GIÁO TRÌNH MẠNG MÁY TÍNH

2003

Võ Thanh Tú - Hoàng Hữu Hạnh

MỤC LỤC

Trong quá trình hoàn thành giáo trình không thể tránh khỏi những sai sót, rất mong được sự đóng góp ý kiến của các đọc giả để giáo trình ngày càng hoàn thiện hơn. Xin cám ơn.

CHƯƠNG 1
TỔNG QUAN VỀ MẠNG MÁY TÍNH

Ngày nay, nhu cầu sử dụng máy tính không ngừng được tăng lên về cả số lượng và ứng dụng, đặc biệt là sự phát triển hệ thống mạng máy tính, kết nối các máy tính lại với nhau thông qua môi trường truyền tin để cùng nhau chia sẻ tài nguyên trên mạng góp phần làm tăng hiệu quả của các ứng dụng trong tất cả các lĩnh vực khoa học kỹ thuật, kinh tế, quân sự, văn hoá.... Sự kết hợp của máy tính với hệ thống truyền thông (communication) đặc biệt là viễn thông (telecommunication) đã tạo ra một sự chuyển biến có tính cách mạng trong vấn đề tổ chức khai thác và sử dụng các hệ thống máy tính. Từ đó đã hình thành các môi trường trao đổi thông tin tập trung, phân tán, cho phép đồng thời nhiều người cùng trao đổi thông tin với nhau một cách nhanh chóng và hiệu quả từ những vị trí địa lý khác nhau. Các hệ thống như thế được gọi là mạng máy tính (computer networks).

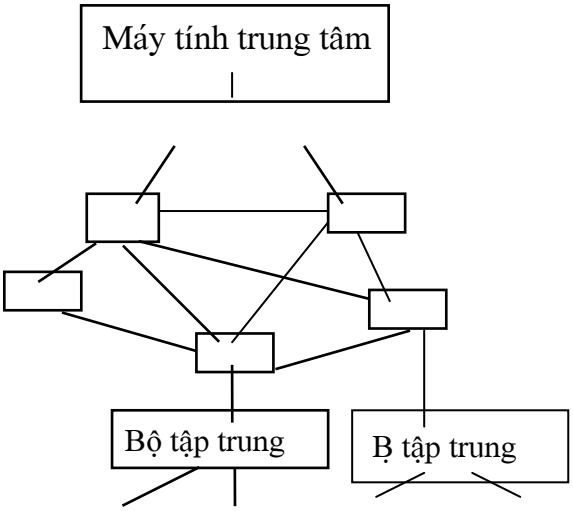
Mạng máy tính trở thành lĩnh vực nghiên cứu, phát triển rất quan trọng bảo đảm truyền tin đáng tin cậy, chính xác, phù hợp tốc độ và đảm bảo an toàn thông tin trên mạng.

I. SỰ HÌNH THÀNH VÀ PHÁT TRIỂN CỦA MẠNG MÁY TÍNH

Trước những năm 1970 đã bắt đầõu hình thành các máy tính nối với nhau thành mạng và các thiết bị đầu cuối dữ liệu đã kết nối trực tiếp vào máy tính trung tâm để tận dụng tài nguyên chung, khai thác dữ liệu, giảm giá thành truyền số liệu, sử dụng tiện lợi và nhanh chóng hơn. Cùng với thời gian xuất hiện các máy tính Mini Computer và máy tính cá nhân (Personal Computer) đã tăng yêu cầu truyền số liệu giữa máy tính - trạm đầu cuối (Terminal) và ngược lại hình thành nhiều mạng cục bộ, mạng diện rộng trong phạm vi lớn. Do đó mạng máy tính ngày càng được phát triển để đáp ứng với nhu cầu của người sử dụng. Sự hình thành của mạng máy tính được mô tả như sau:

Ban đầu là sự kết nối các thiết bị đầu cuối trực tiếp đến máy tính lớn, tiếp theo do sự phát triển ngày càng nhiều các trạm nên chúng được kết nối thành từng nhóm qua bộ tập trung rồi nối đến máy chủ trung tâm. Trong giai đọan này máy tính trung tâm có chức năng quản lý truyền tin qua các tấm ghép nối điều khiển cứng đó để tăng sức mạnh quản lý toàn hế thống trước khi dữ liệu được đưa đến máy tính trung tâm người ta thay thế các tấm ghép nối, quản lý đường truyền bằng máy tính MINI. Bộ tiền xử lý gắn chặt với trung tâm, các xử lý ngọai vi đưa vào máy chủ trong những trạm đầu cuối thông minh.

Trong giai đọan cuối đưa vào mạng truyền tin cho phép xây dựng mạng máy tính rộng lớn .



Hình 1: Mô hình mạng tổng quát

Mạng truyền tin bao gồm các nút truyền tin và các đường dây truyền tin nối giữa các nút để đảm bảo vận chuyển tin. Các thiết bị đầu cuối, thiết bị tập trung, bộ tiền xử lý và các máy tính được ghép nối vào các nút mạng.

Trong giai đoạn này xuất hiện các trạm đầu cuối thông minh mà nó ngày càng liên kết với các máy Mini.

Chức năng của máy tính trung tâm:

- Xử lý các chương trình ứng dụng, phân chia tài nguyên và ứng dụng.
- Quản lý hàng đợi và các trạm đầu cuối.

Chức năng của bộ tiền xử lý :

- Điều khiển mạng truyền tin (Đường dây, cất giử tập tin, trạm đầu cuối)
- Điều khiển chuyển ký tự lên đường dây, bổ sung hay bỏ đi những ký tự đồng bộ.

Chức năng của bộ tập trung: Quản lý truyền tin, các đầu cuối. Tiền xử lý, lưu trữ số liệu, điều khiển giao dịch.

Chức năng của thiết bị đầu cuối:

- Quản lý truyền tin, thủ tục truyền tin, ghép nối với người sử dụng.
- Điều khiển truy nhập số liệu và lưu trữ số liệu.

Do số lượng các trạm đầu cuối ngày càng tăng, nếu nối trực tiếp với máy tính trung tâm, tốn vật liệu nối ghép, quản lý nặng nề, không tương xứng với nhiệm vụ của máy tính, hiệu suất thấp nên đưa ra bộ tập trung để khắc phục những nhược điểm trên.

Tóm lại, việc kết nối các máy tính thành mạng nhằm vào các mục đích chính sau:

- Tận dụng tài nguyên chung, chinh phục khỏang cách.
- Tăng chất lượng hiệu quả khai thác, xử lý thông tin và độ tin cậy của hệ thống.

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. Tất cả các tín hiệu đó biểu thị các dữ liệu dưới dạng xung nhị phân.

Có hai loại đường truyền: Hữu tuyến (cable), vô tuyến (wireless) được sử dụng trong việc kết nối mạng. Đường truyền hữu tuyến gồm có cáp đồng trục, cáp xoắn đôi, cáp sợi quang, đường truyền vô tuyến gồm có: sóng Radio, sóng cực ngắn (viba), tia hồng ngoại (infrared).

Tất cả các tín hiệu truyền giữa các máy tính có dạng sóng điện từ và có tần số trãi từ tần số cực ngắn đến tia hồng ngoại. Tùy theo tần số của sóng điện từ mà có thể dùng các đường truyền vật lý khác nhau để truyền. Đường truyền vật lý có những đặc trưng cơ bản sau: Giải thông, độ suy hao, độ nhiễu từ.

+ **Giải thông** (*bandwidth*) của đường truyền là độ đo phạm vi tần số mà nó có thể đáp ứng được.
+ **Thông lượng** của một đường truyền chính là tốc độ truyền dữ liệu trên đường truyền đó, tính bằng số bit/giây.
+ **Độ suy hao** là độ đo độ suy yếu của tín hiệu trên đường truyền. Cáp càng dài thì độ suy hao càng lớn.
+ **Độ nhiễu điện từ** làm nhiễu tín hiệu trên đường truyền.

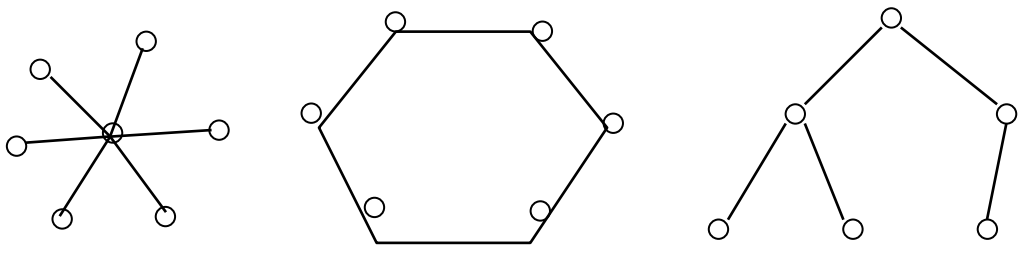
2. Kiến trúc mạng

Kiến trúc mạng máy tính là thể hiện cách nối ghép các máy tính với nhau như thế nào 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 mạng hoạt động tốt. Cách nối các máy tính được gọi là hình trạng (topolopy) của mạng.

*** Topo mạng:**

Có hai kiểu nối mạng chủ yếu là *điểm - điểm* (*point - to - point*) và quảng bá (*broadcast hay point - to - multipoint*).

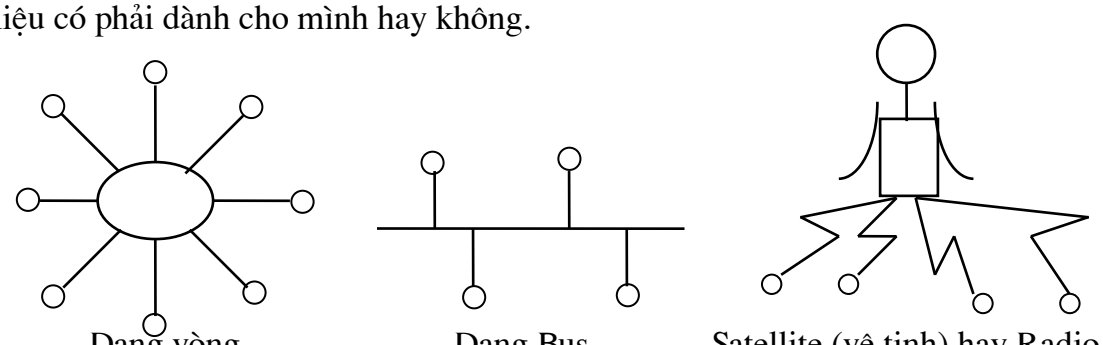
Theo kiểu *điểm - điểm,* các đường truyền nối từng cặp nút với nhau và mỗi nút đều có trách nhiệm lưu trữ tạm thời sau đó chuyển tiếp dữ liệu đi cho tới đích. Do cách thức làm việc như thế nên mạng kiểu này còn được gọi là mạng □*Lưu và chuyển tiếp*□ (*store and forward*). Hình 1-4 cho một số dạng Topo mạng *Điểm - Điểm* :



Hình Sao Chu trình Cây

Hình 1-2 : Một số topo mạng kiểu Điểm - Điểm

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



Dạng vòng Dạng Bus Satellite (vệ tinh) hay Radio

Hình 1- 3: Topo của mạng kiểu quảng bá.

3. Giao thức mạng (Network protocol)

Việc trao đổi thông tin, cho dù là đơn giản nhất, cũng đều phải tuân theo những quy tắc nhất định. Việc truyền tín hiệu trên mạng 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, chất lượng truyền tin và xử lý các lỗi. Yêu cầu về xử lý và trao đổi thông tin của người sử dụng càng cao thì các quy tắc càng nhiều và phức tạp hơn. Tập hợp tất cả những quy tắc, quy ước đó được gọi là giao thức *(Protocol)* của mạng. Rõ ràng là các mạng có thể sử dụng các giao thức khác nhau tùy sự lựa chọn của người thiết kế, tuy nhiên các tổ chức chuẩn quốc tế đã đưa ra một số giao thức chuẩn được dùng trong nhiều mạng khác nhau để thuận lợi cho việc kết nối chung.

III. PHÂN LOẠI MẠNG MÁY TÍNH

Có nhiều cách phân loại mạng khác nhau tùy theo yếu tố chính được chọn để làm chỉ tiêu phân loại.

1. Phân loại mạng theo khoảng cách địa lý

Nếu lấy "*khoảng cách địa lý* □ làm yếu tố chính thì mạng được phân chia thành mạng cục bộ, mạng đô thị, mạng diện rộng, mạng toàn cầu.

+ **Mạng cục bộ** (LAN: Local Area Network): là mạng được cài đặt trọng một phạm vi tương đối nhỏ (ví dụ trong một cơ quan, công ty, trường học ...).
+ **Mạng đô thị** (MAN: Metropolitan Area Network): là mạng được cài đặt trong phạm vi một thành phố, một trung tâm kinh tế, phạm vi địa lý là hàng trăm Km.
+ **Mạng diện rộng** (WAN: Wide Area Network): phạm vi hoạt động của mạng có thể vượt qua biên giới một quốc gia, có thể cả một khu vực.
+ **Mạng toàn cầu** (VAN: Vast Area Network): phạm vi của mạng trải rộng khắp lục địa của trái đất.

Khoảng cách địa lý có tính chất tương đối đặc biệt trong thời đại ngày nay những tiến bộ và phát triển của công nghệ truyên dẫn và quản lý mạng nên ranh giới khoảng cách địa lý giữa các mạng là mờ nhạt.

Tuy nhiên về sau người ta thường quan niệm chung bằng cách đồng nhất 4 loại thành 2 loại sau:

WAN là mạng lớn trên diện rộng, hệ mạng này có thể truyền thông và trao đổi dữ liệu với một phạm vi lớn có khỏang cách xa như trong một quốc gia hay quốc tế.

LAN là mạng cục bộ được bố trí trong phạm vi hẹp như một cơ quan, một Bộ, Nghành... Một số mạng LAN có thể nối lại với nhau để tạo thành một mạng LAN lớn hơn.

2. Phân loại mạng theo kỹ thuật chuyển mạch

Nếu lấy kỹ thuật chuyển mạch so sánh thì có thể phân chia mạng ra thành: *Mạng chuyển mạch kênh, mạng chuyển mạch thông báo, mạng chuyển mạch gói.*

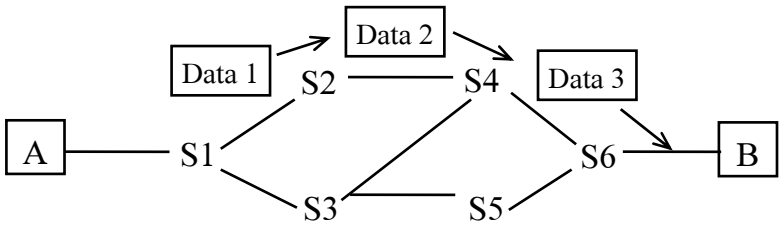
2.1 Mạng chuyển mạch kênh (Cirucuit - Switched - Network)

Đây là mạng giữa hai thực thể muốn liên lạc với nhau thì giữa chúng tạo ra một kênh cứng, cố định được duy trì liên tục cho đến khi một trong hai thực thể ngắt liên lạc như mạng điện thoại. Phương pháp chuyển mạch này có hai nhược điểm chính:

+ Hiệu xuất sử dụng đường truyền không cao vì có khi kênh bị bỏ không.

+ Tiêu tốn thời gian cho việc thiết lập kênh cố định giữa hai thực thể.

Mô tả chuyển mạch kênh:



2.2. Mạng chuyển mạch thông báo (Message - Switched - Network)

Các nút của mạng căn cứ vào địa chỉ đích của □*thông báo*□ để chọn nút kế tiếp trên đường dẫn tới đích. Như vậy các nút cần lưu trữ tạm thời và đọc tin nhận được, quản lý việc chuyển tiếp thông báo đi. Tùy thuộc vào điều kiện mạng mà các thông báo khác nhau có thể được gửi trên các con đường khác nhau. Phương pháp chuyển mạch thông báo có những **ưu điểm** sau:

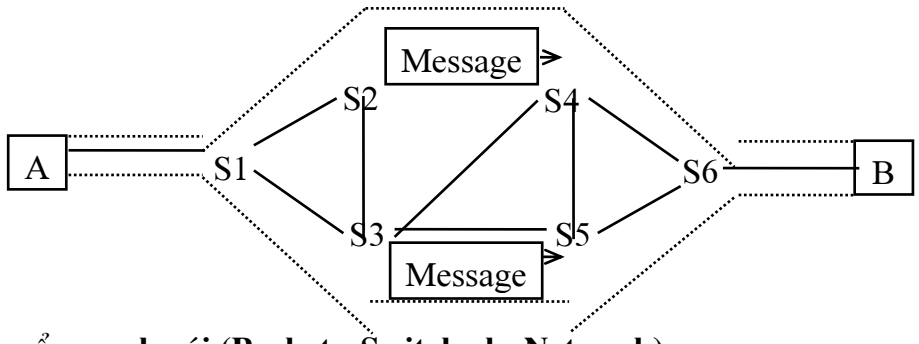
+ Hiệu suất sử dụng đường truyền cao vì không bị chiếm dụng độc quyền mà được phân chia giữa nhiều thực thể.

+ Mỗi nút mạng có thể lưu trữ thông báo cho tới khi kênh truyền rỗi mới chuyển thông báo đi, do đó giảm tình trạng tắc nghẽn trên mạng.

+ Có thể điều khiển truyền tin bằng cách sắp xếp mức độ ưu tiên của các thông báo. Trong mạng chuyển mạch thông báo ta có thể làm tăng hiệu suất sử dụng giải thông của mạng bằng cách gán địa chỉ quảng bá cho các thông báo để gửi nó đồng thời đến nhiều đích khác nhau.

Nhược điểm chủ yếu là trong trường hợp một thông báo dài bi lỗi, phải truyền thông báo này lại nên hiệu suất không cao. Phương pháp này thích hợp với phương pháp truyền thư tín điện tử (*Electronic mail*).

Mô tả:



2.3 Mạng chuyển mạch gói (Packet - Switched - Network)

Trong trường hợp này một thông báo có thể chia ra thành nhiều gói tin (Packet) khác nhau, độ dài khoảng 256 byte, có khuôn dạng quy định. Các gói tin chứa thông tin điều khiển, trong đó có địa chỉ nguồn và địa chỉ đích. Các gói tin của một thông báo có thể gửi đi bằng nhiều đường khác nhau.

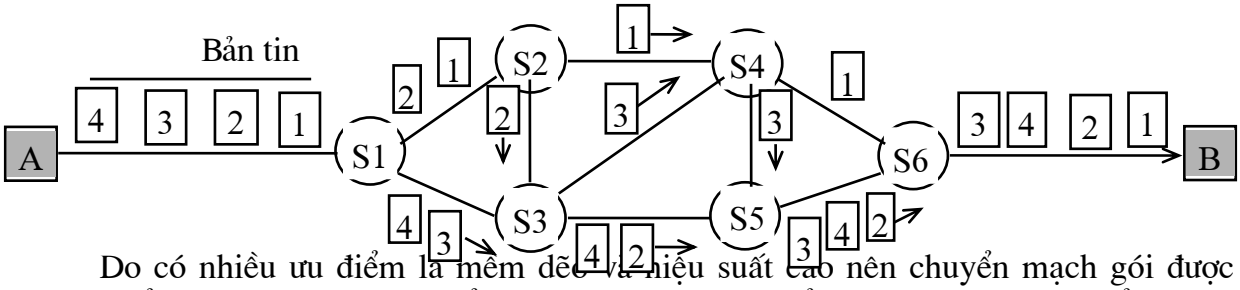
+ Mạng chuyển mạch gói có hiệu suất cao hơn mạng chuyển mạch thông báo vì kích thước của gói tin là hạn chế sao cho các nút mạng có thể xử lý toàn bộ gói tin trong bộ nhớ mà không cần lưu trữ tạm thời trên đĩa, do đó mạng chuyển các gói tin nhanh hơn.

+ Mỗi đường truyền chiếm thời gian rất ngắn vì có thể dùng bất kỳ đường nào để đi đến đích và khả năng đồng bộ bit rất cao. Tuy nhiên

+ Là thời gian truyền tin rất ngắn nên nếu thời gian chuyển mạch lớn thì tốc độ truyền không cao vì nó đòi hỏi thời gian chuyển mạch cực ngắn.

+ Việc tập hợp các gói tin để tạo lại để thông báo là khó khăn, đặc biệt là trong trường hợp các gói được truyền đi theo nhiều đường khác nhau.

Mô tả chuyển mạch gói:



Do có nhiều ưu điểm là mềm dẻo và hiệu suất cao nên chuyển mạch gói được dùng phổ biến hiện nay. Việc tổ hợp hai kỹ thuật chuyển mạch kênh và chuyển mạch

gói trong cùng một mạng thống nhất gọi tắc là **ISDN** (*Intergrated Service digital Network*) đang là xu hướng phát triển hiện nay, đó chính là mạng dịch vụ tích hợpỹ số.

Ngòai ra, có thể phân loại theo cách Khai Thác Dữ Liệu

Nếu xem xét mạng theo góc độ logic (hay kiểu khai thác dữ liệu) thì mạng chia thành hai kiểu.

- Bình đẳng (peer to peer), trong kiểu này các máy tính được nối lại với nhau, máy này có thể sử dụng tài nguyên của các máy kia và ngược lại, không có máy nào được coi là máy chủ.

- Kiểu chủ | khách (server/client) ít nhất một máy gọi là máy chủ (server), đó là máy trên đó có cài đặt các phần mềm hệ điều hành mạng (NETWARE SYSTEM), máy này có chức năng điều khiển và phân chia việc khai thác tài nguyên theo yêu cầu của máy khác.

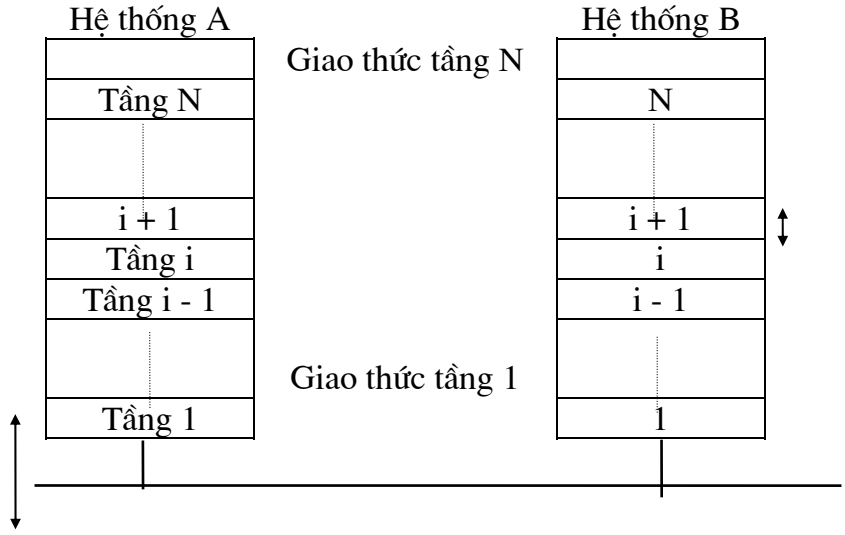
Thuật ngữ CLIENT được dùng để chỉ người khai thác hệ thống mạng. Mỗi người khai thác mạng phải sử dụng một máy tính nào đó có nối với máy chủ để khai thác mạng, người này gọi là client.

IV. KIẾN TRÚC PHÂN TẦNG VÀ MÔ HÌNH OSI

1. Kiến trúc phân tầng

Để giảm phức tạp của việc thiết kế và cài đặt mạng, hầu hết các mạng máy tính đều có phân tích, thiết kế theo quan điểm phân tầng (layering). Sự phân tầng giao thức rất quan trọng vì nó cung cấp sự hiểu biết sâu sắc về các thành phần giao thức khác nhau cần thiết cho mạng và thuận tiện cho vệc thiết kế và cài đặt các phần mềm truyền thống. Mỗi tầng thực hiện một số chức năng xác định và cung cấp một số dịch vụ nhất định cho tầng cao hơn.

Kiến trúc phân tầng tổng quát:



Hình 1-4: Mô hình kiến trúc phân tầng

Mỗi hệ thống trong mạng đều có cấu trúc tầng dựa vào: Số lượng tầng, chức năng mỗi tầng và định nghĩa mối quan hệ giữa 2 tầng đồng mức, giữa 2 tầng kề nhau

Khi ta nghiên cứu hoạt động mạng gồm kết nối Vật lý, giao thức và ứng dụng ta có thể thấy những yếu tố mạng này từ một hệ thống phân cấp các ứng dụng ở trên đỉnh và kết nối ở dưới đáy. Những giao thức cung cấp một cầu nối giữa các ứng dụng và kết nối vật lý. Để hiểu hệ thống phân cấp giữa các yếu tố mạng ta cần một "tiêu chuẩn so sánh" hoặc mô hình xác định những chức năng này. Một mô hình phổ biến nhất là *mô hình OSI*. Một mô hình khác, *mô hình DoD* (Department of Defense), được thiết kế đặc biệt cho việc mô tả các giao thức TCP/IP.

2. Mô hình OSI (Open System Interconnection)

2.1. Chuẩn hóa mạng

Tình trạng không tương thích giữa các mạng, đặc biệt là mạng bán trên thị trường gây trở ngại cho những người sử dụng, tác động đến mức tiêu thụ các sản phẩm về mạng. Do đó, cần xây dụng các mô hình chuẩn làm căn cứ cho các nhà nghiên cứu và thiết kế mạng tạo ra các sản phẩm có tính chất mở về mạng, đưa tới dễ phổ cập, sản xuất và sử dụng ....Hai tổ chức chuẩn chính là ISO và CCITT

ISO (*International Organization for Standardization*) thành lập năm 1946 dưới sự bảo trợ của liên hợp quốc, các thành viên là các cơ quan tiêu chuẩn của các quốc gia. ISO đã xây dựng hơn 500 chuẩn ở tất cả các lĩnh vực. ISO được chia thành các ủy ban kỹ thuật (*Technical Committee - TC)* TC97 đảm bảo lĩnh vực chuẩn hóa xử lý tin. Mỗi TC lại chia thành nhiều tiểu ban (*SubCommitee - SC*) và mỗi SC lại chia thành nhiều nhóm làm việc khác nhau, đảm nhiệm các nhiệm vụ khác nhau.

Các chuẩn do hội đồng ISO ban hành như là các chuẩn quốc tế chính thức.

CCITT tổ chức tư vấn quốc tế về điện tín và điện thoại hoạt động dưới sự bảo trợ của liên hiệp quốc, các thành viên chủ yếu là các cơ quan bưu chính - viễn thông của các quốc gia và tư nhân. CCITT đã đưa ra các khuyến nghị loại V liên quan đến truyền dữ liệu, các khuyến nghị loại X liên quan đến mạng truyền dữ liệu công cộng và loại I dành cho các mạng ISDN.

Ngoài ISO, CCITT trên thế giới còn có các tổ chức khác như ECMA, ANSI, IEEE .... là những tổ chức đã có nhiều đóng góp trong chuẩn hóa mạng. Tổ chức ISO đã đưa ra một số các nguyên tắc chính để xây dựng mô hình 7 tầng là:

- Chỉ thiết lập một lớp khi cần đến 1 cập độ trừu tượng khác nhau.

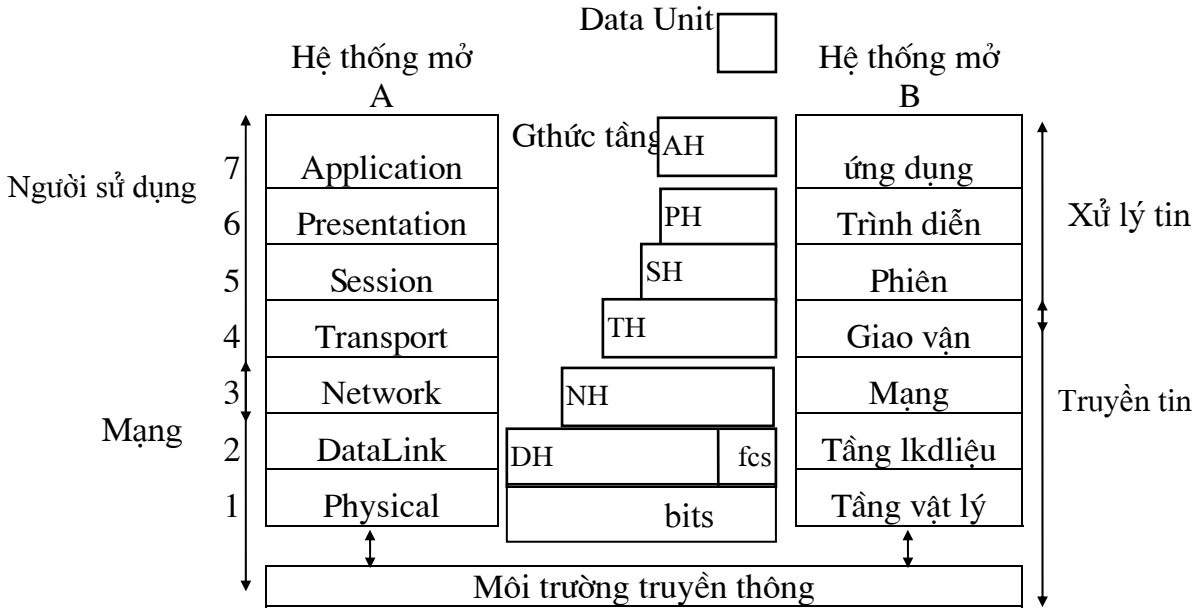
- Mỗi lớp phải thực hiện chức năng rỏ ràng.

- Chức năng của mỗi lớp phải định rỏ những giao thức theo đúng tiêu chuẩn quốc tế.

- Ranh giới các lớp phải giảm tối thiểu lưu lượng thông tin truyền qua giao diện lớp.

- Các chức năng khác nhau phải được xác định trong lớp riêng biệt, song số lượng lớp phải vừa đủ để cấu trúc không trở nên quá phức tạp.

Từ đó chuẩn OSI đưa ra mô hình 7 mức sau:



+ *Sự ghép nối giữa các mức:*

- *Khi máy A gởi* tin đi, các đơn vị dữ liệu đi từ tầng trên xuống dưới. Qua môi trường nó được bổ sung thông tin điều khiển của môi trường.

- *Khi nhận tin*, thông tin từ dưới lên, qua mỗi tầng thông tin điều khiển được tách ra để xử lý gói. Cuối cùng máy nhận B được bản tin của máy phát A

3. Chức năng các lớp của mô hình OSI

- *Lớp vật lý:* Cung cấp phương tiện truyền tin, thủ tục khởi động, duy trì, hủy bỏ các liên kết vật lý cho phép truyền các dòng dữ liệu ở dòng bit. Nói cách khác ở mức Vật lý đảm bảo cho các yêu cầu về thiết bị như máy tính, thiết bị đầu cuối, bus truyền tin...

- *Lớp liên kết dữ liệu :*Thiết lập, duy trì, hủy bỏ các liên kết dữ liệu, kiểm sóat luồng dữ liệu, khắc phục sai sót, cắt hợp dữ liệu.

Ví dụ: Giao thức BSC, SDLC, HDLC, LAPB, LAPD.

- *Lớp mạng:* Định rỏ các thủ tục cho các chức năng như định tuyến, điều khiển độ lưu lượng, thiết lập cuộc gọi và kết thúc các thông tin người sử dụng mạng lưới, xây dựng dựa trên kiểu kết nối từ nút đến nút do lớp liên kết thông tin cung cấp.

Ví dụ: Giao thức IPX ,X.25PLP, IP

- *Lớp vận chuyển:* Định rõ giao thức và các cấp dịch vụ cho thông tin không lời giữa các HOST đi qua mạng con.

Ví du : Giao thức SPX, TCP, UDP.

- *Lớp phiên:* Định rõ thông tin từ quá trình này đến quá trình kia, khôi phục lỗi, đồng bộ phiên. Lớp phiên có nhiệm vụ thiết lập (và hủy bỏ) một kênh thông tin (đối thoại) giữa hai thực thể giao thức lớp ứng dụng đang thông tin trong một giao dịch mạng đầy đủ.

- *Lớp trình bày:* liên quan đến việc biểu diễn (cú pháp) của số liệu khi chuyển đi giữa hai tiến trình ứng dụng đang thông tin. Để có được một kết nối các hệ thống mở

đúng nghĩa, một số dạng cú pháp số liệu trừu tượng phổ biến được định nghĩa để các tiến trình ứng dụng sử dụng cùng với những cú pháp chuyển số liệu có liên quan. Một chức năng khác của lớp trình bày liên quan đến vấn đề an tòan số liệu..

- *Lớp ứng dụng:* Là mức cao nhất của mô hình OSI, cung cấp phương tiện để người sử dụng có thể truy cập được vào môi trường OSI đồng thời cung cấp dịch vụ thông tin phân tán, thông thường là một chương trình/tiến trình ứng dụng - một loạt các dịch vụ thông tin phân tán trên khắp mạng. Các dịch vụ này bao gồm quản lý và truy cập việc chuyển file, các dịch vụ trao đổi thông báo và tài liệu chung như thư tín điện tử.

4. Các giao thức chuẩn ISO

Việc trao đổi thông tin, cho dù là đơn gỉan nhất, cũng đều phải tuân theo những qui tắc nhất định. Do vậy việc truyền tin trên mạng cần phải có những qui tắc, qui ước về nhiều mặt, từ khuôn dạng (cú pháp, ngữ nghĩa) của dữ liệu cho tới các thủ tục gởi, nhận dữ liệu kiểm sóat hiệu quả và chất lượng truyền tin, xử lý các lỗi và sự cố. Các giao thức chuẩn ISO đưa tới cách xây dựng cho giao thức từng tầng.

Trong mạng chuyển mạch gói có thể truyền theo phương pháp:

- Truyền cóù liên kết (connection)

-Truyền không có liên kết (connectionless)

Với các mạng có liên kết các dịch vụ và giao thức ở mỗi tầng trong mô hình OSI phải thực hiện 3 giai đọan theo thứ tự thời gian:

- Thiết lập liên kết.

- Truyền dữ liệu.

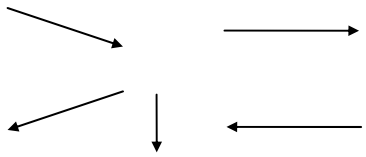
- Hủy bỏ liên kết.

Với các mạng không liên kết thì chỉ có một giai đọan truyền dữ liệu, các gói dữ liệu được truyền độc lập và theo một con đường xác định.

- Trong giai đọan thiết lập liên kết hai thực thể cùng tầng ở hai đầu của liên kết sẽ thương lượng về tập các tham số sử dụng trong giai đọan truyền dữ liệu và trong giai đọan này các cơ chế kiểm sóat bởi luồng dữ liệu, ghép kênh, cắt hợp dữ liệu được thực hiện để tăng cường độ tin cậy và hiệu suất.

Các giao thức chuẩn hóa của ISO đươc xây dựng trên cơ sở 4 hàm nguyên thủy

Ví dụ:	tương ứng
- Request (yêu cầu)	quay số
- Indication (chỉ báo)	chuông đổ
- Response (trả lời)	nhấc máy
- Confirm (xác nhận)	nối



Request được gởi bởi người sử dụng dịch vụ ở tầng N+1 trong hệ thống A để gọi thủ tục của giao thức ở tầng N. Yêu cầu cấu tạo dưới dạng 1 hoặc nhiều đối với dữ liệu của giao thức (PDU) (Protocol data unit) để gởi tới B.

B sẽ thông báo yêu cầu đó lên tầng N+1 bằng hàm indication. Sau đó response được gởi tới từ N+1 của B xuống N để gọi thủ tục giao thức tầng N để trả lời cho A.

5. Các chuẩn hệ thống mở (Open System Standards)

Mô hình tham chiếu ISO chỉ đơn giản là một mô hình cho cấu trúc của một hệ thống con thông tin, nó làm chỗ dựa cho các hoạt động chuẩn hóa liên quan đến từng lớp. Nó không có nghĩa là phải có một giao thức chuẩn cho mỗi lớp. Đúng hơn là mỗi lớp phải có một tập hợp các chuẩn, mỗi chuẩn cung ứng các mức chức năng khác nhau. Như vậy, đối với một môi trường kết nối các hệ thống nhất định, ta phải xác định một tập hợp các chuẩn có chọn lựa để tất cả các hệ thống trong môi trường đó sử dụng.

Ba tổ chức Quốc tế chính tích cực tạo ra các chuẩn cho thông tin máy tính là ISO, IEEE và CCITT. Về cơ bản, ISO và IEEE đưa ra các chuẩn để sử dụng cho các nhà sản xuất máy tính, trong khi đó CCITT định nghĩa các chuẩn dùng cho việc kết nối các thiết bị vào các kiểu mạng công cộng Quốc gia và Quốc tế khác nhau. Tuy nhiên, khi mức độ xen phủ lên nhau giữa công nghiệp máy tính và công nghiệp viễn thông tăng lên thì mức độ cộng tác và mức độ chung nhau giữa các chuẩn được đưa ra bởi các tổ chức này cũng tăng lên.

Ngòai ra, trước và song hành với các hoạt động chuẩn hóa của ISO, Bộ Quốc phòng Mỹ cũng đã nghiên cứu và kết nối mạng trong nhiều năm thông qua cơ quan DARPA (Defense Advanced Research Projects Agency). Kết quả là sự ra đời của mạng được phát triển bởi các tổ chức chính phủ khác. Liên mạng tổ hợp đó hiện nay được gọi đơn giản là Internet.

Bộ giao thức được dùng trong Internet được gọi là TCP/IP (Transmission Control Protocol/Internet Protocol). Nó bao gồm cả các giao thức định hướng mạng và các giao thức hổ trợ ứng dụng. Bởi vì TCP/IP đang được sử dụng rộng rãi với một liên mạng đang tồn tại cho nên rất nhiều giao thức của TCP/IP đã được sử dụng rộng rãi bởi các tổ chức thương mại và các cơ quan Nhà nước để tạo ra các môi trường kết nối hệ thống mở. Do đó trong thực tế có hai chuẩn chính cho hệ thống mở là giao thức TCP/IP và các giao thức dựa trên chuẩn ISO. Bởi vì TCP/IP được phát triển đồng thời với người khởi xướng ISO cho nên nó không chứa các giao thức riêng biệt cho từng lớp của tất cả các lớp ISO. Hơn nữa, phương pháp luận đặc tả dùng trong TCP/IP cũng khác với trong các chuẩn ISO. Tuy nhiên, hầu hết các chức năng của lớp ISO đều có trong bộ giao thức TCP/IP.

Mô hình DoD bao gồm 4 lớp:

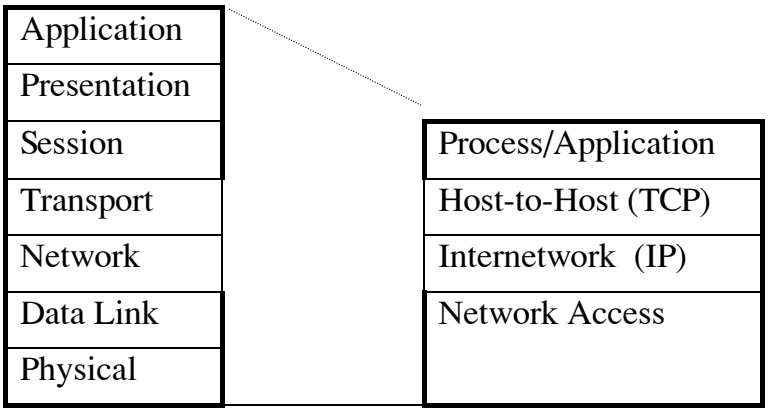
- Lớp dưới cùng là lớp truy cập mạng đại diện cho các bộ phận kết nối Vật lý, giao thức kết nối, giao thức truy cập mạng.

- Lớp IP cung cấp một địa chỉ logic cho giao diện mạng vật lý với giao thức IP.

- Lớp TCP thực hiện kết nối giữa hai máy chủ trên một mạng với giao thức TCP.

- Lớp Tiến trình/ứng dụng đại diện cho giao diện người sử dụng trên chồng giao thức TCP/IP.

Nếu so sánh mô hình OSI với DoD ta thấy chúng tương đồng nhau như hình 1.4.



Hình 1.4: Mô hình OSI và DoD

V. 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, Linux.

VI. XU HƯỚNG PHÁT TRIỂN MẠNG MÁY TÍNH HIỆN NAY

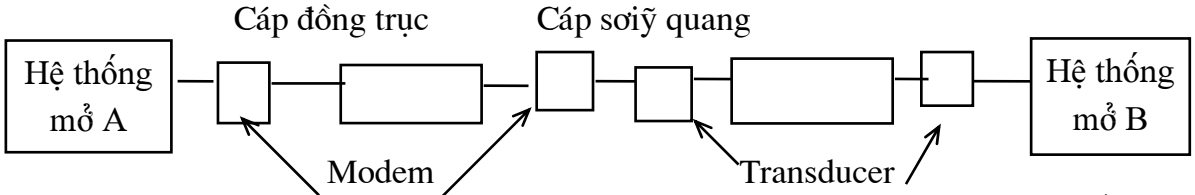
Ngày nay nhu cầu truyền các loại thông tin khác nhau như tiếng nói, hình ảnh, số liệu cùng một lúc trên mạng, nhu cầu truyền thông tin từ một điểm đến nhiều điểm, từ nhiều điểm tới nhiều điểm với tốc độ cao cùng tăng lên mạnh mẽ. Với mạng thông tin hiện tại không còn đáp ứng được các nhu cầu hướng tới truyền thông đa phương tiện (multimedia) bởi tính không mềm dẽo của chúng. Thông tin đa phương tiện vừa là ước mơ vừa là hiện thực của sự phát triển mạng thông tin hiện tại và tương lai. Từ đó ra đời mạng tổ hợp dịch vụ số băng rộng (Broadband Intergrated Server Digital Network: B-ISDN) có khả năng truyền các thông tin liên quan tới nhiều ứng dụng khác nhau như truyền hình số, truyền hình độ phân giải cao, điện thoại truyền hình với chất lượng cao, các dịch vụ hình ảnh, các dịch vụ truyền số liệu tốc độ cao với kiểu truyền không đồng bộ ATM (Asynchronous Transfer Mode).

CHƯƠNG 2
TẦNG VẬT LÝ
I. VAI TRÒ CHỨC NĂNG CỦA TẦNG VẬT LÝ

Tầng vật lý cung cấp các phương tiện điện, cơ, chức năng thủ tục để kích hoạt, duy trì và hủy bỏ kiểu kết Vật lý giữa các hệ thống.

Phương tiện điện liên quan đến sự biểu diễn các bít (mức thể hiện) và tốc độ truyền các bít, đặc tính cơ liên quan đến các tính chất Vật lý của giao diện với một đường truyền (kích thước, cấu hình). Thuộc tính chức năng chỉ ra các chức năng được thực hiện bởi các phần tử của giao điện Vật lý, giữa một hệ thống đường truyền còn thủ tục liên quan đến giao thức điều khiển việc truyền các xâu bít qua đường truyền Vật lý.

Tầng Vật lý là tầng thấp nhất giao điện với đường truyền không có PDU (Protocol Data Unit) cho tầng vật lý, không có phần header chứa thông tin điều khiển,dữ liệu được truyền đi theo dòng bít. Ví dụ một hệ thống đường truyền như sau:



Trong môi trường thực Avà B là hai hệ thống mở được nối với nhau bằng một đoạn cáp đồng trục và một đoạn cáp quang. Modem C để chuyển đổi từ tín hiệu số sang tín hiệu tương tự để truyền trên cáp đồng trục. Modem D lại chuyển đổi tín hiệu tương tự ù thành tín hiệu số và qua Transducer E để chuyển đổi từ xung điện sang xung ánh sáng để truyền qua cáp quang. Cuối cùng Transducer F chuyển đổi xung ánh sáng đó thành xung điện và đi vào B.

Một giao thức tầng Vật lý tồn tại giữa các thực thể đó để quy định về phương thức (đồng bộ, dị bộ) và tốc độ truyền. Điều này mong muốn là giao thức đó độc lập tối đa với đường truyền Vật lý để cho một hệ thống có thể giao diện với nhiều đường truyền Vật lý khác nhau. Các chuẩn cho tầng Vật lý bao gồm các phần tử giao thức giữa các thực thể và đặc tả của giao diện với đường truyền đảm bảo yêu cầu trên.

II. MÔI TRƯỜNG TRUYỀN THÔNG

1. Dây cáp xoắn (Twisted Pair):

Thông thường được dùng trong hệ thống điện thoại. Đôi dây này có thể dùng để truyền tín hiệu analog cũng như digital. Với khoảng cách vài km dùng cáp dây xoắn không cần bộ khuyếch đại.

Với tốc độ truyền mbps (megabit/sec) trong khoảng cách vài km.

2. Cáp đồng trục băng cơ sở (Baseband Cooxial Cable)

Hai loại được dùng rộng rãi là:

- Cáp 50 Ω dùng truyền tín hiệu số.

- Cáp 70 Ω dùng truyền tín hiệu Analog.

Độ rộng băng phụ thuộc đường kích thích lõi cáp, khoảng cách một km tốc độ 10mbps. Cáp đồng trục được sử dụng rộng rãi ở mạng cục bộ và hệ thống điện thoại đường dài.

3. Cáp đồng trục băng rộng (Broadband Cooxial Cable)

Dùng cho truyền tín hiệu Analog và tín hiệu truyền hình. Đó là băng có độ rộng lớn hơn 4khz, chuẩn là Mhz có thể truyền tín hiệu Analog đi xa 100 km.

Để truyền tín hiệu Digital (số) trên mạng Analog (tương tự) cần có bộ biến đổi D/A (Digital/ Analog) và A/D.

Băng cơ sở (Baseband) đơn giản, ghép nối rẻ. Nó cho kênh số đơn giản nối tốc độ 10 Mbps đáp ứng truyền số liệu.

Băng rộng (broadband) cho nhiều kênh nối với kênh 3 Mbsp. Có thể truyền số liệu, tiếng nói, hình ảnh trên cùng một cáp với khoảng cách hơn 100 km.

4. Cáp quang (Fiber Optics)

Nó có nhiều ưu thế: dung lượng truyền cao, giá rẻ. Sợi quang gồm 1 lõi làm bằng thủy tinh rất mỏng không có cấu trúc tinh thể, không dẫn điện, cỡ 1 μm. Bên ngoài được bọc bởi một chất khác có hệ thống chiết quang nhỏ hơn. Aùnh sáng truyền đi trong sợi quang theo hai chế đô (chế độ đơn và đa). Độ suy hao cơ sở 2db/ km - thấp. Aùnh sáng trông thấy có tầng số 10^8 MH z nên độ rông băng của cáp quang rất lớn.

Tốc độ truyền có thể đạt 26 bytes/s trong khoảng 10 - 100 km. Để ứng dụng kỷ thuật cáp quang cần có những bộ biến đổi điện/ quang, quang/điện.

5. Vệ tinh thông tin (Communication Satellites)

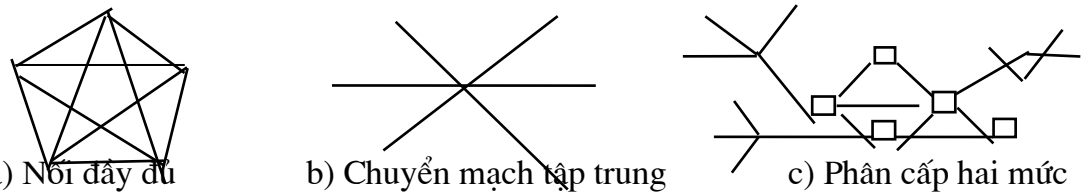
Vệ tinh nhận thông tin từ mặt đất, khuếch đại tín hiệu thu được và phát lại xuống mặt đất ở tầng số khác để tránh Interfakence với tín hiệu thu được. Các vệ tinh có vai trò như những trạm lập thông tin giữa các trạm mặt đất với nhau. Một vệ tinh có thể có rất nhiều trạm mặt đất và nó quét được một vùng rất lớn. Thường vệ tinh hoạt động ở tần số 12 -14 Ghz. Truyền tin qua vệ tinh có dãi truyền rộng bảo đảm chất lượng tin.

III. TRUYỀN TIN TƯƠNG TỰ

1. Hệ thống điện thoại

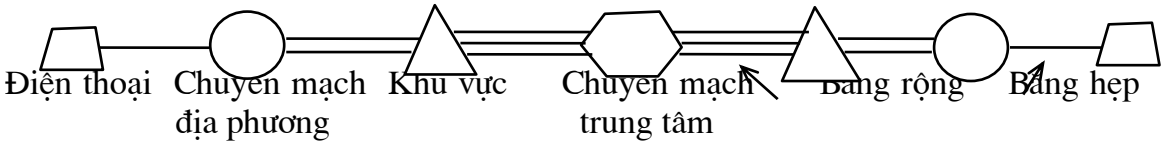
Để truyền số liệu có thể dùng mạng điện thoại hoặc đường truyền riêng có tốc độ cao. Dịch vụ truyền số liệu bằng điện thoại là một trong những dịch vụ đầu tiên về truyến số liệu.

Mạng điện thoại có thể nối đầy đủ, chuyển mạch tập trung hoặc phân cấp 2 mức.



a) Nối đầy đủ b) Chuyển mạch tập trung c) Phân cấp hai mức

Trong thực tế mạng điện thoại tổ chức phân cấp nhiều mức:



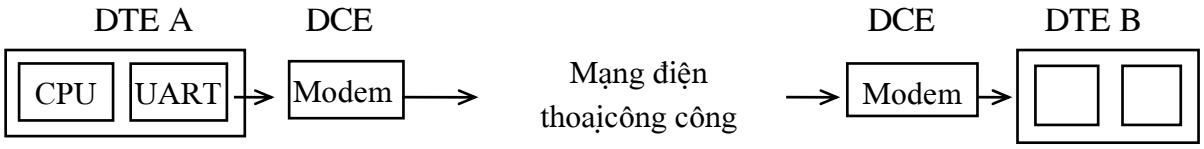
Khi 2 điện thoại cùng mắc vào một chuyển mạch địa phương thì chuyển mạch này sẽ nối 2 điện thoại này với nhau. Nếu hai điện thoại nối vào hai chuyển mạch địa phương khác nhau và hai chuyển mạch này cùng nối với một khu vực thì hai điện thoại được nối qua chuyển mạch địa phương và chuyển mạch khu vực, nếu ở xa nữa thì nó được nối qua chuyển mạch trung tâm.

Phụ thuộc vào dung lượng cần truyền mà ta dùng đôi dây xoắn, cáp đồng trục, hay cáp quang.

2. Modem

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

Sơ đồ đơn giản truyền tin giữa 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 thoại. Tín hiệu này đến Modem ở điểm B được biến đổi ngược lại thành tín hiệu số đưa vào máy tính ở B.

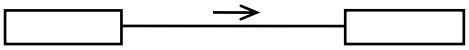
Các kỹ thuật điều chế cơ bản:

- Điều chế biến đổi biên độ (Amplitude Modulation)
- Điều chế tần số (Frequency Modulation)
- Điều chế Pha (Phase Modulation)

Hiện có rất nhiều modem hiện đại từ loại thấp: 300, 600, 1200, 2400bit/s đến loại 9600, 14400, 28800, 56600 bit/s. Với tốc độ truyền tương đối cao trên đường biên hẹp nên đòi hỏi những điều chế phức tạp.

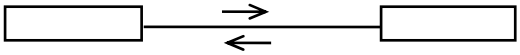
Các phương thức truyền giữa hai điểm có thể làõ:

- Đơn công (Simplex):



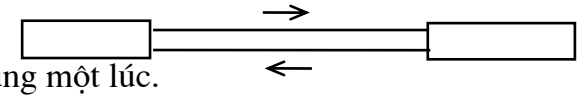
Chỉ cho phép truyền một hướng.

- Bán song công (Haft - duplex):



Có thể truyền theo hai hướng nhưng mỗi thời điểm chỉ truyền một hướng.

- Song công (Duplex):



Có thể nhận hoặc phát cùng một lúc.

Các Modem hiện đại đều có kiểu hoạt động ở hai chế độ song công và bán song công.

3. Chuẩn RS - 232-C

Là chuẩn của EIA (Electrical Industres Association) nhằm định nghĩa giao diện tầng vật lý giữa DTE và DCE (Chẳng hạn một máy và một modem).

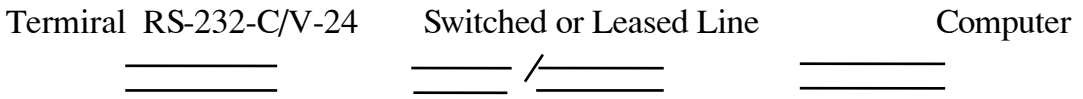
DCE (***Data circuit terminal Equipment***) là thuật ngữ dùng chung chỉ các thiết bị làm nhiệm vụ nối các DTE với các đường truyền thông. Nó có thể là một Modem, Transducer, Multiplexer... hoặc một thiết bị số nào đó (máy tính chẳng hạn trong trường hợp máy tính đó là một nút mạng và DTE được nối với mạng qua nút nối mạng đó). DCE có thể được cài đặt ngay bên trong bên DTE hoặc đứng riêng như một thiết bị độc lập.

DTE (Data Terminal Equipmeut) là thuật ngữ chung cho các máy của người sử dụng cuối có thể là máy tính hoặc một trạng cuối (Terminal). Như vậy tất cả các ứng dụng của người sử dụng (chương trình dữ liệu) đều nằm ở DTE lại cho phép chúng ta phân chia tài nguyên, trao đổi dữ liệu và lưu trữ thông tin dùng chung.

Chuẩn RS 323C đầy đủ gồm 25 đường nhưng phần lớn là các đường đặc biệt và một số đường bỏ không dùng. Các đầu cuối của máy tính đòi hỏi một phần các đường này là đủ hoạt động.

Các chuẩn này sử dụng các đầu nối 25 chân nên về lý thuyết cần dùng cáp 25 sợi để nối DTE với DCE. Về phần điện, chuẩn này qui định các tín hiệu số nhị phân 0 và 1 tương ứng với các tiín hiệu điện nhỏ hơn -3V và lớn hơn +3V. Tốc độ tín hiệu qua giao

diện không vượt quá 20 Kb/s và với khoảng cách dưới 15m, tuy nhiên có thiết kế tốt để đạt được tốc độ và khoảng cách lớn hơn.



Bảng tóm tắt các đặc tả chức năng của mạch (Circuit) quan trọng nhất:

Tên mạch (*)	Hướng	Chức năng
* DATA SIGNALS		
- Transmitted Data (BA)	DTE ⮜ DCE	- Dữ Liệu được tạo bởi DTE
- Received Data (BB)	DCE ⮜ DTE	- Dữ Liệu nhận được bởi DTE
* CONTROL SIGNALS		
- Request to Send (CA)	DTE ⮜ DCE	- DTE muốn truyền dữ liệu
- Clear to Send (CB)	DCE ⮜ DTE	- DCE Sẳn sàng để truyền
- Data set Ready (CC)	DCE ⮜ DTE	- DCE Sẳn sàng làm việc
- Data terminal Ready (CD)	DTE ⮜ DCE	- DTE Sẳn sàng làm việc
- Ring Indicator (CE)	DCE ⮜ DTE	- chỉ ra rằng dce đang nhận một ringing signal trên kênh
- Carrier Dectect (CF)	DCE ⮜ DTE	- Chỉ ra rằng dce đang nhận một carrier signal
- Signal Quality Detector (CG)	DCE ⮜ DTE	- Khẳng định khi có căn cứ để tin rằng dữ liệu nhận được đã bị lỗi
- Data Signal Rate Selector (CH)	DTE ⮜ DCE	- Khẳng định để chọn tốc độ cho dữ liệu
- Data SignalRate Selector (CI)	DCE ⮜ DTE	- Khẳng định để chọn tốc độ cho dữ liệu
* TIMI NO SIGNAL		
- Transmitter Signal Element Tinming (DA)	DTE ⮜ DCE	- clocking signal,các chuyển độ on và off xảy ra ở trung tâm của mỗi phần tử tín hiệu.
- Transmitter Signal Element Timing (DD)	DCE ⮜ DTE	- clocking như trên, liên quan tới mạch ba.
- Flox Signal - Receirer Signal Element (DD)		- clocking như trên, liên quan tới mạch bb.
* GROUND		
- Protective Ground (AA)	NA	- Nối với khung máy và có thể với đất bên ngoài.
- Signal Ground (AB)	NA	- Thiết lập tiếp đất chung cho mọi mạch.

Mỗi chiều có một mạch dữ liệu do vậy có thể chấp nhận phương thức hoạt động hai chiều đồng thời (Full - duplex). Một dây đất được bảo vệ, cách ly, còn lại làm việc như mạch trả lời cho cả hai mạch dữ liệu. Các tín hiêu điều khiển được dùng để định nghĩa các đặc tả thủ tục của chuẩn.

Trong trường hợp truyền theo phương thức đồng bộ (Synchronous) cần phải có tín hiệu đồng bộ để đồng bộ hóa các bit. Hơn nữa, nếu một modem đồng bộ được dùng thì cả hai chức năng điều chế (Modulation) và giải điều chế (Demodulation) đều đòi hỏi một tín hiệu đồng bộ để thực hiện mã và giải mã tín hiệu. Vậy nên, Modem cần cung cấp các đồng hồ gửi và nhận cho các mạch điều khiển giao diện trong các DTE. Trường hợp dùng Modem không đồng bộ (Asynchronous) thì không cần có đồng hồ ở trong Modem.

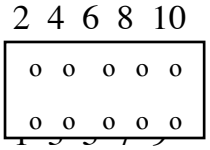
Trong trường hợp đặc biệt, khoảng cách giữa các thiết bị quá gần đến mức cho phép hai DTE có thể truyền trực tiếp tín hiệu cho nhau, lúc đó các mạch RS 232 C vẫn có thể được dùng nhưng không cần có mặt DCE nữa. Trong sơ đồ hoạt động ta đưa vào khái niệm Modem có chức năng liên kết các mạch sao cho các DTE bị đánh lừa là chúng vẫn được nối với Modem.

Đối với PC - AT, PC - XT có hai cổng COM1, COM2 dùng cho trường hợp nối tiếp là:

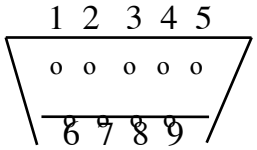
COM 1: Địa chỉ vào/ra 3F8 - 3FF hex, ngắt IRQ4.

COM 2: Địa chỉ vào/ra 2F8 - 3FF hex, ngắt IRQ3.

Các chân cắm ở đây cũng được chuẩn hóa để thuận tiện cho sử dụng:



1 CD (Vào)
2 DSR (Vào)
3 RXD (Vào)
4 RTS (Ra)
5 TXD (Ra)
6 CTS (Vào)
7 DTR (Ra)
8 RI (Vào)
9 GNI



1 CD (Vào)
2 RDX (Vào)
3 TXD (Ra)
4 DTR (Ra)
5 GND
6 DSR (Vào)
7 RTS (Ra)
8 CTS (Vào)
9 RI (Vào)

Thủ tục giao tiếp

Khi có nguồn DTR = 1 (máy tính sẵn sàng), DSR = 1 (Modem sẵn sàng). Modem kiểm tra tín hiệu trên đường dây, nếu có CD = 1. REQUEST TO SEND chỉ rằng TERMIRAL muốn gửi số liệu. CLEAR TO SEND nói lên MODEM chuẩn bị nhận số liệu.

Connection được thiết lập bởi USER quay số gọi máy tính ở xa và đợi trả lời. Nếu máy tính sẵn sàng nối, chuông đổ và nghe trả lời. USER bấm vào DATA - BUTTON, Terminal được nối lên đường dây (DTR = 1) và Modem Local trả lời bằng đặt DSR = 1. Lúc này đèn báo mối nối đã được thiết lập.

Khi có cuộc gọi, Modem ở chổ máy tính reo chuông (RI = 1), giả sử máy tính đã sàng nhận cuộc gọi (DTR = 1), nó trả lời bằng đặt RTS = 1. Điều này có hai hiệu ứng:

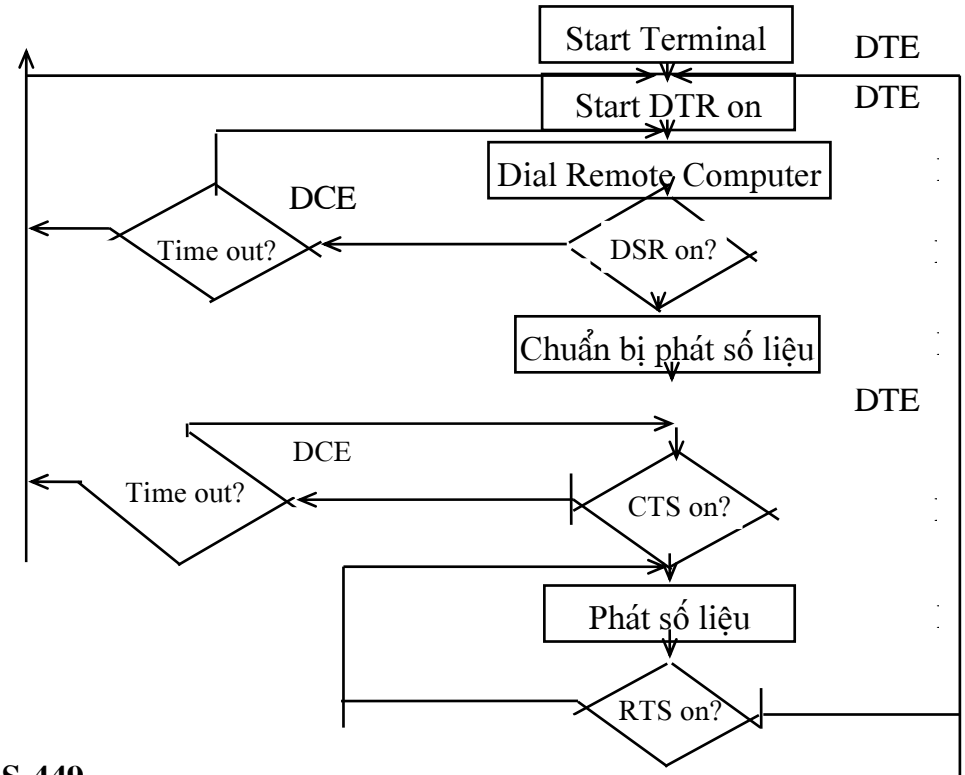
a) Modem gởi tín hiệu CARRIER đến CALLING - MODEM để báo cuộc gọi được chấp nhận.

b) Sau thời gian trể MODEM đặt CTS = 1 để máy tính có thể bắt đầu gởi số liệu. Máy tính gởi lời mời tới TERMIRAL rồi chuẩn bị nhận trả lời của USER, bằng cách đặt RTS OFF. Kết quả TONE - OFF.

Khi CALLING - MODEM kiểm tra thấy mất CARRIER, nó đặt CD - OFF. Termiral đặt RTS = 1 và nhận tín hiệu CTS từ Modem. USER gỏ bản tin trả lời.

Cuối cùng buổi giao dịch đã xong, cả hai tín hiệu sóng mang SWITCHES - OFF và kết thúc cuộc gọi.

Typical Modem Signal Logic:



4. Chuẩn RS-449

Nhược điểm chính của chuẩn RS-232-C là hạn chế về tốc độ và khoảng cách. Để cải thiện nhược điểm đó, EIA đã đưa ra chuẩn mới để thay thế, đó là chuẩn RS-449. Mặc dù chuẩn RS-232C vẫn là chuẩn thông dụng nhất cho giao diện DTE/DCE, nhưng chuẩn RS449 và một số chuẩn khác (RS-442-A và RS-423-A) được áp dụng ngày một rộng rải hơn. RS-449 tương tự như RS-232-C và có thể liên tác với chuẩn củ. Về phương diện chức năng, RS-449 giữ lại toàn bộ các mạch trao đổi của RS-232-C (trừ mạch AA) và thêm vào 10 mạch mới, trong đó có các mạch quan trọng nhất la:ỡ

Termiral in Service (IS), New Signal (NS), Select Frequency (SF), Local Loopback (LL), Remote Loopback (RL), Test mode (TM). Mỗi macỷh có một chức năng riêng và việc truyền tin dựa vào các cặp "tác động - phản ứng". Ví dụ DTE thực hiện Request to send thì sau đó nó lại đợi DCE trả lời với Clear to send.

Về phương diện cơ, RS-449 dùng đầu nối 37 chân cho giao diện cơ bản và dùng một đầu nối 9 chân riêng biệt nếu có kênh phụ. Tuy nhiên, cũng giống như RS - 232 - C, thực tế trong nhiều trường hợp chỉ có một số ít chân được dùng.

Cải tiến chủ yếu của RS-449 so với RS232C là ở các đặc trưng điện, và các chuẩn RS-442-A, RS-423-A, định nghĩa các đặc trưng đó. RS232 được thiết kế ở thời đại của các linh kiện điện tử rời rạc còn các chuẩn này đã tiếp nhận các ưu việt của công nghệ mạch tổ hợp (ISDN). RS-423-A sử dụng phương thức truyền không cân bằng đạt tốc độ 3Kb/s ở khoảng cách 1000 m và 300 Kb/s ở khoảng cách 10 m. RS-442-A sử dụng phương thức truyền cân bằng và có thể đạt tộc độ cao hơn: 100Kb/s ở 1200m và đạt tới 20 Kb/s ỏ khoảng cách 12m. So với tốc độ 20 Kb/s của chuẩn RS232C thì cao hơn rất đáng kể.

IV. TRUYỀN TÍN HIỆU SỐ (DIGITAL TRANSMISSION)

Cùng với tiến bộ của máy tính và điện tử số, các chuyển mạch trung tâm dần dần chuyển sang dùng truyền số (Phát đi các Bit 0 và 1 thay thế các tín hiệu liên tục). Chúng ta xét thấy những ưu việt của truyền số so với truyền tương tự:

Độ tin cậy cao vì chỉ có những giá trị 0 và 1, giảm được lỗi do suy giảm và nhiễu trên đường dây gây ra.

. Tốc độ truyền số liệu cao hơn.

. Thiết bị truyền số dung cho cả điện thoại, số liệu, âm nhạc, hình ảnh.

. Giá máy tính và vì mạch rẻ, nên truyền số rẻ hơn truyền tương tự.

1. Điều chế xung mã -PCM (Pulse Code Modulation)

Khi có cuộc gọi qua chuyển mạch số (Digital End Office), tín hiếu phát ra là tín hiệu Analog. Tín hiệu này được số hóa ở End Office bởi Code, tạo nên số 7 hay 8 bit. Codec là ngược của Modem. Modem đổi dòng bit số thành tín hiệu Analog được điều chế, Codec đổi tín hiệu Analog thành dòng bit số.

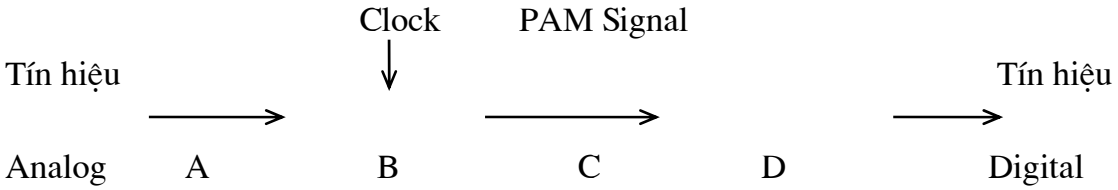
Nguyên lý làm việc của Codec:

Kỹ thuật này được gọi là PMC (Pulse Code Modulation) Codec làm 8000 mẩu/sec ứng với dải băng 4Khz.

Phương pháp đang được dùng rộng rải là TRIBUNAL DESCONOMIE1 carrier của Bell System. T1 Carrier có thể quản lý 24 kênh thoại. Các tín hiệu tương tự được lấy mẩu qua Codec đầu ra là Digital Output.

Tốc độ truyền là 1,554 Mbps, Bell system có thêm các chuẩn T2, T3, T4 ở 6.312, 44.763, 565.148 Mbps.

Nguyên lý điều chế tín hiệu:



Aùp dụng định lý Nyquist cho việc biến đổi tín hiệu Analog và Digital, tần số trích mẩu chỉ cần gấp đôi tấn số của tín hiệu tương tự thì đã khôi phục được tín hiệu tương tự (Analog).

(Giả sử kênh tiếng nói dải tầng 4 Khz thì tần số lấy mẫu là 8 Khz)

Hãng Bell đưa ra đường truyền 24 kênh tiếng nói (T1) mỗi tín hiệu được mã hóa 8 bits.

Chuẩn T2 = 4.T1 = 96 kênh tiếng nói - tốc độ 6.312 Mbít/s.

T3 = 7.T2 = 672 kênh tiếng nói - tốc độ 44.736 Mbít/s

T4 = 6.T3 = 4032 kênh tiếng nói - tốc độ 274.176 Mbít/s.

2. Chuẩn X 21

Đây là chuẩn khuyến nghị loại X21 đặc tả một đầu nối 15 chân với các mạch được chỉ ra trong bảng. Giống như RS-232-C và R-449, nó có một mạch truyền theo cả hai chiều (T và R). Tuy vậy các mạch đó ở đây có thể cung cấp cả dữ liệu người sử dụng lẩn thông tin điều khiển và còn có thêm hai mạch khác (C và I) tương ứng cho mỗi chiều dành cho thông tin điều khiển và trạng thái. Chúng không mang các dữ liệu số mà có thể trạng thái ON hoặc OFF. X-21 được định nghĩa chỉ cho chế độ truyền đồng bộ nên có một mạch đồng bộ bít.

X-21 chấp nhận các chế độ truyền cân bằng và không cân bằng như trong RS-422-A và RS-423-A, do vậy có cùng giới hạn tốc độ/khoảng cách.

Trong nhiều trường hợp chỉ có chế độ cân bằng được sử dung trên tất cả các mạch. Hầu hết các thủ tục định nghĩa cho các mạch X-21 được thực hiện qua một mạng chuyển mạch kênh. X-21 thể hiện tính mềm dẻo, hiệu quả hơn so với RS-232-C và RS-449. Việc sử dụng các chuỗi ký tự điều khiển tạo ra một tập không giới hạn các khả năng tùy chọn dành cho các yêu cầu công nghệ mới.

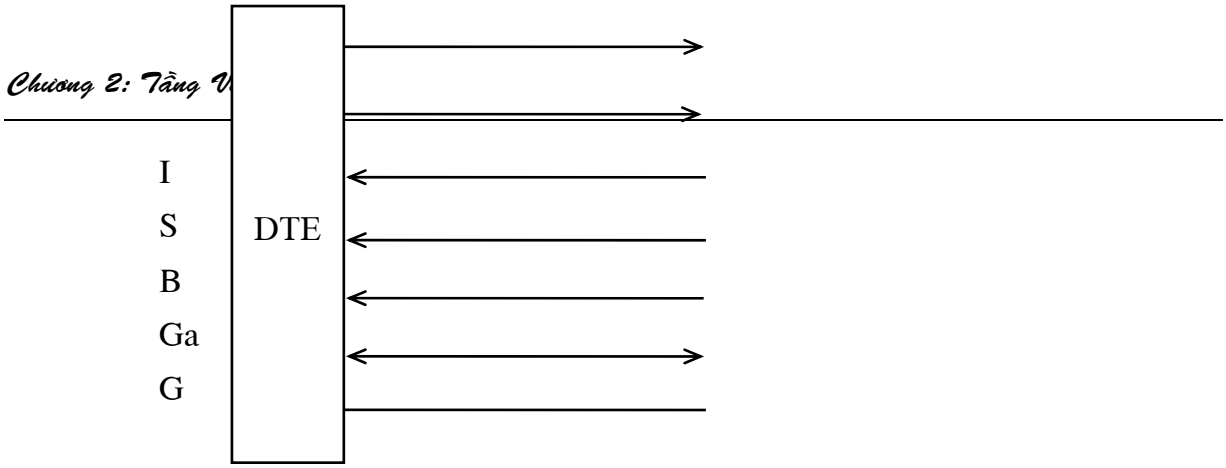
Bảng Định nghĩa mạch X-21:

TêN MạCH	HướNG	CHứC NăNG
Signal Ground (G).	NA	Tín hiệu masse
DTE Common Return (RA).	DTE ⌫ DCE	
Trasnmit (T).		Dùng cảc dử liệu người sử dụng lẩn thông tin điều khiển, phụ thuộc vào trạng thái C và I.
Receiver (R).	DEC ⌫ DTE	Như T cho hướng ngược lại.
Control (C).	DTE ⌫ DCE	Cung cấp thông tin điều khiển tới DCE.
Indication (I).	DCE ⌫ DTE	Cung cấp các chỉ báo cho DTE
Signal Element Tinming (S).	DCE ⌫ DTE	Thực hiện đồng bộ bít.
Byte Tinming (B).	DCE ⌫ DTE	Thực hiện đồng bộ byte.

Mô tả: T

C

R



Ví dụ: dùng X-21:

Bước	C	I	Event in Telephone Analogy	DTE Sends on T	DCE Sends on R
0	off	off	No Connection - Line idle	T = 1	R = 1
1	on	off	DTE Pick up Phone	T = 0	
2	on	off	DCE Gives Dial Tomes		R = “ + ... + “
3	on	off	DTE Dials Phone Number	T = Address	
4	on	off	Remote Phone Rings		R =Call Progress
5	on	on	Remote Phone Pick Up		R = 1
6	on	on	Conversation	T = Delta	R = Delta
7	off	on	DTE Say Goobye	T = 0	R = 0
8	off	off	DCE Say Goobye		R = 0
9	off	off	DCE Hang Up		R = 1
10	off	off	DTE Hangs Up	T = 1	

CHƯƠNG 3

TẦNG LIÊN KẾT DỮ LIỆU

I. VAI TRÒ VÀ CHỨC NĂNG TẦNG LIÊN KẾT DỮ LIỆU

Việc xây dựng giao thức mạng chuẩn để so sánh đối chiếu các giao thức của các mạng rất quan trọng trong việc xác lập cấu hình, gở rối trong mạng và nâng cao chất lượng về mạng. Trên cơ sở của giao thức truyền tin chúng ta nắm được cách thức nhận biết gói tin, kiểm sóat lỗi truyền tin và cơ chế kiểm sóat thông lượng để giải quyết vấn đề tắc nghẽn thông tin trên mạng.

1. Cơ sở nhận biết gói tin

1.1. Khung tin

Lớp Liên kết dữ liệu dựa vào khả năng chuyển tải của lớp Vật lý. Các bít thông tin truyền đi hoặc nhận về đều được nhóm lại thành những đơn vị logic gọi là khung (frame). Trong khung ngoài bit thông tin còn chứa các trường địa chỉ, trường điêfu khiển, trường nhận biết, trường kiểm sóat lỗi.

Tầng 2 tách dòng bit thành Frame và tính checksum cho mỗi frame trước khi truyền, khi có lỗi (error) nó thông báo cho nơi gởi để truyền lại.

1.2. Nhận biết gói tin

Để tách frame người ta đưa ra các phương pháp cơ bản sau:

- *Đếm số ký tự* : phương pháp này ít dùng vì từ đếm cũng bị lỗi khi truyền.

- *Dùng ký tự bắt đầu và kết thúc* STX, ETX thường được dùng trong giao thức hướng ký tự.

- *Dùng cờ (flags) bắt đầu và kết thúc* với bit (01111110) thừơng được dùng trong giao thức hướng bit.

2. Kiểm soát lỗi

- 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 luôn có thể. Các kênh vào ra thường xãy ra lỗi, đặc biệt là ở truyền số liệu. Để kiểm tra lỗi ta có thể:

- *Dùng Timer*, nghĩa là nếu quá thời gian qui định bên gởi không nhận được tín hiệu trả lời, xem như lỗi, phát lại gói tin hỏng.

- *Đánh số Frame gởi đi*, nếu không nhận đúng thứ tự khung là lỗi, yêu cầu phát lại.

- Để kiểm tra thu đúng gói tin gởi đi thường khi phát tin có kèm theo *trường kiểm tra lỗi (FCS)* bằng cách sử dụng các phương pháp sau:

- *Phương pháp bit chẵn lẽ.*
- *Phương pháp mã đa thức.*
- *Phương pháp mã sữa sai dùng nguyên lý cân bằng parity để chỉ ra các bit lỗi.*

Khi điều khiển xử lý tiếp nhận cần phải thực hiện thủ tục điều khiển lỗi tự động bằng cách tính trường lỗi khung tin thu được so với trường lỗi truyền qua nếu đúng thì trả lời *ACK*, nếu sai trả lời *NAK* hoặc bên thu không nhận được tín hiệu ACK sau một thời gian để bên phát truyền lại khung hỏng.

Kiểu điều khiển lỗi này gọi là **yêu cầu lặp lại tự động** (ARQ: Automatic Repeat Request).

3. Điều khiển luồng

Nếu số lượng dữ liệu truyền giữa 2 thiết bị phát và thu là nhỏ thì thiết bị phát có thể phát tức thời. Nếu 2 thiết bị hoạt động tốc độ khác nhau, chúng ta phải điều khiển số liệu ở ngõ vào để ngăn chặng tình trạng tắc nghẽn trong mạng. Trong các mạng chuyển mạch gói (PSN) thường vẫn xảy ra trường hợp lượng tải đưa ra từ bên ngoài vào vượt quá khả năng phục vụ của mạng. Thậm chí đôi khi điều này vẫn xảy ra khi đã sử dụng thuật toán định tuyến tối ưu. Các gói không có chỗ xếp hàng sẽ bị loại bỏ, và tất nhiên sau đó bên thu sẽ yêu cầu truyền lại, dẫn đến việc lãng phí hiệu quả sử dụng mạng. Bên cạnh đó, khi lượng tải áp đặt lớn quá mức sẽ làm giảm tính khả thông của mạng và trễ của gói trở nên rất lớn. Cho nên đôi lúc vẫn phải hạn chế bớt một phần tin truy nhập vào mạng để tránh trường hợp mạng bị quá tải như trên. Đó chính là chức năng của thuật toán điều khiển luồng.

4. Các giao thức liên kết dữ liệu

Kiểm soát lỗi và điều khiển luồng là hai thành phần thiết yếu của giao thức điều khiển liên kết dữ liệu. Để đảm bảo thông tin được trao đổi xuyên qua một liên kết số liệu nối tiếp được tiếp nhận và biên dịch ra một cách chính xác giao thức liên kết dữ liệu định nghĩa những chi tiết sau:

- Khuôn dạng của mẫu số liệu trao đổi.
- Dạng và thứ tự các thông điệp trao đổi.

II. CÁC PHƯƠNG PHÁP KIỂM SOÁT LỖI

Khi dữ liệu truyền giữa hai DTE gặp các hiện tượng điện từ cảm ứng lên đường dây sẽ bị thay đổi. Để xác suất thông tin thu được ở DTE đích giống như thông tin đã truyền từ nguồn cần có biện phấp để kiểm tra lỗi như rau:

-Kiểm soát lỗi hướng tới, trong dữ liệu truyền bổ sung thêm thông tin giúp máy thu thu phát hiện và đảo ngược các bít lỗi để có được thông tin chính xác.

-Kiểm soát lỗi quay lui, trong đó dữ liệu truyền có chứa thêm trường kiểm soát, nếu bên thu phát hiện sai thì yêu cầu bên phát phát lại bản sao.

1. Phương pháp kiểm tra bit chẳn lẻ

Phương pháp thông dụng nhất được dùng để phát hiện các lỗi của bít trong truyền dữ liệu hướng ký tự là phương pháp parity bit. Máy phát sẽ thêm vào mỗi ký tự truyền 1 bit kiểm tra parity đã được tính toán trước khi truyền. Khi tiếp nhận thông tin, máy thu sẽ tính toán tương tự như máy phát và so sánh kết quả, nếu sai sẽ thông báo lỗi. Mạch được dùng để tính toán parity bit cho mỗi ký tự gồm tập các cổng XOR được nối với nhau như là một bộ cộng modulo-2.

2. Phương pháp kiểm tra vòng

Phương pháp này khai thác đặt trưng của các số nhị phân khi dùng phép toán modulo-2. Giả sử M(x) là một số m bit cần truyền, G(x) là đa thức sinh có bậc r (phần tử chia). Ta có các bước thực hiện như sau:

Bước1: Thêm r bit 0 vào cuối xâu bit cần truyền. Xâu ghép có m+r bits, tương ứng với đa thức xrM(x).

Bước 2: Chia modulo-2 xâu bit tương ứng với xrM(x) cho xâu bit tương ứng với G(x.

Bước 3: Lấy số bị chia trong bước 2 trừ (modulo-2) cho số dư.

Kết quả sẽ là xâu bit được truyền đi (xâu gốc ghép với checksum).

Chú ý: Hiện nay có 3 đa thức sinh được xem là chuẩn quốc tế:

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

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

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

III. KIỂM SOÁT LUỒNG

3.1. Chức năng

Cơ chế điều khiển luồng được thiết lập nhằm các mục đích sau:

- Thiết lập sự cân đối giữa việc hạn chế người sử dụng và giữớ trễ truyền tin trung bình ở mức hợp lý .

- Đảm bảo sự công bằng giữa những người sữ dụng khi hạn chế một phần thông tin truy nhập vào mạng

- Duy trì khả thông của mạng ở mức cần thiết và không để xảy ra tình huống "khóa chết" (deadlock) do tràn bộ nhớ đệm (buffer-overflow).

Rõ ràng đối với người sử dụng thì trễ mạng trung bình càng nhỏ càng tốt . Cho nên ta cần phải nhận thức rằng điều khiển luồng không phải làm trễ trung bình cho người sử dụng mạng, nó chỉ đơn thuần chuyển trễ của lớp mạng lên lớp cao hơn. Điều đó có nghĩa là điều khiển luồng bắt các gói đợi ở ngoài mạng chứ không phải bên trong mạng bằng cách hạn chế đầu vào mạng. Chính vì vậy, đôi khi điều khiển luồng không những không làm giảm trễ của mạng mà còn làm tăng nó lên. Người thiết kế mạng khi tính đến vấn đề trễ của người sử dụng có thể giaiớ quyết bằng một trong các phương pháp sau:

Tăng khả năng thông tin của mạng (ví dụ, tăng dung lượng các đường dây dữ liệu...) cải thiện thuật toán tạo tuyến hoặc phải ngăn người sử dụng muốn truy nhập vào mạng khi tình huống tắc nghẽn xảy ra.

Một nguyên nhân làm ảnh hưởng đến trễ trung bình của gói ở trong mạng là việc sử dụng kỹ thuật truyền lặp lại gói. Các gói phải truyền lặp lại do hai nguyên nhân:

- Khi kích thước của hàng trở nên quá dài làm tràn bộ đệm phải hủy một số gói không có

- Khi phúc đáp một số gói trở về quá chậm nên nút nguồn cho rằng các gói này bị mất và lặp lại cho các gói này.

Truyền lặp làm lãng phí hiệu quả sử dụng mạng và làm giảm khả thông của nó, mặc dù đó là kỹ thuật không thể thiếu được để đảm bảo quá trình thông tin chính xác.

3.2. Phân loại

Dựa trên các yêu cầu đối với cơ chế điều khiêớn luồng, người ta đã nghĩ ra hàng loạt các thuật toán giải quyết, tuy nhiên ta có thể phân chúng thành hai nhóm chính:

. *Điều khiển luồng bằng cửa sổ (Window Flow control)*

. *Điều khiển luồng bằng phương pháp điều chỉnh tốc độ vào các gói* (Input - Limiting Flow control)

Các thông số chủ yếu của cửa sổ là độ rộng W[gói] của nó, số thứ tự P(S) của gói cuối cùng vừa được gởi đi và số thứ tự P(R) của gói mới nhận được sau cùng.

Ví dụ: Với w=8, P(R) =2 cho biết số lượng gói đã có ACK là 2, P(S)=6 cho biết số lượng truyền đi trong phạm vi cửa sổ, số gói X còn có thể truyền đi được là :

$$X = W - P(S) = 8 - 6 = 2$$

Số lượng gói đang đợi phúc đáp vào thời điểm này là :

$$Y = P(S) - P(R) = 6 - 2 = 4$$

Trường hợp chúng ta vừa xét gọi là *cửa sổ cố định (Fixed Window),* có nghĩa là cửa sổ sẽ không thay đổi vị trí chừng nào chưa nhận được ACK của gói cuối cùng trong cửa sổ gởi đi. Ta có thể thấy ngay rằng tốc độ truyền sẽ phụ thuộc một phần vào việc nhận đủ các thông tin ACK của cửa sổ.

Để nâng cao hiệu quả truyền, ta có thể sử dụng kỹ thuật *cửa sổ trượt (Sliding Window)* khi ta đặt kích thước cửa sổ là không thay đổi và sau mỗi lần nhận thông tin ACK cho một gói từ bên thu thì cạnh dưới của cửa sổ lại được tự động dịch lên một đơn vị (gói), cho phép gói tiếp theo được vào cửa sổ để truyền, trong trường hợp này đòi hỏi ta phải xác định kích thước tối ưu cho cửa sổ truyền.

ý tưởng cơ bản của chiến lược *cửa sổ trượt* là làm *giảm cường độ luồng tin* đưa vào bên thu khi các phúc đáp bị chậm trễ. Chiến lược này còn cho bên thu một khả năng *khống chế tốc độ bên phát bằng cách cố ý trễ* (chậm gởi các ACK) khi thấy mình không đủ khả năng tiếp nhận các gói đến. Có 2 phương pháp thông dụng để điều khiển luồng:

a. Điều khiển luồng bằng các cửa sổ nút-tới-nút

b. Điều khiển luồng bằng các cửa sổ đầu cuối-tới-đầu cuối

Một câu hỏi có thể đặt ra: "Vậy điều khiển luồng là chức năng của lớp nào trong cấu trúc của mạng chuyển mạch gói ?". Thực tế, cả hai lớp liên kết dữ liệu và mạng đều có cơ chế điều khiển luồng. Ta thấy rằng lớp liên kết dữ liệu phụ trách việc truyền tin trong phạm vi một đường ghép nối dữ liệu, có nghĩa là từ nút nọ tới nút kia, do vậy nó tương ứng với thuật tóan (**a**). Lớp mạng đảm bảo thông tin giữa hai bên sử dụng nên tương ứng là thuật tóan **(b).**

3.3 Điều khiển luồng bằng cửa sổ ở lớp liên kết dữ liệu

3.3.1 Nguyên lý

Kỹ thuật cửa sổ trong lớp liên kết dữ liệu thường được gắn liền với phương thức tự động yêu cầu truyền lặp ARQ trong phần này chúng ta mô tả các *thủ tục kết hợp giữa nguyên lý ARQ với cửa sổ trượt* để thực hiện chức năng điều khiển luồng cần thiết.

Giả thiết rằng các lớp vật lý, liên kết dữ liệu và mạng là các quá trình độc lập có thể trao đổi với nhau thông qua phương thức truyền các gói thông tin qua lại.

Trường hợp đường truyền được coi là song công, và hai DTE A và B đều có thông tin muốn trao đổi với nhau. Như vậy cả A và B đều dùng chung một mạch truyền dữ liệu nhưng theo hai hướng ngược nhau. Nếu chúng ta sử dụng phương thức ARQ trong hệ thống này thì các khung dữ liệu được hòa lẫn với các khung phúc đáp ở cả hai đầu A và B. Bên thu xem xét trường kiểu trong tiếp đầu khung để phân biệt đó là khung dữ liệu hay khung phúc đáp. Nhưng để nâng cao hơn nữa hiệu quả sử dụng mạng, người ta tìm cách tổ hợp hai khung này thành khung chung và khi cần thiết thì cũng có thể tách rời chúng ra được. Việc tổ hợp chúng lại được thực hiện như sau:

Khi bên thu nhận được khung dữ liệu của bên phát, nó không vội vàng gửi trả khung phúc đáp ngay mà hõan lại một thời gian, đợi cho gói dữ liệu tiếp theo được gởi từ trên lớp mạng của nó xuống, nó tạo cho khung gói này và đồng thời gắn luôn cho phúc đáp vào phần cuối của khung mới được tạo ra. Như vậy thực chất có thể nói phúc đáp đã được đi xe không mất tiền, vì bên thu không phải tạo khung cho nó. Kỹ thuật làm trễ phúc đáp để móc nó vào khung dữ liệu tiếp theo gọi là *piggyback*.

Trở lại với kỹ thuật cửa sổ, ta biết rằng các khung gởi đi được đánh số thứ tự từ 0 tới cực đại là 2^n-1 tương ứng với trường n bit. Cả bên phát và bên thu đều sử dụng cửa sổ trượt trong khi trao đổi thông tin, tuy nhiên bên phát có cửa sổ truyền (Sending Windowư) và bên thu cũng có cửa sổ thu (Receiving Window) tương ứng.

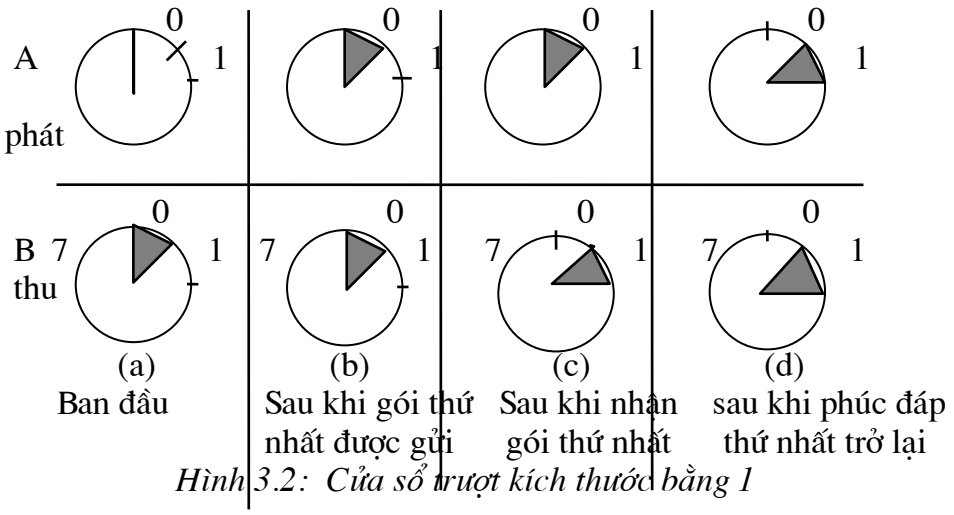
Trong trường hợp tổng quát hai cửa sổ này không nhất thiết phải có cùng chung giá trị cạnh trên và cạnh dưới trong cùng một thời điểm cũng như không nhất thiết phải có cùng chung kích thước. Các số thứ tự trong cửa sổ truyền cho biết số khung đã được gửi đi song chưa có phúc đáp. Do các khung này có thể bị thất lạc hoặc bị hư hỏng trong quá trình lưu thông nên chúng phải được lưu vào trong bộ nhớ của bên phát để khi cần có thể truyền lặp lại.

Như vậy, nếu kích thước lớn nhất của cửa sổ là n thì nó phải có ít nhất **n đệm** nhớ để lưu **n khung** chưa có phúc đáp. Còn ở bên thu, với kích thước cửa sổ là hữu hạn thì khi số lượng khung đến vượt quá giá trị của cửa sổ thì sao?

Cách đơn giản nhất và cũng thông dụng nhất là hủy các khung này và bắt buộc bên phát truyền lặp lại. Khung đến có số thứ tự trùng với cạnh dưới của cửa sổ thu sẽ được chấp nhận, dữ liệu của nó (gói) được chuyển lên lớp mạng và phúc đáp được tạo ra, đồng thời cửa sổ dịch lên một đơn vị. Cửa sổ thu, khác với cửa sổ phát, luôn luôn không đổi về giá trị. Trong quá trình này, bên thu luôn phải nhớ rằng nó phải nhận các khung theo đúng thứ tự mà bên phát truyền lên kênh.

3.3.2 Thủ tục cửa sổ trượt (Sliding Window) có kích thước một bit

Giả thiết rằng bên phát luôn có khung để truyền, nói cách khác là lớp điều khiển dữ liệu luôn có sẵn các gói do lớp mạng cung cấp để thực hiện phép truyền liên tục. Chiến lược *truyền lặp ARQ* được kết hợp với *cửa sổ* để điều khiển số lượng khung lưu thông trên đường truyền giữa A và B. Mô hình ARQ đơn giản nhất là *ARQ dừng - và đợi*, có nghĩa là sau khi bên phát đã truyền đi một khung dữ liệu, nó dừng lại và đợi phúc đáp của bên thu. Nhận được phúc đáp nó mới gửi tiếp khung tiếp theo. Như vậy, ta thấy ngay thực tế đây cũng chính là mô hình cửa sổ trượt với kích thước cửa sổ bằng 1.



Hình 3.2: Cửa sổ trượt kích thước bằng 1

Trao đổi bản tin với cửa sổ 1 bit như sau:

Phần điều khiển gồm seq là số thứ tự phát, ack số thứ tự nhận bản tin, phần điều khiển, số gói tin. Máy A ở tầng 2 nhận gói tin từ tầng 3, tạo bản tin gởi đi. Khi bản tin này đến tầng 2 máy B, nó sẽ tự 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 dịch đi một nấc. Vùng ACK chứa số bản tin cuối đã được nhận không lỗi. Nếu số này trùng với số bản tin vừa gởi, bên phát sẽ lấy gói tin tiếp theo từ tầng mạng. Nếu số không đúng nó phải gởi lại bản tin củ.

Với thuật toán dùng cửa sổ có kích thước bằng 1, một phần lớn thời gian sau khi đã truyền xong một khung A và B phải đợi phản hồi ngược lại mới có thể truyền tiếp được khung khác nên hiệu quả phép truyền không thể cao được.

Để có thể sử dụng kênh hiệu quả hơn cần có các thuật tóan khác với kích thước cửa sổ lớn hơn.

3.3.3 Thủ tục cửa sổ trượt dùng kỹ thuật tạo đường ống(pipelining)

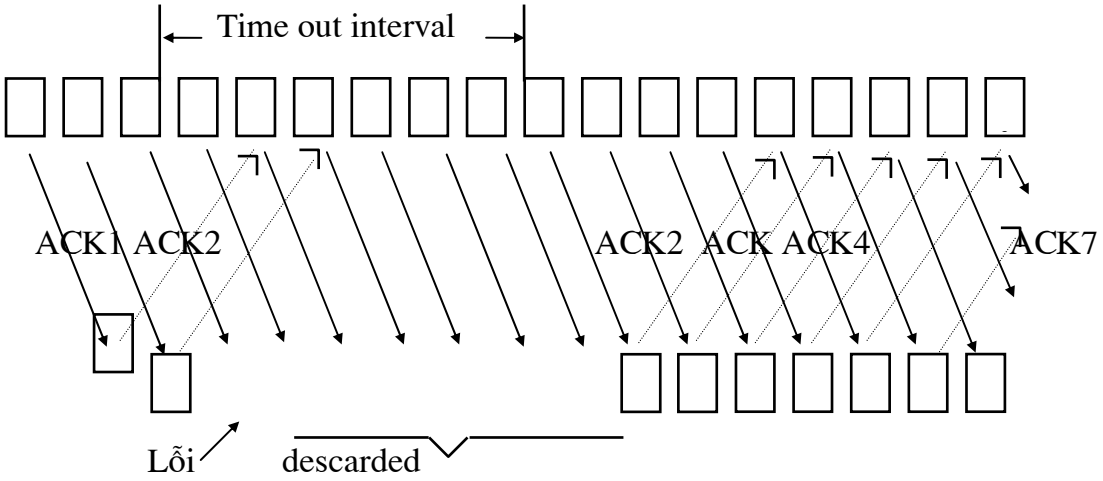
Như ta giới thiệu ở trên, khi thiết lập thủ truyền tin giữa hai DTE ta phải quan tâm tới trễ truyền lan của các gói trên đường truyền để sử dụng kênh một cách có hiệu qủa. Giả thiết dung lượng kênh là b bit/s, kích thước của khung là 1 bit và trễ truyền lan theo đường kín (từ bên phát đến bên thu và ngược lại) là R giây với R/2 giây cho mỗi chiều. Trong thuật tóan sử dụng ARQ dừng và đợi, thời gian đường dây bận là 1/b và thời gian rỗi là R, hiệu dụng của đường dây là 1/(1+bR).

Nếu 1< bR thì độ hiệu dụng không vượt quá 50%, mà trễ truyền lan bao giờ cũng co,ù cho nên ta có thể dùng thuật tóan có kích thước cửa sổ truyền lớn hơn 1. Khi đó người ta nói ta sử dụng tạo đường ống (Pipelinting). Các khung pipelinting khi được truyền lên kênh không tin cậy có thể làm nảy sinh một số vấn đề cần đươc giải quyết.

Nếu một khung nằm giữa luồng trên tuyến bị hỏng hoặc mất thì sao? Khi khung hỏng này đến, bên thu sẽ hủy nó và gởi NAK cho bên phát, nhưng các gói đến tiếp sau đó thì phải làm gì với chúng, trong khi mô hình của chúng ta yêu cầu lớp liên kết dữ liệu thu phải đưa các khung lên lớp mạng theo thứ tự.

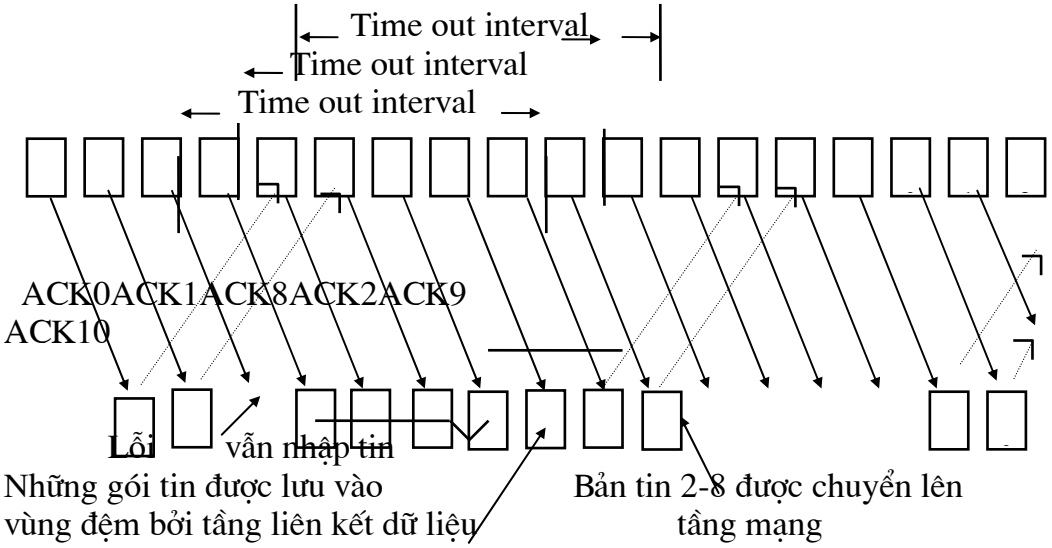
Ta có hai cách giải quyết vấn đề lỗi khi sử dụng pipeline:

Cách thứ nhất, **gọi là ARQ phát lại lại gói N**, bên thu hủy tòan bộ các gói đứng sau khung bị hỏng bằng cách không phúc đáp. Nó tương ứng với trường hợp cửa sổ thu bằng 1. Cuối cùng thì bên phát, sau khỏang thời gian Timeout, sẽ gửi lại cho bên thu tất cả những gói tin chưa được biên nhận bắt đầu từ gói tin hỏng thứ N. Phương pháp này nó có Cách thứ hai, gọi là **ARQ phát lại có chọn lọc**, cho phép bên thu lưu tòan bộ các khung đến nguyên vẹn đến sau khung hỏng trong bộ đệm của mình. Khi bên phát nhận thấy có sự cố, nó chỉ truyền lặp lại khung hỏng mà thôi, còn bên thu nếu nhận được khung này lần thứ hai không có lỗi thì lớp liên kết dữ liệu của nó chỉ việc xếp đặt lại các khung theo thứ tự và gởi các khung tương ứng lên cho lớp mạng.



Những gói tin bị hủy bởi tầng liên kết dữ liệu

Hình 2.4 : Kỹ thuật yêu câu phát lại tự động từ gói tin hỏng thứ N



Hình 2.5: Kỹ thuật yêu cầu phát lại tự động có chọn lọc

Phương pháp này tương ứng với trường hợp cửa sổ thu lớn hơn 1. Tuy nhiên nó cũng đòi hỏi *bộ đệm của lớp liên kết dữ liệu lớn* trong trường hợp cửa *sổ thu có kích thước lớn.*

3.3.4 Đánh giá hiệu quả ARQ phát lại có chọn lọc và ARQ phát lại từ gói N

Hai phương pháp này cho thấy tương phản giữa hiệu dụng của băng dải và dung lượng của bộ đệm lớp liên kết dữ liệu. Tùy theo khả năng và mức độ yêu cầu để sử dụng cách này hay cách khác.

Ngoài ra, do phương pháp kể trên cho phép gởi nhiều gói trong phạm vi cửa sổ nên cũng cần nhiều bộ đếm thời gian để xác định Timeout cho từng gói. Thông số này thường được mô phỏng trong chương trình phần mềm có sử dụng đồng hồ phần cứng để tạo các ngắt theo chu kì.

Phương pháp ARQ phát lại gói tin hỏng thứ N tỏ ra rất hữu hiệu khi tốc độ lỗi là nhỏ, còn khi đường truyền có chất lượng xấu thì nó làm lãng phí rất nhiều băng dải vì các khung đến sau khung hỏng bị hủy và truyền lặp lại, khi đó người ta dùng đến phương pháp có sử dụng *ARQ phát lại có chọn lọc*.

Trong phương pháp này, cửa sổ truyền bắt đầu từ kích thước bằng 0 tăng dần đến MaxSeq, còn cửa sổ thu luôn giữ giá trị bằng MaxSeq không đổi. Máy thu có bộ đệm lưu từng số thứ tự nằm trong giới hạn cửa sổ của nó. ứng với mỗi đệm này là 1 bit đến cho biết là đệm đang trống hay đã bị chiếm. Khi một khung mới đến, số thứ tự của nó được kiểm tra bằng thủ tục between xem nó có nằm trong phạm vi cửa sổ hay không, nếu đúng là khung này không trùng với khung nào khác đến trước thì nó được chấp nhận và lưu vào đệm. Sau khi đã nhận hết tất cả các khung trong phạm vi cửa sổ của mình, lớp liên kết dữ liệu sẽ gởi các gói cho lớp mạng theo đúng thứ tự truyền đi của chúng.

Tuy vậy, việc nhận các khung không theo thứ tự cũng làm nảy sinh một vấn đề cần phải giải quyết: Thí dụ, MaxSeq =7, bên phát gởi các gói từ 0 đến 7 lên kênh, bên thu nhận được đầy đủ và không có lỗi, nó phúc đáp lại cho bên phát và dịch cửa sổ của mình đi cho phép nhận các khung mới, bắt đầu từ khung số 0. Song trên đường trở lại bên phát, sự cố xảy ra, ví dụ dưới dạng sét đánh vào đường dây thoại, làm mất tòan bộ các ack mà bên thu gửi. Bên phát sau khỏang Timeout sẽ truyền lặp lại các khung kể trên, đáng buồn là số thứ tự của chúng lại nằm trong phạm vi cửa sổ thu nên tòan bộ số khung này được chấp nhận. Như vậy là máy thu nhận hai lần cùng một thông tin. Nguyên nhân của việc này là cửa sổ mới cho phép các số thứ tự trùng với cửa sổ trước đó. Để tránh trường hợp kể trên, người ta chỉ cho phép cửa sổ có kích thước lớn nhất là bằng nửa tổng số thứ tự các khung mà thôi, tức là bằng (MaxSeq+1)/2.

Ví dụ, nếu ta dùng 4 bit để đánh số thứ tự thì có thể truyền các khung có số thứ tự từ 0 đến 15, nhưng chỉ có nhiều nhất là 8 khung cùng được truyền lên kênh.

Khi đó, áp dụng cho ví dụ trên, ta thấy bên thu có thể phát hiện ngay được đâu là khung truyền lặp (từ 0 đến 7) và đâu là khung mới (từ 8 đến 15). Trong khi đó số đệm thu vẫn giữ nguyên (bằng8). Khi một khung i tới, nó được đặt trong đệm số i mod 8, mặc dù khung i và khung i+8 sử dụng chung một đệm, song thực tế chúng không bao giờ cùng được nằm trong cùng một cửa sổ.

Trong thuật tóan sử dụng ARQ lùi lại gói N, ta giả thiết là *DTE thu* cũng có thông tin cần phải trao đổi với *DTE phát*, nên các phúc đáp không được gửi ngay mà đợi một thời gian để dùng kỹ thuật piggyback. Nhưng nếu *DTE thu* không có nhu cầu này thì vấn đề được giải quyết ra sao?

Trong thuật tóan dùng ARQ phát lại có chọn lọc, ta dùng thêm thủ tục tính thời gian mà bên thu có thể đợi lớp mạng của mình gửi gói xuống, nếu không có thì nó sẽ tự động tạo ra khung phúc đáp riêng cho khung dữ liệu đã đến để không làm gián đoạn hoạt động chung.

Một cải tiến nữa trong thuật tóan này là việc sử dụng phúc đáp NAK khi bên thu nhận được khung có lỗi, giúp cho bên phát có thể truyền lặp lại nhanh hơn so với việc đợi Timeout. Để trách không gửi nhiều NAK cho cùng một khung có lỗi ta sử dụng cờ NoNak.

Tóm lại, trong quá trình truyền tin trong mạng máy tính việc xãy ra lỗi là không thể tránh khỏi, nó làm giảm tốc độ truyền tin đồng thời nhiều lúc gây tắc nghẽn đường truyền làm mất dữ liệu do đó việc điều chỉnh tốc độ truyền phù hợp là rất cần thiết. Trong bất kỳ hệ mạng nào điều không nằm ngòai những phương pháp điều khiển lỗi và luồng đã khảo sát và đánh gía cụ thể ở phần trên, giúp cho việc truyền tin ngày một nhanh hơn và đáng tin cậy hơn.

IV. CÁC GIAO THỨC ĐIỀU KHIỂN LIÊN KẾT DỮ LIỆU

Lớp điều khiển liên kết số liệu (Data link layer) nghiên cứu các thuật tóan thực hiện thông tin hiệu suất, tin cậy giữa hai máy cạnh nhau ở tầng hai. Cung cấp các phương tiện để truyền thông tin qua liên kết Vật lý đảm bảo tin cậy thông qua cơ chế đồng bộ hóa, kiểm sóat lỗi có thể xãy ra do nhiễu đường dây, sự trễ do lan truyền và kiểm sóat luồng dữ liệu.

Cũng giống như tầng Vật lý có rất nhiều giao thức xây dựng cho tầng liên kết dữ liệu DLP (Data Link Protocol). Các DLP được phân chia thành dị bộ và đồng bộ, trong đó đồng bộ lại chia thành hai nhóm là hướng ký tự và hướng bit.

Các DLP hướng ký tự được xây dựng dựa trên các ký tự đặc biệt của một bộ mã chuẩn nào đó (như ASCII hay EBCDIC) như Kermit. BSC, trong khi các DLP hướng bit lại dùng cấu trúc nhị phân để xây dựng các phần tử của giao thức và khi nhận, dữ liệu sẽ được tiếp nhận lần lược từng bit một như HDLC, LAP-B, LAP-D, SLIP, PPP. Trong phần này chúng ta sẽ khảo sát các giao thức liên kết dữ liệu của tầng hai.

1. Giao thức KERMIT

Đây là lớp giao thức đơn giản nhất do nó chỉ cho phép truyền số liệu một chiều từ một máy tính (DTE) này đến một máy tính khác thông qua liên kết số liệu *point to point* được sử dụng một cách rộng rãi để truyền file. Sự liên kết hay thiết lập kênh thông qua chuyển mạch điện thoại dùng qua Modem

1.1. Khuôn dạng bản tin:

SOH	LEN	SEQ	TYPE	DATA	BCC	CR

Trong đó:

SOH = Đánh dấu bắt đầu một khung
LEN = Số ký tự /bytes trong khung
SEQ = Số thứ tự gửi của khung
TYPE = Kiểu khung được mã hóa dùng cho ký tự đơn

S = Gởi khung mời	B = Kết thúc truyền
F = Tên file	Y = Báo đã nhận
D = File số liệu	N = Không báo nhận
Z = Kết thúc file	E = Lỗi
BCC = Ký tự kiểm tra khối	CR = Đánh dấu kết thúc khối

DATA = Nội dung khung

1.2. Phương thức hoạt động

Máy tính nguồn

User	Kermit
KERMIT CONNETCT SEND {filename} DATA BLOCK[1]SEND DATA BLOCK[2]SEND DATABLOCK[N]SEND END OF FILE EXIT	

Máy tính đích

Kermit	User
	KERMIT CONNECT RECEIVE DATA BLOCK[1] RECEIVE DATA BLOCK[2] RECEIVE DATA BLOCK[N] RECEIVE END OF FILE END OF TRANSMISSION EXIT

Hình 3.1: Trao đổi dữ liệu

Ngòai ra Kermit cho phép dùng để truyền các file giữa hai máy tính cá nhân hoặc giữa máy tính cá nhân và File Server hoặc Mainframe computer. Tuy nhiên cấu trúc truyền file cơ bản là tương tự nhau. Sự khác nhau chính là cách người dùng can thiệp vào máy tính nguồn cho phù hợp thông qua chương trình Kermit đến máy thu ở trạng thái đang hoạt động Header.

Nếu dùng Modem thì một Modem phải được dùng ở chế độ chủ gọi (Mode Originate) và modem khác dùng chế độ bị gọi (Mode Answer). Dĩ nhiên cả hai Modem hoạt động cùng tốc độ baud. Mỗi người sử dụng chạy chương trình Kermit và sau đó vào lệnh CONNECT, kết quả là thiết lập một liên kết vật lý giữa hai hệ thống. Một Sever trong hệ thống muốn nhận một file (hoặc nhiều file) thì vào lệnh RECEIVE và người sử dụng trong hệ thống gởi lệnh SEND theo sau tên file khi đó Kermit trong hệ thống gởi sẽ truyền tòan bộ file. Khi mỗi đọan file được truyền, một thông báo được xuất ra trên màn hình sử dụng. Sau khi tất cả các đọan file được truyền, tất cả người sử dụng thóat khỏi Kermit và trở lại hoạt động hệ thống cục bộ bằng lệnh EXIT.

Có thể thấy rằng Kermit là một giao thức liên kết số liệu không đơn giản vì nó thực hiện thêm một số chức năng như đọc/viết file, chia đọan file và tập hợp file.

Nội dung của file text được gởi tuần tự mỗi khối 80 ký tự, còn file nhị phân được gởi theo từng chuỗi byte 8 bit. Bất kỳ ký tự điều khiển định dạng nào trong nội dung file text hoặc nhị phân - đều được mã hóa trước khi truyền để đảm bảo rằng chúng không ảnh hưởng đến trạng thái thông tin thiết bị trong qúa trình truyền.

Giao thức Kermit khi truyền file máy phát gởi khung thông tin đầu tiên là khung mời S (invitation). Nó gồm một bảng thông số giao thức như chiều dài lớn nhất của khung và khỏang thời gian cho phép để truyền lại. Máy thu báo đã nhận (Y) khung với thông số điều khiển cho phép truyền.

Bên gởi tiến hành truyền nội dung file. Trước tiên là khung đầu file chứa tên file được gởi đi, tiếp theo là tuần tự các khung số liệu (D) chứa nội dung file, sau đó khung

số liệu cuối cùng trong file được gởi đi, bộ phận nhận được báo cho biết bởi việc gởi một khung kết thúc file (Z).

Cơ chế lỗi: Trong quá trình truyền từng khối máy Phát chờ cho đến khi nhận được khung ACK-BCC đúng thì truyền tiếp hoặc khung ACK-BCC sai thì truyền lại. Số thứ tự trong mỗi khung ACK (Y) và NAK (N) mang cùng số thứ tự với khung thông tin được báo đã nhận hoặc không.

Cuối cùng, khi tất cả các file đều được truyền hết, máy Phát (nguồn) gởi một khung kết thúc hoạt động truyền.

2. Giao thức BSC (Binary Synchronous Communication)

BSC là giao thức định hướng ký tự hoạt động ở chế độ bán song công (half-duplex)ỡ và điều khiển việc truyền đồng bộ là giao thức nổi tiếng nhất được IBM phát triển.

2.1. Khuôn dạng bản tin

Để thực hiện những chức năng khác nhau phù hợp với sự quản lý liên kết, các trường điều khiển cần được thêm vào trong những khung thông tin.

Tập ký tự điều khiển:

Ký tự	Chức năng	Ký tự	Chức năng
SOH	Bắt đầu Header	ACK	Ký tự báo cho biết đã nhận số liệu
STX	Bắt đầu tin	NAK	Ký tự báo cho biết chưa nhận số liệu
ETX	Kết thúc tin	DLE	byte chèn trong suốt tin (stuffing)
EOT	Kết thúc truyền tin	SYN	Ký tự đồng bô bản tinỹ
ENQ	Yêu cầu nối	ETB	Ký tự kết thúc đọan tin

Một đơn vị dữ liệu (Frame) dùng trong khung này có khuôn dạng tổng quát như sau:

2.1.1 Dạng khung số liệu

SYN	SYN	SOH	Header	STX	Tin	ETX/ETB	BCC

Hình 3.2 Các định dạng khung/khối của BSC

Trong đó:

- BCC kiểm tra khối đơn là 8 bit để kiểm tra partity theo chiều dọc cho các ký tự thuộc vùng Text, hoặc 16 bit kiểm tra lỗi theo phương pháp CRC-16.

- Để trong suốt bản tin (DataTransparency) dùng ký tự DLE nghĩa là khi phát nếu ký tự phát trùng với DLE thì ta chenỡ thêm DLE và khi thu thì ký tự DLE được bỏ.

-Header: bao gồm địa chỉ nơi nhận, số gói tin, điều khiển , biên nhận ACK

2.2. Hoạt động của giao thức

2.2.1 Cách trao đổi bản tin

Giả sử ta có hai máy A và B cần trao đổi thông tin với cách trao đổi bản tin dựa vào tập ký tự điều khiển như sau:

```
          A                                  B
 Yêu cầu nối          SYN  ENQ -->
                   <--       SYN ACK            Trả lời
 Chuyển số liệu     DLE STX   ...   DLE ETX  -->
```

	<--	SYN ACK	Trả lời đã nhận
Yêu cầu tách		SYN EOT -->	
	<--	SYN ACK	Trả lời kết thúc

***Hình 3.3*. Quá trình hoạt động của BSC**

Đầu tiên A gửi một thông báo điều khiển yêu cầu liên kết. Khi B được chọn sẵn sàng nhận bản tin, nó trả lời với một thông báo điều khiển ACK. Sau đó A gửi bản tin. B tính toán lại thứ tự , kiểm tra parity và chắc chắn truyền không có lỗi thì trả lời ACK cho mỗi khối. Quá tình truyền số liệu xãy ra có thể theo dạng thông thường hoặc dạng hội thoại. Cuối cùng sau khi gửi tòan bộ bản tin, A gửi 1 thông báo điều khiển EOT để kết thúc việc truyền bản tin và xóa đường kết nối logic.

2.2.2 Nhận xét

BSC là giao thức bán song công (half-duplex) hiệu qủa, BSC không thể khai thác sự truyền full- duplex dù có liên kết vật lý phụ trợ. Tuy nhiên trong những năm gần đây có sự thay đổi theo hướng phức tạp hơn và hiệu qủa hơn là *giao thức định hướng bit*. Trong trường hợp mạng máy tính yêu cầu làm việc thông suốt thì giao thức định hướng bit đáp ứng tốt .

3. Giao thức HDLC (Hight Level Data Link Control)

Giao thức định hướng bit là giao thức được dùng phổ biến hiện nay, tất cả các loại dữ liệu có thể được truyền dưới dạng bit nghĩa là phải được giải mã thành các bit trước khi truyền. Tất cả những giao thức định hướng bit đều bắt nguồn từ giao thức HDLC.

Giao thức HDLC là chuẩn quốc tế được ISO đề nghị, dùng cho tất cả liên kết số liệu point to point và mutipoint. Nó hổ trợ cho đường truyền song công, tiền thân của HDLC là giao thức SDLC (điều khiển liên kết số liệu đồng bộ) của IBM. và giao thức điều khiển truyền số liệu cấp cao ADCCP (Advanced Data Communication Control Procedure) của ANSI .

3.1. Khuôn dạng bản tin

3.1.1 Định dạng chuẩn/mở rộng

8	8/16	8/16	O - N	16/32	8
Flag	Address	Control	Information	FCS	Flag

Hình 3.4. Khuôn dạng khung HDLC

Trong đó:

+ Flag: Để nhận biết gói tin dùng cờ bắt đầu và kết thúc :01111110

+ Address: là địa chỉ người nhận.

+ Control: là phần điều khiển.

Không như BSC, HDLC được dùng cho cả số liệu và thông báo điều khiển được thực hiện theo khuôn dạng khung chuẩn. Có 3 loại khung được dùng trong HDLC

I *(Information) khung thông tin :* Mang thông tin thật hoặc số liệu. Các khung I có thể được dùng để mang thông tin ACK liên quan đến luồng khung I trong hướng ngược lại khi liên kết đang được hoạt động trong ABM và ARM.

S *(Supervisor) khung giám sát:* Được dùng để điều khiển luồng và điều khiển lỗi và do đó chứa số thứ tự gởi và nhận, có hiệu lực điều hành sự nối.

N *(Unnumbered) khung không đánh số:* Được dùng cho những chức năng như thiết lập liên kết và xóa kết nối.

3.1.2. Các định nghĩa bit trong trường điều khiển chuẩn

	1	2	3	4	5	6	7	8
Information	O	N(S)			P/F	N(R)		
Supervisor	1	O	S		P/F	N(R)		
Unnumbered	1	1	M		P/F	M		

3.1.3 Các định nghĩa bit trong trường điều khiển mở rộng

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
I	0	N(S)							P/F	N(R)						
S	1	0	S		-				P/F	N(R)						
U	1	1	M		P/F		S		P/F	-						

Hình 3.5. Các kiểu và định dạng khung của HDLC

+ *Information:* là vùng ghi thông tin cần truyền đi. Để không bị dừng khi gặp bit số liệu bằng cờ ta phải dùng thông suốt bản tin bằng cách :

Khi phát tin : Cứ sau 5 con 1 liên tiếp thì thêm một số 0.

Khi thu tin: bit 0 chèn thêm sẽ được hủy bỏ.

+ *FCS (Frame Check Sequence):* Chuỗi kiểm tra dư vòng 16 bit cho tòan bộ nội dung của khung bao quanh giữa hai cờ giới hạn. Thông thường HDLC dùng đa thức sinh CRC-CCITT: $x^{16} + x^{12} + x^5 + 1$

HDLC có 3 chế độ hoạt động:

- Chế độ dị bộ cân bằng (SABM: 1111P1000): được dùng chủ yếu trong những liên kết điểm - điểm, 2 chiều(duplex), trong đó các trạm có vai trò tương đương, giao thức tầng 2 của thủ tục X.25 được xây dựng theo phương thức này của HDLC.

- Chế độ trả lời chuẩn (SNRM: 1100P001): được dùng trong cấu hình không cân bằng.

- Chế độ trả loiĩ dị bộ (SARM: 1111P001): được dùng trong cấu hình không cân bằng. nhưng có nới rộng quyền của trạm tớ nghĩa là cho phép một trạm tớ thiết lập đường truyền mà không cần trạm chủ cho phép. Chế độ này thường dùng cho cấu hình điểm - điểm với liên kết 2 chiều (Duplex) và cho phép trạm tớ gởi những khung không đồng bộ đối với trạm chủ.

Trường S trong khung giám sát được định nghĩa như sau:

00 RR sẵn sàng nhận tin, đã nhận tới N(R)-1

01 REJ yêu cầu phát hay phát lại từ N(R).

10 RNR chưa sẵn sàng nhận, đã nhận tới N(R)-1.

11 SREJ yêu cầu truyền một Frame I duy nhất có số hiệu N(R).

Trường N trong khung không đánh số được dùng để định nghĩa các kiểu khung đặc biệt.

1100 P010 DISC: yêu cầu tách.

1100 P110 UA : đã nhận được lệnh và tiếp nhận sự điều khiển.

1110 F 001 CMDR/FRMR (LAP-B): không tiếp nhận sự điều khiển.

Đối với Frame loại I, có 2 tham số N(S) và N(R) được dùng trong sự liên kết thủ tục điều khiển luồng và điều khiển lỗi có ý nghĩa như sau:

N(S): là số thứ tự của frame I gởi đi.

N(R): chỉ số thứ tự của frame I mà trạm gởi đang chờ để nhận.

Sử dụng 3 bit cho N(S) và N(R) nghĩa là số thứ tự có thể trong khỏang từ 0-7. Tức là cửa sổ gởi lớn nhất có thể chọn là 7. Khuôn dạng mở rộng dùng 7 bit, vì thế làm tăng cửa sổ gởi lớn nhất đến 127.

Bit P/F(poll/final)**:** Bit này có ý nghĩa P nếu đó là frame yêu cầu, và F nếu đó là frame trả lời.

3.1.4. Nhận xét

Nội dung của trường địa chỉ phụ thuộc vào chế độ hoạt động. Trong chế độ SNRM, mỗi trạm tớ được ấn định một địa chỉ duy nhất, nên bất kỳ lúc nào trạm chủ thông tin với một trạm tớ, trường địa chỉ cũng chứa địa chỉ của trạm tớ. Ngoài ra, một địa chỉ quảng bá (Broatcast) cũng có thể được dùng để truyền một khung đến tất cả các trạm tớ trong mạng liên kết.

Trường địa chỉ không được dùng theo cách này trong ABM bởi vì chỉ liên quan đến liên kết điểm - điểm trực tiếp. Thay vào đó, nó được dùng để chỉ hướng của những yêu cầu phù hợp với sự trả lời.

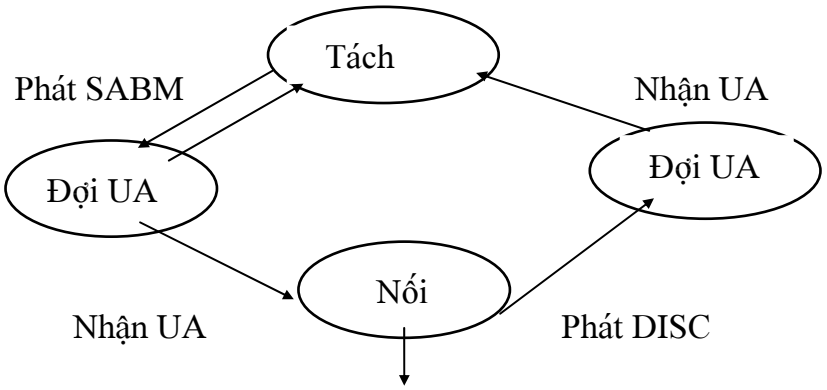
Mặc dù có 4 loại khung giám sát, chỉ có RR và RNR được dùng cho cả SNRM và SABM. Hai khung REJ và SREJ được dùng trong ABM mà cho phép đồng thời hai đường thông tin qua liên kết điểm - điểm. Hai loại khung này được dùng để chỉ đến 1 trạm khác cóỡ một lỗi đã xảy ra, khung I chứa thứ tự N(S) nhận được. Khung SREJ được dùng với thủ tục truyền dẫn lặp lại có lựa chọn, trong khi khung REJ được dùng với thủ tục truyền lại từ khung N.

3.2 Hoạt động của giao thức

Cơ chế vận hành của HDLC xoay quanh hai chức năng cơ bản là *quản lý liên kết và chuyển số liệu* (bao gồm điều khiển luồng và điều khiển lỗi):

3.2.1 Quản lý liên kết

Trước khi truyền một thông tin bất kỳ giữa hai trạm kết nối bằng liên kết điểm - điểm (point to point), một kết nối logic được thiết lập giữa hai bộ phận truyền thông tin. Điều này được thực hiện bằng sự trao đổi hai khung không đánh số, được trình bày hình 3.4. Thủ tục có tác dụng khởi động biến thứ tự ban đầu có trong mỗi trạm. Những biến này được dùng trong thủ tục điều khiển luồng và điều khiển lỗi. Cuối cùng, sau khi truyền tất cả số liệu, gởi khung DISC để xóa liên kết và trả lời với một khung UA. Trong quá trình thiết lập nối tách. nếu quá thời gian qui định thì phát lại hoặc thóat khỏi liên kết.

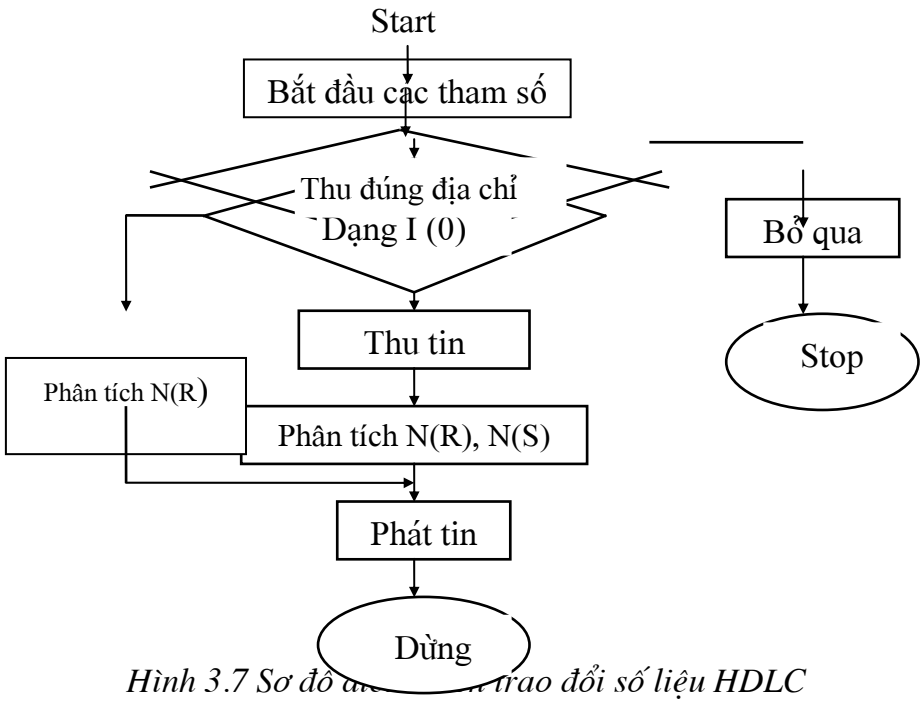


Hình 3.6: Quá trình liên kết

3.2.2 Truyền số liệu

Hai khía cạnh quan trọng nhất trong giai đoạn chuyển số liệu là *điều khiển lỗi và điều khiển luồng*. Điều khiển lỗi dùng thủ tục vận chuyển liên tục sử dụng phương pháp truyền lại từ khung thứ N (*go back N)* hoặc truyền lại chọn lọc (*selective repeat)*, điều khiển luồng dựa trên cơ chế cửa sổ trượt đã được trình bày trong chương 2.

Quá trình thu phát số liệu được minh họa bằng sơ đồ sau:



Hình 3.7 Sơ đồ thuật toán trao đổi số liệu HDLC

Khi mỗi khung I được nhận, cả N(S) và N(R) đều được đọc. Đầu tiên so sánh N(S) với N(R). Nếu chúng bằng nhau tức là khung đúng thứ tự và được chấp nhận. Nếu chúng không bằng nhau, khung sẽ bị hủy bỏ và trở lại khung REJ hoặc khung SREJ. Sau đó N(R) được kiểm tra trong danh sách truyền lại.

3.2.3 Nhận xét

Giao thức HDLC là giao thức chuẩn định hướng bit có kết nối, nó được ứng dụng trong rất nhiều mạng hiện nay và tỏ ra là giao thức hoạt động có hiệu quả trên mạng diện rộng và mạng cục bộ.

Rất nhiều trong số các giao thức hướng bit cho tầng 2 là tập con hoặc cải biên từ HDLC như LAP, LAP-B, LAP-D, SDLC, ADCCP.

4. Giao thức truy cập đường truyền cân bằng LAP-B

LAP-B là một bộ phận của HDLC được dùng để điều khiển việc truyền các khung thông tin qua liên kết số liệu 2 chiều (duplex), điểm - điểm (point to point) để nối một máy tính đến mạng chuyển mạch gói công cộng.

LAP-B nghĩa là phương thức truy cập tuyến có cân bằng, có 2 thủ tục đơn tuyến và đa tuyến giữa DTE và DCE. ở thủ tục đa tuyến nếu một trong các tuyến có sự cố thì các tuyến khác được tuyển dụng mà không bị mất số liệu.

LAP-B được mở rộng của mạng con đầu tiên là thủ tục truy cập liên kết hay LAP(Link Access Procedure).

Máy tính là DTE và tổng đài chuyển mạch gói là DCE. LAPB được dùng để điều khiển việc truyền của những khung thông tin qua giao diện cục bộ DTE-DCE và vì thế nó có ý nghĩa cục bộ.

Khuôn dạng của giao thức LAP-B giống như thủ tục HDLC. Thủ tục điều khiển, LAPB sử dụng chế độ cân bằng không đồng bộ SABM với DTE và DCE và tất cả các khung thông tin được xử lý như những khung lệnh. Tóm tắt những khung sử dụng LAPB như sau:

LAP-B

Kiểu	Lệnh	Đáp ứng
S	RR	RR
	RNR	RNR
	REJ	REJ
U	SABM	UA
	DISC	FRMR
I	I	

Bảng 3.1

Chủ yếu có hai kiểu khung : khung lệnh và khung đáp ứng. Khung đáp ứng được phát để xác nhận công việc thu 1 lệnh. Khung S có thể là khung lệnh hoặc khung đáp ứng.

Các khung S có 3 kiểu RR, RNR, REJ liên quan tới việc điều khiển luồng cho khung I và khắc phục lỗi truyền thông tin do hỏng khung.

Để phân biệt giữa hai trạm, địa chỉ của DTE và DCE được dùng như trên Nghĩa là nếu DCE phát lệnh thì dùng địa chỉ A và DTE phát lệnh thì dùng địa chỉ B.

	Địa chỉ	
Hướng	Lệnh (Commands)	Trả lời (Responses)
DTE DCE	01 Hex (B)	03 Hex (A)

DCE DTE	03 Hex (A)	01 Hex (B)

Bảng 3.2

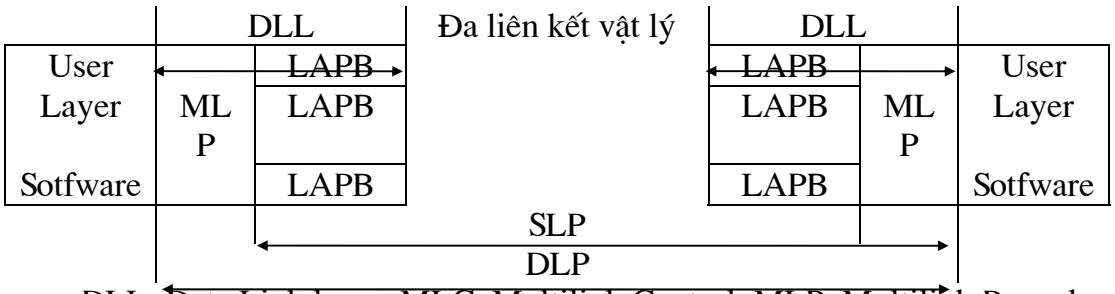
LAP-B hoạt động ở chế độ SABM với số thứ tự gởi và nhận mỗi lần là 3 bit hay cho phép gởi tối đa cửa sổ bằng 7. Tuy nhiên, nếu chọn chế độ mở rộng (SABME), 2 bytes cho trường điều khiển thì số thứ tự gởi và nhận được mở rộng thành 7 bit cho phép cửa sổ lớn hơn nhiều. Khi trường điều khiển có độ dài thay đổi thì nhiều thủ tục của X.25 không trợ giúp cho phương thức làm vệc này.

Những mạch tích hợp có thể thực hiện LAP-B được lập trình trong bộ nhớ. Chúng thường được gọi là mạng X.25 mặc dù chúng chỉ thi hành giao thức LAP-B ở tầng 2 của giao thức X.25 đầy đủ. Tuy nhiên có thể thay đổi những mạch này làm tăng ý nghĩa việc sử dụng LAP-B thêm cho nhiều ứng dụng truyền thông tin từ máy tính đến máy tính.

Do nhu cầu ứng dụng tăng, trong một vài trường hợp đặc biệt, số liệu truyền qua với chỉ một liên kết đơn không có khả năng để đáp ứng những yêu cầu nên phải sử dụng đa liên kết. Vì thế, để cho phép thực hiện điều này việc mở rộng LAP-B gọi là thủ tục đa liên kết hay MLP (Multi Link Protocol)

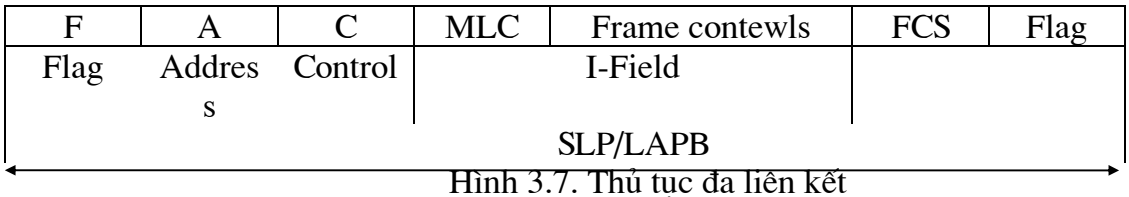
Các vị trí liên quan đến lớp liên kết số liệu

a)



DLL: Data Link layer, MLC: Multilink Control, MLP: Multilink Procedure

b)



Hình 3.7. Thủ tục đa liên kết

a) Các vị trí liên quan đến lớp liên kết số liệu

b) Định dạng khung

Như đã trình bày ở hình 3.7(a), việc chuyển những khung qua mỗi liên kết vật lý được điều khiển bởi thủ tục liên kết đơn riêng biệt theo cách mô tả. Một MLP đơn hoạt động và xử lý giản, tập trung của những biến đổi liên kết để truyền thông tin sử dụng. Điều này có nghĩa là phần mềm ứng dụng không nhận ra đa liên kết vật lý đang được sử dụng.

MLP đơn giản xử lý một tập hợp những thủ tục liên kết đơn như một liên kết chung qua đó để chuyển các khung người sử dụng. Vì vậy nó hoạt động với tập số thứ tự và các thủ tục điều khiển lỗi và luồng độc lập với mỗi thủ tục liên kết đơn

SLP(Simple Link Protocol). Do đó nếu một SLP không hoạt động thì MLP sẽ đánh dấu và truyền lại những khung nhưng có thể giảm các biến liên kết.

Để thực hiện sơ đồ này, MLP thêm vào một trường điều khiển ở đầu mỗi khung một trường điều khiển đa liên kết MLC. SLP xử lý MLC như một trường thông tin và cộng thêm trường địa chỉ (A) và trường điều khiển (C) riêng của nó như ở phần (b) của hình. Cấu trúc điều khiển luồng và cấu trúc điều khiển lỗi trong MLP có tính chất như những cấu trúc đã dùng với LAP-B.

Trường điều khiển đa liên kết gồm hai octets và chứa một chuỗi số 12 bit. Điều này cung cấp 4096 số thứ tự (0-4095) và do đó kích thước cửa sổ lớn nhất là 4095, cho phép nhiều liên kết được sử dụng, hoạt động ở tốc đố số liệu cao. Ví dụ khi hai mạng chuyển mạch gói X.25 đang được kết nối với nhau.

5. Giao thức truy cập liên kết kênh D (LAP-D)

LAP-D là một phần của HDLC dùng cho mạng số đa dịch vụ ISDN. Nó được định nghĩa để điều khiển luồng khung thông tin phù hợp với kênh báo hiệu sau đó được gọi là kênh D, do đó có khái niệm LAPD. Nó cũng được dùng trong dạng mở rộng để điều khiển luồng khung thông tin qua một kênh người sử dụng gắn với một dịch vụ gọi là khung trể.

Hoạt động cơ bản của LAPD và sự liên quan đến HDLC như thế nào.

ISDN giống như PSTN là mạng chuyển mạch - trong thực tế là một đường dẫn ảo phải được thiết lập trước khi bất kỳ thông tin nào được truyền điều này được truyền bằng cách dùng sự phân chia kênh báo hiệu có giao thức khởi tạo riêng mà LAPD là một bộ phận tạo thành. Dịch vụ kết nối định hướng được dùng để truyền cuộc gọi thiết lập giữa một bộ phận của thiết bị sử dụng điện thoại hoặc DTE và một tổng đài địa phương (chuyển mạch cục bộ).

5.1. Khuôn dạng bản tin.

1	Flag(01111110)
2 3	Address (1) Address (2)
4 5	Control (1) Control (2)
	Data
N-2 N-1	FCS (1) FCS (2)
N	Flag(01111110)

+ Flag: là cờ định dạng đầu và cuối khung dùng các bit 01111110

+ Trường địa chỉ có dạng như sau:

EA bit

SAPI	C/R	0
TEI		1

Một trong những đặc điểm chính của LAP-D là cấu trúc trường địa chỉ và khả năng ghép một vài tuyến logic trên cùng một kênh Vật lý. Địa chỉ được gọi là bộ nhận dạng điều khiển truyền số liệu DLCL dài 13 bit, gồm hai dãi con:

TEI: bộ nhận dạng điểm cuối của thiết bị đầu cuối.

SAPI: bộ nhận dạng điểm nhập vào của dịch vụ.

EA: bit mở rộng địa chỉ.

C/R: bit trả lời lệnh để phân biệt khung lệnh và khung trả lời.

+ Trường FCS: sử dụng phương chia đa thức với đa thức sinh $X^{16} + X^{12} + X^5 + 1$

+ Trường điều khiển: xác định loại khung phát đi, giống HDLC có 3 loại I,S,U.

8	7	6	5	4	3	2	1	
N(S)							0	C
N(R)							P	
0	0	0	0	0	0	0	1	C/R
N(R)							P/F	
0	0	0	0	0	1	0	1	C/R
N(R)							P/F	
0	0	0	0	1	0	0	1	C/R
N(R)							P/F	

Khung không đánh số U

SABME	0	1	1	P	1	1	1	1	C
DM	0	0	0	F	1	1	1	1	R
UI	0	0	0	P	0	0	1	1	C
DISC	0	1	0	P	0	0	1	1	C
UA	0	1	1	F	0	0	1	1	R
FRMR	1	0	0	F	0	1	1	1	R

C: Command
R: Response

Hình 3.8. Các định nghĩa bit của trường điều khiển LAPD

Có các thiết bị đầu cuối khác nhau - điện thoại, DTE hoặc hợp nhất cả hai loại - có thể chia ra kênh truy cập cơ bản (cũng là kênh D) giữa những phần liên quan của khách hàng và tổng đài ISDN cục bộ. Tuy nhiên tất cả các thông báo thiết lập cuộc gọi được gởi đến thiết bị đầu cuối bằng cách dùng trường địa chỉ LAPD. Cơ chế của nguyên lý tương tự như cơ chế địa chỉ sử dụng trong Mode NRM ngoại trừ rằng với LAPD không có cấu trúc Bus vật lý và Master đi kèm với thiết bị đầu cuối cho phép mỗi đầu cuối truy cập các Bus trong luồng, cấu trúc chính của mỗi khung LAPD trình bày trong hình 3.8.

Hai Octect được dùng cho trường địa chỉ gồm hai phần địa chỉ con SAPI và TEI (bộ nhận dạng điểm truy cập dịch vụ và bộ nhận dạng điểm kết thúc đầu cuối). SAPI nhận dạng dịch vụ liên quan đến đầu cuối - thoại, số liệu, thoại và số liệu, TEI là nhận dạng đầu cuối duy nhất có trong lớp địa chỉ Broadcast (tất cả đều 1) cho phép gởi một thông báo đến tất cả đầu cuối trong một lớp. Ví dụ cho phép tất cả các điện thoại nhận thông báo yêu cầu thiết lập cuộc gọi đến.

Trong LAPD, việc thêm vào khung không đánh số gọi là UI. LAPD dùng khung này với dịch vụ không kết nối.

6. Giao thức SLIP/PPP

Cùng với sự phát triển rất nhanh của mạng Internet bao gồm rất nhiều liên kết point - to point giữa các mạng LAN hay các trạm đơn lẻ chạy trên nền vật lý khác nhau, sử dụng một số giao thức khác nhau. Một trong những môi trường truyền tương đối phổ biến là môi trường điện thoại công cộng, kết nối các trạm đơn lẻ hay các mạng LAN vào các mạng diện rộng, khai thác chạy trên các ứng dụng của Internet. Để thực hiện điều này, những người phát triển bộ giao thức TCP/IP đã xây dựng các giao thức SLIP và PPP quy định các quy tắc truyền dữ liệu TCP/IP qua môi trường trên.

SLIP (Serial line internet protocol) và PPP (Point to point protocol) cả hai giao thức cung cấp sự kết nối thông qua đường nối tiếp. SLIP và PPP cho phép hai máy tính chuyển đổi thông tin sử dụng cổng nối tiếp thay thế cho cáp Ethernet. Cả hai giao thức này đều sử dụng đường dây thuê bao. Tốc độ truyền chỉ phụ thuộc tốc độ giới hạn của đường truyền (đường dây điện thoại bình thường có thể từ 1.2Kb/sec ≈ 19.2 Kb sec hoặc hơn). Vì hiện nay các modem tốc độ cao có khả năng tự sửa lỗi nên có thể tăng tốc độ truyền một cách đáng kể, cải thiện được chất lượng truyền tin.

Hiện nay, do sự ra đời của các model tốc độ cao có khả năng tự sửa lỗi nên có thể tăng tốc độ truyền một cách đáng kể, cải thiện được chất lượng truyền dữ liệu.

6.1. SLIP (Serial line internet protocol)

Giao thức SLIP cho phép các trạm làm việc độc lập sử dụng TCP/IP nối qua mạng điện thoại, SLIP cung cấp phương pháp đóng khung các gói dữ liệu trước khi truyền qua đường nối tiếp, nó gởi các gói dữ liệu đi theo một dòng byte và sử dụng các ký tự đặc biệt END để đánh dấu các nhóm byte là thuộc về một gói dữ liệu. SLIP khi nhận gói dữ liệu phát hiện ra ký tự END nghĩa là đã nhận toàn bộ gói dữ liệu và gởi lên lớp IP

Các gói IP chuyển xuống được SLIP gói vào trong khung SLIP rất đơn giản mà trong khung không bao gồm bất kỳ địa chỉ, kiểu gói, kiểm tra lỗi hay chức năng lỗi nào và SLIP chỉ cho phép truyền không đồng bộ các dữ liệu. Tuy nhiên, ngày nay đã xuất hiện các modem có khả năng tự kiểm tra sửa chữa lỗi và SLIP có thêm tính năng nén làm tăng hiệu suất truyền dữ liệu được sử dụng nhiều trong việc kết nối các trạm làm việc cô lập, nhưng trong môi trường truyền rộng lớn. (WAN), nó không có nhiều ưu điểm như PPP.

6.2. Giao thức PPP (Point - to - Point - Protocol)

6.2.1. Chức năng

Tương tự như SLIP nhưng nó cung cấp một số tính năng ưu việt hơn SLIP bao gồm kiểm tra, sửa lỗi, khả năng truyền đồng bộ và không đồng bộ. Giao thức PPP cung cấp một phương thức để truyền các gói dữ liệu đa giao thức trên đường kết nối điểm với điểm, và được hỗ trợ bởi các giao thức sau :

- Giao thức điều khiển lớp liên kết DLLP (Data link Layer Protocol). Tương tự HDLC cho phép PPP hoạt động trong các môi trường sử dụng nhiều giao thức lớp mạng khác nhau (HDLC là chuẩn cung cấp dịch vụ truyền dữ liệu tin cậy qua các đường đồng bộ nối tiếp).

- LCP (Link Control Protocol) : giao thức điều khiển liên kết, điều khiển cở gói thông suốt bản tin.

- NCP (Network Control Protocol) : cung cấp thông tin về cấu hình và điều khiển ở lớp mạng như việc gán và quản lý địa chỉ IP, nén hay không nén phần header của TCP/IP và gói dữ liệu IP.

Ngoài ra, PPP còn có những ưu điểm so với SLIP :

- Dịch vụ thiết lập kết nối động để giảm cước điện thoại trong thời gian tạm ngưng.

- Hỗ trợ các đường kết nối tốc độ cao.

- Giao thức PPP hoạt động ở chế độ 2 chiều đồng thời và ngày càng được phát triển trong phần mền mạng hỗ trợ cho phần lớn các trạm làm việc, các bộỹ chọn đường (router), các bộ bắt cầu (bridge). Phương pháp đóng gói PPP cho phép sử dụng các phương thức mạng khác nhau cùng một lúc.

6.2.2. Khuôn dạng PPP

Dạng các khung PPP cùng giống như chuẩn HDLC như sau nhưng có thêm trường Protocol:

Flag	Address	Control	Protocol	Information	FCS	Flag
1	1	1	2		2	byte

trong đó:

Flag: 01111110 : xác định giới hạn khung

Address: Trường địa chỉ là địa chỉ quảng bá (Broadcast)

Control: Vùng điều khiển nhận dạng 1 khung thông tin loại U của HDLC

Protocol: Thường là 2 byte quyết định kiểu gói trong trường thông tin, nếu trường này mang giá trị CO21 thì trường thông tin là các gói giao thức điều khiển liên kết (LCP), nếu là 8021 thì trường thông tin là các gói giao thức điều khiển mạng (NCP), nếu trường này 0021 thì trường thông tin là gói IP Datagram.

FCS: dùng để kiểm tra lỗi trong khung dùng phương pháp kiểm tra độ dư vòng CRC.

Protocol	Kiểu
0021	IP data
C021	LCP data
8021	NCP data

6.2.3. Phương thức hoạt động

Để thiết lập cuộc nối điểm điểm, mỗi trạm của liên kết PPP đầu tiên phải gởi các gói LCP để cấu hình và kiểm tra tầng datalink. Sau đó, các máy có thể có những yêu cầu cụ thể. Tiếp theo gởi NCP cho phép chọn lựa và cấu hình các giao thức lớp mạng (IP, IPX, Appletalk) khi giao thức ở lớp mạng đã được xác định, các ứng dụng thực sự của người dùng sẽ được yêu cầu PPP bắt đầu trao đổi các gói dữ liệu lớp mạng. Kết nối sẽ được duy trì cho đến khi LCP, NCP gởi các gói yêu cầu kết thúc cuộc nối.

CHƯƠNG 4

TẦNG MẠNG

I. VAI TRÒ VÀ CHỨC NĂNG TẦNG MẠNG

Các giao thức tầng mạng được nhiều chuyên gia đánh giá là phức tạp nhất trong các tầng của mô hình OSI. Tầng mạng cung cấp phương tiện để truyền các đơn vị dữ liệu qua mạng, đảm bảo truyền tin end-to-end, bởi vậy nó 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 và chuyển tiếp. Ngoài hai chức năng quan trọng trên tầng mạng cũng thực hiện một số chức năng khác như:

Thiết lập, duy trì và giải phóng các liên kết logic, kiểm soát lỗi, kiểm soát luồng dữ liệu, dồn kênh/phân kênh, cắt/hợp dữ liệu v.v....

II. DỊCH VỤ CUNG CẤP CHO TẦNG MẠNG

1. Phân loại

Có hai loại dịch vu cung cấp cho tầng mạng ỷ:

Dịch vụ truyền tin có liên kết.

Dịch vụ truyền tin không liên kết.

Sự khác nhau giữa hai dịch vụ:

Vấn đề	*Dịch vụ có liên kết*	*Dịch vụ không liên kết.*
Khởi đông kênh	Cần thiết	Không
Địa chỉ đích	Chỉ cần ở lúc khởi động	Cần ở mọi gói tin
Thứ tự gói tin	Được đảm bảo	Không đảm bảo.
Kiểm soát lỗi	ở tầng mạn	ở tầng Giao Vận
Điều khiển thông lượng	ở tầng mạng	ở tầng Giao Vận.
Thảo luận tham số	Có	Không
Nhận dạng liên kết	Có	Không.

Cũng như đối với các tầng khác trong mô hình OSI, ngoài các giao thức ISO còn định nghĩa các dịch vụ mà tầng mạng cung cấp cho các thực thể ở tầng trên dưới dạng một tập các hàm dịch vụ nguyên thủy.

Chú ý:

- Các dịch vụ phải độc lập với công nghệ dùng trong mạng.
- Tầng Giao Vận phải độc lập với một số, loại và cấu hình mạng.

- Các địa chỉ mạng phải thống nhất để tầng Giao Vận có thể dùng cả mạng LAN và WAN.

2. Các hàm cơ bản của dịch vụ trường hợp có liên kết

N-connect.request (callce, caller, acks_wanted, exp_wanted, qos, uses_data).

N-connect.indication (callce,caller,acks_wanted, exp_wanted, qos, uses_data).

N-connect.response (responder, acks_wanted, exp_wanted, qos, uses_data).

N-connect.confirmation (responder,acks_wanted,exp_wanted, qos, uses_data)

N-disconnect.request (responder, acks_wanted, exp_wanted, qos, uses_data)

N-disconnect.indication (originator, reason, user_data, responding_address).

N-data.request (user_data).

N-data.indication (user_data).

N-data-acknowledge.request().

N-data-acknowledge.indication().

N-expedited-data.request (user_data).

N-expedited-data.indication (user_data).

N-reset.request (originator, reason).

N-rest.indication (originator, reason).

N-reset.response().

N-reset.confirm().

3. Các hàm cơ bản của dịch vụ trường hợp không liên kết

Ngoài dịch vụ và giao thức chuẩn cho tầng mạng trong trường hợp có liên kết, ISO cũng đã định nghĩa các dịch cụ và giao thức cho tầng mạng trong trường hợp không liên kết .

*** Về dịch vụ:** chỉ có Primitives được định nghĩa, đó là:

N-Unitdata.request (source address, Destination address, Quality of service, Ns-User data).

N-Unitdata.indication (source address, Destination address, Quality of service, Ns-User data).

Trong đó "Source address" và "Destination address" là các địa chỉ liên mạng toàn cục định danh một cách duy nhất các hệ thống cuối. "Quality of Service" bao gồm một tập các tham số đó là:

Transit delay: Chỉ thời gian trễ cần thiết giữa một N-UnitData.request và N-UnitData.indication tương ứng.

Protection: Bảo vệ tránh các truy nhập bất hợp pháp.

Cost Determinants: Cho phép người sử dụng chỉ rỏ tính chất của giá cước phương tiện được sử dụng (rẻ nhất hoặc đắt nhất chấp được).

Residual Error Probability: Chỉ ra xác xuất một NSDU có thể bị mất, bị trùng lập hoặc bị lỗi khi nhận.

Priority: Độ ưu tiên đối với mỗi NSDU, đặc biệt khi cần loại bỏ chúng để phục hồi các tài nguyên.

Ví dụ: ***Về giao thức*** ISO công bố chuẩn IP để cung cấp các dịch vụ mạng không liên kết và cung cấp khả năng nối kết liên mạng.

III. TỔ CHỨC CÁC KÊNH TRUYỀN TIN TRONG MẠNG

Trong ngữ cảnh của tầng mạng, hoạt động trong mạng ta có hai khái niệm:

Kênh ảo: 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 sẽ được truyền cũng tương tự trong mạng điện thoại cho đến khi liên kết bị hủy.

Datagram: Tương đương với điện báo sử dụng trong mạng không liên kết. Trong mạng Datagram, không có một tuyến đường nào được thiết lập. Các gói tin có thể đi theo các đường khác nhau không nhất thiết phải theo một trình tự nhất định. Datagram phức tạp về điều khiển, nhưng nếu kênh hỏng thì dễ dàng đi theo kênh khác. Vấn đề tắc nghẽn dữ liệu dễ dàng giải quyết hơn.

Vấn đề	Mạng Datagram	Mạng kênh ảo
Khởi động kênh	Không.	Cần thiết.
Địa chỉ hóa	Gói tin phải có đ/c nguồn và đ/c đích.	Gói tin chỉ cần số của kênh ảo.
Thông tin tìm đường	Không cần bất cứ thông tin nào.	Mỗi kênh ảo cần 1 vùng trong bảng.
Roudage	Mỗi gói tin tìm đường đi độc lập.	Được thiết lập khi khởi động kênh.
Điều khiển	Chỉ mất gói tin ở nút hỏng.	Kênh ảo đi qua nút hỏng sẽ bị hủy.
Hậu quả của hỏng nút	Khó khắc phục.	Dễ khắc phucỷ hơn.
Độ phức tạp	Trong tầng Giao Vận.	Trong tầng mạng.
Thích hợp	Các dịch vụ liên kết và không liên kết.	Các dịch vụ liên kết.

Tổ chức kênh ảo: Một nút mạng chứa một bảng, với cửa vào cho một kênh ảo. Khi một liên kết được khởi động, một kênh ảo chưa dùng sẽ được chọn.

Một 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 có kênh ảo 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.

Ví dụ:

- Mạng có 6 nút. Có 8 kênh ảo. Bảng của một nút có hai phần vào và ra.

- Khi gói tin đến, nút mạng sẽ tìm trong bên trái bảng tên nút đưa gói tin đến và tên kênh ảo.

- Bên phải của bảng sẽ chứa kênh ảo và nút mạng mà gói tin sẽ được gói tin được gửi tiếp. Số kênh ảo mới sẽ được thay thế số kênh cũ trong gói tin.

- Khi một trạm muốn thiết lập một kênh ảo mới, nó phải chọn số kênh ảo thấp nhất chưa dùng

- Nút mạng sẽ tham khảo bảng. Trong bảng chứa tất cả các kênh đang dùng, hướng về nút tiếp theo, nút sẽ chọn số thấp nhất còn rỗi chưa dùng và thay vào số kênh của gói tin.

IV. CÁC KỸ THUẬT ĐỊNH ĐƯỜNG TRONG TẦNG MẠNG:

1. Tổng quan về định đường

Chức năng quan trọng nhất của tầng mạng là dẫn đường cho các gói tin từ trạm nguồn đến trạm đích. Trong hầu hết các mạng con các gói yêu cầu đa bước nhảy (*multiple hops*) để tạo nên chuyến đi (trừ các mạng quảng bá). Tuy nhiên trong mạng quảng bá, nếu nguồn và đích cùng ở tren cùng một mạng thì việc định đường cũng được đặt ra. Như vậy kỹ thuật định đường và cấu trúc dữ liệu mà chúng sử dụng là phạm vi chủ yếu của thiết kế mạng.

Kỹ thuật định đường (*theo nghĩa bao gồm cả thuật toán định đường, các tiêu chuẩn thực hiện và sự cập nhật thông tin*) là một phần của phần mềm lớp mạng có nhiệm vụ quyết định chọn một đường ra mà gói tin sẽ được truyền trên đó.

Thuật toán tìm đường đi là quy trình để quyết định chọn đường ra khỏi nút mạng nhằm gửi gói tin đi tới nút khác.

+ Nếu mạng con sử dụng kênh ảo nội thì các quyết định định đường được tạo ra khi một kênh ảo mới được thiết lập. Sau đó các gói dữ liệu chỉ đi theo một đường đã được thiết lập và định đường này gọi là định đường phiên.

+ Nếu một mạng con sử dụng các gói tin nội (Datagram) thì quyết định định đường phải được tạo thêm một lần nữa khi các gói dữ liệu đến, bởi vì tuyến đường tốt nhất có thể đã thay đổi kể từ khi cập nhật lần cuối cùng.

2 Yêu cầu kỹ thuật chọn đường

Chọn đường là sự lựa chọn một con đường để truyền một đơn vị dữ liệu (một gói tin chẳng hạn) từ trạm nguồn đến trạm đích của nó. Một kỹ thuật chọn đường do vậy phải thực hiện 2 chức năng sau đây:

1. Quyết định chọn đường, những tiêu chuẩn (tối ưu) nào đó.

2. Cập nhập thông tin chọn đường khác nhau, tức là thông tin dùng cho chức năng 1.

Có rất nhiều kỹ thuật chọn đường khác nhau. Sự phân biệt giữa chúng chủ yếu căn cứ vào các yếu tố liên quan đến 2 chức năng trên.

Các yếu tố đó thường là:

a. Sự phân tán của các chức năng chọn đường trên các nút của mạng.

b. Sự thích nghi với trạng thái hiện hành của mạng.

c. Các tiêu chuẩn (tối ưu) để chọn đường.

Dựa trên yếu tố (a) ta có kỹ thuật chọn đường Tập trung hoặc Phân tán. Dựa trên yếu tố (b) ta có kỹ thuật chọn tĩnh hoặc thích nghi.

Cuối cùng, các kỹ thuật chọn đường cùng loại lại có thể phân biệt bởi yếu tố (c). Tiêu chuẩn (tối ưu) để chọn đường được xác định bởi người quản lý hoặc người thiết kế mạng, nó có thể là:

- Độ trễ trung bình của việc truyền gói tin.

- Số lượng nút trung gian giữa nguồn và đích của gói tin.

- Độ an toàn của việc truyền tin.

- Cước phí truyền tin.

Việc chọn tiêu chuẩn (tối ưu) như vậy phụ thuộc vào nhiều bối cảnh mạng (thông lượng, mục đích sử dụng ....). Các tiêu chuẩn có thể thay đổi vì bối cảnh mạng cũng có thể thay đổi theo thời gian.

3. Kỹ thuật chọn đường tập trung và kỹ thuật chọn đường phân tán

Để thực hiện việc định đường các gói tin trong mạng máy tính, người ta đã đưa ra nhiều kỹ thuật định đường. Các kỹ thuật này có những đặc điểm, tính chất, mục đích sử dụng có thể giống nhau hoặc khác nhau và người ta tìm cách phân loại chúng. Trong quá trình phát triển của mạng máy tính một số kỹ thuật định đường mới ra đời đồng thời những kỹ thuật cũ cũng được cải tiến, do đó tùy theo thời gian, tùy theo quan điểm đánh giá mà người ta phân loại chúng khác nhau như:

+ Định đường tập trung hay định đường phân tán

+ Định đường tĩnh hay định đường thích nghi.

Qua đó chúng ta thấy sự so sánh, phân loại và đánh giá các kỹ thuật định đường là một công việc khó khăn và có tính chất tương đối. Chẳng hạn định đường Flooding là một kỹ thuật định đường tỉnh nhưng khi trong mạng có một vài Router hỏng hoặc hồi phục trở lại thì việc định đường vẫn thực hiện được, các gói tin vẫn đi đến đích. Như vậy Flooding có khả năng thích nghi khi với sự thay đổi hình trạng mạng (giống kỹ thuật định đường thích nghi).

Mặt khác nếu dựa vào tiêu chuẩn thực hiện thì có nhiều tiêu chuẩn khác nhau: Giá liên kết, độ trể thời gian, khoản cách địa lý, số các hop, ...

3.1 Kỹ thuật chọn đường tập trung

Được đặc trưng bởi sự tồn tại của một (hoặc vài) trung tâm điều khiển mạng thực hiện việc chọn đường sau đó gửi các bảng chọn đường tới tất cả các nút dọc theo con đường đã được chọn đó. Trong trường hợp này, thông tin tổng thể của mạng cần dùng cho việc chọn đường chỉ được cất giữ tại trung tâm điều khiển mạng. Các nút mạng có thể không gữi bất cứ thông tin nào về trạng thái của chúng tới trung tâm, hoặc gữi theo định kỳ, hoặc chỉ gữi khi xảy ra một sự kiện nào đó. Trung tâm điều khiển sẽ cập nhập các bảng chọn đường dựa trên các thông tin nhận được đó.

3.2 Kỹ thuật chọn đường phân tán

Trong kỹ thuật này không tồn tại các trung tâm điều khiển. Quyết định chọn đường được thực hiện tại mỗi nút của mạng. Điều này đòi hỏi việc trao đổi thông tin giữa các nút, tùy theo mức độ thích nghi của giải thuật được sử dụng.

4. Kỹ thuật chọn đường thích nghi và chọn đường không thích nghi

4.1 Kỹ thuật chọn đường không thích nghi (hay còn gọi tĩnh)

Trong kỹ thuật này có thể là tập trung hoặc phân tán nhưng nó không đáp ứng với mọi sự thay đổi trên mạng. Trong trường hợp này, việc chọn đường thực hiện mà không có sự trao đổi thông tin, không đo lường và không cập nhập thông tin. Tiêu chuẩn (tối ưu) để chọn đường và bản thân con đường được chọn một lần cho toàn cuộc, không hề có sự thay đổi giữa chúng. Kỹ thuật chọn đường này rất đơn giản, do vậy được sử dụng rộng rãi, đặc biệt trong các mạng tương đối ổn định ít có thay đổi về địa hình và lưu thông trên mạng.

4.2 Kỹ thuật chọn đường thích nghi (hay còn gọi kỹ thuật chọn đường động):

Kỹ thuật này đã thu hút sự quan tâm đặc biệt những nhà thiết kế mạng do khả năng đáp ứng với các trạng thái khác nhau của mạng. Đây là một yếu tố rất quan trọng, đặc biệt đối với các ứng dụng thời gian thực trong đó yếu cầu đầu tiên của người sử dụng mạng là phải có khả năng cung cấp được các con đường khác nhau để dự phòng sự cố và thích nghi nhanh chóng với các thay đổi trên mạng. Mức độ thích nghi này được đặc trưng bởi sự trao đổi thông tin chọn đường trong mạng. Đơn giản nhất là không trao đổi gì hết. Mỗi nút (hoặc trung tâm điều khiển trong trường hợp kỹ thuật tập trung) hoạt động một cách độc lập với thông tin riêng của mình để thích nghi với sự thay đổi của mạng theo một phương pháp nào đó. ở mức độ cao hơn, thông tin về trạng thái của mạng có thể được cung cấp từ các nút láng giềng hoặc từ tất cả các nút khác. Thông thường, các thông tin được đo lường và sử dụng cho việc chọn đường bao gồm:

- Các trạng thái của đường truyền.
- Các độ trể truyền dẫn.
- Mức độ lưu thông.
- Các tài nguyên khả dụng.

Khi có sự thay đổi trên mạng (ví dụ thay đổi do sự cố hoặc do sự phục hồi của một nút mạng v.v...) các thông tin trên cần phải được cập nhật. Thực tế cho thấy rằng phần lớn các kỹ thuật chọn đường phân tán và thích nghi đáp ứng nhanh với các 'tin lành' nhưng lại đáp ứng chậm đối với các 'tin xấu'. Chẳng hạn thông tin về sự cố của một đường truyền nằm trên một con đường đã chọn đôi khi không được truyền với tốc

độ cần thiết làm cho các gói tin vẫn được gửi đến đường truyền đó gây nên hiện tượng tắc nghẽn, chúng ta cần phải có các giải pháp cho vấn đề này.

Trong kỹ thuật chọn đường phân tán và thích nghi cũng gặp một số các hiện tượng khác nhau. Ví dụ như các gói tin bị quẩn trong mạng và không bao giờ đến được đích.

5. Một số kỹ thuật định đường khác

5.1 Định đường phân cấp

Khi số nút mạng tăng lên đáng kể, các bẳng định đường tăng lên. Router không chỉ tốn kém bộ nhớ mà còn cần nhiều thời gian CPU và nhiều giải thông cần để gửi các báo cáo trạng thái về chúng. Do đó định đường phải được phân cấp kiểu như mạng Telephone.

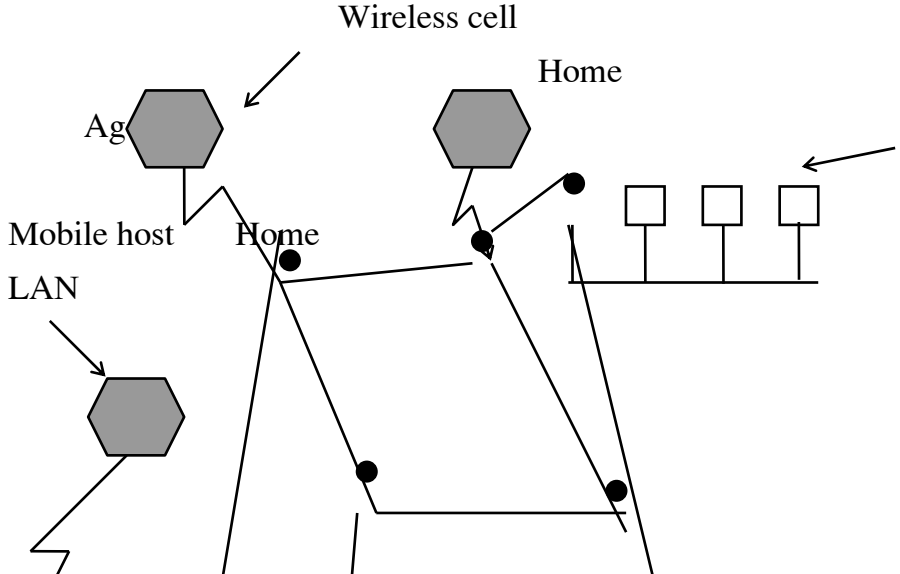
Khi định đường phân cấp được sử dụng các router được phân chia thành những cụm khác nhau mà ta gọi là vùng, mỗi router biết cách định đường các gói đến các đích trong vùng của nó, nhưng không biết gì về cấu trúc bên trong của vùng khác. Khi những mạng khác nhau được ghép nối với nhau thì coi mỗi mạng như là một vùng phân cách. Điều này nhằm giải phóng các router trong một mạng khỏi bận tâm đến cấu trúc topolopy của các mạng khác.

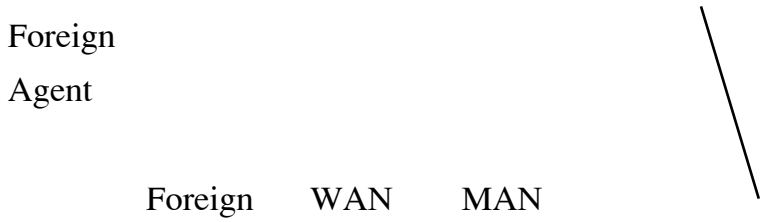
Cho một hệ thống mạng khổng lồ, phân cấp 2 mức có thể không đủ, lúc đó cần phân các vùng vào những Cluster, các cluster vào trong các miền, các miền vào trong các nhóm và cứ như vậy cho đến khi chúng ta đưa ra tên của các khối kết hợp.

Một ví dụ của một hệ thống phân cấp đa mức, xét xem làm thế nào một gói có thể được định đường từ Mỹ, Anh, Pháp .... Router Mỹ có thể không biết topolopy chi tiết bên trong của Nga nhưng có thể gửi luồng lưu thông ra ngoài tới router ở Nga. Router ở Nga có thể gửi luồng lưu thông tới tất cả các router trong nước mình vò có thể gửi luông lưu thông ra các nước khác.

5.2 Định đường cho máy chủ di động (Routing for mobile host)

Hiện nay trên thế giới hàng triệu người có máy tính xách tay, họ muốn đọc những Email và truy cập hệ thống file thông thường của họ ở bất cứ nơi đâu trên thế giới. Những máy chủ di động này mở ra sự phức tạp mới cho việc định đường các gói tin đến một máy chủ di động. Mô hình thế giới mà những nhà thiết kế mạng sử dụng được biểu diễn ở hình2.1. Có một mạng WAN bao gồm các router, các máy chủ, được kết nối với WAN là các LAN, MAN và những phần tử không dây khác. Đối với người dùng có hai loại khác nhau, đó là :Người dùng đứng yên và người dùng di động.





Người dùng đứng yên là người dùng kết nối vật lý với mạng bởi các dây cáp. Người dùng di động có thể chia làm hai loại phân biệt khác nhau, đó là:

+ Người dùng di động mà đứng yên cơ bản: là những người dùng mà chỉ di chuyển từ vị trí cố định này sang vị trí cố định khác, từ thời gian này qua thời gian khác, nhưng sử dụng mạng chỉ khi nối kết vật lý với nó.

+ Người dùng di động: là những người dùng mà tính toán thực sự trên đường đi và duy trì những kết nối của họ khi đang chuyển động.

Chúng ta sẽ xét đến người dùng di động, đó là tất cả những người dùng xa nha. Người dùng luôn luôn có một địa chỉ cố định ở nhà dùng để xác định vị trí của họ.

Do đó, mục đích định đường trong hệ thống có người dùng di động là gửi các gói tin đến người dùng di động bằng cách sử dụng địa chỉ nhà của họ và gửi những gói tin một cách hữu hiệu đến họ ở bất cứ nơi đâu mà họ đến.

5.3 Định đường quảng bá (broadcast routing)

Đối với một vài ứng dụng các Host cần gửi các thông báo tới nhiều hoặc tất cả các host khác nhau. Ví dụ dịch vụ phân tán báo cáo thời tiết, cập nhật thị trường chứng khoán hoặc các chương trình Radio trực tiếp .... có thê thực hiện tốt nhất bằng cách quảng bá tới tất cả các máy.

Việc gửi tất cả các gói tới tất cả các đích một cách đồng thời gọi là quảng bá (broadcast routing). Có nhiều phương pháp quảng bá khác nhau như:

1. Phương pháp quảng bá đơn giản nhất là gửi các gói phân biệt đến mỗi đích mà không yêu cầu một đặc trưng nào từ mạng con đối với nguồn.

2. Flooding là một kỹ thuật được đưa ra để lựa chọn, mặc dù nó không phù hợp với truyền thông điểm - điểm thông thường. Tuy nhiên, flooding sinh ra quá nhiều gói và lãng phí quá nhiều giải thông.

3. Phương pháp định đường đa đích (Multi Destination Routing) nếu phương pháp này được sử dụng mỗi gói chứa hoặc là danh sách các đỉnh hoặc là một bản đồ bit chỉ báo đến các đích mong muốn. Khi một gói đến tại một router, router đó kiểm tra tất cả các đích để xác định một tập các đường ra mà chúng sẽ cần tới (một đường ra là cần thiết nếu nó là tuyến đường tốt nhất tới ít nhất một điểm trong đích). Router tạo ra một bản sao mới của gói cho mỗi đường ra được sử dụng, chứa trong mỗi gói chỉ là các đích mà chúng đến. Do đó, số đích của các gói giảm dần. Sau mọt số đủ các hops, mỗi gói sẽ chỉ mang một đích và khi đó có thể coi như một gói thông thường. Trong định

đường đa đích các gói được đánh địa chỉ riêng rẽ, trừ các gói đi theo cùng tuyến đường đến cùng một đích. Một gói trong chúng trả "tiền vé" và những gói khác còn lại đi tự do.

4. Phương pháp dùng cây khung "Sink tree" đối với router khởi đầu quảng bá hoặc bất kỳ cây khung thích hợp khác cho router.

Một cây khung là một đồ thị con của mạng con chứa tất cả các router, nhưng không có chu trình. Nếu mỗi router biết một đường nào đó trong đường dọc theo cây khung, nó có thể sao một gói mới quảng bá ra tất cả những đường của cây khung trừ đường nó đến. Phương pháp này sử dụng giải thông tốt hơn và số gói cần thiết tạo ra là cực tiểu tuyệt đối. Vấn đề còn lại là router phải có thông tin về vài cây khung mà nó có thể áp dụng được.

Thông tin có thể có sẵn (như định đường trang thái liên kết) hoặc không có sẵn (như định đường vecto khoảng cách).

5. Phương pháp định đường quảng bá cuối cùng là thử nghiệm của một thuật toán trước đây, ngay cả khi các router không biết gì về tất cả các cây khung. Khi một gói quảng bá đến một router, router kiểm tra để xem xét gói được đến trên đường mà nó thường sử dụng để gửi các gói tới nguồn quảng bá hay không. Như vậy đây là một cơ hội tốt để gói quảng bá tự nó đi theo tuyến đường tốt nhất từ router và do đó bản sao đầu tiên đến tại router. Đây là trường hợp router chuyển tiếp các bản sao của nó trên tất cả các đường, trừ đường mà nó tới.

Thuật toán chuyển tiếp đường đi ngược trở lại có hiệu quả cao và cài đặt dể dàng vì nó không yêu cầu các router biết về cây khung. Mặt khác tổng phí cho nó không lớn. Đặc biệt là nó không yêu cầu một cơ chế để dừng quá trình xử lý như Flooding.

6. Multicast routing: Đối với một vài ứng dụng, quá trình xử lý phân cách rộng lớn làm việc ghép nối với nhau tạo thành từng nhóm. Ví dụ, một nhóm xử lý hệ thống CSDL phân tán cần thiết cho quá trình xử lý trật tự để gửi các thông báo đến tất cả các thành viên của nhóm. Nếu nhóm nhỏ, nó chỉ gửi thông báo đến thành viên từ điểm này tới điểm khác. Nếu nhóm lớn thì chiến lượt này rất đắt, khi đó quảng bá được dùng. Nhưng dùg quảng bá để truyền cho 1000 máy trên một mạng hàng triệu nút là điều không thể được. Như vậy chúng ta cần có một cách để gửi các thông báo đến các nhóm đã xác định (các nhóm này dù lớn về số lượng nhưng khi so sánh toàn bộ mạng thì nó là nhỏ). Việc gửi một thông báo đến các nhóm xác định gọi là Multicast routing. Để thực hiện Multicast, trước hết phải biết cách quản lý nhóm, việc kết nối và tách rời khỏi nhóm. Các router cần biết chủ của chúng thuộc nhóm nào. Muốn vậy hoặc là nhóm thông báo cho các router biết về các thành viên cũng như sự thay đổi của các thành viên trong nhóm, hoặc là các router phải hỏi các chủ của chúng một cách định kỳ. Các router thông báo tới các router lân cận của nó, vì thế thông tin được lan truyền qua mạng con .

6. Các giải thuật tìm đường tối ưu

Bài toán tìm đường đi "tối ưu" (theo tiêu chuẩn "tối ưu" được chọn) trong số các con đường tồn tại giữa 2 điểm đã được giải quyết từ lâu và thuần túy toán học. Các giải thuật đó có thể áp dụng vào kỹ thuật chọn đường trong mạng với một số ít thay đổi cho phù hợp với bối cảnh từng ứng dụng. Yêu cầu của giải thuật khi áp dụng cần phải:

- Chính xác, đơn giản.

- Vững vàng, ổn định.
- Công bằng, tối ưu

Các giải thuật tìm đường đi phải có khả năng thay đổi cấu hình và đường vận chuyển để không phải khởi động lại mạng khi có một nút hỏng hoặc phải ngừng hoạt của các máy ở trạm.

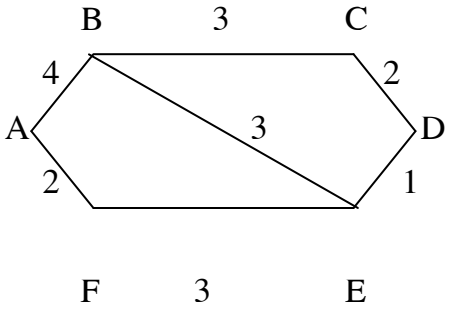
6.1. Thuật toán định đường không thích nghi:

Trong phần mô phỏng các thuật toán định đường không thích nghi ta sẽ xem xét đến thuật toán Dijkstra (1959) còn gọi là thuật toán Shortest Path Routing, thuật toán Dijkstra cải tiến, thuật toán định luồng cơ sở và một số ứng dụng của chúng trong việc định đường tối ưu.

6.1.1. Shortest Path Routing : (thuật toán Dijkstra - 1959)

Đồ thị trong thuật toán này gồm mỗi điểm đại diện cho mỗi router của mạng, cung giữa 2 điểm của đồ thị là đường đi giữa 2 router trong mạng. Việc chọn đường đi giữa 2 nút trong mạng là tìm đường đi ngắn nhất giữa chúng. Mỗi nút được gán nhận với khoảng cách của nó tới nguồn. Bắt đầu các nút là vô tận, rồi nguồn xét các nút cạnh nó, các nút này sẽ có nhãn hoặc dự kiến hoặc xác định. Các nhãn có thể thay đối, phản ánh con đường tốt hơn, khi phát hiện nhãn là con đường ngắn nhất tời nguồn tới nút, thì nó là cố định (*permanent*) và sau đó không thay đổi. Mỗi nút có chứa một nhãn với độ dài từ nút nguồn cho tới nó. Lúc ban đầu, thì đường đi này chưa được biết, vì vậy tất cả các nút được gán là vô cực. Thuật toán sẽ tìm ra đường đi và xử lý chúng, mỗi nhãn có sự thay đổi, phản ánh đường đi. Một nhãn sẽ chứa hoặc là nhãn tạm hoặc là nhãn cố định. Đầu tiên, tất cả các nhãn sẽ là nhãn tạm, khi các nhãn được tìm ra thì nó sẽ đại diện cho một nút trên đường đi từ nguồn tới nó, nhãn đó sẽ được gán nhãn cố định và không thay đổi về sau.

Ví dụ: Tìm đường đi ngắn nhất từ A $\rightarrow$ D trong đồ thị sau:



Xuất phát từ A có 2 đỉnh B và F liên thuộc với A nên chỉ có hai đường đi xuất phất từ A là A, B và A, F với các độ dài tương ứng là 4 và 2. Do đó F là đỉnh gần A nhất. Bây giờ ta tìm đỉnh tiếp theo gần A nhất trong tất cả các đường đi qua A và F (cho đến khi đạt tới đỉnh cuối cùng). Đường đi như thế ngắn nhất tới B là A, B với độ dài là 4 và đường đi như thế ngắn nhất tới E là A, F, E độ dài 5. Do vây đỉnh tiếp theo là B. Để tìm đỉnh thứ 3 gần A nhất, ta chỉ xét các đường qua A, F và B. Đó là đường đi A, B, C độ dài là 7và đường đi A, F, E , D độ dài là 6. Vậy D là đỉnh tiếp theo gần A nhất va độ dài của đường đi ngắn nhấ từ A tới D là 6.

Tuy nhiên phương pháp này không thể dùng cho người và máy trong trường hợp khi đồ thị có nhiều cạnh.

Thủ tục mô phỏng:

Khai báo:

```
Type nodelabel
   predecessor As Integer
         length As Long
           labl As Boolean
End Type
Dim so (1 To 6, 1 To 6) As Integer
Dim path (1 To 10) As Integer

Private Sub short(s As Integer, t As Integer, dd As Integer, kc As Integer)
Dim state(1 To 6) As nodelabel
Dim i,j,min,dem,infinity As Integer
infinity = 32767
For i = 1 To n
  For j = 1 To n
    If so(i, j) = -1 Then
      so(i, j) = infinity
    End If
  Next j
Next i

 If s = t Then
    dd = 1
    path(dd) = s
 Else
   For i = 1 To n
      state(i).predecessor = 0
      state(i).length = infinity
      state(i).labl = False
   Next i
    state(t).length = 0
    state(t).labl = True
    k = t
    Do While k <> s
```

```
      For i = 1 To n
       If (so(k, i) <> 32767) And (state(i).labl = False) Then
        If (state(k).length + so(k, i)) < state(i).length Then
            state(i).predecessor = k
            state(i).length = state(k).length + so(k, i)
        End If
       End If
      Next i
       min = infinity
       k = 0
    For i = 1 To n
     If (state(i).labl = False) And (state(i).length < min) Then
          min = state(i).length
          k = i
     End If
    Next i
      state(k).labl = True
    Loop
    k = s
    i = 0
    Do
     i = i + 1
     path(i) = k
     k = state(k).predecessor
    Loop While k <> 0
    dd = i
    kc = state(s).length
  End If
End Sub
```

Trong đó: s : nút nguồn

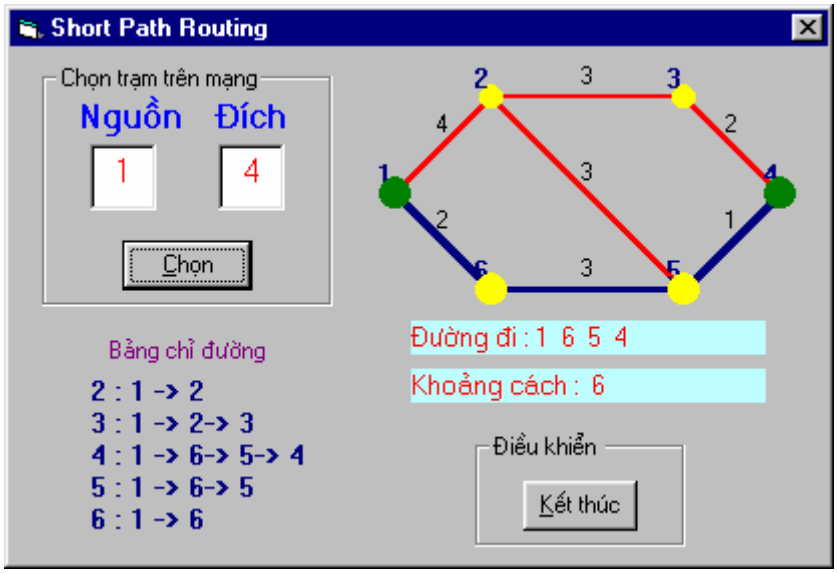
t : nút đích

so(i,j) : ma trận đồ thị của mạng

path : mảng lưu đường đi

dd : số nút đường đi ngắn nhất tìm được đi qua

kc : khoảng cách ngắn nhất.



6.1.2. Thuật toán Dijsktra : (sử dụng cho định đường tập trung)

Cùợng với dữ liệu đầu vào như thuật toán trên, nhưng thuật toán này được mô tả như sau: Gọi C là tập hợp các đỉnh chưa được chọn, S là tập hợp các đỉnh được chọn. Tại mỗi thời điểm, tập S chứa các đỉnh mà khoảng cách nhỏ nhất từ nguồn đến chúng đã được xác định. Khi đó tập C chứa các đỉnh còn lại. Giải thuật bắt đầu tập S chứa đỉnh nguồn, khi giải thuật kết thúc thì tập S chứa tất cả các đỉnh của đồ thị. Tại mỗi bước ta chọn một đỉnh của tập C mà khoảng cách từ nguồn đến đích này là nhỏ nhất và đưa vào tập S. Ta nói rằng đường đi từ nguồn đến đích khác là riêng biệt nếu tất cả các đỉnh trung gian trên đường này đều nằm ở trong tập S. Tại mỗi bước của giải thuật, một mảng 1 chiều D dùng để chứa chiều dài đường đi riêng biệt.

Giả sử các đỉnh của đồ thị được đánh số từ 1 đến n, không mất tính tổng quát ta chọn đỉnh nguồn là1 và L là ma trận chứa chiều dài các cung.

Ma trận được mô tả:

L[i,i] = 0 với ∀i = 1..n

L[i,j]>=0 nếu tồn tại cung từ đỉnh i đến j

L[i,j] = ∞ nếu không tồn tại cung từ đỉnh i đến j.

Sơ đồ thuật toán:

Thủ tục :

Dim L(1 To 6, 1 To 6) As Long

```
Dim d(1 To 6) As Integer
Dim P(1 To 6) As Integer
Dim cc(1 To 6) As Integer
Dim path(1 To 6) As Integer

Private Sub dijkstra()
Dim i,j,k,mk,min,x,n,mx As Integer

For i = 1 To n
  For j = 1 To n
    If L(i, j) = -1 Then
      L(i, j) = 32767
    End If
  Next j
Next i

k = n - 1          'so phan tu cua tap C

For i = 2 To n
  cc(i - 1) = i     'C : tap cac dinh tu 2..n
  d(i) = L(1, i)
  P(i) = 1
Next i

For i = 1 To n - 2
  ' tim dinh  v thuoc C va D[v] nho nhat
  min = d(cc(1))
  mx = 1
  For j = 2 To k
    If d(cc(j)) < min Then
      min = d(cc(j))
      mx = j
    End If
  Next j
```

```
 'loai bo C[mx] ra khoi C
 mk = cc(mx)
 cc(mx) = cc(k)
 k = k - 1

 For j = 1 To k
  x = cc(j)
  If d(x) > d(mk) + L(mk, x) Then
    d(x) = d(mk) + L(mk, x)
    P(x) = mk
  End If
 Next j
Next i
End Sub
```

6.1.3. Thuật toán Dijkstra: (sử dụng cho định đường phân tán)

Thuật toán này dựa trên một dãy các bước lặp. Một tập đặc biệt các đỉnh được xây dựng bằng cách cộng thêm một đỉnh trong một bước lặp. Thủ tục gán nhãn được thực hiện trong mỗi lần lặp đó. Trong thủ tục gán nhãn này, đỉnh w được gán nhãn bằng độ dài đường đi ngắn nhất từ a đến w chỉ đi qua các đỉnh thuộc tập đặc biệt. Đỉnh được thêm vào là đỉnh có nhãn nhỏ nhấto với các đỉnh chưa có trong tập đó.

Thuật toán Dijkstra được xây dựng theo phương pháp gán nhãn:

Procedure Dijkstra (G : đồ thị trọng số)

{G có các đỉnh a = v_0 , v_1 ...vn = z và trọng số w(vi , vj),

với w(vi , vj) = ∞ nếu {vi , vj} không là cạnh trong G}

```
for i:=1 to n
    L(vi) := ∞
    L(a) := 0
    S := ∅
```

{Ban đầu các nhãn được khởi tạo sao cho nhãn của a bằng 0, các đỉnh khác bằng ∞, S là tập rỗng}

```
while z ∉ S
   begin
      u := đỉnh không thuộc S có nhãn L(u) nhỏ nhất
```

S := S ∪ {u}

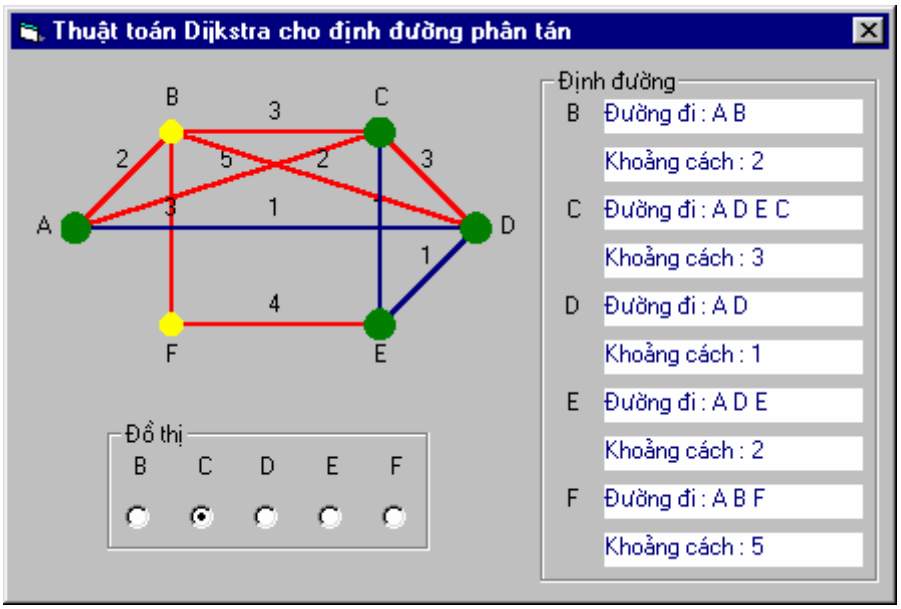
for tất cả các đỉnh v không thuộc S

if L(u) + w(u,v) < L(v) then L(v) := w(u,v)

{thêm vào S đỉnh có nhãn nhỏ nhất,

và sữa đổi nhãn của các đỉnh không thuộc S}

end {L(z) = độ dài đường đi ngắn nhất từ a tới z}



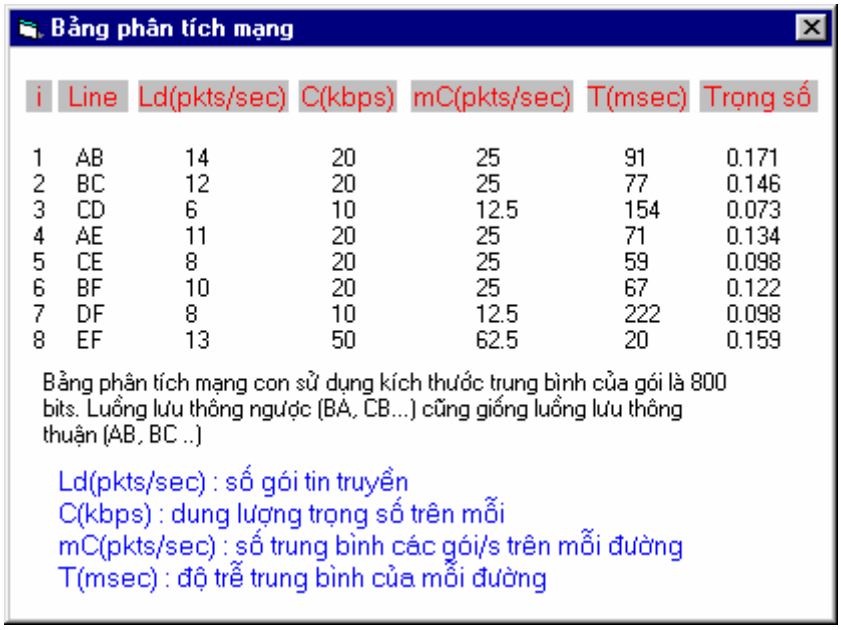
Nhận xét: Trong thuật toán này khi tính toán đường đi từ nút nguồn đến nút n nào đó, ta không cần biết giá của tất cả các liên kết trong mạng mà chỉ cần biết giá từ nút đó đến các nút lân cận của nó và nhãn của các nút lân cậnđó. Như vậy thuật toán phù hợp với định đường phân tán.

6.1.4. Thuật toán định luồng cơ sở :

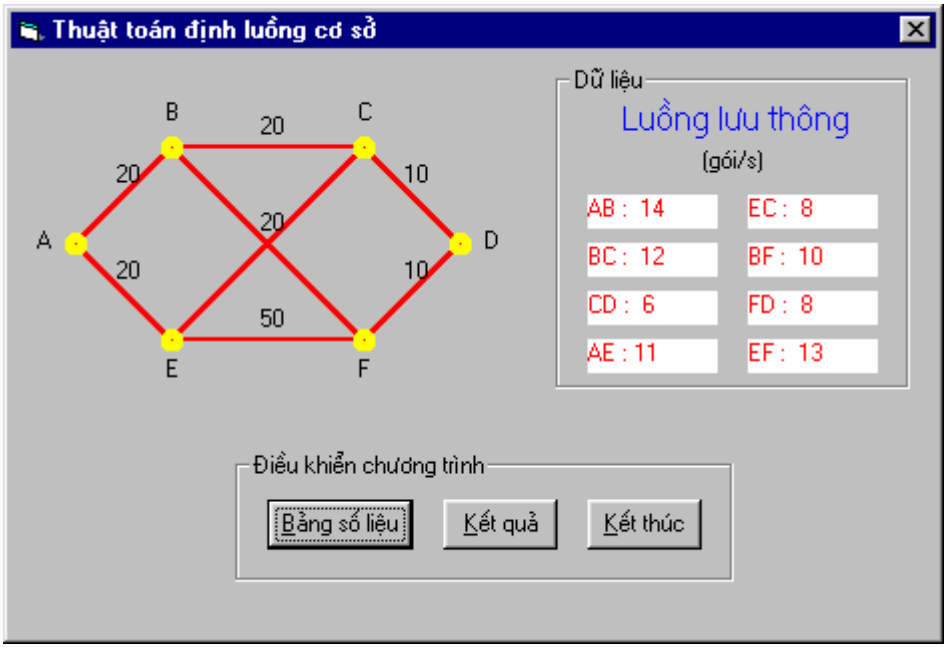
Dữ liệu đầu vào của thuật toán bao gồm :

- Ma trận luồng cơ sở.
- Ma trận dung lượng các đường.

Kết quả cho một bảng thông tin bao gồm :



Căn cứ vào, T (msec) *(độ trễ trung bình của mỗi đường)* và chọn một thuật toán định đường (như 2 thuật toán nêu ở trên) ta sẽ có đường đi từ nguồn đến đích mà có xét đến cả tải và topogoly.



6.2. Thuật toán định đường thích nghi:

Trong phần này trình bầy áp dụng của thuật toán Định đường vector khoảng cách để cập nhật những bảng định đường cho những nút mạng và thuật toán liên kết trạng thái.

Thuật toán Định đường vector khoảng cách:

Dữ liệu vào là bảng định đường những nút lân cận đối với một nút muốn cập nhật bảng định đường và độ trễ từ nút đó đến những nút lân cận. Một bảng định đường mới sẽ được cập nhật cho nút này đến tất cả các nút khác thông qua những nút lân cận.

Giả sử muốn cập nhật bảng định đường cho nút J, và giả sử muốn cập nhật đường đi từ J đến C xem thử sẽ đi qua trạm nào, ta thấy độ trễ từ J qua nút I đến C là ngắn nhất, nên đường đi từ J đến C phải đi qua nút I.

Trong mạng các trạm có một bảng định đường như vậy và thường được cập nhật thông qua các bảng định đường của các trạm lân cận, sự cập nhật này có thể được thực hiện một cách tự động thông qua một giao thức. (ví dụ giao thức RIP - *Routing Information Protocol* thường được sử dụng trong một số hệ điều hành mạng như : Windows NT Server ...,các router chạy giao thức này đều đặng phát quảng bá bảng định đường của nó 2 lần/phút, bất cứ nút làm việc nào chạy RIP sẽ nhận được thông tin này và tự động cập nhật vào bảng định đường của mình).

V. GIAO THỨC X.25 PLP

Có chức năng quản lý ghép nối giữa DTE/ DTE ở 2 đầu nút mạng (end-to-end) và DTE/DCE trong đó DCE đóng vai trò nút mạng chuyển mạch gói X.25. X25.PLP định nghĩa 2 loại liên kết logic:

- Liên kết ảo có tính tạm thời.
- Liên kết ảo được thiết lập vĩnh viễn.

1. Dạng gói tin X.25.PLP

0 0 0 1	Đánh số mạch ảo
Đánh số mạch ảo (12 bit)	
Type (00001011)	Control (1)
Độ dài địa chỉ DTE được yêu cầu	Độ dài địa chỉ DTE yêu cầu
Địa chỉ nguồn Địa chỉ đích	
Độ dài vùng khai báo thủ tục phụ	
Khai báo lần lượt các thủ tục sử dụng	
Dữ liệu phụ có tính chất thông báo(16bytes)	

Hình 3.9: Định dạng gói yêu cầu thiết lập liên kết

1 8

0 0 0 1	4bit
Số hiệu của liên kết logic 12 bits	8bit

Loại thông tin	1
Thông tin bổ sung	

Hình 3.10 : Định dạng gói điều khiển

1 8

Q	D	0 1		
Số hiệu của liên kết logic 12 bit				
Số hiệu gói gởi		M	Số hiệu gói đang chờ để nhận	0
Dữ liệu				

Hình3.11: Định dạng gói dữ liệu

trong đó:M= 0 thì còn tin và 1 là báo hết tin

D: để chỉ thị về cơ chế báo nhận gói tin

Q: dùng để định tính thông tin chứa trong gói tin

2. Trao đổi gói tin ở X 25.PLP

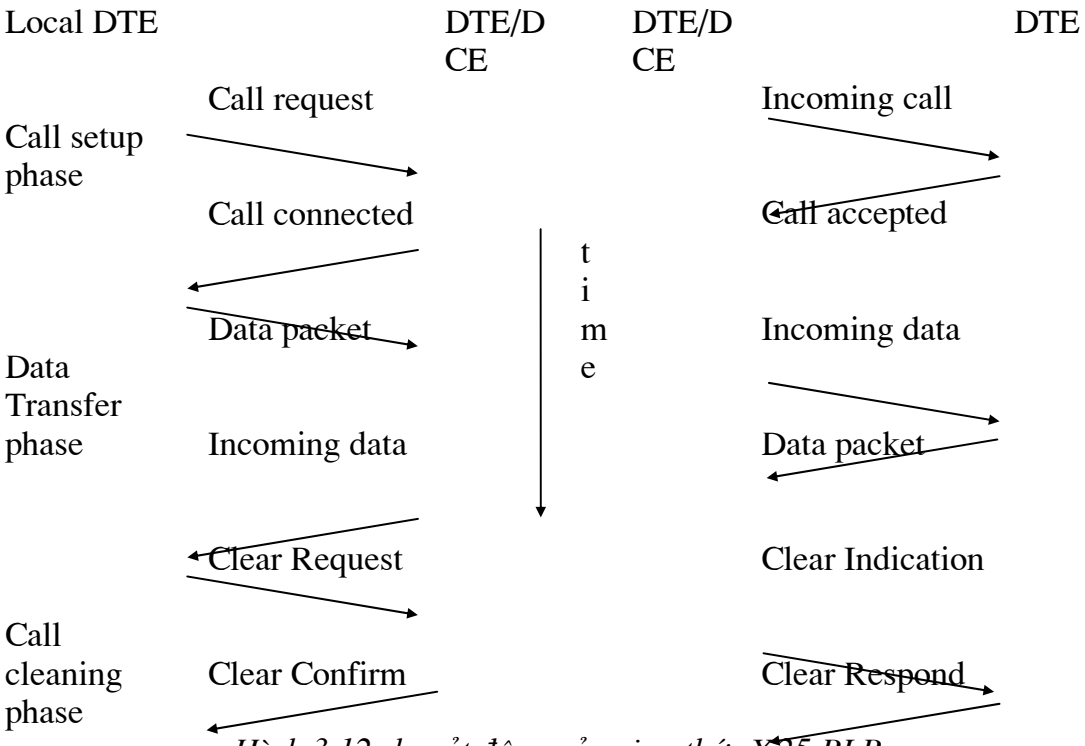
X25.PLP có các thủ tục chính như sau :

- *Thiết lập, xóa, khởi động lại liên kết.*

- *Truyền dữ liệu thường, khẩn.*

- *Khởi động lại một giao diện.*

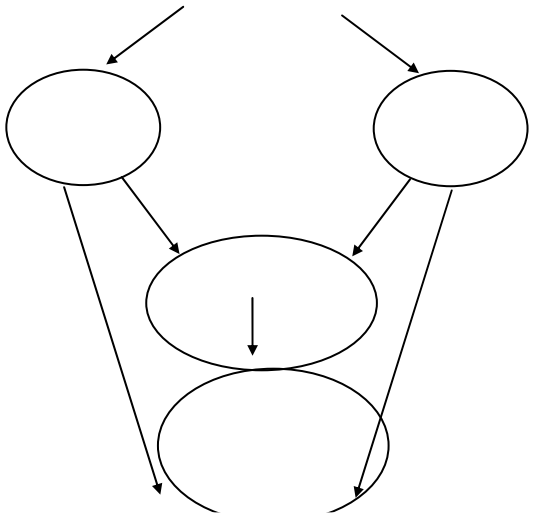
Quá trình trao đổi gói tin được mô tả bằng hình sau:



Hình 3.12: hoạyt động của giao thức X.25 PLP

Có thể xảy ra trường hợp cả hai phía cùng chọn một yêu cầu, dẫn đến việc đụng độ giữa các cuộc gọi (call collision)

Đồ thị trạng thái của quá trình nối-tách:



Qúa độ	Gây bởi	Gói tin gửi
1	DTE	Call Request
2	DCE	Call Connected
3	DCE	Incoming Call
4	DTE	Call Accepted
5	DCE	Incoming Call
6	DTE	Call Request
7	DCE	Call Connected

Hình 3.13:Đồ thi trang thái

VI. VẤN ĐỀ TẮC NGHẼN

1. Tắc nghẽn

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

- Khi số gói tin dựa vào mạng ít hơn khả năng vận chuyển của nút mạng thì gói tin dựa vào mạng sẽ bằng số gói tin được gữi đi.

- Nếu số gói tin dựa vào mạng càng nhiều hơn khả năng vận chuyển của nút mạng thì gói tin chuyển đi càng chậm và cuối cùng dẫn đến tắc nghẽn.

Nguyên nhân:

- Hàng đợi sẽ bị đầy (phải lưu tệp, phải tạo các bảng ...), nếu khả năng xử lí của nút yếu.

- Hàng đợi bị đầy khi thông tin vào nhiều hơn khả năng của đường ra, mặc dù tốc độ xử lí của nút nhanh.

Cần phân biệt hai khái niệm:

- Điều khiển dòng dữ liệu là xử lý giao thông giữa điểm với điểm, giữa trạm phát với trạm thu.

- 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.

2. Chống tắc nghẽn

Mặc dù sinh ra cơ chế kiểm soát luồng dữ liệu nhằm tránh tình trạng ùn tắc trên mạng nhưng trong thực tế thì nó vẫn cứ xảy ra và người ta phải dự kiến các giải pháp thích hợp. Nhiệm vụ giải quyết ùn tắc này thường dành cho tầng Mạng. Có thể dùng một số biện pháp sau đây:

- Dành sẵn các bộ đệm chỉ để dùng khi xẩy ra ùn tắc. Phương pháp này đã được dùng trong mạng ARPANET nhưng hiệu quả không cao vì bản thân bộ nhớ đệm rồi cũng nhanh chóng ùn tắc.

- Gắn cho các gói tin một thời gian "sống" xác định trước, nếu quá thời gian đó thì chúng bị hủy. Tuy nhiên giải pháp này khá nguy hiểm vì có thể hủy bỏ các gói tin ngay khi chúng vừa đạt đích. Nhưng dẫu sao thì nó cung có ích trong việc ngăn chặn hiện tượng ùn tắc nên người ta cũng thường hay dùng. Đơn giản hơn, ta có thể loại bỏ các gói tin muốn đi qua một liên kết đã quá tải. Giao thức tầng Giao Vận sẽ chịu trách nhiệm truyền lại các gói tin bị loại bỏ đó.

- Trong các mạng dùng mạch ảo như là mạng X25, sự ùn tắc có thể do mở ra quá nhiều VC qua một nút. Cần phải đóng bớt một số để tránh ùn tắc. Tầng mạng chịu trách nhiệm mở lại các VC đó thì không còn nguy cơ ùn tắc nữa.

Ngoài ra còn có các biện pháp sau:

- Bố trí khả năng vận chuyển, lưu trữ, xử lý của mạng dư so với yêu cầu.

- Hủy bỏ các gói tin bị tắc nghẽn quá thời hạn.

- Hạn chế số gói tin vào mạng nhờ cơ chế của sổ.

- Chặng đường vào khi của các gói tin khi mạng quá tải.

3. Điều khiển tắc nghẽn ở mạng con mạch ảo :

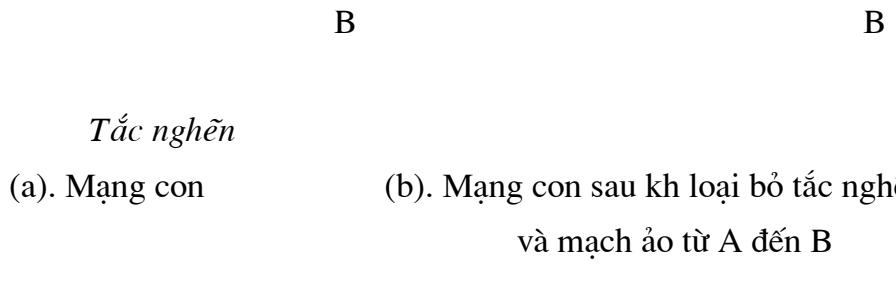
Những phương pháp điều khiển tắc nghẽn được mô tả ở trên về cơ bản là vòng mở : chúng ngăn ngừa tắc nghẽn xảy ra ở nơi đầu tiên hơn là việc xử lý tắc nghẽn sau này. Trong phần này sẽ mô tả vài phương pháp năng động để điều khiển trong mạng con mạch ảo.

Một kỹ thuật được sử dụng rộng rãi để giữ cho tắc nghẽn vừa xảy ra không diễn biến xấu đó là điều khiển nơi nhận (*admission control*). ý tưởng là đơn giản : một khi có tín hiệu tắc nghẽn, một một mạch ảo nào được thiết lập cho tới khi vấn đề được giải quyết. Do đó, việc cố gắng thiết lập một tầng giao vận mới là không xảy ra. Một phương pháp đơn giản dễ thực hiện như trong hệ thống điện thoaĩi, khi chuyển mạch có sự quá tải, nó cũng áp dụng điều khiển đầu nhận, cho ngừng quay số.

Phương pháp thay thế là cho phép thiết lập mạch ảo nhưng cẩn thận tất cả các mạch ảo này khi di chuyển quanh khu vực có sự cố. Ví dụ xem mạng con hình (a) bên dưới, có 2 router bị tắc nghẽn như mô tả.

A A

Tắc nghẽn



(a). Mạng con (b). Mạng con sau kh loại bỏ tắc nghẽn và mạch ảo từ A đến B

Giả sử 1 máy chủ gắn với router A muốn kết nối với máy chủ gắn với router B. Thông thường, đây là liên kết sẽ đi qua một trong những router bị tắc nghẽn. Để tránh tình trạng này, chúng ta có thể vẽ một mạng con như hình (b), bỏ qua những router tắc nghẽn và tất cả các đường của chúng. Đường gạch (hình b) cho biết đường có thể đi của mạch ảo để tránh những router tắc nghẽn.

Một chiến lược khác liên quan đến mạch ảo là thỏa thuận giữa máy chủ và mạng con khi thiết lập mạch ảo. Sự thỏa thuận này thường chỉ định rõ dung lượng và hình dạng lưu thông, chất lượng dịch vụ yêu cầu và một số tham số khác. Để giữ phần của mình trong thỏa thuận, mạng con sẽ lưu giữ nguồn tin theo dọc đường dẫn khi mạch được thiết lập. Những nguồn tin đó có thể bao gồm bảng, khoảng bộ nhớ đệm của những router và giải thông trên các đường. Theo cách này tắc nghẽn chắc chắn không xảy ra ở những mạch ảo mới bởi vì tất cả các nguồn tin cần thiết được bảo đảm có sẵn.

Phương pháp này được thực hiện mọi thời gian như là tiến trình vận hành chuẩn hoặc chỉ khi mạng xảy ra tắc nghẽn. Sự bất lợi cho việc thực hiện điều này là tiêu phi nguồn tin. Nếu 6 mạch ảo sử dụng 1 Mbps, tất cả đều qua một đường 6 Mbps, thì đường này được xem như là đầy, thậm chí hiếm khi xảy ra tất cả 6 mạch ảo lại được truyền cùng một lúc. Kết quả, giá trị của điều khiển tắc nghẽn là giải thông vô dụng.

VII. CÁC CÔNG NGHỆ CHUYỂN MẠCH NHANH TỪ X.25 ĐẾN ATM

1. Frame Relay

Trong X.25 chức năng dồn kênh đối với các liên kết ảo chỉ đảm bảo sự kiểm soát lỗi cho các khung gởi đi qua giao tiếp DTE/DCE cục bộ. 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 chi phí xử lí các gói tin tăng lên. Do đó sự xuất hiện của công nghệ Frame Relay được phù hợp hơn để sử dụng với bộ giao thức TCP/IP.

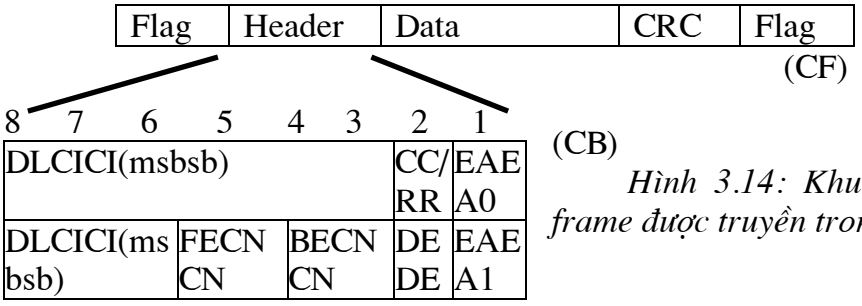
Trái lại, với Frame Relay chức năng dồn kênh, chọn đường được thực hiện ở tầng hai. Hơn nữa việc chọn đường cho các Frame rất đơn giản làm cho thông lượng có thể cao hơn nhiều so với kỹ thuật chuyển mạch gói và đồng thời frame Relay không có tính năng sửa lỗi vì các phương tiện phần cứng phục vụ dịch vụ thông tin số ngày nay

đã trở nên rất tinh cậy nên những quy trình sửa lỗi trước đây không cần thiết do đó tốc độ chuyển mạch nhanh.

Frame Relay cho phép đa cuộc gọi đến các địa chỉ khác nhau trong tiến trình đường hiện hành. Khi mỗi cuộc gọi đầu tiên được thiết lập sử dụng kênh D để trả lời cho dịch vụ nguyên thủy L-CONNECT request gọi là DLCI (data link connection identifier). Tất cả các yêu cầu truyền dữ liệu liên tục, liên quan với cuộc gọi này thì DLCI xem như là một tham số. DLCI được gắn vào phần đầu của các Frame cuối để chọn đường các Frame đến các đích của chúng.

1.1. Khuôn dạng bảng tin

+ Khuôn dạng tổng quát dùng trong kỹ thuật Frame Relay cũng giống như HDLC, chỉ khác trong nội dung của vùng thông tin điều khiển. Khung dữ liệu có kích thước gói từ 64bytes đến 1500 bytes



Hình 3.14: Khuôn dạng của mỗi frame được truyền trong kênh B

DLCI : Data Link Connection Identifier: Định danh kết nối liên kết dữ liệu.

EA : Extended Address

C/R : Command/Response: Thực hiện lệnh/Trả lời

FECN : Forward Explicit Congestion Notification (CF)

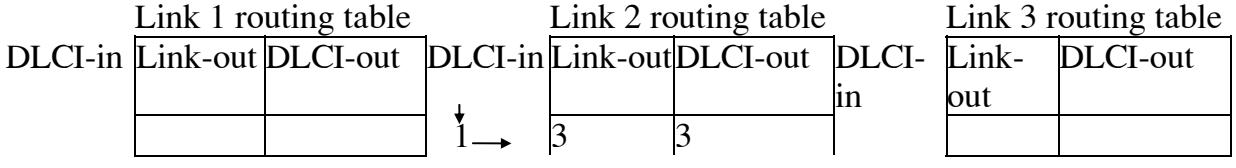
BECN : Backward Explicit Congestion Notification (CB)

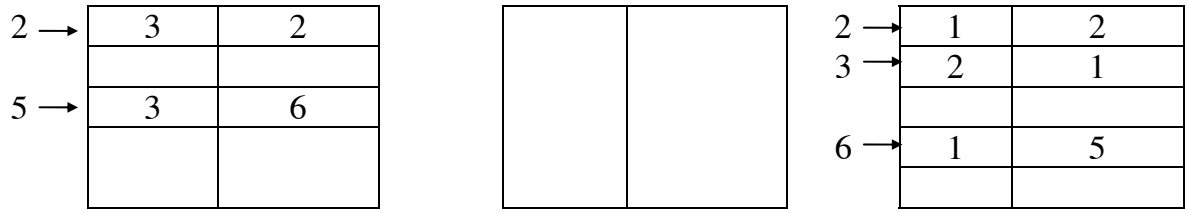
DE : Discard elegibility

1.2. Phương thức hoạt động

Trong vùng Header của frame có chứa tham số DLCI để định danh các liên kết dữ liệu được thiết lập. Mỗi khi một liên kết dữ liệu được thiết lập thì nó được gán 1 DLCI và giá trị này sẽ luôn được khai báo trong tất cả frame dữ liệu và frame điều khiển liên quan đến liên kết đó. Cũng giống như tham số VCI trong X.25 PLP, DLCI chỉ có ý nghĩa cục bộ và được dùng để chọn đường (chuyển tiếp cho frame tới đích của nó).

ở mỗi nút khi nhận được 1 frame dữ liệu, chương trình điều khiển được cài ở đó sẽ đọc giá trị DLCI trong vùng header và kết hợp với số liệu của đường truyền vào để xác định đường truyền ra và giá trị DLCI đi vaò tương ứng. Giá trị DLCI mới này sẽ được ghi vào header của frame và frame sẽ được đưa vào hàng đợi để gởi tiếp đi trên đường ra được chọn. Trật tự các frame được chuyển tiếp, do đó được báo trước và lộ trình của nó cực nhanh.





Hình 3.15: Frame routing

Vì nhiều liên kết dữ liệu có thể đồng thời phân chia cho một đường truyền vật lý, mặt khác các frame liên quan đến một liên kết dữ liệu nào đó lại có thể được tạo ra ở các thời điểm ngẫu nhiên nên hiện tượng tắc nghẽn có thể xảy ra đối với một đường truyền ra nào đó khi lưu thông trong mạng quá lớn. Các bit, CF, CB và DE trong vùng header của frame được dùng để kiểm soát hiện tượng tắc nghẽn.

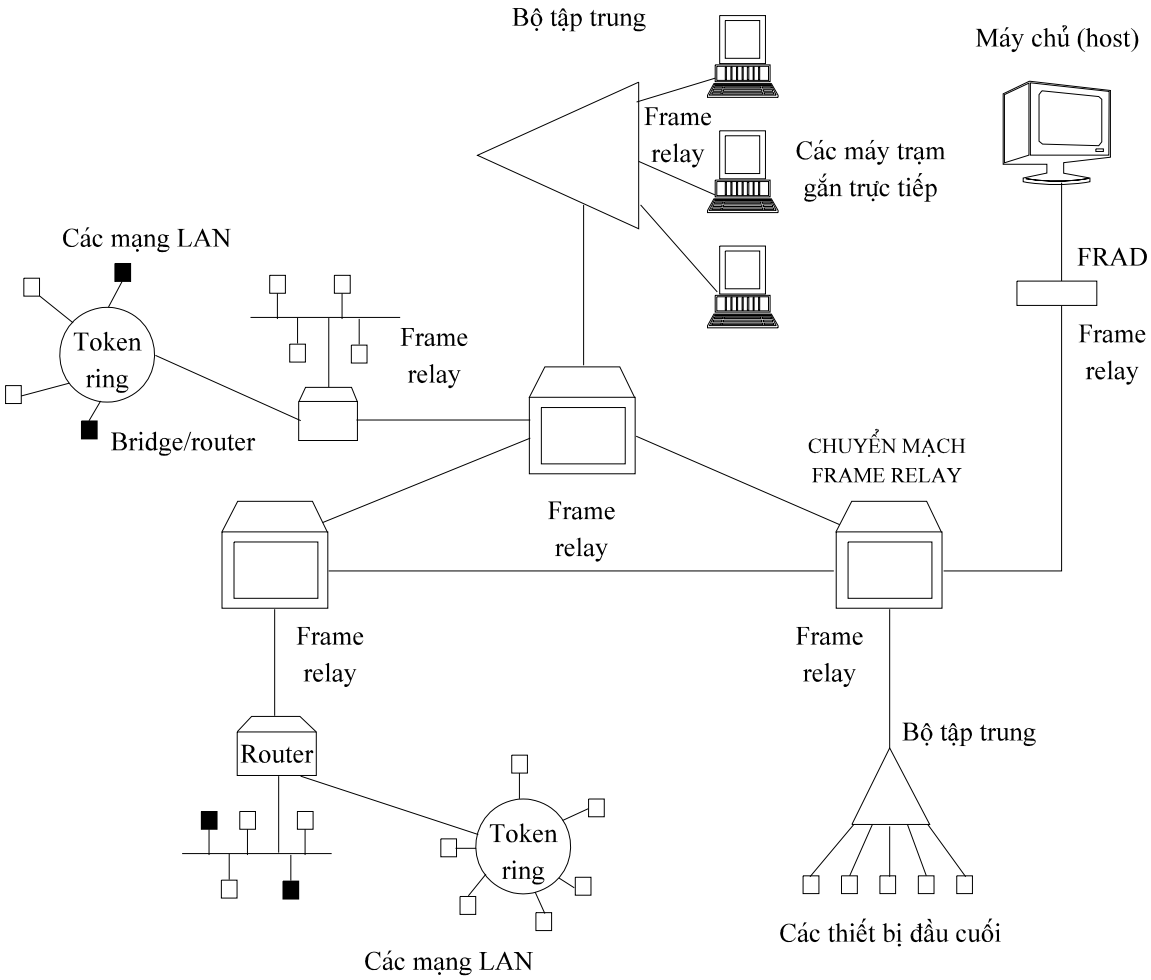
Mỗi khi frame handler chuyển tiếp một frame vào hàng đợi ra, nó phải kiểm tra kích thước của hàng đợi, nếu vượt quá một giới hạn cho trước thì nó thông báo tình trạng đó cho người sử dụng ở hai đầu liên kết bằng cách đặt giá trị cho bít CF hoặc CB tùy theo chiều đi hay chiều về của frame.

Khi frame handler trong máy của người sử dụng cuối nhận được thông báo về tình trạng tắc nghẽn mạng, nó sẽ tạm thời giảm tốc độ gởi frame của nó cho tới khi không còn tín hiệu về tắc nghẽn nữa.

Tuy nhiên trong trường hợp quá tải nhiều thì phải thực hiện loại bỏ bớt frame. Frame handler trong hệ thống của người sử dụng cuối sẽ dùng bit DE trong header để thực hiện loại bỏ bớt frame khi thấy hiện tượng vượt quá thông lượng đã thỏa thuận.

Để hạn chế tối đa gói bị giao nhầm, CRC trong mỗi mã kết thúc gói được dùng để khám phá các lỗi bit trong vùng điều khiển gói. Khi đó nếu lỗi được tìm ra, gói sẽ được phân tán đi. Sự phục hồi lỗi để lại cho các lớp giao thức cao hơn.

Ví dụ: mạng chuyển tiếp khung điển hình: Hình 3.16



Hình 3.16 Mạng chuyển tiếp khung điển hình

Tóm lại, Frame Relay là một cầu nối giữa các dịch vụ truyền dẫn băng hẹp hiện có với các dịch vụ truyền dẫn tốc độ cao, trong tương lai với khả năng truyền dẫn dữa liệu trên 2Mbps và dễ dàng tiến tới sử dụng ATM.

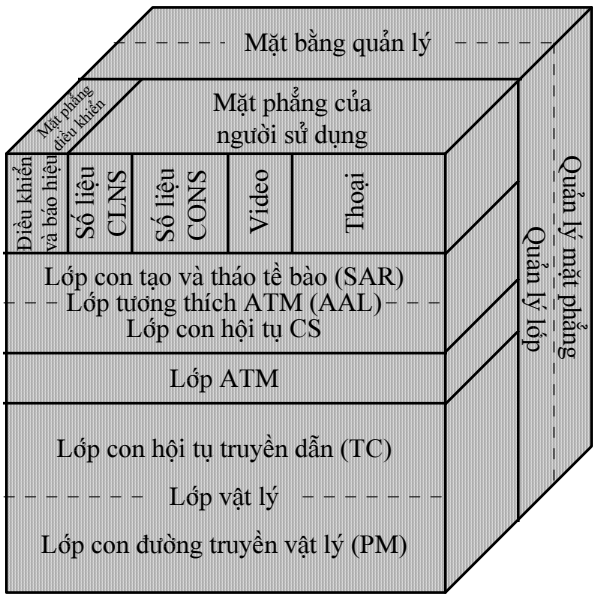
2. Giao thức ATM

ATM, viết tắt của Asynchorous Transfer Mode được CCITT (1990) đã định nghĩa về ATM như sau :

" *ATM là phương thức truyền tin mà trong đó thông tin được chia thành các gói gọi là tế bào thông tin. Các tế bào này được truyền độc lập và được xếp lại theo thứ tự ở nơi nhận. ATM có tính chất không đồng bộ bởi vì sự xuất hiện của các tế bào ATM tiếp theo ở mỗi kênh không nhất thiết phải mang tính chu kỳ...*"

2.1. Mô hình tham chiếu giao thức: PRM (Protocol Reference Model)

Mô hình tham chiếu PRM (Protocol Reference Model) của B-ISDN (Broadband - Intergrated Digital Network) dựa trên một mô hình tham chiếu liên kết hệ thống mở OSI (hình 14), có cấu trúc phân lớp từ trên xuống bao gồm các chức năng chuyển mạch, truyền dẫn, các giao thức báo hiệu, điều khiển.



Hình 2.7 : Mô hình tham chiếu giao thức B-ISD (B-ISDN PRM)

2.2. Chức năng của từng lớp

Trong phần này chúng ta khảo sát các chức năng từng lớp.

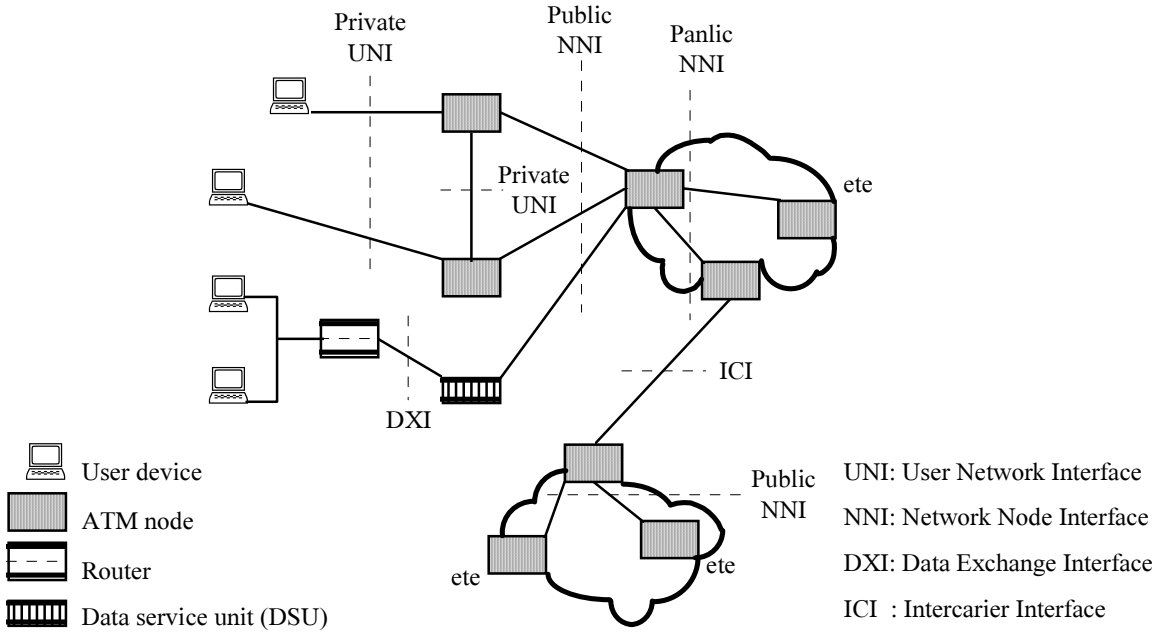
+ *Mặt bằng người khách hàng (user plane)* cung cấp chức năng điều khiển như vận chuyển các luồng thông tin người sử dụng, điều khiển dòng thông tin, sửa lỗi... Trong trường hợp này thông tin người sử dụng chỉ ra các thông tin dịch vụ trong BISDN khác nhau như thoại, hình ảnh, ... dữ liệu. Thông tin người sử dụng có thể được truyền một cách trong suốt qua B-ISDN hoặc qua các thủ tục tương ứng. Mặt bằng người sử dụng nó cũng có cấu trúc phân lớp, mỗi lớp nó thực hiện một chức năng riêng biệt liên quan đến việc cung cấp dịch vụ cho người sử dụng.

+ *Mặt bằng điều khiển (control plane)* nó cung cấp các chức năng kết nối và điều khiển cuộc gọi. Nói một cách khác mặt bằng điều khiển cung cấp các chức năng liên quan đến thiết lập cuộc gọi, giám sát cuộc gọi, giải phóng cuộc gọi. Ngoài ra nó cũng có thể cung cấp các chức năng điều khiển để thay đổi các đặc tính của dịch vụ đối với đường kết nối đã được thực hiện.

+ *Mặt bằng quản lý (management plane)* cung cấp chức năng giám sát mạng thông tin, nó liên quan đến việc truyền thông tin khách hàng (user) và thông tin điều khiển. Nó được phân loại thành chức năng *quản lý mặt bằng* và chức năng *quản lý lớp*. Chức năng quản lý mặt bằng điều khiển tổng thể hệ thống bằng cách can thiệp vào giữa các mặt bằng. Và chức năng điều khiển lớp cũng cung cấp việc điều hành liên quan đến nguồn tài nguyên và các tham số của giao thức tương ứng. Ngoài ra nó còn điều khiển luồng thông tin OAM của từng lớp liên quan.

2.3. Các giao diện ATM (ATM Interfaces)

Đa số các giao thức được đưa ra nhằm để trợ giúp các hoạt động của ATM . Một số giao thức đưa ra còn phụ thuộc vào lưu lượng của người sử dụng (user traffic) được truyền tải (Tranported). Hình 3.20 sẽ cho thấy bốn giao thức khác nhau và các giao thức có thể được đưa ra thực hiện.



Hình 3.20: Giao diện ATM

Giao diện mạng - người sử dụng (UNI :User Network Interface) là giao thức quan trọng nhất bởi vì nó định rõ những thủ tục liên kết hoạt động giữa các thiết bị người sử dụng (user equipment) và nút mạng. Như hình vẽ chỉ cho ta thấy hai dạng UNI đó là private UNI và public UNI. Sự khác nhau chính giữa hai giao diện này liên quan đến những liên kết thông tin vật lý giữa các thiết bị chuyên dụng .

Giao diện nút mạng NNI (Network node Interface) tồn tại cả hai loại giao diện private và public nó định rõ sự liên kết hoạt động (Interworking) của các nút mạng ATM. Theo cách viết này thì nó không đầy đủ ý nghĩa như của ITU-I và ATM Forun.

Giao diện ICI (Intercarier Interface) là giao thức liên kết các mạng hoạt động. Như vậy nó định rõ các thủ tục và hoạt động giữa các mạng.

Giao diện trao đổi số liệu DXI (Data exchange Interface) được phát triển bởi ATM Forum, nó cung cấp các thủ tục chuẩn đối với giao diện của thiết bị trong ATM node. The DXI là giao thức rất đơn giản và cho phép di trú vào ATM dễ dàng.

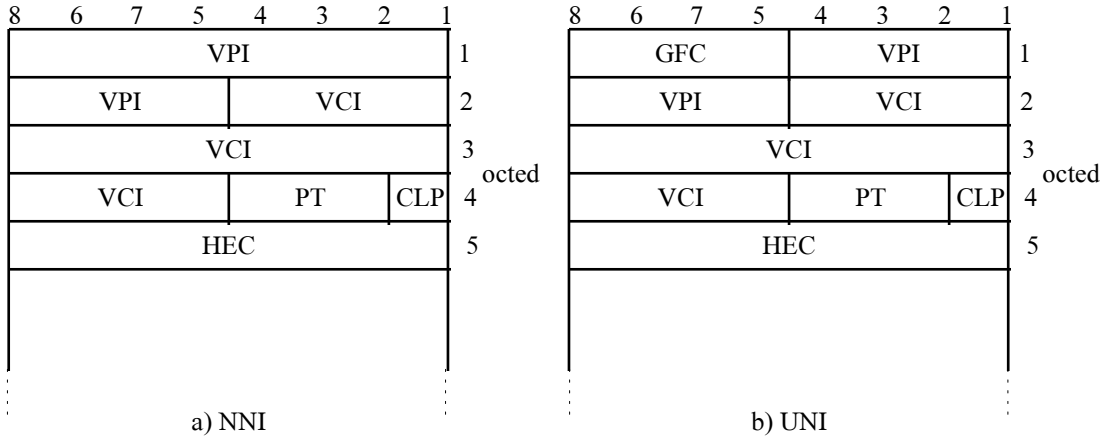
2.4 Cấu trúc tế bào

Tế bào ATM là đơn vị truyền tin cơ bản trong phương pháp truyền tin ATM. Tế bào ATM có cấu trúc gồm 53 byte, 5 byte đầu tiên gọi là tiêu dề (header), 48 byte còn lại là trường thông tin của tế bào ATM.

ATM cell header 5 bytes	ATM cell Information 48 bytes

Hình 3.21: Khuôn dạng tế bào ATM

Phần tiêu đề của tế bào có hai dạng tương ứng với hai giao diện : giao diện giữa người sử dụng và mạng UNI (user - network interface), giao diện giữa các nút mạng NNI (Network node interface). Hình vẽ sau đây sẽ cho ta thấy cấu trúc của tế bào ATM ở hai giao diện UNI và NNI.



Hình 18 : a) Cấu trúc tế bào ở giao diện NNI

b) Cấu trúc tế bào ở giao diện UNI

Sự khác nhau của hai kiểu tế bào này là đối với tế bào ATM ở giao diện NNI thì không có trường GFC. Trong khi đó thì tế bào ở UNI lại có trường GFC. Nhưng bù lại thì trường VPI của tế bào ở giao diện UNI ngắn hơn trường VPI của tế bào ở giao diện NNI.

2.4.1 Trường nhận dạng đưởng dẫn ảo VPI và nhận dạng kênh ảo VCI (Virtual path Identifier và Virtual channel Identifier)

Trường VCI có độ dài là 16 bít nó được dùng để nhận dạng các kênh được truyền đồng thời trên đường truyền dẫn. Do đặc điểm của mạng ATM là hướng liên kết nên mỗi cuộc nối được gán một số liệu nhận dạng VCI tại thời điểm thiết lập. Mỗi giá trị VCI có ý nghĩa tại từng chặng liên kết từ nút đến nút. Khi cuộc nối kết thúc VCI được giải phóng để dùng cho cuộc nối khác. Ngoài ra VCI còn có ưu điểm trong việc sử dụng cho các cuộc nối đa dịch vụ. Thí dụ trong dịch vụ điện thoại truyền hình âm thanh và hình ảnh sẽ được truyền trên hai kênh có VCI riêng biệt do đó ta có thể bổ sung hoặc hủy bỏ một dịch vụ trong khi đang thực hiện một dịch vụ khác.

Trường VPI có độ dài tùy thuộc vào tế bào ATM đang được truyền qua giao diện nào. Đối với giao diện UNI thì VPI có độ dài là 8 bít, đối với giao diện NNI thì VPI có độ dài là 12 bít nó được sử dụng để thiết lập cuộc nối đường ảo cho một số cuộc nối kênh ảo VCC (Virtual channel connection). VPI cho phép đơn giản hóa các thủ tục chọn tuyến cũng như quản lý.

Tổ hợp VPI và VCI tạo thành một giá trị duy nhất cho mỗi cuộc nối. Tùy thuộc vào vị trí tương đối với hai điểm cuối của cuộc nối mà nút chuyển mạch ATM sẽ tạo tuyến dựa trên giá trị của VPI và VCI hay chỉ dựa trên VPI. Tuy vậy cần lưu ý rằng VPI và VCI chỉ có ý nghĩa trên từng chặng liên kết của cuộc nối. Chúng được sử dụng để việc chọn đường dựa trên các chặng này dễ dàng hơn do số VPI và VCI quá nhỏ nên chúng không thể được sử dụng như một số liệu nhận dạng toàn cục vì khả năng xảy ra hai cuộc nối sử dụng ngẫu nhiên cùng số VPI và VCI là rất cao. Để khắc phục điều này người ta cho VPI và VCI là duy nhất trên mỗi đoạn liên kết. Trên từng chặng liên kết này hai nút chuyển mạch sử dụng VPI và VCI như số liệu nhận dạng cho mỗi cuộc nối trên đoạn đó. Khi qua nút chuyển mạch giá trị VCI và VPI nhận giá trị mới phù hợp với đoạn tiếp theo.

2.4.2 Trường ưu tiên mất tế bào CLP (Cell Loss Priority)

Trường này có độ dài là một bít nó dùng để phân biệt mức ưu tiên của các cuộc nối khi các tài nguyên trên mạng khung còn là tối ưu nữa. Ví dụ trong trường hợp quá tải chỉ có các cuộc nối có ưu tiên thấp là bị mất thông tin.

Các mức ưu tiên được ấn định dựa trên cơ sở cuộc nối (qua mỗi VCI hoặc VPI) hoặc trên cơ sở tế bào. Trong trường hợp ưu tiên dựa trên cơ sở cuộc nối tất cả các tế bào thuộc về một đường ảo hoặc kênh ảo sẽ có cùng mức ưu tiên xác định. Trong trường hợp dựa trên cơ sở tế bào. Mỗi tế bào thuộc về một kênh ảo hoặc đường ảo sẽ có mức ưu tiên khác nhau tùy thuộc vào loại tế bào có thêố là tế bào OAM lớp vật lý, tế bào trống, tế bào chỉ định...

Có hai loại ưu tiên đó là ưu tiên về mặt nội dung và ưu tiên về mặt thời gian. Trong chế độ ưu tiên về mặt thời gian thì có vài tế bào có thể có độ trễ trong mạng dài hơn các tế bào khác. Trong chế độ ưu tiên về mặt nội dung thì tế bào nào có độ ưu tiên cao hơn sẽ không bị mất còn các tế bào có độ ưu tiên thấp có thể bị mất.

2.4.3. Trường kiểu tải PT (Payload Type)

Trường này có chiều dài gồm 3 bít từ bít thứ 2 đến bít thứ 4 của Octect thứ 4 trong phần tiêu đề nó được sử dụng để phân biệt loại tải của tế bào như tế bào mang thông tin của người sử dụng, tế bào mạng thông tin về OAM (Operation Administration Maintencance) biừt đầu của trường PT có thể phân biệt được đó là tế bào của người sử dụng hay tế bào OAM.

Nếu có giá trị 0 là tế bào của người sử dụng

Nếu có giá trị 1 là tế bào OAM

Ngoài ra còn có hai kiểu tế bào đặc biệt là tế bào chưa được gán (Unassigned cell) và tế bào rỗi (Free cell). Hai loại này có điểm chung là không mang thông tin của người sử dụng.

2.4.4. Trường điều khiển lỗi tiêu đề HEC (Header Error Control)

Trường này có chiều dài là 8 bít nằm ở Octect thứ 5 của phần tiêu đề tế bào ATM nó chứa mã dự vòng CRC (Cyclic Redundancy Check), mã này cần được kiểm tra và tính toán lại đối với mỗi chặng.bộ mã với đa thức sinh được dùng ở đây là $X^3 + X^2 + X + 1$ có thể sửa toàn bộ lỗi đơn và phát hiện ra phần lớn các lỗi nhóm.

2.4.5. Trường điều khiển luồng chung GFC (Generic Flow Control)

Trường GFC chỉ có trong tế bào ở giao diện giữa người sử dụng và nút mạng, nó có chiều dài 4 bít nằm ở 4 bít cao của Octect đầu tiên của tiêu đề tế bào ATM.

Cơ chế của GFC cho phép điều khiển luồng các cuộc nối ở giao diện UNI, nó được sử dụng để làm giảm tình trạng quá tải trong thời gian ngắn có thể xảy ra trong mạng của người sử dụng. Cơ chế GFC dùng cho cả cuộc nối từ điểm đến điểm (Point to point) và từ điểm đến đa điểm (Point to Multipoint).

Khi kết hợp mạng ATM với mạng khác như DQDB (Distribute queue dual Bus), SMDS (Switch Multi-megabit data Service). GFC đưa ra 4 bít nhằm báo hiệu cho các mạng này làm thế nào để kết hợp kênh các tế bào của các tế bào khác nhau. Mỗi mạng đều có một giao thức truy nhập riêng. Do đó hầu như mỗi mạng đều phải có một logic điều khiển tương ứng dùng GFC cho các giao thức truy nhập của riêng các mạng này.

Do đó trong trường hợp này GFC thực chất là một bộ các giá trị chuẩn để định nghĩa mức độ ưu tiên của ATM đối với các qui luật truy nhập vào các mạng khác nhau.

Việc buộc phải sử dụng trường GFC là một nhược điểm cơ bản của ATM. Nó tạo ra sự khác nhau giữa các tế bào tại các giao diện UNI và NNI do đó giao thức trong ATM không phải là giao thức đồng nhất. Các thiết bị viễn thông có thể được lắp đặt vào bất kỳ trong mạng. Trong khi đó ATM ta phải chú ý xem thiết bị được lắp đặt có thích hợp với giao diện đã cho không.

2.5 Lớp Vật lý (Physical Layer)

Lớp vật lý được tạo lên bởi lớp con môi trường vật lý PM (Physical Medium) và lớp con hội tụ truyền dẫn TC (Transmission Convergence), chức năng của mỗi lớp được mô tả trong bảng 1. Lớp con PM cung cấp thông tin liên quan đến môi trường vật lý và các thông tin thời gian bít và lớp con TC chuyển đổi luồng tế bào ATM thành luồng mã hóa bít dữ liệu.

Chức năng môi trường vật lý :

- *Chức năng PM* (Physical Medium) : Liên quan đến môi trường vật lý để truyền dẫn như sợi quang, phần tử quang bộ nối... Nói tóm lại là chức năng của nó phụ thuộc vào môi trường truyền dẫn cụ thể.

- *Chức năng thông tin thời gian bít* : Chức năng này chuyển đổi luồng bít dữ liệu thành dạng sóng phù hợp môi trường vật lý hoặc ngược lại,và đưa vào hoặc lấy ra các thông tin về thời gian của bít và thực hiện mã hóa và giải mã đường truyền. Như vậy thông tin được chuyển từ phân lớp PM (Physical Medium) sang phân lớp TC (Transmission convergence) bao gồm luồng mã / bít dữ liệu và thông tin thời gian tương ứng.

- *Chức năng tạo và nhận dạng khung* : Chức năng này tạo ra hoặc xác định khung truyền dẫn để ghép các tế bào ATM vào những khung này. Kích thước khung truyền dẫn phụ thuộc vào tốc độ truyền. Trong trường hợp truyền dẫn trong SDH thì cần có khung STM-n (STM-1 : 155,5 Mbit/s, STM-4 : 622 Mbit/s, STM-16 : 2,5 Gbit/s). Trong trường hợp truyền dẫn dựa trên khuyến nghị G.702 cần có khung tín hiệu SD-3. Trong trường hợp truyền dẫn trên cơ sở các tế bào ATM thì chức năng này không cần không có khung truyền dẫn riêng biệt.

- *Chức năng thích ứng khung truyền dẫn* : Chức năng này ghép các tế bào vào những khoảng trống với tải phù hợp của khung truyền dẫn hoặc lấy lại luồng các tế bào từ khung truyền dẫn. Chức năng này chỉ phù hợp với truyền dẫn trên cơ sở SDH hay trên cơ sở khuyến nghị G.702.

- *Chức năng nhận dạng biên của tế bào* : Chức năng này xác định giới hạn của tế bào trong luồng tế bào ATM. Nó thực hiện việc ngẫu nhiên hóa tế bào ATM đối với hướng phát. Xác định và khẳng định đường biên tế bào và thực hiện việc giải ngẫu nhiên luồng tế bào theo hướng ngược lại.

- *Chức năng tạo và xác định tín hiệu Hec* : Chức năng này tạo và xác định tín hiệu Hec (Header Error Control) tín hiệu tiêu đề của tế bào ATM. ở phía phát mã Hec được tạo ra nhờ 4 byte đầu của tế bào ATM trong phần tiêu đề. Kết quả tính toán được đưa vào trong byte thứ 5, giá trị Hec là phần dư của phép chia mô đun 2 của tích 4 octet đầu tiên nhân với x^3 cho đa thức sinh $x^3 + x^2 + x + 1$. Đa thức này có khả năng sửa các

lỗi bít đơn và phát hiện lỗi nhóm ở tiêu đề của tế bào. Theo hướng ngược lại nó kiểm tra tính thích hợp của tín hiệu Hec đối với tín hiệu nhận được trong cùng một quá trình và bỏ qua tế bào nếu phát hiện ra lỗi không sửa được.

- *Chức năng phân định tốc độ tế bào* : Chức năng này thêm các tế bào rỗi để các tế bào ATM có thông tin có ích để tạo ra tốc độ dòng tế bào phù hợp với dung lượng tốc độ của đường truyền dẫn hoặc loại bỏ các tế bào trống để tách các tế bào có dữ liệu.

2.6 Lớp ATM (ATM layer)

Lớp ATM độc lập với lớp vật lý và nó cung cấp các chức năng :

- *Chức năng ghép và tách tế bào* (Cell Multiplexing and Demultiplexing Funtion). Chức năng này ghép các tế bào ATM với các đường ảo VP (Virtual path) và các kênh ảo VC (Virtual channel) để tạo nên dòng tế bào tổng hợp hoặc ngược lại cung cấp các chức năng tách các tế bào.

- *Chức năng biên dịch VCI / VPI của tế bào* (Cell VPI / VCI translation Function) : Chức năng này được yêu cầu đối với tổng đài ATM hay các nút liên kết chéo ATM (ATM cross link mode). Nó ghép giá trị mới vào các giá trị trong trường VPI / VCI trống. Tại nút chuyển mạch ATM cả giá trị VPI / VCI đều thay đổi. Còn tại bộ nối xuyên thì chỉ có giá trị VPI bị thay đổi.

- *Chức năng tạo và tháo phần tiêu đề của tế bào* (Cell Header generation and extraction Function) : Chức năng này được dùng cho điểm xác định lớp ATM để tạo và tách 4 byte đầu của phần tiêu đề tế bào ATM. Nó ghép các thông tin thu được từ lớp cao vào các trường tương ứng đối với việc tạo tiêu đề tế bào và thực hiện việc ngược lại đối với việc tách phần tiêu đề của tế bào. Ngoài ra nó còn dịch tín hiệu nhận dạng điểm truy nhập dịch vụ SAPI (Service access point Identifier) thành tín hiệu VPI và VCI.

- *Chức năng điều khiển luồng chung* (General flow control Function) : Chức năng này điều khiển việc truy cập và luồng thông tin trong UNI. Nó cung cấp các giao thức điều khiển luồng thông tin tới từ mạng của người sử dụng CN (Customer Network) hoặc từ thuê bao. GFC còn có thể dùng để giảm bớt tình trạng quá tải tức thời của mạng.

2.7 Lớp phối hợp ATM (AAL : ATM adaptation layer)

Lớp phối hợp ATM (ATM adaptation layer) được hình thành bởi hai lớp con : *lớp con thiết lập và tháo tế bào* SAR (Segmentation and Reasseenbly) và *lớp con hội tụ* CS (Convergence Sub-layer). SAR có chức năng là chia các PDU của lớp cao hơn thành các phần tương ứng 48 byte của trường dữ liệu của tế bào ATM và ngược lại. CS tạo ra CS-PDU từ thông tin dịch vụ khách hàng lớp cao hơn và ngược lại. Mặt khác nó còn cung cấp các dịch vụ của AAL cho lớp cao hơn thông qua điểm truy nhập dịch vụ SAP (Servive access point).

Khi thiết lập kết nối, máy chủ phải xác định giao thức lớp phối hợp để sử dụng. Cả hai đầu cuối của kết nối phải chấp nhận theo giao thức đã lựa chọn và lớp phối hợp không thể thay đổi được mỗi khi kết nối đã được thiết lập.

2.7.1. Tạo và xử lý the AAL - PDU (Creating and Procesing the AAL-PDU)

Theo hình mô tả thì AAL có trách nhiệm nhận U-SDU có kích thước từ một đến vài ngàn octect thông qua điểm truy nhập dịch vụ AAL-SAP và thêm các phần đuôi

(trailer) và tiêu đề (header) có thể có các octect đệm vào đầu và cuối của U-SDU để trở thành CS-PDU có kích thước là bội số của 48. Chiều dài của tiêu đề(header) và phần đuôi (trailer) phụ thuộc vào công nghê.

Sau đó CS-PDU được phân thành những đơn vị số liệu có kích thước từ 44 đến 47 octect. Sự thay đổi này phụ thuộc vào loại dữ liệu như tiếng nói, video, data... sau đó tiếp tục đưa thêm các phần đuôi (trailer) và tiêu đề (header) vào các đơn vị số liệu này và cuối cùng thành SAR-PDU 48 octect.

Các SAR-PDU được đưa qua lớp ATM thông qua điểm truy nhập dịch vụ ATM-SAP và lớp ATM đưa thêm 5 byte tiêu đề vào dữ liệu này thành tế bào ATM 53 byte.

2.7.2. Phân loại

Tùy theo các đặc điểm dịch vụ của nó mà người ta có thể phân chia AAL thành các loại khác nhau. Các dịch vụ được phân thành bốn loại A, B, C, D về đặc điểm của từng loại được tóm tắt trong bảng sau đây :

	Nhóm A	Nhóm B	Nhóm C	Nhóm D
Mối quan hệ thời gian giữa nguồn và đích	Yêu cầu thời gian thực		Không yêu cầu thời gian thực	
Tốc độ truyền	Không đổi	Thay đổi		
Kiểu liên kết	Hướng liên kết			Không liên kết

Bảng 4 : Các nhóm dịch vụ

Tương ứng với bốn loại dịch vụ ta cũng có bốn loại AAL khác nhau :

AAL-1, AAL-2, AAL-3, AAL-4

AAL-1 cung cấp chức năng AAL cho các dịch vụ A yêu cầu thời gian thực, tốc độ truyền không đổi kiểu truyền hướng liên kết, Các dịch vụ này thuộc về loại thường là tiếng nói, tín hiệu video có tốc độ không đổi bảo đảm cho truyền dẫn tín hiệu hình không bị dừng tĩnh hoặc rung.

AAL-2 cung cấp chức năng AAL cho các dịch vụ thuộc loại B : Tốc độ truyền thay đổi, thời gian thực, kiểu hướng liên kết các dịch vụ thuộc loại này thường là audio và video có tốc độ thay đổi.

AAL-3 cung cấp chức năng AAL cho các dịch vụ thuộc loại C : Không yêu cầu thời gian thực, tốc độ truyền thay đổi, phương pháp truyền hướng liên kết. Nó phục vụ cho các dịch vụ truyền số liệu hướng liên kết và báo hiệu.

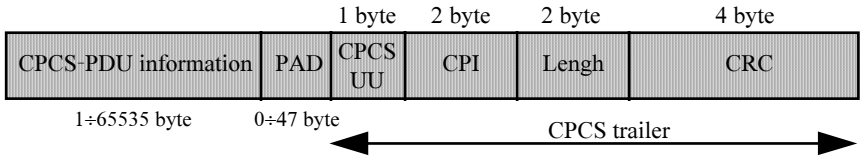
AAL-4 cung cấp chức năng AAL cho các dịch vụ thuộc loại D : Không yêu cầu thời gian thực, tốc độ truyền thay đổi, kiểu truyền không liên kết.

Tuy nhiên, AAL-3 và AAL-4 được kết hợp lại thành AAL-3/4 vì chúng tương tự ở nhiều điểm và nó cung cấp các dịch vụ loại C và D và AAL-5 được đưa thêm vào, nó đơn giản hóa chức năng AAL-3/4 để cung cấp thông tin tốc độ cao, không theo thời gian thực. Điểm khác nhau chính của hai loại này là AAL-5 không đưa ra khả năng phân hợp kênh, do đó không có trường MID chủ yếu được sử dụng cho báo hiệu trong mạng ATM.

Để chuyển các gói dữ liệu không qua mạng. Mặc dù ATM sử dụng các tế bào có kích thước nhỏ cố định ở mức thấp nhất, AAL-5 đưa ra một giao tiếp để nhận và phân

phát gói dữ liệu có kích thước lớn và độ dài thay đổi. Cụ thể, AAL-5 cho phép mỗi gói chứa từ 1 đến 65535 byte dữ liệu, xem (hình 19)

Cấu trúc của AAL-5 (Structure of an AAL-5 CPCS-PDU) :



Hình 3.21: Cấu trúc của CPCS-SDU AAL-5

CPCS-PDU AAL-5 bao gồm trường thông tin có chiều dài thay đổi từ 1 - 65535 byte, trường đệm 1 - 47 byte và 8 byte phần đuôi (trailer).

- Trường đệm (the padding field) : Chiều dài của CPCS-PDU AAL-5 là tạo nên số của bội 48 byte bằng cách chèn 0 ÷ 47 byte đệm.

- Trường length : Trường chỉ thị chiều dài, chỉ thị chiều dài của trường thông tin CPCS nó bao gồm 2 byte và có thể chiếm giữ các giá trị từ 1 đến 65535. CPCS-PDUs với giá trị trường chiều dài là 0 là "PDUs không hợp pháp" (Abort PDUs), chỉ thị rằng chuyển giao CPCS SDU hiện hành là không hợp pháp.

Mỗi gói AAL-5 sẽ được chia thành các tế bào để chuyển tải qua mạng ATM và tổ hợp lại thành gói trước khi trao cho máy chủ nhận. Nếu gói có kích thước không phải là bội số của 48 byte thì tế bào cuối cùng sẽ không đầy. Để kết hợp các gói có độ dài tùy ý. AAL-5 cho phép tế bào cuối cùng chứa từ 0 đến 40 byte dữ liệu, tiếp theo là các số zeso đệm thêm và cuối cùng là 8-byte trailer. Nói cách khác AAL-5 đặt trailet ở 8 byte cuối cùng, để có thể tách trailer dễ dàng mà không cần biết độ dài của gói.

CHƯƠNG 5

TẦNG GIAO VẬN

I. VAI TRÒ VÀ CHỨC NĂNG CỦA TẦNG GIAO VẬN

Trong mô hình OSI, người ta thường phân biệt 4 tầng thấp (Physical, Data Link, Network, Transport) và ba tầng cao (Session, Presention, Application). Các tầng thấp quan tâm đến việc truyền dữ liệu giữa các hệ thống cuối qua phương tiện truyền thông, còn các tầng cao tập trung đáp ứng các yêu cầu và các ứng dụng của người sử dụng. Tầng Giao Vận là tầng cao nhất của nhóm các tầng thấp, mục đích của nó là cung cấp dịch vụ truyền dữ liệu sao cho các chi tiết cụ thể của phương tiện truyền thông được sử dụng ở bên dưới trở nên "trong *suốt"* đối với tầng cao. Nói cách khác, có thể hình dung tầng Giao Vận như một □*bức màn*□ che phủ toàn bộ hoạt động các tầng thấp bên dưới nó. Từ đó, nhiệm vụ của tânửg Giao Vận rất phức tạp. Nó phải được tính đến khả năng thích ứng với một phạm vi rất rộng các đặc trưng của mạng. Chẳng hạn một mạng có thể □*có liên kết*□ hoặc □*không liên kết*□ , có thể tin cậy hoặc có thể chưa tin cậy ... Nó phải biết được yêu cầu về chất lượng dịch vụ của người sử dụng, đồng thời cũng phải biết được khả năng cung cấp dịch vụ của mạng bên dưới. Chất lượng của các dịch vụ mạng tùy thuộc vào các loại mạng khả dụng cho tầng Giao Vận và cho người sử dụng cuối. CCITT và ISO đã định nghĩa ba loại mạng sau đây:

- 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 Giao Vận 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 lỗi hay sự cố.

- Mạng loại C: Có tỷ suất lỗi không chấp nhận được (không tin cậy). Tầng Giao vận phải có khả năng phục hồi lại khi xảy ra lỗi và sắp xếp lại thứ tự các gói tin.

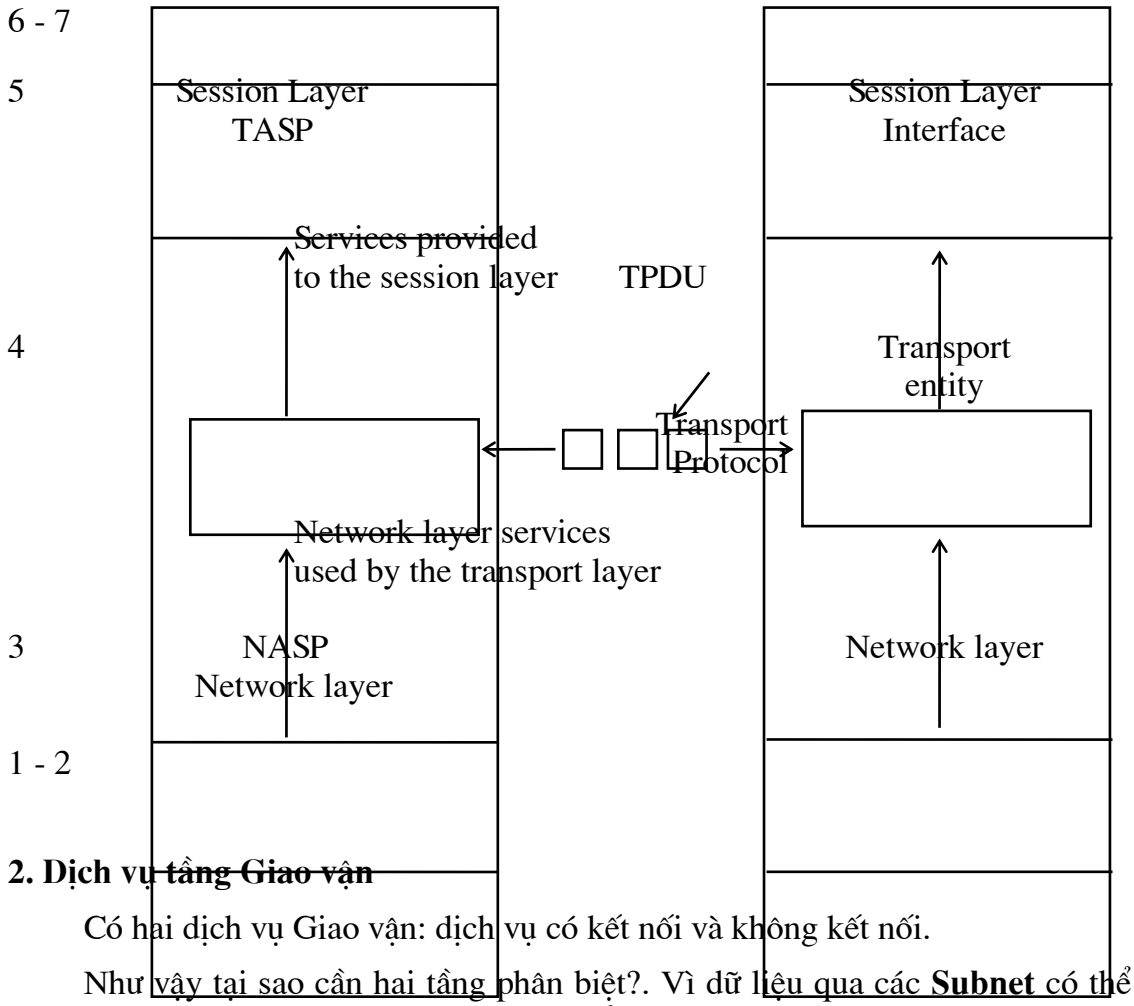
Rõ ràng là với mạng loại A thì công việc của tầng Giao vận sẽ dễ dàng hơn. Tuy nhiên, điều không may là rất nhiều mạng lại chỉ có được chất lượng dịch vụ của mạng loại B và loại C. Do vậy, khi xác định dịch vụ và giao thức cho tầng Giao vận cần phải quan tâm đến cả những trường hợp chất lượng dịch vụ mạng là xấu nhất. Và nhiệm vụ của tầng Giao vận là phải lựa chọn được dịch vụ và giao thức Giao vận thích hợp với loại mạng cho trước.

II. CÁC DỊCH VỤ CUNG CẤP CHO TẦNG 5 (SESSION LAYER)

1. Quan hệ giữa tầng 3, 4, 5

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 mềm trong tầng 4 để thực hiện công việc coi là transport entity. Mối quan hệ giữa các lớp 3, 4, 5 được mô tả bởi hình sau:

A **B**



2. Dịch vụ tầng Giao vận

Có hai dịch vụ Giao vận: dịch vụ có kết nối và không kết nối.

Như vậy tại sao cần hai tầng phân biệt?. Vì dữ liệu qua các **Subnet** có thể bị 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 tầng ba để cải thiện chất lượng dịch vụ. Nếu giữa chừng một tầng Giao vận được thông báo là kết nối mạng bị kết thúc đột ngột và không biết được sự cố gì đã xảy ra, nó có thể thiết lập một kết nối mới ở lớp mạng tới tầng Giao vận ở xa và gởi yêu cầu hỏi số liệu nào đến, số liệu nào không từ đó biết được sai sót xảy ra ở đâu. Tầng 4 có thể phát hiện mất gói tin, số liệu bị biến đổi ở lớp mạng.

3. Các hàm cơ bản của dịch vụ Giao Vận

3.1 Các chuẩn cho giao thức và dịch vụ Giao Vận trong trường hợp có liên kết

T-CONNECT request (callce, caller, exp_wanted, qos, uses_data).

T-CONNECT indication (callce, caller, exp_wanted, qos, uses_data).

T-CONNECT, uses_data **response** (responder, exp_wanted, qos).

T-CONNECT confirmation (responder, exp_wanted, qos, uses_data)

T-DISCONNECT request (uses_data)

T-DISCONNECT indication (reason, user_data).

T-DATA request (user_data).

T-DATA indication (user_data).

T - EXPEDITED - DATA request(user_data).

T - EXPEDITED - DATA indication(user_data).

ISO cũng đã công bố các chuẩn cho dịch vụ này là: ISO 8027/DAD

3.2 Các giao thức (ISO 8620) cho tầng Giao Vận không liên kết

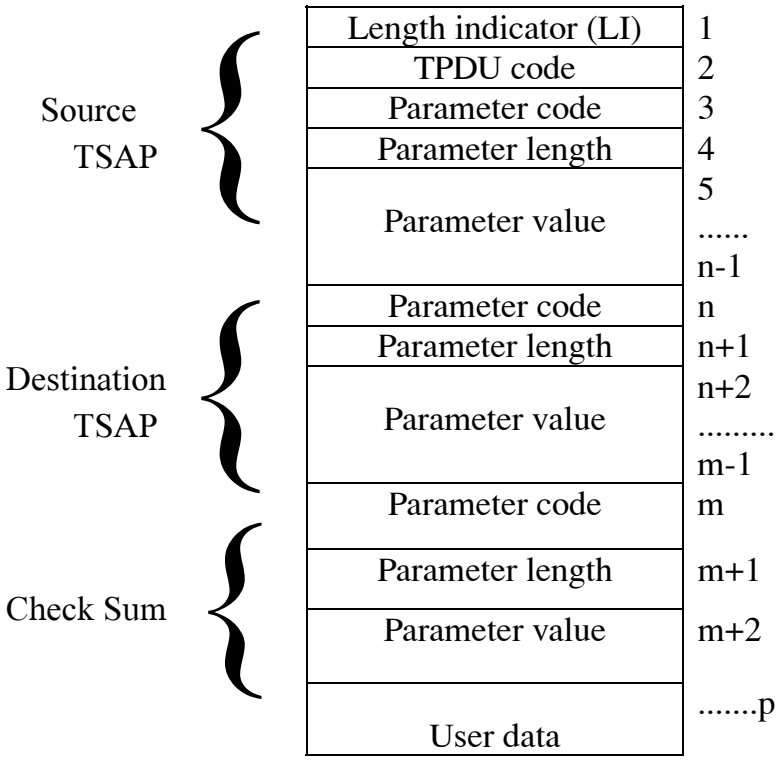
Về dịch vụ, chỉ có 2 Priminitives đó là

T-unitdata.request (Source address, Dest address, Quality of service, Ts-user data).

T-unitdata.indication (Source address, Dest address, Quality of service, Ts-user data). Trong đó các địa chỉ nguồn và đích (Source address, Destination address) định danh một cách duy nhất các điểm truy nhập dịch vụ Giao vận (TSAP), còn các tham số của ***chất lượng dịch vụ (***Quality of service) bao gồm:

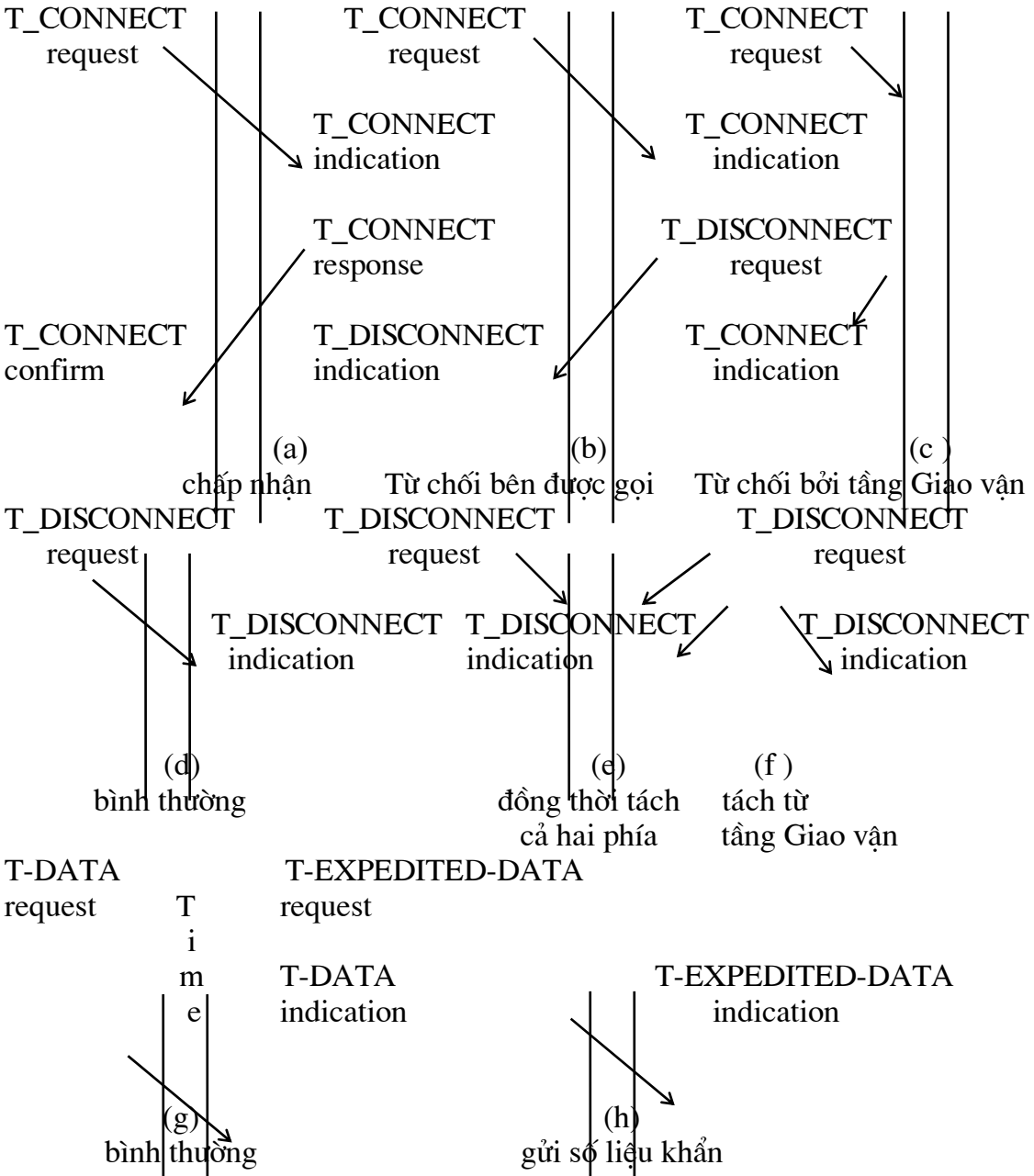
- Độ trễ truyền dẫn (Transit delay).
- Bảo vệ tránh các truy nhập bất hợp pháp (Protection).
- Xác suất lỗi (residual error probabillity).
- Độ ưu tiên (Priority).

Về giao thức, chỉ có duy nhất một đơn vị dữ liệu (TPDU) được dùng, đó là UNITDATA (viết tắt là UD). Khuôn dạng của UD được thể hiện như hình sau:



So sánh các hàm cơ bản của dịch vụ Giao vận và dịch vụ mạng, ta thấy dịch vụ Giao vận và dịch vụ mạng là giống nhau. Mặc dù vậy, sự khác nhau là dịch vụ mạng cho phép người sử dụng xử lý Acknowledement và N-reset. Ngược lại dịch vụ Giao vận

không quan tâm đến vì dịch vụ lớp Giao vận là tin cậy, không có lỗi. Và dịch vụ mạng được dùng bởi lớp Giao vận.



ở 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 này, không có gì được phát qua mạng vì vậy đầu kia không nghe được gì cả.

III. CHẤT LƯỢNG DỊCH VỤ

Chức năng cơ bản của tầng 4 là tăng cường chất lượng dịch vụ được cung cấp bởi tầng 3. Nếu lớp mạng chất lượng chưa tốt, lớp Giao vận sẽ bổ sung. QOS được đặc trưng bởi một số tham số đặc biệt.

- *Thời gian thiết lập liên kết* là thời gian từ khi gửi yếu cầu tới thời điểm nhận được xác nhận liên kết.

- *Xác xuất 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 1 giây.

Theo cách tính: * Trong một cuộc trao đổi.

* Khả năng của mạng/ theo hai chiều.

- *Thời gian chuyển tiếp* là thời gian giữa thời điểm người sử dụng dịch vụ của tầng liên vận gửi một tin báo và thời điểm thực thể của tầng Giao Vận trạm thu nhận được. Đánh giá theo hai chiều.

- *Tỷ lệ lỗi* là tỷ số giữa tin báo bị lỗi (mất) trên tổng số tin báo được truyền trong một chu kỳ đỉnh trước.

- *Xác xuất sự cố truyền*: tỷ số giữa thời gian có sự cố trong một chu kỳ quan sát.

- *Thời gian hủy liên kết* là thời gian từ khi một người sử dụng phát yêu cầu hủy liên kết đến khi liên kết được hủy thật sự tại đầu cuối từ xa.

- *Xác xuất lỗi khi hủy liên kết* là tỷ số yêu cầu hủy liên kết không được thực hiện trong thời gian lớn nhất.

- *Khả năng bảo vệ* là khả năng của người sử dụng cấm thiết bị đầu cuối bên ngoài chen vào hay giao thoa trên đường dây dọc hay thay đổi số liệu truyền.

- *Thông số ưu tiên* cho phép người sử dụng có quyền ưu tiên cao hơn được phục vụ dối với một liên kết.

- *Thông số hủy bỏ* để tầng Giao Vận tự quyết định hủy liên kết do 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 hay tối thiểu tới tầng liên vận và bắt đầu quá trình đàm thoại về các tham số đó.

IV. CÁC LỚP GIAO THỨC CỦA TẦNG GIAO VẬN

1. Yêu cầu

Các dịch vụ tầng Giao vận được bảo đảm bằng cách giao thức giữa hai 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 đảm bảo trình tự bản tin.

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

Tầng Giao Vận đòi hỏi khả năng lưu trữ trong SubNet để giữ những gói tin bị trục trặc và đòi hỏi thủ tục đặc biệt.

ở tầng Giao Vận, số các kết nối lớn hơn nên các vấn đề Buffering và Flow Control phức tạp hơn.

Từ quan điểm thiết lập thủ tục Giao Vận, các tính chất thực tế của SubNet ít quan trọng hơn các dịch vụ được cho bởi mạng, mặc dù cái sau ít bị ảnh hưởng mạnh bởi cái trước. Tuy vậy, đến chừng mực nào đó, dịch vụ mức mạng có thể che những mặt ít được chú ý của SubNet và cung cấp ghép nối tốt hơn.

2. Lớp giao thức

Dịch vụ mạng xấu thì giao thức của tầng Giao vận sẽ phức tạp hơn. OSI đã tính đến vấn đề này và chia giao thức của tầng Giao vận thành năm lớp.

Lớp 0:. Lớp mạng đơn giản, kết nối mạng khi có yêu cầu Giao vận không giải quyết lỗi. Chủ yếu tạo ra trình tự, điều khiển dòng dữ liệu để làm cho tầng mạng hoạt động tốt hơn. Bao gồm cơ cấu thiết lập và hủy liên kết ở tầng giao diện.

Lớp 1:Các tính chất tương tự lớp 0, ngoài ra còn thêm:

. Khởi động lại mạng sau khi N_RESET.

. 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.

Lớp 2: Là phiên bản của lớp 0 và được xây dựng cho mạng tin cậy, nhiều kết nối 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.

Lớp 3:Là tổ hợp lớp 1 và lớp 2. Cho phép dồn kênh, khởi động lại, điều khiển dòng dữ liệu.

Lớp 4: Phải có biện pháp giải quyết vấn đề mất gói tin và các gói tin bị hỏng đồng thời có giải quyết yêu cầu khởi động lại, chọn lớp giao thức sẽ được thực hiện mỗi khi thiết lập liên kết

V. THỦ TỤC GIAO VẬN TRÊN X.25

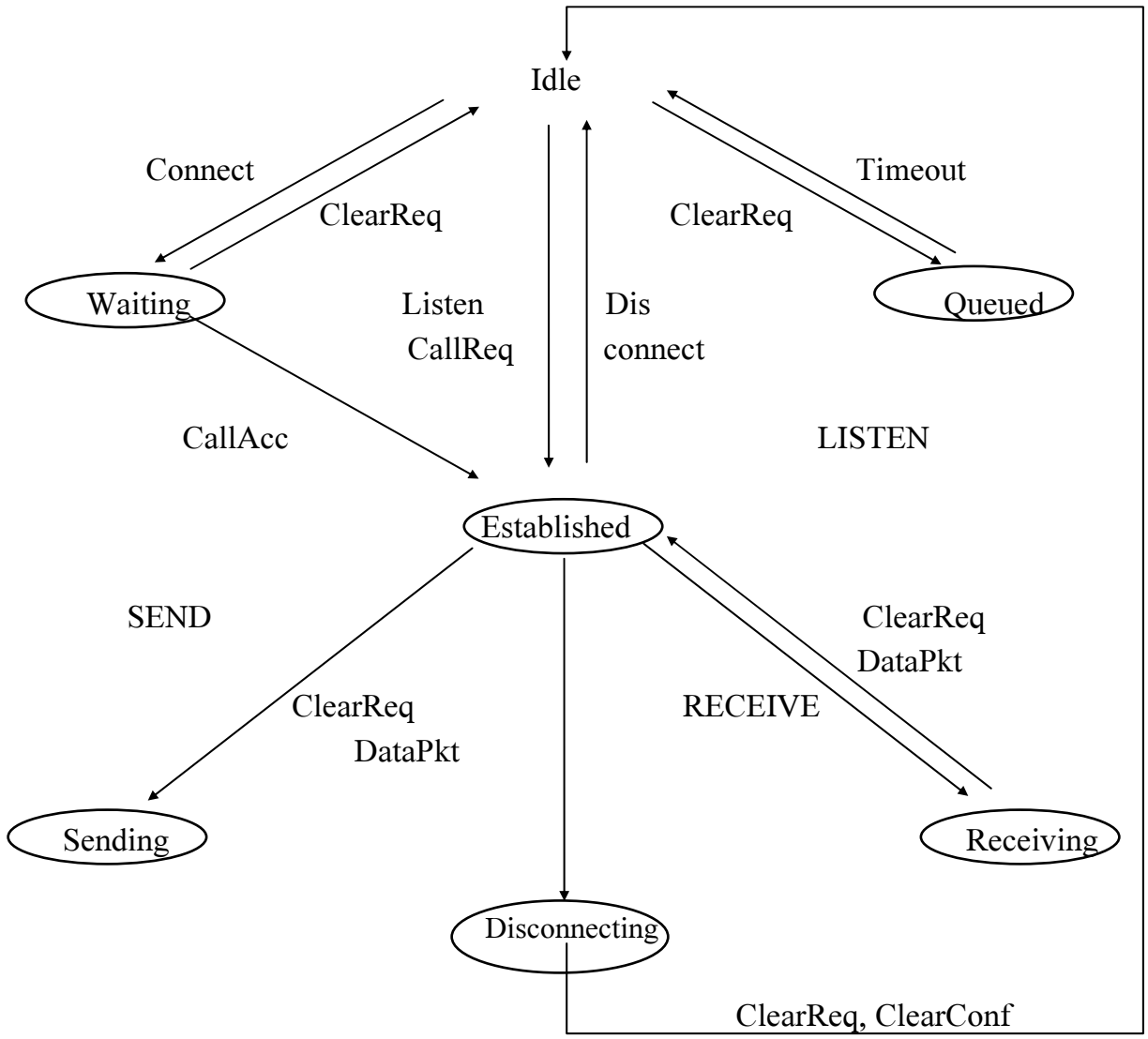
1. Quá trình nối-tách và trao đổi số liệu

Mỗi kết nối được duy trì ở tầng giao vận luôn ở trong một của 7 trạng thái sau:

1. Idle: kết nối chưa được thiết lập
2. Waiting: yêu cầu kết nối đã tiến hành và chờ trả lời
3. Queuced: yêu cầu kết nối đến và chờ nghe (nhấc máy)
4. Established: kết nối đã được thiết lập
5. Sending: chờ biên nhận để phát tin tiếp.
6. Receiving: nhận tin
7. Disconnecting: chờ tách

Quá độ giữa các trạng thái xảy ra khi thực hiện các hàm dịch vụ cơ bản hoặc có gói tin đến hay TimeOut. Quá độ giữa các trạng thái được thể hiện trên bảng trạng thái hay đồ thị trạng thái. Đó là cơ sở cho viết chương trình thực hiện thủ tục giao vận trên X.25.

2. Đồ thị trạng thái của thủ tục giao vận trên X.25



Hình 3.16 Đồ thị trạng thái của thủ tục giao vận trên X.25

Giải thích đồ thị trạng thái.

Idle: (Khi hệ thống chưa nối)

Connect: phát CallReq và sang Waiting (chờ câu trả lời)

Listen: đang đợi CallReq thì phát CallAcc và sang Estab (nối)

CallReq: đang đợi nghe thì sang Estab, ngược lại thì sang Queued (đợi trả lời) Start Timer

Waiting: (chờ câu trả lời)

CallAcc thì sang Estab

ClearReq thì về Idlc

Queued: (tìm người trả lời)

Listen (có người nghe) thì sang Estab

TimeOut thì về Idle

Estab (hệ thống đã được nối)

SEND: đã có credit (biên nhận) thì gửi tin, chưa có credit thì sang Sending

RECEIVE: gửi credit và sang Receiving

Disconnect: đang đợi giải quyết ClearREQ thì phát ClearConf và về Idle, ngược lại sang Disconnecting

ClearReq: đặt cờ ClrReq và ở lại Estab

Credit: ghi nhận credit và ở lại Estab

Sending (chờ credit để phát tin)

Credit: gửi tin và về Estab

ClearReq: đặt cờ ChReq và về Estab

Disconnecting (chờ tách)

ClearReq: về Idle

ClearConf: về Idle

VI. NHẬN XÉT VÀ ĐÁNH GIÁ

1. Những đơn vị dữ liệu giao thức

Sự khác nhau quan trọng giữa mô hình OSI và TCP/IP là khác nhau về thuật ngữ sử dụng mô tả dữ liệu tại mỗi lớp.

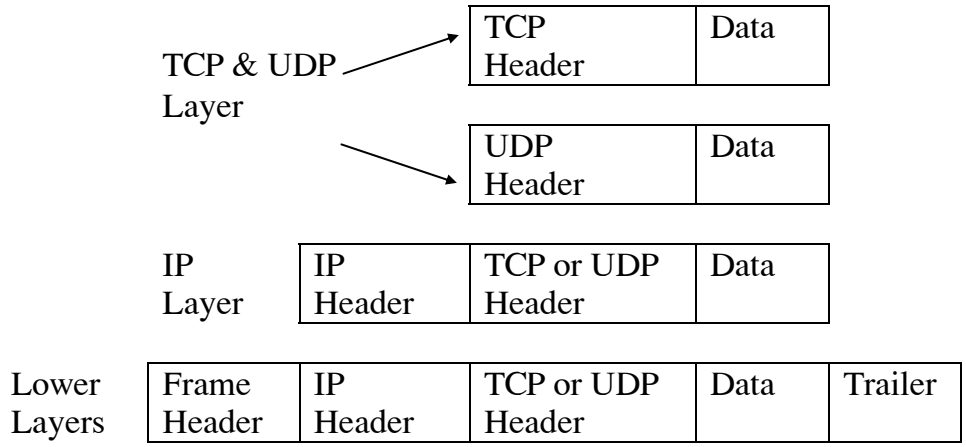
Mô hình OSI sử dụng từ *đơn vị dữ liệu giao thức (PDU: Protocol Data Unit)* tầng thứ N chỉ cho đơn vị thông tin mà giao thức tầng thứ N giải quyết. Một đơn vị dữ liệu giao thức PDU gồm một phần đầu (Header) và một số dữ liệu được tùy chọn được đóng vào.

Bộ giao thức TCP/IP sử dụng đơn vị dữ liệu *segment* cho giao thức TCP, *User Datagram* cho giao thức UDP và *Datagram* cho giao thức IP. Những phần đầu được thêm vào lần lượt tại mỗi lớp để định kiểu PDU của nó. Dữ liệu người sử dụng được gửi qua đến tầng TCP hoặc tầng giao thức UDP.

Một phần Header của một Segment của tầng TCP chứa thông tin như là: Một *số thứ tự* sử dụng để giữ dữ liệu theo thứ tự, *một ACK* cho việc nhận dữ liệu, và thông tin nhận dạng những ứng dụng đang gửi và nhận trên kết nối.

Một phần Header của PDU của tầng UDP chứa những vùng *nhận dạng* những ứng dụng UDP đang nhận và gửi.

Một phần Header của PDU của tầng giao thức IP chứa thông tin về *địa chỉ mạng của nguồn và đích* cho dữ liệu.



Hình 3.25: Những phần đầu (header) của PDU.

Một đơn vị dữ liệu giao thức tầng thấp thì được gọi là *khung (frame).* Phần đầu (Header) của một khung chứa những vùng xác định những thiết bị vật lý nguồn và đích.

Trong vài trường hợp cá biệt, phần đầu sẽ được theo sau bởi một header thứ hai được gọi là *header LLC (Logical Link Contol*) hoặc header liên kết dữ liệu

Frame Header	Data Link Header	IP Header	TCP Header	Frame Check Sequence

Hình 3.26: Đầy đủ bộ Header của PDU

Hầu hết các khung chứa đựng một header và một Trailer. Trailer chứa mộŸt vùng FCS (Frame check sequence) sử dụng để phát hiện những lỗi truyền dẫn. Vùng FCS chứa đựng kết quả của một phép tóan mà người gửi thực hiện trên những bít của một thông báo, người nhận sẽ thực hiện phép tính giống như vậy và so sánh kết quả với giá trị ở trên Trailer. Kết quả của phép toán được tách ra nếu những giá trị phù hợp nhau thì chắc chắn dữ liệu đã được bảo quản tòan vẹn trong suốt quá trình truyền.

2. So sánh chế độ truyền bất đồng bộ với chế độ truyền đồng bộ

ATM được đánh giá là công nghệ tiên tiến nhất hiện nay. Nó được coi là nền tảng của mạng B-ISDN với những ưu điểm của nó. Nó có thể phục vụ được tất cả các dịch vụ hiện nay và trong tương lai. Để thấy được điều đó ta hãy xem xét ATM với công nghệ đang sử dụng hiện nay STM (Synchronous Transfer Mode).

2.1. Chế độ truyền dẫn đồng bộ STM (Synchronous Transfer Mode)

- Phân bố một khe thời gian trong một khung cho dịch vụ trong thời gian của cuộc gọi.

- Toàn bộ kênh STM được xác định bởi vị trí các khe thời gian của nó trong một khung.

- Khi một khe thời gian đã được chỉ định cho một kênh nào đó, nó sẽ được dành riêng cho kênh đó trong suốt thời gian của cuộc gọi. Điều này đảm bảo cung cấp dịch vụ cho người sử dụng và cũng đủ cho các dịch vụ tạo ra thông tin liên lạc với tốc độ cố định. Nhưng *nhược điểm* là hiệu suất sử dụng băng thông thấp khi nguồn tin không tạo ra thông tin liên tục ở một tốc độ cố định.

- Hơn nữa cấu trúc cứng nhắc của STM không linh hoạt lắm cho việc phân bổ băng thông cần thiết cho nhiều loại dịch vụ khác nhau trong B-ISDN. Mặc dù có thể phân bổ linh hoạt các bộ khe thời gian đối với một kênh cho các dịch vụ chuyển mạch khác nhau. STM yêu cầu sự phối hợp các chức năng ánh xạ khá phức tạp tại các giao diện giữa người sử dụng và mạng ở cả hai phía.

Để đơn giản hóa chức năng ánh xạ này thì STM có thể có cấu trúc phù hợp để phục vụ cho các kênh có tốc độ khác nhau. Điều này được thực hiện bằng cách : chia một khung thành các bộ có số khe thời gian cố định khác nhau nhưng cần phải nói rằng việc tìm ra các khe thời gian chuẩn cho các kênh đa tốc độ không phải là dễ vì cho đến nay các dịch vụ mạng mà B-ISDN sẽ cung cấp vẫn chưa được xác định hoàn chỉnh.

- Kiểu STM đa tốc độ còn làm phức tạp hóa hệ thống chuyển mạch vì có thể phải dùng một cấu trúc chuyển mạch riêng cho mỗi tốc độ kênh ,dẫn đến có nhiều cấu trúc chuyển mạch khác nhau trong hệ thống làm phức tạp công tác vận hành, bảo dưỡng mạng. Chính vì hạn chế bởi băng thông cố định đã làm cho STM khó có thể mang nhiều dịch vụ hỗn hợp thay đổi liên tục với nhiều tốc độ cố định khác nhau. Nên STM không phù hợp cho mạng số B-ISDN phục vụ thông tin đa thể loại.

2.2. Chế độ truyền dẫn không đồng bộ ATM (Asynchronous Transfer Mode)

- ATM được coi là cơ sở của mạng số đa dịch vụ băng rộng B-ISDN, là mạng phục vụ thông tin đa thể loại trong tương lai. Nó cho băng thông rộng, thời gian trễ nhỏ, sử dụng kỹ thuật chuyển mạch giống với chuyển mạch gói và cả kỹ thuật ghép kênh.

- ATM phân bổ băng thông theo yêu cầu do đó mở ra khả năng sử dụng băng thông hết sức hiệu quả và linh hoạt.

- Kỹ thuật ATM chia dòng bit thông tin thành các gói gọi là tế bào có độ dài cố định. Mỗi tế bào gồm phần tiêu đề để mang thông tin điều khiển mạng và trường thông tin mang thông tin của người sử dụng.

- Không giống kỹ thuật STM phân biệt các cuộc gọi nhờ vị trí của khe thời gian trong khung, ATM liên hệ các tế bào tin với các cuộc gọi nhờ nhãn trong trường tiêu đề của tế bào tin đó.

- Các cuộc nối được thiết lập nhờ các bảng dịch tại các tổng đài và các điểm ghép kênh, ở đó đối chiếu nhãn của tế bào tin với tuyến ra và nhãn ra. Cuộc nối theo nhu cầu này được gọi là kênh ảo vì nó không phân bố băng thông trong toàn bộ thời gian của cuộc gọi.

- Thuật ngữ không đồng bộ trong ATM không ám chỉ sự không đồng bộ của khía cạnh không có tính chu kỳ về thứ tự của các thông tin riêng biệt mà chúng tạo thành một kênh ATM gồm nhiều loại thông tin khác nhau như thoại, số liệu, hình ảnh,... vì một nguồn sinh ra các tế bào tin theo tốc độ dịch vụ của nó nên không cần phải cố định tốc độ kênh. Chính vì vậy mà chỉ cần một loại cấu trúc chuyển mạch cho tất cả các loại dịch vụ.

- Các tế bào tin có độ dài cố định cũng làm giảm việc xử lý và đồng bộ các tế bào tin.

ATM còn được gọi là hệ thống chuyển mạch gói nhanh là công nghệ chuyển mạch mới.

CHƯƠNG 6

MẠNG CỤC BỘ

I. GIớI THIệU

Khi mạng mở rộng chúng ta phải kết nối các mạng LAN riêng biệt nhằm cung cấp một mạng máy tính hợp nhất. Công nghệ mạng LAN (Local Area Network), cung cấp tính năng cao, nhưng chúng chỉ thích hợp sử dụng trong phạm vi địa lý giới hạn.

Nếu kết nối với khoảng cách dài hơn thường đượỹc dùng mạng WAN, do đó việc nghiên cứu các phương thức giao tiếp là cần thiết nhằm đánh gía đúng hiệu quả sử dụng trong môi trường hiện nay.

Sự khác nhau chủ yếu giữa một đường thông tin được thiết lập thông qua LAN có tốc độ truyền dẫn số liệu cao hơn nhiều so với một kết nối được thiết lập thông qua một mạng số liệu công cộng vì khoảng cách địa lý tương đối ngắn.

Tuy nhiên, theo mô hình tham chiếu OSI của tổ chức ISO, sự khác nhau này chỉ thể hiện ở các lớp thấp phụ thuộc mạng (physical, datalink, network), trong nhiều trường hợp khác các lớp giao thức lớp cao trong mô hình tham chiếu (application, presentation, session) thường giống nhau đối với các kiểu mạng.

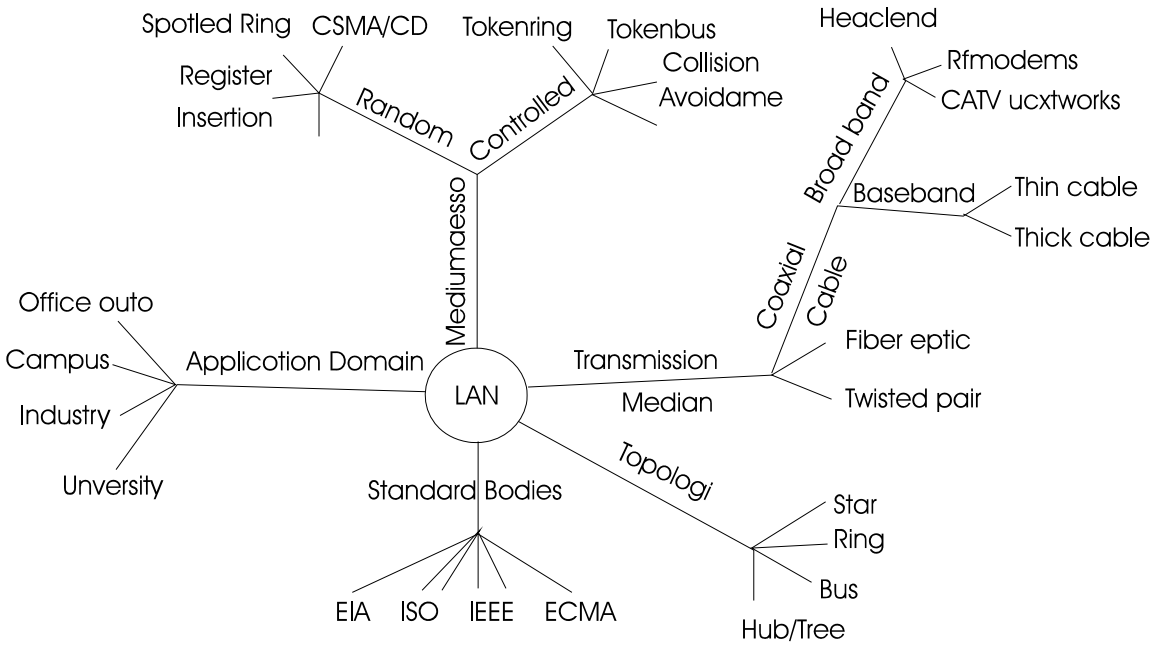
Đặc điểm chính của mạng cục bộ:

- 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 xuất lỗi rất thấp đạt tới 10^{-11}.

Qủan lý khai thác mạng hòan tòan tập trung, thống nhất. Xuất phát từ những đặc trưng trên, kiến trúc mạng cục bộ cũng có những đặc thù riêng.

Trong những năm trước đây những kỹ thuật mới được áp dụng trong công nghệ nối mạng LAN, WAN. Tốc độ T1 và các kỹ thuật của ISDN, Frame Relay, ATM dịch vụ chuyển mạch dữ liệu tốc độ Multimegabit đã hứa hẹn sự kết nối vùng diện rộng nhanh hơn.

*** Sơ đồ mạng LAN**



Hình 6.1. Sơ đồ tóm tắt mạng cục bộ

II. CÁC GIAO THỨC ĐIỀU KHIỂN TRUY NHẬP PHƯƠNG TIỆN TRUYỀN

Khi đường truyền thông được thiết lập, giữa 2 DTE thông qua một mạng hình sao, thành phần điều khiển trung tâm, đảm bảo đường truyền giữa 2 DTE trong một khoảng thời gian yêu cầu. Tuy nhiên với mạng bus và vòng chỉ có một đường truyền dẫn duy nhất có tính logic kết nối đồng thời với tất cả các DTE. Do đó một quy luật phải được tuân theo trên mọi DTE được kết nối với mạng để đảm bảo phương tiện truyền dẫn được truy cập và sử dụng 1 cách hợp lý. CSMA/CD sử dụng cho mạng bus và to-ken để điều khiển được sử dụng cả mạng bus và ring. Một phương thức truy nhập khác gọi là tạo khe-vòng (slotted ring) cũng được sử dụng rộng rãi trong mạng vòng.

1. CSMA/CD (Carrier Sense Multiple Access with Collision Detection).

Phương pháp được truy cập sử dụng sóng mang chỉ được sử dụng trong mạng bus. Với topo này, tất cả các DTE được kết nối với cùng một bus nên ở thời đoạn ngẫu nhiên nào đó có thể có DTE bất kỳ truyền dữ liệu lên bus. Cable khi đó sẽ hoạt động theo chế độ gọi là đa truy cập (multiple access: MA). Tất cả dữ liệu được phát bởi 1 DTE, trước hết nó phải được đóng gói trong một khung cùng với địa chỉ đích ở phần đầu của khung. Khung khi đó sẽ được truyền đi trên cable. Tất cả DTE được kết nối với cable sẽ phát hiện địa chỉ của mình tại phần đầu của khung, nó tiếp tục đọc dữ liệu trong khung và đáp lại theo giao thức đã được quy định.

Với kiểu hoạt động này, hai hay nhiều DTE có thể cùng một lúc truyền khung lên cable, có thể làm hỏng dữ liệu nguồn phát đi. Để giảm tình trạng này, trước khi phát đi một khung, DTE nguồn phát lắng nghe, xem đường truyền rỗi hay bận. Nếu rỗi thì truyền và bận thì thực hiện một trong 3 giải thuật.

- Trạm tạm "rút lui" chờ một thời gian ngẫu nhiên rồi nghe đường truyền với cách này thời gian chết lớn nhưng ít xung đột.

- Tiếp tục nghe đến khi đường truyền rỗi nên thời gian chết nhỏ nhưng dễ xảy ra xung đột.

- Trạm tiếp tục "nghe" đến khi đường truyền rỗi với xác suất p nào đó. *Để có thể phát hiện xung đột, CSMA/CD đã bổ sung thêm quy tắc*:

Khi trạm đang truyền nó vẫn "nghe" đường truyền, nếu phát hiện thấy xung đột thì nó ngừng ngay việc truyền nhưng vẫn tiếp tục gởi tín hiệu sóng mang thêm một thời gian nữa để đảm bảo các trạm trên mạng đều có thể nghe được sự kiện xung đột đó.

Sau khi chờ đợi một thời đoạn ngẫu nhiên trạm lại thử truyền lại bằng sử dụng CSMA.

Trên thực tế tốc độ bit được sử dụng trên cable rất cao (lên đến 10Mbps) nên sự tăng tải có khuynh hướng thấp và việc truyền khung chỉ được bắt đầu khi cable rỗi nên xác suất xung đột xảy ra thấp.

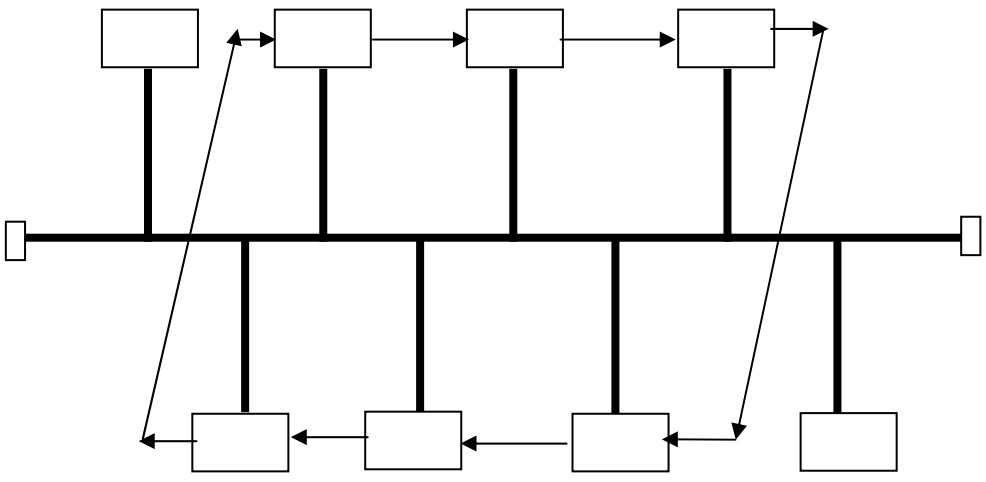
2. Điều khiển truy cập bằng Token

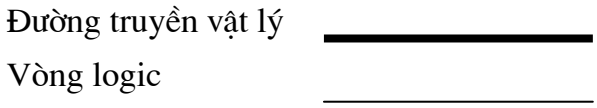
Để cấp phát quyền truy cập đường truyền cho các trạm đang có nhu cầu truyền dữ liệu, token này đi từ 1 DTE qua tất cả các DTE khác cùng kết nối trong đường trruyền. Một DTE có thể chuyển một khung khi nào DTE ấy sở hửu token. Sau đó, nó sẽ chuyển token đó cho các DTE khác để cho phép truy cập đường truyền. Sự hoạt động liên tiếp nối tiếp như sau:

- Một vòng logic (hay còn gọi là vòng ảo) đầu tiên được thiết lập liên kết tất cả các DTE được kết nối phương tiện vật lý và 1 token điều khiển đã tạo ra.
- Token được đi qua từ DTE đến DTE, quanh vòng logic cho đến khi nào nhận bởi DTE đang chờ gởi 1 hay nhiều khung.
- DTE khi đó gởi một (hay nhiều) khung đang sử dụng phương tiện vật lý, sau đó token đi qua đến DTE tiếp theo trong vòng logic.

Những chức năng kiểm tra trong phạm vi các DTE được kết nối đến phương tiện vật lý cung cấp 1 nền tảng cho việc khởi tạo và khôi phục vòng logic và cung cấp chức năng cài đặt tại token khi token bị tổn thất. Mặc dù, các thủ tục kiểm tra thông thường trong tất cả các DTE kết nối với phương tiện. Chỉ có một DTE có trách nhiệm xác định trong một khỏang thời gian cho trước để nhận biết được thẻ bài đã bị mất, lúc đó trạm sẽ phát hiện và gởi thông báo "yêu cầu thẻ bài" tới 1 trạm đã được chỉ định có trách nhiệm sinh thẻ bài mới và tiếp tục lưu chuyển trong vòng logic, có 2 loại:IEEE 802.4 (Token bus) cấp phát truyền dữ liệu trên bus và IEEE 802.5 (Token ring) cấp phát truyền dữ liệu trên ring.

Phương pháp Token bus





Hình 3.6: Sơ đồ vòng logic

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 cuối cùng của chuỗi sẽ tiếp liền sau bởi trạm đầu tiên. Mỗi trạm sẽ biết địa chỉ của trạm liền trước và kề sau nó. Thứ tự của các trạm trên vòng logic có thể độc lập với thứ tự vật lý. Các trạm không hoặc chưa có nhu cầu truyền dữ liệu không được vào trong vòng logic.

Trong ví dụ trên, có 2 trạm nằm ngoài vòng logic do đó chỉ có thể tiếp nhận được dữ liệu dành cho chúng.

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

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

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

c) Quản lý lỗi : một số lỗi có thể xẩy ra như trùng hợp địa, 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.

Phương pháp Token Ring

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

Thẻ bài là một đơn vị truyền dữ liệu đặc biệt trong đó có một bit biểu diễn trạng thái của rhẻ (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 giả quyết hai vấn đề có thể dẫn đến phá vỡ hệ thống đó là mất thẻ bài và thẻ bài "bận" lưu chuyển không dừng trên vòng .Có nhiều phương pháp giải quyết các vấn đề trên, dưới đây là một phương pháp được khuyến nghị:

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

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

3. So sánh CSMA/CD với các phương pháp Token:

- Độ phức tạp của các phương pháp dùng thẻ bài lớn hơn nhiều so CSMA/CD

- Những công việc của một trạm phải làm của CSMA/CD đơn giản hơn phương pháp thẻ bài.

- Hiệu qủa phương pháp thẻ bài không cao đối với tải nhẹ và cao ở tải nặng.

- ưu thẻ bài: khả năng điều hòa lưu thông trong mạng.

Vì các khung truyền dẫn khác nhau được sử dụng với 3 kiểu LAN cơ bản nên chúng có khung truyền dần khác nhau. Việc sử dụng chế độ quản bá bởi 802.3 và 802.4 đã cho thấy rằng chúng đã tận dụng 1 vị trí đồng bộ (preamble) tại phần đầu của mỗi khung để cho phép một trạm thu đạt được sự đồng bộ bit trước lúc bắt đầu nhận nội dung của khung. Điều này không cần thiết với mạng token ring, vì các đồng bộ cục bộ trong tất cả các trạm được duy trì sự đồng bộ bởi 1 tuyến bit lan truyền liên tục trong mạng.

Tương tự như vậy, sử dụng một token cho việc điều khiển truy cập phương tiện truyền cho thấy 802.4 và 802.5 đều có hướng điều khiển khung(FC) các vùng địa chỉ và các trường kết thúc khung (end delimiter-ED) nằm sau FSC. Tuy nhiên một LAN 802.3 không sử dụng vùng này, mặc dù vậy nó sử dụng 1 byte cho vùng chỉ độ dài vùng dữ liệu và vài byte đệm bổ sung đối với những khung nhỏ.

Một token ring có thêm một vùng điều khiển truy cập (AC) tại nơi bắt đầu của mỗi khung để quản lý thứ tự ưu tiên và dành riêng để mô tả những nét đặc biệt của khung. Tập hợp những nút đối tượng đó là khi một khung đi qua từ một kiểu của đoạn LAN này đến LAN khác phải được định dạng lại trước khi chuyển tiếp trên một kiểu LAN mới, bằng cách tự động cộng vào bởi MAC chipset tại giao diện LAN trước khi truyền.

III. KHUÔN DẠNG FRAME VÀ TỐC ĐỘ CỦA CÁC LAN

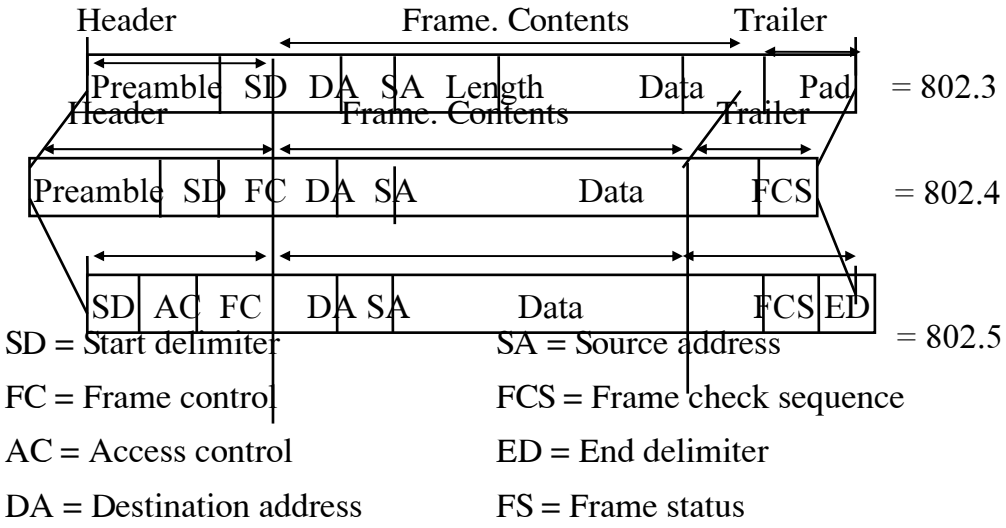
1. Khuôn dạng khung

Vì các chế độ truyền dẫn khác nhau được sử dụng với 3 kiểu LAN cơ bản.

Mạng LAN quảng bá với tiêu chuẩn 802.3 tương ứng phương thức CSMA/CD và tiêu chuẩn 802.4 tương ứng phương thức Token bus.

- Việc sử dụng chế độ quảng bá bởi chuẩn 802.3 và 802.4 chúng đã tận dụng một vị trí đồng bộ tại phần đầu của mỗi khung để cho phép một trạm thu đạt được sự đồng bộ bit trước lúc bắt đầu nhận nội dung của khung.

- Điều này không cần thiết với mạng tokenring (chuẩn 802.5) , vì các đồng bộ cục bộ trong tất cả các trạm được duy trì sự đồng bộ bởi một bit lan truyền liên tục trong mạng.



Hình 6.2. So sánh các khuôn dạng frame của LAN

Việc sử dụng 1 token cho việc điều khiển truy cập phương tiện cho thấy 802.4 và 802.5 đều có trường điều khiển (FC) trước các vùng địa chỉ và trường kết thúc khung (ED) nằm sau FCS. Tuy nhiên, một LAN 802.3 không sử dụng vùng này mà nó sử dụng 1 byte cho vùng chỉ độ dài vùng dữ liệu (Length) và vài byte đệm (pad) bổ sung cho các khung cở nhỏ.

Một token-ring có thêm vùng điều khiển truy cập (AC) để qủan lý thứ tự ưu tiên và FS dành riêng để mô tả những nét đặc biệt của khung.

2. So sánh kích thước gói tin và tốc độ truyền giữa các LAN

2.1 Kích thước gói tin (Packet size):

Các Topology cấu thành mạng khác nhau với các cở gói tin cực đại khác nhau. Có 3 kiểu mạng LAN, mỗi kiểu sử dụng một kích thước khung cực đại khác nhau.

-Ethernet (802.3) dùng kích thước khung cực đại là 1518 bytes (trong đó 1024 bytes dữ liệu).

-Token Bus (802.4) dùng kích thước khung tin cực đại là 8191 bytes

-Token Ring (802.5) mang dữ liệu cực đại là 16 KB ở chế độ truyền 16 Mbp và 4 KB ở chế độ truyền 4 Mbps

Vấn đề ở đây là nếu kích thước khung của một đoạn LAN 802.4 được chuyển tiếp một đoạn 802.3 thì xảy ra việc không tương thích kích thước cũng như khuôn dạng mỗi kiểu.

Mặc dù có thể thực hiện được điều này, bằng cách phân đoạn nhưng sự phân đoạn không phải là chức năng của tiêu chuẩn 802.1 nên các cầu nối sẽ không đưa vào chức năng này. Hơn nữa nó sẽ thêm những overhead trong cầu nối. Như vậy, nếu các cầu nối chuẩn được sử dụng để thực iện chức năng liên kết, thì chỉ một giải pháp là mỗi trạm nguồn phải biết giới hạn của các kích thước khung cực đại được sử dụng trong các LAN được bắc cầu. Rõ ràng giải pháp này là không đáp ứng đặc tính trong suốt của các LAN cầu nối 802.1 và do đó thường sử dụng các cầu nối có khả năng phân đoạn bổ sung.

Một giải pháp khác là sử dụng một thiết bị gọi là bridge-router hoặc brouter để thực hiện chức năng liên kết các segment có kiểu khác nhau.

Như vậy một brouter có thể thực hiện cả 2 chức năng chuyển tiếp như thường lệ của các cầu nối hoặc như là một chức năng của bộ định tuyến trong việc liên kết các kiểu segment khác nhau.

2.2. Thời gian truy cập đường truyền (Media access time) và tốc độ truyền.

Đây là tham số quan trọng bị tác động bởi nhiều yếu tố sau.

- Độ trễ danh nghĩa (nominal delay) kế thừa từ phương pháp luận truy cập đã chọn của đường truyền.

  - Token Ring sử dụng sơ đồ "chuyển thẻ" (token-pasring) để kiểm soát và cấp quyền truy cập đối với đường truyền.
  - Ethernet sử dụng phương pháp CSMA/CD nhanh hơn phương pháp "chuyển thẻ" từ 5 đến 10 lần.

- Thời gian truy cập đường truyền tác động bởi lượng tranh chấp xuất hiện trên một đoạn cụ thể của đường truyền. Số tranh chấp càng nhiều thì thời gian truy cập trung bình càng dài.

2.3. Tốc độ truyền bit của các loại LAN như sau.

Ethernet (802.3) là 1, 2, 10 Mbps

Token Bus (802.4) là 1, 5, 10 Mbps

Token Ring (802.5) là 1, 4, 16 Mbps

Rõ ràng nếu các khung nhận được trên một segment chậm và được chuyển tiếp trên một segment nhanh hơn thì không có vấn đề gì và nếu ngược lại LAN nạp nhiều tải (heavily loaded) nảy sinh các khung phải đợi tại cổng ra của LAN chậm hơn. Điều này vẫn đúng với 2 LAN cùng kiểu.

Ví dụ, nếu hai đoạn LAN hoạt động 1Mbps, bộ nhớ hiện tại đã được giới hạn. Cầu nối sẽ loại bỏ khung bởi vì bộ nhớ tích lũy không hết. Mặc dù trong thực tiễn các thực thể giao thức vận chuyển trong các trạm nguồn ảnh hưởng sẽ khởi động truyền lại nhưng thời gian time out dài nên độ trễ truyền dẫn khung tăng. Hơn nữa, không có sự bảo đảm các bản sao mới, tránh được tình trạng tương tự.

Tham số Lưu tốc tín hiệu (Signaling Speed) hay giải thông (Bandwidth) ít tác động nhất trong số các tham số điều chỉnh được.

Tóm lại:

Với lưu tốc 16 Mbps, mạng Token Ring đáp ứng được cở gói tin sẵn dụng to nhất nên cho ta hiệu năng lớn nhất trong môi trường luôn có các lượng dữ liệu lớn cần truyền tải. Song:

ở những nơi kích cở gói tin không mấy quan trọng như truy cập về máy chủ hay ứng dụng mô hình "Client/Server" thì mạng Ethernet lại đưa ra được giải pháp đạt hiệu năng cao nhất và chi phí thấp. Do đó giải pháp chúng ta chọn còn tùy thuộc vào môi trường và ứng dụng.

IV. PHƯƠNG THỨC HOẠT ĐỘNG GIAO TIẾP GIỮA CÁC LAN.

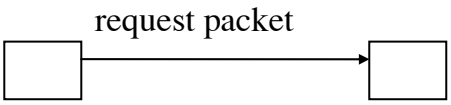
Tập hợp những nét đặc trưng đó nên khi một khung đi qua từ một kiểu của đoạn LAN này đến LAN khác nó cần phải được định dạng lại trước khi chuyển tiếp trên một kiểu LAN mới. Các vùng trong mỗi khung được nhận dạng là tự động cộng vào bởi MAC chipset tại giao diện LAN trước khi các nội dung khung hiện thời được truyền đi (lưu trữ). Thông thường khung này không đúng chiều dài và vùng đệm được dùng với các LAN 802.3 nên các chipset MAC định dạng lại trong cầu nối trước khi khung chuyển tiếp. Chính vì vậy làm tăng thời gian xử lý gây trễ trong phạm vi cầu nối. Thêm vào nữa là trường FCS mới cần được tính lại trong MAC chipset khi khung lưu trữ được chuyển tiếp.

Vì vậy nguồn gốc lỗi của các LAN là do bit lỗi được tạo ra trong các khung khi chúng được lưu trữ và phục hồi trong bộ nhớ giới hạn. Dĩ nhiên lỗi được phát hiện bởi trường FCS mới.

Người ta phải đưa ra một giải pháp để cho tất cả LAN Segment cùng 1 kiểu, sử dụng cùng một vùng FSC từ nguồn đến đích. Nhưng rõ ràng điều này không thể thực hiện được nếu một khung định dạng lại bởi một cầu nối và các lỗi được tạo ra (trong thời gian xử lý và tích lũy) sẽ bị phát hiện lại thì cần phải dùng bộ nhớ sữa lỗi.

Khi giao tiếp giữa các LAN hay giữa FileServer và Worstation thì đọc dữ liệu chiếm tỷ lệ cao hơn ghi rất nhiều nên các chu trình đọc của LAN là chu trình đọc ở đó thông tin được chuyển từ FileServer đến Workstation. Tại vì LAN phổ biến được dùng cho các trình ứng dụng dùng chung Server, ngay cả khi trình ứng dụng đó là 1 ứng dụng CSDL lớn thì dữ liệu đọc ra cũng nhiều hơn là ghi vào khỏang 75 - 90%.

- Chu trình khởi đầu từ lúc trạm làm việc tạo ra một "gói yêu cầu" (request packet) rồi chuyển nó tới server.



+ *Server* cần thời gian để làm các tác vụ sau:

- Giải mã các gói tin
- Nhận thông tin yêu cầu đọc (từ đĩa hoặc từ bộ cache)
- Chuyến thông tin ấy bên trong Server.
- Tạo ra gói tin trả lời.
- Chờ được truy cập kênh truyền (media) .
- Server truyền gói tin trả lời.

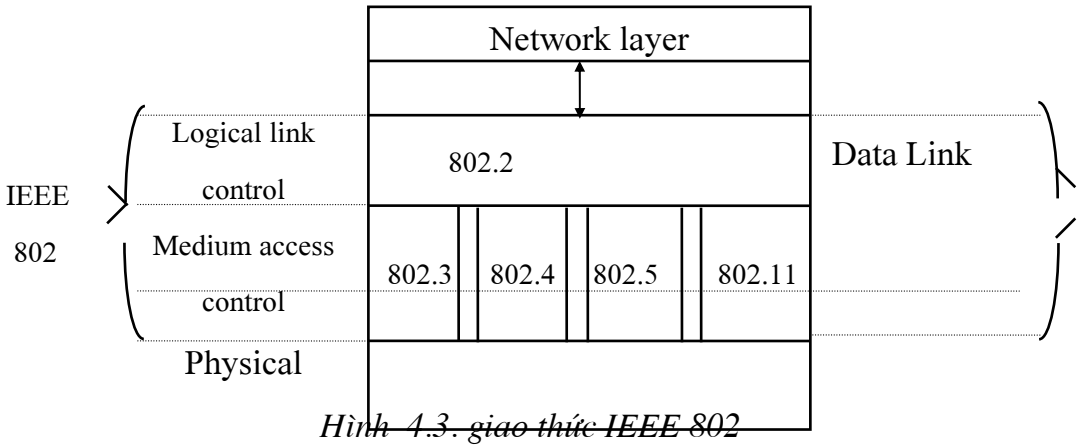
+ *Trạm làm việc* phải thực hiện những xử lý nội bộ giống như server, chu trình ấy lặp lại cho đến khi cả hay một phần tập tin yêu cầu được truyền xong.

Kỹ thuật nối mạng giải quyết về vấn đề đường truyền vật lý và những sự điều khiển thâm nhập đường truyền, những giao thức tầng liên kết dữ liệu và những vấn đề lưu thông trong mạng, đều được gán phần đầu MAC và bộ quy tắc điều khiển thâm nhập đường truyền.

V. CÁC GIAO THỨC MẠNG LAN

Các chuẩn giao thức dành cho các mạng LAN là những giao thức được quy định theo tiêu chuẩn IEEE 802. Chuẩn này qui định một họ giao thức, mỗi giao thức liên quan đến một kiểu của phương pháp truy cập phương tiện truyền riêng. Do đặc trưng riêng việc chuẩn hóa LAN chỉ dùng hai tầng thấp 1 là tầng vật lý và liên kết dữ liệu (LLC, MAC).

Các tiêu chuẩn IEEE và mối quan hệ của chúng với mô hình ISO như sau:



Hình 4.3. giao thức IEEE 802

802.2 = Logical link control Protocol

802.3 = CSMA/CD

802.4 = Token bus Medium access control protocols

802.5 = Token ring

802.11 = Wireless

- Tầng MAC: Đảm bảo điều khiển truy cập đường truyền với phương thức CSMA/CD, token ring, token bus.

- Tầng LLC: Đảm bảo tính độc lập của việc quản lý các liên kết dữ liệu đường truyền vật lý và phương pháp truy cập MAC được sử dụng. LLC bắt nguồn từ HDLC được dùng cho mạng cục bộ LAN. Về khuôn dạng, trường địa chỉ nguồn và đích chỉ gán cho điểm truy cập dịch vụ LLC, chúng không chứa địa chỉ để truyền cho môi trường mạng, chúng không có trường FCS.

Vì thế lớp con MAC giải quyết các chức năng địa chỉ mạng và phát hiện lỗi. Đó là lý do mà trong nội dung của mô hình tham chiếu ISO lớp liên kết là tương đương với sự hợp nhất của các lớp con LLC và một phần của MAC.

Giao thức LLC cung cấp hai kiểu hoạt động:

- *Không kết nối không báo nhận*

- *Kết nối định hướng bit.*

Trong thực tế cả hai kiểu cũng tương tự như giao thức HDLC ngoại trừ chức năng phát hiện lỗi và tạo khung được cung cấp bởi lớp con MAC.

Điểm khác nhau lớn nhất giữa giao thức LLC và HDLC là sự cung cấp dịch vụ không kết nối không báo nhận. Việc thiết lập lệnh và trả lời được cung cấp trong kiểu không kết nối là:

Commands	Responses
UI	-----
XID	XID
TEST	TEST

Khung lệnh UI được dùng để gởi số liệu đến một hoặc nhiều LLC. Vì vậy không có thứ tự hoặc báo nhận, khung UI không chứa trường N(S) hoặc N(R). Như vậy không có trả lời từ khung UI.

Các khung lệnh thay đổi nhận dạng XID và TEST là có lựa chọn. Tuy nhiên nếu chúng được gởi thì bắt buộc phải có trả lời từ LLC. Các lệnh này được dùng như sau:

* Lệnh XID với một địa chỉ nhóm được dùng để xác định thành phần hiện hành của nhóm. Mỗi thành phần của nhóm trả lời lệnh bằng cách truyền trở lại một khung trả lời XID đến nơi phát LLC.

* LLC có thể dùng lệnh XID với địa chỉ đích Broadcast để công bố sự có mặt của nó trên môi trường mạng.

* Lệnh TEST được sử dụng để cung cấp khả năng kiểm tra vòng trên mỗi LLC đến đường dẫn truyền LLC.

Đặc điểm của những mạng này là dùng trong phạm vi nhỏ, tỷ lệ bit lỗi thấp, liên kết hoạt động ở tốc độ cao (~10Mbps), chức năng điều khiển luồng và điều khiển

truyền lại ở lớp giao thức cao hơn trong hệ thống đầu cuối DCE nên thời gian truyền khung end-to-end là rất nhanh.

VI. KHẢO SÁT MẠNG

1. Thiết kế hệ thống mạng

Có nhiều kiểu thiết kế hệ thống mạng nhưng trong thực tế lắp đặt, bạn phải chọn một trong các phương án hiệu quả nhất như địa hình, cơ sở vật chất hiện có cần tận dụng, những yêu cầu quản lý dữ liệu đặt ra....và cuối cùng là tài chính .

1.1 Yêu cầu hệ thống

Đảm bảo độ tin cậy về hệ thống: Có phương án xử lý các lỗi, các sự cố từ máy trạm, máy chủ, các thiết bị để đảm bảo thông tin thông suốt, quá trình xử lý thông tin không bị gián đoạn .

Dễ bảo hành: Trong quá trình hoạt động, hệ thống có sự cố, cần phải thiết kế sao cho có thể dễ dàng và nhanh chóng có thể phát hiện ra vị trí , nguyên nhân của sự cố. Đồng thời có biện pháp khắc phục nhanh nhất.

Dễ mở rộng và phát triển: Khi thiết kế hệ thống mạng cần phải tính cả đến nhu cầu xử lý thông tin hiện đại, khả năng của thiết bị khi lắp mạng và cả các yêu cầu của tương lai. Điều này liên quan đến một loạt các yếu tố sau cần phải tính đến như:

* Có thể mở rộng mạng bằng cách tăng số máy trạm hoặc nâng cấp thiết bị.

* Có thể thay đổi và nâng cấp hệ điều hành mạng mà không phải làm hư hỏng số liệu. Có thể tăng năng lực xử lý của hệ thống và tính đến tính phổ dụng, tính tương thích của phần mềm và thiết bị.

An toàn và kinh tế: Cần thiết kế để tận dụng được tất cả khả năng an toàn dữ liệu của hệ thống. Chẳng hạn như dùng nhiều ổ đĩa cứng, dùng nhiều card mạng trên một máy, dùng máy cho dự phòng. Cần cân nhắc tính toán, lựa chọn sơ đồ ,lựa chọn thiết bị chủng loại thiết bị sao cho chi phí giảm tối đa nhưng vẫn có được một hệ thống mạng đáp ứng được mọi yêu cầu cần thiết.

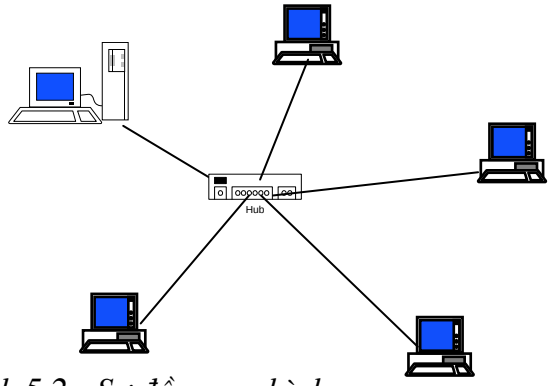
1.2 Quy trình thiết kế

* Lập yêu cầu hệ thống, yêu cầu về số lượng máy trạm .
* Yêu cầu về mạch xử lý dữ liệu, phương thức, khoảng cách truyền dữ liệu.
* Yêu cầu về nội dung làm việc của hệ thống .
* Yêu cầu xử lý thông tin của từng nhóm trạm, từng trạm.
* Khảo sát địa hình và lên sơ đồ hệ
* Lựa chọn thiết bị và phần mềm

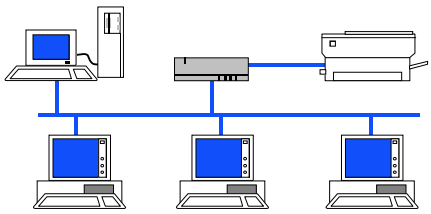
2. Các phương án thiết kế mạng thông dụng

2.1 Thiết kế mạng trong một phòng máy

Thường dùng là kiểu BUS hoặc hình sao. Các kiểu này thường thích hợp với nhà trường, cơ quan nhỏ có phạm vi trong một nhà.



Hình 5.2 : Sơ đồ mạng hình sao



Hình 5.3 : Sơ đồ mạng hình BUS

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 đếùn 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 của topo mạng hình sao:*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 của topo mạng hình sao: Độ dài đường truyền nối một trạm với thiết bị trung tâm bị hạn chế (trong vòng 500m, với công nghệ hiện nay).

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

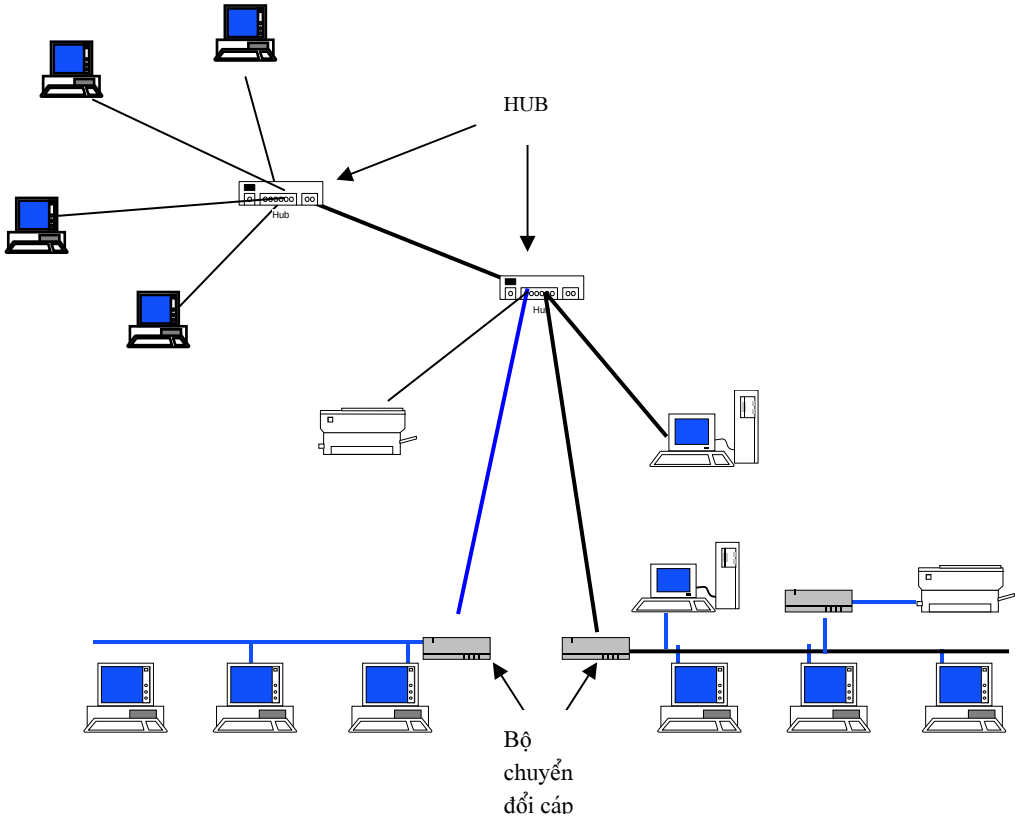
Khi một trạm truyền dữ liệu tín hiệu được quảng bá trên cả hai chiều của bus, tức là mọi trạm còn lại đều có thể thu được tín hiệu đó trực tiếp. Đối với các bus một chiều thì tín hiệu chỉ đi về một phía, lúc đó các terminator phải được thiết kế sao cho các tín hiệu đó phải được dội lại trên bus để cho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

ưu điểm : Dễ thiết kế, chi phí thấp

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

Kết nối hỗn hợp

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



Hình 5.4 : Sơ đồ mạng hổn hợp

Trong hệ thống mạng cục bộ chỉ cần một máy chủ đủ mạnh , các máy trạm chỉ cần cấu hình tối thiểu, có thể tận dụng các máy tính như AT486, Pentium hiện có và dễ nâng cấp chỉ cần nâng cấp máy chủ và bộ nhớ của các máy trạm cho đủ để sử dụng chương trình.

3. Truyền dữ liệu trên mạng

Khi các máy tính được nối với nhau thành mạng, quá trình khai thác tài nguyên trong mạng dẫn đến quá trình truyền dữ liệu các máy tính trong hệ thống mạng. Quá trình truyền dữ liệu giữa hai máy tính diễn ra gồm ba bước cơ bản:

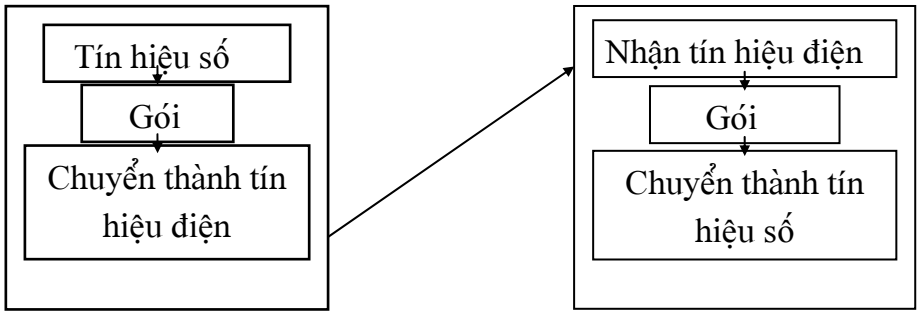
1. Mã hóa dữ liệu khi chuyển thành tín hiệu.
2. Truyền tín hiệu .
3. Tiếp nhận tín hiệu và giải mã để nhận lại tín hiệu .

Bước 1: Dữ liệu được chia cắt thành nhiều khối hay gói (packet), sau đó mã hóa thành tín hiệu. Song như thế chưa đảm bão dữ liệu đi đến đích và nhận đúng, cần phải bổ sung một số thông tin khác như địa chỉ nơi nhận, nơi gửi, tốc độ truyền, kiểu truyền....

Bước 2: Làm nhiệm vụ truyền tín hiệu đã được trộỹn thành gói ở bước 1 bước này gọi là Transmiter .

Bước 3: Nhận và giải mã, trong bước này máy nhận tín hiệu truyền đến, lọc bỏ những thông tin không phải là dữ liệu để tiếp nhận lại đúng dữ liệu. Bước này được gọi là bước tiếp nhận dữ liệu hay Receiver .

Quá trình trên có thể minh họa theo sơ đồ sau:



4. Yêu cầu về thiết bị

Máy chủ (server): có vai trò đặc biệt quan trọng trong hệ thống mạng, nó thường xuyên phải tiếp nhận, phân tích các yêu cầu khác nhau của người sử dụng (client) về tài nguyên và đáp ứng các yêu cầu này, vì vậy đòi hỏi dung tích bộ nhớ phải lớn , tốc độ đủ nhanh, phải có độ tin cậy và ổn định cao. Nói một cách khác cấu hình của máy chủ phải đủ mạnh, tất nhiên cấu hình này còn phụ thuộc vào hệ điều hành mạng và version của nó, vào số lượng người dùng (client). Nói chung, một máy chủ máy cần có cấu hình tối thiểu sau: Hệ máy Pentium, dung tích bộ nhớ RAM 512Mb,dDung tích ổ đĩa cứng trên 40 Gb.

Các máy trạm (worktations): không có yêu cầu cấu hình mạnh, máy trạm thường tận dụng các máy hiện có. Nhưng cấu hình của máy trạm yếu sẽ làm ảnh hưởng đến khả năng khai thác thông tin. Nếu không dùng ổ cứng phải có ổ đĩa mềm hoặc bootRom để khởi động mạng.

Card mạng (NIC):

Tên gọi	Họ card
Novell NE_2000	Ethernet
Novell RX_Net	ARCNet
IBM PC Network II (for PC)	RG_59 Coaxial
IBM Token Ring/A	Token Ring
3Com 3C508	Ethernet
vv.....	vv.....

Cáp nối mạng: có nhiều loại, việc chọn loại cáp nào phụ thuộc vào kiểu nối mạng, loại card mạng và khả năng kinh tế đầu tư cho mạng. Nói chung không có sự khác nhau lớn giữa các loại cáp nối về giá trị sử dụng. Tuy nhiên, trước khi quyết định chọn loại cáp nào hãy xem xét tổng thể từ sơ đồ mạng đến cổng (Port) trên card mạng. Mỗi loại cáp nối chỉ dùng được cho một loại cổng trên Card mạng.

Hiện nay cáp nối mạng có ba loại sau:

- Coaxial cable (đồng trục)

- Twisted pair cable (cáp xoắn đôi)

- Filer optic cable (cáp quang)

Loại cáp đồng trục có lẽ là loại được sử dụng phổ biến nhất hiện nay để nối mạng .

Loại cáp twisted pair chia thành hai loại :

+ Loại shielted twisted pair (cáp đôi chống nhiễu)

+ Loại unshielted twisted pair (cáp đôi không chống nhiễu)

Loại cáp filer optic có ưu điểm là tốc độ truyền cao (trên 100 Mbps), có khả năng chống nhiễu, chống ồn, song nhược điểm là đắt.

Với mạng Ethernet sẽ thích hợp hơn nếu bạn dùng loại cáp đồng trục (Coaxial cable), với cáp đồng trục dùng cho mạng Ethernet người ta lại chia thành hai loại:

+ Loại cáp béo (thick cable)

+ Loại cáp gầy (thin cable)

Việc chọn loại cáp nào phụ thuộc vào chiều dài trong hệ thống mạng. Nếu khoảng cách nối giữa các máy dài, bạn nên chọn loại cáp béo .

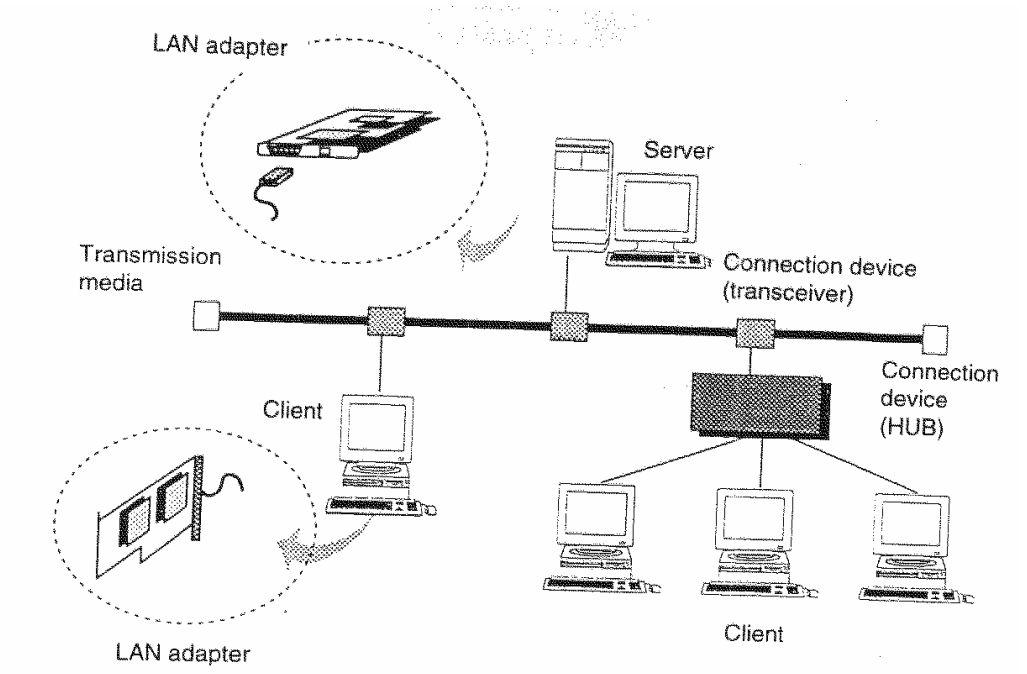
Cút nối mạng Ethernet:

- BNC T connector : cút nối cáp với máy .

- BNC Terminator : cút bịt đầu cuối .

- BNC ground terminator.

Chúng ta lưu ý rằng trên đây là những thiết bị cơ bản cần thiết phục vụ cho việc nối mạng, ngoài ra phụ thuộc vào sơ đồ mạng, kiểu nối mạng, khoảng cách nối có thể có thêm các thiết bị khác như HUB, REPEATER, BOOTPROM, Brigde, Router, Brouter Gateway v.v..



Hình 5.6: Ví dụ 1 dạng sơ đồ kết nối chuẩn

Tóm lại: Hệ thống mạng là một thể thống nhất từ sơ đồ mạng, thiết bị nối mạng và phần mềm trên mạng có sự liên quan và phụ thuộc nhất định, do vậy việc ghép nối mạng đòi hỏi phải lựa chọn thiết bị và thiết kế trước khi lắp đặt mạng.

5. Bộ giao thức IPX/SPX

5.1 Giao thức IPX (Internetwork Packet Exchange)

IPX là giao thức lớp mạng cung cấp dịch vụ bó dữ liệu không kết nối ở đỉnh của các giao thức lớp liên lết dữ liệu như giao thức Ethernet, Tokengring, ARCnet và PPP và IPX có thể được thiết lập để hoạt động trên hầu như tất cả các giao thức liên kết dữ liệu.

Thông điệp được gửi đi bằng cách tách chúng thành nhiều gói (datagram) và gửi đi tòan bộ địa chỉ nguồn cũng như thông tin nơi đến ở mỗi gói. Để cung cấp sự an toàn cho gói truyền đi người ta dùng lớp trên là SPX hoặc NCP (Netware Core Protocol: giao thức mạng lõi). Datagram làm việc tốt với các dịch vụ mạng đòi hỏi khả năng truyền phát.

Do nguồn gốc của IPX ở trong giao thức XNSIDP, nên địa chỉ nút 48 bit được sử dụng. Mỗi nút trên mạng Netware có thể có nhiều qui trình phần mềm cùng chạy, chẳng hạn như các dịch vụ NCP, SAP, RIP. Để xác định gói cho mỗi qui trình người ta dùng số hiệu socket (16 bit), bên trong số liệu socket được dùng truy cập các cấu trúc dữ liệu dùng để liên lạc với các giao thức IPX. Địa chỉ đầy đủ của một qui trình trên 1 nút trên mạng Netware bao gồm 3 phần (số liệu mạng, số liệu nút, số liệu socket).

Network number: Là định danh của mỗi Segment của multiserver Netware được cài đặt.

Node address: Là định danh duy nhất của card mạng.

Soket: Đại diện cho chính ứng dụng gởi đến đang chạy trên W đích.

- Để gọi 1 IPX packet bạn phải ấn định 1 địa chỉ chính (Network, Node, Socket) nhưng khi nhận chỉ cần ấn định 1 Socket.

- Có thể quản lý việc giao tiếp PC với PC bằng cách dùng một thiết lập của những phục vụ mà IPX đưa ra cho phần mềm của người lập trình.

+ Khuôn dạng của IPX packet.

Checksum	2 bytes
Length	2
Transport Control	1
Packet Type	1
Dest Network	4
Dest Node	6
Dest Socket	2
Source Network	4

Source Node	6
Source Socket	2
Data	0-546 bytes

Chức năng của các trường như sau:

Checksum: gồm 2 byte được định nghĩa giao thức mức thấp của mạng luôn kiểm tra lỗi, khi lập trình không cần thiết lập tính năng này nên IPX tự động tính ở phần cứng .

Length: độ dài của gói IPX thường được giới hạn 576 bytes.

Transport Control: trường đếm bước để đếm số bộ định tuyến đi qua và được giới hạn là 16.

Transport Control = 0 khi 1 packet được truyền đi đầu tiên và sau đó trường này tăng lên, nếu = 16 thì packet bị loại bỏ

Packet Type: nhận diện lớp trên nào phải nhận phần dữ liệu của gói IPX.

Dest Network, Dest Node, Dest Socket nhận diện các qui trình trong nút đích và *Source Network/Node, Socket* nhận diện các qui trình trong nút nguồn, số hiệu mạng nguồn.

5.2 Giao thức SPX

Sequence Packet exchange (SPX) là giao thức lớp vận chuyển cung cấp dịch vụ hướng kết nối trên đỉnh của giao thức IPX không kết nối. SPX được dùng khi cần có 1 nối kết mạch ảo đáng tin cậy giữa 2 trạm. Giao thức SPX liên quan đến vấn đề trật tự và kiểm soát luồng nhằm đảm bảo cho gói đến nơi đúng thứ tự. SPX cũng đảm bảo rằng bộ đệm của nút đích không bị quá tải với dữ liệu gửi đến quá dồn dập.

Trước khi gởi dữ liệu những gói điều khiển SPX được gởi đến để thiết lập một kết nối, và số bảo mật kết nối được kết hợp cho mạch ảo đó. Số bảo mật kết nối nàydược sử dụng trong tất cả những cuộc truyền dữ liệu. Kết thúc cuộc truyền một gói điều khiển có nội dung rõ ràng, xác thực được gởi đến để phá vỡ nối kết.

Cấu trúc gói SPX gồm có các trường sau:

1 byte	1 byte	2 bytes	2 bytes	2 bytes	2 bytes	2 bytes	
Connection Control	Data Stream Type	Source Connect ID	Dest Connect ID	Sequence number	Ackno-wledge number	Alloation number	Data

trong đó:

+ *Connection Control:* trường kiểm sóat kết nối để điều hòa luồng dữ liệu ngang qua kết nối.

+ *Data Stream Type*: định danh kiểu dữ liệu cho mỗi packet

+ *Source/Dest Connection ID*: dùng để nhận diện một phiên làm việc

+ *Sequence number*: định danh và loại bỏ những packet bị lặp lại. Đánh số từng gói gởi đi, dò tìm những gói bị thất lạc nằm ngoài thứ tự.

+ *Acknowledge number* số ACK cho biết gói dữ liệu kế tiếp mà bên tiếp nhận đang chờ đợi.

+ *Alloation number*: cho biết dung lượng bộ nhớ đệm còn trống mà bên tiếp nhận có sẵn trên một kết nối. Giá trị này được bên gọi dùng để điều chỉnh tốc độ truyền dữ liệu và giúp bên nhận tránh được tình trạng ngập dữ liệu vì bộ đệm không đủ sức chứa.

5.3 Khuôn dạng của gói tin truyền đi

Khuôn dạng gói tin truyền đi có 4 loại

Frame 802.3, 802.2, Ethernet II, Ethernet SNAP

Trong đó frame 802.3 là kiểu frame chuẩn của mạng Ethernet có cấu trúc sau :

IEEE 802.2 Ethernet

Destiration	Source	Length	Data
6 byte	6 byte	2 byte	từ 4 đến 1500 byte

Ethernet II

Destiration	Source	Type	Data
6 byte	6 byte	2 byte	từ 46 đến 1500 byte

IEEE 802.3 with 802.2

Destintion	Source	Length	802.2 header	Data
6 byte	6 byte	6 byte	2 byte	từ 46 đến 1500 byte

IEEE 802.3 with 802.2 và SNAP

Destination	Source	Length	802.2 header	Data
6 byte	6 byte	2 byte		từ 46 đến 1500 byte

Chú ý:

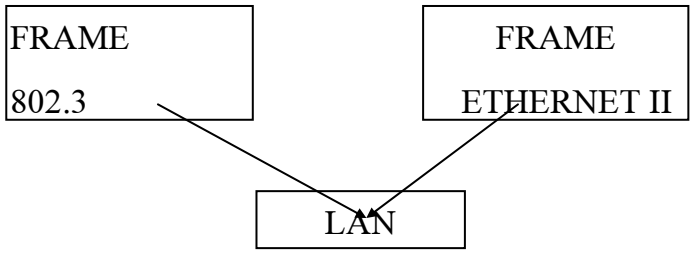
- Giao thức IPX/SPX chỉ dùng với frame 802.3.

- Giao thức IPX/SPX và giao thức TCP/IP dùng với frame Ethernet II, nếu trên mạng có dùng giao thức TCP/IP thì buộc phải dùng frame Ethernet II.

- Frame SNAP là frame dùng để thay cho frame 802.2, 802.3 và cả các frame không thuộc họ Ethernet như Tokenring , Apple talk.

- Frame 802.2 và 802.3 về cơ bản là giống nhau và bạn có thể dùng để thay thế chúng với nhau.

Quan hệ giữa các thành phần nêu trên có thể mô tả theo sơ đồ sau:



6. Cách tổ chức thông tin của hệ điều hành mạng Novell 4.x

Các tài nguyên trên mạng được quản lý nhờ cây thư mục **NDS**, mỗi nút trên cây là một đối tượng, các đối tượng ứng với các tổ chức khai thác hoặc người khai thác tài nguyên trên mạng. Tài nguyên tương ứng với dữ liệu, thiết bị được đặt tên các *volume object*. Cách tổ chức này làm đơn giản cho người sử dụng không cần biết tài nguyên để ở đâu trên đĩa về mặt vật lý mà chỉ cần biết volume và thư mục cất giữ số liệu.

Các thư mục chuẩn

TRONG quá trình cài đặt hệ điều hành mạng vào máy chủ, hệ điều hành tự động sinh ra volume object có tên gọi SYS, đồng thời sinh thêm một loạt các thư mục chuẩn của hệ điều hành mạng, đó là các thư mục :

SYS VOLUME

SYSTEM <DIR>

PUBLIC <DIR>

LOGIN <DIR>

MAIL <DIR>

DELETE.SAV <DIR>

Thư mục **SYSTEM** dùng để chứa hệ điều hành mạng các file hệ thống, tập lệnh của NETWARE và các công cụ dành cho người quản lý mạng (*Supervisor*) mới có thể truy cập thư mục này .

Thư mục **PUBLIC** dùng để chứa các chương trình phổ dụng dùng cho người khai thác mạng, kể cả các chương trình tiện ích .

Thư mục **LOGIN** chứa các chương trình tiện ích phục vụ cho việc truy cập vào mạng .

Thư mục **MAIL** dùng để chứa các số ID của người khai thác mạng, chứa các thông điệp dạng thư tín. Trong nó còn có các thư mục con chứa các thông tin về người khai thác mạng gọi là file login script và khuôn mẫu tác vụ in ***(print jobs configuration).***

Thư mục **DELETE.SAV** dùng để lưu giữ các file đã có trên đĩa trước khi cài đặt.

Để chỉ ra vị trí một file trên volume:

DHKH\SYS:\TMUC1\ TMUC2\.....\TMUCN\DIEM.SV

Trong đó :

DHKH: là tên của *server* ***(file server name)*** đặt khi cài đặt hệ điều hành .

SYS:là tên của *volume object* .

TMUC1,TMUC2,.....TMUCN: là tên các thư mục trong *volume object* .

Ngoài các thư mục chuẩn trên server còn có các thư mục được tạo bởi khi cài đặt các chương trình ứng dụng vào máy chủ.

7. Quyền khai thác tài nguyên của người sử dụng

Quyền khai thác mạng

Mạng máy vi tính là hệ thống cho phép người ta khai thác chung các tài nguyên, song việc khai thác chung này sẽ trở nên mất ý nghĩa nếu mọi người đều có quyền truy cập, khai thác, hủy bỏ tùy tiện các tài nguyên trên mạng. Vì vậy hệ thống mạng phải đảm bảo tính an toàn, bí mật của dữ liệu. Để thực hiện được chức năng này trên mạng người ta phải tổ chức theo hai nguyên tắc sau:

Quyền với tài nguyên trên mạng: Trên mạng Novell v.4x tồn tại tấc cả 4 loại quyền sau:

Quyền đối tượng (Object rights): Quyền đối tượng dùng để kiểm tra xem quyền nào có thể làm việc với đối tượng, nếu quyền không đảm bảo thì không được phép truy nhập vào các thông tin chứa trong đối tượng.

Quyền thuộc tính (Property rights): Quyền thuộc tính được dùng để kiểm tra xem quyền nào được phép truy nhập vào các thông tin là thuộc tính của đối tượng như số điện thoại, địa chỉ....

Quyền thư mục (Directory rights): được dùng để kiểm tra quyền truy nhập thư mục.

Quyền file (File rights): được dùng để kiểm tra truy nhập vào các file.

Người sử dụng muốn khai thác tài nguyên trên mạng họ phải đăng ký với người quản lý mạng là **SUPERVISOR,** nội dung đăng ký bao gồm :

- Phạm vi khai thác như các file, các thư mục cần làm việc.

- Mức độ khai thác

Dựa vào yêu cầu của người khai thác Supervisor sẽ phân quyền cho người sử dụng. Trên mạng có 8 quyền dưới đây phản ánh mức đôĩ được phép khai thác đối với tài nguyên:

- Quyền ***Supervisor :*** Đây là quyền cao nhất trên mạng. Người có quyền này có mọi quyền mà mạng có như tổ chức, điều hành, quản lý mọi hoạt động trên mạng. Để có quyền này người sử dụng phải có mật khẩu của Supervisor .
- Quyền ***Access control : Người*** sử dụng có thể thêm, bớt, thay đổi các quyền với các file và thư mục. Quyền này cần thiết cho người quản lý nhóm.
- Quyền ***Read:*** Người sử dụng có thể mở, đọc file, thực hiện các file ứng dụng.
- Quyền ***Write***: Người sử dụng có thể mở, thêm, bớt, sửa chữa file.

- Quyền ***Create: Người*** sử dụng có thể tạo file, tạo thư mục con.
- Quyền ***Erase:*** cho phép người sử dụng xóa file, xóa thư mục.
- Quyền ***Modify***: cho phép người sử dụng sửa đổi tên file, tên thư mục, thay đổi thuộc tính file, thư mục.
- Quyền ***File Scan:*** cho phép người sử dụng xem tên file, tên thư mục trong cấu trúc của hệ thống. Cho phép chạy các file chương trình.

Chú ý: Các quyền trên không hoàn toàn độc lập nhau mà chúng có quan hệ với nhau. Chẳng hạn người có quyền ***Access control*** đương nhiên có quyền ***File Scan.***

Trên mạng các quyền có tính thừa kế, nghĩa là một đối tượng có một quyền nào đó thì các đối tượng thành viên sẽ được thừa hưởng quyền này ta gọi là quyền thừa kế. Dựa vào tính chất đó người quản lý mạng có thể chia sẻ bớt quyền hoặc giao quyền cho nhiều thành viên khai thác mạng một cách nhanh chóng.

CHƯƠNG 7
MẠNG INTERNET

I. GIỚI THIỆU CHUNG

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

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

Tuy nhiên cho tới năm 1988, việc sử dụng INTERNET còn hạn chế trong các dịch vụ truyền mạng (FTP), thư điện tử (E-mail), truy nhập từ xa (TELNET) không thích ứng với nhu cầu kinh tế và đời sống hàng ngày. INTERNET chủ yếu được dùng trong môi trường nghiên cứu khoa học và giảng dạy đại học. Trong năm 1988, tại trung tâm nghiên cứu nguyên tử của Pháp CERN (Centre Euro de Recherche Nuclaire) ra đời đề án *Mạng nhện thế giới* WWW(World Wide Web). Đề án này, nhằm xây dựng một phương thức mới sử dụng INTERNET, gọi là phương thức *Siêu văn bản* (HyperText). Các tài liệu và hình ảnh được trình bày bằng ngôn ngữ HTML (HyperText Markup Language) và được phát hành trên INTERNET qua các hệ chủ làm việc với nghi thức HTTP (HyperText Transport Protocol). Từ năm 1992, phương thức làm việc này được đưa ra thử nghiệm trên INTERNET. Rất nhanh chóng, các công ty tư nhân tìm thấy qua phương thức này cách sử dụng INTERNET trong kinh tế và đời sống. Vốn đầu tư vào INTERNET được nhân lên hàng chục lần. Từ năm 1994 INTERNET trở thành siêu mạng kinh doanh.

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

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

Internet nổi bật bởi các đặc điểm sau:

- Internet là một công cụ khá tiêu biểu để trao đổi thông tin trên các máy tính toàn cầu.
- Internet cung cấp cho các nhà nghiên cứu và nhiều đối tượng khác nhiều thông tin cần thiết.
- Internet không phân biệt về khoảng cách truy cập và không có một chủ sở hữu.

Một trong những thành công lớn của ARPANET chính là giao thức mạng (Network Protocol) mới. Giao thức này liên quan đến một công nghệ mới chính là Chuyển mạch gói (Packet Swiching).

II. KIẾN TRÚC TCP/IP

1. Giới thiệu

Vào những năm 1970 Bộ giao thức TCP/IP ít được thông dụng, nhưng ngày nay nó đã được sử dụng rộng rãi. Những giao thức TCP/IP kết nối những thiết bị từ những nhà cung cấp (Vendor) khác nhau. Chúng có khả năng liên kết những mạnh riêng rẽ vào một liên mạng, những người sử dụng trong những mạng này có thể truy cập vào một bộ dịch vụ chung. Hơn nữa, các tổ chức khoa học, quân đội đỡ đầu TCP/IP muốn có khả năng kết nối những mạnh mới vào liên mạng của họ. Xuất phát từ những nhu cầu này đã cấu hình nên kiến trúc của giao thức. Sự cần thiết cho tính đa năng và độc lập của công nghệ phương tiện tạo ra một cấu trúc phân tầng linh hoạt.

Một lớp dành cho việc chọn dữ liệu. Được truyền bởi mô hình chuyển mạch gói ARPANET, những nhà thiết kế di chuyển dữ liệu ngang qua một liên mạng bằng cách chia nó vào những mảnh (Piece) và chọn đường cho mỗi mảnh như những đơn vị độc lập. Những tầng khác chứa những chức năng đảm bảo truyền dữ liệu tin cậy, những chức năng này được đặt chỉ trong những máy chủ nguồn và đích.

2. Sự phân tầng (Layering)

Trong cấu trúc phân lớp nầy khi dữ liệu truyền từ lớp ứng dụng (Application) cho đến truy cập mạng (Network Access) thì mỗi tầng đều cộng thêm vào dữ liệu phần điều khiển của mình để đảm bảo cho việc truyền tin được chính xác. Mỗi thông tin điều khiển nầy được gọi là Header và được đặt trước phần dữ liệu được truyền, mỗi lớp đều xem thông tin mà nó nhận được từ lớp trên là dữ liệu và đặt thêm phần thông tin điều khiển 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 bao bọc (Encapsulation). Quá trình nhận dữ liệu theo chiều ngược lại nghĩa là mỗi lớp sẽ tách ra phần Header trước khi truyền dữ liệu lên lớp trên.

Mỗi lớp có cấu trúc dữ liệu độc lập, và mỗi lớp không cần biết đến cấu trúc dữ liệu được dùng ở lớp trên hay lớp dưới của nó. Trong thực tế cấu trúc dữ liệu của một lớp được cấu tạo tương thích với cấu trúc dữ liệu ở các lớp ngay cạnh để cho việc truyền dữ liệu được hiệu quả hơn.

Tuy nhiên mỗi lớp vẫn có cấu trúc dữ liệu riêng và có thuật toán riêng để mô tả cấu trúc của nó.

Để thực hiện một sự trao đổi đáng tin cậy giữa các máy tính với nhau, có nhiều quá trình phải được thực hiện là:

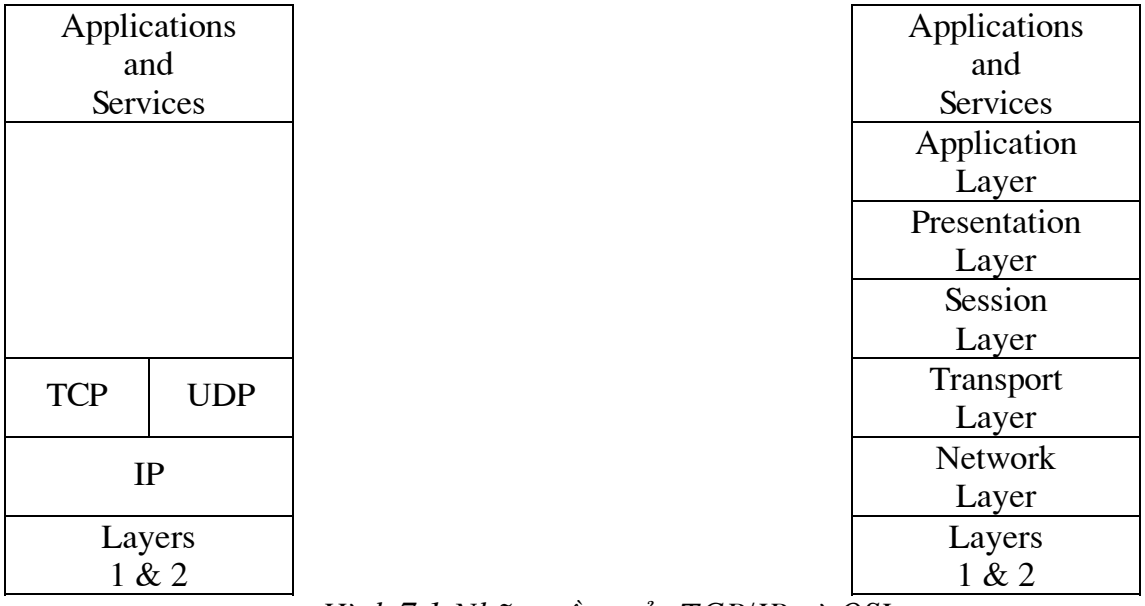
- Định dạng dữ liệu
- Đóng gói dữ liệu
- Quyết định đường dẫ cho dữ liệu.
- Qui định tốc độ truyền dữ liệu theo độ rộng băng tầng sẵn có và khả năng nơi nhận để nhận dữ liệu vào.

- Truyền dữ liệu trên môi trường vật lý.
- Tập hợp dữ liệu vào một cách tuần tự ở những mảnh (Piece).
- Kiểm tra những mảnh xem có sự trùng lặp nhau không.
- Thông báo cho bên gửi biết có bao nhiêu dữ liệu đã được nhận an tòan.
- Phân phát dữ liệu đến đúng những ứng dụng.
- Xử lý lỗi và vấn đề về những sự cố.

Chúng ta có thể thấy tất cả những qui trình ở trên làm cho phần mềm truyền thông quá phức tạp.

Một động lực theo sau mô hình phân tầng là để phần mềm truyền thông có một cấu trúc đơn giản, hợp lý và dễ dàng để thay đổi. Sự phân tầng rõ ràng dành cho những giao thức TCP/IP đã được đưa ra bởi những đòi hỏi của những tổ chức nghiên cứu khóa học, quốc phòng. Giao thức liên mạng IP (Internet Protocol) được cần thiết để kết nối những kiểu mạng khác nhau vào một liên mạng. Nó cung cấp một dịch vụ phân phát dữ liệu không kết nối (Connecctionless) đến tầng giao vận (Transfort Layyer). Chức năng chính của nó là những giao thức chọn đường, cung cấp những phương tiện cho những thiết bị để khám phá topo của mạng, cũng như dó tìm những sự thay đổi trạng thái trong những nút mạng, những liên kết và những máy chủ. Giao thức TCP (Transmition Control Protocol) cung cấp việc truyền dữ liệu đáng tin cậy nó điều khiển lỗi, phát lại, điều khiển dòng và cung cấp sự phân phát End-To-End đáng tin cậy.

Sự phân lớp của OSI về sau đã bị ảnh hưởng mạnh mẽ bởi phương pháp tổ chức của TCP/IP. Mô hình phân lớp OSI và những ngôn ngữ OSI trở thành một phần chuẩn của sự mở rộng truyền số liệu.



Hình 7.1 Những tầng của TCP/IP và OSI.

Hình 7.1 giới thiệu những tầng của máy chủ được phân tầng theo TCP/IP và OSI. Những tầng dưới là tầng vật lý và tầng liên kết dữ liệu, sẽ được bàn chi tiết trong chương IV. Khác với ngôn ngữ của OSI ngôn ngữ của TCP/IP xem những tầng thấp là tầng 1 và tầng 2.

***2.1** Lớp truy cập mạng (Network Access Layer: 1&2).*

Lớp truy cập mạng giải quyết những vấn đề như: Những tín hiệu vật lý, những bộ ghép nối vật lý, điều khiển thâm nhập đường truyền, những chương trình điều khiển thiết bị. Chúng đóng gói dữ liệu vào những khối được gọi là những khung (Frames) hoặc những gói (Packets) và gởi dữ liệu từ giao tiếp trên hệ thống nội bộ đến một giao tiếp đích được ghép đến cùng lớp vật lý của mạng. Những mạng LAN và những mạng WAN cung cấp những chức năng lớp thấp này.

Ranh giới giữa IP và những lớp thấp là một vấn đề quan trọng. Khi một nhà cung cấp thực hiện ranh giới này tốt thì:

Một kiểu giao tiếp mạng mới và môi trường cho IP có thể được thêm vào một máy tính một cách khá dễ dàng.

Giao thức liên mạng (IP) có thể dùng chung một giao tiếp mạng đường truyền với những giao thức khác. Chẳng hạn cả hai kiểu lưu thông TCP/IP và DECnet có thể dùng chung giao tiếp Ethernet.

2.2 Lớp mạng IP và OSI (Tầng 3)

Lớp IP gửi dữ liệu giữa các máy chủ với nhau. Dữ liệu có thể truyền thông qua một mạng đơn giản hoặc có thể vài mạng trong một liên mạng. Dữ liệu được đưa vào những khối được gọi là những Datagram. Tầng IP được gọi là không kết nối (Connectionless) bởi vì mỗi Datagram được chọn đường độc lập và giao thức IP không đảm bảo độ tin cậy hoặc sự phân phát tuần tự những Datagram.

Tầng IP tương ứng với tầng mạng của mô hình OSI (tầng 3). OSI còn xác định một dịch vụ định hướng kết nối (Connection-oriented) tại tầng này. Kết nối X.25 là ví dụ của kiểu dịch vụ này.

2.3 Lớp giao vận TCP, UDP và OSI (lớp 4)

Lớp giao vận nằm ngay trên lớp liên mạng. Hai giao thức quan trọng của lớp nầy là TCP (Transmission Control Protocol) và UDP (User Datagram Protocol). TCP cung cấp dịch vụ truyền dữ liệu để tin tưởng với khả năng phát hiện lỗi và sửa chữa theo kiểu End_to_End còn UDP cung cấp các chương trình ứng dụng thâm nhập trực tiếp đến các dịch vụ lưu truyền Datagram, điều nầy cho phép trao đổi các thông điệp ra ngoài mạng với một số lượng nhỏ các giao thức. Cả hai giao thức nầy đều truyền dữ liệu giữa lớp ứng dụng và Internet.

Trong khi UDP là thuộc loại "*không liên kết*" như đã nói ở trên thì TCP là giao thức thuộc loại "*có liên kết*" nghĩa là phải có các thủ tục thiết liên kết và thủ tục giải phóng liên kết. Về chức năng TCP tương đương với lớp giao thức đầy đủ nhất của lớp giao vận trong mô hình OSI. Tuy nhiên TCP có điểm khác là TCP sử dụng phương thức trao đổi các dòng dữ liệu (Data Stream) giữa người sử dụng. Dữ liệu theo dòng cũng được phân đoạn thành các TPDU (Transport Protocol Data Unit) để truyền đi. Giao thức UDP là một giao thức "*không liên kết*", trong hệ thống mạng UDP truyền dữ liệu một cách trực tiếp, UDP sử dụng 16 bit để ghi nhận cổng nguồn và cổng đích trong phần Header của dữ liệu. Cổng (Port) ở đây được đánh số từ 0 đến 1023, các cổng chuẩn là các cổng hay dùng tới, ý nghĩa của một cổng là được quy định theo một chuẩn nhất định. UDP làm công việc rất đơn giản, nó truyền thông diệp tới IP để

yêu cầu truyền, do IP là loại giao thức không thực nên ở đó không có gì đảm bảo cho sự truyền thành công hay không. Khi lớp ứng dụng (Application) gửi một yêu cầu qua UDP Datagram và lời đáp không quay trở lại một lần nào đó thì nó lại yêu cầu lớp ứng dụng gửi yêu cầu lại.

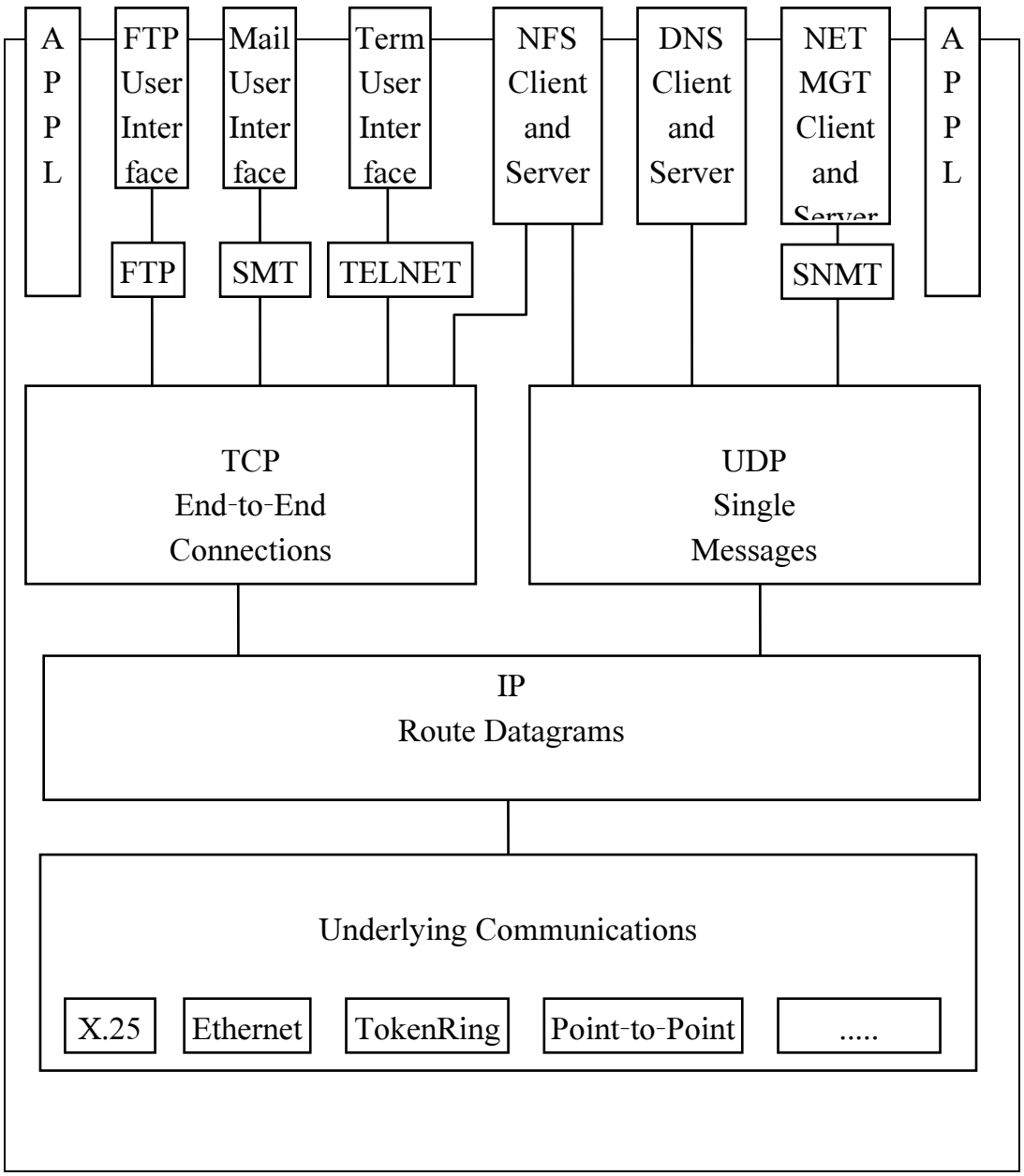
Tầng TCP cung cấp một dịch vụ kết nối dữ liệu không bị lỗi, đầy đủ, tuần tự một cách đáng tin cậy đến các ứng dụng. Chúng gửi những đoạn (Segment) đến tầng IP. Sau đó tầng IP chọn đường cho chúng đến đích. Giao thức điều khiển truyền phát chấp nhận những đoạn đi đến nó từ tầng IP, nếu quy định ứng dụng là nơi nhận, và gửi dữ liệu đến ứng dụng đúng thứ tự mà nó được gửi.

Tầng giao vận trong mô hình OSI có kiểu kết nối định hướng đảm bảo truyền dữ liệu tin cậy, nhưng không giao tiếp trực tiếp với những ứng dụng.

Những tầng OSI cao hơn cung cấp vài chức năng hấp dẫn. Tầng phiên (Session) thiết lập và kết thúc sự truyền thông ứng dụng - ứng dụng. Một cặp ứng dụng sử dụng những phương tiện tầng phiên để thực hiện sự đàm thoại của chúng. Chẳng hạn, chúng quyết định thiết lập, duy trì, thiết lập đồng bộ hóa và hủy bỏ các phiên truyền thông. Những ứng dụng tầng thể hiện (Presentation) để thương lượng một khuôn dạng truyền dữ liệu mà cả hai bên tham gia đều hiểu được.

2.4 Lớp ứng dụng (Application Layer).

Bộ giao thức TCP/IP bao gồm một bộ dịch vụ ứng dụng chuẩn bao gồm sự truyền thông chương trình - chương trình (Program-to-program communications) những dịch vụ truyền file FTP, truyền thư SMTP, truy cập đầu cuối Telnet và thư mục hệ thống tên miền DSN (Domain Name System).



Hình 7.3: Kiến trúc bộ giao thức TCP/IP

Hầu hết những sản phẩm TCP/IP nâng đỡ những chủ dịch vụ file và những khách hàng file hệ thống file mạng NSF (Network system File) cũng như một bộ chức năng mạng đã được dùng một phương tiện RPC.

Thường những sản phẩm còn bao gồm những thư viện chương trình mà có thể được sử dụng bởi những người phát triển phần mềm. Một trong những thư viện chương trình chuẩn gồm giao tiếp chương trình socket. Giao tiếp chương trình socket bao gồm những cuộc gọi cho phép những ứng dụng tuơng tác với tầng giao thức TCP, UDP, hoặc trực tiếp với tầng IP. Thư viện khác được sử dụng để viết những ứng dụng Client/server dựa trên phương tiện RFC.

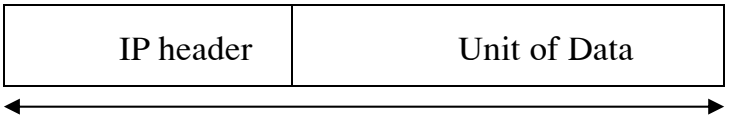
III. GIAO THỨC LIÊN MẠNG IP(INTERNET PROTOCOL)

1. Giới thiệu. Internet Protocol (IP) là giao thức tầng mạng dùng để truyền dữ liệu qua các mạng kết hợp, các nhà nghiên cứu và thiết kế tạo ra IP đáp ứng các yêu cầu sau:

- Thiếp lập hệ thống sử dụng các máy tính, các thiết bị dẫn đường được chế tạo từ các nhà sản xuất khác nhau. Đáp ứng được sự phát triển nhanh chóng của các loại mạng khác nhau đồng thời thừa kế được công nghệ mạng củ.

- Hỗ trợ tầng trên dịch vụ có kết nối và không kết nối.

Giao thức IP cung cấp phương thức truyền các Datagram trên một mạng kết hợp bất kỳ. Cũng giống như một frame trong mạng vật lý. Khái niệm Datagram bao gồm hai phần phần đầu IP header (nơi chứa các thông tin cần thiết cho việc truyền dữ liệu như địa chỉ nguồn , đích...) và phần dữ liệu (Unit of Data).



Datagram

Mỗi Datagram được truyền độc lập với nhau, do vậy thứ tự các Datagram nhận được có thể khác thứ tự các Datagram lúc phát đi. IP không chịu trách nhiệm về việc các Datagram sẽ được truyền đến đích an toàn hay không. IP chỉ có trách nhiệm về truyền các Datagram càng nhanh càng tốt, các Datagram có thể bị mất trong quá trình truyền do các nguyên nhân sau đây:

- "Bit" lỗi xuất hiện trong quá trình truyền.

- Sự quá tải của các Buffer sẽ xoá bỏ các Datagram.

- Tạm thời chưa tìm được đường truyền nào tới đích.

Tất cả các biện pháp nhằm đảm bảo các Datagram được truyền đến đích một cách an toàn, đầy đủ và khôi phục các dữ liệu đã mất đều do TCP đảm nhiệm.

2. Hệ phát chuyển không kết nối (Connectionless).

Dịch vụ internet cơ bản nhất bao gồm một hệ chuyển phát gói dữ liệu. Về mặt kỷ thuật, dịch vụ nầy được định nghĩa như là dịch vụ không có độ tin cậy (unreliable), hệ phát chuyển connectionless tương tự như dịch vụ cung cấp bởi phần cứng mạng mà hoạt động trên mô hình nỗ lực tối đa (best-effort). Dịch vụ nầy được gọi là không có độ tin cậy vì việc phát chuyển không được bảo đảm. Gói dữ liệu có thể bị thất lạc, bị trùng lặp, bị chuyển chậm, hoặc di chuyển không theo đúng thứ tự, dịch vụ nầy không nhận ra được những sự việc nầy, và nó cũng không thông báo nơi gửi hoặc nơi nhận. Dịch vụ nầy được gọi là connectionless vì mỗi gói dữ liệu được xử

lý độc lập với các gói khác. Một chuỗi các gói dữ liệu được gửi từ một máy tới máy khác có thể di chuyển theo những con đường khác nhau, hoặc một số bị mất trong khi một số khác vẫn đến được đích. Ngoài ra, dịch vụ nầy được gọi là phát chuyển nỗ lực tối đa vì phần mềm internet thực hiện một số cố gắng lớn nhất để phát chuyển các gói tin. Nghĩa là, Internet không bỏ sót, làm mất các gói dữ liệu một cách bất thường, không có độ tin cậy chỉ xảy ra khi các tài nguyên quá tải hoặc mạng bị hỏng.

3. Mục đích của IP (Internet Protocol).

Giao thức mà xác định cơ chế phát chuyển connectionless, không có độ tin cậy, được gọi là Internet Protocol và thường được gọi tắt là IP. IP cung cấp ba định nghĩa quan trọng. Đầu tiên, giao thức IP định nghĩa đơn vị cơ sở của việc truyền dữ liệu được sử dụng thông qua một TCP/IP Internet. Như thế, nó xác định định dạng chính xác của tất cả dữ liệu khi nó đi qua Internet. Thứ hai, phần mềm IP thực hiện chức năng định tuyến (routing), chọn một con đường mà dữ liệu sẽ được gửi đi. Thứ ba, cùng với độ chính xác, đặc tả chính thức của định dạng dữ liệu và việc định tuyến, IP bao gồm một tập hợp các quy tắc mà thể hiện ý tưởng của hệ phát chuyển dữ liệu không có độ tin cậy. Các quy tắc nầy đặc trưng cho cách mà máy tính và bộ định tuyến xử lý các gói dữ liệu, làm thế nào và khi nào thì các thông điệp lỗi được phát sinh, và dưới những điều kiện nào thì các gói dữ liệu được hủy bỏ.

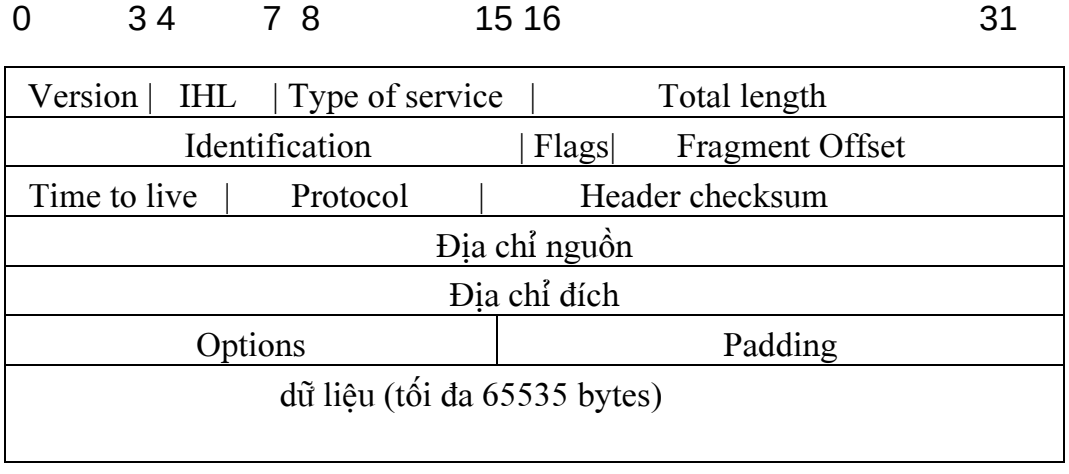
4. Khuôn dạng dữ liệu của IP (IP Datagram).

Bản tin ở lớp giao vận có độ dài 64 Kbyte được truyền xuống lớp mạng. IP cắt thành các gói nhỏ gửi đi. Khi các gói tin tới nơi nhận, chúng được gộp lại bởi lớp giao vận để tạo lại bản tin ban đầu.

Một IP Datagram gồm có phần Header và phần dữ liệu (Data). Phần Header có một phần cố định là 20 byte và một phần tùy ý độ rộng thay đổi.

Mục đích chính của IP là cung cấp khả năng kết nối các mạng con thành liên mạng để truyền dữ liệu. Tất cả các hệ thống thành viên của liên mạng đòi hỏi phải cài đặt IP ở tầng mạng.

Không như thủ tục X.25 hướng kết nối, IP là giao thức không kết nối. Bản tin ở lớp giao vận có độ dài 64 Kbytes được chuyển xuống lớp mạng. IP cắt thành các gói nhỏ gởi đi. Khi đến nơi nhận chúng được gộp lại bởi lớp giao vận để tạo lại bản tin ban đầu.



Hình 7.3: Khuôn dạng của IP

Trong đó:

- Version (4bits) : Chỉ Version của IP hiện hành được cài đặt, để đảm bảo tính tương thích.
- IHL (4bits): Chỉ độ dài phần đầu, để đảm bảo có thể nâng cấp, thêm các thành phần vào cho cấu trúc mà không làm ảnh hưởng đến các phần khác.
- Total length (16bits): Trường nầy chứa độ dài của Datagram (bao gồm header và Data) đo bằng byte. Do số bit của trường nầy là 16 bit nên độ dài lớn nhất có thể là 65535 byte. IP chuẩn yêu cầu tất cả các máy phải có khả năng nhận Datagram có độ dài 576 byte.
- Flags (3bits): liên quan đến phân đọan các datagram
- Header checksum (16bits): mã kiểm sóat lỗi CRC.
- Options: lựa chọn chứa danh sách địa chỉ của Router mà datagram đi qua
- Padding: là vùng đệm.
- Protocol (8bits): chỉ giao thức tầng trên kế tiếp TCP hay UDP
- Time to live (8bits): Trường Time-to-live (TTL) chứa số giây lớn nhất có thể (nhiều nhất là 255 giây) mà Datagram được phép tồn tại trong mạng trước khi tới đích, bất cứ một Datagram nào không tới đích trong khoảng thời gian TTL thì sẽ bị loại bỏ.

Trên thực tế không có một cách xác đinh chính xác nào để theo dõi được trường thời gian nầy. TTL được cài đặt như một máy đếm thời gian đơn giản và khi truyền qua Router thì được giảm đi 1. Tuy nhiên nó sẽ được giảm đi nhiều hơn 1 nếu dữ liệu được chuyển đi với tốc độ chậm.

Giá trị Default của TTL được xác định bằng xấp xỉ hai lần đường truyền dài nhất trên mạng mà Datagram có thể được truyền, đường truyền dài nhất này đôi khi được gọi là bán kính của mạng.

- Identification (16bits): định danh duy nhất cho một datagram
- Fragment Offset (13bits): chỉ vị trí của đọan ở trong datagram. Các trường Indentification, flasg, Fragment Ofset đóng một vai trò quan trọng trong quá trình phân đoạn (ở máy phát) và ghép nối ở máy nhận, trường Indentification chứa nội dung cho phép máy nhận biết được phân đoạn của Datagram có thuộc một Datagram hay không.
- Type of service (8bits): đặc tả các tham số về dịch vụ như độ trễ, thông lượng. quyền ưu tiên, độ tin cậy.

Trường nầy chứa thông tin về quyền ưu tiên của việc truyền các Datagram và những ảnh hưởng có thể xảy ra trong quá trình truyền các Datagram đó. Trường nầy có độ dài 8 bit, IP chuẩn không yêu cầu chỉ ra các hành động cụ thể dựa trên các giá trị của trường Type of Service. IP chỉ định sử dụng nó trong trong việc thiết lập các tùy chọn cho các mạng con mà nó sẽ truyền qua trong bước nhảy tới.

Ví dụ việc truy cập 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 ưu tiên tương ứng của mạng Token Ring.

Một vài máy và Router không quan tâm đến giá trị của trường nầy, trong khi một số khác lại dựa vào đây để giải quyết đường truyền.

Trường nầy có dạng cụ thể như sau:

Frecedence	D	T	R	Resrved

Trong đó : Frecedence (3 bit): Chỉ thị về quyền ưu tiên gửi Datagram cụ thể là:

111: Network Control (cao nhất).

110 : Internet Control.

101 : CRITIC/ECP.

101 : Flag Override.

011 : Flash.

010 : Immediate.

001 : Priority.

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 (Theroughtput) (1 bit): chỉ thông lượng yêu cầu.

  T = 0 : thông lượng bình thường.

  T = 1 : thông lượng cao.

- R (Reliabitily) (1 bit) : chỉ độ tin cậy yêu cầu.

  R = 0 : độ tin cậy bình thường.

R = 1 : độ tin cậy cao.

5. Cấu trúc địa chỉ IP

5.1 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 ôctet (mỗi ôctet có 8 bit, tương đương 1 byte) cách đếm đều từ trái qua phải bít 1 cho đến bít 32, các ôctet tách biệt nhau bằng dấu chấm (.), bao gồm có 3 thành phần chính.

Bit 1..... 32

- Bit nhận dạng lớp (Class bit)
- Địa chỉ của mạng (Net ủD)
- Địa chỉ của máy chủ (Host ủD).

Ghi chú: Tên là Địa chỉ máy chủ nhưng thực tế không chỉ có máy chủ mà tất cả các máy con (Workstation), các cổng truy nhập v.v..đều cần có địa chỉ.

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.**	**0 1 1 1 1 0 1 1.**	**0 1 1 0 1 1 1 0.**	**1 1 1 0 0 0 0 0**
nhận dạng	ôctet 1	ôctet 2	ôctet 3	ôctet 4

2/ - Địa chỉ ủnternet biểu hiện ở dạng thập phân: xxx.xxx.xxx.xxx

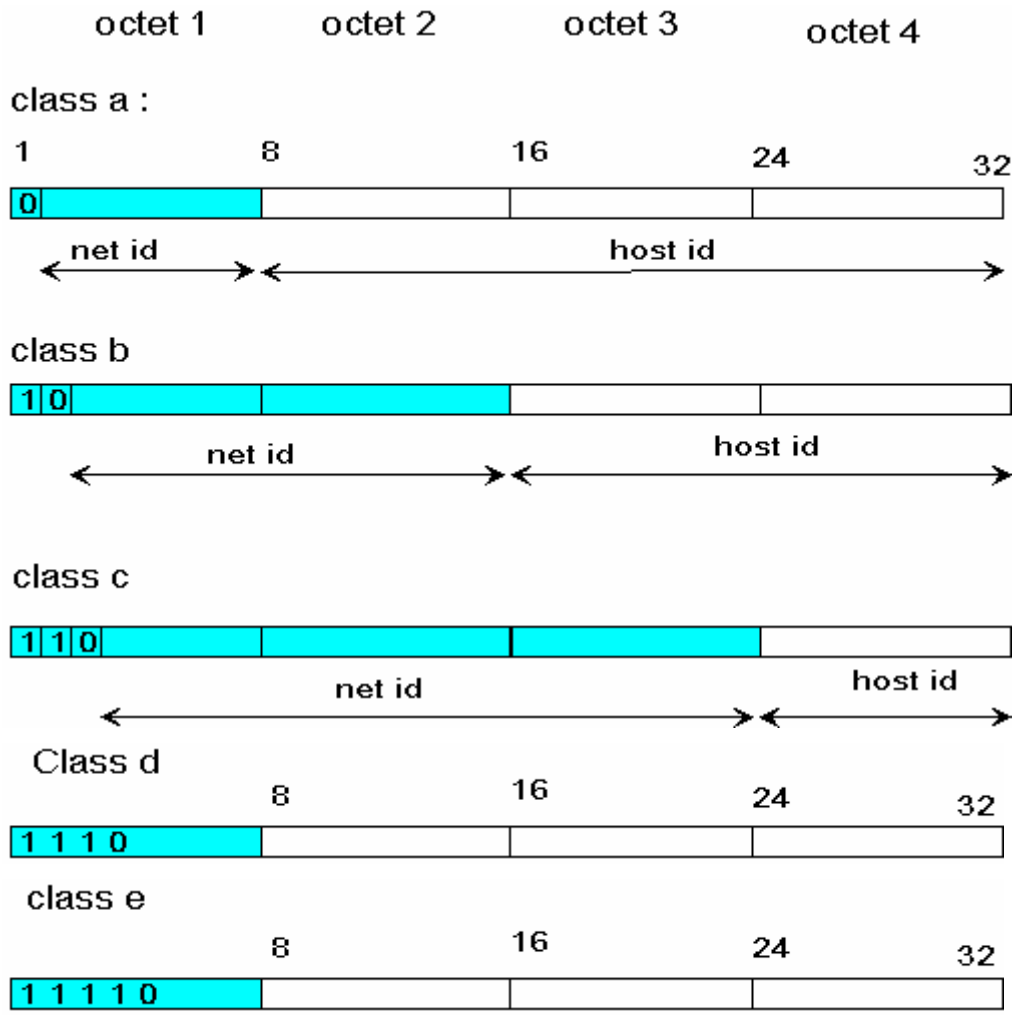
x là số thập phân từ 0 đến 9

Ví dụ: 146. 123. 110. 224

Dạng viết đầy đủ của địa chỉ IP là 3 con số trong từng ôctet. 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.

5.2 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:

- nhận dạng là những bit đầu tiên - của lớp A là 0, của lớp B là 10, của lớp C là 110.
- D có 4 bit đầu tiên để nhận dạng là 1110, còn lớp E có 5 bít đầu tiên để nhận dạng là 11110.
- chỉ lớp A: Địa chỉ mạng ít và địa chỉ máy chủ trên từng mạng nhiều.
- chỉ lớp B: Địa chỉ mạng vừa phải và địa chỉ máy chủ trên từng mạng vừa phải.
- chỉ lớp C: Địa chỉ mạng nhiều, địa chỉ máy chủ trên từng mạng ít.

Địa *chỉ lớp*	*địa chỉ lý thuyết*	*mạng tối đa sử dụng*	*Số máy chủ tối đa trên từng mạng*
	0.0.0.0 đến 127.0.0.0	126	16777214
	128.0.0.0 đến 191.255.0.0	16382	65534
	192.0.0.0 đến 223.255.255.0	2097150	254
	224.0.0.0 đến 240.0.0.0	phân	
	241.0.0.0 đến 255.0.0.0	phân	

Địa *chỉ lớp*	*Vùng địa chỉ sử dụng*	*nhận dạng*	*bit dùng để phân cho mạng*
	1 đến 127	0	7
	128.1 đến 191.254	10	14
	192.0.1 đến 223.255.254	110	21
		1110	---
		11110	---

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.

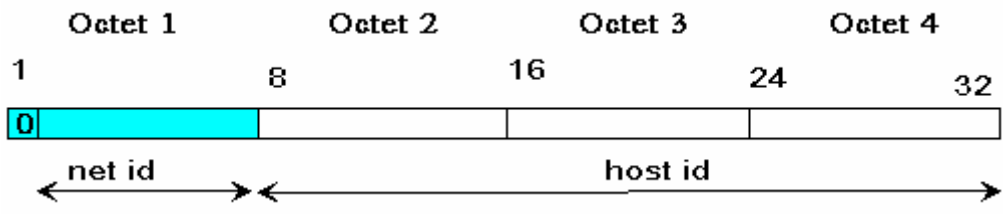
Ghi nhớ: Địa chỉ thực tế không phân trong trường hợp tất cả các bit trong một hay nhiều Octet sử dụng cho địa chỉ mạng hay địa chỉ máy chủ đều bằng 0 hay đều bằng 1. Điều này đúng cho tất cả các lớp địa chỉ

5.3 Địa chỉ Lớp A

Tổng quát chung:

- Bit thứ nhất là bit nhận dạng lớp A = 0.
- 7 bit còn lại trong Octet thứ nhất dành cho địa chỉ mạng.
- 3 Octet còn lại có 24 bit dành cho địa chỉ của máy Chủ.

Class A: (0 - 126)



- net id: 126 mạng
- host id:16.777.214 máy chủ trên một mạng

5.3.1 Địa chỉ mạng (Net ID)

Khả năng phân địa chỉ

Khi đếm số bit chúng ta đếm từ trái qua phải, nhưng khi tính giá trị thập phân 2^n của bit lại tính từ phải qua trái, bắt đầu từ bit 0. Octet thứ nhất dành cho địa chỉ mạng, bit 7 = 0 là bit nhận dạng lớp A. 7 bit còn lại từ bit 0 đến bit 6 dành cho địa chỉ mạng $(2^7) = 128$. Nhưng trên thực tế địa chỉ khi tất cả các bit bằng 0 hoặc bằng 1 đều không phân cho mạng. Khi giá trị các bit đều bằng 0, giá trị thập phân 0 là không có nghĩa, còn địa chỉ là 127 khi các bit đều bằng 1 dùng để thông báo nội bộ, nên trên thực tế còn lại 126 mạng.

Octet 1

Cách tính địa chỉ mạng lớp A.

- Số thứ tự Bit (n)- tính từ phải qua trái: 6 5 4 3 2 1 0
- Giá trị nhị phân (0 hay 1) của Bit: x x x x x x x
- Giá trị thập phân tương ứng khi giá trị bit = 1 sẽ là 2^n
- Giá trị thập phân tương ứng khi giá trị bit = 0 không tính.
- Giá trị thập phân lớn nhất khi giá trị của 7 bit đều bằng 1 là 127.

Như vậy khả năng phân địa chỉ của lớp A cho 126 mạng -

Biểu hiệu địa chỉ trên thực tế: Từ 001 đến 126

5.3.2 Địa chỉ của các máy chủ trên một mạng

Khả năng phân địa chỉ

Ba Octet sau gồm 24 bit được tính từ bit 0 đến bit 23 dành cho địa chỉ máy chủ trên từng mạng.

Với cách tính như trên, để được tổng số máy chủ trên một mạng ta có.

Gía trị tương ứng với Bit n

	trị 2^n	*Địa chỉ*
23.22.21.20.19.18.16.|15.14.13.12.11.10.9.8.|7.6.5.4.3.2.1.0		
..0...0...0...0...0...0...0.|.0...0...0...0...0...0..0.0.|0.0.0.0.0.0.0.0		000
..0...0...0...0...0...0...0.|.0...0...0...0...0...0..0.0.|0.0.0.0.0.0.0.0	2^0	001
..0...0...0...0...0...0...0.|.0...0...0...0...0...0..0.0.|0.0.0.0.0.0.0.0	2^1	002
.....	. . . . .	. . . . .
.....	. . . . .	. . . . .
..1...1...1...1...1...1...1.|.1...1...1...1...1...1..1.1.|1.1.1.1.1.1.1.0	$2^{23}+...+2^1$	16777214
..1...1...1...1...1...1...1.|.1...1...1...1...1...1..1.1.|1.1.1.1.1.1.1.1		16777215
<--------Octet2--------->|<--------Octet3---------->|<---Octet4--->		

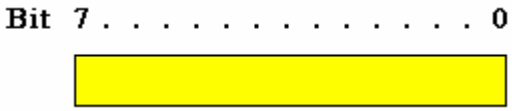
Địa chỉ khi các bit đều bằng 0 hay bằng 1 bỏ ra. Trên thực tế còn lại 224-2 = 16 777 214

Như vậy khả năng phân địa chỉ cho 16 777 214 máy chủ.

Biểu hiện địa chỉ trên thực tế

Octet 2 **Octet 3** **Octet 4**

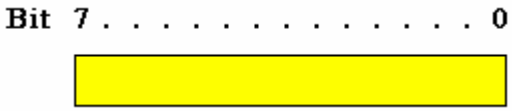
Octet 2



Gía trị tương ứng với thứ tự bit (n) 76543210	*Giá trị 2n*	*Địa chỉ máy chủ*
00000000		000
00000001	2^0	001
00000010	2^1	002
00000011	2^1+2^0	003
.....	.....	.....
.....	.....	.....
11111111	$2^7+2^6+2^5+2^4+2^3+2^2+2^1+2^0$	255

Như vậy giá trị thập phân ở Octet 2 tính từ 000 tới 255.

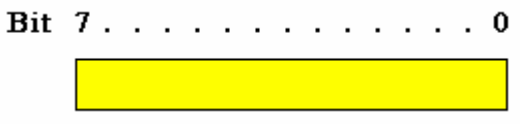
Octet 3



Gía trị tương ứng với thứ tự bit (n) 76543210	*Giá trị 2^n*	*Địa chỉ máy chủ*
00000000		000
00000001	2^0	001
00000010	2^1	002
00000011	2^1+2^0	003
.....	.....	.....
.....	.....	.....
11111111	$2^7+2^6+2^5+2^4+2^3+2^2+2^1+2^0$	255

Như vậy giá trị thập phân ở Octet 3 tính từ 000 tới 255.

Octet 4



Giá trị tương ứng với thứ tự bit (n) 76543210	*Giá trị 2n*	*Địa chỉ máy chủ*
00000000		000 Không phân
00000001	2^0	001
00000010	2^1	002
00000011	2^1+2^0	003
.....	.....	.....
.....	.....	.....
11111110	$2^7+2^6+2^5+2^4+2^3+2^2+2^1$	254
11111111	$2^7+2^6+2^5+2^4+2^3+2^2+2^1+2^0$	255 Không phân

Như vậy giá trị thập phân ở Octet 4 tính từ 001 tới 254.

Tổng quát lại tại địa chỉ của một mạng, khi lần lượt thay đổi các giá trị của các Octet 2, 3, 4. ta sẽ có 16 777 216 khả năng thay đổi mà các con số không trùng lặp nhau (Combinations) có nghiã là 16 777 216 địa chỉ của máy chủ trên mạng, nhưng thực tế phân chỉ là

(256 x 256 x 256) - 2 =16 777 214

Biểu hiện trên thực tế là ba số thập phân trong 3 Octet cách nhau dấu.

Từ 000. 000. 0001 đến 255. 255. 254

Kết luận: Địa chỉ lớp A có thể phân cho 126 mạng và mỗi một mạng có 16 777 214 máy chủ. Nói cách khác địa chỉ thực tế sẽ từ 001.000.000.001 đến 126.255.255.254

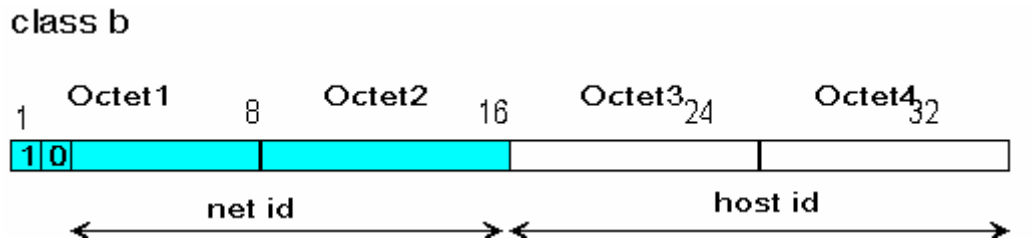
Ví dụ: Một địa chỉ đầy đủ của lớp A: 124. 234. 200. 254. Trong đó:

- Địa chỉ mạng: 124
- Địa chỉ máy chủ: 234.200.254

5.4 Địa chỉ Lớp B

Tổng quát chung:

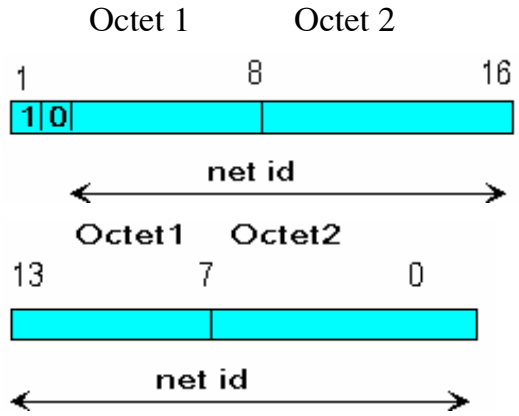
- 2 bit đầu tiên để nhận dạng lớp B là 1 và 0.
- 14 bit còn lại trong 2 Octet đầu tiên dành cho địa chỉ mạng.
- 2 Octet còn lại gồm 16 bit dành cho địa chỉ máy Chủ.



- Net ID: 16.382 mạng
- Host ID: 65.534 máy chủ trên một mạng

5.4.1 Địa chỉ mạng

Khả năng phân địa chỉ



Hai Octet đầu tiên có 16 bit để phân cho địa chỉ mạng, 2 bit (bit 1 và bit 2) kể từ trái sang có giá trị lần lượt là 1 và 0 dùng để nhận dạng địa chỉ lớp B. Như vậy còn lại 14 bit để cho Net ID - địa chỉ mạng.

Theo cách tính như của địa chỉ mạng Lớp A ta có.

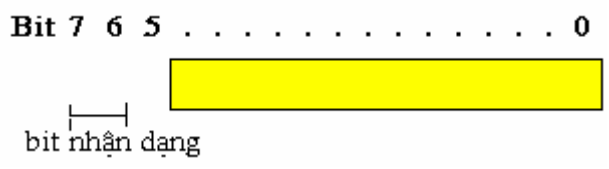
Gía trị bit	*Giá trị 2^n*	*Địa chỉ mạng*
13.12.11.10.9.87.6.5.4.3.2.1.0		
..0...0...0...0..0.00.0.0.0.0.0.0.0		000
..0...0...0...0..0.00.0.0.0.0.0.0.1	2^0	001
..0...0...0...0..0.00.0.0.0.0.0.1.0	2^1	002
.....	. . . . .	. . . . .
.....	. . . . .	. . . . .
..1...1...1...1..1.11.1.1.1.1.1.1.0	2^{13}+...2^1	16 382
..1...1...1...1..1.11.1.1.1.1.1.1.1	2^{13}+... 2^0	Không phân
<-----Octet1-----><--Octet2----->		

Tương tự như địa chỉ Lớp A, các bit đều bằng 0 và các bit đều bằng 1 được bỏ ra, nên thực tế giá trị thập phân chỉ từ 1 đến 16 382 có nghĩa phân được cho 16 382 mạng.

Biểu hiện trên thực tế

Biểu hiện địa chỉ trên thực tế thể hiện số thập phân trong 2 Octet cách nhau bằng dấu chấm (.). Cách tính số thập phân cho từng Octet một.

Octet 1

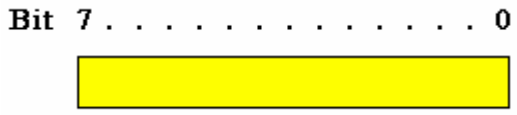


Gía trị tương ứng với thứ tự bit (n) 76543210	*Giá trị 2n*	*Net ID Địa chỉ mạng*
10000000	2^7	128
10000001	2^7+2^0	129
10000010	2^7+2^1	130
10000011	$2^7+2^1+2^0$	131
.....	.....	.....
.....	.....	.....
10111111	$2^7+2^6+2^5+2^4+2^3+2^2+2^1+2^0$	191

Địa chỉ mạng của Lớp A từ 001 đến 126. (không phân 127). Như vậy địa chỉ mạng của Lớp B ở Octet thứ nhất sẽ từ 128 cho đến 191.

Như vậy giá trị thập phân của Octet 1 từ 128 đến 191.

Octet 2



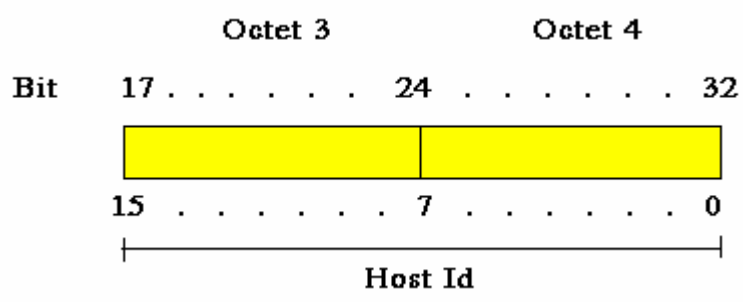
Gía trị tương ứng với thứ tự bit (n) 76543210	*Giá trị 2n*	*Net ID Địa chỉ mạng*
00000000		000 Không phân
00000001	2^0	001
00000010	2^1	002
00000011	2^1+2^0	003
.....	.....	.....
.....	.....	.....
11111110	$2^7+2^6+2^5+2^4+2^3+2^2+2^1$	254
11111111	$2^7+2^6+2^5+2^4+2^3+2^2+2^1+2^0$	255 Không phân

Như vậy giá trị thập phân của Octet 2 từ 001 đến 254.

Như vậy: Địa chỉ mạng lớp B biểu hiện trên thực tế gồm 2 Octet **từ 128.001 cho đến 191. 254** có nghĩa phân được cho 16 382 mạng (214 - 2).

5.4.2 Địa chỉ các máy chủ trên một mạng

Khả năng phân địa chỉ



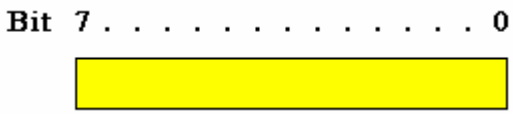
Octet 3 và 4 gồm 16 bit để dành cho địa chỉ của các máy chủ trên từng mạng.

Gía trị Bit .15.14.13.12.11.10..9.8.|7.6.5.4.3.2.1.0	*Giá trị 2^n*	*Địa chỉ*
..0...0...0...0...0...0..0.0.|0.0.0.0.0.0.0.0		000
..0...0...0...0...0...0..0.0.|0.0.0.0.0.0.0.1	2^0	001
..0...0...0...0...0...0..0.0.|0.0.0.0.0.0.1.0	2^1	002
..0...0...0...0...0...0..0.0.|0.0.0.0.0.0.1.1	2^1+2^0	003
.....	. . . . .	. . . . .
.....	. . . . .	. . . . .
..1...1...1...1...1...1..1.1.|1.1.1.1.1.1.1.0	$2^{15}+...2^1$	65534
..1...1...1...1...1...1..1.1.|1.1.1.1.1.1.1.1	$2^{15}+...\ 2^0$	65535
<--------Octet 3---------->|<---Octet 4-->		

Địa chỉ của các bit bằng 0 và bằng 1 bỏ ra, Khả năng thực tế còn lại **65534 địa chỉ** (2^{16} - 2)để phân cho các máy chủ trên một mạng.

Biểu hiện địa chỉ trên thực tế

Octet 3

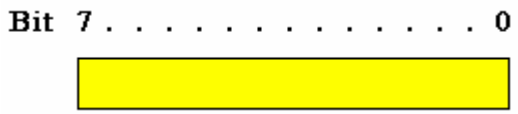


Gía trị tương ứng với thứ tự bit (n) 76543210	*Giá trị 2^n*	*Địa chỉ máy chủ*
00000000		000
00000001	2^0	001

00000010	2^1	002
00000011	2^1+2^0	003
	.....	.....
.....	.....	.....
11111111	$2^7+2^6+2^5+2^4+2^3+2^2+2^1+2^0$	255

Như vậy giá trị thập phân của Octet 3 từ 000 đến 255.

Octet 4



Gía trị tương ứng với thứ tự bit (n) 76543210	***Giá trị 2^n***	***Địa chỉ máy chủ***
00000000		000 Không phân
00000001	2^0	001
00000010	2^1	002
00000011	2^1+2^0	003
.....	.....	.....
.....	.....	.....
11111110	$2^7+2^6+2+2^5+2^4+2^3+2+2^2+2^1$	254
11111111	$2^7+2^6+2^5+2^4+2^3+2^2+2^1+2^0$	255 Không phân

Như vậy giá trị thập phân của Octet 4 từ 001 đến 254.

Biểu hiện địa chỉ máy chủ trên thực tế của Lớp B là từ 000. 001 đến 255. 254

Kết luận: Địa chỉ Lớp B có thể phân cho 16 382 mạng và mỗi mạng có đến 65 534 máy chủ. Nói cách khác địa chỉ phân trong thực tế sẽ từ 128. 001. 000. 001 đến 191. 254. 255. 254

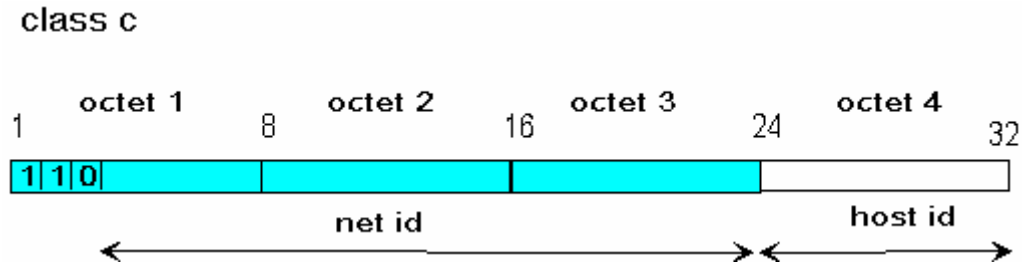
Ví dụ: Một địa chỉ đầy đủ của lớp B là 130.130.130.130. Trong đó:

- **Địa chỉ mạng: 130.130**
- **Địa chỉ máy chủ: 130.130**

5.5 Địa chỉ Lớp C

Tổng quát chung.

- 3 bit đầu tiên để nhận dạng lớp C là 1,1,0.
- 21 bit còn lại trong 3 Octet đầu dành cho địa chỉ mạng.
- Octet cuối cùng có 8 bit dành cho địa chỉ máy chủ.



- net id: 2.097.150 mạng
- host id: 254 máychủ/1 mạng

5.5.1 Địa chỉ Mạng

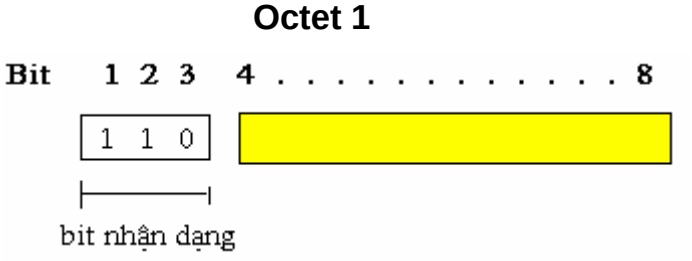
Khả năng phân địa chỉ

21 bit còn lại của 3 Octet đầu dành cho địa chỉ mạng

Giá trị tương ứng với bit n	*trị 2^n*	*chỉ mạng*
20.19.18.17.16.|15.14.13.12.11.10.9.8.|7.6.5.4.3.2.1.0		
.0...0...0...0...0..|.0...0...0...0...0...0.0.0.|0.0.0.0.0.0.0.0.		0
.0...0...0...0...0..|.0...0...0...0...0...0.0.0.|0.0.0.0.0.0.0.1.	20	1
.0...0...0...0...0..|.0...0...0...0...0...0.0.0.|0.0.0.0.0.0.1.0.	21	2
.....	. .	.
.....	. .	.
.1...1...1...1...1..|.1...1...1...1...1...1.1.1.|1.1.1.1.1.1.1.0.	2^{20}+...+2^1	2097150
.1...1...1...1...1..|.1...1...1...1...1...1.1.1.|1.1.1.1.1.1.1.1.	2^{20}+...+2^0	2097151
<----Octet 1---->|<--------Octet 2-------->|<----Octet 3---->		

Các bit đều bằng 0 hay bằng 1 không phân, nên khả năng phân địa chỉ cho mạng ở lớp C là **2 097 150** hoặc bằng 2^{21} - 2.

Biểu hiện trên thực tế

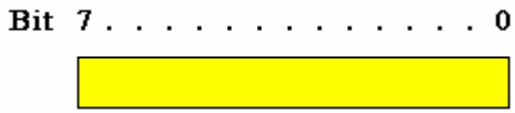


Gía trị tương ứng với thứ tự bit (n)	*Giá trị 2^n*	*Net ID Địa chỉ mạng*

76543210		
11000000	2^7+2^6	192
11000001	$2^7+2^6+2^0$	193
11000010	$2^7+2^6+2^1$	194
11000011	$2^7+2^6+2^1+2^0$	195
.....	.....	.....
.....	.....	.....
11011111	$2^7+2^6+2^5+2^4+2^3+2^2+2^1+2^0$	223

Như vậy giá trị thập phân của Octet 1 từ 192 đến 223.

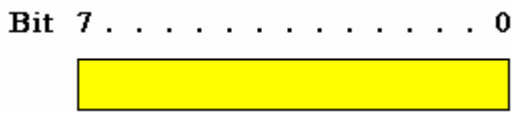
Octet 2



Gía trị tương ứng với thứ tự bit (n) 76543210	*Giá trị 2^n*	*Net ID Địa chỉ mạng*
00000000		000
00000001	2^0	001
00000010	2^1	002
00000011	2^1+2^0	003
.....	.....	.....
.....	.....	.....
11111111	$2^7+2^6+2^5+2^4+2^3+2^2+2^1+2^0$	255

Như vậy giá trị thập phân của Octet 2 từ 000 đến 255.

Octet 3



Gía trị tương ứng với thứ tự bit (n) 76543210	*Giá trị 2^n*	*Net ID Địa chỉ mạng*
00000000		000 Không phân
00000001	2^0	001
00000010	2^1	002
00000011	2^1+2^0	003

.....	.....	.....
.....	.....	.....
11111110	$2^7+2^6+2+2^5+2^4+2^3+2+2^2+2^1$	254
11111111	$2^7+2^6+2^5+2^4+2^3+2^2+2^1+2^0$	255 Không phân

Như vậy giá trị thập phân của Octet 3 từ 001 đến 254.

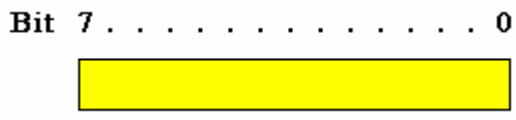
Kết luận: Địa chỉ dành cho mạng của lớp C có khả năng phân cho 2097150 mạng, nói cách khác trên thực tế sẽ từ 192. 000. 001 đến 223. 255. 254.

5.5.2 địa chỉ máy chủ trên từng mạng

Khả năng phân địa chỉ

Octet 4 có 8 bit để phân địa chỉ cho các máy chủ trên một mạng.

Octet 4



Gía trị tương ứng với thứ tự bit (n) 76543210	***Giá trị 2^n***	***Địa chỉ máy chủ***
00000000		000 Không phân
00000001	2^0	001
00000010	2^1	002
00000011	2^1+2^0	003
.....	.....	.....
.....	.....	.....
11111110	$2^7+2^6+2+2^5+2^4+2^3+2+2^2+2^1$	254
11111111	$2^7+2^6+2^5+2^4+2^3+2^2+2^1+2^0$	255 Không phân

Như vậy giá trị thập phân của Octet 4 từ 001 đến 254.

Như vậy khả năng cho máy chủ trên từng mạng của địa chỉ lớp C là 254 hay 2^8-2.

Biểu hiện trên thực tê: Từ 001 đến 254.

Kết luận: Địa chỉ lớp C có thể phân cho 2 097 150 mạng và mỗi một mạng có 254 máy chủ. Nói cách khác sẽ từ 192. 000. 001. 001 đến 223. 255. 254.254

Ví dụ một địa chỉ Internet lớp C đầy đủ: 198. 010. 122. 230. Trong đó:

- Địa chỉ mạng: **198.010.122**
- Địa chỉ máy chủ: 230

Ví dụ: Trung tâm thông tin mạng Internet vùng Châu á - Thái bình dương (APNIC) phân cho VDC 8 địa chỉ của lớp C có thể phân cho 8 mạng từ 203.162.0.0 cho đến 203.162.7.0. Nhóm số thứ nhất là 203 cho biết đây là những khối địa chỉ ở lớp C.

Địa chỉ đầy đủ của một khối địa chỉ 203.162.0.0 phải là 203.162.000.000, chúng ta được sử dụng trọn vẹn octet cuối cùng có nghĩa là được 254 địa chỉ máy chủ và đầu cuối trên một mạng. Ví dụ mạng 203.162.0 sẽ có địa chỉ đầu cuối từ 203.162.0.000 đến 203.162.0. 255. Như vậy tổng cộng VDC có 8x254=2032 địa chỉ lý thuyết để phân cho các máy chủ và đầu cuối trên 8 mạng 203.162.0 ; 203.162.1;.....203.162.7 v.v..

Như vậy địa chỉ mạng là cố định, chúng ta chỉ được quyền phân địa chỉ cho máy chủ trên mạng đó.

6. Địa chỉ Mạng con của Internet (IP subnetting)

6.1 Nguyên nhân

Như đã nêu trên địa chỉ trên Internet thực sự là một tài nguyên, một mạng khi gia nhập Internet được Trung tâm thông tin mạng Internet (NIC) phân cho một số địa chỉ vừa đủ dùng với yêu cầu lúc đó, sau này nếu mạng phát triển thêm lại phải xin NIC thêm, đó là điều không thuận tiện cho các nhà khai thác mạng.

Hơn nữa các lớp địa chỉ của Internet không phải hoàn toàn phù hợp với yêu cầu thực tế, địa chỉ lớp B chẳng hạn, mỗi một địa chỉ mạng có thể cấp cho 65534 máy chủ, Thực tế có mạng nhỏ chỉ có vài chục máy chủ thì sẽ lãng phí rất nhiều địa chỉ còn lại mà không ai dùng được . Để khắc phục vấn đề này và tận dụng tối đa địa chỉ được NIC phân, bắt đầu từ năm 1985 người ta nghĩ đến Địa chỉ mạng con.

Như vậy phân địa chỉ mạng con là mở rộng địa chỉ cho nhiều mạng trên cơ sở **một địa chỉ mạng** mà NIC phân cho, phù hợp với số lượng thực tế máy chủ có trên từng mạng.

6.2 Phương pháp phân chia địa chỉ mạng con

Trước khi nghiên cứu phần này chúng ta cần phải hiểu qua một số khái niệm liên quan tới việc phân địa chỉ các mạng con.

1/ - Default Mask: (Giá trị trần địa chỉ mạng) được định nghĩa trước cho từng lớp địa chỉ A,B,C. Thực chất là giá trị thập phân cao nhất (khi tất cả 8 bit đều bằng 1) trong các Octet dành cho địa chỉ mạng - Net ID.

Default Mask:

Lớp A: 255.0.0.0

Lớp B: 255.255.0.0

Lớp C: 255.255.255.0

2/ - Subnet Mask: (giá trị trần của từng mạng con)

Subnet Mask là kết hợp của Default Mask với giá trị thập phân cao nhất của các bit lấy từ các Octet của địa chỉ máy chủ sang phần địa chỉ mạng để tạo địa chỉ mạng con.

Subnet Mask bao giờ cũng đi kèm với địa chỉ mạng tiêu chuẩn để cho người đọc biết địa chỉ mạng tiêu chuẩn này dùng cả cho 254 máy chủ hay chia ra thành các mạng con. Mặt khác nó còn giúp Router trong việc định tuyến cuộc gọi.

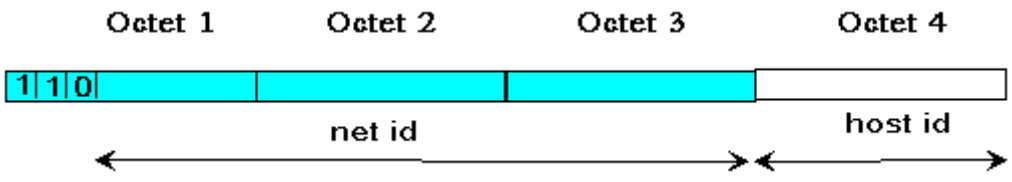
Nguyên tắc chung:

- Lấy bớt một số bit của phần địa chỉ máy chủ để tạo địa chỉ mạng con.
- Lấy đi bao nhiêu bit phụ thuộc vào số mạng con cần thiết (Subnet mask) mà nhà khai thác mạng quyết định sẽ tạo ra.

Vì địa chỉ lớp A và B đều đã hết, hơn nữa hiện tại mạng Internet của Tổng công ty do VDC quản lý đang được phân 8 địa chỉ mạng lớp C nên chúng ta sẽ nghiên cứu kỹ phân chia địa chỉ mạng con ở lớp C.

6.3 Địa chỉ mạng con của địa chỉ lớp C

Class C:



Địa chỉ lớp C có 3 octet cho địa chỉ mạng và 1 octet cuối cho địa chỉ máy chủ vì vậy chỉ có 8 bit lý thuyết để tạo mạng con, thực tế nếu dùng 1 bit để mở mạng con và 7 bit cho địa chỉ máy chủ thì vẫn chỉ là một mạng và ngược lại 7 bit để cho mạng và 1 bit cho địa chỉ máy chủ thì một mạng chỉ được một máy, như vậy không logic, ít nhất phải

dùng 2 bit để mở rộng địa chỉ và 2 bit cho địa chỉ máy chủ trên từng mạng. Do vậy trên thực tế chỉ dùng như bảng sau.

Default Mask của lớp C : 255.255.255.0

```
                                  Địa chỉ
                                 máy chủ
                                <-------->
255.255.255.1   1 0 0 0 0 0 0 ;  192 (2 bit đ/c mạng con 6 bit đ/chỉ máy chủ)
255.255.255.1   1 1 0 0 0 0 0 ;  224 (3 bit đ/c mạng con 5 bit đ/chỉ máy chủ)
255.255.255.1   1 1 1 0 0 0 0 ;  240 (4 bit đ/c mạng con 4 bit đ/chỉ máy chủ)
255.255.255.1   1 1 1 1 0 0 0 ;  248 (5 bit đ/c mạng con 3 bit đ/chỉ máy chủ)
255.255.255.1   1 1 1 1 1 0 0 ;  252 (6 bit đ/c mạng con 2 bit đ/chỉ máy chủ)
<--------------->   <--------->
 Default Mask         Địa chỉ
                      mạng con
```

Trường hợp	Subnetmask	Số lượng mạng con	Số máy chủ trên từng mạng
1	255.255.255.192	2	62
2	255.255.255.224	6	30
3	255.255.255.240	14	14
4	255.255.255.248	30	6
5	255.255.255.252	62	2

Bảng 1: Khả năng chia mạng con của địa chỉ Lớp C

Như vậy một địa chỉ mạng ở lớp C chỉ có **5 trường hợp lựa chọn** trên (Hay 5 Subnet Mask khác nhau), tuỳ từng trường hợp cụ thể để quyết định số mạng con.

1/ Trường hợp 1 - Hai mạng con

Subnet Mask 255.255.255.192.

Từ một địa chỉ tiêu chuẩn tạo được địa chỉ cho hai mạng con, mỗi một mạng có 62 máy chủ.

Sử dụng hai bit (bit 7 và 6) của phần địa chỉ máy chủ để tạo mạng con. Như vậy còn lại 6 bit để phân cho máy chủ.

a/ Tính địa chỉ mạng

	Octet 4		
Bit	7 6	5 4 3 2 1 0	
xxx.xxx.xxx.	0 0	0 0 0 0 0 0	= xxx.xxx.xxx.0
xxx.xxx.xxx.	0 1	0 0 0 0 0 0	= xxx.xxx.xxx.64
xxx.xxx.xxx.	1 0	0 0 0 0 0 0	= xxx.xxx.xxx.128

xxx.xxx.xxx. 1 1 0 0 0 0 0 0 = xxx.xxx.xxx.192

Ghi chú: xxx.xxx.xxx là địa chỉ mạng tiêu chuẩn của lớp C.

Địa chỉ của mạng là giá trị của bit 7 và 6 lần lượt bằng 0 và 1. Trong trường hợp chia địa chỉ mạng con không bao giờ được dùng địa chỉ khi các bit đều bằng 0 hay bằng 1. Do vậy trường hợp 2 mạng con nói trên, địa chỉ mạng con sẽ là:

- Mạngcon 1: Địa chỉ mạng xxx.xxx.xxx.64
- Mạng con 2: Địa chỉ mạng xxx.xxx.xxx.128

b/ Tính địa chỉ cho máy chủ cho mạng con 1

Chúng ta chỉ còn 6 bit cho địa chỉ máy chủ trên từng mạng.

Octet 4

	Bit 7 6	5 4 3 2 1 0	
xxx.xxx.xxx.	0 1	0 0 0 0 0 0	= xxx.xxx.xxx.64
			Địa chỉ mạng
xxx.xxx.xxx.	0 1	0 0 0 0 0 1	= xxx.xxx.xxx.65
xxx.xxx.xxx.	0 1	0 0 0 0 1 0	= xxx.xxx.xxx.66
. . . . .	. . . . .	. . . . .	. . . . .
xxx.xxx.xxx.	0 1	1 1 1 1 1 0	= xxx.xxx.xxx.126
xxx.xxx.xxx.	0 1	1 1 1 1 1 1	=xxx.xxx.xxx.127 Không phân
Địa chỉ mạng con 1			

Mỗi mạng còn lại 62 địa chỉ cho máy chủ.

Mạng 1: Từ xxx.xxx.xxx. 065 đến xxx.xxx.xxx.126

c/ Tính địa chỉ cho máy chủ cho mạng con 2

Tương tự như cách tính trên ta có

Octet 4

Bit 7 6	5 4 3 2 1 0

xxx.xxx.xxx. 1 0	0 0 0 0 0 0	= xxx.xxx.xxx.128 Địa chỉ mạng
xxx.xxx.xxx. 1 0	0 0 0 0 0 1	= xxx.xxx.xxx.129
xxx.xxx.xxx. 1 0	0 0 0 0 1 0	= xxx.xxx.xxx.130
. . . . .	. . . . .	. . . . .
xxx.xxx.xxx. 1 0	1 1 1 1 1 0	= xxx.xxx.xxx.190
xxx.xxx.xxx. 1 0	1 1 1 1 1 1	= xxx.xxx.xxx.191 Không phân
Địa chỉ mạng con 2		

Mạng 2: Địa chỉ máy chủ trên mạng 2.

Từ xxx.xxx.xxx.129 đến xxx.xxx.xxx.190.

Tổng quát lại:

Subnet ID	*Hosts*
0	1-62
64	65-126
128	129-190
192	193-254

a/ Mạng con thứ nhất

* / Địa chỉ mạng con: xxx.xxx.xxx.064

* / Địa chỉ các máy chủ trên mạng con này từ.

xxx.xxx.xxx. 065
xxx.xxx.xxx. 066
xxx.xxx.xxx. 067
.....
õóỳn xxx.xxx.xxx. 126

b/ Mạng con thứ 2

*/ Địa chỉ mạng con: xxx.xxx.xxx. 128

*/ Địa chỉ các máy chủ trên mạng con này từ.

xxx.xxx.xxx. 129
xxx.xxx.xxx. 130
.....
xxx.xxx.xxx. 190

Địa chỉ máy chủ từ 1 đến 62 và từ 193 đến 254 và 127 ; 191 bị mất, nghĩa là mất 130 địa chỉ.

Ví dụ: Địa chỉ tiêu chuẩn lớp C là 196. 200. 123

Subnetmask 255.255.255.192

Từ địa chỉ này ta có 2 mạng con là:

* Mạng 1: Địa chỉ mạng 196.200.123.064

Địa chỉ Máy chủ trên mạng này.

Từ 196.200.123.065 đến 196. 200. 123. 126.

* Mạng 2: Địa chỉ mạng 196.200.123.128

Địa chỉ máy chủ trên mạng này.

Từ 196.200.123.129 đến 196.200.123. 190

2/ Trường hợp 2 - Sáu mạng con

Subnetmask: 255.255.255.224.

Tạo được 6 mạng con, mỗi mạng con có 30 máy chủ

a/ Tính địa chỉ Mạng con

Trường hợp này sử dụng 3 bit (bit 7,6,5) của địa chỉ máy chủ (Octet 4) bổ sung cho địa chỉ mạng tiêu chuẩn để tạo mạng con.

		Octet 4	
Bit	7 6 5	4 3 2 1 0	
xxx.xxx.xxx.	0 0 0	0 0 0 0 0	= xxx.xxx.xxx.0
xxx.xxx.xxx.	0 0 1	0 0 0 0 0	= xxx.xxx.xxx.32
xxx.xxx.xxx.	0 1 0	0 0 0 0 0	= xxx.xxx.xxx.64
xxx.xxx.xxx.	0 1 1 1 0 0	0 0 0 0 0	= xxx.xxx.xxx.96

xxx.xxx.xxx.		0 0 0 0 0	= xxx.xxx.xxx.128
xxx.xxx.xxx.	1 0 1	0 0 0 0 0	= xxx.xxx.xxx.160
xxx.xxx.xxx.	1 1 0	0 0 0 0 0	= xxx.xxx.xxx.192
xxx.xxx.xxx.	1 1 1	0 0 0 0 0	= xxx.xxx.xxx.224

Bỏ trường hợp các bit đều bằng 0 hay 1, chúng ta còn lại địa chỉ của 6 mạng con sau.

xxx.xxx.xxx.32 ; Mạng con 1

xxx.xxx.xxx.64 ; Mạng con 2

xxx.xxx.xxx.96 ; Mạng con 3

xxx.xxx.xxx.128 ; Mạng con 4

xxx.xxx.xxx.160 ; Mạng con 5

xxx.xxx.xxx.192 ; Mạng con 6

b / Tính địa chỉ máy chủ cho mạng con 1

Octet 4

	Bit 7 6 5	4 3 2 1 0	
xxx.xxx.xxx.	0 0 1	0 0 0 0 0	= xxx.xxx.xxx. 32 Địa chỉ mạng
xxx.xxx.xxx.	0 0 1	0 0 0 1 1	= xxx.xxx.xxx.33
xxx.xxx.xxx.	0 0 1	0 0 0 0 0	= xxx.xxx.xxx.34
xxx.xxx.xxx.	0 0 1	0 0 0 1 1	= xxx.xxx.xxx.35
xxx.xxx.xxx.	0 0 1	0 0 1 0 0	= xxx.xxx.xxx.36
. . . . .	. . . .	. . . .	. . . . .
xxx.xxx.xxx.	0 0 1	1 1 1 1 0	= xxx.xxx.xxx.62
xxx.xxx.xxx.	0 0 1	1 1 1 1 1	= xxx.xxx.xxx.63

Không phân

Như vậy địa chỉ máy chủ của mạng con 1 sẽ từ 33 đến 62.

Tương tự như cách tính đã nêu trên chúng ta có thể tính được cho tất cả các trường hợp còn lại (xem bảng 1) và được tổng hợp lại như sau.

1/ Trường hợp 1: Subnetmask 255.255.255.192

- 2 mạng con.
- 62 máy chủ mỗi mạng.

2/ Trường hợp 2: Subnetmask 255.255.255.224

- 6 mạng con.
- 30 máy chủ mỗi mạng.

3/ Trường hợp 3: Subnetmask 255.255.255.240

- 14 mạng con.
- 14 máy chủ mỗi mạng

4/ Trường hợp 4: Subnetmask 255.255.255.248

- 30 mạng con.
- 6 máy chủ mỗi mạng.

5/ Trường hợp 5: Subnetmask 255.255.255.252.

- 62 mạng con.
- 2 máy chủ mỗi mạng.

Xem **Error! Bookmark not defined.** cho các trường hợp trên

Bảng địa chỉ cho các Trường hợp

2 subnets 62 hosts per net 255.255.255.19		6 subnets 30 hosts per net 255.255.255.224		14 subnets 14 hosts per net 255.255.255.240		30 subnets 6 hosts per net 255.255.255.248		62 subnets 2 hosts per net 255.255.255.252	
subnet id	hosts	subnet id	hosts	subnet id	hosts	subnet id	hosts	subnet id	hosts
0	1-62	0	1-30	0	1-14	0	1-6	0	1-2

								4	5-6
								8	9-10
64	65-126	32	33-62	16	17-30	8	9-14	12	13-14
								16	17-18
								20	21-22
128	129-190	64	65-94	32	33-46	16	17-22	24	25-26
								28	29-30
								32	33-34
192	193-254	96	97-126	48	49-62	24	25-30	36	37-38
								40	41-42
								44	45-46
		128	129-158	64	65-78	32	33-38	48	49-50
								52	53-54
								56	57-58
		160	161-190	80	81-94	40	41-46	60	61-62
								64	65-66
								68	69-70
		192	193-222	96	97-110	48	49-54	72	73-74
								76	77-78
								80	81-82
		224	225-254	112	113-126	56	57-62	84	85-86
								88	89-90
								92	93-94
				128	129-142	64	65-70	96	97-98
								100	101-102
								104	105-106
				144	145-158	72	73-78	108	109-110
								112	113-114
								116	117-118
				160	161-174	80	81-86	120	121-122
								124	125-126
								128	129-130
				176	177-190	88	89-94	132	133-134
								136	137-138
								140	141-142
				192	193-206	96	97-102	144	145-146
								146	149-150
								152	153-154
				208	209-222	104	105 -110	156	157-158
								160	161-162
								164	165-166
				224	225-238	112	113-118	168	169-170
								172	173-174
								176	177-178
				240	241-254	120	121-126	180	181-182
								184	185-186
								188	189-190
						128	129-134	192	193-194
				Truong hop 3				196	197-198
								200	201-202
						136	137-142	204	205-206

		208	209-210
		212	213-214
144	145-150	216	217-218
		220	221-222
		224	225-226
152	153-158	228	229-230
		232	233-234
		236	237-238
160	161-166	240	241-242
		244	245-246
		248	249-250
168	169-174	252	253-254
176	177-182		
184	185-190		
192	193-198		
200	201-206		
208	209-214		
216	217-222		
224	225-230		
232	233-238		
240	241-246		
248	249-254		
Truong hop 4		Truong hop 5	

Ví dụ: Địa chỉ mạng lớp C mà NIC phân cho VDC là 203.162.4.0. Trên địa chỉ này phân ra 2 mạng con thì địa chỉ sẽ là.

Mạng 1: Địa chỉ mạng 203.162.4.64.

Địa chỉ máy chủ trên mạng đó từ 203.162.4.65 đến 203.162.4.126

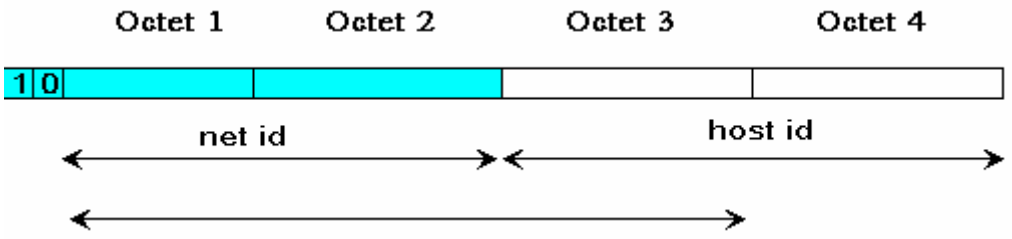
Mạng 2: Địa chỉ mạng 203.162.4.128.

Địa chỉ máy chủ trên mạng đó từ 203.162.4.129 đến 203.162.4.190

6.4 Địa chỉ mạng con từ địa chỉ lớp B

Default Mask của lớp B là 255.255.0.0

class b:



Net ID - Khi phân địa chỉ mạng con sử dụng Octet 3

Địa chỉ lớp B có 2 Octet thứ 3 và thứ 4 dành cho địa chỉ máy chủ nên về nguyên lý có thể lấy được cả 16 bit để tạo địa chỉ mạng . Nếu từ một địa chỉ mạng được NIC phân chúng ta định mở rộng lên 254 mạng và mỗi mạng sẽ có 254 máy chủ. Trường hợp này sẽ lấy hết 8 bit của octet thứ 3 bổ sung vào địa chỉ mạng và chỉ còn lại 8 bit thực tế cho địa chỉ máy chủ, theo cách tính số thập phân 2^n giá trị của 8 bit như đã nêu ở phần lớp C, chúng ta sẽ có:

Bảng phân chia địa chỉ mạng con ở lớp B

Class ***B*** *Subnetting (Default Subnet mask)* **255.255.0.0**	*Mask*	*#of subnets Số mạng con*	*#of hosts per subnet Số máy chủ trên mỗi mạng con*
dụng Octet 3 để mở rộng mạng con	255.255.192.0	2	16382
	255.255.224.0	6	8190
	255.255.240.0	14	4094
	255.255.248.0	30	2460
	255.255.252.0	62	1022
	255.255.254.0	126	510
	255.255..255.0	254	254
dụng cả Octet 4 để mở rộng mạng con	255.255.255.128	510	126
	255.255.255.192	1022	62
	255.255.255.224	2046	30
	255.255.255.240	4094	14
	255.255.255.248	8190	6
	255.255.255.252	16382	2

Địa chỉ lớp B về lý thuyết có 2 octet đầu cho địa chỉ mạng, khi chia mạng con theo phương pháp sử dụng tất cả 8 bit trong 3 octet cho địa chỉ mạng, trên thực tương ứng với lớp C, như vậy về địa chỉ NIC phân là lớp B nhưng cách tổ chức địa chỉ lại ở lớp C (Xem Bảng phụ lục phân địa chỉ mạng con ở lớp B).

Trong bảng này cần chú ý ở cột 6 - khoảng cách địa chỉ giữa 2 mạng con giới thiệu cho chúng ta cách tính địa chỉ các mạng con, địa chỉ các máy chủ trên từng mạng liên quan tới cột 7,8,9,10.

Ví dụ: Trường hợp Subnetmask 255.255.240.0 là rõ nhất.

Chia được 14 mạng con, mỗi mạng con có 4094 máy chủ, khoảng cách địa chỉ giữa hai mạng con là 16.0 có nghĩa.

- Mạng con 1 có địa chỉ là xxx.yyy.16.0 ; Mạng con 2 sẽ có địa chỉ là xxx.yyy.16.0 + 16.0 = xxx.yyy.32.0 cứ tiếp tục như vậy ta sẽ tính được địa chỉ của từng mạng con và mạng con 14 là xxx.yyy. 224.0.
- Địa chỉ máy chủ đầu tiên trên mạng con 1 là xxx.yyy.16.1 ; địa chỉ máy chủ đầu tiên trên mạng con 2 sẽ là xxx.yyy.16.1 + 16.0 = xxx.yyy.32.1. Tiếp tục như vậy ta sẽ tính địa chỉ được máy chủ đầu tiên của mạng con 14 là xxx.yyy.224.1 v.v..
- Tương tự chúng ta biết được địa chỉ cuối cùng của các máy chủ trên một mạng con.

Theo hướng dẫn này chúng ta sẽ tìm được các trường hợp khác.

Tóm lại chia địa chỉ mạng con cũng phải theo một quy luật nhất định ngoài ý muốn của chúng ta, khi chia mạng con cũng bị mất khá nhiều địa chỉ, mất ít hay nhiều tuỳ thuộc vào các trường hợp cụ thể.

6. Các vấn đề khi thực hiện giao thức liên mạng IP.

Sự thực hiện của giao thức liên mạng phụ thuộc vào chất lượng các tài nguyên trên các máy, các Router của mạng đó và hiệu quả sử dụng các tài nguyên như thế nào.

Các tài nguyên bao gồm:

- Độ lớn của băng truyền.
- Bộ nhớ đệm (Buffer).
- Tốc độ xử lý của CPU.

6.1 Độ lớn của băng truyền.

IP sử dụng băng truyền một cách rất hiệu quả, các Datagram được xếp hàng để chuyển tới trạm tiếp theo ngay khi băng truyền có thể truyền được. Sẽ không có hiện tượng sử dụng lãng phí do việc dành riêng băng truyền cho một đường truyền cụ thể nào hay phải đợi xác nhận rồi mới tiếp tục truyền.

Hơn thế nữa, các giao thức truyền tin IP mới ngày nay có thể chia băng truyền ra từng đường truyền và có khả năng chọn lựa đường truyền linh hoạt để tránh hiện tượng tắc nghẽn. Việc sử dụng các giao thức IP như thế sẽ giúp chúng ta duy trì và sử dụng tối đa khả năng sẵn có của tài nguyên truyền thông.

6.2 Bộ nhớ đệm (Buffer).

Khi đã truyền Datagram đi khỏi thì trách nhiệm của IP đối với Datagram là đã hết. Vùng nhớ đệm dùng để xử lý các Datagram này được giải phóng để sử dụng lại. Tuy nhiên, IP tại máy nhận thì phải sử dụng một bộ nhớ đệm để tái tạo lại các Datagram từ phân đoạn của nó.

Vấn đề tắc nghẽn có thể xảy ra khi Router làm công việc đấu nối giữa các mạng có tốc độ nhanh với các mạng có tốc độ chậm. Các Datagram từ mạng có tốc độ nhanh làm đầy vùng đệm của Router, điều này thường xuyên xảy ra khi mạng LAN được đấu nối với mạng khác. Mạng khu vực như vậy ISDN, TI, SMDS hoặc LAN là lựa chọn thích hợp khi ta muốn lưu giữ được tính đầy đủ của băng truyền khi truyền dữ liệu.

IV. GIAO THỨC ĐIỀU KHIỂN TRUYỀN TCP (TRANSMISSION CONTROL PROTOCOL)

Tại mức thấp nhất, các mạng truyền thông máy tính cung cấp dịch vụ phát chuyển không tin cậy. Các gói dữ liệu có thể bị mất hay bị hỏng khi các lỗi đường truyền tác động lên dữ liệu, hoặc khi phần cứng mạng bị hỏng, hay khi mạng bị quá tải bởi vì lượng giao dịch vượt quá khả năng của mạng. Với những mạng chuyển gói tin tự động cũng có thể phát chuyển chúng không theo đúng thứ tự, phát chuyển chúng với độ trì hoãn lớn, hay phát chuyển bị trùng lặp.

Tại mức cao nhất, các chương trình ứng dụng thường phải gửi một khối lượng lớn dữ liệu từ máy này đến máy khác. Sẽ rất khó khăn khi phải sử dụng hệ phát chuyển Connectionless, không tin cậy để truyền một khối lượng lớn dữ liệu.

Vì vậy một trong những mục đích của việc nghiên cứu giao thức mạng là để tìm ra giải pháp chung cho vấn đề cung cấp dịch vụ phát chuyển theo dòng (stream) đáng tin cậy, giúp cho việc xây dựng duy nhất một phiên bản phần mềm giao thức Stream mà tất cả chương trình ứng dụng có thể sử dụng. Việc có được duy nhất một giao thức cũng giúp tách biệt các chương trình ứng dụng khỏi chi tiết của mạng, và ta cũng có thể định nghĩa một giao thức thống nhất cho dịch vụ truyền Stream.TCP là một giao thức vận chuyển hướng kết nối, nó đảm bảo độ tin cậy end-to-end đối với lớp mạng.

1. Các tính chất của dịch vụ phát chuyển tin cậy.

Sự giao tiếp giữa các chương trình ứng dụng và dịch vụ phát chuyển tin cậy TCP/IP có thể được đặc trưng bởi 5 khía cạnh:

- **Định hướng Stream:** Khi hai chương trình ứng dụng truyền những khối lượng dữ liệu lớn, dữ liệu này được xem như một chuỗi các bit, được chia thành các

octet - 8 bit mà chúng ta thường gọi là byte. Dịch vụ phát chuyển Stream trên máy đích chuyển đến nơi nhận một cách chính xác cùng một chuỗi các octet mà máy đích gửi nó đi.

- **Kết nối mạch ảo:** Thực hiện việc truyền Stream cũng tương tự như thực hiện một cuộc gọi điện thoại, trước khi việc truyền có thể bắt đầu, cả hai chương trình ứng dụng gửi và nhận tương tác với hệ điều hành của chúng, thông báo về việc chúng muốn có được việc truyền Stream. Các modules phần mềm giao thức trong hai hệ điều hành liên lạc với nhau, kiểm tra xem việc truyền đã được cho phép hay chưa, nơi gửi và nơi nhận đã sẵn sàng chưa. Một khi tất cả các chi tiết đã được thiết lập, các Modules thông báo cho các chương trình ứng dụng rằng kết nối đã được thiết lập và có thể bắt đầu truyền.

- **Việc truyền có vùng đệm:** Khi truyền dữ liệu, mỗi chương trình ứng dụng có thể sử dụng bất kỳ kích thước đơn vị truyền nào nó thấy thuận tiện, mà có thể chỉ bằng nột octet. Tại nơi nhận, phần mềm giao thức phát chuyển tự động dữ liệu theo đúng chính xác thứ tự mà chúng gửi đi làm cho chúng được sử dụng với chương trình ứng dụng ở nơi nhận, ngay sau khi chúng được nhận và kiểm tra. Phần mềm giao thức tự do phân chia dòng dữ liệu thành gói dữ liệu độc lập với đơn vị mà chương trình ứng dụng truyền đi. Để làm cho việc truyền hiệu quả hơn và để tối thiểu giao thông trên mạng.

Đối với chương trình mà dữ liệu phải được phát chuyển ngay cả khi nó không đầy một vùng đệm, dịch vụ Stream cung cấp một cơ chế đẩy (Push) mà các chương trình ứng dụng sử dụng để bắt buộc truyền đi.

- **Stream không có cấu trúc:** Dịch vụ TCP/IP Stream không xác định dòng dữ liệu có cấu trúc. Ví dụ chương trình trả lương nhân viên, không có cách nào để mà dịch vụ Stream đánh dấu biên giới giữa các bản ghi nhân viên. Các chương trình ứng dụng sử dụng dịch vụ Stream phải hiểu nội dung Stream và thống nhất với nhau về định dạng Stream trước khi khởi động việc kết nối.

- **Kết nối hai chiều:** Các kết nối được cung cấp bởi dịch vụ TCP/IP Stream cho phép truyền đồng thời từ cả hai chiều. Cách kết nối này được gọi là Full Duplex. ưu điểm của việc kết nối hai chiều là phần mềm giao thức cơ sở có thể gửi thông tin điều khiển cho một Stream trở về nguồn trong khi những Datagram khác có thể dịch chuyển theo chiều ngược lại. Điều này giúp giảm bớt giao thông trên mạng.

2. Khuôn dạng bảng tin

TCP là thủ tục khá phức tạp, nó đảm bảo độ tin cậy end-to-end đối với 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 và đến đầu bên kia lại được gộp lại thành bản tin ban đầu.

Cấu trúc đơn vị dữ liệu của TCP như sau :

<table>
<tr><td colspan="6">Source Port</td><td colspan="3">Destination Port</td></tr>
<tr><td colspan="9">Sequence Num ber</td></tr>
<tr><td colspan="9">Piggy back Acknowledgement</td></tr>
<tr><td>TCP</td><td></td><td>U</td><td>A</td><td>P</td><td>P</td><td>S</td><td>F</td><td></td></tr>
</table>

header length	reServer	RG	CK	SH	ST	YN	IN	Window
Checksum								Urgent Pointer
Options (0 or more 32 bit word)								
Data								

Hình 7.4: Khuôn dạng bản tin TCP

trong đó:

- *Source port và Destination Port* là các địa chỉ điểm thâm nhập dịch vụ lớp giao vận (CCISAP address). TCP có số lượng các cổng trong khoảng 0 cho đến 2^{16} -1. Các cổng có số nằm trong khoảng từ 0 tới 1023 là được biết nhiều nhất vì các cổng này được sử dụng cho việc truy nhập tới các dịch vụ tiêu chuẩn.

- *Sequence Number* : là số thứ tự đầu tiên của các byte dữ liệu được gửi đi.

- *Piggy back Acknowledgement* : số thứ tự đầu tiên của các byte dữ liệu đang chờ thu. Thông số này chỉ được xác định khi ACK = 1.

- *TCP header length* : độ dài của TCP header.

- *Reserved* : dành cho sau này (đặt zero).

Các bít điều khiển hay là:

- *URG* : phải xử lý trước các số liệu khác hay là vùng con trỏ có hiệu lực.

- *ACK* : biên nhận số liệu đã thu đúng.

- *PS :* chuyển số liệu

- *RST :* hủy bỏ kết nối do lỗi phần mền hoặc cứng.

- *SYN* : đồng bộ để thiết lập kết nối.

- *FIN* : để kết thúc kết nối.

- *Window* : để điều khiển thông lượng và quản lý bộ đệm (buffer).

- *Checksum* : từ tổng kiểm tra để đảm bảo thu nhận đúng.

- *Urgent Pointer* : Con trỏ này trỏ tới số hiệu tuần tự của byte đi theo sau dữ liệu khẩn.

- *Options* : tùy ý, ví dụ để thông báo kích thước buffer.

3. Quá trình Nối - Tách.

- *Thiết lập kết nối bằng thủ tục bắt tay 3 lần* để tăng độ tin cậy (three-way hand shake)/Client gửi bản tin với SYN = 1 (yêu cầu kết nối)/Server nhận được, nó gửi bản tin với SYN = 1 và ACK = 1/Client lại đáp lại với bản tin ACK = 1.

Qúa trình nối

Client yêu cầu nối **Server**

Gởi Syn SYN = 1, Seq = X

SYN = 1, ACK = 1, Ack = X + 1, Seq = Y trả lời đồng ý nối

Trả lời ACK = 1, Ack = Y + 1 ⌫ trả lời cho Y

- Kết thúc kết nối bằng thủ tục bắt tay 2 lần (two-way hand shake)

Bên kết thúc gửi số liệu, nó gửi bản tin với FIN = 1. TCP cho phép nhận tiếp tục số liệu cho bên kia gửi bản tin FIN = 1.

Quá trình tách

Client **Server**

Gửi yêu cầu kết thúc ⌫ thiết lập FIN = 1

Đồng ý gửi trả lời

FIN = 1

4. Quá trình trao đổi số liệu

Chúng ta khảo sát quá trình trao đổi dữ liệu giữa Client và Server thông qua các hàm nguyên thủy, cơ chế báo lỗi ACK và kiểm soát luồng bằng cửa sổ W

Client Server

Send DATA

REQ = 1, PSH = 1, Seq = X

ACK = 1, Ack = X + N + 1 Send ACK

Window = N

SEQ = 1, Seq = Y Send DATA

SEQ = 1, Seq = Y + W Send DATA

Send ACK ACK = 1, Ack = Y + W + 1

Send ACK ACK = 1, Ack = 2W + 1 Window = W

Window = W Send DATA

SEQ = 1, Seq = Y + 2W

Send ACK ACK = 1, Ack = Y + 3W + 1

Window = W

W = Maximum segment size (W>N)

2W = Windows limit

Trong đó PSH = 1: đẩy dữ liệu đi ACK = 1. Xác nhận biên nhận Act = X+N+1 sẽ nhận gởi tiếp theo và cửa sổ N.

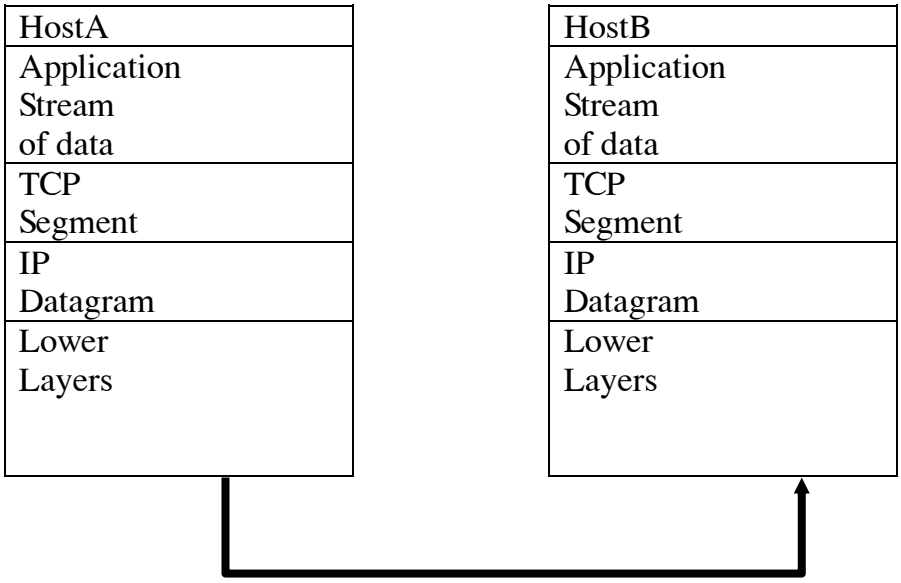
TCP trên máy host có nhiệm vụ đảm bảo dữ liệu được truyền tới đích phải:

- Chính xác
- Liên tục
- Trọn vẹn
- Không có lặp

Khi 1 ứng dụng gửi một dòng byte đến tầng TCP. Tầng TCP chia dòng byte này thành các gói nhỏ (piece) và thêm vào mỗi gói nhỏ một phần đầu (Header) tạo thành một đoạn (Segment) sau đó đưa xuống tầng IP để tạo thành các Datagaram

Khi TCP nhận nó kiểm tra xem có bao nhiêu dữ liệu đúng đã được nhận bởi ý nghĩa vùng ACK (Acknowledgment). Nếu một ACK cho một đoạn không đến trong một khoảng thời gian nhất định. TCP gửi lại đoạn đó. Phương pháp này được gọi là sự phát lại dựa vào sự báo nhận. Thỉnh thoảng một sự phát lại sẽ gây ra những đoạn giống nhau được phân phát đến TCP nhận. Khi TCP nhận nó phải sắp xếp những Segment đúng thứ tự, loại bỏ sự giống nhau và khi truyền ngược lại TCP phân phát dữ liệu đến với ứng dụng của nó theo thứ tự mà không có sự sai sót ở những mảnh. (đoạn dữ liệu)

Trong thực tế có hai dòng dữ liệu được truyền. TCP có thể tham gia vai trò của người gửi và đồng thời tham gia vai trò của người nhận.



Hình 7.5: Một ứng dụng sử dụng tầng giao thức TCP

Để đạt được tính tin cậy, nơi gửi truyền một gói dữ liệu và sau đó đợi lời đáp (ACK) trước khi truyền gói dữ liệu khác. Khi đó mạng sẽ hoàn toàn ở trạng thái nhàn rỗi trong khoảng thời gian máy tính trì hoãn lời đáp (ví dụ trong khi máy phải tính Checksum hay định tuyến). Nếu một mạng có độ trì hoãn lớn thì điều này sẽ rõ ràng hơn.

Từ những lí do đó đã hình thành nên một khái niệm với tên gọi *cửa sổ trượt* (Sliding Window), làm cho việc truyền đạt hiệu quả hơn.

Kỷ thuật cửa sổ trượt là một dạng phức tạp hơn của lời đáp tích cực và truyền lại. Các giao thức cửa sổ trượt sử dụng băng thông của mạng tốt hơn bởi vì chúng cho phép nơi gửi truyền nhiều gói tin trước khi qua trạng thái đợi lời đáp.

Khi nơi gửi nhận lới đáp của của gói dữ liệu đầu tiên bên trong cửa sổ, nó trượt cửa sổ qua bên phải và gửi gói dữ liệu kế tiếp. Cửa sổ vẫn tiếp tục trượt khi nơi gửi vẫn còn nhận được lới đáp. Hiệu suất của cửa sổ trượt phụ thuộcvào kích thước cửa sổ và tốc độ nhận dữ liệu của mạng. Cửa sổ phân chia dãy các gói dữ liệu thành ba tập hợp:

bên trái cửa sổ là những gói dữ liệu đã được truyền đi thành công, đầu kia đã nhận được, đầu này đã nhận được lời đáp. Bên phải cửa sổ là những gói dữ liệu chưa được truyền đi. Bên trong cửa sổ là những gói dữ liệu đã được truyền đi. Gói dữ liệu được đánh số thấp nhất trong cửa sổ là gói dữ liệu đầu tiên trong dãy này mà chưa nhận được lời đáp.

5. Các vấn đề khi thực hiện giao thức TCP.

5.1 Cách thiết lập kết nối. TCP là giao thức kết nối có định hướng (Connecttion - Oriented) đòi hỏi cả hai máy tham gia kết nối để truyền dữ liệu. Trước khi một giao dịch TCP có thể chuyển qua Internet, các chương trình ứng dụng ở hai đầu của kết nối phải cùng đồng ý rằng chúng mong muốn có kết nối. Để làm việc này máy chủ thực hiện một chức năng *mở thụ động* (Passive Open) bằng cách liên hệ với hệ điều hành của nó và chỉ ra rằng nó đã sẵn sàng cho việc kết nối. Lúc này hệ điều hành sẽ gán một giá trị cổng TCP cho kết nối tại máy chủ. Chương trình ứng dụng ở máy trạm liên hệ với hệ điều hành của nó và sử dụng chức năng *mở chủ động* (Active Open) để thiết lập kết nối.

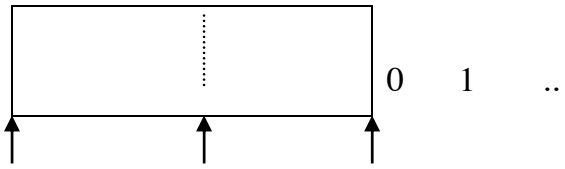
Hai module phần mềm TCP sẽ thông tin liên lạc với nhau để thiết lập và kiểm tra kết nối. Một khi kết nối đã được thực hiện xong, các chương trình ứng dụng có thể bắt đầu việc truyền dữ liệu, các module phần mềm TCP tại mỗi đầu trao đổi thông điệp với nhau để đảm bảo việc phát chuyển đáng tin cậy.

5.2 Segment, stream và số thứ tự

TCP xem một dòng dữ liệu như một dãy các octet hay byte mà nó chia thành những đoạn (segment) để truyền đi. Mỗi Segment di chuyển qua Internet trong một IP Datagram.

TCP sử dụng một cơ chế cửa sổ trượt đặc biệt để giải quyết hai vấn đề quan trọng đó là: hiệu quả của việc truyền và điều khiển tốc độ dòng dữ liệu. Giống như giao thức cửa sổ trượt đã được mô tả, cơ chế cửa sổ trượt TCP cho phép gửi đi nhiều Segment trước khi nhận được lời đáp (ACK). Như vậy sẽ tăng được toàn bộ hiệu suất và giảm thời gian nhàn rỗi của mạng. Dạng TCP của giao thức cửa sổ trượt cũng giải quyết vấn đề điều khiển tốc độ dòng chuyển End - to - End, bằng cách cho phép nơi nhận giới hạn lại việc truyền cho đến khi nó có đủ không gian vùng đệm để chấp nhận thêm dữ liệu.

Cơ chế cửa sổ trượt TCP hoạt động theo octet, không phải theo Segment hay theo gói dữ liệu. Các octet của dòng dữ liệu đánh số tuần tự, và nơi gửi duy trì ba con trỏ phối hợp với mỗi kết nối. Con trỏ đầu tiên đánh biên bên trái cửa sổ trượt, tách biệt với những octet đã được gửi và đã nhận được lời đáp ra khỏi những octet còn chưa được đáp lời. Con trỏ thứ hai đánh dấu biên bên phải cửa sổ trượt và xác định octet cao nhất trong dãy này mà có thể được gửi đi trước khi nhận được thêm lời đáp. Con trỏ thứ ba đánh dấu biến bên trong cửa sổ tách biệt những octet đã được gửi đi và những octet chưa được gửi đi. Phần mềm giao thức gửi đi tất cả các octet trong cửa sổ mà không hề trì hoãn, vì vậy đường biên bên trong cửa sổ trượt luôn luôn di chuyển nhanh chóng từ trái sang phải. Hình 2-5 mô tả hoạt động của cửa sổ này.



Hình 7.5 Cửa sổ trượt của TCP.

Bởi vì các kết nốiTCP là hai chiều, hai quá trình truyền xảy ra đồng thời trên mỗi kết nối, mỗi quá trình theo một chiều. Như thế phần mềm TCP tại mỗi đầu duy trì hai cửa sổ cho mỗi kết nối (tổng cộng hai đầu là 4 cửa sổ), một cửa sổ trượt theo dòng dữ liệu được gửi đi và một cửa sổ trượt theo dữ liệu được nhận vào.

5.3 Cửa sổ với kích thước thay đổi và việc điều khiển tốc độ truyền.

Có một sự khác biệt giữa cửa sổ trượt TCP và cửa sổ trượt được đơn giản hóa trước đây, đó là cửa sổ trượt TCP cho phép kích thước cửa sổ có thể thay đổi qua tùy thời điểm. Với mỗi lời đáp, xác định có bao nhiêu octet đã được nhận, và chứa một thông cáo cửa sổ để xác định có thêm bao nhiêu octet mà máy nhận được chuẩn bị để nhận. Thông cáo cửa sổ này như một cách xác đinh kích thước vùng đệm hiện tại của máy nhận. Để đáp lại việc gia tăng kích thước thông cáo cửa sổ, máy gửi sẽ tăng kích thước cửa sổ trượt của nó và tiến hành gửi các octet còn chưa được đáp lời. Để đáp lại việc giảm bớt kích thước thông cáo cửa sổ, máy gửi sẽ giảm kích thước cửa sổ trượt của nó và thôi gửi các octet vượt qua các vị trí chấp nhận được trước đó trong mỗi chuỗi các octet.

Việc sử dụng cửa sổ trượt có kích thước thay đổi là hổ trợ việc điều khiển tốc độ truyền dữ liệu cũng như là việc truyền đáng tin cậy. Để tránh việc nhận nhiều dữ liệu hơn khả năng lưu trữ, nơi nhận sẽ gửi đi thông cáo cửa sổ nhỏ hơn. Trong trường hợp xấu nhất, nơi nhận sẽ gửi đi thông cáo cửa sổ có kích thước là zero để ngưng tất cả việc truyền. Sau khi vùng đệm đã được giải phóng bớt, nơi nhận lại gửi đi thông cáo cửa sổ là khác zero để kích hoạt trở lại việc truyền.

5.4 Lời đáp (Acknowledgement) và việc truyền lại.

TCP gửi dữ liệu đi trong những Segment có độ dài thay đổi và vì các Segment được truyền lại có thể bao gồm nhiều hơn dữ liệu góc, các lời đáp không thể dễ dàng tham chiếu tới Datagram hay Segment. Thay vì vậy, chúng chỉ tới vị trí ở trong dòng dữ liệu, được đánh theo số thứ tự. Nơi nhận tập hợp các octet dữ liệu từ những Segment gửi đến và xây dựng lại một phiên bản giống như dòng dữ liệu gửi đi. Vì các Segment di chuyển trong IP Datagram, chúng có thể bị mất hoặc phát chuyển không đúng thứ tự , nơi nhận sử dụng số thứ tự này để sắp xếp lại thứ tự các Segment. Tại một thời điểm bất kỳ, nơi nhận sẽ xây dựng lại zero hoặc nhiều hơn octet liên tục nhau từ đầu của dòng dữ liệu nhưng có thể có thêm một số dữ liệu vừa đến từ các Datagram không theo đúng thứ tự. Nơi nhận sẽ luôn đáp lời cho tiền tố dài nhất liên tục nhau của dòng dữ liệu mà nó đã nhận được một cách chính xác. Mỗi lời đáp xác định một số thứ tự có giá trị lớn hơn một so với vị trí octet cao nhất trong tiền tố liên

tục nhau mà nó đã nhận. Như thế nơi gửi sẽ nhận được thông tin phản hồi liên tục từ nơi nhận trong qúa trình xử lý dòng dữ liệu.

Mô hình lời đáp TCP được gọi là tích lũy bởi vì nó cho biết bao nhiêu dữ liệu của dòng dữ liệu đã được tích lũy. ưu điểm của mô hình lời đáp tích lũy là dễ phát sinh vừa không nhầm lẫn, và việc thất lạc lời đáp không nhất thiết phải truyền lại. Khuyết điểm chính là nơi gửi không nhận được thông tin về tất cả các cuộc truyền thành công, nhưng chỉ là một vị trí trong dòng dữ liệu mà đã được nhận.

5.5 ép buộc truyền dữ liệu.

TCP được tự do phân chia dòng dữ liệu thành các Segment để truyền đi mà không xét đến kích thước của đơn vị truyền mà chương trình ứng dụng đang sử dụng. ưu điểm của việc phân chia này là hiệu quả truyền tin. Nó có thể tích lũy đủ lượng octet trong vùng đệm để hình thành nên những Segment có độ dài hợp lý.

Tuy vậy việc sử dụng vùng đệm nó có thể ảnh hưởng đến một số ứng dụng. Chẳng hạn sử dụng kết nối TCP để truyền những ký tự (Character) từ một trạm làm việc tới một máy ở xa. Người sử dụng muốn có lời đáp tức thời cho mọi ký tự nhập vào. Nếu TCP tại nơi gửi lưu trữ dữ liệu trong vùng đệm, lời đáp có thể bị trì hoãn, có thể lên đến cả trăm ký tự. Tương tự tại nơi nhận có thể lưu dữ liệu tạm thời này trong vùng đệm trước khi chuyển đến cho ứng dụng, việc bắt buộc nơi gửi truyền dữ liệu đi có thể chưa đủ để đảm bảo cho việc phát chuyển.

Để giải quyết vấn đề này, TCP cung cấp một thao tác *push* mà chương trình ứng dụng có thể sử dụng để ép buộc phát chuyển các octet hiện đang có trong dòng dữ liệu mà không phải đợi đến lúc đầy vùng đệm. Nó yêu cầu TCP thiết lập bit PSH trong vùng Code của Segment này, để cho dữ liệu sẽ được phát chuyển đến chương trình ứng dụng nơi nhận.

5.6 Đáp ứng với việc nghẽn mạch (Congestion).

Sự nghẽn mạch là một trạng thái mà sự trì hoãn là rất cao gây ra bởi sự quá tải của Datagram tại một hay nhiều điểm (ví dụ tại bộ định tuyến). Khi sự nghẽn mạch xãy ra, độ trì hoãn gia tăng và bộ định tuyến bắt đầu xếp hàng các Datagram cho đến khi nó có thể chuyển chúng đi nhưng vì khả năng lưu trữ của máy là có giới hạn và các Datagram phải cạnh tranh nhau để vào đó. Khi các Datagram đã sắp xếp đầy bộ đệm, thì các Datagram đến sau sẽ bị hủy bỏ.

Thông thường các điểm đầu cuối thường không nhận biết sự nghẽn mạch, và tại sao chúng xảy ra. Bởi vì nghẽn mach là do sự trì hoãn gia tăng. Nên hầu hết các phần mềm giao thức sử dụng bộ đếm thời gian và truyền lại. Việc truyền lại có ảnh hưởng lớn đến hệ thống vì nó sẽ làm tăng thêm sự nghẽn mạch, và đến một lúc nào đó mạng sẽ trở nên vô dụng. Vấn đề này được gọi là *sự sụp đổ do nghẽn mạch*.

Để tránh sự sụp đổ do nghẽn mạch, TCP phải giảm mật độ truyền khi xảy ra nghẽn mạch. Các bộ định tuyến theo dõi độ dài hàng đợi và sử dụng những kỷ thuật

giống như làm nguội nguồn ICMP để thông báo với các máy tính rằng đã xảy ra sự nghẽn mạch. Đồng thời TCP sử dụng kỹ thuật: *khởi đầu chậm và giảm theo cấp số nhân*. TCP duy trì một cửa sổ gọi là cửa sổ nghẽn mạch dùng để giới hạn lượng dữ liệu ở mức ít hơn kích thước vùng đệm của nơi nhận khi xảy ra sự nghẽn mạch. Kích thước cửa sổ được tính như sau :

Kích_thước_được_phép = min (kích thước_thông báo,

kích_thước_cửa_sổ_nghẽn_mạch).

Khi bị mất một Segment, giảm kích thước cửa sổ nghẽn mạch đi một nữa (cho tới khi chỉ còn kích thước của một Segment). Với những Segment vẫn còn nằm trong cửa sổ được phép, nhượng bộ bằng cách gia tăng bộ đếm thời gian truyền lại theo hàm mũ.

Để phục hồi lại việc truyền khi không còn nghẽn mạch TCP sử dụng một kỷ thuật được gọi là *khởi động chậm* nhằm mục đích gia tăng từ từ việc truyền dữ liệu.

5.7 Sự nghẽn mạch cắt bớt phần đuôi.

Như đã trình bày khi hệ thống xảy ra sự nghẽn mạch, bộ định tuyến sẽ lưu trữ các Datagram gửi đến trong một hàng đợi của bộ nhớ cho đến khi nó có thể được xử lý. Khi các Datagram gửi đến nhanh hơn là chúng được chuyển đi thì hàng đợi sẽ dài ra, khi các Datagram chuyển đến chậm hơn thì hàng đợi thu ngắn lại. Nhưng vì bộ nhớ là hửu hạn, hàng đợi không thể dài ra quá hạn. Vì vậy để quản lý hàng đợi bị tràn phần mềm của bộ định tuyến sử dụng chính sách *" cắt bớt phần đuôi"* .

Việc *"cắt bớt phần đuôi"* có ảnh hưởng đáng kể với TCP, trong trường hợp đơn giản khi các Datagram di chuyển qua bộ định tuyến mạng theo các Segment của chỉ một kết nối TCP, việc mất này sẽ làm cho TCP đi vào trạng thái khởi động chậm, nghĩa là giảm bớt tốc độ truyền cho tới khi TCP bắt đầu nhận các lời đáp và gia tăng kích thước cửa sổ nghẽn mạch. Ngoài ra việc *"cắt bớt phần đuôi"* có thể ảnh hưởng đến toàn bộ Internet, khi các Datagram di chuyển qua bộ định tuyến mạng theo các Segment của nhiều kết nối TCP.

5.8 Hủy bỏ sớm ngẩu nhiên RED (Random Early Discard).

Việc *"cắt bớt phần đuôi"* có thể ảnh hưởng đến toàn bộ Internet, điều này đòi hỏi phải có một mô hình khác để thay thế. Mô hình này có tên *hủy bỏ sớm ngẩu nhiên* (Random Early Discar), thường được gọi tắt là RED. Bộ định tuyến cài đặt RED sử dụng hai giá trị là chặn trên và chặn dưới để đánh dấu các vị trí trong hàng đợi : Tmin và Tmax. Hoạt động của RED được mô tả bởi ba quy tắc để xác định vị trí của mỗi Datagram gửi đến :

- Nếu hiện tại, hàng đợi chứa ít hơn Tmin Datagram, thêm Datagram mới vào hàng đợi

- Nếu hàng đợi chứa nhiều hơn Tmax Datagram, hủy bỏ những Datagram mới

- Nếu hàng đợi chứa trong khoảng Tmin và Tmax Datagram, hủy bỏ Datagram một cách ngẫu nhiên tùy theo một hàm xác suất P.

Tính ngẫu nhiên của RED có nghĩa là thay vì đợi đến khi hàng đợi bị đầy và buộc nhiều kết nối TCP phải chuyển qua trạng thái khởi động chậm, bộ định tuyến huỷ bỏ các Datagram một cách ngẫu nhiên và từ từ theo sự gia tăng của sự nghẽn mạch.

Để cho RED hoạt động tốt thì phải chọn các giá trị Tmin, Tmax và hàm xác suất P như thế nào cho phù hợp. Tmin phải đủ lớn để đảm bảo rằng đường liên kết để dữ liệu đi được sử dụng với hiệu suất cao. Tmax phải lớn hơn Tmin, ít nhất là phải gấp đôi. Nếu không thì RED cũng gây ra những ảnh hưởng như *"cắt bớt phần đuôi"*.

Việc tính hàm xác suất là một trong những giai đoạn phức tạp của RED. Giá trị này phụ thuộc vào kích thước hiện tại và các giá trị chặn trên và chặn dưới. Khi kích thước hàng đợi nhỏ hơn Tmin, RED không hủy bỏ bất kỳ một Datagram nào, thì cho xác suất hủy bỏ là 0. Khi kích thước hàng đợi lớn hơn Tmax, RED hủy bỏ tất cả các Datagram đến sau, thì cho xác suất hủy bỏ là 1. Đối với những giá trị trung gian khác của kích thước hàng đợi, xác suất P có thể thay đổi từ 0 đến 1 một cách tuyến tính.

5.9 Đóng lại một kết nối.

Hai chương trình ứng dụng (nơi gửi và nơi nhận) sử dụng TCP để thông tin liên lạc có thể kết thúc trao đổi dữ liệu bằng cách đóng lại kết nối. Các bước đóng lai kết nối diễn ra như như sau:

- Máy chủ kết thúc công việc và báo cho TCP biết là nó muốn kết thúc kết nối.

- TCP máy chủ sẽ gửi thông báo FIN (kết thúc) để báo cho đầu bên kia biết rằng nó sẽ không truyền dữ liệu nữa.

- TCP trạm làm việc xác nhận đã nhận được thông báo FIN.

- TCP trạm thông báo cho ứng dụng của nó biết rằng nó sẽ kết thúc kết nối.

- Trạm làm việc báo cho TCP để kết thúc kết nối.

- TCP trạm gửi thông báo FIN.

- TCP máy chủ nhận được thông báo FIN của TCP trạm và đáp lại bằng thông báo ACK.

- TCP báo cho ứng dụng của nó biết là kết nối đã được đóng.

6. Tầng giao vận của OSI và TCP

Tầng *TCP* cung cấp một dịch vụ kết nối dữ liệu không bị lỗi, đầy đủ, tuần tự một cách đáng tin cậy đến các ứng dụng. Chúng gửi những đoạn (Segment) đến tầng IP. Sau đó tầng IP chọn đường cho chúng đến đích. Giao thức điều khiển truyền phát chấp nhận những đoạn đi đến nó từ tầng IP, nếu quy định ứng dụng là nơi nhận, và gửi dữ liệu đến ứng dụng đúng thứ tự mà nó được gửi.

Tầng giao vận trong mô hình OSI có kiểu kết nối định hướng đảm bảo truyền dữ liệu tin cậy, nhưng không giao tiếp trực tiếp với những ứng dụng.

Tầng phiên (Session) thiết lập và kết thúc sự truyền thông ứng dụng - ứng dụng. Một cặp ứng dụng sử dụng những phương tiện tầng phiên để thực hiện sự đàm thoại của chúng. Chẳng hạn, chúng quyết định thiết lập, duy trì, thiết lập đồng bộ hóa và hủy bỏ các phiên truyền thông.

Một header datagram IP chứa từ 20 đến 60 bytes. Tỷ lệ của 1 datagram phụ thuộc vào thông tin của header tác động lên lưu lượng, kích thước vùng dữ liệu cực đại có thể thay đổi từng loại mạng nhưng khi truyền dữ liệu đến một máy chủ ở xa ngang qua nhiều kiểu mạng chưa từng biết thì cách tốt nhất là nên sử dụng một kích thước để đảm bảo cho việc truyền ổn định.

Một vấn đề gây rắc rối là việc sử dụng khuôn dạng của giao thức không có tiêu chuẩn bởi vài phiên bản lỗi thời của TCP/IP. Hiện nay để tương thích người ta dùng phần mềm phân tán với những khuôn dạng khung tiêu chuẩn cho những khung MAC Ethernet, di chuyển vùng kiểu khung và header tầng 3, 4 và một đầu cuối (trailer)

- Vài giao thức liên kết dữ liệu và môi trường vật lý được sử dụng cho TCP/IP và là như nhau. *Chẳng hạn*, OSI và TCP/IP đều hoạt động trên những chuẩn X.25, 802.5, 802.4, 802.3, 802.2. Tất nhiên, những vùng (như là LLC và những header SNAP) nhận giao thức mức cao hơn của 1 bản tin sẽ phân biệt sự lưu thông giữa TCP và ISO. *Sự hội tụ giữa TCP/IP và OSI* tại mức này tạo cho chúng có khả năng dùng chung những phương tiện vật lý.

V. GIAO THỨC DỮ LIỆU NGƯỜI DÙNG UDP (USER DATAGRAM PROTOCOL).

Giao thức UDP là giao thức "không kết nối" được sử dụng thay thế cho giao thức điều khiển truyền phát ở trên theo yêu cầu của ứng dụng.

Cấu trúc đơn vị dữ liệu của UDP là đơn giản, nhanh

0	15	16	31	
Source Port		Destination Port		UDP
Length		Check sum		header
Data				

Khác với giao thức điều khiển truyền phát TCP, giao thức UDP không có chức năng thiết lập và giải phóng liên kết, tương tự như giao thức liên mạng IP. Nó cũng không cung

cấp cơ chế báo nhận (Acknowlement) không sắp xếp tuần tự các đơn vị dữ liệu Datagram đến và có thể dẫn đến tình trạng mất hoặc trùng dữ liệu mà không hề có thông báo lỗi cho bên gửi. UDP là thủ tục không tin cậy, dùng cho dịch vụ không tin cậy 100%. Thực tế khi qua các mạng, 90% bản tin UDP được giao nhận. Giao thức UDP thường được dùng cho các ứng dụng không đòi hỏi độ tin cậy cao trong tầng vận chuyển.

Một ứng dụng muốn gửi dữ liệu nhờ giao thức UDP. Dữ liệu tại tầng ứng dụng phải đưa các khối rồi chuyển xuống tầng giao thức UDP. Sau đó nó thêm vào mỗi khối dữ liệu một phần đầu Header, dạng User Datagram. User Datagram sau đó được đưa đến tầng IP Datagram.

VI. CẤU TRÚC TÊN VÀ ĐỊA CHỈ CỦA INTERNET

Internet là mạng máy tính toàn cầu, Internet có hàng chục triệu máy tính tham gia, do đó việc đánh địa chỉ cho các máy tính làm sao cho có logic và thuận tiện cho quá trình trao đổi thông tin là một vấn đề không đơn giản. Internet có quy ước trong vấn đề này, đó là Domain Name System. Domain Name System định nghĩa tên theo cấu trúc sau :

Host.[subdomain].[subdomain].[...].<domain>

Cấu trúc trên được xem từ bên trái qua bên phải theo chiều rộng dần. Tên bao gồm các thành phần và nhãn được phân biệt bởi dấu '.'

Đây là một địa chỉ của máy. trên một máy có thể có nhiều người sử dụng có tên đăng ký riêng của mình.

Account.@Host.[subdomain].[subdomain].[...].<domain>

Account :

Tên này không được vượt quá 63 ký tự, được bắt đầu bởi chữ cái, kết thúc bởi chữ cái hoặc số, có thể có chữ số hoặc có dấu gạch ngang nhưng không có dấu cách.

Domain :

Phần này chỉ ra các nước nếu Domain này là khu vực hoặc chỉ ra các tổ chức quốc tế, hoặc một lĩnh vực kinh tế, xã hội, quốc phòng.

Subdomain :

Để thuận lợi trong việc tìm kiếm, từ khái niệm Domain hệ thống Domain Name System phân chia ra các Domain con (Subdomain) bao gồm các nhóm người sử dụng.

Như chúng ta đã thấy Domain Name System cung cấp cho chúng ta hệ thống đánh tên hết sức logic và dễ hiểu. Nhưng bản chất và giá trị thực sự của chúng thì lại ẩn dưới hệ thống tên Domain Name System - người ta gọi chúng là địa chỉ IP (Internet Protocol Address) (đã khảo sát ở chương 3). Trên thực tế người ta hiếm khi sử dụng địa chỉ thực này vì chúng khó nhớ, nhưng chính nhờ chúng mà chúng ta có thể truy cập đến một máy khác. Khi sử dụng tên có dạng Domain Name System thì máy chủ sẽ tự động chuyển đổi sang dạng địa chỉ IP trước khi quá trình truyền được thực hiện.

Việc cung cấp địa chỉ mạng được thực hiện bởi một ủy ban có tên là NIC (Network Information Center). Ví dụ về một cách viết địa chỉ : 137.92.11.125 (Trường University of Canberra được cấp một địa chỉ thuộc lớp địa chỉ B).

Cách quản lý của Domain Name System :

Như đã nói trên Domain Name System là một hệ thống quản lý chuyển tên thành đối tượng được duy trì bởi nhiều tổ chức. Mỗi tổ chức nắm một phần.

Ví dụ :

COM	Commercial Organizations
EDU	Education Organizations
GOV	Government Institutions
MIC	Military Groups
NET	(Network Support Center)
ORG	Other Organizations
US	(Tên nước)
VN	(Tên nước)
.....	.....

Domain Name System có cấu trúc cây :

Về mặt cơ chế mỗi mạng địa phương sẽ có một Domain Name Server, nó có một cơ sở dữ liệu chưa danh mục thông tin của địa phương. Tên và địa chỉ IP sẽ được cập nhật vào CSDL này. Để tiến hành giao dịch mỗi một user phải biết địa chỉ IP của Domain Name Server địa phương và gởi một gói tin cần cung cấp thông tin của đối tượng có tên X nào đó. Việc này được thực hiện tự động. Sau khi nhận được nhu cầu tại user (client) chương trình Domain Name Server sẽ tìm kiếm và cho lại đối tượng theo yêu cầu.

VII. ĐỊNH TUYẾN VÀ CHỌN ĐƯỜNG TRÊN INTERNET

1. Một số khái niệm chung và nguyên tắc hoạt động của việc định tuyến và chọn đường

Trong vấn đề định tuyến, người ta phân biệt hai loại, đó là trực tiếp và không trực tiếp.

Việc truyền tin giữa hai máy được gọi là trực tiếp nếu hai máy này được nối vào cùng một mạng vật lý. Còn nối trực tiếp xảy ra khi cả máy nguồn và máy đích không cùng nối vào một mạng vật lý, vì vậy việc truyền tin giữa chúng phải được thực hiện thông qua các trạm trung gian là các gateway.

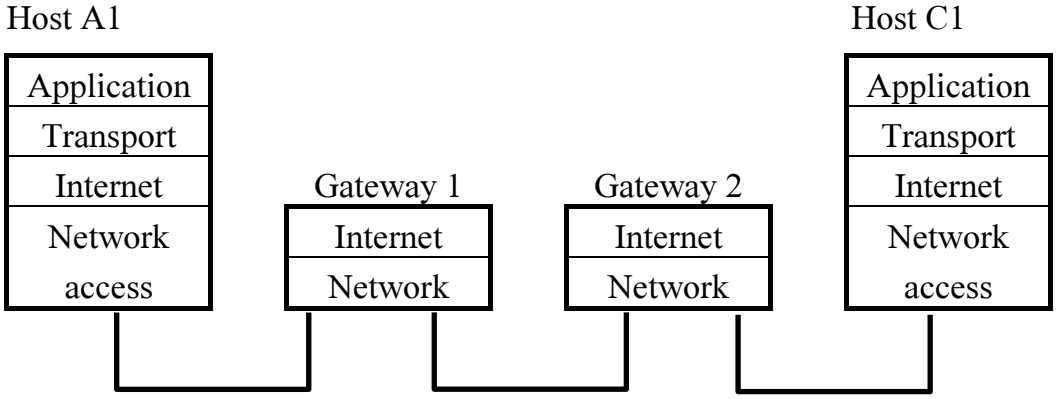
Để kiểm tra xem máy đích có nằm trên cùng mạng vật lý với máy nguồn hay không thì người gửi phải tách lấy phần địa chỉ mạng của máy đích ở trong phần địa chỉ máy đích của datagram, và so sánh với phần địa chỉ mạng trong phần địa chỉ IP của nó. Nếu hai địa chỉ này là giống nhau thì datagram sẽ được truyền đi trực tiếp, còn nếu hai địa chỉ này khác nhau thì người gửi phải xác định được một gateway để thông qua

gateway này các datagram được truyền đi. Gateway này sau đó sẽ hướng về mạng đích của nó.

Ví dụ như khi có một mạng Internet lớn với nhiều mạng cục bộ nối với nhau bởi các gateway, nhưng chỉ có hai trạm ở cách xa về hai phía. Khi một trạm muốn gởi các gói dữ liệu (datagram) đến một trạm khác thì nó phải đóng gói datagram vào một khung (frame) và gởi nó 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 dọc theo đường dẫn đến đích. Datagram sau đó lại được đóng gói vào một frame khác và được gởi đến mạng vật lý để gởi đến gateway tiếp theo trên đường truyền, và cứ tiếp tục như thế cho đến khi datagram được truyền đến đích.

Việc định tuyến đường để gửi các gói dữ liệu:

Hình vẽ sau mô phỏng cho ta thấy việc dùng các gateway để gửi các gói dữ liệu:



Trong thuật ngữ truyền thống của TCP/IP chỉ có hai kiểu thiết bị, đó là các cổng truyền (gateways) và các trạm (hosts). Các cổng truyền có vai trò gởi 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 hòan tòan như một gateway.

Các trạm lưu chuyển các gói dữ liệu xuyên suốt qua cả bốn lớp, trong khi đó chuyển các gói lên đến lớp Internret, là nơi quyết định tuyến đường tiếp theo để gởi các gói dữ liệu đi.

Các máy chỉ có thể truyền dữ liệu đến các máy khác nằm trên cùng một mạng vật lý. Các gói từ A1 được dành riêng cho C1 sẽ được hướng đến gateway G1 và G2, trạm A1 đầu riên sẽ truyền các gói đến gateway G1 thông qua mạng A, sau đó G1 truyền tiếp đến G2 thông qua mạng B, cuối cùng G2 sẽ truyền các gói đến 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. Nó gởi các gói được dành 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 gởi các gói của mình đến cho G2, và G2 sẽ gởi đi tiếp cho các trạm ở trên mạng A cũng như ở trên mạng B.

2. Bảng định tuyến (Routing Table)

Routing table là nơi lưu giữ thông tin về các đích có thể với tới được và cách thức để với tới địa chỉ đó. Khi phần mềm IP routing tại một trạm hay một cổng truyền nhận được yêu cầu truyền một gói dữ liệu đi thì trước hết nó phải tham khảo bảng định tuyến của nó để quyết định xem nó phải gửi datagram đến đâu. Tuy nhiên không phải bảng thông tin chọn đường của mỗi trạm (hay cổng) là chứa tất cả các thông tin về các tuyến đường có thể với tới được.

Một bảng thông tin chọn đường bao gồm các cặp (N,G), trong đó N là địa chỉ IP của mạng đích, còn G là địa chỉ của cổng tiếp theo dọc theo đường truyền đến mạng N.

Như vậy, mỗi cổng truyền sẽ không biết được đường truyền đầy đủ để đi đến đích. Trong bảng thông tin chọn đường còn có những thông tin về các cổng có thể với đến nhưng không nằm trên cùng một mạng vật lý, phần thông tin này được che khuất đi và được gọi là Default. Khi không tìm thấy các thông tin của địa chỉ đích cần tìm thì các gói dữ liệu sẽ được gởi đến cổng truyền ngầm định.

Để hiển thị nội dung của bảng thông tin chọn đường, ta dùng lệnh netstat với tùy chọn -rn. Tùy chọn -r sẽ hiện nội dung của bảng thông tin chọn đường, còn tùy cọn -n sẽ hiện nội dung của bảng thông tin chọn đường, còn tùy chọn -n sẽ hiện nội dung này dưới dạng số.

Ví dụ như khi dùng lệnh netstat ở trên một máy UNIX, ta nhận được bảng nội dung sau:

# netstat Routing Tabele:					
Destination	Gateway	Flags	Refcnt	Use	Interface
127.0.0.1	127.0.0.1	UH	0	12	Io0
203.160.0.0	203.160.0.10	U	3	140	Ie0

Trong đó:

- Trường Destination chỉ địa chỉ đích của mạng hay của trạm

- Trường Gateway chỉ cổng dùng để với tới đích đã được chỉ định.

- Trường Flags mô tả những đặc trưng của tuyến đường này như:

U - chỉ ra rằng tuyến đường này là hoạt động.

H - chỉ ra rằng đây là một tuyến đường với tới một trạm đặc biệt

G - chỉ ra rằng tuyến đường này dùng gateway.

- Trường Refcnt chỉ số lần mà một tuyến đường được đề cập đến để thực hiện việc kết nối. Trường Use chỉ ra các số gói (packet) đã được chuyển qua tuyến đường này.

- Trường Interface chỉ ra tên của giao diện mạng được dùng của tuyến đường này.

3. Thuật toán chọn đường trên IP

- Tách phần địa chỉ mạng đích, In.

- Nếu In tương ứng với bất kỳ địa chỉ mạng được kết nối nào thì gởi gói dữ liệu đến địa chỉ đích ở trên mạng đó. (Phần này bao gồm cả việc phân tích Io để có được phần địa chỉ vật lý tương ứng, đóng gói các gói dữ liệu trong các khung (frame) và gởi các khung này đi).

- Nếu không thì kiểm tra xem nếu Io là một tuyến đường đến trạm cụ thể thì gởi các gói dữ liệu đến địa chỉ đã được chỉ ra ở trong bảng thông tin chọn đường.

- Nếu không thì kiểm tra xem In có ở trong bảng thông tin chọn đường hay không. Nếu In có ở trong bảng thông tin chọn đường thì các gói dữ liệu sẽ được gởi đi theo địa chỉ được chỉ ở trong bảng thông tin chọn đường.

- Nếu tuyến đường Default được chỉ định thì các gói dữ liệu được gởi đến cổng ngầm định.

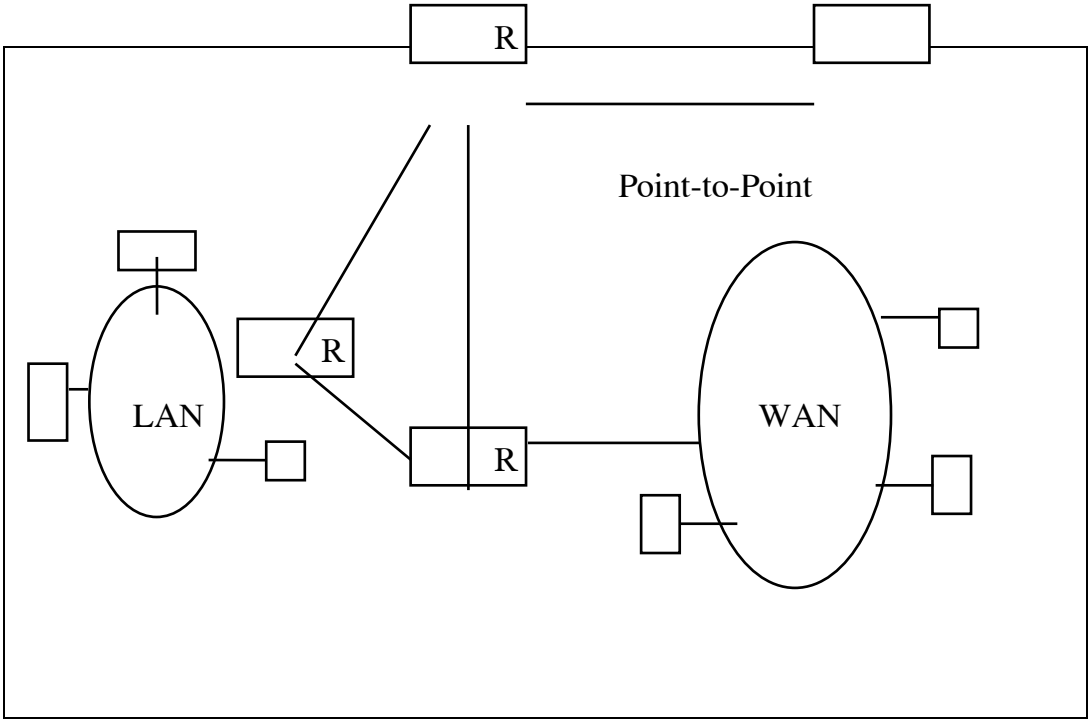
- Nếu không sẽ có thông báo lỗi về tuyến đường.

Tóm lại TCP/IP là một giao thức mở chuẩn có khả năng tương thích với nhiều mạng vật lý, các tính năng của TCP/IP đã được hòan thiện dần và trở nên một bộ giao thức được dùng rộng rãi như một ngôn ngữ chung để kết nối các máy tính trên khắp thế giới với nhau.

4. Vấn đề liên mạng trên Internet

4.1 Khái niệm

Bộ giao thức TCP/IP có thể được dùng trên những mạng LAN, WAN độc lập hoặc trên những liên mạng phức tạp. Vài máy chủ được trang bị TCP/IP có thể truyền với một máy chủ khác ngang qua một liên kết điểm-điểm. Những mạng này được giao nhập vào một liên mạng nhờ bộ định tuyến IP.



Hình 7.6: Một liên mạng được tạo ra nhờ các bộ định tuyến

Trên lý thuyết, những liên mạng có thể có những Topo khác nhau. Tuy nhiên, khi một liên mạng có một cấu trúc rõ ràng, thì nó dễ dàng làm cho những bộ định tuyến thực hiện những công việc của chúng có hiệu quả và phản ứng nhanh đến mọi sự cố trong vài khu vữ của mạng, thay đổi những đường dẫn để những Datagram tránh được sự trục trặc.

Phần mềm giao thức liên mạng hoạt động trong những máy chủ và những bộ định tuyến IP. Thông thường một phần mềm giao thức liên mạng IP của máy tính sẽ cho phép nó thao tác như là một máy chủ giao thức liên mạng IP, hay một bộ định tuyến IP, hoặc cả hai, hầu hết các tổ chức thích dùng thiết bị Router được chuẩn hóa hơn để gia nhập vào những mạng. Tuy nhiên nó là thuận lợi để có khả năng đưa một máy tính chưa được sử dụng vào dịch vụ bởi một Router.

4.2 Hoạt động của giao thức liên mạng IP

Nếu đích của Datagram không nằm trên cùng một mạng với máy chủ nguồn, giao thức IP trong máy chủ (host) hướng Datagram đến một bộ định tuyến nội bộ. Nếu bộ định tuyến này không được nối đến mạng đích, Datagaram phải được gửi đến một bộ định tuyến khác. Cứ như thế cho đến khi đến được trạm đích.

Giao thức IP thực hiện một quyết định chọn đường bằng cách tìm một trạm đích ở xa trong một bảng chọn đường tương ứng với trạm đích với mã định danh của Router kế tiếp để lưu thông Datagaram.

Việc quy định truyền theo đường truyền nào của Router dựa trên bảng đường truyền Routing Table.

- Những bộ định tuyến có thể phát hiện những sự kiện như là:

- Một mạng mới đã được thêm vào liên mạng.

- Đường dẫn tới trạm đích đã bị hư.

Một bộ định tuyến mới đã được thêm vào. Bộ định tuyến này cung cấp một đường dânự tới những đích ngắn hơn.

Sự trao đổi thông tin giữa hai bộ định tuyến Router - Router được điều khiển của một tổ chức được gọi là hệ thống tự quản (Autonomous System). Tổ chức này có thể chọn vài giao thức để trao đổi thông tin giữa các router.

Tóm lại: Các bước thực hiện bởi một thực thể IP như sau.

Đối với thực thể IP ở trạm nguồn, khi nhận được một primitive SEND từ tầng trên, nó thực hiện các bước sau :

- Tạo một IP datagram dựa trên các tham số của primitive SEND.

- Tính checksum và ghép vào phần đầu của datagram.

- Ra quyết định dọn đường hoặc là trạm đích trên cùng một mạng, hoặc là một gateway sẽ được chọn cho chặng tiếp.

- Chuyển datagram xuống tầng dưới.

Đối với gateway khi nhận được datagram quá cảnh, nó thực hiện các tác động sau:

- Tính checksum nếu không đúng thì loại bỏ datagram.

- Giảm giá trị của tham số thời gian tồn tại. Nếu thời gian đã hết thì loại bỏ datagram.

- Ra quyết định chọn đường.

- Phân đoạn datagram nếu cần.

- Kiến tạo lại phần đầu IP bao gồm giá trị mới của vùng :

Time to live, Fragrmentation, Checksum

- Chuyển datagram xuống tầng dưới để truyền qua mạng.

Cuối cùng, khi một datagram được nhận bởi một thực thể IP ở trạm đích, nó sẽ thực hiện các công việc sau :

- 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.

Tóm lại: Các datagram IP được chuyển giao theo cách hiệu quả nhất, nghĩa là không cần khả năng hiệu chỉnh lỗi và không cần thông tin về phát thành công. Chỉ trong trường hợp địa chỉ đích không rõ ràng thì sử dụng ICMP (Internet control message Protocol) để lưu ý cho người gửi các bản tin ICMP được đóng gói và chuyển tải trong các gói IP.

4.3 Thông tin bảng chọn đường

Trong một liên mạng nhỏ và tĩnh, những bảng chọn đường có thể được vào và lưu giữ nhân công. Trong một liên mạng lớn, những bộ định tuyến giữ những bảng của nó với những thông tin mới nhất bởi sự trao đổi thông tin với một bộ định tuyến khác. Những bộ địnnh tuyến có thể phát hiện những sự kiện như là:

Một mạng mới đã được thêm vào liên mạng.

Đường dẫn tới trạm đích đã bị hư.

Một bộ định tuyến mới đã được thêm vào. Bộ định tuyến này cung cấp một đường dẫ tới những đích ngắn hơn.

Không có một chuẩn đơn giản nào được chọn cho sự trao đổi thông tin giữa hai bộ định tuyến (Router - Router). Những bộ định tuyến dưới sự điều khiển của một tổ chức được gọi là hệ thống tự quản (Autonomous System). Tổ chức này có thể chọn vài giao thức để trao đổi thông tin giữa các router. Một giao thức chuyển đổi thông tin cho bộ định tuyến được dùng trong một hệ thống tụ quản được gọi là IGP (Interior Gateway).

Giao thức thông tin chọn đường (Routing Information Protocol) là một IGP biến. Tuy nhiên, giao thức OSPE (Open Shortest Path First) mới hơn các đặc điểm tiện ích, phong phú. Sự giá trị và phổ biến của OSPE đang phát triển đều.

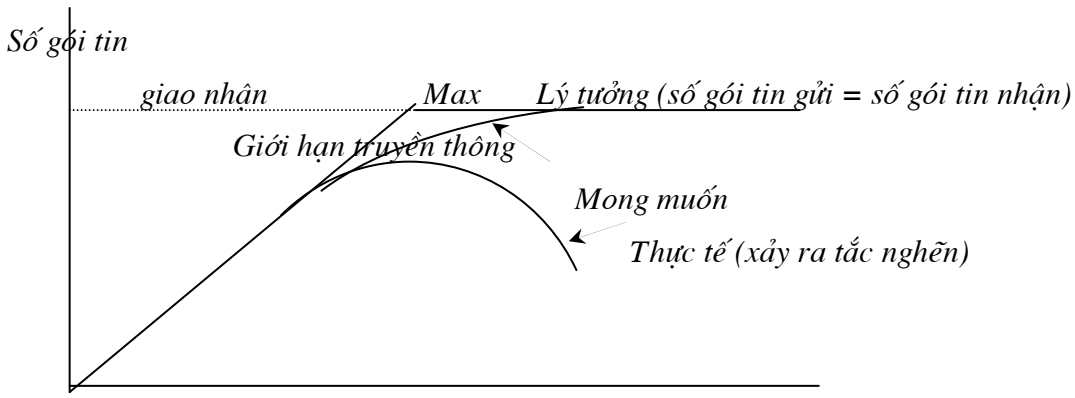
Vài nhà cung cấp bộ định tuyến cung cấp giao thức để trao đổi thông tin giữa những bộ định tuyến (Router-to-Router) cho riêng họ cũng như phụ trợ cho những giao thức chuẩn. Một số những nhà cung cấp có khả năng hoạt động vài giao thức cùng một lúc, những bộ định tuyến của họ có thể trao đổi thông tin với những bộ định tuyến khác sử dụng vài giao thức này.

5. Sự tắc nghẽn trên 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, gữi đi và chúng bắt đầu bị mất các gói tin. Hiện tượng này gọi là sự tắc nghẽn trong mạng.

- Khi số gói tin đưa vào mạng ít hơn khả năng vận chuyển thì số gói tin đưa vào sẽ bằng số gói tin được gửi đi.

- Nếu số gói tin dựa vào mạng càng nhiều hơn khả năng vận chuyển của nút mạng thì gói tin chuyển đi càng chậm và cuối cùng dẫn đến tắc nghẽn.



Số gói tin gửi đi

Khi máy chủ truyền các gói tin vào mạng con. Trong vòng lượng thông tin có thể truyền tốt thì các gói tin này sẽ được truyền đi, ngoại trừ vài gói tin bị hỏng do lỗi truyền và số gói tin được truyền đi tương ứng với số gói tin chuyển đến. Tuy nhiên khi số lượng gói tin tăng lên, những router không còn khả năng điều chỉnh đánh mất chúng. Điều này có khuynh hướng làm cho vấn đề trầm trọng hơn khi lượng lưu thông quá cao, sự truyền bị phá bỏ hoàn toàn và hầu như không có gói tin nào được truyền đi.

Sự tắc nghẽn có thể xảy ra do vài yếu tố sau :

1. Nếu luồng các gói tin đột ngột bắt đầu đến từ 3 hay 4 đường vào và tất cả đều cần ra cùng một đường, một hàng đợi sẽ được thiết lập. Hàng đợi sẽ bị đầy (phải lưu tệp, phải tạo các bảng ...), nếu khả năng xử lí của nút yếu, hay nói cách khác các CPU tại các router xử lý chậm các yêu cầu sẽ dẫn đến tắc nghẽn.

   Nếu bộ nhớ không đủ để lưu chúng lại thì một số gói tin sẽ mất. Việc thêm vào nhiều bộ nhớ hơn sẽ có ích, nhưng theo Nagle (1987) cho rằng nếu các router có lượng nhớ không xác định thì sự tắc nghẽn chẳng tốt hơn tí nào, mà trở nên xấu đi bởi vì số bản sao được gửi đi tăng, sẽ đến đường tiếp theo làm tăng lượng thông tin ở nơi nhận tin.

2. Sự tắc nghẽn có khuynh hướng tác động lại chính nó và trở nên tồi hơn, nếu một router không có bộ đệm tự do, nó sẽ bỏ qua những gói tin mới đến. Khi một gói tin bị loại bỏ, router gửi gói tin đó tiếp tục chuyển lại gói tin. Vì máy chuyển tiếp theo không thể loại bỏ gói tin cho đến khi gói tin được thu nhận, sự tắc nghẽn ở đầu nhận sẽ buộc đầu gửi tự dừng lại để giải phóng bộ nhớ đệm tự do.

Cần phải phân biệt 2 khái niệm điều khiển sự tắc nghẽn và điều khiển lưu thông vì mối quan hệ giữa chúng khó tìm ra.

- Điều khiển tắc nghẽn phải được thực hiện thông qua việc chắc chắn mạng con có khả năng xử lý thông tin đưa vào. Đó là vấn đề liên quan đến việc xử lý của máy chủ, tất cả các router quá trình lưu giữ, chuyển tin của router và tất cả các yếu tố khác mà có khả năng làm giảm khả năng thực hiện của mạng con.

  Như vây, điều khiển tránh tắc nghẽn là một vấn đề tổng quát 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.

- Điều khiển lưu thông liên quan đến vấn đề lưu thông, nơi này đến nơi khác, giữa nơi chuyển tin và nơi nhận tin. Nhiêm vụ của nó là chắc chắn rằng nơi gửi dù nhanh thì không thể chuyển dữ liệu nhanh hơn việc tiếp nhận của nơi nhận tin. Điều khiển lưu thông liên quan đến sự đáp ứng trực tiếp của nơi nhận tin đến nơi gửi tin để thông báo công việc tiến hành như thế nào ở đầu kia. Như vậy điều khiển lưu thông là xử lý lưu thông giữa điểm với điểm, giữa trạm phát với trạm thu...

Để xem xét sự khác nhau giữa 2 khái niệm này, ta xét mạng cáp quang với công suất 1000 gigabit/s ở đó siêu máy tính đang cố gắng chuyển một tệp đến 1

máy tính cá nhân 1 Gbps. Mặc dù không có sự tắc nghẽn (mạng tự nó không gặp trở ngại) sự điều khiển lưu thông là cần thiết để buộc siêu máy tính dừng lại để máy tính cá nhân có thời gian để nhận. ở đầu kia (máy nhận), xem xét mạng lưu giữ và chuyển tin với đường dẫn 1 Mbps và 1000 máy tính, một nữa trong số chúng đang cố gắng chuyển các tệp ở 100 Kbps đến nữa kia. Vấn đề ở đây không phải là nơi gửi nhanh lấn lướt, nơi nhận tin xử lý chậm, mà đơn giản là tổng lượng thông tin cung cấp vượt qua những gì mạng có thể quản lý.

Lý do điều khiển tắc nghẽn và điều khiển lưu thông không rõ ràng dễ lẫn lộn vì một vài nguyên tắc điều khiển sự tắc nghẽn được thực hiện bằng việc gửi thông điệp đến lại nguồn khác để báo chúng làm chậm tiến trình khi mạng có sự cố, như vậy một máy chủ có thể nhận thông điệp làm chậm bởi vì nơi nhận tin không thể quản lý tải hoặc vì mạng không thể quản lý nó.

Như vậy nguyên nhân chủ yếu xảy ra tắc nghẽn :

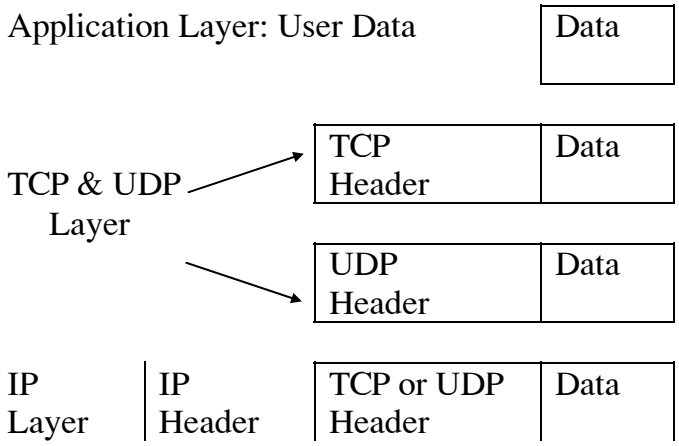
- Hàng đợi sẽ bị đầy (phải lưu tệp, phải tạo bảng ...), nếu khả năng xử lý của nút yếu.

- Hàng đợi bị đầy khi thông tin vào nhiều hơn khả năng của đường ra, mặc dù tốc độ xử lí của nút nhanh.

VII. NHẬN XÉT NHỮNG ĐƠN VỊ DỰ LIỆU GIAO THỨC

1. Đơn vị dữ liệu

Mô hình OSI sử dụng từ đơn vị dữ liệu giao thức tầng thứ N hoặc PDU tầng N chỉ cho đơn vị thông tin mà giao thức tầng thứ N giải quyết. Một đơn vị dữ liệu giao thức PDU gồm một phần đầu (Header) và một số dữ liệu được tùy chọn được đóng vào. Bộ giao thức TCP/IP sử dụng đơn vị dữ liệu segment cho giao thức TCP, User Datagram cho giao thức UDP và Datagram cho giao thức IP. Hình 3.9 chỉ rõ những phần đầu được thêm vào lần lượt tại mỗi lớp để định kiểu PDU của nó. Dữ liệu người sử dụng được gửi qua đến tầng TCP hoặc tầng giao thức UDP. Một phần Header của một Segment của tầng TCP chứa thông tin như là: Một số thứ tự sử dụng để giữ dữ liệu theo thứ tự, một ACK cho việc nhận dữ liệu, và thông tin nhận dạng những ứng dụng đang gửi và nhận trên kết nối. Một phần đầu của PDU của tầng UDP chứa những vùng nhận dạng những ứng dụng UDP đang nận và gửi. Một phần đầu của PDU của tầng giao thức IP chứa thông tin về địa chỉ mạng của nguồn và đích cho dữ liệu.



Lower Layers	Frame Header	IP Header	TCP or UDP Header	Data	Trailer

Hình 7.7: Những phần đầu (header) của PDU.

Một đơn vị dữ liệu giao thức tầng thấp thì được gọi là khung (frame). Phần đầu (Header) của một khung chứa những vùng xác định những thiết bị vật lý nguồn và đích. Trong vài trường hợp cá biệt, phần đầu sẽ được theo sau bởi một header thứ hai được gọi là header LLC (Logical Link Contol) hoặc header liên kết dữ liệu xem hình vẽ 3.10

Frame Header	Data Link Header	IP Header	TCP Header	Frame Check Sequence

Hình 7.8: Đầy đủ bộ Header của PDU

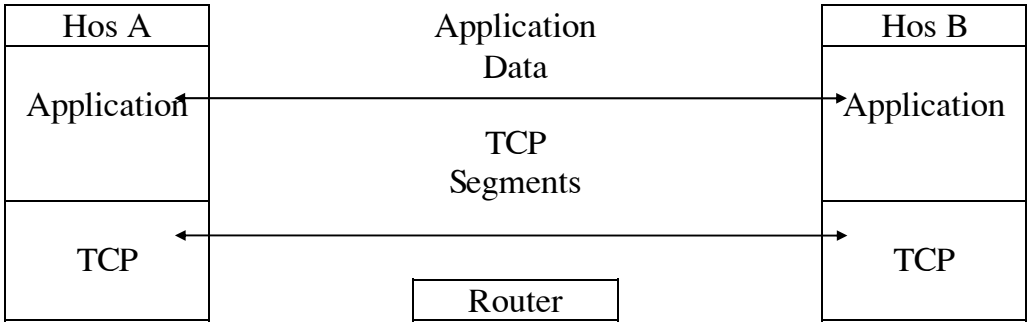
Hầu hết các khung chứa đựng một header và một Trailer. Trailer chứa moọt vùng FCS (Frame check sequence) sử dụng để phát hiện những lỗi truyền dẫn. Vùng FCS chứa đựng kết quả của một phép tóan mà người gửi thực hiện trên những bít của một thông báo, người nận sẽ thực hiện phép tính giống như vậy và so sánh kết quả với giá trị ở trên Trailer. Kết quả của phép toán được tách ra nếu những giá trị phù hợp nhau thì chắc chắn dữ liệu đã được bảo quản tòan vẹn trong suốt quá trình truyền.

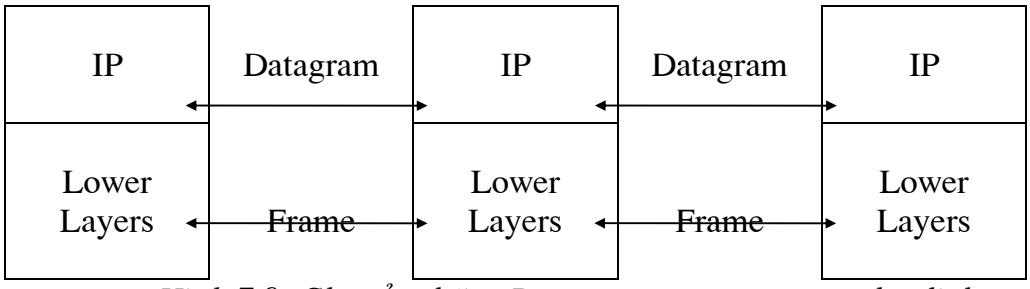
2. Nh÷ng t-¬ng t¸c ®ơng ®¼ng (Peer-to-Peer)

Những tầng thấp thì chịu trách nhiệm vận chuyển dữ liệu ngang qua một mạng cục bộ hay mạng diện rộng.

Những tầng giao thức IP trong những hệ thống mà có kết nối mạng diện rộng hoặc mạng cục bộ tuyệt đối chuyển những Datagram IP với nhau bằng cách đua chúng vào những khung. Những Datagram IP được trao đổi bởi những máy chủ được nối đến những mạng khác nhau được chuyển ngang qua một liên mạng là nhờ một hay nhiều những bộ định tuyến (Router).

Hình 3.10 minh họa sự tương tác những tầng đồng đẳng như thế nào, những ứng dụng trao đổi thông tin bằng cách sử dụng những phương tiện End-to-End được cung cấp bởi giao thức TCP. Một Segment của TCP được quấn vào bên trong của một Datagram IP và sau đó được chọn đường từ máy chủ nguồn của nó đến máy chủ đích. Những Datagram được đặt vào trong cái khung và đi ngang qua bộ đường truyền vật lý.





Hình 7.9: Chuyển những Datagram ngang qua một bộ định tuyến

VIII. CÁC ỨNG DỤNG TRÊN INTERNET

Dịch vụ trên TCP/IP rất đa dạng, phong phú và được ứng dụng sớm. Sớm nhất là Telnet, FTP , SMTP , DNS .... Với sự phát triển của công nghệ thông tin và nhu cầu xã hội, có nhiều sản phẩm của các nhà cung cấp dịch vụ khác nhau ra đời. Các dịch vụ này thường sử dụng giao thức Client/Server (chủ/khách) cụ thể là:

Client: Chịu trách nhiệm thu nhận yêu cầu của người sử dụng, biến đổi nó và gửi về Server dưới một dạng thích hợp. Nó cũng làm nhiệm vụ nhận kết quả từ Server gửi đến và hiển thị thông tin cho người sử dụng.

Server: nhận các yêu cầu từ Client, xử lý chung bằng nhiều cách như đọc tệp, tìm kiếm cơ sở dữ liệu . . . , rồi gửi trả lại kết quả cho Client.

Client và Server : có thể trên cùng một máy hoặc thường là trong hai máy tính khác nhau nằm trên mạng, có thể chạy trên các hệ điều hành khác nhau. Việc kết nối giữa Client và server thường tuân theo các giao thức nhất định. Và xử lý thông tin thực hiện chủ yếu trên Server, Client đóng vai trò giao tiếp với người sử dụng và thực hiện truyền thông với Server nếu cần.

1 Dịch vụ thư tín sử dụng SMTP.

Đây là một trong những ứng dụng được sử dụng rộng rãi nhất trên Internet. Nhiều giao thức cho dịch vụ thư tín có thể sử dụng được, nhưng giao thức được sử dụng rộng rãi nhất là SMTP (Simple Mail Transfer Protocol). SMTP cho phép gửi những thông điệp chuỗi ASCII đến hộp thư trên máy chủ được cấu hình với dịch vụ thư tín. Người sử dụng muốn gửi thông tin qua lại phải thông qua hệ thống USER AGENT. Thư tín được đặt trước trong hộp thư cục bộ hoặc hộp thư gửi đi. Quá trình của SMTP là nơi gửi sẽ duyệt hộp thư gửi đi và khi tìm thấy tín hiệu, trong hộp thư sẽ thiết lập một kết nối TCP với máy chủ đến địa chỉ của nơi nhận. Máy chủ đích sẽ nhận kết nối và thư tín hiệu sẽ gửi lên kết nối đó. Tiến trình SMTP nơi nhận đặt thư tín trong hộp đến trên máy chủ đích. Nếu không tìm thấy hộp thư trên máy chủ đích, một thông điệp dạng thư tín sẽ gửi trở lại nơi gửi và báo rằng hộp thư không tồn tại .Địa chỉ thư tín được sử dụng trong SMTP tuân theo chuẩn RFC 882.

Một địa chỉ của thư tín gồm 2 phần: phần trước dấu @ xác định tên hộp thư và sau @ xác định tên máy chủ..

Ví dụ: Hue!

Địa chỉ này sẽ gửi thư đến máy Hue, sau đó Hue gửi thư đến và ở đó thư sẽ được đưa đến người dùng B.

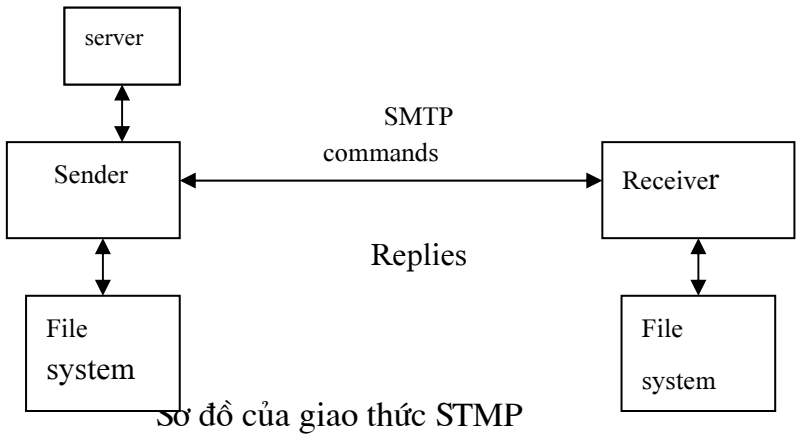
SMTP không thực tế nếu thiết lập một phiên làm việc với máy ngừng hoạt động sau mỗi ngày.Trong nhiều môi trường làm việc ,thư tín SMTP được nhận bằng một máy phục vụ SMTP luôn luôn hoạt động trên mạng. Khi gửi một thông điệp phi văn bản sử dụng SMTP thì có thể mã hóa thành một thông điệp văn bản bằng cách sử dụng tiện ích UUDECODE .

Ngoài ra, còn có thể sử dụng giao thức MIME (Multipurpose Internet Mail Extensions). Thông thường giao thức MIME được sử dụng nhiều hơn vì phần lớn các hệ thống thư tín xử lý việc mã hóa và giải mã MIME đính kèm một cách trong suốt. Nhưng bây giờ thường sử dụng giao thức POP3 (Post Office Protocol,phiên bản 3) để truyền thông tin và SMTP để nhận thông tin tiện lợi hơn vì lúc nào người sử dụng cũng có thể truy cập vào hộp thư của mình trên hệ thông máy chủ.

Hoạt động của giao thức SMTP

SMTP (Simple Mail Transfer Protocol) là một giao thức chuẩn được sử dụng để truyền thông điệp từ người gửi tới người nhận. SMTP cung cấp 4 cách thức truyền thông điệp như sau:

- Truyền thông điệp trực tiếp đến hộp thư của người nhận.
- Thể hiện thông điệp ngay trên thiết bị đầu cuối mà người nhận đang ở trên đó.
- Thể hiện thông điệp ngay trên thiết bị đầu cuối nếu như người nhận đang truy nhập vào mạng hoặc là lưu thông điệp vào hộp thư của họ nếu họ hiện đang không ở trên mạng.
- Phân thông điệp ngay vào hộp thư của người nhận, nếu họ đang truy nhập mạng thì hiển thị thông điệp cho họ xem.



Sơ đồ của giao thức STMP

Giao thức SMTP có cơ chế hoạt động rất đơn giản như sau:

- Đầu tiên máy phục vụ SMTP đợi các yêu cầu từ máy khách SMTP tại cổng 25.
- Khi có nhu cầu kết nối với máy phục vụ SMTP để truyền thông điệp, máy khách SMTP phải thiết lập một kết nối TCP tới máy phục vụ SMTP và đợi sự đồng ý của nó.
- Nếu như máy phục vụ SMTP chấp nhận thì máy khách SMTP sẽ khởi tạo một hay nhiều giao dịch SMTP.

- Khi một máy khách SMTP thiết lập một kết nối TCP tới máy phục vụ SMTP, máy phục vụ SMTP sẽ trả lại mã trạng thái MTA (Message Transfer Agent) cục bộ của SMTP sẽ trả lại một trong hai mã trạng thái sau:

220	MTA chấp nhận
421	MTA không chấp nhận

Mã trạng thái của MTA cục bộ

MTA có nhiệm vụ định tuyến thông điệp và xử lý các thông điệp đến từ hệ thống của người dùng sao cho các thông điệp đó đến được hệ thống đích.

Nếu như máy phục vụ SMTP trả lại mã trạng thái 220 thì có nghĩa là kết nối TCP từ máy khách SMTP tới nó đã được chấp nhận. Mọi giá trị mã trạng thái khác 220 đều có nghĩa là kết nối từ máy khách SMTP tới máy phục vụ không được thiết lập.

Sau khi kết nối đã được chấp nhận, máy khách SMTP giới thiệu chính nó sử dụng câu lệnh HELLO đi kèm với câu lệnh này là tên miền cuả máy có liên quan tới MTA cục bộ của máy khách SMTP.

Sau khi nhận được câu lệnh trên, máy phục vụ SMTP sẽ trả lời bằng một trong các mã trạng thái sau:

250	Chấp nhận máy khách SMTP
500	Sai về cú pháp câu lệnh
501	Sai về cú pháp của biến
504	Biến không thực hiện được
421	MTA không chấp nhận

Mã trả về bởi lệnh HELLO

Sau khi máy khách SMTP giới thiệu chính nó, nó có thể khởi tạo một hay nhiều giao dịch truyền thông điệp. Mỗi giao dịch truyền thông điệp sẽ bắt đầu khi máy khách SMTP đưa ra địa chỉ thư của người gửi thông điệp cùng với một trong bốn mode phần thông điệp đã đề cập.

Máy khách SMTP sẽ sử dụng một trong bốn câu lệnh sau:

MAIL FROM	SEND FROM
SAML FROM	SMOL FROM

Các câu lệnh khai báo người gửi

Người gửi có thể chọn một trong bốn mode thông điệp theo ý muốn của họ.

- MAIL FROM: thông điệp sẽ được phân ngay tới hộp thư của người nhận mà không cần kiểm tra xem người nhận có đang ở trên mạng hay không.
- SAML FROM: thông điệp sẽ được phân ngay tới hộp thư và thiết bị đầu cuối của người nhận. Có nghĩa là nếu người nhận đang ở trên mạng thì thông điệp sẽ được hiển thị ngay trên thiết bị đầu cuối và hộp thư của người nhận, trường hợp ngược lại chỉ phân vào hộp thư.

- SEND FROM: thông điệp được phân ngay tới thiết bị đầu cuối của mạng (không phân vào hộp thư). Nếu người nhận không ở trên mạng thì thông báo sẽ được tự động hiện lên sau.
- SMOL FROM: thông điệp được phân tới thiết bị đầu cuối hoặc hộp thư của người nhận. Điều này có nghĩa là nếu người nhận đang ở trên mạng thì thông điệp chỉ hiển thị trên thiết bị đầu cuối trường hợp ngược lại thông điệp được phân tới hộp thư.

Sau khi nhận được một trong bốn câu lệnh trên, máy phục vụ SMTP sẽ trả về một trong các trạng thái sau:

250	Người gửi được chấp nhận
552	Vượt giới hạn chứa cục bộ
451	Lỗi cục bộ
452	Tràn bộ đệm
500	Sai về cú pháp lệnh
501	Sai về cú pháp biến
421	MTA không chấp nhận
502	Lệnh không thực hiện

Mã trả về bởi lệnh MAIL FROM

Sau khi máy khách SMTP giới thiệu địa chỉ thư của người gửi thông điệp và nhận được mã trạng thái trả về từ máy phục vụ SMTP là 250, máy khách SMTP sẽ lần lượt giới thiệu từng địa chỉ thư của những người được nhận thông điệp. Trong trường hợp này máy khách SMTP sẽ sử dụng câu lệnh RCPT TO ví dụ như sau:

C: RCPT TO:

Máy phục vụ SMTP sẽ trả về một trong những mã trạng thái trong bảng ở hình dưới

Mỗi câu lệnh RCPT TO sẽ chỉ giới thiệu địa chỉ thư của một trong số những người nhận. Do đó nếu máy khách SMTP muốn gửi thông điệp cho bao nhiêu người thì phải thực hiện từng đó câu lệnh RCPT TO. Tuỳ thuộc vào từng địa chỉ thư mà máy phục vụ SMTP sẽ đưa ra mã trạng thái khác nhau. Nếu máy phục vụ SMTP chấp nhận địa chỉ thư của người nhận, nó sẽ trả về mã trạng thái 250. Nếu khác, có nghĩa máy phục vụ không chấp nhận địa chỉ thư của người nhận vì một lý do nào đó. Nếu máy khách SMTP không muốn máy phục vụ SMTP truyền thông điệp (mã 251), máy khách SMTP sẽ vô hiệu toàn bộ tiến trình với câu lện RSET và sau đó bắt đầu một tiến trình truyền mới nếu cần hay huỷ bỏ giao dịch.

250	Địa chỉ người nhận được chấp nhận
251	Truyền đến người nhận
550	Không có người nhận

553	Địa chỉ người nhận không hợp lệ
551	Địa chỉ thư không cục bộ
450	Hộp thư đang bị khoá
451	Lỗi cục bộ
452	Tràn bộ đệm
551	Vượt quá giới hạn chứa
500	Sai về cú pháp lệnh
501	Sai về cú pháp biến
502	Không tồn tại lệnh này
421	MTA không chấp nhận

Mã trả về bởi lệnh RCPT TO

- Trong trường hợp mã lỗi 551 ứng với người nhận là không cục bộ và máy phục vụ SMTP từ chối truyền thông điệp, máy khách SMTP sẽ xét máy phục vụ SMTP có khả năng thích hợp hơn để sử dụng. Máy khách SMTP thực hiện được điều này bằng cách tham chiếu bản ghi MX (MX record) Với địa chỉ mềm của người nhận
- Trong trường hợp máy phục vụ SMTP trả về mã lỗi 450, 451, 452 hoặc 552, máy khách SMTP sẽ ghi nhớ địa chỉ thư của người nhận để thử tiếp và giao dịch SMTP tiếp theo.
- Trong trường hợp máy phục vụ SMTP trả về mã 500, 501, 503 máy khách SMTP sẽ thử một máy phục vụ SMTP khác. Lỗi này được xem như lỗi tạm thời. Cuối cùng, nếu MTA cục bộ của máy phục vụ SMTP không hợp lệ thì máy khách SMTP sẽ vô hiệu hoá toàn bộ giao dịch bằng câu lệnh RSET ghi nhớ địa chỉ người nhận để thử vào phiên giao dịch SMTP sau. Nừu có dù chỉ một địa chỉ người nhận được máy phục vụ SMTP chấp nhận, máy khách SMTP sẽ tiến hành truyền nội dung thông điệp. Nếu không, máy SMTP sẽ đưa ra câu lệnh RSET để bắt đầu một giao dịch mới hoặc là huỷ bỏ giao dịch.
- Để thực hiện việc truyền một thông điệp, máy khách SMTP sẽ thực hiện câu lệnh DATA

Ví dụ

C: DATA

Các mã trạng thái máy phục vụ SMTP có thể trả về như sau:

354	Chờ nội dung
451	Lỗi cục bộ
554	Giao dịch thất bại
500	Sai về cú pháp lệnh
501	Sai về cú pháp biến
503	Lệnh không thực hiện
521	MTA không chấp nhận

Mã trả về bởi lệnh DATA

Nếu mã trạng thái trả về là 354 thì máy khách SMTP có nhiệm vụ gửi thông điệp. Thông điệp được gửi qua mối liên kết từng dòng một, mỗi dòng kết thúc bởi cặp kí tự CR-LF (\r\n). Nội dung của thông điệp phải được kết thúc bởi một dòng trắng có chứa duy nhất một ký tự ".".

Nếu một dòng trong thông điệp lại được bắt đầu bởi ký tự "." Thì để tránh nhầm lẫn với dòng kết thúc thông điệp máy khách SMTP phải thêm vào trước dòng đó một ký tự "." Khi toàn bộ thông điệp đã được gửi xong, máy khách SMTP sẽ gửi thêm ký tự ".". Để chứa các thông điệp mới, máy phục vụ SMTP sẽ tạo một bộ đệm và sau đó đọc các thông điệp từ mối liên kết TCP vào trong bộ đệm. Mỗi khi máy phục vụ SMTP nhận được một dòng bắt đầu bởi ký tự ".". Nó sẽ bỏ ký tự đó đi.

Máy phục vụ SMTP sẽ trả về một trong những mã trạng thái bảng 2.7:

Khi máy phục vụ SMTP nhận được thông điệp một cách thành công, nó sẽ trả về mã trạng thái 250. Máy khách SMTP sẽ xoá bỏ dần các địa chỉ người nhận mà máy phục vụ SMTP đã chấp nhận trên phong bì cho tới khi không còn địa chỉ người nhận nào nữa.

250	Chấp nhận thông điệp
550	Vượt quá giới hạn chứa
553	Giao dịch thất bại
451	Lỗi cục bộ
452	Tràn bộ đệm

Mã trả về bởi lệnh kết thúc "." Thông điệp

Câu lệnh kiểm tra: (Probe)

Mỗi khi máy khách SMTP giới thiệu bản thân với máy phục vụ SMTP xong, nó có thể yêu cầu máy phục vụ SMTP xác nhận hộp thư của người nhận thông điệp là cục bộ hay không.

C: VRFY mrose

Máy khách SMTP yêu cầu máy phục vụ SMTP xác nhận hộp thư mang tên mrose là cục bộ hay không?

Máy phục vụ SMTP có thể trả lời bằng một trong những mã trạng thái sau:

250	Địa chỉ cục bộ
251	Địa chỉ không cục bộ truyền
552	Hộp thư không hợp lệ
500	Sai về cú pháp lệnh
501	Sai về cú pháp biến
502	Không thực hiện lệnh
503	Không thực hiện biến
421	MTA không chấp nhận

Mã trả về bởi lệnh VRFY

Nếu máy khách SMTP muốn xem những người nào sẽ nhận được thông điệp gửi tới một địa chỉ cục bộ nó sẽ làm như sau:

C: EXPN st-columnist

250	Người dùng là cục bộ
550	Không tồn tại người dùng như vậy
500	Sai về cú pháp lệnh
501	Sai về cú pháp biến
502	Không thực hiện lệnh
503	Không thực hiện biến
421	MTA không chấp nhận

Mã trả về bởi lệnh EXPN

Nếu mã trạng thái là 250, máy phục vụ SMTP sẽ xác định các địa chỉ mà sẽ được nhận thông điệp.

Giao thức SMTP không đưa ra độ dài tối đa của một thông điệp. Trong thực tế kích thước lớn nhất của thông điệp là 64 K.

2. Dịch vụ FTP:

Việc truyền file dùng giao thức FTP không phân biệt dạng tệp dù đó là ASCII hay nhị phân . . .chỉ cần một máy cấu hình tốt thiểu và một máy FTP server, bạn có thể phân lớp người sử dụng nào có quyền truy nhập phần nào trong kho dữ liệu của bạn, giới hạn số người sử dụng dịch vụ cùng một thời điểm v.v. FTP giúp cho người sử dụng truy cập File và thư mục một cách tương tác trên một máy chủ ở xa và thực hiện thao tác trên thư mục như sau:

-Liệt kê các File trong thư mục cục bộ hoặc ở xa.

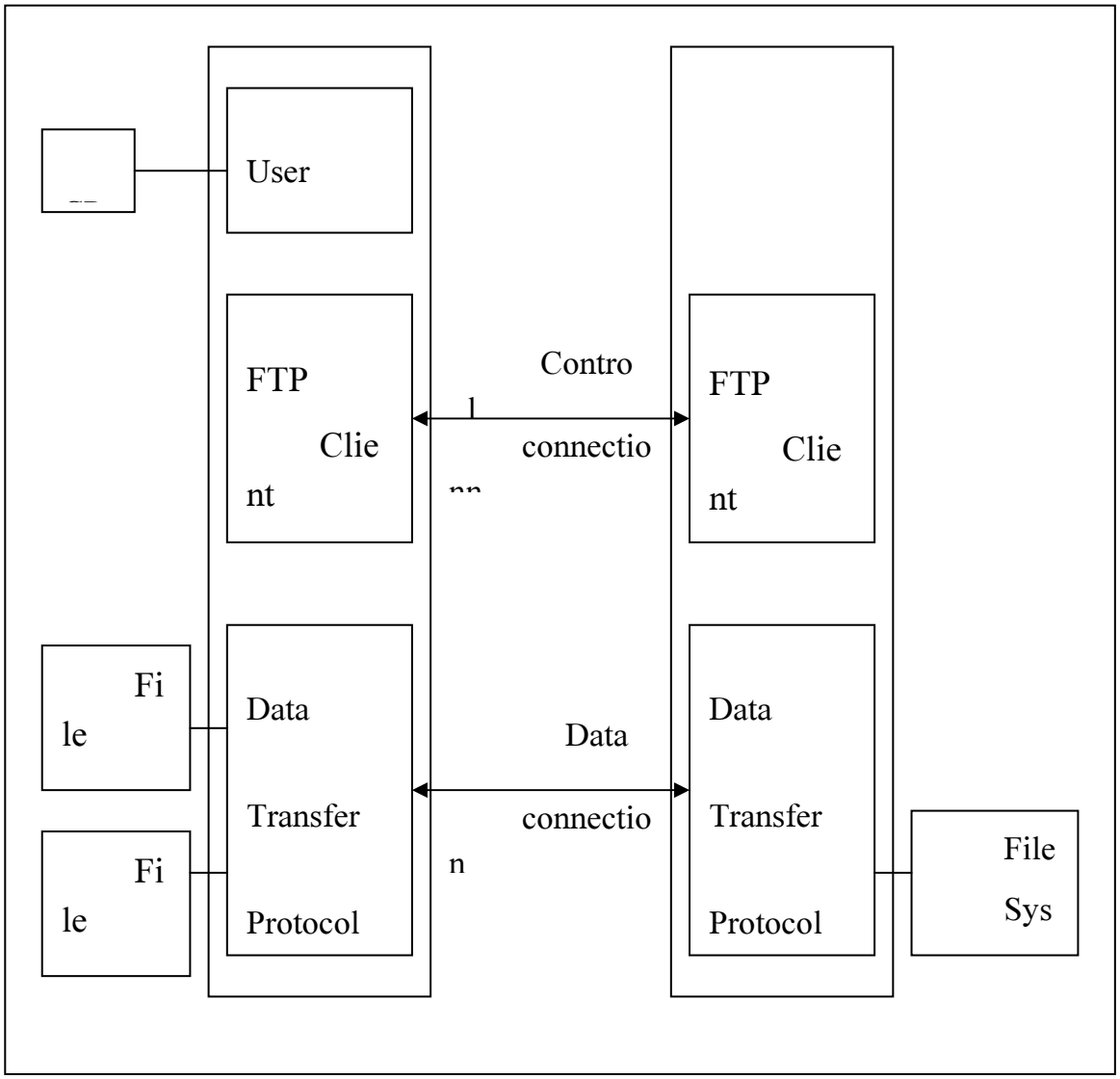
-Đổi tên và xóa tập tin (nếu người dùng có quyền).

-Truyền File từ máy chủ ở xa về máy cục bộ (download: nạp về).

-Truyền File từ máy máy cục bô đến máy ở xaỹ (upload:truyền lên).

Điểm đáng nhớ rằng FTP chỉ chuyển những tập tin từ máy chủ ở xa về máy cục bộ, nếu đang dùng một kết nối quay số để kết nối với Internet thì có sự khác nhau giữa máy chủ và hệ thống đang dùng. Nếu nối trực tiếp với Internet thì máy chủ và hệ thống là một và như nhau. Bởi vì FTP cho phép truyền tập tin nên nó là một chương trình dùng thường xuyên nhất khi được nối mạng với Internet. Thật ra có hàng nghìn vùng FTP sẵn có trên Internet, tất cả những vùng này đều được truy cập một cách như nhau.

Hình vẽ sau đây minh họa mô hình FTP.



Mô hình trên minh hoạ sự tương quan giữa Client và Server. Người sử dụng sẽ "vào" một Server khác để truy cập dữ liệu.Việc thực hiện truyền dữ liệu không thực hiện trên một kết nối điều khiển mà được thực hiện trên một kết nối dữ liệu.

Các yếu tố mà chúng tạo thành giao thức truyền File là:

♦ **Khuôn dạng cúa dữ liệu được truyền**: để thực hiện việc truyền và nhận dữ liệu có hiệu quả giữa bên nhận và bên gửi thì hai bên phải có sự thoả thuận chung về dạng dữ liệu mà chúng sẽ được truyền, nhận. Dữ liệu có thể tồn tại ở dạng văn bản hoặc nhị phân và có một vài cấu trúc của dữ liệu được xây dựng ở dạng nhị phân bảng ghi hoặc ở dạng khối.

♦ **Kiểu dữ liệu**: một File có thể chứa văn bản ở dạng ASCII, EDCDIC text hoặc dữ liệu hình ảnh ở dạng nhị phân.

♦ **Cấu trúc File**: hầu hết những cấu trúc chung gán đến File được gọi là cấu trác File.

Tuy nhiên là có sự hạn chế, những người bình thường chỉ cho phép sao chép các tệp chứ không thể tạo ra tệp mới hoặc biến đổi các tệp hữu hiệu. Khi dịch vụ này được cung cấp thì nó sẽ có một Login name đặc biệt là ANONYMOUS và nếu dùng nó làm login - name thì FTP sẽ chấp nhận một xâu kí tự bất kỳ như password. Sau khi đã đăng nhập như một "anonymous", chúng ta sẽ được phép lấy các tệp mà người ta đã dành riêng cho những kẻ "vô danh"!.

Để thực hiện việc truyền File ta cần thực hiện các bước sau:

1- Gõ lệnh FTP và cung cấp tên máy chủ

♦ FTP < Tên máy chủ>

Ví du

C:\> ftp 200.201.202.2

2- Nếu máy chủ không đăng nhập được thì một thông báo xuất hiện. Chi tiết thông báo này hiển thị có thể khác nhau.Nhưng hầu hết hiện ngay thông báo này :

ftp trav.trs.com

trav.trs.com:unknow host ftp

Khi nhận thông báo này có thể một trong những điều sau đã xảy ra:

♦ Dùng địa chỉ máy chủ không chính xác. Kiểm tra lại chính tả và trật tự vùng sau khi thử lại.

♦ Máy chủ này không hiện hành trên mạng, sau đó thử lại.

♦ Có sự cố đối với chủ dịch vụ DNS, nghĩa là nó không hiển thị được tên máy chủ cung cấp. Nếu nghi ngờ khả năng này thử gọi lệnh lần nữa, lần này dùng địa chỉ IP thay thể cho tên máy chủ .

Khi máy chủ đăng nhập được thì dòng thông báo sau đây xuất hiện (của máy đăng nhập ở ví dụ trên):

220 www Microsoft FTP Service (version 3.0).

3- Cung cấp tên người và mật khẩu.

Sau khi kết nối tên máy chủ xong thì người sử dụng phải cung cấp mật khẩu còn tên người (password) có thể để trống

Ví du

Sau khi đăng nhập thì dòng thông báo sau xuất hiện :

User (200.201.202.2:(none)):anonymous

331 Anonymous access allowed, send identity(E-mail name) as password.

Password:(để trống)

230- welcome to FTP service from IT Dept.

230 Anonymous user logged in.

Một số máy phục vụ FTP đòi hỏi mật khẩu là địa chỉ thư điện tử của người dùng. Mặc dù tính hiệu lực của địa chỉ thư điện tử không được kiểm tra, người sử dụng nên tuân theo các yêu cầu của máy phục vụ FTP. Một số máy phục vụ thực sự kiểm tra địa chỉ của người dùng, sử dụng cơ chế điều khiển đảo DNS và không cấp quyền truy cập các dịch vụ của chúng trừ khi địa chỉ người sử dụng cung cấp phù hợp với giá trị nhận dạng DNS khi gán cho địa chỉ IP của hệ thống mà lưu thông của người sử dụng xuất phát từ đó.

4- Thực hiện công việc truyền:

Thế là người sử dụng đã đăng nhập được vào giao thức, con trỏ đang ở **ftp>**, từ bây giờ có thể sử dụng các lệnh của FTP để thực hiện việc truyền File. Khi chưa nắm rõ các lệnh của FTP ta dùng lệnh "?".

Ví dụ.

ftp> ?

Commands may be abbreviated. Commands are:

!	delete	literal	prompt	send
?	debug	ls	put	status
append	dir	mdelete	pwd	trace
ascii	disconnect	mdir	quit	type
bell	get	mget	quote	user
binary	glob	mkdir	recv	verbose
bye	hash	msl	remotehelp	
cd	hepl	mput	rename	
close	lcd	open	rmdir	

ý nghĩa các lệnh trên:

Lệnh	**ý nghĩa**
!	Đưa ra lệnh phần mềm tại máy chủ điều khiển từ xa.
?	Hiển thị danh sách lệnh.
Bell	Reo chuông sau mỗi File truyền đi
Bye	Kết thúc sự kết nối và thoát khỏi FTP
Cd	Chuyển đổi thư mục .
Close	Kết thúc sự kết nối

Delete	xóa tập tin trên hệ thống ở xa
Dir	Liệt kê những tập tin trong thư mục
Disconnect	Kết thúc sự kết nối
Get	Chuyển tập tin ở xa đến hệ thống cục bộ
Hash	Cho phép/hủy bỏ hiển thị dấu hiệu # cho mỗi khối dữ liệu được truyền đi
Help	Hiển thị danh sách lệnh
Lcd	Chuyển đổi thư mục trên hệ thống cục
Ls	Tóm tắt danh sách tập tin trên thư mục
Mdelete	xóa tất cả các tập tin trên thư mục ở xa
Mdir	Liệt kê tất cả các tập tin trong thư mục ở xa
Mget	chuyển những tập ở xa về hệ thống cục bộ
Mkdir	Tạo thư mục trên hệ thống ở xa
Mls	Danh sách tóm tắt các tập tin trong nhiều thư mục trên hệ thống ở xa
Mput	Chuyển đổi tập tin từ hệ thống xa đến hệ thống cục bộ
Open	Thành lập một kết nối với một máy chủ từ xa
Put	Chuyển tập tin từ hệ thống cục bộ đến hệ thống từ xa
Pwd	Hiển thị tên các thư mục hiện hành trên hệ thống từ xa
Quit	Kết thúc kết nối và ra khỏi FTP
Recv	Chuyển tập tin từ hệ thống ở xa đến thư mục cục bộ
Rename	Đổi tên một tập tin trên hệ thống ở xa
Send	Chuyển tập tin từ hệ thống cục bộ đến hệ thống ở xa
Status	Hiển thị tình trạng của FTP
Verbose	Cho phép/ hủy bỏ đáp ứng Verbose.

Ví dụ:

ftp> dir

200 PORT command logged in.

150 Opening ASCII mode date connection for /bin/ls.

Dr-xr-xr-x	1 owner	group	0 Apr 8 1998 h2h
Dr-xr-xr-x	1 owner	group	0 Apr 8 1998 Tu
Dr-xr-xr-x	1 owner	group	0 Apr 9 6:56 H2H

226 Transfer complete.

ftp: 191 bytes received in 0. 06Seconds 3.18Kbytes/sec

- Vào thư mục Tu

ftp> cd tu

250 CWD command successful.

ftp> dir

200 PORT command logged in.

150 Opening ASCII mode date connection for /bin/ls.

- r-xr- xr 1 owner group 500 May 15 1998 D2.COM

- r-xr- xr 1 owner group 64600 May 15 1998 VRE.COM

226 Transfer complete.

ftp: 135 bytes recieved in 0. 06 seconds 2.25Kbytes/sec.

Nghiã là trong hệ thống 200.201.202.2 có 3 thư mục h2h, Tu, H2H. Trong thư mục Tu có 2 File D2.COM và VER.COM . Muốn sao chép File về thư mục hiện thời thì dùng:

ftp> get

200 PORT command Successful.

550 xer: The system cannol find the file specified

Thế là đã hoàn thành một phiên là việc của FTP

ftp> quit

221 Good Bye !

3. Dịch vụ tên miền DNS (Domain name system): Việc định danh các phần tử của mạng bằng các con số như trong địa chỉ IP rõ ràng là không làm cho người sử dụng hài lòng, bởi chúng khó nhớ, dể nhầm lẫn. Vì thế người ta đã xây dựng hệ thống tên (name) cho các phần tử của Internet, cho phép người sử dụng chỉ cần nhớ đến các tên chứ không cần nhớ đến các địa chỉ IP nữa.

Hệ thống DNS chủ yếu hoạt động như một hệ quản trị tên. Khi được cung cấp tên máy chủ, DNS định tên đó sang địa chỉ IP. DNS cũng có thể thực hiện chuyển đổi ngược lại, nghĩa là khi được cung cấp một địa chỉ IP, DNS có thể trả về máy chủ được đăng ký cho địa chỉ IP đó.

DNS được thực hiện như một cơ sở dữ liệu phân tán việc tìm kiếm cho sự kết hợp từ tên sang địa chỉ IP và ngược lại. Nói cách khác, để thực hiện việc tìm kiếm tên là lưu trữ thông tin từ tên sang địa chỉ IP trong một tập tin tĩnh.Việc ánh xạ giữa địa chỉ IP và các tên miền được thực hiện bởi 2 thực thể có tên là Name Resolver và Name Server .

- *Name Resolver* được cài đặt trên trạm làm việc (workstation) .
- *Name server* được cài đặt trên máy chủ (server).

Người sử dụng làm việc gọi chương trình Name Resolver để gửi yêu cầu ánh xạ địa chỉ (host name - to - IP address) tới Name server. Nếu host name được tìm thấy thì Name Servers sẽ gửi địa chỉ IP tương ứng về trạm làm việc. Sau đó trạm làm việc sẽ thử liên kết với host bằng cách dùng địa chỉ IP chứ không dùng tên nữa.

4. Dịch vụ đăng nhập từ xa (TELNET):

TELNET cho phép người sử dụng từ trạm làm việc của mình có thể đăng nhập (login) vào một trạm ở xa qua mạng và làm việc với hệ thống y như là một trạm cuối (Terminal) nối trực tiếp với trạm xa đó. Telnet là một giao thức tương đối đơn giản so với các chương trình

phỏng tạo trạm cuối (Terminal emulator) phức tạp hiện nay. Đây là một ứng dụng hoàn toàn khác, vì các emulator đó thường cung cấp liên kết phỏng tạo trạm cuối dị bộ (asynchronous), trong khi Telnet cung cấp sự phỏng tạo trạm cuối của mạng. Lý do chính của sự phổ biến của Telnet vì đó là một đặc tả mở và khả dụng rộng rãi cho tất cả các hệ nền chủ yếu hiện hay.

Để khởi động một Telnet, từ trạm làm việc của mình người sử dụng chỉ cần gõ:

Telnet <tên máy chủ>

Khi bắt đầu Telnet, thông báo sau sẽ xuất hiện: **Trying IP adress (IP adress: là địa chỉ máy tính được Telnet vào)**. Nếu thành công thì thông tin về trình login sẽ được hiển thị và tại dấu nhắc hệ thống, người sử dụng phải nhập vào **username** và **password**. Bây giờ đã có thể làm việc với hệ thống này.

Ví dụ c:\> tenlet 200.201.202.2

Trying 200.201.202.2

Connected 200.201.202.2

5. Dịch vụ thư tín điện tử (E-MAIL):

Đây là một trong những dịch vụ thông tin phổ biến nhất trên Internet. Tuy nhiên, dịch vụ này khác với các dịch vụ trên dịch vụ thư điện tử không phải là dịch vụ " từ đầu - đến cuối "(end- to end), nghĩa là máy gửi thư và máy nhận thư không cần phải liên kết trực tiếp với nhau để thực hiện việc chuyển thư. Nó là dịch vụ kiểu lưu và chuyển tiếp. Thư điện tử được chuyển từ máy này sang máy khác cho tới máy đích .

Mỗi người sử dụng phải kết nối với một E- Mail Server gần nhất, người sử dụng sẽ gửi thư tới E- Mail server của mình. E- Mail Server này có nhiệm vụ chuyển thư đến đích hoặc đến một E- Mail Server trung tâm khác. Thư sẽ chuyển đến E- Mail Server người nhận và được lưu ở đó. Đến khi người nhận thiết lập một cuộc kết nối tới E- Mail Server đó thì thư sẽ được chuyển về máy của người nhận, nếu không thì thư vẫn cứ tiếp tục được giữ lại Server để bảo đảm không bị mất thư. Giao thức truyền thông sử dụng hệ thống thư của Internet là SMTP. Hệ thống địa chỉ thư điện tử trên Internet không chỉ định danh cho các Host của mạng mà còn phải xác định rõ người sử dụng trên các Host đó để trao đổi thư . Cấu trúc thư điện tử gồm hai phần :

- Phần đầu thư : có chứa địa chỉ người nhận, người gửi và một số thông tin khác. Thư được chuyển đến đích được hay không là ở phần này.

- Phần thân thư : có nội dung bức thư ,tất cả đều ở dạng ASCII 7 bit.

Dựa trên E- Mail, người ta tạo ra các dịch vụ mở rộng của E-Mail, có hai dịch vụ phổ biến dựa trên E- Mail đó là:

- *Mailing lists* : phương thức cung cấp thông tin tới một nhóm người dùng điện thư cùng một lúc, khi có một bức thư được gửi cho nhóm thì cả nhóm đều nhận được, qua dịch vụ này người ta có thể tạo ra các nhóm thảo luận, khi người trong nhóm đưa ra ý khiến nào thì mọi người trong nhóm đều nhận được .

- *E- Mail information Server*: là một chương trình , nó nhận các yêu cầu về thông tin bằng E- Mail, sau đó tìm kiếm thông tin theo yêu cầu và trả lại các thông tin tìm kiếm được bằng E-Mail hoặc bằng đường truyền file như ftp mail, archive Server . . .

6. Dịch vụ Gopher:

Đây là dịch vụ cho phép tra cứu thông tin trên mạng theo chủ đề trên hệ thống thực đơn (menu) mà không biết đến địa chỉ IP tương ứng.

Gopher hoạt động theo phương thức khách / chủ. Nghĩa là phải có hai chương trình: Gopher client và Gopher server. Bạn có thế lựa chọn một chương trình Gopher client tương ứng với hệ điều hành sử dụng. Mỗi chương trình client này được cấu hình trước với địa chỉ IP của một Gopher server nào đó. Khi khởi động Gopher server và trên màn hình sẽ hiển thị bảng thực đơn chính. Người dùng sẽ chọn đề mục mà mình quan tâm. Người dùng có thể lấy các tệp văn bản về máy của mình để xử lý. Gopher clinet "nói chuyện" với Gopher Server theo một giao thức gọi là Gopher protocol. Một thế mạnh của Gopher so với các dịch vụ trên là nó không những cho phép lấy dữ liệu cục bộ mà còn lấy dữ liệu trên các máy khác trên mạng mà nó chỉ tới và điều này không ảnh hưởng tới clinet .

Điều hạn chế lớn nhất của dịch vụ này là việc hiển thị thông tin theo đề mục rất tóm tắt. Mặt khác, Gopher cung cấp khả năng rất hạn chế trong việc tìm kiếm thông tin khiến người sử dụng có thể bị nhầm lẫn trong quá trình tra cứu thông tin.

7 Dịch vụ WWW(Word Wide Web):

WWW hay còn gôi là Web, đây là dịch vụ lớn nhít, phát triển mạnh nhít và híp dĩn nhít trên Internet. Nê dựa trên mĩt kỹ thuịt biểu diển thông tin cê tên là siêu văn bản. Các thông tin trên Web cê thể liên kết với các tài liệu khác cê chứa những thông tin bư sung .

Để xây dựng các trang thông tin đa phương tiện, chúng ta sử dụng ngôn ngữ HTML (Hyper Text Markup Language). HTML cho phép đôc và liên kết các dữ liệu khác nhau trên cùng mĩt trang thông tin. Nê là mĩt ngôn ngữ định dạng. Mìi tệp văn bản được đánh díu bằng các "thẻ" (tag), thẻ của HTML là mĩt đoạn mã được giới hạn bịi các díu ngươc nhôn "<","">".

Để thực hiện việc truy cịp, liên kết các tài nguyên thông tin khác nhau theo kỷ thuịt siêu văn bản, Web sử dụng điều kiên URL (Uniform Resource Locator). Đây chính là mĩt dạng tên để định danh duy nhít cho mĩt tài liệu hươc mĩt dịch vụ trong Web. Cíu trúc của mĩt URL thứng bao gơm các thành phìn thông tin như: giao thức Internet được sử dụng, vị trí của Server, tài liệu cụ thể trên Server và cê thể thêm các hoạt đĩng thông tin định danh khác. **Cụ thể là**:

máy chủ>/[<thư mục>]/[<tài liệu cìn truy cịp>]

<u>Ví dụ</u>:

Chú ý: díu :// không thể bâ sêt.

Các phìn mềm web brower líy các tài liệu HTML từ Server, dịch tài liệu này và hiển thị nĩi dung ra màn hình, ngứi ta gôi là các trang Web, trình brower sẽ tạo mĩt liên kết tới đích mà ngứi dùng trâ đến. Đích này cê thể là mĩt trang Web khác. Tài liệu HTML cê khả năng liên kết với rít nhiều dạng thông tin khác như văn bản, hình ảnh , âm thanh . . ..Tuy nhiên, do tính đa dạng của trang Web, nên để vịn dụng hết

tính ưu việt của nê thì dòi hâi những ngưới cê đứng kết nỉi tỉc đĩ cao vào mạng Internet.

8 Dịch vụ Wais (Wide Area Information Server):

Cũng giỉng như Gopher, WWW , Wais cho phép tìm kiếm và truy cịp thông tin trên mạng mà không còn biết chúng đang thực sự nằm ị đâu. *Dịch vụ Wais* cho phép tra cứu thông tin trên mạng. Ngưới sử dụng còn đến mĩt thông tin văn bản nào đê chỉ còn cung cíp từ khêa và sẽ nhịn được nĩi dung văn bản.

Wais hoạt đĩng theo mô hình " chủ/khách ". Wais cê chức năng tìm kiếm dữ liệu hơn hẳn Gopher và WWW, Wais không những dùng giao diện cho ngưới dùng để hiển thị thông tin mà còn hì trợ tìm kiếm thông tin rít hữu hiệu. Về khía cạnh nào đê, ngưới ta coi Wais như là mĩt bư sung rít tỉt cho Gopher và WWW.

Dịch vụ của Wais ngoài các chương trình Wais clienet và Wais Server còn cê thêm chương trình Wais Indexer thực hiện việc truy cịp dữ liệu mới, sắp xếp theo chỉ sỉ để tiện việc tìm kiếm . Server nhịn câu hâi từ Clinet rơi tìm kiếm trong cơ sị dữ liệu các tệp phù hợp, đánh giá đĩ phù hợp của các tệp đê và gửi về cho Clinet. Câu hâi tìm kiếm được xây dựng theo chuỉn Z39.50 của ANSI. Cũng như Gopher, với mìi hệ điều hành thông dụng hiện nay đều cê các chương trình Wais Clinet tương ứng .Ngoài những chức năng đã nêu Wais còn hiển thị tệp đơ hôa.

Mĩt vín đề nảy sinh là các chỉ mục dữ liệu thứng rít lớn so với chính bản thân dữ liệu. Khi ta đánh chỉ mục các tệp văn bản thì cê thể tệp chỉ mục sẽ rít lớn. Nếu Wais bao gơm nhiều loại thông tin đế tìm kiến thì ta phải trả giá về không gian đĩa để chạy. Vì vịy, ngưới ta đang tìm biện pháp để giải quyết vín đề này.

IX. CÔNG NGHỆ CHUYỂN MẠCH NHANH TRONG LAN VÀ WAN :

1. Đánh giá quá trình chuyển mạch gói từ mạng X.25 đến ATM :

Trong truyền thông, vấn đề tốc độ cựỵc kỳ quan trọng, mọi hướng giải quyết, xây dựng giao thức tầng nhằm đưa chất lượng thông tin và tốc độ truyền lên cao. Trong những năm gần đây các quan điểm mới về hệ thống mạng được phát triển rất mạnh, từ mạng cục bộ cho đến mạng diện rộng, từ những máy tính với những hệ thống mạng khác nhau trên thế giới đều có nhu cầu trao đổi thông tin. Do đó, hệ thống truyền thông phải có độ mềm dẻo thích hợp để thích ứng với những môi trường truyền khác nhau và đảm bảo tính trong suốt về nội dung và thời gian, nghĩa là đảm bảo việc truyền đúng các bit từ đầu phát cho đến đầu thu và thời gian trễ ngắn.

Trong các mạng chuyển mạch gói như X.25 ta đã khảo sát, chất lượng truyền số liệu còn kém do công nghệ điện tử có độ ổn định chưa cao nên để đảm bảo chất lượng truyền chấp nhận được người ta phải thực hiện chức năng điều khiển lỗi trên mọi liên kết. Việc điều khiển lỗi này được thực hiện bởi giao thức HDLC và các giao thức từ HDLC như LAP.B bao gồm các chức năng : giới hạn khung, đảm bảo truyền bit chính xác. Kiểm tra lỗi (kiểm tra mà dư vùng CRC - Cyclic Redumdancy Check), sửa lỗi bằng các thủ tục truyền lại.

ở đây, quá trình điều khiển lỗi được thực hiện trên mọi liên kết (Link by Link) thông qua nút chuyển mạch, do đó nút chuyển mạch phải xử lý một loạt các thủ tục phức tạp khác nhau làm ảnh hưởng đến tốc độ xử lý chung của hệ thống.

Sau này với chất lượng của hệ thống truyền dần ; các công nghệ bán dẫn ; công nghệ quang phát triển mạnh đảm bảo xác suất truyền lỗi thấp và không có nhiễu xuyên âm nên tỷ lệ lỗi trên mạng giảm.

Với một mạng chất lượng cao như vậy, người ta chỉ cần thực hiện một số chức năng truyền bit chính xác, kiểm tra lỗi, trên cơ sở từ liên kết đến liên kết còn chức năng khác nhau sửa lỗi sẽ được thực hiện trên cơ sở từ đầu cuối tới đầu cuối (End to end). Bằng cách này người ta đã giảm được khối lượng thông tin mà nút chuyển mạch cần xử lý, đặc biệt trong giai đoạn hiện nay sự phát triển của mạng diện rộng cùng với sự kết nối với các mạng LAN, thông qua mạng WAN làm cho số nút chuyển mạch tăng nhiều nên việc giảm chức năng sửa lỗi tại nút là cần thiết để tăng tốc độ xử lý của nút.

Như vây, lớp 2 trên mô hình OSI được chia thành 2 lớp con :

- 2a chuyên cung cấp các chứa năng cơ bản của lớp 2.

- 2b cung cấp các chức năng bổ sung.

Hệ thống ứng dụng nguyên lý này gọi là *chuyển tiếp khung* (frame Relay) đã khảo sát. Với ý tưởng giảm chức năng ở nút chuyển mạch ngày càng được mở rộng

trong mạng D-ISDN do người ta đã tính được khả năng lỗi thấp vì thiết bị truyền dẫn ngày càng có ổn định cao về mặt vật lý nên chức năng điều khiển lỗi không còn được cung cấp ở các nút chuyển mạch trong mạng vừa mà trong trường hợp cần thiết, sẽ được cung cấp bởi thiết bị đầu cuối. Như vậy, các chức năng được thực hiện trong mạng giảm từ điều khiển lỗi đầy đủ ở mạch chuyển mạch gói với giao thức tầng 2 LAP.B của X.25 xuống còn tối thiểu ở mạng ATM.

Do đó, các nút của ATM có độ phức tạp tối thiểu vì thế tốc độ truyền rất cao.

So sánh chức năng giữa chuyển mạch gói, chuyển tiếp khung và ATM được trình bày bảng sau :

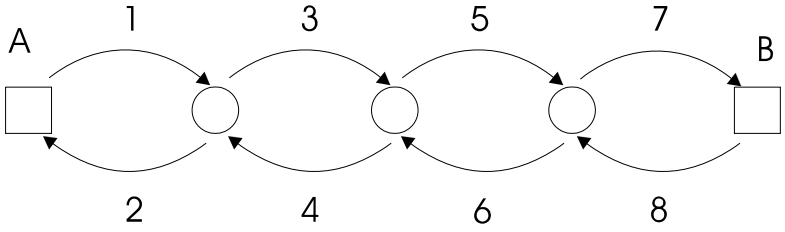
Chức năng	**Chuyển tiếp gói X.25**	**Chuyển tiếp khung(Frame Relay)**	**ATM**
Truyền lại gói	X	-	-
Giới hạn khung	X	X	-
Kiểm tra lỗi	X	X	-

Bảng 4.1. So sánh chức năng tại các nút chuyển mạch

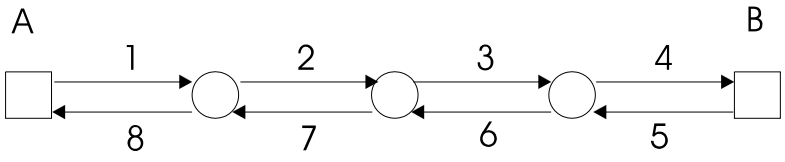
So sánh	Chuyển tiếp gói X.25	Frame Relay	ATM
Kích thước gói tin	biến đổi	biến đổi	cố định 53 bytes
Tốc độ	64 Kbps	<10 Mbps	>100Mbps

Bảng 4.2. So sánh khuôn dạng dữ liệu và tốc độ truyền:

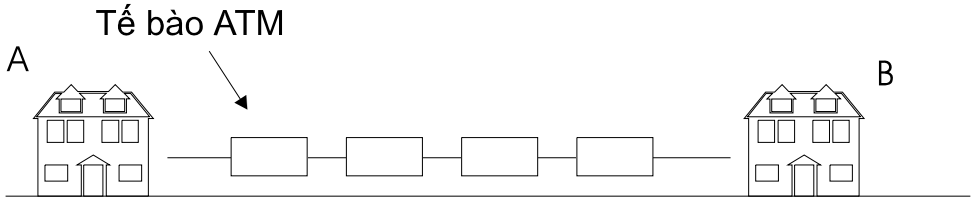
Minh họa hoạt động bằng các mô hình sau:



Hình 7.6: Qúa trình vận chuyển gói tin của X25 giữa 2 trạm A và B qua các nút chuyển mạch.



Hình 7.7: Qúa trình vận chuyển của Frame relay giữa 2 trạm A và B qua các nút chuyển mạch.



Hình 7.8: Qúa trình vận chuyển ATM

Sự vận chuyển giữa hai trạm nguồn và đích ở tầng vật lý thường xuyên có khung chứa thông tin vận chuyển không ngừng một cách đồng bộ với kích thước cố định. Khi có dữ liệu cần truyền chúng sẽ được cấu tạo thành các tế bào và được xếp vào các khung rỗng không đồng bộ cho đến hết thì thôi, thực hiện ở tầng ATM do đó tốc độ rất nhanh.

2. Đánh giá về chất lượng mạng:

Để đánh giá đúng về chất lượng của các mạng LAN và WAN, thông qua truyền thông tin một cách tin cậy, mạng phải đảm bảo 2 chỉ tiêu :

- Trong suửt v mỬt nũi dung.

- Trong suửt v mỬt thúi gian.

* *Tính trong suốt về mặt nội dung* đảm bảo cho mạng khả năng truyền thông tin một cách chính xác từ nguồn tới đích với số lỗi cho phép. Trong thức tế có 3 loại lỗi.

- Lỗi đơn vị số liệu dù là lỗi không thể khắc phục được và ít xảy ra.

- Lỗi số liệu bị phân phối nhầm là lỗi khi truyền tới đích sai.

- Lỗi số liệu không được truyền đi tức là số liệu không được truyền tới địa chỉ cho trước.

* *Trong suốt về mặt thời gian* : khi truyền một thông tin nào đó ta cấn phải xác định được thời gian truyền tới đích là bao lâu để đưa ra những phương pháp xử lý kịp thời, làm ảnh hưởng đến quá trình truyền hay cần phải đảm bảo độ trễ đủ nhỏ cho các dịch vụ thông tin trên mạng, Đặc biệt là dịch vụ thời gian thực. Trong suốt về mặt thời gian được đặc trưng bởi 3 tham số là :

Trễ truyền, trễ xử lý (delay) và biến động trễ (delay Jitter).

Trong đó trễ xử lý xảy ra tại các nút chuyển mạch và được quyết định bởi cấu tạo vật lý của mỗi nút cũng như phương pháp xử lý thông tin của chúng nên để khắc phục ta dùng những thiết bị tốt hơn là đủ. Trong ATM lỗi này rất bé nên tốc độ xử lý đã tăng đáng kể. Còn trễ truyền, quá trình lan truyền trên hệ thống mạng rất lớn nếu đường càng dài thì trễ truyền càng lớn nên cần phải chọn đường tập trung hay phân tán để tiết kiệm được thời gian trễ, đây là vấn đề khá phức tạp khi hệ thống mạng hiện nay quá nhiều loại mạng với tốc độ truyền lại khác nhau, như vậy phải hòa hợp được giữa chọn đường ngắn nhất và tốc độ trên mỗi hệ thống.

Biến động trễ là khỏang thời gian giữa độ trễ cực đại và cực tiểu hay độ trễ không đồng đều của các thông tin tới cùng một điểm cuối tại các thời điểm khác nhau.= Nó dẫn tới việc khôi phục tín hiệu không chính xác trong các dịch vụ yêu cầu thời gian thực.

* *Trong hệ thống mạng hiện nay,* việc xảy ra lỗi trong quá trình truyền tin đến đích là không thể tránh khỏi.

Trong trường hợp độ dài gói cố định như 53 byte của ATM. Yêu cầu về kích thước hàng đợi phụ thuộc vào tải và tỷ lệ mất gói lớn thì kích thước hàng đợi càng lớn.

Trong trường hợp độ dài thay đổi, tính toán kích thước hàng đợi phức tạp hơn nhiều và sẽ phụ thuộc vào độ dài gói. Nên đơn giản nhất là định kích thước hàng đợi tương ứng với gói có độ dài lớn nhất, lúc đó kích thước hàng đợi sẽ lớn hơn nhiều so với trường hợp gói có kích thước cố định.

Để đảm bảo chất lượng truyền chấp nhận được giữa hai đầu cuối (end - to - end) cần có các thủ tục phức tạp của X.25, nhằm xử lý lỗi và điều khiển luồng giữa các chặng liên kết (link - by - link). Mặt khác vì gói có độ dài khác nhau, nên yêu cầu cần phải có các thủ tục quản lý bộ đệm rất phức tạp. Do đó tốc độ không cao.

Trong X.25, lớp 2 sử dụng thủ tục truy nhập đường liên kết cân bằng LAPB (Balanced Link Access Produce). LAPB được sử dụng để thực hiện các chức năng nhận biết giới hạn khung, chèn, tách các bit lỗi, truyền lại các khung bị mất bằng thủ tục ARQ (Automatic Repeat Request) điều khiển luồng. Các hệ chuyển mạch gói sau này được cải tiến thành hai hệ thống là chuyển mạch khung (Frame Switching) và chuyển tiếp khung (Frame Relaying). Lúc này do chất lượng đường truyền tăng lên nên các yêu cầu về các chức năng điều khiển luồng và chống lỗi ở nút chuyển mạch có thể giảm xuống so với X.25 vì vậy tốc độ truyền cao hơn.

Trong chuyển tiếp khung, việc truyền lại các khung số liệu bị lỗi chỉ được thực hiện giữa hai đầu cuối của người sử dụng. Tại nút chuyển mạch chỉ có khả năng phát hiện lỗi để hủy bỏ các khung lỗi vì không cần thiết phải truyền các khung này.Ngoài ra cũng không có chức năng điều khiển luồng hoặc phân / hợp kênh. Trong chuyển mạch khung, các chức năng phát hiện lỗi và điều khiển luồng vẫn còn được giữ lại ở nút mạng. Do đó việc truyền lại khung và điều khiển luồng bằng cửa sổ trượt vẫn được thực hiện trên cơ sở các liên kết.

Hai hệ thống chuyển mạch khung và chuyển tiếp khung có rất nhiều ưu điểm. Tuy vậy chúng vẫn không có khả năng thực hiện các dịch vụ thời gian do trể lớn.

Với thời gian trể nhỏ ATM là mạng phục vụ cho các dịch vụ băng rộng và có nhiều ưu điểm hơn là:

- Mềm dẻo và phù hợp với các dịch vụ tương lai
- Có hiệu quả trong việc sử dụng tài nguyên
- Chỉ sử dụng một mạng duy nhất cho tất cả các dịch vụ.

X. TCP/IP QUA MẠNG ATM:

1. Giới thiệu:

Trong phần trước chúng ta đã khảo sát giao thức TCP/IP và hoạt động của mạng ATM. Trong đó TCP/IP là giao thức điều khiển truyền dẫn và giao thức liên mạng được sử dụng rộng rãi nhất trong lĩnh vực truyền thông dùng máy tính, với sự hỗ trợ của TCP/IP, các mạng dựa trên cơ sở ATM (phương thức chuyển giao không đồng bộ) có thể quản lý một lượng rất lớn các máy chủ, các trạm làm việc và các máy tính nối mạng.

Trong phần này chúng khảo sát mối quan hệ giữa ATM và TCP/IP.

2. Các giải pháp trong phạm vi IP và ALL:

2.1. Sự bao bọc (Encapsulation):

Việc chuyển giao các datagram IP đòi hỏi đóng gói vào trong các tế bào ATM. Sự phối hợp được thực hiện dựa trên ALL kiểu 5. Có hai cách giải quyết vấn đề này khi sử dụng nhóm giao thức ở đỉnh của ATM.

- *Cần chỉ định giao thức nào được sử dụng:* Chỉ định này được cung cấp bởi header LLC (Logacal Link Control) có thể theo sau header SNAP (Subnetwork attachment point). Các header này đặt ở mặt ngoài của đơn vị dữ liệu giao thức PDU ALL kiểu 5.

- *Sử dụng các kết nối ảo dành riêng cho mỗi giao thức:* Trong trường hợp này một phần từ mạng (bridge, router) nhận dạng giao thức được đóng gói trong ALL thông qua VPI/VCI.

2.2. Hội tụ - Phân đoạn - Và tái hợp trong AAL-5.

Khi một ứng dụng gửi dữ liệu qua một kết nối ATM sử dụng AAL-5, máy chủ trao một khối dữ liệu cho giao tiếp AAL-5, giao tiếp này sinh ra một trailer, chia thông tin thành các khối 48 bytes, và chuyển mỗi khối qua mạng ATM dưới dạng một tế bào đơn. Bên đầu cuối thu của kết nối, AAL-5 tái hợp các tế bào đến vào một gói, kiểm tra CRC để bảo đảm rằng gói dữ liệu đến là chính xác, và đưa kết quả cho phần mềm ở máy chủ. Qúa trình chia gói thành các tế bào và tập hợp chúng lại được gọi là phân đoạn và tái hợp ATM (SAR).

Để cho AAL-5 phía thu biết được có bao nhiêu tế bào hợp thành gói, AAL-5 phía phát sử dụng bit thấp trong trường kiểu payload của header trong tế bào ATM để đánh dấu tế bào cuối trong một gói. Như vậy AAL-5 phía thu sẽ gộp các tế bào đến cho đến khi nó tìm thấy trường kiểu có bit kết thúc gói được thiết lập. Các chuẩn ATM sử dụng khái niệm "hội tụ" để mô tả các cơ chế nhận dạng việc kết thúc một gói. Lưu ý rằng các giao thức lớp điều hợp ATM khác sử dụng các cơ chế hội tụ khác, còn AAL-5 thì sử dụng một bit đơn trong header của tế bào.

2.3. Đóng gói datagram và kích thước của IP-MTU.

Khi TCP/IP gửi dữ liệu thông qua một mạng ATM, nó chuyển tòan bộ dữ liệu để bằng cách dùng AAL-5. Mặc dầu AAL-5 có thể nhập và chuyển giao các gói chứa tối đa 65 kbyte, các chuẩn TCP/IP xác định một MTU ngầm định là 9180 bytes. IP phải chia nhỏ một datagram bất kỳ lớn hơn 9180 bytes trước khi chuyển nó cho AAL-5.

2.4. Kiểu gói và ghép kênh:

Trong trailer của AAL-5 không có trường kiểu vì vậy một khung AAL-5 không có tính tự nhận dạng. Có hai trường hợp có thể xảy ra:

- Hai máy tính ở các đầu cuối của một mạch ảo chấp nhận rằng mạch được sử dụng với một giao thức nhất định (nghĩa là mạch chỉ dùng để gửi các datagram IP).

- Hai máy tính ở các đầu cuối của một mạch ảo chấp nhận một số byte của vùng dữ liệu sẽ được dành cho trường kiểu.

Như vậy trong trường hợp đầu có:

- *ưu điểm*: Không cần thêm thông tin vào gói.

- *Nhược điểm:* Có thể tạo ra nhiều mạch ảo giữa hai máy tính cùng gửi một gói giữa hai máy tính, làm tăng chi phí không cần thiết.

Trường hợp sau: Hai máy tính sử dụng một mạch ảo duy nhất cho các giao thức khác nhau.

- *ưu điểm*: Tòan bộ lưu lượng đi trên cùng một mạch ảo

- *Nhược điểm*: Gói phải dành một số byte cho nhận dạng kiểu giao thức. Các gói theo các giao thức khác nhau phải chọn chung một khỏang trễ và một thông tin tiền định.

Các chuẩn TCP/IP định rằng các máy tính có thể chọn giữa hai phương pháp sử dụng AAL-5. Với các chuẩn thường được chọn kèm theo cấu hình khai thác, và phổ biến nhất là IEEE 802.2, xác định một header điều khiển đường logic *LLC* (Logic Link Control) kèm theo header điểm gắn mạng con *SNAP* (Sub Network Altachment Point). Hình 20 mô tả thông tin LLC/SNAP thêm vào datagram trước khi gởi cho mạch ảo ATM.

0 16

31

LLC (AA.AA 03)	OUI_1 (00)
OUI_2 (00.00)	TYPE (08.00)
IP DATA GRAM	
...	

Hình 7.8: Định dạng gói được dùng để gởi 1 datagram IP dưới ATM khi đa giao thức ghép kênh trong một mạch ảo đơn.

Trong đó:

LLC gồm 3 byte: chứa số hexa AA.AA.03

SNAP gồm 5 byte: trong đó 3 byte chứa số nhận dạng đơn nhất có tổ chức (Organizationally Unique Identifier) (OUI). OUI là 00-00-00 thì xác định các chuẩn Ethernet.

Phần còn lại 2 byte là trường *TYPE*, với 08.00 quy định cho mạch đóng gói IP theo khung Ethernet.

Như vậy: Phần mềm gởi phải gói thêm header *LLC*/*SNAP* và gói trước khi gửi và phần mềm nhận phải kiểm tra header để xác định cách thao tác gói.

3. Đánh địa chỉ IP trong mạng ATM.

Giống như các kỹ thuật mạng khác, ATM gán cho mỗi máy tính một địa chỉ vật lý để có thể sử dụng khi thiết lập một mạch ảo. Mặt khác, do một địa chỉ vật lý thường lớn hơn địa chỉ IP, nên một địa chỉ vật lý ATM không thể mã hóa trong một địa chỉ IP. Như vậy IP không thể sử dụng ARP để đánh địa chỉ trên các mạng ATM.

Các mạch ảo cố định ATM kết hợp luôn đánh địa chỉ. Do bộ phận quản lý đặt cấu hình mỗi mạch ảo cố định một cách tùy ý, nên máy chủ chỉ biết cặp VPI/VCI của mạch. Phần mềm trên máy chủ không thể biết địa chỉ IP hoặc địa chỉ phần cứng ATM của điểm cuối điều khiển từ xa. Như vậy cơ chế đánh địa chỉ IP phải cung cấp nhận dạng về một máy tính điều khiển từ xa thêm một mạch ảo cố định PVC cũng như việc tạo lập động của các mạch ảo được chuyển mạch SVC để biết được địa chỉ đích.

Các kỹ thuật định hướng kết nối theo chuyển mạch kết hợp luôn việc đánh địa chỉ bởi vì chúng đòi hỏi hai mức đánh địa chỉ:

Đầu tiên khi tạo lập một mạch ảo để gửi các datagram, địa chỉ IP của đích phải được ánh xạ thành một địa chỉ điểm cuối ATM. Địa chỉ điểm cuối được sử dụng để thiết lập một mạch ảo.

Thứ hai khi gửi datagram đến một máy tính được điều khiển từ xa trên một mạch ảo đang tồn tại, địa chỉ IP của đích phải được ánh xạ thành cặp VPI/VCI đối với mạch. Mức đánh địa chỉ thứ hai này được sử dụng mỗi khi một datagram được gửi trên một mạng ATM; mức thứ nhất chỉ cần thiết khi máy chủ tạo lập một SVC.

4. Quản lý kết nối :

4.1 Khái niệm về mạng con IP LOGIC (LIS: Logic IP Subnet):

TCP/IP cho phép một số máy tính gắn vào mạng ATM để vận hành như một mạng LAN độc lập. Một nhóm như vậy được gọi là LIS (Logical IP Subnet).

Các máy tính trong một LIS có thể liên lạc trực tiếp với một máy tính khác trong cùng một LIS, nhưng khi liên lạc với một máy tính ở một LIS khác thì cần phải sử dụng router.

4.2. Qủan lý kết nối:

Các máy chủ phải quản lý các mạch ảo cẩn thận vì việc thiết lập mạch mất nhiều thời gian và đối với các dịch vụ ATM thương mại, có thể làm tăng giá thành. Như vậy, nếu cứ tiếp nhận đơn giản theo trình tự thiết lập mạch, gửi một datagram, và sau đó đóng mạch thì quá đắt. Thay vì làm như vậy, một máy chủ phải duy trì một bản ghi về các mạch được mở để có thể sử dụng lại.

Việc quản lý mạch xuất hiện trong phần mềm giao tiếp mạng dưới IP. Khi một máy chủ cần gửi một datagram, nó sử dụng IP để định tuyến tìm đến địa chỉ nhảy tiếp theo N + 1 và thông qua nó đưa datagram đến giao tiếp mạng. Giao tiếp mạng kiểm tra bảng các mạch ảo đã mở đến N, máy chủ sử dụng AAL-5 để gửi datagram. Nếu không máy chủ phải định vị một máy tính với địa chỉ N, tạo lập mạch và bổ sung vào bảng trước khi gửi datagram.

Khái niệm về các mạng con IP Logical ràng buộc việc định tuyến IP. Trong một bảng định tuyến, địa chỉ nhảy tiếp theo đối với một đích phải là một máy tính nằm trong cùng một mạng con Logic với máy gởi. Lưu ý rằng mỗi LIS được thiết kế để vận hành như một mạng LAN. Sự ràng buộc đối với máy chủ nối với một mạng LAN cũng

giống như vậy, lúc đó mỗi địa chỉ nhảy tiếp theo trong bảng định tuyến phải là một router nối đến mạng LAN.

Đó là một trong những lý do để phân chia các máy tính với các mạng con logic sinh ra từ các ràng buộc về phần cứng và phần mềm. Một máy chủ không thể duy trì một lượng lớn các mạch ảo mở cùng một lúc bởi vì một mạch ảo đòi hỏi các tài nguyên trong phần cứng ATM và hệ điều hành. Việc phân chia các máy tính thành các mạng con logic để hạn chế số lượng tối đa các mạch được mở đồng thời đến các máy tính trong LIS.

5. Mối quan hệ giữa địa chỉ host ATM đến địa chỉ IP của host

5.1. Đánh địa chỉ trong một LIS:

Khi một máy chủ tạo một mạch ảo đến một máy tính trong LIS của nó, máy chủ phải xác định địa chỉ phần cứng ATM đích. Lúc đó máy chủ không thể phát quãng bá một yêu cầu đến tất cả các máy tính trong LIS bởi vì ATM không cho phép quảng bá phần cứng mà nó phải liên hệ với Server để lấy bản đồ (địa chỉ). *Việc truyền thông giữa máy chủ và Server* sử dụng *ATMARP*.

Với ARP, người gửi lập nên một yêu cầu bao gồm IP của người gửi, các địa chỉ phần cứng ATM cũng như địa chỉ IP của nơi nhận để theo đó xác định địa chỉ phần cứng ATM cần thiết. Sau đó người gửi chuyển yêu cầu cho Server ATMARP của mạng con logic. Nếu Sevrer biết địa chỉ phần cứng ATM, nó gởi một phúc đáp ATMARP. Ngược lại Server sẽ gửi phúc đáp âm ATMARP.

5.2. Khuôn dạng gói ATMARP:

Khuôn dạng gói ATMARP có sửa đổi chút ít so với khuôn dạng gói ARP. Sự thay đổi chính nằm ở chỗ các *trường độ dài địa chỉ* được thêm vào để kết hợp với các địa chỉ ATM. Các công ty điện thoại cho phép các mạng ATM công cộng sử dụng một khuôn dạng 8 bytes, trong đó mỗi địa chỉ là một số điện thoại ISDN được xác định theo công bố chuẩn ITU-TS, số E.164. Ngược lại, diễn đàn (Forum) ATM cho phép mỗi máy tính gắn với một mạng ATM công cộng được gán một địa chỉ 20 bytes NSAP (Network Service Aceess Point). Như vậy, một địa chỉ tuần tự hai mức có thể cần để xác định một địa chỉ E.164 cho phía điều khiển từ xa và một địa chỉ NSAP của một máy chủ trên một chuyển mạch cục bộ ở phía này.

Để kết hợp các khuôn dạng đa địa chỉ và hai mức tuần tự, một gói ATMARP chứa hai trường độ dài dành cho mỗi địa chỉ ATM, cũng như một trường độ dài cho mỗi địa chỉ giao thức.

0 8 16 24 31

Hardware Type (0 × 0013)		Protocol Type (0 × 0800)	
Send. Hlen (20)	Send. Hlen 2 (0)	Operation	
Send. Plen (4)	Tar. Hlen (20)	Tar. Hlen 2 (0)	Tar. Plen (4)
Sender's ATM Address (bytes 0-3)			

Sender's ATM Address (bytes 4-7)
Sender's ATM Address (bytes 8-11)
Sender's ATM Address (bytes 12-15)
Sender's ATM Address (bytes 16-19)
Sender's Protocol Address
Target's ATM Address (bytes 0-3)
Target's ATM Address (bytes 4-7)
Target's ATM Address (bytes 8-11)
Target's ATM Address (bytes 12-15)
Target's ATM Address (bytes 16-19)
Target's Protocol Address

Hình 7.9 : Định dạng gói ATMARP khi dùng 20 byte địa chỉ ATM

Hình 7.9 minh họa một gói ATMARP bắt đầu với các trường kích thước cố định chỉ các độ dài địa chỉ. Hai trường đầu tiên có khuôn dạng như ARP thông thường. Trường có tên HARDWARE TYPE chứa giá trị hexa Ox0013 đối với ATM và trường có tên PROTOCOL TYPE chứa giá trị hexa Ox0800 đối với IP.

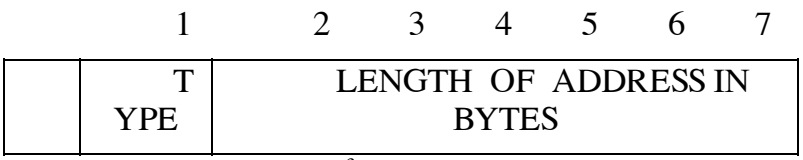
Do *khuôn dạng địa chỉ* người *gửi* và *đích* có thể khác nhau, mỗi địa chỉ ATM yêu cầu một trường độ dài. Trường SEND HLEN xác định độ dài của địa chỉ ATM của người gửi và trường SEND HLEN 2 xác định độ dài của địa chỉ con ATM của người gửi. Các trường TAR HLEN và TAR HLEN 2 xác định các độ dài của địa chỉ ATM của nơi nhận và địa chỉ con. Cuối cùng các trường SEND PLEN và TAR-PLEN xác định các độ dài của các địa chỉ giao thức của nguồn gửi và của đích.

Theo sau các trường độ dài trong header, một gói ATMARP chứa sáu địa chỉ. Ba địa chỉ đầu là địa chỉ ATM, địa chỉ con ATM và địa chỉ giao thức của người gửi. Ba địa chỉ sau gồm địa chỉ ATM, địa chỉ con ATM và địa chỉ giao thức của nơi nhận.

Trong hình 3.23 cả hai trường độ dài địa chỉ con của nơi gửi và nơi nhận đều *bằng 0* và như vậy gói không chứa các byte dành cho các địa chỉ con.

✭ *Khuôn dạng các trường độ dài địa chỉ ATM*.

Do ATMARP được thiết kế để dùng cho các địa chỉ E.164 hoặc các địa chỉ NSAP 20-bytes. Các trường chứa một độ dài địa chỉ bao gồm một bit chỉ thị qui cách địa chỉ. Hình 23 mô tả ATM ARP mã hóa kiểu địa chỉ và độ dài trong một trường 8 bit.



Hình 7.10: mã địa chỉ ATM, kiểu, độ dài trong một trường 8 bit

Bit 1 phân biệt 2 kiểu của các địa chỉ ATM.

Nếu bit 1 bằng không, địa chỉ thuộc về khuôn dạng NASP được khuyến nghị bởi ITU-TS. Do mỗi trường độ dài địa chỉ ATM trong một gói ATM ARP có khuôn dạng như hình 3.24 một gói đơn có thể chứa nhiều kiểu địa chỉ ATM.

✸ Các mã điều hành được sử dụng với giao thức ATM ARP.

Khuôn dạng gói trong hình 23 được sử dụng để yêu cầu một phép đánh địa chỉ, một phúc đáp cho yêu cầu, hoặc yêu cầu một phép đánh địa chỉ ngược lại. Khi một máy tính gửi một gói ATM ARP, nó phải thiết lập trường OPERATION để xác định kiểu đánh địa chỉ. Bảng 18.11 dưới đây thể hiện các giá trị có thể được sử dụng trong trường OPERATION của một gói ATM ARP và ý nghĩa của chúng.

Code	ý nghĩa
1	ATM ARP yêu cầu
2	ATM ARP phúc đáp
8	Yêu cầu ATM ARP ngược
9	Phúc đáp ATM ARP ngược
10	Phúc đáp âm tính ATM ARP

Tóm lại:

ATM là một kỹ thuật mạng tốc độ cao trong đó bao gồm một hoặc nhiều chuyển mạch liên kết với nhau tạo thành một cơ cấu chuyển mạch. Về mặt logic, một cơ cấu chuyển mạch ATM hoạt động như một mạng đơn rất lớn, nó cho phép một máy chủ bất kỳ liên lạc với các máy chủ khác bất kỳ.

Bởi vì ATM là một kỹ thuật định hướng kết nối, hai máy tính phải thiết lập một mạch ảo thông qua mạng trước khi chúng có thể truyền dữ liệu, một máy chủ có thể lựa chọn giữa kiểu cố định hoặc kiểu chuyển mạch của mạch ảo. Các mạch chuyển mạch được thiết lập theo yêu cầu, các mạch cố định đòi hỏi cấu hình thao tác. Trong mọi trường hợp, ATM gán mỗi mạch đã mở với một số nguyên nhận dạng. Mỗi khung mà một máy chủ gửi và mỗi khung mà mạng phân phát chứa một số nhận dạng mạch, một khung không chứa địa chỉ nguồn và địa chỉ đích.

Mặc dù mức thấp nhất của ATM sử dụng các tế bào 53-byte để chuyển giao thông tin. ATM kèm theo các cơ chế phụ trong lớp điều hợp của nó được các ứng dụng sử dụng. Cụ thể là AAL-5 được sử dụng để gửi dữ liệu qua mạng ATM. AAL-5 được đưa ra một giao tiếp để nhận và phân phát các khối dữ liệu có kích thước khác nhau, trong đó mỗi khối có thể lên đến 64 K byte.

Để gởi một datagram IP qua một mạng ATM phải hình thành một mạch ảo kết nối đến đích, sử dụng AAL-5 và gửi datagram cho AAL-5 như một kiểu dữ liệu đơn. AAL-5 cộng thêm một trailer, chia dữ liệu và trailer thành các tế bào để truyền qua mạng và sau đó tái hợp datagram trước khi chuyển nó cho hệ điều hành trên máy đích. Như vậy khi gửi datagram qua ATM IP không phân chia thành kích thước tế bào ATM. Thay vì cách đó IP sử dụng một MTU của 9180 và cho phép AAL-5 để phân đoạn datagram thành các tế bào.

Một mạng con IP logic (LIS) bao gồm một số máy tính sử dụng ATM thay vì một mạng LAN, các máy tính tạo nên các mạch ảo trong đó chính chúng sẽ trao đổi dữ liệu với nhau. Cả hai kiểu mạch ảo chuyển mạch và cố định trong một LIS kết hợp cả vấn đề đánh địa chỉ. Một giao thức ARP có sửa đổi là ATM ARP dùng để đánh địa chỉ cho các máy tính trong LIS đặt trên một Server ATM ARP để chuyển địa chỉ IP của máy tính khác trong LIS thành một địa chỉ ATM tương ứng. Mỗi máy tính trong LIS phải đăng ký với Server bằng cách cung cấp địa chỉ IP và địa chỉ ATM của nó cho Server. Các máy tính khác có thể tiếp xúc với Server để nhận lấy địa chỉ cần thiết. Giống như ARP thông thường cách đánh địa chỉ thu được từ ATM ARP có tính cấp thời. Sau một khỏang thời gian xác định, việc đánh địa chỉ phải cập nhật giá trị trở lại hoặc bỏ đi. Một giao thức liên quan là ATM ARP ngược, được sử dụng để khám phá các địa chỉ ATM và địa chỉ IP của một máy tính điều khiển từ xa được nối bởi một mạch ảo cố định.

CHƯƠNG 8

MẠNG DỊCH VỤ TÍCH HỢP SỐ

Các mạng truyền thông hiện nay đòi hỏi phải có khả năng đồng thời truyền được nhiều dạng thông tin khác nhau như tiếng nói, hình ảnh, dữ liệu, fax, thông tin điều khiển từ xa ..Tập hợp các dịch vụ để truyền các loại thông tin khác nhau đó đòi hỏi phải được phân tán đến tận văn phòng hoặc nhà riêng của người sử dụng. Khả năng đó sẽ phá vỡ tính độc quyền truyền thông của các hãng hoặc tổ chức chính phủ, mỗi nhà sẽ có thể được gắn một hộp liên kết đặt ở một nút của đường truyền dữ liệu cao tốc nối với mạng điện thoại số, điện thoại truyền hình hoặc môt dịch vụ giá trị gia tăng khác .

Một mạng có khả năng đáp ứng các yêu cầu đa dạng như vậy được đặt tên là "Mạng dịch vụ tích hợp số (Intergrated Services Digital Network: ISDN). CCITT đã định nghĩa ISDN như một mạng hoàn toàn số hóa có khả năng cung cấp một phạm vi rộng rãi các dịch vụ thoại và phi thoại truy nhập bởi một tập các giao diện người sử dụng. Như vậy, ở dạng đơn giản nhất thì ISDN đơn thuần là sự nâng cấp đường điện thoại nội hạt cho phép truyền cả tiếng nói và sốù liệu trên cùng một đôi dây. Còn ở dạng mong muốn thì ISDN là một mạng có thể cung cấp thuận tiện cho người sử dụng vô số các dịch vụ viễn thông đa phương tiện ,bao gồm tiếng nói , số liệu, âm thanh nổi, hình ảnh , truyền hình ..nhờ các hệ thống chuyển mạch số hiện đại .

Trên thực tê , ISDN không phải là một cuộc cách mạng về công nghệ thông tin , bởi công ty ở Mỹ và các nước phát triển sử dụng từ gần 30 năm qua. Và việc số hóa cung cấp nhiều dịch vụ là phù hợp với sự phát triển của viễn thông ngày nay. Tuy nhiên tính chất cách mạng lại xuất hiện ở khía cạnh phục vụ khách hàng, tạo một quan hệ rất thân thiện giữa đông đảo người sử dụng với các dịch vụ thông tin đa năng, phù hợp với nhu cầu trao đổi thông tin ngày một cao của xã hội phát triển .

I. KHÁI NIỆM KÊNH TRONG ISDN:

"KêNH " là đường truyền dẫn giữa thông tin người sử dụng và mạng, được gọi là kênh thuê bao. Trong ISDN kênh thuê bao chỉ truyền các tín hiệu số và được chia thành 3 loại kênh cơ bản khác nhau là : kênh D, kênh B, kênh H.

Kênh D: để truyền các thông báo, báo hiệu giữa người sử dụng và mạng. Vì khối lượng trao đổi các thông báo báo hiệu có thể không sử dụng hết độ rộng băng tần dùng cho kênh nên có thể dùng kênh D để truyền các gói tin của người sử dụng. Kênh D hoạt động với tốc độ 16kb/s hoặc 64kb/s phụ thuộc vào giao diện người sử dụng .

Kênh B : để truyền các tín hiệu tiếng nói, âm thanh, số liệu và hình ảnh (video) của người sử dụng. Kênh B có thể sử dụng cho cả chuyển mạch kênh lẫn chuyển mạch gói. Kênh B hoạt động ở tốc độ 64kb/s.

Kênh H: truyền thông tin với tốc độ cao hơn gồm có các loại như sau:

Kênh H0 tương đương 6 kênh B, tốc độ 384Kb/s

Kênh H1 có 2 mức :

- H11= 4H0 = 24B, có tôcỳ độ 1,536Mb/s
- H22 có tốc độ từ 43 - 45 Mb/s

Kênh H4 có tốc độ từ 132_- 138,24Mb/s

II. CÁC GIAO DIỆN VÀO ISDN:

Mục tiêu của ISDN là cung cấp tất cả các dịch vụ trên một giao diện truy nhập vào mạng duy nhất, không phụ thuộc vào loại thiết bị hoặc loại dịch vụ. Các tiêu chuẩn ISDN hiện nay định nghĩa 2 giao diện vào ISDN, đó là giao diện tốc độ cơ bản (Basic Rate Interface: BRI) và giao diện tốc độ cơ sở (PRI).

Mô hình phân bố các khuyến nghị loại I về ISDN của CCITT

Giao diện	Cấu trúc kênh	Tốc độ tổng cộng	Tốc độ dữ liệu người sử dụng
BRI	2B+D16	192 Kb/s	144kb/s
PRI	23B+D64 30B+D64	1,544Mb/s 2,048Mb/s	1,536Mb/s 1,984Mb/s

Giao diện BRI có cấu trúc kênh là 2B+D, trong đó kênh D luôn hoạt động với tốc độ 16kb/s. BRI thường sử dụng để cung cấp lối vào giữa thiết bị người sử dụng và tổng đài trung tâm ISDN. Tốc độ dữ liệu người sử dụng đối với BRI là 144kb/s, mặc dù các thông báo báo hiệu bổ sung yêu cầu BRI hoạt động ở tốc độ tổng cộng là 192kb/s.

Giao diện PRI có 2 cấu trúc kênh : 23B+D dùng cho Bắc Mỹ và 30B+D dùng cho Tây âu

Trong cả 2 trường hợp, kênh D đều hoạt động ở tốc độ 64kb/s. PRI chứa nhiều kênh, cho phép cung cấp lối vào cho nhiều loại thiết bị của người sử dụng .

3.Các thiết bị chức năng và điểm chuẩn của ISDN:

Để đặc tả các giao diện truy nhập ISDN của người sử dụng, các tiêu chuẩn ISDN đưa vào 2 khái niệm :

_Các nhóm chức năng(functional groups)

Các điểm tham chiếu (reference_points)

Nhóm các chức năng là một tập hợp các chức năng nhất định được thực hiện bởi các phần tử vật lý của người sử dụng, còn các điểm tham chiếu là khái niệm dùng để phân tách các nhóm chức năng khác nhau.

4.Chuẩn hóa ISDN:

CCITT là tổ chức chịu trách nhiệm chuẩn hóa ISDN với các khuyến nghị loại I. Các tổ chức tiêu chuẩn hóa khác như ANSI, ISO,.. cũng tham gia bổ sung các chuẩn cho ISDN. Vidụ: ANSI với họ chuẩn T1E1 về các giao diện mạng và họ chuẩn T1M1 về các hoạt động nội bộ mạng ,quản lý ,..

III. CÁC DỊCH VỤ ISDN:

ISDN với các khả năng chuyển mạch khác nhau có thể cung cấp rất nhiều dịch vụ thông tin cho khách hàng theo mô hình công sở hoặc mô hình nhà riêng

1. Các nhu cầu dịch vụ:

ISDN cần phải có nhiều khả năng để có thể điều chỉnh các dịch vụ mong đợi khác nhau của nó mà một số trong mạng hiện nay chưa sử dụng. Mạng có khả năng để:

a.Phân phối độ rộng băng tần trên cơ sở nhu cầu

b.Cho phép thiết lập và chấm dứt cuộc gọi nhanh

c. Điều khiển một khoảng rộng các tốc độ truyền dẫn và thời gian chiếm giữ cuộc gọi.

d. Đảm bảo các tỉ lệ lỗi bít thấp, giảm nhỏ thời gian trễ thông tin. Cung cấp các mức độ an toàn thông tin khác nhau.

Các nhu cầu liên kết ở trên hầu hết phù hợp với khả năng của ISDN cung cấp một tập lớn các dịch vụ số. Tất cả các dịch có thể được cung cấp từ một mạng ISDN duy nhất

Dịch vụ ISDN có tầm quan trọng là quản lý các cuộc gọi vào .

2. Các dịch vụ và các thuộc tính của ISDN

Các dịch vụ ISDN được phân loại dựa vào mục tiêu của chúng và nguồn dịch vụ .

thuộc tính truy nhập

thuộc tính truyền đạt tin,

phạm vi các dịch truyền tin

phạm vi hoạt động của dịch vụ từ xa

Các dịch vụ từ xa và dịch vụ bổ sung giá trị cho mạng cung cấp, nó có thể cung cấp liên lạc từ đầu cuối đến đầu cuối. Các dịch vụ truyền tin không cải biến dạng tin do ISDN tạo ra được mô tả trong các loại khuyến nghị I.210 và I.230. Chúng được định nghĩa :

-Thuộc tính lối vào là các đặc tính mô tả các chức năng và phương của người sử dụng mạng như thế nào.

-Các thuộc tính truyền đạt tin là các đặc trưng gắn với truyền đạt tin qua mạng .

-Các thuộc tính tổng quát mô tả các đặt trưng khác của dịch vụ như các tham số về chất của dịch vụ và các quá trình liên kết mạng nội tại.

3. Các dịch vụ ISDN khác:

3.1.Phối hợp tốc độ:

Các khuyến nghị I.460 của CCITT mô tả các thuật toán phối hợp tốc độ chuẩn bằng cách sử dụng một bộ phối hợp tốc độ đầu cuối để đưa các dòng bít hoạt động ở một tốc độ truyền dẫn chung bất kỳ vào kênh B_64kbps.

Khuyến nghị I.460 của CCITT mô tả nguyên lý chung của việc phối hợp tốc độ và ghép trợ giúp các giao diện người sử dụng mạng hiện có của khuyến nghị X.21 và X.21bis trên ISDN. Khuyến nghị X.31 mô tả trợ giúp các thiết bị số liệu đầu cuối X.25 trên ISDN. Sự phối hợp trong khuyến nghị này có thể dùng cho ứng dụng phương thức mạch gói và ghép , phát hiện lỗi và sữa lỗi như X.25.

3.2 Các dịch vụ băng rộng

Các dịch vụ băng rộng (B-ISDN) các dịch vụ yêu cầu tốc độ lớn hơn so với tốc độ đi ra từ một trung kế giao diện sơ cấp các khuyến nghị CCITT chưa xác định đầy đủ các dịch vụ B-ISDN. Các dịch vụ B-ISDN gồm dịch vụ điện thoại hình ,video và các dịch vụ tìm tài liệu ,truyền hình có độ phân giải cao (HDTV)

Các dịch vụ B-ISDN là các dịch vụ liên kết hoặc các dịch vụ phân bố. Các dịch vụ liên lạc gồm: dịch vụ mạng điện thoại, các dịch vụ đàm thoại và tìm kiếm. Các dịch vụ phân bố có thể hoạt động hoặc không hoạt động dưới sự điều khiển của người sử dụng.

3.3.Các kịch bản lấy mẫu:

Các dịch vụ truyền tin không biến đổi dạng tin của ISDN cho phép độ linh hoạt ở các dịch vụ. Thiết bị ISDN báo hiệu cho mạng thiết lập một cuộc gọi bằng cách xác định dạng thuộc tính đối với dịch vụ mong muốn .

Các loại dịch vụ truyền tin không biến đổi dạng tin:

a.64kbps không hạn chế ,tính trung thực 8khz phụ trợ truyền đạt UDI để trợ giúp các ứng dụng của người dùng khác nhau

b.Truyền đạt tiếng nói, độ trung thực 8khz, 64kbps

c.Truyền đạt tin audio 3.1khz , độ trung thực 8khz , 64kbps

d.Tiếng nói luân phiên và 64kbps không hạn chế , độ trung thực 8khz

e. 128kbps không hạn chế ,độ trung thực 8khz

f. 384kbps không hạn chế ,độ trung thực 8khz

g.1536kbps không hạn chế ,độ trung thực 8khz

h.1920kbps không hạn chế ,độ trung thực 8khz

Các dịch vụ truyền tin không biến đổi dạng tin phương thức gói này:

-cuộc gọi ảo và mạch ảo cố định .

-dịch vụ truyền tin không biến đổi dạng tin phương thức gói không kết nối

-dịch vụ truyền tin có báo hiệu cho người sử dụng .

Tóm lại: Sự phân biệt thuộc tính truyền đạt tin và thuộc tính lối vào là quan trọng. Nếu yêu cầu của dịch vụ đòi hỏi kênh B và kênh H, thì liên lạc giữa người dùng đến người dùng sẽ đảm bảo trên kênh đạt yêu cầu ISDN phải biết làm thế nào để nghi nhận cuộc gọi vào. Nếu cuộc goi vào có các thuộc tính phù hợp với ứng dụng số liệu thì máy tính lưu ý đến cuộc nối, còn các điện thoại vẫn nằm im không hoạt động.

IV. CÁC GIAO THỨC CỦA LỚP VẬT LÝ ISDN:

1.Cấu trúc giao thức ISDN:

Các giao thức ISDN đối với kênh D tương đương với ba lớp thấp của mô hình chuẩn OSI

a. Lớp 1:mô tả cuộc nối vật lý giữa thiết bị đầu cuối(TE) và thiết bị đầu cuối mạng(NT)

b. Lớp 2: mô tả các thủ tục để đảm bảo không có lỗi qua kênh vật lý và xác định cuộc nối logic giữa người sử dụng và mạng.

c. Lớp 3: xác định giao diện người sử dụng và mạng, các thông tin về báo hiệu được sử dụng để giữ các yêu cầu dịch vụ từ mạng.

2. Giao thức tốc độ cơ bản

Khuyến nghị I.430 xác định cuộc liên lạc ISDN giữa thiết bị đầu cuối và thiết bị đầu cuối mạng ngang qua điểm chuẩn S/T

Lối vào tốc độ cơ bản có thể sử dụng đến cấu hình điểm đến điểm hoặc điểm đến đa điểm. Có 2 cách lựa chọn điểm đến đa điểm :

a. Khi chọn bus thụ động ngắn thì có thể nối 8 TE đến một NT duy nhất trên một bus có khoảng cách 500ft(150m).

b. Khi chọn bus thụ động mở rộng, nhiều TE được nhóm lại với nhau ở đầu cuối bus, cách NT đến 3300ft

Bộ nối vật lý đối với BRI là loại 8 chân(RJ-45)

Việc truyền dẫn trên BRI được sắp thành các khối bit gọi là các khung I.430, mỗi khung có 48 bit..

Trong cấu hình điểm đến đa điểm việc các TE nối đến bus thụ động có 2 điểm :

a. Tất cả các TE trên bus tuân theo các luật tạo khung.

b. Các TE được nối tiếp đến bus trong dạng song song thích hợp hơn dạng nối tiếp .

Khuyến nghị I.430 xác định 5 mẫu tin khác nhau gọi là các tín hiệu INFO biểu thị trạng thái của tuyến vật lý BRI

- INFO 0: không có tín hiệu đường dây, có thể gửi NT hoặc TE

- INFO 1: tín hiệu liên tục với tốc độ 192kbps,theo hướng NT đến TE

- INFO 2:KHUNG I.430, các bit B, D, E và A là tập 0 và tất cả các bit khác là tập tương ứng tạo khung thích hợp,theo hướng NT,TE.

- INFO 3:khung I.430 có số kiệu hoạt động trên các kênh B và D, gửi theo hướng TE đến NT

- INFO 4: khung I.430 hoạt động trên kênh B, D, gửi theo hướng NT đến TE

→ Mào đầu

Tóm lại: BRI có thể sử dụng trong 2 chế độ tổng quát là: cung cấp dịch vụ ISDN từ PBX hoặc từ bộ ghép kênh ISDN đến cơ quan riêng

BRI sử dụng để tăng cấp bằng cách ấn định 2 số điện thoại khác nhau cho một đường BRI và bố trí mỗi kênh B cho một sô, một BRI duy nhất có thể cung cấp dịch vụ 1B-D cho 2 cơ quan khác nhau .

3.Giao tiếp tốc độ sơ cấp

Khuyến nghị I.430 _CCITT xác định giao thức lớp vật lý cho giao diện tốc độ sơ cấp. PRI có cấu hình song song, điểm nối điểm, nối tiếp, đồng bộ bằng cách sử dụng 2 kênh vật lý. Khuyến nghị I.430 cung cấp tốc độ số liệu 1,544 Mbps và 2,048Mbps.

3.1.Giao tiếp 1,544 Mbps

PRI 1,544Mbps ghép 24 kênh 24kbps. Một khung PRI gồm một bit tạo khung và một mẫu đơn 8 bit từ 1 trong 24 kênh, tổng cộng 193 bit trên mỗi khung. Số liệu người dùng là 1,536 Mbps.

PRI 1,544Mbps dùng để báo hiệu biến đổi dấu xen kẽ (AMI).Với mã AMI, các bit 0 được biếu thị không có điện áp trên đường dây và các bit 1 biểu thị các xung điện áp có cực tính xen kẽ .

3.2Giao tiếp 2,048Mbps

Giao tiếp tốc độ sơ cấp 2,048 Mbps dựa vào khuyến nghị CEPT E1 đã được cộng PRI 2,048 ghép 32 kênh 64 kbps.

Một khung trong PRI 2.048 Mbps chứa một mẫu 8 bit duy nhất cho khe hở thời gian.Với 8000 khung/s ,tốc độ số liệu tổng cộng là 2,048 Mbps và số liệu người dùng là 1,984 Mbps .

PRI 2,048Mbps sử dụng tín hiệu số 3 zero lưỡng cực mật độ cao (H0B3)

3.3Phụ trợ PRI của các kênh H

Theo khuyến nghị I.430 .PRI _1,544 Mbps có thể phụ trợ 3 kênh H0, khi không có kênh D. PRI 2,048 Mbps phụ trợ 5 kênh H0 cho kênh D dựa vào.

V. GIAO THỨC LỚP 3 CỦA KÊNH D:

1.Báo hiệu người dùng và mạng lớp 3:

Thuật ngữ người dùng và mạng nói lên việc các thủ tục này được sử dụng ngang qua giao diện giữa đầu cuối ISDN của người dùng và mạng phục vụ.

Các thủ tục giao tiếp của người sử dụng và mạng chỉ tồn tại qua giao tiếp cục bộ giữa người dùng ISDN và mạng phục vụ, đươcỹ sử dụng giữa các nút chuyển mạch trong mạng và không mở rộng ngang qua mạng .

Các thủ tục báo hiệu là các thủ tục được thiết bị đầu cuối người sử dụng báo hiệu đi lại giữa chúng. Các tin tức được tạo nên bởi một header và một dãy các phần tử thông tin .

Header cần thiết cho mọi tin tức. Chúng là bộ phân biệt giao thức để nhận mạng giao thức thuộc về loại tin nào , giá trị chuẩn cuộc gọi (CRV) để nhận dạng cuộc gọi xãc định mà tin tức gắn vào và để nhận dạng tin tức trong số 33 loại tin .

2.Các cuộc gọi phương thức mạng cơ bản:

Cuộc gọi phương thức mạng là cuộc gọi trong đó toàn bộ kênh truyền tin không biến đổi, giành cho người dùng trong khoảng thời gian gọi .

2.1Nối cuộc gọi

Phía gọi bắt đầu gửi tin tức SETUP đến mạng. Trong thông báo SETUP người dùng gửi mạng thông tin bằng mạng cần nối cuộc gọi.Những thông tin như vậy là khả năng truyền tin không biến đổi yêu cầu , nhận dạng bên bị gọi và kênh B mà thiết bị đầu cuối người dùng đề nghị được sử dụng cho cuộc gọi này. Khi kết thúc cuộc gọi , mạng gửi một thông báo SETUP đến phía bị gọi.Thông báo này không giống với thông báo mà bên gọi đã gửi đến mạng, nó ghép nhau cùng một đường và gồm nhiều thông tin giống nhau. Các giá trị khác nhau trong thông báo SETUP kết thúc và xuất phát sẽ bao gồm giá trị chuẩn bị của cuộc gọi .

Sau khi thu được một chỉ thị phía họ gọi cảnh tỉnh, mạng tạo ra thông báo cảnh tỉnh và gửi đến thiết bị đầu cuối của phía bị gọi. Khi thiết bị đầu cuối phía bị gọi chấp nhận cuộc gọi, thì nó gửi thông báo CONNECT cho mạng, khi mạng thu được thông báo CONNECT nó dừng các bộ định thời của nó, hoàn chỉnh đường chuyển mạch đến kênh truyền tin không biến đổi, gửi thông báo CONNECT ACKNOWLEDGE đến phía bị gọi và bắt đầu các thủ tục gọi .

2.2 Ngắt cuộc gọi

Bắt đầu từ phía gửi thông báo ngắt DISCONNECT đến mạng và tự ngắt ra khỏi kênh B. Mạng gửi trở lại thông báo RELEASE đến phía khởi đầu ngắt. Đầu cuối nhận tin tức RELEASE COMPLETE.

2.3 L ối vào kênh B đối với dịch vụ mạch ảo ISDN:

Lối vào kênh B đối với bộ điều khiển gói ISDN là một kỹ thuật mà các thuê bao dùng để thiết lập một cuộc nối lối vào qua kênh B trực tiếp đến dịch vụ mạch ảo X.25. Các thủ tục báo hiệu không tác động mạnh đối với bất kỳ hạn chế nào về vị trí của bộ điều khiển này, nhưng bình thường nó là một bộ phận đối với ISDN.

3.3 Lối vào kênh D đối với dịch vụ mạch ảo ISDN

Lối vào kênh D đối với dịch vụ mạch ảo ISDN là một kỹ thuật thứ 2 cho phép người dùng thiết lập trực tiếp các cuộc nối lối vào khả năng chuyển mạch gói X.25 của ISDN.Với kỹ thuật này, thuê bao đơn giản gói X.25 trong khung thông tin LAPD ,đặt bộ nhận dạng của điểm nối lối vào dịch vụ (SAPI) đến 16, và gửi khung đến mạng qua kênh D.

VI. HỆ THỐNG BÁO HIỆU SỐ 7:

1.Các hệ thống báo hiệu của mạng :

1.1 Báo hiệu kênh chung:

Báo hiệu kênh chung được đưa vào mạng điện thoại US. Mạng CCS được thiết kế để chuyển thông tin báo hiệu giữa các trạm chuyển mạch trang bị vi xử lý. Mạng CCS có thể kiểm tra tất cả các phần của tuyến của một cuộc gọi để xác định nếu các cuộc gọi là khả dụng, mạng báo hiệu có thể định vị tất cả các nguồn lực cần thiết. Dùng mạng CCS thì thời gian trung bình để thiết lập một cuộc gọi là 3->7s. ở phía sau mạng là các tín hiệu của mạng được truyền trên một kênh riêng so với các tín hiệu tiếng nói của người dùng trên các trung kế giữa trạm .

1.2 Các phương thức báo hiệu CCS:

Trong phương thức báo hiệu liên kết, các thông báo hiệu liên quan đến một thông tin đã cho truyền giữa 2 điểm báo hiệu được truyền trên một trung kế báo hiệu nối trực tiếp giữa 2 điểm báo hiệu .

1.3 Báo hiệu giữa các trạm kênh chung:

Hệ thống báo hiệu CCITT là một phương án quốc tế của mạng CCS được sử dụng khắp nơi trên thế giới . Khi quay số, mạng CCS có thể hỏi cơ sở dữ liệu trung tâm của mạng, dịch chuyển số điện thoại 10 số chuẩn , chọn giữa các tổng đài, xác định tuyến khả dụng qua mạng và thiết lập cuộc gọi .

1.4.Các phần tử của mạng CCS:

a. Bộ xử lý điều khiển các tổng đài của mạng .

b. Tổng đài gọi là điểm báo hiệu SS7(SP).

c. Điểm truyền đạt báo hiệu (STP) tập trung thông tin báo hiệu từ các điểm báo hiệu.

d. SCP là cơ sở dữ liệu lưu trữ thông tin liên quan đến các dịch vụ của khách hàng.

e. Độ dư là một phần quan trọng của CCS. Nó sẽ làm mất hàng ngàn cuộc gọi, nếu mất một SCP hoặc STP liên kết.

2. Phần điều khiển nối báo hiệu SS7:

Đối với các ứng dụng phi báo hiệu do mạng báo hiệu trợ giúp, thì việc lập địa chỉ là không thích hợp. Mỗi một ứng dụng phi báo hiệu có thể được dự kiến như một phần của người dùng và có thể cung cấp các chức năng định tuyến và phân bố riêng của

nó.Tuy vậy, điều này có thể đưa đến kết qủa là một số ứng dụng có thể thực hiện đầy đủ một số chức năng, ngược hoàn toàn với các khái niệm OSI của các khái niệm đã phân lớp và tính modul.

3. Các tiêu chuẩn của SS7

- Tổng quan SS7; khuyến nghị Q.700
- Tổng quan phần truyền thông báo: Khuyến nghị Q.701
- Tuyến số liệu báo hiệu (mức 1 MTP): khuyến nghị Q.702
- Tuyến báo hiệu (mức 2 MTP) : Q.703
- Mức 3 MTP: khuyến nghih Q.704
- Phần điều khiển nối báo hiệu: Q.716 (ANSI T1.112)
- Phần người dùng điện thoại: Q.721 - Q725
- Các dịch phụ trợ ISDN: khuyến nghị Q.730
- Phần của người dùng số liệu: Q.741
- Phần của người dùng ISDN: Q716 - Q766
- Phần vận hành bảo dưỡng và quản lý: Q.795

VII. CÁC MẠNG THÔNG MINH VÀ SS7:

1. Mạng thông minh (IN):

Thực chất là một mạng cung cấp một tập dịch vụ lớn cho khách hàng và cho phép các mạng điện thoại, số liệu và báo hiệu dễ dàng và nhanh chóng kết hợp chặt chẽ, cách sử dụng logic phân bố.Tuy vậy công nghệ IN/2 và các yêu cầu dịch vụ liên quan đến một số lý do. Một trong lý do đó là các phần tử chức năng mới trong mạng để trợ giúp logic vẫn còn đang phát triển. Các thành tựu chủ yếu được yêu cầu trong các khả năng của phần mềm báo hiệu mạng và phần mềm điều khiển mạng.

2 Mạng SS7:

INWATS cung cấp phương tiện cho phép con người tiến hành cuộc gọi đường dài sẽ được tính cước ngược cho thuê bao 800. Vì thuê bao 800 trả tiền cho các cuộc gọi, họ chọn các người cung cấp đường dài hoặc các đường truyền giữa các tổng đài thích hợp hơn các phía gọi .

Dữ liệu 800 tham gia sau lúc ứng dụng SS7 có thể khắc phục được sự hạn chế của mỗi NXX (mã 3 số). Nó cho phép người sử dụng IEC thuận lợi nhất cho một cuộc gọi đặc biệt dựa trên một số tạp các tham số xác định của người dùng .

Các tổ chức lớn có dịch vụ INWATS,các hệ thống thông tin ,thường sử dụng thiết bị phân số cuộc gọi tự động(ACD) ở vị trí của chúng để định tuyến các cuộc gọi khả dụng cho các đại lý dịch vụ khách hàng.

Cơ sở dữ liệu thông tin đường dây (LIBD) là cơ sở dữ liệu đa mục đích có thông tin về các đường dây thuê bao riêng biệt. Nó cung cấp khả năng như dịch vụ dề vào chương trình xen kẽ để kiểm tra dữ liệu các thẻ gọi điệỷn thoại, bản thông báo để trả tiền điện thoại.

Citywide centre là dịch vụ SS7 nó cung cấp một phương án khác cho các mạng PBX tư nhân.

3. Các dịch vụ báo hiệu phạm vi địa phương của khách hàng:

Các dịch vụ đã được đặt mua có thể đưa đến cho thuê bao công cụ và thuê bao gia đình gọi là dịch vụ báo hiệu phạm vi địa phương của khách hàng (CLASS). Các dịch vụ CLASS khác với SS7 ở chỗ, trong đó sự dự phòng dịch vụ được điều khiển trên cơ sở gọi lần lượt và dựa vào số liệu đã biết ở C.O.

Nhận dạng phía bị gọi cũng được gọi là nhận dạng số tự động (ANI) biểu thị số điện thoại của phía gọi và hoặc danh bạ ở thiết bị điện thoại phía bị gọi trong chu trình rung chuông .Điều này cho phép gọi nên trả lời hay không.

Một số dịch vụ SS7 khi một cuộc gọi vào xuất hiện :

- *Gạt cuộc gọi lựa chọn:* cuộc gọi vào xuất phát từ một số máy bất kỳ thuộc danh sách sẽ tự động hướng đến trạm nơi nhận xác định .

- *Tiến hành cuộc gọi lựa chọn* : cuộc gọi vào xuất phát từ một máy bất kỳ thuộc danh sách tự động hướng đến trạm mới nhận xác định.

- *Chuông đặc biệt* : các cuộc gọi vào mà số máy nằm trong danh sách sẽ bị chặn lại người dùng sẽ không được thông báo cuộc gọi và điệỷn thoại không rung chuông xuất phát từ một số máy thuộc danh sách gây ra một tín hiệu chuông đặc biệt.

- *Chờ gọi quan trọng* : nếu cuộc gọi vào thu được từ một số máy thuộc danh sách trong lúc đường dây của khách bận, sẽ có một tín hiệu chờ đặc biệt gửi đến khách hàng.

4. SS7 và ISDN:

Các dịch vụ mạng trí tuệ đã mô tả ở trên sẽ khả dụng đối với C-O khi đã triển khai rộng rãi SS7. Các dịch vụ này không trực tiếp khả dụng đối với người dùng nếu không có các thủ tục của người dùng và mạng bổ sung. ISDN sẽ cung cấp lối vào người dùng cho các dịch vụ SS7 thêm vào các đặc trưng khác của no .

Sự liên quan giữa tính khả dụng của các dịch vụ CLASS và SS7 là một mối quan hệ tốt trong tương lai của ISDN .

Bất chấp nhiều chuyển mạch C.O được nâng lên bậc cao để phụ trợ SS7 và ISDN, các trạm đó chỉ là các thành phần của ISDN cho đến khi các công ty điện thoại đường dài và nội hạt có sự trợ giúp rộng rãi của SS7.

Tương lai của ISDN và SS7 cần có sự liên kết giữa các chuyển mạch. Đã tiến hành một số kiểm tra một số hoạt động bên trong của chuyển mạch do các thực hiện khác nhau của ISDN và SS7 gây ra đối với các chuyển mạch khác nhau.

Kết luận:

Mạng số liên kết dịch ISDN là mạng sẽ được sử dụng rộng rãi trên toàn thế giới. ISDN là chiến lược để cung cấp cho người sử dụng các thông tin bổ sung, mạng có chi phí rẽ hơn đối với người dùng so với mạng tương tự hiện tại. Hơn nữa về mặt kinh tế nó

sẽ là cuộc thử nghiệm đối với các khách hàng: nhà riêng, công sở, các mạng LAN. Mạng dịch vụ ISDN cần phải hoàn thiện các ứng dụng mới, phần cứng, phần mềm để khách hàng sẵn lòng thuê ISDN.

CHƯƠNG 9:

AN TOÀN VÀ BẢO MẬT THÔNG TIN TRÊN MẠNG MÁY TÍNH

I. CÁC NGUY CƠ ĐE DOẠ HỆ THỐNG VÀ MẠNG MÁY TÍNH

1. Mô tả các nguy cơ

Chúng ta hãy hình dung với một hệ thống thông tin (Mạng LAN, mạng INTRANET. .) đang hoạt động, bỗng đến một ngày nào đó nó bị tê liệt toàn bộ (điều này không phải là không thể xảy ra) bởi một kẻ phá hoại cố tình nào đó; hoặc nhẹ nhàng hơn bạn phát hiện thấy các dữ liệu của mình bị sai lạc một cách cố ý, thậm chí bị mất mát, bị copy.

Xử lý, phân tích, tổng hợp và bảo mật thông tin là hai mặt của một vấn đề không thể tách rời nhau. Ngay từ khi máy tính ra đời, cùng với nó là sự phát triển ngày càng lớn mạnh và đa dạng của các hệ thống xử lý thông tin người ta đã nghĩ ngay đến các giải pháp đảm bảo an toàn cho hệ thống thông tin của mình.

Với một mạng máy tính bạn sẽ có bao nhiêu nguy cơ bị xâm phạm ? Câu trả lời chính xác đó là ở mọi thời điểm, mọi vị trí trong hệ thống đều có khả năng xuất hiện.

Chúng ta phải kiểm soát các vấn đề an toàn mạng theo các mức khác nhau đó là :

- Mức mạng: Ngăn chặn kẻ xâm nhập bất hợp pháp vào hệ thống mạng.

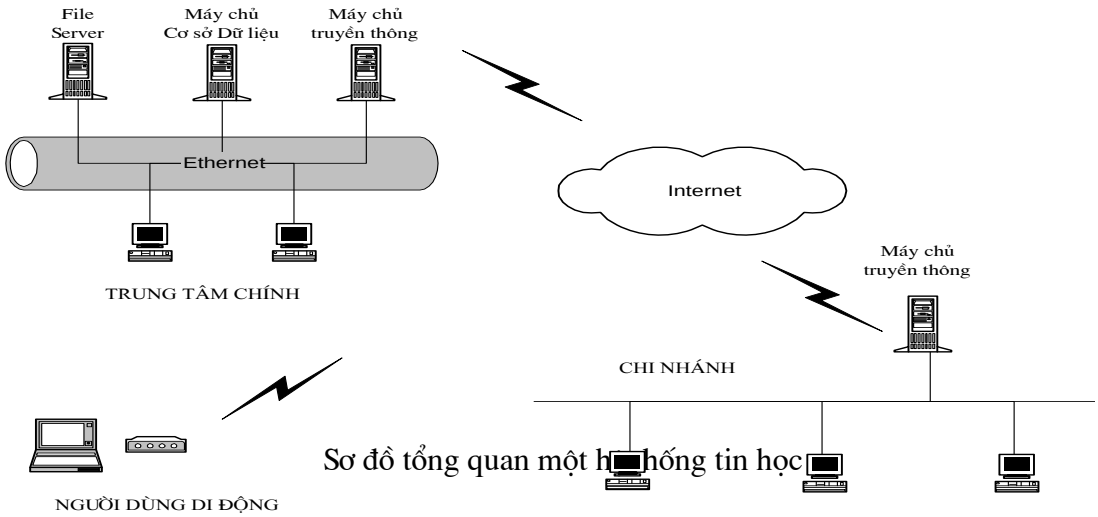
- Mức Server: Kiểm soát quyền truy cập, các cơ chế bảo mật, quá trình nhận dạng người dùng, phân quyền truy cập, cho phép các tác vụ
- Mức CSDL: Kiểm soát ai? được quyền như thế nào ? với mỗi cơ sở dữ liệu.
- Mức trường thông tin: Trong mỗi cơ sở dữ liệu kiểm soát được mỗi trường dữ liệu chứa thông tin khác nhau sẽ cho phép các đối tượng khác nhau có quyền truy cập khác nhau.
- Mức mật mã: Mã hoá toàn bộ file dữ liệu theo một phương pháp nào đó và chỉ cho phép người có " chìa khoá" mới có thể sử dụng được file dữ liệu.

Theo quan điểm hệ thống, một xí nghiệp (đơn vị kinh tế cơ sở) được thiết lập từ ba hệ thống sau:

- ❑ Hệ thống thông tin quản lý.
- ❑ Hệ thống trợ giúp quyết định.
- ❑ Hệ thống các thông tin tác nghiệp.

Trong đó hệ thống thông tin quản lý đóng vai trò trung gian giữa hệ thống trợ giúp quyết định và hệ thống thông tin tác nghiệp với chức năng chủ yếu là thu thập, xử lý và truyền tin.

Trong thời gian gần đây, số vụ xâm nhập trái phép vào các hệ thống thông tin qua mạng Internet và Intranet ngày càng tăng. Có nhiều nguyên nhân dẫn đến việc các mạng bị tấn công nhiều hơn, trong số những nguyên chính có thể kể đến xu hướng chuyển sang môi trường tính toán client/server (khách/chủ), các ứng dụng thương mại điện tử, việc hình thành các mạng Intranet của các công ty với việc ứng dụng công nghệ Internet vào các mạng kiểu này dẫn tới xoá nhoà ranh giới giữa phần bên ngoài (Internet) và phần bên trong (Intranet) của mạng, tạo nên những nguy cơ mới về an toàn thông tin. Cũng cần lưu ý rằng những nguy cơ mất an toàn thông tin không chỉ do tấn công từ bên ngoài mà một phần lớn lại chính là từ nội bộ: nhân viên bất mãn, sai sót của người sử dụng, ý thức bảo mật kém, . . .



Sơ đồ tổng quan một hệ thống tin học

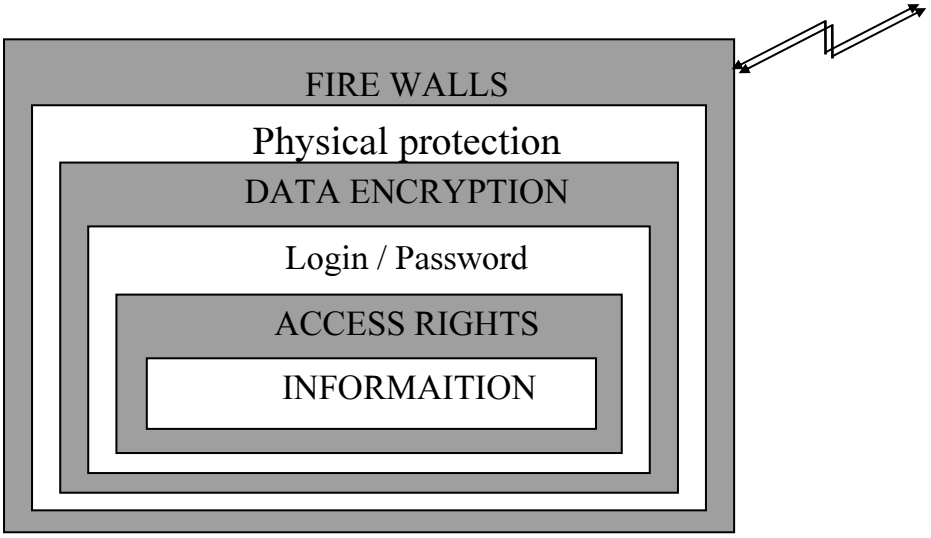
Qua sơ đồ tổng quan một hệ thống tin học ta có thể thấy các vị trí có nguy cơ về an toàn dữ liệu. Các phương pháp tấn công vào hệ thống thông tin của những kẻ phá hoại

(hacker) ngày càng trở nên tinh vi, lợi dụng những điểm yếu cơ bản của môi trường tính toán phân tán. Một số các phương pháp tấn công thường gặp:

- Các thủ thuật quan hệ: Hacker mạo nhận là người trong cơ quan, người phụ trách mạng hoặc nhân viên an ninh để hỏi mật khẩu của người sử dụng. Với những mạng có người sử dụng từ xa thì hacker lấy lý do quên mật khẩu hoặc bị hỏng đĩa cứng để yêu cầu cấp lại mật khẩu.
- Bẻ mật khẩu: Hacker tìm cách lấy file mật khẩu và sau đó tấn công bằng từ điển, dựa trên các thuật toán mã hoá mà các hệ điều hành sử dụng. Những mật khẩu yếu rất dễ bị phát hiện bằng cách này.
- Virus và các chương trình tấn công từ bên trong. Hacker có thể sử dụng chúng để thực hiện những việc như: bắt các ký tự gõ vào từ bàn phím để tìm mật khẩu, chép trộm file mật khẩu, thay đổi quyền của người sử dụng . . .
- Các công cụ tấn công giả mạo địa chỉ (IP spoofing): hacker có thể dùng những công cụ này để làm hệ thống tưởng lầm máy tính của hacker là một máy trong mạng nội bộ, hoặc để xoá dấu vết tránh bị phát hiện.
- Phong toả dịch vụ (DoS - Denial of Service): kiểu tấn công này nhằm làm gián đoạn hoạt động của mạng, ví dụ gây lỗi của chương trình ứng dụng để làm treo máy, tạo những thông điệp giả trên mạng để chiếm đường truyền hoặc làm cạn công suất xử lý của máy chủ.

2. Các mức bảo vệ an toàn mạng

Vì không thể có một giải pháp an toàn tuyệt đối nên người ta phải sử dụng đồng thời nhiều mức bảo vệ khác nhau tạo thành nhiều lớp "rào chắn" đối với các hoạt động xâm phạm. Việc bảo vệ thông tin trên mạng chủ yếu là bảo vệ thông tin cất giữ trên các máy tính, đặc biệt là trong các Server của mạng. Vì thế mọi cố gắng tập trung vào việc xây dựng các mức "rào chắn" từ ngoài vào trong cho các hệ thống kết nối vào mạng.



- Lớp bảo vệ trong cùng là ***quyền truy nhập*** (Access rights) nhằm kiểm soát các tài nguyên (thông tin) của mạng và quyền hạn (có thể thực hiện các thao tác gì) trên tài nguyên đó. Dĩ nhiên là kiểm soát được cấu trúc dữ liệu càng chi tiết càng tốt. Hiện tại việc kiểm soát thường ở mức File

- Lớp bảo vệ tiếp theo là ***đăng ký tên / mật khẩu*** (Login/Password). Thực ra đây cũng là kiểm soát quyền truy nhập nhưng không phải truy nhập ở mức thông tin mà ở mức hệ thống (tức là truy nhập vào mạng). Đây là phương pháp bảo vệ phổ biến nhất vì nó đơn giản ít phí tổn và rất có hiệu quả. Mỗi người sử dụng (kể cả người được quyền giám quản mạng - supervisor) muốn được vào mạng để sử dụng các tài nguyên của mạng đề phải có đăng ký tên và mật khẩu trước. Người giám quản mạng có trách nhiệm quản lý, kiểm soát mọi hoạt động của mạng và xác định quyền truy nhập người sử dụng khác tuỳ theo thời gian và không gian.
- Để bảo mật thông tin truyền trên mạng, người ta sử dụng các phương pháp ***mã hoá*** (Encryption). Dữ liệu được biến đổi từ dạng nhận thức được sang dạng không nhận thức được theo một thuật toán nào đó (tạo mật mã) và sẽ được biến đổi ngược lại (giải mã) ở trạm nhận. Đây là lớp bảo vệ thông tin rất quan trọng và được sử dụng rộng rãi trong môi trường mạng .
- Bảo vệ ***vật lý*** (Physical Protection) nhằm ngăn cản các truy nhập vật lý bất hợp pháp vào hệ thống. Thường dùng các biện pháp truyền thống như ngăn cấm tuyệt đối người không phận sự vào phòng đặt máy mạng, dùng ổ khoá máy tính, hoặc cài đặt cơ chế báo động khi có truy nhập vào hệ thống...
- Để bảo vệ từ xa một máy tính hay cho cả một mạng nội bộ (Intranet), người ta thường dùng các hệ thống đặc biệt là ***tường lửa*** (Firewall). Chức năng của tường lửa là ngăn chặn các truy nhập trái phép (theo danh sách truy nhập đã xác định trước) và thậm chí có thể lọc các gói tin mà ta không muốn gửi đi hoặc nhận vào vì một lý do nào đó. Phương thức bảo vệ này được dùng nhiều trong môi trường liên mạng Internet.

II. THIẾT KẾ CHÍNH SÁCH AN NINH CHO MẠNG

Kế hoạch an toàn thông tin phải tính đến các nguy cơ từ bên ngoài và từ trong nội bộ, đồng thời phải kết hợp cả các biện pháp kỹ thuật và các biện pháp quản lý. Sau đây là các bước cần tiến hành:

- Xác định các yêu cầu và chính sách an toàn thông tin: Bước đầu tiên trong kế hoạch an toàn thông tin là xác định các yêu cầu truy nhập và tập hợp những dịch vụ cung cấp cho người sử dụng trong và ngoài cơ quan, trên cơ sở đó có được các chính sách tương ứng.
- Thiết kế an toàn vòng ngoài: Việc thiết kế dựa trên các chính sách an toàn đã xác định trước. Kết quả của bước này là kiến trúc mạng cùng với các thành phần phần cứng và phần mềm sẽ sử dụng. Trong đó cần đặc biệt chú ý hệ thống truy cập từ xa và cơ chế xác thực người dùng.
- Biện pháp an toàn cho các máy chủ và máy trạm: Các biện pháp an toàn vòng ngoài, dù đầy đủ đến đâu, cũng có thể không đủ để chống lại sự tấn công, đặc biệt là sự tấn công từ bên trong. Cần phải kiểm tra các máy chủ và máy trạm để phát hiện những sơ hở về bảo mật. Đối với filewall và các máy chủ ở ngoài cần kiểm tra những dạng tấn công denial of service.
- Kiểm tra thường kỳ: Cần có kế hoạch kiểm tra định kỳ toàn bộ hệ thống an toàn thông tin, ngoài ra cần kiểm tra lại mỗi khi có sự thay đổi về cấu hình

1. Kế hoạch an ninh mạng

Chúng ta sẽ cần một chính sách an ninh mạng nếu tài nguyên và thông tin của công ty cần được bảo vệ. Đa số các công ty và tổ chức đều có các thông tin riêng, các bí mật cạnh tranh trên mạng. Những thông tin này cũng phải được bảo vệ như các tài sản khác của công ty.

Để có một chính sách an ninh mạng hiệu quả thì chúng ta phải trả lời được câu hỏi: loại dịch vụ nào, loại tài nguyên nào người dùng được phép truy nhập và loại nào thì bị cấm ?

Nếu hiện thời những người dùng trên mạng của chúng ta vẫn truy nhập không hạn chế thì cũng tương đối khó khăn khi áp dụng một chính sách hạn chế truy nhập của họ. Chính sách mạng không phải là để làm giảm chức năng của tổ chức chúng ta bởi vì nếu chính sách ấy làm hạn chế khả năng thực hiện công việc của người dùng thì hậu quả sẽ là: Những người dùng trên mạng sẽ tìm cách để bỏ qua thực hiệnchính sách, làm cho chính sách mất hiệu lực.

2. Chính sách an ninh nội bộ

Một tổ chức có thể có nhiều bộ phận ở nhiều nơi, mỗi bộ phận có mạng riêng. Nếu tổ chức lớn thì mỗi mạng phải có ít nhất một người quản trị mạng. Nếu các nơi không nối với nhau thành mạng nội bộ thì chính sách an ninh cũng có những điểm khác nhau.

Thông thường thì tài nguyên mạng ở mỗi nơi bao gồm:

* Các trạm làm việc
* Các thiết bị kết nối: Gateway, Router, Bridge, repeater
* Các Server
* Phần mềm mạng và phần mềm ứng dụng
* Cáp mạng
* Thông tin trong các tệp và các CSDL

Chính sách an ninh tại chỗ phải cân nhắc đến việc bảo vệ các tài nguyên này. Đồng thời cũng phải cân nhắc giữa các yêu cầu an ninh với các yêu cầu kết nối mạng bởi vì một chính sách bảo vệ tốt cho mạng này lại bất lợi cho mạng khác

3. Phương thức thiết kế

Tạo ra một chính sách mạng có nghĩa là lập lên các thủ tục và kế hoạch bảo vệ tài nguyên của chúng ta khỏi mất mát và hư hại. Một hướng tiếp cận khả thi là trả lời các câu hỏi sau :

* Chúng ta muốn bảo vệ tài nguyên nào ?
* Chúng ta cần bảo vệ tài nguyên trên khỏi những người nào ?
* Có các mối đe doạ như thế nào ?
* Tài nguyên quan trọng tới mức nào ?

* Chúng ta sẽ dùng cách nào để bảo vệ tài nguyên theo cách tiết kiệm và hợp lý nhất

* Kiểm tra lại chính sách theo chu kỳ nào để phù hợp với các thay đổi về mục đích cũng như về hiện trạng của mạng ?

Thường thì chi phí bảo vệ an ninh mạng vẫn còn ít hơn chi phí phục hồi lại mạng khi hiểm hoạ xảy ra. Nếu người quản trị mạng không đủ kiến thức về việc bảo vệ này nhất thiết phải hỏi những người khác, chuyên về phần tài nguyên mà người quản trị không biết. Đồng thời cũng phải có một nhóm người thuộc nhiều khu vực tham gia vào việc thiết kế chính sách an ninh thì chính sách mới toàn diện, có tính hợp tác và mọi người đều chấp nhận.

4. Phân tích nguy cơ mất an ninh

Trước khi thiết lập chính sách ta cần phải biết rõ tài nguyên nào cần được bảo vệ, tức là tài nguyên nào có tầm quan trọng lớn hơn để đi đến một giải pháp hợp lý về kinh tế. Đồng thời ta cũng phải xác định rõ đâu là nguồn đe doạ tới hệ thống. Nhiều nghiên cứu cho thấy rằng, thiệt hại do những kẻ "đột nhập bên ngoài" vẫn còn nhỏ hơn nhiều so với sự phá hoại của những "người bên trong". Phân tích nguy cơ bao gồm những việc :

- Ta cần bảo vệ những gì ?
- Ta cần bảo vệ những tài nguyên khỏi những gì ?
- Làm thế nào để bảo vệ ?

Các nguy cơ cũng phải được xếp hạng theo tầm quan trọng và mức độ trầm trọng của thiệt hại. Có hai hệ số sau :

1. Ri là nguy cơ mất mát tài nguyên i

2. Wi là tầm quan trọng của tài nguyên i

Ri có các giá trị từ 0.0 đến 1.0 trong đó :

Ri = 0.0 là không có nguy cơ mất mát tài nguyên

Ri = 1.0 là có nguy cơ mất mát tài nguyên cao nhất

Wi có các giá trị từ 0.0 đến 1.0 trong đó :

Wi = 0.0 là tài nguyên không có tầm quan trọng

Wi = 1.0 là tài nguyên có tầm quan trọng cao nhất

Khi đó trọng số nguy cơ của tài nguyên là tích của hai hệ số :

WRi = Ri * Wi

Các hệ số khác cần xem xét là tính hiệu lực, tính toàn vẹn và tính cẩn mật. Tính hiệu lực của một tài nguyên là mức độ quan trọng của việc tài nguyên đó luôn sẵn sàng dùng được mọi lúc. Tính toàn vẹn là tầm quan trọng cho các tài nguyên CSDL. Tính cẩn mật áp dụng cho các tài nguyên như tệp dữ liệu mà ta có hạn chế được truy nhập tới chúng.

5. Xác định tài nguyên cần bảo vệ

Khi thực hiện phân tích ta cũng cần xác định tài nguyên nào có nguy cơ bị xâm phạm. Quan trọng là phải liệt kê được hết những tài nguyên mạng có thể bị ảnh hưởng khi gặp các vấn đề về an ninh.

1. ***Phần cứng***: Vi xử lý, bản mạch, bàn phím, terminal, trạm làm việc, máy tính các nhân, máy in, ổ đĩa, đường liên lạc, server, router

2. ***Phần mềm***: Chương trình nguồn, chương trình đối tượng, tiện ích,chương trình khảo sát, hệ điều hành, chương trình truyền thông.

3. ***Dữ liệu***: Trong khi thực hiện, lưu trữ trực tuyến, cất giữ off-line, backup, các nhật ký kiểm tra, CSDL truyền trên các phương tiện liên lạc.

4. ***Con người***: Người dùng, người cần để khởi động hệ thống.

5. ***Tài liệu***: Về chương trình , về phần cứng, về hệ thống, về thủ tục quản trị cục bộ.

6. ***Nguồn cung cấp***: giấy in, các bảng biểu, băng mực, thiết bị từ.

6. Xác định mối đe doạ an ninh mạng

Sau khi đã xác định những tài nguyên nào cần được bảo vệ, chúng ta cũng cần xác định xem có các mối đe doạ nào nhằm vào các tài nguyên đó. Có thể có những mối đe doạ sau:

Truy nhập bất hợp pháp:

Chỉ có những người dùng hợp pháp mới có quyền truy nhập tài nguyên mạng, khi đó ta gọi là truy nhập hợp pháp. Có rất nhiều dạng truy nhập được gọi là bất hợp pháp chẳng hạn như dùng tài khoản của người khác khi không được phép. Mức độ trầm trọng của việc truy nhập bất hợp pháp tuỳ thuộc vào bản chất và mức độ thiệt hại do truy nhập đó gây nên.

Để lộ thông tin:

Để lộ thông tin do vô tình hay cố ý là một mối đe doạ khác. Chúng ta nên định ra các giá trị để phản ánh tầm quan trọng của thông tin. Ví dụ đối với các nhà sản xuất phần mềm thì đó là: mã nguồn, chi tiết thiết kế, biểu đồ, thông tin cạnh tranh về sản phẩm... Nếu để lộ các thông tin quan trọng, tổ chức của chúng ta có thể bị thiệt hại về các mặt như uy tín, tính cạnh tranh, lợi ích khách hàng...

Từ chối cung cấp dịch vụ:

Mạng thường gồm những tài nguyên quý báu như máy tính, CSDL ... và cung cấp các dịch vụ cho cả tổ chức. Đa phần người dùng trên mạng đều phụ thuộc vào các dịch vụ để thực hiện công việc được hiệu quả.

Chúng ta rất khó biết trước các dạng từ chối của một dịch vụ. Có thể tạm thời liệt kê ra một số dạng sau:

* Mạng không dùng được do một gói gây lỗi
* Mạng không dùng được do quá tải giao thông
* Mạng bị phân mảnh do một router quan trọng bị vô hiệu hoá

* Một virus làm chậm hệ thống do dùng các tài nguyên mạng
* Thiết bị bảo vệ mạng bị vô hiệu hoá

7. Trách nhiệm sử dụng mạng

Ai được quyền dùng tài nguyên mạng

Ta phải liệt kê tất cả người dùng cần truy nhập tới tài nguyên mạng. Không nhất thiết liệt kê toàn bộ người dùng. Nếu phân nhóm cho người dùng thì việc liệt kê sẽ đơn giản hơn. Đồng thời ta cũng phải liệt kê một nhóm đặc biệt gọi là các người dùng bên ngoài, đó là những người truy nhập từ một trạm đơn lẻ hoặc từ một mạng khác.

Sử dụng tài nguyên thế nào cho đúng ?

Sau khi xác định những người dùng được phép truy nhập tài nguyên mạng, chúng ta phải tiếp tục xác định xem các tài nguyên đó sẽ được dùng như thế nào. Như vậy ta phải đề ra đường lối cho từng lớp người sử dụng như: Những nhà phát triển phần mềm, sinh viên, những người ngoài.

Sau đây là một số điều khoản cần có cho đường lối chỉ đạo chung:

* Sử dụng tài khoản người khác có được phép không ?
* Có được phép dùng chương trình tìm mật khẩu không ?
* Có được phép ngắt một dịch vụ không ?
* Có được sửa đổi một tệp không thuộc sở hữu nhưng lại có quyền ghi không ?
* Có được phép cho người khác dùng tài khoản riêng không ?

Ai có quyền cấp phát truy nhập ?

Chính sách an ninh mạng phải xác định rõ ai có quyền cấp phát dịch vụ cho người dùng. Đồng thời cũng phải xác định những kiểu truy nhập mà người dùng có thể cấp phát lại. Nếu đã biết ai là người có quyền cấp phát truy nhập thì ta có thể biết được kiểu truy nhập đã được cấp phát, biết được người dùng có được cấp phát quá quyền hạn không. Ta phải cân nhắc hai điều sau:

* Truy nhập dịch vụ có được cấp phát từ một điểm trung tâm không ?
* Phương thức nào được dùng để tạo tài khoản mới và kết thúc truy nhập ?

Nếu một tổ chức lớn mà không tập trung thì tất nhiên là có nhiều điểm trung tâm để cấp phát truy nhập, mỗi điểm trung tâm phải chịu trách nhiệm cho tất cả các phần mà nó cấp phát truy nhập.

Người dùng có quyền hạn và trách nhiệm gì ?

Sau đây là danh sách các điều khoản áp dụng cho người dùng:

* Phải tuân thủ mọi đường lối liên quan đến việc sử dụng mạng.
* Phải chịu phạt nếu vi phạm những gì được coi là lạm dụng tài nguyên, ảnh hưởng đến hoạt động hệ thống.

* Người dùng được phép chia sẻ tài khoản không ?

* Người dùng có được phép tiết lộ mật khẩu để người khác làm việc hộ mình không ?

* Tuân theo mọi chính sách về mật khẩu bao gồm: thời hạn thay đổi mật khẩu, những yêu cầu đối với mật khẩu...

* Người dùng có trách nhiệm sao lưu dữ liệu của mình không hay đây là trách nhiệm của người quản trị ?

* Hậu quả của việc người dùng tiết lộ các thông tin độc quyền, người này sẽ bị phạt thế nào ?

* Đảm bảo các điều khoản về tính riêng tư của thư tín điện tử.

Người quản trị hệ thống có quyền hạn và trách nhiệm gì ?

Người quản trị hệ thống thường xuyên phải thu thập thông tin về các tệp trong các thư mục riêng của người dùng để tìm hiểu các vấn đề hệ thống. Ngược lại, người dùng phải giữ gìn bí mật riêng tư về thông tin của họ. Vì thế mà chính sách mạng phải xác định xem người quản trị có được phép kiểm tra thư mục của người dùng khi có vi phạm an ninh hay không. Nếu an ninh có nguy cơ thì người quản trị phải có khả năng linh hoạt để giải quyết vấn đề. Còn các điều khoản có liên quan khác như sau:

Người quản trị hệ thống có được theo dõi hay đọc các tệp của người dùng với bất cứ lý do gì hay không ?

Người quản trị mạng có quyền kiểm tra giao thông mạng và giao thông đến trạm hay không ?

Người dùng, người quản trị hệ thống, các tổ chức có trách nhiệm pháp lý nào đối với việc truy nhập trái phép tới dữ liệu riêng tư của người khác, của tổ chức khác?

Làm gì với các thông tin quan trọng

Theo quan điểm an ninh, các dữ liệu cực kỳ quan trọng phải được hạn chế, chỉ một số ít máy và ít người có thể truy nhập. Trước khi cấp phát truy nhập cho một người dùng, phải cân nhắc xem nếu anh ta có khả năng đó thì anh ta có thể thu được các truy nhập khác không ? Ngoài ra cũng phải báo cho người dùng biết là dịch vụ nào tương ứng với việc lưu trữ thông tin quan trọng của anh ta.

8. Kế hoạch hành động khi chính sách bị vi phạm

Mỗi khi chính sách bị vi phạm cũng có nghĩa là hệ thống đứng trước nguy cơ mất an ninh. Khi phát hiện vi phạm, chúng ta phải phân loại lý do vi phạm chẳng hạn như do người dùng cẩu thả, lỗi hoặc vô ý, không tuân thủ chính sách...

Phản ứng khi có vi phạm

Khi vi phạm xảy ra thì mọi người dùng có trách nhiệm đều phải liên đới. ta phải định ra các hành động tương ứng với các kiểu vi phạm. Đồng thời mọi người đều phải biết các quy định này bất kể người trong tổ chức hoặc người ngoài đến sử dụng máy. Chúng ta phải lường trước trường hợp vi phạm không cố ý để giải quyết linh hoạt, lập các sổ ghi chép và định kỳ xem lại để phát hiện các khuynh hướng vi phạm cũng như để điều chỉnh các chính sách khi cần.

Phản ứng khi người dùng cục bộ vi phạm

Người dùng cục bộ có các vi phạm sau:

* Vi phạm chính sách cục bộ.
* Vi phạm chính sách của các tổ chức khác.

Trường hợp thứ nhất chính chúng ta, dưới quan điểm của người quản trị hệ thống sẽ tiến hành việc xử lý. Trong trường hợp thứ hai phức tạp hơn có thể xảy ra khi kết nối Internet, chúng ta phải xử lý cùng các tổ chức có chính sách an **ninh bị vi phạm.**

Chiến lược phản ứng

Chúng ta có thể sử dụng một trong hai chiến lược sau:

- Bảo vệ và xử lý.
- Theo dõi và truy tố.

Trong đó, chiến lược thứ nhất nên được áp dụng khi mạng của chúng ta dễ bị xâm phạm. Mục đích là bảo vệ mạng ngay lập tức xử lý, phục hồi về tình trạng bình thường để người dùng tiếp tục sử dụng được, như thế ta phải can thiệp vào hành động của người vi phạm và ngăn cản không cho truy nhập nữa. Đôi khi không thể khôi phục lại ngay thì chúng ta phải cáh ly các phân đoạn mạng và đóng hệ thống để không cho truy nhập bất hợp pháp tiếp tục.

9. Định các lỗi an ninh

Ngoài việc nêu ra những gì cần bảo vệ, chúng ta phải nêu rõ những lỗi gì gây ra mất an ninh và làm cách nào để bảo vệ khỏi các lỗi đó. Trước khi tiến hành các thủ tục an ninh, nhất định chúng ta phải biết mức độ quan trọng của các tài nguyên cũng như mức độ của nguy cơ.

9.1. Lỗi điểm truy nhập

Lỗi điểm truy nhập là điểm mà những người dùng không hợp lệ có thể đi vào hệ thống, càng nhiều điểm truy nhập càng có nguy có mất an ninh.

9.2. Lỗi cấu hình hệ thống

Khi một kẻ tấn công thâm nhập vào mạng, hắn thường tìm cách phá hoại các máy trên hệ thống. Nếu các máy được cấu hình sai thì hệ thống càng dễ bị phá hoại. Lý do của việc cấu hình sai là độ phức tạp của hệ điều hành, độ phức tạp của phần mềm đi kèm và hiểu biết của người có trách nhiệm đặt cấu hình. Ngoài ra, mật khẩu và tên Login dễ đoán cũng là một sơ hở để nhữ kẻ tấn công có cơ hội truy nhập hệ thống.

9.3. Lỗi phần mềm

Phần mềm càng phức tạp thì lỗi của nó càng phức tạp. Khó có phần mềm nào mà không gặp lỗi. Những kẻ tấn công nắm được lỗi của phần mềm, nhất là phần mềm hệ thống thì việc phá hoại cũng khá dễ dàng. Chẳng hạn nếu dùng hệ điều hành nổi tiếng thì các lỗi an ninh cũng nổi tiếng, việc dùng điểm yếu của phần mềm để thu được các truy nhập ưu tiên không phải là khó. Người quản trị cần có trách nhiệm duy trì các bản cập nhật, các bản sửa đổi cũng như thông báo các lỗi cho người sản xuất chương trình.

9.4. Lỗi của người dùng nội bộ

Người dùng nội bộ thường có nhiều truy nhập hệ thống hơn những người bên ngoài, nhiều truy nhập tới phần mềm hơn phần cứng do đó dễ dàng phá hoại hệ thống. Đa số các dịch vụ TCP/IP như telnet, tfp, rlogin đều có điểm yếu là truyền mật khẩu trên mạng mà không mã hoá nên nếu là người trong mạng thì họ có khả năng rất lớn và dễ dàng nắm được mật khẩu với sự trợ giúp của các chương trình đặc biệt.

9.5. Lỗi an ninh vật lý

Nếu máy tính không an toàn về mặt vật lý thì các cơ cấu an ninh phần mềm dễ dàng bị vượt qua. Nếu các trạm không có ai trông coi, dữ liệu trên ổ cứng dễ bị xoá sạch hoặc nếu nó đang ở chế độ có quyền hạn cáo thì quyền hạn này có thể bị lợi dụng làm những việc không được phép.

Các tài nguyên trong các trục xương sống (backbone), đường liên lạc, server quan trọng... đều phải được giữ trong các khu vực an toàn về vật lý. An toàn vật lý có nghĩa là máy được khoá ở trong một phòng kín hoặc đặt ở những nơi người ngoài không thể truy nhập vật lý tới dữ liệu trong máy.

9.6. Lỗi bảo mật

Bảo mật mà chúng ta hiểu ở đây là hành động giữ bí mật một điều gì, thông tin rất dễ lộ ra trong những trường hợp sau:

Khi thông tin lưu trên máy tính.

Khi thông tin đang chuyển tới một hệ thống khác.

Khi thông tin lưu trên các băng từ sao lưu.

Đối với thông tin lưu trên máy tính thì việc truy nhập được truy nhập bởi quyền hạn tệp, danh sách điều khiển truy nhập ALC (Access Control List)... Với các thông tin trên đường truyền thì có thể bảo vệ bằng mã hoá hoặc Gateway tường lửa. Mã hoá có thể dùng bảo vệ cho cả ba trường hợp. Còn với các thông tin lưu trên băng từ thì an ninh vật lý là quan trọng, nên cất băng từ trong tủ bảo mật.