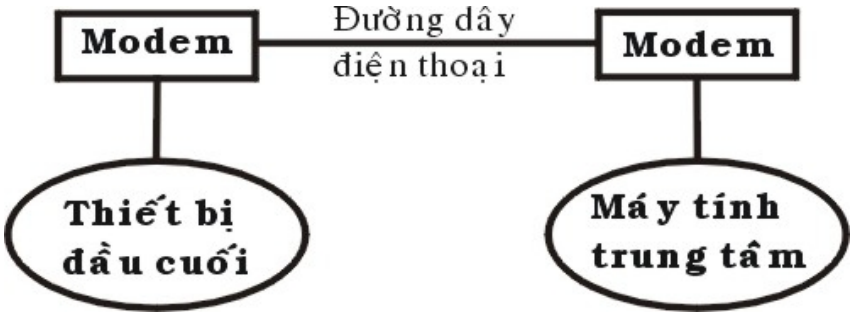
Chương 1

Sơ lược lịch sử phát triển của mạng máy tính

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

Cùng với sự phát triển của những ứng dụng trên máy tính các phương pháp nâng cao khả năng giao tiếp với máy tính trung tâm cũng đã được đầu tư nghiên cứu rất nhiều. Vào giữa những năm 60 một số nhà chế tạo máy tính đã nghiên cứu thành công những thiết bị truy cập từ xa tới máy tính của họ. Một trong những phương pháp thâm nhập từ xa được thực hiện bằng việc cài đặt một thiết bị đầu cuối ở một vị trí cách xa trung tâm tính toán, thiết bị đầu cuối này được liên kết với trung tâm bằng việc sử dụng đường dây điện thoại và với hai thiết bị xử lý tín hiệu (thường gọi là Modem) gắn ở hai đầu và tín hiệu được truyền thay vì trực tiếp thì thông qua dây điện thoại.



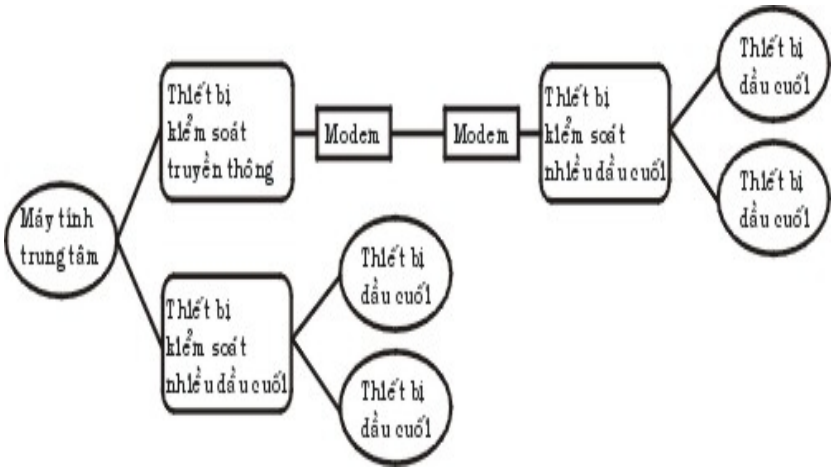
Hình 1.1. Mô hình truyền dữ liệu từ xa đầu tiên

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 hiên 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 sữ 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.

Chương 2

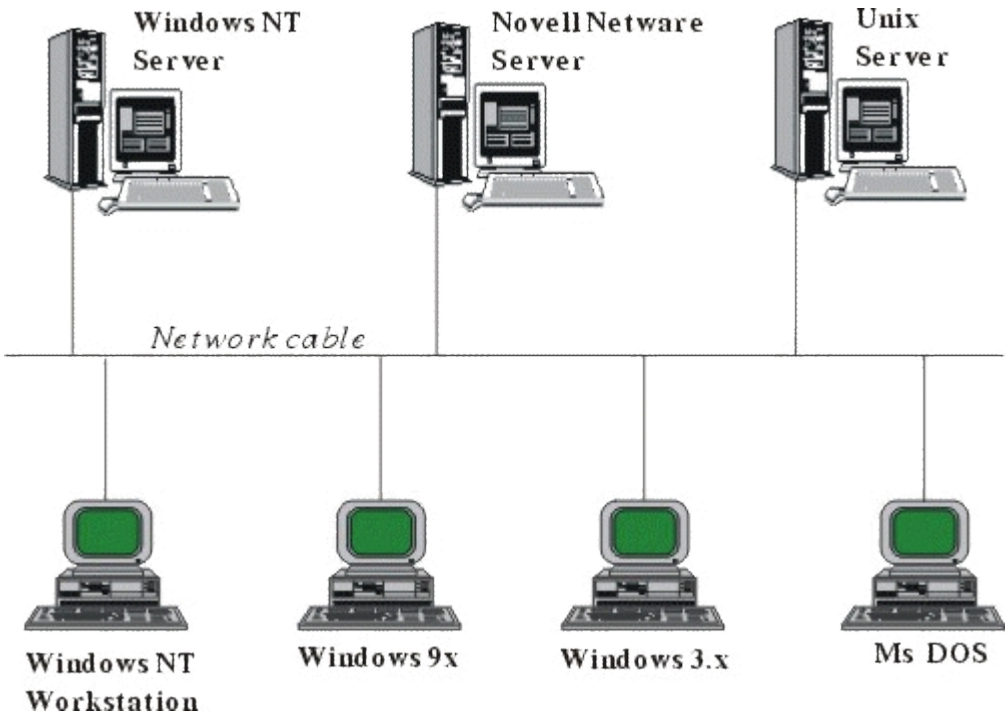
Những khái niệm cơ bản của mạng máy tính

Với sự phát triển của khoa học và kỹ thuật, hiện nay các mạng máy tính đã phát triển một cách nhanh chóng và đa dạng cả về quy mô, hệ điều hành và ứng dụng. Do vậy việc nghiên cứu chúng ngày càng trở nên phức tạp. Tuy nhiên các mạng máy tính cũng có cùng các điểm chung thông qua đó chúng ta có thể đánh giá và phân loại chúng.

I. Định nghĩa mạng máy tính

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

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



Hình 2.1: Một mô hình liên kết các máy tính trong mạng

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

Đặc trưng cơ bản của đường truyền vật lý là giải thông. Giải thông của một đường chuyền chính là độ đo phạm vi tần số mà nó có thể đáp ứng được. Tốc độ truyền dữ liệu trên đường truyền còn được gọi là thông lượng của đường truyền - thường được tính bằng số

lượng bit được truyền đi trong một giây (Bps). Thông lượng còn được đo bằng đơn vị khác là Baud (lấy từ tên nhà bác học - Emile Baudot). Baud biểu thị số lượng thay đổi tín hiệu trong một giây.

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

II. Phân loại mạng máy tính

Do hiện nay mạng máy tính được phát triển khắp nơi với những ứng dụng ngày càng đa dạng cho nên việc phân loại mạng máy tính là một việc rất phức tạp. Người ta có thể chia các mạng máy tính theo khoảng cách địa lý ra làm hai loại: Mạng diện rộng và Mạng cục bộ.

Mạng cục bộ (Local Area Networks - LAN) là mạng được thiết lập để liên kết các máy tính trong một khu vực như trong một toà nhà, một khu nhà.

Mạng diện rộng (Wide Area Networks - WAN) là mạng được thiết lập để liên kết các máy tính của hai hay nhiều khu vực khác nhau như giữa các thành phố hay các tỉnh.

Sự phân biệt trên chỉ có tính chất ước lệ, các phân biệt trên càng trở nên khó xác định với việc phát triển của khoa học và kỹ thuật cũng như các phương tiện truyền dẫn. Tuy nhiên với sự phân biệt trên phương diện địa lý đã đưa tới việc phân biệt trong nhiều đặc tính khác nhau của hai loại mạng trên, việc nghiên cứu các phân biệt đó cho ta hiểu rõ hơn về các loại mạng.

III. Sự phân biệt giữa mạng cục bộ và mạng diện rộng

Mạng cục bộ và mạng diện rộng có thể được phân biệt bởi: địa phương hoạt động, tốc độ đường truyền và tỷ lệ lỗi trên đường truyền, chủ quản của mạng, đường đi của thông tin trên mạng, dạng chuyển giao thông tin.

Địa phương hoạt động: Liên quan đến khu vực địa lý thì mạng cục bộ sẽ là mạng liên kết các máy tính nằm ở trong một khu vực nhỏ. Khu vực có thể bao gồm một tòa nhà hay là một khu nhà... Điều đó hạn chế bởi khoảng cách đường dây cáp được dùng để liên kết các máy tính của mạng cục bộ (Hạn chế đó còn là hạn chế của khả năng kỹ thuật của đường truyền dữ liệu). Ngược lại mạng diện rộng là mạng có khả năng liên kết các máy tính trong một vùng rộng lớn như là một thành phố, một miền, một đất nước, mạng diện rộng được xây dựng để nối hai hoặc nhiều khu vực địa lý riêng biệt.

Tốc độ đường truyền và tỷ lệ lỗi trên đường truyền: Do các đường cáp của mạng cục bộ đươc xây dựng trong một khu vực nhỏ cho nên nó ít bị ảnh hưởng bởi tác động của thiên nhiên

(như là sấm chớp, ánh sáng...). Điều đó cho phép mạng cục bộ có thể truyền dữ liệu với tốc độ cao mà chỉ chịu một tỷ lệ lỗi nhỏ. Ngược lại với mạng diện rộng do phải truyền ở những khoảng cách khá xa với những đường truyền dẫn dài có khi lên tới hàng ngàn km. Do vậy mạng diện rộng không thể truyền với tốc độ quá cao vì khi đó tỉ lệ lỗi sẽ trở nên khó chấp nhận được.

Mạng cục bộ thường có tốc độ truyền dữ liệu từ 4 đến 16 Mbps và đạt tới 100 Mbps nếu dùng cáp quang. Còn phần lớn các mạng diện rộng cung cấp đường truyền có tốc độ thấp hơn nhiều như T1 với 1.544 Mbps hay E1 với 2.048 Mbps.

(Ở đây bps (Bit Per Second) là một đơn vị trong truyền thông tương đương với 1 bit được truyền trong một giây, ví dụ như tốc độ đường truyền là 1 Mbps tức là có thể truyền tối đa 1 Megabit trong 1 giây trên đường truyền đó).

Thông thường trong mạng cục bộ tỷ lệ lỗi trong truyền dữ liệu vào khoảng $1/10^7$-10^8 còn trong mạng diện rộng thì tỷ lệ đó vào khoảng $1/10^6$ - 10^7

Chủ quản và điều hành của mạng: Do sự phức tạp trong việc xây dựng, quản lý, duy trì các đường truyền dẫn nên khi xây dựng mạng diện rộng người ta thường sử dụng các đường truyền được thuê từ các công ty viễn thông hay các nhà cung cấp dịch vụ truyền số liệu. Tùy theo cấu trúc của mạng những đường truyền đó thuộc cơ quan quản lý khác nhau như các nhà cung cấp đường truyền nội hạt, liên tỉnh, liên quốc gia. Các đường truyền đó phải tuân thủ các quy định của chính phủ các khu vực có đường dây đi qua như: tốc độ, việc mã hóa.

Còn đối với mạng cục bộ thì công việc đơn giản hơn nhiều, khi một cơ quan cài đặt mạng cục bộ thì toàn bộ mạng sẽ thuộc quyền quản lý của cơ quan đó.

Đường đi của thông tin trên mạng: Trong mạng cục bộ thông tin được đi theo con đường xác định bởi cấu trúc của mạng. Khi người ta xác định cấu trúc của mạng thì thông tin sẽ luôn luôn đi theo cấu trúc đã xác định đó. Còn với mạng diện rộng dữ liệu cấu trúc có thể phức tạp hơn nhiều do việc sử dụng các dịch vụ truyền dữ liệu. Trong quá trình hoạt động các điểm nút có thể thay đổi đường đi của các thông tin khi phát hiện ra có trục trặc trên đường truyền hay khi phát hiện có quá nhiều thông tin cần truyền giữa hai điểm nút nào đó. Trên mạng diện rộng thông tin có thể có các con đường đi khác nhau, điều đó cho phép có thể sử dụng tối đa các năng lực của đường truyền hay nâng cao điều kiện an toàn trong truyền dữ liệu.

Dạng chuyển giao thông tin: Phần lớn các mạng diện rộng hiện nay được phát triển cho việc truyền đồng thời trên đường truyền nhiều dạng thông tin khác nhau như: video, tiếng nói, dữ liệu... Trong khi đó các mạng cục bộ chủ yếu phát triển trong việc truyền dữ liệu thông thường. Điều này có thể giải thích do việc truyền các dạng thông tin như video, tiếng nói trong một khu vực nhỏ ít được quan tâm hơn như khi truyền qua những khoảng cách lớn.

Các hệ thống mạng hiện nay ngày càng phức tạp về chất lượng, đa dạng về chủng loại và phát triển rất nhanh về chất. Trong sự phát triển đó số lượng những nhà sản xuất từ phần mềm, phần cứng máy tính, các sản phẩm viễn thông cũng tăng nhanh với nhiều sản phẩm đa dạng. Chính vì vậy vai trò chuẩn hóa cũng mang những ý nghĩa quan trọng. Tại các nước các cơ quan chuẩn quốc gia đã đưa ra các những chuẩn về phần cứng và các quy định về giao tiếp nhằm giúp cho các nhà sản xuất có thể làm ra các sản phẩm có thể kết nối với các sản phẩm do hãng khác sản xuất.

Chương 3
Mô hình truyền thông

I. Sự cần thiết phải có mô hình truyền thông

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

Mỗi máy tính cần phải có một địa chỉ phân biệt trên mạng.

Việc chuyển dữ liệu từ máy tính này đến máy tính khác do mạng thực hiện thông qua những quy định thống nhất gọi là giao thức của mạng.

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

Máy tính cần truyền cần biết địa chỉ của máy nhận.

Máy tính cần truyền phải xác định được máy tính nhận đã sẵn sàng nhận thông tin

Chương trình gửi file trên máy truyền cần xác định được rằng chương trình nhận file trên máy nhận đã sẵn sàng tiếp nhận file.

Nếu cấu trúc file trên hai máy không giống nhau thì một máy phải làm nhiệm vụ chuyển đổi file từ dạng này sang dạng kia.

Khi truyền file máy tính truyền cần thông báo cho mạng biết địa chỉ của máy nhận để các thông tin được mạng đưa tới đích.

Điều trên đó cho thấy giữa hai máy tính đã có một sự phối hợp hoạt động ở mức độ cao. Bây giờ thay vì chúng ta xét cả quá trình trên như là một quá trình chung thì chúng ta sẽ chia quá trình trên ra thành một số công đoạn và mỗi công đoạn con hoạt động một cách độc lập với nhau. Ở đây chương trình truyền nhận file của mỗi máy tính được chia thành ba module là: Module truyền và nhận File, Module truyền thông và Module tiếp cận mạng. Hai module tương ứng sẽ thực hiện việc trao đổi với nhau trong đó:

Module truyền và nhận file cần được thực hiện tất cả các nhiệm vụ trong các ứng dụng truyền nhận file. Ví dụ: truyền nhận thông số về file, truyền nhận các mẫu tin của file, thực hiện chuyển đổi file sang các dạng khác nhau nếu cần. Module truyền và nhận file không cần thiết phải trực tiếp quan tâm tới việc truyền dữ liệu trên mạng như thế nào mà nhiệm vụ đó được giao cho Module truyền thông.

Module truyền thông quan tâm tới việc các máy tính đang hoạt động và saün sàng trao đổi thông tin với nhau. Nó còn kiểm soát các dữ liệu sao cho những dữ liệu này có thể trao đổi một cách chính xác và an toàn giữa hai máy tính. Điều đó có nghĩa là phải truyền file trên nguyên tắc đảm bảo an toàn cho dữ liệu, tuy nhiên ở đây có thể có một vài mức độ an toàn khác nhau được dành cho từng ứng dụng. Ở đây việc trao đổi dữ liệu giữa hai máy tính không phụ thuộc vào bản chất của mạng đang liên kết chúng. Những yêu cầu liên quan đến mạng đã được thực hiện ở module thứ ba là module tiếp cận mạng và nếu mạng thay đổi thì chỉ có module tiếp cận mạng bị ảnh hưởng.

Module tiếp cận mạng được xây dựng liên quan đến các quy cách giao tiếp với mạng và phụ thuộc vào bản chất của mạng. Nó đảm bảo việc truyền dữ liệu từ máy tính này đến máy tính khác trong mạng.

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

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

Nguyên tắc của phương pháp phân tầng là:

Mỗi hệ thống thành phần trong mạng được xây dựng như một cấu trúc nhiều tầng và đều có cấu trúc giống nhau như: số lượng tầng và chức năng của mỗi tầng.

Các tầng nằm chồng lên nhau, dữ liệu được chỉ trao đổi trực tiếp giữa hai tầng kề nhau từ tầng trên xuống tầng dưới và ngược lại.

Cùng với việc xác định chức năng của mỗi tầng chúng ta phải xác định mối quan hệ giữa hai tầng kề nhau. Dữ liệu được truyền đi từ tầng cao nhất của hệ thống truyền lần lượt đến tầng thấp nhất sau đó truyền qua đường nối vật lý dưới dạng các bit tới tầng thấp nhất của hệ thống nhận, sau đó dữ liệu được truyền ngược lên lần lượt đến tầng cao nhất của hệ thống nhận.

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

Hình 3.1: Mô hình phân tầng gồm N tầng

II. Mô hình truyền thông đơn giản 3 tầng

Nói chung trong truyền thông có sự tham gia của các thành phần: các chương trình ứng dụng, các chương trình truyền thông, các máy tính và các mạng. Các chương trình ứng dụng là các chương trình của người sử dụng được thực hiện trên máy tính và có thể tham gia vào quá trình trao đổi thông tin giữa hai máy tính. Trên một máy tính với hệ điều hành đa nhiệm (như

Windows, UNIX) thường được thực hiện đồng thời nhiều ứng dụng trong đó có những ứng dụng liên quan đến mạng và các ứng dụng khác. Các máy tính được nối với mạng và các dữ liệu được trao đổi thông qua mạng từ máy tính này đến máy tính khác.

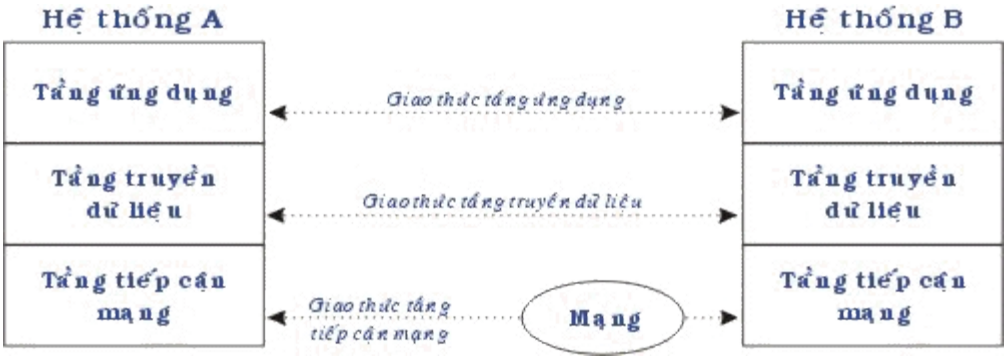
Việc gửi dữ liệu được thực hiện giữa một ứng dụng với một ứng dụng khác trên hai máy tính khác nhau thông qua mạng được thực hiện như sau: Ứng dụng gửi chuyển dữ liệu cho chương trình truyền thông trên máy tính của nó, chương trình truyền thông sẽ gửi chúng tới máy tính nhận. Chương trình truyền thông trên máy nhận sẽ tiếp nhận dữ liệu, kiểm tra nó trước khi chuyển giao cho ứng dụng đang chờ dữ liệu.

Với mô hình truyền thông đơn giản người ta chia chương trình truyền thông thành ba tầng không phụ thuộc vào nhau là: tầng ứng dụng, tầng chuyển vận và tầng tiếp cận mạng.

Tầng tiếp cận mạng liên quan tới việc trao đổi dữ liệu giữa máy tính và mạng mà nó được nối vào. Để dữ liệu đến được đích máy tính gửi cần phải chuyển địa chỉ của máy tính nhận cho mạng và qua đó mạng sẽ chuyển các thông tin tới đích. Ngoài ra máy gửi có thể sử dụng một số phục vụ khác nhau mà mạng cung cấp như gửi ưu tiên, tốc độ cao. Trong tầng này có thể có nhiều phần mềm khác nhau được sử dụng phụ thuộc vào các loại của mạng ví dụ như mạng chuyển mạch, mạng chuyển mạch gói, mạng cục bộ.

Tầng truyền dữ liệu thực hiện quá trình truyền thông không liên quan tới mạng và nằm ở trên tầng tiếp cận mạng. Tầng truyền dữ liệu không quan tâm tới bản chất các ứng dụng đang trao đổi dữ liệu mà quan tâm tới làm sao cho các dữ liệu được trao đổi một cách an toàn. Tầng truyền dữ liệu đảm bảo các dữ liệu đến được đích và đến theo đúng thứ tự mà chúng được xử lý. Trong tầng truyền dữ liệu người ta phải có những cơ chế nhằm đảm bảo sự chính xác đó và rõ ràng các cơ chế này không phụ thuộc vào bản chất của từng ứng dụng và chúng sẽ phục vụ cho tất cả các ứng dụng.

Tầng ứng dụng sẽ chứa các module phục vụ cho tất cả những ứng dụng của người sử dụng. Với các loại ứng dụng khác nhau (như là truyền file, truyền thư mục) cần các module khác nhau.



Hình 3.2 Mô hình truyền thông 3 tầng

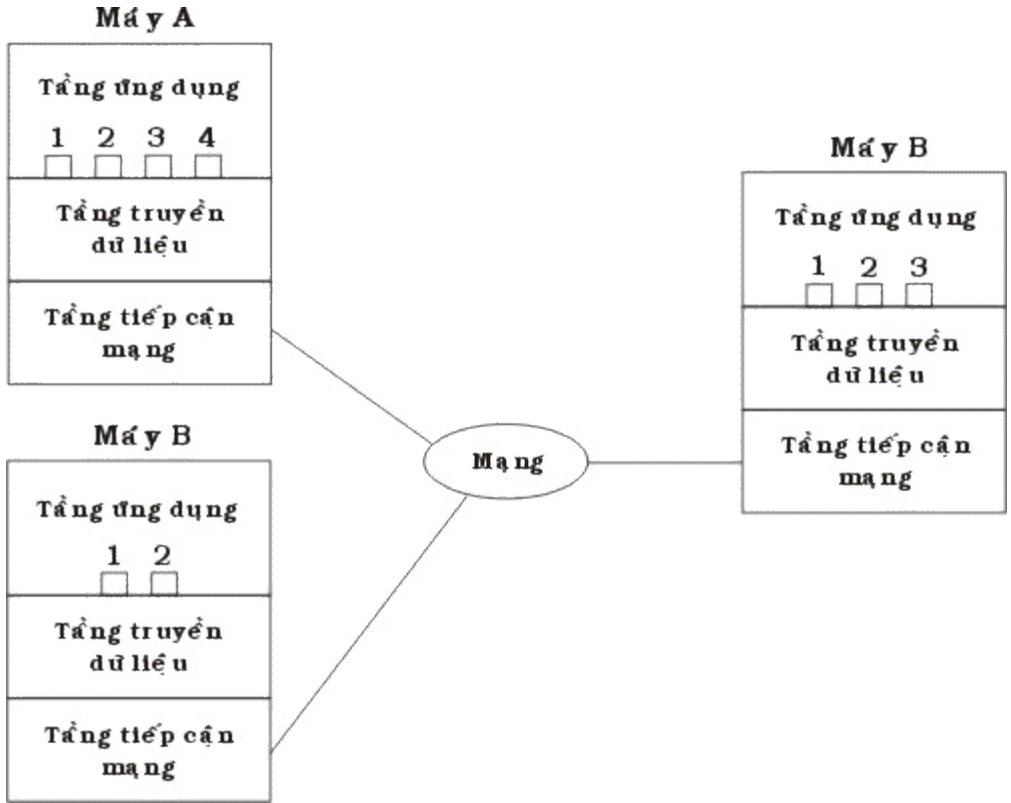
Trong một mạng với nhiều máy tính, mỗi máy tính một hay nhiều ứng dụng thực hiện đồng thời (Tại đây ta xét trên một máy tính trong một thời điểm có thể chạy nhiều ứng dụng và các ứng dụng đó có thể thực hiện đồng thời việc truyền dữ liệu qua mạng). Một ứng dụng khi cần truyền dữ liệu qua mạng cho một ứng dụng khác cần phải gọi 1 module tầng ứng dụng của chương trình truyền thông trên máy của mình, đồng thời ứng dụng kia cũng sẽ gọi 1 module tầng ứng dụng trên máy của nó. Hai module ứng dụng sẽ liên kết với nhau nhằm thực hiện các yêu cầu của các chương trình ứng dụng.

Các ứng dụng đó sẽ trao đổi với nhau thông qua mạng, tuy nhiên trong 1 thời điểm trên một máy có thể có nhiều ứng dụng cùng hoạt động và để việc truyền thông được chính xác thì các ứng dụng trên một máy cần phải có một địa chỉ riêng biệt. Rõ ràng cần có hai lớp địa chỉ:

Mỗi máy tính trên mạng cần có một địa chỉ mạng của mình, hai máy tính trong cùng một mạng không thể có cùng địa chỉ, điều đó cho phép mạng có thể truyền thông tin đến từng máy tính một cách chính xác.

Mỗi một ứng dụng trên một máy tính cần phải có địa chỉ phân biệt trong máy tính đo. Nó cho phép tầng truyền dữ liệu giao dữ liệu cho đúng ứng dụng đang cần. Địa chỉ đó được gọi là điểm tiếp cận giao dịch. Điều đó cho thấy mỗi một ứng dụng sẽ tiếp cận các phục vụ của tầng truyền dữ liệu một cách độc lập.

Các module cùng một tầng trên hai máy tính khác nhau sẽ trao đổi với nhau một cách chặt chẽ theo các qui tắc xác định trước được gọi là giao thức. Một giao thức được thể hiện một cách chi tiết bởi các chức năng cần phải thực hiện như các giá trị kiểm tra lỗi, việc định



dạng các dữ liệu, các quy trình cần phải thực hiện để trao đổi thông tin.

Hình 3.3 Ví dụ mô hình truyền thông đơn giản

Chúng ta hãy xét trong ví dụ (như hình vẽ trên): giả sử có ứng dụng có điểm tiếp cận giao dịch 1 trên máy tính A muốn gửi thông tin cho một ứng dụng khác trên máy tính B có điểm tiếp cận giao dịch 2. Ứng dụng trên máy tính A chuyển các thông tin xuống tầng truyền dữ liệu của A với yêu cầu gửi chúng cho điểm tiếp cận giao dịch 2 trên máy tính B. Tầng truyền dữ liệu máy A sẽ chuyển các thông tin xuống tầng tiếp cận mạng máy A với yêu cầu chuyển chúng cho máy tính B (Chú ý rằng mạng không cần biết địa chỉ của điểm tiếp cận giao dịch mà chỉ cần biết địa chỉ của máy tính B). Để thực hiện quá trình này, các thông tin kiểm soát cũng sẽ được truyền cùng với dữ liệu.

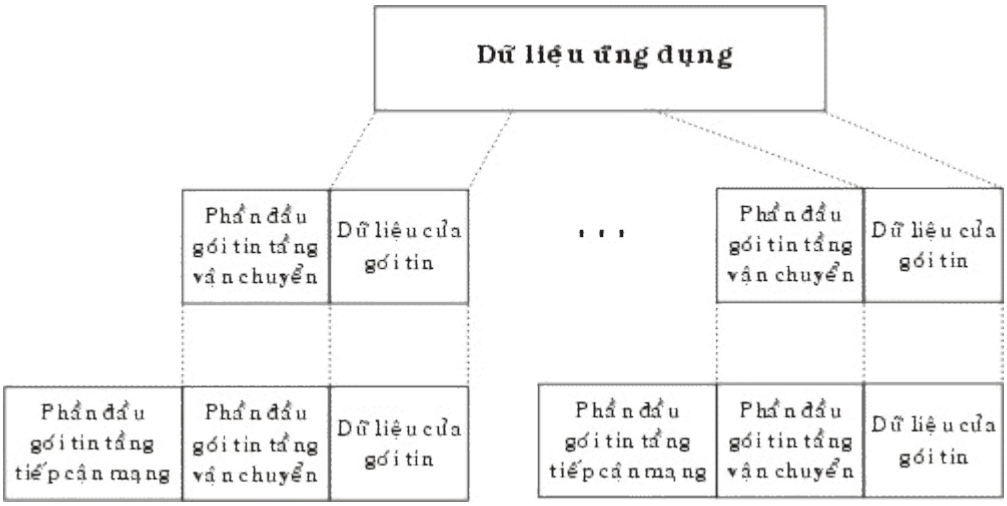
Đầu tiên khi ứng dụng 1 trên máy A cần gửi một khối dữ liệu nó chuyển khối đó cho tầng vận chuyển. Tầng vận chuyển có thể chia khối đó ra thành nhiều khối nhỏ phụ thuộc vào yêu cầu của giao thức của tầng và đóng gói chúng thành các gói tin (packet). Mỗi một gói tin sẽ được bổ sung thêm các thông tin kiểm soát của giao thức và được gọi là phần đầu (Header) của gói tin. Thông thường phần đầu của gói tin cần có:

Địa chỉ của điểm tiếp cận giao dịch nơi đến (Ở đây là 3): khi tầng vận chuyển của máy B nhận được gói tin thì nó biết được ứng dụng nào mà nó cần giao.

Số thứ tự của gói tin, khi tầng vận chuyển chia một khối dữ liệu ra thành nhiều gói tin thì nó cần phải đánh số thứ tự các gói tin đó. Nếu chúng đi đến đích nếu sai thứ tự thì tầng vận chuyển của máy nhận có thể phát hiện và chỉnh lại thứ tự. Ngoài ra nếu có lỗi trên đường truyền thì tầng vận chuyển của máy nhận sẽ phát hiện ra và yêu cầu gửi lại một cách chính xác.

Mã sửa lỗi: để đảm bảo các dữ liệu được nhận một cách chính xác thì trên cơ sở các dữ liệu của gói tin tầng vận chuyển sẽ tính ra một giá trị theo một công thức có sẵn và gửi nó đi trong phần đầu của gói tin. Tầng vận chuyển nơi nhận thông qua giá trị đó xác định được gói tin đó có bị lỗi trên đường truyền hay không.

Bước tiếp theo tầng vận chuyển máy A sẽ chuyển từng gói tin và địa chỉ của máy tính đích (ở đây là B) xuống tầng tiếp cận mạng với yêu cầu chuyển chúng đi. Để thực hiện được yêu cầu này tầng tiếp cận mạng cũng tạo các gói tin của mình trước khi truyền qua mạng. Tại đây giao thức của tầng tiếp cận mạng sẽ thêm các thông tin điều khiển vào phần đầu của gói tin mạng.



Hình 3.4: Mô hình thiết lập gói tin

Trong phần đầu gói tin mạng sẽ bao gồm địa chỉ của máy tính nhận, dựa trên địa chỉ này mạng truyền gói tin tới đích. Ngoài ra có thể có những thông số như là mức độ ưu tiên.

Như vậy thông qua mô hình truyền thông đơn giản chúng ta cũng có thể thấy được phương thức hoạt động của các máy tính trên mạng, có thể xây dựng và thay đổi các giao thức trong cùng một tầng.

III. Các nhu cầu về chuẩn hóa đối với mạng

Trong phần trên chúng ta đã xem xét một mô hình truyền thông đơn giản, trong thực tế việc phân chia các tầng như trong mô hình trên thực sự chưa đủ. Trên thế giới hiện có một số cơ quan định chuẩn, họ đưa ra hàng loạt chuẩn về mạng tuy các chuẩn đó có tính chất khuyến nghị chứ không bắt buộc nhưng chúng rất được các cơ quan chuẩn quốc gia coi trọng.

Hai trong số các cơ quan chuẩn quốc tế là:

ISO (The International Standards Organization) - Là tổ chức tiêu chuẩn quốc tế hoạt động dưới sự bảo trợ của Liên hợp Quốc với thành viên là các cơ quan chuẩn quốc gia với số lượng khoảng hơn 100 thành viên với mục đích hỗ trợ sự phát triển các chuẩn trên phạm vi toàn thế giới. Một trong những thành tựu của ISO trong lãnh vực truyền thông là mô hình hệ thống mở (Open Systems Interconnection - gọi tắt là OSI).

CCITT (Commité Consultatif International pour le Telegraphe et la Téléphone) - Tổ chức tư vấn quốc tế về điện tín và điện thoại làm việc dưới sự bảo trợ của Liên Hiệp Quốc có trụ sở chính tại Geneva - Thụy sỹ. Các thành viên chủ yếu là các cơ quan bưu chính viễn thông các quốc gia. Tổ chức này có vai trò phát triển các khuyến nghị trong các lãnh vực viễn thông.

IV. Một số mô hình chuẩn hóa

1. Mô hình OSI (Open Systems Interconnection)

Mô hình OSI là một cơ sở dành cho việc chuẩn hoá các hệ thống truyền thông, nó được nghiên cứu và xây dựng bởi ISO. Việc nghiên cứu về mô hình OSI được bắt đầu tại ISO vào năm 1971 với mục tiêu nhằm tới việc nối kết các sản phẩm của các hãng sản xuất khác nhau và phối hợp các hoạt động chuẩn hoá trong các lĩnh vực viễn thông và hệ thống thông tin. Theo mô hình OSI chương trình truyền thông được chia ra thành 7 tầng với những chức năng phân biệt cho từng tầng. Hai tầng đồng mức khi liên kết với nhau phải sử dụng một giao thức chung. Trong mô hình OSI có hai loại giao thức chính được áp dụng: giao thức có liên kết (connection - oriented) và giao thức không liên kết (connectionless)

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

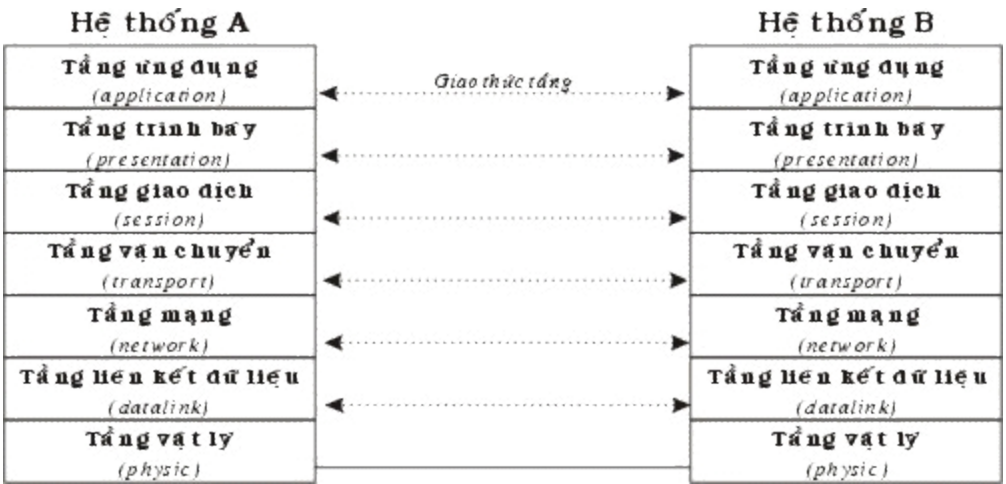
Nhiệm vụ của các tầng trong mô hình OSI:

Tầng ứng dụng (Application layer): tầng ứng dụng quy định giao diện giữa người sử dụng và môi trường OSI, nó cung cấp các phương tiện cho người sử dụng truy cập vả sử dụng các dịch vụ củ mô hình OSI.

Tầng trình bày (Presentation layer): tầng trình bày chuyển đổi các thông tin từ cú pháp người sử dụng sang cú pháp để truyền dữ liệu, ngoài ra nó có thể nén dữ liệu truyền và mã hóa chúng trước khi truyền đễ bảo mật.

Tầng giao dịch (Session layer): tầng giao dịch quy định một giao diện ứng dụng cho tầng vận chuyển sử dụng. Nó xác lập ánh xa giữa các tên đặt địa chỉ, tạo ra các tiếp xúc ban đầu giữa các máy tính khác nhau trên cơ sở các giao dịch truyền thông. Nó đặt tên nhất quán cho mọi thành phần muốn đối thoại riêng với nhau.

Tầng vận chuyển (Transport layer): tầng vận chuyển xác định địa chỉ trên mạng, cách thức chuyển giao gói tin trên cơ sở trực tiếp giữa hai đầu mút (end-to-end). Để bảo đảm được



việc truyền ổn định trên mạng tầng vận chuyển thường đánh số các gói tin và đảm bảo chúng chuyển theo thứ tự.

Hình 3.5: Mô hình 7 tầng OSI

Tầng mạng (Network layer): tầng mạng có nhiệm vụ xác định việc chuyển hướng, vạch đường các gói tin trong mạng, các gói tin này có thể phải đi qua nhiều chặng trước khi đến được đích cuối cùng.

Tầng liên kết dữ liệu (Data link layer): tầng liên kết dữ liệu có nhiệm vụ xác định cơ chế truy nhập thông tin trên mạng, các dạng thức chung trong các gói tin, đóng các gói tin...

Tầng vật lý (Phisical layer): tầng vật lý cung cấp phương thức truy cập vào đường truyền vật lý để truyền các dòng Bit không cấu trúc, ngoài ra nó cung cấp các chuẩn về điện, dây cáp, đầu nối, kỹ thuật nối mạch điện, điện áp, tốc độ cáp truyền dẫn, giao diện nối kết và các mức nối kết..

2. Mô hình SNA (Systems Netword Architecture)

Tháng 9/1973, Hãng IBM giới thiệu một kiến trúc mạng máy tính SNA (System Network Architecture). Đến năm 1977 đã có 300 trạm SNA được cài đặt. Cuối năm 1978, số lượng đã tăng lên đến 1250, rồi cứ theo đà đó cho đến nayđã có 20.000 trạm SNA đang được hoạt động. Qua con số này chúng ta có thể hình dung được mức độ quan trọng và tầm ảnh hưởng của SNA trên toàn thế giới.

Cần lưu ý rằng SNA không là một chuẩn quốc tế chính thức như OSI nhưng do vai trò to lớn của hãng IBM trên thị trường CNTT nên SNA trở thành một loại chuẩn thực tế và khá phổ biến. SNA là một đặc tả gồm rất nhiều tài liệu mô tả kiến trúc của mạng xử lý dữ liệu phân tán. Nó định nghĩa các quy tắc và các giao thức cho sự tương tác giữa các thành phần (máy tính, trạm cuối, phần mềm) trong mạng.

SNA được tổ chức xung quanh khái niệm miền (domain). Một SNA domain là một điểm điều khiển các dịch vụ hệ thống (Systems Services control point - SSCP) và nó sẽ điều khiển tất cả các tài nguyên đó, Các tài nguyên ở đây có thể là các đơn vị vật lý, các đơn vị logic, các liên kết dữ liệu và các thiết bị. Có thể ví SSCP như là "trái tim và khối óc" của SNA. Nó điều khiển SNA domain bằng cách gói các lệnh tới một đơn vị vật lý, đơn vị vật lý này sau khi nhận được lệnh sẽ quản lý tất cả các tài nguyên trực tiếp với nó. đơn vị vật lý thực sự là một "đối tác" của SSCP và chứa một tập con các khả năng của SSCP. Các Đơn vị vật lý đảm nhiệm việc quản lý của mỗi nút SNA.

SNA phân biệt giữa các nút miền con (Subarea node) và các nút ngoại vi (peripheral node).

Một nút miền con có thể dẫn đường cho dữ liệu của người sử dụng qua toàn bộ mạng. Nó dùng địa chỉ mạng và một số hiệu đường (router suember) để xác định đường truyền đi tới nút kế tiếp trong mạng.

Một nút ngoại vi có tính cục bộ hơn. Nó không dẫn đường giữa các nút miền con. Các nút được nối và điều khiển theo giao thức SDLC (Synchronous Data Link Control). Mỗi nút ngoại vi chỉ liên lạc được với nút miền con mà nó nối vào.

Mạng SNA dựa trên cơ chế phân tầng, trước đây thì 2 hệ thống ngang hàng không được trao đổi trực tiếp. Sau này phát triển thành SNA mở rộng: Lúc này hai tầng ngang hàng nhau có thể trao đổi trực tiếp. Với 6 tầng có tên gọi và chức năng tất như sau:

Tầng quản trị chức năng SNA (SNA Function Manegement) Tầng này thật ra có thể chia tầng này làm hai tầng như sau:

Tầng dịch vụ giao tác (Transaction) cung cấp các dịch vụ ứng dụng đến người dùng một mạng SNA. Những dịch vụ đó như : DIA cung cấp các tài liệu phân bố giữa các hệ thống văn phòng, SNA DS (văn phòng dịch vụ phân phối) cho việc truyền thông bất đồng bộ giữa các ứng dụng phân tán và hệ thống văn phòng. Tầng dịch vụ giao tác cũng cung cấp các dịch vụ và cấu hình, các dịch vụ quản lý để điều khiển các hoạt động mạng.

Tầng dịch vụ trình diễn (Presentation Services): tầng này thì liên quan với sự hiển thị các ứng dụng, người sử dụng đầu cuối và các dữ liệu hệ thống. Tầng này cũng định nghĩa các giao thức cho việc truyền thông giữa các chương trình và điều khiển truyền thông ở mức hội thoại.

Tầng kiểm soát luồng dữ liệu (Data flow control) tầng này cung cấp các dịch vụ điều khiểnluồng lưu thông cho các phiên từ logic này đến đơn vị logic khác (LU - LU). Nó thực hiện điều này bằng cách gán các số trình tự, các yêu cầu và đáp ứng, thực hiện các giao thức yêu cầu về đáp ứng giao dịch và hợp tác giữa các giao dịch gởi và nhận. Nói chung nó yểm trợ phương thức khai thác hai chiều đồng thời (Full duplex).

Tầng kiểm soát truyền (Transmission control): Tầng này cung cấp các điều khiển cơ bản của các phần tài nguyên truyền trong mạng, bằng cách xác định số trình tự nhận được, và quản lý việc theo dõi mức phiên. Tầng này cũng hỗ trợ cho việc mã hóa dữ liệu và cung cấp hệ thống hỗ trợ cho các nút ngoại vi.

Tầng kiểm soát đường dẫn (Path control): Tầng này cung cấp các giao thức để tìm đường cho một gói tin qua mạng SNA và để kết nối với các mạng SNA khác, đồng thời nó cũng kiểm soát các đường truyền này.

Tầng kiểm soát liên kết dữ liệu (Data Link Control): Tầng này cung cấp các giao thức cho việc truyền các gói tin thông qua đường truyền vật lý giữa hai node và cũng cung cấp các điều khiển lưu thông và phục hồi lỗi, các hỗ trợ cho tầng này là các giao thức SDLC, System/370, X25, IEEE 802.2 và 802.5.

Tầng kiểm soát vật lý (Physical control): Tầng này cung cấp một giao diện vật lý cho bất cứ môi trường truyền thông nào mà gắn với nó. Tầng nào định nghĩa các đặc trưng của tín hiệu cần để thiết lập, duy trì và kết thúc các đường nối vật lý cho việc hỗ trợ kết nối.

<table>
<tr><th>SNA</th><th>OSI</th></tr>
<tr><td rowspan="2">Tầng quản trị chức năng SNA
(SNA Function Management)
(Transaction)
(Presentation Services)</td><td>Tầng ứng dụng
(application)</td></tr>
<tr><td>Tầng trình bày
(presentation)</td></tr>
<tr><td>Tầng kiểm soát luồng dữ liệu
(Data flow control)</td><td>Tầng giao dịch
(session)</td></tr>
<tr><td>Tầng kiểm soát truyền
(Transmission control)</td><td>Tầng vận chuyển
(transport)</td></tr>
<tr><td>Tầng kiểm soát đường dẫn
(Path control)</td><td>Tầng mạng
(network)</td></tr>
<tr><td>Tầng kiểm soát liên kết dữ liệu
(Data Link Control)</td><td>Tầng liên kết dữ liệu
(datalink)</td></tr>
<tr><td>Tầng kiểm soát vật lý
(Physical control)</td><td>Tầng vật lý
(physic)</td></tr>
</table>

Hình 3.6: Tương ứng các tầng các kiến trúc SNI và OSI

Chương 4
Mô hình kết nối các hệ thống mở
Open Systems Interconection

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.

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

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

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

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

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

II. Các giao thức trong mô hình OSI

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

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

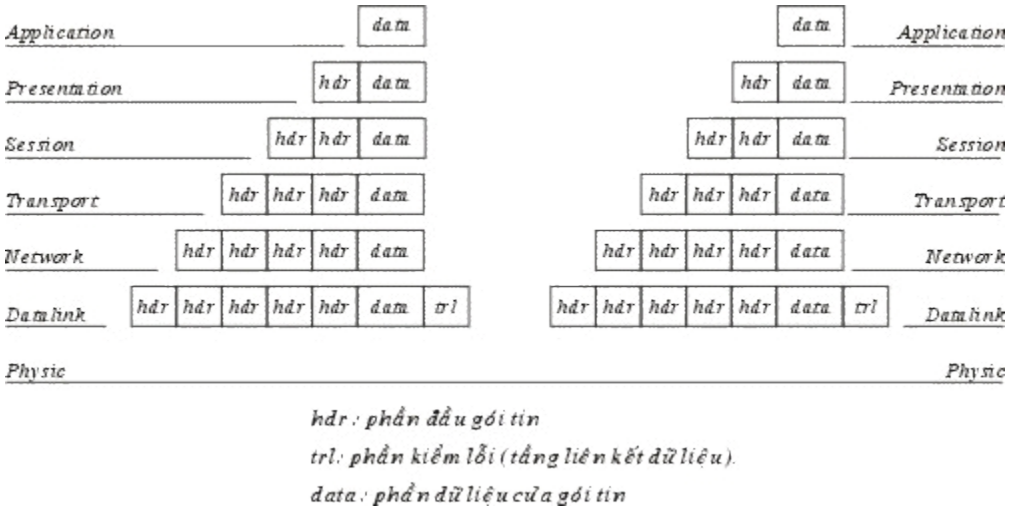
Thiết lập liên kết (logic): hai thực thể đồng mức ở hai hệ thống thương lượng với nhau về tập các tham số sẽ sử dụng trong giai đoạn sau (truyền dữ liệu).

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.



hdr : phần đầu gói tin
trl: phần kiểm lỗi (tầng liên kết dữ liệu).
data : phần dữ liệu của gói tin

Hình 4.1: Phương thức xác lập các gói tin trong mô hình OSI

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

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

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

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

Tầng 1: Vật lý (Physical)

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

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

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

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

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

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

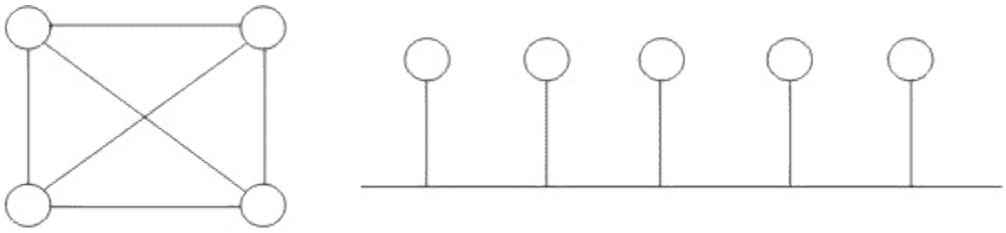
truyền đi. Nó cho phép một ký tự được truyền đi bất kỳ lúc nào mà không cần quan tâm đến các tín hiệu đồng bộ trước đó.

Phương thức truyền đồng bộ: sử dụng phương thức truyền cần có đồng bộ giữa máy gửi và máy nhận, nó chèn các ký tự đặc biệt như SYN (Synchronization), EOT (End Of Transmission) hay đơn giản hơn, một cái "cờ " (flag) giữa các dữ liệu của máy gửi để báo hiệu cho máy nhận biết được dữ liệu đang đến hoặc đã đến.

Tầng 2: Liên kết dữ liệu (Data link)

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

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



truyền vật lý.

Hình 4.2: Các đường truyền kết nối kiểu "một điểm - một điểm" và "một điểm - nhiều điểm".

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

Các giao thức tầng liên kết dữ liệu chia làm 2 loại chính là các giao thức hướng ký tư và các giao thức hướng bit. Các giao thức hướng ký tự được xây dựng dựa trên các ký tự đặc biệt của một bộ mã chuẩn nào đó (như ASCII hay EBCDIC), trong khi đó các giao thức hướng bit lại

dùng các cấu trúc nhị phân (xâu bit) để xây dựng các phần tử của giao thức (đơn vị dữ liệu, các thủ tục.) và khi nhận, dữ liệu sẽ được tiếp nhận lần lượt từng bit một.

Tầng 3: Mạng (Network)

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

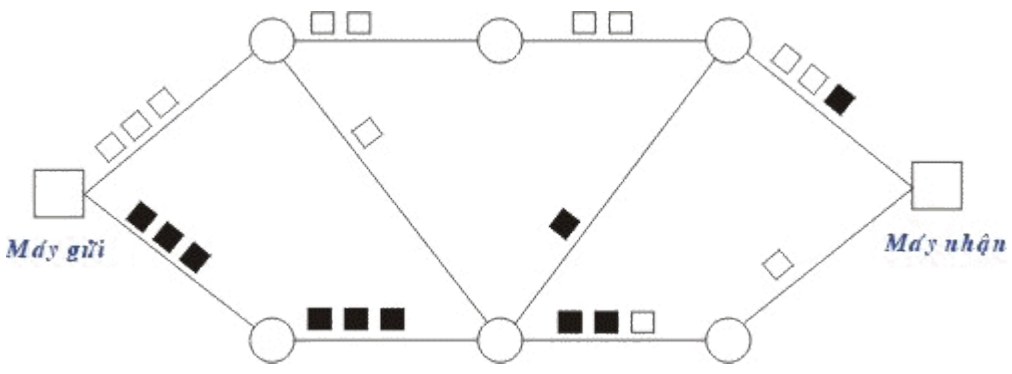
Tầng mạng cung các các phương tiện để truyền các gói tin qua mạng, thậm chí qua một mạng của mạng (network of network). Bởi vậy nó cần phải đáp ứng với nhiều kiểu mạng và nhiều kiểu dịch vụ cung cấp bởi các mạng khác nhau. hai chức năng chủ yếu của tầng mạng là chọn đường (routing) và chuyển tiếp (relaying).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

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

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

Quyết định chọn đường tối ưu dựa trên các thông tin đã có về mạng tại thời điểm đó thông qua những tiêu chuẩn tối ưu nhất định.

Cập nhật các thông tin về mạng, tức là thông tin dùng cho việc chọn đường, trên mạng luôn có sự thay đổi thường xuyên nên việc cập nhật là việc cần thiết.



Hình 4. 3: Mô hình chuyển vận các gói tin trong mạng chuyển mạch gói

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

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

Phương thức chọn đường xử lý tại chỗ được đặc trưng bởi việc chọn đường được thực hiện tại mỗi nút của mạng. Trong từng thời điểm, mỗi nút phải duy trì các thông tin của mạng và tự xây dựng bảng chọn đường cho mình. Như vậy các thông tin tổng thể của mạng cần dùng cho việc chọn đường cần cập nhập và được cất giữ tại mỗi nút.

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

Trạng thái của đường truyền.

Thời gian trễ khi truyền trên mỗi đường dẫn.

Mức độ lưu thông trên mỗi đường.

Các tài nguyên khả dụng của mạng.

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

Hiện nay khi nhu cầu truyền thông đa phương tiện (tích hợp dữ liệu văn bản, đồ 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.

Tầng 4: Vận chuyển (Transport)

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

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

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

Mạng loại A: Có tỷ suất lỗi và sự cố có báo hiệu chấp nhận được (tức là chất lượng chấp nhận được). Các gói tin được giả thiết là không bị mất. Tầng vận chuyển không cần cung cấp các dịch vụ phục hồi hoặc sắp xếp thứ tự lại.

Mạng loại B: Có tỷ suất lỗi chấp nhận được nhưng tỷ suất sự cố có báo hiệu lại không chấp nhận được. Tầng giao vận phải có khả năng phục hồi lại khi 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) được đánh số. Ngoài ra giao thức còn có khả năng báo nhận cho nơi gửi và truyền dữ liệu khẩn. So với giao thức lớp 0 giao thức lớp 1 có thêm khả năng phục hồi lỗi.

Giao thức lớp 2 (Multiplexing Class - lớp dồn kênh) là một cải tiến của lớp 0 cho phép dồn một số liên kết chuyển vận vào một liên kết mạng duy nhất, đồng thời có thể kiểm soát luồng dữ liệu để tránh tắc nghẽn. Giao thức lớp 2 không có khả năng phát hiện và phục hồi lỗi. Do vậy nó cần đặt trên một tầng mạng loại A.

Giao thức lớp 3 (Error Recovery and Multiplexing Class - lớp phục hồi lỗi cơ bản và dồn kênh) là sự mở rộng giao thức lớp 2 với khả năng phát hiện và phục hồi lỗi, nó cần đặt trên một tầng mạng loại B.

Giao thức lớp 4 (Error Detection and Recovery Class - Lớp phát hiện và phục hồi lỗi) là lớp có hầu hết các chức năng của các lớp trước và còn bổ sung thêm một số khả năng khác để kiểm soát việc truyền dữ liệu.

Tầng 5: Giao dịch (Session)

Tầng giao dịch (session layer) thiết lập "các giao dịch" giữa các trạm trên mạng, nó đặt tên nhất quán cho mọi thành phần muốn đối thoại với nhau và lập ánh xa giữa các tên với địa

chỉ của chúng. Một giao dịch phải được thiết lập trước khi dữ liệu được truyền trên mạng, tầng giao dịch đảm bảo cho các giao dịch được thiết lập và duy trì theo đúng qui định.

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

Điều phối việc trao đổi dữ liệu giữa các ứng dụng bằng cách thiết lập và giải phóng (một cách lôgic) các phiên (hay còn gọi là các hội thoại - dialogues)

Cung cấp các điểm đồng bộ để kiểm soát việc trao đổi dữ liệu.

Áp đặt các qui tắc cho các tương tác giữa các ứng dụng của người sử dụng.

Cung cấp cơ chế "lấy lượt" (nắm quyền) trong quá trình trao đổi dữ liệu.

Trong trường hợp mạng là hai chiều luân phiên thì nẩy sinh vấn đề: hai người sử dụng luân phiên phải "lấy lượt" để truyền dữ liệu. Tầng giao dịch duy trì tương tác luân phiên bằng cách báo cho mỗi người sử dụng khi đến lượt họ được truyền dữ liệu. Vấn đề đồng bộ hóa trong tầng giao dịch cũng được thực hiện như cơ chế kiểm tra/phục hồi, dịch vụ này cho phép người sử dụng xác định các điểm đồng bộ hóa trong dòng dữ liệu đang chuyển vận và khi cần thiết có thể khôi phục việc hội thoại bắt đầu từ một trong các điểm đó

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

Tầng giao dịch có các hàm cơ bản sau:

Give Token cho phép người sử dụng chuyển một token cho một người sử dụng khác của một liên kết giao dịch.

Please Token cho phép một người sử dụng chưa có token có thể yêu cầu token đó.

Give Control dùng để chuyển tất cả các token từ một người sử dụng sang một người sửdụng khác.

Tầng 6: Trình bày (Presentation)

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

để truyền thông và cho phép chuyển đổi từ dạng biểu diễn cục bộ sang biểu diễn chung và ngược lại.

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

Tầng 7: Ứng dụng (Application)

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

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

Chương 5

Các đặc tính kỹ thuật của mạng cục bộ

Trên thực tế mạng cục bộ là một hệ thống truyền dữ liệu giữa các máy tính với một khoảng cách tương đối hẹp, điều đó cho phép có những lựa chọn đa dạng về thiết bị . Tuy nhiên những lựa chọn đa dạng này lại bị hạn chế bởi các đặc tính kỹ thuật của mạng cục bộ, đó làø tập hợp các quy tắc chuẩn đã được quy ước mà tất cả các thực thể tham gia truyền thông trên mạng phải tuân theo để đảm bảo cho mạng hoạt động tốt. Các đặc tính chính của mạng cục bộ mà chúng ta nói tới sau đây là:

Cấu trúc của mạng (hay topology của mạng mà qua đó thể hiện cách nối các mạng máy tính với nhau ra sao).

Các nghi thức truyền dữ liệu trên mạng (các thủ tục hướng dẫn trạm làm việc làm thế nào và lúc nào có thể thâm nhập vào đường dây cáp để gửi các gói thông tin).

Các loại đường truyền và các chuẩn của chúng .

Các phương thức tín hiệu

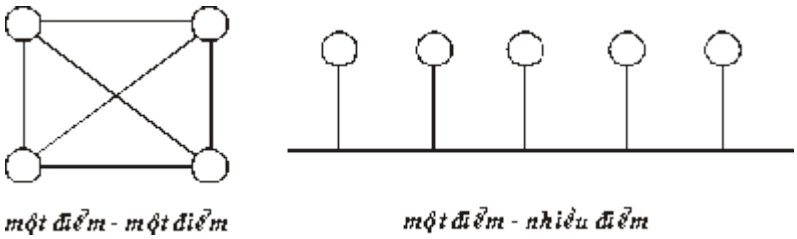
I. Cấu trúc của mạng (Topology)

Hình trạng của mạng cục bộ thể hiện qua cấu trúc hay hình dáng hình học 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 saün liên kết các máy tính và các thiết bị có liên quan.

Trước hết chúng ta xem xét hai phương thức nối mạng chủ yếu được sử dụng trong việc liên kết các máy tính là "một điểm - một điểm" và "một điểm - nhiều điểm ".

Với phương thức "một điểm - một điểm" các đường truyền riêng biệt được thiết lâp để nối các cặp máy tính lại với nhau. Mỗi máy tính có thể truyền và nhận trực tiếp dữ liệu hoặc có thể làm trung gian như lưu trữ những dữ liệu mà nó nhận được rồi sau đó chuyển tiếp dữ liệu đi cho một máy khác để dữ liệu đó đạt tới đích.

Theo phương thức "một điểm - nhiều điểm " tất cả các trạm phân chia chung một đường truyền vật lý. Dữ liệu được gửi đi từ một máy tính sẽ có thể được tiếp nhận bởi tất cả các máy tính còn lại, bởi vậy cần chỉ ra địa chỉ đích của dữ liệu để mỗi máy tính căn cứ vào đó kiểm tra xem dữ liệu có phải dành cho mình không nếu đúng thì nhận còn nếu không thì bỏ qua.



Hình 5.1: Các phương thức liên kết mạng

Tùy theo cấu trúc của mỗi mạng chúng sẽ thuộc vào một trong hai phương thức nối mạng và mỗi phương thức nối mạng sẽ có những yêu cầu khác nhau về phần cứng và phần mềm.

II. Những cấu trúc chính của mạng cục bộ

1. Dạng đường thẳng (Bus)

Trong dạng đường thẳng các máy tính đều được nối vào một đường dây truyền chính (bus). Đường truyền chính này được giới hạn hai đầu bởi một loại đầu nối đặc biệt gọi là terminator (dùng để nhận biết là đầu cuối để kết thúc đường truyền tại đây). Mỗi trạm được nối vào bus qua một đầu nối chữ T (T_connector) hoặc một bộ thu phát (transceiver). Khi một trạm truyền dữ liệu, tín hiệu được truyền trên cả hai chiều của đường truyền theo từng gói một, mỗi gói đều phải mang địa chỉ trạm đích. Các trạm khi thấy dữ liệu đi qua nhận lấy, kiểm tra, nếu đúng với địa chỉ của mình thì nó nhận lấy còn nếu không phải thì bỏ qua.

Sau đây là vài thông số kỹ thuật của topology bus. Theo chuẩn IEEE 802.3 (cho mạng cục bộ) với cách đặt tên qui ước theo thông số: tốc độ truyền 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.

Dạng kết nối này có ưu điểm là ít tốn dây cáp, tốc độ truyền dữ liệu cao tuy nhiên nếu lưu lượng truyền tăng cao thì dễ gây ách tắc và nếu có trục trặc trên hành lang chính thì khó phát hiện ra.

Hiện nay các mạng sử dụng hình dạng đường thẳng là mạng Ethernet và G-net.

2. Dạng vòng tròn (Ring)

Các máy tính được liên kết với nhau thành một vòng tròn theo phương thức "một điểm - một điểm ", qua đó mỗi một trạm có thể nhận và truyền dữ liệu theo vòng một chiều và dữ liệu được truyền theo từng gói một. Mỗi gói dữ liệu đều có mang địa chỉ trạm đích, mỗi trạm khi nhận được một gói dữ liệu nó kiểm tra nếu đúng với địa chỉ của mình thì nó nhận lấy còn nếu không phải thì nó sẽ phát lại cho trạm kế tiếp, cứ như vậy gói dữ liệu đi được đến đích. Với dạng kết nối này có ưu điểm là không tốn nhiều dây cáp, tốc độ truyền dữ liệu cao, không gây ách tắc tuy nhiên các giao thức để truyền dữ liệu phức tạp và nếu có trục trặc trên một trạm thì cũng ảnh hưởng đến toàn mạng.

Hiện nay các mạng sử dụng hình dạng vòng tròn là mạng Tocken ring của IBM.

3. Dạng hình sao (Star)

Ở dạng hình sao, tất cả các trạm được nối vào một thiết bị trung tâm có nhiệm vụ nhận tín hiệu từ các trạm và chuyển tín hiệu đến trạm đích với phương thức kết nối là phương thức "một điểm - một điểm ". Thiết bị trung tâm hoạt động giống như một tổng đài cho phép thực hiện việc nhận và truyền dữ liệu từ trạm này tới các trạm khác. Tùy theo yêu cầu truyền thông trong mạng , thiết bị trung tâm có thể là một bộ chuyển mạch (switch), một bộ chọn đường (router) hoặc đơn giản là một bộ phân kênh (Hub). Có nhiều cổng ra và mỗi cổng nối với một máy. Theo chuẩn IEEE 802.3 mô hình dạng Star thường dùng:

10BASE-T: dùng cáp UTP, tốc độ 10 Mb/s, khoảng cách từ thiết bị trung tâm tới trạm tối đa là 100m.

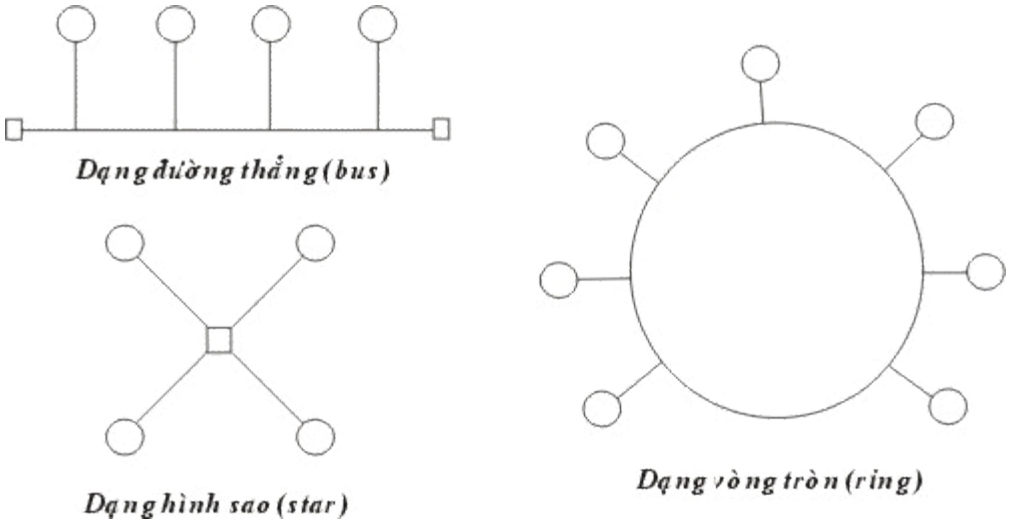
100BASE-T tương tự như 10BASE-T nhưng tốc độ cao hơn 100 Mb/s.

Ưu và khuyết điểm

Ưu điểm: Với dạng kết nối này có ưu điểm là không đụng độ hay ách tắc trên đường truyền, lắp đặt đơn giản, dễ dàng cấu hình lại (thêm, bớt trạm). 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 đại) tốn đường dây cáp nhiều, tốc độ truyền dữ liệu không cao.

Hiện nay các mạng sử dụng hình dạng hình sao là mạng STARLAN của AT&T và S-NET của Novell.



Hình 5.2 : Các loại cấu trúc chính của mạng cục bộ.

	Đường thẳng	Vòng Tròn	Hình sao
Ứng dụng	Tốt cho trường hợp mạng nhỏ và mạng có giao thông thấp và 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.	hiên 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	Phải dự trù gấp đôi nguồn lực hoặc phải có 1 phương thức thay thế khi 1 nút không hoạt động nếu vẫn	Tổng phí rất cao khi làm nhiêm vụ của thiết bị trung tâm, thiết bị trung tâm ï không được

	trường .Sự dư thừa kênh truyền được khuyến để giảm bớt nguy cơ xuất hiện sự cố trên mạng	muốn mạng hoạt động bình thường	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	Mơt 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 rộng 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 rộng 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 .

Hình 6.4 : Bảng so sánh tính năng giữa các cấu trúc của mạng LAN

III. Phương thức truyền tín hiệu

Thông thường có hai phương thức truyền tín hiệu trong mạng cục bộ là dùng băng tần cơ sở (baseband) và băng tần rộng (broadband). Sự khác nhau chủ yếu giữa hai phương thức truyền tín hiệu này là băng tầng cơ sở chỉ chấp nhận một kênh dữ liệu duy nhất trong khi băng rộng có thể chấp nhận đồng thời hai hoặc nhiều kênh truyền thông cùng phân chia giải thông của đường truyền.

Hầu hết các mạng cục bộ sử dụng phương thức băng tần cơ sở. Với phương thức truyền tín hiệu này này tín hiệu có thể được truyền đi dưới cả hai dạng: tương tự (analog) hoặc số (digital). Phương thức truyền băng tần rộng chia giải thông (tần số) của đường truyền thành

nhiều giải tần con trong đó mỗi dải tần con đó cung cấp một kênh truyền dữ liệu tách biệt nhờ sử dụng một cặp modem đặc biệt gọi là bộ giải / Điều biến RF cai quản việc biến đổi các tín hiệu số thành tín hiệu tương tự có tần số vô tuyến (RF) bằng kỹ thuật ghép kênh.

IV. Các giao thức truy cập đường truyền trên mạng LAN

Để truyền được dữ liệu trên mạng người ta phải có các thủ tục nhằm hướng dẫn các máy tính của mạng làm thế nào và lúc nào có thể thâm nhập vào đường dây cáp để gửi các gói dữ kiện. Ví dụ như đối với các dạng bus và ring thì chỉ có một đường truyền duy nhất nối các trạm với nhau, cho nên cần phải có các quy tắc chung cho tất cả các trạm nối vào mạng để đảm bảo rằng đường truyền được truy nhập và sử dụng một cách hợp lý.

Có nhiều giao thức khác nhau để truy nhập đường truyền vật lý nhưng phân thành hai loại: các giao thức truy nhập ngẫu nhiên và các giao thức truy nhập có điều khiển.

1. Giao thức chuyển mạch (yêu cầu và chấp nhận)

Giao thức chuyển mạch là loại giao thức hoạt động theo cách thức sau: một máy tính của mạng khi cần có thể phát tín hiệu thâm nhập vào mạng, nếu vào lúc này đường cáp không bận thì mạch điều khiển sẽ cho trạm này thâm nhập vào đường cáp còn nếu đường cáp đang bận, nghĩa là đang có giao lưu giữa các trạm khác, thì việc thâm nhập sẽ bị từ chối.

2. Giao thức đường dây đa truy cập với cảm nhận va chạm (Carrier Sense Multiple Access with Collision Detection hay CSMA/CD)

Giao thức đường dây đa truy cập cho phép nhiều trạm thâm nhập cùng một lúc vào mạng, giao thức này thường dùng trong sơ đồ mạng dạng đường thẳng. Mọi trạm đều có thể được truy nhập vào đường dây chung một cách ngẫu nhiên và do vậy có thể dẫn đến xung đột (hai hoặc nhiều trạm đồng thời cùng truyền dữ liệu). Các trạm phải kiểm tra đường truyền gói dữ liệu đi qua có phải của nó hay không. Khi một trạm muốn truyền dữ liệu nó phải kiểm tra đường truyền xem có rảnh hay không để gửi gói dữ liệu của, nếu đường truyền đang bận trạm phải chờ đợi chỉ được truyền khi thấy đường truyền rảnh. Nếu cùng một lúc có hai trạm cùng sử dụng đường truyền thì giao thức phải phát hiện điều này và các trạm phải ngưng thâm nhập, chờ đợi lần sau các thời gian ngẫu nhiên khác nhau.

Khi đường cáp đang bận trạm phải chờ đợi theo một trong ba phương thức sau:

Trạm tạm chờ đợi một thời gian ngẫu nhiên nào đó rồi lại bắt đầu kiểm tra đường truyền.

Trạm tiếp tục kiểm tra đường truyền đến khi đường truyền rảnh thì truyền dữ liệu đi.

Trạm tiếp tục kiểm tra đường truyềnđến khi đường truyền rảnh thì truyền dữ liệu đi với xác suất p xác định trước ($0 < p < 1$).

Tại đây phương thức 1 có hiệu quả trong việc tránh xung đột vì hai trạm cần truyền khi thấy đường truyền bận sẽ cùng rút lui và chờ đợi trong các thời gian ngẫu nhiên khác nhau. Ngược lại phương thức 2 cố gắng giảm thời gian trống của đường truyền bằng các cho phép trạm có thể truyền ngay sau khi một cuộc truyền kết thúc song nếu lúc đó có thêm một trạm khác đang đợi thì khả năng xẩy ra xung đột là rất cao. Phương thức 3 với giá trị p phải lựa chọn hợp lý có thể tối thiểu hóa được khả năng xung đột lẫn thời gian trống của đường truyền.

Khi lưu lượng các gói dữ liệu cần di chuyển trên mạng quá cao, thì việc đụng độ có thể xẩy ra với sồ lượng lớn có gây tắc nghẽn đường truyền dẫn đến làm chậm tốc độ truyền tin của hệ thống.

3. Giao thức dùng thẻ bài vòng (Token ring)

Đây là giao thức truy nhập có điều khiển chủ yếu dùng kỹ thuật chuyển thẻ bài (token) để cấp phát quyền truy nhập đường truyền tức là quyền được truyền dữ liệu đi. Thẻ bài ở đay là một đơn vị dữ liệu đặc biệt, có kích thước và nội dung (gồm các thông tin điều khiển) được quy định riêng cho mỗi giao thức. Theo giao thức dùng thẻ bài vòng trong đường cáp liên tục có một thẻ bài chạy quanh trong mạng Thẻ bài là một đơn vị dữ liệu đặc biệt trong đó có một bit biểu diễn trạng thái sử dụng của nó (bận hoặc rỗi). Một trạm muốn truyền dữ liệu thì phải đợi đến khi nhận được một thẻ bài rảnh. Khi đó trạm sẽ đổi bit trạng thái của thẻ bài thành bận, nép gói dữ liệu có kèm theo địa chỉ nơi nhận vào thẻ bài và truyền đi theo chiều của vòng.

Vì thẻ bài chạy vòng quang trong mạng kín và chỉ có một thẻ nên việc đụng độ dữ liệu không thể xẩy ra, do vậy hiệu suất truyền dữ liệu của mạng không thay đổi.

Trong các giao thức này cần giải quyết hai vấn đề có thể dẫn đến phá vỡ hệ thống. Một là việc mất thẻ bài làm cho trên vòng không còn thẻ bài lưu chuyển nữa. Hai là một thẻ bài bận lưu chuyển không dừng trên vòng.

4. Giao thức dung thẻ bài cho dạng đường thẳng (Token bus)

Đây là giao thức truy nhập có điều khiển trong để cấp phát quyền truy nhập đường truyền cho các trạm đang có nhu cầu truyền dữ liệu, một thẻ bài được lưu chuyển trên một vòng logic thiết lập bởi các trạm đó. Khi một trạm có thẻ bài thì nó có quyền sử dụng đường truyền trong một thời gian xác định trước. Khi đã hết dữ liệu hoặc hết thời đoạn cho phép, trạm chuyển thẻ bài đến trạm tiếp theo trong vòng logic.

Như vậy trong mạng phải thiết lập được vòng logic (hay còn gọi là vòng ảo) bao gồm các trạm đang hoạt động nối trong mạng được xác định vị trí theo một chuỗi thứ tự mà trạm cuối cùng của chuỗi sẽ tiếp liền sau bởi trạm đầu tiên. Mỗi trạm được biết địa chỉ của các trạm kề trước và sau nó trong đó thứ tự của các trạm trên vòng logic có thể độc lập với thứ tự vật lý.

Cùng với việc thiết lập vòng thì giao thức phải luôn luôn theo dõi sự thay đổi theo trạng thái thực tế của mạng.

V. Đường cáp truyền mạng

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

1. Cáp xoắn cặp

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

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

2. Cáp đồng trục

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

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

Hình 5.3: Tính năng kỹ thuật của một số loại cáp mạng

Cáp đồng trục có độ suy hao ít hơn so với các loại cáp đồng khác (ví dụ như cáp xoắn đôi) do ít bị ảnh hưởng của môi trường. Các mạng cục bộ sử dụng cáp đồng trục có thể có kích thước trong phạm vi vài ngàn mét, cáp đồng trục được sử dụng nhiều trong các mạng dạng

đường thẳng. Hai loại cáp thường được sử dụng là cáp đồng trục mỏng và cáp đồng trục dày trong đường kính cáp đồng trục mỏng là 0,25 inch, cáp đồng trục dày là 0,5 inch. Cả hai loại cáp đều làm việc ở cùng tốc độ nhưng cáp đồng trục mỏng có độ hao suy tín hiệu lớn hơn

Hiện nay có cáp đồng trục sau:

RG -58,50 ohm: dùng cho mạng Thin Ethernet

RG -59,75 ohm: dùng cho truyền hình cáp

RG -62,93 ohm: dùng cho mạng ARCnet

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

3. Cáp sợi quang (Fiber - Optic Cable)

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

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

Dải thông của cáp quang có thể lên tới hàng Gbps và cho phép khoảng cách đi cáp khá xa do độ suy hao tín hiệu trên cáp rất thấp. Ngoài ra, vì cáp sợi quang không dùng tín hiệu điện 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 khó lắp đặt và giá thành còn cao , nhìn chung cáp quang thích hợp cho mọi mạng hiện nay và sau này.

4. Các yêu cầu cho một hệ thống cáp

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

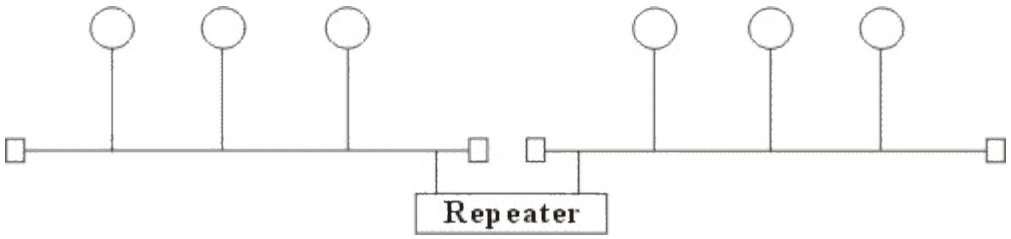
Đúng chuẩn: hệ thống cáp phải thực hiện đúng chuẩn, đảm bảo cho khả năng nâng cấp sau này cũng như dễ dàng cho việc kết nối các thiết bị khác nhau của các nhà sản xuất khác nhau. Tiêu chuẩn quốc tế dùng cho các hệ thống mạng hiện nay là EIA/TIA 568B.

Tiết kiệm và "linh hoạt" (flexible): hệ thống cáp phải được thiết kế sao cho kinh tế nhất, dễ dàng trong việc di chuyển các trạm làm việc và có khả năng mở rộng sau này.

Chương 6
Các thiết bị liên kết mạng

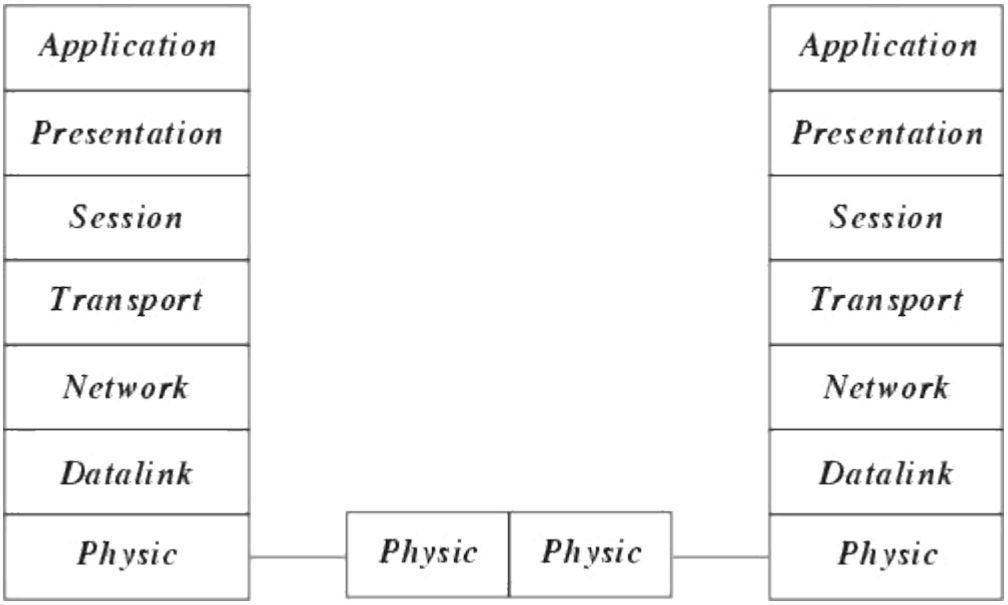
I. Repeater (Bộ tiếp sức)

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



Hình 6.1: Mô hình liên kết mạng của Repeater.

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



Hình 6.2: Hoạt động của bộ tiếp sức trong mô hình OSI

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

Repeater điện nối với đường dây điện ở cả hai phía của nó, nó nhận tín hiệu điện từ một phía và phát lại về phía kia. Khi một mạng sử dụng Repeater điện để nối các phần của mạng lại thì có thể làm tăng khoảng cách của mạng, nhưng khoảng cách đó luôn bị hạn chế bởi một khoảng cách tối đa do độ trễ của tín hiệu. Ví dụ với mạng sử dụng cáp đồng 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.

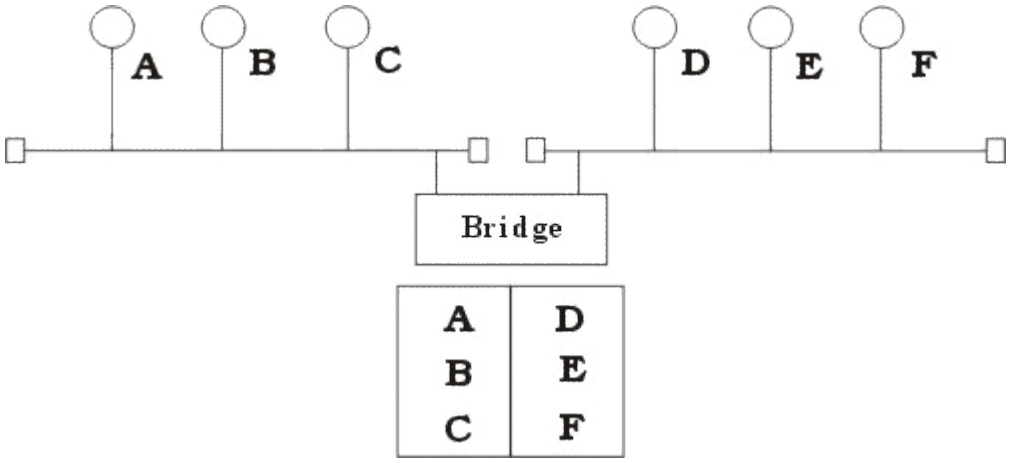
Việc sử dụng Repeater không thay đổi nội dung các tín hiện đi qua nên nó chỉ được dùng để nối hai mạng có cùng giao thức truyền thông (như hai mạng Ethernet hay hai mạng Token ring) nhưng không thể nối hai mạng có giao thức truyền thông khác nhau (như một mạng Ethernet và một mạng Token ring). Thêm nữa 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 lưa chọn sử dụng Repeater cần chú ý lựa chọn loại có tốc độ chuyển vận phù hợp với tốc độ của mạng.

II. Bridge (Cầu nối)

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

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

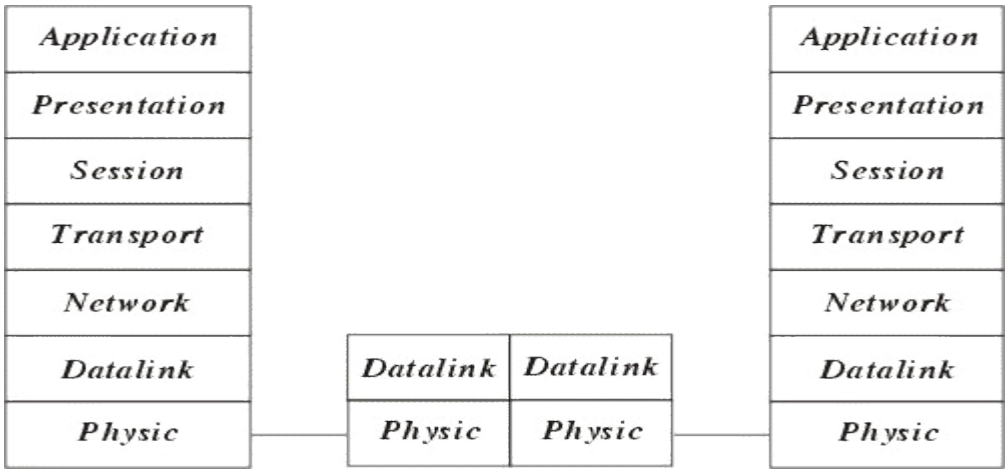
Để thực hiện được điều này trong Bridge ở mỗi đầu kết nối có một bảng các địa chỉ các trạm được kết nối vào phía đó, khi hoạt động cầu nối xem xét mỗi gói tin nó nhận được bằng cách đọc địa chỉ của nơi gửi và nhận và dựa trên bảng địa chỉ phía nhận được gói tin nó quyết định gửi gói tin hay không và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



Hình 6.3: Hoạt động của Bridge

Khi đọc địa chỉ nơi gửi Bridge kiểm tra xem trong bảng địa chỉ của phần mạng nhận được gói tin có địa chỉ đó hay không, nếu không có thì Bridge tự động 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 6.4: Hoạt động của Bridge trong mô hình OSI

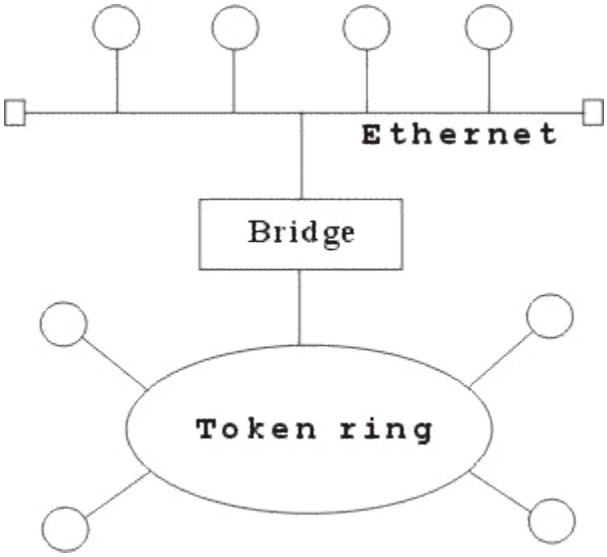
Để đánh giá một Bridge người ta đưa ra hai khái niệm : Lọc và chuyển vận. Quá trình xử lý mỗi gói tin được gọi là quá trình lọc trong đó tốc độ lọc thể hiện trực tiếp khả năng hoạt động của Bridge. Tốc độ chuyển vận được thể hiện số gói tin/giây trong đó thể hiện khả năng của Bridge chuyển các gói tin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

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

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

Ví dụ : Bridge biên dịch nối một mạng Ethernet và một mạng Token ring. Khi đó Cầu nối thực hiện như một nút token ring trên mạng Token ring và một nút 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 6.5: Ví dụ về Bridge biên dịch

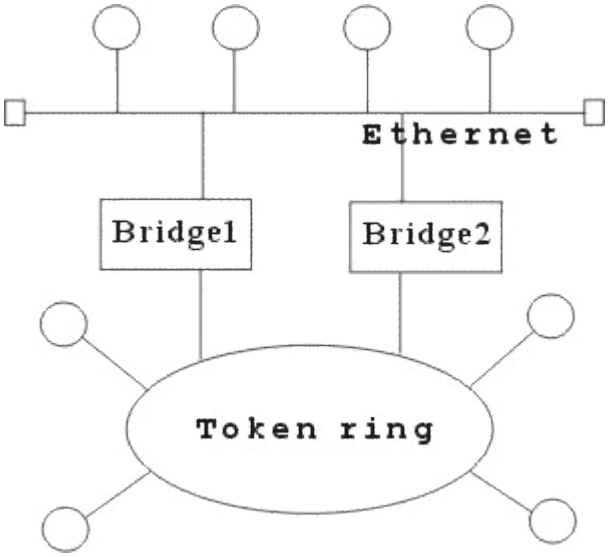
Người ta sử dụng Bridge trong các trường hợp sau :

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.

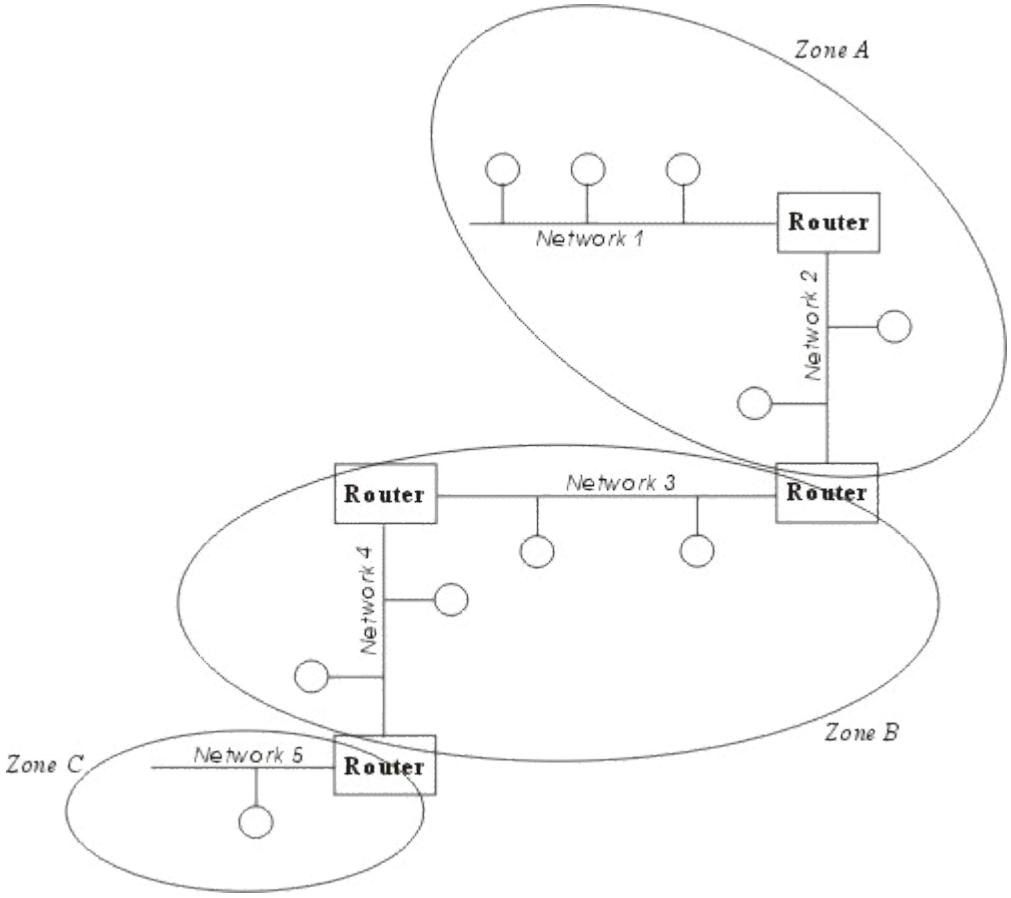
Hình 6.6 : Liên kết mạng với 2 Bridge

Một số Bridge được chế tạo thành một bộ riêng biệt, chỉ cần nối dây và bật. Các Bridge khác chế tạo như card chuyên dùng 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.

III. Router (Bộ tìm đường)

Router là một thiết bị hoạt động trên tầng mạng, nó có thể tìm được đường đi tốt nhất cho các gói tin qua nhiều kết nối để đi từ trạm gửi thuộc mạng đầu đến trạm nhận thuộc mạng

cuối. Router có thể được sử dụng trong việc nối nhiều mạng với nhau và cho phép các gói tin có thể đi theo nhiều đường khác nhau để tới đích.



Hình 6.7: Hoạt động của Router.

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

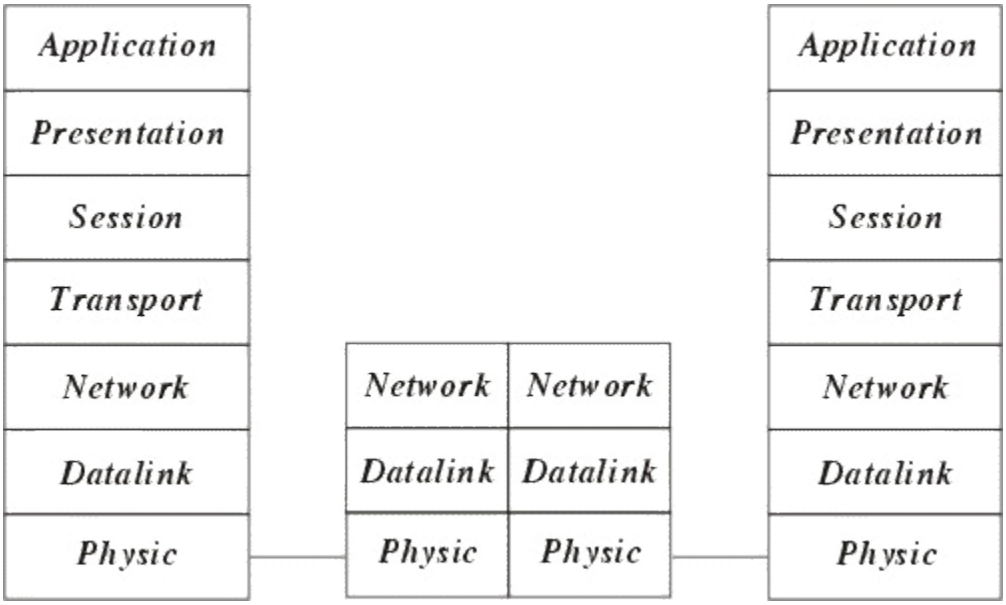
Khi xử lý một gói tin Router phải tìm được đường đi của gói tin qua mạng. Để làm được điều đó Router phải tìm được đường đi tốt nhất trong mạng dựa trên các thông tin nó có về mạng, thông thường trên mỗi Router có một bảng chỉ đường (Router table). Dựa trên dữ liệu về

Router gần đó và các mạng trong liên mạng, Router tính được bảng chỉ đường (Router table) tối ưu dựa trên một thuật toán xác định trước.

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 đôiø gói tin của giao thức này sang gói tin của giao thức kia, Router cũng ù 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 6.8: Hoạt động của Router trong mô hình OSI

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

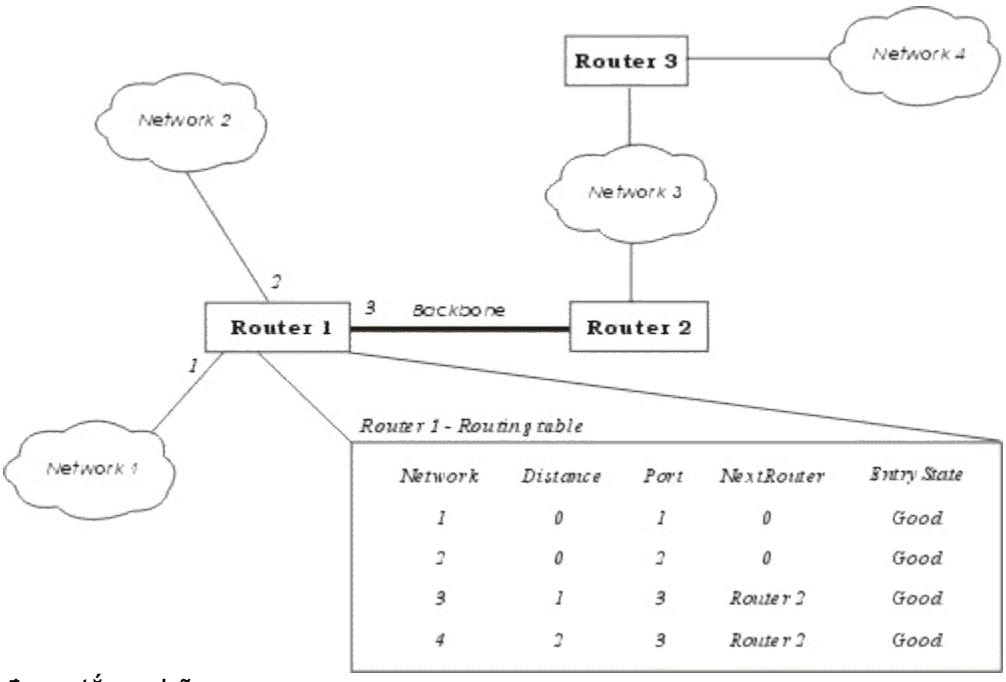
Các lý do sử dụng Router :

Router có các phần mềm lọc ưu việt hơn là Bridge do các gói tin 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 6.9: Ví dụ về bảng chỉ đường (Routing table) của Router.

Các phương thức hoạt động của Router

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

Phương thức véc tơ khoảng cách : mỗi Router luôn luôn truyền đi thông tin về bảng chỉ đường của mình trên mạng, thông qua đó các Router khác sẽ cập nhật lên bảng chỉ đường của mình.

Phương thức trạng thái tĩnh : Router chỉ truyền các thông báo khi có phát hiện có sự thay đổi trong mạng 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.

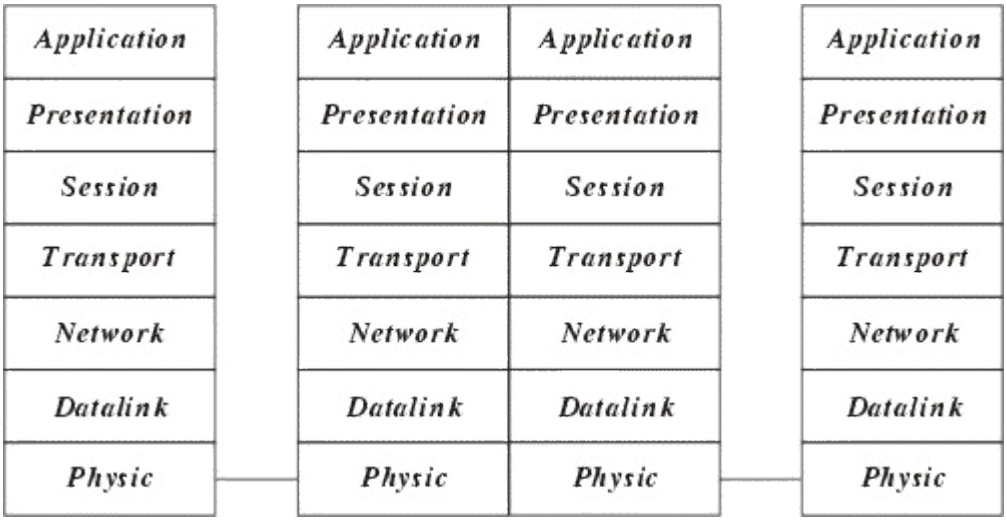
NLSP (Netware Link Service Protocol) được phát triển bởi Novell dùng để thay thế RIP hoạt động theo phương thức véctơ khoảng cách, mỗi Router được biết cấu trúc của mạng và việc truyền các bảng chỉ đường giảm đi..

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...

IV. 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 6.10: Hoạt động của Gateway trong mô hình OSI

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

V. Hub (Bộ tập trung)

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

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

Hub bị động (Passive Hub) : Hub bị động không chứa các linh kiện điện tử và cũng không xử lý các tín hiệu dữ liệu, nó có chức năng duy nhất là tổ hợp các tín hiệu từ một số đoạn cáp mạng. Khoảng cách giữa một máy tính và Hub không thể lớn hơn một nửa khoảng cách tối đa cho phép giữa 2 máy tính trên mạng (ví dụ khoảng cách tối đa cho phép giữa 2 máy tính của mạng là 200m thì khoảng cách tối đa giữa một máy tính và hub là 100m). Các mạng ARCnet thường dùng Hub bị động.

Hub chủ động (Active Hub) : Hub chủ động có các linh kiện điện tử có thể 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.

Chương 7

Giao thức TCP/IP

Giao thức TCP/IP được phát triển từ mạng ARPANET và Internet và được dùng như giao thức mạng và vận chuyển trên mạng Internet. TCP (Transmission Control Protocol) là giao thức thuộc tầng vận chuyển và IP (Internet Protocol) là giao thức thuộc tầng mạng của mô hình OSI. Họ giao thức TCP/IP hiện nay là giao thức được sử dụng rộng rãi nhất để liên kết các máy tính và các mạng.

Hiện nay các máy tính của hầu hết các mạng có thể sử dụng giao thức TCP/IP để liên kết với nhau thông qua nhiều hệ thống mạng với kỹ thuật khác nhau. Giao thức TCP/IP thực chất là một họ giao thức cho phép các hệ thống mạng cùng làm việc với nhau thông qua việc cung cấp phương tiện truyền thông liên mạng.

I. Giao thức IP

1. Tổng quát

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

Sơ đồ địa chỉ hóa để định danh các trạm (host) trong liên mạng được gọi là địa chỉ IP 32 bits (32 bit IP address). Mỗi giao diện trong 1 máy có hỗ trợ giao thức IP đều phải được gán 1 địa chỉ IP (một máy tính có thể gắn với nhiều mạng do vậy có thể có nhiều địa chỉ IP). Địa chỉ IP gồm 2 phần: địa chỉ mạng (netid) và địa chỉ máy (hostid). Mỗi địa chỉ IP có độ dài 32 bits được tách thành 4 vùng (mỗi vùng 1 byte), có thể biểu thị dưới dạng thập phân, bát phân, thập lục

phân hay nhị phân. Cách viết phổ biến nhất là dùng ký pháp thập phân có dấu chấm (dotted decimal notation) để tách các vùng. Mục đích của địa chỉ IP là để định danh duy nhất cho một máy tính bất kỳ trên liên mạng.

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

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

Cấu trúc của các địa chỉ IP như sau:

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

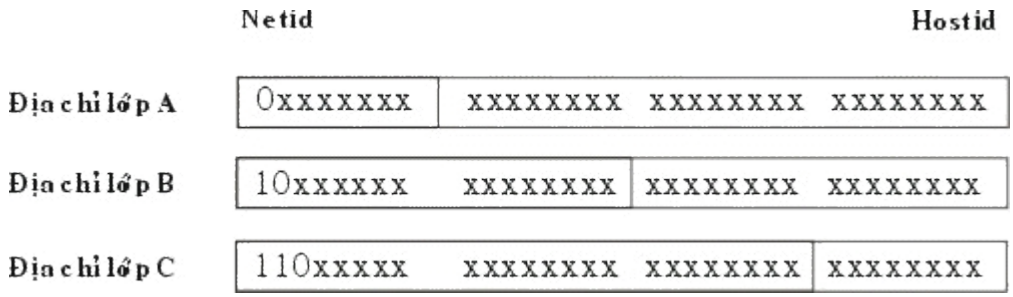
Mạng lớp B: địa chỉ mạng (netid) là 2 Byte và địa chỉ host (hostid) là 2 byte.

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

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

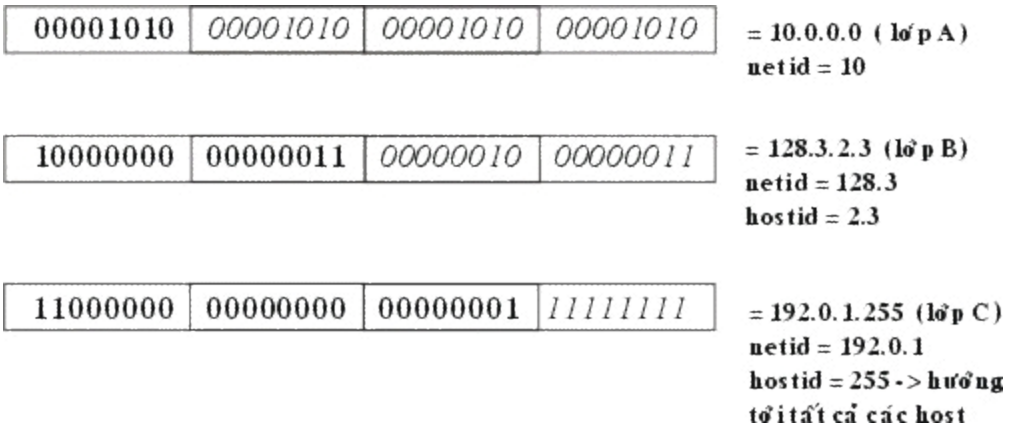
Lớp B cho phép định danh tới 16384 mạng, với tối đa 65534 host trên mỗi mạng.

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



Hình 7.1: Cấu trúc các lớp địa chỉ IP

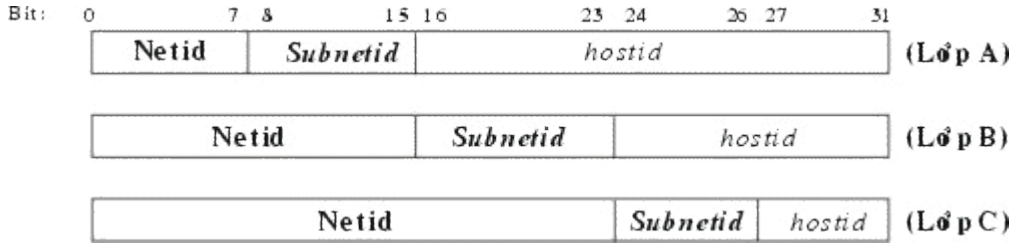
Một số địa chỉ có tính chất đặc biệt: Một địa chỉ có hostid = 0 được dùng để hướng tới mạng định danh bởi vùng netid. Ngược lại, một địa chỉ có vùng hostid gồm toàn số 1 được dùng để hướng tới tất cả các host nối vào mạng netid, và nếu vùng netid cũng gồm toàn số 1 thì nó hướng tới tất cả các host trong liên mạng



Hình 7.2: Ví dụ cấu trúc các lớp địa chỉ IP

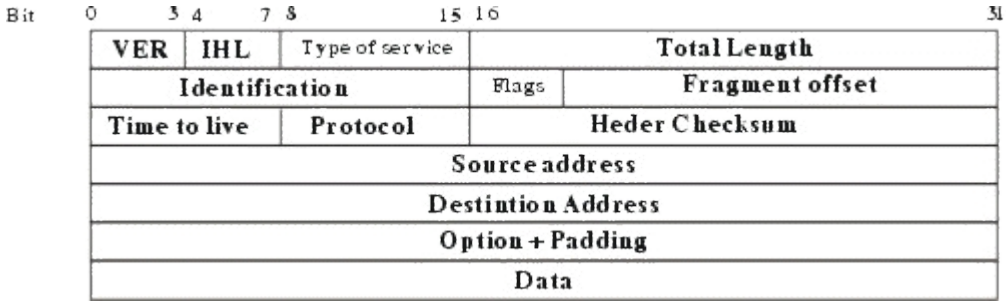
Cần lưu ý rằng các địa chỉ IP được dùng để định danh các host và mạng ở tầng mạng của mô hình OSI, và chúng không phải là các địa chỉ vật lý (hay địa chỉ MAC) của các trạm trên đó một mạng cục bộ (Ethernet, Token Ring.).

Trong nhiều trường hợp, một mạng có thể được chia thành nhiều mạng con (subnet), lúc đó có thể đưa thêm các vùng subnetid để định danh các mạng con. Vùng subnetid được lấy từ vùng hostid, cụ thể đối với lớp A, B, C như ví dụ sau:



Hình 7.3: Ví dụ địa chỉ khi bổ sung vùng subnetid

Đơn vị dữ liệu dùng trong IP được gọi là gói tin (datagram), có khuôn dạng



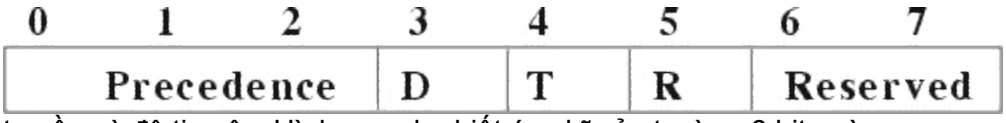
Hình 7.4: Dạng thức của gói tin IP

Ý nghĩa của thông số như sau:

VER (4 bits): chỉ version hiện hành của giao thức IP hiện được cài đặt, Việc có chỉ số version cho phép có các trao đổi giữa các hệ thống sử dụng version cũ và hệ thống sử dụng version mới.

IHL (4 bits): chỉ độ dài phần đầu (Internet header Length) của gói tin datagram, tính theo đơn vị từ (32 bits). Trường này bắt buột phải có vì phần đầu IP có thể có độ dài thay đổi tùy ý. Độ dài tối thiểu là 5 từ (20 bytes), độ dài tối đa là 15 từ hay là 60 bytes.

Type of service (8 bits): đặc tả các tham số về dịch vụ nhằm thông báo cho mạng biết dịch vụ nào mà gói tin muốn được sử dụng, chẳng hạn ưu tiên, thời hạn chậm trễ, năng suất truyền và độ tin cậy. Hình sau cho biết ý nghĩ của trường 8 bits này.



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

D (Delay) (1 bit): chỉ độ trễ yêu cầu trong đó

D = 0 gói tin có độ trễ bình thường

D = 1 gói tin độ trễ thấp

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

T = 0 thông lượng bình thường và

T = 1 thông lượng cao

R (Reliability) (1 bit): chỉ độ tin cậy yêu cầu

R = 0 độ tin cậy bình thường

R = 1 độ tin cậy cao

Total Length (16 bits): chỉ độ dài toàn bộ gói tin, kể cả phần đầu tính theo đơn vị byte với chiều dài tối đa là 65535 bytes. Hiện nay giới hạn trên là rất lớn nhưng trong tương lai với những mạng Gigabit thì các gói tin có kích thước lớn là cần thiết.

Identification (16 bits): cùng với các tham số khác (như Source Address và Destination Address) tham số này dùng để định danh duy nhất cho một datagram trong khoảng thời gian nó vẫn còn trên liên mạng.

Flags (3 bits): liên quan đến sự phân đoạn (fragment) các datagram, Các gói tin khi đi trên đường đi có thể bị phân thành nhiều gói tin nhỏ, trong trường hợp bị phân đoạn thì trường Flags được dùng điều khiển phân đoạn và tái lắp ghép bó dữ liệu. Tùy theo giá trị của Flags sẽ có ý nghĩa là gói tin sẽ không phân đoạn, có thể phân đoạn hay là gói tin phân đoạn cuối cùng. Trường ***Fragment Offset*** cho biết vị trí dữ liệu thuộc phân đoạn tương ứng với đoạn bắt đầu của gói dữ liệu gốc. Ý nghĩa cụ thể của trường Flags là:

bit 0: reserved - chưa sử dụng, luôn lấy giá trị 0.

bit 1: (DF) = 0 (May Fragment) = 1 (Don't Fragment)

bit 2: (MF) = 0 (Last Fragment) = 1 (More Fragments)

Fragment Offset (13 bits): chỉ vị trí của đoạn (fragment) ở trong datagram tính theo đơn vị 8 bytes, có nghĩa là phần dữ liệu mỗi gói tin (trừ gói tin cuối cùng) phải chứa một vùng dữ liệu có độ dài là bội số của 8 bytes. Điều này có ý nghĩa là phải nhân giá trị của Fragment offset với 8 để tính ra độ lệch byte.

Time to Live (8 bits): qui định thời gian tồn tại (tính bằng giây) của gói tin trong mạng để tránh tình trạng một gói tin bị quẩn trên mạng. Thời gian này được cho bởi trạm gửi và được giảm đi (thường qui ước là 1 đơn vị) khi datagram đi qua mỗi router của liên mạng. Thời lượng này giảm xuống tại mỗi router với mục đích giới hạn thời gian tồn tại của các gói tin và kết thúc những lần lặp lại vô hạn trên mạng. Sau đây là 1 số điều cần lưu ý về trường ***Time To Live***:

Nút trung gian của mạng không được gởi 1 gói tin mà trường này có giá trị= 0.

Một giao thức có thể ấn định ***Time To Live*** để thực hiện cuộc ra tìm tài nguyên trên mạng trong phạm vi mở rộng.

Một giá trị cố định tối thiểu phải đủ lớn cho mạng hoạt động tốt.

Protocol (8 bits): chỉ giao thức tầng trên kế tiếp sẽ nhận vùng dữ liệu ở trạm đích (hiện tại thường là TCP hoặc UDP được cài đặt trên IP). Ví dụ: **TCP** có giá trị trường **Protocol** là 6, **UDP** có giá trị trường **Protocol** là 17

Header Checksum (16 bits): Mã kiểm soát lỗi của header gói tin IP.

Source Address (32 bits): Địa chỉ của máy nguồn.

Destination Address (32 bits): địa chỉ của máy đích

Options (độ dài thay đổi): khai báo các lựa chọn do người gửi yêu cầu (tuỳ theo từng chương trình).

Padding (độ dài thay đổi): Vùng đệm, được dùng để đảm bảo cho phần header luôn kết thúc ở một mốc 32 bits.

Data (độ dài thay đổi): Trên một mạng cục bộ như vậy, hai trạm chỉ có thể liên lạc với nhau nếu chúng biết địa chỉ vật lý của nhau. Như vậy vấn đề đặt ra là phải thực hiện ánh xạ giữa địa chỉ IP (32 bits) và địa chỉ vật lý (48 bits) của một trạm.

2. Các giao thức trong mạng IP

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

Giao thức ARP (Address Resolution Protocol): Ở đây cần lưu ý rằng các địa chỉ IP được dùng để định danh các host và mạng ở tầng mạng của mô hình OSI, và chúng không phải là các địa chỉ vật lý (hay địa chỉ MAC) của các trạm trên đó một mạng cục bộ (Ethernet, Token Ring.). Trên một mạng cục bộ hai trạm chỉ có thể liên lạc với nhau nếu chúng biết địa chỉ vật lý của nhau. Như vậy vấn đề đặt ra là phải tìm được ánh xạ giữa địa chỉ IP (32 bits) và địa chỉ vật lý của một trạm. *Giao thức ARP* đã được xây dựng để tìm địa chỉ vật lý từ địa chỉ IP khi cần thiết.

Giao thức RARP (Reverse Address Resolution Protocol): Là giao thức ngược với *giao thức ARP.* Giao thức RARP được dùng để tìm địa chỉ IP từ địa chỉ vật lý.

Giao thức ICMP (Internet Control Message Protocol): Giao thức này thực hiện truyền các thông báo điều khiển (báo cáo về các tình trạng các lỗi trên mạng.) giữa các gateway hoặc một nút của liên mạng. Tình trạng lỗi có thể là: một gói tin IP không thể tới đích của nó, hoặc một router không đủ bộ nhớ đệm để lưu và chuyển một gói tin IP, Một thông báo ICMP được tạo và chuyển cho IP. IP sẽ "bọc" (encapsulate) thông báo đó với một IP header và truyền đến cho router hoặc trạm đích.

3. Các bước hoạt động của giao thức IP

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

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

Tạo một IP datagram dựa trên tham số nhận được.

Tính checksum và ghép vào header của gói tin.

Ra quyết định chọn đường: hoặc là trạm đích nằm trên cùng mạng hoặc một gateway sẽ được chọn cho chặng tiếp theo.

Chuyển gói tin xuống tầng dưới để truyền qua mạng.

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

1) Tính chesksum, nếu sai thì loại bỏ gói tin.

2) Giảm giá trị tham số Time - to Live. nếu thời gian đã hết thì loại bỏ gói tin.

3) Ra quyết định chọn đường.

4) Phân đoạn gói tin, nếu cần.

5) Kiến tạo lại IP header, bao gồm giá trị mới của các vùng Time - to -Live, Fragmentation và Checksum.

6) Chuyển datagram xuống tầng dưới để chuyển qua mạng.

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

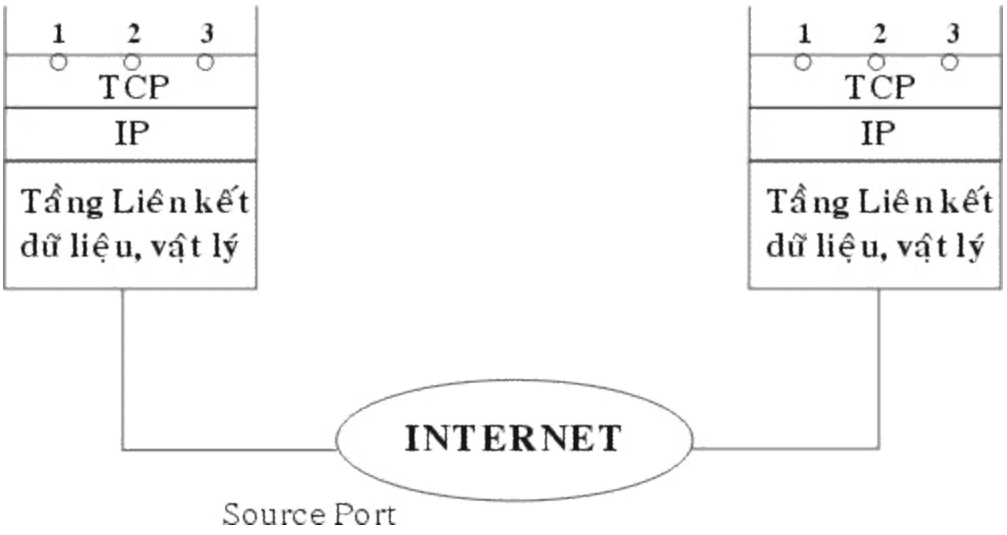
1) Tính checksum. Nếu sai thì loại bỏ gói tin.

2) Tập hợp các đoạn của gói tin (nếu có phân đoạn)

3) Chuyển dữ liệu và các tham số điều khiển lên tầng trên.

II. Giao thức điều khiển truyền dữ liệu TCP

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



Hình 7.5: Cổng truy nhập dịch vụ TCP

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

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

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

Phương thức bị động, người sử dụng yêu cầu TCP chờ đợi một yêu cầu liên kết gửi đến từ xa thông qua một đầu nối TCP/IP (tại chỗ). Người sử dụng dùng hàm passive Open có khai báo cổng TCP và các thông số khác (mức ưu tiên, mức an toàn)

Với phương thức chủ động, người sử dụng yêu cầu TCP mở một liên kết với một một đầu nối TCP/IP ở xa. Liên kết sẽ được xác lập nếu có một hàm Passive Open tương ứng đã được thực hiện tại đầu nối TCP/IP ở xa đó.

Bảng liệt kê một vài cổng TCP phổ biến.

Số hiệu cổng	Mô tả
0	Reserved
5	Remote job entry

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

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

Thông số Open ID được TCP trả lời ngay lập tức để gán cho một liên kết cục bộ (local connection name) cho liên kết được yêu cầu. Thông số này về sau được dùng để tham chiếu tới liên kết đó. (Trong trường hợp nếu TCP không thể thiết lập được liên kết yêu cầu thì nó phải gửi tham số Open Failure để thông báo.)

Khi TCP thiết lập được liên kết yêu cầu nó gửi tham số Open Sucsess được dùng để thông báo liên kết đã được thiết lập thành công. Thông báo này dược chuyển đến trong cả hai trường hợp bị động và chủ động. Sau khi một liên kết được mở, việc truyền dữ liệu trên liên kết có thể được thực hiện.

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

Hàm Send: Dữ liệu được gửi xuống TCP theo các khối (block). Khi nhận được một khối dữ liệu, TCP sẽ lưu trữ trong bộ đệm (buffer). Nếu cờ PUSH được dựng thì toàn bộ dữ liệu trong bộ đệm được gửi, kể cả khối dữ liệu mới đến sẽ được gửi đi. Ngược lại cờ PUSH không được dựng thì dữ liệu được giữ lại trong bộ đệm và sẽ gửi đi khi có cơ hội thích hợp (chẳng hạn chờ thêm dữ liệu nữa để gửi đi với hiệu quả hơn).

Hàm reveive: Ở trạm đích dữ liệu sẽ được TCP lưu trong bộ đệm gắn với mỗi liên kết. Nếu dữ liệu được đánh dấu với một cờ PUSH thì toàn bộ dữ liệu trong bộ đệm (kể cả các dữ liệu được lưu từ trước) sẽ được chuyển lên cho người sữ dụng. Còn nếu dữ liệu đến không được đánh dấu với cờ PUSH thì TCP chờ tới khi thích hợp mới chuyển dữ liệu với mục tiêu tăng hiệu quả hệ thống.

Nói chung việc nhận và giao dữ liệu cho người sử dụng đích của TCP phụ thuộc vào việc cài đặt cụ thể. Trường hợp cần chuyển gấp dữ liệu cho người sử dụng thì có thể dùng cờ URGENT và đánh dấu dữ liệu bằng bit URG để báo cho người sử dụng cần phải sử lý khẩn cấp dữ liệu đó.

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

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

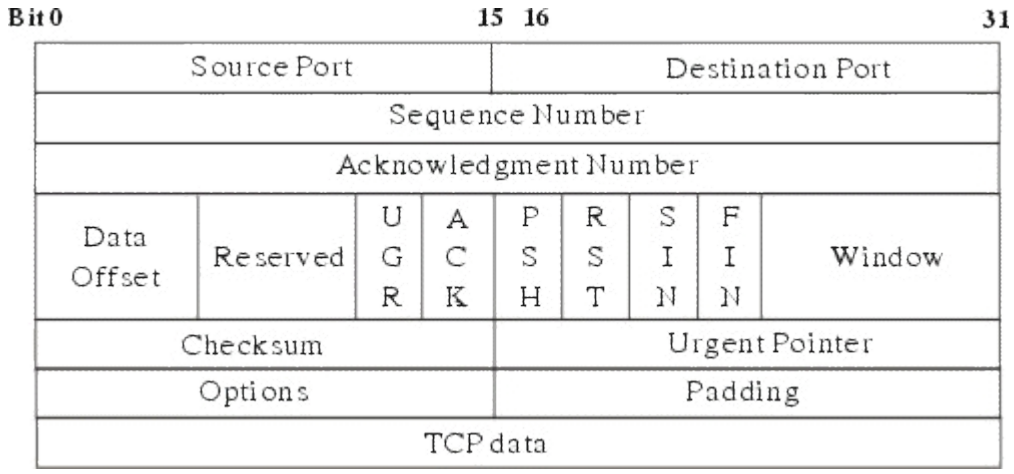
Hàm Abort: Người sử dụng có thể đóng một liên kết bất và sẽ không chấp nhận dữ liệu qua liên kết đó nữa. Do vậy dữ liệu có thể bị mất đi khi đang được truyền đi. TCP báo cho TCP ở xa biết rằng liên kết đã được hủy bỏ và TCP ở xa sẽ thông báo cho người sử dụng cũa mình.

Một số hàm khác của TCP:

Hàm Status: cho phép người sử dụng yêu cầu cho biết trạng thái của một liên kết cụ thể, khi đó TCP cung cấp thông tin cho người sử dụng.

Hàm Error: thông báo cho người sử dụng TCP về các yêu cầu dịch vụ bất hợp lệ liên quan đến một liên kết có tên cho trước hoặc về các lỗi liên quan đến môi trường.

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



Hình 7.5: Dạng thức của segment TCP

Source Por (16 bits): Số hiệu cổng TCP của trạm nguồn.

Destination Port (16 bit): Số hiệu cổng TCP của trạm đích.

Sequence Number (32 bit): số hiệu của byte đầu tiên của segment trừ khi bit SYN được thiết lập. Nếy bit SYN được thiết lập thì Sequence Number là số hiệu tuần tự khởi đầu (ISN) và byte dữ liệu đầu tiên là ISN+1.

Acknowledgment Number (32 bit): số hiệu của segment tiếp theo mà trạm nguồn đang chờ để nhận. Ngầm ý báo nhận tốt (các) segment mà trạm đích đã gửi cho trạm nguồn.

Data offset (4 bit): số lượng bội của 32 bit (32 bit words) trong TCP header (tham số này chỉ ra vị trí bắt đầu của nguồn dữ liệu).

Reserved (6 bit): dành để dùng trong tương lai

Control bit (các bit điều khiển):

URG: Vùng con trỏ khẩn (Ucgent Poiter) có hiệu lực.

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

PSH: Chức năng PUSH.

RST: Khởi động lại (reset) liên kết.

SYN: Đồng bộ hóa số hiệu tuần tự (sequence number).

FIN: Không còn dữ liệu từ trạm nguồn.

Window (16 bit): cấp phát credit để kiểm soát nguồn dữ liệu (cơ chế cửa sổ). Đây chính là số lượng các byte dữ liệu, bắt đầu từ byte được chỉ ra trong vùng ACK number, mà trạm nguồn đã saün sàng để nhận.

Checksum (16 bit): mã kiểm soát lỗi cho toàn bộ segment (header + data)

Urgemt Poiter (16 bit): con trỏ này trỏ tới số hiệu tuần tự của byte đi theo sau dữ liệu khẩn. Vùng này chỉ có hiệu lực khi bit URG được thiết lập.

Options (độ dài thay đổi): khai báo các option của TCP, trong đó có độ dài tối đa của vùng TCP data trong một segment.

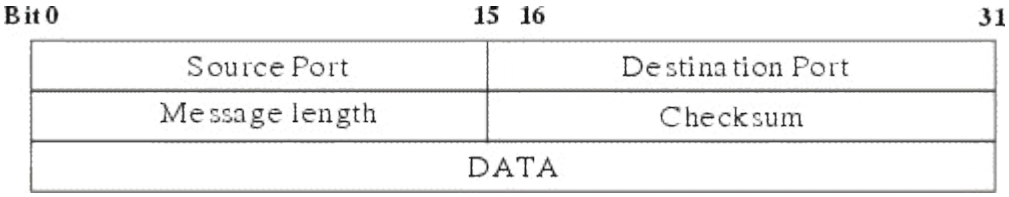
Paddinh (độ dài thay đổi): phần chèn thêm vào header để đảm bảo phần header luôn kết thúc ở một mốc 32 bit. Phần thêm này gồm toàn số 0.

TCP data (độ dài thay đổi): chứa dữ liệu của tầng trên, có độ dài tối đa ngầm định là 536 byte. Giá trị này có thể điều chỉnh bằng cách khai báo trong vùng options.

III. Giao thức UDP (User Datagram Protocol)

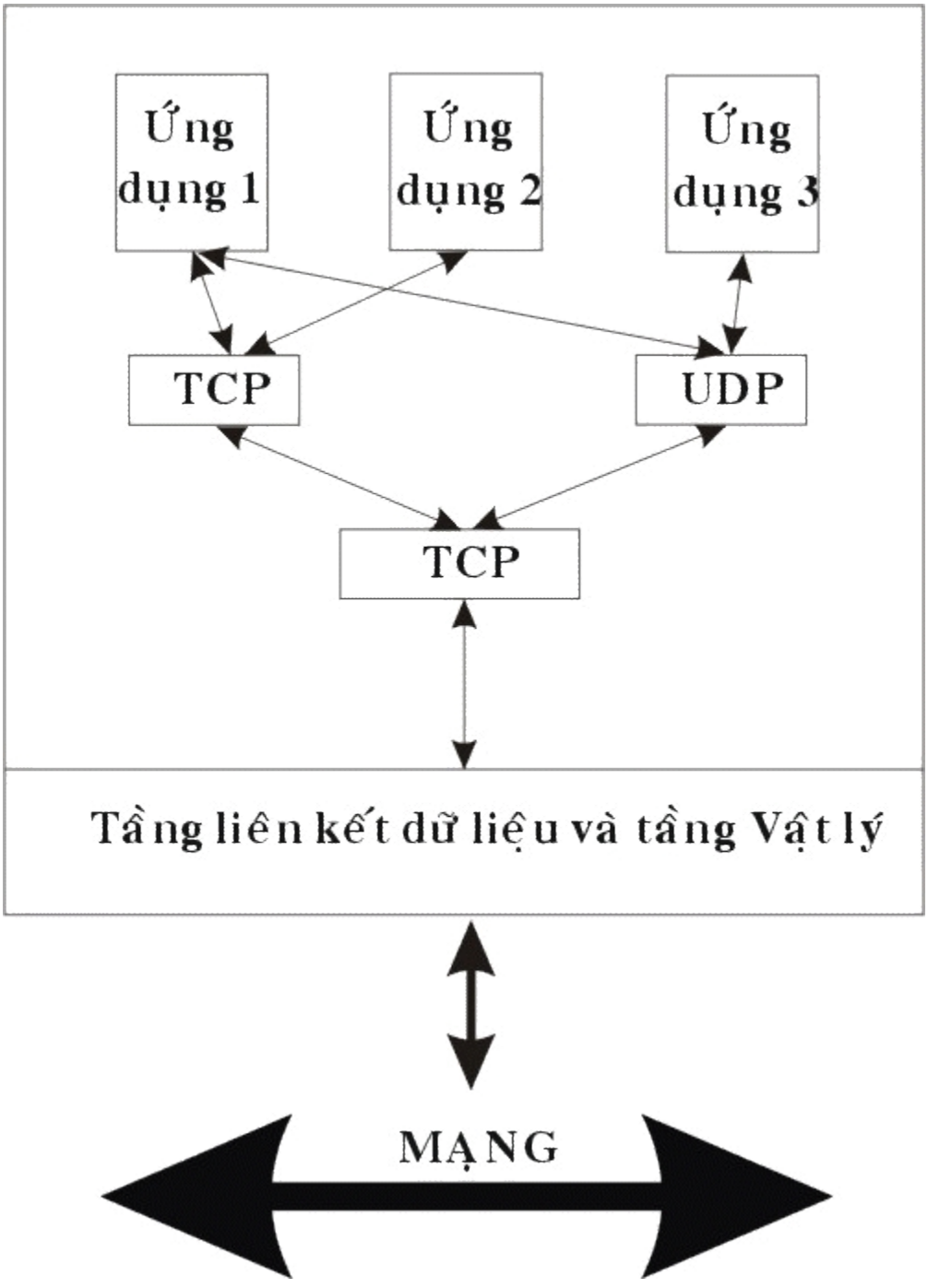
UDP (User Datagram Protocol) là giao thức theo phương thức không liên kết được sử dụng thay thế cho TCP ở trên IP theo yêu cầu của từng ứng dụng. Khác với TCP, UDP không có các chức năng thiết lập và kết thúc liên kết. Tương tự như IP, nó cũng không cung cấp cơ chế báo nhận (acknowledgment), không sắp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

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



Hình 7.7: Dạng thức của gói tin UDP

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


Ứng dụng 1
Ứng dụng 2
Ứng dụng 3
TCP
UDP
TCP
Tầng liên kết dữ liệu và tầng Vật lý
MẠNG

Hình 7.8: Mô hình quan hệ họ giao thức TCP/IP

Chương 8

Các dịch vụ của mạng diện rộng (WAN)

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

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

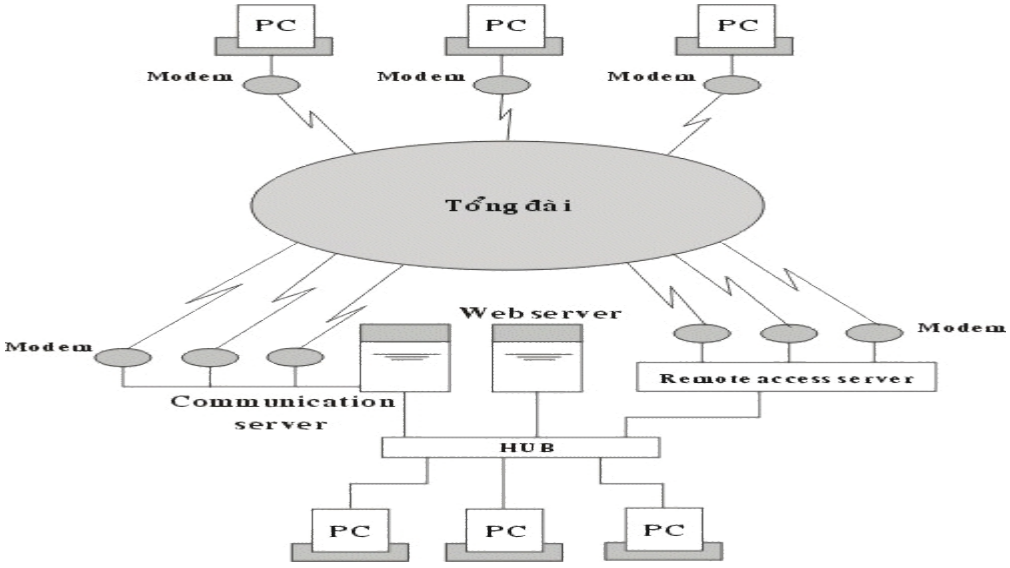
Mạng chuyển mạch (Circuit Swiching Network)

Mạng thuê bao (Leased lines Network)

Mạng chuyển gói tin (Packet Switching Network)

I. Mạng chuyển mạch (Circuit Swiching Network)

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



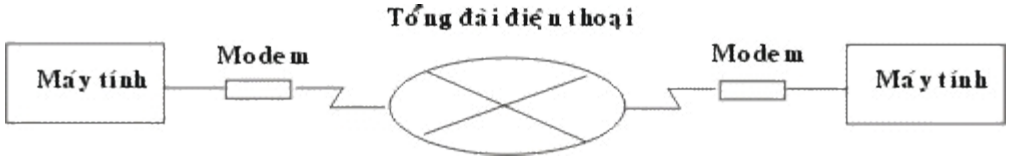
Hình 8.1: Mô hình mạng chuyển mạch

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

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

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

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



Hình 8.2: Mô hình chuyển mạch tương tự

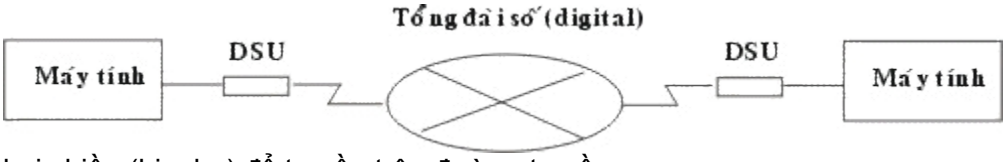
Khi sử dụng đường truyền điện thoại để truyền số liệu thì các chuẩn của modem và các tính chất của nó sẽ quyết định tốc độ của đường truyền. Cùng với các kỹ thuật chuyển đổi tín hiệu các tính năng mới như nén tín hiệu cho phép nâng tốc độ truyền dữ liệu lên rất cao.

Loại	Tốc độ (bps)	Loại nén	Tốc độ thực tế (bps)
Bell 212A	1200		
CCITT V22	1200		
CCITT V22 bis	2400	MNP Class 5	2400 - 3600
CCITT V32	9600	MNP Class 5, V42 bis	9600 - 19200
CCITT V32 bis	14400	MNP Class 5, V42 bis	14400 - 33600

Hình 8.3: Bảng kỹ thuật modem

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

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



hai chiều (bipolar) để truyền trên đường truyền.

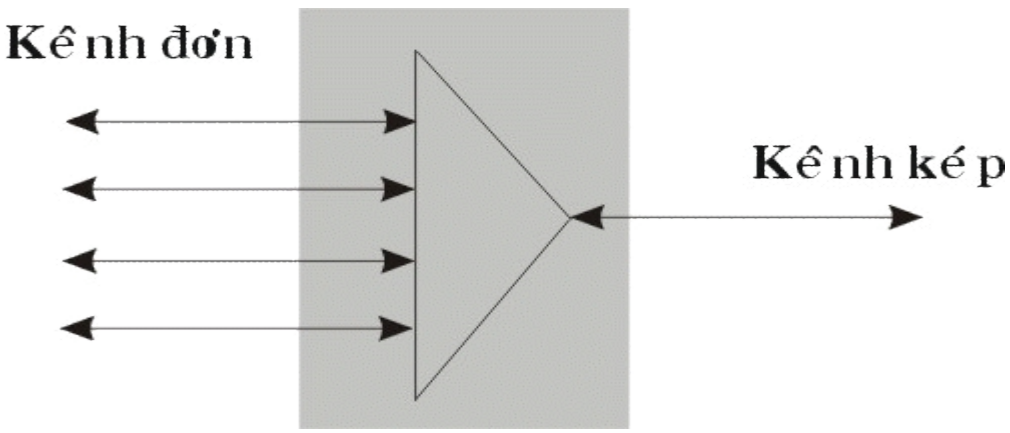
Hình 8.3: Mô hình chuyển mạch số

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

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

II. Mạng thuê bao (Leased line Network)

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



mạng người ta đưa ra một kỹ thuật gọi là ghép kênh.

Hình 8.4: Mô hình ghép kênh

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

Có hai phương thức ghép kênh chính là ghép kênh theo tần số và ghép kênh theo thời gian, hai phương thức này tương ứng với mạng thuê bao tuần tự và mạng thuê bao kỹ thuật số. trong thời gian hiện nay mạng thuê bao kỹ thuật số sử dụng kỹ thuật ghép kênh theo thời gian với đường truyền T đang được sử dụng ngày một rộng rãi và dần dần thay thế mạng thuê bao tuần tự.

1. Phương thức ghép kênh theo tần số

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

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

2.Phương thức ghép kênh theo thời gian:

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

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

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

III. Mạng chuyển gói tin (Packet Switching NetWork)

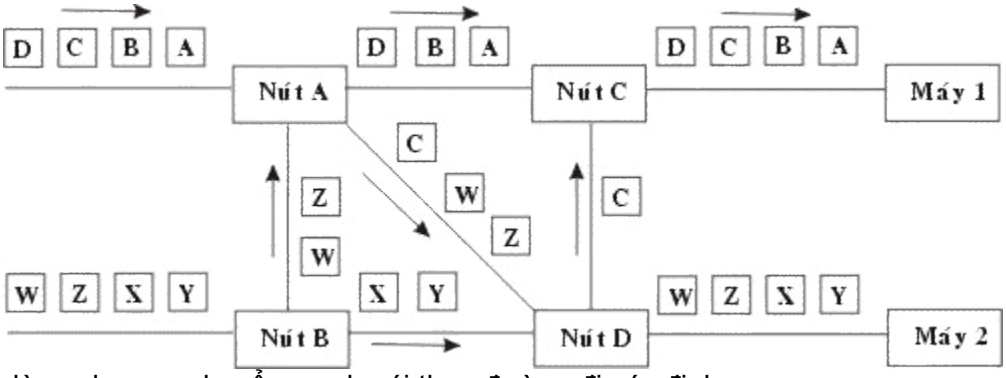
Mạng chuyển mạch gói hoạt động theo nguyên tắc sau : Khi một trạm trên mạng cần gửi dữ liệu nó cần phải đóng dữ liệu thành từng gói tin, các gói tin đó được đi trên mạng từ nút này tới nút khác tới khi đến được đích. Do việc sử dụng kỹ thuật trên nên khi một trạm không gửi tin thì mọi tài nguyên của mạng sẽ dành cho các trạm khác, do vậy mạng tiết kiệm được các tài nguyên và có thể sử dụng chúng một cách tốt nhất.

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

Phương thức chuyển mạch gói theo sơ đồ rời rạc.

Phương thức chuyển mạch gói theo đường đi xác định.

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

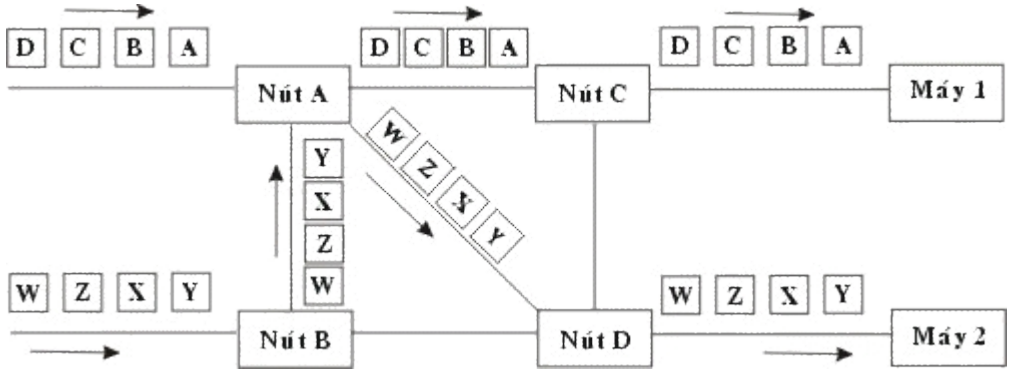


Hình 8.5: Ví dụ phương thức sơ đồ rời rạc.

Phương thức chuyển mạch gói theo đường đi xác định:

Trước khi truyền dữ liệu một đường đi (hay còn gọi là đường đi ảo) được thiết lập giữa trạm gửi và trạm nhận thông qua các nút của mạng. Đường đi trên mang số hiệu phân biệt với các đường đi khác, sau đó các gói tin được gửi đi theo đường đã thiết lập để tới đích, các gói

tin mang số hiệu củ đường ảo để có thể được nhận biết khi qua các nút. Điều này khiến cho việc tính toán đường đi cho phiên liên lạc chỉ cần thực hiện một lần.



Hình 8.6: Ví dụ phương thức đường đi xác định

1. Mạng X25

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

X25 cung cấp quy trình kiểm soát luồng giữa các đầu cuối đem lại chất lương đường truyền cao cho dù chất lương đương dây truyền không cao.

X25 được thiết kế cho cả truyền thông chuyển mạch lẫn truyền thông kiểu điểm nối điểm.

Được quan tâm và tham gia nhanh chóng trên toàn cầu.

Trong X25 có chức năng dồn kênh (multiplexing) đối với liên kết logic (virtual circuits) chỉ làm nhiệm vụ kiểm soát lỗi cho các frame đi qua. Điều này làm tăng độ phức tạp trong việc phối hợp các thủ tục giữa hai tầng kề nhau, dẫn đến thông lượng bị hạn chế do tổng phí xử lý mỗi gói tin tăng lên. X25 kiểm tra lỗi tại mỗi nút trước khi truyền tiếp, điều này làm cho đường truyền

chó chất lượng rất cao gần như phi lỗi. Tuy nhiên do vậy khối lượng tích toán tại mỗi nút khá lớn, đối với những đường truyền của những năm 1970 thì điều đó là cần thiết nhưng hiện nay khi kỹ thuật truyền dẫn đã đạt được những tiến bộ rất cao thì việc đó trở nên lãng phí

2. Mạng Frame Relay

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

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

3. Mạng ATM (Cell relay)

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

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

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

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

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

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

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

Nhận thức được vị trí chưa thể thay thế được (ít nhất cho đến những năm đầu của thế kỷ 21) của kỹ thuật ATM, hầu hết các hãng khổng lồ về máy tính và truyền thông như IBM, ATT, Digital, Hewlett - Packard, Cisco Systems, Cabletron, Bay Network,... đều đang quan tâm đặc biệt đến dòng sản phẩm hướng đến ATM của mình để tung ra thị trường. Có thể kể ra đây một số sản phẩm đó như DEC 900 Multiwitch, IBM 8250 hub, Cisco 7000 rounter, Cablectron, ATM module for MMAC hub.

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

Chương 9

Ví dụ một số mạng LAN và WAN

Hiện nay trên thế giới có rất nhiều mạng máy tính, chúng được sử dụng để phục vụ cho nhiều lĩnh vực khác nhau như nghiên cứu khoa học, truyền dữ liệu, kinh doanh. Vì vậy nên các mạng này cũng rất đa dạng về chủng loại. Trong phần này ta xem xét một số mạng LAN và WAN thông dụng.

I. Mạng Novell NetWare

Được đưa ra bởi hãng Novell từ những năm 80 và đã được sử dụng nhiều trong các mạng cục bộ với số lượng ước tính hiện nay vào khoảng 50 -60%. Hệ điều hành mạng Novell NetWare là một hệ điều hành có độ an toàn cao đặc biệt là với các mạng có nhiều người sử dụng. Hệ điều hành mạng Netware khá phức tạp để lắp đặt và quản lý nhưng nó là một hệ điều hành mạng đang được dùng phổ biến nhất hiện nay. Hệ điều hành mạng Novell NetWare được thiết kế như một hệ thống mạng *client-server* trong đó các máy tính được chia thành hai loại:

Những máy têêính cung cấp tài nguyên cho mạng gọi là *server* hay còn gọi là máy chủ mạng.

Máy sử dụng tài nguyên mạng gọi là *clients* hay còn gọi là trạm làm việc.

Các server (File server) của Netware không chạy DOS mà bản thân Netware là một hệ điều hành cho server điều đó đã giải phóng Netware ra khỏi những hạn chế của DOS. Server của Netware dùng một cấu trúc hiệu quả hơn DOS để tổ chức các tập tin và thư mục, với Netware, chúng ta có thể chia mỗi ổ đĩa thành một hoặc nhiều tập đĩa (volumes), tương tự như các ổ đĩa logic của DOS. Các tập đĩa của Novell có tên chứ không phải là chữ cái. Tuy nhiên,

để truy cập một tập đĩa của Netware từ một trạm làm việc chạy DOS, một chữ cái được gán cho tập đĩa.

Với các hệ điều hành Netware 3.x và 4.x các server phải được dành riêng, trong đó chúng ta không thể dùng một file server làm thêm việc cùa Workstation, tuy điều đó tốn kém hơn vì phải mua một máy tính để làm server nhưng nó có hiệu quả hơn vì máy tính server có thể tập trung để phục vụ mạng. Còn với Netware 2.x thì có thể lưa chọn trong đó một file server có thể làm việc như một Workstation như hai tiến trình Server và Workstation tách tời nhau hoàn toàn.

Các trạm làm việc trên một mạng Netware có thể là các máy tính DOS, chạy OS/2 hoặc các máy Macintosh. Nếu mạng vừa có máy PC và Macintosh thì Netware có thể là sự lựa chọn tốt.

Tất cả các phiên bản của Netware đều có đặc trưng được gọi là tính chịu đựng sai hỏng của hệ (System Fault Tolerance SFT) được thiết kế để giữ cho mạng vẫn chạy ngay cả khi phần cứng có sai hỏng.

NetWare là một hệ điều hành nhưng không phải là một hệ điều hành đa năng mà tập trung chủ yếu cho các ứng dụng truy xuất tài nguyên trên mạng, nó có một tập hợp xác định saün các dịch vụ dành cho người sử dụng. Tại đây Novell NetWare có một hệ thống các yêu cầu và trả lời mà Client và Server đều hiểu, nó bao gồm:

Nhóm chương trình trên máy người dùng: Hệ điều hành trạm, các giao diện cho phép nhười sử dụng chi xuất các tài nguyên của mạng như là các tài nguyên của máy cục bộ, chương trình truyền số liệu qua mạng.

Hệ điều hành trên máy máy chủ: Chương trình thực hiên từ DOS, Lưu các thông số của DOS, chuyển CPU của server qua chế độ protectied mode, quản lý việc sử dụng tài nguyên của mạng cho người sử dụng.

Các tiện ích trên mạng: dành cho người sử dụng và người quản trị mạng.

Novell NetWare hỗ trợ các giao thức cơ bản sau:

Giao thức truy xuất (Access Protocol) (Ethernet, Token Ring, ARCnet, ProNET-10, FDDI)

Giao thức trao đổi gói tin trên mạng (Internet Packet Exchange -IPX)

Giao thức thông tin tìm đường (Routing Information Protocol - RIP)

Giao thức thông báo dịch vụ (Sevice Advertising Protocol - SAP)

Giao thức nhân NetWare (NetWare Core Protocol - NCP) cho phép người dùng truy xuất vào file server

Do nhu cầu cần thích nghi với nhiều kiểu mạng và để dễ dàng nâng cấp và quản lý, Novell NetWare cũng được chia thành nhiều tầng giao thức tương tự cấu trúc 7 tầng cuả hệ thống mở OSI.

<table>
<tr><td>Tầng ứng dụng
(Application)</td><td rowspan="2">Giao thức
thông báo dịch vụ
(Service advertising
protocol - SAP)</td><td rowspan="2">Giao thức thông
tin tìm đường
(Routing Information
Protocol - RIP)</td><td rowspan="2">Giao thức
nhân NetWare
(NetWare core
protocol - NCP)</td></tr>
<tr><td>Tầng trình bày
(Presentation)</td></tr>
<tr><td>Tầng giao dịch
(Session)</td><td colspan="3">Hệ thống nhập xuất cơ bản trên mạng
(NetBIOS)</td></tr>
<tr><td>Tầng vận chuyển
(Transport)</td><td colspan="3">Trao đổi gói tin tuần tự
(Sequence Packet eXchange - SPX)</td></tr>
<tr><td>Tầng mạng
(Network)</td><td colspan="3">Trao đổi gói tin liên mạng
(Internet Packet Exchange - IPX)</td></tr>
<tr><td>Tầng liên kết dữ liệu
(Data link)</td><td colspan="3">Giao thức truy xuất và kỹ thuật mạng lưới
(Access protocol and wiring techniques)
(Chuẩn giao tiếp liên kết dữ liệu mở ODI)</td></tr>
<tr><td>Tầng vật lý
(Physical)</td><td colspan="3">Ethernet, Token Ring, ARCnet
cáp đồng trục, cáp trần xoắn cặp
(IEEE 802.X hoặc FDDI)</td></tr>
</table>

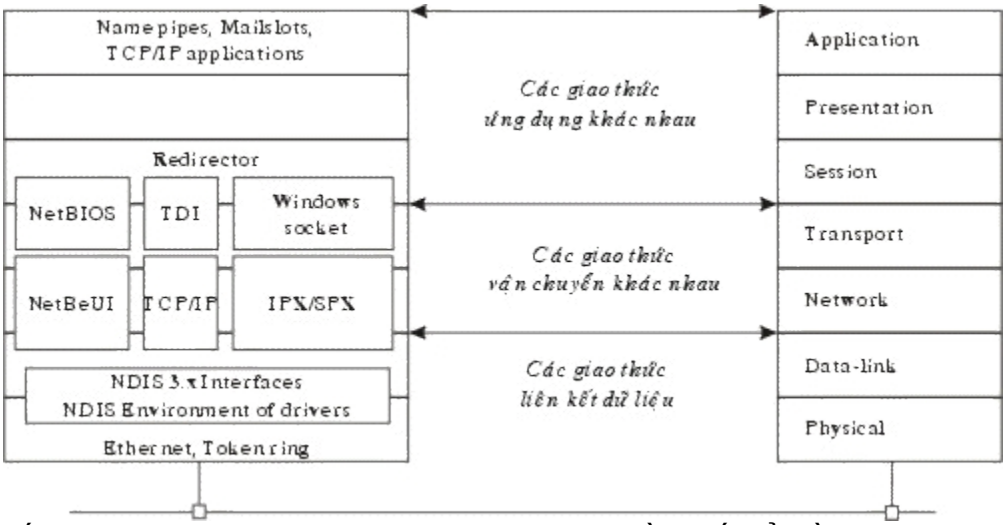
Hình 9.1: Cấu trúc của Hệ điều hành Novell NetWare

II. Mạng Windows NT

Mạng dùng hệ điều hành **Windows NT** được đưa ra bởi hãng Microsoft với phiên bản mới nhất hiện nay là Windows NT 5.0, cụm từ windows NT được hiểu là công nghệ mạng trong môi trường Windows (Windows Network Technology). Hiện mạng Windows NT đang được đánh giá cao và được đua vào sử dụng ngày một nhiều. Windows NT là một hệ điều hành đa

nhiệm, đa xử lý với địa chỉ 32 bit bộ nhớ. Ngoài việc yểm trơ các ứng dụng DOS, Windows 3.x, Win32 GUI và các ứng dụng dựa trên ký tự, Windows NT còn bao gồm các thành phần mạng, cơ chế an toàn, các công cụ quản trị có khả năng mạng diện rộng, các phần mềm truy cập từ xa. Windows NT cho phép kết nối với máy tính lớn, mini và máy Mac.

Hệ điều hành mạng Windows NT có thể chay trên máy có một CPU cũng như nhiều CPU. Hệ điều hành mạng còn có đưa vào kỹ thuật gương đĩa qua đó sử dụng tốt hệ thống nhiều đĩa nâng cao năng lực hoạt động. Hệ điều hành mạng Windows NT đảm bảo tránh được những người không được phép vào trong hệ thống hoặc thâm nhập vào các file và chương trình trên đĩa cứng. Hệ điều hành mạng Windows NT cung cấp các công cụ để thiết lập các lớp quyền dành cho nhiều nhiệm vụ khác nhau làm cho phép xây dựng hệ thống an toàn một cách mềm dẻo. Windows NT được thiết kế dành cho giải pháp nhóm (Workgroup) khi bạn muốn có kiểm soát nhiều hơn đối với mạng ngang hàng (như Windows For Workgroup, LANtastic hay Novell lite). Ngoài ra chức năng mới của Windows NT server là mô hình vùng (Domain) được thiết lập cho các mạng lớn với khả năng kết nối các mạng toàn xí nghiệp hay liên kết các kết



nối mạng với các mạng khác và những công cụ cần thiết để điều hành.

Hình 9.2: Cấu trúc của Hệ điều hành Windows NT

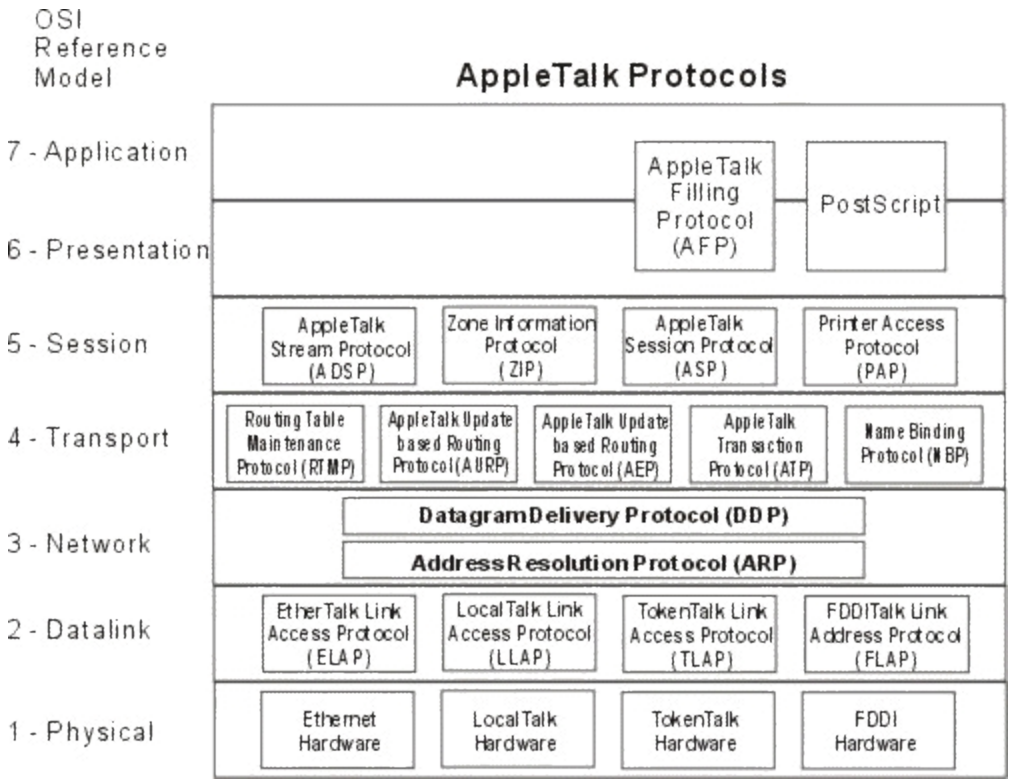
III. Mạng Apple talk

Vào đầu những năm 1980, khi công ty máy tính Apple chuẩn bị giới thiệu máy tính Macintosh, các kỹ sư Apple đã thấy rằng mạng sẽ trở nên rất cần thiết. Họ muốn rằng mạng MAC cũng là một bước tiến mơí trong cuộc cách mạng về giao diện thân thiện người dùng do

Apple khởi xướng. Với ý định như vậy, Apple xây dựng một giao thức mạng cho họ máy Macintosh, và tích hợp giao thức trên vào máy tính để bàn. Cấu trúc mạng mới do Apple xây dựng được gọi là Apple Talk.

Mặc dù Apple Talk là giao thức mạng độc quyền của Apple, nhưng Apple cũng đã ấn hành nhiều tài liệu về Apple Talk trong cố gắng khuyến khích các nhà sản xuất phần mềm khác phát triển trên Apple Talk. Ngày nay đã có nhiều sản phẩm thương mại trên nền Apple Talk như của Novell, Microsoft.

Ban đầu **AppleTalk** chỉ cài đặt trên hệ thống cáp riêng của hãng là LocalTalk và có phạm vi ứng dụng rất hạn chế. Phiên bản đầu của Apple Talk được thiết kế cho nhóm người dùng cục bộ hay được gọi là *Apple Talk phase 1*. Sau khi tung ra thị trường 5 năm, số người dùng đã vượt quá 1,5 triệu người cài đặt, Apple nhận thấy những nhóm người dùng lớn đã vượt quá giới hạn của *Apple Talk phase 1*, nên họ đã nâng cấp giao thức. Giao thức đã được cải tiến được biết dưới cái tên *Apple Talk phase 2,* cải tiến khả năng tìm đường của Apple Talk và cho phép Apple Talk chạy trên những mạng lớn hơn.



Hình 9.3: Cấu trúc của Hệ điều hành Appletalk

Hãng Apple thiết kế Apple Talk độc lập với tầng liên kết dữ liệu. Apple hỗ trợ nhiều loại cài đặt của tầng liên kết dữ liệu, bao gồm *Ethernet, Token Ring, Fiber Distributed Data Interface* (FDDI), và *Local Talk*. Trên Apple Talk, Apple xem Ethernet như *ethertalk*, Token Ring như *tokentalk*, và FDDI như *fddittalk*.

Các giao thức chính của mạng AppleTalk:

LLAP *(Local Talk Link Access)* là giao thức do Apple phát triển để hoạt động với cáp riêng của hãng (cũng được gọi là LocalTalk**)** dựa trên cáp xoắn đôi bọc kim (STP), thích hợp với các mạng nhỏ, hiệu năng thấp. Tốc độ tối đa là 230,4 Kb/s và khoảng cách các đoạn cáp có độ dài giới hạn là 300m, số lượng trạm tối đa là 32.

ELAP *(Ethertalk Link Access)* và *TLAP (tokentalk Link Access)* là các giao thức cho phép sử dụng các mạng vật lý tương ứng là Ethernet và Token Ring.

AARP *(AppleTalk Addresss Resolution Protocol)* là các giao thức cho phép ánh xạ giữa các địa chỉ vật lý của Ethernet và Token Ring, là giao diện giữa các tầng cao của AppleTalk với các tầng vật lý của Ethernet và Token Ring.

DDP *(Datagram Delivery Protocol)* là giao thức tầng Mạng cung cấp dịch vụ theo phương thức không liên kết giữa 2 sockets (để chỉ 1 địa chỉ dịch vụ; một tổ hợp của địa chỉ thiết bị, địa chỉ mạng và socket sẽ định danh 1 cách duy nhất cho môãi tiến trình). DDP thực hiện chức năng chọn đường (routing) dựa trên các bảng chọn đường cho RTMP bảo trì.

RTMP *(Routing Table Maintenance protocol)* cung cấp cho DDP thông tin chọn đường trên phương pháp vector khoảng cách tương tự như RIP (Routing Information Protocol) dùng trong Netware IPX/SPX.

NBP *(Naming Binding Protocol)*: cho phép định danh các thiết bị bởi các tên lôgic (ngoài địa chỉ của chúng). Các tên này ẩn dấu địa chỉ tầng thấp đối với người sử dụng và đối với các tầng cao hơn.

ATP *(AppleTalk Transaction Protocol)* là giao thức thức tầng vận chuyển hoạt động với phương thức không liên kết. Dich vụ vận chuyển này được cung cấp thông qua một hệ thống các thông báo nhận và truyền lại. Độ tin cậy cũa ATP dưạ trên các thao tác (transaction) (một thao tác bao gồm một cặp các thao tác hỏi-đáp).

ASP *(AppleTalk Section Protocol)* là giao thức tầng giao dịch của AppleTalk, cho phép thiết lập, duy trì và hủy bỏ các phiên liên lạc giữa người yêu cầu dịch vụ và người cung cấp dịch vụ.

ADSP *(AppleTalk Data Stream Protocol)* là một giao thức phủ cả tầng vận chuyển và tầng giao dịch, có thể thay cho nhóm giao thức dùng với ATP.

ZIP *(Zone Information Protocol)* là giao thức có chức năng tổ chức các thiết bị thành các vùng (zone) để làm giảm độ phức tạp của 1 mạng bằng cách giới hạn sự tương tác của người sử dụng vào đúng các thiết bị mà anh ta cần.

PAP *(Printer Access protocol)* cũng là 1 giao thức của tầng giao dịch tương tự như ASP. Nó không chỉ cung cấp các dịch vụ in như tên gọi mà còn yểm trợ các kiểu liên kết giữa người yêu cầu và ngươi cung cấp dịch vụ.

AFP *(AppleTalk Filling Protocol)* là giao thức cung cấp dịch vụ File và đảm nhận việc chuyển đổi cú pháp dữ liệu, bảo vệ an toàn dữ liệu (tương tự tầng trình bày trong mô hình OSI).

IV. Mạng Arpanet

Đây là mạng được thiết lập tại Mỹ vào giữa những năm 60 khi bộ quốc phòng Mỹ muốn có một mạng dùng để ra lệnh và kiểm soát mà có khả năng sống còn cao trong trường hợp có chiến tranh hạt nhân. Những mạng sử dụng đường điện thoại thông thường vào lúc đó tỏ ra không đủ an toàn khi mà một đường dây hay một tổng đài bị phá hủy cũng có thể dẫn đến mọi

cuộc nói chuyện hay liên lạc thông qua nó bị gián đoạn, việc đó còn đôi khi dẫn đến cắt rời liên lạc.

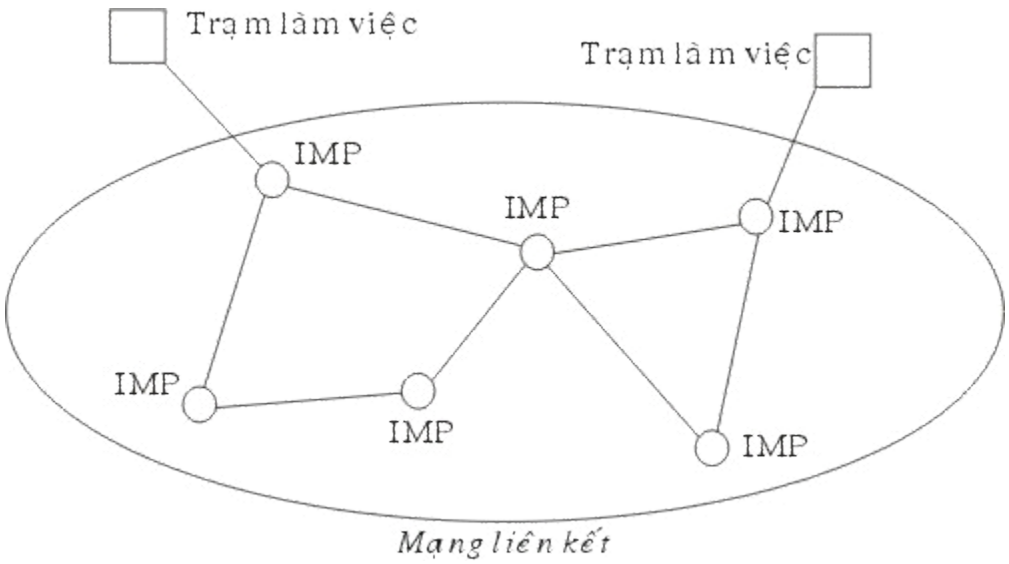
Để làm được điều này khi bộ quốc phòng Mỹ đưa ra chương trình ARPA (Advanced Research Projects Agency) với sự tham gia của nhiều trường đại học và công ty dưới sự quản lý của khi bộ quốc phòng Mỹ.

Vào đầu những năm 1960 những ý tưởng chủ yếu của chuyển mạch gói đã được Paul Baran công bố và sau khi tham khảo nhiều chuyên gia thì chương trình ARPA quyết định mạng tương lai của khi bộ quốc phòng Mỹ sẽ là mạng chuyển mạch gói và nó bao gồm một mạng liên kết và các trạm (host). Mạng liên kết bao gồm các máy tính dùng để liên kết các đường truyền dữ liệu được gọi là các điểm trung chuyển thôâng tin (IMP - Interface Message Processor).

Một IMP sẽ được liên kết với ít nhất là hai IMP khác với độ an toàn cao, các thông tin được chuyển trên mạng liên kết dưới dạng các gói dữ liệu tách rời, có nghĩa là khi có một số đường và nút bị phá hủy thì các gói tin tự động được chuyển theo những đường khác. Mỗi nút một máy tính của hệ thống bao gồm một trạm có được kết nối với một IMP trên mạng, nó gửi thông tin của mình đến IMP để rồi sau đó IMP sẽ phân gói, rồi lần lượt gửi các gói tin theo những đường mà nó lựa chọn để đến đích.

Tháng 10 năm 1968 ARPA quyết định lựa chọn hãng BBN một hãng tư vấn tại Cambridge, Massachsetts làm tổng thầu. Lúc đó BBN đã lựa chon máy DDP-316 làm IMP, các IMP được nối với đường thuê bao 56 Kbps từ các công ty điện thoại. Phần mềm được chia làm hai phần: phần liên kết mạng và phần cho nút, với phần mềm cho liên kết mạng bao gồm phần mềm tại các IMP đầu cuối và các IMP trung gian, các giao thức liên kết IMP với khả năng đảm bảo an toàn cao.

Phần mềm tại nút bao gồm phần mềm danh cho việc liên kết giữa nút với IMP, các giao thức giữa các nút với nhau trong quá trình truyền dữ liệu.



Hình 9.4: Cấu trúc ban đầu của mạng ARPANET

Vào tháng 10 năm 1969 mạng ARPANET bắt đầu được đưa vào hoạt động thử nghiệm với 4 nút là những trường đại học và trung tâm nghiên cứu tham gia chính vào dự án, mạng phát triển rất nhanh đến tháng 3 năm 1971 đã có 15 nút và tháng 9 năm 1972 đã có tới 35 nút. Các cải tiến tiếp theo cho phép nhiều trạm có thể liên kết với một IMP do vậy sẽ tiết kiệm tài nguyên và một trạm có thể liên kết với nhiều IMP nhằm tránh việc IMP hư hỏng làm gián đoạn liên lạc.

Cùng với việc phát triển các nút ARPA cũng dành ngân khoản cho phát triển các mạng truyền dữ liệu dùng kỹ thuật vệ tinh và dùng kỹ thuật radio. Điều đó cho phép thiết lập các nút tại những điểm các khoảng cách rất xa. Về các giao thức truyền thông thì sau khi thấy rằng các giao thức của mình không chạy được trên nhiều liên kết mạng vào năm 1974 ARPA đã đầu tư nghiên cứu hệ giao thức TCP/IP và dựa trên hợp đồng giữa BBN và Trường đại học tổng hợp Berkeley - California các nhà nghiên cứu của trường đại học đã viết rất nhiều phần mềm, chương trình quản trị trên cơ ở hệ điều hành UNIX. Dựa trên các phần mềm mới về truyền thông trên cơ sở TCP/IP đã cho phép dễ dành liên kết các mạng LAN vào mạng ARPANET. Vào năm 1983 khi mạng đã hoạt động ổn định thì phần quốc phòng của mạng (gồm khoảng 160 IMP với 110 IMP tại nước Mỹ và 50 IMP ở nước ngoài, hàng trăm nút) được tách ra thành mạng MILNETvà phần còn lại vẫn tiếp tục hoạt động như là một mạng nghiên cứu.

Trong những năm 1980 khi có nhiều mạng LAN được nối vào ARPANET để giảm việc tìm kiếm địa chỉ trên mạng người ta chia vùng các máy tính đưa tên các máy vào địa chỉ IP và xây dựng hệ quản trị cơ sở phân tán các tên các trạm của mạng Hệ cơ sở dữ liệu đó gọi là DNS (Domain Naming System) trong đó có chức mọi thông tin liên quan đến tên các trạm.

Vào năm 1990 với sự phát triển của nhiều mạng khác mà ARPANET là khởi xướng thì ARPANET đã kết thúc hoạt động của mình, tuy nhiên MILNET vẫn hoạt động cho đến ngày nay.

V. Mạng NFSNET

Vào cuối những năm 1970 khi Quỹ khoa học quốc gia Hoa kỳ (NFS - The U.S. National Science Foundation) thấy được sự thu hút của ARPANET trong nghiên cứu khoa học mà qua đó các nhà khoa học có thể chia sẻ thông tin hay cùng nhau nghiên cứu các đề án. Tuy nhiên việc sử dụng ARPANET cần thông qua bộ quốc phòng Mỹ với nhiều hạn chế và nhiều cơ sở nghiên cứu khoa học không có khả năng đó. Điều đó khiến NFS thiết lập một mạng ảo có tên là CSNET trong đó sử dụng các máy tính tại công ty BBN cho phép các nhà nghiên cứu có thể kết nối vào để tiếp tục nối với mạng ARPANET hay gửi thư điện tử cho nhau. Vào năm 1984 NFS bắt đầu nghiên cứu tới việc thiết lập một mạng tốc độ cao dành cho các nhóm nghiên cứu khoa học nhằm thay thế mạng ARPANET, bước đầu NFS quyết định xây dựng được đường trục truyền số liệu nối 6 máy tính lớn (Supercomputer) tại 6 trung tâm máy tính. Tại mỗi trung tâm máy tính lớn tại đây được nối với một máy mini loại LSI-11 và các máy mini được nối với nhau bằng đường thuê bao 56 Kbps tương tự như kỹ thuật đã sử dụng ở mạng ARPANET. Đồng thời NFS cũng cung cấp ngân khoản cho khoảng 20 mạng vùng để liên kết với các máy tính lớn trên và qua đó tới các máy tính lớn khác. Toàn bộ mạng bao gồm mạng trục và các mạng vùng được gọi là NFSNET, mạng NFS có được kết nối với mạng ARPANET.

Mạng NFS được phát triển rất nhanh, sau một thời gian hoạt động đường trục chính được thay thế bằng đường cáp quang 448 Kbps và các máy IBM RS6000 được sử dụng làm công việc kết nối. Đến năm 1990 đường trục đã được nâng lên đến 1.5 Mbps.

Với việc phát triển rất nhanh và NFS thấy rằng chính quyền không có khả năng tiếp tục tài trợ nhưng do các công ty kinh doanh không thể sử dụng mạng NFSNET (do bin cấm theo luật) nên NFS yểm trợ các công ty MERIT, MCI, IBM thành lập một công ty không sinh lợi (nonprofit corporation) có tên là ANS (Advanced Networks and Services) nhằm phát triển việc kinh doanh hóa mạng. ASN tiếp nhận mạng NFSNET và bắt đầu nâng cấp đường trục lên từ 1.5 Mbps lên 45 Mbps để thành lập mạng ANSNET.

Vào năm 1995 khi các công ty cung cấp dịch vụ liên kết phát triển khắp nơi thì mạng trục ANSNET không còn cần thiết nữa và ANSNET được bán cho công ty America Online. Hiện

nay các mạng vùng của NFS mua các dịch vụ truyền dữ liệu để liên kết với nhau, mạng NFS đang sử dụng dịch vụ của 4 mạng truyền dữ liệu là PacBell, Ameritech, MFS, Sprint mà qua đó các mạng vùng NFS có thể lựa chọn để kết nối với nhau.

VI. Mạng Internet

Cùng với sự phát triển của NFSNET và ARPANET nhất là khi giao thức TCP/IP đã trở thành giao thức chính thước duy nhất trên các mạng trên thì số lượng các mạng, nút muốn tham gia kết nối vào hai mạng trên đã tăng lên rất nhanh. Rất nhiều các mạng vùng được kết nối với nhau và còn liên kết với các mạng ở Canada, châu Âu.

Vào khoảng giữa những năm 1980 người ta bắt đầu thấy được sự hình thành của một hệ thống liên mạng lớn mà sau này được gọi là Internet. Sự phát triển của Internet được tính theo cấp số nhân, nếu như năm 1990 có khoảng 200.000 máy tính với 3.000 mạng con thì năm 1992 đã có khoảng 1.000.000 máy tính được kết nối, đến năm 1995 đã có hàng trăm mạng cấp vùng, chục ngàn mạng con và nhiều triệu máy tính. Rất nhiều mạng lớn đang hoạt động cũng đã được kết nối vào Internet như các mạng SPAN, NASA network, HEPNET, BITNET, IBM network, EARN. Việc liên kết các mạng được thực hiện thông qua rất nhiều đường nối có tốc độ rất cao.

Hiện nay một máy tính được gọi là thành viên của Internet nếu máy tính đó có giao thức truyền dữ liệu TCP/IP, có một địa chỉ IP trên mạng và nó có thể gửi các gói tin IP đến tất cả các máy tính khác trên mạng Internet.

Tuy nhiên trong nhiều trường hợp thông qua một nhà cung cấp dịch vụ Internet người sử dụng kết nối máy của mình với máy chủ của nhà phục vụ và được cung cấp một địa chỉ tạm thời trước khi khai thác các tài nguyên của Internet. Máy tính của người đó có thể gửi các gói tin cho các máy khác bằng địa chỉ tạm thời đó và địa chỉ đó sẽ trả lại cho nhà cung cấp khi kết thúc liên lạc. Vì máy tính của người đó sử dụng trong thời gian liên kết với Internet cũng có một địa chỉ IP nên người ta vẫn coi máy tính đó là thành viên của Internet.

Vào năm 1992 cộng đồng Internet đã ra đời nhằm thúc đẩy sự phát triển của Internet và điều hành nó. Hiện nay Internet có 5 dịch vụ chính:

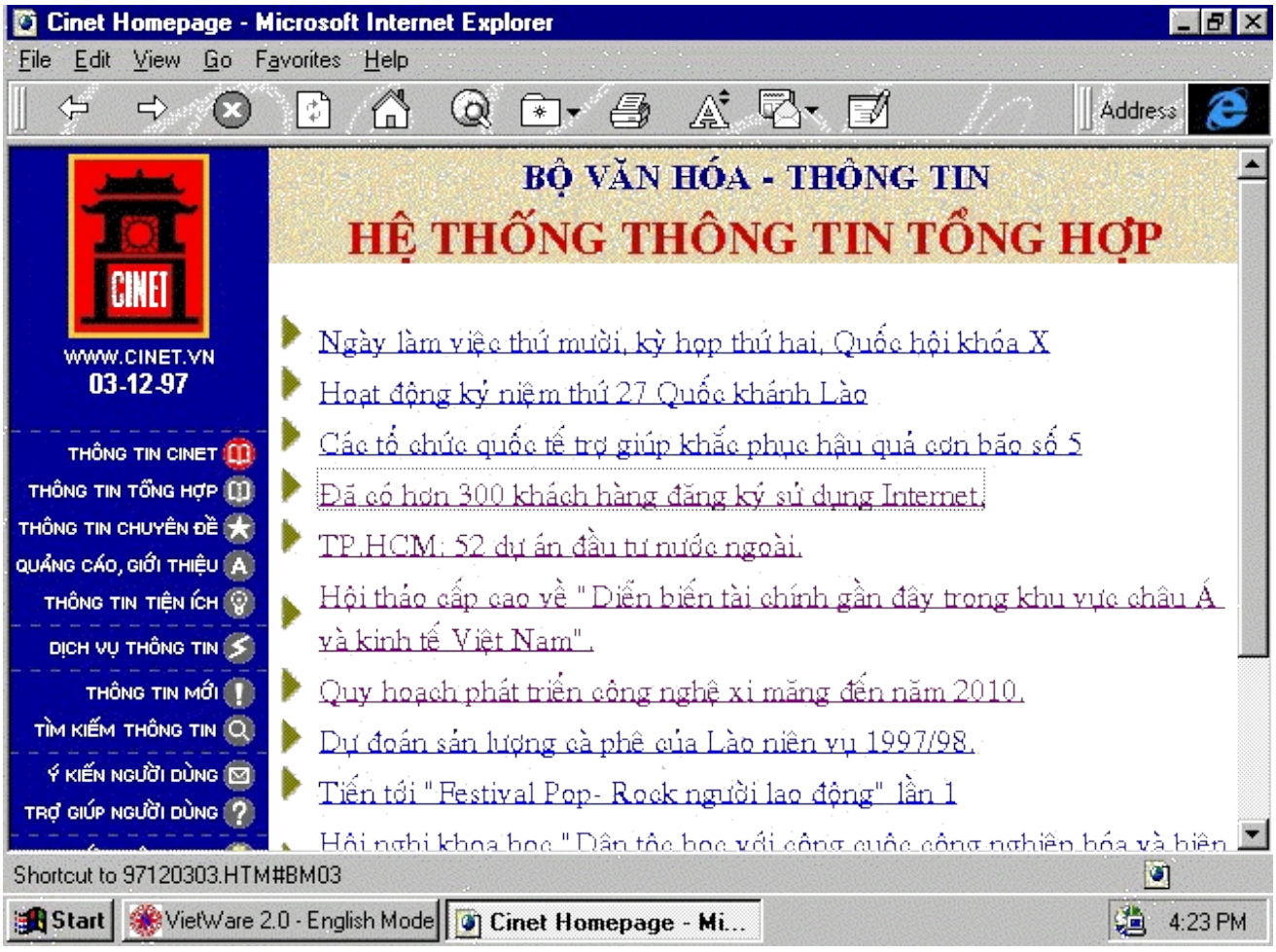
Thư điện tử (Email): đây là dịch vụ đã có từ khi mạng ARPANET mới được thiết lập, nó cho phép gửi và nhận thư điến tử cho mọi thành viên khác trong mạng.

Thông tin mới (News): Các vân đề thời sự được chuyển thành các diễn đàn cho phép mọi người quan tâm có thể trao đổi các thông tin cho nhau, hiện nay hiện nay có hàng nghìn diễ đàn về mọi mặt trên Internet.

Đăng nhập từ xa (Remote Login): Bằng các chương trình như Telnet, Rlogin người sử dụng có thể từ một trạm của Internet đăng nhập (logon) vào một trạm khác nếu như người đó được đăng ký trên máy tính kia.

Chuyển file (File transfer): Bằng chương trình FTP người sử dụng có thể chép các file từ một máy tính trên mạng Internet tới một máy tính khác. Người ta có thể chép nhiều phần mềm, cơ sở dữ liệu, bài báo bằng cách trên.

Dịch vụ WWW (World Wide Web): WWW là một dịch vụ đặc biệt cung cấp thông tin từ xa trên mạng Internet. Các tập tin siêu văn bản được lưu trữ trên máy chủ sẽ cung cấp các thông tin và dẫn đường trên mạng cho phép người sử dụng dễ dàng Truy cập các tập tin văn bản, đồ họa, âm thanh.



Hình 9.5: Ví dụ một trang Web cho phép dễ dàng khai thác các trang Web khác

Người sử dụng nhận được thông tin dưới dạng các trang văn bản, một trang là một đơn thể nằm trong máy chu. Đây là dịch vụ đang mang lại sức thu hút to lớn cho mạng Internet, chúng ta có thể xây dựng các trang Web bằng ngôn ngữ HTML (Hypertext Markup Language) với nhiều dạng phong phú như văn bản, hình vẽ, video, tiếng nói và có thể có các kết nối với các trang Web khác. Khi các trang đó được đặt trên các máy chủ Web thì thông qua Internet người ta có thể xem được sự thể hiện của các trang Web trên và có thể xem các trang web khác mà nó chỉ đến.

Các phần mềm thông dụng được sử dụng hiện nay để xây dựng và duyệt các trang Web là Mosaic, Navigator của Netscape, Internet Explorer của Microsoft, Web Access của Novell.

Chương 10 :

Giới thiệu về hệ điều hành mạng Windows NT

I. Thế nào là một hệ điều hành mạng

Với việc ghép nối các máy tính thành mạng thì cần thiết phải có một hệ thống phần mềm có chức năng quản lý tài nguyên, tính toán và xử lý truy nhập một cách thống nhất trên mạng, hệ như vậy được gọi là hệ điều hành mạng. Mỗi tài nguyên của mạng như tệp, đĩa, thiết bị ngoại vi được quản lý bởi một tiến trình nhất định và hệ điều hành mạng điều khiển sự tương tác giữa các tiến trình và truy cập tới các tiến trình đó.

Căn cứ vào việc truy nhập tài nguyên trên mạng người ta chia các thực thể trong mạng thành hai loại chủ và khách, trong đó máy khách (Client) truy nhập được vào tài nguyên của mạng nhưng không chia sẻ tài nguyên của nó với mạng, còn máy chủ (Server) là máy tính nằm trên mạng và chia sẻ tài nguyên của nó với các người dùng mạng.

Hiện nay các hệ điều hành mạng thường được chia làm hai loại là hệ điều hành mạng ngang hàng (Peer-to-peer) và hệ điều hành mạng phân biệt (client/server).

Với hệ điều hành mạng ngang hàng mỗi máy tính trên mạng có thể vừa đóng vai trò chủ lẫn khách tức là chúng vừa có thể sử dụng tài nguyên của mạng lẫn chia sẻ tài nguyên của nó cho mạng, ví dụ: LANtastic của Artisoft, NetWare lite của Novell, Windows (for Workgroup, 95, NT Client) của Microsoft.

Với hệ điều hành mạng phân biệt các máy tính được phân biệt chủ và khách, trong đó máy chủ mạng (Server) giữ vai trò chủ và các máy cho người sử dụng giữ vai trò khách (các trạm). Khi có nhu cầu truy nhập tài nguyên trên mạng các trạm tạo ra các yêu cầu và gửi chúng tới máy chủ sau đó máy chủ thực hiện và gửi trả lời. Ví dụ các hệ điều hành mạng phân biệt: Novell Netware, LAN Manager của Microsoft, Windows NT Server của Microsoft, LAN Server của IBM, Vines của Banyan System với server dùng hệ điều hành Unix.

II. Hệ điều hành mạng Windows NT

Windows NT là hệ điều hành mạng cao cấp của hãng Microsoft. Phiên bản đầu có tên là Windows NT 3.1 phát hành năm 1993, và phiên bản server là Windows NT Advanced Server (trước đó là LAN Manager for NT). Năm 1994 phiên bản Windows NT Server và Windows NT Workstation version 3.5 được phát hành. Tiếp theo đó ra đời các bản version 3.51. Các phiên bản workstation có sử dụng để thành lập mạng ngang hàng; còn các bản server dành cho quản lý file tập trung, in ấn và chia sẻ các ứng dụng.

Năm 1995, Windows NT Workstation và Windows NT Server version 4.0 ra đời đã kết hợp shell của người anh em Windows 95 nổi tiếng phát hành trước đó không lâu (trước đây shell của Windows NT giống shell của Windows 3.1) đã kết hợp được giao diện quen thuộc, dễ sử dụng của Windows 95 và sự mạnh mẽ, an toàn, bảo mật cao của Windows NT.

Windows NT có hai bản mà nó đi đôi với hai cách tiếp cận mạng khác nhau. Hai bản này gọi là Windows NT Workstation và Windows NT server. Với hệ điều hành chuẩn của NT ta có thể xây dựng mạng ngang hàng, máy chủ mạng và mọi công cụ quản trị cần thiết cho một máy chủ mạng ngoài ra còn có thể có nhiều giải pháp về xây dựng mạng diện rộng. Cả hai bản Windows NT station và Windows NT server cùng được xây dựng trên cơ sở nhân NT chung và các giao diện và cả hai cùng có những đặc trưng an toàn theo tiêu chuẩn C2. Windows NT Wordstation được sử dụng để kết nối những nhóm người sử dụng nhỏ, thường cùng làm việc trong một văn phòng. Tuy nhiên với Windows NT server ta có được một khả năng chống hỏng hóc cao, những khả năng cung cấp dịch vụ mạng lớn và những lựa chon kết nối khác nhau, Windows NT Server không hạn chế về số người có thể thâm nhập vào mạng.

Với Windows NT ta cũng có những công cụ quản trị từ xa vào mạng mà có thể thực hiện được việc quản trị từ những máy tính ở xa. Nó thích hợp với tất cả các sơ đồ mạng BUS, STAR, RING và hỗn hợp.

Windows NT là hệ điều hành có sức mạnh công nghiệp đầu tiên cho số lượng khổng lồ các máy tính IBM compatible. Windows NT là một hệ điều hành thực sự dành cho người sử dụng, các cơ quan, các công ty xí nghiệp. Windows NT là một hệ điều hành đa nhiệm, đa xử lý với địa chỉ 32 bit bộ nhớ. Nó yểm trợ các ứng dụng DOS, Windows, Win32 GUI và các ứng dụng dựa trên ký tự. Windows NT server là một hệ điều hành mạng hoàn chỉnh, nó nhanh chóng được thừa nhận là một trong những hệ điều hành tốt nhất hiện nay vì:

Là hệ điều hành mạng đáp ứng tất cả các giao thức truyền thông phổ dụng nhất. Ngoài ra nó vừa cho phép giao lưu giữa các máy trong mạng, vừa cho phép truy nhập từ xa, cho phép

truyền file v.v... Windows NT là hệ điều hành vừa đáp ứng cho mạng cục bộ (LAN) vừa đáp ứng cho mạng diện rộng (WAN) như Intranet, Internet.

Windows NT server hơn hẳn các hệ điều hành khác bởi tính mềm dẻo, đa dạng trong quản lý. Nó vừa cho phép quản lý mạng theo mô hình mạng phân biệt (Clien/Server), vừa cho phép quản lý theo mô hình mạng ngang hàng (peer to peer).

Windows NT server đáp ứng tốt nhất các dịch vụ viễn thông, một dịch vụ được sử dụng rộng rãi trong tương lai.

Windows NT server cài đặt đơn giản, nhẹ nhàng và điều quan trọng nhất là nó tương thích với hầu như tất cả các hệ mạng, nó không đòi hỏi người ta phải thay đổi những gì đã có.

Cho phép dùng các dịch vụ truy cập từ xa (Remote access service - RAS), có khả năng phụp vụ đến 64 cổng truy nhập từ xa (trong đó Lan manager 16 cổng).

Đáp ứng cho cả các máy trạm Macintosh nối với Windows NT server.

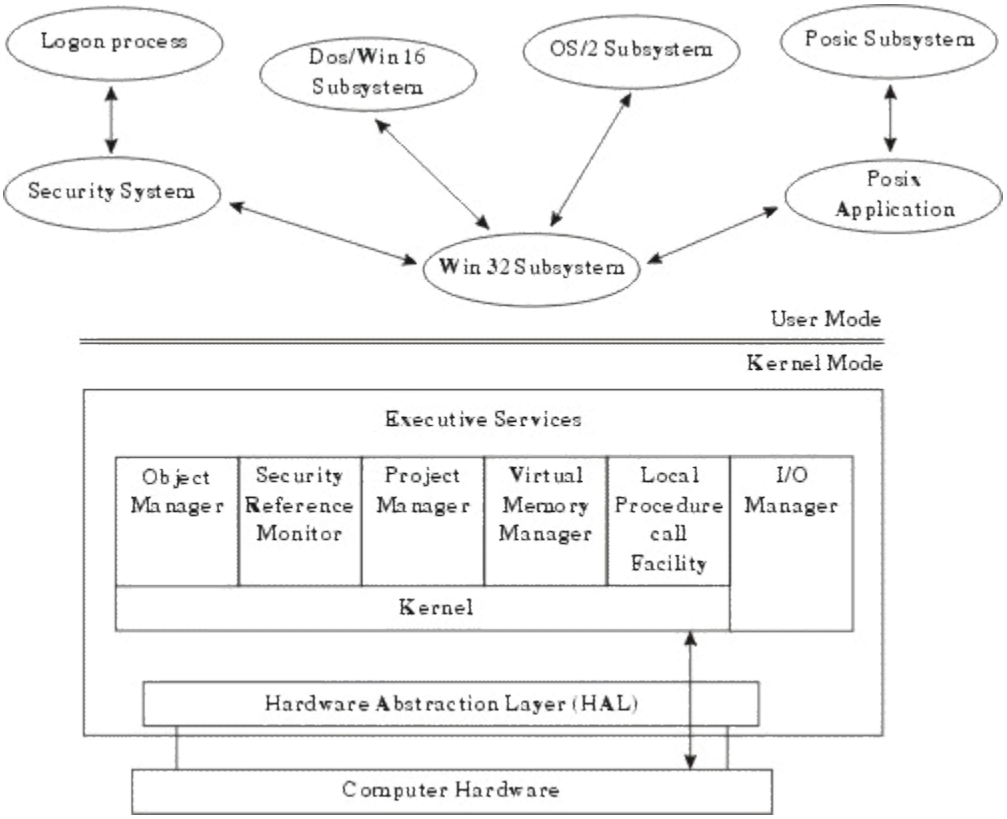
Windows NT yểm trợ mọi nghi thức mạng chuẩn như NetBUEI, IPX/SPX, TCP/IP và các nghi thức khác. Windows NT cũng tương thích với những mạng thông dụng hiên nay như Novell NetWare, Banyan VINES, và Microsoft LAN Manager. Đối với mạng lớn và khả năng thâm nhập từ xa sản phẩm Windows NT Server cũng cũng cấp các chức năng bổ xung nhu khả năng kết nối với máy tính lớn và máy MAC.

III. Cấu trúc của hệ điều hành Windows NT

Windows NT được thiết kế sử dụng cách tiếp cận theo đơn thể (modular). Các đơn thể khác nhau (còn được gọi là các bộ phận, thành phần) của Windows NT được trình bày trong hình 1 Các bộ phận của Windows NT có thể chạy dưới hai chế độ: User (người sử dụng) và Kernel (cốt lõi của hệ điều hành). Khi một thành phần của hệ điều hành chạy dưới cốt lõi của hệ điều hành (Kernel), nó truy cập đầy đủ các chỉ thị máy cho bộ xử lý đó và có thể truy cập tổng quát toàn bộ tài nguyên trên hệ thống máy tính.

Trong Windows NT: Executive Services, Kernel và HAL chạy dưới chế độ cốt lõi của hệ điều hành.

Hệ thống con (Subsystem) Win 32 và các hệ thống con về môi trường, chẳng hạn như DOS/Win 16.0S/2 và hệ thống con POSIX chạy dưới chế độ user. Bằng cách đặt các hệ thống con này trong chế độ user, các nhà thiết kế Windows NT có thể hiệu chỉnh chúng dễ dàng hơn mà không cần thay đổi các thành phần được thiết kế để chạy dưới chế độ Kernel.



Hình 10.1: Cấu trúc Windows NT

Các lớp chính của hệ điều hành WINDOWS NT SERVER gồm:

Lớp phần cứng trừu tượng (Hardware Astraction Layer - HAL): Là phần cứng máy tính mà cốt lõi của hệ điều hành (Kernel) có thể đươc ghi vào giao diện phần cứng ảo, thay vì vào phần cứng máy tính thực sự. Phần lớn cốt lõi của hệ điều hành sử dụng HAL để truy cập các tài nguyên máy tính. Điều này có nghĩa là cốt lõi của hệ điều hành và tất cả các thành phần khác phụ thuộc vào cốt lõi có thể dễ dàng xuất (Ported) thông qua Microsoft đến các nền

(Platform) phần cứng khác. Một thành phần nhỏ trong cốt lõi của hệ điều hành, cũng như bộ quản lý Nhập / Xuất truy cập phần cứng máy tính trực tiếp mà không cần bao gồm HAL.

Lớp Kernel cốt lõi của hệ điều hành): Cung cấp các chức năng hệ điều hành cơ bản được sử dụng bởi các thành phần thực thi khác. Thành phần Kernel tương đối nhỏ và cung cấp các thành phần cốt yếu cho những chức năng của hệ điều hành. Kernel chủ yếu chịu trách nhiệm quản lý luồng, quản lý phần cứng và đồng bộ đa sử lý.

Các thành phần Executive: Là các thành phần hệ điều hành ở chế độ Kernel thi hành các dịch vụ như :

Quản lý đối tượng (object manager)

Bảo mật (security reference monitor)

Quản lý tiến trình (process manager)

Quản lý bộ nhớ ảo (virtual memory manager)

Thủ tục cục bộ gọi tiện ích, và quản trị nhập/xuất (I/O Manager)

IV.Cơ chế quản lý của Windows NT

1. Quản lý đối tượng (Object Manager):

Tất cả tài nguyên của hệ điều hành được thực thi như các đối tượng. Một đối tượng là một đại diện trừu tượng của một tài nguyên. Nó mô tả trạng thái bên trong và các tham số của tài nguyên và tập hợp các phương thức (method) có thể được sử dụng để truy cập và điều khiển đối tượng.

Ví dụ một đối tượng tập tin sẽ có một tên tập tin, thông tin trạng thái trên file và danh sách các phương thức, như tạo, mở,đóng và xóa, đối tượng mô tả các thao tác có thể được thực hiện trên đối tượng file.

Bằng cách xử lý toàn bộ tài nguyên như đối tượng Windows NT có thể thực hiện các phương thức giống nhau như: tạo đối tượng, bảo vệ đối tượng, giám sát việc sử dụng đối tượng (Client object) giám sát những tài nguyên được sử dụng bởi một đối tượng.

Việc quản lý đối tượng (Object Manager) cung cấp một hệ thống đặt tên phân cấp cho tất cả các đối tượng trong hệ thống. Do đó, tên đối tượng tồn tại như một phần của không gian tên toàn cục và được sử dụng để theo dõi việc tạo và sử dụng đối tượng.

Sau đây là một số ví dụ của loại đối tượng Windows NT :

Đối tượng Directory (thư mục).

Đối tượng File (tập tin).

Đối tượng kiểu object.

Đối tượng Process (tiến trình).

Đối tượng thread (luồng).

Đối tượng Section and segment (mô tả bộ nhớ).

Đối tượng Port (cổng).

Đối tượng Semaphore và biến cố.

Đối tượng liên kết Symbolic (ký hiệu).

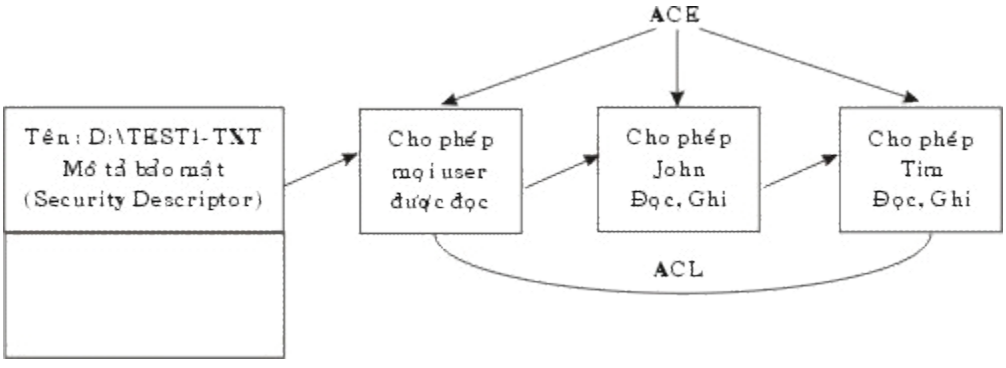
***2. Cơ chế bảo mật* (SRM - Security Reference Monitor):**

Được sử dụng để thực hiện vấn đề an ninh trong hệ thống Windows NT. Các yêu cầu tạo một đối tượng phải được chuyển qua SRM để quyết định việc truy cập tài nguyên được cho phép hay không. SRM làm việc với hệ thống con bảo mật trong chế độ user. Hệ thống con này được sử dụng để xác nhận user login vào hệ thống Windows NT.

Để kiểm soát việc truy cập, mỗi đối tượng Windows NT có một danh sách an toàn (Access Control List - ACL). Danh sách an toàn của mỗi đối tượng gồm những phần tử riêng biệt gọi là Access Control Entry (ACE). Mỗi ACE chứa một SecurityID (SID: số hiệu an toàn) của người sử dụng hoặc nhóm. Một SID là một số bên trong sử dụng với máy tính Windows NT mô tả một người sử dụng hoặc một nhóm duy nhất giữa các máy tính Windows NT.

Ngoài SID, ACE chứa một danh sách các hành động (action) được cho phép hoặc bị từ chối của một user hoặc một nhóm. Khi người sử dụng đăng nhập vào mạng Windows NT, sau khi việc nhận dạng thành công, một Security Access Token (SAT) được tạo cho người dùng đó. SAT chứa SID của người dùng và SID của tất cả các nhóm người dùng thuộc mạng Windows NT. Sau đó SAT hoạt động như một "passcard" (thẻ chuyển) cho phiên làm việc của người dùng đó và được sử dụng để kiểm tra tất cả hoạt động của người dùng.

Khi người dùng tham gia mạng truy cập một đối tượng, Security Reference Monitor kiểm tra bộ mô tả bảo mật của đối tượng xem SID liệt kê trong SAT có phù hợp với giá trị trong ACE không. Nếu phù hợp, các quyền về an ninh được liệt trong ACE áp dụng cho người dùng đó.



Hình 10.2: Ví dụ về danh sách an toàn (Access Control List).

3. Quản lý nhập / xuất (I/O Manager) :

Chịu trách nhiệm cho toàn bộ các chức năng nhập / xuất trong hệ điều hành Windows NT. I/O Manager liên lạc với trình điều khiển của các thiết bị khác nhau.

4. I/O *Manager:*

Ssử dụng một kiến trúc lớp cho các trình điều khiển. Mỗi bộ phận điều khiển trong lớp này thực hiện một chức năng được xác định rõ. Phương pháp tiếp cận này cho phép một thành phần điều khiển được thay thế dễ dàng mà không ảnh hưởng phần còn lại của các bộ phận điều khiển.

Hình 10.3:Các trình điều khiển thiết bị theo lớp của I / O Manager

V. Các cơ chế bảo vệ dữ liệu trong Windows NT

Cơ chế bảo vệ dữ liệu của Windows NT gọi là fault tolerance, nó cho phép hệ thống khả năng tiếp tục làm việc và bảo toàn dữ liệu của hệ thống trong trường hợp một phần của hệ thống có sự cố hỏng hóc sai lệch. Trong Windows NT cơ chế fault tolerance bao gồm các biện pháp sau:

Chống cúp điện bất thường.

Cung cấp khả năng bảo vệ hệ thống đĩa (fault tolerance disk subsystem).

Cung cấp khả năng sao chép dự phòng (backup) từ băng từ.

Khả năng bảo vệ hệ thống đĩa của Windows NT là RAID ø (viết tắt của Redundant Array of Inexpensiredisk). Thực chất RAID là một loạt các biện pháp để bảo vệ hệ thống đĩa. Các biện pháp trong RIAD được chia thành 6 mức sau:

***Mức 0*:** Đây là mức ứng với biện pháp chia nhỏ đĩa (disk striping). Thực chất nội dung của biện pháp này là phân chia dữ liệu thành khối và sau đó sắp xếp các khối dữ liệu theo thứ tự trong tất cả các đĩa thành 1 mảng.

***Mức 1*:** Mức này ứng với biện pháp disk Mirroring, biện pháp này cho phép tạo ra 2 đĩa giống nhau. Nếu trong quá trình vận hành mạng một đĩa có sự cố thì hệ thống sử dụng dữ liệu của đĩa kia.

***Mức 2*:** Mức này ứng với biện pháp phân chia nhỏ đĩa bằng cách phân chia các file thành các byte và sắp xếp các byte sang nhiều đĩa. Mức này sử dụng mã sửa sai (error correcting code) trong quá trình phân chia đĩa. Nói chung biện pháp dùng ở mức này tốt hơn biện pháp dùng trong mức 1.

***Mức 3*:** Mức này sử dụng biện pháp giống mức 2. Tuy nhiên mã sửa sai (error correction code) chỉ sử dụng cho một đĩa. Không áp dụng cho nhiều đĩa như ở mức 2. Người ta thường dùng mức này để truy nhập vào một số ít file có dung tích lớn.

***Mức 4*:** Mức này sử dụng biện pháp giống ở mức 2 và 3 nhưng bằng phương pháp phân chia đĩa thành các khối lớn. Giống như mức 3 tất cả các mã sửa sai (error correction code) được hgi vào một đĩa và tách khỏi khối dữ liệu.

***Mức 5*:** Trong mức này người ta sử dụng biện pháp phân chia đĩa thành từng phần gọi là Striping with party. Biện pháp sử dụng ở mức này tương tự như ức 4, số liệu được phân nhỏ thành các khối lớn và sau đó ghi vào tất cả các đĩa. Các thông tin (party Infomation) được coi như các dữ liệu dùng tạm thời (data redundancy).

Ngoài ra chúng ta còn có thể áp dụng các biện pháp bảo vệ dữ liệu trong Windows NT:

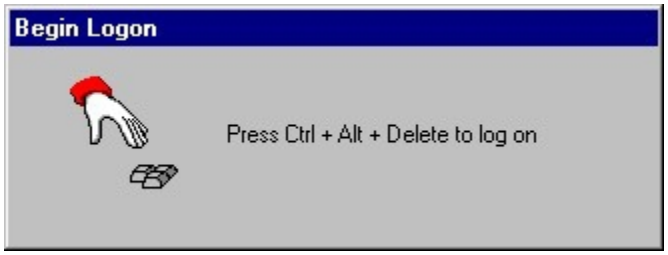
Biện pháp Disk mirroring: Disk mirroring là cách sao tạm (redundant) lại đĩa hoặc partition. Biện pháp này bảo vệ dữ liệu tránh các sự cố bằng cách dưa ra chế độ thường xuyên backup đĩa hoặc partition. Hình dưới chỉ ra cách dùng biện pháp Mirroring:

Disk Duplexing: Biện pháp dùng đĩa kép (Disk Duplexing) tường tự như disk mirroring chỉ khác là chúng dùng 2 disk controler. Diều này cho thên hả năng bảo vệ khi controler của một đĩa có sự cố. Trong khi đó biện pháp Mirror không thể khắc phục được tình huống này.

Mirror Set: Các partition hoặc đĩa trong chế độ Mirror được tạo ra bằng cách lặp sao lại partition hoặc đĩa trên đĩa khác cùng một tên ổ đĩa được gán cho cả 2 partition. Ta có thể dùng establish Mirror trong menu Fault tolerance. Nếu đĩa hoặc partition trong chế độ Mirror bị lỗi thì chế độ Mirror cần phải ngắt để thực hiện chế độ sao chép dự phòng vào một đĩa riệng. Sau đó sao backup trở lại.

VI. Giới thiệu về hoạt động của Windows NT Server

Khi chúng ta khởi động Windows NT Server hộp Begin logon sẽ hiện ra, server chờ đợi để chúng ta bấm Ctrl+Alt +Del để có thể tiếp tục hoạt động. Ở đây có điểm khác với các hệ điều hành DOS, Windows 95 là tổ hợp Ctrl+Alt +Del không phải là khởi động lại máy. Trong trường hợp này Windows NT loại bỏ mọi chương trình Virus hay không có phép đang hoạt động trước khi bước vào làm việc.



Hình 10.4: Thông báo gia nhập mạng

Lúc này chúng ta sẽ thấy hộp Logon Information xuất hiện và yếu cầu chúng ta phải đánh đúng tên và mật khẩu thì mới được đăng nhập vào Server. Nếu là người dùng mới thì phải được người quản trị khai báo tên và mật khẩu trước khi đăng nhập..

Hình 10.5: Màn hình gia nhập mạng

Cũng giống như màn hình nền của hệ điều hành Windows 95 khi muốn thực hiện các trình, gọi các menu hệ thống chúng ta dùng nút Start ở cuối màn hình

Hình 10.6: Điểm khởi đầu của Windows

Trước muốn kết thúc chương trình và tắt máy chúng ta phải bấm phím Start rồi chọn ShutDown, màn hình kết thúc sẽ hiện ra cho chúng ta lựa chon công yêu cầu về tắt hay khởi động lại.

Hình 10.7: Màn hình thoát khỏi Windows

Chương 11

Hệ thống quản lý của mạng Windows NT

Các mạng máy tính hiện nay được thiết kế rất đa dạng và đang thực hiện những ứng dụng trên nhiều lĩnh vực của đời sống xã hội. Điều đó có nghĩa là các thông tin lưu trữ trên mạng và các thông tin truyền giao trên mạng ngày càng mang nhiều giá trị có ý nghĩa sống còn. Do vậy những người quản trị mạng ngày càng phải quan tâm đến việc bảo vệ các tài nguyên của mình.

Việc bảo vệ an toàn là quá trình bảo vệ mạng khỏi bị xâm nhập hoặc mất mát, khi thiết kế các hệ điều hành mạng người ta phải xây dựng một hệ thống quản lý nhiều tầng và linh hoạt giúp cho người quản trị mạng có thể thực hiện những phương án về quản lý từ đơn giản mức độ thấp cho đến phức tạp mức độ cao trong những mạng có nhiều người tham gia. Thông qua

những công cụ quản trị đã được xây dựng saün người quản trị có thể xây dựng những cơ chế về an toàn phù hợp với cơ quan của mình.

Thông thường hệ thống mạng có những mức quản lý chính sau:

Mức quản lý việc thâm nhập mạng (Login/Password): Mức quản lý việc thâm nhập mạng (Login/Password) xác định những ai và lúc nào có thể vào mạng. Đối với người quản trị và người sử dụng mạng, mức an toàn này dường như khá đơn giản mà theo đó mỗi người sử dụng (người sử dụng) có một tên login và mật khẩu duy nhất.

Mức quản lý trong việc quản lý sử dụng các tài nguyên của mạng: Kiểm soát những tài nguyên nào mà người sử dụng được phép truy cập, sử dụng và sử dụng như thế nào.

Mức quản lý với thư mục và file: Mức an toàn của file kiểm soát những file và thư mục nào người sử dụng được dùng trên mạng và được sử dụng ở mức độ nào

Mức quản lý việc điều khiển File Server: Mức an toàn trên máy chủ kiểm soát ai có thể được thực hiện các thao tác trên máy chủ như bật, tắt, chạy các chương trình khác. Người ta cần có cơ chế như mật khẩu để bảo vệ.

I. Quản lý các tài nguyên trong mạng

Như chúng ta đã biết, mạng LAN cung cấp các dịch vụ theo hai cách: qua cách chia sẻ tài nguyên theo nguyên tắc ngang hàng và thông qua những máy chủ trung tâm. Dù bất cứ phương pháp nào được sử dụng, vấn đề cần phải giải quyết là là giúp người sử dụng xác định được các tài nguyên có saün ở đâu để có thể sử dụng.

Các kỹ thuật sau đây đã được sử dụng để tổ chức tài nguyên mạng máy tính:

1. Quản lý đơn lẻ từng máy chủ (Stand-alone Services)

Với cách quản lý này trong mạng LAN thường chỉ có một vài máy chủ, mỗi máy chủ sẽ quản lý tài nguyên của mình, mỗi người sử dụng muốn thâm nhập những tài nguyên của máy chủ nào thì phải khai báo và chịu sự quản lý của máy chủ đó. Mô hình trên phù hợp với những mạng nhỏ với ít máy chủ và khi có trục trặc trên một máy chủ thì toàn mạng vẫn hoạt động. Cũng vì trong mạng LAN chỉ có ít máy chủ, do đó người sử dụng không mấy khó khăn để tìm các tập tin, máy in và các tài nguyên khác của mạng (plotter, CDRom, modem...).

Việc tổ chức như vậy không cần những dịch vụ quản lý tài nguyên phức tạp. Tuy nhiên khi trong mạng có từ hai máy chủ trở lên vấn đề trở nên phức tạp hơn vì mỗi máy chủ riêng lẻ giữ riêng bảng danh sách các người sử dụng và tài nguyên của mình. Khi đó mỗi người sử dụng phải tạo lập và bảo trì tài khoản của mình ở hai máy chủ khác nhau mới có thể đăng nhập

(logon) và truy xuất đến các máy chủ này. Ngoài ra việc xác định vị trí của các tài nguyên trong mạng cũng rất khó khăn khi mạng có qui mô lớn.

2. Quản lý theo dịch vụ thư mục (Directory Services)

Hệ thống các dịch vụ thư mục cho phép làm việc với mạng như là một hệ thống thống nhất, tài nguyên mạng được nhóm lại một cách logic để dễ tìm hơn. Giải pháp này có thể được dùng cho những mạng lớn. Ở đây thay vì phải đăng nhập vào nhiều máy chủ, người sử dụng chỉ cần đăng nhập vào mạng và được các dịch vụ thư mục cấp quyền truy cập đến tài nguyên mạng, cho dù được cung cấp bởi bất kể máy chủ nào.

Người quản trị mạng chỉ cần thực hiện công việc của mình tại một trạm trên mạng mặc dù các điểm nút của nó có thể nằm trên cả thế giới. Hệ điều hành Netware 4.x cung cấp dịch vụ nổi tiếngï và đầy ưu thế cạnh tranh này với tên gọi ***Netware Directory Services (NDS).***

Giải pháp này thích hợp với những mạng lớn. Các thông tin của NDS được đặt trong một hệ thống cơ sở dữ liệu đồng bộ, rộng khắp được gợi là DIB (Data Information Base). Cơ sở dữ liệu trên quản lý các dữ liệu dưới dạng các đối tượng phân biệt trên toàn mạng. Các định nghĩa đối tượng sẽ được đặt trên các tập tin riêng của một số máy chủ đặc biệt, mỗi đối tượng có các tính chất và giá trị của mỗi tính chất. Đối tượng bao hàm tất cả những gì có tên phân biệt như Người sử dụng, File server, Print server, group. Mỗi loại đối tượng có những tính chất khác nhau ví dụ như đối tượng Người sử dụng có tính chất về nhóm mà người sử dụng đó thuộc, còn nhóm có các tính chất về người sử dụng mà nhóm đó chứa.

Việc thiết lập các dịch vụ như vậy cần được lập kế hoạch, thiết kế rất cẩn thận, liên quan đến tất cả các đơn vị phòng ban có liên quan. Loại mạng này có khuyết điểm là việc thiết kế, thiết lập mạng rất phức tạp, mất nhiều thời gian nên không thích hợp cho các mạng nhỏ.

3. Quản lý theo nhóm (Workgroup)

Các nhóm làm việc làm việc theo ý tưởng ngược lại với các dịch vụ thư mục. Nhóm làm việc dựa trên nguyên tắc mạng ngang hàng (peer-to-peer network), các người sử dụng chia sẻ tài nguyên trên máy tính của mình với những người khác, máy nào cũng vừa là chủ (server) vừa là khách (client). Người sử dụngï có thể cho phép các người sử dụng khác sử dụng tập tin, máy in, modem... của mình, và đến lượt mình có thể sử dụng các tài nguyên được các người sử dụng khác chia sẻ trên mạng. Mỗi cá nhân người sử dụng quản lý việc chia sẻ tài nguyên trên máy của mình bằng cách xác định cái gì sẽ được chia sẻ và ai sẽ có quyền truy cập. Mạng này hoạt động đơn giản: sau khi logon vào, người sử dụng có thể duyệt (browse) để tìm các tài nguyên có saün trên mạng.

Workgroup là nhóm logic các máy tính và các tài nguyên của chúng nối với nhau trên mạng mà các máy tính trong cùng một nhóm có thể cung cấp tài nguyên cho nhau. Mỗi máy tính trong một workgroup duy trì chính sách bảo mật và CSDL quản lý tài khoản bảo mật SAM (Security Account Manager) riêng ở mỗi máy. Do đó quản trị workgroup bao gồm việc quản trị CSDL tài khoản bảo mật trên mỗi máy tính một cách riêng lẻ, mang tính cục bộ, phân tán. Điều này rõ ràng rất phiền phức và có thể không thể làm được đối với một mạng rất lớn.

Nhưng workgroup cũng có điểm là đơn giản, tiện lợi và chia sẽ tài nguyên hiệu quả, do đó thích hợp với các mạng nhỏ, gồm các nhóm người sử dụng tương tự nhau.

Tuy nhiên Workgroup dựa trên cơ sở mạng ngang hàng (peer-to-peer), nên có hai trở ngại đối với các mạng lớn như sau:

Đối với mạng lớn, có quá nhiều tài nguyên có saün trên mạng làm cho các người sử dụng khó xác định chúng để khai thác.

Người sử dụng muốn chia sẻ tài nguyên thường sử dụng một cách dễ hơn để chia sẻ tài nguyên chỉ với một số hạn chế người sử dụng khác.

Điển hình cho loại mạng này là Windws for Workgroups, LANtastic, LAN Manager... Window 95, Windows NT Workstation.

4. Quản lý theo vùng (Domain)

Domain mượn ý tưởng từ thư mục và nhóm làm việc. Giống như một workgroup, domain có thể được quản trị bằng hỗn hợp các biện pháp quản lý tập trung và địa phương. Domain là một tập hợp các máy tính dùng chung một nguyên tắc bảo mật và CSDL tài khoản người dùng (người sử dụng account). Những tài khoản người dùng và nguyên tắc an toàn có thể được nhìn thấy khi thuộc vào một CSDL chung và được tập trung.

Giống như một thư mục, một domain tổ chức tài nguyên của một vài máy chủ vào một cơ cấu quản trị. Người sử dụng được cấp quyền logon vào domain chứ không phải vào từng máy chủ riêng lẻ. Ngoài ra, vì domain điều khiển tài nguyên của một số máy chủ, nên việc quản lý các tài khoản của người sử dụng được tập trung và do đó trở nên dễ dàng hơn là phải quản lý một mạng với nhiều máy chủ độc lập.

Các máy chủ trong một domain cung cấp dịch vụ cho các người sử dụng. Một người sử dụng khi logon vào domain thì có thể truy cập đến tất cả tài nguyên thuộc domain mà họ được cấp quyền truy cập. Họ có thể dò tìm (browse) các tài nguyên của domain giống như trong một workgroup, nhưng nó an toàn, bảo mật hơn.

Để xây dựng mạng dựa trên domain, ta phải có ít nhất một máy Windows NT Server trên mạng. Một máy tính Windows NT có thể thuộc vào một workgroup hoặc một domain,

nhưng không thể đồng thời thuộc cả hai. Mô hình domain được thiết lập cho các mạng lớn với khả năng kết nối các mạng toàn xí nghiệp hay liên kết các kết nối mạng với các mạng khác và những công cụ cần thiết để điều hành.

Việc nhóm những người sử dụng mạng và tài nguyên trên mạng thành domain có lợi ích sau:

Mã số của người sử dụng được quản lý tập trung ở một nơi trong một cơ sở dữ liệu của máy chủ, do vậy quản lý chặt chẽ hơn.

Các nguồn tài nguyên cục bộ được nhóm vào trong một domain nên dễ khai thác hơn.

Quản lý theo Workgroup và domain là hai mô hình mà Windows NT lựa chọn. Sự khác nhau căn bản giữa Workgroup và domain là trong một domain phải có ít nhất một máy chủ (máy chủ) và tài nguyên người sử dụng phải được quản lý bởi máy chủ đó.

II. Hệ thống quản lý trên Hệ điều hành mạng Windows NT Server

Windows NT cung cấp những chức năng tuân theo chuẩn C2 (chuẩn về an toàn quốc tế) trong đó Windows NT đảm bảo tránh được những người không được phép vào trong hệ thống hoặc thâm nhập vào các file và chương trình trên đĩa cứng. Người ta không thể thâm nhập vào được nếu không có mật khẩu đúng. và qua đó đã bảo vệ được các file. Windows NT cung cấp công cụ để xây dựng các lớp quyền dành cho nhiều nhiệm vụ khác nhau nhằm xây dựng hệ thống an toàn một cách mềm dẻo.

Nhiều người sử dụng có thể có quyền vào một máy chủ Windows NT. Một tài khoản của người sử dụng trên máy bao gồm tên, mật khẩu và nhiều tính chất được cho bởi người quản trị mạng. Người sử dụng có thể che các thư mục hay file của mình từ những người khác và cài đặt các thông số của File manager, Programe Manager, Control Panel một cách phù hợp.

Khi người dùng thâm nhập vào hệ thống thì tự động khởi động mọi thông số đã được lưu trữ từ trước. Nếu người sử dụng có quyền cao hơn thì họ có thể chia sẻ hoặc ngừng các tài nguyên đang dùng chung trên mạng như máy in hay file hoặc họ có thể thay đổi quyền của những người dùng mạng khác khi thâm nhập vào mạng.

1. Mô hình Workgroup (nhóm) của mạng Windows NT

Mỗi người truy cập vào mạng Windows NT tổ chức theo mô hình Workgroup cần phải đăng ký:

Tên vào mạng

Mật khẩu vào mạng

Dựa vào tên và mật khẩu đã cho, Windows NT cung cấp cho người một số gọi là mã số của người sử dụng (user account). Mã số này được lưu dữ trong cơ sở dữ liệu là hệ thống

quản trị tài nguyên (SAM - Security Account Manager database). Hệ thống quản trị tài nguyên dùng để đảm bảo an toàn về tài nguyên trên mạng. Người vào mạng muốn truy nhập vào tài nguyên phải qua sự kiểm duyệt của hệ thống quản trị tài nguyên. Trong mô hình Workgroup mỗi máy trạm có một nguồn tài nguyên tương ứng với một hệ thống quản trị tài nguyên bảo vệ nó.

Chú ý: Mỗi người khai thác mạng phải nhớ nhiều mã số, vì ứng với mỗi máy trạm có một hệ thống quản trị tài nguyên riêng của nó.

2. Mô hình vùng (Domain)

Domain là một khái niệm rất cơ bản trong Windows NT server, nó là hạt nhân để tổ chức các mạng có quy mô lớn.

Mỗi người tham gia trong Domain cần phải đăng ký thông tin sau:

Tên Domain

Tên người sử dụng

Mật khẩu

Các thông tin này được lưu ở máy chủ dưới dạng một mã số, gọi là tài khoản người sử dụng (user account) và các mã số cũa người sử dụng trong một domain được tổ chức thành một cơ sở dữ liệu trên máy chủ. Khi người sử dụng muốn truy nhập vào một Domain người đó phải chọn tên Domain trong hộp thoại trên máy trạm. Máy trạm sẽ chuyển các thông tin về hệ thống quản trị tài nguyên (SAM - Security Account Manager database) của Domain để kiểm tra. Khi đó hệ thống quản trị tài nguyên trên máy chủ sẽ kiểm tra các thông tin này, nếu kết quả kiểm tra là đúng, người khai thác mới được quyền truy nhập vào tài nguyên của Domain.

Một máy Windows NT mà không tham gia vào một Domain có nhược điểm sau:

Máy trạm chỉ có thể cung cấp các mã số được tạo ra trên nó. Nếu máy này bị hư hỏng thì những người khai thác mạng không thể truy nhập bằng mã số của họ. Nếu máy này nằm trong một Domain nào đó thì các mã số này còn được lưu trong SAM của một Domain trên máy Máy chủ.

Qua máy trạm không tham gia vào Domain, người khai thác mạng không thể truy nhập vào tài nguyên của Domain, mặc dù mã số của của người này có trong SAM của Domain

Trong một Domain thường có các loại máy thực hiện những công việc sau:

Primary domain Controller (PDC), bao giờ cũng phải có để quản trị hệ thống các người sử dụng và các tài khoản trong Domain (hệ thống này gọi là cơ sở dữ liệu SAM - Security Account Manager của Domain). SAM trên máy chủ được thiết kế như hệ thống kiểm soát Domain. Trong một Domain chỉ có duy nhất một PDC.

Ngoài ra hệ thống còn có một hay nhiều máy làm Backup Domain Controller (BDC). Các BDC có thể dùng thay thế cho máy PDC trong trường hợp cần thiết, chẳng hạn máy PDC bị hư Người quản trị Domain chỉ cần tạo tài khoản người sử dụng (user account) chỉ một lần trên máy Primary Domain Controller, thông tin được tự dộng copy đến các máy Backup Domain Controller.

3. Mô hình quan hệ giữa các Domain trong mạng Windows NT

Trong một mạng có thể có nhiều Domain nhưng một máy tính Windows NT là thành viên của chỉ một domain tại mỗi thời điểm. Tuy nhiên, có một vài trường hợp đôi khi chúng ta cần truy cập tài nguyên trong những domain khác, để là được điều này hệ điều hành Windows NT server cho phép giữa các Domain có thể tồn tại một quan hệ gọi là quan hệ tin cậy (trust relationship). Chúng ta có thể sử dụng quan hệ tin cậy giữa các Domain cho phép người dùng trên một Domain truy cập tài nguyên trong Domain khác.

Hai Domain A, B gọi là quan hệ tin cậy (trust relationship) mà trong đó Domain A tin cậy Domain B nếu giữa chúng có một mối liên kết sao cho người khai thác mạng của Domain B có thể truy nhập vào Domain A từ một máy trạm trong Domain B.

Từ góc độ của người quản trị mạng mục đích của việc thiết lập quan hệ tin cậy giữa các Domain là làm cho việc quản lý mạng trở lên đơn giản hơn bằng cách kết hợp các Domain vào một đơn vị quản lý. Trong quan hệ tin cậy các Domain được chia ra như sau:

Domain được tin cậy (trusted domain)

Domain tin cậy (trusting domain)

Một Domain là loại này hoặc loại kia *thông thường* phụ thuộc vào nó chứa mã số của người sử dụng (người sử dụng account) hay chỉ chứa tài nguyên (resource)

Domain tin cậy (trusting domain) là Domain chứa tài nguyên.

Domain được tin cậy (trusted domain) là Domain chứa mã số người sử dụng.

Khi người sử dụng truy nhập từ một máy trạm trong Domain tin cậy (trusting domain) vào Domain được tin cậy (trusted domain) thì quá trình kiểm soát diễn ra như sau:

Người sử dụng phải cho mã số (mã số này ứng với tên, mật khẩu, tên domain cần truy nhập)

Mã số được chuyển về máy chủ của Domain tin cậy.

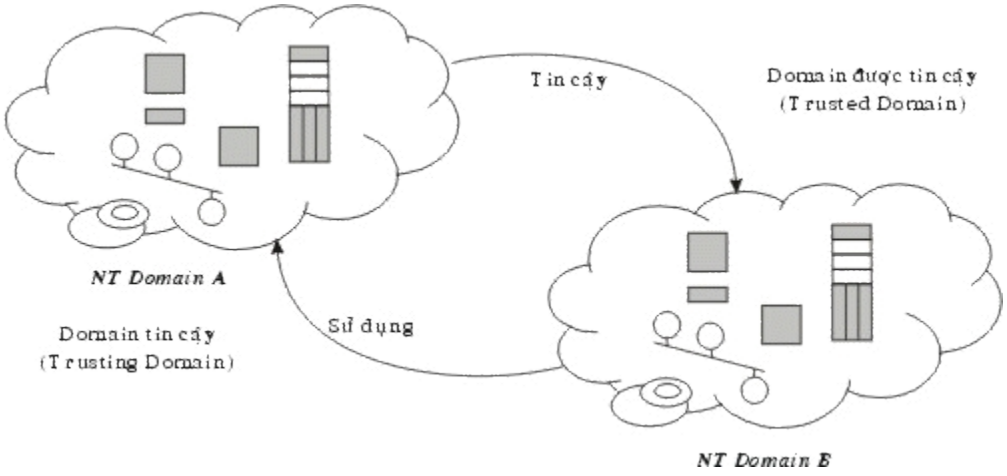
Máy chủ của Domain tin cậy chuyển mã số này sang Domain được tin cậy.

Kết quả kiểm tra của máy chủ trong Domain được tin cậy diễn ra theo quá trình ngược lại

Ở đây chúng ta chú ý:

Việc liên kết giữa các Domain không có tính bắc cầu.

Thông qua việc thiết lập mối quan hệ tin tưởng, chúng ta có thể sử dụng một tài khoản để truy xuất đến nhiều tài nguyên của nhiều Domain. Có thể quản trị nhiều Domain từ một vị trí tập trung.



Hình 11.1: Mô hình tin cậy của các Domain trong mạng Windows NT

4. Nhóm (group) trong Windows NT

Trong mạng Windows NT khái niệm nhóm (group) là một trong những khái niệm quan trọng đối với công việc quản lý, điều hành mạng Windows NT. Nhóm làm cho việc khai thác tài nguyên được dễ dàng thuận lợi và đơn giản hóa việc quản trị. Mỗi nhóm được đăng ký bởi một tài khoản (group account) và có các thành viên của nó. Các quyền đã được gán cho nhóm sẽ tự động gán cho các người sử dụng là thành viên của nhóm. Các tiện lợi của nhóm như sau:

Quyền có thể được gán cho, hoặc hủy đi trên mọi thành viên của nhóm.

Khi một người sử dụng bị loại ra khỏi nhóm, thì tự động bị mất các quyền đã được cấp khi còn trong nhóm.

Trong mạng Windows NT người ta phân biệt phân biệt hai loại nhóm là nhóm toàn cục (global group) và nhóm cục bộ (local group).

5. Nhóm toàn cục (global group)

Nhóm toàn cục còn được gọi là nhóm vùng (domain group). Thành viên của nhóm là các người dùng cấp vùng (domain user). Họ ngược lại với người dùng cục bộ (local user) là người có phạm vi giới hạn trong máy tính mà họ được xác định. Thành viên của nhóm toàn cục được phép chuyển ra ngoài (export) một Domain khác. Phạm vi của nhóm toàn cục là toàn bộ vùng trên đó user dược xác định, và thấy được từ bất kỳ máy tính NT nào trong vùng đó.

Quyền có thể được gán cho nhóm toàn cục cho các tài nguyên trên một máy NT Server hay NT Workstation trong vùng.

Các tài khoản nhóm toàn cục được lưu ở PDC (Primary DomainController) của Domain, và được sao lưu đến các BDC (Backup Domain Controller) trong Domain đó.

Nhóm toàn cục có những đặc trưng sau:

Thành viên của nhóm phải là các người sử dụng của domain (domain user account).

Nhóm toàn cục có thể được gán quyền cho tài nguyên bất kỳ trong vùng mà chúng được xác định.

Nhóm toàn cục có thể được gán quyền đến các tài nguyên trong vùng khác với vùng chúng được xác định khi quan hệ tin cậy (trust relationship) giữa các vùng có hiệu lực.

Các thành viên của nhóm toàn cục có thể sử dụng nguồn tài nguyên trong vùng bất kỳ mà nhóm toàn cục có quyền.

Nhóm toàn cục chỉ chứa mã số của người sử dụng trong Domain của nó. Nó không thể chứa các nhóm cục bộ và nhóm toàn cục khác.

6. Nhóm cục bộ (local group)

Nhóm cục bộ, trái lại, được gán quyền cho nguồn tài nguyên trên máy NT mà nó được xác định. Nếu máy NT là một phần của vùng, thì để tiện cho việc gán quyền, một nhóm cục bộ có thể chứa các tài khoản người dùng cấp vùng (domain user account) và các nhóm toàn cục trong Domain đó, nơi máy tính NT là thành viên, hoặc những người dùng từ Domain được tin cậy. Các người dùng cấp vùng (domain user) có thể được gán quyền truy cập đến tài nguyên bất kỳ trong Domain đó.

Nếu Windows NT computer không nối với mạng thì các thành viên trong local group có thể được gán quyền để truy xuất đến tài nguyên trên máy tính mà trong đó các thành viên được tạo ra còn nếu Windows NT computer nối vào mạng thì để tiện lợi cho việc phân quyền thì người quản trị mạng có thể đưa global group và domain user vào trong local group .

Có hai loại nhóm cục bộ: ***nhóm cục bộ trạm làm việc (workstation local group)*** và ***nhóm cục bộ vùng (domain local group).*** Một mạng làm việc theo cơ chế vùng bao gồm cả Windows NT Server và Windows NT Workstation việc hiểu rõ sự khác nhau giữa hai loại nhóm cục bộ là rất quan trọng.

a. Nhóm cục bộ trạm làm việc (Workstation local group):

Nhóm cục bộ trạm làm việc hiện diện trên Windows NT Workstation trên đó chúng được tạo ra. Chúng được chứa trong dữ liệu SAM lưu trữ trên Windows NT Workstation. Một người dùng cục bộ được tạo ra bằng công cụ *User Manager* của Windows NT Workstation (khác với

công cụ *User Manager for Domains* trên Windows NT Server) có thể có quan hệ thành viên chỉ trong nhóm cục bộ của trạm làm việc đó. Một nhóm cục bộ trong một trạm làm việc chỉ có thể được dùng trên máy tính trên đó nhóm được tạo ra, và không thể làm việc rên bất kỳ máy Windows NT nào khác.

Nhóm cục bộ trạm làm việc có thể chứa:

Các tài khoản người dùng cục bộ từ trạm làm việc trên đó nó được xác định.

Các tái khoản người dùng cấp vùng (domain user account) và các nhóm toàn cục từ vùng trong đó họ được xác định.

Các tái khoản người dùng cấp vùng (domain user account) và các nhóm toàn cục từ các vùngï được ủy quyền.

b. Nhóm cục bộ vùng (Domain local group):

Nhóm cục bộ vùng hoạt động trên Windows NT Server ở mức vùng, và được tạo ra bằng *User Manager for Domains* (trên Windows NT Server). Các nhóm cục bộ vùng chỉ có thể hiện hữu trên máy Windows NT Server tạo ra nó. Do đó, các nhóm cục bộ vùng có thể dùng để truy cập nguồn tài nguyên trên máy tính Windows NT Server trong vùng đó, mà không dùng để truy cập nguồn tài nguyên trên máy tính Windows NT Workstation trong vùng này. Nhóm cục bộ vùng không thể được gán quyền trên bộ điều khiển không có cấp vùng, thậm chí cả các máy chủ.

III. Các mô hình Domain trong mạng Windows NT

Windows NT máy chủ cung cấp 4 kiểu tổ chức domain gọi tắt là các mô hình domain (domain models). Dưới đây là 4 mô hình tổ chức của nó:

1. Mô hình Domain đơn (single domain)

Mô hình domain đơn là mô hình trong mạng chỉ có một domain. Mô hình này thích hợp cho mạng ít người khai thác, cần quản lý tập trung. Mô hình đơn nói chung tương tự như mô hình workgroup, trong mô hình này người sử dụng có thể xem xét, khai thác tài nguyên theo cả mô hình workgroup và mô hình domain.

Loại mô hình này không có các quan hệ ủy quyền vì chỉ có một domain duy nhất, domain này cũng chứa CSDL SAM cho toàn bộ mạng và việc quản trị mạng có thể thực hiện từ một vị trí trung tâm.

Các tài khoản người dùng trong vùng (domain user account) và tài khoản nhóm trong vùng (domain group acconunt) có thể được xây dựng và có các quyền truy cập tài nguyên được gán trên các nhóm và người dùng riêng rẽ và có một phạm vi bao gồm tất cả các máy vi tính trong vùng.

Trong mô hình Domain đơn vấn đề an toàn dữ liệu, quản lý hệ thống được xem xét một cách tốt hơn so với Workgroup.

2. Mô hình Domain chính (Master domain)

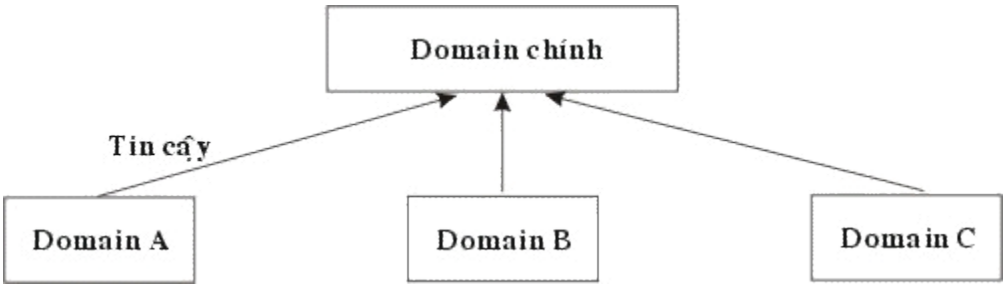
Mô hình Domain chính có thể được sử dụng cho các cơ quan khi họ muốn tổ chức mạng thành nhiều Domain tài nguyên (Resource domain) nhưng vẫn có những tiện lợi trong việc quản lý tập trung. Bằng cách phân chia tài nguyên mạng vào nhiều Domain, chúng ta sẽ tiện tổ chức và quản lý một lượng tài nguyên lớn. Một Domain chủ (master domain) được sử dụng để hỗ trợ việc quản trị tập trung mà trong đó tất cả mã số của người sử dụng và mã số các nhóm toàn cục (global group) trên mạng được lưu giữ.

Đặc điểm của mô hình domain chính :

Mô hình Master Domain là mô hình có nhiều Domain, trong đó có 1 Domain là Domain chính (premery domain). Mô hình này thích hợp cho mạng có số người dùng không quá lớn, nhưng cần phải phân chia thành các đơn vị nhỏ hơn nhưng việc quản lý được tiến hành tập trung.

Trong mô hình này tất cả mã số của người khai thác mạng và mã số của các nhóm toàn cục (global group) đều chứa trên server trên Domain chính.

Trong mô hình này tất cả các khác Domain đều tin cậy với Domain chính.



Hình 11.2: Mô hình Domain chính

Trong mô hình này mã số của người sử dụng quản lý tập trung và các nhóm toàn cục chỉ cần xác định một lần trong Domain chính. Tài nguyên được nhóm logic thành các đơn vị nhỏ hơn để có thể quản lý bởi từng Domain.

Mô hình Domain chính là mô hình quản lý tập trung vì vậy chiến lược phát triển mạng cần dựa vào các nhóm cục bộ và các nhóm toàn cục.

Mô hình này không những quản lý tập trung các mã số của người sử dụng mà còn cung cấp các dịch vụ như cài đặt phần mềm, sao chép backup cho tất cả các máy chủ trên mạng.

Tuy nhiên mô hình này có nhược điểm có thể gây ùn tắc nếu có quá nhiều nhóm và nhiều người dùng và các nhóm cục bộ cần phải xác định trong mỗi Domain mà chúng được sử dụng.

3. Mô hình nhiều Domain chính (muliple master domain)

Mô hình **nhiều Domain chính** (muliple master domain) có thể được sử dụng cho các tổ chức có nhiều khu vực và mỗi khu vực có nhiều bộ phận. Trong nhiều mạng kiểu như vậy, bộ phận điều hành riêng biệt cho mỗi khu vực muốn quản lý tập trung các tài nguyên mạng trong khu vực. Chúng ta xây dựng một Domain chủ (master domain) cho mỗi khu vực và chia các tài nguyên trong mỗi khu vực thành nhiều Domain tài nguyên (resoure domain) riêng biệt.

Trên mô hình này tồn tại các quan hệ sau:

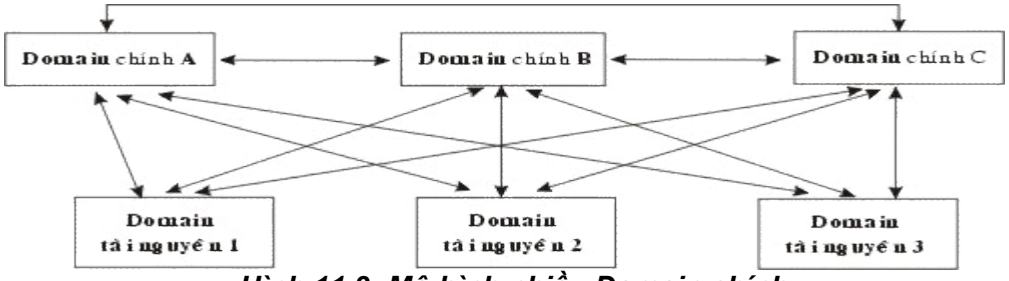
Mỗi Domain chính quan hệ tin cậy hai chiều với các domain chính khác. Điều này cho phép mỗi Domain chính có thể quản lý các domain chính khác.

Các Domain không phải là chính không có mã số của người sử dụng mà chỉ cung cấp tài nguyên trên mạng.

Các Domain không phải là chính tin cậy đối với tất cả các Domain chính. Nhờ điều này mỗi mã số của người sử dụng sẽ được sử dụng trên tất cả các Domain chính và có được quyền truy nhập vào tài nguyên trong các tài nguyên trên các Domain khác của mạng.

Bằng cách phân chia tài nguyên mạng thành nhiều Domain, chúng ta có nhiều thuận lợi trong việc tổ chức quản lý một số lượng lớn các tài nguyên trong các đơn vị phù hợp.

Mô hình nhiều Domain chính có ưu điểm đối với mạng nhiều người dùng trong đó các tài nguyên được nhóm một cách logic theo công việc. Tuy nhiên các nhóm cục bộ và toàn cục phải xác định nhiều lần và mã số của người sử dụng phải chứa ở nhiều Domain chính .

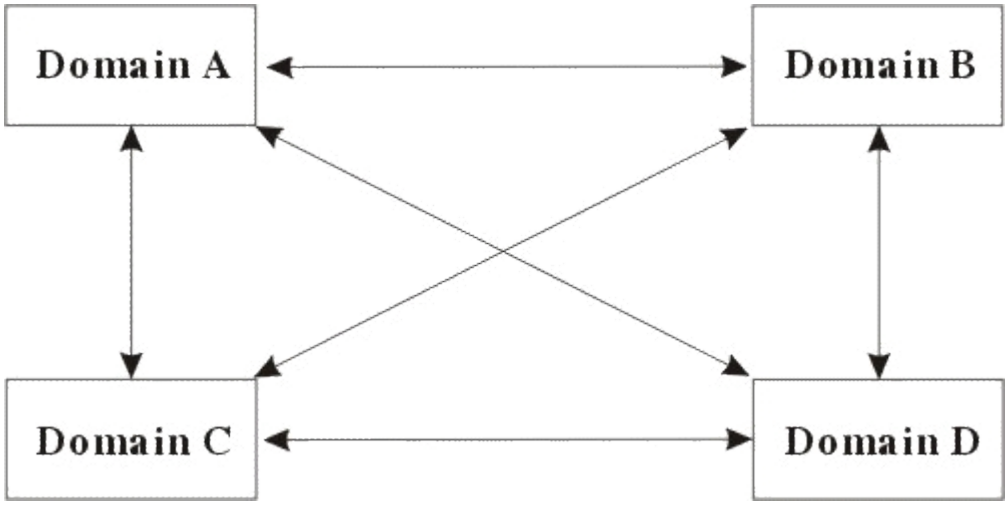


Hình 11.3: Mô hình nhiều Domain chính

4. Mô hình tin cậy hoàn toàn (complete trust)

Mô hình tin cậy hoàn toàn là mô hình mà trong đó mỗi Domain là quan hệ tin cậy 2 chiều với các Domain khác. Với mô hình này, người sử dụng có thể truy nhập vào bất kỳ Domain nào trên mạng từ một máy trạm nào đó.

Mô hình này có thể áp dụng với qui mô mạng tùy ý và phù hợp cho các cơ quan không có nhóm quản trị tập trung, nó cho phép không hạn chế số người khai thác mạng và số nhóm. Mỗi bộ phận trong đơn vị có thể kiểm soát được mã số của người sử dụng cũng như tài nguyên của bộ phận mình trong đó tài nguyên và mã số người sử dụng được nhóm thành một Domain.



Hình 11.4: Mô hình nhiều Mô hình tin cậy hoàn toàn

IV. Các mặt hạn chế của những mô hình Domain

Mô hình vùng có một số kẽ hở về cấu trúc. Những hạn chế về domain được thảo luận ở đây nhằm mục đích giúp bạn thiết kế mạng chính xác và hoàn hảo.

Domain NT đơn điệu theo nghĩa là không có cách nào diễn tả quan hệ phân cấp hoặc nhóm tài nguyên trong một vùng đơn. Người dùng có thể sử dụng những quyền được ủy thác thể hiện các quan hệ giữa những vùng, nhưng đây là quan hệ sử dụng và không thích hợp cho việc tổ chức mạng dựa trên phạm vi địa lý, tài nguyên sở hữu, logic hoặc nền tảng sơ đồ tổ chức.

Mô hình vùng Domain chính duy nhất theo Microsoft thích hợp cho các mạng ít hơn 40.000 người dùng và nhóm. Khi số người dùng và nhóm tăng lên, số quan hệ ủy quyền và chi phí quản lý quan hệ cũng tăng. Nói cách khác chi phí quản lý mạng có thể tăng bất thình lình khi kích thước mạng tăng.

Người dùng phải cẩn trọng về kẻ hở của quan hệ ủy quyền - đặc biệt quan hệ ủy quyền hai chiều. Nếu không cẩn thận trong việc gán các quan hệ ủy quyền và không có kế hoạch đúng đắn, người sử dụng có thể kết thúc bằng một mô hình ủy quyền trọn vẹn, với tất cả những hạn chế của mô hình đi kèm.

Ngoài ra có một nguy cơ thực sự sẽ xảy ra là người cài đặt mạng có thể cài đặt một mạng hoạt động tốt trong thời gian ngắn còn khi mạng hoạt động dài hạn này sẽ ù nảy sinh vấn đề về mặt chính sách là ai ủy quyền cho ai.

Chương 12

Cài đặt, quản trị, sử dụng mạng Windows NT

I. Cài đặt hệ điều hành mạng Windows NT server

Trước khi cài đặt mạng Windows NT thì cũng giống như cài các hệ điều hành khác chúng ta phải cắm card mạng vào máy, thiết lập mạng và đảm bảo nó được hoạt động tốt. Khi cài chúng ta có thể sử dụng phần mềm trên đĩa CD ROM (nếu máy của chúng ta là PC thì chúng ta sử dụng thư mục I386) hoặc chúng ta chép thư mục I386 lên đĩa cứng trước khi cài đặt. Để cài đặt Windows NT ta và trong thư mục I386 và chạy lệnh "WINNT"

Chú ý trong trường hợp này chương trình sẽ yêu cầu chuẩn bị 3 đĩa mềm loại 1.44Mb để cài các chương trình khởi động cần thiết và trong quá trình cài đặt các đĩa mềm trên sẽ được sử dụng. Nếu ta không muốn thì thực hiện lệnh "WINNT /B" và phải chỉ đường dẫn của chương trình nguồn như d:\I386.

Yêu cầu về phần cứng cho việc cài đặt windows NT

Thiết bị phần cứng	Yêu cầu
Processor	Intel 486, Pentium, Pentium Pro, những hệ thống chạy trên RISC (Ex: MIPS R4x00, DEC s Alpha AXP). Windows NT hỗ trợ lên đến 4 CPU ở Mode Symmetriccal Multi-Processing
Display device	VGA hay những thiêt bị có độ phân giải cao hơn
Hard disk	Tối thiểu phải có 110 MB Hard Disk còn trống trong suốt quá trình cài đặt
Floppy disk	31/2 inch hay 51/4 inch
CD-ROM	CD-ROM drive hay đĩa CD-ROM mà ta có thể truy xuất được thông qua đường mạng
Network adapter	Một hay nhiều card mạng, card mạng không có cũng được nhưng chức năng mạng sẽ không có
Memory	NT khuyến cáo ít nhất phải có 16 MB Ram cho cả hai hệ thống chạy trên Intel và RISC

Khi cài đặt chúng ta tuân theo những yêu cầu của chương trình đòi hỏi, một điểm quan trọng là Windows NT luôn luôn thông báo và chỉ dẫn cho người cài đặt khi cần phải thực hiện một điểm gì. Sau đây là tóm tắt các bước cài đặt chính :

1) Boot máy bằng đia Windows NT setup hay dùng lệnh WINNT /B từ thư mục I386 trên đĩa CD-ROM. Nếu cài UPGRATE dùng lệnh WINNT32

2) Xác định lại hay nếu cần thiết thay đổi các thành phần Hardware và Software mà quá trình Setup nhận diện ra

3) Chọn Partition mà hệ điều hành Windows NT sẽ được cài đặt lên. Phải quyết định việc file hệ thống sẽ được định dạng theo kiểu nào FAT hay NTFS

4) Format bảng Partition đã lựa chọn

5) Chọn lựa thư mục mà các file của hệ điều hành Windows NT sẽ đuộc cài đặt lên đó

6) Nhập vào tên và công ty

7) Chọn License Mode. Chọn Per server hay Per seat

8) Nhập vào tên máy tính và tên này phải là duy nhất

9) Quyết định vai trò của file server trên mạng (Primary Domain Controller, Back Up Domain Controller, Stand-Alone Server)

10) Nhập Password cho người quản trị mạng Administrator

11) Lựa chọn Option để tạo ra các đĩa Emergency Repair Disk

12) Chọn các thành phần để install như là: Accessibility Option, Accessories, Communication, Games, Microsoft Exchace, And Multimedia

13) Quyết định kiểu kết nối máy tính vào mạng (kết nối bằng đường dây mạng hay bằng remote access)

14) Chọn Install Microsoft Internet Information Server

15) Quyết định phương pháp dò tìm card mạng (autodetect hay manual). Một số crad mạng như Xircom Credit Card và Xircom Pocket Ethernet chỉ có thể dùng phương pháp manual

16) Lựa chọn phương thức truyền trên mạng network protocol (TCP/IP Protocol, Nwlink IPX/SPX Compatible Transport và Netbeui Protocol)

17) Chọn lựa các dịnh vụ trên mạng. Các dịch vụ như là Microsoft Internet Information server, RPC Configuration, Netbios Interface, Workstation, Server.

18) Nhập vào cá thông số của card mạng như IRQ, địa chỉ IO port, DMA.

19) Nếu chọn Nwlink IPX/SPX hay TCP/IP Tranposrt Protocol thì phải định cấu hình cho chúng

20) Nếu chọn Primary Domain Controller thì phải nhập tên Computer và tên của Domain mà PDC sẽ quản lý.

21) Nếu cài Internet Information Server thì phải định cấu hình cho nó

22) Chọn Date/Time.

23) Chọn chế độ màn hình

24) Tạo đĩa Emergency Repair Disk

Khi cài đặt Windows NT chú ý những điểm sau:

Lựa chọn khuôn dạng của hệ thống sắp xếp file trên đĩa trong đó Windows NT cho phép chúng ta lựa chọn thay đổi sang hệ thống sắp xếp file của NT (NTFS) hoặc duy trì hệ thống sắp xếp file cũ của DOS (FAT). Hệ thống sắp xếp file của NT có tên là NTFS - New Technology File System có những ưu điểm như như chấp nhận tên file dài tới 256 ký tự, nó có đảm bảo an toàn trên máy chủ bằng cách không cho những người không có thẩm quyền vượt qua khi họ khởi động máy chủ bằng đĩa mềm.

Lựa chọn số người tối đa có thể thâm nhập vào hệ thống cùng một lúc (Windows NT không hạn chế số người tối đa vào trong mạng tuy nhiên để đảm bảo sử dụng tài nguyên hợp lý chúng ta phải quy định số người tối đa có thể vào một lúc)

Lựa chọn kiểm máy chủ, Windows NT cho phép chúng ta lựa chọn 3 kiểu máy chủ:

Primary Domain Controller: trong trường hợp mạng sử dụng quản trị theo vùng thì mỗi vùng phải có duy nhất một máy chủ làm nhiệm vụ trên. và trên đó sẽ lưu dự trữ cơ sở dữ liệu quản trị vùng (SAM) và hệ thống quản trị hoạt động khi mạng hoạt động

Backup Domain Controller: trong trường hợp mạng sử dụng quản trị theo vùng, ngoài máy chủ kiểu Primary Domain Controller có thể có một vài máy chủ lựa chọn kiểu này và trên đó sẽ lưu dự trữ cơ sở dữ liệu quản trị vùng (SAM) và được sử dụng khi máy chủ Primary Domain Controller có trụ trặc.

Stand - Alone Server: trong trường hợp mạng sử dụng quản trị theo nhóm thì máy chủ phải lựa chọn kiểu này, ngoài ra trong trường hợp mạng sử dụng quản trị theo vùng máy chủ có thể lựa chon này khi trong mạng đã có máy chủ Primary Domain Controller. Trong trường hợp này trên máy chủ không cơ sở dữ liệu quản trị Domain.

BẢNG SO SÁNH GIỮA FAT VÀ NTFS

FEATURE	FAT	NTFS
File Name	8 cộng 3 ký tự mở rộng chỉ được phép có một dấu chấm	255 ký tụ, 16 bit unicode cho phép có nhiều dấu chấm
Maximum Path Name	64	Không giới hạn
File Size	2^{32} bytes	2^{64} byte
Partition	2^{32} bytes	2^{64} byte
Directory	Không được sắp xếp	Theo cấu trúc B-Tree
Attribute	Có một vài bit cờ	Tất cả các thông tin bao gồm cả dữ liệu đều có thuộc tính
Cho phép bảo mật về thư mục và file ngay trong kiểu Format	Không	Có
Giải pháp thiết kế	Đơn giản	Truy xuất nhanh với khả năng bảo mật và phục hồi

Lựa chọn loại card mạng, ngắt, địa chỉ port của card mạng.

Lựa chọn các giao thức truyền thông cho hệ thống mạng như trong hộp Windows NT

Server setup

Hình 12.1: Chọn lựa giao thức truyền thông

Giao thức TCP/IP: Nếu ta muốn kết nối Windows NT với Internet hay với các máy chạy trên hệ điều hành Unix thì phải chọn TCP/IP Protocol. (Có thể chọn lựa giao thức này sau khi đã cài đặt xong Windows NT).

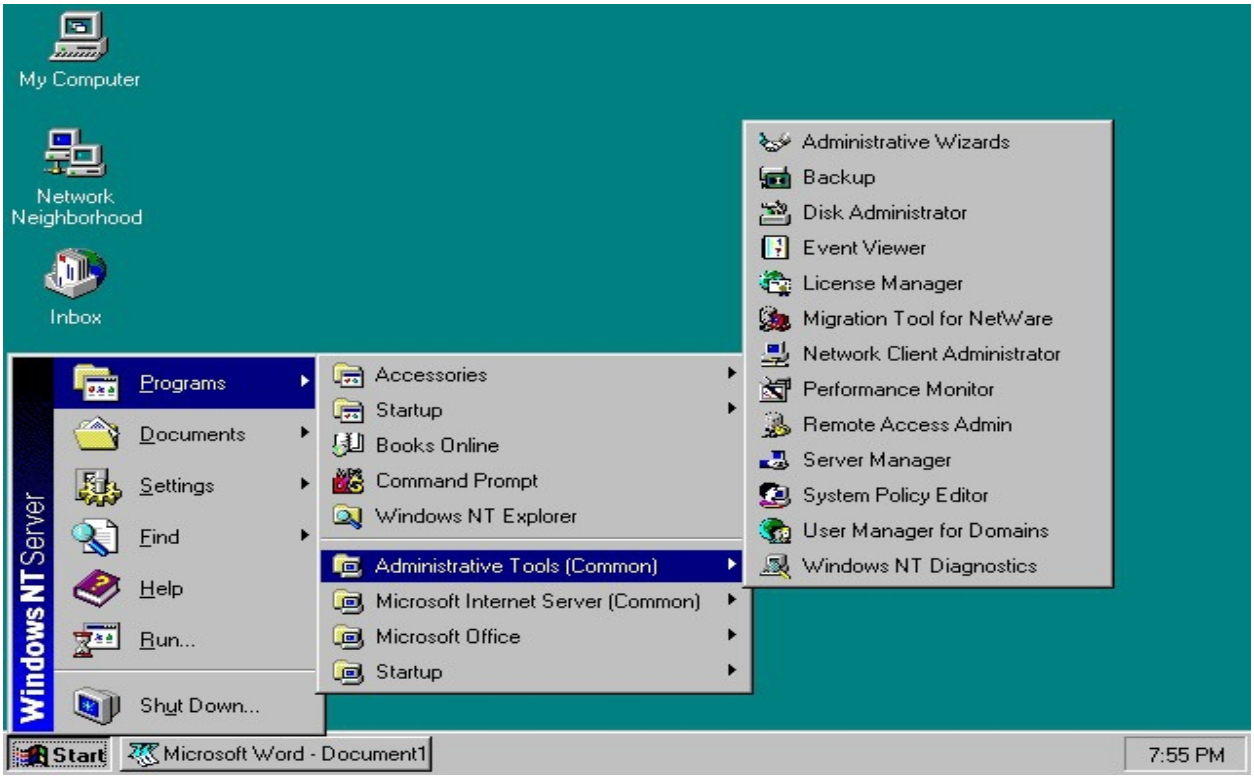
Giao thức NetBEUI: Là giao thức gốc của Windows NT. Nếu File server kết nối với các máy con trên mạng mà sử dụng giao thức NetBEUI thì phải chọn giao thức này.

Giao thức IPX/SPX: Là giao thức được dùng cho những ứng dụng chạy trên Netware.

Lựa chọn tên vùng mà máy chủ tham gia, nếu máy chủ là Primary Domain Controller thì một vùng mới được thiết lập, nếu không thì tên vùng phải là một vùng đã có.

II. Quản trị mạng Windows NT

Người quản trị mạng Windows NT có các công cụ có thể kiểm soát một cách chính xác đối với việc thâm nhập vào file và thư mục của các người sử dụng. Windows NT đưa vào một loạt các công cụ giúp ta quản lý máy tính. Muốn dùng công cụ này, ta nhắp nút Start, trỏ vào mục program và sau đó chọn menu Administrative Tool (Common) như hình sau.



Hình 12.2: Các công cụ quản trị mạng trong Windows NT Server

Để sử dụng bất kỳ một công cụ nào trong Administrative Tool, ta đều phải vào mạng với quyền của người quản trị mạng.

Tóm tắt các công cụ của người quản trị mạng

Biểu tượng	Menu	Ý nghĩa
	Administrative Wizards	Công cụ này giúp ta thực hiện công việc một cách dễ dàng. ta có thể dùng nó để thêm một mã số mới của người sử dụng, đặt chế độ an toàn cho các file, folder, các folder dùng chung, tạo, sửa các nhóm người sử dụng và kiểm tra tính đúng đắn của sản phẩm đã cài đặt (license).
	Backup	Là công cụ dùng để sao chép dự phòng các thông tin trên máy tính vào băng từ để phòng sự cố.
	Disk Administrator	Là công cụ cho phép quản lý tài nguyên trên đĩa. Dùng công cụ này để tạo ra các thay đổi trên đĩa cứng hoặc bảng partition trên đĩa cứng nắp thêm.

	Event Viewer	Trong Windows NT, một sự kiện là một biến cố quan trọng nào đó xảy ra trong hệ thống hoặc trong chương trình mà nó yêu cầu phải được lưu ý. Công cụ này lưu ý ta về các sự kiện trong khi vào mạng.
	License Manager	Công cụ này cho phép ta kiểm tra license trên các trạm và trên các server.
	Network Client Administrator	*Network Client Administraor*: Sử dụng Network Client Administraor để cà đặt (Install) hay cập nhật (update network client) cho các máy trạm.
	Performance Monitor	Là công cụ phản ánh quá trình thực hiện trên máy tính của ta và các máy tính khác trên mạng.
	Remote Access Admin	Dùng công cụ này để kiểm tra quá trình nhập từ xa vàp server, xem xét người sử dụng, cài đặt mã số của người sử dụng, màn hình của những máy truy nhập từ xa.
	Server Manager	Dùng công cụ này để hiện danh sách các máy trạm, các server trong Domain.
	System Policy Editor	Cho ta khả năng kiểm tra việc cài đặt môi trường sử dụng trong Windows NT và Windows 95. Công cụ này thay đổi cách cài đặt và đăng ký người sử dụng nào có thể làm công việc thay đổi này.
	User Manager for Domains	Công cụ này cho phép ta thiết lập, xóa các mã số của người sử dụng khỏ domain. Với công cụ này, ta có thể đặt phương án an toàn, thêm mã số của người sử dụng vào nhóm.
	Windows NT Diagnostics	Hiển thị các thông tin về tài nguyên của máy tính.

Người sử dụng trong mạng được tạo ra bởi người quản trị mạng, mỗi người sử dụng có tài khoản (account) riêng của từng người và những tài khoản này cũng do người quản trị mạng tạo ra có thể bao gồm các giới hạn :

***Giới hạn của Login*:** Người quản trị mạng có thể kiểm soát xem người sử dụng có thể thâm nhập vào mạng như thế nào. Ở đây người sử dụng có thể được đặt cho một thời hạn nhất định thì phải thay mật khẩu và kích thước tối thiểu của mật khẩu và có thể tự thay mật khẩu hay không.

***Hạn chế về thời gian*:** Người quản trị mạng có thể hạn chế người sử dụng thâm nhập vào trong mạng trong những khoảng thời gian nhất định trong một ngày. Điều đó có thể hạn chế việc vào trong mạng trong những khoảng thời gian khó kiểm soát được như là buổi tối, giờ nghỉ v.v. Khi người sử dụng đang chạy trong mạng mà đã đến thời gian hạn chế thì họ sẽ được nhận thông báo là cần phải ra khỏi mạng. Nếu họ bỏ ra ngòai tai thông báo đó thì sẽ tự động bị đưa ra khỏi mạng.

***Hạn chế về địa chỉ*:** Người quản trị mạng có thể xác định những địa chỉ mà người sử dụng được phép thâm nhập. Điều đó có thể hạn chế người sử dụng vào trong mạng bằng máy của người khác. Để làm được điều này người quản trị mạng cần phải biết địa chỉ mạng và mã số của card mạng trên trạm. Địa chỉ mạng là địa chỉ của phần mềm mạng và được cho khi mà giao thức mạng được liên kết với chương trìng quản lý card mạng, Mã số của thiết bị phần cứng là mã số của bản thân card mạng khi được chế tạo và khi đó người quản trị mạng sẽ lựa chọn những chặng nào mà người sử dụng được phép dùng.

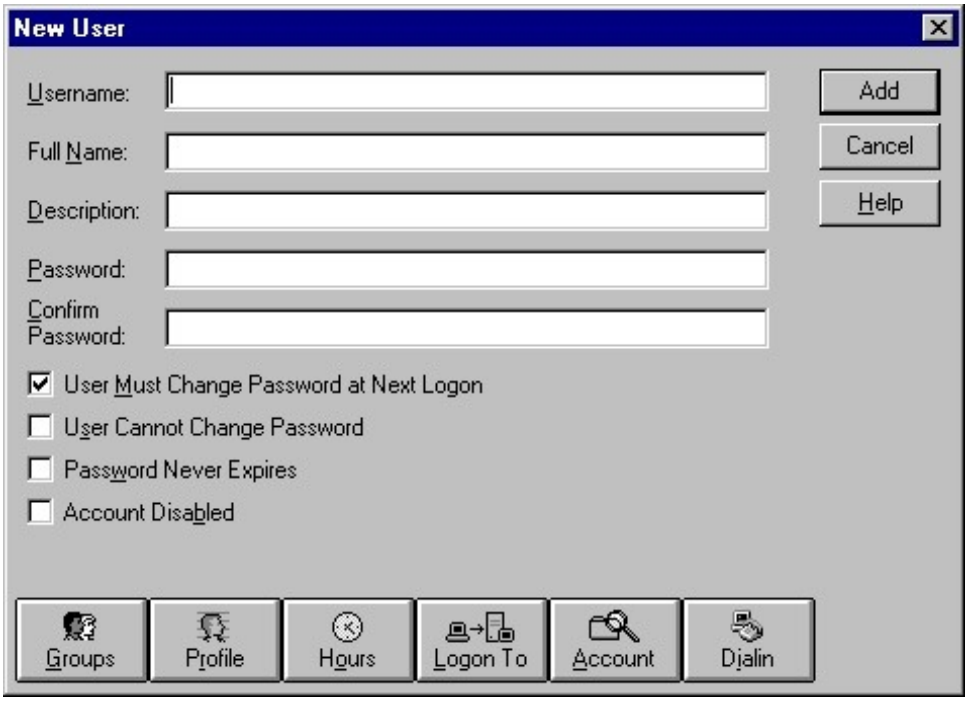
***Quyền của người sử dụng*:** Để xác định được quyền hạn của người sử dụng trên mạng chúng ta phải lựa chọn nhóm với những quyền đã định trước.

Khai báo người sử dụng:

1) Login vào mạng bằng tên administrator

2) Chọn Start, chọn Program, chọn Administrator Tool, chọn Users Manager for Domain sẽ thấy xuất hiện màn hình User Manager

3) Chọn User, New User. Hộp hội thoại New User sẽ xuất hiện:

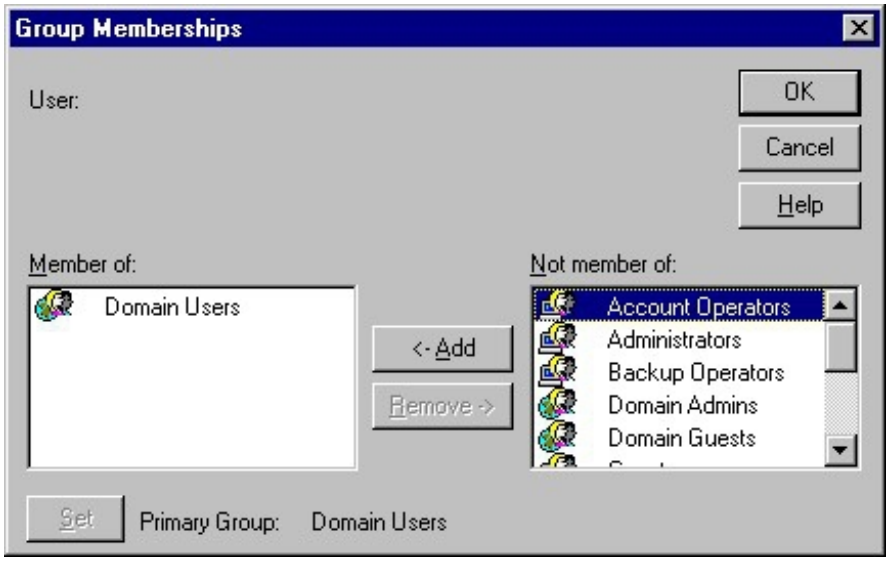


Hình 12.3: Thêm một người sử dụng vào hệ thống

4) Nhập vào thông tin về người sử dụng cần tạo như yêu cầu (tên trong mục Name, tên đầy đủ trong mục Fullname, lời mô tả về người sử dụng đó trong mục Description, mật khẩu trong mục Password và Confirm Password)

5) Đưa người sử dụng mới tạo vào một nhóm nào đó phù hợp với yêu cầu của người sử dụng đo. Để thực hiện điều này chọn Groups, màn hình Group memberships sẽ hiện ra. Để ý rằng user mới ban đầu là thành viên của Domain users. Chọn nhóm mà muốn người sử dụng mới tạo được tham gia và bấm nút Add. Ta có thể chọn nhiều nhóm cùng lúc

6) Để thay đổi thời gian được phép vào mạng của người sử dụng thì từ màn hình New User chọn nút Hours. Màn hình Logon Hour sẽ xuất hiện dưới hình thức thời khóa biểu trong tuần. Sau đó ta có thể chọn ngày nào, giờ nào trong tuần mà user đó được phép login vào mạng bằng cách cho ngời sáng những vị trí đó trong thời khóa biểu và chọn nút Allow hoặc Disallow.



Hình 12.4:Nhóm làm việc

7) Để giới hạn trạm làm việc đối với người sử dụng chọn nút Logon To. Màn hình Logon Worstation sẽ xuất hiện. Để giới hạn người sử dụng chỉ có thể vào mạng từ workstation nào ta gõ tên của workstation đó vào các ô được đánh số từ 1 đến 8 và nhấn OK.

8) Để định ngày hết hạn được vào mạng của người sử dụng chọn nút Account. Khung hội thoại Account information sẽ hiện ra để ta có thể định ngày hết hạn. Ban đầu thì account không bao giờ hết hạn. Nếu muốn set ngày hết hạn thì vào trường End of.

9) Để tạo môi trường làm việc cho từng người sử dụng trên mạng ta bấm nút Profile. Màn hình User Environment Profile sẽ hiện ra ta có thể sử dụng mục này để tạo Profile cho từng user và home directory cho từng người sử dụng.

10) Sau đó bấm OK để lưu các thông tin của người sử dụng đó.

11) Đối với những người sử dụng đã có saün người điều hành có thể sử dụng công cụ User Manager for Domains để thay đổi, bổ xung, lựa chọn những đặc tính trên.

2. Quyền của người sử dụng trong Windows NT

Mỗi một người sử dụng muốn đăng nhập vào trong mạng cần phải được khai báo tên và một mật khẩu riêng. Chỉ khi người sử dụng vào đúng tên và mật khẩu của mình thì họ mới thâm nhập vào trong mạng. Tuy nhiên để người đó có thể khai thác được mạng thi người đó phải có các quyền. Trong Windows NT có những khái niệm về quyền như sau:

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

***User right (quyền người dùng)*:** tức là quyền của người sử dụng đó ở trên mạng, quyền này khác với quyền của người sử dụng trên thư mục hay file. Các người sử dụng này có thể không hề có bất cứ một quyền hạn nào trên thư mục hay file mà chỉ có những quyền ví dụ như tắt (shutting down) hệ thống, back up và hồi phục dữ liệu. Như vậy các người sử dụng này sẽ thuộc về một trong những Domain Local Group (ví dụ: nếu người sử dụng đó có quyền Backup data thì người sử dụng này sẽ thuộc về nhóm Backup Operators)

***Bilt-in capabilities (khả năng thiết lập)*:** tức là khả năng có saün của người sử dụng, khả năng không thể thay đổi được.

Trong mạng Windows NT có các quyền người dùng (User right) sau:

***Log on locally*:** người sử dụng có thể được truy nhập từ máy chủ.

***Shutdown the system*:** người sử dụng có thể shutdows hệ thống trực tiếp từ máy chủ.

***Access this computer from network*:** cho phép truy nhập nào tài nguyên của người sử dụng đang phân quyền từ máy khác trên mạng (có thể truy nhập từ máy Client vào người sử dụng này).

***Backup file and Directories*:** có quyền lưu trữ các file và thư mục.

***Restorre file and directories*:** có quyền phục hồi lại các file và thư mục từ lưu trữ.

***Change the system time*:** có quyền thay đổi đồng hồ của hệ thống.

***Force shutdown from a remote system*:** người sử dụng này có thể shutdows hệ thống từ xa.

***Load and unload device drivers*:** cho phép nạp hay không chương trình điều khiển ổ đĩa.

***Manager auditting and security log*:** quyền truy xuất mã số (accound) và sự an toàn khi truy nhập mạng.

***Take ownership of files or other obiects*:** dành cho các quan hệ riêng của các file và các đối tượng khác (them các thành phần, đối tượng khác).

Người điều hành có thể sử dụng công cụ User Manager for Domains để thay đổi, bổ xung, lựa chọn những quyền trên cho người sử dụng.

Ngoài ra trong mạng Windows NT có các khả năng thiết lập (Bilt-in capabilities) sau:

Create and manage users: tạo và quản lý tài khoản người dùng.

Create and manage global group: Tạo và quản lý nhóm toàn cục

Create and manage local groups: Tạo và quản lý nhóm cục bộ.

Assign user rights: cho phép gán quyền cho người dùng.

Manage and auditing of system events: Quản lý và kiểm định các sự kiện của hệ thống.

Lock Server: Cho phép khóa máy chủ.

Override lock of server: Cho phép mở khóa máy chủ.

Format server s hard drive: Cho phép Format lại ổ đĩa máy chủ.

Create common program group: Cho phép tạo ra các nhóm chương trình chung.

Keep local profile: Duy trì các hệ lưu trữ cục bộ.

Share and stop share directories: Chia sẻ và ngừng chia sẻ các thư mục.

Share and stop share printer: Chia sẻ và ngừng chia sẻ máy in.

3. Tạo nhóm (Group) trong Windows NT:

Người quản trị mạng có thể tạo ra các nhóm với công cụ User Manager for Domain như sau:

Tạo nhóm toàn cục:

1) Login vào mạng với tên

2) Khởi động User Manager for Domain. Màn hình User Manager for Domain sẽ hiện lên

3) Để tạo nhóm mới chọn User, New Global Group. Màn hình New Global Group xuất hiện

Hình 12.5: Thêm một nhóm toàn cục mới

Trong màn hình New Global Group nhập vaò tên của nhóm đó trong mục Group Name và lời mô tả về nhóm đó trong mục Description.

4) Sau khi hòan thành chọn OK để kết thúc

Tạo cục bộ (Local Group):

1) Login vào mạng với tên Administrator

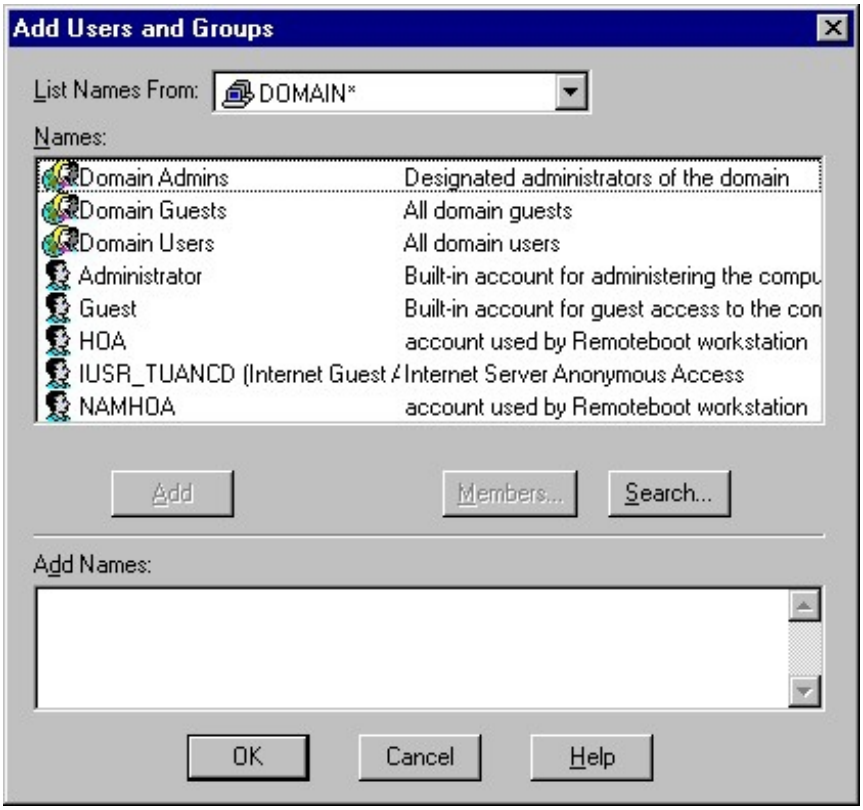
2) Khởi động User Manager for Domain. Màn hình User Manager for Domain sẽ hiện lên

3) Để tạo Local Group mới chọn User, New local Group. Màn hình New local Group xuất hiện

4) Trong màn hình New Global Group nhập tên của nhóm đó trong mục Group Name và lời mô tả về nhóm đó trong mục Description. Ta có thể click vào nút Show Full Names để hiện thị tên đầy đủ của các nhóm thành viên.

Hình 12.6: Thêm một nhóm cục bộ mới

5) Để thêm thành viên vào trong local group ta chọn nút Add. Màn hình sau sẽ hiện lên



Hình 12.7: Thêm một thành viên vào nhóm

6) Sau khi thêm các thành viên vào rồi chọn nút OK thì màn hình New Local Group sẽ liệt kê ra các thành viên mới:

7) Chọn OK để lưu Local Group

4. Các nhóm tạo saün trong Windows NT

Khi cài đặt một mạng Windows NT có những nhóm cục bộ và nhóm toàn cục (Domain) được thiết lập saün, người quản trị có thể cho người sử dụng tham gia vào các nhóm và như vậy họ có được các quyền một cách dễ dàng.

Các nhóm tạo saün trong Windows NT:

***Adminintrator Group*:** những thành viên nằm trong nhóm này có thể thực hiện hầu hết các chức năng quản lý trên Domain đó. Những chức năng quản lý này bao gồm tạo, xóa, quản lý local group, global group, gán quyền cho users, quản lý việc chia sẽ tài nguyên trên mạng, cài đặt hệ điều hành, format điã cứng của máy chủ.

Backup Operator: Những thành viên nào được đưa vào nhóm này có thể login vào máy chủ để thực hiện việc Back up và phục hồi dử liệu. Những users thuộc nhóm này có thể

thực hiện việc back up và hồi phục dử liệu ngay khi họ không có quyền read/ write trên thư mục hoặc file cần back up. Ngòai ra nhóm này cò có thể shutdown hệ thống.

Account Operator: Những thành viên nằm trong nhóm này có thể tạo, xóa, và quản lý hầu hết các users và nhóm trên mạng nhưng họ không có khả năng gán quyền cho users.

Guest: Những users nằm trong nhóm này bị giới hạn quyền họ chỉ có quyền truy xuất vào mạng thôi ngoài ra không còn quyền gì khác

Print operator: Những thành viên trong nhóm này có thể quản lý máy in mạng như tạo print server, share (đưa một tài nguyên nào đó lên mạng cho mọi người thấy để sử dụng) máy in, stop share máy in .

Server operator: Những thành viên nằm trong nhóm này có nhiều quyền giống như những users nằm trong nhóm Admintrator nhưng họ không thể quản lý việc bảo mật trên server. Họ có thể share, stop share maý in, thư mục và file, format điã cứng, họ cũng có thể back up và restore dữ liệu, shutdown hệ thống. Nhưng họ không thể start hay stop các dịch vụ trong mạmg

Domain Administrator: đây là global group và là thành viên của administrator local group nó chứa user administrator.

Domain Users: Khi một người sử dụng mới được tạo ra thì người sử dụng nằm trong nhóm domain users.

Domain Guest: Domain này lúc đầu tiên chứa domain users Domain này bị quản lý bởi Administrator và Account operator.

Sau đây là bảng phân quyền (user rights) đối với các nhóm được tạo trên

User Rights	Adminis -trator	Server Operator	Account Operator	Print Operator	Backup Operator	Every one	Users	Guest
Log on Localy	X	X	X	X	X			
Network access to this computer	X					X		
Manage Auditing and security log	X							
Change the system time	X	X						
Shut down the system	X	X	X	X	X			
Force the system down from remote system	X	X						
Back up files nd Directory	X	X			X			
Restore files and directory	X	X			X			
Load and Unload device drivers	X							
Add workstation to domain	X							

Khả năng được thiết lập saün (Built-in capabilities) của các nhóm:

Built-in capabilities	Adminis -trator	Server Operator	Account Opertor	Print Operator	Backup Operator	Every one	Users	Guest
Create and manage users	X		X					
Create and manage global group	X		X					
Create and manage local groups	X		X					
Assign user rights	X							
Manage and audit ing of system events	X							
Lock Server	X	X				X		
Override lock of server	X	X						
Format server s hard drive	X	X						
Create common program group	X	X						
Keep local profile	X	X	X	X	X			
Share and stop share directories	X							
Share and stop share printer	X	X		X				

5. User profile trong Windows NT

Khi một người thâm nhập vào mạng thì User Profiles của người đó là file chứa thông tin về môi trường làm việc. Khi người sử dụng tạo ra các thay đổi đối vời môi trường thì những thay đổi này được ghi vào profile và lần truy nhập sau môi trường mới được sử dụng. Ở các

máy workstation, các profile được tự động tạo ra cho người sử dụng, người quản trị mạng không có vai trò trong công việc này.

Khi người sử dụng ra khỏi mạng (log off) hệ thống sẽ ghi lại các thông số đã thay đổi, những thông số đó có thể là: máy có nối mạng hay không, các nhóm chương trình đang quản lý, kích thước windows, hình thức màn hình.

Các profile cục bộ không ảnh hưởng đếm máy khác. Trên máy chủ có thể tạo ra các profile cho người sử dụng ở các trạm nếu người sử dụng có mã số Domain và profile của họ chứa trên server. Một profile chuẩn trên server có thể dùng cho các máy trạm windows NT. Tính cục bộ và tên gọi của profile tương ứng mã số người sử dụng, mỗi người sử dụng chỉ có 1 profile.

Trong Domain có hai kiểu profile, kiểu profile cá nhân (Profile personal) và kiểu profile chuẩn (Profile Mandatory). Mỗi kiểu có profile ứng với file có đuôi chuẩn là URS và MAN

Profile cá nhân (Profile personal): Với profile cá nhân, trong mỗi ca làm việc, người sử dụng có thể tạo ra những thay đổi đối với môi trường làm việc. Nếu người sử dụng có profile các nhân là profile chuẩn trên server thì những thay đổi này được ghi lại để tạo ra môi trường mới trong ca làm việc sau. Các profiel cá nhân thường trùng với tên người sử dụng.

Mandatory Profile (Profile chuẩn): khi người sử dụng có Mandatory Profile thì mọi thay đổi về môi trường trong một ca làm việc sẽ không được ghi lại cho ca sau. Mandatory Profile co ích cho việc kiểm tra quá trình truy nhập vào môi trường.

Profile có 3 lợi ích chính đó là:

Bảo đảm cho người sử dụng vào máy trạm có môi trường như nhau mỗi khi họ vào mạng.

Người quản trị có thể tạo ra môi trường làm việc giống nhau cho nhiều người sử dụng, bằng cách tạo ra Profile chung cho nhóm những người sử dụng.

Nhờ Profile tính an toàn trên mạng cao hơn, bởi vì người sử dụng không thể tùy tiện thay đổi môi trường làm việc. Họ chỉ được thay đổi môi trường nếu họ được phép.

Trong Windows NT có 1 Profile hệ thống mặc định, còn gọi là Profile hệ thống chuẩn. Profile này dùng để xác định môi trường làm việc của máy chủ, nó không cho phép người sử dụng truy nhập vào. Chẳng hạn Profile hệ thống qui định chế độ màn hình, chế độ nền, chế độ ghi màn hình.

Muốn tạo ra hoặc thay đổi User Profile, chương trình tiện ích User Profile Editor sẽ giúp chúng ta làm công việc này. Mỗi lần Profile được tạo ra ta có thể dùng User manager Profile for Domain để gán Profile cho người sử dụng hoặc nhóm những người sử dụng. Khi Profile đã

được gán cho mã số của người sử dụng thì Profile chỉ được sửa 1 lần và sẽ nhìn thấy những thay đổi này ở lần vào mạng sau.

Chương 13 :

Quản lý và khai thác File, thư mục trong mạng Windows NT

Trong số các tài nguyên của mạng chia sẻ cho người sử dụng thông tin lưu trữ trên đĩa cứng của các máy chủ là tài nguyên quan trọng nhất. Không phải ngẫu nhiên mà cái tên "File server" trở nên rất quen thuộc với những người dùng mạng giống như "Network server". Tuy nhiên để làm sao có thể sử dụng, quản lý các tài nguyên đó một cách tốt nhất Windows NT cung cấp cho chúng ta một cơ chế quản lý và phương thức khai thác. Thông thường chúng ta phải khai báo các tài nguyên trước khi chúng được người sử dụng khai thác. Ngoài ra người sử dụng cũng được cung cấp quyền sử dụng một cách phù hợp.

I. Cơ chế an toàn của File và thư mục trong Windows NT

Quá trình truy cập tập tin (File hoặc thư mục) **trong Windows NT:** Khi một người sử dụng muốn truy cập một tập tin thì tất cả các thông tin về phương thức phục hồi giao dịch và phục hồi giao dịch khi bị lỗi sẽ được đăng ký bởi Log File Server. Nếu giao dịch thành công, tập tin đó sẽ truy xuất được, ngược lại giao dịch sẽđược phục hồi. Nếu có lỗi trong quá trình giao dịch, tiến trình giao dịch sẽ kết thúc.

Việc truy xuất tập tin (File hoặc thư mục) được quản lý thông qua các quyền truy cập (right), quyền đó sẽ quyết định ai có thể truy xuất và truy xuất đến tập tin đó với mức độ giới hạn nào. Những Quyền đó là Read, Execute, Delete, Write, Set Permission, Take Ownership.

Trong đó:

Read (R): Được đọc dữ liệu, các thuộc tính, chủ quyền của tập tin.

Execute (X): Được chạy tập tin.

Write (W): Được phép ghi hay thay đổi thuộc tính.

Delete (D): Được phép xóa tập tin.

Set Permission (P): Được phép thay đổi quyền hạn của tập tin.

Take Ownership (O): Được đặt quyền chủ sở hữu của tập tin.

Bảng tóm tắt các mức cho phép

Permission	R	X	W	D	P	O
No Access						
Read	X	X				
Change	X	X	X	X		
Full Control	X	X	X	X	X	X
Special Access	?	?	?	?	?	?

Để đảm bảo an toàn khi truy xuất đến tập tin (File và thư mục)ä, chúng ta có thể gán nhiều mức truy cập (permission) khác nhau đến các tập tin thông qua các quyền được gán trên tập tin. Có 5 mức truy cập được định nghĩa trước liên quan đến việc truy xuất tập tin (File và thư mục) là: No Access, Read, Change, FullControl, Special Access. Special Access được tạo bởi người quản trị cho bất cứ việc chọn đặt sự kết hợp của R, X, W, D, P, O. Những người có quyền hạn Full Control, P, O thì họ có quyền thay đổi việc gán các quyền hạn cho Special Access.

Khi một người quản trị mạng định dạng một partition trong Windows NT, hệ thống sẽ mặc định có cấp cho quyền Full Control tới partition đó cho nhóm Everyone. Điều này có nghĩa không hạn chế truy xuất của tất cả người dùng.

Tùy thuộc trên yêu cầu bảo mật cho các tập người quản lý sẽ cân nhắc việc xóa bỏ nhóm Everyone trong danh sách các quyền hạn sau khi định dạng hay hạn chế nhóm Everyone với quyền Read. Nếu sự hạn chế này là cần thiết, người quản trị nên cấp quyền hạn Full Control cho nhóm Administrators tới partition gốc.

Ở đây quyền truy cập được gán cho người sử dụng và nhóm người sử dụng do vậy quyền truy cập của một người sử dụng được tính bởi quyền hạn người đó và các nhóm mà người đó là thành viên. Khi người dùng đó truy xuất tài nguyên, các quyền hạn của người dùng được tính theo lối sau:

Những quyền hạn của ngươì dùng và các nhóm trùng nhau.

Nếu một trong những quyền là No Access thì quyền hạn chung là No Access.

Nếu những quyền hạn đã yêu cầu được liệt kê không rõ ràng trong danh sách các quyền hạn, yêu cầu truy xuất này là không chấp nhận.

Một người sử dụng thuộc hai nhóm, nếu một nhóm quyền hạn của người dùng là No Access, nó luôn được liệt kê đầu tiên trong danh sách Access Control List.

Quyền sở hữu của các tập tin: Người tạo ra tập tin đó có thể cho các nhóm khác hay người dùng khác khả năng làm quyền sở hữu. Administrator luôn có khả năng làm quyền sở hữu của các tập tin.

Nếu thành viên của nhóm Administrator có quyền sở hữu một tập tin thì nhóm những Aministrator trở thành chủ nhân. Nếu người dùng không phải là thành viên của nhóm Administrator có quyền sở hữu thì chỉ người dùng đó là chủ nhân.

Những chủ nhân của tập tin có quyền điều khiển của tập tin đó và có thể luôn luôn thay đổi các quyền hạn. Trong File Manager, dưới Security Menu, sau khi xuất hiện hộp thoại Owner, chúng ta lựa chọn tập tin, chủ nhân hiện thời và nhấn nút Take Ownership, cho phép lập quyền sở hữu nếu được cấp quyền đó.

Để có quyền sở hữu một tập tin chúng ta cần một trong những điều kiện sau:

Có quyền Full Control.

Có những quyền Special Access bao gồm Take Ownership.

Là thành viên của nhóm Administrator.

II. Các thuộc tính của File và thư mục

Archive: Thuộc tính này được gán bởi hệ điều hành chỉ định rằng một File đã được sửa đổi từ khi nó được Backup. Các phần mềm Backup thường xóa thuộc tính lưu trữ đó. Thuộc tính lưu trữ này có thể chỉ định các File đã được thay đổi khi thực thi việc Backup.

Compress: Chỉ định rằng các File hay các thư mục đã được nén hay nên được nén. Thông số này chỉ được sử dụng trên các partition loại NTFS.

Hidden: Các File và các thư mục có thuộc tính này thường không xuất hiện trong các danh sách thư mục.

Read Only: Các File và các thư mục có thuộc tính này sẽ không thể bị xóa hay sửa đổi.

System: Các File thường được cho thuộc tính này bởi hệ điều hành hay bởi chương trình OS setup. Thuộc tính này ít khi được sửa đổi bởi người quản trị mạng hay bởi các User.

Ngoài ra các File hệ thống và các thư mục còn có cả hai thuộc tính chỉ đọc và ẩn.

Lưu ý: Việc gán thuộc tính nén cho các File hay thư mục mà ta muốn Windows NT nén sẽ xảy ra trong chế độ ngầm (background). Việc nén này làm giảm vùng không gian đĩa mà File chiếm chỗ. Có một vài thao tác chịu việc xử lý chậm vì các File nén phải được giải nén trước khi sử dụng. Tuy nhiên việc nén File thường xảy ra thường xuyên như là các File dữ liệu quá lớn mà có nhiều người dùng chia sẻ.

III. Chia sẻ Thư mục trên mạng

Không có một người sử dụng nào có thể truy xuất các File hay thư mục trên mạng bằng cách đăng nhập vào mạng khi không có một thư mục nào được chia sẻ.

Việc chia sẻ này sẽ làm việc với bảng FAT và NTFS file system. Để nâng cao khả năng an toàn cho việc chia sẻ, chúng ta cần phải gán các mức truy cập cho File và Thư mục.

Khi chúng ta chia sẻ một thư mục, thì chúng ta sẽ chia sẻ tất cả các File và các Thư mục con. Nếu cần thiết phải hạn chế việc truy xuất tới một phần của cây thư mục, chúng ta phải sử dụng việc cấp các quyền cho một user hay một nhóm đối với các Thư mục và các File đó.

Để chia sẻ một Thư mục, ta phải Login như một thành viên của nhóm quản trị mạng hay nhóm điều hành server.

Tất cả các thủ tục chia sẻ thư mục được thực thi trong Windows NT Explorer.

Để chia sẻ một thư mục ta phải thực hiện các bước sau:

Right-click lên Thư mục đó trong Windows NT Explorer. Hiện ra menu

Click **Properties** trong Menu. Hiện ra hộp đối thoại sau:

Chọn **Sharing tab** hiện ra hộp đối thoại sau:

Chọn **Shared As** để kích hoạt việc chia sẻ.

Đưa một tên cần chia sẻ vào hộp **Share name**. Mặc nhiên tên Thư mục được chọn sẽ hiện ra. Đưa dòng ghi chú liên quan đến việc chia sẻ thư mục đó vào hộp **Comment**

Thiết lập giới hạn số lượng các user bằng cách gỏ một con số vào hộp **Allow**

Nếu muốn hạn chế việc truy xuất thì click **Permissions button.**

Click OK.

Sau khi một thư mục được chia sẻ Icon cho thư mục đó có 1 bàn tay chỉ định rằng thư mục đó đã được chia sẻ.

Nếu chúng ta muốn thêm một chia sẻ mới với cùng một thư mục đã được chia sẻ (có thể với hai chia sẻ có hai quyền truy cập khác nhau), ta thực hiện các bước sau:

Right-click vào thư mục đã được chia sẻ trong Windows NT Explorer.

Click **Properties** trong **Menu** rút gọn, hiện ra hộp đối thoại **Properties**

Click **Sharing tab.**

Click button **New Share** để tạo một sự chia sẻ mới, hiện ra hộp đối thoại sau

Mỗi lần tạo một sự chia sẻ chúng ta phải đưa một tên mới cũng như những lời chú thích việc chia sẻ đó sẽ cho ai sử dụng.

IV. Thiết lập quyền truy cập cho một người sử dụng hay một nhóm

Để thiết lập các quyền truy cập đối với một thư mục đã được chia sẻ cho một người sử dụng hay một nhóm ta thực hiện:

Right-click lên thư mục đó trong Windows NT Explorer.

Click **Properties** trong menu rút gọn**.**

Chọn **Sharing** tab để hiện các tính chất của thư mục đó

Click button **Permissions** trong **sharing tab** . Hiện ra Cửa sổ ***The Access Through Share Permissions.***

Chọn button **Add**, hiện ra cửa sổ ***Add User and group*.**

Chọn một tên trong hộp ***Names*** và click button **Add.** Kết quả là tên đó được đưa vào hộp ***Add Names.***

Chọn quyền truy xuất trong hộp ***Type of Access*** cho các tên đã chọn .

Click button **OK.**

Khi chúng ta tạo một sự chia sẻ mới, quyền truy cập mặc nhiên cho nhóm **Everyone** là đầy đủ (**Full Control**). Giả sử rằng chúng ta sẽ gán giá trị mặc nhiên này cho quyền truy cập của thư mục và File. Khi cần thiết sẽ hạn chế việc truy xuất tới thư mục đó.

Ở đây có một vài chú ý:

Các người sử dụng thường chỉ cóù quyền đọc trong các thư mục chứa các chương trình ứng dụng vì họ không cần phải sửa đổi các File.

Trong một vài trường hợp, các chương trình ứng dụng đòi hỏi các user chia sẻ một thư mục cho các File tạm thời. Nếu thư mục đó nằm trong cùng thư mục chứa trình ứng dụng, chúng ta có thể cho phép user tạo hay xóa các File trong thư mục đó bằng việc gán quyền **Change**.

Thông thường các người sử dụng cần quyền **Change** trong bất kỳ thư mục nào chứa các Files dữ liệu và chỉ trong các thư mục cá nhân của ho là có đầy đủ các quyền truy cậpï.

Để sửa đổi các quyền truy cập đối với một thư mục đã được chia sẻ ta thực hiện:

Right-click lên thư mục được chia sẻ trong Windows NT Explorer.

Click **Properties**

Click **Sharing** tab.

Click button **Permissions** hiện ra cửa sổ ***Access Through Share Permissions*** sau:

Chọn 1 tên trong hộp ***Name***

Chọn một quyền khác trong hộp ***Type of Access*** mà ta muốn gán.

Click **OK**.

Thông qua việc chia sẻ một thư mục cho một user hay một nhóm cũng góp phần vào việc bảo đảm an toàn cho một thư mục không cho user khác hay nhóm khác truy xuất thư mục đó.

V. Sử dụng các thư mục mạng

Muốn sử dụng các thư mục mạng thì trước hết thư mục đó được cho phép chia sẻ, chúng ta phải liên kết thư mục mạng đó với tên một chữ cái tương ứng như một tên đĩa mạng (E,F ,G ,H I,...). Sau khi thư mục được chia sẻ đã kết nối với ký tự ổ đĩa mạng người dùng có thể truy cập thư mục được chia sẻ, các thư mục và file con của nó như là nó đang ở trên máy tính của mình .

Có thể dùng Network Neighborhood để thực hiện công việc trên như sau :

Click đúp trên **Network Neighborhood** để mở trình duyệt mạng.

Duyệt qua **Network Neighborhood** để tìm nơi muốn liên kết.

Click phải vào thư mục đã được chia sẻ mà chúng ta muốn truy cập và chọn **Map Network Drive** trong thực đơn **Options** ta thấy hộp **Map Network Drive** hiện ra

Trong trường **Drive** của hộp thoại **Map Network Drive**, chọn ổ đĩa mạng chúng muốn liên kết với thư mục chia sẻ.

Nếu thấy cần, chọn Path và gõ vào tên theo tổng quát UNC (Universal Naming Convention - xem cấu trúc ở phần dưới) để sửa lại đường dẫn tới tài nguyên được chia sẻ. (Việc này chỉ thực hiện khi sử dụng Network Neighborhood.)

Nếu chúng ta không được quyền để truy cập vào tài nguyên chia sẻ trên nhưng trong cương vị người dùng khác thì chúng ta được quyền truy cập, trong trường hợp đó hãy gõ tên người dùng đó vào trường **Connect As**.

Kích hoạt hộp kiểm tra **Reconnect at Logon** nếu muốn liên kết lâu dài, đó là loại kết nối được phục hồi mỗi lần chú ta đăng nhập vào mạng.

Chọn **OK** để lưu các thông tin trên.

Ngoài ra ta có thể dùng lệnh **NET USE** để thực hiện các công việc trên.

Lệnh NET USE dùng Universal Naming Convention (UNC) để truy cập các tài nguyên dùng chung. Tên UNC bắt đầu bằng một dấu phân cách đặt biệt \\, dấu này chỉ sự bắt đầu của tên UNC (tên UNC có dạng "\\computer_name\share_name[\sub_directory]". NET USE được dùng đểû truy cập một nguồn tài nguyên dùng chung. Lệnh NET USE dùng bộ hướng dẫn mạng (Network Redirector) trên máy tính NT để thiết lập sự nối kết dùng nguồn tài nguyên chung.

Chúng ta có thể xem ai dùng các file dùng chung khi ta đang xem trạng thái của một file dùng chung, File Manager sẽ cung cấp cho ta các thông tin bằng dùng chọn Properties trong thực đơn File

Đề mục	Nội dung
Total Opens	Tổng số các user đang làm việc với file đó
Total Locks	Tổng số các khóa trên file
Open By	Tên của người dùng đã mở file
For	Loại truy xuất mà người dùng đã mở file
Locks	Một số khóa mà người dùng đặt trên file
File ID	Con số nhận diện của file

Khi chúng ta dùng Windows Explorer để xem các tài nguyên chúng ta có thì các ổ đĩa mạng xuất hiện và cho chúng ta khai thác.

Chương 14 :

Sử dụng máy in trong mạng Windows NT

Hiện nay máy in trên mạng cũng là một tài nguyên việc chia sẻ của mạng cho người sử dụng. Tuy các máy in đang ngày càng rẻ đi nhưng với nhu cầu về chất lượng đang ngày một cao thì việc chia sẻ các máy in đắt tiền trên mạng vẫn đang cần thiết. Windows NT là một hệ điều hành mạng mà bất kỳ máy tính Windows NT nào cũng có thể cung cấp các dịch vụ in ấn cho người sử dụng trong mạng.

Khi chia sẻ một máy in trên mạng (cho nhiều người có thể cùng sử dụng) chúng ta cần phải giải quyết những vấn đề sau :

Máy in không làm được 2 việc một lúc, nếu phải nhận cùng một lúc thì sẽ có va chạm, do vậy mạng phải có cơ chế sắp xếp công việc sao cho máy in có thể thực hiện một cách lần lượt các công việc in.

Các công việc in được thực hiện bởi những người sử dụng khác nhau có thể cần những mức độ ưu tiên khác nhau và hệ thống quan lý in cần có khả năng thực hiện điều này.

I. Cơ chế in trong mạng Windows NT

Thông thường máy in mạng được quản lý thông qua một máy chủ mà trên đó thực hiện nhiệm vụ quản lý các công việc in, máy chủ đó thường được gọi là máy chủ in (Print server) và

chạy chương trình quản lý in. Windows NT cho phép cài đặt máy in tại bất cứ đâu trên mạng, mỗi một máy có cài đặt Windows NT đều có thể thực hiện nhiệm vụ máy chủ in. Nó có thể quản lý máy in gắn trực tiếp vào nó hay một máy in gắn vào máy khác trên mạng.

Để giải quyết những vấn đề đặt ra với công việc in trên mạng Windows NT sử dụng kỹ thuật gọi là Spooling mà chủ yếu như sau:

Khi người sử dụng quyết định thực hiện một công việc in thì công việc in đó không trực tiếp gửi ra máy in mà nó được đặt trong một file tại máy chủ in. Ở đây việc thực hiện giống như hàng đợi rạp hát, nó là một vùng lưu trữ các công việc in và có nhiệm vụ ngăn chặn xung đột khi các user chi xuất đồng thời ra máy in.

Máy chủ in duy trì các hàng đợi để cất giữ các công việc in và đưa chúng tới máy in ngay khi có thể. Trong khi đó người sử dụng có thể làm tiếp công việc ngay khi công việc in được cất vào hàng đợi.

Khi máy in rảnh máy chủ in sẽ chuyển lần lượt các công việc in đang đứng đợi trong hàng tới máy in. Tại đây máy chủ in phải có một khả năng lưu trữ dữ liệu lớn để có thể lưu trữ nhiều công việc in một lúc và cần phải có khả năng đáp ứng những yêu cầu đa dạng của các công việc in.

Để giải quyết vấn đề nẩy sinh với máy in trong mạng Windows NT tiến hành phân biệt giữa máy in vật lý gọi là Printing device và một thực thể logic của máy in gọi là logic printer. Máy in logic được sử dụng để kiểm soát các tác vụ sau đây :

Công việc in được gởi đi đâu.

Công việc in ấn gởi đi khi nào.

Thứ tự ưu tiên của các tác vụ in.

Người sử dụng in ra spool thông qua việc in ra máy in logic, họ sử dụng máy in logic như là máy in đang được gắn là máy của họ nhưng thực sự các dữ liệu được in ra máy in logic được chuyển cho mạng và qua đó đến máy chủ in trước khi được đưa ra máy in mạng.

Máy chủ in sẽ liên kết các máy in logic với máy in vật lý, nó phải đảm bảo các công việc in phải được đưa đúng đến máy in vật lý. Tại đây có 3 trường hợp có thể đối với mối quan hệ giữa máy in logic và máy in vật lý

Một máy in logic liên kết với một máy in vật lý.

Nhiều máy in logic liên kết với một máy in vật lý.

Một máy in logic liên kết với nhiều máy in vật lý.

Nếu Server chưa cài đặt máy in logic, ta phải cài đặt máy in logic tương ứng với một máy in thực tế cho Server. Vào menu **Start**, chọn **Settings**, chọn **Printers**, chọn **Add Printer** như:

Hộp sau đó hộp hội thoại **Add printer** winzar hiện ra

Chọn My Computer nếu máy in của chúng ta không có card mạng và được nối trực tiếp vào Server.

Chọn Network printer server nếu máy in của chúng ta nối trực tiếp vào mạng.

Chọn Next, chọn cổng nối với máy in (thường là LPT1). Chọn tên hãng sản xuất và loại máy in ta đang dùng, chọn Next, ta phải trả lời thêm vài câu hỏi phụ như ta có muốn in trang test không? Có muốn đặt máy in này là ngầm định không?

Sau khi cài đặt, chúng ta sẽ thấy xuất hiện thêm biểu tượng máy in mà vừa được cài đặt trong khung máy in. Chúng ta phải cho phép dùng chung máy in nàybằng cách lựa chọn máy in đó Trong khung Printers

Ta nhắp chuột phải vào tên máy in đó, chọn **Sharing** như hình sau:

Khung **Printer properties** hiện ra cho chúng ta nhập các thông số như: tên máy in logic (Share namem), các tính chất khác như về an toàn. mà chúng ta muốn khi phục vụ mạng.

Cuối cùng chọn **OK**, lúc này, ta sẽ thấy ở dưới biểu tượng máy in có bàn tay đỡ chứng tỏ máy in này đã được phép dùng chung. Nếu trên Server cài đặt nhiều loại máy in với nhiều chế độ khác nhau, ta có thể chọn máy in ngầm định bằng cách đánh dấu vào mục **Set As Default**.

Để máy trạm có thể in được qua Server, nếu chưa cài đặt chúng ta phải cài máy in như sau: nhắp đúp vào tên Server có nối với máy in, khung **Shared Printers** sẽ hiện ra danh sách các máy in đã cài trên Server, chúng ta chọn tên máy in cần nối rồi bấm **OK**.

Quay trở lại khung màn hình **Print Manager** chúng ta nhìn thấy thông báo máy in này đã được phép sử dụng. Thoát ra khỏi **Print Manager** và chúng ta có thể in qua máy in mạng trên bất cứ một phần mềm nào trên Windows như Winword, Excel, v.v...

Bất kỳ máy tính Windows NT có thể được cấu hình như là một **print server**. Tuy nhiên chỉ có những người là thành viên của những nhóm sau đây mới có quyền tạo ra các máy in:

Administrator (NT Worstation and Server).

Server Operator (NT Server).

Print Operator (NT Server).

Power Users (NT Worstation).

II. Bảo mật của máy in

Windows NT có các mức độ bảo mật trong in ấn như sau:

Quyền sở hữu máy in (Ownership) : người sử dụng tạo ra một máy in chính là người chủ sở hữu máy in đó và có toàn quyền trên tất cả các thuộc tính của máy in logic. Người chủ sở hữu máy in có thể gán quyền cho những người dùng khác quản lý tài liệu hay toàn quyền điều khiển việc in ấn. Một người sử dụng có toàn quyền thì họ toàn quyền sở hữu máy in logic đó.

Quản lý thuộc tính máy in (Permissions): quyền quản lý máy in bao gồm 4 quyền sau:

No access: không được phép truy cập.

Print: in

Manage document: quản lý văn bản, có khả năng thực hiện các thao tác: Điều khiển khởi đặt tài liệu, Ngừng, phục hồi, khởi động lại,và xóa các tài liệu.

Full control: toàn quyền điều khiển, thực hiện các quyền quản lý tài liệu và các quyền sau đây:

Thay đổi trật tự in ấn tài liệu.

Ngừng, tổng hợp lại,che dấu các máy in logic.

Thay đổi thuộc tính của máy in logic.

Hủy các máy in logic.

Thay đổi quyền của máy in logic

Có thể xem tài liệu ở máy in logic và quản lý chúng theo nhiều cách. Người sử dụng luôn quản lý được tất cả các tài liệu mà họ tạo ra. Để quản lý được các tài liệu của các người sử dụng khác, phải là người chủ sở hữu của máy in logic hay là thành viên của các nhóm:

Administrator.

Server Operator

Print operator.

Bất kỳ một máy in nào cũng có thể làm việc trong môi trường mạng nhưng điều quan trọng là xem xét **chu kỳ làm việc (duty cycle)** của máy in. Nghĩa là phải xem xét số lượng trang in tối đa mà máy in có thể in ra trong một khoảng thời gian nhất định.

Các máy in được thiết kế cho mạng thường có **chu kỳ làm việc (duty cycle)** cao. Các máy in có thể gắn vào bất cứ nơi đâu trên mạng. Công việc in không phù thuộc vào các thiết bị phần cứng hay các thiết bị kết nối mà do được quản lý bởi một **print server** và dữ liệu được chuyển vận trên mạng.

Chương 15 :

Các dịch vụ mạng của Windows NT Server

Cũng như các hệ điều hành khác Windows NT cũng có những ưu, khuyết điểm của nó, tuy nhiên Windows NT hiện nay chinh phục được nhiều người dùng với những ưu điểm không thể chối cãi. Là hệ điều hành mạng cho phép tổ chức quản lý một cách chủ động theo nhiều mô hình khác nhau: peer-to-peer, clien/server. Nó thích hợp với tất cả các kiến trúc mạng hiện nay như: hình sao (start), đường thẳng (bus), vòng (ring) và phức hợp. Nó có một số đặc tính ưu việt bảo đảm thực hiện cùng lúc nhiều chương trình mà không bị lỗi. Bản thân Windows NT đáp ứng được hầu hết các giao thức phổ biến nhất trên mạng và cũng hỗ trợ được rất nhiều những dịch vụ truyền thông trên mạng. Nó vừa đáp ứng được cho mạng cục bộ (LAN) và cho cả mạng diện rộng (WAN).

Windows NT cho phép dùng giao thức Windows NT TCP/IP, vốn là một giao thức được sử dụng rất phổ biến trên hầu hết các mạng diện rộng và trên Internet. Giao thức TCP/IP dùng tốt cho nhiều dịch vụ mạng trên môi trường Windows NT.

I. Internet Information Server (IIS)

Internet Information Server là một ứng dụng chạy trên Windows NT, tích hợp chặt với Windows NT, khi cài đặt IIS, IIS có đưa thêm vào tiện ích màn hình kiểm soát (Performance monitor) một số mục như thống kê số lượng truy cập, số trang truy cập. Việc kiểm tra người dùng truy cập cũng dựa trên cơ chế quản lý người sử dụng của Windows NT. Sau khi cài đặt IIS, trong thư mục InetSrv sẽ có các thư mục gốc tương ứng cho từng dịch vụ chọn cài đặt.

IIS bao gồm 3 dịch vụ: World Wide Web (WWW), chuyển file (FTP - File Transfer Protocol) và Gopher. Cả 3 dịch vụ này đều sử dụng kết nối theo giao thức TCP/IP.

1. Cài đặt dịch vụ Internet Information Server

Khi cài đặt hệ điều hành Windows NT đến phần mạng Windows NT sẽ hỏi chúng ta xem có cài đặt dịch vụ Internet Information Server hay không với hộp hội thoại

Để thực hiện việc cài đặt chúng ta Click vào phím Next và Hệ thống sẽ bắt đầu cài đặt các dịch vụ Internet Information Server.

2. Các dịch vụ trong IIS

a. WWW (World Wide Web) :

Là một trong những dịch vụ chính trên Internet cho phép người sử dụng xem thông tin một cách dễ dàng, sinh động. Dữ liệu chuyển giữa Web Server và Web Client thông qua nghi thức HTTP (Hypertext Transfer Protocol).

Người quản trị có thể xem các thông tin như các người dùng đã truy cập, các trang được truy cập, các yêu cầu được chấp nhận, các yêu cầu bị từ chối. thông qua các file có thể được lưu dưới dạng cơ sở dữ liệu.

b. FTP (File Transfer Protocol)

Sử dụng giao thức TCP để chuyển file giữa 2 máy và cũng hoạt động theo mô hình Client/Server, khi nhận được yêu cầu từ client, đầu tiên FTP Server sẽ kiểm tra tính hợp lệ của người dùng thông qua tên và mật mã. Nếu hợp lệ, FTP Server sẽ kiểm tra quyền người dùng trên tập tin hay thư mục được xác định trên FTP Server. Nếu hợp lệ và hệ thống file là NTFS thì sẽ có thêm kiểm tra ở mức thư mục, tập tin theo NTFS. Sau khi tất cả hợp lệ, người dùng sẽ được quyền tương ứng trên tập tin, thư mục đó.

Để sử dụng FTP có nhiều cách:

Sử dụng Web Browser.

Sử dụng Command line.

Sử dụng từ <Run> command trong Windows.

c. Gopher

Là một dịch vụ sử dụng giao diện menu để Gopher Client tìm và chuyển bất kỳ thông tin nào mà Gopher Server đã được cấu hình. Gopher cũng sử dụng kết nối theo giao thức TCP/IP.

II. Dynamic Host Configuration Protocol (DHCP) :

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

Trong mạng máy tính 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 phương pháp này sẽ được gán vĩnh viễn cho DHCP client và địa chỉ này sẽ không bao giờ được sử dụng bởi một DHCP client khác

Trong phương pháp gán địa chỉ IP động thì DHCP server gán địa chỉ IP cho DHCP client tạm thời. Sau đó địa chỉ IP này sẽ được DHCP client sử dụng trong một thời gian đặc biệt.

Đến khi thời gian này hết hạn thì địa chỉ IP này sẽ bị xóa mất. Sau đó nếu DHCP client cần nối kết vào mạng thì nó sẽ được cấp một địa chủ IP khác

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

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

Login vào Server với tên Administrator .

Click hai lần vào icon **Network** . Ta sẽ thấy hộp hội thoại **Network dialog box**

Chọn tab **service** và click vào nút **Add** .

Ta sẽ thấy một loạt các service của Windows NT server nằm trong hộp hội thoại **Select Network Service**. Chọn **Microsoft DHCP server** từ danh sách các service 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.

III. Dịch vụ Domain Name Service (DNS)

Hiện nay trong mạng Internet số lượng các nút (host) lên tới hàng triệu nên chúng ta không thể nhớ hết địa chỉ IP được, Mỗi host ngoài địa chỉ IP còn có một cái tên phân biệt, DNS là 1 cơ sở dữ liệu phân tán cung cấp ánh xạ từ tên host đếùn 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 tụ 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

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 dươi 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

IV. 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 người 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 hoạc 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.

Để cài đặt RAS chúng ta lưa 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.