các option:

INS Thêm một đường dẫn (insert).

DEL Xoá một đường dẫn (delete).

N Thêm một đường dẫn với tên ổ đĩa hợp lệ tiếp theo.

R Thêm ổ đĩa như là thư mục gốc.

/VER Cho biết version mạng ta đang sử dụng.

/W Không thay đổi (ghi lại) môi trường chính.

Ví dụ

Map N TH/SYS:Login

Thêm một đường dẫn với tên ổ đĩa hợp lệ tiếp theo, chỉ tới thư mục Login trong Volume SYS của máy chủ tên là TH.

Map S10:=W:=TH/Data:setup

Thêm đường dẫn thứ 10 với tên ổ đĩa logic là W chỉ tới đường dẫn là thư mục setup trong volume có tên Data của máy chủ TH.

MAP R H:= TH/data:User/KT

Ấn định ổ đĩa logic gốc H là thư mục KT trong volume có tên

8.7. Lệnh WHOAMI

Chức năng: cho biết người đang vào mạng tại trạm làm việc hiện tại là ai.

Cú pháp:

Whoami [Server] [/S] [/G] [/W] [/R] [/O] [/ALL] [/C] [/VER]

Các option:

Server: Chỉ định tên máy chủ, để trống nếu muốn xem toàn bộ các máy chủ có liên quan.

/S Cho biết quyền tương đương (với ai) của người đang login.

/G Cho biết người đang login thuộc nhóm nào.

/W Cho biết thông tin về nhóm của người đang login.

/R Cho biết các quyền sử dụng mạng của người đang login.

/C Cho phép xem từng trang màn hình.

/Ver Cho biết version mạng đang sử dụng.

8.8. Lệnh SETPASS.

Chức năng: Thay đổi mật khẩu của user đang trong mạng.

Cú pháp:

Setpass [Ver] [[Server name/] [username]]

Các option:

/Ver cho biết version mạng đang sử dụng.

Servername thay đổi mật khẩu trong máy chủ có tên là Servername

Username thay đổi mật khẩu của user khác có tên Username (nếu ta có quyền)

8.9. Lệnh SEND.

Chức năng: gửi một thông báo tới một đối tượng.

Cú pháp:

Send "message" [TO] <object>

Các option:

message dòng thông báo mà ta muốn gửi.

object đối tượng mà ta cần gửi thông báo tới (user, group, server).

Ví dụ:

Send "Hi" to Guest Gửi thông báo "Hi" tới user tên là Guest

Send "Good Morning" to FIS Gửi thông báo " Good Morning " tới group tên
là FIS

8.10. Lệnh Rconsole.

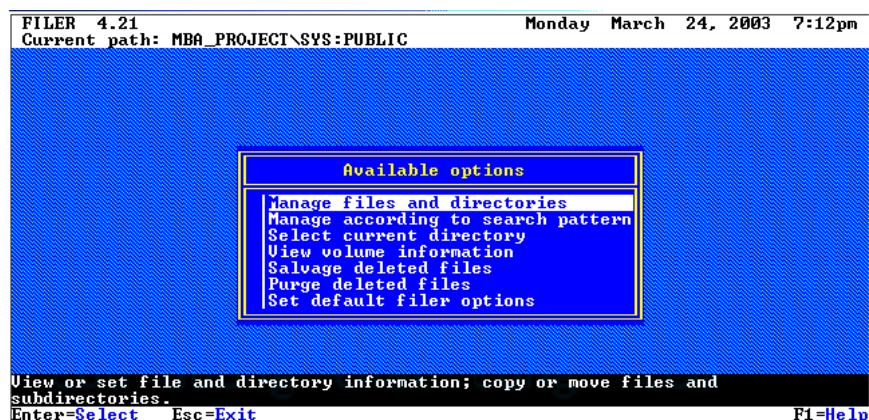
Chức năng: Dùng để thao tác với máy chủ và các lệnh trên nó ở trạm làm việc (remote console).

Cú pháp: Rconsole Tên máy chủ

Nếu không vào tên máy chủ, máy sẽ đưa ra danh sách các máy chủ đang hoạt động và hỏi ta muốn làm việc với máy chủ nào, và dạng connection của trạm làm việc đang dùng.

8.11. Lệnh Filer

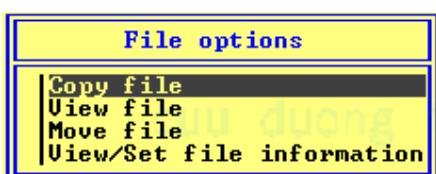
Chức năng: tiện ích về thư mục và tệp tin



Cú pháp: Đây là một trình làm theo giao diện thực đơn, các chức năng cơ bản được thể hiện như sau:

- Manage files and directories: Sao chép, xem, thay đổi, quyền hạn và thuộc tính của tệp tin, thư mục.

Sau khi lựa chọn thư mục và tệp tin, thực đơn cuối cùng cho phép thực hiện các chức năng như sau:



- Manage according to search pattern: tìm kiếm tệp tin
- View volume information: Xem các thông tin về volume
- Salvage deleted files: Khôi phục tệp tin bị xóa, nếu chưa dùng lệnh Purge
- Purge deleted files: xóa vĩnh viễn tệp tin

PHẦN III

HỆ ĐIỀU HÀNH MẠNG WINDOWS 2000

§ 1. TỔNG QUAN VỀ MICROSOFT WINDOWS 2000

1.1. Windows 2000 Server

Windows 2000 Server là hệ điều hành trên các File Server để quản lý mạng cục bộ, mạng diện rộng cũng như phục vụ các ứng dụng, đây là phiên bản kế tiếp của Windows NT Server. Windows 2000 Server cho phép quản lý, chia sẻ thông tin, truy nhập máy in và các thiết bị ngoại vi trên mạng. Nó cung cấp cơ sở hạ tầng ứng dụng, hỗ trợ nhiều giải pháp nghiệp vụ cho các hệ quản trị cơ sở dữ liệu, các ứng dụng khác của Oracle, Sybase, Btrieve, v.v. ... Windows 2000 Server có nhiều tính năng mới so với phiên bản Windows NT Server.

Có bốn phiên bản của hệ điều hành Windows 2000, một phiên bản dành cho các máy trạm (workstation) và các phiên bản khác là các cấp độ phức tạp dành cho server khác nhau.

Windows 2000 Professional

Phiên bản "Professional" được dành cho các máy trạm kế tiếp bản Windows NT4 Workstation. Phiên bản này có thể sử dụng trong văn phòng các doanh nghiệp và các chuyên gia với các tính năng về cấu hình và bảo mật mở rộng. Giao diện Windows 2000 Professional tương tự như Windows 95/98 trên màn hình nhưng hoàn toàn khác về mặt kỹ thuật. Nó hoàn toàn không phải là một sản phẩm kế thừa trực tiếp với Windows 95 hay 98 và không dành để sử dụng tại nhà. Phiên bản Professional sẽ có thể dùng đồng thời hai chip xử lý (nếu được cài đặt).

Windows 2000 Server

Đây là tùy chọn dành cho server cơ sở trong các doanh nghiệp trung bình và nhỏ và kèm thêm một Web server, thiết bị đầu cuối, và các dịch vụ truy cập từ xa. Nó sẽ có thể hỗ trợ tới bốn bộ xử lý được cài đặt đồng thời trên một máy tính.

Windows 2000 Advanced Server

Advanced Server giữ vai trò của "Phiên bản NT Enterprise" với việc có thể hỗ trợ đến tám bộ vi xử lý cài đặt đồng thời. Nó dành để thực hiện các cơ sở dữ liệu chuyên sâu.

Windows 2000 Datacenter Server

Xuất hiện vào cuối năm 2000 là phiên bản về Windows 2000 rất mạnh đối với các mạng lớn như là công ty, trong các trường đại học, học viện. Có thể sử dụng đồng thời đến 16 bộ xử lý và 64 GB bộ nhớ.

1.2. Active Directory (AD)

a. Khái niệm

AD là một dịch vụ của Windows 2000 Server, là cơ sở dữ liệu của hệ thống có chức năng nhằm quản lý toàn bộ hệ thống tài nguyên của mạng. Thiết lập, quản lý và cung cấp các dịch vụ mạng cho người dùng.

- Vấn đề bảo mật: AD cung cấp các công cụ nhằm xác minh (authentication) và cấp phép (authorization) cho người dùng mạng để có thể truy cập mạng, đồng thời ngăn chặn những truy cập bất hợp pháp.

+ Duy trì một danh bạ về người dùng và các đối tượng khác trên mạng.

+ Tập trung các danh bạ để hình thành một Server truy nhập.

- Vấn đề tìm kiếm thông tin trên mạng:

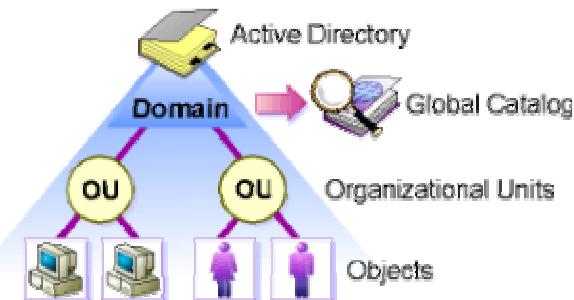
+ Tìm kiếm tên các server thông qua tên

+ Tìm kiếm, giải đáp tên qua IP

- Phân cấp quản trị mạng

- Liên lạc và sao chép thông tin trên mạng lớn

- Có thể quản lý một hệ thống mạng rất lớn



b. Các nội dung, đặc điểm của AD

Miền (domain)

Đơn vị bảo mật của Windows 2000 dùng lưu trữ cơ sở dữ liệu người dùng mạng, Server lưu trữ CSDL này được gọi là domain controller, Active Directory server hay có thể được gọi là Logon server. Nhóm các máy phải thông qua máy domain controller để biết thông tin xác minh về người dùng được gọi là một domain (miền), Microsoft cho phép lưu trữ 1,5 triệu tài khoản người dùng trên một domain. Mỗi một máy server W2k có chứa một bản sao tài khoản người dùng mức mạng thì được coi là một domain controller.

Nhóm (group)

Tập hợp một nhóm đối tượng nào đó trên mạng cùng một số quyền, hoặc cùng chịu chung một chính sách quản lý được coi là một nhóm (group), quyền của đối tượng này sẽ được gán gián tiếp thông qua group, đối tượng nào là thành viên của nhóm sẽ có tất cả các quyền của nhóm này. Để áp dụng các chính sách lên nhóm, Windows 2000 cho phép có thể tạo nhóm chứa người dùng, nhóm chứa các máy trên mạng. Các nhóm có thể được lồng vào nhau sâu hơn một cấp, song không được phép đệ qui. Windows 2000 cung cấp bốn loại nhóm:

- Machine local group (nhóm máy cục bộ): nhóm này có chức năng cho máy cục bộ, nó có thể chứa các nhóm miền cục bộ, nhóm toàn miền, nhóm chung.
- Domain local group (nhóm miền cục bộ): nhóm có chức năng cho một miền, nó có thể chứa các nhóm khác miễn là chúng cùng một miền với domain local group này.
- Nhóm toàn miền (global group): nhóm có chức năng cho nhiều miền
- Nhóm chung (universal group): có thể chứa bất kỳ một global hoặc một universal group nào

Để tương thích với tên miền ở phiên bản trước Windows NT, khi cài đặt Windows 2000 để ngầm định chế độ quản lý tên miền hỗn hợp (mixed mode), nó không tạo ra các nhóm universal. Nếu tất cả các máy domain controller trong mạng đều cài windows 2000 thì có thể chuyển sang chế độ native mode và có thể thực hiện được các nhóm universal.

Kích thước các nhóm được windows 2000 giới hạn ở mức 5000 thành viên, nếu muốn tạo nhóm có số thành viên lớn hơn thì cần phải tạo ra một số nhóm nhỏ sau đó đặt số nhóm này vào một nhóm khác.

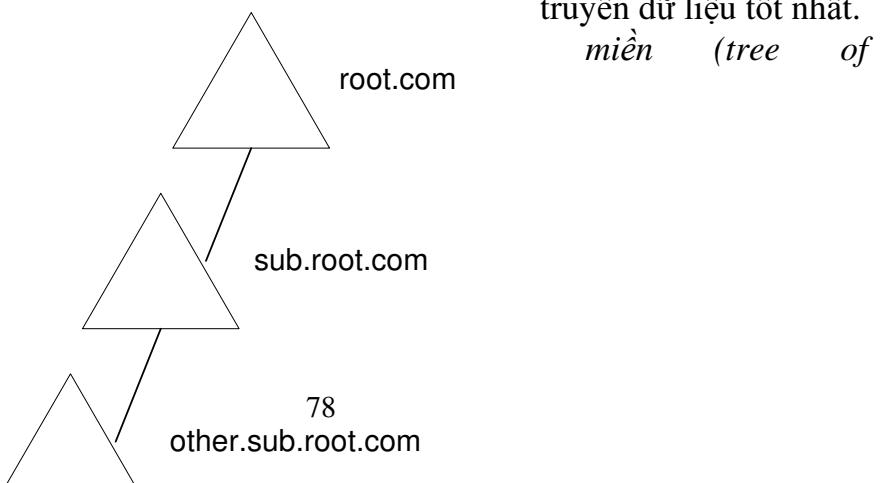
Đơn vị tổ chức (Organizational unit – OU)

Windows 2000 chia miền thành đơn vị nhỏ hơn đó là OU, OU được tạo ra và có thể được trao quyền kiểm soát gọi là “sự ủy quyền kiểm soát” (delegating control). Một hoặc một tập hợp người dùng có thể được trao quyền kiểm soát này.

Địa bàn (site)

Nếu te được AD dùng để quản lý theo giác độ địa lý của mạng, mỗi khu vực được kết nối bằng LAN thì được gọi là một site. Để quản lý windows 2000 cần được cung cấp thông tin chi tiết về cách bố trí vật lý của mạng, nó có thể tính ra nơi nào có những đường liên kết LAN, WAN. Khi cần sao chép dữ liệu qua lại giữa các domain controller, nó sẽ nén dữ liệu, dùng những thông tin về route để tính ra đường truyền dữ liệu tốt nhất.

Cây của các domains



Hệ thống tên miền trong các doanh nghiệp có mạng đa miền được xây dựng theo cấu trúc hình cây. Miền đầu tiên được gọi là gốc (root), các miền dưới nó được gọi là miền con (child domain), dưới nó có thể có một số cấp nữa. Windows 2000 có thể tự động tạo các quan hệ ủy quyền giữa mỗi miền và miền con.

Rừng của các miền (forest of domains)

Tập hợp các cây (tree) được khorp lại gọi là rừng (forest), các cây trong rừng có cấu trúc giống như một cây, nếu xét theo các mối quan hệ ủy quyền. Có thể quyết định miền đầu tiên được tạo ra sẽ là gốc (root). 

1. 3. Địa chỉ trong giao thức TCP/IP

a. Khái niệm

Địa chỉ của nút là địa chỉ thực thể hay địa chỉ của thiết bị trên mạng, để xác định vị trí của nút mạng TCP/IP sử dụng nguyên tắc đánh số duy nhất gọi là địa chỉ IP. Tất cả các thiết bị trên mạng nào sử dụng bộ giao thức TCP/IP đều cần một địa chỉ IP độc nhất. Địa chỉ IP được dùng phổ biến hiện tại gọi là (IPv4 - Internet Protocol Address Version 4), về cấu tạo IPv4 có 32 bit, trên lý thuyết IPv4 có thể cung cấp $2^{32} = 4\ 294\ 967\ 296$ địa chỉ. Tuy nhiên với số lượng địa chỉ trên thì chỉ có thể cung cấp cho hệ thống mạng doanh nghiệp. Ngày nay khi Internet đã trở nên phổ biến, tốc độ tăng trưởng của mạng rất cao, IPv4 không đáp ứng được. Nhóm chuyên trách về kỹ thuật của tổ chức Hiệp hội Internet IETF (Internet Engineering Task Force) đã đề xuất và thực hiện địa chỉ thế hệ mới IPv6 (IP Address Version 6). Về cấu tạo IPv6 có 128 bit, trên lý thuyết IPv6 cung cấp $2^{128} = 340\ 282\ 366\ 920\ 938\ 463\ 463\ 374\ 607\ 431\ 768\ 211\ 456$ địa chỉ.

b. Xác định địa chỉ IP(v4)

- Cách cấu tạo: (4 bytes)

X.X.X.X

X=0 ÷ 255

Cách nhau dấu chấm(.)
IP chia làm 5 lớp: theo giá trị của X

X	Lớp (class)	Subnet mask
1 - 126	A	255.0.0.0
128 - 191	B	255.255.0.0
192 - 223	C	255.255.255.5
224 - 239	D	Địa chỉ đặc biệt
240 - 247	E	Chưa dùng tới

- Địa chỉ măt lưới: IP được chia làm 2 phần: địa chỉ măt lưới (Network portion or netid), địa chỉ máy tính (host portion or hostid).

Lớp	Địa chỉ măt lưới	Địa chỉ máy tính trong lưới
A 9.67.5.12	X.0.0.0 9.0.0.0	X.X.X 67.5.12
B 150.5.7.9	X.X.0.0 150.5.0.0	X.X 7.9
C 212.15.17.19	X.X.X.0 212.15.17.0	X 19

Với nguyên tắc này các Routers căn cứ vào địa chỉ măt lưới và sẽ chuyển tiếp bó tin từ măt lưới này qua măt lưới khác cho tới khi đúng địa chỉ của măt lưới đó. Khi bó tin đã tới đúng măt lưới Routers chuyển bó tin cho máy nhận căn cứ vào phần địa chỉ của máy nhận.

§ 2. CÀI ĐẶT WINDOWS 2000 SERVER

2.1. Một số vấn đề chung

Hệ thống files trên của MicroSoft

- FAT của DOS, dùng trên DOS, NT, Windows 2000; có thể định dạng khi setup. FAT cho phép truy nhập từ các hệ điều hành khác như Windows NT, Windows 9.X, DOS. Windows NT, W2000 không hỗ trợ chế độ bảo mật trên FAT

- FAT32 dùng trên Windows 98 và các phiên bản tiếp theo, Windows 2000 không hỗ trợ chế độ bảo mật trên FAT32

- NTFS 4 của NT, NTFS 5 của Windows 2000; có thể định dạng khi setup. Các hệ điều hành khác không thể truy nhập. Windows NT, Windows 2000 hỗ trợ chế độ bảo mật trên NTFS, chế độ bảo mật đã được nâng cấp trên NTFS 5.

- HPFS hệ thống files có chế độ thực hiện cao dùng trên NT và OS/2 ; không định dạng khi setup

Tên SERVER

- Là một dãy ký tự đại diện cho máy tính
- Qui ước đặt tên: Theo qui định của hệ điều hành, ngắn gọn, có qui luật
- Chọn lựa cách kết nối mạng*
 - Giao thức: TCP/IP, NetBEUI
 - Quan hệ thành viên của server
 - + Xác định: thành viên của nhóm công tác, thành viên của miền, hay một Domain Controller
 - + Có thể không cần quyết định vai trò khi cài đặt, chỉ cần lựa chọn cho máy tham gia một nhóm công tác hay một miền, sau khi cài đặt xong có thể thăng cấp máy thành DC.
 - Các thành phần bổ xung
Dịch vụ khác như Internet Information Server, dịch vụ DHCP, ... có thể không cần phải lựa chọn khi cài đặt, những dịch vụ này sẽ được bổ xung khi mạng có nhu cầu

Vấn đề cấp phép: lựa chọn một trong những cách cấp phép sau

- Cấp phép theo chỗ ngồi (per-seat licensing): Đòi hỏi mỗi máy khách trên mạng khi truy cập vào server đều phải có giấy phép riêng của nó. Cần phải tính trên mạng có bao nhiêu máy khách và khai báo số chỗ ngồi. Theo cách này sẽ không cần tính đến có bao nhiêu mối liên kết (connection) đồng thời từ các máy khách vào cùng một server, hoặc mỗi máy khách giữ bao nhiêu mối nối kết với các server.
- Cấp phép theo server (per-server licensing): đòi hỏi mỗi nối kết giữa máy khách với server phải có một giấy phép, nếu một máy khách nối với 5 server khác nhau thì sẽ cần 5 giấy phép.

2.2. Cài đặt windows 2000 server

a. Yêu cầu cơ bản

Yêu cầu về phần cứng:Tối thiểu

- Pentium 166
- 64 MB RAM
- HD 850 MB thêm 100 MB ứng với 64 MB RAM bộ nhớ bị thiếu
- Các phần cứng khác phải tương thích với Windows 2000, danh sách phần cứng được ghi trên đĩa CD cài đặt và trên trang Web www.microsoft.com/hwtest/hcl
 - Card mạng, dây mạng đã được lắp đặt, lưu ý về kiểu card mạng (ISA, PCI), cấu hình card mạng như IRQ, địa chỉ I/O, những thông số khác về card mạng.
 - Các thiết bị ngoại vi khác như máy in: kiểu, cổng máy in; MODEM ...

- Loại vi xử lý (Intel, Alpha, ...) thư mục I386 chứa phần SETUP cho Intel và tương thích. Khi cài đặt chạy SETUP ở thư mục thích hợp, hoặc bộ đĩa cài đặt được dùng cho bộ vi xử lý phù hợp.

- Phần mềm:*

- Đĩa cài đặt từ CD ROM
 - Các Driver cho thiết bị

- Chuẩn bị*

- Thiết lập cấu hình trong BIOS của máy tính: nếu để chế độ PnP, thì cần dành IRQ cho các thiết bị cũ theo chuẩn ISA như card mạng, card âm thanh.
 - Chuẩn bị đĩa cứng:
 - + Nếu dùng toàn bộ đĩa cứng cho Windows 2000: không cần phân chia Partition, định dạng (format) trước.
 - + Nếu chỉ dùng 1 phần của đĩa cứng: cần phân chia Partition, có thể định dạng (format) trước.

- b. Một số phương pháp cài đặt:*

- Cài đặt từ đĩa cứng*

- Giai đoạn 1: chuẩn bị và bắt đầu cài đặt
Chuẩn bị đĩa cứng: Tạo trên đĩa cứng 2 Primary Partition (FAT16 hoặc FAT32) trong đó có 1 Partition có thể khởi động được từ DOS (ở đĩa C:), Partition thứ hai có thể sử dụng để ghi chép các tệp tin cài đặt (ở đĩa D:). Sao chép toàn bộ thư mục I386 ở đĩa cài đặt vào ổ đĩa D:

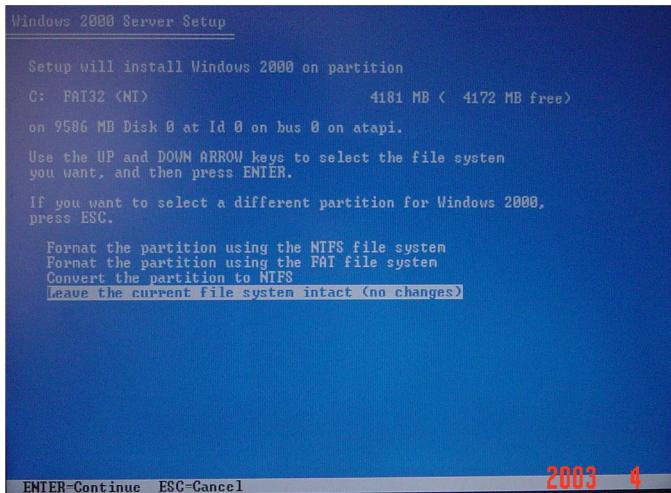
Sau khi máy tính đã khởi động từ DOS, chạy tệp Winnt.exe trong thư mục I386, trên màn hình hiện thị hộp hội thoại để xác định đường dẫn của tệp các tin cài đặt (Enter the path where Windows 2000 files are to be found), nếu trên màn hình đã hiển thị đúng đường dẫn , bấm Enter để tiếp tục.

Chương trình setup của Windows bắt đầu thực hiện việc cài đặt: sao chép các tệp tin cần thiết lên đĩa cứng, trên màn hình hiển thị quá trình sao chép tệp tin (Setup is copying files ...), sau khi sao chép xong máy tính yêu cầu khởi động lại.

- Giai đoạn 2

Sau khi khởi động lại chương trình setup tìm kiếm các thiết bị trên máy , qua giai đoạn này máy dừng lại để yêu cầu xác định: cài đặt Windows 2000 từ đầu hoặc cài đặt kiểu sửa lỗi (repair) nếu trên đĩa cứng đã cài Windows 2000. Bấm Enter để tiếp tục cài đặt, trên màn hình hiển thị các thông tin về bản quyền (Windows 2000 Licensing Agreement), bấm F8 để tiếp tục. Tiếp theo trên màn hình hiển thị tất cả các Partition của đĩa cứng mà có thể cài đặt Windows 2000,

cần xác định các Partition sẽ cài đặt. Sau khi chọn Partition tiếp tục lựa chọn cấu trúc hệ thống files:



- + Convert the partition to NTFS: Chuyển cấu trúc tệp tin sang dạng NTFS
- + Leave the current file system intact (no changes): Giữ nguyên cấu trúc tệp tin cũ

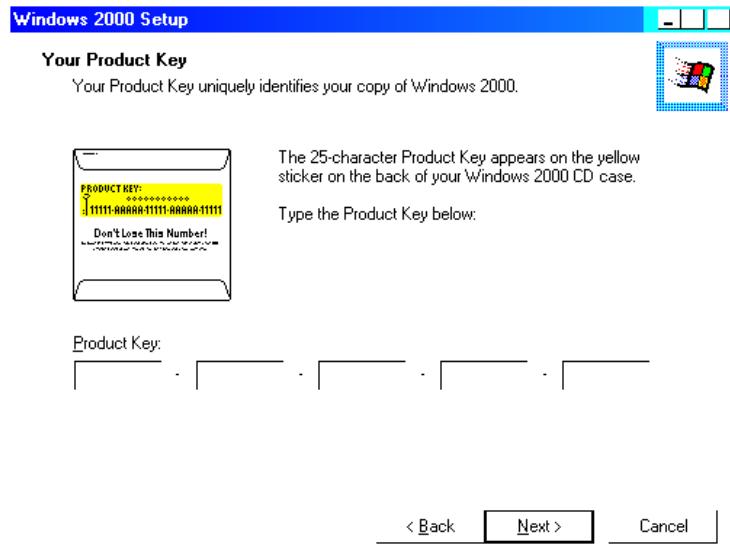
Thực hiện một trong hai lựa chọn trên, máy sẽ khởi động lại và chuyển sang giai đoạn 3, giai đoạn màn hình Graphic.

- Giai đoạn 3

Sau khi khởi động lại, trình setup thực hiện việc xác định và cài đặt thiết bị trên máy (Installing devices), công việc này diễn ra khá lâu nếu gặp các thiết bị mà Windows 2000 không thể cài đặt được có thể dẫn đến treo máy, kết thúc quá trình cài đặt mà không thành công. Tiếp theo thực hiện các lựa chọn về ngôn ngữ, bàn phím sử dụng (Regional settings), bấm Next để tiếp tục. Các lựa chọn tiếp theo:

- + Xác định tên người và tổ chức (cơ quan) sử dụng hệ điều hành.
- + Xác định Product key: bấm chính xác các ký tự vào các ô theo mẫu sau, sau đó chọn Next

cuu duong than cong. com



- + Xác định kiểu cấp phép (licensing) có hai kiểu để có thể lựa chọn per-server và per-seat
- + Xác định tên máy tính (Computer name) và mật khẩu của user quản trị mạng (Administrator)



- + Xác định các thành phần của Windows (Add or remove components of windows 2000), nếu để các tham số ngầm định, bấm Next.
- + Xác định ngày, giờ , múi giờ quốc tế của hệ thống
- + Cài đặt các thông số mạng (Networking settings): có hai lựa chọn Typical setting hoặc Custom settings, bấm Next. Tiếp theo xác định các tham số trên Workgroup or computer domain. Chọn “NO, ...” và bấm trên ô workgroup một dãy ký tự để có thể làm tên cho một workgroup, lựa chọn này để có thể cấu

hình máy thành máy Server. Nếu chọn “YES, ...” cần phải điền tên domain đã có ở trên mạng, và làm các bước tiếp theo hướng dẫn trên màn hình.

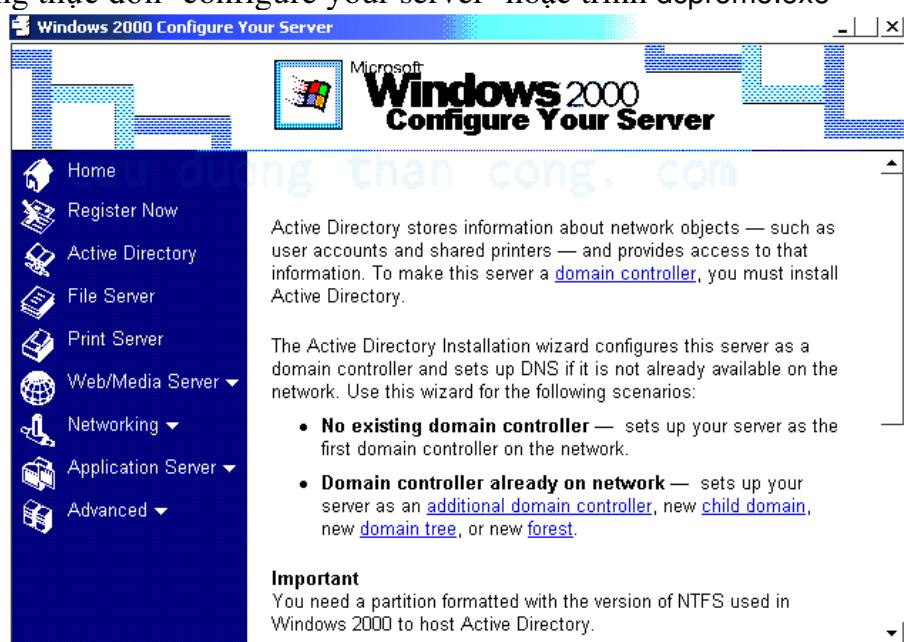
Trình Setup tiếp tục thực hiện quá trình cài đặt, nếu thiết bị phần cứng không có lỗi và nếu các thiết bị đó được Windows 2000 chấp nhận, thì quá trình cài đặt thành công, máy sẽ khởi động lại.

Cài đặt từ bộ đĩa CD ROM Windows 2000

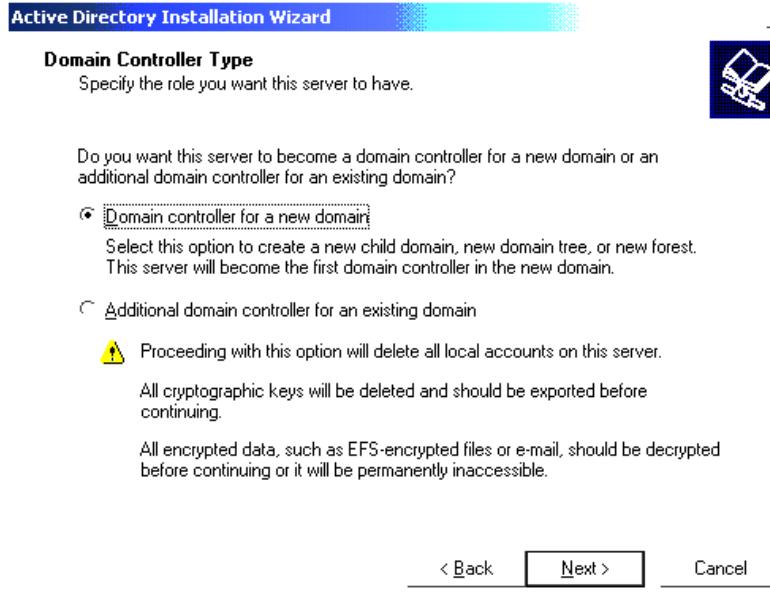
- Yêu cầu:
 - + Máy tính có ổ đĩa CD ROM, có thể khởi động được từ ổ CD
 - + Đĩa CD ROOM cài đặt Windows 2000.
- Cài đặt
 - + Thiết lập chế độ khởi động máy tính từ ổ đĩa CD
 - + Đưa đĩa CD ROOM cài đặt Windows 2000, khởi động máy
 - + Nhập các tham số cần thiết

2.3. Cài đặt Active Directory

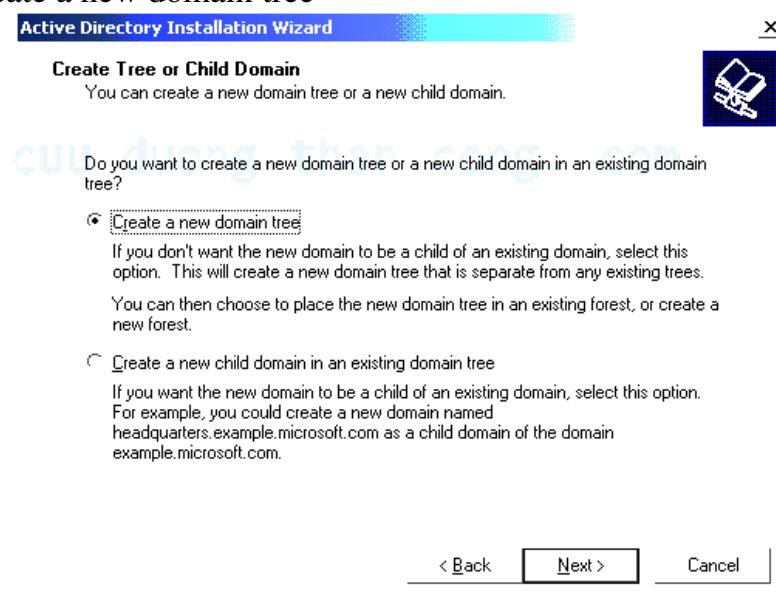
Sử dụng thực đơn “configure your server” hoặc trình dcpromo.exe



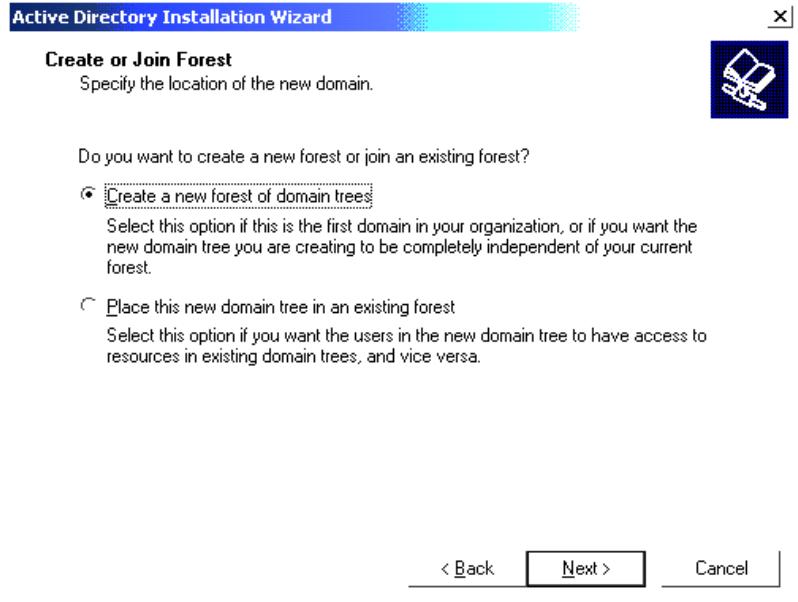
Lựa chọn tạo miền mới



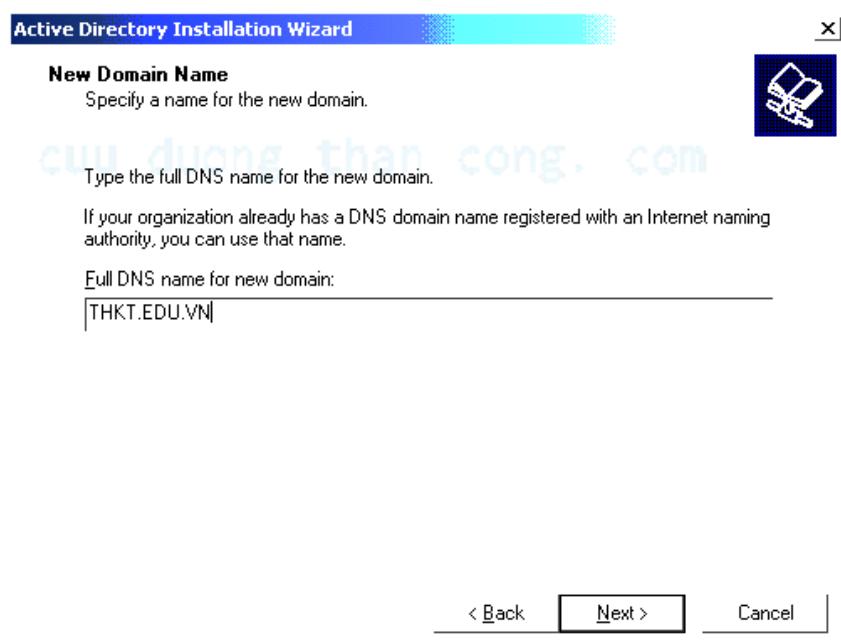
Mỗi miền phải thuộc về một cây nào đó, đây là miền đầu tiên trong một cây mới chọn “create a new domain tree”



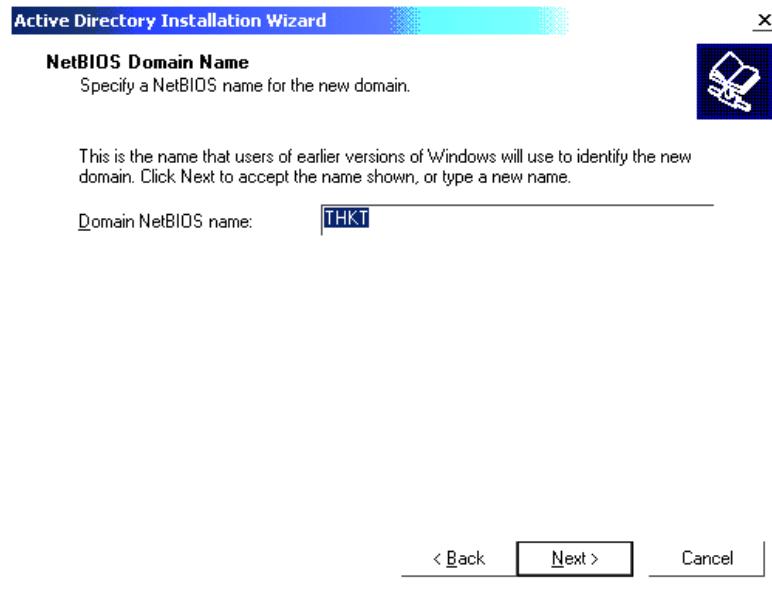
Xác định cây mới này trong rừng mới, chọn “create a new forest of domain tree”



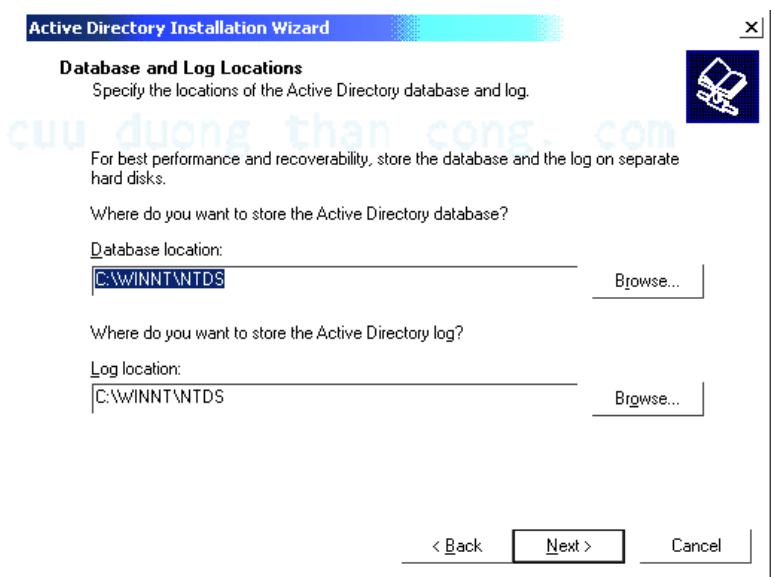
Xác định tên đầy đủ của miền mới



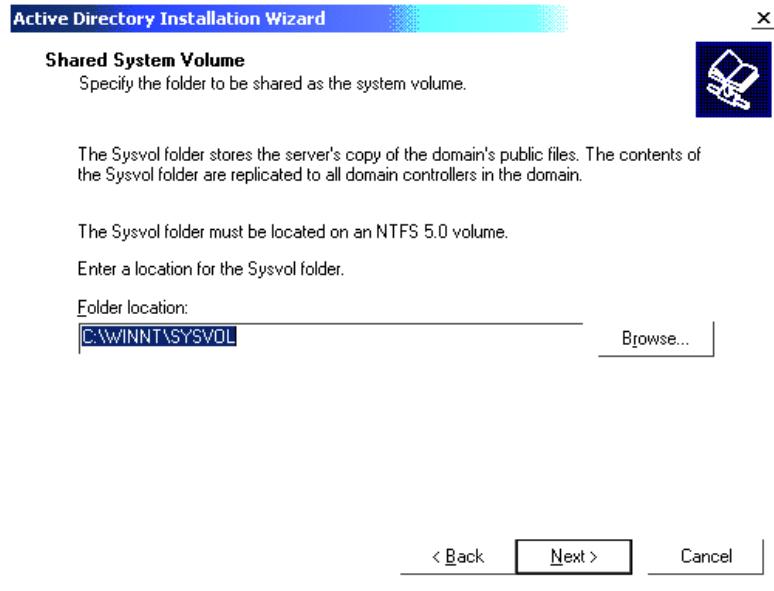
Tên kiểu cũ sẽ được xác lập



Chọn chỗ đặt tệp tin cơ sở dữ liệu AD và tệp tin ghi chép giao dịch, chọn theo chế độ ngầm định của Windows 2000



Chọn chỗ đặt folder SYSVOL



2.4. Hiệu chỉnh các tham số

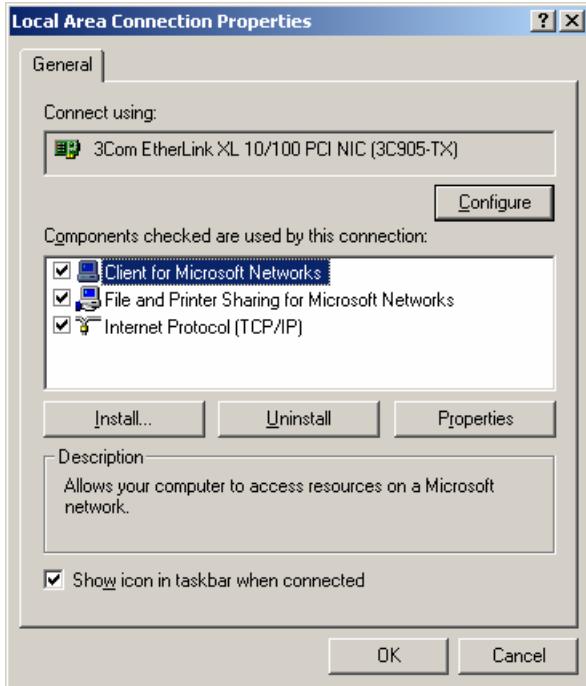
Sử dụng CONTROL PANEL , đây là một nhóm phần mềm cung cấp các công cụ cho người quản trị mạng, có thể hiệu chỉnh các tham số liên quan về phần cứng phần mềm. Mỗi một biểu tượng trên cửa sổ CONTROL PANEL sẽ đảm nhiệm một chức năng nhất định.



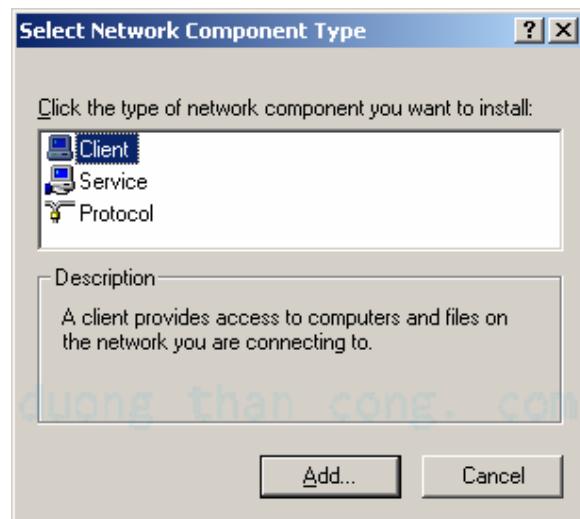
a. Hiệu chỉnh các tham số về mạng

Bao gồm các công việc

Chọn biểu tượng NETWORK and Dial-up, tiếp theo bấm phải chuột vào dòng Local Area Connection và chọn Properties, trên màn hình hiển thị cửa sổ sau:



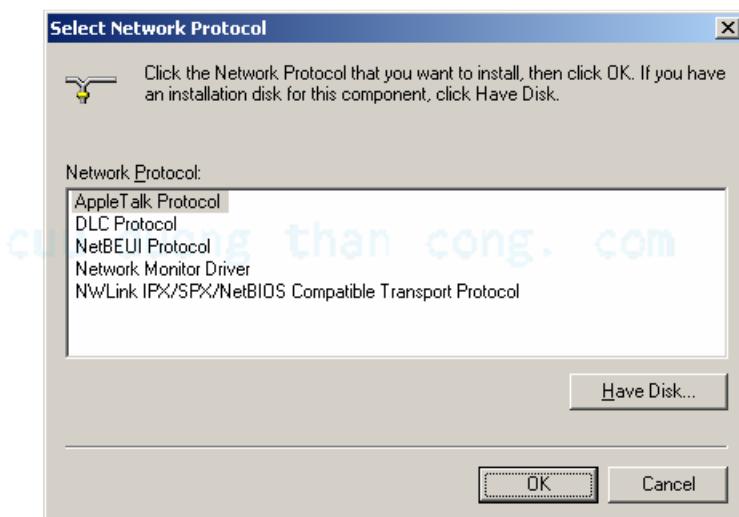
Chọn Install để thêm hoặc loại bỏ các dịch vụ (Service), các bộ giao thức (Protocol), các client cho Server. Chọn Uninstall để gỡ bỏ các dịch vụ, giao thức và client. Chọn Properties để điều chỉnh các tham số chi tiết.



Các dịch vụ mạng Windows 2000 Server cho phép các máy tính trong mạng truy cập và sử dụng nguồn tài nguyên của mạng.



Tùy từng loại giao thức, người quản trị mạng cần chọn Properties để điều chỉnh các thông tin chi tiết.



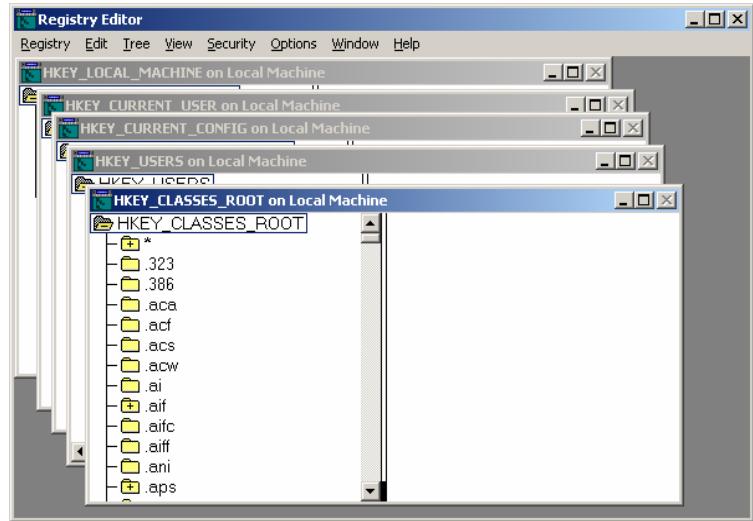
b. Hiệu chỉnh các tham số khác

2.5. Cơ sở dữ liệu Registry

a. Khái niệm

Registry của Windows 2000 là một cơ sở dữ liệu có cấp bậc của những thiết định dùng để mô tả tài khoản người dùng, phần cứng của máy, và các ứng dụng. Mỗi khi thay đổi một lựa chọn về phần cứng hay phần mềm, thì những thay đổi này thường được ghi lại trong registry. Registry còn lưu nhiều thiết định của hệ thống ví dụ như khi khởi động máy Windows 2000 sẽ tự kiểm tra những thiết bị phần cứng được gắn vào máy. Có thể xem và sửa registry bằng trình REGEDT32.EXE (nằm trong thư mục \winnt\system32).

b. Nội dung Registry



Cây con (subtree)

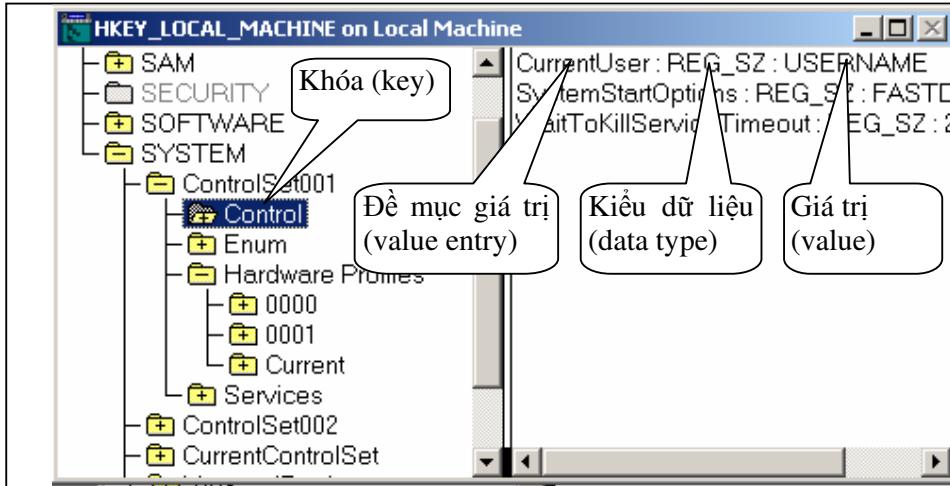
Registry lưu trữ tất cả những thông tin bằng cách chia chúng ra làm năm cây con:

- HKEY_LOCAL_MACHINE: Chứa thông tin về phần cứng, những thiết định dành cho các hệ thống đang chạy trên máy.
- HKEY_CURRENT_USER: Chứa thông tin về người dùng (user profile) được truy cập server, chứa các cấu hình, các thiết định dành cho các desktop đang chạy trên server. longthanhcong.com
- HKEY_USER: Chứa con trỏ (pointer) chỉ đến cây con HKEY_CURRENT_USER và đến một default profile. Default profile chứa các thiết định ngầm định.
- HKEY_CLASSES_ROOT: Giữ các thông tin về file association , giúp hệ điều hành biết cách mở tin bằng chương trình nào.

Khóa (key), để mục giá trị, tên, giá trị, kiểu dữ liệu

Khóa là một đề mục có tác dụng chia tách thông tin ra thành các đoạn, có thể có các khóa bên trong các khóa, gọi là các khóa con (subkey), khóa con có thể có nhiều cấp. Khóa có tên, tên khóa được viết liền và thường được đặt ngắn gọn để có thể viết vừa một hàng chữ.

longthanhcong.com



Dữ liệu trong registry được qui định như sau:

- REG_BINARY: dữ liệu nhị phân thô
 - REG_DWORD: Kiểu nhị phân khác dài 4 bytes
 - REG_EXPAND_SZ: chuỗi ký tự có kích thước thay đổi
 - REG_MULTI_SZ: một kiểu dữ liệu chuỗi khác, cho phép nhập thêm tham số
 - REG_SZ: chuỗi đơn giản
- Các tổ của registry (hive)

Registry chủ yếu được chứa trong các tệp tin gọi là tổ (hive), các tổ là các tệp nhị phân do vậy muốn đọc nó cần có trình s;oạn thảo phù hợp. Việc chia các tổ nhằm nạp, sao lưu dự phòng một cách thuận tiện. Các tệp tin tổ được tổ chức như sau:

Cây/khóa	Tệp tin
HKEY_LOCAL_MACHINE\SAM	SAM (chính) và SAM.LOG (dự phòng)
HKEY_LOCAL_MACHINE\SECURITY	SECURITY (chính) SECURITY.LOG (dự phòng)
HKEY_LOCAL_MACHINE\SOFTWARE	SOFTWARE (chính) SOFTWARE.LOG (dự phòng)
HKEY_LOCAL_MACHINE\SYSTEM	SYSTEM (chính) SYSTEM. ALT (dự phòng)
HKEY_USER\DEFAULT	DEFAULT (chính) DEFAULT. LOG (dự phòng)
HKEY_USER\SECURITY ID	NTUSER.DAT
HKEY_CURRENT_USER	NTUSER.DAT
HKEY_CLASSES_ROOT	Được tạo lúc boot máy

- Lưu dự phòng và khôi phục

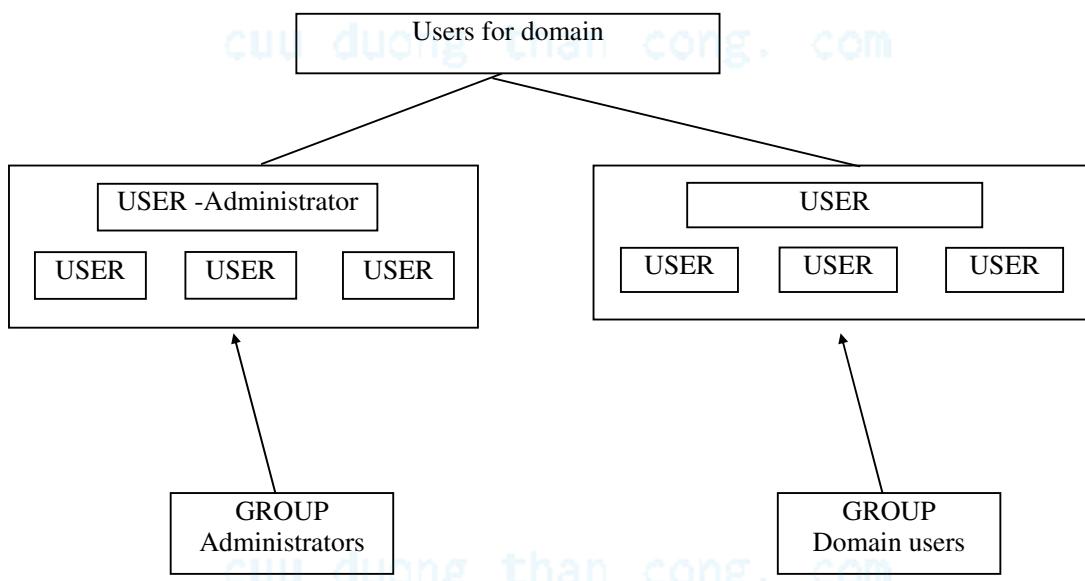
Mỗi khi tệp tin tổ bị thay đổi, trước tiên nó sẽ ghi vào các tệp tin dự phòng (LOG) của nó, khi sự mô tả về những thay đổi đối với tệp tin tổ đã hoàn tất, nó mới thực sự ghi chính tệp tin tổ. Nếu hệ thống gặp sự cố trong

thao tác ghi vào tệp tin tǒ, thì hệ thống có thể lấy thông tin từ tệp dự phòng để khôi phục tệp tin tǒ trở lại tình trạng trước đó. Trong một số trường hợp registry bị lỗi thì có khả năng gây lỗi cho Windows 2000, do vây cần phải sao lưu registry. Để sao lưu toàn bộ registry có thể dùng trình tiện ích ntbackup.exe (trong thư mục system32). Để sao lưu một phần của registry có thể dùng luôn trình REGEDT32.EXE

§ 3. QUẢN TRỊ USER VÀ GROUP

3.1. Khái niệm user và group

User là một định danh, thông qua định danh này người dùng có thể truy cập và sử dụng các dịch vụ mạng, user có thể gọi là “tài khoản người dùng”. Windows 2000 Server có khả năng cung cấp một hệ thống user rất lớn và được quản lý bởi AD. Các tài khoản người dùng khi được tạo ra đều tự động được cấp cho một mã nhận diện bảo mật (security identifier – SID) Mỗi SID là một con số duy nhất để nhận diện một tài khoản, các SID không bao giờ được tái sử dụng, khi một tài khoản bị xóa, nó cũng bị xóa theo. Khi có tài khoản mới sẽ được cấp một SID mới không trùng lặp, nhờ đó tài khoản mới sẽ không có quyền hạn và quyền truy cập trùng với tài khoản cũ và hệ thống vẫn giữ được tính bảo mật. Hệ thống tài khoản được tổ chức theo mô hình:

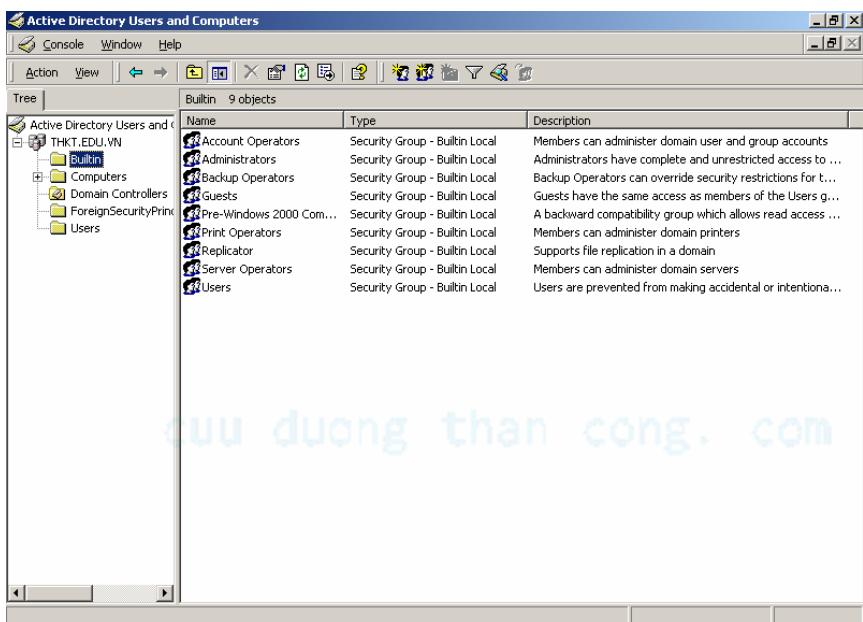


Sau khi cài đặt Windows 2000 tạo ra một user đặc biệt có tên Administrator, tài khoản này có toàn bộ quyền hạn trên một máy hay một miền, không thể xóa tài khoản này nhưng có thể đổi tên.

Một số user có cùng quyền hạn trên mạng có thể được xếp vào một nhóm gọi là group, group được đặt tên (group name) . Một user có thể là thành viên của

nhiều group, khi là thành viên của group nào thì user sẽ có quyền hạn của nhóm đó. Windows 2000 server cung cấp hai loại nhóm, nhóm bảo mật (security group) và nhóm phân phối (distribution group). Nhóm bảo mật là nhóm được dùng để cấp các quyền hạn và quyền truy cập, mỗi nhóm bảo mật đều được cấp một mã nhận diện bảo mật (SID). Có ba kiểu nhóm bảo mật là nhóm bảo mật tại chỗ (local group), nhóm toàn miền (global group), nhóm chung (universal group). Nhóm phân phối được tạo ra không vì mục đích bảo mật, nó không có (SID), nó có thể được dùng để cấp phát thư tín, dùng để thông báo cho một nhóm người. Windows 2000 server cung cấp các nhóm tạo sẵn như sau:

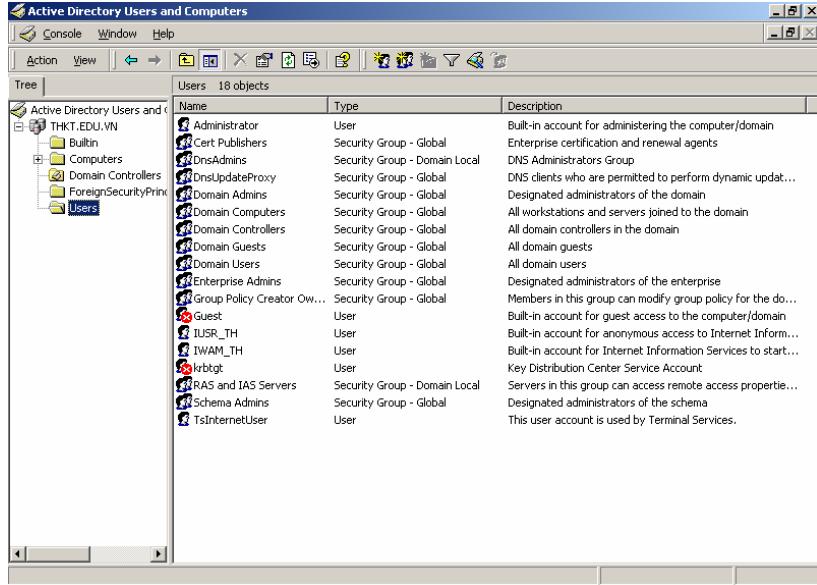
- Các domain local group trong container builtin



Quyền hạn các người dùng của nhóm ngầm định	Họ cũng có thể
Administrators: Truy nhập tại chỗ Truy cập máy này từ mạng Chiếm quyền sở hữu các tập tin Quản lý bản ghi chép kiểm toán và bảo mật Thay đổi giờ giấc của máy Tắt máy Buộc tắt máy này từ một máy ở xa Lưu dự phòng các tập tin và thư mục Khôi phục lại các tập tin và thư mục Thêm và bớt các device driver Tăng độ ưu tiên của một quá trình xử	Tạo ra và quản lý các tài khoản người dùng Tạo ra và quản lý các global group Trao quyền hạn cho người dùng Quản lý chính sách kiểm toán và bảo mật Khoá chặt server console Mở khoá server console Định dạng đĩa cứng của server Tạo ra các nhóm chương trình chung Giữ riêng một profile tại chỗ Chia sẻ và chấm dứt chia sẻ các thư mục Chia sẻ và chấm dứt chia sẻ các tài

lý	nguyên khái
Server Operators Truy nhập tại chỗ Thay đổi giờ giấc của máy server này Tắt máy server này Buộc tắt máy server này từ một máy ở xa Lưu dự phòng các tập tin và thư mục Khôi phục lại các tập tin và thư mục	Khoá chặt server Phủ quyết khoá của server Định dạng đĩa cứng của server Tạo các nhóm chung Giữ riêng một Profile tại chỗ Chia sẻ và chấm dứt chia sẻ các thư mục Chia sẻ và chấm dứt chia sẻ các máy in
Account Operators Truy nhập tại chỗ Tắt máy server này	Tạo ra và quản lý các người dùng, các global, các local group, không có quyền sửa đổi tài khoản của Administrator, global group Domain Admins hoặc các local group Administrator, Server Operators và Backup Operators Giữ riêng một Profile tại chỗ
Print Operators Truy nhập tại chỗ Tắt máy	Giữ riêng một Profile tại chỗ Chia sẻ và chấm dứt chia sẻ các máy in
Backup Operators Truy nhập tại chỗ Tắt máy Lưu dự phòng các tập tin và thư mục Khôi phục lại các tập tin và thư mục	Giữ riêng một Profile tại chỗ
Everyone Truy cập máy này từ mạng	Khoá chặt server – nếu có quyền truy nhập tại chỗ
Users (Không có quyền gì)	Tạo ra và quản lý các local group- nếu có quyền truy nhập tại chỗ
Guets (Không có quyền gì)	(Không có quyền gì)
Replicator (Không có quyền gì)	(Không có quyền gì)

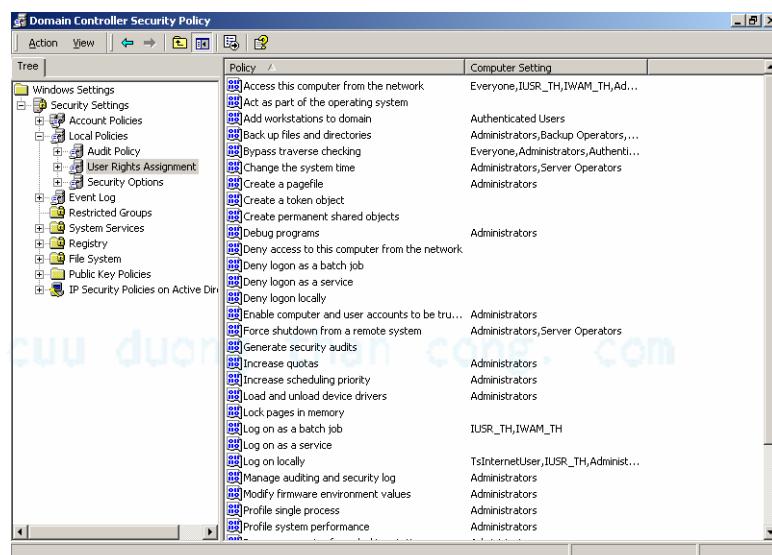
Các domain global group trong container users



Nhóm	Công dụng của nó
Domain Admins	Bằng cách đặt một tài khoản người dùng vào trong global group này, bạn cung cấp được các năng lực ở mức độ quản trị cho người dùng đó. Các thành viên của Domain Admins của một miền có thể quản trị miền nhà, các máy trạm của miền ấy và mọi miền được ủy quyền khác nếu đã lồng global group Domain Admins của miền ấy vào các Local Administrators của chúng. Theo mặc định global group Domain Admins được tạo sẵn của một miền sẽ là một thành viên của cả Local Administrators của miền ấy lẫn các Local group Administrators của mọi máy trạm NT hoặc Win2K Pro trong miền ấy. Global group Domain Admins của một miền sẽ tự động có một thành viên là tài khoản Administrators được tạo sẵn của miền ấy.
Domain Users	Các thành viên của global group Domain Users của một miền có quyền truy cập và quyền hành của người dùng bình thường đối với cả miền ấy lẫn mọi máy trạm NT/ Win2K trong miền ấy. Nhóm này chứa tất cả các tài khoản của người dùng của miền ấy, và theo mặc định, là một thành viên của mọi Local group Users trên mọi máy trạm NT/ Win2K trong miền ấy.
Domain Guests	Miền này cho phép các tài khoản khách vãng lai (Guests) truy cập được các tài nguyên ngang qua ranh giới miền nếu họ đã được các quản trị viên miền này cho phép làm như thế

3.2. Khái niệm quyền hạn

Windows 2000 cung cấp cho người dùng khả năng truy cập mạng để quản lý hoặc sử dụng tài nguyên. Để kiểm soát truy cập windows 2000 chia ra hai nhóm quyền, thứ nhất đó là quyền hạn (right) đối tượng nào có quyền hạn thì có khả năng gán hoặc hạn chế khả năng truy cập vào một vài đối tượng hệ thống. Thứ hai là quyền truy cập (permission) hay giấy phép truy cập, đối tượng nào có quyền này thì được phép sử dụng đối với tài nguyên của mạng. Theo nguyên tắc, các quyền hạn được ưu tiên hơn quyền truy cập, các quyền hạn thường được gán cho những công việc liên quan đến việc quản lý hệ thống. Windows 2000 đã gán ngầm định các quyền hạn cho các nhóm tạo sẵn, ngoài ra quản trị mạng có thể tạo nhóm mới rồi gán quyền hạn phù hợp cho nhóm này. Các quyền hạn được tạo sẵn bao gồm:



Quyền hạn người dùng	Giải thích ý nghĩa
Access this computer from the network	Nối kết vào máy này ngang qua mạng
Act as part of the Operation system	Đóng vai trò như một phần được ủy quyền của hệ điều hành; một số tiêu hệ thống được cấp quyền hạn này.
Add wortation to domain	Làm cho các máy trạm trở thành viên của miền
Back up files and directoies	Lưu dự phòng các tập tin và thư mục. Như đã nói ở trên quyền này đã phủ quyết các quyền truy cập tập tin và thư mục.
Bypass traverse checking	Duyệt lướt qua một cây thư mục, cho dù người dùng đó không có

	quyền truy cập nào đó với thư mục đó.
Change the system time	Định giờ giấc đồng hồ bên trong máy tại chỗ.
Create a pagefile	Tạo một tập tin phân trang (bộ nhớ ảo)
Create a token object	Tạo các thẻ hiệu truy cập (access token) chỉ bô phận Local security Authority mới có quyền này.
Create permanent shared objects	Tạo những đối tượng vĩnh viễn đặc biệt
Debug programs	Gỡ rối các ứng dụng
Deny access to this computer from the network	Ngược lại với quyền Access this computer from the network; thu hồi riêng quyền này đối với những người hay nhóm mà bình thường vẫn có nó.
Deny logon as batch job	Thu hồi quyền Log on as a batch job
Deny logon as a service	Thu hồi quyền Log on as a service
Deny logon locally	Thu hồi quyền Log on locally
Enable computer and user accounts to be trusted for delegation	Chỉ định các tài khoản có thể được ủy quyền
Force shutdown from a remote system	Quyền shutdown máy từ xa
Generate security audits	Tạo ra các đề mục ghi chép kiểm toán
Increase quotas	Tăng các hạn ngạch về dung lượng đĩa cứng
Increase scheduling priority	Tăng cường độ ưu tiên lịch biểu của một quá trình xử lý.
Load and unload device drivers	Nạp (hoặc bớt) driver vào (hoặc ra khỏi) hệ thống.
Lock pages in memory	Khoá chặt các trang vào trong bộ nhớ để ngăn không cho chúng bị đưa vào trong bộ lưu trữ dự phòng(như Pagefile. Sys chẵng hạn)
Log on as a batch job	Đăng nhập vào hệ thống như một phương tiện hàng đợi theo lô (Batch queue facility)
Log on as a service	Thực hiện các dịch vụ bảo mật (vd; người dùng mà thực hiện việc sao chép sẽ đăng nhập với tính cách

	như một dịch vụ)
Log on locally	Đăng nhập tại chỗ, tại chính máy server này.
Manager auditingand security log	Chỉ rõ những sự kiện và kiểu truy cập tài nguyên gì sẽ được kiểm toán. Ngoài ra còn cho phép xem và xoá sạch bản ghi chép bảo mật (security log)
Modify firmware envionment values	Sửa đổi các biến môi trường của hệ thống (không phải biến môi trường của người dùng)
Profile single process	Sử dụng những khả năng ghi chép hoạt động(profiling) của Win2K để quan sát, nhận xét hoạt động của một quá trình xử lý.
Profile system perfromance	Sử dụng các khả năng ghi chép hoạt động của Win2K để quan sát nhận xét hoạt động của hệ thống.
Remove computer from docking station	Tháo gỡ một máy laptop ra khỏi hộp nối ghép vào mạng (docking station) của nó.
Replace a process level token	Sửa đổi thẻ hiệu truy cập của một quá trình.
Restore files and directories	Khôi phục lại các tập tin và thư mục, quyền này phủ quyết các quyền truy cập tập tin và thư mục.
Shut down the system	Tắt máy Win2K
Synchronize directory service data	Cập nhật thông tin của Active directory
Take ownership of files or other objects	Chiếm quyền sở hữu của các tập tin, thư mục, và các đối tượng khác, vốn trước đó được các người dùng khác sở hữu.

Quyền truy cập (permission)

Quyền tuy cập hay giấy phép truy cập (permission) chỉ định user nào, group nào được phép sử dụng tài nguyên và với điều kiện gì.

3.3. Thiết kế hệ thống user và group

Trước khi tạo hệ thống user và group cho một mạng máy tính cần thiết kế hệ thống user cho tổ chức đó. Thiết kế này là cơ sở để thực hiện các tác vụ cụ thể liên quan đến user, nó cũng là cơ sở để quản lý hệ thống user trong quá trình hoạt động mạng. Khi thiết kế cần tuân thủ một số nguyên tắc sau:

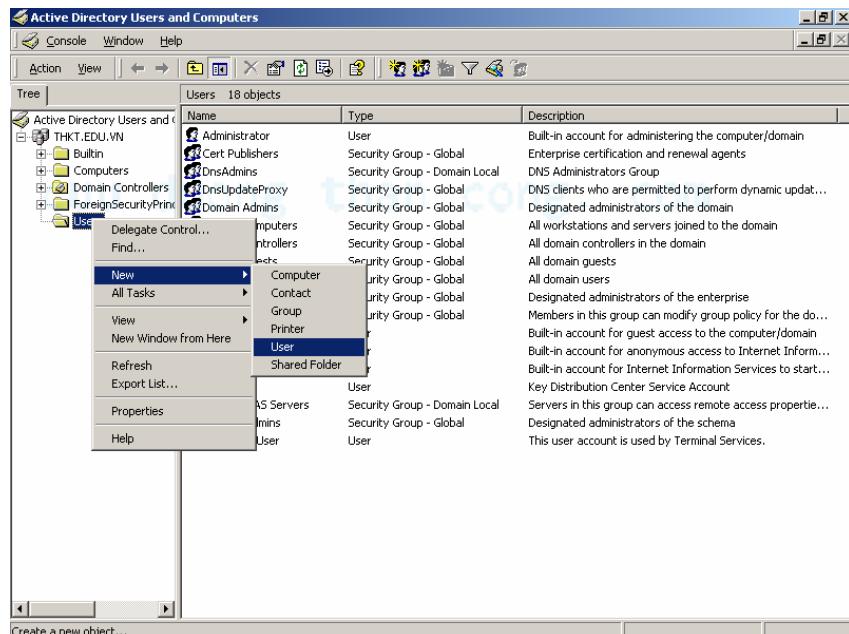
- Tên phải là tên duy nhất, tên user không được trùng tên nhóm.
- Độ dài của tên dài nhất đến 20 ký tự, có thể chứa chữ hoa, chữ thường hoặc cả hai.
- Tên không được chứa các ký tự: “ / \ : | + * ? < > ” ; các ký tự mở rộng.
- Phân loại user quản trị mạng và user sử dụng tài nguyên mạng
- Sắp đặt các user vào các group phù hợp
- Lập bảng thiết kế users

3.4. Tạo user và group

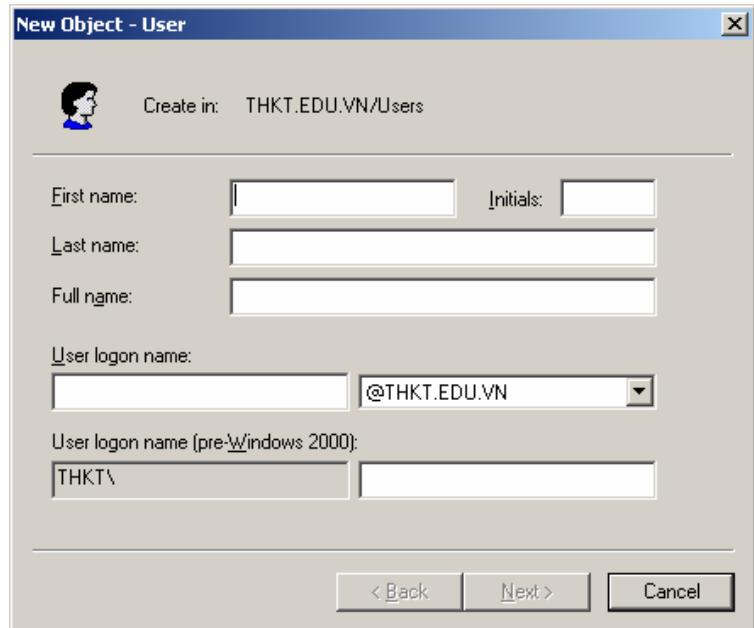
a. USER

Tạo user

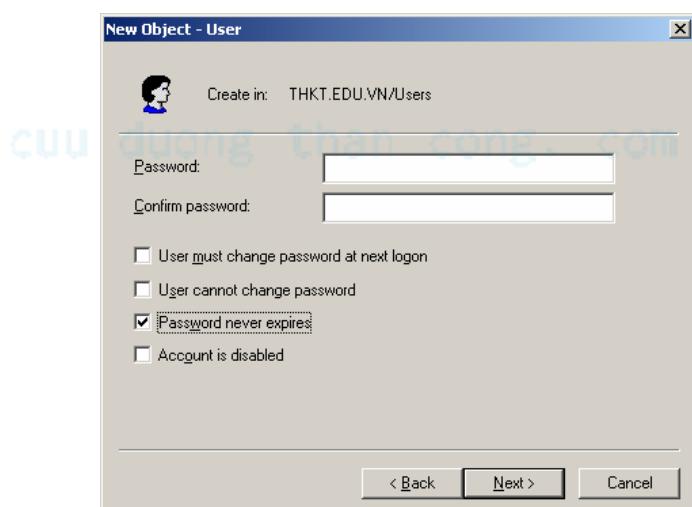
- Chạy trình Active Directory Users and Computer, bấm phải chuột vào OU users, chọn new – user. Trên màn hình sẽ hiển thị cửa sổ NEW OBJECT – USER



- Trên cửa sổ này cần điền các tham số

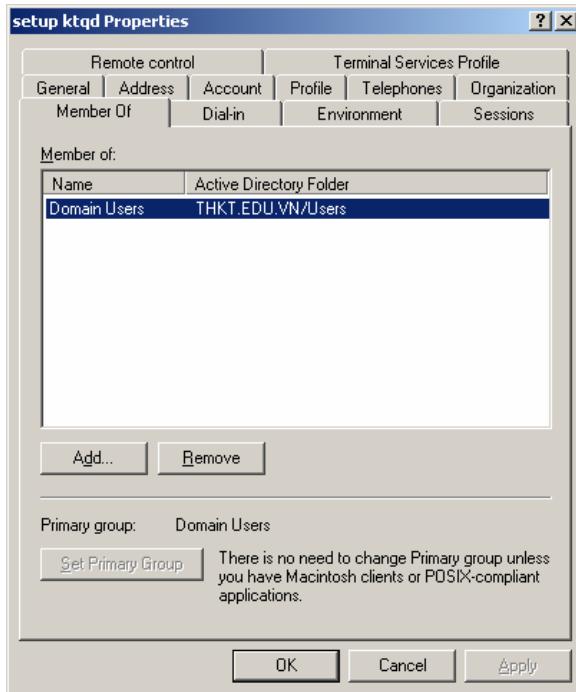


Bấm next để tiếp tục, trên màn hình hiển thị cửa sổ để điền tiếp các tham số



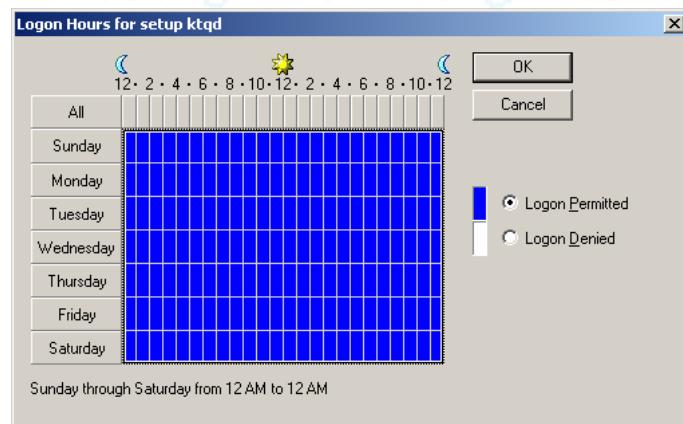
Các đặc tính của user, xem thông tin và hiệu chỉnh

- Chọn user – Properties



Các thiết định về tài khoản

- Chọn user – Properties, chọn mục Account
- Chọn hạn chế về thời gian cho việc truy nhập



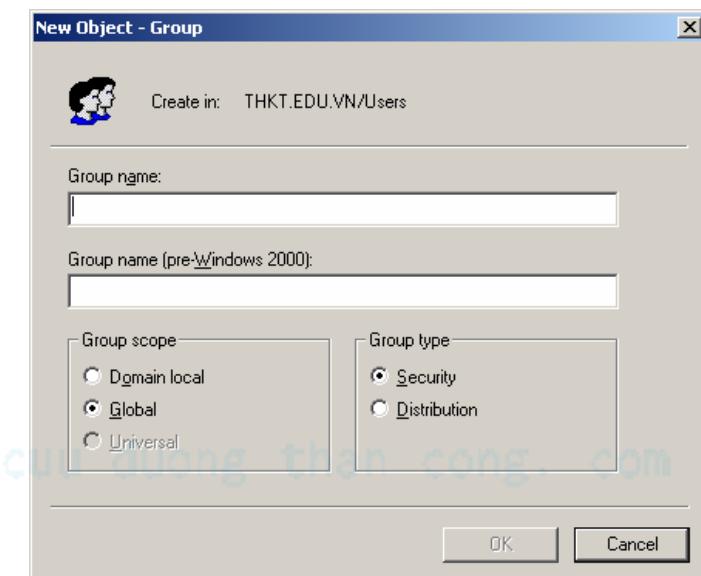
- Chỉ định các máy trạm được phép truy nhập



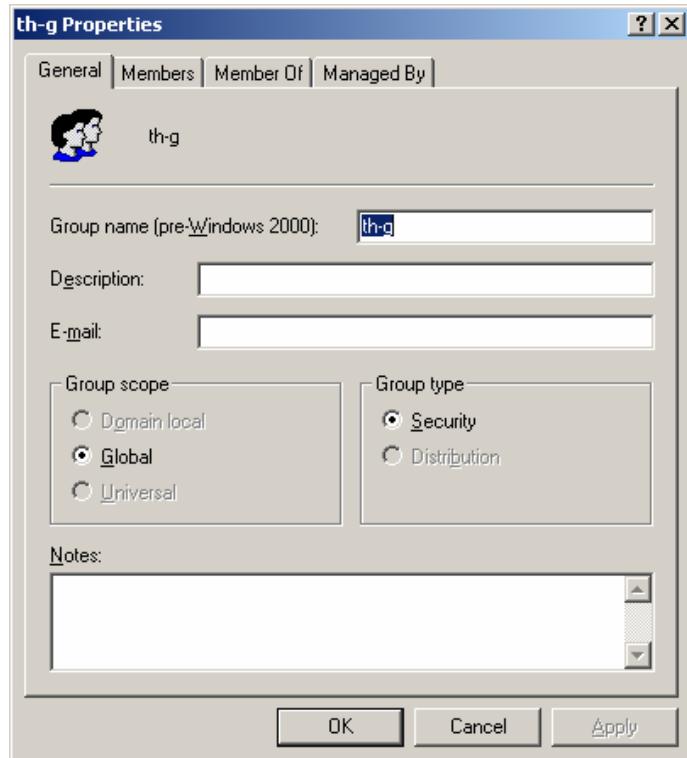
b. Group

□ Tạo group

- Chạy trình Activate Directory Users and Computer, bấm phải chuột vào OU users, chọn new – group. Trên màn hình sẽ hiển thị cửa sổ NEW OBJECT – GROUP



- Đưa user vào nhóm phù hợp



cuu duong than cong. com

3.5. Login Script

Login script là một chương trình máy tính được sử dụng để định hình cho môi trường làm việc, Login script được thực hiện khi user truy nhập mạng. Login script có thể viết bằng nhiều ngôn ngữ như các lệnh shell của DOS/NT/Windows 2000, Windows Scripting Host (WSH), KiXtart, XLNT, Perl, VBScript, Jscript, Login script được viết phụ thuộc vào yếu tố: người xây dựng kịch bản (quản trị mạng), máy khách. Để sử dụng các ngôn ngữ khác thì máy khách cần phải hiểu được ngôn ngữ này, tức là phải cài đặt các trình thông dịch. Để đơn giản có thể chọn các lệnh shell của Windows 2000 / NT/ Windows 9x. Có thể tạo login script bằng các trình soạn thảo như NC, Notepad, ..., dùng trình soạn thảo này tạo tệp có cấu trúc TEXT có phần mở rộng là BAT (DOS, Windows 9X) , hoặc có phần mở rộng là CMD (Windows 2000 / NT) và ghi tệp tin này lên thư mục

C:\WINNT\SYSVOL\sysvol\domainname\scripts

Ví dụ: domain có tên thkt.edu.vn thì login script phải được ghi lên thư mục C:\WINNT\SYSVOL\sysvol\THKT.EDU.VN\scripts

- Một số biến sử dụng:

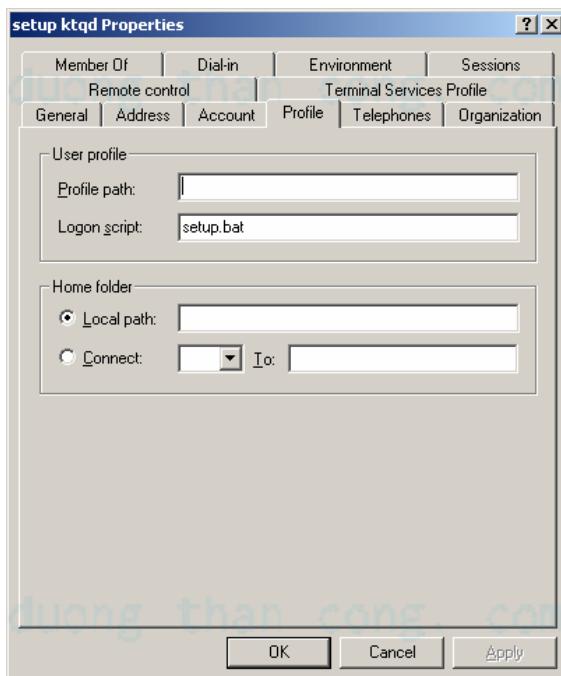
%HOMEDRIVE%	Cho tên ổ đĩa cục bộ ở máy trạm nối với user's home directory
%HOMEPATH%	Cho tên đường dẫn thư mục ngầm định của user (user's home directory)
%OS%	Cho tên hệ điều hành ở workstation
%PROCESSOR_LEVEL	Cho kiểu processor ở workstation
%	
%USERDOMAIN%	Cho tên domain chứa tài khoản của user
%USERNAME%	Cho tên user

Sử dụng trình NET.EXE : Dùng NET USE theo chế độ dòng lệnh

NET.EXE có trong các máy đã cài Dos client, Windows 9X, Windows 2000/NT

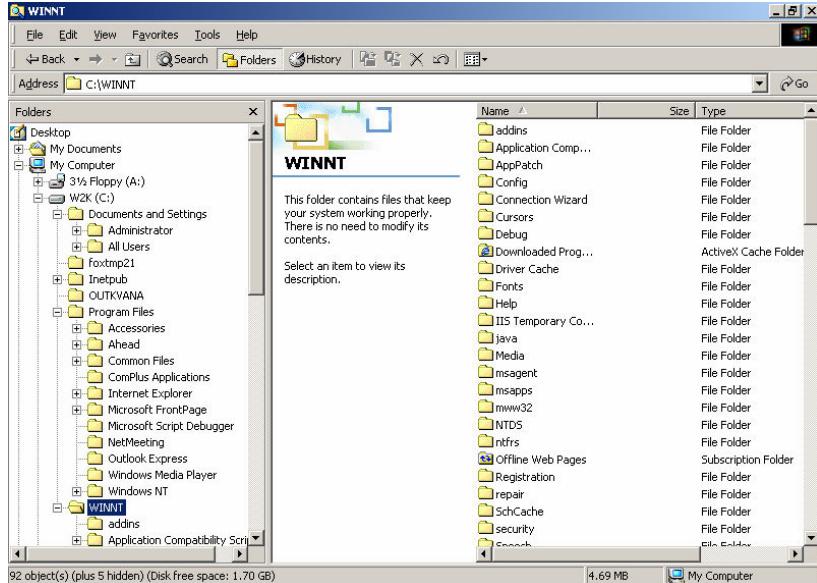
Khai báo login script cho user

Chạy trình Activate Directory Users and Computer, chọn user cần khai báo login script, chọn Properties của user này, sau đó điền tham số.



§ 4. QUẢN TRỊ HỆ THỐNG THƯ MỤC VÀ FILES

4.1 Cấu trúc thư mục của Windows 2000



4.2 Thiết kế hệ thống thư mục cho người dùng

Nguyên lý chung

Tùy qui mô và nhu cầu cung cấp dịch vụ của mạng mà từng hệ thống hệ thống thư mục có thể để riêng trên ổ đĩa logic hoặc để riêng trên một máy.

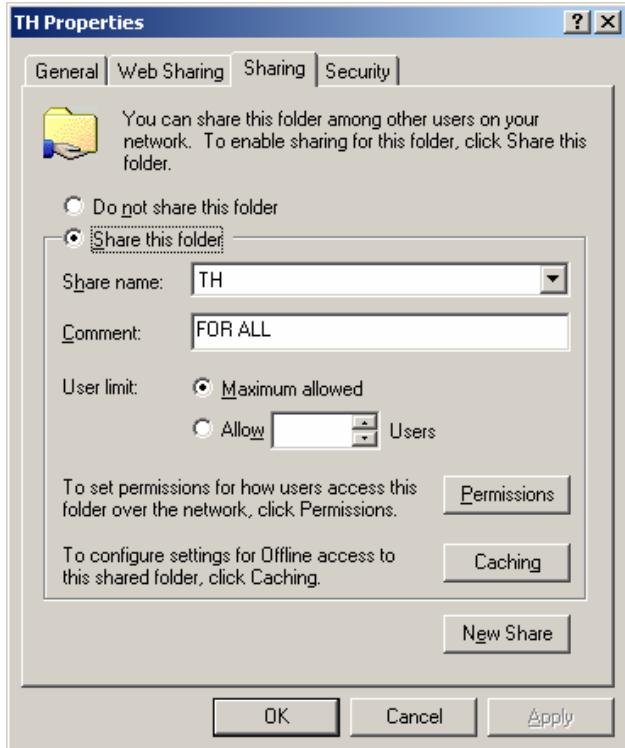
- Dành riêng ổ đĩa logic (c:) cho hệ thống thư mục của Windows 2000.
- Hệ thống thư mục của các chương trình ứng dụng nên phân loại và để theo nhóm, có thể để trên ổ đĩa của windows 2000 nếu dung lượng cho phép, nếu dung lượng lớn cần để riêng trên ổ đĩa logic.
- Hệ thống thư mục của các USER nên tập trung để dễ dàng theo dõi và kiểm soát.
- Hệ thống thư mục của các group nên tập trung để dễ dàng theo dõi và kiểm soát.
- Hệ thống các trình cài đặt của mạng nên để riêng trên ổ đĩa logic
- Tên của các thư mục nên đặt ngắn gọn và có qui luật

4.3 Quản lý quyền truy cập

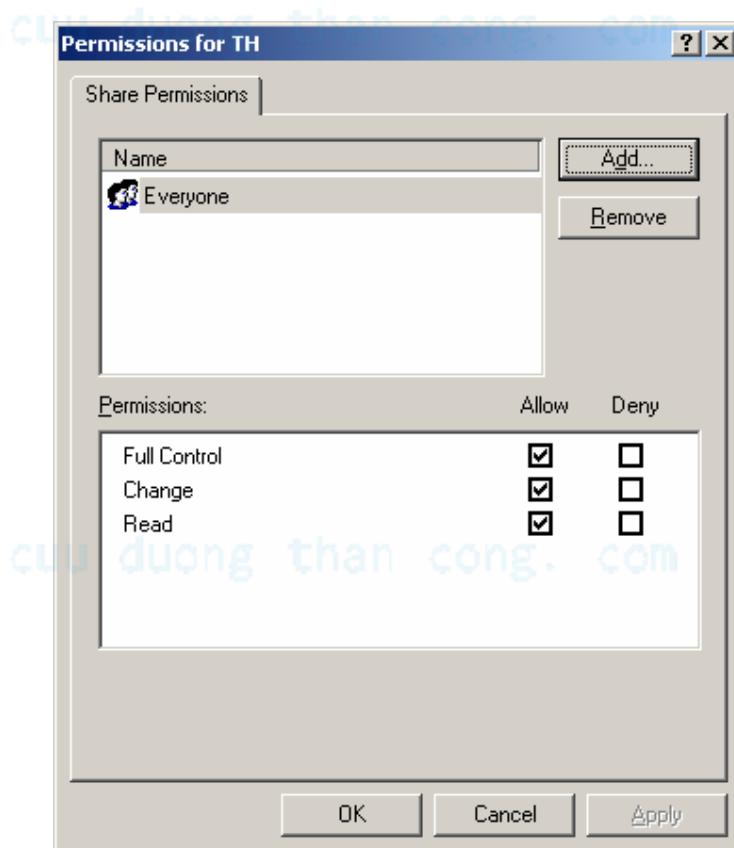
a. Quyền truy cập ở cấp share

Share là hình thức cung cấp dịch vụ ghi chép tệp tin lên ổ đĩa cứng của mạng. Để cung cấp dịch vụ này, quản trị mạng cần tạo share và gán quyền truy cập phù hợp cho user.

- Tạo share: đặt tên share



- Chọn permission để gán quyền truy cập cho user



Full Control: Quyền thực hiện tất cả các công việc trên thư mục và tệp tin

Change: Quyền đọc, thi hành, thay đổi, xóa thư mục và tệp tin

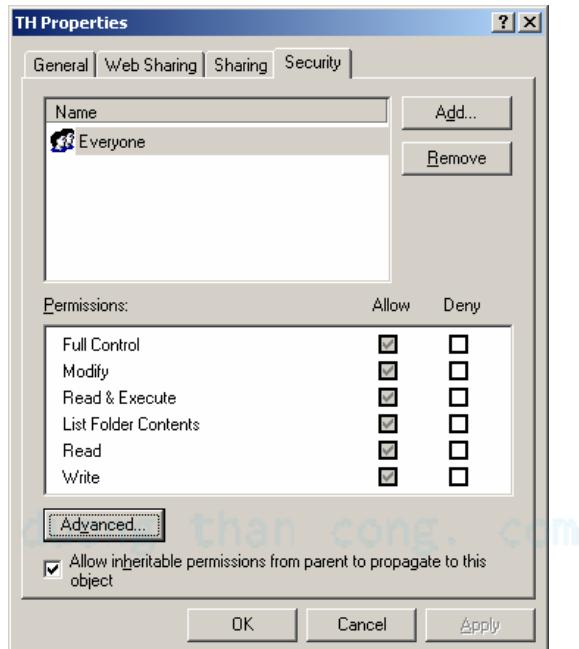
Read: Quyền đọc và thi hành thư mục và tệp tin không có khả năng sửa đổi

b. *Quyền truy cập ở cấp thư mục và tệp tin*

Quy định permission ở mức thư mục và tệp tin, các quyền được chia nhỏ mờ mức chi tiết.

- Chọn Properties của thư mục, chọn security

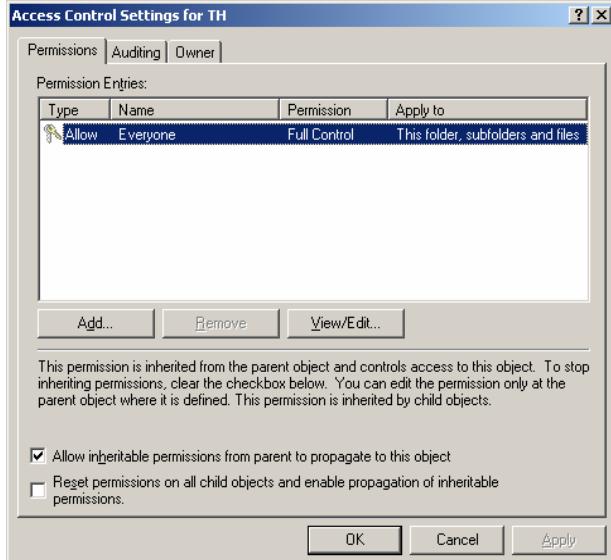
- Các permission mức phân tử (molecular level):



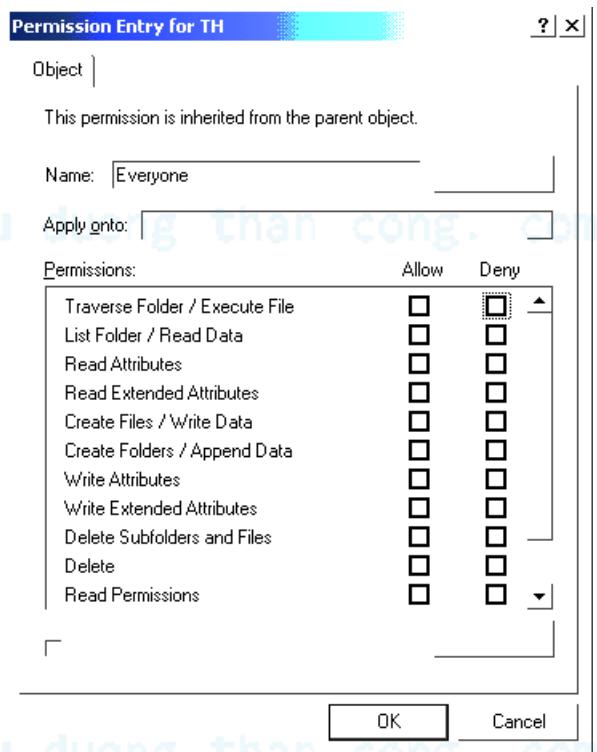
Allow inheritable permissions parent to propagate to this object: Cho phép các thư mục con thừa hưởng các quyền của thư mục mức cao hơn nó.

- Các permission mức nguyên tử (atomic level)

- Chọn Properties của thư mục, chọn Advanced



- Chọn View/Edit



Write Traverse Folder/Execute File
 List Folder/Read Data
 Read Attributes
 Read Extended Attributes
 Create Files/Write Data
 Create Folders/Append Data

Write Attributes
Write Extended Attributes
Delete Subfolders and Files
Delete
Read
Change
Take Ownership
Synchronize

Quyền sở hữu (ownership)

Chủ nhân của một đối tượng (tệp tin, thư mục, ...) có một thuộc tính gọi là ownership, owner tách biệt với permission. Nếu có owner đối với một đối tượng thì có thể phân bố lại permission cho đối tượng này. Người tạo ra đối tượng sẽ là owner ngầm định của đối tượng.

c. Các share hệ thống

Các share được tạo sẵn được dùng chung cho hệ thống, cuối tên share chứa ký tự \$, các share này đều là các share ẩn.

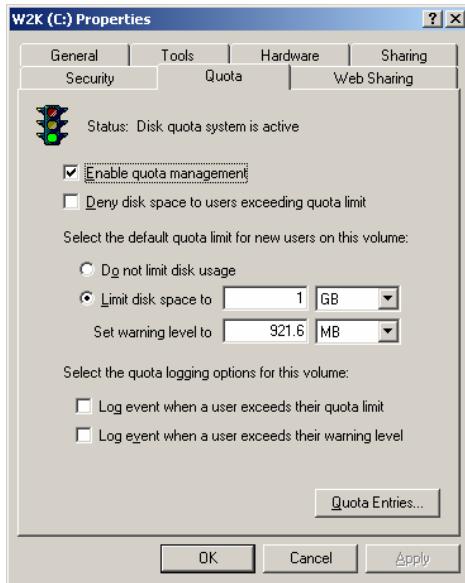
Tất cả các ổ đĩa đều có một share ẩn ứng với thư mục gốc của mỗi ổ đĩa đó. Các share này gọi là share phục vụ việc quản trị (administrative share). Không thể thay đổi các permission hoặc đặc tính của các share này, nhưng có thể chấm dứt hoàn toàn việc chia sẻ chúng, ví dụ các share C\$, D\$, ...

Các share khác được dùng vào mục đích cụ thể:

- Admin\$: ứng với thư mục gốc của hệ thống (thư mục chứa tệp tin của windows 2000 ví dụ c:\winnt)
- Print\$: Khi tạo một máy in chung, hệ thống sẽ đặt các driver cho máy in đó vào trong share này.
- IPC\$: Dùng để truyền thông giữa các máy tính
- Repl\$: Sao chép dữ liệu giữa các server khi các máy dùng dịch vụ sao chép (replication service)
- Các share có thể ẩn nếu khi đặt ký tự \$ vào cuối tên share

4.4 Cáp phát hạn ngạch đĩa (quota)

Để kiểm soát dung lượng đĩa cứng trên server, windows 2000 cung cấp một công cụ nhằm chỉ định dung lượng đĩa mà người sử dụng có thể ghi lên server. Để thực hiện chức năng này chọn properties của ổ đĩa trong cửa sổ explore.

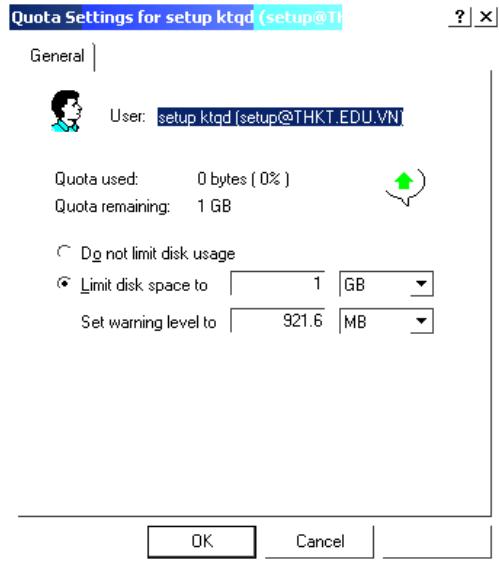


Chọn ô quota, trên màn hình hiển thị cửa sổ properties, chọn enable quota management, chọn quota entries

Quota Entries for W2K (C:)					
Status	Name	Logon Name	Amount Used	Quota Limit	Warning Level
OK	BUILTIN\Administrators		1.25 GB	No Limit	No Limit
OK	NT AUTHORITY\SYSTEM		1.19 MB	1 GB	921.6 MB
OK	setup ktqd	setup@THKT.EDU.VN	0 bytes	1 GB	921.6 MB

3 total item(s), 1 selected.

Trên màn hình hiển thi danh sách các user được cấp quota, click chuột vào tên user để hiệu chỉnh tham số. Thêm user vào danh sách cấp hạn ngạch, chọn trên thực đơn quota – new quota entry. Chon user của domain trên danh sách hiển thị trên màn hình, tiếp theo xác định dung lượng đĩa cần hạn chế.



§ 5. CÀI ĐẶT CLIENT, TRUY NHẬP VÀO MẠNG

Sau khi Windows 2000 được cài đặt trên SERVER cần phải được SHARE đĩa cứng, gán quyền truy cập và quyền sử dụng cho các USER và GROUP. Windows 2000 cho phép các Workstation (DOS, WINDOWS For Workgroup, WINDOWS 9X, Windows NT Workstation, Macintosh) truy nhập các tài nguyên hệ thống. Tuy nhiên tùy theo từng hệ điều hành mà trên SERVER và Workstation cần phải cấu hình phù hợp.

5.1. Hệ điều hành DOS

Các máy sử dụng điều hành DOS có thể truy cập vào Windows 2000 bằng các phần mềm Microsoft Network Client hoặc Microsoft LAN Manager.

Cài đặt Microsoft Network Client

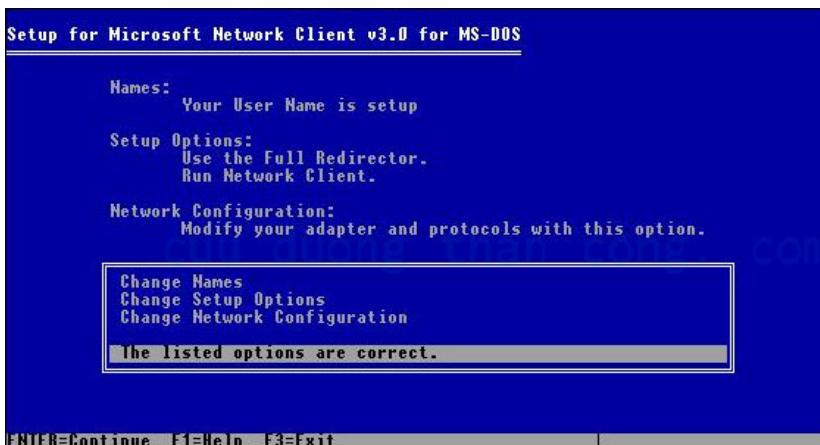
Sử dụng đĩa cài đặt (trên đĩa CD Windows NT Server, có thể copy ra đĩa mềm)

- Khởi động DOS và chạy trình SETUP

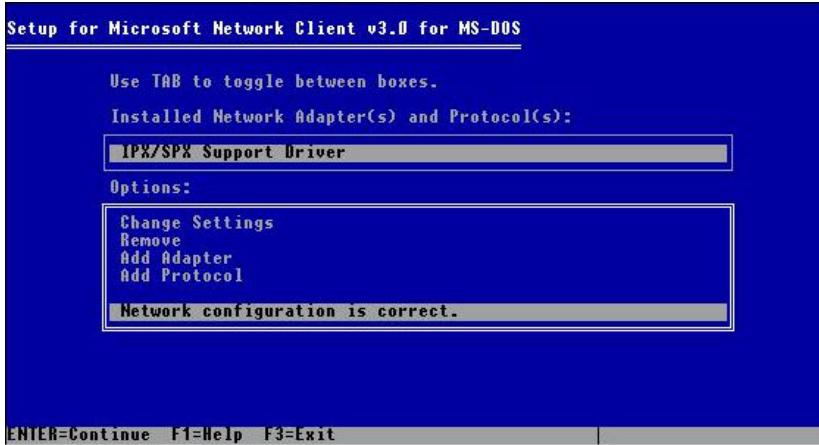
cuu duong than cong. com



- + Chọn thư mục cài đặt (ngầm định c:\net)
- Bấm enter để tiếp tục



- + Chọn change name: để hiệu chỉnh các tham số về
 - + User name
 - + Computer name
 - + Workgroup name
 - + Domain name
- + Chọn change setup options: để hiệu chỉnh các tham số về
 - + Redir options: nếu chọn Full Redirector thì có khả năng
 - + Truy cập vùng và Login script
 - + Remote Access Service
 - + Gửi thông báo
 - + Các cơ chế truyền thông liên kết xử lý như Remote procedure calls, Windows Sockets (Winsock- giao diện giữa chương trình và giao thức vận chuyển).
 - + Logon validation: chọn logon to domain
- + Chọn network configuration: để hiệu chỉnh các tham số về



+ Add adapter: Chọn card mạng, chọn trên danh sách, nếu MS client không hỗ trợ thì cần khai báo thư mục chứa driver card mạng.

+ Add protocol: Các giao thức hỗ trợ

+ NetBEUI

+ IPX Compatible Transport

+ TCP/IP: có hỗ trợ DHCP, không hỗ trợ phân giải tên DNS

Sau khi chọn, hiệu chỉnh các tham số, hệ thống sẽ được cài đặt và yêu cầu khởi động lại máy tính.

Truy nhập vào mạng:

Nếu quá trình cài đặt thành công, các tệp tin của hệ thống đã được tạo ra, nội dung của các tệp tin như sau:

+ Tệp tin CONFIG.SYS

FILES=45

device=a:\himem.sys

device=a:\MSCLIENT\ifshlp.sys

dos=high

LASTDRIVE=Z

+ Tệp tin AUTOEXEC.BAT

SET PATH=a:\MSCLIENT

a:\MSCLIENT\net start

Sau khi các tệp tin đã được nạp thành công (Đã login vào mạng), có thể sử dụng dịch vụ đơn giản của mạng.

Có thể dùng lệnh NET.EXE để thực hiện một số công việc về mạng như ánh xạ ổ đĩa (map), khai báo máy in mạng.

Một số hướng dẫn về NET.EXE

- Chức năng: hỗ trợ user sử dụng tài nguyên của mạng như đĩa cứng, máy in, hiển thị thông tin kết nối.

NET: thực hiện theo giao diện thực đơn

NET HELP: trợ giúp

NET USE

NET USE [drive: | *] [\computer\directory [password | ?]]
[/PERSISTENT:YES | NO] [/SAVEPW:NO] [/YES] [/NO]
NET USE [port:] [\computer\printer [password | ?]]
[/PERSISTENT:YES | NO] [/SAVEPW:NO] [/YES] [/NO]

NET USE drive: | \\computer\directory /DELETE [/YES]

NET USE port: | \\computer\printer /DELETE [/YES]

NET USE * /DELETE [/YES]

drive Ký tự chữ cái tên ổ đĩa

* Tự gán chữ cái tên ổ đĩa tiếp theo. Nếu dùng /DELETE, ngắt
các kết nối

port Cổng LPT cho máy in

computer Tên SERVER

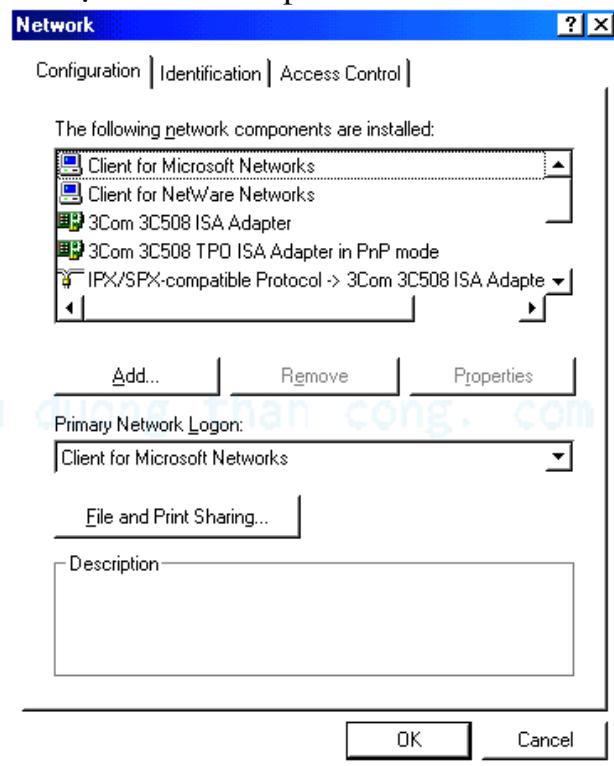
directory Tên thư mục được shared

printer Tên máy in

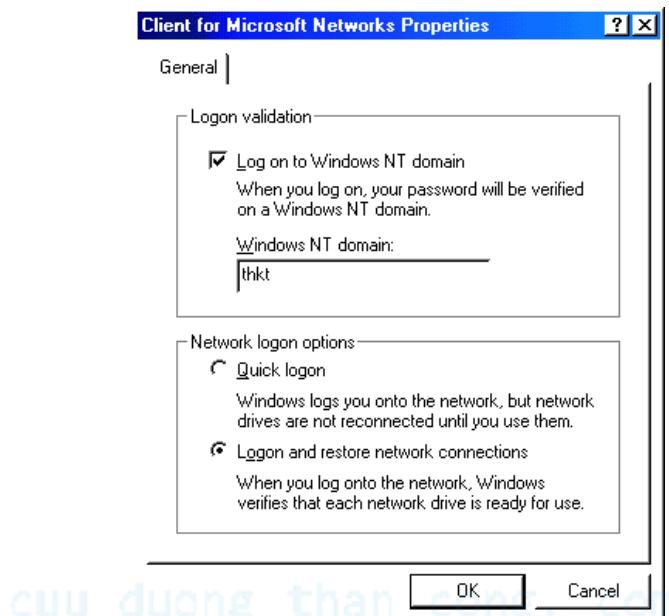
5.2. Hệ điều hành WINDOWS 9X

□ Cài đặt

- Máy phải được cài đặt phần cứng như dây cáp mạng, card mạng
- Máy phải được cài đặt và cấu hình phần mềm



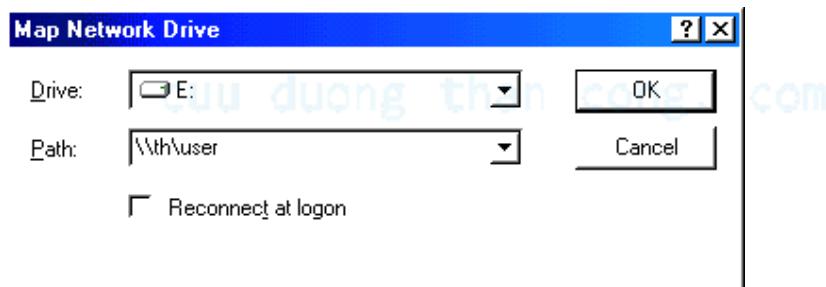
- + Card mạng
- + Dịch vụ: Client for Microsoft Network
- + Protocol: TCP/IP
- Khai báo tên domain trong Properties của dịch vụ Client for Microsoft Network



Sử dụng

- Khi khởi động máy: nhập tên và mật khẩu hợp lệ
- Có thể sử dụng dịch vụ ghi chép thư mục, tệp tin lên ổ đĩa mạng bằng cách ánh xạ ổ đĩa mạng thành ổ đĩa logic của máy.

Chọn Map Network Driver (trong EXPLORE)



- + Driver: đặt tên ổ đĩa logic
- + Path: \server_name\Share_name

- Sử dụng dịch vụ in ấn
- Có thể sử dụng các dịch vụ khác như: mail, internet, nếu trên máy server có cung cấp những dịch vụ này.

5.3. Truy nhập vào Workstation khác trong mạng (mạng ngang hàng)

Tùy từng hệ điều hành được cài đặt ở máy trạm mà cách cài đặt cụ thể có khác nhau, đối với mạng ngang hàng chỉ có thể cung cấp một số dịch vụ mạng đơn giản như chia sẻ tệp tin, thư mục, chia sẻ máy in. Nếu các máy trạm để cài đặt windows 9x, windows NT, hoặc windows 2000 thì về nguyên tắc có thể cấu hình như sau:

- Ở máy cần truy nhập (đích, chứa tài nguyên) đã được cài đặt phần cứng, cấu hình đầy đủ phần mềm cho mạng. Máy này cần chia sẻ tài nguyên để dùng chung trên mạng bằng cách chọn Share và điền các tham số:

+ Điền Share Name: Đặt tên cho ổ đĩa, hoặc thư mục để máy khác có thể truy nhập

+ Gán quyền truy cập hoặc những hạn chế nếu có, đối với windows 9x thì chỉ có thể đặt password, đối với windows NT thì có thể gán quyền truy nhập chi tiết hơn.

- Ở máy truy nhập (sử dụng tài nguyên) đã được cài đặt phần cứng, cấu hình đầy đủ phần mềm cho mạng. Login vào mạng với đủ thẩm quyền.

+ Có thể sử dụng dịch vụ ghi chép thư mục, tệp tin lên ổ đĩa mạng bằng cách ánh xạ ổ đĩa mạng thành ổ đĩa logic của máy.

Chọn Map Network Driver (trong EXPLORE), điền các tham số

+ Driver: đặt tên ổ đĩa logic

+ Path: \\server_name\Share_name

§ 6. QUẢN TRỊ PHƯƠNG TIỆN LUU TRỮ

6.1. Một số khái niệm

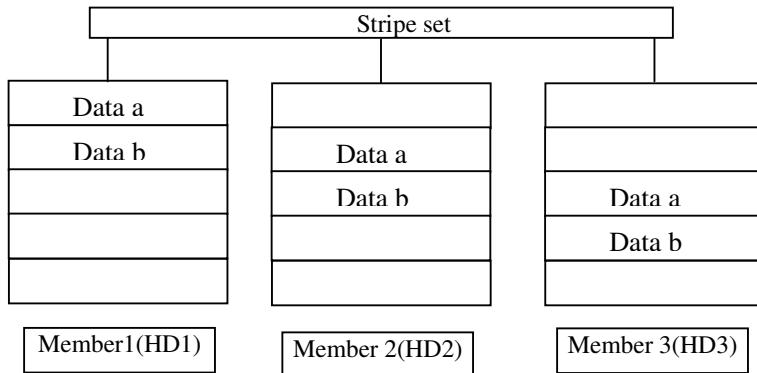
a. Raid

Phương pháp bảo vệ dữ liệu của hệ thống bằng cách kết hợp các đĩa cứng để tăng tính an toàn dữ liệu. Có sáu kiểu thực hiện raid (raid level), windows 2000 hỗ trợ các mức raid 0, 1, 5 .

Raid 0: chia dải không chẵn lẻ (striping without parity)

Kỹ thuật chia dải không chẵn lẻ là kỹ thuật liên kết các chỗ trống trên các đĩa vật lý thành một bộ đĩa chia dải (stripe set). Mỗi thành viên trong stripe set được chia thành các dải (stripe) có kích thước bằng nhau, khi hệ thống ghi dữ liệu vào stripe set, dữ liệu sẽ được phân bố trên các dải này. Để thực hiện kỹ

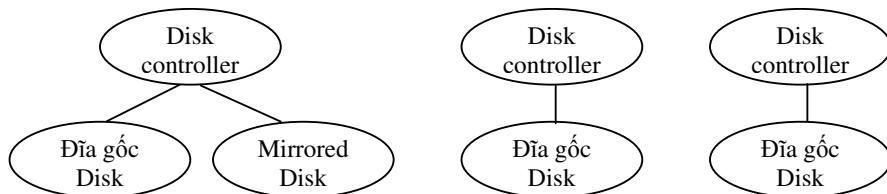
thuật này cần ít nhất hai đĩa, tối đa 32 đĩa, có thể mô tả kỹ thuật stripe set như sau:



Khi hệ thống đọc hoặc ghi dữ liệu thì tất cả các thành viên của bộ đĩa đều đọc và ghi do vậy thời gian đọc ghi sẽ được cải thiện.

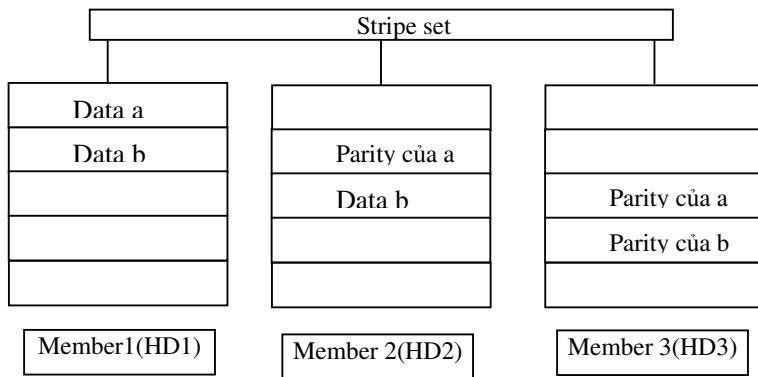
Raid 1: phản chiếu đĩa (disk mirroring)

Kỹ thuật phản chiếu đĩa là kỹ thuật ghi dữ liệu lên hai đĩa vật lý riêng biệt nhưng có chung một bộ điều khiển đĩa (disk controller). Trong trường hợp một đĩa bị lỗi thì vẫn còn dữ liệu ở đĩa còn lại. Disk mirroring khác với trường hợp nhân đôi đĩa (disk duplexing), kỹ thuật disk duplexing sử dụng hai đĩa cứng với hai bộ điều khiển đĩa.



Raid 5: chia dải có chẵn lẻ (striping with parity)

Kỹ thuật chia dải chẵn lẻ là kỹ thuật liên kết các chỗ trống trên các đĩa vật lý thành một bộ đĩa chia dải (stripe set). Theo kỹ thuật này khi hệ thống ghi dữ liệu lên đĩa, dữ liệu được ghi rải ra khắp các đĩa trong dải. Thông tin chẵn lẻ ứng với dữ liệu cũng được ghi vào đĩa, bằng cách này nếu có sự cố xảy ra với một trong các đĩa, phần dữ liệu trên đĩa này có thể được tái tạo từ những thông tin chẵn lẻ trên các đĩa còn lại.



b. Basic disk và dynamic disk

Đĩa cơ bản (Basic disk) là loại kỹ thuật lưu trữ thông thường theo chuẩn dos , các đĩa cơ bản không hỗ trợ các phân vùng chịu lỗi. Đĩa động (dynamic disk) là kỹ thuật lưu trữ đĩa cho phép tạo ra, mở rộng và xóa bỏ các phân vùng trên nhiều đĩa vật lý. Đĩa động không có tính tương thích, mọi hệ điều hành không phải Window 2000 đều không đọc được chúng.

c. Phân khu đĩa (partition)

Một phân khu đĩa (partition) theo kiểu đĩa cơ bản, là một phần của đĩa vật lý được chia làm hai loại phân khu chính (primary partition) và phân khu mở rộng (extended partition).

- Phân khu chính: là phân khu mà hệ điều hành có thể khởi động được, không thể chia phân khu chính ra làm phân khu con. Một đĩa cứng có thể chia tối đa 4 phân khu chính.
- Phân khu mở rộng: để lưu trữ được dữ liệu, thì trên phân khu này cần tạo thành một hoặc nhiều ổ đĩa logic, các hệ điều hành không thể khởi động được từ phân khu này.

d. (Volume set)

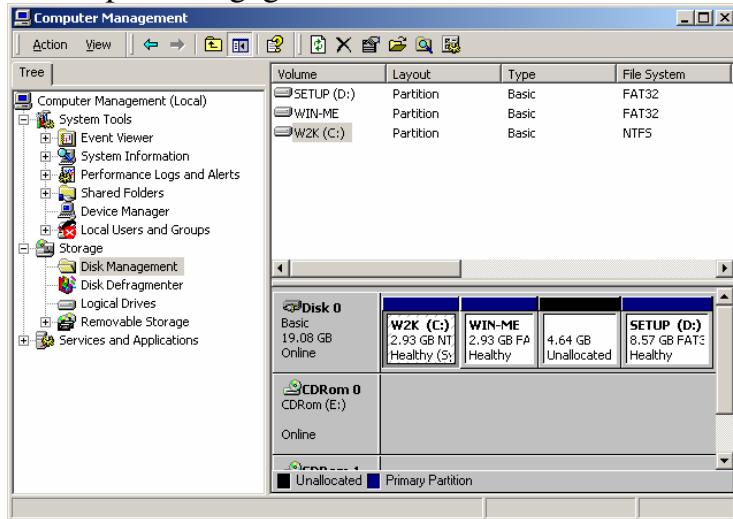
Volume set là hình thức liên kết các phân vùng của một hoặc nhiều đĩa cứng vật lý thành ổ đĩa logic, Windows 2000 hỗ trợ hai loại volume set. Volume set đơn giản (simple volume set) được tạo từ một đĩa cứng, volume set trải dàn (spanned volume set) được tạo từ nhiều đĩa cứng. Các volume set không trợ giúp tính năng chịu lỗi, chúng chỉ cho phép sử dụng đĩa cứng thành đĩa logic với dung lượng lớn. Một trong các đĩa cứng dùng volume set bị lỗi thì volume set cũng lỗi.

6.2. Quản lý đĩa cứng

Để quản lý đĩa windows 2000 cung cấp công cụ disk management trong thực đơn computer management, công cụ này hỗ trợ việc khởi tạo một đĩa cứng mới

thành đĩa làm việc, kiểm tra việc hoạt động của đĩa, xem và có thể hiệu chỉnh các thông tin về đĩa.

Chọn thực đơn computer management



Khởi tạo một đĩa cứng mới

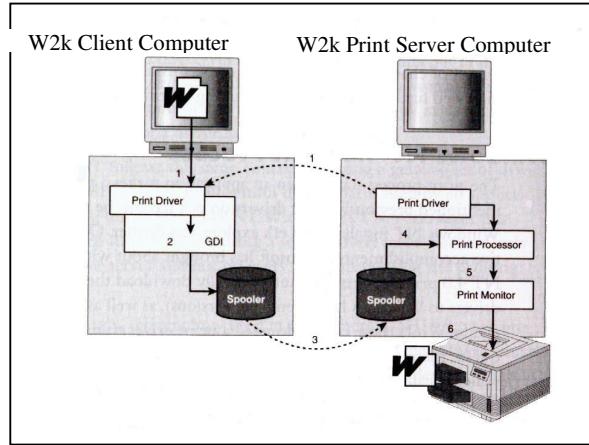
- Tạo đĩa sử dụng theo kiểu đĩa cơ bản (basic disk)
- Tạo đĩa sử dụng theo kiểu đĩa động (dynamic disk)

Giải phân mảnh đĩa

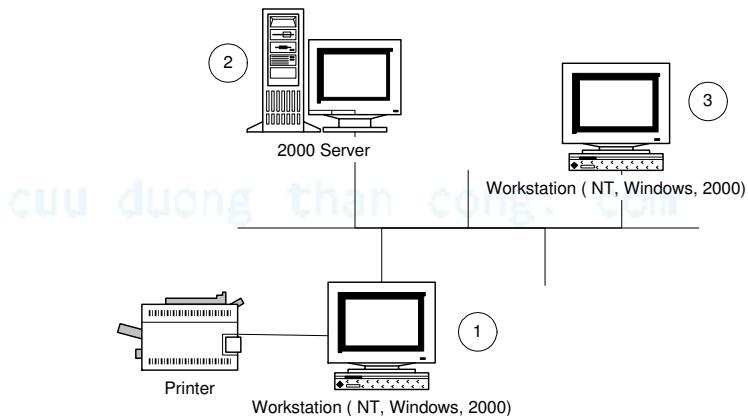
§ 7. QUẢN TRỊ DỊCH VỤ IN ẨN TRÊN MẠNG

7.1. Nguyên lý in ẩn trên windows 2000 :

- 1- Client (workstation) gửi yêu cầu in
- 2- Client tạo tác vụ in, ngầm định GDI (Graphics Device Interface)
- 3- Spooler trên máy client gửi đến Spooler của máy Server
- 4- Print processor: xử lý
- 5- Máy in

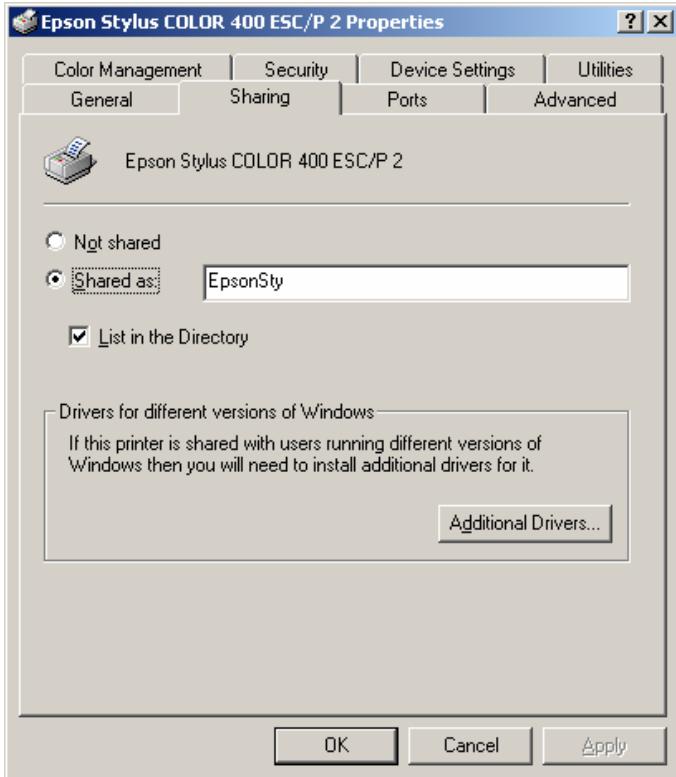


7.2. Một kiểu cấu hình in trên mạng:



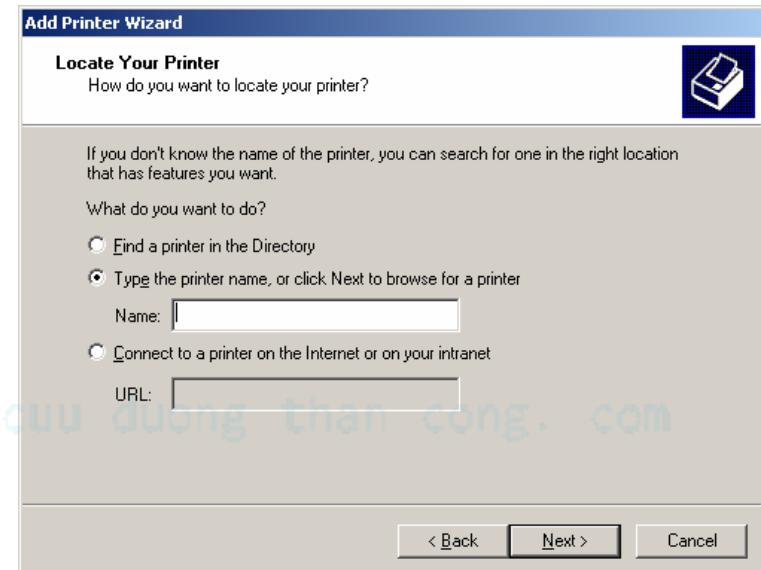
Máy tính cảm máy in (W2k): (1)

- Phải là thành viên của domain Windows 2000 server
- Login vào mạng (domain) với đủ thẩm quyền
- Cài đặt máy in: nối máy in vào máy tính, cài đặt driver
- Share máy in

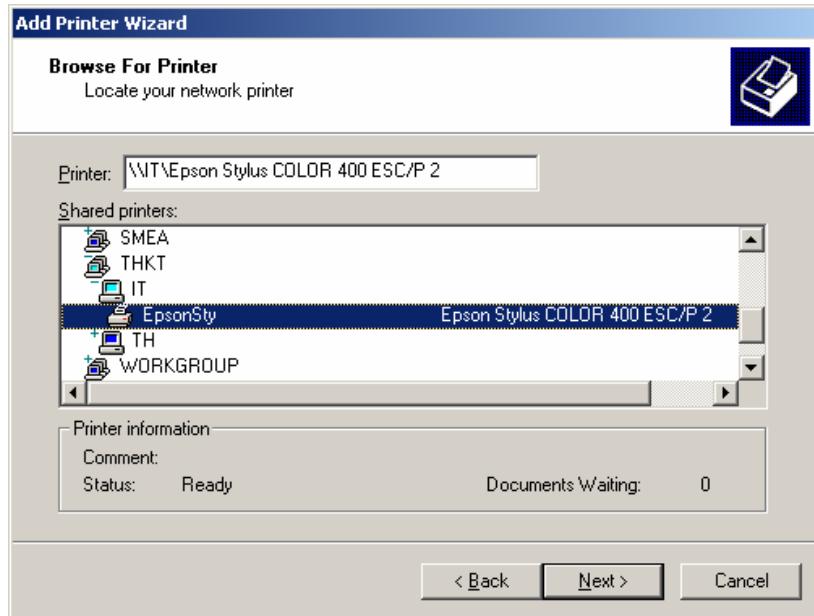


Printer Server (domain) (2) than cong. com

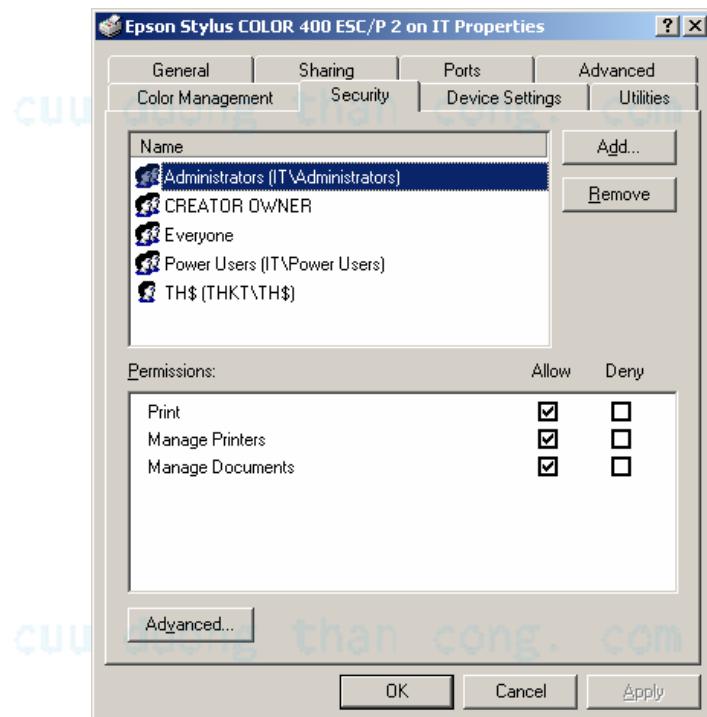
- Add máy in (chọn máy in trên mạng):



- Có thể dùng chức năng brow để tìm kiếm máy in trên mạng



Sau đó hiệu chỉnh các tham số về máy in (nếu cần), gán quyền in điều khiển và sử dụng máy in:

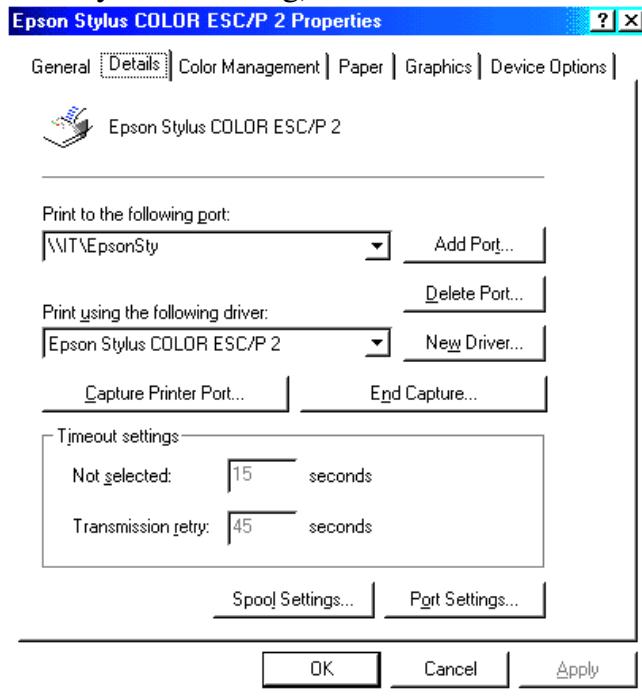


Việc sử dụng máy in có thể chọn các Permission sau:

- + Print: chỉ được quyền in
- + Manage Printer: Quyền quản lý máy in
- + Manage Document: Quyền quản lý tài liệu in ấn như tạm dừng in, xóa các tác vụ in.

Máy cǎn in Windows 9x (3)

- Login vào mạng (domain) với đủ thẩm quyền in
- Add máy in (chọn máy in trên mạng)



Trong cửa sổ PRINT TO THE FOLLOWING PORT:

\\ Server name \Printer Share name (\\IT\EpsonSty)

+ Server name: Tên máy tính cǎm máy in đã được share

+ Printer Share name: tên share của máy in

§ 8. QUẢN TRỊ SAO LUU DỮ LIỆU

8.1. Khái niệm

Trong quá trình hoạt động máy tính có thể gặp các sự cố như mất điện đột ngột, hoặc các thiết bị như đĩa cứng có thể gặp lỗi, và nhiều nguyên nhân khác, khi đó có thể xảy ra việc mất một phần hoặc toàn bộ dữ liệu trên Server. Sao lưu dữ liệu là một công việc quan trọng của quản trị mạng, có thể phân chia các công việc sao lưu dữ liệu như sau:

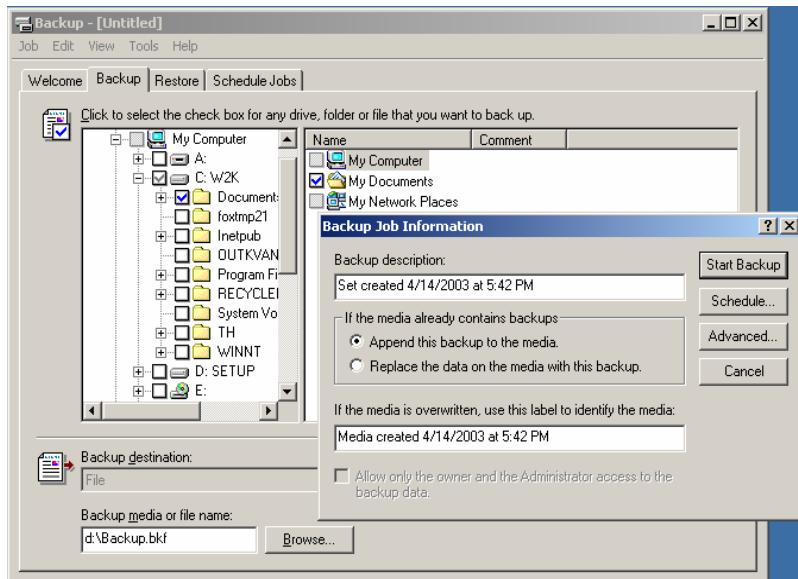
Sao lưu hệ thống: sao lưu Windows 2000 Server, cơ sở dữ liệu của hệ thống như registry và các phần mềm chạy trên nền Windows 2000 Server như SQL, Lotus notes ... Sự thay đổi của những files bao giờ cũng gắn liền với hệ thống, việc sao lưu những files này đòi hỏi can thiệp như: ngừng hoạt động chương trình, tắt các dịch vụ

Sao lưu dữ liệu của người dùng: Những dữ liệu do người dùng ghi lên mạng, những files này không làm ảnh hưởng đến hệ thống.

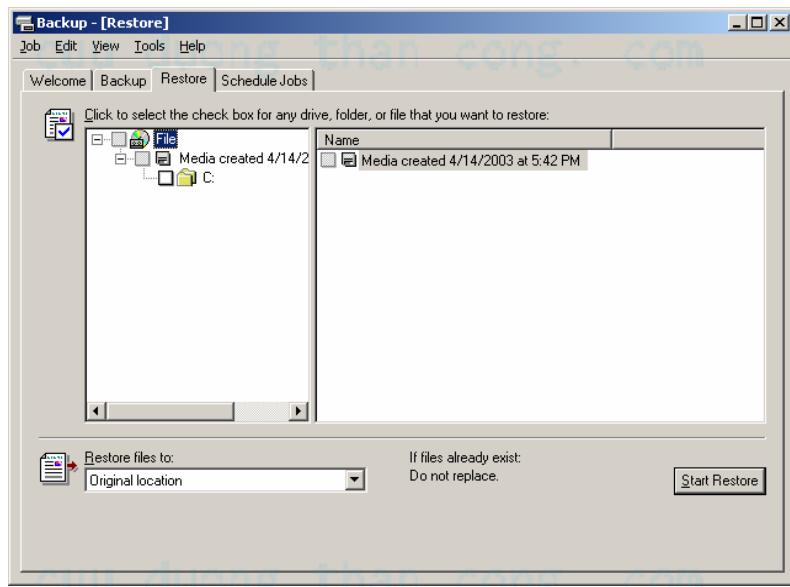
8.2. Sao lưu hệ thống

Sử dụng trình backup của windows 2000 trong thực đơn hệ thống

- Sau lưu:



- Khôi phục:



Sử dụng các giải pháp khác

- Hệ thống server song hành
- Giải pháp đồng bộ về sao lưu dữ liệu của HP
- Giải pháp sao lưu dữ liệu của các hãng khác như Seagate Technology
- Các phần mềm sao lưu dữ liệu

8.3. Sao lưu dữ liệu

Có thể dùng băng từ, đặt lịch sao lưu dữ liệu tự động.

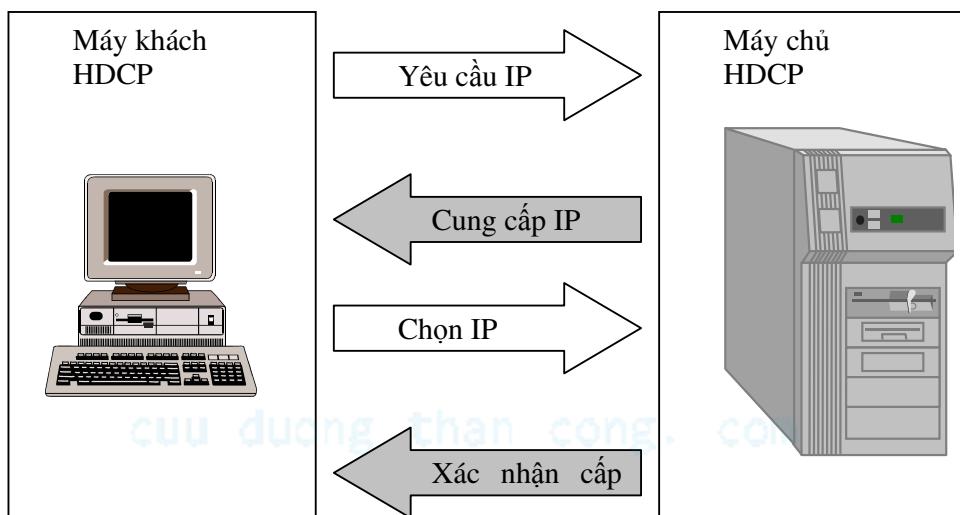
Nếu trên Server có ổ đĩa cứng dự phòng có thể sử dụng các chương trình lập lịch để tự động Copy dữ liệu.

Nếu trên Workstation dung lượng ổ đĩa cứng còn dư có thể sử dụng các chương trình lập lịch để tự động Copy dữ liệu.

§ 9. MỘT SỐ DỊCH VỤ MẠNG CỦA WINDOWS 2000

9.1. Giao thức cấu hình máy động (Dynamic Host Configuration Protocol - DHCP)

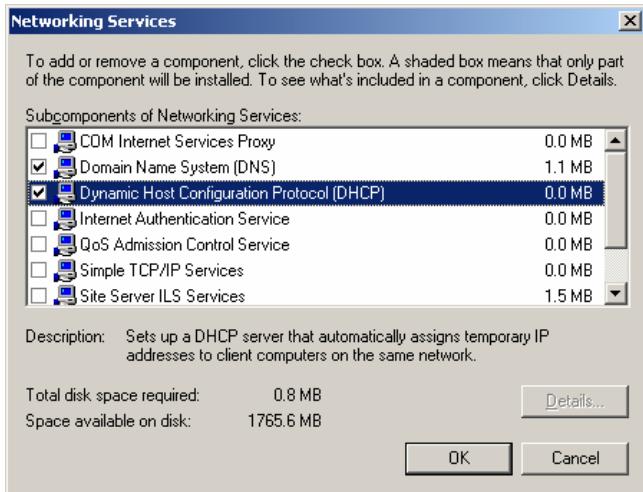
a. Khái niệm



Giao thức cấu hình máy động (DHCP) được thiết kế để tập trung hóa cấu hình và quản lý thông tin cấu hình TCP/IP bằng cách gán tự động các địa chỉ IP cho các máy được cấu hình theo DHCP. Phần mềm DHCP được cài đặt trên cả máy chủ và máy khách. Trên mạng cần ít nhất một máy server được cài đặt DHCP server. Microsoft cung cấp bộ giao thức TCP/IP với các DHCP client có sẵn trên windows 9x, windows 2000.

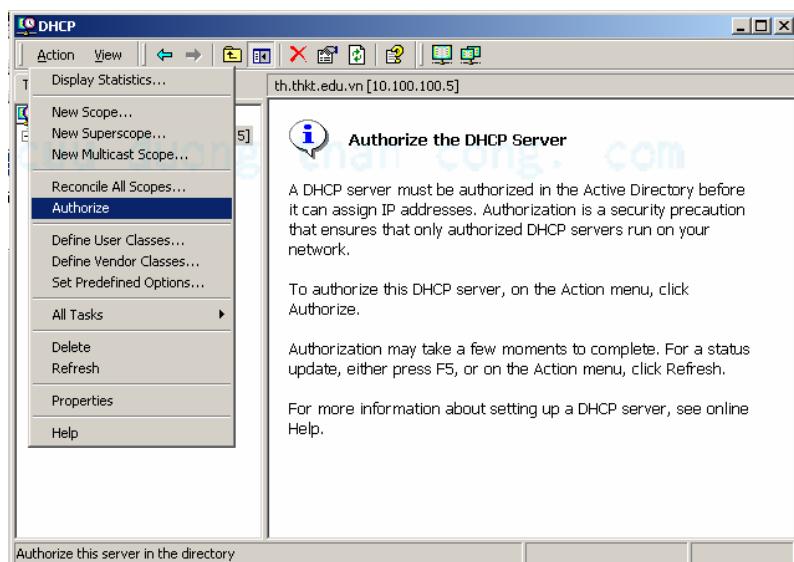
b. Cấu hình DHCP Server

- Cài đặt:
 - + Add dịch vụ DHCP trong Control Panel – Add/Remove program
 - + Chọn Add/Remove Windows Components
 - + Chọn Networking Services, chọn Details
 - + Chọn DHCP



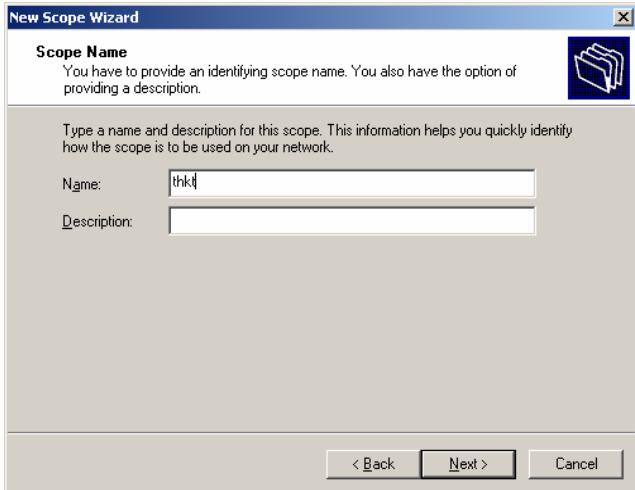
- Cấu hình DHCP được thực hiện thông qua trình DHCP Manager của Administrative Tools

+ Trao quyền cho DHCP

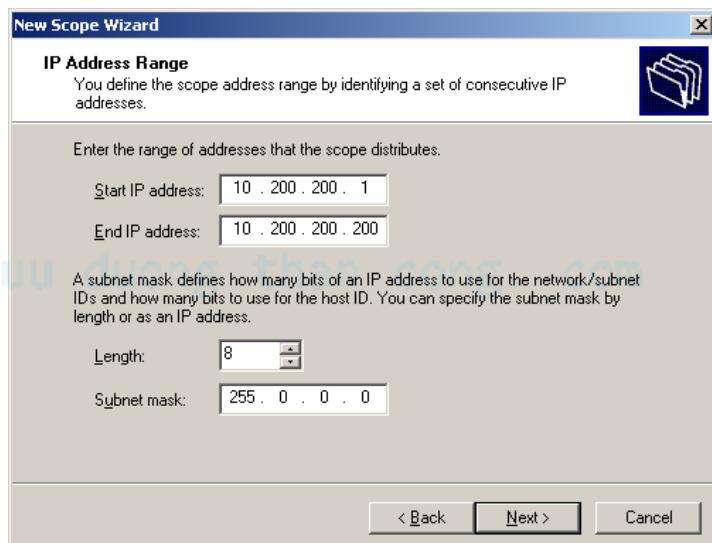


+ Tạo khu vực (Scope DHCP)

+ Đặt tên cho khu vực:



+ Chỉ định phạm vi



- + Start IP Address: Bắt đầu địa chỉ IP có thể cấp cho máy khách DHCP
- + End IP Address: Kết thúc địa chỉ IP có thể cấp cho máy khách DHCP
- + Subnet Mask: Để gán cho mọi máy khách DHCP

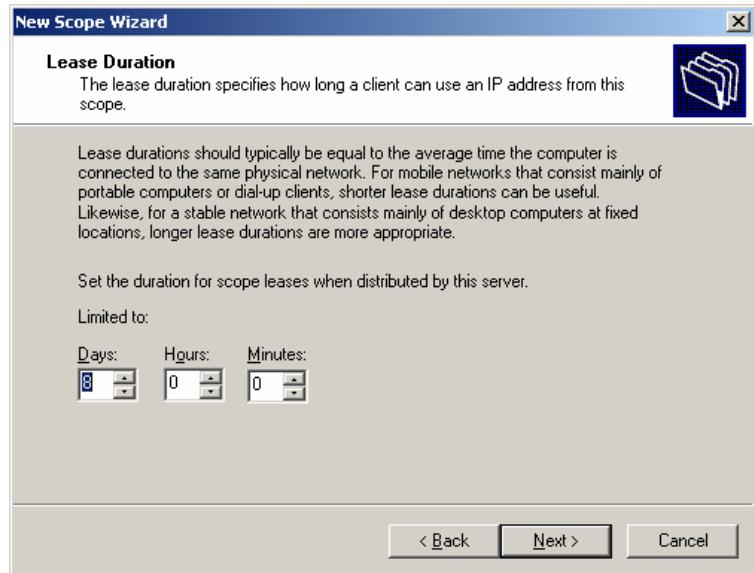
Theo ví dụ trên dải địa chỉ từ 10.200.200.1 đến 10.200.200.200 sẽ được cấp lần lượt cho các máy trạm khi truy cập mạng.

- + Có thể chọn tiếp tham số để loại ra một vài địa chỉ IP đã được dùng cho mạng

Exclusion Range – Start Address: bắt đầu địa chỉ IP cần loại bỏ

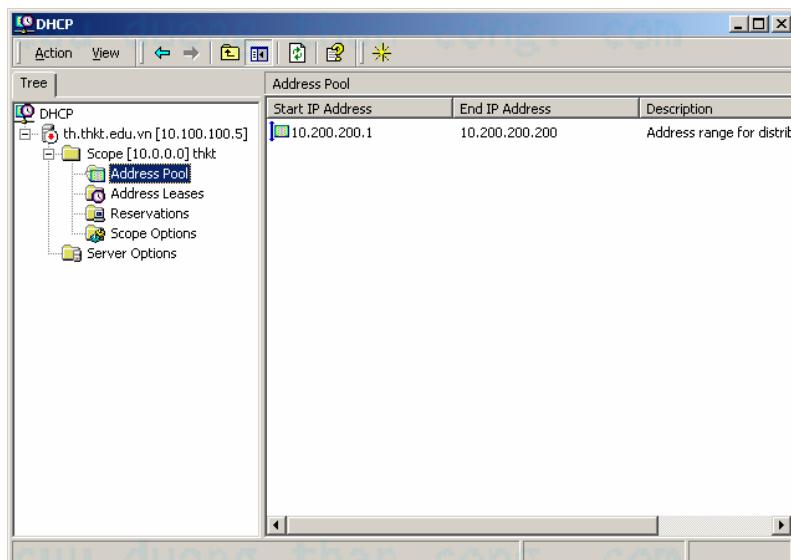
Exclusion Range – End Address: kết thúc địa chỉ IP cần loại bỏ

- + Chỉ định khoảng thời gian thuê bao (lease duration): thời gian mà DHCP cấp cho máy trạm



Lease Duration – Unlimited: không giới hạn thời gian cấp IP
 Lease Duration – Limited: Thời gian IP có hiệu lực

- + Chỉ định các tham số khác
- + Xem và hiệu chỉnh các tham số



9.2. Domain Name System (DNS)

a. *Chức năng*

DNS là một dịch vụ mạng của Windows 2000, DNS chứa cơ sở dữ liệu phân tán nhằm cung cấp hệ thống tên có thứ bậc để nhận dạng vị trí máy trên mạng, trên Internet, DNS được dùng để quản lý quản trị vùng và tên của các máy tính. DNS sử dụng mô hình máy khách – chủ.

DNS là hệ thống phân giải tên miền được phát minh vào năm 1984, ngày nay nó được coi là một dịch vụ chuẩn của mạng dùng bộ giao thức TCP/IP và Internet. Nhiệm vụ cơ bản của DNS là đổi tên miền thành địa chỉ IP và ngược lại, hỗ trợ hoạt động của các mail server.

Cấu trúc tên miền:

Bao gồm các ký tự viết cách nhau bởi dấu chấm (.), phần cuối cùng của tên miền thể hiện quốc gia quản lý tên miền này. Hiện nay tồn tại hai dạng tên miền, dạng thứ nhất, phần cuối cùng của tên miền có thể là:

Tên	Mô tả
Com	Tổ chức thương mại
Gov	Tổ chức chính phủ
Mil	Tổ chức quân sự
Net	Các nhà cung cấp mạng và dịch vụ internet
org	Tổ chức phi thương mại và phi lợi nhuận
int	Tổ chức quốc tế
edu	Tổ chức giáo dục

Ví dụ: www.cnn.com website của hãng tin CNN

Tất cả những tên miền này do Hoa Kỳ quản lý, dạng thứ hai có phần trước đuôi của tên miền giống như trên, phần cuối cùng là tên viết tắt của các quốc gia. Ví dụ VN là tên viết tắt của Việt nam , JP tên viết tắt của Nhật, ví dụ tên miền có dạng bsneu.edu.vn.

b. Một số đặc điểm

Kiểm soát tại chỗ, truy cập toàn thế giới

Internet không quản lý tập trung tên miền, mỗi tổ chức có mạng vận hành và duy trì DNS server của riêng mình. Cơ quan quản lý internet vùng (InterNIC) quản lý tất cả các tên miền đã được đăng ký, tên và địa chỉ của các DNS server của tên miền đã được đăng ký. InterNIC không cho biết địa chỉ tên miền cụ thể nhưng nó cho biết những DNS server có thể trả lời câu hỏi này.

Khả năng chịu lỗi

Mỗi miền chỉ có một DNS server chính (primary) chịu trách nhiệm giải đáp tên đối với miền đó. Khi thiết lập một server mới cần khai báo là primary DNS server, hoặc nó chỉ có thể là server phụ (secondary), thông thường DNS server phụ sẽ nối và sao chép cơ sở dữ liệu từ server chính. Trong trường hợp server chính bị lỗi hoặc có quá nhiều yêu cầu thì server phụ có thể đáp ứng yêu cầu tra vấn tin.

Các zone, các domain, và sự ủy quyền

Zone (khu vực) nó có nhiệm vụ lưu trữ phạm vi các địa chỉ IP mà DNS phải quan tâm. Trong trường hợp domain phải quản lý nhiều server của nhiều khu vực, để đơn giản trong việc tìm kiếm và xác định tên máy đó thuộc khu vực nào, có thể chia tách miền ra thành miền con. Khi chia tách thành miền con thì DNS server cấp trên cùng phải ủy quyền (delegate) cho server cấp dưới nó.

□ *Các zone tra cứu xuôi và ngược*

Quá trình chuyển đổi một tên host thành một địa chỉ IP được gọi là forward name resolution (phân giải tên xuôi). Quá trình chuyển đổi một địa chỉ IP ra tên host tương ứng được gọi là reverse name resolution (phân giải tên ngược).

□ *Những loại bản ghi DNS phổ biến*

Các bản ghi A (loại host): loại bản ghi chỉ đơn giản liên hệ một tên nào đó với một địa chỉ IP. Đây là tập hợp các tệp tin ASCII có tên là zone files, sử dụng một chữ A để biểu thị bản ghi này là một bản ghi host.

Các bản ghi SOA (start of authority): Nó là bản ghi dành cho tên của DNS server chính của miền, cung cấp địa chỉ IP cho người quản trị của miền, chỉ ra khoảng thời gian đệm trứ dữ liệu.

Các bản ghi NS: dành cho DNS server, qui định các tên server trong miền.

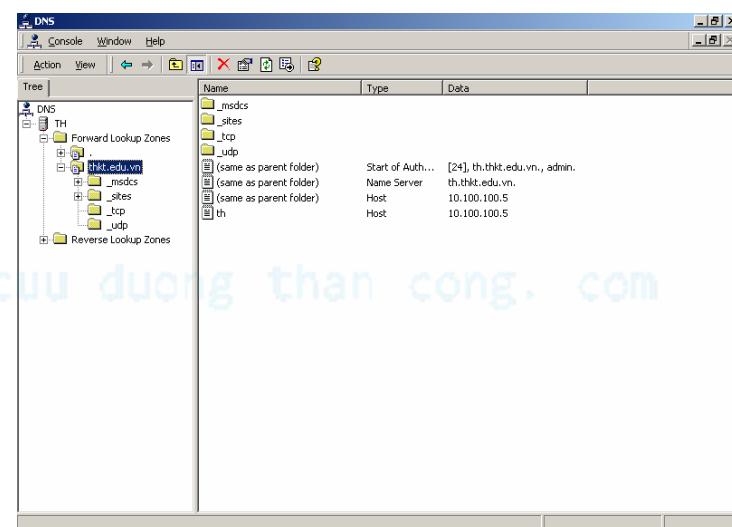
Các bản ghi CNAME: bản ghi alias hay tên kinh điển hay tên chuẩn tắc (canonical name)

Các bản ghi MX: bản ghi mail exchange

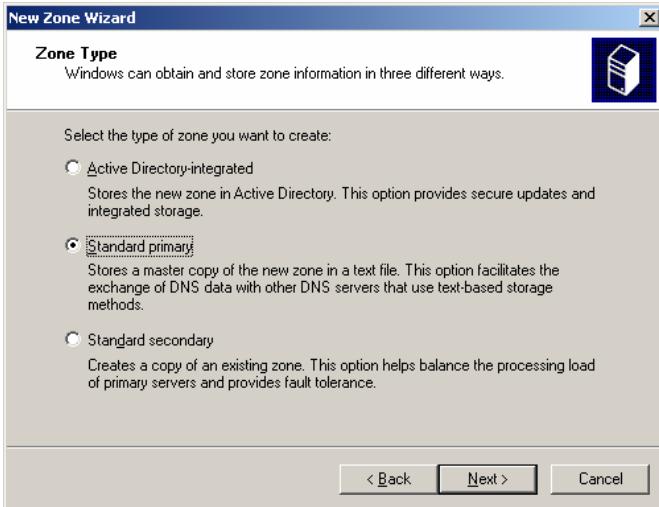
Các bản ghi PTR: bản ghi reverse host, bản ghi thông dụng trong một khu vực tra cứu xuôi.

b. Cài đặt, cấu hình

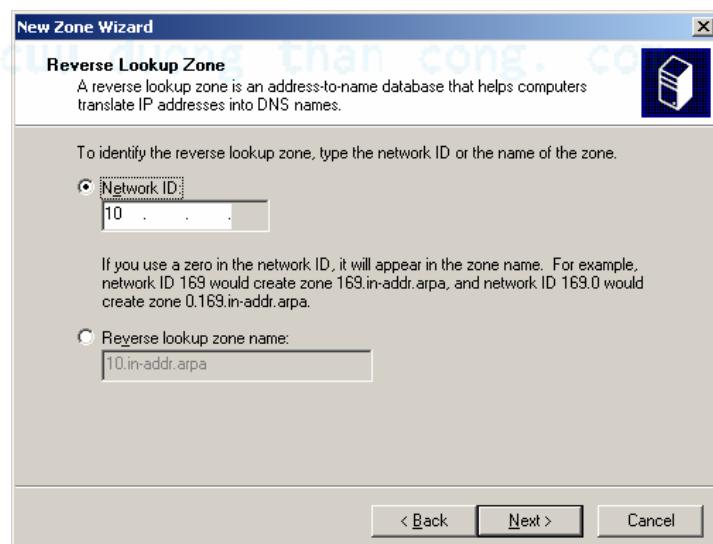
Khi cài đặt AD trên server DNS được tự động cài đặt theo, DNS cần được hiệu chỉnh các tham số.



- Tạo ra Reverse lookup zone: chọn add a new zone



- + Activate Directory Integrated: tích hợp với AD
- + Standard Primary: Tạo ra một zone chính
- + Standard secondary: tạo ra một zone phụ
- Nếu chọn Activate Directory Integrated, bước tiếp theo cần điền tham số địa chỉ mạng của lô địa chỉ IP mà mạng đang sử dụng, nhập vào mục Network ID



- Khi mạng chưa có DNS hoặc muốn tạo một dịch vụ cài đặt như sau:

 - + Add dịch vụ DNS trong Control Panel – Add/Remove program
 - + Chọn Add/Remove Windows Components
 - + Chọn Networking Services, chọn Details
 - + Chọn DNS

- Điền các tham số mà trình cài đặt yêu cầu

§ 10. TÍCH HỢP NOVELL NETWARE VỚI WINDOWS 2000

X.1. Khả năng liên kết với Novell Netware

Một phần tài nguyên của mạng có thể nằm trên máy chủ Novell Netware, mạng Windows 2000 cần phải giao tiếp và chia sẻ tài nguyên với Novell Netware. Giao thức NWLink của Windows 2000 và dịch vụ Gateway Service for Netware (GSNW) hỗ trợ các máy khách của mạng Microsoft giao tiếp và sử dụng tài nguyên trên mạng Netware.

Các đặc tính của NWLink

SPX II- NWLink hỗ trợ Windows Sockets trên giao thức Novell SPX II. SPX II được tăng cường để hỗ trợ chế độ cửa sổ và có khả năng đặt kích thước khung lớn nhất.

Da gắn kết (multiple Bindings) – NWLink có thể được gắn vào nhiều vi mạng với nhiều kiểu khung khác nhau (Frame)

Tự động phát hiện kiểu khung (Frame Type Auto Detect), có thể cấu hình để trong quá trình cài đặt tự động phát hiện kiểu khung nào là tốt nhất trên mạng và sử dụng nó.

Kiểu khung và gắn kết

Kiểu khung: Cách mà vi mạng định dạng dữ liệu để gửi lên mạng. Các máy Novell có thể được cấu hình với nhiều kiểu khung khác nhau. Để có thể giao tiếp được chúng cần phải được cấu hình với cùng một kiểu khung, ví dụ kiểu khung 802.2, 802.3. Ngoài ra mỗi Topology (Ethernet, Token Ring, ...) đòi hỏi một định dạng kiểu khung khác nhau.

10.2. Gắn kết với NWLink

Dịch vụ gắn kết, liên kết dịch vụ với giao thức và vi mạng nó sẽ sử dụng, Dịch vụ này được gắn cả với NWLink NetBIOS và NWLink IPX/SPX, do vậy hỗ trợ cho liên lạc thẳng trên thành phần máy chủ. Dịch vụ máy trạm chỉ được gắn với NWLink NetBIOS không hỗ trợ cho liên lạc thẳng với thành phần máy chủ.

Để quản lý và điều phối hiệu suất NWLink có thể dùng công cụ của Microsoft (Performance Monitor). Công cụ này cho phép hiển thị thông tin về hiệu suất của mạng, theo dõi các đối tượng nào đang sử dụng.

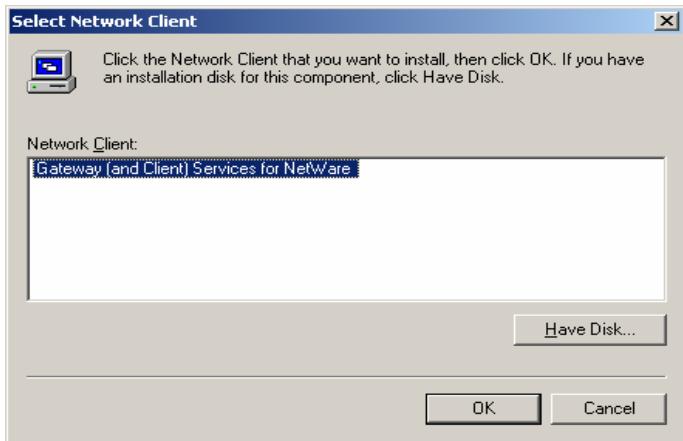
10.3. Cấu hình dịch vụ cổng nối cho Novell

Trên máy chủ Netware

Dùng tiện ích của Novell tạo nhóm người dùng NTGATEWAY, tạo user và các tham số cần thiết, bổ sung tài khoản cổng giao tiếp vào nhóm NTGATEWAY. Gắn các quyền cần thiết để các user thuộc nhóm này có thể sử dụng tài nguyên của Novell.

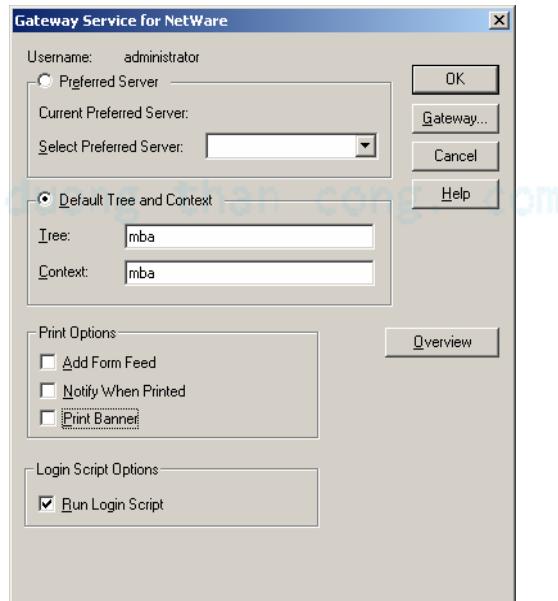
Trên máy Windows 2000

Cài đặt dịch vụ GSNW: add dịch vụ trong Control Panel – Network



Cài đặt, hiệu chỉnh các tham số

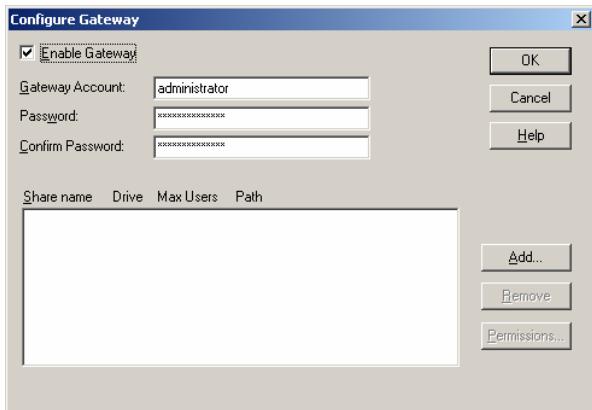
Trong Control Panel chọn biểu tượng GSNW, hiệu chỉnh các tham số sau



Lựa chọn Nội dung

Prerred Server	Máy chủ Novell sẽ được tự động nối đến
Default Tree	Nhập các thông số của cây thư mục NDS
Default Context	Nhập ngữ cảnh ngầm định
Run Login Script	Chạy Login script
Gateway	Cấu hình cổng nối cho các tài nguyên

Cấu hình cho Gateway



Đánh dấu vào mục Enable Gateway và điền các tham số về user

Chọn ADD để cấu hình đường dẫn đến tài nguyên trên Novell

Điền đường dẫn đầy đủ trong hộp Network Path của máy chủ Novell

§ 11. MỘT SỐ TIỆN ÍCH

a. *Ipconfig*

- Có trên Windows 9x, Windows 2000

Lệnh này hiển thị các giá trị cấu hình mạng TCP/IP đang hoạt động. Lệnh này đặc biệt có ý nghĩa đối với mạng có sử dụng DHCP, nó cho phép người sử dụng xác định cấu hình TCP/IP mà được cung cấp bởi DHCP

ipconfig [/all | /renew [adapter] | /release [adapter]]

Tham số

All : Hiển thị đầy đủ. Bỏ tham số này, **ipconfig** sẽ chỉ hiển thị địa chỉ IP, subnet mask, và default gateway.

/renew [adapter] : Thay mới cấu hình cung cấp bởi DHCP. Lựa chọn này chỉ tồn tại trên hệ thống chạy dịch vụ DHCP client. Để chỉ định card, đánh tên card khi sử dụng **ipconfig** mà không cần đánh tham số.

/release [adapter] Bỏ cấu hình DHCP hiện thời. Mục chọn này ngừng hoạt động của TCP/IP trên hệ thống và chỉ tồn tại trên các hệ thống chạy DHCP client. Để chỉ định card, đánh tên card khi sử dụng **ipconfig** mà không cần đánh tham số.

Không điền tham số, **ipconfig** sẽ hiển thị toàn bộ cấu hình TCP/IP hiện tại bao gồm địa chỉ IP và subnet mask.

b. *Ping*

Kiểm tra kết nối tới một hệ thống khác. Lệnh này chỉ tồn tại nếu TCP/IP được cài đặt.

ping [-t] [-a] [-n count] [-l length] [-f] [-i ttl] [-v tos] [-r count] [-s count] [[-j computer-list] | [-k computer-list]] [-w timeout] destination-list

Tham số

-t : Chỉ ngừng khi bị ngắt bởi người sử dụng.

-a : Tìm tên máy khi biết địa chỉ IP.

-n count

Gửi một số lần nhất định bó dữ liệu ECHO, số lần được xác định bởi count, ngầm định là 4 lần.

-l length : Gửi dữ liệu ECHO với độ dài được xác định bởi length, ngầm định là 32 byte, tối đa là 65527.

-f : Gửi lệnh với cờ hiệu “Do not Fragment” trong bó dữ liệu. Bó dữ liệu sẽ không bị chia tách trong khi chuyển tới đích.

-i ttl : Đặt trường ”Time To Live” giá trị chỉ định ở tham số *ttl*.

-v tos : Đặt trường ”Type Of Service” giá trị chỉ định bởi *tos*.

-r count : Ghi lại đường đi của bó dữ liệu và bó dữ liệu trả về được đặt ở trường ”Record Route” . Nhỏ nhất là 1 và lớn nhất là 9 đối với tham số *count*

-s count : Chỉ rõ thời gian đối với mỗi hop bởi *count*.

-j computer-list : Chỉ rõ đường đi qua danh sách các máy chỉ định bởi *computer-list*. Các địa chỉ máy tiếp được ngăn cách bởi các gateway. Số lượng tối đa danh sách là 9 IP.

-k computer-list : Chỉ rõ đường đi qua danh sách các máy chỉ định bởi *computer-list*. Các địa chỉ máy tiếp không được ngăn cách bởi các gateway. Số lượng tối đa danh sách là 9 IP.

-w timeout : Chỉ rõ khoảng thời gian ngắn dưới dạng milliseconds.

destination-list : Chỉ rõ các máy sẽ được ping.

c. Tracert

Chương trình này xác định đường đi tới một địa chỉ bằng cách gửi bó dữ liệu kiểu Internet Control Message Protocol (ICMP) với các giá trị Time-To-Live (TTL) khác nhau. Mỗi một router trên đường đi qua của bó dữ liệu sẽ giảm biến TTL của bó dữ liệu ít nhất là 1 đơn vị trước khi chuyển tiếp bó dữ liệu, do đó, biến TTL rất hữu ích khi dùng để đếm các hop. Khi giá trị của TTL của bó dữ liệu giảm còn 0, router sẽ gửi trả hệ thống một message “ICMP Time Exceeded”. **Tracert** xác định đường đi bằng cách gửi bó dữ liệu đầu tiên với giá trị của TTL là 1 và sau đó sẽ tăng TTL lên 1 sau mỗi lần gửi tiếp theo cho đến khi hệ thống đích trả lời hoặc TTL tiến tới giá trị tối đa. Đường đi được xác định bởi kiểm tra message “ICMP Time Exceeded” mà được gửi trả lại bởi các router

trung gian. Tuy nhiên, một số router hủy các gói dữ liệu mà không gửi lại message khi TTL về không sẽ làm cho **tracert** không xác định được.

tracert [-d] [-h maximum_hops] [-j computer-list] [-w timeout] target_name

Tham số

-d : Chỉ rõ không tìm tên máy.

-h maximum_hops : Chỉ rõ số hop tối đa trước khi tới hệ thống đích.

-w timeout : Chỉ rõ thời gian đợi của mỗi lần trả về thông tin trả lời theo milliseconds .

target_name : Tên của hệ thống đích.

d. Ftp

Tải file về máy hoặc tải sang một hệ thống chạy dịch vụ FTP server. **Ftp** can be used interactively. Lệnh này chỉ tồn tại nếu giao thức TCP/IP đã được cài đặt. FTP là 1 dịch vụ khi chạy tạo ra một môi trường mà bạn có thể sử dụng các lệnh con của FTP, sau đó có thể thoát ra bằng lệnh **quit**. Khi đang trong môi trường của FTP thì dấu nhắc **ftp** sẽ xuất hiện.

ftp [-v] [-n] [-i] [-d] [-g] [-s:filename] [-a] [-w:windowsize] [computer]

Tham số

-v : Bỏ qua các dòng trả lời từ server **ftp**

-n : Không tự động yêu cầu login sau khi chạy **ftp**.

-i : Bỏ các dòng thông báo trong khi chuyển nhiều file.

-d : Cho phép dò lỗi, hiển thị tất cả các lệnh được thực hiện giữa ứng dụng khách ftp và server ftp.

-s:filename : Chỉ rõ 1 file dạng text chứa các lệnh ftp; các lệnh này sẽ chạy sau khi ftp khởi động.

Computer : Chỉ rõ tên máy hoặc IP của hệ thống từ xa cần truy cập. Nếu có tham số này thì nó phải là tham số đứng cuối cùng trong dòng lệnh.

e. Finger

Hiển thị tất cả các thông tin về người dùng trên một hệ thống chạy dịch vụ Finger. Các thông tin hiển thị sẽ thay đổi tùy theo hệ thống từ xa. Lệnh này chỉ tồn tại khi có cài TCP/IP.

finger [-l] [user]@computer [...]

Tham số

-l : Hiển thị liệt kê dài.

User : Tên người sử dụng cần biết. Nếu không chỉ rõ thì thông tin của tất cả người sử dụng sẽ hiển thị

TỪ ĐIỂN THUẬT NGỮ

Access permission	Quyền truy cập
Account lockout	Khoá tài khoản
Account policy	Chính sách tài khoản
Address	Địa chỉ
Address class	Lớp địa chỉ
Administrative account	Tài khoản quản trị
Administrative alert	Báo động quản trị
Administrator	Nhà quản trị
Administrator privilege	Đặc quyền (ở cấp độ) nhà quản trị; đặc quyền Administrator
Archive bit	Bít lưu trữ
Associate	Phối hợp
Attribute	Thuộc tính
Auditing	Kiểm toán
Audit policy	Chính sách Audit
Backup domain controller (BDC);	Máy điều khiển vùng dự phòng
Bits per second (BPS)	Số bít/giây.
Boot partition	Phần đĩa khởi động
Bridge	Cầu nối
Broadcast message	Thông điệp phát rộng
Brouter	Kết hợp các phần tử của cầu nối và bộ định tuyến.
Browse	Duyệt xem
Built-in group	Nhóm cài sẵn
Capture	Chụp ảnh
Client	Máy khách
Client application	Ứng dụng máy khách.
Client service for Netware	Client Service for Netware
Common group	Nhóm chung
Communications setting	Xác lập truyền thông
Compact	Tiện ích dạng dòng lệnh, dùng để nén tập tin trên volume NTFS.
Computer account	Tài khoản máy tính.
Computer browser server	Dịch vụ Computer Browser.
Computer name	Tên máy tính
Configure	Lập cấu hình
Connect	Nối kết
Connected user	Người dùng được nối kết
Connection oriented protocol	Giao thức hướng nối kết
Default gateway	Cổng giao tiếp mặc định

Default network	Mạng mặc định
Default user	Người dùng mặc định
Dial-up line	Đường truyền quay số
Dial-up networking	Nối mạng qua đường quay số
Disabled user account	Tài khoản người dùng bị cấm sử dụng
DNS name server	Máy phục vụ tên DNS
DNS service	Dịch vụ DNS
Domain	Vùng
Domain controller	Máy điều khiển vùng
Domain name	Tên vùng
Domain name system (DNS)	Hệ thống tên vùng
Dynamic host configuration protocol (DHCP)	Giao thức cung cấp cấu hình động của địa chỉ IP và các thông tin liên quan
Extended partition	Phần chia mở rộng
Fault tolerance	Cơ chế dung lõi
File allocation table (FAT)	Bảng phân phối tệp tin
File sharing	Chia sẻ tệp tin
File system	Hệ thống tệp tin
File transfer protocol (FTP)	Dịch vụ hỗ trợ việc chuyển tải tệp tin giữa những hệ thống cục bộ và ở xa nào chấp nhận giao thức này.
Gateway	Cổng giao tiếp
Geteway service for Netware	Được kèm theo Windows NT Server, W2K cho phép máy tính chạy Windows NT, W2K kết nối với máy phục vụ Netware.
Global account	Tài khoản toàn cục
Global group	Nhóm toàn cục
Gopher	Hệ thống thứ bậc để tìm và phục hồi thông tin từ Internet hoặc một Intranet nào đó.
Group	Nhóm
Group account	Tài khoản nhóm
Guest	Người dùng vãng lai, khách vãng lai
Home Directory	Thư mục cá nhân
Host	Máy chủ
Home page	Trang chủ
Host ID	Số nhận diện máy chủ
Internet Protocol (IP)	Giao thức truyền thông điệp của dãy giao thức TCP/IP

Internet Router	Bộ định tuyến Internet
IP address	Địa chỉ IP
IP Router	Bộ định tuyến IP
ISO	Viết tắt từ International Standards Organization (Tổ chức tiêu chuẩn hóa quốc tế)
Kermit	Giao thức chuyển tải các tệp tin nhị phân
Kernel	Thành phần của Windows NT Executive W2K, chịu trách nhiệm quản lý bộ vi xử lý.
Local account	Tài khoản cục bộ
Local group	Nhóm cục bộ
Local printer	Máy in cục bộ
Localtalk	Ten do Apple Computer dùng để gọi phần cứng nối mạng Apple
Log off	Tách khỏi mạng
Log on	Truy nhập
Logon script	Script đăng nhập, kịch bản đăng nhập
Mac address	Địa chỉ MAC
Macintosh accessible volume	Volume có thể truy cập bởi macintosh
Mapping	Sự ánh xạ
Mapping file	Tệp tin ánh xạ
Master Boot Record	Vùng quan trọng trên đĩa cứng, chứa cấu trúc dữ liệu bắt đầu quy trình khởi động máy tính
Master domain	Vùng chính
Member server	Máy phục vụ thành viên
Migration Tool for Netware	Được cung cấp kèm theo Windows NT, cho phép chuyển tải các tài khoản và các thông tin liên quan đến máy tính chạy Windows NT Server, W2K
Mirror set	Một bản sao hoàn chỉnh của dữ liệu
Modem	Modulator/Demodulator, thiết bị truyền, nhận dữ liệu qua đường điện thoại chuẩn
Name mapping	Ánh xạ tên
Name Resolution Service	Dịch vụ phân giải tên
Net Logon Service	Dịch vụ Net logon
Netware Directory Services (NDS)	Một dịch vụ Netware chạy trên các

	máy phục vụ Netware, dịch vụ này cho phép định rõ địa điểm của tài nguyên trên mạng (từ Netware 4.x)
Network adapter card	Thiết bị dùng nối mạng máy tính (card mạng)
Network ID	Số nhận diện mạng
Network protocol	Giao thức mạng
Network sniffer	Công cụ giải đoán mạng
Node	Nút, điểm nối
NT file system, NTFS	Hệ thống tệp tin NT, W2K
Object	Đối tượng
Open Systems Interconnection (OSI) model	Mô hình OSI
Orphan	Thành viên mồ côi
Owner	Chủ sở hữu
Packet	Gói dữ liệu
Page fault	Lỗi trang nhớ
Paging file	Tệp tin phân trang
Parity	(thông tin) chẵn lẻ
Partition	Phần chia (đĩa)
Partition Table	Bảng quản lý đĩa
Permission	Quyền truy cập
Personal group	Nhóm cá nhân
Ping	Lệnh Ping, có thể dùng để kiểm tra các kết nối với một hay nhiều máy chủ ở xa
Point-to-Point protocol (PPP)	Tập hợp giao thức và tạo khung theo chuẩn công nghiệp, là thành phần của Windows 2000
Port ID	Số nhận diện cổng
Primary domain controller (PDC)	Máy điều khiển vùng chính
Primary Partition	Phần chia chính
Printer permission	Quyền truy cập máy in
Print sharing	Chia sẻ máy in
Print spooler	Bộ đệm in
Privilege level	Cấp độ đặc quyền
Property	Thuộc tính
Proxy	Máy được uỷ nhiệm
Queue	Hàng chờ
Raid (Redundant Array off Inexpensive Disks)	Một phương pháp dùng để chuẩn hóa và phân loại các hệ dung lõi đĩa.

Remote Access Service (RAS)	Dịch vụ truy cập từ xa
Remote Procedure Call (RPC)	Cuộc gọi thủ tục từ xa
Repeater	Bộ đổi hướng
Resource	Tài nguyên
Roaming user profile	Hệ lưu trữ người dùng lưu động
Router	Bộ định tuyến
Security Accounts Manager (SAM)	Một cơ sở dữ liệu chứa thông tin bảo mật của Windows NT, W2K
Secure Sockets Layer (SSL)	Giao thức cung cấp truyền thông dữ liệu an toàn thông qua cơ chế mã hoá và giải mã dữ liệu
Server message block (SMB)	Khối thông điệp máy phục vụ
Server zone	Khu vực máy phục vụ
Session	Phiên, kỳ làm việc
Share	Chia sẻ
Share resource	Tài nguyên dùng chung
Simple Mail Transfer protocol (SMTP)	Giao thức chuyển thư giản đơn
Simple Network Management Protocol (SNMP)	Giao thức quản lý mạng giản đơn
Acronym for structured query language (SQL)	Ngôn ngữ hỏi có cấu trúc
System partition	Phần chia hệ thống
System police	Chính sách hệ thống
Transforms	Nguyên tắc biến đổi
Trap	Bẫy
True Type Font	Một kiểu phông chữ
Trust relationship	Quan hệ uỷ quyền
Uninterruptible power supply (UPS)	Bộ cung cấp điện năng liên tục
User account database	Cơ sở dữ liệu tài khoản người dùng
User Datagram Protocol (UDF)	Giao thức bó dữ liệu người dùng
User right policy	Chính sách về quyền người dùng
Variables	Biến
Virtual server	Máy phục vụ ảo

TÀI LIỆU THAM KHẢO

1. Mạng máy tính và các hệ thống mở, GS. TS. Nguyễn Thúc Hải, NXB Giáo dục 1999
2. Mạng máy tính, Lược dịch và biên soạn Hồ Anh Phong Nhà xuất bản Thông kê, 2002
3. Cốt túy về mạng (Networking Essentials) , biên dịch Phạm Cao Hoàn, Phạm Đình Phước, Nguyễn Văn Khôi, NXB Đồng Nai 2000
4. Upgrading and Repairing Networks, Craig Zacker, Publisher: Que ,1/1995
5. High-Performance Networking Unleashed, Macmillan Computer Publishing
- CNE Training Guide Netware 4.1 Administration, KARANJIT SIYAN, PH.D. Publisher: New Riders, Sep-1995
6. Novell Netware 4.1, Novell, Inc. December 1994
7. Làm chủ Windows 2000 Server, Phạm Hoàng Dũng, Hoàng Đức Hải, NXB Giáo dục 2000
8. Microsoft Windows 2000 Server Unleashed, Sams Publishing 2000
9. Windows 2000 Server Study Guide, SYBEC 2000
10. Administrating W2K Network Infrastructure, SYBEC 2000
11. Windows 2000 Server, Syngress 2001
12. Các trang web: www.microsoft.com , www.novell.com, www.cisco.com,

cuu duong than cong. com