

QUẢN TRỊ MẠNG

Mạng máy tính không thể tự hoạt động mà phải có người *quản trị mạng (administrator)*, công việc chính của anh ta là quản lí tài khoản người dùng và các tài nguyên. Chương này trình bày khái quát về những công việc đó.

1. QUẢN LÍ TÀI KHOẢN MẠNG

1.1. Khái niệm tài khoản (Account)

Mỗi người muốn làm việc trên mạng đều cần phải có một *tài khoản người dùng (User Account)*. Tài khoản gồm những thông tin sau:

- Tên người sử dụng (user name). Mỗi người dùng phải có một tên riêng không trùng với những người, nhóm người hay tên những đối tượng khác trên mạng.
- Mật khẩu (password) dùng để chứng thực người sử dụng.
- Các thông số dùng cho việc thiết lập môi trường làm việc của người đó trên mạng. Đó là quyền truy cập hệ thống và sử dụng những tài nguyên trên mạng, các thông tin về tài khoản của người sử dụng đó như tên nhóm làm việc (group), vùng làm việc (domain)... mà tài khoản đó trực thuộc.

Sau đây là một số tài khoản thông dụng mà các hệ điều hành mạng đều có.

- *Tài khoản của Người quản trị mạng*

Người đầu tiên đăng nhập (login) vào mạng thường chính là người đứng ra cài đặt hệ điều hành mạng. Trong quá trình cài đặt, phần mềm cài đặt luôn tự động tạo ra một tài khoản có đầy đủ mọi quyền tối cao trên mạng như:

- Khởi động (Start) và chấm dứt hoạt động của mạng (Shutdown).
- Tạo ra, ban quyền, giám sát những tài khoản người dùng, tài khoản nhóm (Group account).

– Trực tiếp hay gián tiếp quản lý mọi tài nguyên mạng, kiểm soát mọi hoạt động của mạng.

Tài khoản tối cao đó Windows gọi là Administrator. Novell Netware ban đầu gọi là Supervisor, trong các phiên bản từ 4.0 trở lên gọi là Admin.

• *Tài khoản Khách vãng lai (Guest)*

Trình cài đặt có thể tự động tạo ra tài khoản *Guest*, nếu không thì người quản trị cũng nên làm việc đó. *Guest* là một tài khoản dành cho những khách vãng lai, khách đến tham quan công ti trực tiếp hay qua Internet ... Chủ tài khoản này có thể đăng nhập mạng nhưng không có một quyền hạn gì đáng kể, chỉ có thể xem lướt qua những thông tin mà công ti muốn tự giới thiệu về mình.

Kích hoạt, vô hiệu hóa, hủy bỏ tài khoản

Hủy bỏ (delete) tài khoản là cần thiết đối với những người sử dụng bị khai trừ vĩnh viễn khỏi mạng và nếu để tài khoản đó tiếp tục tồn tại có thể gây hậu quả xấu như rò rỉ thông tin, phá hoại dữ liệu...

Đối với những tài khoản không còn hữu ích nữa, nhưng cũng chưa cần phải xóa bỏ hẳn thì Administrator có thể vô hiệu hóa. Một tài khoản bị *vô hiệu hóa (Disable)* thì vẫn tồn tại trong cơ sở dữ liệu tài khoản của hệ thống nhưng không ai có thể sử dụng nó để đăng nhập mạng. Người quản trị mạng nên vô hiệu hóa tài khoản ngay khi đã xác minh được rằng người sử dụng không còn được giao quyền sử dụng nó nữa, tạm thời hay là vĩnh viễn. Các trường hợp thực tế áp dụng biện pháp này là: viên chức đó tạm thời nghỉ việc không rõ lí do, nghỉ ốm, chuyển chuyển vị trí...

1.2. Chiến lược quản trị tài khoản

Mạng có thể có rất nhiều người sử dụng cùng với tài khoản của họ. Sẽ có nhiều trường hợp Người quản trị mạng cần tiến hành một thao tác quản lý đối với một nhóm trong số đó, hay liên tiếp thực hiện nhiều thao tác trên nhiều nhóm khác nhau. Chẳng hạn như gửi giấy mời đến các cán bộ của Phòng Tổ chức, cấp phát thêm tài nguyên cho mọi người thuộc Phòng Kế hoạch và Phòng Tài vụ... Cần phải có biện pháp để tiết kiệm thời gian cho những công việc đó.

Tất cả các hệ điều hành mạng đều giải quyết vấn đề này bằng cách tập hợp các tài khoản riêng lẻ vào một *Tài khoản nhóm (Group Account)*. Nhóm là một tài khoản chứa những tài khoản khác. Lí do thành lập nhóm

là để đơn giản hóa công việc quản trị, nó giúp người quản trị mạng có khả năng xử lý một số lượng lớn tài khoản một cách đơn giản như một tài khoản đơn.

Các tài khoản có vai trò thực tế phù hợp với nhau, chức năng trong cơ quan giống nhau thường được gom vào cùng một nhóm. Chẳng hạn tài khoản của tất cả nhân viên trong một Phòng ban, của các trưởng phòng một công ti... thường được tập hợp trong cùng một nhóm. Nếu giám đốc cần triệu tập cuộc họp các nhân viên phòng Hành chính quản trị, ông ta chỉ cần gửi thông điệp mời họp đến tài khoản nhóm của phòng đó thay vì phải gửi tới từng nhân viên.

Sử dụng tài khoản Nhóm

Quản trị tài khoản thông qua nhóm là biện pháp căn bản, thông thường những người quản trị giàu kinh nghiệm không để tồn tại một tài khoản cá nhân nào cả. Mọi tài khoản nên nằm trong một nhóm hoặc một vài nhóm khác nhau thì mới duy trì được tính đồng bộ trong quản lý. Làm như vậy sẽ cho phép quản lý một cách có tổ chức đối với Khả năng (Permission) và Quyền hạn (Right) của người dùng.

Khả năng (Permission) của một tài khoản người dùng là giới hạn những tài nguyên mạng như tệp dữ liệu, máy in mạng... mà người đó được phép sử dụng.

Quyền hạn (Right) của một tài khoản là mức độ cho phép người đó thực hiện một thao tác, một công việc nào đó. Chẳng hạn quyền của các trưởng nhóm cho phép anh ta tạo mới, hủy bỏ... đối với các tài khoản trong nhóm của anh ta, hoặc một ví dụ khác như quyền backup dữ liệu, quyền thay đổi giờ hệ thống...

Các loại nhóm

Mỗi hệ điều hành mạng phân loại và gọi tên nhóm theo cách khác nhau. Trong chương cuối chúng ta sẽ xem xét chi tiết các nhóm của Windows 2000 Server. Nói chung thường có những loại nhóm với chức năng như mô tả dưới đây, còn tên gọi và chi tiết cụ thể có thể khác đôi chút.

- *Nhóm cục bộ (Local group)*. Dạng nhóm này được sử dụng trong cơ sở dữ liệu tài khoản của từng máy tính cục bộ. Local group bao gồm các tài khoản người dùng cá thể với Right và Permission chỉ áp dụng trên máy tính cục bộ và những tài khoản nhóm muốn truy xuất đến dữ liệu và tài nguyên trên máy đó.

• *Nhóm toàn cục (Global group)*. Dạng này được sử dụng trong phạm vi toàn vùng. Nhóm toàn cục được thiết lập trên máy server điều khiển vùng.

• *Nhóm cài sẵn (Built-in group)*. Chứa đựng hầu hết những Right và Permission phục vụ cho việc quản trị mạng. Người quản trị mạng thường không thể tự mình làm hết mọi việc mà phải có những quản trị viên lo phụ trách từng mảng công việc. Chẳng hạn như các quản trị viên lo backup dữ liệu sẽ được kết nạp vào nhóm *Backup Operator*, những người chuyên theo dõi tình trạng hoạt động của server thì nằm trong nhóm *Server Operator*... Những nhóm đó phải có Right và Permission thích hợp đảm bảo cho họ có thể thực hiện được nhiệm vụ của mình, và thường được hệ điều hành mạng tính toán từ trước một cách tối ưu, sau đó được tự động tạo ra trong quá trình cài đặt. Người quản trị chỉ việc đặt tài khoản của quản trị viên vào nhóm *built-in* tương ứng với công việc của anh ta là quản trị viên đó có mọi quyền đủ cho công việc của anh ta.

2. PHÒNG CHỐNG MẤT DỮ LIỆU

2.1. Những nguy cơ đe dọa dữ liệu

Bảo vệ dữ liệu luôn trong tình trạng tốt là điều sống còn của người quản trị mạng. Có rất nhiều nguy cơ luôn đe dọa an toàn dữ liệu trên mạng. Ở đây chúng ta không bàn tới những hiểm họa bị gây ra một cách có chủ ý như virus, xâm nhập trái phép... mà chỉ xem xét việc phòng chống những thiệt hại ngẫu nhiên mang tính khách quan như sự cố mất điện, bề mặt đĩa cứng bị hỏng vài sector hay thậm chí động cơ của một đĩa cứng đột nhiên ngừng quay.

Đối với loại nguy cơ kể trên, các chiến lược chính để bảo vệ dữ liệu bao gồm:

- Các hệ thống dung lỗi
- Nguồn cấp điện liên tục (UPS)
- Lưu trữ dự phòng.

UPS (*Uninterruptible Power Supply* - nguồn cấp điện liên tục) là một loại ắc quy đặc biệt (đôi khi cũng có thể là một máy phát điện) nhằm cung cấp điện cho hệ thống trong trường hợp điện lưới bị cắt đột ngột. Khi nguồn điện bị mất, UPS lập tức hoạt động không để mạng bị cắt điện dẫn

tới mất dữ liệu và gián đoạn hoạt động của mạng. UPS có thể cung cấp điện trong một khoảng thời gian từ 30 phút cho tới vài chục giờ (thậm chí lâu hơn nhiều nếu sử dụng máy phát điện). UPS có thể được điều khiển bằng phần mềm đi kèm để gửi những thông báo về sự cố mất điện, thời hạn mà UPS còn duy trì được nguồn điện... đến người quản trị mạng và những người dùng. Những thông tin này thường được gửi qua cổng COM của UPS.

Một hệ thống UPS hiệu quả có thể:

- Ngăn không cho quá nhiều người truy nhập máy phục vụ.
- Gửi thông báo lỗi đến Người quản trị mạng thông qua server khi có sự cố về điện.

Sau đây chúng ta sẽ xem xét hai phương thức còn lại, đó là các hệ thống dung lỗi và lưu trữ dự phòng.

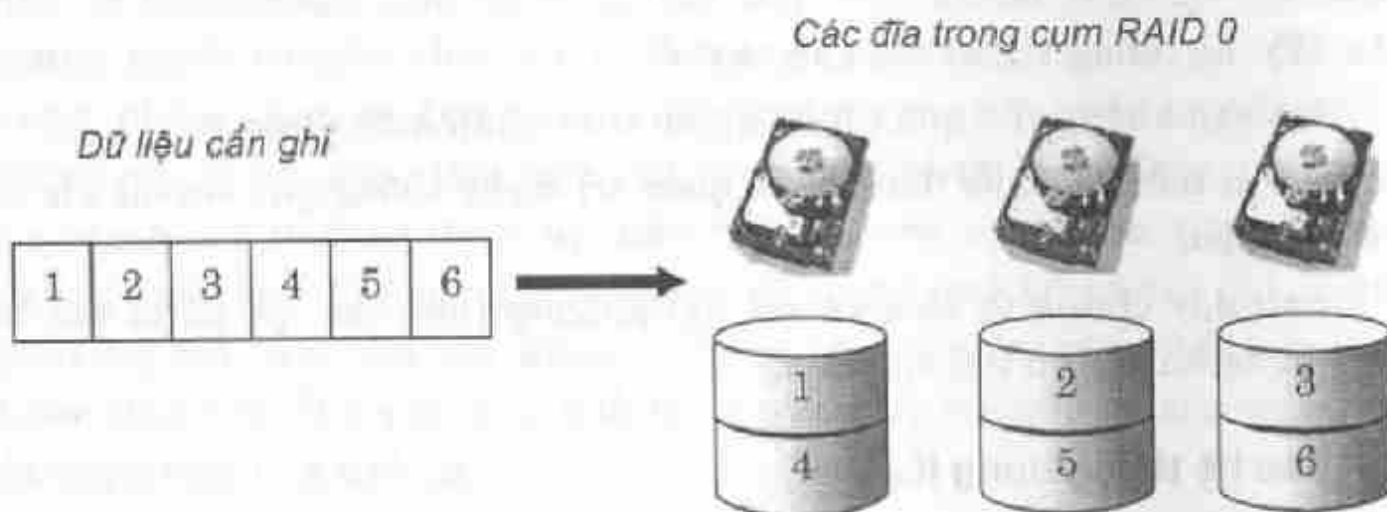
2.2. Các hệ thống dung lỗi

Các hệ thống dung lỗi thường được gọi là RAID - *Redundant Arrays of Inexpensive Disks: cụm đĩa rẻ tiền dự phòng*. Tên gọi này có lịch sử từ khi công nghệ chế tạo đĩa cứng còn sơ khai, giá thành các đĩa cứng khi ấy khá cao mà dung lượng lại nhỏ. Ý tưởng RAID khi đó là thay vì dùng chỉ một đĩa cứng chất lượng rất cao thì người ta mua nhiều đĩa cứng loại rẻ hơn và liên kết chúng trong một hệ thống RAID, cái nọ dự bị cho cái kia nhằm làm giảm đến mức tối thiểu thiệt hại khi có sự cố xảy ra. Ngày nay khi công nghệ chế tạo đã phát triển cao, giá thành và dung lượng đĩa không còn là vấn đề nữa thì thuật ngữ RAID còn được hiểu là *Redundant Arrays of Independent Disks: cụm đĩa dự phòng độc lập*. Có nhiều phương án thực hiện RAID khác nhau nhằm mang lại khả năng chống chịu lỗi, tự phục hồi và tăng tốc độ đọc ghi dữ liệu. Khả năng chống chịu lỗi (fault tolerance - dung lỗi) có thể được hiểu là nếu xảy ra sự cố không vượt quá một mức độ cho phép với các thiết bị lưu trữ như đĩa cứng thì hệ thống vẫn tiếp tục làm việc được mà không cần phải tạm dừng để phục hồi. Việc khôi phục lại dữ liệu được tiến hành sau đó, trong khi hệ thống vẫn tiếp tục hoạt động.

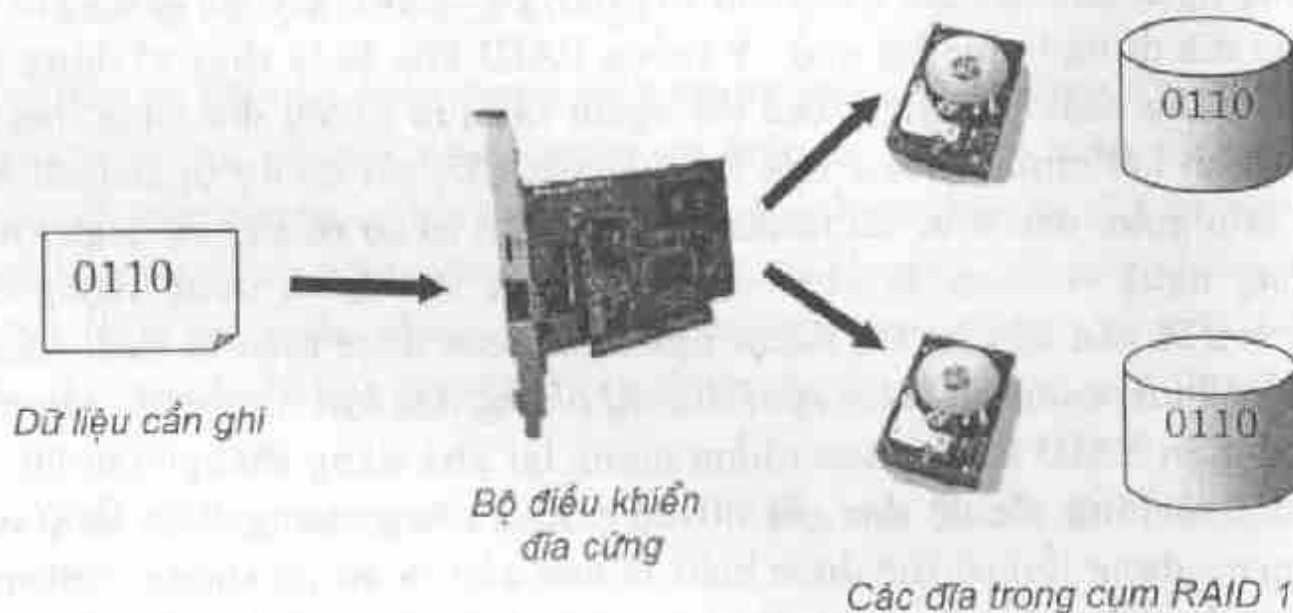
2.2.1. RAID 0 (Disk striping - cắt lát dữ liệu)

Khi cần ghi cơ chế này chia dữ liệu thành từng khối (gọi là Stripe

block) và rải đều chúng lên các đĩa trong cụm. Điều này làm cho tốc độ đọc dữ liệu tăng lên nhiều và cho phép tạo ra những volume có kích thước lớn từ nhiều đĩa vật lí. Tuy nhiên nếu sự cố xảy ra dù chỉ với một trong các đĩa thì toàn bộ nhóm dữ liệu liên quan sẽ bị mất. Vì vậy cơ chế RAID 0 không có khả năng dung lỗi và người ta thường phải áp dụng nó phối hợp với các phương án RAID khác.



Hình 5.1. Mô hình RAID 0



Hình 5.2. Mô hình RAID 1

2.2.2. RAID 1 (Disk Mirroring - soi gương đĩa)

Theo chiến lược này, cùng một dữ liệu sẽ được ghi thành hai bản sao giống nhau đặt trên hai đĩa vật lí khác nhau. Khi xóa cũng xóa đồng thời

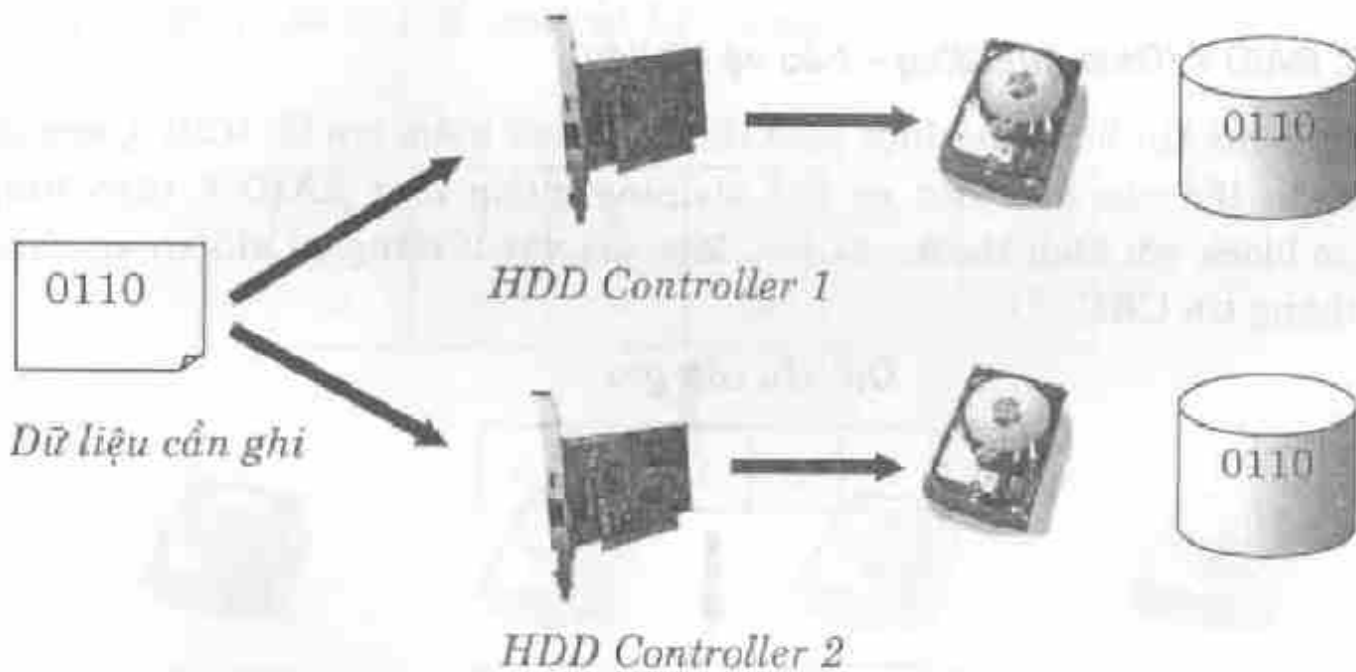
trên cả hai đĩa. Để thấy cơ chế RAID 1 đòi hỏi phải có một số chẵn đĩa cứng để phân thành hai cụm, một cụm chính và một cụm dự phòng. Khi có sự cố xảy ra với cụm đĩa chính, cụm dự phòng sẽ được sử dụng để lấy thông tin ra và cập nhật lại những lỗi tại cụm đĩa kia.

Khi đọc, dữ liệu có thể được đọc đồng thời từ cả hai đĩa để tăng tốc độ đọc nhưng khi ghi dữ liệu vào thì phải ghi đồng thời trên cả hai cụm đĩa nên tốc độ không tăng.

Trong thực tế người ta áp dụng RAID 1 theo nhiều cách khác nhau

- **Hardware Mirroring:** dữ liệu được phân tán trên hai cụm đĩa vật lý với số lượng và dung lượng tương đương nhau.

- **Software Mirroring:** thay vì phân tán bản sao dữ liệu trên cụm đĩa vật lý thứ hai, phương án này tạo ra hai vùng tương đương trên cùng một đĩa vật lý. Rõ ràng phương pháp này kém hiệu quả hơn Hardware Mirroring về độ an toàn, tốc độ đọc dữ liệu ra và nhiều điểm khác.



Duplexing: Hai cụm đĩa được điều khiển bởi hai Controller riêng biệt

Hình 5.3. Mô hình RAID 1 với Duplexing

Disk Duplexing: Ta để ý rằng trong kỹ thuật Hardware Mirroring, cả hai cụm đĩa vật lý đều hoạt động dưới sự điều khiển của một Disk Controller (bộ điều khiển đĩa) chung, do đó nếu sự cố xảy ra không phải với từng đĩa mà với chính Disk Controller thì Hardware Mirroring cũng đành bó tay. Tuy khả năng rất hiếm khi xảy ra nhưng người ta cũng đã

tính đến việc phòng chống nó bằng cách sử dụng hai Disk Controller phân biệt để điều khiển hai cụm đĩa.

2.2.3. RAID 2

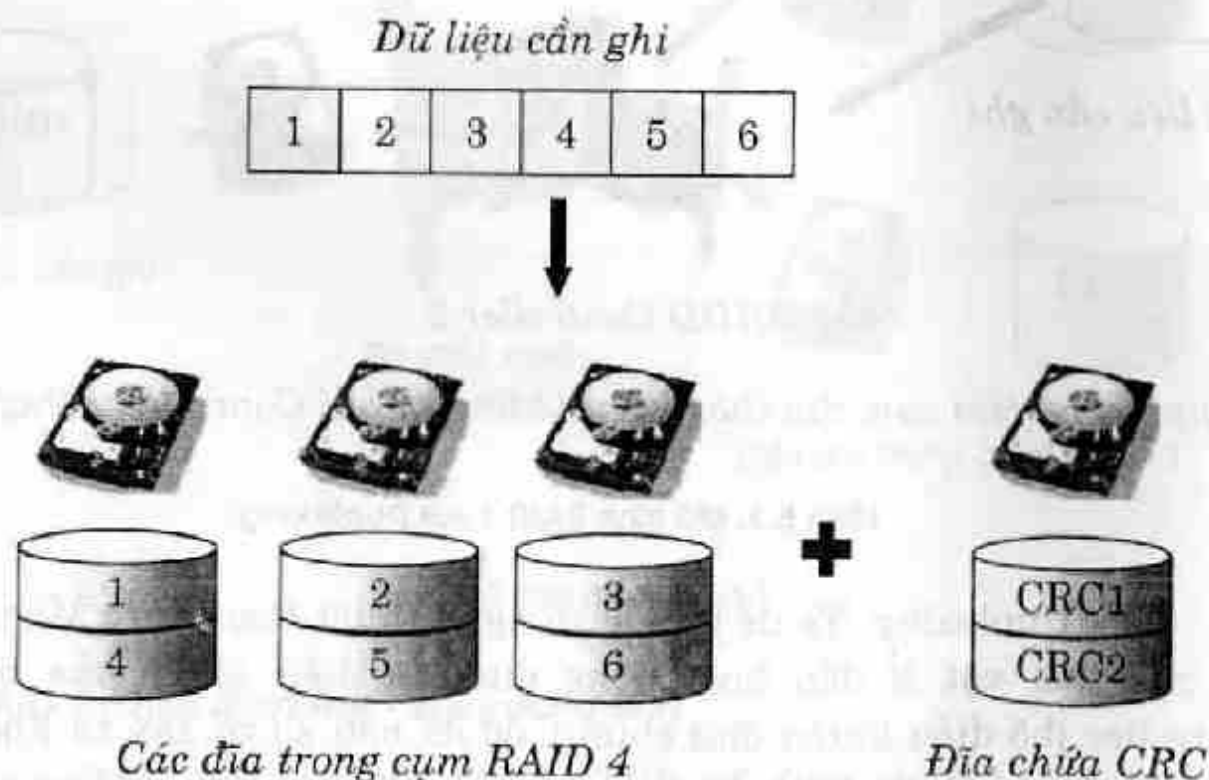
Ít phổ biến hơn các loại kể trên, RAID 2 chủ yếu được áp dụng cho máy tính lớn và siêu máy tính. RAID 2 cho phép hiệu chỉnh dữ liệu ngay trong khi đang hoạt động, thích nghi với với những đòi hỏi cao về kiểm tra lỗi và hiệu chỉnh. Khi một khối dữ liệu được ghi, nó bị tách ra và rải đều theo kiểu Striping trên tất cả các đĩa vật lí trong cụm.

2.2.4. RAID 3

Tư tưởng chính của RAID 3 là truyền song song có mã sửa lỗi ECC (Error Correcting Code). Cơ chế kiểm tra Chẵn lẻ được áp dụng trong RAID 3 với từng nhóm bit. Lượng không gian đĩa hữu ích chiếm khoảng 85% tổng dung lượng đĩa.

2.2.5. RAID 4 (Data guarding – bảo vệ dữ liệu)

Thông tin ban đầu được kèm thêm các mã kiểm tra lỗi (CRC), sau đó được ghi lên các đĩa theo cơ chế striping giống như RAID 0 theo từng Stripe block với kích thước rất lớn. Một đĩa vật lí riêng có nhiệm vụ chứa các thông tin CRC.

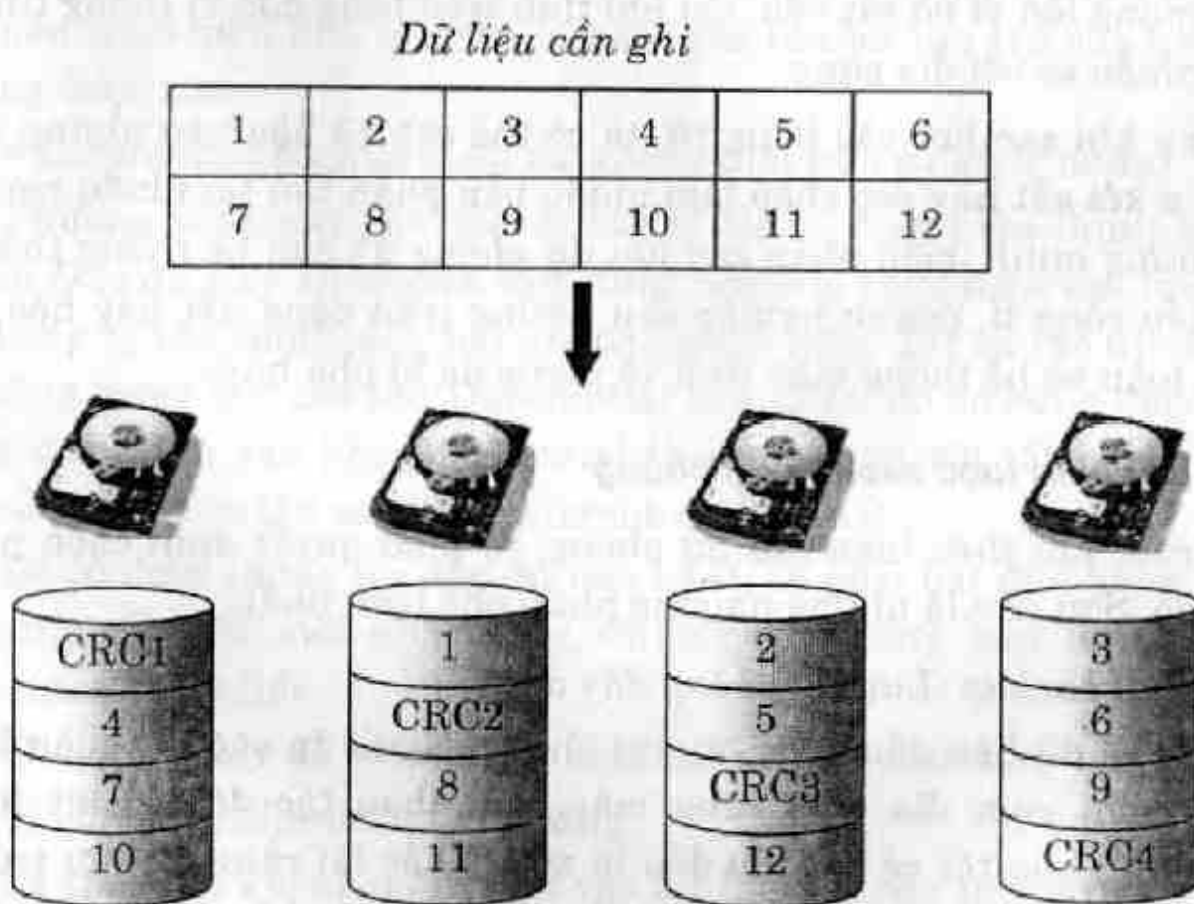


Hình 5.4. Sơ đồ RAID 4

Khả năng chống chịu lỗi của RAID 4 rất cao. Ngay cả khi một đĩa trong cụm đĩa vật lí bị hỏng, dữ liệu vẫn có thể được khôi phục từ những đĩa còn lại và hệ thống vẫn không phải dừng hoạt động, do vậy cơ chế này còn được gọi là *N+1 data guarding*. Nhược điểm của RAID 4 cũng giống như RAID 1, đó là khi Disk controller bị sự cố thì toàn bộ hệ thống phải dừng. Ngoài ra còn một điểm yếu nữa là, đĩa chứa CRC phải hoạt động với cường độ cao nên dễ trở thành một nút cổ chai (*bottle-neck*) làm giảm hiệu suất chung của mạng.

2.2.6. RAID 5 (Distributed Data guarding – phân phối việc bảo vệ dữ liệu)

Chiến lược RAID 5 tương tự như RAID 4, chỉ cải tiến một điểm. Đó là thông tin CRC không nằm tập trung tại một đĩa vật lí nữa mà cũng được rải đều lên các đĩa trong cụm giống như dữ liệu thông thường. Làm như vậy khiến cho vai trò của các đĩa trong cụm trở nên bình đẳng như nhau, không còn đĩa nào phải gánh phần việc nặng hơn các đĩa khác do đó loại bỏ nguy cơ trở thành nút cổ chai của hệ thống.



Hình 5.5. Sơ đồ RAID 5

2.3. Lưu trữ dự phòng

Các cơ chế RAID đã cung cấp cho chúng ta khả năng phòng chống và thậm chí sửa chữa "nóng" đối với trường hợp có trục trặc xảy ra với dữ liệu, khi đó hệ thống mạng không phải dừng hoạt động mà vẫn phát hiện và hiệu chỉnh được lỗi. Nhưng có những nguy cơ mà các hệ thống dung lỗi dù tinh xảo đến đâu cũng không phòng chống nổi, đó là động đất, hỏa hoạn hay sự cố chập điện gây cháy nổ máy móc.

Hãy tưởng tượng nếu một công ti bố trí hệ thống văn phòng trong một tòa nhà cao tầng, nếu xảy ra hỏa hoạn toàn bộ các máy móc trong đó bị phá hủy hay hư hỏng thì các biện pháp RAID cũng đành bó tay vì toàn bộ các ổ cứng cùng với máy server, máy trạm... đều bị thiêu trụi, còn nếu xảy ra động đất thì tòa nhà đó thậm chí có thể bị đổ sập hoàn toàn.

Biện pháp duy nhất đối với những loại nguy cơ kể trên là *Sao lưu dự phòng*. Các cơ chế sao lưu thường chọn băng từ (tape) làm nơi chứa dữ liệu vì tính bền vững và giá thành của nó. Băng từ là giải pháp rất tốt cho những mạng lớn vì nó rất bền, chi phí tính trên từng đơn vị thông tin (MB) rẻ hơn nhiều so với đĩa cứng.

Sau khi sao lưu vào băng từ, ta có thể cất dữ liệu vào những nơi an toàn như két sắt hay sao chép làm nhiều bản phân tán tại nhiều nơi. Thực tế đã chứng minh, biện pháp sao lưu dự phòng đã cứu hệ thống thông tin của nhiều công ti, doanh nghiệp sau những trận động đất hay hỏa hoạn, khi mà toàn bộ hệ thống máy tính và mạng đã bị phá hủy.

2.3.1. Các chiến lược sao lưu dự phòng

Trước khi thực hiện lưu dự phòng, ta phải quyết định chọn phương pháp nào. Sau đây là những phương pháp phổ biến nhất:

- *Full backup (Lưu dự phòng đầy đủ)*

Tất cả dữ liệu đều được lưu dự phòng. Người ta sao lưu toàn bộ một đĩa hay một cụm đĩa trên từng máy, sau thao tác đó các bit lưu trữ (archive bit) của tất cả các tệp đều bị xóa. Nhắc lại rằng bit lưu trữ - còn gọi là thuộc tính lưu trữ - của một file có tác dụng thông báo rằng file đó đã được sao lưu hay chưa. Nếu nó được cập nhật hay sửa đổi, bit này sẽ tự động bật lên để nhắc nhở rằng file đó cần phải được sao lưu, còn sau khi sao lưu chương trình sẽ tự động tắt các bit này đi.

Chiến lược sao lưu *Đầy đủ* là phương pháp lưu dự phòng toàn diện và chắc chắn nhất, tuy nhiên do dung lượng thông tin nhiều nên chi phí cho thiết bị lưu trữ và thời gian cũng lớn nhất. Người ta luôn tiến hành sao lưu *Đầy đủ* ở lần đầu tiên, sau đó mới phối hợp với các phương pháp khác.

- *Incremental backup (Lưu dự phòng tăng dần)*

Phương pháp này được sử dụng để lưu dự phòng tất cả các file đã được cập nhật kể từ lần sao lưu *Đầy đủ* hay *Tăng dần* cuối cùng trước đó, còn những file không bị thay đổi gì thì bỏ qua.

Thông tin đầy đủ mới nhất = Bản sao đầy đủ ban đầu + P1 + P2 + + Pi
trong đó P_i là bản sao tăng dần thứ i

Phương pháp này cung cấp lịch sử tuần tự của các file trong quá trình chúng được cập nhật. Do đó muốn phục hồi lại cần có bản lưu dự phòng đầy đủ ban đầu và các bản lưu dự phòng tăng dần sau đó. Chỉ cần dữ liệu của một lần sao lưu, tức một P_i , bị hỏng thì toàn bộ dữ liệu coi như mất giá trị.

Vì chỉ sao lưu những file có thay đổi nên chiến lược lưu dự phòng tăng dần thực hiện khá nhanh, sau khi sao lưu bit lưu trữ của những file đó cũng được xóa.

- *Differential backup (Lưu dự phòng dựa trên sự khác nhau)*

Phương pháp này sao lưu tất cả các file đã được hiệu chỉnh kể từ lần sao lưu *Đầy đủ* hay *Tăng dần* sau cùng. Sau khi thực hiện sao lưu bit lưu trữ không bị xóa như trong hai phương pháp trên. Tất cả các file được lưu dự phòng trong lần sao lưu Differential thứ nhất, do đó cũng được lưu dự phòng trong lần sao lưu Differential thứ hai cùng với tất cả các file đã được sửa đổi kể từ lần sao lưu Differential thứ nhất.

Để có được thông tin đầy đủ mới nhất, ta phải bắt đầu bằng bản lưu dự phòng đầy đủ mới nhất cộng với các file trong bản lưu dự phòng Differential mới nhất.

Thông tin đầy đủ mới nhất = Bản sao đầy đủ sau cùng + D

với D là bản sao Differential sau cùng.

Ta thấy, do không đánh dấu vào bit lưu trữ nên lượng thông tin cần lưu theo phương pháp Differential cứ tăng dần sau mỗi ngày, bất kể là có cập nhật hay không. Ưu điểm của chiến lược này là khi cần khôi phục thông tin ta chỉ phải lấy từ cuộn băng *Đầy đủ* cuối cùng và cuộn Differential gần nhất.

• *Custom backup (Lưu dự phòng theo ý muốn)*

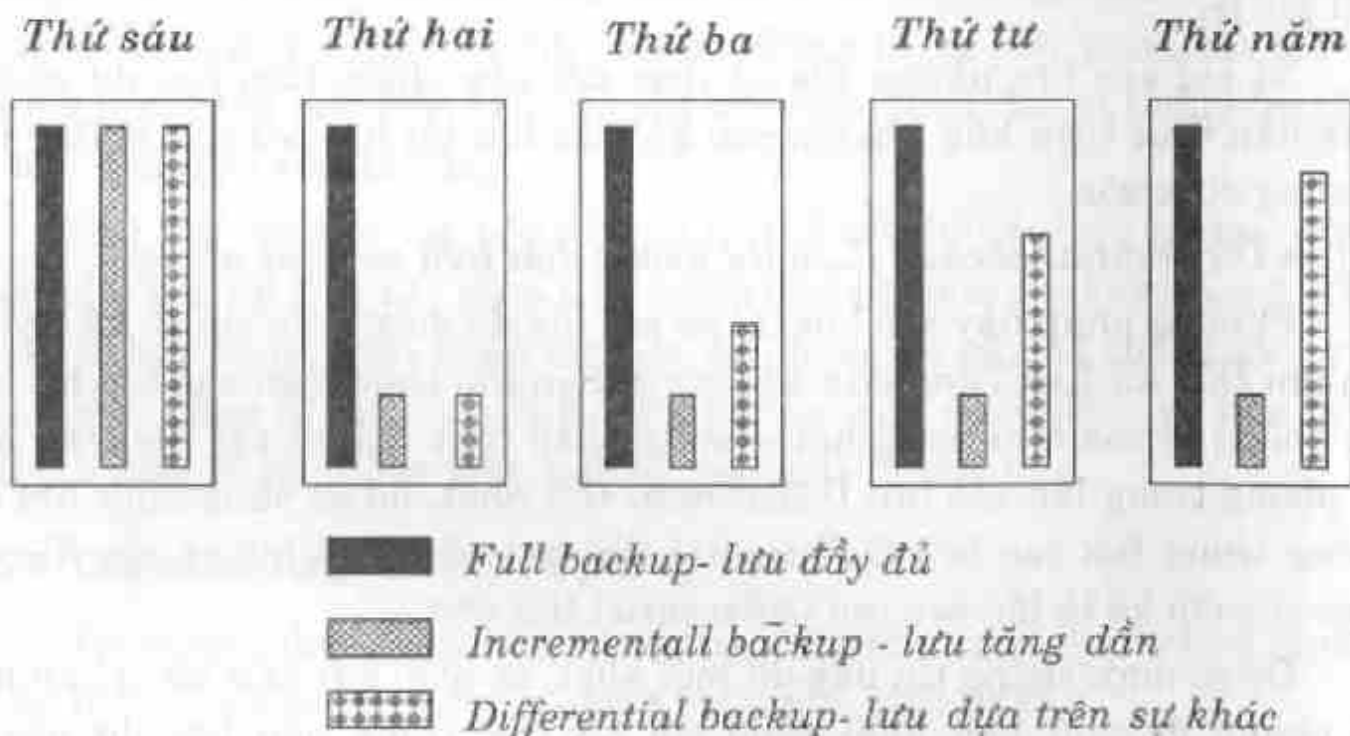
Chiến lược này sao lưu các file theo ý muốn chủ quan của thao tác viên mà không tác động lên bit lưu trữ do đó không ảnh hưởng gì tới các lần sao lưu theo những phương pháp khác.

• *Daily backup (Lưu dự phòng hàng ngày)*

Sao lưu những file được cập nhật trong ngày mà không thay đổi bit lưu trữ. Chiến lược này hữu ích nếu ta muốn mang dữ liệu về nhà và cần nhanh chóng chọn ra những file đã được cập nhật trong ngày hôm đó.

2.3.2. Ví dụ áp dụng phối hợp các loại hình sao lưu trong thực tế

Người ta thường phối hợp các chiến lược sao lưu với nhau vì mỗi cách có ưu nhược điểm riêng. Có loại cần nhiều thời gian nhưng lại đầy đủ, có loại nhanh nhưng khi cần khôi phục phải có đầy đủ nhiều cuộn băng của những lần sao lưu trước đó.



Hình 5.6. Lịch sao lưu

Lưu dự phòng đầy đủ

Nếu ta lựa chọn phương pháp sao lưu *Đầy đủ* thì mỗi ngày phải tiến hành sao lưu toàn bộ khối lượng dữ liệu. Làm như vậy rõ ràng tốn kém về thời gian và dung lượng băng từ để lưu trữ, nhưng có ưu điểm là bất kể hư hỏng xảy ra lúc nào, để tiến hành khôi phục chỉ cần một cuộn băng của lần sao lưu gần nhất.

Kết hợp chiến lược Full backup với Incremental backup

Vào thứ Sáu cuối tuần ta phải tiến hành sao lưu *đầy đủ*. Thứ hai, tất cả những thay đổi tính từ thứ sáu sẽ được sao lưu. Thứ ba lại sao lưu những thay đổi so với thứ hai... cứ như vậy. Cách làm này có lợi ở chỗ giảm được lượng dữ liệu phải sao lưu mỗi ngày đến mức thấp nhất. Tuy nhiên, giả sử hệ thống bị sự cố vào thứ năm thì phải cần 5 cuộn băng tính từ thứ sáu tuần trước để khôi phục lại thông tin.

Kết hợp chiến lược Full backup với Differential backup

Với cách làm này, vào thứ sáu hàng tuần ta phải tiến hành sao lưu *Đầy đủ*. Thứ hai, tất cả các thay đổi tính từ thứ sáu sẽ được sao lưu. Thứ ba, sao lưu tất cả những thay đổi tính từ thứ sáu ... Lượng dữ liệu phải sao lưu cứ lớn dần từng ngày, đổi lại nếu sự cố xảy ra với hệ thống vào thứ năm thì chỉ cần hai cuộn băng của thứ tư và thứ sáu tuần trước là ta có thể khôi phục được dữ liệu.

Duy trì nhật kí sao lưu

Đây là công việc cực kì quan trọng đối với việc phục hồi dữ liệu và phải được tiến hành thường xuyên đều đặn. Sổ nhật kí cần phải ghi nhận những thông tin sau đây:

- Ngày sao lưu
- Chiến lược sao lưu đã áp dụng
- Số hiệu máy trạm được sao lưu
- Những tập tin hay thư mục được sao lưu
- Số hiệu bộ băng từ lưu giữ thông tin sao lưu
- Nơi cất giữ băng từ
- Cuối cùng là tên nhân viên thực hiện công việc sao lưu

CÂU HỎI CUỐI CHƯƠNG

Điền từ (cụm từ) thích hợp vào chỗ trống

1. Người đầu tiên đăng nhập vào mạng sẽ sử dụng tài khoản....
.....
2. Tài khoản người dùng chứa những thông tin cho phép hệ thống
..... của mạng nhận diện anh ta
3. Hai thông tin chủ chốt của tài khoản mà khi đăng nhập người dùng
phải khai báo vào là..... và
4. Tài khoản dành cho những người khách tham quan là
5. Người quản trị mạng tạo một tài khoản nhằm
đơn giản hóa việc quản lý nhiều tài khoản có chức năng tương tự
nhau.
6. Thuộc tính của tài khoản cho phép chủ tài khoản thực
hiện những tác vụ hệ thống, chẳng hạn như sao lưu và phục hồi tệp.
7. Người quản trị trao cho nhóm để các thành viên
có thể truy cập các tài nguyên mạng như tập tin, máy in ...
8. Biện pháp hàng đầu để bảo vệ dữ liệu thường là một hệ thống
9. Khi tiến hành sao lưu dữ liệu cần phải thường xuyên duy trì
10. Khi tiến hành sao lưu, có thể giảm bớt lượng dữ liệu lưu thông trên
đường truyền bằng cách đặt hệ thống sao lưu trên một
- riêng biệt.
11. Các hệ thống dung lỗi (fault tolerance system) bảo vệ dữ liệu bằng
cách nhân bản và đặt dữ liệu trên những khác nhau.
12. RAID 0, còn gọi là..... chia dữ liệu thành từng khối
gọi là và phân bố đều trên các đĩa vật lý trong cụm.
13. Cơ chế RAID không cung cấp khả năng dung lỗi.
14. RAID..... nhân bản dữ liệu sao cho luôn tồn tại hai bản sao
giống nhau của dữ liệu trên hai đĩa vật lý khác nhau.
15. Duplexing được thiết kế nhằm tránh khỏi sự cố xảy ra với

HỆ ĐIỀU HÀNH WINDOWS 2000 SERVER

Chương này trình bày tóm lược cách cài đặt, vận hành khai thác và quản trị một trong những hệ điều hành mạng phổ biến nhất hiện nay, đó là Windows 2000 Server cùng với các máy trạm Windows 2000.

1. CÀI ĐẶT

1.1. Yêu cầu phần cứng

Là phiên bản tiếp nối của Windows NT 4.0, Windows 2000 Server đòi hỏi cấu hình máy tối thiểu là

- Bộ xử lí Pentium 166 trở lên. Trong thực tế không nên sử dụng các bộ xử lí từ Pentium II trở xuống.
- Tốc độ bus tối thiểu 350 MHz, đối với Celeron phải từ 500 MHz trở lên.
- Bộ nhớ không dưới 64 MB RAM, nếu là loại RAM có ECC (Error Correcting Code - Mã sửa lỗi) càng tốt.

Dung lượng đĩa cứng tối thiểu 850MB, cộng thêm với khoảng 100MB ứng với mỗi 64MB RAM. Như vậy thấp nhất phải có từ 1GB đến 2GB tùy theo những thành phần tiện ích cài đặt thêm.

Các con số nêu trên chỉ là tối thiểu, nói chung chúng ta nên và có thể dễ dàng có được cấu hình mạnh hơn nhiều dành cho máy chủ để cài đặt Windows 2000 Server. Chúng ta cũng nên lắp một ổ đĩa CDROM khởi động được (bootable) để trong trường hợp đĩa cứng gặp sự cố ta có thể khởi động máy và cài đặt hay khôi phục từ đĩa CD. Cuối cùng ta nên chú ý tới HCL* (Hardware Compatibility List - danh sách phần cứng tương thích) của Windows 2000 Server, tốt nhất là nên loại khỏi máy những thiết bị không có tên trong danh sách này vì không có gì đảm bảo là chúng hoạt động tốt, nếu không thì ít nhất ta phải có OEM driver đảm bảo tương thích với Windows 2000 Server. HCL của Windows 2000 Server có thể

* Khái niệm HCL và OEM Driver đã trình bày trong phần 3.3

xem tại địa chỉ www.microsoft.com/hwtest/hcl hoặc hiển thị ngay trong lúc cài đặt, còn OEM driver luôn đi kèm thiết bị.

1.2. Trù tính trước khi tiến hành cài đặt

1.2.1. Chuẩn bị các thông số BIOS

Nếu như Server có các card không thuộc dạng Plug and Play (PnP), chẳng hạn như một NIC hay Internal modem card thuộc loại ISA, thì chúng ta cần chạy trước các phần mềm đặt cấu hình IRQ, I/O Port... sao cho chúng không xung đột với nhau và với các thiết bị PnP còn lại. Trong mục Setup của máy, có thể truy nhập bằng cách ấn Del hay F10 khi máy đang khởi động, thường có mục Plug and Play quy định những IRQ nào được dùng cho mục đích tổng quát, nghĩa là có thể được cấp một cách linh hoạt cho các thiết bị PnP, và những ngắt nào để dành riêng cho các bo mạch non-PnP đời cũ. Nếu chúng ta không làm điều này, các card PnP có thể tự chọn nhầm phải những IRQ mà các card đời cũ đã chiếm lấy một cách cố định, khi đó máy sẽ "treo".

Nói chung, theo đà phát triển của công nghệ phần cứng, hiện nay các card non-PnP không còn phổ biến và nếu có thể chúng ta nên loại trừ chúng ra khỏi các máy, nhất là trên server vì ngoài việc gây xung đột ngắt, hiệu suất của chúng cũng rất thấp làm giảm tốc độ của mạng đi rất nhiều.

1.2.2. Trù tính các phân khu đĩa

Rõ ràng là không nên để nguyên đĩa cứng server chỉ gồm một phân khu duy nhất. Làm như vậy, nếu có sự cố gì xảy ra với dữ liệu thì sự cố đó dễ dàng ảnh hưởng đến các tệp tin hệ thống có thể dẫn đến việc server không khởi động được. Nhưng vấn đề là nên chọn cách phân chia phân khu như thế nào.

Việc chia đĩa cứng server thành các phân khu còn phụ thuộc vào những chức năng mà server đó đảm nhiệm. Nếu như chỉ là File server hay Print server thì việc phân chia sẽ đơn giản hơn các server đóng nhiều vai trò như Mail server, Application server...

Với Windows NT và Windows 2000 Server, chúng ta có hai lựa chọn kiểu hệ thống tập tin: kiểu NTFS và kiểu FAT (gồm FAT 16 và FAT 32). Với FAT 16 chúng ta đã làm quen trong các hệ điều hành như MSDOS, Windows 3.1 còn FAT 32 xuất hiện trong Windows 9x và Windows 2000.

Riêng NTFS là kiểu hệ thống file chỉ có trong Windows NT trước kia và Windows 2000 Server hiện nay. NTFS an toàn hơn FAT nhiều vì nó cho phép chúng ta thiết lập cơ chế hàng rào bảo mật đến từng file và thư mục. Tuy nhiên nếu chúng ta có ý định giữ server ở tình trạng dual-boot, tức là khi khởi động có thể chọn một trong nhiều hệ điều hành khác nhau như Windows 9x, Windows 2000 Server ... và các hệ điều hành kia cũng có thể truy cập dữ liệu trên các phân khu của Windows 2000 Server thì ta phải chọn FAT vì Windows 9x không thể truy nhập hệ thống file NTFS.

Một cách làm thường được áp dụng là tạo một phân khu khởi động (sẽ trở thành ổ đĩa C:) được định dạng theo kiểu FAT 32, có kích thước khoảng 1-3 GB. Trên phân khu này chứa các tập tin của những hệ điều hành ta muốn cài đặt cùng với cả *bộ cài đặt* (tức là những chương trình cài đặt được copy từ đĩa CDROM) của chúng. Làm như vậy khi cần bổ sung, loại bớt các thành phần tiện ích ta không phải tìm đĩa CDROM để lấy những driver tương ứng, tất cả đã có sẵn trong máy.

Sau đó, có thể có một phân khu NTFS chứa những dữ liệu chung của mạng cần được bảo mật và một phân khu FAT 32 chứa những dữ liệu, bộ cài đặt những tiện ích cần được chia sẻ chung trên mạng.

1.2.3. Lựa chọn tên Server, domain, group

Tên của máy chủ, các máy trạm cũng như các nhóm làm việc cần phải được đặt một cách có tính toán sao cho:

- Dễ nhớ
- Ngắn gọn đến mức tối đa
- Không trùng hợp ngay cả khi hệ thống mở rộng trong tương lai.

1.2.4. Lựa chọn giao thức kết nối


Chủ yếu chúng ta chỉ cần xem xét TCP/IP và NetBEUI. Theo mặc định, giao thức được chọn sẽ là TCP/IP và nói chung lựa chọn này là thích hợp nhất. NetBEUI là một giao thức *bất khả tiếp vận (non-routeable protocol)* nghĩa là các thiết bị cầu nối (router) giữa các mạng con sẽ không chuyển những gói dữ liệu tuân theo giao thức NetBEUI từ mạng con này sang mạng con khác. Tuy nhiên nó cũng có ưu điểm so với TCP/IP.

Nếu dùng TCP/IP thì ta sẽ phải tính đến việc có sử dụng DHCP Server hay không, sau đó gán các địa chỉ IP, Subnet mask... Nếu mạng của chúng ta cần liên kết với server nằm trên các mạng khác thì sẽ phải

quy định rõ địa chỉ gateway (cổng) mặc định nữa. Trong khi đó NetBEUI là một giao thức đơn giản, dễ hiểu được thiết kế cho những mạng LAN nhỏ có yêu cầu thấp về cấu hình và ta không phải bận tâm về tất cả những vấn đề nêu trên.

1.3. Các giai đoạn cài đặt Windows 2000 Server

1.3.1. Giai đoạn Preinstallation (Khởi động cài đặt)


 Đầu tiên ta phải truy cập vào nguồn cài đặt (setup source), tức là thư mục chứa bộ cài đặt. Thông thường bộ cài đặt của ta nằm trên đĩa CDROM và CPU là Intel, như thế thì nguồn cài đặt sẽ là thư mục I386 của đĩa CD đó.

Trong một số trường hợp, chẳng hạn máy chưa có hệ điều hành, chúng ta không có công cụ truy cập và khởi động trình cài đặt từ ổ đĩa CDROM thì phải dùng phương pháp cài đặt từ đĩa mềm. Các bước tiến hành như sau:

- Chuẩn bị bốn đĩa mềm 1.44 MB trống
- Sử dụng một máy khác có ổ đĩa CDROM, truy cập vào thư mục BOOTDISK trên đĩa CDROM chứa bộ cài đặt
- Thực hiện lệnh makeboot.exe
- Lần lượt đưa các đĩa mềm vào ổ theo các chỉ dẫn xuất hiện trên màn hình.
- Sau đó ta đã có bộ đĩa khởi động tiến trình cài đặt. Ta sẽ dùng đĩa thứ nhất để khởi động máy server và các đĩa sau để tiếp tục tiến trình cài đặt.
- Nếu trên máy server đã có một hệ điều hành như DOS, Windows 3.1 thì ta phải bắt đầu tiến trình cài đặt trong chế độ DOS (gõ lệnh tại dấu nhắc) bằng lệnh WINNT.EXE.

Nếu hệ điều hành có sẵn trên máy server là Windows 9x, Windows NT thì ta chỉ việc thực hiện lệnh WINNT32.EXE, chẳng hạn chọn **Start/Run** rồi gõ


F:\I386\WINNT32.EXE

 Thỏa thuận về giấy phép sử dụng (licensing). Có hai kiểu cấp phép sử dụng:

Cấp phép theo chỗ ngồi (per-seat licensing): đòi hỏi mỗi máy trạm truy cập vào server đang cài đặt phải có một giấy phép. Làm theo cách

này ta chỉ cần đếm số máy trạm mà không cần quan tâm đến việc có bao nhiêu mối liên kết (connection) đồng thời vào server hay từ mỗi máy trạm có thể có bao nhiêu connection đến server.

Cấp phép theo server (per-server licensing): mỗi liên kết từ máy trạm vào server đều phải có một giấy phép. Nếu một máy trạm có 10 connection đến 10 server đồng thời thì phải có 10 giấy phép.

 **Special Options.** Tại đây ta phải lựa chọn các mục sau:

- Language options: chọn ngôn ngữ sử dụng sau này
- Advanced options: chọn cách thức cài đặt
- Location of Windows 2000 files: chỉ ra vị trí của bộ cài đặt, chẳng hạn F:\I386\
 - Windows installation folder: chỉ ra vị trí thư mục mà ta muốn Windows 2000 Server sẽ được cài đặt vào đó.
 - Copy all Setup files from the Setup CD to the hard drive: copy bộ cài đặt vào đĩa cứng để dùng sau này, mỗi khi cần bổ sung thêm một thành phần tiện ích hay thiết bị nào đó.
 - I want to choose the installation partition during Setup: chỉ ra phân khu đĩa mà ta định cài đặt Windows 2000 vào đó.
 - Accessibility options: gồm hai lựa chọn giúp theo dõi quá trình cài đặt sau này. Narrator: có giọng tường thuật quá trình thao tác, Magnifier: có kính lúp phóng đại cho dễ theo dõi

1.3.2. Giai đoạn *Text-based setup* (cài đặt trên màn hình văn bản)

So với các phiên bản Windows NT trước kia, công đoạn *Text-based setup* lần này đơn giản hơn nhiều. Trước tiên chúng ta sẽ gặp màn hình chào đón (Welcome screen), thực hiện vài lựa chọn về nơi cài đặt sau đó chỉ việc ngồi đợi và xem chương trình cài đặt sao chép các tệp. Trong giai đoạn này chỉ có một số bước cần chú ý sau đây:

– Nếu máy Server của chúng ta có những card điều khiển như SCSI hay RAID mà ta biết chắc rằng chúng sẽ không hoạt động nếu thiếu trình OEM Driver thì đây chính là lúc chúng ta cài đặt những trình điều khiển đó. Ấn F6 ngay khi thấy xuất hiện lời nhắc phía dưới màn hình rồi chọn loại card và vị trí thư mục chứa OEM driver.

– Tiếp theo là một khâu cực kì quan trọng: chia đĩa cứng thành các phân khu. Ta sẽ thực hiện những ý đồ trừu tượng trước bằng một công cụ

phân chia và định dạng đĩa rất mạnh mẽ. Tại đây ta có thể xóa bỏ các phân vùng đã có, tạo ra những phân vùng mới và các ổ đĩa logic, định dạng (format) chúng theo kiểu NTFS hay FAT32, FAT 16. Cần phải hết sức cẩn thận vì một khi đã bấm phím xóa phân khu thì không có cách nào khôi phục lại những dữ liệu được lưu trên phân khu đó.

– Cuối cùng trước khi chuyển sang bước Graphical-based setup (mục 1.3.3 dưới đây), trình cài đặt còn tiến hành thêm bước kiểm tra cấu trúc tệp tương tự như CHKDSK trên các đĩa logic, sau đó khởi động lại máy.

1.3.3. Giai đoạn Graphical-based setup

⌚ Sau khi khởi động lại, máy sẽ bước vào giai đoạn thứ ba và cũng là cuối cùng. Tại đây trình cài đặt sẽ dò tìm để phát hiện tất cả các thiết bị PnP có trong máy và thử điều khiển nó bằng một driver thích hợp nhất mà Windows 2000 có được. Kho driver của Windows 2000 khá phong phú nên ít khi ta phải dùng đến các OEM driver, trừ những trường hợp rất đặc biệt mà ta biết chắc rằng chỉ có driver của chính hãng sản xuất mới điều khiển thiết bị hoạt động chính xác.

⌚ Khung hội thoại **Regional Configuration**. Tại đây ta sẽ chọn những mục như: dạng kí hiệu số, đơn vị tiền tệ, dạng thức ngày tháng, kiểu bố trí bàn phím hiện tại ...

⌚ Khung hội thoại **Name and Organization**. Tại đây ta sẽ khai báo tên người dùng và tên cơ quan.

⌚ Khung hội thoại kế tiếp xác định kiểu cấp phép mà ta đang sử dụng là Per-seat hay Per-server. Sau đó là phần khai báo **Computer name** (tên Server) và **Administrator password** (mật khẩu của người quản trị mạng). Ta cần hết sức cẩn thận khi lựa chọn mật khẩu cho Administrator vì đây là cấp tối cao của mạng, nếu để mật khẩu đơn giản có thể sẽ bị người khác đoán ra, nếu để thất lạc hay quên thì chỉ còn cách cài đặt lại từ đầu.

⌚ Khung hội thoại **Components Selection** giúp ta chọn những thành phần dịch vụ bổ sung được đóng gói chung với Windows 2000 như:

- Internet Information Server
- Management and Monitoring Tools
- Connection Manager Component

- Network Monitor Tools
- SNMP
- Networking Services
- Domain Name System
- DHCP
- Simple TCP/IP Services

.....



Khung hội thoại **Network Settings** cho phép ta chọn một trong hai kiểu cấu hình mạng: **Typical** và **Custom**. Kiểu **Typical** ngầm định rằng mạng của chúng ta chỉ dùng **Client for Microsoft Networks**, **File and Print Sharing** và giao thức **TCP/IP** kèm theo sự hỗ trợ của **DHCP**. Kiểu **Custom** cho phép ta thoải mái thêm vào hay bỏ bớt đi các giao thức, các dịch vụ mạng.



Tại trang chọn lựa **Workgroup/Domain** ta có thể lựa chọn việc máy đang cài sẽ gia nhập một **Workgroup** (nhóm) hay **Domain** (miền). Để gia nhập **Domain** cần phải tạo ra một tài khoản cho máy theo một trong các cách:

Chọn nút **Create Computer Account**, sau đó gõ tên tài khoản và mật khẩu. Tài khoản này phải có quyền hạn **Administrator** hoặc **Account Operator**. Nếu định dùng một tài khoản từ miền mà ta đang định gia nhập thì phải gõ tên và mật khẩu của tài khoản đó. Nếu định dùng tài khoản từ miền được ủy quyền của miền định gia nhập thì phải nhập đầy đủ tên miền và tên tài khoản theo dạng **DOMAIN\USERNAME**.

Cách thứ hai là không chọn **Create Computer Account** mà dùng một tài khoản được tạo từ trước. Cách này được dùng khi người cài đặt không có đủ những quyền hạn thích hợp. Ta phải đến màn hình **Server Manager** dành cho miền đang định gia nhập, chọn **Computer/Add to Domain**/gõ tên máy.

Đến đây, việc cài đặt gần như hoàn tất. Trình cài đặt sẽ sao chép nốt một số file, định cấu hình cho hệ thống và các thao tác dọn dẹp những tệp trung gian. Tệp **boot.ini** được sửa lại lần cuối và từ nay về sau sẽ được sử dụng mỗi lần khởi động máy.

2. TÌM HIỂU ACTIVE DIRECTORY

Active Directory, gọi tắt là AD, là thành phần quan trọng nhất của Windows 2000 và có mặt gần như trong mọi chức năng chủ yếu của Windows 2000. Nó là sự mở rộng của cấu trúc quản lý mạng theo Miền (domain), Nhóm (group)... của Win NT trước kia với sự bổ sung các khái niệm mới như: Cây (Tree), Rừng (Forest), Đơn vị tổ chức (Organization unit)...

Mọi hệ thống bảo mật đều lưu trữ các tài khoản người dùng trên các cơ sở dữ liệu tồn tại dưới dạng tệp. Với Windows NT, đó là một tệp duy nhất có tên là SAM (Security Accounts Manager). Trong đó là các thông tin như: user name (tên đăng nhập), full name (tên đầy đủ), password (mật khẩu), allowed logon hours (những giờ được phép đăng nhập), account expiration date (ngày tài khoản hết hiệu lực), danh sách các nhóm mà user đó trực thuộc, profile... Tất nhiên các thông tin đó đã được mã hóa trước khi ghi ra tệp.

Windows 2000 Server cũng sử dụng một tệp để lưu các thông tin tương tự, tệp đó có tên là NTDS.DIT. Tệp NTDS.DIT của Windows 2000 khác với SAM của Windows NT ở một số điểm, ví dụ như các thông tin về người dùng trong NTDS.DIT đa dạng hơn SAM nhiều.

2.1. Miền (domain)

Miền, hay còn gọi là **Vùng**, là một đơn vị, một cấp trong hệ thống bảo mật của mạng Windows 2000, gồm những máy tính và người sử dụng dùng chung một nguyên tắc bảo mật và một cơ sở dữ liệu tài khoản người dùng. Khi một tài khoản người dùng thuộc vào một miền, những quyền hạn của người này sẽ có phạm vi tác dụng trên toàn miền đó. Chẳng hạn anh ta có thể đăng nhập (login) từ bất kỳ một máy trạm nào thuộc miền, những cập nhật về tài khoản của anh ta chỉ cần tiến hành một lần duy nhất mà vẫn có tác dụng trên toàn miền đó. Mô hình quản lý theo miền hỗ trợ cho việc quản lý mạng một cách tập trung, nó cho phép xây dựng một chính sách mạng đồng nhất và thuận lợi.

Cũng như Windows NT, trong miền Windows 2000 tất cả server đều chứa một bản sao danh sách tài khoản người dùng để dễ dàng kiểm tra việc đăng nhập và giám sát sự truy cập tài nguyên trên toàn miền. Còn bản chính của danh sách đó chỉ nằm trên một hoặc một vài server, những

server này được gọi là **Domain Controller**. Khi bản chính có sự thay đổi (chẳng hạn bổ sung thêm một người dùng) thì sẽ xảy ra sự đồng bộ hóa giữa bản chính với các bản sao để chúng luôn luôn nhất quán. Miền chính là tập hợp những máy tính sử dụng và tham khảo cùng một danh sách tài khoản người dùng.

2.2. Nhóm (group)

Như đã trình bày trong Chương 5 – Quản trị mạng, Nhóm là công cụ giúp cho Người quản trị dễ dàng thiết lập, áp dụng những chế độ, mức quyền hạn cho một nhóm những người sử dụng nào đó. Chẳng hạn ta cần ban quyền truy cập tệp `CHINH_SACH_LUONG.DBF` cho các vị trưởng phòng trong cơ quan thì chỉ việc ban quyền đó cho nhóm `TRUONG_PHONG` rồi kết nạp các vị trên vào nhóm đó. Sau này nếu cần cho phép các vị đó truy nhập các tài nguyên khác thì chỉ cần làm một thao tác là ban quyền sử dụng tài nguyên đó cho nhóm `TRUONG_PHONG` là đủ.

Điểm mở rộng của Windows 2000 so với NT 4 là ngoài tài khoản người dùng thì nhóm của Windows 2000 bây giờ có thể chứa cả tài khoản máy, và các nhóm có thể lồng nhau sâu hơn một cấp. Trước kia với NT 4, chỉ có Nhóm cục bộ (local group) mới có thể chứa Nhóm toàn miền (Global group), còn Nhóm toàn miền không thể chứa được bất kì nhóm gì, và Nhóm cục bộ cũng không thể chứa một nhóm cục bộ khác. Như vậy thành ra việc lồng nhau chỉ có thể có tối đa đến hai cấp, đó là một nhóm cục bộ chứa một nhóm toàn miền mà thôi.

Để cải thiện tình trạng đó, Windows 2000 tăng số loại nhóm từ hai lên đến bốn và nhờ đó cho phép lồng nhau sâu hơn hai cấp. Đó là các loại nhóm:

- Machine local group (Nhóm tại chỗ của máy)
- Domain local group (Nhóm tại chỗ của miền)
- Global group (vẫn là nhóm toàn miền như trước kia)
- Universal group (Nhóm toàn rừng)

Cuối cùng, một hạn chế của Windows 2000 là mỗi nhóm chỉ được phép có không quá 5000 thành viên.

2.2.1. Nhóm tại chỗ của máy (Machine local group)

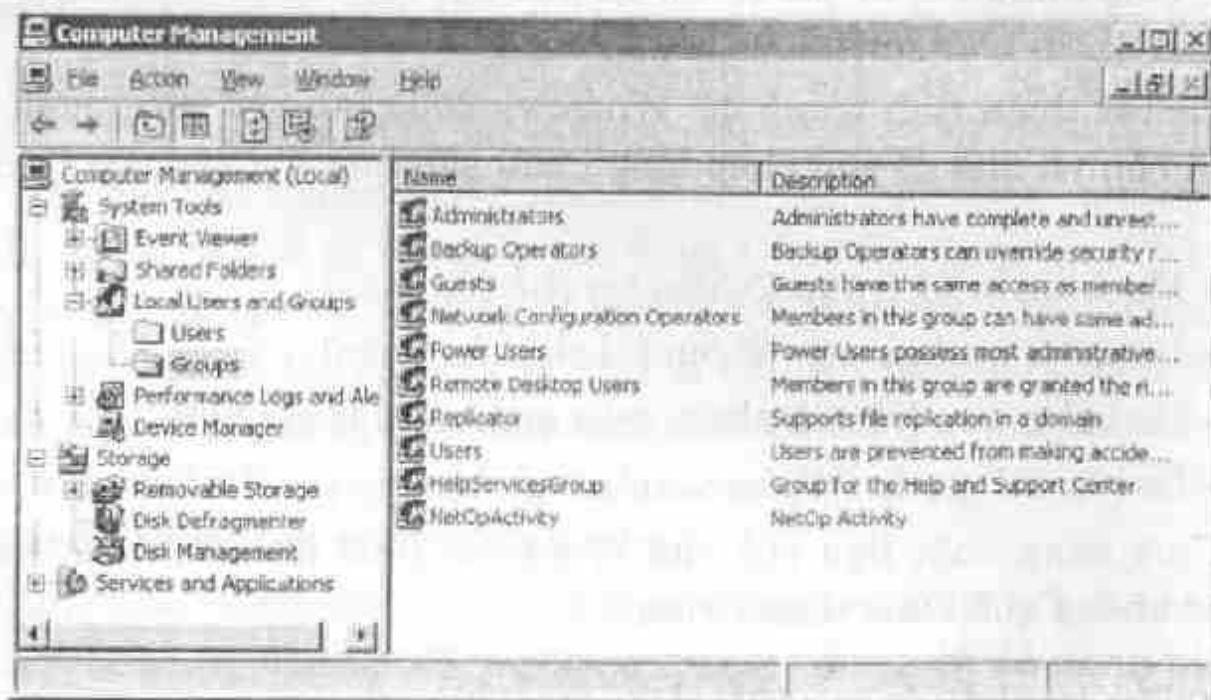
Các nhóm tại chỗ của máy có chức năng giống như nhóm cục bộ của

NT 4 trước kia. Mỗi máy tính trong mạng đều có những nhóm cục bộ được ban sẵn những quyền hạn để sử dụng những tài nguyên tại chỗ của máy đó, chẳng hạn quyền truy nhập các thư mục nằm trên đĩa cứng tại máy đó hay quyền sử dụng máy in đang nối vào cổng LPT của máy đó. Mỗi server đều có sẵn nhóm cục bộ Administrator dành cho quản trị viên, những người có toàn quyền làm mọi chuyện trên máy đó, hay như nhóm User gồm những người có thể đăng nhập vào máy đó và thực hiện một số công việc cơ bản.

Ngoài ra còn có các nhóm tại chỗ của máy khác nữa. Ta có thể xem danh sách của chúng bằng cách: bấm phím phải vào My computer, chọn Manager. Khi đó cửa sổ Microsoft Management Console (MMC) hiện ra. Ta kích đúp vào Local Users and Groups / Group và sẽ thấy danh sách như sau:

Các nhóm tại chỗ có thể chứa các nhóm toàn miền, bằng cách đó mới có thể cho phép phạm vi tác dụng của một người dùng bao phủ mọi máy của miền đó. Tổng quát, một nhóm tại chỗ của máy có thể chứa:

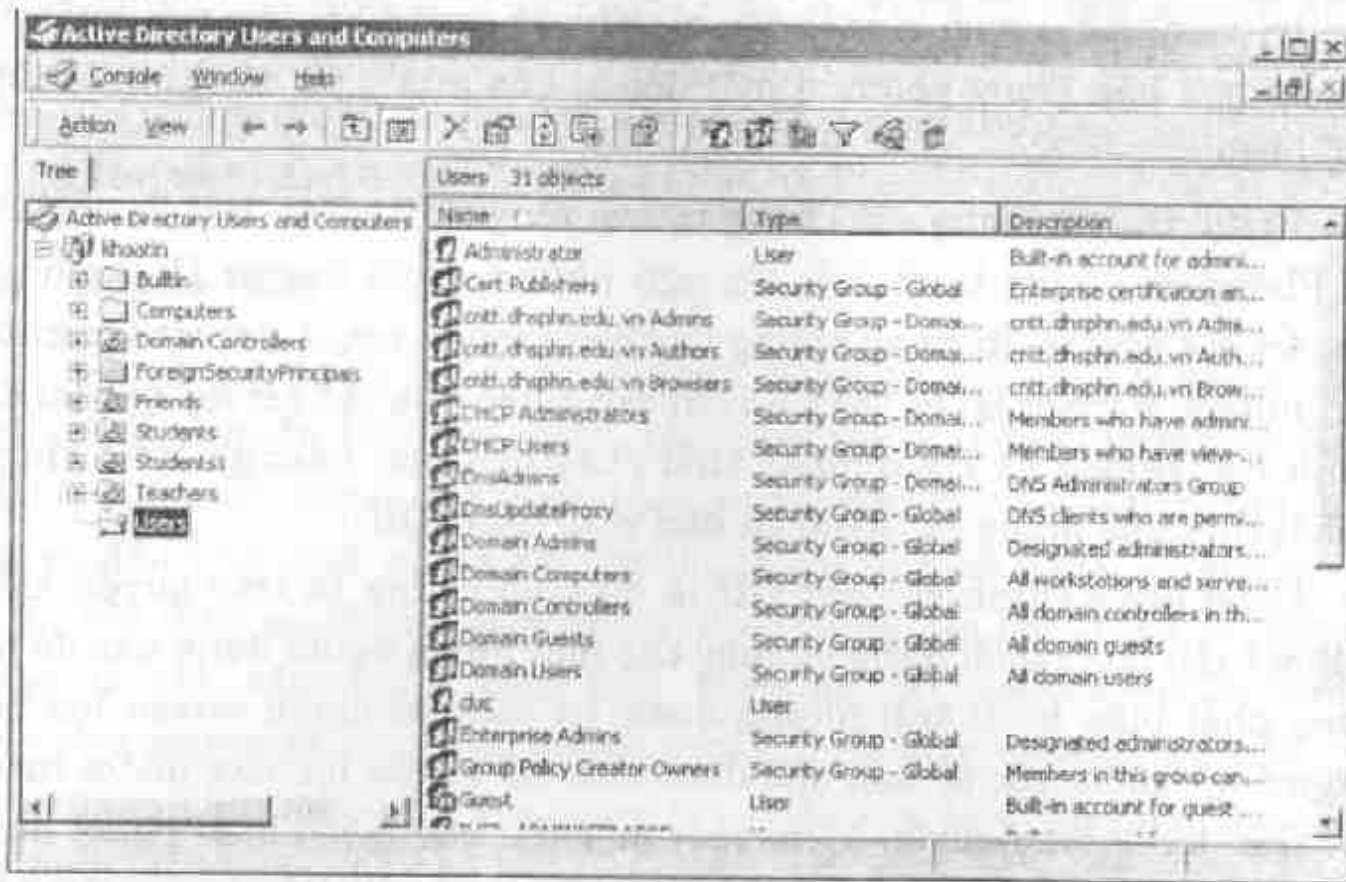
- Các nhóm Universal, nhóm Global và nhóm Domain Local tại miền nhà của chúng.
- Các nhóm Universal, nhóm Global của một miền được ủy quyền (Trusted domain)
- Các nhóm Global của một miền NT 4 được ủy quyền.



Hình 6.1

2.2.2. Nhóm tại chỗ của miền (Domain local group)

Để quan sát loại nhóm này, ta thực hiện một chương trình bổ túc cho MMC là Active Directory Users and Computers trên menu chương trình Administrative tools hoặc gõ trực tiếp: **Start/Run: dsa.msc**



Hình 6.2

2.2.3. Nhóm toàn miền (Global group)

Hoàn toàn giống với các nhóm toàn miền của NT 4, Global group của Windows 2000 là công cụ quản trị thống nhất của người quản trị mạng. Các Global group chỉ có thể được tạo ra trên các máy Domain controller.

2.2.4. Nhóm toàn rừng (Universal group)

Nhóm tại chỗ (local group) thường chỉ nhằm mục đích chứa những người dùng và các nhóm khác (global group), ngược lại nhóm toàn miền (global group) lại chủ yếu được kết nạp vào trong một nhóm tại chỗ (local group). Nhóm toàn rừng là loại nhóm có cả hai tính năng đó, nghĩa là nó có thể chứa bất kì một global group hay universal group nào, từ bất kì một miền nào trong rừng.

2.3. Đơn vị tổ chức (Organization Unit - OU)

Miền là một đơn vị tổ chức rất lớn, nếu chỉ có một người thì khó lòng quản lý xuể. Có nhiều trường hợp chúng ta phải chia nhỏ miền ra thành những đơn vị nhỏ hơn để trao nhiệm vụ điều khiển cho một nhóm những quản trị viên, mỗi người lo một đơn vị. Khi đó quyền lực của mỗi quản trị viên chỉ giới hạn trong phạm vi một đơn vị của mình, và đó chính là **đơn vị tổ chức**.

Ví dụ: Giả sử mạng của chúng ta trải rộng từ Hà Nội, Hải Dương đến Hải Phòng và chúng ta có một đội ngũ những người Server Operator để quản trị các server. Rõ ràng chúng ta không muốn người Server Operator ở chi nhánh Hà Nội lại có toàn quyền can thiệp vào các server đặt tại chi nhánh Hải Dương và Hải Phòng. Giải pháp cho tình huống này là chúng ta phải chia nhỏ mạng ra thành ba đơn vị tổ chức (OU).

Công dụng chính của các OU là nó giúp chúng ta trao quyền kiểm soát một tập hợp người dùng và máy cho một nhóm người dùng nào đó mà không phải biến họ thành những quản trị viên có nhiều quyền lực hơn mức mong muốn, tức là hạn chế được mức độ quyền lực của nhóm người này. Quá trình trao quyền kiểm soát một OU cho một nhóm người dùng được gọi là *sự ủy quyền kiểm soát (delegating control)* OU. Ta chỉ cần bấm phím phải vào OU và một *wizard* có tên là Delegation sẽ tự động được kích hoạt để giúp chúng ta thực hiện điều này.

So sánh giữa OU và nhóm:

Chúng ta có thể nhận xét rằng OU và nhóm có vẻ giống nhau. Thực ra OU dùng để chứa những gì mà ta muốn quản lý, sau đó ta sẽ trao quyền kiểm soát OU cho một nhóm gồm những người được trao nhiệm vụ quản lý những thứ trong OU. Ví dụ như ta muốn giao cho một số quản trị viên nhiệm vụ quản lý phòng Kế hoạch, ta chỉ việc tạo một OU ứng với phòng Kế hoạch, tạo một nhóm gồm số quản trị viên kia, sau đó ủy quyền kiểm soát OU mới tạo cho nhóm đó.

2.4. Địa bàn (site)

Ngoài những thông tin về người dùng và cấu hình máy, AD còn xem xét cả vị trí địa lý của các máy trạm trong mạng (tất nhiên chúng ta phải

cung cấp những thông tin đó cho Windows 2000). Mỗi khu vực địa lí gồm những nhóm máy trạm đặt gần nhau và được kết nối bằng LAN sẽ được tổ chức thành một site. Như vậy Windows 2000 sẽ biết được đâu là những đường truyền WAN, là những đường truyền qua khoảng cách xa, tốn nhiều chi phí và thường chậm chạp. Sau đó Windows 2000 sẽ nén những thông tin phải gửi trên đường truyền này theo tỉ lệ rất tuyệt vời (có thể đến 10:1) đồng thời tìm cách gửi sao cho thời gian chuyển nhanh nhất mà chi phí lại rẻ nhất.

2.5. Cây và rừng

Cây là hệ thống phân cấp của các miền. Giả sử công ti Acme có hai chi nhánh ở miền Đông và miền Tây, như vậy ta nên chia mạng công ti thành ba miền: `acme.com`, `westcost.acme.com`, `eastcost.acme.com`. Miền tạo ra đầu tiên được gọi là *gốc (root)* của cây, giả sử đó là `acme.com`. Các miền bên dưới nó là các *miền con*, ví dụ như nếu ta chia theo tổ chức của công ti thì cấp miền con tiếp theo sẽ là: `sales.ecoast.acme.com`, `finance.ecoast.acme.com`, `sales.wcoast.acme.com`, `finance.wcoast.acme.com` ...

Trong khi chúng ta xây dựng cây phân cấp như vậy, Windows 2000 tự động tạo ra các quan hệ ủy quyền giữa mỗi miền và miền con của nó. Ví dụ khi chúng ta tạo ra miền con `wcoast.acme.com` thì mối quan hệ ủy quyền hai chiều sẽ được tự động tạo ra giữa nó và `acme.com`. Ngoài ra, trong Windows 2000 các mối quan hệ ủy quyền có tính bắc cầu (transitive). Có mối quan hệ ủy quyền hai chiều giữa `finance.wcoast.acme.com` với `wcoast.acme.com`, và giữa `wcoast.acme.com` với `acme.com` cho nên cũng có mối quan hệ ủy quyền hai chiều giữa `finance.wcoast.acme.com` với `acme.com`.

Rừng trong Windows 2000 là một nhóm các cây. Giả sử hai công ti `acme` và `apex` sáp nhập lại với nhau, mạng của công ti mới rõ ràng phải có hai miền: `acme.com` và `apex.com` và hai miền này không thể thuộc cùng một cây. Trường hợp này chúng ta sẽ tạo ra một rừng để chứa hai cây `acme.com` và `apex.com`. Trong hai miền đó, miền được tạo ra trước tiên sẽ là gốc của rừng.

3. MỘT SỐ CÔNG CỤ CỦA WINDOWS 2000

Tìm kiếm các công cụ quản trị mạng của Windows 2000 trên màn hình và menu Start chúng ta thấy có nhiều khác biệt so với Windows NT trước kia. Chẳng hạn như trong **Control Panel** không còn applet **Network** và **Services**, còn trong nhóm công cụ **Administrative Tools** cũng không thấy hai tiện ích rất cơ bản là **Server Manager** và **User Manager for Domains** bởi vì chúng đã được đưa vào một đối tượng mới của Windows 2000 có tên là **Microsoft Management Console (MMC)**.

3.1. Chức năng Network

Trước kia với Windows NT các công việc quản lý thiết bị mạng tập trung tại thẻ applet trong Control Panel, còn giờ đây chức năng này được chia thành nhiều công cụ nằm tại nhiều nơi khác nhau.

3.1.1. Đổi tên máy, tên miền

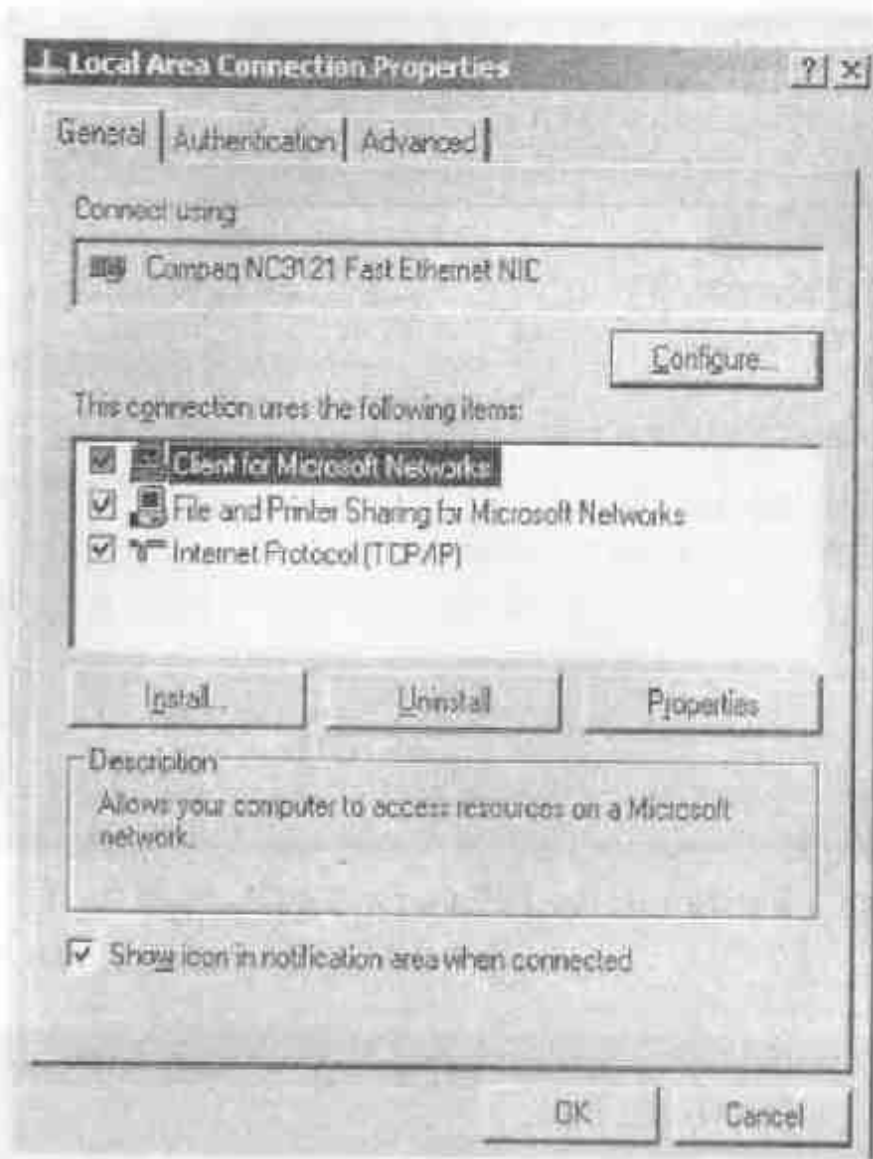
Để thay đổi tên máy trạm, tên miền hoặc nhóm làm việc, gia nhập một miền mới chúng ta mở khung hội thoại **System Properties** bằng cách chọn **Start/Settings/Control Panel/System** (Hoặc bấm phím phải tại **My Computer/ Properties**). Chọn thẻ **Network Identification**. Bấm nút **Properties** vào khung hội thoại **Identification Changes** để thay đổi tên máy, tên miền và nhóm.

Nếu muốn thay đổi cả phần hậu tố DNS trong tên miền thì bấm **More**. Chú ý rằng để gia nhập một nhóm làm việc hoặc một miền ta phải đăng nhập với tư cách một quản trị viên tại chỗ (**Local Administrator**), nếu muốn đưa máy này gia nhập một miền ta phải cung cấp một tài khoản người dùng hợp lệ của miền đó để tạo ra tài khoản máy cho mình.

3.1.2. Điều chỉnh các giao thức mạng

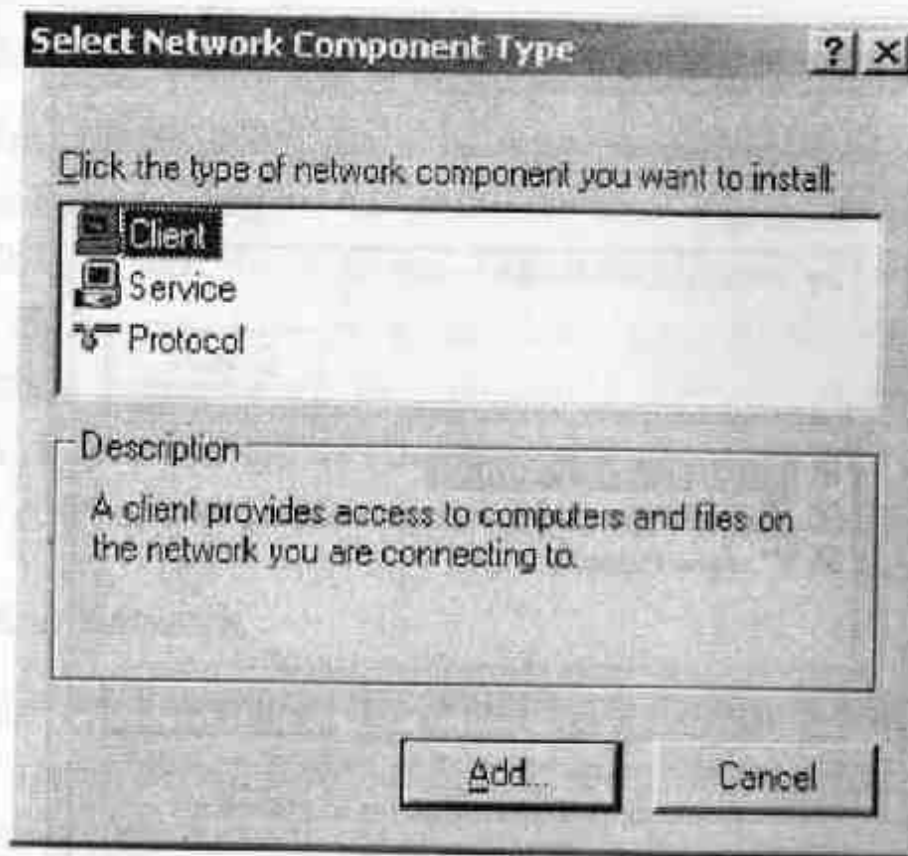
Ta bấm **Start/Settings/Network and Dial-Up Connections**

Để bổ sung giao thức cho server, ta chọn biểu tượng **Local Area Connection**, bấm phím phải và chọn **Properties**, ta sẽ có cửa sổ như hình 6.3.



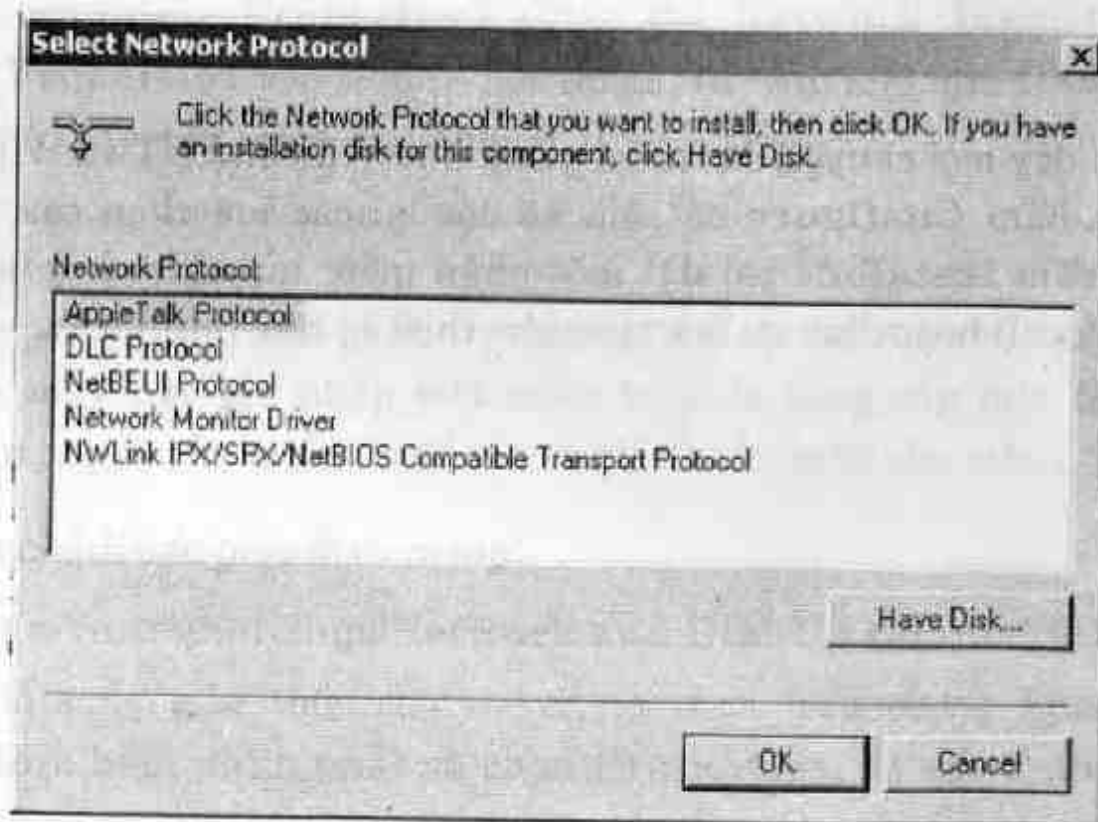
Hình 6.3

Đến đây mọi chuyện đã trở lại giống như Windows NT và Windows 9x. Chúng ta bấm **Configure** để xem và đặt lại các lựa chọn cấu hình cho thiết bị, bấm **Install** để cài đặt một phần mềm máy khách (client), giao thức (protocol) hoặc dịch vụ (service) cho thiết bị này (hình 6.4).



Hình 6.4

Giả sử ta chọn bổ sung thêm giao thức, danh sách những giao thức được hỗ trợ sẽ hiện lên (hình 6.5).



Hình 6.5

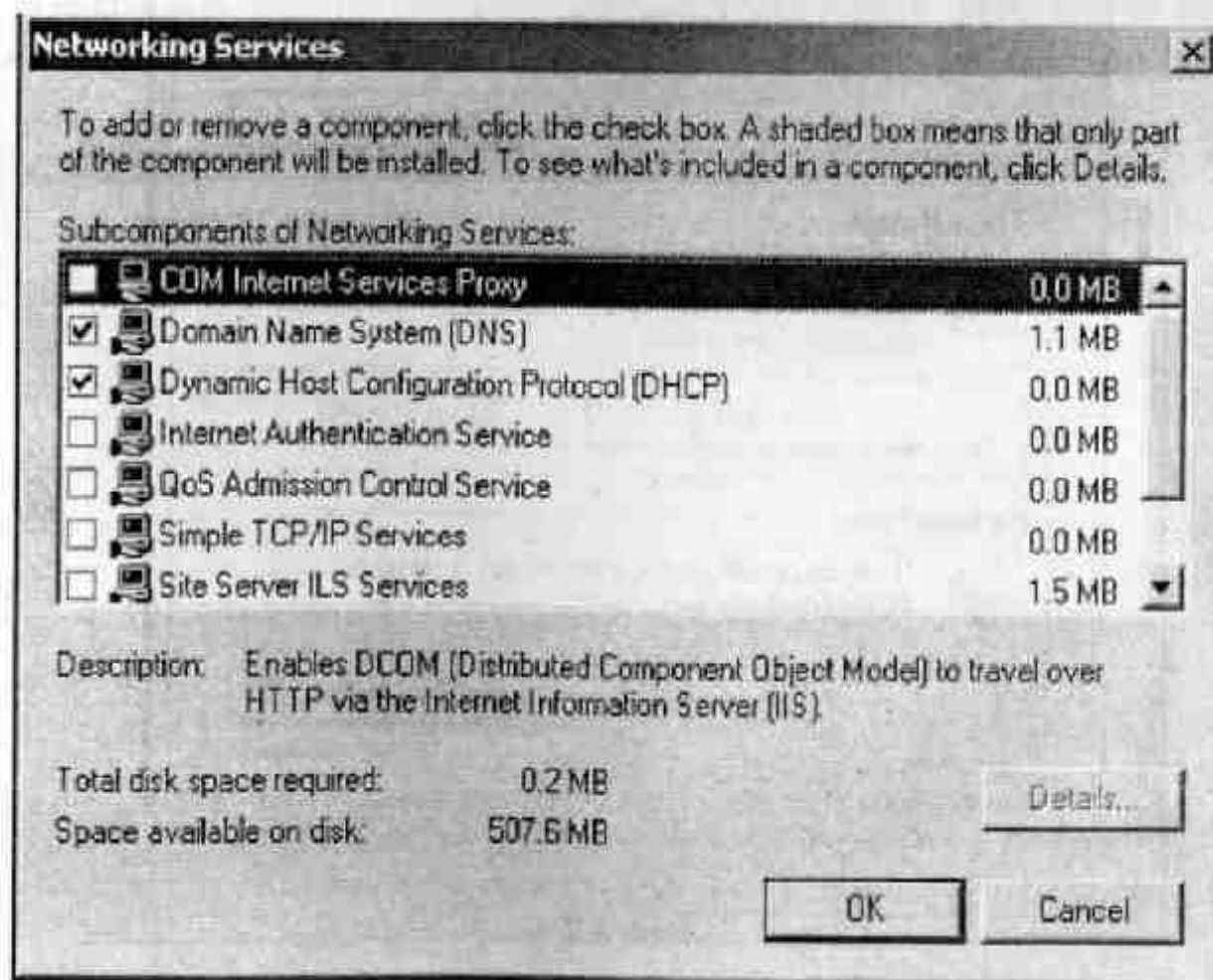
3.1.3. Điều chỉnh các dịch vụ mạng

Ta có thể cài đặt bổ sung, gỡ bỏ hoặc điều chỉnh tham số cho các dịch vụ mạng như:

- Microsoft File and Print Services,
- Gateway Services for Netware
- Client Services for Netware

bằng cách chọn biểu tượng phù hợp trong cửa sổ **Network and Dial-Up Connections** như đã mô tả trong mục 3.1.2. Chú ý rằng dịch vụ **Workstation** trong NT giờ đây được đổi tên thành **Client for Microsoft Networks**, còn dịch vụ **Server** đổi thành **File and Printer Sharing for Microsoft Networks** giống như cách gọi tên của Windows 9x.

Các dịch vụ như DNS, WINS và DHCP được bổ sung bằng cách chọn **Control Panel**, sau đó chọn **Add/Remove Programs /Add or Remove Windows Components**. Làm như vậy **Windows Components Wizard** sẽ được kích hoạt, ta chọn tiếp **Networking Services / Details** và trông thấy bảng chọn sau (hình 6.6).

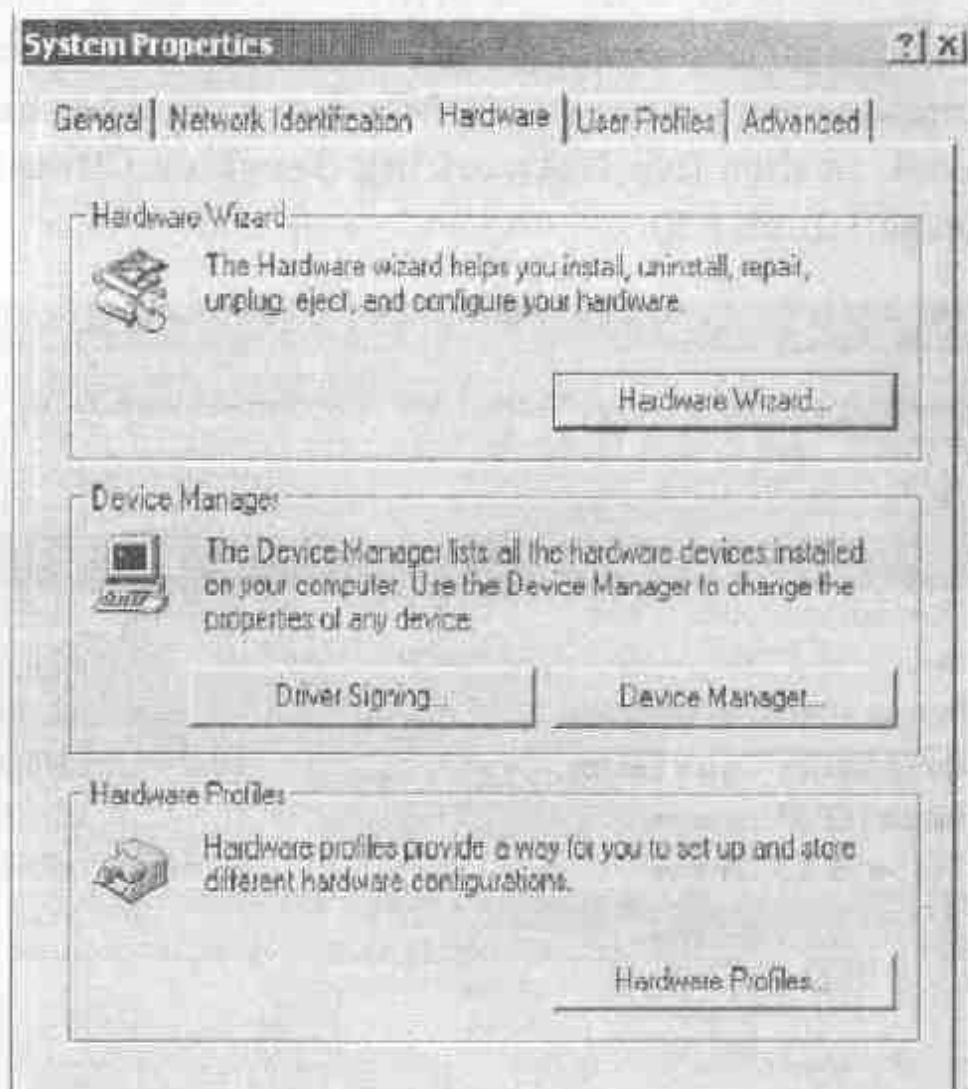


Hình 6.6

3.1.4. Cài đặt và gỡ bỏ các trình điều khiển thiết bị mạng

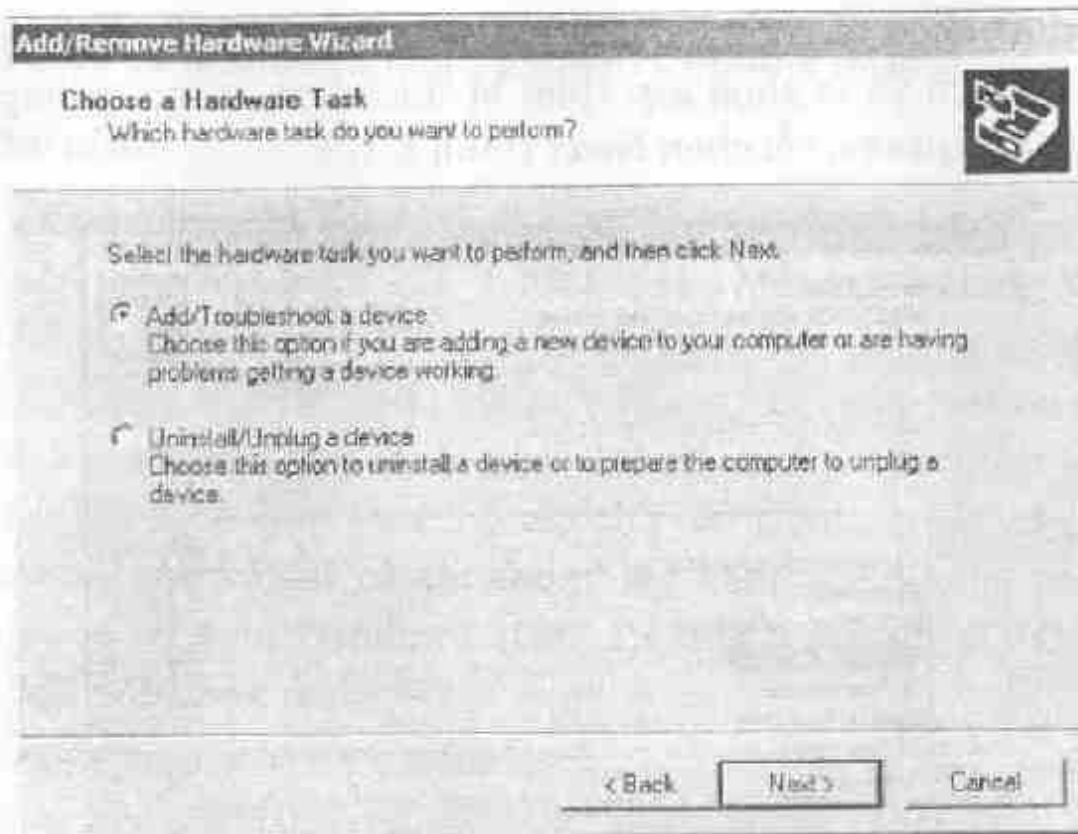
Windows 2000 là hệ điều hành có khả năng Plug and Play rất mạnh nên thông thường chúng ta không phải tự tay làm công việc này. Tuy nhiên có một số trường hợp đặc biệt, chẳng hạn như các Card RAID, mà chúng ta biết rõ rằng thiết bị sẽ làm việc tốt hơn nếu chúng ta thay trình điều khiển mặc định của Windows 2000 bằng các trình điều khiển OEM Driver. Khi đó chúng ta phải nhờ đến **Add/Remove Hardware Wizard** (hình 6.8). Để cài đặt thêm một trình điều khiển NIC chẳng hạn, chúng ta làm như sau:

Chọn **Start/Settings/Control Panel** sau đó chọn **Add/Remove Programs**. Ta cũng có thể mở applet **System/Hardware** rồi bấm nút **Hardware Wizard** (hình 6.7).



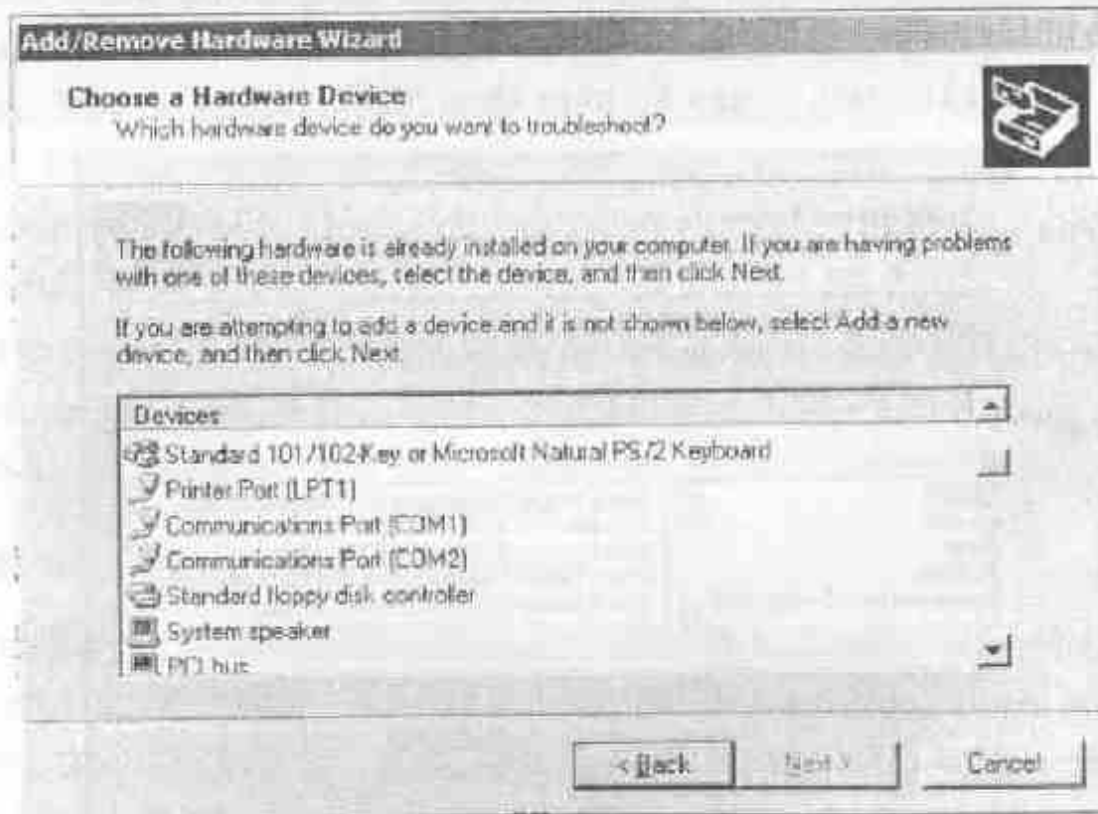
Hình 6.7

Tại màn hình Welcome, chọn Next/ Add/ Troubleshoot a Device.



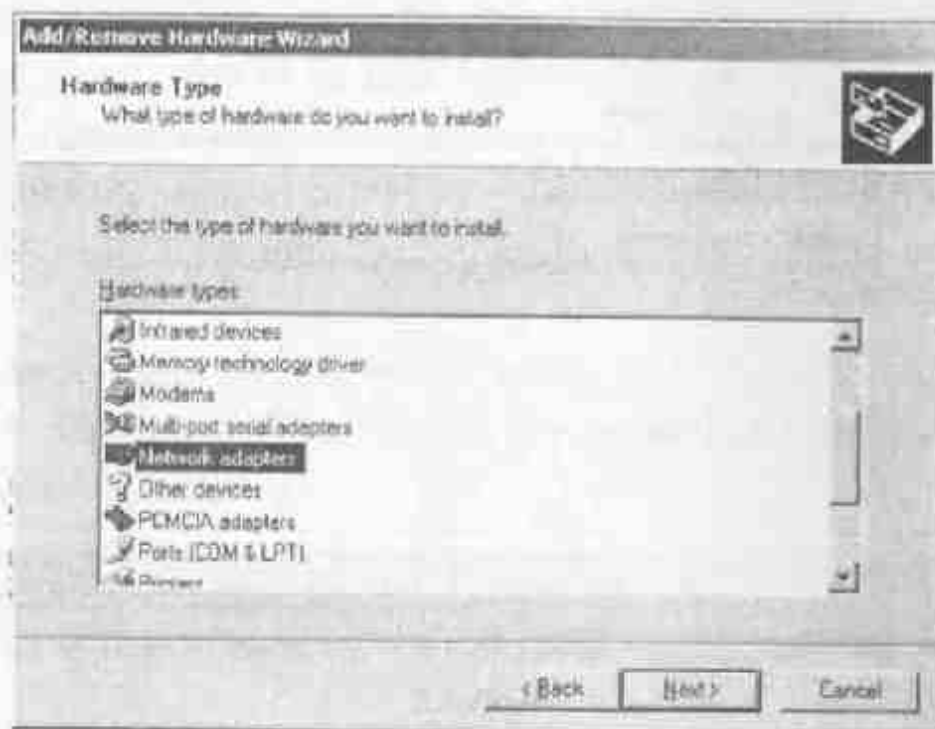
Hình 6.8

Wizard bắt đầu dò tìm các thiết bị PnP mới, sau đó nó sẽ hiện lên danh sách những gì mà nó tìm thấy. Ta chọn **Add a new device/Next**



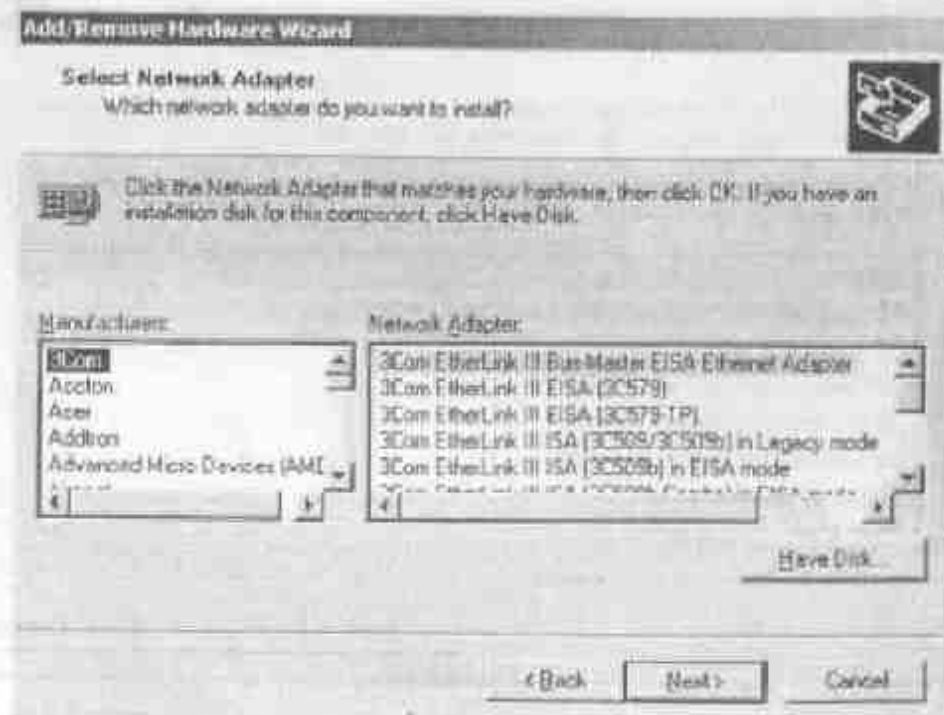
Hình 6.9

Tiếp theo chọn phương án lấy thiết bị từ danh sách, wizard sẽ hiển thị một danh sách và ta chọn loại thiết bị thích hợp, trong trường hợp này là **Network adapters**, rồi chọn **Next** (hình 6.10).



Hình 6.10

Sau đó ta chọn tên NIC, tên hãng sản xuất trong danh sách HCL, nếu NIC không có trong danh sách thì chọn **Have Disk** và sử dụng OEM Driver do hãng sản xuất cung cấp kèm theo NIC



Hình 6.11

3.2. Sơ lược về Microsoft Management Console (MMC)

3.2.1. Khái niệm

MMC là một cải tiến mới mẻ của Windows 2000, các công cụ quản trị quen thuộc của Windows NT 4 như User Manager, User Manager for Domain, Server Manager, Event Viewer, Disk Manager đều được đồng hóa vào trong MMC, nhờ đó người quản trị mạng chỉ cần làm quen và thành thạo một cửa sổ giao diện là đã có thể điều khiển được hàng loạt công cụ. Mặt khác, MMC là nền tảng hỗ trợ cho các công cụ của các hãng phần mềm khác và nhờ vậy sẽ có đất cho nhiều hãng phần mềm phát triển các công cụ quản trị trên Windows 2000. Để làm quen với MMC ta cần hiểu một số khái niệm của nó.

Console (cửa sổ điều khiển) là một hoặc nhiều công cụ quản trị trong bộ khung của MMC, chẳng hạn như Active Directory Users and Computers là một console có sẵn. Ngoài ra chính chúng ta cũng có thể tạo ra các console cho riêng mình, chúng sẽ tồn tại dưới dạng những file *.MSC (Microsoft Saved Console).

Snap-in (phần ghép thêm) là các công cụ quản trị được đưa vào một console, ví dụ như công cụ quản trị DHCP hay Disk Defragmenter. Các Snap-in có thể được Microsoft tạo ra hay do các hãng phần mềm khác xây dựng nên. Mỗi Snap-in có thể chứa các thành phần như node (đoạn, phần), container (đối tượng chứa). Các công cụ của Windows 2000 chỉ bao gồm một snap-in duy nhất, nhưng chúng ta có thể nạp thêm cho chúng những snap-in khác.

Extension (phần mở rộng) là một snap-in không tự mình nằm trên console được mà phải lệ thuộc vào một snap-in khác để bổ sung thêm chức năng cho snap-in đó.

3.2.2. Một số công cụ MMC thông dụng

Sau đây là một số công cụ quản trị MMC thông dụng, chúng ta biết tên của chúng để có thể gọi chúng ra nhanh hơn bằng cách gõ thẳng từ Start/Run. Hầu hết chúng đều nằm tại thư mục `\winnt\system32` và vì thế nằm trong đường dẫn mặc định nên chỉ cần gõ tên file, nhưng phải có cả phần mở rộng .MSC. Chỉ có tệp đầu và cuối danh sách là nằm tại `\winnt\system32\inetsrv`.

TÊN FILE MSC	TÊN THƯỜNG GỌI
MSINFO32.MSC	System information
COMPMGMT.MSC	Computer Management
DCPOL.MSC	Domain Controller Security Policy
DEVMGMT.MSC	Device Manager
DFRG.MSC	Disk Defragmenter
DFSGUL.MSC	Distributed File System
DISKMGMT.MSC	Disk Management
DOMPOL.MSC	Domain Security Policy
DOMAIN.MSC	Active Directory Domain and Trusts
DSA.MSC	Active Directory Users and Computers
DSSITE.MSC	Active Directory Sites and Services
EVENTVWR.MSC	Event Viewer
LUSRMgr.MSC	Local User Manager
DHCPMGMT.MSC	DHCP
DnSMGMT.MSC	DNS
IIS.MSC	Internet Information Services

3.2.3. Công cụ Computer Management

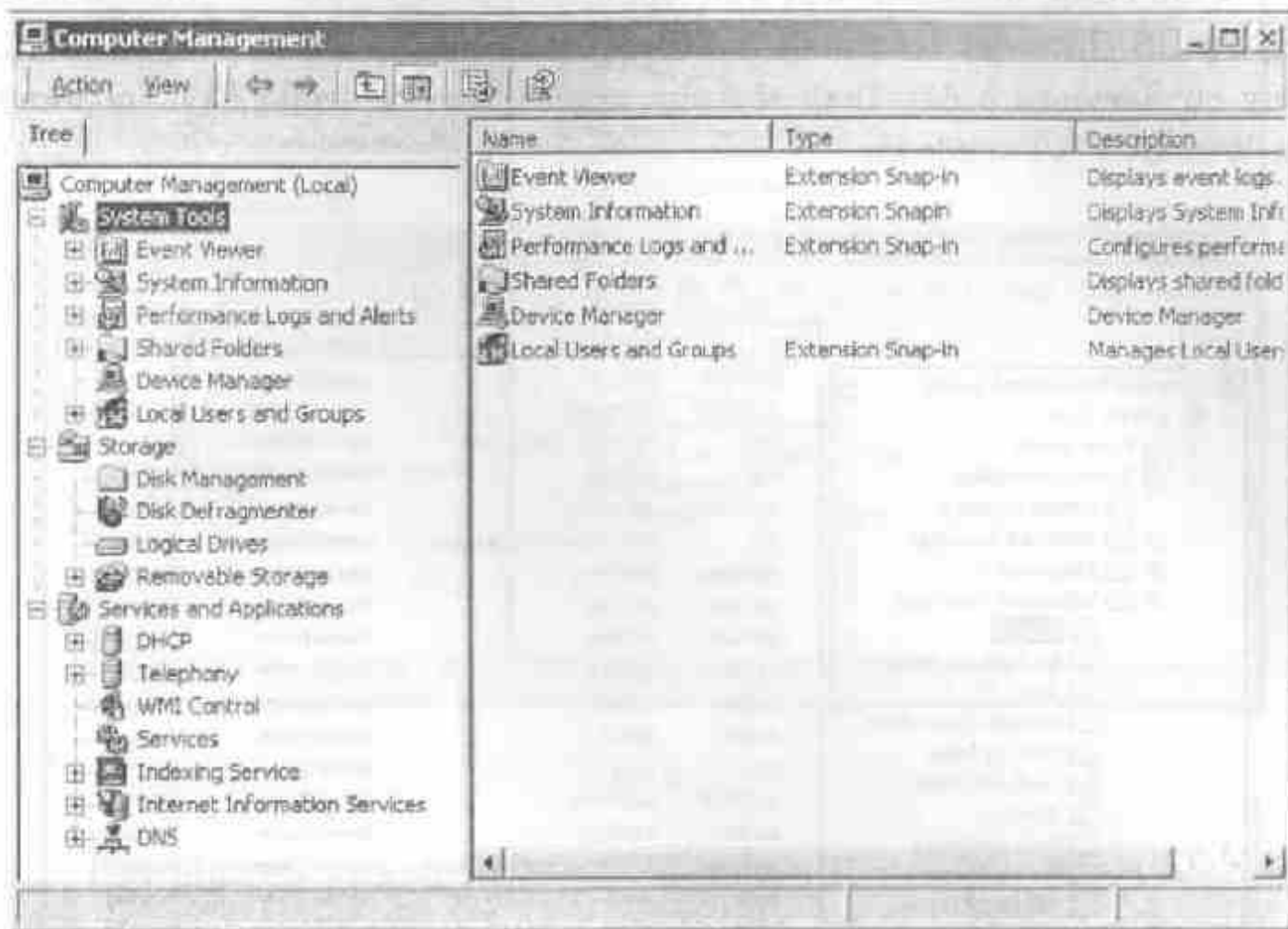
Đây là công cụ quản trị chính của Windows 2000 dùng để quản trị các server tại chỗ hay từ xa. Để mở cửa sổ chính của công cụ này ta chọn **Administrative Tools / Computer Management** hoặc bấm phím phải tại **My Computer/ Manager** (hình 6.12).

Có ba node trong console tree của cửa sổ điều khiển: **System Tools, Storage, Services and Applications**

Hầu hết các chức năng chính của công cụ này đều nằm trong node **System Tools**, với nó ta có thể:

- Xem các sự cố và quản lý danh bạ Event Logs. Đây là chức năng trước kia của Event Viewer được chuyển thành một snap-in MMC. Riêng

các dịch vụ DNS và Directory Service đã có các danh bạ ghi chép riêng của chúng.



Hình 6.12

- Xem các thông tin hệ thống. Mục chọn **System Information** sẽ cung cấp các thông tin chi tiết về tài nguyên phần cứng, về cấu hình các thành phần hệ thống và các chương trình ứng dụng cũng như hoạt động của hệ điều hành.

- Tiến hành các thao tác với các thư mục dùng chung như: xem, tạo các thư mục dùng chung, quan sát các phiên truy cập và các tập tin đang được mở, cắt đứt các phiên truy cập nếu cần... Đây là chức năng của applet Server trong Control Panel trước kia.

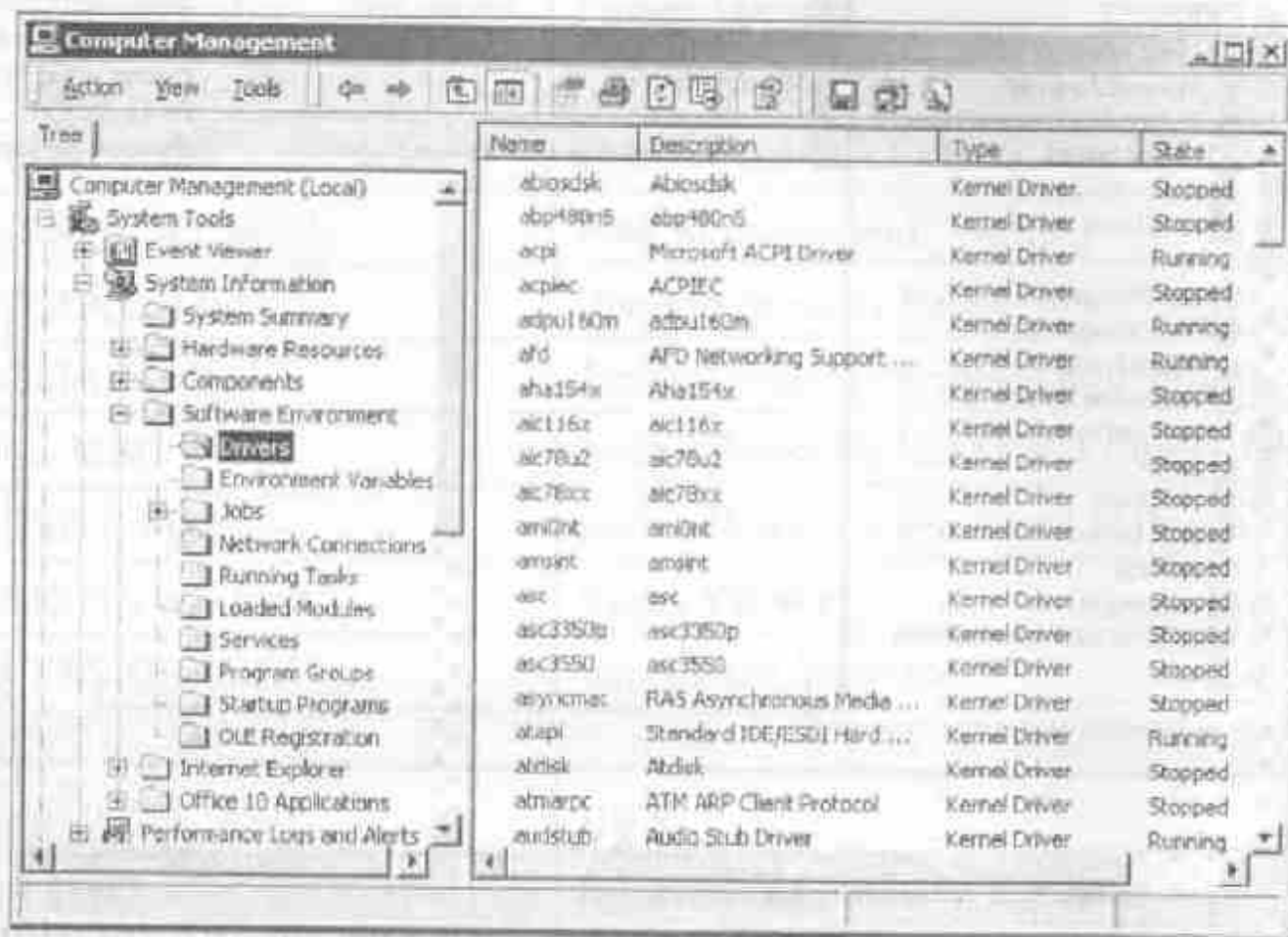
- Quản lí các thiết bị phân cứng tại chỗ hay từ xa. Ta có thể theo dõi những thông tin về phần cứng, giải quyết xung đột về tài nguyên máy.

- Cuối cùng và hết sức quan trọng là chức năng tạo và quản lí tài khoản người dùng, tài khoản nhóm tại chỗ.

Với node **Storage** ta có thể quản lí các thiết bị lưu trữ ở xa với công

cụ Disk Defragmenter và Disk Management. Tại đây ta có thể xem các ổ đĩa logic, các ảnh xạ ổ đĩa mạng, xác định dung lượng đĩa còn trống...

Cuối cùng, node Services and Applications bao gồm các mục chọn về dịch vụ IIS (Internet Information Server), dịch vụ lập chỉ mục (Indexing)... Công cụ Services ở đây thay thế cho applet Service trong Control Panel của Windows NT trước kia.

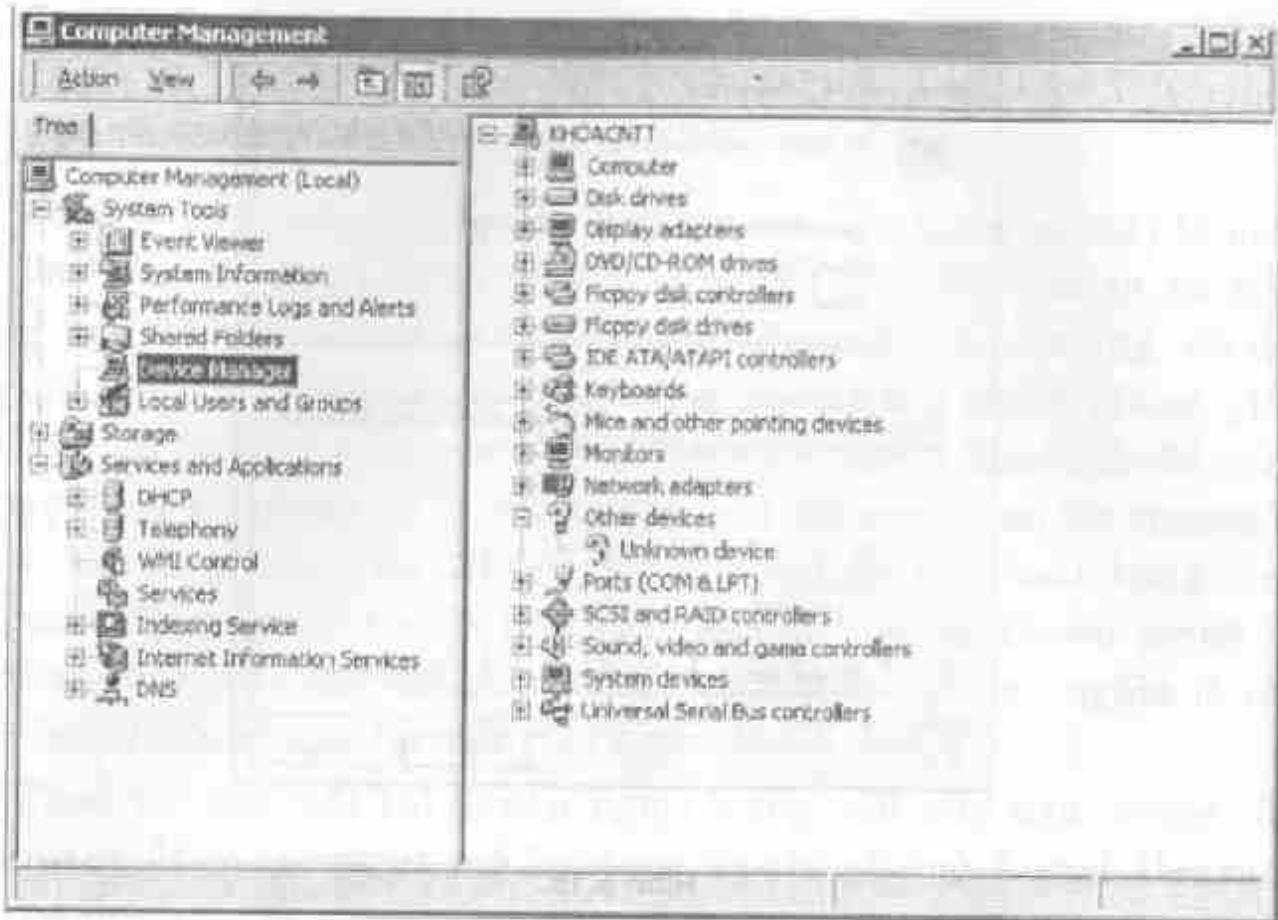


Hình 6.13

3.3. Quản lí các thiết bị phần cứng bằng Device Manager

Tại cửa sổ Device Manager có bốn cách quan sát cấu hình thiết bị của máy

- View Devices by Type: xem danh sách thiết bị theo từng loại
- View Devices by Connection: xem danh sách thiết bị theo tình trạng kết nối hiện thời.
- View Resource by Type: xem danh sách phân loại tài nguyên
- View Resource by Connection: xem danh sách tài nguyên theo tình trạng kết nối hiện thời.



Hình 6.14

Hai phương pháp cuối chính là điểm cải tiến của Windows 2000. Trước kia, với Windows NT và Win 9x, nếu muốn biết IRQ 5 đang được chiếm dụng bởi thiết bị nào thì phải tìm vào properties của từng thiết bị hoặc dùng một phần mềm chuyên dụng kiểu như MSD hay QAPLus, PCCheck... Nay thì với chế độ **View Resource by** ta có thể thấy danh sách các tài nguyên máy cùng với các thiết bị đang sử dụng những tài nguyên ấy.

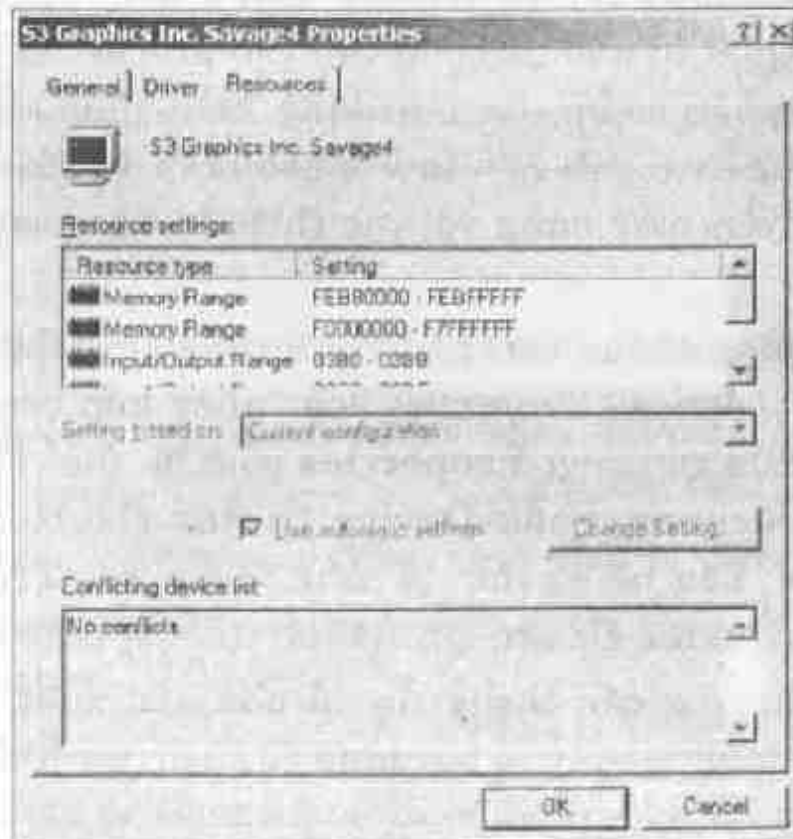
Để xem những thông tin chi tiết về từng thiết bị: *chọn thiết bị đó trong danh sách (Action/ Properties* hoặc nhấp kép vào thiết bị đó ngay tại danh sách. Hiện ra trang **Properties** gồm ba thẻ. Thẻ **General** cung cấp các thông tin chung. Phần **Device Status** cho biết tình trạng hoạt động của thiết bị, nếu nó có vấn đề có thể bấm nút **Troubleshooter** để giải quyết. Phần **Device Usage** quyết định thiết bị được sử dụng khi nào.

Thẻ **Driver** cung cấp thông tin về nhà sản xuất, phiên bản... của Driver. Nút Uninstall tại đây có tác dụng gỡ bỏ driver khỏi hệ thống.



Hình 6.15

Thẻ **Resource** chứa thông tin về cấu hình hiện tại (IRQ, địa chỉ I/O...) của thiết bị. Nếu có một số thiết bị đang tranh chấp tài nguyên ta có thể quan sát chúng trong mục **Conflicting device list** (hình 6.16).



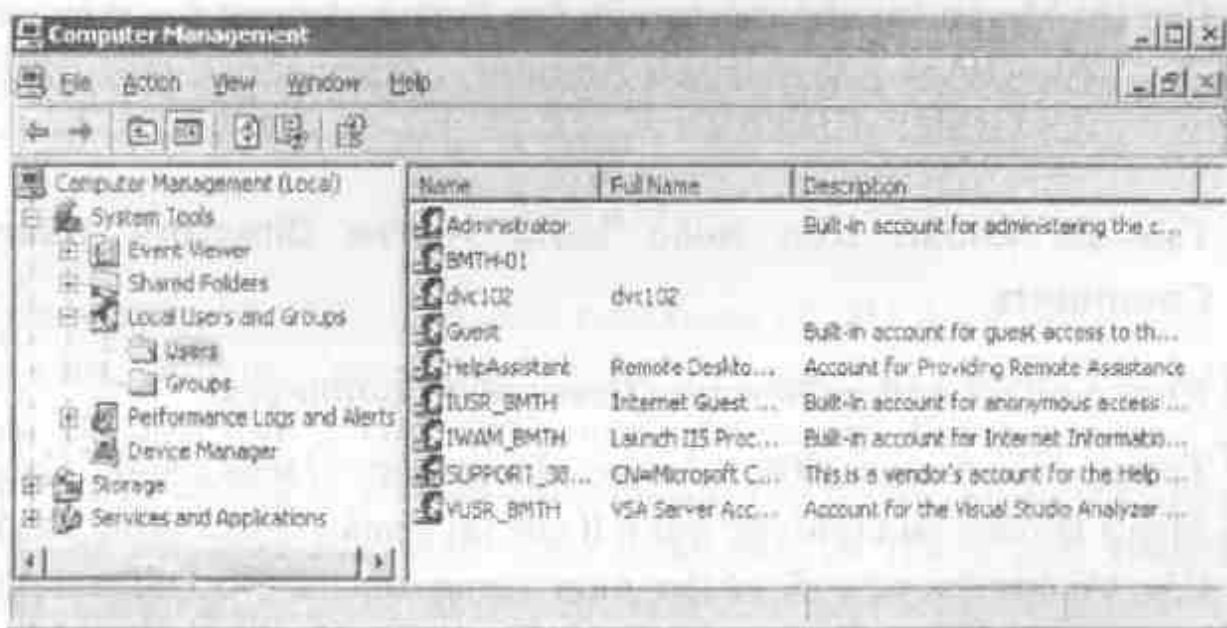
Hình 6.16

4. QUẢN LÝ CÁC TÀI KHOẢN NGƯỜI DÙNG

4.1. Tạo và quản lý các tài khoản tại chỗ

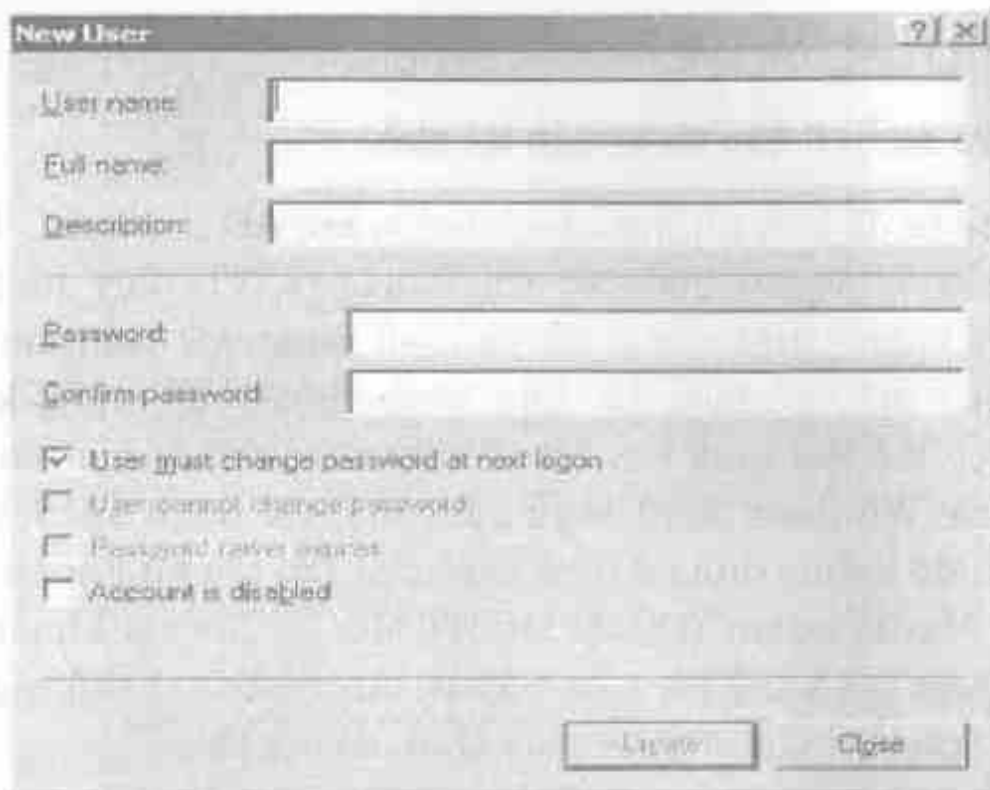
Chúng ta đã biết những lợi ích to lớn mà AD mang lại, đây là một cải cách lớn của Windows 2000 so với Windows NT. Tuy nhiên có một số trường hợp không thật cần thiết phải sử dụng AD trên mạng, đó là khi mạng có quy mô nhỏ hoặc hệ điều hành chính của mạng không phải là Windows (có thể là Linux hay Novell Netware chẳng hạn) mà chỉ một vài máy trạm cài Windows 2000 để sử dụng một vài trình tiện ích chuyên môn nào đó. Khi đó không dùng AD và chúng ta tạo các tài khoản bằng công cụ Computer Management (COMPMGMT.MSC). Các tài khoản người dùng và nhóm được tạo bằng công cụ này là tài khoản tại chỗ, nghĩa là chúng chỉ có hiệu lực trên chính chiếc máy trạm đó mà thôi.

Thao tác tạo một tài khoản người dùng mới như sau: trong cửa sổ Computer Management mở System Tools rồi mở Local Users and Groups (hình 6.17).



Hình 6.17

Mở thư mục **Users**, chọn menu **Action/NewUser**. Sau đó điền vào các mục **User Name** (tên người dùng), **Password** (mật khẩu), **Confirm Password** (gõ nhắc lại mật khẩu) cuối cùng bấm nút **Create**. Nếu muốn kiểm tra các thông tin trong một tài khoản, thay đổi một vài mục, đưa tài khoản đó gia nhập một nhóm khác... ta bấm phím phải vào tài khoản đó rồi chọn **Properties**. Để ấn định mật khẩu cho một tài khoản, cũng bấm phím phải và chọn **Set Password**.



Hình 6.18

Các tài khoản tại chỗ mà ta vừa tạo được lưu ngay tại máy, trong cơ sở dữ liệu SAM (Security Account Manager) tại thư mục `\WINNT\SYSTEM32\CONFIG`

4.2. Tạo tài khoản trên miền bằng Active Directory Users and Computers

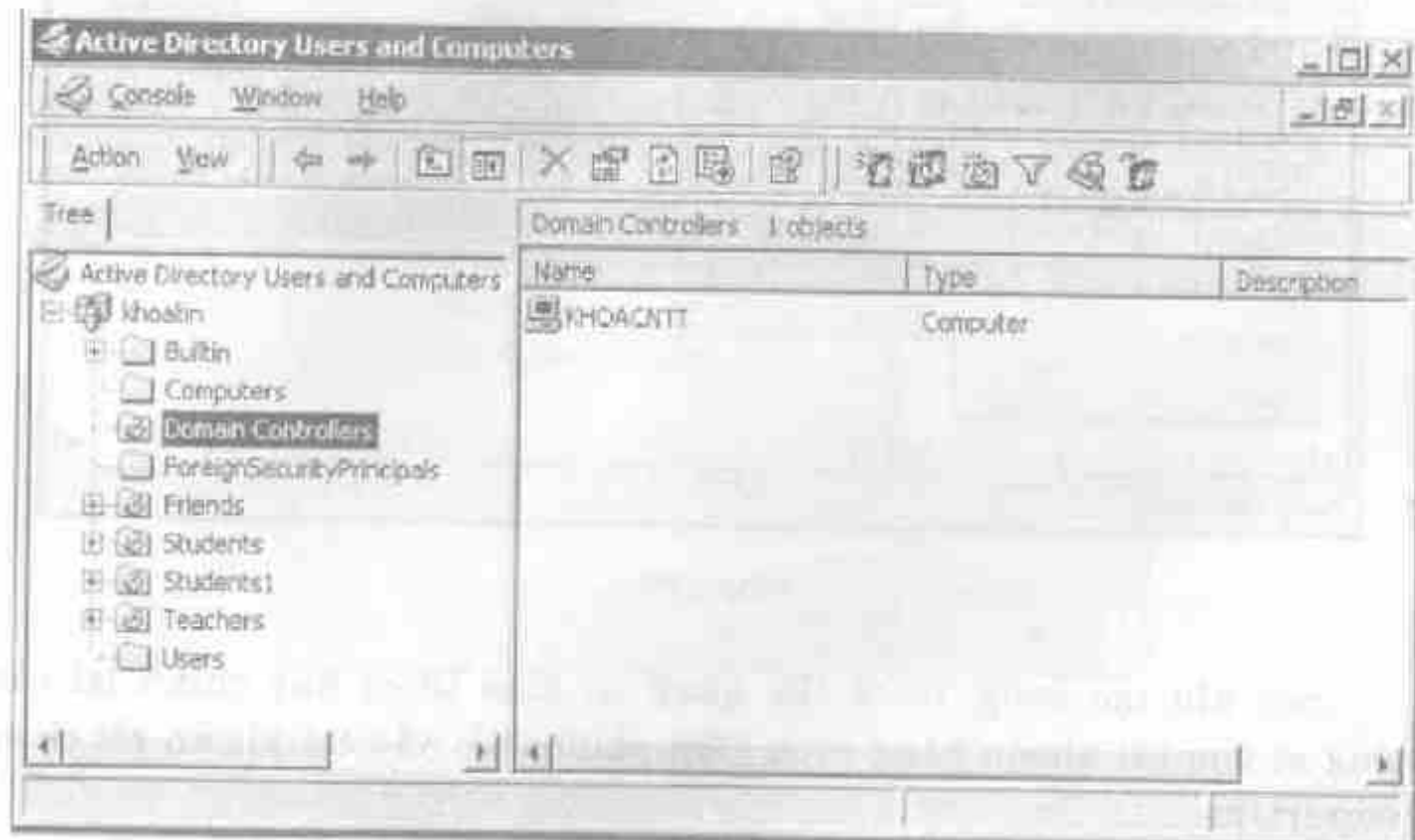
4.2.1. Khái quát về Active Directory Users and Computers

Trong Windows 2000, Active Directory Users and Computers (DSA.MSC) là công cụ chính để quản lý các tài khoản người dùng, nhóm, đơn vị ... Các tài khoản này dĩ nhiên nằm trong tệp NTDS.DIT tại thư mục `%systemroot%\NTDS` của máy Domain Controller và được nhân bản thành nhiều bản sao đặt trên các server. Công cụ Active Directory Users and Computers cung cấp cho người quản trị mạng những khả năng sau đây:

- Tạo mới, sửa đổi, xóa bỏ các tài khoản người dùng.
- Xây dựng kịch bản đăng nhập (login script) cho tài khoản người dùng.
- Quản lý các nhóm
- Xây dựng và quản lý các chính sách nhóm.

Trước hết chúng ta khởi động Active Directory Users and Computers bằng cách gõ thẳng tên tệp DSA.MSC từ Start/Run, hoặc thông qua

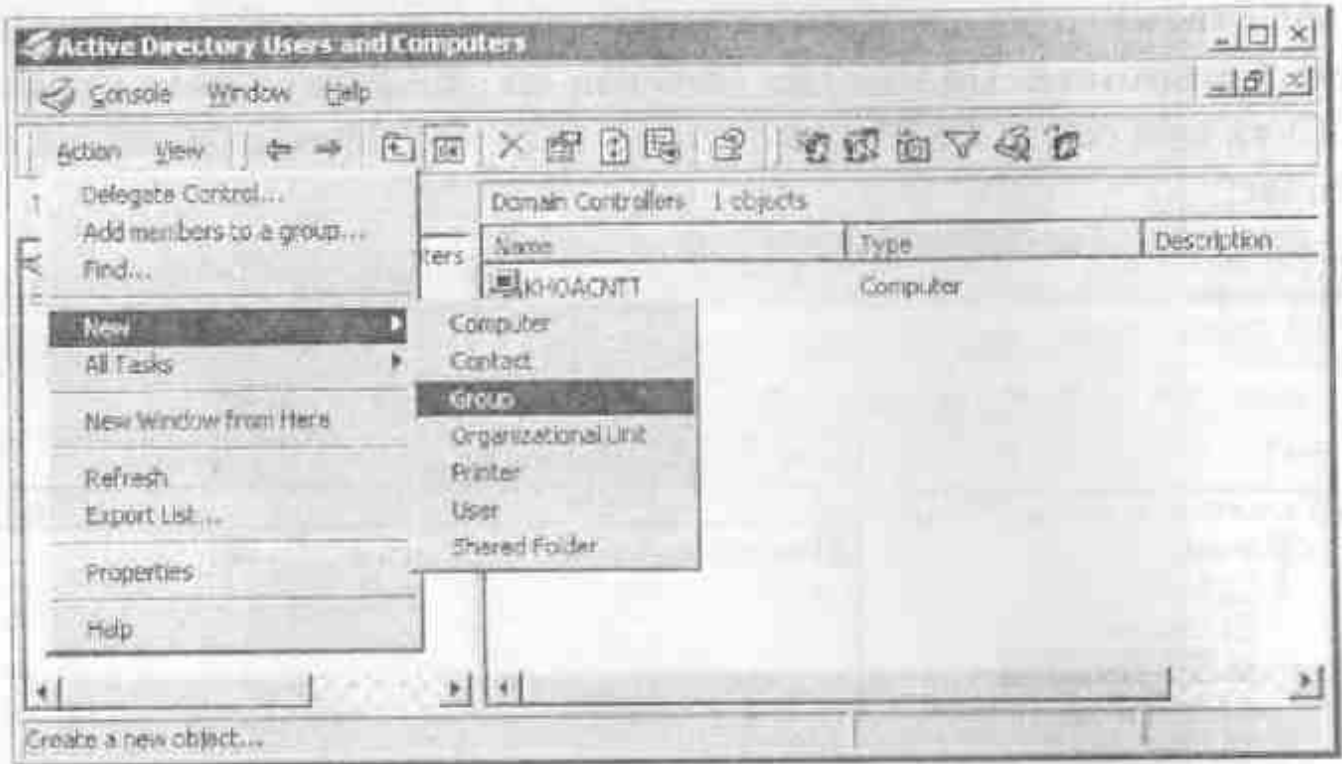
menu **Start/Programs /Administrative Tools/Active Directory Users and Computers**. DSA sẽ tìm cách liên lạc với máy Domain Controller (DC) và trên cửa sổ DSA ta sẽ quan sát thấy tên của máy DC mà nó đang liên lạc.



Hình 6.19

Trong ngăn bên trái là một số container và OU được tạo ra một cách tự động như **Builtin**, **Computers**, **Domain Controllers**... cũng như các OU được tạo ra theo chủ ý của người quản trị mạng. Các container **User**, **Computers** là những vị trí mặc định để đặt các tài khoản người dùng, tài khoản nhóm và máy khi máy được nâng cấp từ NT 4 lên. **Builtin** là container dành cho các local group được tạo sẵn như **Administrators**, **Account Operators**, **Guest**... **Domain Controllers** là OU mặc định dành cho máy DC để chứa tài khoản máy đó. **ForeignSecurityPrincipals** là container mặc định dành cho các tài khoản thuộc các miền bên ngoài được ủy quyền.

Để tạo mới một tài khoản người sử dụng, tài khoản máy, nhóm hay đơn vị (OU)... ta chọn đối tượng chứa container chứa tài khoản sắp tạo, chọn menu **Action /New** rồi chọn loại tài khoản mình cần.

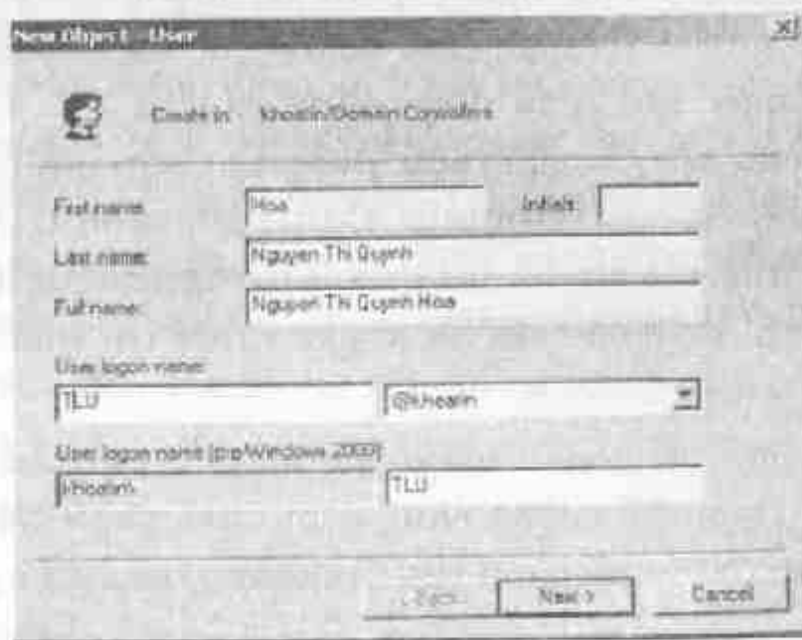


Hình 6.20

Sau khi tạo xong, ta có thể quay lại điền thêm hay chỉnh lại các thông số của tài khoản bằng cách bấm phím phải vào tài khoản rồi chọn **Properties**.

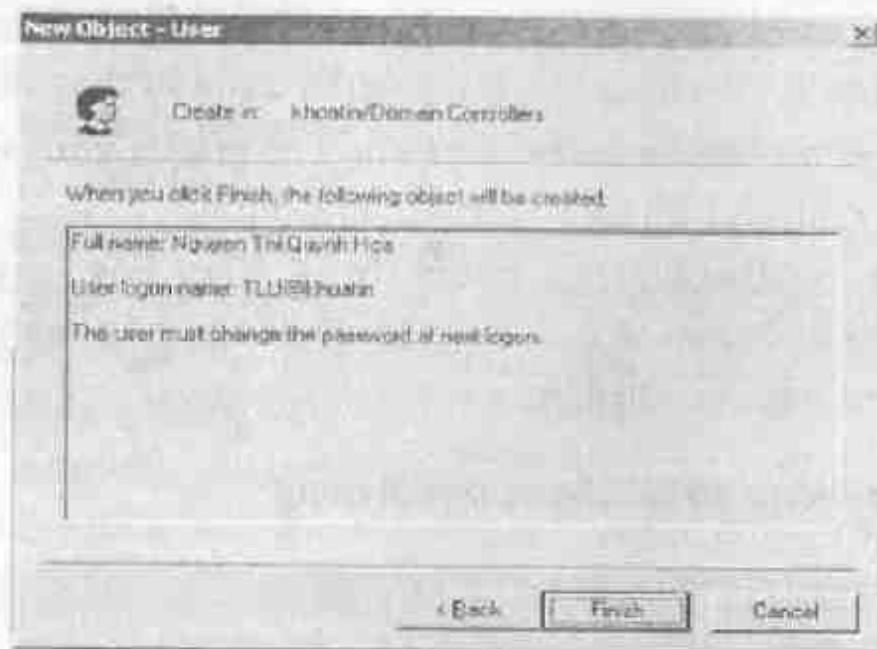
4.2.2. Tạo một tài khoản người dùng mới

Tại cửa sổ DSA.MSC ta chọn container sẽ chứa tài khoản người dùng sắp tạo, thông thường là container User, chọn menu Action/User. Một wizard sẽ xuất hiện để hướng dẫn ta từng bước.



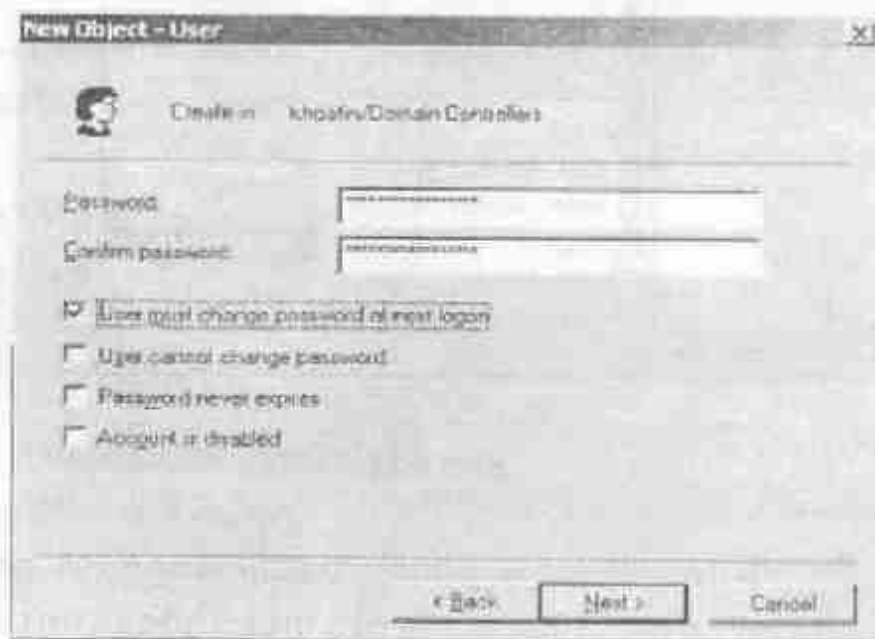
Hình 6.21

Ta phải điền vào Tên (first name), họ (last name), tên đầy đủ (full name), các mẫu viết tắt của tên (initials), tên dùng khi đăng nhập (User logon name), hậu tố UPN (User Principal Name) để nối vào đuôi username lúc đăng nhập.



Hình 6.22

Hậu tố UPN thường là tên DNS của miền. Chú ý rằng các username trong Windows 2000 phải là duy nhất trên từng máy, không được trùng với tên nhóm tại chỗ, có thể dài đến 20 kí tự và có thể chứa dấu cách, dấu chấm nhưng nên tránh các dấu cách vì khi đưa vào script phải bao chúng trong cặp nháy kép "".



Hình 6.23

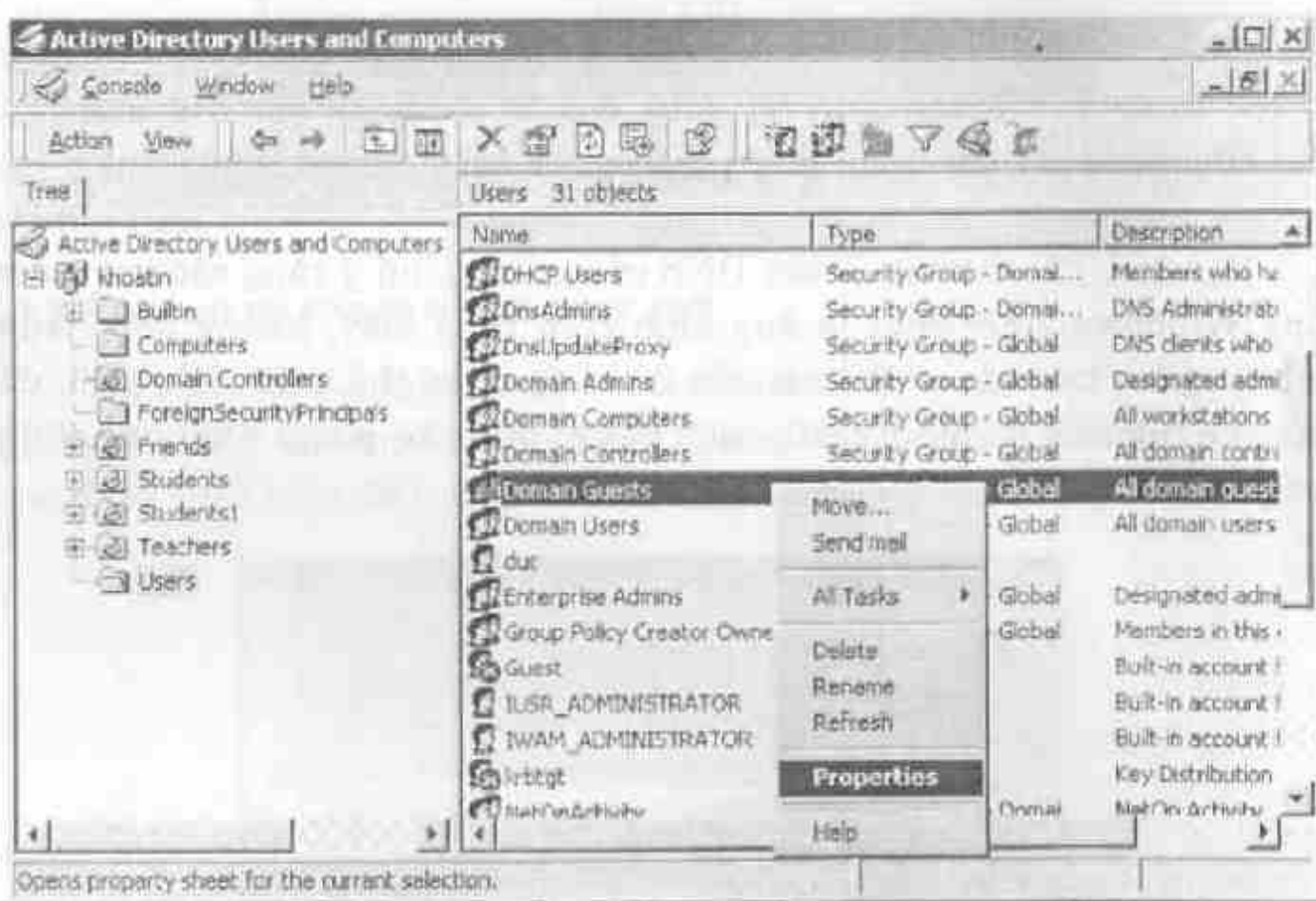
Bước tiếp theo ta chọn Next rồi gõ mật khẩu cho tài khoản

Ý nghĩa các mục đánh dấu:

- **User must change password at next logon:** trong lần đăng nhập đầu tiên người dùng phải tự ấn định lại mật khẩu cho mình.
- **User cannot change password:** mục chọn này thường dùng cho các tài khoản dùng chung, nó không cho phép người dùng tự thay đổi mật khẩu.
- **Password never expires:** mật khẩu có giá trị vĩnh viễn, bất chấp các chính sách quy định thời gian hết hạn mật khẩu.
- **Account is disable:** tài khoản bị vô hiệu hóa, tuy vẫn tồn tại trong SAM nhưng không ai có thể dùng nó để đăng nhập mạng.

Cuối cùng ta bấm nút Finish

4.2.3. Quản lí các thông số tài khoản người dùng



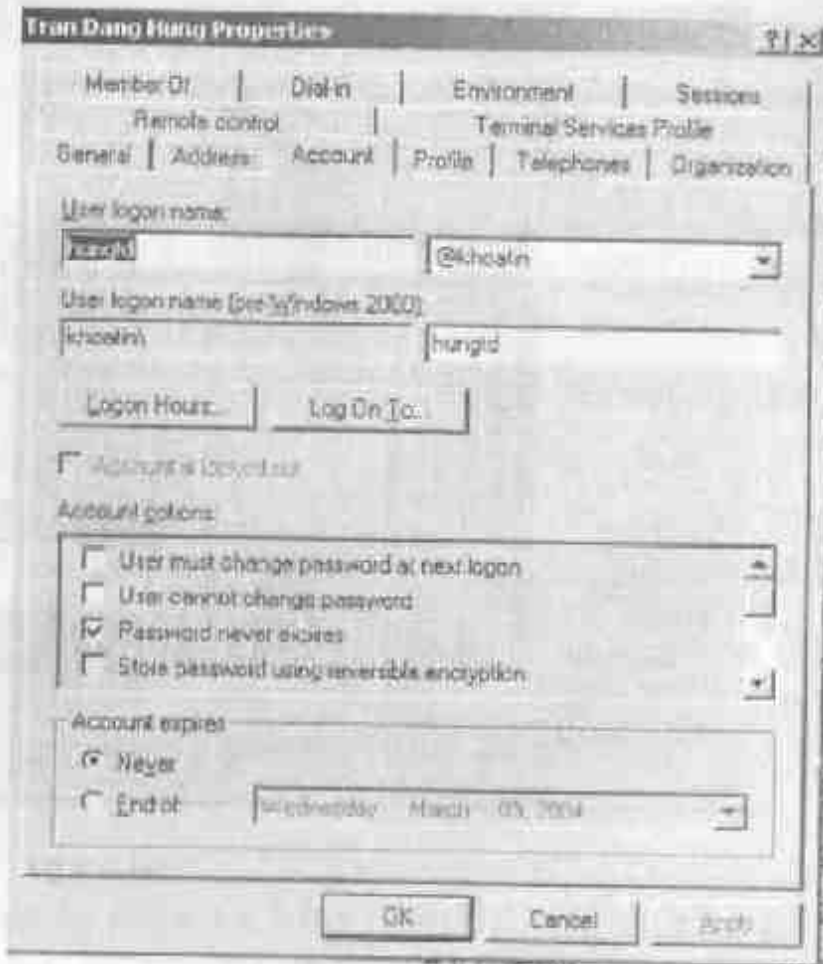
Hình 6.24

Ngoài nhiệm vụ tạo mới tài khoản người dùng, có những lúc người quản trị mạng phải giám sát, cập nhật các mục thông tin trong tài khoản.

Trong cửa sổ Active Directory Users and Computers bấm phím

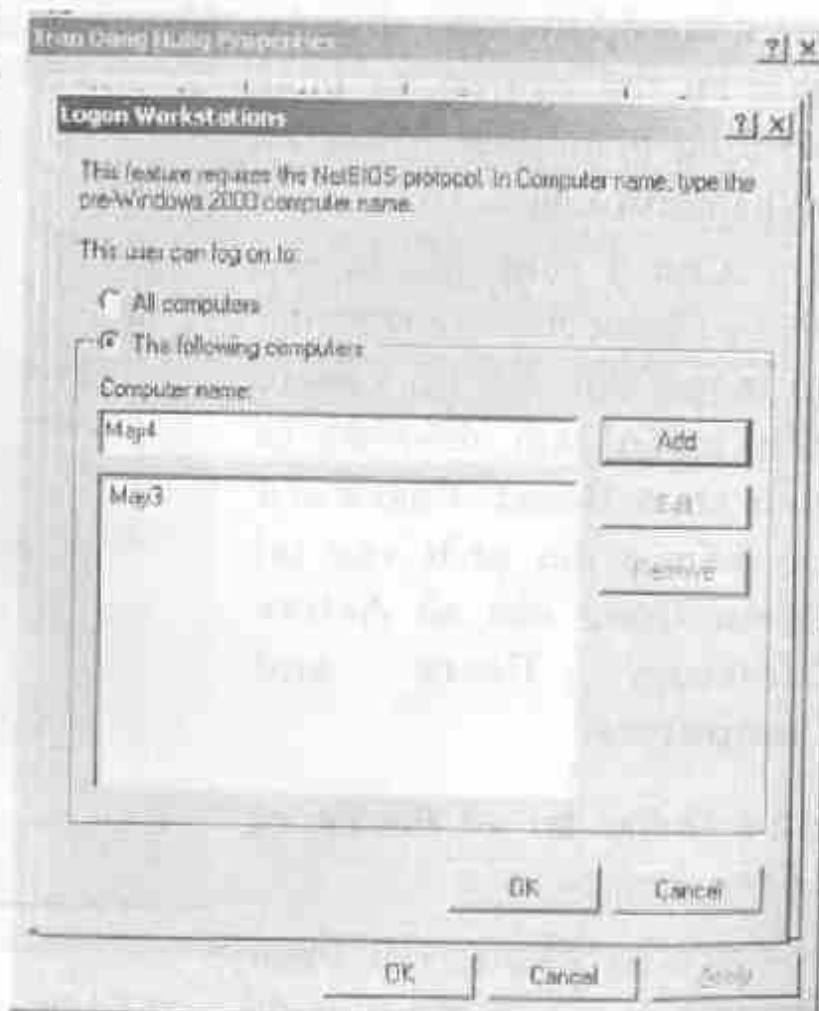
phải tại tài khoản cần xét, chọn **Properties**. Khung hội thoại **Properties** sẽ hiện ra như sau

Có rất nhiều mục thông tin ứng với các thẻ, tại đây chúng ta chỉ xét một số mục quan trọng nhất. Thẻ **General** là thông tin về văn phòng làm việc, số điện thoại, địa chỉ E-mail và Home Page ... của người có tài khoản đang xét. Thẻ **Address** cung cấp các loại địa chỉ. Ta hãy quan sát thẻ **Account**

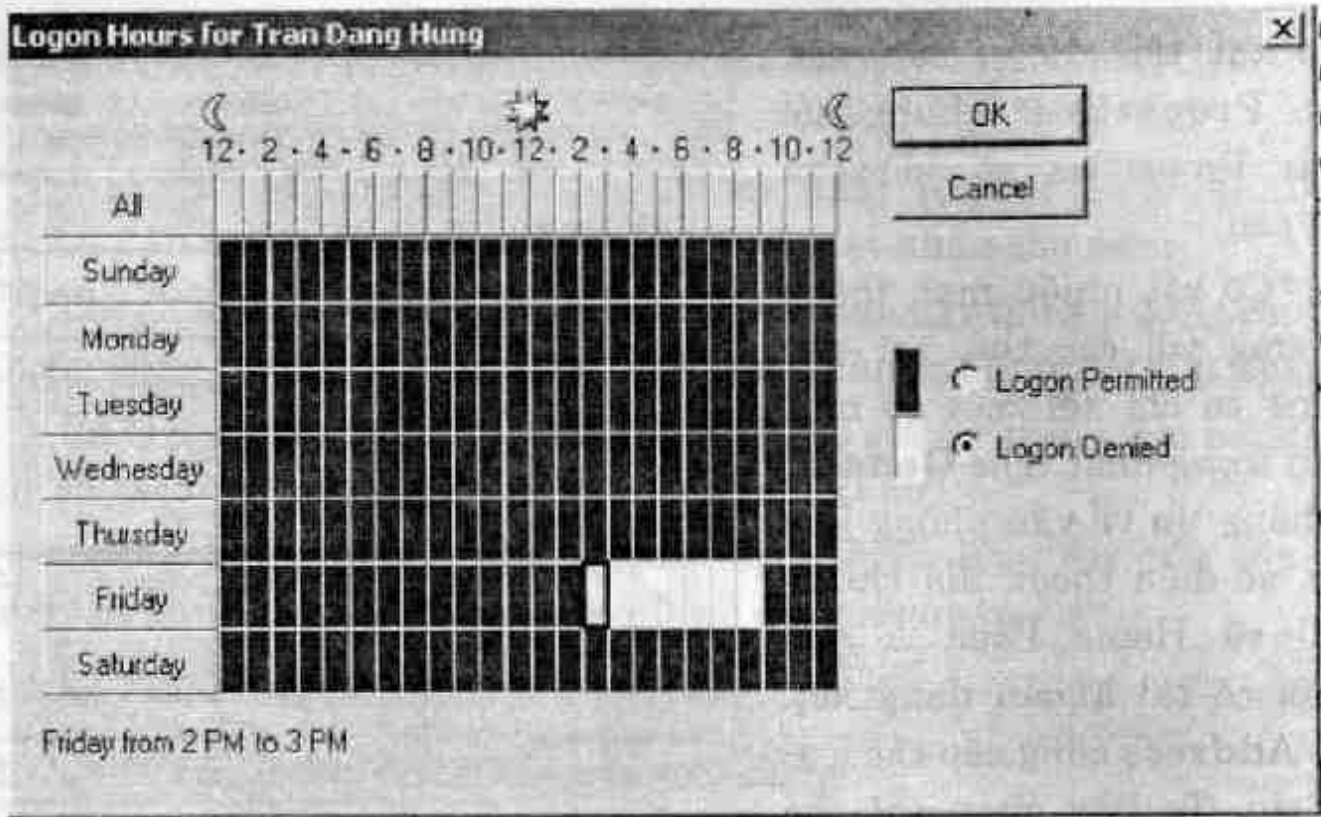


Hình 6.25

Tại đây ta có thể sửa đổi Tên đăng nhập (logon name), giới hạn khoảng thời gian được phép đăng nhập mạng (bấm vào nút **Logon Hours**) ... Chế độ mặc định là người dùng sẽ không bị trục xuất khỏi mạng khi hết giờ đăng nhập, nếu muốn hệ thống tự động làm điều đó ta phải vào snap-in **Group Policy**, dưới **Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options** rồi chọn chế độ **Automatically Log Off Users When Logon Hour Expire**.



Hình 6.26



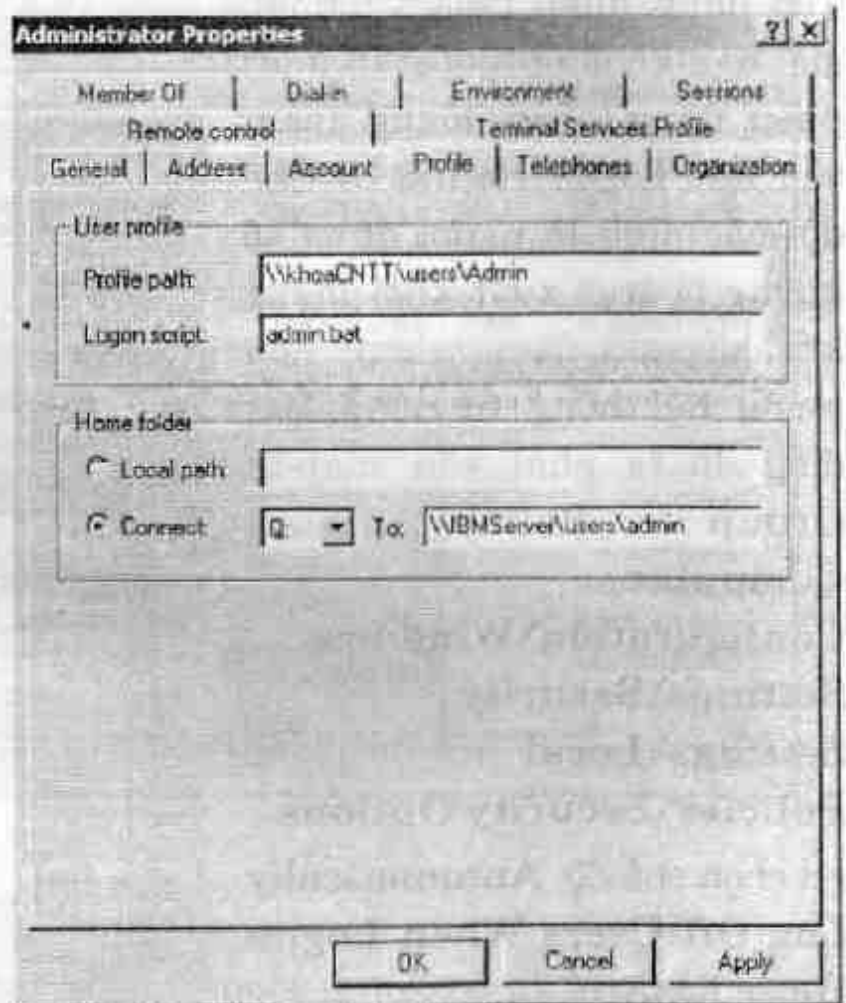
Hình 6.27

Nếu muốn quy định người sử dụng chỉ được đăng nhập mạng từ một số máy trạm cụ thể nào đó, ta phải sử dụng giao thức NetBIOS rồi bấm nút Logon To.

Chú ý rằng tại đây ta không có lựa chọn để thay đổi lại mật khẩu của tài khoản. Nếu muốn làm điều đó ta phải chọn **Reset Password** khi bấm phím phải vào tài khoản trong cửa sổ **Active Directory Users and Computers**.

4.2.4. Thông tin về Profile và Logon Script

Trong khung hội thoại Properties còn có các mục để



Hình 6.28

ta ấn định Profile, Logon Script và Home Folder. Chú ý rằng sự có mặt của các công cụ này chỉ nhằm tương thích với Windows NT và 9x, còn Windows 2000 đã có công cụ mới hơn là Group Policy.

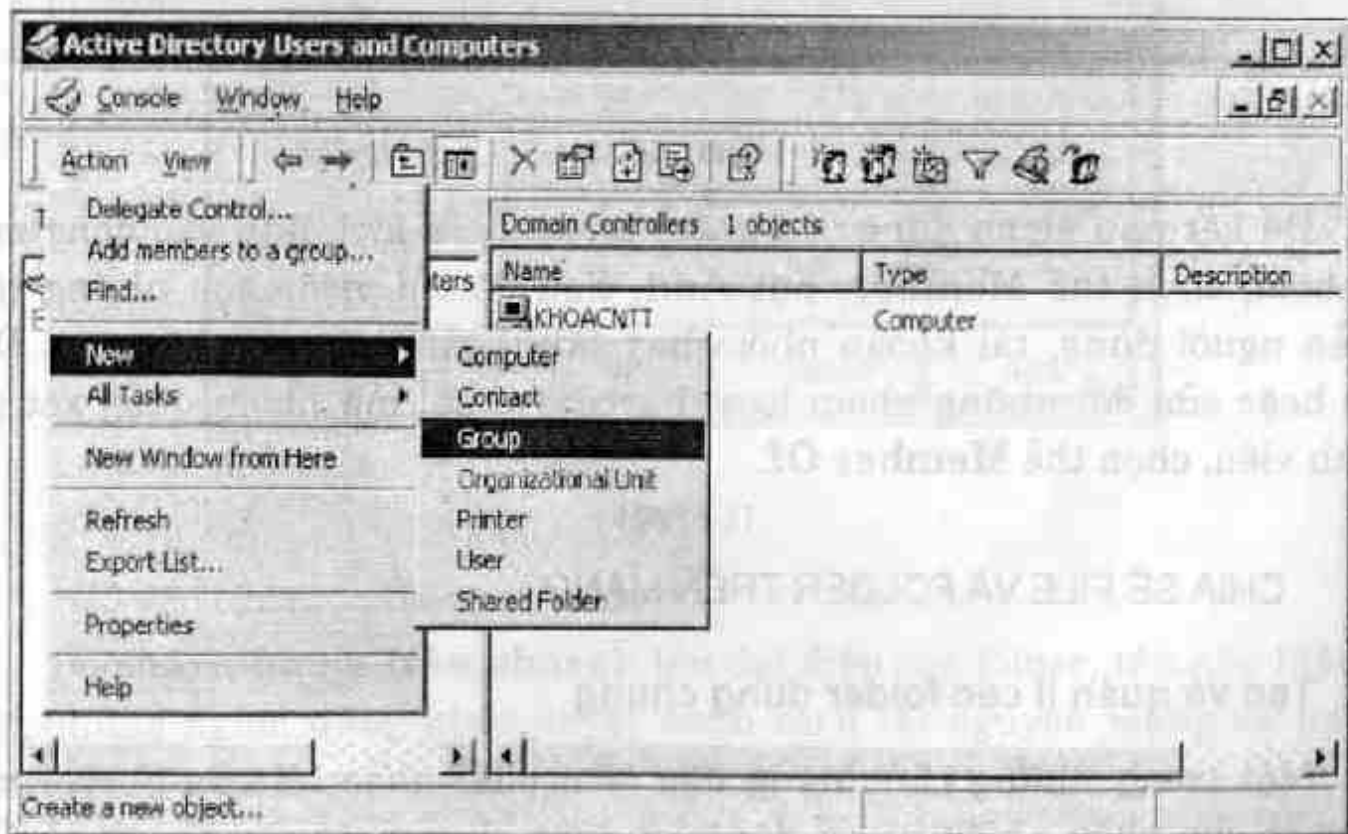
User Profile (biên dạng người dùng) là tập hợp các lựa chọn về giao diện màn hình của người dùng như nội dung của menu Start, các thiết lập về mouse, màu sắc màn hình và cửa sổ... ấn định sao cho người dùng dù đăng nhập mạng từ bất kì máy trạm nào cũng vẫn có một môi trường làm việc như nhau.

Login hay **Logon Script** là một kịch bản được kích hoạt vào lúc người dùng đăng nhập mạng nhằm thiết lập môi trường làm việc và cấp phát các tài nguyên mạng cho người đó.

Home folder, còn gọi là home directory (thư mục cơ sở), là thư mục được cấp cho một người dùng để anh ta sử dụng vào mục đích riêng.

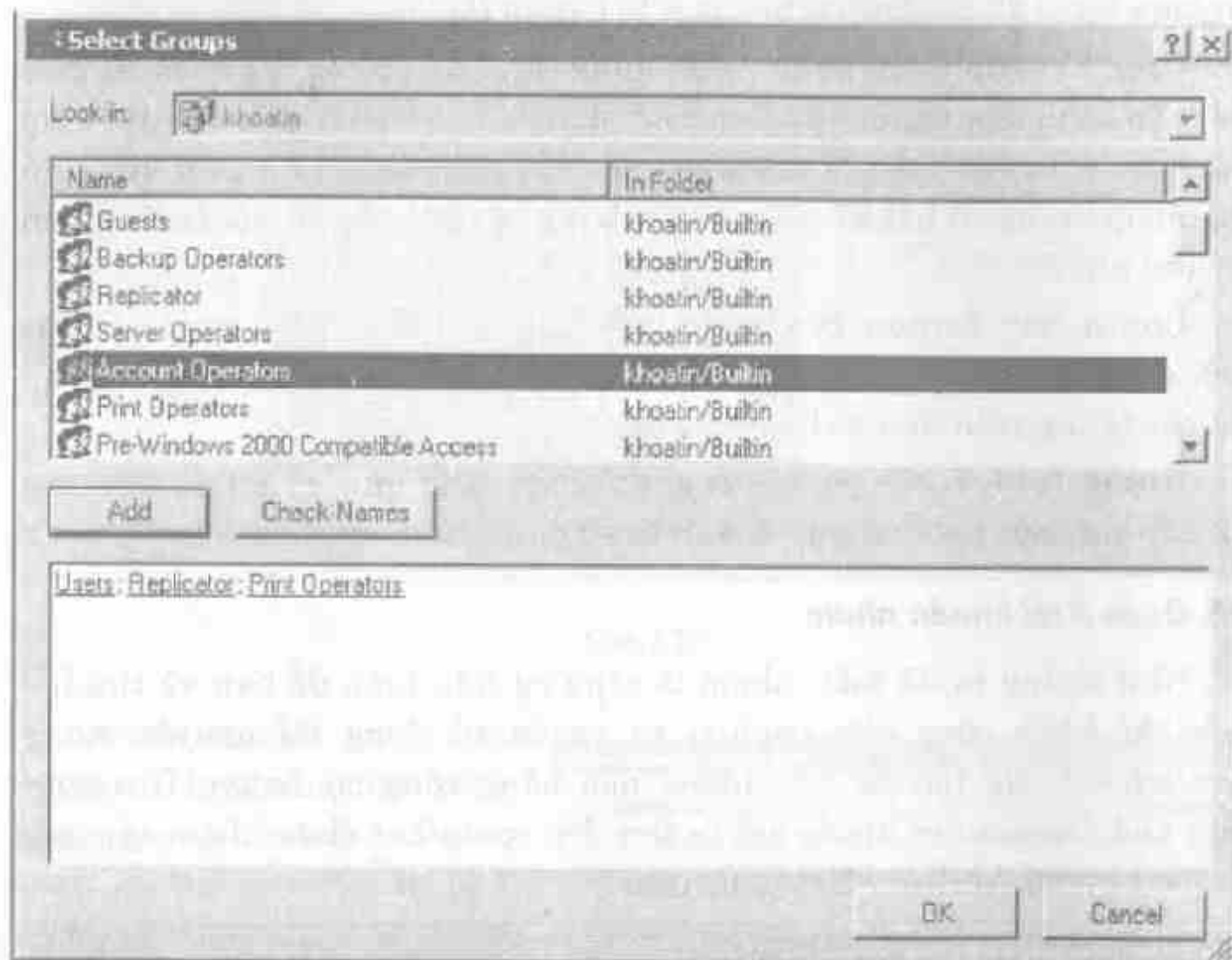
4.2.5. Quản lí tài khoản nhóm

Như chúng ta đã biết, nhóm là công cụ hữu hiệu để ban và thu hồi quyền thi hành công việc (*rights*) và quyền sử dụng tài nguyên mạng (*permissions*). Để tạo ra một nhóm mới bằng công cụ Active Directory Users and Computers, trước hết ta tìm đến container chứa nhóm sắp tạo, kích hoạt menu **Action / New / Group**



Hình 6.29

Trong hộp thoại **New Object** ta gõ tên nhóm (Group name), phạm vi của nhóm (group scope), kiểu nhóm (group tipe)



Hình 6.30

Để kết nạp người dùng vào nhóm mới tạo, ta kích đúp vào dòng mô tả nhóm, chọn thẻ **Member**, nút **Add**. Sau đó chỉ việc chọn những tài khoản người dùng, tài khoản nhóm hay tài khoản máy cần kết nạp. Để xem hoặc sửa đổi những nhóm local hay universal mà nhóm đang xét là thành viên, chọn thẻ **Member Of**.

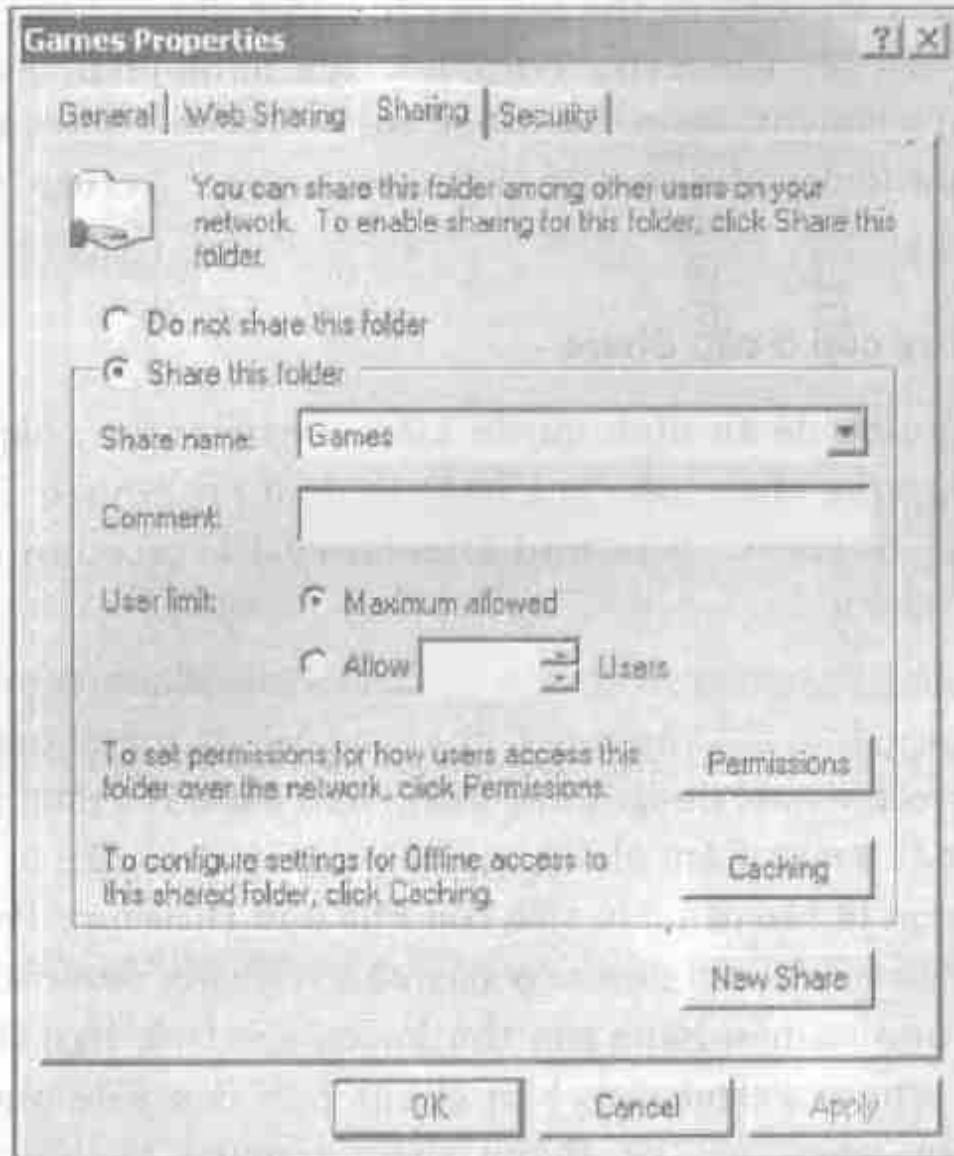
5. CHIA SẺ FILE VÀ FOLDER TRÊN MẠNG

5.1. Tạo và quản lí các folder dùng chung

Một trong những chức năng đầu tiên phải nhắc tới của Server và mạng là cho phép nhiều người dùng sử dụng chung các tập tin từ nhiều máy trạm khác nhau, nói cách khác là chia sẻ (sharing) các folder trên

mạng. Khi ta chia sẻ một folder A trên mạng cho những người dùng khác, họ phải ánh xạ folder A thành một ổ đĩa logic (ta gọi chung là một share) mỗi trên máy trạm của mình và thiết lập một mối liên kết (connection) giữa ổ đĩa logic đó với folder A trên máy của ta. Để chia sẻ folder ta làm như sau:

Trong cửa sổ **Explorer**, bấm phím phải vào folder định chia sẻ, chọn **Sharing /Share this folder**



Hình 6.31

Gõ vào các mục thông tin sau:

- **Share name (tên share):** tên đại diện cho folder, tên này hiện ra khi những người dùng khác duyệt danh sách tài nguyên mạng và họ chỉ làm việc với tên này chứ không cần biết đến tên thật của folder.
- **Comment:** lời mô tả, dòng giải thích về folder.
- **Permissions:** quy định quyền truy cập đối với folder này. Trong đó

nút **Caching** (đệm lưu trữ) cho phép những người dùng khác truy cập folder này (thực ra là một bản sao từ trước) ngay cả khi họ không đăng nhập vào mạng.

- **New Share:** tạo tiếp một folder dùng chung (share) khác.
- **User limit:** quy định tối đa bao nhiêu người dùng có thể đồng thời kết nối vào folder. Con số này được đặt ra trên cơ sở giấy phép (license) hiện có đang cho phép tối đa bao nhiêu truy cập đồng thời.

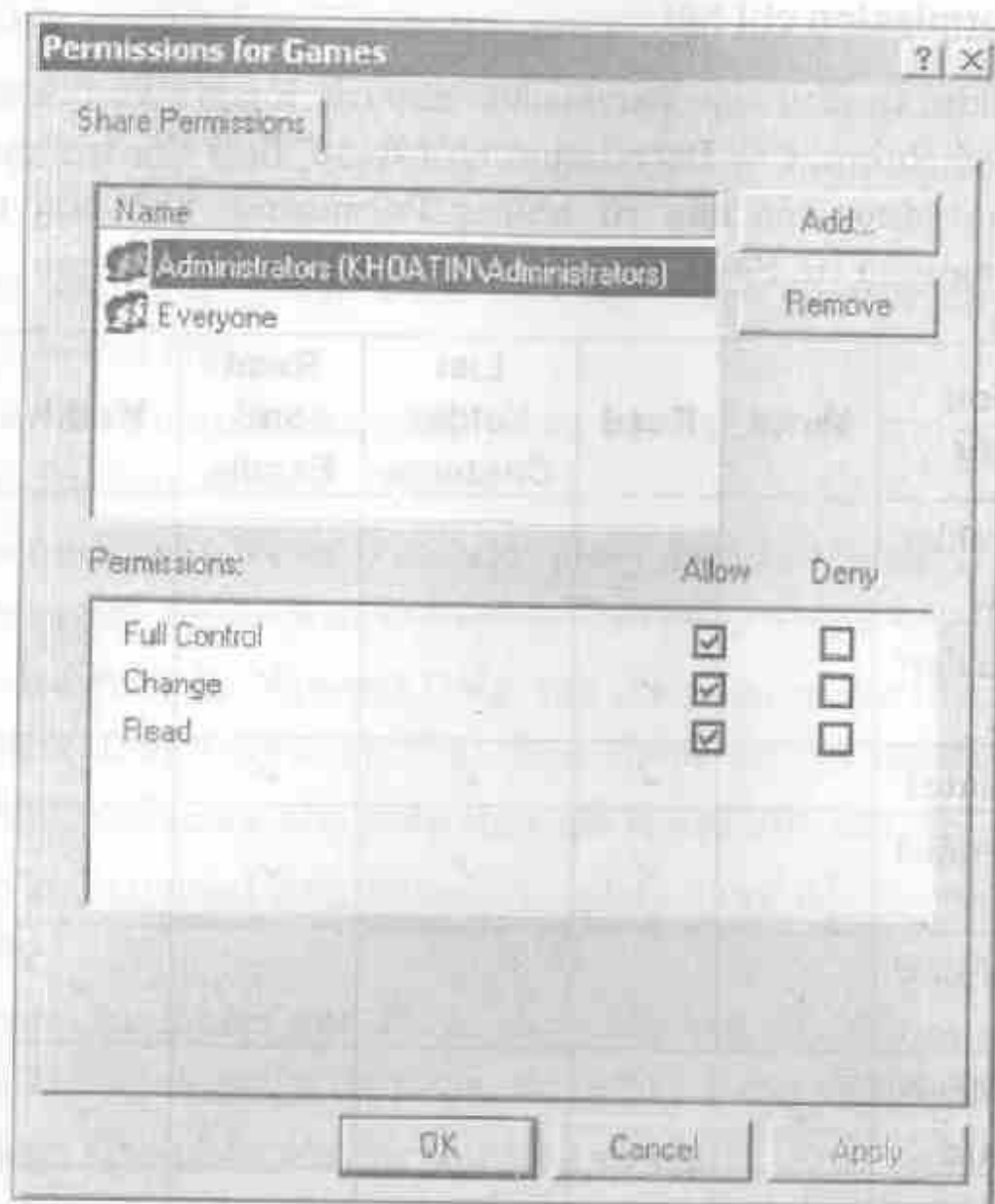
Người quản trị cũng có thể tạo ra các folder dùng chung từ xa bằng công cụ Computer Management. Trước hết bấm phím phải vào biểu tượng Computer Management, chọn **Connect to Another Computer**, gõ vào tên server chứa folder cần chia sẻ. Kích hoạt menu **Action / New File Share**.

5.2. Quyền truy cập ở cấp Share

Có nhiều cách để ấn định quyền kiểm soát việc truy cập các share, trong đó hai phương pháp hiệu quả nhất là thiết lập **Share Permission** (quyền truy cập Share) và **File and Directory Permission** (quyền truy cập file và thư mục).

Một folder trên server được ánh xạ thành một share trên máy khách và như vậy share được coi như một ổ đĩa logic đối với máy khách. Như thế thì quyền truy cập ở mức Share cũng giống như cái nút chống ghi trên đĩa mềm, chỉ cần đặt ở mức **Cấm** ghi là mọi cố gắng ghi vào đều bị ngăn chặn. Share Permission là rào cản đầu tiên còn File and Directory Permission là hàng rào tiếp theo. Lớp rào cản đầu tiên này sẽ lấn quyền (override) File and Directory Permission nếu hàng rào thứ hai này ít tính hạn chế hơn. Nói chung nên để Share Permission hạn chế ít hơn mọi File and Directory Permission bên trong nó, và thông thường người ta hay đặt Share Permission sao cho mọi người đều có đầy đủ quyền truy cập để đơn giản hóa việc quản lý share đó đồng thời kiểm soát việc truy cập share thông qua lớp rào chắn: File and Directory Permission.

Thao tác quy định Share Permission như sau: trong cửa sổ **Computer Management**, chọn share cần bảo vệ, bấm nút phải chuột, chọn **Properties**. Nếu ngồi tại server, ta kích hoạt **Explorer**, bấm nút phải chuột vào folder chia sẻ, chọn **Sharing / Share Permissions**.



Hình 6.32

Khung **Name** liệt kê những người dùng và nhóm được quyền truy cập share đó ở các mức độ khác nhau được liệt kê trong khung **Permission** bên dưới. Có ba mức độ truy cập

Full Control: được phép thực hiện tất cả mọi công việc trên các file và folder trong share. (Chú ý rằng điều này còn phải phụ thuộc vào các File and Directory Permission bên trong nữa, nếu rào cản bên trong đó cấm thì quyền Full Control cũng vô hiệu)

Change: có quyền đọc, thực hiện chương trình, thay đổi cập nhật và xóa các file và folder trong share.

Read: được phép đọc và thực hiện chương trình nhưng không được phép thay đổi hay xóa gì bên trong share.

5.3. Các Permission chi tiết

Trước khi ấn định các Permission cho các tập tin và folder chúng ta cần hiểu rõ về chúng. Các Permission như Read, Full Control mà chúng ta vừa ban phát được tạo nên từ những Permission nhỏ hơn tạm gọi là Permission nguyên tử. Sau đây là bảng cấu tạo các Permission

Permission nguyên tử	Write	Read	List Folder Contents	Read and Excute	Modify	Full Control
Traverse Folder / Excute File			✓	✓	✓	✓
List Folder/ Read Data		✓	✓	✓	✓	✓
Read Attributes		✓	✓	✓	✓	✓
Read Extended Attributes		✓	✓	✓	✓	✓
Create Files/ Write Data	✓				✓	✓
Create Folders /Append Data	✓				✓	✓
Write Attributes	✓				✓	✓
Write Extended Attributes	✓				✓	✓
Delete Subfolder and File						✓
Delete					✓	✓
Read Permissions	✓	✓	✓	✓	✓	✓
Change Permissions						✓
Take Ownership						✓

Ý nghĩa của các Permission nguyên tử:

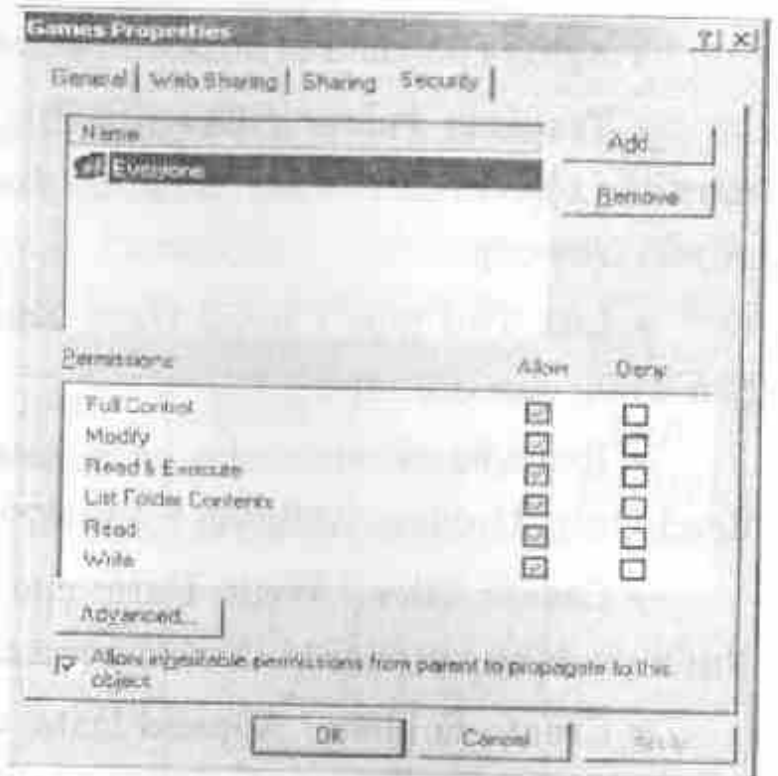
- **Traverse Folder / Execute File:** trong quá trình tìm theo cây thư mục đến tệp tin cần thiết, cho phép đi qua những thư mục mà ta không có quyền truy cập.
- **List Thư mục / Read Data:** cho phép xem tên các file và thư mục bên trong của thư mục.
- **Read Attributes:** cho phép quan sát các thuộc tính của tệp như: Read-Only, Hidden, Archive, System.
- **Create Files / Write Data:** cho phép đặt các tệp tin mới bên trong thư mục đang xét, nghĩa là có thể tạo ra, sao chép từ thư mục khác tới.
- **Create Folders / Append Data:** cho phép tạo ra các thư mục con bên trong thư mục đang xét và cập nhật thêm thông tin vào tệp data.
- **Write Attributes:** cho phép thay đổi thuộc tính các tệp.
- **Write Extended Attributes:** cho phép thay đổi các thuộc tính mở rộng của tệp.
- **Delete Subfolder and Files:** cho phép xóa các thư mục con và các tệp mặc dù không có quyền truy cập các thư mục con và tệp đó.
- **Delete:** Cho phép xóa các thư mục và tệp.
- **Read Permissions:** cho phép quan sát các Permission nhưng không được thay đổi chúng.
- **Change Permissions:** cho phép thay đổi các Permission.
- **Take Ownership:** cho phép ta chiếm quyền sở hữu đối với một tệp.

5.4. Phân bổ Permission trên File và Folder

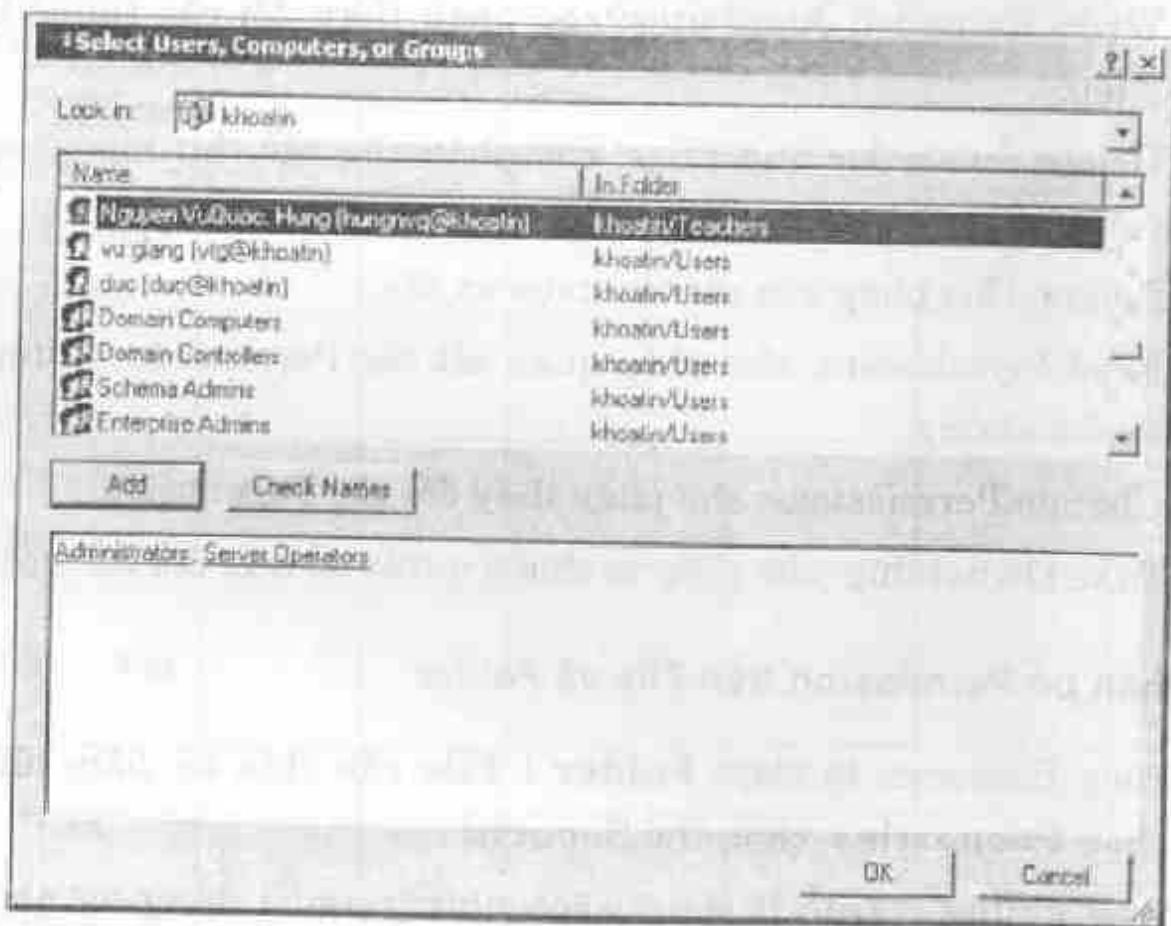
Trong Explorer, ta chọn **Folder / File** cần chia sẻ, bấm phím phải chuột, chọn **Properties**, chọn thẻ **Security**.

Trong khung **Name** là danh sách những người dùng và nhóm được quyền truy cập vào thư mục hay tệp đang xét, và khung **Permissions** bên dưới là các mức quyền tương ứng của họ. Ta thấy ở đây danh sách những Permission cấp cao như **Full Control, Read, Write...** còn nếu muốn kiểm soát đến từng Permission nguyên tử thì ta phải vào sâu thêm nữa.

Để bổ sung thêm người dùng hay nhóm vào danh sách này, ta tìm chọn những tài khoản người dùng hay nhóm cần ban quyền, bấm nút **Add**; còn để loại bỏ đi thì dùng nút **Remove**. Như trong hình vẽ dưới đây, đã có một người dùng (Administrator) và một nhóm (Server Operator) được bổ sung vào danh sách.



Hình 6.33



Hình 6.34

Để quản lý các Permission chi tiết hơn, bấm nút **Advanced** trong khung hội thoại **Properties**. Trong thẻ **Permission**, khung **Permission**

Entries sẽ cho ta thấy danh sách các nhóm và người dùng cùng với những mức quyền của họ. Tại đây ta cũng có thể bổ sung hay loại bỏ tài khoản này khỏi danh sách truy cập thư mục đang xét bằng nút **Add** hay **Remove**. Chọn một người dùng hay nhóm, bấm nút **View/Edit** ta sẽ đi vào quản lý các Permission nguyên tử của tài khoản đó.

6. CHIA SẼ MÁY IN TRÊN MẠNG

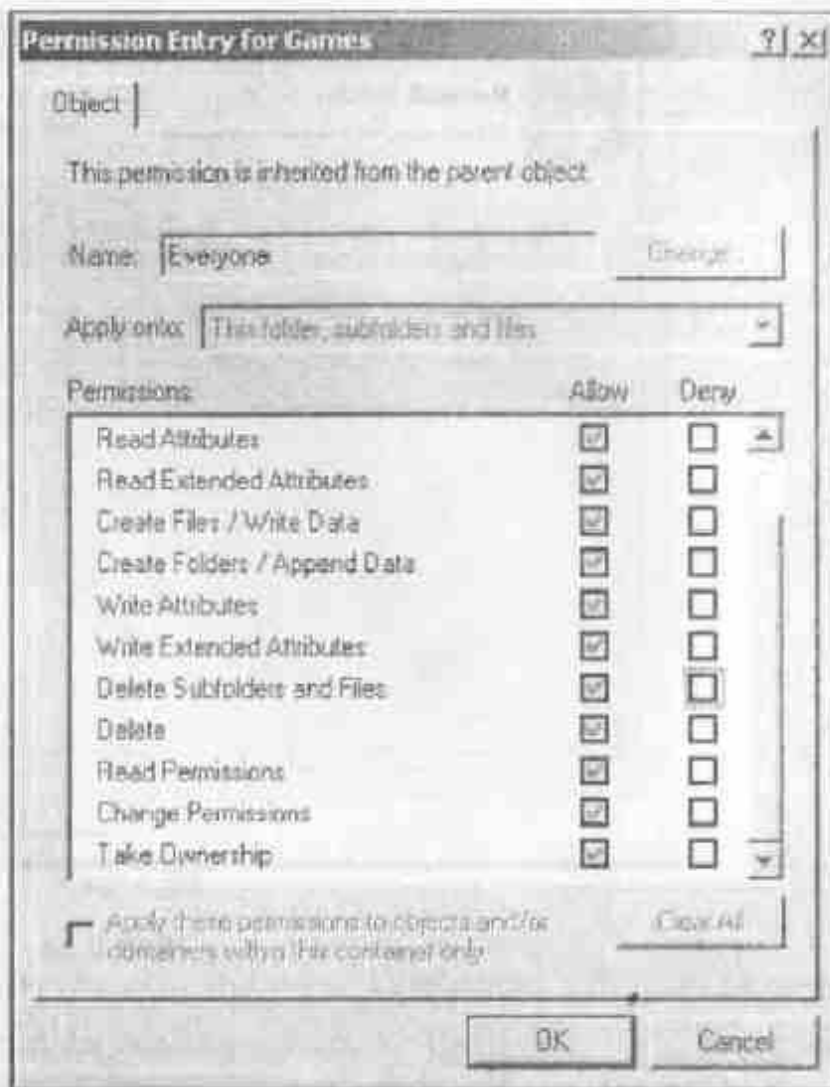
6.1. Chia sẻ máy in từ Print Server

Trong các phần trình bày sau đây, giả sử rằng chúng ta đã nắm vững cách cài đặt các thông số như công, cỡ giấy, độ đậm nhạt của chế độ in... cho một máy in cục bộ. Đây là công việc khá đơn giản và không yêu cầu hiểu biết về mạng máy tính.

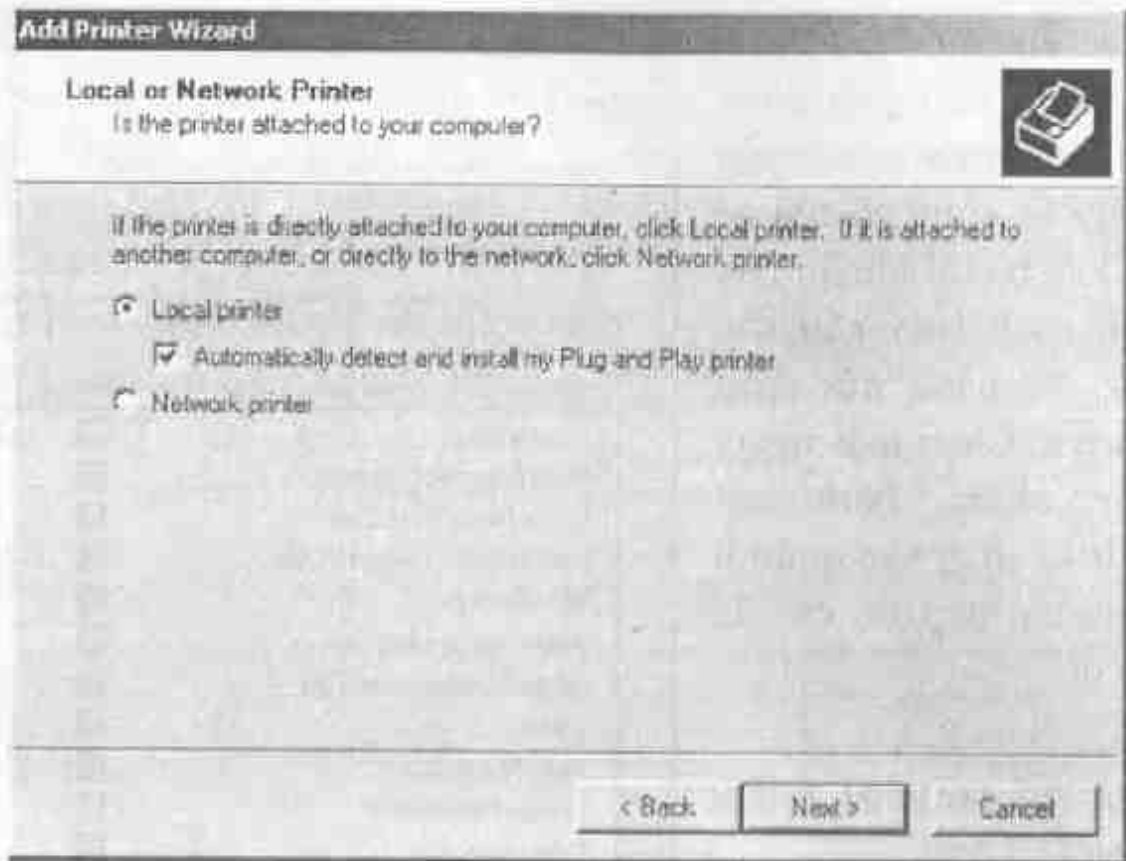
Ở đây chúng ta dùng thuật ngữ Print Server để chỉ máy tính mà trên đó cài đặt trình điều khiển máy in và nối cáp trực tiếp với máy in đó - có nghĩa là đối với máy tính đó thì máy in là cục bộ. Còn một loại Print Server nữa không xét đến ở đây, nó có dạng một card cắm vào máy in có nối cáp vào mạng hay một hộp nhỏ cắm trực tiếp vào đường truyền mạng.

Print Server của mạng Windows 2000 không nhất thiết phải cài đặt hệ điều hành này mà có thể chạy Win 9x, Windows NT hoặc thậm chí là DOS, LAN Manager hay Windows for Workgroup. Sau đây là quá trình chia sẻ máy in từ một print server Windows 2000.

Đầu tiên, ta bấm **Start / Setting / Printers**. Chọn **Add Printer**. Trong màn hình **Add Printer Wizard** bấm **Next**.



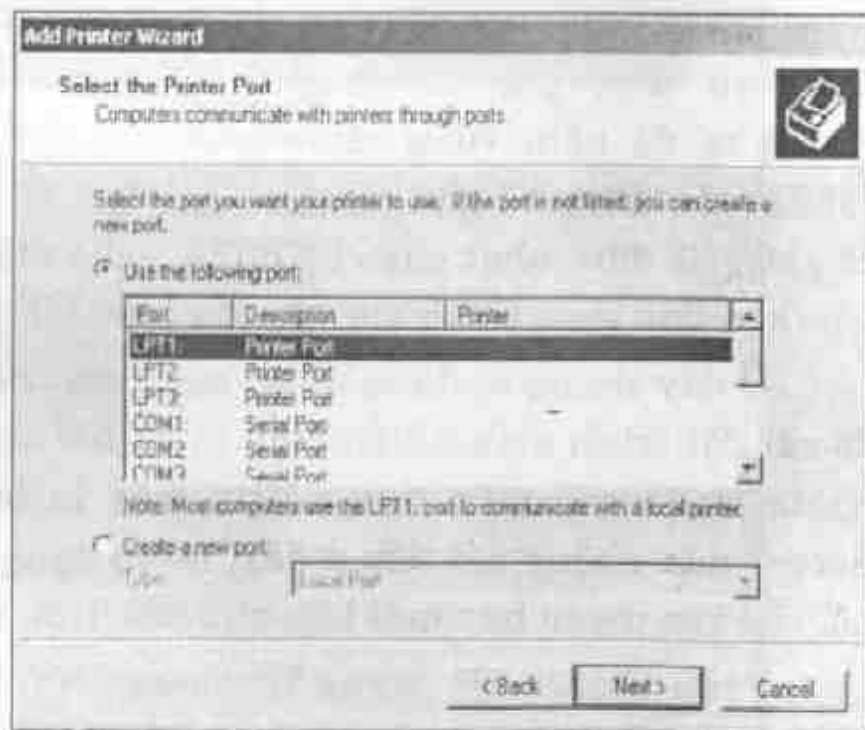
Hình 6.35



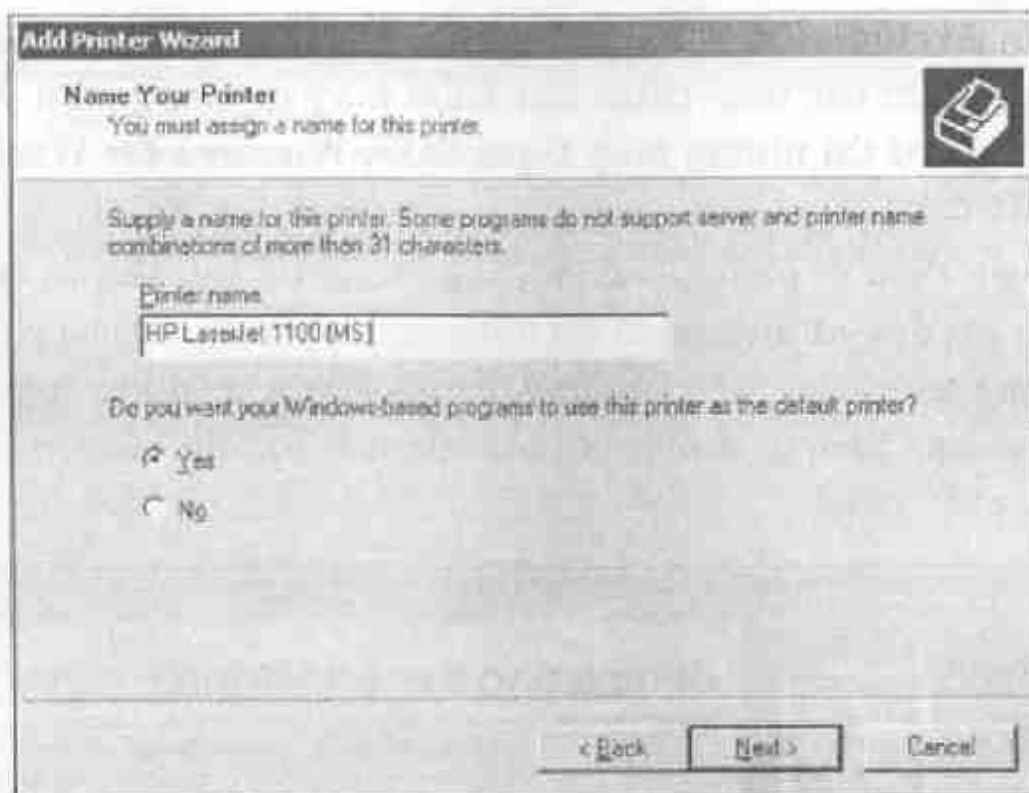
Hình 6.36

Chọn **Local printer / Next** Nếu đang dùng một máy in Plug and Play ta có thể yêu cầu Windows 2000 tự nhận diện nó bằng cách đánh dấu vào ô **Automatically detect and install my Plug and Play printer**. Trong màn hình kế tiếp ta phải chọn cổng cho máy in, thông thường là LPT 1.

Nếu không tìm thấy cổng mà ta định chọn, có thể bấm **Create new Port**.

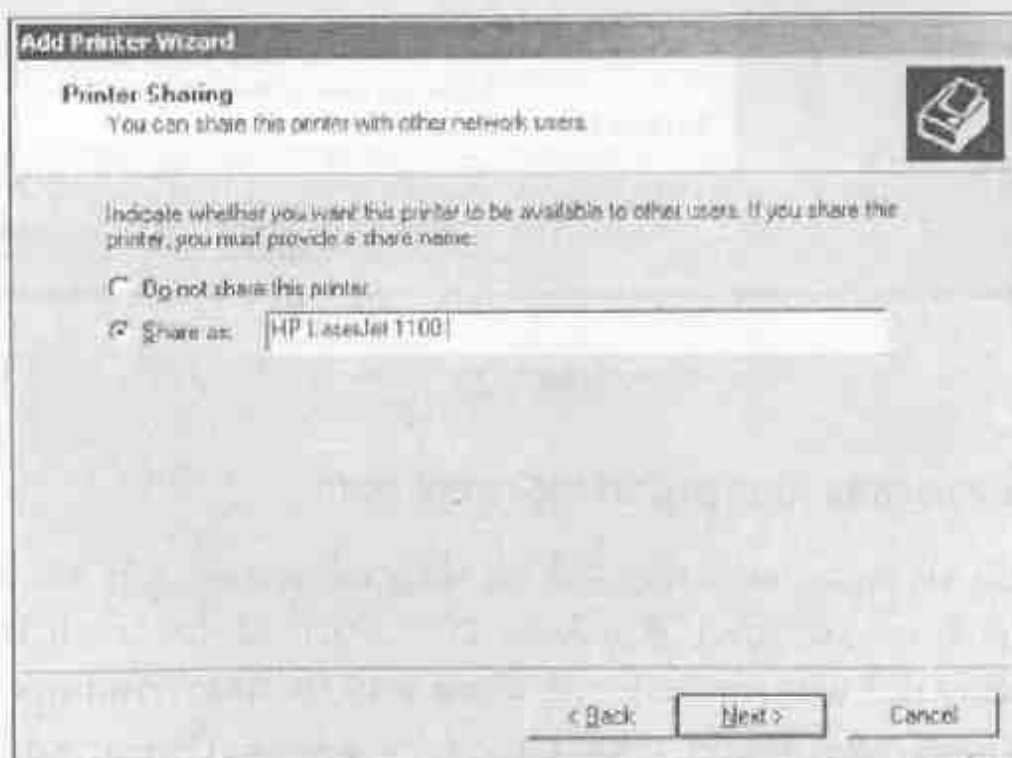


Hình 6.37



Hình 6.38

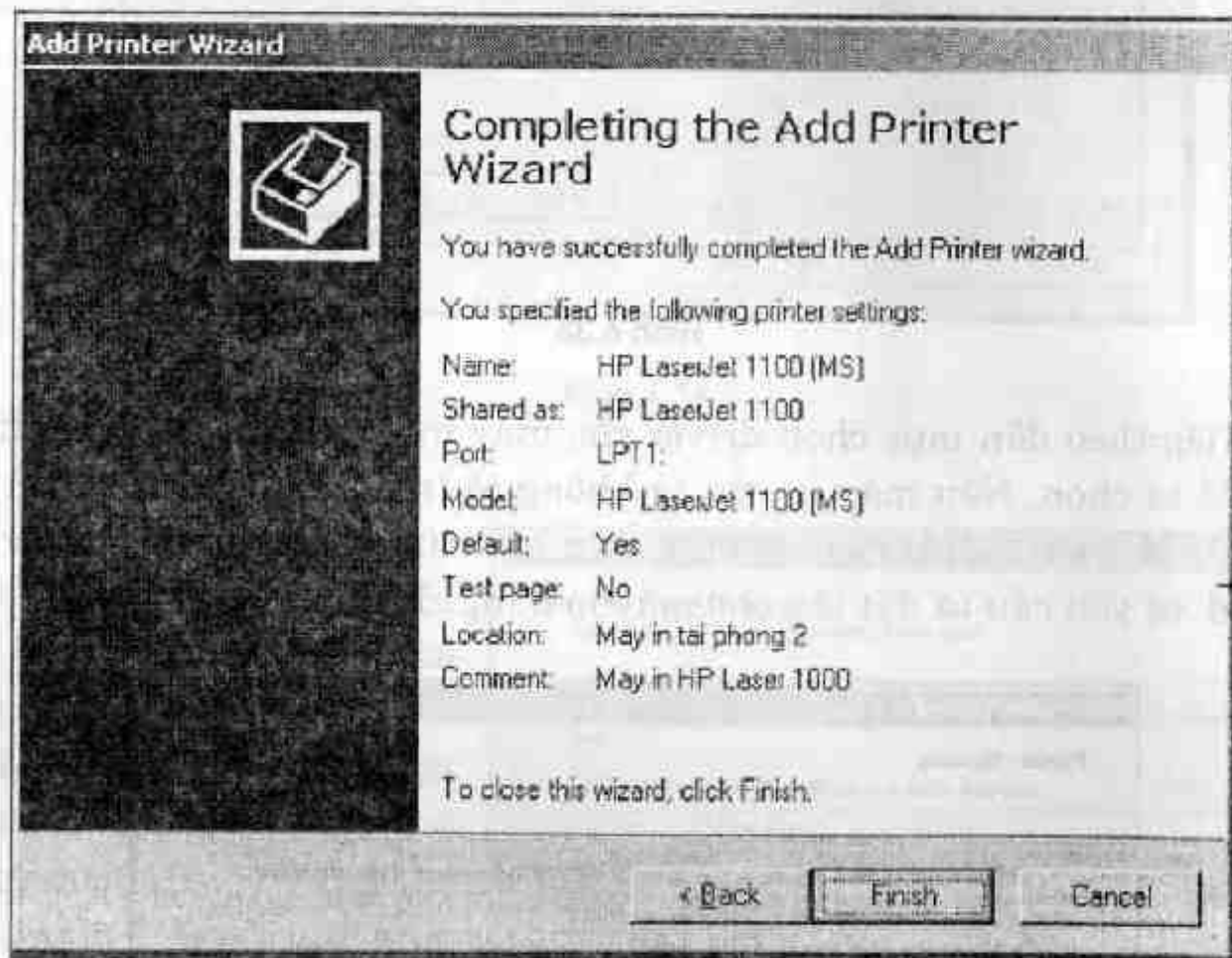
Tiếp theo đến mục chọn driver cho máy in. Windows 2000 sẽ đưa ra HCL để ta chọn. Nếu máy in của ta không có trong danh sách đó thì phải dùng OEM Driver đi kèm theo máy. Sau khi bấm **Next**, trình Add Printer Wizard sẽ yêu cầu ta đặt tên cho máy in đang chia sẻ.



Hình 6.39

Sau đó, để chia sẻ máy in trên mạng, ta cần phải đặt tên Share, tên này sẽ hiển thị khi các máy trạm tìm kiếm máy in mạng, chú ý rằng nếu tên dài quá 8 kí tự thì những máy trạm DOS, Windows for Workgroup sẽ không đọc hết được.

Bước tiếp theo ta phải gõ vào những thông tin mô tả vắn tắt về chiếc máy in đang cài đặt, ví dụ như vị trí đặt máy, loại máy in laser hay in kim ... cho các máy trạm tìm hiểu khi duyệt trên mạng. Sau khi lựa chọn có in thử trang test hay không, chúng ta kết thúc việc cài đặt máy in bằng trang thông tin tóm tắt về nó.

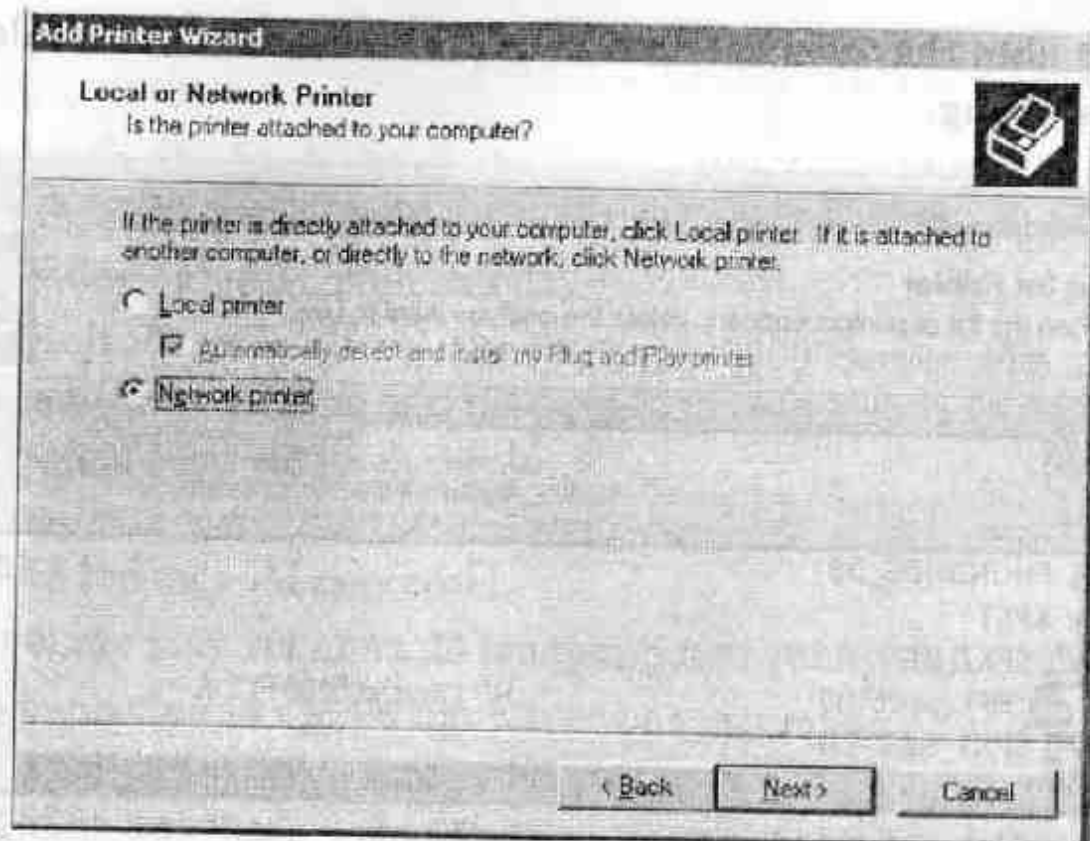


Hình 6.40

6.2. Kết nối vào máy in mạng từ một máy trạm

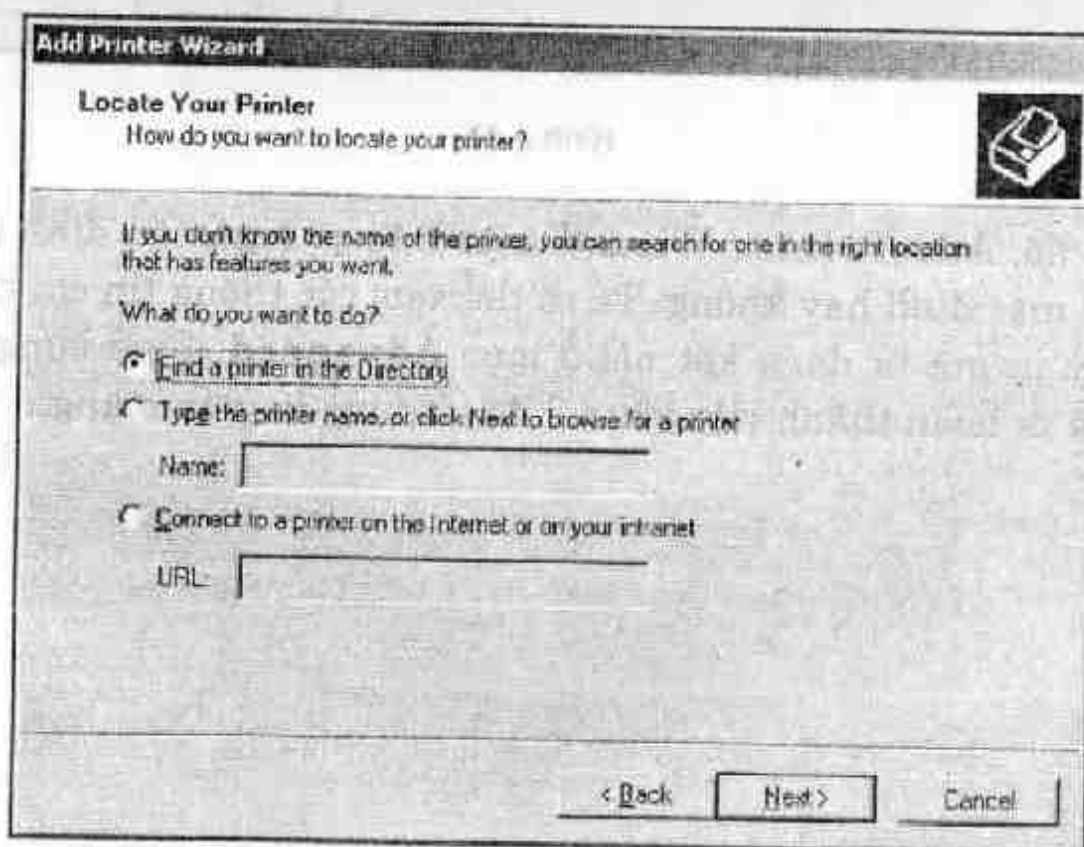
Các hình vẽ trong mục này giả sử rằng máy trạm kết nối để sử dụng máy in mạng đang sử dụng Windows 2000, tuy nhiên trình tự các bước không có gì thay đổi nếu như máy đó dùng Win 9x hay Windows NT.

Đầu tiên, ta bấm **Start / Setting / Printers**. Chọn **Add Printer**. Trong màn hình **Add Printer Wizard** bấm **Next**, sau đó chọn ô **Network printer/ Next**.



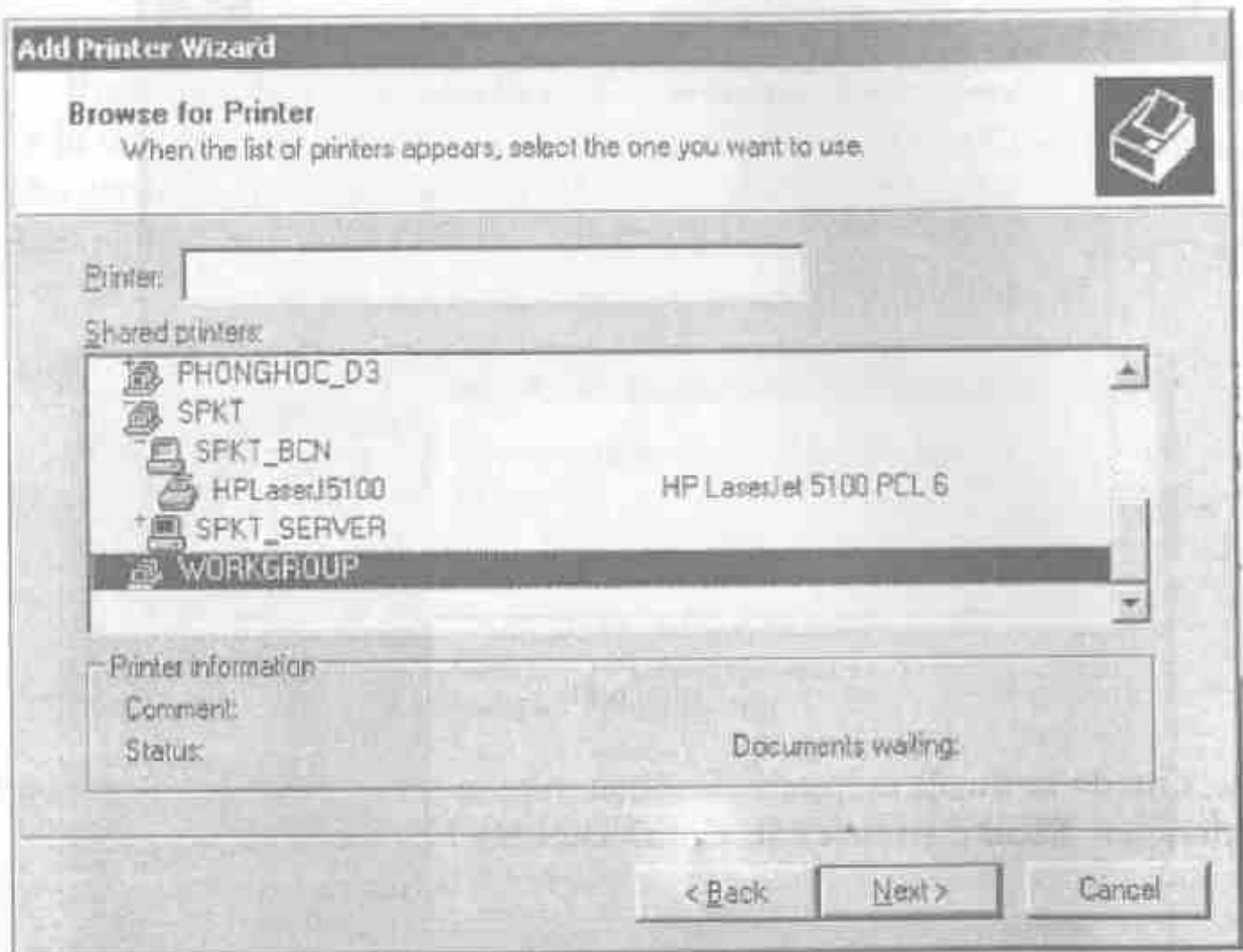
Hình 6.41

Sau đó ta duyệt mạng để tìm chọn máy in mạng thích hợp bằng cách đánh dấu ô **Find a printer in the Directory / Next.**



Hình 6.42

Ta sẽ nhìn thấy tên, vị trí và lời mô tả về các máy in hiện đang được chia sẻ trên mạng.



Hình 6.43

Sau đó, **Add Printer Wizard** sẽ hỏi ta có muốn ấn định máy in đó là máy in mặc định hay không. Ta có thể xem các thông tin chi tiết hơn về chiếc máy in mà ta đang kết nối ở mục **Advanced**. Cuối cùng bấm nút **Finish** và ta hoàn thành việc kết nối để sử dụng máy in mạng.

BÀI TẬP CUỐI CHƯƠNG

Nếu muốn vận hành thành thạo mạng Windows, không gì tốt hơn là phải tự mình bắt tay vào cài đặt và vận hành thử nó. Vì vậy chúng ta hãy thực hiện những bài thực hành sau đây.

1. Cấu hình tối thiểu để cài đặt Windows 2000 Server gồm những gì? Hãy lựa chọn cấu hình tốt nhất theo khả năng của bạn để thực hiện tiếp những công việc dưới đây.
2. Cài đặt Windows 2000 Server lên máy chủ và Windows 2000 hay Win XP lên một vài máy trạm.
3. Kết nối các máy với nhau để tạo thành mạng máy tính.
4. Tiến hành chia sẻ các tài nguyên cơ bản của mạng như: tệp, thư mục, máy in.
5. Tiến hành xây dựng miền (domain), tạo ra các tài khoản người dùng.
6. Phân chia các tài khoản theo các nhóm dựng sẵn (built-in group) và nhóm tự tạo.
7. Phân quyền truy cập các tệp và thư mục vừa chia sẻ. Quan sát các Permission nguyên tử và Permission cấp cao.

BẢNG TRA CỨU THUẬT NGỮ

A

access permission

Sự cho phép có quyền truy nhập.

account

Tài khoản người dùng mạng.

APPC – advanced program to program communication

Truyền thông cấp cao từ chương trình đến chương trình.

ARC – advance RISC computing

Tiêu chuẩn cho máy tính dùng bộ xử lí RISC

AFP – AppleTalk Filing Protocol

Giao thức quản lí tệp trên mạng của chồng giao thức AppleTalk.

agent

Phần mềm đại lí.

ANSI – American National Standards Institute

Viện tiêu chuẩn quốc gia Hoa kì.

analog

Tương tự

analog line

Đường truyền thông tin dạng tương tự.

AppleTalk

Chồng giao thức mạng của hãng Apple kèm theo hệ điều hành trên máy Macintosh.

Application layer

Tầng Ứng dụng

API – application programing interface

Giao diện chương trình ứng dụng.

Application protocol

Giao thức chương trình ứng dụng

ArcNet – Attached resource Computer Network

Một kiến trúc mạng LAN.

ATM – Asynchronnous Transfer Mode

Chế độ truyền không đồng bộ.

asynchronnous transmision

Sự truyền không đồng bộ.

AUI – Attachment Unit Interface

Bộ nối của kiến trúc mạng Ethernet, nối cáp đồng trục béo vào NIC.

B

backbone

Đường cáp trục chính.

back end

Trong ứng dụng client/server, ám chỉ chương trình chạy trên máy server.

backup

Bản sao lưu dự phòng.

BDC – backup domain controller

Hệ điều khiển vùng dự phòng.

bandwidth

Giải thông, chỉ ra khả năng chuyển dữ liệu của một đường truyền.

base I/O port

Cổng nhập xuất cơ sở.

baseband

Dải thông cơ sở.

baund

Đơn vị đo tốc độ truyền dữ liệu, chỉ một biến cố thay đổi tín hiệu.

baunde rate

Số đo tốc độ truyền dữ liệu của modem, chỉ số lượng biến cố thay đổi tín hiệu trong một giây (khác với bps).

binding

Sự liên kết.

Entries sẽ cho ta thấy danh sách các nhóm và người dùng cùng với những mức quyền của họ. Tại đây ta cũng có thể bổ sung hay loại bỏ tài khoản này khỏi danh sách truy cập thư mục đang xét bằng nút **Add** hay **Remove**. Chọn một người dùng hay nhóm, bấm nút **View/Edit** ta sẽ đi vào quản lý các Permission nguyên tử của tài khoản đó.

6. CHIA SẼ MÁY IN TRÊN MẠNG

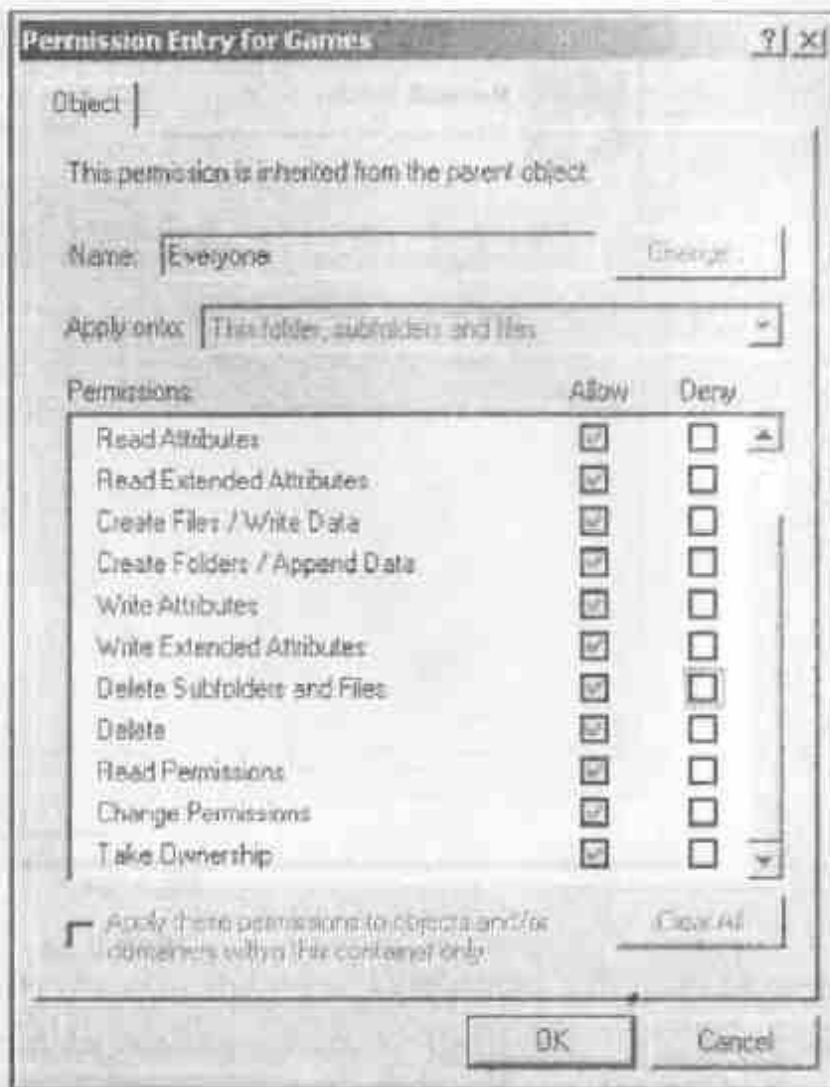
6.1. Chia sẻ máy in từ Print Server

Trong các phần trình bày sau đây, giả sử rằng chúng ta đã nắm vững cách cài đặt các thông số như công, cỡ giấy, độ đậm nhạt của chế độ in... cho một máy in cục bộ. Đây là công việc khá đơn giản và không yêu cầu hiểu biết về mạng máy tính.

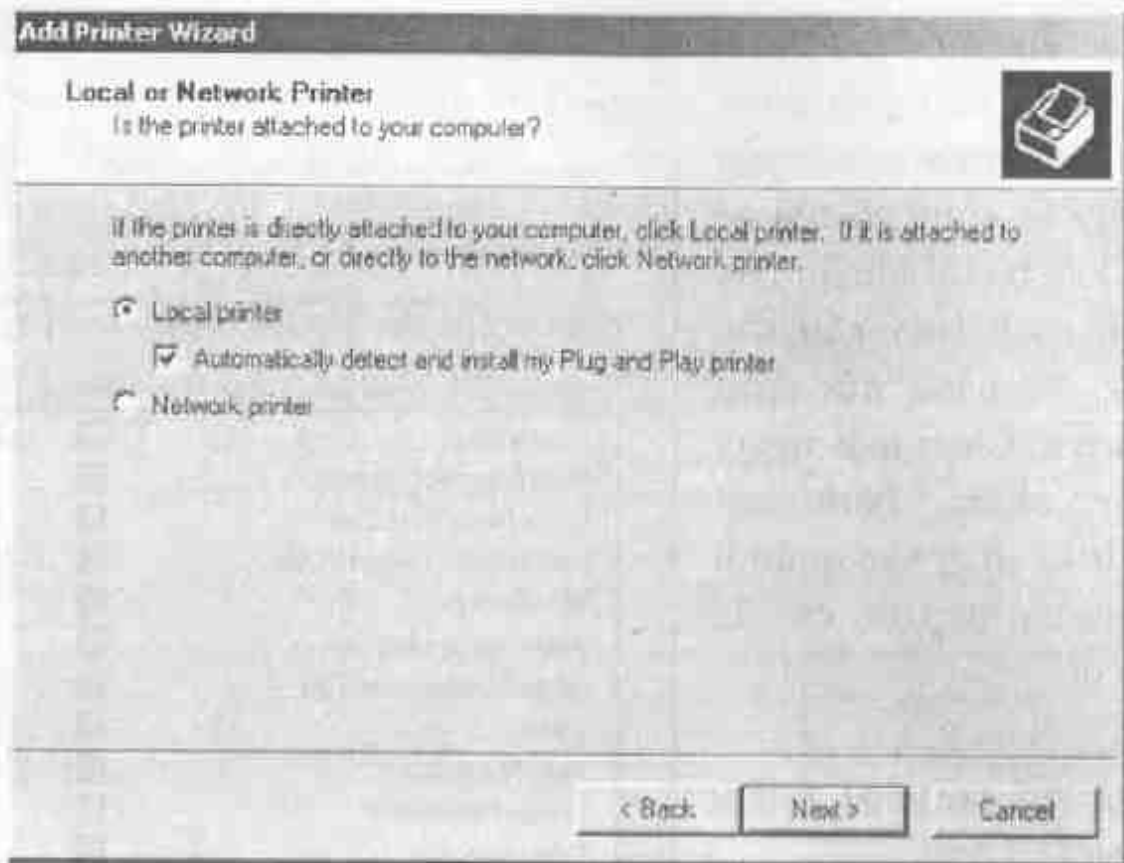
Ở đây chúng ta dùng thuật ngữ Print Server để chỉ máy tính mà trên đó cài đặt trình điều khiển máy in và nối cáp trực tiếp với máy in đó - có nghĩa là đối với máy tính đó thì máy in là cục bộ. Còn một loại Print Server nữa không xét đến ở đây, nó có dạng một card cắm vào máy in có nối cáp vào mạng hay một hộp nhỏ cắm trực tiếp vào đường truyền mạng.

Print Server của mạng Windows 2000 không nhất thiết phải cài đặt hệ điều hành này mà có thể chạy Win 9x, Windows NT hoặc thậm chí là DOS, LAN Manager hay Windows for Workgroup. Sau đây là quá trình chia sẻ máy in từ một print server Windows 2000.

Đầu tiên, ta bấm **Start / Setting / Printers**. Chọn **Add Printer**. Trong màn hình **Add Printer Wizard** bấm **Next**.



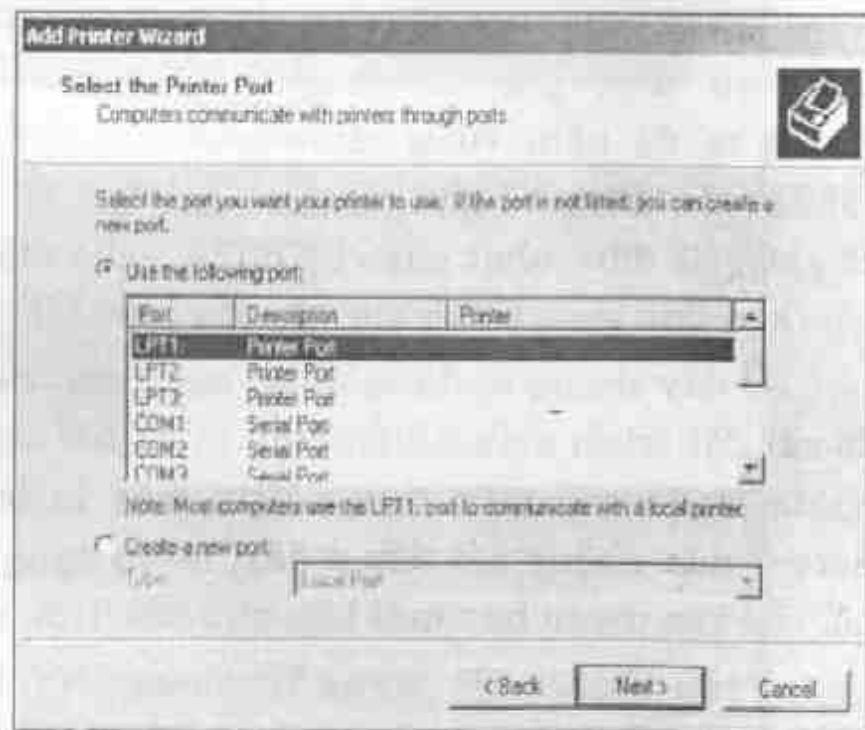
Hình 6.35



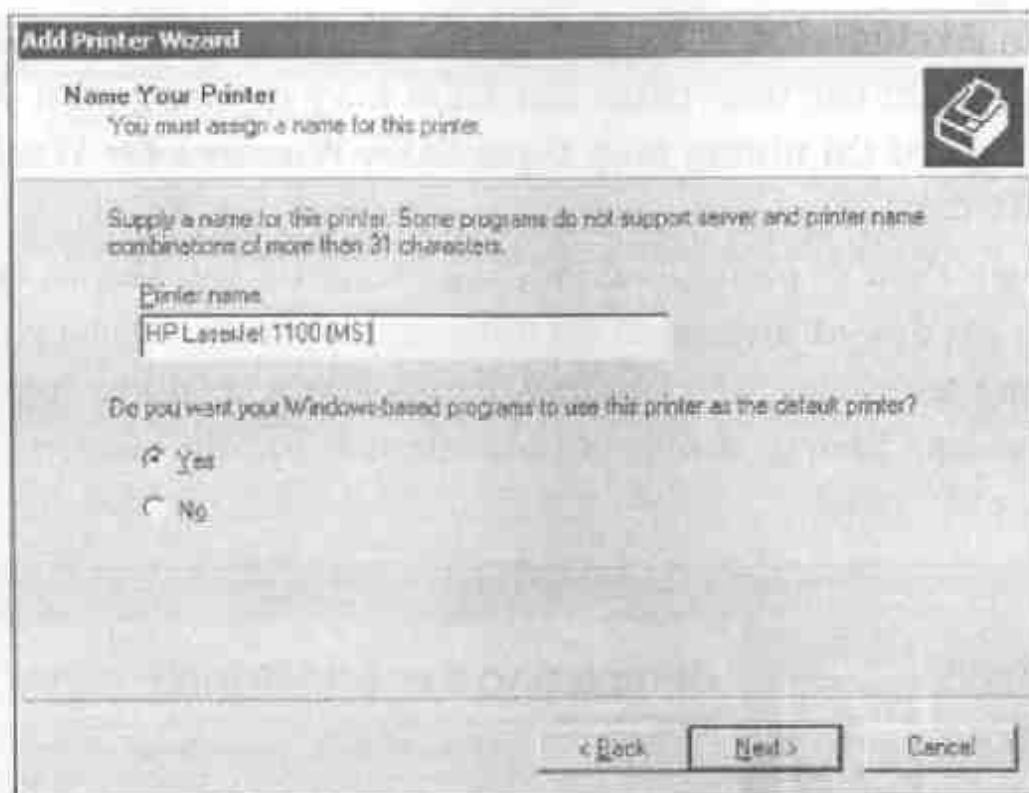
Hình 6.36

Chọn **Local printer / Next** Nếu đang dùng một máy in Plug and Play ta có thể yêu cầu Windows 2000 tự nhận diện nó bằng cách đánh dấu vào ô **Automatically detect and install my Plug and Play printer**. Trong màn hình kế tiếp ta phải chọn cổng cho máy in, thông thường là LPT 1.

Nếu không tìm thấy cổng mà ta định chọn, có thể bấm **Create new Port**.

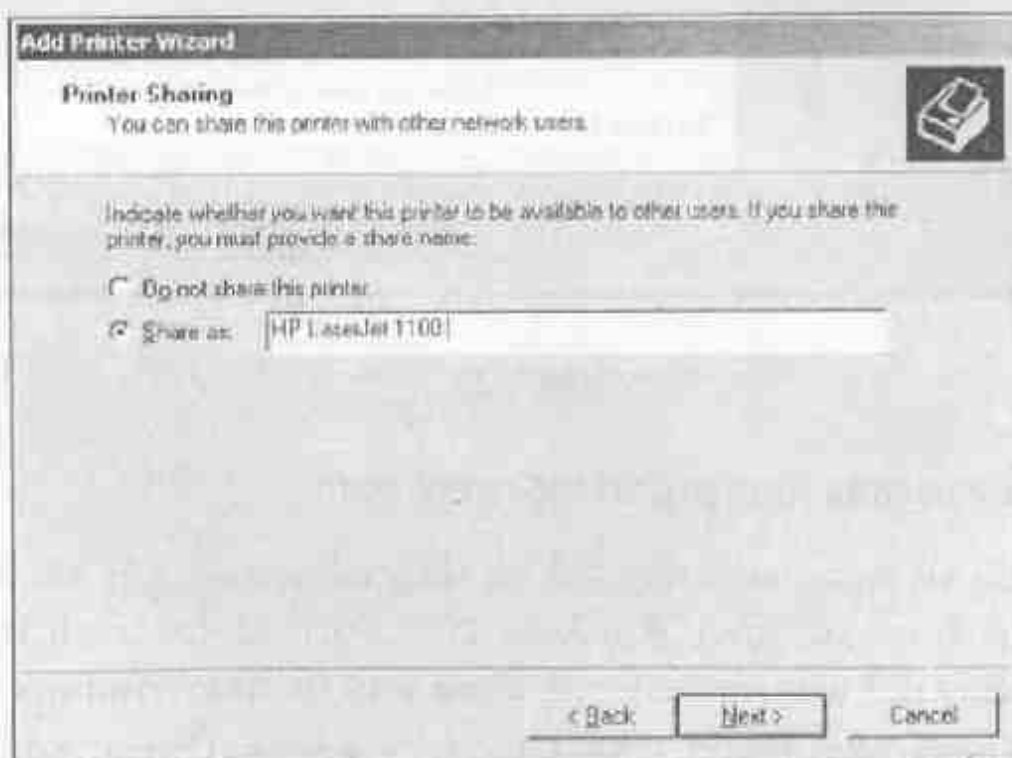


Hình 6.37



Hình 6.38

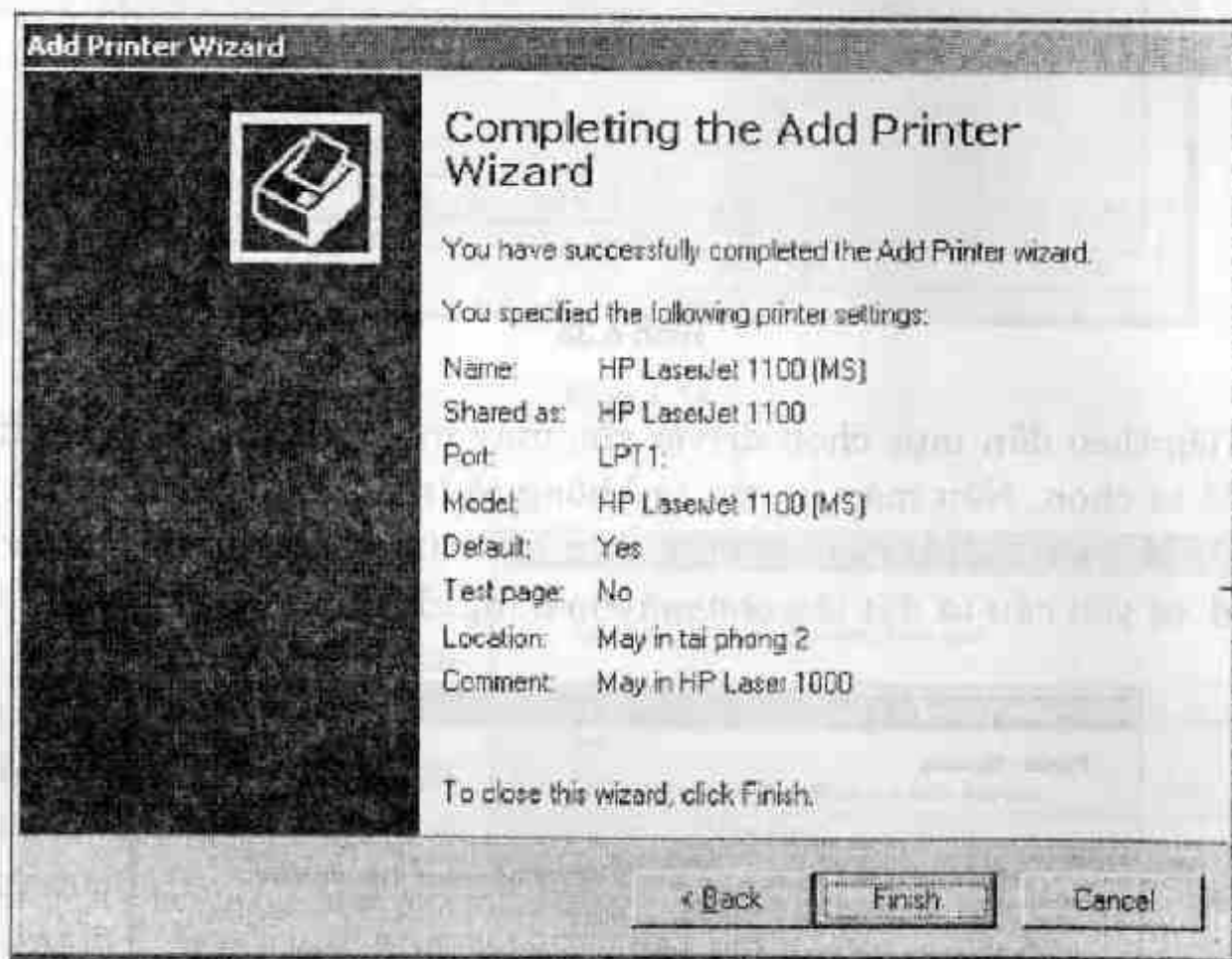
Tiếp theo đến mục chọn driver cho máy in. Windows 2000 sẽ đưa ra HCL để ta chọn. Nếu máy in của ta không có trong danh sách đó thì phải dùng OEM Driver đi kèm theo máy. Sau khi bấm **Next**, trình Add Printer Wizard sẽ yêu cầu ta đặt tên cho máy in đang chia sẻ.



Hình 6.39

Sau đó, để chia sẻ máy in trên mạng, ta cần phải đặt tên Share, tên này sẽ hiển thị khi các máy trạm tìm kiếm máy in mạng, chú ý rằng nếu tên dài quá 8 kí tự thì những máy trạm DOS, Windows for Workgroup sẽ không đọc hết được.

Bước tiếp theo ta phải gõ vào những thông tin mô tả vắn tắt về chiếc máy in đang cài đặt, ví dụ như vị trí đặt máy, loại máy in laser hay in kim ... cho các máy trạm tìm hiểu khi duyệt trên mạng. Sau khi lựa chọn có in thử trang test hay không, chúng ta kết thúc việc cài đặt máy in bằng trang thông tin tóm tắt về nó.

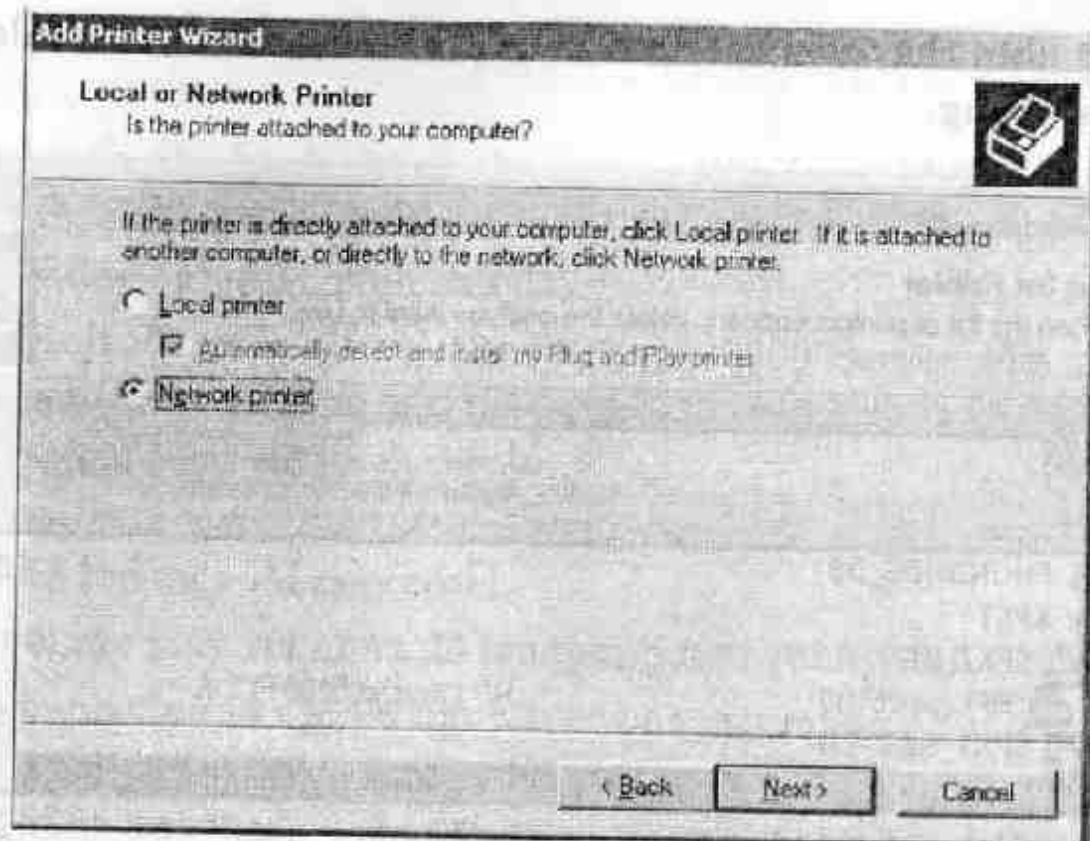


Hình 6.40

6.2. Kết nối vào máy in mạng từ một máy trạm

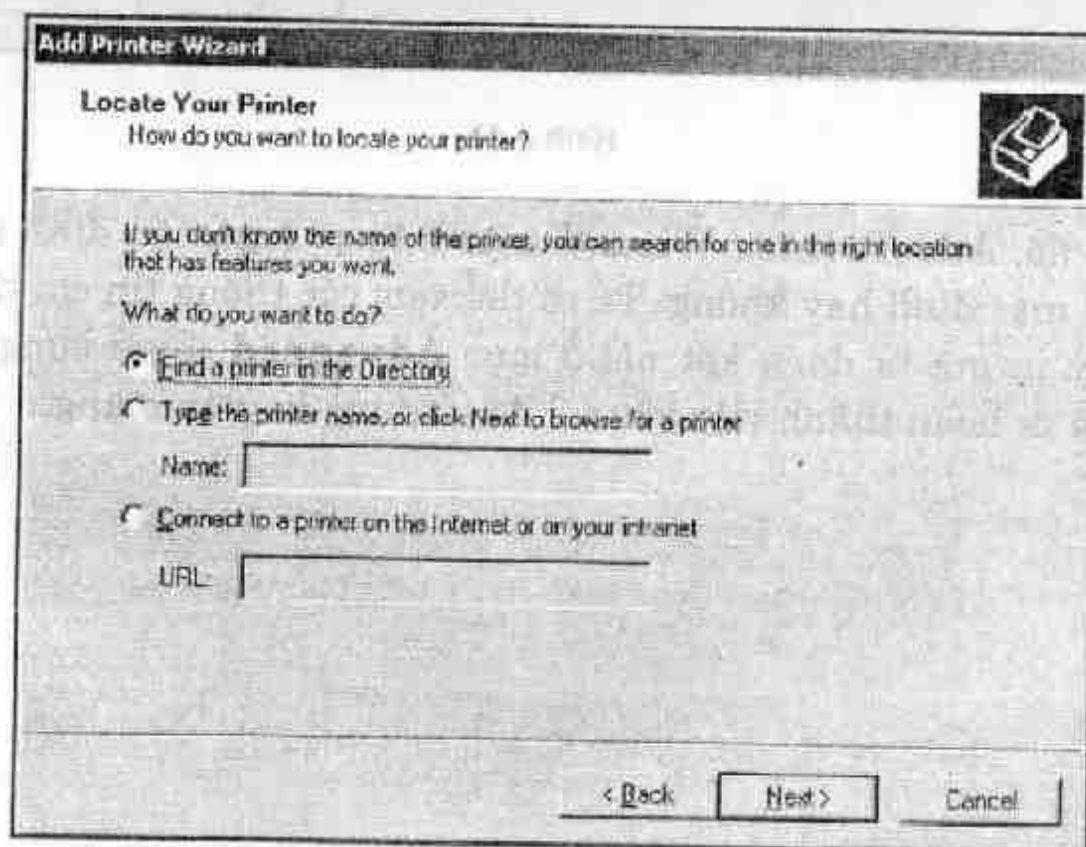
Các hình vẽ trong mục này giả sử rằng máy trạm kết nối để sử dụng máy in mạng đang sử dụng Windows 2000, tuy nhiên trình tự các bước không có gì thay đổi nếu như máy đó dùng Win 9x hay Windows NT.

Đầu tiên, ta bấm **Start / Setting / Printers**. Chọn **Add Printer**. Trong màn hình **Add Printer Wizard** bấm **Next**, sau đó chọn ô **Network printer/ Next**.



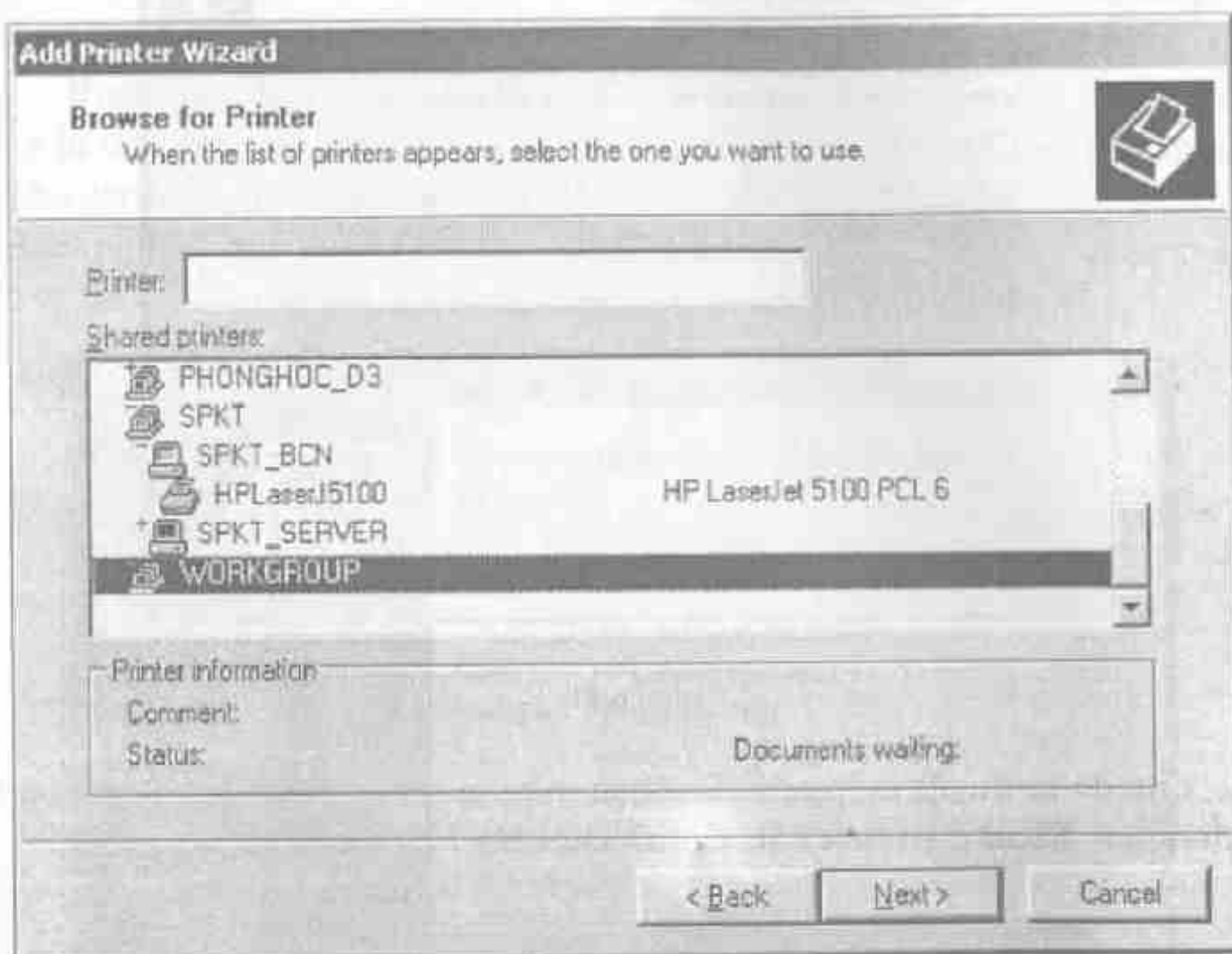
Hình 6.41

Sau đó ta duyệt mạng để tìm chọn máy in mạng thích hợp bằng cách đánh dấu ô **Find a printer in the Directory / Next.**



Hình 6.42

Ta sẽ nhìn thấy tên, vị trí và lời mô tả về các máy in hiện đang được chia sẻ trên mạng.



Hình 6.43

Sau đó, **Add Printer Wizard** sẽ hỏi ta có muốn ấn định máy in đó là máy in mặc định hay không. Ta có thể xem các thông tin chi tiết hơn về chiếc máy in mà ta đang kết nối ở mục **Advanced**. Cuối cùng bấm nút **Finish** và ta hoàn thành việc kết nối để sử dụng máy in mạng.

BÀI TẬP CUỐI CHƯƠNG

Nếu muốn vận hành thành thạo mạng Windows, không gì tốt hơn là phải tự mình bắt tay vào cài đặt và vận hành thử nó. Vì vậy chúng ta hãy thực hiện những bài thực hành sau đây.

1. Cấu hình tối thiểu để cài đặt Windows 2000 Server gồm những gì? Hãy lựa chọn cấu hình tốt nhất theo khả năng của bạn để thực hiện tiếp những công việc dưới đây.
2. Cài đặt Windows 2000 Server lên máy chủ và Windows 2000 hay Win XP lên một vài máy trạm.
3. Kết nối các máy với nhau để tạo thành mạng máy tính.
4. Tiến hành chia sẻ các tài nguyên cơ bản của mạng như: tệp, thư mục, máy in.
5. Tiến hành xây dựng miền (domain), tạo ra các tài khoản người dùng.
6. Phân chia các tài khoản theo các nhóm dựng sẵn (built-in group) và nhóm tự tạo.
7. Phân quyền truy cập các tệp và thư mục vừa chia sẻ. Quan sát các Permission nguyên tử và Permission cấp cao.

BẢNG TRA CỨU THUẬT NGỮ

A

access permission

Sự cho phép có quyền truy nhập.

account

Tài khoản người dùng mạng.

APPC – advanced program to program communication

Truyền thông cấp cao từ chương trình đến chương trình.

ARC – advance RISC computing

Tiêu chuẩn cho máy tính dùng bộ xử lí RISC

AFP – AppleTalk Filing Protocol

Giao thức quản lí tệp trên mạng của chồng giao thức AppleTalk.

agent

Phần mềm đại lí.

ANSI – American National Standards Institute

Viện tiêu chuẩn quốc gia Hoa kì.

analog

Tương tự

analog line

Đường truyền thông tin dạng tương tự.

AppleTalk

Chồng giao thức mạng của hãng Apple kèm theo hệ điều hành trên máy Macintosh.

Application layer

Tầng Ứng dụng

API – application programing interface

Giao diện chương trình ứng dụng.

Application protocol

Giao thức chương trình ứng dụng

ArcNet – Attached resource Computer Network

Một kiến trúc mạng LAN.

ATM – Asynchronnous Transfer Mode

Chế độ truyền không đồng bộ.

asynchronnous transmision

Sự truyền không đồng bộ.

AUI – Attachment Unit Interface

Bộ nối của kiến trúc mạng Ethernet, nối cáp đồng trục béo vào NIC.

B

backbone

Đường cáp trục chính.

back end

Trong ứng dụng client/server, ám chỉ chương trình chạy trên máy server.

backup

Bản sao lưu dự phòng.

BDC – backup domain controller

Hệ điều khiển vùng dự phòng.

bandwidth

Giải thông, chỉ ra khả năng chuyển dữ liệu của một đường truyền.

base I/O port

Cổng nhập xuất cơ sở.

baseband

Dải thông cơ sở.

baund

Đơn vị đo tốc độ truyền dữ liệu, chỉ một biến cố thay đổi tín hiệu.

baunde rate

Số đo tốc độ truyền dữ liệu của modem, chỉ số lượng biến cố thay đổi tín hiệu trong một giây (khác với bps).

binding

Sự liên kết.

BISDN – broadband ISDN

Mạng số dịch vụ tích hợp dải rộng (broadband Integrated Services Digital Network).

BISYNC – Binary Synchronous Communication Protocol

Giao thức truyền thông đồng bộ nhị phân.

bps – bits per second

Đơn vị đo tốc độ truyền dữ liệu của một thiết bị, chỉ số lượng bit truyền được trong một giây.

BNC – British Naval Connector

Bộ nối BNC dành cho cáp đồng trục.

bottleneck

Tác nhân gây ùn tắc, nút cổ chai.

bridge

Cầu nối.

broadband network

Mạng dải rộng.

broadcast

Truyền phát quảng bá.

brouter

Một thiết bị kết hợp cả cầu nối và bộ định tuyến (router và bridge)

built in group

Nhóm cài sẵn.

bus topology

Cấu hình mạng tuyến tính.

C

CSMA/CD – Carrier Sence Multiple Access with Collision Detection

Giao thức mạng bus, đa truy nhập cảm sóng mang dò xung đột.

CCITT – Comité Consultatif Internationale de Telegraphie et Telephonie

Ủy ban tư vấn quốc tế về điện báo và điện thoại, trụ sở đặt tại Thụy Sĩ.

central file server

Máy phục vụ tập tin trung tâm.

client

Máy khách

client/server

Môi trường mạng máy khách / máy phục vụ.

coaxial cable

Cáp đồng trục

CRC – Cyclical redundancy check

Kiểm tra vòng.

crosstalk

Nhiều xuyên âm, nhiễu từ một đường dây kế cận.

D

daisy chain

Tập hợp thiết bị kết nối thành chuỗi.

DCE - Data Communication Equipment

Thiết bị truyền thông dữ liệu.

DES – Data Ecryption Standard

Tiêu chuẩn mã hóa dữ liệu.

data frame

Khung dữ liệu

Data Link Layer

Tầng Liên kết dữ liệu.

data stream

Luồng dữ liệu

DTE – data terminal equipment

Thiết bị đầu cuối dữ liệu.

DECnet

Các sản phẩm mạng kĩ thuật số của DEC (Digital Equipment Corporation)

delicated server

Máy phục vụ chuyên dụng.

DHCP – Dynamic Host Configuration Protocol

Giao thức trong TCP/IP có khả năng quản lí và phân phối địa chỉ tĩnh và động.

digital line

Đường truyền dạng tín hiệu số.

disk duplicating

Nhân bản đĩa.

disk mirroring

Kĩ thuật nhân bản đĩa.

diskless computer

Máy tính không ổ đĩa, khởi động nhờ BOOTROM.

DIX – Digital Intel Xerox Connector

Bộ nối DIX, chính là đầu nối AUI

domain

Vùng, tập hợp máy tính và người dùng chung một cơ sở dữ liệu và được quản lí bởi một máy phục vụ vùng, một khái niệm trong Windows NT.

domain controller

Máy phục vụ điều khiển vùng trên Windows NT

downtime

Thời gian ngừng hoạt động.

driver

Chương trình điều khiển.

dumb terminal

Trạm cuối không thông minh, thiết bị không có năng lực xử lí.

duplex transmision

Truyền song công, truyền thông đồng thời cả hai chiều.

E

EISA – Enhanced Industry Standard Architecture

Kiến trúc chuẩn công nghiệp cải tiến, tiêu chuẩn cho bus 32 bit cho máy tính x86, ra đời năm 1988.

Ethernet

Mạng cục bộ (LAN) do Xerox phát triển năm 1976, dùng cấu hình tuyến tính.

F

FDDI – Fiber Distributed Data Interface

Giao diện phân phối dữ liệu qua cáp quang, tốc độ truyền 100Mbps.

FTAM – File Transfer Access and Management

Một giao thức truy cập tập tin.

FTP – File Transfer Protocol

Giao thức chuyển tệp.

fire wall

Trạm kiểm soát, bức tường lửa. Một chương ngại nhằm sàng lọc thông tin.

flow control

Điều khiển luồng thông tin.

frame

Khung dữ liệu.

frame relay

Công nghệ chuyển gói tin theo dạng số. Đây là hệ thống từ điểm đến điểm sử dụng mạch ảo truyền các frame có độ dài thay đổi.

front end

Trong ứng dụng client/server ám chỉ một chương trình chạy trên máy khách.

G

gateway

Cổng giao tiếp, thiết bị dùng để nối các mạng sử dụng các giao thức khác nhau.

global group

Nhóm toàn cục để quản lý người dùng trong Windows NT.

gopher

Hệ thống tìm kiếm tài liệu phân tán trên Internet.

group

Tài khoản nhóm, khái niệm trong mạng Windows.

groupware

Chức năng hỗ trợ đa xử lý giữa nhiều người dùng trên mạng.

H

handshaking

Xác nhận thiết lập quan hệ.

HCL – Hardward Compatibiliti List

Danh sách phần cứng tương thích.

HDLC – High-Level Data Link Control

Giao thức điều khiển liên kết dữ liệu mức cao.

hop

Việc truyền gói dữ liệu qua một bộ định tuyến.

hot fixing

Sửa chữa tức thời.

HTML – Hypertext Markup Language

Ngôn ngữ đánh dấu văn bản đa năng (siêu văn bản).

HTTP – Hypertext Transport Protocol

Giao thức chuyển tải văn bản đa năng, dùng để chuyển tải các trang World Wide Web qua mạng.

hub

Thành phần kết nối trung tâm.

I

IDE – Integrated Device Electronics

Bộ điện tử tích hợp vào thiết bị.

IEEE – Institute of Electrical and Electronics Engineers

Viện Công nghệ Điện và Điện tử.

IEEE Project 802

Mô hình nối mạng do IEEE thiết kế (sinh ra vào 2/1980) định nghĩa các tiêu chuẩn LAN cho tầng Vật lý và Liên kết dữ liệu, chia Data Link thành hai tầng con Media Access Control (MAC) và Logical Link Control (LLC)

ISA – Industry Standard Architecture

Kiến trúc tiêu chuẩn công nghiệp.

ISDN – Integrated Services Digital Network

Mạng số dịch vụ tích hợp.

Intermediate system

Hệ thống trung gian, chỉ một tập hợp các cầu nối, bộ định tuyến, cổng giao tiếp, ...

ISO – International Standards Organization

Tổ chức tiêu chuẩn hóa quốc tế.

IP – Internet Protocol

Giao thức TCP/IP

IPX/SPX – Internetwork Packet Exchange/Sequenced Packet Exchange

Chống giao thức được dùng trong mạng Novell. IPX giao thức gửi gói dữ liệu và định tuyến. SPX giao thức gửi dữ liệu hướng nối kết, đảm bảo giao dữ liệu tận nơi. NWLink là ứng dụng của hai giao thức này của Microsoft.

IRQ – Interrupt request

Yêu cầu ngắt.

L

LAN – Local Area Network

Mạng cục bộ

LAT – Local Area Transport

Vận chuyển cục bộ.

link

Liên kết.

local group

Nhóm cục bộ, khái niệm của Windows NT chỉ các tài khoản của mỗi trạm.

LocalTalk

Thành phần cáp mạng trong mạng AppleTalk

LLC – Logical Link Control

Tầng con LLC, một tầng con tương ứng nằm trong tầng Data Link của mô hình OSI. (xem IEEE 802).

M

MIB – Management Information Base

Cơ sở thông tin quản lí, cơ sở dữ liệu chứa thông tin mọi tài nguyên mạng.

MAU (MSAU) – Multistation Access Unit

Thiết bị truy nhập đa trạm.

MAC driver – Media Access Control driver

Trình điều khiển thiết bị bố trí tại tầng con MAC của mô hình OSI, còn gọi là trình điều khiển NIC.

MAC sublayer - Media Access Control sublayer

Tầng con MAC, một tầng con nằm trong tầng Liên kết dữ liệu của mô hình OSI, chịu trách nhiệm giao tiếp với card mạng và chuyển giao dữ liệu giữa hai máy tính trên mạng.

medium

Phương tiện truyền dẫn.

mesh network topology

Sơ đồ mạng lưới ở mạng WAN. Mạng lưới dùng bộ định tuyến tìm kiếm lộ trình thích hợp nhất tại thời điểm cụ thể.

Micro Channel Architecture

Kiến trúc vi kênh. Một kiến trúc BUS trong máy PS/2

MNP – Microcom Network Protocol

Giao thức mạng Microcom điều khiển lỗi dữ liệu không đồng bộ do Microcom System Inc. phát triển, thường được sử dụng điều khiển modem.

Mpbs – Millions of bits per second

Đơn vị đo tốc độ truyền tin trên cáp đồng trục, cáp xoắn đôi và cáp quang.

modem

Thiết bị truyền thông cho phép máy tính truyền tin qua đường điện thoại chuẩn, đây là thiết bị chuyển đổi tương tự – số.

MUX – Multiplexer

Bộ dồn kênh.

multitasking

Chế độ hoạt động đa nhiệm.

N

NBP – Name Binding Protocol

Giao thức liên kết tên, một giao thức của hãng Apple, giao thức này hoạt động tại tầng Giao vận của mô hình OSI.

NCP – NetWare Core Protocol

Giao thức của hãng Novell dùng cho các hệ điều hành Novell NetWare.

NDIS – Network Device Interface Specification

Quy cách giao diện thiết bị mạng, nó định nghĩa một giao diện truyền thông giữa tầng con MAC với các trình điều khiển giao thức. NDIS cung cấp đặc tính cho phép nhiều chồng giao thức được sử dụng cùng lúc.

NetBEUI - NetBIOS Extended User Interface

Giao thức kèm theo mọi sản phẩm mạng của Microsoft, giao thức có ưu điểm chạy trên máy tính dùng MSDOS, dùng trên LAN, không hỗ trợ định tuyến, chỉ chạy trên mạng của Microsoft.

NetBIOS – Network Basic Input/Output System

Một API được chương trình ứng dụng sử dụng trên LAN.

network

Mạng máy tính.

network analyzer

Công cụ phân tích mạng dùng để dò tìm và xử lý lỗi trên mạng.

NIC – Network Interface Card hoặc Network adapter card

Card mạng, card mở rộng dùng để nối máy tính với mạng LAN.

network layer

Tầng Mạng (mô hình OSI).

network monitor

Bộ giám sát mạng.

node

Điểm nối kết, nút mạng (máy trạm, máy phục vụ, bộ chuyển tiếp, ...)

noise

Nhiều.

O

ODI – Open Data Link Interface

Giao diện liên kết dữ liệu mở, một tiêu chuẩn do Novell và Apple định nghĩa, cho phép sử dụng nhiều cổng giao thức cùng lúc.

OSPF – Open Shortest Path First

Thuật toán tình trạng liên kết có nguồn gốc từ giao thức định tuyến nội vùng.

OSI – Open Systems Interconnection reference model

Mô hình tham chiếu mạng hệ thống mở (mô hình kiến trúc mạng 7 tầng).

Optical fiber

Sợi quang, phương tiện truyền dẫn tín hiệu số của dữ liệu bằng xung ánh sáng.

P

packet

Gói tin (bó tin), đơn vị thông tin để truyền đi trên mạng.

PAD – Packet assembler/disassembler

Bộ tách / ghép gói tin.

packet switching

Chuyển gói.

PDL – Page description language

Ngôn ngữ mô tả trang in, định nghĩa hình dạng cuối cùng của trang in.

pariti

Thủ tục kiểm lỗi chẵn lẻ.

partition

Phân khu trên đĩa cứng, phần này hoạt động như đơn vị độc lập vật lí.

PBX - Private Branch Exchange (PABX - Private Automated Branch Exchange)

Mạng chuyển đổi dùng đường truyền tiếng nói hoặc dữ liệu.

PDA - Personal Digital Assitant

Một loại máy tính cầm tay, mọi chương trình trên nó đều được cứng hóa.

PDC - Primary Domain Controller

Hệ điều khiển vùng chính.

PDN - Public Data Network

Dịch vụ chuyển mạch hoặc chuyển gói qua mạng điện thoại công cộng.

peer-to-peer network

Mạng ngang hàng.

PVC - Permanent Virual Circuit

Mạch ảo thường trực, tương tự đường thuê bao, tuy nhiên chỉ phải trả tiền cho khoảng thời gian sử dụng đường truyền, dùng trong dịch vụ ATM và frame relay.

physical layer

Tầng Vật lí (trong mô hình OSI)

piercing tab

Bộ nối xuyên lỗ, một dàn kim xuyên qua lớp cách điện tiếp xúc với lõi dây dẫn.

point-to-point

Từ điểm đến điểm, một loại mạch chuyên dụng, còn gọi là đường truyền riêng (thuê bao).

Presentation layer

Tầng Biểu diễn thông tin (mô hình OSI)

Project 802

Các định nghĩa của IEEE trên các tầng mạng.

protocol

Giao thức.

protocol driver

Chương trình điều khiển giao thức.

punchdown block

Một terminal, chuỗi terminal mà cáp có thể cắm vào (hộp đầu cắm cáp) giá phân phối (patch panel).

R

RAID – Redundant Arrays of Inexpensive Disk

Sự tiêu chuẩn hóa các tùy chọn dung lỗi theo 5 cấp độ.

redirector

Bộ chuyển hướng, phần mềm mạng tiếp nhận yêu cầu nhập xuất các tệp ở xa, sau đó đổi hướng đi của chúng và gửi đến một dịch vụ mạng thích hợp.

repeater

Bộ chuyển tiếp.

requester (LAN requester)

Phần mềm thường trú gửi yêu cầu cung cấp dịch vụ mạng đến một máy server thích hợp.

resource

Tài nguyên mạng.

RG-58 A/U

Cáp đồng trục gây lỗi bện.

RG-58 /U

Cáp đồng trục gây lỗi đặc.

right

Đặc quyền, quyền. Quyền cho phép người sử dụng có quyền thi hành những hoạt động nhất định trong hệ thống (khác với sự cho phép – permission).

ring topology

Cấu hình mạng vòng.

RIP – Routing Information Protocol

Giao thức thông tin định tuyến.

RJ-11

Bộ nối môđun 4 dây, dùng để nối đường truyền điện thoại với một thiết bị truyền thông.

RJ-45

Bộ nối môđun 8 dây, dùng để nối cáp xoắn với NIC.

router

Bộ định tuyến.

RS-232 standard

Tiêu chuẩn RS-232 là một tiêu chuẩn công nghiệp cho các kết nối truyền thông được xây dựng bởi Hiệp hội các ngành công nghiệp điện tử (EIA).

S

SAP – Service Access Point

Điểm truy cập dịch vụ. Giao diện giữa mỗi tầng (OSI) có các điểm nối kết dùng để giao tiếp giữa mỗi tầng.

SDLC – Synchronous Data Link Control

Điều khiển liên kết dữ liệu đồng bộ.

sector sparing

Hệ dung lỗi còn được gọi là hot fixing (sửa chữa tức thời), hệ này có khả năng phục hồi sector cho tệp tin trong quá trình hoạt động

segment

Phân đoạn mạng, chiều dài cáp giữa hai điểm kết thúc trên mạng.

server

Máy phục vụ.

server-based network

Mạng máy tính dựa trên máy phục vụ.

SMB – Server Message Block

Khối thông điệp máy phục vụ. Một giao thức của Microsoft, Intel và IBM.

session

Phiên làm việc.

Session layer

Tầng Phiên.

session management

Quản lý phiên làm việc.

shell

Phần mềm cung cấp khả năng truyền thông trực tiếp giữa người dùng và hệ điều hành. Chẳng hạn Program Manager trong Windows.

STP - Shielded Twisted-Pair

Cáp xoắn đôi có lớp bảo vệ.

shielding

Vỏ lưới bảo vệ cáp.

signal bounce

Đội tín hiệu.

SNMP – Simple Network Management Protocol

Giao thức quản lý mạng đơn giản.

SMDS – Switched Multimegabit Data Services

Dịch vụ chuyển gói cao tốc, tốc độ lên tới 34 Mbps.

SMP – Symetric Multiprocessing

Đa xử lý đối xứng.

SNA – Systems Network Architecture

Kiến trúc mạng hệ thống do IBM xây dựng.

SMTP – Simple Mail Transfer Protocol

Một giao thức chương trình ứng dụng thuộc TCP/IP dùng để chuyển e-mail.

SONET – Synchronous Optical Network

Mạng quang đồng bộ. Công nghệ sợi quang có thể truyền dữ liệu đến 1GB/s.

STA – Spanning Tree Algorithm

Thuật toán dạng cây mở rộng, thuật toán này loại bỏ các tuyến thừa trong một liên mạng.

stand-alone computer

Máy tính độc lập, không là thành viên của mạng.

star topology

Cấu hình mạng sao.

SVCs – Switched Virtual Circuit

Mạch ảo chuyển mạch. Một kết nối giống Point to Point

T

T connector

Bộ nối cáp đồng trục hình chữ T.

T1 service

T1 là dịch vụ đường truyền dạng số chuẩn, tốc độ truyền đến 1.544 Mbps.

tap

Một kết nối với mạng, ám chỉ nối kết với đường cáp.

TCP – Transmission Control Protocol

Giao thức TCP/IP dành cho truyền dữ liệu tuần tự.

TCP/IP - Transmission Control Protocol/Internet Protocol

TCP/IP là chồng giao thức tiêu chuẩn công nghiệp cung cấp các cuộc truyền thông trong môi trường không đồng nhất. TCP/IP cung cấp một giao thức có định tuyến và có khả năng truy nhập các tài nguyên trên Internet.

TDR – time-domain reflectometer

Công cụ dò và xử lý lỗi, có nhiệm vụ gửi các xung siêu âm dọc theo đường cáp nhằm tìm một chỗ đứt.

Telnet

Giao thức thuộc TCP/IP dùng để đăng nhập máy chủ từ xa.

terminator

Điện trở cuối, bộ nối cuối. Thiết bị nhằm chặn tín hiệu phản hồi trên đường cáp Ethernet.

terminator resistance

Mức trở kháng trong terminator, đo bằng Ohm, phải khớp với kiến trúc mạng.

thicknet

Cáp đồng trục dày (cáp béo) của Ethernet.

thinnet

Cáp đồng trục mảnh (cáp gầy) của Ethernet

throughput

Năng suất truyền. Tốc độ truyền tải dữ liệu qua một nối kết.

token

Thẻ bài.

token passing

Chuyển thẻ bài.

token ring network

Mạng vòng chuyển thẻ bài.

topology

Lược đồ mạng, sơ đồ mạng, cấu hình mạng.

transceiver

Máy thu phát. Một thiết bị nối máy tính với mạng.

Transport layer

Tầng Giao vận (mô hình OSI)

transport protocols

Các giao thức vận tải.

trust relationship

Quan hệ ủy quyền.

twisted-pair cable

Cáp xoắn đôi.

U

UART – Universal Asynchronous Receiver Transmitter.

Máy thu phát đa năng không đồng bộ.

URL – Uniform Resource Locator

Thông tin định vị tài nguyên đồng dạng (tức địa chỉ Web). URL được sử dụng trong nhiều giao thức khác nhau như FTP, http hoặc gopher.

UPS – Uninterruptible Power Supply

Nguồn cung cấp điện liên tục.

UTP - Unshielded Twisted-Pair

Cáp xoắn đôi trần (không có lớp bảo vệ)

user account

Tài khoản người dùng.

V

vampire tap (piercing tap)

Bàn kẹp xuyên qua lớp bảo vệ tiếp xúc với lõi dây.

virtual circuit

Mạch ảo.

W

WAN – Wide Area Network

Mạng diện rộng.

workgroup

Nhóm làm việc.

WWW – World Wide Web

WWW là một loại dịch vụ đa phương tiện của Internet.

X

X.25

Tập hợp tiêu chuẩn do CCITT xây dựng, nó định nghĩa kết nối giữa một terminal và mạng chuyển gói.

X.400

Giao thức dành cho các cuộc truyền e-mail quốc tế do CCITT ban hành.

X.500

Giao thức dành cho việc duy trì tập tin và thư mục ngang qua nhiều hệ thống, do CCITT ban hành.

XNS – Xerox Network System

Giao thức dành cho mạng cục bộ Ethernet của Xerox.

Z

zone

Khu vực, một đơn vị quản lý của mạng LocalTalk.

TÀI LIỆU THAM KHẢO

1. Tanenbaum A.S. *Computer Network*. Prentice Hall, 1996.
2. Matthew F.A. *Inside TCP/IP*. New Rider Publishing, 1997.
3. Microsoft. *Windows 2000 Server User Guide*. 2001.
4. Phạm Mạnh Dũng - Hoàng Đức Hải. *Làm chủ Microsoft Windows 2000 Server*. 3 tập. NXB Thống kê, 2004.
5. VNGuide. *Mạng căn bản*. NXB Thống kê, 1998.
6. Nguyễn Thúc Hải. *Mạng máy tính và các hệ thống mở*. NXB Giáo dục, 1997.
7. Nguyễn Gia Hiếu. *Mạng máy tính*. NXB Giáo dục, 1998.
8. Nguyễn Tiến - Đặng Xuân Hường - Nguyễn Văn Hoài. *Giáo trình căn bản về mạng*. NXB Giáo dục, 1999.

Chịu trách nhiệm xuất bản:

Giám đốc ĐINH NGỌC BẢO

Tổng biên tập LÊ A

Người nhận xét:

TS NGUYỄN MẠNH HÙNG

TS TRẦN CÔNG NHƯỢNG

Biên tập nội dung:

VŨ THỊ MINH LUẬN

Kỹ thuật vi tính:

VŨ ANH TUẤN

Trình bày bìa:

PHẠM VIỆT QUANG

MẠNG MÁY TÍNH

In 3100 cuốn, khổ 17x24cm tại Nhà in Hồ Nội.

Giấy phép xuất bản số: 156 – 452/XB – QLXB, kí ngày 1/4/2005.

In xong và nộp lưu chiểu tháng 9 năm 2005.