Chương 8

CÁC DỊCH VỤ CỦA MẠNG DIỆN RỘNG (WAN)

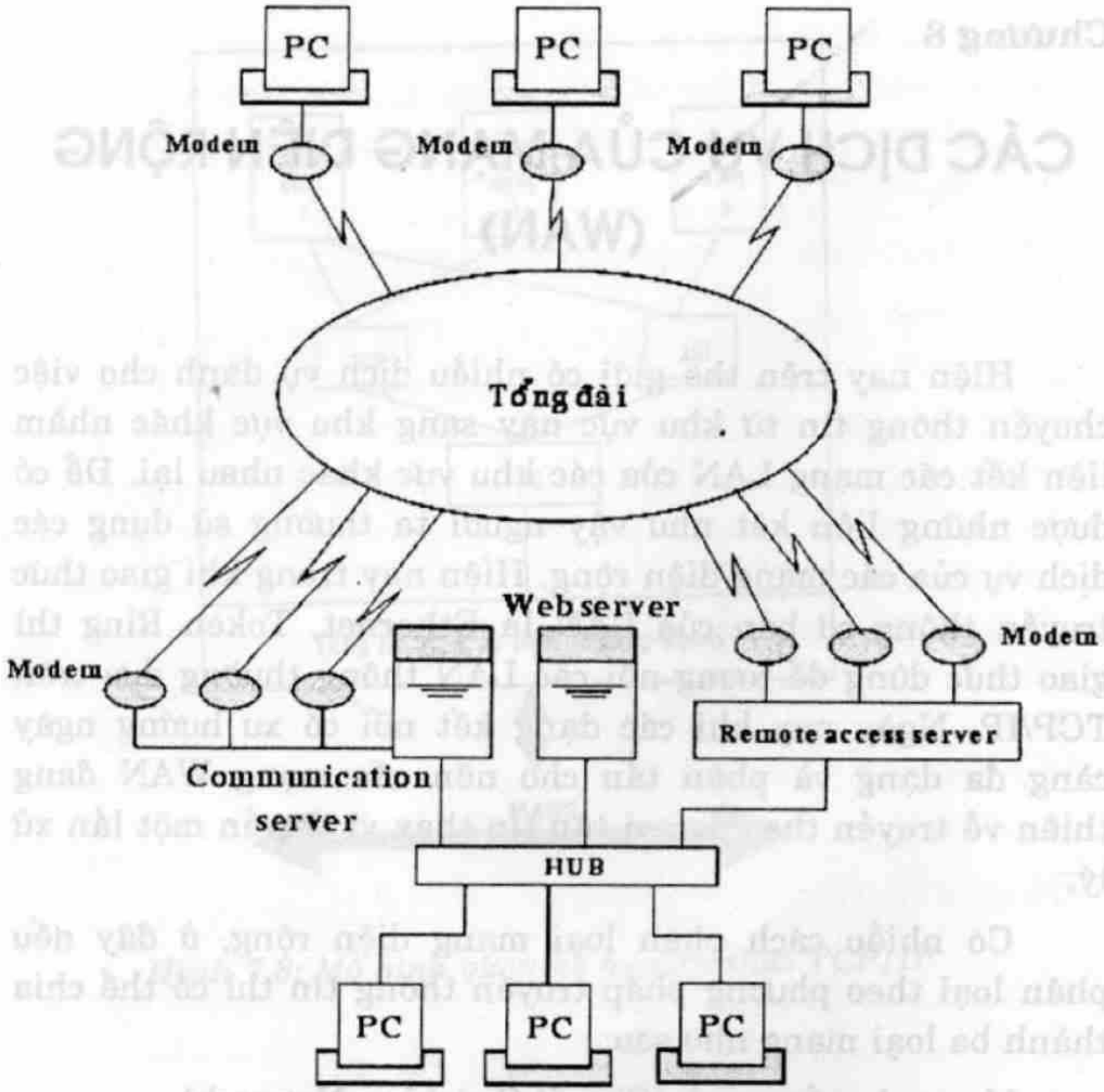
Hiện nay trên thế giới có nhiều dịch vụ dành cho việc chuyển thông tin từ khu vực này sang khu vực khác nhằm liên kết các mạng LAN của các khu vực khác nhau lại. Để có được những liên kết như vậy người ta thường sử dụng các dịch vụ của các mạng diện rộng. Hiện nay trong khi giao thức truyền thông cơ bản của LAN là Ethernet, Token Ring thì giao thức dùng để tương nối các LAN thông thường dựa trên 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 ba 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 lên kết giữa hai điểm nút, một đường nối giữa điểm nút này và điểm 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*

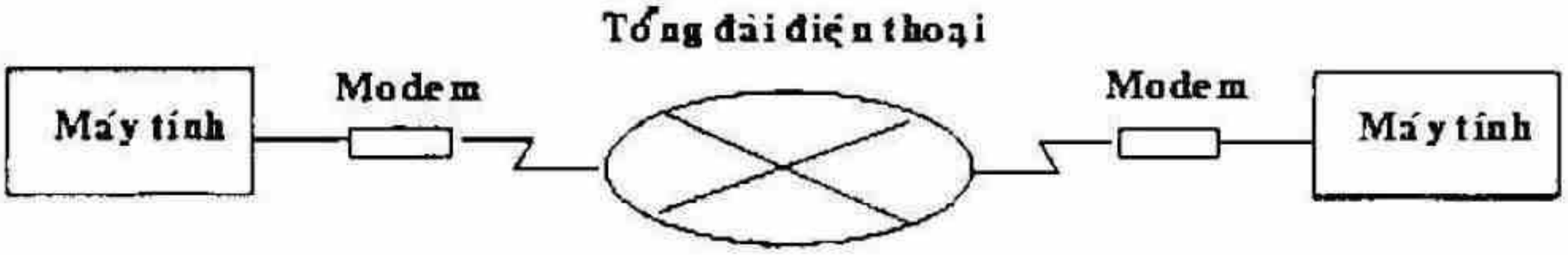
Một ví dụ của mạng chuyển mạch là hoạt động của mạng điện thoại, các thuê bao khi biết số của nhau có thể gọi cho nhau và có một đường nối vật lý tạm thời được thiết lập giữa hai thuê bao.

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 hai 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 mạng sử dụng một thiết bị có tên là modem, thiết bị này sẽ chuyển các tín hiệu số này từ máy tính sao tín hiệu tuần tự có thể truyền đi trên mạng điện thoại và ngược lại.



Hình 8.2: *Mô hình chuyển mạch tương tự*

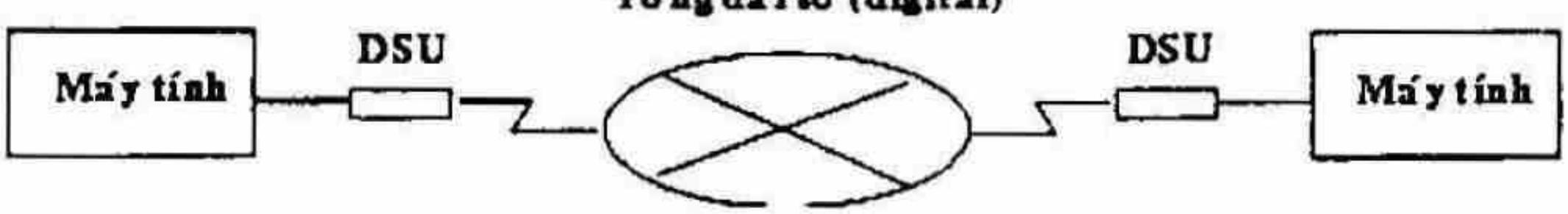
Khi sử dụng đường truyền điện thoại để truyền số liệu thì các chuẩn của modem và các tính chất của nó sẽ quyết định tốc độ của đường truyền. Cùng với các kỹ thuật chuyển đổi tín hiệu, các tính năng mới như nén tín hiệu cho phép nâng tốc độ truyền dữ liệu lên rất cao.

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 V22 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 Accunet 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.



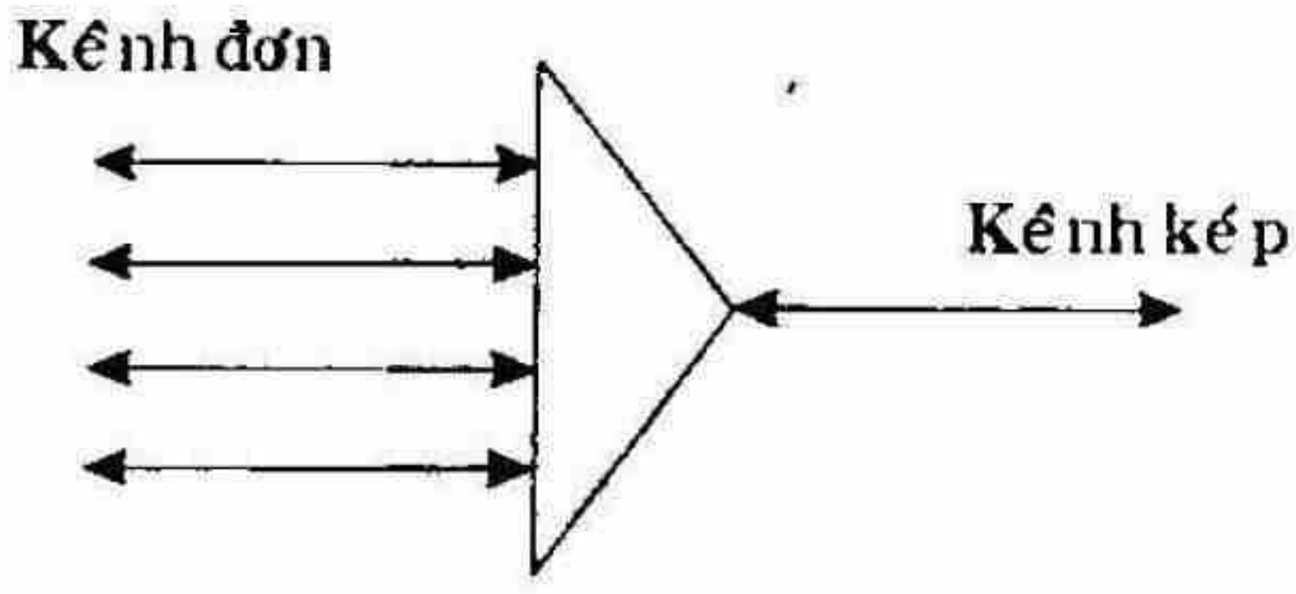
Hình 8.4: *Mô hình chuyển mạch số*

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 8.5: 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 dữ liệu, mỗi kênh truyền từ người sử dụng đến nút sẽ được chuyển thành một kênh con với tần số xác định và được truyền thông qua bộ ghép kênh đến nút cuối và tại đây nó được tách ra thành kênh riêng biệt để truyền tới người nhận. Theo các chuẩn của CCITT có các phương thức ghép kênh cho phép ghép 12, 60, 300 kênh đơn.

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

- *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 truyền 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 với tốc độ 64 kbps và 8000 bit điều khiển trong 1 giây.

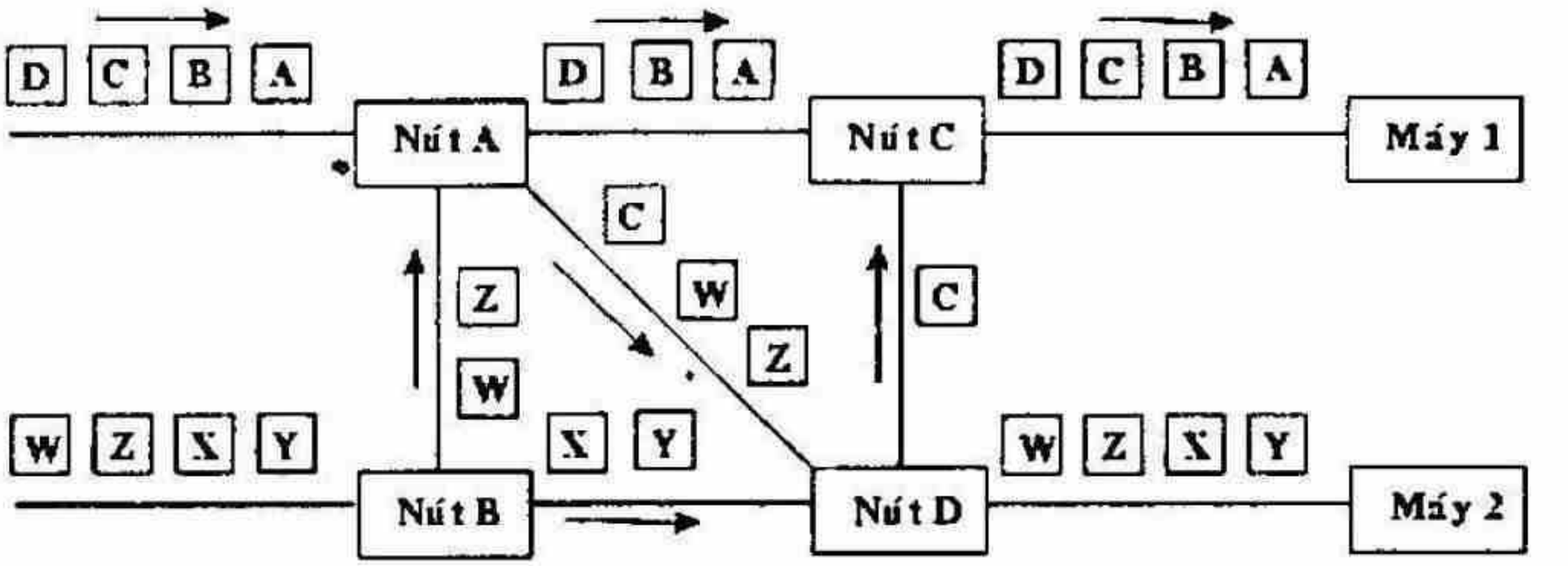
III. MẠNG CHUYỂN GÓI TIN (PACKET SWITCHING NETWORK)

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 hai phương thức:

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

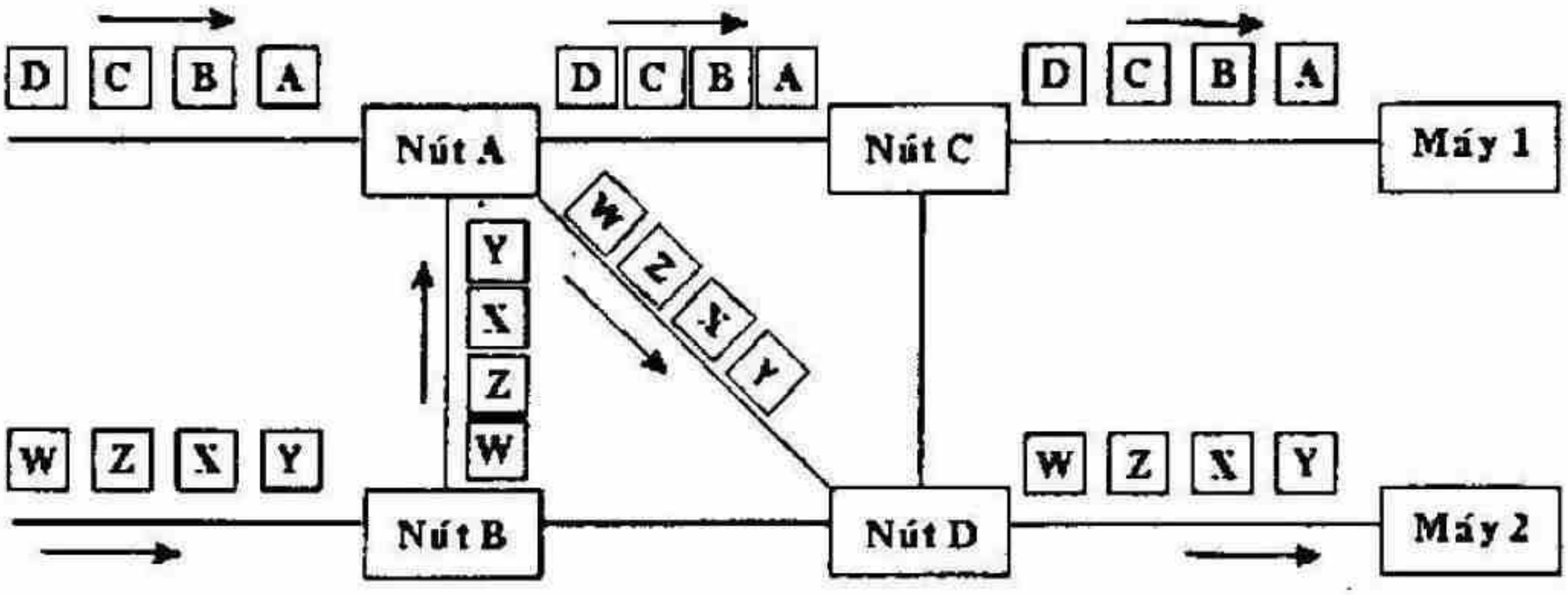
Với phương thức chuyển mạch gói theo sơ đồ rời rạc các gói tin được chuyển đi trên mạng một cách độc lập, mỗi gói tin đều có mang địa chỉ nơi gửi và nơi nhận. Mỗi nút trong mạng khi tiếp nhận gói tin sẽ quyết định xem đường đi của gói tin phụ thuộc vào thuật toán tìm đường tại nút và những thông tin 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 8.6: Ví dụ phương thức sơ đồ rời rạc

Phương thức chuyển mạch gói theo đường đi xác định:

Trước khi chuyển 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 mạng 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 cũ 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 8.7: 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 lượng đường truyền cao cho dù chất lượng đường 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. Điềuu 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 cho chất lượng rất cao gần như phi lỗi. Tuy nhiên do vậy khối lượng tính 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 là mạng Frame Relay 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 2 Mbps 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 byte, trong đó 5 byte dành cho phần chứa thông tin điều khiển (cell header) và 48 byte 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 dụng 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 ảnh 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 đáp ứng cho các dạng truyền thông đa phương tiện (multimedia).

Chuyển mạch cell cần thiết cho việc cung cấp các kết nối đòi hỏi băng thông cao, tình trạng tắc nghẽn thấp, hỗ 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 thông đồng bộ (asynchronouns) các tế 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 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 tính 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 của 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 lựa chọn trong đó một file server có thể làm việc như một Workstation như hai tiến trình server và workstation tách rời 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 sẵn 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 điện cho phép người 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 chủ: Chương trình thực hiện từ DOS. Lưu các thông số của DOS, chuyển CPU của server qua chế độ protected 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 bảy tầng của 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></td><td>Hệ thống nhập xuất cơ bản trên mạng
(NetBIOS)</td><td></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>

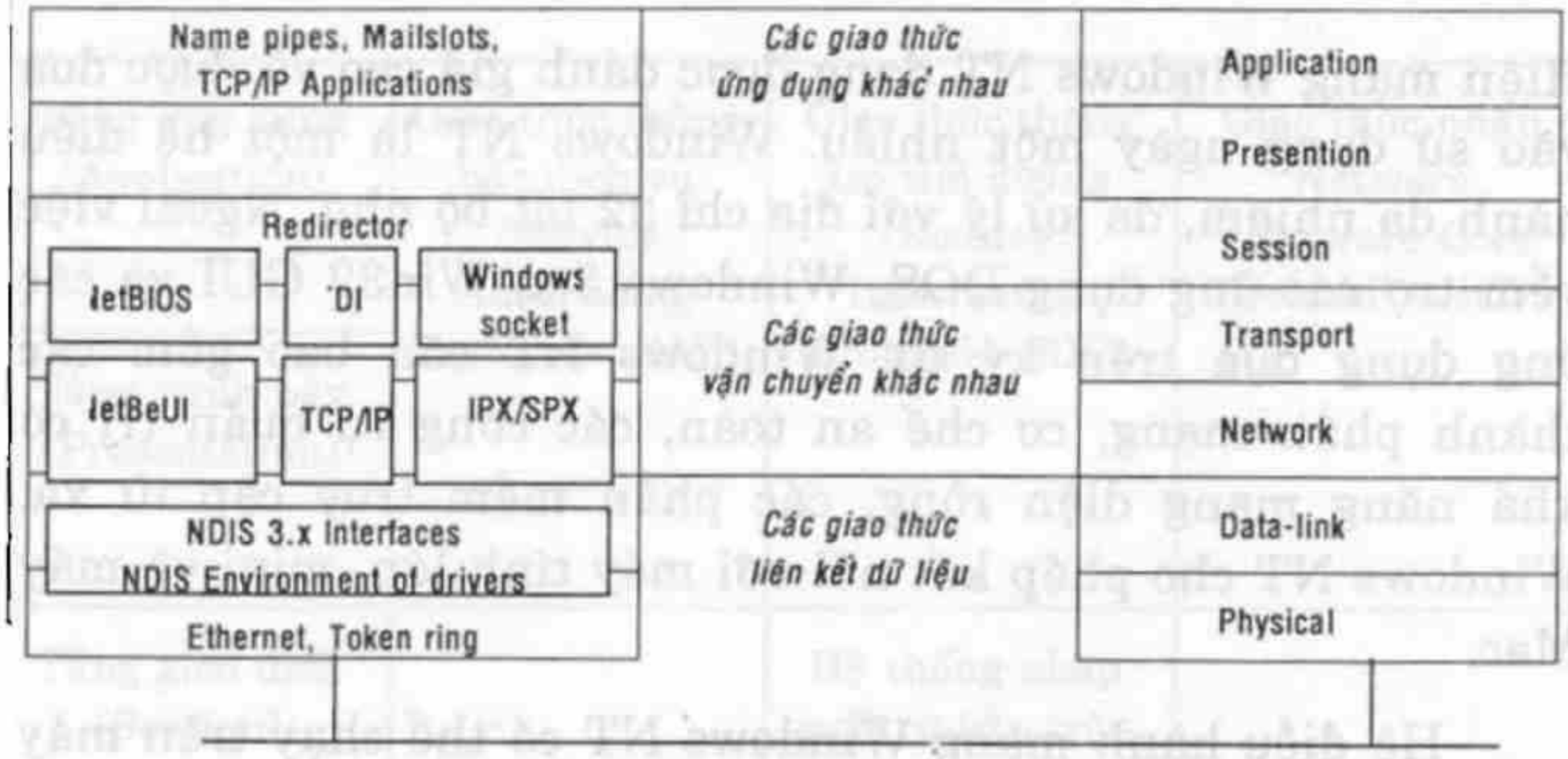
Hình 9.1: *Cấu trúc của Hệ điều hành Novell Netware*

II. MẠNG WINDOWS NT

Mạng dùng hệ điệu 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 đưa 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 trợ 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 chạy 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 letis). 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*

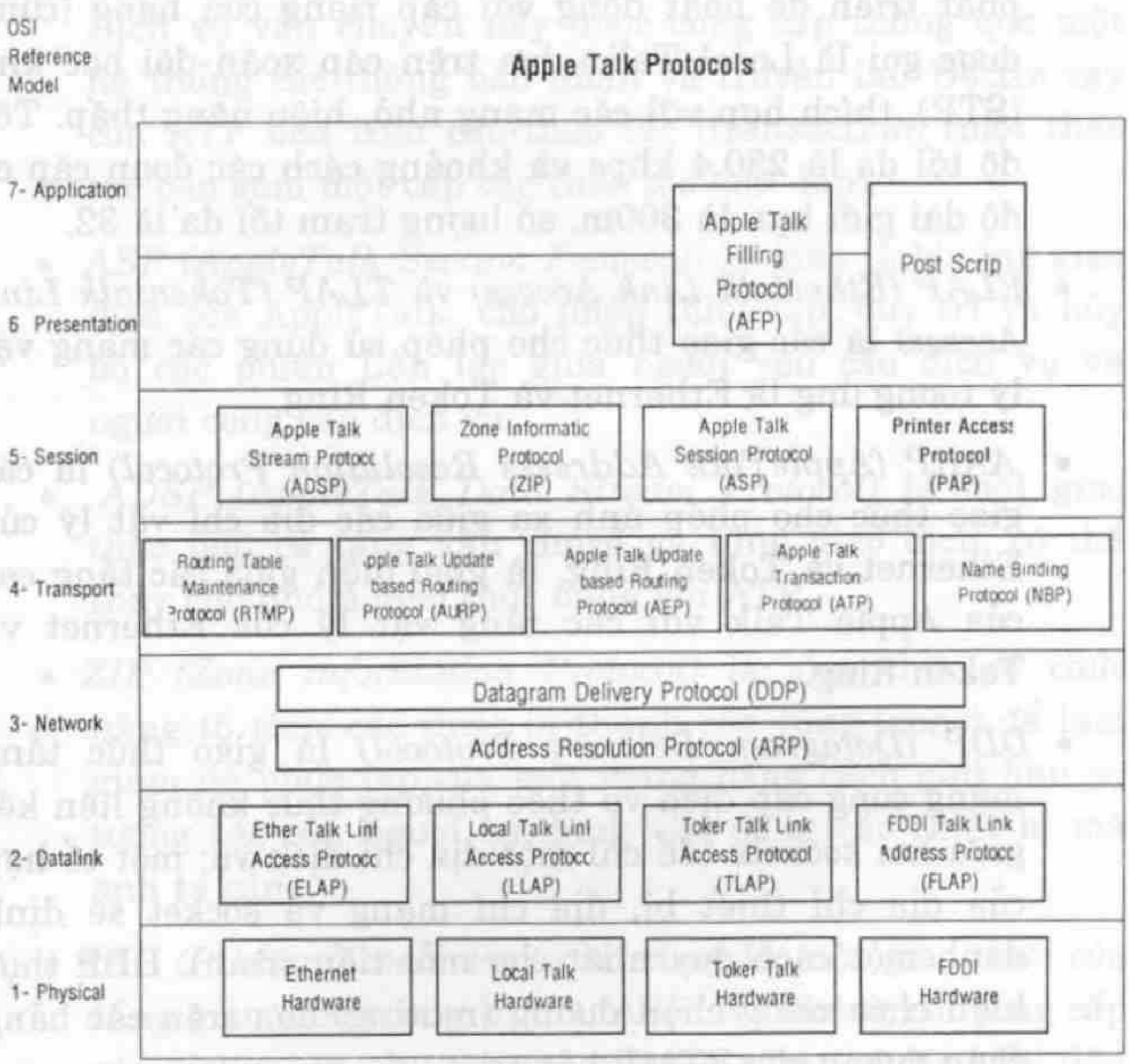
III. MẠNG APPLE TALK

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 AMC cũng là một bước tiến mới 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 **Apple Talk** chỉ cài đặt trên hệ thống cáp riêng của hãng là Local Talk 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 *fdditalk*.

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 Local Talk) dựa trên cáp xoắn đôi bọc kim (STP), thích hợp với các mạng nhỏ, hiệu năng thấp. Tốc độ tối đa là 230,4 kbps 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 Apple Talk với các tầng vật lý của Ethernet và Token Ring.
- *DDP (Dotagram Delivery Protocol)* là giao thức tầng mạng cung cấp dịch vụ theo phương thức không liên kết giữa hai sockets (để chỉ một địa chỉ dịch vụ; một tổ hợp của địa chỉ thiết bị, địa chỉ mạng và socket sẽ định danh một cách duy nhất cho mỗi 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 tầng vận chuyển hoạt động với phương thức không liên kết. Dịch vụ vận chuyển này được cung cấp thông qua một hệ thống các thông báo nhận và truyền lại. Độ tin cậy của ATP dựa 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 chuyể 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 một 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 một 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 người 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.

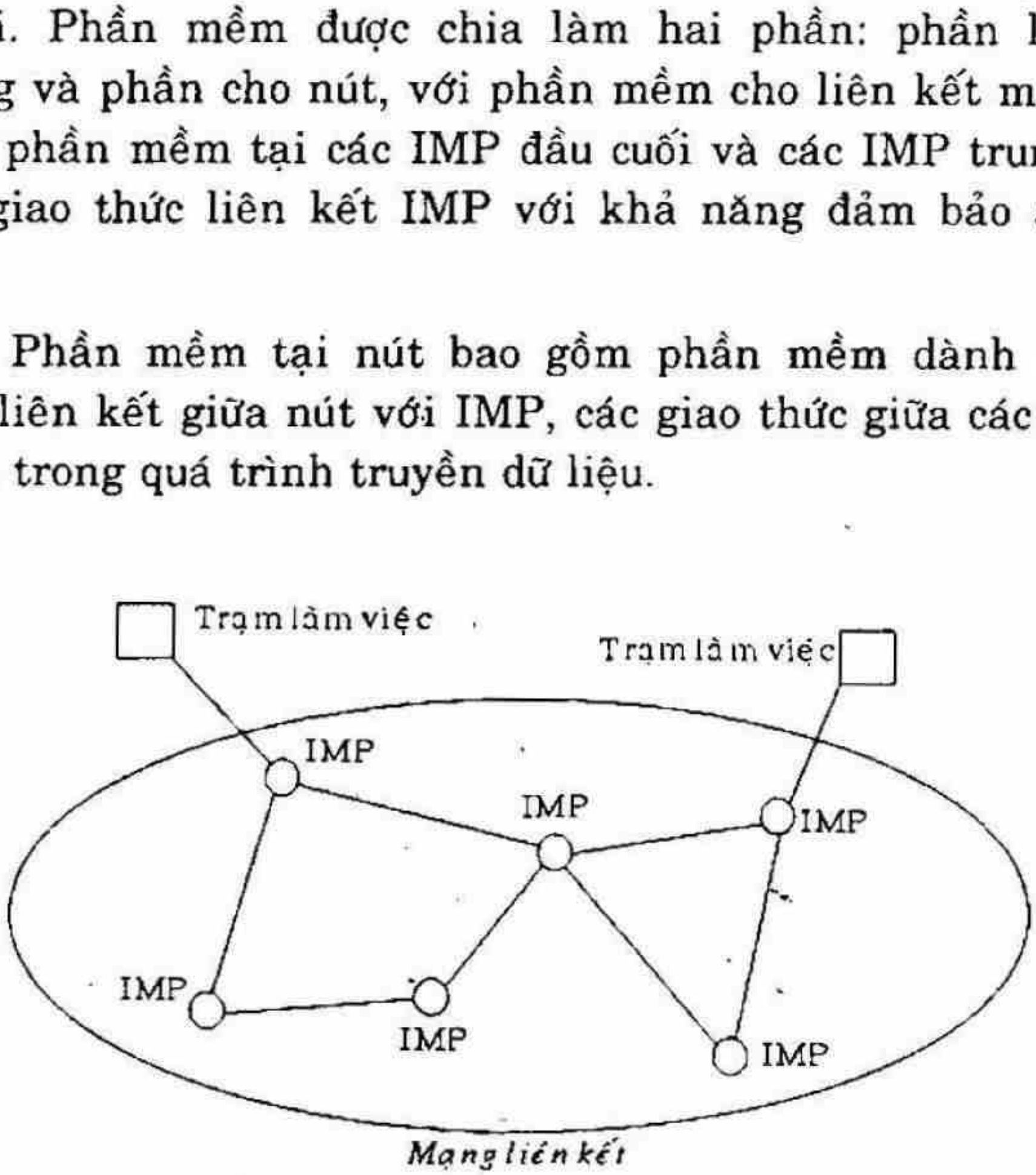
Vào đầu những năm 1960, những ý tưởng chủ yếu của chuyển mạch gói đã được Paul Baran công bố và sau khi tham khảo nhiều chuyên gia thì chương trình ARPA quyết định mạng tương lai của Bộ quốc phòng Mỹ sẽ là mạng chuyển mạch gói và nó bao gồm một mạng liên kết và các trạm (host). Mạng liên kết bao gồm các máy tính dùng để liên kết các đường truyền dữ liệu được gọi là các điểm trung chuyển thông 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 môt 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 phối, 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 chọn 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 dành cho các 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 bốn 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 Berkeley – California, các nhà nghiên cứu của trường đại học đã viết rất nhiều phần mềm, chương trình quản trị trên cơ sở hệ điều hành UNIX. Dựa trên các phần mềm mới về truyền thông trên cơ sở TCP/IP đã cho phép dễ dàng 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 MILNET và 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 chứa 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 khoảng 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 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 bốn 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.

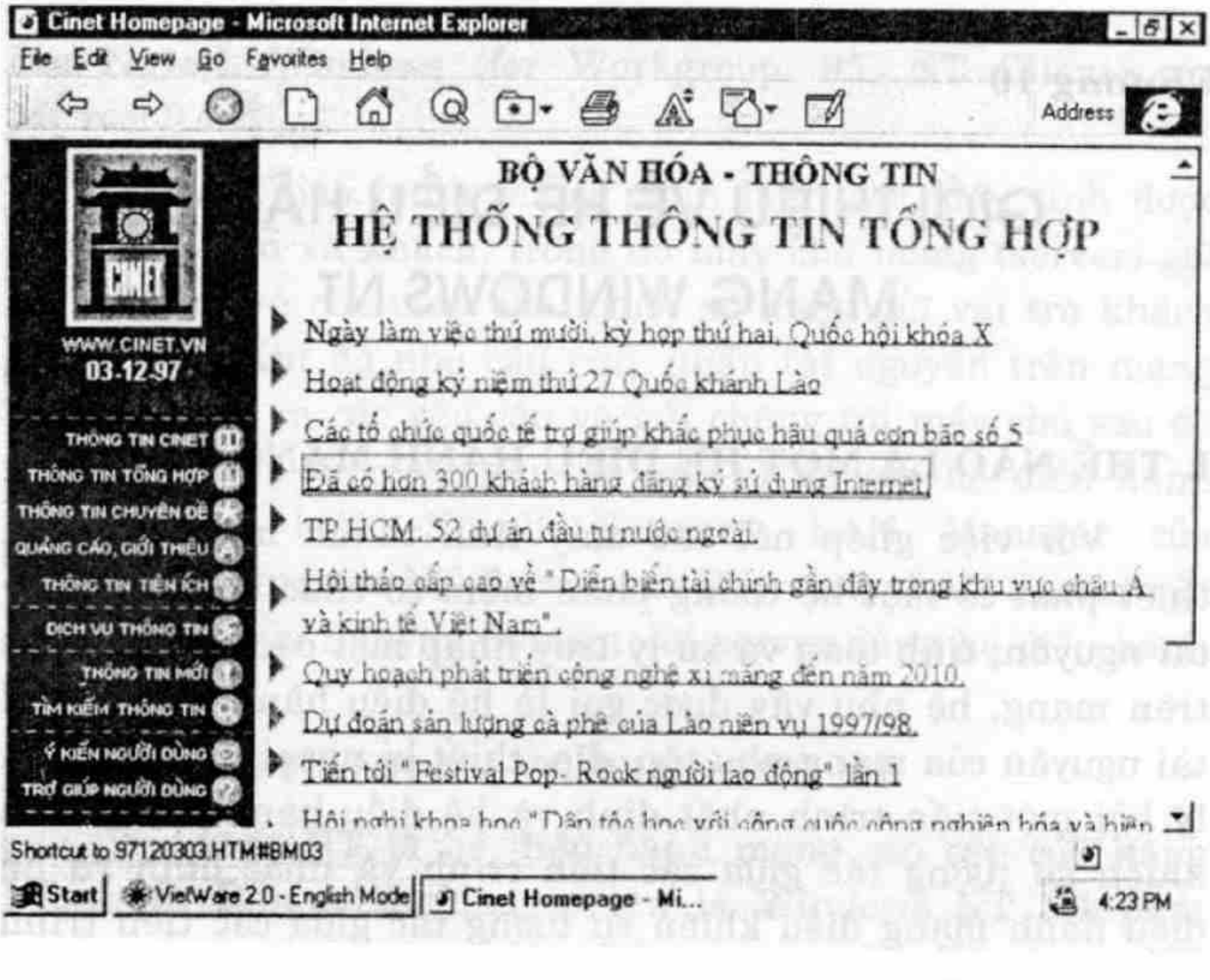
Hiện nay một máy tính được gọi là thành viên của Internet nếu máy tính đó có giao thức truyền dữ liệu TCP/IP, có một địa chỉ IP trên mạng và nó có thể gửi các gói tin IP đến tất cả các máy tính khác trên mạng Internet.

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 đó. Hiện nay Internet có năm dịch vụ chính:

- Thư điện tử (Email): Đấy là dịch vụ đã có từ khi mạng ARPANET mới được thiết lập, nó cho phép gửi và nhận thư điện tử cho mọi thành viên khác trong mạng.
- Thông tin mới (News): Các vấn 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 có hàng nghìn diễn 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.

Người sử dụng nhận được thông tin dưới dạng các trang văn bản, một trang là một đơn thể nằm trong máy chủ. 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 HTLM (Hypertext Markup Language) với nhiều dạng phong phú như văn bản, hình vẽ, video, tiếng nói và có thể có các kết nối 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.



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

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 DIỀU 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 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 chu và các máy cho người sử dụng giữ vai trò khách (các trạm). Khi đó 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 station

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 Workstation 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 chọn 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 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, ... 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 (client/ 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 phục 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 hiện 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 cung cấp các chức năng bổ sung như 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 10.1. 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.

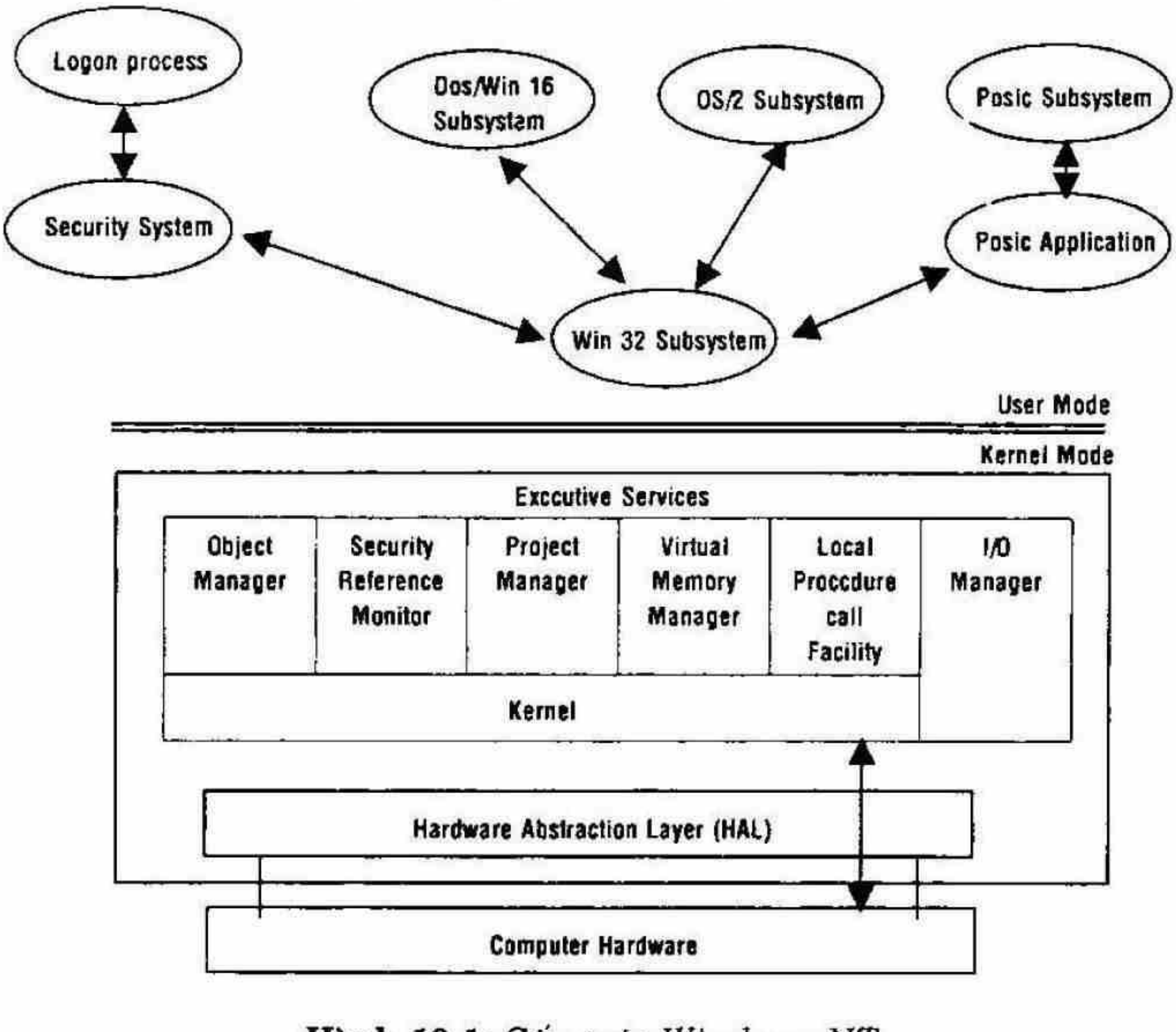
Hệ thống con (Subsystem) Win32 và các hệ thống con về môi trường, chẳng hạn như DOS/Win 16.0S/2 và hệ thống con POSIX chạy dưới chế độ user. Bằng cách đặt các hệ thống con này trong chế độ user, các nhà thiết kế Windows NT có thể hiệu chỉnh chúng dễ dàng hơn mà không cần thay đổi các thành phần được thiết kế để chạy dưới chế độ Kernel.

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 được 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 xử lý.



Hình 10.1: *Cấu trúc Windows NT*

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 trịnh (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

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 trên 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 (tuồng);
- 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).

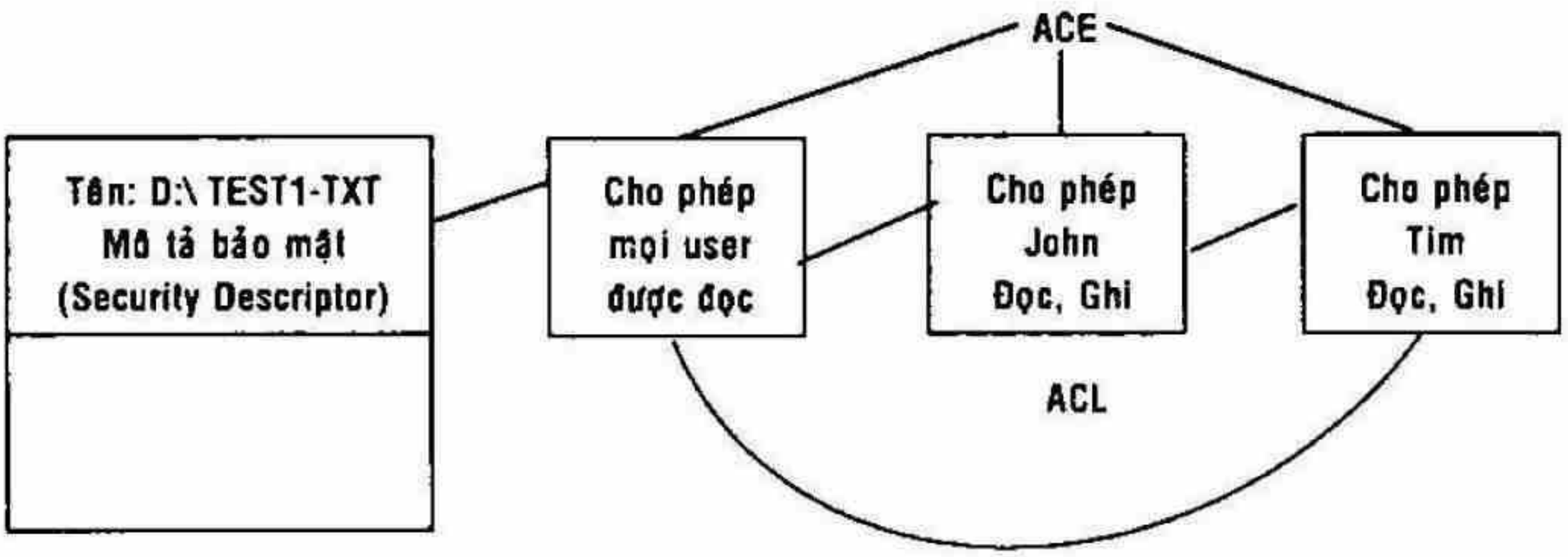
Cơ chế bảo mật (SRM – Security Reference Monitor) được sử dụng để thực hiện vấn đề an ninh trong hệ thống Windows NT. Các yêu cầu tạo một đối tượng phải được chuyển qua SRM để quyết định việc truy cập tài nguyên được cho phép hay không. SRM làm việc với hệ thống con bảo mật trong chế độ user. Hệ thống 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.

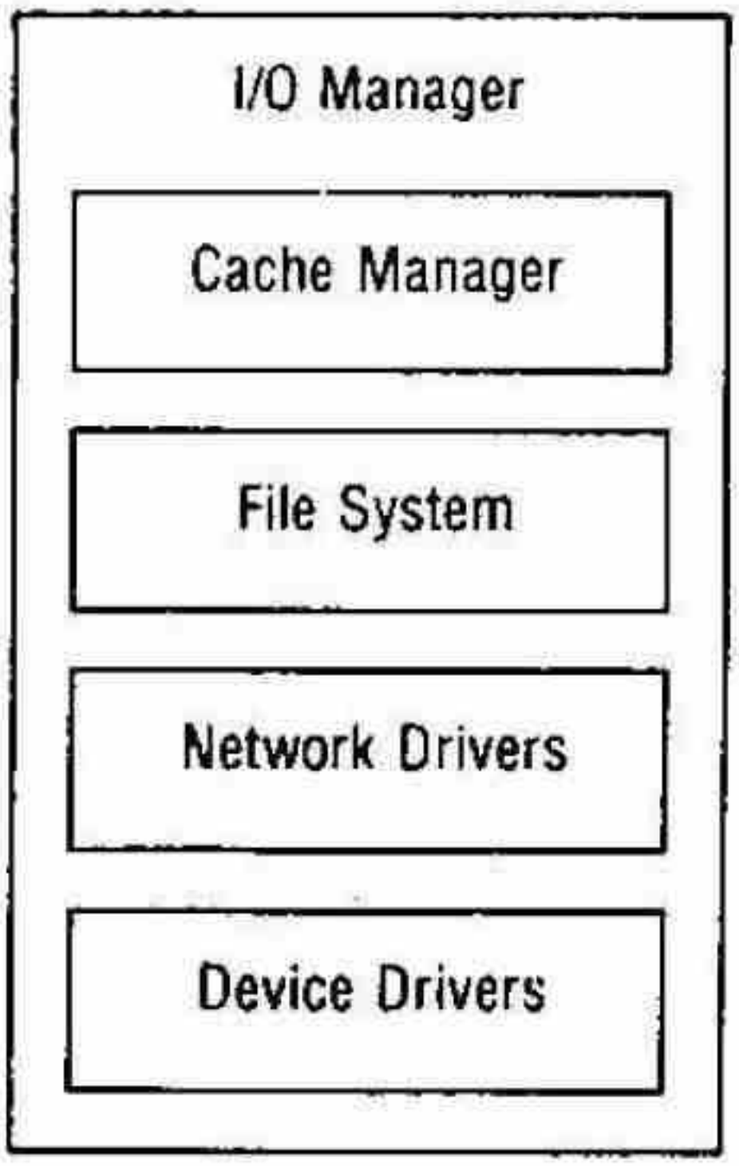
Khi người dùng tham gia mạng truy cập một đối tượng, Security Reference Monitor kiểm tra bộ mô tả bảo mật của đối tượng xem SID liệt kê trong SAT có phù hợp với giá trị trong ACE không. Nếu phù hợp, các quyền về an ninh được liệt trong ACE áp dụng cho người dùng đó.



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

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.

I/O Manager sử 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 (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 sáu 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 một mảng.
- *Mức 1*: Mức này ứng với biện pháp disk Mirroring, biện pháp này cho phép tạo ra hai 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 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 ghi 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 mức 4, số

liệu được phân nhỏ thành các khối lớn và sau đó ghi vào tất cả các đĩa. Các thông tin (party information) 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 patition. Biện pháp này bảo vệ dữ liệu tránh các sự cố bằng cách đưa ra chế độ thường xuyên backup đĩa hoặc partition.

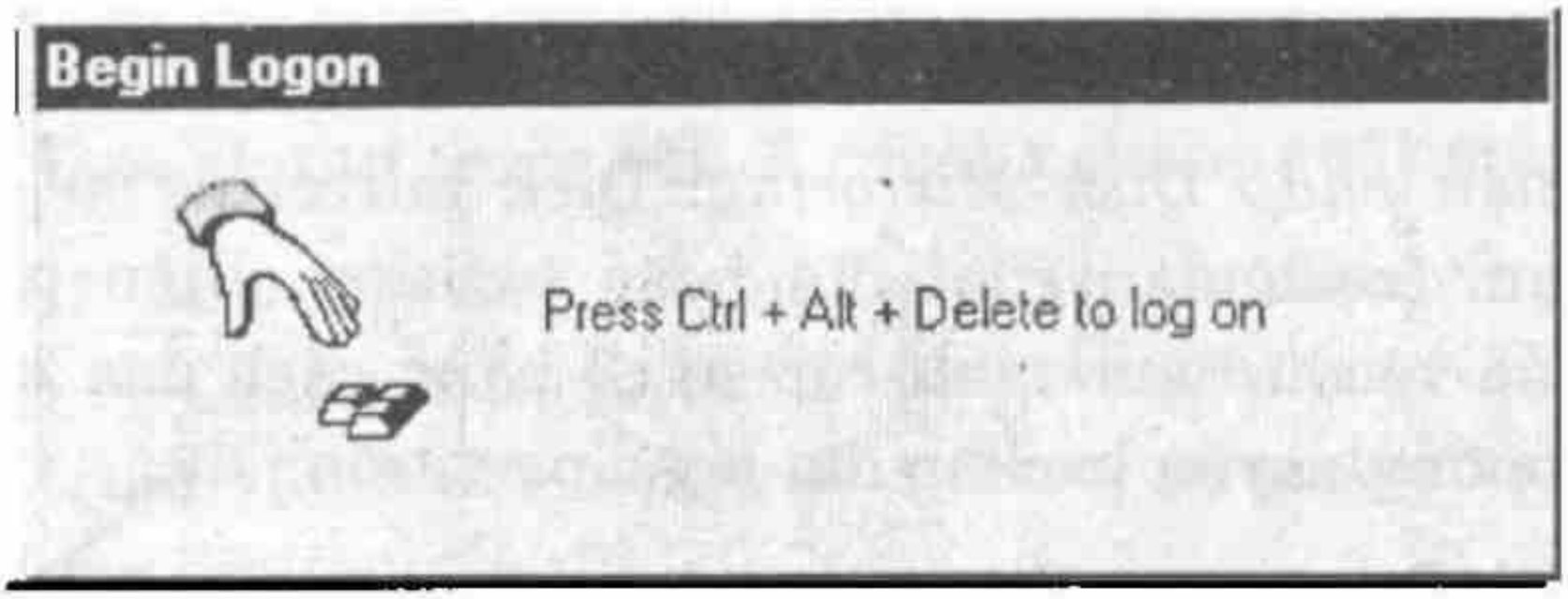
- *Disk Duplexing*: Biện pháp dùng đĩa kép (Disk Diplexing) tương tự như Disk Mirroring, chỉ khác là chúng dùng hai disk controler. Điều này cho thấy khả năng bảo vệ khi controler của một đĩa có sự cố. Trong khi đó biện pháp mirroring không thể khắc phục được tình huống này.

- *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 hai 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 riêng. Sau đó sao backup trở lại.

VI. GIỚI THIỆU VỀ HOẠT ĐỘNG CỦA WINDOWS NT SERVER

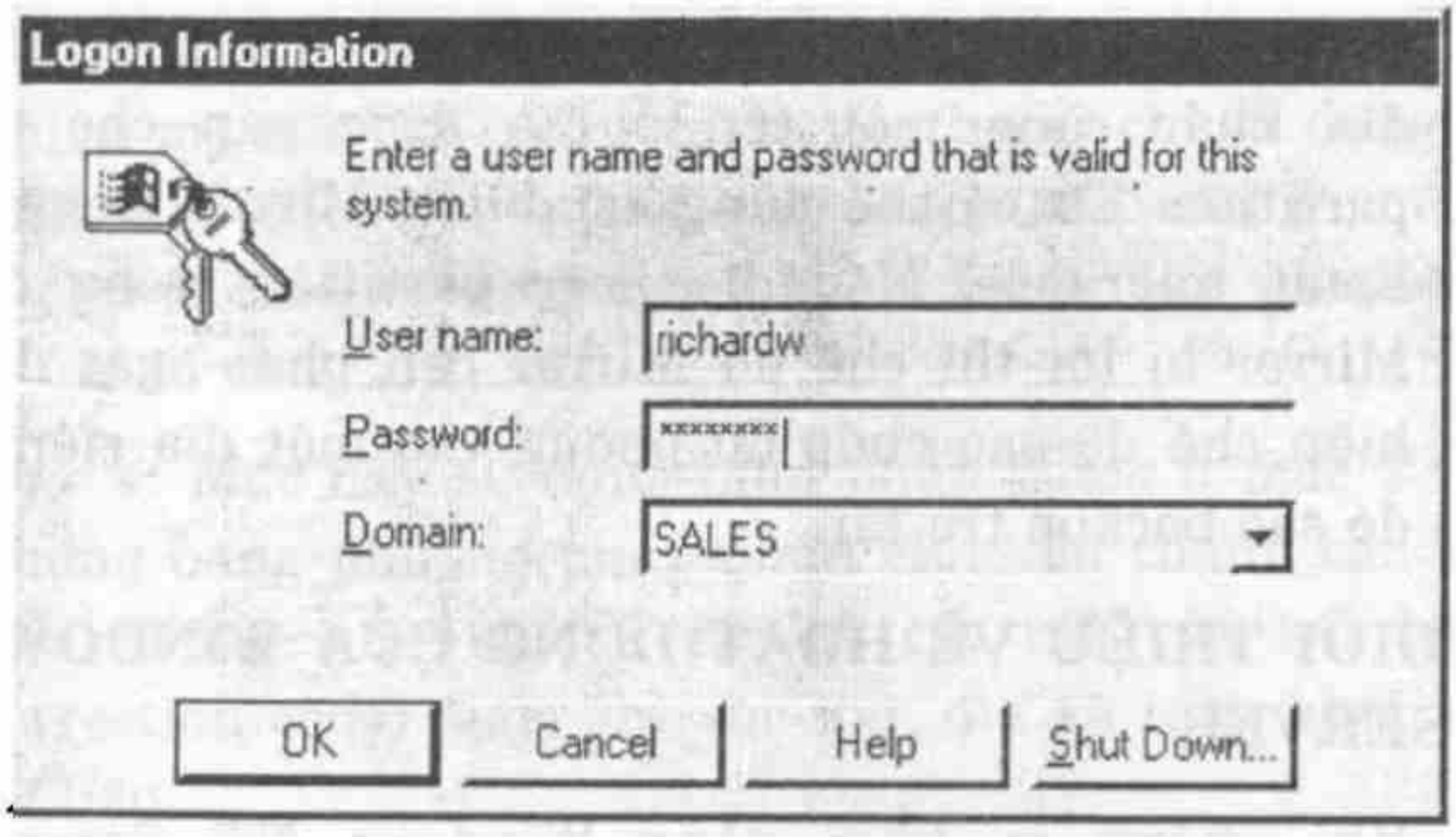
Khi chúng ta khởi động Windows NT Server hộp Begin logon sẽ hiện ra, server chờ đợi để chúng ta bấm Ctrl + Alt + Del để có thể tiếp tục hoạt động. Ở đây có điểm

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 yêu 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.

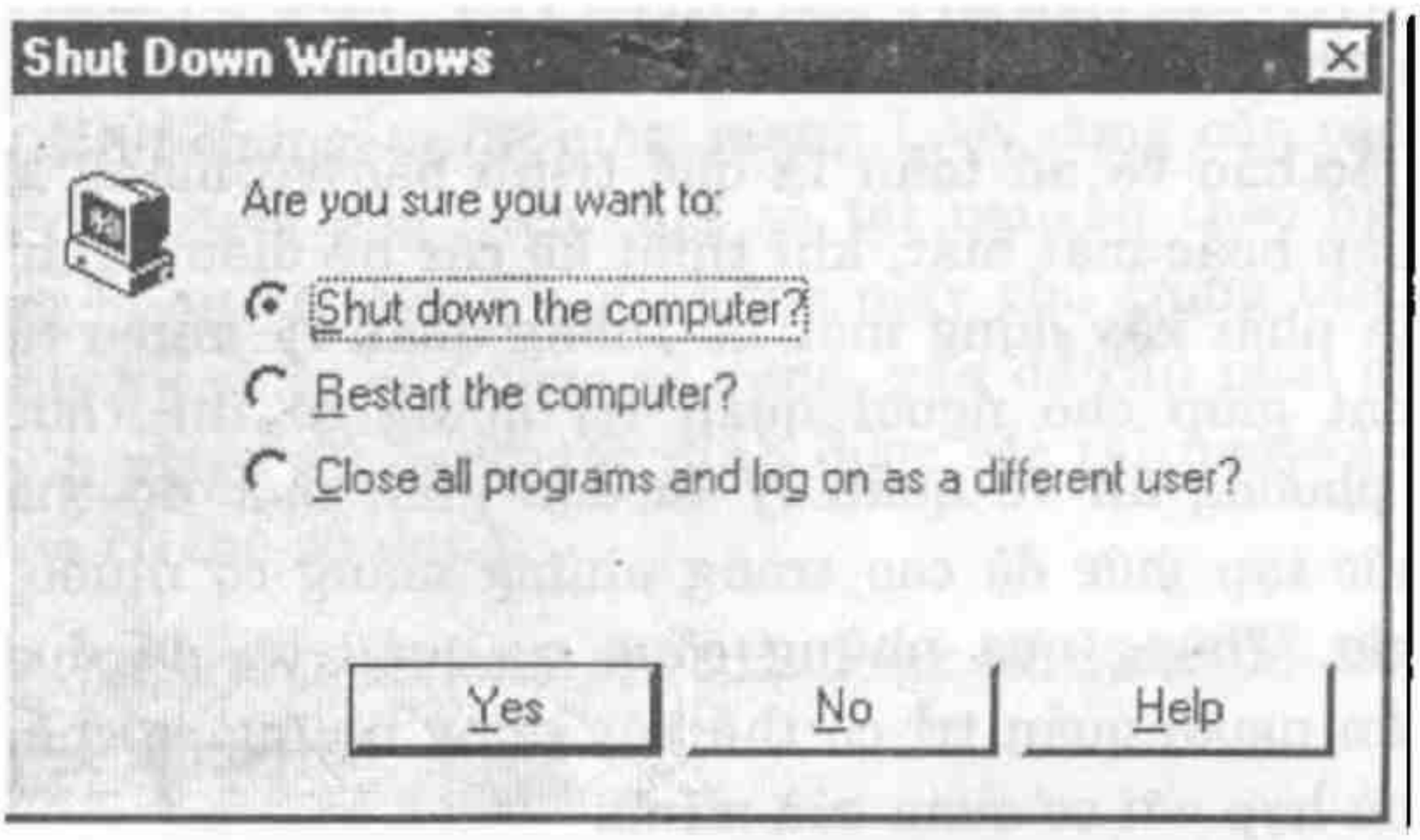


Hình 10.5: *Màn hình gia nhập mạng*

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 chọn 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 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 sẵn 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 giúp người sử dụng xác định được các tài nguyên có sẵn ở đâu để có thể sử dụng.

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

- Quản lý đơn lẻ từng máy chủ (stand–alone services);
- Quản lý theo dịch vụ như (directory services);
- Quản lý theo nhóm (workgroups);
- Quản lý theo domain (domains).

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 Servies)

Hệ thống các dịch vụ thư mục cho phép làm việc với mạng như là một hệ 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 hoặc dù các điểm nút của nó có thể nằm trên cả thế giới. Hệ điều hành Netware 4.x cung cấp dịch vụ nổi tiếng và đầy ưu thế cạnh tranh này với tên gọi ***Nerware Directory Services (NDS).***

Giải pháp này thích hợp với những mạng lớn. Các thông tin của NDS được đặt trong mô hệ thống cơ sở dữ liệu đồng bộ, rộng khắp được gọi 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 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 dụng 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 sẵn 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 ✔ ản 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 sẻ 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 sẵn 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 Windows for Workgroup, 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 và 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 các 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, Program 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 máy 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 của 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 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 người này có trong SAM của domain.

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

- Primary Domain Controller (PDC) bao giờ cũng phải có để quản trị hệ thống các người sử dụng các tài khoản trong domain (hệ thống này gọi là cơ sở dữ liệu SAM – Security Account Maganer 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 động 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 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 làm 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.

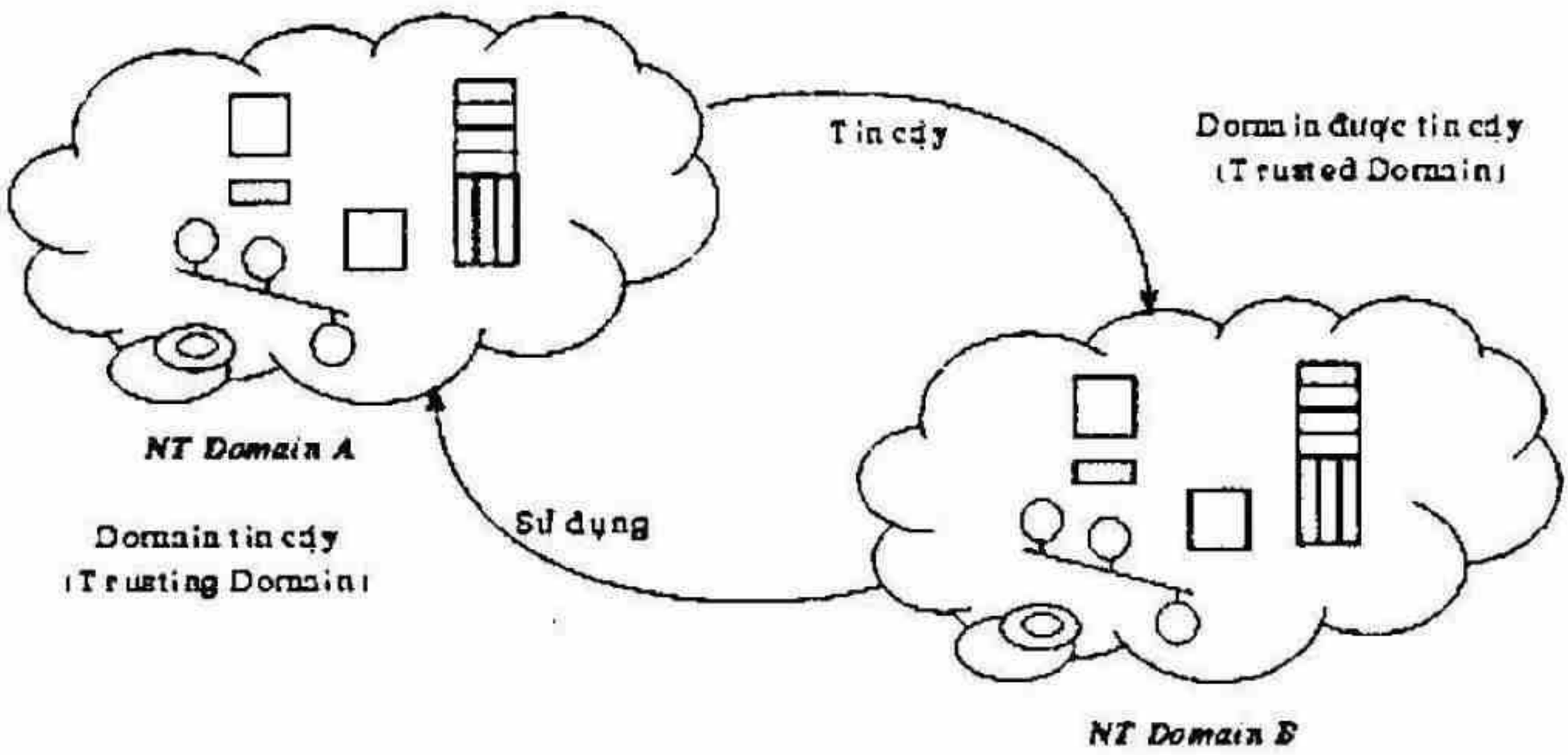
Khi người sử dụng truy nhập từ một máy trạm trong domain tin cậy (trusting domain) vào domain được tin cậy (trusted domain) thì quá trình kiểm soát diễn ra như sau:

- 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 giao 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 sử dụng 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 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 gorup). 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 vị của nhóm toàn cục là toàn bộ vùng trên đó user được 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 Domain Controller) của domain và được giao lưu đến các BDC (Backup Domain Controller) trong domain đó.

Nhóm toàn cục cố gắng toàn bộ cục được lưu ở PCD (Primary Domain Controller) của domain, và được sao lưu đến các PDC. (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 vào cấp cùng (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 truy xuất đến tài nguyên trên máy vi tính mà không 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 theo Sever 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 Managet* 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 trên 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 tài khoản người dùng cấp vùng (domain user account) và các nhóm toàn cục từ vùng trong đó họ được xác định.
- Các tài khoản người dùng cấp vùng (domain user account) và các nhóm toàn cục từ các vùng 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 server cung cấp 4 kiểu tổ chức domain gọi tắt là các mô hình domain (Domain models). Dưới đây là bốn mô hình tổ chức của nó:

- Mô hình domain đơn (single domain);
- Mô hình domain chính (master domain);
- Mô hình Multiple master domain;
- Mô hình Complete truts.

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.

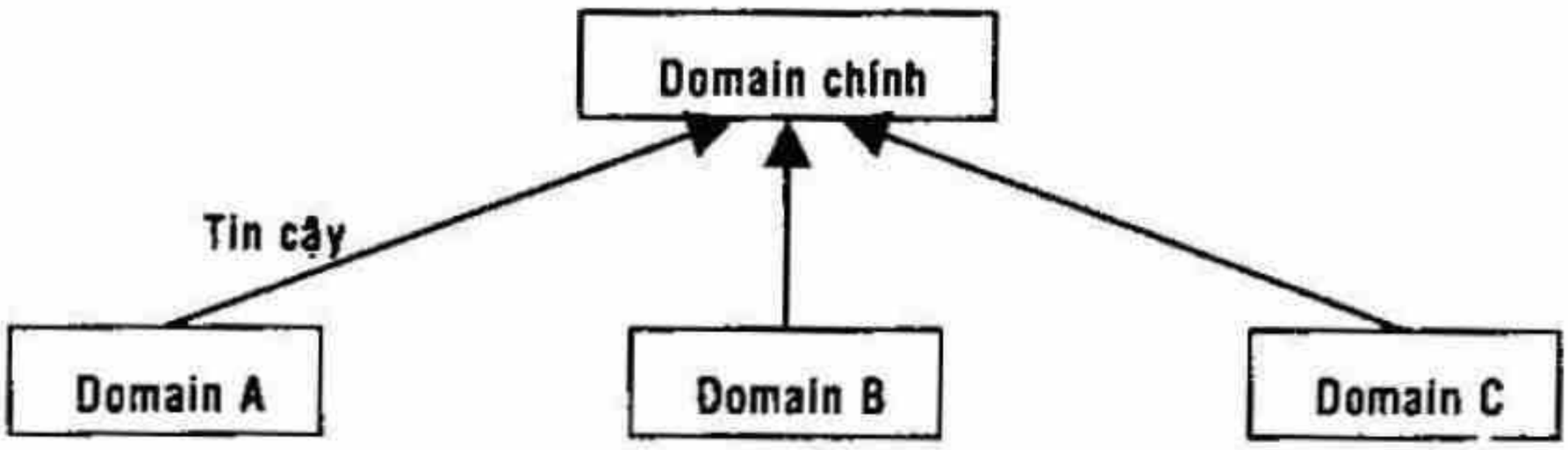
2. Mô hình domain chính (Master Domain)

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 đối tượng 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 một 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 domain khác 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)

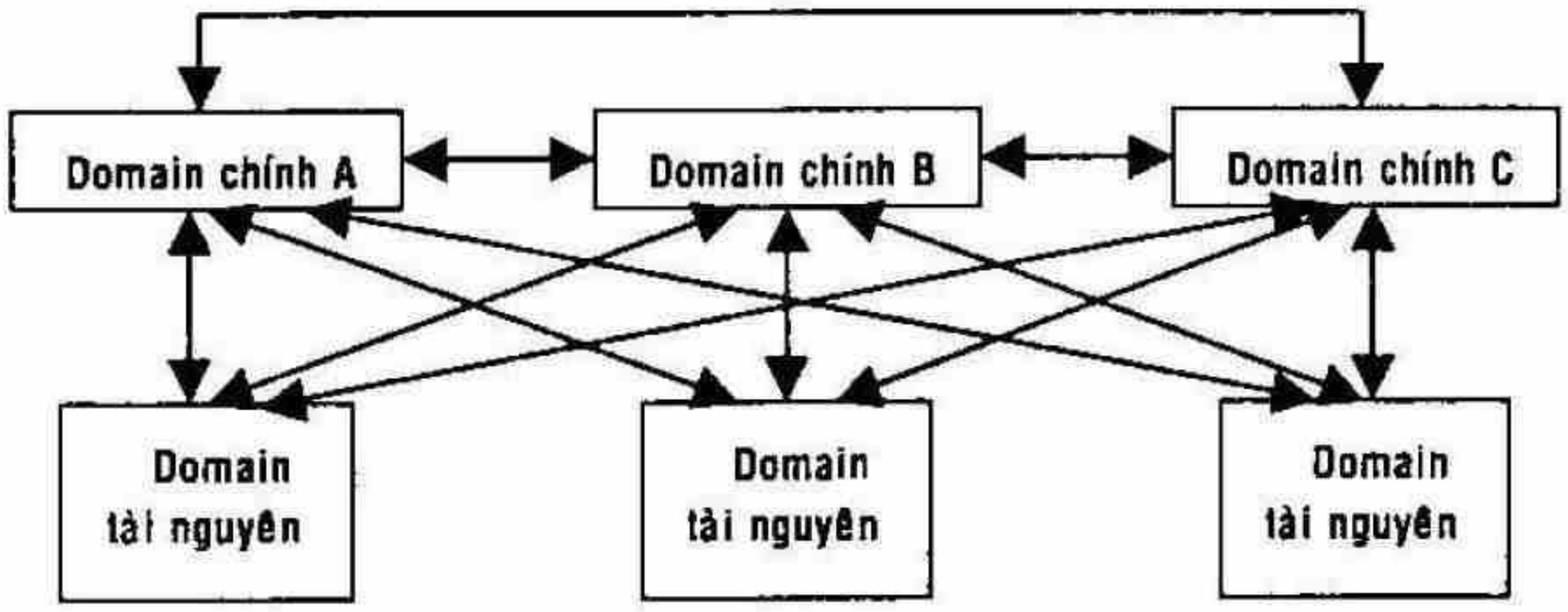
Mô hình nhiều domain chính (Muliple master domain) có thể được sử dụng cho các tổ chức có nhiều khu vực muốn quản lý tập trung các tài nguyên mạng trong khu vực. Chúng ta xây dựng một Domain chủ (master domain) cho mỗi khu vực và chia các tài nguyên trong mỗi khu vực thành nhiều Domain tài nguyên (Resoure 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 các 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.

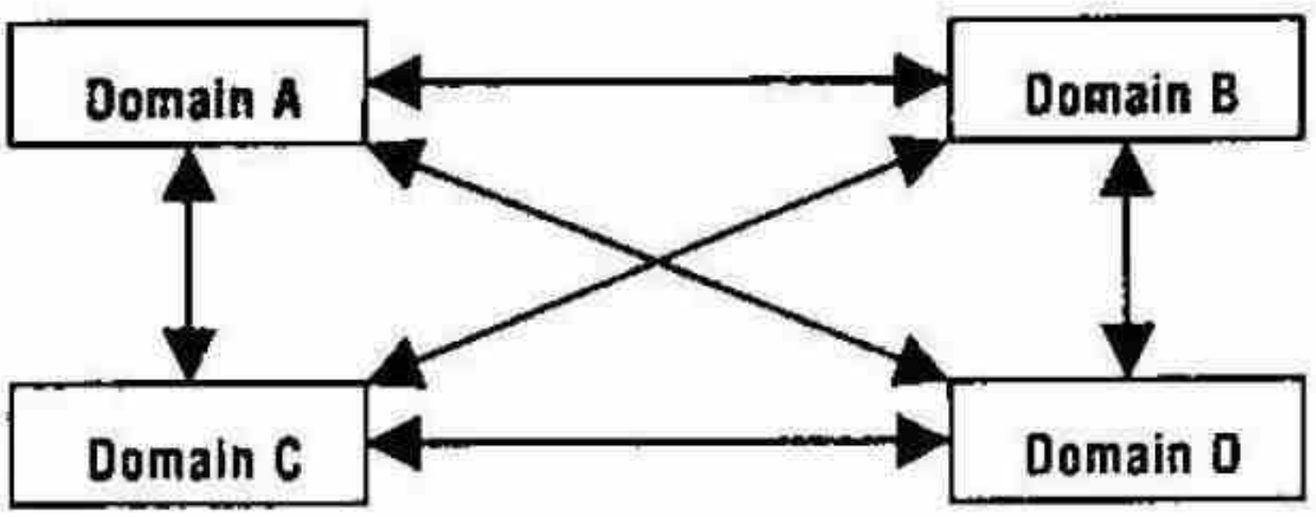


Hình 11.3: Mô hình nhiều domain chính

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 hai 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 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 kẽ 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 sẽ 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 1386) hoặc chúng ta chép thư mục 1386 lên đĩa cứng trước khi cài đặt. Để cài đặt Windows NT ta vào trong thư mục 1386 và chạy lệnh "WINNT".

Chú ý: Trong trường hợp này chương trình sẽ yêu cầu chuẩn bị ba 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:\1386.

Yêu cầu về phần cứng cho việc cài đặt Windows NT

Thiết bị phần cứng	YÊU CẦU
Processor	Intel 486, Pentium, Pentium Pro, hoặc 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 những thiết bị phân giải cao hơn

Hard disk	Tối thiểu phải có 110MB 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 đĩa Windows NT setup hay dùng lệnh WINNT/B từ thư mục 1386 trên đĩa CD-ROM. Nếu cài UPGRATE dùng lệnh WINNT32.
2) Xác định lại hay nếu cần thiết thay đổi 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 bằng Partition đã lựa chọn.
5) Chọn lựa thư mục mà các file của hệ điều hành Windows NT sẽ được 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 dĩa Emergency Repair Disk.

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

13) Quyết định 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 card 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 dịch vụ trên mạng. Các dịch vụ như là Microsoft Internet Information server, RPC Configuration, Netbios Interface, Workstation, Server.

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

19) Nếu chọn Nwlink IPX/SPX hay ICP/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 NT có tên là NTFS – New Technology File System có những ưu điểm 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 ba 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.

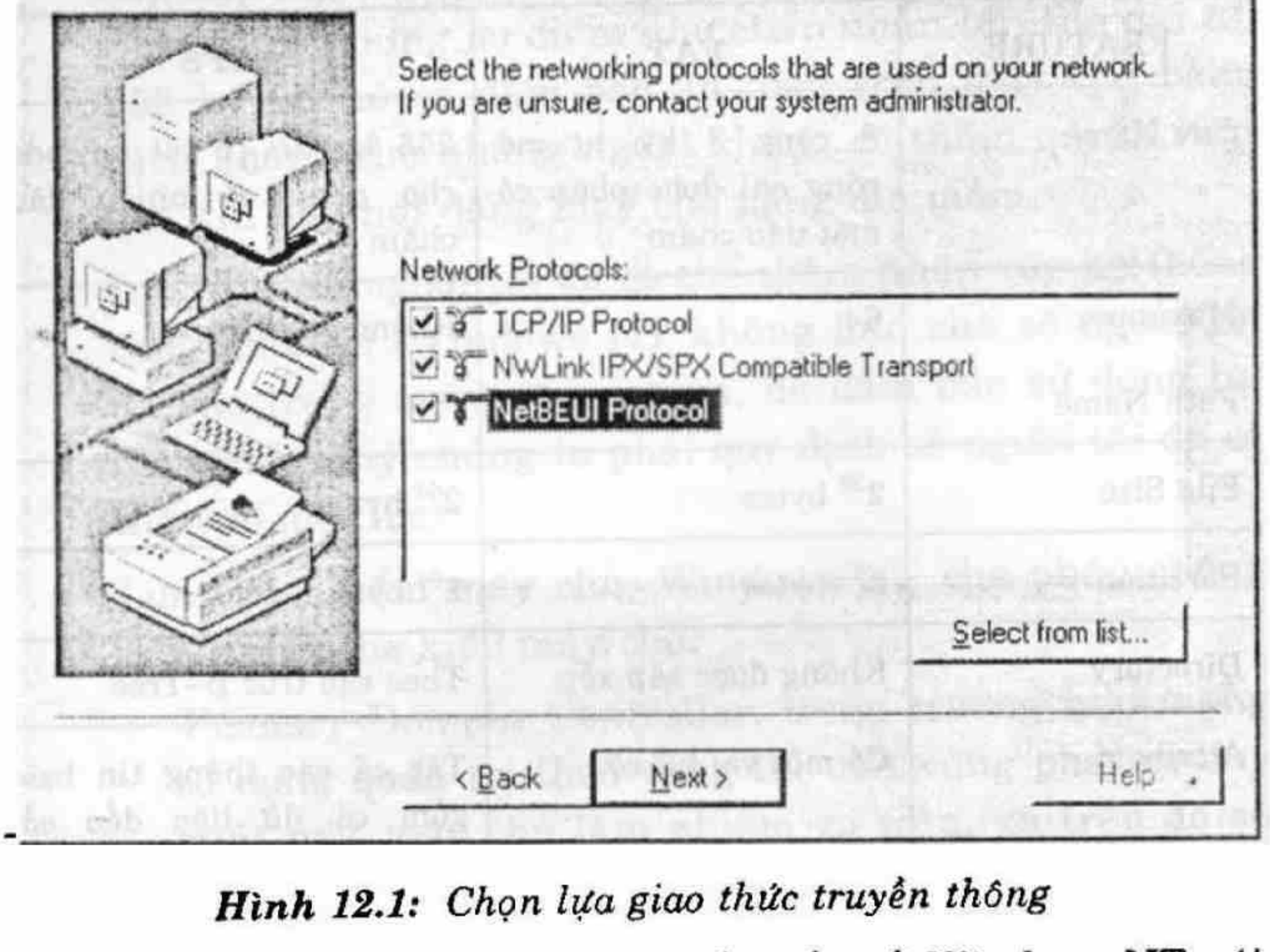
  + Backup Domain Controller: trong trường hợp mạng sử dụng quản trị theo vùng, ngoài máy chủ kiểu Primary Domain Controller có thể có một vài máy chủ lựa chọn kiểu này và trên đó sẽ lưu trữ cơ sở dữ liệu quản trị vùng (SAM) và được sử dụng khi máy chủ Prinary Domain Controller có trục trặc.

  + 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 chọn 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 tự, 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.

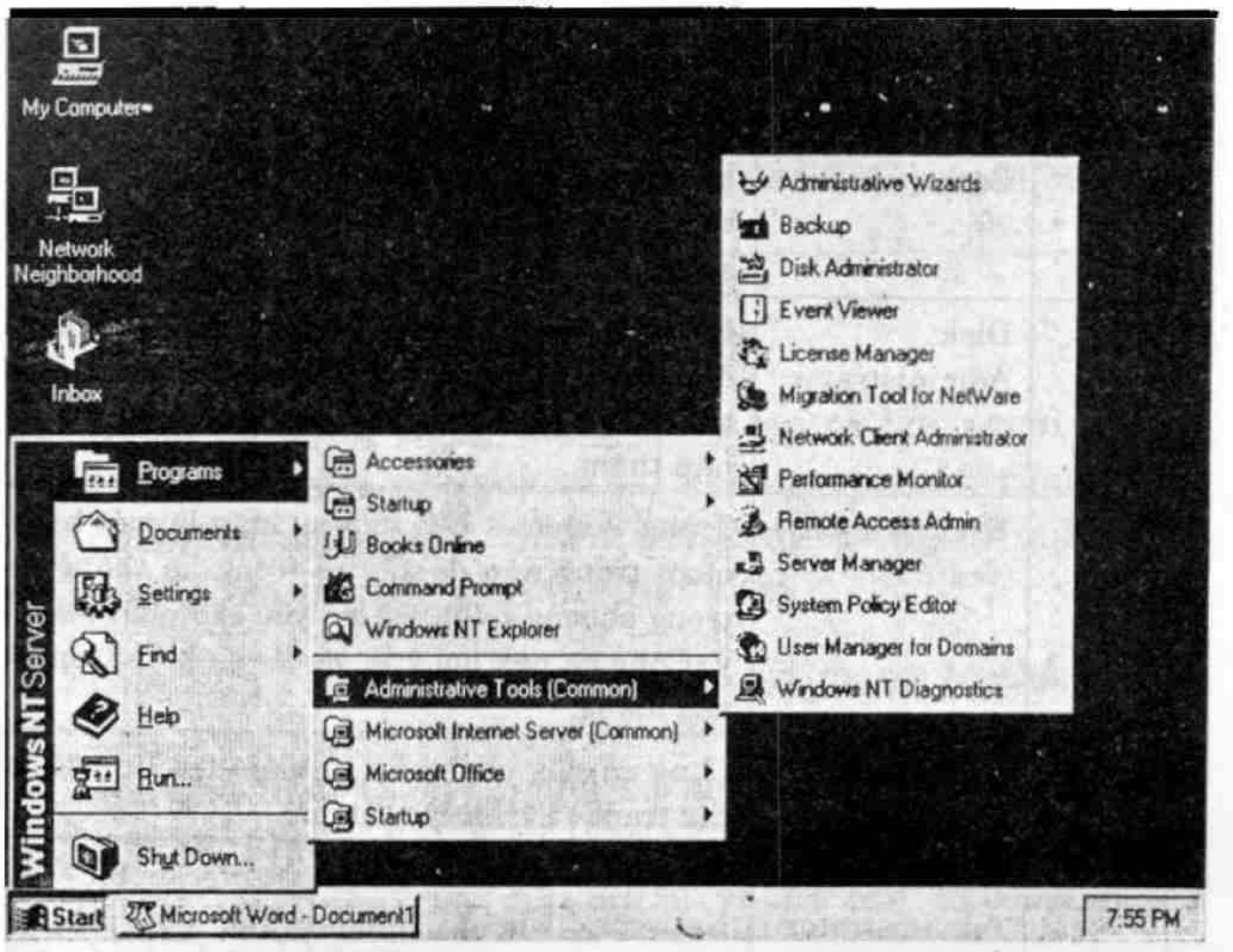


Hình 12.1: *Chọn lựa giao thức truyền thông*

- 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 lựa chọn 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 Contpoller 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 nhấp 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 sử dụng 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 băng 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 Administrator:* Sử dụng Network Client Adminitrator để cài 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 khác trên mạng.
	Remote Access Admin	Dùng công cụ này để kiểm tra quá trình nhập từ xa vào 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 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.
	Người sử dụng Manager for Domain	Công cụ này cho phép ta thiết lập, xóa các mã số của người sử dụng khỏi 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.

1. Khai báo một người sử dụng

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 vào buổi tối, giờ nghỉ, ... Khi người sử dụng đang chạy trong

mạng mà đã đến thời gian hạn chế thì họ sẽ nhận được thông báo là cần phải ra khỏi mạng. Nếu họ bỏ ra ngoài 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.

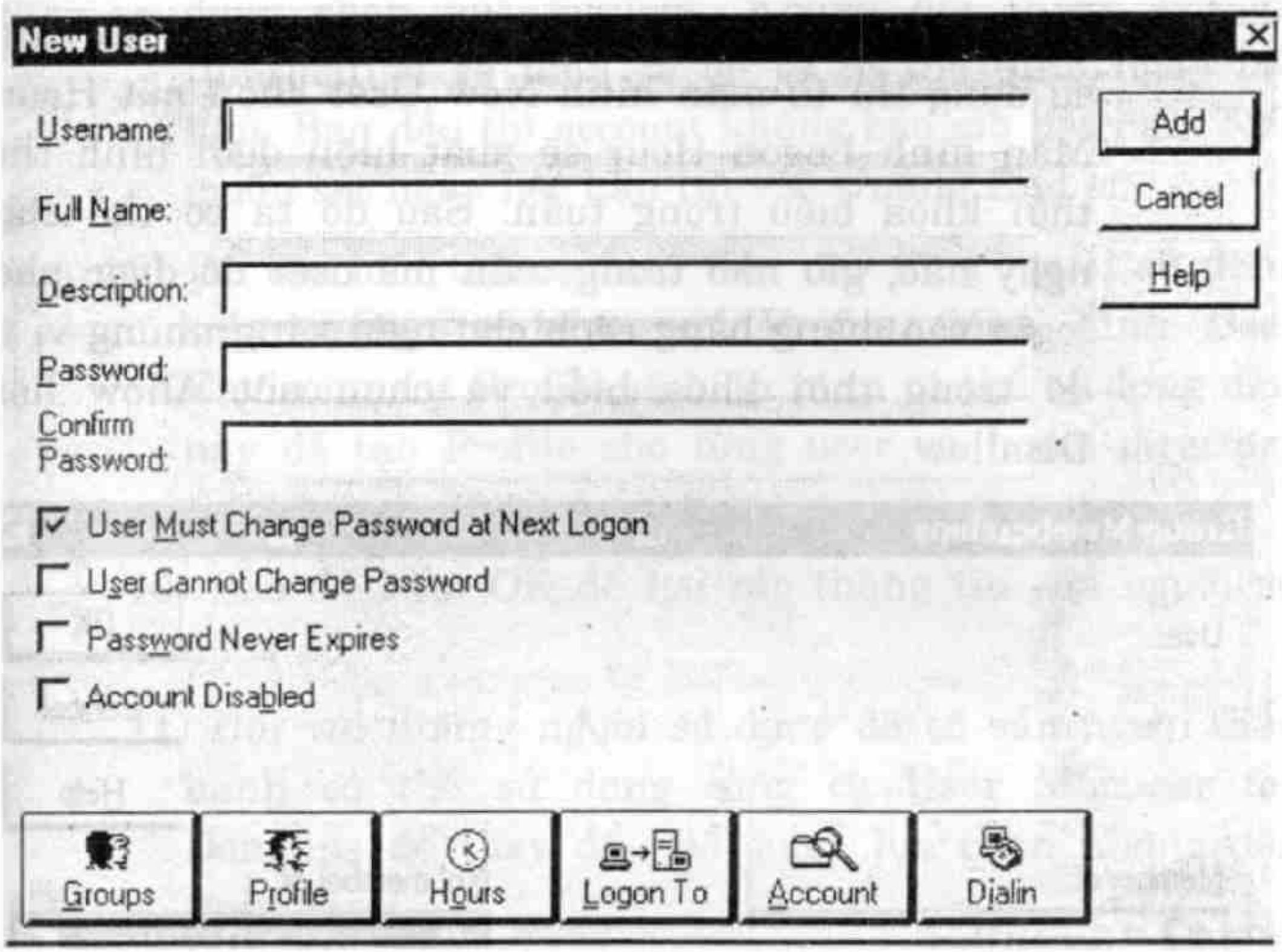
- *Quyền của người sử dụng*: Để xác định được quyền hạn của người sử dụng trên mạng chúng ta phải lựa chọn nhóm với những quyền đã được định trước.

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:

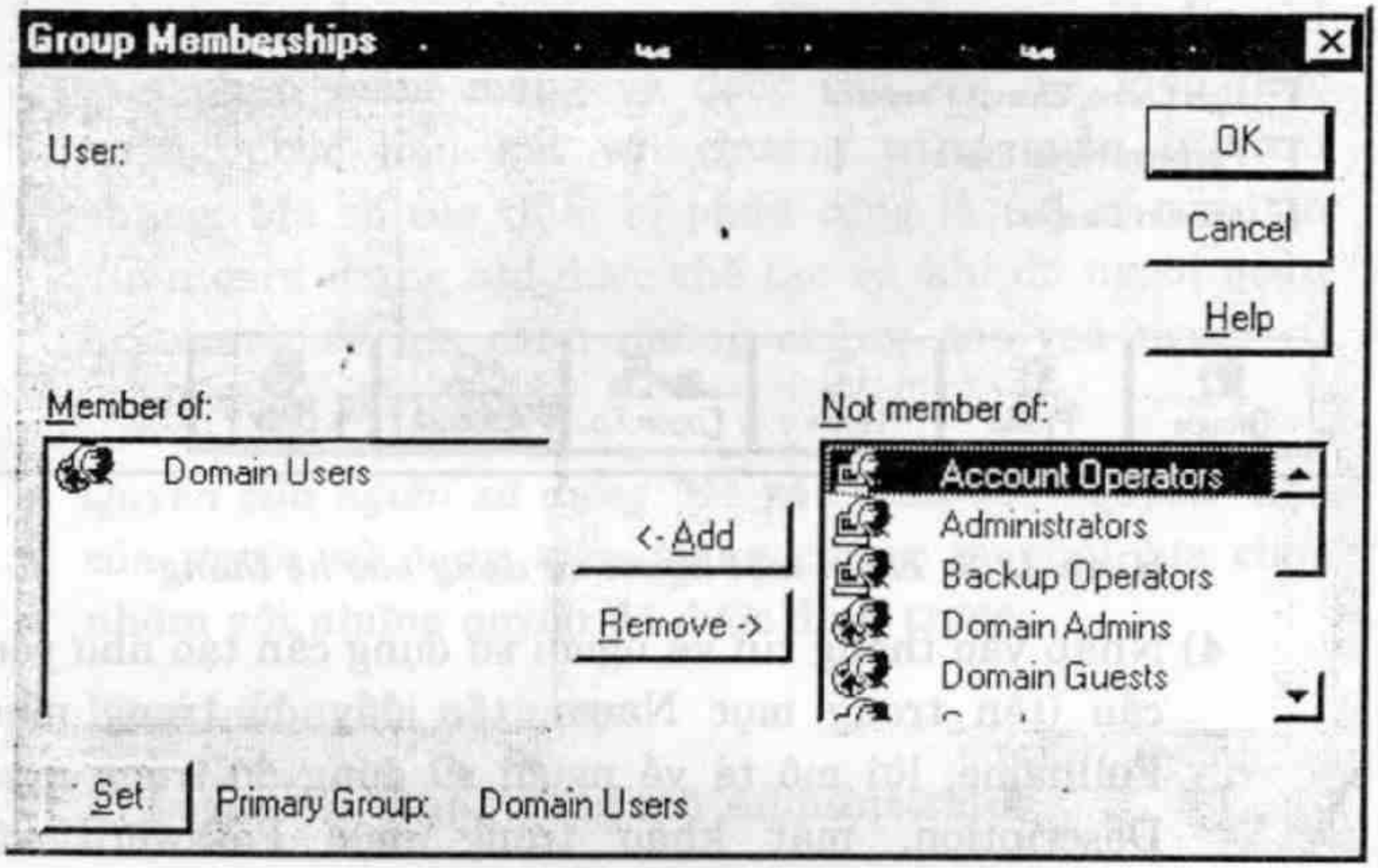


Hình 12.3: *Thêm một người sử dụng vào hệ thống*

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 đó. 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 Workstation sẽ xuất hiện. Để có thể 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 sẵn người điều hành có thể sử dụng công cụ User Manager for Domains để thay đổi, bổ sung, 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 thì 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 sẵn 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 devide drivers*: cho phép nạp hay không chương trình điều khiển ổ đĩa.
- *Manager auditting and security log*: quyền truy xuất mã số (account) 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 (thêm các thành phần, đối tượng khác).

Người điều hành có thể sử dụng công cụ User Manager for Domain để thay đổi, bổ sung, 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.
- *Creat and manage local groups*: tạo và quản lý nhóm cục bộ.
- *Assign users rights*: cho phép gán quyền cho người dùng.
- *Manage and auditting 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 driver*: 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:

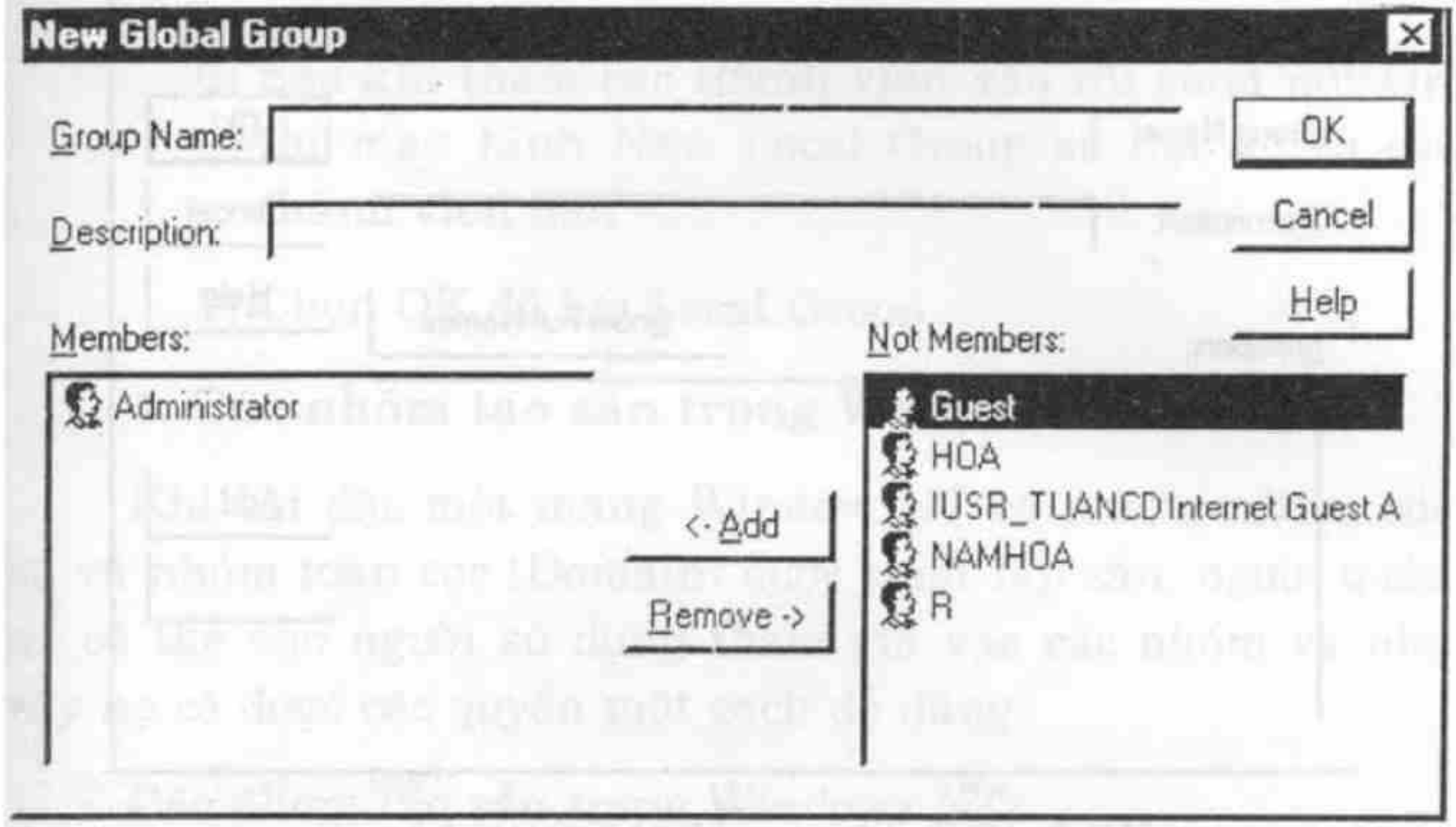
* Tạo nhóm toàn cục:

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

4) Sau khi hoàn thành chọn OK để kết thúc



Hình 12.5: *Thêm một nhóm toàn cục mới*

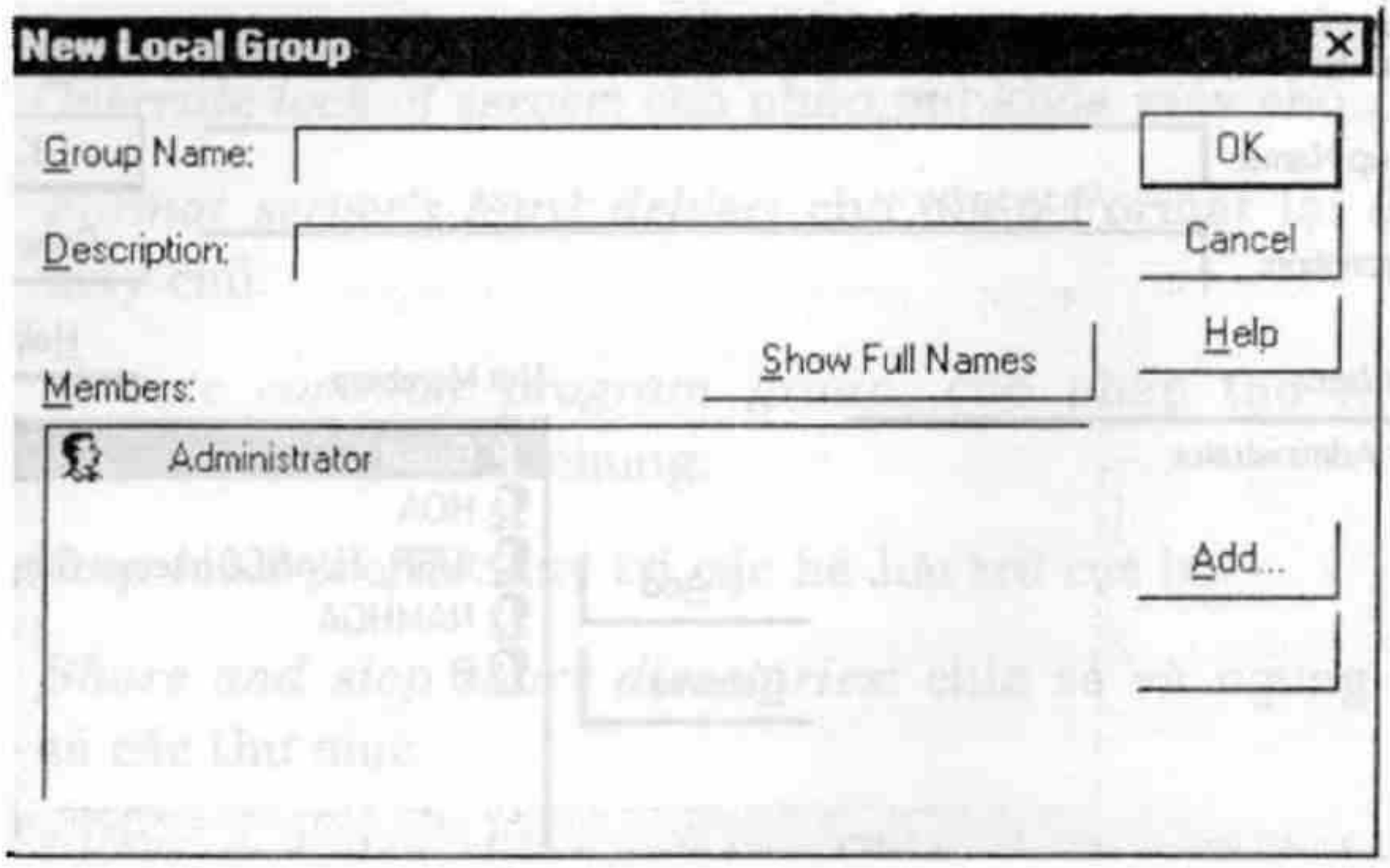
* Tạo cục bộ (Local Group):

1) Login vào mạng với tên Adminitrator

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

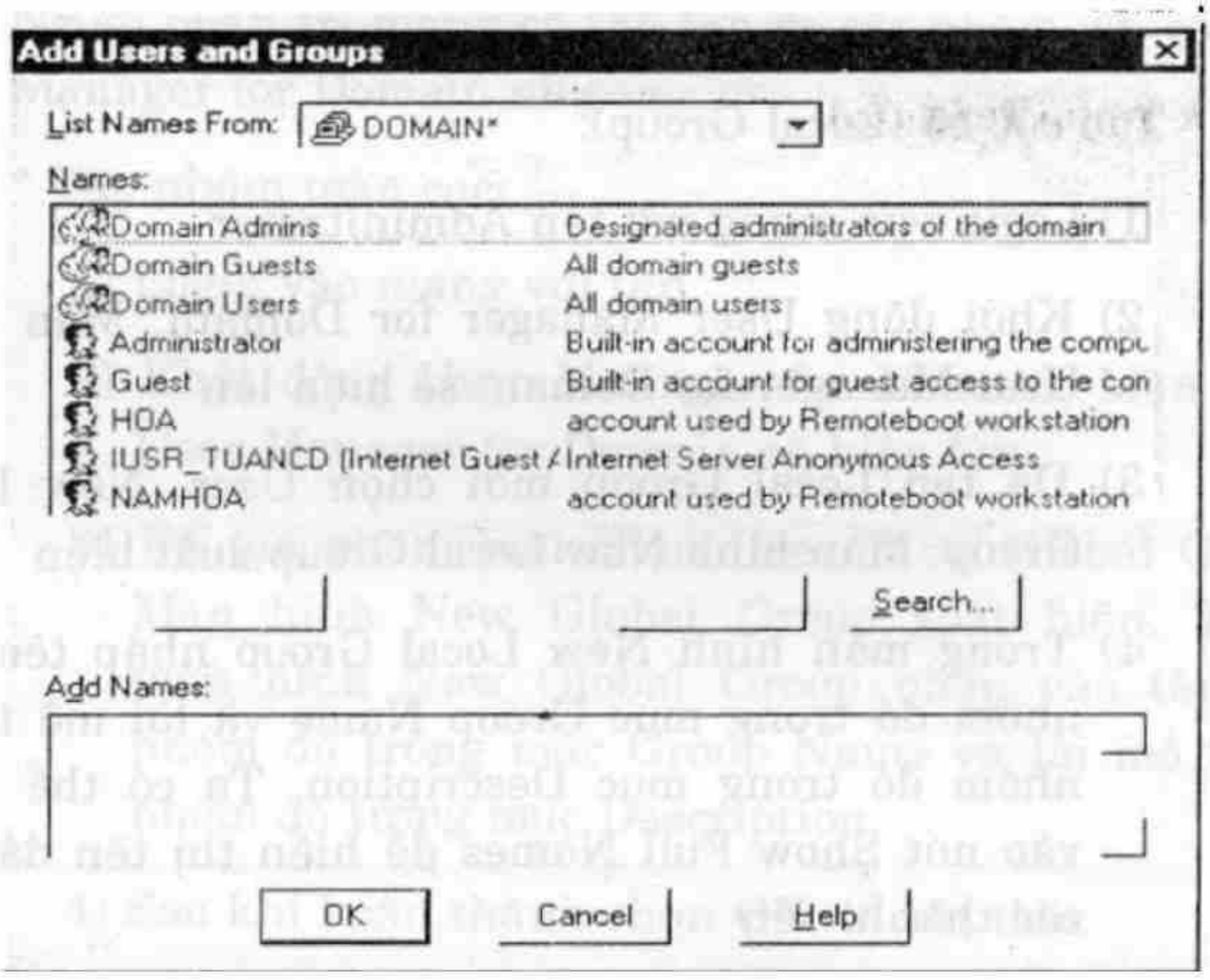
3) Để tạo Local Group mới chọn User, New Local Group. Màn hình New Local Group xuất hiện

4) Trong màn hình New Local 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 hiển thị tên đầy đủ các 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 sẵn trong Windows NT

Khi cài đặt một mạng Window NT có những nhóm cục bộ và nhóm toàn cục (Domain) được thiết lập sẵn, 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 sẵn trong Windows NT:

- *Adminitrator 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 sẻ tài nguyên trên mạng, cài đặt hệ điều hành, format đĩa 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 Backup và phục hồi dữ liệu. Những users thuộc nhóm này có thể thực hiện việc backup và hồi phục dữ liệu ngay khi họ không có quyền read / write trên thư mục hoặc file cần backup. Ngoài ra nhóm này còn có thể Shutdown hệ thống.

- *Account Operater*: 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 Adminitrator nhưng họ không thể quản lý việc bảo mật trên server. Họ có thể share, stop share máy in, thư mục và file, format đĩa cứng, họ cũng có thể backup và restore dữ liệu, shutdown hệ thống. Nhưng họ không thể start hay stop các dịch vụ trong mạng.

- *Domain Adminitrator*: đây là Global group và là thành viên của Adminitrator Local Group nó chứa User Adminitrator.

- *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 Adminitrator 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	Eveyone	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 and Directory	X	X			X			
Restore files and directory	X	X			X			
Load and Unload device drivers	X							
Add workstation to domani	X							

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

Built-in capabilities	Adminis-trator	Server Operator	Account Opertor	Print Operator	Backup Operator	Eveyone	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 với 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 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 đến 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 một 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 cá 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 profile 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 có ích cho việc kiểm tra quá trình truy nhập vào môi trường.

Profile có ba lợi ích chính 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 cho phép.

Trong Window NT có một 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 quy 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 một 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 sẽ được 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 được 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, Wrire, 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), Chúng ta có thể gán nhiều mức truy cập (permission) khác nhau đến các tập tin thông qua các quyền được gán trên các tập tin. Có năm mức truy cập được định nghĩa trước liên quan đến việc truy xuất tập tin (File và thư mục) là: No Access, Read, Change, Full Control, Special

Access. Special Access được tạo ra 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 Window 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 người dùng và các nhóm trùng nhau.
- Nếu một trong các 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 Administrator 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 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 được 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 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 cùng 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

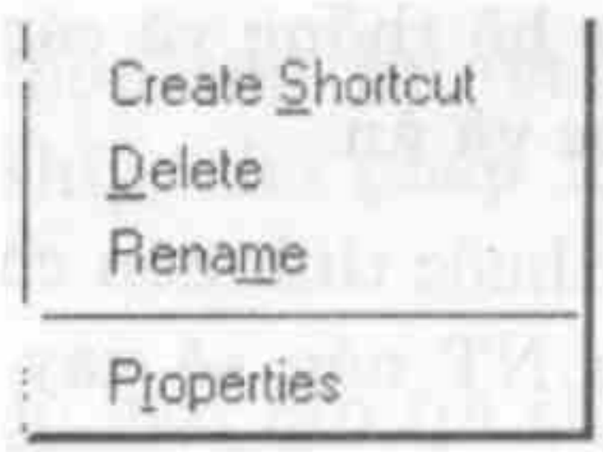
chế việc truy xuất tới một phần của cây thư mục, chúng ta phải sử dụng việc cấp các quyền cho một user hay một nhóm đối với các thư mục và các file đó.

Để chia sẻ một thư mục ta phải Login như một thành viên của nhóm quản trị mạng hay nhóm điều hành server.

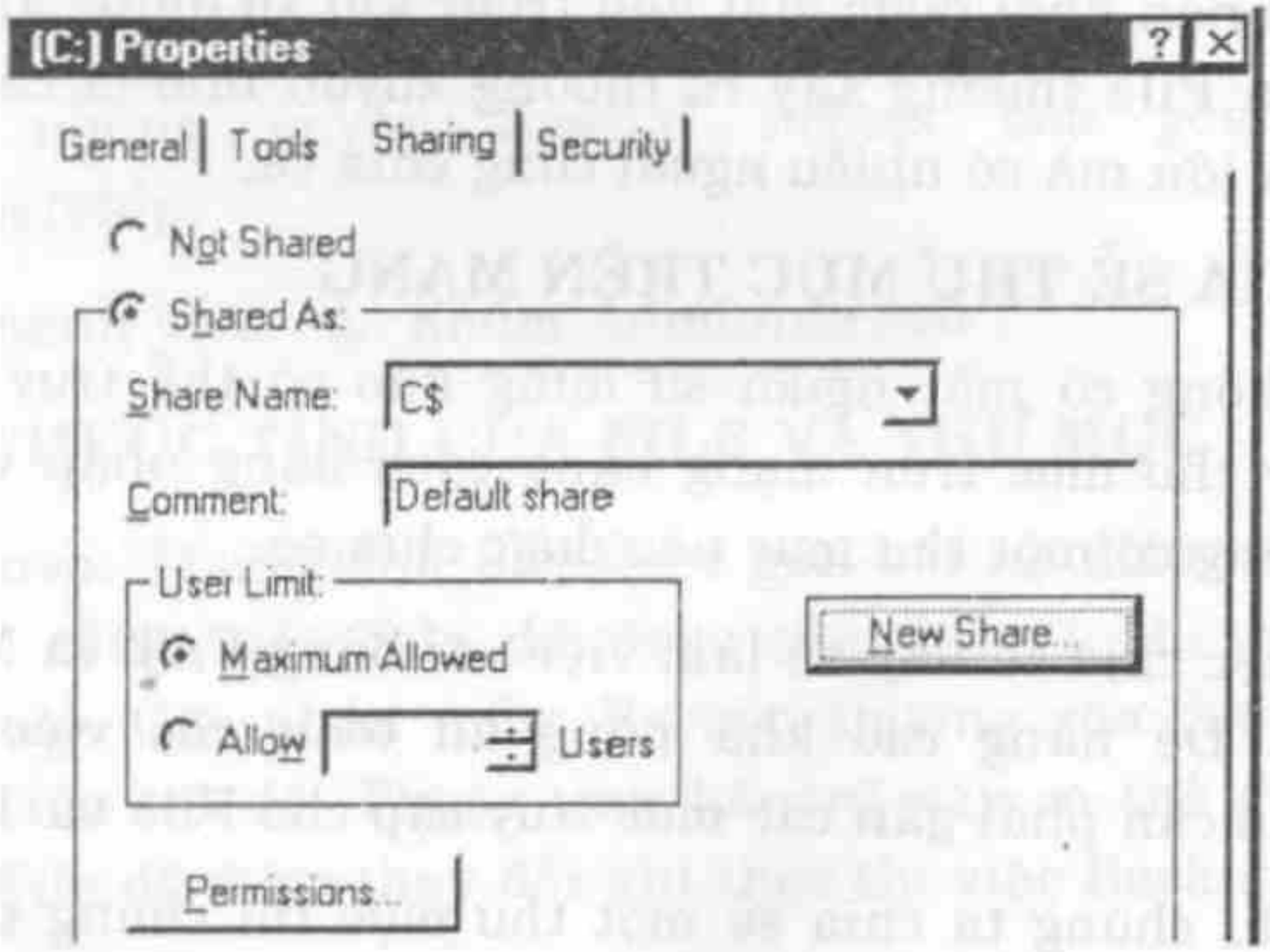
Tất cả các thủ tục chia sẻ thư mục được thực thi trong Windows NT Explorer.

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 hội thoại sau:

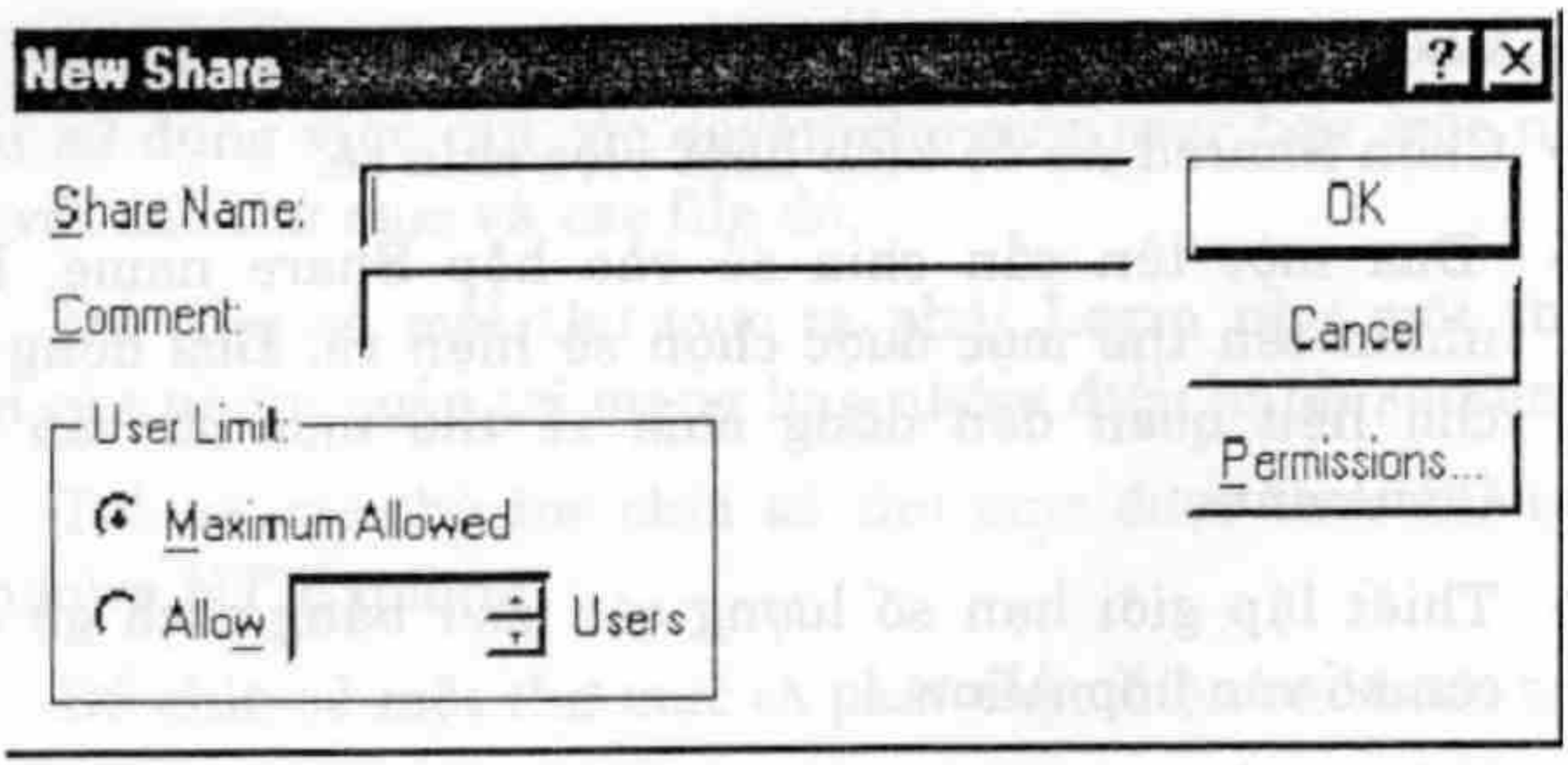


- Chọn Sharing tab hiện ra hộp đối thoại sau:
- Chọn Shared As để kích hoạt việc chia sẻ.
- Đưa một tên cần chia sẻ vào hộp Share name. Mặc nhiên tên thư mục được chọn sẽ hiện ra. Đưa dòng ghi chú liên quan đến dòng chia sẻ thư mục đó vào hộp Comment.
- Thiết lập giới hạn số lượng các user bằng cách gõ 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 một 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 thoại Properties
- Click Sharing tab.
- Click button New Share để tạo một sự chia sẻ mới, hiện ra hộp đối thoại sau:

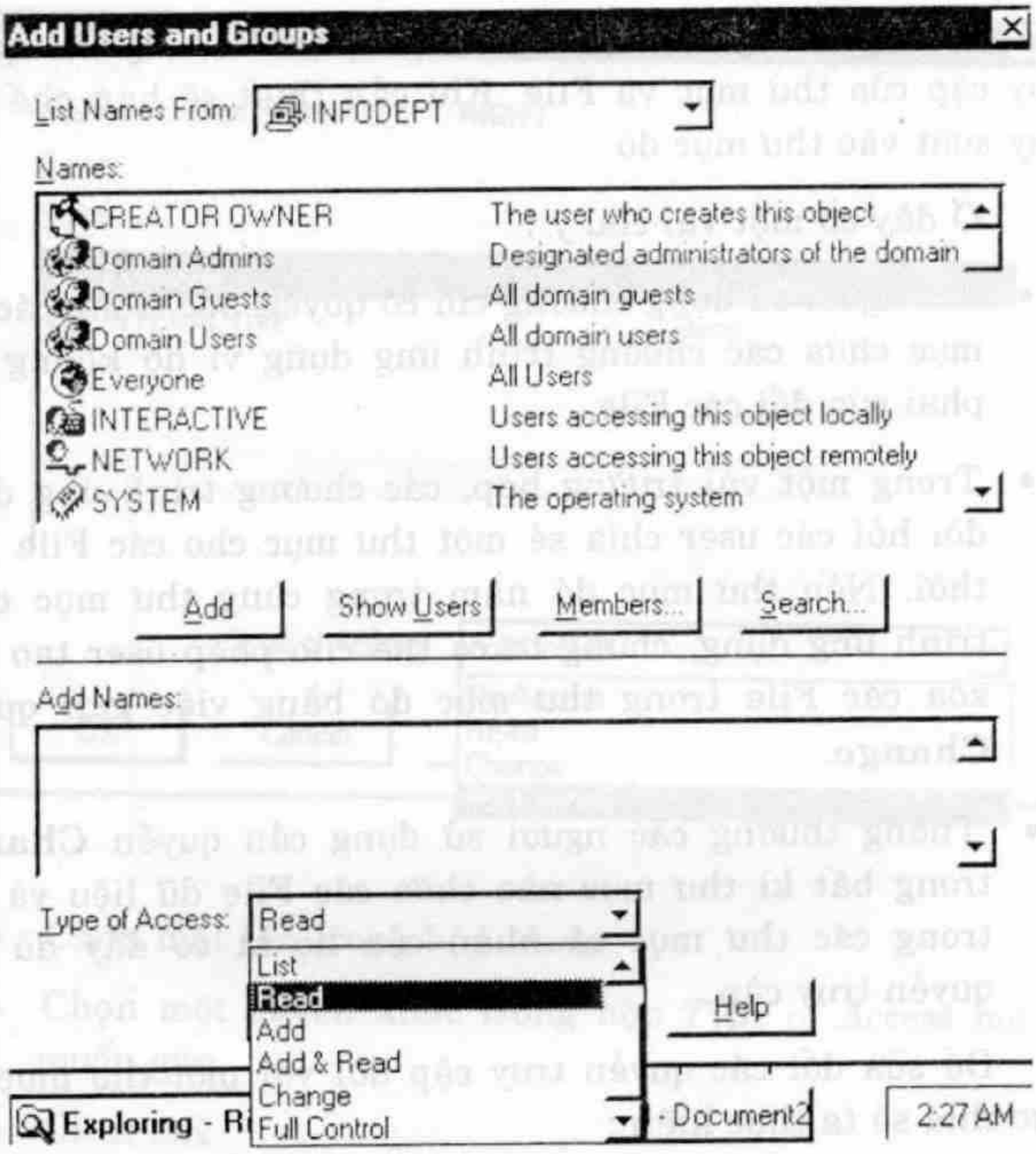


- Mỗi lần tạo một sự chia sẻ chúng ta phải đưa một tên mới cũng như những lời chú thích việc chia sẻ đó sẽ cho ai sử dụng.

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 name*.

- 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 một nhóm Everyone là đầy đủ (**Full Control**).

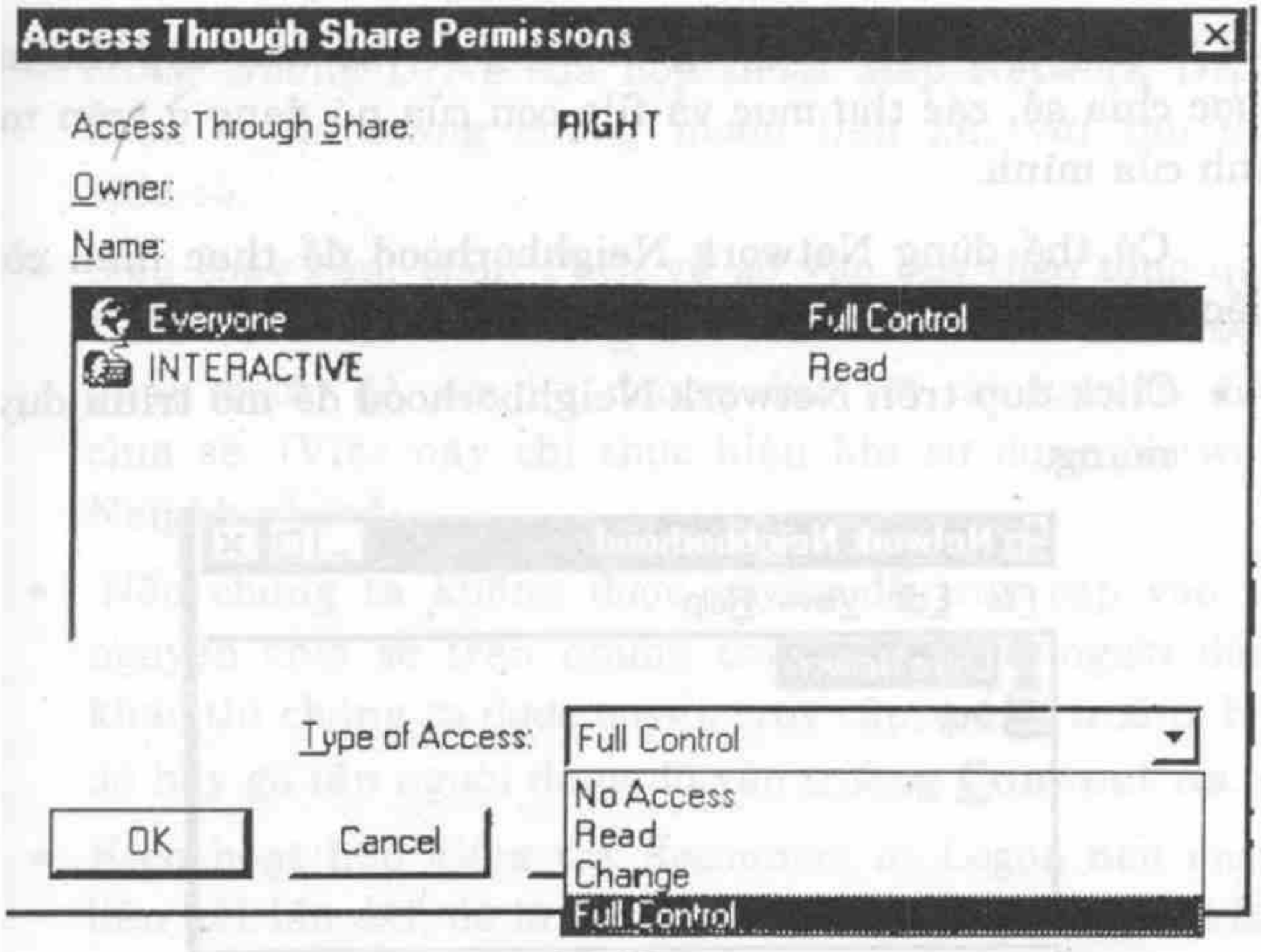
Giả sử rằng chúng ta sẽ gán giá trị mặc nhiên này cho quyền truy cập của thư mục và File. Khi cần thiết sẽ hạn chế việc truy xuất vào thư mục đó .

Ở đây có một vài chú ý :

- Các người sử dụng thường chỉ có 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 kì thư mục nào chứa các File dữ liệu và chỉ trong các thư mục cá nhân của họ là có đầy đủ các quyền truy cập.

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 một 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.

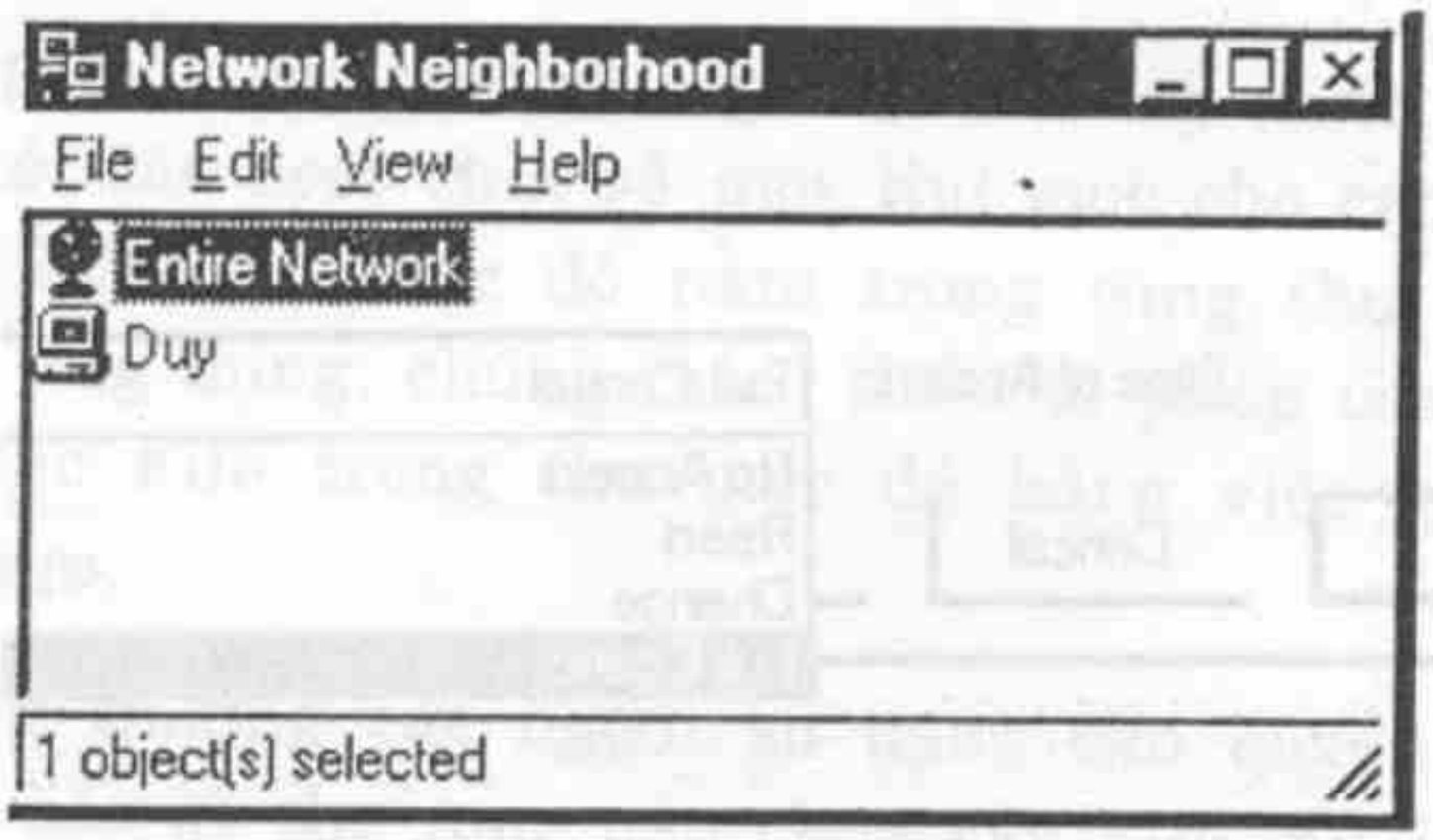
V. SỬ DỤNG CÁC THƯ MỤC MẠNG

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

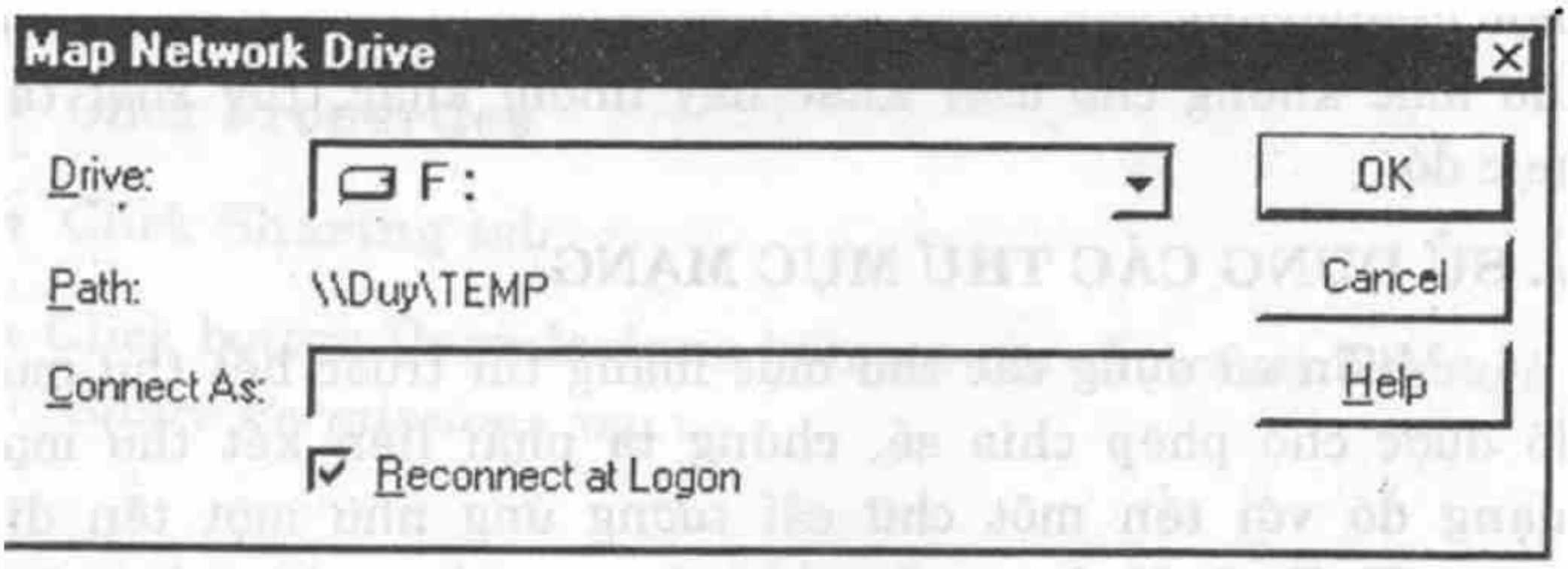
nối với ký tự ổ đĩa mạng người dùng có thể truy cập thư mục được chia sẻ, các thư mục và file con của nó đang ở trên máy tính của mình.

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 **Conneet As**.
- Kích hoạt hộp kiểm tra Reconneet at Logon nếu muốn liên kết lâu dài, đó là loại kết nối được phục hồi mỗi lần chúng 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.

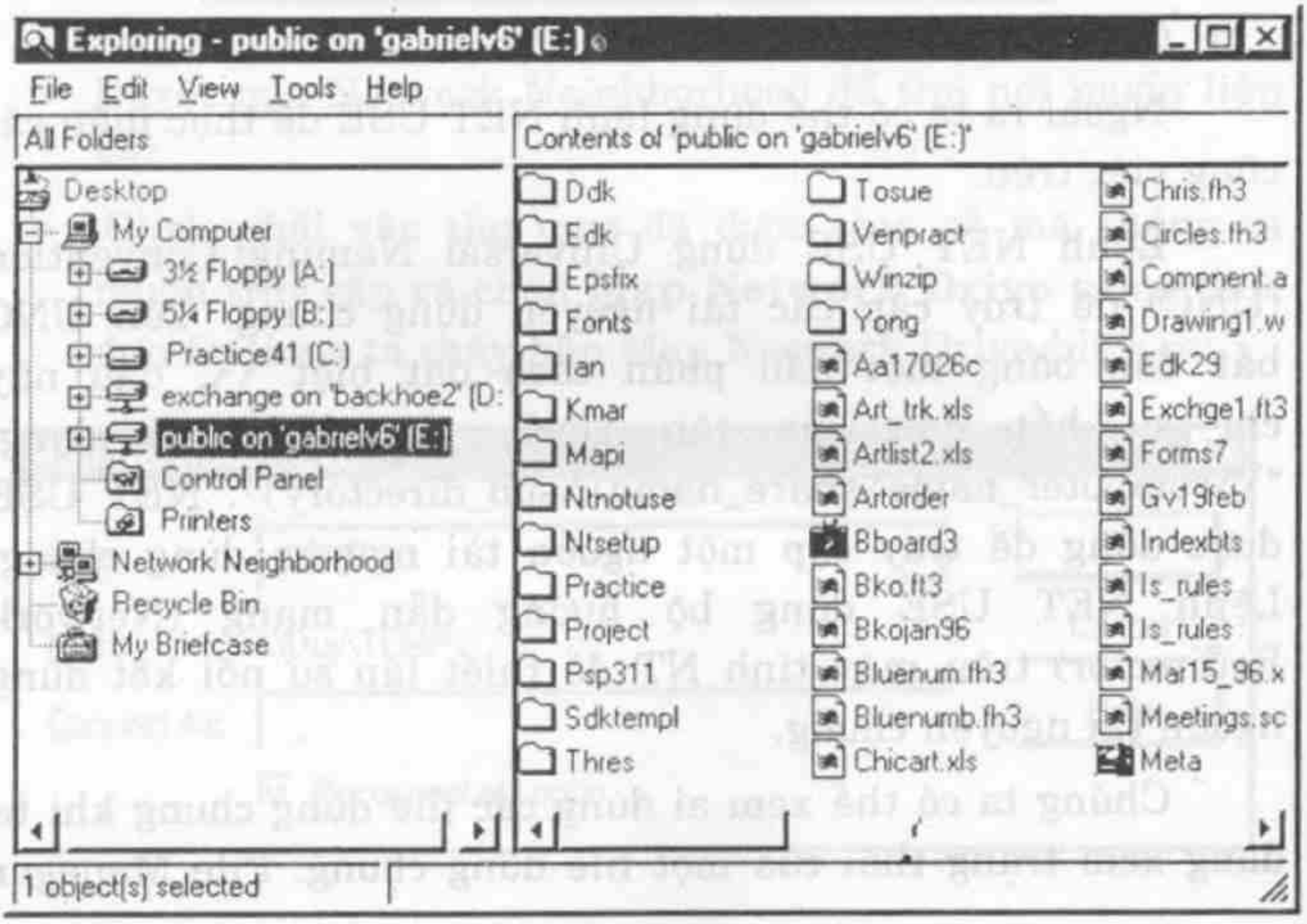
Lệnh NET USE dùng Universal Naming Convention (UNC) để truy cập các tài nguyên dùng chung. Tên UNC bắt đầu bằng một dấu phân cách đặt biệt \\, dấu này chỉ sự bắt đầu của tên UNC, tên UNC có dạng: "\\computer_name\share_name|\sub_directory|". NET USE được dùng để truy cập một nguồn tài nguyên dùng chung. 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 tên 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 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 mà bất kì máy tính Windows NT nào cũng có thể cung cấp các dịch dụ 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 hai việc một lúc, nếu phải nhận cùng một lúc thì sẽ có xung đột, 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 quản 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 truy xuất đồng thời ra máy in.

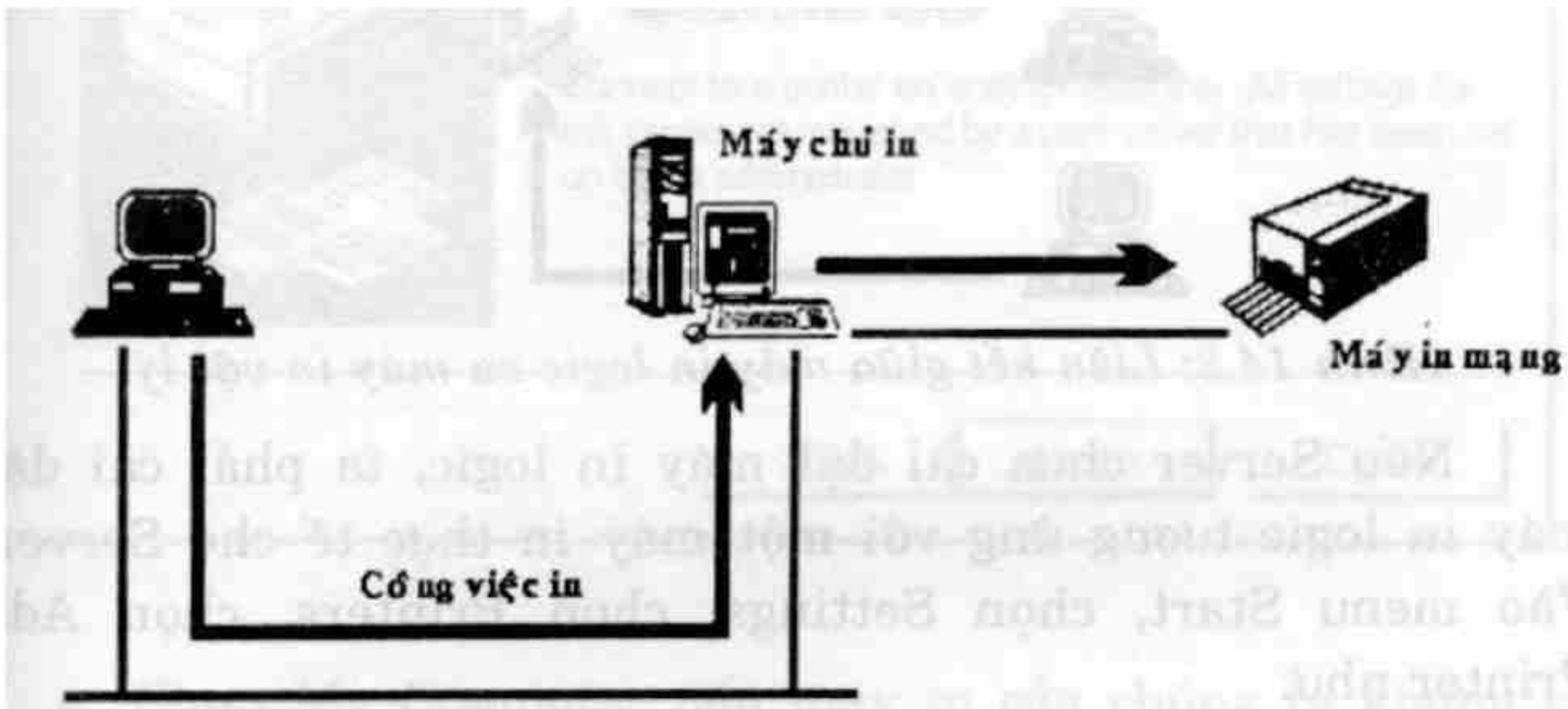
- Máy chủ in duy trì các hàng đợi để cất giữ các công việc in và đưa chúng tới máy in ngay khi có thể. Trong khi đó người sử dụng có thể làm tiếp công việc ngay khi công việc in được cất vào hàng đợi.

- 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 nảy 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 gửi đi đâu;
- Công việc in ấn gửi đi khi nào;
- Thứ tự ưu tiên của các tác vụ in.

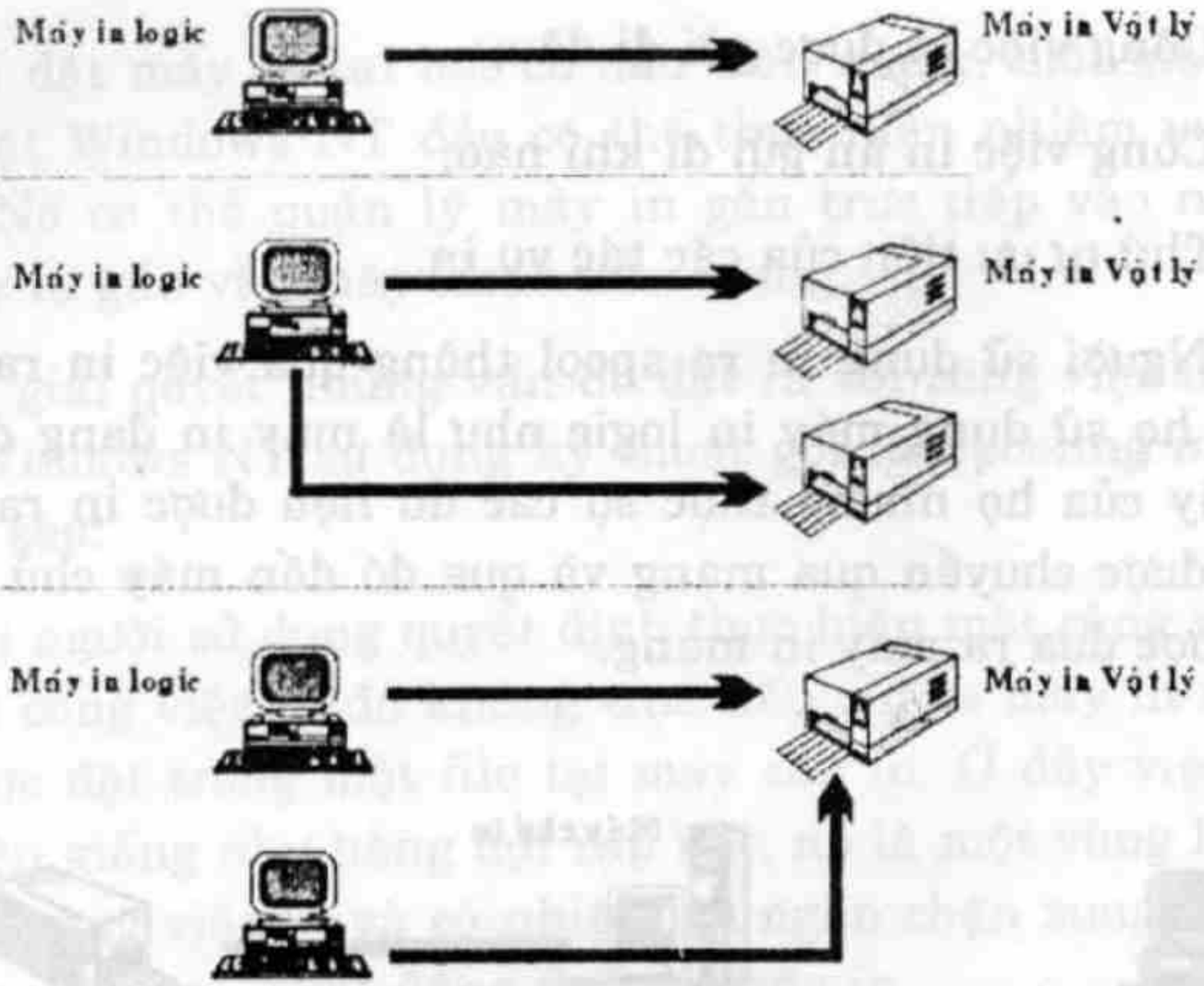
Người sử dụng in ra spool thông qua việc in ra máy in logic, họ sử dụng máy in logic như là máy in đang được gắn là máy của họ nhưng thực sự các dữ liệu được in ra máy in logic được chuyển qua mạng và qua đó đến máy chủ in trước khi được đưa ra máy in mạng.



Hình 14.1: *Máy chủ in và spool*

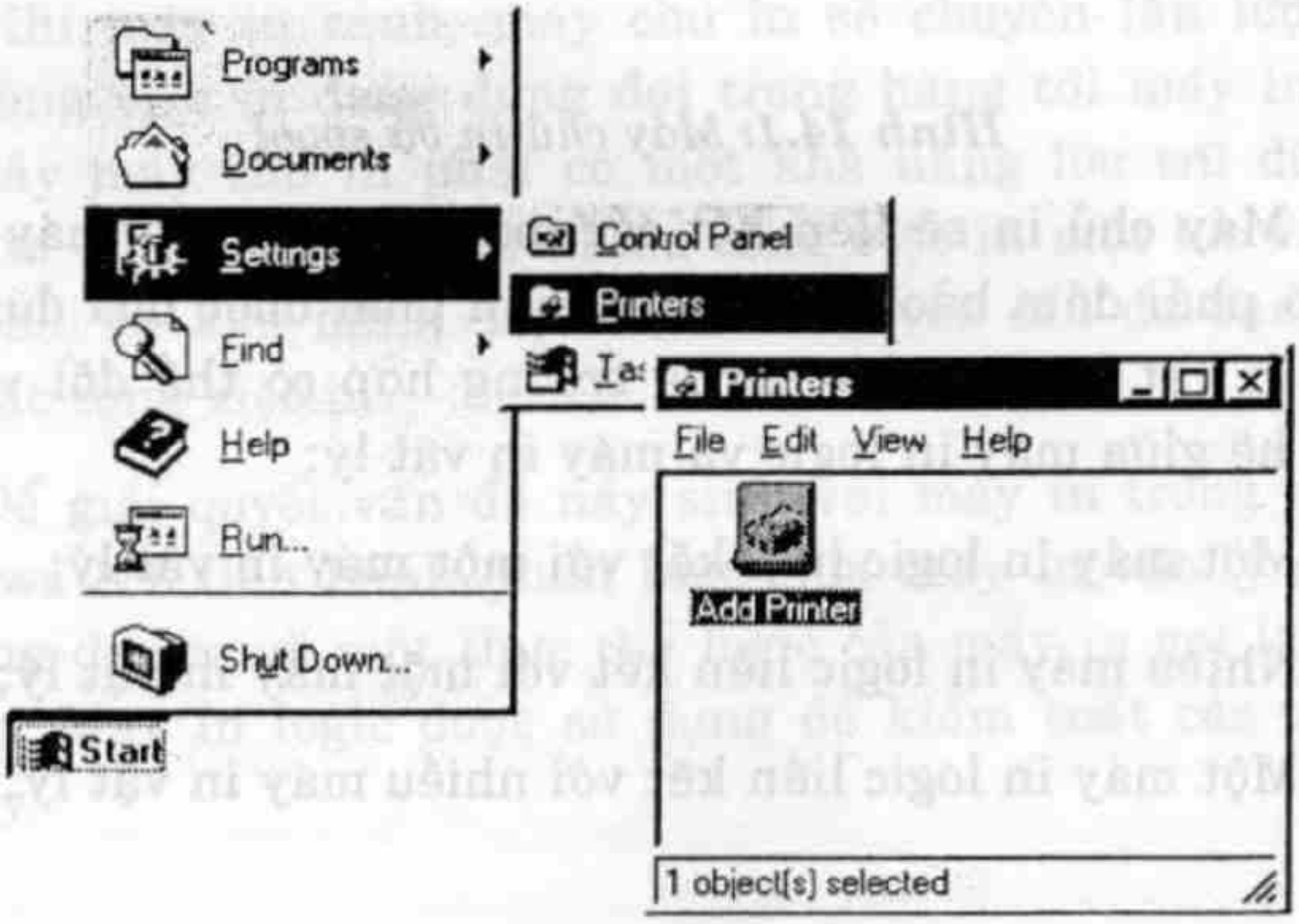
Máy chủ in sẽ liên kết các máy in logic với máy in vật lý, nó phải đảm bảo các công việc in phải được đưa đúng đến máy in vật lý. Tại đây có ba trường hợp có thể đối với mối quan hệ giữa máy in logic và máy in vật lý:

- 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.

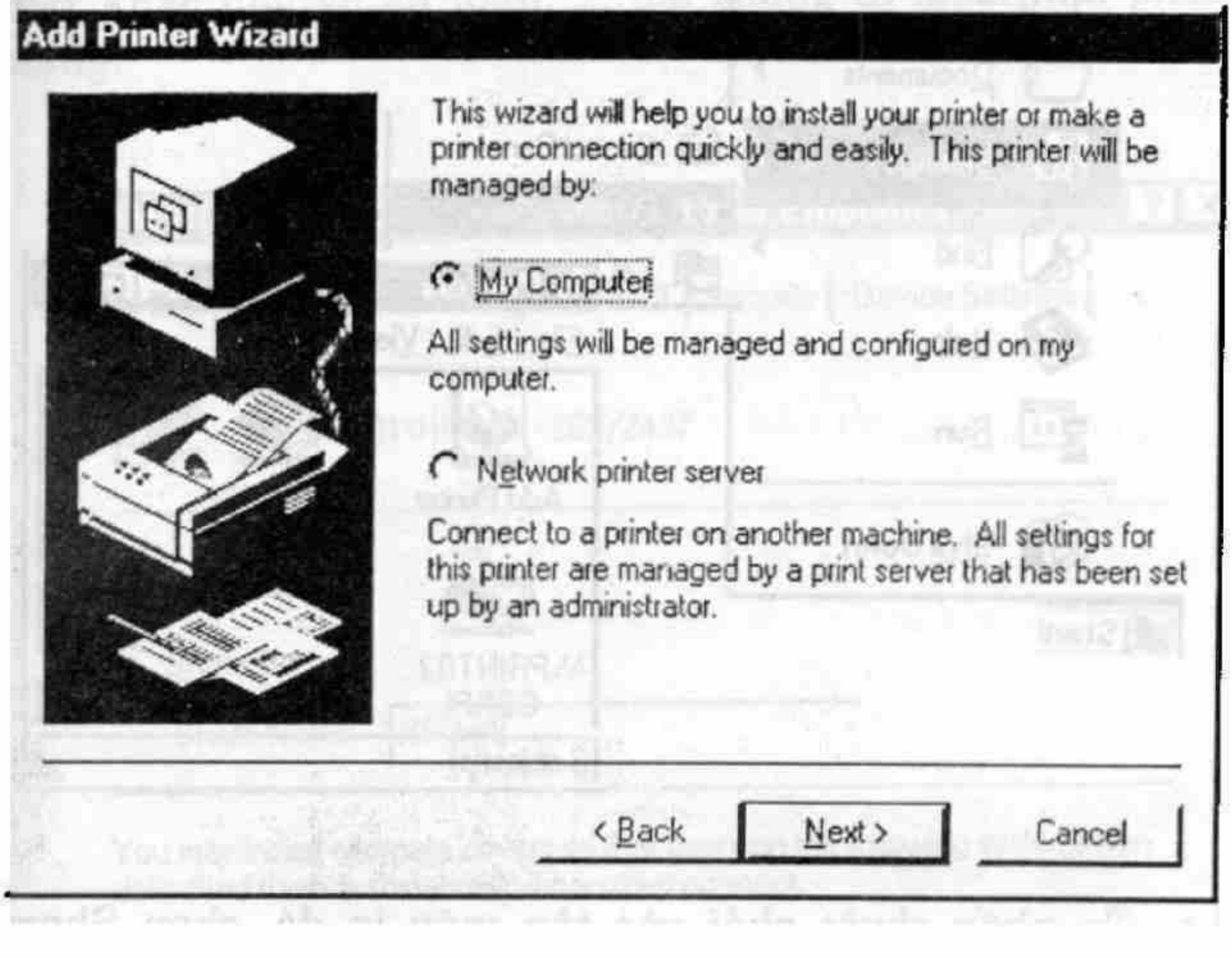


Hình 14.2: *Liên kết giữa máy in logic và máy in vật lý*

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:

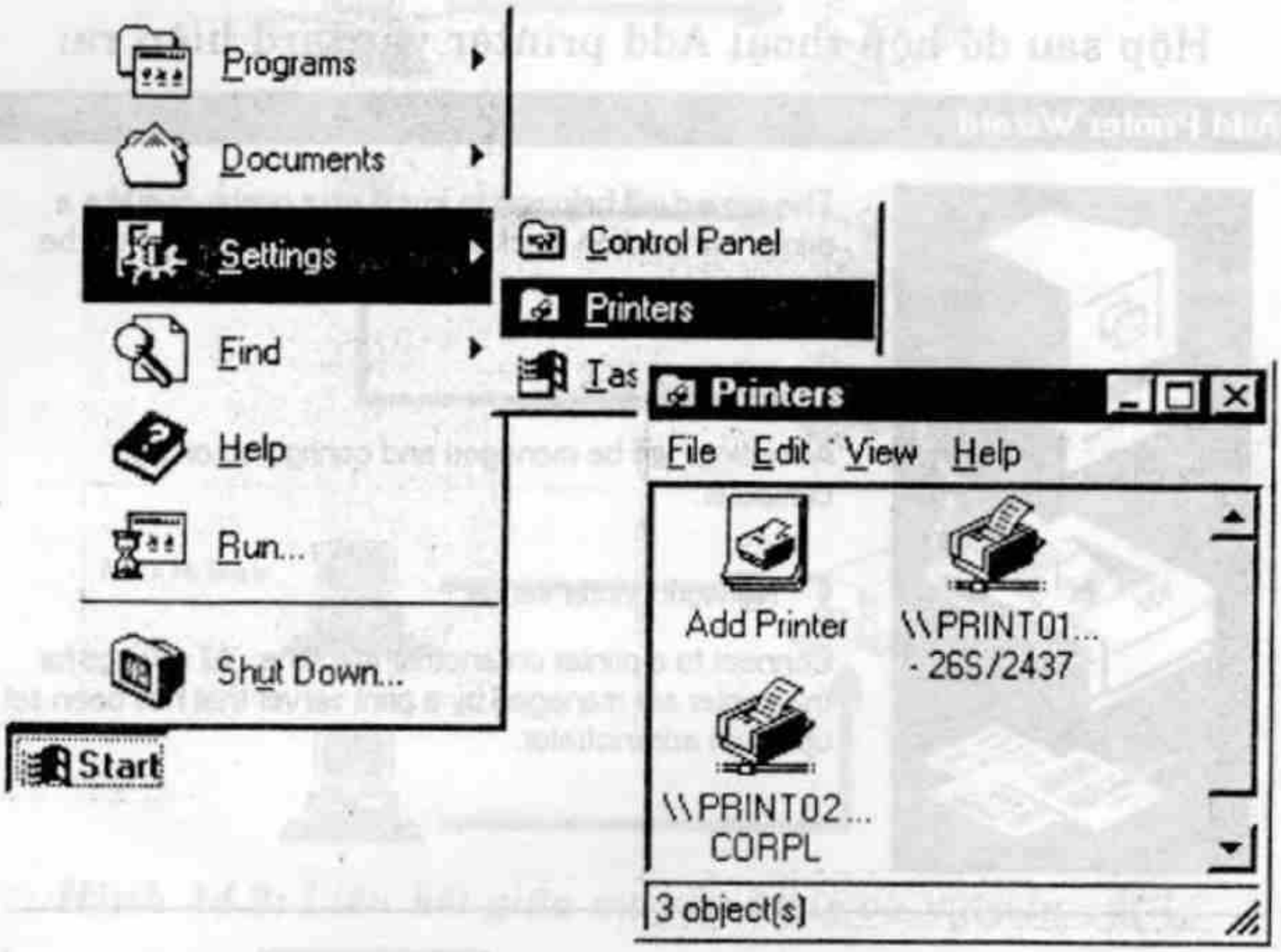


Hộp sau đó hộp thoại Add printer winzard hiện ra:

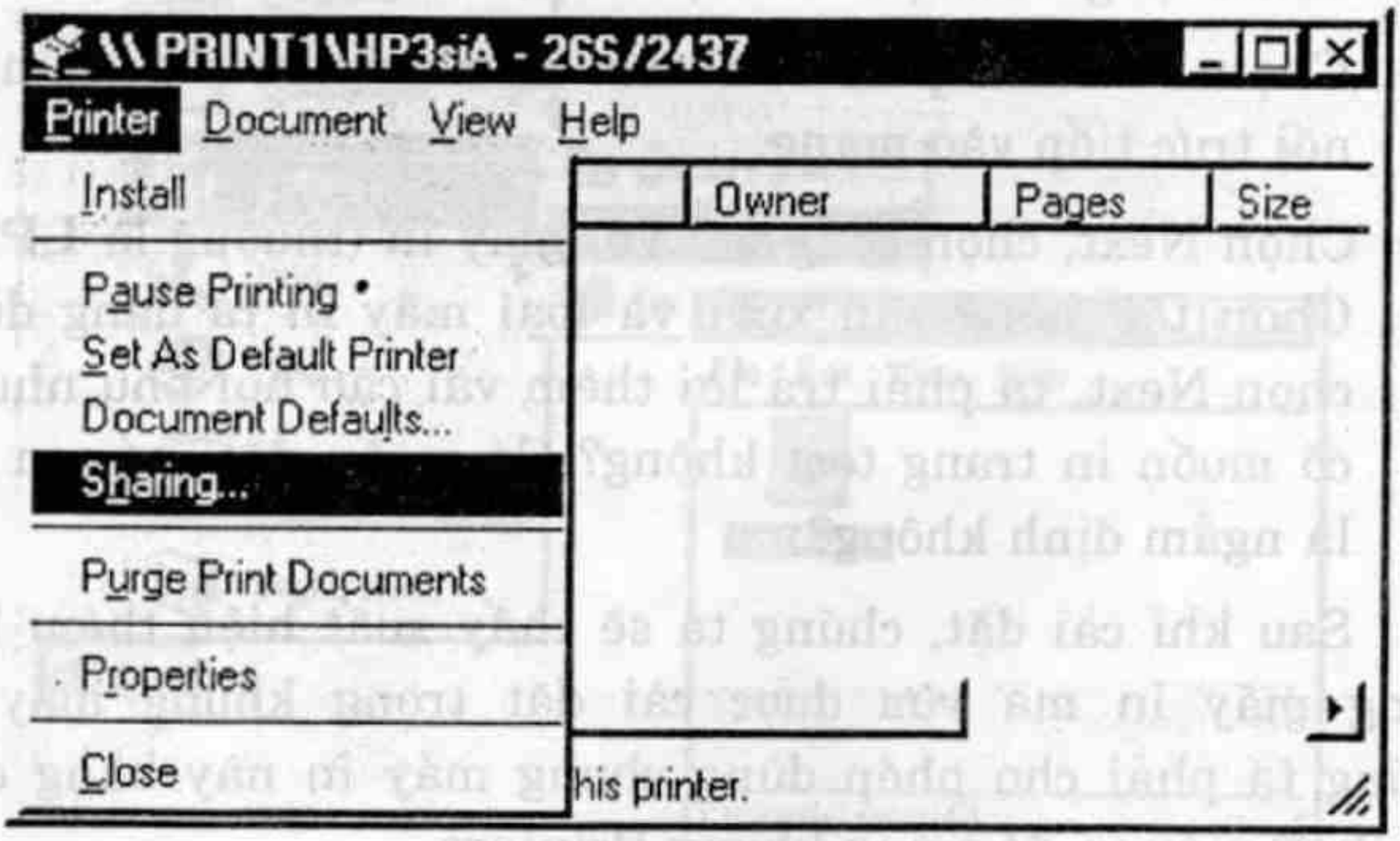


- Chọn My Computer nếu máy in của chúng ta không có card mạng và được nối trực tiếp vào Server .
- Chọn Network printer server nếu máy in của chúng ta nối trực tiếp vào mạng.
- Chọn Next, chọn cổng nối với máy in (thường là **LPT1**). Chọn tên hãng sản xuất và loại máy in ta đang dùng, chọn Next, ta 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?

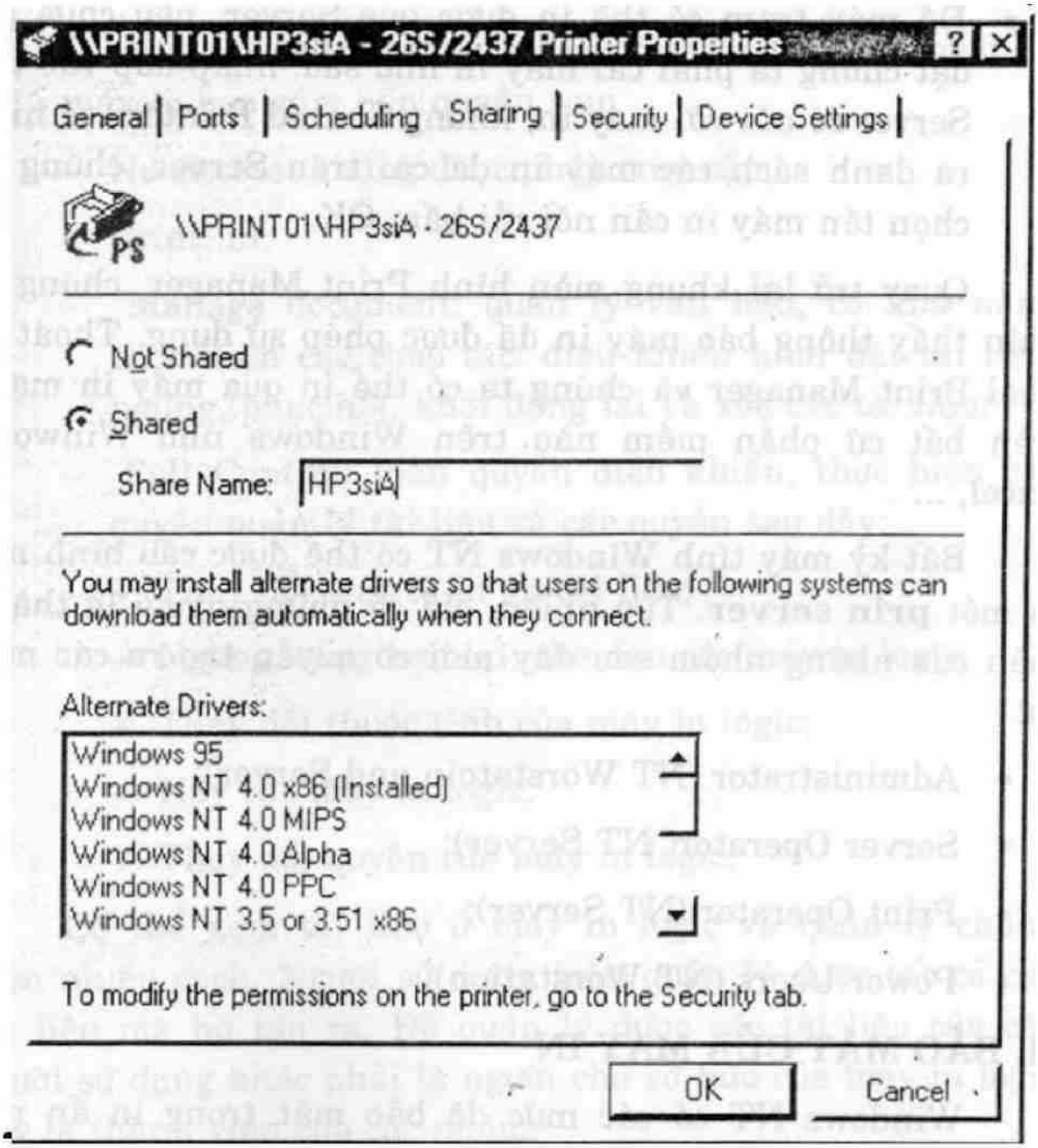
Sau khi cài đặt, chúng ta sẽ thấy xuất hiện thêm biểu tượng máy in mà vừa được cài đặt trong khung máy in. Chúng ta phải cho phép dùng chung máy in này bằng cách lựa chọn máy in đó trong khung Printers.



- Ta nhấp 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 name), 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: nhấp 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 đã được phép sử dụng. Thoát ra khỏi Print Manager và chúng ta có thể in qua máy in mạng trên bất cứ phần mềm nào trên Windows như Winword, Excel, ...

Bất kỳ máy tính Windows NT có thể được cấu hình như là một **prin 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 Worstatoin 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 sở hữu máy in logic đó.

- Quản lý thuộc tính máy in (Permissions): quyền quản lý máy in bao gồm bốn 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:

- Adminitrator;
- Sever 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 phụ 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 mó, 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 (star), 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 phức 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 cả cho 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)

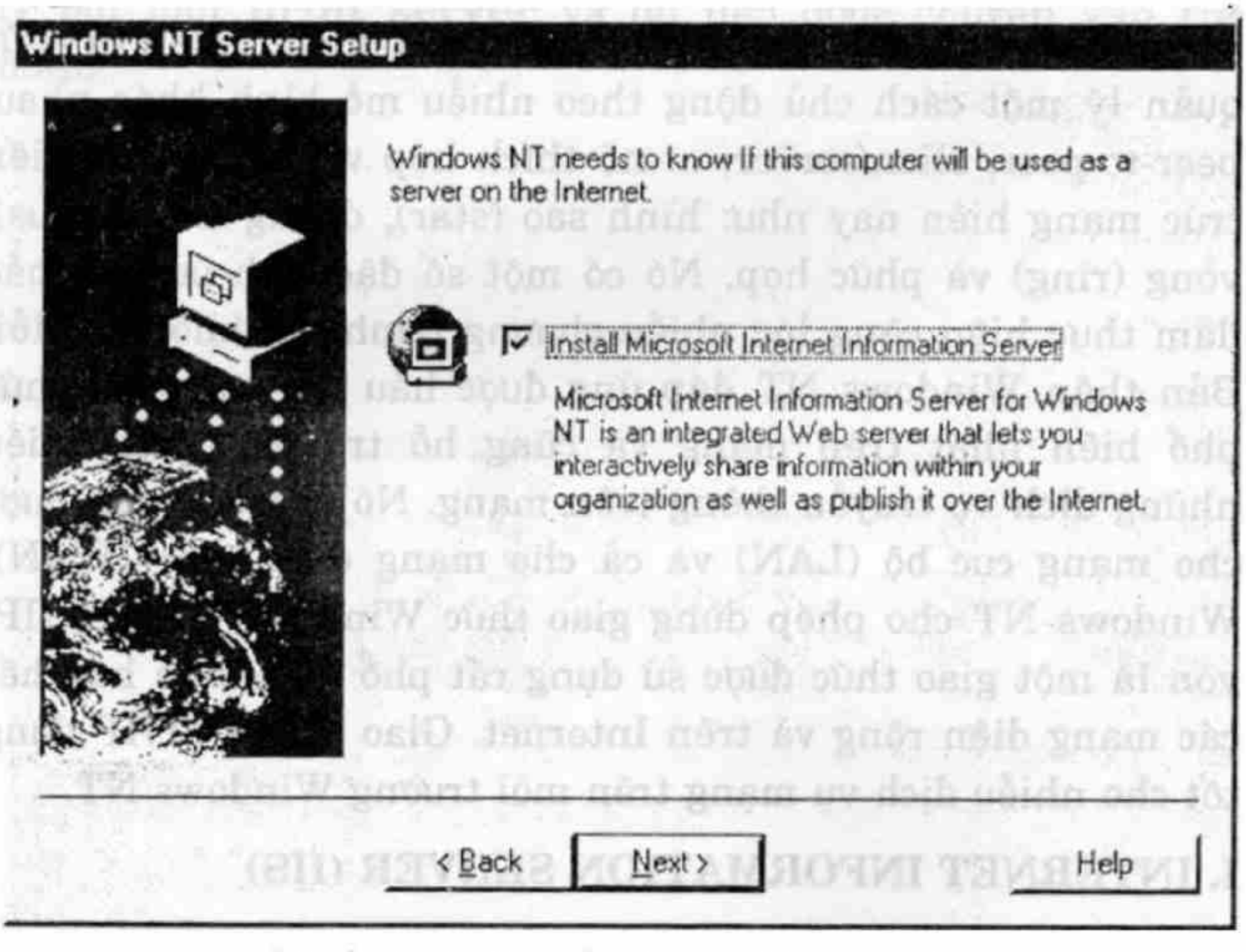
Internet Information Server là một ứng dụng chạy trên Windows NT, tích hợp chặt với Windows NT, khi cài đặt IIS, IIS có đưa thêm vào tiện ích màn hình kiểm soát (Performance monitor) một số mục như thống kê số lượng truy cập, số trang truy cập. Việc kiểm tra người dùng truy cập cũng dựa trên cơ chế quản 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 ba 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 thoại



Hình 15.1: *Màn hình cài đặt của IIS*

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 hai máy và cũng hoạt động theo mô hình Client/Server, khi nhận được yêu cầu từ clien, 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.

II. DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP)

Trong một mạng máy tính, việc cấp các địa chỉ IP tính 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 một địa chỉ IP theo bốn bước sau:

- Gửi thông báo đến tất cả các DHCP server để yêu cầu được cấp địa chỉ;
- Tất cả các DHCP server gửi trả lời địa chỉ sẽ cấp đến cho user đó;
- User chọn 1 địa chỉ trong số các địa chỉ, gửi thông báo đến server có địa chỉ được chọn;
- Server được chọn gửi 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.

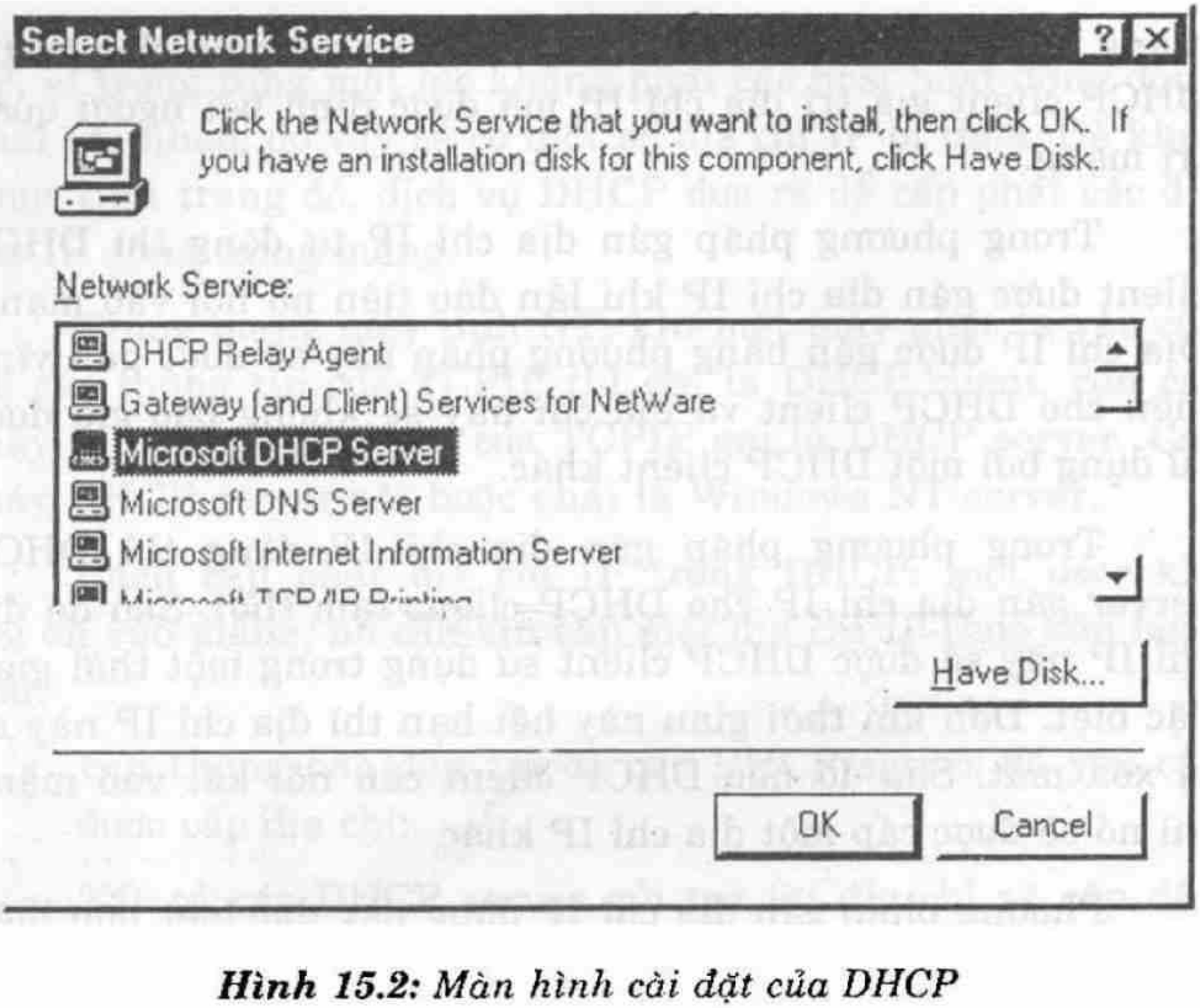
Trong phương pháp gán địa chỉ IP tự động thì DHCP client được gán địa chỉ IP khi lần đầu tiên nó nối vào mạng. Địa chỉ IP được gán bằng phương pháp này sẽ được gán vĩnh viễn cho DHCP client và địa chỉ này sẽ không bao giờ được sử dụng bởi một DHCP client khác.

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 chỉ 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 kết nối 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 thoại Network dialog box:



Hình 15.2: *Màn hình cài đặt của DHCP*

- Chọn tab service và click vào nút Add.
- Ta sẽ thấy một loạt các service của Windows NT server nằm trong hộp 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 Network 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.

DSN là một cơ sở dữ liệu phân tán cung cấp ánh xạ từ tên host đến địa chỉ IP. Khi đưa ra một tên host, DNS server sẽ trả về địa chỉ IP hay một 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:

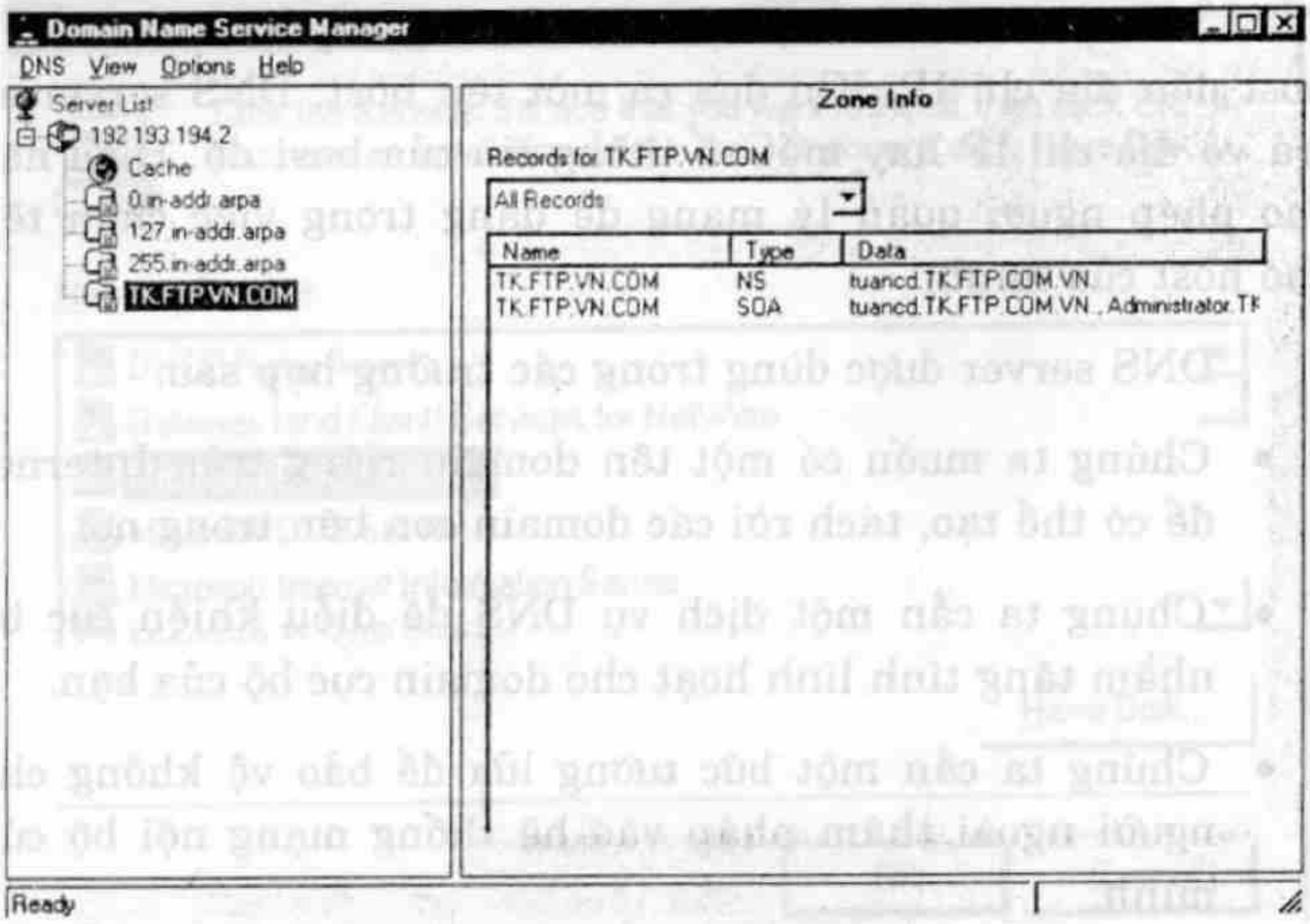
- Chúng ta muốn có một tên domain riêng trên Internet để có thể tạo, tách rời các domain con bên trong nó.
- Chúng ta cần một dịch vụ DNS để điều khiển cục bộ nhằm tăng tính linh hoạt cho domain cục bộ của bạn.
- Chúng ta cần một bức tường lửa để bảo vệ không cho người ngoài thâm nhập vào hệ thống mạng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

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

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

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



***Hình 15.3:** Màn hình DNS Manager*

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

Tên Record	Mô tả
A (Address)	Đường dẫn 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 một tên 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)	Đường dẫn một địa chỉ IP đến tên host trong DNS server zone
SOA (Star of authority)	Hiển thị rằng tên server DNS này thì chứa những thông tin tốt nhất

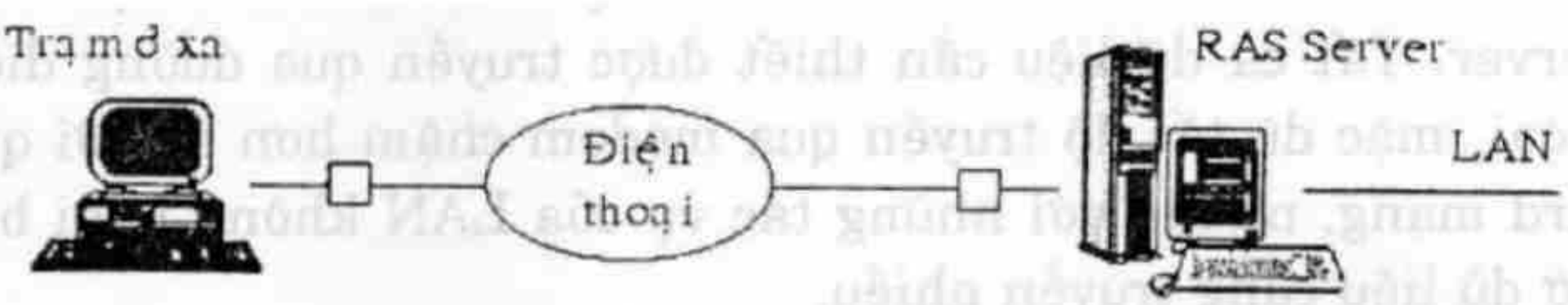
IV. REMOTE ACCESS SERVICE (RAS)

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, ...

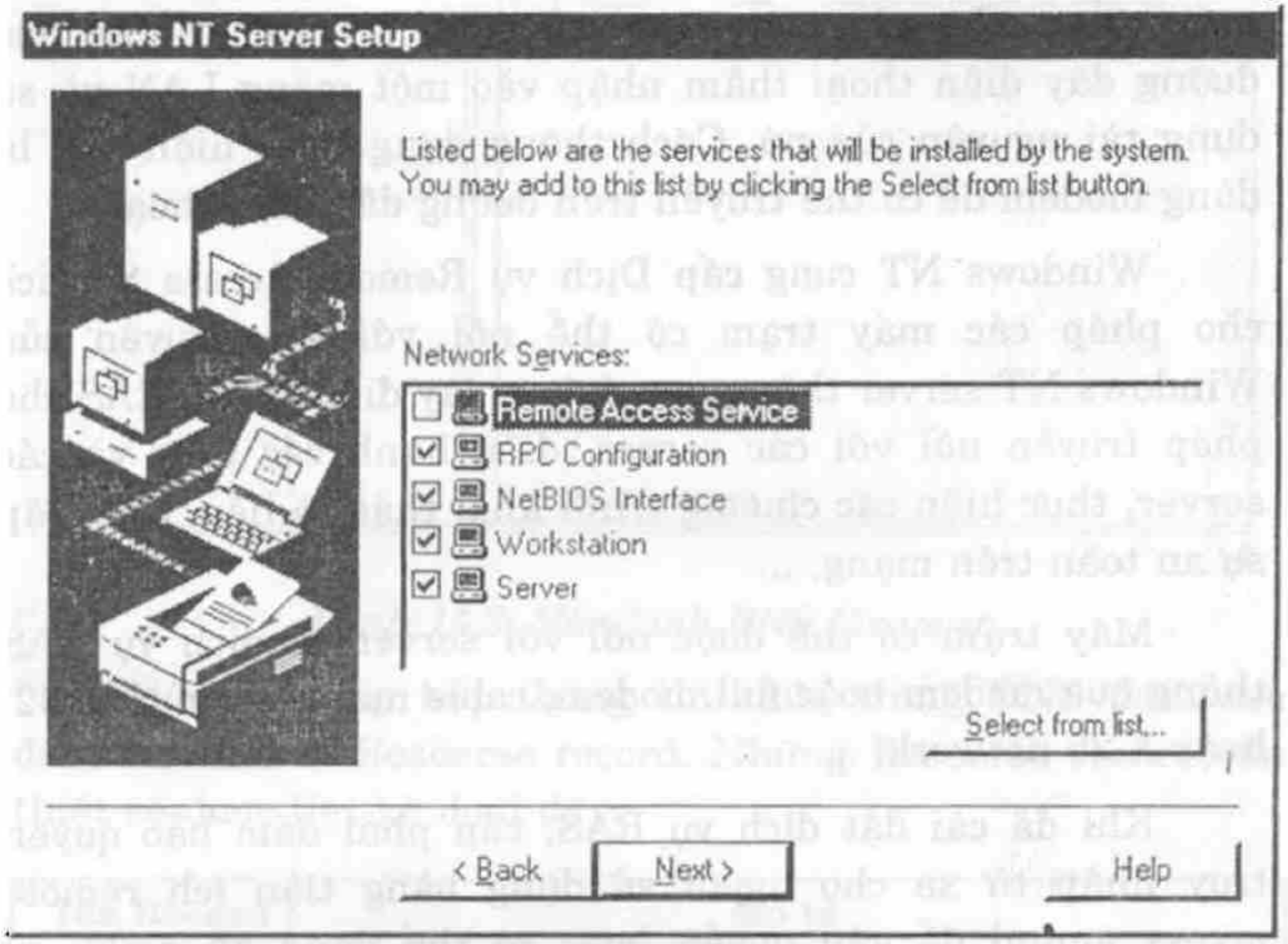
Máy trạm có thể được nối với server có dịch vụ RAS thông qua modem hoặc full modem, cable null modem (RS232) hoặc X.25 network, ...

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



Hình 15.4: *Mô hình truy cập từ xa bằng dịch vụ RAS*

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



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

TÀI LIỆU THAM KHẢO

1. **Matthew Naugle** – *Network Protocol Handbook* – McGraw Hill – 1994.

2. **Drew Heywood** – *Inside Windows NT Server 4.0* – New Riders – 1997.

3. **Andrew S. Tanenbaum** – *Computer Network* – Prentice Hall PTR – 1996.

4. **William Stallings** – *Handbook of computer – communications* (volume 1, 2, 3) – Macmillan Computer Publishing – 1994.

5. **Douglas E. Comer** – *Internetworking With TCP/IP* (volume 1, 2, 3) – Prentice Hall – 1994.

6. **Nguyễn Thúc Hải** – *Mạng máy tính và các hệ thống mở* – Nhà xuất bản Giáo dục – 1997.

MỤC LỤC

GIÁO TRÌNH
MẠNG MÁY TÍNH

Nguyễn Bình Dương, Đàm Quang Hồng Hải

NHÀ XUẤT BẢN
ĐẠI HỌC QUỐC GIA TP HỒ CHÍ MINH
KP 6, P. Linh Trung, Q. Thủ Đức, TPHCM
ĐT: 7242181 + 1421, 1422, 1423, 1425, 1426
Fax: 7242194; Email: vnuhp@vnuhcm.edu.vn

★★★

Chịu trách nhiệm xuất bản
TS. HUỲNH BÁ LÂN
Biên tập
NGUYỄN TIẾN NAM
NGUYỄN HUỲNH
Sửa bản in
TRẦN VĂN THẮNG
Trình bày bìa
XUÂN THẢO
Đơn vị/Người liên kết:
TRƯỜ[illegible]H CNTT

GT. 03. TH(V) **484-2009/CXB/141-45** **TH.GT.409-10(T)**
ĐHQG.HCM-10

In tái bản 500 cuốn khổ 14.5 x 20.5cm. Số đăng ký kế hoạch xuất bản: 484- 2009/CXB/141-45/ĐHQGTPHCM. Quyết định xuất bản số: 307/QĐ-ĐHQGTPHCM cấp ngày 14/06/2010 của NXB ĐHQGTPHCM. In tại Công ty TNHH In và Bao bì Hưng Phú. In xong và nộp lưu chiểu tháng 7 năm 2010

Giá: 28.000đ