ĐẠI HỌC CÔNG NGHỆ ĐÔNG Á

KHOA CÔNG NGHỆ THÔNG TIN

GIÁO TRÌNH

MẠNG MÁY TÍNH CĂN BẢN

Chủ biên: TS. Đinh Văn Thành

Hà Nội – 2020

ĐẠI HỌC CÔNG NGHỆ ĐÔNG Á

KHOA CÔNG NGHỆ THÔNG TIN

GIÁO TRÌNH

MẠNG MÁY TÍNH CĂN BẢN

Chủ biên: **TS. Đinh Văn Thành**

Thành viên: **ThS. Lê Văn Hùng**

ThS. Nguyễn Thanh Thụy

ThS. Giang Thị Thu Huyền

Hà Nội – 2020

LỜI NÓI ĐẦU

Mạng máy tính kể từ khi ra đời nó đã và đang hỗ trợ rất nhiều trong mọi lĩnh vực của đời sống kinh tế xã hội như khoa học, quân sự, quốc phòng, thương mại, dịch vụ, giáo dục, … Việc kết nối các máy tính lại thành mạng để trao đổi thông tin, làm giảm giá thành phần cứng trong khi đó hiệu quả sử dụng lại cao trong quản lý kinh doanh và trong tất cả các mặt của đời sống kinh tế, chính trị xã hội. Không thể phủ nhận rằng nhiều ngành kinh tế không còn sức cạnh tranh, không còn tồn tại nếu không có sự giúp đỡ của mạng máy tính.

Vấn đề hiện nay là làm sao để có được một hệ thống mạng chạy thật tốt, thật an toàn, thật tin cậy, thật ổn định với lợi ích kinh tế cao đang rất được quan tâm. Để đáp ứng được yêu cầu trên, giáo trình "Mạng máy tính căn bản" được biên soạn gồm 157 trang với cấu trúc gồm 6 chương. Giáo trình cung cấp cho sinh viên ngành công nghệ thông tin, ngành hệ thống thông tin quản lý và những bạn đọc quan tâm về kiến thức cơ bản và nâng cao cả lý thuyết và thực hành về khối kiến thức chuyên ngành mạng máy tính. Giúp người học tiếp cận một cách dễ dàng các kiến thức tổng quát về mạng máy tích; tổ chức và hoạt động của một hệ thống mạng; cách thức các máy tính trong mạng trao đổi dữ liệu với nhau; các kiến thức về mô hình tham chiếu OSI, kiến trúc TCP/IP; các giao thức tại các tầng khác nhau như ARP, RARP, giao thức định tuyến và các dịch vụ chạy trên mô hình TCP/IP như HTTP, FTP, SMTP,…; các kiến thức cơ bản về thiết bị mạng. Ngoài ra giáo trình cũng cung cấp các khái niệm về thiết bị mạng, an ninh mạng máy tính,…

Giáo trình gồm 6 chương:

- *Chương 1: Tổng quan về mạng máy tính*. Chương này nhằm giới thiệu cho sinh viên các khái niệm cơ bản của mạng máy tính; phân loại mạng máy tính; các dịch vụ của mạng; những lợi ích mà mạng máy tính mang lại và các ứng dụng của mạng máy tính.
- *Chương 2: Các mô hình truyền thông*. Chương này nhằm giới thiệu cho sinh viên các kiến thức về chuẩn mạng truyền thông; kiến trúc phần mềm của một hệ thống mạng; mô hình OSI 7 tầng và mô hình TCP/IP.
- *Chương 3: Mạng cục bộ*. Chương này nhằm giới thiệu cho sinh viên các khái niệm cơ bản về kỹ thuật mạng cục bộ; các hình trạng mạng cục bộ cùng với ưu nhược điểm của từng loại cấu trúc; các phương pháp truy nhập ngẫu nhiên và có điều khiển được sử dụng trong các mạng quảng bá; mạng không dây và quy trình thiết kế mạng cục bộ.
- *Chương 4: Các mạng diện rộng*. Chương này nhằm giới thiệu cho sinh viên các kiến thức về mạng chuyển mạch; mạng thuê bao; mạng chuyển gói tin; mạng tốc độ cao và mạng NGN.

- *Chương 5: Mạng Internet*. Chương này nhằm giới thiệu cho sinh viên các kiến thức về kiến trúc mạng internet; các giao thức của internet; định tuyến trên internet; một số dịch vụ nổi bật trên internet và hoạt động của chúng.
- *Chương 6: An ninh mạng máy tính.* Chương này nhằm cung cấp cho sinh viên các kiến thức cơ bản về an ninh mạng; các biện pháp đảm bảo an ninh an toàn dữ liệu cho mạng máy tính và một số giao thức an ninh điển hình trên mạng Internet.

Dù đã rất cố gắng nhưng chắc chắn cuốn giáo trình này còn có những thiếu sót. Rất mong nhận được sự đóng góp ý kiến của các đồng nghiệp, các bạn đọc để cuốn giáo trình này ngày càng được hoàn thiện hơn.

Xin trân trọng cảm ơn./.

ĐẠI HỌC CÔNG NGHỆ ĐÔNG Á

MỤC LỤC

CHƯƠNG 1. TỔNG QUAN VỀ MẠNG MÁY TÍNH

Mạng máy tính hiện nay trở nên quá quen thuộc đối với chúng ta, trong mọi lĩnh vực như khoa học, quân sự, quốc phòng, thương mại, dịch vụ, giáo dục, cũng như trong công việc, trong học tập, giải trí và giao tiếp của mọi cá nhân… Mạng mang lại rất nhiều lợi ích và tiện ích cho chúng ta: thư điện tử (email), trò chuyện trực tuyến (chat), tìm_kiếm (search), các dịch vụ thanh toán và thương mại, và các dịch vụ về y tế giáo dục như là chữa bệnh từ xa hoặc tổ chức các lớp học trực tuyến... Vì vậy mà ngày nay mạng đã trở thành một nhu cầu không thể thiếu.

Mục tiêu

Chương này nhằm giới thiệu cho người học những nội dung sau:

a. Các khái niệm cơ bản về mạng máy tính

b. Những lợi ích mà mạng máy tính mang lại.

c. Phân loại mạng máy tính

d. Các dịch vụ mạng.

1.1 KHÁI NIỆM CƠ BẢN VỀ MẠNG MÁY TÍNH

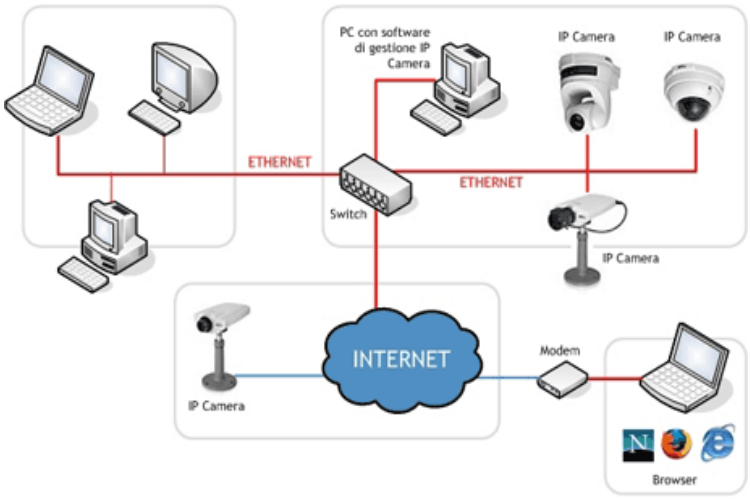
Mạng máy tính là một tập hợp các máy tính được nối với nhau bởi đường truyền theo một cấu trúc nào đó và thông qua đó các máy tính trao đổi thông tin qua lại cho nhau.

Đường truyền là hệ thống các thiết bị truyền dẫn có dây hay không dây dùng để chuyển các tín hiệu điện tử từ máy tính này đến máy tính khác. Các tín hiệu điện tử đó biểu thị các giá trị dữ liệu dưới dạng các xung nhị phân (on - off). Tất cả các tín hiệu được truyền giữa các máy tính đều thuộc một dạng sóng điện từ. Tùy theo tần số của sóng điện từ có thể dùng các đường truyền vật lý khác nhau để truyền các tín hiệu. Ở đây đường truyền được kết nối có thể là dây cáp đồng trục, cáp xoắn, cáp quang, dây điện thoại, sóng vô tuyến... Các đường truyền dữ liệu tạo nên cấu trúc của mạng. Vì vậy, hai khái niệm đường truyền và cấu trúc mạng là những đặc trưng cơ bản của mạng máy tính.

Với sự trao đổi qua lại giữa máy tính này với máy tính khác đã phân biệt mạng máy tính với các hệ thống thu phát một chiều như truyền hình, phát thông tin từ vệ tinh xuống các trạm thu thụ động... vì tại đây chỉ có thông tin một chiều từ nơi phát đến nơi thu mà không quan tâm đến có bao nhiêu nơi thu, có thu tốt hay không.

Đặc trưng cơ bản của đường truyền vật lý là giải thông. Giải thông của một đường chuyền chính là độ đo phạm vi tần số mà nó có thể đáp ứng được. Tốc độ truyền dữ liệu trên đường truyền còn được gọi là thông lượng của đường truyền - thường được tính bằng số lượng bit được truyền đi trong một giây (Bps). Thông lượng còn được đo bằng đơn vị khác là

Baud (*lấy từ tên nhà bác học* - Emile Baudot). Baud biểu thị số lượng thay đổi tín hiệu trong một giây.



Hình 1 - Một mô hình liên kết các máy tính trong mạng

Ở đây Baud và Bps không phải bao giờ cũng đồng nhất. Ví dụ: nếu trên đường dây có 8 mức tín hiệu khác nhau thì mỗi mức tín hiệu tương ứng với 3 bit hay là 1 Baud tương ứng với 3 bit. Chỉ khi có 2 mức tín hiệu trong đó mỗi mức tín hiệu tương ứng với 1 bit thì 1 Baud mới tương ứng với 1 bit.

1.2 CÁC LỢI ÍCH CỦA MẠNG MÁY TÍNH

1.2.1 Mạng tạo khả năng dùng chung tài nguyên cho các người dùng

Vấn đề là làm cho các tài nguyên trên mạng như chương trình, dữ liệu và thiết bị, đặc biệt là các thiết bị đắt tiền, có thể sẵn dùng cho mọi người trên mạng mà không cần quan tâm đến vị trí thực của tài nguyên và người dùng.

Về mặt thiết bị, các thiết bị chất lượng cao thường đắt tiền, chúng thường được dùng chung cho nhiều người nhằm giảm chi phí và dễ bảo quản.

Về mặt chương trình và dữ liệu, khi được dùng chung, mỗi thay đổi sẽ sẵn dùng cho mọi thành viên trên mạng ngay lập tức. Điều này thể hiện rất rõ tại các nơi như ngân hàng, các đại lý bán vé máy bay...

1.2.2 Mạng cho phép nâng cao độ tin cậy

Khi sử dụng mạng, có thể thực hiện một chương trình tại nhiều máy tính khác nhau, nhiều thiết bị có thể dùng chung. Điều này tăng độ tin cậy trong công việc vì khi có máy tính hoặc thiết bị bị hỏng, công việc vẫn có thể tiếp tục với các máy tính hoặc thiết bị khác trên mạng trong khi chờ sửa chữa.

1.2.3 Mạng giúp cho công việc đạt hiệu suất cao hơn

Khi chương trình và dữ liệu đã dùng chung trên mạng, có thể bỏ qua một số khâu đối chiếu không cần thiết. Việc điều chỉnh chương trình (nếu có) cũng tiết kiệm thời gian hơn do chỉ cần cài đặt lại trên một máy.

Về mặt tổ chức, việc sao chép dữ liệu phòng hờ tiện lợi hơn do có thể giao cho chỉ một người thay vì mọi người phải tự sao chép phần của mình.

1.2.4 Tiết kiệm chi phí

Việc dùng chung các thiết bị ngoại vi cho phép giảm chi phí trang bị tính trên số người dùng. Về phần mềm, nhiều nhà sản xuất phần mềm cung cấp cả những ấn bản cho nhiều người dùng, với chi phí thấp hơn tính trên mỗi người dùng.

1.2.5 Tăng cường tính bảo mật thông tin

Dữ liệu được lưu trên các máy phục vụ tập tin (file server) sẽ được bảo vệ tốt hơn so với đặt tại các máy cá nhân nhờ cơ chế bảo mật của các hệ điều hành mạng.

1.2.6 Việc phát triển mạng máy tính đã tạo ra nhiều ứng dụng mới

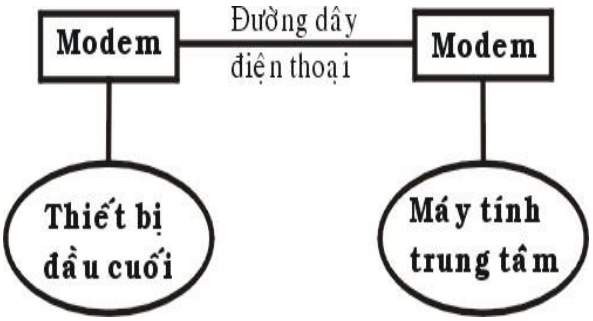
Một số ứng dụng có ảnh hưởng quan trọng đến toàn xã hội: khả năng truy xuất các chương trình và dữ liệu từ xa, khả năng thông tin liên lạc dễ dàng và hiệu quả, tạo môi trường giao tiếp thuận lợi giữa những người dùng khác nhau, khả năng tìm kiếm thông tin nhanh chóng trên phạm vi toàn thế giới,...

1.3 LỊCH SỬ PHÁT TRIỂN CỦA MẠNG MÁY TÍNH

Vào giữa những năm 50 khi những thế hệ máy tính đầu tiên được đưa vào hoạt động thực tế với những bóng đèn điện tử thì chúng có kích thước rất cồng kềnh và tốn nhiều năng lượng. Hồi đó việc nhập dữ liệu vào các máy tính được thông qua các tấm bìa mà người viết chương trình đã đục lỗ sẵn. Mỗi tấm bìa tương đương với một dòng lệnh mà mỗi một cột của nó có chứa tất cả các ký tự cần thiết mà người viết chương trình phải đục lỗ vào ký tự mình lựa chọn. Các tấm bìa được đưa vào một "thiết bị" gọi là thiết bị đọc bìa mà qua đó các thông tin được đưa vào máy tính (hay còn gọi là trung tâm xử lý) và sau khi tính toán kết quả sẽ được đưa ra máy in. Như vậy các thiết bị đọc bìa và máy in được thể hiện như các thiết bị vào ra (I/O) đối với máy tính. Sau một thời gian các thế hệ máy mới được đưa vào hoạt động trong đó một máy tính trung tâm có thể được nối với nhiều thiết bị vào ra (I/O) mà qua đó nó có thể thực hiện liên tục hết chương trình này đến chương trình khác.

Cùng với sự phát triển của những ứng dụng trên máy tính các phương pháp nâng cao khả năng giao tiếp với máy tính trung tâm cũng đã được đầu tư nghiên cứu rất nhiều. Vào giữa những năm 60 một số nhà chế tạo máy tính đã nghiên cứu thành công những thiết bị truy cập từ xa tới máy tính của họ. Một trong những phương pháp thâm nhập từ xa được thực hiện

bằng việc cài đặt một thiết bị đầu cuối ở một vị trí cách xa trung tâm tính toán, thiết bị đầu cuối này được liên kết với trung tâm bằng việc sử dụng đường dây điện thoại và với hai thiết bị xử lý tín hiệu (thường gọi là Modem) gắn ở hai đầu và tín hiệu được truyền thay vì trực tiếp thì thông qua dây điện thoại.

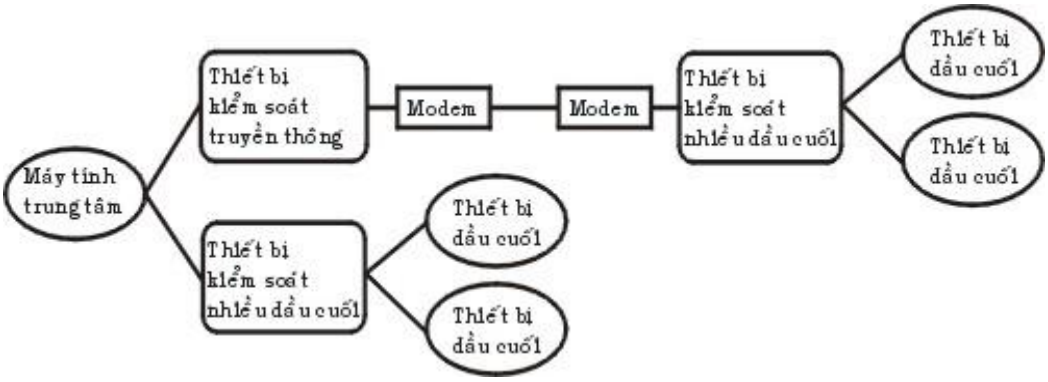


Hình 2 - Mô hình truyền dữ liệu từ xa đầu tiên

Những dạng đầu tiên của thiết bị đầu cuối bao gồm máy đọc bìa, máy in, thiết bị xử lý tín hiệu, các thiết bị cảm nhận. Việc liên kết từ xa đó có thể thực hiện thông qua những vùng khác nhau và đó là những dạng đầu tiên của hệ thống mạng.

Trong lúc đưa ra giới thiệu những thiết bị đầu cuối từ xa, các nhà khoa học đã triển khai một loạt những thiết bị điều khiển, những thiết bị đầu cuối đặc biệt cho phép người sử dụng nâng cao được khả năng tương tác với máy tính. Một trong những sản phẩm quan trọng đó là hệ thống thiết bị đầu cuối 3270 của IBM. Hệ thống đó bao gồm các màn hình, các hệ thống điều khiển, các thiết bị truyền thông được liên kết với các trung tâm tính toán. Hệ thống 3270 được giới thiệu vào năm 1971 và được sử dụng dùng để mở rộng khả năng tính toán của trung tâm máy tính tới các vùng xa. Để làm giảm nhiệm vụ truyền thông của máy tính trung tâm và số lượng các liên kết giữa máy tính trung tâm với các thiết bị đầu cuối, IBM và các công ty máy tính khác đã sản xuất một số các thiết bị sau:

- **Thiết bị kiểm soát truyền thông**: có nhiệm vụ nhận các bit tín hiệu từ các kênh truyền thông, gom chúng lại thành các byte dữ liệu và chuyển nhóm các byte đó tới máy tính trung tâm để xử lý, thiết bị này cũng thực hiện công việc ngược lại để chuyển tín hiệu trả lời của máy tính trung tâm tới các trạm ở xa. Thiết bị trên cho phép giảm bớt được thời gian xử lý trên máy tính trung tâm và xây dựng các thiết bị logic đặc trưng.
- **Thiết bị kiểm soát nhiều đầu cuối**: cho phép cùng một lúc kiểm soát nhiều thiết bị đầu cuối. Máy tính trung tâm chỉ cần liên kết với một thiết bị như vậy là có thể phục vụ cho tất cả các thiết bị đầu cuối đang được gắn với thiết bị kiểm soát trên. Điều này đặc biệt có ý nghĩa khi thiết bị kiểm soát nằm ở cách xa máy tính vì chỉ cần sử dụng một đường điện thoại là có thể phục vụ cho nhiều thiết bị đầu cuối.



Hình 3 - Mô hình trao đổi mạng của hệ thống 3270

Vào giữa những năm 1970, các thiết bị đầu cuối sử dụng những phương pháp liên kết qua đường cáp nằm trong một khu vực đã được ra đời. Với những ưu điểm từ nâng cao tốc độ truyền dữ liệu và qua đó kết hợp được khả năng tính toán của các máy tính lại với nhau. Để thực hiện việc nâng cao khả năng tính toán với nhiều máy tính các nhà sản xuất bắt đầu xây dựng các mạng phức tạp. Vào những năm 1980 các hệ thống đường truyền tốc độ cao đã được thiết lập ở Bắc Mỹ và Châu Âu và từ đó cũng xuất hiện các nhà cung cấp các dịnh vụ truyền thông với những đường truyền có tốc độ cao hơn nhiều lần so với đường dây điện thoại. Với những chi phí thuê bao chấp nhận được, người ta có thể sử dụng được các đường truyền này để liên kết máy tính lại với nhau và bắt đầu hình thành các mạng một cách rộng khắp. ở đây các nhà cung cấp dịch vụ đã xây dựng những đường truyền dữ liệu liên kết giữa các thành phố và khu vực với nhau và sau đó cung cấp các dịch vụ truyền dữ liệu cho những người xây dựng mạng. Người xây dựng mạng lúc này sẽ không cần xây dựng lại đường truyền của mình mà chỉ cần sử dụng một phần các năng lực truyền thông của các nhà cung cấp.

Vào năm 1974 công ty IBM đã giới thiệu một loạt các thiết bị đầu cuối được chế tạo cho lĩnh vực ngân hàng và thương mại, thông qua các dây cáp mạng các thiết bị đầu cuối có thể truy cập cùng một lúc vào một máy tính dùng chung. Với việc liên kết các máy tính nằm ở trong một khu vực nhỏ như một tòa nhà hay là một khu nhà thì tiền chi phí cho các thiết bị và phần mềm là thấp. Từ đó việc nghiên cứu khả năng sử dụng chung môi trường truyền thông và các tài nguyên của các máy tính nhanh chóng được đầu tư.

Vào năm 1977, công ty Datapoint Corporation đã bắt đầu bán hệ điều hành mạng của mình là "Attached Resource Computer Network" (hay gọi tắt là Arcnet) ra thị trường. Mạng Arcnet cho phép liên kết các máy tính và các trạm đầu cuối lại bằng dây cáp mạng, qua đó đã trở thành là hệ điều hành mạng cục bộ đầu tiên.

Từ đó đến nay đã có rất nhiều công ty đưa ra các sản phẩm của mình, đặc biệt khi các máy tính cá nhân được sử dụng một cánh rộng rãi. Khi số lượng máy vi tính trong một văn

phòng hay cơ quan được tăng lên nhanh chóng thì việc kết nối chúng trở nên vô cùng cần thiết và sẽ mang lại nhiều hiệu quả cho người sử dụng.

Ngày nay với một lượng lớn về thông tin, nhu cầu xử lý thông tin ngày càng cao. Mạng máy tính hiện nay trở nên quá quen thuộc đối với chúng ta, trong mọi lĩnh vực như khoa học, quân sự, quốc phòng, thương mại, dịch vụ, giáo dục... Hiện nay ở nhiều nơi mạng đã trở thành một nhu cầu không thể thiếu được. Người ta thấy được việc kết nối các máy tính thành mạng cho chúng ta những khả năng mới to lớn như:

- **Sử dụng chung tài nguyên**: Những tài nguyên của mạng (như thiết bị, chương trình, dữ liệu) khi được trở thành các tài nguyên chung thì mọi thành viên của mạng đều có thể tiếp cận được mà không quan tâm tới những tài nguyên đó ở đâu.
- **Tăng độ tin cậy của hệ thống**: Người ta có thể dễ dàng bảo trì máy móc và lưu trữ (backup) các dữ liệu chung và khi có trục trặc trong hệ thống thì chúng có thể được khôi phục nhanh chóng. Trong trường hợp có trục trặc trên một trạm làm việc thì người ta cũng có thể sử dụng những trạm khác thay thế.
- **Nâng cao chất lượng và hiệu quả khai thác thông tin**: Khi thông tin có thể được sử dụng chung thì nó mang lại cho người sử dụng khả năng tổ chức lại các công việc với những thay đổi về chất như:

  - Đáp ứng những nhu cầu của hệ thống ứng dụng kinh doanh hiện đại.
  - Cung cấp sự thống nhất giữa các dữ liệu.
  - Tăng cường năng lực xử lý nhờ kết hợp các bộ phận phân tán.
  - Tăng cường truy nhập tới các dịch vụ mạng khác nhau đang được cung cấp trên thế giới.

Với nhu cầu đòi hỏi ngày càng cao của xã hội nên vấn đề kỹ thuật trong mạng là mối quan tâm hàng đầu của các nhà tin học. Ví dụ như làm thế nào để truy xuất thông tin một cách nhanh chóng và tối ưu nhất, trong khi việc xử lý thông tin trên mạng quá nhiều đôi khi có thể làm tắc nghẽn trên mạng và gây ra mất thông tin một cách đáng tiếc.

Hiện nay việc làm sao có được một hệ thống mạng chạy thật tốt, thật an toàn với lợi ích kinh tế cao đang rất được quan tâm. Một vấn đề đặt ra có rất nhiều giải pháp về công nghệ, một giải pháp có rất nhiều yếu tố cấu thành, trong mỗi yếu tố có nhiều cách lựa chọn. Như vậy để đưa ra một giải pháp hoàn chỉnh, phù hợp thì phải trải qua một quá trình chọn lọc dựa trên những ưu điểm của từng yếu tố, từng chi tiết rất nhỏ.

Để giải quyết một vấn đề phải dựa trên những yêu cầu đặt ra và dựa trên công nghệ để giải quyết. Nhưng công nghệ cao nhất chưa chắc là công nghệ tốt nhất, mà công nghệ tốt nhất là công nghệ phù hợp nhất.

1.4 PHÂN LOẠI MẠNG MÁY TÍNH

1.4.1 Phân loại mạng máy tính theo kỹ thuật truyền tin

Dựa theo kỹ thuật truyền tải thông tin, người ta có thể chia mạng thành hai loại là Mạng quảng bá (Broadcast Network) và mạng điểm nối điểm (Point – to – point Network)

a. Mạng quảng bá

Trong hệ thống mạng quảng bá chỉ tồn tại một kênh truyền được chia sẻ cho tất cả các máy tính. Khi một máy tính gửi tin, tất cả các máy tính còn lại sẽ nhận được tin đó. Tại một thời điểm chỉ cho phép một máy tính được phép sử dụng đường truyền.

b. Mạng điểm nối điểm

Trong hệ thống mạng này, các máy tính được nối lại với nhau thành từng cặp. Thông tin được gửi đi sẽ được truyền trực tiếp từ máy gửi đến máy nhận hoặc được chuyển tiếp qua nhiều máy trung gian trước khi đến máy tính nhận.

1.4.2 Phân loại theo khoảng cách địa lý

Mạng cục bộ (Local Area Networks viết tắt là LAN): là mạng máy tính được tổ chức trong phạm vi nhỏ khoảng vài kilômét trở lại, ví dụ mạng nội bộ cơ quan, trường học, xí nghiệp, văn phòng,...

Mạng đô thị (Metropolitan Area Networks viết tắt là MAN): là mạng máy tính được tổ chức trong phạm vi 100 kilômét trở lại, ví dụ mạng thành phố, trung tâm kinh tế, khu công nghệ cao,...

Mạng diện rộng (Wide Area Network viết tắt là WAN): là mạng máy tính được tổ chức trong phạm vi rộng, như mạng quốc gia, liên bang, châu lục.

Mạng toàn cầu (Global Area Network viết tắt là GAN): là mạng máy tính được tổ chức rộng khắp toàn cầu.

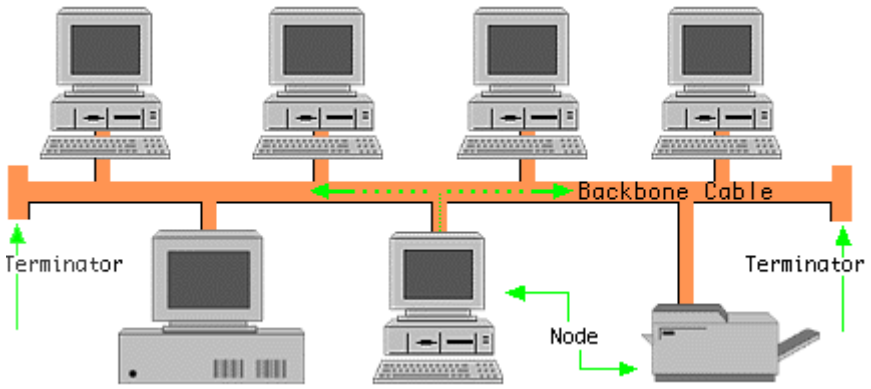
1.4.2.1. Mạng cục bộ

Đây là mạng thuộc loại mạng quảng bá, sử dụng một đường truyền có tốc độ cao, băng thông rộng, có hình trạng (topology) đơn giản như mạng hình bus, mạng hình sao (Star topology), mạng hình vòng (Ring topology).

- **Mạng hình bus**

Tất cả các máy tính được nối lại bằng một dây dẫn (Cáp đồng trục gầy hoặc đồng trục béo). Khi một trong số chúng thực hiện truyền tin, tín hiệu sẽ lan truyền đến tất cả các máy

tính còn lại. Nếu có hai máy tính truyền tin cùng một lúc thì sẽ dẫn đến tình trạng đụng độ và trạng thái lỗi xảy ra.



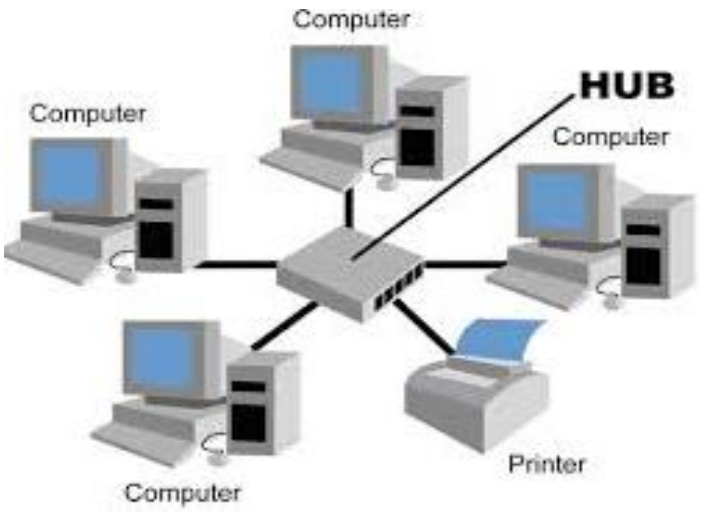
Hình 4– Mạng hình Bus

- **Mạng hình sao**

Các máy tính được nối trực tiếp vào một Bộ tập trung nối kết, gọi là Hub. Dữ liệu được chuyển qua Hub trước khi đến các máy nhận. Hub có nhiều cổng (port), mỗi cổng cho phép một máy tính nối vào. Hub đóng vai trò như một bộ khuyếch đại (repeater). Nó khuyếch đại tín hiệu nhận được trước khi truyền lại tín hiệu đó trên các cổng còn lại.

Ưu điểm của mạng hình sao là dễ dàng cài đặt, không dừng mạng khi nối thêm vào hoặc lấy một máy tính ra khỏi mạng, cũng như dễ dàng phát hiện lỗi. So với mạng hình Bus, mạng hình sao có tín ổn định cao hơn.

Tuy nhiên nó đòi hỏi nhiều dây dẫn hơn so với mạng hình bus. Toàn mạng sẽ bị ngưng hoạt động nếu Hub bị hư. Chi phí đầu tư mạng hình sao cao hơn mạng hình Bus.

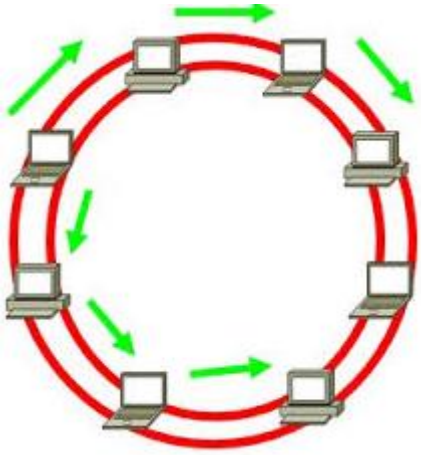


Hình 5– Mạng hình sao

- **Mạng hình vòng**

Tồn tại một thẻ bài (token: một gói tin nhỏ) lần lượt truyền qua các máy tính. Một máy tính khi truyền tin phải tuân thủ nguyên tắc sau:

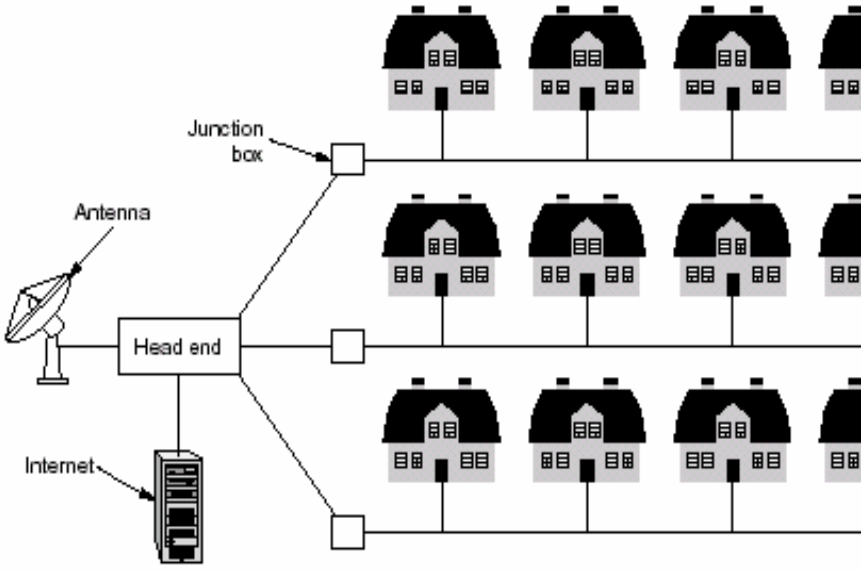
- Chờ cho đến khi token đến nó và nó sẽ lấy token ra khỏi vòng tròn.
- Gửi gói tin của nó đi một vòng qua các máy tính trên đường tròn.
- Chờ cho đến khi gói tin quay về
- Đưa token trở lại vòng tròn để nút bên cạnh nhận token



Hình 6– Mạng vòng

1.4.2.2. Mạng đô thị

Mạng MAN được sử dụng để nối tất cả các máy tính trong phạm vi toàn thành phố. Ví dụ như mạng truyền hình cáp trong thành phố.



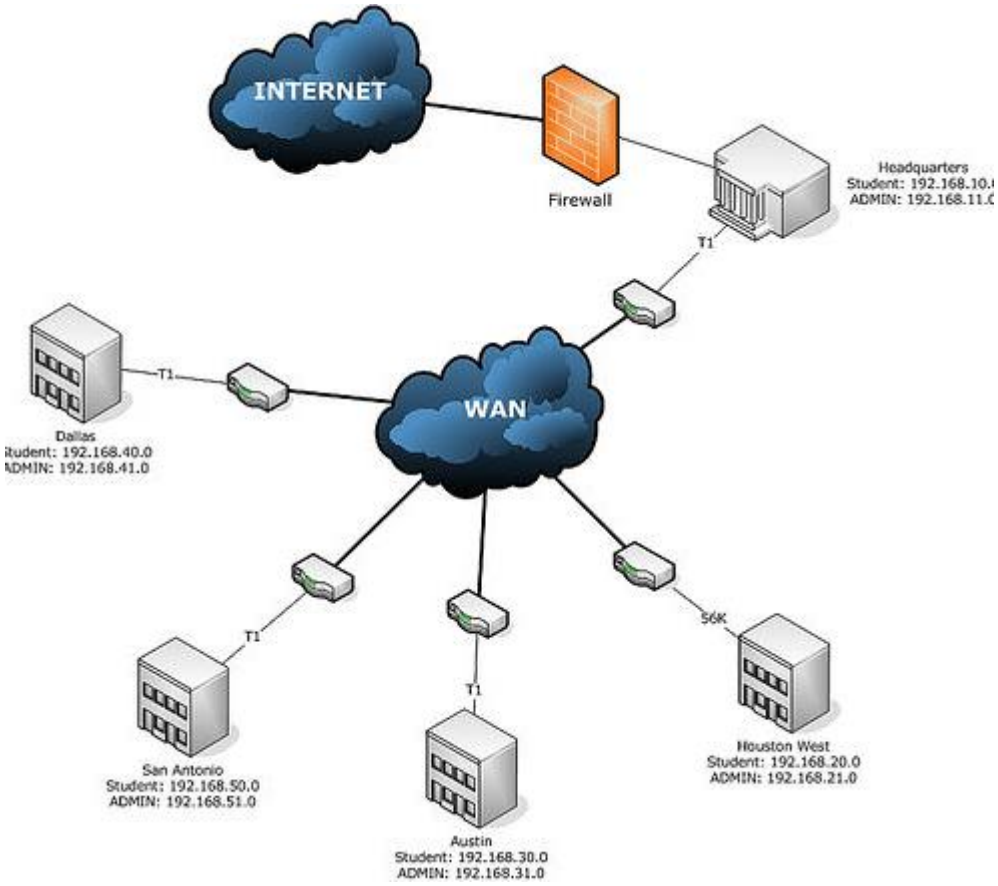
Hình 7– Mạng đô thị

1.4.2.3. Mạng diện rộng

Mạng LAN và mạng MAN thông thường không sử dụng các thiết bị chuyển mạch, điều đó hạn chế trong việc mở rộng phạm vi mạng về số lượng máy tính và khoảng cách. Chính vì thế mạng diện rộng được phát minh.

Trong một mạng WAN, các máy tính (**hosts**) được nối vào một mạng con (subnet) hay đôi khi còn gọi là đường trục mạng (Backbone), trong đó có chứa các bộ chọn đường (**routers**) và các đường truyền tải (**transmission lines**).

Các Routers thông thường có nhiệm vụ lưu và chuyển tiếp các gói tin mà nó nhận được theo nguyên lý cơ bản sau: Các gói tin đến một router sẽ được lưu vào trong một hàng chờ, kế đến router sẽ quyết định nơi gói tin cần phải đến và sau đó sẽ chuyển gói tin lên đường đã được chọn.



Hình 8– Mạng diện rộng

1.4.3 Phân loại theo kỹ thuật chuyển mạch

- *Mạng chuyển mạch kênh* (Circuit-switched Networks):
  - Là mạng thực hiện việc kết nối hai thực thể ở hai đầu theo một kênh cố định trong thời gian truyền tin.
  - *Nhược điểm*:
    - ✓ Tốn thời gian để thiết lập kênh cố định giữa hai thực thể

- ✓ Hiệu suất sử dụng đường truyền thấp vì sẽ có lúc kênh bị bỏ không do cả hai bên đều hết thông tin cần truyền trong khi các thực thể khác không được phép sử dụng kênh truyền này.

- *Mạng chuyển mạch thông báo* (Message-Switched Networks):
  - Thông tin truyền đi theo một khuôn dạng quy định, trong đó được chỉ định đích đến. Căn cứ vào thông tin đích đến các thông báo có thể được truyền qua nhiều con đường khác nhau để đến đích.
  - *Ưu điểm so với mạng chuyển mạch kênh:*
    - ✓ Hiệu suất sử dụng đường truyền cao vì không bị chiếm dụng độc quyền mà được phân chia giữa nhiều thực thể
    - ✓ Mỗi nút mạng có thể lưu trữ thông báo cho tới khi kênh truyền rỗi mới gửi thông báo đi → giảm được tình trạng tắc nghẽn mạch
    - ✓ Có thể điều khiển việc truyền tin bằng cách sắp xếp độ ưu tiên cho các thông báo
    - ✓ Có thể tăng hiệu suất sử dụng giải thông bằng cách gán địa chỉ quảng bá để gửi thông báo đồng thời tới nhiều đích
  - *Nhược điểm:*
    - ✓ Không hạn chế kích thước của các thông báo, dẫn đến phí tổn lưu trư tạm thời cao và ảnh hưởng tới thời gian đáp và chất lượng truyền
    - ✓ Thích hợp cho các dịch vụ thư tín điện tử hơn là các áp dụng có tính thời gian thực vì tồn tại độ trễ do lưu trữ và xử lý thông tin điều khiển tại mỗi nút.

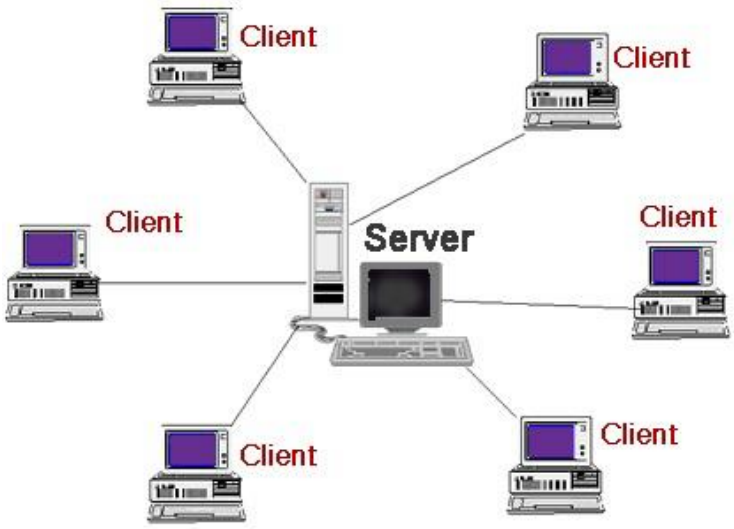
- *Mạng chuyển mạch gói* (Packet-Switched Networks): là mạng trong đó thông báo cần gửi đi được chia nhỏ thành các gói (packet) có số lượng bytes cố định. Mỗi gói tin có địa chỉ đích và đánh dấu thứ tự và có thể đi theo nhiều đường khác nhau để tới đích. Khi tới đích, chúng được kết nối lại với nhau theo thứ tự đã được đánh số.
- *So sánh mạng chuyển mạch thông báo và mạng chuyển mạch gói*
  - Giống nhau: phương pháp giống nhau
  - Khác nhau: Các gói tin được giới hạn kích thước tối đa sao cho các nút mạng có thể xử lý toàn bộ gói tin trong bộ nhớ mà không cần phải lưu trữ tạm thời trên đĩa. Vì thế mạng chuyển mạch gói truyền các gói tin qua mạng nhanh chóng và hiệu quả hơn so với mạng chuyển mạch thông báo. Nhưng vấn đề khó khăn của mạng loại này là việc tập hợp các gói tin để tạo lại thông báo ban đầu của người sử dụng, đặc biệt trong trường hợp các gói được truyền theo nhiều đường khác nhau. Cần phải cài đặt cơ chế "đánh dấu" gói tin và phục hồi gói tin bị thất lạc hoặc truyền bị lỗi cho các nút mạng.
  - Do có ưu điểm mềm dẻo và hiệu suất cao hơn nên hiện nay mạng chuyển mạch gói

được sử dụng phổ biến hơn các mạng chuyển mạch thông báo.

- Xu hướng phát triển của mạng ngày nay là tích hợp cả hai kỹ thuật chuyển mạch (kênh và gói) trong một mạng thống nhất → mạng dịch vụ tích hợp số

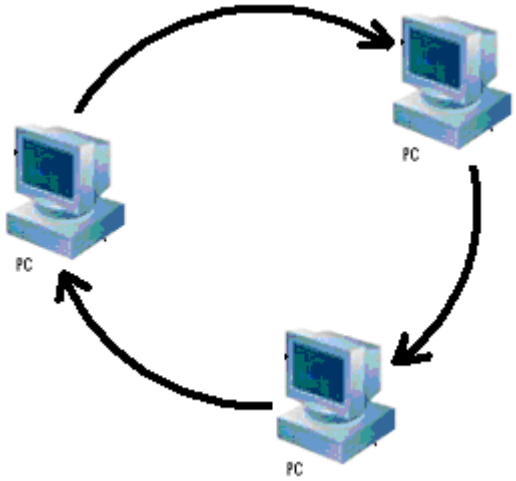
1.4.4 Phân loại theo chức năng

***Mô hình Client-Server*:** Các máy khách là những trạm làm việc hay máy trạm, nơi người dùng chạy các ứng dụng để xử lý dữ liệu. Các Server là những kho chứa thông tin và cung cấp các dịch vụ cho các máy trạm. Máy khách và máy trạm được nối kết thông qua nhiều thiết bị và cáp nối. Server luôn là máy tính phức tạp và mạnh mẽ hơn, chạy những phần mềm cũng phức tạp và mạnh mẽ hơn các máy khách. Một tính chất nữa là Server được tăng cường khả năng lưu trữ dự liệu một cách mạnh mẽ. Các Server có thể lưu trữ các chương trình ứng dụng, dữ liệu, hệ điều hành mạng, các thư mục, tập tin, và nhưng tiện ích quản lý dành cho mạng. Do bởi có những phần cứng mạnh hơn và phần mềm được chuyên biệt hoá, nên mạng Client-Server thông thường có phí tổn để thực hiện cao hơn mạng peer-to-peer. Những mối nối kết giữa các nút mạng đòi hỏi phải có những thiết bị nối kết ngoại vi (router, hub, bridge) và các nối cũng nhiều hơn.



Hình 9- Mô hình mạng Client-Server

Mô hình mạng peer-to-peer: mỗi nút mạng đều có vai trò ngang nhau. Trong mô hình hày thì không có máy chủ ở trung ương chuyên cung cấp các dịch vụ xử lý cho mọi nút mạng hay máy khách. Mọi nút mạng có thể thực hiện chức năng như một máy khách mà cũng có thể như một Server trong mạng, có nghĩa là việc liên lạc trực tiếp giữa các máy khách của mạng diễn ra mà không cần có một Server chuyên trách nào cả. Mỗi nút mạng đều có thiết bị lưu trữ của riêng nó và đều có thể truy cập đến các nút mạng khác.



Hình 10 - Mô hình mạng peer-to-peer

1.5 CÁC DỊCH VỤ MẠNG MÁY TÍNH

1.5.1 File và Print

File server hay là máy phục vụ tập tin. Nó cung cấp khả năng truy nhập đến các tài nguyên mạng nhưng đảm bảo chỉ những người sử dụng đã được kiểm soát mới được truy cập vào những tài nguyên này. Các File server làm giảm đi những chỗ thắt cổ chai trong lưu thông dữ liệu bằng cách cho phép các tác vụ xử lý được thực hiện trên mỗi nút mạng trong mô hình Client-Server và loại trừ đi sự dư thừa bằng cách cho phép những máy tính riêng lẻ thực hiện những chức năng giống nhau mà không cần đặt những tài nguyên riêng lẻ trên mỗi nút.

Print Server một máy phục vụ in ấn cho phép nhiều người sử dụng mạng chia sẻ dùng chungcác máy in và máy vẽ ở rải rác khắp nơi trên mạng như thể người dùng này được nối kết trực tiếp với các thiết bị in ấn đó vậy.

1.5.2 Các dịch vụ truyền thông

Các dịch vụ truyền thông bao gồm *Communication Server* và *Fax Server* là được sử dụng phổ biến nhất.

Communication Server là một máy phục vụ truyền thông thực ra là một nhóm các kiểu Server khac nhau có thể xử lý các hoạt động truyền thông đồng bộ và không đồng bộ bao gồm các Access Server (máy phục vụ truy cập gồm dial-in và dial-out server), các Bulletin Board Server (máy phục vụ bảng tin điện tử) và các Electronic Mail Server (máy phục vụ thư điện tử). Máy phục vụ truyền thông cung cấp một điểm truy cập ở trung ương cho mối nối kết từ xa với mạng, quản lý các mối nối kết giữa các nút mạng và các địa điểm ở xa muốn truy cập vào mạng.

Các Fax Server hay máy phục vụ Fax quản lý các bức fax đi xa và đến những người dùng mạng bằng cách lưu trữ và gửi chuyển tiếp các bức fax thông qua hệ thống điện thoại hoặc thông qua bản thân mạng.

1.5.3 Các dịch vụ Internet

- *WWW*

Đây là dịch vụ phổ biến nhất hiện nay trên Internet, dịch vụ này đưa ra cách truy xuất các tài liệu của các máy phục vụ dễ dàng qua các giao tiếp đồ hoạ. Các tài liệu này liên kết với nhau tạo nên kho tài liệu khổng lồ. Để sử dụng dịch vụ này cần có một chương trình hỗ trợ gọi là WEB Browser. Thông qua Internet các Browser truy nhập thông tin của các Web Server.

- *Email*

Đây là dịch vụ được sử dụng nhiều nhất trên Internet, dịch vụ này cho phép các cá nhân trao đổi thư với nhau qua Internet. Trên mạng internet có hàng triệu máy chủ thư (mail server) của các nhà cung cấp dịch vụ (Internet Service Provider – ISP) khác nhau cung cấp dịch vụ email cho hàng trăm triệu người trên toàn thế giới. Dịch vụ thư điện tử không những làm hạ giá thành, chuyển phát nhanh… mà nội dung của nó còn có thể tích hợp các loại dữ liệu âm thanh, hình ảnh, đồ họa, …trên một bức thư mà thư truyền thống không thể có được.

- *FTP*

Đây là dịch vụ truyền nhận tập tin trên Internet, thông qua dịch vụ này Client có thể download các tập tin từ Server về máy cục bộ hay upload các tập tin vào Server. Dịch vụ này thường được sử dụng để sao chép các phần mềm freeware, các bản update cho driver, ...

- *Dịch vụ tìm kiếm thông tin trên internet*

Tìm kiếm thông tin là hoạt động phổ biến đối với người dùng internet. So với các thông tin được lưu trữ trên các phương tiện khác, thông tin được lưu trữ trên internet có thể truy cập và tìm kiếm dễ dàng hơn. Có hai cách tìm kiếm thường được sử dụng hiện nay:

- ***Tìm kiếm theo danh mục hay địa chỉ liên kết*** được các nhà cung cấp dịch vụ đặt trên các trang web.
- ***Tìm kiếm nhờ các máy tìm kiếm*** (search Engine): Máy tìm kiếm cho phép tìm kiếm thông tin trên internet theo yêu cầu của người dùng. Hiện nay có rất nhiều website cung cấp các máy tìm kiếm, chẳng hạn: http://www.Google.com, http://www.yahoo.com, http://www.msn.com, …

- *Dịch vụ chat*

Chat là dịch vụ được người sử dụng internet ưa chuộng nhất. Nó cho phép người dùng thiết lập các cuộc đối thoại thông qua máy tính với người dùng khác trên internet.

Hiện nay trên internet có hai hình thức Chat phổ biến là Web Chat và Instant Message (IM). Web Chat là dịch vụ thường được cung cấp trên các trang Web dạng diễn đàn, được dùng để cung cấp cho các thành viên thông tin cần được thảo luận trực tuyến với nhau khi cùng đang có mặt trên diễn đàn. IM được sử dụng khá phổ biến, được các nhà cung cấp lớn như Yahoo, MSN, AOL, … Để sử dụng dịch vụ này, người dùng cần đăng ký một tài khoản và sử dụng tài khoản đó để chat với các thành viên khác trong nhóm. Điểm khác nhau giữa IM với Web Chat là khi người dùng muốn sử dụng IM trên một máy tính nào đó, thì trên máy tính này bắt buộc phải cài phần mềm để Chat.

1.5.4 Các dịch vụ quản lý

- *Dynamic Host Configuration Protocol (DHCP)*

Trong một mạng máy tính, việc cấp các địa chỉ IP tĩnh cố định cho các host sẽ dẫn đến tình trạng lãng phí địa chỉ IP, vì trong cùng một lúc không phải các host hoạt động đồng thời với nhau, do vậy sẽ có một số địa chỉ IP bị thừa. Để khắc phục tình trạng đó, dịch vụ DHCP đưa ra để cấp phát các địa chỉ IP động trong mạng.

Trong mạng máy tính NT khi một máy phát ra yêu cầu về các thông tin của TCP/IP thì gọi là DHCP client, còn các máy cung cấp thông tin của TCP/IP gọi là DHCP server. Các máy DHCP server bắt buộc phải là Windows NT server.

Cách cấp phát địa chỉ IP trong DHCP: Một user khi log on vào mạng, nó cần xin cấp 1 địa chỉ IP, theo 4 bước sau :

- Gởi thông báo đến tất cả các DHCP server để yêu cầu được cấp địa chỉ.
- Tất cả các DHCP server gởi trả lời địa chỉ sẽ cấp đến cho user đó.
- User chọn 1 địa chỉ trong số các địa chỉ, gởi thông báo đến server có địa chỉ được chọn.
- Server được chọn gởi thông báo khẳng định đến user mà nó cấp địa chỉ.

Quản trị các địa chỉ IP của DHCP server: Server quản trị địa chỉ thông qua thời gian thuê bao địa chỉ (lease duration). Có ba phương pháp gán địa chỉ IP cho các Worstation :

- Gán thủ công.

- Gán tự động.
- Gán động.

Trong phương pháp gán địa chỉ IP thủ công thì địa chỉ IP của DHCP client được gán thủ công bởi người quản lý mạng tại DHCP server và DHCP được sử dụng để chuyển tới DHCP client giá trị địa chỉ IP mà được định bởi người quản trị mạng.

Trong phương pháp gán địa chỉ IP tự động DHCP client được gán địa chỉ IP khi lần đầu tiên nó nối vào mạng. Địa chỉ IP được gán bằng phong pháp này sẽ được gán vĩnh viễn cho DHCP client và địa chỉ này sẽ không bao giờ được sử dụng bởi một DHCP client khác.

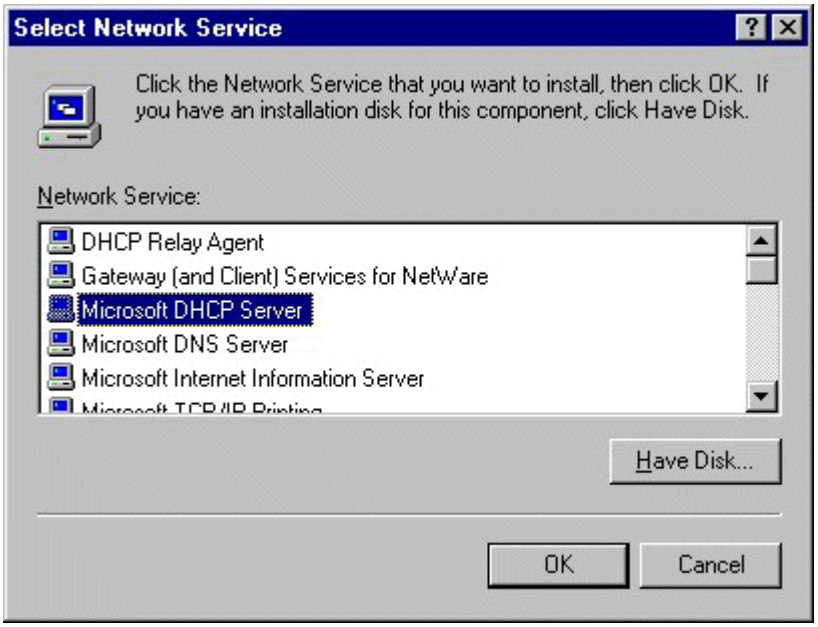
Trong phương pháp gán địa chỉ IP động thì DHCP server gán địa chỉ IP cho DHCP client tạm thời. Sau đó địa chỉ IP này sẽ được DHCP client sử dụng trong một thời gian đặc biệt. Đến khi thời gian này hết hạn thì địa chỉ IP này sẽ bị xóa mất. Sau đó nếu DHCP client cần nối kết vào mạng thì nó sẽ được cấp một địa chủ IP khác.

Phương pháp gán địa chỉ IP động này đặc biệt hữu hiệu đối với những DHCP client chỉ cần địa chỉ IP tạm thời để kết nối vào mạng. Ví dụ một tình huống trên mạng có 300 users và sử dụng subnet là lớp C. Điều này cho phép trên mạng có 253 nodes trên mạng. Bởi vì mỗi computer nối kết vào mạng sử dụng TCP/IP cần có một địa chỉ IP duy nhất do đó tất cả 300 computer không thể đồng thời nối kết vào mạng. Vì vậy nếu ta sử dụng phương pháp này ta có thể sử dụng lại những IP mà đã được giải phóng từ các DHCP client khác.

Cài đặt DHCP chỉ có thể cài trên Windows NT server mà không thể cài trên Client. Các bước thực hiện như sau:

- Login vào Server với tên Administrator .
- Click hai lần vào icon **Network** . Ta sẽ thấy hộp hội thoại **Network dialog box**
- Chọn tab service và click vào nút Add .
- Ta sẽ thấy một loạt các service của Windows NT server nằm trong hộp hội thoại Select Network Service. Chọn Microsoft DHCP server từ danh sách các service đ-ược liệt kê ở phía dưới và nhấn OK và thực hiện các yêu cầu tiếp theo của Windows NT.

Để cập nhật và khai thác DHCP server chúng ta chọn mục DHCP manager trong Netwrok Administrator Tools.



Hình 11 - Màn hình cài đặt của DHCP

- *Dịch vụ Domain Name Service (DNS)*

Hiện nay trong mạng Internet số lượng các nút (host) lên tới hàng triệu nên chúng ta không thể nhớ hết địa chỉ IP được. Mỗi host ngoài địa chỉ IP còn có một cái tên phân biệt, DNS là 1 cơ sở dữ liệu phân tán cung cấp ánh xạ từ tên host đến địa chỉ IP. Khi đưa ra 1 tên host, DNS server sẽ trả về địa chỉ IP hay 1 số thông tin của host đó. Điều này cho phép người quản lý mạng dễ dàng trong việc chọn tên cho host của mình.

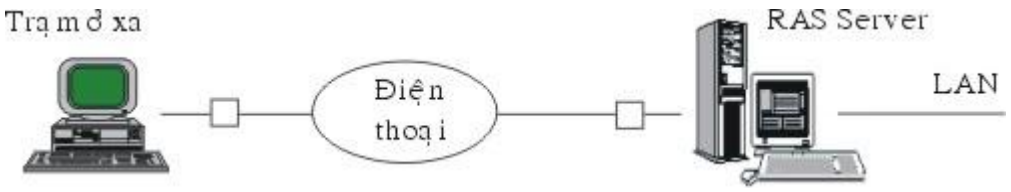
- *Remote Access Service (RAS)*

Ngoài những liên kết tại chỗ với mạng cục bộ (LAN) các nối kết từ xa vào mạng LAN hiện đang là những yêu cầu cần thiết của ngời sử dụng. Việc liên kết đó cho phép một máy từ xa như của một người sử dụng tại nhà có thể qua đường dây điện thoại thâm nhập vào một mạng LAN và sử dụng tài nguyên của nó. Cách thông dụng nhất hiện nay là dùng modem để có thể truyền trên đường dây điện thoại.

Windows NT cung cấp Dịch vụ Remote access Service cho phép các máy trạm có thể nối với tài nguyên của Windows NT server thông qua đường dây điện thoại. RAS cho phép truyền nối với các server, điều hành các user và các server, thực hiện các chương trình khai thác số liệu, thiết lập sự an toàn trên mạng. .

Máy trạm có thể được nối với server có dịch vụ RAS thông qua modem hoặc pull modem, cable null modem (RS232) hoặc X.25 network.

Khi đã cài đặt dịch vụ RAS, cần phải đảm bảo quyền truy nhập từ xa cho người sử dụng bằng tiện ích remote access amind để gán quyền hoặc có thể đăng ký người sử dụng ở remote access server. RAS cũng có cơ chế đảm bảo an toàn cho tài nguyên bằng cách kiểm soát các yếu tố sau: quyền sử dụng, kiểm tra mã số, xác nhận người sử dụng, đăng ký sử dụng tài nguyên và xác nhận quyền gọi lại.



Hình 12- Mô hình truy cập từ xa bằng dịch vụ RAS

1.6 ỨNG DỤNG MẠNG MÁY TÍNH TRONG KINH DOANH

Mạng máy tính có vai trò quan trọng đối với các doanh nghiệp quá trình sản xuất và kinh doanh. Mạng không chỉ giúp cho những ứng dụng trong nội bộ doanh nghiệp được trao đổi thông suốt mà nó còn có tác dụng to lớn trong việc liên kết với khách hàng, bạn hàng, các đối tác kinh doanh. Ví dụ như để phát triển hoạt động kinh doanh của mình thì doanh nghiệp giới thiệu sản phẩm và quảng bá thông tin trên mạng để nhiều người biết đến và sử dụng thông qua nhiều cách khác nhau như gửi thư điện tử, xây dựng trang web giới thiệu… Ngoài ra, ứng dụng của mạng máy tính còn được thể hiện rõ nét trong các hệ thống thương mại điện tử:

- Thư tín điện tử.
- Thanh toán điện tử.
- Trao đổi dữ liệu điện tử.
- Gửi số hoá các dữ liệu.
- Bán hàng hoá hữu hình.
- Giao dịch thương mại điện tử.

Để liên kết với các khách hàng và các đối tác kinh doanh các doanh nghiệp dùng mạng có một trang web động giới thiệu và cập nhật các thông tin của công ty các khách hàng muốn tìm hiểu truy nhập vào trang web của công ty thông qua website các doanh nghiệp quảng cáo sản phẩm và giới thiệu về công ty đồng thời công ty cũng tiến hành tiếp thị nhằm hướng tới các đối tượng mà công ty mong muốn.

Để hiểu được những ứng dụng trong nội bộ doanh nghiệp ta tìm hiểu một cách tường tận hơn về những ứng dụng đó.

Trong nội bộ doanh nghiệp: mạng liên kết các thành viên trong doanh nghiệp một cách gần gũi chặt chẽ hơn làm cho các thành viên trong doanh nghiệp cảm thấy gắn bó hơn với doanh nghiệp đó, là động lực giúp họ gắng sức phấn đấu và làm việc cho doanh nghiệp.

Thông qua mạng máy tính, doanh nghiệp có thể lập lịch làm việc cụ thể của các phòng ban, dễ dàng kiểm tra kiểm soát các thông tin được gửi tới các phòng ban thông qua hệ thống máy tính tránh được sử dụng các văn bản rườm rà, lịch làm việc rõ ràng giúp các bộ phận làm đúng chức năng công việc được điều hành một cách khoa học không bị chồng chéo. Lịch làm việc từ nhà quản lý được chuyển tới các máy của các phòng ban, tới người quản lý trực tiếp sản xuất đảm bảo mọi người được cung cấp đầy đủ về lịch trình làm việc.

Trong ứng dụng công việc: Thông qua mạng của doanh nghiệp, doanh nghiệp sử dụng các chương trình quản lý nhân sự, quản lý tiền lương, quản lý tài chính, quản lý vật tư hệ thống kế toán của doanh nghiệp ... nhờ sử dụng hệ thống mạng doanh nghiệp tin học hoá những những quá trình quản lý nhân sự, tiền lương và hệ thống kế toán, quản lý tài chính, quản lý vật tư. Quá trình quản lý nhân sự nhân sự qua hệ thống mạng giúp doanh nghiệp dễ dàng bố trí và điều chỉnh nhân sự trong doanh nghiệp một cách hợp lý những thông tin về sự thay đổi nhân sự luôn được kiểm soát chặt chẽ. Hệ thống quản lý lương thông qua mạng nội bộ giúp doanh nghiệp tính toán một cách chính xác những đóng góp của các thành viên để có hệ thống thanh toán lương một cách thoả đáng và kịp thời giúp cho các thành viên an tâm hoàn thành công việc của mình một cách tốt nhất. Hệ thống kế toán giúp các nhân viên kế toán giảm bớt khối lượng tính toán và tính toán một cách đơn giản, số lượng được thống nhất trong toàn bộ công ty giúp cho công ty dễ dàng quản lý các báo cáo kế toán. Hệ thống quản lý tài chính của doanh nghiệp giúp doanh nghiệp quản lý ngân sách của mình một cách đảm bảo điều tiết về vốn đầu tư, chi tiêu ngân sách một cách tối ưu để đem lại lợi ích mong muốn cho doanh nghiệp. Thông qua hệ thống mạng, xây dựng hệ thống xử lý đơn hàng cho người cung cấp hàng cũng như khách hàng một cách nhanh nhất và thuận lợi nhất cho cả doanh nghiệp cũng như các bên đối tác.

Các sự kiện của công ty nhanh chóng được cập nhật giúp cho các thành viên trong doanh nghiệp có được những thông tin đầy đủ kịp thời và chính xác đem lại lợi ích cho công ty cũng như các thành viên trong doanh nghiệp. Chẳng hạn doanh nghiệp ra quyết định tuyển dụng cho một chức vụ trưởng phòng một phòng chức năng mới thông tin được cập nhật qua mạng tới tất cả các thành viên trong doanh nghiệp quá trình tuyển chọn thông qua các bài kiểm tra về tâm lý cũng như trình độ và các sáng kiến giúp cho các nhân viên dễ dàng tham gia một cách nhanh nhất mà không cần thông qua các công văn không mất nhiều thời gian và ảnh hưởng tới công việc của công ty hoặc có những có những điều chỉnh về nhân sự, dự kiến công việc thông qua mạng nhân viên trong công ty nhanh chóng biết biết được thông tin và sự kiện của công ty mình. Doanh nghiệp khi cần có thể gửi các thông tin khẩn cấp tới các nhân viên của mình.

Để nâng cao hiệu quả làm việc thông qua mạng của mình doanh nghiệp có thể xúc tiến quá trình đào tạo thông qua hệ thống mạng cho các nhân viên của mình nhằm nâng cao tay nghề cũng như tầm hiểu biết về quản lý thông qua những chương trình đào tạo được mua cài đặt trên hệ thống mạng của công ty cũng như được cập nhật vào mạng. Ứng dụng này làm giảm bớt chi phí đào tạo. Mặt khác giúp cho người học dễ dàng bố trí thời gian phù hợp cho quá trình học tập mà không ảnh hưởng tới công việc.

Sử dụng mạng cục bộ trong doanh nghiệp giúp cho doanh nghiệp trong quá trình quản lý hàng hoá của mình lượng xuất nhập được kiểm soát thường xuyên và luôn được cập nhật. Thông qua hệ thống quản lý vật tư cán bộ quản lý luôn nắm vững lượng tồn kho hoặc thiếu hụt theo kế hoạch giúp cán bộ điều hành quản lý ra những quyết định về tiến độ công việc một cách hợp lý và khoa học.

Ngoài những ứng dụng to lớn trong nội bộ doanh nghiệp nhưng ứng dụng quan trọng và to lớn nhất cuả mạng đó là quá trình cải tiến kinh doanh của doanh nghiệp thông qua hoạt động thương mại điện tử quá trình kinh doanh của doanh thông qua hệ thống mạng thông qua trang web của doanh nghiệp liên kết với bên ngoài.

Những ứng dụng của mạng thông qua hệ thông qua hệ thống thương mại điện tử:

- **Thư tín điện tử**: Thông qua hệ thống thư tín điện tử các doanh nghiệp dễ dàng liên hệ trao đổi với bạn hàng, các đối tác (người tiêu thụ, doanh nghiệp, các cơ quan chính phủ). Thư tín điện tử giúp cho các doanh nghiệp liên hệ với bạn hàng một cách nhanh nhất tới nhiều đôí tượng cùng một lúc đồng thời doanh nghiệp cũng nhận được thông tin từ các đối tác cũng như ý kiến phản hồi từ khách hàng giúp cho doanh nghiệp có những thông tin cần thiết trong chiến lược kinh doanh của mình.
- **Thanh toán điện tử** (electronic payment): là thanh toán tiền thông qua thông điệp tử, thay cho việc giao tay tiền mặt, việc trả lương bằng cách chuyển tiền trực tiếp vào tài khoản, trả tiền mua hàng bằng thẻ mua hàng, thẻ tín dụng … đã quen thuộc bấy lâu nay thực chất đều là thanh toán điện tử. Ngày nay với sự phát triển của thương mại điện tử thanh toán điện tử đã chuyển sang các lĩnh vực mới đáng đề cập là: *Trao đổi dữ liệu điện tử tài chính* (chuyên phục vụ cho việc thanh toán điện tử giữa các công ty giao dịch bằng điện tử); *Tiền mặt Internet* (là tiền mặt được mua từ một nơi phát hành sau đó được chuyển đổi tự do sang các đồng tiền khác thông qua intrenet, áp dụng cả trong phạm vi một nước cũng như các quốc gia); *ví điện tử; thẻ thông minh.*
- **Trao đổi dữ liệu điện tử** (electronic data interchange gọi tắt là EDI): là việc trao đổi các dữ liệu dưới dạng "có cấu trúc" (structured form) từ máy tính điện tử này sang máy tính điện tử khác, giữa các Công ty hay tổ chức đã thoả thuận buôn bán với nhau theo cách này một cách tự động mà không cần có sự can thiệp của con người (gọi là dữ liệu có cấu trúc, vì các bên đối tác phải thoả thuận từ trước khuôn dạng cấu trúc của các thông tin). Uỷ ban Liên hợp quốc về Luật thương mại quốc tế (UNCITRAL)

đã định nghĩa pháp lý sau đây: *"Trao đổi dữ liệu điện tử (EDI) là việc chuyển giao thông tin từ máy tính điện tử này sang máy tính điện tử khác bằng phương tiện điện tử mà sử dụng một tiêu chuẩn đã được thoả thuận để cấu trúc thông tin".*

- **Quảng cáo và tiếp thị qua website:** Thông qua trang web của mình trên mạng các hãng tiến hành các hình thức giới thiệu sản phẩm của mình các hình thức mẫu mã, các tính năng của sản phẩm của mình hay những tính năng cải tiến về hình thức dịch vụ mà các hãng cung cấp. Khi xây dựng trang quảng cáo các nhà quản lý của các hãng đã nghiên cứu những sản phẩm và dịch vụ cung cấp mục đích phục vụ những đối tượng nào để xây dựng có sức thu hút và lôi kéo các khách hàng truy nhập vào trang web của hãng nhằm tăng cường tính cạnh tranh và quảng bá rộng rãi sản phẩm và dịch vụ của mình tới khách hàng.
- **Bán lẻ hàng hoá hữu hình:** ở một số nước internet bắt đầu trở thành công cụ để cạnh tranh bán lẻ hàng hoá hữu hình. Tận dụng tính năng tối ưu của môi trường web người ta xây dựng trên mạng các "cửa hàng ảo" để thực hiện bán hàng. Người sử dụng internet /web tìm trang web của cửa hàng xem hàng hóa hiện thị trên màn hình, xác nhận mua và trả tiền bằng thanh toán điện tử. Lúc đầu việc mua bán như vậy còn ở dạng sơ khai, người mua chọn hàng rồi đặt hàng thông qua mẫu đơn (form) cũng đặt ngay trên Web. Nhưng cũng có trường hợp khách hàng muốn lựa chọn nhiều loại hàng hóa ở các trang web khác nhau (của cùng một cửa hàng) thì hàng hóa được miêu tả nằm ở trang khác, đơn hàng lại nằm ở một trang khác gây ra phiền toái. Để khắc phục điều này, các hãng đưa ra phần mềm mới gọi là "xe mua hàng" mà trên màn hình có dạng tương tự như giỏ mua hàng hay xe mua hàng thật mà người mua thường dùng khi vào siêu thị hoặc giỏ đi theo người mua từ trang web này đến trang web khác để chọn hàng, khi người mua tìm thấy món hàng vừa ý thì ấn vào nút chức năng "bỏ vào giỏ/xe". Các giỏ/xe sẽ tự động tính tiền (kể cả thuế, cước vận chuyển) để thanh toán với khách hàng mua. Ngày nay các phần mềm mới hơn nữa cho phép người mua thoải mái hơn nữa với cửa hàng và hàng hóa. Vì hàng hóa là hữu hình nên tất yếu sau đó cửa hàng phải dùng các phương tiện gửi hàng truyền thống để đưa hàng đến tay khách hàng. Như vậy, điều quan trọng nhất ở phương thức kinh doanh này là khách hàng có thể mua hàng tại nhà mà không cần đến cửa hàng.

BÀI TẬP CHƯƠNG I

Bài 1: Các trường hợp dưới đây, trường hợp nào được gọi là mạng LAN

Có một số máy tính:

a. Được đặt chung trong 1 phòng và dùng chung hệ điều hành WinXP

b. Được đặt chung trong 1 phòng và chia sẻ dữ liệu với nhau bằng đĩa mềm hoặc USB.

c. Được đặt trong nhiều phòng và có kết nối với nhau bằng dây cable, chia sẻ dữ liệu được với nhau.

d. Đặt trong 1 phòng, kết nối với nhau bằng sóng Wifi và dùng nhiều hệ điều hành.

Bài 2: Có một máy tính là thành viên của một mạng LAN trong cơ quan A. Cơ quan này có thuê 1 đường truyền ADSL để kết nối internet. Khi nào ta có thể nói máy tính này đang làm việc trên mạng LAN và khi nào ta có thể nói máy tính này làm việc trên mạng WAN?

Bài 3: Có mấy phương pháp phân loại mạng máy tính, trình bày chi tiết phương pháp phân loại mạng theo kỹ thuật chuyển mạch.

Bài 4: Trong các mô hình sau, mô hình nào là mô hình mạng được dùng phổ biến hiện nay:

a. Peer - to – Peer b. Remote Access

c. Terminal – Mainframe d. Client – Server

Bài 5: Trong số các Hệ điều hành sau, Hệ điều hành mạng là:

a. Windows 98

b. Windows 2003 Professional

c. Windows 2003 Server

d. Windows XP

Bài 6: Công nghệ mạng LAN nào được sử dụng rộng rãi nhất hiện nay?

a. Token Ring b. Ethernet

c. ArcNet d. FDDI

Bài 7: Dịch vụ nào cho phép người sử dụng từ một trạm làm việc của mình có thể đăng nhập vào một trạm ở xa qua mạng và có thể làm việc với hệ thống:

a. FTP b. Email c. Telnet d. WWW

Bài 8: Dịch vụ nào cho phép chuyển các file từ trạm này sang trạm khác, bất kể yếu tố địa lý hay hệ điều hành sử dụng:

a. FTP b. Telnet c. Email d. WWW

Bài 9: Chương trình Telnet cho phép:

a. Người sử dụng từ xa có thể chạy các chương trình ở trên host

b. Gọi một cuộc điện thoại liên quốc gia

c. Hiển thị danh sách các tập tin và thư mục

d. Theo dõi toàn bộ hoạt động của mạng

Bài 10: Đặc điểm nào sau đây không đúng với mạng LAN:

a. Băng thông lớn. b. Băng thông nhỏ

c. Phạm vi hẹp d. Truyền tải dữ liệu tốc độ cao

CHƯƠNG II – CÁC MÔ HÌNH TRUYỀN THÔNG

Mục tiêu

Chương này nhằm giới thiệu cho người học những vấn đề sau:

a. Các chuẩn mạng.

b. Kiến trúc phần mềm của một mạng máy tính, đặc biệt là kiến trúc có thứ bậc của các giao thức mạng.

c. Mô hình tham khảo OSI.

d. Mô hình TCP/IP

2.1 CƠ SỞ LÝ THUYẾT

Để các em nắm bắt được sự cần thiết phải có mô hình truyền thông của mạng máy tính, sau đây chúng ta tìm hiểu quy trình tín dụng của ngân hàng và sự cần thiết của nó trong hoạt động tín dụng của ngân hàng.

Quy trình tín dụng là bảng tổng hợp mô tả công việc của ngân hàng từ khi tiếp nhận hồ sơ vay vốn của một khách hàng cho đến khi quyết định cho vay, giải ngân, thu nợ và thanh lý hợp đồng tín dụng.

Một quy trình tín dụng căn bản

Bước 1: Lập hồ sơ vay vốn

Bước 2: Phân tích tín dụng

Phân tích tín dụng là xác định khả năng hiện tại và tương lai của khách hàng trong việc sử dụng vốn vay + hoàn trả nợ vay.

Bước 3: Ra quyết định tín dụng

Trong khâu này, ngân hàng sẽ ra quyết định đồng ý hoặc từ chối cho vay đối với một hồ sơ vay vốn của khách hàng.

Bước 4: Giải ngân

Ở bước này, ngân hàng sẽ tiến hành phát tiền cho khách hàng theo hạn mức tín dụng đã ký kết trong hợp đồng tín dụng.

Bước 5: Giám sát tín dụng

Nhân viên tín dụng thường xuyên kiểm tra việc sử dụng vốn vay thực tế của khách hàng, hiện trạng tài sản đảm bảo, tình hình tài chính của khách hàng,... để đảm bảo khả năng thu nợ.

Bước 6: Thanh lý hợp đồng tín dụng

Việc xác lập một quy trình tín dụng và không ngừng hoàn thiện nó đặc biệt quan trọng đối với một ngân hàng thương mại. Khi ngân hàng có quy trình tín dụng hợp lý sẽ giúp cho ngân hàng nâng cao chất lượng tín dụng và giảm thiểu rủi ro tín dụng.

Bạn thử tưởng tượng nếu ngân hàng hoạt động tín dụng mà không có quy trình tín dụng thì sẽ ra sao?

Với mạng máy tính cũng vậy, để mạng hoạt động thì phải có một tập các quy tắc nhất định gọi là *mô hình truyền thông*.

Để một mạng máy tính trở thành một môi trường truyền dữ liệu thì nó cần phải có những yếu tố sau:

- Mỗi máy tính cần phải có một địa chỉ phân biệt trên mạng.
- Việc chuyển dữ liệu từ máy tính này đến máy tính khác do mạng thực hiện thông qua những quy định thống nhất gọi là giao thức của mạng.

Khi các máy tính trao đổi dữ liệu với nhau thì một quá trình truyền giao dữ liệu đã được thực hiện hoàn chỉnh. Ví dụ như để thực hiện việc truyền một file giữa một máy tính với một máy tính khác cùng được gắn trên một mạng các công việc sau đây phải được thực hiện:

- Máy tính cần truyền cần biết địa chỉ của máy nhận.
- Máy tính cần truyền phải xác định được máy tính nhận đã sẵn sàng nhận thông tin
- Chương trình gửi file trên máy truyền cần xác định được rằng chương trình nhận file trên máy nhận đã sẵn sàng tiếp nhận file.
- Nếu cấu trúc file trên hai máy không giống nhau thì một máy phải làm nhiệm vụ chuyển đổi file từ dạng này sang dạng kia.
- Khi truyền file máy tính truyền cần thông báo cho mạng biết địa chỉ của máy nhận để các thông tin được mạng đưa tới đích.

Điều trên đó cho thấy giữa hai máy tính đã có một sự phối hợp hoạt động ở mức độ cao. Bây giờ thay vì chúng ta xét cả quá trình trên như là một quá trình chung thì chúng ta sẽ chia quá trình trên ra thành một số công đoạn và mỗi công đoạn con hoạt động một cách độc lập

với nhau. Ở đây chương trình truyền nhận file của mỗi máy tính được chia thành ba module là: Module truyền và nhận File, Module truyền thông và Module tiếp cận mạng. Hai module tương ứng sẽ thực hiện việc trao đổi với nhau trong đó:

- *Module truyền và nhận file:* cần được thực hiện tất cả các nhiệm vụ trong các ứng dụng truyền nhận file. Ví dụ: truyền nhận thông số về file, truyền nhận các mẫu tin của file, thực hiện chuyển đổi file sang các dạng khác nhau nếu cần. Module truyền và nhận file không cần thiết phải trực tiếp quan tâm tới việc truyền dữ liệu trên mạng như thế nào mà nhiệm vụ đó được giao cho Module truyền thông.
- *Module truyền thông:* quan tâm tới việc các máy tính đang hoạt động và sẵn sàng trao đổi thông tin với nhau. Nó còn kiểm soát các dữ liệu sao cho những dữ liệu này có thể trao đổi một cách chính xác và an toàn giữa hai máy tính. Điều đó có nghĩa là phải truyền file trên nguyên tắc đảm bảo an toàn cho dữ liệu, tuy nhiên ở đây có thể có một vài mức độ an toàn khác nhau được dành cho từng ứng dụng. Ở đây việc trao đổi dữ liệu giữa hai máy tính không phụ thuộc vào bản chất của mạng đang liên kết chúng. Những yêu cầu liên quan đến mạng đã được thực hiện ở module thứ ba là module tiếp cận mạng và nếu mạng thay đổi thì chỉ có module tiếp cận mạng bị ảnh hưởng.
- *Module tiếp cận mạng:* được xây dựng liên quan đến các quy cách giao tiếp với mạng và phụ thuộc vào bản chất của mạng. Nó đảm bảo việc truyền dữ liệu từ máy tính này đến máy tính khác trong mạng.

Như vậy thay vì xét cả quá trình truyền file với nhiều yêu cầu khác nhau như một tiến trình phức tạp thì chúng ta có thể xét quá trình đó với nhiều tiến trình con phân biệt dựa trên việc trao đổi giữa các Module tương ứng trong chương trình truyền file. Cách này cho phép chúng ta phân tích kỹ quá trình file và dễ dàng trong việc viết chương trình.

Việc xét các module một cách độc lập với nhau như vậy cho phép giảm độ phức tạp cho việc thiết kế và cài đặt. Phương pháp này được sử dụng rộng rãi trong việc xây dựng mạng và các chương trình truyền thông và được gọi là phương pháp phân tầng (layer).

Nguyên tắc của phương pháp phân tầng là:

- Mỗi hệ thống thành phần trong mạng được xây dựng như một cấu trúc nhiều tầng và đều có cấu trúc giống nhau như: số lượng tầng và chức năng của mỗi tầng.
- Các tầng nằm chồng lên nhau, dữ liệu được chỉ trao đổi trực tiếp giữa hai tầng kề nhau từ tầng trên xuống tầng dưới và ngược lại.
- Cùng với việc xác định chức năng của mỗi tầng chúng ta phải xác định mối quan hệ giữa hai tầng kề nhau. Dữ liệu được truyền đi từ tầng cao nhất của hệ thống truyền lần lượt đến tầng thấp nhất sau đó truyền qua đường nối vật lý dưới dạng các bit tới tầng

thấp nhất của hệ thống nhận, sau đó dữ liệu được truyền ngược lên lần lượt đến tầng cao nhất của hệ thống nhận.

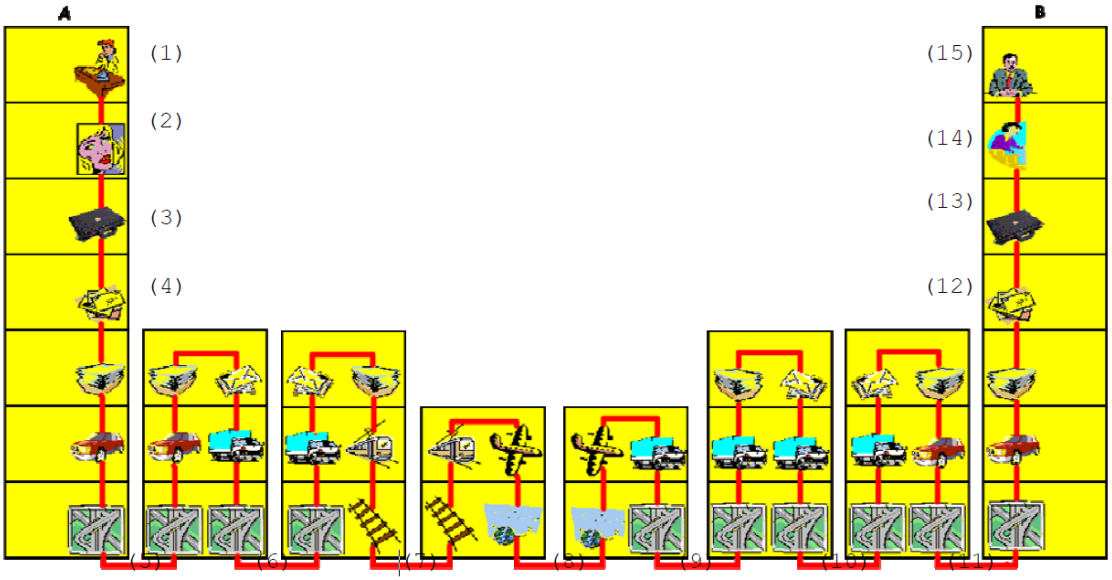
- Chỉ có hai tầng thấp nhất có liên kết vật lý với nhau còn các tầng trên cùng thứ tư chỉ có các liên kết logic với nhau. Liên kết logic của một tầng được thực hiện thông qua các tầng dưới và phải tuân theo những quy định chặt chẽ, các quy định đó được gọi giao thức của tầng.

Để minh họa ý nghĩa của nó ta xem xét mô hình hoạt động của hệ thống gửi nhận thư tín thế giới. Hai đối tác A ở Paris và B ở Thành phố Hà Nội thường xuyên trao đổi thư từ với nhau. Vì A không thể nói tiếng Việt và B không thể nói tiếng Pháp, trong khi đó cả hai có thể hiểu tiếng Anh, cho nên nó được chọn là ngôn ngữ để trao đổi thư từ, văn bản giữa A và B. Cả hai gửi thư từ cơ quan của họ. Trong công ty có bộ phận văn thư lãnh trách nhiệm tập hợp và gửi tất cả các thư của công ty ra bưu điện.

Tiến trình A gửi cho B một lá thư diễn ra như sau:

1. A viết một lá thư bằng tiếng Pháp.
2. A đưa lá thư cho thư ký, biết tiếng Anh để thông dịch lá thư ra tiếng Anh, sau đó bỏ lá thư vào bao thư với địa chỉ người nhận là địa chỉ của B.
3. Nhân viên của bộ phận văn thư chịu trách nhiệm thu thập thư của công ty ghé qua văn phòng của A để nhận thư cần gửi đi.
4. Bộ phận văn thư thực hiện việc phân loại thư và dán tem lên các lá thư bằng một máy dán tem.
5. Lá thư được gửi đến bưu điện ở Paris.
6. Lá thư được ô tô chuyển đến trung tâm phân loại ở Paris.
7. Những lá thư gửi sang Việt Nam được chuyển đến sân bay ở Paris bằng tàu điện ngầm.
8. Lá thư gửi sang Việt nam được chuyển đến sân bay Tân Sơn Nhất (Thành Phố Hồ Chí Minh) bằng máy bay.
9. Thư được ô tô chở đến trung tâm phân loại thư của Thành Phố Hồ Chí Minh.
10. Thư cho cơ quan của B được chuyển về Bưu điện Cần Thơ bằng ô tô.
11. Thư cho cơ quan của B được chuyển đến công ty của B bằng ô tô.
12. Bộ phận văn thư của công ty của B tiến hành phân loại thư.
13. Thư được phát vào một giờ đã định đến các người nhận, trong trường hợp này có văn phòng của B.
14. Thư ký của B mở thư ra và dịch nội dung lá thư gửi cho B sang tiếng Việt.
15. B đọc lá thư của A đã gửi cho anh ta.

Ta có thể tóm tắt lại tiến trình trên bằng một mô hình phân tầng với các nút của mạng thư tín này như sau:



Hình 13- Mô hình gửi nhận thư tín thế giới

Trong mô hình trên,mỗi tầng thì dựa trên tầng phía dưới. Ví dụ, các phương tiện của giao thông của tầng như ô tô, tàu hỏa, máy bay (của tầng liên kết dữ liệu) tầng vận chuyển thì cần hạ tầng cơ sở như đường ô tô, đường sắt, sân bay (của tầng vật lý).

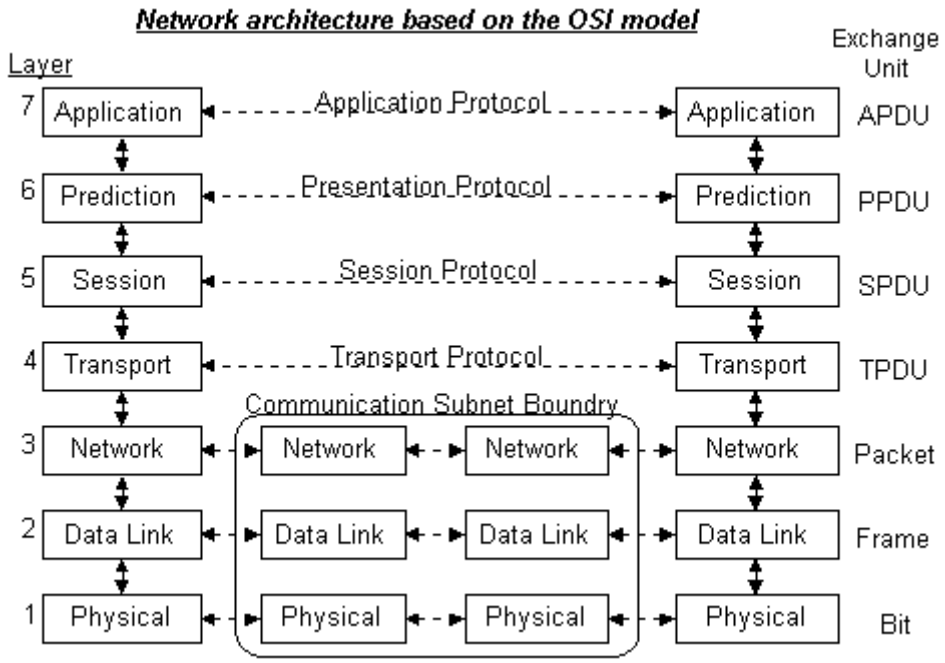
Đối với mỗi tầng, các chức năng được định nghĩa là các dịch vụ cung cấp cho tầng phía trên nó. Các đường thẳng màu đỏ trong sơ đồ xác định các dịch vụ được cung cấp bởi các tầng khác nhau. Thêm vào đó, các chức năng của từng tầng tương ứng với các luật được gọi là các giao thức (Protocols).

2.2 MÔ HÌNH OSI (Open Systems Interconnection) 7 tầng

Để dễ dàng cho việc nối kết và trao đổi thông tin giữa các máy tính với nhau, vào năm 1983, tổ chức tiêu chuẩn thế giới ISO (***The International Standards Organization***) đã phát triển một mô hình cho phép hai máy tính có thể gửi và nhận dữ liệu cho nhau. Mô hình này dựa trên tiếp cận phân tầng (lớp), với mỗi tầng đảm nhiệm một số các chức năng cơ bản nào đó.

Để hai máy tính có thể trao đổi thông tin được với nhau cần có rất nhiều vấn đề liên quan. Ví dụ như cần có Card mạng, dây cáp mạng, điện thế tín hiệu trên cáp mạng, cách thức đóng gói dữ liệu, điều khiển lỗi đường truyền vv... Bằng cách phân chia các chức năng này vào những tầng riêng biệt nhau, việc viết các phần mềm để thực hiện chúng trở nên dễ dàng hơn. Mô hình OSI giúp đồng nhất các hệ thống máy tính khác biệt nhau khi chúng trao đổi thông tin.

Mô hình này gồm có 7 tầng:



Hình 14- Mô hình OSI 7 tầng

Tầng 7: Tầng ứng dụng (Application Layer)

Đây là tầng trên cùng, cung cấp các ứng dụng truy xuất đến các dịch vụ mạng. Nó bao gồm các ứng dụng của người dùng, ví dụ như các Web Browser (Netscape Navigator, Internet Explorer), các Mail User Agent (Outlook Express, Netscape Messenger, ...) hay các chương trình làm server cung cấp các dịch vụ mạng như các Web Server (Netscape Enterprise, Internet Information Service, Apache, ...), Các FTP Server, các Mail server (Send mail, MDeamon). Người dùng mạng giao tiếp trực tiếp với tầng này.

Tầng 6: Tầng trình bày (Presentation Layer)

Tầng này đảm bảo các máy tính có kiểu định dạng dữ liệu khác nhau vẫn có thể trao đổi thông tin cho nhau. Thông thường các mày tính sẽ thống nhất với nhau về một kiểu định dạng dữ liệu trung gian để trao đổi thông tin giữa các máy tính. Một dữ liệu cần gửi đi sẽ được tầng trình bày chuyển sang định dạng trung gian trước khi nó được truyền lên mạng. Ngược lại, khi nhận dữ liệu từ mạng, tầng trình bày sẽ chuyển dữ liệu sang định dạng riêng của nó.

Tầng 5: Tầng giao dịch (Session Layer)

Tầng này cho phép các ứng dụng thiết lập, sử dụng và xóa các kênh giao tiếp giữa chúng (được gọi là giao dịch). Nó cung cấp cơ chế cho việc nhận biết tên và các chức năng về bảo mật thông tin khi truyền qua mạng.

Tầng 4: Tầng vận chuyển (Transport Layer)

Tầng này đảm bảo truyền tải dữ liệu giữa các quá trình. Dữ liệu gửi đi được đảm bảo không có lỗi, theo đúng trình tự, không bị mất mát, trùng lắp. Đối với các gói tin có kích

thước lớn, tầng này sẽ phân chia chúng thành các phần nhỏ trước khi gửi đi, cũng như tập hợp lại chúng khi nhận được.

Tầng 3: Tầng mạng (Network Layer)

Tầng này đảm bảo các gói tin dữ liệu (Packet) có thể truyền từ máy tính này đến máy tính kia cho dù không có đường truyền vật lý trực tiếp giữa chúng. Nó nhận nhiệm vụ tìm đường đi cho dữ liệu đến các đích khác nhau trong mạng.

Tầng 2: Tầng liên kết dữ liệu (Data-Link Layer)

Tầng này đảm bảo truyền tải các khung dữ liệu (Frame) giữa hai máy tính có đường truyền vật lý nối trực tiếp với nhau. Nó cài đặt cơ chế phát hiện và xử lý lỗi dữ liệu nhận.

Tầng 1: Tầng vật ký (Physical Layer) Điều khiển việc truyền tải thật sự các bit trên đường truyền vật lý. Nó định nghĩa các tín hiệu điện, trạng thái đường truyền, phương pháp mã hóa dữ liệu, các loại đầu nối được sử dụng.

Về nguyên tắc, tầng n của một hệ thống chỉ giao tiếp, trao đổi thông tin với tầng n của hệ thống khác. Mỗi tầng sẽ có các đơn vị truyền dữ liệu riêng:

- *Tầng vật lý*: bit
- *Tầng liên kết dữ liệu*: Khung (Frame)
- *Tầng Mạng*: Gói tin (Packet)
- *Tầng vận chuyển*: Đoạn (Segment)

2.2.1 Các giao thức trong mô hình OSI

Trong mô hình OSI có hai loại giao thức chính được áp dụng: giao thức có liên kết (connection - oriented) và giao thức không liên kết (connectionless).

- *Giao thức có liên kết*: trước khi truyền dữ liệu hai tầng đồng mức cần thiết lập một liên kết logic và các gói tin được trao đổi thông qua liên kết náy, việc có liên kết logic sẽ nâng cao độ an toàn trong truyền dữ liệu.
- *Giao thức không liên kết*: trước khi truyền dữ liệu không thiết lập liên kết logic và mỗi gói tin được truyền độc lập với các gói tin trước hoặc sau nó.

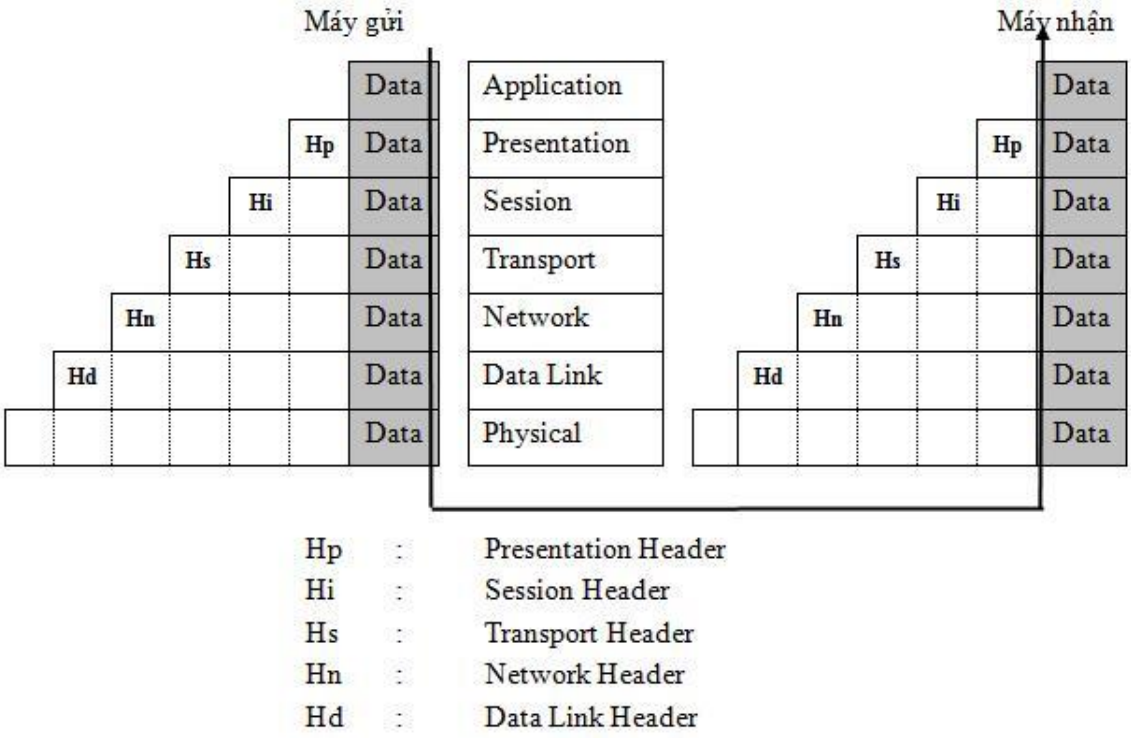
Như vậy với giao thức có liên kết, quá trình truyền thông phải gồm 3 giai đoạn phân biệt:

- *Thiết lập liên kết (logic):* hai thực thể đồng mức ở hai hệ thống thương lượng với nhau về tập các tham số sẽ sử dụng trong giai đoạn sau (truyền dữ liệu).

- *Truyền dữ liệu*: dữ liệu được truyền với các cơ chế kiểm soát và quản lý kèm theo (như kiểm soát lỗi, kiểm soát luồng dữ liệu, cắt/hợp dữ liệu...) để tăng cường độ tin cậy và hiệu quả của việc truyền dữ liệu.
- *Hủy bỏ liên kết (logic):* giải phóng tài nguyên hệ thống đã được cấp phát cho liên kết để dùng cho liên kết khác.

Đối với giao thức không liên kết thì chỉ có duy nhất một giai đoạn truyền dữ liệu mà thôi.

Gói tin của giao thức: Gói tin (Packet) được hiểu như là một đơn vị thông tin dùng trong việc liên lạc, chuyển giao dữ liệu trong mạng máy tính. Những thông điệp (message) trao đổi giữa các máy tính trong mạng, được tạo dạng thành các gói tin ở máy nguồn. Và những gói tin này khi đích sẽ được kết hợp lại thành thông điệp ban đầu. Một gói tin có thể chứa đựng các yêu cầu phục vụ, các thông tin điều khiển và dữ liệu.



Hình 15 - Phương thức xác lập các gói tin trong mô hình OSI

Trên quan điểm mô hình mạng phân tầng tầng mỗi tầng chỉ thực hiện một chức năng là nhận dữ liệu từ tầng bên trên để chuyển giao xuống cho tầng bên dưới và ngược lại. Chức năng này thực chất là gắn thêm và gỡ bỏ phần đầu (header) đối với các gói tin trước khi chuyển nó đi. Nói cách khác, từng gói tin bao gồm phần đầu (header) và phần dữ liệu. Khi đi đến một tầng mới gói tin sẽ được đóng thêm một phần đầu đề khác và được xem như là gói

tin của tầng mới, công việc trên tiếp diễn cho tới khi gói tin được truyền lên đường dây mạng để đến bên nhận.

Tại bên nhận các gói tin được gỡ bỏ phần đầu trên từng tầng tướng ứng và đây cũng là nguyên lý của bất cứ mô hình phân tầng nào.

2.2.2 Các chức năng chủ yếu của các tầng của mô hình OSI.

2.2.2.1. Tầng 1- Vật lý (Physical)

Tầng vật lý (*Physical layer*) là tầng dưới cùng của mô hình OSI là. Nó mô tả các đặc trưng vật lý của mạng: Các loại cáp được dùng để nối các thiết bị, các loại đầu nối được dùng, các dây cáp có thể dài bao nhiêu v.v... Mặt khác các tầng vật lý cung cấp các đặc trưng điện của các tín hiệu được dùng để khi chuyển dữ liệu trên cáp từ một máy này đến một máy khác của mạng, kỹ thuật nối mạch điện, tốc độ cáp truyền dẫn.

Tầng vật lý không qui định một ý nghĩa nào cho các tín hiệu đó ngoài các giá trị nhị phân 0 và 1. Ở các tầng cao hơn của mô hình OSI ý nghĩa của các bit được truyền ở tầng vật lý sẽ được xác định.

Ví dụ: Tiêu chuẩn Ethernet cho cáp xoắn đôi 10 baseT định rõ các đặc trưng điện của cáp xoắn đôi, kích thước và dạng của các đầu nối, độ dài tối đa của cáp.

Khác với các tầng khác, tầng vật lý là không có gói tin riêng và do vậy không có phần đầu (header) chứa thông tin điều khiển, dữ liệu được truyền đi theo dòng bit. Một giao thức tầng vật lý tồn tại giữa các tầng vật lý để quy định về phương thức truyền (đồng bộ, phi đồng bộ), tốc độ truyền.

Các giao thức được xây dựng cho tầng vật lý được phân chia thành phân chia thành hai loại giao thức sử dụng phương thức truyền thông dị bộ (asynchronous) và phương thức truyền thông đồng bộ (synchronous).

- *Phương thức truyền dị bộ*: không có một tín hiệu quy định cho sự đồng bộ giữa các bit giữa máy gửi và máy nhận, trong quá trình gửi tín hiệu máy gửi sử dụng các bit đặc biệt START và STOP được dùng để tách các xâu bit biểu diễn các ký tự trong dòng dữ liệu cần truyền đi. Nó cho phép một ký tự được truyền đi bất kỳ lúc nào mà không cần quan tâm đến các tín hiệu đồng bộ trước đó.
- *Phương thức truyền đồng bộ*: sử dụng phương thức truyền cần có đồng bộ giữa máy gửi và máy nhận, nó chèn các ký tự đặc biệt như SYN (Synchronization), EOT (End Of Transmission) hay đơn giản hơn, một cái "cờ " (flag) giữa các dữ liệu của máy gửi để báo hiệu cho máy nhận biết được dữ liệu đang đến hoặc đã đến.

2.2.2.2.Tầng 2 - Liên kết dữ liệu (Data link)

Tầng liên kết dữ liệu (*data link layer*) là tầng mà ở đó ý nghĩa được gán cho các bit được truyền trên mạng. Tầng liên kết dữ liệu phải quy định được các dạng thức, kích thước, địa chỉ máy gửi và nhận của mỗi gói tin được gửi đi. Nó phải xác định cơ chế truy nhập thông tin trên mạng và phương tiện gửi mỗi gói tin sao cho nó được đưa đến cho người nhận đã định.

Tầng liên kết dữ liệu có hai phương thức liên kết dựa trên cách kết nối các máy tính, đó là phương thức "*một điểm - một điểm*" và phương thức "*một điểm - nhiều điểm*". Với phương thức "một điểm - một điểm" các đường truyền riêng biệt được thiết lập để nối các cặp máy tính lại với nhau. Phương thức "một điểm - nhiều điểm " tất cả các máy phân chia chung một đường truyền vật lý.

Tầng liên kết dữ liệu cũng cung cấp cách phát hiện và sửa lỗi cơ bản để đảm bảo cho dữ liệu nhận được giống hoàn toàn với dữ liệu gửi đi. Nếu một gói tin có lỗi không sửa được, tầng liên kết dữ liệu phải chỉ ra được cách thông báo cho nơi gửi biết gói tin đó có lỗi để nó gửi lại.

Các giao thức tầng liên kết dữ liệu chia làm 2 loại chính là các giao thức hướng ký tư và các giao thức hướng bit. Các giao thức hướng ký tự được xây dựng dựa trên các ký tự đặc biệt của một bộ mã chuẩn nào đó (như ASCII hay EBCDIC), trong khi đó các giao thức hướng bit lại dùng các cấu trúc nhị phân (xâu bit) để xây dựng các phần tử của giao thức (đơn vị dữ liệu, các thủ tục.) và khi nhận, dữ liệu sẽ được tiếp nhận lần lượt từng bit một.

2.2.2.3. Tầng 3 - Mạng (Network)

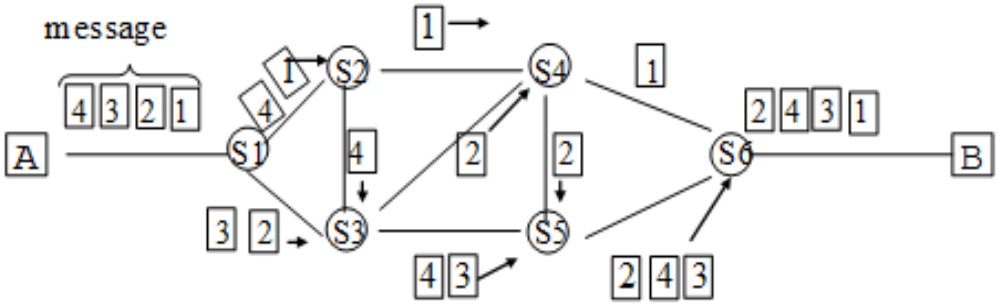
Tầng mạng (*network layer*) nhắm đến việc kết nối các mạng với nhau bằng cách tìm đường (routing) cho các gói tin từ một mạng này đến một mạng khác. Nó xác định việc chuyển hướng, vạch đường các gói tin trong mạng, các gói này có thể phải đi qua nhiều chặng trước khi đến được đích cuối cùng. Nó luôn tìm các tuyến truyền thông không tắc nghẽn để đưa các gói tin đến đích.

Tầng mạng cung các các phương tiện để truyền các gói tin qua mạng, thậm chí qua một mạng của mạng (network of network). Bởi vậy nó cần phải đáp ứng với nhiều kiểu mạng và nhiều kiểu dịch vụ cung cấp bởi các mạng khác nhau. hai chức năng chủ yếu của tầng mạng là chọn đường (routing) và chuyển tiếp (relaying). Tầng mạng là quan trọng nhất khi liên kết hai loại mạng khác nhau như mạng Ethernet với mạng Token Ring khi đó phải dùng một bộ tìm đường (quy định bởi tầng mạng) để chuyển các gói tin từ mạng này sang mạng khác và ngược lại.

Đối với một mạng chuyển mạch gói (packet - switched network) - gồm tập hợp các nút chuyển mạch gói nối với nhau bởi các liên kết dữ liệu. Các gói dữ liệu được truyền từ một hệ thống mở tới một hệ thống mở khác trên mạng phải được chuyển qua một chuỗi các nút. Mỗi nút nhận gói dữ liệu từ một đường vào (incoming link) rồi chuyển tiếp nó tới một đường ra (outgoing link) hướng đến đích của dữ liệu. Như vậy ở mỗi nút trung gian nó phải thực hiện các chức năng chọn đường và chuyển tiếp.

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

- Quyết định chọn đường tối ưu dựa trên các thông tin đã có về mạng tại thời điểm đó thông qua những tiêu chuẩn tối ưu nhất định.
- Cập nhật các thông tin về mạng, tức là thông tin dùng cho việc chọn đường, trên mạng luôn có sự thay đổi thường xuyên nên việc cập nhật là việc cần thiết.



Hình 16 - Mô hình chuyển vận các gói tin trong mạng chuyễn mạch gói

Người ta có hai phương thức đáp ứng cho việc chọn đường là phương thức xử lý tập trung và xử lý tại chỗ.

- *Phương thức chọn đường xử lý tập trung* được đặc trưng bởi sự tồn tại của một (hoặc vài) trung tâm điều khiển mạng, chúng thực hiện việc lập ra các bảng đường đi tại từng thời điểm cho các nút và sau đó gửi các bảng chọn đường tới từng nút dọc theo con đường đã được chọn đó. Thông tin tổng thể của mạng cần dùng cho việc chọn đường chỉ cần cập nhập và được cất giữ tại trung tâm điều khiển mạng.
- *Phương thức chọn đường xử lý tại chỗ* được đặc trưng bởi việc chọn đường được thực hiện tại mỗi nút của mạng. Trong từng thời điểm, mỗi nút phải duy trì các thông tin của mạng và tự xây dựng bảng chọn đường cho mình. Như vậy các thông tin tổng thể của mạng cần dùng cho việc chọn đường cần cập nhập và được cất giữ tại mỗi nút.

Thông thường các thông tin được đo lường và sử dụng cho việc chọn đường bao gồm:

- Trạng thái của đường truyền.
- Thời gian trễ khi truyền trên mỗi đường dẫn.
- Mức độ lưu thông trên mỗi đường.
- Các tài nguyên khả dụng của mạng.

Khi có sự thay đổi trên mạng (ví dụ thay đổi về cấu trúc của mạng do sự cố tại một vài nút, phục hồi của một nút mạng, nối thêm một nút mới... hoặc thay đổi về mức độ lưu thông) các thông tin trên cần được cập nhật vào các cơ sở dữ liệu về trạng thái của mạng.

Hiện nay khi nhu cầu truyền thông đa phương tiện (tích hợp dữ liệu văn bản, đồ hoạ, hình ảnh, âm thanh) ngày càng phát triển đòi hỏi các công nghệ truyền dẫn tốc độ cao nên việc phát triển các hệ thống chọn đường tốc độ cao đang rất được quan tâm.

2.2.2.4. Tầng 4 - Vận chuyển (Transport)

Tầng vận chuyển cung cấp các chức năng cần thiết giữa tầng mạng và các tầng trên. nó là tầng cao nhất có liên quan đến các giao thức trao đổi dữ liệu giữa các hệ thống mở. Nó cùng các tầng dưới cung cấp cho người sử dụng các phục vụ vận chuyển.

Tầng vận chuyển (transport layer) là tầng cơ sở mà ở đó một máy tính của mạng chia sẻ thông tin với một máy khác. Tầng vận chuyển đồng nhất mỗi trạm bằng một địa chỉ duy nhất và quản lý sự kết nối giữa các trạm. Tầng vận chuyển cũng chia các gói tin lớn thành các gói tin nhỏ hơn trước khi gửi đi. Thông thường tầng vận chuyển đánh số các gói tin và đảm bảo chúng chuyển theo đúng thứ tự.

Tầng vận chuyển là tầng cuối cùng chịu trách nhiệm về mức độ an toàn trong truyền dữ liệu nên giao thức tầng vận chuyển phụ thuộc rất nhiều vào bản chất của tầng mạng. Người ta chia giao thức tầng mạng thành các loại sau:

- ***Mạng loại A***: Có tỷ suất lỗi và sự cố có báo hiệu chấp nhận được (tức là chất lượng chấp nhận được). Các gói tin được giả thiết là không bị mất. Tầng vận chuyển không cần cung cấp các dịch vụ phục hồi hoặc sắp xếp thứ tự lại.
- ***Mạng loại B***: Có tỷ suất lỗi chấp nhận được nhưng tỷ suất sự cố có báo hiệu lại không chấp nhận được. Tầng giao vận phải có khả năng phục hồi lại khi xảy ra sự cố.
- ***Mạng loại C***: Có tỷ suất lỗi không chấp nhận được (không tin cậy) hay là giao thức không liên kết. Tầng giao vận phải có khả năng phục hồi lại khi xảy ra lỗi và sắp xếp lại thứ tự các gói tin.

Trên cơ sở loại giao thức tầng mạng chúng ta có 5 lớp giao thức tầng vận chuyển đó là:

- *Giao thức lớp 0 (Simple Class - lớp đơn giản)*: cung cấp các khả năng rất đơn giản để thiết lập liên kết, truyền dữ liệu và hủy bỏ liên kết trên mạng "có liên kết" loại A. Nó có khả năng phát hiện và báo hiệu các lỗi nhưng không có khả năng phục hồi.
- *Giao thức lớp 1 (Basic Error Recovery Class - Lớp phục hồi lỗi cơ bản)* dùng với các loại mạng B, ở đây các gói tin (TPDU) được đánh số. Ngoài ra giao thức còn có khả năng báo nhận cho nơi gửi và truyền dữ liệu khẩn. So với giao thức lớp 0 giao thức lớp 1 có thêm khả năng phục hồi lỗi.
- *Giao thức lớp 2 (Multiplexing Class - lớp dồn kênh)* là một cải tiến của lớp 0 cho phép dồn một số liên kết chuyển vận vào một liên kết mạng duy nhất, đồng thời có thể kiểm soát luồng dữ liệu để tránh tắc nghẽn. Giao thức lớp 2 không có khả năng phát hiện và phục hồi lỗi. Do vậy nó cần đặt trên một tầng mạng loại A.
- *Giao thức lớp 3 (Error Recovery and Multiplexing Class - lớp phục hồi lỗi cơ bản và dồn kênh)* là sự mở rộng giao thức lớp 2 với khả năng phát hiện và phục hồi lỗi, nó cần đặt trên một tầng mạng loại B.
- *Giao thức lớp 4 (Error Detection and Recovery Class - Lớp phát hiện và phục hồi lỗi)* là lớp có hầu hết các chức năng của các lớp trước và còn bổ sung thêm một số khả năng khác để kiểm soát việc truyền dữ liệu.

2.2.2.5. Tầng 5 - Giao dịch (Session)

Tầng giao dịch (session layer) thiết lập "các giao dịch" giữa các trạm trên mạng, nó đặt tên nhất quán cho mọi thành phần muốn đối thoại với nhau và lập ánh xa giữa các tên với địa chỉ của chúng. Một giao dịch phải được thiết lập trước khi dữ liệu được truyền trên mạng, tầng giao dịch đảm bảo cho các giao dịch được thiết lập và duy trì theo đúng qui định.

Tầng giao dịch còn cung cấp cho người sử dụng các chức năng cần thiết để quản trị các giao dịnh ứng dụng của họ, cụ thể là:

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

Trong trường hợp mạng là hai chiều luân phiên thì nẩy sinh vấn đề: hai người sử dụng luân phiên phải "lấy lượt" để truyền dữ liệu. Tầng giao dịch duy trì tương tác luân phiên bằng cách báo cho mỗi người sử dụng khi đến lượt họ được truyền dữ liệu. Vấn đề đồng bộ hóa trong tầng giao dịch cũng được thực hiện như cơ chế kiểm tra/phục hồi, dịch vụ này cho phép

người sử dụng xác định các điểm đồng bộ hóa trong dòng dữ liệu đang chuyển vận và khi cần thiết có thể khôi phục việc hội thoại bắt đầu từ một trong các điểm đó

Ở một thời điểm chỉ có một người sử dụng đó quyền đặc biệt được gọi các dịch vụ nhất định của tầng giao dịch, việc phân bổ các quyền này thông qua trao đổi thẻ bài (token). Ví dụ: Ai có được token sẽ có quyền truyền dữ liệu, và khi người giữ token trao token cho người khác thi cũng có nghĩa trao quyền truyền dữ liệu cho người đó.

Tầng giao dịch có các hàm cơ bản sau:

- *Give Token* cho phép người sử dụng chuyển một token cho một người sử dụng khác của một liên kết giao dịch.
- *Please Token* cho phép một người sử dụng chưa có token có thể yêu cầu token đó.
- *Give Control* dùng để chuyển tất cả các token từ một người sử dụng sang một người sử dụng khác.

2.2.2.6. Tầng 6 - Trình bày (Presentation)

Trong giao tiếp giữa các ứng dụng thông qua mạng với cùng một dữ liệu có thể có nhiều cách biểu diễn khác nhau. Thông thường dạng biểu diễn dùng bởi ứng dụng nguồn và dạng biểu diễn dùng bởi ứng dụng đích có thể khác nhau do các ứng dụng được chạy trên các hệ thống hoàn toàn khác nhau (như hệ máy Intel và hệ máy Motorola). Tầng trình bày (Presentation layer) phải chịu trách nhiệm chuyển đổi dữ liệu gửi đi trên mạng từ một loại biểu diễn này sang một loại khác. Để đạt được điều đó nó cung cấp một dạng biểu diễn chung dùng để truyền thông và cho phép chuyển đổi từ dạng biểu diễn cục bộ sang biểu diễn chung và ngược lại.

Tầng trình bày cũng có thể được dùng kĩ thuật mã hóa để xáo trộn các dữ liệu trước khi được truyền đi và giải mã ở đầu đến để bảo mật. Ngoài ra tầng biểu diễn cũng có thể dùng các kĩ thuật nén sao cho chỉ cần một ít byte dữ liệu để thể hiện thông tin khi nó được truyền ở trên mạng, ở đầu nhận, tầng trình bày bung trở lại để được dữ liệu ban đầu.

2.2.2.7. Tầng 7- Ứng dụng (Application)

Tầng ứng dụng (Application layer) là tầng cao nhất của mô hình OSI, nó xác định giao diện giữa người sử dụng và môi trường OSI và giải quyết các kỹ thuật mà các chương trình ứng dụng dùng để giao tiếp với mạng.

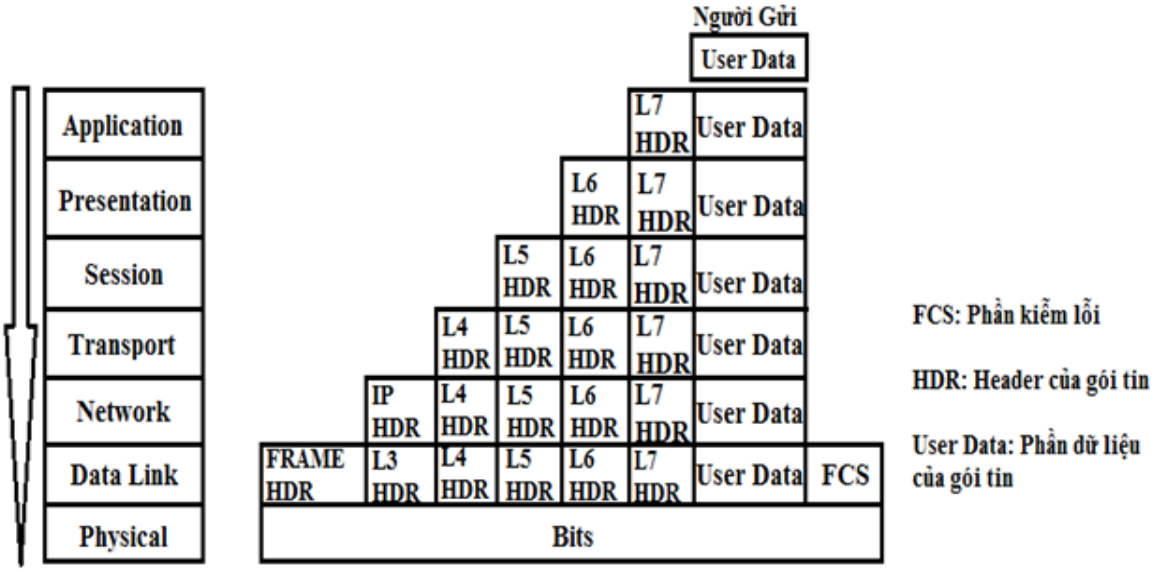
Để cung cấp phương tiện truy nhập môi trường OSI cho các tiến trình ứng dụng, Người ta thiết lập các thực thể ứng dụng (AE), các thực thể ứng dụng sẽ gọi đến các phần tử dịch vụ

ứng dụng (Application Service Element - viết tắt là ASE) của chúng. Mỗi thực thể ứng dụng có thể gồm một hoặc nhiều các phần tử dịch vụ ứng dụng. Các phần tử dịch vụ ứng dụng được phối hợp trong môi trường của thực thể ứng dụng thông qua các liên kết (association) gọi là đối tượng liên kết đơn (Single Association Object - viết tắt là SAO). SAO điều khiển việc truyền thông trong suốt vòng đời của liên kết đó cho phép tuần tự hóa các sự kiện đến từ các ASE thành tố của nó.

2.2.3 Hoạt động của Mô hình OSI 7 tầng

2.2.3.1. Quá trình đóng gói dữ liệu (Data Encaspulation)

Người gửi: Gửi một dữ liệu người dùng,dữ liệu này đi đầu tiên vào tầngứng dụng và được đóng thêm một nhãnởtầngưng dụng, sau đó đi xuống tầng trình diễn lúc này toàn bộ nội dung của gói tin ở tầngứng dụng trở thành data của gói tin tầng trình diễn và tầng trình diễn đóng thêm một nhãn vào gói tin, tương tự với các tầng còn lại, tức là toàn bộ gói tin tầng trên sẽ là dữ liệu gói tin tầng dưới, riêng tầng mạng sẽ được đóng IP header, còn tầng kết nối dữ liệu sẽ được đóng Frame header và bọc thêm phần kiểm tra lỗi FCS, sau khi gói tin đến tầng vật lý sẽ được chuyển sang dạng tín hiệu điện và được truyền dưới dạng bit 1 và bit 0.

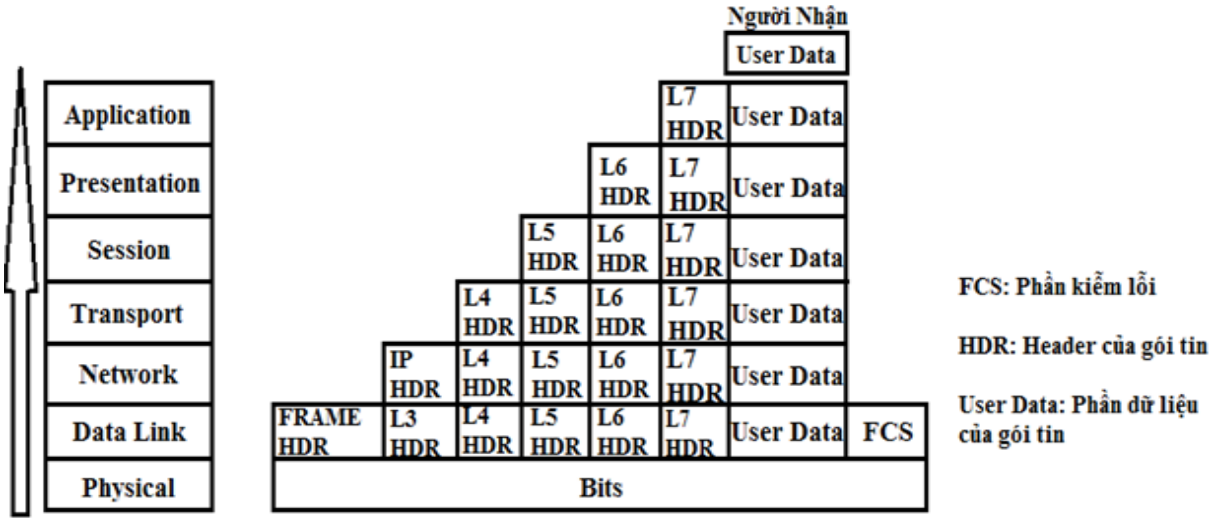


Hình 17 – Quá trình đóng gói dữ liệu

2.2.3.2. Quá trình mở dữ liệu (Data decapsulation)

Người Nhận: Lúc này quá trình diễn ra ngược lại so với quá trình người gửi, lúc này dòng bit nhị phân đi vào đường truyền vật lý và được đưa dần lên trên, đầu tiên khi đưa lên tầng liên kết dữ liệu nó sẽ được chuyển thành cấu trúc khung thành một đơn vị dữ liệu tầng liên kết dữ liệu, sau đó dữ liệu bắt đầu gỡ bỏ Frame header và FCS ở tầng liên kết dữ liệu để chuyển lên

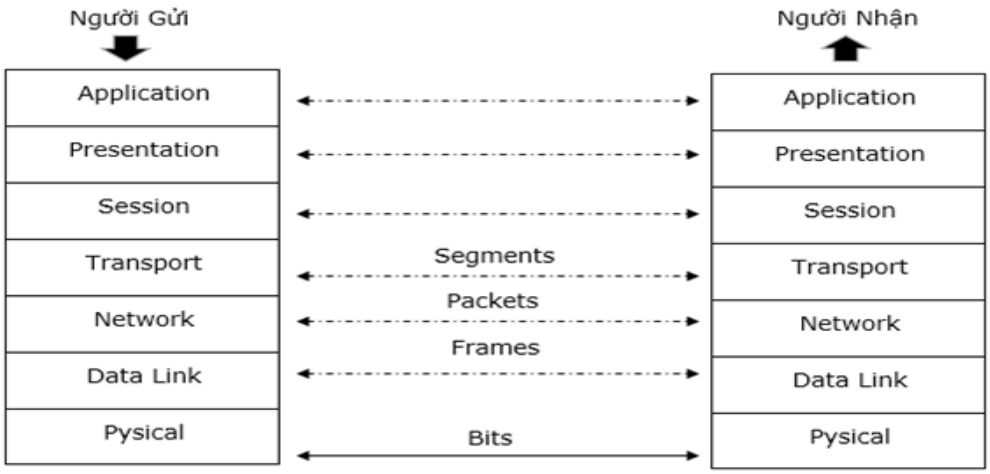
tầng mạng, tầng mạng tiếp tục gỡ bỏ IP header để chuyển lên tầng phiên cứ như thế mỗi lần đi lên lần lượt dữ liệu lại bỏ đi một header và cuối cùng khi đến tay người nhận thì nó trả lại nguyên vẹn dữ liệu ban đầu.



Hình 18 – Quá trình mở dữ liệu

2.2.3.3. Quá trình truyền thông ngang hàng (peer to peer)

Quá trình truyền thông ngang hàng mô phỏng cuộc nói chuyện đồng cấp chứ không phải di chuyển từ trên xuống, lúc này ta có tầng ứng dụng như thể đang nói chuyện với ứng dụng vậy, tương tự cho các tầng còn lại, lúc này chúng ta có đơn vị dữ liệu của các kết nối ngang hàng là có tên riêng, đơn vị của tầng Giao vận là **Segment** hoặc **Datagram**, đơn vị của tầng Mạng là Packet, đơn vị của tầng Liên kết dữ liệu là Frame, đơn vị của tầng Vật lý là Bit.



Hình 19 – Quá trình truyền thông ngang hàng

2.3 MÔ HÌNH TCP/IP

Bộ giao thức liên mạng xuất phát từ công trình DARPA, từ những năm đầu thập niên kỷ 1970. Sau khi đã hoàn thành việc xây dựng ARPANET tiên phong, DARPA bắt đầu công việc trên một số những kỹ thuật truyền thông dữ liệu khác. Vào năm 1972, Robert E. Kahn đã được thuê vào làm việc tại Văn phòng kỹ thuật điều hành tin tức (*Information Processing Technology Office*) của DARPA, phòng có chức năng liên quan đến mạng lưới truyền thông dữ liệu thông qua vệ tinh và mạng lưới truyền thông bằng sóng radio trên mặt đất. Trong quá trình làm việc tại đây Kahn đã phát hiện ra giá trị của việc liên thông giữa chúng. Vào mùa xuân năm 1973, Vinton Cerf, kỹ sư thiết kế bản giao thức NCP hiện dùng (*chương trình ứng dụng xử lý mạng lưới truyền thông - nguyên tiếng Anh là "Network Control Program"*), được phân công cùng làm việc với Kahn trên các mô hình liên kết nối kiến trúc mở (*open-architecture interconnection models*) với mục đích thiết kế giao thức sắp tới của ARPANET.

Vào mùa hè năm 1973, Kahn và Cerf đã nhanh chóng tìm ra một phương pháp tái hội nhập căn bản, mà trong đó những khác biệt của các giao thức liên kết mạng được che lấp đi bằng một giao thức liên kết mạng chung, và thay vì mạng lưới truyền thông phải chịu trách nhiệm về tính đáng tin cậy, như trong ARPANET, thì các máy chủ (*hosts*) phải chịu tránh nhiệm.

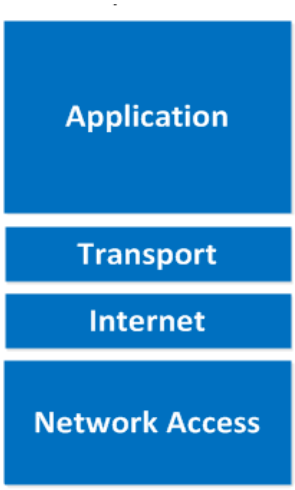
Với nhiệm vụ là một mạng lưới truyền thông bị hạ cấp tới mức cơ bản tối thiểu, khiến việc hội nhập với các mạng lưới truyền thông khác trở nên hầu như bất khả thi, mặc dầu đặc tính của chúng là gì, và vì thế, giải đáp nan đề đầu tiên của Kahn. Một câu nói cửa miệng vì thế mà TCP/IP, sản phẩm cuối cùng do những cống hiến của Cerf và Kahn, sẽ chạy trên "đường dây nối giữa hai ống bơ rỉ", và quả nhiên nó đã được thực thi dùng các con chim bồ câu đưa thư (*homing pigeons*). Một máy vi tính được dùng là *cổng nối* (*gateway*) (sau này đổi thành *bộ định tuyến* (*router*) để tránh nhầm với những loại *cổng nối* khác) được thiết bị một giao diện với từng mạng lưới truyền thông, truyền tải gói dữ liệu qua lại giữa chúng.

Ý tưởng này được nhóm nghiên cứu mạng lưới truyền thông của Cerf, tại Stanford, diễn giải ra tỉ mỉ, cụ thể vào khoảng thời gian trong năm 1973-1974. (Những công trình về mạng lưới truyền thông trước đó tại Xerox PARC, nơi sản sinh ra bộ giao thức PARC Universal Packet, phần lớn được dùng vào thời kỳ đó, cũng gây ảnh hưởng về kỹ thuật không ít; nhiều người nhảy qua nhảy lại giữa hai cái.)

Sau đó DARPA ký hợp đồng với BBN, Stanford, và Trường đại học chuyên nghiệp Luân Đôn (*The University College London - viết tắt là UCL*) kiến tạo một số phiên bản của giao thức làm việc được, trên các nền tảng phần cứng khác nhau. Có bốn phiên bản đã được xây dựng—TCP v1, TCP v2. Phiên bản 3 được tách ra thành hai phần TCP v3 và IP v3, vào mùa xuân năm 1978, và sau đó ổn định hóa với phiên bản TCP/IP v4—giao thức tiêu chuẩn hiện dùng của Internet ngày nay.

2.3.1 Kiến trúc mô hình TCP/IP

Mô hình TCP/IP tổ chức các tác vụ của việc truyền dữ liệu thành 4 tầng thay vì 7 tầng của mô hình OSI. Các tầng từ trên xuống dưới lần lượt là: Application (tầng ứng dụng) , Transport (Tầng vận chuyển), Internet (tầng Internet), và Network Access (Tầng truy nhập mạng)



Hình 20- Kiến trúc Mô hình TCP/IP

2.3.1.1.Tầng truy nhập mạng (Network Interface Layer)

Tầng thấp nhất của mô hình TCP/IP chính là tầng truy nhập mạng, tầng này có trách nhiệm nhận các IP datagram và truyền chúng trên một mạng nhất định.

Tầng truy nhập mạng bao gồm tầng Liên kết dữ liệu (Data Link) và tầng Vật lý (Physical) của mô hình OSI. Tầng truy nhập mạng bao gồm các thiết bị giao tiếp mạng và các chương trình cung cấp các thông tin cần thiết để có thể hoạt động, truy nhập đường truyền vật lý qua các thiết bị giao tiếp mạng đó. Tại tầng này, hệ thống giao tiếp với rất nhiều kiểu mạng khác nhau. Cung cấp các trình điều khiển để tương tác với các thiết bị phần cứng ví dụ như Token Ring, Ethernet, FDDI…

2.3.1.2. Tầng Internet

Tầng Internet có nhiệm vụ tương tự tầng mạng trong mô hình OSI 7 tầng. Tầng này xử lý quá trình truyền gói tin trên mạng, các giao thức của tầng này bao gồm: IP (Internet Protocol) , ICMP (Internet Control Message Protocol) , IGMP (Internet Group Message Protocol)

- Giao thức IP - (Internet Protocol) là một giao thực có khả năng dẫn đường cho các địa chỉ IP, phân chia và tập hợp lại các gói tin.

- Giao thức ARP - Address Resolution Protocol (giao thức phân giải địa chỉ) chịu trách nhiệm phân giải địa chỉ tầng Internet chuyển thành địa chỉ tầng giao tiếp mạng, như địa chỉ phần cứng.
- Giao thức ICMP - Internet Control Message Protocol chịu trách nhiệm đưa ra các chức năng chuẩn đoán và thông báo lỗi hay theo dõi các điều kiện lưu chuyển các gói tin IP.
- Giao thức IGMP – Internet Group Management Protocol chịu trách nhiệm quản lý các nhóm IP truyền multicast.

2.3.1.3. Tầng vận chuyển

Tầng vận chuyển (còn được gọi là tầng truyền Trạm-tới-Trạm Host-to-Host Transport Layer) tương tự như tầng vận chuyển của mô hình OSI 7 tầng, chịu trách nhiệm cung cấp cho tầng ứng dụng các dịch vụ tạo lập phiên và truyền dữ liệu. Tầng vận chuyển thiết lập một cầu nối logic giữa các đầu cuối của mạng, giữa host truyền và host nhận. Giao thức vận chuyển phân chia và tái thiết lập dữ liệu của các ứng dụng lớp trên thành luồng dữ liệu giống nhau giữa các đầu cuối. Luồng dữ liệu của lớp vận chuyển cung cấp các dịch vụ truyền tải từ đầu cuối này đến đầu cuối kia của mạng. Ngày nay Internet thường được biểu diễn bằng một đám mây (cloud). Vì vậy, tầng vận chuyển vận chuyển gửi các gói từ nguồn đến đích xuyên qua mây mạng này. Điều khiển end-to-end, được cung cấp bởi cửa sổ trượt (sliding windows) và tính tin cậy trong các số tuần tự và sự báo nhận, là nhiệm vụ then chốt của lớp vận chuyển khi dùng TCP. Tầng vận chuyển cũng định nghĩa kết nối end-to-end giữa các ứng dụng của host.

Các giao thức lõi của tầng vận chuyển là TCP và UDP (User Datagram Protocol).

- TCP cung cấp các dịch vụ truyền thông tin cậy một-một (one-to-one), hướng liên kết (connection-oriented). TCP chịu trách nhiệm thiết lập các kết nối TCP, gửi các gói tin có sắp xếp, thông báo, và các gói tin phục hồi dữ liệu bị mất trong quá trình truyền.
- UDP cung cấp các dịch vụ truyền tin một-một, một-nhiều, không liên kết và không tin cậy. UDP được sử dụng khi lượng dữ liệu cần truyền nhỏ (ví dụ dữ liệu không điền hết một gói tin), khi việc thiết lập liên kết TCP là không cần thiết, hoặc khi các ứng dụng hoặc các giao thức tầng trên cung cấp dịch vụ đảm bảo trong khi truyền.

2.3.1.4. Tầng ứng dụng

Tầng ứng dụng cung cấp các ứng dụng với khả năng truy cập các dịch vụ của các tầng khác và định nghĩa các giao thức mà các ứng dụng sử dụng để trao đổi dữ liệu. Một ứng dụng tương tác với một trong những protocol ở mức giao vận (transport) để gửi hoặc nhận dữ liệu. Mỗi chương trình ứng dụng chọn một kiểu giao vận mà nó cần, có thể là một dãy tuần tự từng thông điệp hoặc một chuỗi các byte liên tục. Chương trình ứng dụng sẽ gửi dữ liệu đi dưới dạng nào đó mà nó yêu cầu đến lớp giao vận.

Các giao thức được ứng dụng rộng rãi nhất của tầng ứng dụng được sử dụng để trao đổi thông tin của người sử dụng là:

- Giao thức truyền tin siêu văn bản HTTP (HyperText Transfer Protocol) được sử dụng để truyền các tệp tạo nên trang web của World Wide Web.
- Giao thức FTP - File Transfer Protocol được sử dụng để thực hiện truyền file.
- Giao thức SMTP - Simple Mail Transfer Protocol được sử dụng để truyền các thông điệp thư và các tệp đính kèm.
- Telnet, một giao thức mô phỏng trạm đầu cuối, được sử dụng để đăng nhập từ xa vào các máy trạm trên mạng.

Hơn nữa, các giao thức ứng dụng sau tạo giúp dễ dàng sử dụng và quản lý mạng TCP/IP.

- Domain Name System (DNS) được sử dụng để chuyển từ tên trạm thành địa chỉ IP.
- Giao thức RIP - Routing Information Protocol là giao thức dẫn đường mà các router sử dụng để trao đổi các thông tin dẫn đường gói tin IP trong mạng.
- Giao thức SNMP - Simple Network Management Protocol được sử dụng giữa giao diện quản lý mạng và các thiết bị mạng (router, bridges, và hub thông minh) để thu thập và trao đổi thông tin quản lý mạng.

Ví dụ của tầng ứng dụng giao tiếp với các ứng dụng TCP/IP là Windows Sockets và NetBIOS. Windows Sockets cung cấp một chuẩn giao diện lập trình ứng dụng API (application-programming interface) trên nên hệ điều hành Windows. NetBIOS là một chuẩn công nghiệp giao tiếp dể truy cập các dịch vụ như dịch vụ phiên, truyền dữ liệu, và phân giải tên. Thông tin chi tiết về NetBIOS được cung cấp ở cuối chương này.

2.3.2 Giao thức IP

2.3.2.1. Địa chỉ Ipv4

2.3.2.1.1. Địa chỉ Ipv4

Nhiệm vụ chính của giao thức IP là cung cấp khả năng kết nối các mạng con thành liên kết mạng để truyền dữ liệu, vai trò của IP là vai trò của giao thức tầng mạng trong mô hình OSI. Giao thức IP là một giao thức kiểu không liên kết (connectionlees) có nghĩa là không cần có giai đoạn thiết lập liên kết trước khi truyền dữ liệu.

Sơ đồ địa chỉ hóa để định danh các trạm (host) trong liên mạng được gọi là địa chỉ IP 32 bits (32 bit IP address). Mỗi giao diện trong 1 máy có hỗ trợ giao thức IP đều phải được gán 1 địa chỉ IP (một máy tính có thể gắn với nhiều mạng do vậy có thể có nhiều địa chỉ IP). Địa chỉ Ipv4 gồm 2 phần: địa chỉ mạng (netid) và địa chỉ máy (hostid). Mỗi địa chỉ Ipv4 có độ dài 32

bits được tách thành 4 vùng (mỗi vùng 1 byte), có thể biểu thị dưới dạng thập phân, bát phân, thập lục phân hay nhị phân. Cách viết phổ biến nhất là dùng ký pháp thập phân có dấu chấm (dotted decimal notation) để tách các vùng. Mục đích của địa chỉ Ipv4 là để định danh duy nhất cho một máy tính bất kỳ trên liên mạng.

Do tổ chức và độ lớn của các mạng con (subnet) của liên mạng có thể khác nhau, người ta chia các địa chỉ Ipv4 thành 5 lớp, ký hiệu là A, B, C, D và E. Trong lớp A, B, C chứa địa chỉ có thể gán được. Lớp D dành riêng cho lớp kỹ thuật multicasting. Lớp E được dành những ứng dụng trong tương lai.

Netid trong địa chỉ mạng dùng để nhận dạng từng mạng riêng biệt. Các mạng liên kết phải có địa chỉ mạng (netid) riêng cho mỗi mạng. Ở đây các bit đầu tiên của byte đầu tiên được dùng để định danh lớp địa chỉ (0 - lớp A, 10 - lớp B, 110 - lớp C, 1110 - lớp D và 11110 - lớp E). Ở đây chúng ta xét cấu trúc của các lớp địa chỉ có thể gán được là lớp A, lớp B, lớp C

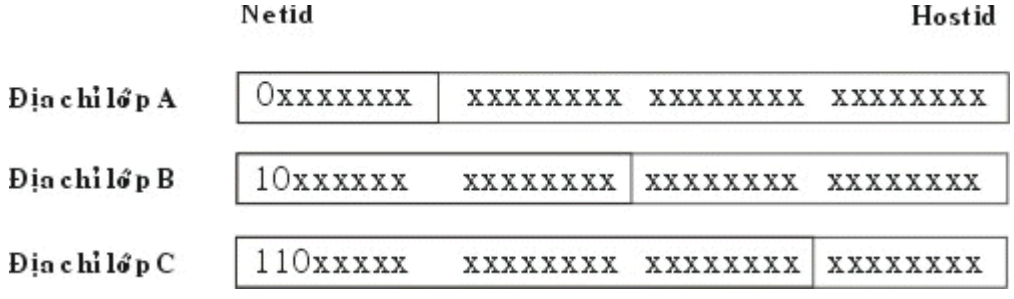
Cấu trúc của các địa chỉ Ipv4 như sau:

- Mạng lớp A: địa chỉ mạng (netid) là 1 Byte và địa chỉ host (hostid) là 3 byte.
- Mạng lớp B: địa chỉ mạng (netid) là 2 Byte và địa chỉ host (hostid) là 2 byte.
- Mạng lớp C: địa chỉ mạng (netid) là 3 Byte và địa chỉ host (hostid) là 1 byte.

Lớp A cho phép định danh tới 126 mạng, với tối đa 16 triệu host trên mỗi mạng. Lớp này được dùng cho các mạng có số trạm cực lớn.

Lớp B cho phép định danh tới 16384 mạng, với tối đa 65534 host trên mỗi mạng.

Lớp C cho phép định danh tới 2 triệu mạng, với tối đa 254 host trên mỗi mạng. Lớp này được dùng cho các mạng có ít trạm.



Hình 21- Cấu trúc các lớp địa chỉ Ipv4

2.3.2.1.2. Các loại địa chỉ Ipv4

- *Địa chỉ Unicast*

Khi bạn muốn gửi gói tin đến một máy tính cụ thể, khi đó địa chỉ để bạn gửi tới sẽ là một địa chỉ unicast. Đây đơn giản chỉ là địa chỉ IP của một thiết bị nào đó trong cùng hoặc mạng cục bộ khác.

- *Địa chỉ Multicast*

Trường hợp muốn gửi gói tin đến nhiều máy tính, ta không thể gửi lần lượt đến tất cả các máy được. Vì thế, địa chỉ bạn cần gửi tới trong trường hợp này sẽ là một địa chỉ Multicast, địa chỉ này đại diện cho một nhóm các thiết bị.

Địa chỉ multicast này chính là các địa chỉ trong dải địa chỉ lớp D.

- *Địa chỉ Broadcast*

Khi muốn gửi thông điệp đến tất cả các máy trong mạng nội bộ, đó là lúc ta cần sử dụng đến địa chỉ Broadcast. Địa chỉ Broadcast là địa chỉ có toàn bộ các bits phần host-id là 1. Khi gói tin được gửi đến địa chỉ Broadcast, thì nó sẽ được gửi tới tất cả các máy cùng mạng, tức là cùng phần net-id. Vì đại diện cho toàn bộ thiết bị trong mạng nên địa chỉ Broadcast không thể đặt được cho bất kỳ thiết bị nào.

Ví dụ: 192.168.1.255/24 là địa chỉ Broadcast của mạng 192.168.1.0/24.

- *Địa chỉ mạng*

Không chỉ các thiết bị mới có địa chỉ IP, mà các mạng thành phần của Internet hay mạng cục bộ cũng có một địa chỉ để xác định chính xác mạng đó. Khi tất cả các bits phần Host của một địa chỉ IP là 0, thì địa chỉ đó được gọi là địa chỉ mạng của mạng đó. Vì đại diện cho mạng nên địa chỉ mạng cũng không thể đặt được cho bất kỳ thiết bị nào.

Ví dụ: 192.168.1.0/24 là địa chỉ mạng của mạng 192.168.1.0/24.

- *Default Gateway*

Như một cổng thoát hiểm, khi gói tin cần gửi đến địa chỉ không cùng mạng hiện tại, hoặc đơn giản là không biết gửi đi đâu, thì gói tin đó sẽ được gửi tới địa chỉ Default gateway, thường là một interface của Router nối trực tiếp với mạng đó. Tại đây, Router sẽ dùng các chức năng định tuyến để chuyển tiếp gói tin đi các hướng khác nhau.

Default Gateway thường là địa chỉ IP có thể sử dụng đầu tiên của mạng đó.

Ví dụ: Default gateway của mạng 192.168.1.0/24 là 192.168.1.1/24.

- *Sự giới hạn của đia chỉ IP*

Số lượng địa chỉ IP là rất lớn, nhưng không phải là vô hạn. Vì vậy để bảo tồn địa chỉ IP, người ta chia địa chỉ IP ra làm 2 loại là địa chỉ public và địa chỉ private.

Địa chỉ public: Là các địa chỉ độc nhất, sử dụng được trong môi trường Internet.

Địa chỉ private: Chỉ sử dụng được trong mạng cục bộ, có thể tái sử dụng lại ở mạng cục bộ khác, nhưng trong một mạng thì vẫn phải mang giá trị duy nhất. Với mỗi phân lớp địa chỉ IP, thì có một dải địa chỉ dùng để làm địa chỉ private cho lớp đó:

- Lớp A: Từ 10.0.0.0 đến 10.255.255.255, subnet mask 255.0.0.0
- Lớp B: Từ 172.16.0.0 đến 172.31.255.255, subnet mask 255.240.0.0
- Lớp C: Từ 192.168.0.0 đến 192.168.255.255, subnet mask 255.255.0.0

Khi các thiết bị sử dụng địa chỉ IP private trong mạng cục bộ muốn truy cập được Internet – môi trường không sử dụng địa chỉ private, công nghệ NAT (Network Address Translation) được cài đặt trên các thiết bị router(đã được gán 1 địa chỉ IP Public) được sử dụng để chuyển IP private thành IP public và ngược lại, giúp cho các thiết bị trong mạng cục bộ vẫn có thể truy cập được Internet.

2.3.2.1.3. Ip tĩnh và IP động

Mỗi thiết bị trong một mạng IP được chỉ định bằng một địa chỉ vĩnh viễn (IP tĩnh) bởi nhà quản trị mạng hoặc một địa chỉ tạm thời, có thể thay đổi (IP động) thông qua công cụ DHCP (giao thức cấu hình host động sẽ tự động xác định địa chỉ IP tạm thời) ngay trên Windows Server.

Các router (bộ định tuyến), firewall (tường lửa) và máy chủ proxy dùng địa chỉ IP tĩnh còn máy khách có thể dùng IP tĩnh hoặc động.

Thường thì các nhà cung cấp Internet DSL hay cáp sẽ chỉ định loại IP động cho bạn. Trong các router và hệ điều hành, cấu hình mặc định cho các máy khách cũng là IP động. Loại địa chỉ này hay được dùng cho máy tính xách tay kết nối Wi-Fi, PC truy cập bằng Dial-up hay mạng riêng.

2.3.2.1.4. Mặt nạ mạng (Netmask)

Mặt nạ mạng chuẩn (Netmask) : Là địa chỉ IP mà giá trị của các bits ở phần nhận dạng mạng đều là 1, các bits ở phần nhận dạng máy tính đều là 0. Như vậy ta có 3 mặt nạ mạng tương ứng cho 3 lớp mạng A, B và C là :

- Mặt nạ mạng lớp A : 255.0.0.0
- Mặt nạ mạng lớp B : 255.255.0.0
- Mặt nạ mạng lớp C : 255.255.255.0

Với một địa chỉ IP và một Netmask cho trước, ta có thể dùng phép toán AND BIT để tính ra được địa chỉ mạng mà địa chỉ IP này thuộc về: Network Address = IP Address & Netmask.

2.3.2.1.5. Phân chia mạng con

- ***Sự cần thiết phải phân chia mạng con:***

Ta xét thí dụ một công ty được cấp một địa chỉ lớp B, tức có thể có tới tối đa 65.000 thiết bị. Tuy nhiên, các kiến trúc mạng hiện nay đều có giới hạn vật lý về số máy có thể kết nối tới, thường nhỏ hơn số địa chỉ có thể có trong một mạng lớp B rất nhiều. Hơn nữa, việc quản trị trên một mạng có quá nhiều thiết bị cũng là một khó khăn lớn. Để khắc phục những vấn đề này thì giải pháp dễ dàng nhất là phân chia mạng thành nhiều mạng nhỏ hơn. Như vậy, nhìn từ ngoài vào, địa chỉ mạng lớp B này sẽ xác định một mạng riêng trong mạng toàn cầu nhưng trên góc độ bên trong công ty, mạng lớp B này lại được phân chia tiếp thành các mạng con và mỗi mạng con này có một địa chỉ riêng. Với sự phân chia như vậy, số máy tính trên toàn mạng LAN có thể lên tới số tối đa mà địa chỉ lớp B có thể hỗ trợ.

- ***Lợi ích của phân chia mạng con:***

Phân chia thành mạng con còn có những lợi ích dưới đây:

- Giảm nghẽn mạng bằng cách tái định hướng các giao vận và giới hạn phạm vi của các thông điệp quảng bá.
- Giới hạn trong phạm vi từng mạng con các trục trặc có thể xảy ra (không ảnh hưởng tới toàn mạng LAN)
- Giảm % thời gian sử dụng CPU do giảm lưu lượng của các giao vận quảng bá
- Tăng cường bảo mật (các chính sách bảo mật có thể áp dụng cho từng mạng con)
- Cho phép áp dụng các cấu hình khác nhau trên từng mạng con

- **Cách phân chia mạng con:**

Để tạo ra một mạng con người quản trị mạng sẽ tiến hành mượn các bit cao nhất trong phần bit dành cho Host ID và gán chúng như là Subnet ID (như hình)

Hình 22– Phân chia mạng con

Chú ý: Số bit mượn từ host id ban đầu để chia mạng con cần thỏa mãn: subnetid ≤ hostid – 2.

- **Mặt nạ mạng con (subnet mask)**

Mặt nạ mạng con là một địa chỉ IP mà giá trị các bit ở phần nhận dạng mạng (Network Id) và Phần nhận dạng mạng con (Subnet Id) đều là 1, phần nhận dạng máy tính (Host Id) đều là 0. Ví dụ một Subnet mask tùy biến của lớp A với 4 bit được mượn từ phần địa chỉ cho Host ID có giá trị như sau: 11111111.11110000.00000000.00000000 hay đổi sang hệ 10 là: 255.240.0.0

Khi có được mặt nạ mạng con, ta có thể xác định địa chỉ mạng con (Subnetwork Address) mà một địa chỉ IP được tính bằng công thức sau :

Subnetwork Address = IP & Subnetmask

- **Ví dụ phân chia mạng con:**

Cho địa chỉ IP 172.16.115.100/28. Hãy cho biết (giải thích):

1. Địa chỉ host này thuộc lớp địa chỉ nào?Mạng chứa host đó có chia mạng con hay không? Nếu có thì cho biết có bao nhiêu mạng con và có bao nhiêu host trong mỗi mạng con?
2. Host nằm trong mạng có địa chỉ là gì? Địa chỉ broadcast dung cho mạng đó?
3. Liệt kê danh sách các địa chỉ host nằm chung mạng con với host trên.

Để giải quyết bài toán trên chúng ta làm như sau:

Địa chỉ IP: 172.16.115.100

Dạng nhị phân: 10101100 00010000 01110011 01100100

1. Địa chỉ IP có byte đầu tiên dạng nhị phân là 10101100 thuộc lớp B. Vậy địa chỉ host thuộc lớp B

Lớp B có: network_id: 8bit x 2byte = 16bit

Host_id: 8bit x 2byte = 16 bit

Địa chỉ IP: 172.16.115.100/28 ở đây 28 bit cho phần network_id, $16 \neq 28$ nên mạng chia được mạng con.

Mượn: 28-16=12 bit của phần host_id để chia mạng con.

Số mạng con: 2^{12}-2=65534 mạng con.

Host_id còn: 16-12=4 bit

Số host trong mạng con: 2^4-2=14 host

2. Network mask mặc định của lớp B: 255.255.0.0

Quy định mặt nạ mạng con (subnet mask) là tất cả các bit phần host_id =0, network_id=1.

Ta có subnet mask mới: 11111111 11111111 11111111 11110000

Dạng thập phân : 255 255 255 240

Thực hiện phép toán AND giữa IP và subnet mask

IP : 10101100 00010000 01110011 01100100

Subnet mask : 11111111 11111111 11111111 11110000

Kết quả : 10101100 00010000 01110011 01100000

Dạng thập phân: 172 16 115 96

Địa chỉ mạng : 172.16.115.96

Quy định địa chỉ broadcast, tất cả các bit phần host_id của địa chỉ mạng.

3. Ta có địa chỉ mạng: 172.16.115.96

Dạng nhị phân: 10101100 00010000 01110011 01100000

Dặt tất cả các bit phần host_id =1. Ta có:

10101100 00010000 01110011 01101111

Dạng thập phân: 172 16 115 111

Địa chỉ broadcast của mạng con: 172.16.115.111

Địa chỉ đầu tiên là:

Địa chỉ mạng:172.16.115.96

Thêm 1 vào octet cuối cùng : 172.16.115.97

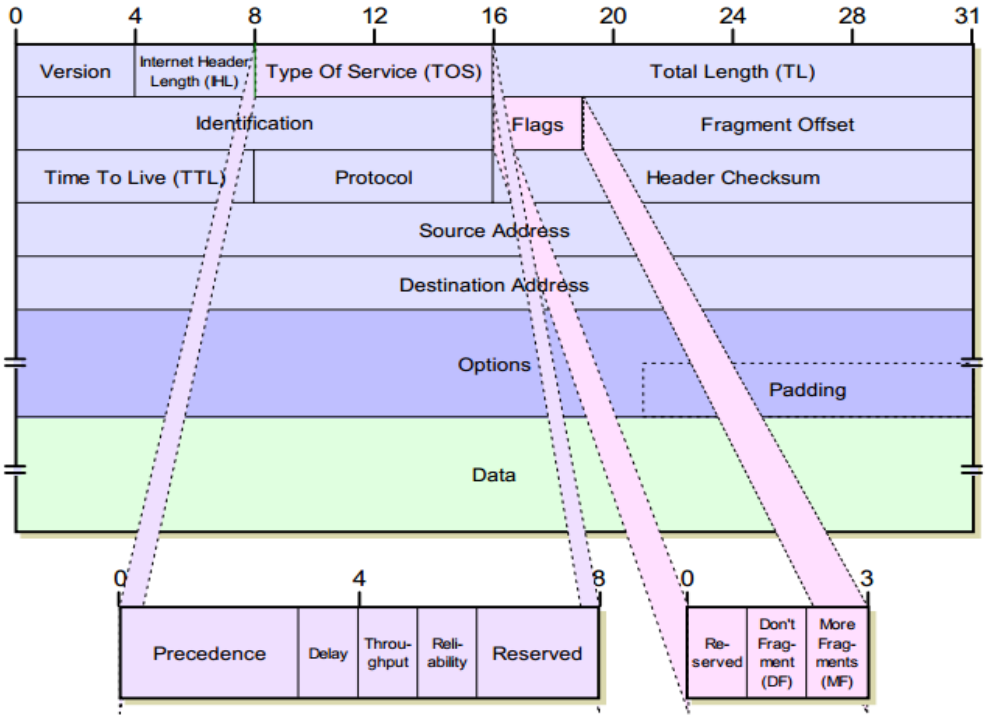
Địa chỉ cuối cùng là:

Địa chỉ broadcast: 172.16.115.111

Bớt 1 ở octet cuối cùng: 172.16.115.110

2.3.2.2. Giao thức IP

Giao thức liên mạng IP là một trong những giao thức quan trọng nhất của bộ giao thức TCP/IP. Mục đích của giao thức liên mạng IP là cung cấp khả năng kết nối các mạng con thành liên mạng để truyền dữ liệu. IP là giao thức cung cấp dịch vụ phân phát datagram theo kiểu không liên kết và không tin cậy nghĩa là không cần có giai đoạn thiết lập liên kết trước khi truyền dữ liệu, không đảm bảo rằng IP datagram sẽ tới đích và không duy trì bất kỳ thông tin nào về những datagram đã gửi đi.



Hình 23 – Cấu trúc gói tin Ipv4

IP Header bao gồm nhiều thông tin thích hợp gồm Số phiên bản, mà, trong phạm vi này là 4. Các thông tin chi tiết khác như sau:

- **Phiên bản (Version):** Phiên bản số bao nhiêu của IP được sử dụng (ví dụ IPv4).
- **IHL:** Độ dài internet Header (Internet Header Length).
- **Type of service** (8 bits): đặc tả các tham số về dịch vụ nhằm thông báo cho mạng biết dịch vụ nào mà gói tin muốn được sử dụng, chẳng hạn ưu tiên, thời hạn chậm trễ, năng suất truyền và độ tin cậy. Hình sau cho biết ý nghĩ của trường 8 bits này.

0	1	2	3	4	5	6	7
Precedence			D	T	R	Reserved	

Precedence (3 bit): chỉ thị về quyền ưu tiên gửi datagram, nó có giá trị từ 0 (gói tin bình thường) đến 7 (gói tin kiểm soát mạng).

D (Delay) (1 bit): chỉ độ trễ yêu cầu trong đó: D = 0 gói tin có độ trễ bình thường, D = 1 gói tin độ trễ thấp.

T (Throughput) (1 bit): chỉ độ thông lượng yêu cầu sử dụng để truyền gói tin với lựa chọn truyền trên đường thông suất thấp hay đường thông suất cao. T = 0 thông lượng bình thường và T = 1 thông lượng cao.

R (Reliability) (1 bit): chỉ độ tin cậy yêu cầu. Nếu R = 0 thì độ tin cậy bình thường, ngược lại R = 1 thì độ tin cậy cao.

- **Total Length:** Độ dài của toàn bộ gói IP (bao gồm cả IP Header và IP Payload).
- **Identification:** Nếu gói IP bị phân mảnh trong suốt quá trình truyền tải, tất cả các mảnh chứa cùng một số xác nhận, để xác nhận gói IP ban đầu chúng sở hữu.
- **Flags:** Là các cờ hiệu. Khi được yêu cầu bởi các nguồn mạng, nếu Gói IP là quá lớn để kiểm soát, những "cờ hiệu" này chỉ rằng nếu chúng có thể được phân mảnh hoặc không. Trong cờ hiệu 3 bit này, MSB thường được thiết lập là 0.
- **Fragment Offset:** Offset này chỉ vị trí chính xác của mảnh trong Gói IP ban đầu.
- **Thời gian sống (Time to Live):** Để tránh các vòng lặp trong mạng, mọi gói được gửi với một số thiết lập giá trị TTL, mà chỉ cho mạng biết bao nhiêu router (hop) mà gói này có thể qua. Tại mỗi hop, giá trị của nó được giảm đi 1 và khi giá trị tiến tới 0, gói này bị loại bỏ.
- **Protocol:** Chỉ cho Tầng mạng tại host đích đến, tới Giao thức mà gói này sở hữu, ví dụ: Giao thức ở trên. Ví dụ: số hiệu giao thức của ICMP là 1, TCP là 6 và UDP là 17.
- **Header Checksum:** Trường này được sử dụng để giữ việc tổng kiểm tra giá trị của cả Header mà sau đó được sử dụng để kiểm tra nếu gói được nhận là lỗi.
- **Source Address:** Địa chỉ nguồn 32 bit của trạm gửi (hoặc nguồn) của gói.
- **Destination Address:** Địa chỉ 32 bit của trạm nhận (hoặc đích đến) của gói.
- **Options:** Trường tùy ý này, mà được sử dụng nếu giá trị của IHL là lớn hơn 5. Những tùy chọn này có thể chứa các giá trị của tùy chọn như Sự bảo mật (Security), Trình ghi tuyến (Record Route), Nhãn thời gian (Time Stamp), ….
- *Data (độ dài thay đổi)*: Trên một mạng cục bộ như vậy, hai trạm chỉ có thể liên lạc với nhau nếu chúng biết địa chỉ vật lý của nhau. Như vậy vấn đề đặt ra là phải thực hiện ánh xạ giữa địa chỉ IP (32 bits) và địa chỉ vật lý (48 bits) của một trạm.

- **Các giao thức trong mạng IP**

Để mạng với giao thức IP hoạt động được tốt người ta cần một số giao thức bổ sung, các giao thức này đều không phải là bộ phận của giao thức IP và giao thức IP sẽ dùng đến chúng khi cần.

- *Giao thức ARP (Address Resolution Protocol):* Ở đây cần lưu ý rằng các địa chỉ IP được dùng để định danh các host và mạng ở tầng mạng của mô hình OSI, và chúng không phải là các địa chỉ vật lý (hay địa chỉ MAC) của các trạm trên đó một mạng cục bộ (Ethernet, Token Ring.). Trên một mạng cục bộ hai trạm chỉ có thể liên lạc với nhau nếu chúng biết địa chỉ vật lý của nhau. Như vậy vấn đề đặt ra là phải tìm được ánh xạ giữa địa chỉ IP (32 bits) và địa chỉ vật lý của một trạm. *Giao thức ARP* đã được xây dựng để tìm địa chỉ vật lý từ địa chỉ IP khi cần thiết.
- *Giao thức RARP (Reverse Address Resolution Protocol)*: Là giao thức ngược với *giao thức ARP*. Giao thức RARP được dùng để tìm địa chỉ IP từ địa chỉ vật lý.
- *Giao thức ICMP (Internet Control Message Protocol):* Giao thức này thực hiện truyền các thông báo điều khiển (báo cáo về các tình trạng các lỗi trên mạng.) giữa các gateway hoặc một nút của liên mạng. Tình trạng lỗi có thể là: một gói tin IP không thể tới đích của nó, hoặc một router không đủ bộ nhớ đệm để lưu và chuyển một gói tin IP, Một thông báo ICMP được tạo và chuyển cho IP. IP sẽ "bọc" (encapsulate) thông báo đó với một IP header và truyền đến cho router hoặc trạm đích.

- **Các bước hoạt động của giao thức IP**

Khi giao thức IP được khởi động nó trở thành một thực thể tồn tại trong máy tính và bắt đầu thực hiện những chức năng của mình, lúc đó thực thể IP là cấu thành của tầng mạng, nhận yêu cầu từ các tầng trên nó và gửi yêu cầu xuống các tầng dưới nó.

Đối với thực thể IP ở máy nguồn, khi nhận được một yêu cầu gửi từ tầng trên, nó thực hiện các bước sau đây:

- Tạo một IP datagram dựa trên tham số nhận được.
- Tính checksum và ghép vào header của gói tin.
- Ra quyết định chọn đường: hoặc là trạm đích nằm trên cùng mạng hoặc một gateway sẽ được chọn cho chặng tiếp theo.
- Chuyển gói tin xuống tầng dưới để truyền qua mạng.

Đối với router, khi nhận được một gói tin đi qua, nó thực hiện các động tác sau:

- Tính chesksum, nếu sai thì loại bỏ gói tin.
- Giảm giá trị tham số Time - to Live. nếu thời gian đã hết thì loại bỏ gói tin.
- Ra quyết định chọn đường.
- Phân đoạn gói tin, nếu cần.

- Kiến tạo lại IP header, bao gồm giá trị mới của các vùng Time - to -Live, Fragmentation và Checksum.
- Chuyển datagram xuống tầng dưới để chuyển qua mạng.

Cuối cùng khi một datagram nhận bởi một thực thể IP ở trạm đích, nó sẽ thực hiện bởi các công việc sau:

- Tính checksum. Nếu sai thì loại bỏ gói tin.
- Tập hợp các đoạn của gói tin (nếu có phân đoạn)
- Chuyển dữ liệu và các tham số điều khiển lên tầng trên.

2.3.3 Giao thức điều khiển truyền dữ liệu TCP (Transmission Control Protocol)

2.3.3.1. Khái niệm

TCP là một giao thức "có liên kết" (connection - oriented), nghĩa là cần phải thiết lập liên kết giữa hai thực thể TCP trước khi chúng trao đổi dữ liệu với nhau. Một tiến trình ứng dụng trong một máy tính truy nhập vào các dịch vụ của giao thức TCP thông qua một cổng (port) của TCP. Số hiệu cổng TCP được thể hiện bởi 2 bytes.

Một cổng TCP kết hợp với địa chỉ IP tạo thành một đầu nối TCP/IP (socket) duy nhất trong liên mạng. Dịch vụ TCP được cung cấp nhờ một liên kết logic giữa một cặp đầu nối TCP/IP. Một đầu nối TCP/IP có thể tham gia nhiều liên kết với các đầu nối TCP/IP ở xa khác nhau. Trước khi truyền dữ liệu giữa 2 trạm cần phải thiết lập một liên kết TCP giữa chúng và khi không còn nhu cầu truyền dữ liệu thì liên kết đó sẽ được giải phóng.

Các thực thể của tầng trên sử dụng giao thức TCP thông qua các hàm gọi (function calls) trong đó có các hàm yêu cầu để yêu cầu, để trả lời. Trong mỗi hàm còn có các tham số dành cho việc trao đổi dữ liệu.

Các bước thực hiện để thiết lập một liên kết TCP/IP: Thiết lập một liên kết mới có thể được mở theo một trong 2 phương thức: chủ động (active) hoặc bị động (passive).

- Phương thức bị động, người sử dụng yêu cầu TCP chờ đợi một yêu cầu liên kết gửi đến từ xa thông qua một đầu nối TCP/IP (tại chỗ). Người sử dụng dùng hàm passive Open có khai báo cổng TCP và các thông số khác (mức ưu tiên, mức an toàn)
- Với phương thức chủ động, người sử dụng yêu cầu TCP mở một liên kết với một một đầu nối TCP/IP ở xa. Liên kết sẽ được xác lập nếu có một hàm Passive Open tương ứng đã được thực hiện tại đầu nối TCP/IP ở xa đó.

Số hiệu cổng	**Mô tả**
0	Reserved
5	Remote job entry
7	Echo
9	Discard
11	Systat
13	Daytime
15	Nestat
17	Quotd (quote odd day
20	ftp-data
21	ftp (control)
23	Telnet
25	SMTP
37	Time
53	Name Server
102	ISO – TSAP
103	X.400
104	X.400 Sending
111	Sun RPC
139	Net BIOS Session source
160 - 223	Reserved

Bảng 1 - Các cổng TCP phổ biến.

Khi người sử dụng gửi đi một yêu cầu mở liên kết sẽ được nhận hai thông số trả lời từ TCP.

- Thông số Open ID được TCP trả lời ngay lập tức để gán cho một liên kết cục bộ (local connection name) cho liên kết được yêu cầu. Thông số này về sau được dùng để tham chiếu tới liên kết đó. (Trong trường hợp nếu TCP không thể thiết lập được liên kết yêu cầu thì nó phải gửi tham số Open Failure để thông báo.)
- Khi TCP thiết lập được liên kết yêu cầu nó gửi tham số Open Sucsess được dùng để thông báo liên kết đã được thiết lập thành công. Thông báo này dược chuyển đến trong cả hai trường hợp bị động và chủ động. Sau khi một liên kết được mở, việc truyền dữ liệu trên liên kết có thể được thực hiện.

Các bước thực hiện khi truyền và nhận dữ liệu: Sau khi xác lập được liên kết người sữ dụng gửi và nhận dữ liệu. Việc gửi và nhận dữ liệu thông qua các hàm Send và receive.

- *Hàm Send:* Dữ liệu được gửi xuống TCP theo các khối (block). Khi nhận được một khối dữ liệu, TCP sẽ lưu trữ trong bộ đệm (buffer). Nếu cờ PUSH được dựng thì toàn bộ dữ liệu trong bộ đệm được gửi, kể cả khối dữ liệu mới đến sẽ được gửi đi. Ngược lại cờ PUSH không được dựng thì dữ liệu được giữ lại trong bộ đệm và sẽ gửi đi khi có cơ hội thích hợp (chẳng hạn chờ thêm dữ liệu nữa để gữi đi với hiệu quả hơn).
- *Hàm reveive*: Ở trạm đích dữ liệu sẽ được TCP lưu trong bộ đệm gắn với mỗi liên kết. Nếu dữ liệu được đánh dấu với một cờ PUSH thì toàn bộ dữ liệu trong bộ đệm (kể cả các dữ liệu được lưu từ trước) sẽ được chuyển lên cho người sữ dụng. Còn nếu dữ liệu đến không được đánh dấu với cờ PUSH thì TCP chờ tới khi thích hợp mới chuyển dữ liệu với mục tiêu tăng hiệu quả hệ thống.
- Nói chung việc nhận và giao dữ liệu cho người sử dụng đích của TCP phụ thuộc vào việc cài đặt cụ thể. Trường hợp cần chuyển gấp dữ liệu cho người sử dụng thì có thể dùng cờ URGENT và đánh dấu dữ liệu bằng bit URG để báo cho người sử dụng cần phải sử lý khẩn cấp dữ liệu đó.

Các bước thực hiện khi đóng một liên kết: Việc đóng một liên kết khi không cần thiết được thực hiên theo một trong hai cách: *dùng hàm Close* hoặc *dùng hàm Abort*.

- *Hàm Close*: yêu cầu đóng liên kết một cách bình thường. Có nghĩa là việc truyền dữ liệu trên liên kết đó đã hoàn tất. Khi nhận được một *hàm Close* TCP sẽ truyền đi tất cả dữ liệu còn trong bộ đệm thông báo rằng nó đóng liên kết. Lưu ý rằng khi một người sử dụng đã gửi đi một *hàm Close* thì nó vẫn phải tiếp tục nhận dữ liệu đến trên liên kết

đó cho đến khi TCP đã báo cho phía bên kia biết về việc đóng liên kết và chuyển giao hết tất cả dữ liệu cho người sử dụng của mình.

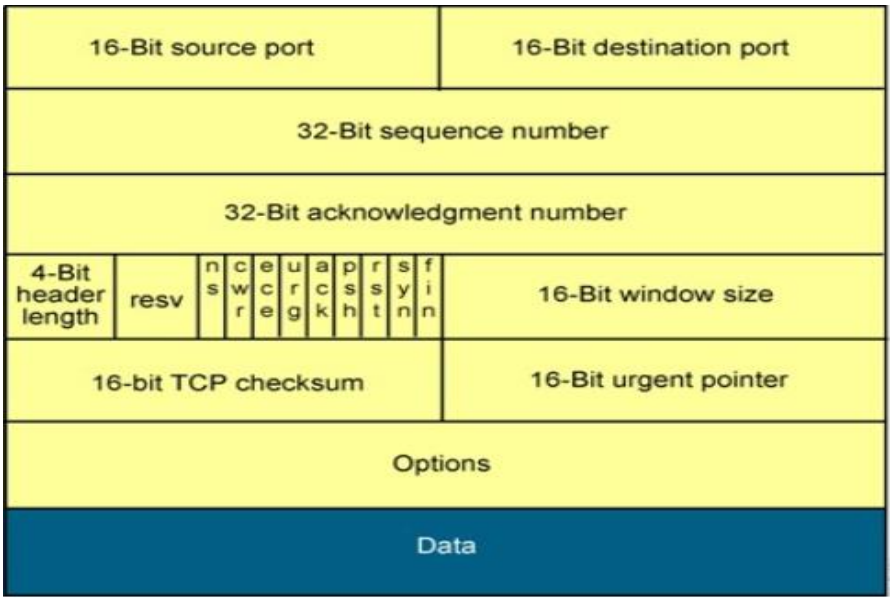
- *Hàm Abort*: Người sử dụng có thể đóng một liên kết bất và sẽ không chấp nhận dữ liệu qua liên kết đó nữa. Do vậy dữ liệu có thể bị mất đi khi đang được truyền đi. TCP báo cho TCP ở xa biết rằng liên kết đã được hủy bỏ và TCP ở xa sẽ thông báo cho người sử dụng cũa mình.

Một số hàm khác của TCP:

- *Hàm Status*: cho phép người sử dụng yêu cầu cho biết trạng thái của một liên kết cụ thể, khi đó TCP cung cấp thông tin cho người sử dụng.
- *Hàm Error*: thông báo cho người sử dụng TCP về các yêu cầu dịch vụ bất hợp lệ liên quan đến một liên kết có tên cho trước hoặc về các lỗi liên quan đến môi trường.

2.3.3.2. Định dạng dữ liệu của TCP

Đơn vị dữ liệu sử dụng trong TCP được gọi là segment (đoạn dữ liệu), có các tham số với ý nghĩa như sau:



Hình 24- Dạng thức của segment TCP

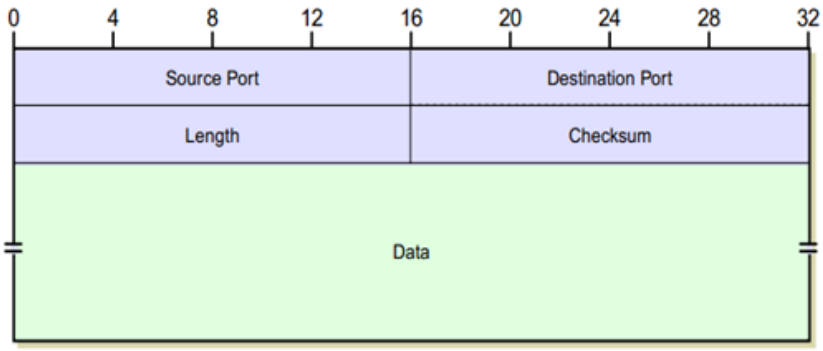
- Source Por (16 bits): Số hiệu cổng TCP của trạm nguồn.
- Destination Port (16 bit): Số hiệu cổng TCP của trạm đích.
- Sequence Number (32 bit): số hiệu của byte đầu tiên của segment trừ khi bit SYN được thiết lập. Nếy bit SYN được thiết lập thì Sequence Number là số hiệu tuần tự khởi đầu (ISN) và byte dữ liệu đầu tiên là ISN+1.

- Acknowledgment Number (32 bit): số hiệu của segment tiếp theo mà trạm nguồn đang chờ để nhận. Ngầm ý báo nhận tốt (các) segment mà trạm đích đã gửi cho trạm nguồn.
- Data offset (4 bit): số lượng bội của 32 bit (32 bit words) trong TCP header (tham số này chỉ ra vị trí bắt đầu của nguồn dữ liệu).
- Reserved (6 bit): dành để dùng trong tương lai
- Control bit (các bit điều khiển):
- URG: Vùng con trỏ khẩn (Ucgent Poiter) có hiệu lực.
- ACK: Vùng báo nhận (ACK number) có hiệu lực.
- PSH: Chức năng PUSH.
- RST: Khởi động lại (reset) liên kết.
- SYN: Đồng bộ hóa số hiệu tuần tự (sequence number).
- FIN: Không còn dữ liệu từ trạm nguồn.
- Window (16 bit): cấp phát credit để kiểm soát nguồn dữ liệu (cơ chế cửa sổ). Đây chính là số lượng các byte dữ liệu, bắt đầu từ byte được chỉ ra trong vùng ACK number, mà trạm nguồn đã sẵn sàng để nhận.
- Checksum (16 bit): mã kiểm soát lỗi cho toàn bộ segment (header + data)
- Urgemt Poiter (16 bit): con trỏ này trỏ tới số hiệu tuần tự của byte đi theo sau dữ liệu khẩn. Vùng này chỉ có hiệu lực khi bit URG được thiết lập.
- Options (độ dài thay đổi): khai báo các option của TCP, trong đó có độ dài tối đa của vùng TCP data trong một segment.
- Paddinh (độ dài thay đổi): phần chèn thêm vào header để đảm bảo phần header luôn kết thúc ở một mốc 32 bit. Phần thêm này gồm toàn số 0.
- TCP data (độ dài thay đổi): chứa dữ liệu của tầng trên, có độ dài tối đa ngầm định là 536 byte. Giá trị này có thể điều chỉnh bằng cách khai báo trong vùng options.

2.3.4 Giao thức UDP (User Datagram Protocol)

UDP (User Datagram Protocol) là giao thức theo phương thức không liên kết được sử dụng thay thế cho TCP ở trên IP theo yêu cầu của từng ứng dụng. Khác với TCP, UDP không có các chức năng thiết lập và kết thúc liên kết. Tương tự như IP, nó cũng không cung cấp cơ chế báo nhận (acknowledgment), không sắp xếp tuần tự các gói tin (datagram) đến và có thể dẫn đến tình trạng mất hoặc trùng dữ liệu mà không có cơ chế thông báo lỗi cho người gửi. Qua đó ta thấy UDP cung cấp các dịch vụ vận chuyển không tin cậy như trong TCP.

Khuôn dạng UDP datagram được mô tả với các vùng tham số đơn giản hơn nhiều so với TCP segment.



Hình 24 - Dạng thức của gói tin UDP

UDP cũng cung cấp cơ chế gán và quản lý các số hiệu cổng (port number) để định danh duy nhất cho các ứng dụng chạy trên một trạm của mạng. Do ít chức năng phức tạp nên UDP thường có xu thế hoạt động nhanh hơn so với TCP. Nó thường được dùng cho các ứng không đòi hỏi độ tin cậy cao trong giao vận.

BÀI TẬP CHƯƠNG II

Bài 1: Một hệ thống mạng có địa chỉ IP được thiết lập ở lớp 192.168.17.1/24. Hãy chia hệ thống mạng này thành ba mạng con Net 1: có 20 Host, Net 2: có 25 Host, Net 3: có 68 Host. Mỗi mạng con hãy liệt kê địa chỉ *đầu* và *cuối của mỗi mạng*?

Bài 2: Cho địa chỉ IP : 192.168.5.39/27

a. Địa chỉ host này thuộc lớp địa chỉ nào ?

b. Mạng chứa host đó có chia mạng con hay không ? Nếu có thì cho biết có bao nhiêu mạng con và có bao nhiêu host trong mỗi mạng con ?

c. Host nằm trong mạng có địa chỉ là gì ?

d. Địa chỉ broadcast dùng cho mạng con đó ?

e. Liệt kê danh sách các địa chỉ host nằm chung mạng con với host trên ?

Bài 3: Một công ty nhỏ có một địa chỉ mạng thuộc class C network,. người ta cần tạo 5 mạng con, mỗi mạng con có ít nhất 20 host. Vậy subnet nào dưới đây được sử dụng cho yêu cầu trên?

a. 255.255.255.0 b. 255.255.255.192

c. 255.255.255.224 d. 255.255.255.240

Bài 4: Một cong ty XYZ sử dụng địa chỉ mạng 192.168.4.0 và sử dụng subnet mask là

255.255.255.224 để tạo mạng con. Vậy số mạng con và số địa chỉ IP host trên mỗi mạng con là bao nhiêu.

Bài 5: Một công ty A thuê địa chỉ IP: 193.87.98.13/24. Công ty cần chia làm 3 mạng con như sau: mạng 1 có 15 máy, mạng 2 có 30 máy và mạng 3 có 55 máy. Hãy nêu địa chỉ cho từng mạng và mặt nạ mạng của từng máy trong mạng của công ty.

Bài 6: Cho địa chỉ IP của một host

172.29.32.30/255.255.240.0 hoặc 172.29.32.30/20

Hãy cho biết:

a. Mạng chứa host đó có chia mạng con hay không?
b. Nếu có thì có bao nhiêu mạng con
c. Và bao nhiêu host trong mỗi mạng con?
d. Địa chỉ broadcast dùng cho mạng đó?
e. Liệt kê danh sách các địa chỉ host nằm chung mạng con với host trên

Bài 7: Một mạng lớp C cần chia thành 5 mạng con, sử dụng Subnet Mask nào sau đây:

a. 255.255.224.0 b. 255.0.0.224

c. 255.224.255.0 d. 255.255.255.224

Bài 8: Địa chỉ nào sau đây là địa chỉ mạng con của host 172.16.25.14/30

a. 172.16.25.4 b. 172.16.25.12

c. 172.16.25.8 d. 172.16.25.16

Bài 9: Địa chỉ nào sau đây là địa chỉ quảng bá của mạng 192.168.25.128/27

a. 192.168.25.255 b. 192.168.25.128

c. 192.168.25.159 d. 192.168.25.100

Bài 10: Một mạng con lớp A mượn 19 bit để chia Subnet thì Subnet Mask sẽ là:

a. 255.255.248.0 b. 255.255.255.1

c. 255.255.255.224 d. 255.248.0.0

CHƯƠNG III – MẠNG CỤC BỘ

Mục tiêu

Nội dung của chương sẽ trình bày các khái niệm cơ bản về kỹ thuật mạng cục bộ, các hình trạng mạng cục bộ cùng với ưu nhược điểm của từng loại cấu trúc, các phương pháp truy nhập ngẫu nhiên và có điều khiển được sử dụng trong các mạng quảng bá. Nội dung của chương bao gồm các phần:

a. Khái niệm chung về mạng cục bộ

b. Kỹ thuật mạng cục bộ

c. Các phương pháp truy cập đường truyền vật lý

d. Mạng cục bộ không dây.

e. Thiết kế mạng cục bộ.

3.1 KHÁI NIỆM MẠNG CỤC BỘ

Trong những năm 80 vừa qua, mạng cục bộ LAN đã phát triển một cách nhanh chóng. Khi trong một tổ chức nào đó (cơ quan, nhà máy, trường đại học…) có nhiều hệ thống nhỏ đó được sử dụng thì nảy sinh nhu cầu kết nối chúng lại với nhau

Tên gọi "Mạng cục bộ" được xem xét từ quy mô của mạng hay khoảng cách địa lý. Tuy nhiên, đó không phải là đặc tính duy nhất của mạng cục bộ, nhưng trên thực tế quy mô của mạng quyết định nhiều đặc tính và công nghệ của mạng.

Vậy **Mạng cục bộ (Local Area Networks - LAN)** là mạng được thiết lập để liên kết các máy tính trong một phạm vi tương đối nhỏ (như trong một toà nhà, một khu nhà, trường học ...) với khoảng cách lớn nhất giữa các máy tính nút mạng chỉ trong vòng vài chục km trở lại.

Đề phân biệt mạng LAN với các loại mạng khác người ta dựa trên một số đặc trưng sau:

- *Đặc trưng địa lý:* mạng cục bộ thường được cài đặt trong phạm vi nhỏ (toà nhà, một căn cứ quân sự ...) có đường kính từ vài chục mét đến vài chục km trong điều kiện công nghệ hiện nay.
- *Đặc trưng về tốc độ truyền:* mạng cục bộ có tốc độ truyền cao hơn so với mạng diện rộng, khoảng 100 Mb/s và tới nay tốc độ này có thể đạt tới 1Gb/s với công nghệ hiện nay.
- *Đặc trưng độ tin cậy:* tỷ suất lỗi thấp hơn so với mạng diện rộng (như mạng điện thoại chẳng hạn), có thể đạt từ 10^{-8} đến 10^{-11}.

- *Đặc trưng quản lý: mạng cục bộ thường là sở hữu riêng của một tổ chức nào đó (như* trường học, doanh nghiệp ...) do vậy việc quản lý khai thác mạng hoàn toàn tập trung và thống nhất.

Tuy nhiên, với sự phát triển nhanh chóng của công nghệ mạng hiện nay các đặc trưng nói trên chỉ mang tính tương đối. Sự phân biệt giữa mạng cục bộ và mạng diện rộng sẽ ngày càng "mờ" đi.

3.2 KỸ THUẬT MẠNG CỤC BỘ

3.2.1 Hình trạng mạng (Topology)

Hình trạng của mạng cục bộ thể hiện qua cấu trúc hay hình dáng hình học cuả các đường dây cáp mạng dùng để liên kết các máy tính thuộc mạng với nhau. Các mạng cục bộ thường hoạt động dựa trên cấu trúc đã định sẵn liên kết các máy tính và các thiết bị có liên quan.

Về nguyên tắc mọi topology của mạng máy tính nói chung đều có thể dùng cho mạng cục bộ. Song do đặc thù của mạng cục bộ nên chỉ có 3 topology thường được sử dụng: *hình sao* (star), *hình vòng* (ring), *tuyến tính* (bus)

3.2.1.1. Mạng hình sao (star)

Ở dạng hình sao, tất cả các trạm được nối vào một thiết bị trung tâm có nhiệm vụ nhận tín hiệu từ các trạm và chuyển tín hiệu đến trạm đích với phương thức kết nối là phương thức điểm-điểm (point - to - point). Thiết bị trung tâm hoạt động giống như một tổng đài cho phép thực hiện việc nhận và truyền dữ liệu từ trạm này tới các trạm khác.

Hình 26– Mạng hình sao

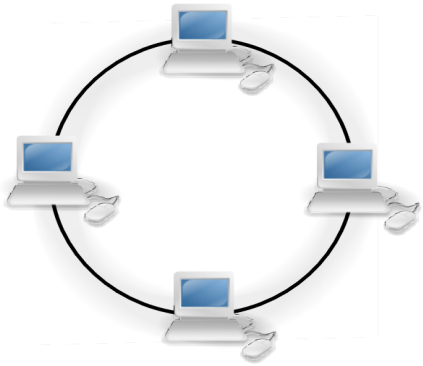
Tùy theo yêu cầu truyền thông trong mạng , thiết bị trung tâm có thể là một bộ chuyển mạch (switch), một bộ chọn đường (router) hoặc đơn giản là một bộ phân kênh (Hub). Có nhiều cổng ra và mỗi cổng nối với một máy. Theo chuẩn IEEE 802.3 mô hình dạng Star thường dùng:

- *10BASE-T*: dùng cáp UTP (Unshield Twisted Pair_ cáp không bọc kim), tốc độ 10 Mb/s, khoảng cách từ thiết bị trung tâm tới trạm tối đa là 100m.
- *100BASE-T* tương tự như 10BASE-T nhưng tốc độ cao hơn 100 Mb/s.

Ưu và nhược điểm của mạng hình sao:

- *Ưu điểm:* Với dạng kết nối này có ưu điểm là không đụng độ hay ách tắc trên đường truyền, tận dụng được tốc độ tối đa đường truyền vật lý, lắp đặt đơn giản, dễ dàng cấu hình lại mạng (thêm, bớt trạm). Nếu có trục trặc trên một trạm thì cũng không gây ảnh hưởng đến toàn mạng qua đó dễ dàng kiểm soát và khắc phục sự cố.
- *Nhược điểm:* Độ dài đường truyền nối một trạm với thiết bị trung tâm bị hạn chế (trong vòng 100 m với công nghệ hiện nay) tốn đường dây cáp nhiều.

3.2.1.2.Mạng hình vòng (ring)



Hình 27– mạng vòng

Tín hiệu được lưu chuyển theo một chiều duy nhất. Các máy tính được liên kết với nhau thành một vòng tròn theo phương thức điểm-điểm (point - to - point), qua đó mỗi một trạm có thể nhận và truyền dữ liệu theo vòng một chiều và dữ liệu được truyền theo từng gói một. Mỗi trạm của mạng được nối với vòng qua một bộ chuyển tiếp (Repeater) có nhiệm vụ nhận tín hiệu rồi chuyển tiếp đến trạm kế tiếp trên vòng. Như vậy tín hiệu được lưu chuyển trên vòng theo một chuỗi các liên kết điểm - điểm giữa các Repeater do đó cần có giao thức điều khiển việc cấp phát quyền được truyền dữ liệu trên vòng cho các trạm có nhu cầu.

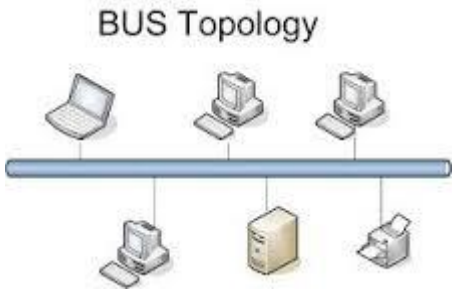
Mỗi gói dữ liệu đều có mang địa chỉ trạm đích, mỗi trạm khi nhận được một gói dữ liệu nó kiểm tra nếu đúng với địa chỉ của mình thì nó nhận lấy còn nếu không phải thì nó sẽ phát lại cho trạm kế tiếp, cứ như vậy gói dữ liệu đi được đến đích.

Để tăng độ tin cậy của mạng, phải lắp vòng dự phòng, khi đường truyền trên vòng chính bị sự cố thì vòng phụ được sử dụng với chiều đi của tín hiệu ngược với chiều đi của mạng chính.

Ưu và nhược điểm của mạng hình vòng

- *Ưu điểm:* Với dạng kết nối này có ưu điểm là không tốn nhiều dây cáp, tốc độ truyền dữ liệu cao, không gây ách tắc
- *Nhược điểm:* Các giao thức để truyền dữ liệu phức tạp và nếu có trục trặc trên một trạm thì cũng ảnh hưởng đến toàn mạng.

3.2.1.3. Mạng hình tuyến (Bus)



Hình 28– mạng hình tuyến

Trong dạng đường thẳng các máy tính đều được nối vào một đường dây truyền chính (bus). Đường truyền chính này được giới hạn hai đầu bởi một loại đầu nối đặc biệt gọi là terminator (dùng để nhận biết là đầu cuối để kết thúc đường truyền tại đây). Mỗi trạm được nối vào bus qua một đầu nối chữ T (T_connector) hoặc một bộ thu phát (transceiver).

Khi một trạm truyền dữ liệu tín hiệu được quảng bá trên cả hai chiều của bus (tức là mọi trạm còn lại đều có thể thu được tín hiệu đó trực tiếp) theo từng gói một, mỗi gói đều phải mang địa chỉ trạm đích. Các trạm khi thấy dữ liệu đi qua nhận lấy, kiểm tra, nếu đúng với địa chỉ của mình thì nó nhận lấy còn nếu không phải thì bỏ qua.

Đối với bus một chiều thì tín hiệu chỉ đi về một phía, lúc đó các terminator phải được thiết kế sao cho các tín hiệu đó phải được dội lại trên bus để cho các trạm trên mạng đều có thể thu nhận được tín hiệu đó. Như vậy với topo mạng dạng bus dữ liệu được truyền theo các liên kết điểm - nhiều điểm (point - to - multipoint) hay quảng bá (broadcast).

Sau đây là vài thông số kỹ thuật của topology bus. Theo chuẩn IEEE 802.3 (cho mạng cục bộ) với cách đặt tên qui ước theo thông số: tốc độ truyền tính hiệu (1,10 hoặc 100 Mb/s); BASE (nếu là Baseband) hoặc BROAD (nếu là Broadband).

- *10BASE5*: Dùng cáp đồng trục đường kính lớn (10mm) với trở kháng 50 Ohm, tốc độ 10 Mb/s, phạm vi tín hiệu 500m/segment, có tối đa 100 trạm, khoảng cách giữa 2 tranceiver tối thiểu 2,5m (Phương án này còn gọi là Thick Ethernet hay Thicknet)
- *10BASE2*: tương tự như Thicknet nhưng dùng cáp đồng trục nhỏ (RG 58A), có thể chạy với khoảng cách 185m, số trạm tối đa trong 1 segment là 30, khoảng cách giữa hai máy tối thiểu là 0,5m.

Ưu và nhược điểm của mạng hình tuyến

- *Ưu điểm:* Với dạng kết nối này có ưu điểm là không tốn nhiều dây cáp, tốc độ truyền dữ liệu cao, dễ thiết kế.
- *Nhược điểm:* Nếu lưu lượng truyền tăng cao thì dễ gây ách tắc và nếu có trục trặc trên hành lang chính thì khó phát hiện ra.

3.2.1.4. Mạng kết hợp

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

  - Cấu hình mạng dạng này có bộ phận tách tín hiệu (*spitter*) giữ vai trò thiết bị trung tâm, hệ thống dây cáp mạng có thể chọn hoặc *Ring Topology* hoặc *Linear Bus Topology*.
  - Lợi điểm của cấu hình này là mạng có thể gồm nhiều nhóm làm việc ở cách xa nhau, ARCNET là mạng dạng kết hợp *Star/Bus Topology*. Cấu hình dạng này đưa lại sự uyển chuyển trong việc bố trí đường dây tương thích dễ dàng đối với bất cứ toà nhà nào.

- Kết hợp hình sao và vòng *(Star/Ring Topology):*

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

3.2.1.5. So sánh tính năng giữa các cấu trúc của các mạng cục bộ cơ bản

	Đường thẳng	**Vòng Tròn**	**Hình sao**
Ứng dụng	Tốt cho trường hợp mạng nhỏ và mạng có giao thông thấp và lưu lượng dữ liệu thấp	Tốt cho trường hợp mạng có số trạm ít hoạt động với tốc độ cao,không cách nhau xa lắm hoặc mạng có lưu lượng dữ liệu phân bố không đều.	Hiện nay mạng sao là cách tốt nhất cho trường hợp phải tích hợp dữ liệu và tín hiệutiếng.Các mạng đện thoại công cộng có cấu trúc này
Độ phức tạp	Tương đối không phức tạp	Đòi hỏi thiết bị tương đối phức tạp. Mặt khác việc đưa thông điệp đi trên tuyến là đơn giản, vì chỉ có 1 con đường, trạm phát chỉ cần biết địa chỉ của trạm nhận , các thông tin để dẫn đường khác thì không cần thiết	Mạng sao được xem là khá phức tạp. Các trạm được nối với thiết bị trung tâm và lần lượt hoạt động như thiết bị trung tâm hoặc nối được tới các dây dẫn truyền từ xa
Hiệu suất	Rất tốt dưới tải thấp có thể giảm hiệu suất rất mau khi tải tang	Có hiệu quả trong trường hợp lượng lưu thông cao và khá ổn định nhờ sự tăng chậm thời gian trễ và sự xuống cấp so với các mạng khác	Tốt cho trường hợp tải vừa tuy nhiên kích thước và khả năng , suy ra hiệu suất của mạng phụ thuộc trực tiếp vào sức mạnh của thiết bị trung tâm.
Tổng phí	Tương đối thấp đặc biệt do nhiều thiết bị đã phát triển hòa chỉnh và bán sảm phẩm ở thị trường .Sự dư thừa kênh truyền được khuyến để giảm bớt nguy cơ xuất hiện sự cố trên mạng	Phải dự trù gấp đôi nguồn lực hoặc phải có 1 phương thức thay thế khi 1 nút không hoạt động nếu vẫn muốn mạng hoạt động bình thường	Tổng phí rất cao khi làm nhiêm vụ của thiết bị trung tâm, thiết bị trung tâm không được dùng vào việc khác .Số lượng dây riêng cũng nhiều.
Nguy cơ	Một trạm bị hỏng không ảnh	Một trạm bị hỏng có thể ảnh	Độ tin cậy của hệ thống phụ thuộc vào

	hưởng đến cả mạng. Tuy nhiên mạng sẽ có nguy cơ bị tổn hại khi sự cố trên đường dây dẫn chính hoặc có vấn đề với tuyến. Vấn đề trên rất khó xác định được lại rất dễ sửa chữa	hưởng đến cả hệ thống vì các trạm phục thuộc vào nhau. Tìm 1 repeater hỏng rất khó ,vả lại việc sửa chữa thẳng hay dùng mưu mẹo xác định điểm hỏng trên mạng có địa bàn rô#ng rất khó	thiết bị trung tâm, .nếu bị hỏng thì mạng ngưng hoạt động Sự ngưng hoạt động tại thiết bị trung tâm thường không ảnh hươdng đến toàn bộ hệ thống .
Khả năng mở rộng	Việc thêm và định hình lại mạng này rất dễ.Tuy nhiên việc kết nối giữa các máy tính và thiết bị của các hãng khác nhau khó có thể vì chúng phải có thể nhận cùng địa chỉ và dữ liệu	Tương đối dễ thêm và bớt các trạm làm việc mà không phải nối kết nhiều cho mỗi thay đổi Giá thành cho việc thay đổi tương đối thấp	Khả năng mở rộâng hạn chế, đa số các thiết bị trung tâm chỉ chịu đựng nổi 1 số nhất định liên kết. Sự hạn chế về tốc độ truyền dữ liệu và băng tần thường được đòi hỏi ở mỗi người sử dụng. Các hạn chế này giúp cho các chức năng xử lý trung tâm không bị quá tải bởi tốc độ thu nạp tại tại cổng truyền và giá thành mỗi cổng truyền của thiết bị trung tâm thấp .

Bảng 2 - So sánh tính năng giữa các cấu trúc của mạng LAN

3.2.2 Đường truyền vật lý

Đường truyền vật lý dùng để chuyển các tín hiệu giữa các máy tính. Các tín hiệu đó biểu thị các giá trị dữ liệu dưới dạng các xung nhị phân (on - off). Tất cả các tín hiệu đó đều thuộc dạng sóng điện từ (trải từ tần số sóng radio, sóng ngắn, tia hồng ngoại). Ứng với mỗi loại tần số của sóng điện tử có các đường truyền vật lý khác nhau để truyền tín hiệu.

Hiện nay có hai loại đường truyền:

- *Đường truyền hữu tuyến:* cáp đồng trục, cáp đôi dây xoắn (có bọc kim, không bọc kim), cáp sợi quang.

- *Đường truyền vô tuyến:* radio, sóng cực ngắn, tia hồng ngoại.

Mạng cục bộ thường sử dụng 3 loại đường truyền vật lý và cáp đôi xoắn, cáp đồng trục, và cáp sợi quang. Ngoài ra gần đây người ta cũng đã bắt đầu sử dụng nhiều các mạng cục bộ không dây nhờ radio hoặc viba.

Cáp đồng trục đường sử dụng nhiều trong các mạng dạng tuyến tính, hoạt động truyền dẫn theo dải cơ sở (baseband) hoặc dải rộng (broadband). Với dải cơ sở, toàn bộ khả năng của đường truyền được dành cho một kênh truyền thông duy nhất, trong khi đó với dải rộng thì hai hoặc nhiều kênh truyền thông cùng phân chia dải thông của kênh truyền.

Hầu hết các mạng cục bộ đều sử dụng phương thức dải rộng. Với phương thức này tín hiệu có thể truyền đi dưới cả hai dạng: *tương tự* (analog) và *số* (digital) không cần điều chế.

Cáp đồng trục có hai loại là cáp gầy (thin cable) và *cáp béo* (thick cable). Cả hai loại cáp này đều có tốc độ làm việc 10Mb/s nhưng cáp gầy có độ suy hao tín hiệu lớn hơn, có độ dài cáp tối đa cho phép giữa hai repeater nhỏ hơn cáp béo→ Cáp gầy thường dùng để nối các trạm trong cùng một văn phòng, phòng thí nghiệm, còn cáp béo dùng để nối dọc theo hành lang, lên các tầng lầu,..

Phương thức truyền thông theo dải rộng có thể dùng cả cáp đôi xoắn, nhưng cáp đôi xoắn chỉ thích hợp với mạng nhỏ hiệu năng thấp và chi phí đầu tư ít.

Phương thức truyền theo dải rộng chia dải thông (tần số) của đường truyền thành nhiều dải tần con (kênh), mỗi dải tần con đó cung cấp một kênh truyền dữ liệu tách biệt nhờ sử dụng một cặp modem đặc biệt. Phương thức này vốn là một phương tiện truyền một chiều: các tín hiệu đưa vào đường truyền chỉ có thể truyền đi theo một hướng → không cài đặt được các bộ khuyếch đại để chuyển tín hiệu của một tần số theo cả hai chiều. Vì thế xảy ra tình trạng chỉ có trạm nằm dưới trạm truyền là có thể nhận được tín hiệu. Vậy làm thế nào để có hai đường dẫn dữ liệu trên mạng. Điểm gặp nhau của hai đường dẫn đó gọi là điểm đầu cuối. Ví dụ, trong topo dạng bus thì điểm đầu cuối đơn giản chính là đầu mút của bus (terminator), còn với topo dạng cây (tree) thì chính là gốc của cây (root). Các trạm khi truyền đều truyền về hướng điểm đầu cuối (gọi là đường dẫn về), sau đó các tín hiệu nhận được ở điểm đầu cuối sẽ truyền theo đường dẫn thứ hai xuất phát từ điểm đầu cuối (gọi là đường dẫn đi). Tất cả các trạm đều nhận dữ liệu trên đường dẫn đi. Để cài đặt đường dẫn về và đi, có thể sử dụng cấu hình vật lý sau:

Trong cấu hình cáp đôi (dual cable), các đường dẫn về và đi chạy trên các cáp riêng biệt và điểm đầu cuối đơn giản chỉ là một đầu nối thụ động của chúng. Trạm gửi và nhận cùng một tần số. Trong cấu hình tách (split), cả hai đường dẫn đều ở trên cùng một cáp nhưng tần

số khác nhau: đường dẫn về có tần số thấp và đường dẫn đi có tần số cao hơn. Điểm đầu cuối là bộ chuyển đổi tần số.

Việc lựa chọn đường truyền và thiết kế sơ đồ đi cáp (trong trường hợp hữu tuyến) là một trong những công việc quan trọng nhất khi thiết kế và cài đặt một mạng máy tính nói chung và mạng cục bộ nói riêng. Giải pháp lựa chọn pháp đáp ứng được nhu cầu sử dụng mạng thực tế không chỉ cho hiện tại mà cho cả tương lai. Chẳng hạn muốn truyền dữ liệu đa phương tiện thì không thể chọn loại cáp chỉ cho phép thông lượng tối đa là vài Mb/s, mà phải nghĩ đến loại cáp cho phép thông lượng trên 100 Mb/s. Việc lắp đặt hệ thống trong cáp trong nhiều trường hợp (toà nhà nhiều tầng) là tốn rất nhiều công của → phải lựa chọn cẩn thận, không thể để xảy ra trường hợp chọn cáp bừa bãi rồi sau đó một hai năm lại gỡ bỏ, lắp đặt lại hệ thống mới hoàn toàn mới.

Đường cáp truyền mạng là cơ sở hạ tầng của một hệ thống mạng, nên nó rất quan trọng và ảnh hưởng rất nhiều đến khả năng hoạt động của mạng. Hiện nay người ta thường dùng 3 loại dây cáp là cáp đôi xoắn, cáp đồng trục và cáp quang.

3.2.2.1. Cáp đôi xoắn

Đây là loại cáp gồm hai đường dây dẫn đồng được xoắn vào nhau nhằm làm giảm nhiễu điện từ gây ra bởi môi trường xung quanh và giữa chúng với nhau.

Hiện nay có hai loại cáp xoắn là cáp có bọc kim loại (STP - Shield Twisted Pair) và cáp không bọc kim loại (UTP -Unshield Twisted Pair).

- Cáp có bọc kim loại (STP): Lớp bọc bên ngoài có tác dụng chống nhiễu điện từ, có loại có một đôi giây xoắn vào nhau và có loại có nhiều đôi giây xoắn với nhau.
- Cáp không bọc kim loại (UTP): Tính tương tự như STP nhưng kém hơn về khả năng chống nhiễu và suy hao vì không có vỏ bọc.

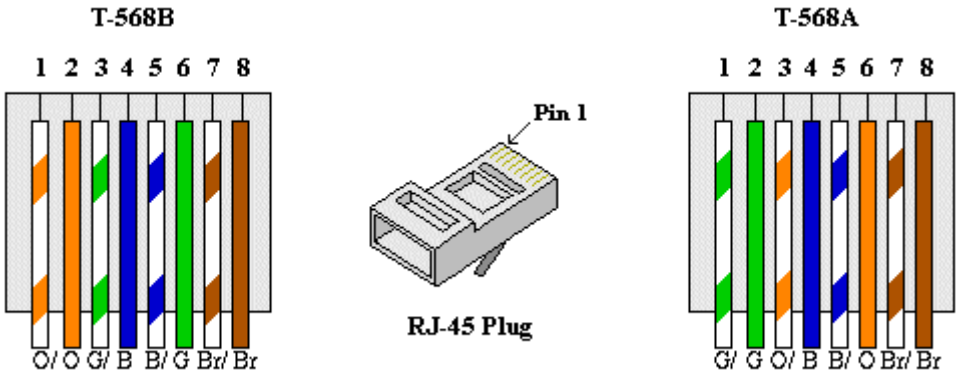
STP và UTP có các loại (Category - Cat) thường dùng:

- Loại 1 & 2 (Cat 1 & Cat 2): Thường dùng cho truyền thoại và những đường truyền tốc độ thấp (nhỏ hơn 4Mb/s).
- Loại 3 (Cat 3): tốc độ truyền dữ liệu khoảng 16 Mb/s , nó là chuẩn cho hầu hết các mạng điện thoại.
- Loại 4 (Cat 4): Thích hợp cho đường truyền 20Mb/s.
- Loại 5 (Cat 5): Thích hợp cho đường truyền 100Mb/s.
- Loại 6 (Cat 6): Thích hợp cho đường truyền 300Mb/s.

Đây là loại cáp rẻ, dễ cài đặt tuy nhiên nó dễ bị ảnh hưởng của môi trường.

Chiều dài tối đa đã được quy định trong Network Architecture cho từng loại cáp và chiều dài không phụ thuộc vào kiểu dây hay cách bấm dây. Đối với UTP thì chiều dài tối đa là 100m và tối thiểu là 0.5m tính từ HUB to PC, còn PC to PC thì 2.5m.

Cách bấm dây mạng có nhiều cách tùy vào mục đích sử dụng. Chọn cách bấm nào còn phụ thuộc loại dây cáp. Chẳng hạn loại cáp UTP cat 5 và cat 5e sẽ cho tốc độ truyền tải khác nhau thì sẽ có cách bấm khác nhau. Có 2 cách bấm dây chuẩn cho các loại cáp UTP gọi là T568A và T568B.



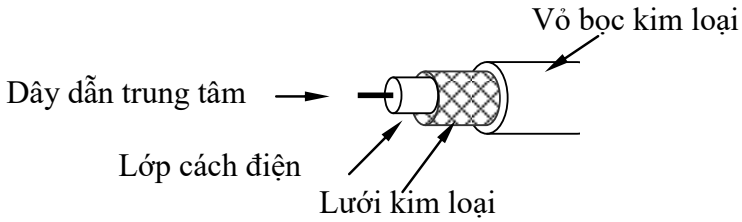
Hình 29 - Có 2 kiểu: straight-through và cross-cable hay còn gọi là crossover.

Straight: dùng để nối PC -> HUB/SWITCH hay các thiết bị mạng khác có hổ trợ. Đối với kiểu straight thì ở một đầu dây bạn sắp xếp thứ tự dây thế nào thì ở đầu dây còn lại phải đúng y như thế.

Crossover: dùng để nối trực tiếp PC->PC, HUB->HUB hay các thiết bị mạng cùng layer với nhau. Kiểu này phải bấm đảo đầu dây tức là cặp TX (cặp truyền) ở đầu này sẽ trở thành RX (nhận) ở đầu kia bằng cách đổi vị trí của cặp xoắn 2 và 3. Dễ hiểu hơn thì trộn T-568A và T-568B = CrossOver

3.2.2.2. Cáp đồng trục

Cáp đồng trục có hai đường dây dẫn và chúng có cùng một trục chung, một dây dẫn trung tâm (*thường là dây đồng cứng*) đường dây còn lại tạo thành đường ống bao xung quanh dây dẫn trung tâm (*dây dẫn này có thể là dây bện kim loại và vì nó có chức năng chống nhiễu nên còn gọi là lớp bọc kim*). Giữa hai dây dẫn trên có một lớp cách ly (*lớp cách điện*), và bên ngoài cùng là lớp vỏ plastic để bảo vệ cáp.



Hình 30 - Cáp đồng trục

Các loại cáp	***Dây xoắn cặp***	***Cáp đồng trục mỏng***	***Cáp đồng trục dày***	***Cáp quang***
Chi tiết	Bằng đồng, có 4 và 25 cặp dây (loại 3, 4, 5)	Bằng đồng, 2 dây, đường kính 5mm	Bằng đồng, 2 dây, đường kính 10mm	Thủy tinh, 2 sợi
Loại kết nối	RJ-25 hoặc 50-pin telco	BNC	N-series	ST
Chiều dài đoạn tối đa	100m	185m	500m	1000m
Số đầu nối tối đa trên 1 đoạn	2	30	100	2
Chạy 10 Mbit/s	Được	Được	Được	Được
Chạy 100 Mbit/s	Được	Không	Không	Được
Chống nhiễu	Tốt	Tốt	Rất tốt	Hoàn toàn
Bảo mật	Trung bình	Trung bình	Trung bình	Hoàn toàn
Độ tin cậy	Tốt	Trung bình	Tốt	Tốt
Lắp đặt	Dễ dàng	Trung bình	Khó	Khó
Khắc phục lỗi	Tốt	Dở	Dở	Tốt
Quản lý	Dễ dàng	Khó	Khó	Trung bình
Chi phí cho 1 trạm	Rất thấp	Thấp	Trung bình	Cao
Ứng dụng tốt nhất	Hệ thống Workgroup	Đường backbone	Đường backbone trong tủ mạng	Đường backbone dài trong tủ mạng hoặc các tòa nhà

Bảng 3 - Tính năng kỹ thuật của một số loại cáp mạng

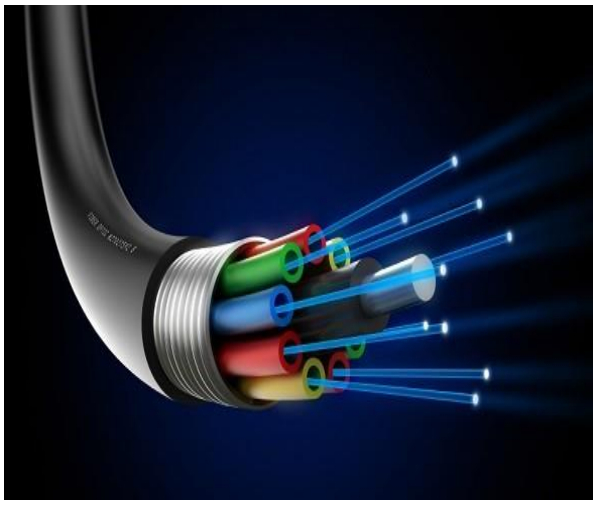
Cáp đồng trục có độ suy hao ít hơn so với các loại cáp đồng khác (ví dụ như cáp xoắn đôi) do ít bị ảnh hưởng của môi trường. Các mạng cục bộ sử dụng cáp đồng trục có thể có kích thước trong phạm vi vài ngàn mét, cáp đồng trục được sử dụng nhiều trong các mạng dạng đường thẳng. Hai loại cáp thường được sử dụng là cáp đồng trục mỏng và cáp đồng trục dày trong đường kính cáp đồng trục mỏng là 0,25 inch, cáp đồng trục dày là 0,5 inch. Cả hai loại cáp đều làm việc ở cùng tốc độ nhưng cáp đồng trục mỏng có độ hao suy tín hiệu lớn hơn

Hiện nay có cáp đồng trục sau:

- RG -58,50 ohm: dùng cho mạng Thin Ethernet
- RG -59,75 ohm: dùng cho truyền hình cáp
- RG -62,93 ohm: dùng cho mạng ARCnet

Các mạng cục bộ thường sử dụng cáp đồng trục có dải thông từ 2,5 - 10 Mb/s, cáp đồng trục có độ suy hao ít hơn so với các loại cáp đồng khác vì nó có lớp vỏ bọc bên ngoài, độ dài thông thường của một đoạn cáp nối trong mạng là 200m, thường sử dụng cho dạng Bus.

3.2.2.3. Cáp sợi quang (Fiber - Optic Cable)



Hình 31- Cáp sợi quang

Cáp sợi quang bao gồm một dây dẫn trung tâm *(là một hoặc một bó sợi thủy tinh có thể truyền dẫn tín hiệu quang)* được bọc một lớp vỏ bọc có tác dụng phản xạ các tín hiệu trở lại để giảm sự mất mát tín hiệu. Bên ngoài cùng là lớp vỏ plastic để bảo vệ cáp. Như vậy cáp sợi quang không truyền dẫn các tín hiệu điện mà chỉ truyền các tín hiệu quang (các tín hiệu dữ liệu phải được chuyển đổi thành các tín hiệu quang và khi nhận chóng sẽ lại được chuyển đổi trở lại thành tín hiệu điện).

Cáp quang có đường kính từ 8.3 - 100 micron, Do đường kính lõi sợi thuỷ tinh có kích thước rất nhỏ nên rất khó khăn cho việc đấu nối, nên cần công nghệ đặc biệt với kỹ thuật cao đòi hỏi chi phí cao.

Dải thông của cáp quang có thể lên tới hàng Gbps và cho phép khoảng cách đi cáp khá xa do độ suy hao tín hiệu trên cáp rất thấp. Ngoài ra, vì cáp sợi quang không dùng tín hiệu điện từ để truyền dữ liệu nên nó hoàn toàn không bị ảnh hưởng của nhiễu điện từ và tín hiệu truyền không thể bị phát hiện và thu trộm bởi các thiết bị điện tử của người khác.

Chỉ trừ nhược điểm khã lắp đặt vì giá thành còn cao, nhìn chung cáp quang thích hợp cho mọi mạng hiện nay và sau này.

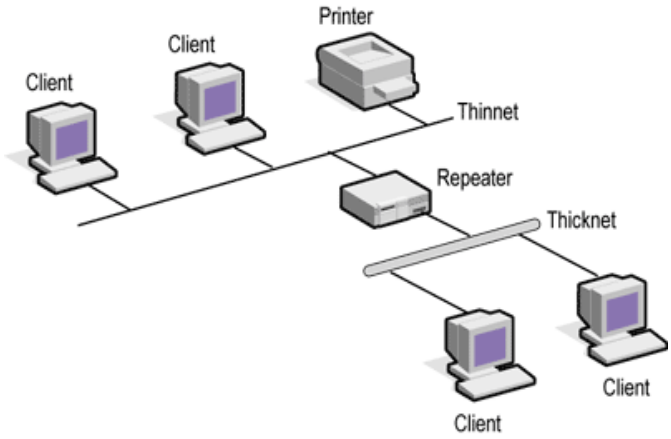
Các yêu cầu cho một hệ thống cáp:

- An toàn, thẩm mỹ: tất cả các dây mạng phải được bao bọc cẩn thận, cách xa các nguồn điện, các máy có khả năng phát sóng để tránh trường hợp bị nhiễu. Các đầu nối phải đảm bảo chất lượng, tránh tình trạng hệ thống mạng bị chập chờn.
- Đúng chuẩn: hệ thống cáp phải thực hiện đúng chuẩn, đảm bảo cho khả năng nâng cấp sau này cũng như dễ dàng cho việc kết nối các thiết bị khác nhau của các nhà sản xuất khác nhau. Tiêu chuẩn quốc tế dùng cho các hệ thống mạng hiện nay là EIA/TIA 568B.
- Tiết kiệm và "linh hoạt" (flexible): hệ thống cáp phải được thiết kế sao cho kinh tế nhất, dễ dàng trong việc di chuyển các trạm làm việc và có khả năng mở rộng sau này.

3.2.3 Các thiết bị mạng

a. Repeater (Bộ tiếp sức)

Repeater là loại thiết bị phần cứng đơn giản nhất trong các thiết bị liên kết mạng, nó được hoạt động trong tầng vật lý của mô hình hệ thống mở OSI. Repeater dùng để nối 2 mạng giống nhau hoặc các phần một mạng cùng có một nghi thức và một cấu hình. Khi Repeater nhận được một tín hiệu từ một phía của mạng thì nó sẽ phát tiếp vào phía kia của mạng.



Hình 32– Mô hình liên kết mạng của Repeater

Repeater không có xử lý tín hiệu mà nó chỉ loại bỏ các tín hiệu méo, nhiễu, khuếch đại tín hiệu đã bị suy hao (vì đã được phát với khoảng cách xa) và khôi phục lại tín hiệu ban đầu. Việc sử dụng Repeater đã làm tăng thêm chiều dài của mạng.

Hình 33 –Thiết bị Repeater

Hiện nay có hai loại Repeater đang được sử dụng là Repeater điện và Repeater điện quang.

- ***Repeater điện:*** nối với đường dây điện ở cả hai phía của nó, nó nhận tín hiệu điện từ một phía và phát lại về phía kia. Khi một mạng sử dụng Repeater điện để nối các phần của mạng lại thì có thể làm tăng khoảng cách của mạng, nhưng khoảng cách đó luôn bị hạn chế bởi một khoảng cách tối đa do độ trễ của tín hiệu. Ví dụ với mạng sử dụng cáp đồng trục 50 thì khoảng cách tối đa là 2.8 km, khoảng cách đó không thể kéo thêm cho dù sử dụng thêm Repeater.
- ***Repeater điện quang:*** liên kết với một đầu cáp quang và một đầu là cáp điện, nó chuyển một tín hiệu điện từ cáp điện ra tín hiệu quang để phát trên cáp quang và ngược lại. Việc sử dụng Repeater điện quang cũng làm tăng thêm chiều dài của mạng.

Việc sử dụng Repeater không thay đổi nội dung các tín hiện đi qua nên nó chỉ được dùng để nối hai mạng có cùng giao thức truyền thông (như hai mạng Ethernet hay hai mạng Token ring) nhưng không thể nối hai mạng có giao thức truyền thông khác nhau (như một mạng Ethernet và một mạng Token ring). Thêm nữa Repeater không làm thay đổi khối lượng chuyển vận trên mạng nên việc sử dụng không tính toán nó trên mạng lớn sẽ hạn chế hiệu năng của mạng. Khi lựa chọn sử dụng Repeater cần chú ý lựa chọn loại có tốc độ chuyển vận phù hợp với tốc độ của mạng.

b. Bridge (Cầu nối)

Hình 34– Thiết bị cầu nối

Bridge là một thiết bị có xử lý dùng để nối hai mạng giống nhau hoặc khác nhau, nó có thể được dùng với các mạng có các giao thức khác nhau. Cầu nối hoạt động trên tầng liên kết dữ liệu nên không như bộ tiếp sức phải phát lại tất cả những gì nó nhận được thì cầu nối đọc được các gói tin của tầng liên kết dữ liệu trong mô hình OSI và xử lý chúng trước khi quyết định có chuyển đi hay không.

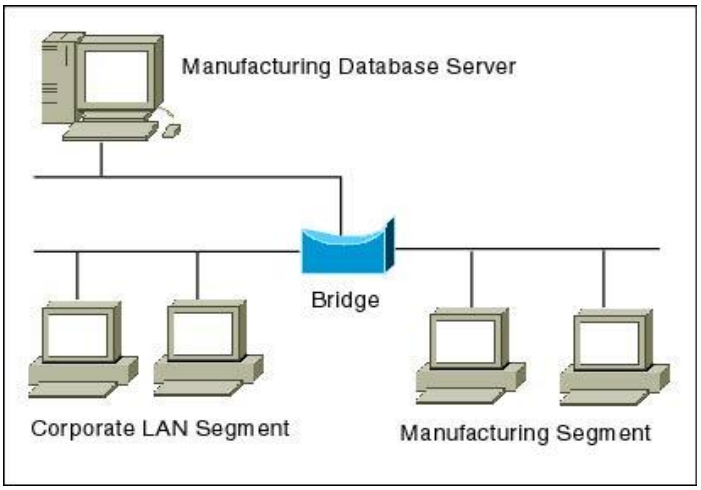
Khi nhận được các gói tin Bridge chọn lọc và chỉ chuyển những gói tin mà nó thấy cần thiết. Điều này làm cho Bridge trở nên có ích khi nối một vài mạng với nhau và cho phép nó hoạt động một cách mềm dẻo.

Để thực hiện được điều này trong Bridge ở mỗi đầu kết nối có một bảng các địa chỉ các trạm được kết nối vào phía đó, khi hoạt động cầu nối xem xét mỗi gói tin nó nhận được bằng cách đọc địa chỉ của nơi gửi và nhận và dựa trên bảng địa chỉ phía nhận được gói tin nó quyết định gửi gói tin hay không và bổ xung bảng địa chỉ.

Khi đọc địa chỉ nơi gửi Bridge kiểm tra xem trong bảng địa chỉ của phần mạng nhận được gói tin có địa chỉ đó hay không, nếu không có thì Bridge tự động bổ xung bảng địa chỉ (*cơ chế đó được gọi là tự học của cầu nối*).

Khi đọc địa chỉ nơi nhận Bridge kiểm tra xem trong bảng địa chỉ của phần mạng nhận được gói tin có địa chỉ đó hay không, nếu có thì Bridge sẽ cho rằng đó là gói tin nội bộ thuộc phần mạng mà gói tin đến nên không chuyển gói tin đó đi, nếu ngược lại thì Bridge mới

chuyển sang phía bên kia. ở đây chúng ta thấy một trạm không cần thiết chuyển thông tin trên toàn mạng mà chỉ trên phần mạng có trạm nhận mà thôi.



Hình 35 – Mô hình cầu nối

Để đánh giá một Bridge người ta đưa ra hai khái niệm: Lọc và chuyển vận. Quá trình xử lý mỗi gói tin được gọi là quá trình lọc trong đó tốc độ lọc thể hiện trực tiếp khả năng hoạt động của Bridge. Tốc độ chuyển vận được thể hiện số gói tin/giây trong đó thể hiện khả năng của Bridge chuyển các gói tin từ mạng này sang mạng khác.

Hiện nay có hai loại Bridge đang được sử dụng là Bridge vận chuyển và Bridge biên dịch. Bridge *vận chuyển* dùng để nối hai mạng cục bộ cùng sử dụng một giao thức truyền thông của tầng liên kết dữ liệu, tuy nhiên mỗi mạng có thể sử dụng loại dây nối khác nhau. Bridge vận chuyển không có khả năng thay đổi cấu trúc các gói tin mà nó nhận được mà chỉ quan tâm tới việc xem xét và chuyển vận gói tin đó đi.

Bridge biên dịch dùng để nối hai mạng cục bộ có giao thức khác nhau nó có khả năng chuyển một gói tin thuộc mạng này sang gói tin thuộc mạng kia trước khi chuyển qua.

Ví dụ : Bridge biên dịch nối một mạng Ethernet và một mạng Token ring. Khi đó Cầu nối thực hiện như một nút token ring trên mạng Token ring và một nút Enthernet trên mạng Ethernet. Cầu nối có thể chuyển một gói tin theo chuẩn đang sử dụng trên mạng Enthernet sang chuẩn đang sử dụng trên mạng Token ring.

Tuy nhiên chú ý ở đây cầu nối không thể chia một gói tin ra làm nhiều gói tin cho nên phải hạn chế kích thước tối đa các gói tin phù hợp với cả hai mạng. Ví dụ như kích thước tối đa của gói tin trên mạng Ethernet là 1500 bytes và trên mạng Token ring là 6000 bytes do vậy nếu một trạm trên mạng token ring gửi một gói tin cho trạm trên mạng Ethernet với kích thước lớn hơn 1500 bytes thì khi qua cầu nối số lượng byte dư sẽ bị chặt bỏ.

Người ta sử dụng Bridge trong các trường hợp sau:

- Mở rộng mạng hiện tại khi đã đạt tới khoảng cách tối đa do Bridge sau khi sử lý gói tin đã phát lại gói tin trên phần mạng còn lại nên tín hiệu tốt hơn bộ tiếp sức.
- Giảm bớt tắc nghẽn mạng khi có quá nhiều trạm bằng cách sử dụng Bridge, khi đó chúng ta chia mạng ra thành nhiều phần bằng các Bridge, các gói tin trong nội bộ tùng phần mạng sẽ không được phép qua phần mạng khác.
- Để nối các mạng có giao thức khác nhau.

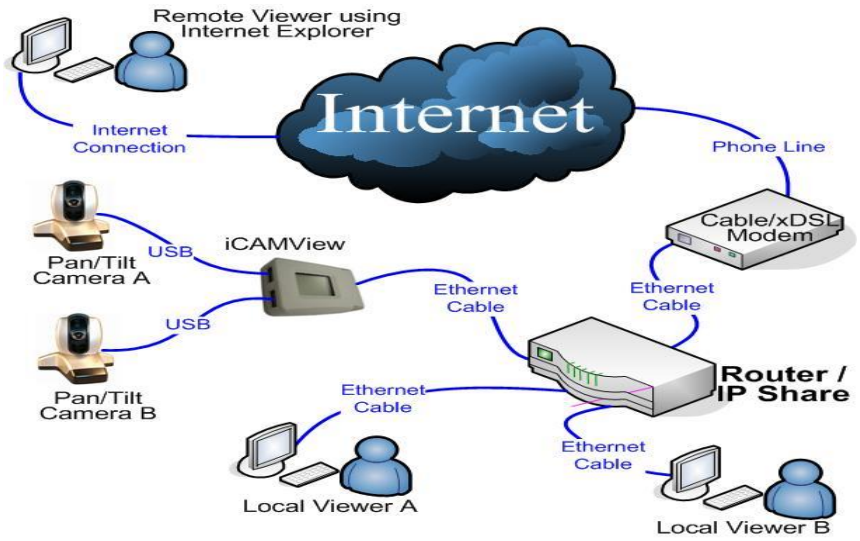
Một vài Bridge còn có khả năng lựa chọn đối tượng vận chuyển. Nó có thể chỉ chuyển vận những gói tin của nhưng địa chỉ xác định. Ví dụ : cho phép gói tin của máy A, B qua Bridge 1, gói tin của máy C, D qua Bridge 2.

Một số Bridge được chế tạo thành một bộ riêng biệt, chỉ cần nối dây và bật. Các Bridge khác chế tạo như card chuyên dùng cắm vào máy tính, khi đó trên máy tính sẽ sử dụng phần mềm Bridge. Việc kết hợp phần mềm với phần cứng cho phộp uyển chuyển hơn trong hoạt động của Bridge.

c. Router (Bộ tìm đường)

Hình 36 – Thiết bị Router

Router là một thiết bị hoạt động trên tầng mạng, nú có thể tìm được đường đi tốt nhất cho các gói tin qua nhiều kết nối để đi từ trạm gửi thuộc mạng đầu đến trạm nhận thuộc mạng cuối. Router có thể được sử dụng trong việc nối nhiều mạng với nhau và cho phộp các gói tin có thể đi theo nhiều đường khác nhau để tới đích.



Hình 37 – Hoạt động của Router

Khác với Bridge hoạt động trên tầng liên kết dữ liệu nên Bridge phải xử lý mọi gói tin trên đường truyền thì Router có địa chỉ riêng biệt và nó chỉ tiếp nhận và xử lý các gói tin gửi đến nó mà thôi. Khi một trạm muốn gửi gói tin qua Router thì nó phải gửi gói tin với địa chỉ trực tiếp của Router (*trong gói tin đó phải chứa các thông tin khác về đích đến*) và khi gói tin đến Router thì Router mới xử lý và gửi tiếp.

Khi xử lý một gói tin Router phải tìm được đường đi của gói tin qua mạng. Để làm được điều đó Router phải tìm được đường đi tốt nhất trong mạng dựa trên các thông tin nó có về mạng, thông thường trên mỗi Router có một bảng chỉ đường (Router table). Dựa trên dữ liệu về Router gần đó và các mạng trong liên mạng, Router tính được bảng chỉ đường (Router table) tối ưu dựa trên một thuật toán xác định trước.

Người ta phân chia Router thành hai loại là Router có phụ thuộc giao thức (The protocol dependent routers) và Router không phụ thuộc vào giao thức (The protocol independent router) dựa vào phương thức xử lý các gói tin khi qua Router.

- *Router có phụ thuộc giao thức:* Chỉ thực hiện việc tìm đường và truyền gói tin từ mạng này sang mạng khác chứ không chuyển đổi phương cách đóng gói của gói tin cho nên cả hai mạng phải dùng chung một giao thức truyền thông.
- *Router không phụ thuộc vào giao thức*: có thể liên kết các mạng dùng giao thức truyền thông khác nhau và có thể chuyển gói tin của giao thức này sang gói tin của giao thức kia, Router cũng chấp nhận kích thước các gói tin khác nhau (Router có thể chia nhỏ một gói tin lớn thành nhiều gói tin nhỏ trước truyền trên mạng).

Để ngăn chặn việc mất mát số liệu Router còn nhận biết được đường nào có thể chuyển vận và ngừng chuyển vận khi đường bị tắc.

Các lý do sử dụng Router :

- Router có các phần mềm lọc ưu việt hơn là Bridge do các gói tin muốn đi qua Router cần phải gửi trực tiếp đến nó nên giảm được số lượng gói tin qua nó. Router thường được sử dụng trong khi nối các mạng thông qua các đường dây thuê bao đắt tiền do nó không truyền dư lên đường truyền.
- Router có thể dùng trong một liên mạng có nhiều vùng, mỗi vùng có giao thức riêng biệt.
- Router có thể xác định được đường đi an toàn và tốt nhất trong mạng nên độ an toàn của thông tin được đảm bảo hơn.
- Trong một mạng phức hợp khi các gói tin luân chuyển các đường có thể gây nên tình trạng tắc nghẽn của mạng thì các Router có thể được cài đặt các phương thức nhằm tránh được tắc nghẽn.

Các phương thức hoạt động của Router

Đó là phương thức mà một Router có thể nối với các Router khác để qua đó chia sẻ thông tin về mạng hiện co. Các chương trình chạy trên Router luôn xây dựng bảng chỉ đường qua việc trao đổi các thông tin với các Router khác.

- *Phương thức véc tơ khoảng cách* : mỗi Router luôn luôn truyền đi thông tin về bảng chỉ đường của mình trên mạng, thông qua đó các Router khác sẽ cập nhật lên bảng chỉ đường của mình.
- *Phương thức trạng thái tĩnh* : Router chỉ truyền các thông báo khi có phát hiện có sự thay đổi trong mạng vàchỉ khi đó các Routerkhác ù cập nhật lại bảng chỉ đường, thông tin truyền đi khi đó thường là thông tin về đường truyền.

Một số giao thức hoạt động chính của Router

- *RIP (Routing Information Protocol)* được phát triển bởi Xerox Network system và sử dụng SPX/IPX và TCP/IP. RIP hoạt động theo phương thức véc tơ khoảng cách.
- *NLSP (Netware Link Service Protocol)* được phát triển bởi Novell dùng để thay thế RIP hoạt động theo phương thức véctơ khoảng cách, mỗi Router được biết cấu trúc của mạng và việc truyền các bảng chỉ đường giảm đi..
- *OSPF (Open Shortest Path First)* là một phần của TCP/IP với phương thức trạng thái tĩnh, trong đó có xét tới ưu tiên, giá đường truyền, mật độ truyền thông...

- *OSPF-IS (Open System Interconnection Intermediate System to Intermediate System)* là một phần của TCP/IP với phương thức trạng thái tĩnh, trong đó có xét tới ưu tiên, giá đường truyền, mật độ truyền thông...

d. Gateway (cổng nối)

Hình 38 – Thiết bị Gateway

Gateway dùng để kết nối các mạng không thuần nhất chẳng hạn như các mạng cục bộ và các mạng máy tính lớn (Mainframe), do các mạng hoàn toàn không thuần nhất nên việc chuyển đổi thực hiện trên cả 7 tầng của hệ thống mở OSI. Thường được sử dụng nối các mạng LAN vào máy tính lớn. Gateway có các giao thức xác định trước thường là nhiều giao thức, một Gateway đa giao thức thường được chế tạo như các Card có chứa các bộ xử lý riêng và cài đặt trên các máy tính hoặc thiết bị chuyên biệt.

Hoạt động của Gateway thông thường phức tạp hơn là Router nên thông suất của nó thường chậm hơn và thường không dùng nối mạng LAN -LAN.

e. Hub (bộ tập trung)

Hình 39 – Thiết bị Hub

Hub thường được dùng để nối mạng, thông qua những đầu cắm của nó người ta liên kết với các máy tính dưới dạng hình sao.

Người ta phân biệt các Hub thành 3 loại như sau sau:

- ***Hub bị động (Passive Hub) :*** Hub bị động không chứa các linh kiện điện tử và cũng không xử lý các tín hiệu dữ liệu, nó có chức năng duy nhất là tổ hợp các tín hiệu từ một số đoạn cáp mạng. Khoảng cách giữa một máy tính và Hub không thể lớn hơn một nửa khoảng cách tối đa cho phép giữa 2 máy tính trên mạng (ví dụ khoảng cách tối đa cho phép giữa 2 máy tính của mạng là 200m thì khoảng cách tối đa giữa một máy tính và hub là 100m). Các mạng ARCnet thường dùng Hub bị động.
- ***Hub chủ động (Active Hub) :*** Hub chủ động có các linh kiện điện tử có thể khuyếch đại và xử lý các tín hiệu điện tử truyền giữa các thiết bị của mạng. Qúa trình xử lý tín hiệu được gọi là tái sinh tín hiệu, nó làm cho tín hiệu trở nên tốt hơn, ít nhạy cảm với lỗi do vậy khoảng cách giữa các thiết bị có thể tăng lên. Tuy nhiên những ưu điểm đó cũng kéo theo giá thành của Hub chủ động cao hơn nhiều so với Hub bị động. Các mạng Token ring có xu hướng dùng Hub chủ động.
- ***Hub thông minh (Intelligent Hub):*** cũng là Hub chủ động nhưng có thêm các chức năng mới so với loại trước, nó có thể có bộ vi xử lý của mình và bộ nhớ mà qua đó nó không chỉ cho phép điều khiển hoạt động thông qua các chương trình quản trị mạng mà nó có thể hoạt động như bộ tìm đường hay một cầu nối. Nó có thể cho phép tìm đường cho gói tin rất nhanh trên các cổng của nó, thay vì phát lại gói tin trên mọi cổng thì nó có thể chuyển mạch để phát trên một cổng có thể nối tới trạm đích.

3.2.4 Các phương pháp truy cập đường truyền vật lý

Đối với topo dạng hình sao, khi một liên kết được thiết lập giữa hai trạm thì thiết bị trung tâm sẽ đảm bảo đường truyền được dành riêng trong suốt cuộc truyền. Tuy nhiên đối với topo dạng vòng và tuyến tính thì chỉ có một đường truyền duy nhất nối tất cả các trạm với nhau bởi vậy cần phải có một quy tắc chung cho tất cả các trạm nối vào mạng để bảo đảm rằng đường truyền được truy nhập và sử dụng một cách tốt đẹp.

Có nhiều phương pháp khác nhau để truy nhập đường truyền vật lý, được phân làm hai loại: *phương pháp truy nhập ngẫu nhiên (random access)* và *phương pháp truy nhập có điều khiển (contronlled access).*

Trong đó có 3 phương pháp hay dùng nhất trong các mạng cục bộ hiện nay: phương pháp CSMA/CD, Token Bus, Token Ring.

3.2.4.1. Phương pháp truy cập ngẫu nhiên

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

Phương pháp này sử dụng cho topo dạng bus, trong đó tất cả các trạm của mạng đều được nối trực tiếp vào bus. Mọi trạm đều có thể truy nhập vào bus chung (đa truy nhập) một cách ngẫu nhiên và do vậy rất có thể dẫn đến xung đột (hai hoặc nhiều trạm đồng thời truyền dữ liệu). Dữ liệu được truyền trên mạng theo một khuôn dạng đã định sẵn trong đó có một vùng thông tin điều khiển chứa địa chỉ trạm đích.

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

- Giải thuật 1: Tạm "rút lui" chờ đợi trong một thời gian ngẫu nhiên nào đó rồi lại bắt đầu nghe đường truyền (Non persistent - không kiên trì).
- Giải thuật 2: Tiếp tục "nghe" đến khi đường truyền rỗi thì truyền dữ liệu đi với xác suất = 1.
- Giải thuật 3: Tiếp tục "nghe" đến khi đường truyền rỗi thì truyền đi với xác suất p xác định trước ($0 < p < 1$).

Với giải thuật 1 có hiệu quả trong việc tránh xung đột vì hai trạm cần truyền khi thấy đường truyền bận sẽ cùng "rút lui" chờ đợi trong các thời đoạn ngẫu nhiên khác. Tuy nhiên nó lại có nhược điểm là: có thể có thời gian "chết" sau mỗi cuộc truyền.

Giải thuật 2: khắc phục nhược điểm có thời gian chết bằng cách cho phép một trạm có thể truyền ngay sau khi một cuộc truyền kết thúc. Nhưng nó lại có nhược điểm là: nếu lúc đó có hơn một trạm đang đợi thì khả năng xảy ra xung đột là rất cao

Giải thuật 3: Trung hoà giữa hai giải thuật trên. Với giá trị p lựa chọn hợp lý có thể tối thiểu hoá được cả khả năng xung đột lẫn thời gian chết của đường truyền. Xảy ra xung đột là do độ trễ của đường truyền dẫn: một trạm truyền dữ liệu đi rồi nhưng do độ trễ đường truyền nên một trạm khác lúc đó đang nghe đường truyền sẽ tưởng là rỗi và cứ thể truyền dữ liệu đi dẫn đến xung đột. Nguyên nhân xảy ra xung đột của phương pháp này là các trạm chỉ "nghe trước khi nói" mà không "nghe trong khi nói" do vậy trong thực tế có xảy ra xung đột mà không biết, vẫn cứ tiếp tục truyền dữ liệu đi, gây ra chiếm dụng đường truyền một cách vô ích.

Để có thể phát hiện xung đột, cải tiến thành phương pháp CSMA/CD (LWT - Listen While Talk - nghe trong khi nói) tức là bổ xung thêm các quy tắc:

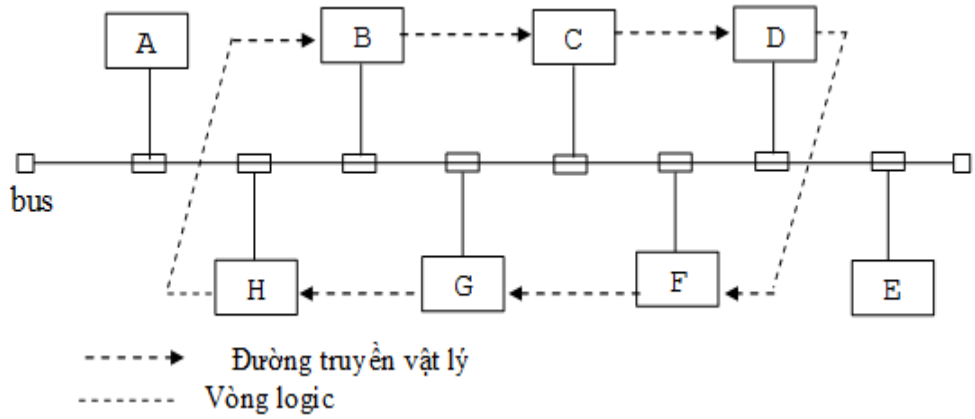
- Khi một trạm đang truyền, nó vẫn tiếp tục nghe đường truyền. Nếu phát hiện thấy xung đột thì nó ngừng ngay việc truyền nhưng vẫn tiếp tục gửi sóng mang thêm một thời gian nữa để đảm bảo rằng tất cả các trạm trên mạng đều có thể nghe được sự kiện xung đột đó.
- Sau đó trạm chờ đợi một thời gian ngẫu nhiên nào đó rồi thử truyền lại theo các quy tắc của CSMA. Rõ ràng với CSMA/CD thời gian chiếm dụng đường truyền vô ích giảm xuống bằng thời gian để phát hiện xung đột. CSMA/CD cũng sử dụng một trong 3 giải thuật "kiên nhẫn" ở trên, trong đó giải thuật 2 được ưa dùng hơn cả.

3.2.4.2. Phương pháp truy nhập có điều khiển

Các phương pháp truy nhập có điều khiển chủ yếu dùng kỹ thuật chuyển thẻ bài (token passing) để cấp phát quyền truy nhập đường truyền. 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. Có 2 phương pháp : Token Bus (Bus với thẻ bài) và Token Ring (Vòng với thẻ bài).

a. Phương pháp Token BUS (bus với thẻ bài)

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



Hình 40 - Ví dụ vòng logic trong mạch bus

Trong hình vẽ, các trạm A, E nằm ngoài vòng logic, chỉ có thể tiếp nhận dữ liệu dành cho chúng.

Vấn đề quan trọng là phải duy trì được vòng logic tuỳ theo trạng thái thực tế của mạng tại thời điểm nào đó. Cụ thể cần phải thực hiện các chức năng sau:

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

Các giải thuật cho các chức năng trên có thể làm như sau:

- Bổ sung một trạm vào vòng logic, mỗi trạm trong vòng có trách nhiệm định kỳ tạo cơ hội cho các trạm mới nhập vào vòng. Khi chuyển thẻ bài đi, trạm sẽ gửi thông báo "tìm trạm đứng sau" để mời các trạm (có địa chỉ giữa nó và trạm kế tiếp nếu có) gửi yêu cầu nhập vòng. Nếu sau một thời gian xác định trước mà không có yêu cầu nào thì trạm sẽ chuyển thẻ bài tới trạm kề sau nó như thường lệ. Nếu có yêu cầu thì trạm gửi thẻ bài sẽ ghi nhận trạm yêu cầu trở thành trạm đứng kề sau nó và chuyển thẻ bài tới trạm mới này. Nếu có hơn một trạm yêu cầu nhập vòng thì trạm giữ thẻ bài sẽ phải lựa chọn theo giải thuật nào đó.

- Loại một trạm khỏi vòng logic: Một trạm muốn ra khỏi vòng logic sẽ đợi đến khi nhận được thẻ bài sẽ gửi thông báo "nối trạm đứng sau" tới trạm kề trước nó yêu cầu trạm này nối trực tiếp với trạm kề sau nó
- Quản lý lỗi: Để giải quyết các tình huống bất ngờ. Chẳng hạn, trạm đó nhận được tín hiệu cho thấy đã có các trạm khác có thẻ bài. Lập tức nó phải chuyển sang trạng thái nghe (bị động, chờ dữ liệu hoặc thẻ bài). Hoặc sau khi kết thúc truyền dữ liệu, trạm phải chuyển thẻ bài tới trạm kề sau nó và tiếp tục nghe xem trạm kề sau đó có hoạt động hay đã bị hư hỏng. Nếu trạm kề sau bị hỏng thì phải tìm cách gửi các thông báo để vượt qua trạm hỏng đó, tìm trạm hoạt động để gửi thẻ bài.
- Khởi tạo vòng logic: Khi một trạm hay nhiều trạm phát hiện thấy đường truyền không hoạt động trong một khoảng thời gian vượt quá một giá trị ngưỡng (time out) cho trước - thẻ bài bị mất (có thể do mạng bị mất nguồn hoặc trạm giữ thẻ bài bị hỏng). Lúc đó trạm phát hiện sẽ gửi đi 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.

b. Phương pháp Token Ring (Vòng với thẻ bài)

Phương pháp này dựa trên nguyên lý dùng thẻ bài để cấp phát quyền truy nhập đường truyền. Thẻ bài lưu chuyển theo vòng vật lý chứ không cần thiết lập vòng logic như phương pháp trên

Thẻ bài là một đơn vị dữ liệu đặc biệt trong đó có một bít biểu diễn trạng thái sử dụng của nó (bận hoặc rỗi). Một trạm muốn truyền dữ liệu thì phải đợi đến khi nhận được một thẻ bài rỗi. Khi đó nó sẽ đổi bít trạng thái thành bận và truyền một đơn vị dữ liệu cùng với thẻ bài đi theo chiều của vòng. Giờ đây không còn thẻ bài rỗi trên vòng nữa, do đó các trạm có dữ liệu cần truyền buộc phải đợi. Dữ liệu đến trạm đích sẽ được sao lại, sau đó cùng với thẻ bài đi tiếp cho đến khi quay về trạm nguồn. Trạm nguồn sẽ xoá bỏ dữ liệu, đổi bít trạng thái thành rỗi cho lưu chuyển tiếp trên vòng để các trạm khác có thể nhận được quyền truyền dữ liệu.

Hình 41 - Hoạt động của phương pháp Token Ring

Sự quay về trạm nguồn của dữ liệu và thẻ bài nhằm tạo một cơ chế nhận từ nhiên: trạm đích có thể gửi vào đơn vị dữ liệu các thông tin về kết quả tiếp nhận dữ liệu của mình.

- Trạm đích không tồn tại hoặc không hoạt động.
- *Trạm đích tồn tại nhưng dữ liệu không sao chép được.*
- *Dữ liệu đã được tiếp nhận .*

Phương pháp này cần phải giải quyết hai vấn đề có thể gây phá vỡ hệ thống:

- *Mất thẻ bài: trên vòng không còn thẻ bài lưu chuyển nữa*
- *Một thẻ bài bận lưu chuyển không dừng trên vòng*

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

Đối với vấn đề thẻ bài bận lưu chuyển không dừng, trạm monitor sử dụng một bit trên thẻ bài (gọi là monitor bit) để đánh dấu đặt giá trị 1 khi gặp thẻ bài bận đi qua nó. Nếu nó gặp lại một thẻ bài bận với bít 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 thành rỗi và chuyển tiếp trên vòng. Các trạm còn lại trên trạm sẽ có vai trò bị động: chúng theo dõi phát hiện tình trạng sự cố của trạm monitor chủ động và thay thế vai trò đó. Cần có một giải thuật để chọn trạm thay thế cho trạm monitor hỏng.

3.3 THIẾT KẾ MẠNG CỤC BỘ

3.3.1 Các yêu cầu khi thiết kế

Để xây dựng nên một hệ thống mạng cục bộ hoạt động tốt ta phải đảm bảo các yêu cầu sau:

- ***Đảm bảo độ tin cậy của hệ thống mạng.***

Phải có các phương án xử lý sự cố, lỗi ở máy chủ hoặc máy trạm hay các thiết bị khác để đảm bảo thông tin trong mạng luôn được thông suốt không bị gián đoạn.

- ***Dễ bảo hành và sửa chữa.***

Khi thiết kế mạng ta phải thiết kế sao cho: nếu như trong quá trình vận hành mạng mà hệ thống có sự cố thì dễ dàng và nhanh chóng phát hiện ra nơi có sự cố để có biện pháp khắc

phục kịp thời. Thiết kế hệ thống sao cho có thể phân loại, cô lập hoặc cắt bỏ từng phần của hệ thống mà không ảnh hưởng tới sự hoạt động của hệ thống.

- ***Dễ mở rộng phát triển và nâng cấp.***

Khi thiết kế phải tính đến khả năng xử lý thông tin ở hiện tại cũng như nhu cầu phát triển trong tương lai.

- Có thể mở rộng bằng cách thêm số máy trạm.
- Có thể nâng cấp thiết bị bằng cách mua thêm thiết bị mới mà không phải bỏ các thiết bị cũ đã dùng trước đó.
- Có thể thay đổi hoặc nâng cấp hệ điều hành mà không làm hư hỏng hoặc mất dữ liệu.
- Có thể làm tăng tính xử lý dữ liệu của hệ thống bằng cách nâng cấp thiết bị và phần mềm để có thể đáp ứng nhu cầu của hệ thống. Do đó khi thiết kế ta nên tìm các thiết bị cho mạng và cài đặt các phần mềm sao cho dễ sử dụng và phổ biến nhất.

- ***An toàn và bảo mật dữ liệu .***

An toàn và bảo mật dữ liệu là yếu tố rất quan trọng khi xây dựng một hệ thống mạng cục bộ, do vậy phải thiết kế sao cho tài nguyên, dữ liệu trên mạng phải được an toàn và bảo mật ở mức cao nhất.

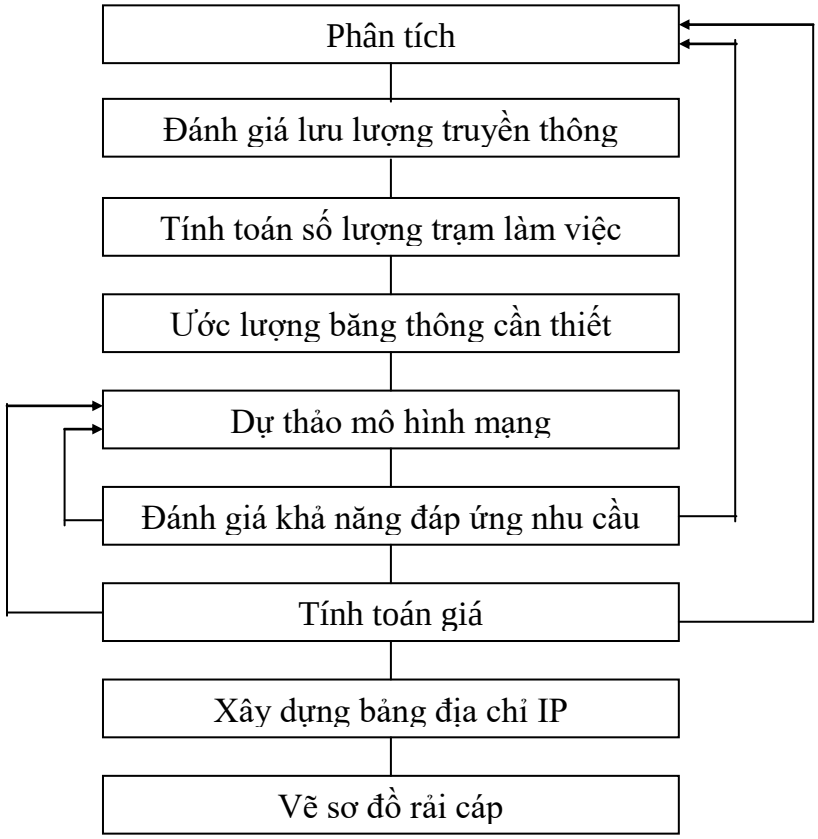
- ***Tính kinh tế.***

Tính kinh tế là một tiêu điểm để đánh giá việc xây dựng một hệ thống mạng cục bộ. Vì vậy khi thiết kế hệ thống mạng chúng ta phải tính toán và quan tâm đến việc lựa chọn sơ đồ, lựa chọn thiết bị để có thể giảm tối đa chi phí mà vẫn đáp ứng được những yêu cầu của hệ thống.

3.3.2 Quy trình thiết kế

Thiết kế mạng là công việc dựa trên sự phân tích đánh giá khối lượng thông tin phải lý và giao tiếp trong hệ thống để xác định mô hình mạng, phần mềm và tập hợp các máy tính, thiết bị, vật liệu xây dựng

Các bước và trình tự thực hiện trong công tác thiết kế mạng được minh hoạ trong sơ đồ sau:



Hình 42 – Sơ đồ qui trình thiết kế mạng

Bước 1: Phân tích

- Mạng máy tính là cơ sở hạ tầng của hệ thống thông tin. Vì vậy trước khi thiết kế mạng phải phân tích hệ thống thông tin.
- Mục đích của phân tích là để hiểu được nhu cầu về mạng của hệ thống, của người dùng .
- Để thực hiện được mục đích đó phải phân tích tất cả các chức năng nghiệp vụ, giao dịch của hệ thống.
- Trong giai đoạn phân tích cần tránh những định kiến chủ quan về khả năng, cách thức sử dụng mạng cũng như những nghiệp vụ nào sẽ thực hiện trên máy tính, trên mạng hay những nghiệp vụ nào không thể thực hiện trên máy tính, trên mạng.

  Như vậy, giai đoạn này chúng ta cần phải xác định các số liệu sau :

  - **Tra** (Traffic) : số lượng các giao dịch phải xử lí trong một ngày
  - **CBH** (Concertration Ratio to Busy Hours) :độ tập trung truyền thông cao điểm = số giờ truyền cao điểm/tổng số giờ truyền trong ngày
  - **ML** (Message length Incoming/Outming) : độ dài đoạn tin truyền đi và gửi về
  - **CPT** (Center Processing Time) : thời gian xử lí đáp ứng yêu cầu tại server từ các client

- **RT** (Response Time) : đòi hỏi thời gian chờ đợi lớn nhất cho việc xử lí một giao tác
- **THT** (Terminal Hold Time) : tổng thời gian mà một giao dịch chiếm giữ một terminal
- **LHT** (Line Hold Time) : tổng thời gian chiếm giữ đường truyền = thời gian gửi + thời gian nhận + thời gian xử lí
- Số ngày làm việc trong một tháng
- Kiểu thủ tục truyền thông được sử dụng.

Bước 2: Đánh giá lưu lượng truyền

- Việc đánh giá lưu lượng truyền thông dựa trên các nguồn thông tin chủ yếu:
  - Lưu lượng truyền thông đòi hỏi bởi mỗi giao dịch.
  - Giờ cao điểm của các giao dịch.
  - Sự gia tăng dung lượng truyền thông trong tương lai.
- Để đơn giản, có thể đưa ra các giả thuyết định lượng ở bước cơ sở để tiến hành tính toán được ở bước sau. Cũng có thể giải thiết rằng mỗi giao dịch cũng sử dụng một khối lượng như nhau về dữ liệu và có lưu lượng truyền thông giống nhau.
- Để xác định giờ cao điểm và tính toán dung lượng truyền thông trong giờ cao điểm cần thống kê dung lượng truyền thông trong từng giờ làm việc hàng ngày. Giờ cao điểm là giờ có dung lượng truyền thông cao nhất trong ngày.
- Tỷ số giữa dung lượng truyền thông trong giờ cao điểm trên dung lượng truyền thông hàng ngày được gọi là độ tập trung truyền thông cao điểm.
- Sự gia tăng dung lượng truyền thông trong tương lai có thể đến vì hai lý do:
  - Sự tiện lợi của hệ thống sau khi nó được hoàn thành làm người sử dụng nó thường xuyên hơn
  - Nhu cầu mở rộng hệ thống do sự mở rộng hoạt động của cơ quan trong tương lai.

Công thức tính dung lượng truyền thông trong giờ cao điểm:

$$\mathbf{T_n = DT. (TR / 100) . (1 + a) . (1 + b)^n}$$

Trong đó:

n: Số năm kể từ thời điểm tính hiện tại

T_n : Dung lượng truyền thông hàng ngày tại thời điểm hiện tại

TR: Độ tập trung truyền thông cao điểm

a: Tỷ lệ gia tăng truyền thông vì sự tiện lợi.

b: Tỷ lệ gia tăng truyền thông hàng năm

Bước 3: Tính toán số trạm làm việc

Có hai phương pháp tính toán số trạm làm việc cần thiết

- Tính số trạm làm việc cho mỗi người
- Tính số trạm làm việc cần thiết để hoàn thành tất cả các giao dịch trong các hoàn cảnh:
  - Số trạm làm việc cần thiết để hoàn thành tất cả các giao dịch trong giờ cao điểm
  - Số trạm làm việc cần thiết để hoàn thành tất cả các giao dịch hàng ngày

Chú ý rằng, các điều kiện sau phải thoả mãn:

- *Số các trạm làm việc >= DT . TR . T / 60*
- *Số các trạm làm việc >= DT . T / W*

Trong đó T là thời gian tính bằng phút để hoàn thành một giao dịch. W là thời gian tính bằng phút của một ngày làm việc.

Công thức tính toán số trạm quản lí (tối thiểu)

$T \geq (THT \,.\, BHT) / (3600 \,.\, TUR)$

$BHT = Traffic \,.\, CBH$

Trong đó: BHT – Busy Hours Traffic là truyền thông giờ cao điểm

TUR = 0.7 ÷ 0.8 (TUR - Terminal Utilization Rate) : Tỉ lệ sử dụng hữu ích trạm làm việc

Bước 4: Ước lượng băng thông cần thiết

Việc ước lượng băng thông cần thiết cần căn cứ vào các thông tin sau:

- Hiệu quả truyền thồn (H): được tính bằng tỷ số giữa kích thước dữ liệu (byte) trên tổng số byte của một khung dữ liệu.
- Tỷ lệ hữu ích của đường truyền (R): được khuyến cáo cho hai cơ chế truy nhập truyền thông là: CSMA/CD: 0.2, Token Ring: 0.4
- Băng thông đòi hỏi phải thoả mãn điều kiện là lớn hơn hoặc bằng: Dung lượng truyền thông (tính theo byte/giờ) . 8 (3600 . H . R)
- *Tốc độ đường truyền (Speed Line)*:

$V \geq$ (ML .numbers of bits/byte) / ((RT - CPT) . LUR . TE . (1 - Re))

Trong đó :

LUR (Line Utilization Rate) : Tỉ lệ sử dụng hữu ích đường truyền

TE (Tramsmission Efficidency) : Hiệu suất truyền thông

Re (Retransmission Rate) : Tỉ lệ lỗi đường truyền buộc phải truyền lại thông tin (HDCL = 0.05 và ≠ là 0.15)

TE = 0.9 với thủ tục truyền thông HDCL và = 0.8 với thủ tục truyền thông cơ bản khác. (Với TE = tổng số byte dữ liệu/tổng số byte của gói tin)

- Số lượng đường truyền :

N = (LHT . BHT) / (3600 . LUR)

LHT = [f(ML) . numbers of bit/byte] / [Speed Line . TE . (1 - Re)] + t

Trong đó:

f(ML) = incoming time + outcoming time với 'half duplex'

max(incoming time, out coming time) với 'full duplex'

t = Ct với 'half duplex'

0 với 'full duplex'

Bước 5: Dự thảo mô hình mạng

Bước này là bước thực hiện các công việc:

- Khảo sát vị trí đặt các trạm làm việc, vị trí đi đường cáp mạng, ước tính độ dài, vị trí có thể đặt các repeater...
- Lựa chọn công nghệ mạng: có nhiều công nghệ mạng (FDDI, Token Ring, Ethernet...) nhưng trong bài thực hành này ta sẽ lựa chọn công nghệ Ethernet.
- *Layer 1 LAN topology*:
  - Chọn cáp: thường dùng cáp CAT5 UTP
  - Chọn topo của mạng: thường chọn topo hình sao mở rộng

- Chọn chuẩn Ethernet: thông dụng nhất là 10Base-T và 100Base-TX (còn gọi là Fast Ethernet). Nếu có điều kiện nên chọn 100Base-TX dùng cho toàn bộ mạng. Nếu không thì dùng Fast Ethernet để kết nối điểm điều khiển trung tâm của mạng đến các phân khu khác.
- Ngoài ra còn dùng các hub, transceiver cùng với các thiết bị Layer 1 khác như plug, patch panel, jack.
- Kết thúc bước này ta thu được topo logic và topo vật lý của mạng.

➢ *Layer 2 LAN topology*: Bổ sung các switch để giảm phạm vi vùng xung đột và tắc nghẽn. Trong tương lai chúng ta có thể sẽ thay thế các hub bằng các switch cũng như thay thế các thiết bị của Layer 1 bằng các thiết bị thông minh hơn của tầng Layer 2.

➢ *Layer 3 LAN topology:*

- Bổ sung các router vào bản thiết kế. Ta có thể dùng router để xây dựng các liên mạng (các LAN lớn hơn nữa, các mạng WAN, mạng của các mạng), hoặc để thiết đặt một kiến trúc logic cho mạng mà ta đang xây dựng, hoặc để phân đoạn (router chia tách cả các miền xung đột và các miền quảng bá, điều này hub, switch và bridge không làm được).
- Xác định vị trí đặt các file server, database, các tài nguyên để chia sẻ trên mạng, đường link kết nối từ LAN vào WAN và vào Internet.
- Cuối cùng lập tài liệu về topo logic và vật lý của mạng đang thiết kế. Ghi rõ cả những ý tưởng phát sinh, các vấn đề cần giải quyết, các chú ý hình thành trong quá trình ra quyết định.
- Tính toán diện tích mặt bằng lắp đặt LAN: Diện tích phải phù hợp với qui mô của mạng LAN và các kiểu thiết bị dùng trong mạng. Một mạng LAN nhỏ chỉ cần diện tích cỡ 1 cabin, trong khi mạng LAN lớn hơn có thể yêu cầu toàn bộ căn phòng và hơn nữa. Nhiệt độ thích hợp của không gian LAN hoạt động là xấp xỉ 21 độ C. Không được có nước hoặc ống dẫn hơi nước đi qua ngoại trừ hệ thống bình phun dùng trong cứu hộ. Độ ẩm không khí khoảng 30-40%, yêu cầu này có liên quan đến sự ăn mòn dây cáp mạng (như UTP hay STP). Độ ăn mòn có ảnh hưởng đến hiệu quả chức năng của mạng. Sàn nhà phải chịu được lực tải do sức nặng của máy móc và các thiết bị khác, cả lực rung sinh ra khi toàn bộ chúng hoạt động.

Bước 6: Đánh giá khả năng đáp ứng nhu cầu

➢ Mục đích của bước này là đánh giá xem dự thảo thực hiện trong bước 5 có đáp ứng được nhu cầu của người sử dụng hay không. Có thể phải quay trở lại bước 5 để thực hiện bổ sung sửa đổi, thậm chí phải xây dựng lại bản dự thảo mới. Đôi khi cũng phải đối chiếu, xem xét lại các chi tiết ở bước1.

- Có nhiều khía cạnh khác nhau cần đánh giá về khả năng thực hiện và đáp ứng nhu cầu của một mạng, nhưng điều quan trọng trước tiên là thời gian trễ của mạng (delay time) cũng như thời gian hồi đáp của mạng (response time) vì thời gian trễ dài cũng có nghĩa là thời gian hồi đáp lớn
- Để tính toán được delay time có hai phương pháp:

  – *Thực nghiệm*: Xây dựng một mạng thí nghiệm có cấu hình tương tự như dự thảo. Đây là việc đòi hỏi có cơ sở vật chất, nhiều công sức và tỷ mỉ.
  – *Mô phỏng*: Dùng các công cụ mô phỏng để tính toán. Dùng phương pháp này buộc phải có công cụ mô phỏng, mà các công cụ mô phỏng đều rất đắt tiền

- Công thức tính thời gian hồi đáp (Response Time Check)
  - Actual Line Utilization Rate: R = (LHT . BHT) / (3600 . number of line)
  - Wait Time: W = [R / 2.(1 - R)] * LHT
  - Actual Response Time: RT = W + Transmission Time + CPT

Trong đó Transmission Time = [8 . (incoming + outcoming)] / [speed . Efficiency . (1 - Re)]

Bước 7: Tính toán giá

Dựa trên danh sách thiết bị mạng có từ bước 5, ở bước này nhóm thiết kế phải thực hiện các công việc:

- Khảo sát thị trường, lựa chọn sản phẩm thích hợp. Đôi khi phải quay lại thực hiện các bổ sung, sửa đổi ở bước 5 hay phải đối chiếu lại các yêu cầu đã phân tích ở bước 1.
- Bổ sung danh mục các phụ kiện cần thiết cho việc thi công
- Tính toán nhân công cần thiết để thực hiện thi công bao gồm cả nhân công quản lý điều hành.
- Lên bảng giá và tính toán tổng giá thành của tất cả các khoản mục.

Bước 8: Xây dựng bảng địa chỉ IP

- Lập bảng địa chỉ network cho mỗi subnet.
- Lập bảng địa chỉ IP cho từng trạm làm việc trong mỗi subnet.

Bước 9: Vẽ sơ đồ rải cáp

- Sơ đồ đi cáp phải được thiết kế chi tiết để hướng dẫn thi công và là tài liệu phải lưu trữ sau khi thi công.

- Cần phải xây dựng sơ đồ tỷ mỉ để đảm bảo tính thực thi, tránh tối đa các sửa đổi trong quá trình thi công.
- *Vẽ sơ đồ mạng: vẽ sơ đồ của các toà nhà và các phòng sẽ đi dây, chi tiết tới* các vị trí của mạng trong các phòng. Phải tính toán các khoảng cách từ các máy tính đến các Hub hoặc Switch và đến các mạng khác.
- Định đường đi cho cáp: có thể cài đặt dây mạng bên trong các bức tường hay dọc theo các góc tường.
- Đặt nhãn cho các cáp mạng: Các mạng không phải luôn ở trạng thái tĩnh, các thiết bị nối với mạng và các kết nối bị thay đổi khi cần thiết và sự cố định của mạng bị thay đổi. Đặt nhãn cho cáp mạng để khi bản đồ mạng không có giá trị thì vẫn có thể truy tìm và hiểu cấu trúc đi dây.

Trong quá trình thi công nếu có lý do bắt buộc phải sửa đổi đường đi cáp thì phải cập nhật lại bản vẽ để sau khi thi công xong, bản vẽ thể hiện chính xác sơ đồ đi cáp mạng.

BÀI TẬP CHƯƠNG III

Bài 1: Máy chủ nào trong các máy chủ sau phải sử dụng Router để liên lạc với máy 191.24.174.12 biết SubnetMask của máy này là 255.255.192.0? Giải thích.

A.191.24.153.35 B.191.24.169.2 C.191.24.158.3 D.191.24.147.86

Bài 2: Địa chỉ nào được SWITCH sử dụng khi quyết định gửi data sang cổng (port) nào ?

A. Soure MAC address B. Destination MAC address

C. Network address D. Subnet work address.

Bài 3: Điều gì xảy ra với dữ liệu khi có va chạm (collision) ?

A. HUB/SWITCH sẽ gửi lại dữ liệu B. Dữ liệu sẽ bị phá hỏng từng bit.

C. Dữ liệu sẽ được xây dựng lại từ máy nhận. D. Router sẽ hủy dữ liệu.

Bài 4: Các dịch vụ quay số tương tự (Dial-up) sử dụng thiết bị nào để chuyển đổi tín hiệu số sang tín hiệu tương tự?

A. Repeater B. Modem

C. Router D. NIC

Bài 5: Hub là thiết bị hoạt động ở tầng nào của mô hình OSI:

A. Tầng Vật lý B. Tầng Data Link

C. Tầng Transport D. Tầng Network

Bài 6: Một Hub tốc độ 100Mbps có 12 cổng thì tốc độ của mỗi cổng sẽ là:

A. Tối đa 100Mbps khi chỉ có một máy tính cắm vào Hub

B. Tối đa 100Mbps khi có 12 máy tính cắm vào Hub

C. Tối thiểu 8.3Mbps khi có 12 máy tính cắm vào Hub

D. Tối thiểu 100Mbps khi chỉ có một máy tính cắm vào Hub

Bài 7: Switch là thiết bị hoạt động ở lớp nào của mô hình OSI:

A. Lớp 1 B. Lớp 2

C. Lớp 3 D. Lớp 4

Bài 8: Topo thường dùng hiện nay trong các mạng LAN:

A. Ethernet bus B. Bus

C. Token Ring D. Token bus

Bài 9: Thiết bị mạng nào dùng để nối các mạng và kiểm soát được broadcast?

A. Hub B. Bridge

C. Ethernet switch D. Router

CHƯƠNG IV – CÁC DỊCH VỤ MẠNG DIỆN RỘNG

Mục tiêu

Hiện nay trên thế giới có nhiều dịch vụ dành cho việc chuyển thông tin từ khu vực này sang khu vực khác nhằm liên kết các mạng LAN của các khu vực khác nhau lại. Để có được những liên kết như vậy người ta thường sử dụng các dịch vụ của các mạng diện rộng. Hiện nay trong khi giao thức truyền thông cơ bản của LAN là Ethernet, Token Ring thì giao thức dùng để tương nối các LAN thông thường dựa trên chuẩn TCP/IP. Ngày nay khi các dạng kết nối có xu hướng ngày càng đa dạng và phân tán cho nên các mạng WAN đang thiên về truyền theo đơn vị tập tin thay vì truyền một lần xử lý.

Có nhiều cách phân loại mạng diện rộng, ở đây nếu phân loại theo phương pháp truyền thông tin thì có thể chia thành 3 loại mạng như sau:

a. Mạng chuyển mạch (Circuit Swiching Network)

b. Mạng thuê bao (Leased lines Network)

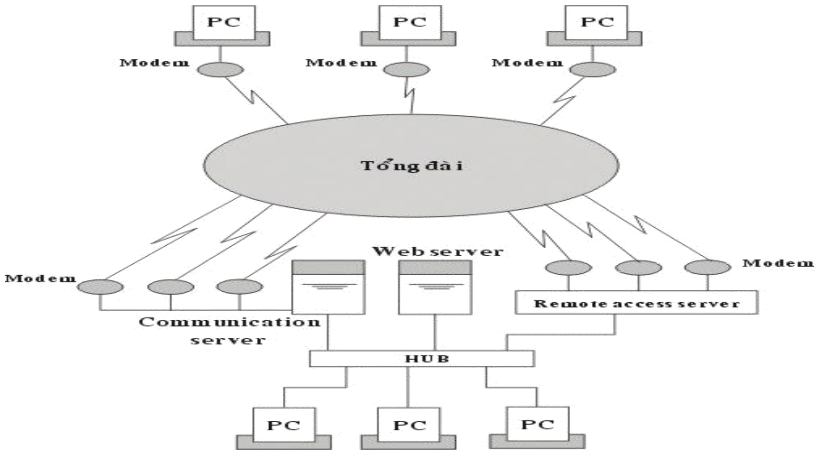
c. Mạng chuyển gói tin (Packet Switching Network)

d. Mạng tốc độ cao.

e. Mạng NGN.

4.1 MẠNG CHUYỂN MẠCH (Circuit Swiching Network)

Để thực hiện được việc liên kết giữa hai điểm nút, một đường nối giữa điểm nút này và điêm nút kia được thiết lập trong mạng thể hiện dưới dạng cuộc gọi thông qua các thiết bị chuyển mạch.



Hình 43 - Mô hình mạng chuyển mạch

Một ví dụ của mạng chuyển mạch là hoạt động của mạng điện thoại, các thuê bao khi biết số của nhau có thể gọi cho nhau và có một đường nối vật lý tạm thời được thiết lập giữa hai thuê bao.

Với mô hình này mọi đường đều có thể một đường bất kỳ khác, thông qua những đường nối và các thiết bị chuyên dùng người ta có thể liên kết một đường tạm thời từ nơi gửi tới nơi nhận một đường nối vật lý, đường nối trên duy trì trong suốt phiên làm việc và chỉ giải phóng sau khi phiên làm việc kết thúc. Để thực hiện một phiên làm việc cần có các thủ tục đầy đủ cho việc thiết lập liên kết trong đó có việc thông báo cho mạng biết địa chỉ của nút nhận.

Hiện nay có 2 loại mạng chuyển mạch là chuyển mạch tương tự (analog) và chuyển mạch số (digital)

- *Chuyển mạch tương tự (Analog):* Việc chuyển dữ liệu qua mạng chuyển mạch tương tự được thực hiện qua mạng điện thoại. Các trạm sử dụng một thiết bị có tên là modem, thiết bị này sẽ chuyển các tín hiệu số từ máy tính sao tín hiệu tuần tự có trể truyền đi trên mạng điện thoại và ngược lại.

Hình 44 - Mô hình chuyển mạch tương tự

Khi sử dụng đường truyền điện thoại để truyền số liệu thì các chuẩn của modem và các tính chất của nó sẽ quyết định tốc độ của đường truyền. Cùng với các kỹ thuật chuyển đổi tín hiệu các tính năng mới như nén tín hiệu cho phép nâng tốc độ truyền dữ liệu lên rất cao.

Các kỹ thuật nén thường dùng là MNP Class 5 và V42 bis, MNP Class 5 cho phép nén với tỷ lệ 1.5:1 và V42 bis nén với tỷ lệ 2:1. Tuy nhiên trên thực tế tỷ lệ nén có thể thay đổi dựa vào dạng dữ liệu được truyền.

- *Chuyển mạch số (Digital):* Đường truyền chuyển mạch số lần đầu tiên được AT&T thiệu vào cuối 1980 khi AT&T giới thiệu mạng chuyển mạch số Acnet với đường truyền 56 kbs. Việc sử dụng đường chuyển mạch số cũng đòi hỏi sử dụng thiết bị phục vụ truyền dữ liệu số (Data Service Unit - DSU) vào vị trí modem trong chuyển mạch tương tự. Thiết bị phục vụ truyền dữ liệu số có nhiệm vụ chuyển các tín hiệu số đơn chiều (unipolar) từ máy tính ra thành tín hiệu số hai chiều (bipolar) để truyền trên đường truyền.

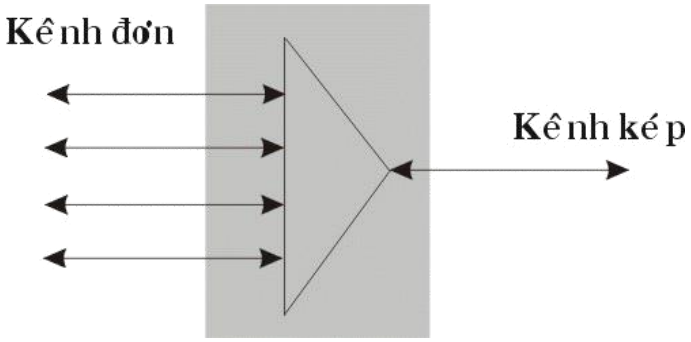
Hình 45 - Mô hình chuyển mạch số

Mạng chuyển mạch số cho phép người sử dụng nâng cao tốc độ truyền (ở đây do khác biệt giữa kỹ thuật truyền số và kỹ thuật truyền tương tự nên hiệu năng của truyền mạch số cao hơn nhiều so với truyền tương tự cho dù cùng tốc độ), độ an toàn.

Vào năm 1991 AT&T giới thiệu mạng chuyển mạch số có tốc độ 384 Kbps. Người ta có thể dùng mạng chuyển mạch số để tạo các liên kết giữa các mạng LAN và làm các đường truyền dự phòng.

4.2 MẠNG THUÊ BAO (Leased line Network)

Với kỹ thuật chuyển mạch giữa các nút của mạng (tương tự hoặc số) có một số lượng lớn đường dây truyền dữ liệu, với mỗi đường dây trong một thời điểm chỉ có nhiều nhất một phiên giao dịch, khi số lượng các trạm sử dụng tăng cao người ta nhận thấy việc sử dụng mạng chuyển mạch trở nên không kinh tế. Để giảm bớt số lượng các đường dây kết nối giữa các nút mạng người ta đưa ra một kỹ thuật gọi là ghép kênh.



Hình 46 - Mô hình ghép kênh

Mô hình đó được mô tả như sau: tại một nút người ta tập hợp các tín hiệu trên của nhiều người sử dụng ghép lại để truyền trên một kênh nối duy nhất đến các nút khác, tại nút cuối người ta phân kênh ghép ra thành các kênh riêng biệt và truyền tới các người nhận.

Có hai phương thức ghép kênh chính là ghép kênh theo tần số và ghép kênh theo thời gian, hai phương thức này tương ứng với mạng thuê bao tuần tự và mạng thuê bao kỹ thuật số. trong thời gian hiện nay mạng thuê bao kỹ thuật số sử dụng kỹ thuật ghép kênh theo thời

gian với đường truyền T đang được sử dụng ngày một rộng rãi và dần dần thay thế mạng thuê bao tuần tự.

4.2.1 Phương thức ghép kênh theo tần số

Để sử dụng phương thức ghép kênh theo tần số giữa các nút của mạng được liên kết bởi đường truyền băng tần rộng. Băng tần này được chia thành nhiều kênh con được phân biệt bởi tần số khác nhau. Khi truyền dữ liệu, mỗi kênh truyền từ người sử dụng đến nút sẽ được chuyển thành một kênh con với tần số xác định và được truyền thông qua bộ ghép kênh đến nút cuối và tại đây nó được tách ra thành kênh riêng biệt để truyền tới người nhận. Theo các chuẩn của CCITT có các phương thức ghép kênh cho phép ghép 12, 60, 300 kênh đơn.

Người ta có thể dùng đường thuê bao tuần tự (Analog) nối giữa máy của người sử dụng tới nút mạng thuê bao gần nhất. Khi máy của người sử dụng gửi dữ liệu thì kênh dữ liệu được ghép với các kênh khác và truyền trên đường truyền tới nút đích và được phân ra thành kênh riêng biệt trước khi gửi tới máy của người sử dụng. Đường nối giữa máy trạm của người sử dụng tới nút mạng thuê bao cũng giống như mạng chuyển mạch tuần tự sử dụng đường dây điện thoại với các kỹ thuật chuyển đổi tín hiệu như V22, V22 bis, V32, V32 bis, các kỹ thuật nén V42 bis, MNP class 5.

4.2.2 Phương thức ghép kênh theo thời gian

Khác với phương thức ghép kênh theo tần số, phương thức ghép kênh theo thời gian chia một chu kỳ thời gian hoạt động của đường truyền trục thành nhiều khoảng nhỏ và mỗi kênh tuyền dữ liệu được một khoảng. Sau khi ghép kênh lại thành một kênh chung dữ liệu được truyền đi tương tự như phương thức ghép kênh theo tần số. Người ta dùng đường thuê bao là đường truyền kỹ thuật số nối giữa máy của người sử dụng tới nút mạng thuê bao gần nhất.

Hiện nay người ta có các đường truyền thuê bao như sau :

Đường T1 với tốc độ 1.544 Mbps nó bao gồm 24 kênh vớp tốc độ 64 kbps và 8000 bits điều khiển trong 1 giây.

4.3 MẠNG CHUYỂN GÓI TIN (Packet Switching NetWork)

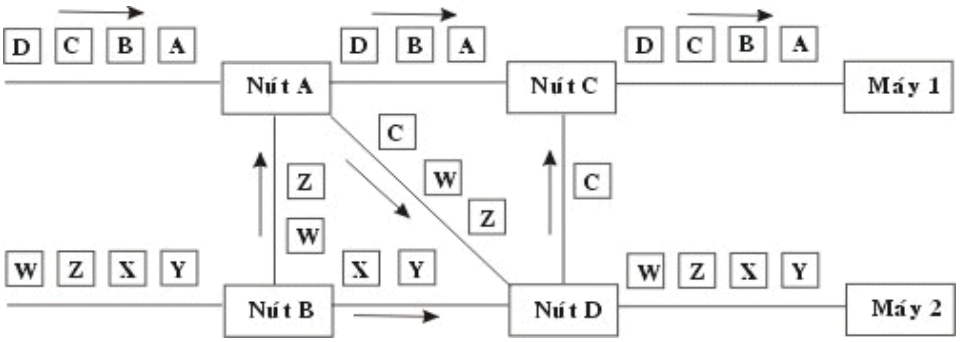
Mạng chuyển mạch gói hoạt động theo nguyên tắc sau : Khi một trạm trên mạng cần gửi dữ liệu nó cần phải đóng dữ liệu thành từng gói tin, các gói tin đó được đi trên mạng từ nút này tới nút khác tới khi đến được đích. Do việc sử dụng kỹ thuật trên nên khi một trạm

không gửi tin thì mọi tài nguyên của mạng sẽ dành cho các trạm khác, do vậy mạng tiết kiệm được các tài nguyên và có thể sử dụng chúng một cách tốt nhất.

Người ta chia các phương thức chuyển mạch gói ra làm 2 phương thức:

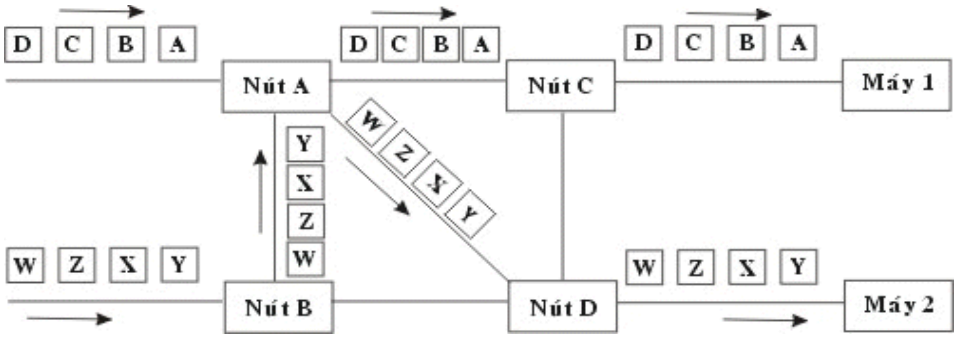
- Phương thức chuyển mạch gói theo sơ đồ rời rạc.
- Phương thức chuyển mạch gói theo đường đi xác định.

Với phương thức chuyển mạch gói theo sơ đồ rời rạc: các gói tin được chuyển đi trên mạng một cách độc lập, mỗi gói tin đều có mang địa chỉ nơ i gửi và nơi nhận. Mỗi nút trong mạng khi tiếp nhận gói tin sẽ quyết định xenm đường đi của gói tin phụ thuộc vào thuật toán tìm đường tại nút và những thông tin về mạng mà nút đó có. Việc truyền theo phương thức này cho ta sự mềm dẻo nhất định do đường đi với mỗi gói tin trở nên mềm dẻo tuy nhiên điều này yêu cầu một số lượng tính toán rất lớn tại mỗi nút nên hiện nay phần lớn các mạng chuyển sang dùng phương chuyển mạch gói theo đường đi xác định.



Hình 47 - Ví dụ phương thức sơ đồ rời rạc.

Phương thức chuyển mạch gói theo đường đi xác định: Trước khi truyền dữ liệu một đường đi (hay còn gọi là đường đi ảo) được thiết lập giữa trạm gửi và trạm nhận thông qua các nút của mạng. Đường đi trên mang số hiệu phân biệt với các đường đi khác, sau đó các gói tin được gửi đi theo đường đã thiết lập để tới đích, các gói tin mang số hiệu củ đường ảo để có thể được nhận biết khi qua các nút. Điều này khiến cho việc tính toán đường đi cho phiên liên lạc chỉ cần thực hiện một lần.



Hình 48 - Ví dụ phương thức đường đi xác định

4.3.1 Mạng X25

Được CCITT công bố lần đầu tiên vào 1970 lúc lĩnh vực viễn thông lần đầu tiên tham gia vào thế giới truyền dữ liệu với các đặc tính:

- X25 cung cấp quy trình kiểm soát luồng giữa các đầu cuối đem lại chất lương đường truyền cao cho dù chất lương đương dây truyền không cao.
- X25 được thiết kế cho cả truyền thông chuyển mạch lẫn truyền thông kiểu điểm nối điểm.
- Được quan tâm và tham gia nhanh chóng trên toàn cầu.

Trong X25 có chức năng dồn kênh (multiplexing) đối với liên kết logic (virtual circuits) chỉ làm nhiệm vụ kiểm soát lỗi cho các frame đi qua. Điều này làm tăng độ phức tạp trong việc phối hợp các thủ tục giữa hai tầng kề nhau, dẫn đến thông lượng bị hạn chế do tổng phí xử lý mỗi gói tin tăng lên. X25 kiểm tra lỗi tại mỗi nút trước khi truyền tiếp, điều này làm cho đường truyền chó chất lượng rất cao gần như phi lỗi. Tuy nhiên do vậy khối lượng tích toán tại mỗi nút khá lớn, đối với những đường truyền của những năm 1970 thì điều đó là cần thiết nhưng hiện nay khi kỹ thuật truyền dẫn đã đạt được những tiến bộ rất cao thì việc đó trở nên lãng phí

4.3.2 Mạng Frame Relay

Mỗi gói tin trong mạng gọi là Frame, do vậy mạng gọi là Frame relay. Đặc điểm khác biệt giữa mạng Frame Relay và mạng X25 mạng Frame Relay là chỉ kiểm tra lỗi tại hai trạm gửi và trạm nhận còn trong quá trình chuyển vận qua các nút trung gian gói tin sẽ không được kiểm lỗi nữa. Do vậy thời gian xử lý trên mỗi nút nhanh hơn, tuy nhiên khi có lỗi thì gói tin phải được phát lại từ trạm đầu. Với độ an toàn cao của đường truyền hiện nay thì chi phí việc phát lại đó chỉ chiếm một tỷ lệ nhỏ nếu so với khối lượng tính toán được giảm đi tại các nút nên mạng Frame Relay tiết kiệm được tài nguyên của mạng hơn so với mạng X25.

Frame relay không chỉ là một kỹ thuật mà còn là thể hiện một phương pháp tổ chức mới. Với nguyên lý là truyền mạch gói nhưng các thao tác kiểm soát giữa các đầu cuối giảm đáng kể Kỹ thuật Frame Relay cho phép thông luợng tối đa đạt tới 2Mbps và hiện nay nó đang cung cấp các giải pháp để tương nối các mạng cục bộ LAN trong một kiến trúc xương sống tạo nên môi trường cho ứng dụng multimedia.

4.3.3 Mạng ATM (Cell relay)

Hiện nay kỹ thuật Cell Relay dựa trên phương thức truyền thông không đồng bộ (ATM) có thể cho phép thông lương hàng trăm Mbps. Đơn vị dữ liệu dùng trong ATM được gọi là tế bào (cell). các tế bào trong ATM có độ dài cố định là 53 bytes, trong đó 5 bytes dành cho phần chứa thông tin điều khiển (cell header) và 48 bytes chứa dữ liệu của tầng trên.

Trong kỹ thuật ATM, các tế bào chứa các kiểu dữ liệu khác nhau được ghép kênh tới một đường dẫn chung được gọi là đường dẫn ảo (virtual path). Trong đường dẫn ảo đó có thể gồm nhiều kênh ảo (virtual chanell) khác nhau, mỗi kênh ảo được sử dụng bởi một ứng dung nào đó tại một thời điểm.

ATM đã kết hợp những đặc tính tốt nhất của dạng chuyển mạch liên tục và dạng chuyển mạch gói, nó có thể kết hợp dải thông linh hoạt và khả năng chuyển tiếp cao tốc và có khả năng quản lý đồng thời dữ liệu số, tiếng nói, hình ành và multimedia tương tác.

Mục tiêu của kỹ thuật ATM là nhằm cung cấp một mạng dồn kênh, và chuyển mạch tốc độ cao, độ trễ nhỏ dáp ứng cho các dạng truyền thông đa phương tiện (multimedia)

Chuyển mạch cell cần thiết cho việc cung cấp các kết nối đòi hỏi băng thông cao, tình trạng tắt nghẽn thấp, hổ trợ cho lớp dịch vụ tích hợp lưu thông dữ liệu âm thanh hình ảnh. Đặc tính tốc độ cao là đặc tính nổi bật nhất của ATM.

ATM sử dụng cơ cấu chuyển mạch đặc biệt: ma trận nhị phân các thành tố chuyển mạch (a matrix of binary switching elements) để vận hành lưu thông. Khả năng vô hướng (scalability) là một đặc tính của cơ cấu chuyển mạch ATM. Đặc tính này tương phản trực tiếp với những gì diễn ra khi các trạm cuối được thêm vào một thiết bị liên mạng như router. Các router có năng suất tổng cố định được chia cho các trạm cuối có kết nối với chúng. Khi số lượng trạm cuối gia tăng, năng suất của router tương thích cho trạm cuối thu nhỏ lại. Khi cơ cấu ATM mở rộng, mỗi thiết bị thu trạm cuối, bằng con đường của chính nó đi qua bộ chuyển mạch bằng cách cho mỗi trạm cuối băng thông chỉ định. Băng thông rộng được chỉ định của ATM với đặc tính có thể xác nhận khiến nó trở thành một kỹ thuật tuyệt hảo dùng cho bất kỳ nơi nào trong mạng cục bộ của doanh nghiệp.

Như tên gọi của nó chỉ rõ, kỹ thuật ATM sử dụng phương pháp truyền không đồng bộ (asynchronouns) các tề bào từ nguồn tới đích của chúng. Trong khi đó, ở tầng vật lý người ta có thể sử dụng các kỹ thuật truyền thông đồng bộ như SDH (hoặc SONET).

Nhận thức được vị trí chưa thể thay thế được (ít nhất cho đến những năm đầu của thế kỷ 21) của kỹ thuật ATM, hầu hết các hãng khổng lồ về máy tính và truyền thông như IBM,

ATT, Digital, Hewlett - Packard, Cisco Systems, Cabletron, Bay Network,... đều đang quan tâm đặc biệt đến dòng sản phẩm hướng đến ATM của mình để tung ra thị trường. Có thể kể ra đây một số sản phẩm đó như DEC 900 Multiwitch, IBM 8250 hub, Cisco 7000 rounter, Cablectron, ATM module for MMAC hub.

Nhìn chung thị trường ATM sôi động do nhu cầu thực sự của các ứng dụng đa phương tiện. Sự nhập cuộc ngày một đông của các hãng sản xuất đã làm giảm đáng kể giá bán của các sản phẩm loại này, từ đó càng mở rộng thêm thị trường. Ngay ở Việt Nam, các dự án lớn về mạng tin học đều đã được thiết kế với hạ tầng chấp nhận được với công nghệ ATM trong tương lai.

4.4 MẠNG NGN

Cùng với sự phát triển của các ngành điện tử – tin học, công nghệ viễn thông trong những năm vừa qua phát triển rất mạnh mẽ cung cấp ngày càng nhiều các loại hình dịch vụ mới đa dạng, an toàn và chất lượng cao đáp ứng ngày càng tốt hơn yêu cầu của khách hàng. Trong xu hướng phát triển và hội tụ của viễn thông và tin học, cùng với sự phát triển nhanh chóng về nhu cầu của người dùng đối với những dịch vụ đa phương tiện chất lượng cao đã làm cho cơ sở hạ tầng thông tin và viễn thông đã có những thay đổi lớn về cơ bản. Những tổng đài chuyển mạch kênh truyền thống(*CS-Circuit Switching*) đã không còn có thể đáp ứng được những đòi hỏi của người dùng về những dịch vụ tốc độ cao, chính vì thế đòi hỏi cần phải có một giải pháp đáp ứng được yêu cầu đó. Xu hướng viễn thông dựa trên nền tảng chuyển mạch gói (*PS-Packet Switching*) tốc độ cao, dung lượng lớn và hội tụ được các loại dịch vụ trên cùng một hạ tầng mạng là điều tất yếu.

Mạng NGN ra đời đã đáp ứng được các yêu cầu này. Sự ra đời của NGN ngoài mặt có ý nghĩa về công nghệ và dịch vụ, nó còn đem lại cơ hội cho những công ty nhỏ, ít tên tuổi hoặc những công ty mới tham gia vào thị trường viễn thông có thể đứng vững trên thị trường mà trước đây nằm trong sự kiểm soát của một số ít nhà cung cấp lớn. Đứng trước xu hướng tự do hoá thị trường, cạnh tranh và hội nhập, việc phát triển mạng viễn thông theo cấu trúc thế hệ sau (NGN) với các công nghệ phù hợp là bước đi tất yếu của viễn thông thế giới và mạng viễn thông Việt Nam.

4.4.1 Tổng quan về mạng NGN

Mạng NGN là một cụm từ phổ biến được dùng để mô tả mạng thế hệ mới sẽ dần thay thế các mạng PSTN hiện tại trên thế giới được sử dụng để thực hiện thoại, fax, truyền số liệu trên mạng thoại...

Theo định nghĩa, NGN là thực chất là mạng quản lý trên nền mạng IP cho phép nhiều loại dịch vụ như: dịch vụ VoIP, Video phone, Voice/Video Conferencing, gửi tin nhắn, voice-mail...

Các định nghĩa của ITU về thuật ngữ NGN trong Khuyến nghị Y.2001 như sau: Next Generation Network (NGN): mạng chuyển mạch gói có thể cung cấp dịch vụ viễn thông và có thể tận dụng nhiều băng thông rộng, cho phép truyền thông với tiêu chuẩn chất lượng cho phép. Nó không giới hạn việc truy cập của người dùng tới các nhà cung cấp dịch vụ khác nhau. Nó cho phép cung cấp linh hoạt các dịch vụ phù hợp với mục đích của người dùng.

Một trong những khía cạnh quan trọng nhất của NGN là tách có chủ ý giữa nhà cung cấp truy cập với nhà cung cấp dịch vụ. Điều đó có nghĩa là các nhà cung cấp truy cập (các nhà cung cấp dịch vụ cung cấp cho khách hàng, với quyền truy cập vào các NGN) có thể khác với các nhà cung cấp dịch vụ cung cấp cho bạn các dịch vụ khác nhau, như voice, video, e-mail, báo tỉ giá cổ phiếu, hoặc các dịch vụ khác. Chúng ta nói "có thể", bởi vì các nhà cung cấp truy cập và cung cấp dịch vụ có thể là cùng một công ty. Ví dụ, như là một thuê bao đến các dịch vụ truyền hình cáp, bạn có thể chọn để sử dụng dịch vụ điện thoại từ công ty cáp. Trong trường hợp đó, nhà cung cấp truy cập và cung cấp dịch vụ điện thoại của bạn là một. Tuy nhiên, NGN sẽ loại bỏ hạn chế này tùy thuộc vào sự lựa chọn của bạn. Nếu bạn có một đường kết nối tới nhà cung cấp A (VNPT) nhưng muốn mua dịch vụ từ một công ty B(Viettel), bạn hoàn toàn có thể thực hiện nếu sử dụng ứng dụng của NGN. Điều này là không thể thực hiện được trong mạng hiện tại.

Tất nhiên, không phải tất cả các nhà cung cấp đều hài lòng với khả năng cho phép người dùng có sự lựa chọn sử dụng dịch vụ tùy ý. Tại sao? Bởi vì NGN đại diện cho một mối đe dọa thực sự đối với các mô hình kinh doanh hiện nay của các nhà cung cấp dịch vụ hiện tại. Các nhà cung cấp dịch vụ hiện tại luôn mong muốn kiểm soát tất cả twf việc truy cập đến việc sử dụng dịch vụ, ngăn chặn đối thủ cạnh tranh thâm nhập vào thị trường và cung cấp các dịch vụ cạnh tranh.

Tuy nhiên, thời gian đã thay đổi và người tiêu dùng có quyền lựa chọn các nhà cung cấp dịch vụ cung cấp cho họ các dịch vụ. Chúng ta vừa bước vào một kỷ nguyên mới mà khách hàng có quyền truy cập Internet băng thông rộng hiện nay có thể chọn nhà cung cấp dịch vụ thoại theo ý của riêng mình.

Khi mạng NGN được triển khai, người dùng có thể có một hoặc nhiều nhà cung cấp truy cập cung cấp phương thức truy cập theo một số cách, bao gồm cả cáp, DSL, Wi-Fi, WiMAX, Fiber... vào mạng NGN. Khi đã kết nối, các tùy chọn cho các nhà cung cấp dịch vụ cho thoại, video, và các dịch vụ dữ liệu hầu như không giới hạn.

Hiện nay, một số nhà cung cấp cũng đã từng bước triển khai mạng NGN để cung cấp các tiện ích của NGN tới khách như: VNPT, Viettel, EVN, SPT, Vishipel...

4.4.2 Các dịch vụ chủ yếu đang triển khai trên nền mạng NGN

a. Dành cho người sử dụng (cá nhân) có ba dịch vụ

- *Dịch vụ điện thẻ trả trước (calling card):* Đây là dịch vụ gọi điện thoại nội hạt, đường dài trong nước và quốc tế với hình thức khách hàng mua thẻ mệnh giá để sử dụng. Người sử dụng chỉ cần mua thẻ điện thoại trả tiền trước có mệnh giá từ 30.000 đồng đến 500.000 đồng là có thể thực hiện cuộc gọi từ bất kỳ máy cố định nào thông qua việc gọi vào số dịch vụ của nhà cung cấp. Cước phí sẽ được trừ trực tiếp vào tài khoản của thẻ. Với cùng một thẻ khách hàng có thể lựa chọn thoại với tốc độ 64kbps hoặc tốc độ 8 kbps có mức giá khác nhau thực hiện các cuộc gọi liên tỉnh, quốc tế hoặc sang mạng di động. Đây là một dịch vụ rất tiện lợi khi không phải đăng ký dịch vụ, sử dụng dịch vụ VoIP giá rẻ ở bất kỳ đâu, người gọi chủ động mức tiền gọi và thẻ gọi có thời hạn lâu dài.
- *Dịch vụ Call waiting Internet (báo cuộc gọi từ Internet):* Cho phép người dùng nhận cuộc gọi đến số điện thoại cố định khi số này đang truy nhập Internet: Khi thuê bao đang vào mạng Internet mà có cuộc gọi đến thì màn hình máy tính sẽ hiển thị thông báo và thuê bao có thể có lựa chọn trả lời bằng máy tính, trả lời bằng điện thoại, chuyển sang máy điện thoại khác hay từ chối cuộc gọi.
- *Dịch vụ Web Dial Page (gọi điện thoại qua trang Web):* Dịch vụ Webdial page cho phép người sử dụng dịch vụ thực hiện cuộc gọi từ một trang Web trên Internet (Webdial page Server) tới một thuê bao PSTN. Cuộc gọi có thể là Phone-to-Phone (điện thoại tới điện thoại) hoặc PC-to-phone (máy tính tới điện thoại).

b. Dành cho doanh nghiệp có năm dịch vụ

- *Dịch vụ Free Phone 1800:* Dịch vụ miễn cước ở người gọi là dịch vụ này cho phép thực hiện cuộc gọi miễn phí tới nhiều đích khác nhau thông qua một số truy nhập thống nhất trên mạng với cước phí thuê bao gọi bằng cuộc gọi nội hạt. Cước phí đường dài của cuộc gọi sẽ được tính cho thuê bao đăng ký dịch vụ 1800.

Đối với người sử dụng: không phải trả tiền cho cuộc gọi và có thể gọi tại bất kỳ nơi nào mà chỉ cần nhớ một số gọi.

Đối với doanh nghiệp: Dịch vụ Free Phone đáp ứng nhu cầu của các doanh nghiệp cung cấp sản phẩm hoặc dịch vụ và các tổ chức mang tính xã hội như các công ty quảng cáo... có số lượng khách hàng đông đảo. Các công ty sử dụng dịch vụ Free Phone sẽ tăng khả năng tiếp xúc với khách hàng, tạo điều kiện cho doanh nghiệp thực hiện tốt hơn việc tiếp thị sản phẩm và dịch vụ qua đó chăm sóc khách hàng của mình được tốt hơn.

- *Dịch vụ gia tăng 1900 về thông tin, giải trí, thương mại:* Dịch vụ này được cung cấp bởi nhà khai thác viễn thông và công ty cung cấp dịch vụ thông tin cho khách hàng. Người sử dụng dịch vụ gọi đến một số điện thoại dễ nhớ do nhà khai thác viễn thông cung cấp để nghe thông tin (thể thao, thời tiết...), giải trí hoặc thương mại của công ty

cung cấp dịch vụ thông tin. Mức cước cuộc gọi sẽ được thu cao hơn cước thoại thông thường và tiền cước thu được của người sử dụng được chia theo công thức thoả thuận giữa nhà khai thác và công ty cung cấp thông tin. Với dịch vụ này nhà cung cấp thông tin dễ dàng cung cấp thông tin về thời tiết, thể thao, thị trường giá cả hoặc tư vấn về y tế, giáo dục...

- *Dịch vụ Free call button (gọi miễn phí từ trang Web):* Cho phép thuê bao sử dụng Internet (ngay trên Website của doanh nghiệp) để thực hiện các cuộc gọi không mất tiền đến các trung tâm hỗ trợ bán hàng và phía doanh nghiệp sẽ trả tiền cho cuộc gọi này. Trong trang web của doanh nghiệp dịch vụ này sẽ có những biểu tượng cho phép người truy cập gọi từ máy tính sang số điện thoại của thuê bao dịch vụ khi bấm chuột vào biểu tượng.
- *Dịch vụ gọi thương mại miễn phí (Commercial Free Call Service):*Với dịch vụ này người sử dụng có thể gọi đến một số dịch vụ đặc biệt và sẽ được nghe một đoạn quảng cáo tương ứng. Sau khi nghe hết đoạn quảng cáo, người gọi sẽ được hướng dẫn thực hiện một cuộc gọi không mất tiền.
- *Dịch vụ mạng riêng ảo Mega WAN:*Mạng riêng ảo (VPN) là sự mở rộng của mạng riêng sử dụng các đường truyền qua mạng công cộng ví dụ như Internet.

Dịch vụ mạng riêng ảo cung cấp kết nối mạng riêng ảo (LAN/WAN) cho khách hàng bằng các kênh riêng ảo trên nền mạng NGN. Khách hàng chỉ cần đăng ký các điểm và tốc độ cổng kết nối theo nhu cầu sử dụng. Nó giảm chi phí hơn rất nhiều so với dịch vụ thuê kênh riêng. Dịch vụ này rất hữu dụng cho những công ty mới không đủ khả năng xây dựng mạng WAN cho riêng mình: Giảm chi phí thông tin liên lạc nội bộ công ty (Intranet voice, video và data), tăng băng thông (bandwidth on demand) với xu hướng tin học hoá văn phòng và các hoạt động kinh doanh. Các dịch vụ IT trên mạng ngày càng da dạng (Tele-education, Tele-medecine, E-shopping.v.v..). Khách hàng chuyển từ thuê bao dịch vụ TDM Leased-line truyền thống sang dịch vụ VPN.

BÀI TẬP CHƯƠNG IV

Bài 1: Nêu khái niệm NGN. Phân tích 4 đặc điểm cơ bản của NGN.

Bài 2: Nêu những ưu nhược điểm của phương thức chuyển mạch gói so với phương thứcchuyển mạch kênh kênh?

Bài 3: X.25 là giao thức của công nghệ chuyển mạch gói, đặc tả giao tiếp giữa:

a. Các giao diện mạng b.Các giao diện người sử dụng

c. DTE và DCE d. Các thiết bị khác

Bài 4: Mạng X25 có các cơ chế kiểm soát lỗi, điều khiển luồng, cung cấp các dịch vụ tin cậy, tốc độ trao đổi thông tin tối đa:

a. 128 Kbps b. 2 Mbps

c. 100 Mbps d. 64 Kbps

Bài 5: Kích thước phần dữ liệu trong khung X.25 chỉ có thể đạt tối đa là:

a. 128 bytes. b. 256 bytes.

c. 4096 bytes d. 1500 bytes.

Bài 6: Mạng Frame Relay được gọi là mạng:

a. Chuyển mạch kênh. b.ISDN tốc độ cao

c. Đúng chuyển mạch gói tốc độ cao. d. Chuyển mach gói

Bài 7: Dữ liệu trong mạng Frame Relay được tổ chức thành các khung có độ dài:

a. Không cố định b. Cố định

c. 4096 byte. D. 1500 byte

Bài 8: ATM có tốc độ trao đổi thông tin từ:

a. 2 Mbps đến 8 Mbps b. 155 Mbps đến 1 Gbps

c. 100 Mbps đến 155 Mbps d. 155 Mbps đến 622 Mbps

CHƯƠNG 5. MẠNG INTERNET

Mục tiêu :

Sau khi nghiên cứu chương này sinh viên nắm được các kiến thức sau :

a. Kiến trúc mạng Internet, giao thức liên mạng IP, cách đánh địa chỉ trên mạng Internet và vấn đề chuyển đổi từ IPv4 sang IPv6.

b. Vấn đề định tuyến trên Internet

c. Một số dịch vụ nổi bật trên Internet và hoạt động của chúng.

5.1 LỊCH SỬ INTERNET

- *Lịch sử hình thành Internet*

Tháng 8 năm 1962, giáo sư Licklider của viện công nghệ Masachusset (Mỹ) đã đưa ra khái niệm mạng Galactic. Licklider đã tưởng tượng ra một tập các máy tính được kết nối toàn cầu mà có thể truy cập dữ liệu, chương trình từ bất kỳ nơi nào trên thế giới. Khái niệm này là tương tự như internet ngày nay. Tháng 7 năm 1961, Leonard Kleinrock của viện công nghệ Masachusset (Mỹ) xuất bản một bài báo về lý thuyết công nghệ chuyển mạch gói. Cuối năm 1966, Roberts gia nhập cơ quan nghiên cứu tiên tiến của bộ quốc phòng Mỹ (DARPA) để phát triển các khái niệm về mạng máy tính và ARPANET. Trong thời gian này, công ty BNN đã phát triển các switch ARPANET. Cũng trong thời gian này, công ty Network Analysis nghiên cứu tối ưu cấu hình và hiệu quả kinh tế mạng. Vào tháng 9 năm 1969, máy tính đầu tiên đã được kết nối với switch. Quá trình khởi tạo giao thức kết nối hai máy tính trong ARPANET gọi là giao thức điều khiển mạng (Network Control Protocol-NCP) được thực hiện bởi nhóm NWG đã kết thúc vào tháng 12 năm 1970. Các điểm ARPANET cài đặt xong giao thức NCP trong khoảng thời gian 1971-1972 và người dùng mạng có thể bắt đầu phát triển các ứng dụng trên mạng. Sự chứng minh thành công của mạng ARPANET ở quy mô rộng được thực hiện vào tháng 10 năm 1972. Cũng trong năm 1972, thư điện tử đã được giới thiệu. Internet được phát triển từ ARPANET dựa trên những ý tưởng kết nối các mạng độc lập. Bắt đầu với ARPANET như là công nghệ chuyển mạch gói tiên phong, Internet đã phát triển bao gồm các mạng vệ tinh, các mạng radio và các mạng khác. Internet ngày nay dựa trên ý tưởng kỹ thuật then chốt: mạng kiến trúc mở. Theo cách tiếp cận này, sự lựa chọn công nghệ của mỗi mạng riêng biệt không bị bắt buộc theo một kiểu kiến trúc mạng mà được chọn tùy ý bởi nhà cung cấp và các mạng kết nối với nhau thông qua một kiến trúc kết nối. Mỗi mạng được thiết kế để thích hợp với một môi trường mạng xác định và yêu cầu của người dùng. Ý tưởng thiết kế mạng kiến trúc mở được đề xuất bởi Kahn cuối năm 1972. Ý tưởng này gồm bốn luật cơ bản sau :

- Mỗi mạng riêng biệt phải tự hoạt động và có thể không bị thay đổi bên trong trước khi kết nối internet.
- Nếu một gói tin không đến đích thì nguồn nhanh chóng truyền lại gói tin đó.
- Cổng và bộ định tuyến được dùng để kết nối các mạng.
- Không có sự điều khiển toàn cục ở các tầng

Cụm từ "Internet" ra đời vào giai đoạn năm 1974. Lúc bấy giờ mạng internet vẫn được gọi là ARPANET. Năm 1983, giao thức TCP/IP bắt đầu được chấp nhận như một chuẩn hóa đối với lĩnh vực quân sự Mỹ và tất cả các máy vi tính nối với ARPANET phải sử dụng chuẩn mới này. Năm 1984, ARPANET được chia ra thành hai phần: phần một vẫn được gọi là ARPANET, phục vụ cho công tác tìm hiểu và phát triển; phần thứ hai được đặt tên là MILNET, là mạng dùng cho các mục đích quân sự. Đến năm 1985, internet đã được thiết lập như một công nghệ hỗ trợ cộng đồng rộng lớn các nhà nghiên cứu và phát triển và đã bắt đầu được sử dụng bởi các cộng đồng khác trong liên lạc hàng ngày.

Năm 1985, lãnh đạo chương trình NFSNET của cơ quan khoa học quốc gia Mỹ thông báo sử dụng chương trình NSFNET phục vụ cho cộng đồng giáo dục bậc cao và sử dụng giao thức TCP/IP cho chương trình này. NSF khuyến khích khách hàng trong lĩnh vực thương mại và không thuộc lĩnh vực hàn lâm. Đến năm 1995, NFSNET đã bao gồm nhiều mạng vùng, mạng riêng và mạng đường dài. Đến 1990, ARPANET đã kết thúc sự tồn tại của nó thì giao thức TCP/IP được dùng để thay thế.

Ngày nay internet có lượng người dùng rất đông đảo trên khắp thế giới. Internet đóng góp rất to lớn cho sự phát triển của nhân loại. Tuy nhiên, cấu trúc của Internet hiện tại vẫn còn nhiều nhược điểm vì vậy các nhà khoa học đã và đang nghiên cứu cải tiến để Internet có thể phục vụ ngày càng tốt hơn.

- *Lịch sử hình thành Internet ở Việt Nam:*

Vào năm 1991, Giáo sư Rob Hurle (Trường Đại học Quốc gia Australia - ANU) cùng với Viện Công nghệ thông tin tại Hà Nội (IOIT) đã thí nghiệm kết nối các máy tính ở Úc và Việt Nam thông qua đường dây điện thoại. Ông Rob cũng viết một phần mềm mới để có thể sử dụng modem liên lạc sang Việt Nam.

Năm 1992, thí nghiệm thành công và IOIT Hà Nội có hộp thư điện tử riêng với "đuôi" ở tận Úc. Email này được phía Việt Nam dùng để trao đổi nội dung với ông Rob, và có lẽ đó là lần đầu tiên người ở Việt Nam gửi email ra nước ngoài. Tới tháng 9 năm sau, ông Rob và một đồng nghiệp Việt kiều (Trường Đại học Tasmania) đã tới Hà Nội bàn về kế hoạch phát triển Internet tại Việt Nam.

Sau một thời gian dài nghiên cứu, phát triển, lịch sử Internet Việt Nam ghi nhận ngày 19.11.1997 là ngày mà quốc gia hình chữ S kết nối với xa lộ thông tin của thế giới. Cũng

trong ngày này, một số doanh nghiệp tiên phong đã chính thức nhận giấy phép trở thành nhà cung cấp dịch vụ Internet theo quyết định của Tổng cục Bưu điện. Trong đó, FPT là doanh nghiệp duy nhất tại Việt Nam vừa là nhà cung cấp dịch vụ Internet (ISP) vừa là nhà cung cấp thông tin lên mạng Internet (ICP) tại thời điểm này.

Tới tháng 10.2003, bên cạnh VNPT, FPT Telecom đã tự mình triển khai được cơ sở hạ tầng riêng và bắt đầu cung cấp ADSL với gói MegaNet và MegaBiz. Không lâu sau đó, thị trường Internet trong nước ghi nhận một cột mốc mới khi vào ngày 1.6.2006, chính nhà mạng này đã chính thức cung cấp dịch vụ truy cập Internet tốc độ cao bằng kết nối cáp quang (FTTH).

FTTH sử dụng tuyến cáp quang kết nối từ ISP đến nhà khách hàng, do đó chất lượng tốt hơn và băng thông cao hơn cáp đồng (ADSL). Cáp quang không bị nhiễu do độ dài, điện từ, không bị ảnh hưởng bởi thời tiết tác động, băng thông FTTH được tính bằng Gigabit/giây. Với công nghệ này, các nhà mạng có thể cung cấp đường truyền Internet có tốc độ tải lên đến 10 Gigabit/giây, nhanh gấp 200 lần so với ADSL 2+ (20 Megabit/giây).

Sau một thời gian mạng Inernet với IPv4 đi vào hoạt động ổn định rồi cạn kiệt, thì thời của IPv6 đã bắt đầu. IPv4 dễ quản lý với cấu trúc định tuyến phân cấp, bảo mật cao và hỗ trợ thiết bị di động tốt hơn. IPv6 sử dụng 128 bit để đánh địa chỉ, do đó có thể hỗ trợ tới 2.128 địa chỉ khác nhau, phục vụ gần như vô hạn các thiết bị. Đây là một thay đổi lớn mà Việt Nam đang triển khai đồng bộ cùng với thế giới.

5.2 GIAO THỨC TRUY CẬP WEB HTTP

World Wide Web (WWW) bắt đầu vào năm 1989 tại trung tâm nghiên cứu nguyên tử Châu Âu (CERN) xuất phát từ nhu cầu chia sẻ các báo cáo, các bảng biểu, hình vẽ và các tài liệu khác của các nhà khoa học quốc tế làm việc ở nhiều nơi.

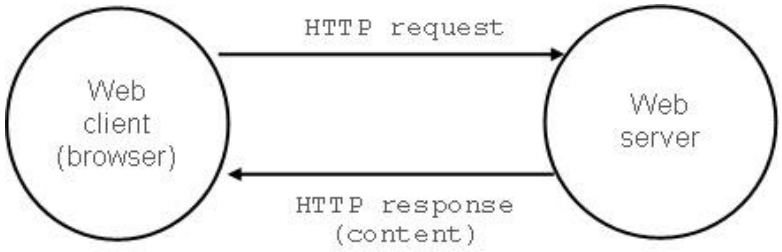
Một trang Web bao gồm các đối tượng. Một đối tượng đơn giản là một tập tin(file) như tập tin HTML, một tập tin ảnh hay một đoạn âm thanh... mà được xác định bằng URL. Mỗi URL có hai thành phần gồm tên máy chủ và tên đường dẫn của đối tượng. Ví dụ : URL

www.hvnh.edu/thttql/picture.jpg

www.hvnh.edu là tên máy chủ và /thttql/picture.jpg là đường dẫn của đối tượng.

HTTP là giao thức ở tầng ứng dụng và là trái tim của Web. HTTP được cài ở cả hai phía: chương trình khách(client) và chủ(server). Các chương trình khách và chủ trên các hệ thống đầu cuối khác nhau giao tiếp với nhau qua các thông điệp HTTP. Cấu trúc của thông điệp HTTP và cách thức trao đổi thông điệp giữa khách và chủ được HTTP quy định.

Một trình duyệt web(browser) là một chương trình cho phép hiển thị những yêu cầu ở phía người dùng. Các trình duyệt thông dụng hiện nay là : Chrom, Firefox, Internet explorer. Web server được cài ở phía server chứa đối tượng mà được xác định thông qua địa chỉ URL.

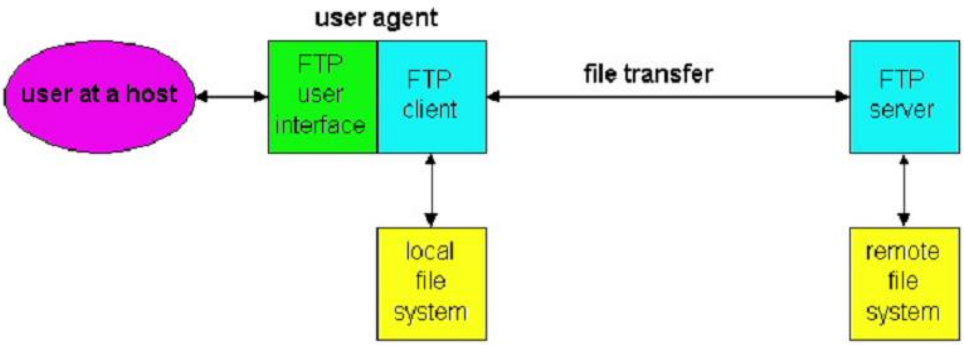


Hình 49 - Hành vi request-response

HTTP phiên bản 1.0 và 1.1 đều sử dụng giao thức TCP như là giao thức tầng giao vận phía dưới của chúng. Đầu tiên, HTTP phía client khởi tạo một kết nối TCP với phía server. Khi kết nối TCP thành công, browser và server truy cập TCP thông qua socket. Ở phía client, socket được xem như "cửa" giữa client và kết nối TCP. Ở phía server socket được xem như "cửa" giữa server và kết nối TCP. Client gửi yêu cầu tới socket của nó và được TCP chuyển tới server. Nhận được yêu cầu server gửi trả lời tới socket của nó và được TCP chuyển đến socket của client.

5.3 GIAO THỨC TRUYỀN FILE FTP

FTP (File Transfer Protocol) xuất hiện vào năm 1971. FTP cho phép truyền file từ máy này sang máy khác.



Hình 50- Các dịch vụ cung cấp bởi FTP

Các chức năng của FTP được mô tả như hình sau:

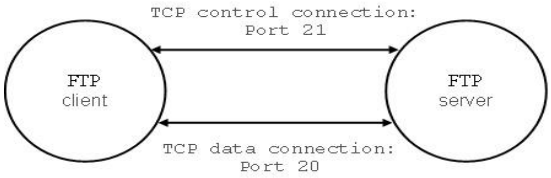
Trong một phiên làm việc của FTP, một người dùng muốn truyền file từ máy của họ tới một máy khác hoặc từ một máy khác tới máy của họ, người dùng phải cung cấp định danh người dùng và mật khẩu. Sau khi xác thực thông tin, người dùng có thể truyền file.

Để tương tác với FTP, người dùng đầu tiên cung cấp tên máy tính ở đầu kia để tạo kết nối với FTP server trên máy ở đầu kia. Sau khi xác thực người dùng, người dùng có thể truyền file từ máy của họ đến máy đầu kia và ngược lại.

FTP sử dụng hai kết nối song song để truyền file: một kết nối điều khiển và một kết nối dữ liệu. Kết nối điều khiển sử dụng để truyền thông tin điều khiển(đinh danh người dùng, mật

khẩu, lệnh chuyển thư mục trên máy ở đầu kia, lệnh "put" và "get" file) giữa hai máy. Kết nối truyền dữ liệu là đường thực sự để truyền dữ liệu giữa các máy.

Kết nối điều khiển và kết nối truyền dữ liệu được minh họa như hình sau:

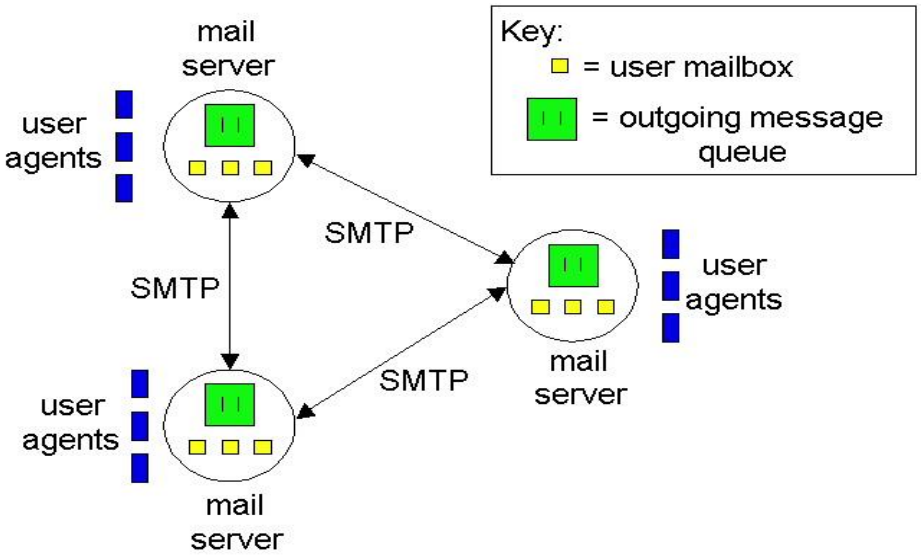


Hình 51 - Kết nối điều khiển và dữ liệu

Khi bắt đầu một phiên kết nối FTP với một máy khác, FTP thiết lập một kết nối điều khiển TCP ở cổng số 21 trên server. Phía client của FTP gửi thông tin định danh người dùng và mật khẩu đến FTP server qua đường điều khiển TCP này. Lệnh thay đổi thư mục trên máy ở đầu kia cũng được FTP client gửi qua đường điều khiển này. Khi người dùng muốn truyền file, FTP mở một liên kết truyền dữ liệu TCP ở cổng số 20 trên server. FTP gửi đúng một file rồi đóng liên kết dữ liệu. Nếu người dùng muốn truyền thêm file trong cùng phiên, FTP mở một liên kết TCP khác. Do đó, trong FTP, liên kết điều khiển được mở suốt thời gian tồn tại của phiên người dùng còn kết nối dữ liệu được mở mỗi khi file được truyền.

5.4 THƯ ĐIỆN TỬ TRÊN INTERNET (Email)

Thư điện tử (Email) là một trong những ứng dụng phổ biến nhất của Internet. Giống với thư tay, chúng ta có thể đọc thư điện tử khi thuận tiện tuy nhiên thư điện tử dễ gửi, gửi nhanh và rẻ. Một thông điệp của thư điện tử có thể kèm theo hình ảnh, video, tài liệu... Các thành phần chính của hệ thống thư điện tử được mô tả như hình dưới đây:

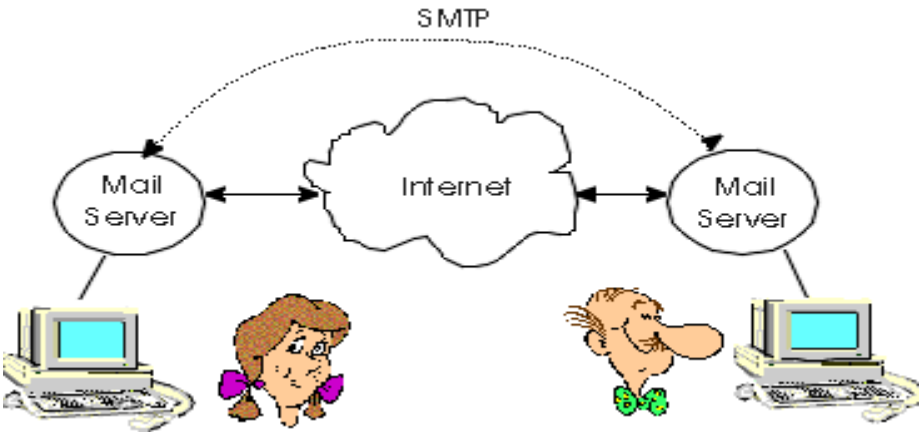


Hình 52 - Hệ thống email Internet

A gửi một thông điệp email tới B. Tác nhân người dùng (User agent) cho phép người dùng đọc, trả lời, chuyển tiếp, lưu, và soạn thư. Khi A kết thúc soạn thư, user agent gửi thư của nó đến mail server của nó. Thư này nằm ở hàng đợi gửi đi của mail server. Khi B muốn đọc thư, user agent của nó lấy thư từ hộp thư trên mail server của nó.

Mỗi người có một hộp thư trên mail server. Hộp thư quản lý và duy trì thư gửi đến. Khi một người dùng A gửi thư đến B, đầu tiên thư đi đến user agent của A, tiếp theo nó đến mail server của A, sau đó thư đến mail server của người nhận B. Để đọc được thư, B cần xác thực tên và mật khẩu. Sau khi xác thực thành công B có thể đọc thư trên hộp thư của nó.

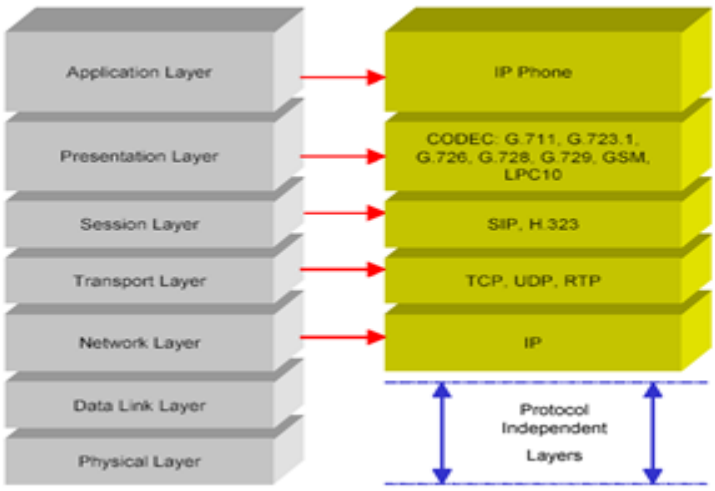
Quá trình gửi và nhận thư ở trên được thực hiện bởi giao thức SMTP (The Simple Mail Transfer Protocol). SMTP là giao thức tầng ứng dụng cho thư điện tử trên Internet. SMTP sử dụng dịch vụ truyền dữ liệu tin cậy của TCP để truyền thư từ mail server của người gửi đến mail server của người nhận. SMTP hoạt động ở cả hai phía client(người gửi) và server (người nhận). Phía client thực hiện trên mail server của người gửi còn phía server thự hiện trên mail server của người nhận.



Hình 53- Giao thức SMTP

5.5 GỌI ĐIỆN THOẠI TRÊN INTERNET (Voip)

Voip (Voice over Internet protocol) là công nghệ cho phép truyền tiếng nói qua giao thức Internet. Voip phát triển nhanh chóng và được sử dụng rộng rãi hiện nay. Các công nghệ truyền tiếng nói qua mạng trước đây như mạng điện thoại công cộng (public telephone network) hay mạng tích hợp dịch vụ số (Integrated Sevice Degital Network-ISDN) sử dụng công nghệ chuyển mạch kênh(circuit-switched network) nghĩa là thiết lập kênh giữa nguồn và đích trước khi truyền dữ liệu. Nhược điểm của chuyển mạch kênh là phải mất thời gian thiết lập kênh và hiệu suất sử dụng đường truyền không cao. Ngược lại, Voip sử dụng công nghệ chuyển mạch gói(packet-switched network) để tăng hiệu quả truyền dữ liệu.



Hình 54- Mô hình Voip

a. Thành phần của Voip

Voip gồm 4 thành phần chính sau : tạo và quản lý cuộc gọi, nén tín hiệu, truyền tín hiệu và chuyển đổi tín hiệu.

- Tạo và quản lý cuộc gọi

Chức năng này tạo và kết nối giữa hai điểm cuối cũng như tạo và quản lý cuộc gọi.

- Nén và giải nén tín hiệu

Tín hiệu giọng nói của con người dạng tương tự được chuyển và nén thành đinh dạng tín hiệu số thích hợp để truyền qua mạng IP

- Truyền tín hiệu

Tín hiệu được truyền theo một đường truyền đảm bảo chất lượng tiếng nói. Vấn đề xử lý tín hiệu của Voip được chuẩn hóa bởi công nghệ H323.

- Bộ chuyển đổi

Chuyển đổi tín hiệu từ một định dạng sang định dạng thích hợp với nơi nhận.

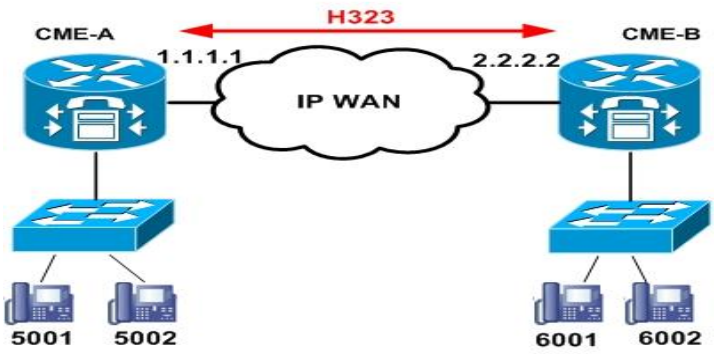
b. Chuẩn H323

Chuẩn H323 là công nghệ nền tảng cho phép truyền dữ liệu, âm thanh, hình ảnh thời gian thực qua mạng chuyển mạch gói. Nó xác định các thành phần, các giao thức và các thủ tục cung cấp truyền dữ liệu đa phương tiện qua môi trường mạng chuyển mạch gói bao gồm mạng Internet, mạng diện rộng, mạng cục bộ. H323 có thể được ứng dụng đưới nhiều dạng :

chỉ dùng âm thanh, âm thanh và video, âm thanh và dữ liệu, dữ liệu và video... H323 cho phép truyền đa phương tiện tới nhiều điểm.

Các thành phần của H323 gồm :

- Các thiết bị đầu cuối (Terminal): Sử dụng để truyền đa phương tiện hai chiều thời gian thực. Thiết bị đầu cuối có thể là một máy tính cá nhân, một thiết bị độc lập mà hỗ trợ truyền âm thanh, video và dữ liệu.
- Các gateway: Gateway dùng để kết nối giữa mạng sử dụng công nghệ H323 và mạng không sử dụn g công nghệ H323. Sự kết nối giữa các mạng khác nhau đạt được bởi các giao thức cho phép thiết lập, giải phóng cuộc gọi, chuyển đổi dữ liệu có định dạng khác nhau giữa các mạng và truyền thông tin giữa các mạng qua các gateway.
- Các gatekeeper: Gatekeeper được xem như bộ não của mạng H323. Nó là điểm đầu mối cho các cuộc gọi trong mạng H323. Nó cung cấp nhiều dịch vụ quan trọng như xác định địa chỉ, vấn đề ủy quyền và xác thực các thiết bị đầu cuối và các gateway. Nó cũng quản lý băng thông, tài khoản, chi phí.
- Các bộ điều khiển đa điểm (Multipoint Control Units-MCU): Hỗ trợ cho các hội thảo qua mạng với nhiều điểm cuối H323. Tất cả các thiết bị điểm cuối H323 tham gia hội thảo được kết nối với MCU. MCU quản lý tài nguyên của hội thảo, thỏa thuận với các thiết bị đầu cuối về việc mã hóa/giải mã tín hiệu và xử lý tín hiệu.



Hình 55 - H323

5.6 DỊCH VỤ TÊN MIỀN DNS

Cá nhân mỗi con người có thể được xác định theo nhiều cách. Chẳng hạn, chúng ta có thể được xác định qua tên trong giấy khai sinh hay bằng số chứng minh thư. Tương tự như vậy, máy tính trên Internet cũng có thể xác định bằng nhiều cách, ví dụ tên máy tính(hostname). Tên máy tính như cnn.cn, yahoo.com là dễ nhớ đối với con người. Tên máy tính cũng có thể bao gồm nhiều chữ cái, chữ số có độ dài thay đổi nên khó xử lý đối với router. Vì lý do đó máy tính được xác định bằng địa chỉ IP. Địa chỉ IP được phân cấp và gồm

4 byte. Giá trị mỗi byte được đổi sang số thập phân có giá trị từ 0 đến 255 và mỗi byte cách nhau bởi một dấu chấm. Ví dụ, một địa chỉ IP là 155.48.17.6.

a. Các dịch vụ của DNS

Một máy tính trên mạng Internet có thể xác định bằng tên máy hoặc địa chỉ IP. Con người thích sử dụng tên máy vì dễ nhớ trong khi router thích sử dụng địa chỉ IP. Để dung hòa giữa hai cách khác nhau này chúng ta cần một dịch vụ chuyển đổi từ tên máy sang địa chỉ IP. Đây là nhiệm vụ chính của Dịch vụ tên miền (DNS).

DNS có những đặc điểm chính sau:

- Là cơ sở dữ liệu phân tán được đặt trên các máy phân cấp phục vụ tên.
- Là giao thức tầng ứng dụng cho phép máy tính và máy phục vụ tên liên lạc với nhau để cung cấp dịch vụ đổi từ tên máy sang địa chỉ IP.

DNS cũng cung cấp một số dịch vụ quan trọng sau:

- Một máy tính có thể có nhiều bí danh dễ nhớ thay vì một tên phức tạp. DNS chuyển từ bí danh sang tên của máy tính địa chỉ IP.
- Máy chủ phục vụ thư (mail server) có thể có tên phức tạp. DNS cho phép đặt bí danh dễ nhớ cho máy chủ phục vụ thư.
- Thực hiện phân tán tải trên các máy chủ khác nhau. Các trang web có nhiều người truy cập được đặt trên nhiều máy chủ.

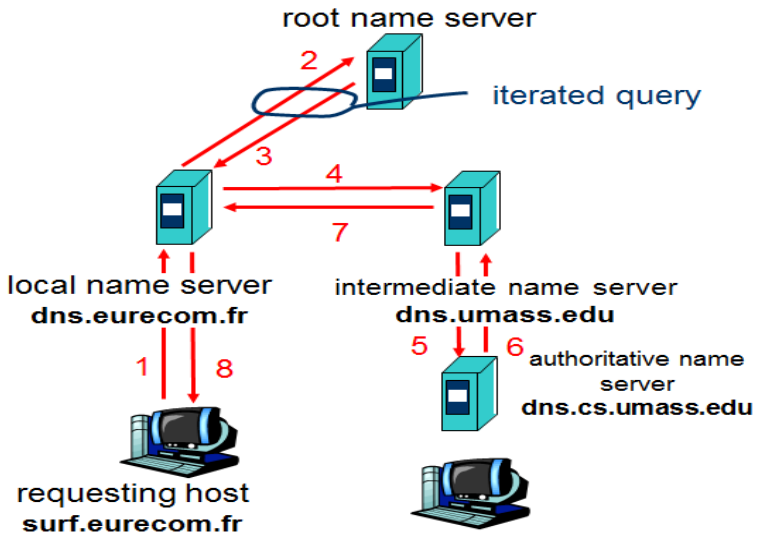
b. Hoạt động của DNS

Mục này tập trung vào vấn đề chuyển từ tên máy tính sang địa chỉ IP. Đối với người dùng, DNS là dịch vụ đơn giản nhưng thực tế dịch vụ này phức tạp, bao gồm các máy chủ tên đặt khắp toàn cầu và một giao thức quy định cách thức trao đổi giữa các máy chủ tên và các máy tính. Cách thiết kế đơn giản là chỉ có một máy chủ tên. Trong cách thiết kế tập trung này các client gửi trực tiếp tất cả các truy vấn tới máy chủ tên và máy chủ tên sẽ trả lời trực tiếp cho các client. Tuy nhiên, cách thiết kế này không phù hợp bởi vì:

- Nếu máy phục vụ tên bị hỏng thì toàn bộ internet không hoạt động
- Một máy chủ tên duy nhất khó có thể đáp ứng được toàn bộ các yêu cầu từ HTTP, email, và hàng triệu các máy tính khác.
- Một máy chủ tên không thể gần với tất cả các client dẫn đến truy cập chậm và tắc nghẽn.
- Một máy chủ tên phải lưu toàn bộ thông tin của tất cả các máy tính vì vậy cơ cở dữ liệu là rất lớn.

Vì lý do trên nên DNS được thiết kế phân tán. DNS sử dụng nhiều máy chủ tên được tổ chức phân cấp và phân bố khắp thế giới. Có ba loại máy chủ tên chính là: máy chủ tên địa phương (local name server), máy chủ tên gốc(root name server) và máy chủ tên thẩm quyền(authoriative name server). Tương tác giữa các máy chủ tên này với nhau và các máy tính như sau:

- Máy chủ tên địa phương: Mỗi cơ quan (công ty, trường đại học...) có một máy chủ địa phương. Khi một máy tính yêu cầu DNS, đầu tiên yêu cầu này được gửi đến máy chủ địa phương. Nếu máy chủ địa phương có DNS thích hợp thì nó sẽ gửi trả lời ngay lập tức.
- Máy chủ tên gốc: Có nhiều máy chủ tên gốc. Phần lớn máy chủ tên gốc đặt ở Bắc Mỹ. Khi máy chủ địa phương không có câu trả lời thích hợp với yêu cầu của một máy tính nó sẽ gửi yêu cầu DNS này đến một trong số các máy chủ tên gốc. Nếu máy chủ tên gốc có câu trả lời nó sẽ gửi trả lời DNS đến máy chủ địa phương và máy chủ địa phương sẽ trả lời DNS này đến máy tính yêu cầu. Nếu máy chủ địa phương không thể trả lời thì nó sẽ chỉ đến địa chỉ IP của máy chủ tên có thẩm quyền quản lý máy tính đó.
- Máy chủ tên có thẩm quyền: Mọi máy tính phải đăng ký với một máy chủ tên có thẩm quyền. Nói chung mỗi máy tính có ít nhất hai máy chủ tên có thẩm quyền phòng trường hợp một máy máy chủ tên có thẩm quyền bị lỗi.



Hình 56- DNS

Máy chủ tên có thẩm quyền thường là máy chủ tên địa phương. Theo định nghĩa, máy chủ tên có thẩm quyền luôn luôn có bản ghi DNS cho phép đổi tên máy tính sang địa chỉ IP của máy tính đó. Khi được máy chủ tên gốc yêu cầu, máy chủ tên có thẩm quyền gửi trả lời DNS đến máy chủ tên gốc. Tiếp theo máy chủ tên gốc gửi trả lời DNS đến máy chủ tên địa phương. Máy chủ tên địa phương gửi trả lời DNS đến máy tính yêu cầu.

5.7 GIAO THỨC INTERNET (Internet Protocol)

Giao thức Internet (IP protocol) là giao thức ở lớp mạng của Internet. Hiện tại có hai phiên bản của giao thức IP là giao thức IP phiên bản 4 (IPv4) và giao thức IP phiên bản 6 (IPv6).

a. Địa chỉ IP

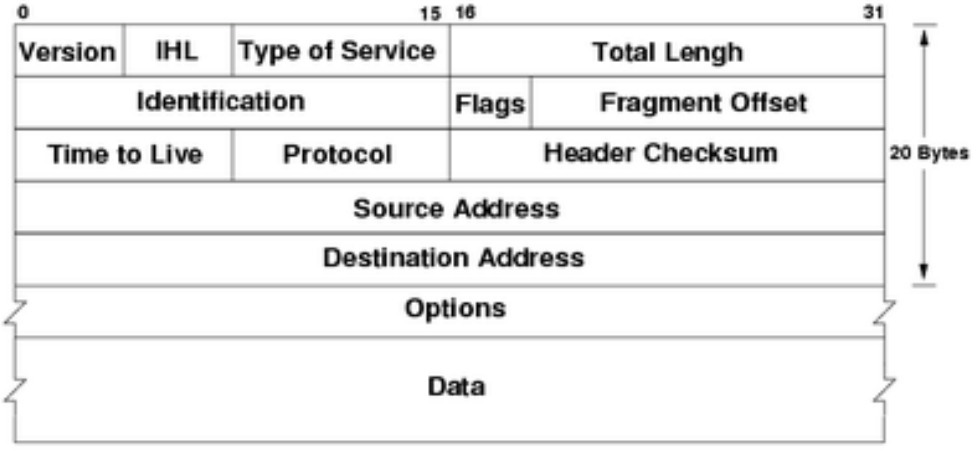
Mỗi địa chỉ IP gồm 32 bit tương ứng với 4 bytes. Địa chỉ IP được viết dưới dạng số thập phân trong đó mỗi byte được quy đổi ra hệ thập phân và các byte cách nhau bằng dấu chấm. Ví dụ địa chỉ IP là 193.32.216.9. 193 là số thập phân tương ứng với 8 bit đầu tiên, 32 là số thập phân tương ứng với 8 bit thứ hai, v..v. Như vậy địa chỉ trên dưới dạng nhị phân là:

11000001 00100000 11011000 00001001

Mỗi máy tính trên mạng có duy nhất một địa chỉ IP. Tùy theo độ lớn của các mạng con(sub network) mà người ta chia địa chỉ IP thành 5 lớp mạng ký hiệu là A,B,C,D,E như sau:

- Lớp A: Dùng bit 0 đầu tiên để đánh dấu và cho phép định danh 128 mạng, mỗi mạng có thể có 16 triệu máy.
- Lớp B: Dùng hai bit 10 để đánh dấu, lớp này có thể định danh 16384 mạng, mỗi mạng có nhiều nhất 65534 máy.
- Lớp C: Đánh dấu bởi 3 bit 110, lớp C định danh tối đa tới 2 triệu mạng, mỗi mạng tối đa 254 máy.
- Lớp D: Dùng 4 bit 1110 để đánh dấu, lớp này dùng để gửi gói dữ liệu IP đến một nhóm các máy.
- Lớp E: Dự phòng cho tương lai.

b. Khuôn dạng gói dữ liệu IPv4



Hình 57 – Khuôn dạng gói tin IPv4

Các trường chính trong IPv4 như sau:

Phiên bản (Version): Dùng 4 bit để xác định phiên bản giao thức IP của gói dữ liệu. Dựa vào phiên bản, bộ định tuyến (router) có thể xác định được ý nghĩa các trường còn lại của gói dữ liệu. Các phiên bản khác nhau thì cấu trúc gói dữ liệu cũng khác nhau.

Độ dài tiêu đề (Header length):Trường tiêu đề dài 4 bit dùng để xác định vị trí thực sự của dữ liệu trong gói dư liệu IP.

Kiểu dịch vụ (Type of service): 4 bit của trường kiểu dịch vụ cho phép phân biệt kiểu của các gói dữ liệu IP. Ví dụ, phân biệt gói dữ liệu thời gian thực với gói dữ liệu không thời gian thực.

Độ dài gói dữ liệu IP: Đây là độ dài tổng cộng của gói dữ liệu IP được tính bằng byte. Về mặt lý thuyết độ dài gói dữ liệu IP có thể lên tới 65535 bytes nhưng thực tế độ dài tối đa ít khi vượt quá 1500 bytes.

Định danh, cờ, phân mảnh offset: Những trường này được dùng trong trường hợp gói dữ liệu IP cần phải phân mảnh.

Thời gian tồn tại (Time-to-live TTL): Trường này xác định thời gian tồn tại của gói dữ liệu trong mạng. Mỗi lần gói dữ liệu được xử lý bởi bộ định tuyến (router) thì trường này giảm 1 đơn vị. Nếu TTL bằng 0 thì gói dữ liệu phải bị loại bỏ.

Giao thức (Protocol): Trường giao thức chỉ được sử dụng khi gói dữ liệu IP đến đích cuối cùng của nó. Trường này cho biết nơi mà dữ liệu thực của gói dữ liệu IP sẽ được chuyển đến.

Checksum của tiêu đề (header checksum): Trường này dùng để kiểm tra lỗi trong gói dữ liệu IP nhận được ở router. If checksum được tính lại của gói dữ liệu IP đến khác với checksum có sẵn trong gói dữ liệu IP thì gói dữ liệu IP có lỗi.

Địa chỉ nguồn và đích (source and desination IP address): Những trường này cho biết địa chỉ nơi gửi gói dữ liệu IP và nơi nhận nó.

Lựa chọn (options): Trường này cho phép mở rộng tiêu đề IP nhưng hiếm khi được sử dụng.

Dữ liệu (data): Đây là trường quan trọng nhất. Hầu hết các trường hợp trường này mang dữ liệu được gửi đến đích. Tuy nhiên trường này có thể mang kiểu dữ liệu khác như thông điệp ICMP...

c. Khuôn dạng gói dữ liệu IPv6

Bởi vì số máy tính kết nối Internet tăng mạnh dẫn tới địa IPv4 đã bắt đầu được sử dụng hết. Để mà giải quyết vấn đề địa chỉ IP, IPv6 đã được phát triển để thay thế cho IPv4. IPv6 được thiết kế bằng cách cải tiến IPv4.

Một số thay đổi quan trọng nhất của IPv6 là:

- **Tăng không gian đánh địa chỉ**: Địa chỉ của IPv6 được tăng từ 32 lên 128 bit. Điều này đảm bảo không bị hết địa chỉ IP. Ngoài địa chỉ địa chỉ duy nhất (unicast) và địa

chỉ đa đích (multicast), một loại địa chỉ mới được thêm vào trong IPv6 là anycast mà cho phép một gói tin được gửi đến một nhóm các máy tính bất kỳ.

- **Trường tiêu đề dài 40 bytes**: Trường tiêu đề có độ dài cố định 40 bytes cho phép xử lý các gói tin IP nhanh hơn.
- **Nhãn luồng và mức độ ưu tiên**: Trong IPv6, có thể dán nhãn cho các gói tin thuộc về các luồng đặc biệt để được xử lý đặc biệt theo yêu cầu. Ví dụ, truyền dữ liệu dạng âm thanh, video có thể xem như một luồng. Trường ưu tiên trong IPv6 có 4 bit. Trường này có thể sử dụng để gán độ ưu tiên cho các gói tin trong một luồng hoặc trong các ứng dụng.

Khuôn dạng gói tin của IPv6 như sau:

Hình 58 – Khuôn dạng gói tin Ipv6

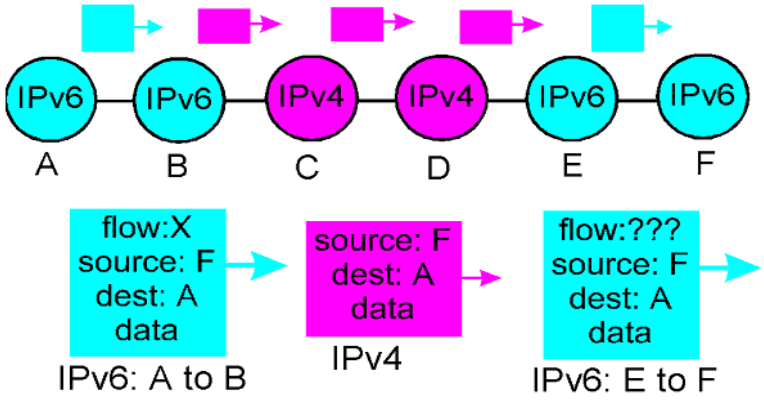
- **Trường phiên bản**(Version): Trường này dài 4 bit xác định phiên bản của IP. Trong IPv6 trường này mang giá trị 6.
- **Ưu tiên** (Priority): Trường 4 bit này tương tự như trường ToS trong IPv4.
- **Nhãn luồng** (Flow label): Trường này dùng để xác định luồng của các gói tin.
- **Next header**: Trường này xác định giao thức mà dữ liệu trong trường data field sẽ được gửi đến.
- **Số chặng** (Hop limit): Trường này xác định số chặng tối đa mà gói dữ liệu được phép chuyển đi. Mỗi lần đến router giá trị trường này giảm 1 đơn vị. Nếu giá trị trường này bằng 0 thì gói tin phải bị xóa bỏ.
- **Địa chỉ nguồn và đích** (Source and destiantion address): Địa chỉ nguồn và đích trong IPv6 dài 128 bit.
- **Dữ liệu**(Data): Khi gói tin đến đích, phần dữ liệu thực trong gói tin sẽ được chuyển đến giao thức tiếp theo mà được chỉ ra trong trường Next header.

d. Chuyển đổi từ IPv4 sang IPv6

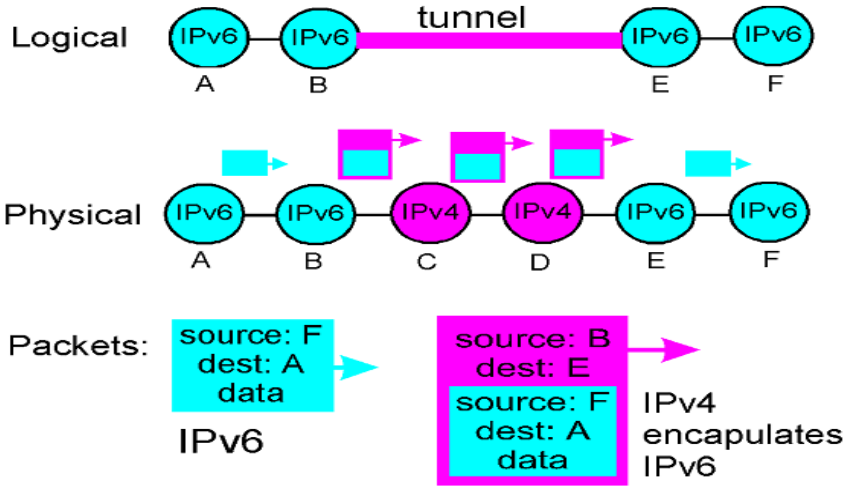
Như đã trình bày ở các phần trên, cách thiết kế IPv6 và IPv4 có nhiều điểm khác nhau. Một vấn đề được đặt ra khi đưa IPv6 vào sử dụng là việc chuyển đổi từ hệ thống Internet sử dụng IPv4 sang IPv6. Một hệ thống IPv6 có thể gửi, định tuyến và nhận gói tin IPv4 nhưng hệ thống IPv4 không thể xử lý gói tin IPv6.

Một cách tiếp cận cho vấn đề này như theo chuẩn RFC 1993 là một node bao gồm cặp IPv6 và IPv4. Một node như vậy có thể gửi, nhận cả gói IPv6 và IPv4. Khi tương tác với node IPv4 cặp IPv4/IPv6 sử dụng gói tin IPv4 còn khi tương tác với node IPv6 thì sử dụng gói tin IPv6. Như vậy một node IPv4/IPv6 bao gồm cả địa chỉ IPv4 và IPv6.

Một cách tiếp cận khác là sử dụng phương pháp đường ống. Giả sử một hệ thống như hình vẽ dưới đây. Một node A truyền một gói tin IPv6 đến một node E. Node B và E là IPv6, các router giữa B và E là IPv4. Để gửi gói tin IPv6 đến E, node B đặt toàn bộ gói tin IPv6 vào trường Data của gói tin IPv4. B gửi gói tin IPv4 chứa gói tin IPv6 qua các router IPv4 đến node IPv6 đầu tiên E. E sẽ lấy gói tin IPv6 trong IPv4.



Hình 59 - Dual Stack Approach



Hình 60- Tunnel

5.8 Định tuyến trên Internet

Để chuyển các gói tin từ một máy gửi đến máy đích, lớp mạng phải xác định tuyến đường các gói tin sẽ đi. Cho dù các lớp mạng cung cấp dịch vụ gói (trong trường hợp các gói khác nhau giữa một cặp nguồn-đích có thể sử dụng các tuyến khác nhau) hoặc một dịch vụ mạch ảo (trong trường hợp tất cả các gói dữ liệu giữa một cặp nguồn-đích đi theo con đường giống nhau), lớp mạng phải xác định đường đi cho gói tin. Đây là công việc định tuyến của lớp mạng.

Trung tâm của bất kỳ giao thức định tuyến nào là thuật toán (các " thuật toán định tuyến") xác định con đường cho một gói tin. Mục đích của một thuật toán định tuyến rất đơn giản: cho một tập hợp các thiết bị định tuyến, với các liên kết kết nối các thiết bị định tuyến, một thuật toán định tuyến tìm thấy một đường "tốt" đi từ nguồn tới đích đến. Thông thường, một con đường "tốt" là một con đường trong đó có " chi phí thấp nhất", nhưng chúng ta sẽ thấy rằng trong thực tế, các vấn đề như chính sách (ví dụ , một quy định như là " bộ định tuyến X thuộc tổ chức Y không nên chuyển tiếp các gói có nguồn gốc từ mạng thuộc sở hữu của tổ chức Z") làm phức tạp các thuật toán đơn giản mà làm nền tảng cho các giao thức mạng ngày nay.

Đồ thị trừu tượng được sử dụng để xây dựng các thuật toán định tuyến được thể hiện trong hình 4,2-1. (Để xem một số đồ thị đại diện cho bản đồ mạng thực sự, xem [Dodge 1999]; cuộc thảo luận về các mô hình đồ thị mô hình Internet khác nhau như thế nào, xem [Zegura 1997]). Ở đây, các nút trong đồ thị thể hiện các bộ định tuyến - những điểm mà tại đó các quyết định định tuyến gói tin được thực hiện - và các đường ("cạnh" trong thuật ngữ lý thuyết đồ thị) kết nối các nút thể hiện cho các liên kết vật lý giữa các bộ định tuyến. Một liên kết cũng có một giá trị thể hiện cho các "chi phí" gửi một gói tin qua liên kết. Chi phí có thể phản ánh mức độ tắc nghẽn trên liên kết (ví dụ, sự chậm trễ trung bình hiện tại để gửi một gói tin qua liên kết đó) hoặc khoảng cách vật lý truyền qua liên kết đó (ví dụ, một liên kết xuyên đại dương có thể có chi phí cao hơn một liên kết trên đất liền). Ở đây, chúng ta chỉ đơn xem chi phí của một liên kết như một giá trị cho trươc và không quan tâm đến cách thức chúng được xác định.

Cho đồ thị trừu tượng, vấn đề của việc tìm kiếm đường đi chi phí ít nhất từ một nguồn đến đích yêu cầu xác định một loạt các liên kết mà:

- Liên kết đầu tiên của đường được kết nối với nguồn
- Liên kết cuối cùng của đường dẫn được kết nối với đích
- Với tất cả i, liên kết i và i-1 của đường được kết nối với cùng một nút
- Với đường dẫn chi phí thấp nhất, tổng các chi phí của các liên kết trên con đường là tối thiểu từ nguồn đến đích.

5.8.1 Phân loại các thuật toán định tuyến

Nói rộng ra, một trong những cách chúng ta có thể phân loại thuật toán định tuyến là chúng là thuật toán tập trung hay phân tán:

Các thuật toán định tuyến tập trung tính toán con đường chi phí ít nhất giữa nguồn và đích sử dụng kiến thức toàn diện và đầy đủ về mạng. Thuật toán loại này lấy các kết nối giữa tất cả các nút và tất cả các chi phí của các liên kết như là đầu vào.

Bằng cách nào đó thuật toán có được thông tin này trước khi thực hiện tính toán. Việc tính toán có thể được chạy tại một địa điểm (một giải thuật định tuyến tập trung) hoặc nhân rộng ở nhiều địa điểm. Đặc trưng phân biệt chính ở đây là thuật toán tập trung có thông tin đầy đủ về các liên kết và các chi phí của các liên kết. Trong thực tế, các thuật toán với thông tin trạng đầy đủ thường được gọi là link state algorithms, bởi vì thuật toán này phải biết được tình trạng (chi phí) của mỗi liên kết trong mạng.

Trong một thuật toán định tuyến phân tán, việc tính toán đường chi phí ít nhất là thực hiện bằng cách lặp lại phân tán. Không có nút nào có thông tin đầy đủ về các chi phí của tất cả các liên kết mạng. Thay vào đó, mỗi nút bắt đầu với chỉ kiến thức về các chi phí liên kết trực tiếp của riêng nó và sau đó, thông qua một quá trình lặp lại các tính toán và trao đổi thông tin với các nút hàng xóm (ví dụ, các nút ở " đầu kia" của liên kết) tính đường chi phí ít nhất đến một đích hoặc nhiều đích. Thuật toán định tuyến phân tán còn được gọi là distance vector algorithm (thuật toán vector khoảng cách). Nó được gọi là thuật toán vector khoảng cách bởi vì một nút trên thực tế chưa bao giờ biết đường đi đầy đủ từ nguồn tới đích. Thay vào đó, nó chỉ biết hướng (hàng xóm) mà nó sẽ gửi gói tin để gói tin đến đích với chi phí ít nhất.

Cách thứ hai để phân loại các thuật toán định tuyến là phân loại theo tính chất tĩnh hay động. Trong thuật toán định tuyến tĩnh, các tuyến đường thay đổi rất chậm theo thời gian, như là kết quả của sự can thiệp của con người (ví dụ , một con người tự chỉnh sửa bảng định tuyến của router).

Trong thuật toán định tuyến động, các tuyến đường thay đổi khi cấu trúc mạng thay đổi. Một thuật toán động có thể được thực hiện định kỳ hoặc khi cấu trúc mạng, chi phí của liên kết thay đổi. Trong khi các thuật toán động đáp ứng nhiều hơn với sự thay đổi của mạng nhưng chúng cũng nhạy cảm với các vấn đề : như các vòng lặp định tuyến và dao động trong các tuyến đường.

Chỉ có hai loại thuật toán định tuyến được thường được sử dụng trong Internet : link state algorithm động và dynamic decentralized distance vector algorithm (thuật toán vector khoảng cách động).

Một mạng Internet bao gồm nhiều vùng tự trị, mỗi vùng tự trị bao gồm nhiều mạng. Mỗi vùng tự trị chọn một thuật toán định tuyến cho nó.

5.8.2 Giao thức định tuyến trong vùng tự trị trên Internet

Một số giao thức định tuyến trong vùng tự trị nổi tiếng là: RIP (Routing Information Protocol), OSFP (Open Shortest Path First) và IGRP (Interier Gateway Routing Protocol). Phần này sẽ giới thiệu đặc điểm chính của các giao thức trên.

a. Giao thức RIP

RIP là một trong những giao thức cho vùng tự trị đầu tiên và được sử dụng rộng rãi. RIP sử dụng thuật toán véc-tơ khoảng cách. Đường ngắn nhất giữa hai điểm trong RIP là đường có số bước nhảy ngắn nhất giữa hai điểm đó. Số bước nhảy nhiều nhất giữa hai điểm là 15(hai điểm kề nhau thì số bước nhảy là 1).

b. Giao thức OSFP

Khác với RIP, OSFP là giao thức Link state và sử dụng thuật toán Dijkstra để tìm đường ngắn nhất giữa hai điểm. OSFP có thể chọn nhiều đường nếu có nhiều đường cùng giá. Tiêu chí xác định đường ngắn nhất của OSFP không cố định(có thể là băng thông, độ trễ...).

c. Giao thức IGRP

IGRP là giao thức được đề xuất bởi Cisco. IGRP là giao thức vec-tơ khoảng cách. Các tiêu chí chọn đường của IGRP bao gồm độ trễ, băng thông, độ tin cậy và tải nạp. Quyết định chọn đường theo tiêu chí nào phụ thuộc vào người quản trị.

5.8.3 Định tuyến giữa các vùng tự trị

BGP (Border Gateway Protocol) là một giao thức định tuyến giữa các vùng tự trị trên Internet. BGP có nhiều điểm giống với giao thức véc-tơ khoảng cách. Các router trong BGP không thông báo thông tin về giá tới đích (ví dụ số chặng tới đich...) mà thông báo số thứ tự của các vùng tự trị trên đường đến đích. BGP không chọn đường đến đích mà quyền chọn thuộc về người quản trị.

BÀI TẬP CHƯƠNG V

Bài 1: Câu nào sau đây mô tả về mạng LAN

A. Mạng có khu vực địa lý lớn hơn mạng WAN

B. Mạng kết nối các máy tính trong khu vực một đô thị

C. Mạng kết nối các máy tính và các switch trong một toà nhà

D. Mạng phục vụ người sử dụng thông qua vùng địa lý rộng lớn mà thường sử dụng các thiết bị truyền thông được cung cấp bởi các nhà cung cấp đường truyền

Bài 2: Quá trình download thư điện tử từ Email Server về Email client sử dụng giao thức nào sau đây

A. POP3 B. HTTP C. FTP D. UDP

Bài 3: Quá trình gửi và nhận thông điệp giữa hai Email Server sử dụng giao thức nào trong các giao thức sau

A. TFTP B. NFL C. SQLSEC D. SMTP E. POP3

Bài 4: Dịch vụ web sử dụng giao thức nào trong các giao thức sau

A. HTTP B. FTP C. NETBIOS D. IPX

Bài 5: Một tài khoản thư điện tử bao gồm những yếu tố nào sau đây

A. Tên người dùng và số hòm thư B. Tên người dùng và mật khẩu

C. Mật khẩu và tên miền của Email server D. Tên người dùng và tên miền của Email Server.

Bài 6: Hai người cùng chát với nhau qua mạng Yahoo Messenger trong cùng một phòng nét

a. Dữ liệu truyền từ máy đang chát lên máy chủ phòng nét và quay về máy chát bên kia

b. Dữ liệu đi trực tiếp giữa hai máy đang trong phòng chát

c. Dữ liệu truyền về máy chủ Yahoo và quay về máy bên kia

d. Dữ liệu truyền về máy chủ internet Việt Nam và quay về máy đang chat

Bài 7: Trong khi soạn thảo email nếu muốn gởi kèm file chúng ta bấm vào nút

a. send b.copy

c. attachment d.file/save

Bài 8: Chọn phát biểu đúng về Email

A. Là phương thức truyền tập tin từ máy này đến máy khác trên mạng.

B. Là dịch vụ cho phép ta truy cập đến hệ thống máy tính khác trên mạng.

C. Là dịch vụ cho phép ta gởi và nhận thư điện tử.

D. Là hình thức hội thoại trực tiếp trên Internet

CHƯƠNG 6 – AN NINH MẠNG MÁY TÍNH

Mục tiêu :

Sau khi nghiên cứu chương này sinh viên nắm được các kiến thức sau :

a. Các biện pháp bảo vệ và đảm bảo an toàn dữ liệu cho mạng máy tính

b. *Một số giao thức an ninh điển hình trên mạng Internet*

6.1 GIỚI THIỆU VỀ AN NINH MẠNG

6.1.1 An Ninh mạng là gì.

Máy tính có phần cứng chứa dữ liệu do hệ điều hành quản lý, đa số các máy tính nhất là các máy tính trong công ty, doanh nghiệp được nối mạng Lan và Internet. Nếu như máy tính, hệ thống mạng của bạn không được trang bị hệ thống bảo vệ vậy chẳng khác nào bạn đi khỏi căn phòng của mình mà quên khóa cửa, máy tính của bạn sẽ là mục tiêu của virus, worms, unauthorized user … chúng có thể tấn công vào máy tính hoặc cả hệ thống của bạn bất cứ lúc nào.

Vậy an toàn mạng có nghĩa là bảo vệ hệ thống mạng, máy tính khỏi sự phá hoại phần cứng hay chỉnh sửa dữ liệu (phần mềm) mà không được sự cho phép từ những người cố ý hay vô tình. An toàn mạng cung cấp giải pháp, chính sách, bảo vệ máy tính, hệ thống mạng, ngăn không cho những người dùng trái phép, cũng như các phần mềm chứa mã độc xâm nhập bất hợp pháp vào máy tính, hệ thống mạng.

6.1.2 Các yếu tố cần được bảo vệ trong hệ thống mạng

Yếu tố đầu tiên phải nói đến là dữ liệu, những thông tin lưu trữ trên hệ thống máy tính cần được bảo vệ do các yêu cầu về tính bảo mật, tính toàn vẹn hay tính kịp thời. Thông thường yêu cầu về bảo mật được coi là yêu cầu quan trọng đối với thông tin lưu trữ trên mạng. Tuy nhiên, ngay cả khi những thông tin không được giữ bí mật, thì yêu cầu về tính toàn vẹn cũng rất quan trọng. Không một cá nhân, một tổ chức nào lãng phí tài nguyên vật chất và thời gian để lưu trữ những thông tin mà không biết về tính đúng đắn của những thông tin đó.

Yếu tố thứ hai là về tài nguyên hệ thống, sau khi các Attacker đã làm chủ được hệ thống chúng sẽ sử dụng các máy này để chạy các chương trình như dò tím mật khẩu để tấn công vào hệ thống mạng.

Yếu tố thứ ba là danh tiếng một khi dữ liệu bị đánh cắp thì việc nghi ngờ nhau trong công ty là điều không tránh khỏi, vì vậy sẽ ảnh hưởng đến danh tiếng của công ty rất nhiều.

6.1.3 Các yếu tố đảm bảo an toàn thông tin

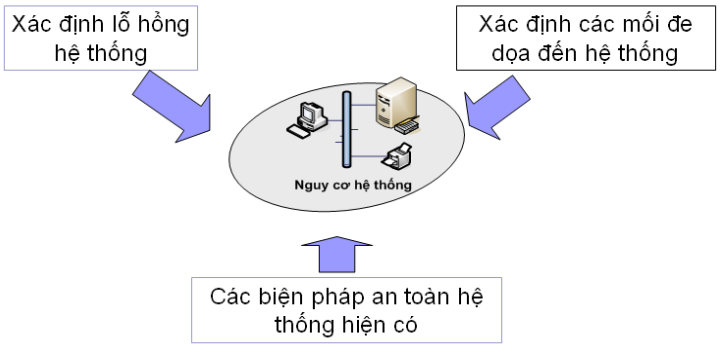
An toàn thông tin nghĩa là thông tin được bảo vệ, các hệ thống và những dịch vụ có khả năng chống lại những tai hoạ, lỗi và sự tác động không mong đợi. Mục tiêu của an toàn bảo

mật trong công nghệ thông tin là đưa ra một số tiêu chuẩn an toàn và ứng dụng các tiêu chuẩn an toàn này để loại trừ hoặc giảm bớt các nguy hiểm.

Hiện nay các biện pháp tấn công càng ngày càng tinh vi, sự đe doạ tới độ an toàn thông tin có thể đến từ nhiều nơi khác nhau theo nhiều cách khác nhau, vì vậy các yêu cầu cần để đảm bảo an toàn thông tin như sau:

- *Tính bí mật*: Thông tin phải đảm bảo tính bí mật và được sử dụng đúng đối tượng.
- *Tính toàn vẹn*: Thông tin phải đảm bảo đầy đủ, nguyên vẹn về cấu trúc, không mâu thuẫn.
- *Tính sẵn sàng*: Thông tin phải luôn sẵn sàng để tiếp cận, để phục vụ theo đúng mục đích và đúng cách.
- *Tính chính xác*: Thông tin phải chính xác, tin cậy.
- *Tính không khước từ* (chống chối bỏ): Thông tin có thể kiểm chứng được nguồn gốc hoặc người đưa tin.

Nguy cơ hệ thống (Risk) được hình thành bởi sự kết hợp giữa lỗ hổng hệ thống và các mối đe doạ đến hệ thống, nguy cơ hệ thống có thể định nghĩa trong ba cấp độ thấp, trung bình và cao. Để xác định nguy cơ đối với hệ thống trước tiên ta phải đánh giá nguy cơ hệ thống theo sơ đồ sau.



Hình 61- Quá trình đánh giá nguy cơ của hệ thống

- Xác định các lỗ hổng hệ thống

Việc xác định các lỗ hổng hệ thống được bắt đầu từ các điểm truy cập vào hệ thống như:

- Kết nối mạng Internet
- Các điểm kết nối từ xa
- Kết nối các tổ chức khác
- Các môi trường truy cập vật lý hệ thống
- Các điểm truy cập người dùng
- Các điểm truy cập không dây

Ở mỗi điểm truy cập, ta phải xác định được các thông tin có thể truy cập và mức độ truy cập vào hệ thống.

- Xác định các mối đe đoạ

Đây là một công việc khó khăn vì các mối đe dọa thường không xuất hiện rõ ràng (ẩn), thời điểm và quy mô tấn công không biết trước. Các hình thức và kỹ thuật tấn công đa dạng như:

- DoS/DDoS, BackDoor, Tràn bộ đệm,…
- Virus, Trojan Horse, Worm
- Social Engineering

- Các biện pháp an toàn hệ thống

Các biện pháp an toàn hệ thống gồm các biện pháp: Như firewall, phần mềm diệt virut, điều khiển truy cập, hệ thống chứng thực (mật khẩu, sinh trắc học, thẻ nhận dạng), mã hoá dữ liệu, hệ thống xâm nhập IDS, các kỹ thuật khác, ý thức người dùng, hệ thống chính sách bảo mật và tự động vá lỗ hệ thống

6.2 CÁC LỖ HỔNG BẢO MẬT

Có nhiều các tổ chức đã tiến hành phân loại các dạng lỗ hổng đặc biệt. Theo bộ quốc phòng Mỹ các loại lỗ hổng được phân làm ba loại như sau:

6.2.1 Lỗ hổng loại C

Cho phép thực hiện các hình thức tấn công theo DoS (Denial of Services- Từ chối dịch vụ) Mức độ nguy hiểm thấp chỉ ảnh hưởng tới chất lượng dịch vụ, làm ngưng trệ gián đoạn hệ thống, không làm phá hỏng dữ liệu hoặc đạt được quyền truy cập bất hợp pháp.

DoS là hình thức tấn công sử dụng các giao thức ở tầng Internet trong bộ giao thức TCP/IP để làm hệ thống ngưng trệ dẫn đến tình trạng từ chối người sử dụng hợp pháp truy nhập hay sử dụng hệ thống.

Các dịch vụ có lỗ hổng cho phép các cuộc tấn công DoS có thể được nâng cấp hoặc sửa chữa bằng các phiên bản mới hơn của các nhà cung cấp dịch vụ. Hiện nay chưa có một biện pháp hữu hiệu nào để khắc phục tình trạng tấn công kiểu này vì bản thân thiết kế ở tầng Internet (IP) nói riêng và bộ giao thức TCP/IP nói chung đã ẩn chứa những nguy cơ tiềm tang của các lỗ hổng loại này.

6.2.2 Lỗ hổng loại B

Cho phép người sử dụng có thêm các quyền trên hệ thống mà không cần kiểm tra tính hợp lệ dẫn đến mất mát thông tin yêu cầu cần bảo mật. Lỗ hổng này thường có trong các ứng dụng trên hệ thống . Có mức độ nguy hiểm trung bình.

Lỗ hổng loại B này có mức độ nguy hiểm hơn lỗ hổng loại C. Cho phép người sử dụng nội bộ có thể chiếm được quyền cao hơn hoặc truy nhập không hợp pháp.Những lỗ hổng loại này thường xuất hiện trong các dịch vụ trên hệ thống. Người sử dụng local được hiểu là người đã có quyền truy nhập vào hệ thống với một số quyền hạn nhất định.

Một dạng khác của lỗ hổng loại B xảy ra với các chương trình viết bằng mã nguồn C. Những chương trình viết bằng mã nguồn C thường sử dụng một vùng đệm, một vùng trong bộ nhớ sử dụng để lưu trữ dữ liệu trước khi xử lý. Người lập trình thường sử dụng vùng đệm trong bộ nhớ trước khi gán một khoảng không gian bộ nhớ cho từng khối dữ liệu. Ví dụ khi viết chương trình nhập trường tên người sử dụng quy định trường này dài 20 ký tự bằng khai báo:

Char first_name [20]; Khai báo này cho phép người sử dụng nhập tối đa 20 ký tự. Khi nhập dữ liệu ban đầu dữ liệu được lưu ở vùng đệm. Khi người sử dụng nhập nhiều hơn 20 ký tự sẽ tràn vùng đệm. Những ký tự nhập thừa sẽ nằm ngoài vùng đệm khiến ta không thể kiểm soát được. Nhưng đối với những kẻ tấn công chúng có thể lợi dụng những lỗ hổng này để nhập vào những ký tự đặc biệt để thực thi một số lệnh đặc biệt trên hệ thống. Thông thường những lỗ hổng này được lợi dụng bởi những người sử dụng trên hệ thống để đạt được quyền root không hợp lệ. Để hạn chế được các lỗ hổng loại B phải kiêm soát chặt chẽ cấu hình hệ thống và các chương trình.

6.2.3 Lỗ hổng loại A

Cho phép người ngoài hệ thống có thể truy cập bất hợp pháp vào hệ thống. Có thể làm phá huỷ toàn bộ hệ thống. Loại lỗ hổng này có mức độ rất nguy hiểm đe dọa tính toàn vẹn và bảo mật của hệ thống. Các lỗ hổng này thường xuất hiện ở những hệ thống quản trị yếu kém hoặc không kiểm soát được cấu hình mạng. Ví dụ với các web server chạy trên hệ điều hành Novell các server này có một scripst là convert.bas chạy scripst này cho phép đọc toàn bộ nội dung các file trên hệ thống.

Những lỗ hổng loại này hết sức nguy hiểm vì nó đã tồn tại sẵn có trên phần mềm sử dụng, người quản trị nếu không hiểu sâu về dịch vụ và phần mềm sử dụng có thể bỏ qua điểm yếu này. Vì vậy thường xuyên phải kiểm tra các thông báo của các nhóm tin về bảo mật trên mạng để phát hiện những lỗ hổng loại này. Một loạt các chương trình phiên bản cũ thường sử dụng có những lỗ hổng loại A như: FTP, Gopher, Telnet, Sendmail, ARP, finger...

6.3 CÁC KIỂU TẤN CÔNG CỦA HACKER

6.3.1 Tấn công trực tiếp

Sử dụng một máy tính để tấn công một máy tính khác với mục đích dò tìm mật mã, tên tài khoản tương ứng, …. Họ có thể sử dụng một số chương trình giải mã để giải mã các file chứa password trên hệ thống máy tính của nạn nhân. Do đó, những mật khẩu ngắn và đơn giản thường rất dễ bị phát hiện.

Ngoài ra, hacker có thể tấn công trực tiếp thông qua các lỗi của chương trình hay hệ điều hành làm cho hệ thống đó tê liệt hoặc hư hỏng. Trong một số trường hợp, hacker đoạt được quyền của người quản trị hệ thống.

6.3.2 Kỹ thuật đánh lừa : Social Engineering

Đây là thủ thuật được nhiều hacker sử dụng cho các cuộc tấn công và thâm nhập vào hệ thống mạng và máy tính bởi tính đơn giản mà hiệu quả của nó. Thường được sử dụng để lấy cấp mật khẩu, thông tin, tấn công vào và phá hủy hệ thống.

Ví dụ : kỹ thuật đánh lừa Fake Email Login.

Về nguyên tắc, mỗi khi đăng nhập vào hộp thư thì bạn phải nhập thông tin tài khoản của mình bao gồm username và password rồi gởi thông tin đến Mail Server xử lý. Lợi dụng việc này, những người tấn công đã thiết kế một trng web giống hệt như trang đăng nhập mà bạn hay sử dụng. Tuy nhiên, đó là một trang web giả và tất cả thông tin mà bạn điền vào đều được gởi đến cho họ. Kết quả, bạn bị đánh cắp mật khẩu !

Nếu là người quản trị mạng, bạn nên chú ý và dè chừng trước những email, những messengers, các có điện thoại yêu cầu khai báo thông tin. Những mối quan hệ cá nhân hay những cuộc tiếp xúc đều là một mối nguy hiểm tiềm tàng.

6.3.3 Kỹ thuật tấn công vào vùng ẩn

Những phần bị dấu đi trong các website thường chứa những thông tin về phiên làm việc của các client. Các phiên làm việc này thường được ghi lại ở máy khách chứ không tổ chức cơ sở dữ liệu trên máy chủ. Vì vậy, người tấn công có thể sử dụng chiêu chức View Source của trình duyệt để đọc phần đầu đi này và từ đó có thể tìm ra các sơ hở của trang Web mà họ muốn tấn công. Từ đó, có thể tấn công vào hệ thống máy chủ.

6.3.4 Tấn công vào các lỗ hổng bảo mật

Hiện, nay các lỗ hổng bảo mật được phát hiện càng nhiều trong các hệ điều hành, các web server hay các phần mềm khác, ... Và các hãng sản xuất luôn cập nhật các lỗ hổng và đưa ra các phiên bản mới sau khi đã vá lại các lỗ hổng của các phiên bản trước. Do đó, người sử dụng phải luôn cập nhật thông tin và nâng cấp phiên bản cũ mà mình đang sử dụng nếu không các hacker sẽ lợi dụng điều này để tấn công vào hệ thống.

Thông thường, các forum của các hãng nổi tiếng luôn cập nhật các lỗ hổng bảo mật và việc khai thác các lỗ hổng đó như thế nào thì tùy từng người.

6.3.5 Khai thác tình trạng tràn bộ đệm

Tràn bộ đệm là một tình trạng xảy ra khi dữ liệu được gởi quá nhiều so với khả năng xử lý của hệ thống hay CPU. Nếu hacker khai thác tình trạng tràn bộ đệm này thì họ có thể làm cho hệ thống bị tê liệt hoặc làm cho hệ thống mất khả năng kiểm soát.

Để khai thác được việc này, hacker cần biết kiến thức về tổ chức bộ nhớ, stack, các lệnh gọi hàm. Shellcode.

Khi hacker khai thác lỗi tràn bộ đệm trên một hệ thống, họ có thể đoạt quyền root trên hệ thống đó. Đối với nhà quản trị, tránh việc tràn bộ đệm không mấy khó khăn, họ chỉ cần tạo các chương trình an toàn ngay từ khi thiết kế.

6.3.6 Nghe trộm

Các hệ thống truyền đạt thông tin qua mạng đôi khi không chắc chắn lắm và lợi dụng điều này, hacker có thể truy cập vào data paths để nghe trộm hoặc đọc trộm luồng dữ liệu truyền qua.

Hacker nghe trộm sự truyền đạt thông tin, dữ liệu sẽ chuyển đến sniffing hoặc snooping. Nó sẽ thu thập những thông tin quý giá về hệ thống như một packet chứa password và username của một ai đó. Các chương trình nghe trộm còn được gọi là các sniffing. Các sniffing này có nhiệm vụ lắng nghe các cổng của một hệ thống mà hacker muốn nghe trộm. Nó sẽ thu thập dữ liệu trên các cổng này và chuyển về cho hacker.

6.3.7 Kỹ thuật giả mạo địa chỉ

Thông thường, các mạng máy tính nối với Internet đều được bảo vệ bằng bức tường lửa(fire wall). Bức tường lửa có thể hiểu là cổng duy nhất mà người đi vào nhà hay đi ra cũng phải qua đó và sẽ bị "điểm mặt". Bức tường lửa hạn chế rất nhiều khả năng tấn công từ bên ngoài và gia tăng sự tin tưởng lẫn nhau trong việc sử dụng tào nguyên chia sẻ trong mạng nội bộ.

Sự giả mạo địa chỉ nghĩa là người bên ngoài sẽ giả mạo địa chỉ máy tính của mình là một trong những máy tính của hệ thống cần tấn công. Họ tự đặt địa chỉ IP của máy tính mình trùng với địa chỉ IP của một máy tính trong mạng bị tấn công. Nếu như làm được điều này, hacker có thể lấy dữ liệu, phá hủy thông tin hay phá hoại hệ thống.

6.3.8 Kỹ thuật chèn mã lệnh

Một kỹ thuật tấn công căn bản và được sử dụng cho một số kỹ thuật tấn công khác là chèn mã lệnh vào trang web từ một máy khách bất kỳ của người tấn công.

Kỹ thuật chèn mã lệnh cho phép người tấn công đưa mã lệnh thực thi vào phiên làm việc trên web của một người dùng khác. Khi mã lệnh này chạy, nó sẽ cho phép người tấn

công thực hiện nhiều nhiều chuyện như giám sát phiên làm việc trên trang web hoặc có thể toàn quyền điều khiển máy tính của nạn nhân. Kỹ thuật tấn công này thành công hay thất bại tùy thuộc vào khả năng và sự linh hoạt của người tấn công.

6.3.9 Tấn công vào hệ thống có cấu hình không an toàn

Cấu hình không an toàn cũng là một lỗ hổng bảo mật của hệ thống. Các lỗ hổng này được tạo ra do các ứng dụng có các thiết lập không an toàn hoặc người quản trị hệ thống định cấu hình không an toàn. Chẳng hạn như cấu hình máy chủ web cho phép ai cũng có quyền duyệt qua hệ thống thư mục. Việc thiết lập như trên có thể làm lộ các thông tin nhạy cảm như mã nguồn, mật khẩu hay các thông tin của khách hàng.

Nếu quản trị hệ thống cấu hình hệ thống không an toàn sẽ rất nguy hiểm vì nếu người tấn công duyệt qua được các file pass thì họ có thể download và giải mã ra, khi đó họ có thể làm được nhiều thứ trên hệ thống.

6.3.10 Tấn công dùng Cookies

Cookie là những phần tử dữ liệu nhỏ có cấu trúc được chia sẻ giữa website và trình duyệt của người dùng.

Cookies được lưu trữ dưới những file dữ liệu nhỏ dạng text (size dưới 4KB). Chúng được các site tạo ra để lưu trữ, truy tìm, nhận biết các thông tin về người dùng đã ghé thăm site và những vùng mà họ đi qua trong site. Những thông tin này có thể bao gồm tên, định danh người dùng, mật khẩu, sở thích, thói quen,

Cookies được Browser của người dùng chấp nhận lưu trên đĩa cứng của máy tính, không phải Browser nào cũng hổ trợ cookies.

6.3.11 Can thiệp vào tham số trên URL

Đây là cách tấn công đưa tham số trực tiếp vào URL. Việc tấn công có thể dùng các câu lệnh SQL để khai thác cơ sở dữ liệu trên các máy chủ bị lỗi. Điển hình cho kỹ thuật tấn công này là tấn công bằng lỗi "SQL INJECTION".

Kiểu tấn công này gọn nhẹ nhưng hiệu quả bởi người tấn công chỉ cần một công cụ tấn công duy nhất là trình duyệt web và backdoor.

6.3.12 Vô hiệu hóa dịch vụ

Kiểu tấn công này thông thường làm tê liệt một số dịch vụ, được gọi là DOS (Denial of Service - Tấn công từ chối dịch vụ).

Các tấn công này lợi dụng một số lỗi trong phần mềm hay các lỗ hổng bảo mật trên hệ thống, hacker sẽ ra lệnh cho máy tính của chúng đưa những yêu cầu không đâu vào đâu đến các máy tính, thường là các server trên mạng. Các yêu cầu này được gởi đến liên tục làm cho hệ thống nghẽn mạch và một số dịch vụ sẽ không đáp ứng được cho khách hàng.

Đôi khi, những yêu cầu có trong tấn công từ chối dịch vụ là hợp lệ. Ví dụ một thông điệp có hành vi tấn công, nó hoàn toàn hợp lệ về mặt kỹ thuật. Những thông điệp hợp lệ này sẽ gởi cùng một lúc. Vì trong một thời điểm mà server nhận quá nhiều yêu cầu nên dẫn đến tình trạng là không tiếp nhận thêm các yêu cầu. Đó là biểu hiện của từ chối dịch vụ.

6.3.13 Một số kiểu tấn công khác

Lỗ hổng không cần login: Nếu như các ứng dụng không được thiết kế chặt chẽ, không ràng buộc trình tự các bước khi duyệt ứng dụng thì đây là một lỗ hổng bảo mật mà các hacker có thể lợi dụng để truy cập thẳng đến các trang thông tin bên trong mà không cần phải qua bước đăng nhập.

Thay đổi dữ liệu: Sau khi những người tấn công đọc được dữ liệu của một hệ thống nào đó, họ có thể thay đổi dữ liệu này mà không quan tâm đến người gởi và người nhận nó. Những hacker có thể sửa đổi những thông tin trong packet dữ liệu một cách dễ dàng.

Password-base Attact: Thông thường, hệ thống khi mới cấu hình có username và password mặc định. Sau khi cấu hình hệ thống, một số admin vẫn không đổi lại các thiết lập mặc định này. Đây là lỗ hổng giúp những người tấn công có thể thâm nhập vào hệ thống bằng con đường hợp pháp. Khi đã đăng nhập vào, hacker có thể tạo thêm user, cài backboor cho lần viến thăm sau.

Identity Spoofing: Các hệ thống mạng sử dụng IP address để nhận biết sự tồn tại của mình. Vì thế địa chỉ IP là sự quan tâm hàng đầu của những người tấn công. Khi họ hack vào bất cứ hệ thống nào, họ đều biết địa chỉ IP của hệ thống mạng đó. Thông thường, những người tấn công giả mạo IP address để xâm nhập vào hệ thống và cấu hình lại hệ thống, sửa đổi thông tin, …

Việc tạo ra một kiểu tấn công mới là mục đích của các hacker. Trên mạng Internet hiện nay, có thể sẽ xuất hiện những kiểu tấn công mới được khai sinh từ những hacker thích mày mò và sáng tạo. Bạn có thể tham gia các diễn đàn hacking và bảo mật để mở rộng kiến thức.

6.4 NHỮNG CÁCH PHÁT HIỆN HỆ THỐNG BỊ TẤN CÔNG

Không có một hệ thống nào có thể đảm bảo an toàn tuyệt đối; bản thân mỗi dịch vụ đều có những lỗ hổng bảo mật tiềm tàng. Đứng trên góc độ người quản trị hệ thống, ngoài việc tìm hiểu phát hiện những lỗ hổng bảo mật còn luôn phải thực hiện các biện pháp kiểm tra hệ thống xem có dấu hiệu tấn công hay không. Các biện pháp đó là:

- 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 về phần cứng hay không, nếu không phải phần cứng hãy nghĩ đến khả năng máy bị tấn công
- Kiểm tra các tài khoản người dùng mới trên hệ thống: một số tài khoản lạ, nhất là uid của tài khoản đó có uid= 0

- Kiểm tra xuất hiện các tập tin lạ. Thường phát hiện thông qua cách đặt tên các tệp tin, mỗi người quản trị hệ thống nên có thói quen đặt tên tập tin theo một 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).
- Kiểm tra thời gian thay đổi trên hệ thống, đặc biệt là các chương trình login, sh hoặc các scripts khởi động trong /etc/init.d, /etc/rc.d …
- 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 …
- Kiểm tra hoạt động của các dịch vụ mà hệ thống cung cấp. Chúng ta đã biết rằng 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.
- Kiểm tra truy nhập hệ thống bằng các account thông thường, đề phòng trường hợp các account này bị truy nhập trái phép và thay đổi quyền hạn mà người sử dụng hợp pháp không kiểm sóat được.
- 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.
- Kiểm tra các phiên bản của sendmail, /bin/mail, ftp; tham gia các nhóm tin về bảo mật để có thông tin về lỗ hổng của dịch vụ sử dụng

6.5 CÁC CHIẾN LƯỢC BẢO VỆ MẠNG

6.5.1 Quyền hạn tối thiểu (Least Privilege)

Mỗi chương trình và mỗi người sử dụng hệ thống nên hoạt động bằng cách sử dụng quyền hạn tối thiểu cần thiết để hoàn thành công việc.

Về cơ bản, nguyên tắc này làm hạn chế những thiệt hại mà có thể là kết quả của một tai nạn hoặc lỗi. Nó cũng làm giảm số lượng các tương tác tiềm năng giữa các quyền hạn chương trình ở mức tối thiểu cho hoạt động chính xác, để mà các sử dụng không chủ ý, không mong muốn, hoặc không đúng quyền hạn ít có khả năng xảy ra. Do đó, nếu câu hỏi đặt ra liên quan đến việc lạm dụng quyền hạn, số lượng các chương trình mà phải được kiểm toán giảm thiểu. Nói cách khác, nếu một cơ chế có thể cung cấp 'tường lửa, "nguyên tắc quyền hạn tối thiểu là cơ sở cho các nơi cài đặt tường lửa. Các quy tắc bảo mật quân sự "cần-thì-biết" là một ví dụ của nguyên tắc này.

6.5.2 Bảo vệ theo chiều sâu (Defence in Depth)

Khái niệm bảo vệ theo chiều sâu được dựa trên tiền đề phòng thủ nhiều lớp bao gồm một chiến lược toàn diện mà vượt rất nhiều bất kỳ một hệ thống duy nhất nào. Các bảo vệ trải dài trên nhiều giải pháp công nghệ, quy trình vận hành và giáo dục của nhân viên. Bảo vệ

hoàn chỉnh theo cách tiếp cận theo chiều sâu sẽ bao gồm hầu hết hoặc tất cả các công cụ sau đây :

- Tường lửa lọc gói với kiểm tra tình trạng
- DMZ cho cô lập, bên ngoài phải đối mặt với các máy chủ
- Lớp ứng dụng tường lửa với kiểm tra gói tin sâu
- Phát hiện xâm nhập / phòng chống
- Proxy server
- Xác thực và mã hóa mạng không dây
- Antivirus bảo vệ cho mạng, máy chủ tập tin và khách hàng
- Lọc thư rác tại máy chủ và máy khách
- Giám sát nội dung và lọc
- Xác nhận thiết bị di động
- Hệ thống tường lửa dựa trên cho các máy chủ và khách hang
- Quản lý Patch
- Các chính sách kiểm soát truy cập dựa trên quyền hạn tối thiểu
- Chính sách mật khẩu mạnh
- Quy tắc Workstation lockdown
- Tính năng bảo mật ứng dụng
- Sử dụng thích hợp mã hóa dữ liệu
- Các chính sách người dùng và đào tạo

6.5.3 Tính đơn giản

Giữ các thứ đơn giản là một phần quan trọng của an toàn dữ liệu. Nó làm cho chúng dễ hiểu, dễ quản lý và dễ khắc pục sự cố. Khi mọi thứ quá phức tạp làm cho khó hiểu, khó quản lý và phức tạp khi sử lý sự cố. Thêm nữa khó xác định hệ thống phức tạp đủ an toàn hay chưa.

Sự đơn giản không phải luôn luôn có thể đạt được đặc biệt đối với hạ tầng mạng và phần mềm. Khi lựa chọn giữa một giải pháp đơn giản và một giải pháp phức tạp hơn thì giải pháp đơn giản dễ thực hiện hơn và dễ kiểm định mức độ an toàn hơn.

6.5.4 Nút thắt

Nút thắt buộc tất cả các luồng, các hoạt động phải qua một đường đơn hoặc một kênh. Đường này được dùng để điều khiển tiêu thụ băng thông, lọc nội dung và cung cấp các dịch vụ xác thực. Mục đích của nút thắt là để đảm bảo rằng thiết bị an ninh ở vị trí điều khiển điều khiển mọi thứ. Mọi luồng, người dùng, dữ liệu đều được kiểm tra. Một nút thắt là có giá trị nếu và chỉ nếu nó khó có thể bị vượt qua. Nếu một hacker có thể tương tác với một đích trong hệ thống mà không qua nút thắt thì nút thắt này là không có giá trị.

6.5.5 Liên kết yếu nhất

Độ an toàn của một chuỗi chính là độ an toàn của liên kết yếu nhất. Độ an toàn của một cơ sở hạ tầng chính là độ an toàn của thành phần yếu nhất của nó. Mỗi lần chúng ta làm cho an toàn liên kết yếu nhất hiện tại thì nó không còn là liên kết yếu nhất nữa. Do đó một liên kết yếu nhất mới xuất hiện. Lặp lại vòng này để tìm liên kết yếu nhất và cải tiến nó.

Liên kết yếu nhất là không thể tránh khỏi nhưng liên kết yếu nhất mạnh luôn tốt hơn liên kết yếu nhất yếu.

6.5.6 Hỏng an toàn

Hỏng an toàn cũng là một phương pháp phổ biến để đảm bảo an toàn cho một hệ thống. Hỏng an toàn không chỉ áp dụng đối với các thiết bị an ninh mà còn đối với toàn bộ cơ sở hạ tầng. Khi khía cạnh an ninh bất kỳ thất bại, kết quả tốt nhất của thất bại đó là thất bại rơi vào một trạng thái được hỗ trợ hoặc duy trì sự bảo vệ an ninh thiết yếu. Điều này có nghĩa là luôn duy trì sự tin cậy và bảo vệ sự toàn vẹn.

6.5.7 Sự dạng của bảo vệ

Sự dạng của bảo vệ tương tự như bảo vệ theo chiều sâu nhưng nó không chỉ sử dụng các lớp khác nhau mà còn sử dụng các loại bảo vệ khác nhau. Ví dụ sử dụng khóa cửa và một khóa đánh lửa trên một chiếc xe là độ sâu của sự bảo vệ, thêm một hệ thống báo động tạo ra không chỉ tăng độ sâu mà còn thêm sự đa dạng bằng cách thêm một loại hoàn toàn khác nhau của sự bảo vệ. Bây giờ, hệ thống bảo vệ không chỉ cố gắng để giữ cho mọi người có thể sử dụng chiếc xe mà nó còn đang cố gắng để thu hút sự chú ý cho những người đang tấn công nó.

Thực hiện đúng, sự đa dạng của sự bảo vệ tạo nên một sự khác biệt đáng kể đối với an ninh của hệ thống. Tuy nhiên, nhiều nỗ lực để tạo ra sự đa dạng của sự bảo vệ là không đặc biệt hiệu quả. Một lý thuyết phổ biến là sử dụng các loại khác nhau của hệ thống. Ví dụ, trong một kiến trúc có hai hệ thống lọc gói, có thể tăng tính đa dạng của sự bảo vệ bằng cách sử dụng hệ thống từ các nhà cung cấp khác nhau. Nếu toàn bộ hệ thống là như nhau, ai đó biết cách đột nhập vào một trong số chúng thì có thể biết cách đột nhập vào tất cả hệ thống.

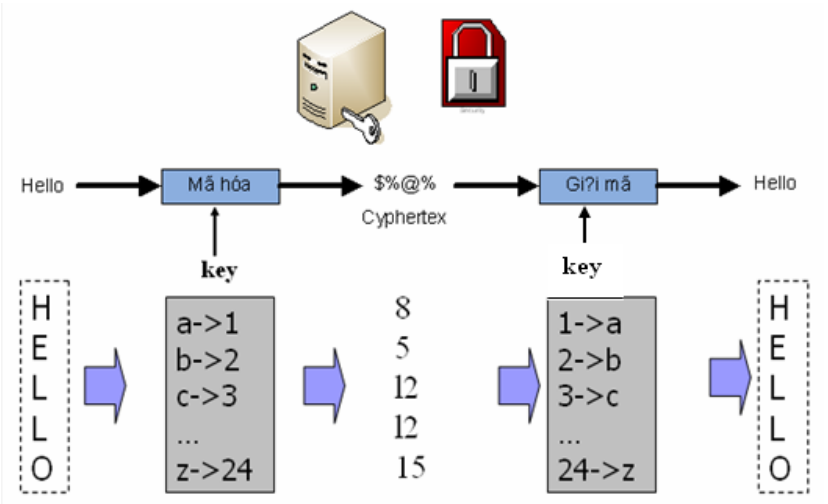
Sử dụng hệ thống bảo mật từ các nhà cung cấp khác nhau có thể làm giảm nguy cơ gây lỗi phổ biến hoặc lỗi cấu hình. Tuy nhiên, có một sự đánh đổi về độ phức tạp và chi phí. Mua sắm và lắp đặt nhiều hệ thống khác nhau là khó khăn hơn, mất nhiều thời gian hơn, và đắt hơn so với mua sắm và lắp đặt một hệ thống đơn.

Nếu không cẩn thận, chúng ta có thể tạo ra sự đa dạng yếu thay vì sự đa dạng trong bảo vệ. Nếu có hai bộ lọc gói khác nhau, một trong số chúng sử dụng trước, sau đó sử dụng cái còn lại sẽ giúp bảo vệ những điểm yếu. Nếu có hai bộ lọc gói tin khác nhau, mỗi bộ lọc riêng biệt cho phép lưu lượng đi vào, sau đó sử dụng các sản phẩm khác nhau chỉ làm cho dễ bị tổn thương cả hai bộ lọc thay vì một.

6.6 CÁC BIỆN PHÁP BẢO MẬT MẠNG

6.6.1 Mã hoá

Mã hoá là cơ chế chính cho việc bảo mật thông tin. Nó bảo vệ chắc chắn thông tin trong quá trình truyền dữ liệu, mã hoá có thể bảo vệ thông tin trong quá trình lưu trữ bằng mã hoá tập tin. Tuy nhiên người sử dụng phải có quyền truy cập vào tập tin này, hệ thống mã hoá sẽ không phân biệt giữa người sử dụng hợp pháp và bất hợp pháp nếu cả hai cùng sử dụng một key giống nhau. Do đó mã hoá chính nó sẽ không cung cấp bảo mật, chúng phải được điều khiển bởi key mã hoá và toàn bộ hệ thống.



Hình 62 - Quá trình mã hoá

Mã hoá nhằm đảm bảo các yêu cầu sau:

- *Tính bí mật* (confidentiality): dữ liệu không bị xem bởi "bên thứ 3".
- *Tính toàn vẹn* (Integrity): dữ liệu không bị thay đổi trong quá trình truyền.

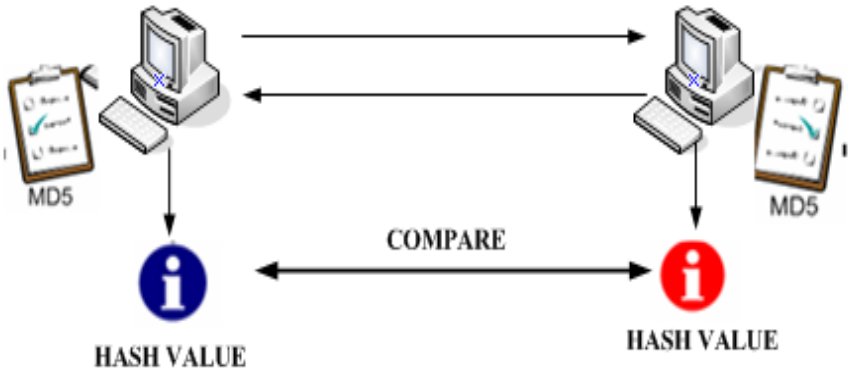
Tính không từ chối (Non-repudiation): là cơ chế người thực hiện hành động không thể chối bỏ những gì mình đã làm, có thể kiểm chứng được nguồn gốc hoặc người đưa tin.

6.6.2 Các giải thuật mã hoá

a. Giải thuật băm (Hashing Encryption)

Là cách thức mã hoá một chiều tiến hành biến đổi văn bản nhận dạng (cleartext) trở thành hình thái mã hoá mà không bao giờ có thể giải mã. Kết quả của tiến trình hashing còn được gọi là một hash (xử lý băm), giá trị hash (hash value), hay thông điệp đã được mã hoá (message digest) và tất nhiên không thể tái tạo lại dạng ban đầu.

Trong xử lý hàm băm dữ liệu đầu vào có thể khác nhau về độ dài, thế nhưng độ dài của xử lý Hash lại là cố định. Hashing được sử dụng trong một số mô hình xác thực password. Một giá trị hash có thể được gắn với một thông điệp điện tử (electronic message) nhằm hỗ trợ tính tích hợp của dữ liệu hoặc hỗ trợ xác định trách nhiệm không thể chối từ (non-repudiation).



Hình 63- Mô hình giải thuật băm

Một số giải thuật băm

- MD5 (Message Digest 5): **giá trị băm 128 bit.**
- SHA-1 (Secure Hash Algorithm): **giá trị băm 160 bit.**

b. Giải thuật mã hoá đồng bộ/đối xứng (Symmetric)

Mã hoá đối xứng hay mã hoá chia sẻ khoá (shared-key encryption) là mô hình mã hoá hai chiều có nghĩa là tiến trình mã hoá và giải mã đều dùng chung một khoá. Khoá này phải được chuyển giao bí mật giữa hai đối tượng tham gia giao tiếp. Có thể bẻ khoá bằng tấn công vét cạn (Brute Force).

Hình 64- Giải thuật mã hoá đồng bộ/đối xứng

Cách thức mã hoá như sau:

- Hai bên chia sẻ chung 1 khoá (được giữ bí mật).
- Trước khi bắt đầu liên lạc hai bên phải trao đổi khoá bí mật cho nhau.
- Mỗi phía của thành phần liên lạc yêu cầu một khoá chia sẻ duy nhất, khoá này không chia sẻ với các liên lạc khác.

Bảng 4 dưới đây cho thấy chi tiết các phương pháp mã hóa đối xứng thông dụng.

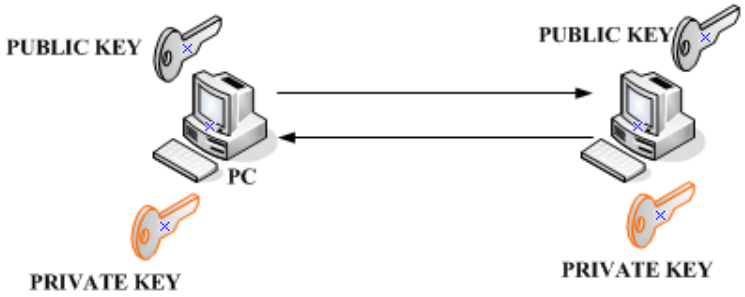
Các loại mã hóa	Đặc tính
Data Encryption Standard (DES)	- Sử dụng một khối 64 bit hoặc một khóa 56 bit.

	- Có thể dễ dàng bị bẻ khóa.
Triple DES (3DES)	- Áp dụng DES 3 lần. - Sử dụng một khóa 168bit. - Bị thay thế bởi AES.
Advanced Encryption Standard (AES)	- Sử dụng Rhine doll có khả năng đề kháng với tất cả tấn công đã biết. - Dùng một khóa và khóa chiều dài có thể thay đổi (128-192 hoặc 256 bit).

Bảng 4 – Các phương pháp mã hóa đối xứng thông dụng

c. Giải thuật mã hóa không đồng bộ/không đối xứng (Asymmetric)

Mã hóa bất đối xứng, hay mã hóa khóa công khai(public-key encryption), là mô hình mã hóa 2 chiều sử dụng một cặp khóa là khóa riêng (private key) và khóa công (public keys). Thông thường, một thông điệp được mã hóa với private key, và chắc chắn rằng key này là của người gửi thông điệp (message sender). Nó sẽ được giải mã với public key, bất cứ người nhận nào cũng có thể truy cập nếu họ có key này. Chú ý, chỉ có public key trong cùng một cặp khóa mới có thể giải mã dữ liệu đã mã hóa với private key tương ứng. Và private key thì không bao giờ được chia sẻ với bất kỳ ai và do đó nó giữ được tính bảo mật, với dạng mã hóa này được ứng dụng trong chữ ký điện tử.



Hình 65 - Giải thuật mã hóa không đồng bộ/không đối xứng

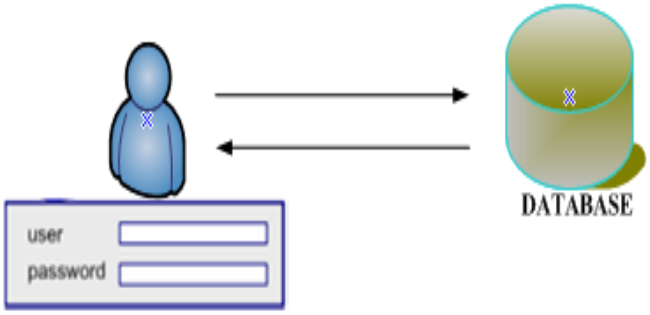
Các giải thuật:

- RSA (Ron Rivest, Adi Shamir, and Leonard Adleman).
- DSA (Digital Signature Standard).
- Diffie-Hellman (W.Diffie and Dr.M.E.Hellman).

6.6.3 Chứng thực người dùng

Là quá trình thiết lập tính hợp lệ của người dùng trước khi truy cập thông tin trong hệ thống. Các loại chứng thực như:

- Username/password: Là loại chứng thực phổ biến nhất và yếu nhất của chứng thực, username/password được giữ nguyên dạng chuyển đến Server.



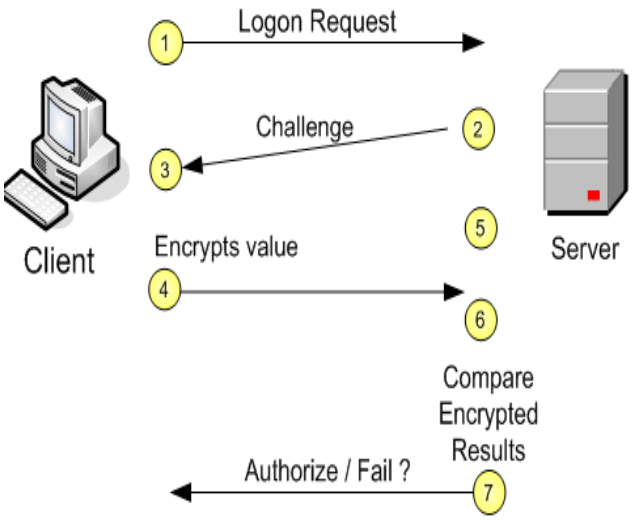
Hình 66 - Chứng thực bằng user và password

Tuy nhiên phương pháp này xuất hiện những vấn đề như dễ bị đánh cắp trong quá trình đến server

- Giải pháp

  - Đặt mật khẩu dài tối thiểu là tám kí tự, bao gồm chữ cái, số, biểu tượng.
  - Thay đổi password: 01 tháng/lần.
  - Không nên đặt cùng password ở nhiều nơi.
  - Xem xét việc cung cấp password cho ai.

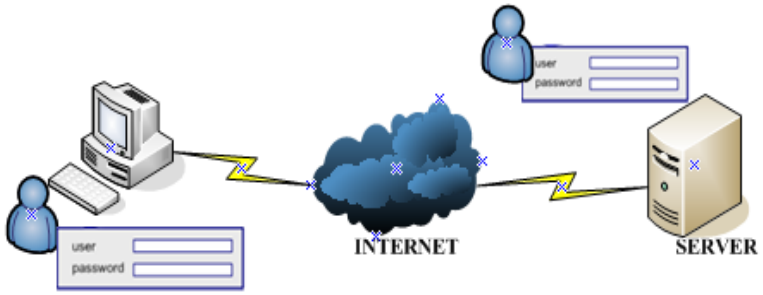
- *CHAP* (Challenge Hanshake Authentication Protocol): Dùng để mã hóa mật khẩu khi đăng nhập, dùng phương pháp chứng thực thử thách/hồi đáp. Định kỳ kiểm tra lại các định danh của kết nối sử dụng cơ chế bắt tay 3 bước và thông tin bí mật được mã hóa sử dụng MD5. Hoạt động của CHAP như sau:



Hình 67 - Hoạt động của CHAP

- *Kerberos:* Kerberos là một giao thức mật mã dùng để xác thực trong các mạng máy tính hoạt động trên những đường truyền không an toàn. Giao thức Kerberos có khả năng chống lại việc nghe lén hay gửi lại các gói tin cũ và đảm bảo tính toàn vẹn của dữ liệu. Mục tiêu khi thiết kế giao thức này là nhằm vào mô hình máy chủ-máy khách (client-server) và đảm bảo nhận thực cho cả hai chiều.

Kerberos hoạt động sử dụng một bên thứ ba tham gia vào quá trình nhận thực gọi là key distribution center – KDC (KDC bao gồm hai chức năng: "máy chủ xác thực" (authentication server - AS) và "máy chủ cung cấp vé" (ticket granting server - TGS). "Vé" trong hệ thống Kerberos chính là các chứng thực chứng minh nhận dạng của người sử dụng.). Mỗi người sử dụng trong hệ thống chia sẻ một khóa chung với máy chủ Kerberos. Việc sở hữu thông tin về khóa chính là bằng chứng để chứng minh nhận dạng của một người sử dụng. Trong mỗi giao dịch giữa hai người sử dụng trong hệ thống, máy chủ Kerberos sẽ tạo ra một khóa phiên dùng cho phiên giao dịch đó.



Hình 68- Mã hóa Kerberos

- Chứng chỉ (Certificates): Một Server (Certificates Authority - CA) tạo ra các certificates.

  – Có thể là vật lý: smartcard
  – Có thể là logic: chữ ký điện tử

Sử dụng public/private key (bất cứ dữ liệu nào được mã hóa bằng public key chỉ có thể giải mã bằng private key). Sử dụng "công ty thứ 3" để chứng thực. Được sử dụng phổ biến trong chứng thực web, smart cards, chữ ký điện tử cho email và mã hóa email.

6.6.4 Bảo mật máy trạm

Sự kiểm tra đều đặn mức bảo mật được cung cấp bởi các máy chủ phụ thuộc chủ yếu vào sự quản lý. Mọi máy chủ ở trong một công ty nên được kiểm tra từ Internet để phát hiện lỗ hổng bảo mật. Thêm nữa, việc kiểm tra từ bên trong và quá trình thẩm định máy chủ về căn bản là cần thiết để giảm thiểu tính rủi ro của hệ thống, như khi firewall bị lỗi hay một máy chủ, hệ thống nào đó bị trục trặc.

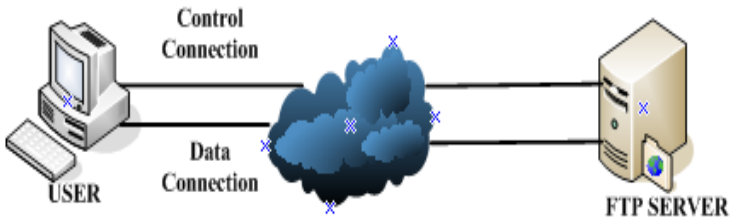
Hầu hết các hệ điều hành đều chạy trong tình trạng thấp hơn với mức bảo mật tối thiểu và có rất nhiều lỗ hổng bảo mật. Trước khi một máy chủ khi đưa vào sản xuất, sẽ có một quá trình kiểm tra theo một số bước nhất định. Toàn bộ các bản sửa lỗi phải được cài đặt trên máy chủ, và bất cứ dịch vụ không cần thiết nào phải được loại bỏ. Điều này làm tránh độ rủi ro xuống mức thấp nhất cho hệ thống.

Việc tiếp theo là kiểm tra các log file từ các máy chủ và các ứng dụng. Chúng sẽ cung cấp cho ta một số thông tin tốt nhất về hệ thống, các tấn công bảo mật. Trong rất nhiều trường hợp, đó chính là một trong những cách để xác nhận quy mô của một tấn công vào máy chủ.

6.6.5 Bảo mật truyền thông

Tiêu biểu như bảo mật trên FTP, SSH..

- Bảo mật truyền thông FTP



Hình 69- Bảo mật FTP

FTP là giao thức lớp ứng dụng trong bộ giao thức TCP/IP cho phép truyền dữ liệu chủ yếu qua port 20 và nhận dữ liệu tại port 21, dữ liệu được truyền dưới dạng clear-text, tuy nhiên

nguy cơ bị nghe lén trong quá trình truyền file hay lấy mật khẩu trong quá trình chứng thực là rất cao, thêm vào đó user mặc định Anonymous không an toàn tạo điều kiện cho việc tấn công tràn bộ đệm.

Biện pháp đặt ra là sử dụng giao thức S/FTP (S/FTP = FTP + SSL/TSL) có tính bảo mật vì những lí do sau:

- Sử dụng chứng thực RSA/DSA .
- Sử dụng cổng TCP 990 cho điều khiển, cổng TCP 989 cho dữ liệu.
- Tắt chức năng Anonymous nếu không sử dụng.
- Sử dụng IDS để phát hiện tấn công tràn bộ đệm.
- Sử dụng IPSec để mã hóa dữ liệu.

➢ Bảo mật truyền thông SSH

SSH là dạng mã hóa an toàn thay thế cho telnet, rlogin..hoạt động theo mô hình client/server và sử dụng kỹ thuật mã hóa public key để cung cấp phiên mã hóa, nó chỉ cung cấp khả năng chuyển tiếp port bất kỳ qua một kết nối đã được mã hóa. Với telnet hay rlogin quá trình truyền username và password dưới dạng cleartext nên rất dễ bị nghe lén, bằng cách bắt đầu một phiên mã hóa.

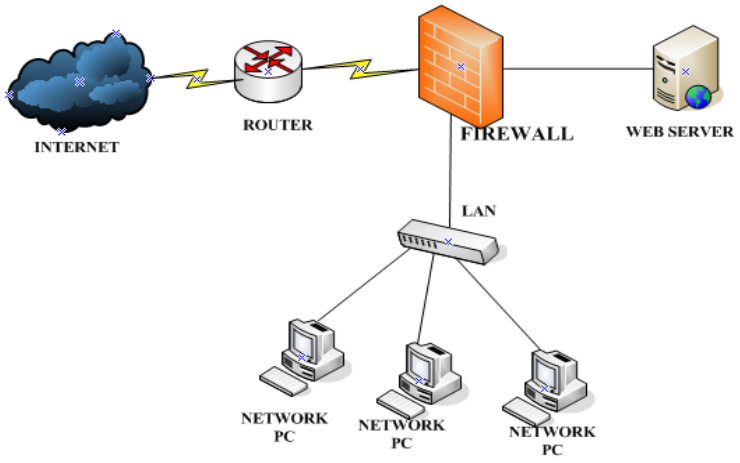
Khi máy client muốn kết nối phiên an toàn với một host, client phải bắt đầu kết nối bằng cách thiết lập yêu cầu tới một phiên SSH. Một khi server nhận dược yêu cầu từ client, hai bên thực hiện cơ chế three-way handshake trong đó bao gồm việc xác minh các giao thức, khóa phiên sẽ được thay đổi giữa client và server, khi khóa phiên đã trao đổi và xác minh đối với bộ nhớ cache của host key, client lúc này có thể bắt đầu một phiên an toàn.

6.6.6 Các công nghệ và kỹ thuật bảo mật

a. Bảo mật bằng firewall

Là một hàng rào giữa hai mạng máy tính, nó bảo vệ mạng này tránh khỏi sự xâm nhập từ mạng kia, đối với những doang nghiệp cỡ vừa là lớn thì việc sử dụng firewall là rất cần thiết, chức năng chính là kiểm soát luồng thông tin giữa mạng cần bảo vệ và Internet thông qua các chính sách truy cập đã được thiết lập.

Firewall có thể là phần cứng, phần mềm hoặc cả hai. Tất cả đều có chung một thuộc tính là cho phép xử lý dựa trên địa chỉ nguồn, bên cạnh đó nó còn có các tính năng như dự phòng trong trường hợp xảy ra lỗi hệ thống.

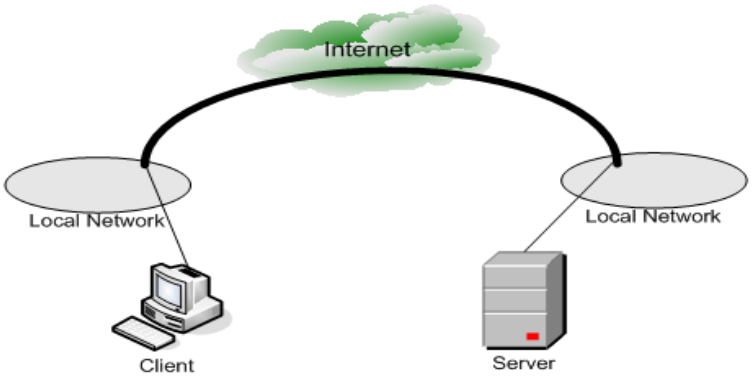


Hình 70 - Mô hình tổng quát firewall

Do đó việc lựa chọn firewall thích hợp cho một hệ thống không phải là dễ dàng. Các firewall đều phụ thuộc trên một môi trường, cấu hình mạng, ứng dụng cụ thể. Khi xem xét lựa chọn một firewall cần tập trung tìm hiểu tập các chức năng của firewall như tính năng lọc địa chỉ, gói tin.

b. Bảo mật bằng VPN (Vitual Private Network)

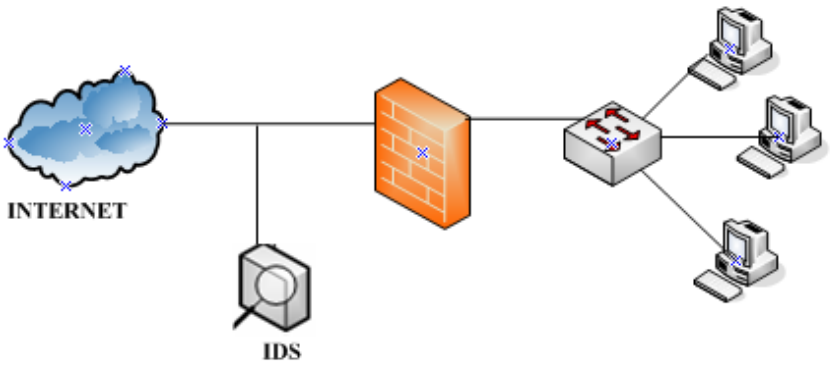
VPN là một mạng riêng ảo được kết nối thông qua mạng công cộng cung cấp cơ chế bảo mật trong một môi trường mạng không an toàn. Đặc điểm của VPN là dữ liệu trong quá trình truyền được mã hóa, người sử dụng đầu xa được chứng thực, VPN sử dụng đa giao thức như IPSec, SSL nhằm tăng thêm tính bảo mật của hệ thống, bên cạnh đó tiết kiệm được chi phí trong việc triển khai.



Hình 71 - Bảo mật bằng VPN

Bảo mật bằng IDS (Phát hiện tấn công)

IDS (Intrusion Detection System) là hệ thống phát hiện xâm nhập, hệ thống bảo mật bổ sung cho firewall với công nghệ cao tương đương với hệ thống chuông báo động được cấu hình để giám sát các điểm truy cập có thể theo dõi, phát hiện sự xâm nhập của các attacker. Có khả năng phát hiện ra các đoạn mã độc hại hoạt động trong hệ thống mạng và có khả năng vượt qua được firewall. Có hai dạng chính đó là network based và host based



Hình 72 - Hệ thống chống xâm nhập IDS

6.7 MỘT SỐ GIAO THỨC AN NINH TRÊN INTERNET

6.7.1 Giao thức SSL (Secure Socket Layer)

SSL là giao thức cung cấp truyền tin cậy giữa các thiết bị đầu cuối. SSL record cung cấp các dịch vụ an ninh cơ bản cho các giao thức tầng trên trong đó có HTTP. HTTP là giao thức cung cấp dịch vụ trên môi trường web giữa client và server. Các thành phần của SSL gồm ba giao thức tầng cao hơn: Handshake Protocol, The Change Cipher Spec Protocol và Alert Protocol. Hai khái niệm cơ bản của SSL là SSL session (phiên làm việc) và SSL connection (SLL liên kết).

- *Liên kết* : cung cấp dịch vụ thích hợp. Các liên kết trong SSL là các quan hệ ngang hàng. Các liên kết là tạm thời và được kết hợp với các phiên.
- *Phiên làm việc* : Một phiên làm việc của SSL là một sự kết hợp của client và server. Một phiên được tạo ra bởi giao thức Handshake Protocol. Các phiên xác định một tập các tham số an toàn bảo mật mà có thể được chia sẻ trong các liên kết. Giữa các cặp thành phần (ví dụ client và server) có thể có nhiều liên kết. Các phiên có thể được thực hiện đồng thời giữa các thành phần.

a. SSL Record

Giao thức SSL Record cung cấp hai dịch vụ cho SSL liên kết:

- Tính bảo mật: Giao thức Handshake Protocol xác định khóa bí mật được chia sẻ sử dụng cho mã hóa dữ liệu.
- Tính toàn vẹn: Giao thức Handshake Protocol xác định khóa bí mật được chia sẻ sử dụng để tạo mã xác thực thông tin.

Hoạt động của SSL Record:

- Truyền dữ liệu: chia dữ liệu thành các phần nhỏ, nén dữ liệu, tạo mã xác thực, mã hóa, đặt tiêu đề (header) và truyền các phần dữ liệu.
- Nhận dữ liệu: Giải mã, xác thực, giải nén, hợp nhất dữ liệu và truyền dữ liệu lên tầng trên.

b. The Change Cipher Spec Protocol

The Change Cipher Spec Protocol là giao thức đơn giản nhất trong ba giao thức của SSL. Giao thức này gồm một thông điệp chứa một byte đơn với giá trị 1. Mục đích của byte này để thể hiện trạng thái hiện tại.

c. Alert Protocol

Giao thức Alert Protocol sử dụng để chuyển các cảnh báo đến các thực thể ngang hàng. Mỗi thông điệp của giao thức này gồm 2 byte. Byte đầu tiên chứa các giá trị 1 hoặc 2 để thông báo mức độ nghiêm trọng. Nếu byte này có giá trị 2 thì SSL kết thúc liên kết hiện tại ngay lập tức. Các liên kết khác trong cùng phiên có thể tiếp tục nhưng không thiết lập thêm các liên kết mới. Byte thứ hai chứa các mã cảnh báo đặc biệt.

d. Handshake Protocol

Phần phức tạp nhất của SSL là giao thức Handshake Protocol. Giao thức này cho phép server và client xác thực lẫn nhau và thỏa thuận thuật toán và khóa mã hóa để bảo vệ dữ liệu. Giao thức Handshake Protocol được sử dụng trước khi truyền dữ liệu.

Giao thức Handshake protocol gồm bốn giai đoạn:

- Giai đoạn 1: Thiết lập. Giai đoạn này thiết lập liên kết logic và mức độ bảo mật giữa server và client.
- Giai đoạn 2: Xác thực server và trao đổi khóa. Server được xác thực trong giai đoạn này và nó tạo một khóa công cộng gửi cho client.
- Giai đoạn 3: Xác thực client và trao đổi khóa. Client kiểm tra các thông tin nhận được từ server. Client gửi cho server một thông điệp xác nhận trạng thái thông tin mà nó nhận được. Sau đó client gửi tiếp một thông điệp mà nội dung phụ thuộc vào kiểu khóa trao đổi.
- Giai đoạn 4: Kết thúc. Client gửi một thông điệp kết thúc bao gồm các thuật toán mới, các khóa và các bí mật. Thông điệp kết thúc cũng thông báo quá trình trao đổi khóa và xác thực đã thành công.

6.7.2 Giao thức HTTPS

Giao thức HTTPS là sự kết hợp giữa hai giao thức HTTP và SSL hoặc TLS để đảm bảo an toàn trong truyền thông giữa web server và web browser.

- Khởi tạo liên kết : Client khởi tạo một liên kết với server trên cổng thích hợp sau đó gửi một thông điệp TSL ClientHello để bắt đầu thử tục "bắt tay". Khi thủ tục "bắt tay" kết thúc, client có thể khởi tạo yêu cầu HTTP đầu tiên. Một liên kết của HTTPS có ba mức: Ở tầng HTTP, HTTP client yêu cầu một liên kết với HTTP server bằng việc gửi một yêu cầu đến tầng thấp nhất tiếp theo là TCP hoặc SSL/TLS. Ở tầng TLS, một phiên được thiết lập giữa TLS client và TLS server. Một yêu cầu TLS được thực hiện thì cần một liên kết giữa một thực thể TCP client và TCP server.
- Đóng liên kết: HTTP client hoặc HTTP server có thể yêu cầu đóng liên kết. Việc đóng kết nối ở HTTP cũng yêu cầu đóng liên kết giữa các thực thể ở tầng TLS và cũng sẽ đóng liên kết ở tầng TCP. Quá trình đóng liên kết ở các tầng TLS và TCP được thực hiện bằng cách gửi các thông điệp yêu cầu "đóng liên kết" giữa các thực thể ở mỗi tầng.

6.7.3 Giao thức SSH (Secure Shell)

SSH là giao thức truyền thông an toàn trên mạng. SSH được thiết kế đơn giản và không đắt khi cài đặt. Phiên bản đầu tiên SSH1 tập trung vào đăng nhập từ xa an toàn thay cho Telnet và các đăng nhập khác mà không an toàn. SSH cũng có thể sử dụng cho truyền file hoặc email. SSH phiên bản 2 xem xét một số lỗ hổng bảo mật.

SSH client và server được ứng dụng rộng rãi trong các hệ điều hành. Nó trở thành phương thức được lựa chọn cho các đăng nhập từ xa và trở thành một trong các ứng dụng phổ biến nhất cho công nghệ mã hóa bên ngoài hệ thống nhúng. SSH gồm ba giao thức SSH Transport layer protocol, SSH User authentication protocol và SSH connection protocol. Các giao thức này chạy phía trên giao thức TCP.

6.7.3.1. Giao thức SSH Transport Layer Protocol

Xác thực server xảy ra ở tầng giao vận trên trên cơ sở server xử lý cặp khóa công khai/riêng. Một server có thể có nhiều khóa sử dụng các thuật toán mã hóa bất đối xứng khác nhau. Nhiều máy có thể có chung khóa. Trong trường hợp bất kỳ, khóa của server được sử dụng trong trao đổi khóa để xác thực danh tính của client. Trong trường hợp này, client phải biết khóa công khai của server.

Trao đổi dữ liệu giữa client và server được thực hiện khi đã tạo một liên kết TCP giữa client và server. Quá trình trao đổi dữ liệu bao gồm một số bước. Đầu tiên là trao đổi định danh (identification string exchange) giữa client và server. Client gửi cho server một mã định danh. Nhận được mã định danh này, server gửi trả lời client mã định danh của nó. Tiếp theo, server và client thỏa thuận về các thuật toán bao gồm trao đổi khóa, thuật toán mã hóa, thuật toán xác thực và thuật toán nén. Bước tiếp đến là trao đổi khóa. Sau bước này client và server chia sẻ với nhau khóa chính và server đã được xác thực bởi client. Bước tiếp theo là kết thúc trao đổi khóa được thực hiện bởi một thông điệp giữa client và server. Cuối cùng là yêu cầu

dịch vụ. Client có thể gửi yêu cầu đến User Authentication hoặc Connnection Protocol. Dữ liệu này được mã hóa cũng như xác thực.

Tạo khóa: Các khóa dùng để mã hóa và xác thực được tạo từ khóa bí mật, giá trị hàm băm từ sự trao đổi khóa và số hiệu của phiên làm việc.

6.7.3.2. Giao thức xác thực người dùng (User authentication protocol)

Giao thức này cung cấp sự xác thực người dùng của server.

Server yêu cầu một trong số các phương thức xác thực như sau:

- *Khóa công kha*i: Client gửi một thông điệp chứa khóa công khai được ký bởi khóa riêng của client tới server. Khi server nhận được thông điệp này nó kiểm tra xem khóa có thể được chấp nhận cho xác thực hay không. Nếu được, nó kiểm tra chữ ký là đúng hay không.
- *Mật khẩu:* client gửi một mật khẩu được mã hóa bởi giao thức Transport layer protocol đến server.
- *Xác nhận máy* (Hostbased): Xác thực được thực hiện trên máy của client. Do đó một máy có nhiều client sẽ được xác thực cho tất cả các client của máy. Client gửi chứ ký được tạo bởi khóa riêng của máy. Bởi vậy, thay vì xác nhận định danh của user, SSH xác nhận định danh của máy.

6.7.3.3. Giao thức liên kết (Connnection Protocol)

SSH Connnection Protocol chạy phía trên của SSH transport layer protocol và đảm nhiệm xác thực các liên kết.

- *Cơ chế kênh truyền*: Các loại truyền sử dụng SSH được hỗ trợ sử dụng kênh riêng biệt. Mỗi phía có thể mở một kênh. Với mỗi kênh, mỗi phía kết hợp với một số hiệu duy nhất. Các kênh được điều khiển bằng cơ chế cửa sổ. Dữ liệu chỉ được truyền khi không gian của cửa sổ là sẵn sàng. Vòng đời của một kênh có ba giai đoạn: mở kênh, truyền dữ liệu và đóng kênh.
- *Các loại kênh:* Bốn loại được sử dụng trong SSH connection protocol.
- *Phiên* (Phiên làm việc): cho phép thực hiện các chương trình ở xa. Chương trình có thể là các ứng dụng như truyền file, email, một lệnh hệ thống hay hệ thống con tích hợp. Khi một phiên của kênh được mở thì có thể bắt đầu thực hiện các chương trình ở xa.
- *Cổng chuyển tiếp*: Một trong những đặc trưng được sử dụng nhiều nhất trong SSH là cổng chuyển tiếp. Cổng chuyển tiếp có khả năng chuyển bất kỳ một liên kết TCP không an toàn sang một liên kết SSH an toàn. Một cổng là một định danh của người dùng của TCP. Bởi vậy bất cứ ứng dụng nào chạy trên TCP đều có một số hiệu cổng.

Dữ liệu đến ở TCP được phân phát tới ứng dụng thích hợp dựa trên số hiệu cổng. SSH hỗ trợ hai loại cổng chuyển tiếp: công chuyển tiếp địa phương và cổng chuyển tiếp ở xa. Cổng chuyển tiếp địa phương cho phép chuyển lưu lượng tầng ứng dụng từ liên kết TCP không an toàn sang dạng "đường ống" SSH an toàn.

- *Cổng chuyển tiếp ở xa*: Client nhận được một luồng dữ liệu với một số hiệu cổng đích nó đặt luồng dữ liệu vào đúng cổng và gửi đến đích.

6.7.4 Giao thức IPsec (IP Security Protocol)

Vào năm 1994, ban kiến trúc Internet đã công bố một bản báo cáo với nhan đề "An ninh trong kiến trúc Internet". Báo cáo đã chỉ ra những vùng chính cho cơ chế an ninh Internet. Hai trong số đó là an ninh cho cơ sở hạ tầng mạng bằng việc kiểm soát, điều khiển luồng dữ liệu và đảm bảo an toàn dữ liệu giữa các thiết bị đầu cuối dựa trên cơ chế xác thực và mã hóa. Để đảm bảo an ninh, IP thế hệ mới bao gồm cơ chế xác thực và mã hóa. Điều đó có nghĩa là những nhà cung cấp đã đưa IPsec vào sản phẩm của họ.

6.7.4.1. Ứng dụng của IPsec

IPsec đảm bảo an ninh khi truyền qua LAN, WAN, Internet bao gồm:

- An toàn kết nối giữa các chi nhánh qua Internet: Một công ty có thể xây dựng một mạng riêng ảo an toàn qua Internet hoặc WAN. Điều này cho phép các hoạt động diễn ra trên Internet giúp tiết kiệm chi phí.
- *An toàn kết nối từ xa qua Internet:* Người dùng ở xa của những hệ thống được trang bị IPsec có thể truy cập mạng một cách an toàn và giảm chi phí đi lại của nhân viên.
- *Thiết lập kết nối Extranet và Intranet với các đối tác:* IPsec có thể sử dụng để đảm bảo an toàn truyền thông với các tổ chức khác, đảm bảo tính xác thực, bảo mật và cung cấp cơ chế trao đổi khóa.
- *Nâng cao an ninh thương mại điện tử:* IPsec cho phép nâng cao độ an toàn trong thương mại điện tử. Nó đảm bảo rằng luồng dữ liệu được thiết kế bởi người quản trị được xác thực và mã hóa.

6.7.4.2. Lợi ích của IPsec

Khi IPsec được cài trong tường lửa (firewall) hoặc bộ định tuyến(router) nó cung cấp một mức độ an toàn cao

IPsec trong firewall để ngăn chặn những luồng dữ liệu bất hợp pháp từ Internet vào một tổ chức.

IPsec nằm phía dưới tầng giao vận (TCP, UDP) và trong suốt với các ứng dụng. Khi cài IPsec trong firewall hoặc bộ định tuyến không cần phải thay đổi phần mềm trên server hoặc user. Thậm chí cài IPsec trên hệ thống user thì các phần mềm ở tầng cao hơn (gồm các ứng dụng) không bị ảnh hưởng.

IPsec có thể cung cấp sự an toàn cho những người dùng độc lập. Điều này có ích cho việc thiết lập an ninh cho các mạng con ảo trong một tổ chức.

Các ứng dụng trong định tuyến: IPsec có vai trò sống còn trong kiến trúc định tuyến được yêu cầu cho kết nối liên mạng. IPsec có thể đảm bảo rằng:

- Quảng bá bộ định tuyến từ một bộ định tuyến được ủy quyền.
- Quảng bá hàng xóm từ một bộ định tuyến được ủy quyền.
- Không bị giả mạo khi cập nhật sự định tuyến

6.7.4.3. Các dịch vụ của IPsec

IPsec cung cấp các dịch vụ an ninh ở tầng IP bằng cách cho phép các hệ thống chọn giao thức an ninh theo yêu cầu, xem xét các thuật toán sử dụng cho các dịch vụ và đặt các khóa mã hóa vào nơi được yêu cầu. Hai giao thức cung cấp dịch vụ an ninh là: giao thức xác thực được chỉ định bởi tiêu đề của giao thức (Authentication Header-AH) và giao thức kết hợp mã hóa/xác thực được chỉ định bởi khuôn dạng của gói tin (Encapsulating Security Payload-ESP). Chuẩn RFC 4301 liệt kê các dịch vụ sau:

- Điều khiển truy cập
- Tính toàn vẹn
- Xác thực nguồn gốc dữ liệu
- Xóa gói tin bị lặp
- Tính bảo mật

6.7.4.4 Chế độ giao vận(Transport) và đường ống(Tunel)

AH và ESP hỗ trợ hai chế độ truyền thông và đường ống:

- *Chế độ giao vận*(Transport): Chế độ giao vận cung cấp sự bảo vệ cơ bản cho các giao thức tầng trên. Chế giao vận cũng bảo vệ cho dữ liệu trong trường Payload của gói tin. Chế độ này cung cấp sự bảo vệ truyền thông giữa hai thiết bị đầu cuối. Khi một máy dùng AH hoặc ESP trên IPv4 thì dữ liệu của gói tin IP trong payload theo sau tiêu đề (IP header). Với IPv6, dữ liệu theo sau cả hai tiêu đề IP (IP header) và tiêu đề mở rộng IPv6. ESP trong chế độ giao vận mã hóa và xác thực dữ liệu nhưng không mã hóa và xác thực tiêu đề. AH trong chế độ giao vận xác thực dữ liệu của gói tin IP và cổng được chọn của tiêu đề.
- *Chế độ đường ống* (Tunnel): Chế độ đường ống bảo vệ toàn bộ gói tin IP. Để thực hiện điều này, sau khi trường ESP và AH được thêm vào gói tin IP thì toàn bộ gói tin và các trường an ninh (security fields) được xem như trường payload của gói tin IP ngoài mới và có một tiêu đề IP ngoài mới. Toàn bộ gói tin gốc đi qua một đường ống giữa đầu này và đầu kia của mạng. Bởi vì gói tin gốc được đóng gói nên gói tin mới

kích thước to hơn có thể có địa chỉ nguồn và đích khác. Chế độ đường ống được sử dụng khi một trong hai đầu cuối hoặc cả hai đầu của sự kết hợp an ninh (security association-SA) là một cổng an toàn như tường lửa(firewall) hoặc router được cài IPsec. Với chế độ đường ống, các máy của mạng phía sau tường lửa có thể tham gia vào truyền thông an toàn mà không cần cài IPsec. Các gói tin không được bảo vệ được tạo bởi các máy như vậy được truyền qua đường ống qua các mạng bên ngoài theo cơ chế đường ống. Các SA được thiết lập bởi phần mềm IPsec dạng tường tửa(firewall) hoặc bộ định tuyến an toàn(security router) ở đường biên của mạng cục bộ.

ESP trong chế độ đường ống mã hóa và xác thực toàn bộ gói dữ liệu IP bên trong bao gồm cả tiêu đề IP bên trong. AH trong chế đường ống xác thực dữ liệu của gói tin IP bên trong và cổng được chọn của tiêu đề bên ngoài.

6.7.4.5. Chính sách an ninh của IPsec

Chính sách an ninh của IPsec là sự an toàn của mỗi gói tin được truyền từ nguồn đến đích. Chính sách của IPsec là sự tương tác giữa cơ sở dữ liệu an ninh kết hợp (Security Association Database-SAD) và cơ sở dữ liệu chính sách an ninh (Security Policy Database).

6.7.4.6. An ninh kết hợp (Security Association-SA)

An ninh kết hợp là sự kết hợp của hai cơ chế xác thực và mã hóa. Một sự kết hợp là kết nối logic một chiều giữa nơi gửi và nơi nhận mà đảm bảo an toàn cho luồng giữ liệu. Nếu mối quan hệ ngang hàng cần thiết cho sự trao đổi hai chiều an toàn thì hai an ninh kết hợp được yêu cầu.

An ninh kết hợp được xác định bởi ba tham số:

- Chỉ số của tham số an ninh (Security Parameter Index-SPI): Một bit dạng string được gán cho SA và chỉ có ý nghĩa địa phương. SPI được đặt trong tiêu đề AH và ESP cho phép hệ thống nhận chọn SA mà gói tin nhận được sẽ được xử lý.
- Địa chỉ đích IP: Đây là địa chỉ đích của SA mà có thể là một hệ thống người dùng hoặc một hệ thống như tường lửa hoặc bộ định tuyến.
- Trường định danh giao thức an ninh (Security Protocol Identifier): Trường này chỉ ra có hay không an ninh kết hợp là AH hay ESP.

6.7.4.7. Cơ sở dữ liệu an ninh kết hợp

Trong mỗi cài đặt IPsec có một cơ sở dữ liệu an ninh kết hợp mà định nghĩa các tham số kết hợp với mỗi SA. Một an ninh kết hợp bao gồm các tham số sau:

- Chỉ số của tham số an toàn(Security Parameter Index): Là một giá trị 32 bit được chọn bởi phía nhận của một SA để xác định duy nhất SA.

- Bộ đếm số thứ tự: Một giá trị 32 bit dùng để tạo trường số thứ tự trong tiêu đề của AH và ESP.
- Sự tràn bộ đếm thứ tự: Một cờ chỉ ra có hay không sự tràn của bộ đếm số thứ tự tạo ra một sự kiện có thể kiểm tra hoặc ngăn chặn sự truyền thêm gói tin trên SA.
- Cửa sổ chống phát lại: Sử dụng để xem xét có hay không gói tin AH hay ESP bên trong là một sự phát lại.
- Thông tin AH: Thuật toán xác thực, các khóa, vòng đời của khóa và các tham số khác được sử dụng với AH.
- Thông tin ESP: Các thuật toán mã hóa và xác thực, các khóa, các giá trị khởi tạo, vòng đời của khóa và các tham số khác được sử dụng với ESP.
- Vòng đời của an ninh kết hợp: Khoảng thời gian mà một SA được thay thế bằng một SA mới hoặc kết thúc.
- Chế độ giao thức IPsec: kiểu đường ống, truyền(transport) hay wildcard.
- Kích thước gói tin lớn nhất: Là kích thước lớn nhất của gói tin mà không phải phân mảnh khi truyền.

6.7.4.8 Cơ sở dữ liệu chính sách an ninh (Security Policy Database-SPD)

Một SPD gồm các thực thể mà mỗi trong chúng xác định một tập con của luồng dữ liệu IP và các điểm đến SA cho luồng đó. Trong môi trường phức tạp hơn, có thể có nhiều thực thể có quan hệ với một SA đơn hoặc nhiều SA kết hợp với một thực thể SPD đơn. Mỗi thực thể SPD được xác định bởi một tập IP và các giá trị trong trường giao thức tầng trên.

- Xử lý gói tin IP: Mỗi gói tin IP bên ngoài được xử lý bởi IPsec trước khi truyền. Mỗi gói tin IP bên trong được xử lý sau khi nhận được và trước khi truyền nội dung lên tầng cao hơn.
- Trao đổi khóa: Quản lý khóa của IPsec bao gồm sự xác định và phân bố khóa bí mật. Yêu cầu điển hình là bốn khóa cho truyền giữa hai ứng dụng: tính bảo mật và toàn vẹn trong truyền và nhận. Kiến trúc IPsec hỗ trợ hai loại quản lý khóa:
  - Thủ công: Người quản lý hệ thống đặt cho mỗi hệ thống một khóa riêng. Cách này chỉ có thể thực hiện với môi trường tương đối nhỏ và tĩnh.
  - Tự động: Hệ thống tự động cho phép tạo các khóa cho các SA và làm cho sử dụng khóa thuận tiện trong các hệ thống phân tán. Giao thức quản lý khóa tự động cho IPsec là ISAKMP/Oakley.
- Giao thức xác định khóa Oakley: là giao thức trao đổi khóa trên cơ sở thuật toán Diffie-Hellman nhưng sự an toàn cao hơn.

- Giao thức quản lý khóa và an ninh kết hợp (SAKMP): SAKMP cung cấp một nền tảng cho quản lý khóa và hỗ trợ cho các giao thức riêng biệt như định dạng và các thuộc tính an toàn.

BÀI TẬP CHƯƠNG VI

Bài 1: Tham khảo hình sau. Hai phát biểu nào sau đây đúng với định tuyến trên VLAN?

A. Máy E và máy F có cùng default gateway

B. Router1 và Switch2 phải được kết nối bằng cáp chéo.

C. Cổng FastEthernet 0/0 trên Router1 phải được cấu hình với sub-interface.

D. Cổng trunk trên FastEthernet 0/0 của Router1 và Switch2 phải được cấu hình cùng kiểu giao thức đóng gói.

Bài 2: Các máy trong cùng một VLAN có thể truyền thông với nhau, nhưng chúng không thể truyền thông với các máy thuộc VLAN khác. Bạn cần phải làm gì để chúng có thể truyền thông với nhau?

A. Router phải được cấu hình sub-interface trên giao tiếp vật lý mà nó được kết nối tới switch.

B. Cấu hình địa chỉ IP trên giao tiếp vật lý của router mà có cổng kết nối tới switch.

C. Cấu hình chế độ trunk cho hai cổng nối giữa hai con switch

D. Cấu hình chế độ access cho hai cổng nối giữa hai con switch

Bài 3: Mục nào sau đây không là tấn công chủ động

A. Tấn công nghe lén B. Tấn công từ chối dịch vụ

C. Tấn công replay D. Tấn công giả mạo

Bài 4: Tiện ích nào sau đây là một phương thức bảo mật truy cập từ xa tốt hơn Telnet:

A. SSL B. SSH C. IPsec D. VPN

Bài 5: Các giao thức nào sau đây làm việc trên lớp IP để bảo vệ thông tin IP trên mạng?

A. IPX B. IPsec C. SSH D. VPN

Bài 6: Thiết bị nào cho phép ta nối đến một mạng LAN của công ty qua internet thông qua một kênh được mã hóa an toàn?

A. WEP B. VPN C. MODEM D. TELNET

TÀI LIỆU THAM KHẢO

[1] Nguyễn Thúc Hải, 1999, *Mạng máy tính và các hệ thống mở,* NXB Giáo dục.

[2] Nguyễn Quốc Cường, 2001, *Internetworking với TCP/IP*, Nxb Giáo dục.

[3] Nguyễn Thế Hùng, 2002, *Mạng và truyền thông dữ liệu*, Nxb Thống kê.

[4] Th.S Đàm Quang Hồng Hải, KS. Nguyễn Bình Dương, 2009, *Giáo trình mạng máy tính*, NXB Đại học Quốc gia TP Hồ Chí Minh.

[5] Hồ Đắc Phương, 2006 , *Mạng máy tính*, NXB Đại học Quốc gia Hà Nội.

[6] Ngô Bá Hùng, Phạm Thế Phi, 2014, *Mạng máy tính*, Nhà xuất bản Đại học Cần Thơ

[7] Andrew S. Tanenbeau, 2003, *Computer Networks*, Fourth Edition, Prentice Hall Inc.

[8] Jim Kurose và Keith Ross, 2010, "*Computer Networking: A top down Approach Futuring the Internet"*, Addison-Wesley, 5rd edition,

[9] W.Stallings, *Cryptography and Network Security Principles and Practice*, 5th Edition