CHƯƠNG 1. TỔNG QUAN VỀ MẠNG MÁY TÍNH

I. CÁC KHÁI NIỆM CƠ BẢN VỀ MẠNG MÁY TÍNH

Mạng máy tính hai hoặc nhiều máy tính được kết nối với nhau để trao đổi thông tin và dùng chung các dữ liệu hay tài nguyên. Mạng máy tính hình thành từ nhu cầu chia sẻ và dùng chung các thông tin giữa các máy tính với nhau.

Ưu điểm của mạng máy tính:

Giảm các chi phí khi dùng chung các tài nguyên mạng bao gồm các thiết bị ngoại vi và dữ liệu

Chuẩn hoá các ứng dụng

Thu thập dữ liệu 1 cách kịp thời

Tăng thời gian làm việc

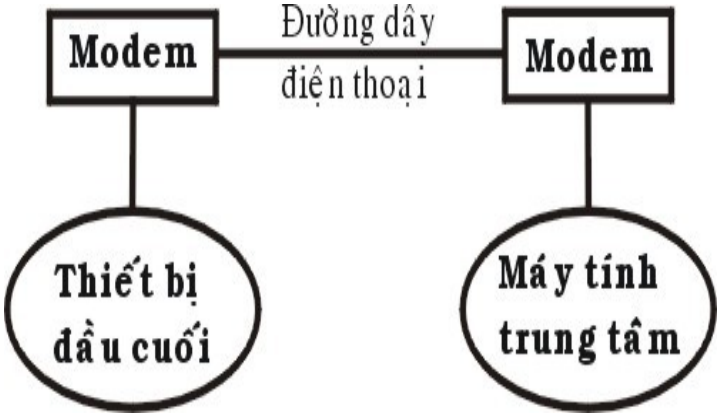
Nhược điểm:

Dễ bị mất mát hay thất lạc thông tin khi truyền hoặc khi thiết lập chế độ bảo mật không tốt.

II. LỊCH SỬ PHÁT TRIỂN CỦA MẠNG MÁY TÍNH NÓI CHUNG

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 đợc truyền thay vì trực tiếp thì thông qua dây điện thoại.



Hình 1.1. Mô hình truyền dữ liệu từ xa đầu tiên

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

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

Thiết bị kiểm soát truyền thông: có nhiệm vụ nhận các bit tín hiệu từ các kênh truyền thông, gom chúng lại thành các byte dữ liệu và chuyển nhóm các byte đó tới máy tính trung tâm để xử lý, thiết bị này cũng thực hiện công việc ngược lại để chuyển tín hiệu trả lời của máy tính trung tâm tới các trạm ở xa. Thiết bị trên cho phép giảm bớt được thời gian xử lý trên máy tính trung tâm và xây dựng các thiết bị logic đặc trưng.

Thiết bị kiểm soát nhiều đầu cuối: cho phép cùng một lúc kiểm soát nhiều thiết bị đầu cuối. Máy tính trung tâm chỉ cần liên kết với một thiết bị như vậy là có thể phục vụ cho tất cả các thiết bị đầu cuối đang được gắn với thiết bị kiểm soát trên. Điều này đặc biệt có ý nghĩa khi thiết bị kiểm soát nằm ở cách xa máy tính vì chỉ cần sử dụng một đường điện thoại là có thể phục vụ cho nhiều thiết bị đầu cuối.

Hình 1.2. Mô hình trao đổi mạng của hệ thống 3270

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

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

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

Từ đó đến nay đã có rất nhiều công ty đưa ra các sản phẩm của mình, đặc biệt khi các máy tính cá nhân được sử dụng một cánh rộng rãi. Khi số lượng máy vi tính trong một văn phòng hay cơ quan được tăng lên nhanh chóng thì việc kết nối chúng trở nên vô cùng cần thiết và sẽ mang lại nhiều hiệu quả cho người sử dụng.

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

Sử dụng chung tài nguyên: Những tài nguyên của mạng (như thiết bị, chương trình, dữ liệu) khi được trở thành các tài nguyên chung thì mọi thành viên của mạng đều có thể tiếp cận được mà không quan tâm tới những tài nguyên đó ở đâu.

Tăng độ tin cậy của hệ thống: Người ta có thể dễ dàng bảo trì máy móc và lưu trữ (backup) các dữ liệu chung và khi có trục trặc trong hệ thống thì chúng có thể được khôi phục nhanh chóng. Trong trường hợp có trục trặc trên một trạm làm việc thì người ta cũng có thể sử dụng những trạm khác thay thế.

Nâng cao chất lượng và hiệu quả khai thác thông tin: Khi thông tin có thể được 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.

Hình 1.3. Sự tiến hoá của các hệ thống mạng máy tính

III. PHÂN LOẠI MẠNG MÁY TÍNH

Với kiểu mạng mainframe và nhiều trạm đầu cuối, máy mainframe đóng vai trò là điểm xử lý ở trung ương, còn các trạm đầu cuối cung cấp các yêu cầu và nhận lại thông tin đã qua xử lý, kiểu bố trí này được gọi là môi trường mạng tập trung (centrialized network environment).

Môi trường mạng phân tán phân bố cân bằng trách nhiệm công việc giữa một máy phục vụ (server) ở trung ương và những máy trạm cho nên mạng này mạnh mẽ hơn mạng tập trung. Môi trường này phản ánh khuynh hướng tránh xa các mainframe và minicomputer và chuyển dịch theo hướng dùng các máy tính cá nhân trơng một mạng máy tính. Có hai mô hình mạng phân tán: mô hình peer-to-peer (mạng nganh hàng) và mô hình client-server (khách hàng/người phục vụ)

+Mô hình Client-Server: không giống môi trường mainframe xử lý tập trung client-server phân tán các tài nguyên và dịch vụ trên toàn mạng. Netware và intraNetware là ví dụ về mạng Client-server, bởi có các Server chuyên tráhc chạy những phần mềm Server đặc biệt và cung cấp các dịch vụ cho các máy khách. 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 1.4. Mô hình mạng Client-Server

+Trong một 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 1.5. Mô hình mạng peer-to-peer

Nếu kết hợp 2 mô hình mạng trên ta được một mô hình mạng pha trộn hay mạng không đồng nhất đó là khả năng tích hợp Netware. Đó là khi mà Novell tích hợp máy tính cá nhân vừa như một Server vừa như một máy trạm vào trong NetWare và Microsoft tích hợp khả năng chạy một mạng peer-to-peer bên trong hệ điều hành đa nhiệm như OS/2 thì sự phân biệt giữa các mạng peer-to-peer và Client-Server đã trở nên mờ nhạt đi.

IV. CÁC DỊCH VỤ MẠNG MÁY TÍNH

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.

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 dồng bộ và không đồng bộ bao gồm các Access Server (máy phục vụ truy cập dồm 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.

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. Để sử dụng dịch vụ này người sử dụng cần mở một hộp thư tại các máy Internet Service Provider (ISP-Cung cấp dịch vụ Internet). Sau khi mở hộp thư người sử dụng được cấp một địa chỉ E-mail và mật khẩu để truy xuất hộp thư của mình. Ngoài ra, máy Client cần có một chương trình Mail Client thích hợp để truyền nhận thư của mình từ hộp thư trên máy Server. Chương trình quản lý hộp thư gọi trên máy Server là Mail Server.

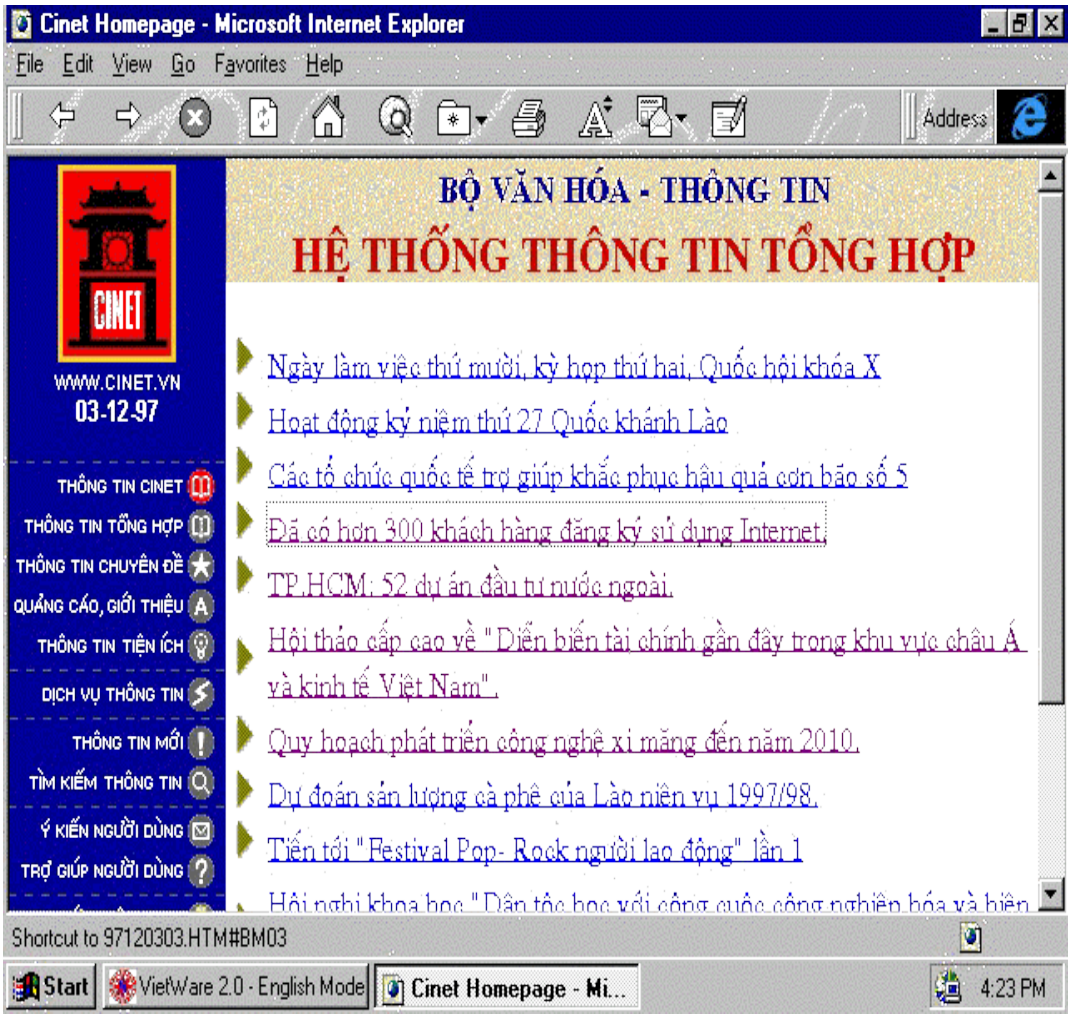
FTP

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, ...

Gopher

Gopher là công cụ được sử dụng rộng rãi trên Internet, đây là chương trình dựa trên menu cho phép duyệt thông tin mà không cần biết tài liệu cụ thể được đặt ở đâu. Nó cho phép tìm kiếm danh sách các tài nguyên và gửi trở lại các tài liệu, nó là một trong những hệ thống duyệt toàn diện nhất và được tích hợp nhằm cho phép truy cập những dịch vụ khác như FTP và Telnet

E-Commerce



Hình 1.6. Ví dụ một trang Web cho phép dễ dàng khai thác các trang Web khác

Internet Telephone

Bạn có thể nói chuyện trực tuyến như thực tế với bất kỳ một người sử dụng nào khác ở bất cứ nơi đâu trên Iternet. Tuy đàm thoại trực tuyến gần như vô ích với những người rất gần nơi đang cư trú nhưng nó lại làm được điều lớn lao với những người ở các lục địa khác nhau đặc biệt là những người không sử dụng tiếng Anh.

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 TCPIP thì gọi là DHCP client, còn các máy cung cấp thông tin của TCPIP gọi là DHCP server. Các máy DHCP server bắt buộc phải là Windows NT server.

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

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

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

- Gán thủ công.
- Gán tự động.
- Gán động.

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

Trong phương pháp gán địa chỉ IP tự động DHCP client được gán địa chỉ IP khi lần đầu tiên nó nối vào mạng. Địa chỉ IP được gán bằng 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

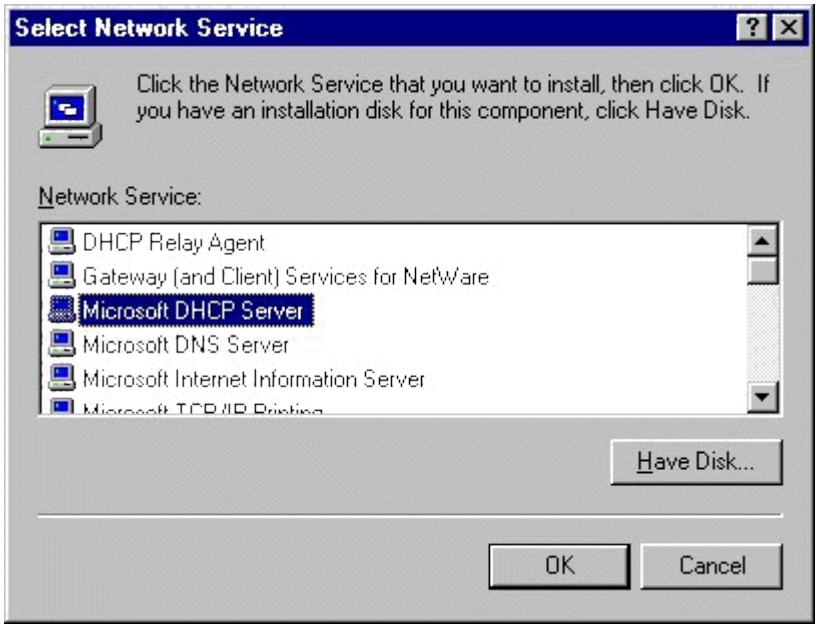
Trong phương pháp gán địa chỉ IP động thì DHCP server gán địa chỉ IP cho DHCP client tạm thời. Sau đó địa chỉ IP này sẽ được DHCP client sử dụng trong một thời gian đặc biệt. Đến khi thời gian này hết hạn thì địa chỉ IP này sẽ bị xóa mất. Sau đó nếu DHCP client cần nối kết vào mạng thì nó sẽ được cấp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



Hình 1.7: Màn hình cài đặt của DHCP

- Chọn tab service và click vào nút Add .
- Ta sẽ thấy một loạt các service của Windows NT server nằm trong hộp hội thoại Select Network Service. Chọn Microsoft DHCP server từ danh sách các service được liệt kê ở phía dưới và nhấn OK và thực hiện các yêu cầu tiếp theo của Windows NT.

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

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.

DNS server được dùng trong các trường hợp sau :

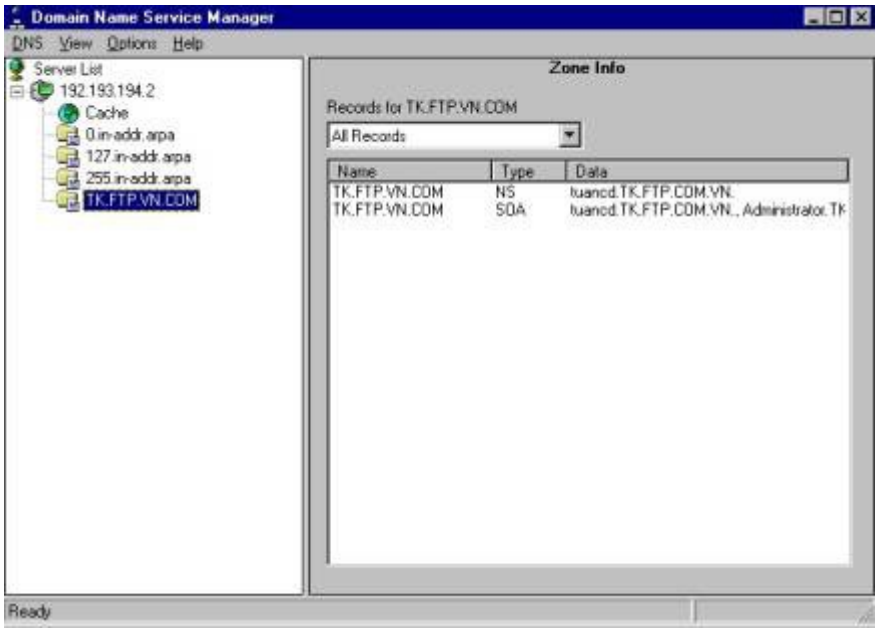
- Chúng ta muốn có 1 tên domain riêng trên Interner để có thể tạo, tách rời các domain con bên trong nó.
- Chúng ta cần 1 dịch vụ DNS để điều khiển cục bộ nhằm tăng tính linh hoạt cho domain cục bộ của bạn.
- Chúng ta cần một bức tường lửa để bảo vệ không cho người ngoài thâm nhập vào hệ thống mạng nội bộ của mình

Có thể quản lý trực tiếp bằng các trình soạn thảo text để tạo và sửa đổi các file hoặc dùng DNS manager để tạo và quản lý các đối tượng của DNS như: Servers, Zone, Các mẫu tin, các Domains, Tích hợp với Win.

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

- Login vào Server với tên Administrator.
- Click hai lần vào icon Network. Ta sẽ thấy hộp hội thoại Network dialog box tương tự như trên và lựa chọn Microsoft DNS Server.

Để cập nhật và khai thác DNS server chúng ta chọn mục DNS manager trong Netwrok Administrator Tools. Hộp hội thoại sau đây sẽ hiện ra



Hình 1.8: Màn hình DNS Manager

Mỗi một tập hợp thông tin chứa trong **DNS database** được coi như là **Resourse record**. Những **Resourse record** cần thiết sẽ được liệt kê dưới đây:

Tên Record	Mô tả
A (Address)	Dẫn đường một tên host computer hay tên của một thiết bị mạng khác trên mạng tới một địa chỉ IP trong DNS zone

CNAME ()	Tạo một tên Alias cho tên một host computer trên mạng
MX ()	Định nghĩa một sự trao đổi mail cho host computer đó
NS (name server)	Định nghĩa tên server DNS cho DNS domain
PTR (Pointer)	Dẫn đường một địa chỉ IP đến tên host trong DNS server zone
SOA (Start of authority)	Hiển thị rằng tên server DNS này thì chứa những thông tin tốt nhất

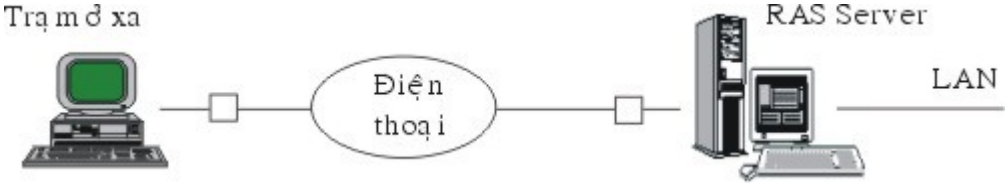
Remote Access Service (RAS)

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. .

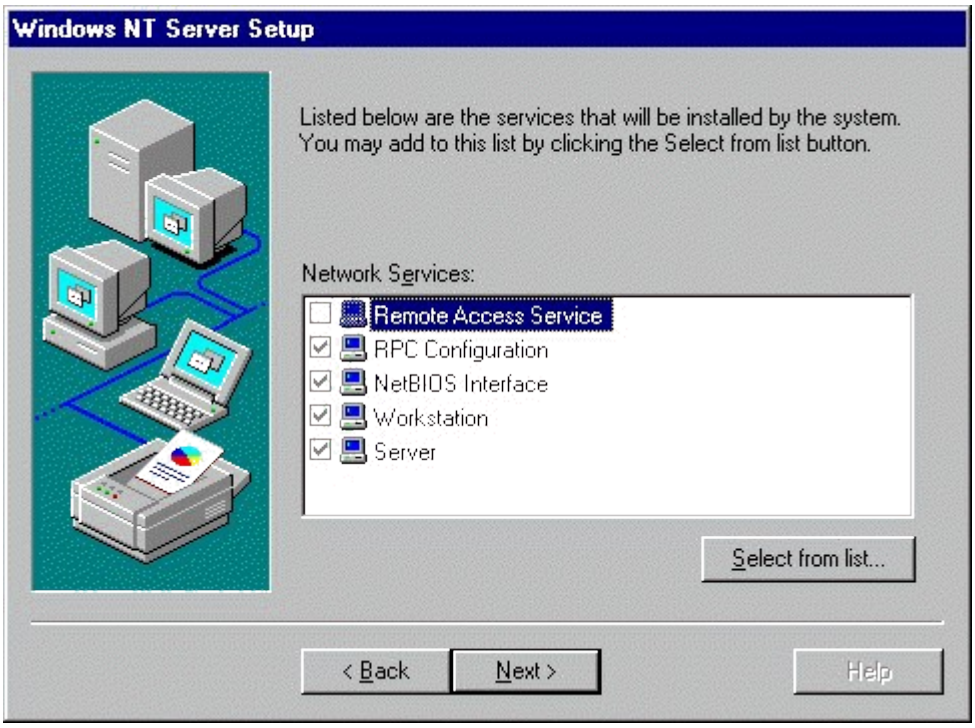
Máy trạm có thể được nối với server có dịch vụ RAS thông qua modem hoặc pull modem, cable null modem (RS232) hoặc X.25 network.

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.



Hình1.9. Mô hình truy cập từ xa bằng dịch vụ RAS

Để cài đặt RAS chúng ta lựa chọn yêu cầu hộp Windows NT server setup hiện ra lúc cài đặt hệ điều hành Windows NT.



Với RAS tất cả các ứng dụng đều thực hiện trên máy từ xa, thay vì kết nối với mạng thông qua card mạng và đường dây mạng thì máy ở xa sẽ liên kết qua modem tới một RAS Server. Tất cả dữ liệu cần thiết được truyền qua đường điện thoại, mặc dù tốc độ truyền qua modem chậm hơn so với qua card mạng nhưng với những tác vụ của LAN không phải bao giờ dữ liệu cũng truyền nhiều.

Với những khả năng to lớn của mình trong các dịch vụ mạng, hệ điều hành Windows NT là một trong những hệ điều hành mạng tốt nhất hiện nay. Hệ điều hành Windows NT vừa cho phép giao lưu giữa các máy trong mạng, vừa cho phép truy nhập từ xa, cho phép truyền file, vừa đáp ứng cho mạng cục bộ (LAN) vừa đáp ứng cho mạng diện rộng (WAN) như Intranet, Internet. Với những khả năng như vậy hiện nay hệ điều hành Windows NT đã có những vị trí vững chắc trong việc cung cấp các giải pháp mạng trên thế giới.

CHƯƠNG 2. CÁC CHUẨN MẠNG VÀ MÔ HÌNH OSI

I. GIỚI THIỆU CÁC CHUẨN MẠNG

Vào tháng 1 năm 1985, Học viện các Kỹ sư điện và điện tử Mỹ (IEEE) đã ban hành đặc tả kỹ thuật Ethernet được đặt tên chính thức là chuẩn "IEEE 802.3 Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Layer and Physical Specifications" và thường được gọi là tiêu chuẩn IEEE 802.3. Tiêu chuẩn này qui định một hệ thống nối mạng xuất phát từ chuẩn Ethernet, nhưng cấu trúc gói của nó thì khác với chuẩn Ethernet gốc. Chuẩn 802.3 cung cấp những khả năng dùng hệ thống cáp mạng bao gồm: cáp đồng trục, cáp sợi quang và cáp xoắn không bọc. Ethernet là công nghệ baseband được thiết kế như một mạng chuyển mạch. Trong một số cách thực hiện chuẩn này, người ta có thể dùng những công nghệ chuyển mạch tốc độ cao bên trong các hub hoặc concentrator để cho phép thực hiện nhiều cuộc trao đổi đồng thời giữa các nút. Chuẩn IEEE 802.x được dùng để giải quyết một số vấn đề liên quan đến các mạng LAN, các chuẩn thông dụng nhất là:

+ 802.1: Qui định về kiến trúc chung của mạng LAN, việc nối kết mạng và quản lý mạng ở cấp độ phần cứng.

+ 802.2: Qui định lớp con LLC (Logical Link Control-Điều khiển liên kết vật lý) dành cho một mạng có topology tuyến tính và phương thức truy cập CSMA/CD.

+ 802.3: Qui định lớp MAC (Medium Access Control-Kiểm soát truy cập truyền thông) dành cho một mạng có topology bus và phương thức truy cập CSMA/CD.

+ 802.4: Qui định lớp MAC dành cho một mạng Token-passing bus.

+ 802.5: Qui định lớp MAC dành cho một mạng Token-ring bus.

+ 802.6: Qui định một MAN dựa trên một vòng cáp quang dài 30 dặm Anh.

+ 802.7: Một báo cáo của nhóm Tư vấn kỹ thuật về các mạng boardband.

+ 802.8: Một báo cáo của TAG về các mạng sợi cáp quang.

+ 802.9: Qui định về việc tích hợp giọng nói và dữ liệu khi truyền.

+ 802.11: Nhóm công tác có liên quan đến việc thiết lập những chuẩn về mạng không dây.

+ 802.12: Một tiêu chuẩn dành cho các mạng Ethernet 100 VG/AnyLAN Ethernet.

Hình 2.1. Mối quan hệ giữa các tiêu chuẩn IEEE 802 và mô hình OSI

II. MÔ HÌNH THAM KHẢO OSI

Để giảm độ phức tạp thiết kế, các mạng được tổ chức thành một cấu trúc đa tầng, mỗi tầng được xây dựng trên tầng trước nó và sẽ cung cấp một số dịch vụ cho tầng cao hơn. Ở mỗi tầng có hai quan hệ: theo chiều ngang và theo chiều dọc. Quan hệ theo chiều ngang nói lên sự hoạt động của các máy tính đồng tầng có nghĩa là chúng phải hội thoại được với nhau trên cùng một tầng. Muốn vậy thì phải có qui tắc để hội thoại mà ta gọi đó là giao thức hay thủ tục (Protocol). Quan hệ theo chiều dọc là quan hệ giữa các tầng kề nhau trong cùng một máy, giữa hai tầng có một giao diện ghép nối, nó xác định các thao tác nguyên thuỷ và các dịch vụ mà tầng dưới cung cấp cho tầng trên, Tình trạng không tương thích giữa các mạng trên thị trường gây nên trở ngại cho người sử dụng các mạng khác nhau. Chính vì thế cần xây dựng một mô hình chuẩn làm cho các nhà nghiên cứu và thiết kế mạng để tao ra các sản phẩm mở về mạng. Việc nghiên cwus sự kết nối hệ thống mở đã được tổ chức tiêu chuẩn Quốc tế đề ra vào tháng 3/1977 với mục tiêu kết nối các hệ thống sản phẩm của các hãng sản xuất khác nhau và phối hợp các hoạt động chuẩn hoá trong lĩnh vực viễn thông-tin học. Và vào năm 1984 tổ chức tiêu chuẩn quốc tế đã công bố mô hình OSI (Open System Interconnections-hệ thống ghép nối hệ thống mở) bao gồm 7 tầng:

Tầng 1 (tầng vật lý-Physical): cung cấp các phương tiện truyền tin, thủ tục khởi động, duy trì huỷ bỏ các liên kết vật lý cho phép truyền các dòng dữ liệu dở dòng bit.

Tầng 2 (tầng liên kết dữ liệu-Data Link): thiết lập, duy trì, huỷ bỏ các liên kết dữ liệu kiểm soát luồng dữ liệu, phát hiện và khắc phục các sai sót truyền tin.

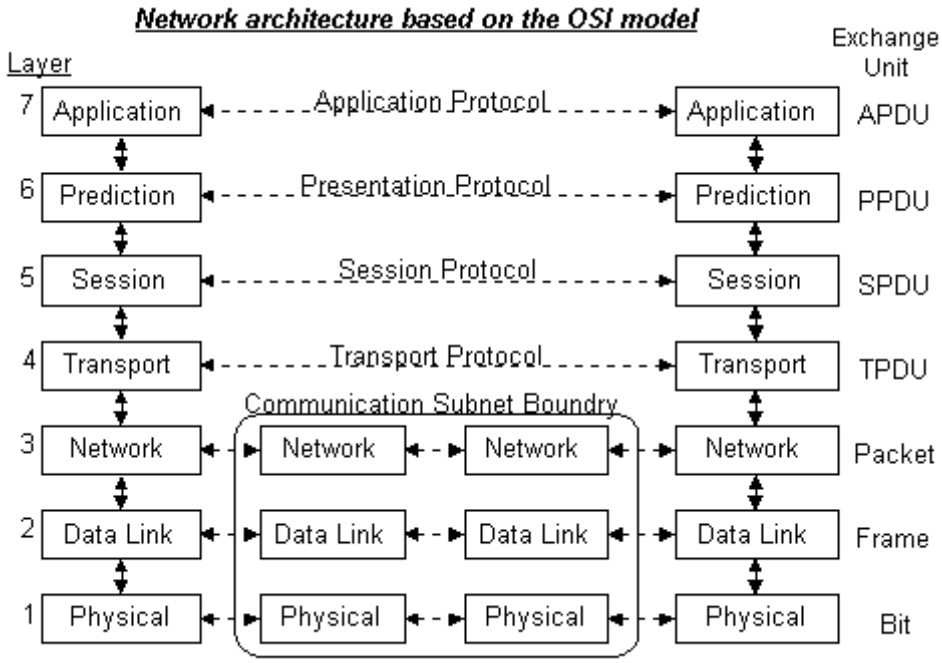
Tầng 3 (tầng mạng-Network): chọn đường truyền tin trong mạng, thực hiện kiểm soát luồng dữ liệu, khắc phục sai sót, cắt hợp dữ liệu.

Tầng 4 (tầng giao vận-Transport): kiểm soát giữa các nút của luồng dữ liệu, khắc phục sai sót, có thể thực hiện ghép kênh và cắt hợp dữ liệu.

Tầng 5 (tầng phiên-Session): thiết lập, duy trì đồng bộ hoá và huỷ bỏ các phiên truyền thông. Liên kết phiên phải được thiết lập thông qua đối thoại và các tham số điều khiển.

Tầng 6 (tầng trình dữ liệu-Presentation): biểu diễn thông tin theo cú pháp dữ liệu của người sử dụng. Loại mã sử dụng và vấn đề nén dữ liệu.

Tầng 7 (tầng áp dụng-Application): là giao diện giữa người và môi trường hệ thống mớ. Xử lý ngữ nghĩa thông tin, tầng này cũng có chức năng cho phép truy cập và quản chuyển giao tệp, thư tín điện tử . . .



Hình 2.2. Mô hình 7 mức OSI

Thủ tục truyền tin trên mạng dựa chủ yếu vào các nghi thức giao thiệp hay giao thức được qui định trước. Tuy nhiên việc liên lạc chỉ xảy ra ở lớp thuộc cấp thấp trên mỗi máy, rồi sau đó truyền dần lên phía trên đến nhưng lớp thích hợp. Như ở bài trước chúng ta đã học cứu qua về mô hình 7 mức OSI, sau đây chúng ta sẽ tìm hiểu xem mô hình OSI hoat động như thế nào. Khái niệm nền tảng của mô hình OSI là dòng lưu chuyển của một yêu cầu truy cập vào một tài nguyên mạng xuyên qua bảy lớp phân biệt. Sự yêu cầu đó khởi đầu từ lớp trên cùng của mô hình. Khi nó lưu chuyển xuống dưới, yêu cầu đó được chuyển đổi từ một lời gọi API (Giao diện lập trình ứng dụng) bên trong ứng dụng xuất phát thành một chuỗi các xung được mã hoá để truyền đi những thông tin nhị phân đến một thiết bị khác trên mạng. Những xung này có thể là điện, quang, từ, vi ba hoặc những tần số sóng mang vô tuyến. Quá trình mã hoá đó cho phép những lớp cụ thể nào đó của mô hình OSI trên một máy tính nguồn để liên lạc với những lớp giống hệt của chúng trên một máy tính đích. Quá trình này được gọi là những giao thức, khi những quá trình này đến đích của chúng, chúng chuyển ngược lên các lớp của mô hình OSI theo chiều ngược với lúc được gửi đi và được giải mã cho tới khi chúng đến lớp có chức năng tương đương ở trên cùng trên máy tính đích. Kết quả của chương trình đó là hai máy phân biệt liên lạc được với nhau và hoạt động một cách độc lập như thể là những tài nguyên được nối mạng đang được truy cập đó không có gì khác biệt như tài nguyên ở trên máy tại chỗ vậy. Mô hình OSI không chỉ rõ rằng giao thức nào sẽ được dùng để truyền dữ liệu ngang qua mạng, mà nó cũng chẳng chỉ định thiết bị dùng được truyền. Thay vì vậy, nó cung cấp một đề cương để các thiết bị khác nhau làm theo để đảm bảo thông tin liên

lạc đúng đắn ngang qua mạng. Vậy việc đóng gói dữ liệu để truyên đi qua mạng thực hiện như thế nào?

Những dữ liệu lưu thông trên mạng nói chung có thể chia làm hai nhóm: các yêu cầu được tạo ra ở máy tính nguồn và các hồ đáp từ nơi mà yêu cầu kia được gửi đến. Đơn vị cơ bản của dữ liệu mạng là gói dữ liệu (packet). Thông tin muốn đi ngang qua một mạng nào đó thì phải đi xuống dọc theo một chồng giao thức, khi nó đi qua chồng giao thức đó nó trải qua những quá trình đóng gói và đóng gói lại. Những cách thức đóng gói tuỳ thuộc vào các khuôn dạng và các lược đồ biểu diễn được qui định cho những giao thức có mặt tại mỗi lớp của chồng giao thức đó. Phần quan trọng nhất của mỗi gói là một yêu cầu hoặc hồi đáp cho một yêu cầu. Tuy nhiên, gói cũng phải chứa địa chỉ mạng, một phương tiện để hồi báo rằng gói đã đến địa chỉ đích của nó. Một cơ chế kiểm tra lỗi để đảm bảo rằng gói đến đích trong tình trạng giống như khi nó được gửi đi, một cơ chế định thời gian để đảm bảo rằng gói không được gửi đi quá nhanh, đây gọi là sự kiểm soát dòng. Sự phân phối có đảm bảo, sự kiểm tra lỗi và sự kiểm soát dòng được cung cấp dưới dạng những thông tin được chứa trong các khung dữ liệu, vốn tạo ra bởi các lớp khác nhau của mô hình OSI. Khi gói đi xuyên qua các lớp của mô hình OSI, phía trước của nó được các giao thức đặt thêm vào những phần đầu đề (header) gồm một chuỗi các trường nào đó, còn đằng sau có thể được nối thêm phần đuôi vốn cũng gồm một chuỗi các trường nào đó.

Nhưng trước khi truyền nó phải được thiết lập kết nối, có nghĩa là hai thực thể ở cùng tầng ở hai đầu liên kết sẽ thương lượng với nhau về tập tham số sử dụng trong quá trình truyền dữ liệu. Quá trình truyền dữ liệu thực hiện như sau: Dữ liệu được gửi hoặc nhận từ một lớp trên cùng đó là lớp 7 (Application), lớp cao nhất của mô hình OSI. Nó được chuyển xuống dưới đến lớp 6 (Presentation), nơi quá trình bao gói bắt đầu.Từ đây, dữ liệu được bao lại trong một phần đầu đề, gồm các thông tin nhận diện và trợ giúp để chuyển tiếp dữ liệu đến một lớp nào đó khi nó được chuyển xuống đến lớp kế đó. Cũng giống ở trên khi dữ liệu ngang qua các lớp 5 (Session), lớp 4 (Transport), lớp 3 (Network) những giao thức hoạt động ở các lớp đó gắn thêm một phần đầu đề khác ở mỗi lớp và có thể dữ liệu được phân thành những mảnh nhỏ hơn để dễ quản lý hơn. Khi dữ liệu đi đến lớp 2 (Data Link) các giao thức tại chỗ đó sẽ lắp ráp dữ liệu thành các khung bằng cách gắn thêm vào một phần đầu và một phần cuối, sau đó các khung được chuyển xuống lớp 1 (Physical) để truyền đi trên phương tiện nối mạng. Khi các khung đến đích cảu nó, quá trình đó được lặp lại theo chiều ngược lại quá trình này được gọi là tách bỏ liên kết. Có nghĩa là qua mỗi tầng các phần đầu và phần cuối được gắn vào trên các tầng tương ứng khi gửi dữ liệu sẽ được tháo ra và so sánh. Ở trên là mạng chuyển mạch gói được truyền theo phương pháp có liên kết. Nếu chuyển mạch gói được truyền dưới dạng

không liên kết thí chỉ có một giai đoạn truyền dữ liệu (các gói dữ liệu) được truyền độc lập với nhau theo một con đường xác định bằng cách trong mỗi gói dữ liệu chứa địa chỉ đích.

Hình 2.3. Các tầng của Mô hình OSI

Việc nghiên cứu về OSI được bắt đầu tại ISO vào năm 1971 với các mục tiêu nhằm nối kết các sản phẩm của các hãng sản xuất khác. Ưu điểm chính của OSI là ở chỗ nó hứa hẹn giải pháp cho vấn đề truyền thông giữa các máy tính không giống nhau. Hai hệ thống, dù có khác nhau đều có thể truyền thông với nhau một các hiệu quả nếu chúng đảm bảo những điều kiện chung sau đây:

Chúng cài đặt cùng một tập các chức năng truyền thông.

Các chức năng đó được tổ chức thành cùng một tập các tầng. các tầng đồng mức phải cung cấp các chức năng như nhau.

Các tầng đồng mức khi trao đổi với nhau sử dụng chung một giao thức

Mô hình OSI tách các mặt khác nhau của một mạng máy tính thành bảy tầng theo mô hình phân tầng. Mô hình OSI là một khung mà các tiêu chuẩn lập mạng khác nhau có thể khớp vào. Mô hình OSI định rõ các mặt nào của hoạt động của mạng có thể nhằm đến bởi các tiêu chuẩn mạng khác nhau. Vì vậy, theo một nghĩa nào đó, mô hình OSI là một loại tiêu chuẩn của các chuẩn.

1. Nguyên tắc sử dụng khi định nghĩa các tầng hệ thống mở

Sau đây là các nguyên tắc mà ISO quy định dùng trong quá trình xây dựng mô hình OSI

Không định nghĩa quá nhiều tầng để việc xác định và ghép nối các tầng không quá phức tạp.

Tạo các ranh giới các tầng sao cho việc giải thích các phục vụ và số các tương tác qua lại hai tầng là nhỏ nhất.

Tạo các tầng riêng biệt cho các chức năng khác biệt nhau hoàn toàn về kỹ thuật sử dụng hoặc quá trình thực hiên.

Các chức năng giống nhau được đặt trong cùng một tầng.

Lựa chọn ranh giới các tầng tại các điểm mà những thử nghiệm trong quá khứ thành công.

Các chức năng được xác định sao cho chúng có thể dễ dàng xác định lại, và các nghi thức của chúng có thể thay đổi trên mọi hướng.

Tạo ranh giới các tầng mà ở đó cần có những mức độ trừu tượng khác nhau trong việc sử dụng số liệu.

Cho phép thay đổi các chức năng hoặc giao thức trong tầng không ảnh hưởng đến các tầng khác.

Tạo các ranh giới giữa mỗi tầng với tầng trên và dưới nó.

2. Các giao thức trong mô hình OSI

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

Giao thức có liên kết: trước khi truyền dữ liệu hai tầng đồng mức cần thiết lập một liên kết logic và các gói tin được trao đổi thông qua liên kết 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).

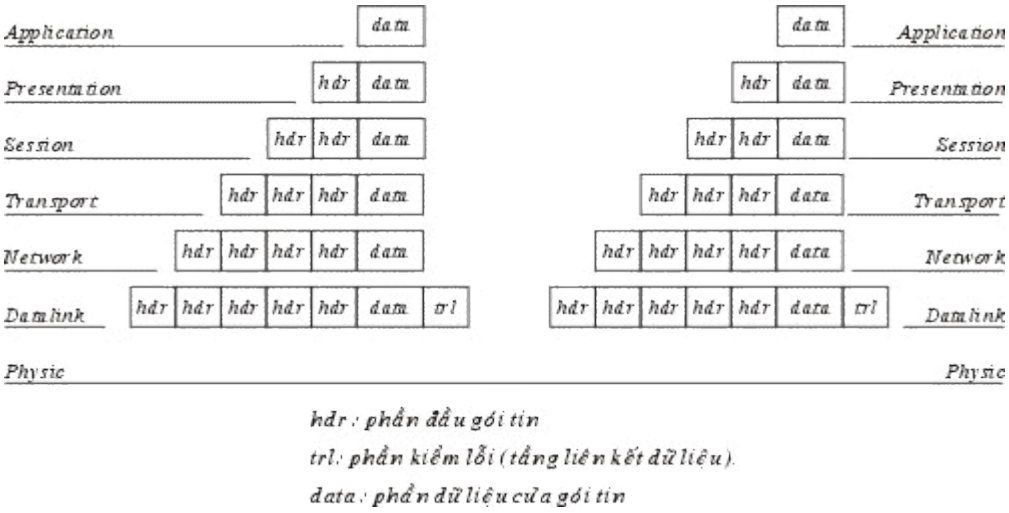
Truyền dữ liệu: dữ liệu được truyền với các cơ chế kiểm soát và quản lý kèm theo (như kiểm soát lỗi, kiểm soát luồng dữ liệu, cắt/hợp dữ liệu...) để tăng cường độ tin cậy và hiệu quả của việc truyền dữ liệu.

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 2.4. Phương thức xác lập các gói tin trong mô hình OSI

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

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

Chú ý: Trong mô hình OSI phần kiểm lỗi của gói tin tầng liên kết dữ liệu đặt ở cuối gói tin.

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

a. Tầng 1: Vật lý (Physical)

Tầng vật lý (Physical layer) là tầng dưới cùng của mô hình OSI. 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 đợc 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).

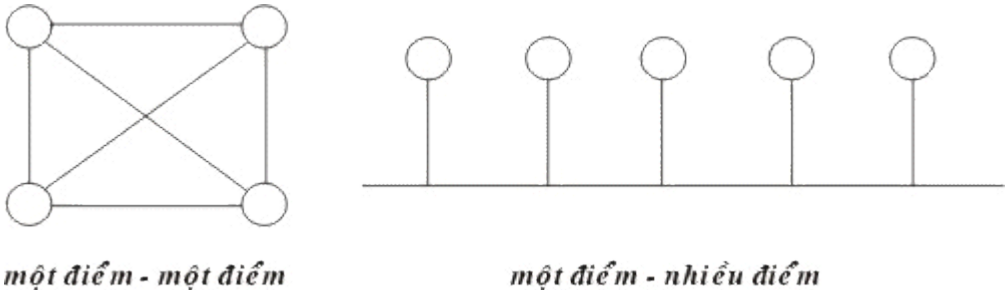
Phương thức truyền dị bộ: không có một tín hiệu quy định cho sự đồng bộ giữa các bit giữa máy gửi và máy nhận, trong quá trình gửi tín hiệu máy gửi sử dụng các bit đặc biệt START và STOP được dùng để tách các xâu bit biểu diễn các ký tự trong dòng dữ liệu cần truyền đi. Nó cho phép một ký tự được truyền 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.

b. Tầng 2: Liên kết dữ liệu (Data link)

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

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



Hình 2.5. Các đường truyền kết nối kiểu "một điểm-một điểm" và "một điểm-nhiều điểm"

Tầng liên kết dữ liệu cũng cung cấp cách phát hiện và sửa lỗi cơ bản để đảm bảo cho dữ liệu nhận được giống hoàn toàn với dữ liệu gửi đi. Nếu

một gói tin có lỗi không sửa được, tầng liên kết dữ liệu phải chỉ ra được cách thông báo cho nơi gửi biết gói tin đó có lỗi để nó gửi lại.

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

c. 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 đa các gói tin đến đích.

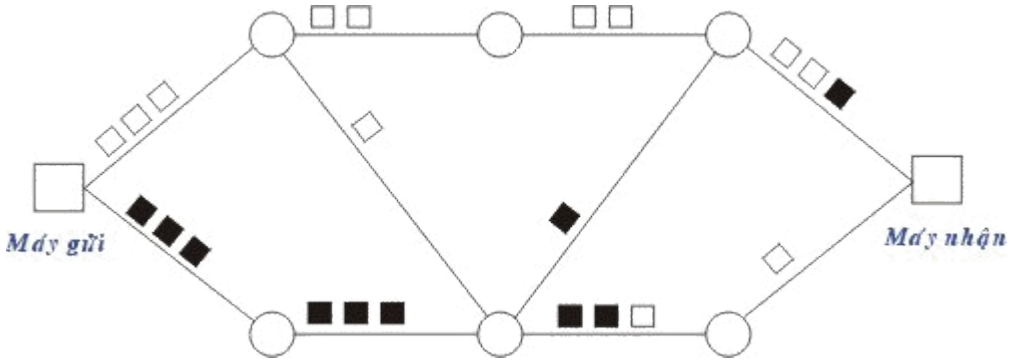
Tầng mạng cung các các phương tiện để truyền các gói tin qua mạng, thậm chí qua một mạng của mạng (network of network). Bởi vậy nó cần phải đáp ứng với nhiều kiểu mạng và nhiều kiểu dịch vụ cung cấp bởi các mạng khác nhau. hai chức năng chủ yếu của tầng mạng là chọn đường (routing) và chuyển tiếp (relaying). 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 2.6. 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.

d. 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 đợc nhưng tỷ suất sự cố có báo hiệu lại không chấp nhận được. Tầng giao vận phải có khả năng phục hồi lại khi xẩy ra sự cố.

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

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

Giao thức lớp 0 (Simple Class - lớp đơn giản): cung cấp các khả năng rất đơn giản để thiết lập liên kết, truyền dữ liệu và hủy bỏ liên kết trên mạng "có liên kết" loại A. Nó có khả năng phát hiện và báo hiệu các lỗi nhưng không có khả năng phục hồi.

Giao thức lớp 1 (Basic Error Recovery Class - Lớp phục hồi lỗi cơ bản) dùng với các loại mạng B, ở đây các gói tin (TPDU) đợc 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.

e. 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 xạ 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 lợt" (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 cha 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.

f. 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.

g. Tầng 7: ứng dụng (Application)

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

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

CHƯƠNG 3. CÁC GIAO THỨC TRUYỀN THÔNG

I. GIỚI THIỆU CHUNG VỀ GIAO THỨC

II. GIỚI THIỆU VỀ GIAO THỨC TCP/IP

Các chuẩn dành cho TCP/IP được công bố theo một chuỗi các tài liệu được gọi là RFCs (Request for Comments). RFCs mô tả cách làm việc nội tại của Internet. Một số RFCs mô tả các dịch vụ mạng hoặc các giao thức mạng và các cài đặt của nó, ngược với các khoản tóm tắt khác. Các chuẩn TCP/IP luôn được công bố bằng các RFCs, tuy nhiên không phải tất cả các chuẩn RFCs đều mô tả chuẩn này.

Các chuẩn TCP/IP không được phát triển bởi một uỷ ban, nhưng bởi sự nhất trí. Bất kỳ ai cũng có thể gửi tài liệu để công bố như một RFC. Các tài liệu được xem xét lại bởi một chuyên gia, một đơn vị có thẩm quyền, hoặc người chịu trách nhiệm về RFC, rồi gán cho nó một trạng thái. Trạng thái chỉ ra một tài liệu có được coi là một chuẩn.

Có năm trạng thái có thể gán cho các RFCs, như mô tả trong bảng 1.

Trạng thái	Mô tả
Required (cần thiết)	Phải được cài đặt trên tất cả các trạm và getway hoạt động dựa trên giao thức TCP/IP.
Recommended (gợi ý)	Khuyến khích tất cả các trạm và getway hoạt động dựa trên giao thức TCP/IP cài đặt các đặc tả RFC này. Các RFC được gợi ý thường được cài đặt.
Elective (có thể lựa chọn)	Cài đặt này là một lựa chọn. ứng dụng của nó đã được chấp nhận, nhưng không bắt buộc.
Limited Use (giới hạn sử dụng)	Không dùng cho mục đích chung.
Not recommended (không nên dùng)	Không được khuyến khích cài đặt.

Bảng 3.1. Các trạng thái được gán cho các RFCs

Nếu một tài liệu được coi là chuẩn, nó phải qua các bước phát triển, kiểm tra, và được sự chấp nhận của Internet Standards Process (quá trình chuẩn internet). Những mức này được đặt tên là các mức tin cậy (maturity levels). Bảng 2 liệt kê ba mức tin cậy cho các chuẩn Internet.

Mức tin cậy	Mô tả
Proposed Standard (chuẩn đề nghị)	Đặc tả một chuẩn đề nghị thường ổn định, đã được các nhà thiết kế lựa chọn, được tin cậy và dễ hiểu, đã nhận được sự xem xét ủng hộ của cộng đồng, và có được sự quản tâm ủng hộ đủ lớn của cộng đồng coi là có giá trị.
Draft Standard (chuẩn phác thảo)	Một chuẩn phác thảo phải khá dễ hiểu và được biết là khá ổn định, cả hai điều này theo đúng nghĩa của nó và là cơ sở cho việc phát triển và cài đặt.
Internet Standard (chuẩn Internet)	Đặc tả chuẩn Internet (có thể được nhắc đến đơn giản là chuẩn Internet) được chi tiết hoá ở mức tin cậy kỹ thuật cao và giữ được độ tin cậy mà đặc tả giao thức hoặc dịch vụ đó cung cấp những lợi ích có ý nghĩa cho cộng động Internet).

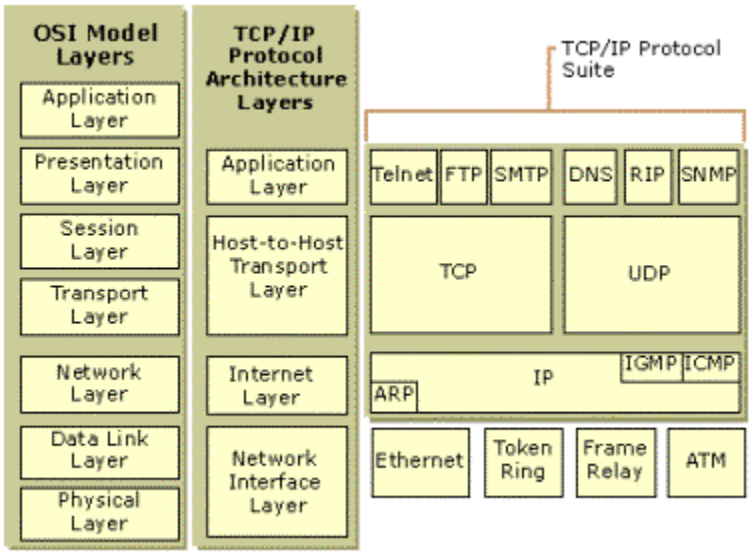
Bảng 3.2. Các mức tin cậy cho chuẩn Internet

Khi một tài liệu được công bố, nó được gán một số RFC. RFC gốc không bao giờ được cập nhật. Nếu thay đổi là cần thiết, một tài liệu RFC mới sẽ được công bố với một số mới. Vì vậy, việc kiểm tra rằng bạn có phải bạn có tài liệu RFC gần nhất trong một chủ đề nhất định không là quan trọng.

Các RFCs có thể nhận được bằng nhiều cách. Cách đơn giản nhất để nhận RFC bất kỳ hoặc danh sách đánh chỉ mục cập nhật đầy đủ tất cả các RFC đã công bố là truy cập vào địa chỉ www.rfc-editor.org/rfc. RFCs cũng có thể lấy được qua địa chỉ FTP từ nis.nsf.net, nisc.jvnc.net, venera.isi.edu, wuarchive.wustl.edu, src.doc.ic.ac, uk, ftp.concert.net, internic.net, hoặc nic.ddn.mil.

1. Kiến trúc giao thức TCP/IP

Các tầng giao thức TCP/IP được chia làm bốn tầng chức năng được biết đến như là mô hình DARPA, được đặt tên sau khi chính phủ Mĩ bắt đầu phát triển TCP/IP. Bốn tầng của mô hình DARPA là: ứng dụng (Application), Giao vận (Transport), Internet, và tầng Giao tiếp mạng (Network Interface). Mỗi tầng trong mô hình DARPA tương ứng với một hoặc nhiều tầng trong mô hình bẩy tầng của mô hình OSI. Hình 1 biểu diễn kiến trúc giao thức TCP/IP.



Hình 3.3. Kiến trúc giao thức TCP/IP

a. Tầng giao tiếp mạng (Network Interface Layer)

Tầng Giao tiếp mạng (còn được gọi là tầng Truy cập mạng) chịu trách nhiệm đặt các gói tin TCP/IP trên môi trường mạng và nhận các gói tin TCP/IP từ môi trường mạng. TCP/IP được thiết kế độc lập với phương pháp truy cập mạng, định dạng khung dữ liệu, và môi trường mạng. Bằng cách này, TCP/IP có thể được sử dụng để kết nối các loại mạng khác nhau. Bao gồm các kỹ thuật mạng LAN nh Ethernet hoặc Token Ring và các kỹ thuật mạng WAN như X.25 hay Frame Relay. Sự độc lập với bất kỳ kỹ thuật mạng nào cho phép TCP/IP có khả năng tương tích với các kỹ thuật mới như ATM (Asynchronous Transfer Mode).

Tầng Giao tiếp mạng bao gồm tầng Liên kết dữ liệu (Data Link) và tầng Vật lý (Physical) của mô hình OSI. Chú ý rằng tầng Internet không có được các ưu điểm của các dịch vụ sắp xếp gói tin và thông báo có ở tầng Data Link. Một tầng Giao tiếp mạng được giả thiết, và việc truyền thông tin cậy qua các phiên thiết lập, sắp xếp và thông báo các gói tin thuộc về trách nhiệm của tầng Giao vận.

b. Tầng Internet

Tầng Internet chịu trách nhiệm địa chỉ hoá, đóng gói, và dẫn đường. Lõi các giao thức lõi của tầng Internet là IP, ARP, ICMP, và IGMP.

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.

Tầng Internet tương tự như tầng Network của mô hình OSI.

c. Tầng giao vận

Tầng giao vận (còn được gọi là tầng truyền Trạm-tới-Trạm Host-to-Host Transport Layer) chịu trách nhiệm cung cấp cho tầng ứng dụng các dịch vụ tạo lập phiên và truyền dữ liệu. Các giao thức lõi của tầng Giao vận 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.

Tầng Giao vận chịu trách nhiệm tầng Giao vận trong mô hình OSI và một số nhiệm vụ của tầng Phiên (Session) của OSI.

d. Tầng ứng dụng

Tầng ứng dụng cung cấp các ứng dụng với khả năng truy cập các dịch vụ của các tầng khác và định nghĩa các giao thức mà các ứng dụng sử dụng để trao đổi dữ liệu. Có nhiều giao thức tầng ứng dụng và các giao thức mới luôn luôn được phát triển.

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

Giao thức truyền tin siêu văn bản HTTP (HyperText Transfer Protocol) được sử dụng để truyền các tệp tạo nên trang web của World Wide Web.

Giao thức FTP - File Transfer Protocol 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 để 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. Giao thức lõi TCP/IP

Thành phần giao thức TCP/IP được cài trong hệ điều hành mạng của bạn là một chuỗi các giao thức liên hệ với nhau được gọi là các giao thức lõi TCP/IP. Tất cả các ứng dụng khác và các giao thức khác trong bộ giao thức TCP/IP dựa trên các dịch vụ cơ sở cung cấp bởi các giao thức sau: IP, ARP, ICMP, IGMP, TCP, và UDP.

a. IP

IP là một giao thức không liên kết, truyền tin không chắc chắn chủ yếu chịu trách nhiệm địa chỉ hoá và dẫn đường các gói tin giữa các trạm. Không liên kết có nghĩa là phiên làm việc không được thiết lập trước khi trao đổi dữ liệu. Không chắc chắn có nghĩa là việc gửi đi các gói tin IP không được đảm bảo chắc chắn là tới đích. Giao thức IP sẽ luôn luôn thực hiện cố gắng nhất để truyền gói tin. Một gói tin IP có thể bị mất, truyền đi không đúng thứ tự, truyền đúp, hoặc bị trễ. Giao thức IP không cố gắng phục hồi những loại lỗi như vậy. Các gói tin thông báo (acknowledgment) truyền đi và việc khôi phục các gói tin bị mất thuộc về trách nhiệm của các tầng cao hơn, như TCP. IP được định nghĩa trong RFC 791.

Một gói tin IP bao gồm một phần đầu gói tin IP (IP header) và một phần dữ liệu trong gói tin IP (IP payload). Bảng 3 mô tả các trường chính trong phần đầu gói tin IP.

Các trường trong phần	Chức năng

đầu gói tin IP	
Địa chỉ IP nguồn	Địa chỉ IP của nguồn truyền gói tin IP.
Địa chỉ IP đích	Địa chỉ IP đích đến của gói tin IP.
Định danh (Identification)	Được sử dụng để xác định gói tin IP cụ thể và để xác định tất cả các phân đoạn của một gói tin IP cụ thể nếu việc phân đoạn xẩy ra.
Giao thức	Khẳng định giao thức IP được dùng tại trạm đích cho dù gói tin được truyền dựa trên các giao thức TCP, UDP, ICMP, hoặc các giao thức khác.
Checksum	Một phép tính toán học đơn giản để kiểm tra tính toàn vẹn của phần đầu gói tin IP.
Thời gian sống TTL (Time to Live)	Là số được thiết kế của mạng trên đó gói dữ liệu được phép truyền trước khi bị bỏ qua bởi router. TTL được đặt bởi trạm gửi gói tin và được sử dụng để ngăn không cho một gói tin truyền lòng vòng không kết thúc trong mạng sử dụng giao thức IP. Khi một gói tin IP được truyền tiếp, router cần giảm giá trị của TTL ít nhất là 1.

Bảng 3.4. Các trường chính trong phần đầu gói tin IP.

Phân đoạn và tập hợp lại (fragmentation and reassembly)

Nếu router nhận được một gói tin IP quá lớn đối với mạng trong đó gói tin được gửi tiếp đi, gói tin IP sẽ được phân chia thành nhiều gói nhỏ vừa với kích thước của mạng được truyền tiếp. Khi gói tin tới địa chỉ đích, giao thức IP tại trạm đích sẽ tập hợp lại các phân đoạn thành gói tin gốc. Quá trình này gọi là phân đoạn. Phân đoạn có thể xẩy ra trong môi trường sử dụng kết hợp nhiều công nghệ mạng, ví dụ cả Ethernet và Token Ring.

Việc phân đoạn và tập hợp được thực hiện như sau:

1. Khi một gói tin IP được gửi bởi nguồn gửi, nó đặt một giá trị duy nhất vào trường định danh (Identification).
2. Gói tin IP nhận được tại router. Các nút router IP mà đơn vị truyền tin lớn nhất MTU (maximum transmission unit) của mạng trong đó gói tin được gửi đi mà nhỏ hơn kích thước của gói tin IP.
3. Giao thức IP sẽ phân đoạn gói tin dữ liệu IP (IP payload) gốc thành nhiều đoạn sao cho kích thước vừa với kích thước đơn vị truyền tin

của mạng tiếp theo. Mỗi đoạn được gửi đi với phần đầu gói tin IP riêng của nó chứa:

Trường định danh (identification) gốc, trường này sẽ xác định tất cả các phân đoạn thuộc về cùng một gói tin gốc.

Cờ thêm phân đoạn (More Fragments Flag), sẽ chỉ ra còn phân đoạn khác tiếp theo hay không. Cơ này không được đặt ở phân đoạn cuối cùng, bởi vì không còn phân đoạn nào tiếp theo nó.

Vị trí phân đoạn (Fragment Offset) chỉ ra vị trí tương đối của phân đoạn so với gói tin dữ liệu IP gốc.

4. Khi các phân đoạn nhận được bởi giao thức IP tại máy trạm từ xa, chúng xác định bởi trường định danh có giống nhau không, và vị trí phân đoạn (Fragment Offset) được sử dụng để tập hợp các phân đoạn thành gói tin dữ liệu IP gốc.

b. ARP

Khi các gói tin IP được gửi trên môi trường chia sẻ truy cập, các công nghệ mạng dựa trên công nghệ truyền quảng bá như Ethernet hoặc Token Ring, Media Access Control (MAC) địa chỉ tương ứng với địa chỉ các gói tin IP phải được chuyển hoá. ARP sử dụng MAC mức truyền quảng bá để phân giải một địa chỉ IP gửi đi thành một địa chỉ MAC. ARP được định nghĩa trong RFC 826.

Để có thêm thông tin về ARP, xem phần "Phân giải địa chỉ vật lý" trong đoạn cuối của chương này.

c. ICMP

Giao thức điều khiển thông điệp Internet ICMP cung cấp tiện ích sửa chữa sự cố và thông báo lỗi cho các gói tin không truyền đi được. Ví dụ, nếu một gói tin IP không truyền tới trạm đích được, ICMP sẽ gửi thông điệp thông báo không tiếp cận đích được "Destination Unreachable" tới trạm nguồn. Bảng 4 biểu diễn các thông điệp ICMP thông thường nhất.

Thông điệp ICMP	**Chức năng**
Echo Request (yêu cầu phản hồi)	Thông điệp báo sự cố đơn giản được sử dụng để kiểm tra kết nối IP tới trạm mong muốn.
Echo Reply (trả lời phản hồi)	Dùng để trả lời cho Echo Request.
Redirect (định hướng lại)	Được gửi bởi một router để khẳng định một trạm gửi tin dẫn đường tốt hơn tới một địa

	chỉ IP đích.
Source Quench (tắt nguồn)	Được gửi bởi một router để gẳng định trạm gửi tin mà dữ liệu IP bị loại bởi nghẽn tại router. Trạm gửi tin sẽ hạ thấp tỉ lệ truyền. Source Quench là một thông điệp ICMP không bắt buộc và thường không được cài đặt.
Destination Unreachable (không thể tiếp cận đích)	Được gửi bởi một router hoặc trạm đích để thông báo cho trạm gửi tin rằng gói tin không thể truyền được.

Bảng 3.5. Các thông điệp ICMP thông thường

Để gửi một gói tin phản hồi yêu cầu ICMP và hiển thị thống kê trên các thông điệp trả lời trên máy sử dụng Windows NT chúng ta sử dụng tiện ích ping trong dấu nhắc lệnh.

ICMP không làm cho giao thức IP trở nên tin cậy. ICMP cố gắng thông báo các lỗi và đưa ra phản hồi trong các điều kiện cụ thể. Các thông điệp ICMP được truyền đi như một gói tin IP không thông báo và bản thân chúng là không chắc chắn có tới được đích không. ICMP được định nghĩa trong RFC 792.

d. IGMP

Giao thức quản lý nhóm Internet IGMP (Internet Group Management Protocol) là một giao thức quản lý các trạm thành viên trong nhóm truyền IP multicast. Một nhóm IP multicast, được biết đến như một nhóm trạm. Gói tin IP multicast được truyền tới một địa chỉ MAC đơn nhưng được xử lý bởi nhiều trạm sử dụng giao thức IP. Một trạm cụ thể sẽ nghe một địa chỉ gói tin IP multicast cụ thể và nhận tất cả các gói tin từ địa chỉ đó.

e. TCP

TCP là một dịch vụ truyền tin tin cậy, có liên kết. Dữ liệu được truyền theo các phân đoạn. Truyền tin có liên kết có nghĩa là kết nối phải được thiết lập trước khi các trạm có thể trao đổi dữ liệu. Việc truyền tin tin cậy đạt được bằng cách gán các số thứ tự tới mỗi đoạn gói tin được truyền đi. Một thông báo được sử dụng để kiểm tra rằng dữ liệu đã được nhận bởi trạm khác. Với mỗi phân đoạn được gửi, trạm nhận tin phải tra về một gói thông báo ACK trong một chu kỳ nhất định các byte dữ liệu nhận được. Nếu một gói tin ACK không được nhận, dữ liệu sẽ được truyền lại. Giao thức TCP đợc định nghĩa trong RFC 793.

TCP sử dụng phơng pháp truyền các luồng byte dữ liệu (byte-stream communications), các dữ liệu trong phân đoạn TCP được xử lý như một chuỗi

các byte không phân biệt thành bản ghi hay biên giới các trường dữ liệu. Bảng 6 mô tả các trường chính trong phần đầu gói tin TCP.

Trường	Chức năng
Source Port (cổng nguồn)	Cổng TCP của trạm gửi tin.
Destination Port (Cổng đích)	Cổng TCP của trạm đích.
Sequence Number (số thứ tự)	Số thứ tự byte đầu tiên của dữ liệu trong phân đoạn TCP.
Acknowledgment Number (số thông báo)	Số thứ tự của byte mà trạm gửi tin muốn nhận từ phía bên kia của trạm truyền tin trong liên kết.
Window (cửa số)	Kích thước hiện thời của vùng đệm TCP trên trạm gửi phân đoạn TCP để lưu trữ các phan đoạn tới.
TCP Checksum	Kiểm tra tính toàn vẹn của phần đầu và phần dữ liệu của gói tin TCP.

Bảng 3. 6. Các trường chính trong phần đầu gói tin TCP

Các cổng TCP

Một cổng TCP cung cấp một vị trí cụ thể để truyền các phân đoạn TCP. Các cổng có số dưới 1024 là các cổng thông dụng và được gán bởi tổ chức IANA (Internet Assigned Numbers Authority). Bảng 7 liệt kê một số cổng TCP thông dụng.

Số cổng TCP	Mô tả
20	FTP (Kênh dữ liệu).
21	FTP (Kênh điều khiển).
23	Tiện ích Telnet.
80	Giao thức truyền tin HTTP sử dụng cho World Wide Web.
139	Dịch vụ phiên NetBIOS.

Bảng 3.7. Các cổng TCP thông dụng

Để xem hết danh sách các cổng TCP đã được gán, tham khảo RFC 1700.

Ba bước bắt tay của giao thức TCP (three-way handshake)

Một liên kết TCP được khởi tạo thông qua bước cách bắt tay. Mục đích của ba bước bắt tay là đồng bộ hoá số thứ tự và số gói tin thông báo của cả hai phía trong liên kết, kích thước cửa số TCP để trao đổi, và các thông số trao đổi TCP khác như kích thước phân đoạn tối đa. Các bước sau phác thảo quá trình:

1. Máy client gửi một phân đoạn TCP tới máy chủ với số thứ tự (Sequence Number) khởi tạo cho liên kết và kích thước cửa sổ (Window) chỉ ra kích thước vùng đệm trên phía máy client để lưu trữ các phân đoạn tới từ server.
2. Server gửi trả lại một phân đoạn TCP chứa số thứ tự khởi tạo mà nó chọn, gói tin thông báo số thứ tự của máy client, và kích thước cửa sổ chỉ ra kích thước vùng đệm trên server để lu trữ các phân đoạn đến từ client.
3. Máy client gửi một phân đoạn TCP tới server chứa thông báo số thứ tự gói tin của server.

Giao thức TCP sử dụng một quá trình bắt tay tương tự để kết thúc liên kết. Điều này đảm bảo cả hai phía trạm truyền tin đều kết thúc việc truyền và tất cả dữ liệu truyền đã được nhận.

f. UDP

UDP cung cấp dịch vụ truyền tin không liên kết, không tin cậy, cách hiệu quả nhất để truyền các thông điệp. Điều này có nghĩa rằng tất cả các gói tin truyền đi là không được đảm bảo chắc chắn tới đích, hoặc không đúng thứ tự truyền. UDP không phục hồi được các gói tin đã bị mất bằng cách truyền lại. UDP được định nghĩa trong RFC 768.

UDP được sử dụng bởi các ứng dụng không cần thông báo khẳng định việc nhận dữ liệu thành công và được sử dụng điển hình trong việc truyền lượng nhỏ dữ liệu thực hiện trong chỉ một lần. Như dịch vụ tên NetBIOS, dịch vụ gói tin NetBIOS, và giao thức SNMP (Simple Network Management Protocol) là các ví dụ về các dịch vụ và ứng dụng sử dụng UDP. Bảng 8 mô tả các trường chính trong phần đầu gói tin UDP.

Trường	**Chức năng**
Source Port (cổng nguồn)	Cổng UDP của trạm gửi tin.
Destination Port (cổng đích)	Cổng UDP của trạm nhận tin.
UDP Checksum	Kiểm tra tính toàn vẹn của phần đầu và phần dữ liệu gói tin UDP.

Acknowledgment Number (số thông báo)	Số thứ tự của byte mà phía gửi cần nhận tiếp theo thừ phía trạm còn lại của liên kết.

Bảng 3.8. Các trường chính trong phần đầu gói tin UDP.

Các cổng UDP

Để sử dụng UDP, một ứng dụng phải cung cấp địa chỉ IP và cổng UDP của ứng dụng đích. Một cổng cung cấp vị trí để gửi thông điệp. Một cổng có chức năng như một bộ đồn kênh hàng đợi thông điệp, có nghĩa là nó có thể nhận nhiều thông điệp tại cùng thời điểm. Mỗi công được xác định bởi một số duy nhất. Cần chú ý là cổng UDP phân biệt và khác với các cổng TCP mặc dù một số trong đó có cùng số cổng. Bảng 9 liệt kê các cổng UDP thông dụng.

Số cổng UDP	**Mô tả**
53	Truy vấn tên từ hệ thống tên miền DNS (Domain Name System).
69	Giao thức TFTP (Trivial File Transfer Protocol).
137	Dịch vụ tên NetBIOS.
138	Dịch vụ truyền dữ liệu NetBIOS.
161	Giao thức SNMP (Simple Network Management Protocol).

Bảng 3.9. Các cổng UDP thông dụng

Để tham khảo toàn bộ danh sách các cổng UDP đã được gán xem RFC 1700

III. CÁC GIAO THỨC KHÁC

1. Giao thức NetBIOS

NetBIOS (Network Basic Input/Output System) được phát triển cho IBM vào năm 1983 bởi Sytek Corporation để cho phép các ứng dụng giao tiếp qua mạng. NetBIOS định nghĩa hai thực thể, một ở mức phiên giao tiếp và một ở mức giao thức quản lý phiên truyền dữ liệu.

NetBIOS cũng định nghĩa một giao thức có các chức năng tại mức phiên/giao vận. Các chức năng này được cài đặt dựa trên giao thức phần mềm, ví dụ như giao thức NBFP (NetBIOS Frame Protocol) là một thành phần của NetBEUI hoặc NetBIOS trên TCP/IP (NetBT), để thực hiện các cổng

mạng cần cho hoàn thiện tập lệnh giao tiếp. NetBIOS dựa trên TCP/IP được định nghĩa trong RFCs 1001 và 1002.

NetBIOS cung cấp các lệnh và hỗ trợ cho quản lý tên NetBIOS Name Management, NetBIOS Datagram, và NetBIOS Sessions.

NetBIOS Name Management

Quản lý tên NetBIOS

Các dịch vụ quản lý tên NetBIOS cung cấp các chức năng sau:

Đăng ký và giải phóng tên

Khi một trạm TCP/IP khởi tạo, nó đăng ký tên NetBIOS bằng cách lan truyền hoặc hướng một yêu cầu đăng ký tên NetBIOS tới một máy chủ tên NetBIOS Name Server, ví dụ như máy chủ WINS (Windơs Internet Name Service). Nếu một trạm khác đã đăng ký cùng tên NetBIOS đó, hoặc là trạm hoặc là server tên NetBIOS trả lời với một thông điệp phủ định đăng ký tên (negative name registration response). Trạm khởi tạo nhận được một kết quả khởi tạo lỗi.

Khi dịch vụ trên một trạm dừng hoạt động, trạm đó sẽ ngừng lan toả trả lời phủ định việc đang ký tên và giải phóng tên để cho trạm khác có thể sử dụng.

Dịch vụ tên NetBIOS sử dụng giao thức UDP cổng 137.

Dịch vụ gói dữ liệu NetBIOS (NetBIOS Datagrams).

Dịch vụ gói dữ liệu NetBIOS cung cấp dịch vụ truyền các gói dữ liệu không liên kết, không có thứ tự, và không tin cậy. Các gói dữ liệu có thể hướng tới một tên máy NetBIOS hoặc lan truyền quảng bá tới một nhóm tên. Việc truyền các gói tin NetBIOS là không tin cậy, trong đó chỉ người sử dụng đã đăng nhập vào mạng mới nhận được các thông điệp. Dịch vụ gói tin có thể khởi tạo và nhận cả các thông điệp truyền quảng bá và truyền có định hướng. Dịch vụ gói tin NetBIOS sử dụng giao thức UDP cổng 138.

Dịch vụ phiên NetBIOS (NetBIOS sessions)

Dịch vụ phiên NetBIOS cung cấp khả năng truyền các thông điệp NetBIOS có liên kết, có thứ tự, và tin cậy. Dịch vụ phiên NetBIOS sử dụng giao thức TCP cung cấp, duy trì, và kết thúc các phiên. Dịch vụ phiên cho phép luồng dữ liệu truyền theo hai hướng sử dụng giao thức TCP cổng 139.

Địa chỉ IP

Mỗi trạm sử dụng giao thức TCP/IP được định danh bởi một địa chỉ IP luận lý. Địa chỉ IP là một địa chỉ tầng mạng và không phụ thuộc vào địa chỉ tầng liên kết dữ liệu (như địa chỉ MAC của card giao tiếp mạng). Một địa chỉ duy nhất được gán cho mỗi trạm và các thành phần của mạng sử dụng giao thức TCP/IP.

Địa chỉ IP xác định vị trí của hệ thông trên mạng tương tự như xác định địa chỉ nhà trong một khu phố. Địa chỉ của đường xác chỉ định nơi cư trú, địa chỉ IP phải là duy nhất trên toàn cầu và sử dụng cùng định dạng.

Each IP address includes a network ID and a host ID.

Mỗi địa chỉ IP bao gồm địa chỉ mạng NetWork ID và địa chỉ trạm host ID.

> Network ID (còn được gọi là địa chỉ mạng) xác định hệ thống trên cùng mạng vật lý giới hạn bởi IP của router. Tất cả các hệ thống trên cùng mạng vật lý phải có cùng địa chỉ mạng network ID. Network ID phải là duy nhất trong toàn mạng tương tác.
>
> Host ID (hay địa chỉ máy trạm) xác định một trạm, server, router, hoặc trạm TCP/IP khác trong mạng. Địa chỉ cho mỗi trạm phải là duy nhất trong cùng một network ID.

Chú ý: Cách sử dụng khái niệm network ID nói tới bất kỳ IP network ID nào, có dựa trên phân lớp, subnet, hay supernet hay không.

Một địa chỉ IP gồm 32 bit. Thay vì làm việc với 32 bit liền lúc, nó thường phân đoạn 32 bit địa chỉ IP thành các trường 8-bit được gọi là các octet. Mỗi octet được chuyển thành số thập phân trong phạm vi từ 0-255 và cách nhau bởi dấu chấm. Định dạng này được gói là ký hiệu chấm thập phân (dotted decimal notation). Bảng 10 đưa ra một ví dụ của một địa chỉ IP ở dạng nhị phân và dạng chấm thập phân.

Dạng nhị phân	Dạng chấm thập phân
11000000 10101000 00000011 00011000	192.168.3.24

Ký hiệu w.x.y.z được sử dụng khi nói tới địa chỉ IP tổng quát hoá và biểu diễn trong hình 3.

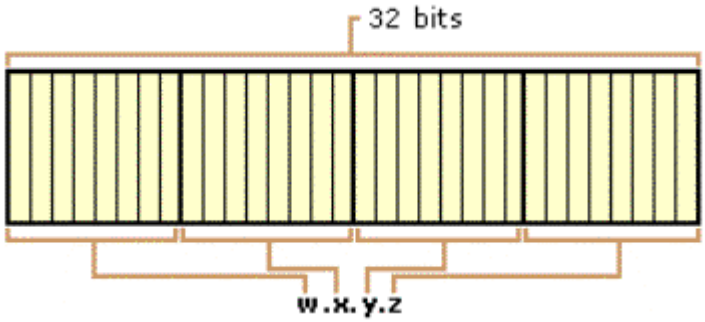


Figure 3. Địa chỉ IP

Lớp địa chỉ

Ngay từ đầu cộng đồng Internet đã định nghĩa năm lớp địa chỉ phù hợp với sự thay đổi kích cỡ của các mạng. Giao thức TCP/IP của Microsoft hỗ trợ các lớp địa chỉ A, B, và C gán cho các trạm. Các lớp địa chỉ đinh nghĩa những bit nào được sự dụng làm network ID và những bit nào được sử dụng làm host ID. Nó cũng định nghĩa số các mạng có thể có và số các trạm có thể có trên mạng.

Lớp A

Lớp địa chỉ A được gán cho các mạng có số lượng trạm rất lớn. Bit có thứ tự cao nhất trong lớp A luôn được đặt là 0. 7 bit tiếp theo (đủ octet đầu tiên) hoàn thành địa chỉ mạng. 24 bits còn lại (3 octet còn lại) biểu diễn địa chỉ máy host ID. Điều này có nghĩa là lớp A cho phép 126 mạng và 16777214 máy trạm trên một mạng. Hình 4 minh hoạ cấu trúc của địa chỉ lớp A

.

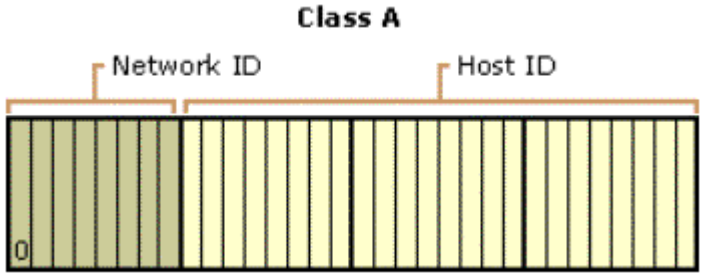
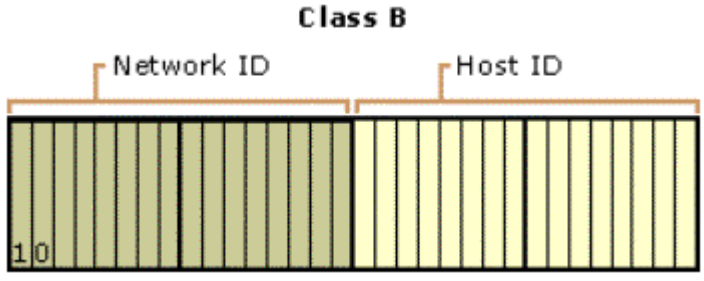


Figure 4. Địa chỉ IP lớp A

Lớp B

Địa chỉ lớp B được gán cho mạng có kích thước vừa và lớn. Hai bit cao nhất của lớp địa chỉ B luôn được đặt là 10. 14 bit tiếp theo (đủ hai octet đầu) hoàn thành địa chỉ mạng network ID. 16 bit còn lại (hai octet cuối) biểu diễn địa chỉ trạm host ID. Điều này có nghĩa lớp B cho phép 16384 mạng và 65534 trạm trên một mạng. Hình 5 minh họa cấu trúc địa chỉ lớp



B.

Figure 5. Địa chỉ IP lớp B

Lớp C

Địa chỉ lớp C sử dụng cho mạng nhỏ. 3 bit cao nhất của lớp C luôn được đặt là 110. 21 bit tiếp theo (đủ 3 octet đầu) hoàn thành địa chỉ mạng network ID. Còn lại 8 bit (octet cuối cùng) biểu diễn địa chi máy host ID. Điều này cho phép sử dụng 2097152 mạng và 254 máy trên mỗi mạng. Hình 6 minh hoạ cấu trúc của địa chỉ lớp C.

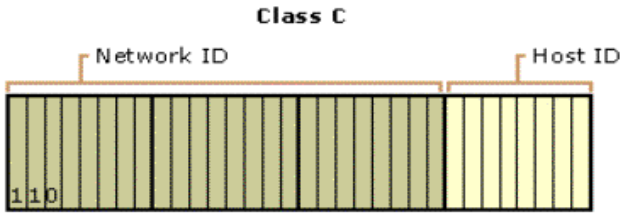


Figure 6. Địa chỉ IP lớp C

Lớp D

Địa chỉ lớp D dành riêng cho các địa chỉ IP multicast. 4 bit cao nhất trong lớp D luôn được đặt là 1110. Các bit còn lại để đánh địa chỉ các máy có liên quan.

Lớp E

Lớp địa chỉ E để dành riêng cho việc sử dụng sau này. 4 bit cao nhất trong lớp địa chỉ E luôn được đặt là 1111.

Bảng 11 tổng kết các lớp địa chỉ A, B, và C có thể sử dụng bao nhiêu địa chỉ IP cho máy trạm.

Bảng 11. Tổng kết các lớp địa chỉ IP

Lớp	**Giá trị w**	**Phần network ID**	**Phần host ID**	**Số mạng có thể dùng**	**Số máy trên một mạng**
A	1–126	w	x.y.z	126	16,777,214
B	128–191	w.x	y.z	16,384	65,534
C	192–223	w.x.y	z	2,097,152	254

Địa chỉ 127.x.y.z của lớp A được dùng dành riêng cho việc kiểm tra vòng phản hồi (loopback) và truyền thông trên máy cục bộ.

Cách đánh địa chỉ mạng network ID

Network ID xác định các máy sử dụng TCP/IP trên cùng một mạng vật lý. Tất cả các trạm trên cùng một phân đoạn vật lý phải có cùng một địa chỉ mạng network ID để có thể giao tiếp với các máy khác.

Sau đây là cách gán network ID:

Địa chỉ mạng phải là duy nhất với mạng kết nối liên mạng. Nếu bạn có kế hoạch dẫn trực tiếp kết nối tới Internet công cộng, network ID phải duy nhất đối với Internet. Nếu bạn không có kết hoạch kết nối tới Internet công cộng, network ID cục bộ phải là duy nhất đối với mạng kết nối liên mạng.

Network ID không thể bắt đầu bởi số 127. Số 127 trong lớp A được dành riêng cho các chức năng lặp phản hồi.

Tất cả các bit trong phần network ID không thể đặt bằng 1. Tất cả các bít đặt bằng 1 trong phần network ID được dành riêng để sử dụng truyền quảng bá các gói tin IP.

Tất cả các bit trong phần network ID không thể đặt bằng 0. Tất cả các bit 0 trong network ID được sử dụng để biểu diễn một trạm cụ thể trên mạng cục bộ sẽ không được dẫn đường.

Bảng 12 liệt kê dải các network ID hợp lệ dựa trên lớp các địa chỉ IP. Để biểu diễn IP network ID, các bit địa chỉ trạm được đặt bằng 0. Chú ý rằng qua cách biểu diễn dạng chấm thập phân, network ID không phải là một địa chỉ IP.

Bảng 12. Dải các lớp network ID

Lớp địa chỉ	**Network ID đầu tiên**	**Network ID cuối cùng**
A	1.0.0.0	126.0.0.0
B	128.0.0.0	191.255.0.0
C	192.0.0.0	223.255.255.0

Cách đánh địa chỉ máy host ID.

Host ID xác định địa chỉ TCP/IP của một máy trên mạng. Sự kết hợp IP của network ID và IP của host ID thành một địa chỉ IP.

Sau đây là cách gán địa chỉ host ID:

Host ID phải là duy nhất trong một mạng (cùng network ID).

Tất cả các bit trong host ID không thể đặt bằng 1, bởi vì host ID này dành riêng cho địa chỉ truyền quảng bá các gói tin truyền tới tất cả các trạm trên một mạng.

Tất cả các bit trong host ID không thể đặt bằng 0, vì host ID này dành riêng để ký hiệu địa chỉ IP mạng (network ID).

Bảng 13 liệt kê dải các giá trị host ID hợp lệ dựa trên lớp các địa chỉ IP.

Bảng 13. Dải các host ID.

Lớp địa chỉ	**Host ID đầu tiên**	**Host ID cuối cùng**
A	w.0.0.1	w.255.255.254
B	w.x.0.1	w.x.255.254
C	w.x.y.1	w.x.y.254

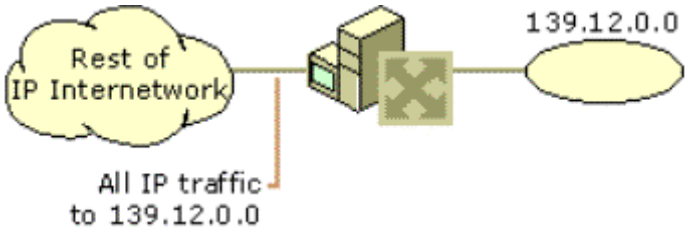
Subnets và Subnet Masks

Phân lớp địa chỉ Internet được thiết kế để cung cấp ba dải IP khác nhau trong kết nối mạng, trong đó 32 bit của địa chỉ IP đợc chia ra thành network ID và host ID tuỳ theo số mạng và số trạm trên mạng cần sử dụng. Tuy nhiên, hãy khảo sát network ID của lớp A, nó cho phép trên 16 triệu trạm được đánh địa chỉ trên một mạng. Tất cả các trạm trên cùng một mạng vật lý lại bị giới hạn bởi IP của router chia sẻ cùng đường truyền quảng bá; chúng có cùng vùng truyền quảng bá. Sẽ là không thực tế để có 16 triệu nút trong cùng một vùng quảng bá. Kết quả là hầu hết trong số 16 triệu địa chỉ trạm không thể gán được và bị bỏ phí. Mặc dù lớp B với 65 nghìn trạm nhưng vẫn là không thực tế.

Trong nỗ lực để tạo ra các vùng truyền quảng bá nhỏ hơn và sử dụng hiệu quả hơn, các bit trong host ID của một network ID có thể được chia thành mạng nhỏ hơn, mỗi mạng giới hạn bởi một IP router và được gán một giá trị mạng con subnetted network ID, là một mạng con của mạng gốc ban đầu trên cùng một network ID.

Điều này tạo ra các subnet (mạng con), sự phân chia địa chỉ IP mạng, mỗi mạng con có một địa chỉ network ID con. Phân chia mạng con được tạo ra bằng cách sử dụng phần địa chỉ host ID của lớp network ID cơ sở.

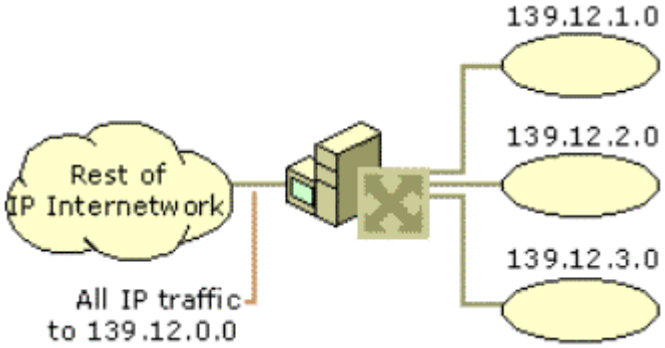
Hãy xem hình 7. Một địa chỉ lớp B 139.12.0.0 có thể có 65534 nút. Giá trị này quá lớn và trong thực tế các mạng hiện này nó trở thành bão hòa với truyền thông quảng bá. Việc chỉ mạng 139.12.0.0 có thể được thực hiện theo một cách mà không ảnh hưởng hay không cần cấu hình lại các địa chỉ IP còn lại của mạng.



Hình 7. Mạng 139.12.0.0 trước khi chia

Mạng 139.12.0.0 được chia bằng cách sử dụng bit trong phần địa chỉ trạm (octet thứ 3) cho địa chỉ mạng con mới network ID. Khi địa chỉ 139.12.0.0 được chỉ nhỏ như trong hình 8, chia mạng thành các mạng con khác có địa chỉ network ID (139.12.1.0, 139.12.2.0, 139.12.3.0) được tạo ra. Router nhận các ID của các mạng con này và nó sẽ dẫn các gói IP tới đúng mạng con tương ứng.

Phần còn lại của địa chỉ IP vẫn dành cho tất cả các nút trên ba mạng con như với mạng 139.12.0.0. Các router khác trong mạng sẽ không nhận ra việc phân chia mạng 139.12.0.0 và vì vậy không cần cấu hình lại.



Hình 8. Mạng 139.12.0.0 sau khi chia mạng con

Nhân tố chính trong việc chia mạng vẫn thiết. Đó là cách router mà mạng bị chia 139.12.0.0 làm thế nào mà biết mạng bị chia và mạng con nào sẵn sàng trên giao tiếp router đó? Để đưa ra địa chỉ IP của một nút với với mức nhận dạng mới, router phải nói chính xác cách phân biệt mạng địa chỉ mạng con mới so với lớp địa chỉ Internet. Để nói chính xác địa chỉ IP nút, dựa trên lớp hoặc mạng con, một subnet mask được sử dụng.

Subnet masks

Với sự phát triển của việc phân chia mạng, khi đó địa chỉ IP không chỉ xác định vào lớp các địa chỉ để xác định network ID trong một địa chỉ IP. Một giá trị mới được dùng để xác định phần nào của địa chỉ IP là network ID và phần nào là host ID, dựa trên phân lớp IP hoặc sự trên network ID mạng con được sử dụng

RFC 950 định nghĩa cách sử dụng subnet mask (còn được gọi là địa chỉ mặt nạ - address mask) như một giá trị 32-bit được sử dụng để phân biệt địa chỉ mạng network ID với địa chỉ máy:

Tất cả các bit tương ứng với network ID được đặt bằng 1.

Tất cả các bit tương ứng với host ID được đặt bằng 0.

Mỗi trạm trên một mạng TCP/IP cần một subnet mask, dù trên một phân đoạn mạng. Hoặc subnet mask mặc định được sử dụng khi network ID dựa trên phân lớp được sử dụng, hoặc một subnet mask tuỳ biến được sử dụng khi chia mạng con hoặc mạng cao hơn được cấu hình trên mỗi nút TCP/IP.

Biểu diễn chấm thập phân của subnet mask

Subnet mask thường được biểu diễn theo dạng chấm thập phân. 32 bit được chuyển thành dạng chấm thập phân, nhưng lưu ý là subnet mask không phải địa chỉ IP.

Một subnet mask mặc định dựa trên địa chỉ lớp IP được sử dụng trên mạng TCP/IP không bị chia thành các mạng con. Bảng 14 liệt kê các subnet mask mặc định sử dụng biểu diễn chấm thập phân.

Bảng 14. Các subnet mask mặc định ở dạng chấm thập phân

Lớp địa chỉ	**Các bit của subnet mask**	**Subnet Mask dạng chấm thập phân**
A	11111111 00000000 00000000 00000000	255.0.0.0
B	11111111 11111111 00000000 00000000	255.255.0.0
C	11111111 11111111 11111111 00000000	255.255.255.0

Subnet mask tuỳ biến khác với các subnet mask mặc định khi chia mạng hoặc gộp mạng. Ví dụ, 138.96.58.0 là một mạng con 8-bit của lớp B. 8 bit của lớp dựa trên địa chỉ host ID đợc sử dụng để biểu diễn ID của mạng được chia. Subnet mask sử dụng tổng cộng 24 bit (255.255.255.0) để định nghĩa địa chỉ mạng con, và được biểu diễn ở dạng chấm thập phân như sau:

138.96.58.0, 255.255.255.0

b. Giao thức IPX/SPX

1. So sánh mô hình mạng của Netware với mô hình OSI.

SAP, NCP

SPX
IPX
MAC Protocols
Application
Presentation
Session
Transport
Network
Data Link
Physical

SAP (Service Access Point): Trong mô hình OSI SAP có một vị trí được xác định rõ, qua đó một thực thể tại một tầng cụ thể có thể đưa ra các dịch vụ để xử lý phục vụ tầng trên.

Để chỉ ra sự phân tầng, chữ cái đầu tiên của tầng đó thường được thêm vào trước cụm từ SAP. Ví dụ: một thực thể của tầng giao vận cung cấp các dịch vụ cho tầng phiên thông qua một TSAP (T-SAP).

Mỗi SAP có một địa chỉ duy nhất. Địa chỉ này có thể được phục vụ như một điểm truy cập tới các dịch vụ của người sử dụng.

NCP (Netware Core Protocol): là giao thức dùng để mã hoá các yêu cầu tới Server và trả lời cho client.

Mỗi gói tin NCP được gửi đi phải được ký bởi client hoặc server gửi gói tin đó. Chữ ký này là khác nhau đối với mỗi gói tin. Nếu nhận được một gói gin NCP không hợp lệ, một thông điệp cảnh báo sẽ được đưa vào trong file nhật ký ở cả hai phía client và server. Thông điệp cảnh báo này chứa địa chỉ của client.

Giao thức IPX (Internetwork Packet Exchange)/SPX (Sequenced Packet Exchange) được xây dựng và sử dụng trong hệ điều hành Netware từ những năm 80.

Novell Netware cung cấp các dịch vụ chia sẻ file, máy in, và ứng dụng, cùng với dịch vụ thư mục đều dựa trên giao thức IPX/SPX.

2. Giao thức IPX

Cấu trúc gói tin IPX:

- Giao thức IPX là một giao thức không liên kết:
- The Transport control field is used for routing. It is set to zero at the source node and then, as the packet passes each router, it is incremented by one. When it reaches 16, the packet is considered undeliverable and is discarded.
- Routing is dependent on the IPX address. IPX addresses are usually written in hexadecimal format, which means that each byte is represented by two characters in the range from A through F or numbers from 0 through 9. This consists of the 4-byte network number assigned by the network administrator, the 6-byte node number (copied from the hardware address of the NIC), and the 2-byte socket address predetermined by the application. When the network administrator assigns the 4-byte network number, it is eight characters long-for example, 4A31F80C. The IPX node address is written as 0A-56-78-9A-BB-FF.
- Việc dẫn đường phụ thuộc vào địa chỉ trên gói tin IPX. Địa chỉ gói tin IPX thường được viết ở dạng chữ số hex, có nghĩa là mỗi byte được biểu diễn bằng hai ký tứ tụ nằm trong khoảng từ A-F, hoặc số từ 0-9. Trong đó bao gồm 4-byte số địa chỉ mạng được gán bởi người quản trị mạng, 6-byte chứa địa chỉ nút (copy từ địa chỉ phần cứng của card mạng), và 2-byte địa chỉ socket được xác định trước bởi ứng dụng. Khi quản trị mạng gán 4 byte địa chỉ mạng, nó gồm 6 ký tự - ví dụ, 4A31F80C. Địa chỉ IPX của nút được viết dưới dạng 0A-56-78-9A-BB-FF.
- Khía cạnh dễ nhầm lẫn nhất của địa chỉ IPX là nó có thể được viết ở nhiều dạng. Hầu hết, khi một địa chỉ mạng IPX được viết ra, những số không ở đầu bị bỏ đi và chỉ viết ở dạng rút gọn; vì vậy một địa chỉ mạng là 0000002A được viết thành 2A. Ký hiệu có thể biến đổi một chú trong cách địa chỉ hoá IPX. Đôi khi một dấu hai chấm được đặt ở giữa, vì vậy một địa chỉ mạng 44ABF128 trở thành 44AB:F128. Các số không không bao giờ được bỏ đi trong địa chỉ của nút, nhưng các dấu hai chấm thờng được thêm vào sau mỗi chu ký 4 số hexa (tương đương với 16 bít). Địa chỉ mạng 44ABF128 trở thành 44AB:F128. Địa chỉ mạng 0A-01-23-FF-45-79 cũng được viết thành 0A01:23FF:4579 hoặc 0A01.23FF.4579.

Một địa chỉ IPX bao gồm ứng dụng, máy tính mà nó chạy trên đó, và vị trí trong mạng vật lý sẽ bao gồm địa chỉ mạng, theo sau bởi địa chỉ của nút và

cuối cùng là địa chỉ của dịch vụ. Điều này có nghĩa là 2AFF:3829:8FC6:7788:AAAA:0004 bao gồm địa chỉ mạng 2AFF3829, địa chỉ của nút 8F-C6-77-88-AA-AA, và địa chỉ dịch vụ 0004.

Các thiết bị định tuyến IPX lan truyền các thông tin định tuyết và quảng cáo (advertisements) tới tất cả các trạm trên mạng sử dụng giao thức RIP (Routing Information Protocol) và dịch vụ Service Advertising Protocol (SAP) hoặc NLSP - NetWare Link Services Protocol. Các thiết bị định tuyến chia xẻ thông tin mà mọi trạm làm việc trên bất kỳ phân đoạn mạng nào cũng có thể truy cập thông tin về các dịch vụ cung cấp trên các phân đoạn khác.

Tìm hiểu RIP và NLSP

Giao thức thông tin định tuyến (RIP) được sử dụng trong bộ giao thức IPX/SPX là một giao thức định tuyến theo vector khoảng cách (Distance Vector) dùng cho quản lý động các bảng dẫn đường IPX. Mặc dù các tên là đồng nhất, không nhầm lẫn RIP của IPX với RIP của bộ giao thức TCP/IP. Hai giao thức này là khác nhau hoàn toàn và không hoạt động cùng nhau được.

Cứ 60 giây RIP gửi các thông điệp cập nhận định tuyến tới tất cả lân cận của server hoặc thiết bị định tuyến. Những gói thông tin lan truyền này không vượt tới các điểm ở xa. Thay vào đó, thiết bị định tuyến nhận được gói thông tin lan truyền RIP cập nhật thông tin trong bảng định tuyến của riêng nó và lại gửi theo kiểu quản bá tới các láng giềng của nó. Giống như một chuỗi các domino bị đổ, mỗi thiết bị định tuyến được cập nhật thông tin mới. Bởi vì RIP sử dụng thông tin gián tiếp, gói tin lỗi có thể gây ra những cơn bão lan truyền làm sập mạng.

NLSP là giao thức khác mà các router IPX có thể sử dụng để xác định đường đi. NLSP là một giao thức tìm đường theo trạng thái liên kết (Link State rout-discovery). Thuật toán Link State NLSP sử dụng cho phép mỗi router nhận được thông tin gốc (firsthand) về trạng thái của các router khác trên mạng, điều này ngăn chặn một số hiện tượng ngẽn và các vấn đề xuất hiện trong các mạng RIP.

Một địa chỉ phụ (thêm vào) được sử dụng trên server NetWare là số mạng nội bộ (internal network number), đó là số định danh logic mọi dịch vụ chạy nội bộ trong mạng. Bởi vì điều này, các server NetWare đều tự động cấu hình dữ liệu định tuyến giữa mạng bên ngoài và mạng nội bộ của nó.

Checksum	Length	Transport control	Packet type	Destination network	Destination node	Source network	Source node	Source socket

SPX và các giao thức khác

Khi một ứng dụng cần đảm bảo việc truyền tin và không cần bao gồm thông tin điều khiển hướng liên kết trong tầng trên của nó, nó phải sử dụng

SPX kết hợp với IPX. SPX hoạt động trên tầng giao vận, cung cấp các chức năng truyền tin hướng liên kết tới các ứng dụng cần nó.

Từ khi SPXX đa đảm bảo việc truyền dữ liệu, tại sao không sử dụng nó với mọi thao tác truyền dữ liệu? Đây là một câu hỏi hay. Lý do chính là SPX được đặt trên tầng mạng. SPX phải gửi các gói tin xác nhận (acknowledgment) theo cả hai hướng để đảm bảo rằng dữ liệu được gửi đi. Nút gửi truyền dữ liệu trước, và rồi nút nhận gửi lại một gói tin xác nhận ACK. Nếu nút gửi không nhận được một gói tin ACK, nó yêu cầu một gói tin ACK hoặc gửi lại dữ liệu. Như bạn thấy, nếu bạn có một ứng dụng vừa phải gửi và nhận các gói tin ACK, quá trình này trở nên rườm rà, không cần bàn đến tính không hiệu quả. Như một phần của dịch vụ phát tin, SPX cung cấp dịch vụ kiểm tra lỗi, điều khiển luồng giữ liệu giữa hai đầu mút (end-to-end), chuỗi, và sửa lỗi. Những dịch vụ này không thêm sự chồng chéo, nhưng chúng cũng làm việc với nhau để đảm bảo dữ liệu được truyền.

Bộ giao thức IPX/SPX bao gồm nhiều dịch vụ có chức năng thuộc các tầng trên của mô hình tham chiếu OSI. Những dịch vụ này bổ sụng chức năng vào bộ giao thức, cho phép ngời sử dụng có được đầy đủ các lợi thế của khả năng mạng.

NetWare shell: NetWare shell làm việc trên các trạm sử IPX/SPXX trong các ứng dụng NetWare client. Nó trong suốt với các lời gọi và ngăn không cho các lời gọi đó thấy mạng hoạt động như thế nào. Nếu lời gọi cần các tài nguyên trên mạng, NetWare shell định hướng lại lời gọi bằng cách truyền nó tới tầng giao thức thấp hơn tương ứng và cuối cùng gửi tới đúng tài nguyên. NetWare shell cung cấp một môi trường trung gian tuyệt vời giữa các ứng dụng không làm việc với mạng. Ví dụ, một trình xử lý văn bản không làm việc với mạng có yêu cầu in qua NetWare shell khi tác vụ in được hướng trực tiếp tới máy in mạng.

Service Advertising Protocol (SAP): SAP đảm bảo rằng tất cả các nút mạng nhận được các dịch vụ đang chia sẻ trên mạng. Cứ 60 giây các gói tin quảng bá SAP được truyền từ server tới các láng giềng của nó. Các láng giềng cập nhận thông tin mới trong bảng SAP của nó và truyền tiếp tới các láng giềng khác của nó. Số dịch vụ có 2 byte ở dạng hex. Ví dụ, mỗi file server NetWare gửi địa chỉ SAP 007 để thông báo cho các trạm rằng nó chia sẻ các máy in.

NetWare Core Protocol (NCP): NCP là giao thức được sử dụng để truy nhập file, máy in, và các dịch vụ bảo mật. Thông qua NCP, các trạm làm việc thâu tóm các dịch vụ từ xa theo cung cách với các dịch vụ cục bộ.

CHƯƠNG 4. MẠNG CỤC BỘ

I. KHÁI NIỆM CHUNG VỀ 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.

Để 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.

II. KỸ THUẬT MẠNG CỤC BỘ.

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)

a. 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.

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

- *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.

b. Mạng hình vòng (ring)

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

- *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.

c. Mạng trục tuyến tính (Bus)

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

Khi một trạm truyền dữ liệu tín hiệu được 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

- *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.

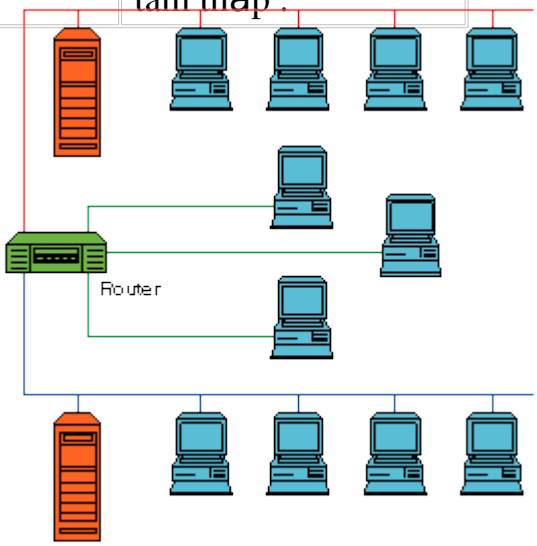
***) So sánh tính năng giữa các cấu trúc của mạng cục bộ.**

	Đường thẳng	**Vòng Tròn**	**Hình sao**
ứng dụng	Tốt cho trường hợp mạng nhỏ và mạng có giao thông thấp và lưu lượng dữ liệu thấp	Tốt cho trường hợp mạng có số trạm ít hoạt động với tốc độ cao,không cách nhau xa lắm hoặc mạng có lưu lượng dữ liệu phân bố không đều.	Hiện nay mạng sao là cách tốt nhất cho trường hợp phải tích hợp dữ liệu và tín hiệutiếng.Các mạng đện thoại công cộng có cấu trúc này
Độ phức tạp	Tương đối không phức tạp	Đòi hỏi thiết bị tương đối phức tạp. Mặt khác việc đưa thông điệp đi trên tuyến là đơn giản, vì chỉ có 1 con đường, trạm phát chỉ cần biết địa chỉ của trạm nhận , các thông tin để dẫn đường khác thì không cần thiết	Mạng sao được xem là khá phức tạp. Các trạm được nối với thiết bị trung tâm và lần lượt hoạt động như thiết bị trung tâm hoặc nối được tới các dây dẫn truyền từ xa
Hiệu suất	Rất tốt dưới tải thấp có thể giảm hiệu suất rất mau khi tải tăng	Có hiệu quả trong trường hợp lượng lưu thông cao và khá ổn định nhờ sự tăng chậm thời gian trễ và sự xuống cấp so với các mạng khác	Tốt cho trường hợp tải vừa tuy nhiên kích thước và khả năng , suy ra hiệu suất của mạng phụ thuộc trực tiếp vào sức mạnh của thiết bị trung tâm.

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

			mỗi cổng truyền của thiết bị trung tâm thấp .

Bảng so sánh tính năng giữa các cấu trúc của mạng LAN



d. 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.

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.

- Chú ý: 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.

- VD: 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.

a. 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:

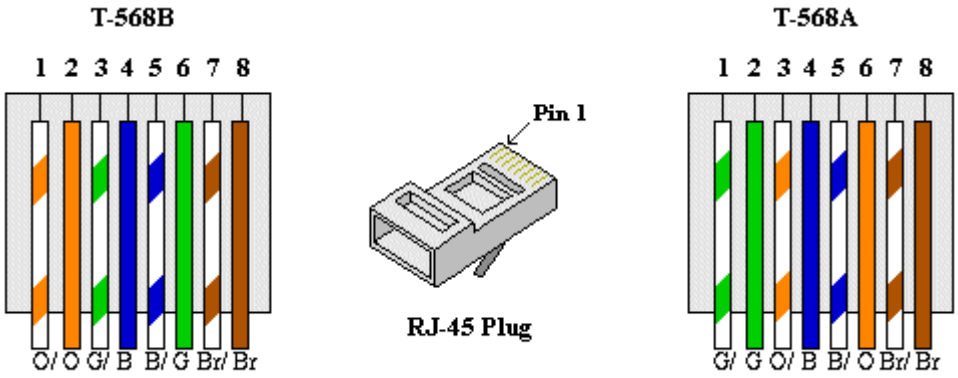
- Loại 1 & 2 (Cat 1 & Cat 2): Thường dùng cho truyền thoại và những đường truyền tốc độ thấp (nhỏ hơn 4Mb/s).
- Loại 3 (Cat 3): tốc độ truyền dữ liệu khoảng 16 Mb/s , nó là chuẩn cho hầu hết các mạng điện thoại.
- Loại 4 (Cat 4): Thích hợp cho đường truyền 20Mb/s.
- Loại 5 (Cat 5): Thích hợp cho đường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

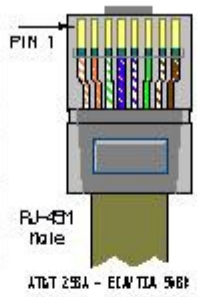


Có 2 kiểu: straight-through và cross-cable hay còn gọi là crossover.

1. 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.

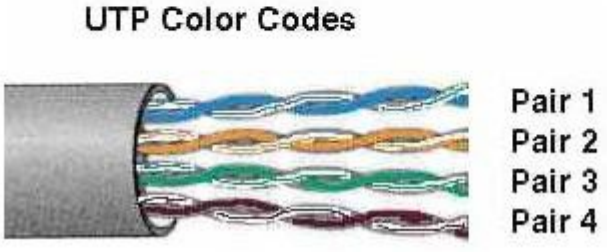
2. Crossover: dùng để nối trực tiếp PC->PC, HUB->HUB hay các thiết bị mạng cùng layer với nhau. Kiểu này phải bấm đảo đầu dây tức là cặp TX (cặp truyền) ở đầu này sẽ trở thành RX (nhận) ở đầu kia bằng cách đổi vị trí của cặp xoắn 2 và 3. Dễ hiểu hơn thì trộn T-568A và T-568B = CrossOver

Crossover Cable	
RJ-45 PIN	RJ-45 PIN
1 Rx+	3 Tx+
2 Rc-	6 Tx-
3 Tx+	1 Rc+
6 Tx-	2 Rc-



Straight Through Cable	
RJ-45 PIN	RJ-45 PIN
1 Tx+	1 Rc+
2 Tx-	2 Rc-
3 Rc+	3 Tx+
6 Rc-	6 Tx-

Note: 1 và 2 là một cặp xoắn, 3 và 6 là một cặp xoắn khác. Số thứ tự 1 2 3 6 là số thứ tự trên đầu nối RJ45. Xem hình RJ45 số 1 được bắt đầu từ bên trái.



Cách bấm cho mạng Lan PC -> HUB/SWITCH

1) Dùng dao cắt bỏ lớp vỏ nhựa bọc ngoài một đoạn khoảng 1,5cm ở đầu dây (nên nhẹ tay vì rất dễ cắt đứt luôn vỏ nhựa của từng sợi dây).

2) Sắp xếp các sợi dây theo thứ tự từ trái qua phải theo sơ đồ sau:

Pin	ID	Dây
1		Cam-trắng
2		Cam
3		Xanh lá cây-trắng
4		Xanh biển
5		Xanh biển-trắng
6		Xanh lá cây
7		Nâu-trắng
8		Nâu

Lưu ý: Hầu hết các đôi xoắn của cáp UTP bán trên thị trường đều theo mầu qui ước (cam + cam-trắng, nâu + nâu-trắng...) , tuy nhiên cũng có những loại cáp mà dây thứ hai trong đôi xoắn chỉ có một mầu trắng rất dễ nhầm lẫn. Bạn cần tách theo từng đôi xoắn để sắp xếp cho đúng.

3) Dùng lưỡi cắt trên kìm bấm để cắt bằng các đầu dây (để lại độ dài khoảng 1,2cm)

4) Lật ngửa đầu nhựa RJ-45 (phía lưng có cái nẫy cho quay xuống phía dưới)

5) Giữ nguyên sự sắp xếp của các dây và đẩy đầu dây vào trong đầu RJ-45 (mỗi sợi dây sẽ nằm gọn trong một rãnh) sao cho các dầu sợi dây nằm sát vào đỉnh rãnh.

6) Kiểm tra lại một lần nữa thứ tự của các sợi dây rồi cho vào kìm bấm thật chặt.

Với đầu dây còn lại bạn hãy làm tương tự như trên.

Sau khi làm xong cả hai đầu thì sợi dây đã sẵn sàng để sử dụng. Không có sự khác biệt về công năng giữa hai đầu dây. Bạn nên đánh dấu từng cặp đầu dây để dễ dàng trong việc kiểm tra sửa lỗi.

b. 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.

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	Bằng đồng, 2 dây, đường kính 5mm	Bằng đồng, 2 dây, đường kính 10mm	Thủy tinh, 2 sợi

	3, 4, 5)			
Loại kết nối	RJ-25 hoặc 50-pin telco	BNC	N-series	ST
Chiều dài đoạn tối đa	100m	185m	500m	1000m
Số đầu nối tối đa trên 1 đoạn	2	30	100	2
Chạy 10 Mbit/s	Được	Được	Được	Được
Chạy 100 Mbit/s	Được	Không	Không	Được
Chống nhiễu	Tốt	Tốt	Rất tốt	Hoàn toàn
Bảo mật	Trung bình	Trung bình	Trung bình	Hoàn toàn
Độ tin cậy	Tốt	Trung bình	Tốt	Tốt
Lắp đặt	Dễ dàng	Trung bình	Khó	Khó
Khắc phục lỗi	Tốt	Dở	Dở	Tốt
Quản lý	Dễ dàng	Khó	Khó	Trung bình
Chi phí cho 1 trạm	Rất thấp	Thấp	Trung bình	Cao
ứng dụng tốt nhất	Hệ thống Workgroup	Đường backbone	Đường backbone trong tủ mạng	Đường backbone dài trong tủ mạng hoặc các tòa nhà

Hình 4.6 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.

c. Cáp sợi quang (Fiber - Optic Cable)

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

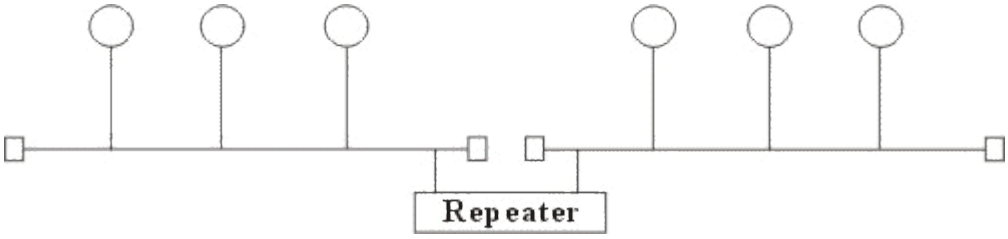
- An toàn, thẩm mỹ: tất cả các dây mạng phải được bao bọc cẩn thận, cách xa các nguồn điện, các máy có khả năng phát sóng để tránh trường hợp bị nhiễu. Các đầu nối phải đảm bảo chất lượng, tránh tình trạng hệ thống mạng bị chập chờn.

- 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. Các thiết bị mạng

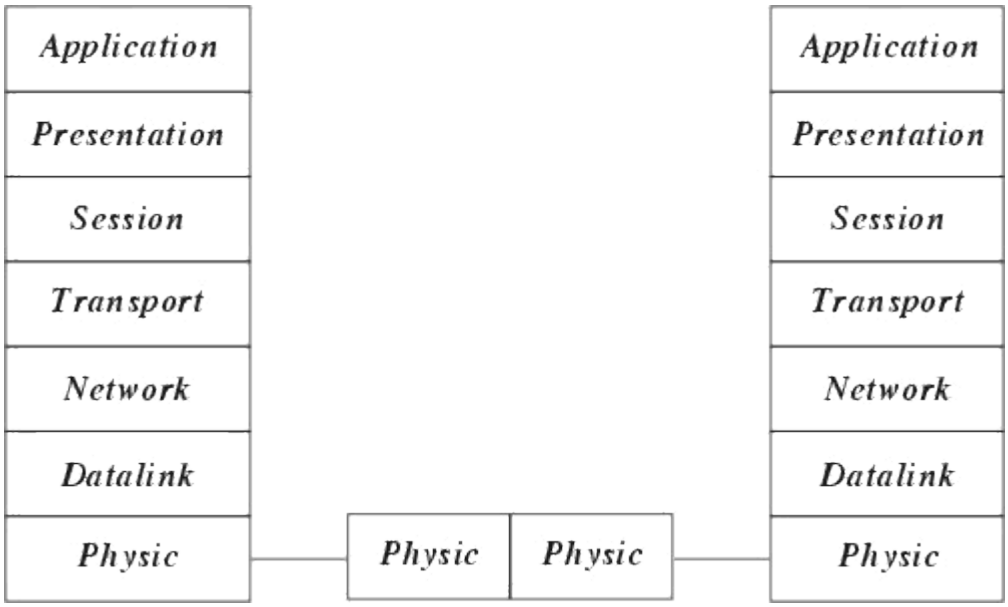
a. Repeater (Bộ tiếp sức)

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 4.7. 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 4.8 Hoạt động của bộ tiếp sức trong mô hình OSI

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

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

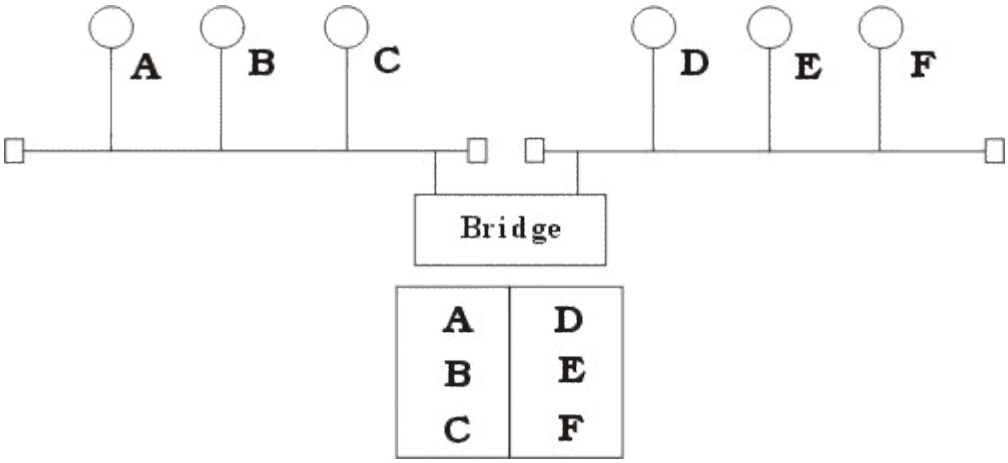
Việc sử dụng Repeater không thay đổi nội dung các tín hiện đi qua nên nó chỉ được dùng để nối hai mạng có cùng giao thức truyền thông (như hai mạng Ethernet hay hai mạng Token ring) nhưng không thể nối hai mạng có giao thức truyền thông khác nhau (như một mạng Ethernet và một mạng Token ring). Thêm nữa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

b. Bridge (Cầu nối)

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

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

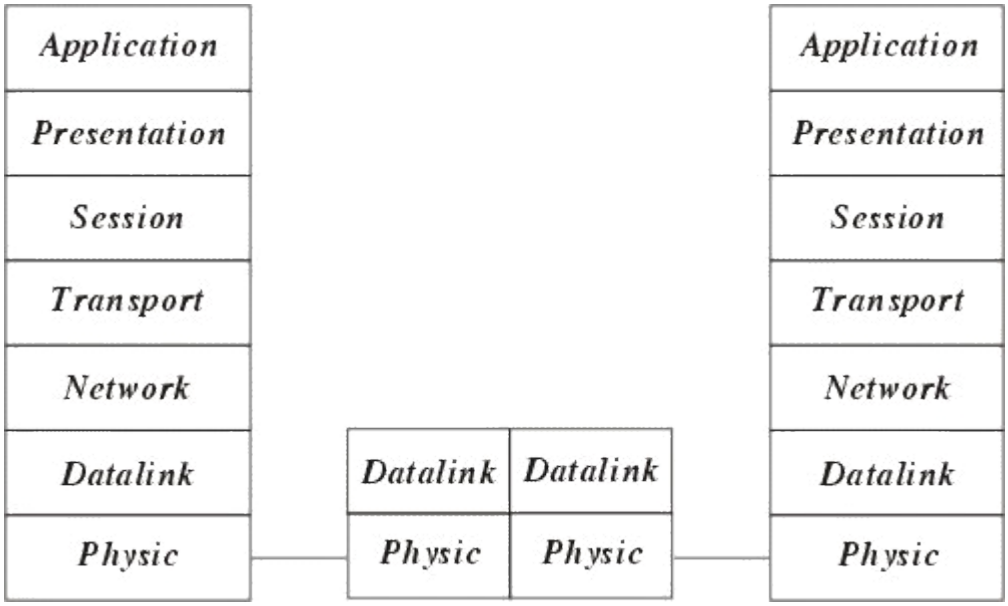
Để thực hiện được điều này trong Bridge ở mỗi đầu kết nối có một bảng các địa chỉ các trạm được kết nối vào phía đó, khi hoạt động cầu nối xem xét mỗi gói tin nó nhận được bằng cách đọc địa chỉ của nơi gửi và nhận và dựa trên bảng địa chỉ phía nhận được gói tin nó quyết định gửi gói tin hay không và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



Hình 4.9 Hoạt động của Bridge

Khi đọc địa chỉ nơi gửi Bridge kióm 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 4.10 Hoạt động của Bridge trong mô hình OSI

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

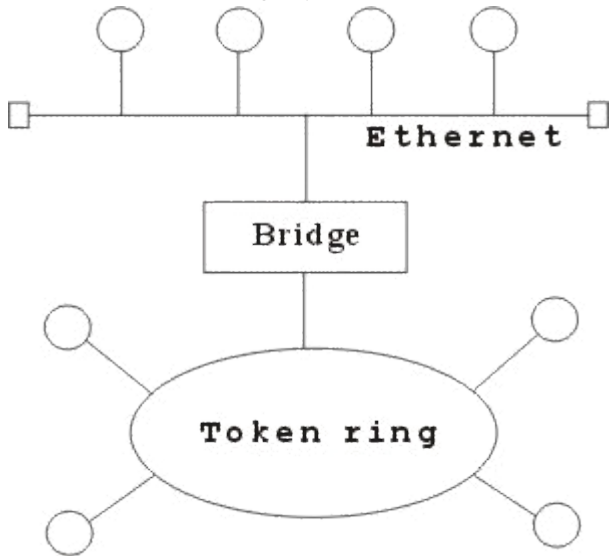
Hiện nay có hai loại Bridge đang được sử dụng là Bridge vận chuyển và Bridge biên dịch. Bridge *vận chuyển* dùng để nối hai mạng cục bộ cùng sử

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

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

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

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

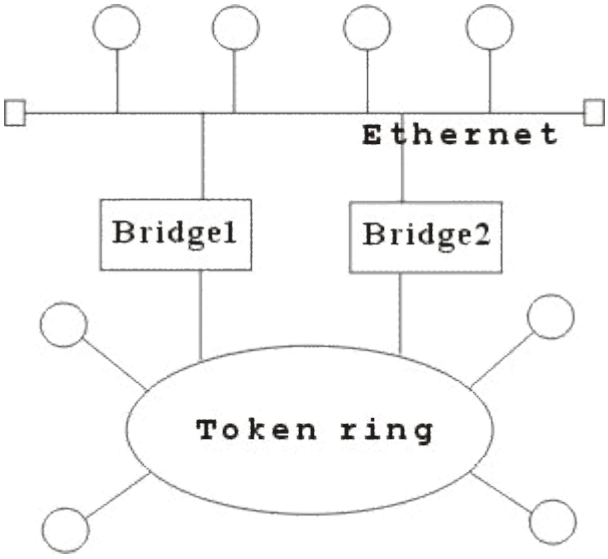


Hình 4.11 Ví dụ về Bridge biên dịch

Người ta sử dụng Bridge trong các trường hợp sau :

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

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

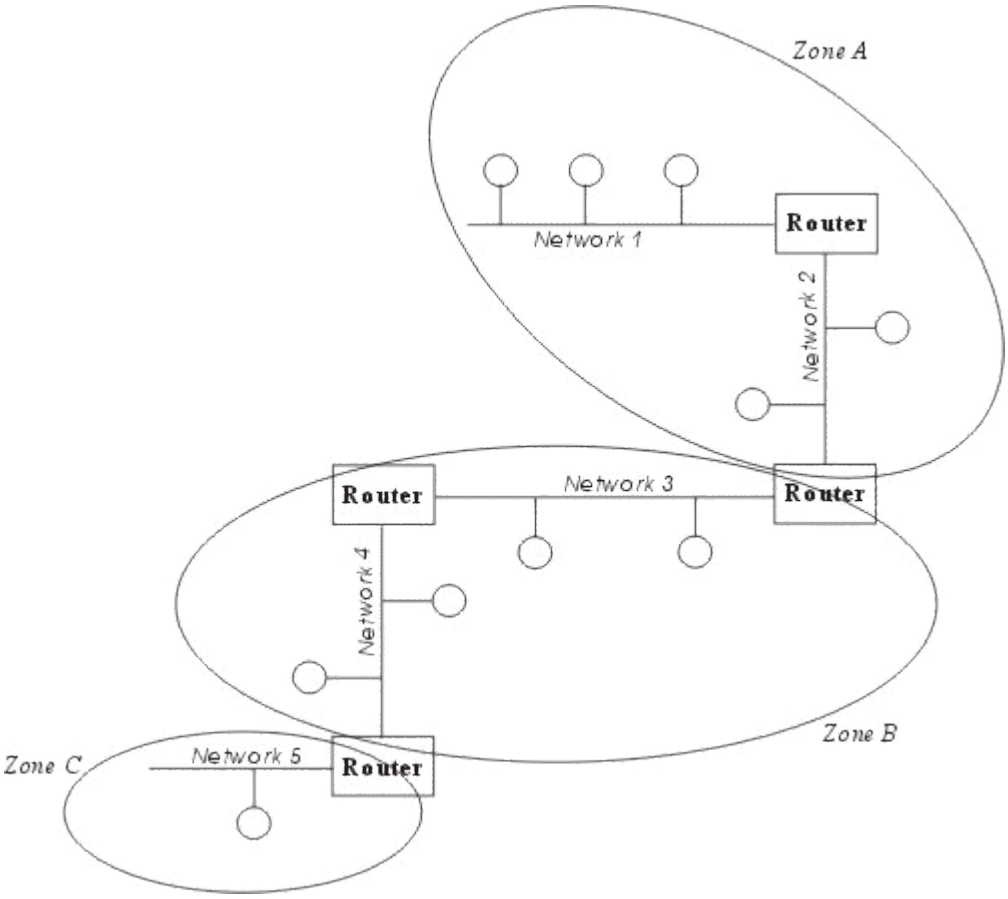


Hình 4.12 Liên kết mạng với 2 Bridge

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

c. Router (Bộ tìm đường)

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



Hình 4.13 Hoạt động của Router.

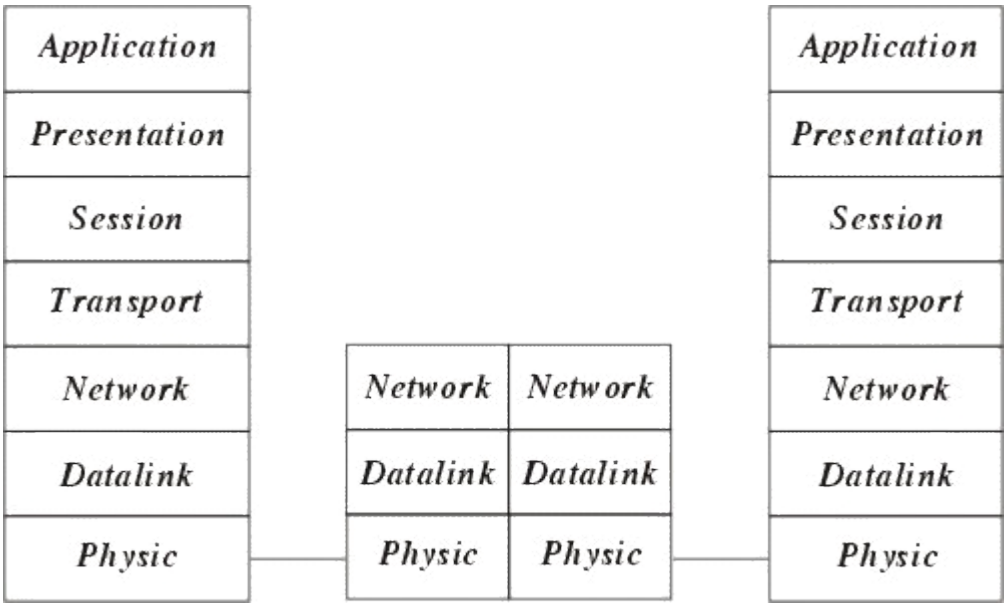
Khác với Bridge hoạt động trên tầng liên kết dữ liệu nên Bridge phải xử lý mọi gói tin trên đường truyền thì Router có địa chỉ riêng biệt và nó chỉ tiếp nhận và xử lý các gói tin gửi đến nó mà thôi. Khi một trạm muốn gửi gói tin qua Router thì nó phải gửi gói tin với địa chỉ trực tiếp của Router (Trong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

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

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

- *Router có phụ thuộc giao thức:* Chỉ thực hiện việc tìm đường và truyền gói tin từ mạng này sang mạng khác chứ không chuyển đổi phương cách đóng gói của gói tin cho nên cả hai mạng phải dùng chung một giao thức truyền thông.

- *Router không phụ thuộc vào giao thức*: có thể liên kết các mạng dùng giao thức truyền thông khác nhau và có thể chuyển đổi gói tin của giao thức này sang gói tin của giao thức kia, Router cũng chấp nhận kích thức các gói tin khác nhau (Router có thể chia nhỏ một gói tin lớn thành nhiều gói tin nhỏ trước truyền trên mạng).

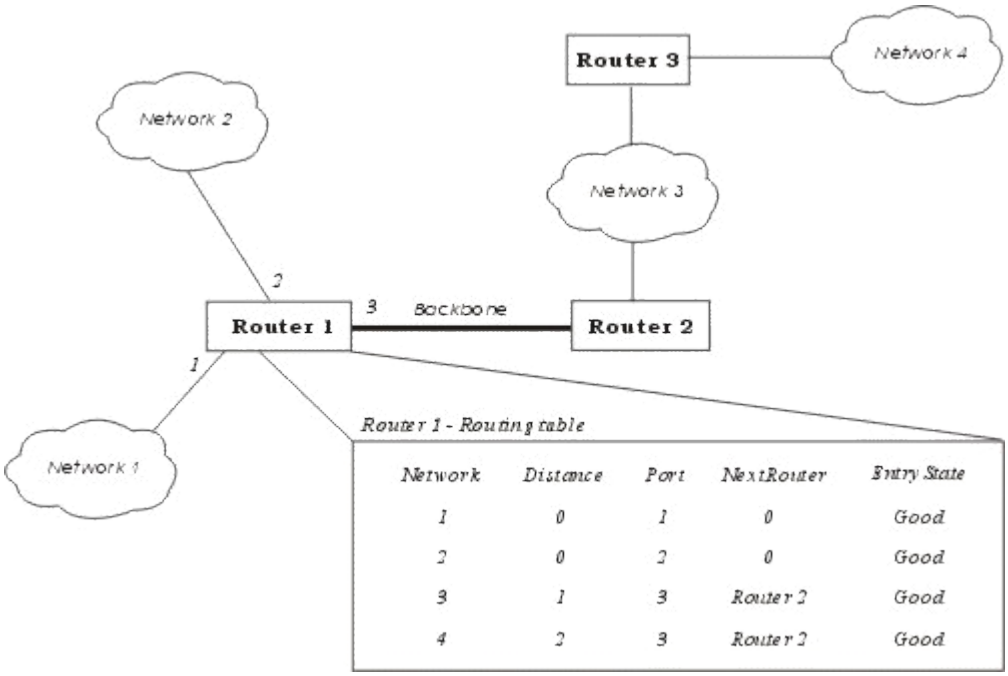


Hình 4.14. Hoạt động của Router trong mô hình OSI

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

Các lý do sử dụng Router :

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



Hình 4.15. Ví dụ về bảng chỉ đường (Routing table) của Router.

Các phương thức hoạt động của Router

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

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

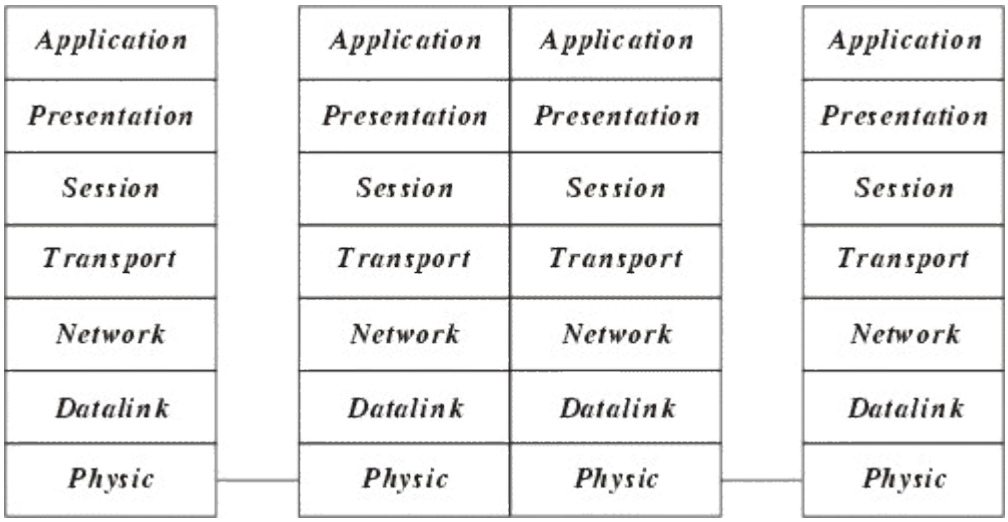
Một số giao thức hoạt động chính của Router

- *RIP(Routing Information Protocol)* được phát triển bởi Xerox Network system và sử dụng SPX/IPX và TCP/IP. RIP hoạt động theo phương thức véc tơ khoảng cách.
- *NLSP (Netware Link Service Protocol)* được phát triển bởi Novell dùng để thay thế RIP hoạt động theo phương 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)

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



Hình 4.16. Hoạt động của Gateway trong mô hình OSI

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

e. Hub (Bộ tập trung)

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

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

- ***Hub bị động (Passive Hub) :*** Hub bị động không chứa các linh kiện điện tử và cũng không xử lý các tín hiệu dữ liệu, nó có chức năng duy nhất là tổ hợp các tín hiệu từ một số đoạn cáp mạng. Khoảng cách giữa một máy tính và Hub không thể lớn hơn một nửa khoảng cách tối đa cho phép giữa 2 máy tính trên mạng (ví dụ khoảng cách tối đa cho phép giữa 2 máy tính của mạng là 200m thì khoảng cách tối đa giữa một máy tính và hub là 100m). Các mạng ARCnet thường dùng Hub bị động.
- ***Hub chủ động (Active Hub) :*** Hub chủ động có các linh kiện điện tử có thể khuyếch đại và xử lý các tín hiệu điện tử truyền giữa các thiết bị của mạng. Qúa trình xử lý tín hiệu được gọi là tái sinh tín hiệu, nó làm cho tín hiệu trở nên tốt hơn, ít nhạy cảm với lỗi do vậy

khoảng cách giữa các thiết bị có thể tăng lên. Tuy nhiên những ưu điểm đó cũng kéo theo giá thành của Hub chủ động cao hơn nhiều so với Hub bị động. Các mạng Token ring có xu hướng dùng Hub chủ động.

- ***Hub thông minh (Intelligent Hub):*** cũng là Hub chủ động nhưng có thêm các chức năng mới so với loại trước, nó có thể có bộ vi xử lý của mình và bộ nhớ mà qua đó nó không chỉ cho phép điều khiển hoạt động thông qua các chương trình quản trị mạng mà nó có thể hoạt động như bộ tìm đường hay một cầu nối. Nó có thể cho phép tìm đường cho gói tin rất nhanh trên các cổng của nó, thay vì phát lại gói tin trên mọi cổng thì nó có thể chuyển mạch để phát trên một cổng có thể nối tới trạm đích.

III. 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.

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")

+ 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).

+ Tiếp tục "nghe" đến khi đường truyền rỗi thì truyền dữ liệu đi với xác suất = 1.

+ 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.

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 điểu 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.

- 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.

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.

IV. THIẾT KẾ MẠNG CỤC BỘ.

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.

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:

<u>Bước1:</u> 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.

<u>Bước2:</u> 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:

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

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

Bước3: 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

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)

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 kiểu LAN.

- Lựa chọn thiết bị mạng, lên danh sách thiết bị.

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

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.

<u>Bước 9:</u> 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.

CHƯƠNG 5. HỆ ĐIỀU HÀNH WINDOWS 2000 SERVER

I. GIỚI THIỆU VỀ WINDOWS 2000 SERVER

II. CÀI ĐẶT

1. Cài đặt máy chủ

Việc cài đặt hệ điều hành có thể thực hiện theo một trong hai cách đó là: cài đặt nâng cấp từ các phiên bản trước của Windows như Win3.x, Win95, 98, NT v.v. hoặc ta có thể cài mới từ đầu. Ở đây chúng ta làm quen với cách cài đặt mới từ đầu.

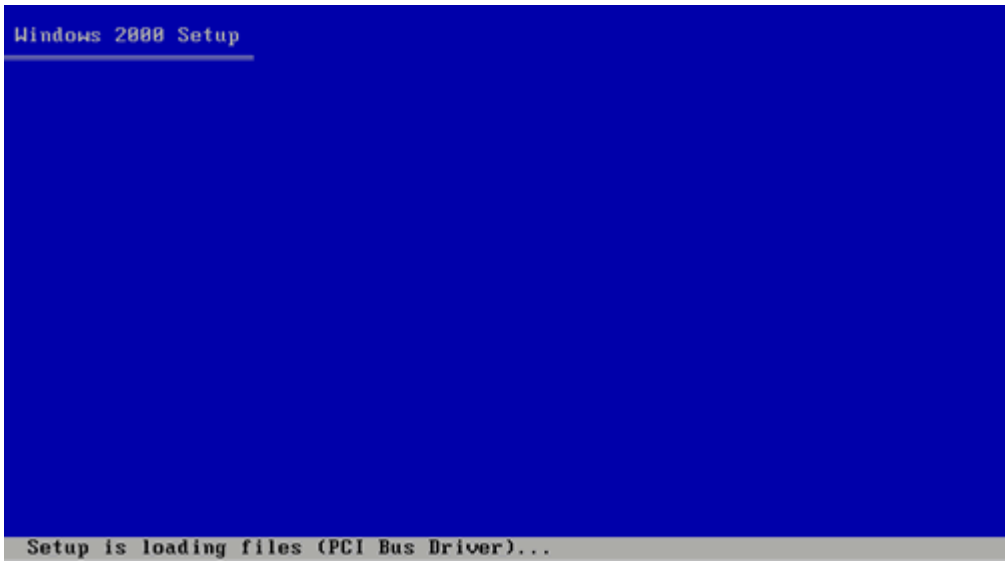
Quá trình cài đặt Windows 2000 thực tế được chia ra làm 3 giai đoạn, giai đoạn đầu tiên là quá trình tiền cài đặt (preinstallation), giai đoạn tiếp theo là cài đặt trên màn hình văn bản (text - based setup), giai đoạn cuối cùng là cài đặt trên màn hình đồ hoạ (graphical – based setup).

) Giai đoạn một: Preinstallation

Để bắt đầu giai đoạn tiền cài đặt Windows 2000, ta truy cập vào nguồn cài đặt vào thư mục I386, tại đây gõ lệnh Winnt.exe hoặc có thể boot trực tiếp từ CD ROM nếu như Bios có hỗ trợ.

) Giai đoạn hai: Text – base setup.

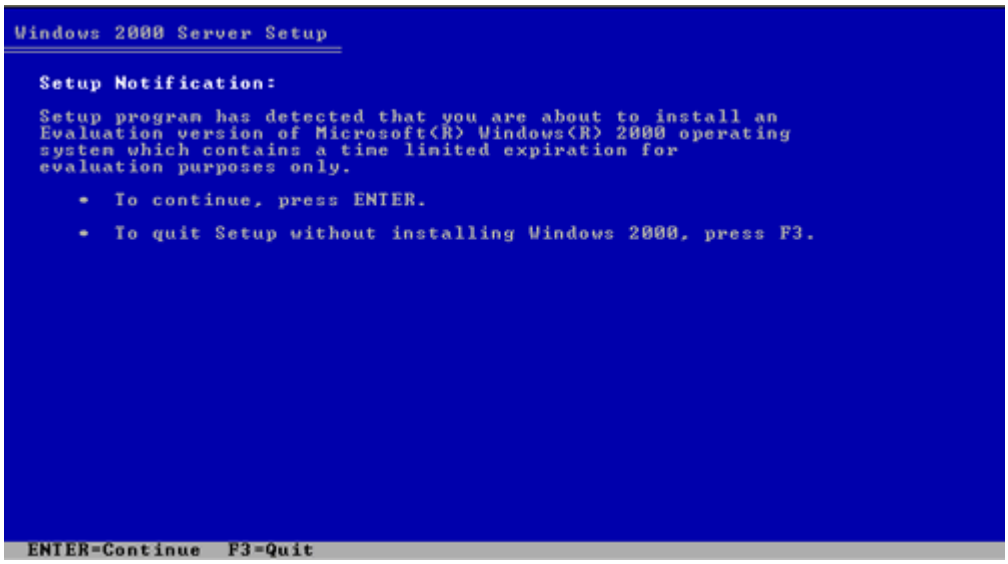
Sau khi boot từ CD ROM hoặc dùng lệnh thì màn hình cài đặt bắt đầu hiện ra như hình 6.1.



Hình 5.1. Màn hình cài đặt

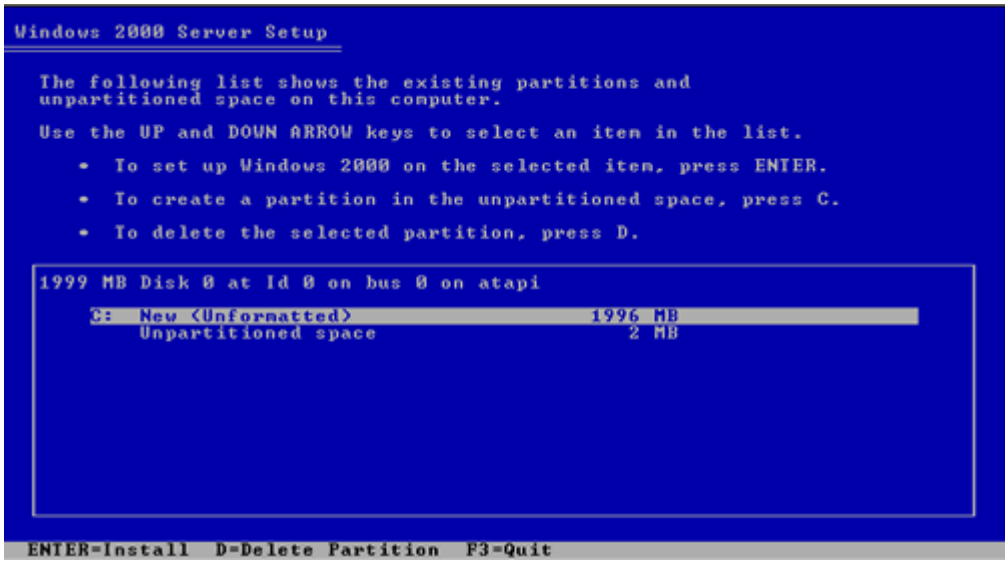
Chương trình cài đặt sẽ xác định các thiết bị phần cứng có trong hệ thống, trong giai đoạn này chương trình sẽ đưa ra lời nhắc rằng hãy ấn F6 nếu bạn cần cài các driver SCSI hoặc RAID, nếu trong máy có các thiết bị theo chuẩn nói trên thì nên chú ý đến lời nhắc đó, nếu không ta chỉ chờ khoảng vài giây thì lời nhắc sẽ kết thúc.

Tiếp theo trong giai đoạn này sẽ bắt đầu bằng một màn hình thông báo để ta lựa chọn (hình 6.2). Ta có thể chọn lựa cài đặt Windows 2000 bằng cách ấn Enter hoặc thoát ra bằng cách bấm phím F3.



Hình 5.2. Màn hình thông báo

Sau khi ấn Enter để tiếp tục quá trình cài đặt thì xuất hiện màn hình 7.3. Tại đây chương trình cho phép ta lựa chọn phân khu để cài đặt Windows 2000, đồng thời cho phép xoá phân khu cũ hoặc tạo ra những phân khu mới.

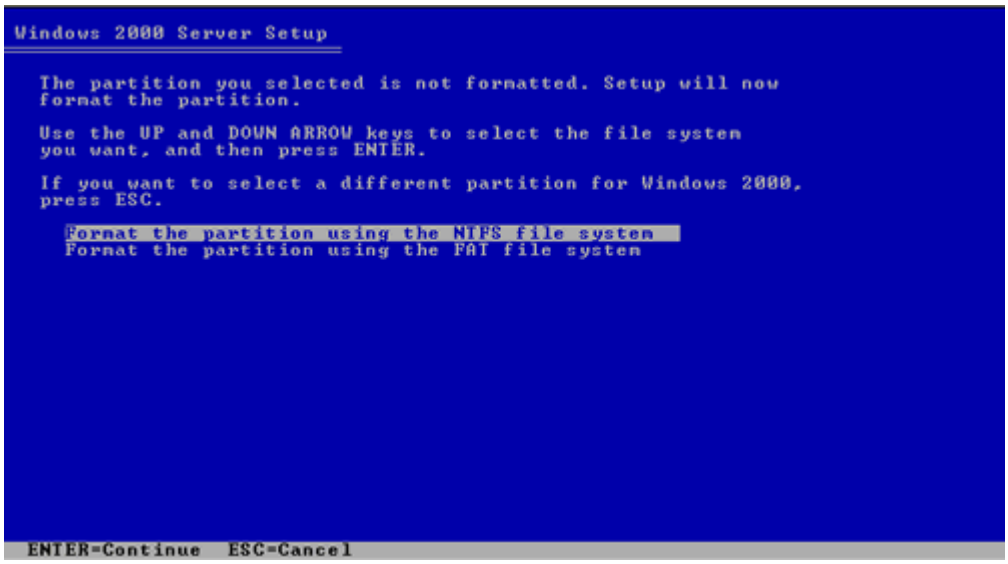


Hình 5.3. Lựa chọn phân khu để cài đặt Windows 2000

Sau khi đã lựa chọn được phân khu, ta có thể lựa chọn khuân dạng của hệ thống sắp xếp các file trên đĩa đồng thời định dạng lại phân khu đó, ở màn hình 7.4. Ta có 2 sự lựa chọn lựa: Hệ thống sắp xếp file kiểu NTFS (New Technology File System) của NT hoặc hệ thống sắp xếp file theo kiểu FAT (File Applocation Table) của DOS.

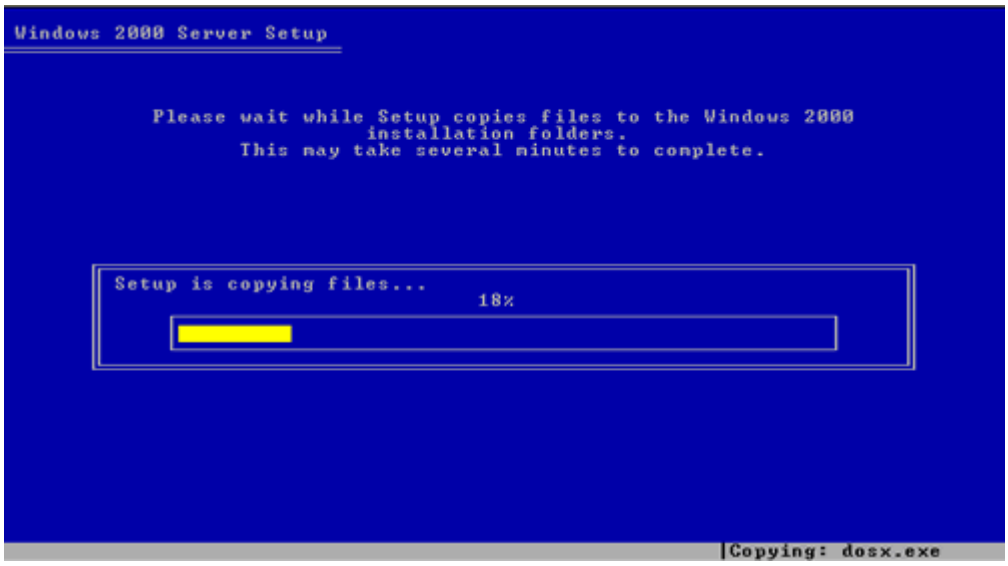
Lựa chọn hệ thống xắp xếp file theo kiểu NTFS nếu ta có ý định nhằm tăng tính bảo mật hoặc khôi phục dữ liệu một cách dễ dàng và sử dụng dịch vụ Active Directory. MicroSoft khuyên nên sử dụng hệ thống file NTFS hơn

FAT. Vì NTFS có tính bảo mật và ổn định cao hơn nhiều so với FAT. Mặc dù vậy cũng nên cân nhắc để sử dụng FAT nếu muốn những hệ điều hành khác có thể truy nhập được vào những phân khu này.



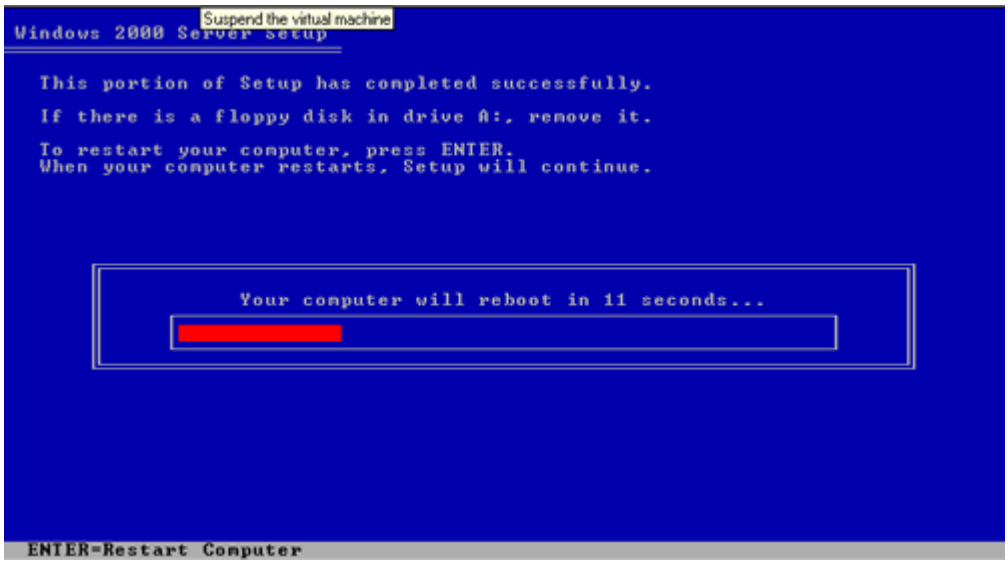
Hình 5.4. Lựa chọn cách sắp xếp hệ thống file khi cài Windows 2000.

Sau khi lựa chọn cách sắp xếp hệ thống file và định dạng lại phân khu, chương trình cài đặt bắt đầu xao chép dữ liệu từ CD ROM vào một thư mục tạm trên ổ cứng để cài đặt Windows 2000 (hình 6.5).



Hình 5.5. Chương trình Setup xao chép file vào đĩa cứng.

Tất cả các file sau khi được xao chép vào một thư mục để cài đặt, trình cài đặt sẽ tự động khởi động lại hệ thống (hình 6.6), và sau đó sẽ tiếp tục quá trình cài đặt.



Hình5.6. Hệ thống khởi động lại để tiếp tục cài đặt.

) Giai đoạn 3: Graphical – based setup.

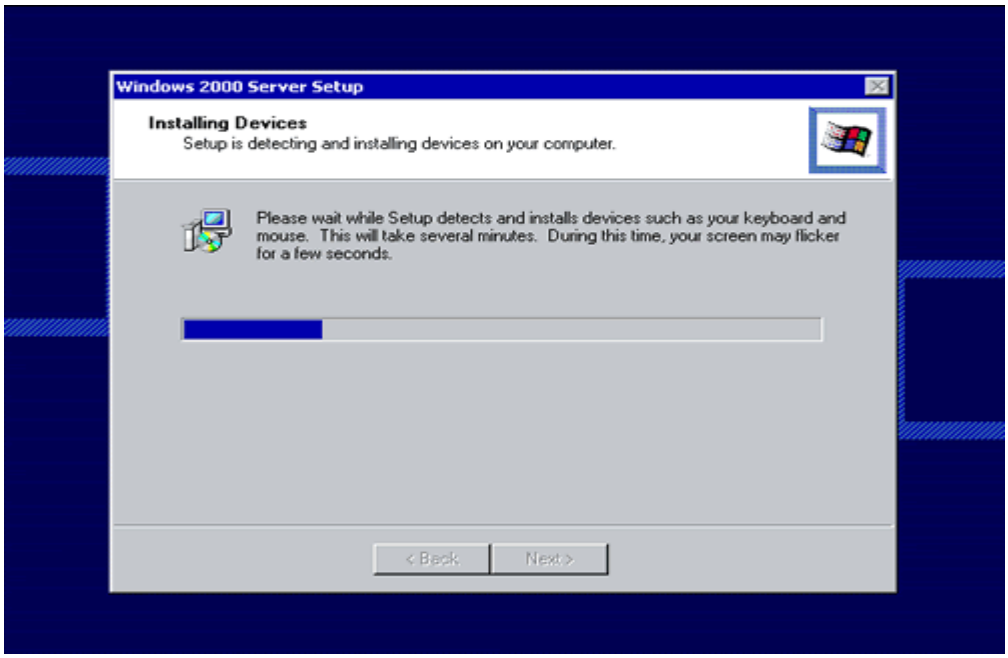
Sau khi hệ thống khởi động lại thì quá trình cài đặt chuyển sang chế độ cài đặt trên màn hình đồ hoạ (Graphical – based setup) (hình 6.7).

Hình 5.7. Giai đoạn cài đặt trong chế độ đồ hoạ

Sau đó màn hình "Welcome to the Windows 2000 setup Wizard" xuất hiện (hình 6.8).

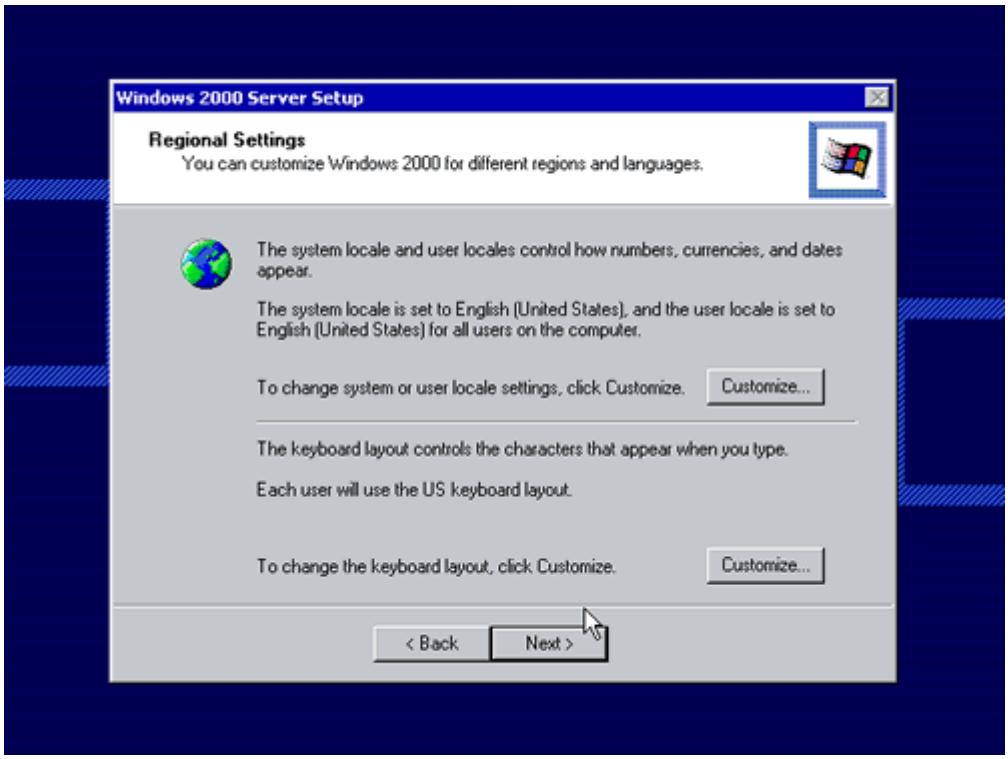
Hình 5.8. Màn hình cài đặt bằng Wizard

Kích vào Next để tiếp tục, màn hình 6.9 hiện ra, Windows tự động dò tìm phát hiện các thiết bị trên máy và tiến hành cài đặt các thiết bị phần cứng trên hệ thống.



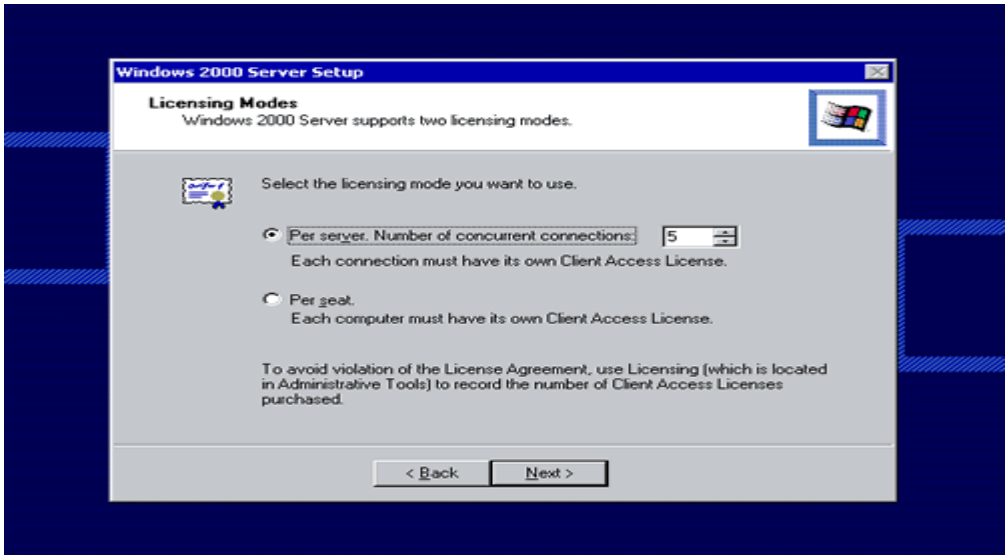
Hình 5.9. Cài đặt các thiết bị phần cứng

Kích vào nút Next để tiếp tục, màn hình 6.10 xuất hiện. Tại đây cho phép ta lựa chọn những định dạng như dạng ký hiệu số, đơn vị tiền tệ, dạng thức ngày tháng, giờ phút, và kiểu bàn phím sử dụng.



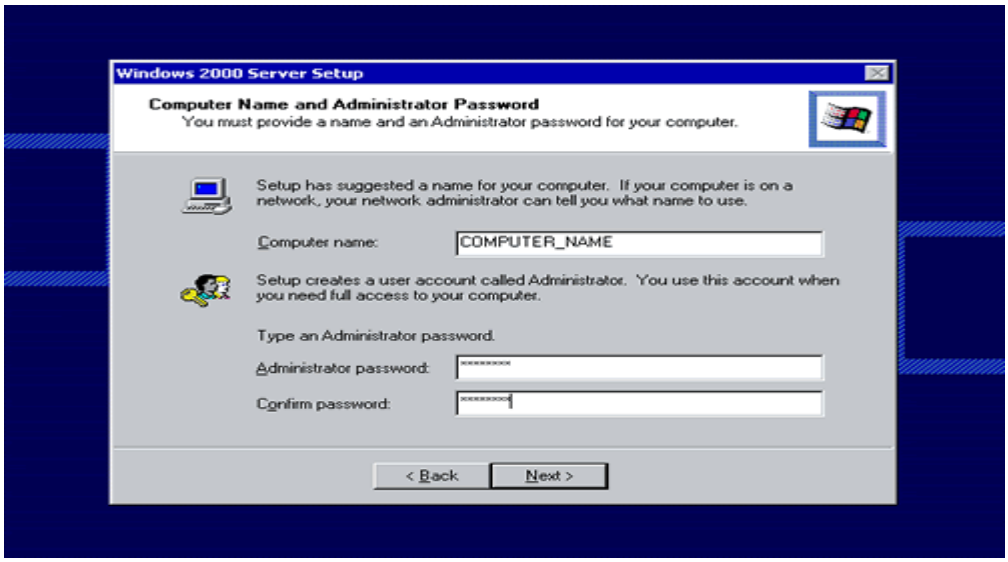
Hình 5.10. Lựa chọn thiết lập

Sau khi lựa chọn khung hội tiếp theo xác định kiểu cấp phép (licesing) hình 6.11. Có hai kiểu Per Server và Per Seat.



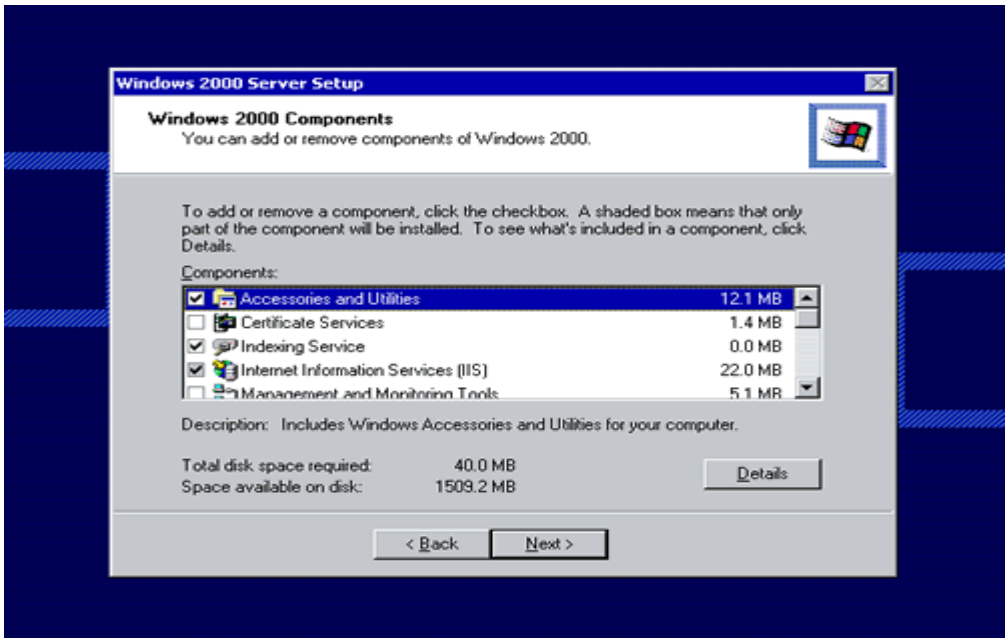
Hình 5.11. Xác lập kiểu cấp phép

Tiếp tục là đến phần xác định tên máy tính (computer name) và mật khẩu quản trị viên (administractor password) hình 6.12.



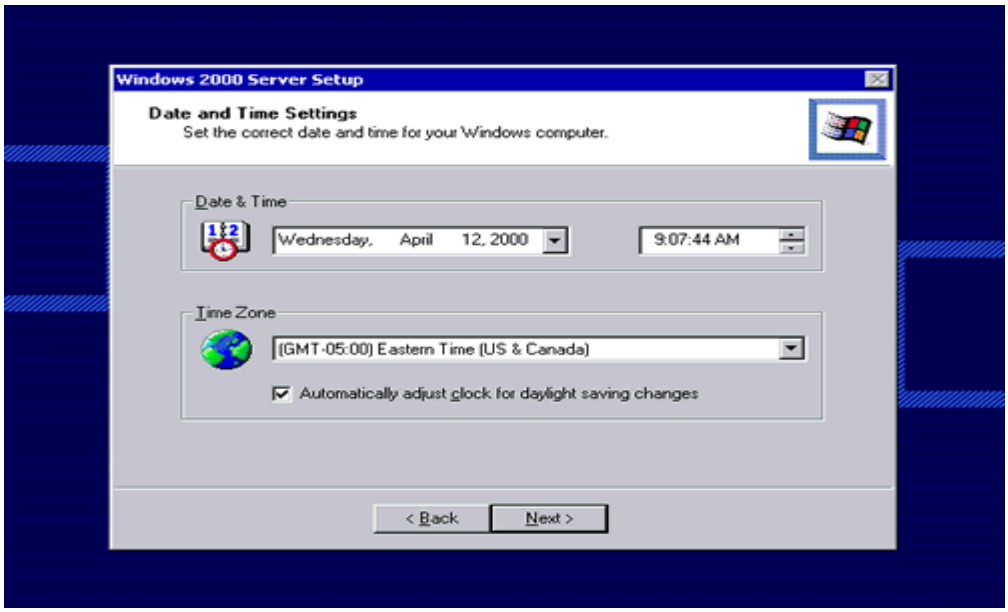
Hình 5.12. Nhập mật khẩu cho người quản trị mạng.

Khung thoại Components Selection giúp ta chọn những thành phần dịch vụ bổ sung được đóng gói trong Windows 2000 (hình 6.13). Phần này ta cũng có thể cài đặt thêm về sau bằng cách vào mục Add/Remove Programs trong Control Panel.



Hình 5.13. Lựa chọn những thành phần cần cài đặt

Khung thoại kế tiếp cho phép ta định cấu hình ngày tháng, múi giờ theo mẫu (hình 6.14).



Hình 5.14. Thiết lập ngày giờ hệ thống và múi giờ.

Khung thoại **Network Settings** hình 6.15 cho phép lựa chọn một trong hai kiểu cấu hình mạng: **Typical** (thông thường) và **Custom** (theo lựa chọn riêng).

- Kiểu **Typical** giả định rằng chỉ cần dùng Client for MicroSoft Network, TCP/IP có dùng cách thức xác định địa chỉ DHCP[1], và File and Print Sharing.

- Kiểu **Custom** ta có thể thêm vào, bớt đi, hoặc tuỳ biến các giao thức, phần mềm nối mạng ở máy khách, và các dịch vụ. Nếu muốn ấn định địa chỉ IP tĩnh, ta chọn **TCP/IP** rồi nhắp nút **Configure**, sau khi nhắp nút **Add**, ta sẽ được chọn lựa **Client**, **Protocol**, hoặc **Service**.

Hình 5.15. Màn hình Network Setting

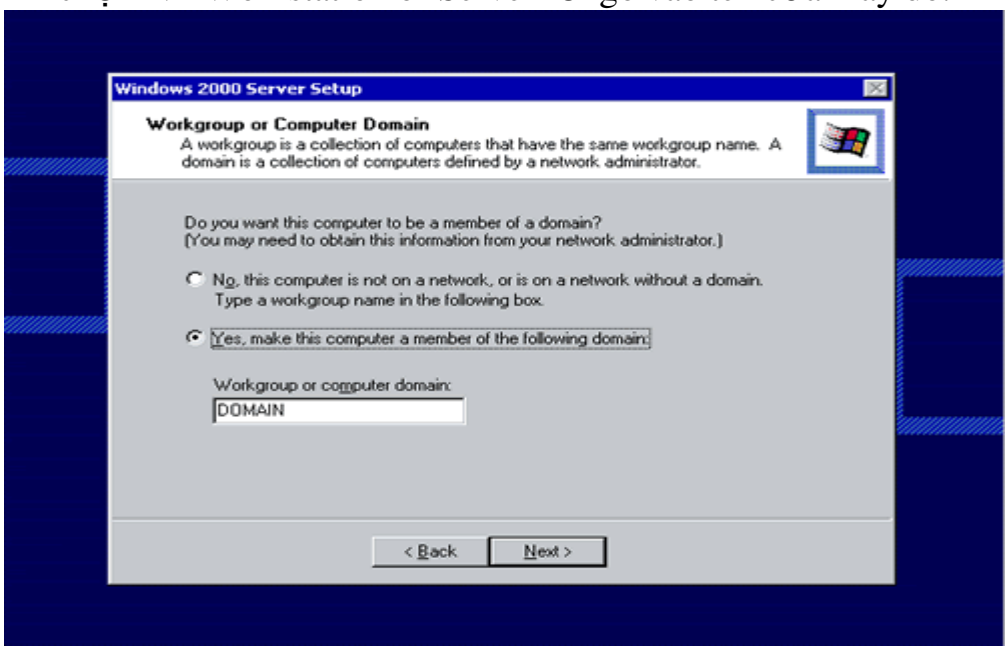
Tại màn hình chọn workgroup/domain hình 6.16 ta có thể chọn máy này ra nhập một nhóm công tác hoặc một miền bằng cách chọn các nút tương ứng rồi gõ vào tên nhóm công tác hoặc tên miền tương ứng. Nếu chọn ra nhập một miền thì ta phải tạo ra một tài khoản giành cho tên máy. Để tạo tài khoản ta có thể làm bằng hai cách.

- Cách 1: Chọn nút **Create Computer Account**. Sau khi nhắp OK để ra nhập vào một miền, ta sẽ được yêu cầu nhập tên một tài khoản để quản trị và mật khẩu tương ứng, tài khoản này phải có quyền hạn **Administractor** hoặc **Account Operator**. Nếu định dùng tài khoản từ một miền được uỷ quyền của miền mà ta định ra nhập, thì nhập đầy đủ tên miền và tên tài

1 Cho phép định địa chỉ IP trên mạng một cách tự động.

khoản theo dạng thức DoMain/username. Như thế sẽ thông báo cho máy DC[2] xác minh về vị trí tài khoản đó sẽ được khởi sự từ Server mà ta đang cài đặt.

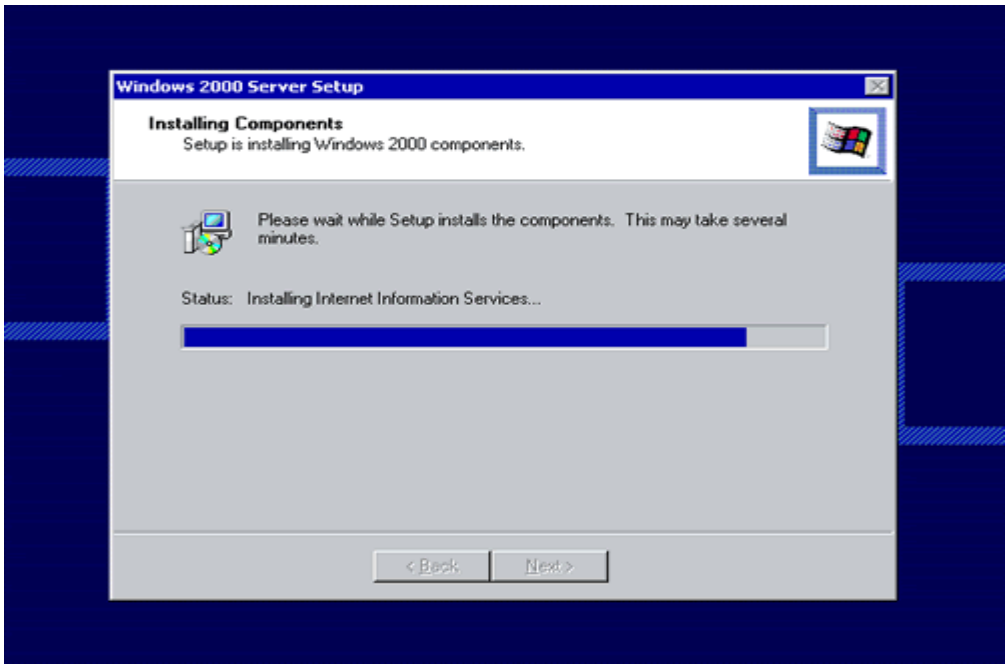
- Cách 2: Không chọn nút **Create Computer Account.** Mà dùng một tài khoản được tạo từ trước. Đến màn hình Server Manager giành cho miền mà ta muốn thêm Server này vào đó rồi chọn Computer, Add to domain, hoặc đến màn hình Active Dierectory Users and Computer rồi chọn New, Computer, chọn NT Workstation or Server rồi gõ vào tên của máy đó.



Hình 5.16. Màn hình chọn workgroup/domain.

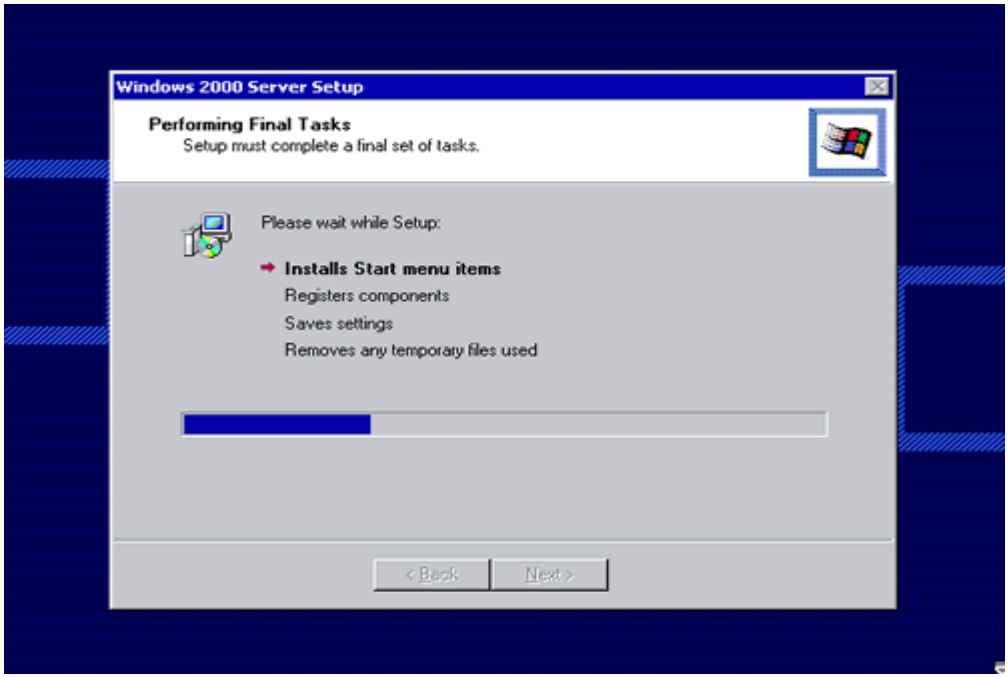
Sau khi cho biết thông tin lựa chọn về Workgroup hoặc Domain, Windows 2000 sẽ bắt đầu tiến hành cài đặt theo những thành phần đã được lựa chọn hình 6.17.

2 DC – Domain Controller là những máy có chức năng xử lý việc đăng nhập và xác minh trong mạng



Hình 5.17. Màn hình Installing Components

Sau đó là màn hình 6.18 xuất hiện để hoàn thành quá trình cài đặt



Hình 5.18. Windows kết thúc quá trình cài đặt

Cài đặt không cần theo dõi.

Cài đăt không cần theo dõi chỉ đơn giản là phương thức cung cấp các câu trả lời cho những câu hỏi của quá trình cài đặt trước khi chúng được hỏi để tự động hoá quá trình cài đặt, cài đặt không cần theo dõi nhằm tiết kiệm thời gian, công sức. Để làm được việc nay ta có 2 cách. Thứ nhất thêm vào các tham biến dòng lệnh sau Winnt.exe hoặc Winnt32.exe. Các tham biến này chỉ ra cách để giai đoạn tiền cài đặt ban đầu sao chép các tập tin và chuẩn bị máy để cài đặt. Thứ hai là, cung cấp một tập tin trả lời (answer file) để trình cài

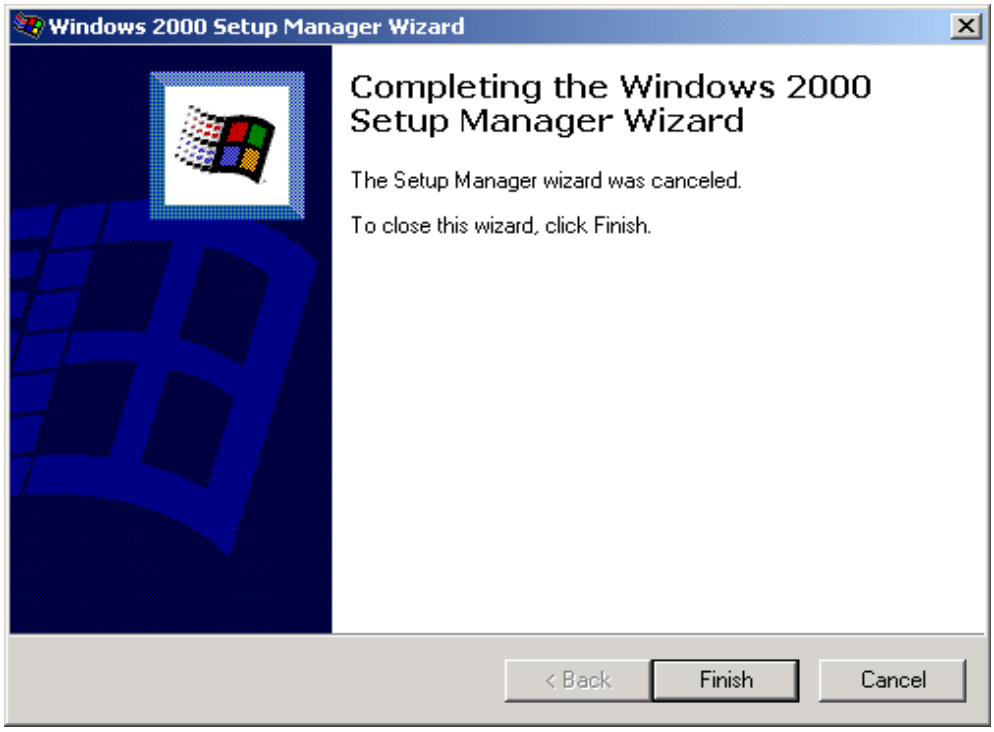
đặt dùng để trả lời cho những câu hỏi về các thành phần cài đặt của Server và những tuỳ trọn trong giai đoạn Graphical – base setup.

2. Tự động hoá bằng các tham biến dòng lệnh.

Các tham biến dòng lệnh báo cho trình cài đặt biết các tập tin nguồn cài đặt ở đâu, muốn cài Windows 2000 Server vào đâu, tập tin trả lời phải được đặt ở đâu, và những thông tin cần thiết khác để chuẩn bị cho việc cài đặt. Cũng có tham biến dòng lệnh để sao chép một folder để bổ xung vào nguồn cài đặt, để có thể dùng được những tập tin đó khi cài đặt.

3. Setup Manager Wizard.

SMW – Setup Manager Winzard là một chương trình cho phép ta tạo ra các tập tin trả lời và tiến hành cài đặt Windows 2000 Server (tức Setupmgr.exe). Được tìm thấy trong chương trình Win2000 Resource Kit Deployment Tool (tức Deploy.cab trong thư mục Support\Tools trên đĩa CD – ROM cài đặt Win2000. Wizard này dẫn ta đi qua tất cả những câu hỏi mà ta cần phải trả lời trong một cuộc cài đặt, và xây dựng cho ta một tập tin trả lời. Màn hình cài đặt của SMW hình 7.1



Hình 5.19. Màn hình cài đặt SMW

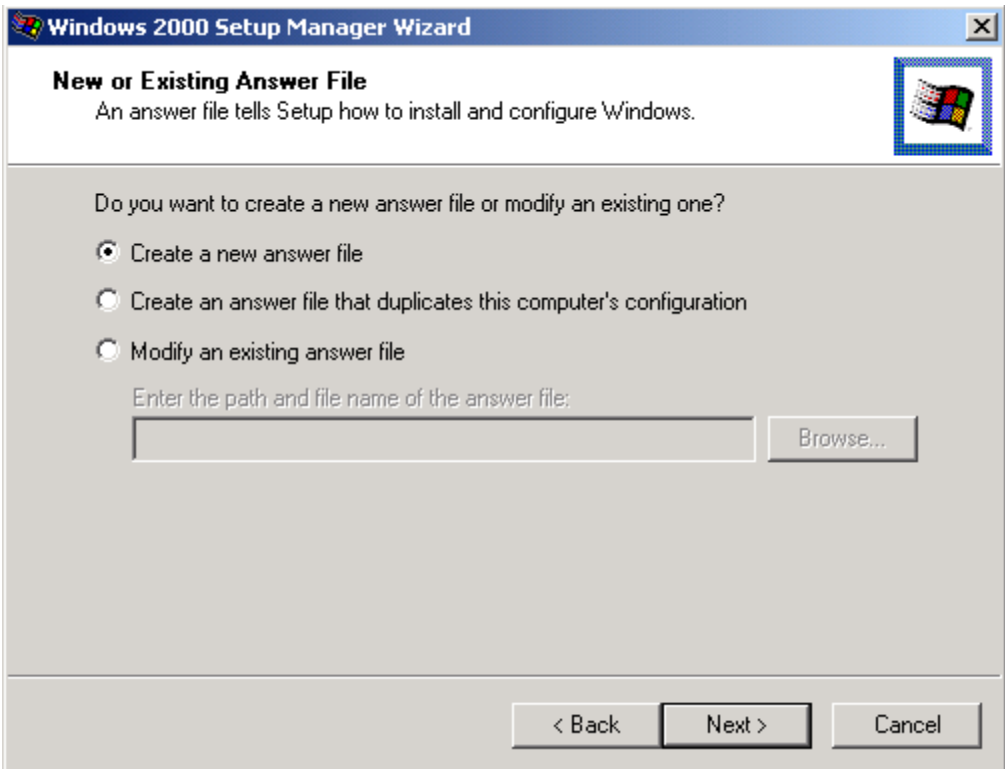
4. Xây dựng tập tin trả lời.

Vào lúc chạy SMW ta sẽ được hỏi một trong 3 điều sau đây hình 6.20:

Xây dựng một tập tin trả lời mới

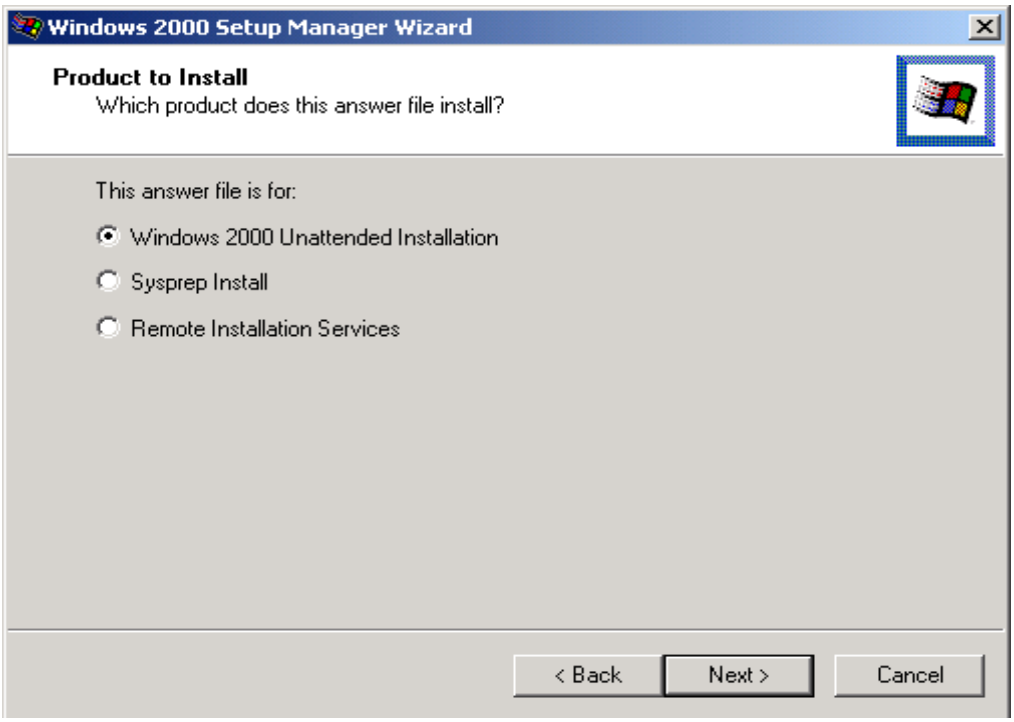
Xây dựng một tập tin trả lời theo cấu hình hiện tại của máy bạn.

Sửa đổi một tập tin trả lời có sẵn



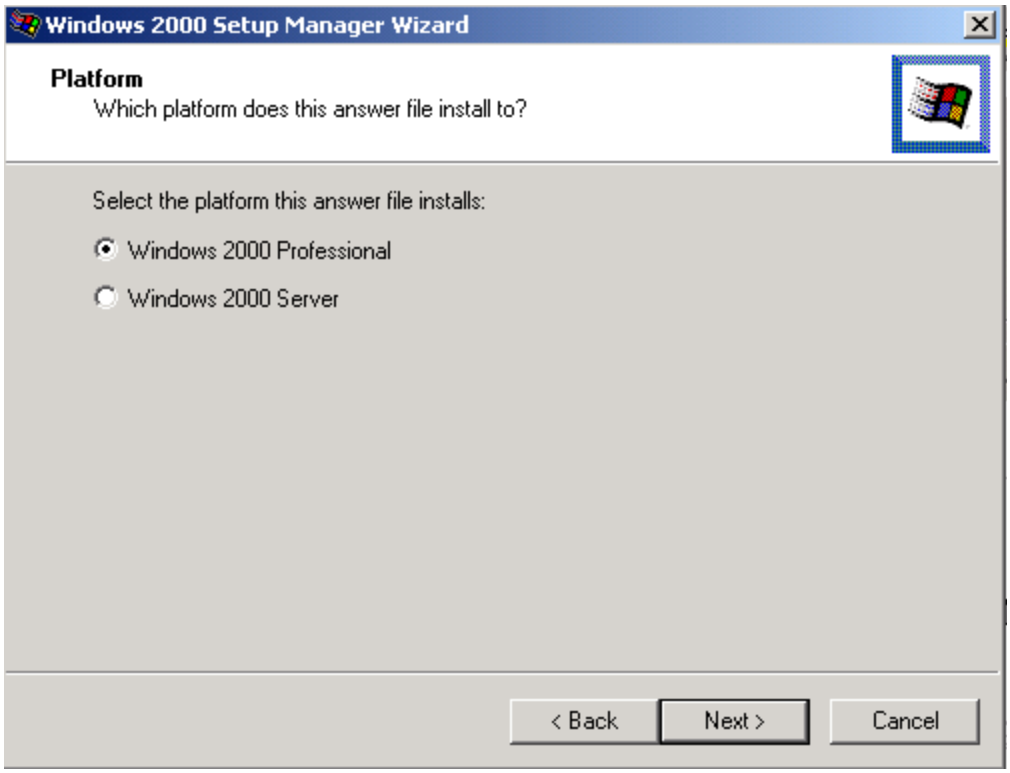
Hình 5.20. Lựa chọn kiểu xây dựng tập tin

Lựa chọn một một mục thích hợp (giả sử mục tạo mới) sau đó ấn Next màn hình 6.21 hiện ra cho phép chọn loại cài đặt cần tự động hoá.



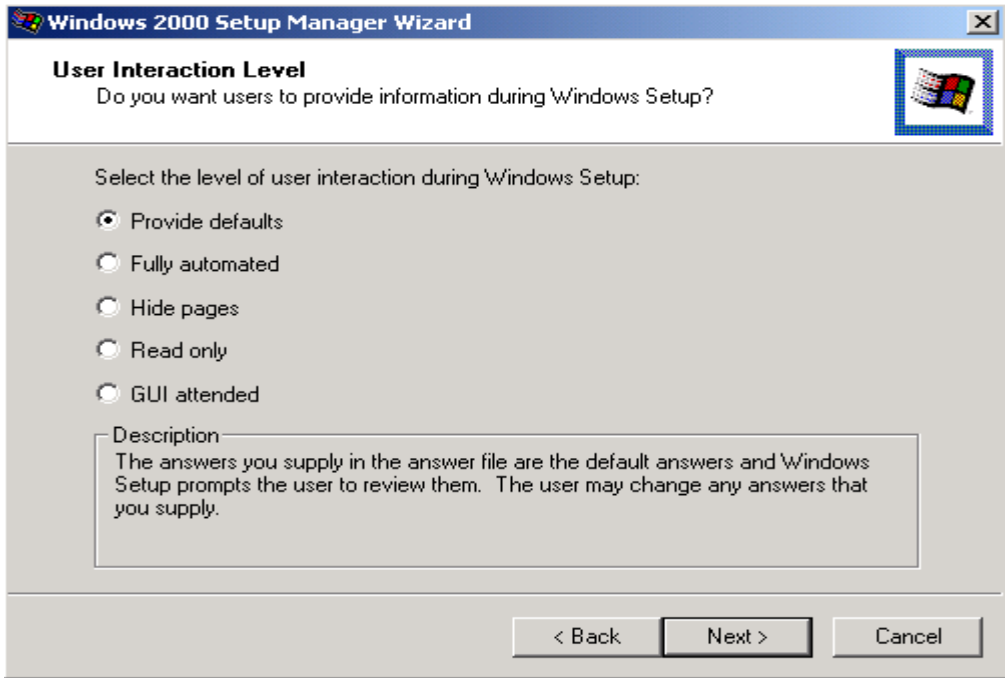
Hình 5.21. Lựa chọn loại cài đặt.

Tiếp theo là lựa chọn hệ điều hành mà ta muốn cài hình 6.22. Ở đây ta có thể chọn tạo tập tin trả lời để cài đặt Win 2000 Server hoặc Pro.



Hình 5.22. Lựa chọn hệ điều hành cần tạo

Sau khi ấn next, màn hinh 6.23 xuất hiện cho phép ta chỉ định cách thức mà cuộc cài đặt sẽ tiếp diễn, theo mức độ nhập liệu cần có từ người sử dụng.



Hình 5.23. Chỉ định cách thức cài đặt

Ý nghĩa các lựa chọn:

Provide defaults Điền vào các câu trả lời mặc định, và người cài đặt chỉ phải chấp nhận các giá trị mặc định đó hoặc thay đổi nếu thấy cần thiết.

Fully automated Điền vào tất cả các câu trả lời, và sau đó để cho chương trình tự động cài đặt hoàn toàn.

Hide pages Người cài đặt chỉ có thể có cơ hội tương tác với trình cài đặt ở nơi nào đã không cung cấp thông tin. Tất cả các trang thoại mà đã được cung cấp thông tin đều được giấu đi.

Read only Tuỳ chọn này cũng tương tự như Hide page, chỉ khác là các trang thoại trong khi cài đặt vẫn sẽ được hiển thị, nhưng người dùng không thay đổi được giá trị mặc định mà đã cung cấp.

GUI attended Với tuỳ chọn này chỉ có giai đoạn cài đặt thứ hai (text base setup) là được tự động hoá, giai đoạn thứ ba (graphical based setup) sẽ giống như một cuộc cài đặt bình thường.

5. Xây dựng một folder phân phối

Sau khi tạo xong tập tin trả lời, Setup Manager Winzard cần biết ta định dùng nó như thế nào. Ta có thể dùng chung nó với nguồn cài đặt trên CD – ROM Win2000 Server hoặc xây dựng một folder phân phối (distribution folder) hình 7.7.

Một folder phân phối là một nguồn duy nhất nhưng chứa đủ thứ: Các tập tin nguồn cài đặt, các tập tin trả lời không cần theo dõi, các tập tin lô để kích hoạt cuộc cài đặt với các tập tin trả lời, các OEM driver, và các tập tin riêng khác mà ta chọn đưa vào đó.

Khảo sát các bước cần thiết để tạo ra một folder.

Điều đầu tiên cần làm là đặt tên cho folder phân phối và chỉ ra vị trí của nó, như minh hoạ ở hình 6.23. Trong hình đó ta chọn folder C:\W2k\disk và để cho nó được dùng chung với tên là w2kdisk.

6. Bắt đầu tiến hành cuộc cài đặt không cần theo dõi.

Bây giờ tất cả những gì cần làm là sử dụng tập tin trả lời. Để bắt đầu cuộc cài đặt không cần theo dõi, ta chỉ việc nối liên lac với folder phân phối hoặc nơi chứa các tập tin mà ta đã tạo ra ở trên. rồi chạy Unattend.bat với một tham biến chứa tên Server thích hợp.

Thay vì dùng Unattend.bat, ta cũng có thể gọi chạy chương trình cài đặt và tập tin trả lời một cách thủ công, sử dụng tham biến dòng lệnh /unattend:filename. Ví dụ ta có một ổ đĩa CD – ROM cài Win2k trong ổ F:, và một kịch bản cài đặt không cần theo dõi tên là Unattend.txt trong ổ C:, ta có thể bắt đầu cuộc cài đặt không cần theo dõi bằng lệnh sau.

F:\I386\WINNT[32] /S:F:\I386 /unattend:C:\unattend.txt

III. CÁC GIAI ĐOẠN HẬU CÀI ĐẶT.

Sau khi hoàn thành 3 giai đoạn cài đặt đối với Windows 2000 Server, vẫn còn vài bước cần thực hiện để định cấu hình lần cuối để chuẩn bị cho nó hoạt động.

Vào lần khởi động đầu tiên, Server Configuration Winzard sẽ tự động hiện lên. Nó sẽ nhận diện vài bước cuối cùng cần phải hoàn tất. Để định cấu hình cho Server ta cần căn cứ vào những thành phần mạng bổ sung mà ta đã cài đặt.

Kiểm tra lại Device Manager xem có thành phần phần cứng nào không được phát hiện hoặc không hoạt động hay không? Trước khi hoàn tất việc cài đặt phải đảm bảo mọi thiết bị phần cứng hoạt động một cách đúng đắn.

Ấn định cho Server một địa chỉ TCP/IP (tĩnh hoặc động).

Cài đặt một số tiện ích để quản trị, và phần mềm để sao lưu dự phòng dữ liệu.

Chạy hết các ứng dụng trong Control Panel để ấn định tất cả cấu hình cho Server.

Khởi động lại máy lần cuối để chắc chắn hệ thống chạy ổn định

CHƯƠNG 6. QUẢN TRỊ MẠNG VỚI WINDOWS 2000 SERVER

I. TẠO RA VÀ QUẢN LÝ CÁC TÀI KHOẢN NGƯỜI DÙNG

Khi cài đặt hệ điều hành thì có hai tài khoản được tạo sẵn đó là Administrator và tài khoản Guest. Ngoài hai tài khoản này người quản trị có thể tạo ra các tài khoản người dùng tương ứng với quyền hạn của người sử dụng trên mạng.

Tạo tài khoản tại chỗ.

Để tạo tài khoản người dùng tại chỗ dùng công cụ **Computer Management.**

Chọn **Start -> Program -> Administrative Tool** -> **Computer Management**. Khi đó sẽ xuất hiện màn hình **Computer Management** như hình 6.25.

Hình 6.1. Màn hình Computer Management.

Trên cây Computer Management lựa chọn **Local Users and Groups**, tiếp tục chọn **Users**, bây giờ kích chuột phải tại Users và chọn New user. Một cửa sổ New user hiện ra và công việc là nhập vào các thông tin yêu cầu như: User name(tên tài khoản); Full name (tên đầy đủ); Description (thông tin mô tả); Password; Comfirm password. Và các lựa chọn như: user must change password at next logon (Người dùng phải thay đổi Password trong lần truy cập đầu tiên); User cannot change password (Người dùng không thể thay đổi Password); Password never expires (); Account is disable (vô hiệu hoá tài khoản) và cuối cùng là kích nút Create như được minh hoạ ở hình 6.26

Hình 6.2. Nhập các thông tin cho user

Muốn thay đổi Password với tài khoản vừa tạo thì chọn tên tài khoản và kích chuột phải sau đó chọn Set Password sau đó nhập tên Password mới và nhấp OK. Tất cả những lựa chọn đối với tài khoản người dùng sẽ được nói rõ hơn trong phần sau.

II. TẠO TÀI KHOẢN TRÊN MIỀN (DOMAIN)

Khi Active Directory được cài đặt thì việc tạo ra các tài khoản người dùng sẽ được tiến hành trên công cụ Active Directory Users and Computers. Sau đây là cách tiến hành tạo các tài khoản người dùng:

Đầu tiên chọn Start\Programs\Administrative Tool, chọn mục Active Directory Users and Computers và cửa sổ Active Directory Users and Computer được mở ra như hình 6.27.

Hình 6.3. Màn hình Active Directory and Computers

Để tạo tài khoản người dùng chọn thành phần Users hay một thành phần nào đó trong cây domain.com (Domain.com là một tên miền mà khi cài đặt hệ điều hành nó được đưa vào). Sau đó từ menu Action chọn New, chọn User (hình 6.28) hoặc chọn biểu tượng Create a new user in then current container trên thanh taskbar.

Hình 6.4. Tạo tài khoản người dùng

Lúc đó sẽ xuất hiện một khung và điền vào tên (First name), họ (Last name), các chữ viết tắt của tên họ (Initials) và tên đầy đủ (Full name). Trong đó Initials và Last name là không bắt buộc phải điền. Tiếp theo điền tên đăng nhập của người dùng (User Logon name), rồi chọn hậu tố của UPN (User Principal Name) để nối vào đuôi của username vào lúc đăng nhập. Hậu tố này thường là tên của Domain như được minh hoạ ở hình 6.29.

Hình 6.5. Màn hình New Object - user

* Chú ý khi đặt tên username

- Username phải là duy nhất trên máy đối với các tài khoản tại chỗ và nó cũng phải độc nhất trên miền đối với các tài khoản trên miền.

- Username không được giống tên của một nhóm trên máy tại chỗ đối với một tài khoản tại chỗ hoặc không được giống như tên của một nhóm trên miền đối với các tài khoản trên miền.

- Username có thể dài đến 20 ký tự có thể là chữ hoa hay chữ thường hoặc kết hợp cả hai.

- Không sử dụng các ký tự sau cho các username: " / \ [ ] : ; | = , + * ? < >

- Usersname có thể có các khoảng trắng và các dấu chấm.

Sau khi điền vào tất cả những thông tin về user thì kích Next. Xuất hiện màn hình đặt mật khẩu để nhập mật khẩu và các tuỳ chọn (hình 6.30)

Hình 6.6. Các lựa chọn

* Giải thích các lựa chọn

- User must change password at next logon: Buộc người dùng này phải thay đổi mật khẩu vào lần đăng nhập kế đó. Sau đó ô này sẽ tự động được bỏ đi.

- User cannot change password: Nếu được chọn nó sẽ ngăn người dùng đổi mật khẩu của tài khoản này. Lựa chọn này phù hợp với tài khoản dùng chung.

- Password never expires: Nếu được chọn, mật khẩu dành cho tài khoản này sẽ không bao giờ hết hạn.

- Account is disabled: Nếu được chọn, tài khoản này sẽ bị vô hiệu hoá và đồng nghĩa với tài khoản này không thể đăng nhập được trừ khi bỏ đánh dấu ở lựa chọn này.

Sau khi đặt password và đánh dấu vào các lựa chọn thì kích vào Next. Sẽ xuất hiện một khung và khung này có nhiệm vụ xác nhận lại tất cả các thông tin đã được cung cấp. Cuối cùng kích Finish để kết thúc việc tạo tài khoản người dùng.

Hình 6.7. Kết thúc tạo tài khoản người dùng

III. CÁC THUỘC TÍNH CỦA TÀI KHOẢN NGƯỜI DÙNG.

Để tìm hiểu các thuộc tính (properties) của tài khoản người dùng tiến hành kích phải chuột vào đối tượng tài khoản đó. Tại đây sẽ có nhiều mục chọn trong menu ngữ cảnh hiện ra lúc này như hình 6.32.

Hình 6.8. Các thuộc tính của tài khoản người dùng

Trên menu ngữ cảnh này ta có thể sao chép tài khoản ấy, làm cho tài khoản người dùng trở thành viên của một nhóm nào đấy (Add members to a group), vô hiệu hoặc hữu hiệu hoá tài khoản (Disable/Enable), ấn định lại mật khẩu của tài khoản, di chuyển tài khoản đến một thành phần khác (Move), mở trang chủ (Open home page) của tài khoản, gửi thư (Send mail) cho tài khoản người dùng và có thể xoá hoặc đổi tên tài khoản.

Để thấy đầy đủ thông tin về tài khoản người dùng thì kích vào mục Properties của menu ngữ cảnh.

Trên Tab General có thể bổ sung một lời mô tả cho tài khoản (Description), tên của văn phòng (office), số điện thoại (Telephone number)...

Tab Address chứa các các trường dành cho địa chỉ (Street,City)....

Nói chung các Tab như: General, Address, Telephones chỉ là những thông tin dùng để giao dịch với người dùng tài khoản đó. Nó không phải là cái mà một quản trị viên quan tâm. Cái mà người quản trị cần quan tâm nó được trình bày ở mục tiếp theo.

IV. CÁC THIẾT LẬP CHO MỘT TÀI KHOẢN.

1. Tìm hiểu trên Tab Account.

- Nếu cần sửa đổi tên đăng nhập của người dùng thì chọn Tab Account trên cửa sổ properties của tài khoản ấy như hình 6.33.

Hình 6.9. Cửa sổ Properties

- Mặc định mọi tài khoản đều được phép đăng nhập vào mọi ngày trong tuần, vào bất kỳ giờ nào trong ngày. Tại Tab này người quản trị có thể thay đổi thời gian được phép vào mạng của người sủ dụng bằng cách kích vào nút

Logon Hours. Màn hình Logon hours xuất hiện dưới hình thức thời khoá biểu trong tuần. Tại màn hình này có thể ấn định ngày nào, giờ nào mà user đó không được phép logon vào mạng bằng cách chọn ngày giờ đó trong thời khoá biểu và chọn Logon Denied (không cho phép Logon) hoặc Logon Permitted (cho phép Logon) như được minh hoạ ở hình 6.34:

Hình 6.10. ấn định quyền truy cập của user

- Để giới hạn trạm làm việc đối với người sử dụng chọn nút Logon To trên Tab Account. Màn hình Logon Workstation xuất hiện. ở đây có hai lựa chọn, lựa chọn thứ nhất (All computer) là tất cả các máy trạm đều có thể đăng nhập được vào tài khoản, Lựa chọn thứ hai (The following computer) thì chỉ có các trạm được thêm vào bởi nút Add mới có thể đăng nhập được vào tài khoản. Ví dụ như hình dưới đây thì chỉ có máy tên là PHONG thì mới đăng nhập được vào tài khoản này.

Hình 6.11. Màn hình Logon Workstation

- Mặc định thì một tài khoản sẽ không bao giờ hết hạn nhưng muốn ấn định khoảng thời gian hết hạnh của một tài khoản thì chọn End of trên Tab Account và kích vào combo box để định ngày hết hạn của tài khoản như được minh hoạ ở hình 6.36.

Hình 6.12. Định ngày tài khoản đăng nhập

2. Tab Profile

Tab Profile là nơi để chỉ định đường dẫn tập tin biên dạng (Profile path), môt kịch bản đăng nhập (Logon script) và một thư mục cơ sở (Home folder) cho người dùng. Các tuỳ chọn này chủ yếu dành cho các phần mềm máy khách đời cũ.

3. Tab Member of

- Dùng để chỉ định các tư cách thành viên nhóm cho một tài khoản người dùng. Theo mặc định một một tài khoản mới tạo ra phải là một thành viên của nhóm Domain users.

Hình 6.13. Chỉ định tư cách thành viên nhóm

- Để thêm một tài khoản người dùng hoặc một nhóm khác vào chọn Add rồi chọn từ một danh sách các nhóm. Nháy kép tên nhóm cần chọn và tên nhóm đó được đưa vào ngăn bên dưới và nhấn OK.

Lúc này tên nhóm được mới được đưa vào cửa sổ Member of

- Để gỡ bỏ người dùng nào đó ra khỏi một nhóm chỉ việc chọn tên nhóm và kich Remove.

CHƯƠNG 7. QUYỀN (RIGHTS) CỦA NGƯỜI SỬ DỤNG TRONG WINDOWS 2000.

Khi một người sử dụng muốn đăng nhập vào mạng thì người đó phải khai báo tên và mật khẩu riêng. Chỉ khi người sử dụng vào đúng tên và mật khẩu của mình thì mới có thể thâm nhập vào được trong mạng. Nhưng để người đó có thể khai thác được tài nguyên mạng thì cần phải có các quyền. Trong Window 2000 có các khái niệm về quyền như sau:

- Permission (quyền truy cập): Là quyền của người sử dụng và nhóm trên thư mục hoặc file. Quản trị viên có thể cho phép người sử dụng hay nhóm nào đó được phép đọc (Read), ghi (Write), xoá (Delete) hoặc thay đổi (Modify) file hay thư mục nào đó.

- User rights (Quyền người dùng): Là quyền của người sử dụng đó ở trên mạng, quyền này hoàn toàn khác với quyền của người sử dụng trên file hay thư mục. Những người sử dụng này có thể không có bất cứ một quyền nào trên file hay thư mục mà chỉ có những quyền ví dụ như shutting down hệ thống, sao lưu và hồi phục dữ liệu. Nói như vậy những người sử dụng này sẽ thuộc về một trong những Domain Local Group nào đó.

- Trong Windows 2000 có các quyền người dùng (user rights) như sau:

+ Access this computer from the network: Nối kết vào máy này ngang qua mạng.

+ Act as part of the operation system: Đóng vai trò như một phần được uỷ quyền của hệ điều hành.

+ Add workstations to domain: làm cho các mày trạm trở thành thành viên của miền.

+ Back up files and directories: Lưu dự phòng các tập tin và thư mục.

+ Bapass traverse checking: Duyệt lướt qua một cây thư mục, cho dù người dùng đó không có quyền truy cập nào đối với thư mục và tập tin đó.

+ Change the system time: Thay đổi giờ giấc hệ thống bên trong máy tại chỗ.

+ Create a pagefile: Tạo một tập tin phân trang (bộ nhớ ảo).

+ Create a token object: tạo các thẻ hiệu truy cập. Chỉ bộ phận Local Security Authority mới có quyền này.

+ Create permanent shared objects: Tạo những đối tượng vĩnh viễn đặc biệt.

+ Debug programs: Gỡ rối các ứng dụng.

+ Deny access to this computer from the network: Thu hồi riêng quyền này đối với những người dùng hay nhóm mà bình thường vẫn có.

+ Deny logon as a batch job: Thu hồi quyền Log on as a batch job.

+ Deny logon as a service: Thu hồi quyền Logon as a service.

+ Enable computer and usre accounts to be trussed for delegation: Chỉ định các tài khoản có thể được uỷ quyền.

+ Force shutdown from a remote system: Buộc máy này phải tắt đi từ một máy ở xa.

+ Generate security audits: Tạo các đề mục ghi chép kiểm toán.

+ Increase quotas: Tăng các hạn ngạch của đối tượng.

+ Increase scheduling priority: Tăng cường độ ưu tiên lịch biểu của một quá trình xử lý.

+ Load and unload device drivers: Thêm hoặc bớt driver vào hoặc ra khỏi hệ thống.

+ Lock pages in memory: Khoá chặt các trang vào trong bộ nhớ để ngăn không cho chúng bị đưa vào trong bộ lưu trữ dự phòng.

+ Log on as a batch job: Đăng nhập vào hệ thống như một phương tiện hàng đợi theo lô.

+ Log on as a service: Thực hiện các dịch vụ bảo mật.

+ Log on locally: Đăng nhập tại chỗ , tại chính máy server này.

+ Manager auditing and security log: Chỉ rõ những loại sự kiện và kiểu truy cập tài nguyên gì sẽ được kiểm toán. Ngoài ra còn cho phép xem và xoá sạch bản ghi chép bảo mật (security log).

+ Modify firmware environment values: Sửa đổi các biến môi trường của hệ thống.

+ Profile single process: Sử dụng những khả năng ghi chép hoạt động của Windows 2000 để kiểm sát, nhận xét hoạt động của một quá trình xử lý.

+Profile system performance: Sủ dụng các khả năng ghi chép hoạt động của Windows 2000 để quan sát, nhận xét hoạt động của hệ thống.

+ Remove computer from docking station: Tháo gỡ một máy laptop ra khỏi hộp nối ghép vào mạng của nó.

+ Replace a process level token: Sửa đổi thẻ hiệu truy cập của một quá trình.

+ Restore files and directories: Khôi phục lại các tập tin và thư mục.

+ Shut down the system: Tắt máy.

+ Synchronize directory service data: Cập nhật thông tin của Active Directory.

+ Take ownership of files or other objects: Chiếm quyền sở hữu của các tập tin, thư mục, và các đối tượng khác, vốn trước đó được những người dùng khác sở hữu.

- Để xem hoặc sửa đổi sự cấp quyền tại chỗ cho một người dùng hoặc nhóm thì dùng công cụ Local Security Policy hoặc công cụ Domain controler

Security Policy, mở cửa sổ Domain controler Security Policy ra bằng đường dẫn : Start\Programs\Administratives Tool. Trong cửa sổ Domain controler Security Policy chọn User Rights Assignment, khi đó một danh sách các quyền được hiện ra bên khung bên phải.

Để thêm hoặc bớt một quyền hạn cho một người dùng hoặc nhóm thì nháy chuột phải vào tên quyền được hiển thị bên ngăn bên phải rồi chọn Security. Nếu tước bỏ một quyền khỏi một nhóm thì chọn tên nhóm và kích nút Remove. Nếu thêm một nhóm hoặc người dùng vào danh sách này thì chọn nút Add, trong hộp thoại Select users of Groups gõ tên người dùng hoặc nhóm cần thêm hoặc kích vào nút Browse để lựa chọn tên người dùng hoặc tên nhóm sau đó chỉ việc nhấp OK. Như hình dưới đây.

I. TẠO NHÓM (GROUP) VÀ TÌM HIỂU CÁC NHÓM TẠO SẴN TRONG WINDOWS 2000.

1. Tạo nhóm trong Windows 2000.

Tài khoản người dùng sẽ có những quyền hạn thực hiện các tác vụ (rights) và quyền truy cập tài nguyên trên mạng (permission) là khác nhau. Để cho dễ quản lý ta đưa cách tài khoản này các nhóm khác nhau tương ứng với các quyền hạn của người dùng tài khoản đó trên mạng. Người quản trị có thể tạo ra các nhóm người dùng theo ý riêng của mình rồi cấp cho chúng những quyền hạn và quyền truy cập nhất định. Sau đây là cách tiến hành tạo nhóm (group) bằng công cụ Active Directory Users and Computers.

Mở của sổ Active Directory Users and Compters bằng cách chọn Start trên thanh taskbar, chọn Programs, chọn Administrative Tool. Khi cửa sổ Active Directory Users and Compters được mở chọn thành phần nào mà muốn đặt nhóm ở đó sau đó chọn Action trên menubar, chọn New, chọn Group.

Một cửa sổ New Object-Group hiện ra. Lúc đó phải cung cấp tên nhóm (Group name), tên kiểu cũ của nhóm (Pre-Windows 2000), chọn phạm vi của nhóm (Group scope) và kiểu của nhóm (Group type) sau đó kích OK như minh hoạ ở hình sau.

Tiếp theo chọn tên nhóm vừa tạo và kích chuột phải chọn properties. Cửa sổ properties của nhóm đó hiện ra và điền các thông tin còn lại, tiếp theo đưa tài khoản người dùng vào nhóm mới tạo bằng cách chọn Tab Members rồi chọn Add sẽ xuất hiện một hình sau:

Tại cửa sổ này chọn tên tài khoản và nhap nút Add sau đó chọn OK để hoàn thành việc đưa thành viên mới vào nhóm.

2. Các nhóm tạo sẵn trong Windows 2000

a. Các Builtin Local Group tạo sẵn.

***) Administrator**

Những thành viên nằm trong nhóm này có mọi quyền hành về quản trị mạng như: Tạo ra và quản lý các tài khoản người dùng, tạo ra và quản lý các global group, trao quyền hạn cho người dùng, khoá chặt server console, mở khoá server console, định dạng đĩa cứng của server, tạo ra các nhóm chương trình chung, chia sẻ và chấm dứt chia sẻ các thư mục, máy in. Những thành viên nằm trong nhóm này còn có thể: Đăng nhập tại chỗ, truy nhập máy này từ mạng, chiếm quyền sở hữu các tập tin, thay đổi giờ giấc của máy, tắt máy, buộc tắt máy này từ một máy ở xa, lưu dự phòng các tập tin và thư mục, khôi phục lại các tập tin và thư mục, thêm và bớt các device drive, tăng độ ưu tiên của một quá trình xử lý.

***) Server Operators**

Những thành viên nằm trong nhóm này có tất cả những quyền hạn cần thiết để quản lý các server của miền. Có thể tạo ra, quản lý, và bỏ bớt các đối tượng máy in dùng chung tại các server; tạo ra, quản lý và xoá bỏ các thư mục mạng dùng chung tại các server; lưu dự phòng và khôi phục lại các tập tin trên các server; định dạng đĩa cứng của một server; khoá chặt và mở khoá các server; mở khoá các tập tin và thay đổi giờ giấc của máy. Ngoài ra các thành viên nằm trong nhóm này còn có thể đăng nhập vào mạng từ các server của miền cũng như tắt đi các server đó.

***) Backup Operators**

Các thành viên nằm trong nhóm này có quyền lưu dự phòng và khôi phục các tập tin, ngay cả khi họ không có quyền truy cập các tập tin đó.

***) Account Operators**

Các thành viên nằm trong nhóm này có quyền tạo ra các tài khoản người dùng và nhóm dành cho miền và có thể sửa đổi hoặc xoá bỏ hầu hết các tài khoản người dùng và nhóm của miền. Thành viên của Account Operators không thể sửa đổi hoặc xoá bỏ các nhóm sau: Administrators, Domain

Admins, Account Operators, Backup Operators, Print Operators, và Server Operator. Ngoài ra các thành viên của nhóm này không thể sửa đổi hoặc xoá bỏ các tài khoản người dùng là quản trị viên. Họ không thể quản trị các chính sách bảo mật, nhưng có thể bổ sung tài khoản máy vào một miền, đăng nhập vào các server và tắt các server.

***) Print Operators**

Thành viên của nhóm này có thể tạo ra. quản lý, và xoá bỏ các đối tượng máy in dùng chung dành cho một server Windows 2000. Ngoài ra họ còn có thể đăng nhập và tắt server.

***) Power users**

Thành viên của nhóm này có thể tạo các tài khoản người dùng và các local group (nhóm cục bộ), quản lý các danh sách thành viên của các nhóm users. Power users và Guest, cũng như quản trị những tài khoản người dùng và nhóm mà họ tạo ra.

***) users**

Thành viên của nhóm này có thể chạy các ứng dụng, nhưng không thể cài đặt chúng. Họ có thể tắt và khoá chặt wordstation (máy trạm). Nếu một thành viên có quyền đăng nhập tại chỗ vào một máy trạm, họ cũng có quyền tạo ra các local group và quản lý các nhóm mà họ đã tạo.

***) Guests**

Thành viên của nhóm này có thể đăng nhập và chạy các ứng dụng. Họ cũng có thể tắt máy.

***) Replicator**

Thành viên của nhóm này chỉ được sao chép danh bạ. Một tài khoản người dùng có thể chạy dịch vụ Replicator, và nó phải là thành viên duy nhất của nhóm này.

b. Các Global group tạo sẵn.

***) Domain Admins**

Khi một tài khoản người dùng được đặt trong global group này thì tài khoản đó có các năng lực ở mức độ quản trị cho ngươì dùng đó. Các thành viên của Domain Admins của một miền có thể quản trị miền đó. Global group này là thành viên của local group Administrator và nó chứa user Administrator.

***) Domain users**

Khi một tài khoản người dùng mới được tạo ra thì nó được nằm trong Domain users.

II. CHIA SẺ (SHARE) TÀI NGUYÊN VÀ QUẢN LÝ CÁC QUYỀN TRUY CẬP.

1. Chia sẻ tài nguyên.

Không có một người sử dụng nào có thể truy xuất các thư mục (folder) hoặc tập tin (file) trên mạng bằng cách đăng nhập vào mạng khi không có một thư mục nào được chia sẻ. Một thư mục được chia sẻ thì các thư mục con (subfolder) và các tập tin nằm trong thư mục đó cũng được chia sẻ. Nếu cần thiết phải hạn chế việc truy xuất tới một phần của cây thư mục, thì phải sử dụng việc cấp các quyền cho user hay một nhóm đối với thư mục hoặc tập tin đó.

Để tiến hành chia sẻ một thư mục thì login vào mạng với tư cách là một quản trị viên (administrator) hoặc một điều hành viên server (server operator).

Tất cả thủ tục chia sẻ thư mục được thực thi trong Windows 2000 explorer.

**** Các bước tiến hành chia sẻ một thư mục:***

- Kích chuột phải tại thư mục cần chia sẻ trong Windows 2000 Explorer xuất hiện một menu ngữ cành.

- Chọn Properties trong menu ngữ cảnh đó. Một cửa sổ Properties của thư mục đó hiện ra chọn Tab Sharing như hình dưới

- Chọn Share this folder để kích hoạt việc chia sẻ.

- Đưa một tên cần chia sẻ vào hộp Share name. Trong hộp này mặc định là tên của thư mục được chọn. Đưa vào dòng ghi chú liên quan đến việc chia sẻ thư mục đó vào hộp comment

- Thiết lập giới hạn số lượng các user truy cập vào thư mục thì kích vào mục Allow và định số user cho nó.

- Nếu muốn hạn chế việc truy xuất thì chọn Permissions

- cuối cùng kích OK.

Sau khi thư mục được chia sẻ thì trên biểu tượng của thư mục đó có hình bàn tay.

* Nếu muốn thêm một chia sẻ mới vào cùng một thư mục (Có thể hai chia sẻ trên cùng một thư mục có các quyền truy cập thư mục đó khác nhau) đó thì thực hiện tương tự như trên và chọn New Share để tạo chia sẻ mới, xuất hiện hộp thoại

Nhập vào tên chia sẻ mới (Share Name) và lời chú thích và cũng chọn số lượng các user được phép truy cập.

2. Quản lý các quyền truy cập đối với tập tin và thư mục

***) Quyền truy cập ở cấp độ Share**

Đối với thư mục đã được chia sẻ vấn đề là cho phép những người sử dụng hoặc nhóm nào trên mạng được phép truy cập và quyền truy cập (Permission) của các user và group đó ở mức độ nào đối với thư mục đó.

- ở cấp độ Share có các quyền truy cập sau:

+ Full control: Nếu user hoặc group được trao quyền truy cập này thì có thể thực hiện tất cả mọi công việc trên các tập tin và folder trong Share đang xét.

+ Change: Nếu user hoặc group được trao quyền truy cập này có thể đọc và thi hành, cũng như thay đổi và xoá các tập tin và folder trong Share đang xét.

+ Read: Nếu user hoặc group được trao quyền truy cập này thì chỉ có thể đọc và thi hành các tập tin và folder trong Share đang xét.

- Các bước tiến hành thiết lập các quyền truy cập thư mục hoặc tập tin ở cấp độ Share được tiến hành như sau:

+ Kích chuột phải lên thư mục đó (Thư mục này đã được chia sẻ trước đó) trong cửa sổ Explorer của Windows 2000

+ Chọn Properties trên menu ngữ cảnh. Xuất hiện một cửa sổ Properties của thư mục đó, chọn Tab Sharing, trên Tab Sharing chọn nút Permissions, một hộp thoại hiện ra như hình dưới.

Trên hộp thoại này có hai phần. Phần Name để chỉ tên user hoặc tên group được gán quyền truy cập. Phần Permissions là danh sách các quyền được gán cho user hoặc group.

+ Nếu muốn cấp quyền truy cập cho user hoặc group nào kích vào nút Add và một cửa sổ hiện ra chọn tên user hoặc group sau đo nhấn Add và OK.

+ Nút Remove dùng để loại bỏ user hay group nào đó khỏi quyền truy cập thư mục hoặc tập tin.

3. Quyền truy cập ở cấp độ thư mục và tập tin.

Để thấy được các quyền ở cấp độ thư mục và tập tin thì đòi hỏi bảng phân khu (parttion) của đĩa phải là NTFS (New Techology File System). ở cấp độ này có các kiểu quyền truy cập sau:

- Các quyền truy cập mở rộng:

+ Travese Folder/execute File: Travese Folder (đi qua folder) chỉ áp dụng đối với folder. execute File cho phép thi hành các tập tin (.exe, .com, hoặc một kiểu tập tin khả thi khác).

+ List Folder/Read Data: List folder cho phép xem các tập tin và folder bên trong một folder. Read Data cho phép xem nội dung của một tập tin.

+ Read attributes: Cho phép nhìn thấy các thuộc tính cơ bản cơ bản của tập tin như: Read-Only, Hidden, System, Archive.

+ Read Extended Attributes: Cho phép xem các thuộc tính mở rộng của tập tin.

+ Create Files/Write Data: Cho phép đặt các tập tin mới bên trong folder đang xet (có thể sao chép, di dời từ folder khác tới). Write Data thì cho phép ghi đè lên dữ liệu hiện có bên trong một tập tin nhưng nó không cho phép đưa thêm dữ liệu vào một tập tin hiện có.

+ Create Folders/Append Data: Create cho phép tao ra các folder bên trong folder đang xét. Append Data cho phép đưa thêm dữ liệu vào cuối tập tin hiện có nhưng không thay đổi dữ liệu đã có lúc trước bên trong tập tin đó.

+ Write Attributes: Cho phép thay đổi các thuộc tính cơ bản của tập tin.

+ Write Extended Attibutes: Cho phép thay đổi các thuộc tính mở rộng của tập tin.

+ Delete Subfolders and Files: Cho phép xoá bỏ các folder con bà các tập tin, cho dù không có quyền truy cập Delete trên folder con hoặc tập tin đó.

+ Read Permissions: Cho phép xem tất cả các Permission NTFS có liên kết với một tập tin hoặc folder nhưng không thể thay đổi permission nào cả.

+ Change Permissions: Cho phép thay đổi các Permission được ấn định cho một file hoặc folder.

+ Take Ownership: Cho phép chiếm quyền sở hữu của một tập tin.

- Các quyền truy cập thư mục, tập tin chuẩn.

+ Read: Cho phép xem được nội dung, và các thuộc tính có liên kết với một đối tượng.

+ Write: Cho phép tạo một tập tin hoặc thư mục con bên trong thư mục đang xet. Nó có thể kêt hợp với quyền Read để thay đổi nội dung của tập tin.

+ Read and Execute: Cũng giống như Read, nhưng nó bao hàm thêm quyền Traverse Folder.

+ Modify: gồm các quyền như: Read, Execute, Write, Delete.

+ Full Control: bao gồm tất cả các quyền.

+ List Folder Contents: Giống như quyền Read and Execute nhưng chỉ áp dụng với thư mục.

**** Cách tiến hành phân bổ các quyền truy cập đối với tập tin và thư mục.***

+ Tìm đến tập tin hoặc thư mục cần phân bổ quyền truy cập, nhấp phải chuột vào nó, chọn Properties, rồi chọn Tab Security.

+ Khung Name bên trên cho thấy các nhóm hoặc người dùng khác nhau được phép truy cập Folder hay tập tin đang xét còn khung bên dưới cho thấy những quyền truy cập được phân cho người dùng hoặc nhóm được chọn ở khung trên.

+ Muốn loại bỏ một người dùng hoặc nhóm thì chỉ việc chọn tên nhóm hoặc tên người dùng trên khung Name và kích Remove.

+ Muốn thêm người dùng hoặc nhóm được phép truy cập thư mục hoặc tập tin thì nhắp nút Add, một hộp thoại hiện ra lựa chọn tên nhóm hoặc tên người dùng sau đó nhấn nút Add và OK để quay trở lại Tab Security.

+ Lúc này chọn tên nhóm hoặc người dùng trên hộp Name và lựa chọn các quyền tương ứng dưới hộp Permission sau đó kích Allow hoặc Deny.

+ Bây giờ có thể kích vào nút Advanced để thết lập các quyền truy cập mở rộng. Một cửa sổ hiện, ra chọn Tab Permissions như hình sau:

+ Tại cửa sổ này chọn tên người sử dụng hoặc nhóm trong ô Permission Entries, sau đó kích nut View/Edit để thiết lập các quyền truy cập (permissions) mở rộng. Lúc đó một cửa sổ hiện ra với danh sách các quyền mở rộng để lựa chọn.

+ Trong danh sách các quyền này cho phép ta chọn lựa các quyền và chọn Allow hoặc Deny với các quyền tương ứng và kích OK. và OK, OK để kết thúc công việc phân bổ quyển truy cập đối với tập tin và thư mục.

MỤC LỤC