HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

- - - - - - - 🕮 - - - - - - -

SÁCH HƯỚNG DẪN HỌC TẬP

MẠNG MÁY TÍNH

Biên soạn : Ts. PHẠM THẾ QUẾ

Lưu hành nội bộ

HÀ NỘI - 2006

MỞ ĐẦU

Tài liệu này phục vụ cho sinh viên hệ đào đại học từ xa học tập và nghiên cứu về “Mạng máy tính”.

Tài liệu gồm các nội dung chính sau:

Chương I: Giới thiệu tổng quan về mạng máy tính. Khái niệm cơ bản về kiến trúc và các giao thức mạng, các loại mạng máy tính và mục tiêu ứng dụng của nó.

Chương II: Nghiên cứu các nguyên tắc cơ bản để thiết kế một mô hình giao thức mạng máy tính theo quan điểm chia các tiến trình truyền thông thành cấu trúc nhiều tầng, được xếp chồng lên nhau để thực hiện một tiến trình truyền thông hoàn chỉnh. Giới thiệu mô hình OSI, được xem như là một mô hình chuẩn, một chiến lược phát triển các hệ thống mở và một khung khái niệm về giao thức và dịch vụ.

Chương III*:* Giới thiệu một số bộ giao thức mạng mang tính đặc trưng và được áp dụng phổ biến. Đặc biệt trong chương này tìm hiểu sâu hơn bộ giao thức TCP/IP đã trở thành chuẩn chung cho mạng máy tính toàn cầu, mạng Internet.

Chương IV: Chương này giới thiệu các công nghệ mạng cục bộ. Kiến trúc mạng cục bộ Ethrnet, Virtual LAN, Local ATM , LAN ARCnet..

Chương V: Giới thiệu về công nghệ và kỹ thuật mạng diện rộng WAN. Cụ thể xem xét công nghệ các mạng tích hợp số đa dịch vụ ISDN và băng rộng B-ISDN, Frame Relay và X25, dịch vụ SDMS và phương thức truyền dẫn không đồng bộ ATM.

Chương VI: Giới thiệu một số công nghệ mới như công nghệ đường dây thuê bao số DSL, các mạng chuyển mạch gói chuyển tải tiếng nói trên nền IP, ATM và Frame Raly. Các công nghệ chuyển mạch nhãn đa giao thức IP/MPLS, chuyển mạch mềm Softswitch sử dụng trong mạng hội tụ và mạng thế hệ sau NGN.

Chương VII: Đề cập đến một số vấn đề bảo vệ thông tin trên mạng. Chương này giới thiệu cách tiếp cận các hệ mật mã, các giao thức bảo mật, mạng riêng ảo VPN và các giải pháp an toàn mạng, xác thực điện tử, các giải pháp chữ ký điện tử, xác minh chữ ký và từ chối chữ ký giả mạo..

Tài liệu không chỉ đề cập đến những vấn đề cơ sở lý luận mà còn trình bày một số kỹ năng, kinh nghiệm cần thiết để thiết kế và cài đặt các mạng máy tính. Hy vọng sẽ có ích cho các bạn học sinh sinh viên và những người muốn xây dựng các hệ thống tin học ứng dụng phục vụ cho sản xuất, quản lý trong các doanh nghiệp. Có thể còn nhiều thiếu sót trong trình bày và biên soạn do khả năng, trình độ, nhưng người biên soạn mạnh dạn giới thiệu tài liệu này và mong nhận được sự góp ý của bạn đọc.

TS Phạm Thế Quế

CHƯƠNG I: KHÁI NIỆM VỀ MẠNG MÁY TÍNH

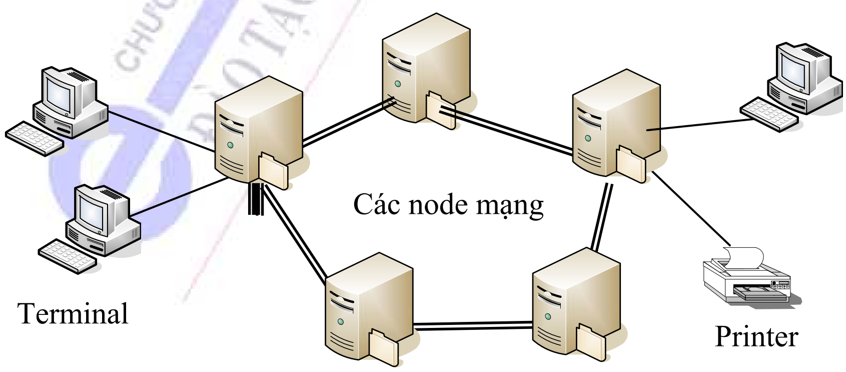
Nội dung của chương sẽ trình bày các khái niệm cơ bản của mạng máy tính, định nghĩa mạng máy tính, mục tiêu và ứng dụng của mạng, cấu trúc và các thành phần cơ bản của một mạng máy tính. Các thực thể trên mạng có thể tham gia truyền thông với nhau cần tuân theo tập các phần mềm điều khiển hoạt động của mạng, được gọi là chuẩn, hay còn gọi là tập các giao thức mạng (Protocols). Nội dung của chương bao gồm các phần sau:

- Định nghĩa mạng máy tính
- Mục tiêu mạng máy tính.
- Các dịch vụ mạng.
- Cấu trúc mạng (Topology)
- Khái niệm giao thức mạng máy tính (Protocols)
- Mạng LAN, MAN, WAN.
- Mạng chuyển mạch kênh (Circuit switched Networks)
- Mạng chuyển mạch gói (Packet Switched Networks).
- Các mô hình xử lý dữ liệu

1.1. Định nghĩa mạng máy tính

Mạng máy tính là tập hợp các máy tính đơn lẻ được kết nối với nhau bằng các phương tiện truyền vật lý (Transmission Medium) và theo một kiến trúc mạng xác định (Network Architecture).

Mạng viễn thông cũng là mạng máy tính. Các node chuyển mạch là hệ thống máy tính được kết nối với nhau bằng các đường truyền dẫn và hoạt động truyền thông tuân theo các chuẩn mô hình tham chiếu OSI. Hình 1.2 mô tả khái quát các thành phần của định nghĩa.



Hình 1.1 Mạng máy tính

Kiến trúc mạng gồm cấu trúc mạng (Topology) và giao thức mạng (Protocols). Topology là cấu trúc hình học của các thực thể mạng và giao thức mạng là tập các quy tắc chuẩn các thực thể hoạt động truyền thông phải tuân theo.

1.2. Mục tiêu mạng máy tính

1.2.1. Mục tiêu kết nối mạng máy tính

- Cùng chia sẻ các tài nguyên chung, bất kỳ người sử dụng nào cũng có quyền khai thác, sử dụng tài nguyên của mạng mà không phụ thuộc vào vị trí địa lý của nó.

- Nâng cao độ tin cậy của hệ thống nhờ khả năng thay thế khi một số thành phần của mạng xẩy ra sự cố kỹ thuật thì vẫn duy trì sự hoạt động bình thường của hệ thống.

- Tạo môi trường giao tiếp giữa người với người. Chinh phục được khoảng cách, con người có thể trao đổi, thảo luận với nhau cách xa nhau hàng nghìn km.

1.2.2. Lợi ích kết nối mạng

- Có thể giảm số lượng máy in, đĩa cứng và các thiết bị khác. Kinh tế trong việc đầu tư xây dựng cho một hệ thống tin học của một cơ quan, xí nghiêp, doanh nghiệp...

- Dùng chung tài nguyên đắt tiền như máy in, phần mềm...Tránh dư thừa dữ liệu, tài nguyên mạng. Có khả năng tổ chức và triển khai các đề án lớn thuận lợi và dễ dàng.

- Bảo đảm các tiêu chuẩn thống nhất về tính bảo mật, an toàn dữ liệu khi nhiều người sử dụng tại các thiết bị đầu cuối khác nhau cùng làm việc trên các hệ cơ sở dữ liệu.

Tóm lại, mục tiêu kết nối các máy tính thành mạng là cung cấp các dịch vụ mạng đa dạng, chia sẻ tài nguyên chung và giảm bớt các chi phí về đầu tư trang thiết bị.

1.3. Các dịch vụ mạng

1.3.1. Các xu hướng phát triển dịch vụ mạng máy tính

- Cung cấp các dịch vụ truy nhập vào các nguồn thông tin ở xa để khai thác và xử lý thông tin. Cung cấp các dịch vụ mua bán, giao dịch qua mạng...

- Phát triển các dịch vụ tương tác giữa người với người trên phạm vi diện rộng. Đáp ứng nhu cầu trao đổi thông tin đa dịch vụ, đa phương tiện. Tạo các khả năng làm việc theo nhóm bằng các dịch vụ thư điện tử, video hội nghị, chữa bệnh từ xa ...

- Xu hướng phát triển các dịch vụ giải trí trực tuyến (Online) hiện đại. Các hình thức dịch vụ truyền hình, nghe nhạc, chơi game trực tuyến qua mạng......

1.3.2. Các dịch vụ phổ biến trên mạng máy tính

- Dịch vụ tệp (File services) cho phép chia sẻ tài nguyên thông tin chung, chuyển giao các tệp dữ liệu từ máy này sang máy khác. Tìm kiếm thông tin và điều khiển truy nhập. Dịch vụ thư điện tử E_Mail (Electronic mail) cung cấp cho người sử dụng phương tiện trao đổi, tranh luận bằng thư điện tử. Dịch vụ thư điện tử giá thành hạ, chuyển phát nhanh, an toàn và nội dung có thể tích hợp các loại dữ liệu.

- Dịch vụ in ấn: Có thể dùng chung các máy in đắt tiền trên mạng. Cung cấp khả năng đa truy nhập đến máy in, phục vụ đồng thời cho nhiều nhu cầu in khác nhau. Cung cấp các dịch vụ FAX và quản lý được các trang thiết bị in chuyên dụng.

- Các dịch vụ ứng dụng hướng đối tượng: Sử dụng các dịch vụ thông điệp (Message) làm trung gian tác động đến các đối tượng truyền thông. Đối tượng chỉ bàn giao dữ liệu cho tác nhân (Agent) và tác nhân sẽ bàn giao dữ liệu cho đối tượng đích.

- Các dịch vụ ứng dụng quản trị luồng công việc trong nhóm làm việc: Định tuyến các tài liệu điện tử giữa những người trong nhóm. Khi chữ ký điện tử được xác nhận trong các phiên giao dịch thì có thể thay thế được nhiều tiến trình mới hiệu quả và nhanh chóng hơn.

- Dịch vụ cơ sở dữ liệu là dịch vụ phổ biến về các dịch vụ ứng dụng, là các ứng dụng theo mô hình Client/Server. Dịch vụ xử lý phân tán lưu trữ dữ liệu phân tán trên mạng, người dùng trong suốt và dễ sử dụng, đáp ứng các nhu cầu truy nhập của người sử dụng.

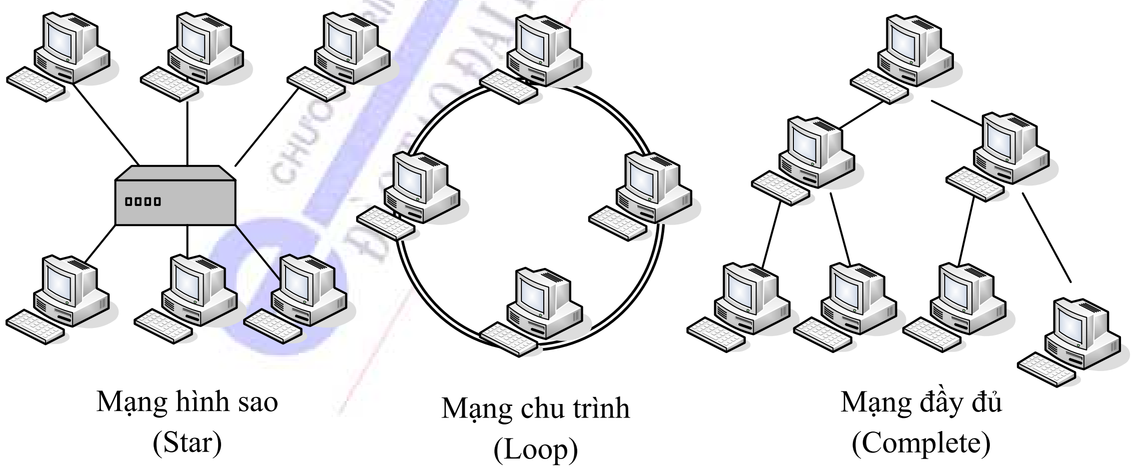
1.4. Cấu trúc mạng (Topology)

Topology là cấu trúc hình học không gian của mạng thực chất là cách bố trí vị trí vật lý các node và cách thức kết nối chúng lại với nhau. Có hai kiểu cấu trúc mạng: kiểu điểm - điểm (Point to Point) và kiểu quảng bá (Multi Point).

1.4.1. Kiểu điểm - điểm (Point to Point)

Đường truyền nối từng cặp node lại với nhau theo một hình học xác định. Một kênh truyền vật lý sẽ được thiết lập giữa 2 node có nhu cầu trao đổi thông tin. Chức năng các node trung gian: tiếp nhận, lưu trữ tạm thời và gửi tiếp thông tin sang node tiếp theo khi đường truyền rỗi. Cấu trúc điểm- điểm gọi là mạng lưu và gửi tiếp (Store - and - Forward).

Ưu điểm là ít khả năng đụng độ thông tin (Collision). Nhược điểm của nó là hiệu suất sử dụng đường truyền thấp. Chiếm dụng nhiều tài nguyên, độ trễ lớn, tiêu tốn nhiều thời gian để thiết lập đường truyền và xử lý tại các node. Vì vậy tốc độ trao đổi thông tin thấp.



Hình 1.2 Các mạng có cấu trúc điểm - điểm

1.4.2. Kiểu đa điểm hay quảng bá (Point to Multipoint, Broadcasting)

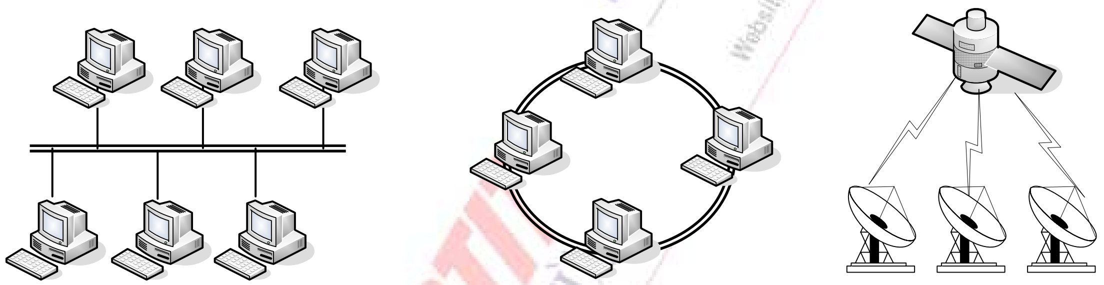
Tất cả các node cùng truy nhập chung trên một đường truyền vật lý. Một thông điệp được truyền đi từ một node nào đó sẽ được tất cả các node còn lại tiếp nhận và kiểm tra địa chỉ đích trong thông điệp có phải của nó hay không. Cần thiết phải có cơ chế để giải quyết vấn đề đụng độ thông tin (Collision) hay tắc nghẽn thông tin trên đường truyền trong các mạng hình BUS và hình RING.

Các mạng có cấu trúc quảng bá được phân chia thành hai loại: quảng bá tĩnh và quảng bá động phụ thuộc vào việc cấp phát đường truyền cho các node. Trong quảng bá động có quảng bá động tập trung và quảng bá động phân tán.

Quảng bá tĩnh: Chia thời gian thành nhiều khoảng rời rạc và dùng cơ chế quay vòng (Round Robin) để cấp phát đường truyền. Các node có quyền được truy nhập khi đến cửa thời gian của nó.

Quảng bá động tập trung: Một thiết bị trung gian có chức năng tiếp nhận yêu cầu liên lạc và cấp phát đường truyền cho các node. Kiểu cấp phát này giảm được tối đa thời gian chết của đường truyền, hiệu suất kênh truyền cao, nhưng thiết kế phức tạp và khó khăn.

Quảng bá động phân tán: Không có bộ trung gian, các node tự quyết định có nên hay không nên truy nhập đường truyền, phụ thuộc vào trạng thái của mạng.



Mạng hình BUS   Mạng hình vòng RING   Vệ tinh

Hình 1.3 Các mạng có cấu trúc quảng bá

1.5. Khái niệm giao thức mạng máy tính (Protocols)

1.5.1. Khái niệm về giao thức

Các thực thể của mạng muốn trao đổi thông tin với nhau phải bắt tay, đàm phán về một số thủ tục, quy tắc... Cùng phải "nói chung một ngôn ngữ". Tập quy tắc hội thoại được gọi là giao thức mạng (Protocols). Các thành phần chính của một giao thức bao gồm:

- Cú pháp: định dạng dữ liệu, phương thức mã hoá và các mức tín hiệu.

- Ngữ nghĩa: thông tin điều khiển, điều khiển lưu lượng và xử lý lỗi..

Trao đổi thông tin giữa hai thực thể có thể là trực tiếp hoặc gián tiếp. Trong hai hệ thống kết nối điểm - điểm, các thực thể có thể trao đổi thông tin trực tiếp không có sự can thiệp của các thực thể trung gian. Trong cấu trúc quảng bá, hai thực thể trao đổi dữ liệu với nhau phải thông qua các thực thể trung gian. Phức tạp hơn khi các thực thể không chia sẻ trên cùng một mạng chuyển mạch, kết nối gián tiếp phải qua nhiều mạng con.

1.5.2. Chức năng giao thức

Đóng gói: Trong quá trình trao đổi thông tin, các gói dữ liệu được thêm vào một số thông tin điều khiển, bao gồm địa chỉ nguồn và địa chỉ đích, mã phát hiện lỗi, điều khiển giao thức... Việc thêm thông tin điều khiển vào các gói dữ liệu được gọi là quá trình đóng gói (Encapsulation). Bên thu sẽ được thực hiện ngược lại, thông tin điều khiển sẽ được gỡ bỏ khi gói tin được chuyển từ tầng dưới lên tầng trên.

Phân đoạn và hợp lại: Mạng truyền thông chỉ chấp nhận kích thước các gói dữ liệu cố định. Các giao thức ở các tầng thấp cần phải cắt dữ liệu thành những gói có kích thước quy định. Quá trình này gọi là quá trình phân đoạn. Ngược với quá trình phân đoạn bên phát là quá trình hợp lại bên thu. Dữ liệu phân đoạn cần phải được hợp lại thành thông điệp thích hợp ở tầng ứng dụng (Application). Vì vậy vấn đề đảm bảo thứ tự các gói đến đích là rất quan trọng. Gói dữ liệu trao đổi giữa hai thực thể qua giao thức gọi là đơn vị giao thức dữ liệu PDU (Protocol Data Unit).

Điều khiển liên kết: Trao đổi thông tin giữa các thực thể có thể thực hiện theo hai phương thức: hướng liên kết (Connection - Oriented) và không liên kết (Connectionless). Truyền không liên kết không yêu cầu có độ tin cậy cao, không yêu cầu chất lượng dịch vụ và không yêu cầu xác nhận. Ngược lại, truyền theo phương thức hướng liên kết, yêu cầu có độ tin cậy cao, đảm bảo chất lượng dịch vụ và có xác nhận. Trước khi hai thực thể trao đổi thông tin với nhau, giữa chúng một kết nối được thiết lập và sau khi trao đổi xong, kết nối này sẽ được giải phóng.

G*iám sát*: Các gói tin PDU có thể lưu chuyển độc lập theo các con đường khác nhau, khi đến đích có thể không theo thứ tự như khi phát. Trong phương thức hướng liên kết, các gói tin phải được yêu cầu giám sát. Mỗi một PDU có một mã tập hợp duy nhất và được đăng ký theo tuần tự. Các thực thể nhận sẽ khôi phục thứ tự các gói tin như thứ tự bên phát.

Điều khiển lưu lượng liên quan đến khả năng tiếp nhận các gói tin của thực thể bên thu và số lượng hoặc tốc độ của dữ liệu được truyền bởi thực thể bên phát sao cho bên thu không bị tràn ngập, đảm bảo tốc độ cao nhất. Một dạng đơn giản của của điều khiển lưu lượng là thủ tục dừng và đợi (Stop-and Wait), trong đó mỗi PDU đã phát cần phải được xác nhận trước khi truyền gói tin tiếp theo. Có độ tin cậy cao khi truyền một số lượng nhất định dữ liệu mà không cần xác nhận. Kỹ thuật cửa sổ trượt là thí dụ cơ chế này. Điều khiển lưu lượng là một chức năng quan trọng cần phải được thực hiện trong một số giao thức.

*Điều khiển lỗ*i là kỹ thuật cần thiết nhằm bảo vệ dữ liệu không bị mất hoặc bị hỏng trong quá trình trao đổi thông tin. Phát hiện và sửa lỗi bao gồm việc phát hiện lỗi trên cơ sở kiểm tra khung và truyền lại các PDU khi có lỗi. Nếu một thực thể nhận xác nhận PDU lỗi, thông thường gói tin đó sẽ phải được phát lại.

Đồng bộ hoá: Các thực thể giao thức có các tham số về các biến trạng thái và định nghĩa trạng thái, đó là các tham số về kích thước cửa sổ, tham số liên kết và giá trị thời gian. Hai thực thể truyền thông trong giao thức cần phải đồng thời trong cùng một trạng thái xác định. Ví dụ cùng trạng thái khởi tạo, điểm kiểm tra và huỷ bỏ, được gọi là đồng bộ hoá. Đồng bộ hoá sẽ khó khăn nếu một thực thể chỉ xác định được trạng thái của thực thể khác khi nhận các gói tin. Các gói tin không đến ngay mà phải mất một khoảng thời gian để lưu chuyển từ nguồn đến đích và các gói tin PDU cũng có thể bị thất lạc trong quá trình truyền.

Địa chỉ hoá: Hai thực thể có thể truyền thông được với nhau, cần phải nhận dạng được nhau. Trong mạng quảng bá, các thực thể phải nhận dạng định danh của nó trong gói tin. Trong các mạng chuyển mạch, mạng cần nhận biết thực thể đích để định tuyến dữ liệu trước khi thiết lập kết nối.

1.6. Cáp mạng - phương tiện truyền (Network Medium)

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

1.6.1. Đặc trưng cơ bản của đường truyền

Băng thông (Bandwidth): Băng thông của một đường truyền là miền tần số giới hạn thấp và tần số giới hạn cao, tức là miền tần số mà đường truyền đó có thể đáp ứng được. Ví dụ băng thông của cáp thoại từ 400 đến 4000 Hz, có nghĩa là nó có thể truyền các tín hiệu với tần số từ 400 đến 4000 chu kỳ/giây. Băng thông của cáp phụ thuộc vào chiều dài của cáp. Cáp ngắn băng thông cao và ngược lại. Vì vậy khi thiết kế lắp đặt cáp, chiều dài cáp sao cho không vượt qua giới hạn cho phép, vì có thể xảy ra lỗi trong quá trình truyền.

Thông lượng (Throughput) Thông lượng của đường truyền là số lượng các bit (chuỗi bit) được truyền đi trong một giây. Hay nói cách khác là tốc độ của đường truyền dẫn. Ký hiệu là bit/s hoặc bps. Tốc độ của đường truyền phụ thuộc vào băng thông và độ dài của nó. Một mạng LAN Ethernet tốc độ truyền 10 Mbps và có băng thông là 10 Mbps.

*Suy hao (Attenuation)***:** Là độ đo sự suy yếu của các tín hiệu trên đường truyền. Suy hao phụ thuộc vào độ dài của cáp, cáp càng dài thì suy hao càng cao. Khi thiết kế cáp cũng rất cần quan tâm đến giới hạn chiều dài cho phép của từng loại cáp.

1.6.2. Các loại cáp mạng

Cáp đồng trục (Coaxial cable): Là phương tiện truyền các tín hiệu có phổ rộng và tốc độ cao. Băng thông của cáp đồng trục từ 2,5 Mbps (ARCnet) đến 10 Mbps (Ethernet). Thường sử dụng để lắp đặt mạng hình BUS (các loại mạng LAN cục bộ Thick Ethernet, Thin Ethernet) và mạng hình sao (mạng ARCnet).

Cáp đồng trục gồm: một dây dẫn trung tâm, một dây dẫn ngoài, tạo nên đường ống bao quanh trục, tầng cách điện giữa 2 dây dẫn và cáp vỏ bọc ngoài.

Các loại cáp đồng trục .

- Cáp RC-8 và RCA-11, 50 Ohm dùng cho mạng Thick Ethernet.
- Cáp RC-58 , 50 Ohm dùng cho mạng Thin Ethernet.
- Cáp RG-59 , 75 Ohm dùng cho truyền hình cáp.
- Cáp RC-62, 93 Ohm dùng cho mạng ARCnet.

Cáp xoắn đôi (*Twisted Pair cable*): *C*áp xoắn đôi được sử dụng trong các mạng LAN cục bộ. Giá thành rẻ, dễ cài đặt, có vỏ bọc tránh nhiệt độ, độ ẩm và có loại có khả năng chống nhiễu

STP (Shield Twisted Pair). Cáp cơ bản có 2 dây đồng xoắn vào nhau, giảm độ nhạy của cáp với EMI, giảm bức xạ âm nhiễu tần số radio gây nhiễu. Các loại cáp xoắn:

- *Cáp có màng chắn (STP):* Loại cáp STP thường có tốc độ truyền vào khoảng 16 Mbps trong loại mạng Token Ring. Với chiều dài 100 m tốc độ đạt 155 Mbps (lý thuyết là 500 Mbps). Suy hao cho phép khoảng 100 m, đặc tính EMI cao. Giá thành cao hơn cáp Thin Ethernet, cáp xoắn trần, nhưng lại rẻ hơn giá thành loại cáp Thick Ethernet hay cáp sợi quang. Cài đặt đòi hỏi tay nghề và kỹ năng cao.

- *Loại cáp không có vỏ bọc UTP (Unshield Twisted Pair):* Cáp trần không có khả năng chống nhiễu, tốc độ truyền khoảng 100 Mbps. Đặc tính suy hao như cáp đồng, giới hạn độ dài tối đa 100m. Do thiếu màng chắn nên rất nhạy cảm với EMI, không phù hợp với môi trường các nhà máy. Được dùng phổ biến cho các loại mạng, giá thành hạ, dễ lắp đặt.

Cáp sợi quang (Fiber Optic Cable) rất lý tưởng cho việc truyền dữ liệu, băng thông có thể đạt 2 Gbps, tránh nhiễu tốt, tốc độ truyền 100 Mbps trên đoạn cáp dài vài km. Cáp sợi quang gồm một hoặc nhiều sợi quang trung tâm được bao bọc bởi một lớp vỏ nhựa phản xạ các tín hiệu trở lại, vì vậy hạn chế sự suy hao, mất mát tín hiệu. Cáp sợi quang chỉ truyền các tín hiệu quang. Các tín hiệu dữ liệu được biến đổi thành các tín hiệu quang trên đường truyền và khi nhận, các tín hiệu quang chuyển thành các tín hiệu dữ liệu. Cáp sợi quang hoạt động một trong hai chế độ: chế độ đơn (Single Mode) và đa chế độ (Multi Mode). Cài đặt cáp sợi quang đòi hỏi phải có kỹ năng cao, quy trình khó và phức tạp.

1.6.3. Các phương tiện vô tuyến

Radio: Quang phổ của điện từ nằm trong khoảng 10 KHz đến 1GHz. Có nhiều giải tần: Sóng ngắn (Short Wave), VHF (VeryHightFrequency)-Tivi&Radio FM và UHF (Ultra Hight Frequency)-Tivi

Đặc tính truyền: tần số đơn, công suất thấp không hỗ trợ tốc độ dữ liệu các mạng cục bộ LAN yêu cầu. Tần số đơn, công suất cao dễ cài đặt, băng thông cao từ 1 - 10 Mbps, suy hao chậm. Khả năng nhiễu từ thấp, bảo mật kém. Giá thành cao trung bình. Radio quang phổ trải (Spread spectrum) độ tin cậy cao, bảo mật dữ liệu. Băng thông cao, tốc độ truyền có thể đạt theo yêu cầu của các mạng cục bộ.

Viba: Truyền thông viba có hai dạng: Viba mặt đất và vệ tinh. Viba mặt đất sử dụng các trạm thu và phát. Kỹ thuật truyền thông vệ tinh sử dụng các trạm thu mặt đất (các đĩa vệ tinh) và các vệ tinh. Tín hiệu đến vệ tinh và từ vệ tinh đến trạm thu một lượt đi hoặc về 23.000 dặm. Thời gian truyền một tín hiệu độc lập với khoảng cách. Thời gian truyền tín hiệu từ vệ tinh đến các trạm nằm vòng tròn 1/3 chu vi quả đất là như nhau, gọi là trễ lan truyền (Propagation Delay). Thông thường là 0,5-5 giây.

Tia hồng ngoại (Infrared system): Có 2 phương thức kết nối mạng Point - to - Point và Multi Point. Point - to – Point tiếp sóng các tín hiệu hồng ngoại từ thiết bị này sang thiết bị khác.Giải tần từ 100 GHz đến 1000 THz, tốc độ truyền khoảng 100 Kbps-16 Mbps. Multi Point truyền đồng thời các tín hiệu hồng ngoại đến các thiết bị. Giải tần số từ 100 GHz đến 1000 THz, nhưng tốc độ truyền chỉ đạt tối đa 1 Mbps.

1.7. Phân loại mạng

1.7.1. Theo khoảng cách

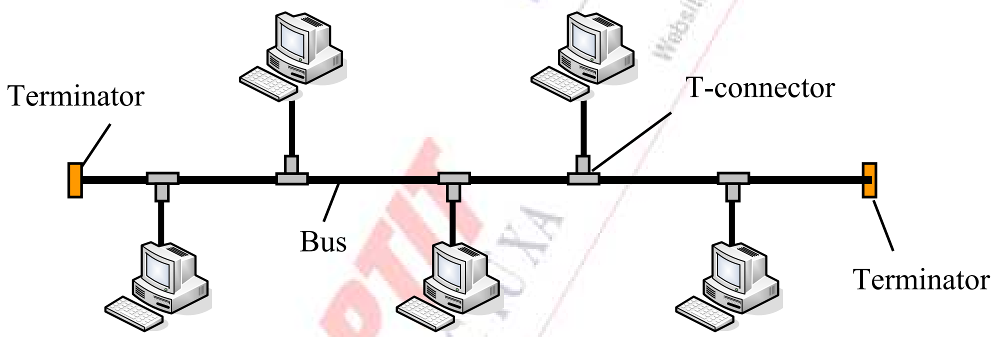
a. Mạng cục bộ LAN (Local Area Networks):

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

Quy mô của mạng nhỏ, phạm vi hoạt động vào khoảng vài km. Các máy trong một tòa nhà, một cơ quan hay xí nghiệp.. nối lại với nhau. Quản trị và bảo dưỡng mạng đơn giản.

Công nghệ truyền dẫn sử dụng trong mạng LAN thường là quảng bá (Broadcast), bao gồm một cáp đơn nối tất cả các máy. Tốc độ truyền dữ liệu cao, từ 10÷100 Mbps đến hàng trăm Gbps, thời gian trễ nhỏ (cỡ 10µs), độ tin cậy cao, tỷ số lỗi bit từ 10^{-8} đến 10^{-11}.

Cấu trúc tôpô của mạng đa dạng. Ví dụ Mạng hình BUS, hình vòng (Ring), hình sao (Star) và các loại mạng kết hợp, lai ghép.....

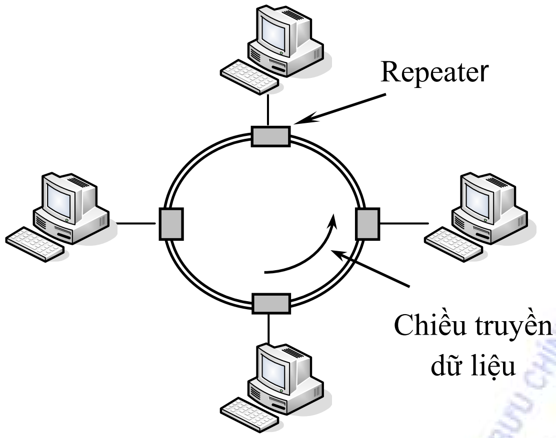


Hình 1.4 Cấu trúc mạng hình BUS

- *Mạng hình BUS* hoạt động theo kiểu quảng bá (Broadcast). Tất cả các node truy nhập chung trên một đường truyền vật lý có đầu và cuối (BUS). Chuẩn IEEE 802.3 được gọi là Ethernet, là một mạng hình BUS quảng bá với cơ chế điều khiển quảng bá động phân tán, trao đổi thông tin với tốc độ 10 Mbps hoặc 100 Mbps.

Phương thức truy nhập đường truyền được sử dụng trong mạng hình BUS hoặc TOKEN BUS, hoặc đa truy nhập sử dụng sóng mang với việc phát hiện xung đột thông tin trên đường truyền CSMA/CD (Carrier Sense Multiple Access with Collision Detection).

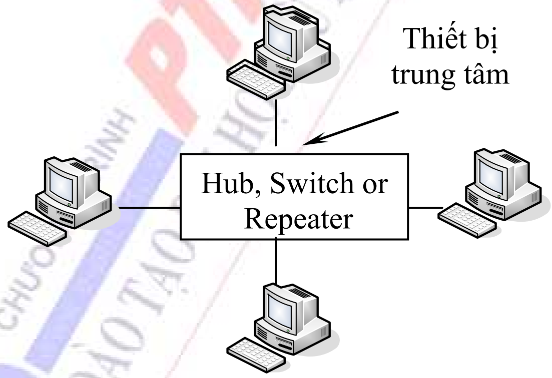
- *Mạng hình vòng (RING)* là mạng quảng bá (Broadcast), tất cả các node cùng truy nhập chung trên một đường truyền vật lý. Tín hiệu được lưu chuyển trên vòng theo một chiều duy nhất, theo liên kết điểm - điểm. Dữ liệu được chuyển một cách tuần tự từng bit quanh vòng, qua các bộ chuyển tiếp. Bộ chuyển tiếp có ba chức năng: chèn, nhận và hủy bỏ thông tin. Các bộ chuyển tiếp sẽ kiểm tra địa chỉ đích trong các gói dữ liệu khi đi qua nó.



Hình 1.5 Cấu trúc mạng hình RING

- *Mạng hình sao (Star)* các trạm kết nối với một thiết bị trung tâm có chức năng điều khiển toàn bộ hoạt động của mạng. Dữ liệu được truyền theo các liên kết điểm - điểm. Thiết bị trung tâm có thể là một bộ chuyển mạch, một bộ chọn đường hoặc đơn giản là một HUB.

- *Mạng LAN hồng ngoại (Infrared)* sử dụng sóng hồng ngoại để truyền dữ liệu. Phạm vi hoạt động của mạng bị hạn chế trong một phòng, vì tín hiệu hồng ngoại không đi xuyên qua t-ường. Có hai phương pháp kết nối điểm- điểm và kết nối quảng bá. Các mạng điểm - điểm hoạt động bằng cách chuyển tiếp các tín hiệu hồng ngoại từ một thiết bị tới thiết bị kế tiếp. Tốc độ dữ liệu đạt khoảng 100Kb/s đến 16Mb/s. Các mạng quảng bá hồng ngoại có tốc độ truyền dữ liệu thực tế chỉ đạt dưới 1Mb/s.



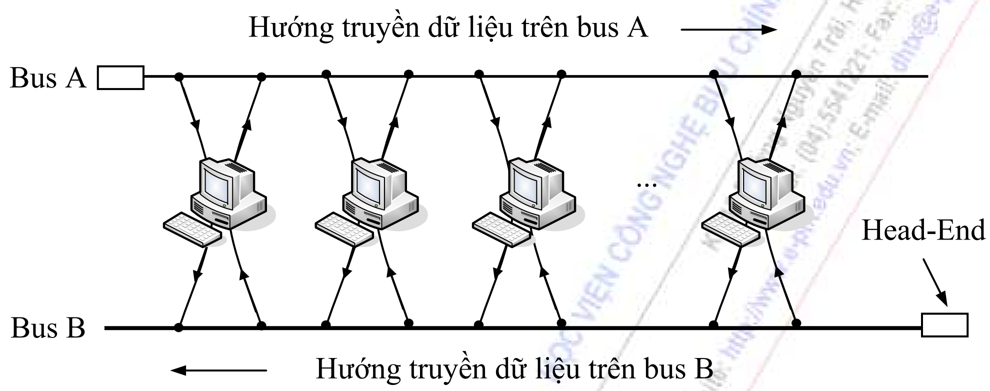
Hình 1.6 Cấu trúc mạng hình sao

- *Mạng LAN trải phổ (Spread spectrum)* Sử dụng kỹ thuật trải phổ, thường dùng trong công nghiệp và y tế.

- *Mạng LAN vi ba băng hẹp:* Hoạt động với tần số vi ba nhưng không trải phổ. Có hai dạng truyền thống: vi ba mặt đất và vệ tinh. Các hệ thống vi ba mặt đất thường hoạt động ở băng tần 4-6 GHz và 21- 23 GHz, tốc độ truyền dữ liệu khoảng vài chục Mbps.

b. Mạng đô thị MAN (Metropolitan Area Networks)

Mạng đô thị MAN hoạt động theo kiểu quảng bá, LAN to LAN. Mạng cung cấp các dịch vụ thoại và phi thoại và truyền hình cáp. Trong một mạng MAN, có thể sử dụng một hoặc hai đường truyền vật lý và không chứa thực thể chuyển mạch. Dựa trên tiêu chuẩn DQDB (Distributed Queue Dual Bus - IEEE 802.6) quy định 2 cáp đơn kết nối tất cả các máy tính lại với nhau, các máy bên trái liên lạc với các máy bên phải thông tin vận chuyển trên đường BUS trên. Các máy bên trái liên lạc với các máy bên phải, thông tin đi theo đường BUS dưới.

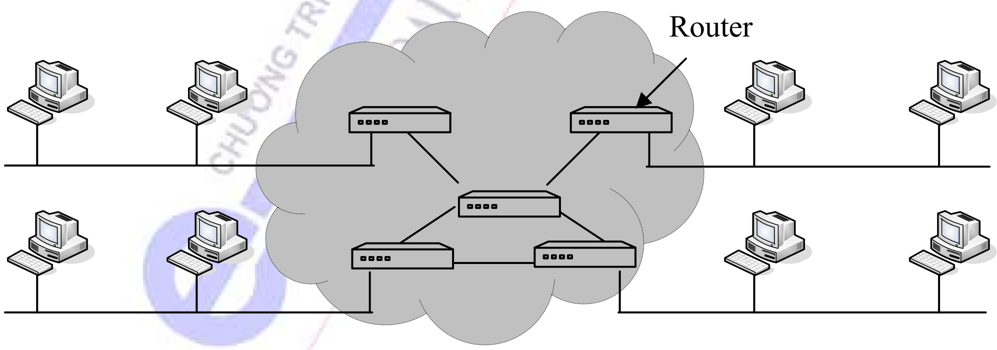


Hình 1.7: Cấu trúc mạng đô thị MAN

c. Mạng diện rộng WAN (Wide Area Networks)

Đặc trưng cơ bản của một mạng WAN:

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



Hình 1.8: Cấu trúc một mạng diện rộng WAN

Một số mạng diện rộng điển hình

- Mạng tích số hợp đa dịch vụ ISDN (Integrated Services Digital Network)

- Mạng X25 và chuyển mạch khung Frame Relay
- Phương thức truyền không đồng bộ ATM (Asynchronous Transfer Mode)
- Mạng hội tụ- mạng thế hệ sau NGN (Next Generation Network)

d. Kết nối liên mạng (Internet Connectivity)

Nhu cầu trao đổi thông tin và chia sẻ tài nguyên chung đòi hỏi các hoạt động truyền thông cần thiết phải kết nối nhiều mạng thành một mạng lớn, gọi là liên mạng.

Liên mạng (internet) là mạng của các mạng con, là một tập các mạng LAN, WAN, MAN độc lập được kết nối lại với nhau. Kết nối liên mạng có một số lợi ích sau:

Giảm lưu thông trên mạng: Các gói tin thường được lưu chuyển trên các mạng con và các gói tin lưu thông trên liên mạng khi các mạng con liên lạc với nhau.

Tối ưu hoá hiệu năng: Giảm lưu thông trên mạng là tối ưu hiệu năng của mạng, tuy nhiên máy chủ (Server Load) sẽ phải tăng tải khi nó được sử dụng như một Router.

Đơn giản hoá việc quản trị mạng: Có thể xác định các sự cố kỹ thuật và cô lập dễ dàng hơn trong một mạng có quy mô nhỏ, thường là trong một mạng cục bộ chẳng hạn.

Hiệu quả hơn so với mạng WAN có phạm vi hoạt động lớn, chi phí giảm, hiệu năng liên mạng tăng và độ phức tạp của việc quản lý nhỏ hơn.

Một trong những chức năng chủ yếu của các thiết bị kết nối liên mạng là chức năng định tuyến (Routing). Có 3 phương thức kết nối liên mạng cơ bản:

- Kết nối các mạng LAN thuần nhất tại tầng vật lý tạo ra liên mạng có phạm vi hoạt động rộng và tăng số lượng các node trên mạng, giảm bớt lưu lượng trên mỗi mạng con, hạn chế tắc nghẽn và đụng độ thông tin. Các mạng con hoạt động hiệu quả hơn.
- Kết nối các mạng LAN không thuần nhất tại tầng 2 (Data Link) tạo ra một liên mạng bao gồm một số mạng LAN cục bộ kết nối với nhau bằng các bộ chuyển mạch đến các máy chủ cô lập với tốc độ cao.
- Kết nối các mạng LAN các kiểu khác nhau tại tầng 3 (Network Layer) tạo ra một mạng WAN đơn. Các node chuyển mạch kết nối với nhau theo một cấu trúc lưới. Mỗi một node chuyển mạch cung cấp dịch vụ cho tập hợp các thiết bị đầu cuối (DTE) của nó.

1.7.2. Mạng chuyển mạch kênh (Circuit Switched Networks)

- Trước khi trao đổi thông tin, hệ thống sẽ thiết lập kết nối giữa 2 thực thể bằng một đường truyền vật lý. Thực thể đích nếu bận, kết nối này sẽ bị huỷ bỏ.
- Duy trì kết nối trong suốt quá trình 2 thực thể trao đổi thông tin.
- Giải phóng kết nối: Sau khi truyền xong dữ liệu, kết nối sẽ được huỷ bỏ, giải phóng các tài nguyên đã bị chiếm dụng để sẵn sàng phục vụ cho các yêu cầu kết nối khác.

Nhược điểm là cần nhiều thời gian để thiết lập kênh truyền, vì vậy thời gian thiết lập kênh chậm và xác suất kết nối không thành công cao. Khi cả hai không còn thông tin để truyền, kênh bị bỏ không trong khi các thực thể khác có nhu cầu.

1.7.3. Mạng chuyển mạch gói (Packet Switched Networks)

Nguyên lý chuyển mạch gói: Thông điệp (Message) của người sử dụng được chia thành nhiều gói nhỏ (Packet) có độ dài quy định. Độ dài gói tin cực đại (Maximum Transfer Unit) MTU trong các mạng khác nhau là khác nhau. Các gói tin của một thông điệp có thể truyền độc lập trên nhiều tuyến hướng đích và các gói tin của nhiều thông điệp khác nhau có thể cùng truyền trên một tuyến liên mạng. Tại mỗi node, các gói tin được tiếp nhận, lưu trữ, xử lý tại bộ nhớ, không cần phải lưu trữ tạm thời trên bộ nhớ ngoài (như đĩa cứng) và được chuyển tiếp đến node kế tiếp. Định tuyến các gói tin qua mạng nhanh hơn và hiệu quả hơn.

Kỹ thuật chuyển mạch gói có nhiều ưu điểm hơn so với chuyển mạch kênh:

- Các gói tin lưu chuyển hướng đích độc lập, trên một đường có thể chia sẻ cho nhiều gói tin. Vì vậy hiệu suất đường truyền cao hơn.
- Các gói tin được xếp hàng và truyền qua tuyến kết nối.
- Hai thực thể có tốc độ dữ liệu khác nhau có thể trao đổi các gói với tốc độ phù hợp.
- Trong mạng chuyển mạch kênh, khi lưu lượng tăng thì mạng từ chối thêm các yêu cầu kết nối (do nghẽn) cho đến khi giảm xuống. Trong mạng chuyển mạch gói, các gói tin vẫn được chấp nhận, nhưng trễ phân phát gói tin có thể tăng lên.

Các công nghệ chuyển mạch gói: Nếu một thực thể gửi một gói dữ liệu qua mạng có độ dài lớn hơn kích thước gói cực đại MTU, nó sẽ được chia thành các gói nhỏ có độ dài quy định và gửi lên mạng. Có hai kỹ thuật được sử dụng trong các mạng chuyển mạch gói là kỹ thuật *datagram* trong mạng không liên kết (Connectionless) và kỹ thuật *kênh ảo* cho mạng hướng liên kết (Connection- Oriented).

- Phương thức datagram sử dụng trong mạng không liên kết: Mỗi một gói tin được lưu chuyển và xử lý độc lập, không cần tham chiếu đến các gói tin đã gửi trước. Mỗi một gói tin được xem như là một datagram.

Ưu, nhược điểm của phương thức datagram: Giai đoạn thiết lập và giải phóng kết nối sẽ được bỏ qua. Phù hợp với yêu cầu truyền khối lượng dữ liệu không lớn trong thời gian ngắn. Phương thức linh hoạt hơn so với phương thức kênh ảo. Nếu xảy ra nghẽn thông tin, các datagram có thể được định tuyến ra khỏi vùng nghẽn. Và nếu có node bị hỏng, các gói tin tự tìm một tuyến khác để lưu chuyển hướng đích, việc phân phát các gói tin tin cậy hơn.

Phương thức kênh ảo VC (Virtual Circuit) sử dụng trong mạng hướng liên kết: Trước khi trao đổi thông tin, hai thực thể tham gia truyền thông đàm phán với nhau về các tham số truyền thông như kích thước tối đa của gói tin, các cửa sổ, đường truyền.... Một kênh ảo đã được hình thành thông qua liên mạng và tồn tại cho đến khi các thực thể ngừng trao đổi với nhau. Tại một thời điểm, có thể có nhiều kênh ảo đi và đến từ nhiều hướng khác nhau. Các gói tin vẫn được đệm tại mỗi node và được xếp hàng đầu ra trên một đường truyền, các gói tin của các thông điệp khác trên kênh ảo khác có thể chia sẻ sử dụng đường truyền này.

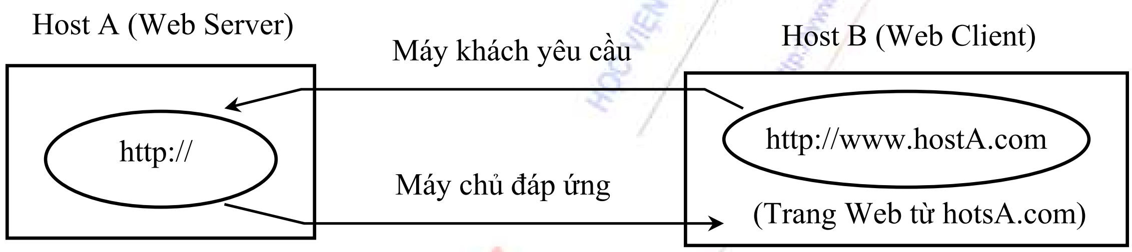
Ưu, nhược điểm của phương pháp kênh ảo: Mạng có thể cung cấp các dịch vụ kênh ảo, bao gồm việc điều khiển lỗi và thứ tự các gói tin. Tất cả các gói tin đi trên cùng một tuyến sẽ đến theo thứ tự ban đầu. Điều khiển lỗi đảm bảo không chỉ các gói đến đích theo đúng thứ tự mà cho tất cả các gói không bị lỗi. Một ưu điểm khác là các gói tin lưu chuyển trên mạng sẽ nhanh hơn vì không cần phải định tuyến tại các node. Tuy nhiên sẽ khó khăn hơn việc thích ứng với nghẽn. Nếu có node bị hỏng thì tất cả các kênh ảo qua node đó sẽ bị mất, việc phân phát datagram càng khó khăn hơn, độ tin cậy không cao.

1.8. Các mô hình xử lý dữ liệu

1.8.1. Mô hình Client-Server

Mô hình Client/Server mô tả các dịch vụ mạng và các ứng dụng được sử dụng để truy nhập các dịch vụ. Là mô hình phân chia các thao tác thành hai phần: phía Client cung cấp cho người sử dụng một giao diện để yêu cầu dịch vụ từ mạng và phía Server tiếp nhận các yêu cầu từ phía Client và cung cấp các dịch vụ một cách thông suốt cho người sử dụng.

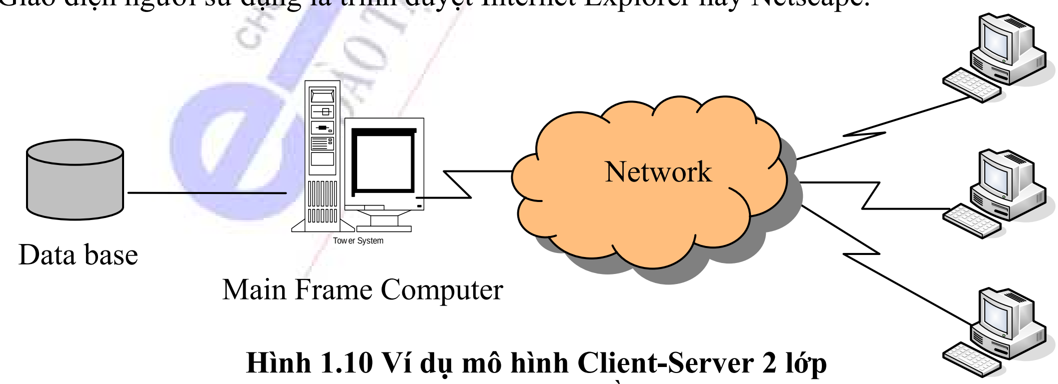
Chương trình Server được khởi động trên một máy chủ và ở trạng thái sẵn sàng nhận các yêu cầu từ phía Client. Chương trình Client cũng được khởi động một cách độc lập với chương trình Server. Yêu cầu dịch vụ được chương trình Client gửi đến máy chủ cung cấp dịch vụ và chương trình Server trên máy chủ sẽ đáp ứng các yêu cầu của Client. Sau khi thực hiện các yêu cầu từ phía Client, Server sẽ trở về trạng thái chờ các yêu cầu khác.



Hình 1.9: Mô hình chủ /khách (Client / Server)

Trong mô hình Client/Server nhiều lớp, quá trình xử lý được phân tán trên 3 lớp khác nhau với các chức năng riêng biệt. Mô hình này thích hợp cho việc tổ chức hệ thống thông tin trên mạng Internet/ Intranet. Phát triển mô hình 3 lớp sẽ khắc phục được một số hạn chế của mô hình 2 lớp. Các hệ cơ sở dữ liệu được cài đặt trên các máy chủ Web Server và có thể được truy nhập không hạn chế các ứng dụng và số lượng người dùng.

Lớp khách (Clients) cung cấp dịch vụ trình bày (Presentation Services), giao tiếp người sử dụng với lớp giao dịch thông qua trình duyệt Browser hay trình ứng dụng để thao tác và xử lý dữ liệu. Giao diện người sử dụng là trình duyệt Internet Explorer hay Netscape.



Hình 1.10 Ví dụ mô hình Client-Server 2 lớp

1. Trình duyệt Browser gửi yêu cầu cho Web Server.

2. Web Server trả kết quả về cho trình duyệt

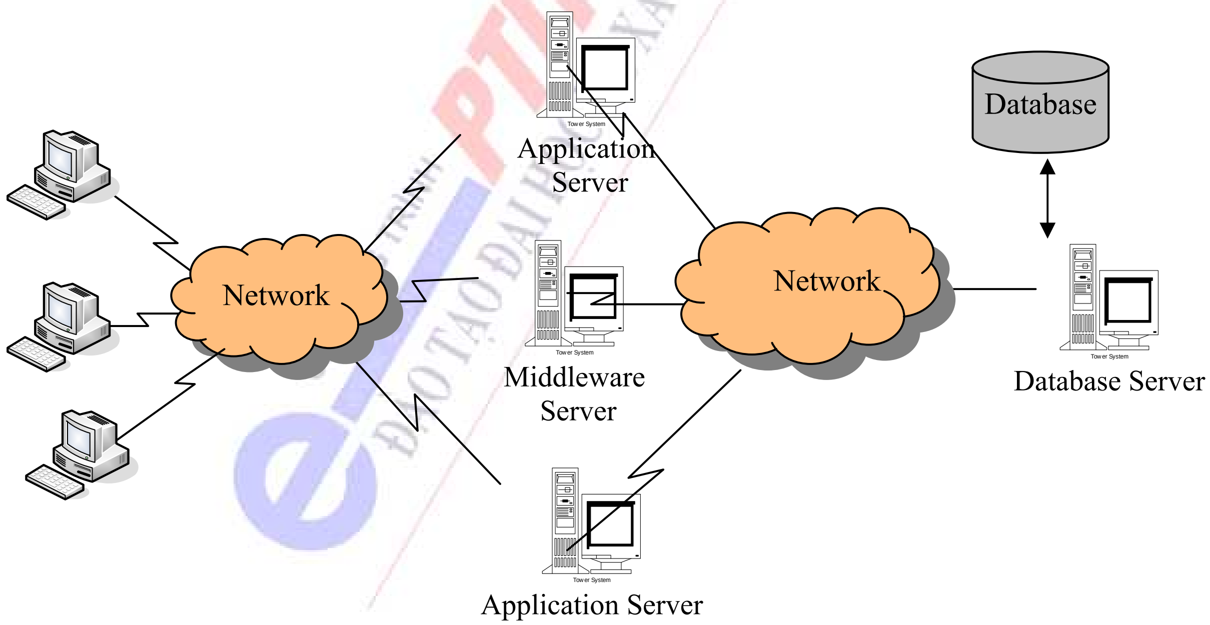
Lớp giao dịch (Business) cung cấp các dịch vụ quản trị, tổ chức và khai thác cơ sở dữ liệu. Các componenet trước đây được cài đặt trên lớp khách, nay được cài đặt trên lớp giao dịch. Ví dụ, một người sử dụng trên máy khách đặt mua hàng, lớp giao dịch kiểm tra mã mặt hàng để quyết định tiếp tục bán hay không bán. Thành phần của lớp giao dịch trong mô hình Internet là Web Server và COM+/MTS. Công nghệ của Microsoft với Web Server là IIS (Internet Information Services) sử dụng ASP để kết nối Client với COM. Web Server giao tiếp với COM+/MTS component qua COM. COM+/MTS component điều khiển tất cả giao tiếp với lớp dữ liệu nguồn thông qua ODBC hoặc OLE - DB.

Lớp nguồn dữ liệu (Data Source) cung cấp các dịch vụ tổ chức và lưu trữ các hệ cơ sở dữ liệu quan hệ. Sẵn sàng cung cấp dữ liệu cho lớp giao dịch. Đặc trưng của lớp này là ngôn ngữ tìm kiếm, truy vấn dữ liệu SQL.

1.8.2. Mô hình ngang hàng (Peer-to-Peer)

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

Mô hình lai (Hybrid): Sự kết hợp giữa Client-Server và Peer-to-Peer. Phần lớn các mạng máy tính trên thực tế thuộc mô hình này.



Hình 1.11 Mô hình Client-Server nhiều lớp

Câu hỏi trắc nghiệm:

1. Hãy chọn câu đúng nhất về định nghĩa mạng máy tính:
   A. Tập các máy tính kết nối với nhau bằng đường truyền vật lý.
   B. Tập các máy tính kết nối với nhau và hoạt động tuân theo tập giao thức.
   C. Tập các máy tính kết nối với nhau bằng các đường truyền vật lý và hoạt động theo một kiến trúc mạng xác định
2. Mục tiêu kết nối mạng máy tính:
   A. Chia sẻ tài nguyên mạng, nâng cao độ tin cậy, chinh phục khoảng cách.
   B. Chia sẻ phần cứng, phần mềm, nâng cao độ tin cậy, chinh phục khoảng cách.
   C. Chia sẻ thông tin, nâng cao độ tin cậy, chinh phục khoảng cách.
   D. Cung cấp các dịch vụ mạng đa dạng, chia sẻ tài nguyên, nâng cao độ tin cậy, chinh phục khoảng cách và giảm bớt các chi phí về đầu tư .
3. Các xu hướng phát triển dịch vụ mạng máy tính:
   A. Cung cấp các dịch vụ truy nhập vào các nguồn thông tin ở xa
   B. Phát triển các dịch vụ tương tác giữa người với người trên phạm vi diện rộng.
   C. Xu hướng phát triển các dịch vụ giải trí trực tuyến (Online) hiện đại.
   D. Cả 3 câu trên.
4. Mạng có cấu trúc điểm- điểm (Point to Point) là:
   A. Mạng lưu và gửi tiếp (Store - and - Forward).
   B. Nối từng cặp node lại với nhau theo một hình học xác định.
   C. Các node trung gian: tiếp nhận, lưu trữ tạm thời và gửi tiếp thông tin
5. Nhược điểm của mạng có cấu trúc điểm- điểm (Point to Point) là:
   A. Khả năng đụng độ thông tin (Collision) thấp.
   B. Hiệu suất sử dụng đường truyền thấp. Chiếm dụng nhiều tài nguyên
   C. Độ trễ lớn, tốn nhiều thời gian để thiết lập đường truyền và xử lý tại các node.
   D. Tốc độ trao đổi thông tin thấp.
6. Đặc trưng của mạng quảng bá (Point to Multipoint, Broadcasting)
   A. Tất cả các node cùng truy nhập chung trên một đường truyền vật lý.
   B. Nối từng cặp node lại với nhau theo một hình học xác định.
   C. Các node trung gian: tiếp nhận, lưu trữ tạm thời và gửi tiếp thông tin
7. Chức năng giao thức:
   A. Đóng gói, phân đoạn và hợp lại
   B. Điều khiển liên kết và giám sát.
   C. Điều khiển lưu lượng và điều khiển lỗi.
   D. Đồng bộ hoá và địa chỉ hoá.

E. Tất cả các khẳng định trên.

8. Đặc trưng cơ bản của đường truyền
   A. Băng thông (Bandwidth).
   B. Thông lượng (Throughput)
   C. Suy hao (Attenuation)
   D. Tốc độ truyền dẫn.
9. Mạng cục bộ LAN (Local Area Networks):
   A. Quy mô của mạng nhỏ, phạm vi khoảng vài km.
   B. Công nghệ truyền dẫn sử dụng thường là quảng bá (Broadcast)
   C. Tốc độ truyền dữ liệu cao, từ 10÷100 Mbps đến hàng trăm Gbps,
   D. Thời gian trễ cỡ 10μs , độ tin cậy cao, tỷ số lỗi bit từ 10^{-8} đến 10^{-11}.
   E. Cấu trúc tôpô của mạng đa dạng.
   F. Tất cả các khẳng định trên.
10. Đặc trưng cơ bản của một mạng WAN:
    A. Hoạt động trên phạm vi một quốc gia hoặc trên toàn cầu.
    B. Tốc độ truyền dữ liệu thấp so với mạng cục bộ.
    C. Lỗi truyền cao.
    D. Tất cả các khẳng định trên.
11. Lợi ích khi kết nối liên mạng:
    A. Giảm lưu thông trên mạng
    B. Tối ưu hoá hiệu năng
    C. Đơn giản hoá việc quản trị mạng
    D. Hiệu quả hơn so với mạng WAN có phạm vi hoạt động lớn.
12. Mạng chuyển mạch kênh (Circuit Switched Networks)
    A. Thiết lập kết nối vật lý giữa 2 thực thể, duy trì kết nối trong quá trình trao đổi thông tin và giải phóng kết nối khi truyền xong dữ liệu.
    B. Thiết lập kết nối logic giữa 2 thực thể , duy trì kết nối trong quá trình trao đổi thông tin và giải phóng kết nối khi truyền xong dữ liệu.
    C. Truyền dữ liệu giữa 2 thực thể.
13. Khẳng định đúng nhất trong mạng chuyển mạch gói (Packet Switched Networks):
    A. Gói tin lưu chuyển trên các kết nối logic.
    B. Gói tin lưu chuyển trên các kết nối vật lý.
    C. Gói tin lưu chuyển độc lập hướng đích.
    D. Các gói tin lưu chuyển hướng đích độc lập và trên một đường có thể chia sẻ cho nhiều gói tin.

14. Độ dài gói tin cực đại MTU (Maximum Transfer Unit)
    A. Trong các mạng khác nhau là khác nhau.
    B. Trong các mạng khác nhau là như nhau.
    C. Trong các mạng không quan tâm đến độ dài gói tin
15. Hãy chọn những khẳng định đúng sau:
    A. Kỹ thuật datagram sử dụng trong các mạng không liên kết (Connectionless)
    B. Kỹ thuật datagram sử dụng trong các mạng hướng liên kết (Connection- Oriented). Kỹ thuật datagram sử dụng trong các mạng chuyển mạch kênh.
    C. Kỹ thuật datagram sử dụng trong các mạng chuyển gói X25.
16. Hãy chọn những khẳng định đúng sau:
    A. Kỹ thuật kênh ảo VC (Virtual Circuit) sử dụng trong các mạng không liên kết
    B. Kỹ thuật kênh ảo VC sử dụng trong các mạng hướng liên kết
    C. Kỹ thuật kênh ảo VC sử dụng trong các mạng chuyển mạch kênh.
    D. Kỹ thuật kênh ảo VC sử dụng trong các mạng chuyển gói X25.

Câu hỏi

1. Hãy trình bày mục tiêu và ứng dụng mạng máy tính.
2. Hãy phát biểu các lợi ích khi nối máy tính thành mạng.
3. Hãy trình bày tổng quát về xu hướng phát triển các dịch vụ mạng.
4. Hiểu thế nào là mạng máy tính. Hãy trình bày tóm tắt chức năng các thành phần chủ yếu của một mạng máy tính ?.
5. Hãy trình bày khái quát về các đặc trưng cơ bản của đường truyền: Băng thông (bandwidth), thông lượng (throughput) và suy hao (attenuation).
6. Khái quát các đặc trưng cơ bản của các phương tiện truyền: Cáp đồng trục (Coaxial cable), cáp xoắn đôi (Twisted pair cable), cáp sợi quang (Fiber optic cable).
7. Hãy trình bày cấu trúc kiểu điểm - điểm (Point to Point).
8. Trong kỹ thuật chuyển mạch kênh, vai trò địa chỉ như thế nào ?.
9. Hãy trình bày kiểu quảng bá (Point to Multipoint, Broadcast).
10. Trình bày ưu, nhược điểm các phương thức quảng bá tĩnh và động, Quảng bá động tập trung và phân tán ?.
11. Những khác biệt cơ bản giữa kiểu điểm - điểm và quảng bá ?.
12. Hiểu thế nào là giao thức, vai trò của giao thức trong truyền thông ?.
13. Trình bày các chức năng của giao thức.
14. Mạng cục bộ LAN (Local Area Networks) và các đặc trưng cơ bản của nó
15. Hãy trình bày cấu trúc mạng hình BUS, RING và STAR.
16. Sự khác nhau cơ bản giữa mạng hình BUS và mạng hình RING ?.

17. Hãy trình bày những đặc trưng cơ bản của các mạng LAN không dây ?.
18. Mạng đô thị MAN (Metropolitan Area Networks) và đặc trưng cơ bản của nó.
19. Mạng diện rộngWAN và những đặc trưng của mạng diện rộng.
20. Hiểu thế nào là liên mạng (Internetworking). Mạng WAN là một liên mạng ?.
21. Chức năng của các thiết bị kết nối liên mạng.
22. HUB là thiết bị kết nối liên mạng ?.
23. Chức năng của bộ định tuyến ROUTER. Có thể thay thế HUB trong kết nối liên mạng. Ví dụ minh họa ?.
24. Hiểu thế nào là dịch vụ hướng liên kết (Connection - Oriented) và không liên kết (Connectioless). Hãy cho thí dụ minh họa.
25. Nguyên tắc hoạt động của mạng chuyển mạch kênh (Circuit Switched Networks).
26. Trình bày ưu, nhược điểm của kỹ thuật chuyển mạch kênh.
27. Trình bày nguyên tắc hoạt động của mạng chuyển mạch gói (Packet Switched Networks).
28. Vì sao nói kỹ thuật chuyển mạch gói có hiệu suất kênh truyền cao, vì sao ?.
29. Ưu nhược điểm của kỹ thuật chuyển nạch gói ?.
30. Nói mạng chuyển mạch gói là mạng X25 ?.
31. Kỹ thuật chuyển mạch gói nhiều ưu điểm hơn kỹ thuật chuyển mạch kênh, vì sao ?.
32. Trình bày phương thức Datagram.
33. Trình bày phương thức kênh ảo VC (Virtual circuit)
34. So sánh ưu, nhược của phương pháp kênh ảo và Datagram.
35. Phương thức kênh ảo và chuyển mạch kênh khác nhau, giống nhau ?.
36. Vì sao mạng chuyển mạch gói có tốc độ trao đổi thông tin nhanh hơn tốc độ trao đổi thông tin trong mạch chuyển mạch tin báo.
37. Hiểu thế nào là cấu trúc mạng Client/Server, Peer to Peer ?

CHƯƠNG II: KIẾN TRÚC MẠNG VÀ MÔ HÌNH KẾT NỐI CÁC HỆ THỐNG MỞ OSI

Nội dung của chương này sẽ trình bày các khái niệm về kiến trúc phân tầng và mô hình kết nối các hệ thống mở OSI (Open System Interconnection) với mục tiêu kết nối các sản phẩm của các hãng sản xuất khác nhau. Mô hình OSI là giải pháp cho các vấn đề truyền thông giữa các máy tính và được thiết kế theo quan điểm có cấu trúc đa tầng. Mỗi một tầng thực hiện một số chức năng truyền thông, các tầng được xếp chồng lên nhau, gọi là chồng giao thức, thực hiện các tiến trình truyền thông hoàn chỉnh. Giữa các tầng kề nhau được xác định bởi giao diện bằng các hàm dịch vụ nguyên thuỷ. Nội dung gồm các phần như sau:

- Các tổ chức chuẩn hóa mạng
- Mô hình kiến trúc đa tầng và các quy tắc phân tầng.
- Mô hình kết nối các hệ thống mở OSI .
- Những vấn đề cơ bản thiết kế mô hình kiến trúc.
- Đánh giá độ tin cậy của mạng.
- Một số mô hình kiến trúc chuẩn khác.

2.1. Các tổ chức tiêu chuẩn hóa mạng máy tính

2.1.1. Cơ sở xuất hiện kiến trúc đa tầng

Sự khác biệt về kiến trúc mạng đã gây trở ngại cho người sử dụng khi kết nối liên mạng, ảnh hưởng đến sức sản xuất và tiêu thụ các sản phẩm về mạng. Cần xây dựng mô hình chuẩn làm cơ sở cho các nhà nghiên cứu và thiết kế mạng tạo ra các sản phẩm mở về mạng và tạo điều kiện cho việc phát triển và sử dụng mạng. Vì vậy các tổ chức tiêu chuẩn quốc tế đã ra đời. Các nhà sản xuất đã có tiếng nói chung cho các sản phẩm của họ, đó là các chuẩn, các khuyến nghị quy định thiết kế và sản xuất các sản phẩm mạng.

2.1.2. Các tổ chức tiêu chuẩn

ISO (International Standards Organization): Tổ chức tiêu chuẩn quốc tế hoạt động dưới sự bảo trợ của Liên Hiệp Quốc. Chia thành nhiều ban kỹ thuât- Technical Commitee- ký hiệu là TC, trong đó ban TC97 đảm nhận việc nghiên cứu chuẩn hoá xử lý thông tin. Các sản phẩm của nó gọi là các chuẩn- Standard - Mô hình OSI - Open Systems Interconnection là sản phẩm điển hình của tổ chức này.

CCITT (*International Telegraphand Telephone Consultative Commintte*): Uỷ ban tư vấn điện tín & điện thoại quốc tế nay là Hiệp hội Viễn thông quốc tế ITU *(International Telecommunication Union).* Là tổ chức bao gồm các cơ quan Bưu chính Viễn thông của các nước. Các sản phẩm được gọi là các khuyến nghị (Recommendation):

- *Khuyến nghị loại V*: Tập các tiêu chuẩn về truyền dữ liệu bằng Modem: V21 tốc độ 300 bps, V32 tốc độ 9600 - 14.400 bps, V90, V92 cho tốc độ 56 Kbps.

- *Khuyến nghị loại X:* Tập các tiêu chuẩn liên quan đến mạng truyền số liệu. Quy định các thủ tục giao diện người sử dụng và giao diện mạng: X21, X25,...

- *Khuyến nghị loại* I: Các tiêu chuẩn liên quan đến mạng ISDN

- *IEEE (Institute of Electronical And Electronic Engineers)*: Viện các kỹ sư điện và điện tử. Tập các thủ tục tầng vật lý.

2.2. Mô hình kiến trúc đa tầng

Các mạng máy tính được thiết kế và cài đặt theo quan điểm có cấu trúc đa tầng. Mỗi một thành phần của mạng được xem như một hệ thống gồm nhiều tầng và mỗi một tầng bao gồm một số chức năng truyền thông. Các tầng được chồng lên nhau, số lượng và chức năng của các tầng phụ thuộc vào các nhà sản xuất và thiết kế. Tuy nhiên quan điểm chung là trong mỗi tầng có nhiều thực thể (các tiến trình) thực hiện một số chức năng nhằm cung cấp một số dịch vụ, thủ tục cho các thực thể tầng trên hoạt động.

2.2.1. Các quy tắc phân tầng

Tổ chức tiêu chuẩn quốc tế ISO quy định các quy tắc phân tầng như sau:

- Không định nghĩa quá nhiều tầng, số lượng tầng, vai trò và chức năng của các tầng trong mỗi hệ thống của mạng là như nhau, không quá phức tạp khi xác định và ghép nối các tầng. Chức năng các tầng độc lập với nhau và có tính mở.

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

- Xác định mối quan hệ giữa các đồng tầng để thống nhất về các phương thức hoạt động trong quá trình truyền thông, mối quan hệ đó là tập các quy tắc và các thoả thuận trong hội thoại giữa các hệ thống, gọi là giao thức tầng.

- Dữ liệu không được truyền trực tiếp từ tầng thứ *i* của hệ thống phát sang tầng thứ *i* của hệ thống nhận (trừ tầng thấp nhất- tầng vật lý) mà được chuyển từ tầng cao xuống tầng thấp nhất bên hệ thống phát và qua đường truyền vật lý, dữ liệu là chuỗi bit không cấu trúc được truyền sang tầng thấp nhất của hệ thống nhận và từ đó dữ liệu được chuyển ngược lên các tầng trên. Giữa các đồng tầng xác định liên kết logic, giữa các tầng vật lý có liên kết vật lý.

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

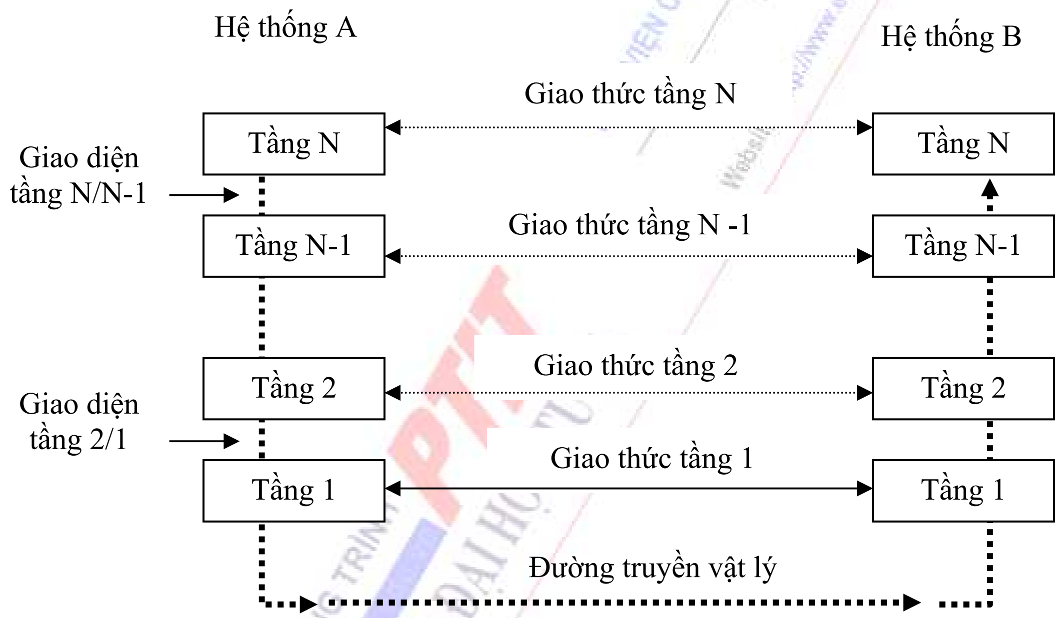
Quan hệ theo chiều ngang phản ánh sự hoạt động của các đồng tầng. Các đồng tầng trước khi trao đổi thông tin với nhau phải bắt tay, hội thoại và thỏa thuận với nhau bằng các tham số của các giao thức (hay là thủ tục), được gọi là giao thức tầng.

Quan hệ theo chiều dọc là quan hệ giữa các tầng kề nhau trong cùng một hệ thống. Giữa chúng tồn tại giao diện xác định các thao tác nguyên thủy và các dịch vụ tầng dưới cung cấp cho tầng trên. Được gọi là giao diện tầng.

Trong mỗi một tầng có một hoặc nhiều thực thể (Entity) hoạt động. Các thực thể có thể là một tiến trình (Process) trong một hệ đa xử lý, hoặc có thể là một chương trình con....Chúng thực hiện các chức năng của tầng N và giao thức truyền thông với các thực thể đồng tầng trong các hệ thống khác. Ký hiệu N_Entity là thực thể tầng N.

Các thực thể truyền thông với các thực thể tầng trên nó và các thực thể tầng dưới nó thông qua các điểm truy nhập dịch vụ trên các giao diện SAP (Service Access Point). Các thực thể phải biết nó cung cấp những dịch vụ gì cho các hoạt động tầng trên kề nó và các hoạt động truyền thông của nó được sử dụng những dịch vụ gì do tầng kề dưới nó cung cấp thông qua các lời gọi hàm qua các điểm truy nhập SAP trên giao diện các tầng.

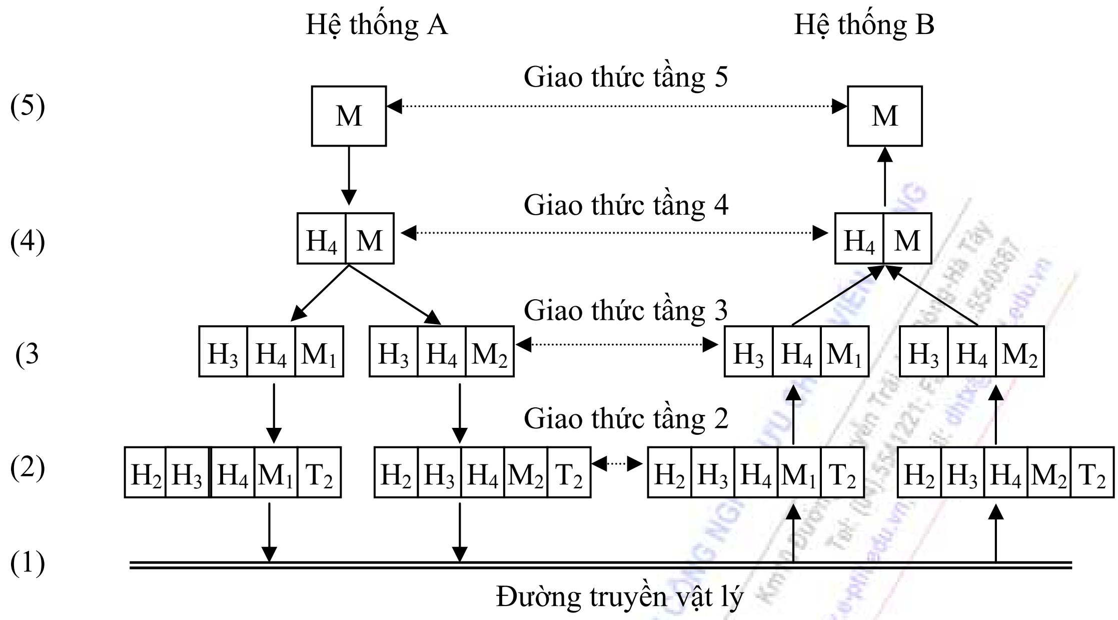
Khi mô tả hoạt động của bất kỳ giao thức nào trong mô hình OSI, cần phải phân biệt được các dịch vụ cung cấp bởi tầng kề dưới, hoạt động bên trong của tầng và các dịch vụ mà nó khai thác. Sự tách biệt giữa các tầng giúp cho việc bổ sung, sửa đổi chức năng của giao thức tầng mà không ảnh hưởng đến hoạt động của các tầng khác.



Hình 2.1 Mô hình kiến trúc phân tầng

2.2.2. Lưu chuyển thông tin trong kiến trúc đa tầng

Hình 2.2 là một ví dụ minh hoạ cho sự lưu chuyển thông tin trong mạng máy tính kết nối giữa 2 hệ thống A và B gồm N=5 tầng.



Hình 2.2 Ví dụ về lưu chuyển thông tin

2.2.3. Nguyên tắc truyền thông đồng tầng

Để truyền thông đồng tầng, gói tin khi chuyển xuống qua các tầng sẽ được bổ sung thêm vào phần đầu bằng thông tin điều khiển của tầng. Việc thêm Header vào đầu các gói tin khi đi qua mỗi tầng trong quá trình truyền dữ liệu được gọi là quá trình *Encapsulation*. Quá trình bên nhận sẽ diễn ra theo chiều ngược lại, khi đi qua các tầng, gói tin sẽ tách thông tin điều khiển thuộc nó trước khi chuyển dữ liệu lên tầng trên.

Đơn vị dữ liệu được sử dụng trong các tầng bao gồm

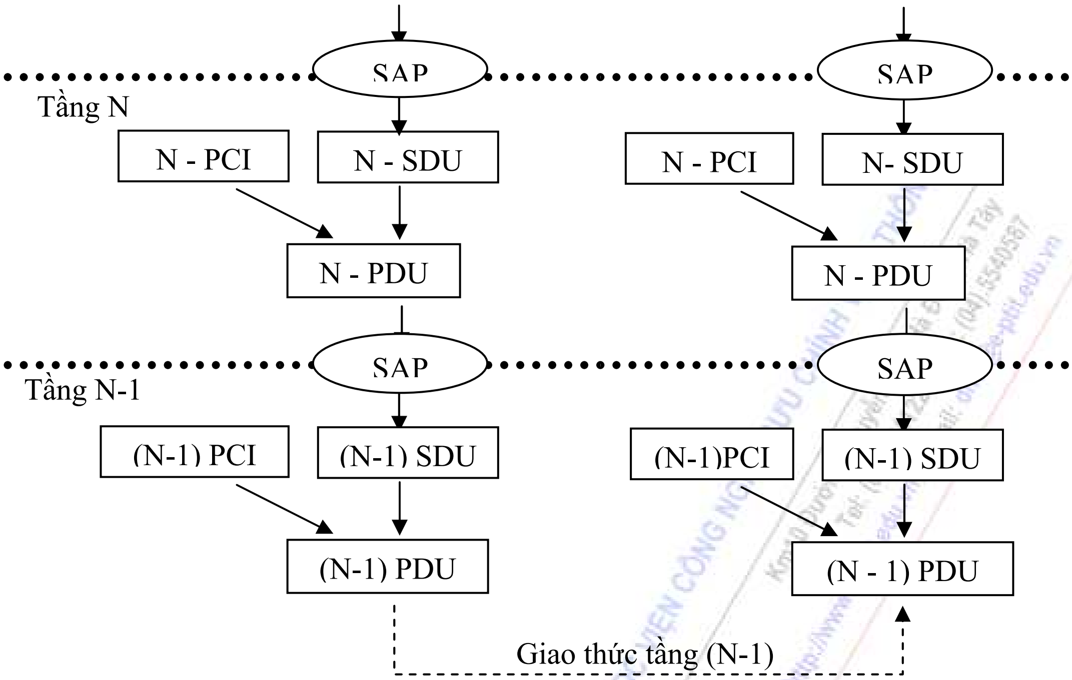
- *Thông tin điều khiển giao thức PCI (Protocol Control Information):* Thông tin được thêm vào đầu các gói tin trong quá trình hoạt động truyền thông của các thực thể. Ký hiệu N_PCI là thông tin điều khiển tầng N.

- *Đơn vị dữ liệu dịch vụ* SDU *(Service Data Unit)*: Là đơn vị dữ liệu truyền thông giữa các tầng kề nhau. Ký hiệu N_SDU là đơn vị dữ liệu truyền từ tầng (N+1) xuống tầng N chưa thêm thông tin điều khiển.

- *Đơn vị dữ liệu giao thức* PDU *(Protocol Data Unit)* : Đơn vị dữ liệu giao thức tầng. Ký hiệu PDU = PCI + SDU, nghĩa là đơn vị dữ liệu giao thức bao gồm thông tin điều khiển PCI được thêm vào đầu đơn vị dữ liệu dịch vụ SDU.

2.2.4. Giao diện tầng, quan hệ các tầng kề nhau và dịch vụ

Chức năng của các tầng là cung cấp dịch vụ cho tầng trên kề nó. Trong mỗi tầng có một hay nhiều thực thể. Thực thể ở tầng N thực hiện các dịch vụ mà tầng N+1 yêu cầu sử dụng, Các thực thể trao đổi dịch vụ với nhau qua các điểm truy cập dịch vụ SAP (Service Access Points). Các thực thể tầng N cung cấp dịch vụ cho tầng N+1 qua các SAP trên giao diện N+1/N. Mỗi một SAP có một nhận dạng duy nhất.



Hình 2.3 Khái niệm giao diện và dịch vụ trong môi trường các hệ thống mở

Hai tầng trao đổi thông tin với nhau phải có những thoả thuận về thiết lập các quy tắc giao diện. Thực thể của tầng N+1 chuyển một PDU tới thực thể tầng N qua SAP. PDU bao gồm một đơn vị dữ liệu dịch vụ SDU và thông tin điều khiển PCI. SDU là thông tin gửi qua mạng tới thực thể đồng tầng và sau đó đưa lên tầng N+1. Nếu độ dài của SDU lớn hơn độ dài quy định, các thực thể tầng N chia SDU ra nhiều gói nhỏ có độ dài quy định và thêm Header PCI vào mỗi gói tin. Header của PDU được các thực thể đồng tầng nhận dạng PDU nào chứa dữ liệu và PDU nào chứa thông tin điều khiển.....

Hình 2.3 minh hoạ giao diện và dịch vụ trong các tầng kề nhau. Như đã biết, thực thể ở tầng N từ hệ thống A không thể truyền dữ liệu trực tiếp sang tầng N của hệ thống B mà phải chuyển tuần tự xuống các tầng dưới nó, cho tới tầng thấp nhất, tầng vật lý. Bằng phương tiện truyền vật lý, dữ liệu là những chuỗi bit 0 và 1 được truyền sang tầng vật lý của hệ thống B. Từ đây dữ liệu được chuyển lên các tầng trên.

2.2.5 Dịch vụ và chất lượng dịch vụ

Tầng N sẽ phải biết sử dụng dịch vụ nào của tầng N-1 và cung cấp những dịch vụ gì cho tầng N+1. Quá trình cung cấp dịch vụ thông qua các điểm truy nhập SAP trên các giao diện tầng N/N+1. Có hai loại dịch vụ khác nhau: dịch vụ hướng liên kết (Connection Oriented) và dịch vụ không liên kết (Connectionless).

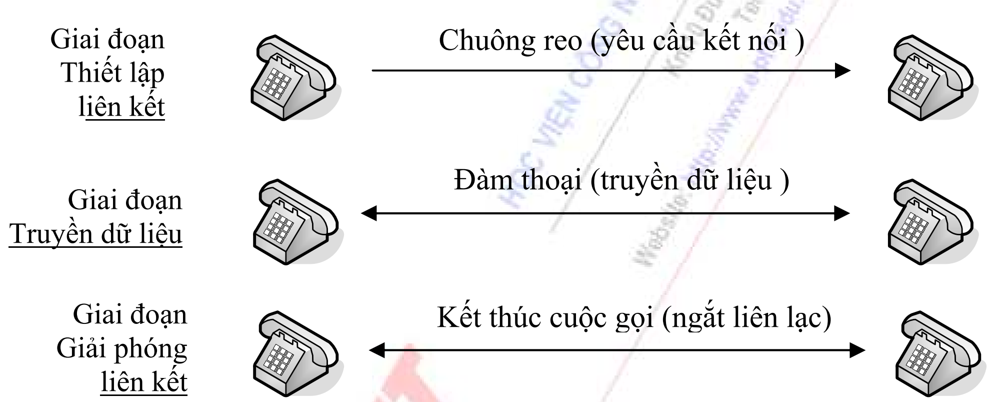
a. Dịch vụ hướng liên kết (Connection Oriented): Các dịch vụ và giao thức trong các mô hình hệ thống mở thực hiện truyền thông 3 giai đoạn theo thứ tự thời gian như sau:

Thiết lập liên kết: Một kênh logic được thiết lập giữa các thực thể đồng tầng của hai hệ thống khác nhau. Chúng sẽ đàm phán, thương lượng với nhau về tập các tham số và sử dụng các tham số này như thế nào trong quá trình truyền số liệu.

Truyền dữ liệu: Dữ liệu được truyền giữa hai tầng đồng tầng theo cơ chế kiểm soát và quản lý quá trình truyền dữ liệu, thực hiện việc ghép kênh, cắt hợp dữ liệu... bảo đảm được thứ tự truyền, phát hiện lỗi, kiểm soát luồng dữ liệu, phát hiện tắc nghẽn thông tin...nhằm tăng cường độ tin cậy cao và hiệu suất truyền.

Giải phóng liên kết: Sau khi kết thúc quá trình truyền dữ liệu, các tài nguyên của hệ thống được cấp phát cho quá trình thiết lập liên kết và truyền dữ liệu sẽ được giải phóng, sẵn sàng cấp phát cho liên kết tiếp theo.

Hình 2.4 minh họa phương thức truyền hướng liên kết trong các dịch vụ thoại.



Hình 2.4 Ví dụ hoạt động kết nối liên kết

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

Mỗi dịch vụ được đặc trưng bởi chất lượng dịch vụ. Một số dịch vụ yêu cầu có độ tin cậy cao, bằng cách yêu cầu thực thể đích gửi xác nhận phản hồi sau khi nhận gói tin. Vì vậy máy thu luôn bảo đảm gói tin đã đến đúng và không để mất dữ liệu. Xử lý xác nhận phản hồi đòi hỏi phải chèn thêm vào gói tin một số thông tin điều khiển và làm tăng thời gian trễ. Một loại dịch vụ hướng liên kết tin cậy là dịch vụ truyền file với yêu cầu mọi bit gửi đến đều chính xác và đúng thứ tự như khi gửi đi. Một số loại dịch vụ chấp nhận có một số lỗi nhưng yêu cầu yêu cầu độ trễ nhỏ như thoại số, video. Với dịch vụ loại này thì không cần xác nhận có báo nhận, nhằm để giảm thời gian trễ tại các nút.

Ngoài dịch vụ hướng liên kết và không liên kết, còn có kiểu dịch vụ hỏi-đáp. Máy gửi sẽ gửi các thông tin chứa yêu cầu xác nhận trong các gói tin và yêu cầu máy nhận trả lời. Khi máy nhận nhận được gói tin, sẽ gửi các trả lời đến máy gửi. Dịch vụ hỏi-đáp được sử dụng truyền thông trong mô hình khách-chủ (Client-Server). Máy khách (Client) gửi các yêu cầu cho máy chủ (Server) và máy chủ trả lời kết quả cho máy khách.

	Dịch vụ	Ví dụ
Hướng liên kết	Truyền/nhận các gói tin, yêu cầu có xác nhận.	Gửi các trang sách theo đúng thứ tự.
	Truyền/nhận dòng byte, yêu cầu có xác nhận.	Truy nhập và khai thác từ xa.
	Kết nối không yêu cầu có xác nhận.	Các dịch vụ thoại số
Không liên kết	Datagram không xác nhận	Thư điện tử, nhắn tin
	Datagram có xác nhận	Thư có đăng ký, thư khẩn
	Hỏi-Đáp	Câu truy vấn trong cơ sở dữ liệu

Hình 2.5 Các loại dịch vụ khác nhau hướng liên kết và không liên kết

2.2.6. Các hàm dịch vụ nguyên thuỷ (Primitive)

Việc cung cấp và nhận các dịch vụ giữa các thực thể trong các tầng kề nhau thông qua việc gọi các *hàm dịch vụ nguyên thủy*. Một dịch vụ được đặc tả hình thức bằng nhiều hàm dịch vụ nguyên thủy. Các hàm dịch vụ nguyên thủy sử dụng để định nghĩa sự tương tác giữa các tầng kề nhau, chỉ rõ chức năng cần thực hiện và sử dụng để chuyển dữ liệu và thông tin điều khiển. Cụ thể hơn, các hàm dịch vụ nguyên thủy là đặc tả các thao tác cần thực hiện một yêu cầu hay trả lời một yêu cầu của các thực thể đồng tầng.

Có bốn kiểu hàm dịch vụ nguyên thủy cơ bản:

1. Request (Yêu cầu): Được một thực thể sử dụng gọi một chức năng, yêu cầu các phương tiện cung cấp dịch vụ mạng.
2. Indication (Chỉ báo): Được một thực thể chỉ báo yêu cầu cung cấp dịch vụ. Chỉ báo yêu cầu bằng cách:

   - Gọi một chức năng nào đó.

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

Hình 2.6 minh họa nguyên lý hoạt động của các hàm dịch vụ nguyên thuỷ.

Trong hệ thống A:

- Tầng (N+1) gửi hàm Request xuống tầng N qua SAP trên giao diện (N+1)/N.

- Tại tầng N, kiến tạo một đơn vị dữ liệu gửi yêu cầu sang tầng N của hệ thống B qua giao thức tầng N.

Trong hệ thống B:

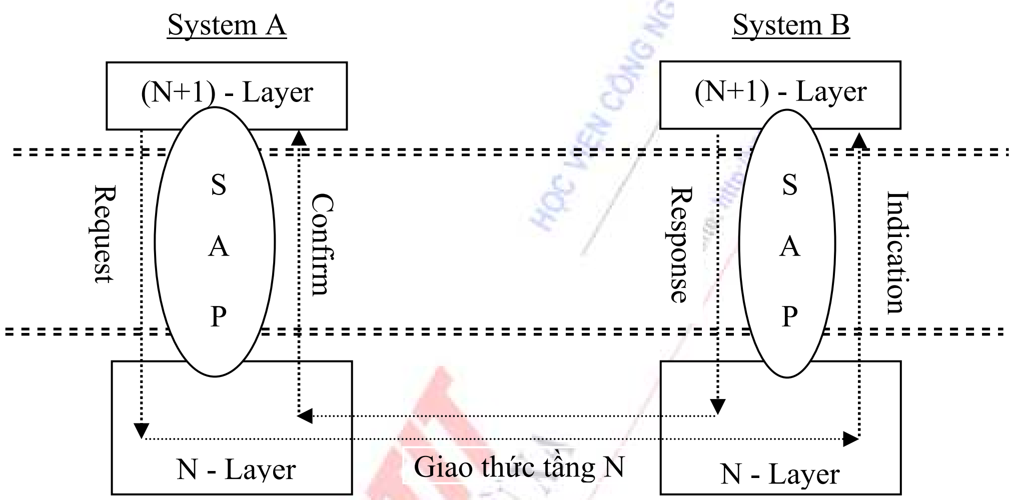
- Tầng N nhận được yêu cầu, chỉ báo- lên tầng (N+1) bằng hàm Indication qua SAP trên giao diện (N+1)/N .

- Tầng (N+1) trả lời tầng N bằng hàm Response qua SAP của giao diện 2 tầng.

- Tâng N, kiến tạo một đơn vị dữ liệu gửi trả lời sang tầng N của hệ thống A qua giao thức tầng N.

Nhận trả lời, tầng N của hệ thống A gửi xác nhận lên tâng (N+1) bằng hàm Confirm qua SAP trên giao diện. Kết thúc giao tác giữa 2 hệ thống.

Quá trình yêu cầu thiết lập liên kết giữa các thực thể đồng tầng có thể có xác nhận (Confirmed) hoặc không có xác nhận (Unconfirmed).

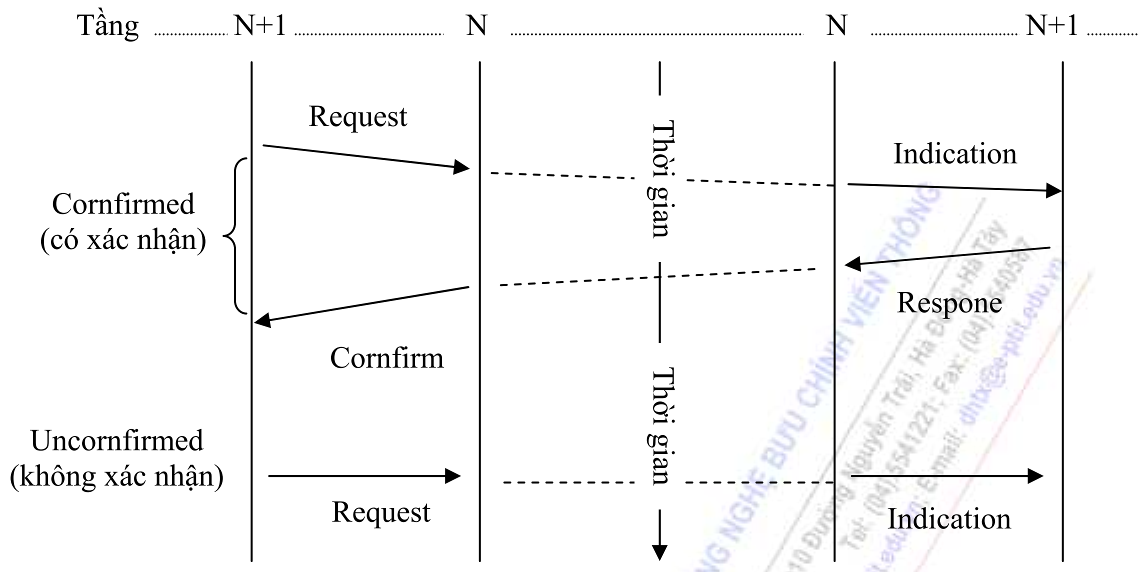


Hình 2.6 Sơ đồ nguyên lý hoạt động của các hàm nguyên thuỷ

2.2.7. Quan hệ giữa dịch vụ và giao thức

Mỗi một lớp giao thức có hai đặc trưng: đặc trưng dịch vụ và đặc trưng giao thức. Đặc trưng dịch vụ là các tham số dịch vụ trong các hàm nguyên thủy. Thông qua các tham số dịch vụ mà các tầng ở trên có thể giao tiếp với đồng tầng trong hệ thống khác. Đặc trưng giao thức bao gồm: Khuôn dạng PDU, các tham số dịch vụ sử dụng cho mỗi một loại PDU và phương thức hoạt của thực thể giao thức.

Dịch vụ và giao thức là những khái niệm khác nhau. Một *dịch vụ* là một tập các các thao tác của các thực thể (thủ tục..) của tầng cung cấp dịch vụ cho các hoạt động các thực thể của tầng trên kề nó. Dịch vụ tầng được định nghĩa trong suốt đối với đối tượng sử dụng dịch vụ. Ngược lại, một *giao thức* là một tập các quy tắc, quy ước về kết nối, ngữ nghĩa, định dạng, ý nghĩa của khung, gói hoặc bản tin… được các thực thể đồng tầng đàm phán, thương lượng với nhau. Các thực thể sử dụng giao thức để thực hiện sự xác định các dịch vụ.

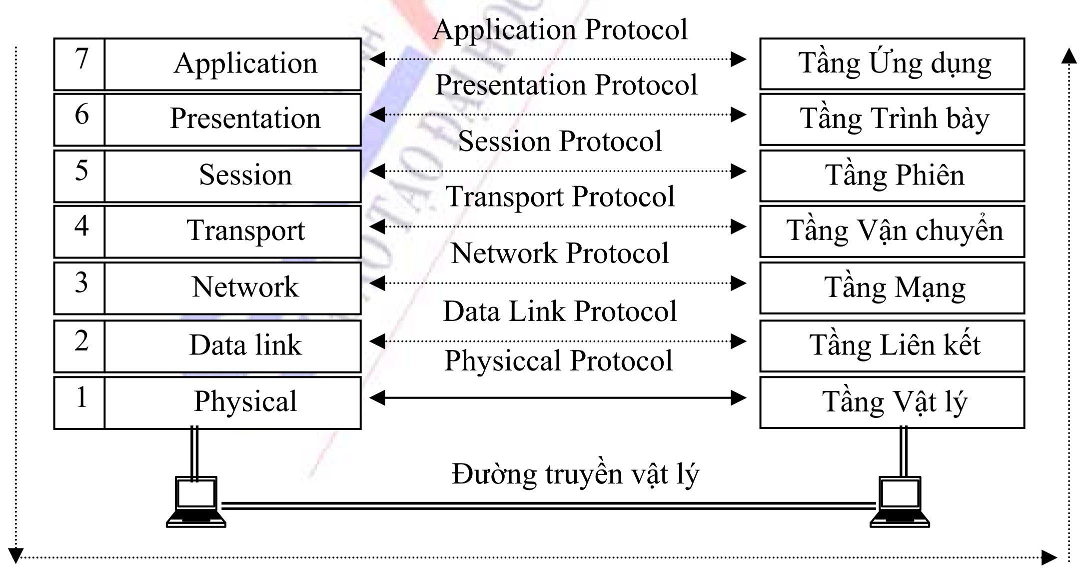


Hình 2.7 Biểu diễn thời gian các hàm dịch vụ nguyên thủy

2.3 Mô hình kết nối các hệ thống mở OSI (Open System Interconnection)

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

2.3.1 Nguyên tắc định nghĩa các tầng hệ thống mở



Hình 2.8 Mô hình kết nối các hệ thống mở OSI

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

- Mô hình gồm N =7 tầng. OSI là hệ thống mở, phải có khả năng kết nối với các hệ thống khác nhau, tương thích với các chuẩn OSI.

- Quá trình xử lý các ứng dụng được thực hiện trong các hệ thống mở, trong khi vẫn duy trì được các hoạt động kết nối giữa các hệ thống.

- Thiết lập kênh logic nhằm thực hiện việc trao đổi thông tin giữa các thực thể.

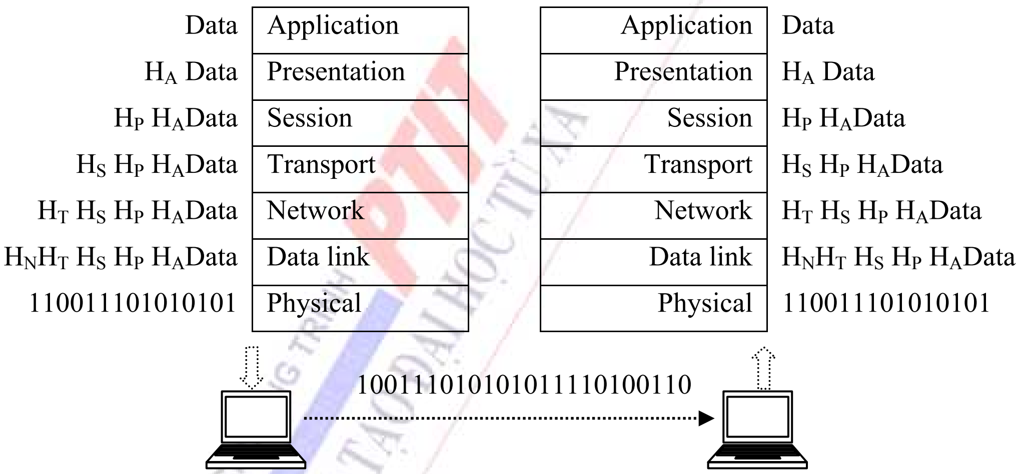
2.3.2. Các giao thức trong mô hình OSI

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

Giao thức hướng liên kết: Trước khi truyền dữ liệu, các thực thể đồng tầng trong hai hệ thống cần phải thiết lập một liên kết logic. Chúng thương lượng với nhau về tập các tham số sẽ sử dụng trong giai đoạn truyền dữ liệu. Dữ liệu được truyền với các cơ chế kiểm soát lỗi, kiểm soát luồng dữ liệu, cắt/hợp dữ liệu, nhằm nâng cao độ tin cậy và hiệu quả của quá trình truyền dữ liệu. Sau khi trao đổi dữ liệu, liên kết sẽ được hủy bỏ. Thiết lập liên kết logic sẽ nâng cao độ tin cậy và an toàn trong quá trình trao đổi dữ liệu.

Giao thức không liên kết: Dữ liệu được truyền độc lập trên các tuyến khác nhau. Với các giao thức không liên kết chỉ có giai đoạn duy nhất truyền dữ liệu.

2.3.3 Truyền dữ liệu trong mô hình OSI



Tầng	Header		Tên dữ liệu
Application	H_A	Application Header	Message & Packet
Presentation	H_P	Presentation Header	Packet
Session	H_S	Session Header	Packet
Transport	H_T	Transport Header	Datagram,Segment & Packet
Network Header	H_N	Network Header	Datagram & Packet
Data Link	H_D	Data Link Header	Frame & Packet
Physical		Physical	Bit

Hình 2.9: Bổ sung phần đầu thông điệp & tên dữ liệu sử dụng

2.3.4. Vai trò và chức năng chủ yếu các tầng

Vai trò & chức năng tầng ứng dụng (Application Layer) Xác định giao diện giữa người sử dụng và môi trường OSI. Bao gồm nhiều giao thức ứng dụng cung cấp các phương tiện cho người sử dụng truy cập vào môi trường mạng và cung cấp các dịch vụ phân tán. Khi các thực thể ứng dụng AE (Application Entity) được thiết lập, nó sẽ gọi đến các phần tử dịch vụ ứng dụng ASE (Application Service Element). Mỗi thực thể ứng dụng có thể gồm một hoặc nhiều các phần tử dịch vụ ứng dụng. Các phần tử dịch vụ ứng dụng được phối hợp trong môi trường của thực thể ứng dụng thông qua các liên kết gọi là đối tượng liên kết đơn SAO (Single Association Object). SAO điều khiển việc truyền thông và cho phép tuần tự hóa các sự kiện truyền thông.

Vai trò & chức năng tầng trình bày (Presentation Layer): Tầng trình bày giải quyết các vấn đề liên quan đến cú pháp và ngữ nghĩa của thông tin được truyền. Biểu diễn thông tin người sử dụng phù hợp với thông tin làm việc của mạng và ngược lại. Thông thường biểu diễn thông tin các ứng dụng nguồn và ứng dụng đích có thể khác nhau bởi các ứng dụng được chạy trên các hệ thống có thể khác nhau. Tầng trình bày phải chịu trách nhiệm chuyển đổi dữ liệu gửi đi trên mạng từ một loại biểu diễn này sang một loại khác. Để đạt được điều đó nó cung cấp một dạng biểu diễn truyền thông chung cho phép chuyển đổi từ dạng biểu diễn cục bộ sang biểu diễn chung và ngược lại.

*Vai trò & chức năng tầng phiên (Session Layer)***:** Tầng phiên cho phép người sử dụng trên các máy khác nhau thiết lập, duy trì, huỷ bỏ và đồng bộ phiên truyền thông giữa họ với nhau. Nói cách khác tầng phiên thiết lập "các giao dịch" giữa các thực thể đầu cuối.

Dịch vụ phiên cung cấp một liên kết giữa 2 đầu cuối sử dụng dịch vụ phiên sao cho trao đổi dữ liệu một cách đồng bộ và khi kết thúc thì giải phóng liên kết. Sử dụng thẻ bài (Token) để thực hiện truyền dữ liệu, đồng bộ hóa và hủy bỏ liên kết trong các phương thức truyền đồng thời hay luân phiên. Thiết lập các điểm đồng bộ hóa trong hội thoại. Khi xẩy ra sự cố có thể khôi phục hội thoại bắt đầu từ một điểm đồng bộ hóa đã thỏa thuận.

Vai trò & chức năng tầng vận chuyển (Transport Layer): Là tầng cao nhất có liên quan đến các giao thức trao đổi dữ liệu giữa các hệ thống mở, kiểm soát việc truyền dữ liệu từ mút tới mút (End- to -End). Thủ tục trong 3 tầng dưới (vật lý, liên kết dữ liệu và mạng) chỉ phục vụ việc truyền dữ liệu giữa các tầng kề nhau trong từng hệ thống. Các thực thể đồng tầng hội thoại, thương lượng với nhau trong quá trình truyền dữ liệu.

Tầng vận chuyển thực hiện việc chia các gói tin lớn thành các gói tin nhỏ hơn trước khi gửi đi và đánh số các gói tin và đảm bảo chúng chuyển theo đúng thứ tự. Là tầng cuối cùng chịu trách nhiệm về mức độ an toàn trong truyền dữ liệu nên giao thức tầng vận chuyển phụ thuộc nhiều vào bản chất của tầng mạng. Tầng vận chuyển có thể thực hiện việc ghép kênh (multiplex) một vài liên kết vào cùng một liên kết nối để giảm giá thành.

Vai trò & chức năng tầng mạng (Network Layer): Thực hiện các chức năng *chọn đường (Routing* đi cho các gói tin từ nguồn tới đích có thể trong cùng một mạng hoặc khác mạng nhau. Đường có thể được cố định, cũng có thể được định nghĩa khi bắt đầu hội thoại và có thể đường đi là động (Dynamic) có thể thay đổi với từng gói tin tuỳ theo trạng thái tải tức thời của mạng. Trong mạng kiểu quảng bá (Broadcast) routing rất đơn giản.

Một chức năng quan trọng khác của tầng mạng là chức năng *điều khiển tắc nghẽn (Congestion Control)*. Nếu có quá nhiều gói tin cùng lưu chuyển trên cùng một đường thì có thể xảy ra tình trạng tắc nghẽn. Thực hiện chức năng *giao tiếp giữa các mạng* khi các gói tin đi từ mạng này sang mạng khác để tới đích.

Vai trò & chức năng tầng liên kết dữ liệu (Data link Layer): Chức năng chủ yếu của tầng liên kết dữ liệu là thực hiện thiết lập các liên kết, duy trì và huỷ bỏ các liên kết dữ liệu. Kiểm soát lỗi và kiểm soát lưu lượng.

Chia thông tin thành các khung thông tin (Frame), truyền các khung tuần tự và xử lý các thông điệp xác nhận (Acknowledgement Frame) từ bên máy thu gửi về. Tháo gỡ các khung thành chuỗi bít không cấu trúc chuyển xuống tầng vật lý. Tầng 2 bên thu, tái tạo chuỗi bít thành các khung thông tin. Đường truyền vật lý có thể gây lỗi, nên tầng liên kết dữ liệu phải giải quyết vấn đề kiểm soát lỗi, kiểm soát luồng, kiểm soát lưu lượng, ngăn không để nút nguồn gây " ngập lụt" dữ liệu cho bên thu có tốc độ thấp hơn. Trong các mạng quảng bá, tầng con MAC (Medium Acces Sublayer) điều khiển việc truy nhập đường truyền.

Vai trò & chức năng tầng Vật lý (Physical layer): Tầng vật lý là tầng thấp nhất trong mô hình 7 lớp OSI. Các thực thể tầng giao tiếp với nhau qua một đường truyền vật lý. Tầng vật lý xác định các chức năng, thủ tục về điện, cơ, quang để kích hoạt, duy trì và giải phóng các kết nối vật lý giữa các hệ thống mạng. Cung cấp các cơ chế về điện, cơ hầm, thủ tục ...nhằm thực hiện việc kết nối các phần tử của mạng thành một hệ thống bằng các phương pháp vật lý. Đảm bảo cho các yêu cầu về chuyển mạch hoạt động nhằm tạo ra các đường truyền thực cho các chuỗi bit thông tin. Các chuẩn trong tầng vật lý là các chuẩn xác định giao diện người sử dụng và môi trường mạng. Các giao thức tầng vật lý có hai loại truyền dị bộ (Asynchronous) và truyền đồng bộ (Synchronous).

Tóm tắt chức năng các tầng như sau:

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

2.4. Một số kiến trúc khác

2.4.1. Systems Nework Architecture (SNA)

Kiến trúc mạng SNA được công ty IBM thiết kế, đặc tả kiến trúc mạng xử lý dữ liệu phân tán. Giao thức định nghĩa các quy tắc, các tiến trình cho sự tương tác giữa các thành phần trong mạng như máy tính, terminal và phần mềm.

- Mạng SNA sử dụng kiến trúc 6 tầng: tầng1- Physical Control (X21,RS-232), tầng 2-Data Link Control (SDLC) , tầng 3- Path Control (chọn đường và kiểm soát dữ liệu), tầng 4 - Transmission Control (kiểm soát truyền), tầng 5- Data Flow Control (kiểm soát luồng) và tầng 6 - Function Management (quản trị).

- Chức năng của các node trong mạng: Node loại 5- kiểm soát tài nguyên mạng và các dịch vụ mạng, gọi là node Host. Node loại 4 định tuyến và điều khiển luồng dữ liệu. Node loại 2.0 và 2.1 là các loại node ngoại vi được nối với node loại 4 hoặc loại 5. Đây là node điều khiển cụm và là bộ xử lý phân tán.

2.4.2. Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX)

Giao thức IPX/SPX được công ty Novell thiết kế sử dụng cho các sản phẩm mạng của chính hãng. SPX hoạt động trên tầng Transport của OSI, có chức năng bảo đảm độ tin cậy của liên kết truyền thông từ mút đến mút. Nó đảm bảo chuyển giao các gói tin đúng trình tự, đúng đích nhưng không có vai trò trong định tuyến. IPX tuân theo chuẩn OSI, hoạt động tầng mạng, chịu trách nhiệm thiết lập địa chỉ cho các thiết bị mạng. Nó là giao thức định tuyến, kết hợp với các giao thức Routing Information Protocol (RIP) và Netware Link Services Protocol (NLSP) để trao đổi thông tin định tuyến với các bộ định tuyến lân cận.

2.4.3. AppleTalk

Là kiến trúc mạng do hãng Apple Computer phát triển cho họ các máy tính cá nhân Macintosh. Giao thức AppleTalk cũng được phát triển trên tầng vật lý của Ethernet và Token Ring.

- Các vùng tối đa trên một phân mạng: Phase 1 là 1; Phase 2 là 255 .

- Các node tối đa trên mỗi mạng: Phase 1: 254; Phase 2: khoảng 16 triệu.

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

- Định tuyến Split-horizon: Phase 1: không; Phase 2: có.

2.4.4. Digital Network Architectur (DNA)

Kiến trúc mạng DNA là sản phẩm của hãng Digital Equipment Corporation. Đặc biệt Digital kết hợp với các hãng Intel và Xerox phát triển các phiên bản Ethernet, trong đó có Ethernet Version 2.

2.4.5. Họ IEEE 802 (Institute of Electrical and Electronic Engineer)

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

- Chuẩn IEEE 802.2 định nghĩa một tầng con LLC được giao thức tầng dưới sử dụng. Giao thức tầng mạng có thể thiết kế độc lập với tầng vật lý.

- Giao thức tầng dưới: 802.3 (1Base5, 10Base5, 10Base2, 10Basef, 10Broad36, 10BaseT, 10BaseX), 802.4 (TokenBus), 802.5 (Token Ring) , 802.6 , 802.9, 802.11, 802.12.

2.4.6. TCP/IP (Transmission Control Protocol/Internet Protocol)

Là họ các giao thức cùng làm việc với nhau để cung cấp phương tiện truyền thông liên mạng. Vì lịch sử của TCP/IP gắn liền với Bộ quốc phòng Mỹ, nên việc phân lớp giao thức TCP/IP được gọi là mô hình DOD (Department of Defense). Đây là họ các giao thức được sử dụng phổ biến trên mạng Internet, mang tính mở nhất , phổ dụng nhất và được hỗ trợ của nhiều hãng kinh doanh. TCP/IP được cài đặt sẵn trong phần thực thi UNIX BSD (Berkely Standard Distribution). Mô hình DOD gồm 4 tầng:

- Network Access Layer (truy nhập mạng) tương ứng Physical Layer & Data Link Layer trong OSI.

- Internetwork Layer: Định tuyến gói dữ liệu giữa các máy chủ.

- Host to Host Layer: Kết nối các thành phần mạng.

- Application Layer: Hỗ trợ các ứng dụng .

Câu hỏi trắc nghiệm

1. Các phát biểu nào về nguyên tắc phân tầng là đúng
   A. Chức năng các tầng độc lập với nhau và có tính mở.
   B. Xác định mối quan hệ giữa các tầng kề nhau
   C. Xác định mối quan hệ giữa các đồng tầng
   D. Dữ liệu không truyền trực tiếp giữa các tầng đồng hệ thống (trừ tầng vật lý).
   E. Cả 4 phát biểu đều đúng.
2. Kiến trúc mạng (Network Architecture) là:
   A. Giao diện Interface giữa 2 tầng kề nhau.
   B. Giao thức tầng- quan hệ đồng tầng
   C. Số lượng tầng.
   D. Dịch vụ tầng.
   E. Tập các giao diện, số lượng tâng và giao thức tầng- quan hệ đồng tầng
3. Điểm truy nhập dịch vụ SAP (Service Access Point) là gì ?
   A. Nơi trao cung cấp dịch vụ các tầng kề nhau.
   B. Nơi hoạt động của các dịch vụ.
   C. Nơi cung cấp dịch vụ của tầng dưới cho các hoạt động tầng trên.
4. Những phát biểu nào đúng:

A. Cung cấp và nhận các dịch vụ giữa các thực thể trong các tầng kề nhau thông qua việc gọi các hàm dịch vụ nguyên thủy.

B. Các dịch vụ nguyên thuỷ là các thủ tục trao đổi thông tin.

C. Các hàm dịch vụ nguyên thủy tương tác giữa các tầng kề nhau.

D. Các hàm dịch vụ nguyên thủy đặc tả các thao tác thực hiện yêu cầu hay trả lời một yêu cầu của các thực thể đồng tầng.

5. Tầng nào xác định giao diện giữa người sử dụng và môi trường OSI.

A. Tầng ứng dụng

B. Tầng trình bày

C. Tầng phiên

D. Tầng vận chuyển

6. Tầng nào cung cấp một dạng biểu diễn truyền thông chung cho phép chuyển đổi từ dạng biểu diễn cục bộ sang biểu diễn chung và ngược lại.

A. Tầng mạng

B. Tầng trình bày

C. Tầng phiên

D. Tầng vật lý

7. Tầng nào thiết lập, duy trì, huỷ bỏ “các giao dịch" giữa các thực thể đầu cuối.

A. Tầng mạng

B. Tầng liên kết dữ liệu

C. Tầng phiên

D. Tầng vật lý

8. Tầng nào có liên quan đến các giao thức trao đổi dữ liệu

A. Tầng mạng

B. Tầng vận chuyển

C. Tầng liên kết dữ liệu

D. Tầng vật lý

9. Những thuật ngữ nào dùng để mô tả các đơn vị dữ liệu sử dụng trong tầng liên kết dữ liệu:

A. Datagram.

B. Packet.(*)

C. Message

D. Frame (*)

10. Tầng nào thay đổi, duy trì tuyến kết nối giữa các thiết bị truyền thông.

A. Tầng vật lý.

B. Tầng con MAC.

C. Tầng con LLC(*)

D. Tầng mạng.

11. Phương pháp chuyển mạch nào sử dụng mạch ảo ?.
    A. Message.
    B. Packet(*).
    C. Bit
    D. Circuit Switching
12. Tầng nào thực hiện mã hoá dữ liệu?
    A. Tầng mạng
    B. Tầng vận chuyển.
    C. Tầng liên kết dữ liệu.
    D. Tầng phiên.
    E. Tầng ứng dụng
    F. Tầng trình bày.(*)
13. Tầng nào thực hiện bàn giao các thông điệp giữa các tiến trình trên các thiết bị?
    A. Tầng mạng.
    B. Tầng vận chuyển.(*).
    C. Tầng liên kết dữ liệu..
    D. Tầng phiên.
    E. Tầng ứng dụng.
14. Tầng nào thực hiện việc phân giải địa chỉ/tên?
    A. Tầng mạng.
    B. Tầng vận chuyển.(*).
    C. Tầng liên kết dữ liệu..
    D. Tầng ứng dụng
15. Khẳng định nào đúng:
    A. Băng thông mạng hiệu suất cao khi sử dụng kỹ thuật chọn đường DIJKTRA.
    B. Băng thông mạng hiệu suất cao khi sử dụng kỹ thuật chọn đường BellMan Ford (*).
    C. Cả hai kết hợp.
16. Hoạt động nào có liên quan đến ID giao kết
    A. Chuyển mạch gói.
    B. Định tuyến.
    C. Phát triển phân đoạn.(*)
    D. Điều khiển luồng
17. Khẳng định nào đúng:
    A. Tầng liên kết dữ liệu xử lý lưu thông giữa các thiết bị.(*).
    B. Tầng mạng xử lý lưu thông giữa các tiến trình của tầng trên..

C. Tầng lvận chuyển xử lý lưu thông giữa các thiết bị đầu cuối.(*)

D. Tất cả đều đúng.

18. Điều khiển cuộc liên lạc là chức năng của tầng:

A. Vật lý.

B. Tầng mạng.

C. Tầng phiên.(*)

D. Tầng trình bày.

19. Chức năng điều khiển phiên làm việc của một cuộc liên lạc là:

A. Thiết lập tuyến liên kết.(*).

B. Phát hiện lỗi bằng CheckSum.

C. Chuyển giao dữ liệu.(*)

D. Giải phóng các liên kết.(*)

20. Chức năng của việc thiết lập liên kết:

A. Bắt đầu khi phiên truyền thông bị gián đoạn.

B. Xác minh tên đăng nhập và mật khẩu.(*)

C. Xác định các dịch vụ cần thiết.(*).

D. Phát tín hiệu báo nhận dữ liệu.

21. Chức năng của tầng trình bày:

A. Mã hoá dữ liệu.(*).

B. Trình bày dữ liệu trên các thiết bị hiển thị.

C. Phiên dịch dữ liệu.(*)

D. Chuyển đổi dạng thức hiển thị.

22. Chức năng của tầng ứng dụng

A. Dịch vụ in mạng.(*).

B. Các ứng dụng của người sử dụng đầu cuối.

C. Hệ khách truy nhập các dịch vụ mạng.(*)

D. Quảng cáo các dịch vụ.(*).

23. Đúng hay sai khẳng định sau: Trong mạng LAN hình BUS, mỗi một máy trên BUS đều có địa chỉ riêng, nhiều máy có thể đồng thời gửi dữ liệu lên mạng mà vẫn đảm bảo được dữ liệu sẽ đến đích?

24. Mô hình tham khảo OSI chia hoạt động truyền thông thành..... tầng.

25. Mục đích của mỗi một tầng là cung cấp các dịch vụ cho tầng ..... và bảo vệ cho tầng ...... khỏi những chi tiết về cách thức dịch vụ được thực hiện. Trong mỗi tầng, các gói dữ liệu được bổ sung thêm thông tin điều khiển, đó là các thông tin về.....

26. Mỗi một tầng hoạt động giao tiếp với ....tầng.... ..

27. Tầng ..... quyết định đường đi của dữ liệu từ node nguồn đến node đích.

28. Tầng Data Link chịu trách nhiệm gửi...... từ tầng Network xuống tầng Physical.
29. Thông tin ...... trong khung dữ liệu (Frame) được sử dụng chỉ rõ loại khung, đường đi và thông tin về phân đoạn.
30. Tầng con ...... giao tiếp trực tiếp với Card mạng và chịu trách nhiệm chuyển giao dữ liệu không lỗi giữa hai máy tính trên mạng.
31. Dữ liệu được phân chia thành nhiều .... nhỏ để ..... xử lý dễ dàng.
32. Nhiều giao thức phối hợp cùng thực hiện hoạt động truyền thông, gọi là.....
33. Sự liên kết ..... sẽ cho biết ...... của tầng nào đang hoạt động.
34. Có ba kiểu giao thức ứng với mô hình OSI, đó là các loại giao thức....
35. Giao thức ứng dụng hoạt động trên tầng cao nhất và cung cấp trao đổi dữ liệu giữa các chương trình ứng dụng. ?
36. Khi gói dữ liệu được truyền giữa các bộ định tuyến với nhau, địa chỉ nguồn và đích của tầng Data Link bị loại bỏ và _________
    A. Sau đó được tạo lại.
    B. tiếp tục được gửi riêng để rồi sẽ được tái tạo tại node đích.
    C. Các gói tin được chuyển tiếp dựa trên độ dài tính bằng Byte
    D. Gói tin được truyền tiếp dựa trên mức độ ưu tiên.
37. Chuyển tiếp gói dữ liệu dựa trên địa chỉ tầng con MAC (Media Access Control________
    A. Bộ chuyển tiếp
    B. Cổng giao tiếp
    C. SONET.
    D. SMDS
    E. Cầu nối (Bridge)
38. Tập hợp các giao thức mạng chuyển mạch gói________
    A. Bộ chuyển tiếp
    B. Cổng giao tiếp
    C. SONET.
    D. X25
39. Liên kết nhiều mạng sử dụng các giao thức khác nhau________
    A. Bộ chuyển tiếp
    B. Cổng giao tiếp
    C. SONET.
    D. Bộ định tuyến.

Câu hỏi và bài tập

1. Hãy cho biết ý nghĩa của khuyến nghị loại V, khuyến nghị loại X và loại I.
2. Tổng quát về khái niệm kiến trúc đa tầng và các quy tắc phân tầng

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

CHƯƠNG 3: MẠNG INTERNET VÀ GIAO THỨC TCP/IPv4

Nội dung của chương sẽ giới thiệu tổng quát về mạng Internet và kiến trúc mô hình TCP/IP. Bộ giao thức TCP/IP đã trở thành chuẩn chung cho mạng máy tính toàn cầu. Tìm hiểu về chồng giao thức TCP/IP sẽ cung cấp những kiến thức cơ bản về các thành phần giao thức khác nhau cần thiết cho các ứng dụng TCP/IP trên nền các hệ điều hành mạng. Phần cuối của chương sẽ trình bày những hạn chế của IPv4 và sự cần thiết ra đời giao thức IPv6. Nội dung của chương bao gồm:

- Giới thiệu mô hình kiến trúc TCP/IP.
- Một số giao thức cơ bản của bộ giao thức TCP/IP
- Một số hạn chế của giao thức IPv4 và nguyên nhân ra đời IPv6
- Các lớp địa chỉ IPv6

3.1. Mô hình TCP/IP

TCP/IP (Transmission Control Protocol/Internet Protocol) là chồng giao thức cùng hoạt động nhằm cung cấp các phương tiện truyền thông liên mạng. Năm 1981, TCP/IP phiên bản 4 (IPv4) được hoàn thành và sử dụng phổ biến trên máy tính sử dụng hệ điều hành UNIX, trở thành một trong những giao thức cơ bản của hệ điều hành Windows 9x. Năm 1994, một phiên bản mới IPv6 được hình thành trên cơ sở cải tiến những hạn chế của IPv4.

3.1.1. Mô hình kiến trúc TCP/IP

Mô hình TCP/IP		Mô hình OSI	
Process Application Layer	Ứng dụng	Ứng dụng	Application
		Trình bày	Presentation
		Phiên	Session
Host -To-Host	Vận chuyển	Vận chuyển	Transport
Internet Layer	Mạng	Mạng	Network
Network Access Layer	Truy nhập mạng	Liên kết dữ	Data Link
		Vật lý	Physical

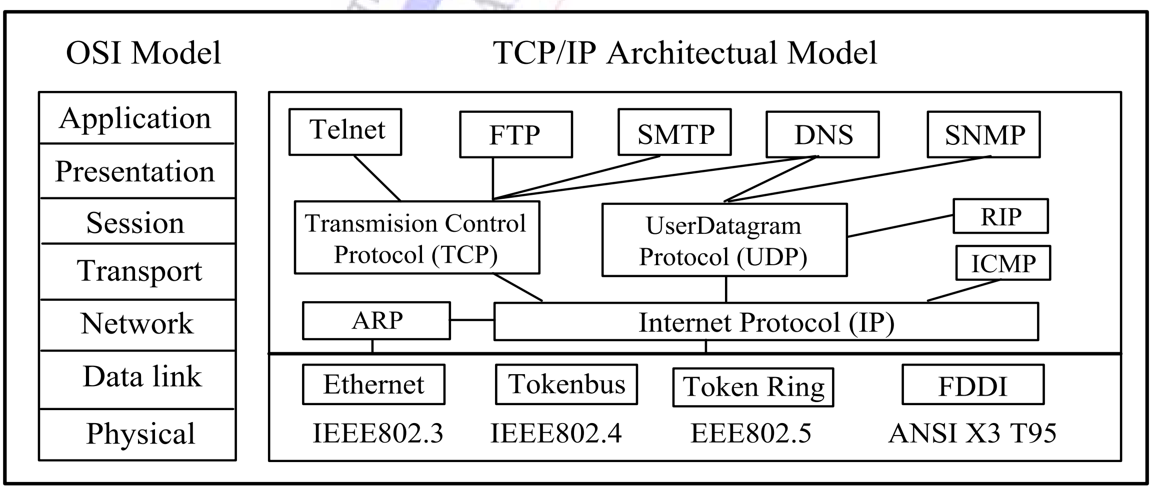
Hình 3.1 Tương quan Mô hình OSI và mô hình TCP/IP

3.1.2. Vai trò và chức năng các tầng trong mô hình TCP/IP

Tầng ứng dụng (Process/Application Layer): Ứng với các tầng Session, Presentation và Aplication trong mô hình OSI. Tầng ứmg dụng hỗ trợ các ứng dụng cho các giao thức tầng Host to Host. Cung cấp giao diện cho người sử dụng mô hình TCP/IP. Các giao thức ứng dụng gồm TELNET(truy nhập từ xa), FTP (truyền File), SMTP (thư điện tử),.......

Tầng vận chuyển Host to Host: Ưng với tầng vận chuyển (Transport Layer) trong mô hình OSI, tầng Host to Host thực hiện những kết nối giữa hai máy chủ trên mạng bằng 2 giao thức: giao thức điều khiển trao đổi dữ liệu TCP (Transmission Control Protocol) và giao thức dữ liệu người sử dụng UDP (User Datagram Protocol).Giao thức TCP là giao thức kết nối hướng liên kết (Connection - Oriented) chịu trách nhiệm đảm bảo tính chính xác và độ tin cậy cao trong việc trao đổi dữ liệu giữa các thành phần của mạng, tính đồng thời và kết nối song công (Full Duplex). Khái niệm tin độ cậy cao nghĩa là TCP kiểm soát lỗi bằng cách truyền lại các gói tin bị lỗi. Giao thức TCP cũng hỗ trợ những kết nối đồng thời. Nhiều kết nối TCP có thể được thiết lập tại một máy chủ và dữ liệu có thể được truyền đi một cách đồng thời và độc lập với nhau trên các kết nối khác nhau. TCP cung cấp kết nối song công (Full Duplex), dữ liệu có thể được trao đổi trên một kết nối đơn theo 2 chiều. Giao thức UDP được sử dụng cho những ứng dụng không đòi hỏi độ tin cậy cao.

*Tầng mạng (Internet Layer):*Ưng với tầng mạng (Network Layer) trong mô hình OSI, tầng mạng cung cấp một địa chỉ logic cho giao diện vật lý mạng. Giao thức thực hiện của tầng mạng trong mô hình DOD là giao thức IP kết nối không liên kết (Connectionless), là hạt nhân hoạt động của Internet. Cùng với các giao thức định tuyến RIP, OSPF, BGP, tầng tầng mạng IP cho phép kết nối một cách mềm dẻo và linh hoạt các loại mạng "vật lý" khác nhau như: Ethernet, Token Ring, X.25... Ngoài ra tầng này còn hỗ trợ các ánh xạ giữa địa chỉ vật lý (MAC) do tầng Network Access Layer cung cấp với địa chỉ logic bằng các giao thức phân giải địa chỉ ARP (Address Resolution Protocol) và phân giải địa chỉ đảo RARP (Reverse Address Resolution Protocol). Các vấn đề có liên quan đến chuẩn đoán lỗi và các tình huống bất thường liên quan đến IP được giao thức ICMP (Internet Control Message Protocol) thống kê và báo cáo. Tầng trên sử dụng các dịch vụ do tầng Liên mạng cung cấp.

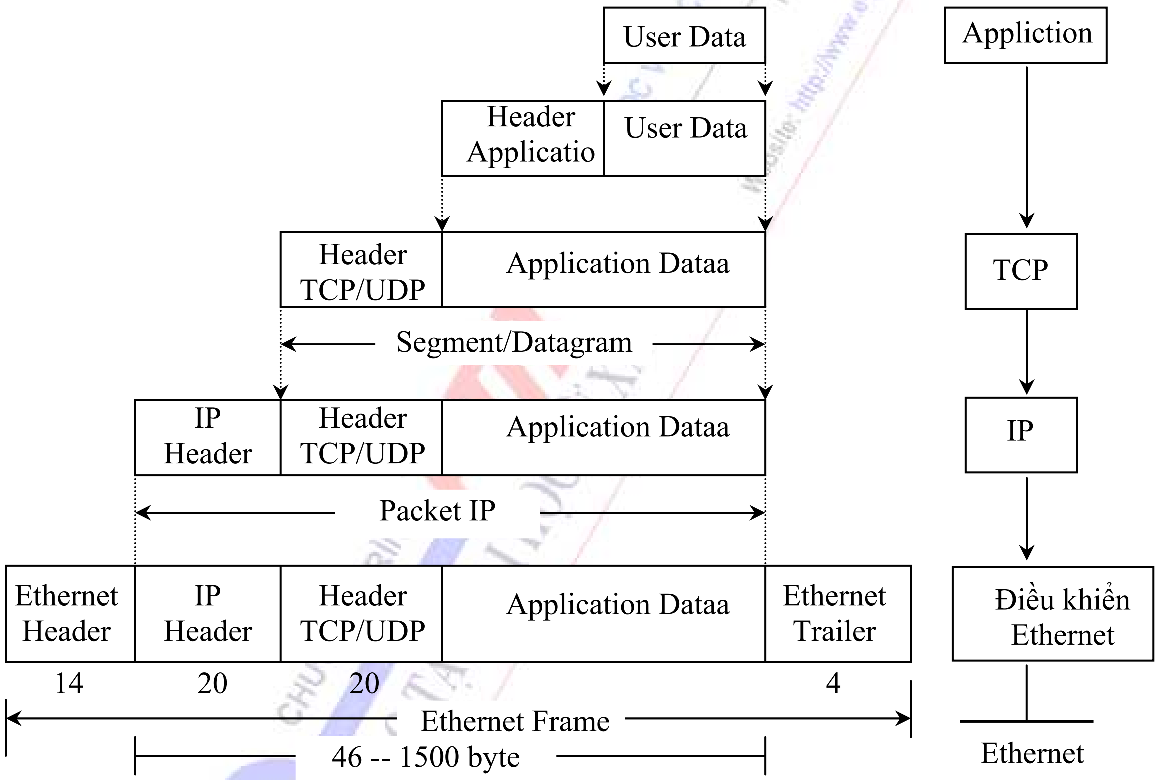


Hình 3.2 Mô hình OSI và mô hình kiến trúc của TCP/IP

Tầng tầng truy nhập mạng (Network Access Layer): Tương ứng với tầng Vật lý và Liên kết dữ liệu trong mô hình OSI, tầng truy nhập mạng cung cấp các phương tiện kết nối vật lý cáp, bộ chuyển đổi (Transceiver), Card mạng, giao thức kết nối, giao thức truy nhập đường truyền như CSMA/CD, Tolen Ring, Token Bus..). Cung cấp các dịch vụ cho tầng Internet phân đoạn dữ liệu thành các khung.

3.1.3. Quá trình đóng gói dữ liệu Encapsulation

Cũng như mô hình OSI, trong mô hình kiến trúc TCP/IP mỗi tầng có một cấu trúc dữ liệu riêng, độc lập với cấu trúc dữ liệu được dùng ở tầng trên hay tầng dưới kề nó. Khi dữ liệu được truyền từ tầng ứng dụng cho đến tầng vật lý, qua mỗi tầng được thêm phần thông tin điều khiển (Header) đặt trước phần dữ liệu được truyền, đảm bảo cho việc truyền dữ liệu chính xác. Việc thêm Header vào đầu các gói tin khi đi qua mỗi tầng trong quá trình truyền dữ liệu được gọi là *Encapsulation*. Quá trình nhận dữ liệu sẽ diễn ra theo chiều ngược lại, khi qua mỗi tầng, các gói tin sẽ tách thông tin điều khiển thuộc nó trước khi chuyển dữ liệu lên tầng trên.



Hình 3.3 Đóng gói dữ liệu khi chuyển xuống tầng kề dưới

- Process/Application Layer: Message (Thông điệp)
- Host - To- Host Layer: Segment/ Datagram (Đoạn/Bó dữ liệu)
- Internet Layer: Packet (Gói dữ liệu)
- Network Layer: Frame (Khung dữ liệu).

3.1.4. Quá trình phân mảnh dữ liệu Fragment

Dữ liệu có thể được truyền qua nhiều mạng khác nhau, kích thước cho phép cũng khác nhau. Kích thước lớn nhất của gói dữ liệu trong mạng gọi là *đơn vị truyền cực đại MTU* (Maximum Transmission Unit). Trong quá trình đóng gói *Encapsulation,* nếu kích thước của một gói lớn hơn kích thước cho phép, tự động chia thành nhiều gói nhỏ và thêm thông tin điều khiển vào mỗi gói. Nếu một mạng nhận dữ liệu từ một mạng khác, kích thước gói dữ liệu lớn hơn MTU của nó, dữ liệu sẽ được phân mảnh ra thành gói nhỏ hơn để chuyển tiếp. Quá trình này gọi là quá trình phân mảnh dữ liệu *Fragment*.

Quá trình phân mảnh làm tăng thời gian xử lý, làm giảm tính năng của mạng và ảnh hưởng đến tốc độ trao đổi dữ liệu trong mạng. Hậu quả của nó là các gói bị phân mảnh sẽ đến đích chậm hơn so với các gói không bị phân mảnh. Mặt khác, vì IP là một giao thức không liên kết, độ tin cậy không cao, khi một gói dữ liệu bị phân mảnh bị mất thì tất cả các mảnh sẽ phải truyền lại. Vì vậy phần lớn các ứng dụng tránh không sử dụng kỹ thuật phân mảnh và gửi các gói dữ liệu lớn nhất mà không bị phân mảnh, giá trị này là Path MTU.

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

3.2.1. Giao thức gói tin người sử dụng UDP (User Datagram Protocol)

UDP là giao thức không liên kết (Connectionless). UDP sử dụng cho các tiến trình không yêu cầu về độ tin cậy cao, không có cơ chế xác nhận ACK, không đảm bảo chuyển giao các gói dữ liệu đến đích và theo đúng thứ tự và không thực hiện loại bỏ các gói tin trùng lặp. Nó cung cấp cơ chế gán và quản lý các số hiệu cổng để định danh duy nhất cho các ứng dụng chạy trên một Client của mạng và thực hiện việc ghép kênh. UDP thường sử dụng kết hợp với các giao thức khác, phù hợp cho các ứng dụng yêu cầu xử lý nhanh như các giao thưc SNMP và VoIP.

- Giao thức SNMP (Simple Network Management Protocol) là giao thức quản lý mạng phổ biến, khả năng tương thích cao. SNMP cung cấp thông tin quản trị MIB (Management Information Base) và hỗ trợ quản lý và giám sát Agent.

- VoIP ứng dụng UDP: Kỹ thuật VoIP (Voice over IP) được thừa kế kỹ thuật giao vận IP. Các mạng IP sử dụng hai loại giao thức định tuyến: định tuyến vectơ khoảng cách và định tuyến trạng thái liên kết. Hệ thống đảm bảo tính năng thời gian thực, tốc độ truyền cao, các gói thoại không có trễ quá mức và độ tin cậy cao.

3.2.2. Giao thức điều khiển truyền TCP (Transmission Control Protocol)

TCP là một giao thức hướng liên kết (Connection Oriented), tức là trước khi truyền dữ liệu, thực thể TCP phát và thực thể TCP thu thương lượng để thiết lập một kết nối logic tạm thời, tồn tại trong quá trình truyền số liệu. TCP nhận thông tin từ tầng trên, chia dữ liệu thành nhiều gói theo độ dài quy định và chuyển giao các gói tin xuống cho các giao thức tầng mạng (Tầng IP) để định tuyến. Bộ xử lý TCP xác nhận từng gói, nếu không có xác nhận gói dữ liệu sẽ được truyền lại. Thực thể TCP bên nhận sẽ khôi phục lại thông tin ban đầu dựa trên thứ tự gói và chuyển dữ liệu lên tầng trên.

TCP cung cấp khả năng truyền dữ liệu một cách an toàn giữa các thành trong liên mạng. Cung cấp các chức năng kiểm tra tính chính xác của dữ liệu khi đến đích và truyền lại dữ liệu khi có lỗi xảy ra. TCP cung cấp các chức năng chính sau:

- Thiết lập, duy trì, giải phóng liên kết giữa hai thực thể TCP.

- Phân phát gói tin một cách tin cậy.

- Tạo số thứ tự (Sequencing) các gói dữ liệu.

- Điều khiển lỗi.

- Cung cấp khả năng đa kết nối cho các quá trình khác nhau giữa thực thể nguồn và thực thể đích thông qua việc sử dụng số hiệu cổng.

- Truyền dữ liệu theo chế độ song công (Full-Duplex).

TCP có những đặc điểm sau:

- Hai thực thể liên kết với nhau phải trao đổi, đàm phán với nhau về các thông tin liên kết. Hội thoại, đàm phán nhằm ngăn chặn sự tràn lụt và mất dữ liệu khi truyền.

- Hệ thống nhận phải gửi xác nhận cho hệ thống phát biết rằng nó đã nhận gói dữ liệu.

- Các Datagram IP có thể đến đích không đúng theo thứ tự , TCP nhận sắp xếp lại.

- Hệ thống chỉ phát lại gói tin bị lỗi, không loại bỏ toàn bộ dòng dữ liệu.

Cấu trúc gói tin TCP: Đơn vị dữ liệu sử dụng trong giao thức TCP được gọi là Segment. Khuôn dạng và nội dung của gói tin TCP được biểu diễn như sau

0 15 16 31

<table>
<tr><td colspan="8">Source port</td><td>Destination port</td></tr>
<tr><td colspan="9">Sequence number</td></tr>
<tr><td colspan="9">Acknowledgment number</td></tr>
<tr><td>Offset</td><td>Reserved</td><td>U</td><td>A</td><td>P</td><td>R</td><td>S</td><td>F</td><td>Window</td></tr>
<tr><td colspan="8">Checksum</td><td>Urgent pointer</td></tr>
<tr><td colspan="8">Options</td><td>Padding</td></tr>
<tr><td colspan="9">TCP data</td></tr>
<tr><td colspan="9">…</td></tr>
</table>

Hình 3.4 Cấu trúc gói tin TCP (TCP Segment)

- Cổng nguồn (Source Port): 16 bít, số hiệu cổng nguồn.

- Cổng đích (Destination Port): Độ dài 16 bít, chứa số hiệu cổng đích.

- Sequence Number: 32 bits, số thứ tự của gói số liệu khi phát.

- Acknowlegment Number (32 bits), Bên thu xác nhận thu được dữ liệu đúng.

- Offset (4 bíts): Độ dài Header gói tin TCP.

- Reserved (6 bít) lưu lại: Lấp đầy bằng 0 để dành cho tương lai.

- Control bits: Các bits điều khiển

URG : Vùng con trỏ khẩn có hiệu lực.

ACK : Vùng báo nhận (ACK number) có hiệu lực .

PSH: Chức năng PUSH.

RST: Khởi động lại (reset) liên kết.

SYN : Đồng bộ các số liệu tuần tự (sequence number).

FIN : Không còn dữ liệu từ trạm nguồn .

- Window (16bits): Số lượng các Byte dữ liệu trong vùng cửa sổ bên phát.
- Checksum (16bits): Mã kiểm soát lỗi (theo phương pháp CRC).
- Urgent Pointer (16 bits): Số thứ tự của Byte dữ liệu khẩn, khi URG được thiết lập .
- Option (độ dài thay đổi): Khai báo độ dài tối đa của TCP Data trong một Segment .
- Padding (độ dài thay đổi): Phần chèn thêm vào Header.

Việc kết hợp địa chỉ IP của một máy trạm và số cổng được sử dụng tạo thành một Socket. Các máy gửi và nhận đều có Socket riêng. Số Socket là duy nhất trên mạng.

Điều khiển lưu lượng và điều khiển tắc nghẽn

Cơ chế cửa sổ động là một trong các phương pháp điều khiển thông tin trong mạng máy tính. Độ lớn của cửa sổ bằng số lượng các gói dữ liệu được gửi liên tục mà không cần chờ thông báo trả lời về kết quả nhận từng gói dữ liệu đó. Độ lớn cửa sổ quyết định hiệu suất trao đổi dữ liệu trong mạng. Nếu chọn độ lớn của sổ cao thì có thể gửi được nhiều dữ liệu trong cùng một đơn vị thời gian. Nếu truyền bị lỗi, dữ liệu phải gửi lại lớn thì hiệu quả sử dụng đường truyền thấp. Giao thức TCP cho phép thay đổi độ lớn của sổ một cách động, phụ thuộc vào độ lớn bộ đệm thu của thực thể TCP nhận.

Cơ chế phát lại thích nghi: Để đảm bảo kiểm tra và khắc phục lỗi trong việc trao đổi dữ liệu qua liên mạng, TCP phải có cơ chế đồng hồ kiểm tra phát (Time Out) và cơ chế phát lại (Retransmission) mềm dẻo, phụ thuộc vào thời gian trễ thực của môi trường truyền dẫn cụ thể. Thời gian trễ toàn phần RTT (Round Trip Time) được xác định bắt đầu từ thời điểm phát gói dữ liệu cho đến khi nhận được xác nhận của thực thể đối tác, là yếu tố quyết định giá trị của đồng hồ kiểm tra phát T_{out}. Như vậy T_{out} phải lớn hơn hoặc bằng RTT.

Cơ chế điều khiển tắc nghẽn**:** Hiện tượng tắc nghẽn dữ liệu thể hiện ở việc gia tăng thời gian trễ của dữ liệu khi chuyển qua mạng. Để hạn chế khả năng dẫn đến tắc nghẽn dữ liệu trong mạng, điều khiển lưu lượng dựa trên việc thay đổi độ lớn của sổ phát.

Thiết lập và huỷ bỏ liên kết: TCP là một giao thức hướng liên kết, tức là cần phải thiết lập một liên kết giữa một cặp thực TCP trước khi truyền dữ liệu. Sau khi liên kết được thiết lập, những giá trị cổng (Port) hoạt động như một nhận dạng logic được sử dụng nhận dạng mạch ảo (Virtual Circuit).Trên kênh ảo dữ liệu được truyền song công (Full Duplex). Liên kết TCP được duy trì trong thời gian truyền dữ liệu. Kết thúc truyền, liên kết TCP được giải phóng, các tài nguyên như bộ nhớ, các bảng trạng thái.. cũng được giải phóng.

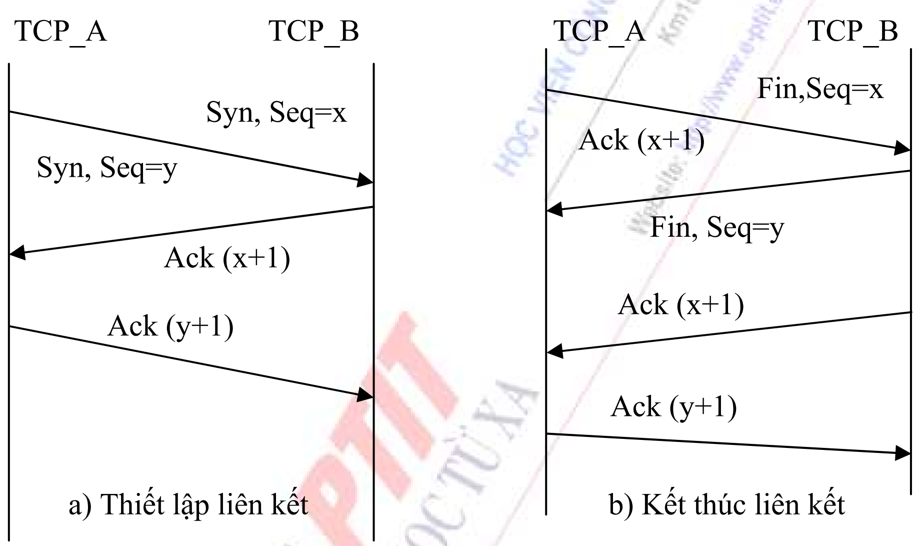
Thiết lập liên kết TCP: Được thực hiện trên cơ sở phương thức bắt tay ba bước (Tree -Way Handsake):

<u>Bước 1:</u> Như hình 3.7 yêu cầu liên kết luôn được trạm nguồn khởi tạo tiến trình bằng cách gửi một gói TCP với cờ SYN=1 và chứa giá trị khởi tạo số tuần tự ISN của Client. Giá trị ISN này là một số 4 byte không dấu và được tăng mỗi khi liên kết được yêu cầu (giá trị này quay về 0 khi nó tới giá trị 232). Trong thông điệp SYN này còn chứa số hiệu cổng TCP của phần mềm dịch vụ mà tiến trình trạm muốn liên kết.

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

Bước 2: Khi thực thể TCP của phần mềm dịch vụ nhận được thông điệp SYN, nó gửi lại gói SYN cùng giá trị ISN của nó và đặt cờ ACK=1 trong trường hợp sẵn sàng nhận liên kết . Thông điệp này còn chứa giá trị ISN của tiến trình trạm trong trường hợp số tuần tự nhận để báo rằng thực thể dịch vụ đã nhận được giá trị ISN của tiến trình trạm.

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



Hình 3.5 Quá trình thiết lập và kết thuc liên kết TCP 3 bước

Kết thúc liên kết: Khi có nhu cầu kết thúc liên kết TCP, ví dụ A gửi yêu cầu kết thúc liên kết với FIN=1. Vì liên kết TCP là song công (Full-Duplex) nên mặc dù nhận được yêu cầu kết thúc liên kết của A, thực thể B vẫn có thể tiếp tục truyền cho đến khi B không còn số liệu để gửi và thông báo cho A bằng yêu cầu kết thúc liên kết với FIN=1. Khi thực thể TCP đã nhận được thông điệp FIN và sau khi đã gửi thông điệp FIN của mình, liên kết TCP thực sụ kết thúc. Như vậy cả hai trạm phải đồng ý giải phóng liên kết TCP bằng cách gửi cờ FIN=1 trước khi chấm dứt liên kết xẩy ra, việc này bảo đảm dữ liệu không bị thất lạc do đơn phương đột ngột chấm dứt liên lạc.

Truyền và nhận dữ liệu Sau khi liên kết được thiết lập giữa một cặp thực thể TCP, các thực thể truyền dữ liệu. Liên kết TCP dữ liệu có thể được truyền theo hai hướng. Khi nhận một khối dữ liệu cần chuyển đi từ người sử dụng, TCP sẽ lưu trữ tại bộ đệm. Nếu cờ PUST được xác lập thì toàn bộ dữ liệu trong bộ đệm sẽ được gửi đi dưới dạng TCP Segment. Nếu PUST không được xác lập thì dữ liệu trong bộ đệm vẫn chờ gửi đi khi có cơ hội thích hợp.

Bên nhận, dữ liệu sẽ được gửi vào bộ đệm. Nếu dữ liệu trong đệm được đánh dấu bởi cờ PUST thì toàn bộ dữ liệu trong bộ đệm sẽ được gửi lên cho người sử dụng. Ngược lại, dữ liệu vẫn được lưu trong bộ đệm. Nếu dữ liệu khẩn cần phải chuyển gấp thì cờ URGENT được xác lập và đánh dấu dữ liệu bằng bit URG để báo dữ liệu khẩn cần được chuyển gấp.

3.2.3. Giao thức mạng IP (Internet Protocol)

Các chức năng chính của IP: IP (Internet Protocol) là giao thức không liên kết. Chức năng chủ yếu của IP là cung cấp các dịch vụ Datagram và các khả năng kết nối các mạng con thành liên mạng để truyền dữ liệu với phương thức chuyển mạch gói IP Datagram, thực hiện tiến trình định địa chỉ và chọn đường. IP Header được thêm vào đầu các gói tin và được giao thức tầng thấp truyền theo dạng khung dữ liệu (Frame). IP định tuyến các gói tin thông qua liên mạng bằng cách sử dụng các bảng định tuyến động tham chiếu tại mỗi bước nhảy. Xác định tuyến được tiến hành bằng cách tham khảo thông tin thiết bị mạng vật lý và logic như ARP giao thức phân giải địa chỉ. IP thực hiện việc tháo rời và khôi phục các gói tin theo yêu cầu kích thước được định nghĩa cho các tầng vật lý và liên kết dữ liệu thực hiện. IP kiểm tra lỗi thông tin điều khiển, phần đầu IP bằng giá trị tổng CheckSum.

Địa chỉ IP : Mỗi một trạm (Host) được gán một địa chỉ duy nhất gọi là địa chỉ IP. Mỗi địa chỉ IP có độ dài 32 bit được tách thành 4 vùng (mỗi vùng 1 byte), có thể được biểu diễn dưới dạng thập phân, bát phân, thập lục phân hoặc nhị phân. Cách viết phổ biến nhất là dưới dạng thập phân có dấu chấm để tách giữa các vùng.

Địa chỉ IP được chia thành 5 lớp ký hiệu là A, B, C, D, E với cấu trúc mỗi lớp được xác định. Các bit đầu tiên của byte đầu tiên được dùng để định danh lớp địa chỉ (0-lớp A, 10 - lớp B, 110 - lớp C, 1110 - lớp D, 11110 - lớp E).

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

0 – 7	8 – 15	16 – 31
Netid	Subnetid	Hostid

- Lớp B cho phép định danh tới 16384 mạng con, với tối đa 65535 Host trên mỗi mạng. Dạng địa chỉ của lớp B: (Network number. Network number.Host.Host).

0 – 15	16 – ...	... – 31
Netid	Subnetid	Hostid

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

0 – 23	24 – 26	27 – 31
Netid	Subnetid	Hostid

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

- Lớp E dự phòng để dùng trong tương lai.

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

Hình 3.6: Cấu trúc các lớp địa chỉ IP

Cấu trúc gói dữ liệu IP: Các gói dữ liệu IP được gọi là các Datagram. Mỗi Datagram có phần tiêu đề (Header) chứa các thông tin điều khiển. Nếu địa chỉ IP đích cùng mạng với trạm nguồn thì các gói dữ liệu sẽ được chuyển thẳng tới đích, nếu địa chỉ IP đích không cùng mạng IP với máy nguồn thì các gói dữ liệu sẽ được gửi đến một máy trung chuyển IP Gateway để chuyển tiếp. IP Gateway là một thiết bị mạng IP đảm nhận việc lưu chuyển các gói dữ liệu IP giữa hai mạng IP khác nhau. Hình 3.3 mô tả cấu trúc gói IP.

- VER (4 bits): Version hiện hành của IP được cài đặt.
- IHL(4 bits): Internet Header Length của Datagram, tính theo đơn vị word (32 bits).
- Type of service(8 bits): Thông tin về loại dịch vụ và mức ưu tiên của gói IP:
- Total Length (16 bits): Chỉ độ dài Datagram,
- Identification (16bits): Định danh cho một Datagram trong thời gian sống của nó.
- Flags(3 bits): Liên quan đến sự phân đoạn (Fragment) các Datagram:
- Fragment Offset (13 bits): Chỉ vị trí của Fragment trong Datagram.
- Time To Live (TTL-8 bits): Thời gian sống của một gói dữ liệu.
- Protocol (8 bits): Chỉ giao thức sử dụng TCP hay UDP.
- Header Checksum (16 bits): Mã kiểm soát lỗi CRC(Cycle Redundancy Check).
- Source Address (32 bits): địa chỉ của trạm nguồn.
- Destination Address (32 bits): Địa chỉ của trạm đích.
- Option (có độ dài thay đổi): Sử dụng trong trường hợp bảo mật, định tuyến đặc biệt.
- Padding (độ dài thay đổi): Vùng đệm cho phần Header luôn kết thúc ở 32 bits
- Data (độ dài thay đổi): Độ dài dữ liệu tối đa là 65.535 bytes, tối thiểu là 8 bytes.

<table>
<tr><td>VERS</td><td>IHL</td><td>Service type</td><td colspan="3">Toltal length</td></tr>
<tr><td colspan="3">Identification</td><td>Flags</td><td colspan="2">Fragment offset</td></tr>
<tr><td colspan="2">Time to live</td><td>Protocol</td><td colspan="3">Header checksum</td></tr>
<tr><td colspan="6">Source IP address</td></tr>
<tr><td colspan="6">Destination IP address</td></tr>
<tr><td colspan="5">IP options(may be none)</td><td>Padding</td></tr>
<tr><td colspan="6">IP Datagram data(up to 65535 bytes)</td></tr>
</table>

Hình 3.7 Cấu trúc gói dữ liệu IP

Phân mảnh và hợp nhất các gói IP: Các gói IP được nhúng trong khung dữ liệu ở tầng liên kết dữ liệu tương ứng trước khi chuyển tiếp trong mạng. Một gói dữ liệu IP có độ dài tối đa 65.536 byte, trong khi hầu hết các lớp liên kết dữ liệu chỉ hỗ trợ các khung dữ liệu nhỏ hơn độ lớn tối đa của gói dữ liệu IP nhiều lần (ví dụ độ dài lớn nhất của một khung dữ liệu Ethernet là 1500 byte). Vì vậy cần thiết phải có cơ chế phân mảnh khi phát và hợp nhất khi nhận đối với các gói dữ liệu IP.

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

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

3.2.4. Giao thức thông báo điều khiển mạng ICMP(Internet Control Message Protocol)

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

Các chức năng chính: ICMP là giao thức điều khiển của tầng IP, sử dụng để trao đổi các thông tin điều khiển dòng dữ liệu, thông báo lỗi và các thông tin trạng thái khác của bộ giao thức TCP/IP.

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

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

- Định hướng lại các tuyến (Redirect Router): Một Router gửi một thông điệp ICMP cho một trạm thông báo nên sử dụng Router khác. Thông điệp này có thể chỉ được dùng khi trạm nguồn ở trên cùng một mạng với hai thiết bị định tuyến.

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

Nhóm	Loại bản tin	Type
Thông điệp truy vấn (ICMP Queries)	Hỏi và phúc đáp Echo (Echo Request và Echo Reply)	8/0
	Hỏi và phúc đáp nhãn thời gian (Timestamp Request và Timestamp Reply)	13/14
	Yêu cầu và phúc đáp mặt nạ địa chỉ (Address mask Request và Address mask Reply)	17/18
	Yêu cầu và quảng bá bộ định tuyến (Router soliciation và Router advertisement)	10/9
Thông điệp thông báo lỗi (ICMP Error Reports)	Không thể đạt tới đích (Destination Unreachable)	3
	Yêu cầu ngừng hoặc giảm tốc độ phát (Source Quench)	4
	Định hướng lại (Redirection)	5
	Vượt ngưỡng thời gian (Time Exceeded)	11

Hình 3.8 Các loại thông điệp ICMP.

Các loại thông điệp ICMP: Các thông điệp ICMP được chia thành hai nhóm: các thông điệp truy vấn và các thông điệp thông báo lỗi. Các thông điệp truy vấn giúp cho người quản trị mạng nhận các thông tin xác định từ một node mạng khác. Các thông điệp thông báo lỗi liên quan đến các vấn đề mà bộ định tuyến hay trạm phát hiện ra khi xử lý gói IP. ICMP sử dụng địa chỉ IP nguồn để gửi thông điệp thông báo lỗi cho node nguồn của gói IP.

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

Giao thức TCP/IP sử dụng ARP để tìm địa chỉ vật lý của trạm đích. Ví dụ khi cần gửi một gói dữ liệu IP cho một hệ thống khác trên cùng một mạng vật lý Ethernet, hệ thống gửi cần biết địa chỉ Ethernet của hệ thống đích để tầng liên kết dữ liệu xây dựng khung gói dữ liệu. Thông thường, mỗi hệ thống lưu giữ và cập nhật bảng thích ứng địa chỉ IP-MAC tại chỗ (còn được gọi là bảng ARP Cache). Bảng thích ứng địa chỉ được cập nhật bởi người quản trị hệ thống hoặc tự động bởi giao thức ARP sau mỗi lần ánh xạ được một địa chỉ tương ứng mới.

Trước khi trao đổi thông tin với nhau, node nguồn cần phải xác định địa chỉ vật lý MAC của node đích bằng cách tìm kiếm trong bảng địa chỉ IP. Nếu không tìm thấy, node nguồn gửi quảng bá(Broadcast) một gói yêu cầu ARP(ARP Request) có chứa địa chỉ IP nguồn, địa chỉ IP đích cho tất cảc các máy trên mạng. Các máy nhận, đọc, phân tích và so sánh địa chỉ IP của nó với địa chỉ IP của gói. Nếu cùng địa chỉ IP, nghĩa là node đích tìm trong bảng thích ứng địa chỉ IP-MAC của nó và trả lời bằng một gói ARP Rely có chứa địa chỉ MAC cho node nguồn. Nếu không cùng địa chỉ IP, nó chuyển tiếp gói yêu cầu nhận được dưới dạng quảng bá cho tất cả các trạm trên mạng.

Tóm lại tiến trình của ARP được mô tả như sau:

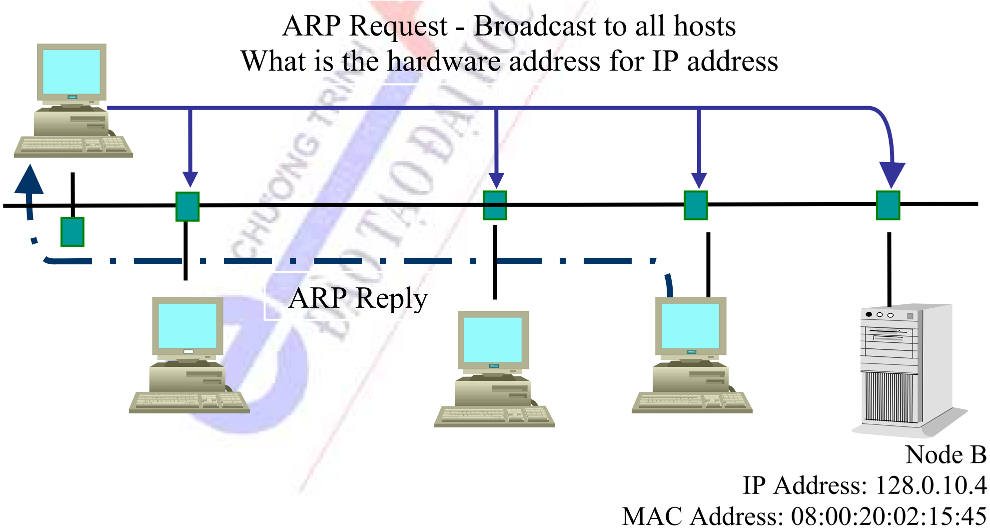
- IP yêu cầu địa chỉ MAC.
- Tìm kiếm trong bảng ARP.
- Nếu tìm thấy sẽ trả lại địa chỉ MAC.
- Nếu không tìm thấy, tạo gói ARP yêu cầu và gửi tới tất cả các trạm.
- Tuỳ theo gói tin trả lời, ARP cập nhật vào bảng ARP và gửi địa chỉ MAC cho IP.

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

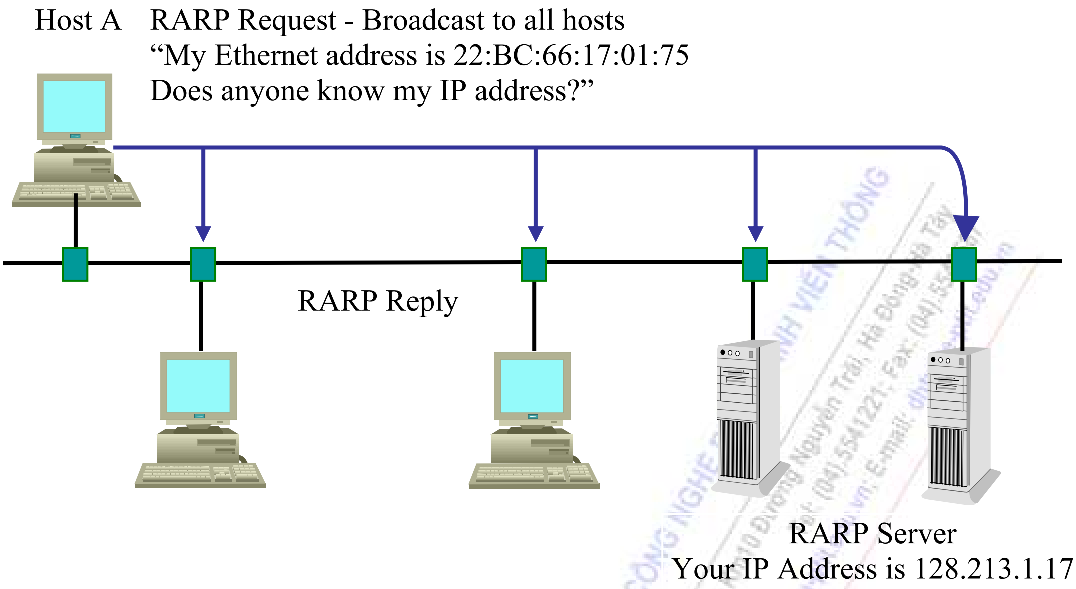
RARP là giao thức phân giải địa chỉ ngược. Quá trình này ngược lại với quá trình ARP ở trên, nghĩa là cho trước địa chỉ mức liên kết, tìm địa chỉ IP tương ứng. Như vậy RARP được sử dụng để phát hiện địa chỉ IP, khi biết địa chỉ vật lý MAC. Và cũng được sử dụng trong trường hợp trạm làm việc không có đĩa

Khuôn dạng gói tin RARP tương tự như khuôn dạng gói ARP đã trình bày, chỉ khác là trường Opcode có giá trị 0×0003 cho mã lệnh yêu cầu(RARP Request) và có giá trị 0×0004 cho mã lệnh trả lời(RARP Reply).

Nguyên tắc hoạt động của RARP ngược với ARP, nghĩa là máy đã biết trước địa chỉ vật lý MAC tìm địa chỉ IP tương ứng của nó. Hình 3.12 minh họa hoạt động của giao thức RARP. Máy A cần biết địa chỉ IP của nó, nó gửi gói tin RARP Request chứa địa chỉ MAC cho tất cả các máy trong mạng LAN. Mọi máy trong mạng đều có thể nhận gói tin này nhưng chỉ có Server mới trả lại RARP Reply chứa địa chỉ IP của nó.



Hình 3.9 Minh hoạ quá trình tìm địa chỉ MAC bằng ARP



Hình 3.10 Minh họa quá trình tìm địa chỉ IP bằng giao thức RARP.

3.3. Giao thức IPv6 (Internet Protocol Version Number 6)

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

3.3.1. Nguyên nhân ra đời của IPv6

- Internet phát triển mạnh, nhu cầu sử dụng địa chỉ IP tăng dẫn đến không gian địa chỉ ngày càng bị thu hẹp và tình trạng thiếu hụt địa chỉ tất yếu sẽ xảy ra trong vài năm tới.

- Việc phát triển quá nhanh của mạng Internet dẫn đến kích thước các bảng định tuyến trên mạng ngày càng lớn.

- Cài đặt IPv4 bằng thủ công hoặc bằng giao thức cấu hình địa chỉ trạng thái DHCP (Dynamic Host Configuration Protocol), khi mà nhiều máy tính và các thiết bị kết nối vào mạng thì cần thiết phải có một phương thức cấu hình địa chỉ tự động và đơn giản hơn.

- Trong quá trình hoạt động IPv4 đã phát sinh một số vấn đề về bảo mật và QoS. Khi kết nối thành mạng Intranet cần nhiều địa chỉ khác nhau và truyền thông qua môi trường công cộng. Vì vậy đòi hỏi phải có các dịch vụ bảo mật để bảo vệ dữ liệu ở mức IP.

- Mặc dù có các chuẩn đảm bảo chất lượng dịch vụ QoS trong IPv4 trường IPv4 TOS (Type of Service), nhưng hạn chế về mặt chức năng, cần thiết hỗ trợ tốt hơn cho các ứng dụng thời gian thực.

Vì vậy việc cần thiết phải thay thế giao thức IPv4 là tất yếu. Thiết kế IPv6 nhằm mục đích tối thiểu hóa ảnh hưởng qua lại giữa các giao thức lớp trên và lớp dưới bằng cách tránh việc bổ sung một cách ngẫu nhiên các chức năng mới.

3.3.2. Các đặc trưng của IPv6

IPv6 được chọn thay thế cho giao thức IPv4 không chỉ do IPv4 không còn phù hợp với yêu cầu phát triển hiện tại của mạng Internet mà còn vì những ưu điểm của giao thức IPv6:

- Đơn giản hoá Header: Một số trường trong Header của IPv4 bị bỏ hoặc chuyển thành các trường tuỳ chọn. Giảm thời gian xử lý và tăng thời gian truyền.

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

- Khả năng địa chỉ hoá và chọn đường linh hoạt: IPv6 cho phép nhiều lớp địa chỉ với số lượng các node. Cho phép các mạng đa mức và phân chia địa chỉ thành các mạng con riêng lẻ. Có khả năng tự động trong việc đánh địa chỉ. Mở rộng khả năng chọn đường bằng cách thêm trường "Scop" vào địa chỉ quảng bá (Multicast).

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

- Khả năng bảo mật: IPsec bảo vệ và xác nhận các gói tin IP:

  + Mã hóa dữ liệu: Phía gửi sẽ tiến hành mã hóa gói tin trước khi gửi.

  + Toàn vẹn dữ liệu: Phía nhận có thể xác nhận gói tin nhận được để đảm bảo rằng dữ liệu không bị thay đổi trong quá trình truyền.

  + Xác nhận nguồn gốc dữ liệu: Phía nhận có thể biết được phía gửi gói tin. Dịch vụ này phụ thuộc vào dịch vụ toàn vẹn dữ liệu.

  + Antireplay: Phía nhận có thể phát hiện và từ chối gói tin gửi lại.

- Chất lượng dịch vụ QoS (Quanlity Of Service): Chất lượng dịch vụ QoS trong IPv4 không cao.Trong Header IPv4 chứa địa chỉ nguồn và địa chỉ đích, truyền có độ tin cậy không cao. IPv6 Header có thêm một số trường mới để xử lý và xác định lưu lượng trên mạng. Do cơ chế xác nhận gói tin ngay trong Header nên việc hỗ trợ QoS có thể thực hiện được ngay cả khi gói tin được mã hóa qua IPsec.

- Giao thức phát hiện lân cận NDP (Neighbor Discovery Protocol) của IPv6 là một dãy các thông báo ICMPv6 cho phép quản lý tương tác giữa các node lân cận, thay thế ARP trong IPv4. Các thông báo ICMPv4 Router Discovery và ICMPv4 Redirect được thay bởi các thông báo Multicast, Unicast Neighbor Discovery.

- Khả năng mở rộng: Thêm vào trường Header mở rộng tiếp ngay sau Header, IPv6 có thể được mở rộng thêm các tính năng mới một cách dễ dàng.

- Tính di động: IPv4 không hỗ trợ cho tính di động, IPv6 cho phép nhiều thiết bị di động kết nối vào Internet theo chuẩn của PCMCIA (Personal Computer Memory Card International Association) qua mạng công cộng nhờ sóng vô tuyến.

3.3.3. So sánh IPv4 và IPv6

IPv4	IPv6
Độ dài địa chỉ là 32 bit (4 byte)	Độ dài địa chỉ là 128 bit (16 byte)
IPsec chỉ là tùy chọn	IPsec được gắn liền với IPv6.
Header của địa chỉ IPv4 không có trường xác định luồng dữ liệu của gói tin cho các Router để xử lý QoS.	Trường Flow Label cho phép xác định luồng gói tin để các Router có thể đảm bảo chất lượng dịch vụ QoS
Việc phân đoạn được thực hiện bởi cả Router và máy chủ gửi gói tin	Việc phân đoạn chỉ được thực hiện bởi máy chủ phía gửi mà không có sự tham gia của Router
Header có chứa trường Checksum	Không có trường Checksum trong IPv6 Header
Header có chứa nhiều tùy chọn	Tất cả các tùy chọn có trong Header mở rộng
Giao thức ARP sử dụng ARP Request quảng bá để xác định địa chỉ vật lý.	Khung ARP Request được thay thế bởi các thông báo Multicast Neighbor Solicitation.
Sử dụng giao thức IGMP để quản lý thành viên các nhóm mạng con cục bộ	Giao thức IGMP được thay thế bởi các thông báo MLD (Multicast Listener Discovery)
Sử dụng ICMP Router Discovery để xác định địa chỉ cổng Gateway mặc định phù hợp nhất, là tùy chọn.	Sử dụng thông báo quảng cáo Router (Router Advertisement) và ICMP Router Solicitation thay cho ICMP Router Discovery, là bắt buộc.
Địa chỉ quảng bá truyền thông tin đến tất cả các node trong một mạng con	Trong IPv6 không tồn tại địa chỉ quảng bá, thay vào đó là địa chỉ Multicast
Thiết lập cấu hình bằng thủ công hoặc sử dụng DHCP	Cho phép cấu hình tự động, không sử dụng nhân công hay cấu hình qua DHCP
Địa chỉ máy chủ được lưu trong DNS với mục đích ánh xạ sang địa chỉ IPv4	Địa chỉ máy chủ được lưu trong DNS với mục đích ánh xạ sang địa chỉ IPv6
Con trỏ địa chỉ được lưu trong IN – ADDR ARPA DNS để ánh xạ địa chỉ IPv4 sang tên máy chủ	Con trỏ địa chỉ được lưu trong Ipv6 – INT DNS để ánh xạ địa chỉ từ IPv4 sang tên máy chủ
Hỗ trợ gói tin kích thước 576 bytes (có thể phân đoạn)	Hỗ trợ gói tin kích thước 1280 bytes (không cần phân đoạn)

Hình 3.11 So sánh IPv4 và IPv6

3.4. Các lớp địa chỉ IPv6

3.4.1. Phương pháp biểu diễn địa chỉ IPv6

Địa chỉ IPv6 được biểu diễn bằng chuỗi số Hexa được chia thành các nhóm 16 bit tương ứng với bốn chữ số Hexa, ngăn cách nhau bởi dấu ":". Ví dụ một địa chỉ IPv6 : 4021 : 0000 : 240E : 0000 : 0000 : 0AC0 : 3428 : 121C.Ccó thể thu gọn bằng cách thay các nhóm 0 liên tiếp bằng kí hiệu "::". Ví dụ 12AB : 0000 : 0000 : CD30 : 0000 : 0000 : 0000 : 0000 /60 có thể viết là 12AB : 0 : 0 : CD30 : 0 : 0 : 0 : 0 /60 hoặc 12AB :: CD30 : 0 : 0 : 0 : 0 /60 hoặc 12AB : 0 : 0 : CD30 :: /60 . Không được viết 12AB :: CD30 /60 hay 12AB :: CD30 :: /60

3.4.2. Phân loại địa chỉ IPv6

- Địa chỉ Unicast: Là địa chỉ của một giao diện. Một gói tin được chuyển đến địa chỉ Unicast sẽ chỉ được định tuyến đến giao diện gắn với địa chỉ đó
- Địa chỉ Anycast: Là địa chỉ của một tập giao diện thuộc của nhiều node khác nhau. Mỗi gói tin tới địa chỉ Anycast được chuyển tới chỉ một trong tập giao diện gắn với địa chỉ đó (là giao diện gần node gửi nhất và có Metrics nhỏ nhất).
- Địa chỉ Multicast: Địa chỉ của tập các giao diện thuộc về nhiều node khác nhau. Một gói tin gửi tới địa chỉ Multicast sẽ được gửi tất cả các giao diện trong nhóm.

3.4.3. So sánh địa chỉ IPv4 và địa chỉ IPv6

Địa chỉ IPv6 và IPv4 có một số điểm chung như cùng sử dụng một số loại địa chỉ với một số chức năng tương tự, nhưng trong IPv6 có một số thay đổi thể hiện trong bảng sau:

Bảng So sánh địa chỉ IPv4 và IPv6

IPv4 Address	IPv6 Address
Phân lớp địa chỉ (Lớp A, B, C và D)	Không phân lớp địa chỉ. Cấp phát theo tiền tố
Lớp D là Multicast (224.0.0.0/4)	Địa chỉ multicast có tiền tố FF00::/8
Sử dụng địa chỉ Broadcast	Không có Broadcast, thay bằng Anycast
Địa chỉ unspecified là 0.0.0.0	Địa chỉ Unspecified là ::
Địa chỉ Loopback 127.0.0.1	Địa chỉ Loopback là ::1
Sử dụng địa chỉ Public	Tương ứng là địa chỉ Unicast toàn cầu
Địa chỉ IP riêng (10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16)	Địa chỉ Site-lLcal (FEC0::/48)
Địa chỉ tự cấu hình (169.254.0.0/16)	Địa chỉ Link-Local (FE80::/64)
Dạng biểu diễn: chuỗi số thập phân cách nhau bởi dấu chấm	Dạng biểu diễn: chuỗi số Hexa cách nhau bởi dấu hai chấm; có thể nhóm chuỗi số 0 liền nhau vào một kí tự
Sử dụng mặt nạ mạng con	Chỉ sử dụng kí hiệu tiền tố để chỉ mạng
Phân giải tên miền DNS: bản ghi tài nguyên địa chỉ máy chủ IPv4 (A)	Phân giải tên miền DNS: bản ghi tài nguyên địa chỉ máy chủ IPv6 (AAAA)
Tên miền ngược: IN-ADDR.ARPA	Tên miền ngược: IP6.INT domain

Câu hỏi và bài tập

1. Hãy trình bày tổng quát mô hình kiến trúc TCP/IP
2. Vai trò và chức năng các tầng trong mô hình TCP/IP
3. Tầng ứng dụng (Process/Application Layer) và các giao thức ứng dụng.
4. Tầng vận chuyển Host to Host và các giao thức.
5. Tầng mạng (Internet Layer) và các giao thức tầng mạng.
6. Trình bày khái quát các giao thức định tuyến RIP, OSPF, BGP.
7. Quá trình đóng gói dữ liệu Encapsulation
8. Quá trình phân mảnh các gói dữ liệu Fragment
9. Khái niệm đơn vị truyền cực đại MTU (Maximum Transmission Unit).
10. Quá trình phân mảnh làm tăng thời gian xử lý, làm giảm tính năng của mạng.
11. Vai trò và chức năng, cấu trúc gói tin của UPP (User Datagram Protocol)
12. Vai trò và chức năng của TCP :
13. Trình bày các đặc điểm của TCP
14. Điều khiển lưu lượng và điều khiển tắc nghẽn
15. Trình bày các cơ chế cửa sổ động, phát lại thích nghi, điều khiển tắc nghẽn.
16. Thiết lập và huỷ bỏ liên kết:
17. Độ tin cậy và điều khiển luồng của TCP:
18. Các chức năng chính của IP:
19. Địa chỉ IP, cấu trúc gói dữ liệu IP.
20. Phân mảnh và hợp nhất các gói IP:
21. Trình bày chức năng giao thức thông báo điều khiển mạng ICMP.
22. Tiến trình của Giao thức phân giải địa chỉ ARP (Address Resolution Protocol)
23. Nguyên tắc hoạt động, khuôn dạng gói tin của giao thức RARP
24. Các đặc trưng của IPv6
25. Chất lượng dịch vụ và bảo mật trong IPv6
26. Cấu trúc khuôn dạng Datagram Ipv6
27. Header mở rộng
28. So sánh IPv4 header và IPv6 header
29. Lớp địa chỉ IPv6, biểu diễn, các loại địa chỉ IPv6
30. So sánh địa chỉ IPv4 và địa chỉ IPv6
31. Mô hình kiến trúc TCP/IP và so sánh với mô hình OSI.

CHƯƠNG 4: KỸ THUẬT MẠNG CỤC BỘ

Nội dung của chương này sẽ trình bày các khái niệm cơ bản về kỹ thuật mạng cục bộ LAN, các phương pháp truy nhập ngẫu nhiên và có điều khiển được sử dụng trong các mạng quảng bá. Nội dung của chương gồm các phần sau:

- Các phương thức truy nhập đường truyền.
- Mạng Ethernet và họ chuẩn IEEE 802.
- Mạng cục bộ Token Ring.
- Giao diện số liệu phân bố sử dụng cáp sợi quang.
- Giới thiệu mạng LAN ATM.

4.1. Các phương thức truy nhập đường truyền

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

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

Nguyên tắc hoạt động: Khi một trạm truyền dữ liệu, trước hết nó sẽ phải "nghe" xem đường truyền "bận" hay "rỗi". Nếu "rỗi" nó sẽ truyền dữ liệu đi (theo khuôn dạng chuẩn), nếu đường truyền đang "bận" thì nó sẽ thực hiện 1 trong 3 giải thuật sau:

1. Trạm tạm "rút lui" chờ đợi trong một thời gian ngẫu nhiên, sau đó lại bắt đầu nghe đường truyền (Non persistent)
2. Trạm tiếp tục "nghe" đến khi đường truyền rỗi thì truyền dữ liệu đi với xác suất bằng 1 (persistent).
3. Trạm tiếp tục "nghe" đến khi đường truyền rỗi thì truyền dữ liệu đi với xác suất bằng $0<p<1$ xác định trước (p-persistent).

Ưu, nhược điểm của từng giải thuật trên: Giải thuật 1 có hiệu quả trong việc tránh xung đột. Tuy nhiên, có thể có thời gian "chết" của đường truyền vì cả hai cùng đợi. Giải thuật 2 ngược lại, cố gắng giảm được thời gian "chết" của đường truyền nhưng nếu có hơn một trạm cùng truyền thì khả năng xảy ra xung đột sẽ cao và giải thuật 3 với giá trị *p* chọn một cách hợp lý có thể tối thiểu hoá được khả năng xung đột cũng như giảm được thời gian "chết" của đường truyền.

Tuy nhiên, xung đột xảy ra thường do độ trễ truyền dẫn. CSMA thực chất là các trạm chỉ "Nghe trước khi nói" mà không "nghe trong khi nói", nên thực tế có xung đột nhưng các trạm vẫn không thể biết và tiếp tục truyền dữ liệu dẫn đến tắc nghẽn, xung đột thông tin trên đường truyền. Giải pháp CSMA/CD (hay còn gọi là LWT - Listen while talk) có thể phát hiện xung đột như sau:

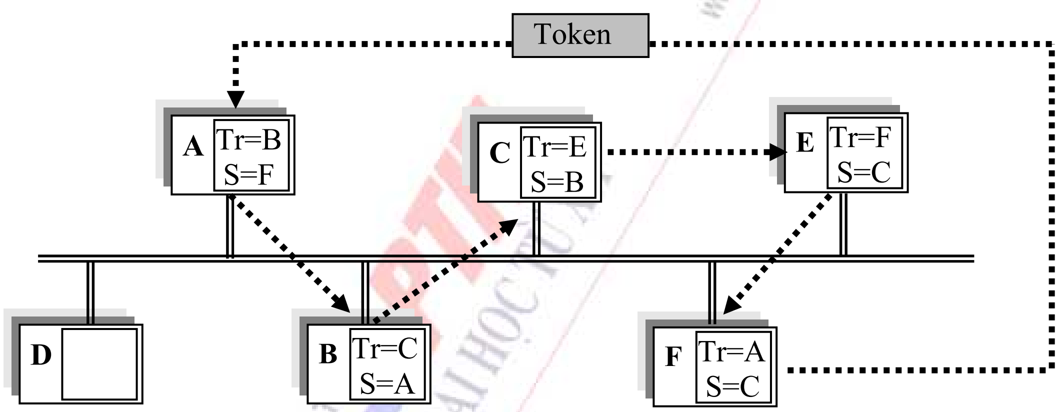
- Khi một trạm đang truyền, vẫn tiếp tục "nghe" đường truyền. Nếu phát hiện thấy xung đột, nó ngừng ngay việc truyền nhưng vẫn tiếp tục gửi sóng mang đi thêm một thời gian để đảm bảo rằng các trạm trên mạng đều có thể "nghe" được xung đột đó.

- Sau đó, trạm chờ đợi trong một thời đoạn ngẫu nhiên, nó tiếp tục thử truyền lại theo nguyên tắc các giải thuật của CSMA.

Với CSMA/CD, thời gian chiếm dụng vô ích đường truyền giảm xuống đúng bằng thời gian dùng để phát hiện một xung đột. CSMA/CD cũng sử dụng 3 giải thuật "kiên nhẫn" của CSMA, trong đó giải thuật (2) (1-persistent) là được dùng hơn cả.

4.1.2. Token Bus

Để cấp phát quyền truy nhập đường truyền cho một trạm cần truyền dữ liệu, một thẻ bài được lưu chuyển trên một vòng logic được thiết lập bởi các trạm có nhu cầu. Khi một trạm nhận được thẻ bài nó có quyền truy nhập đường truyền trong một thời gian xác định và có thể truyền một hoặc nhiều đơn vị dữ liệu. Khi đã hết dữ liệu hoặc hết thời gian cho phép, nó chuyển thẻ bài cho trạm tiếp theo trên vòng logic. Thẻ bài (Token) là một đơn vị dữ liệu đặc biệt, có kích thước và nội dung gồm các thông tin điều khiển được quy định riêng cho mỗi phương pháp.



Hình 4.1 Token BUS

Thiết lập vòng logic: Vòng logic giữa các trạm có nhu cầu truyền, được xác định theo một chuỗi có thứ tự mà trạm cuối cùng liền kề với trạm đầu tiên của vòng. Mỗi trạm được biết địa chỉ của trạm liền kề trước và sau nó. Thứ tự của các trạm trên vòng logic độc lập với thứ tự vật lý. Các trạm không hoặc chưa có nhu cầu truyền dữ liệu thì không đưa vào vòng logic và chúng chỉ có thể tiếp nhận dữ liệu.

Duy trì trạng thái thực tế của mạng

- Bổ sung định kỳ các trạm nằm ngoài vòng logic nếu có nhu cầu truyền dữ liệu.

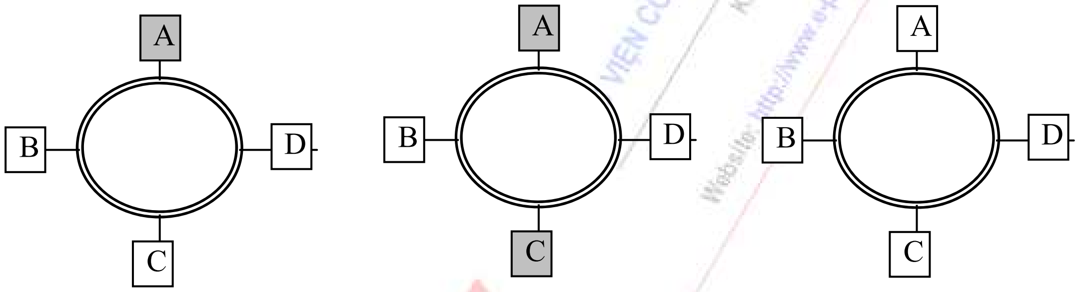
- Loại bỏ một trạm không còn nhu cầu truyền dữ liệu ra khỏi vòng logic.

- Quản lý lỗi: Lỗi: có thể "đứt vòng" hoặc trùng địa chỉ.

- Khởi tạo vòng logic: Khi cài đặt mạng hoặc đứt vòng cần phải khởi tạo lại vòng. Việc khởi tạo vòng logic được thực hiện khi một hoặc nhiều trạm phát hiện Bus hoạt động vượt qua giá trị ngưỡng thời gian (Time-out) hoặc thẻ bài bị mất. Có nhiều nguyên nhân, chẳng hạn mạng mất nguồn hoặc trạm giữ thẻ bài hỏng. Lúc đó, trạm phát hiện sẽ gửi thông báo "yêu cầu thẻ bài" tới một trạm được chỉ định trước có trách nhiệm sinh thẻ bài mới và chuyển đi theo vòng logic.

4.1.3. Token ring

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



A có nhu cầu truyền dữ liệu đến C. Đợi Free Token,chuyển sang trạng thái Busy, gửi kèm Packet dữ liệu

Node B đọc, phân tích và so sánh địa chỉ đích với địa chỉ MAC. Node C sao chép dữ liệu

Khi Packet dữ liệu quay về, Node A chuyển trạng thái Token thành Free.

Hình 4.2 Token Ring

Sự quay về lại trạm nguồn của dữ liệu và thẻ bài nhằm tạo ra cơ chế báo nhận tự nhiên: trạm đích có thể gửi vào đơn vị dữ liệu (phần header) các thông tin về kết quả tiếp nhận dữ liệu của mình. Chẳng hạn, các thông tin đó có thể là: (1) trạm đích không tồn tại hoặc không hoạt động; (2) trạm đích tồn tại nhưng dữ liệu không được sao chép ; (3) dữ liệu đã được tiếp nhận; (4) có lỗi.

Các vấn đề liên quan: Cần giải quyết hai vấn đề có thể dẫn đến phá vỡ hệ thống. Một là mất thẻ bài. Hai là một thẻ bài "bận" lưu chuyển không dừng trên vòng. Có thể có nhiều giải pháp khác nhau để khắc phục vấn đề này, sau đây là một giải pháp được khuyến nghị:

Đối với vấn đề mất thẻ bài: Có thể quy định trước một trạm điều khiển chủ động (Active Monitor), phát hiện mất thẻ bài bằng cách dùng cơ chế ngưỡng thời gian Time-out. Sau khoảng thời gian đó, nếu không nhận lại được thẻ bài, trạm sẽ phát hiện tình trạng phục hồi bằng cách phát lại thẻ bài mới.

Đối với vấn đề thẻ bài "bận"lưu chuyển trên vòng không dừng: trạm Monitor sử dụng một bit trên thẻ bài đánh dấu (M=1) khi gặp một thẻ bài bận đi qua nó. Nếu nó gặp lại một thẻ bài bận với bit đã đánh dấu đó thì có nghĩa là trạm nguồn đã không nhận lại được đơn vị dữ liệu của mình và thẻ bài bận cứ quay vòng mãi. Lúc đó, trạm Monitor sẽ đổi bit trạng thái của thẻ bài thành "rỗi" và chuyển tiếp trên vòng. Tuy nhiên, cần chọn một giải thuật để chọn trạm thay thế cho trạm monitor khi bị hỏng.

4.1.4. So sánh CSMA/CD với các phương pháp dùng thẻ bài

Độ phức tạp của phương pháp dùng thẻ bài lớn hơn nhiều so với phương pháp truy nhập ngẫu nhiên CSMA/CD, xử lý đơn giản hơn.Trong điều kiện tải nhẹ phương pháp thẻ bài không cao do một trạm có thể đợi khá lâu mới đến lượt (có thẻ bài). Ngược lại,: trong điều kiện tải nặng, phương pháp dùng thẻ bài hiệu quả hơn so với CSMA/CD.

Ưu điểm lớn nhất của phương pháp dùng thẻ bài là khả năng điều hoà lưu thông trong mạng bằng cách cho phép các trạm truyền số lượng đơn vị dữ liệu khác nhau khi nhận được thẻ bài hoặc bằng cách lập chế độ ưu tiên cấp phát cho các trạm cho trước.

4.2. Ethernet và chuẩn IEEE 802

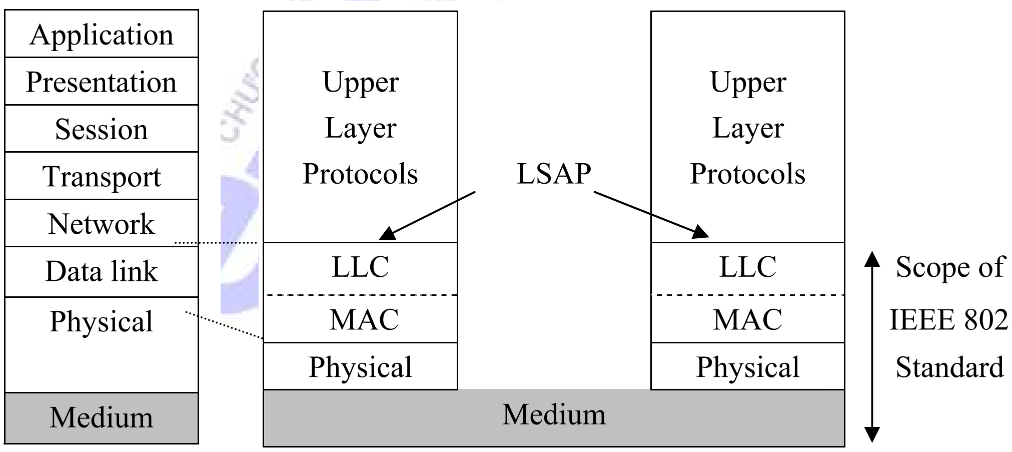
4.2.1. Giới thiệu chung về Ethernet

Ethernet là công nghệ của mạng LAN cho phép truyền tín hiệu giữa các máy tính với tốc độ 10Mb/s đến 10 Gigabit/s. Trong các kiểu Ethernet thì kiểu sử dụng cáp xoắn đôi là hay thông dụng nhất. Hiện nay có khoảng 85% mạng LAN sử dụng công nghệ Ethernet.

Năm 1980, Xerox, tập đoàn Intel và tập đoàn Digital Equipment đưa ra tiêu chuẩn Ethernet 10 Mbps (Tiêu chuẩn DIX).

IEEE (Institute of Electrical and Electronics Engineers, Inc- Viện công nghệ điện và điện tử) đưa ra tiêu chuẩn về Ethernet đầu tiên vào năm 1985 với tên gọi "IEEE 802.3 Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications"

Gần đây, với các phương tiện truyền dẫn và công nghệ mới, công nghệ Ethernet đã ngày càng phát triển và đạt được tốc độ trao đổi số liệu đến 10 Gigabit trên giây.



Hình 4.3 Quan hệ của các chuẩn IEEE 802 với mô hình tham chiếu OSI.

Thành phần mạng Ethernet bao gồm:

- Data terminal Equipment (DTE): Các thiết bị truyền và nhận dữ liệu DTEs thường là PC, Workstation, File Server, Print Server ...

- Data Communication Equipment (DCE): Là các thiết bị kết nối mạng cho phép nhận và chuyển khung trên mạng. DCE có thể là các thiết bị độc lập như Repeter, Switch, Router hoặc các khối giao tiếp thông tin như Card mạng, Modem ..

- Interconnecting Media: Cáp xoắn đôi, cáp đồng (mỏng/dày), cáp quang.

Những đặc điểm cơ bản của Ethernet

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

4.2.2. Chức năng các tầng trong IEEE 802

Chuẩn IEEE 802 bao gồm chức năng tầng vật lý (Physical) và liên kết dữ liệu (Data Link) trong mô hình OSI. Điều này có nghĩa là Uỷ ban 802 của IEEE nhấn mạnh tới việc tiêu chuẩn hoá các công nghệ phần cứng sử dụng tại tầng vật lý và tầng liên kết dữ liệu.

Chuẩn IEEE chia tầng liên kết dữ liệu thành hai tầng con, tầng điều khiển truy nhập MAC (Media Access Control) và điều khiển liên kết logic LLC (Logical Link Control).

*Tầng LLC (Logical Link Control):*Tất cả mạng LAN theo chuẩn IEEE có cùng lớp LLC được định nghĩa bởi 802.2. Dùng chung tầng con LLC, cơ chế các tầng trên như nhau bất kể loại phần cứng nào được sử dụng. Giao diện giữa tầng kề trên với LLC được định nghĩa bởi các điểm LSAP (Link Service Access Points). LSAP là các địa chỉ liên kết logic. Địa chỉ Ethernet có nhiều địa chỉ LSAP, những địa chỉ này cho phép liên kết giữa các thực thể trên mạng. Địa chỉ MAC là duy nhất.

- Nếu thiết bị là DTE, nó quy định giao diện giữa giữa tầng MAC và tầng mạng. LLC quản lý liên kết dữ liệu và định nghĩa các điểm truy nhập dịch vụ (Service Access Point - SAP). LLC Sublayer được tiêu chuẩn hoá trong IEEE 802.2

- Nếu thiết bị DCE là Bridge. Brige cung cấp giao diện LAN-to-LAN sử dụng chung Protocol (Ethenet to Ethenet) hoặc giữa các LAN sử dụng khác Protocol (như Ethernet to Token Ring). Bridge được tiêu chuẩn hoá trong IEEE 802.1

- LLC Header:

DSAP (1)	SSAP (1)	Cont (1)	Data (43 …)

+ DSAP (Destination Service Access Point): Con trỏ thông báo cho NIC vị trí bộ đệm để lưu trữ thông tin nhận.

+ SSAP (Source Service Access Point) Vị trí bộ đệm lưu trữ thông tin đi.

+ DSAP and SSAP cho phép nhiều giao thức cùng sử dụng chung NIC Card.

+ Cont (Control). Kiểu của LLC.

+ Data: Dữ liệu được đưa xuống từ lớp Network, có chiều dài tối đa là 1497 bytes.

Tầng con LLC cung cấp các dịch vụ sau:

- Type 1: Dịch vụ Datagram không liên kết và không có cơ chế báo nhận biết (Unacknowledgement). Cung cấp kết nối Point to Point, Multipoint và Broadcast.

- Type 2: Dịch vụ mạch ảo, kiểu liên kết (Connection -Oriented). Cung cấp các dịch vụ tuần tự, kiểm soát luồng, không lỗi giữa các LSAP.

- Type 3: Dịch vụ Datagram kiểu không liên kết và có cơ chế báo nhận biết (Acknowledgement).

Tầng Ethernet Mac Sublayer: Liên quan đến các phương pháp truy nhập và kiểm soát truy nhập đến đường truyền chung. Token RING và Ethernet thực hiện trong tầng MAC bằng các phương pháp khác nhau cùng chia sẻ đường truyền.

- Tạo Frame: Thêm các trường PRE, SFD, DE, SA, Length/Type, PAD, FCS và dữ liệu từ LLC đưa xuống tạo thành khung dữ liệu cung cấp cho tầng Vật lý.

- Nhận khung dữ liệu từ tầng Vật lý, kiểm tra lỗi và gửi dữ liệu cho tầng LLC.

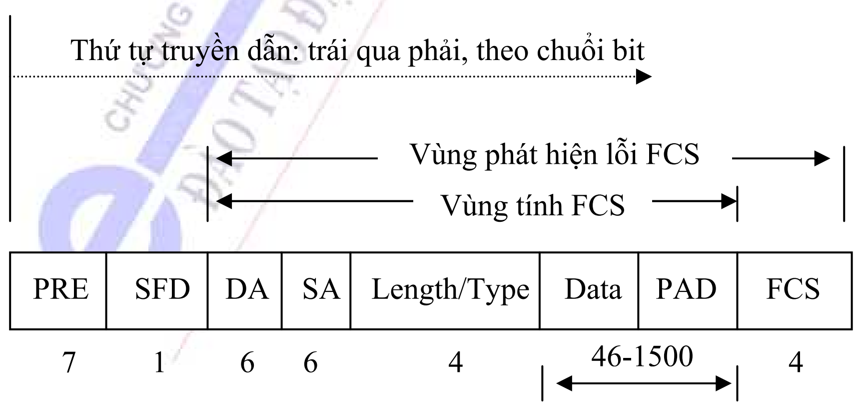
- Điều khiển truy nhập phương tiện truyền dẫn.

Tầng Vật lý: Xác định tốc độ truyền, phương pháp mã hoá và phương tiện truyền dẫn và cách thức kết nối vật lý. Tầng vật lý của IEEE 802.3 được phân chia là 2 phần:

- Phần độc lập với đường truyền đặc tả giao diện giữa tầng MAC và tầng vật lý.

- Phần phụ thuộc đường truyền và đặc tả giao diện với đường truyền của LAN và các tín hiệu trao đổi với đường truyền. Có nhiều tuỳ chọn khác nhau về kiểu đường truyền, phương thức truyền tín hiệu và tốc độ truyền, cách thức mã hoá.

4.2.3. Cấu trúc khung Ethernet:



Hình 4.4 Token Ring

- PRE (7bytes): Đánh dấu điểm đầu khung, đồng bộ.
- SFD (1byte): 10101011
- DA/SA (6 bytes): Địa chỉ đích, địa chỉ nguồn.
- Length/Type (2 bytes): Chiều dài dữ liệu nếu nhỏ hơn 1500.
- Data: Dữ liệu gửi từ LLC đưa xuống, gồm n byte (n<1501).
- PAD: Có thể có hay không. Nếu n<46 thì thêm 1 số byte (toàn 0) vào PAD để chiều dài tổng cộng của Data+Pad là 46 byte
- FCS (4 bytes) kiểm tra lỗi của các trường DA, SA, Length /Type và Data và PAD.

4.2.4. Họ IEEE 802

Bridge được tiêu chuẩn hoá trong IEEE 802.1, kiến trúc mạng, cung cấp giao diện LAN-to-LAN sử dụng chung Protocol LAN (ví dụ: Ethenet to Ethenet) hoặc giữa các LAN sử dụng khác Protocol (như Ethernet to Token Ring).

Logical Link Control (LLC) được tiêu chuẩn hoá trong IEEE 802.2, đặc tả chuẩn giao diện (Interface) giữa MAC và tầng mạng LLC quản lý liên kết dữ liệu và định nghĩa các điểm truy nhập dịch vụ (Service Access Point – SAP). IEEE 802.2 cung cấp 3 kiểu giao thức LLC:Type1, Type2, Type3. Các giao thức này theo phương thức cân bằng (Balanced Mode) của giao thức HDLC và có các khuôn dạng dữ liệu và chức năng tương tự.

EEE 802.3 đặc tả một mạng cục bộ dựa trên mạng Ethernet do Digital, Intel và Xerox hợp tác pháp triển từ năm 1980. IEEE 802.3 tương tự như DIX Ethernet, bao gồm cả tầng vật lý và tầng con MAC với các đặc tả sau:

- Đặc tả dịch vụ MAC (MAC ServicesSecification)
- Giao thức MAC (MAC Protocol).
- Đặc tả vật lý (Medium-Independent Physical Specification) độc lập với đường truyền
- Đặc tả vật lý phụ thuộc đường truyền (Medium - Dependent Physical Specification)
- Đặc tả dịch vụ MAC định nghĩa các dịch vụ IEEE 802.3 cung cấp cho tầng LLC hoặc người sử dụng ở tầng cao hơn.

Tầng MAC với giao thức truy nhập đường truyền CSMA/CD, làm giảm tình trạng xung đột và nghẽn thông tin bằng cách mỗi thiết bị trước khi truyền phải lắng nghe đường truyền và trong khi truyền vẫn tiếp tục nghe để xử lý khi có hiện tượng va chạm.

Tầng vật lý của IEEE 802.3 được chia làm hai phần. Phần độc lập với đường truyền, đặc tả giao diện giữa MAC và tầng vật lý. Phần phụ thuộc đường truyền là bắt buộc phải có và đặc tả giao diện với đường truyền của LAN và các tín hiệu trao đổi với đường truyền. Có các dạng sau cho tầng vật lý của IEEE 802.3:

- Tốc độ truyền tín hiệu (1 Mb /s hoặc 10Mb /s hoặc 100 Mb /s)
- BASE (nếu là Baseband) hoặc BROAD (nếu là Broadband)
- Chỉ định đặc trưng đường truyền.

10BASE -F: Dùng cáp quang, tốc độ 10 Mb/s, phạm vi cáp 4km Chuẩn này được phân thành 3 dạng con: 10BASE-FL, 10BASE-FB và 10BASE-FP.

10BASE-T: Sử dụng nột dải tần rộng hỗ trợ cho các tốc độ tín hiệu 10Mb/s. Dùng cáp UTP, trợ kháng 75 Ohm, với mạng hình sao.

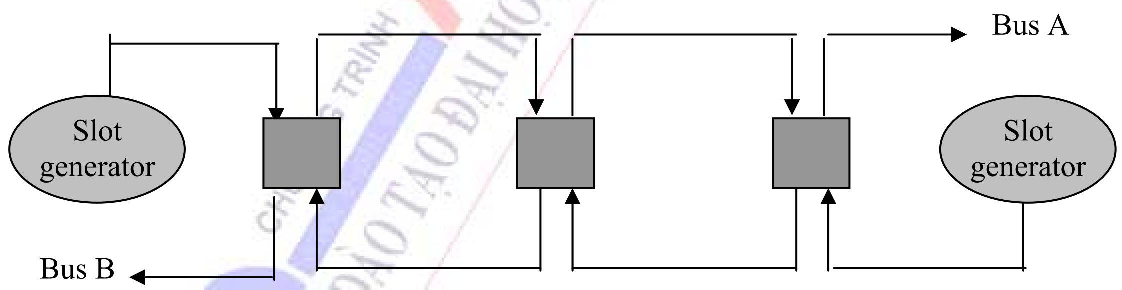
100 BASE-X: Gọi là Fast Ethernet, mạng hình sao tương tự 10BASE-, tốc độ 100Mb/s. Chuẩn này gồm 100 BASE-TX dùng cho cáp UTP hoặc STP 2 đôI, 100 BASE-FX dùng cho cáp quang, 100 BASE-T4 dùng cho cáp UTP 4 đôi (Four Twisted Pairs).

10BROAD36: Dùng Broadband, tốc độ 10Mb/s, cáp đồng trục 75 Ohm, phạm vi cáp 1800 m (lên tới 3600m trong cấu hình cáp đôi), sử dụng topo dạng BUS.

IEEE 802.4: Mô tả một mạng cục bộ với cấu trúc dạng hình BUS và cơ chế điều khiển truy nhập đường truyền thẻ bài Token BUS. Mạng dùng cáp đồng trục 75 ohm với cả hai dạng Baseband và Broadband. IEEE 802.4 bao gồm tầng vật lý và tầng MAC. IEEE 802.4 sử dụng cáp đồng 75-ohm (tốc độ 1 Mbps, 5 Mbps và 10 Mbps) hoặc cáp quang (tốc độ 5 Mbps, 10 Mbps và 20 Mpbs). Nó được thiết kế để ứng dụng trong các văn phòng và trong các môi trường công nghiệp và quân sự.

Chuẩn IEEE 802.5: Là chuẩn đặc tả mạng cục bộ với mạng dạng vòng (RING) sử dụng thẻ bài Token RING để điều khiển truy nhập đường truyền. IEEE 802.5 bao gồm cả tầng vật lý và tầng con MAC.

IEEE 802.6: Mô tả một mạng tốc độ cao kết nối nhiều LAN thuộc các khu vực khác nhau của một đô thị (còn được gọi là MAN - Metropolitan Area Network). Mạng sử dụng cáp quang với mạng dạng Bus kép (Dual - BUS), vì thế còn được gọi là DQDB (Distributed Queue Dual Bus). Lưu thông trên mỗi Bus là một chiều và khi cả cặp Bus cùng hoạt động sẽ tạo thành một cấu hình bỏ qua được các lỗi (Fault - Tolerant). Phương pháp điều khiển truy nhập dựa trên một giải thuật xếp hàng phân tán có tên là QPDS (Queued - Packet, Distrubuted -Switch). DQDB là Bus quảng bá đa truy nhập, tương tự như CSMA/CD, nhưng phải dùng một phương pháp truy nhập theo "khe” (Slotted Access) để khắc phục các hạn chế về truy nhập của CSMA/CD. Để quảng bá dữ liệu cần phải cài đặt Bus dưới dạng cặp Bus một chiều tương tự như một dạng vòng (Ring). Vì hai Bus chuyển dữ liệu ngược chiều nhau nên việc quảng bá dữ liệu đòi hỏi phải truyền cả trên hai Bus.



Hình 4.5: Sơ đồ nối bus của DQDB

Đơn vị dữ liệu được dùng trong các mạng DQDB được thiết kế tương thích với thế hệ mới của các mạng diện rộng công cộng gọi là B-ISDN (Broadband Integrated Services Digital Networks). Các mạng này sử dụng kỹ thuật chuyển mạch gói nhanh (Fast Packet Switching) với công nghệ hứa hẹn nhất là ATM. Vì thế đơn vị dữ liệu dùng trong các mạng DQDB cũng được gọi là "tế bào” (Cell) với khuôn dạng tổng quát gồm 53 bytes, trong đó có bytes của phần Header cố định và 48 bytes dữ liệu.

Các mạng IEEE 802.6 cho phép truyền dữ liệu với tốc độ cao từ vài chục đến hàng trăm Mb/s. Đáp ứng các yêu cầu truyền dữ liệu đa phương diện.

- IEEE 802.9: Đặc tả một mạng tích hợp dữ liệu và tiếng nói bao gồm 1 kênh dị bộ 10 Mb/s cùng với 96 kênh 64 Kb/s (tổng cộng 6Mb/s). Giải thông tổng cộng là 16 Mb/s. Chuẩn này còn được gọi là Isochronous Ethernet (IsoEnet) và nó được thiết kế cho các môi trường có lượng lưu thông lớn và cấp bách.

- IEEE 802.10: Chuẩn đặc tả về an toàn và mã hoá thông tin trong các mạng cục bộ.

- IEEE802.11: lchuẩn đặc tả mạng cục bộ không dây (Wireless LAN), hiện đang tiếp tục phát triển với phương pháp truy nhập CSMA/CD.

- IEEE 802.12 là chuẩn đặc tả mạng cục bộ bởi AT&T, IBM và HP, gọi là 100 VG - AnyLAN hay 100BASE-VG. Mạng sử dụng dạng hình sao xếp tầng (Cascaded Star Topology) và phương pháp truy nhập đường truyền có điều khiển tranh chấp. Khi có nhu cầu truyền dữ liệu, một trạm sẽ gửi yêu cầu đến HUB và trạm chỉ có thể truyền dữ liệu khi HUB cho phép. Chuẩn cung cấp một mạng tốc độ trên 100 Mb/s, có thể hoạt động trong các môi trường hỗn hợp Ethernet và Token Ring. Vì thế nó chấp nhận cả hai dạng Frame.

- IEEE 802.14: Chuẩn cuối cùng hiện nay là 802.14. Chuẩn này dùng cho truyền dữ liệu qua đường cáp TV, nhằm nâng cao tốc độ truy nhập Internet tại gia đình.

4.2.5. Ethernet 100 Mbps

Mạng Ethernet 100 Mbps được gồm 2 chuẩn :

* Fast Ethernet (IEEE 802.3u): 100Base-TX, 100Base-T4 và 100Base-FX.

Các loại cáp sử dụng

- 100BASE-T4 sử dụng bốn đôi dây cân bằng cáp UTP Cat-3 hoặc Cat-5.
- 100BASE-TX sử dụng hai đôi UTP Cat-5 hoặc đôi dây STP.
- 100BASE-FX sử dụng đôi dây cáp quang đa mode.

Mã hóa:

- 100Base-TX và 100Base-FX sử dụng kỹ thuật mã hóa 4B/5B.
- 100Base-T4 sử dụng kỹ thuật mã hóa 8B/6T.

Phương thức điều khiển truy nhập CSMA/CD

- 100Base-T4 sử dụng phương thức hoạt động bán song công.
- 100Base-TX sử dụng phương thức hoạt động song công.
- 100Base-FX sử dụng cả phương thức hoạt động song công và bán song công.

* 100VG-AnyLAN là công nghệ cạnh tranh với Fast Ethernet, ít được sử dụng.

4.2.6. Gigabit Ethernet.

Sự ra đời của Gigabit Ethernet đã mở ra một kỷ nguyên mới Ethernet tốc độ cao. Gigabit Ethernet được thiết lập dựa trên các nguyên lý cơ bản của 10BASE-T, Fast Ethernet và chuyển mạch Ethernet. Có 2 chuẩn Gigabit Ethernet:

* IEEE 802.3z: Mạng Gigabit Ethernet trên cáp quang chuẩn hóa năm 1998. Phương tiện truyền dẫn cơ bản là sợi quang đơn mode (SMF) với đường kính lõi là 10 µm, hay sợi quang đa mode với đường kính lõi là 50 µm hoặc 62.5 µm. Tín hiệu được truyền dẫn chủ yếu trên hai bước sóng là 850nm (bước sóng ngắn) và 1310 nm (bước sóng dài). Nếu sử dụng cáp đồng thì đó là loại cáp bốn đôi Cat-5 UTP, với khoảng cách có thể lên tới 100m.

Tại tầng vật lý: IEEE 802.3z :

1000Base-SX : chuẩn cho cáp quang bước sóng ngắn.

- Với cáp quang đa mode 62.5 µm, khoảng cách tối đa 220-275 m
- Với cáp quang đa mode 50 µm, khoảng cách tối đa 500-550 m

1000Base-LX : chuẩn cho cáp quang bước sóng dài

- Với cáp quang đa mode 62.5/50 µm, khoảng cách tối đa 550 m
- Với cáp quang đơn mode 9 µm, khoảng cách tối đa 5000 m

1000Base-CX : chuẩn cho cáp đồng tuyến ngắn.

- Với cáp đồng trục, khoảng cách tối đa là 25 m

Tại tầng liên kết dữ liệu:

- Hoạt động ở chế độ song công và chuyển mạch.
- Điều khiển truy nhập: CSSMA/CD trong phương thức song công.
- Trong phương thức bán song công sử dụng CSMA/CD cải tiến.

Gigabit Ehernet trên cáp đồng: Chuẩn IEEE 802.3ab đặc trưng bởi 1000Base-T. Sử dụng cả 4 đôi dây cáp UTP Cat 5 (hoặc Cat-6, Cat- 7) với khoảng cách tối đa 100m. Tín hiệu truyền dẫn song công trực tiếp 2 chiều trên cả 4 đôi với tốc độ 250 Mbps/ 1 đôi dây.

4.2.7. Gigabit Ethernet qua cáp sợi quang

10 Gigabit Ethernet (GbE) được trình bày trong dự thảo tiêu chuẩn IEEE 802.3ae. Tốc độ Ethernet đã tăng từ 1 Gbps lên 10 Gbps, cho phép Ethernet có thể tích hợp với những công nghệ tốc độ cao trên mạng đường trục WAN với tốc độ xấp xỉ 9,5 Gbps. Ngoài ra, 10 GbE có thể tương thích với các hệ thống SONET/SDH, có thể hỗ trợ cho tất cả các dịch vụ tại các tầng 2 và 3. Nguyên tắc cơ bản khi xây dựng các mạng chuyển mạch tốc độ cao là kết hợp nhiều đoạn mạng tốc độ thấp lại với nhau. Khi mật độ và số lượng các đoạn có tốc độ 100 Mbps trong mạng tăng lên thì 1000BASE-X và 1000BASE-T trở thành công nghệ truyền dẫn ở mức cao hơn được sử dụng trên các lõi mạng.

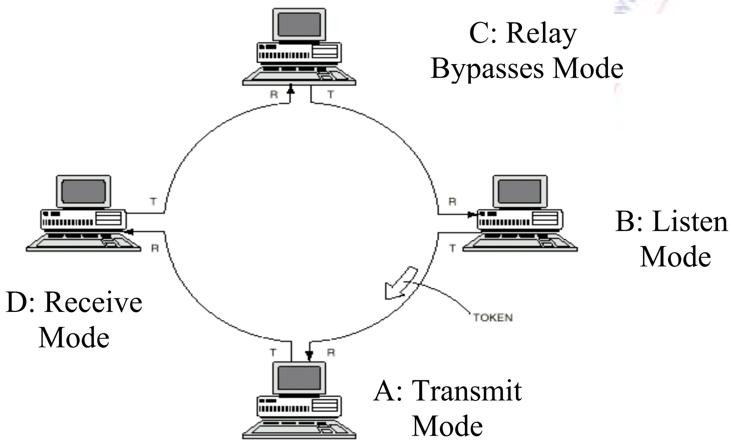
4.3. Mạng cục bộ Token Ring

Cấu trúc mạng hình vòng (Ring) là một chuỗi kết nối điểm - điểm các node lại với nhau tạo thành vòng tròn. Vì vậy Ring LAN không phải là mạng quảng bá như Ethernet, chúng được xem như mạng truyền tuần tự, điểm điểm. Công nghệ Ring LAN là số hoá, không giống như công nghệ mạng Ethernet trong đó cơ chế cảm nhận sóng mang là tín hiệu tương tự (Analog). Ring LAN thường sử dụng là IEEE 802.5

4.3.1. Hoạt động của Token Ring

Mỗi trạm hoạt động như là một bộ chuyển tiếp hỗ trợ cho sự khuyếch đại tín hiệu suy hao. Có thể sử dụng các loại cáp đồng trục, cáp sợi quang, cáp xoắn đôi. Sử dụng phương thức truy nhập đường truyền Token RING, gồm 24 bit. Nếu tốc độ trên vòng là 4 Mbps thì vòng phải có thời gian trì hoãn là 24/2 Mbps = 6 Micro giây.

Các trạm của mạng cục bộ Token Ring hoạt động theo 4 chế độ sau: Chế độ truyền, chế độ lắng nghe, chế độ bỏ qua. và chế độ nhận. Hình 4.6 minh hoạ 4 trạm hoạt động: Giả sử A truyền dữ liệu đến D. Trạm A nhận Token, kiểm tra bit T. Nếu giá trị bằng 0, Token bận, nghĩa là đã có trạm trên mạng đang trong chế độ truyền. Nếu giá trị bit T bằng 1, đường truyền rỗi, trạm chuyển giá trị 1 bằng 0 sang trạng thái bận và A bước vào chế độ truyền (Transmit Mode). Vì A truyền đến D, nên địa chỉ đích sẽ là D, địa chỉ nguồn là A. Vì địa chỉ đích không phải là của B, nó bước vào chế độ lắng nghe (Listen Mode). Trạm C vì không cung cấp điện (giả sử bị mất điện chẳng hạn), do đó nó ở chế độ bỏ qua (Delay bypassesMode). Trạm đích D phát hiện ra rằng địa chỉ đích chính là của nó, nó bước vào chế độ nhận (Receive Mode). Khung dữ liệu được sao chép vào bộ nhớ của trạm.



Hình 4.6 Các chế độ làm việc của các trạm Token Ring

Trong Frame có một số cờ kiểm soát quá trình truyền và nhận dữ liệu. Cờ Frame Status Flags nhận biết dựa vào phần cứng. Cờ Frame Status gồm các cờ nhận biết địa chỉ A (Address Recognized), cờ sao chép khung C (Frame Copied) và cờ lỗi E (Error).

4.3.2. Chuẩn Token Ring

Là chuẩn đặc tả mạng cục bộ với Topo dạng vòng (Ring) sử dụng thẻ bài để điều khiển truy nhập đường truyền tuân thủ chuẩn IEEE 802.5. Chuẩn IEEE 802.5 hoạt động trong tầng vật lý và tầng con MAC .

Giao thức MAC là phần cốt lõi của IEEE 802.5, sử dụng phương pháp Token Ring để điều khiển truy nhập đường truyền. Khuôn dạng của Frame dùng trong giao thức MAC của IEEE 802.5 được trình bày trong hình 4.8

SD	AC	FC	DA	SA	INFO	FCS	ED	ES
SFS		Phạm vi phủ của FCS					EFS	

Hình 4.7 Khuôn dạng tổng quát của IEEE 802.5 Frame

- SFS = Start Frame Sequence .

- SD = Starting Delimiter (1 byte): SD chỉ bắt đầu của một Frame hoặc Token.

- AC = Access Control (1 byte): Điều khiển truy nhập.

- FC=Frame Conrtol (1byte): Điều khiển Frame chứa LLC data hay là một MAC Control Frame.

- DA = Destination Address (2/6 byte): Địa chỉ đích của Frame.

- SA = Source Address (2/6 byte): Địa chỉ nguồn của Frame.

- INFO = Information (0 hoặc nhiều bytes).

- FCS = Frame Check Sequence (4 bytes): FCS: mã kiểm soát lỗi CRC 32 bit cho các vùng FC, DA, SA, và INFO.

- EFS = End - of - Frame Sequence

- ED = Ending Delimiter (1 byte): Các ký hiệu kết thúc Frame.

- FS = Frame Status (1 byte): Tình trạng Frame.

4.4. Giao diện số liệu phân bố sử dụng quang FDDI (Fiber Distributed Data Interface)

4.4.1. Giới thiệu FDDI

FDDI là một tập các giao thức ANSI truyền dữ liệu qua cáp quang. Các mạng FDDI sử dụng phương thức truy nhập Token Passing, tốc độ có thể đạt đến 100 Mbps. FDDI được sử dụng làm Backbone cho các mạng diện rộng MAN,WAN. Cấu hình Ring cáp quang, có thể kết nối trực tiếp các trạm đầu cuối và các máy chủ trong một nhóm làm việc hay liên kết các mạng trong phạm vi một tòa nhà, trong một khu vực hay trong một thành phố. Một trong các ứng dụng là để kết nối các máy chủ tốc độ cao. Khi đóng vai trò là một mạng xương sống (Backbone), FDDI liên kết các thiết bị mạng khác nhau như Router, Switch, Brigde, các bộ tập trung... để tạo thành một mạng lớn hơn từ các mạng con. Tuy nhiên FDDI không được dùng cho các mạng diện rộng (WAN) có bán kính lớn hơn 100 km.

Mặc dù bị thay thế bởi các công nghệ LAN khác, FDDI vẫn có những ưu điểm nhất định.

FDDI có thể được cấu hình như là hai mạng Ring ngược nhau độc lập. Điều này làm tăng tính ổn định hệ thống cao hơn. Nếu cấu hình (Topo) của mạng được thiết kế hai đường quang của cả hai mạng khác nhau về mặt vật lý thì sẽ đảm bảo cho hai mạng không bị phá hủy trong cùng một thời gian khi xảy ra các sự cố liên quan đến hệ thống cáp.

FDDI có đặc tính tự hồi phục bằng kỹ thuật Autowraping. Lỗi phát sinh ở Ring sơ cấp (Ring đang hoạt động) sẽ được khắc phục bằng cách nối vòng với Ring thứ cấp (Ring dự phòng), tạo thành một Ring đơn và cho phép mạng FDDI hoạt động ở tốc độ cao nhất. Phần cứng mạng có khả năng phát hiện ra sự cố của cáp giữa các điểm kết nối, do có hai đường cáp nên trạm phát hiện ra lỗi sẽ tự động nối vòng hai Ring với nhau thành một Ring đơn. Khung tin của FDDI có độ dài tới 4500 Byte, điều này làm tăng hiệu xuất mạng, giảm các thông tin Header giao thức.FDDI mã hóa dữ liệu khác biệt với các công nghệ khác để tăng hiệu quả truyền dẫn.

FDDI-2 là công nghệ mở rộng của FDDI, hỗ trợ truyền dẫn các tín hiệu tiếng nói, hình ảnh và dữ liệu. Một biến thể khác của FDDI là FFDT (FDDI Full Duplex Technology) sử dụng hạ tầng mạng như FDDI nhưng có thể tốc độ truyền số liệu lên đến 200 Mbps.

FDDI sử dụng cấu trúc vòng kép với lưu lượng truyền trên mỗi vòng Ring theo hướng ngược nhau. Vòng Ring kép bao gồm một Ring thứ cấp và một Ring sơ cấp. Trong quá trình hoạt động, Ring thứ cấp sử dụng để truyền số liệu còn Ring sơ cấp ở trạng thái rỗi. Mục đích của việc sử dụng vòng Ring kép là để đảm bảo tính bền vững và ổn định hơn.

4.4.2. So sánh những giữa FDDI và IEEE 802.5

FDDI	IEEE 802.5
- Dùng cáp quang .	- Dùng cáp đôi xoắn
- Tốc độ 100Mb/s	- Tốc độ 1,4 và 16 Mb/s
- Phương pháp mã hoá NRZI -4B/ 5B	- Phương pháp mã hoá Manchester vì sai
- Đặc tả độ tin cậy tường minh	- Đặctả độ tin cậy không tường minh
- Đồng bộ phân tán	- Đồng bộ tập trung
- Quay vòng thẻ bài theo thời gian.	- Sử dụng các bit priority và reservation
- Sinh thẻ bài mới sau khi truyền	- Sinh thẻ bài mới sau khi nhận
- Chiếm thẻ bài bằng cách thu lại	- Chiếm thẻ bài bằng cách đổi bit trạng thái
- Khuôn dạng Frame FDDI	- Khuôn dạng Frame IEEE 802.5
- Kích thước Frame tối đa 4500 Bytes	- Không qui định kích thước Frame tối đa
- Các địa chỉ 16 và / hoặc48 bits	- Các địa chỉ 16 hoặc 48 bits
- Chức năng phục hồi phân tán cho các trạm	- Trạm điều khiển (Active Monitor) đảm nhiệm chức năng phục hồi.

Bảng 4.8 Những điểm khác nhau giữa FDDI và IEEE 802.5

4.4.3. Các kiểu kết nối đầu cuối FDDI

Một trong những đặc điểm đặc trưng của FDDI là việc hỗ trợ nhiều cách kết nối khác nhau giữa các thiết bị trên mạng FDDI. FDDI đưa ra bốn kiểu kết nối

- Trạm kết nối đơn SAS (Single Attachment Station) - được kết nối vào duy nhất một Ring qua một bộ tập trung.

- Trạm kết nối kép DAS (Dual Attachment Station). Mỗi DAS có hai port và được kết nối vào cả hai Ring.

- Bộ tập trung kết nối đơn SAC (Single Attachment Concentrator)

- Bộ tập trung kết nối kép DAC (Dual Attachment Concentrator

4.4.4. Khả năng chịu lỗi của FDDI

FDDI là một công nghệ mạng có đặc tính chịu lỗi cao vì mạng có cấu trúc Ring kép, sử dụng các chuyển mạch vòng quang, hỗ trợ kỹ thuật Dual Homing.

Ring kép: Ring kép có khả năng chịu lỗi cao. Nếu một trạm trên Ring bị lỗi hoặc một đường cáp bị đứt thì các thiết bị ở phần còn lại sẽ tự động khép lại thành một Ring đơn. Các hoạt động của mạng vẫn tiếp tục được duy trì trên các trạm còn lại của Ring.Tuy nhiên FDDI nếu hai hay nhiều lỗi xảy ra, Ring FDDI sẽ bị phân mảnh thành hai hoặc nhiều Ring con độc lập và các thiết bị trên mỗi Ring vẫn có khả năng trao đổi thông tin với nhau.

Chuyển mạch vòng quang (Optical Bypass Switch): Chuyển mạch vòng quang đảm bảo sự hoạt động của Ring kép một cách liên tục nếu một thiết bị nào đó trên Ring bị lỗi. Nó được sử dụng để ngăn chặn việc phân mảnh Ring cũng như loại bỏ các trạm có lỗi ra khỏi Ring. Chuyển mạch vòng quang bằng cách sử dụng các gương quang học để truyền trực tiếp các tia sáng từ Ring tới các thiết bị truy nhập kép DAS. Nếu một lỗi nào đó xảy ra trên thiết bị DAS, thì chuyển mạch quang này sẽ chuyển tia sáng qua chính nó bằng các gương nội tại, vì vậy vẫn duy trì được hoạt động của Ring . Lợi ích mang lại từ khả năng này là Ring sẽ không phải chuyển sang trạng thái Ring đơn khi thiết bị có lỗi. Hình 8 mô tả chức năng của một chuyển mạch vòng quang trong một mạng FDDI.

Các thiết bị quan trọng (Router,Mainframe) có thể sử dụng công nghệ Dual-homing để các kết nối dự phòng, nhằm đảm bảo cho thiết bị hoạt động một cách liên tục. Theo mô hình Dual-homing, các thiết bị quan trọng được gắn vào Ring qua hai bộ tập trung.

FDDI là một công nghệ mạng LAN/MAN sử dụng cáp quang, tốc độ 100 Mbps được thiết kế theo dạng Ring, được thiết kế để đáp ứng nhu cầu của người sử dụng mạng cần tốc độ truyền dẫn lớn hơn so với các mạng Ethernet/802.3 và token Ring hiện thời. Công nghệ này được thực hiện trước khi có sự phát triển của Fast Ethernet và Gigabit Ethernet.

Hiện nay, mạng FDDI không được dùng phổ biến vì chi phí thực hiện lớn, phức tạp (thiết bị quang đắt…) và bị cạnh tranh bởi các mạng Ethernet/802.3 có giá thành rẻ, dễ thực hiện, . Tuy nhiên, vẫn còn có những nghiên cứu với mục đích cải tiến để tận dụng khả năng cung cấp băng thông rất lớn cũng khả năng chống lỗi của nó.

4.5. Mạng LAN ATM

Mạng LAN được xây dựng dựa trên kỹ thuật ATM gọi là Local LAN (LATM). Bộ điều khiển mạng đặt trong tổng đài ATM, tổng đài định lộ trình các thông báo và kiểm soát truy nhập trong trường hợp nghẽn mạch. Ngược với kỹ thuật LAN truyền thống, việc điều khiển được cài đặt trong các bộ giao tiếp mạng.

4.5.1. Đặc trưng của ATM LAN

- Hỗ trợ nhiều lớp dịch vụ tin cậy, ví dụ dịch vụ video trực tuyến có thể yêu cầu một cầu nối tin cậy có tốc độ 2Mbps để chất lượng dịch vụ có thể chấp nhận được.

- Thông lượng rộng, có khả năng mở rộng dung lượng trên từng Host (để cho phép các ứng dụng cần lượng dữ liệu xuất nhập lớn trên một host) và cả trên dung lượng phối hợp (để cho phép cài đặt và mở rộng từ vài host đến vài trăm host tốc độ cao).

- Là phương tiện liên kết mạng giữa kỹ thuật LAN và WAN.

- ATM có thể đáp ứng các yêu cầu nhờ các đường dẫn ảo và các kênh ảo, rất dễ tích hợp các lớp đa dịch vụ. Theo kiểu kết nối cố định hay chuyển mạch, ATM rất dễ mở rộng bằng cách thêm nhiều node chuyển mạch tốc độ cao (hay thấp) cho các thiết bị nối vào.

- Các gói tin là tế bào có độ dài cố định, vì vậy việc dùng ATM trong một mạng đầu cuối cho phép xoá dần ranh giới giữa LAN và WAN.

4.5.2. Các loại ATM LAN

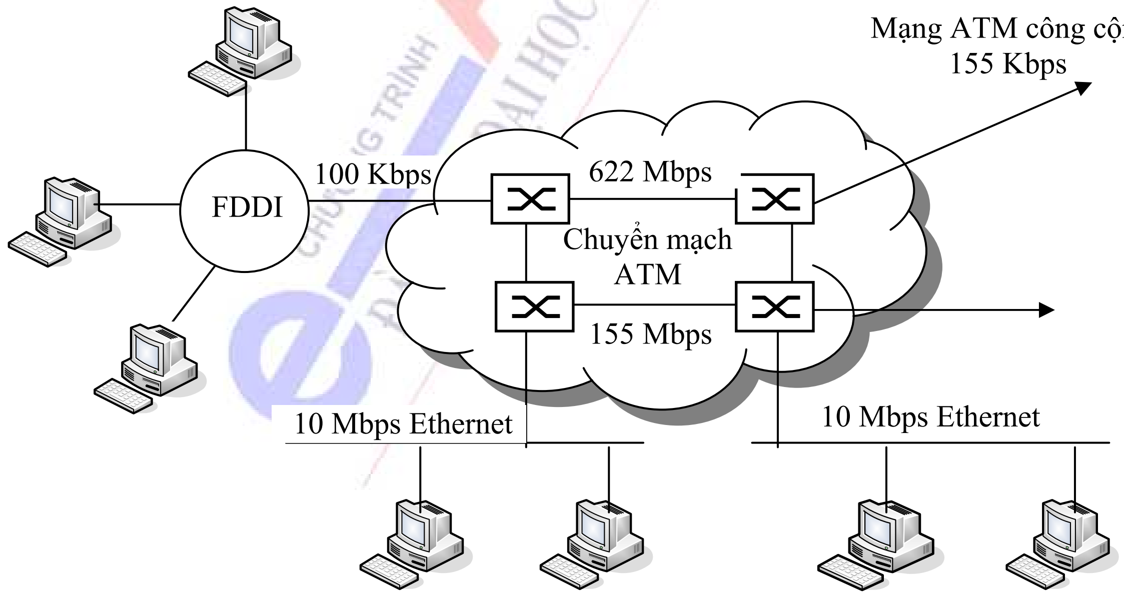
- Getway to ATM LAN: Là một chuyển mạch ATM đóng vai trò nh một Router và bộ tập trung tải để liên kết một mạng đầu cuối phức tạp vào ATM WAN.

- Backbone ATM Switch: Là chuyển mạch ATM hay một chuyển mạch ATM cục bộ liên kết các LAN khác nhau.

- Workgroup ATM: Là các máy trạm đa phương tiện chất lượng cao và các hệ thống đầu cuối được kết nối trực tiếp vào một chuyển mạch ATM .

Trên đây là 3 cấu hình thuần nhất. Trong thực tế một hỗn hợp của 2 hoặc 3 loại cũng có thể được sử dụng để tạo ra một mạng ATM LAN theo yêu cầu của doanh nghiệp.

Hình 4.9 minh hoạ một ví dụ mạng LAN ATM sử dụng bộ định tuyến chuyển mạch ATM và các giao tiếp ATM tại các trạm làm việc.



Hình 4.9 Mạng LAN ATM

4.5.3. Kỹ thuật chuyển mạch ATM LAN

Phải có khả năng chuyển đổi tốc độ từ bộ chuyển mạch ATM đến mạng LAN phải phù hợp với tốc độ dữ liệu của LAN. Đồng thời ATM có nhiệm vụ chuyển đổi giao thức từ MAC (điều khiển truy nhập đa phương tiện) sử dụng cho LAN thành dòng các tế bào ATM dùng trong mạng ATM. Vì vậy cần phải sử dụng thêm cầu nối (Bridge) và định tuyến.

Với chuyển mạch ATM Backbone, có thể thêm các bộ chuyển mạch ATM, nghĩa là tăng thêm dung lượng của trục sương sống, tốc độ dữ liệu của các trung kế giữa các chuyển mạch và LAN lúc này cũng tăng. Tuy nhiên số lượng chuyển mạch thêm vào có hạn và trục chính ATM đơn giản không thể đáp ứng mọi nhu cầu của LAN. Hệ thống đầu cuối bị hạn chế tốc độ dữ liệu, vì vậy cần sử dụng công nghệ ATM với HUB. Một HUB thường có nhiều cổng nối với nhiều thiết bị đầu cuối và các cổng hoạt động với tốc độ dữ liệu và giao thức khác nhau, gọi là ATM - LAN thuần tuý.

Quy ước sử dụng một tập các giao thức tầng vật lý trong các mạng LAN truyền thống khác với quy ước tập các giao thức trong tầng vật lý mạng WAN. Vì vậy khi liên kết các mạng LAN lại thành một mạng diện rộng cần thiết phải sử dụng các thiết bị như Gateway, Router.. để chuyển đổi các giao thức LAN, tốc độ dữ liệu và các tín hiệu giao thức sử dụng cho WAN. Hình 4.54 minh hoạ một mạng LAN/WAN được xây dựng đựa trên các bộ định tuyến ATM, như các mạng LAN/WAN truyền thống.

Trong kỹ thuật ATM, giao thức ATM có thể dùng cho cả mạng LAN và WAN. Điều này cho phép xây dựng một mạng LAN hoặc mạng WAN chỉ cần sử dụng các tổng đài ATM. Để kết nối một mạng Local ATM vào mạng WAN, chỉ cần sử dụng một cổng duy nhất trong tổng đài ATM để kết nối đến mạng của tổng đài TM.

Câu hỏi trắc nghiệm

1. Phát biểu nào đúng:
   A. Dùng thẻ bài luân chuyển trên vòng logiic
   B. Trước khi truyền xác định đường truyền "bận" hay "rỗi", nếu "bận" thì thực hiện 1 trong 3 giải thuật Non persistent, Persistent và P-persistent.
   C. Trong khi truyền phát hiện thấy xung đột, nó ngừng ngay truyền nhưng và thông báo cho các node khác biết. Sau đó chờ đợi với thời đoạn ngẫu nhiên, thực hiện giải thuật của CSMA.
2. Chức năng của Token Bus
   A. Bổ sung định kỳ các trạm nằm ngoài vòng logic nếu có nhu cầu truyền dữ liệu.
   B. Loại bỏ một trạm không còn nhu cầu truyền dữ liệu ra khỏi vòng logic.
   C. Quản lý lỗi.
   D. Khởi tạo vòng logic
   E. Khôi phục dữ liệu bị mất do gẫy vòng logic
3. Trong phương pháp Token ring cần giải quyết vấn đề phá vỡ hệ thống:
   A. Một là mất thẻ bài.
   B. Thẻ bài "bận" lưu chuyển không dừng trên vòng.

C. Khởi tạo vòng logic

D. Khôi phục dữ liệu bị mất do gẫy vòng logic

4. Phương pháp nào có cơ chế xác nhận ACK

A. CSMA/CD

B. TOKEN BUS

C. TOKEN RING

D. Cả 3 phương pháp.

5. Phương pháp nào có độ phức tạp hơn các phương pháp còn lại

A. CSMA/CD

B. TOKEN BUS

C. TOKEN RING

D. Cả 3 phương pháp.

6. Phương pháp nào xử lý hiệu quả hơn trong trường hợp tải nhẹ

A. CSMA/CD

B. TOKEN BUS

C. TOKEN RING

D. Cả 3 phương pháp.

7. Những đặc điểm kỹ thuật cơ bản của Ethernet

A. Cấu hình Bus / Star hoặc lai ghép Bus -Star

B. Quy cách kỹ thuật: IEEE 802.3.Phương pháp truy nhập: CSMA/CD.

C. Vận tốc truyền 10Mbps, 100Mbps ... 10Gbps

D. Loại cáp: Cáp đồng trục mảnh, cáp đồng trục dày, cáp xoắn đôi, cáp quang ...

E. Tất cả đều sai.

Câu hỏi và bài tập

1. Phương thức đa truy nhập sử dụng sóng mang có phát hiện xung đột CSMA/CD
2. Ưu, nhược điểm của từng giải thuật trong CSMA/CD
3. Token Bus: Thiết lập vòng logi, duy trì trạng thái thực tế của mạng và khởi tạo vòng logic khi cài đặt mạng hoặc đứt vòng.
4. Token ring, nguyên tắc của phương pháp. Cần giải quyết hai vấn đề có thể dẫn đến phá vỡ hệ thống.
5. So sánh CSMA/CD với các phương pháp dùng thẻ bài
6. Token ring thế hệ thứ hai: Switched Token Ring, Token ring chuyên dụng (Dedicated Token ring), Full-duplex Token ring (Token ring song công (hai chiều), 100 Mbps Token ring (HSTR- high speed token ring).
7. Ethernet và chuẩn IEEE 802

8. Giới thiệu chung về Ethernet. Thành phần mạng Ethernet, những đặc điểm cơ bản của mạng Ethernet
9. Vai trò, chức năng các tầng trong IEEE 802
10. LLC Header:
11. Các dịch vụ tầng con LLC
12. Tầng Ethernet Mac sublayer:
13. Định dạng khung Ethernet:
14. Họ IEEE 802
15. Chuẩn IEEE 802.5:
16. IEEE 802.6 và các mạng IEEE 802.6
17. IEEE 802.9:
18. IEEE 802.10
19. IEEE802.11:
20. IEEE 802.12
21. IEEE 802.14:
22. Ethernet 100 Mbps.
23. Gigabit Ethernet.
24. Mạng cục bộ Token Ring
25. Chuẩn Token Ring
26. Giao diện số liệu phân bố sử dụng quang FDDI
27. Sự tương quan gữa FDDI và mô hình OSI
28. So sánh FDDI và IEEE 802.5
29. Các kiểu kết nối đầu cuối FDDI
30. Khả năng chịu lỗi của FDDI
31. Khuôn dạng tổng quát của FDDI Frame
32. Mạng LAN ATM, Đặc trưng và các loại ATM LAN
33. Kỹ thuật chuyển mạch ATM LAN
34. Kiến trúc giao thức ATM LAN
35. Tầng nào thay đổi, duy trì tuyến kết nối giữa các thiết bị truyền thông.

CHƯƠNG 5: KỸ THUẬT MẠNG DIỆN RỘNG WAN

Nội dung của chương này sẽ trình bày tổng quát về mạng diện rộng WAN và các loại mạng diện rộng: mạng tích hợp đa dịch vụ số ISDN, B_ISDN, mạng chuyển mạch gói X25, chuyển mạch khung Frame Relay và các ưu nhược điểm của nó và phương thức truyền dẫn không đồng bộ ATM.

- Liên kết liên mạng.
- Mạng tích hợp đa dịch vụ số ISDN
- Băng rộng B_ISDN
- Mạng chuyển mạch gói và chuyển mạch khung Frame Relay.
- Dịch vụ chuyển mạch dữ liệu megabit
- Phương thức truyền dẫn không đồng bộ ATM

5.1. Khái niệm về liên mạng (Internetworking)

Liên mạng (internetworking) là một tập các mạng riêng lẻ được nối với nhau bởi các thiết bị mạng trung gian, có chức năng như là một mạng đơn. Các mạng thành phần tạo nên liên mạng được gọi là mạng con (Subnetworks), Các thiết bị được nối đến các mạng con được gọi là hệ thống đầu cuối (End nodes) và những thiết bị nối các mạng con lại với nhau được gọi là các thiết bị liên kết liên mạng (Intermediate nodes*)*

Thuật ngữ "internetworking" thường được sử dụng dưới dạng rút gọn là "internet". Một cách chung nhất, internet là một tập hợp các mạng được nối với nhau. Khi sủ dụng "I" hoa ở trước, thì thuật ngữ "Internet" là đề cập đến mạng internetwork toàn cầu, bao gồm hàng triệu mạng trên thế giới liên kết với nhau và hoạt động theo chuẩn TCP/IP.

Liên mạng có thể được liên kết bởi LAN to LAN, LAN to WAN và WAN to WAN. Có ba phương pháp liên kết liên mạng phổ biến tương ứng với 3 tầng cuối của mô hình OSI. Phương pháp liên kết tại tầng vật lý, cùng cấu trúc và phương thức trao đổi thông tin. Bộ lặp Repeater hoạt động tại tầng vật lý, là thiết bị được sử dụng để mở rộng chiều dài của một mạng LAN. Phương pháp liên kết tại tầng liên kết dữ liệu (Datalink), có cấu trúc khác nhau và phương thức trao đổi thông tin khác nhau. Cầu (Bridge) và các bộ chuyển mạch (Switched) tầng 2 hoạt động tại tầng liên kết dữ liệu. Những thiết bị này hỗ trợ cho các giao thức tầng vật lý khác nhau và có thể liên kết giữa các mạng LAN có cấu trúc khác nhau. Phương pháp liên kết sử dụng tầng mạng (Network Layer) hay tầng Internet (Inernet Layer) cho các mạng khác nhau về phần cứng, khác nhau về phần mềm, khác nhau về giao thức và thường cung cấp những chức năng và ứng dụng khác nhau. Thiết bị liên kết liên mạng trợ giúp cho các giao thức mạng như IP, IPX, Apple Talk. Việc nối kết được thực hiện bởi việc định dạng gói tin từ một mạng đến một mạng khác bởi thông tin điều khiển tầng mạng như địa chỉ nguồn, địa chỉ đích. Thực hiện chuyển đổi giao thức mạng (Network Protocol Translation). Một thiết bị cung cấp các liên kết tại tầng mạng được gọi là một bộ định tuyến (Router). Chức năng chủ yếu của một Router là liên kết các mạng khác nhau về vật lý và chuyển đổi các gói tin từ một mạng này sang một mạng khác, quyết định đường đi của các gói tin đến node đích.

5.2. Mạng tích hợp đa dịch vụ số ISDN (Integrated Service Digital Network)

5.2.1. ISDN là gì

Khái niệm về mạng tích hợp đa dịch vụ số được CCITT định nghĩa là: "Một mạng viễn thông, dựa trên kỹ thuật chuyển kênh và chuyển mạch gói, cung cấp các đường truyền số, có khả năng phục vụ nhiều loại dịch vụ khác nhau, bao gồm dịch vụ thoại và phi thoại. Các thuê bao liên kết mạng phải tuân theo các chuẩn …"

Mạng ISDN có những đặc điểm sau:

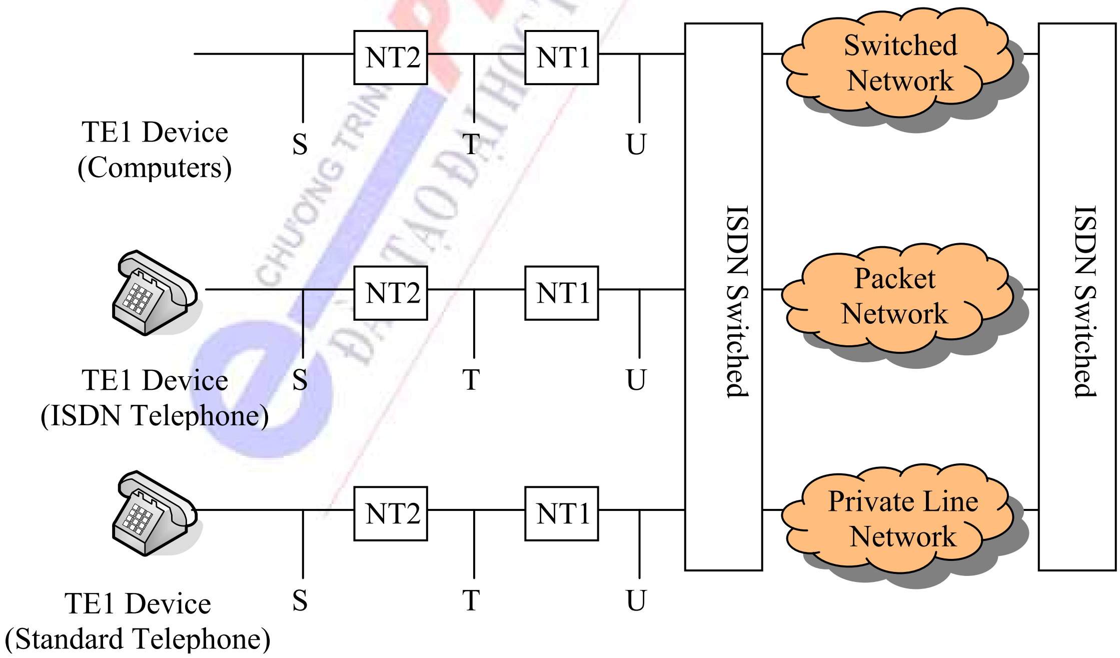
- Là một mạng đa dịch vụ, thay thế nhiều mạng viễn thông khác nhau đang cùng tồn tại bằng một mạng duy nhất có khả năng cung cấp tất cả các dịch vị hiện tại và các dịch vụ tương lai với một giao tiếp thuê bao duy nhất.

- ISDN có hệ thống báo hiệu số 7 và các node chuyển mạch thông minh.

- Kiến trúc ISDN tương thích với mô hình OSI. Các giao thức đã được phát triển có liên quan tới các ứng dụng của mô hình OSI có thể sử dụng được trong ISDN. Các giao thức có thể phát triển sử dụng một cách độc lập cho các tầng khác nhau, cho các chức năng riêng của từng tầng mà không ảnh hưởng đến các tầng kề nhau.

Mục tiêu chính của mạng là chuẩn hoá tất cả các thiết bị đầu cuối, cho phép các phương tiện như âm thanhi, hình ảnh, văn bản...được tích hợp chung vào một mạng duy nhất. Nhằm sử dụng có hiệu quả các tài nguyên của mạng.

Nguyên lý chung của ISDN là liên kết các thiết bị đầu cuối khác nhau lên cùng một đường dây thuê bao và có thể đồng thời truyền thông số giữa thuê bao và mạng. Cước phí được tính theo dung lượng thông tin truyền đi, không tính riêng cho mỗi loại dịch vụ sử dụng. Các dịch vụ khác nhau được hỗ trợ bởi hệ thống báo hiệu số 7 giữa mạng và báo hiệu DSS1 thuê bao.



5.2.2. Các phần tử cơ bản của mạng ISDN

- TE1 (Termination Equipment 1) là các thiết bị đầu cuối có các thuộc tính ISDN như: điện thoại số ISDN, các đầu cuối thoại, số liệu, digital fax,…

- TE2 (Termination Equipment 2) là các thiết bị đầu cuối không có tính năng ISDN, để có thể liên kết với ISDN phải có thêm các bộ phối ghép đầu cuối TA (Terminal Adapter).

- NT1 (Network Termination 1):Thực hiện các chức năng thuộc tầng vật lý của mô hình OSI, tức là các tính năng về điện, về giao tiếp giữa ISDN và người sử dụng, các chức năng kiểm soát chất lượng đường truyền, đấu vòng,…

- NT2 (Network Termination 2) là một thiết bị thông minh có khả năng đáp ứng các chức năng đến tầng mạng của mô hình OSI. NT2 có thể là tổng đài riêng PBAX, bộ điều khiển đầu cuối hoặc là mạng cục bộ LAN.

R, S, T, U : Các điểm chuẩn phân cách (R: rate, S: system, T: terminal, U: user)

5.2.3. Các loại kênh trong mạng ISDN

"Kênh" là đường truyền thông tin giữa người sử dụng và mạng, được gọi là kênh thuê bao. Trong ISDN kênh thuê bao chỉ truyền các tín hiệu số và được chia thành 3 loại kênh cơ bản: kênh D, kênh B và kênh H, được phân biệt với nhau về chức năng và tốc độ:

* Kênh D: Dùng để truyền báo hiệu giữa người sử dụng và mạng. Vì có thể không sử dụng hết băng tần của kênh, nên có thể dùng kênh D để truyền dữ liệu người sử dụng. Kênh D hoạt động với tốc độ 16 Kbps hoặc 64 Kbps, phụ thuộc vào giao diện người sử dụng.

* Kênh B: Dùng để truyền tín hiệu tiếng nói, âm thanh (Audio), số liệu và hình ảnh (Video) của người sử dụng. Kênh B luôn hoạt động ở tốc độ 64 Kbps. Ba loại liên kết có thể thiết lập qua kênh B :

  - Chuyển mạch kênh (Circuit-switched): Quá trình thiết lập liên kết không thực hiện trên kênh B mà sử dụng hệ thống báo hiệu kênh chung.

  - Chuyển mạch gói (Packet-switched): Thuê bao được nối tới một node chuyển mạch gói và số liệu sẽ được chuyển đổi nhờ chuẩn X25.

  - Liên kết bán cố định (Semipermanent): loại liên kết này không đòi hỏi thủ tục thiết lập liên kết, tương tự như thuê bao kênh riêng (Leased line).

* *Kênh H* cung cấp các dịch vụ tốc độ cao và ghép các luồng thông tin ở tốc độ thấp hơn. có 4 loại kênh H :

  - Kênh H0 : tương đương với 6 kênh B, có tốc độ 384 Kbps.
  - Kênh H10 : tương đương với 23 kênh B, có tốc độ 1.472 Mbps.
  - Kênh H11 : tương đương với 24 kênh B, có tốc độ 1.536 Mbps.
  - Kênh H12 : tương đương với 30 kênh B, có tốc độ 1.920 Mbps.

5.2.4. Giao diện ISDN

- Giao diện BRI (Basic Rate Interface): Có cấu trúc kênh là 2B+D, trong đó kênh D hoạt động với tốc độ 16 Kbps. Tổng cộng tốc độ của giao diện này là 144 Kbps nhưng trong thực tế cấu trúc của giao diện tốc độ cơ sở có thể lên tới 192 Kbps. Giao diện này dành cho các thuê bao nhỏ để cung cấp các dịch vụ truy nhập mạng bằng các thiết bị đầu cuối đa năng hoặc các thiết bị riêng lẻ.

- Giao diện PRI (Primary Rate Interface): Dùng cho thuê bao có dung lượng lớn như tổng đài PBAX hoặc các mạng cục bộ LAN. Do các tiêu chuẩn truyền dẫn khác nhau nên có 2 loại truy nhập là: 23B+D cho tiêu chuẩn Bắc Mỹ 1544 Kbps và 30B+D cho tiêu chuẩn Châu Âu 2048 Kbps (ở giao diện này kênh D luôn có tốc độ là 64 Kbps).

5.2.5. Chức năng các tầng trong kiến trúc ISDN

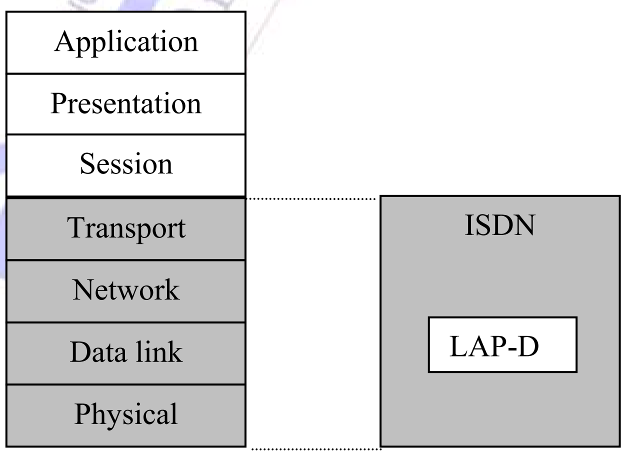
Mạng ISDN là sự tích hợp kỹ thuật chuyển mạch kênh và chuyển mạch gói, trên cơ sở số hoá toàn bộ mạng lưới. Vì vậy nó có ưu thế về dịch vụ mà chưa một mạng nào có được.

*** Tầng vật lý trong ISDN:** Cấu trúc trong tầng này phụ thuộc vào hướng liên kết từ thiết bị đầu cuối đền mạng hay từ mạng đến thiết bị đầu cuối. Giao diện của tầng gồm:

- NT Frame (Network to Terminal)
- TE Frame (Terminal to Network)

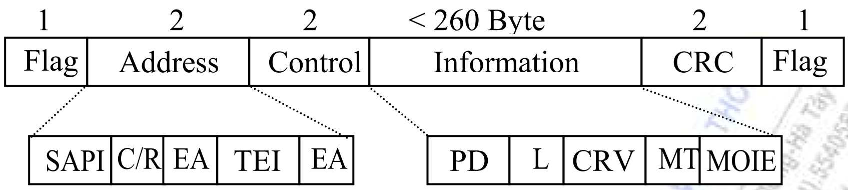
*** Tầng 2 trong ISDN:** Tương ứng với tầng liên kết dữ liệu (Data Link Layer) của mô hình OSI. Hoạt động trong tầng này có giao thức LAP-D (Link Access Protocol - D channel). LAP-D được dẫn xuất từ giao thức HDLC (High Level Data Link Control). LAP-D thực hiện các chức năng sau đây :

- Cung cấp dịch vụ thiết lập một hay nhiều liên kết Data Link trên cùng kênh D cho các hoạt động của các thực thể tầng 3
- Tạo khung (Frame).
- Kiểm soát đồng bộ.
- Phát hiện lỗi và tự động phát lại khung có lỗi.
- Ghi nhận các sai sót về thủ tục.
- Kiểm soát luồng.
- Các chức năng giám sát tầng 2.



Hình 5.2: Kiến trúc ISDN và mô hình OSI

Cấu trúc khung của LAP-D như sau.



Hình 5.3: Cấu trúc khung và các trường của LAP-D

Flag : biểu thị sự bắt đầu hay kết thúc của khung.

Address : Địa chỉ ISDN.

- SAPI (Service Access Point Identifier):Điểm truy nhập dịch vụ cho tầng 3 (6 bit).
- C/R (Command/ Response): Khung này là một lệnh hay một đáp ứng (1 bit).
- EA (Extended Address - Higher/Lower Order) bắt đầu hay kết thúc của trường địa chỉ (bằng 1 là byte cuối của địa chỉ) (2 bit).
- TEI (Terminal Endpoint Identifier) :địa chỉ đặc biệt hoặc ấn định ID cho mỗi thiết bị đầu cuối ISDN liên kết với mạng ISDN thông qua giao diện S/T (7 bit).

Control : Trường điều khiển.

Information : Trường dữ liệu

- PD (Protocol Discriminator) (1 byte).
- L (Length) cho biết chiều dài của trường CRV (1 byte).
- CRV (Call Reference Value) thiết lập số hiệu cho mỗi cuộc gọi (1 hoặc 2 byte).
- MT (Message Type) Loại Message (1byte).
- MOIE (Mandatory/ Optional Information Elements)

CRC : Trường kiểm tra.

*** Tầng 3 trong ISDN:** Chức năng của tầng này là thiết lập, duy trì và giải phóng các liên kết. Các thực thể tầng 3 sẽ cung cấp các thông điệp (Message) để truyền trong các trường tầng 2. Các thông điệp thường có độ dài 8 bit và có nhiều loại thông điệp sử dụng trong các trường hợp khác nhau. Ví dụ như thông điệp SETUP (00000101) thiết lập cuộc gọi.

Mạng tích hợp đa dịch vụ số ISDN nếu được triển khai sẽ thực sự là một cuộc cách mạng trong công nghệ thông tin. Từ một mạng duy nhất nó có thể cung cấp các dịch vụ khác nhau mà hiện nay đang được cung cấp bởi các mạng viễn thông khác nhau. Việc triển khai ISDN không chỉ dừng lại ở việc nâng cấp các hệ thống viễn thông hiện có để có khả năng truyền tải được những dòng dữ liệu lớn với tốc độ nhanh mà còn phải tiến hành đồng bộ về phía người dùng và về phía các nhà cung cấp dịch vụ.

5.3. Mạng băng rộng B_ISDN (Broadband ISDN)

5.3.1. Tổng quan về sự ra đời của B-isdn

Giữa thập kỷ 80, CCITT đã triển khai nghiên cứu mô hình mạng viễn thông mới gọi là ISDN băng rộng (Broadband- ISDN). B-ISDN là mạng thông tin số đa dịch vụ, trợ giúp tất cả các ứng dụng đa dịch vụ trên cùng một hệ thống mạng. Nghĩa là mạng phải có khả năng cung cấp các dịch vụ truyền thông với tốc độ thay đổi từ một vài Kbps đến hàng trăm Gbps cho các loại kênh Analog và kênh Digital bao gồm những dịch vụ đang có và những dịch vụ sẽ có trong tương lai. Công nghệ truyền dẫn không đồng bộ ATM dựa trên nguyên lý truyền dẫn và chuyển mạch gói được CCITT chọn làm giải pháp cho B-ISDN. Đầu những năm 90 các khuyến nghị cho B-ISDN dựa trên công nghệ ATM đã được ban hành.

Giao tiếp B-ISDN ban đầu cung cấp tốc độ truyền 51 Mbps, 155 Mbps hoặc 622 Mbps trên đường cáp quang. Tầng vật lý hỗ trợ B-ISDN được cung cấp bởi SONET (Synchronous Optical Network) và ATM (Asynchronous Transfer Mode). Tầng Client có thể hỗ trợ Frame Relay, SMDS hoặc IEEE 802.2

B-ISDN có thể được xem như một mạng thông tin được phát triển từ mạng ISDN băng hẹp hiện đang được sử dụng.

<table>
<tr><td rowspan="2">B-ISDN</td><td>IEEE 802.2</td><td>SMDS</td><td>Frame Relay</td><td>Other Services</td></tr>
<tr><td>Adaptation Layer</td><td>Adaptation Layer</td><td>Adaptation Layer</td><td>Adaptation Layer</td></tr>
<tr><td colspan="5">ATM</td></tr>
<tr><td colspan="5">SONET/SDH, FDDI ...</td></tr>
</table>

Hình 5.4: B-ISDN hỗ trợ cơ sở hạ tầng

5.3.2. Đặc điểm của dịch vụ B-ISDN

Mục tiêu của B-ISDN là kết hợp tất cả các dịch vụ hiện có vào một mạng truyền thông duy nhất. Về cơ bản nó cung cấp các dịch vụ băng hẹp. Ngoài ra, nó có khả năng cung cấp nhiều dịch vụ băng rộng như điện thoại thấy hình, hội nghị từ xa, truyền số liệu tốc độ cao...

B-ISDN có khả năng cung cấp dịch vụ băng rộng tốc độ đến Mbit/s, còn các tần số mà nó sử dụng và phân bố thời gian sử dụng thì có phạm vi rất rộng.

Đặc tính phân bố khác của tín hiệu dịch vụ B-ISDN là các tín hiệu liên tục. Các tín hiệu tiếng nói và hình ảnh có thể cùng "sống chung" với các tín hiệu nhóm như số liệu đầu cuối. Tuy nhiên, các tín hiệu dữ liệu khác nhau có các tốc độ biến đổi rất rộng. Mặt khác, các tín hiệu hình ảnh và âm thanh đòi hỏi phải xử lý theo thời gian thực.

Kỹ thuật chuyển mạch gói lý tưởng đối với tốc độ thấp hoặc số liệu nhóm, trong khi đó, đối với tín hiệu thoại và hình ảnh thì chuyển mạch kênh là thích hợp. Ngoài ra với các tín hiệu thoại cũng thích hợp chuyển mạch phân chia thời gian và với các tín hiệu video tốc độ cao thì thích hợp với chuyển mạch kênh phân chia theo không gian.

Vì vậy, tìm được một hệ thống truyền dẫn có khả năng trao đổi các tín hiệu tốc độ thấp/cao và các tín hiệu liên tục/ nhóm là cực kỳ khó khăn.

5.3.3. Cấu trúc chức năng của B_ISDN

Mô hình cấu trúc chức năng chung của ISDN băng rộng về cơ bản giống như ISDN băng hẹp. Có nghĩa là về mặt cấu hình tiêu chuẩn, nhóm chức năng và điểm gốc, cả hai cấu trúc đó là như nhau. Nó chỉ ra rằng B-ISDN được hình thành trên cơ sở khái niệm của ISDN. Cấu trúc của ISDN băng rộng bao gồm khả năng mức cao và khả năng mức thấp.

Khả năng mức cao là chức năng liên quan đến thiết bị đầu cuối (TE) và khả năng mức thấp bao gồm khả năng ISDN băng hẹp dựa trên khả năng băng rộng, 64 bit/s và khả năng báo hiệu liên tổng đài.

5.3.4. So sánh giữa ISDN và B_ISDN

B-ISDN là một mạng số liên kết đa dịch vụ như ISDN, nhưng việc thiết lập B-ISDN thực hiện khác với thiết lập ISDN. B_ISDN nó bảo đảm liên kết các tín hiệu băng rộng và có khả năng đồng thời xử lý các tín hiệu băng rộng băng hẹp. Mô hình cấu trúc cơ bản của B-ISDN và ISDN như nhau. Tuy nhiên, chúng chỉ tương tự nhau về mặt khái niệm mà không tương thích về mặt hoạt động. Các thiết bị B_ISDN không thể hoạt động nếu đấu nối vào mạng ISDN hoặc TE của ISDN không thể đấu nối tới NT của B-ISDN. Trong thực tế B-ISDN khác rất xa với ISDN, vì ISDN tích hợp kỹ thuật chuyển mạch kênh và kỹ thuật chuyển mạch gói, trong khi đó B-ISDN sử dụng công nghệ ATM hoàn toàn khác với các hệ thống của ISDN. Nghĩa là, trong khi ISDN chủ yếu điều khiển hệ thống thông tin chuyển mạch kênh thì B-ISDN chủ yếu sử dụng hệ thống thông tin chuyển mạch gói, đồng thời vẫn điều khiển hệ thống thông tin kênh. B-ISDN khác hẳn so với ISDN.

Sự phát triển của ISDN và B_ISDN là bước đệm cho sự ra đời các kỹ thuật mạng viễn thông mới với mục đích cung cấp đa dịch vụ trên cùng một mạng viễn thông duy nhất. Mạng thế hệ sau NGN đang được nghiên cứu và phát triển đáp ứng nhu cầu ngày càng cao của xã hội, đó là một bước tiến mới trong kỹ thuật mạng viễn thông? Một câu hỏi được giải đáp trong tương lai không xa.

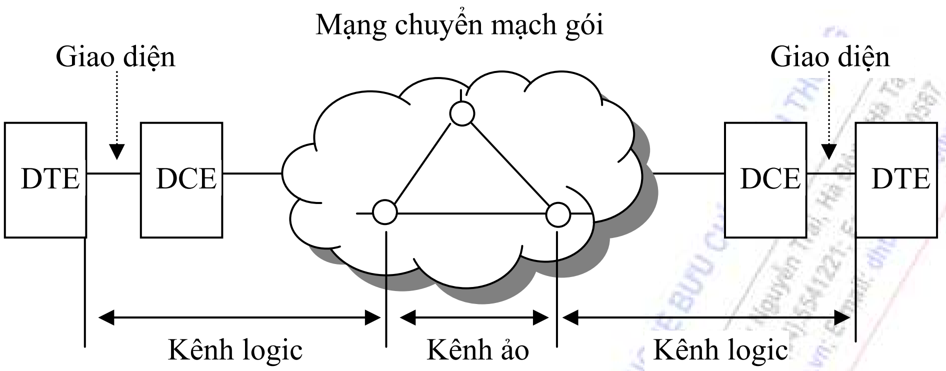
5.4. Mạng chuyển mạch gói X25

5.4.1. Khái quát kỹ thuật mạng X25

X25 định nghĩa chuẩn giao diện giữa các thiết bị đầu cuối số liệu của người sử dụng DTE (Data Terminal Equipment) với thiết bị kết cuối kênh dữ liệu DCE (Data Circuit Terminating). X25 có chức năng vừa điều khiển giao diện DTE/DCE vừa thực hiện chức năng truyền dữ liệu giữa DTE với node của mạng chuyển mạch gói. Các mạng X.25 cung cấp các lựa chọn cho chuyển mạch ảo hoặc cố định. X.25 cung cấp các dịch vụ tin cậy cũng như điều khiển luồng dữ liệu từ node tới node (End to End).

Các mạng X25 có tốc độ tối đa 64 Kbps. Tốc độ này thích hợp với các tiến trình truyền thông chuyển giao tệp và các thiết bị đầu cuối có lượng lưu thông lớn. Tuy nhiên với tốc độ như vậy không thích hợp với việc cung cấp các dịch vụ đòi hỏi từ 1 Mbps trở lên. Vì vậy các mạng

X25 không hấp dẫn khi cung cấp các dịch vụ ứng dụng LAN trong môi trường WAN. Năm 1976, CCITT công bố khuyến nghị loại X về giao thức X25 trong các mạng chuyển mạch gói công cộng (Public Packet Switched Networks).

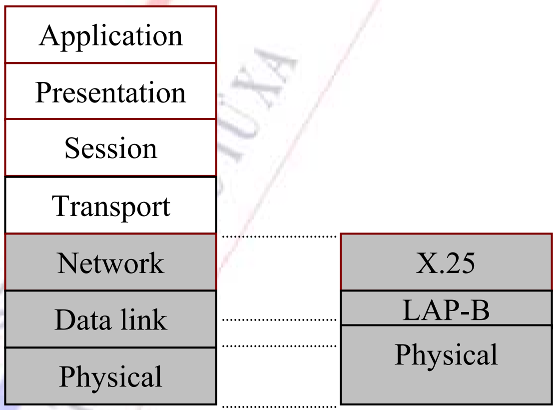


Hình 5.5: Một ví dụ mạng X25 đơn giản

5.4.2. Giao thức X.25

X25 hoạt động trên 3 tầng: tầng vật lý, tầng liên kết dữ liệu và tầng mạng.

Tầng vật lý: Tương ứng với tầng vật lý mô hình OSI, giao thức X25.1 xác định các vấn đề về điện, hàm, thủ tục và kiểu các bộ đấu chuyển được sử dụng. Bao gồm các chuẩn của CCITT X26/27 và EIA (USA Electronic Institue Association), RS :X.21, X.21 Bis, V.32...



Hình 5.6: Mối quan hệ X.25 với mô hình OSI

Tầng liên kết dữ liệu: X.25.2 cung cấp các liên kết giữa hai thiết bị đầu cuối của một tuyến thông tin có độ tin cậy cao, kiểm soát luồng và kiểm soát lỗi. LAP-B (Link Access Procedure Balanced) là giao thức LLC tầng con của Liên kết dữ liệu, chuẩn hướng bit, hoạt động theo chế độ song công và đồng bộ.

Tầng cấp mạng: X.25.3 là giao thức giữa một DTE và một DCE. DTE có thể là một PAD còn DCE có thể là một thiết bị X.25. Giao thức X.25 cung cấp các khả năng chọn mạch ảo thường trực hay theo nhu cầu. X.25 yêu cầu cung cấp dịch vụ tin cậy và tính năng điều khiển luồng dữ liệu End to End. Do các thiết bị trên mạng có thể hoạt động theo nhiều mạch ảo, nên X25 phải cung cấp tính năng điều khiển luồng cho mỗi mạch

Bảng sau tổng kết các chức năng của các tầng trong mô hình X25:

Tầng 1:	Đồng bộ hoá liên kết
Tầng 2:	Phát hiện lỗi và phát lại. Điều khiển luồng
Tầng 3:	Tạo số thứ tự gói tin. Truyền dữ liệu theo phương thức Datagram Thực hiện ghép kênh. Thiết lập kết nối và giảI phóng kênh ảo. Thực hiện báo hiệu

5.4.3. Hoạt động của giao thức X25

X25 hoạt động dựa trên cơ sở kênh cố định PVC (Permanent Virtual Chanel) và kênh ảo chuyển mạch SCV (Switch Virtual Chanel). PCV thay thế chức năng cho kênh liên kết điểm-điểm cố định giữa các thiết bị đầu cuối. Sử dụng loại kênh này, giao diện có hiệu quả hơn nhờ sự liên kết được đảm bảo và không bị trễ cuộc gọi. SVC sử dụng tối đa sự mềm dẻo linh hoạt của chuyển mạch gói trong thực tế.

Hoạt động của X25 theo các giai đoạn: giai đoạn thiết lập kênh ảo, giai đoạn trao đổi thông tin và giai đoạn giải phóng kênh ảo. Ngay sau khi thiết lập kênh ảo, một thông báo tóm tắt của cấu trúc gói tin sẽ được node nguồn gửi đi đến node đích. Nếu chấp nhận, node đích sẽ hiển thị và thông báo lại cho node nguồn. Đường truyền song hướng được thiết lập. Giai đoạn trao đổi dữ liệu: Node nguồn gửi khung thông tin, node đích sẽ tiến hành kiểm tra tính hợp lý của khung thông qua các bit FCS. Nếu không hợp lý thì loại bỏ khung và gửi thông báo lại cho node nguồn biết, yêu cầu truyền lại. Nếu khung là hợp lý thì node này tiếp tục các thủ tục truyền gửi khung tới node tiếp theo trong mạng, đồng thời thông báo lại cho node nguồn biết là đã nhận được thông tin. Node nguồn sau khi đã nhận được thông báo âm từ node đích, tiếp tục gửi gói tin tiếp theo...Sau khi kết thúc, kênh ảo sẽ được giải phóng.

Như vậy hoạt động của X25 cho phép sử dụng một cách có hiệu quả kênh thông tin liên kết giữa người sử dụng và các node mạng. Các thủ tục của tầng mạng đảm bảo trao đổi thông tin có tỷ lệ lỗi bit thấp, với xác suất lớn các gói tin được gửi tới đích không có lỗi, đúng thứ tự, điều này rất cần thiết đối với các đường truyền có độ tin cậy không cao.

5.5. Mạng chuyển mạch khung Frame Relay

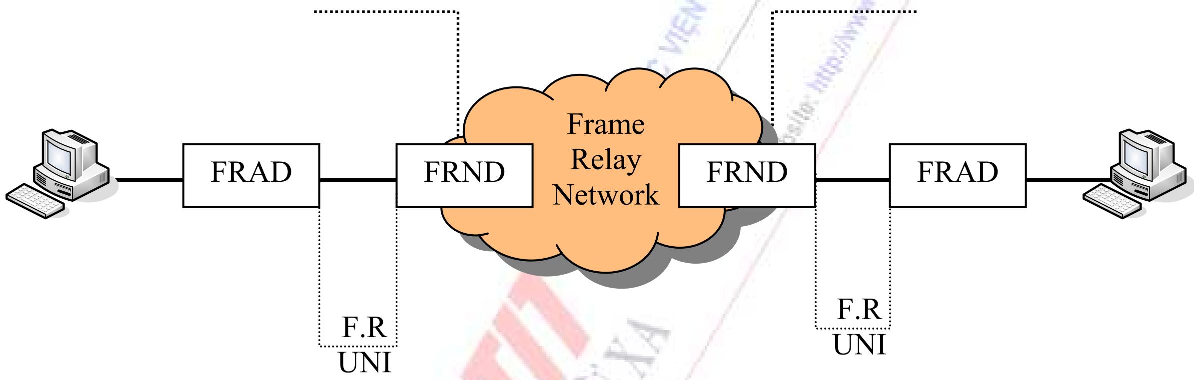
5.5.1. Giới thiệu chung

Những năm cuối của thế kỷ XX các hệ thống viễn thông sử dụng công nghệ cáp quang có độ tin cậy cao, đảm bảo tốc độ và chất lượng truyền dẫn, giảm thiểu tình trạng nghẽn mạch và tỉ lệ lỗi dữ liệu. Các giao thức trước đây cho mạng chuyển mạch gói đặc tả các thủ tục quản lý lưu lượng, quản lý tắc nghẽn và xử lý lỗi, đảm bảo tính thống nhất, toàn vẹn thông tin trên đường truyền đã trở nên phức tạp, cồng kềnh, làm giảm thông lượng.

Frame Relay ra đời như là một công nghệ kế thừa những đặc điểm ưu việt của mạng chuyển mạch gói như tính tin cậy, mềm dẻo, khả năng chia sẻ tài nguyên. Đồng thời hạn chế tối đa thủ tục kiểm soát, hỏi đáp.. không cần thiết gây ra độ trễ lớn. Nó cho phép tận dụng các ưu thế về tốc độ truyền tải và tính ổn định của công nghệ truyền dẫn, thỏa mãn nhu cầu dịch vụ tốc độ cao, sử dụng nhiều thông lượng mạng diện rộng WAN trên đó truyền tải một lượng lớn dữ liệu với nhiều định dạng khác nhau.

Công nghệ Frame Relay tích hợp tính năng dồn kênh tĩnh và chia sẻ công nghệ X.25. Dữ liệu được tổ chức thành các khung có độ dài không cố định được đánh địa chỉ tương tự như X.25. Tuy nhiên, khác với X.25, Frame Relay loại bỏ hoàn toàn các thủ tục ở tầng 3 trong mô hình OSI. Chỉ một số chức năng chính ở tầng 2 được thực hiện. Vì vậy tốc độ truyền trong mạng Frame Relay cao hơn nhiều so với X.25 và mạng Frame Relay được gọi là mạng chuyển mạch gói tốc độ cao.

5.5.2. Cấu hình tổng quát mạng Frame Relay



Hình 5.7 Cấu trúc mạng Frame Relay

Hình 5.7 trình bày các thành phần chính của mạng Frame Relay. Các kênh riêng tạo ra liên kết vật lý giữa DTE và DCE. DTE còn được gọi là thiết bị truy nhập mạng FRAD (Frame Relay Access Device) thường là các Router, Bridge, ATM Switch... DCE còn được gọi là thiết bị mạng FRND (Frame Relay Network Device) là các thiết bị chuyển mạch Frame Relay Switch. FRAD và FRND chuyển đổi dữ liệu thông qua các quy định của giao tiếp UNI. Mạng trục của Frame Relay có thể là các mạng viễn thông IP, PSTN...

5.5.3. So sánh Frame Relay với X25

Sự khác biệt giữa căn bản giữa công nghệ Frame Relay và X.25 là Frame Relay không kế thừa công nghệ X.25 mà là một giao thức tiên tiến có nhiều điểm tương đồng với X.25. X.25 là một giao thức của công nghệ chuyển mạch gói, đặc tả giao tiếp giữa DTE và DCE.

Dữ liệu trong tầng 3 của X.25 sẽ được chia thành các gói (Packet), trong mỗi gói được bổ sung phần Network Header. Các gói này sẽ được chuyển xuống tầng 2, các hàm chức năng của LAP-B sẽ bổ sung Layer 2 Header và các Flag vào mỗi gói tạo thành các khung LAP-B. Các khung sẽ được chuyển xuống tầng vật lý và truyền đến đích.

Hoạt động của các thực thể chặt chẽ, các node mạng X25 phải luôn biết trạng thái của mạng trong mỗi liên kết logic. Các gói tin điều khiển và báo nhận, báo mất (ACK/NACK) thường xuyên được truyền trên cùng liên kết của gói tin dữ liệu không chỉ tại các giao tiếp DTE-DCE mà còn tại tất cả các node mạng. Tại các node mạng phải duy trì bảng trạng thái cho mỗi liên kết logic để quản lý liên kết và điều khiển lỗi và lưu lượng, đảm bảo gói tin đến đúng địa chỉ đích được lưu trong Network Header và số lượng gói tin gửi vào mạng không được vượt quá khả năng xử lý của mạng. Như vậy các giao thức tại tầng mạng là tuyệt đối cần thiết nhất là khi triển khai hệ thống mạng X.25 trên các đường truyền có độ tin cậy thấp, dễ bị nhiễu loạn, suy giảm tín hiệu...

Frame Relay được thiết kế để loại bỏ những hạn chế trong các mạng X.25 khi triển khai trên tuyến truyền dẫn tốc độ cao bằng cách:

- Các gói tin điều khiển và dữ liệu được truyền trên các liên kết logic riêng biệt. Vì vậy, tại các node không cần duy trì bảng trạng thái, không xử lý các gói tin điều khiển.

- Dồn kênh, chuyển mạch các liên kết logic được thực hiện ở tầng liên kết. Loại bỏ các quá trình trình xử lý ở tầng mạng.

- Không điều khiển lưu lượng và điều khiển lỗi theo từng đoạn mạng (Hop-by-Hop Control). Trong trường hợp cần thiết sẽ để các tầng cao hơn đảm trách.

Frame Relay chỉ sử dụng một phần các chức năng ở tầng 2 nên khung thông tin của Frame Relay sẽ có cấu trúc đơn giản hơn so với khung thông tin của X.25 nhưng vẫn duy trì đặc điểm của một khung thông tin quy định bởi giao thức điều khiển.

Khung Frame Relay không có Header của tầng mạng. Vì Frame Relay không sử dụng các thủ tục điều khiển lưu lượng, điều khiển lỗi của tầng mạng. Mặt khác, giao thức được sử dụng tại tầng liên kết chỉ là phần lõi của giao thức điều khiển (LAP-F Core) nên việc xử lý tại các node mạng sẽ ít hơn nhiều so với X.25. Kích thước phần dữ liệu (User Data) trong khung Frame Relay có thể tối đa 2048 byte trong khi phần dữ liệu trong khung X.25 chỉ có thể đạt tối đa 128 byte. DCE thực hiện ba chức năng chính:

- Kiểm tra các khung, loại bỏ các khung có lỗi.

- Căn cứ vào địa chỉ trong khung chọn đường.

- Kiểm tra có bị nghẽn hay không. Nếu có thì lập bit báo nghẽn hoặc loại bỏ khung tùy trường hợp cụ thể.

5.5.4. Frame Relay và mô hình OSI

Tầng vật lý: Các giao thức chuẩn định nghĩa giao tiếp vật lý giữa thiết bị truy nhập FRAD và thiết bị mạng FRND, giữa các node mạng theo chuẩn giao tiếp vật lý của ISDN. Frame Relay tương thích với nhiều giao diện vật lý khác nhau như V.35, X.21...

Tầng liên kết: Các thủ tục liên kết của Frame Relay được định nghĩa bằng giao thức truy cập LAP-D và LAP-F. Giao thức truy cập LAP-F được cải tiến từ LAP-D và được sử dụng phổ biến trong các mạng Frame Relay. Để quản lý liên kết và truyền dữ liệu LAP-F chia thành 2 tầng chức năng là Upper Function (LAP-F Upper) và Coreùunction (LAP-F Core).

- Core Function: có các chức năng kiểm soát độ dài khung, phát hiện lỗi đường truyền, điều khiển nghẽn qua trường báo hiệu trong cấu trúc khung.

- Upper Function: có chức năng điều khiển DLCI (Data Link Connection Identifier), xác định liên kết logic giữa FRAD và FRND.

Tầng mạng (Network Layer): Tầng mạng định nghĩa các khung dữ liệu lưu chuyển trong hệ thống, đảm bảo việc định tuyến trong một mạng hay giữa các mạng với nhau. Trong Frame Relay, các giao tiếp giữa DTE và DCE tầng 3 không có thủ tục nên tốc độ nhanh hơn nhiều so với X.25. Tuy nhiên, nếu một liên kết logic được thiết lập động (SVC), Frame Relay có thể sử dụng một phần của giao thức đặc tả chuẩn Q.931 của giao thức điều khiển ISDN (còn gọi là Q.933) để thiết lập liên kết.

Giao thức liên kết hai node mạng X.25 là X.75, còn để liên kết hai node mạng Frame Relay người ta sử dụng giao diện NNI (Network to Network Interface).

Network	X25 PLP	Management	Q.933 Subnet Management	Full Q.933 Management
Data Link	LAP - B	LAP - F	LAP - F	LAP - F
Physical	X21,V35 (56/64 Kbps)	V35 (DS-0,DS-1..)	V35 (DS-0,DS-1..)	V35 (DS-0,DS-1..)
OSI - RM	X25	PC only (With link Management)	Non ISDN SVC (With link	ISDN SVC (With link Management)

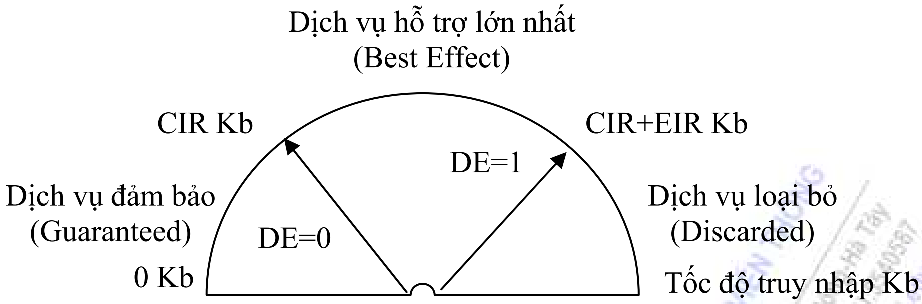
Hình 5.8: So sánh mô hình OSI với X25 và Frame Relay

5.5.5. Điều khiển quản lý lưu lượng

Hầu hết các nhà cung cấp dịch vụ Frame Relay đều sử dụng phương thức tốc độ cam kết CIR (Committed Information Rate) để giải thích chính xác thông tin nào được truyền đến một dịch vụ đảm bảo, thông tin nào nhận được dịch vụ hỗ trợ lớn nhất và thông tin nào bị loại bỏ ở cổng vào của Frame RelayH node nguồn.

Với lưu lượng trên kênh PVC có tốc độ trong khoảng giữa 0 Kbps và phụ thuộc người sử dụng. Khi đó chúng sẽ được truyền đi bình thường qua mạng mà không bị tổn hao đó là dịch vụ đảm bảo "Guaranteed". Đối với các khung thông tin vượt quá CIR một lượng tốc độ thông tin bùng nổ EIR (Excess Information Rate) thì có thể bị Frame Relay node tiếp theo hủy nếu xảy ra nghẽn. Đây chính là dịch vụ hỗ trợ lớn nhất. Khi dữ liệu vượt quá ngưỡng CIR + EIR thì các khung thông tin sẽ bị hủy ngay bởi Frame RelayH node nguồn cho đến khi tốc độ của người sử dụng giảm xuống dưới ngưỡng CIR + EIR.

Tốc độ EIR thường được các nhà khai thác mạng đặt bằng đúng tốc độ CIR.



DE: Discard Eligibility-Bit đánh dấu khung có khả năng bị loại bỏ
CIR: Committed Information Rate- Tốc độ cam kết.
EIR: Eccess Information Rate- Tốc độ thông tin bùng nổ

Hình 5.9: Điều khiển quản lý lưu lượng mạng

5.5.6. Các dịch vụ Frame Relay

Hiện nay, phần lớn các dịch vụ mạng Frame Relay được cung cấp dưới hai dạng:

- Mạng dịch vụ công cộng (Public Carrier-Provided Networks): Frame Relay và FRAD, FRND của nhà cung cấp, khách hàng được tính cước trên cơ sở thông số mạng đã thuê, việc bảo trì và quản trị do các nhà cung cấp thực hiện.

- Mạng riêng doanh nghiệp: Các doanh nghiệp có quy mô toàn cầu triển khai các mạng Frame Relay riêng. Toàn bộ thiết bị mạng là tài sản của doanh nghiệp. Công tác quản trị, vận hành và bảo dưỡng do chính doanh nghiệp đó thực hiện.

Hiện tại, ở Việt Nam phổ biến hình thức mạng dịch vụ công cộng do giá thành sử dụng rẻ hơn, không đòi hỏi doanh nghiệp duy trì đội ngũ nhân viên kỹ thuật chuyên trách. Ngân hàng Á Châu (ACB) là một trong số các đơn vị đang khai thác hiệu quả dịch vụ này.

Frame Relay là công nghệ được ưu tiên lựa chọn bởi ngày càng có nhiều người dùng đang tìm kiếm các giải pháp mạng diện rộng trên nền tảng hạ tầng viễn thông hiện đại. Mặt dù đã có nhiều công nghệ mới ra đời có tính năng hiện đại hơn nhưng với xu thế khách hàng đang ưa chuộng mạng trên nền IP, Frame Relay tiếp tục thể hiện tính ưu việt qua khả năng kết hợp mạng IP với các ưu điểm như quản lý dịch vụ dễ dàng, truyền dữ liệu tốc độ cao an toàn, chi phí liên kết thấp. Có thể khẳng định, công nghệ Frame Relay vẫn có thể được tiếp tục sử dụng hiệu quả trong thời gian dài.

5.6. SMDS (Switched Multimegabit Data Service)

5.6.1. Giới thiệu chung.

SMDS - Switched Multimegabit Data Service là một dịch vụ WAN được thiết kế cho các liên kết LAN-to-LAN. SMDS được Bellcore và Các công ty Regional Bell Operating (RBOCs) phát triển để thoả mãn nhu cầu khách hàng về liên kết LAN Multimegabit trong vùng mạng chính. SMDS được thiết kế là một dịch vụ chuyển mạch gói giá cả hợp lý, cung cấp các liên kết và mở rộng chất lượng cao.

Khác với sự thành công của SMDS ở châu Âu, ở Mỹ SMDS không phát triển. SMDS Interest Group, một tổ chức lớn nhất tài trợ SMDS đã ngừng hoạt động từ năm 1997. Hơn nữa, trong ngày kỷ niệm lần thứ 25 của Truyền thông số liệu - Data Communications (21/10/1997), SMDS được bình chọn là một trong 25 thất bại tiêu biểu nhất - Top 25.

5.6.2. SMDS là gì

SMDS là một dịch vụ mạng diện rộng được thiết kế dành cho liên kết từ mạng LAN với mạng LAN. Là một mạng MAN có đặc trưng: đơn vị dữ liệu là tế bào (Cell-based), không liên kết (Connectionless), tốc độ cao, chuyển mạch gói băng thông rộng. SMDS cũng là một dịch vụ dữ liệu, nghĩa là chỉ truyền dữ liệu (mặc dù nó có thể truyền cả âm thanh và hình ảnh). SMDS là một dịch vụ thật sự, không gắn với một công nghệ truyền số liệu nào.

5.6.3. Tổng quan về SMDS

Tế bào SMDS là đơn vị cơ bản có độ dài cố định. Tương tự như tế bào của ATM gồm 53 bytes - 44-byte dữ liệu, 7-byte Header và 2-byte dấu vết. Điều này tạo cho nó sự tương thích với các mạng diện rộng công cộng B-ISDN sử dụng công nghệ chuyển mạch gói nhanh và công nghệ ATM. Mỗi tế bào của SMDS chứa địa chỉ đích cho phép các thuê bao SMDS có thể truyền dữ liệu với nhau.Là một dịch vụ dữ liệu không liên kết, SMDS thiết lập một đường kênh ảo (Virtual Circuit) giữa thực thể nguồn và đích, các tế bào dữ liệu truyền đi một cách độc lập với nhau và không theo một thứ tự đặc biệt nào.

Mạng SMDS cung cấp băng thông theo yêu cầu cho các bùng nổ giao thông, một thuộc tính của các ứng dụng mạng LAN.Vì không cần phải định nghĩa trước đường truyền giữa các thiết bị, dữ liệu có thể đi qua những đường ít tắc nghẽn nhất trong mạng SMDS, vì vậy sẽ cung cấp một đường truyền nhanh hơn, tăng tính bảo mật và mềm dẻo hơn Khía cạnh băng rộng của SMDS là từ sự tương thích của nó với B-ISDN và tương thích với chuẩn IEEE 802.6 MAN.

5.6.4. Tổng quan về kỹ thuật SMDS

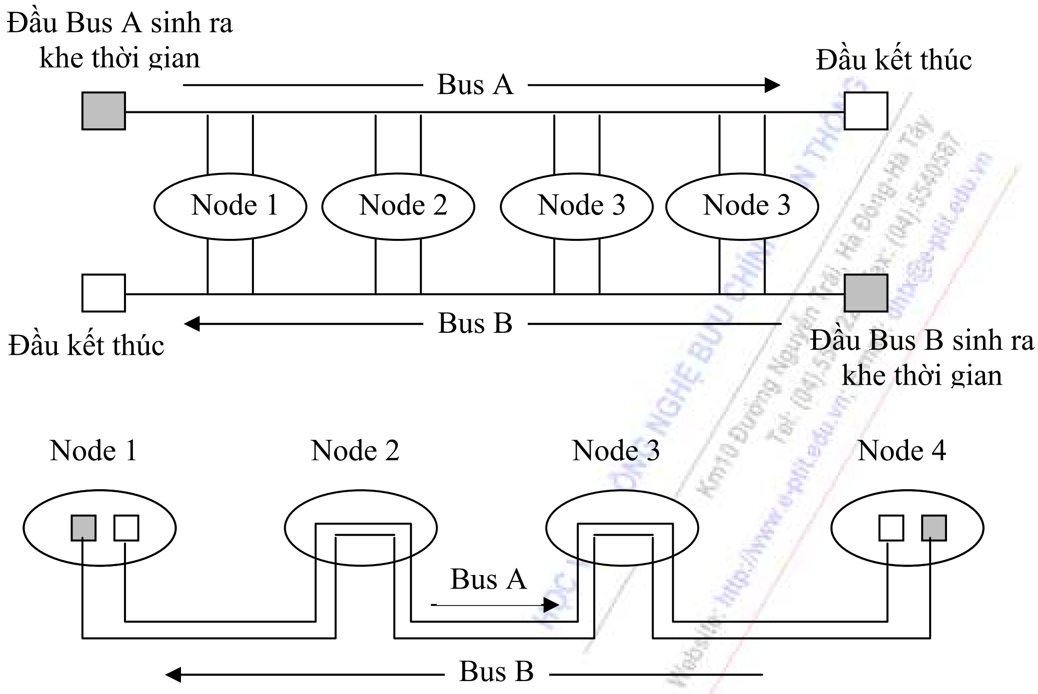
SMDS dựa trên một tập con của tầng vật lý của IEEE 802.6 và chuẩn tầng dưới của MAC (Media Access Control), vì vậy nó hoạt động tương tự như Token Ring tốc độ cao.

- Đặc điểm tầng vật lý: IEEE 802.6 có thể được thiết kế như một Bus hở hoặc một Bus vòng. Khi thiết kế Bus hở, các Bus khởi đầu và kết thúc tại các node khác nhau.Với Bus dạng vòng, các Bus khởi đầu và kết thúc tại cùng một node .

- Đặc điểm tầng liên kết dữ liệu - DQDB (Distributed Queue Dual Bus): Tại tầng liên kết dữ liệu, mạng SMDS được quản lý bởi giao thức DQDB bus quảng bá đa truy nhập. IEEE 802.6, chia nhỏ mỗi bus thành các khe để truyền dữ liệu. Trong mỗi bus có một bit bận và một bit yêu cầu. DQDB làm việc như sau:

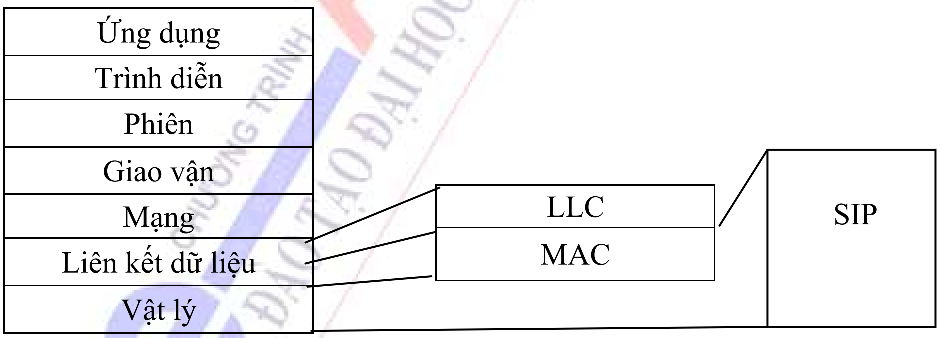
Ví dụ node 2 truyền dữ liệu cho node 3, trước khi truyền, đặt bit Req trên Bus B để thông báo cho các bus phía trên của Bus A biết rằng tại node đó đang có dữ liệu cần gửi. Sau khi yêu cầu một khe, node 2 quan sát cả hai bus và duy trì một số đếm các yêu cầu. Số đếm đó sẽ tăng 1 khi node 2 thấy một bit yêu cầu được thiết lập trên Bus B và giảm đi 1 cho mọi khe trống trên Bus A. Như vậy số đếm tại mỗi node cho biết chiều dài hàng các tế bào đang đợi để truyền bởi các node phía dưới. Khi số đếm bằng 0 nghĩa là không còn node dưới nào có dữ liệu cần gửi thì node đó bắt đầu gửi dữ liệu.

DQDB hỗ trợ dich vụ không liên kết và hướng liên kết và có khả năng truyền dữ liệu, tiếng nói và hình ảnh. Mặc dù là một tập con của IEEE 802.6, SMDS chỉ truyền dữ liệu.



Hình 5.10: Cấu hình vật lý của mạng SMDS.

Giao thức giao diện mạng SMDS (SMDS Interface Protocol - SIP): SIP được định nghĩa bởi Bellcore và cấu thành bởi ba mức giao thức: SIP mức 3, SIP mức 2, và SIP mức 1, hoạt động trong tầng Liên kết dữ liệu và tầng vật lý.



Hình 5.11: Các tầng của SIP tương ứng với mô hình OSI

5.6.5. SMDS so với các công nghệ ATM và Frame Relay.

- SMDS là một dich vụ, không phải một công nghệ; Frame Relay và ATM là công nghệ .
- SMDS dịch vụ chuyển mạch gói không liên kết (Connectionless), Frame Relay và ATM là hướng liên kết (Connection-Oriented).

- SMDS cung cấp nhiều cách quản lý mạng đặc trưng.

- SMDS bị cạnh tranh bởi ATM và Frame Relay ở nước Mỹ.

- DQDB cung cấp các công nghệ cần thiết cho sự truyền các ứng dụng thời gian thực.

- SDMS hỗ trợ tính bảo mật, cho phép dùng các mạng công cộng, chia sẻ một mạng riêng như mạng xương sống. Khái niệm này đã bị che lấp bởi Internet và VPN.

Là một dich vụ, không phải là một công nghệ nên có thể triển khai trên cả Frame Relay và ATM. Không phụ thuộc về giao thức, nên có thể hỗ trợ nhiều giao thức mạng LAN hay mạng máy tính. Có băng thông từ 56/64 Kbps tới tốc độ SONET, phù hợp với giải thông cho mọi ứng dụng. Là dịch vụ không liên kết, không cần định nghĩa các PVC như Frame Relay. Tế bào 53 byte tương thích với ATM, có thể chuyển đổi thuận tiện sang mạng ATM.

Tuy nhiên một số điểm không thuận lợi đã làm cho SMDS bị ATM và Frame Relay che khuất như là được nhìn nhận là một dịch vụ đắt tiền, mặc dù có khả năng truyền được hình ảnh nhưng SMDS không hỗ trợ tính năng này...

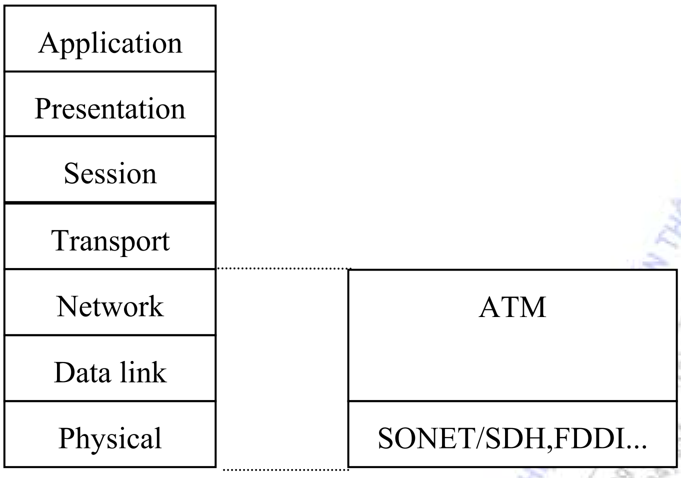
5.7. Phương thức truyền dẫn không đồng bộ ATM (Asynchronous Transfer Mode)

5.7.1. Giới thiệu chung

Công nghệ truyền dẫn không đồng bộ ATM (Asynchronous Transfer Mode) ra đời như là một nền tảng cho mạng tổ hợp đa dịch vụ số băng rộng B-ISDN. ATM cho phép truyền thông đa phương tiện, đáp ứng đầy đủ các loại hình dịch vụ và có khả năng cung cấp chất lượng dịch vụ theo yêu cầu. ATM có một số đặc trưng khác với các công nghệ chuyển mạch khác. Đơn vị dữ liệu dùng trong ATM gọi là tế bàol (Cel), có độ dài 53 byte (5 byte Header và 48 byte dữ liệu). Trong các công nghệ khác độ dài của khung dữ liệu thay đổi (từ 64 đến 1500 Byte). Những Cell này là đơn vị cơ sở cho truyền dữ liệu. Lưu lượng dữ liệu từ nhiều kênh được ghép với nhau tại mức Cell. Kích thước Cell cố định, nên các cơ chế chuyển mạch hoạt động truyền thông của mạng ATM hiệu quả cao, tốc độ cao. Một số mạng ATM có thể hoạt động tới tốc độ 622 Mbps, tốc độ chung 155 Mbps.

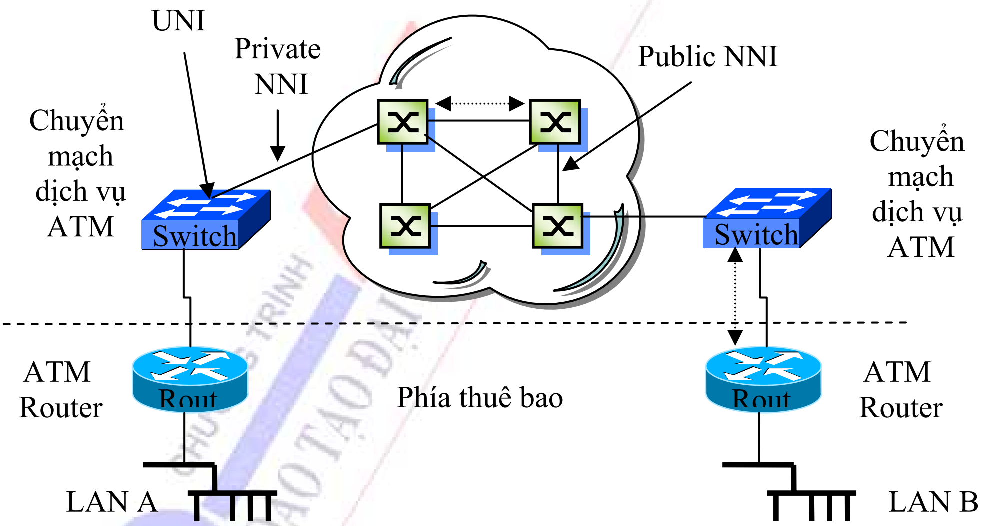
ATM hoạt động ở tầng 2 và 3 trong 3 tầng cuối của OSI. Tầng vật lý có các giao thức hỗ trợ như SONET, FDDI,... ATM hoạt động không phụ thuộc vào đường truyền vật lý. ATM được chia làm hai Channel có chứa các ô (Cell) hoạt động như tốc độ truyền bit cố định khi dữ liệu được truyền giữa các mạch (Circuit) có kích thước khác nhau.

Các thiết bị mạng ATM liên kết với nhau bằng các đường dẫn ảo VPI (Virtual Path Identifier). Trong mỗi đường ảo, có nhiều kênh ảo VCI (Virtual Circuit Identifier). Mặc dù ATM được phát triển như là công nghệ của mạng WAN nhưng ATM có nhiều chức năng hỗ trợ cho các mạng LAN hiệu năng cao. Đó là ATM cho phép sử dụng cùng một công nghệ cho cả mạng LAN và WAN.



Hình 5.12 Mối quan hệ ATM voí mô hình OSI

Về cơ bản, mạng ATM giống như mạng Frame Relay, các tế bào được truyền từ nguồn tới đích qua các mạng con chuyển mạch ATM. Node mạng giao tiếp với thiết bị đầu cuối qua giao diện người sử dụng - mạng UNI (User Network Interface) và thiết bị chuyển mạch ATM giao tiếp với những thiết bị khác qua giao diện mạng-mạng NNI (Network Network Interface). Một mạng ATM đơn giản điển hình như sau:



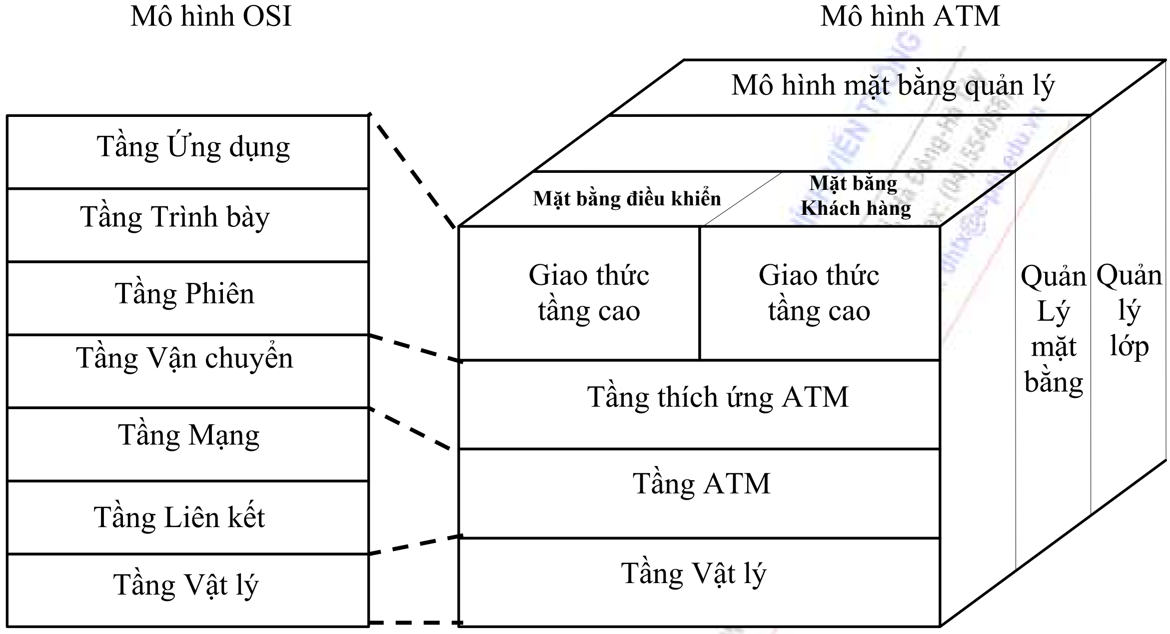
Hình 5.13 Mối quan hệ ATM với mô hình OSI

5.7.2. Kiến trúc phân tầng ATM

Kiến trúc ATM không có sự tương ứng hoàn toàn với các tầng của mô hình OSI. Mô hình kiến trúc ATM bao gồm các mặt bằng quản lý, mặt bằng điều khiển (kiểm tra) và mặt bằng người sử dụng. Mặt bằng quản lý gồm có quản lý mặt bằng và quản lý tầng.

a. Các mặt bằng quản lý

- Mặt bằng điều khiển: Cung cấp các chức năng thiết lập, giám sát và giải phóng liên kết. Mặt bằng này có nhiệm vụ khởi tạo và quản lý các yêu cầu báo hiệu.



Hình 5.14 Kiến trúc phân tầng mô hình ATM

- Mặt bằng khách hàng: Cung cấp chức năng điều khiển vận chuyển các luồng thông tin, điều khiển luồng và quản lý các luồng dữ liệu , sửa lỗi.

- Mặt bằng quản lý: Cung cấp chức năng giám sát mạng liên quan đến dữ liệu và thông tin điều khiển. Gồm các chức năng quản lý lớp và quản lý mặt bằng.

- Quản lý lớp: Thực hiện việc điều hành các tham số người sử dụng, các thông tin quản lý khai thác và bảo dưỡng.

- Quản lý mặt bằng: Điều khiển hệ thống bằng cách can thiệp vào giữa các mặt bằng.

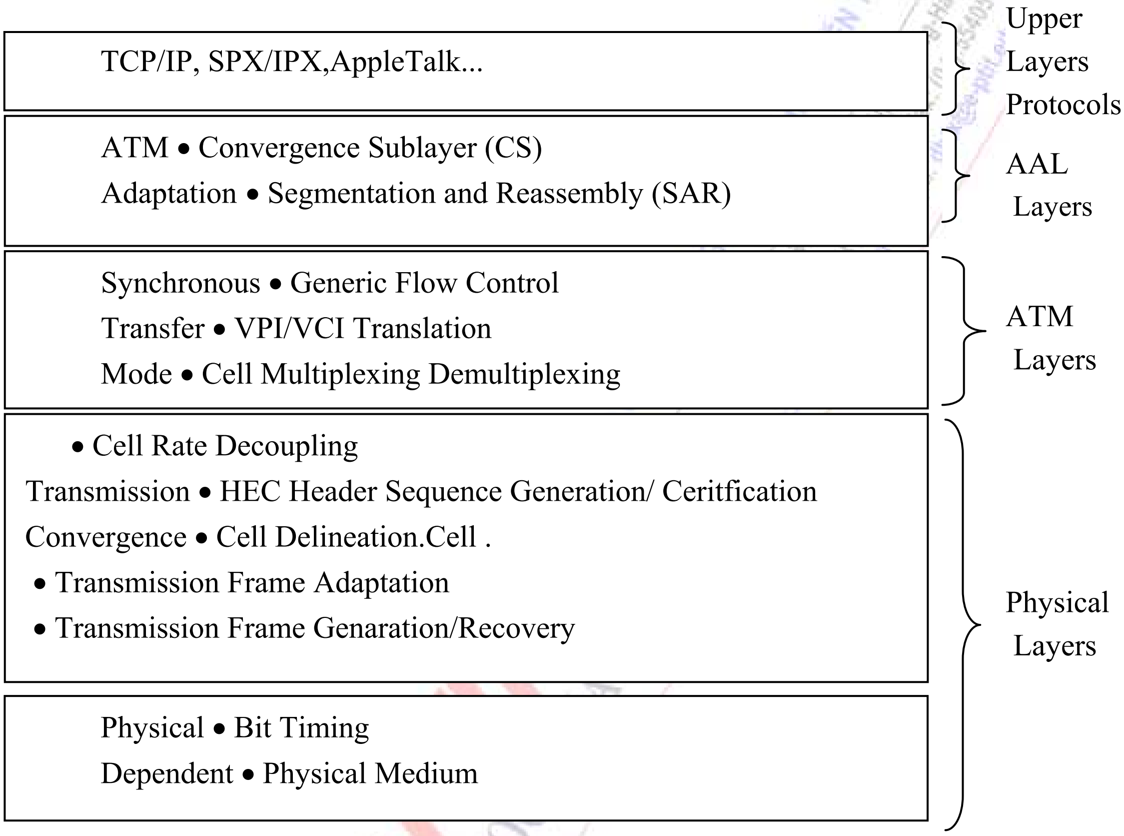
b. Vai trò và chức nằn các tầng ATM

Ngoài ra giao thức của mặt bằng điều khiển và mặt bằng khách hàng được phân loại tiếp thành tầng giao thức mức cao, tầng thích ứng, tầng ATM và tầng vật lý như sau:

- *Tầng vật lý:* Tương tự như lớp vật lý của OSI, ATM quản lý môi trường truyền dẫn, bao gồm 02 tầng con: Tầng con môi trường vật lý PMD (Physical Medium-Dependent) và tầng con kết hợp truyền dẫn TC (Transmission Convergence).

- *Tầng ATM:* Tầng ATM kết hợp với tầng thích ứng ATM có chức năng tương tự như tầng liên kết dữ liệu trong mô hình tham chiếu OSI. Hỗ trợ cho việc tách/ghép tế bào, dịch VPI và VCI, phát sinh tế bào mào đầu, điều khiển luồng chung.

- *Lớp thích ứng ATM - AAL (ATM Adaption Layer):* Có nhiệm vụ giao tiếp với lớp bậc cao. Cung cấp các phương tiện hội tụ cho phép các dạng truyền thông khác nhau có thể tương thích với các dịch vụ ATM. Lớp AAL chuẩn bị dữ liệu của người sử dụng và phân đoạn dữ liệu thành 48 byte trong tế bào ATM. Tầng AAL chia thành hai tầng con: Tầng con hội tụ CS (Convergence Sublayer) và tầng con phân chia và kết hợp SAR (Segmentation and Reassembly Sublayer), thực hiện việc cắt các đơn vị dữ liệu của người sử dụng thành các Cell ATM 48-byte để truyền và hợp các Cell ATM thành đơn vị dữ liệu của người sử dụng khi nhận.



Hình 5.15 Các tầng trong ATM

- *Giao thức các tầng trên (Upper Layers Protocols)* : Nằm trên lớp AAL, nó tập hợp các dữ liệu khách hàng được chấp nhận, sau đó tiến hành sắp xếp vào trong các gói, và liên kết với lớp AAL.

Tầng	Phân tầng	Các chức năng
Tầng bậc cao		Chức năng của tầng bậc cao
Tầng ATM thích ưng	Tầng con hội tụ	Chức năng kết hợp
	Chia và tập hợp lớp	Chức năng phân chia và kết hợp lại
Tầng ATM		Điều khiển lưu lượng chung Tạo và tách thông tin ghép đầu Dịch các tế bào VPI/VCI Ghép và tách tế bào
Tầng vật lý	Truyền dẫn hội tụ tầng con	Phân chia tốc độ tế bào Tạo và xác định tín hiệu HEC Nhận dạng biên của tế báo Tạo và xác định khung truyền dẫn
	Môi trường vật lý	Chức năng thông tin thời gian bít Chức năng tương ứng môi trường vật lý

Hình 5.16 Vai trò & chức năng các tầng trong ATM

5.7.3. Liên kết ảo (Virtual Connections)

Liên kết ATM gồm hai loại liên kết ảo:

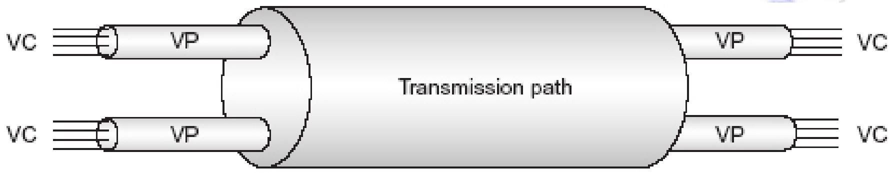
- Liên kết kênh ảo VCC (Virtual Channel Connection): Một kênh ảo cung cấp một liên kết logic giữa các thiết bị đầu cuối ATM. Kênh ảo có thể là kênh ảo cố định PVC (Permanent VC) hoặc kênh ảo chuyển mạch SVC (Switch VC).

- Liên kết đường dẫn ảo VPC (Virtual Path Connection): Một liên kết đường dẫn ảo cung cấp một tập hợp logic các kênh ảo mà có cùng điểm cuối.

Kênh ảo và đường dẫn ảo có thể nhận diện qua các trường VCI và VPI trong Header của ATM Cell. Trong một đường dẫn ảo có thể có nhiều kênh ảo và kênh ảo trong các đường dẫn ảo khác nhau có thể có cùng một VCI. Do đó một kênh ảo hoàn toàn có thể xác định bởi sự kết hợp giữa VPI và VCI.

Trong kỹ thuật ATM, các tế bào chứa các loại dữ liệu khác nhau được dồn kênh trên một đường dẫn ảo VPI, thường một đường trung kế tốc độ cao hoặc một liên kết sử dụng thiết bị ATM. Trong một đường dẫn ảo có thể có một số kênh ảo VCI (Virtual Channel Identìier) riêng biệt. Trong cấu trúc khung của một tế bào ATM, trường VPI là 1 byte, tiếp theo trường VCI 2 byte. Thiết bị chuyển mạch ATM có thể định tuyến ATM trên cơ sở byte đầu tiên. Khi Cell đến đích, VCI được dùng xác định sâu hơn vị trí chính xác để truyền Cell. Như vậy cặp VPI và VCI tạo một trường 3 byte, cho phép sử dụng tối đa 16 triệu kênh ảo trên một giao diện đơn.

VPI/VCI phải qua quá trình ánh xạ dựa trên bảng lộ trình lưu trữ tại các tổng đài chuyển mạch ATM. Khi một kênh ảo được thiết lập, bảng chọn đường tại các node chuyển mạch ATM tìm kiếm và cung cấp địa chỉ đích của các Cell đến dựa trên địa chỉ Header của Cell. Bảng chọn đường thường xuyên được cập nhật các địa chỉ mới VPI/VCI khi được các bộ chuyển mạch ATM chấp nhận. Trong giai đạon thiết lập cuộc gọi, các Cell được truyền từ node này sang node khác, đường dẫn gọi là Virtual.



Hình 5.17 Khái niệm kênh ảo và đường dẫn ảo

Công nghệ truyền dẫn không đồng bộ ATM (Asynchronous Transfer Mode) ra đời như là một nền tảng cho mạng tổ hợp đa dịch vụ số băng rộng B-ISDN. ATM cho phép truyền

5.7.4. So sánh ATM với các dịch vụ và kỹ thuật khác

ATM so sánh với Frame Relay:

- ATM và Frame Relay là hai công nghệ chuyển mạch tốc độ nhanh . Có thể nói ATM tương tự với Frame Relay. Tuy nhiên, khung dữ liệu (Frame) trong Frame Relay có kích thước thay đổi, thì ATM sử dụng các gói tin cố định 53 bytes (được gọi là tế bào – Cell).

- Frame Relay cho phép vượt ngưỡng 64 Kb/s của X25, nhưng thông lượng tối đa chỉ đạt tới 2 Mb/s, trong khi thông lượng ATM có thể đạt 155 Mb/s hoặc 622 Mb/s.

- ATM có thể chèn các tế bào có độ trễ truyền dẫn nhạy cảm, điều này không thể được với Frame Relay, bởi vì Frame Relay có khung dữ liệu dài hơn, độ trễ lớn hơn và không thể dự đoán được độ trễ khi xử lý truyền thông tiếng nói và hình ảnh. Vì vậy Frame Relay không phù hợp cho các dịch vụ yêu cầu thời gian thực cao.

- Mặc dầu chưa đáp ứng được yêu cầu của truyền thông đa phương tiện, Frame Relay vẫn là một giải pháp quá độ được lựa chọn trong khi chờ đợi kỹ thuật ATM đưa vào ứng dụng rộng rãi.

ATM và SONET

- SONET đơn giản là một kỹ thuật truyền dẫn, có thể hỗ trợ cho nhiều loại topo thay đỗi, bao gồm : điểm-điểm, hình sao, hình vòng.

- Khi phát triển ATM, thay vì phát triển một lớp vật lý mới, những nhà thiết kế của ATM đã sử dụng kỹ thuật liên kết dữ liệu của SONET và sử dụng nó cho chuyển mạch ATM. Hơn nữa, ATM Forum xác định tốc độ 622-Mbps ATM để chạy trên SONET. Tóm lại SONET là một dịch vụ vận chuyển bit từ nguồn tới đích và ATM là một kỹ thuật sử dụng SONET như là một dịch vụ vận chuyển của nó.

So Sánh ATM và Ethernet Gigabit

- Tốc độFast Ethernet và Ethernet Gigabit nhanh hơn tốc độ của ATM và ỗây dựng ATM khá đắt. Tuy nhiên ATM Forum đang phát triển ATM 2,5 Gbps cho LAN.

- Ethernet Gigabit có khả năng truyền dữ liệu và tiếng nói ở mức chấp nhận được, tuy nhiên nó vẫn chỉ là một kỹ thuật VBR (tốc độ bit thay đổi) và gặp phải khó khăn khi mạng tắc nghẽn hoặc đòi hỏi truyền hình độ phân giải cao (HDTV).

- Giao thức giữ trước nguồn tài nguyên RSVP (Resource Reservation Protocol) và giao thức truyền dẫn thời gian thực RTP (Realtime Transport Protocol) là phương thức lỗi chất lượng dịch vụ của Ethernet Gigabit. Cả hai giao thức cho phép các ứng dụng bảo tồn tổng số riêng biệt của giải thông truyền dữ liệu. So sánh Ethernet Gigabit với ATM:

Khung Ethernet 802.3 có sự phân chia tốc độ không phù hợp, vì chiều dài thay đổi từ 64 đến 1518 bytes. Trong khi tế bào ATM phân chia tốc độ ổn định và đảm bảo sự phân chia có thứ tự trong khung thời gian riêng biệt mà bit dữ liệu đến theo thứ tự đúng thời gian.

Trong Ethernet 802.3, khung được xếp hàng tại một node chuyển mạch trên cơ sở vào trước-ra trước (FI-FO). Hơn nữa trước khi chuyển mạch để truyền hàng khung 'n' thì toàn bộ dữ liệu chứa trong hàng khung 'n-1' phải được truyền. Theo đó một chuyển mạch phát hàng khung liên tục theo thứ tự chúng được đệm. Sự xử lý này ở trong ATM thì khác hẳn, tại node chuyển mạch ATM , hàng đợi khung không theo thứ tự chúng được đệm, mà chuyển mạch ATM dựa vào sự ưu tiên để truyền dẫn: khung có độ ưu tiên cao hơn sẽ được truyền dẫn trước và ngược lại. Do đó ATM có thể tạo ra đồng thời nhiều hàng dịch vụ độc lập nhau với sự ưu tiên truyền dẫn khác nhau dựa trên loại dịch vụ mà vẫn cung cấp một tốc độ phân chia không đổi. Đây chính là thế mạnh và sự "thông minh" của ATM. Do vậy mạng nhanh không phải là giải pháp cho nhiều vấn đề hội tụ.

Công nghệ ATM xuất hiện với mạng diện rộng, đa dịch vụ băng rộng. Phương thức truyền tải như là một "Mạng trong mạng", không đồng bộ, tích hợp chuyển mạch gói và chuyển mạch kênh. Thông tin được đặt trong các gói có độ dài cố định. ATM sử dụng kênh ảo và nhóm kênh ảo tạo thành một đường dẫn ảo Thích hợp với dịch vụ yêu cầu truyền thời gian thực, đa phương tiện.

Câu hỏi trắc nghiệm:

1. Hãy chọn câu đúng nhất về phương pháp kết nối liên mạng:
   A. Phương pháp kết nối tại tầng vật lý, bộ lặp Repeater.
   B. Phương pháp kết nối tại tầng liên kết dữ liệu, thiết bị sử dụng cầu (Bridge) và các bộ chuyển mạch (Switched)
   C. Phương pháp kết nối tầng mạng. Thiết bị sử dụng bộ định tuyến (Router).
   D. Kết nối liên mạng sử dụng các thiết bị như Modem, cáp Modem, Router..
2. Mạng ISDN có những đặc điểm sau:
   A. Là một mạng đa dịch vụ.
   B. ISDN có hệ thống báo hiệu số 7 và các node chuyển mạch thông minh.
   C. Kiến trúc ISDN tương thích với mô hình OSI.
   D. Tất cả khẳng định trên.
3. Các phần tử cơ bản của mạng ISDN
   A. TE1 là các thiết bị đầu cuối có các thuộc tính ISDN.

B. TE2 là các thiết bị đầu cuối không có tính năng ISDN.

C. NT1 (Network Termination 1) thực hiện các chức năng thuộc tầng vật lý .

D. NT2 (Network Termination 2) là một thiết bị thông minh, thực hện các chức năng đến tầng mạng.

E. Tất cả đều đúng.

4. Các loại kênh trong mạng ISDN

A. Kênh D: Dùng để truyền báo hiệu giữa người sử dụng và mạng.

B. Kênh B: Dùng để truyền dữ liệu

C. Kênh H cung cấp các dịch vụ tốc độ cao và ghép các luồng thông tin ở tốc độ thấp hơn. có 4 loại kênh H.

D. Các loại đường ảo và kênh ảo

5. Giao diện ISDN

A. Giao diện BRI (Basic Rate Interface)

B. Giao diện PRI (Primary Rate Interface)

C. Giao diện giữa các tầng, cung cấp các điểm truy nhập dịch vụ.

6. Hoạt động trong tầng Datalink của ISDN:

D. Giao thức LAP-D

A. Giao thức HDLC

B. Giao thức LAP-B và LAP – F

C. Giao thức LAP-D và LAP – F

7. Đặc tính kỹ thuật mạng của X25

A. X25 định nghĩa chuẩn giao diện giữa DTE và DCE

B. Cung cấp các lựa chọn cho chuyển mạch ảo hoặc cố định. X.25

C. Cung cấp các dịch vụ cóp độ tin cậy cao từ node tới node (End to End).

D. Tốc độ tối đa 64 Kbps.

E. Tất cả đều đúng

8. Trên cáp sợi quang, các tốc độ điển hình của B-ISDN là:

A. 51 Mbps(*)

B. 155 Mbps(*)

C. 312 Mbps

D. 622 Mbps(*)

9. Mạng X25 không hấp dẫn, vì:

A. Tốc độ thấp, không thích hợp các dịch vụ yêu cầu tốc độ cao. Các dịch vụ LAN trong môi trường WAN.

B. Không phù hợp trong môi trường truyền dẫn quang.

C. Tất cả khẳng định trên đều đúng.

10. Hoạt động trong tầng Datalink của X25, có:
    A. Giao thức LAP-B
    B. Giao thức HDLC
    C. Giao thức LAP-B và LAP – F
    D. Giao thức LAP-D và LAP – F
11. Đặc trưng cơ bản của Frame Relay:
    A. Không cần duy trì bảng trạng thái, không xử lý các gói tin điều khiển.
    B. Loại bỏ các quá trình trình xử lý ở tầng mạng.
    C. Không điều khiển lưu lượng và điều khiển lỗi theo từng đoạn mạng (Hop-by-Hop Control).
    D. Khung dữ liệu (Frame) có kích thước thay đổi,
    E. Các trường hợp trên đều đúng.
12. Hoạt động trong tầng Datalink Frame Relay, có:
    A. Giao thức LAP- F
    B. Giao thức HDLC
    C. Giao thức LAP-B và LAP – F
    D. Giao thức LAP-D và LAP – F.
13. Đặc trưng cơ bản SMDS:
    A. SMDS là một dich vụ, không phải một công nghệ.
    B. SMDS dịch vụ chuyển mạch gói không liên kết
    C. SDMS hỗ trợ tính bảo mật, cho phép dùng các mạng công cộng, chia sẻ một mạng riêng như mạng xương sống.
    D. Tất cả phát biểu trên đều đúng.
14. Những khảng định nào sau đây là đúng:
    A. Công nghệ ATM gần giống với công nghệ Frame Relay.
    B. Khung dữ liệu của Frame Relay có kích thước thay đổi, của ATM cố định.
    C. Tốc độ truyền tối đa 2 Mb/s trong Frame Relay, của ATM có thể đạt 155 Mb/s hoặc 622 Mb/s.
15. Những thực thể nào dưới đây là giao thức của WAN
    A. Frame Relay (*).
    B. SLIP
    C. IEEE 802.6
    D. X25(*)
16. Các giao thức nào thường được sử dụng với IEEE 802.2
    A. IEEE 802.3
    B. IEEE 802.5

C. IEEE 802.6
D. Tất cả đều đúng

17. Nêu đặc tính chủ yếu để phân biệt một tế bào và một gói tin.
    A. Các tế bào nhỏ hơn một gói tin.
    B. Các tế bào không có địa chỉ vật lý.
    C. Các tế bào có độ dài cố định (*).
    D. Các gói tin không thể truyền.
18. Giao thức nào được sử dụng trên cáp sợi quang.
    A. Frame Relay
    B. FDDI(*)
    C. SONET(*)
    D. X25
19. Các chuẩn nào sử dụng kỹ thuật truy nhập đường truyền bằng thẻ bài:
    A. IEEE 802.4(*)
    B. IEEE 802.6
    C. Frame Relay
    D. FDDI(*)
20. Giao thức nào phù hợp nhất cho việc giao vận dữ liệu quan trọng về mặt thời gian:
    A. X25.
    B. Frame Relay
    C. IEEE 802.5(*)
    D. ATM(*)

Câu hỏi và bài tập

1. Mạng tích hợp đa dịch vụ số ISDN (Integrated Service Digital Network), Khái niệm. Nguyên lý chung của ISDN.
2. Các dịch vụ ISDN: Dịch vụ tải tin, dịch vụ viễn thông, các dịch vụ bổ sung.
3. Các phần tử cơ bản của mạng ISDN
4. Các loại kênh trong mạng ISDN: Kênh D, Kênh B, Kênh H.
5. Giao diện ISDN:
    - ✓ Giao diện BRI (Basic Rate Interface)
    - ✓ Giao diện PRI (Primary Rate Interface):
6. Địa chỉ của mạng ISDN và cấu trúc địa chỉ trong ISDN:
7. Chức năng các tầng trong kiến trúc ISDN: Tầng vật lý, Tầng 2 và tầng 3.
8. Mạng băng rộng B_ISDN (Broadband ISDN)

9. Đặc điểm của dịch vụ B-ISDN
10. Nền tảng kỹ thuật của B-ISDN
11. Cấu trúc chức năng của B_ISDN
12. So sánh ISDN và B_ISDN
13. Mạng chuyển mạch gói X25
14. Giao thức X.25: Tầng vật lý, Tầng liên kết dữ liệu, Tầng mạng
15. Hoạt động của giao thức X25
16. Mạng chuyển mach khung Frame Relay
17. Cấu hình tổng quát mạng Frame Relay
18. So sánh Frame Relay với X25:
    - ✓ Tầng vật lý (Physical Layer),
    - ✓ Tầng liên kết (Link Access Layer),
    - ✓ Tầng mạng (Packet Layer)
19. Frame Relay được thiết kế loại bỏ những hạn chế trong các mạng X.25, vì sao?.
20. Vì sao thời gian xử lý tại các node trong Frame Relay ít hơn nhiều so với X.25 ?.
21. Frame Relay và mô hình OSI: Tầng vật lý, Tầng liên kết và Tầng mạng .
22. Trình bày giao thức LAP-F, LAP-D.
23. Điều khiển quản lý lưu lượng
24. Khái niệm CIR.
25. Các dịch vụ Frame Relay
26. SDMS (Switched Multimegabit Data Service)
27. SMDS so với các công nghệ ATM và Frame Relay.
28. Phương thức truyền dẫn không đồng bộ ATM (Asynchronous Transfer Mode)
29. Kiến trúc phân tầng ATM:
    - ✓ Các mặt bằng quản lý
    - ✓ Vai trò và chức nằn các tầng.
30. Khuôn dạng Cell ATM
31. UNI-Format Header : Khuôn dạng giao diện người sử dụng và mạng
32. NNI-Format Header: Khuôn dạng giao diện mạng và mạng.
33. Các loại tế bào
34. Liên kết ảo (Virtual Connections)
35. So sánh ATM với các dịch vụ và kỹ thuật khác
36. ATM so sánh với Frame Relay:
37. ATM và SONET
38. So Sánh ATM và Ethernet Gigabit

CHƯƠNG 6: MẠNG TỐC ĐỘ CAO VÀ ỨNG DỤNG CÁC CÔNG NGHỆ MỚI

Nội dung của chương sẽ trình bày một cách tổng quát về các loại mạng tốc độ cao và các ứng dụng công nghệ mới bao gồm đường dây thuê bao số DSL, các mạng truyền tải voice chuyển mạch gói trên nền IP như Voice over Internet Protocol, Voice over ATM và Voice over Frame Relay. Công nghệ MPLS phù hợp với xu thế và nhu cầu truyền thông hiện tại và tương lai. MPLS được ứng dụng trong mạng lõi NGN và nền tảng cho dịch vụ VPN. Mạng thế hệ sau NGN (Next Generation Network) là một trong những mạng hội tụ tiên tiến đang phát triển và thay thế dần các mạng truyền thống. Hoạt động dựa trên các công nghệ chuyển mạch mềm Softswitch, điều khiển chuyển mạch không phụ thuộc vào phần cứng . Có khả năng lập trình độc lập và kiến tạo dịch vụ mềm dẻo. Nội dung của chương gồm:

- Đường dây thuê bao số DSL
- Truyền thoại qua mạng chuyển mạch gói VoPN
- Công nghệ chuyển mạch đa giao thức MPLS.
- Công nghệ chuyển mạch mềm Softwitch
- Mạng hội tu và mạng thế hệ sau NGN.

6.1. Đường dây thuê bao số DSL (Digital Subscribers Line)

6.1.1. *Mở đầu*

Công nghệ đường dây thuê bao số DSL cho phép tận dụng miền tần số cao truyền tín hiệu tốc độ cao trên đôi dây cáp đồng thông thường. Modem DSL biến đổi tín hiệu của người sử dụng như tín hiệu điện thoại, tín hiệu truyền hình, dữ liệu... thành các tín hiệu phù hợp với đường truyền DSL, có cấu trúc dữ liệu riêng, mã đường dây riêng và một số tín hiệu điều khiển nhất định của mạng. Đường dây thuê bao số được sử dụng đầu tiên với mạng số tích hợp đa dịch vụ ISDN (Integrated Services Digital Network) truyền số liệu giữa các đầu cuối. Nhiều phiên bản DSL sau này được thiết kế từ thực tế ISDN DSL. Các thế hệ DSL sau được cải thiện rất nhiều về công suất, cách thức hoạt động, khả năng cung cấp dịch vụ… Kỹ thuật DSL cho phép truyền chế độ song công đối xứng và bất đối xứng.

6.1.2. Tổng quan về họ công nghệ DSL

*IDSL (ISDN DSL):*Công nghệ đường dây thuê bao số truy nhập mạng ISDN sử dụng các kênh đối xứng BRI (128 Kb/s hoặc 144 Kb/s) kết hợp thành một kênh truyền dữ liệu giữa bộ định tuyến và máy tính của khách hàng. DSL làm việc với tốc độ 160 Kb/s tương ứng với 2B+D (144 Kb/s). Để truyền dẫn song công, sử dụng kỹ thuật triệt tiếng vọng. Phần lớn các dạng IDSL làm việc với ISDN NT tiêu chuẩn ở đầu cuối khách hàng của đường dây. Do đó, IDSL chuyển mạch nội hạt ISDN được thay thế bởi bộ định tuyến gói. Cấu hình này được sử dụng cho truy nhập Internet.

HDSL (High Data Rate DSL): Có khả năng truyền tải hai hướng 1,544 Mbps hoặc 2,048 Mbps trên đường dây điện thoại. HDSL truyền dẫn tin cậy tỷ lệ lỗi bit từ 10^{-9} đến 10^{-10}. Hệ thống HDSL DS-1 (1,544 Mbps) sử dụng hai đôi dây, mỗi đôi dây truyền 768 Kb/s trên mỗi hướng. HDSL E1 (2,048 Mbps) có thể lựa chọn sử dụng hai hoặc 3 đôi dây, mỗi đôi dây sử dụng hoàn toàn song công. HDSL 2,048 Mbps 3 đôi dây sử dụng bộ thu phát giống bộ thu phát hệ thống 1,544 Mbps. Mạch vòng HDSL 2,048 Mbps có thể có mạch rẽ nhưng không cân bằng. Tiêu chuẩn HDSL2 có tốc độ bit và độ dài mạch vòng như HDSL thế hệ thứ nhất chỉ khác là sử dụng 1 đôi dây thay vì 2 đôi dây. HDSL2 có kỹ thuật mã hoá cao và điều chế phức tạp hơn. Lựa chọn tần số phát và thu cho HDSL2 để chống xuyên âm. *SDSL (Single Pair DSL)*: Truyền đối xứng tốc độ 784 Kb/s trên một đôi dây, ghép kênh thoại và số liệu trên cùng một đường dây, sử dụng mã 2B1Q. Công nghệ này chưa có các tiêu chuẩn thống nhất nên không được phổ biến cho các dịch vụ tốc độ cao. SDSL mới chỉ ứng dụng truy cập trang Web, tải dữ liệu và thoại với tốc độ 128 Kb/s, khoảng cách nhỏ hơn 6,7 Km và tốc độ tối đa là 1024 Kb/s trong khoảng 3,5 Km.

VDSL (Very High Data Rate DSL): Sử dụng mạch vòng từ tổng đài trung tâm đến khách hàng và các bộ ghép kênh phân phối. Tiêu chuẩn kỹ thuật VDSL được phát triển từ nhóm T1E1.4 mô tả các tốc độ và khoảng cách từ đơn vị mạng quang ONU tới thuê bao. Cáp từ mạng cho tới các ONU có thể được nối trực tiếp đến ONU, theo hình tròn hoặc là bộ tách quang thụ động. Tính năng và ứng dụng của VDSLlà hỗ trợ đồng thời tất cả những ứng dụng thoại, dữ liệu và video. Đặc biêt VDSL hỗ trợ truyền hình có độ phân giải cao (HDTV) và các ứng dụng máy tính tiên tiến. Tính đối xứng của VDSL cung cấp tốc độ dữ liệu 2 chiều lên tới 26 Mbps cho các khu vực không có cáp quang nối tới.

Công nghệ	Tốc độ	Khoảng cách Truyền dẫn	Số đôi dây đồng sử dụng
IDSL	144 Kb/s đối xứng	5km	1 đôi
HDSL	1,544Mb/s đối xứng 2,048Mb/s đối xứng	3,6 km – 4,5 km	2 đôi 3 đôi
HDSL2	1,544Mb/s đối xứng 2,048 Mb/s đối xứng	3,6 km – 4,5 km	1 đôi
SDSL	768kb/s đối xứng 1,544Mb/s hoặc 2,048 Mb/s một chiều	7 km 3 km	1 đôi
ADSL	1,5- 8 Mb/s đường xuống 1,544 Mb/s đường lên	≤ 5km	1 đôi
VDSL	26 Mb/s đối xứng 13–52 Mb/s đường xuống 1,5-2,3 Mb/s đường lên	300 m – 1,5 km (tuỳ tốc độ)	1 đôi

Hình 6.1: So sánh một số tính năng trong họ công nghệ xDSL

ADSL (Asymmetric Digital Subscriber Line): ADSL là công nghệ đường dây thuê bao số bất đối xứng được phát triển cho nhu cầu truy nhập Internet tốc độ cao, các dịch vụ trực tuyến, video,... ADSL cung cấp tốc độ truyền tới 8 Mb/s đường xuống (Download) và 16 - 640 Kb/s đường lên (Upload). Ưu điểm nổi bật của ADSL là cho phép người sử dụng sử dụng đồng thời một đường dây thoại cho cả 2 dịch vụ thoại và số liệu, vì ADSL truyền ở miền tần số cao (4400 Hz÷1,1MHz) không ảnh hưởng tới tín hiệu thoại. Các bộ lọc được đặt ở hai đầu mạch vòng tách tín hiệu thoại và số liệu theo mỗi hướng. ADSL "Lite" hay ADSL không sử dụng bộ lọc chủ yếu cho ứng dụng truy cập Internet tốc độ cao. Kỹ thuật này không đòi hỏi bộ lọc phía thuê bao nên giá thành thiết bị và chi phí lắp đặt giảm đi tuy nhiên tốc độ đường xuống chỉ còn 1,5 Mb/s.

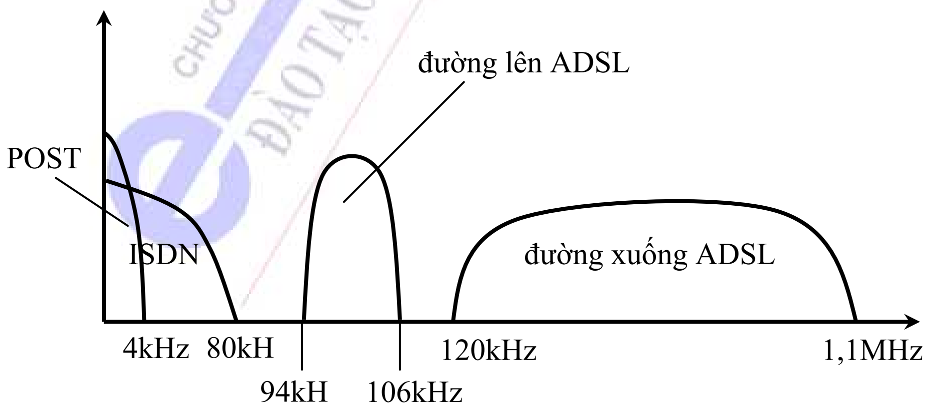
ADSL2 và ADSL2$^+$: ADSL2 được chuẩn hoá trong ITU G.992.3, G.992.4, ADSL2+ được chuẩn hóa trong ITU-T G.925.5 là thế hệ thứ ba của ADSL, phát triển dựa trên nền tảng ADSL và ADSL2 nên mang đầy đủ đặc trưng của ADSL và ADSL2. ADSL2 và ADSL2+ bổ sung nhiều tính năng mới cho các ứng dụng, dịch vụ và tiến trình triển khai mới so với ADSL chuẩn. Công nghệ ADSL2+ đáp ứng các yêu cầu tốc độ cao, băng thông rộng vì nó hỗ trợ được tốc độ truyền số liệu lên 1,2 Mbps và tốc độ xuống 24 Mbps.

6.1.3. Các vấn đề cơ bản công nghệ DSL trên mạng cáp đồng

Phân chia tần số: Phổ tần cáp đồng từ 0 đến 1,1 Mhz được chia thành các khoảng tần số để sử dụng cho các dịch vụ như sau:

- Từ 0 kHz đến 4 kHz: dùng cho điện thoại và các dịch vụ dữ liệu băng tần thấp.
- Từ 0 kHz đến 80 kHz: khoảng tần số dùng cho ISDN.
- Từ 80 kHz đến 94 kHz: đảm bảo sự an toàn phổ tấn thoại và đường lên của ADSL.
- Từ 94 kHz đến 106 kHz: khoảng tần số dùng cho đường lên của ADSL.
- Từ 106 kHz đến 120 kHz: an toàn phổ tần đường lên và xuống của ADSL.
- Từ 120 kHz đến 1,1 MHz: khoảng tần số dùng cho đường xuống của ADSL.

Việc phân tách phổ tần giữa thoại và ADSL cũng như giữa đường xuống và đường lên của ADSL được thực hiện nhờ bộ lọc Spilitter (bộ lọc này ngăn cản cả dòng DC không cho vào modem ADSL).



Hình 6.2 : Phân chia tần số

6.1.4. Các phương pháp mã hóa đường truyền

Phương pháp mã hóa đường dây CAP và DMT sử dụng kỹ thuật điều chế biên độ cầu phương (QAM) là kỹ thuật điều chế kết hợp cả điều chế pha và điều chế biên độ. Một ký hiệu được biểu diễn bằng một điểm của chòm sao. Có các kiểu mã hóa QAM: 4-QAM, 16-QAM, 64-QAM... Số 4,16,64… là số trạng thái mã hóa. Số trạng thái càng nhiều trên mỗi ký hiệu QAM thì tín hiệu càng yếu đi, dẫn đến tỷ số tín hiệu trên tạp âm phải cao để Modem thu có thể phân biệt được tín hiệu từ tạp âm. Khi chòm sao QAM trở nên càng ngày càng lớn thì phải tăng công suất hay giảm nhiễu.

ADSL sử dụng mã đường truyền DMT vì nó được định nghĩa trong ANSI T1.413 và G.992.1. Tuy nhiên, CAP vẫn được một số hãng phát triển áp dụng cho ADSL. Việt Nam khuyến nghị sử dụng phương pháp điều chế DMT.

- Phương pháp điều chế biên độ và pha triệt sóng mang CAP dựa trên kỹ thuật điều chế biên độ cầu phương QAM. Ưu điểm của nó là không có kênh con nên thực thi đơn giản hơn DMT. CAP thích ứng được việc tốc độ khi thay đổi kích cỡ chòm sao mã hoá (4-CAP, 64-CAP, 512-CAP, ...) hoặc là khi tăng hoặc giảm phổ tần sử dụng. Nhược điểm của phương pháp này là không có sóng mang nên năng lượng suy giảm nhanh trên đường truyền và tín hiệu thu chỉ biết biên độ mà không biết đến pha, do đó đầu thu phải có bộ thực hiện chức năng quay nhằm xác định chính xác điểm tín hiệu.

- Phương pháp đa âm tần rời rạc DMT hỗ trợ kiến trúc ghép kênh phân chia theo tần số lẫn triệt tiếng vọng. Sử dụng các phổ tần chồng lấn để có được tốc độ dữ liệu cao hơn nhưng phức tạp và chi phí cũng cao hơn vì cần có bộ sai động để triệt tiếng vọng. Kỹ thuật DMT đã lợi dụng kỹ thuật xử lý tín hiệu số, căn cứ đặc tính mạch điện tự thích ứng điều chỉnh những tham số này, làm cho lỗi bit và xuyên âm nhỏ nhất và dung lượng thông tin ở bất cứ mạch nào cũng lớn nhất. Nguyên lý cơ bản của DMT là chia độ rộng băng tần có thể sử dụng (1104 KHz) thành các kênh con (Subcarrier) và căn cứ vào các đặc tính của kênh t, phân phối dữ liệu đầu vào cho mỗi kênh con. Nếu một kênh con không thể chịu tải số liệu sẽ đóng lại. Mỗi kênh con có thể truyền số liệu 1 đến 15 bit thông tin trong một đơn vị mã.

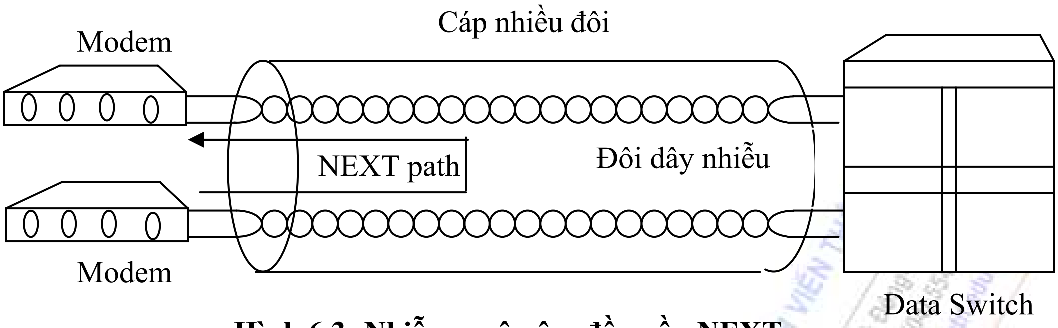
6.1.5. Phát hiện lỗi và sửa lỗi

ADSL sử dụng mã Reed Solomon và Trellis luôn làm việc trong chế độ sửa lỗi. ATM (mã HEC) sử dụng phương pháp sửa lỗi và sẽ chuyển sang phương thức phát hiện lỗi khi có lỗi xảy ra. Sự lựa chọn phương thức sửa lỗi hoặc phát hiện lỗi là thống nhất.

Một số cơ chế mã hoá có thể chuyển đổi từ phương thức phát hiện lỗi ngay khi các lỗi được phát hiện. Khối FEC có tác dụng giúp bên thu có thể thu đúng thông tin, thực hiện bằng cách thêm các byte kiểm tra FCS, công suất 3 dB với tỷ lệ lỗi bit là 10^{-7}.

6.1.6. Nhiễu và chống xuyên nhiễu

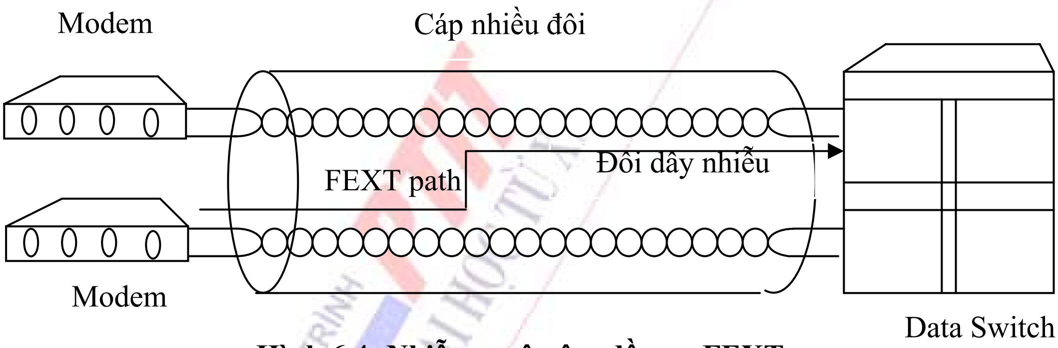
Nhiễu xuyên âm đầu gần NEXT (Near - end Crosstalk): Xuất hiện ở các bộ thu do nguồn nhiễu từ các bộ phát cùng đầu cáp với nó gây ra. Loại nhiễu này là đáng kể nhất. Nhiễu NEXT gây suy giảm cho hệ thống sử dụng cùng băng tần số cho truyền dẫn thu và phát.



Hình 6.3: Nhiễu xuyên âm đầu gần NEXT

Để tránh xuyên âm đầu gần NEXT, hệ thống truyền dẫn có thể sử dụng các dải tần số cho thu và phát khác nhau. Hệ thống ghép kênh theo tần số FDM loại bỏ được NEXT từ các hệ thống giống nhau. Xem xét một tín hiệu V truyền dọc theo một đôi dây, tại khoảng x1dọc theo đôi dây có nhiễu tác động do không cân bằng và truyền trở lại đầu thu như trong H.6.3

Nhiễu xuyên âm đầu xa FEXT (Far - end- Crosstalk): Xuất hiện ở bộ thu đặt ở đầu kia của cáp, khác với đầu phát ra nguồn nhiễu. FEXT thường nhỏ hơn nhiều so với nhiễu xuyên âm đầu gần NEXT vì tín hiệu từ đầu xa bị suy hao khi nó chạy trên mạch vòng thuê bao. FEXT thu được cũng sử dụng phương pháp tương tự như khi sử dụng phương pháp thu NEXT. Hình 6.4 trình bày một ví dụ của FEXT từ một điểm không cân bằng x1.



Hình 6.4: Nhiễu xuyên âm đầu xa FEXT

Nhiễu xuyên âm đầu gần cũng như đầu xa thì công suất của nhiễu phụ thuộc vào phổ của tín hiệu nhiễu. Thông thường người ta chỉ quan tâm đến công suất nhiễu xuyên âm mà không cần quan tâm đến mức điện áp của nhiễu xuyên âm. Vì theo thống kê thì hầu như đối với các mô hình của công suất nhiễu xuyên âm đã có thể cho phép xác định tỷ số tín hiệu trên tạp âm SNR trên đôi dây, còn đối với mô hình mức điện áp thì rất khó xác định.

Chống xuyên nhiễu: Năng lượng điện truyền trên mỗi đôi dây tạo ra một từ trường bao bọc quanh đôi dây gây ra tín hiệu điện, cảm ứng sang các đôi dây xung quanh, gọi là nhiễu xuyên âm. ADSL khắc phục bằng cách giảm tốc độ bit hướng lên, sử dụng dải tần số thấp hơn tần số nơi suy hao truyền dẫn nhỏ và nhiễu xuyên âm nhỏ nhất.

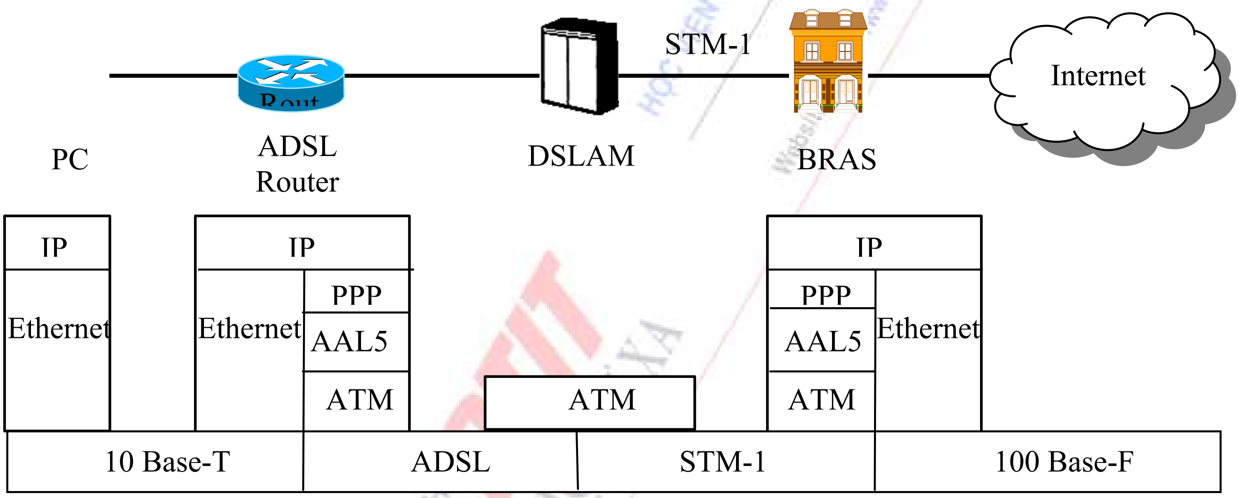
Phương pháp triệt tiếng vọng (EC): Tiếng vọng là sự phản xạ của tín hiệu phát vào bộ thu đầu gần. Tiếng vọng đáng ngại là vì các tín hiệu đi theo cả 2 hướng của truyền dẫn số và cùng tồn tại đồng thời trên các đường truyền dẫn đôi dây xoắn. Do vậy tiếng vọng là tạp âm không mong muốn. Tiếng vọng là một phiên bản bị lọt ra của tín hiệu phát. Bộ triệt tiêu tiếng vọng tạo ra một bản sao của tín hiệu phát bị lọt ra và loại bỏ nó ra khỏi tín hiệu nhận.

Sử dụng một kênh duy nhất cho cả phát và thu nên chỉ cần có một bộ triệt tiếng vọng phía thu. ADSL sử dụng kỹ thuật truyền dẫn triệt tiếng vọng EC, nơi dải tần phát được đặt trong dải tần thu bằng cách chồng dải tần, tổng băng tần truyền có thể giảm. Tuy nhiên, EC khó tránh được tự xuyên nhiễu . Song công triệt tiếng vọng đạt được tốc độ truyền dữ liệu của song công 4 dây trên 1 đôi dây xoắn. Triệt tiếng vọng là dạng phổ biến nhất của ghép kênh trong ADSL.

6.1.7. Các mô hình kết nối ADSL

Kết nối ADSL được thiết lập giữa Modem và tổng đài, các đường truyền kết nối từ DSLAM – BRAS – tới nhà cung cấp dịch vụ ISP cũng phải được cung cấp các kết nối tốc độ cao như STM, ATM hoặc chuyển mạch IP.

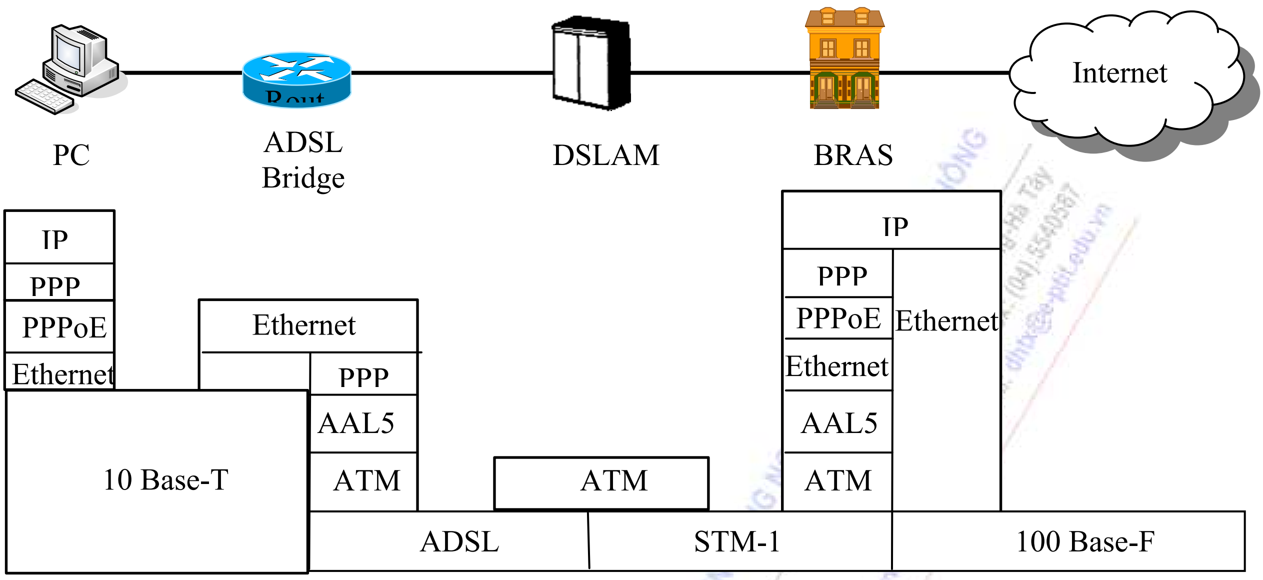
*** Mô hình PPPoA (Point to Point over ATM)**



Hình 6.5 PPPoA : Giao thức nối điểm qua ATM

Mô hình này được dùng trong các thiết bị: Internal ADSL Modem, USB Modem hay ADSL Router (RFC 2364)

*** Mô hình PPPoE (Point to Point over Ethernet) RFC 2516**



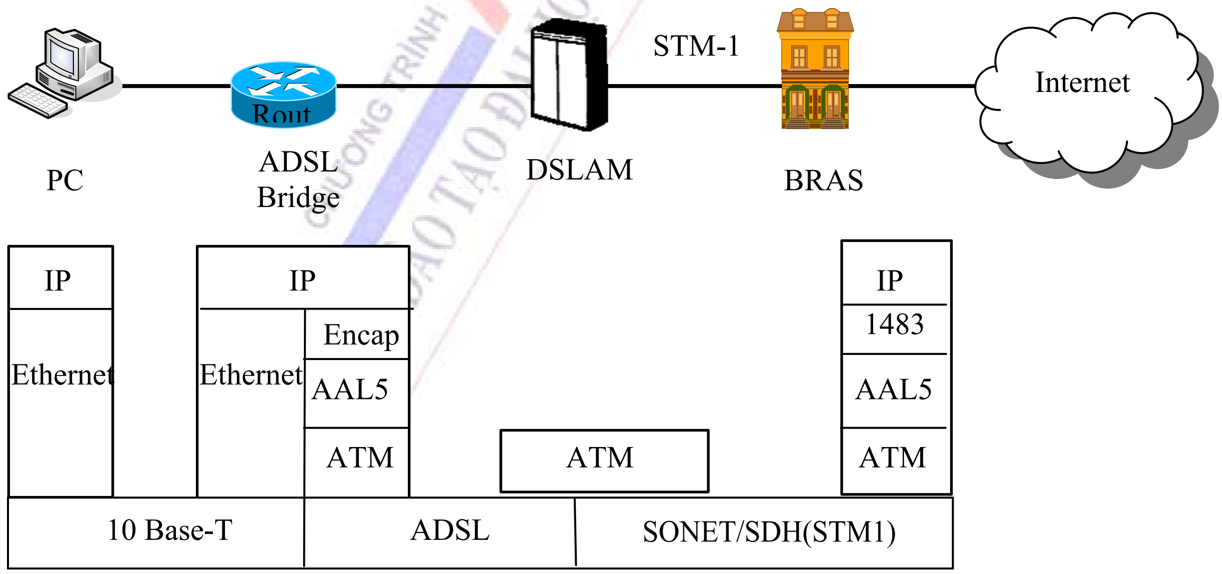
Hình 6.6 PPPoE - Giao thức nối điểm qua Ethernet

PPPoE yêu cầu hầu hết các giao thức đóng khung:

- PPP trên PC để bảo an kết nối từ PC đến bộ định tuyến của ISP.
- PPPoE kết nối từ PC đến modem.
- RFC 1483 kết nối từ modem đến bộ định tuyến của ISP.

*** Mô hình IP over ATM (RFC 1483R)**

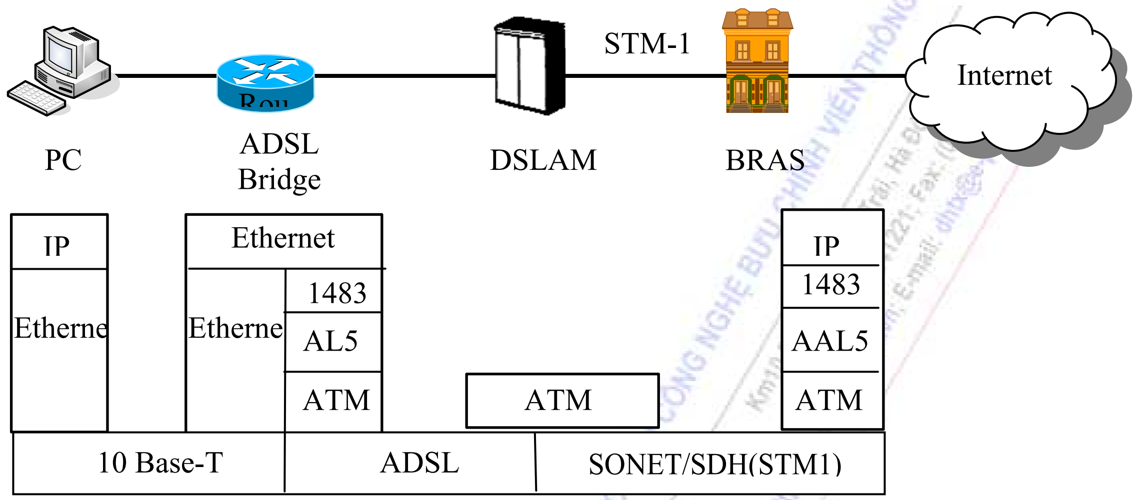
Được xác định trong RFC 1483R. Tiêu chuẩn này hỗ trợ giao thức định hướng (giống IP) và giao thức không định hướng (giống Ethernet). Nó cũng có kết hợp tùy chọn cho VC Multiplexing và LLC Multiplexing.



Hình 6.7 Mô hình IP over ATM (RFC 1483R)

*** Mô hình Ethernet over ATM (RFC 1483B)**

Tiêu chuẩn đa giao thức kết hợp mức đáp ứng AAL5. Tiêu chuẩn này hỗ trợ giao thức định hướng (giống IP) và giao thức không định hướng (giống Ethernet). Nó cũng có kết hợp tùy chọn cho VC Multiplexing và LLC Multiplexing.



Hình 6.8 Mô hình IP over ATM (RFC 1483R)

RFC 1483 (Bridged) sử dụng trong Modem ADSL ngoài với giao thức tạo khung RFC 1483. Hiện nay được triển khai trong các sản phẩm của SBC và Pac Bell .

6.1.8. Các ứng dụng của ADSL

Truy nhập Internet tốc độ cao: Với tốc độ truyền bất đối xứng nên ADSL là công nghệ lý tưởng cho truy nhập Internet tốc độ cao, bởi lẽ nhu cầu tải thông tin từ Internet về lớn hơn rất nhiều so với nhu cầu tải tin đi.

Truyền hình theo yêu cầu (VoD): Truyền hình theo yêu cầu sử dụng các phương pháp nén, số hóa tín hiệu âm thanh, hình ảnh để truyền đi qua mạng. Các nhà cung cấp dịch vụ VoD có thể cung cấp các kênh truyền hình theo yêu cầu với chất lượng khác nhau tùy theo yêu cầu sử dụng. Các kênh truyền hình chuẩn (SDTV) yêu cầu tốc độ truyền là 3-4Mbps. Các kênh truyền hình độ trung thực cao (HDTV) yêu cầu tốc độ truyền là 15-18 Mbps. Như vậy, dịch vụ ADSL với tốc độ hướng xuống tối đa 8 Mbps thì chỉ có thể hỗ trợ tối đa 2 kênh SDTV và không thể hỗ trợ được HDTV, ADSL2+ sẽ hỗ trợ được dịch vụ này.

Hội nghị từ xa: Cho phép nhiều người ở các địa điểm khác nhau có thể hội họp, trao đổi trực tiếp như đang trong cùng một phòng họp. Tăng hiệu quả công việc, tiết kiệm thời gian và chi phí do giảm thiểu việc di chuyển, cũng như công tác tổ chức hội họp.

Truyền hình và phát thanh qua mạng: Các kênh truyền hình và phát thanh từ đài truyền hình và đài phát thanh có thể được truyền hình trực tiếp trên mạng ADSL2+ đến người sử dụng. Vì tín hiệu Video và Audio chỉ chiếm một phần băng thông của đường dây, nên người sử dụng vừa xem video vừa có thể duyệt Web.

Một số các dịch vụ khác: Các dịch vụ có thể triển khai trên công nghệ ADSL như: Truyền số liệu tốc độ cao, học từ xa, game trực tuyến, khám bệnh từ xa, làm việc tại nhà, mua bán hàng qua mạng và các hoạt động giao dịch khác...

Hiện nay, công nghệ đường dây thuê bao số DSL đã được ứng dụng rộng rãI, đáp ứng mọi nhu cầu về các dịch vụ băng rộng trên mạng cáp đồng sẵn có. Với ưu điểm về phương thức truyền cũng như phương pháp mã hoá, sửa lỗi, ADSL rất phù hợp với các dịch vụ Internet tốc độ cao, đưa lại nhiều lợi ích cho người sử dụng cũng như nhà cung cấp dịch vụ.

6.2. Truyền thoại qua mạng chuyển mạch gói VoPN (Voice over Packet Network)

6.2.1. Khái niệm

Là mô hình truyền thoại thời gian thực không sử dụng hệ thống chuyển mạch kênh thông thường mà sử dụng các mạng chuyển mạch gói. Tín hiệu thoại tương tự sau khi được số hóa sẽ được truyền qua mạng chuyển mạch gói dưới dạng các gói dữ liệu.

VoPN đang trở thành một trong những công nghệ viễn thông hấp dẫn nhất hiện nay không chỉ đối với các nhà cung cấp dịch vụ mà với cả những người sử dụng dịch vụ. Sự phát triển của các mạng chuyển mạch gói và đặc biệt là mạng Internet với giao thức IP đã tạo ra nền tảng phát triển các giao thức cho phép truyền dữ liệu thoại qua các mạng số liệu khác nhau. Các mạng chuyển mạch gói thường được sử dụng để truyền thoại là mạng Frame Relay, mạng ATM và mạng IP.

6.2.2. Mô hình truyền thoại qua mạng chuyển mạch gói

Tại phía phát, tín hiệu thoại tương tự từ máy điện thoại hay micro sẽ được số hóa và chuyển đổi thành các gói dữ liệu thích hợp để truyền qua mạng, việc chuyển đổi sẽ được thực hiện thông qua các bộ mã hóa-giải mã CODEC (Coder-Decoder). Bộ xử lý tín hiệu số DSP (Digital Signal Processing) sẽ nén các gói dữ liệu này với tốc độ bit thích hợp để truyền qua mạng chuyển mạch gói.

Tại bên thu, các tiến trình diễn ra ngược lại, khi nhận được các gói tin đã được nén, các DSP sẽ giải nén các gói tin, sau đó giải mã (Decode) các gói tin thành tín hiệu âm thanh tương tự và phát ra điện thoại hoặc loa cho người nghe.

Trong một cuộc đàm thoại, các khoảng lặng chiếm tỉ lệ rất lớn (30% - 40%), khi truyền thoại qua mạng chuyển mạch gói người ta sử dụng kỹ thuật VAD (Voice Activity Detection) để loại bỏ các khoảng lặng nhằm giảm lượng gói tin truyền qua mạng. Tại phía thu các khoảng lặng lại được tái tạo để phát thông tin thoại cho người nghe.

6.2.3. Ưu điểm của truyền thoại qua mạng chuyển mạch gói

- Tiết kiệm chi phí đầu tư hạ tầng mạng và chi phí sử dụng dịch vụ: Việc tiết kiệm chi phí hạ tầng mạng ở đây được hiểu theo nghĩa sử dụng các mạng chuyển mạch gói đã có sẵn để truyền dữ liệu thoại. Thực tế việc đầu tư một hệ thống mạng chuyển mạch gói sử dụng các công nghệ tiên tiến như mạng ATM cũng rất tốn kém và thường chỉ sử dụng cho mạng đường trục. Do tận dụng được các mạng chuyển mạch gói có sẵn, đặc biệt là mạng Internet để thực hiện các cuộc gọi đường dài có thể tiết kiệm được rất nhiều chi phí cuộc gọi so với việc thực hiện cuộc gọi thông qua mạng chuyển mạch kênh thông thường.

- Sử dụng hiệu quả băng thông với chất lượng dịch vụ QoS chấp nhận được: Trong mạng chuyển mạch kênh, băng thông cấp cho một cuộc liên lạc là cố định (một kênh 64kbps) nhưng khi truyền thoại qua mạng chuyển mạch gói việc phân chia tài nguyên cho các cuộc gọi linh hoạt hơn nhiều. Khi một cuộc liên lạc diễn ra, nếu lưu lượng của mạng thấp, băng thông dành cho liên lạc sẽ cho chất lượng thoại tốt nhất có thể, nếu lưu lượng của mạng cao, mạng sẽ hạn chế băng thông của từng cuộc gọi ở mức chất lượng thoại QoS chấp nhận được nhằm phục vụ được nhiều người nhất.

- Kết hợp các dịch vụ thoại, số liệu, video trên một mạng duy nhất: cho phép sử dụng hạ tầng mạng gói đa dịch vụ duy nhất để truyền các loại lưu lượng khác nhau.

6.2.4. Các vấn đề về chất lượng dịch vụ QoS

Khác với mạng chuyển mạch kênh, trong mạng chuyển mạch gói có rất nhiều các gói tin thuộc các loại dữ liệu khác nhau được lưu chuyển hướng đích trên cùng một kênh truyền. Vì vậy cần phải có cơ chế ưu tiên đối với các dữ liệu thời gian thực như dữ liệu thoại. Ngoài ra mạng chuyển mạch gói sử dụng cơ chế lưu và chuyển tiếp (Store-and-Forward) để truyền thông tin nên gây trễ tại các nút chuyển mạch.

*** Trễ (Delay):** Trễ là một nhân tố ảnh hưởng đến chất lượng thoại. Mỗi hệ thống truyền thông chỉ cho phép một giới hạn trễ nhất định. Thời gian trễ có thể chấp nhận được trong khoảng từ 200ms đến 400ms. Chất lượng cuộc gọi tốt thì thời gian trễ yêu cầu không quá 200ms. Yêu cầu giảm trễ là rất cần thiết trong hệ thống VoPN để có thể nâng cao chất lượng dịch vụ. Nguyên nhân gây trễ khi truyền thoại qua mạng chuyển mạch gói có thể do:

- Trễ tích lũy hay trễ thuật toán: là trễ do chờ đủ khung dữ liệu để xử lý ở các bộ mã hóa.

- Trễ xử lý: thời gian mã hóa và đóng gói dữ liệu đã mã hóa để truyền qua mạng

- Trễ truyền qua mạng: trễ truyền dữ liệu qua mạng chuyển mạch gói hoặc do các bộ đệm chống Jitter ở phía thu.

Để giảm thiểu trễ, phải tăng tốc độ mạng, năng lực của các bộ xử lý, mã hóa, ngoài ra cần sử dụng các bộ triệt tiếng vọng Echo Canceller.

*** Trượt (Jitter):** Trượt là sự chênh lệch thời gian đến của các gói tin theo các đường khác nhau từ nguồn đến đích gây ra. Để có thể tái tạo tiếng nói một cách chính xác và trung thực bên thu cần phải loại bỏ Jitter bằng cách sử dụng bộ đệm (Buffer), các gói sau khi nhận sẽ được lưu trong bộ đệm và sẽ được xử lý lần lượt. Dùng bộ đệm sẽ tránh được những thời gian trễ lớn của các gói tin, nhưng làm tăng thời gian trễ trong hệ thống. Thời gian trượt càng lớn thì dung lượng của bộ đệm càng lớn. Bộ đệm càng lớn thì thời gian trễ gây ra càng tăng. Vì vậy việc tính toán dung lượng của bộ đệm thích hợp đối với từng hệ thống là rất cần thiết sao cho tránh được trượt mà thời gian trễ không làm giảm chất lượng của hệ thống.

*** Mất gói (Packet Loss):** Không thể đảm bảo tất cả các gói tin đều đến đích an toàn và đúng thứ tự, nhất là trong mạng IP. Các gói tin có thể bị mất khi mạng bị quá tải hay trong trường hợp nghẽn mạng hoặc do đường kết nối không đảm bảo. Yêu cầu chất lượng dịch vụ tỉ lệ mất gói là nhỏ hơn 10%. Do hạn chế của thời gian trễ nên các giao thức vận chuyển không liên kết giải quyết vấn đề này. Để duy trì chất lượng thoại ở mức chấp nhận được hoặc truyền lại các gói tin bị mất, hoặc thay thế các gói tin mất bằng các khoảng im lặng. Để nâng cao độ tin cậy của đường truyền cần tăng tốc độ kênh truyền, tăng dung lượng hệ thống thiết bị truyền dẫn (sử dụng các mạng tiên tiến như mạng Frame Relay, ATM).

6.2.5. Voice over Frame Relay - VoFR

Các chuẩn VoFR trong Frame Relay Forum FRF, năm 1998: FRF.11 định nghĩa định dạng các khung, FRF.12 định nghĩa quá trình phân mảnh các gói tin (tạo ra các gói tin nhỏ hơn để truyền dữ liệu thoại thời gian thực qua mạng). Các khung dữ liệu trong mạng Frame Relay có kích thước Header nhỏ 2 byte. VoFR thường được sử dụng trong các mạng riêng hoặc mạng riêng ảo VPN kết hợp thoại và số liệu. Việc sử dụng mạng Frame Relay để truyền thoại giúp giảm giá thành. Trong VoFR, các tổng đài PBX được kết nối với nhau thông qua các Permanent Virtual Circuit (PVCs). Trong đó tốc độ kết nối của các kênh trong mạng Frame Relay có thể dễ dàng thay đổi để thích ứng truyền thoại, fax hay số liệu. Khi truyền thoại trong mạng Frame Relay, các gói dữ liệu thoại sẽ được ưu tiên hơn so với các gói dữ liệu khác.

6.2.6. Voice over ATM - VoATM

Phương thức truyền không đồng bộ ATM (Asynchronous Transfer Mode) là công nghệ đa dịch vụ, có thể truyền đồng thời thoai, dữ liệu và video với tốc độ và độ tin cậy cao. Giá thành các hệ thống ATM đắt và chỉ được sử dụng ở một số mạng yêu cầu tốc độ, như mạng đường trục Backbone. Các chuẩn VoATM được định nghĩa bởi ATM Forum và ITU_T.

Giao thức dịch vụ tốc độ bit cố định CBR (Constant Bit Rate) của AAL1 là chuẩn truyền thoại qua ATM. Tuy nhiên giao thức này không hiệu quả đối với các ứng dụng thoại. Dịch vụ mô phỏng kênh CES (Circuit Emulation Service) có chất lượng dịch vụ cao nhất, cung cấp truyền một dòng liên tục các bit thông tin, cấp một lượng không đổi băng thông cho một kết nối trong thời gian truyền. Nhưng CES chiếm băng thông cho các ứng dụng khác. Ngoài ra, nhằm giảm trễ, CES gửi các ATM Cell trống không đợi thêm 6 ms để lấp đầy 47 byte dữ liệu thoại vào Cell. Điều này làm lãng phí băng thông khoảng 20 bytes trên một ATM Cell. Dịch vụ mô phỏng kênh băng thông động DBCES là một biến thể của CES, DBCES không gửi một dòng bit cố định các Cell mà chỉ truyền khi có cuộc thoại hoạt động (Off Hook). Cũng như CES, một phần của Cell rỗng. Do đó sử dụng AAL1 để truyền thoại qua ATM tăng phần tiêu đề dữ liệu thoại và lãng phí băng thông.

Dịch vụ tốc độ bit biến đổi VBR của AAL2 trong khuyến nghị I.363.2 của ITU_T, cho phép đóng gói các gói ngắn từ 1Byte đến 45-64 Bytes, gọi là các Minicells, thành một hoặc nhiều ATM Cell. Khác với AAL1, AAL2 cho phép các Cell có Payload khác thay đổi. AAL2 hỗ trợ nén thoại và nén khoảng lặng và cho phép nhiều kênh thoại có băng thông khác nhau trên một kết nối ATM đơn.

Trong mạng thuần ATM, việc nén thoại là không cần thiết, do băng thông rất lớn. Tuy nhiên trong các mạng ATM-Frame Relay, việc nén thoại là cần thiết vì Frame Relay có nén thoại. Khi truyền thoại qua mạng ATM, các Permanent Virtual Circuit được dùng để truyền thoại và báo hiệu. Các bản tin báo hiệu sẽ được truyền một cách trong suốt trên các Signaling PVCs. Việc kết hợp giữa các hệ thống cuối cho phép chọn ra một PVC để truyền thoại giữa các trạm kết cuối. Trong mô hình dịch báo hiệu VoATM, ATM dịch báo hiệu từ cả các thiết bị mạng ATM và Non-ATM

Do giá thành của một mạng ATM rất cao nên thường chỉ được dùng cho mạng Backbone hoặc nhà cung cấp dịch vụ

6.2.7. Voice over Internet Protocol - VoIP

VoIP là mô hình truyền thoại sử dụng giao thức IP Internet Protocol. VoIP là một công nghệ hấp dẫn nhất hiện nay. Các chuẩn giao thức của VoIP được đưa ra bởi ITU_T (International

Telecomunication Union), ITMC (International Multimedia Telecommunications Consortium) và IETF (Internet Engineering Task Force).

*** Các thành phần chủ yếu của VoIP gồm có:**

- Internet Protocol IP: Định danh địa chỉ các thiết bị và định tuyến các gói tin lưu chuyển mạng. Các gói IP có phần Header 20 Bytes.

- Các chuẩn nén tín hiệu thoại : Chuyển đổi tín hiệu Analog - Digital và nén tín hiệu.

- Chuẩn H.323 hoặc SIP: Thiết lập cuộc gọi

- Real Time Transport Protocol (RTP): Quản lý các kết nối End to End để giảm thiểu mất gói và trễ.

7	Application	Các ứng dụng
6	Presentation	CODECS
5	Session	H323 hoặc SIP
4	Transport	UDP, TCP, RTP
3	Network	IP
2	Data link	ATM,FR,PPP Ethernet
1	Physical	

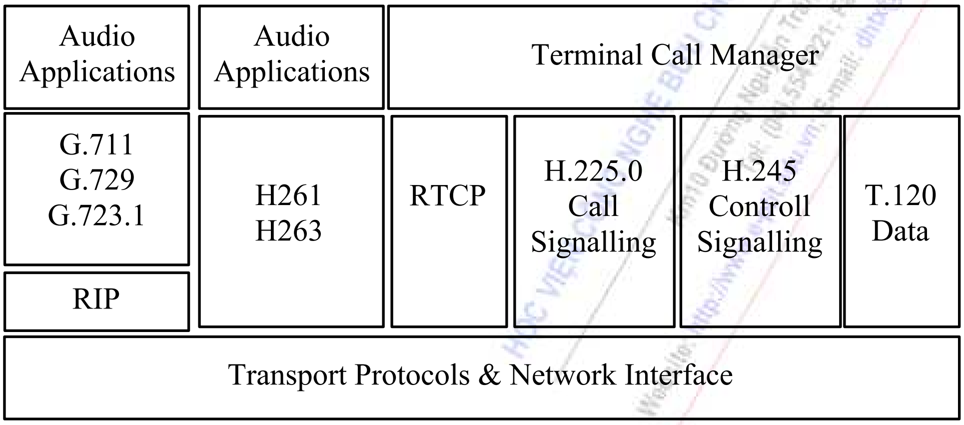
Hình 6.9 Mô hình Voice over Internet Protocol

Các phần tử H.323 bao gồm: Các Gateway, các bộ kiểm soát cổng Gatekeeper và các khối điều khiển đa điểm MCU (Multipoint Control Unit). Các thiết bị đầu cuối hỗ trợ cho hội nghị điểm-điểm và hội nghị đa điểm với nhiều thành phần audio, video, data phối hợp tham gia. Các Gateway liên kết mạng PSTN hoặc ISDN phục vụ cho các điểm cuối thuộc hai mạng làm việc với nhau. Các Gatekeeper cung cấp các dịch vụ như điều khiển tiếp nhận, thông dịch địa chỉ cho các đầu cuối hoặc cho Gateway. Các MCU cho phép các thiết bị đầu cuối hay các Gateway thiết lập hội nghị trên các phiên audio, video và data.

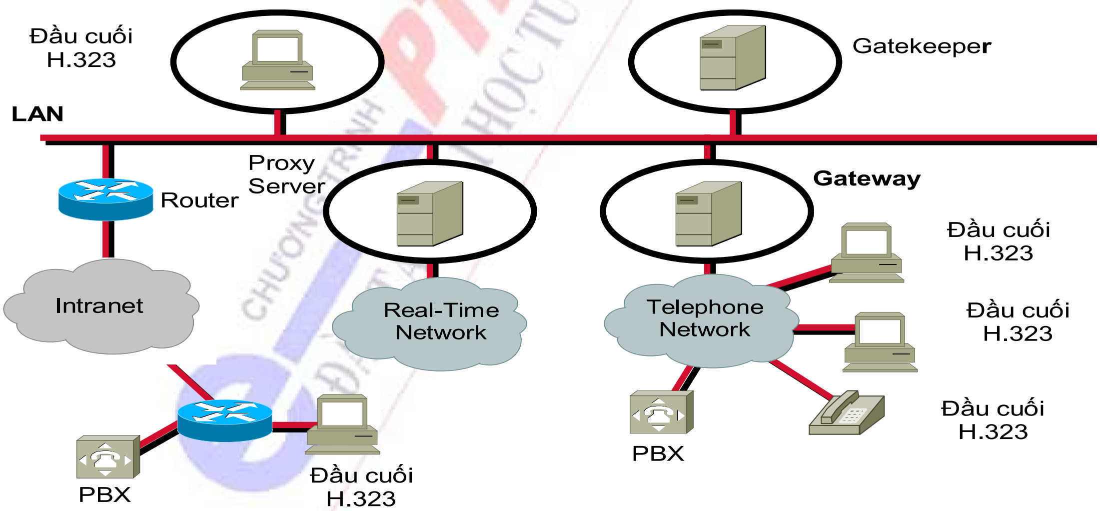
H.323 là một tập các giao thức và thủ tục cung cấp các dịch vụ truyền thông đa phương tiện - truyền thoại, hình ảnh và dữ liệu thời gian thực qua mạng chuyển mạch gói bao gồm mạng IP-based LAN, MAN, WAN… do Hiệp hội viễn thông quốc tế về tiêu chuẩn hoá ITU-T đưa ra. Chuẩn H.323 bao gồm các chức năng như báo hiệu và điều khiển cuộc gọi, vận chuyển và điều khiển đa truyền thông (Multimedia Transport and Control), điều khiển độ rộng băng tần cho hội nghị điểm-điểm và hội nghị đa điểm (Point-to-Point and Multipoint Conferences). Ngoài khuyến nghị H.323, các khuyến nghị thuộc nhóm H (H-Series) còn có: H.320 cho mạng tích hợp số đa dịch vụ ISDN, H.324 cho dịch vụ mạng thoại thông thường POTS (Plain Old Telephone Service) như là các kỹ thuật vận chuyển.

Chuẩn H.323 bao gồm các thành phần và giao thức sau :

Báo hiệu cuộc gọi	H.225
Điều khiển truyền thông	H.245
Mã hoá và giải mã Audio	G.711, G.722, G.723, G.728, G.729
Mã hoá và giải mã Video	H.271, H.263
Chia sẻ dữ liệu	T.120
Giao vận truyền thông	RTP/RTCP



Hình 6.10 Mô hình giao thức H.323



Hình 6.11 Mô hình mạng theo chuẩn H.323

Giao thức SIP (Session Initial Protocol): Giao thức khởi tạo phiên SIP là giao thức điều khiển báo hiệu lớp ứng dụng, thiết lập, duy trì và kết thúc các phiên đa truyền thông bao gồm thoại Internet, các hội nghị và các ứng dụng audio, video và data .. SIP hỗ trợ các phiên điểm - điểm hoặc đa điểm. SIP là giao thức dựa trên kí tự văn bản (Text Based Protocol), kiến trúc đa truyền thông. Các chức năng của SIP độc lập với nhau, có thể giao tiếp, liên kết với các giao thức báo hiệu khác như giao thức H.323 .

Real-time Transport Protocol RTP là một giao thức End to End, thời gian thực như Audio và Video. RTP thực hiện việc quản lý về thời gian truyền, quản lý số hiệu tuần tự, kiểm tra truyền dữ liệu và nhận dạng kiểu dữ liệu được truyền. Nhưng RTP không cung cấp bất cứ một cơ chế nào bảo đảm thời gian truyền và cũng không cung cấp bất cứ một cơ chế nào giám sát chất lượng dịch vụ. Sự giám sát và bảo đảm về thời gian truyền dẫn cũng như chất lượng dịch vụ được thực hiện nhờ hai giao thức là RTCP và RSVP.

Real-time Transport Control Protocol RTCP: Mặc dù RTP là một giao thức độc lập nhưng thường được hỗ trợ bởi giao thức RTCP điều khiển cho phép gửi về các thông tin bên thu và tự thích nghi với bên phát như tự thích nghi kiểu nén tín hiệu và tự điều chỉnh lưu lượng dữ liệu cho phù hợp với bên phát.

Resource Reservation Protocol RSVP: Cung cấp một cơ chế đảm bảo băng thông cho các hoạt động của các ứng dụng. RSVP gửi tham số chất lượng dịch vụ QoS kết hợp với các dữ liệu thời gian thực được truyền trên mạng TCP/IP. Hỗ trợ giao thức RTP, giao thức RSVP có thể giải quyết các lỗi xảy ra trên đường truyền để đảm bảo các tham số chất lượng. Giao thức RTP chỉ hỗ trợ việc truyền thông điểm - điểm và không quản lý các tham số liên kết trên mạng. RSVP không những tác động ở máy phát, máy thu mà còn tác động trên cả các Router trong mạng. RSVP thiết lập và duy trì kết nối duy nhất cho một luồng dữ liệu, xác lập một hệ thống quản lý thứ tự các gói và tạo modun điều khiển để quản lý các nguồn tài nguyên của các nút mạng khác nhau. RSVP đưa ra một mô hình tối ưu để liên kết các dữ liệu từ mộ nguồn tới nhiều đích. RSVP đóng vai trò quản lý một cách độc lập các host đích để tự thích nghi các tham số chất lượng giữa khả năng cung cấp và nhu cầu đáp ứng.

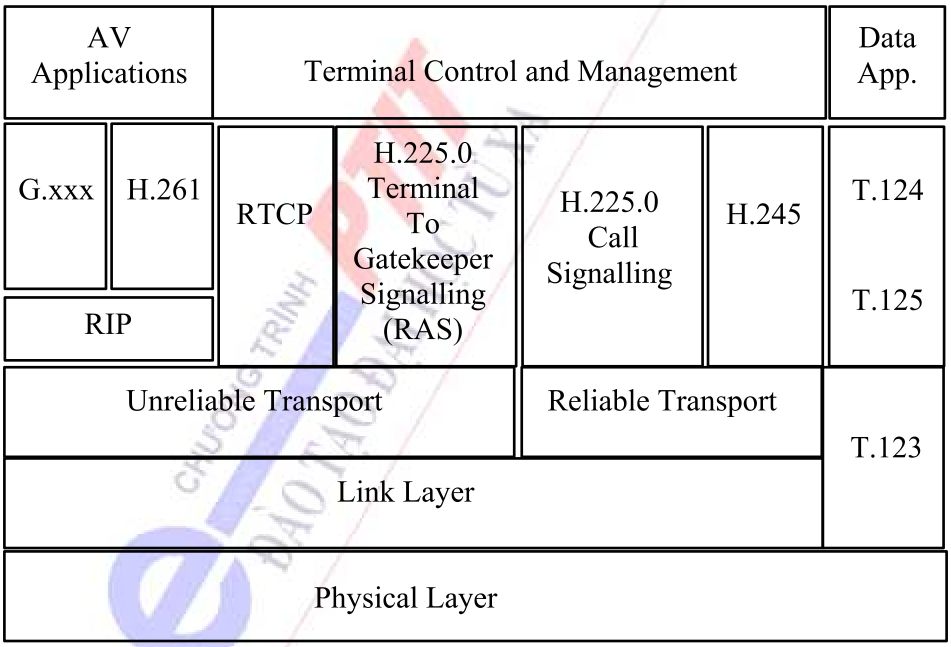
Giao thức MGCP (Media Gateway Control Protocol) cho phép điều khiển các Gateway thông qua các thành phần điều khiển nằm bên ngoài mạng. MGCP sử dụng mô hình kết nối tương tự như SGCP dựa trên các kết nối cơ bản giữa thiết bị đầu cuối và gateway. Các kết nối có thể là kết nối điểm-điểm hoặc kết nối đa điểm. Ngoài các chức năng điều khiển như SGCP, MGCP còn cung cấp thêm các chức năng yêu cầu Gateway xác định kiểu mã hoá ở phía đường dây kết nối đến thiết bị đầu cuối, kiểm tra trạng thái và kết nối ở một thiết bị đầu cuối và thông báo với Call Agent khi nào các thiết bị đầu cuối ngừng sử dụng dịch vụ và khi nào quay lại sử dụng dịch vụ.

Giao thức Megaco/H.248: Kiến trúc chính của Megaco được thể hiện bao gồm hoạt động giữa các hệ thống MG, MGC. Megaco chia các thiết bị có chức năng khác nhau thành phần truyền thông và phần báo hiệu. Trong khi Media Gateway (Cổng giao tiếp truyền thông) điều khiển phần truyền thông thì Media Gateway Controller (Bộ điều khiển cổng giao tiếp truyền thông) hay Call Agents (Các tác nhân gọi) lại điều khiển các MGs để thiết lập các đường dẫn truyền thông thông qua mạng phân tán. Một MGC có thể điều khiển nhiều MGs . Nói một cách khác, một MG có thể đăng ký với nhiều MGCs. Việc trao đổi thông tin giữa hai thiết bị này (MG và MGC) được thực hiện nhờ giao thức Megaco. Vì thế, Megaco là một giao thức chủ/tớ, các tác nhân cuộc gọi hoạt động như các bộ khởi tạo lệnh (máy chủ), còn các MGs hoạt động như các bộ đáp ứng lệnh (máy tớ).

Điều khiển và truyền tải thông tin H.245 mô tả chi tiết cấu trúc và định nghĩa các bản tin, tóm lược những thủ tục điều khiển, thiết lập và giám sát quá trình liên lạc đa phương tiện (dữ liệu và âm thanh) giữa hai điểm cuối. Các bản tin điều khiển H.245 kiểm soát hoạt động của các phần trong mạng H.323 bao gòm khả năng trao đổi, đóng mở kênh logic, yêu cầu chế độ ưu tiên, điều khiển luồng. Các bản tin được truyền trên kênh điều khiển H.245 tương ứng với kênh lôgic 0. Mỗi cuộc gọi chỉ có một kênh điều khiển H.245 được thiết lập chức năng điều khiển đến khi kênh logic 0 được giải phóng. Báo hiệu H.245 được thiết lập giữa hai điểm cuối, có thể là thiết bị đầu cuối, MC, Gateway hoặc Gatekeeper.

Báo hiệu điều khiển cuộc gọi H.225 mô tả phương thức tích hợp dữ liệu, phương thức mã hoá và đóng gói thông tin giữa hai thành phần của mạng H.323. H.225 cũng mô tả các giao thức và định dạng các bản tin cho Gateway H.323 có liên quan đến các thiết bị đầu cuối H.320, H.324 hoặc H.310, H.321 trên các mạng N-ISDN, B-ISDN. Ngoài ra, chuẩn H.225 còn mô tả các giao thức và định dạng các bản tin cho quá trình truyền thông giữa Gateway H.323 và Gateway H.322 cũng như các điểm cuối trong mạng H.322 với sự đảm bảo về chất lượng dịch vụ (QoS).

RTCP: H.225 còn được thiết kế để một Gateway H.323 có khả năng phối hợp hoạt động với các loại thiết bị đầu cuối H.320. Ngoài ra H.225 còn bảo đảm chất lượng dịch vụ của thiết bị đầu cuối H.320 có thể được thay đổi phù hợp với đặc tính và khả năng của Gateway H.323.



Hình 6.12 Mối quan hệ các giao thức trong H323

Báo hiệu đăng ký, chấp nhận và trạng thái RAS: Kênh RAS được sử dụng để truyền các bản tin phục vụ quá trình tìm kiếm Gatekeeper và đăng ký điểm cuối. Các bản tin RAS được truyền trên kênh không được đảm bảo độ tin cậy do đó tất cả các bản tin đều được quy định một khoảng thời gian và một bộ đếm. Khi điểm cuối hoặc Gatekeeper không thể phúc đáp lại yêu cầu trong khoảng thời gian quy định thì có thể sử dụng bản tin RIP (Request in Progress) để chỉ thị rằng yêu cầu vẫn đang được xử lý. Điểm cuối hoặc Gatekeeper nhận được bản tin RIP sẽ đặt lại đồng hồ và bộ đếm.

RAS còn được sử dụng để truyền các bản tin về quá trình chấp nhận, thay đổi độ rộng băng tần, cung cấp thông tin trạng thái. Các bản tin này được trao đổi giữa Gatekeeper và điểm cuối để cung cấp các chức năng điều khiển truy nhập và quản lý băng tần. Điểm cuối gửi bản tin ARQ (Admission Request) đến Gatekeeper bao gồm cả các thông tin về độ rộng băng tần yêu cầu. Đó là tốc độ giới hạn trên cho các luồng tín hiệu phát và thu bao gồm cả kênh Audio kênh Video và các Header như RTP Header, RTCP Header... Gatekeeper có thể chấp nhận hoặc giảm các yêu cầu này.

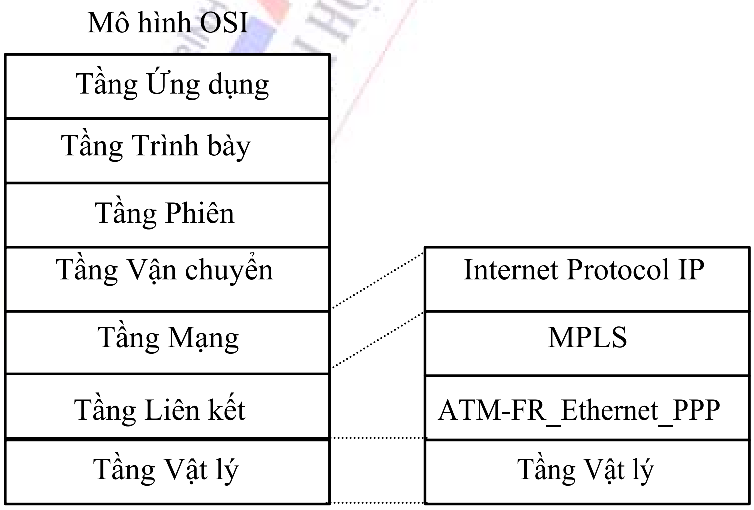
6.3. Công nghệ chuyển mạch nhãn đa giao thức MPLS (MultiProtocol Label Switching)

6.3.1. Mở đầu

Chuyển mạch nhãn đa giao thức MPLS là một kỹ thuật truyền dữ liệu trong công nghệ mạng truyền thông, được chuẩn hóa bởi tổ chức IETF trong khuyến nghị RFC 3031.Ý tưởng cơ bản của MPLS là cung cấp một dịch vụ truyền gói tin thống nhất cho chuyển mạch kênh và chuyển mạch gói dựa trên các thiết bị chuyển mạch tốc độ cao, có cấu trúc đơn giản. MPLS có khả năng hỗ trợ nhiều mô hình dịch vụ và quản lý được lưu lượng nên có thể được dùng để chuyển tải nhiều loại lưu lượng khác nhau như thoại, số liệu, video...

MPLS được xem là sự tích hợp giữa công nghệ chuyển mạch gói và chuyển mạch kênh, giữa chức năng định tuyến trên nền tảng IP và chức năng chuyển mạch trên nền tảng ATM.

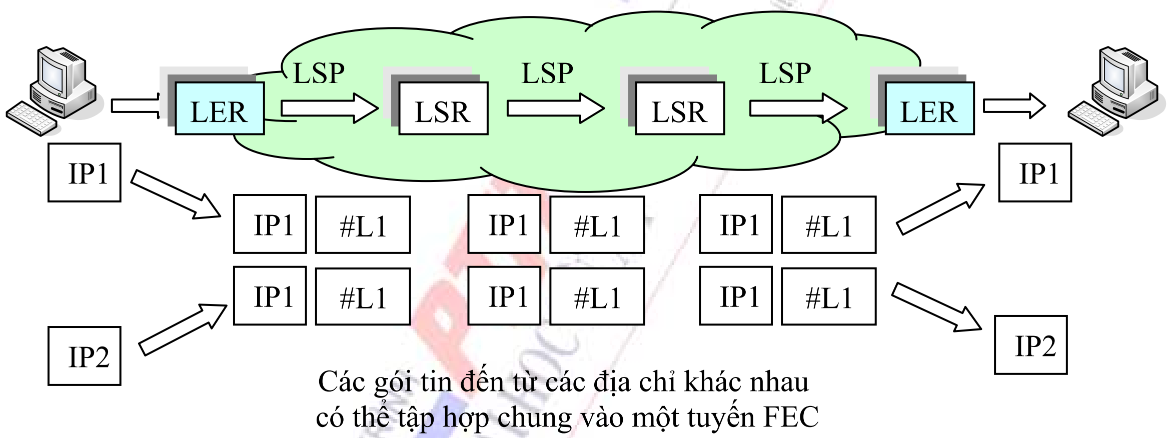
6.3.2. Kiến trúc và nguyên tắc hoạt động MPLS



Hình 6.13 MPLS trong mô hình OSI

Cấu trúc mạng MPLS: Một cách tổng quát, cấu trúc mạng MPLS gồm có 2 phần biên và lõi. Chức năng các thành phần trong mạng tách biệt. Chức năng chuyển mạch nhãn và chuyển gói có xu hướng tập trung ở phần lõi, chức năng xử lý gói và định tuyến được đẩy về thành phần biên. Bộ định tuyến biên LER (Label Edge Router) là phần tử biên của mạng MPLS thường được tích hợp các giao thức định tuyến MPLS và IP. Phần tử này còn được gọi là bộ định tuyến PE (Provider Edge). Tùy theo vị trí của LER đối với chiều đi của gói tin gọi LER là bộ định tuyến đầu vào (Ingress) hay đầu ra (Egress). Bộ định tuyến lõi LSR (Label Switch Router) là phần tử nằm trong mạng MPLS, thực hiện chức năng định tuyến dựa trên việc chuyển mạch nhãn. Phần tử này còn được gọi là bộ định tuyến P (Provider).

Nguyên tắc chuyển mạch nhãn MPLS: Gói tin chưa được gán nhãn MPLS được chuyển đến LER để chuyển qua mạng MPLS, LER sẽ xác định và phân loại gói tin vào các lớp gọi là lớp chuyển tiếp tương đương FEC (Forwarding Equivalence Class). Phần Header MPLS của gói tin sẽ được thêm bằng cách chèn thêm một hoặc nhiều nhãn trước gói tin. Sau đó, gói tin được chuyển đi trên tuyến logic gọi là hầm (Tunnel) để đến Router kế tiếp trên đường đến đích. Việc ấn định FEC dựa trên một phần hoặc toàn bộ địa chỉ lớp mạng đích. Các gói tin thuộc cùng một FEC sẽ được chuyển đi trên cùng một tuyến gọi là LSP (Label Switch Path). Cơ chế chuyển gói theo các LSP cho thấy tính định hướng kết nối của MPLS.



Hình 6.13 Nguyên tắc hoạt động của MPLS

Cơ chế phân phối nhãn nhằm mục đích trao đổi các thông tin liên kết nhãn trong mạng MPLS đảm bảo cho các bộ định tuyến liền kề có thể cập nhật, duy trì và thống nhất với nhau về giá trị nhãn cho các FEC (biểu thị bởi trường Destination) trong cơ sở dữ liệu nhãn. Cơ chế này có thể dựa trên giao thức định tuyến BGP, OSPF, RSVP-TUNNELS hoặc giao thức phân phối nhãn chuyên dụng LDP (Label Distribution Protocol). Việc trao đổi thông tin nhãn trong MPLS theo nguyên tắc ngang hàng. Có 4 loại bản tin trong LDP: Discovery, Session, Advertisement và Notification.

Cơ chế xử lý nhãn và chuyển gói tin: Khi một gói tin đã được gán nhãn MPLS được chuyển đến LSR, phần nhãn ngoài cùng sẽ được phân tích. Tùy theo nội dung của nhãn, một trong ba thao tác sau đây sẽ được thực hiện lên chồng nhãn: tráo đổi hay thay nhãn mới (Swap), lấy nhãn ra (Pop), thêm nhãn vào (Push).

Thao tác Push sẽ cộng thêm nhãn vào phía trước của phần nhãn đang có, nghĩa là đóng gói tin (Encapsulating) vào phân lớp khác trong MPLS. Quá trình này cho phép gói tin MPLS được định tuyến theo cơ chế phân cấp (Hierarchical Routing), đặc biệt là được sử dụng cho dịch vụ VPN.

Cơ chế điều khiển lưu lượng và chất lượng dịch vụ trong MPLS: MPLS hỗ trợ chức năng điều khiển lưu lượng nhờ quản trị mạng tạo ra LSP theo phương pháp định tuyến cưỡng bức để đảm bảo chất lượng dịch vụ hoặc giảm lưu lượng tải qua các nút chuyển tiếp tránh tắc nghẽn trong các tình huống đặc biệt. Với cơ chế định tuyến ràng buộc, người quản lý mạng lập trình các điều kiện ràng buộc và mạng MPLS sẽ tự động thực hiện việc định tuyến thỏa mãn các điều kiện trên. Cơ chế này được hỗ trợ bởi báo hiệu LDP để tạo ra các CR-LSP (Compulsory Routing - LSP). MPLS hỗ trợ chất lượng dịch vụ trên cơ sở phân loại các luồng lưu lượng theo độ trễ, băng tần..... Tại biên của mạng, luồng lưu lượng được nhận dạng thông qua việc phân tích một số trường trong Header của gói tin để phân loại chúng vào các FEC để chuyển đi trong các LSP có thuộc tính CoS hay QoS. Thông tin CoS có thể được truyền trong nhãn của mỗi gói hoặc được gán ngầm định cho LSP. Thông tin QoS được hỗ trợ trong trường hợp mạng MPLS chạy trên nền ATM. Vấn đề đặt ra trong MPLS là tiêu chí để phân loại gói tin thành các FEC. Điều này phụ thuộc nhiều vào công nghệ xử lý gói tải tin.

Đánh giá công nghệ chuyển mạch nhãn đa giao thức MPLS:

a. *Ưu điểm*: Công nghệ MPLS đơn giản, có thể giải quyết được vấn đề độ phức tạp và khả năng mở rộng mạng. Có thể thay thế công nghệ ra đời trước đó như Frame Relay, ATM. Có thể nói MPLS hội tụ những ưu điểm của cơ chế định tuyến gói IP và cơ chế hoán đổi nhãn của ATM, cho phép giảm thiểu thời gian xử lý gói tin mà không cần thay đổi các giao thức định tuyến IP. Nhãn MPLS đơn giản, kích thước nhỏ và linh hoạt. Có thể xếp nối tiếp nhãn để tạo thành chồng nhãn có độ phức tạp cao, rất tiện lợi cho việc đánh địa chỉ và truy tìm.

Nếu so sánh với ATM thì MPLS có ưu điểm là không cần đến các giao thức điều khiển báo hiệu hay chuyển mạch tế bào phức tạp như ATM. Kích thước gói MPLS lớn hơn nhiều so với tế bào ATM nên giảm đáng kể thông tin tiêu đề đóng gói tải tin. Mạng truyền thông hiện đại , công nghệ mạng quang với tốc độ cực lớn (10Gbit/s) không chỉ chuyển tải được các gói tin có độ dài 1518 byte (kích thước cực đại của gói Ethernet) mà còn chuyển tải được gói tin MPLS có kích thước tải tin bất kỳ. Tóm lại, MPLS cho phép nâng cao độ thông (thông lượng) mạng. Mặc khác, MPLS duy trì được chức năng kiểm soát lưu lượng và điều khiển ngoài băng như FR hay ATM. MPLS cũng có thể tận dụng cơ sở hạ tầng mạng ATM vì gói tin MPLS có thể chuyển vào kênh ảo ATM và ngược lại. So với giải pháp IP/ATM, IP/MPLS có topo (cấu trúc lên kết) và cấu hình mạng đơn giản hơn.

Ưu điểm của MPLS so với IP là khả năng điều khiển lưu lượng và hỗ trợ kiểm soát chất lượng dịch vụ (cao hơn DiffServ, thấp hơn ATM). MPLS tách bạch rõ ràng chức năng định tuyến với chức năng chuyển tiếp gói (Routing- Forwarding) mặc dù có thể sử dụng lại kiểu định tuyến IP nếu cần.

Nhìn chung, MPLS là công nghệ phù hợp và bắt kịp với xu thế và nhu cầu công nghệ truyền thông hiện tại và tương lai. MPLS hiện tại đang được ứng dụng trong mạng lõi NGN, trong kỹ thuật lưu lượng và nền tảng cho dịch vụ VPN.

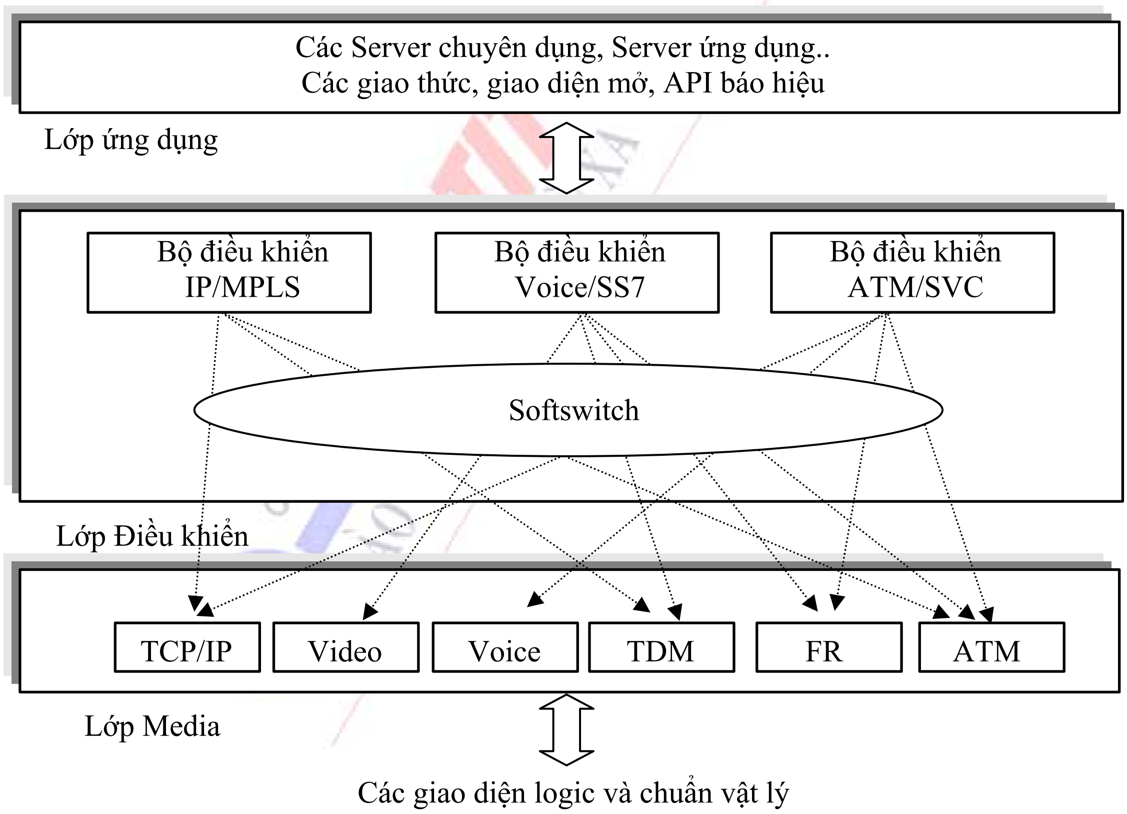
b. Hạn chế của MPLS: MPLS không cung cấp dịch vụ đầu cuối (End-Point) để có thể sử dụng trực tiếp như Ethernet. Về phương diện này, MPLS tương tự như giao thức PPP. MPLS có khả năng bị ảnh hưởng bởi lỗi đường truyền cao hơn các công nghệ khác nên phần nào làm giảm đi độ tin cậy. Đối thủ duy nhất hiện nay của MPLS là giao thức L2TPv3 trong lĩnh vực VPN đặc biệt là trong các mạng có lớp lõi thuần túy là IP.

Xu hướng phát triển: Hướng phát triển mới của MPLS là GMPLS, cung cấp mảng điều khiển chung dựa trên cơ sở IP cho tất cả các lớp. GMPLS sẽ sử dụng kết hợp các thiết bị chuyển mạch gói (bộ định tuyến...) và các thiết bị chuyển mạch kênh (SDH..)

6.4. Công nghệ chuyển mạch mềm (Softswitch)

6.4.1. Mở đầu

Hệ thống chuyển mạch mềm thực hiện chức năng xử lý cuộc gọi trong mạng NGN như định tuyến, báo hiệu, cung cấp dịch vụ cuộc gọi. Chuyển mạch mềm dựa trên ý tưởng tách riêng chức năng điều khiển cuộc gọi (phần mềm) khỏi chức năng chuyển mạch vật lý (phần cứng) và đặt nền tảng trên cơ sở chuyển mạch gói. Chuyển mạch mềm được thực thi bằng các module phần mềm và các giao diện chương trình ứng dụng API (Application Program Interface) chạy trên nền phần cứng là các hệ thống Server dung lượng lớn. Vị trí của chuyển mạch mềm thuộc lớp điều khiển trong mô hình phân lớp chức năng của NGN.



Hình 6.14 Vị trí chuyển mạch mềm trong mô hình phân lớp NGN

Các đặc trưng cơ bản của công nghệ chuyển mạch mềm như sau:

- Dựa trên công nghệ chuyển mạch gói.

- Thiết kế theo mô hình xử lý phân tán

- Giao diện mở API

- Phần mềm điều khiển chuyển mạch không phụ thuộc vào phần cứng chuyển mạch như ở các thiết bị chuyển mạch truyền thống. Có khả năng lập trình được độc lập.

- Tích hợp và liên kết các giao thức khác nhau trong mạng NGN và giữa NGN với mạng truyền thống (PSTN, ATM&IP…).

6.4.2. Cấu trúc và nguyên tắc chuyển mạch mềm

Chuyển mạch mềm hoạt động liên quan đến rất nhiều giao thức ứng dụng khác nhau. Việc liên kết các giao thức được thực hiện nhờ việc liên kết các khối chức năng trong chuyển mạch mềm với sự hỗ trợ đặc biệt của khối liên kết mạng IW-F. Mô hình giao thức sử dụng giải pháp chuyển mạch mềm tổng quát như sau:

BICC (Bearer Independent Call Control): Là giao thức điều khiển cuộc gọi độc lập với kênh truyền tải. Báo hiệu dựa trên ISUP theo chuẩn ITU-T. BICC hỗ trợ các dịch vụ ISDN băng hẹp. BICC thường được dùng cho báo hiệu giữa các chuyển mạch mềm.

MEGACO/H.248/MGCP: Đây là giao thức điều khiển điều khiển giữa Softswitch (MGC) và thiết bị cổng MG theo cơ chế Master/Slave. MGC quyết định chính trong quá trình liên lạc với MG, còn MG là thực thể thụ động thực hiện mọi lệnh do MGC yêu cầu. Các tương tác (transaction) trong MGCP gồm có lệnh và đáp ứng.

RTP/RTCP/RTSP: Real Time Protocol/ Real Time Control Protocol-Real Time Streaming Protocol: là các giao thức hoạt động ngay trên lớp UDP dùng để truyền các thông tin yêu cầu thời gian thực qua mạng gói. RTP được xem như giao thức lớp truyền tải. Bản thân RTP không đảm bảo chất lượng của thông tin cần truyền tải về thời gian thực. Nó chỉ đơn giản cung cấp đầy đủ thông tin lên lớp ứng dụng để xác định độ trễ gói và quyết định cách thức xử lý gói tin như hiệu chỉnh độ di pha. Các dịch vụ mà RTP cung cấp là loại thông tin chuyển tải trong gói, số thứ tự của gói truyền (sequence number), mốc thời gian và thời gian truyền tối đa của 1 gói (Timestamp). Các bản tin RTCP được dùng để trao đổi thông tin phản hồi về chất lượng của phiên RTP đối với tất cả các thành viên tham gia trong phiên truyền tin.

SCTP (Stream Control Transport Protocol) hay SIGTRAN (Signalling Transport): là một giao thức hướng liên kết truyền tải (Transport Protocol) được xây dựng để thay thế TCP (Transmission Control Protocol) trong việc chuyển tải thông tin báo hiệu SS7 trong mạng chuyển mạch vì lý do TCP là giao thức đảm bảo truyền dữ liệu tin cậy thông qua cơ chế xác nhận ACK và cơ chế tuần tự gây trễ gói tin. Các cơ chế này đã có trong giao thức SS7, hơn nữa SS7 yêu cầu thời gian thực nên việc dùng TCP cho SS7 là không hiệu quả.

SCTP chuyển tải theo định hướng bản ghi thay vì định hướng byte như TCP, đồng thời cho phép nhiều luồng dữ liệu logic được ghép kênh để truyền qua một kết nối. SCTP đảm bảo truyền tin cậy theo cơ chế khác với TCP bằng cách thiết lập nhiều kết nối.

SIP (Session Initiation Protocol)/H.323: Các bộ giao thức điều khiển cuộc gọi đa phương tiện (lớp ứng dụng), dùng để thiết lập, điều chỉnh và kết thúc phiên làm việc của thuê bao.

6.4.3. Giao diện ứng dụng API trong chuyển mạch mềm

Chuyển mạch mềm ứng dụng công nghệ phần mềm lập trình theo hướng đối tượng, công nghệ Agent và xử lý phân tán. API là tập hợp các thủ tục, giao thức và các công cụ phần mềm được chuẩn hóa nhằm cho phép liên kết các ứng dụng với nhau. Bằng cách xây dựng các khối chức năng theo API, có thể dễ dàng phát triển ứng dụng phần mềm. API cho phép chia sẻ dữ liệu giữa các ứng dụng trên cùng nền tảng.

a. Các phương thức chia sẻ dữ liệu qua API:

- Gọi thủ tục từ xa RPC (Remote Procedure Calls): Dùng cho các ứng dụng trao đổi thông tin với nhau bởi các thủ tục (Procedure/Task) trên cùng bộ đệm dữ liệu.

- Ngôn ngữ truy vấn chuẩn SQL (Standard Query Language) là ngôn ngữ dùng truy xuất dữ liệu không cần thủ tục, cho phép chia sẻ dữ liệu giữa các ứng dụng bằng cách truy nhập vào cơ sở dữ liệu chung.

- Chuyển file (File Transfer): Phương thức này cho phép chia sẻ số liệu bằng cách trao đổi file đã được định dạng giữa các ứng dụng.

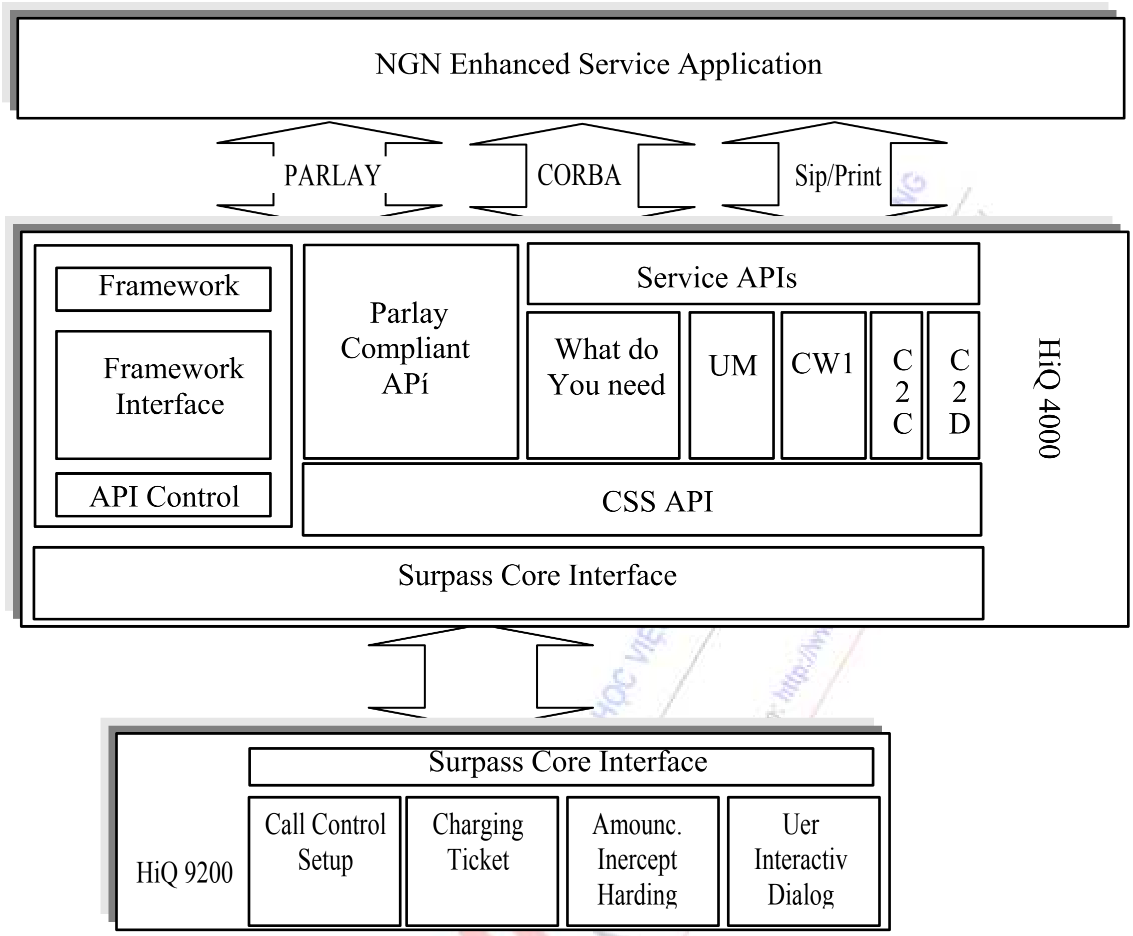
- Phân phát bản tin (Message Delivery): Cho phép chia sẻ dữ liệu bằng cách trao đổi thông tin trực tiếp thông qua các bản tin định dạng có kích thước nhỏ giữa các ứng dụng có liên kết với nhau.

b. Có thể phân lớp các API trong Softswitch thành 3 nhóm chính:

- API liên kết các nguồn tài nguyên mạng (Resources API)

- API liên kết các module có năng lực xử lý trong mạng (Network Capability API)

- API liên kết NGN với môi trường ngoài như nhà cung cấp dịch vụ thứ 3 hay khách hàng có nhu cầu phát triển ứng dụng.



Hình 6.15 Mô hình API trong chuyển mạch mềm giải pháp của SIEMENS

Hiện nay, API liên kết các nguồn tài nguyên mạng và API liên kết các module có năng lực xử lý trong mạng được phát triển nhiều trên cơ sở JAIN (Java API Intergrated Network). Nhóm thứ ba được phát triển theo nhiều hướng như JAIN, 3GPP (3th Generation Ship Project, PARLAY GROUP). Các chuẩn API hiện vẫn đang được phát triển và chuẩn hiện đang được dùng phổ biến là SQL API của ANSI.

6.4.4. Kế hoạch đánh số trong chuyển mạch mềm

Việc đánh địa chỉ cũng như số thuê bao và dịch vụ trong NGN là hoàn toàn linh hoạt bằng cách khai báo dữ liệu kho số vào cơ sở dữ liệu động của máy chủ quản lý địa chỉ. Cơ sở dữ liệu này có thể cập nhật, bổ sung hoặc thay đổi bởi nhà quản trị mạng, tuy nhiên phải dựa các tiêu chí chính như sau:

- Quy luật đánh địa chỉ tuân theo khuyến nghị của ITU-T (E164-E169).
- Quy hoạch địa chỉ cần kế thừa và giữ được thói quen quay số của người dùng.
- Quy hoạch địa chỉ tận dụng một số các mã đặc biệt dành riêng để phát triển về sau với nhiều mục đích khác nhau.

- Việc quy hoạch địa chỉ trong NGN phải đảm bảo không trùng lặp với các dải địa chỉ đang được sử dụng trong các mạng truyền thống kết nối đến mạng NGN.

6.4.5. Đánh giá công nghệ chuyển mạch mềm

Bảng so sánh công nghệ Softwwitch và chuyển mạch kênh.

	Softswitch	**Tổng đài PSTN**
Phương pháp chuyển mạch	Phần mềm	Điện tử
Kiến trúc	Phân tán, theo các chuẩn mở	Riêng biệt của từng nhà sản xuất
Khả năng tích hợp với ứng dụng của nhà cung cấp khác	Dễ dàng	Khó khăn
Khả năng thay đổi mềm dẻo	có	Khó khăn
Giá thành	Rẻ, khoảng bằng một nửa tổng đài điện tử	Đắt
Khả năng nâng cấp	Rất cao	Rất tốt, tuy có hạn chế hơn
Giá thành của cấu hình cơ bản	Thấp, giá thành thay đổi gần như tuyến tính theo số lượng thuê bao. Cấu hình cơ bản có thể sử dụng cho mạng doanh nghiệp	Rất cao, tổng đài PSTN không thích hợp cho mạng doanh nghiệp.
Truyền thông đa phương tiện	Có	Rất hạn chế
Hội nghị truyền hình	Tốt hơn	Có
Lưu lượng	Thoại, fax, dữ liệu, video...	Chủ yếu là thoại và fax
Thiết kế cho độ dài cuộc gọi	Khụng hạn chế	Ngắn (chỉ vài phút)

Công nghệ chuyển mạch mềm có những ưu điểm nổi bật so với các công nghệ truyền thông như sau:

- Cho phép đưa ra giải pháp phần mềm chung đối với việc xử lý cuộc gọi, có thể áp dụng trên nhiều loại mạng khác nhau.

- Đơn giản cấu trúc hệ thống và linh hoạt trong việc thay đổi tính năng, cấu hình, mở rộng phát triển và liên kết giữa các hãng cũng như giữa các nhà cung cấp dịch vụ.

- Cho phép tích hợp và phát triển các phần mềm thông minh của các nhà cung cấp dịch vụ, khai thác tiềm năng của mạng trong tương lai.

- Dễ dàng tích hợp dịch vụ mới từ nhà cung cấp thứ ba đồng thời cho phép người sử dụng có thể tự phát triển ứng dụng và dịch vụ.

6.5. Mạng hội tụ và mạng thế hệ sau NGN (Network Convergence and Next Generation Network)

6.5.1. Mở đầu

Xu hướng công nghệ truyền thông hiện nay đang xóa dần ranh giới giữa công nghệ thông tin và viễn thông. Thế giới đang bước vào kỷ nguyên của sự hội tụ. Các nhà sản xuất và cung cấp dịch vụ không chỉ quan tâm đến việc phát triển dịch vụ mà còn phải xây dựng và củng cố và tối ưu hóa hạ tầng mạng lưới trên cơ sở hội tụ mạng.

Mạng hội tụ là sự tích hợp một cách thông minh giữa các mạng truyền thông, tích hợp giữa cơ sở hạ tầng của mạng mới với mạng hiện có. Nói cụ thể, hội tụ mạng là sự hợp nhất hay tích hợp nhiều công nghệ, phương tiện truy nhập và truyền thông, giao thức, tài nguyên dữ liệu và ứng dụng khác nhau trên một cơ sở hạ tầng và quản lý chung nhằm tạo ra một mạng truyền thông mới, cung cấp đồng thời nhiều loại hình dịch vụ với chất lượng cao, đáp ứng được đồng thời các loại hình dịch vụ khác nhau, mọi nhu cầu của khách hàng.

Sự hội tụ thể hiện ở nhiều khía cạnh như đa công nghệ, đa giao thức, đa truy nhập, đa phương tiện truyền thông, đa dịch vụ …

Giao thức Internet (IP) được sử dụng phổ biến để liên kết các mạng khác nhau tạo nên mạng hội tụ với xu hướng trước mắt là hội tụ giữa mạng thoại và mạng số liệu.

Một trong những mạng hội tụ tiên tiến đang được ứng dụng là mạng thế hệ sau (Next Generation Network - NGN). Ý tưởng về mạng NGN đã được hình thành từ cuối những năm 90 của thế kỷ trước và cho đến nay NGN đã được triển khai rộng khắp ở các nước phát triển và đang phát triển, thay thế dần các mạng truyền thống thế hệ trước.

6.5.2. Tổng quan về mạng thế hệ sau sau - NGN (Next Generation Network)

Mạng thế hệ sau NGN được xây dựng theo các nguyên tắc sau:

- Có kiến trúc mở, phân lớp, linh hoạt, dễ dàng phát triển mở rộng
- Cơ sở hạ tầng dựa trên công nghệ truyền tải băng rộng, công nghệ chuyển mạch gói
- Có khả năng kiểm soát được chất lượng dịch vụ (QoS)
- Đáp ứng được đồng thời và đa dạng các loại hình dịch vụ, cho phép thuê bao truy nhập một cách linh hoạt đến nhiều nhà cung cấp dịch vụ khác nhau.
- Lớp (chức năng) cung cấp dịch vụ độc lập với lớp (công nghệ) truyền tải bên dưới.
- Tương thích và hỗ trợ các mạng và dịch vụ hiện có

NGN hội tụ những ưu điểm của công nghệ chuyển mạch kênh và chuyển mạch gói:

a. Ưu điểm từ chuyển mạch kênh:

- Đảm bảo thời gian thực
- Giảm hiện tượng thất thoát thông tin do nghẽn hay trễ
- Đảm bảo chất lượng dịch vụ

b. Ưu điểm từ chuyển mạch gói:

- Chia xẻ và tận dụng được tài nguyên mạng

- Linh hoạt trong việc định tuyến và điều khiển lưu lượng
- Kích thước tải tin có thể thay đổi

6.5.3. Sự bùng nổ và nhu cầu da dạng của các loại hình dịch vụ

- Dịch vụ băng hẹp (voice) - Dịch vụ băng rộng (video, truyền hình)

- Dịch vụ đơn phương tiện (fax) - Dịch vụ đa phương tiện (hội nghị truyền hình)

- Dịch vụ truyền thông theo thời gian thực (đàm thoại) - Dịch vụ phi thời gian thực (truyền số liệu)

- Dịch vụ truy cập ứng dụng của nhà cung cấp dịch vụ (MegaVNN) - Dịch vụ thuê cơ sở hạ tầng (MegaWAN)

- Dịch vụ đơn giản (giải đáp thông tin) - Dịch vụ thông minh (truy xuất cơ sở dữ liệu thông tin tự động)

- Dịch vụ tương tác 2 chiều (trò chơi) - Dịch vụ phân bố một chiều (quảng bá)

- Dịch vụ chất lượng thấp (VoIP giá rẻ 8Kb/s) - Dịch vụ chất lượng cao (VoIP 64kb/s)

Các dịch vụ băng rộng yêu cầu tốc độ và thời gian chiếm kênh lớn vượt quá khả năng của mạng hiện tại.

6.5.4. Mô hình phân lớp và chức năng các lớp NGN

NGN là xu hướng phát triển kỹ thuật mạng hiện đại. Các hãng cung cấp thiết bị khác nhau có các mô hình phân lớp khác nhau. Tuy nhiên, mô hình NGN chung phân chia lớp dịch vụ với lớp truyền tải, giúp cho các nhà cung cấp dịch vụ có thể đưa vào các dịch vụ mới mà không cần quan tâm đến việc kiến trúc lớp truyền tải. Nói cách khác, lớp dịch vụ là độc lập (trong suốt) đối với lớp truyền tải.

Có thể phân lớp chức năng NGN như sau:

1. Lớp truy nhập (Access): có chức năng kết nối giữa mạng NGN với thiết bị đầu cuối thuê bao hoặc các mạng truyền thống khác.

2. Lớp truyền tải (Transport): có chức năng định tuyến, chuyển mạch và chuyển tiếp gói tin giữa các phần tử mạng.

3. Lớp điều khiển (Control): có chức năng

- Điều khiển kết nối và báo hiệu cuộc gọi
- Điều khiển lưu lượng và chất lượng dịch vụ
- Điều khiển hoạt động của các phần tử thiết bị trong mạng NGN.

4. Lớp ứng dụng/dịch vụ (Application/Service): có chức năng điều phối và cung cấp các loại hình dịch vụ và ứng dụng trên mạng NGN, cung cấp môi trường kiến tạo dịch vụ mạng thông minh (Intelligent Network Service Creation Environment) và các giao diện mở cho các nhà phát triển dịch vụ thứ ba.

5. Lớp quản lý (Management): có chức năng quản lý mạng theo mô hình TMN:

- Quản lý kinh doanh, chăm sóc khách hàng
- Quản lý dịch vụ
- Quản lý kết nối, tính cước

- Quản lý tài nguyên và chất lượng mạng lưới
- Quản lý phần tử thiết bị

Kiến trúc phân lớp mang lại cho NGN các ưu điểm sau:

- Chức năng chuyển mạch vật lý phân tán sẽ giúp giải quyết vấn đề tắc nghẽn

- Chức năng điều phối cuộc gọi tập trung sẽ giúp cho việc quản lý thuận lợi

- Giao diện chuẩn cho phép sự lựa chọn linh hoạt các phần tử mạng của các nhà cung cấp khác nhau, phát huy điểm mạnh của từng nhà cung cấp

- Sự thay đổi hay nâng cấp công nghệ một lớp không ảnh hưởng đến toàn mạng.

- Các nhà cung cấp dịch vụ có thể tự do phát triển các dịch vụ mới mà không quá phụ thuộc vào các nhà khai thác mạng

6.5.5. Cấu trúc và các thành phần hệ thống NGN

Các hãng khác nhau đưa ra các giải pháp khác nhau về cấu trúc NGN. Tuy nhiên, nhìn chung các thành phần cơ bản của hệ thống bao gồm:

Các hệ thống ở lớp truy nhập gồm nhiều chủng loại thiết bị với công nghệ khác nhau như POTS, VOIP, IP, FR, X25, ATM, xDSL… cho phép kết nối tới các thiết bị đầu cuối của người dùng (Residential Gateway), kết nối tới mạng truy nhập (Access Gateway) và cung cấp giao diện kết nối và chuyển đổi dạng thông tin giữa NGN với mạng chuyển mạch kênh (Media gateway hay Trunk Gateway).

Các hệ thống ở lớp chuyển tải bao gồm bộ định tuyến, chuyển mạch IP/MPLS, thiết bị truyền dẫn quang dung lượng lớn DWDM/SONET/SDH.

Các hệ thống ở lớp điều khiển bao gồm chuyển mạch mềm (SoftSwitch) là phần tử điều khiển kết nối cuộc gọi (Call Agent) và điều khiển cổng đa phương tiện MGC (Media Gateway Controller), thiết bị cổng báo hiệu SG (Signalling Gateway) cung cấp giao diện kết nối báo hiệu với mạng truyền thống với các giao thức báo hiệu SS7, SMS, WAP...

Các hệ thống ở lớp dịch vụ và ứng dụng bao gồm các thiết bị máy chủ ứng dụng: Media Server (MS), Application Server (AS), Call Feature Server (FS), Man-machine Server, Subscriber Database Server.

Các hệ thống ở lớp quản lý bao gồm các thiết bị quản lý cước, giám sát sự cố, can thiệp lệnh, quản lý cấu hình, tài nguyên, quản lý chất lượng mạng.

6.5.6. Các công nghệ nền tảng trong NGN

Công nghệ truy nhập thuê bao số xDSL (Digital Subscriber Line): Là công nghệ điều chế cung cấp giải pháp truyền dữ liệu và thoại trên đường dây cáp đồng âm tần nhằm tận dụng được dải thông tần số của cáp đồng. Về bản chất, DSL là công nghệ thực hiện ở Modem DSL chuyển dữ liệu thành dạng tín hiệu số dung lượng lớn, tần số cao, phổ rộng. DSL bao gồm nhiều phiên bản khác nhau như ADSL có tốc độ hai chiều không đối xứng, HDSL, SHDSL, G.SHDSL (tốc độ hai chiều đối xứng) …

Công nghệ truyền dẫn quang tốc độ cao với ghép kênh phân chia bước sóng mật độ cao DWDM (Dense Wavelength Division Multiplexing) theo phân cấp đồng bộ SONET/SDH

(Synchronous Optical Network/Synchronous Digital Hierachy). WDM cho phép sử dụng độ rộng băng tần rất lớn của sợi quang bằng cách kết hợp một số các tín hiệu ghép kênh theo thời gian với bước sóng khác nhau đồng thời có thể tận# dụng được các cửa sổ không gian, thời gian và độ dài bước sóng. Công nghệ WDM cho phép nâng tốc độ các truyền dẫn lên 5 Gb/s, 10 Gb/s và 20 Gb/s.

Phương thức truyền thông không đồng bộ ATM (Asynchronous Transfer Mode): Thông tin của một ứng dụng không nhất thiết phải xuất hiện một cách tuần hoàn và đồng bộ. ATM sử dụng các tế bào có độ dài cố định 53 byte, không định vị theo xung đồng bộ và thay đổi theo nhu cầu truyền tin. ATM cho phép chuyển tải lưu lượng cho nhiều loại dịch vụ với tốc độ khác nhau. Hiện nay, xu hướng kết hợp công nghệ ATM với DSL mang lại một giải pháp hiệu quả cho dịch vụ truy nhập băng rộng.

Các đặc trưng chính của ATM như sau:

- Hỗ trợ đa dịch vụ, đa tốc độ
- Đảm bảo QoS
- Quản lý băng tần
- Kết nối hướng liên kết.
- Tốc độ chuyển gói cao, giảm trễ gói tin

Định tuyến và chuyển mạch gói tin IP (Internet Protocol): Có các đặc trưng cơ bản sau: Qui hoạch địa chỉ toàn cục: Mỗi một giao diện mạng được gán một địa chỉ duy nhất. Tận dụng năng lực truyền tối đa (Best Effort): IP cố gắng tối đa để chuyển các gói tin, tuy nhiên nó không có cam kết về chất lượng dịch vụ (QoS) như tỉ lệ thành công hay thời gian cần để đưa gói tin đến đích. Với phiên bản IPv6, một số tính năng mới được hỗ trợ như phương pháp đánh địa chỉ linh hoạt, không gian địa chỉ lớn. Cơ chế bảo mật cao. Hỗ trợ đa phương tiện. Hỗ trợ chất lượng dịch vụ QoS và có khả năng tự cấu hình

Chuyển mạch nhãn đa giao thức MPLS (Multiprotocol Label Switching) đã trở thành công nghệ nền tảng trong lớp chuyển tải của NGN.

Công nghệ chuyển mạch mềm (Softswitch):là công nghệ cốt lõi trong lớp điều khiển NGN. Phần tử hệ thống trung tâm sử dụng công nghệ này chính là MGC (Media Gateway Controller). Ngoài ra, công cụ lập trình theo module giao diện chương trình ứng dụng API (Application Program Interface) cũng được ứng dụng nhiều ở các lớp ứng dụng/dịch vụ và quản lý cũng như liên kết giữa chúng với lớp điều khiển trong NGN. Có thể xem API như một công nghệ phần mềm nền tảng trong Softswitch nói riêng và NGN nói chung.

Tóm lại xu hướng hiện nay của công nghệ nền tảng theo phân lớp NGN như sau:

- IP/ATM/DSL: công nghệ nền tảng trong lớp truy nhập
- IP/MPLS/SDH/WDM/Optical: công nghệ nền tảng trong lớp truyền tải
- IP/Ehernet (FE,GE) + Softswitch: công nghệ nền tảng trong lớp điều khiển
- IP/FE + API: công nghệ nền tảng trong lớp ứng dụng/dịch vụ và quản
- SCTP chuyển tải theo hướng bản ghi, không như TCP hướng byte, đồng thời cho phép nhiều luồng dữ liệu logic được ghép kênh để truyền qua một kết nối. SCTP đảm bảo truyền tin cậy theo cơ chế khác với TCP bằng cách thiết lập nhiều kết nối.

6.5.7. Mô hình NGN và các giải pháp thiết kế của một số hãng

Trên cơ sở mô hình chung NGN, các hãng viễn thông khác nhau có các giải pháp thiết kế theo nhiều chuẩn khác nhau. Trong đó, một số giải pháp thể hiện tính khả thi, rõ ràng, đáp ứng được mục tiêu đặt ra chung nhất của các mô hình, có nhiều ý tưởng mới và phù hợp với cơ sở hạ tầng mạng hiện tại, đồng thời đảm bảo xu hướng phát triển chung của công nghệ như: giải pháp SURPASS của SIEMENS, Alcatel 1000 SoftSwitch của ALCATEL, ENGINE của ERICSSON… Đặc biệt, mô hình của SIEMENS có nhiều điểm tương đồng với mô hình NGN của tổ chức MSF (MultiService Switching Forum).

* ALCATEL đưa ra giải pháp tổng thể gồm các bước phát triển từ mạng viễn thông hiện tại tiến tới mạng NGN như sau :

1. Duy trì mạng PSTN và hội tụ với mạng số liệu.
2. Phát triển thoại trên công nghệ gói đối với các dịch vụ đường dài.
3. Phát triển thoại trên công nghệ gói đối với các dịch vụ truy nhập nội hạt.
4. Phát triển các dịch vụ đa phương tiện
5. Phát triển mạng NGN hoàn chỉnh

* ERICSSON: Ericsson giới thiệu giải pháp mạng thế hệ mới có tên gọi là ENGINE. Cấu trúc ENGINE hướng tới các ứng dụng và hoạt động theo cơ chế Client/Server và Gateway/Server. Các ứng dụng gồm có hai phần: phần Client trên máy đầu cuối và phần Server chạy trên máy chủ. Hai phần giao tiếp với nhau qua các giao diện mở.

* NORTEL: Mục tiêu chính của Nortel là hoàn thiện mạng lõi, đảm bảo hợp nhất các mạng thoại và số liệu để có thể cung cấp các dịch vụ IP, ATM bằng cách đưa ra giải pháp mạng lõi IP/MPLS bao gồm bộ định tuyến và chuyển mạch MPLS có giao diện quang. Hệ thống chuyển mạch trên cơ sở kết hợp ATM và IP/MPLS có khả năng cung cấp đa dịch vụ cho thuê bao với dung lượng 40 Gbit/s và có khả năng mở rộng lên tới 19,2 Terabit/s.

* JUNIPER: Giới thiệu mô hình NGN gồm các thành phần: POS (Paket over Synchnonization Network). B-RAS (Broadband Remote access Server) và NAS (Narrow Access Server).

* CISCO: DS-1,T1: Digital Signal Level 1, CPE: Customer Premise Equipment, PBX: Private Exchange, SS7: Signalling system no.7, MGCP: Media Gateway Control Protocol.

* LUCENT: Lucent đưa ra giải pháp NGN tập trung chủ yếu vào hai lớp:

1. Lớp lõi ATM/IP và công nghệ truyền dẫn quang tiên tiến DWDM
2. Lớp phân phối dịch vụ

* NEC đưa ra giải pháp chuyển mạch tích hợp IP/ATM/STM với các cổng đa năng.

* SIEMENS đưa ra giải pháp khả thi và khá hoàn chỉnh về cấu trúc mạng NGN, đáp ứng được phần lớn các mục tiêu đặt ra ở mô hình NGN. Giải pháp NGN của SIEMENS có tên gọi là SURPASS. Theo quan điểm của SIEMENS, NGN có cấu trúc phân tán, vì vậy có khả năng điều khiển chuyển mạch NGN, cơ chế truy nhập, cơ chế truyền tải, cơ chế quản lý mạng, cơ chế điều khiển dựa trên hệ thống máy chủ tập trung, cơ chế truy nhập đa dịch vụ, cơ chế truyền tải trên IP/MPLS và giao diện quang, cơ chế điều khiển sử dụng giao thức SNMP (Simple Network Management Protocol) trên nền JAVA/CORBA, với giao diện HTTP để tạo giao diện WEB với người sử dụng.

Nhận xét:

- Qua các giải pháp thiết kế của các hãng, nhìn chung chức năng truyền dẫn và chuyển mạch được tích hợp chung trong lớp chuyển tải hay lớp lõi. Như vậy thiết bị truyền dẫn và chuyển mạch được xem như công cụ thực hiện chức năng chuyển tải lưu lượng. Một số hãng gộp chung lớp truy nhập với lớp chuyển tải.

- Các hãng chú ý đến chức năng điều khiển và quản lý. Tính phức hợp giao thức ở lớp này đòi hỏi khả năng tương thích cao giữa các chủng loại thiết bị.

- Chức năng quản lý có xu hướng tập trung cao và xuyên suốt qua các lớp khác nhau trong cấu trúc mạng lưới.

- Vai trò của các thiết bị điều khiển, thiết bị quang và thiết bị truy nhập và các giao thức chuyển gói như IP đóng vài trò quan trọng trong việc hình thành mạng NGN.

- NGN có thể xem như mạng thế hệ kế tiếp, không phải là mạng hoàn toàn mới, vì vậy các hãng đều cân nhắc đến khía cạnh tương thích với mạng và chủng loại thiết bị hiện có.

- Mỗi giải pháp đều có những ưu điểm và hạn chế nhất định. Việc lựa chọn giải pháp tối ưu cần phải căn cứ trên nhiều tiêu chí và cân nhắc về giữa các yêu cầu và mục tiêu có thể mâu thuẫn nhau.

6.5.8. Một số dịch vụ NGN

Dịch vụ thoại truyền thống sẽ chuyển dần sang VoIP và được tích hợp trong các dịch vụ mới khác. Các dịch vụ truyền số liệu sẽ được thay thế bởi các dịch vụ mạng riêng ảo VPN. Dịch vụ ISDN sẽ được thay thế bằng các dịch vụ MMA trên nền NGN. Dịch vụ truy cập Internet băng hẹp chuyển sang truy cập băng rộng DSL. Các dịch vụ trên nền WEB và dịch vụ thông minh sẽ được tăng cường phát triển trên cơ sở giao diện phần mềm mở, hướng đến nhà cung cấp dịch vụ thứ ba và khách hàng.

- Dịch vụ thẻ trả trước 1719cho phép sử dụng tài khoản thẻ thực hiện cuộc gọi nội hạt, liên vùng và quốc tê. Khách hàng cũng có thể gán một tài khoản trả trước cho một số điện thoại cố định. Ưu điểm nổi bật của dịch vụ 1719 là khả năng cung cấp dịch vụ với nhiều cấp chất lượng dịch vụ trên cùng một hạ tầng mạng. Khách hàng có thể lựa chọn chất lượng cao như PSTN 64kb/s hoặc giá rẻ như VoIP 8kb/s

- Dịch vụ gọi miễn cước 1800 (Freephone) cho phép thực hiện cuộc gọi miễn cước đến nhiều đích khác nhau thông qua một số truy nhập thống nhất. Khi thuê bao quay số Freephone, số Freephone sẽ được chuyển thành một số đích tương ứng tại chuyển mạch mềm và cuộc gọi sẽ được thiết lập đến đích tương ứng. Đích tương ứng được lựa chọn trên cơ sở vùng của thuê bao chủ gọi, mã số dịch vụ và thời điểm gọi trong ngày.

- Các dịch vụ đa phương tiện MMA là dịch vụ cho phép thực hiện cuộc gọi đa phương tiện tích hợp như thoại, số liệu, hình ảnh… đồng thời. Một số dịch vụ MMA đang được triển khai như: hội nghị truyền hình, đào tạo từ xa, y tế, truyền bản tin video tương tác..

- Các dịch vụ thông minh: Một số dịch vụ thông minh được phát triển trên nền NGN như: chuyển đổi ngôn ngữ, game trực tuyến, truy vấn cơ sở dữ liệu, video theo yêu cầu… Ví dụ 1900 là dịch vụ giải trí, tư vấn có nội dung phụ thuộc vào các phần mềm ứng dụng được xây dựng trên các máy chủ của nhà cung cấp dịch vụ.

- Dịch vụ WEB trên NGN có khả năng cung cấp nhiều loại hình dịch vụ WEBk hác nhau. Một trong các dịch vụ thông dụng đang được triển khai là WEB DIAL PAGE cho phép thực hiện cuộc gọi từ trang WEB, WEB CONFERENCE: điện thoại hội nghị qua WEB.

Dịch vụ truy nhập Internet tốc độ cao cung cấp kết nối Internet băng rộng với công nghệ truy nhập DSL, có các cam kết (SLA) như về tốc độ, băng thông … Dịch vụ này cho phép kết nối máy đơn hoặc mạng máy tính với phương thức cấp địa chỉ IP tĩnh hoặc động tùy theo nhu cầu.

- Dịch vụ mạng riêng ảo VPN cung cấp kết nối mạng LAN/WAN riêng cho khách hàng trên nền hạ tầng mạng công cộng NGN IP/MPLS, có hỗ trợ an ninh mạng và thỏa thuận về cấp độ dịch vụ SLA (Service Layer Agreement). Dịch vụ cung cấp cho khách hàng các tài nguyên mạng, các ứng dụng trong VPN là do khách hàng tự xây dựng.

VPN trên nền NGN có nhiều ưu điểm so với các mạng máy tính khác, có khả năng đảm bảo chất lượng dịch vụQoS, khả năng cung cấp các kết nối linh hoạt có thể thay đổi cấu hình dễ dàng, sử dụng tài nguyên mạng một cách hiệu quả., khả năng mở rộng dịch vụ toàn cầu và không hạn chế băng thông kết nối.

6.5.9. NGN trong mạng viễn thông Việt nam

NGN cũng đã được triển khai ở Việt Nam từ năm 2004 theo giải pháp kết hợp: SIEMENS cho lớp điều khiển, JUNIPER cho lớp chuyển tải, ALCATEL cho lớp truy nhập. Trong tương lai, NGN sẽ được phát triển mở rộng trên địa bàn cả nước. Tận dụng năng lực của mạng hiện có, việc chuyển từ mạng viễn thông hiện tại lên mạng thế hệ sau NGN phải trải qua nhiều giai đoạn. từng bước, vẫn phải duy trì hoạt động của các mạng truyền thống. Đồng thời mạng đường trục VNPT sẽ được đầu tư các công nghệ trong NGN. Các mạng truyền thống khác như di động và nội hạt sẽ kết nối với NGN qua thiết bị cổng chuyển đổi. Trong tương lai, các mạng này cũng sẽ được thay thế hoàn toàn bởi công nghệ NGN.

Chức năng các lớp NGN trong mạng viễn thông Việt Nam:

- Lớp quản lý: sẽ hình thành hệ thống quản lý mạng viễn thông tập trung theo mô hình TNM (Telecom Network Management).

- Lớp ứng dụng và dịch vụ mạng: trang bị các server dich vụ tại hai điểm nút Hà Nội và TP Hồ Chí Minh, cung cấp các dịch vụ mới trên nền NGN như dịch vụ giải trí, truy nhập cơ sở dữ liệu thông tin tự động, điện thoại thẻ giá rẻ, điện thoại miễn cước đường dài, cuộc gọi hội nghị, các dịch vụ trên cơ sở WEB, truy nhập Internet băng rộng qua NGN, cho thuê cơ sở hạ tầng mạng dưới hình thức mạng riêng ảo (VPN) có thương hiệu là MegaWAN…

- Lớp điều khiển: Tổ chức 5 nút điều khiển (chuyển mạch mềm) ứng với 5 vùng lưu lượng theo mô hình hai mặt nghĩa là có dự phòng 1+1

- Lớp truyền tải: Lớp truyền tải NGN dựa trên công nghệ IP/MPLS/SDH/WDM/truyền dẫn quang. Lớp truyền tải được tổ chức thành hai cấp: cấp đường trục quốc gia và cấp vùng. Mạng truyền dẫn quang đường trục quốc gia đạt đến dung lượng 20Gb/s.

- Lớp truy nhập: Tại mỗi vùng đều được trang bị các thiết bị truy nhập cho lưu lượng VoiP qua hệ thống MG và lưu lượng truy nhập internet và mạng riêng ảo qua hệ thống DSLAM với công nghệ ADSL và SHDSL.

Câu hỏi trắc nghiệm:

1. Hãy chọn câu đúng nhất về DSL:
   A. Công nghệ DSL cho phép tận dụng miền tần số cao truyền tín hiệu tốc độ cao trên đôi dây cáp đồng thông thường.
   B. Công nghệ DSL biến đổi tín hiệu của người sử dụng thành các tín hiệu phù hợp với đường truyền.
   C. Kỹ thuật DSL cho phép truyền chế độ song công đối xứng và bất đối xứng.
2. Họ công nghệ DSL gồm:
   A. IDSL
   B. HDSL
   C. VDSL
   D. ADSL
   E. ROUTER
3. Các phương pháp mã hóa đường truyền
   A. Phương pháp điều chế biên độ và pha triệt sóng mang CAP
   B. Phương pháp đa âm tần rời rạc DMT
   C. Cả hai phương pháp.
4. Nhiễu trong kỹ thuật DSL:
   D. Nhiễu xuyên âm đầu gần NEXT (Near - end Crosstalk)
   E. Nhiễu xuyên âm đầu xa FEXT (Far - end- Crosstalk)
   F. Cả hai phương pháp.
5. Các phương pháp chống nhiễu trong kỹ thuật DSL:
   A. Chống xuyên nhiễu
   B. Phương pháp triệt tiếng vọng (EC)
   C. Cả hai phương pháp.
6. Các mô hình kết nối ADSL
   A. Mô hình PPPoA (Point to Point over ATM)
   B. Mô hình PPPoE (Point to Point over Ethernet) RFC 2516
   C. Mô hình IP over ATM (RFC 1483R)
   D. Mô hình Ethernet over ATM (RFC 1483B)
7. Công nghệ truyền thoại qua mạng chuyển mạch gói:
   A. Tại phía phát, tín hiệu thoại được mã hóa bằng các bộ CODEC (Coder-Decoder). Bộ xử lý tín hiệu số DSP (Digital Signal Processing) sẽ nén các gói dữ liệu/. VAD (Voice Activity Detection) loại bỏ các khoảng lặng
   B. Tại bên thu, ngược lại, DSP sẽ giải nén các gói tin, CODEC giải mã các gói tin thành tín hiệu âm thanh tương tự. Các khoảng lặng được tái tạo để phát thông tin thoại cho người nghe.
   C. Cả hai phương pháp.

8. Các ưu điểm của truyền thoại qua mạng chuyển mạch gói
   - A. Tiết kiệm chi phí đầu tư hạ tầng mạng và chi phí sử dụng dịch vụ
   - B. Sử dụng hiệu quả băng thông với chất lượng dịch vụ QoS chấp nhận được.
   - C. Kết hợp các dịch vụ thoại, số liệu, video trên một mạng duy nhất
9. Các vấn đề về chất lượng dịch vụ QoS
   - A. Trễ (Delay)
   - B. Trượt (Jitter)
   - C. Mất gói (Packet Loss)
10. Các mô hình truyền thoại qua mạng chuyển mạch gói
    - A. Voice over Frame Relay - VoFR
    - B. Voice over ATM - VoATM
    - C. Voice over Internet Protocol - VoIP
11. Cấu trúc mạng MPLS gồm :
    - A. Bộ định tuyến biên LER gọi là bộ định tuyến PE
    - B. Bộ định tuyến lõi LSR được gọi là bộ định tuyến P
    - C. Cả hai phương pháp.
12. Ưu điểm của công nghệ MPLS:
    - A. Công nghệ MPLS đơn giản, có thể giải quyết các vấn đề phức tạp và khả năng mở rộng mạng.
    - B. Có thể thay thế công nghệ Frame Relay, ATM.
    - C. MPLS hội tụ những ưu điểm của cơ chế định tuyến IP và cơ chế hoán đổi nhãn của ATM
    - D. Giảm thiểu thời gian xử lý gói tin, không thay đổi các giao thức định tuyến IP.
    - E. Nhãn MPLS đơn giản, kích thước nhỏ và linh hoạt. Có thể xếp nối tiếp nhãn thành chồng nhãn. Rất tiện lợi cho việc đánh địa chỉ và truy tìm.
13. Hạn chế của MPLS:
    - A. MPLS không cung cấp dịch vụ đầu cuối (End-Point)
    - B. MPLS bị lỗi đường truyền cao hơn các công nghệ khác, giảm đi độ tin cậy.
    - C. Cả 2 khẳng định.
14. Các đặc trưng cơ bản của công nghệ chuyển mạch mềm như sau:
    - A. Dựa trên công nghệ chuyển mạch gói, thiết kế theo mô hình xử lý phân tán
    - B. Giao diện mở API
    - C. Phần mềm không phụ thuộc vào phần cứng chuyển mạch
    - D. Có khả năng lập trình được độc lập.
    - E. Tích hợp và liên kết các giao thức khác nhau trong mạng NGN và giữa NGN với mạng truyền thống (PSTN, ATM&IP…).
15. API trong Softswitch gồm:
    - A. API liên kết các nguồn tài nguyên mạng.
    - B. API liên kết các module có năng lực xử lý trong mạng
    - C. API liên kết NGN với môi trường ngoài

16. Công nghệ chuyển mạch mềm có những ưu điểm:
    A. Giải pháp phần mềm chung trên nhiều loại mạng khác nhau.
    B. Đơn giản cấu trúc hệ thống và linh hoạt khi thay đổi tính năng, cấu hình, mở rộng phát triển.
    C. Tích hợp và phát triển các phần mềm thông minh, khai thác tiềm năng của mạng trong tương lai.
    D. Dễ dàng tích hợp dịch vụ mới từ nhà cung cấp thứ ba đồng thời cho phép người sử dụng có thể tự phát triển ứng dụng và dịch vụ.

Câu hỏi và bài tập

1. Tổng quan về IDSL (ISDN DSL):
2. Tổng quan về HDSL (High Data Rate DSL):
3. Tổng quan về VDSL (Very High Data Rate DSL):
4. Tổng quan về ADSL (Asymmetric Digital Subscriber Line)
5. Tổng quan về ADSL2 và ADSL2+
6. Các vấn đề cơ bản công nghệ DSL trên mạng cáp đồng
7. Các phương pháp mã hóa đường truyền
8. Kỹ thuật phát hiện lỗi và sửa lỗi
9. Nhiễu xuyên âm đầu xa FEXT (Far - end Crosstalk)
10. Nhiễu xuyên âm đầu gần
11. Chống xuyên nhiễu
12. Phương pháp triệt tiếng vọng (EC)
13. Mô hình PPPoA (Point to Point over ATM)
14. Mô hình PPPoE (Point to Point over Ethernet) RFC 2516
15. Mô hình IP over ATM (RFC 1483R)
16. Mô hình Ethernet over ATM (RFC 1483B)
17. Truyền thoại qua mạng chuyển mạch gói VoPN (Voice over Packet Network)
18. Mô hình truyền thoại qua mạng chuyển mạch gói
19. Ưu điểm của truyền thoại qua mạng chuyển mạch gói
20. Các vấn đề về chất lượng dịch vụ QoS: Trễ , Trượt và mất gói
21. Voice over Frame Relay VoFR
22. Voice over ATM - VoATM
23. Voice over Internet Protocol - VoIP
24. Các thành phần chủ yếu của VoIP: Internet Protocol IP: Các chuẩn nén tín hiệu thoại
25. H.320, H.324 và POTS (Plain Old Telephone Service)
26. Vai trò, chức năng và các thành phần giao thức H.323
27. Giao thức SIP (Session Initial Protocol)
28. Real-time Transport Protocol RTP

29. Real-time Transport Control Protocol RTCP:
30. Resource Reservation Protocol RSVP
31. Giao thức MGCP (Media Gateway Control Protocol)
32. Giao thức Megaco/H.248
33. Kiến trúc và nguyên tắc hoạt động MPLS
34. Cấu trúc mạng MPLS
35. Nguyên tắc chuyển mạch nhãn MPLS
36. Cơ chế phân phối nhãn. Cơ chế xử lý nhãn và chuyển gói tin
37. Cơ chế điều khiển lưu lượng và chất lượng dịch vụ trong MPLS
38. Đánh giá công nghệ chuyển mạch nhãn đa giao thức MPLS:
39. So sánh MPLS với ATM. So sánh MPLS so với IP
40. Hạn chế của MPLS:
41. Cấu trúc và nguyên tắc chuyển mạch mềm
42. MEGACO/H.248/MGCP
43. RTP/RTCP/RTSP: Real Time Protocol/ Real Time Control Protocol-Real Time Streaming Protocol:
44. SCTP (Stream Control Transport Protocol) hay SIGTRAN (Signalling Transport)
45. SIP (Session Initiation Protocol)/H.323
46. Giao diện ứng dụng API trong chuyển mạch mềm
47. Các phương thức chia sẻ dữ liệu qua API:
48. Phân lớp các API trong Softswitch
49. Kế hoạch đánh số trong chuyển mạch mềm
50. Đánh giá công nghệ chuyển mạch mềm
51. So sánh công nghệ Softwwitch và chuyển mạch kênh.
52. Công nghệ chuyển mạch mềm có những ưu điểm nổi bật so với các công nghệ truyền thông khác.
53. Mạng hội tụ và mạng thế hệ sau NGN
54. Các nguyên tắc xây dựng mạng thế hệ sau NGN
55. NGN hội tụ những ưu điểm của công nghệ chuyển mạch kênh và chuyển mạch gói
56. Mô hình phân lớp và chức năng các lớp NGN
57. Vai trò và chức năng Lớp truy nhập (Access)
58. Vai trò và chức năng Lớp truyền tải (Transport)
59. Vai trò và chức năng Lớp ứng dụng/dịch vụ (Application/Service)
60. Vai trò và chức năng Lớp quản lý (Management)
61. Dịch vụ thẻ trả trước 1719, Dịch vụ gọi miễn cước 1800 (Freephone), Các dịch vụ đa phương tiện MMA, Các dịch vụ thông minh, Dịch vụ WEB trên NGN, Dịch vụ truy nhập Internet tốc độ cao, Dịch vụ mạng riêng ảo VPN,
62. NGN trong mạng viễn thông Việt Nam

CHƯƠNG 7: AN TOÀN MẠNG

Nội dung của chương này sẽ trình bày những vấn đề cơ bản về an toàn mạng bao gồm các đặc trưng kỹ thuật, các lỗ hổng và điểm yếu của mạng. Nghiên cứu các phương thức tấn công mạng phổ biến, các biện pháp an toàn mạng bằng kỹ thuật mật mã và Fire wall. Đặc biệt nội dung nghiên cứu mạng riêng ảo và vấn đề bảo mật trong mạng riêng ảo, các giao thức đặc trưng IPSEC, PPP, L2TP. Nội dung chương gồm các phần sau:

- Tổng quan về an ninh mạng.
- Một số kiểu tấn công mạng phổ biến.
- Biện pháp đảm bảo an ninh mạng
- Mạng riêng ảo

7.1. Tổng quan về an ninh mạng

7.1.1. An toàn mạng là gì?

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

An toàn mạng bao gồm:

Xác định chính xác các khả năng, nguy cơ xâm phạm mạng, các sự cố rủi ro đối với thiết bị, dữ liệu trên mạng để có các giải pháp phù hợp đảm bảo an toàn mạng.

Đánh giá nguy cơ tấn công của Hacker đến mạng, sự phát tán virus... Phải nhận thấy an toàn mạng là một trong những vấn đề cực kỳ quan trọng trong các hoạt động, giao dịch điện tử và trong việc khai thác sử dụng các tài nguyên mạng.

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

Sử dụng hiệu quả các công cụ bảo mật (ví dụ như Firewall ...) và những biện pháp, chính sách cụ thể chặt chẽ.

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

7.1.2. Các đặc trưng kỹ thuật của an toàn mạng

1. Xác thực (Authentification): Kiểm tra tính xác thực của một thực thể giao tiếp trên mạng. Một thực thể có thể là một người sử dụng, một chương trình máy tính, hoặc một thiết bị phần cứng. Các hoạt động kiểm tra tính xác thực được đánh giá là quan trọng nhất trong các hoạt động của một phương thức bảo mật. Một hệ thống thông thường phải thực hiện kiểm tra tính xác thực của một thực thể trước khi thực thể đó thực hiện kết nối với hệ thống. Cơ chế kiểm tra tính xác thực của các phương thức bảo mật dựa vào 3 mô hình chính sau:

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

Có thể phân loại bảo mật trên VPN theo các cách sau: mật khẩu truyền thống hay mật khẩu một lần; xác thực thông qua các giao thức (PAP, CHAP, RADIUS…) hay phần cứng (các loại thẻ card: smart card, token card, PC card), nhận diện sinh trắc học (dấu vân tay, giọng nói, quét võng mạc...).

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

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

4. Tính toàn vẹn (Integrity): Là đặc tính khi thông tin trên mạng chưa được uỷ quyền thì không thể tiến hành biến đổi được, tức là thông tin trên mạng khi đang lưu giữ hoặc trong quá trình truyền dẫn đảm bảo không bị xoá bỏ, sửa đổi, giả mạo, làm rối loạn trật tự, phát lại, xen vào một cách ngẫu nhiên hoặc cố ý và những sự phá hoại khác. Những nhân tố chủ yếu ảnh hưởng tới sự toàn vẹn thông tin trên mạng gồm: sự cố thiết bị, sai mã, bị tác động của con người, virus máy tính…

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

- Giao thức an toàn có thể kiểm tra thông tin bị sao chép, sửa đổi hay sao chép. Nừu phát hiện thì thông tin đó sẽ bị vô hiệu hoá.
- Phương pháp phát hiện sai và sửa sai. Phương pháp sửa sai mã hoá đơn giản nhất và thường dùng là phép kiểm tra chẵn - lẻ.
- Biện pháp kiểm tra mật mã ngăn ngừa hành vi xuyên tạc và cản trở truyền tin.
- Chữ ký điện tử: bảo đảm tính xác thực của thông tin.
- Yêu cầu cơ quan quản lý hoặc trung gian chứng minh tính chân thực của thông tin.

5. Tính khống chế (Accountlability): Là đặc tính về năng lực khống chế truyền bá và nội dung vốn có của tin tức trên mạng.

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

7.1.3. Các lỗ hổng và điểm yếu của mạng

1. Các lỗ hổng bảo mật hệ thống là các điểm yếu có thể tạo ra sự ngưng trệ của dịch vụ, thêm quyền đối với người sử dụng hoặc cho phép các truy nhập không hợp pháp vào hệ thống. Các lỗ hổng tồn tại trong các dịch vụ như Sendmail, Web,Ftp ... và trong hệ điều hành mạng như trong Windows NT, Windows 95, UNIX; hoặc trong các ứng dụng. Các loại lỗ hổng bảo mật trên một hệ thống được chia như sau:

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

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

Lỗ hổng loại A: Các lỗ hổng này cho phép người sử dụng ở ngoài cho thể truy nhập vào hệ thống bất hợp pháp. Lỗ hổng rất nguy hiểm, có thể làm phá hủy toàn bộ hệ thống.

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

7.1.4. Các biện pháp phát hiện hệ thống bị tấn công

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

1. Kiểm tra các dấu hiệu hệ thống bị tấn công: Hệ thống thường bị treo hoặc bị Crash bằng những thông báo lỗi không rõ ràng. Khó xác định nguyên nhân do thiếu thông tin liên quan. Trước tiên, xác định các nguyên nhân có phải phần cứng hay không, nếu không phải hãy nghĩ đến khả năng máy bị tấn công.

2. Kiểm tra các tài khoản người dùng mới lạ, nhất là ID của tài khoản đó bằng không.

3. Kiểm tra sự xuất hiện các tập tin lạ. Người quản trị hệ thống nên có thói quen đặt tên tập theo mẫu nhất định để dễ dàng phát hiện tập tin lạ. Dùng các lệnh Ls-l để kiểm tra thuộc tính Setuid và Setgid đối với những tập tinh đáng chú ý, đặc biệt là các tập tin Scripts.

4. Kiểm tra thời gian thay đổi trên hệ thống, đặc biệt là các chương trình Login, Sh hoặc các Scripts khởi động ...

5. Kiểm tra hiệu năng của hệ thống: Sử dụng các tiện ích theo dõi tài nguyên và các tiến trình đang hoạt động trên hệ thống như Ps hoặc Top ...

6. Kiểm tra hoạt động của các dịch vụ hệ thống cung cấp: Một trong các mục đích tấn công là làm cho tê liệt hệ thống (hình thức tấn công DoS). Sử dụng các lệnh như Ps, Pstat, các tiện ích về mạng để phát hiện nguyên nhân trên hệ thống.

7. Kiểm tra truy nhập hệ thống bằng các Account thông thường, đề phòng trường hợp các Âccount này bị truy nhập trái phép và thay đổi quyền hạn mà người sử dụng hợp pháp không kiểm soát được.

9. Kiểm tra các file liên quan đến cấu hình mạng và dịch vụ như /etc/inetd.conf; bỏ các dịch vụ không cần thiết; đối với những dịch vụ không cần thiết chạy dưới quyền Root thì không chạy bằng các quyền yếu hơn; ví dụ Fingerd chỉ chạy với quyền Nobody.

10. Kiểm tra các phiên bản của Sendmail, /bin/mail, ftp, fingerd; tham gia các nhóm tin về bảo mật để có thông tin về lỗ hổng của dịch vụ sử dụng

Các biện pháp này kết hợp với nhau tạo nên một chính sách về bảo mật đối với hệ thống. Chi tiết về phương thức và kế hoạch xây dựng một chính sách bảo mật sẽ được trình bày trong phần ba - xây dựng chính sách bảo mật.

7.2. Một số phương thức tấn công mạng phổ biến

7.2.1. Scanner

Kẻ phá hoạt sử dụng chương trình Scanner tự động rà soát và có thể phát hiện ra những điểm yếu lỗ hổng về bảo mật trên một Server ở xa Scanner là một chương trình trên một trạm làm việc tại cục bộ hoặc trên một trạm ở xa.

Các chương trình Scanner có thể rà soát và phát hiện các số hiệu cổng (Port) sử dụng trong giao thức TCP/UDP của tầng vận chuyển và phát hiện những dịch vụ sử dụng trên hệ thống đó, nó ghi lại những đáp ứng (Response) của hệ thống ở xa tương ứng với các dịch vụ mà nó phát hiện ra. Dựa vào những thông tin này, những kẻ tấn công có thể tìm ra những điểm yếu trên hệ thống. Chương trình Scanner có thể hoạt động được trong môi trường TCP/IP, hệ điều hành UNIX, và các máy tính tương thích IBM, hoặc dòng máy Macintosh.

Các chương trình Scanner cung cấp thông tin về khả năng bảo mật yếu kém của một hệ thống mạng. Những thông tin này là hết sức hữu ích và cần thiết đối với người quản trị mạng, nhưng hết sức nguy hiểm khi những kẻ phá hoại có thông tin này.

7.2.2. Bẻ khoá (Password Cracker)

Chương trình bẻ khoá Password là chương trình có khả năng giải mã một mật khẩu đã được mã hoá hoặc có thể vô hiệu hoá chức năng bảo vệ mật khẩu của một hệ thống. Hầu hết việc mã hoá các mật khẩu được tạo ra từ một phương thức mã hoá. Các chương trình mã hoá sử dụng các thuật toán mã hoá để mã hoá mật khẩu.Có thể thay thế phá khoá trên một hệ thống phần tán, đơn giản hơn so với việc phá khoá trên một Server cục bộ.

Một danh sách các từ được tạo ra và thực hiện mã hoá từng từ. Sau mỗi lần mã hoá, sẽ so sánh với mật khẩu (Password) đã mã hoá cần phá. Nếu không trùng hợp, quá trình lại quay lại. Phương thức bẻ khoá này gọi là Bruce-Force. Phương pháp này tuy không chuẩn tắc nhưng thực hiện nhanh vì dựa vào nguyên tắc khi đặt mật khẩu người sử dụng cũng thương tuân theo một số qui tắc để thuận tiện khi sử dụng.

Thông thường các chương trình phá khoá thường kết hợp một số thông tin khác trong quá trình dò mật khẩu như: thông tin trong tập tin /etc/passwd, từ điển và sử dụng các từ lặp các từ liệt kê tuần tự, chuyển đổi cách phát âm của một từ ...

Biện pháp khắc phục là cần xây dựng một chính sách bảo vệ mật khẩu đúng đắn.

7.2.3. Trojans

Một chương trình Trojan chạy không hợp lệ trên một hệ thống với vai trò như một chương trình hợp pháp. Nó thực hiện các chức năng không hợp pháp. Thông thường, Trojans có thể chạy được là do các chương trình hợp pháp đã bị thay đổi mã bằng những mã bất hợp pháp. Virus là một loại điển hình của các chương trình Trojans, vì các chương trình virus che dấu các đoạn mã trong những chương trình sử dụng hợp pháp. Khi chương trình hoạt động thì những đoạn mã ẩn sẽ thực hiện một số chức năng mà người sử dụng không biết.

Trojan có nhiều loại khác nhau. Có thể là chương trình thực hiện chức năng ẩn dấu, có thể là một tiện ích tạo chỉ mục cho file trong thưc mục, hoặc một đoạn mã phá khoá, hoặc cố thể là một chương trình xử lý văn bản hoặc một tiện ích mạng...

Trojan có thể lây lan trên nhiều môi trường hệ điều hành khác nhau. Đặc biệt thường lây lan qua một số dịch vụ phổ biến như Mail, FTP... hoặc qua các tiện ích, chương trình miễn phí trên mạng Internet. Hầu hết các chương trình FTP Server đang sử dụng là những phiên bản cũ, có nguy cơ tiềm tàng lây lan Trojans.

Đánh giá mức độ phá hoại của Trojans là hết sức khó khăn. Trong một số trường hợp, nó chỉ làm ảnh hương đến các truy nhập của ngwời sử dụng. Nghiêm trọng hơn, nó là những kẻ tán công lỗ hổng bảo mật mạng. Khi kẻ tấn công chiếm được quyền Root trên hệ thống, nó có thể phá huỷ toàn bộ hoặc một phần của hệ thống. Chúng sử dụng các quyền Root để thay đổi logfile, cài đặt các chương trình Trojans khác mà người quản trị không thể phát hiện được và người quản trị hệ thống đó chỉ còn cách là cài đặt lại toàn bộ hệ thống

7.2.4. Sniffer

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

7.3. Biện pháp đảm bảo an ninh mạng

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

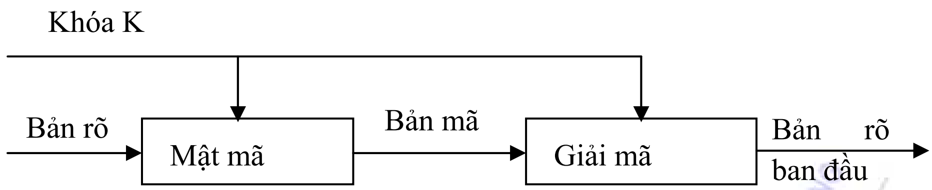
7.3.1. Tổng quan về bảo vệ thông tin bằng mật mã (Cryptography)

Mật mã là quá trình chuyển đối thông tin gốc sang dạng mã hóa (Encryption). Có hai cách tiếp cận để bảo vệ thông tin bằng mật mã: theo đường truyền (Link Oriented Security) và từ mút-đến-mút (End-to-End).

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

Ngược lại, trong cách thứ hai, thông tin được bảo vệ trên toàn đường đi từ nguồn tới đích. Thông tin được mã hoá ngay khi mới được tạo ra và chỉ được giải mã khi đến đích. Ưu điểm của tiếp cận này là người sử dụng có thể dùng nó mà không ảnh hưởng gì đến người sử dụng khác. Nhược điểm của phương pháp là chỉ có dữ liệu người sử dụng được mã hoá, còn thông tin điều khiển phải giữ nguyên để có thể xử lý tại các node.

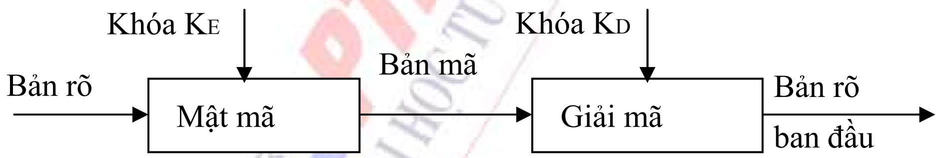
Giải thuật DES mã hoá các khối 64 bits của văn bản gốc thành 64 bits văn bản mật bằng một khoá. Khoá gồm 64 bits trong đó 56 bits được dùng mã hoá và 8 bits còn lại được dùng để kiểm soát lỗi. Một khối dữ liệu cần mã hoá sẽ phải trải qua 3 quá trình xử lý: Hoán vị khởi đầu, tính toán phụ thuộc khoá và hoán vị đảo ngược hoán vị khởi đầu.



Hình 7.1: Mô hình mật mã đối xứng

Phương pháp sử dụng khoá công khai (Public key): Các phương pháp mật mã chỉ dùng một khoá cho cả mã hoá lẫn giải mã đòi hỏi người gửi và người nhận phải biết khoá và giữ bí mật. Tồn tại chính của các phương pháp này là làm thế nào để phân phối khoá một cách an toàn, đặc biệt trong môi trường nhiều người sử dụng. Để khắc phục, người ta thường sử dụng phương pháp mã hoá 2 khoá, một khoá công khai để mã hoá và một mã bí mật để giải mã. Mặc dù hai khoá này thực hiện các thao tác ngược nhau nhưng không thể suy ra khoá bí mật từ khoá công khai và ngược lại nhờ các hàm toán học đặc biệt gọi là các hàm sập bẫy một chiều (trap door one-way functions). Đặc điểm các hàm này là phải biết được cách xây dựng hàm thì mới có thể suy ra được nghịch đảo của nó.

Giải thuật RSA dựa trên nhận xét sau: phân tích ra thừa số của tích của 2 số nguyên tố rất lớn cực kỳ khó khăn. Vì vậy, tích của 2 số nguyên tố có thể công khai, còn 2 số nguyên tố lớn có thể dùng để tạo khoá giải mã mà không sợ bị mất an toàn. Trong giải thuật RSA mỗi trạm lựa chọn ngẫu nhiên 2 số nguyên tố lớn p và q và nhân chúng với nhau để có tích n=pq (p và q được giữ bí mật).



Hình 7.2: Mô hình mật mã không đối xứng

7.3.2. Firewall

Firewall là một hệ thống dùng để tăng cường khống chế truy xuất, phòng ngừa đột nhập bên ngoài vào hệ thống sử dụng tài nguyên của mạng một cách phi pháp. Tất cả thông tin đến và đi nhất thiết phải đi qua Firewall và chịu sự kiểm tra của bức tường lửa. Nói chung Firewall có 5 chức năng lớn sau:

1. Lọc gói dữ liệu đi vào/ra mạng lưới.
2. Quản lý hành vi khai thác đi vào/ra mạng lưới
3. Ngăn chặn một hành vi nào đó.

4. Ghi chép nội dung tin tức và hoạt động thông qua bức tường lửa.
5. Tiến hành đo thử giám sát và cảnh báo sự tấn công đối với mạng lưới.

Ưu điểm và nhược điểm của bức tường lửa:

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

Nhược điểm là hạn chế dịch vụ có ích, vì để nâng cao tính an toàn mạng, người quản trị hạn chế hoặc đóng nhiều dịch vụ có ích của mạng. Không phòng hộ được sự tấn công của kẻ phá hoại trong mạng nội bộ, không thể ngăn chặn sự tấn công thông qua những con đường khác ngoài bức tường lửa. Firewall Internet không thể hoàn toàn phòng ngừa được sự phát tán phần mềm hoặc tệp đã nhiễm virus.

7.3.3. Các loại Firewall

Firewall lọc gói thường là một bộ định tuyến có lọc. Khi nhận một gói dữ liệu, nó quyết định cho phép qua hoặc từ chối bằng cách thẩm tra gói tin để xác định quy tắc lọc gói dựa vào các thông tin của Header để đảm bảo quá trình chuyển phát IP.

Firewall cổng mạng hai ngăn là loại Firewall có hai cửa nối đến mạng khác. Ví dụ một cửa nối tới một mạng bên ngoài không tín nhiệm còn một cửa nối tới một mạng nội bộ có thể tín nhiệm. Đặc điểm lớn nhất Firewall loại này là gói tin IP bị chặn lại.

Firewall che chắn (Screening) máy chủ bắt buộc có sự kết nối tới tất cả máy chủ bên ngoài với máy chủ kiên cố, không cho phép kết nối trực tiếp với máy chủ nội bộ. Firewall che chắn máy chủ là do bộ định tuyến lọc gói và máy chủ kiên cố hợp thành. Hệ thống Firewall có cấp an toàn cao hơn so với hệ thống Firewall lọc gói thông thường vì nó đảm bảo an toàn tầng mạng (lọc gói) và tầng ứng dụng (dịch vụ đại lý).

Firewall che chắn mạng con: Hệ thống Firewall che chắn mạng con dùng hai bộ định tuyến lọc gói và một máy chủ kiên cố, cho phép thiết lập hệ thống Firewall an toàn nhất, vì nó đảm bảo chức năng an toàn tầng mạng và tầng ứng dụng.

7.3.4. Kỹ thuật Fire wall

Lọc khung (Frame Filtering): Hoạt động trong tầng 2 của mô hình OSI, có thể lọc, kiểm tra được ở mức bit và nội dung của khung tin (Ethernet/802.3, Token Ring 802.5, FDDI,...). Trong tầng này các khung dữ liệu không tin cậy sẽ bị từ chối ngay trước khi vào mạng

Lọc gói (Packet Filtering): Kiểu Firewall chung nhất là kiểu dựa trên tầng mạng của mô hình OSI. Lọc gói cho phép hay từ chối gói tin mà nó nhận được. Nó kiểm tra toàn bộ đoạn dữ liệu để quyết định xem đoạn dữ liệu đó có thoả mãn một trong số các quy định của lọc Packet hay không. Các quy tắc lọc Packet dựa vào các thông tin trong Packet Header.

Nếu quy tắc lọc Packet được thoả mãn thì gói tin được chuyển qua Firewall. Nếu không sẽ bị bỏ đi. Như vậy Firewall có thể ngăn cản các kết nối vào hệ thống, hoặc khoá việc truy cập vào hệ thống mạng nội bộ từ những địa chỉ không cho phép.

Một số Firewall hoạt động ở tầng mạng (tương tự như một Router) thường cho phép tốc độ xử lý nhanh vì chỉ kiểm tra địa chỉ IP nguồn mà không thực hiện lệnh trên Router, không xác định địa chỉ sai hay bị cấm. Nó sử dụng địa chỉ IP nguồn làm chỉ thị, nếu một gói tin mang địa chỉ nguồn là địa chỉ giả thì nó sẽ chiếm được quyền truy nhập vào hệ thống. Tuy nhiên có nhiều biện pháp kỹ thuật có thể được áp dụng cho việc lọc gói tin nhằm khắc phục nhược điểm trên, ngoài trường địa chỉ IP được kiểm tra, còn có các thông tin khác được kiểm tra với các quy tắc được tạo ra trên Firewall, các thông tin này có thể là thời gian truy nhập, giao thức sử dụng, cổng ...

Firewall kiểu Packet Filtering có 2 loại:

a. Packet filtering Fire wall: Hoạt động tại tầng mạng của mô hình OSI hay tầng IP trong mô hình TCP/IP. Kiểu Firewall này không quản lý được các giao dịch trên mạng.

b. Circuit Level Gateway: Hoạt động tại tầng phiên (Session) của mô hình OSI hay tầng TCP trong mô hình TCP/IP. Là loại Firewall xử lý bảo mật giao dịch giữa hệ thống và người dùng cuối (VD: kiểm tra ID, mật khẩu...) loại Firewall cho phép lưu vết trạng thái của người truy nhập.

7.3.5. Kỹ thuật Proxy

Là hệ thống Firewall thực hiện các kết nối thay cho các kết nối trực tiếp từ máy khách yêu cầu.Proxy hoạt động dựa trên phần mềm. Khi một kết nối từ một người sử dụng nào đó đến mạng sử dụng Proxy thì kết nối đó sẽ bị chặn lại, sau đó Proxy sẽ kiểm tra các trường có liên quan đến yêu cầu kết nối. Nếu việc kiểm tra thành công, có nghĩa là các trường thông tin đáp ứng được các quy tắc đã đặt ra, nó sẽ tạo một cầu kết nối giữa hai node với nhau. Ưu điểm của kiểu Firewall loại này là không có chức năng chuyển tiếp các gói tin IP, và có thể điều khiển một cách chi tiết hơn các kết nối thông qua Firewall. Cung cấp nhiều công cụ cho phép ghi lại các quá trình kết nối. Các gói tin chuyển qua Firewall đều được kiểm tra kỹ lưỡng với các quy tắc trên Firewall, điều này phải trả giá cho tốc độ xử lý.

Khi một máy chủ nhận các gói tin từ mạng ngoài rồi chuyển chúng vào mạng trong, sẽ tạo ra một lỗ hổng cho các kẻ phá hoại (Hacker) xâm nhập từ mạng ngoài vào mạng trong. Nhược điểm của kiểu Firewall này là hoạt động dựa trên trình ứng dụng uỷ quyền (Proxy).

7.4. Mạng riêng ảo VPN (Virtual Private Networks)

7.4.1. Khái niệm mạng riêng ảo

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

Mạng riêng ảo là một mạng máy tính, trong đó các điểm của khách hàng được kết nối với nhau trên một cơ sở hạ tầng chia sẻ với cùng một chính sách truy nhập và bảo mật như trong mạng riêng. Có 2 dạng chính mạng riêng ảo VPN là: Remote Access VPN , Site - to - Site VPN (Intranet VPN và Extranet VPN).

Remote Access VPN (Client - to - LAN VPN) cho phép thực hiện các kết nối truy nhập từ xa đối với người sử dụng di động (máy tính cá nhân hoặc các Personal Digital Assistant) với mạng chính (LAN hoặc WAN) qua đường quay số, ISDN, đường thuê bao số DSL.

Site- to - Site VPN dùng để kết nối các mạng tại các vị trí khác nhau thông qua kết nối VPN. Có thể chia loại này ra 2 loại khác: Intranet VPN và Extranet VPN. Intranet VPN kết nối các văn phòng ở xa với trụ sở chính thường là các mạng LAN với nhau. Extranet VPN là khi Intranet VPN của một khách hàng mở rộng kết nối với một Intranet VPN khác.

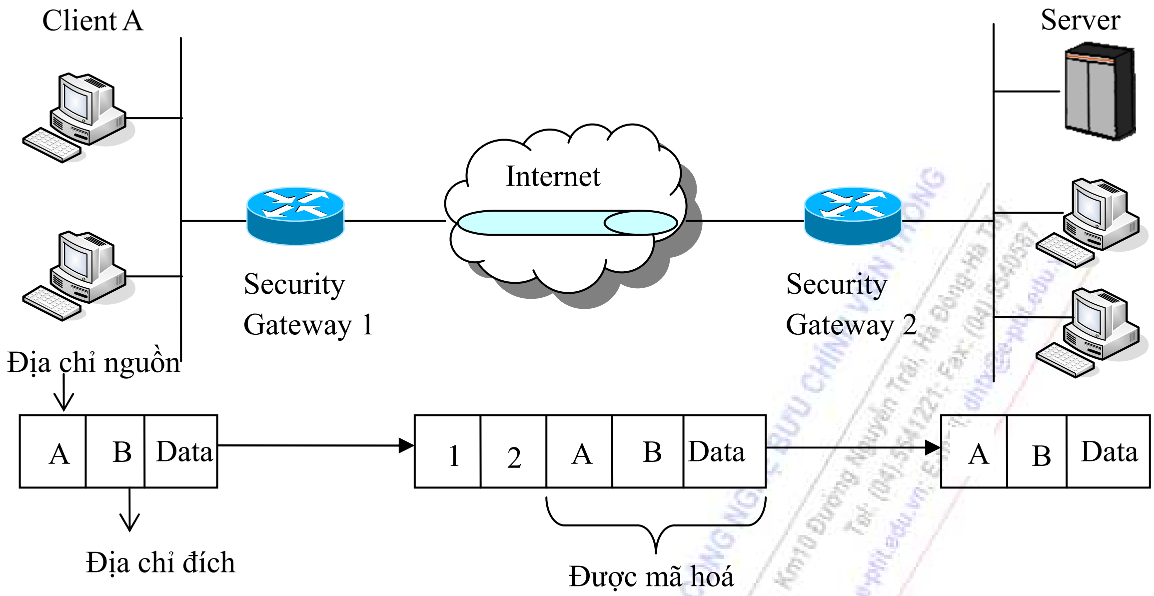
Bảo mật là một yếu tố quan trọng bảo đảm cho VPN hoạt động an toàn và hiệu quả. Kết hợp với các thủ tục xác thực người dùng, dữ liệu được bảo mật thông qua các kết nối đường hầm (Tunnel) được tạo ra trước khi truyền dữ liệu. Tunnel là kết nối ảo điểm - điểm (Point to Point) và làm cho mạng VPN hoạt động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

Chất lượng dịch vụ QoS, các thoả thuận (Service Level Agreement-SLA) với các ISP liên quan đến độ trễ trung bình của gói trên mạng, hoặc kèm theo chỉ định về giới hạn dưới của băng thông. Bảo đảm cho QoS là một việc cần được thống nhất về phương diện quản lý đối với các ISP. Tất cả các giao thức sử dụng trong mạng VPN, các gói dữ liệu IP được mã hoá (RSA RC-4 trong PPTP hoặc mã khóa công khai khác trong L2TP, IPSec) và sau đó đóng gói (ESP), thêm tiêu đề IP mới để tạo đường hầm trên mạng IP công cộng. Như vậy, khi gói tin MTU bị thất lạc trên mạng IP công cộng thì thông tin trong đó đã được mã hoá nên kẻ phá hoại khó có thể dò tìm thông tin thực sự chứa trong bản tin. Trong các giao thức PPTP và L2TP, mã hoá gói tin đã được thực hiện từ người dùng cho đến máy chủ của VPN. Việc mất mát gói tin dẫn đến việc phải truyền lại toàn bộ gói tin, điều này gây nên độ trễ chung đối với VPN và ảnh hưởng đến QoS của mạng VPN.

7.4.2. Kiến trúc của mạng riêng ảo

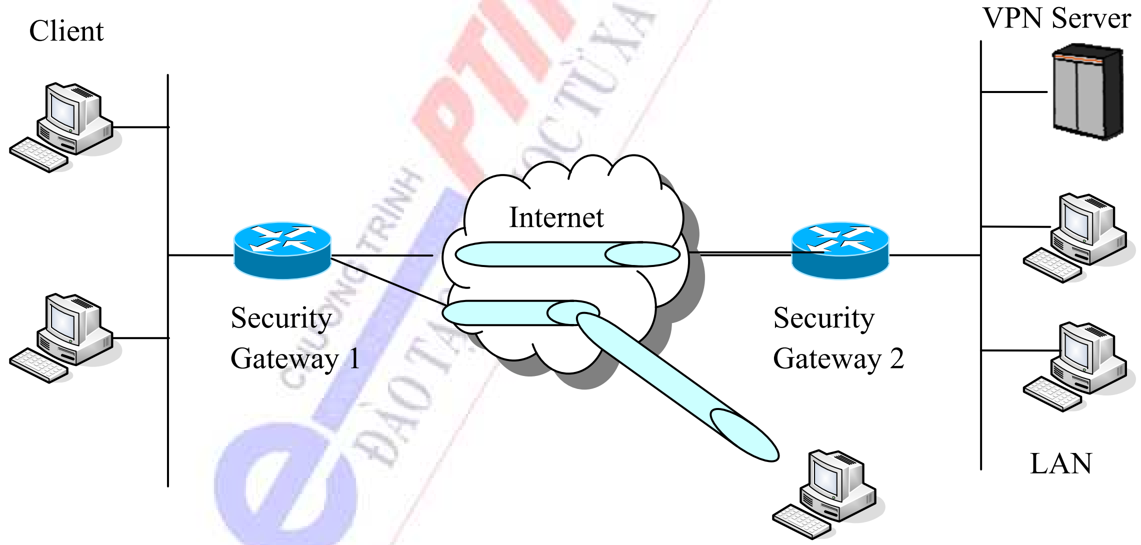
Hai thành phần cơ bản của Internet tạo nên mạng riêng ảo VPN, đó là:

- Đường hầm (Tunnelling) cho phép làm "ảo" một mạng riêng.
- Các dịch vụ bảo mật đa dạng cho phép dữ liệu mang tính riêng tư.



Hình 7.3: Cấu trúc một đường hầm

Đường hầm: là kết nối giữa 2 điểm cuối khi cần thiết. Khi kết nối này sẽ được giải phóng khi không truyền dữ liệu dành băng thông cho các kết nối khác. Kết nối này mang tính lôgích "ảo" không phụ thuộc vào cấu trúc vật lý của mạng. Nó che giấu các các thiết bị như bộ định tuyến, chuyển mạch và trong suốt đối với người dùng.



Hình 7.4: Đường hầm trong các cấu trúc LAN và Client.

Đường hầm được tạo ra bằng cách đóng gói các gói tin (Encapsulate) để truyền qua Internet. Đóng gói có thể mã hoá gói gốc và thêm vào tiêu đề IP mới cho gói. Tại điểm cuối, cổng

Định dạng gói tin tạo đường hầm: IP Header, AH, ESP, Tiêu đề và dữ liệu.

Đường hầm có 2 loại: Thường trực (Permanent) và tạm thời (Temporary hay Dynamic). Thông thường các mạng riêng ảo VPN sử dụng dạng đường hầm động. Đường hầm động rất hiệu quả cho VPN, vì khi không có nhu cầu trao đổi thông tin thì được huỷ bỏ. Đường hầm có thể kết nối 2 điểm cuối theo kiểu LAN- to - LAN tại các cổng bảo mật (Security Gateway), khi đó người dùng trên các LAN có thể sự dụng đường hầm này. Còn đối với trường hợp Client- to - LAN, thì Client phải khởi tạo việc xây dựng đường hầm trên máy người dùng để thông tin với cổng bảo mật để đến mạng LAN đích.

7.4.3. Những ưu điểm của mạng VPN

Chi phí: Công nghệ VPN cho phép tiết kiệm đáng kể chi phí thuê kênh riêng hoặc các cuộc gọi đường dài bằng chi phí cuộc gọi nội hạt. Hơn nữa, sử dụng kết nối đến ISP còn cho phép vừa sử dụng VPN vừa truy nhập Internet. Công nghệ VPN cho phép sử dụng băng thông đạt hiệu quả cao nhất. Giảm nhiều chi phí quản lý, bảo trì hệ thống.

Tính bảo mật: Trong VPN sử dụng cơ chế đường hầm (Tunnelling) và các giao thức tầng 2 và tầng 3, xác thực người dùng, kiểm soát truy nhập, bảo mật dữ liệu bằng mã hoá, vì vậy VPN có tính bảo mật cao, giảm thiểu khả năng tấn công, thất thoát dữ liệu.

Truy nhập dễ dàng: Người sử dụng trên VPN, ngoài việc sử dụng các tài nguyên trên VPN còn được sử dụng các dịch vụ khác của Internet mà không cần quan tâm đến phần phức tạp ở tầng dưới.

7.4.4. Giao thức PPTP (Point to Point Tunnelling Protocol)

PPP là giao thức tầng 2-Data link, truy nhập mạng WAN như HDLC, SDLC, X.25, Frame Relay, Dial on Demand. PPP có thể sử dụng cho nhiều giao thức lớp trên như TCP/IP, Novell/IPX, Apple Talk nhờ sử dụng NCP - Network Control Protocol. PPP sử dụng Link Control Protocol để thiết lập và điều khiển các kết nối. PPP sử dụng giao thức xác thực PAP hoặc CHAP.

PPTP dựa trên PPP để thực thi các chức năng sau:

- Thiết lập và kết thúc kết nối vât lý.
- Xác thực người dùng
- Tạo gói dữ liệu PPP.

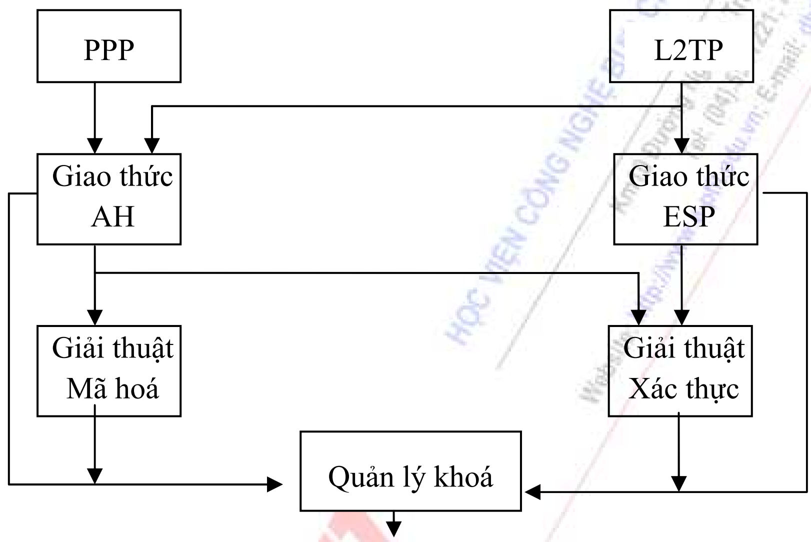
7.4.5. Giao thức L2F (Layer Two Forwarding Protocol)

Giao thức L2FP do hãng Cisco phát triển, dùng để truyền các khung SLIP/PPP qua Internet. L2F hoạt động ở tầng 2 (Data Link) trong mô hình OSI. Cũng như PPTP, L2F được thiết kế như là một giao thức Tunnel, sử dụng các định nghĩa đóng gói dữ liệu riêng của nó để truyền các gói tin ở mức 2. Một sự khác nhau giữa PPTP và L2F là tạo Tunnel trong giao thức L2F không phụ thuộc vào IP và GRE, điều này cho phép nó làm việc với các môi trường vật lý khác nhau.

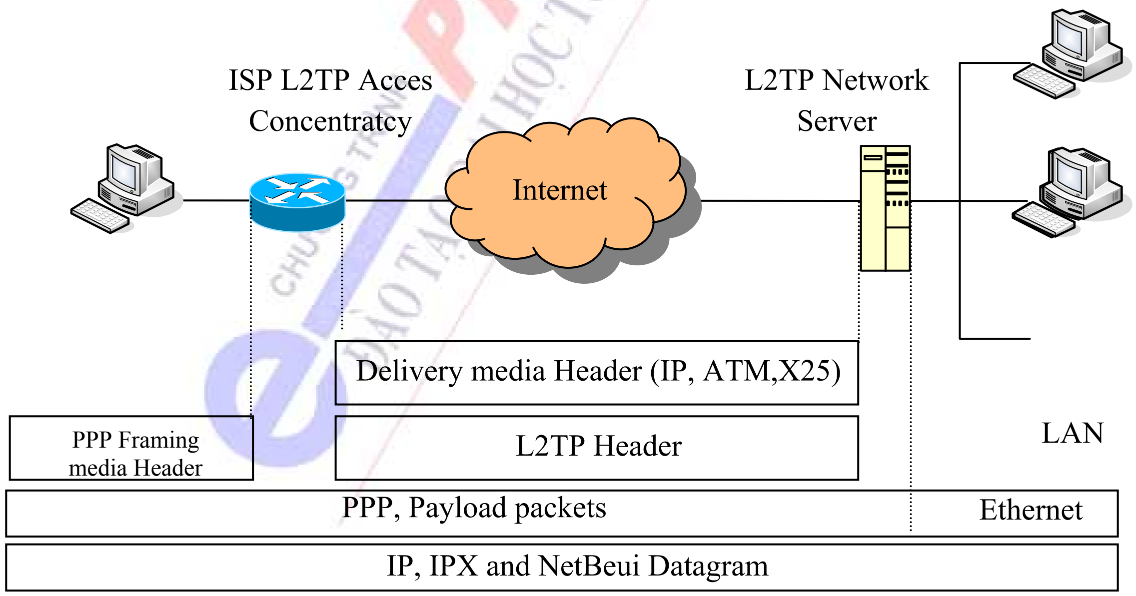
Cũng như PPTP, L2F sử dụng chức năng của PPP để cung cấp một kết nối truy cập từ xa và kết nối này có thể được đi qua một tunnel thông qua Internet để tới đích. Tuy nhiên L2TP định nghĩa giao thức tạo tunnel riêng của nó, dựa trên cơ cấu của L2F. Cơ cấu này tiếp tục định nghĩa việc truyền L2TP qua các mạng chuyển mạch gói như X25, Frame Relay và ATM. Mặc dù nhiều cách thực hiện L2TP tập trung vào việc sử dụng giao thức UDP trên mạng IP, ta vẫn có khả năng thiết lập một hệ thống L2TP không sử dụng IP. Một mạng sử dụng ATM hoặc Frame Relay cũng có thể được triển khai cho các tunnel L2TP.

7.4.6. Giao thức L2TP (Layer Two Tunnelling Protocol)

Giao thức L2TP được sử dụng để xác thực người sử dụng Dial-up và Tunnel các kết nối SLIP/PPP qua Internet. Vì L2TP là giao thức lớp 2, nên hỗ trợ cho người sử dụng các khả năng mềm dẻo như PPTP trong việc truyền tải các giao thức không phải là IP, ví dụ như là IPX và NETBEUI.



Hình 7.5: Kiến trúc của L2TP.



Hình 7.6: Quá trình chuyển gói tin qua Tunnel L2TP

Bảo mật trong L2TP: Việc xác thực người dùng trong 3 giai đoạn: Giai đoạn 1 tại ISP, giai đoạn 2 và giai đoạn 3 (tuỳ chọn) tại máy chủ mạng riêng. Trong giai đoạn 1, ISP có thể sử dụng số điện thoại của người dùng hoặc tên người dùng để xác định dịch vụ L2TP và khởi tạo kết nối đường hầm đến máy chủ của VPN. Khi đường hầm được thiết lập, LAC của ISP chỉ định một số nhận dạng cuộc gọi (Call ID) mới để định dạnh cho kết nối trong đường hầm và khởi tạo phiên làm việc bằng cách chuyển thông tin xác thực cho máy chủ VPN. Máy chủ VPN tiến hành tiếp bước 2 là quyết định chấp nhận hay từ chối cuộc gọi dựa vào các thông tin xác thực từ cuộc gọi của ISP chuyển đến. Thông tin đó có thể mang CHAP, PAP, EAP hay bất cứ thông tin xác thực nào. Sau khi cuộc gọi được chấp nhận, máy chủ VPN có thể khởi động giai đoạn 3 tại lớp PPP, bước náy tương tự như máy chủ xác thực một người dùng quay số truy nhập vào thăngr máy chủ.

Việc sử dụng các giao thức xác thực đơn giản nhưng không bảo mật cho các luồng dữ liệu điều khiển và thông báo dữ liệu tạo kẽ hở cho việc chèn gói dữ liệu để chiếm quyền điều khiển đường hầm, hay kết nối PPP, hoạc phá vỡ việc đàm phán PPP, lấy cắp mật khẩu người dùng. Mã hoá PPP không có xác thực địa chỉ, toàn vẹn dữ liệu, quản lý khoá nên bảo mật này yếu không an toàn trong kênh L2TP. Vì vậy, để có được xác thực như mong muốn, cần phải phân phối khoá và có giao thức quản lý khoá. Về mã hoá, sử dụng IPSec cung cấp bảo mật cao để bảo vệ gói mức IP, tối thiểu cũng phải được thực hiện cho L2TP trên IP. Việc quản lý khoá được thực hiện thông qua liên kết bảo mật - Security Association(SA). SA giúp 2 đối tượng truyền thông xác định phương thức mã hoá, nhưng việc chuyển giao khoá lại do IKE thực hiện. Nội dung này sẽ được nói rõ hơn trong giao thức IPSec.

7.4.7. Giao thức IPSEC

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

*** Xác thực tiêu đề AH:** AH một trong những giao thức bảo mật IPsec đảm bảo tính toàn vẹn cho tiêu đề gói và dữ liệu cũng như việc chứng thực người sử dụng. Nó đảm bảo chống phát lại và chống xâm nhập trái phép như một tùy chọn. Trong những phiên bản đầu của IPsec đóng gói bảo mật tải ESP chỉ thực hiện mã hóa mà không có chứng thực nên AH và ESP được dùng kết hợp còn ở những phiên bản sau ESP đã có thêm khả năng chứng thực. Tuy nhiên AH vẫn được dùng do đảm bảo việc chứng thực cho toàn bộ tiêu đề và dữ liệu cũng như việc đơn giản hơn đối với truyền tải dữ liệu trên mạng IP chỉ yêu cầu chứng thực.

AH có hai chế độ: Transport và Tunnel. Chế độ Tunnel AH tạo ra tiêu đề IP cho mỗi gói còn ở chế độ Transport AH không tạo ra tiêu đề IP mới. Hai chế độ AH luôn đảm bảo tính toàn vẹn (Integrity), chứng thực (Authentication) cho toàn bộ gói.

*** Xử lý đảm bảo tính toàn vẹn:** IPsec dùng thuật toán mã chứng thực thông báo băm HMAC (Hash Message Authentication Code) thường là HMAC-MD5 hay HMAC-SHA-1. Nơi phát giá trị băm được đưa vào gói và gửi cho nơi nhận. Nơi nhận sẽ tái tạo giá trị băm bằng khóa chia sẻ và kiểm tra sự trùng khớp giá trị băm qua đó đảm bảo tính toàn vẹn của gói dữ liệu. Tuy nhiên IPsec không bảo vệ tính toàn vẹn cho tất cả các trường trong tiêu đề của IP. Một số trường trong tiêu đề IP như TTL (Time to Live) và trường kiểm tra tiêu đề IP có thể thay đổi trong quá trình truyền. Nếu thực hiện tính giá trị băm cho tất cả các trường của tiêu đề IP thì những trường đã nêu ở trên sẽ bị thay đổi khi chuyển tiếp và tại nơi nhận giá trị băm sẽ bị sai khác. Để giải quyết vấn đề này giá trị băm sẽ không tính đến những trường của tiêu đề IP có thể thay đổi hợp pháp trong quá trình truyền.

*** ESP cũng có hai chế độ:** Transport và Tunnel. Chế độ Tunnel ESP tạo tiêu đề IP mới cho mỗi gói. Chế độ này có thể mã hóa và đảm bảo tính toàn vẹn của dữ liệu hay chỉ thực hiện mã hóa toàn bộ gói IP gốc. Việc mã hóa toàn bộ gói IP (gồm cả tiêu đề IP và tải IP) giúp che được địa chỉ cho gói IP gốc. Chế độ Transport ESP dùng lai tiêu đề của gói IP gốc chỉ mã hóa và đảm bảo tính toàn vẹn cho tải của gói IP gốc. Cả hai chế độ chứng thực để đảm bảo tính toàn vẹn được lưu ở trường ESP Auth.

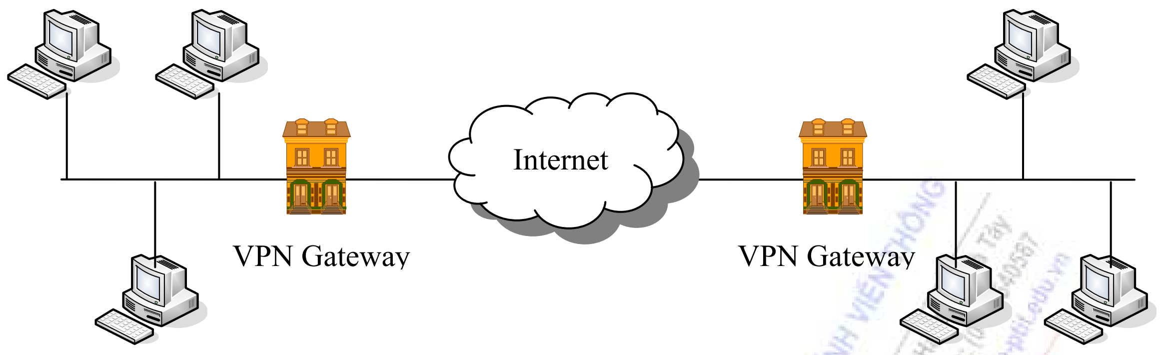
*** Xử lý mã hóa:** ESP dùng hệ mật đối xứng để mã hóa gói dữ liệu, nghĩa là thu và phát đều dùng cùng một loại khóa để mã hóa và giải mã dữ liệu. ESP thường dùng loại mã khối AES-CBC (AES-Cipher Block Chaining), AES-CTR (AES Counter Mode) và 3DES

*** Trao đổi khóa mã hóa IKE (Internet Key Exchange):** Trong truyền thông sử dụng giao thức IPsec phải có sự trao đổi khóa giữa hai điểm kết cuối, do đó đòi hỏi phải có cơ chế quản lý khóa. Có hai phương thức chuyển giao khóa đó là chuyển khóa bằng tay và chuyển khóa bằng giao thức IKE. Một hệ thống IPsec phụ thuộc phải hỗ trợ phương thức chuyển khóa băng tay. Phương thức chìa khóa trao tay chẳng hạn khóa thương mại ghi trên giấy. Phương thức này chỉ phù hợp với số lượng nhỏ các Site, đối với mạng lớn phải thực hiện phương thức quản lý khóa tự động. Trong IPsec người ta dùng giao thức quản lý chuyển khóa IKE (Internet Key Exchange). IKE có các khả năng sau :

- Cung cấp các phương tiện cho 2 bên sử dụng các giao thức, giải thuật và khóa.
- Đảm bảo ngay từ lúc bắt đầu chuyển khóa.
- Quản lý các khóa sau khi chúng được chấp nhận trong tiến trình thỏa thuận.
- Đảm bảo các khóa được chuyển một cách bảo mật.

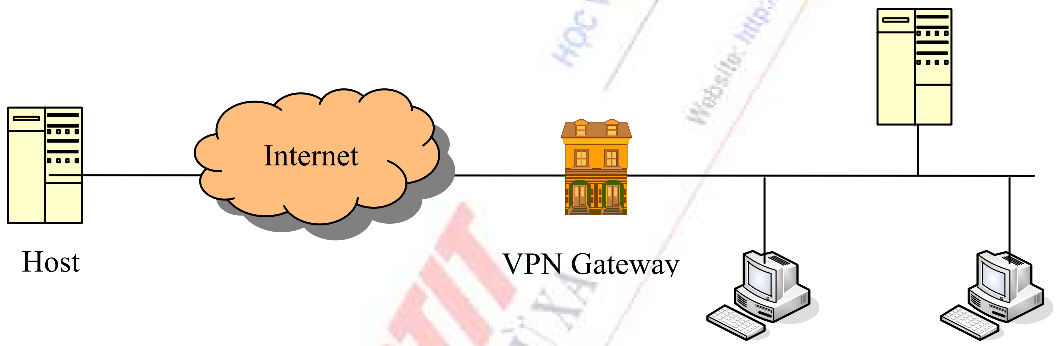
7.4.8. Ứng dụng ESP và AH trong cấu hình mạng

*** ESP trong cấu hình Gateway-to-Gateway:** Trong cấu hình này sẽ thiết lập kết nối có IPsec để mã hoá và đảm bảo tính toàn vẹn của dữ liệu giữa hai điểm A và B (điểm kết cuối A dùng Gateway A trên mạng A, điểm kết cuối B dùng Gateway B trên mạng B).



Hình 7.7 Cấu hình Gateway -to-Gateway

*** ESP và AH trong cấu hình Host-to-Host:** Trong cấu hình này sẽ thiết lập kết nối có IPsec để mã hoá và đảm bảo tính toàn vẹn của dữ liệu giữa hai điểm A và B. Tuỳ thuộc và nhu cầu bảo mật có thể dùng ESP hay AH.



Hình 7.8 Cấu hình Host-to-Host

7.4.9. So sánh các giao thức VPN

Giao thức	Ưu điểm	Nhược điểm	Sử dụng trong mạng
IPSec	Chuẩn giao thức rãnh. Hoạt động độc lập cho các ứng dụng mức caohơn. Giấu địa chỉ mạng không sử dụng dịch địa chỉ mạng NAT. Đáp ứng sự phát triển các kỹ thuật mã hoá .	Không quản lý NSD. Không khả năng tương tác giữa các nhà cung cấp. Không hỗ trợ giao diện. (Desktop support)	Phần mềm tốt nhất cho các giải pháp độc quyền của nhà cung cấp đối với việc truy nhập từ xa bằng quay số.

PPTP	Chạy trên Wind NT, 95 ,98. Cung cấp End to End và định hướng đường hầm kết nối node - to - node. Các đặc điểm giá trị được thêm vào phổ biến cho truy cập từ xa. Xác thực trên nền Windows. Có khả năng đa giao thức. Sử dụng mã hoá RSA RC-4.	Không cung cấp mã hoá dữ liệu từ những máy chủ truy cập từ xa. Mang tính độc quyền, yêu cầu máy chủ chạy Win NT để kết thúc những đường hầm. Chỉ sử dụng mã hoá RSA RC- 4.	Được dùng tại các máy chủ truy nhập từ xa định đường hầm proxy. Có thể được dùng giữa các văn phòng ở xa có máy chủ Win NT để chạy máy chủ truy cập từ xa và định tuyến RRAS. Có thể dùng cho những máy để bàn Win9x hay máy trạm dùng Win NT.
L2F	Cho phép định đường hầm đa giao thức. Có nhiều nhà cung cấp.	Không có mã hoá Xác thực NSD yếu. Không điều khiển luồng cho đường hầm.	Dùng cho truy cập từ xa tại POP.
L2TP	Kết hợp PPTP và L2TP. Chỉ cần một gói dựa trên mạng để chạy trên X.25 và Frame Relay. Sử dụng IPSec iệc mã hoá.	Chưa được cung cấp trong nhiều sản phẩm. Không bảo mật ở giai đoạn cuối.	Dùng cho truy nhập từ xa tại POP.

Câu hỏi và bài tập

1. Tổng quan về an ninh mạng
2. An toàn mạng là gì
3. Các đặc trưng kỹ thuật của an toàn mạng
4. Xác thực (Authentification), Tính khả dụng (Availability), Tính bảo mật (Confidentialy), Tính toàn vẹn (Integrity), Tính khống chế (Accountlability)
5. Các lỗ hổng và điểm yếu của mạng: Lỗ hổng loại C, Lổ hổng loại B, Lỗ hổng loại A
6. Các phương thức tấn tân công mạng
7. Các biện pháp phát hiện hệ thống bị tấn công
8. Một số phương thức tấn công mạng phổ biến: Scanner, Bẻ khoá (Password Cracker), Trojans, Sniffer
9. Tổng quan về bảo vệ thông tin bằng mật mã (Cryptography)
10. Firewall, ưu điểm và nhược điểm của Fire wall
11. Các loại Firewall
12. Kỹ thuật Fire wall

13. Kỹ thuật Proxy
14. Mạng riêng ảo VPN (Virtual Private Networks): khái niệm mạng riêng ảo và kiến trúc của mạng riêng áo
15. Các thành phần cơ bản của mạng riêng ảo VPN:
16. Những ưu điểm của mạng VPN
17. Giao thức PPTP (Point to Point Tunnelling Protocol)
18. Quá trình kết nối của PPTP: Tạo kết nối PPP, tạo kết nối điều khiển PPTP, Truyền dữ liệu qua Tunnel PPTP
19. Bảo mật trong PPTP
20. Giao thức L2F (Layer Two Forwarding Protocol)
21. Giao thức L2TP (Layer Two Tunnelling Protocol)
22. Bảo mật trong L2TP
23. Giao thức IPSEC
24. Ứng dụng ESP và AH trong cấu hình mạng
25. So sánh các giao thức VPN

CÁC TỪ VIẾT TẮT

AAL	ATM Adaptation Layer
ANSI	American National Standard Institute
ABM	Asynchronous Balance Mode
ACK	Acknowledgement
ACSE	Association Control Service Element
ADCCP	Advanced Data Communication Control Procedures
AE	Application Element
AFI	Authority and Format Identifier.
AFP	AppleTalk Filing Protocol.
AIX	Advanced Interactive Executive
ALU	Aritmetic Unit
AM	Amplitude Modulation
ANSI	American National Standard Institute
APDU	Application Protocol Data Unit
API	Application Program Interface
APPC	Advanced Program to Program Communications
APPN	Advanced Peer to Peer Networking
ARCnet	Attached Resolution Protocol
ARP	Address Resolution Protocol.
ARPA	Advanced Research Projects Agency
ARQ	Automatic Repeat Request
ASCII	American Standard Code For Information Interchange
ASDU	Application Service Data Unit
ASE	Application Service Element
ASM	Address Space Manager
ASN.1	Abstract Syntax Notion One

ASP	AppleShere Protocol.
AS	Autonomous System
ATM	Asynchronouse Transfer Mode
ATP	AppleTalk Transaction Protocol
BBS	Bulletin Broad System
BCC	Block Check Character
BCS	Basic Combined Subnet
BECN	Backward explicit Congestion Notification
BER	Basic Wncoding Rules
BERT	Bit Error Ratio Test
B-ISDN	Broadband Intergrated Services Digital Network.
BGP	Border Gateway Protocol
BRI	Basic Rate Interface.
CASE	Common Application Service Element
CATV	Community Antena Television
CCITT	International and Telephone Consultative Committe.
CCRSE	Commitment, Concurrency and Recovery Service Element
CD-ROM	Computer Disk Read Only Memory.
CEPT	Conference of European Postal and Telecommunications Administration
CICS	Customer Information Control System.
CLNP	Connectionless Network Servicess
CLNS	Connectionless Mode Network Service
CMIP	Common Management Information Protocol.
CMOT	CMIP Over TCP/IP.
CRC	Cyclic Redundancy Code.
CSMA/CA	Carrier Sense Multiple Access / Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access / Collision Dectection
CSU/DSU	Channel Service Unit/Digital Service Unit
CSU/DSU	Channel Services Network/Digital Services Unit.
C/R	Command/ Request

DAP	Data Access Protocol.
DAS	Dual Attached Stations.
DCE	Data Circuit Terminating Equipment
DDCMP	Digital Data Communication Message Protocol
DDCMP	Digital Data Communications Protocol.
DDM	Distributed Data Management
DDM	Distributed Data Management.
DES	Dataencryption Standard.
DFC	Data Flow Control.
DHCP	Dynamic Host Configuable Protocol.
DIA	Document Interchange Architecture.
DIA	Document Interchange Architecture.
DIP	Dual In Line Packege
DIX	Digital Intel Xerox.
DLC	Data Link Control
DE	Discard Eligibility
DLE	Data Link Escape.
DMA	Direct Memory Mapping.
DNA	Digital Network Architecture.
DNS	Domain Name System.
DNS-MX	Mail Routing and the Domain System.
DOD	Derpartment Of Defense.
DQDB	Distributed Queue Dual Bus.
DS	Directory Services.
DSP	Domain Specific Part.
DTAM	Document Transfer, Access and Management.
DTE	Data Terminal Equipment.
DTP	Distributed Transaction Processing.
EA	Extend Address
EBCDIC	Extended Binary Coded Decimal Interchange Code.

EGP	Exterior Gateway Protocol
ECMA	European Computer Manufacturers Association.
EIA	Electronic Industries Association
FECN	Forward Explicit Congestion Notification
FCS	Frame Check Sequence.
FDDI	Fiber Distributed Data Interface.
FDM	Frequency Division Multipling.
FEA	Frame Relay Adaptor.
FM	Frequency Modulation.
FR	Frame Relay
FRAD	Frame Relay Access Device
FRND	Frame Relay Network Device
FR UNI	Frame Relay User to Network Interface
FTAM	File Transfer Access and Management.
FTP	File Transfer Protocol.
GGP	Gateway to gateway Protocol.
GOSIP	Goverment OSI Profil.
HDLC	High Level Data Link Control.
HIPPI	High Performance Parellet Interface.
HTML	Hyper Text Markup Language.
HTTP	Hyper Text Transfer Protocol.
IA5	International Alphalbet Number 5.
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol.
IDI	Initial Domain Identifier.
IDP	Initial Domain Part.
IEEE	Institute of Electrical and Electric Engineers.
IETF	Internet Engineering Task Force
IGP	Interior Gateway Protocol.
IMS	Information Management System.

INTERNIC	Internet Netwowrk Information Center.
IP	Internet Protocol.
IPL	Initial Program Load.
IPX	Internetwork Packet Exchange.
ISA	Industry Standard Architecture .
ISDN	Intergrated Services Digital Network
ISO	International Standard Organization.
ISP	Internet Service Provider
ITU	International Telecommunications Union.
JTM	Job Transfer and Management.
LAN	Local Area Network.
LAP-B	Link Access Procedure Balanced
LAP-D	Link Access Procedure Dchannel.
LED	Ligh Emiting Diode.
LLAP	LocalTalk Link Access Protocol.
LLC	Logical Link Control.
LPDU	Link Protocol Data Unit.
LSAP	Link SAP.
LSDU	Link Service Data Unit.
LSL	Link Support Layer.
LU	Logical Unit.
MAC	Media Access Control.
MAN	Metropolitan Area network.
MAP	Manufacturing Automation Protocol.
MAU	Multistation Access Unit.
MCA	Micro Channel Architecture.
MHS	Message Handling System.
MIB	Management Information Base.
MLID	Multiple Link Interface Driver.
MMS	Manufacturing Messaging Service.

MODEM	Mudulation Demodulation.
MUX	Multiplexer.
NAK	Negative Acknowledgment.
NAU	Network Addressable Unit.
NAU	Network Address Unit.
NBS	National Bureau of Standard.
NCP	Netware Core Protocol.
NDS	Network Operating System.
NFS	Network File System.
NFS	Network File System.
NIC	Network Interface Card.
NLM	Netware Loadable Modules.
NLSP	Network Link Services Protocol.
NMS	Network Management System.
NNI	Network to Network Interface
NPDU	Network Protocol Data unit.
NREN	National Research and Education Network.
NRM	Normal Response Mode
NRZ	Non Return to Zero.
NS	Network Services.
NSAP	Network SAP.
NSDU	Network Service Data Unit.
NSP	Network Services Protocol.
NAT	Network Address Translation
NFS	Network File System
NIS	Network Information System
NVTS	Network Virtual Terminal Service.
OC	Optical Carrier.
ODI	Open Data Link Interface.
ODIF	Office Document Interchane Format.

OPA	Office Document Architecture.
OS	Operating System.
OSF	Open Software Foundation.
OSI	Open Systems Interconnection..
OSPF	Open Shortest Path First.
PA	Point of P Attachement.
PAD	Packet Assembler Disassembler.
PAP	Printer Access Protocol.
PBX	Pripheral Component Interconnection.
PDN	Public Data Network.
PDU	Protocol Data Unit.
PE	Presentation Entity.
POP	Post Office Protocol.
POSIX	Portable Operating System Interface Exchange.
PPDU	Presentation Protocol Data Unit.
PPP	Point to Point Protocol.
PPTP	Point to Point Tunneling Protocol
PPSDN	Public Packet Switched Data Network.
PRI	Primary Rate Interface.
PSAP	Presentation Service Access Point.
PSDN	Packet Switched Data Network..
PSDU	Presentation Service Data Unit.
PSTN	Public Switched Telphone network.
PTT	Post, Telphone and Communications.
PU	Physical Unit.
PVC	Permanent Virtual Circuit.
QOS	Quality Of Service
RARP	Reverse Address Resolution Protocol
RAID	Redundant Array of Inexpensive Drives.
RARP	Reverse Address Resolution Protocol.

RAS	Remote Access Services.
RDA	Remote Database Access.
RFC	Request For Command.
RFNM	Ready For Next Message.
RIP	Routing Information Protocol.
RISC	Reduced Instruction Set Computer.
RNR	Receive Not Ready.
ROSE	Remote Operation Service Element.
RPC	Remote Procedure Call.
RR	Receive Ready.
RTMP	Routing Table Maintenance Protocol.
RTSE	Reliable Transfer Service Element.
SAP	Service Access Point.
SAP	Service Advertising Protocol.
SAPI	SAP Identifier.
SAS	Single Attached Stations.
SCSI	Small Computer Systems Interface.
SDH	Synchronouse Digital Hierarchy.
SDLC	Synchronouse Data Link Control.
SE	Session Entity.
SI	Subnet Identifier.
SLIP	Serial Line Internet Protocol.
SMDS	Switched Multimegabit Digital Service.
SMTP	Simple Mail Transfer Protocol.
SNA	System Network Architecture.
SNADS	SNA Distribute Service.
SNAP	Subnetwork Address Protocol.
SNMP	Simple Network Management Protocol.
SONET	Synchronouse Optical Network.
SPDU	Session PDU.

SPX	Sequenced Packet Exchange.
SQL	Structured Query Language.
SSAP	Session SAP.
SSL	Secure Sockets Layer
SSCP	System Services Control Point.
SSDU	Session Service Data Unit.
STP	Shield Twisted Pair.
SVC	Switch Virtual Circuit
TCP	Transmission Control Protocol.
TDM	Time Division Multiplexing.
TE	Transport Entity.
TELNET	Telnet Protocol.
TFTP	Trivial File Transfer protocol.
TPDU	Transport PDU.
TSAP	Transport SAP.
TSDU	Transport SDU.
UART	Universal Asynchronouse Receiver Transmitter.
UDP	User Datafram Protocol.
UNI	User to Network Interface.
UTP	Unshield Twisted Pair.
VC	Virtual Circuit.
VCI	Virtual Circuit Identifier.
VLAN	Virtaul Local Area Network.
VPI	Virtual Path Identifier.
VPN	Virtual Private Network.
VTAM	Virtual Telecommunication Access Method.
WAN	Wide Area network.
WWW	World Wide Web.
XNS	Xerox Network Service.

TÀI LIỆU THAM KHẢO

[1] Malone, D., IPv6 - A Service Provider View in Advancing MPLS Networks, Internet Protocol Journal, Vol. 8, Nr. 2, June 2005

[2] Hinden, R., Advanced Networking Lab (ANML) Internet Protocol, Version 6 (IPv6) Resources, Pervasive Labs at Indiana University

[3] Jason Halpern, Sean Convery, Roland Saville, Safe VPN IPSec Virtual Private Network in depth , White paper of Cisco Systems , 2004.

[4] Guide to IPsec VPNs - Sheila Frankel, Karen Kent, Ryan Lewkowski,Angela D. Orebaugh, Ronald W. Ritchey, Steven R. Sharma - 01/2005.

[5] A Comprehensive Guide to Virtual Private Networks, Volume III: Cross-Platform Key and Policy Management, 2003.

[6] Johan Zuidweg, "Next Generation Intelligent Networks", Artech House Telecommunication Library, Bolton London, 2002.

[7] F.D.Ohrtman Jr, Softswitch architecture for VoIP, McGraw-Hill, 2003.

[8] K.H.Lee, K.O.Lee, K.C.Park, Architecture to be deployed on strategies of Next Generation Networks", IEEE Communication magazine, 2003.

[9] Introduction to MPLS & Its IP VPN, Juniper Networks 2000

[10] MPLS VPN Fundamentals, Juniper Networks 2000

[11] Michael A.Gallo & William M.Hancock: Computer Communications and Networking Technologies, Thomson Learning, 2002.

[12] Malone, D., Misbehaving Name Servers and What They're Missing, Internet Protocol Journal, Vol. 8, Nr. 1, March 2005

13] Carpenter, B. E.; Moore, K.; Fink, B., Connecting IPv6 Routing Domains Over the IPv4 Internet, Internet Protocol Journal, Vol. 3, Nr. 1, March 2000

[14] Andrew S. Tanenbaum, Computer Networks, Prentice Hall, New Jersey, Fourth Edition, 2003.

[15] Man Young Rhee, Wilay, Internet Security - Cryptographic Principles, Algorithms and Protocols, 2003.

[16] William Stallings, Data & Computer Communications, Prentice Hall, New Jersey, Sixth Edition, 2000.

[17] William Stallings, Network Security Essentials, 2000

MỤC LỤC

MẠNG MÁY TÍNH

Mã số: 492MMT450

Chịu trách nhiệm bản thảo

TRUNG TÂM ĐÀO TẠO BƯU CHÍNH VIỄN THÔNG 1

(Tài liệu này được ban hành theo Quyết định số: 352/QĐ-TTĐT1 ngày 12/05/2006 của Giám đốc Học viện Công nghệ Bưu chính Viễn thông)

In tại : *Công ty cổ phần In Bưu điện*
Số lượng : *2000 cuốn, khổ 19 x 26 cm*
Ngày hoàn thành : *01/06/2006.*